【注意事項】

R20TS0634JJ0100
Rev.1.00
2020.11.01 号

# RX ファミリ
# SHA コプロセッサドライバ Firmware Integration Technology

## 概要

タイトルに記載している製品の使用上の注意事項を連絡します。

1. SHA 演算 API 関数の使用に関する注意事項

## 1. SHA 演算 API 関数の使用に関する注意事項

### 1.1 該当製品

RX ファミリ SHA コプロセッサドライバモジュール Firmware Integration Technology

(RX SHA コプロセッサ FIT モジュール)

該当するリビジョンおよびドキュメントは、以下のとおりです。

表 1 RX SHA コプロセッサ FIT モジュール該当製品一覧

| RX SHA コプロセッサ FIT モジュールのリビジョン | 資料番号 |
|---|---|
| Rev.1.00 | R20AN0354JJ0100 |
| Rev.1.01 | R20AN0354JJ0101 |

### 1.2 該当デバイス

RX64M、および RX71M グループ

## 1.3 内容および発生条件

R_Sha1HashDigest()、R_Sha224HashDigest()、R_Sha256HashDigest()において、以下の条件をすべて満たしている場合、API 関数の実行が終了しません。

(a) 制御フラグ R_SHA_FINISH を設定している

(b) メッセージデータバイト長の合計が 64 で割って 4 余るデータ長(4,68,132…) である

[発生例 1] 以下の API 関数が終了しません。

```
ret = R_Sha1HashDigest
      (message, hash, 68, R_SHA_INIT | R_SHA_FINISH, work);
```

[発生例 2] 2 回目の API 関数はメッセージデータバイト長の合計が 68 かつ R_SHA_FINISH を指定しているため終了しません。

```
ret = R_Sha1HashDigest
      (message, hash, 4, R_SHA_INIT, work);
ret = R_Sha1HashDigest
      (message, hash, 64, R_SHA_ADD | R_SHA_FINISH, work);
```

## 1.4 回避策と恒久対策

Rev.1.02 で改修済みです。Rev.1.02 をご使用ください。

以上

## 改訂記録

| Rev. | 発行日 | 改訂内容 | |
|---|---|---|---|
| | | ページ | ポイント |
| 1.00 | Nov.01.20 | - | 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ものですが、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。



TS Colophon 4.1