

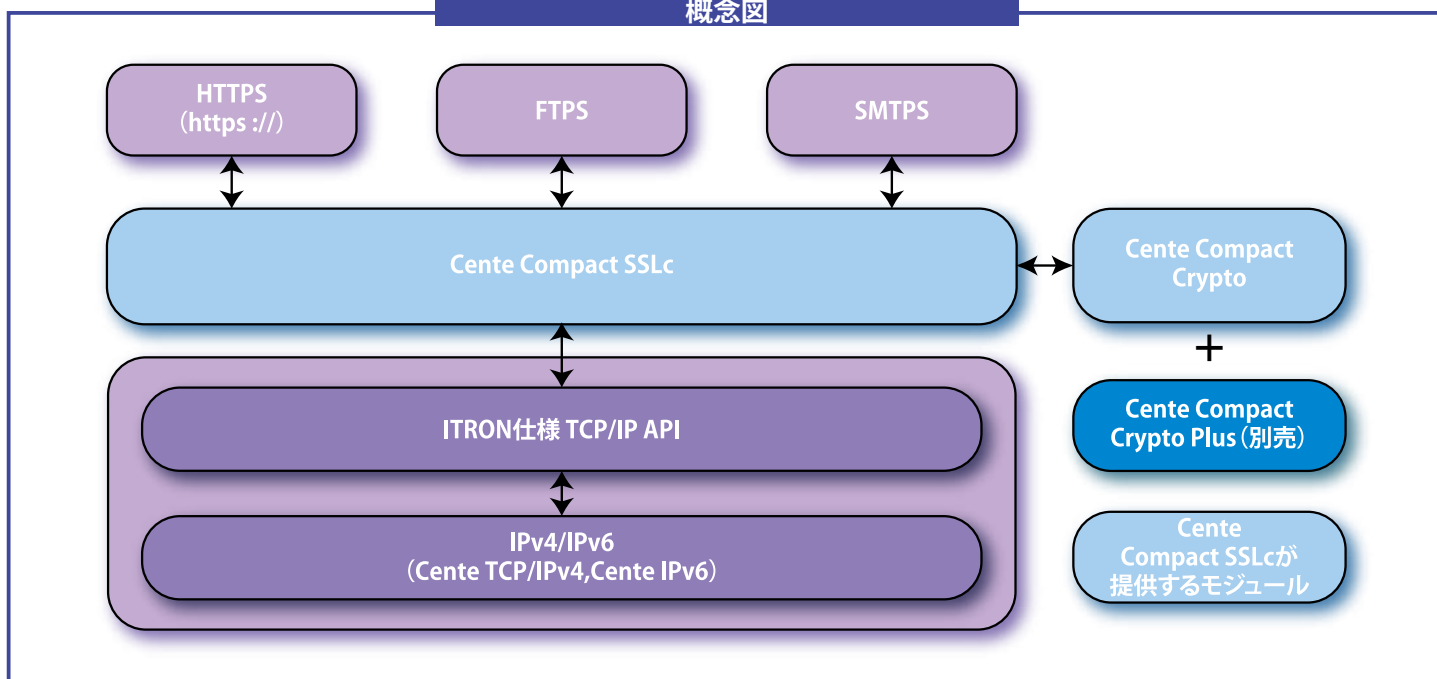
概説

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 Transport Layer Security (TLS v1.0/1.1/1.2/1.3) による暗号・秘匿通信を可能とする組み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 SSLc は TCP/IP から独立しており、BSD ソケットインタフェースでも使用可能です。

概念図



仕様・特徴

- TLS対応バージョン: (SSL 3.0) / TLS 1.0 / 1.1 / 1.2 / 1.3
 - ※SSL3.0は非推奨
 - ※TLS1.3使用時はCente Compact Crypto Plusが必要
 - コンパクトなサイズ
 - ROM: 約85KByte^(*A), 約140KByte^(*B)
 - RAM^(*A): 100Byte、1接続ごとに+約45KByte
 - RAM^(*B): 200Byte、1接続ごとに+約70KByte
 - 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, SHA384
 - ハードウェア暗号エンジンにも対応可能
 - 鍵交換方式: RSA, DHE^(*B), ECDHE^(*B)
 - (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, SHA256_DSA^(*B),
 - SHA384_ECDSA^(*B), SHA512_ECDSA^(*B)
 - Session IDによるセッション再開に対応
 - TLS Session Ticket拡張 (RFC5077) に対応
 - CPU/OS/エンディアン非依存
 - OSリソース非使用
 - 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
 - Server Name Indication (RFC6066) に対応
- ^(*A) ... Cente Compact SSLc/パッケージのみで実現
^(*B) ... Cente Compact Crypto Plusを追加した場合

■製品構成

- SSLc モジュール本体
 - Cente Compact Crypto (暗号・ハッシュアルゴリズム) ライブラリ
- ※本紙面には別売の Cente Compact Crypto Plus に関する情報も含まれます。

■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
- CRLには非対応

■関数一覧

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 1.0/1.1/1.2/1.3)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イクを開始する
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_close_notify	通信の終了を相手に通知する
ssl_handshake	ハンドシェイクを行う
ssl_alert	アラートを送る
ssl_set_sni	Server Name Indication Extensionを設定する

■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_DHE_DSS_WITH_AES_128_CBC_SHA
 TLS_DHE_RSA_WITH_AES_128_CBC_SHA
 TLS_DHE_DSS_WITH_AES_256_CBC_SHA
 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
 TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
 TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
 TLS_RSA_WITH_AES_128_GCM_SHA256
 TLS_RSA_WITH_AES_256_GCM_SHA384
 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
 TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
 TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
 TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
 TLS_AES_128_GCM_SHA256
 TLS_AES_256_GCM_SHA384
 TLS_CHACHA20_POLY1305_SHA256

(*A) ... Cente Compact SSLcパッケージのみで実現

(*B) ... Cente Compact Crypto Plusを追加した場合

【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DMG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】