MiddleWare Package

Cente® Compact SSLd

Suggestion to Embedded

概　説

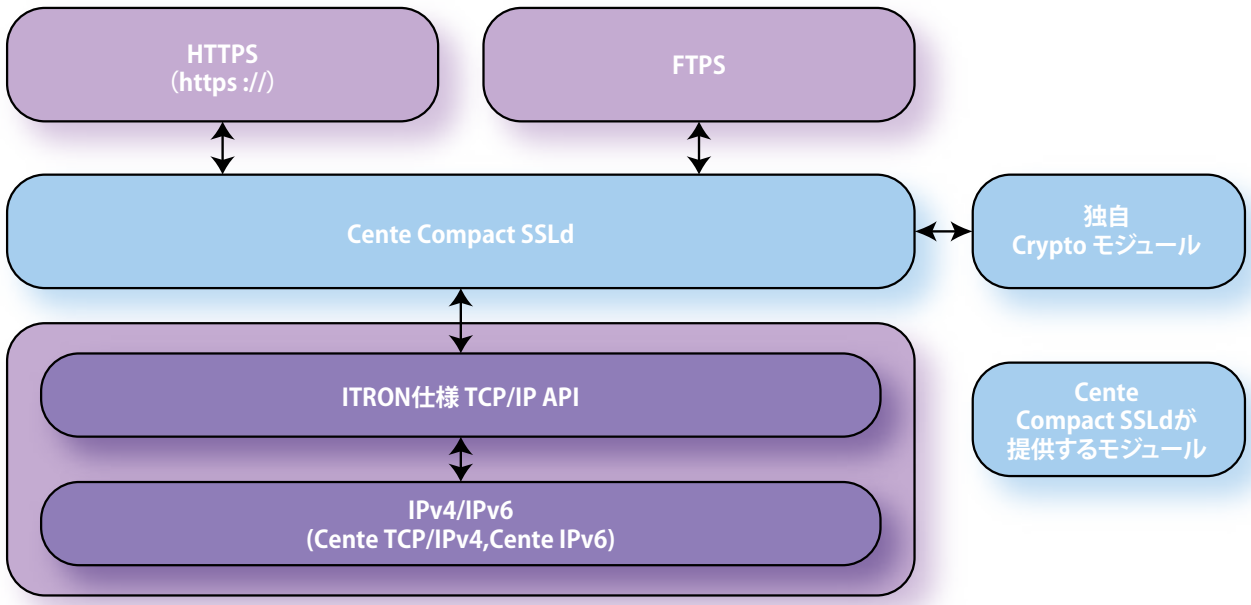
Cente Compact SSLd は IPv4/v6 通信環境上のネットワークアプリケーション間で Secure Sockets Layer（SSLv3.0）/Transport Layer Security（TLSv1.0/v1.1/v1.2）による暗号・秘匿通信を可能とする組込み開発専用のソフトウェアモジュールです。

TCP/IP のコアモジュールである「Cente TCP/IPv4」又は「Cente IPv6」と組み合わせることで、μITRON 環境上で開発された TCP/IP 通信機器を簡単にセキュア通信環境へ移行させることができます。

Cente Compact SSLd は、組込み向けにスクラッチから書き起こしたセキュリティソフトウェアモジュールです。コンパクトなメモリサイズ、高い移植性、動的メモリの不使用、拡張・変更の容易なモジュール構成など、組込み環境に適した設計となっています。

本モジュールは SSL サーバとして動作します。SSL クライアントは別製品（Cente Compact SSLc）をご利用ください。

概念図



仕様・特徴

- SSL対応バージョン SSL 3.0,TLS 1.0/1.1/1.2
- コンパクトなサイズ
  ROM：47KByte / RAM：36Byte、1接続ごとに
  +43KByte
- 暗号化アルゴリズム: ARC4, DES, 3DES, AES
- ハッシュアルゴリズム: MD5, SHA1, SHA256
- 鍵交換方式: RSA（最大鍵長はカスタマイズ可能）
- 証明書方式: X.509v1,v2,v3
- ハードウェア暗号エンジンにも対応可能
- CPU/OS/エンディアン非依存、OSリソースも非使用
  μITRON4、3、Linuxでも動作可能
- I/Oレイヤ非依存、BSDソケットにも容易に対応可能
- 通信途中の再ネゴシエーション（鍵の再生成）可能
- IPv4、IPv6両対応
- 動的メモリ不使用

MiddleWare Package

Cente® Compact SSLd

Suggestion to Embedded

■製品構成

- ●SSLdモジュール本体
- ●独自crypto（暗号・ハッシュアルゴリズム）ライブラリ
- ●shellデバッガ/共通ライブラリ

■ハードウェア暗号エンジンの使用について

●Cente Compact SSLdはソフトウェア暗号・復号アルゴリズムの他、ハードウェア暗号エンジンによる高速暗号・認証にも対応可能です。

■制限事項など

- ●証明書はDER形式のみ（PEMは非対応）
- ●私有鍵はDER形式のみ（PEMは非対応）
- ●クライアント証明には非対応
- ●セッションキャッシュ非対応
- ● CRLには非対応

■対応暗号スイート

- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256 ※

※TLS_RSA_WITH_AES_128_GCM_SHA256
Cente Compact Crypto AES-CCM/GCMを使うと、RFC5288で規定されているTLS_RSA_WITH_AES_128_GCM_SHA256を使用することができます。Cente Compact Crypto AES-CCM/GCMは別パッケージになります。

■関数一覧

ssld_init	SSL情報の初期化
ssld_set_ciphers	使用するcipher suiteを指定する
ssld_set_version	使用するバージョン（SSL 3.0,TLS1.0/1.1/1.2）を指定する
ssld_set_cert	証明書を登録する
ssld_set_privkey_rsa	RSA私有鍵を登録する
ssld_set_sock	I/Oのソケットを指定する
ssld_set_timeout	I/Oのタイムアウトを指定する
ssld_connect	クライアントとのハンドシェークを開始する
ssld_handshake	クライアントとの再ハンドシェークを開始する
ssld_write	データを送信する
ssld_read	データを受信する
ssld_read_autohs	データを受信する（自動再ハンドシェークあり）
ssld_close_notify	通信の終了を相手に通知する
ssld_write_hello_request	再ハンドシェークの要求を送信する
ssld_alert	アラートを送る

【販売・開発・製造】
データテクノロジー株式会社
〒190-0022東京都立川市錦町1-8-7立川錦町ビル8F
TEL：042-523-1177 FAX：042-523-7070
ビー・ユー・ジー森精機株式会社
〒004-0015北海道札幌市厚別区下野幌テクノパーク1-1-14

●お問い合わせ先：詳しくはサイトをご覧ください

www.cente.jp E-mail:sales@cente.jp TEL:042-523-1177

【販売代理店】