MiddleWare Package

# Cente® Add-On PSK Security

Suggestion to Embedded

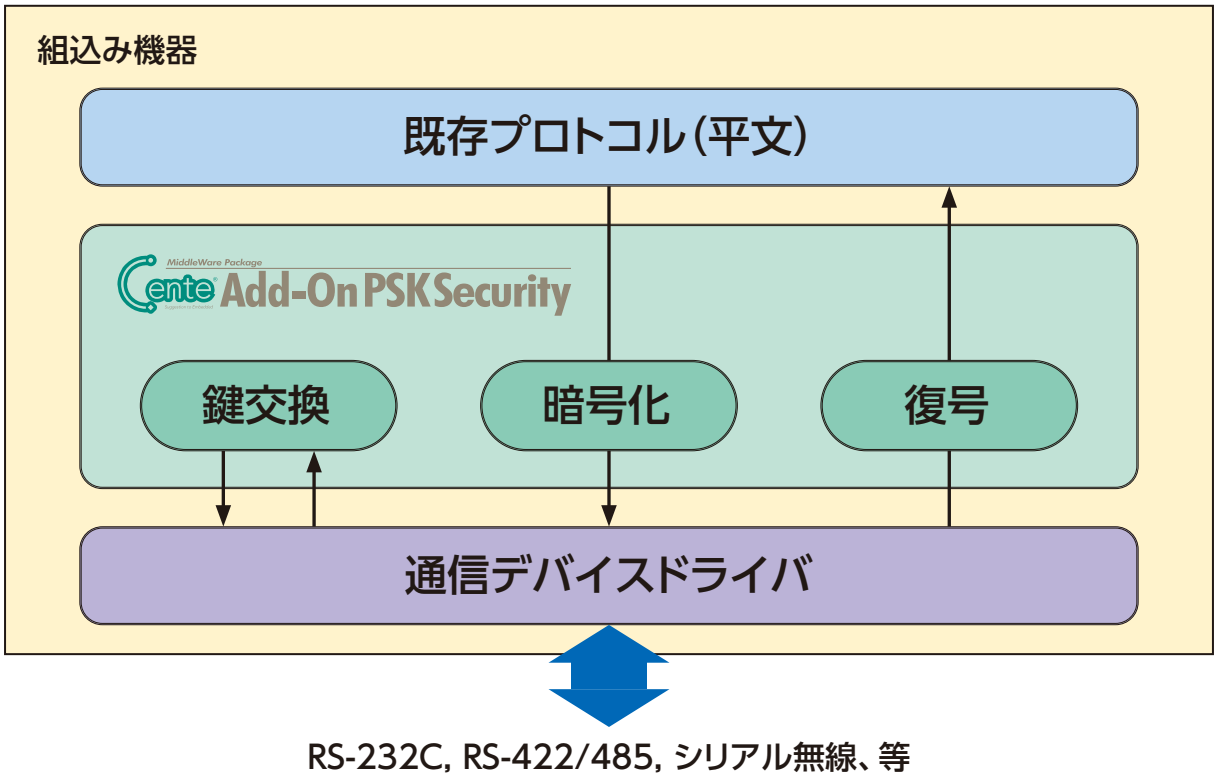
## 概　要

Cente Add-On PSK Securityは独自の通信路をセキュア化する組込みドライバです。

物理層や既存プロトコルに依存しないため、RS-232C, RS-422/485などの通信路上で動作する独自プロトコルを暗号化することが可能です。

Cente Compact SSLシリーズで培ったセキュリティ技術を投入し、小フットプリントで高強度な暗号アルゴリズム(AES256)に対応しております。既存の通信に手を入れることなく、カンタンに通信経路の高度なセキュア化を実現できます。

## 概念図




## 仕様・特長

**●既存通信プロトコルをそのまま利用**

- ✓ 独自仕様の通信処理部と通信デバイスドライバの間に組み込んでAPIをコールするだけ
- ✓ 既存の通信に手を入れることなく、カンタンに独自通信仕様のセキュア化が可能

**●小リソース環境で動作するコンパクトな設計**

- ✓ ROM/RAMサイズに余裕がない小型の組込み機器でも動作可能な小フットプリント仕様(最小:ROM: 約10KB, RAM: 約2KB)

**●書動作環境を選ばないCソースコード提供**

- ✓ CPU非依存、OS非依存のCソースコードで提供

**●セキュリティは最新強度**

- ✓ 暗号アルゴリズムはTLSでも用いられているAES256を採用
- ✓ 通信鍵も随時更新できるため、暗号文を盗聴されても解析は困難

**● 2つのトポロジーに対応**

- ✓ 動的に暗号鍵を更新する1:1向けの「個別モード」
- ✓ 暗号鍵を静的に生成するN:N向けの「共通モード」

MiddleWare Package

# Cente® Add-On PSK Security

Suggestion to Embedded

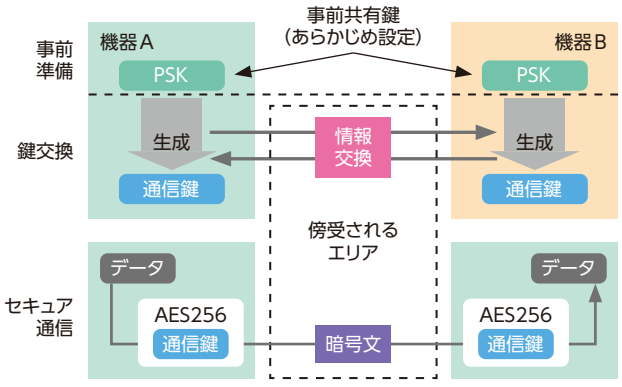
## ■API関数一覧

| ユーザ呼び出しAPI | |
|---|---|
| sersp_ini | 初期化 |
| sersp_connect | 接続 |
| sersp_disconnect | 切断 |
| sersp_write | データ送信 |
| sersp_write_with_keyid | キーID指定データ送信 |
| sersp_proc | 受信処理 |
| **ユーザカスタマイズAPI** | |
| sersp_rand_get | 乱数発生 |
| **コールバックAPI** | |
| send_data | パケット送信 |
| recv_data | データ受信 |
| notify_msg | メッセージ通知 |

| ユーザカスタマイズAPI | |
|---|---|
| sersp_rand_get | 乱数生成 |
| sersp_wai_sem | セマフォ確保(OS使用時) |
| sersp_sig_sem | セマフォ解放(OS使用時) |
| sersp_get_param | パラメータ取得 |

## ■鍵交換と暗号通信について

Cente Add-On PSK Securityの鍵交換と暗号通信は、下記流れで行われます。




## ■その他

<注意事項>
●本製品は対向側の機器と合わせてお使いください。
●製品への採用前に、低コストでお試しいただける「Cente PoCライセンス」もご用意しておりますのでご活用ください。

※本製品の仕様は、改良のため予告なく変更することがあります。

お問い合わせは、上記QRコードをご利用ください




【開発・製造・販売】
**NXTech株式会社** デジタル事業部 IoTソリューション部
〒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
**DMG MORI Digital株式会社**
〒004-0015 札幌市厚別区下野幌テクノパーク1-1-14
TEL.011-807-6666
●問い合わせ先：詳しくはサイトをご覧下さい
お問い合わせは Cente Webサイトから!
技術セミナー開催中! cente.jp

【販売代理店】