(2004/04/15)

SSL アクセラレータボード

SSL アクセラレータボード

1.機能仕様

型名	N8104-110
製品名	SSL **アクセラレータボード**
チップメーカ	AEP systems
チップ名	GSQ210017 CX
拡張スロットバス形式	PCI(32/64bit),33MHz **ショートサイズ**
電圧仕様	**受給電源** :3.3**V** ±5% **信号レベル**:**ユニバーサル対応**(5v/3.3v)
最大転送性能(TPS)	1000(1024bit **鍵長の場合**)
最大セッション数	1000(SSL)
サポートプロトコル	SSL2.0/3.0/TLS1.0
公開暗号化方式	RSA **の鍵交換/認証**
暗号化(鍵のサイズ)	1024bit,2048bit,4096bit
サーバ要求スペック	**メモリ**:1GB **以上** ※**1**
対応 OS	Windows 2000、 Windows Sever 2003※2、 Linux(RHL7.3、RHEL ES2.1/3)※2

※１サーバが要求スペックに満たない場合は、メモリ増設するなどの対応が必要です。

※２このＯＳへの対応は、2004 **年５月以降の新規出荷品からと成ります。**

■ SSL(Secure Socket Layer)とは

SSL とは、インターネット上でのセキュリティを確保するために、クライアント-サーバ間の相互認証と通信の暗号化を行うプロトコルです。

米 NetscapeCommunications 社が HTTP プロトコルにセキュリティ機能を組み込むために開発しました。Web の暗号化通信技術としては事実上の業界標準規格です。

SSL は、各種アプリケーションプロトコルと組み合わせて使用されます。最も有名なのは、HTTP(port 80)に適用したHTTPS(port 443)です。その他に、POP3のSSL(POP3S: Port 995)、IMAP の SSL(IMAPS: Port 993)などもあります。

一般的には、ＳＳＬのセッション開始時のやり取りは以下のように行われます。

(1) クライアントからのアクセス要求（https、POP3s、IMAPs 等）
(2) サーバから、サーバＩＤなどの各種証明書をクライアントに送る
(3) クライアントからサーバに、共通鍵生成の元となる乱数データ（プリマスタシークレット）を送付する　（クライアントより、以後のデータの暗号化に用いられる共通鍵生成の元となる乱数データを送付する。このデータはサーバＩＤによって送付されたサーバ公開鍵によって暗号化されている）
(4) サーバ、クライアント双方で先ほど送付したプリマスタシークレットを元に共通鍵を生成する
(5) お互いの共通鍵を用いて暗号化データのやり取りを開始する

■ SSL アクセラレータの特徴

ＳＳＬアクセラレータは、ＳＳＬの処理によって発生するＣＰＵ負荷の大部分を占める、ＳＳＬのハンドシェイク中に行われる公開鍵暗号の復号に必要な処理などを、サーバのＣＰＵに代わって高速に実行することで、ＣＰＵ負荷を低減させ、サーバのパフォーマンスを向上させます。