MiddleWare Package

Cente® Compact SSLc

MiddleWare Package - SSL Option

Cente® Compact DTLSc

概　説

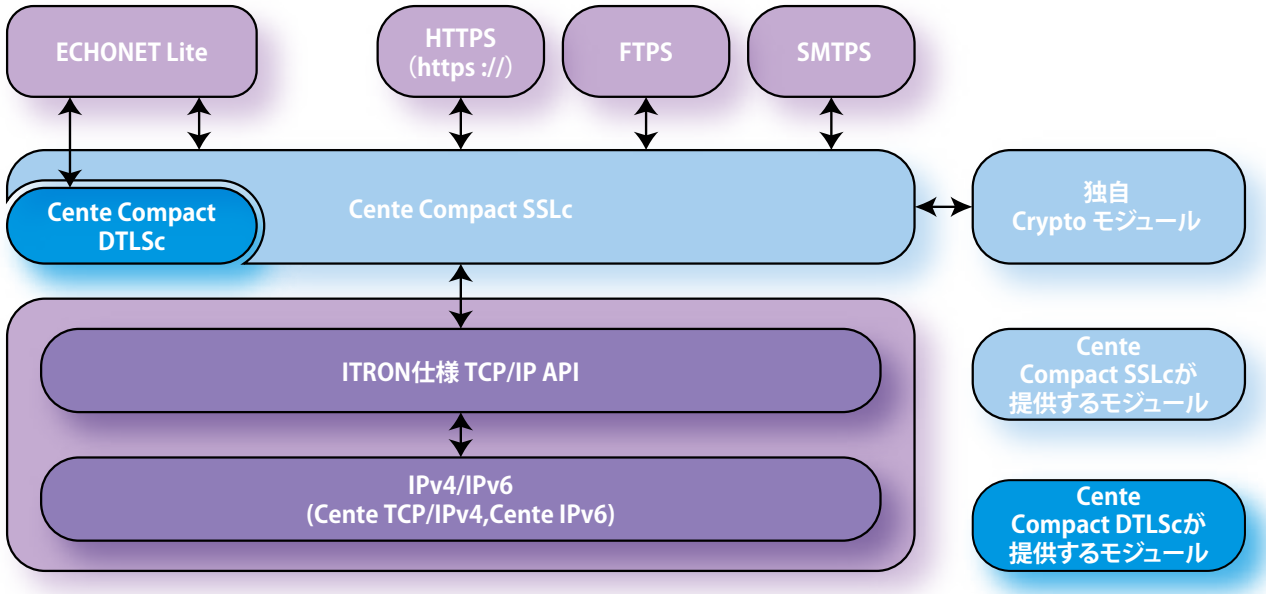
Cente Compact SSLc は IPv4/v6 通信環境上のネットワークアプリケーション間で Secure Sockets Layer（SSL v3.0）/Transport Layer Security（TLS v1.0/1.1/1.2）による暗号・秘匿通信を可能とする組込み開発専用のソフトウェアモジュールです。

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 DTLSc 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 Datagram Transport Layer Security（DTLS v1.0/1.2）による暗号・秘匿通信を可能とし、Cente Compact SSLc に組合わせて使用します。

Cente Compact SSLc / Cente Compact DTLSc は、組込み向けにスクラッチから書き起こした Security 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。

概念図



仕様・特徴

《Cente Compact SSLcパッケージ》

- 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：42KByte / RAM：100Byte、1接続ごとに+42KByte
- 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
- ハードウェア暗号エンジンにも対応可能
- 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
- 証明書の署名アルゴリズム: MD5_RSA, SHA1_RSA, SHA256_RSA
- 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
- 証明書のCommon Nameの正当性チェック機能
  （中間者攻撃の防止）
- 使用する暗号方式の優先順位を柔軟に指定可能
- IPv4, IPv6両対応
- 動的メモリ不使用
- 認証に失敗しても、強制的に接続するオプションあり

《Cente Compact DTLScパッケージ》

- DTLS対応バージョンDTLS 1.0 / 1.2
- ROM：12KByte / RAM：0Byte

MiddleWare Package

Cente® Compact SSLc

MiddleWare Package - SSL Option

Cente® Compact DTLSc

■製品構成

《Cente Compact SSLc》
- ●SSLc 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

《Cente Compact DTLSc》
- ●DTLSc モジュール本体

■ハードウェア暗号エンジンの使用について

●Cente Compact SSLc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)
- ●サーバー証明書無しには非対応
- ●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_EXPORT_WITH_RC4_40_MD5
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_EXPORT_WITH_DES40_CBC_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

《Cente Compact SSLc》	
ssl_init	SSL情報の初期化
ssl_set_ciphers	使用するcipher suiteを指定する
ssl_set_version	使用するバージョン(SSL 3.0,TLS 1.0/1.1/1.2)を指定する
ssl_add_trusted_cert	信頼するCAの証明書を登録する
ssl_set_verify_mode	証明書検証のモードを指定する
ssl_set_hostname	接続するホスト名を指定する
ssl_set_sock	I/Oのソケットを指定する
ssl_set_timeout	I/Oのタイムアウトを指定する
ssl_connect	サーバとのハンドシェークを開始する
ssl_get_verify_result	証明書の検証結果を取得する
ssl_write	データを送信する
ssl_read	データを受信する
ssl_read_autohs	データを受信する　(自動再ハンドシェークあり)
ssl_close_notify	通信の終了を相手に通知する
ssl_handshake	ハンドシェークを行う
ssl_alert	アラートを送る
《Cente Compact DTLSc》	
dtls_int	DTLScを使用する接続のSSL情報の初期化
dtls_set_timeout	データ受信のタイムアウトを指定する
dtls_get_write_size	ssl_writeで送信できるデータサイズの取得

【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】

株式会社 DTS インサイト

［東 京 本 社］〒151-0053 東京都渋谷区代々木4-30-3 新宿MIDWESTビル
TEL:03-6756-9405　FAX:03-6756-9409

URL:https://www.dts-insight.co.jp
E-mail:info-advice@dts-insight.co.jp