

RXファミリ TSIP Security Solution

強固なセキュリティ技術で安全・安心なIoT機器を実現



<https://www.renesas.com/application/technologies/iot-security/renesas-secure-iot>

差別化ポイント

- ✓ 鍵の保護：ハードウェアセキュリティIP(Trusted Secure IP)で鍵の漏えい防止
- ✓ 簡単実装：ワンストップソリューションでIoT機器を強固に守る仕組みを構築
- ✓ 運用管理：製品出荷・市場運用・OTA・EOLまでのライフサイクル管理を支援
- ✓ 安心安全：NIST*1 FIPS140-2 レベル3のCMVP認証取得*2、堅牢で高い信頼性

*1：アメリカ国立標準技術研究所、*2：RX65N取得、CAVP認証はRX231,RX651/Nで取得

脅威から守る



- ・不正読出し、鍵/データ流出
- ・模倣品、盗聴、なりすまし
- ・乗っ取りによる不正操作
- ・システムダウン等…

ソリューション特長

高速暗号アクセラレータ

鍵漏えい防止

開発障壁低減

ハードウェア技術



脅威から守るセキュリティ専用H/W Trusted Secure IP (TSIP) 搭載

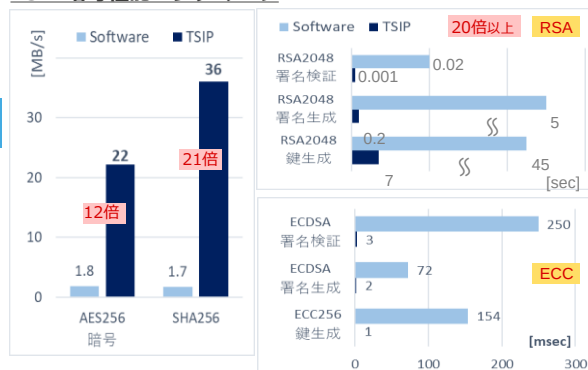
- ・TSIPで「暗号鍵」を漏えいから守る
- ・メモリ保護機能で認証プログラムを改ざんから守る

ドライバ・ソフトウェア

TSIP専用ドライバ無償提供

- ・シンプルなAPIで実装障壁を低減
- ・ドライバの最適化で暗号処理高速化
- ・秘密保持契約書(NDA)締結不要/無償

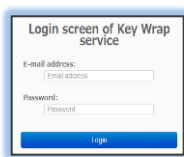
TSIP暗号性能ベンチマーク 専用H/W+ドライバで高速処理を実現



ツール・サービス



Security Key Management Tool



Key Wrap Service

- ・ライフサイクルに合わせた鍵運用(鍵生成/鍵書き込み/鍵更新)をサポート
- ・安全な鍵のインストールをサポート

セキュリティ開発ボード・IoT機器向け評価キット



RSK (Renesas Starter Kit)



EK-RX671 (Evaluation Kit)



CK-RX65N (Cloud Kit)

TSIP搭載の各種RXマイコン評価ボードで即開発着手が可能

- ・安全な鍵管理と暗号機能を即評価可能
- ・本評価キット活用で、セキュリティ導入開発期間を大幅に短縮
- ・RSKは、RX Familyの各マイコン(RX700/600/RX200シリーズ)に対応

RXファミリ TSIP Security Solution 構成要素

MCU

P/N	CPU	周波数	ROM	RAM	Security and Other Function
RX231/W	RXv2	54MHz	512KB	64 KB	TSIP-Lite ^{※1} , USB, CAN, Touch key, Bluetooth 5.0(RX23W)
RX26T	RXv3	120MHz	512KB	64 KB	TSIP-Lite ^{※1} , CAN-FD, PGA, Register Bank Save
RX72T	RXv3	200MHz	1MB	128KB	TSIP-Lite ^{※1} , USB, CAN, PGA
RX66T	RXv3	160MHz	1MB	128KB	TSIP-Lite ^{※1} , USB, CAN, PGA, Register Bank Save
RX65N/1	RXv2	120MHz	2MB	640KB	TSIP ^{※2} , LCD, Dual Bank
RX66N	RXv3	120MHz	4MB	1MB	TSIP ^{※2} , LCD, Dual Bank, Register Bank Save
RX671	RXv3	120MHz	2MB	384KB	TSIP ^{※2} , Dual Bank, Register Bank Save, Touch key
RX72N	RXv3	240MHz	4MB	1MB	TSIP ^{※2} , LCD, Dual Bank, Register Bank Save
RX72M	RXv3	240MHz	4MB	1MB	TSIP ^{※2} , LCD, Dual Bank, EtherCAT, Register Bank Save

周波数/ROM/RAMは最大値を表記

※1 : TSIP-Lite (Trusted Secure IP-Lite): AES暗号アルゴリズムに対応
※2 : TSIP(Trusted Secure IP): AES暗号の他、RSA/ECCなどの公開鍵暗号にも対応

Soft ware

P/N	Functions	Description
Trusted Secure IP Driver	共通鍵暗号 : AES/DES/3DES 公開鍵暗号 : RSA,ECC SHA1/SHA256/MD5 乱数生成器TRNG メッセージ認証,SSL/TLS 連携	・ シンプルAPIの暗号・鍵管理で簡単にセキュリティ導入 ・ 公開鍵暗号やハッシュ関数に対応し、 SSL/TLS通信アクセラレータとしても使用可能 ・ Secure Boot, Secure Updateの サンプルプログラム提供

<https://www.renesas.com/software-tool/trusted-secure-ip-driver>



Tools

P/N	ツールURL	Description
Key Wrap Service	https://dlm.renesas.com/keywrap/	・ ルネサス専用WEBページでユーザ鍵を安全に暗号化するサービス ・ 初回ユーザ登録後、すぐに使用可能 ・ ご使用マニュアルは、左記URL先の『FAQ』欄に掲載
Security Key Management Tool	https://www.renesas.com/ja/software-tool/security-key-management-tool	・ ルネサスのセキュリティIPを使用した鍵管理システムや、セキュアな機能を実現するためのサポートツール ・ ライフサイクルに合わせた鍵運用(鍵生成/鍵書き込み/鍵更新)をサポート ・ 左記URLよりダウンロード可能

Kits

P/N	カテゴリ	ラインナップ	対応マイコン
RSK (Renesas Starter Kit)	標準	RSK-RX*	* RX231, RX23W,RX66T, RX72T, RX65N, RX671, RX72M, RX72N
Evaluation kit	標準	EK-RX671	RX671
Envision Kit	LCD	RX72N Envision Kit	RX72N
Cloud Kit	IoT	CK-RX65N	RX65N
MCB	Motor	MCB-RX26T Type B	RX26T

協業パートナー様の紹介

今後もセキュリティに関する各パートナー企業との連携を強化していく計画です

会社名	提供物	概要	対応国
wolfSSL https://www.wolfssl.jp/	Security Layer Library	・ 組込みセキュリティ専門ベンダー ・ FIPS140-2認証取得 ・ RX TSIP対応SSL/TLS、DTLS etc	W/W
IARシステムズ https://www.iar.com/jp/	Embedded Trust/C-Trust IAR Embedded Workbench for RX	・ RX向けセキュリティコンテキスト対応 ・ IAR Embedded Workbenchに完全統合 ・ セキュアなマスタリングでIPを保護	W/W
ユビキタスAI https://www.ubiquitous-ai.com/	Edge Trust	・ デバイスのライフサイクルマネジメントを実現 ・ 安全なトラストチェーンを構築 ・ TSIP対応TLSライブラリ、AWS IoT接続機能を提供	W/W
NXTech https://nxttech.co.jp/	Cente AWS IoT Connect TSIP対応SSL/TLS Library	・ TLS、HTTP、MQTT、TCP/IPミドルウェア ・ TSIPに対応したSSL/TLSライブラリの提供 ・ 豊富な暗号スイートをサポート	日本
東光高岳 https://uquest.tktk.co.jp/	TSIP対応SSL/TLS Library	・ TLS、Wi-Fiドライバ、TCP/IPミドルウェア ・ TSIPに対応したSSL/TLSライブラリの提供 ・ 豊富な通信I/Fに対応した組込みソフトウェア開発支援	日本
Veridify https://www.veridify.com/	Veridify Security	・ ソフトウェアで実現するセキュリティソリューション ・ RX100 などのTSIP非搭載製品にも適用可能	W/W