P3F1-0450-02

PRIMERGY

PRIMERGY SSLAccelerator 7110/7115

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。

2001 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 7115 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、雷によっては装置を破壊し、火災の原因となります。

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

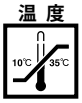
- **装置を移動する場合は、必ず電源プラグをコンセントから抜いてください。また、電源ケーブルなどもはずしてください。作業は足元に十分注意して行ってください。電源ケーブルが傷つき、火災・感電の原因となったり、装置が落ちたり倒れたりしてけがの原因となります。**
- **長時間装置を使用しないときは、安全のため必ず電源プラグをコンセントから抜いてください。火災・感電の原因となります。**

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。
  - **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。**
  - **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。**

		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。

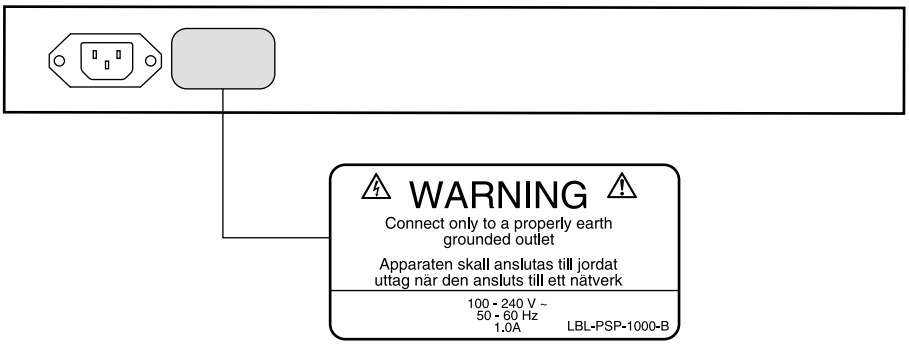
システムの安定稼動を目的に、保守サービス契約を結ばれることを推奨しております。
是非とも保守サービス契約を結ばれますようお願い申し上げます。

警告ラベル

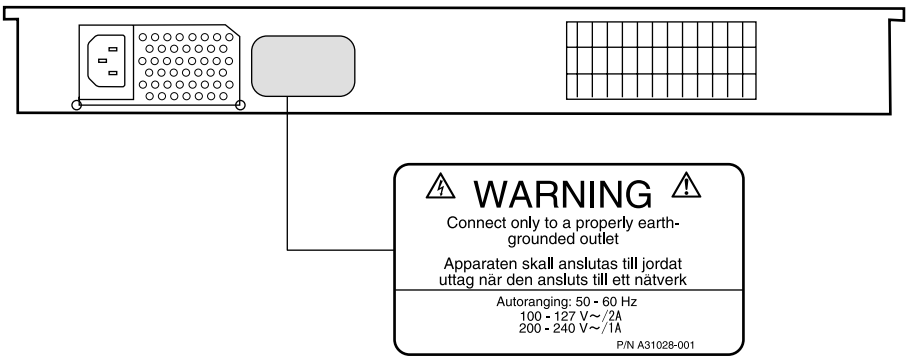
本製品には、下図のように警告ラベルが貼ってあります。警告ラベルは、絶対にはがさないでください。また、**その他のラベルもすべてはがさないでください。**

[装置背面]

[SSLAccelerator 7110**の場合**]



[SSLAccelerator 7115**の場合**]



本書の表記について

■ 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。

Intel7110>
: SSLAccelerator の標準コマンドラインプロンプトです。
なお、本書内ではコマンド記述例などにおいて「Intel 7110>」と表記していますが、SSLAccelerator 7115 をご使用の場合は「Intel 7115>」に読み替えてください。

■ 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 7110 またはPRIMERGY SSLAccelerator 7115 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。

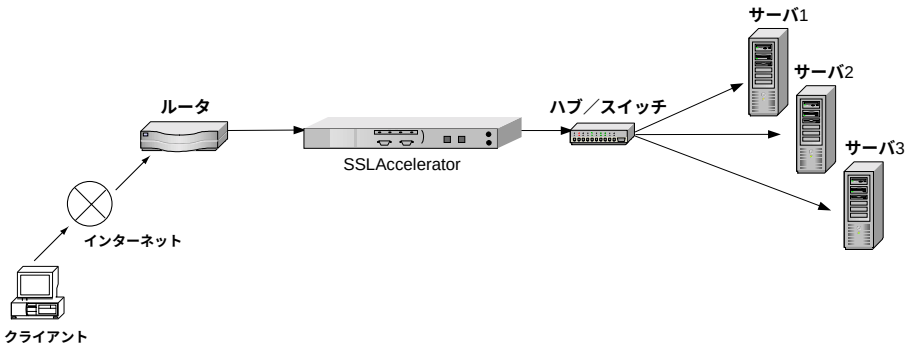
Contents

1.1 概要

PRIMERGY SSLAccelerator 7110 および PRIMERGY SSLAccelerator 7115 （以降、特に明記しないかぎり、これらをまとめて「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。

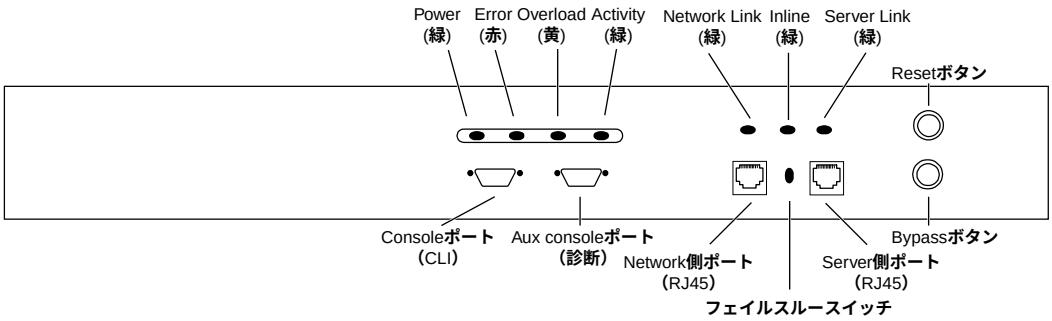
SSLAccelerator には以下の特長があります。

- 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 7110 では毎秒 200 コネクション、SSLAccelerator 7115 では毎秒 600 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	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	物理的にバイパスモード（SSLAccelerator の処理をバイパス）に設定します。
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.4 障害／バイパスモード」（→ 158 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 にわたす方法については、「3.4 カスケード接続する場合」（→ 28 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 - ネットワーク接続が正常です。
	消灯 - ネットワーク接続が異常です。
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 - サーバ接続が正常です。
	消灯 - サーバ接続が異常です。

■ 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（パソコン等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 7110 / 7115 **共通**

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
□**ゴム足**	4 **個** SSLAccelerator 7110 **のみ**
□**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」（→ 35 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

⚠警告

本体のカバーを外さないでください。
ユーザが設定／設置可能な部品／部位は存在しません。

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。

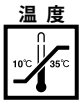
⚠注意

- **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、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。環境条件を外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）**

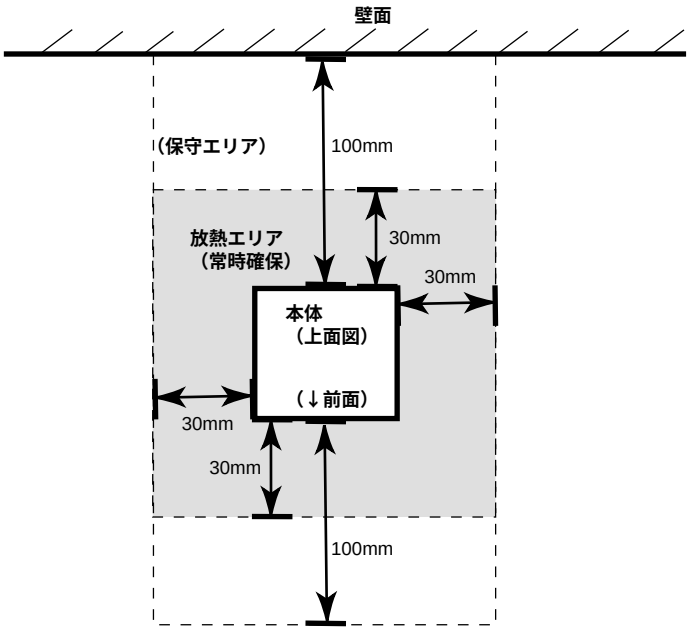
塵埃（ほこり、ちりなど）は磁気媒体やヘッドを傷つけたり、接触不良を起こす原因となります。また、腐食性有害物質および湿気との相乗作用により装置に悪影響を与えるため、空調機を装備したエアフィルタで塵埃を除去するなどの対策が必要です。

■ 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

本装置を設置するときは、以下のスペースを確保してください。



⚠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。

なお、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。

2.3.3 ラックへの設置

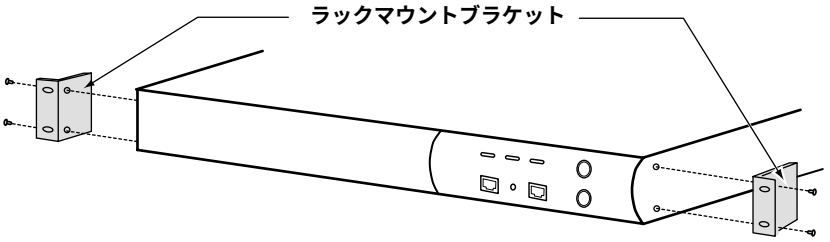
ここでは、本装置をラックに搭載する手順について説明します。

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。手順は次の通りです。**

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。**

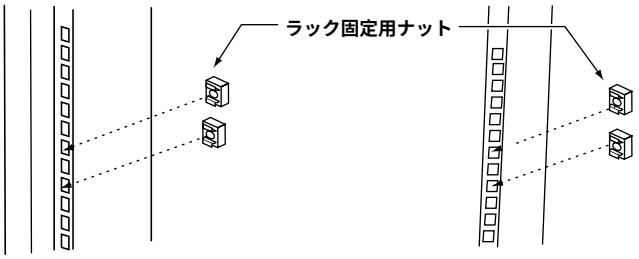


2 **本装置を 19 インチラック上に設置し、ラックマウントブラケットをラックに固定します。手順は次の通りです。**

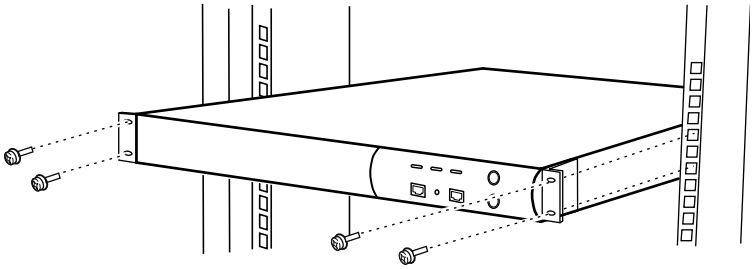
1 **同梱されているラック固定用ナット 4 個と、ネジ 4 本（長い銀色ネジ）を使用します。**

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。**

2.3.4 単体での設置（SSLAccelerator 7110 のみ）

1 **付属の粘着ゴム足を本装置の底面コーナー部** 4 **箇所に取り付けます。**

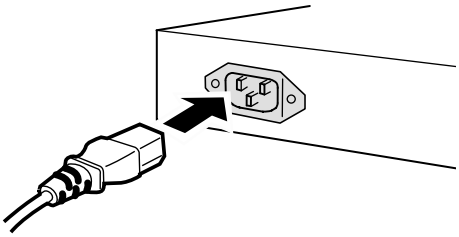
2 **本装置を平坦な場所に設置し、本体の周囲のエアフローがよいことを確認します。**
本装置の設置に関しては、前述の「■ 設置スペース」（→ 13 ページ）を参照してください。

ポイント SSLAccelerator 7115 **はラック搭載が必須となっております。**

2.4 ケーブル接続

1 **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。**

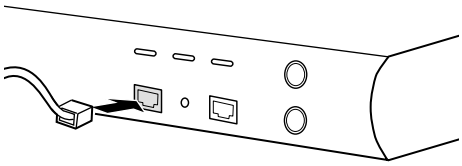
普通の状態では、SSLAccelerator は、約 40 秒ほどの起動時間を必要とします。起動が完了すると、本体の Power LED と Inline LED が点灯します。



⚠注意 **本体に電源を投入しても** Inline LED **が点灯（または点滅）しない場合は、フロントパネルの** Bypass **ボタンを押してください。**

2 **ストレートケーブルを使用して、**SSLAccelerator **の左側の** RJ-45 **コネクタをネットワークに接続します。**

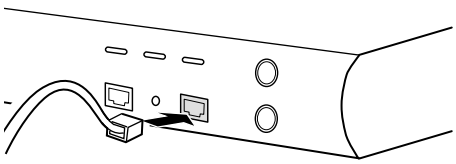
接続が有効であれば、ネットワークポート上の LED が点灯します。LED が点灯しない場合は、クロスケーブルを使用してもう一度接続してください。



⚠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。**

3 **ストレートケーブルを使用して、**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サーバポート 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。



4 **この段階で** Network Link LED **と** Server Link LED **がいずれも点灯しない場合は、「第** 8 **章 トラブルシューティング」（→** 139 **ページ）を参照してください。**

5 **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（例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」（→ 18 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
  Network LED と Server LED が両方と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」（→ 139 ページ）を参照してください。
- Inline LED
  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。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」（→ 139 ページ）または本書の「A.4 障害／バイパスモード」（→ 158 ページ）を参照してください。

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 を想定します）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 **へダイレクト**] **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 **から** 1msec **以上の値に変更します。**
5. [OK] **を** 2 **回クリックして設定を終了します。**

■ 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ない）
Current date: 2000 03/01 15:59
Intel 7110>
```

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。

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。

```
Intel 7110>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 **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。**
電子証明書の有効性は、日付と時刻によって決まります。

```
Intel 7110>set date
```

日付を設定するためには、SSLAccelerator の再起動が必要になります。

4 **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」（→ 66 ページ）でも確認できます。

```
Intel 7110>help
```

5 **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」（→ 35 ページ）を参照してください。

■ 設定を続ける

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」（→ 21 ページ）に進んでください。

3 構成

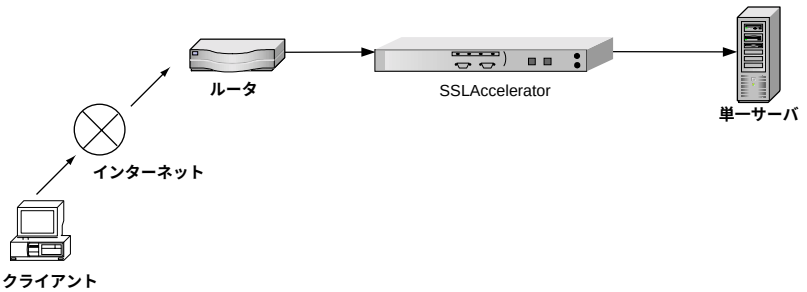
この章では、以下の構成例に対し SSLAccelerator の設定方法を図と共に示します。

- 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 を単一のサーバと共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」（→ 35 ページ）で説明されている手順に従って、適切な鍵と電子証明書の設定を行ってください。**

3 サーバに対するマッピングを作成します。

create map コマンドを用いて、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。

```
Intel 7110>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 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後に、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。

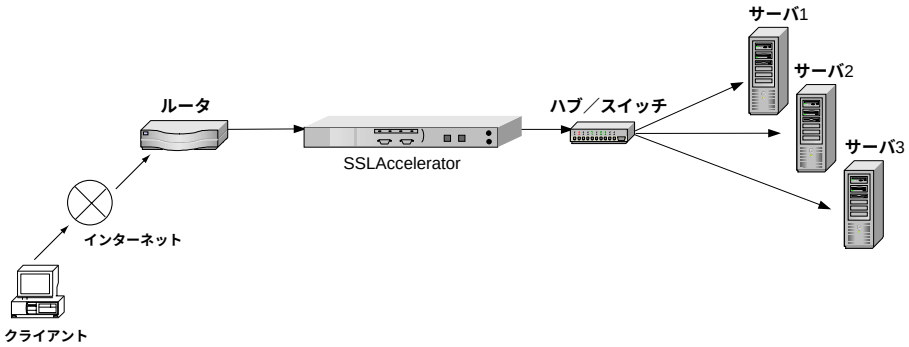
```
Intel 7110>delete map 1
Intel 7110>list maps

Map                              Net   Ser   Cipher          Re-      Client
ID  KeyID      Server IP         Port  Port  Suites          direct   Auth
==  ========== ========== ==== ==== ============ ====== ======
 1  myserver   10.1.1.30    443   80   medium(v2+v3)   n        n
Intel 7110>
```

5 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。

```
Intel 7110>config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

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 をルータとスイッチの間に接続します。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」（→ 35 ページ）で説明されている手順に従って、適切な鍵と電子証明書の設定を行ってください。**

3 **サーバに対するマッピングを作成します。**
create map コマンドを用いて、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。

```
Intel 7110>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 **サーバ 2 に対するマッピングを作成します。**
create map コマンドを用いて、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。

```
Intel 7110>create map
Server IP [0.0.0.0]: 10.1.1.31
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: myserver
```

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。)

```
Intel 7110> list maps
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    medium(v2+v3)       n         n
 3   myserver    10.1.1.31           443   80    medium(v2+v3)       n         n
Intel 7110>
```

7 **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後に、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。

```
Intel 7110>delete map 1
Intel 7110>list maps

Map                                  Net   Ser   Cipher              Re-       Client
ID   KeyID       Server IP           Port  Port  Suites              direct    Auth
==   ========    =========           ====  ====  ==========          ======    ======
 1   myserver    10.1.1.30           443   80    medium(v2+v3)       n         n
 2   myserver    10.1.1.31           443   80    medium(v2+v3)       n         n
Intel 7110>
```

8 **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。**

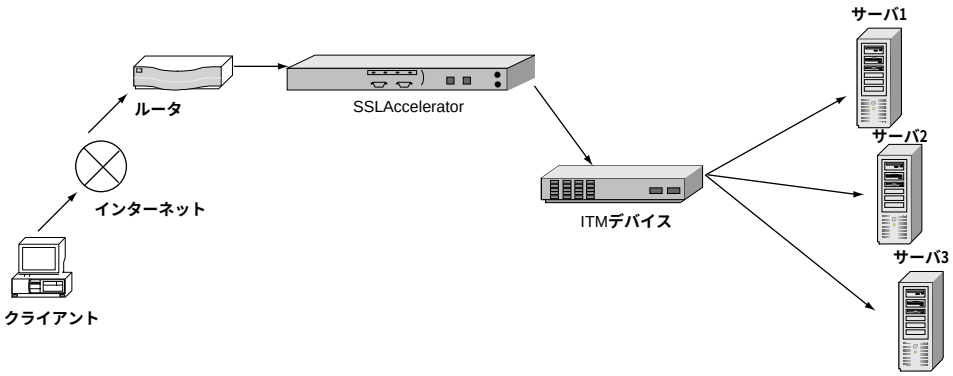
```
Intel 7110>config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

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 デバイスを使用する場合は、SSLAccelerator をルータと ITM デバイスの間に接続するか、ITM デバイスとサーバの間に接続します。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。

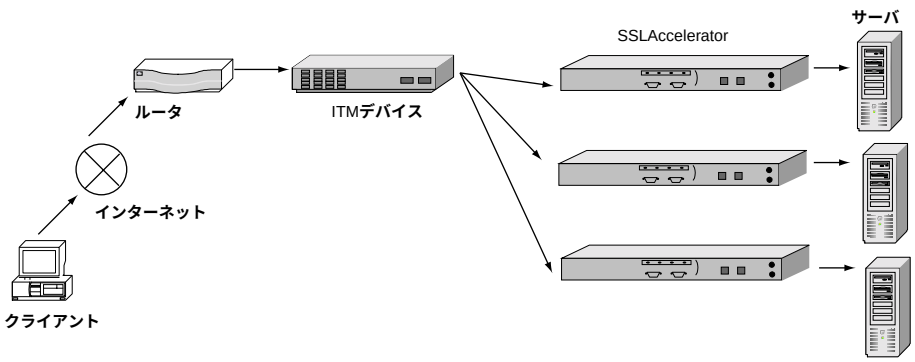
3.3.1 クライアントネットワーク側への配置

ITM デバイスがレイヤ 7 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、レイヤ 7 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。

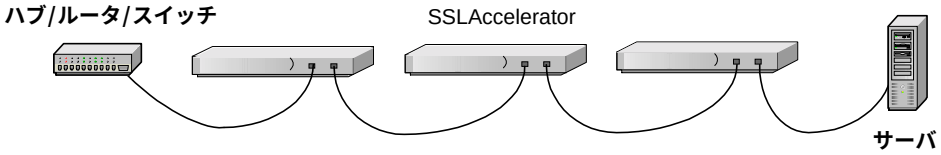
3.4 カスケード接続する場合

■ 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、つまり各 SSLAccelerator ごと単独で、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「5.5.5 操作コマンド」（→ 82 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。



■ 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、SSLAccelerator に障害が発生するか、または Bypass モードに設定すると、SSLAccelerator は、その機能がなんらかの原因によって停止した場合に、その 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.4 障害／バイパスモード」（→ 158 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くりかえし、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。**

```
Intel 7110>config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

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。

```
Intel 7110> export config
Export protocol: (xmodem, ascii)[ascii]: xmodem
Use Ctrl-X 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!
Intel 7110>
```

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コマンドプロンプトを表示させておきます。**

11 **設定をインポートします。**
import config コマンドを用い処理を開始させます。まず、XMODEM を選びます。そして [Enter] キーを押し、SSLAccelerator 本体内の実際のインポート処理を開始させます。

```
Intel 7110> import config
Import protocol: (paste, xmodem)[paste]: xmodem
Use Ctl-X to cancel upload
```

12 **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。**

13 **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。**

14 **送信プロトコルとして** XMODEM **を選択します。**

15 **[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]: y
```

16 **確定** (y) **またはキャンセル** (n) **すると、プロンプトが再表示されます。**

```
Intel 7110>
```

17 **設定を保存します。**

```
Intel 7110>config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

18 **上記の手順** 11 **〜** 17 **を** 3 **段目以降に接続した** SSLAccelerator **に対して繰り返します。**

19 **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

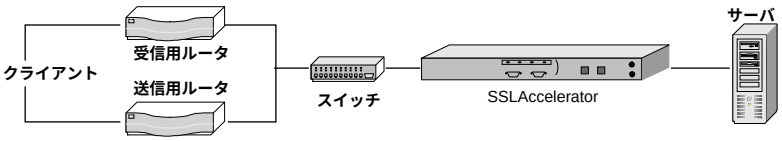
本装置をカスケードで使う場合は、カスケードされる SSLAccelerator **の** IP **アドレスをそれぞれ異なった** IP **アドレスにする必要があります。**

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を異なったものを使用する場合の構成についての説明です。

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 を用います (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)
- 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)



■ 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、例えば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。**

```
Intel 7110>set egress_mac 00:11:22:33:44:55
Egress MAC set to 00:11:22:33:44:55

Intel 7110>config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

設定を無効にするためには以下のように入力します。

```
Intel 7110>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 通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 コマンドを使って鍵を作成します。create sign コマンドを使って、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。

```
Intel 7110> create key
Key strength (512/1024) [512]: <Enter>
New keyID [001]: 002
Keypair was created for keyID: 002.
```

⚠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。

```
Intel 7110> create sign 002
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.
```

以下の説明に従い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：通常、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：通常、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.mysite.com 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、コンソールポートに接続されているパソコン に、XMODEM を使って CSR を送る例を示します。

```
Intel 7110> export sign 002
Export protocol: (xmodem, ascii)[ascii]:xmodem
Use Ctrl-x to kill transmission
Beginning export...
Export successful!
Intel 7110>
```

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-----
MIIBnDCCAQUACQAwXjELMAkGA1UEBhMCQ0ExEDOABgNVBAgTB
09udGFayW8xEDAOBgNVBAcTB01vbnRyYWwxDDAKBgNVBAoTA0
tGQzEdMBsGA1UEAxMUd3d3Lmlsb3ZlY2hpY2tlbi5jb20wgZ0
wDQYJKoZIhvcNAQEBBQADgYsAMIGHAoGBALmJA2FLSGJ9iCF8
uwfPW2AKkyyKoe9aHnnwLLw8WWjhl[ww9pLietwX3bp6Do87m
wV3jrgQ1OIwarj9iKMLT6cSdeZ0OTNn7vvJaNv1iCBWGNypQv
3kVMMzzjEtOl2uGl8VOyeE7jImYj4HlMa+R168AmXT82ubDR2
ivqQwl7AgEDoAAwDQYJKoZIhvcNAQEEBQADgYEAn8BTcPg4Ow
ohGIMU2m39FVvh0M86ZBkANQCEHxMzzrnydXnvRMKPSE208x3
Bgh5cGBC47YghGZzdvxYJAT1vbkfCSBVR9GBxef6ytkuJ9YnK
84Q8x+pS2bEBDnw0D2MwdOSF1sBb1bcFfkmbpjN2N+hqrrvA0
mcNpAgk8nU=
-----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、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（貼り付け）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。

```
Intel 7110> import cert 002
keyid is 002;
Import protocol: (paste, xmodem)[paste]:<Enter>
Type or paste in date, end with ... alone on line.

-----BEGIN CERTIFICATE-----
MIIDKDCCAtKgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBnDELM
AkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMQ4wDAYDVQQHEwVQb3
dheTEaMBgGA1UEChMRQ29tbWVyY2Ug
•
•
•
-----END CERTIFICATE----- <Enter>

... <Enter>
Import successful!
Intel 7110>
```

5 サーバのマッピングを作成します。

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

```
Intel 7110> 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: 002
```

6 マッピングの作成後、設定を保存します。

```
Intel 7110> config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

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 コマンドを使って、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、デフォルトで「貼り付け」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。

```
Intel 7110> import key mywebserver
Import protocol: (paste, xmodem)[paste]: <Enter>
Type or paste in date, end with ... alone on line

-----BEGIN RSA PRIVATE KEY-----
MIIBOgIBAAJBALGOlBH14vIdtfuA+UnyRIoKya13ey8mj3GDQ
akdwoDJALu+jtcC
•
•
•
S9dPdwp6zctsZeztn/ewPeNamz3q8QoEhY8CawEA

-----END RSA PRIVATE KEY-----<Enter>
... <Enter>
Import successful!
Intel 7110>
```

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、デフォルトで「貼り付け」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。

```
Intel 7110> import cert mywebserver
keyid is mywebserver;
Import protocol: (paste, xmodem)[paste]: <Enter>
Type or paste in date, end with ... alone on line

-----BEGIN CERTIFICATE-----
MIIDKDCCAtKgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBnDELM
AkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMQ4wDAYDVQQHEwVQb3
dheTEaMBgGA1UEChMRQ29tbWVyY2Ug
•
•
•

----END CERTIFICATE----- <Enter>
... <Enter>
Import successful!
Intel 7110>
```

3 **サーバのマッピングを作成します。**

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

```
Intel 7110> 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: mywebserver
```

4 **マッピングの作成後、設定を保存します。**

```
Intel 7110> config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

4.5 SSLAccelerator で新しい鍵／電子証明書を作成

create key コマンドと create cert コマンドを使って、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選択できます。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。

⚠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。**

1 次のようにして鍵を作成します。

```
Intel 7110> create key
Key strength (512/1024)[512]: 512
New keyID [001]: mywebserver
Keypair was created for keyID: mywebserver.
```

2 create cert コマンドに KeyID を指定して実行します。

```
Intel 7110> create cert mywebserver
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.myserver.com）
- 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 コマンドを使って、サーバの IP アドレス、ポート、KeyID を指定してください。

```
Intel 7110> 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: mywebserver
```

4　**マッピングの作成後、設定を保存します。**

```
Intel 7110> config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

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。

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なければなりません。

⚠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：

```
Intel 7110> import cert <keyID>
Import protocol: (paste, xmodem)[paste]:
Type or paste in data, end with ... alone on line
-----BEGIN CERTIFICATE-----
MIIFZTCCBM6gAwIBAgIQCTN2wvQH2CK+rgZKcTrNBzANBgkqh
kiG9w0BAQQFADCBujEfMB0GA1UEChMWVmVyaVNpZ24gVHJ1c3
QgTmV0d29yazEXMBUGA1UECxMOVmVyaVNpZ24sIEluYy4xMzA
xBgNVBAsTKlZlcmlTaWduIEludGVybmF0aW9uYWwgU2Vy
:
dmVyIENBIC0gQ2xhc3MgMzFJMEcGA1UECxNAd3d3LnZlcmlza
WduLmNvbS9DUFMg
SW5jb3JwLmJ5IFJlZi4gTElBQklMSVRZIExURC4oYyk5NyBWZ
XJpU2lnbjAeFw05
OTExMTEwMDAwMDBaFw0wMDExMTAyMzU5NTlaMIHHMQswCQYDV
QQGEwJVUzETMBEG
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEMTCCA5qgAwIBAgIQI2yXHivGDQv5dGDe8QjDwzANBgkqh
kiG9w0BAQIFADBfMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVm
VyaVNpZ24sIEluYy4xNzA1BgNVBAsTLkNsYXNzIDMgUHVibGl
jIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcN
OTcwNDE3MDAwMDAwWhcN
:
OTk3IFZlcmlTaWduMA0GCSqGSIb3DQEBAgUAA4GBALiMmMMrS
PVyzWgNGrN0Y7uxWLaYRSLsEY3HTjOLYlohJGyawEK0Rak6+2
fwkb4YH9VIGZNrjcs3S4bmfZv9jHiZ/4PC/
NlVBp4xZkZ9G3hg9FXUbFXIaWJwfE22iQYFm8hDjswMKNXRjM
```

1GUOMxlmaSESQeSltLZl5lVR5fN5qu
-----END CERTIFICATE-----**<Enter>**
...<Enter>
Import successful!
Intel 7110>

4.7 リダイレクション

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 redirect 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 redirect 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なければなりません。
また、リダイレクトページの内容を定義しておかなければなりません。

⚠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。

```
Intel 7110> 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    medium(v2+v3)   n       n
Intel 7110> set redirect 2
Enter a redirect URL at following prompt
e.g. http://www.e-comm_site.com/weakbrowser.html
Enter redirect URL []:http://www.e-comm_site.com/cipher_info.html
Intel 7110> 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    medium(v2+v3)   y       n
Intel 7110> show redirect 2
Redirect URL for map 2 is set: http://www.e-comm_site.com/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。

```
Intel 7110> set redirect 2 none
Intel 7110> show redirect 2
Redirect URL for map 2 is not set
```

4.8 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 maps 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。

```
Intel 7110> list maps
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    medium(v2+v3)     n         n
```

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

```
Intel 7110> import client_ca 2
Import protocol: (paste, xmodem)[paste]: <Enter>
Type or paste in data, end with ... alone on line
-----BEGIN CERTIFICATE-----
MIIDxzCCAzCgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBpDELM
kGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExEjAQBg
NVBAcTCVNhbiBEaWVnbzEUMBIGA1UE
.
.
.
XcCabZcfBRuYcZeUoNrGUl8tD80jp2YNG1vidgLEaD1YCli5I
9/mNrcB25mSfdAR
/08ROTMxm4VKOSA=
-----END CERTIFICATE-----<Enter>
...<Enter>
```

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。

```
Intel 7110> 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    medium(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 CA 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** CA **用の鍵のペアを生成します。**

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

2 **クライアント** CA **電子証明書を生成します。**

```
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、**ca_cert.pem **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 **鍵のペアを生成します。**

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

2 **署名要求を生成します。**

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

3 **クライアント** CA **電子証明書を使用して、クライアント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 **で得られた出力ファイル (署名済みの電子証明書** cert.p12) **を、クライアントブラウザにインポートします。**

4.9 SSL の処理

■ 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 アドレスとネットワーク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った自動マッピング

自動マッピングに使用する鍵と電子証明書をユーザが指定する場合は、create map コマンドを使って、初期設定の自動マッピングエントリを新しいエントリで置き換えます。初期設定の自動マッピングエントリを新しいエントリで上書きするには、同じ一意の識別子（サーバの IP アドレス 0.0.0.0、ネットワーク側ポート 443）とユーザが作成した KeyID を指定します。使用する鍵と電子証明書の取得方法に特に制限はありません（この章で説明した取得方法のうちいずれかを使用）。

■ 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。

■ 自動マッピングエントリの削除

自動マッピングエントリは自由に削除できます。ただし、ほかの自動マッピングエントリを指定していない状態で初期設定時の自動マッピングエントリを削除すると、自動マッピングエントリが自動的に再生成されます。初期設定時の自動マッピングエントリを削除するには、このエントリを新しいエントリで置き換えるか、別のマッピング（自動マッピング）エントリを作成してから delete map コマンドを実行します。

■ 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も作成できます。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」（→ 21 ページ）を参照してください。

⚠注意

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。

■ ブロック

SSLAccelerator では、セキュリティ保護の目的で、指定の IP アドレスの指定のポートに対するブロックを行うことができます。この処理は、次の情報に基づいて行われます。

- 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

⚠注意

ブロックは、常にマッピングの前に実行されます。

■ 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。

1 create block **コマンドを入力します。**

2 IP **アドレスを入力します。**

3 IP **マスクとして、**255.255.255.255 **を入力します。**

4 **指定したいポート番号を入力します。**

5 [Enter] **キーを押し、デフォルトのポートマスクを入力します。**

例：

```
Intel 7110> 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: 80
Server Port mask [0xffff]:<Enter>
```

確認には、show block コマンドを使用します。

```
Intel 7110>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）。

1 **サブネット** IP **アドレスを入力します。**
末尾の値は 0 にします（正確にはサブネットのサイズに合わせて、サブネットサイズ分の下位ビット値を 0 とした値を入力します）。この例では、「10.1.x.x」から「20.1.x.x」のポート 80 へのトラフィックがすべてブロックされます。

2 **サブネットマスクを入力します。**
ビット値に変換した後に 0 となるビットの IP アドレス部分を無視することを示しています。

3 **特定のポートを入力します。**

4 [Enter] **キーを押し、デフォルトのポートマスクを入力します。**

例：

```
Intel 7110> create block
Client IP to block [0.0.0.0]: 10.1.2.1
Client IP mask [0.0.0.0]: 255.255.0.0
Server IP to block [0.0.0.0]: 20.1.2.1
Server IP mask [0.0.0.0]: 255.255.0.0
Server Port to block: 80
Server Port mask [0xffff]:<Enter>
```

確認には、show block コマンドを使用します。

```
Intel 7110> show block
------------
blocks :
------------
(1) block 10.1.2.1 255.255.0.0 20.1.2.1 255.255.0.0 80 0xffff
------------
```


■ すべての IP アドレス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。

1 **ブロック対象の** IP **アドレスとして、**0.0.0.0 **を入力します。**

2 **ブロック対象の** IP **ワイルドカードマスクとして、**0.0.0.0 **を入力します。**

3 **指定のポートを入力します。**

4 [Enter] **キーを押し、デフォルトのポートマスクを入力します。**

例：

```
Intel 7110> 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: 80
Server Port mask [0xffff]:<Enter>
```

確認には、show block コマンドを使用します。

```
Intel 7110> 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。**

```
Intel 7110> 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。**

```
Intel 7110>delete block 1
```

4.10　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.4 障害／バイパスモード」（→ 158 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

ユーザが 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、現在の日付と時刻が表示されます。

■ コマンドラインプロンプト

SSLAccelerator 7110 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。
なお、SSLAccelerator 7115 をご使用の場合は「Intel 7115>」に読み替えてください。

```
Intel 7110>
```

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。例えば、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。

```
Intel 7110> del
Usage: delete item [arg]
        block     blockID
        cert      keyID
        client_ca mapID
        key       keyID
        logs      logID|all
        map       mapID
        patch
        permit    permitID
        sign      keyID
        snmp_community
        trap_community
```

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

```
Intel 7110> sh
```

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

```
Intel 7110> 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	ヒストリバッファ上の 1 つ前のコマンド行を表示します。
ctrl-n	ヒストリバッファ上の 1 つ後ろのコマンド行を表示します。
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	削除された文字をペーストします。
backspace	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」（→ 70 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	compare default reset save
create	block cert <keyID> key <keyID> map permit sign <keyID>
delete	block <blockID> cert <keyID> client_ca <mapID> key <keyID> logs <logID | all> map <mapID> patch permit sign <keyID> snmp_community trap_community
exit	
export	cert <keyID> config key <keyID> log <logID> sign <keyID>
factory_default	
help	help help <command> help usage
import	key <keyID> cert <keyID> client_ca <mapID> config upgrade patch
inline	

コマンド	コマンドオプション
list	blocks filters keys logs maps monitoring permits procs snmp_community system trap_community
nic	
password	
quit	
reboot	
set	alarms <all, esc, rsc, utl, ovl, nls> cache ciphers <mapID> ciphers <mapID> default client_tmo <seconds> date defcert egress_mac x:x:x:x:x:x: egress_mac none ether idleto <timeout> ip <ip> <netmask> kstrength max_remote_sessions<0-5> monitoring <enable | disable> monitoring_interval monitoring_fields more ovl_window <seconds> prompt redirect <mapID> redirect <mapID> none route x.x.x.x rsc_window <seconds> serial server_tmo ssh <enable | disable> ssh_port <port> spill <enable | disable> telnet <enable | disable> telnet_port <port> utl_highwater <percentage> utl_lowwater <percentage> utl_window <seconds>

コマンド	コマンドオプション
show	alarms blocks cache cert <key ID> ciphers <mapID> client_ca <map ID> client_tmo config config default config saved date defcert egress_mac ether filters idleto info ip key <key ID> kstrength logs map max_remote_sessions monitoring monitoring_interval monitoring_fields more ovl_window patch permits redirect <mapID> route rsc_window serial server_tmo ssh ssh_port sign <key ID> spill status <arg> telnet telnet_port utl_highwater utl_lowwater utl_window
setsnmp	snmp <enable | disable> snmp_community snmp_info snmp_port sys_contact sys_location sys_name trap_authen <enable | disable> trap_community trap_port

コマンド	コマンドオプション
showsnmp	snmp snmp_community snmp_info snmp_port sys_contact sys_location sys_name trap_authen trap_community trap_port
status	realtime line alarms <logID>
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	デバイスの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）。 **構文** : Intel 7110> **status <line | realtime | alarm | <log> >** <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。 <alarms> は、現在のアラームイベントを表示します。 <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	status コマンドと同じです。

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** : Intel 7110> **create key** Key strength (512/1024) [512]: **1024** New keyID [001]:**<Enter>** Keypair was created for keyID: 001. Intel 7110>
delete key	**指定した** KeyID **を持つキーペアを削除します。** **構文** : Intel 7110> **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。** **構文** : Intel 7110> **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」(→** 42 **ページ) を参照してください。**
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)。** **構文** : Intel 7110> **export key <keyID>** Export protocol: (xmodem, ascii) [ascii]: **<Enter>** Press any key to start, then again when done...**<Enter>** -----BEGIN RSA PRIVATE KEY----- MIIBOgIBAAJBALqeajCDgfa8fY8FROLi0B8fVp3m4EI2MpO zKvEKKe6K k5pDBkH83tUBkssGBtbnDYHkiAyGzA . . . UFFSNgBRvbkiNvaNiVqKeutwDEhgCL0PDueo -----END RSA PRIVATE KEY-----**<Enter>** Intel 7110> <keyID> **は、エクスポートされるキーペアの** KeyID **です。**

コマンド	説明
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** : Intel 7110> **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** : Intel 7110> **list keys** 001 default Intel 7110>
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** : Intel 7110> **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 で新しい鍵／電子証明書を作成」（→ 44 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** : Intel 7110> **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** : Intel 7110> **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** : Intel 7110> **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。

コマンド	説明
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** : Intel 7110> **show cert <keyID>** <keyID> **は、表示される電子証明書に対応する** KeyID **です。**
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** : Intel 7110> **set ciphers <mapID>** 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** Intel 7110> <mapID> **は、暗号方式を設定する** MapID **です。** **サポートしている暗号方式については、「**A.5 **対応している暗号方式」（→** 160 **ページ）を参照してください。**
set ciphers default	**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。** **構文** : Intel 7110> **set ciphers <mapID> default** <mapID> **は、暗号方式を設定する** MapID **です。**
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** : Intel 7110> **show ciphers <mapID>** <mapID> **は、表示する** MapID **です。**

コマンド	説明
set redirect	**指定した** MapID **の選択された暗号方式をサポートしないクライアントのために、リダイレクト先の代替アドレスを設定します。** **構文** : Intel 7110> **set redirect <mapID> [none]** Enter redirect URL []: <URL> <mapID> **は、リダイレクト** URL **が定義される** MapID **です。**<URL> **は、選択された暗号方式をサポートしないクライアントのリダイレクト先の** Web **アドレスです。** **オプションのパラメタ** [none] **を入力して、指定した** MapID **の既存のリダイレクト** URL **を無効にすることができます。**
show redirect	**選択された暗号方式をサポートしないクライアントのリダイレクト先の代替アドレスを表示します（指定した** MapID **について代替アドレスが設定されている場合)。** **構文** : Intel 7110> **show redirect <mapID>** <mapID> **は、リダイレクト** URL **が表示される** MapID **です。リダイレクトアドレスが定義されていない場合は、コマンドラインに次のようなメッセージが表示されます。** Intel 7110> **show redirect 1** Redirect URL for map 1 is not set Intel 7110>
show client_ca	**指定した** MapID **に対応する、拡張されたクライアント電子証明書（**PEM **形式を含む）を表示します。クライアント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電子証明書が表示されます。** **構文** : Intel 7110> **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、信頼できる 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、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** : Intel 7110> **import client_ca <mapID>** Import protocol: (paste, xmodem) [paste]:**<Enter>** Type or paste in data, end with ... alone on line **（ここに電子証明書を貼り付けます ...）** . . . <mapID> **は、インポートされるクライアント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電子証明書を削除します。** **構文** : Intel 7110> **delete client_ca <mapID>** <mapID> **は、削除されるクライアント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** : Intel 7110> **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」（→** 37 **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** : Intel 7110> **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** : Intel 7110> **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** : Intel 7110> **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用いら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、電子証明書を用いるサイト名、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 **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** : Intel 7110> **set defcert** Country name [US]:**<Enter>** State [California]:**<Enter>** City [San Diego]:**<Enter>** Organization [Intel Corporation]:**<Enter>** Organization unit [Network Equipment Division]:**<Enter>** Issuer name [www.server.com]:**<Enter>** Issuer email address [support@server.com]: **email@server.com** Make changes [y]: **y** Changes applied Intel 7110>

コマンド	説明
show defcert	**電子証明書作成や署名要求の作成時に用いられるデフォルト値を表示します。** **例** : Intel 7110> **show defcert** Country: US State: California City: San Diego Organization: Intel Corporation Unit: Network Equipment Division Name: http://www.intel.com/network/services Email: email@server.com Intel 7110>
set kstrength {512|1024}	**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** : Intel 7110> **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／秘密鍵ペアの強さを表す値を表示します。** **例** : Intel 7110> **show kstrength** Default key strength: 512
set client_tmo	**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この時間値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ります。** **構文** : Intel 7110> **set client_tmo <n>** <n> **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** : Intel 7110> **show client_tmo** Client timeout [secs]: 5 Intel 7110>

コマンド	説明
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** : **サーバタイムアウトの一般的な原因には、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等があります。** **構文** : Intel 7110> **set server_tmo <n>** <n> **は、**5 **〜** 36000 **の範囲の値（秒）です。**
show server_tmo	**現在指定されているサーバタイムアウト値を表示します。** **例** : Intel 7110> **show server_tmo** Server timeout [secs]: 5 Intel 7110>
set cache	SSL session caching **を有効または無効にします。この機能は、**SSL session ID **を** cache **する機能です。** **構文** : set cache **<enable|disable>**
show cache	SSL session caching **オプションのモードの有効または、無効を表示します。** **例：** Intel 7110> **show cache** SSL Session Caching : enabled

5.5.4 マッピングコマンド

マッピングコマンドは、第 4 章の「■ マッピング」（→ 54 ページ）、「■ ブロック」（→ 55 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。一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。** **例** : Intel 7110> **create block** Client IP to block [0.0.0.0]: **10.1.2.1** Client IP mask [0.0.0.0]: **255.255.0.0** Server IP to block [0.0.0.0]: **20.1.2.1** Server IP mask [0.0.0.0]: **255.255.0.0** Server Port to block: **80** Server Port mask [0xffff]:**<Enter>** Intel 7110>
delete block	**索引番号により指定された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 block**（以下を参照）を使用してください。** **例** : Intel 7110> **delete block 1** Intel 7110>
show blocks	**設定されている全ブロックを表示します。** **例** : Intel 7110> **show blocks** -------- blocks : --------- (1) block 10.1.2.1 255.255.0.0 20.1.2.1 255.255.0.0 80 0xffff ----------
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。** **例** : Intel 7110> **create permit** Client IP to permit [0.0.0.0]:**10.1.2.1** Client IP mask [0.0.0.0]:**255.255.0.0** Server IP to permit [0.0.0.0]:**20.1.2.1** Server IP mask [0.0.0.0]:**255.255.0.0** Server Port to permit: 443 Server Port mask [0xffff]:**<Enter>** Intel 7110>

コマンド	説明
delete permit	**索引番号により指定された許可を取り消します。既存の許可とその番号を表示するには、**show permit**（以下を参照）を使用してください。** **例** : Intel 7110> **delete permit 1** Intel 7110>
show permits	**現在有効な許可を表示します。** **例** : Intel 7110> **show permits** -------- permits : --------- (1) permit 10.1.2.1 255.255.0.0 20.1.2.1 255.255.0.0 443 0xffff ---------- Intel 7110>
create map	**サーバの** 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。** **例** : Intel 7110> **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: **4** Intel 7110> **注意** :create map **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 **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 **章を参照）。**
delete map <map ID>	**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 **より上位の** MapID **は、すべて** 1 **ずつデクリメントされます。** **構文** : Intel 7110> **delete map <mapID>** <mapID> **は、削除されるマッピングの** MapID **です。**

コマンド	説明
show map	**すべてのマッピングを表示します（**list maps **と同じ）。**
list maps	**すべてのマッピングを一覧表示します（**show map **と同じ）。** **例** : Intel 7110> **list maps** 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 all (v2+v3) n n Intel 7110>

5.5.5 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。バイパスモードでは、トラフィックは何も処理されずに SSLAccelerator を通過します（フェイルスルーモード時）。バイパスモードの詳細は、「A.4 障害／バイパスモード」（→ 158 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。もし発行すると、SSLAccelerator との接続が直ちに切断されます。 例 : Intel 7110> **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 insert 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。バイパスモードでは、トラフィックは何も処理されずに SSLAccelerator を通過します（フェイルスルーモード時）。 例 : Intel 7110> **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。 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。これについては、「A.4 障害／バイパスモード」（→ 158 ページ）を参照してください。

コマンド	説明
set spill	「spill」モードの有効と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しきい値に達すると、そのしきい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。 例 : Intel 7110> **set spill enable** show spill コマンドを使用して、spill モードの設定を確認できます。 Intel 7110> **show spil**l Spill on overload: enabled Intel 7110>
show spill	「spill」オプションのモードの有効または無効を表示します。 例 : Intel 7110> **show spil**l Spill on overload: disabled
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 : Intel 7110> **reboot** Are you sure you want to reboot [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。）

5.5.6 リモート管理コマンド

コマンド	説明
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。 注意 : • IP アドレスの割り当てには、セキュリティ問題が伴います。 • 現在設定されている IP を無効にするには、set ip に続けて none を指定してください。 例 : Intel 7110> **set ip** Enter IP Address ('none' to delete) [10.1.2.124]:**10.1.1.253** Enter Netmask [255.255.0.0]:**255.255.255.0**
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 : Intel 7110> **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。
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デバイスの 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、デバイスは 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 : Intel 7110> **set telnet enable** Need an IP address to start Telnet service. Enter IP Address [209.218.240.67]: **10.1.1.253** Need a netmask to start Telnet service. Enter Netmask [255.255.255.0]:**<Enter>** Optional Default Route to start Telnet service. Enter Default Route ('none' to delete) [none]:**<Enter>** Telnet Services started. Intel 7110>

コマンド	説明
show telnet	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。 例 : Intel 7110> **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 : Intel 7110> **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 セッションを受け入れるポートを表示します。 例 : Intel 7110> **show telnet_port** Telnet Port Number : 23
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デバイスの 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、デバイスは SSH 接続を受け付けなくなります。デフォルトは disable です。 構文 : Intel 7110> **set ssh <enable|disable>**
show ssh	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。 例 : Intel 7110> **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 : Intel 7110> **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 : Intel 7110> **show ssh_port** SSH Port Number: 22

コマンド	説明
setsnmp snmp	SNMP エージェントの有効／無効を切り替えます。有効にすると、SNMP の情報およびパラメタを設定することができます。デフォルトは disable です。 構文 : Intel 7110> **setsnmp snmp <enable|disable>**
showsnmp snmp	SNMP エージェント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。 例 : Intel 7110> **showsnmp snmp** SNMP: enabled
setsnmp 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 Name • System Location 例 : Intel 7110> **setsnmp snmp_info** SNMP Port [161]: **161** SNMP Trap Port [162]: **162** Contact Person []: **support** System Location []:**San Diego** System Name []: **7110**
showsnmp snmp_info	現在有効な SNMP の情報およびパラメタを表示します。 例 : Intel 7110> **showsnmp snmp_info** SNMP Port Number : 161 SNMP Trap Port Number: 162 SNMP System Contact : support SNMP System Name : 7110 SNMP System Location : San Diego System IP Address : 10.1.2.124 System Netmask : 255.255.255.0 Default Route : None
setsnmp snmp_community	SNMP コミュニティ文字列を設定します。 例 : Intel 7110> **setsnmp snmp_community** SNMP Community String(s) Setting. Enter a SNMP Community IP (q to quit): **10.1.1.6** Enter a SNMP Community String (q to quit): **public** Enter a SNMP Community IP (q to quit): **q** SNMP Service stopped. SNMP Service started.

コマンド	説明
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** : Intel 7110> **list snmp_community** SNMP Community String(s) information. <1> Current SNMP Community String(s): 1.) IP: 10.1.1.6 => String: public=> Rights: read
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** : Intel 7110> **delete snmp_commmunity** SNMP Community String(s) Deletion. <1> Current Available SNMP Community String(s): 1.) IP: 10.20.75.106 => String: public=> Rights: read Enter number (1) to delete (q to quit) [1]: **<Enter>** Enter number (1) to delete (q to quit) [1]: **q** SNMP Service stopped. SNMP Service started.
setsnmp trap_authen	**有効にすると、**SNMP **マネージャは、失敗した認証についてトラップを受け取ります。** **構文** : Intel 7110> **setsnmp trap_authen <enable|disable>**
showsnmp trap_authen	**認証トラップの現在の状況を表示します。** **例** : Intel 7110> **showsnmp trap_authen** SNMP Authorization Trap: enabled
setsnmp trap_community	SNMP **トラップコミュニティ文字列を設定します。** **例** : Intel 7110> **setsnmp trap_community** SNMP Trap Community String(s) Setting. Enter a SNMP Trap Community IP (q to quit): **10.1.1.6** Enter a SNMP Trap Community String (q to quit): **private** Enter a SNMP Trap Community IP (q to quit): **10.1.1.7** 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** : Intel 7110> **list trap_community** SNMP Trap Community String(s) information. <2> Current SNMP Trap Community String(s): 1.) IP: 10.1.1.6 => String: private 2.) IP: 10.1.1.7 => String: public
delete trap_community	SNMP **トラップコミュニティ文字列を削除します。** **例** : Intel 7110> **delete trap_community** SNMP Trap Community String(s) Deletion. <2> Current Available SNMP Trap Community String(s): 1.) IP: 10.1.1.6 => String: private 2.) IP: 10.1.1.7 => String: public Enter number (1 to 2) to delete (q to quit) [1]: **2** Enter number (1 to 2) to delete (q to quit) [1]: **q**

5.5.7 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 : Intel 7110> **set alarms** < all | esc | rsc | utl | ovl | nls > <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。 <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。 <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。 <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。 アラームをすべて無効にするには、none を指定します。 例 : Intel 7110> **set alarms all** Intel 7110> **show alarms** Alarms set: esc rsc utl ovl nls
show alarms	現在有効なアラームのリストを表示します。 例 : Intel 7110> **set alarms none** Intel 7110> **show alarms** Alarms set: 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: の後に何も表示されません。
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 : Intel 7110> **set rsc_window <sec>** <sec> は、検査間隔を示す秒数です。

コマンド	説明
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 : Intel 7110> **show rsc_window** Check for refused SSL connections [secs]: 10
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。しきい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、全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 および set utl_lowwater も参照してください。 構文 : Intel 7110> **set utl_window <sec>** <sec> は、検査間隔を示す秒数です。
set utl_highwater	使用しきい値アラームの最高水準点を設定します。最高水準点 (%) 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 および set utl_lowwater も参照してください。 構文 : Intel 7110> **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、高いほうのしきい値を示します。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。

コマンド	説明
set utl_lowwater	**使用しきい値アラームの低水準値を設定します。低水準値** (%) **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 **および** set utl_highwater **も参照してください。** **構文** : Intel 7110> **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、低いほうのしきい値を示します。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_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** : Intel 7110> **show utl_window** Utilization Window set [secs]: 10
show utl_highwater	**使用しきい値アラームの現在のしきい値（高いほう）を表示します。** **例** : Intel 7110> **show utl_highwater** Utilization High water mark [%]: 80
show utl_lowwater	**使用しきい値アラームの現在のしきい値（低いほう）を表示します。** **例** : Intel 7110> **show utl_lowwater** Utilization Low water mark [%]: 60
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** : Intel 7110> **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** : Intel 7110> **show ovl_window** Check for overload conditions [sec]: 10

5.5.8 設定コマンド

コマンド	説明
show config	**現在の（揮発性の）設定内容を表示します。** **例** : Intel 7110> **show config** **（設定パラメタが表示されます** ...**）** Intel 7110>
show config saved	**保存されている（不揮発性の）設定内容を表示します。** **例** : Intel 7110> **show config saved** Saved configuration ========== **（設定パラメタが表示されます** ...**）** Intel 7110>

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** : Intel 7110> **show config default** Default configuration ========== conlog 0xfffffef 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 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 defcert_cname US defcert_state California defcert_city San Diego defcert_orgname Intel Corporation defcert_orgunit Network Equipment Division defcert_name www.intel.com defcert_email support@intel.com prompt Intel 7110>
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。設定とテストを柔軟に行えるように、**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** : Intel 7110> **config compare** Only in /keys: 4 Intel 7110>

コマンド	説明
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。** **例** : Intel 7110> **config reset** Reverting to saved configuration. Reset (y/n) [n]: **y** Reverting 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。** **例** : Intel 7110> **config default** Reset to factory default configuration [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。** **例** : Intel 7110> **config save** Saving configuration to flash... Configuration saved to flash Intel 7110>
export config	**すべての設定内容と鍵、署名または電子証明書情報をエクスポートします（**ascii、xmodem**）。** **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** : Intel 7110> **export config** Export protocol: (xmodem, ascii) [ascii]:**<Enter>** Press any key to start, then again when done... # default config file created on Mon Feb 14 13:56:46 2000 **(... 設定内容が表示されます ...)** Intel 7110>

コマンド	説明
import config	**設定をインポートします（**paste、xmodem**）。** **例** : Intel 7110> **import config** Import protocol: (paste, xmodem) [paste]:**<Enter>** Type or paste in data, end with ... alone on line . . . Do you want to install this config ? [y]: **n** Intel 7110>
import upgrade	**ソフトウェアアップデータ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、付録を参照）。** **例** : Intel 7110> **import upgrade** Import protocol: (xmodem) [xmodem]:**<Enter>** Start xmodem upload now Use Ctl-x to cancel upload Verifying upgrade image... upgrade image valid vesion x..x, build xx 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。**

コマンド	説明
import patch	**ソフトウェアアップグレードの一部をインポートします。** **例** : Intel 7110> **import patch** Enter patch name [80.patch] **<patch name>** Import protocol: (xmodem) [xmodem]: Start xmodem upload now Use Ctl-x to cancel upload Patch: Imported.
factory_default	**出荷時の設定に戻します。** **例** : Intel 7110> **factory_default** Reset to default configuration [n]: **y** Reset to factory defaults System rebooting...done T941 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:

5.5.9 管理コマンド

コマンド	説明
password	**パスワードを設定します。** **例** : Intel 7110> **password** Old password:**<xxxxx>** Enter new admin password (5 chars min.):**<yyyyy>** Retype new password:**<yyyyy>** Intel 7110>
show info	**ソフトウェアのバージョン情報を表示します。** **例** : Intel 7110> **show info** ========== Intel(R) NetStructure(tm) 7110 e-Commerce Accelerator === Copyright (c) 2000 Intel Corporation === All rights reserved. === === Version 2.3.1, Build 122 ==========
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。** **例** : Intel 7110> **set date** Year [2000]: Month [2]: Day [16]: Hour (24 hour clock) [15]: Minute [10]: The system must reboot for new time to set. Reboot? [y]: **n** Intel 7110>
show date	**現在の日付と時刻を表示します。**
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」（→** 32 **ページ）を参照）。**

コマンド	説明
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** : Intel 7110> **set ether** 1 - auto 2 - 10baseT, half duplex 3 - 10baseT, full duplex 4 - 100baseTX, half duplex 5 - 100baseTX, full duplex Select media type [1]: Media set to auto Intel 7110>
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** : Intel 7110> **show ether** Ethernet media set to auto Intel 7110>
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。** <n> **分間キーボード操作が行われない場合は、そのユーザは自動的にログオフします。** **構文** : Intel 7110> **set idleto <n>** <n> **は制限時間の値（分）です。有効な入力値は** 0 **～** 525600 **です。**0 **に設定すると、コンソールタイムアウトは無効になります。**
show idleto	**コンソールタイムアウト値を表示します。** **例** : Intel 7110> **show idleto** Idle timeout is 5 minutes Intel 7110>
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。（この行数ごとにスクロールが止まります。）** **構文** : Intel 7110> **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、表示の最後までスクロールします。**

コマンド	説明
show more	**コンソールディスプレイの表示ページの長さの設定を表示します。** **例** : Intel 7110> **show more** Paging set [lines per page]: 23
nic	**ネットワークインターフェースカード設定を行います。** **例** : Intel 7110> **nic** 1 - auto 2 - 10baseT, half duplex 3 - 10baseT, full duplex 4 - 100baseTX, half duplex 5 - 100baseTX, full duplex Select media type [1]: Media set to auto
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** : Intel 7110> **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]: **<Enter>** Intel 7110>
show serial	Console **ポートの通信パラメタを表示します。** **例** : Intel 7110> **show serial** Speed : 9600 Bits : 8 Stop bits : 1 Parity : n Intel 7110>
exit	CLI **からログアウトします。** **例** : Intel 7110> **exit** Exiting CLI...

5.5.10 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およびトレースファイルをエクスポートします。** **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** : Intel 7110> **export log <logID>** <logID> **は、エクスポートされるログの** ID **です。** **例** : Intel 7110> **export log 20001120_095345** Export protocol: (xmodem) [xmodem]: **<Enter>** Use Ctrl-X to kill transmission Beginning export...
delete log <logID>	**保存されているログおよびトレースファイルを** /flash/logs **ディレクトリから削除します。** **構文** : Intel 7110> **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** LogID **を表示します。**
show logs	list logs **と同じです。**

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 はリモートで管理することができます。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

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 を使って、リモート管理の設定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（使用方法については、この後のセクションで説明します）。これらのコマンドを以下に示します。

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 <1-5> 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** :

- setsnmp snmp <enable | disable> は、SNMP 管理機能の有効／無効を切り替えます。
- showsnmp 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。
- setsnmp 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
- showsnmp snmp_info は、SNMP の現在の情報およびパラメタを表示します。

- setsnmp 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。
- setsnmp 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、ポート 443 を telnet や SSH、SNMP のために使用できないことを注意してください。

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。

```
Intel 7110> set ip
Enter IP Address ('none' to delete)[10.1.2.56]: 10.1.1.1
Enter Netmask ('none' to delete)[255.255.255.0]: <Enter>
```

IP アドレスおよびネットマスクを確認します（任意）。

```
Intel 7110> show ip
        System IP Address : 10.1.1.1
        System Netmask : 255.255.255.0
Intel 7110>
```

リモート Telnet セッションを有効にします。

```
Intel 7110> set telnet enable
```

ネットワークルートを設定します。

```
Intel 7110> set route
Enter Default Route ('none' to delete)
[10.1.1.1] : 10.1.1.2
```

ルート設定を確認します（任意）。

```
Intel 7110> show route
        Default Route : 10.1.1.2
```

削除するには以下のコマンドを使用します。

```
Intel 7110> set route none
```

以上で SSLAccelerator のリモート Telnet 管理機能が設定され、使用できるようになりました。これで、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 上で有効にしたら、以下の手順で SSLAccelerator の CLI にアクセスします。

```
Unix-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」（→ 103 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、「**MaxRemote 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、セッションを終了するか、許可されるセッションの最大数を増やしてください。**

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> または show telnet_port 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。

```
Intel 7110> set telnet_port 230
```

Telnet ポートを表示するには、次のようにします。

```
Intel 7110> 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。そのための手順を以下に示します。

```
Intel 7110> 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。

```
Intel 7110> 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。

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。

```
Intel 7110> set ip
Enter IP Address ('none' to delete)[10.1.2.56]: 10.1.1.1
Enter Netmask ('none' to delete)[255.255.255.0]: <Enter>
```

IP アドレスおよびネットマスクを確認します（任意）。

```
Intel 7110> show ip
        System IP Address : 10.1.1.1
        System Netmask    : 255.255.255.0
Intel 7110>
```

リモート SSH セッションを有効にします。

```
Intel 7110> set ssh enable
```

ネットワークルートを設定します。

```
Intel 7110> set route
Enter Default Route ('none' to delete)[10.1.1.1] : 10.1.1.2
```

ルート設定を確認します（任意）。

```
Intel 7110> show route
        Default Route : 10.1.1.2
```

削除するには以下のコマンドを使用します。

```
Intel 7110> set route none
```

以上で SSLAccelerator のリモート SSH 管理機能が設定され、使用できるようになりました。これで、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」（→ 103 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、セッションを終了するか、許可されるセッションの最大数を増やしてください。**

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> または show ssh_port 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。

```
Intel 7110> set ssh_port 220
```

SSH ポートを表示するには、次のようにします。

```
Intel 7110> show ssh_port
      SSH Port Number : 220
```

6.3.4 SSH の無効

SSH 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。そのための手順を以下に示します。

```
Intel 7110> set ssh disable
```

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。

```
Intel 7110> 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。Intel 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、spill、throttle の監視

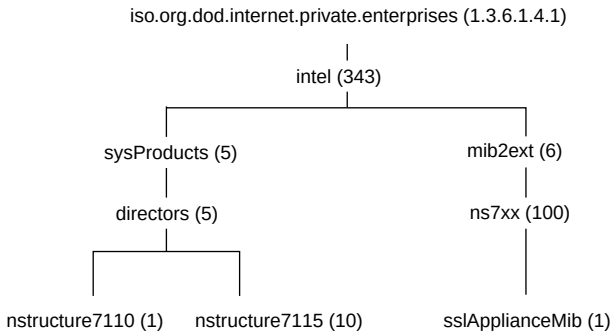
⚠注意 **SNMP 管理機能として SNMP マネージャからの SET には対応していません。SNMP 情報は参照のみでリモートから変更をかけることはできません。**

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。Intel 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 Intel プライベート 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、Intel MIB ツリーの最上位を示しています。



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

ceo-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フロッピィディスクに、SSLAccelerator が使用する Intel 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。

ceo-header.my

ceo-header.my には、Intel® NetStructure™ 製品に対して定義された sysObjectId がすべて含まれています。sysObjectId はすべて、Intel ツリーの sysProducts/directors ブランチの下で定義されます。

この MIB ファイルには、SSLAccelerator に対して、以下のような sysObjectId が定義されています。

- 7110 {343, 5, 5, 1}
- 7115 {343, 5, 5, 10}

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): Two ethernet segments fail open, stopping traffic
through(2): Two ethernet segments fail shorted, allowing traffic to continue

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 hi water mark, CPU utilization state is in alert and is not returned to normal until the lo 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 hi water mark, sslCpsState is in alert and is not returned to normal until the lo 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 lowater 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 lastsslOverloadInterval, 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

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 setsnmp snmp <enable|disable> を使用します。動作状況を調べるには、showsnmp snmp コマンドを使用します。

例 :

```
Intel 7110> setsnmp snmp enable
        SNMP Service started.
Intel 7110> showsnmp snmp
SNMP: enabled
Intel 7110> setsnmp snmp disable
        SNMP Service stopped.
Intel 7110> showsnmp 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、setsnmp 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。

```
Intel 7110> setsnmp snmp_info
SNMP Port [161]: 161
SNMP Trap Port [162]: 162
Contact Person []: support
System Location []:
System Name []: 7110
```

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

```
Intel 7110> showsnmp snmp_info
        SNMP Port Number      : 161
        SNMP Trap Port Number : 162
        SNMP System Contact   : support
        SNMP System Name      : 7110
        SNMP System Location  :
        System IP Address     : 10.1.1.1
        System Netmask: 255.255.255.0
        Default Route: 10.1.1.2
```

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。

- setsnmp snmp_port は、SNMP port を設定します
- setsnmp trap_port は、SNMP trap port を設定します
- setsnmp sys_contact は、Contact Person を設定します
- setsnmp sys_name は、System Name を設定します
- setsnmp sys_location は、System Location を設定します

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。

- showsnmp snmp_port
- showsnmp trap_port
- showsnmp sys_contact
- showsnmp sys_name
- showsnmp sys_location

■ コミュニティ文字列

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 setsnmp snmp_community 、list snmp_community 、delete snmp_community を使用します。

```
Intel 7110> setsnmp snmp_community
SNMP Community String(s) Setting.
Enter a SNMP Community IP(q to quit): 10.1.1.1
Enter a SNMP Community String(q to quit): public
Enter a SNMP Community IP(q to quit): q
Intel 7110>

Intel 7110> list snmp_community
SNMP Community String(s) information.
     <1> Current SNMP Community String(s):
      1.)IP:    10.1.1.1 => String: public =>Rights: read

Intel 7110> delete snmp_community
SNMP Community String(s) Deletion.
     <2> Current Available SNMP Community String(s):
      1.)IP:    10.1.1.1 => String: public =>Rights: read
      2.)IP:    10.1.1.2 => String: private =>Rights: read
Enter number (1 to 2) to delete (q to quit) [1]: 2
Enter number (1 to 2) to delete (q to quit) [1]: 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

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 setsnmp trap_community 、list trap_community 、delete trap_community を使用します。

```
Intel 7110> setsnmp trap_community
SNMP Trap Community String(s) Setting.
Enter a SNMP Trap Community IP (q to quit):10.1.1.6
Enter a SNMP Trap Community String (q to quit):private
Enter a SNMP Trap Community IP (q to quit):10.1.1.7
Enter a SNMP Trap Community String (q to quit):public
Enter a SNMP Trap Community IP (q to quit): q

Intel 7110> list trap_community
SNMP Trap Community String(s) information.
    <2> Current SNMP Trap Community String(s):
      1.) IP:   10.1.1.6 => String: private
      2.) IP:   10.1.1.7 => String: public

Intel 7110> delete trap_community
SNMP Trap Community String(s) Deletion.
    <2> Current Available SNMP Trap Community String(s):
      1.) IP:   10.1.1.6 => String: private
      2.) IP:   10.1.1.7 => String: public
Enter number (1 to 2) to delete (q to quit) [1]: 2
Enter number (1 to 2) to delete (q to quit) [1]: q
```

⚠注意

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」（→** 125 **ページ）を参照してください。**

6.5 アクセス制御

SSLAccelerator は、block コマンドおよび permit コマンドを用意しています。このコマンドを使用すると、IP アドレス、IP マスク、ポート、ポートマスクに基づいて、クライアントによるサーバへのアクセスを制御することができます。
IP アドレス および IP マスクを指定して、クライアントによる特定のサーバへのアクセスを禁止するには、以下に示すように、create block コマンドを使用します。

```
Intel 7110> 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: 80
Server Port mask [0xffff]:<Enter>
```

ポイント

block **の設定および** permit **の設定を表示、削除するには、「**5.5.4 **マッピングコマンド」（→** 79 **ページ）を参照してください。**

IP アドレスおよび IP マスクを指定して、クライアントによる特定のサーバへのアクセスを許可するには、以下に示すように、create permit コマンドを使用します。

```
Intel 7110> 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 [xx]: 443
Server Port mask [0xffff]: <Enter>
```

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*/
```

ここで、

A: Identifies the message as an alarm (as opposed to a monitor report).

yyyymmddhhmmss: The timestamp.

ALARM_CODE: The alarm type: [ESC|RSC|UTL|OVL|NLS].

MODIFIER: The alarm modifier, a code identifying the event that triggered the alarm.

EXTENDED_DATA: Any additional relevant data.

/*message*/: Human-readable text description of the alarm.

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	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。

```
Intel 7110> set alarms all
Intel 7110> show alarms
Alarms set: esc rsc utl ovl nls
Intel 7110> set alarms none
Intel 7110> show alarms
Alarms set:
```

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 INLINE モード／ BYPASS 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*/
```

ここで、

A: identifies the message as an alarm.
yyyymmddhhmmss: is the timestamp.
ESC: identifies the message as an Encryption Status Change Alarm.

■ アラームの修飾子およびメッセージ

HDWR: indicates crypto card failure
CONB: indicates console-controlled bypass
CONI: indicates console-controlled inline
FNTB: indicates front panel-controlled bypass
FNTI: indicates front panel-controlled inline
APPR: indicates application restart

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*/

ここで、

A: identifies the message as an alarm.
yyyymmddhhmmss: is the timestamp.
RSC: identifies the message as an Refused SSL Connections Alarm.

■ アラームの修飾子およびメッセージ

CSMM: Cipher suite mismatch
CCAF: Client certificate authenticate failure

■ 詳細情報

XXX: An integer value indicating the number of refused SSL connections that occurred in the current alarm period.

■ 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 <seconds> (Range: 5-65000, default: 15)

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 :

Intel 7110> **set rsc_window 10**
Intel 7110> **show rsc_window**
Check 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水準点を超えたとき、または、所定の最高水準点を超えたときや所定の最低水準点を下回ったときに、アラームが発行されます。最高水準点および最低水準点は、ユーザが定義します。デフォルトでは、最高水準点は 90%、最低水準点は 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|NMRL:CPU|CON|CPS:/*message*/

ここで、

A: identifies the message as an alarm.
yyyymmddhhmmss: is the timestamp.
UTL: identifies the message as an Utilization Threshold Alarm.

■ アラームの修飾子およびメッセージ

ALRT: Message: [CPU|Open connections|CPS] exceed high water mark

NMRL: Message: [CPU|Open connections|CPS] drop below low water mark

■ 詳細情報

CPU: Indicates that CPU Utilization triggered the alarm.

CON: Indicates that Total Active Connections triggered the alarm.

CPS: Indicates that Connections per Second triggered the alarm.

■ 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 <seconds> (Range: 5-65000, default: 15)

使用しきい値アラームの最高水準点を設定するには、以下のコマンドを使用します。

set utl_highwater <percentage> (Range: 2-100,default: 90)

使用しきい値アラームの最低水準点を設定するには、以下のコマンドを使用します。

set utl_lowwater <percentage> (Range: 1-99, default: 60)

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 :

Intel 7110> **set utl_window 10**
Intel 7110> **show utl_window**
Utilization window set [secs]: 10.
Intel 7110> **set utl_highwater 80**
Intel 7110> **show utl_highwater**
Utilization High water mark [%]: 80
Intel 7110> **set utl_lowwater 60**
Intel 7110> **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。

⚠警告 **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。**

形式 :

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

ここで、

A: identifies the message as an alarm.
yyyymmddhhmmss: is the timestamp.
OVL: identifies the message as an Overload Alarm.

■ アラームの修飾子およびメッセージ

SPIL: indicates overload resulting in a spill.
Message: Spill mode.

THRT: indicates overload resulting in a throttle.
Message: Throttle mode.

■ 詳細情報

XXX: An integer value indicating the total number of overload events that occurred during the most recent alarm period.

■ 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。

Intel 7110> **set ovl_window <seconds>** (Range: 5-65000, default: 15)

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。

Intel 7110> **show ovl_window**

例 :

Intel 7110> **set ovl_window 10**
Intel 7110> **show ovl_window**
Check for overload conditions [sec]: 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*/

ここで、

A: identifies the message as an alarm.
yyyymmddhhmmss: is the timestamp.
NLS: identifies the message as a Network Link Status Alarm.

■ アラームの修飾子およびメッセージ

NETL: indicates the network port status.
Message: [No carrier|10Mb/s|100Mb/s][half duplex|full duplex]

SVRL: indicates the server port status.
Message:[No carrier|10Mb/s|100Mb/s] [half duplex|full duplex]

■ 詳細情報

NC: indicates no carrier.
10HDX: indicates 10Mb/s, half duplex.
10FDX: indicates 10Mb/s, full duplex.
100HDX: indicates 100Mb/s, half duplex.
100FDX: indicates 100Mb/s, full duplex.

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直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 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> 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）。

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。

```
Intel 7110> list logs
20000727_145544
Intel 7110> 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 Wrote:             0
Plain Bytes Wrote:              0
Bytes Allocated to dbufs:       0
Bytes Per dbuf:                 0

Spill Mode:                     disable
Transactions Spilled:           0
Times Thottled Accepts:         0
Bypass Mode:                    disable
L&M board status:               RESPEND INLINE
(0x00000060)
```

Network NIC: 100baseTX Half Duplex

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

---------- Configuration ----------
conlog 0xffffffef
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
defcert_cname US
defcert_state California
defcert_city San Diego
defcert_orgname Intel Corporation
defcert_orgunit Network Equipment Division
defcert_name www.intel.com
defcert_email support@intel.com
prompt Intel 7110>
trap_authen
remote_if exp0
ip 10.1.11.34
netmask 255.255.0.0
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
*/
Intel 7110>
```

status alarms コマンドの使用例を示します。

```
Intel 7110> 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 */
Intel 7110>
```

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、CLI monitor... 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」（→ 138 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、mode、failmode、CPU、SSLCS、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。

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

ここで、

M Monitor report yyyymmddhhmmss Timestamp
mode Bypass mode status [INLINE|BYPASS]
failmode Fail mode status [SAFE|THRU]
CPU;i,k,a CPU%; (i)dle, (k)ernel, (a)pplication
SSLCS;c,m,t SSL Connections per Second;(c)urrent, (m)ax, (t)otal
OVR;r,c,m,t Overload events; (r)esponse[SPIL|THRT], (c)urrent, (m)ax,(t)otal
NetIF;s Net interface; (s)tatus
[NC|10HDX|10FDX|100HDX|100FDX]
SvrIF;s Svr interface; (s)tatus
[NC|10HDX|10FDX|100HDX|100FDX]
BES;c,m,t Bytes Encrypted per Second;(c)urrent, (m)ax, (t)otal
BDS;c,m,t Bytes Decrypted per Second;(c)urrent, (m)ax, (t)otal

■ 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ための CLI コマンドです。デフォルトやレンジが設定されたコマンドもあります。

set monitoring_interval <seconds> (Range: 5-65000; Default: 15)
show monitoring_interval
set monitoring_fields <fields> (Range: all,mode, failmode, cpu, cps, ovrld, link, enc, dec; Default: mode, failmode, cpu, cps, ovrld)
show monitoring_fields
set monitoring enable|disable (Default:disable)
show monitoring

例 :

Intel 7110> **set monitoring_interval 15**
Intel 7110> **show monitoring_interval**
Monitoring report interval [secs]: 15
Intel 7110> **set monitoring disable**
Intel 7110> **show monitoring**
Monitoring for this terminal: disabled
Intel 7110> **set monitoring_fields all**
Intel 7110> **show monitoring_fields**
Monitoring report fields: mode failmode cpu cps ovrld link enc dec
Intel 7110> **set monitoring enable**
Intel 7110> **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てしまう場合があります。**
export/import **コマンドを使用する場合は以下のコマンドによってモニタ機能を無効にしてください。**

Intel 7110>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。

■ 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。
すべての LED が点滅している。	起動中の自己診断。	SSLAccelerator は起動時に自己診断を行います。起動中以外にこの現象が発生する場合は、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 ポート、Server 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.4 障害／バイパスモード」（→ 158 ページ）を参照。）
HTTP 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。	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.4 障害／バイパスモード」（→ 158 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「■ マッピング」（→ 54 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。 Intel 7110> **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.5 対応している暗号方式」（→ 160 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。 Intel 7110> **set client_tmo <n>** <n> 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」（→ 46 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	**サーバポートとネットワークポートが、異なるメディア設定を自動認識している。**	status **コマンドを使用して、メディア設定を確認します。** Intel 7110> **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：** Intel 7110> **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 **に、**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 エンドユーザライセンス

Intel Corporation
END USER TERMS AND CONDITIONS OF SALE AND SOFTWARE LICENSE

IF THE PRODUCT IS PURCHASED DIRECTLY FROM INTEL AND UNLESS SUCH PARTIES HAVE ENTERED INTO A BILATERALLY EXECUTED AGREEMENT, WHICH EXPRESSLY TAKES PRECEDENCE, THE TERMS AND CONDITIONS STATED HEREIN WILL APPLY.

IF THE PRODUCT WAS PURCHASED FROM AN INTEL CHANNEL PARTNER, THEN ONLY SECTIONS 13-23 APPLY TO THE END USER.

1. Entire Agreement: These terms and conditions ("Agreement") for the sale of hardware and license of software, which includes the associated documentation shipped with the hardware and software ("Product"), constitute the complete and exclusive statement of all the terms of the Agreement between Intel Corporation, ("Intel") and the purchaser using the Product for its ordinary internal operation of its business and not for resale ("End User") and supersedes all prior understandings, writings, proposals, representations or communications, oral or written, relating to the subject matter hereof and unless subsequent different, contradictory or additional terms and conditions are agreed to in a writing signed by authorized representatives of both parties. In no event shall this Agreement be deemed an acceptance by Intel of any terms and conditions included with End User’s purchase order or similar End User document. Intel’s performance hereunder is expressly conditioned on End User’s assent to this Agreement.

2. Orders: End User may purchase Product by submitting a valid purchase order ("Order") to Intel at the corporate address stated herein. Orders are subject to Intel’s written acceptance ("Order Acceptance").
Order Acceptance is based in part to approval of credit by Intel to End User as set forth in the "Credit Terms" Section of this Agreement.

3. Term and Termination Date: This Agreement shall be effective on the date of the Order Acceptance and continue in effect until terminated by either party upon thirty (30) days advance written notice unless terminated earlier for breach.

4. Price: The price to be paid by End User shall be that stated on the Order as accepted on the Order Acceptance. All prices are in U.S. dollars.

5. Credit Terms: Credit terms are made at Intel’s sole discretion by analysis of End User’s current and historical financial and credit information, bank and trade references, payment practices, etc. End User agrees to provide such information to Intel upon request. Intel reserves the right to refuse payment terms if, in Intel’s sole discretion, such terms would create an unreasonable credit risk. In that event, deliveries will be available only on a C.O.D., cash-in-advance, or irrevocable letter of credit basis.

6. Delivery: Subject to the Section below entitled "Leasing/Renting," if applicable, Products shall be shipped ExWorks (1990 Incoterms), Intel's shipping dock. End User is responsible for payment of all costs relating to transportation, delivery, and insurance, which shall be pre-paid by Intel and added to the invoice, unless otherwise agreed to on the Order Acceptance. Title and risk of loss shall pass to End User upon delivery to the first common carrier except that shipments to destinations outside of the United States are subject to the "Security Interest and Reservation of Title" Section of this Agreement.

7. Security Interest And Reservation Of Title: End User hereby grants to Intel a purchase money security interest covering each shipment of Products made hereunder (and any proceeds thereof) in the amount of Intel's invoice for such shipment until Intel receives payment in full. (A purchase money security interest only applies to Products purchased by End User and the proceeds from the sale of such Products by End User.)

End User agrees to sign and execute any and all documents as required by Intel to perfect such security interest. For Products shipped to destinations outside of the United States, Intel reserves title in such Products until End User pays Intel in full for such Products, at which time title in such Products shall pass to End User (except that in the case of software, only title to the media shall pass).

8. Cancellation: Orders cancelled within five (5) days of scheduled shipment may be subject to a ten percent (10%) cancellation charge.

9. Payment Terms: Payment in full is due thirty (30) days after date of the invoice. Intel may charge End User interest on any delinquent balance at the lesser of eighteen percent (18%) per year or the maximum amount permitted by law. Intel may refuse shipment to End User if End User is delinquent in making payments to Intel.

10. Taxes and Duties: End User is responsible for all taxes imposed in connection with sale to End User of Products or services which Intel may incur under this Agreement (except taxes imposed on Intel's income) including but not limited to all import duties, customs fees, levies or imposts, and all sales, use, value added, gross receipts or other taxes of any nature and any penalties, interest and collection or withholding costs associated with any of the foregoing items. All such amounts are in addition to other amounts payable hereunder and this obligation shall survive termination or expiration of this Agreement. If applicable law requires End User to withhold any income taxes levied by the authorities of Canada on payments to be made pursuant to this Agreement ("Withholding Tax"), End User shall take advantage of the reduced Withholding Tax provided for by the Canada-United States tax treaty then in force and shall be entitled to deduct such Withholding Tax from the payments due to Intel hereunder. End User is further responsible for obtaining import licenses and preparing and submitting all required documentation in connection with importing Products including obtaining and providing to Intel International Import Certificates and other supporting documentation required by Intel in order to apply for United States export licenses.

11. Leasing/Renting: Subject to the provisions of this Section, End User may request to have Products delivered to it under a leasing/renting arrangement between End User and a lessor/owner ("Lessor"). Intel's obligations to accept any Order from Lessor and to deliver Product pursuant to such Order from Lessor are limited to the following circumstances:

11. 1. The Lessor is Intel who will retain title to the Product and accept lease or rent payments; or

11. 2. Any Lessor, other than Intel Order, provided that:

11. 2. 1. The Order indicates on its face that Lessor is ordering the Product identified in the Order on behalf of End User;

ii. The Order indicates on its face that it is in accordance with, and subject to,

iii. The terms and conditions of this Agreement; and

iv. Intel's credit department has approved the Lessor.

With respect to any Order issued by any Lessor, other than Intel, subject to any specific provisions found in a bilaterally-executed agreement between Intel and Lessor, Lessor will be considered End User's agent for the purpose of ordering Product and making payment and the rights and obligations of End User and Intel identified in this Agreement shall remain except for the following:

(1). Title to Product delivered pursuant to such Order shall be presumed vested in Lessor;

(2). The license accompanying the Product shall apply to Lessor; and

(3). Notwithstanding anything to the contrary in the license accompanying the Product, Lessor may transfer such title and license rights to End User under a leasing arrangement.

12. Returns: No Product may be returned except under warranty for repair or due to shipment error by Intel.

13. Software License: Intel grants End User a non-exclusive, non-transferable (except as set forth in this Section) non-exclusive, restricted right to use the Intel® software as incorporated in or supplied with the Intel hardware and solely in connection with the operation of the Product for End User's own internal business purposes. End User understands that Intel may update the Intel Product from time to time and such changes shall be subject to this license grant. End User may transfer the license to use the Intel software only in connection with a sale or transfer of the Product and as included with the Product and not on a standalone basis, provided the transferee agrees to be bound by the terms and condition of this Agreement. Intel and its suppliers retain all title to, and, except as expressly licensed herein, all rights to the software, all copies thereof, and all related documentation and materials. End User may not use, copy, modify, create derivative works of, distribute, sell, assign, pledge, sublicense, lease, loan, rent, timeshare, deliver or otherwise transfer the Intel software, nor permit any other party to do any of the foregoing.

14. No Modifications To Product: Product is shipped in its complete form and structure; no modifications are needed. End User shall not, nor permit any other party to modify, reverse engineer, reverse compile, or disassemble any part of Product, including any attempt to translate the Intel software, derive or attempt to derive the software source code or any part thereof. Any modification or attempt described herein will void the warranties of this Agreement.

15. Limited Software Warranty: Intel warrants to the first End User purchaser that the media containing the software is free from defects for a period of ninety (90) days from date of shipment. End User assumes responsibility for the selection of the appropriate network or computing equipment, software, and associated materials. Intel makes no warranty or representation that the software will work in combination with any third-party network or computing equipment or software, that the operation of the software will be uninterrupted or error free, or that all defects in the software will be corrected. No updates are provided under this Agreement. No warranties for third party software are provided by this warranty.

16. Limited Hardware Warranty: Intel warrants to the original owner that the product delivered in this package will be free from material defects in material and workmanship for one (1) year following the latter of: (i) the date of purchase only if you register by returning the registration card as indicted thereon with proof of purchase; or (ii) the date of manufacture; or (iii) the registration date if by electronic means provided such registration occurs within 30 days from purchase. This warranty does not cover the product if it is damaged in the process of being installed.

THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

This warranty does not cover replacement of products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing. If the product is found to be otherwise defective, Intel, at its option, will replace or repair the product at no charge except as set forth below, provided that you deliver the product along with a return material authorization (RMA) number (see below) either to the company from whom you purchased it or to Intel. If you ship the product, you must assume the risk of damage or loss in transit. You must use the original container (or the equivalent) and pay the shipping charge. Intel may replace or repair the product with either a new or reconditioned product, and the returned product becomes Intel's property. Intel warrants the repaired or replaced product to be free from defects in material and workmanship for a period of the greater of: (i) ninety (90) days from the return shipping date; or (ii) the period of time remaining on the original one (1) year warranty.

This warranty gives you specific legal rights and you may have other rights which vary from state to state. All parts or components contained in this product are covered by Intel's limited warranty for this product; the product may contain fully tested, recycled parts, warranted as if new. For warranty information call one of the numbers below.

Returning a Defective Product (RMA): Before returning any product, contact an Intel Customer Support Group and obtain an RMA number by calling the non-toll free numbers below:

North America only: (800) 838-7136 or (916) 377-7000

Other locations: Return the product to the place of purchase.

If the Customer Support Group verifies that the product is defective, they will have the Return Material Authorization Department issue you an RMA number to place on the outer package of the product. Intel cannot accept any product without an RMA number on the package.

Limitation of Liability and Remedies: INTEL SHALL HAVE NO LIABLILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING, WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL AND SPECIAL DAMAGES) ARISING FROM THE USE OF OR INABILITY TO USE THE PRODUCT, WHETHER ARISING OUT OF CONTRACT, NEGLIGENCE, TORT, OR UNDER ANY WARRANTY, IRRESPECTIVE OF WHETHER INTEL HAS ADVANCED NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES, INCLUDING, BUT NOT LIMITED TO LOSS OF USE, INFRINGEMENT OF INTELLECTUAL PROPERTY, BUSINESS INTERRUPTIONS, AND LOSS OF PROFITS, NOTWITHSTANDING THE FOREGOING, INTEL'S TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. INTEL NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you.

Europe only

Intel warrants to the original owner that the product delivered in this package will be free from defects in material and workmanship for one (1) year following the later of: (i) the date of purchase only if you register by returning the registration card as indicated thereon with proof of purchase; or (ii) the date of manufacture; or (iii) the registration date if by electronic means provided such registration occurs within 30 days from purchase. This warranty does not cover the product if it is damaged in the process of being installed.

THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

This warranty does not cover replacement of products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing. If the product is found to be otherwise defective, Intel, at its option, will replace or repair the product at no charge except as set forth below, provided that you deliver the product along with a return material authorization (RMA) number (see below) either to the company from whom you purchased it or to Intel. If you ship the product, you must assume the risk of damage or loss in transit. You must use the original container (or the equivalent) and pay the shipping charge. Intel may replace or repair the product with either a new or reconditioned product, and the returned product becomes Intel's property. Intel warrants the repaired or replaced product to be free from defects in material and workmanship for a period of the greater of: (i) ninety (90) days from the return shipping date; or (ii) the period of time remaining on the original one (1) year warranty.

All parts or components contained in this product are covered by Intel's limited warranty for this product; the product may contain fully tested, recycled parts, warranted as if new. For warranty information call one of the numbers below.

English	+44 1793 404900
French	+44 1793 404988
German	+44 1793 404777
Italian	+44 1793 404141

Returning a Defective Product (RMA): Return the product to the place of purchase for a refund or replacement.

Limitation of Liablility and Remedies: INTEL SHALL HAVE NO LIABILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING, WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL AND SPECIAL DAMAGES) ARISING FROM THE USE OF OR INABILITY TO USE THIS PRODUCT, WHETHER ARISING OUT OF CONTRACT, NEGLIGENCE, TORT, OR UNDER ANY WARRANTY, IRRESPECTIVE OF WHETHER INTEL HAS ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF USE, BUSINESS INTERRUPTIONS, AND LOSS OF PROFITS, NOTWITHSTANDING THE FOREGOING, INTEL'S TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITIES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. INTEL NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

This limited Hardware Warranty shall be governed by and construed in accordance with the Laws of England and Wales. The courts of England shall have exclusive jurisdiction regarding any claim brought under this warranty.

17. Export Law Regulations:

17. 1. Applicable Laws. End User acknowledges that all Products, spares, documentation or other materials (collectively "Product") are subject to applicable import and export regulations of the United States and of the countries in which End User transacts business, specifically including U.S. Export Administration Act and Export Administration Regulations. This Agreement is also specifically subject to U.S.

Department of Commerce regulations relating to restrictive trade practices or boycotts and the Foreign Corrupt Practices Act. In no event shall Intel be bound by any terms and conditions which contravene applicable laws. End User shall comply with all laws and regulations applicable to the Product. Without limiting the generality of the foregoing, End User agrees that it shall not export, re-export, transfer or divert any of the Product or the direct product thereof to any restricted place or party in accordance with U.S. export regulations.

17. 2. License Exceptions. End User acknowledges that certain of the Product are exported under U.S.

Export Administration Regulation license exceptions which prohibit transfer, export or re-export to military end-users or for military uses or for use with regard to nuclear, chemical or biological weapons activity including projects, design, production or stockpiling such weapons. End User is responsible for compliance with all such license exceptions.

17. 3. Responsibility for Export Licensing. Intel agrees to use commercially reasonable steps to obtain, at Intel's expense, all documentation required by the United States Office of Export Administration and/or other authorities to permit the exportation of Product to End User. End User shall take all actions and provide all information reasonably requested by Intel in order for Intel to obtain such export licenses.

Intel shall have no liability or obligation to End User if the responsible government authorities decline to issue any such export licenses. ALL ORDERS ISSUED PURSUANT TO THIS AGREEMENT ARE SUBJECT TO THE OBTAINING SAID LICENSES.

17. 4. Import Certificates. End User is responsible for obtaining and providing to Intel International Import Certificates and other supporting documentation required by Intel in order to apply for United States export licenses.

17. 5. Encrypted Products. Products containing encryption may require additional restrictions. Sale of these specific items may require End User's written consent to comply with any such additional restrictions prior to shipment of the Products.

17. 6. Letter of Compliance. Intel may require End User to execute a Letter of Compliance, as it deems reasonable to meet the requirements of applicable export regulations.

18. United States Government Legend: The software and documentation is commercial in nature and developed solely at private expense. The software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in this Agreement. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov. 1995) or FAR 52.227-14 (June 1987), whichever is applicable.

19. Copyrights; Trade Secrets: End User acknowledges and agrees that the structure, sequence and organization of the software (including but not limited to any images, photographs, animations, video, audio, music, and text) are the valuable trade secrets of Intel and its suppliers. End User agrees to hold such trade secrets in confidence. End User further acknowledges and agrees that ownership of, and Intel and its suppliers hold title to, the Product, its copyrights and patents and all subsequent copies thereof regardless of the form or media. End User may not remove from the Product, or alter, any of the trademarks, trade names, logos, patent or copyright notices or making, or add any other notices or marking to the Product.

20. Governing Law: The rights and obligations of the parties hereunder shall be construed in accordance with, and all disputes hereunder shall be governed by, the laws of the State of California excluding conflict of law rules and excluding the United Nations Convention on Contracts for the International Sale of Goods. The Superior Court of San Diego County, California and/or the United States District Court for the Southern District of California shall have jurisdiction and venue over all disputes between the parties.

21. Attorney's Fees And Costs: In any legal action to enforce this Agreement, or arising out of the sale or licensing of Products hereunder, the prevailing party shall be awarded all court costs and reasonable attorney's fees incurred.

22. Force Majeure: Intel shall not be liable to End User for any alleged loss or damage resulting from the delivery of the Products being delayed by acts of End User, acts of civil or military authority, governmental priorities, earthquake, fire, flood, epidemic, quarantine, energy crisis, strike, labor trouble, war, riot, accident, shortage, delays in transportation, or any other causes beyond Intel's reasonable control.

23. Excusable Delay: Neither party shall be liable to the other for any alleged loss or a damage resulting from a delay in performance resulting from a cause beyond the reasonable control of the party whose performance is delayed.

24. Choice Of Language. The original of this Agreement is in English and End User waives any right to have it written in any other language.

25. Notices. Any notice regarding non-performance, breach, termination, or renewal required or permitted to be given under this Agreement shall be given in writing and shall be hand delivered or deposited, postage prepaid, registered or certified mail, in the United States or other country 's mail, or sent by express delivery, addressed to End User or Intel, as the case may be, at the addresses stated on the Order or at such other address as shall be given by either one to the other in writing. All other notices may be sent by regular mail or facsimile. All notices shall be deemed given and received on the earlier of actual delivery or three (3) days from the date of postmark.

26. No Assignment: End User may not transfer or assign the Product or this Agreement to another party without the prior written consent of Intel.

A.2　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、各装置に添付の取扱説明書をご覧ください。

装置名称	SSLAccelerator 7110	SSLAccelerator 7115
接続インタフェース	LAN (100BASE-TX/10BASE-T) × 2 、**シリアル**× 2	
外形寸法	423.9(W) × 44.5(H) × 423.9 (D)mm	424.9(W) × 44.5(H) × 469.9(D)mm
質量	**最大** 3.6Kg	**最大** 4.5Kg

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.3　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。

■ 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 7 分かかります (115.2 kbps の場合)。

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。**

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] **を押して、デフォルト** (XMODEM) **を選択します。**

```
Intel 7110>import upgrade
Import protocol: (xmodem)[xmodem]: <Enter>
Start xmodem upload now
Use Ctl-X 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 Mar 3 11:31:51 2000
```

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

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

System rebooting...done
```

⚠警告 **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] を押してデフォルト (XMODEM) を選択します。

```
Intel 7110> import patch
Import protocol: (xmodem)[xmodem]:<Enter>
Start xmodem upload now
Use Ctl-X 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。万一、パッチのインポートに失敗した場合は、前回正常にインポートしたパッチが再び適用されます。

A.4　障害／バイパスモード

SSLAccelerator には、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、ネットワークリンク、インライン、サーバリンクの 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。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。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、障害が発生するか、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)。点滅状態である場合、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、点滅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、点灯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ればトラフィックはそこで遮断され、またフェイルスルーモードに設定されていれば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、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）

A.5　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。次に、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	RSA	3DES(168)	SHA1	H
IDEA-CBC-SHA	SSLv3	RSA	RSA	IDEA(128)	SHA1	M
RC4-SHA	SSLv3	RSA	RSA	RC4(128)	SHA1	M
RC4-MD5	SSLv3	RSA	RSA	RC4(128)	MD5	M
DES-CBC-SHA	SSLv3	RSA	RSA	DES(56)	SHA1	L
DES-CBC3-MD5	SSLv2	RSA	RSA	3DES(168)	MD5	H
IDEA-CBC-MD5	SSLv2	RSA	RSA	IDEA(128)	MD5	M
RC2-CBC-MD5	SSLv2	RSA	RSA	RC2(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-MD5	SSLv2	RSA	RSA	RC4(128)	MD5	M
RC4-64-MD5	SSLv2	RSA	RSA	RC4(64)	MD5	L
DES-CBC-MD5	SSLv2	RSA	RSA	DES(56)	MD5	L
EXP-DES-CBC-SHA	SSLv3	RSA(512)	RSA	DES(40)	SHA1	E
EXP-RC2-CBC-MD5	SSLv3	RSA(512)	RSA	RC2(40)	MD5	E
EXP-RC4-MD5	SSLv3	RSA(512)	RSA	RC4(40)	MD5	E
EXP-RC2-CBC-MD5	SSLv2	RSA(512)	RSA	RC2(40)	MD5	E
EXP-RC4-MD5	SSLv2	RSA(512)	RSA	RC4(40)	MD5	E

■ SSH のバージョン

以下の表は、SSLAccelerator が SSH1 と SSH2 に対して対応している暗号方式を示しています。

	SSH1	SSH2
暗号方式	3DES、DES、Blowfish	3DES、Twofish、RC4、**なし**
MAC		MD5、**なし**

A.6　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.7　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。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。

● **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。

● **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。

● **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。

● 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

た

て

と

に

ね

ひ

ふ

ほ

ま

ゆ

ら

り

ろ

C

S

T

PRIMERGY SSLAccelerator 7110/7115

取扱説明書

P3F1-0450-02-00

発行日　2001 **年** 5 **月**

発行責任　**富士通株式会社**

Printed in Japan

FUJITSU

本マニュアルは、 100%リサイクル可能な用紙を使用しています。