MiddleWare Package

Cente® IPSec

Suggestion to Embedded

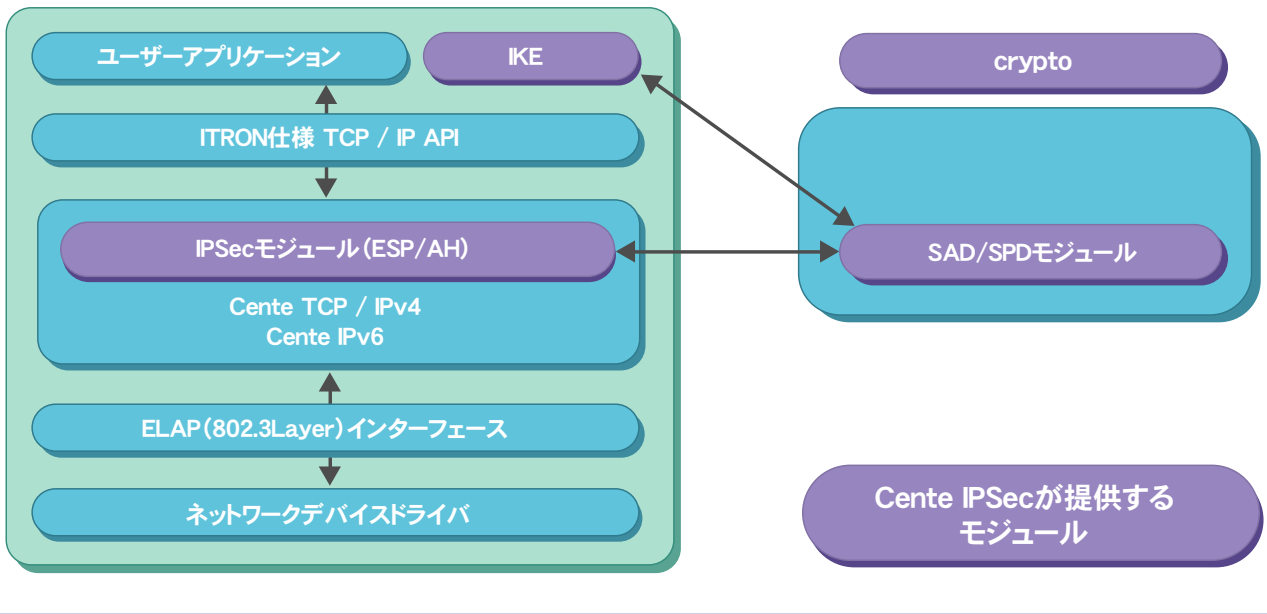
概　説

Cente IPSecはTCP/IPv4,TCP/IPv6ネットワークシステム環境上でIPSec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。

Cente TCP/IPのコアモジュールである「CenteTCP/IPv4」又は「CenteIPv6」と組合わせることで、μITRON環境で開発されたTCP/IP通信機器を、簡単にセキュアな通信環境へ移行させることができます。

Cente IPSecはソフトウェアによる暗号・認証に対応しているほか、ハードウェア暗号アクセラレータ環境でも使用可能であり、より高速な暗号化通信を行うことができます。またIKE機能も標準搭載しておりますので、より強力な次世代のセキュリティ通信が可能になります。

概 念 図



仕　様・特　長

- IPv4／IPv6(又は混在)のどちらの環境でも使用可能
- トランスポートモードをサポート
- トンネルモードをサポート
  (ただしIPv6 over IPv4, IPv4 over IPv6は未サポート)
- AHヘッダ/ESPヘッダパケット処理
- 暗号アルゴリズム:
  NULL, DES-CBC, 3DES-CBC, AES(RIJNDAEL)
- 認証アルゴリズム:MD5, SHA-1
- ハードウェアアクセラレータ(IPSecエンジン)によるアルゴリズム使用可能
- SPD/SADデータベース管理とSP/SA探索,登録,削除処理
- IKE(InternetKeyExchenge)機能を標準搭載
  - レスポンダ／イニシエータとして動作可能
  - フェイズ1モード：メインモード, アグレッシブモード
  - フェイズ2モード：クイックモード
  - フェイズ1認証方式：事前鍵共有方式
  - 暗号アルゴリズム：DES, 3DES, AES
  - 認証アルゴリズム：MD5, SHA-1
  - DHグループ：1, 2
  - PFSグループ：1, 2
- "TAHI"<http://www.tahi.org>のテスト項目をクリア

MiddleWare Package

Cente® IPSec

Suggestion to Embedded

■製品構成

- ●IPSecモジュール
- ●SAD/SPDモジュール
- ●IKEモジュール
- ●crypto(暗号・認証アルゴリズム)
- ●Shellデバッガ/共通ライブラリ

■ハードウェアアクセラレータの使用について

●Cente IPSecはソフトウェア暗号・認証アルゴリズムの他、ハードウェアアクセラレータによる高速暗号・認証にも対応可能です。
標準対応アクセラレータ:SH7710内蔵暗号エンジン

※Cente IPSecは様々なハードウェアに対応可能ですが、ハードウェアの指定や条件によって動作環境が異なりますので、別途ご相談の上でのご提供とさせていただいております。

■cryptoについて

●cryptoモジュールは、OpenSSLの各種暗号・認証アルゴリズムをベースにし、組み込み機器で利用可能にするためのカスタマイズを行った暗号・認証モジュール集です。
OpenSSL はEric A. Young とTim J. Hudson によって開発されたSSLeayというライブラリを基にし、いくつかの簡単なライセンスの制約下でなら商用・非商用の利用は自由なオープンソースです。
各アルゴリズムやソースファイルについて詳細は以下のサイトを参照してください。

- ●OpenSSL Ver.0.9.7
  http://www.openssl.org

■オプションサービス

IPSec/IKE機能の実装・動作確認は大変難易度の高い作業です。また、RFCで仕様策定中の項目も多々あり、最新のネットワーク事情に合わせた対応が必要になります。当社ではネットワーク機器開発現場での実績を踏まえ、ハードウェア/ソフトウェア両方の側面から開発をお手伝いするサービスも行っておりますのでお気軽にご相談ください。

■API関数一覧

●SAの制御API

conf_sad_add	SAを一件SADに登録
conf_sad_delete	SAを一件SADから削除
conf_sad_flush	登録されているSAの全削除
conf_sad_getstart	登録されているSAの取得開始
conf_sad_get	登録されているSAに関する情報を取得
conf_sad_getend	SAの取得終了

●SPの制御API

conf_spd_add	SPを一件SPDに登録
conf_spd_delete	SPを一件SPDから削除
conf_spd_flush	登録されているSPの全削除
conf_spd_getstart	登録されているSPの取得開始
conf_spd_get	登録されているSPに関する情報を取得
conf_spd_getend	SPの取得終了

●IKEの制御API

conf_ike_ph1_add	IKEのPhase1プロポーザルの登録
conf_ike_ph1_flush	登録されているIKE Phase1プロポーザルの全削除
conf_ike_ph2_add	IKEのPhase2プロポーザルの登録
conf_ike_ph2_flush	登録されているIKE Phase2プロポーザルの全削除

●IKEパラメータ取得関数

getParam_PSK	事前共有鍵の取得

●IPSecのテスト関数

ipsec_v4_test	IPv4上でのIPSecテスト
ipsec_v6_test	IPv6上でのIPSecテスト

■他の関連パッケージ

Cente IPv6	Cente HTTPd/c	Cente PPP	Cente SSL	Cente 802.11b/PRISM
Cente TCP/IPv4	Cente SMTP/POP	Cente SNMPv2	Cente FileSystem	Cente 802.11g/PRISM

【開発・製造・販売】

データテクノロジー株式会社

〒190-0022 東京都立川市錦町1-6-6 岩崎錦町ビル6F TEL:042-523-1177 FAX:042-523-7070

株式会社ビー・ユー・ジー

〒004-0015 北海道札幌市厚別区下野幌テクノパーク1-1-14 TEL:011-807-6612 FAX:011-807-6645

●問い合わせ先 : 詳しくはサイトをご覧ください

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

技術セミナー開催中！
www.cente.jp

【販売代理店】

[DTCT200605-CTIPSec]