RL78/G23

サードパーティプログラム保護

要旨

本アプリケーションノートは、RL78/G23 のサードパーティプログラム保護について説明します。

ここでのサードパーティプログラムとは、ライブラリなどの形式で提供される、価値のあるソフトウェア IP を示しています。RL78/G23 の有するセキュリティ機能を用いて、そのソフトウェア IP の不正利用を抑止することが可能です。

サードパーティプログラム保護は、RL78/G23 の以下の機能を用います。

- メモリ保護機能（フラッシュ・リード・プロテクション）
- ユニーク ID
- カスタマ ID

目次

1. 概要

1.1 本アプリケーションノートについて

本アプリケーションノートでは、RL78/G23 の機能を用いて実現できるサードパーティプログラム（ソフトウェア IP）保護について説明します。

1.2 サードパーティプログラム（ソフトウェア IP）保護が求められる背景

ソフトウェア IP は以下のような問題を抱えています。

- ソフトウェア IP がバイナリ提供であっても、提供した先で複製利用される。
- ソフトウェア IP をマイコンに搭載した最終製品であっても、フラッシュから読み出して解析される。

1.3 考えられる対策

RL78/G23 で これらの問題からソフトウェア IP を保護するため、考えられる対策の例を示します。

- メモリ保護
  フラッシュ上のソフトウェア IP プログラムコードを読み出し不可にする方法
  メモリ保護機能を用いてコード・フラッシュの特定領域を読み出し禁止にすることが可能です。ソフトウェア IP を読み出し禁止に設定した MCU を提供することで、より強力に IP を保護します。

  ⇒「2.1 メモリ保護(フラッシュ・リード・プロテクション)」を参照

- 起動制御
  ソフトウェア IP 起動時に、フラッシュに書き込まれた ID をチェックする方法
  ソフトウェア IP 開発元がバイナリを提供する場合に適切な方法です。

  ⇒「2.2 起動制御（ユニーク ID 連携）」を参照
  ⇒「2.3 起動制御（カスタマ ID 連携）」を参照

目的	制御方法	使用する機能
ソフトウェア IP 保護	メモリ保護	フラッシュ・リード・プロテクション
	起動制御	ユニーク ID
		カスタマ ID

2. RL78/G23 のセキュリティ機能

RL78/G23 は、以下のセキュリティ機能を有しています。これらの機能を単体や組み合わせて利用することで、ソフトウェア IP を不正利用から保護することが可能です。

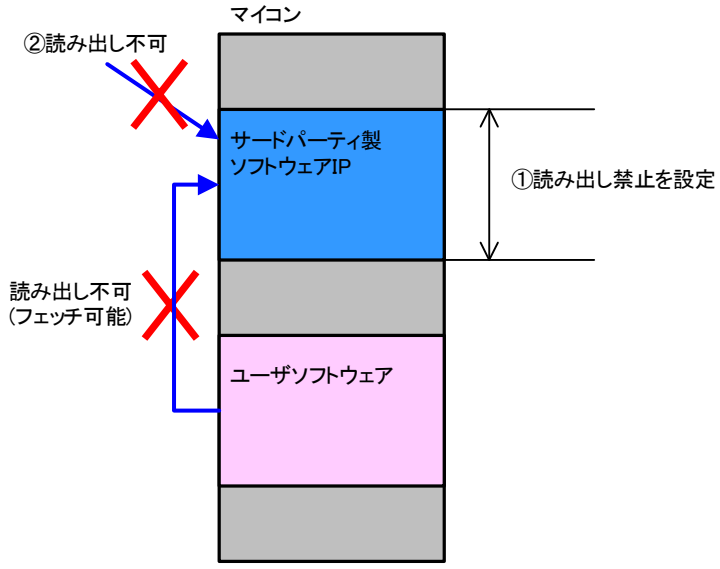
メモリ保護機能（フラッシュ・リード・プロテクション）

ユニーク ID

カスタマ ID

2.1 メモリ保護(フラッシュ・リード・プロテクション)

フラッシュ・リード・プロテクションは、コード・フラッシュの指定した領域に対し CPU、DTC、SMS からの読み出しを不可にする機能です。この機能を用い、コード・フラッシュ上のソフトウェア IP を読み出し禁止に設定します。読み出し禁止に設定した領域は、CPU による命令フェッチのみ可能です。ただし、読み出し禁止領域で実行するプログラムでも禁止領域のデータの読み出しはできません。読み出し禁止領域で実行するプログラムで使用するデータはプロテクトされていない領域に配置してください。



① ソフトウェア IP が格納されるブロックを読み出し禁止の領域に指定する

② ソフトウェア IP の実行はできるが、ユーザソフトウエアからソフトウェア IP のプログラムコードの読み出し不可

外部からフラッシュライタ等での読み出しも不可

特徴 : 読み出し禁止に設定したソフトウェア IP に対し、解析やコピー自体を強力に防止できるソフトウェア IP 提供先での不正使用や流用を抑止する場合は、ソフトウェア IP を格納して読み出し禁止に設定した MCU を提供する必要がある。

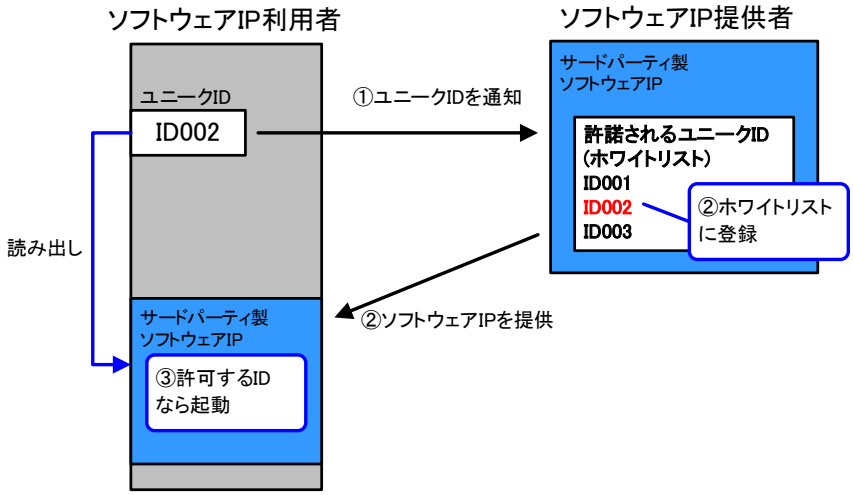
読み出し禁止の設定方法は「4 メモリ保護の設定方法」を参照してください。

2.2 起動制御（ユニーク ID 連携）

ユニーク ID は、MCU を製造する際に格納される製品個体ごとのユニークな値です。

プログラム内に特定のユニーク ID を登録することで、実行できる個体を制限します。

ソフトウェアライセンスが製品コピー数に依存する場合は、ソフトウェア内にライセンスするユニーク ID のリストを保持し、ライセンスされたユニーク ID を持つユーザ製品によってのみ実行されるソフトウェアを管理することが可能です。



① ソフトウェア IP 利用者がユニーク ID を読み出し、ソフトウェア IP 提供者に通知

② ソフトウェア IP 提供者は通知されたユニーク ID をソフトウェア IP 内のホワイトリストに登録し利用者に提供

③ ユニーク ID が合致する場合ソフトウェア IP を起動

特徴 ： ソフトウェア IP のコピーは禁止できないが不正利用を抑止。
他のユニーク ID を持つマイコンにソフトウェア IP をコピーしても起動できない。

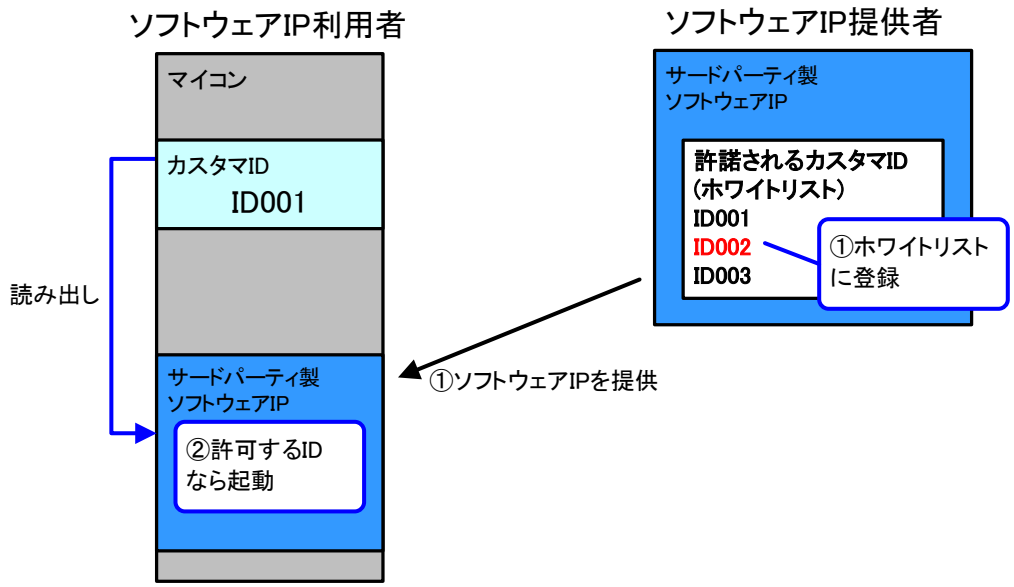
ユニーク ID の読み出しについては「RL78/G23 ユニーク ID リードドライバ アプリケーションノート (R20AN0615JJ)」を参照してください。

2.3 起動制御（カスタマ ID 連携）

カスタマ ID は、マイコン利用者が設定可能なユニークな値です。

プログラム内に特定のカスタマ ID を登録することで、実行できる個体を制限します。

ソフトウェアライセンスが製品コピー数に依存する場合は、ソフトウェア内にライセンスするカスタマ ID のリストを保持し、ライセンスされたカスタマ ID を持つユーザ製品によってのみ実行されるソフトウェアを管理することが可能です。



① カスタマ ID をソフトウェア IP 内のホワイトリストに登録し利用者に提供

② カスタマ ID が合致する場合ソフトウェア IP を起動

機能的にはユニーク ID に類似していますが、カスタマ ID の読み出しに制限が掛かっているため、ユニーク ID よりも強力な保護を期待できます。

カスタマ ID 機能の詳細については、ルネサスの QA や販売店にご相談ください。

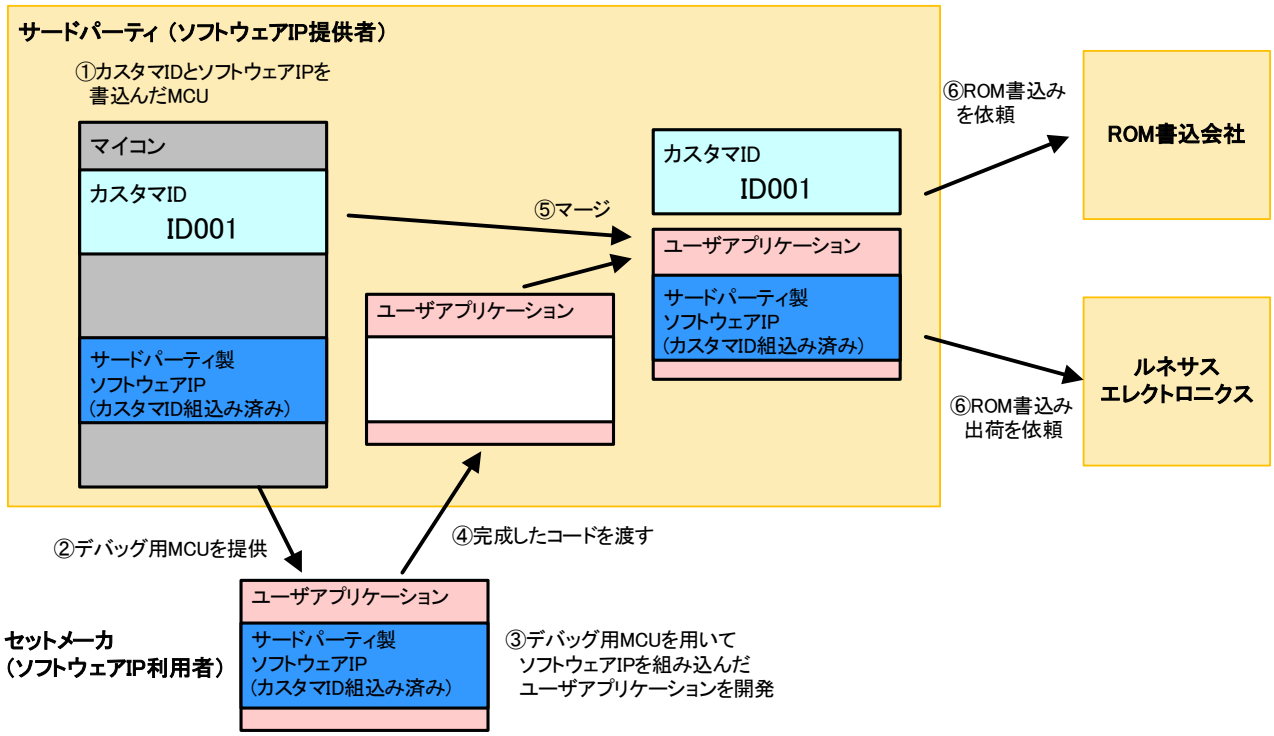
3. サードパーティプログラム（ソフトウェア IP）保護のユースケース

カスタマ ID を例に、サードパーティプログラム（ソフトウェア IP）保護のユースケースを示します。

また、サードパーティプログラム（ソフトウェア IP）と同様にユーザアプリケーションプログラムについても保護が可能ですので、同様にユースケースを示しています。

3.1 サードパーティプログラム保護

サードパーティがソフトウェア開発を丸ごと請け負うケースで、サードパーティのソフトウェア IP を保護します。
一般ユーザおよびセットメーカのソフトウェア IP 不正使用を防ぎます。



① カスタマ ID とソフトウェア IP(カスタマ ID 組込み済)を書込んだ MCU を作成

② セットメーカでのデバッグ用にカスタマ ID とソフトウェア IP を書込んだ MCU を提供

③ デバッグ用 MCU を用いてソフトウェア IP を組み込んだユーザアプリケーションを開発

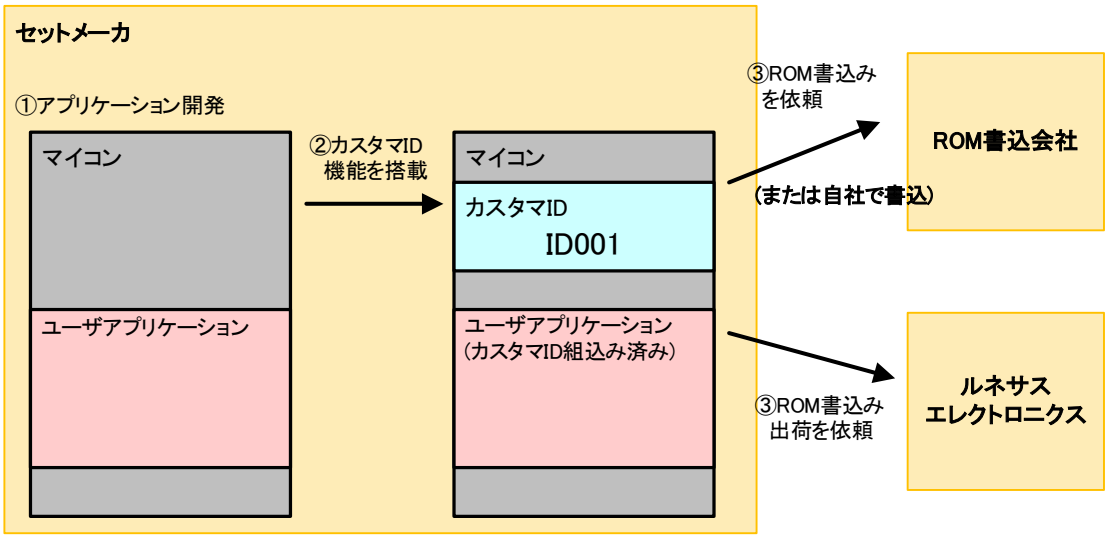
④ 完成したユーザアプリケーションコードをサードパーティに渡す

⑤ サードパーティでセットメーカのアプリケーションコードとマージ

⑥ ROM 書込みを依頼

3.2 ユーザアプリケーション保護 (1/2)

セットメーカでソフトウェア開発を行うケースで、セットメーカのユーザアプリケーションを保護します。
一般ユーザのユーザアプリケーション不正使用を防ぎます。



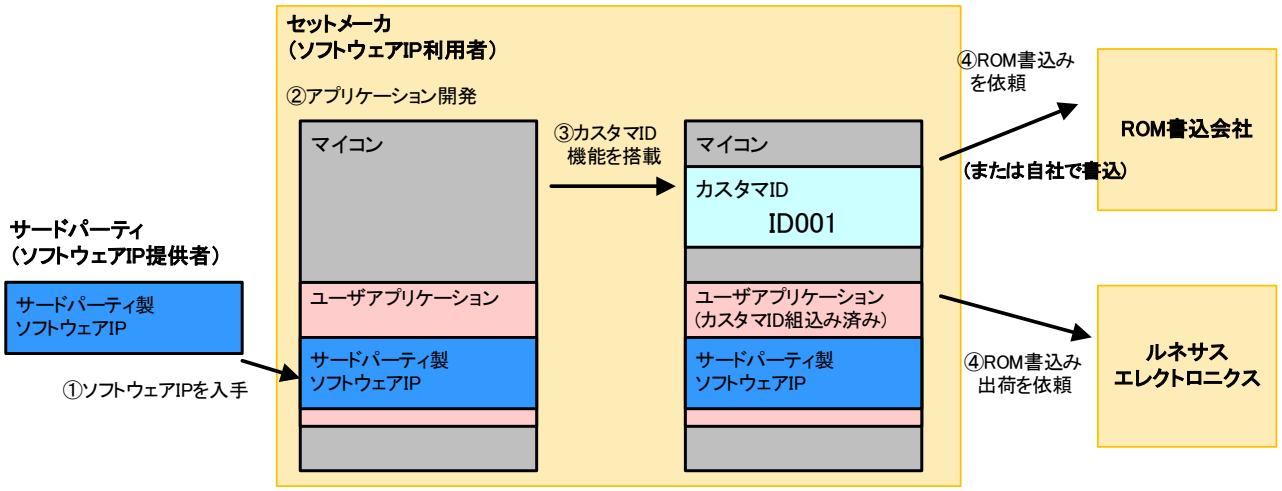
① セットメーカでユーザアプリケーションを開発

② マイコン及びユーザアプリケーションにカスタマ ID 機能を組み込む

③ ROM 書込みを依頼

3.3 ユーザアプリケーション保護 (2/2)

サードパーティよりソフトウェア IP の提供を受け、セットメーカでソフトウェア開発を行うケースで、サードパーティ製ソフトウェア IP 及びセットメーカのユーザアプリケーションを保護します。
一般ユーザのサードパーティ製ソフトウェア IP 及びユーザアプリケーション不正使用を防ぎます。



① サードパーティ製ソフトウェア IP を入手

② セットメーカで、サードパーティ製ソフトウェア IP を組み込んだユーザアプリケーションを開発

③ マイコン及びユーザアプリケーションにカスタマ ID 機能を組み込む

④ ROM 書込みを依頼

4. メモリ保護の設定方法

メモリ保護の設定は以下の方法で行います。

1. フラッシュ・プログラマによる設定
   (1). Renesas Flash Programmer (Programming GUI)
   メモリ保護設定、保護設定の解除方法を「4.1Renesas Flash Programmer によるメモリ保護設定」に示します。

   (2). フラッシュメモリプログラマ PG-FP6
   プログラミング GUI「FP6 Terminal」によりメモリ保護の設定・解除が可能です。

   (3). メモリフラッシュプログラマ FL-PR6
   FP6 Terminal（GUI ソフトウエア）によりメモリ保護の設定・解除が可能です。

2. セルフ・プログラミングによる設定
   Renesas Flash Driver を用いたセルフ・プログラミングによるメモリ保護設定が可能です。

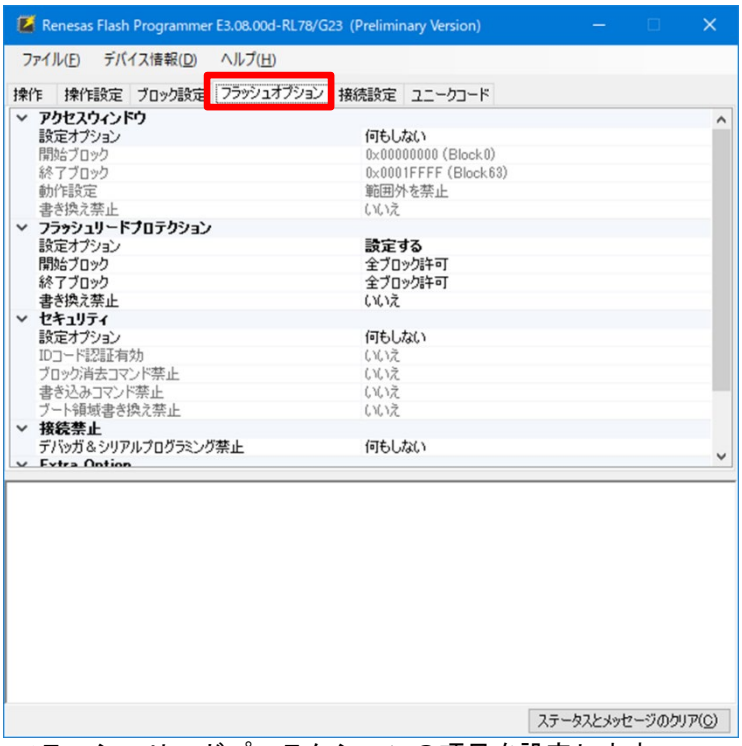
   詳細は下記マニュアルの API 関数 R_RFD_SetExtraSoftwareReadProtectAreaReq()の関連項目を参照ください。

   RL78 ファミリ Renesas Flash Driver RL78 Type01 ユーザーズマニュアル

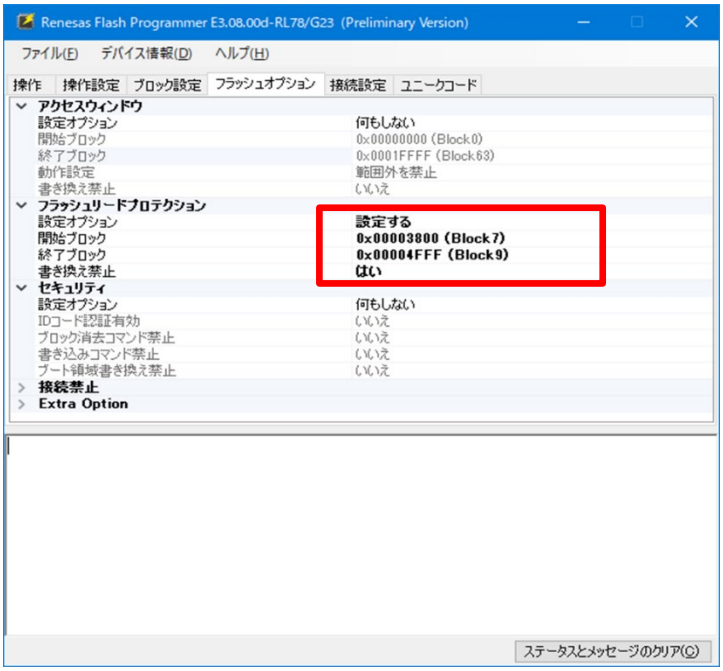
4.1 Renesas Flash Programmer によるメモリ保護設定

4.1.1 メモリ保護の設定

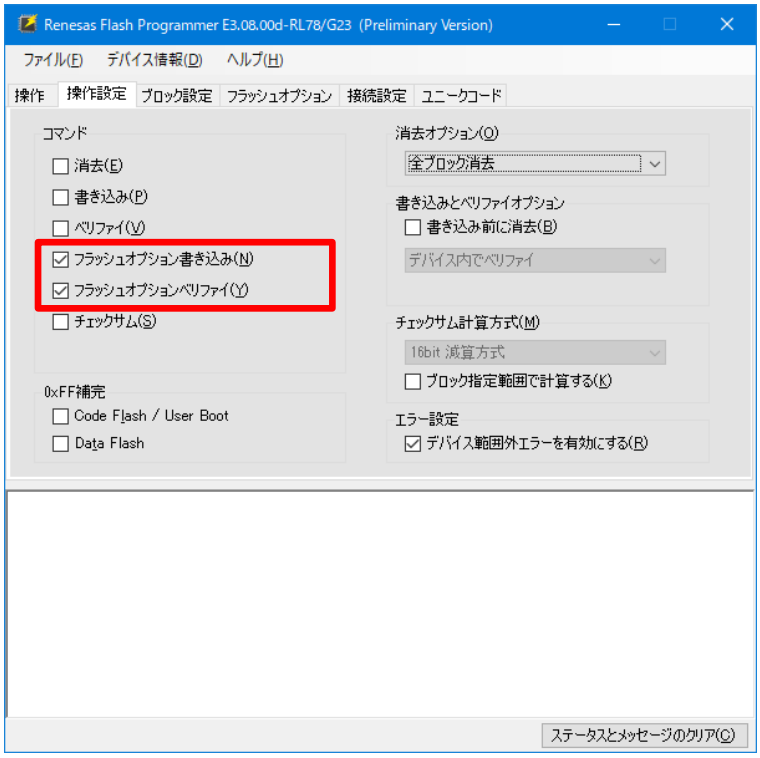
1. Renesas Flash Programmer を起動しフラッシュオプションのタブを選択します。



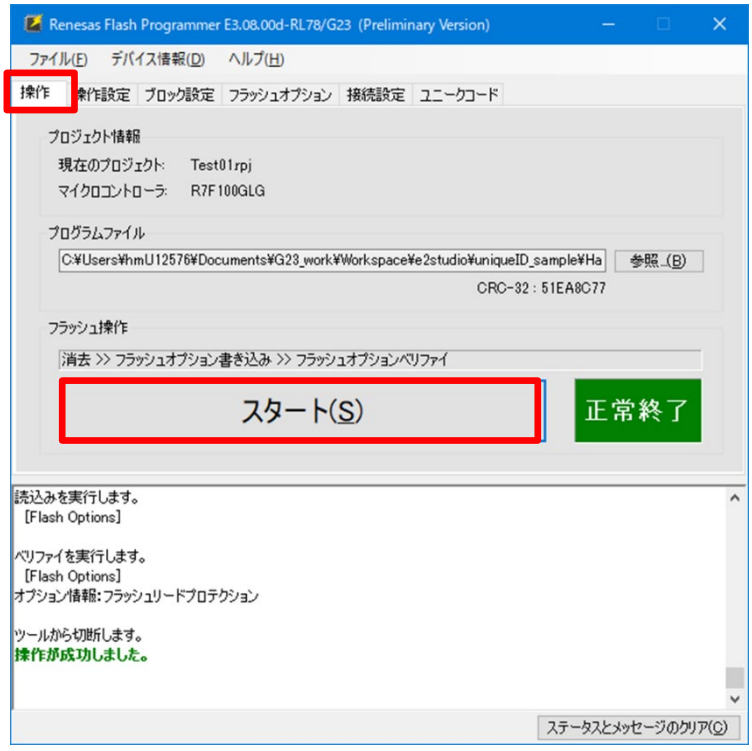
2. フラッシュリードプロテクションの項目を設定します。
設定オプション：[何もしない] → [設定する]
開始ブロック：開始ブロックを選択する
終了ブロック：終了ブロックを選択する



3. 詳細設定のタブを選択し以下の項目にチェックをチェックします。
   ☑ フラッシュオプション書込み(N)
   ☑ フラッシュオプションベリファイ(Y)

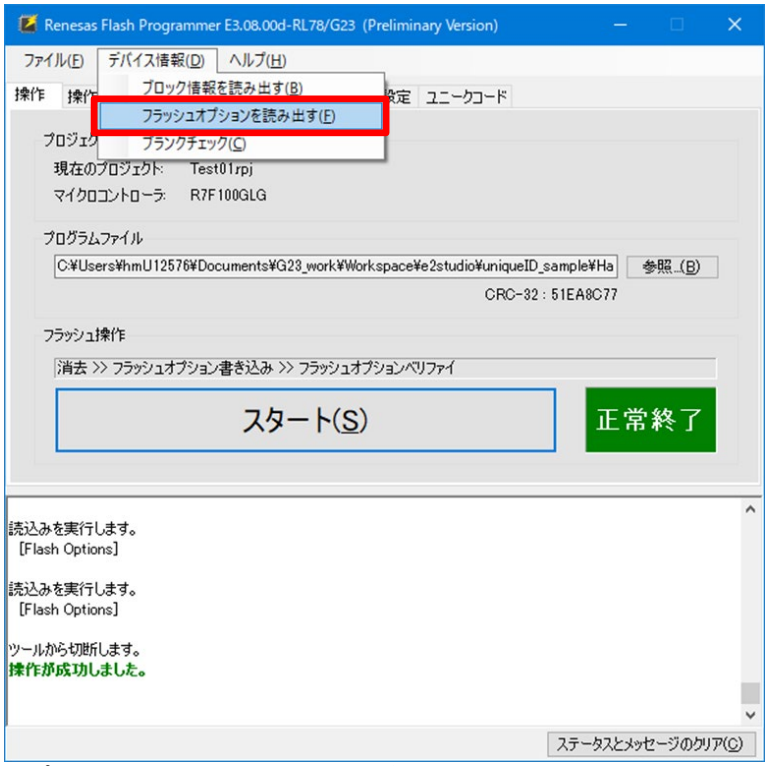


4. 設定に間違いが無ければ[操作]タブを選択し[スタート]を押下します。

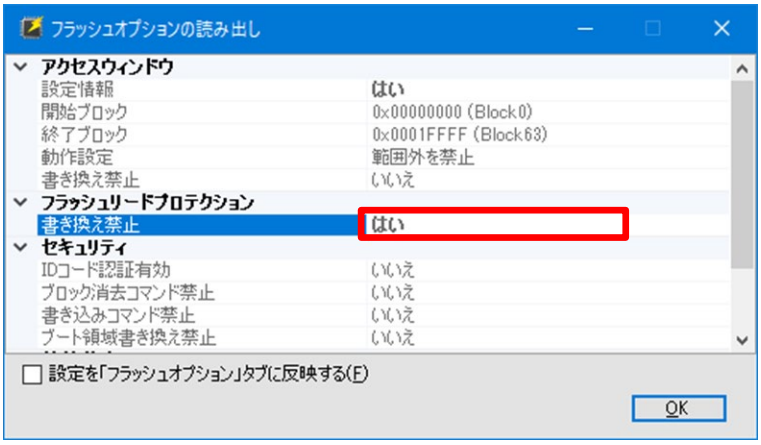


4.1.2 メモリ保護設定の確認

[デバイス情報(D)]から[フラッシュオプションを読み出す(F)]を選択します。



リードプロテクションの書込み禁止が[はい]になっています。

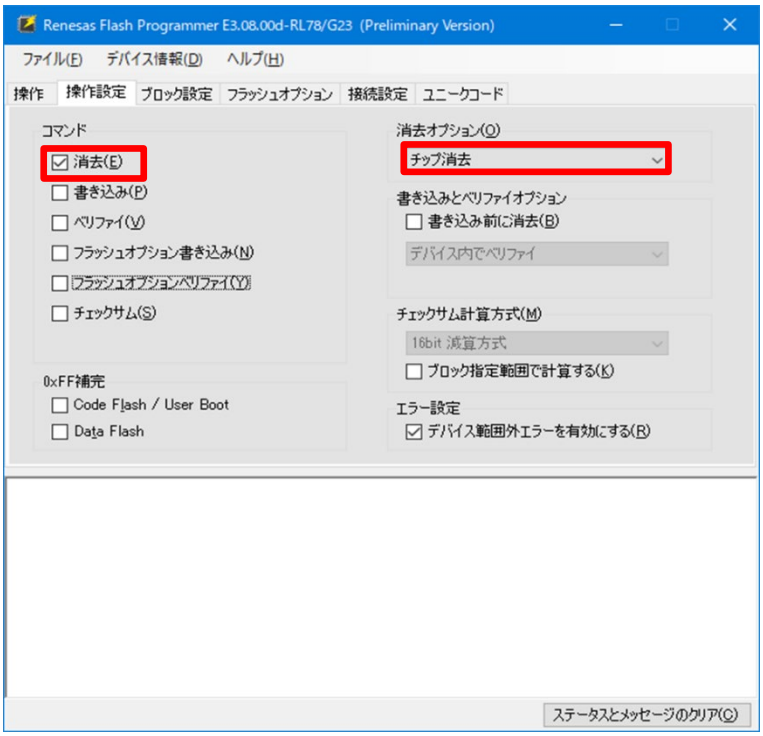


4.1.3 メモリ保護の解除

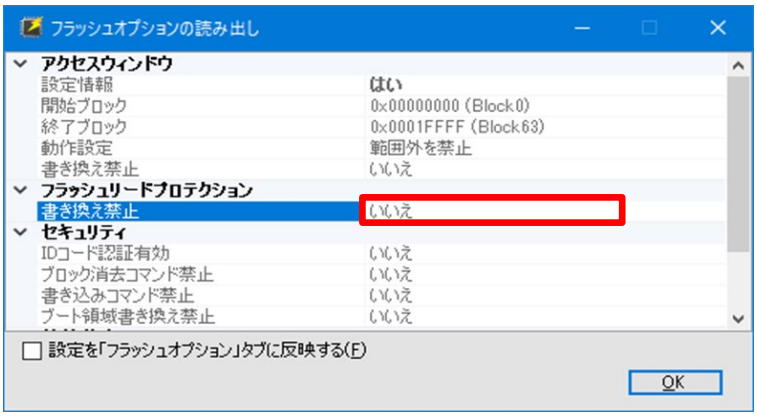
フラッシュ・リード・プロテクションの設定の解除にはチップ消去が必要です。チップ消去時にフラッシュオプションのクリアが行われます。

以下を設定し、チップ消去を行います。

☑ 消去、消去オプションで[チップ消去]を選択し、チップ消去を行います。



リードプロテクションの書込み禁止が[いいえ]になります。



5. 関連アプリケーションノート

本アプリケーションノートに関連するアプリケーションノートを以下に示します。

併せて参照してください。

(1) RL78 ファミリ Renesas Flash Driver RL78 Type01 ユーザーズマニュアル (R20UT4830JJ)

(2) RL78/G23 ユニーク ID リードドライバ アプリケーションノート (R20AN0616JJ)

6. 参考ドキュメント

RL78/G23 ユーザーズマニュアル　ハードウェア編（R01UH0896J）

RL78 ファミリ　ユーザーズマニュアル　ソフトウェア編（R01US0015J）

テクニカルアップデート／テクニカルニュース

（最新版の情報をルネサスエレクトロニクスホームページから入手してください。）

改訂記録

Rev.	発行日	改訂内容	
		ページ	ポイント
1.00	Apr.13.21	-	初版発行
1.01	Oct.8.21	4 6 7 ～ 9	章の名称を変更 「2. サードパーティプログラム（ソフトウェア IP）保護のユースケース」→「2. RL78/G23 のセキュリティ機能」 「2.3 起動制御（カスタマ ID 連携）」を追加 「3. サードパーティプログラム（ソフトウェア IP）保護のユースケース」を追加

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。