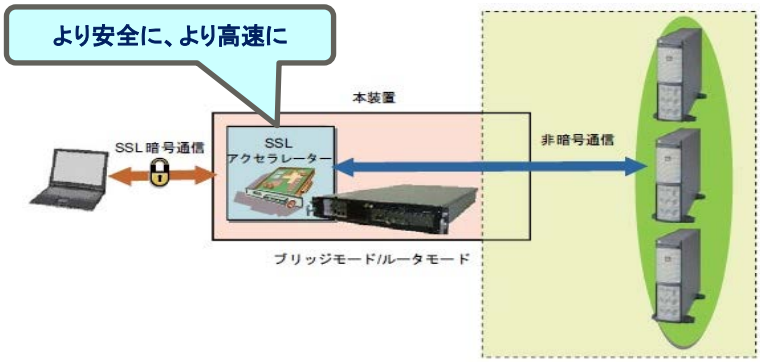
SSLアクセラレーター機能、暗号強化、性能改善

ハードウェアアクセラレーションによる高強度のアルゴリズム対応と性能を実現

IPCOM EXシリーズのSSL アクセラレーター機能は、高速な暗号/ 復号ハードウェアを使用してSSL 通信を行います。WebサーバのSSL 暗号化/復号化処理をSSLアクセラレータ機能にオフロードすることにより、サーバの処理負荷を大幅に軽減できます。

また、既存の暗号アルゴリズムは時間とともに解読されるリスクが高くなっていきます。これはICT環境の処理能力が日々向上しているため、暗号の解読時間がより短くなるためです。このため、より安全な暗号アルゴリズム、より大きな鍵長の証明書を使用したSSL暗号通信が必要となります。こうして、より安全に、より高速に暗号通信を行うには、より高いSSL処理性能が必要となります。

IPCOM EXシリーズでは、暗号カードCの使用で、より安全に、より高速なSSL通信ができます。



【お客様メリット】

■通信量が増大するネットワーク環境において、より高い安全性、より高い性能でのSSL通信を実現します。

＜ 暗号カードC　搭載による暗号強化と性能改善　＞

アクセラレータハードウェア暗号カードCの搭載により、以下のSSL通信が可能となります。

- **より安全なSSL通信が可能**
  当社従来の通信方式 （ ネットワークセキュリティプロトコルにTLS1.2、
  鍵交換アルゴリズム(鍵長最大4096ﾋﾞｯﾄ証明書) にRSA、
  暗号化にAES(256)、
  ハッシュアルゴリズムにSHA2 ）
  に加えて、
  楕円曲線暗号（ECDHE_RSA）の鍵交換アルゴリズムの利用により、
  暗号強度を向上させた、より安全な通信が可能となります。

- **SSL通信処理性能を向上**
  当社の既存の暗号カードハードウェアとの比較で大幅に向上できます。
  トランザクション処理性能：EX2500 11,000TPS (アップグレードオプション使用時)
  EX2700 14,000TPS
  (鍵長2048bit　CA証明書・サーバ証明書使用時)

【仕様】

IPCOM EXシリーズのSSLアクセラレータが提供する主な機能について記述します。

SSL暗号通信には以下のプロトコル、暗号スイートをサポートします。

SSL暗号通信

■プロトコル　：TLS v1.2/v1.1/v1.0 (TLS拡張 SNI含む), SSL v3.0/v2.0
■暗号スイート：鍵交換　RSA, 楕円曲線暗号（ECDHE_RSA鍵交換アルゴリズム（※））
暗号化　AES, RC4, RC2, 3DES, DES
ハッシュ　SHA256, SHA1, MD5
中継するサービス： HTTPS, SMTPS, NNTPS, LDAPS, TELNETS, IMAPS, POP3S

（※）暗号カードC 搭載時のみ利用可能 **(製品型名：IX251CP3)**　EX2500/EX2700に搭載可能

SSLアクセラレータ機能を安全に運用するための機能です。

クライアント認証 ・・・ 正当な証明書を持っているユーザーだけにアクセスを許可

クライアント認証とは、アクセス元のサーバ（IPCOM EX）がクライアントに証明書の提示を要求して、提示されたクライアント証明書の正当性（厳格な本人特定）と信頼できる認証機関の保証の有無を検証することで、アクセスの可否を判断するしくみです。クライアント認証では、証明書の認証機関名、有効期限、公開鍵用途、失効状況の検証を行います。

IPCOMでは、以下のクラアント認証方式をサポートします。
■仮想SSLサーバ単位のクライアント認証
■HTTPパス単位のクライアント認証

SSL暗号通信と非SSL暗号通信を混在運用する場合に必要な情報のやりとり、および安全な運用に必要な機能です。

HTTPヘッダ書き換え機能

HTTPS/HTTP サービス中継時に利用できるHTTPヘッダーの操作機能をサポートします。この機能を使用することで、SSL アクセラレーター機能を利用しているIPCOMの他の機能やWebサーバにさまざまな通信中の情報を通知できます。

IPCOMでは、以下のHTTPヘッダ書き換え機能をサポートします。
■HTTPリクエストヘッダー
■HTTPレスポンスヘッダー書き換え
（ Set-cookieヘッダーにセキュア属性を付加し、非暗号通信(http)時のcookie情報漏洩を防止）

SSLアクセラレータと同時に他の機能を一台のIPCOM EXで併用でき、シンプルな運用が可能となります。

併用動作可能な機能が豊富

IPCOMがもつ他の豊富な機能とともに動作することで、安全な通信、安全な制御ができます。

- **サーバ負荷分散**
- **アクセス制御**
- **IPsec-VPN**
- **アンチウイルス**
- **HTTPコンテンツ圧縮**
- **QoS制御(帯域制御)**
- **アノマリIPS**
- **Webアプリケーションファイアーウォール**
- **Webコンテンツフィルタリング**
- **認証・検疫ゲートウェイ**
- **リンク負荷分散機能**
- **シグネチャーIPS**

お問い合わせ先

富士通コンタクトライン　0120-933-200
受付時間 9:00～17:30（土・日・祝日・当社指定の休業日を除く）

富士通公開サイト　http://jp.fujitsu.com
詳細はこちら IPCOMシリーズ：　http://fenics.fujitsu.com/products/ipcom/