Renesas Synergy™

SCE 機能を使用した Secure な外部 Storage 使用例

R30AN0318JJ0100
Rev.1. 00
2017.11.30

要旨

Synergy MCU アプリケーションは、使用するデータを MCU 内外のメモリに置きます。MCU 内部のメモリは、ID Code Protection 等の機能で外部からの不正アクセスを防ぐことが可能です。一方、外部メモリはこのような機能がない場合もあります。この際、重要なデータは秘匿のために暗号化が必要です。そこで、本アプリケーションノートはデータを SD カード上で暗号化された状態で扱う事例を紹介します。

本書に付属のサンプルプログラムは、表 1 の環境で動作します。また、表 2 に示す SSP モジュールを使用しており、これらの使用例としてもご参照頂けます。

表 1: 動作環境

使用プロジェクト	開発環境	SSP	評価ボード
Secure_Storage_Sample_DK-S7G2.zip	e²studio v5.4.0	v1.3.0	DK-S7G2 v3.0
Secure_Storage_Sample_DK-S7G2.zip	EW for Synergy v7.71.3 + SSC v5.4.0	v1.3.0	DK-S7G2 v3.0

表 2：使用する主な SSP モジュール

モジュール種別	モジュール名
X-ware	ThreadX®
	FileX®
	USBX™
Framework	sf_el_fx
	sf_block_media_sdmmc
	sf_el_ux_dcd_fs
HAL Driver	r_sdmmc
	r_dmac
	r_sce_aes
	r_sce

目次

1. はじめに

1.1 概要

Renesas Synergy™プラットフォームは、組込みシステム開発の複雑化、コスト増加、開発期間の長期化といった問題を解決するために提案された新しいプラットフォームです。その中で、Renesas Synergy™ Software Package（以下、SSP）は、RTOS、HAL ドライバ、ソフトウエアフレームワークを動作保証(warranty)した形で提供されるため、開発者はアプリケーション開発に集中することができます。本アプリケーションノートは、アプリケーションでデータをセキュアに扱う事例を紹介します。

一般に、アプリケーションは使用するデータを MCU 内外のメモリに置きます。MCU 内部のメモリは、ID Code Protection 等の機能で外部からの不正アクセスを防ぐことが可能です。一方、外部メモリはこのような機能がない場合もあります。この際、重要なデータは秘匿のために暗号化が必要です。そこで、本アプリケーションノートのサンプルアプリケーションは SD カード上のデータを暗号化します。暗号化処理はソフトウエアフレームワークのレイヤで実施され、アプリケーションレイヤで使用する API(FILEX の API)に影響ありません。

1.2 参考文献

[1] Renesas, “Renesas Synergy™ Development Kit DK-S7G2 User's Manual (R12UM0002EUxxxx)”.

[2] Renesas, “S7G2 User's Manual: Microcontrollers (R01UM0001EUxxxx)”.

[3] Renesas, “Renesas Synergy™ Renesas Synergy Software Package User's Manual (R01US0315EUxxxx)”.

[4] Renesas, “Synergy Project Import Guide (R11AN0023EUxxxx)”

[5] Renesas, “SCE HAL Module Guide (R11AN0088EUxxxx)”

[6] Renesas, “FileX Port Block Media Framework Module Guide (R11AN0147EUxxxx)”

2. ハードウエア

2.1 評価に必要なハードウエア

本書に付属のサンプルアプリケーション実行に必要なハードウエア構成を表 3 に示します。各構成の接続箇所は、図 1 を参照してください。

表 3: ハードウエア構成

デバイス	製品名	DK-S7G2 接続箇所	用途
メインボード	DK-S7G2M v3.0	-	-
拡張ボード	DK-S7G2B v3.0	-	-
AC アダプタ	-	J1	DK-S7G2 への電源供給
USB ケーブル	-	J2	アプリケーションの操作(データ書き込み/読出し)
USB ケーブル		J17	DK-S7G2 への SW 書き込み/デバッグ
SD カード	-	SD カードスロット (SD100)	データの格納
Windows PC (Windows10)	-	USB ケーブル経由	DK-S7G2 への SW 書き込み/デバッグ アプリケーションの操作(データ書き込み/読出し)

2.2 評価ボードの設定

本書に付属のサンプルアプリケーション実行時の DK-S7G2 メインボードのディップスイッチ S5 の設定を表 4、拡張ボードのディップスイッチ S101 の設定を表 5 に示します。

表 4: DK-S7G2M スイッチ S5 設定

番号	名称	設定*1
S5-1	DRAM	OFF
S5-2	QSPI	OFF
S5-3	ENET1	OFF
S5-4	PMOD	OFF
S5-5	PBs	ON
S5-6	JTAG	**ON**
S5-7	EXP	OFF
S5-8	BOOT	**OFF**

*1 : グレー表示は任意

表 5: DK-S7G2B スイッチ S101 設定

番号	名称	設定*1
S101-1	RS	OFF
S101-2	CAN	OFF
S101-3	ENET0	**OFF**
S101-4	SD	**ON**
S101-5	MMC	**OFF**
S101-6	PMODB	OFF
S101-7	BLE	OFF
S101-8	CAM	OFF

*1 : グレー表示は任意

2.3 評価ボードの使用機能

本書に付属のサンプルアプリケーションが使用するボード上の主な機能を表 6 に示します。また、各機能のボード上の配置を図 1 に示します。

表 6: 使用機能

名称	用途
J1	ボードへの電源供給
J2	Windows PC からのアプリケーション操作
J17	Windows PC からのデバッグアクセス
SD100(SD カードスロット)	bitmap ファイルが格納された SD カードの挿入個所

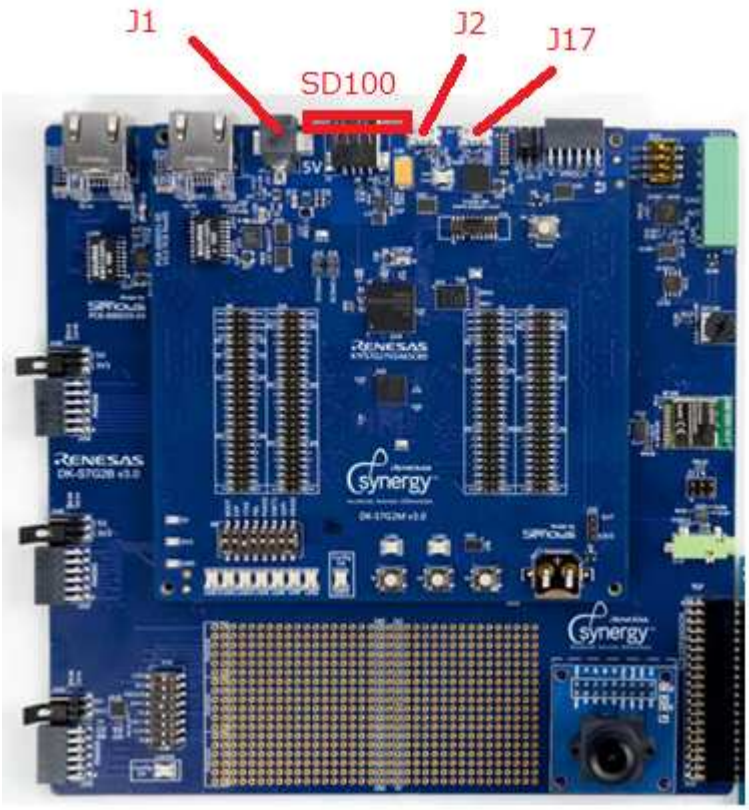

図 1： 機能の配置

3. ソフトウエア

3.1 ソフトウエアのインストール

-付属の”Synergy Project Import Guide” に従い Secure_Storage_Sample_DK-S7G2.zip を e2studio または EWSYN に Import してください。

-Windows10 PC に TeraTerm(https://ttssh2.osdn.jp/)等のターミナルソフトウエアをインストールしてください。

-

3.2 ソフトウエア構成

3.2.1 使用 SSP モジュール

本書に付属のサンプルアプリケーションで使用する主な SSP モジュールを表 7 に示します。

表 7: 主な SSP モジュール

モジュール種別	モジュール名	用途
X-ware	ThreadX®	OS
	FileX®	SD カード内のファイルへのアクセス
	USBX™	Windows PC のと通信
Framework	sf_el_fx	FileX の下位モジュール
	sf_block_media_sdmmc	SD カードへのアクセス
	sf_el_ux_dcd_fs	USBX の下位モジュール
HAL Driver	r_sdmmc	sf_block_media_sdmmc の下位モジュール
	r_dmac	r_sdmmc の下位モジュール
	r_sce_aes	AES 暗号
	r_sce	r_sce_aes の下位モジュール

3.2.2 アプリケーション構成

本書に付属のサンプルアプリケーションの機能構成を図２、それぞれの機能の詳細を表 8 に示します。

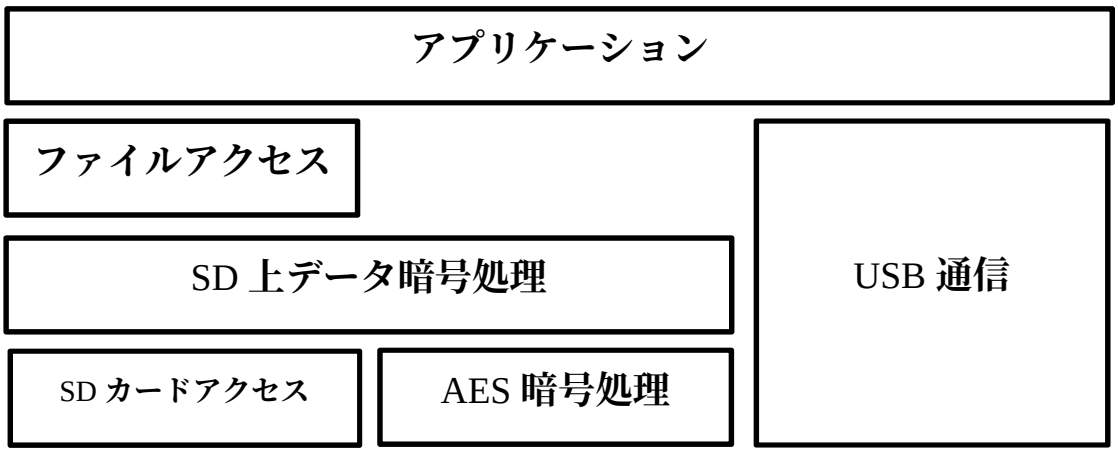

図２:サンプルアプリケーションの機能構成

表 8:サンプルアプリケーションに含まれる機能詳細

機能	説明	含まれる SSP モジュール
アプリケーション	・USB 経由で受信したテキストをファイルとして保存 ・ファイルに含まれるテキストを USB 経由で送信	なし
ファイルアクセス	・上位アプリケーションにファイルアクセス機能を提供 ・FAT ファイルシステムを管理し、必要に応じてクラスター単位で SD カード read/write を実施	FileX® sf_el_fx
SD 上データ暗号処理	・SD カード read/write の際、データを AES 暗号処理で復号/暗号化	なし
SD カードアクセス	・上位モジュールにクラスター単位の SD カード read/write 機能を提供	sf_block_media_sdmmc r_sdmmc r_dmac
AES 暗号処理	・データを AES 暗号化/復号	r_sce_aes r_sce
USB 通信	・上位アプリケーションに USB 経由のデータ送受信機能を提供	USBX™ sf_el_ux_dcd_fs

3.2.3 ファイル構成

本書に付属のサンプルアプリケーションの主要なファイル/ディレクトリを表 9 に示します。

表 9:プロジェクトで使用する主要なファイル/ディレクトリ

ファイル/ディレクトリ名	説明
synergy	表 7 に示す SSP モジュールのソースコード/ライブラリを格納するディレクトリ。Synergy Configurator で選択されたモジュールのコードが自動で格納される。
src¥synergy_gen	SSP モジュールの主な設定/初期化コードを格納するディレクトリ。Synergy Configurator の設定が自動で反映される。本ディレクトリ下の common_data.c は未使用。代わりに、src¥common_data.c を使用。
src¥common_data.c	src¥synergy_gen¥common_data.c をコピーした上で、表 8 の「ファイルアクセス」機能が「SD 上データ暗号処理」機能を参照するように修正したコード。該参照は Synergy Configurator で設定できず、上書きを防ぐためにコピーした上でコードを直接修正している。
src¥main_thread_entry.c	表 8 の「アプリケーション」機能を提供するサンプルコード
src¥secure_sd.c	表 8 の「SD 上データ暗号処理」機能を提供するサンプルコード

3.2.4 スレッド構成

本書に付属のサンプルアプリケーションのユーザスレッド一覧を表 10 に示します。

表 10: スレッド構成

エントリ関数	機能
main_thread_entry()	・本アプリケーション唯一のユーザスレッド

4. サンプルアプリケーション

4.1 サンプルアプリケーションの特徴

- SD カード上の FAT ファイルシステム全体を暗号化します。
- 暗号アルゴリズム：AES / 暗号モード：CBC/ 鍵長：128bit
- アプリケーションとファイルアクセス機能との間のインターフェイス(FILEX の API)は暗号処理有無に関わらず共通です。言い換えればアプリケーションと暗号処理は相互に独立しています。

4.2 評価手順

1. 本サンプルアプリケーションを e2studio でビルドし・DK-S7G2 ボードにアップロードします。
2. USB ケーブルで J2 端子と Windows10 PC を接続します。
3. DK-S7G2 ボードを起動します。
4. PC のデバイス マネージャーで、DK-S7G2 ボードが COM ポートとして認識されるのを待ちます。
5. PC 上でターミナルソフトウエアを起動し、DK-S7G2 の COM ポートに接続します。
6. ターミナルソフトウエアの改行コード設定で、送信時の改行コードを「CR+LF」にします。
7. SD カードスロット(SD100)に SD カードを挿入します。
8. ターミナルソフトウエア上で「It seems unformatted. So try to format SD card.」と表示され、SD カードのフォーマットを実行するので、暫く待ちます。(本アプリケーションは暗号化された FAT ファイルシステムで動作します。このため、暗号化されていない SD カードは未フォーマットとして扱われます。)
9. ターミナルソフトウエア上で「please enter text you want to add to log.txt」と表示されたら、任意の文字列を入力する。
10. ボードの電源を一旦落とし、SD カードを抜いてから 3~7 の操作を再度実施する。
11. ターミナルソフトウエア上に、先に入力した文字列が表示されます。(SD カードに保存されていることの確認)
12. SD カードを抜いて、PC に挿入します。PC 上で SD カードはファイルシステムとして認識されません。（SD カードが暗号化されていることの確認）

4.3 考察

- 鍵長を 192bit/256bit にするとより安全性は高まりますが、SD カードへのアクセス速度は低下します。
- 暗号モード ECB の使用は非推奨です。理由は、同じ内容のクラスターであれば同じ暗号化結果となるため、未使用クラスター等を容易に推測でき、安全性が低くなるためです。
- XTS/GCM 等の認証機能を持った暗号機能を使用すると、データの秘匿だけでなく改竄検出も可能です。この場合、改竄検出のための認証タグも SD カードに保存する必要があるので、SD カードの実効サイズは小さくなります。
- 本アプリケーションは、鍵をソースコード上の即値で扱います。すなわち、鍵は MCU 内部フラッシュに秘匿せずに保管されます。従って、内部フラッシュにアクセス可能であれば鍵を取得して SD カードにもアクセス可能です。このため、SD カード内のデータの安全性は、原則として MCU 内部フラッシュ内のデータの安全性を超えることはありません。Synergy MCU 搭載の HRK(Hidden Root Key)機能を使用して鍵を秘匿して取り扱う場合、この欠点は解消されます。HRK 機能は、今後の SSP でサポートを拡大する予定です。

ホームページとサポート窓口
ルネサス エレクトロニクスホームページ
http://japan.renesas.com/

お問合せ先
http://japan.renesas.com/contact/

改訂記録

Rev.	発行日	改訂内容	
		ページ	ポイント
1.00	2017-11-30	-	初版

製品ご使用上の注意事項

ここでは、マイコン製品全体に適用する「使用上の注意事項」について説明します。個別の使用上の注意事項については、本ドキュメントおよびテクニカルアップデートを参照してください。

1. 未使用端子の処理
   【注意】未使用端子は、本文の「未使用端子の処理」に従って処理してください。
   CMOS製品の入力端子のインピーダンスは、一般に、ハイインピーダンスとなっています。未使用端子を開放状態で動作させると、誘導現象により、LSI周辺のノイズが印加され、LSI内部で貫通電流が流れたり、入力信号と認識されて誤動作を起こす恐れがあります。未使用端子は、本文「未使用端子の処理」で説明する指示に従い処理してください。
2. 電源投入時の処置
   【注意】電源投入時は，製品の状態は不定です。
   電源投入時には、LSIの内部回路の状態は不確定であり、レジスタの設定や各端子の状態は不定です。
   外部リセット端子でリセットする製品の場合、電源投入からリセットが有効になるまでの期間、端子の状態は保証できません。
   同様に、内蔵パワーオンリセット機能を使用してリセットする製品の場合、電源投入からリセットのかかる一定電圧に達するまでの期間、端子の状態は保証できません。
3. リザーブアドレス（予約領域）のアクセス禁止
   【注意】リザーブアドレス（予約領域）のアクセスを禁止します。
   アドレス領域には、将来の機能拡張用に割り付けられているリザーブアドレス（予約領域）があります。これらのアドレスをアクセスしたときの動作については、保証できませんので、アクセスしないようにしてください。
4. クロックについて
   【注意】リセット時は、クロックが安定した後、リセットを解除してください。
   プログラム実行中のクロック切り替え時は、切り替え先クロックが安定した後に切り替えてください。
   リセット時、外部発振子（または外部発振回路）を用いたクロックで動作を開始するシステムでは、クロックが十分安定した後、リセットを解除してください。また、プログラムの途中で外部発振子
   （または外部発振回路）を用いたクロックに切り替える場合は、切り替え先のクロックが十分安定してから切り替えてください。
5. 製品間の相違について
   【注意】型名の異なる製品に変更する場合は、製品型名ごとにシステム評価試験を実施してください。
   同じグループのマイコンでも型名が違うと、内部ROM、レイアウトパターンの相違などにより、電気的特性の範囲で、特性値、動作マージン、ノイズ耐量、ノイズ輻射量などが異なる場合があります。型名が違う製品に変更する場合は、個々の製品ごとにシステム評価試験を実施してください。

ご注意書き

1. 本資料に記載された回路、ソフトウェアおよびこれらに関連する情報は、半導体製品の動作例、応用例を説明するものです。お客様の機器・システムの設計において、回路、ソフトウェアおよびこれらに関連する情報を使用する場合には、お客様の責任において行ってください。これらの使用に起因して、お客様または第三者に生じた損害に関し、当社は、一切その責任を負いません。
2. 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。
3. 本資料に記載された製品データ、図、表、プログラム、アルゴリズム、応用回路例等の情報の使用に起因して発生した第三者の特許権、著作権その他の知的財産権に対する侵害に関し、当社は、何らの責任を負うものではありません。当社は、本資料に基づき当社または第三者の特許権、著作権その他の知的財産権を何ら許諾するものではありません。
4. 当社製品を改造、改変、複製等しないでください。かかる改造、改変、複製等により生じた損害に関し、当社は、一切その責任を負いません。
5. 当社は、当社製品の品質水準を「標準水準」および「高品質水準」に分類しており、
   各品質水準は、以下に示す用途に製品が使用されることを意図しております。
   標準水準： コンピュータ、OA機器、通信機器、計測機器、AV機器、
   家電、工作機械、パーソナル機器、産業用ロボット等
   高品質水準：輸送機器（自動車、電車、船舶等）、交通用信号機器、
   防災・防犯装置、各種安全装置等
   当社製品は、直接生命・身体に危害を及ぼす可能性のある機器・システム（生命維持装置、人体に埋め込み使用するもの等）、もしくは多大な物的損害を発生させるおそれのある機器・システム（原子力制御システム、軍事機器等）に使用されることを意図しておらず、使用することはできません。たとえ、意図しない用途に当社製品を使用したことによりお客様または第三者に損害が生じても、当社は一切その責任を負いません。なお、ご不明点がある場合は、当社営業にお問い合わせください。
6. 当社製品をご使用の際は、当社が指定する最大定格、動作電源電圧範囲、放熱特性、実装条件その他の保証範囲内でご使用ください。当社保証範囲を超えて当社製品をご使用された場合の故障および事故につきましては、当社は、一切その責任を負いません。
7. 当社は、当社製品の品質および信頼性の向上に努めていますが、半導体製品はある確率で故障が発生したり、使用条件によっては誤動作したりする場合があります。また、当社製品は耐放射線設計については行っておりません。当社製品の故障または誤動作が生じた場合も、人身事故、火災事故、社会的損害等を生じさせないよう、お客様の責任において、冗長設計、延焼対策設計、誤動作防止設計等の安全設計およびエージング処理等、お客様の機器・システムとしての出荷保証を行ってください。特に、マイコンソフトウェアは、単独での検証は困難なため、お客様の機器・システムとしての安全検証をお客様の責任で行ってください。
8. 当社製品の環境適合性等の詳細につきましては、製品個別に必ず当社営業窓口までお問合せください。ご使用に際しては、特定の物質の含有・使用を規制するRoHS指令等、適用される環境関連法令を十分調査のうえ、かかる法令に適合するようご使用ください。お客様がかかる法令を遵守しないことにより生じた損害に関して、当社は、一切その責任を負いません。
9. 本資料に記載されている当社製品および技術を国内外の法令および規則により製造・使用・販売を禁止されている機器・システムに使用することはできません。また、当社製品および技術を大量破壊兵器の開発等の目的、軍事利用の目的その他軍事用途に使用しないでください。当社製品または技術を輸出する場合は、「外国為替及び外国貿易法」その他輸出関連法令を遵守し、かかる法令の定めるところにより必要な手続を行ってください。
10. お客様の転売等により、本ご注意書き記載の諸条件に抵触して当社製品が使用され、その使用から損害が生じた場合、当社は何らの責任も負わず、お客様にてご負担して頂きますのでご了承ください。
11. 本資料の全部または一部を当社の文書による事前の承諾を得ることなく転載または複製することを禁じます。

注1. 本資料において使用されている「当社」とは、ルネサス エレクトロニクス株式会社およびルネサス エレクトロニクス株式会社がその総株主の議決権の過半数を直接または間接に保有する会社をいいます。
注2. 本資料において使用されている「当社製品」とは、注１において定義された当社の開発、製造製品をいいます。

ルネサス エレクトロニクス株式会社

■営業お問合せ窓口

http://www.renesas.com

※営業お問合せ窓口の住所は変更になることがあります。最新情報につきましては、弊社ホームページをご覧ください。

ルネサス エレクトロニクス株式会社　〒135-0061　東京都江東区豊洲3-2-24（豊洲フォレシア）

■技術的なお問合せおよび資料のご請求は下記へどうぞ。
総合お問合せ窓口：http://japan.renesas.com/contact/