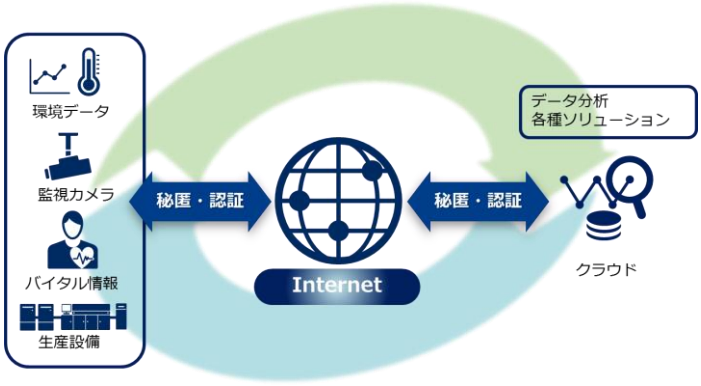
セキュアなIoTを実現する

軽量暗号 開発キット

NEC独自開発による世界トップクラスの優れた実装性をもつ軽量暗号TWINE、認証暗号OTRを各種プラットフォーム向けにソフトウェアライブラリとして提供

背景

- システムのIoT化により様々なデバイスがネットワークに接続され、データ収集、分析、対処といったデータ利活用が行われるようになります。
- 一方で、IoT化によりセキュリティリスクの懸念が高まります。IoTにおいてはセンシングデータが価値創出の源泉となるため、情報漏えいの防止やデータの信頼性確保が重要になります。



お客様の課題

- 情報漏えいが心配だが、マイコンのリソースが少なく標準暗号だと載せられない
- 情報漏えいだけでなく、改ざんによる影響も心配（データの正しさを保証したい）

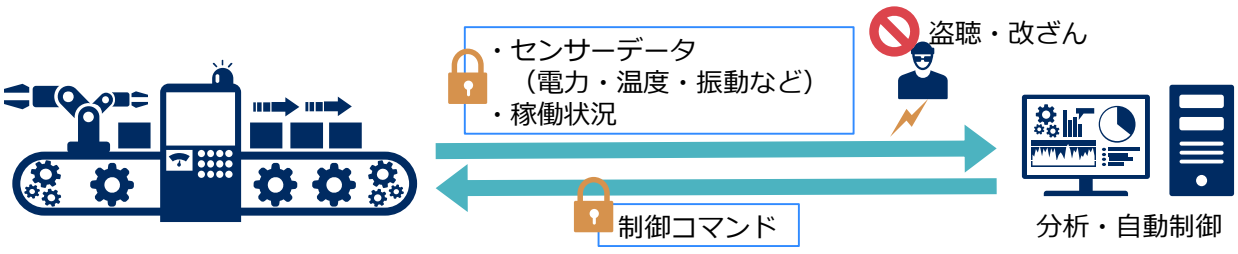
軽量暗号TWINE・認証暗号OTR

- TWINEは、ブロック長64ビット、秘密鍵長80/128ビットのブロック暗号です。AESなど標準的な暗号と同等の安全性（秘密鍵の総当たり計算量）でありながら、省リソースで実装が可能という特徴を有します。そのため、ROM/RAMの制約が大きい組み込み用途に適した暗号化方式です。
- OTRは、TWINEなどのブロック暗号をコンポーネントとして利用し、データの暗号化・復号と改ざん検知用の認証タグの生成・検証を行います。OTRはその優れた方式により、暗号化のみの場合とほぼ同じ処理時間で認証タグの生成まで行えます。またブロック暗号の復号関数を必要としないため、既存方式と比べ省メモリな実装が可能となります。

軽量暗号 開発キットの特徴

- 暗号化、復号機能のみだけでなく、鍵交換、共有鍵ベースの認証機能を用意しました。
  ユーザアプリケーション側は決められた順序でAPIを呼び出すだけで機能を実現できます。
- エッジ、クラウド向けには鍵データを暗号化して保存する機能を用意しました。
  単純なメモリダンプだけで暗号鍵が読まれることを防ぎます。
- エッジ、クラウド向けにはファイル暗号化のコマンドとしても利用可能です。
- 組込み向けには機能を限定し、ライブラリサイズは6キロバイトまで削減しました。
- ECDH鍵交換機能（拡張パックとして提供）もわずか6キロバイトで実装できます。

適用イメージ



機能・動作環境

		デバイス向け	エッジ・クラウド向け
暗号方式（暗号アルゴリズム－暗号利用モード）		• TWINE-OTR	• TWINE-OTR • TWINE-CBC • TWINE-CTR
提供機能	①データ暗号化・改ざん検知機能	○	○
	②鍵ファイル暗号化機能	ー	○
	③暗号化ファイル生成・読み込み機能	ー	○
	④相手認証機能	○	○
	⑤鍵更新機能	○	○
	⑥ECDH鍵交換機能 ※	○（Cortex-M向けのみ）	○
提供形態		✓ SWライブラリ（C言語）	✓ SWライブラリ（C言語） ✓ ファイル暗号化コマンド
対応CPU・OS		■Arm Cortex-M [ARMv6-M, ARMv7-M] ・mbed OS 5 ・No-OS ■Renesas RL78/G14 ■Renesas RX65N ・No-OS	■Intel x86／x64 互換CPU ・Debian 8 (32-bit) ・Red Hat Enterprise Linux 7.1 (64-bit) ・Red Hat Enterprise Linux 7.3 (64-bit) ・Windows 7/10（32/64-bit） ・Windows Server 2012 R2 ■Arm Cortex-A [ARMv7] ・Debian 8 (32-bit) ・Raspbian Stretch

※　軽量暗号 開発キット 拡張パックを別途ご購入ください。

機能概要

機　能	概　要
① データ暗号化・改ざん検知機能	メモリ上のデータの暗号化・復号を行います。暗号利用モードはOTR・CBC・CTRの３つに対応しています。OTRのみデータ認証機能を有します。
② 鍵ファイル暗号化機能	事前共有鍵などストレージに保存する鍵を暗号化してファイル出力します。
③ 暗号化ファイル生成・読み込み機能	データ暗号化機能により暗号化したデータを独自フォーマットでファイルに出力、読み込みをします。
④ 相手認証機能	チャレンジレスポンスによる（相互）相手認証を行います。
⑤ 鍵更新機能	エッジ・クラウド側からデバイスに対して、新しい暗号鍵を送信、共有します。
⑥ ECDH鍵交換機能	楕円曲線暗号を用いたディフィー・ヘルマン鍵交換を行います。

NEC　デジタルネットワーク事業部

https://jpn.nec.com/iot/platform/security/lcdk/

2020年9月版