

【注意事項】RX ファミリ AES/RSA/SHA ライブラリ

R20TS0892JJ0100

Rev.1.00

Firmware Integration Technology

2022.11.01 号

概要

RX ファミリ AES ライブラリ Firmware Integration Technology

RX ファミリ RSA ライブラリ Firmware Integration Technology

RX ファミリ SHA ライブラリ Firmware Integration Technology

の使用上の注意事項を連絡します。

1. RXv3 CPU 製品で本ソフトウェアを使用する際の注意事項

1. RXv3 CPU 製品で本ソフトウェアを使用する際の注意事項

1.1 該当製品

表 1 に該当製品一覧を記します。

表 1 RX AES/RSA/SHA ライブラリ FIT モジュール該当製品一覧

製品名	バージョン	資料番号
RX ファミリ AES ライブラリ Firmware Integration Technology	1.06	R20AN0044JJ0106
RX ファミリ RSA ライブラリ Firmware Integration Technology	1.03	R20AN0292JJ0103
RX ファミリ SHA ライブラリ Firmware Integration Technology	1.04	R20AN0157JJ0104

1.2 該当デバイス

RXv3 CPU 製品

RX660, RX66N, RX66T, RX671, RX72M, RX72N, RX72T

1.3 内容及び発生条件

コンパイラオプションの命令セットアーキテクチャに RXv3 を指定すると、以下ビルドエラーが発生。

```
#error "None-support combination of CPU and endian"
```

ビルドエラーが発生する命令セットアーキテクチャのコンパイラオプションは以下の通りです。

CCRX : -isa=rxv3

GCC : -misa=v3

IAR : --core rxv3

1.4 回避策

エラーの発生するファイルの記述を、以下の通り書き換えて下さい。

- ・ AES ライブラリ
r_aes_version.c
r_gcm_version.c
- ・ RSA ライブラリ
r_rsa_version.c
- ・ SHA ライブラリ
r_sha_version.c

[対策前]

```
#if (defined (__RXV2) && defined (__BIG))
    #define __TARGET_CPU__ "RXV2 BIG endian"
    #define __COMPILER_VER__ (__RENESAS_VERSION__)
#elif (defined (__RXV2) && defined (__LIT))
    #define __TARGET_CPU__ "RXV2 LITTLE endian"
    #define __COMPILER_VER__ (__RENESAS_VERSION__)
#elif (defined (__RXV1) && defined (__BIG))
    #define __TARGET_CPU__ "RXV1 BIG endian"
    #define __COMPILER_VER__ (__RENESAS_VERSION__)
#elif (defined (__RXV1) && defined (__LIT))
    #define __TARGET_CPU__ "RXV1 LITTLE endian"
    #define __COMPILER_VER__ (__RENESAS_VERSION__)
#elif (defined (__RX600) && defined (__BIG))
    #define __TARGET_CPU__ "RX600 BIG endian"
    #define __COMPILER_VER__ (__RENESAS_VERSION__)
#elif (defined (__RX600) && defined (__LIT))
    #define __TARGET_CPU__ "RX600 LITTLE endian"
    #define __COMPILER_VER__ (__RENESAS_VERSION__)
#elif (defined (__RX200) && defined (__BIG))
    #define __TARGET_CPU__ "RX200 BIG endian"
    #define __COMPILER_VER__ (__RENESAS_VERSION__)
#elif (defined (__RX200) && defined (__LIT))
    #define __TARGET_CPU__ "RX200 LITTLE endian"
    #define __COMPILER_VER__ (__RENESAS_VERSION__)
```

[対策後]

```
#if (defined (__RX) && defined (__BIG))
    #define __TARGET_CPU__ "RX BIG endian"
    #define __COMPILER_VER__ (__RENESAS_VERSION__)
#elif (defined (__RX) && defined (__LIT))
    #define __TARGET_CPU__ "RX LITTLE endian"
    #define __COMPILER_VER__ (__RENESAS_VERSION__)
```

1.5 恒久対策

次期バージョンで改修予定です。(2022年11月予定)

以上

改訂記録

Rev.	発行日	改訂内容	
		ページ	ポイント
1.00	Nov.01.22	-	新規発行

本資料に記載されている情報は、正確を期すため慎重に作成したのですが、誤りがないことを保証するものではありません。万一、本資料に記載されている情報の誤りに起因する損害がお客様に生じた場合においても、当社は、一切その責任を負いません。

過去のニュース内容は発行当時の情報をもとにしており、現時点では変更された情報や無効な情報が含まれている場合があります。

ニュース本文中の URL を予告なしに変更または中止することがありますので、あらかじめご承知ください。

本社所在地

〒135-0061 東京都江東区豊洲 3-2-24 (豊洲フォレシア)

www.renesas.com

お問合せ窓口

弊社の製品や技術、ドキュメントの最新情報、最寄の営業お問合せ窓口に関する情報などは、弊社ウェブサイトをご覧ください。

www.renesas.com/contact/

商標について

ルネサスおよびルネサスロゴはルネサス エレクトロニクス株式会社の商標です。すべての商標および登録商標は、それぞれの所有者に帰属します。