発行日：2020年6月16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*-A0004A/J	Rev.	第1版
題名	SCE5 に関するユーザーズマニュアルの修正		情報分類	技術情報	
適用製品	RA4M1 グループ	対象ロット等	関連資料	Renesas RA4M1 グループ ユーザーズマニュアル ハードウェア編 Rev1.00	
		すべて			

SCE5 は、ユーザーモードと特権モードで使用可能なので、以下の記述を削除します。

・表 46.1 SCE5 の仕様、特権モード：特権モード信号はアクセス管理回路に接続されており、特権モードでのみ SCE5 を制御できるようにするのに使用

・図 46.1 SCE5 ブロック図、特権モード信号

表 46.1 SCE5の仕様

項目	内容
アクセス制御	アクセス管理回路 • 不正プログラムやプログラム実行の暴走によりSCE5に異常なアクセスがあった場合、この回路は後続のすべてのアクセスを遮断し、SCE5からのデータ出力を停止します。
暗号エンジン	Advanced Encryption Standard（AES）：NIST FIPS PUB 197 アルゴリズムに準拠 • キーサイズ：128、256ビットのいずれか • ブロックサイズ：128ビット • 連鎖モード - ECB、CBC、CTR：NIST SP 800-38Aに準拠 - GCM：NIST SP 800-38Dに準拠 - XTS：NIST SP 800-38Eに準拠 - GCTR • 128ビットデータに対するスループット - 128ビット鍵に対して44 PCLKAサイクル - 256ビット鍵に対して61 PCLKAサイクル AES-GCM • AES-GCMはAES-GCTRとGHASHを組み合わせることにより実現 キー管理 • ラップされた鍵はSCE5でのみ有効
乱数の生成	32ビット真正乱数発生器
ユニークID	• MCU固有のID（ユニークID）では、アクセス管理回路から専用バスまでアクセスが可能 • ユニークIDと鍵生成情報を組み合わせることにより、他のMCUへの不正なデータコピーを防止
~~特権モード~~	~~• 特権モード信号はアクセス管理回路に接続されており、特権モードでのみSCE5を制御できるようにするのに使用~~
低消費電力	モジュールストップ状態の設定が可能

(c) 2020. Renesas Electronics Corporation. All rights reserved.

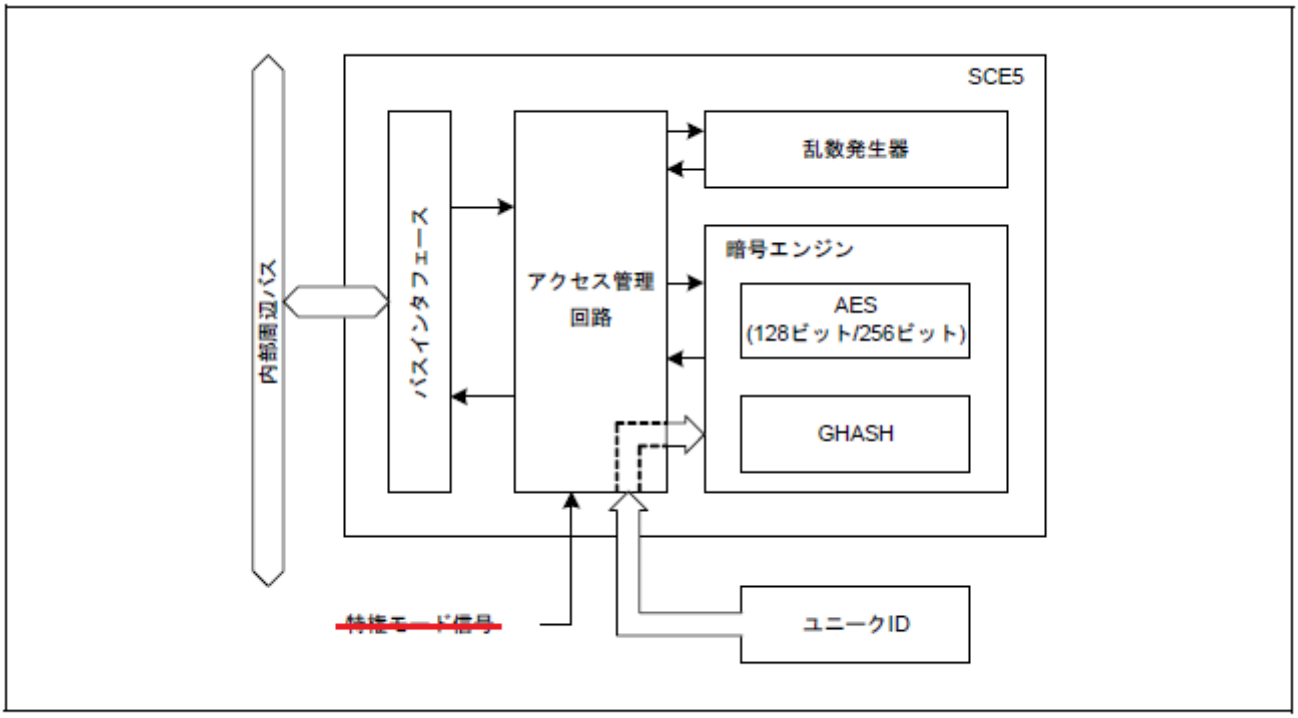

図 46.1　SCE5 ブロック図