RX ファミリ

暗号機能搭載 MCU　セキュリティガイド

要旨

本資料は、暗号機能を搭載した RX ファミリ MCU をセキュリティ的に安全にご使用いただくためのガイダンス文書です。

対象製品

Trusted Secure IP/Trusted Secure IP Lite 搭載製品：RX671 グループ

Trusted Secure IP/Trusted Secure IP Lite 非搭載製品：RX140 グループ

目次

1. イントロダクション 2

2. 一般的セキュリティ要件 3
2.1 機密技術情報および開発ツールの保護 3
2.2 廃棄物処理 3

3. プログラミングおよび使用ガイダンス 4
3.1 内蔵ソフトウェアの開発に関する一般的要件 4
3.2 チップ内蔵メモリの使用 5
3.2.1 フラッシュメモリの使用 5
3.2.2 トランスポートキー 5
3.2.3 RAM の使用 5
3.3 暗号 6
3.4 データ伝送 6
3.5 乱数 6
3.5.1 TRNG の使用 6
3.5.1.1 TRNG ハードウェアのチェック 6

4. 最後に 7

改訂記録 8

1. イントロダクション

暗号機能を搭載した RX ファミリ MCU をセキュリティ的に安全にご使用いただくために、このセキュリティガイドをご用意いたしました。

ルネサスでは、セキュリティ機能の実装に加え、設計工程において特別なセキュリティ管理を行っています。その一環として、お客様にも本文書で説明する環境的セキュリティ要件を満たしていただくことを推奨しています。本ガイドは、特に断り書きのない限りすべての対象製品に適用されます。

本文書は、MCU のセキュリティ情報の保護およびセキュリティを意識したソフトウェアを開発するためのガイダンス文書です。このガイダンス文書は、一般的なセキュリティプログラミング手法、MCU 動作に関する知識や、評価機関を含めた脆弱性分析に基づいています。これらは、ガイドであり必須要求ではありません。これらのガイドの適用が使用用途に適切であるかどうか、そのガイドにある実装方法のどれが（または別の方法が）使用用途に要求されるかの判断は、お客様（または評価機関）の評価に委ねられています。

本 MCU をより効果的にご使用頂くためのガイダンスを記載していますが、アプリケーションやそれに関わる要件は様々であるため、ある対策が特定の用途に適している、あるいは十分であるという保証は致しかねますのでご了承ください。通常、完成品としてこの点を確認するために、ハードウェアと内蔵ソフトウェアを組み合わせた製品で最終的な評価を行う必要があります。

本文書は、ルネサスとの契約の一部をなすものではありません。矛盾がある場合には、関連する納入仕様書（該当する場合）や、ユーザーズマニュアル　ハードウェア編の現行版に記載されている仕様や性能が適用されます。

2.　一般的セキュリティ要件

MCU 内の情報保護のため、最終製品が通常使用される環境ではない状況に置かれた場合に、MCU 内の情報に対して、どのような脅威が存在するかを検討されることを推奨します。

2.1　機密技術情報および開発ツールの保護

本 MCU をベースにしたアプリケーション開発のために、通常、ユーザーズマニュアル　ハードウェア編、アプリケーションノートやサンプルソフトウェアなど種々のツールや情報を提供しています。これらは、機密保持契約に基づき提供される場合があり、機密保持契約の内容は厳守されなければなりません。これらの情報やツールが不正に開示された場合、本 MCU に実装されているセキュリティ機能の効果が軽減されてしまう可能性があります。

同様に、コードフラッシュメモリおよびデータフラッシュメモリの情報の機密性および完全性を、ライフサイクルにわたって保持することがお客様の製品の要件である場合には、それらの要件を満たす必要があります。データの生成、配布、管理や廃棄もこれに含まれます。

暗号ソフトウェア用の鍵は、そのライフサイクルにわたって安全な方法で生成し、保存、使用してください。

2.2　廃棄物処理

MCU やアプリケーションへのアタック方法を検討するために廃棄品が利用されることがないよう、全ての廃棄品を安全な方法で廃棄することが重要です。MCU のメモリにセキュリティ上重要な情報が保存されている場合は、廃棄前にその情報を消去することを推奨します。また、廃棄手段の一つとして、粉砕機を用いて小さな破片になるまで MCU を非常に細かく砕くという方法もあります。

3.　プログラミングおよび使用ガイダンス

MCU のセキュリティについての要件は、多くの場合、内蔵ソフトウェアとハードウェア機能の相互作用に関わっています。本章では、本 MCU において推奨される事項を取り上げます。

3.1　内蔵ソフトウェアの開発に関する一般的要件

暗号機能を利用したソフトウェアの開発では、ユーザーズマニュアル　ハードウェア編に記載されている使用方法の準拠と、本文書のガイダンス内容の考慮が必要です。

暗号機能を利用した暗号処理では、ソフトウェアが実行される際に暗号鍵が損なわれる危険性を最小限に抑えられるように、鍵取扱いルーチンを実装し、運用してください。

例えば、以下にあげるような方法があります。

- 鍵（および鍵ペア）の完全性を確保すること
- 鍵が固有であり、暗号的にも強いものであると、十分な信頼性をもって保証できること
- 非対称アルゴリズムの場合、実質上、公開鍵から秘密鍵を引き出せないこと
- 外部から鍵をインポートする場合、その鍵がアプリケーションの要求に十分見合う品質と機密性を保持できるようなシステムであること

TSIP または TSIP-Lite 搭載製品の場合、鍵の管理に関しては、ルネサスの専用 Web ページにてお客様の鍵を安全に暗号化する Key Wrap サービスをご提供しておりますので、TSIP ドライバでご用意している鍵生成情報生成 API と併せてご利用ください。ご要望の際は、弊社営業窓口にお問い合わせください。

3.2　チップ内蔵メモリの使用

本 MCU は、コードフラッシュメモリ、データフラッシュメモリおよび RAM の 3 種類のメモリを搭載しています。セキュリティや用途はメモリごとに異なります。以下のガイダンスは、各種メモリのセキュリティを最大限に高めるためのものです。

重要なデータをメモリから読み出す、または書き込む際には、本項以外で提示されている要件についても考慮が必要です。

3.2.1　フラッシュメモリの使用

本 MCU は、ユーザプログラムの保護機能を備えています。詳細はユーザーズマニュアル　ハードウェア編をご参照ください。

- コードフラッシュメモリ、スタートアッププログラム保護機能
  リセット後に起動するプログラム（スタートアッププログラム）を保護する機能です。本機能は、スタートアッププログラムの更新中に、リセットなどが発生したことによる書き換え動作の中断に対して、安全な更新方法を提供しています。また、エリアプロテクション機能の設定によるスタートアッププログラムの保護、オプション設定メモリの設定によるスタートアップ領域の選択状態の固定化をすることができます。これらの機能を利用して、安全性の高いスタートアッププログラムで本 MCU を起動することができます。
  このスタートアッププログラムにて、コードフラッシュメモリ内のデータを検証し、改竄されていないことを確認してから、お客様のプログラムを実行されることをお勧めします。TSIP または TSIP-Lite 搭載品では、TSIP ドライバにセキュアブート API をご用意していますので、ご利用ください。

- オンチップデバッガ、シリアルプログラマ接続保護機能
  オプション設定メモリの設定により、オンチップデバッガの接続許可/禁止、およびコードフラッシュメモリ、データフラッシュメモリに対するシリアルプログラマの接続許可/禁止を制御できます。機密データの漏洩防止のため、お客様の製品出荷時にはオンチップデバッガとシリアルプログラマの両方を接続禁止に設定することをお勧めします。

- パラレルプログラマ接続保護機能
  ROM コードプロテクトレジスタの ROM コードビット設定による、パラレルプログラマ接続時のコードフラッシュメモリのリード、プログラム、イレーズアクセス制御を行う機能です。機密データの漏洩防止および意図しない書き換え防止のため、お客様の製品出荷時には保護機能の設定を行うことをお勧めします。

3.2.2　トランスポートキー

お客様の製品が不正に使用される危険性を軽減するため、内蔵ソフトウェアになんらかのトランスポートキーを実装することをお勧めします。これにより、本 MCU へのアクセスに秘密データ（パスワードなど）を要求するよう設定でき、最終利用者へ送られるまでの間、本 MCU へのアクセスが制限できます。

オール"1"やオール”0”の値をトランスポートキーとして用いるのは避けてください。"1"と"0"を組み合わせれば、偶発的あるいは意図的にコードが変造された場合の危険性を大幅に軽減できます。

3.2.3　RAM の使用

セキュリティ処理が完了した後、不要になったデータが RAM に残らないようデータを消去することを推奨します。

3.3　暗号

暗号は、アプリケーションで用いられる主要なセキュリティシステムのひとつです。暗号技術により、MCU に格納されているデータを保護し、また外部デバイスやシステムとのデータ転送、認証、検証などのプロセスを保護します。

3.4　データ伝送

TSIP/TSIP-lite 非搭載製品では、可能な限り、重要なデータの設定および転送をする前に必ずユーザや外部デバイスの認証を行うなど、なんらかのデータ保護手段を講じることをお勧めします。また、認証システムにはセキュアカウンタを入れ、照合を試みる回数を制限することをお勧めします。

3.5　乱数

良質な乱数は、セキュリティ環境を向上させます。

TSIP/TSIP-lite 搭載製品の真性乱数生成回路（TRNG）は、正常な動作環境において、良質な乱数を生成するよう設計、検証されています。

TSIP/TSIP-lite 非搭載製品では、乱数生成器の出力をそのまま鍵情報には使用せず、conditioning 後にご使用ください。

3.5.1　TRNG の使用

TRNG は、様々な用途で重要な役割を果たしています。特に、鍵の生成など、TRNG の出力を重要な用途に用いる場合は、ここで示すガイダンスに必ず従ってください。それ以外の用途の場合は、乱数の使用目的やソフトウェアによる後処理などを考慮し、適切な検証方法を決定してください。

3.5.1.1　TRNG ハードウェアのチェック

TRNG で起こり得る故障を検証するため、TRNG の生成した乱数を使用する前に、TRNG が機能していることを内蔵ソフトウェアで必ず検証してください。

最も起こる可能性の高い故障メカニズムを検出するために、TRNG の出力について適切な統計テストを行うことをお勧めします。

4.　最後に

本ガイダンスは、本 MCU のセキュリティ機能を有効にご使用いただくための推奨事項を記載しています。内蔵ソフトウェアの機能が損なわれることがないように保護するための手段は、本書で言及したもの以外にも存在しますので、必要に応じて対策を行ってください。

お客様のシステム構築の際は、外部からの不正アクセスから情報システムを守るために、TSIP/TSIP-lite 搭載製品では TSIP ドライバを使用したセキュリティ機能をご利用ください。また、一般的に、お客様の使用環境に適した多層防御（ソフトウェアアップデート、データアクセス制限、ネットワークの分散等、複数のセキュリティ対策）の実施をご検討ください。

ルネサスでは、ルネサス PSIRT（ルネサス製品セキュリティインシデント対応チーム）の体制を構築しています。ルネサス製品に関して脆弱性が疑われる場合には、ルネサス PSIRT にご連絡ください。

ルネサス PSIRT　Web URL: https://www.renesas.com/psirt

さらに情報をご希望の場合は、弊社営業窓口までお問合せください。

改訂記録

Rev.	発行日	改訂内容	
		ページ	ポイント
1.00	2021.09.3	—	初版発行
1.01	2022.05.11	全項	RX140 に対応

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. 静電気対策
   CMOS 製品の取り扱いの際は静電気防止を心がけてください。CMOS 製品は強い静電気によってゲート絶縁破壊を生じることがあります。運搬や保存の際には、当社が出荷梱包に使用している導電性のトレーやマガジンケース、導電性の緩衝材、金属ケースなどを利用し、組み立て工程にはアースを施してください。プラスチック板上に放置したり、端子を触ったりしないでください。また、CMOS 製品を実装したボードについても同様の扱いをしてください。
2. 電源投入時の処置
   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. 電源オフ時における入力信号
   当該製品の電源がオフ状態のときに、入力信号や入出力プルアップ電源を入れないでください。入力信号や入出力プルアップ電源からの電流注入により、誤動作を引き起こしたり、異常電流が流れ内部素子を劣化させたりする場合があります。資料中に「電源オフ時における入力信号」についての記載のある製品は、その内容を守ってください。
4. 未使用端子の処理
   未使用端子は、「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。
5. クロックについて
   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。
6. 入力端子の印加波形
   入力ノイズや反射波による波形歪みは誤動作の原因になりますので注意してください。CMOS 製品の入力がノイズなどに起因して、V_{IL}（Max.）から V_{IH}（Min.）までの領域にとどまるような場合は、誤動作を引き起こす恐れがあります。入力レベルが固定の場合はもちろん、V_{IL}（Max.）から V_{IH}（Min.）までの領域を通過する遷移期間中にチャタリングノイズなどが入らないように使用してください。
7. リザーブアドレス（予約領域）のアクセス禁止
   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、将来の拡張機能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。
8. 製品間の相違について
   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、フラッシュメモリ、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、ノイズ幅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。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、お客様の責任において、お客様の機器・システムを設計ください。これらの使用に起因して生じた損害（お客様または第三者いずれに生じた損害も含みます。以下同じです。）に関し、当社は、一切その責任を負いません。
2. 当社製品または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またはこれらに関する紛争について、当社は、何らの保証を行うものではなく、また責任を負うものではありません。
3. 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. 当社製品を組み込んだ製品の輸出入、製造、販売、利用、配布その他の行為を行うにあたり、第三者保有の技術の利用に関するライセンスが必要となる場合、当該ライセンス取得の判断および取得はお客様の責任において行ってください。
5. 当社製品を、全部または一部を問わず、改造、改変、複製、リバースエンジニアリング、その他、不適切に使用しないでください。かかる改造、改変、複製、リバースエンジニアリング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。
6. 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）、交通制御（信号）、大規模通信機器、金融端末基幹システム、各種安全制御装置等

   当社製品は、データシート等により高信頼性、Harsh environment 向け製品と定義しているものを除き、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（宇宙機器と、海底中継器、原子力制御システム、航空機制御システム、プラント基幹システム、軍事機器等）に使用されることを意図しておらず、これらの用途に使用することは想定していません。たとえ、当社が想定していない用途に当社製品を使用したことにより損害が生じても、当社は一切その責任を負いません。
7. あらゆる半導体製品は、外部攻撃からの安全性を 100%保証されているわけではありません。当社ハードウェア／ソフトウェア製品にはセキュリティ対策が組み込まれているものもありますが、これによって、当社は、セキュリティ脆弱性または侵害（当社製品または当社製品が使用されているシステムに対する不正アクセス・不正使用を含みますが、これに限りません。）から生じる責任を負うものではありません。当社は、当社製品または当社製品が使用されたあらゆるシステムが、不正な改変、攻撃、ウイルス、干渉、ハッキング、データの破壊または窃盗その他の不正な侵入行為（「脆弱性問題」といいます。）によって影響を受けないことを保証しません。当社は、脆弱性問題に起因しまたはこれに関連して生じた損害について、一切責任を負いません。また、法令において認められる限りにおいて、本資料および当社ハードウェア／ソフトウェア製品について、商品性および特定目的との合致に関する保証ならびに第三者の権利を侵害しないことの保証を含め、明示または黙示のいかなる保証も行いません。
8. 当社製品をご使用の際は、最新の製品情報（データシート、ユーザーズマニュアル、アプリケーションノート、信頼性ハンドブックに記載の「半導体デバイスの使用上の一般的な注意事項」等）をご確認の上、当社が指定する最大定格、動作電源電圧範囲、放熱特性、実装条件その他指定条件の範囲内でご使用ください。指定条件の範囲を超えて当社製品をご使用された場合の故障、誤動作の不具合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。
9. 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、データシート等において高信頼性、Harsh environment 向け製品と定義しているものを除き、耐放射線設計を行っておりません。仮に当社製品の故障または誤動作が生じた場合であっても、人身事故、火災事故その他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。
10. 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。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。
11. 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。当社製品および技術を輸出、販売または移転等する場合は、「外国為替及び外国貿易法」その他日本国および適用される外国の輸出管理関連法規を遵守し、それらの定めるところに従い必要な手続きを行ってください。
12. お客様が当社製品を第三者に転売等される場合には、事前に当該第三者に対して、本ご注意書き記載の諸条件を通知する責任を負うものといたします。
13. 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。
14. 本資料に記載されている内容または当社製品についてご不明な点がございましたら、当社の営業担当者までお問合せください。

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直接的、間接的に支配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。

(Rev.5.0-1　2020.10)

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。