発行日：2024年7月4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-RA*-A0116A/J	Rev.	第1版
題名	セキュア暗号エンジン(SCE5)の使用に関する注意事項		情報分類	技術情報	
適用製品	RA4M1 グループ、RA4W1 グループ、 RA6T2 グループ	対象ロット等 全ロット	関連資料	末尾の表を参照	

上記適用製品において、セキュア暗号エンジン(SCE5)に不具合があり、以下の事象が発生することがあります。
下記の条件に該当する場合は、対策に記載する対応を取ってください。

発生条件

下記の 1)または 2)に該当するときに発生します。 ()内は、関連する FSP User's Manual の章番号です。

1) 鍵長 256bit の AES 鍵を使用した演算、および AES の CCM または XTS の演算において、
以下のいずれかのモジュールで Hardware Acceleration を使用するとき
・Azure RTOS NetX Crypto HW Acceleration / rm_netx_secure_crypto (5.2.15.2 章)
・Mbed Crypto H/W Acceleration / rm_psa_crypto (5.2.15.3 章)
2) 以下のモジュールを用いて鍵長 256bit の AES 鍵を注入または AES 鍵を更新するとき
・Secure Key Injection / r_sce_key_injection (5.2.15.7 章)

発生事象

CCM 演算の条件に該当した場合
メッセージ認証は合格するが、暗号化データの特定ブロックが正常に復号されない場合がある。

鍵長 256bit の AES 鍵の演算、または XTS 演算の条件に該当した場合
演算に使用する AES 鍵のアンラップの際に不正な動作を行い、不正な AES 鍵で演算を行ってしまう場合がある。

鍵長 256bit 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い、AES 演算時に鍵をアンラップした際に元の AES 鍵と異なる場合がある。
あるいは、AES 演算時の鍵のアンラップにおいてエラーが発生することがあります。

対策

Renesas Flexible Software Package(FSP) v5.2.0 以降のドライバを使用することで、本不具合を回避できます。

関連資料表

製品	資料名
RA4M1 グループ	Renesas RA4M1 グループ ユーザーズマニュアル ハードウェア編 Rev.1.10
RA4W1 グループ	Renesas RA4W1 グループ ユーザーズマニュアル ハードウェア編 Rev.1.00
RA6T2 グループ	Renesas RA6T2 グループ ユーザーズマニュアル ハードウェア編 Rev.1.40
Renesas Flexible Software Package (FSP)	Renesas Flexible Software Package (FSP) v5.1.0 User's Manual