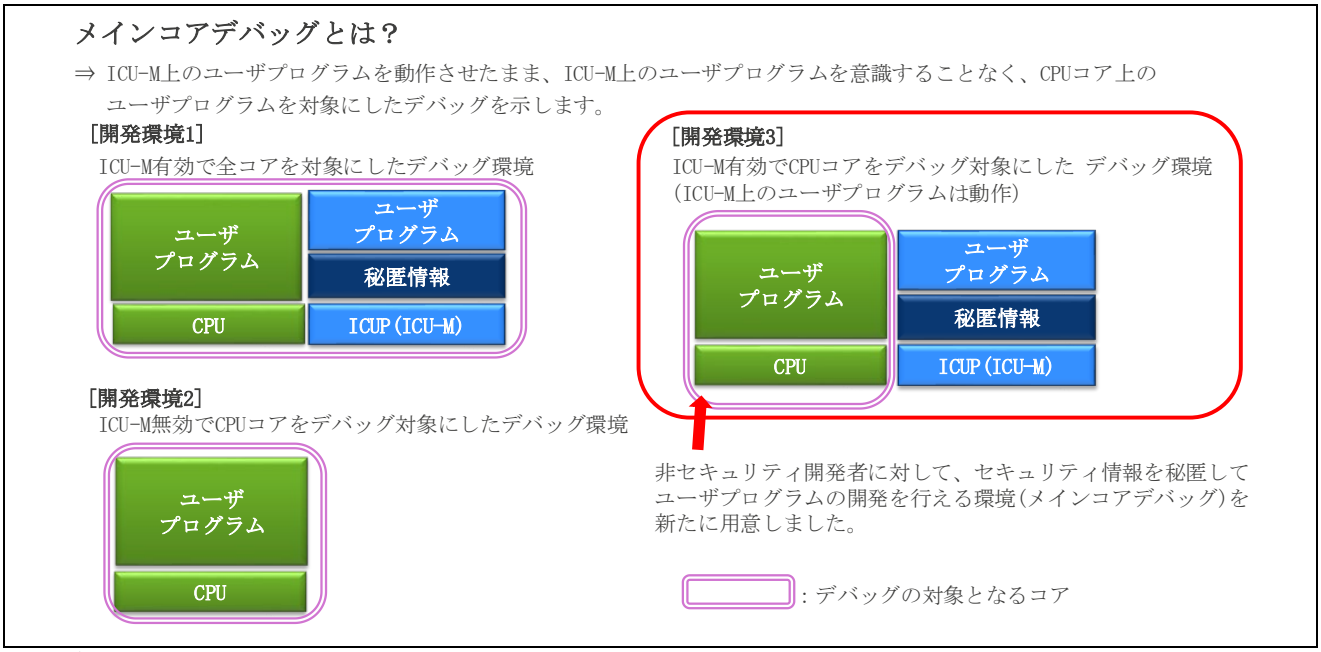
RH850 セキュリティを意識したデバッグ手法（メインコアデバッグ編）

R20AN0511JJ0101
Rev.1.01
Mar.17.20

要旨

RH850 に搭載されたハードウェアセキュリティモジュールである Intelligent Cryptographic Unit Master(以降 ICU-M と記載)を使用したアプリケーションにおいて、ICU-M コア上で動作するセキュリティ対象のユーザプログラムと CPU コア上で動作する非セキュリティ対象のユーザプログラムを分割して管理することにより、非セキュリティ開発者に対してセキュリティ情報を秘匿して ユーザプログラムの開発を行うことができます。本書では、CPU コア上で動作する非セキュリティ対象のユーザプログラムのデバッグ(以降メインコアデバッグと記載)について、使用方法、および注意事項を記載します。



対象デバイス

RH850/F1KH-D8、RH850/F1KM-S4

RH850/E2x、RH850/U2A

目次

用語説明

本書で使用する用語は、以下に示すように定義して使用します。

統合開発環境：

ルネサス製マイクロコンピュータの組み込み用アプリケーションの開発を強力にサポートするツールです。ホストマシンからインタフェースを介してエミュレータを制御するエミュレータデバッガ機能を有しています。また、同一アプリケーション内でプロジェクトのエディットからビルドおよびデバッグまでを可能にし、バージョン管理をサポートしています。

エミュレータデバッガ：

統合開発環境から起動され、エミュレータを制御してデバッグを可能とするソフトウェアツール機能を指します。

ホストマシン：

エミュレータを制御するためのパーソナルコンピュータを指します。

ターゲットデバイス：

デバッグ対象のデバイスを指します。

ユーザシステム：

デバッグ対象のデバイスを使用した、お客様のアプリケーションシステムを指します。

ユーザプログラム：

デバッグ対象のアプリケーションプログラムを指します。

ユーザインタフェース：

ターゲットデバイスと E1/E20/E2/IE850A エミュレータを接続するインタフェースを指します。

マニュアル構成

E1/E20/E2/IE850A エミュレータを使用して、RH850 ファミリのデバッグを行う場合は、(1)、(2)のユーザーズマニュアルを必ずお読みください。

(1) E1/E20/E2/IE850A エミュレータユーザーズマニュアル

E1/E20/E2/IE850A エミュレータユーザーズマニュアルには、ハードウェア仕様が記載されています。

・エミュレータの構成

・エミュレータのハードウェア仕様

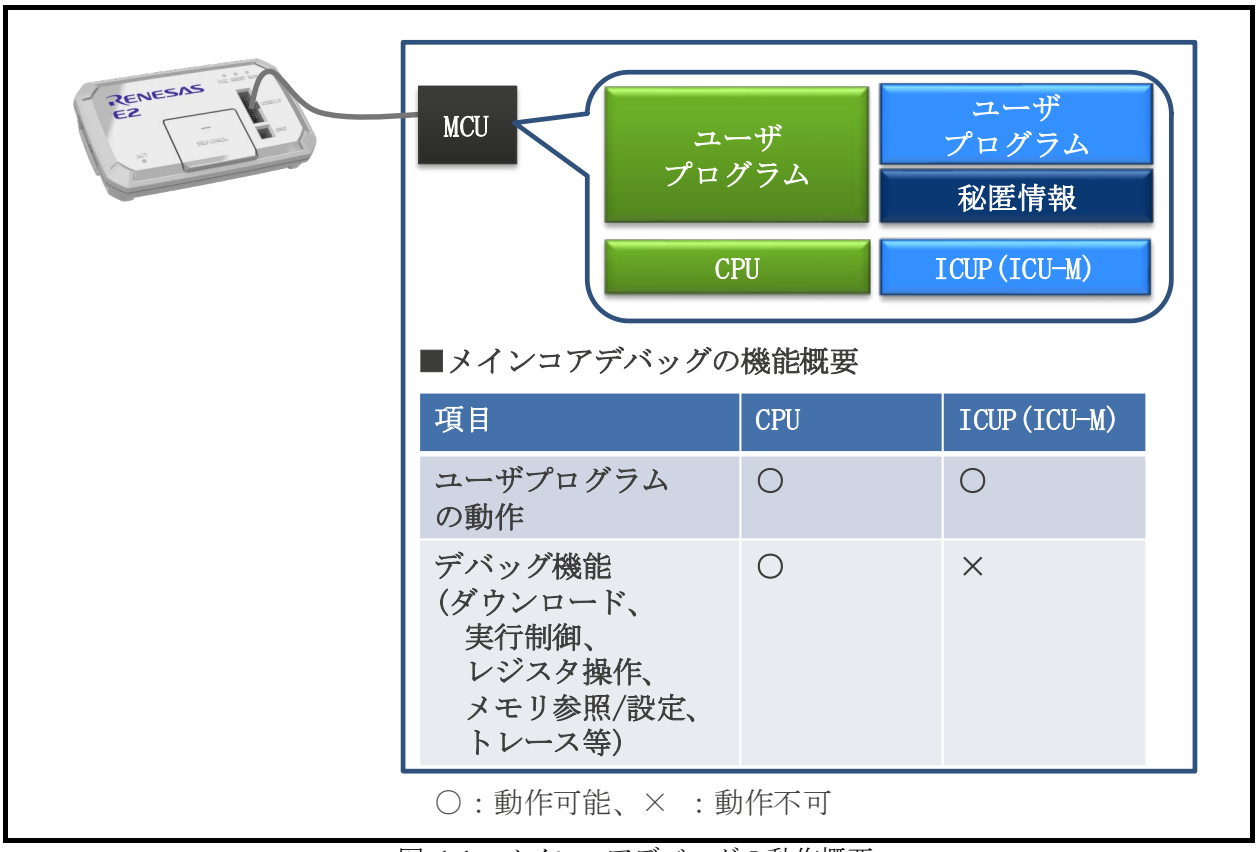
・エミュレータとホストマシンおよびユーザシステムとの接続

(2) E1/E20/E2/IE850A エミュレータユーザーズマニュアル別冊

E1/E20/E2/IE850A エミュレータユーザーズマニュアル別冊には、デバッガの機能説明および各マイコンに依存する内容、注意事項が記載されています。

1. 概要

E1/E20/E2/IE850A エミュレータで提供するメインコアデバッグ機能は、ICU-M を動作させたまま、CPU 上で動作するユーザプログラムを対象にしたデバッグを行うことが可能となります。



■メインコアデバッグの機能概要

項目	CPU	ICUP(ICU-M)
ユーザプログラムの動作	○	○
デバッグ機能（ダウンロード、実行制御、レジスタ操作、メモリ参照/設定、トレース等）	○	×

○：動作可能、×　：動作不可

図 1-1　メインコアデバッグの動作概要

1.1 メインコアデバッグの活用事例

メインコア側のソフトウェア開発者に対して ICU-M の動作を秘匿したまま開発を行えるため、各ソフトウェア開発者のセキュリティレベルに応じた開発体制を構築することが可能となります。

(1) 開発ユーザの想定

運用例を説明する際の開発ユーザの想定例を図 1-2 に示します。

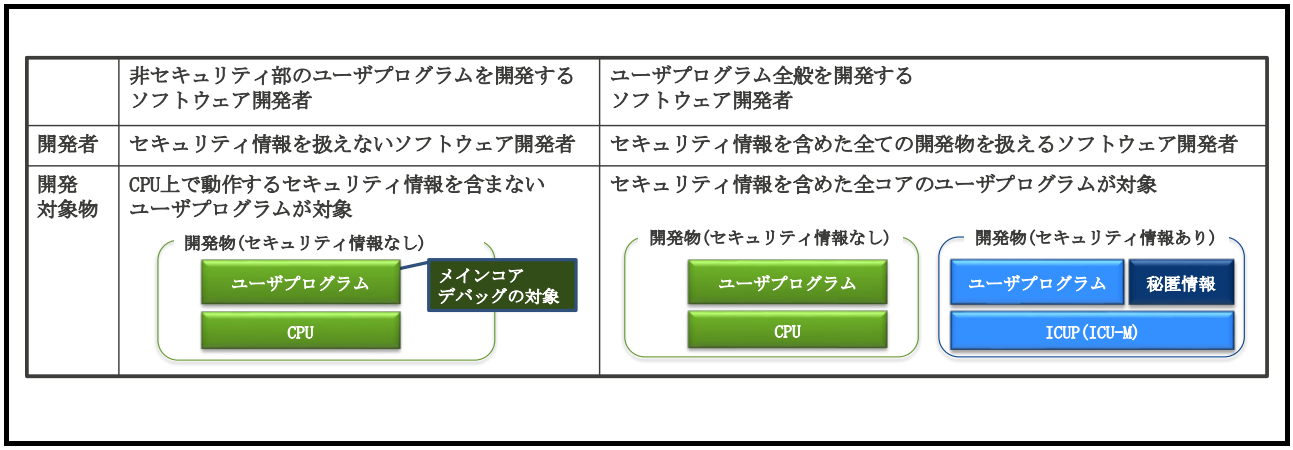


図 1-2 メインコアデバッグの活用事例(開発ユーザの想定例)

(2) 運用例

運用例を図 1-3 に示します。

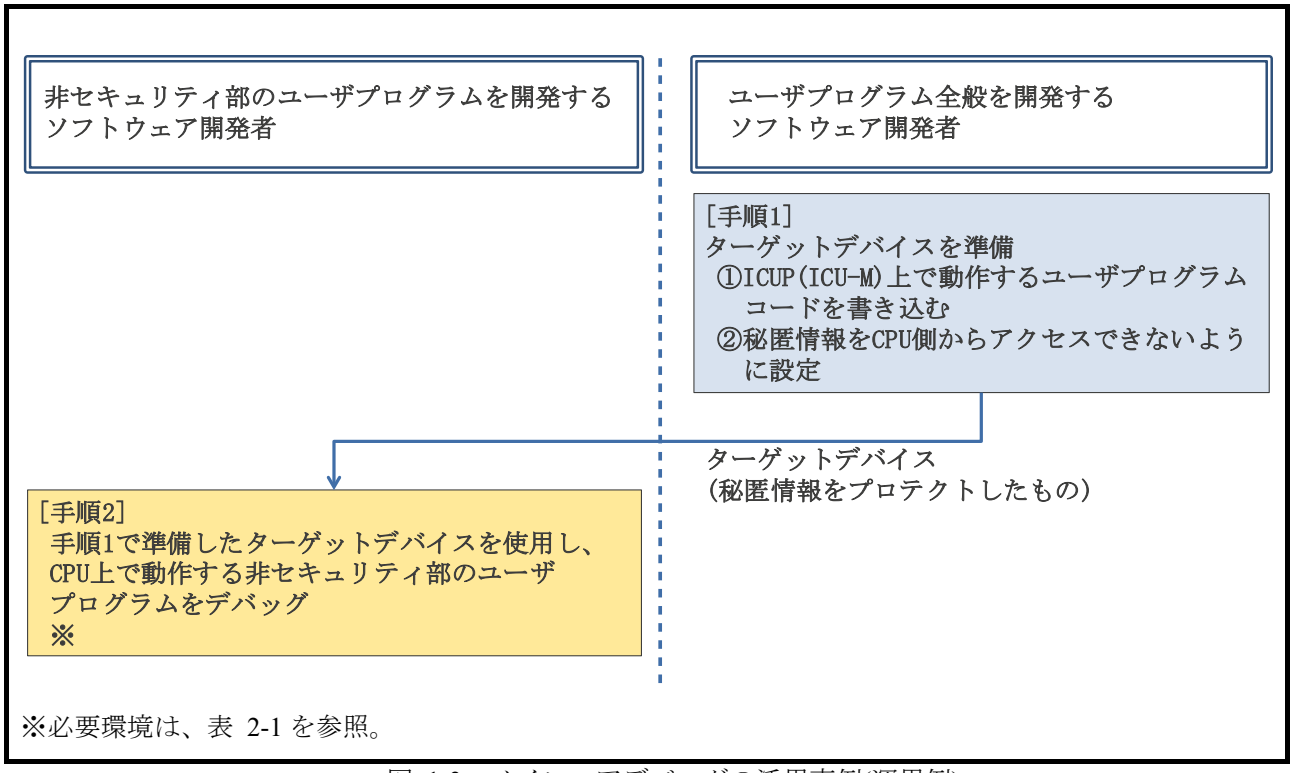


図 1-3 メインコアデバッグの活用事例(運用例)

2. 必要環境

2.1 システム構成と必要環境

システム構成を図 2-1 に必要環境を表 2-1 に示します。

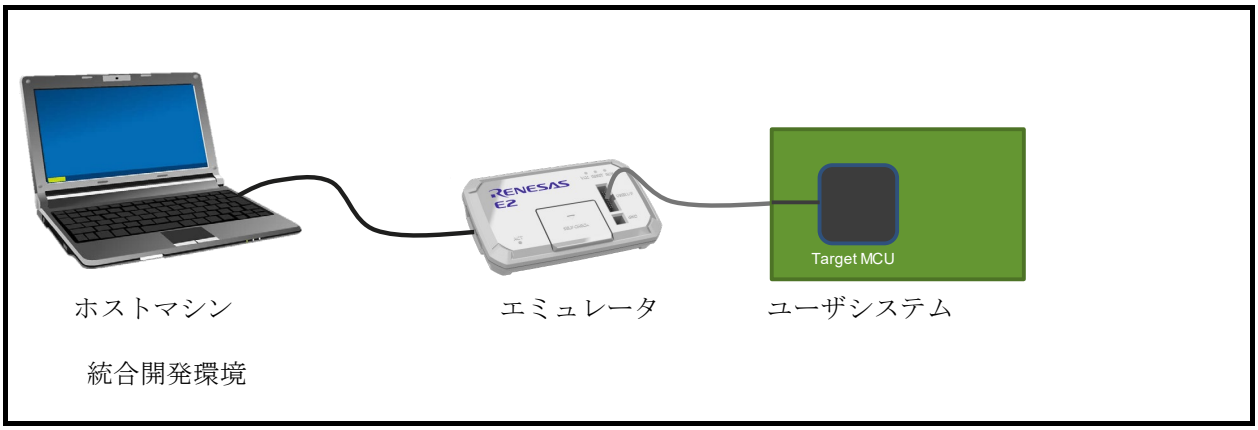


図 2-1 システム構成図

表 2-1 必要環境

項目	ターゲットデバイス	説明
ターゲットデバイスと 対応エミュレータ	RH850/F1KH-D8 RH850/F1KM-S4	[対応エミュレータ] RENESAS E1/E20/E2 エミュレータ
	RH850/E2x RH850/U2A	[対応エミュレータ] RENESAS E2/IE850A エミュレータ
統合開発環境 （バージョン）	RH850/F1KH-D8 RH850/F1KM-S4	RENESAS CS+ (V6.01 以降)
		Green Hills Software MULTI (850eserv2 V2.047 以降)
	RH850/E2x RH850/U2A	RENESAS CS+ (V8.03 以降)
		Green Hills Software MULTI (850eserv2 V2.057 以降)

3. 使用方法

3.1 メインコアデバッグの起動方法

図 3-1 にメインコアデバッグの起動方法を説明します。

C&R 認証を行わない場合は、既存デバッガの使用方法と同じです。

起動後のデバッグ機能は、既存デバッガの使用方法と同じです。

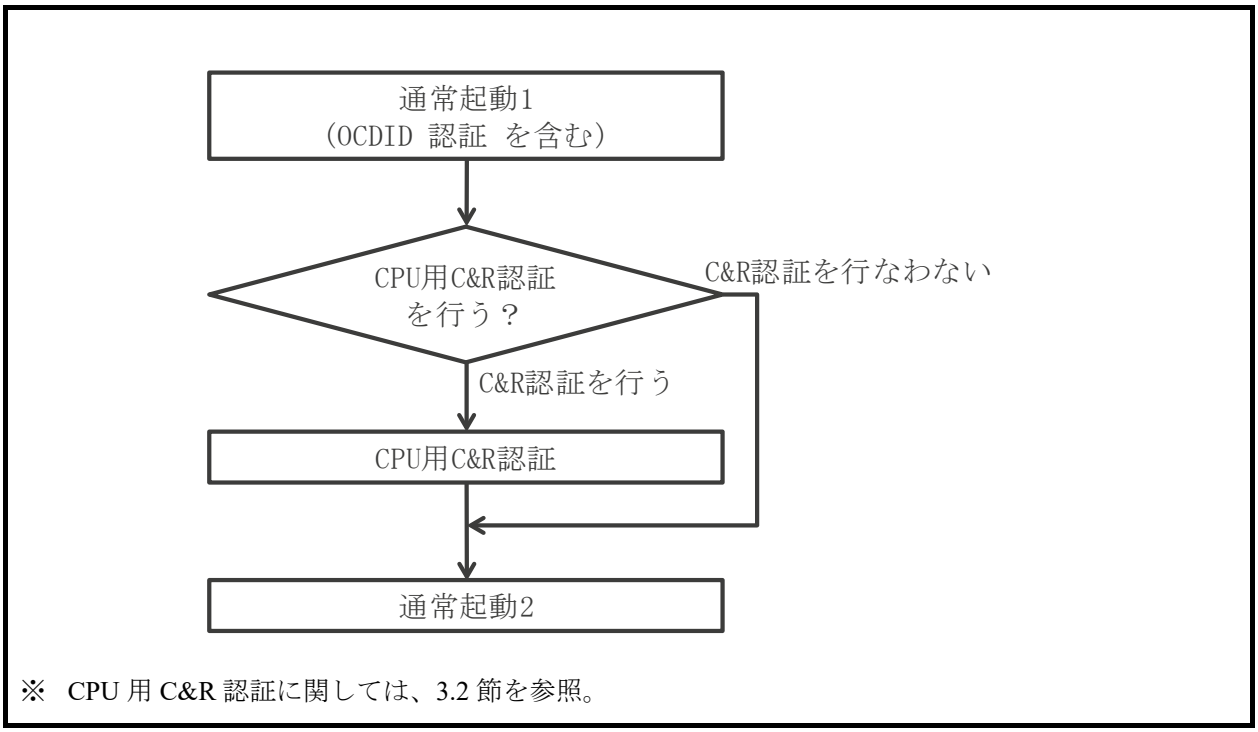


図 3-1 起動方法

3.2 デバッガによる C&R 認証方法

C&R 認証方法には「ダイアログ方式」と「DLL 方式」の 2 種類あります。ダイアログ方式では、ICU-M から取得したチャレンジデータをデバッガ上に表示し、それをユーザが読み取りレスポンスデータを生成し、ダイアログにレスポンスデータを入力することで認証する方式です。それに対し DLL 方式では、事前にユーザがレスポンスデータ生成用の DLL を作成しておき、デバッガに登録します。ICU-M から取得したチャレンジデータをデバッガが DLL に渡し、DLL により生成されたレスポンスデータをデバッガが ICU-M に送信することで認証する方式です。

3.2.1 DLL 方式

(1) 認証 DLL の作成方法

以下の関数を実装した DLL を作成してください。

int ConvertData(char target, unsigned int number, unsigned int* challenge, unsigned int* response)

- 引数

  target ： (入力) CPU 用 C&R:0、ICU-M 用 C&R:1

  number ： (入力)チャレンジデータの配列の数

  challenge ： (入力)チャレンジデータが格納された配列

  response ： (出力)レスポンスデータが格納された配列

- 戻り値

  0 なら成功、1 なら失敗

- 機能

  デバッガは配列 challenge に、ICU-M から取得したチャレンジデータを渡します。それを元に、レスポンスデータを生成し、配列 response に格納してください。デバッガはそのレスポンスデータを受け取り、ICU-M に送信することで認証を行います。

(2)　認証 DLL の設定方法

作成した DLL はデバッガに登録する必要があります。以下の設定例に従い、認証 DLL をデバッガに登録してください。

例)CS+

[RH850 E2(LPD)(デバッグ・ツール)]を右クリックし、[プロパティ(P)]を開きます。
[接続用設定]タブの[セキュリティ] -> [認証 DLL を使用する]を“はい”に変更してください。
[接続用設定]タブの[セキュリティ] -> [認証 DLL]に使用する認証 DLL の絶対パスを設定してください。

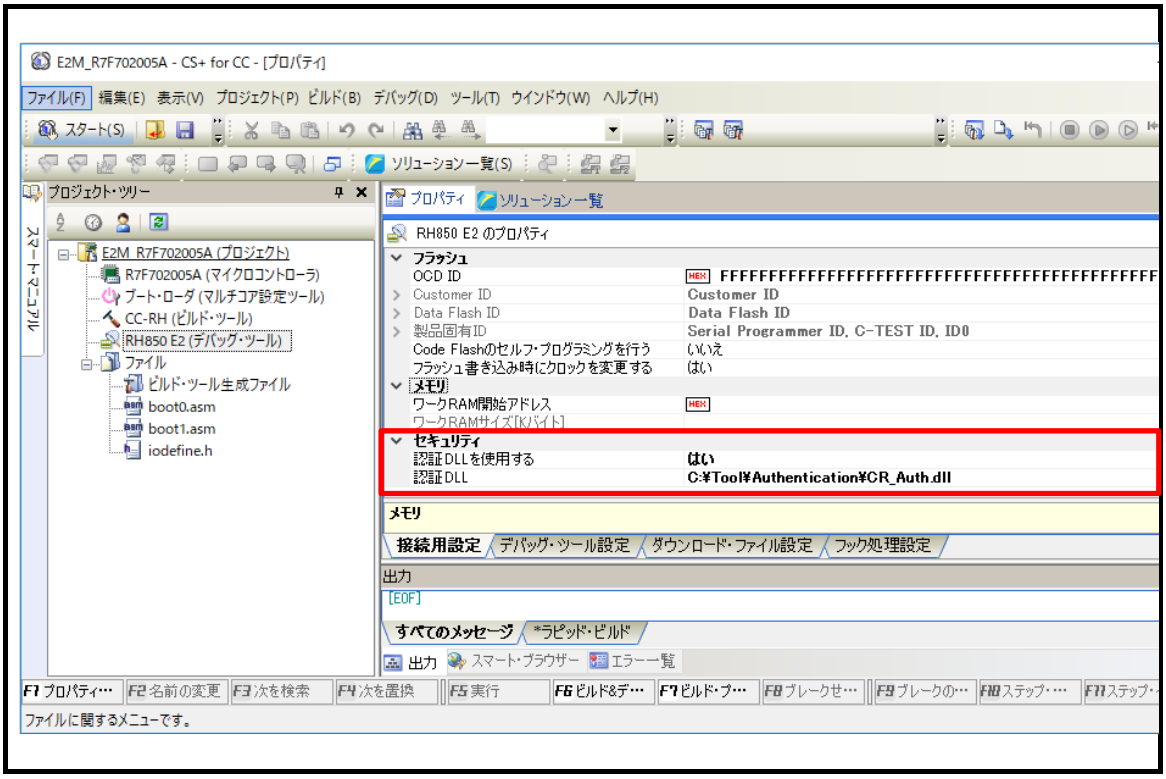


図 3-2 認証 DLL の設定方法

例)GHS MULTI

850eserv2 起動時の connect コマンドに-cr_dll=<dll_path>オプションを指定。
dll_path には認証 DLL をフルパスで指定します。
connect 850eserv2 -rh850 -e2lpd4=default … -cr_dll=c:¥Tool¥Authentication¥CR_Auth.dll

3.2.2 ダイアログ方式

例)CS+の場合

[RH850 E2(LPD)(デバッグ・ツール)]を右クリックし、[プロパティ(P)]を開きます。
[接続用設定]タブの[セキュリティ] -> [認証 DLL を使用する]を“いいえ”に変更してください。
[デバッグ(D)] -> [デバッグ・ツールへ接続(C)]を選択します。デバッガが正常にチャレンジデータを取得した場合は図 3-3 のようにダイアログに表示されます。レスポンスデータを入力して[OK]を押すことで認証します。データの並びは左端から bit127 - bit0 の順となります。

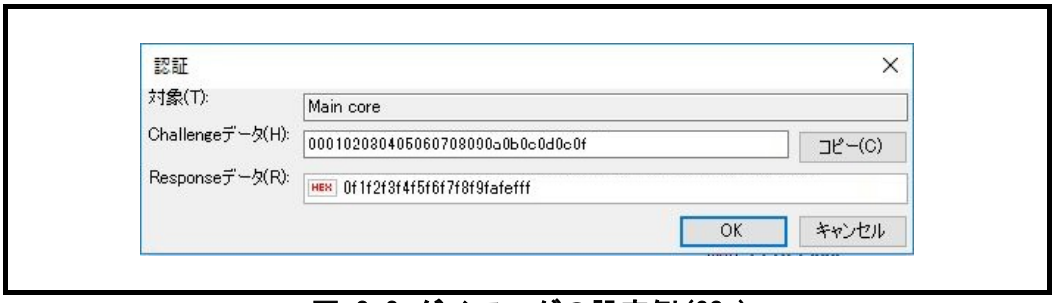


図 3-3 ダイアログの設定例(CS+)

例)GHS MULTI の場合

850eserv2 起動時の connect コマンドに-cr オプションを指定

connect 850eserv2 -rh850 -e2lpd4=default … -cr

デバッガが正常にチャレンジデータを取得した場合は図 3-4 のようにダイアログに表示されます。レスポンスデータを入力して Authentication を押すことで認証します。データの並びは左端から bit127 - bit0 の順となります。

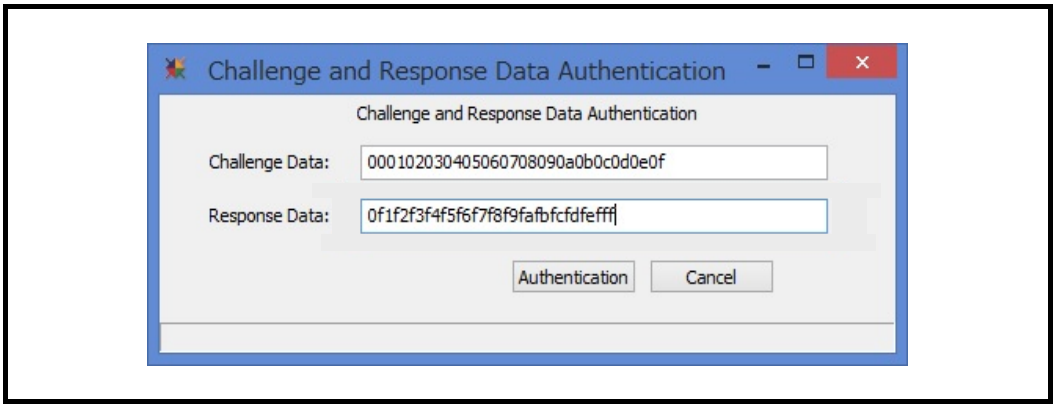


図 3-4 ダイアログの設定例(MULTI)

認証に成功した場合はコマンドペインに"C&R security Authentication success"が表示されデバッガ接続が完了します。認証に失敗した場合は"C&R security Authentication error"が表示されます。

4. 注意事項

(1)エミュレータデバッガ上から下記操作を行った場合、ICU-M と ICU-M 以外のコア間で共有資源のアクセス競合を起こさないように ICU-M の動作を一時的に停止します。

・Code Flash/Data Flash 領域のリード/ライト、ダウンロード時

例 1: ユーザプログラムのダウンロード時

例 2: ソフトウェアブレークを Code Flash に設定したままプログラムを実行した時

(プログラムの実行時にブレーク専用命令に書き換えるための処理を行ないます)

・Option Byte のリード/ライト時

(2)エミュレータデバッガ上からリセットを行うと ICU-M を含むすべてのコアに対してリセットが入ります。

(3)ICU-M からリセットを発効しようとしても、メインコアがブレークしているとリセットは発生しません。

(4)メインコアデバッグ時に周辺ブレーク機能を有効にした場合、周辺ブレーク機能の対象となる周辺モジュールはメインコアがブレーク中に動作を停止します。このとき、ICU-M 上で実行中のユーザプログラムが、停止中の周辺モジュールをアクセスしてしまうと、プログラムが正しく動作しない可能性があります。このような場合は、周辺ブレーク機能を無効にしてください。周辺ブレーク機能の対象となる周辺モジュールについては、対象デバイスのユーザーズマニュアルのオンチップデバッグユニット（OCD)章をご確認ください。

改訂記録

Rev.	発行日	改訂内容	
		ページ	ポイント
1.00	2018.09.03	-	初版
1.01	2020.03.17	-	対象デバイス(RH850/E2x, RH850/U2A)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. 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、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、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。
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。
6. 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。
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、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。
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。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. 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。
10. 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。
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。
12. 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.4.0-1 2017.11)

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。