M16C/63,64A,64C,65,65C,6C グループ

内蔵フラッシュメモリのセキュリティ機能の説明

R01AN0836JJ0100
Rev.1.00
2011.10.31

要旨

本アプリケーションノートでは、M16C/63,64A,64C,65,65C,6C グループのフラッシュメモリのセキュリティ機能について説明します。

フラッシュメモリ書き換えモードの標準シリアル入出力モード、パラレル入出力モードによるフラッシュメモリの書き込み、読み出し、消去のアクセス制限を設定する方法を説明しています。

本アプリケーションノートでフラッシュメモリという場合は、マイクロコンピュータ内部のフラッシュメモリを指します。

対象デバイス

M16C/63,64A,64C,65,65C,6C グループ

本アプリケーションノートを他のマイコンへ適用する場合、そのマイコンの仕様にあわせて変更し、十分評価してください。

目次

1. 仕様

フラッシュメモリへのアクセス制限を用途に応じて設定することができます。表 1.1にソフトウェア開発時のセキュリティの例、表 1.2に量産時のセキュリティの例を示します。

ユーザーブートを使用する場合は、「3.4 ユーザブートモードを使用する場合のセキュリティ」を参照してください。

表 1.1　ソフトウェア開発時のセキュリティの例(注1、2)

セキュリティレベル	実現したい内容	シリアルライタ		パラレルライタ		節
		読み出し	書き込み	読み出し	書き込み	
なし	開発効率が優先であるため、誰でもフラッシュメモリへアクセスできるようにしたい。	○	○	○	○	3.1.1 セキュリティなし
低	簡易的なセキュリティをかけたい。万が一、IDコードを紛失しても、シリアルライタでフラッシュメモリを全消去できるようにしておきたい。	△	△	○	○	3.1.2 セキュリティレベル1

注1.　○：可、△：IDコードを知っている場合は可

注2.　IDコードが“Protect”の場合でもユーザーブートは起動することが可能です。

表 1.2　量産時のセキュリティの例(注1、2)

セキュリティレベル	実現したい内容	シリアルライタ		パラレルライタ		節
		読み出し	書き込み	読み出し	書き込み	
低 ↕ 高	IDを知る者だけがフラッシュメモリにアクセスできるようにしたい。	△	△	×	×	3.1.3 セキュリティレベル2
	誰にもフラッシュメモリが読み出されないようにしたい。フラッシュメモリは更新できるようにしておきたい。	×	△	×	×	3.1.4 セキュリティレベル3
	ライタによるフラッシュメモリへのアクセスをすべて禁止したい。	×	×	×	×	3.1.5 セキュリティレベル4

注1.　△：IDコードを知っている場合は可、×：不可

注2.　IDコードが“Protect”の場合でもユーザーブートは起動することが可能です。

2. 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。

- M16C/63 グループ High-performance Embedded Workshop スタートアッププログラムの説明 (R01AN0042JJ)
- M16C/64A グループ High-performance Embedded Workshop スタートアッププログラムの説明 (R01AN0044JJ)
- M16C/65 グループ High-performance Embedded Workshop スタートアッププログラムの説明 (R01AN0045JJ)
- M16C/65C グループ High-performance Embedded Workshop スタートアッププログラムの説明 (R01AN0046JJ)
- M16C/6C グループ High-performance Embedded Workshop スタートアッププログラムの説明 (R01AN0047JJ)

3. 周辺機能説明

3.1 内蔵フラッシュメモリのセキュリティについて

セキュリティレベルごとの設定内容やメリットとデメリットを説明します。

IDコードおよびROMコードプロテクトの設定方法については「3.2 IDコードの設定」、「3.3 ROMコードプロテクトの設定」に示します。

3.1.1 セキュリティなし

シリアルライタおよびパラレルライタのアクセスを制限しません。

表 3.1に設定内容を、表 3.2にメリットとデメリットを示します。

表 3.1　設定内容

IDコード	ROMコードプロテクト
FFFFFFFFFFFFFFh(デフォルト値)	設定しない

表 3.2　メリットとデメリット

メリット	デメリット
IDコードの管理が不要である。	誰でもシリアルライタやパラレルライタでアクセスできるため、第三者にフラッシュメモリを読み出し、書き込み、および、消去される可能性がある。

3.1.2 セキュリティレベル1

シリアルライタのアクセスをIDコードを知っている者だけに制限します。パラレルライタのアクセスは制限しません。

表 3.3に設定内容を、表 3.4にメリットとデメリットを示します。

表 3.3　設定内容

IDコード	ROMコードプロテクト
任意のID(注1)	設定しない

注1.　“Protect”および“ALeRASE”を除く

表 3.4　メリットとデメリット

メリット	デメリット
IDコードを知らない者は、シリアルライタでアクセスできない。 IDコードを紛失しても強制イレーズ機能を使用して、IDコード領域を含むフラッシュメモリを全消去できる。 パラレルライタでフラッシュメモリへのアクセスができる。	強制イレーズ機能によりフラッシュメモリを消去され、その後フラッシュメモリへ書き込みされる可能性がある。 誰でもパラレルライタでアクセスできるため、第三者にフラッシュメモリを読み出し、書き込み、および、消去される可能性がある。

3.1.3　セキュリティレベル2

シリアルライタのアクセスをIDコードを知っている者だけに制限します。また、パラレルライタのアクセスを禁止します。

表3.5に設定内容を、表3.6にメリットとデメリットを示します。

表 3.5　設定内容

IDコード	ROMコードプロテクト
任意のID(注1)	設定する

注1.　“Protect”および“ALeRASE”を除く

表 3.6　メリットとデメリット

メリット	デメリット
IDコードを知らない者は、シリアルライタでアクセスできない。 強制イレーズ機能も使用できない。	IDコードを紛失すると、フラッシュメモリにアクセスできなくなる。

3.1.4　セキュリティレベル3

シリアルライタでアクセスする際のID照合が承認されると、フラッシュメモリを全消去し、フラッシュメモリを読み出されないようにします。また、パラレルライタのアクセスを禁止します。

表3.7に設定内容を、表3.8にメリットとデメリットを示します。

表 3.7　設定内容

IDコード	ROMコードプロテクト
“ALeRASE”	設定する

表 3.8　メリットとデメリット

メリット	デメリット
シリアルライタでアクセスする際に、フラッシュメモリが全消去されるため、フラッシュメモリが読み出されない。 規定のIDコードを使用するため、IDコードの管理が不要である。	シリアルライタでアクセスする際に、フラッシュメモリが全消去されるため、開発者もフラッシュメモリを読み出すことができない。 強制イレーズ機能によりフラッシュメモリを消去され、その後フラッシュメモリへ書き込みされる可能性がある。

3.1.5　セキュリティレベル4

シリアルライタおよびパラレルライタのアクセスを禁止します。
表 3.9に設定内容を、表 3.10にメリットとデメリットを示します。

表 3.9　設定内容

IDコード	ROMコードプロテクト
“Protect”	設定する

表 3.10　メリットとデメリット

メリット	デメリット
シリアルライタおよびパラレルライタのアクセスを禁止するため、フラッシュメモリが読み出し、書き込み、および、消去されない。 強制イレーズ機能も使用できない。	一切のフラッシュメモリの書き換えができない。

3.2　IDコードの設定

IDコードは、1バイト目からそれぞれ0FFFDFh、0FFFE3h、0FFFEBh、0FFFEFh、0FFFF3h、0FFFF7h、0FFFFBh番地に割り当てられた7バイトのデータです。これらの番地にIDコードを設定したプログラムをフラッシュメモリへ書くことで設定できます。IDコード格納番地に任意の値を設定してください。

HEW(High-performance Embedded Workshop)で「C source startup Application」を選択して、新規プロジェクトワークスペースを作成すると、fvector.cが生成されます。fvector.cにIDコードの設定コードがあります。

図3.1にfvector.cに作成されるIDコードの設定コードを示します。

fvector.cでは、拡張機能指示命令“.id”を使用しています。拡張機能指示命令“.id”を使用することで、IDコード格納番地に設定する7バイトのIDコードを記述することができます。

デフォルトで“FFFFFFFFFFFFFFh”が設定されていますので、IDコードの設定を変更したい場合は、設定されている値を変更してください。

```
_asm(" .id ""¥"#FFFFFFFFFFFFFF¥"""); ←IDコードを設定
```

図3.1　fvector.cに作成されるIDコードの設定コード

3.3　ROMコードプロテクトの設定

ROMコードプロテクトは、オプション機能選択1番地(OFS1)のROMCP1ビットとROMCRビットで設定できます。ROMコードプロテクトを有効にする場合は、オプション機能選択1番地のROMCP1ビットを“0”、ROMCRビットを“1”にしてください。オプション機能選択領域はSFRではありませんので、プログラムでは書き換えられません。フラッシュメモリにプログラムを書き込むときに同時に適切な値を書き込んでください。

HEW(High-performance Embedded Workshop)で「C source startup Application」を選択して、新規プロジェクトワークスペースを作成すると、fvector.cが生成されます。fvector.cにオプション機能選択1番地(OFS1)の設定コードがあります。

図3.2にfvector.cに作成されるオプション機能選択1番地(OFS1)の設定コードを示します。

fvector.cでは、拡張機能指示命令“.ofsreg”を使用しています。拡張機能指示命令“.ofsreg”を使用することで、オプション機能選択1番地(OFS1)に設定する1バイトを記述することができます。

デフォルトで“FFh”が設定されていますので、ROMコードプロテクトを有効/無効を変更したい場合は、設定されている値を変更してください。

```
_asm("  .ofsreg 0FFH"); ←OFS1番地にFFhを書き込み設定
```

図3.2　fvector.cに作成されるオプション機能選択1番地(OFS1)の設定コード

3.4　ユーザブートモードを使用する場合のセキュリティ

ユーザブートモードを使用する場合、「図 3.3 モード判定のフローチャート」に示すようにIDコードの判定を行いません。このため、IDコードやROMコードプロテクトによるセキュリティの設定は無効となります。よって「1. 仕様」で述べたセキュリティ機能は使用できません。

ユーザブートモードにセキュリティを設ける場合は、ユーザブートプログラムにて、セキュリティ処理を行ってください。

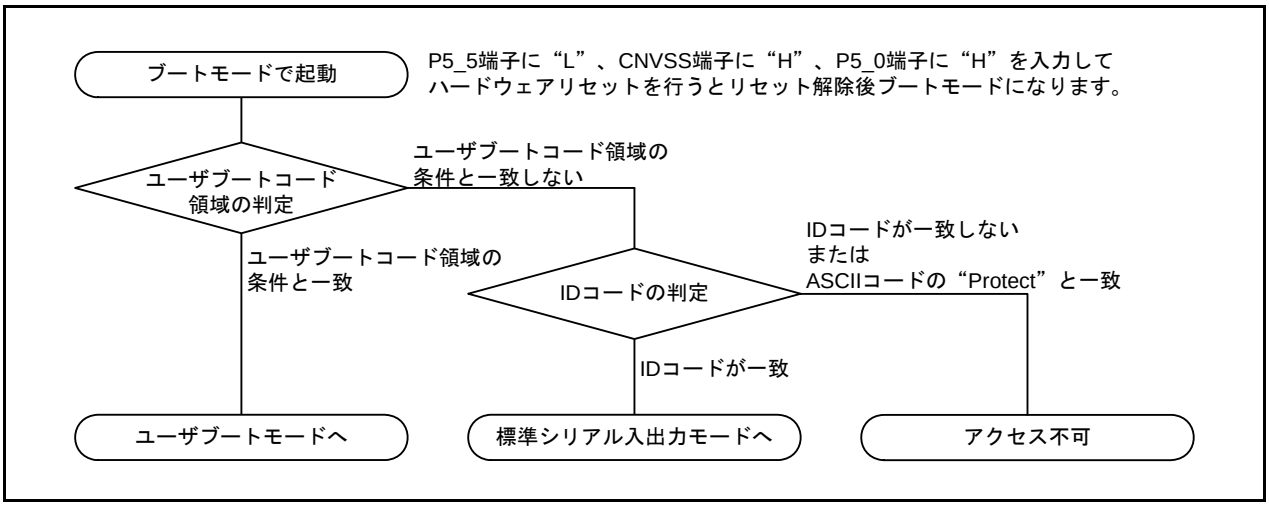

図 3.3　モード判定のフローチャート

4.　参考ドキュメント

M16C/63 グループ ユーザーズマニュアル ハードウェア編　Rev.2.00
M16C/64A グループ ユーザーズマニュアル ハードウェア編　Rev.2.00
M16C/64C グループ ユーザーズマニュアル ハードウェア編　Rev.1.00
M16C/65 グループ ユーザーズマニュアル ハードウェア編　Rev.2.00
M16C/65C グループ ユーザーズマニュアル ハードウェア編　Rev.1.00
M16C/6C グループ ユーザーズマニュアル ハードウェア編　Rev.2.00
(最新版をルネサス エレクトロニクスホームページから入手してください。)

テクニカルアップデート/テクニカルニュース
(最新の情報をルネサス エレクトロニクスホームページから入手してください。)

C コンパイラマニュアル
M16C シリーズ, R8C ファミリ C コンパイラパッケージ　V.5.45
C コンパイラユーザーズマニュアル　Rev.2.00
(最新版をルネサス エレクトロニクスホームページから入手してください。)

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/inquiry

改訂記録	M16C/63,64A,64C,65,65C,6C グループ 内蔵フラッシュメモリのセキュリティ機能の説明

Rev.	発行日	改訂内容	
		ページ	ポイント
1.00	2011.10.31	–	初版発行

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、本文を参照してください。なお、本マニュアルの本文と異なる記載がある場合は、本文の記載が優先するものとします。

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. 本資料に記載されている内容は本資料発行時点のものであり、予告なく変更することがあります。当社製品のご購入およびご使用にあたりましては、事前に当社営業窓口で最新の情報をご確認いただきますとともに、当社ホームページなどを通じて公開される情報に常にご注意ください。
2. 本資料に記載された当社製品および技術情報の使用に関連し発生した第三者の特許権、著作権その他の知的財産権の侵害等に関し、当社は、一切その責任を負いません。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。
3. 当社製品を改造、改変、複製等しないでください。
4. 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。
5. 輸出に際しては、「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。本資料に記載されている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の目的で使用しないでください。また、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に使用することができません。
6. 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。
7. 当社は、当社製品の品質水準を「標準水準」、「高品質水準」および「特定水準」に分類しております。また、各品質水準は、以下に示す用途に製品が使われることを意図しておりますので、当社製品の品質水準をご確認ください。お客様は、当社の文書による事前の承諾を得ることなく、「特定水準」に分類された用途に当社製品を使用することができません。また、お客様は、当社の文書による事前の承諾を得ることなく、意図されていない用途に当社製品を使用することができません。当社の文書による事前の承諾を得ることなく、「特定水準」に分類された用途または意図されてい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生じた損害等に関し、当社は、一切その責任を負いません。なお、当社製品のデータ・シート、データ・ブック等の資料で特に品質水準の表示がない場合は、標準水準製品であることを表します。

   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

   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、生命維持を目的として設計されていない医療機器（厚生労働省定義の管理医療機器に相当）

   特定水準： 航空機器、航空宇宙機器、海底中継機器、原子力制御システム、生命維持のための医療機器（生命維持装置、人体に埋め込み使用するもの、治療行為（患部切り出し等）を行うもの、その他直接人命に影響を与えるもの）（厚生労働省定義の高度管理医療機器に相当）またはシステム等
8. 本資料に記載された当社製品のご使用につき、特に、最大定格、動作電源電圧範囲、放熱特性、実装条件その他諸条件につきましては、当社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。
9. 当社は、当社製品の品質および信頼性の向上に努めておりますが、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、社会的損害など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、機器またはシステムとしての出荷保証をお願いいたします。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、お客様が製造された最終の機器・システムとしての安全検証をお願いいたします。
10. 当社製品の環境適合性等、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。
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固くお断りいたします。
12. 本資料に関する詳細についてのお問い合わせその他お気付きの点等がございましたら当社営業窓口までご照会ください。

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・電話番号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 エレクトロニクス販売株式会社　〒100-0004　千代田区大手町2-6-2（日本ビル） (03)5201-5307

■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/inquiry