発行日：2024年4月17日

RENESAS TECHNICAL UPDATE

〒135-0061 東京都江東区豊洲 3-2-24 豊洲フォレシア
ルネサス エレクトロニクス株式会社
問合せ窓口 https://www.renesas.com/jp/ja/support/contact/

製品分類	MPU & MCU	発行番号	TN-RX*-A0277A/J	Rev.	第1版
題名	Trusted Secure IP Lite (TSIP-Lite) の使用に関する注意事項		情報分類	技術情報	
適用製品	RX231 グループ、RX23W グループ、 RX26T グループ、RX66T グループ、 RX72T グループ	対象ロット等 全ロット	関連資料	各製品のユーザーズマニュアル ハードウェア編 (詳細は最終ページの表をご参照ください)	

上記適用製品の Trusted Secure IP Lite (TSIP-Lite) モジュールにおいて不具合がありましたので、以下のとおり連絡いたします。

1. 注意事項

Trusted Secure IP Lite (TSIP-Lite) モジュールを使用して、CCM 演算や、鍵長 256 ビットの AES 鍵の注入または更新を実施すると、そのタイミングにより、まれに以下のような不具合が発生する恐れがあります。

(1) CCM 演算の場合

復号処理において、メッセージ認証は合格するにもかかわらず、特定ブロックが正常に復号されない場合があります。

具体的には、TSIP ドライバの下記関数を使用した場合に本不具合が発生することがあります。

R_TSIP_Aes128CcmDecryptUpdate

R_TSIP_Aes256CcmDecryptUpdate

(2) 鍵長 256 ビットの AES 鍵の注入または AES 鍵の更新の場合

AES 鍵のラップの際に不正な動作を行うことがあります。

このため、AES 演算時に鍵をアンラップすると、エラーが発生してアンラップできなかったり、元の鍵と異なる鍵が得られたりする場合があります。

具体的には、TSIP ドライバの下記関数を使用した場合に本不具合が発生することがあります。

R_TSIP_GenerateUpdateKeyRingKeyIndex

R_TSIP_GenerateAes256KeyIndex

R_TSIP_UpdateAes256KeyIndex

2. 対策

Ver.1.20 以降の TSIP ドライバを使用することで、本不具合を回避できます。

3. 関連資料

グループ	タイトル	Rev.	ドキュメント番号
RX26T グループ	RX26T グループ ユーザーズマニュアル ハードウェア編	Rev.1.10	R01UH0979JJ0110
RX230 グループ、RX231 グループ	RX230 グループ、RX231 グループ ユーザーズマニュアル ハードウェア編	Rev.1.20	R01UH0496JJ0120
RX23W グループ	RX23W グループ ユーザーズマニュアル ハードウェア編	Rev.1.10	R01UH0823JJ0110
RX66T グループ	RX66T グループ ユーザーズマニュアル ハードウェア編	Rev.1.30	R01UH0749JJ0130
RX72T グループ	RX72T グループ ユーザーズマニュアル ハードウェア編	Rev.1.10	R01UH0803JJ0110

以上