

RX 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ア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…

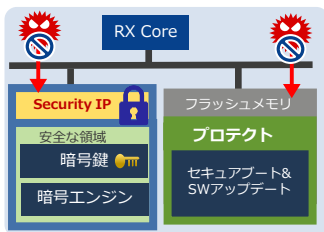
ソリューション特長

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

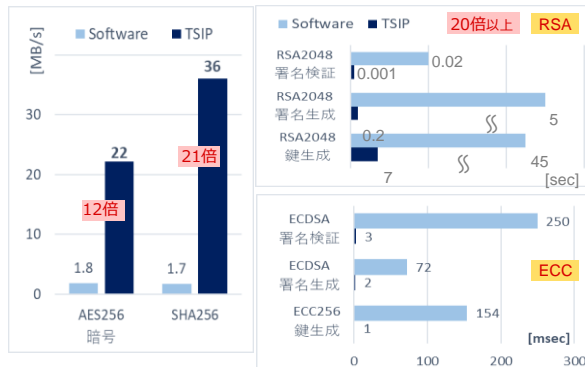
- ・TSIPで「暗号鍵」を漏えいから守る
- ・メモリ保護機能で認証プログラムを改ざんから守る

ドライバ・ソフトウェア

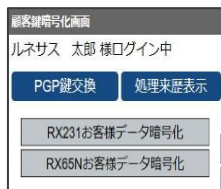
TSIP専用ドライバ無償提供

- ・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



Key Wrap Service

- ・予めお客様がユーザ鍵束を準備
- ・ルネサス専用WEBを通じてユーザ鍵束を安全に暗号化
- ・生成した暗号鍵束を無償提供

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)



GR-ROSE RX65N(TSIP)搭載

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セキュリティソリューション構成要素

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	<ul style="list-style-type: none"> 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>

* Trusted Secure IP Driverは、海外輸出時の外為法リスト規制該当品の扱いとなります

Tools	P/N	ツールURL	Description
	Key Wrap Service	https://dlm.renesas.com/keywrap/	<ul style="list-style-type: none"> 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

Kits	P/N	対応マイコン	Status	対応国***	ご購入方法
	RSK (Renesas Starter Kit)	RX231, RX23W,RX66T, RX72T,RX65N, RX66N**, RX671, RX72M, RX72N	MP	W/W	チップワンストップ (取り扱いのない物はお担当取扱店/営業経由でお問合せください)
	Renesas Flexible Motor Control CPU Board	RX26T	MP	W/W	チップワンストップ (取り扱いのない物はお担当取扱店/営業経由でお問合せください)
	Envision Kit	RX72N	MP	W/W	チップワンストップ マルツエレクト
	GR-ROSE	RX65N	MP	W/W	秋月電子通商 チップワンストップ マルツエレクト
	CK-RX65N (RYZ014A)	RX65N	MP	W/W	チップワンストップ

** : RX72Nでご評価下さい *** : 一部の製品は、海外輸出時の外為法リスト規制該当品の扱いとなります

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	強み	対応国
wolfSSL Inc. https://www.wolfssl.jp/	Security Layer Library	<ul style="list-style-type: none"> 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システムズ株式会社 https://www.iar.com/jp/	Embedded Trust/C-Trust IAR Embedded Workbench for RX	<ul style="list-style-type: none"> 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
株式会社ユビキタスAI https://www.ubiquitous-ai.com/	Edge Trust	<ul style="list-style-type: none"> 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
ITbookテクノロジー株式会社 https://www.itbook-tec.co.jp/	Cente AWS IoT Connect TSIP対応SSL/TLS Library	<ul style="list-style-type: none"> 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
株式会社東光高岳 https://uquest.ttkk.co.jp/	TSIP対応SSL/TLS Library	<ul style="list-style-type: none"> 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 Security Inc. https://www.veridify.com/	Veridify Security	<ul style="list-style-type: none"> 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