

RX ファミリ

RX74M デバイスライフサイクルマネージメント

要旨

ルネサス RX ファミリデバイスライフサイクルマネージメント(Device Lifecycle Management、DLM)は、RX ファミリ固有のデバイス状態管理を含むセキュリティ制御機構です。DLM は、デバイスが現在どのライフサイクルフェーズ（開発、製造、または製品展開）にあるかを識別し、その状態に応じて、デバッグ機能、シリアルプログラミングインタフェース、およびルネサステストモードの各機能を制御します。

本アプリケーションノートは、RX ファミリ向け DLM の使用方法に関するガイドラインです。

必要な開発環境およびツール

本アプリケーションノートでは、以下の開発環境とツールを参照しています。

ソフトウェアと開発ツール

- Renesas Flash Programmer (RFP) v3.21 以降
<https://www.renesas.com/ja/software-tool/renesas-flash-programmer-programming-gui>
- Renesas Security Key Management Tool (SKMT) v1.12 以降
<https://www.renesas.com/ja/software-tool/security-key-management-tool>
- Gpg4win
<https://www.gpg4win.org/>

ハードウェア

- EK-RX74M、RX74M グループ用評価キット([renesas.com/ek-rx74m](https://www.renesas.com/ek-rx74m))
- Windows®11 を実行可能な PC
- USB デバイスケーブル(USB Type-C®オス - USB Type-C®オス)1 本

参考情報

本アプリケーションノートに記載されている操作を行うためには、RFP や SKMT 等の開発ツールを使用する必要があります。また、本アプリケーションノートは、RX ファミリ MCU のセキュリティ機能についての知識が必要となります。必要に応じて、*RX74M グループ ユーザーズマニュアル ハードウェア編 のセキュリティ機能* 章や、SKMT のユーザーズマニュアルを参照してください。

本アプリケーションノートは、製品開発者、製品メーカ、製品サポート、または RX ファミリ MCU の DLM の任意段階に関与するエンドユーザが読むことを想定して作成されています。

目次

1. RX74M グループ DLM の紹介	4
1.1 概要	4
1.2 用語	5
1.3 ライフサイクル状態	6
1.4 保護レベルと認証レベル	7
1.4.1 保護レベルの遷移	7
1.4.2 認証レベル鍵と認証レベル遷移	8
1.4.3 保護レベルと認証レベルの使用例	8
1.5 ALx_KEY と RMA_KEY	9
2. RX74M DLM のユースケース	10
2.1 IP 保護を必要とするケース	10
2.1.1 開発 (Valuable IP 書き込みおよび外部提供準備)	11
2.1.2 開発 (アプリケーション開発)	12
2.1.3 生産 (最終製品化)	13
2.2 IP 保護を必要としないケース	14
2.2.1 Protect Zone を使用するケース	14
2.2.1.1 開発フェーズ	16
2.2.1.2 生産フェーズ	16
2.2.2 Protect Zone を使用しないケース	17
2.2.2.1 開発フェーズ	18
2.2.2.2 生産フェーズ	18
2.3 ルネサス RMA	19
3. ALx_KEY / RMA_KEY の作成と注入	20
3.1 ALx_KEY 注入プロセスで使用するツール	20
3.2 ALx_KEY 注入の概要	20
3.3 ルネサス Key Wrap サービスとの PGP 暗号化通信の確立	21
3.3.1 ルネサス Key Wrap サービスの概要	21
3.3.2 PGP 鍵ペアの作成	22
3.3.3 ルネサス Key Wrap サービスへの登録	25
3.3.4 PGP 公開鍵交換	26
3.3.5 ルネサスの PGP 公開鍵を Kleopatra にインポート	29
3.4 UFPK と W-UFPK の作成	30
3.4.1 SKMT の紹介	30
3.4.2 UFPK ファイルの作成	30
3.4.3 ルネサス PGP 公開鍵による UFPK の暗号化	34
3.4.4 UFPK をルネサス Key Wrap サービスに送信	36
3.4.5 暗号化された W-UFPK の受信	37
3.4.6 暗号化された W-UFPK の復号	38
3.5 SKMT によるラップされた ALx_KEY の作成	39
3.5.1 AL2_KEY のラップ	39
3.5.2 AL1_KEY のラップ	40
3.6 RFP を使用した認証鍵の注入	42

3.6.1	AL2_KEY を注入	42
3.6.2	AL1_KEY を注入	44
4.	認証レベルと保護レベルの遷移	46
4.1	認証なしの状態遷移	46
4.1.1	RFP を使用した認証なしの状態遷移	46
4.1.2	Renesas Device Partition Manager(RDPM)を使用した認証不要の状態遷移	47
4.2	認証付きの状態遷移	50
4.2.1	RFP を使用した認証付き遷移	50
4.2.2	e ² studio を使用した認証付き遷移	52
5.	References	54
6.	ウェブサイトとサポート	55
	改訂記録	56

1. RX74M グループ DLM の紹介

1.1 概要

ルネサスの RX74M DLM は、MCU の製品ライフサイクル全体を通じて知的財産(IP)を保護することを目的に設計されています。本機能は、製品開発、製品出荷後の展開、フィールドアップデート、ならびに製品終息時の故障解析といった、製品の各フェーズに要求される機能に対応します。

また RX74M DLM は、以下の 2 つの要素によって制御されます。

- ・ ライフサイクル状態：製品のフェーズに合わせた MCU の状態
- ・ 保護レベル(PL2 → PL1 → PL0)および認証レベル(AL2 → AL1 → AL0)：デバッグ、シリアルプログラミング、ルネサステストモードの有効機能を決定

1.2 用語

本資料中で使用する用語の説明をいたします。

表 1-1 用語説明

用語	内容	詳細が記載されている章
保護レベル	NVRAM に格納される DLM の状態。 下位権限への遷移は任意に実施することができる。上位権限への遷移は認証レベルの反映または初期化コマンドにより実施する。 権限の高い方から順に PL2、PL1、PL0 がある。	1.4.1
OEM_PLx	デバイスライフサイクルの OEM 状態と保護レベルを併せた記載。 OEM 状態では保護レベルにより実施可能な操作が変化する。	2
認証レベル	RAM に格納される DLM の状態。 下位権限への遷移は任意に実施することができる。上位権限への遷移は ALx_KEY を用いた認証を実行したうえで実施する。 権限の高い方から順に AL2、AL1、AL0 がある。	1.4.2
ALx_KEY	認証レベルの上位権限への遷移に使用する鍵。 使用するためには、下位権限に遷移する前の認証レベルの状態で注入しておく必要がある。	1.5
初期化コマンド	シリアルプログラミングインタフェースもしくはデバッガからデバイスに送信できるコマンド。 デバイスの内部メモリを消去して、DLM を OEM、保護レベルを PL2 に遷移する。Renesas Flash Programmer (RFP) または Renesas Device Partition Manager (RDPM) で実行できる。	1.4.1
RMA	Return Material Authorization ルネサスにデバイスの故障解析を依頼するために実施する操作。デバイスからユーザーアプリケーションを消去することができる。	1.5、2.3
ルネサステストモード	故障したデバイスに対して、ルネサスにおいて故障解析するためのモード。 RMA が承認されている状態において使用可能となる。	2.3
RMA_KEY	ルネサステストモードへの遷移に使用する鍵。 使用するためには、認証レベルが AL2 の状態で注入する必要がある。	2.3
ルネサス Key Wrap サービス	Renesas が提供する鍵管理サービス。UFPK のラッピングに使用する。	3

1.3 ライフサイクル状態

表 1-2 は、ライフサイクル状態と、各状態の有効機能の概要です。

表 1-2 デバイスライフサイクル状態の定義および各状態で使用できる機能

ライフ サイクル	定義	保護 レベル	デバッグ機能	シリアル プログラミング	ルネサス テストモード
OEM	Original Equipment Manufacturer	PL2、 PL1、 PL0 の いずれ か	認証レベル(AL)に依存		使用不可
LCK_BOOT	LoCKed BOOT interface(ブートインタ フェースロック中) デバッグインタフェース とシリアルプログラミン グインタフェースは永久 に無効です。	PL0	使用不可	使用不可	使用不可
RMA_REQ	Return Material Authorization REQuest(RMA 要求) お客様は、この状態でデ バイスをルネサスに送っ てください。 OEM から RMA_REQ へ の遷移には、RMA_KEY と AL2_KEY が必要で す。	PL0	使用不可	使用可能 コード/データ MRAM 領域へ のアクセス不 可	使用不可
RMA_ACK	Return Material Authorization ACKnowledged(RMA 承 認) ルネサスでの故障解析	PL2	Secure デバッ グと Non- secure デバッ グで使用可能	使用可能 コード/データ MRAM 領域へ のアクセス不 可	使用可能
RMA_RET	Return Material Authorization RETurn(RMA 返却) 本デバイスはお客様に返 却されたものです。本デ バイスはブートしませ ん。	PL0	使用不可	使用不可	使用不可

図 1-1 に、デバイスライフサイクルの状態遷移を示します。

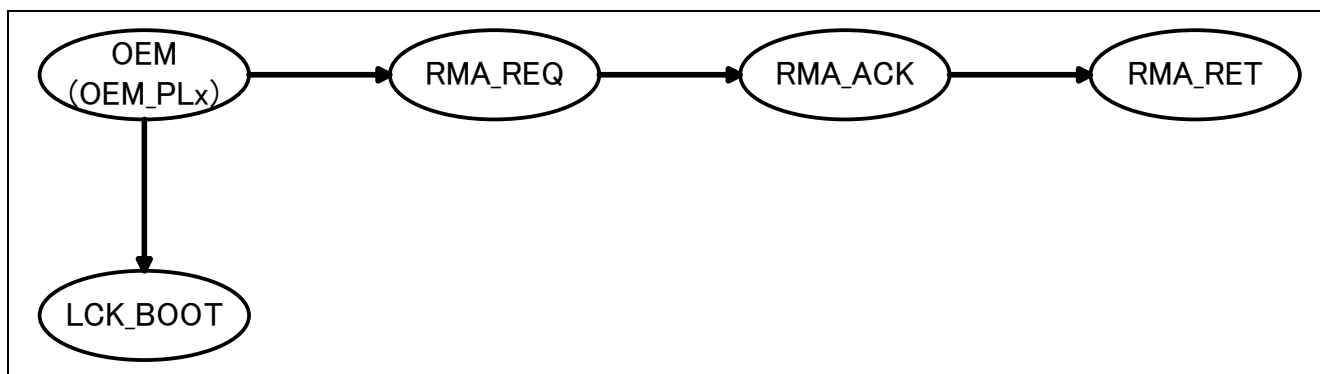


図 1-1 RX74M デバイスライフサイクル

RMA_ACK に遷移すると、MRAM の内容(恒久ブロックプロテクトされたメモリまたはレジスタを除く)が消去されます。ルネサスは、故障解析中に恒久ブロックプロテクトされたメモリまたはレジスタの内容を読み取ることができます。AL2_KEY が無効の場合、RMA_REQ への遷移はできません。

1.4 保護レベルと認証レベル

保護レベル(PL)と認証レベル(AL)はデバッグとシリアルプログラミング機能の可用性を決定します。OEM 状態の場合を除き、PL と AL は固定されています。OEM 状態では、PL と AL にはそれぞれ 3 つのレベルが設定できます。

AL はデバッグもしくはシリアルプログラマ接続後の一時的な認証状態を示し、PL は AL の MCU パワーオンリセット後の初期値を決定します。

PL と AL は、OEM 状態の時に、工場出荷時のシリアルプログラミングインタフェース(UART、USB、FINE、SWD、JTAG)を介して変更できます。

表 1-3 保護/認証レベル

保護/認証レベル	デバッグ、シリアルプログラミングによる Read/Erase/Write
PL2 / AL2	Secure と Non-secure が可能
PL1 / AL1	Non-secure のみ可能
PL0 / AL0	不可

1.4.1 保護レベルの遷移

下位権限 PL(数字の小さい PL)への遷移は制限がありません。初期化コマンドを使用することで、MCU を PL2 に初期化できます。上位権限 PL(数字の大きい PL)に遷移するには、MCU が AL の数字が PL の数字以上の認証レベルである必要があります。

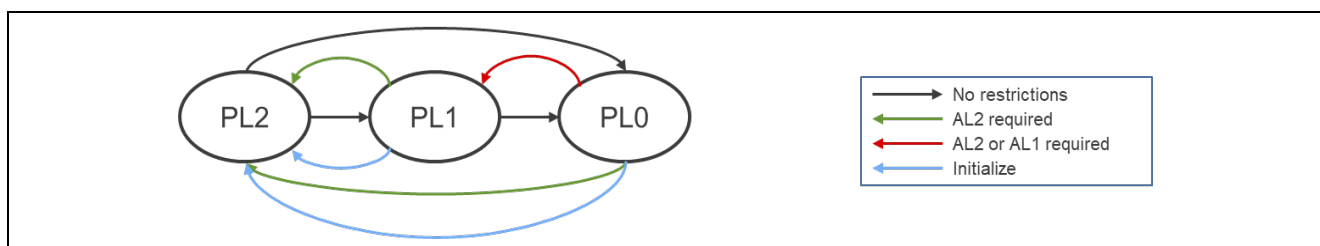


図 1-2 保護レベルの遷移

1.4.2 認証レベル鍵と認証レベル遷移

下位権限 AL(数字の小さい AL)への遷移は、認証を必要としません。上位権限 AL(数字の大きい AL)に遷移するには、適切な認証レベル鍵を使用した認証が必要です。ブートファームウェアは、認証レベルを下位権限から上位権限に変更することのみをサポートします。

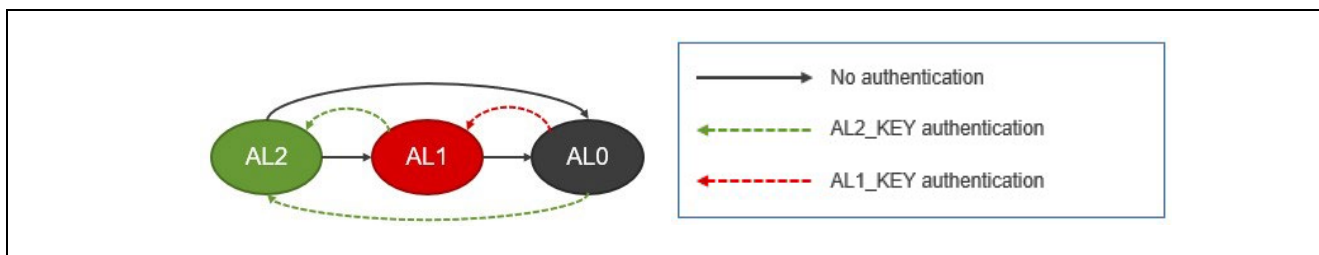


図 1-3 認証レベルの遷移

図 1-1 に示すように、PL 状態と AL 状態は OEM デバイスライフサイクル状態内で適用されます。以降は、簡潔かつ開発ツールの用語に合わせるため、デバイスライフサイクル OEM 状態の保護レベルを "OEM_PLx" と表します。

1.4.3 保護レベルと認証レベルの使用例

保護レベルと認証レベルの使用例を図 1-4 に示します。

OEM 状態において、PL 状態はパワーオンリセット時に AL 状態に反映されます。AL 状態は 1.4.1 と 1.4.2 に記載の方法で遷移することができ、PL に反映されます。

開発フェーズにおいて IP 保護を必要とする場合に、AL2 状態と AL1 状態を活用して開発フェーズを分割することができます。図 1-4 に示すように、開発フェーズ 1 では AL2 状態で開発し、開発フェーズ 2 に引き渡す際に AL1 状態とすることで、開発フェーズ 2 でのアクセス権を管理することができます。このユースケースの詳細は 2.1 で示します。また最終製品で OEM 状態を使用する場合は、PL0 を使用することを推奨します。

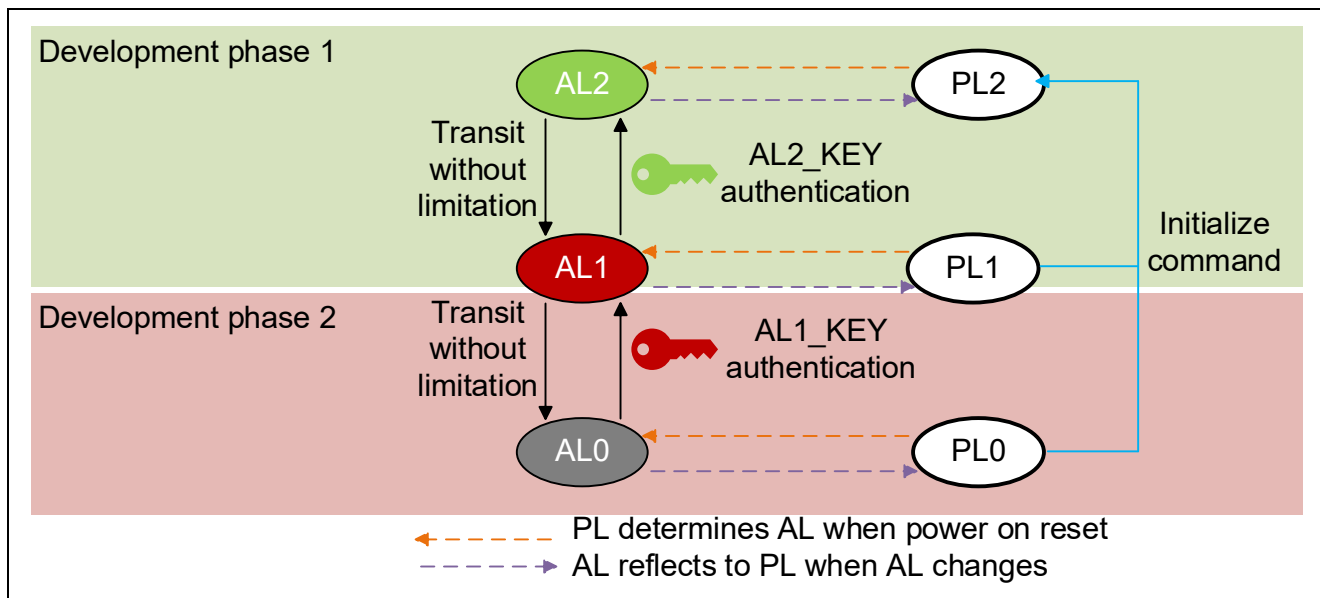


図 1-4 保護レベルと認証レベルの使用例 (OEM 状態)

1.5 ALx_KEY と RMA_KEY

認証レベルの遷移やデバイスライフサイクル状態遷移は、認証レベル鍵(AL 鍵)もしくは RMA_KEY を使用します。これらの鍵は特定の認証レベルでセキュアな鍵の注入により、MCU に書き込まれます。認証はチャレンジレスポンス方式で実行され、盗聴攻撃やリプレイ攻撃から保護します。これらの鍵は、MCU のマッピングされていない MRAM 領域に注入されます。主な鍵は以下の通りです。

- AL1_KEY - 認証レベル 1 鍵(Authentication Level 1 Key)は、AL2 または AL1 の OEM 状態で注入できます。OEM 状態の時に AL0 から AL1 に遷移するために使用します。ブートファームウェアパラメータ設定コマンドにより、AL2 または AL1 の OEM 状態で AL1_KEY を失効することができます。
- AL2_KEY - 認証レベル 2 鍵(Authentication Level 2 Key)は、AL2 の OEM 状態で注入できます。OEM 状態の時に AL0 または AL1 から AL2 に遷移するために使用します。ブートファームウェアパラメータ設定コマンドにより、AL2 の OEM 状態で AL2_KEY を失効することができます。
- RMA_KEY - Return Material Authorization Key(RMA_KEY)は、AL2 の OEM 状態で注入できます。返品承認プロセスを通じて故障解析のために MCU をルネサスに送信するために使用します。AL2_KEY が無効でない場合は、任意の OEM 状態で RMA_REQ 状態に遷移するために使用できます。

2. RX74M DLM のユースケース

本章では、Protect Zone をサポートする RX74M DLM の使用例について説明します。

開発においては、保護が必要な資産（例：価値の高い IP など）を適切に扱うために、「領域の分離」と「アクセスの制御」を組み合わせた多層的な防御設計が重要となります。Protect Zone 技術では、重要な資産を Secure 領域に配置し、それ以外のアプリケーションを Non-secure 領域に分離することで、システムレベルでの隔離を実現します。

一方で、DLM はデバッグやシリアルプログラミングといった外部からのアクセス経路を管理し、不正な操作や意図しないアクセスを防止します。

このように、Protect Zone による「実行環境の分離」と、DLM による「アクセス経路の統制」という異なるレイヤーの保護機構を組み合わせることで、単一の対策に依存しない堅牢なセキュリティ設計が可能となります。

本章では、このような設計思想に基づく活用例について紹介します。

2.1 IP 保護を必要とするケース

IP 保護が必要となるユースケースとして、価値の高い IP (Valuable IP) を MCU にあらかじめ書き込み、その MCU を外部開発者に提供し、最終アプリケーションを開発するケースが挙げられます。この開発フローでは、IP 開発者が作成した Valuable IP を保護しながら、外部開発者によるアプリケーション開発を可能にする必要があります。具体的には、以下を満たす必要があります。

- Valuable IP がデバッガやプログラマなどの外部インタフェースから読み出されないこと
- 外部開発者によるアプリケーション開発およびデバッグが可能であること
- 開発完了後にデバイスを回収し、IP 開発者が Valuable IP を再度デバッグ可能な状態に戻せること

RX74M の DLM は、PL の状態遷移と認証鍵 (AL1_KEY、AL2_KEY)、および初期化コマンドを組み合わせることで、これらの要件を満たします。すなわち、開発委託中は IP を保護しながら開発を可能とし、回収後は IP を再び扱える状態へ戻すというライフサイクル管理を実現します。図 2-1 に、本ユースケースにおける開発フローと DLM による状態遷移の概要を示します。

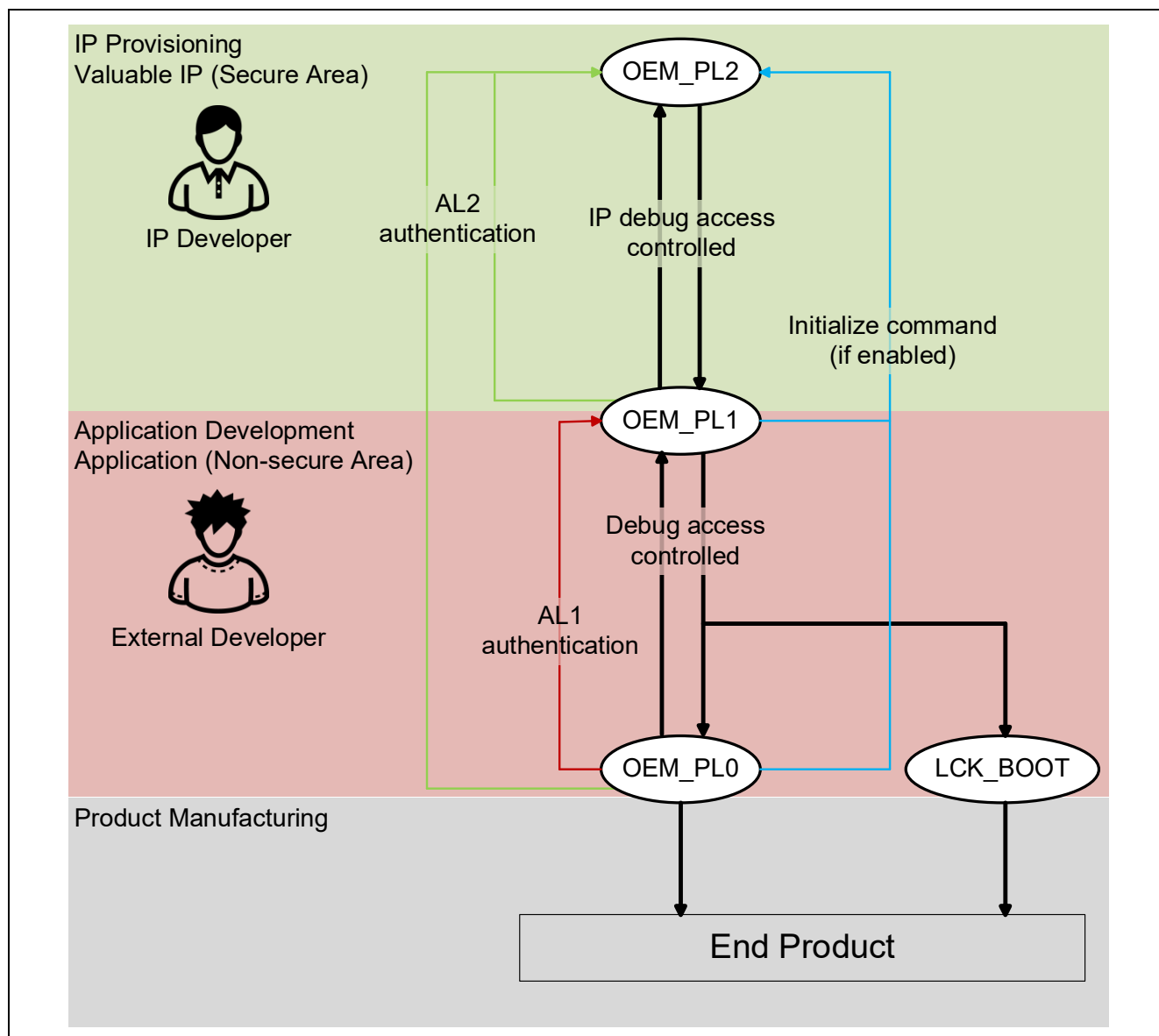


図 2-1 IP 保護を伴う開発フローと DLM 状態遷移

本図では、IP 開発者が書き込んだ Valuable IP が Secure 領域に保持されたまま外部開発者に提供され、アプリケーション開発が可能であることを示しています。また、デバイス回収後に状態遷移を行うことで、Valuable IP を再びデバッグ可能な状態に戻せることも示しています。

2.1.1 開発（Valuable IP 書き込みおよび外部提供準備）

IP 開発者は MCU を OEM_PL2 の状態に遷移させ、Valuable IP を Secure 領域に書き込みます。その後、外部開発者へ提供するために、OEM_PL1 状態へ遷移させ、デバイスのアクセス制御条件(PL 設定およびキー設定)を構成します。この工程では、以下の 2 点を同時に満たす必要があります。

- Valuable IP を保護したまま外部開発者に提供すること
- 外部開発者によるアプリケーション開発に必要な操作性を確保すること

このとき、デバイスへの外部アクセスは DLM によって制御されるため、Valuable IP の読み出しや改ざんは防止されます。一方で、設定内容により、IP の復帰性やデバッグ手段の制約が変化するため、運用目的に応じた設定の選択が重要となります。

表 2-1 に、外部開発者へデバイスを提供する際の代表的な DLM 設定と、IP 保護状態・PL 遷移可否・初期化可否の関係を示します。

表 2-1 外部開発者提供時における DLM 設定と IP 保護・PL 遷移・初期化動作の関係

DLM/PL 状態	初期化 コマンド	注入している ALx_KEY	動作内容 (IP 保護・遷移・初期化)
OEM_PL1	有効	なし	Valuable IP は保護される。初期化コマンドによりデバイスの初期化が可能。認証鍵が存在しないため、PL2 へは遷移できない (認証不可による遷移制限)。
OEM_PL1	有効	AL2_KEY	Valuable IP は保護される。初期化コマンドによりデバイスの初期化が可能。AL2 認証により PL2 へ遷移可能。
OEM_PL1	無効	なし	Valuable IP は保護される。初期化コマンドは実行できない。認証鍵が存在しないため、PL2 へは遷移できない (認証不可による遷移制限)。
OEM_PL1	無効	AL2_KEY	Valuable IP は保護される。初期コマンドは実行できない。AL2 認証により PL2 へ遷移可能。

各設定は、「IP 消去リスク」「復帰可能性」「デバッグ制限」の観点で特性が異なります。用途に応じて、これらのバランスを考慮して設定を選択することが重要です。

2.1.2 開発 (アプリケーション開発)

外部開発者は OEM_PL1 状態のデバイスを受領し、アプリケーションの開発およびデバッグを実施します。このとき、Secure 領域に配置された Valuable IP は保護されたままであり、外部開発者は以下の条件で開発を行います。

- Valuable IP の読み出しおよび書き換えは不可
- Non-secure 領域のアプリケーションは通常通り開発可能

製品状態に近い条件で評価やデバッグを行う場合には、Valuable IP を保持したまま DLM 状態の遷移が可能となる AL1_KEY の利用が有効です。AL1_KEY を使用しない場合には、以下の制約があります。

- 初期化コマンドを使用すると、Valuable IP を含む領域が消去される可能性がある
- 初期化コマンドを使用しない場合、DLM 状態の遷移が制限され、十分な評価が行えない

このため、AL1_KEY による認証により DLM 状態の遷移を行うことで、Valuable IP を保持したまま評価やデバッグが可能となります。

2.1.3 生産（最終製品化）

最終製品として出荷する際には、デバイスを OEM_PL0 に遷移させ、DLM 設定を確定します。出荷時の設定は、以下の要素の組み合わせにより決定されます。

- AL1_KEY（フィールドでのデバッグ制御）
- AL2_KEY（IP 開発者による復帰制御）
- 初期化コマンドの有効/無効

表 2-2 に、最終製品出荷時の代表的な DLM 設定と、許可されるアクセス・認証による PL 遷移・初期化可否の関係を示します。

表 2-2 IP 保護した最終製品における、出荷時の DLM 設定パターン

DLM/PL 状態	初期化 コマンド	注入している ALx_KEY	動作内容（アクセス・遷移・初期化）
OEM_PL0	無効	AL2_KEY, AL1_KEY	シリアルプログラミングインタフェースによる限定的なアクセスが可能(【注】)。AL1 認証で PL1、AL2 認証で PL2 へ遷移可能。
OEM_PL0	無効	AL2_KEY	シリアルプログラミングインタフェースによる限定的なアクセスが可能(【注】)。AL2 認証により PL2 へ遷移可能。
OEM_PL0	無効	AL1_KEY	シリアルプログラミングインタフェースによる限定的なアクセスが可能(【注】)。AL1 認証により PL1 へ遷移可能。
OEM_PL0	無効	なし	シリアルプログラミングインタフェースによる限定的なデータリードが可能(【注】)。認証鍵が存在しないため、認証による PL 遷移不可。
OEM_PL0	有効	AL2_KEY, AL1_KEY	シリアルプログラミングインタフェースによる限定的なアクセスが可能(【注】)。AL 認証により PL 遷移可能。初期化コマンドによりデバイスの初期化が可能。
OEM_PL0	有効	なし	シリアルプログラミングインタフェースによる限定的なアクセスが可能(【注】)。初期化コマンドによりデバイスの初期化が可能。
LCK_BOOT	使用不可	なし	アクセス不可。PL 遷移不可。

【注】 MCU ユニーク ID 等の限定的な MCU の情報を取得可能

これらの設定により、出荷後のデバッグ可否、フィールドでの保守性、およびセキュリティレベルを用途に応じて設計することができます。

2.2 IP 保護を必要としないケース

本節では、2.1 で示したように外部開発者へ Valuable IP を提供するケースではなく、同一の開発主体がアプリケーション全体を開発するケースについて説明します。このケースでは、外部からの IP 保護は主目的ではありません。一方で、アプリケーション内で扱うデータや処理内容によっては、秘密情報の保護が必要となります。本デバイスでは、RSIP-E50D（ラップ鍵を取り扱うことができる Security IP）を使用することで、Protect Zone を使用しない構成でもセキュアブートや各種セキュリティ処理を実現できます。したがって、Protect Zone はすべての用途で必須ではありません。

Protect Zone の使用を検討する代表的なケースは、RSIP-E50D Compatibility Mode で平文鍵を使用するシステムのように、ソフトウェアが平文の秘密鍵を直接扱う場合です。本節では、以下の 2 つの構成について説明します。

- Protect Zone を使用するケース
- Protect Zone を使用しないケース

2.2.1 Protect Zone を使用するケース

本ケースでは、RSIP-E50D Compatibility Mode で平文鍵を使用するシステムのように、ソフトウェアが平文の秘密情報を扱う場合を想定します。このような場合、秘密鍵やセキュリティ処理を Protect Zone の Secure 領域に配置することで、アプリケーションの他の領域から分離できます。これにより、

- デバッガやプログラマからの不用意な参照
- アプリケーションバグによる意図しないアクセス

を抑制できます。

なお、本デバイスでは RSIP-E50D を使用することでラップ鍵ベースのセキュリティ構成も実現可能です。この場合、ソフトウェアで平文鍵を直接扱わない構成となるため、Protect Zone は必須ではありません。

図 2-2 に、Protect Zone を使用して平文の秘密情報を保護する場合の開発フローと DLM 状態遷移の概要を示します。

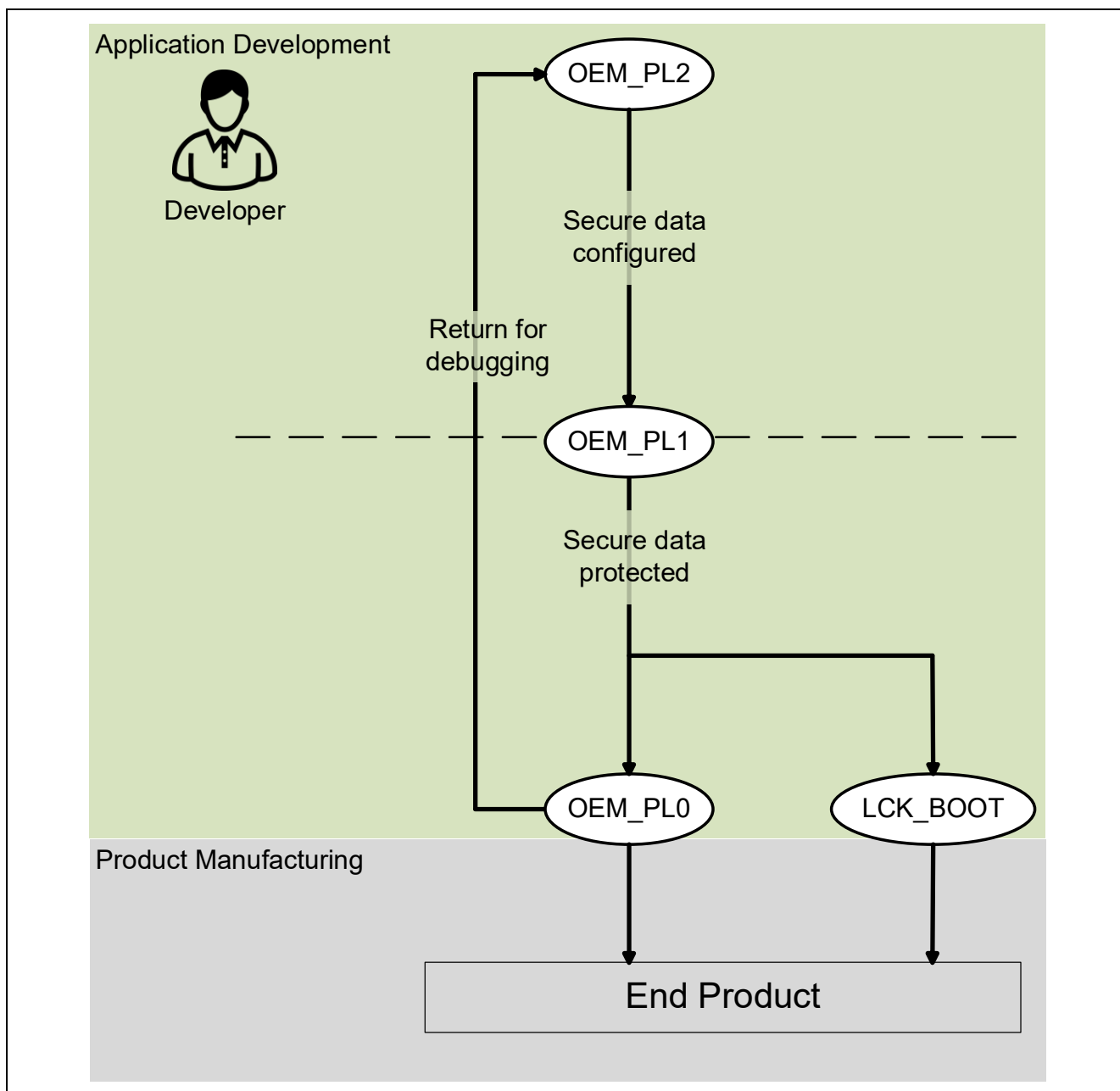


図 2-2 IP 保護を必要とせず Protect Zone を使用するケース

本図では、平文の秘密鍵やセキュリティ処理を Secure 領域に配置し、Protect Zone により他領域から分離する構成を示しています。同一の開発主体が開発を行うため IP の受け渡しはありませんが、Secure 領域の開発時に設定された Secret Data（秘密情報）は、Non-secure 領域開発時には Protect Zone により保護されます。また、生産時に Block Protect を設定することで、Secure 領域の書き換えを恒久的に禁止する構成とすることも可能です。

2.2.1.1 開発フェーズ

同一の開発主体がアプリケーション全体を開発するため、2.1 のような外部開発者との分離はありません。開発時には OEM_PL2 状態で、

- 平文鍵を扱う処理
- セキュリティ処理（例：Root of Trust）

を配置します。その後、Non-secure 領域にアプリケーションを配置し、システム全体の評価を行います。このケースでは、開発中に AL キーを必ずしも使用する必要はありません。

注：開発段階では、MRAM のブロックプロテクトを設定しないでください。ブロックプロテクトを使用すると初期化コマンドが使用できず、デバイスの再プログラムができなくなります。

2.2.1.2 生産フェーズ

量産時には、Secure 領域に配置された平文秘密情報を保護するために、DLM 設定を確定します。選択の主な観点は以下です：

- 出荷後に解析や保守を許可するか
- 平文秘密情報の保護をどの程度強化するか

強い保護が必要な場合は、ブロックプロテクトを使用して Secure 領域の書き換えを禁止します。一方、解析や保守を行う可能性がある場合は、AL1_KEY や AL2_KEY を設定し、認証付きで PL 遷移できるようにします。

表 2-3 Protect Zone 使用時における DLM 設定とデバッグ可否・初期化可否の関係

DLM/PL 状態	初期化 コマンド	注入してい る ALx_KEY	動作内容（アクセス・遷移・初期化）
OEM_PL0	無効	AL2_KEY, AL1_KEY	ブートモードによる限定的なアクセスが可能(【注】)。AL1 および AL2 認証により PL1 および PL2 に遷移可能。
LCK_BOOT	使用不可	なし	アクセス不可。PL 遷移不可。

【注】 MCU ユニーク ID 等の限定的な MCU の情報を取得可能

Protect Zone を使用する場合は、平文秘密情報をどの程度保護するか（強度）と、出荷後に解析や保守を可能とするか（利便性）のバランスを考慮して設定を選択します。

2.2.2 Protect Zone を使用しないケース

本ケースでは、Protect Zone 使用せず、フラットな構成でアプリケーションを開発します。本デバイスでは、RSIP-E50D（ラップ鍵を取り扱うことができる Security IP）を使用することで、平文の秘密鍵を扱わない構成を採ることができます。この構成は、セキュリティ機能を必要とするシステムだけでなく、一般的なアプリケーション開発にも広く適用されます。例えば、

- ラップ鍵を用いたセキュアブート
- セキュリティ IP により管理された鍵を用いる処理
- 特別な分離を必要としない一般的なアプリケーション

などに適しています。

図 2-3 に、Protect Zone を使用しない場合の構成と開発フローおよび状態遷移の概要を示します。

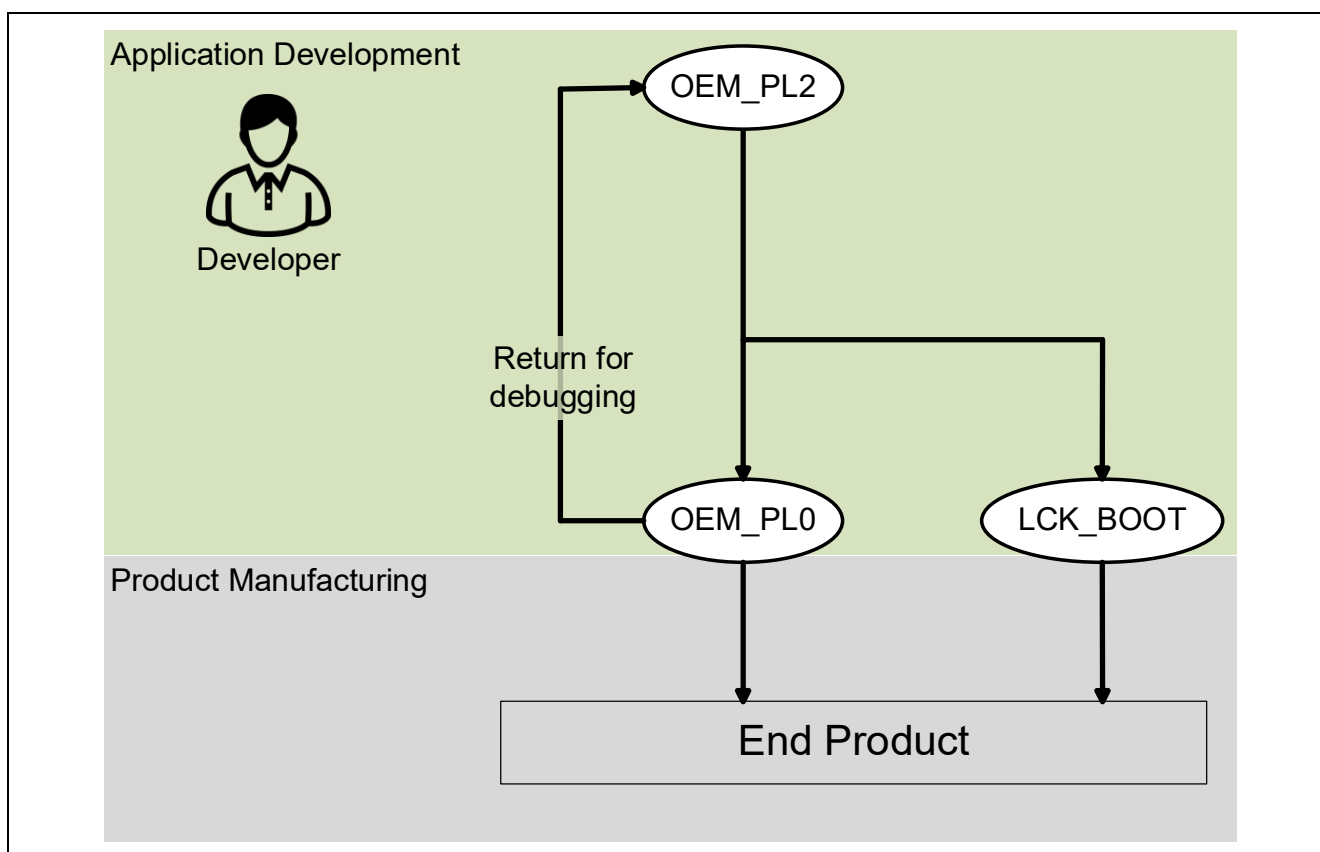


図 2-3 IP 保護を必要とせず Protect Zone を使用しないケース

本図では、Protect Zone を使用せず、フラットな構成でアプリケーションを開発する場合を示しています。RSIP-E50D によりラップ鍵を使用することで、ソフトウェアは平文の秘密鍵を扱う必要がなく、構成を簡素化できます。このため、開発の自由度が高く、特別な領域分離を必要としない用途に応じた構成となります。

2.2.2.1 開発フェーズ

開発は OEM_PL2 状態で実施し、AL キーは必須ではありません。量産前の評価では、必要に応じて PL0 へ遷移して確認を行います。

注: 開発段階では、MRAM のブロックプロテクトを設定しないでください。ブロックプロテクトを設定すると初期化コマンドが使用できず、デバイスの再プログラムができなくなります。

2.2.2.2 生産フェーズ

出荷後の解析や再プログラムが必要な場合は、AL2_KEY を設定します。不要な場合は、PL0 または LCK_BOOT 状態で出荷することで、より制限された運用が可能です。

表 2-4 Protect Zone 未使用時における DLM 設定とアクセス制御・PL 遷移・初期化動作の関係

DLM/PL 状態	初期化 コマンド	注入している ALx_KEY	有効な機能
OEM_PL0	無効	AL2_KEY	ブートモードによる限定的なアクセスが可能(【注】)。AL2 認証により PL2 へ遷移可能。
OEM_PL0	有効	AL2_KEY	ブートモードによるアクセス制限が可能(【注】)。AL2 認証により PL2 へ遷移可能。初期化コマンドによりデバイスの初期化が可能。
OEM_PL0	無効	なし	ブートモードによる限定的なアクセスが可能(【注】)。
OEM_PL0	有効	なし	ブートモードによる限定的なアクセスが可能(【注】)。初期化コマンドによりデバイスの初期化が可能。
LCK_BOOT	使用不可	なし	アクセス不可。

【注】 MCU ユニーク ID 等の限定的な MCU の情報を取得可能

2.3 ルネサス RMA

ルネサスによる故障解析のために MCU を提出するには、RMA_KEY を注入し、デバイスを RMA_REQ 状態に遷移させる必要があります。なお、AL2_KEY が認識不能な場合、OEM_PL2 から RMA_REQ への遷移はできません。RMA_REQ への遷移により、永続的に保護されていない全てのコードおよびデータは消去され、故障解析のために MCU をルネサスへ送付することができます。このユースケースは、上記のすべての構成と組み合わせて利用することができます。

図 2-4 に、製品出荷後に不具合が発生した場合の RMA フローと DLM 状態遷移の概要を示します。

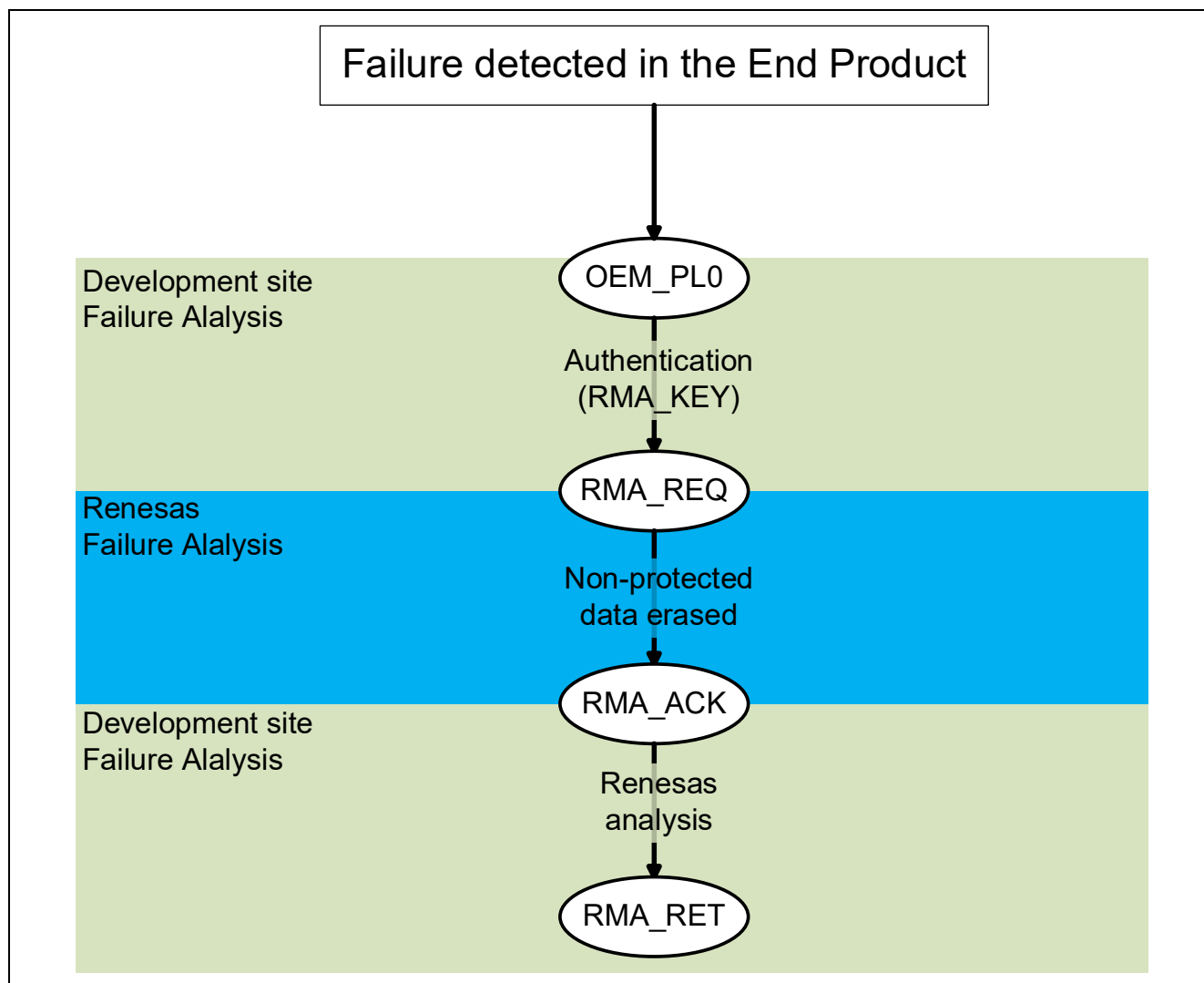


図 2-4 ルネサス RMA

本図では、製品出荷後に不具合が検出された場合、RMA_KEY による認証によりデバイスを RMA_REQ 状態へ遷移させる流れを示しています。この遷移により、保護されていないコードおよびデータは消去され、その後ルネサスによる故障解析が可能となります。

3. ALx_KEY / RMA_KEY の作成と注入

本章では、ALx_KEY を生成し、MCU に注入する手順を説明します。RMA_KEY の生成と注入も同様の手順を使用します。

3.1 ALx_KEY 注入プロセスで使用するツール

ALx_KEY の作成と注入のプロセスでは、3 つのツールを使用します。

- Gpg4win - このツールは、開発者とルネサス Key Wrap サービスとの間に安全な通信チャネルを確立するために使用される PGP 鍵を生成および使用する際に使用します。ここでは Gpg4win をデモンストレーションに使用していますが、任意の PGP 管理ツールを使用できます。
- SKMT - このツールは、ALx_KEY 注入に必要な各種鍵ファイルを生成します。
- RFP - このツールは、ALx_KEY の注入に使用します。

3.2 ALx_KEY 注入の概要

ALx_KEY を MCU に注入するには、大きく 3 つの手順が必要です。

1. 任意の 256 ビットの User Factory Programming Key(UFPK)を作成します。UFPK は ALx_KEY を暗号化するために使用され、注入プロセス中に平文鍵が露出しないようにします。
2. ラップされた UFPK(W-UFPK)を取得します。W-UFPK を取得するには、ルネサス Key Wrap サービスで UFPK をラッピングする必要があります。

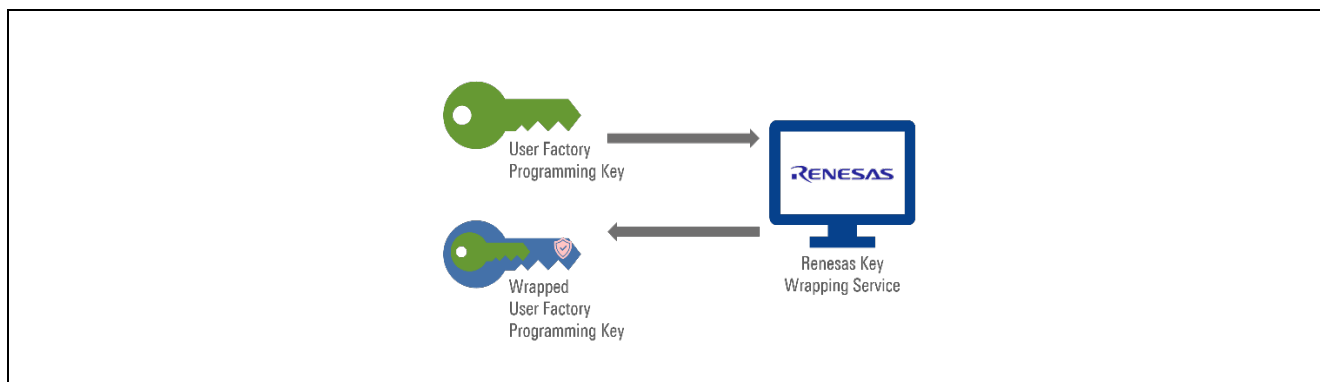


図 3-1 UFPK をラップ

3. UFPK を使用して ALx_KEY をラップします。

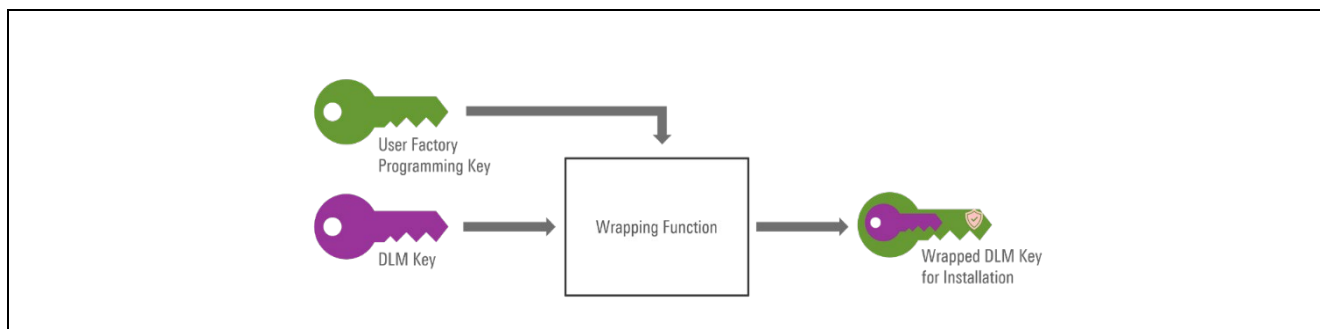


図 3-2 UFPK を使用して ALx_KEY をラップする

4. W-UFPK とラップされた ALx_KEY を、シリアルプログラミングインタフェースを使用して MCU に送信し、ALx_KEY を注入します。

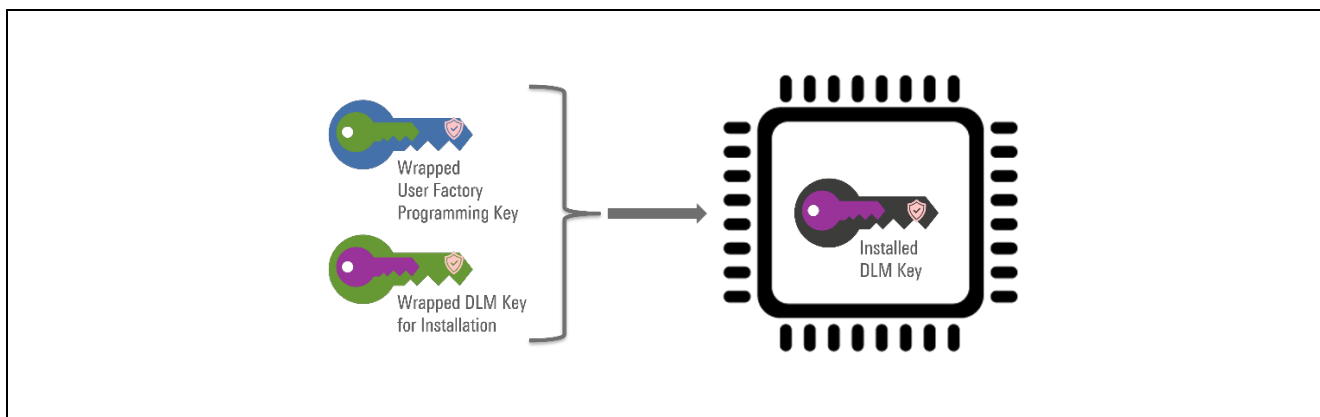


図 3-3 ラップされた ALx_KEY を作成

3.3 ルネサス Key Wrap サービスとの PGP 暗号化通信の確立

ラップされた UFPK を取得するために、UFPK を PGP 暗号化してルネサス Key Wrap サービスに送る必要があります。これには公開鍵の交換が必要です。これは一度だけ実施する処理です。

3.3.1 ルネサス Key Wrap サービスの概要

ウェブブラウザを使用して、ルネサス Key Wrap サービスにアクセスする URL <https://dlm.renesas.com/keywrap/> を入力します。

Key Wrap サービス操作マニュアルは、画面右側の [FAQ](#) リンクからアクセスできます。Key Wrap サービス操作マニュアルへのリンクは、図 3-4 に示すように、FAQ の質問「Is there a manual of this system?」の回答にあります。

図 3-4 ルネサス Key Wrap サービスの FAQ と Key Wrap サービス操作マニュアル

ユーザとルネサス Key Wrap サービス間で通信される情報は、OpenPGP によって暗号化される必要があります。図 3-5 は、転送中の UFPK を保護するためのセキュリティ対策として OpenPGP 暗号化を使用したルネサス Key Wrap サービスの運用フローの概要を示しています。

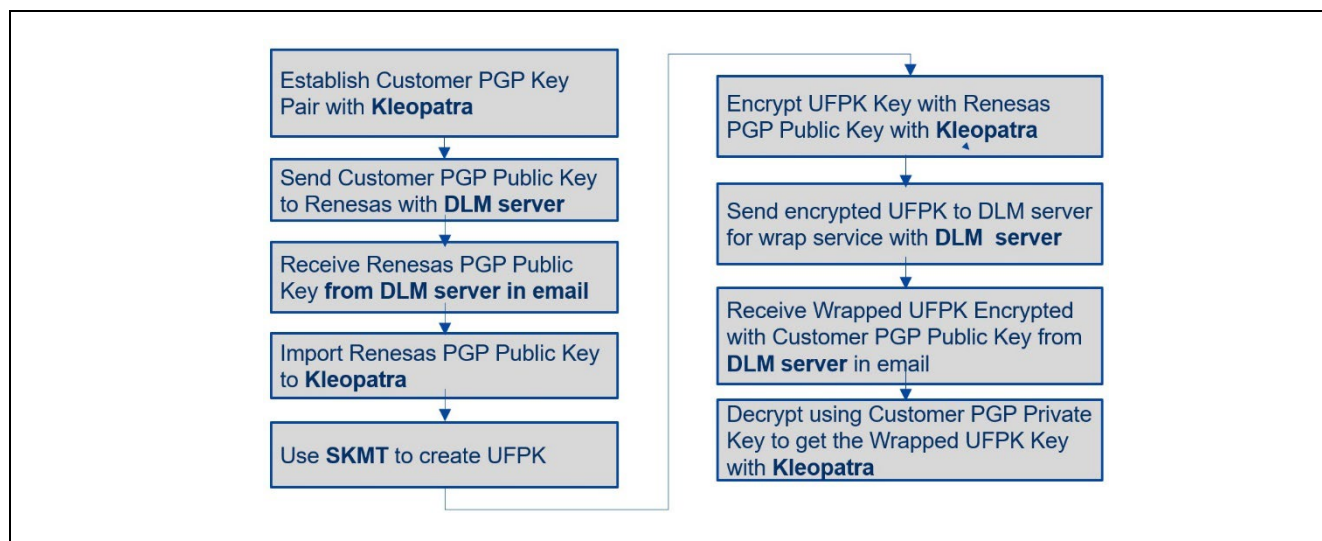


図 3-5 PGP を使用したルネサス Key Wrap サービスの概要

3.3.2 PGP 鍵ペアの作成

すでに PGP 鍵ペアがある場合は、この手順をスキップできます。それ以外の場合は、次の手順を使用して OpenPGP 鍵ペアを作成します。

本アプリケーションノートでは、Windows®用の公式 GnuPG ディストリビューションである Gpg4win を PGP 鍵生成、暗号化、および復号サービスに使用しています。生成された秘密鍵は、安全に管理し、漏えいしないように注意してください。

Gpg4win は、次の URL <https://www.gpg4win.org> からダウンロードできます。

Kleopatra は、Gpg4win で提供される証明書マネージャおよび統合暗号 GUI です。本アプリケーションノートに含まれるスクリーンショットは、Gpg4win-4.0.0 に基づいています。新しいバージョンでは、グラフィックインターフェースが若干更新される可能性があります。但し、本アプリケーションノートで使用する機能は保持される必要があります。

Kleopatra を起動します。**ファイル > 新しい OpenPGP 鍵ペアを作成** の順にクリックします。



図 3-6 PGP 鍵ペアの生成

表示されているように詳細を入力します。生成する鍵はパスフレーズで保護されます。をチェックします。



図 3-7 PGP 鍵ペアを作成するための資格情報入力

高度なオプションをクリックし、rsa3072 を選択します。OK をクリックします。

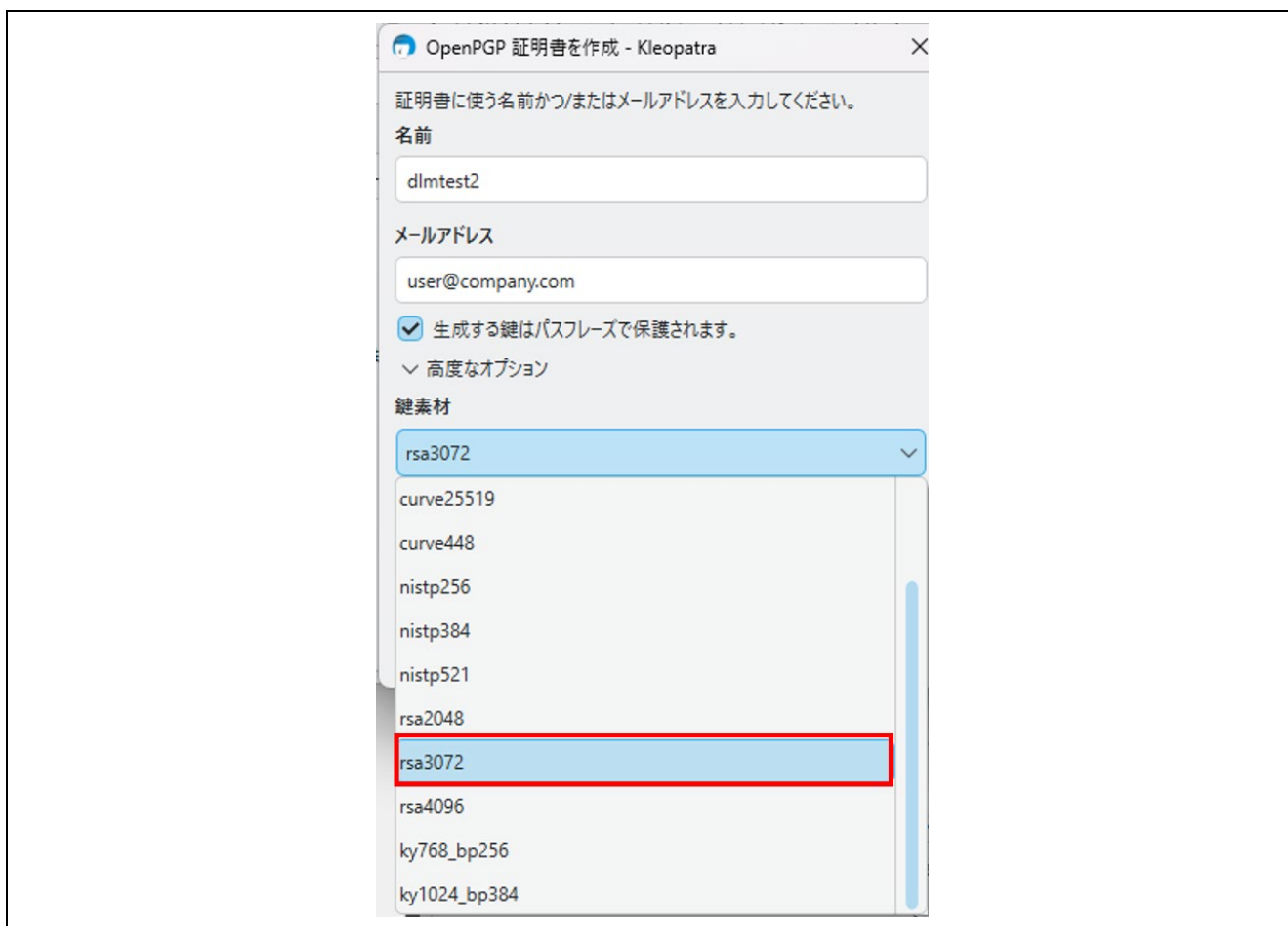


図 3-8 PGP 鍵ペアの詳細設定

秘密鍵を保護するためのパスフレーズを指定します。以降の処理において、秘密鍵を使用する際にパスフレーズの入力が必要となるため、**パスフレーズは必ず保存してください。**

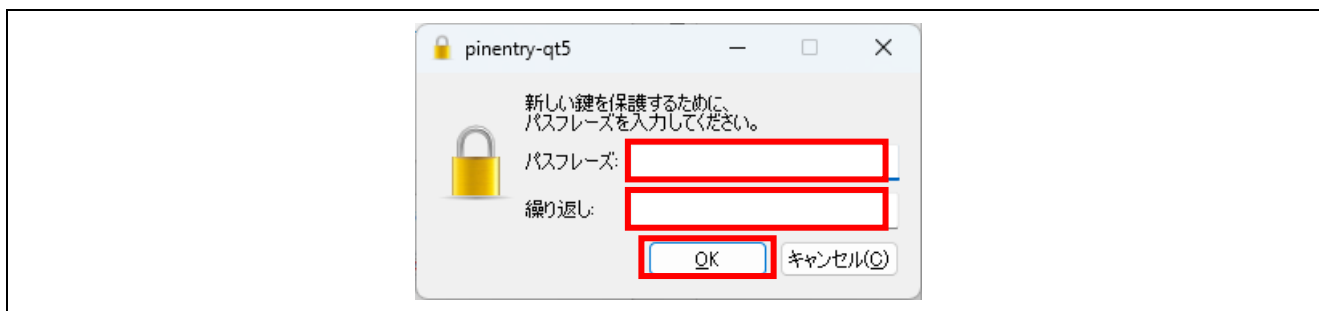


図 3-9 パスフレーズの指定

PGP 鍵ペアが正常に作成されたことを確認します。

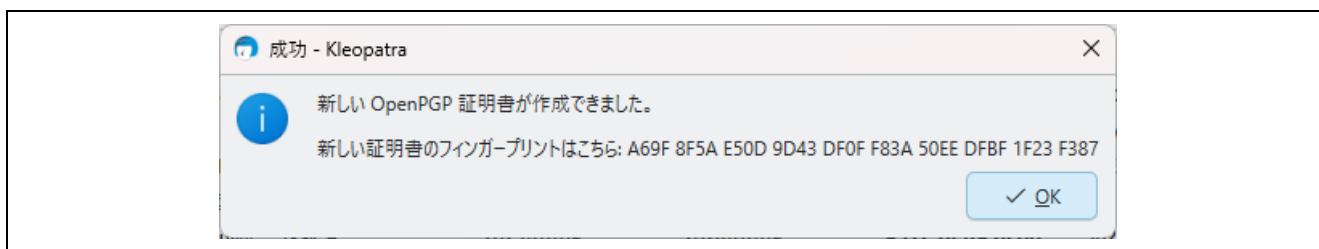


図 3-10 鍵ペア作成成功

公開鍵をエクスポートするには、次に示すように、作成した名前を右クリックし、**エクスポート**を選択します。

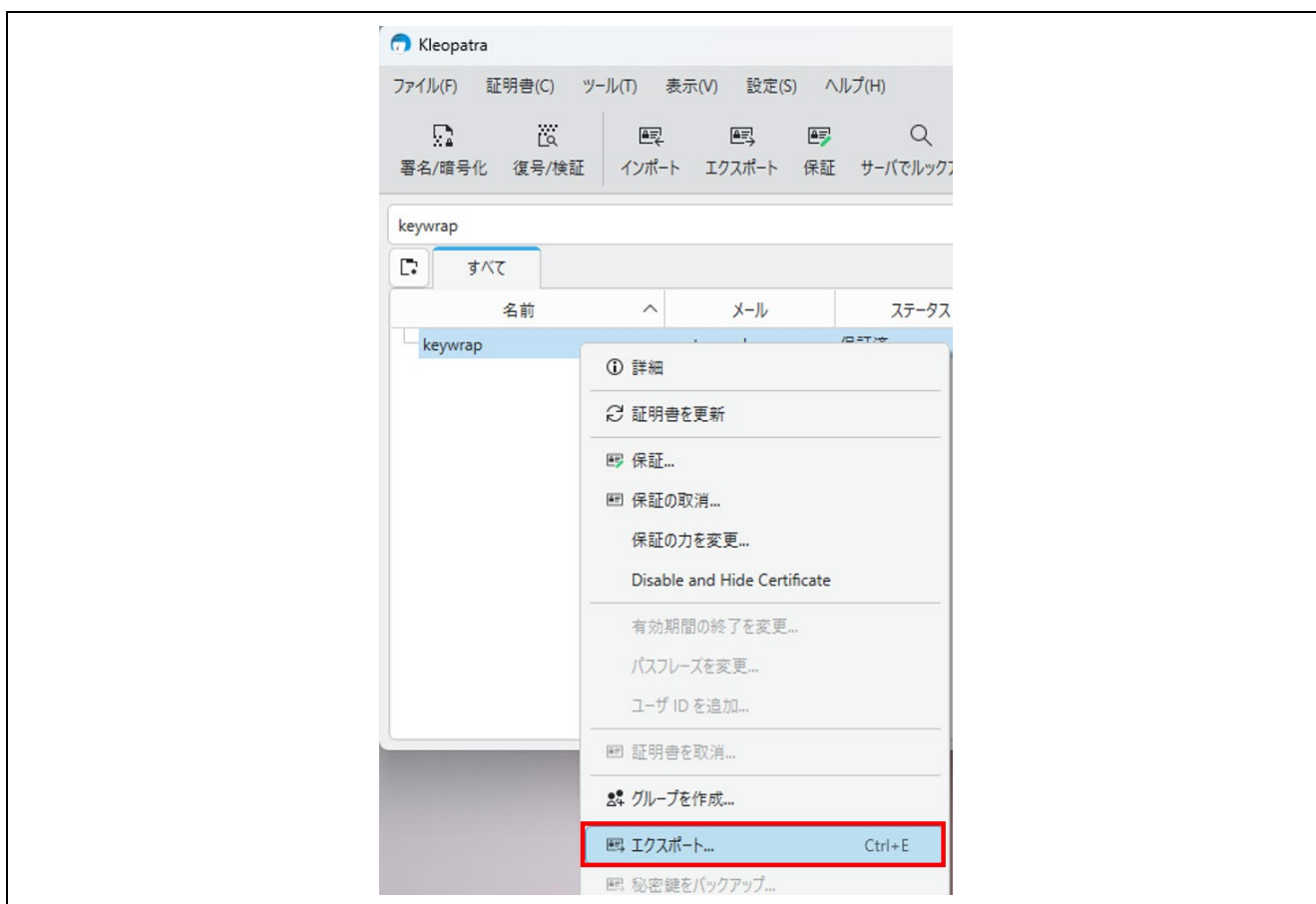


図 3-11 公開鍵のエクスポート

公開鍵を public_key.asc など拡張子が*.asc のファイルに保存します。

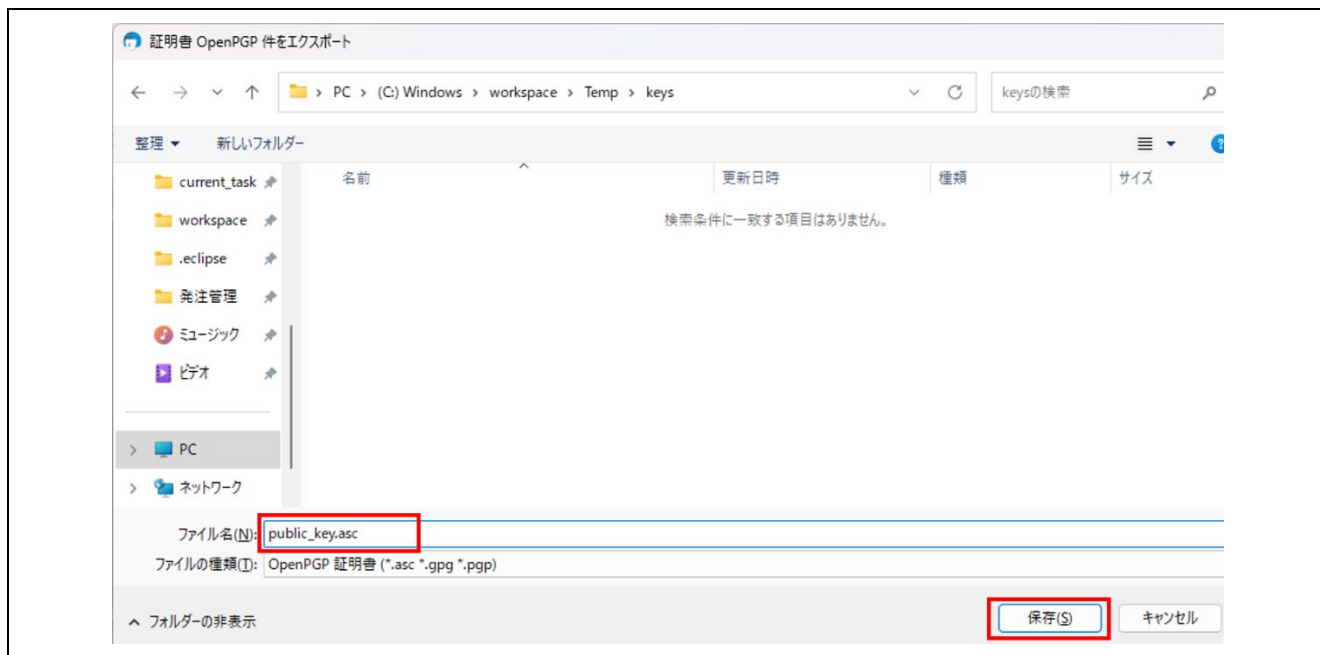


図 3-12 公開鍵の保存

3.3.3 ルネサス Key Wrap サービスへの登録

本項では、ルネサス Key Wrap サービスの登録手順について概要を示します。これは、新規ユーザ向けの一度だけ実施する処理です。また、Key Wrap サービス操作マニュアルの「New registration」章で、新規登録手順の詳細を確認することもできます。

ウェブブラウザで URL <https://dlm.renesas.com/keywrap/> を開き、**新規登録**をクリックします。プロンプトに従ってメールアドレスを入力し、**メール送付**をクリックします。

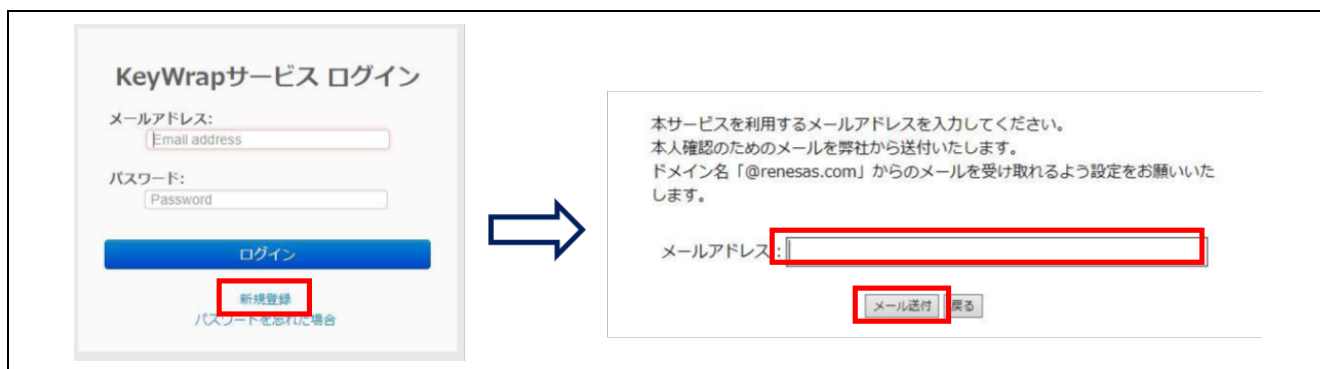


図 3-13 新規登録用電子メールアドレスの入力

図 3-14 に示すように、登録リンクが電子メールで送信されます。

お客様各位

KeyWrapサービスに登録していただき、ありがとうございます。
本サービスをご利用になるためには下記のURLをクリックして
お客様の情報を登録していただく必要がございます。

<http://dlm.renesas.com/keywrap/?menu=reg%2Fregist%2Ffixed%2F¶m=id%3D49iqnhs%2FyrsD>

■注意事項
お客様情報の登録は本メール受信後3時間以内に行ってください。
3時間を超えますと、新規登録処理から行っていただく必要がございます。

このメールに心あたりがない場合、当メールを破棄していただきますようお願いいたします。

※このメールは送信専用メールアドレスからお送りしています。
返信いただいても回答できませんので、ご了承ください。
※パスワードをお忘れの場合、本サイトのログインページにある
「パスワードを忘れた場合」からパスワードをリセットしてください。

以上、よろしくお願いいたします。

ルネサスエレクトロニクス株式会社

図 3-14 登録リンクが記載されたメール

確認メールに記載されている URL をクリックし、必要な情報を入力します。**次へ (確認)**ボタンをクリックします。確認画面が表示されたら、**登録**ボタンをクリックしてユーザ登録を完了します。

お客様情報の登録を行います。以下の項目を全て入力してください。
パスワードは8文字以上32文字以下の半角英数と半角記号「!@」で指定してください。

メールアドレス:

氏名:

会社名:

パスワード:

パスワード再入力:

図 3-15 お客様情報登録

3.3.4 PGP 公開鍵交換

登録が完了すると、以下の画面が開きます。**サービス開始**ボタンをクリックして、鍵暗号化システムの使用を開始します。

登録しました。

メールアドレス:

氏名:

会社名:

図 3-16 ルネサス Key Wrap サービスの使用開始

以下に示すように、利用規約を確認してから**トラステッドセキュア IP Key Wrap サービス利用規約に同意します** をクリックして、**トラステッドセキュア IP Key Wrap サービス利用規約**を受諾します。この規約は、ルネサス Key Wrap サービスにログインするたびに表示されます。

重要-以下の利用規約を注意してお読みください。

以下のトラステッドセキュアIP Key Wrapサービス利用規約（以下「本利用規約」といいます。）は、お客様およびお客様が所属する企業等の団体を代表して当社とのトラステッドセキュアIP Key Wrapサービス利用契約（以下「本契約」といいます。）を締結する場合のお客様が所属する企業等の団体（以下総称して「お客様および所属企業等」といいます。）がトラステッドセキュアIP鍵暗号化に係るサービス（以下「本サービス」といいます。）を利用する際に適用される条件を定めたものです。慎重に内容をお読みください。お客様および所属企業等は、本利用規約に定める条件に従って、本サービスを利用しなければなりません。本利用規約の内容に同意できない場合は、本サービスを利用しないでください。本サービスを利用した場合、お客様および所属企業等は本契約に同意したものとみなされます。

お客様が「トラステッドセキュアIP Key Wrapサービス利用規約に同意します」ボタンをクリックすることにより、(a)お客様は、お客様が所属する企業等の団体を代表して本契約を締結し、それにより当該団体が本利用規約の定める条件に法的に拘束されることを承諾の上、本契約を締結する意思表示を行ったこととなり、仮に、お客様がこのような団体に属さない場合には、お客様がご自身のために本契約を締結し、それによりお客様が本利用規約の定める条件に法的に拘束されることを承諾の上、本契約を締結する意思表示を行ったこととなります。また、これにより、(b) お客様は当該団体（所属する場合）を代表しまたはお客様自身のために行動し、当該団体または自身を拘束する権利、権能および権限を有することを表明しかつ保証したことになります。

本契約は、お客様が「トラステッドセキュアIP Key Wrapサービス利用規約に同意します」ボタンをクリックすることにより、お客様と当社の間で有効に成立します。

図 3-17 ルネサス Key Wrap サービス利用規約に同意する

ユーザとルネサス Key Wrap サービス間の通信では、PGP を使用して転送される全てのデータが暗号化されます。これらの転送を有効にするには、PGP 公開鍵を交換する必要があります。

PGP 鍵を交換せずにルネサス Key Wrap サービスにデータを転送しようとすると、次のエラーメッセージが表示されます。

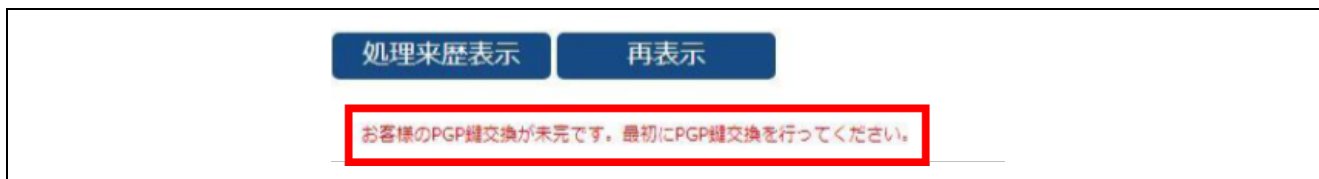


図 3-18 PGP 鍵交換のリクエスト

PGP 鍵を交換するには、**PGP 鍵交換**ボタンをクリックします。図 3-19 に示すダイアログが開きます。**参照**をクリックし、前に作成してエクスポートした公開鍵を選択します(3.3.2、図 3-12)。

次に、**PGP 鍵交換**をクリックし、登録時に指定したメールアドレスにルネサス PGP 公開鍵が届くのを待ちます。

戻る ログアウト

お客様のPGP公開鍵をエクスポート形式にしたものを選択後、“PGP鍵交換ボタン”を押してください。

お客様のPGP公開鍵がルネサスに送られ、ルネサスのPGP公開鍵がお客様のメールアドレスに送信されます。

参照 PGP鍵交換

ルネサスPGP公開鍵のFingerprintは以下のとおりです。

FB18 EB66 1F61 20E9 9613
8DF7 F517 189C 1EA5 E55D

図 3-19 ルネサス Key Wrap サービスへの PGP 公開鍵の提供

図 3-20 に示すような内容(ルネサス PGP 公開鍵を含む)が記載されたメールが届きます。受信したルネサス PGP 公開鍵(keywrap-pub.key)を保存します。この鍵のフィンガープリントは、図 3-19 に示すように、PGP 鍵交換ダイアログで表示されることに注意してください。

PGP 鍵は何度でも交換できます。鍵が複数回交換された場合、以前の全ての PGP 鍵は破棄され、ルネサス Key Wrap サービスは、正常に交換された最新の PGP 公開鍵を使用して、転送されたデータを暗号化します。

ルネサス 太郎 様

KeyWrapサービスをご利用いただき、ありがとうございます。
登録いただいたPGP公開鍵のインポート処理を行いました。
弊社PGP公開鍵を添付ファイルにて送信いたします。
暗号化処理のご依頼は添付のルネサスPGP公開鍵を使用して暗号化処理後、
Webから送信してください。

このメールに心あたりがない場合、当メールを破棄していただきますようお願いいたします。

※このメールは送信専用メールアドレスからお送りしています。
返信いただいても回答できませんので、ご了承ください。

以上、よろしくお願いいたします。

ルネサスエレクトロニクス株式会社

添付ファイル:

[keywrap-pub.key](#) 2.3 k [application/octet-stream]

図 3-20 ルネサス PGP 公開鍵の受信

3.3.5 ルネサスの PGP 公開鍵を Kleopatra にインポート

Kleopatra アプリケーションに戻り、図 3-21 に示すように、ルネサス PGP 公開鍵を Kleopatra にインポートします。

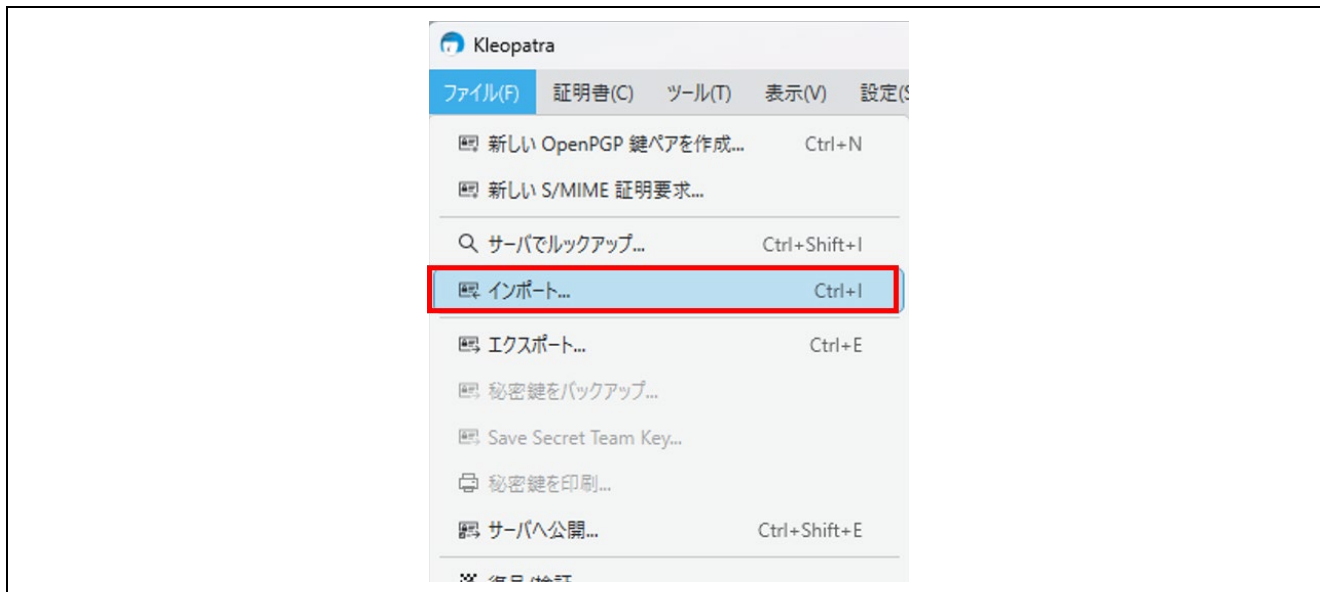


図 3-21 ルネサス公開鍵を Kleopatra にインポート

ファイル > インポートをクリックし、ルネサス Key Wrap サービスから受信した keywrap-pub.key ファイルを選択します。

Kleopatra のインポートされた証明書に次の項目が表示され、ルネサス公開鍵を使用する準備が整いました。

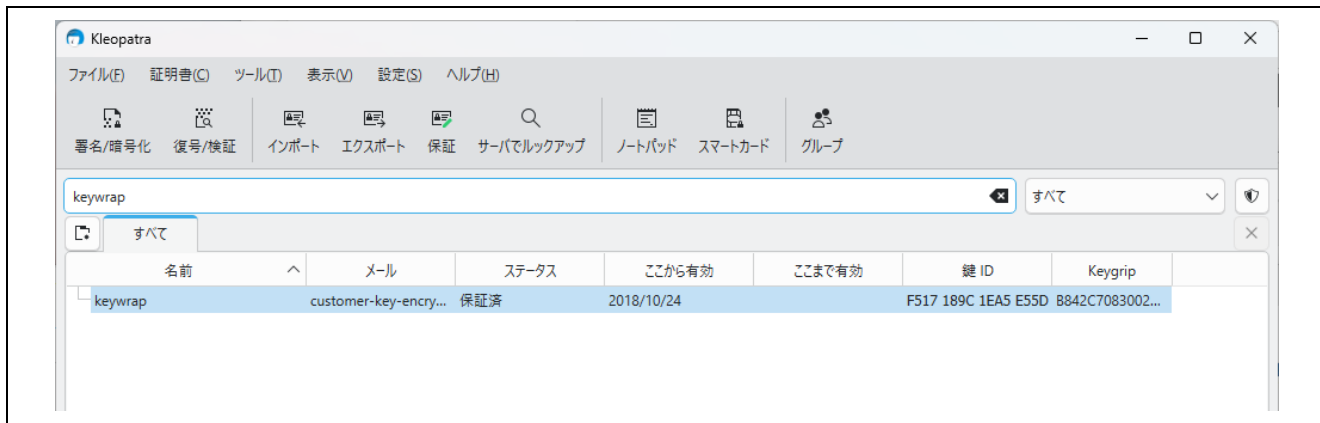


図 3-22 ルネサス PGP 公開鍵

3.4 UFPK と W-UFPK の作成

本節では、UFPK 作成と W-UFPK 取得のプロセスについて説明します。

3.4.1 SKMT の紹介

SKMT は、ALx_KEY 注入プロセス中に各種機能を実行します。SKMT は、次のリンクから入手できます。

<https://www.renesas.com/ja/software-tool/security-key-management-tool>

Downloads 欄のリンクから、最新の SKMT インストーラをダウンロードして、動作環境の必要に応じてインストールします。このツールは、Windows、Linux および macOS をサポートしています。

このツールのユーザーズマニュアルは、\doc フォルダにあります。事前にユーザーズマニュアルを参照してください。

SKMT は、Command Line Interface(CLI)と Graphic User Interface(GUI)の 2 つのインタフェースをユーザーに提供します。GUI は、主に開発での使用を目的としています。CLI は、主要なファイル生成スクリプトを作成できるため、主に実稼働サポートまたは複数の鍵を含む開発作業を目的としています。本アプリケーションノートでは、主に GUI ツールを使用して機能を示します。SKMT ユーザーズマニュアルには、お客様が参照できるように CLI の広範な使用例が記載されています。

3.4.2 UFPK ファイルの作成

SKMT は、GUI モードまたは CLI モードのいずれかで使用して、UFPK ファイルを作成できます。この例では、GUI を使用します。

Security Key Management Tool の実行ファイルを起動します。

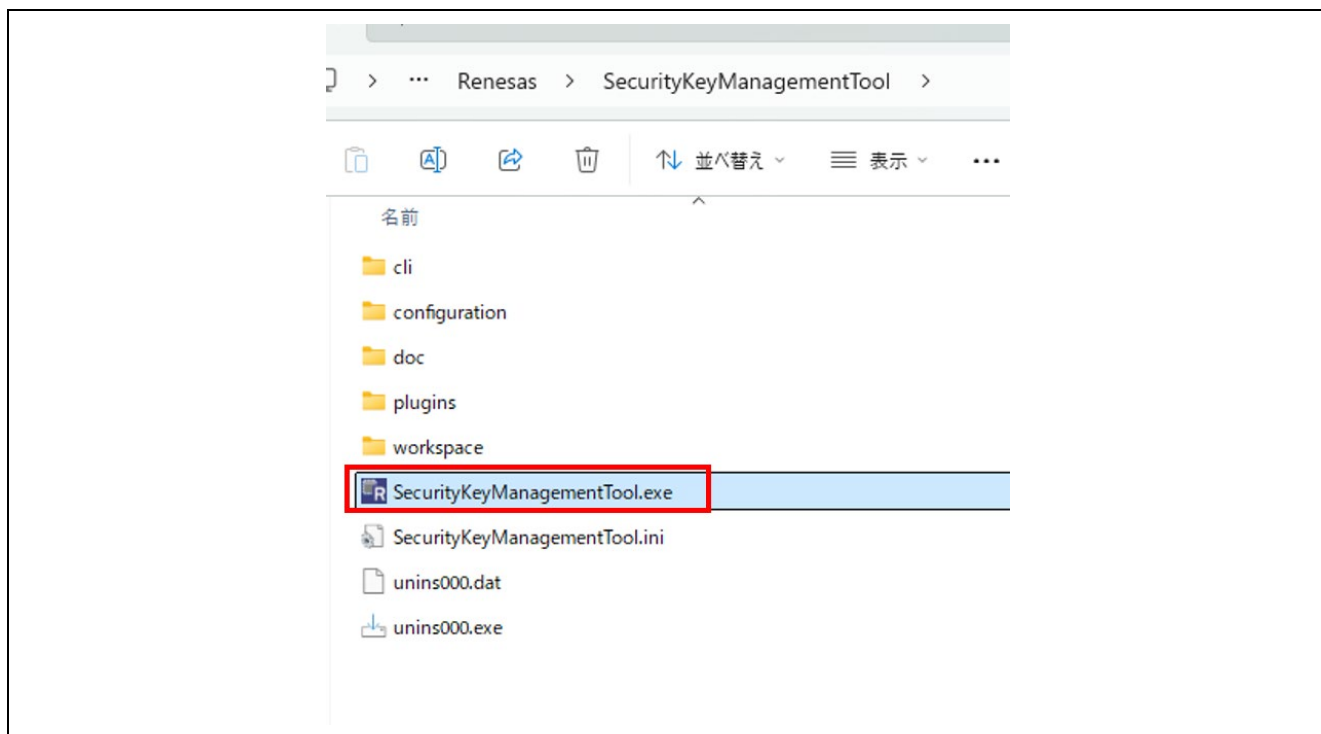


図 3-23 SKMT GUI の起動

概要タブで、MCU/MPU と暗号エンジンを RX Family, RSIP-E50D Security Functions and Protected Mode として選択します。



図 3-24 RX Family, RSIP-E50D Security Functions and Protected Mode を選択

次に、**UFPK 生成**タブをクリックします。

図 3-25 と図 3-26 に示すように、UFPK に必要な値を指定することも、ツールでランダムな値を作成することもできます。図 3-25 は、**乱数生成機能を使用する** を選択してランダム値をツールで生成することを示しています。図 3-26 は、**指定値を使用する** を選択し、32 バイトの鍵値をビッグエンディアン形式で入力して、特定の値を指定する方法を示しています。

参照ボタンをクリックして、生成鍵ファイルのファイル名を入力します。ここでは、ufpk.key としています。

最後に、**UFPK を生成する**ボタンをクリックして、鍵ファイル ufpk.key を生成します。

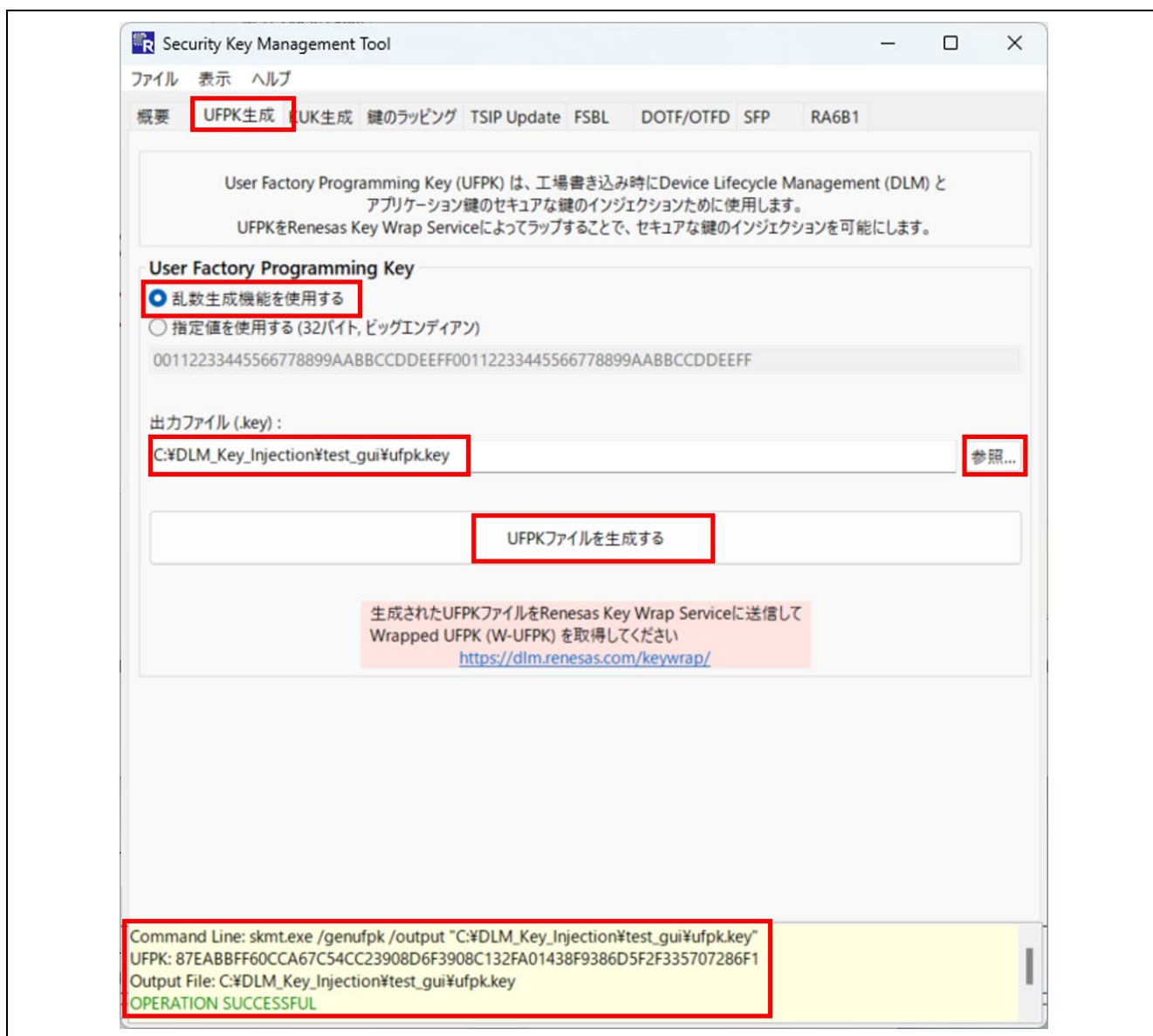


図 3-25 GUI を使用したランダム UFPK の生成

図 3-26 では、次の 32 バイト鍵を使用します。

000102030405060708090a0b0c0d0e0f000102030405060708090a0b0c0d0e0f

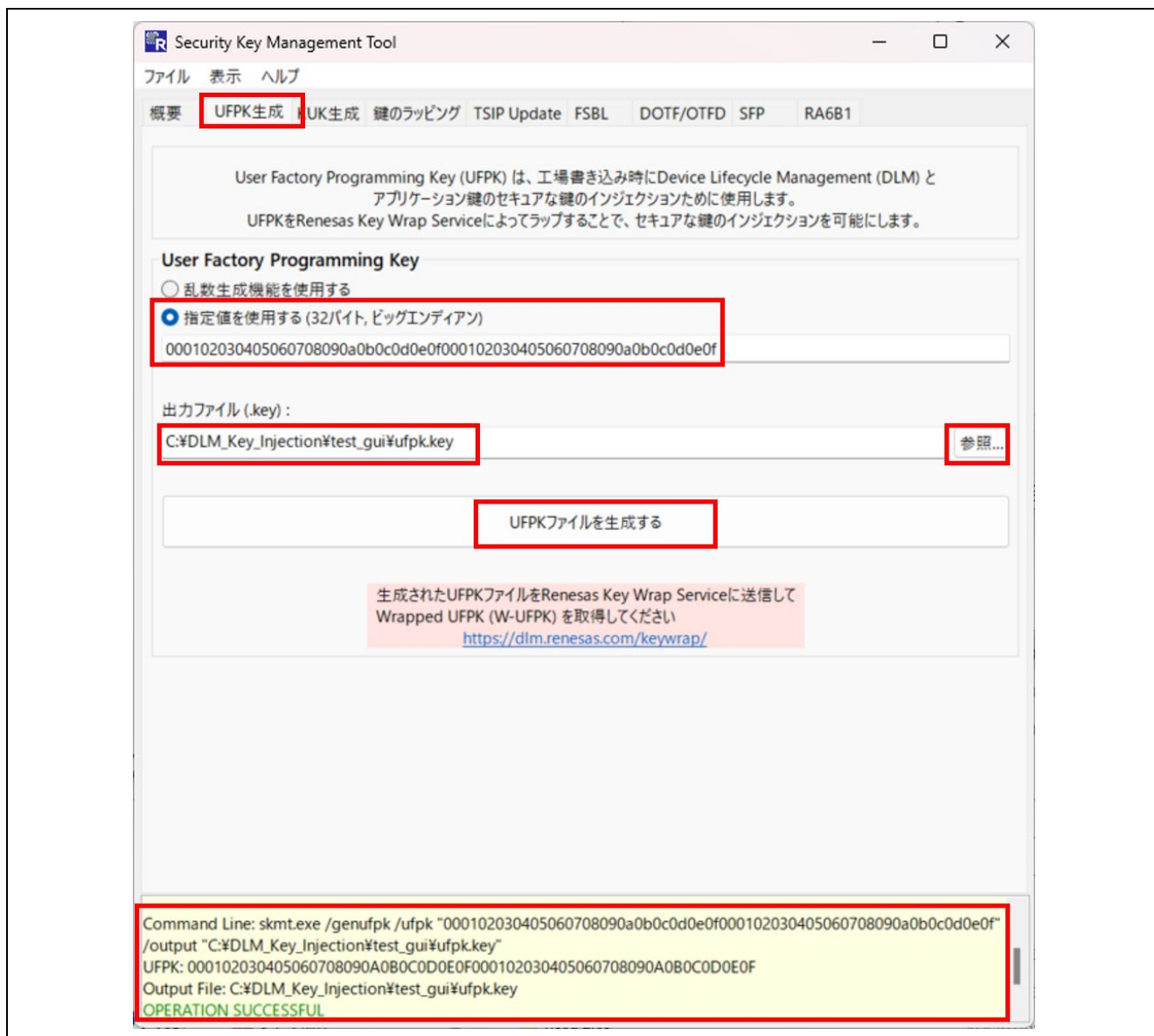


図 3-26 GUI を使用した固定 UFPK の作成

3.4.3 ルネサス PGP 公開鍵による UFPK の暗号化

Kleopatra から署名/暗号化を選択し、ルネサス PGP 公開鍵で `ufpk.key` ファイルを暗号化します。

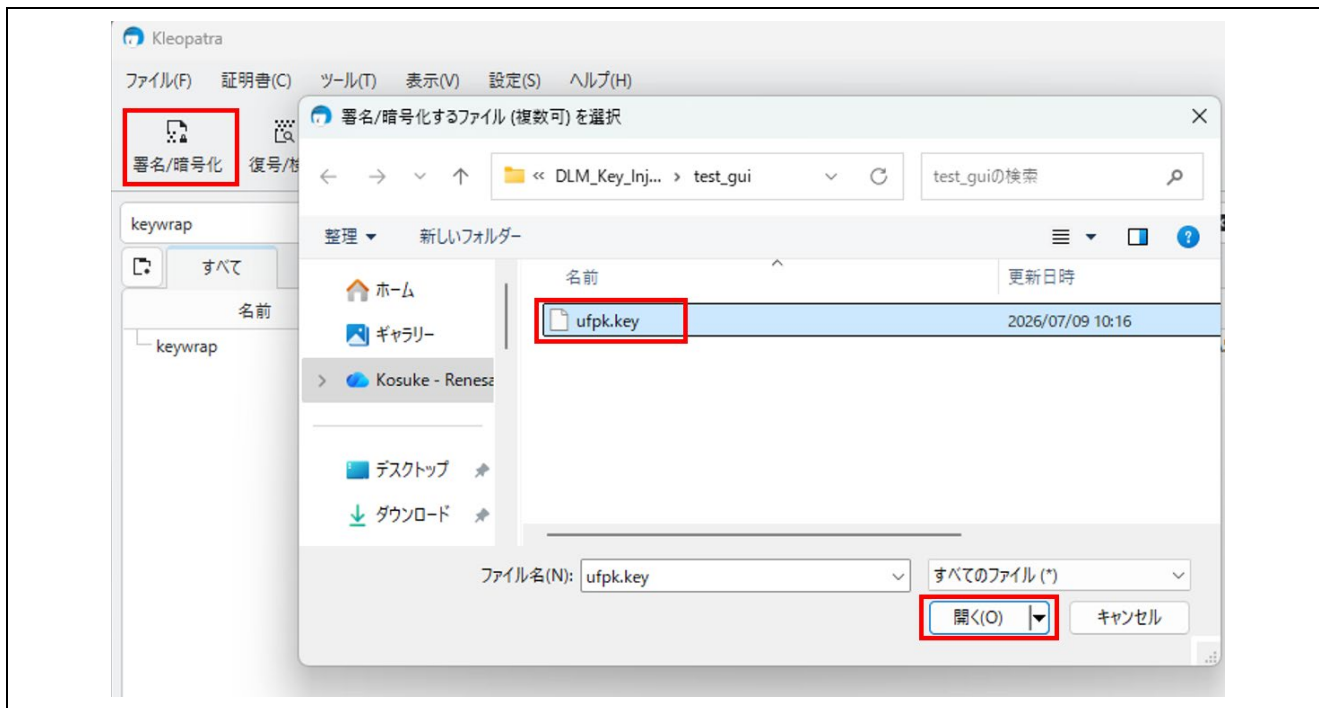


図 3-27 暗号化する UFPK を選択

他の方のために暗号化 を選択し、ルネサス PGP 公開鍵を選択します。**Sign/Encrypt** をクリックします。

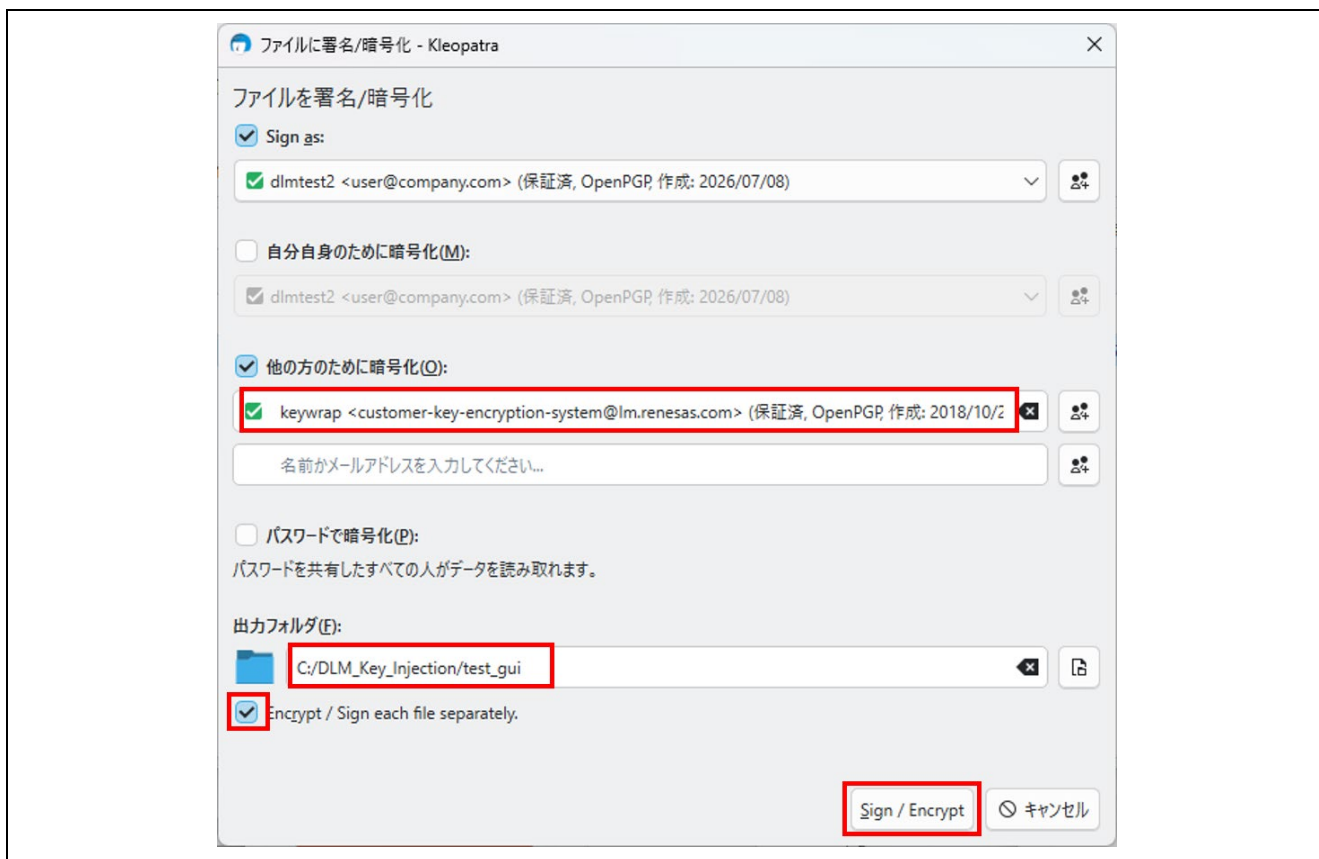


図 3-28 ルネサス公開鍵を使用して UFPK を暗号化

また、自分自身のために暗号化を選択して、暗号化したバージョンの UFPK ファイルをアーカイブすることもできます。これを行わない場合、データを復号できないという Encrypt-To-Self 警告が表示されます。続行を押します。

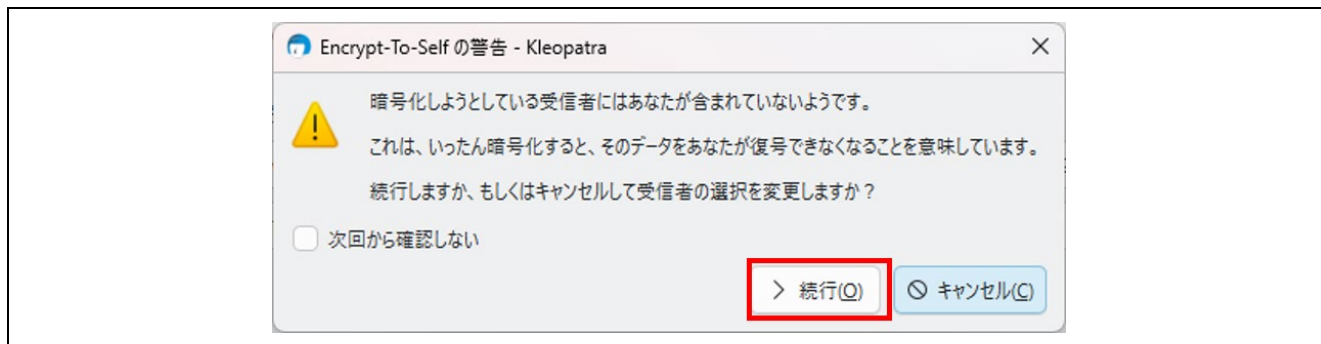


図 3-29 暗号化オプションの確認

ルネサス公開鍵で暗号化された UFPK は、選択したフォルダに .gpg を拡張子として生成します。この例では、ufpk.key.gpg が生成されます。終了をクリックします。



図 3-30 ルネサス公開鍵による UFPK の暗号化

3.4.4 UFPK をルネサス Key Wrap サービスに送信

これで、暗号化された UFPK をルネサス Key Wrap サービスに送信でき、ルネサスの秘密鍵によって復号され、W-UFPK の生成に使用されます。

ルネサス Key Wrap サービスのユーザインタフェースから RX ファミリシリーズを選択し、以下に示すように **RX74M Wrap UFPK** を選択します。

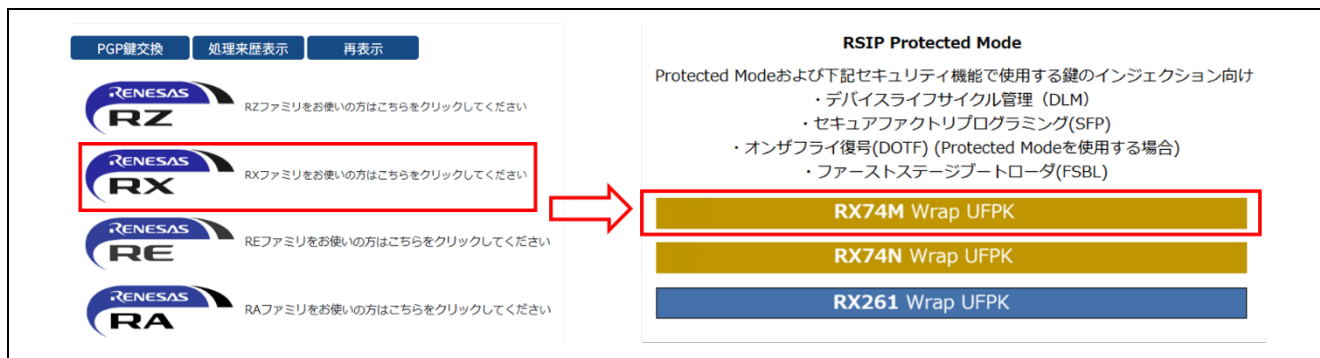


図 3-31 RX デバイス RSIP Protected Mode を選択

次の画面で、**製品用暗号化サービス**を選択します。

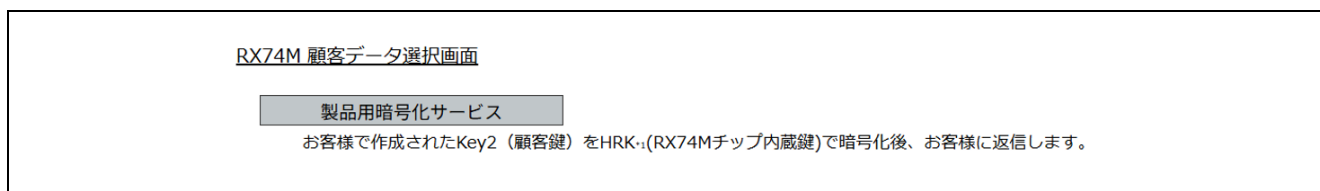


図 3-32 製品用暗号化サービスを選択

次に、**参照**をクリックし、図 3-30 から生成された .pgp ファイルを選択します。

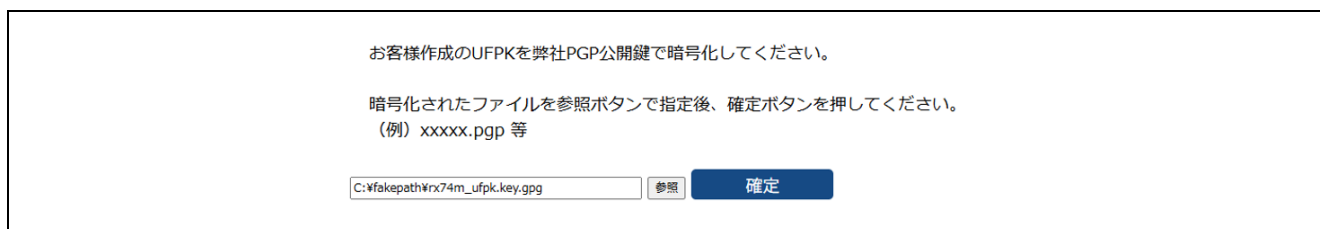


図 3-33 暗号化された UFPK をルネサス Key Wrap サービスに送信

確定をクリックします。ルネサス Key Wrap サービスには、メッセージが表示され、登録したメールアドレスに W-UFPK が送信されます。

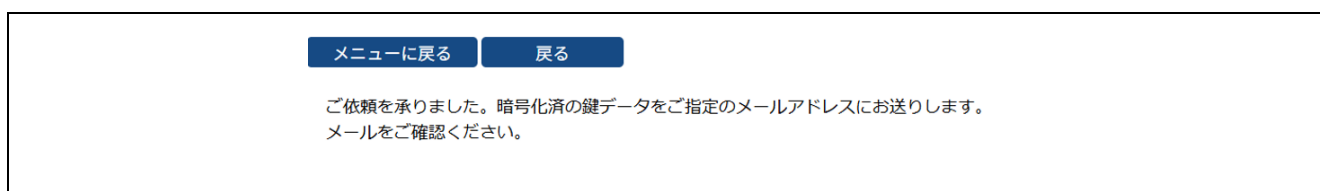


図 3-34 ルネサス Key Wrap サービスからのメッセージ

3.4.5 暗号化された W-UFPK の受信

PGP 公開鍵で暗号化された W-UFPK は、数分以内にメールが届くはずです。

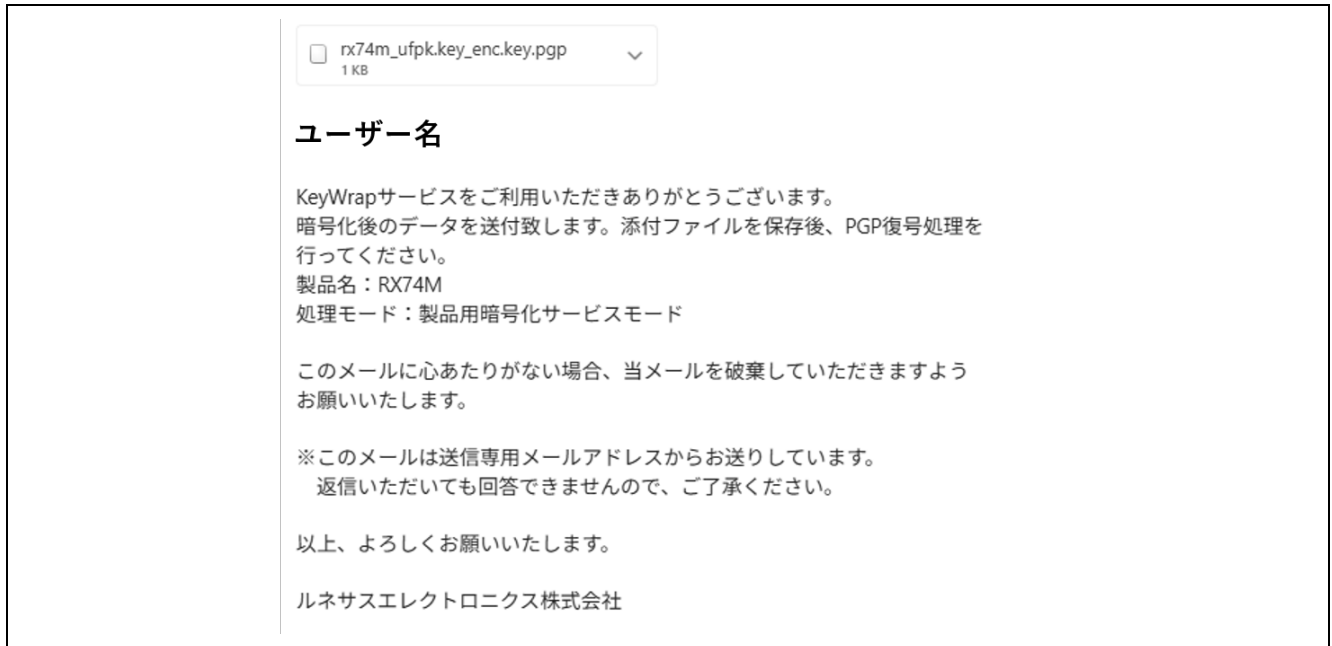


図 3-35 W-UFPK の受信

次の手順で使用するために、このファイルを保存します。

3.4.6 暗号化された W-UFPK の復号

メールから受信した W-UFPK は、公開鍵で暗号化されています。秘密鍵を使用して W-UFPK ファイルを復号する必要があります。

Kleopatra で**復号/検証**をクリックし、暗号化された W-UFPK ファイルを選択します。

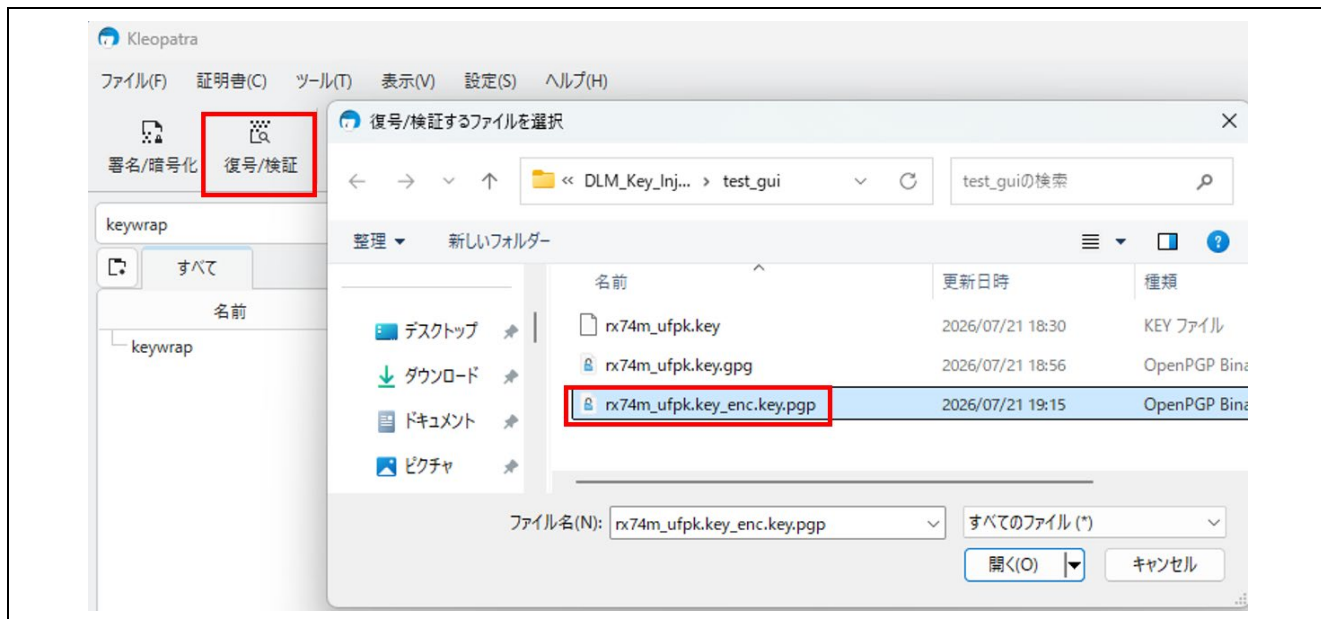


図 3-36 暗号化された W-UFPK ファイル

プロンプトが表示されたら、PGP 鍵のパスフレーズを入力します。復号されたファイルは、指定された場所に保存されます。

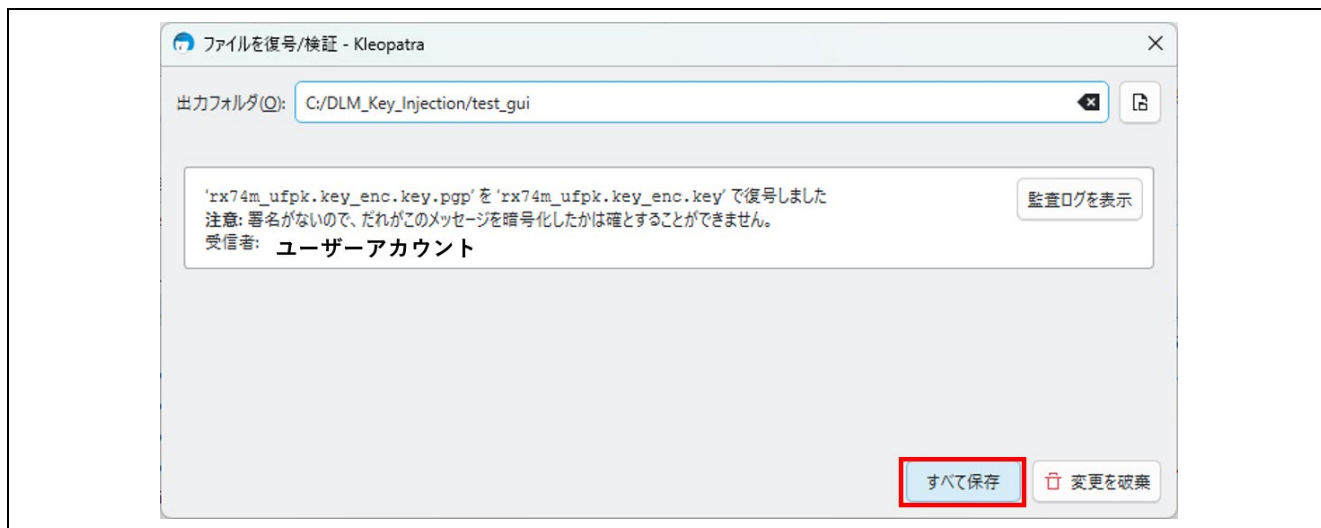


図 3-37 PGP 秘密鍵による復号

3.5 SKMT によるラップされた ALx_KEY の作成

ALx_KEY を注入するには、鍵を UFPK でラップし、ラップされた ALx_KEY と W-UFPK の両方をシリアルプログラミングインタフェース経由で MCU に送信する必要があります。SKMT は、ラップされた ALx_KEY と W-UFPK を含む RFP 鍵注入ファイルを作成できます。

本節では、GUI を使用して AL2_KEY と AL1_KEY の鍵注入ファイルを作成する方法を示します。

3.5.1 AL2_KEY のラップ

SKMT GUI を起動し、**鍵のラッピングタブ**を選択します。次に、**鍵の種類タブ**を開き、**DLM/AL** を選択します。まずは AL2_KEY を注入します。

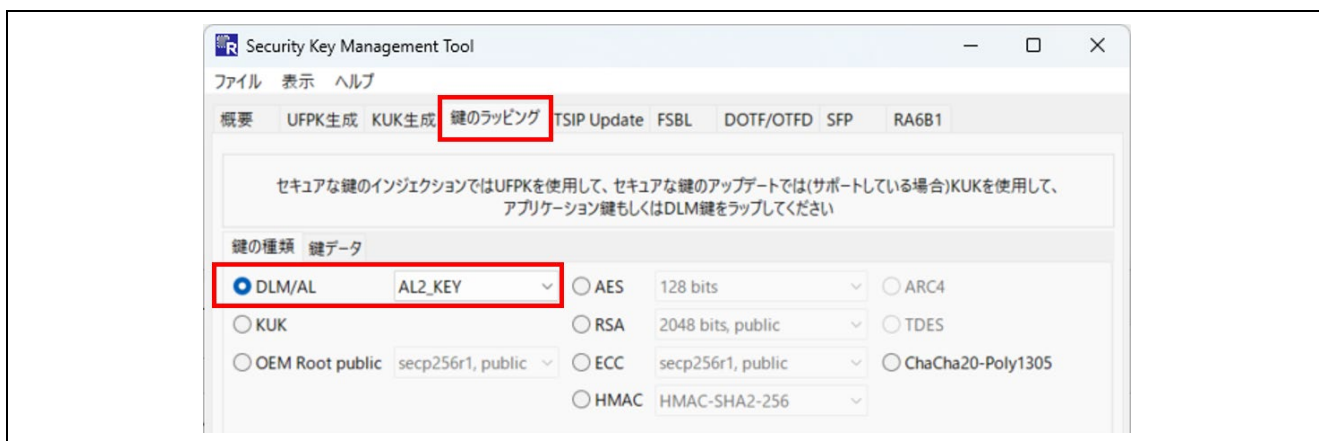


図 3-38 鍵の種類として AL2_KEY を選択

鍵データタブを選択します。この例では、**平文データ**を選択して鍵値(000102030405060708090A0B0C0D0E0F)を入力して、鍵を平文として指定しますが、鍵値を含むバイナリキーファイルを指定することもできます。

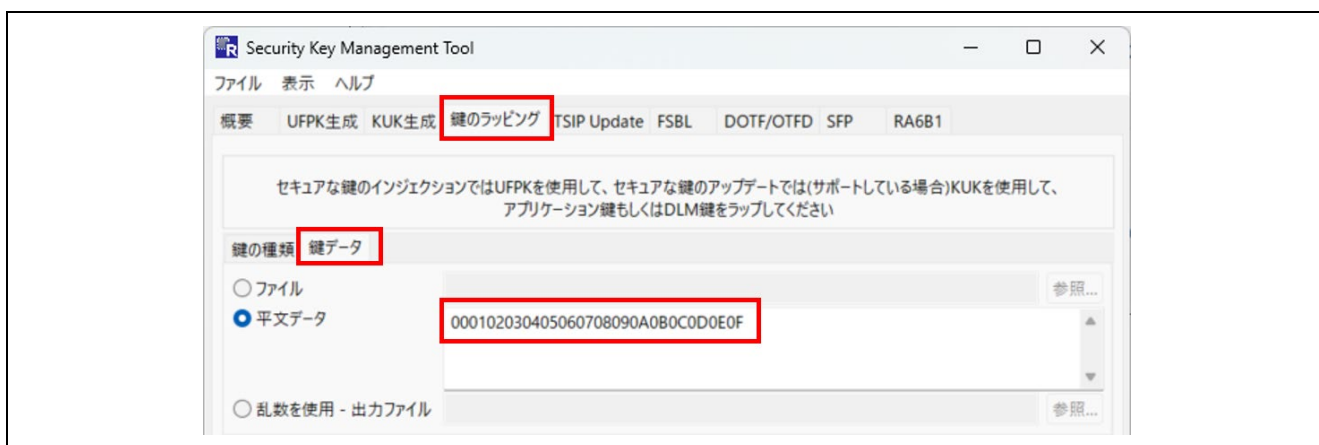


図 3-39 AL2_KEY データを入力

ラッピング鍵セクションで、対応する参照ボタンをクリックして、3.4.2 と 3.4.6 で作成した UFPK と W-UFPK のペアを選択します。IV の乱数生成機能を使用する を選択します。出力セクションで、RFP を選択し、参照ボタンをクリックして出力ファイル名を入力します。

次に、ファイルを生成する ボタンをクリックします。ルネサスキーファイル(AL2_KEY.rkey)が生成されます。

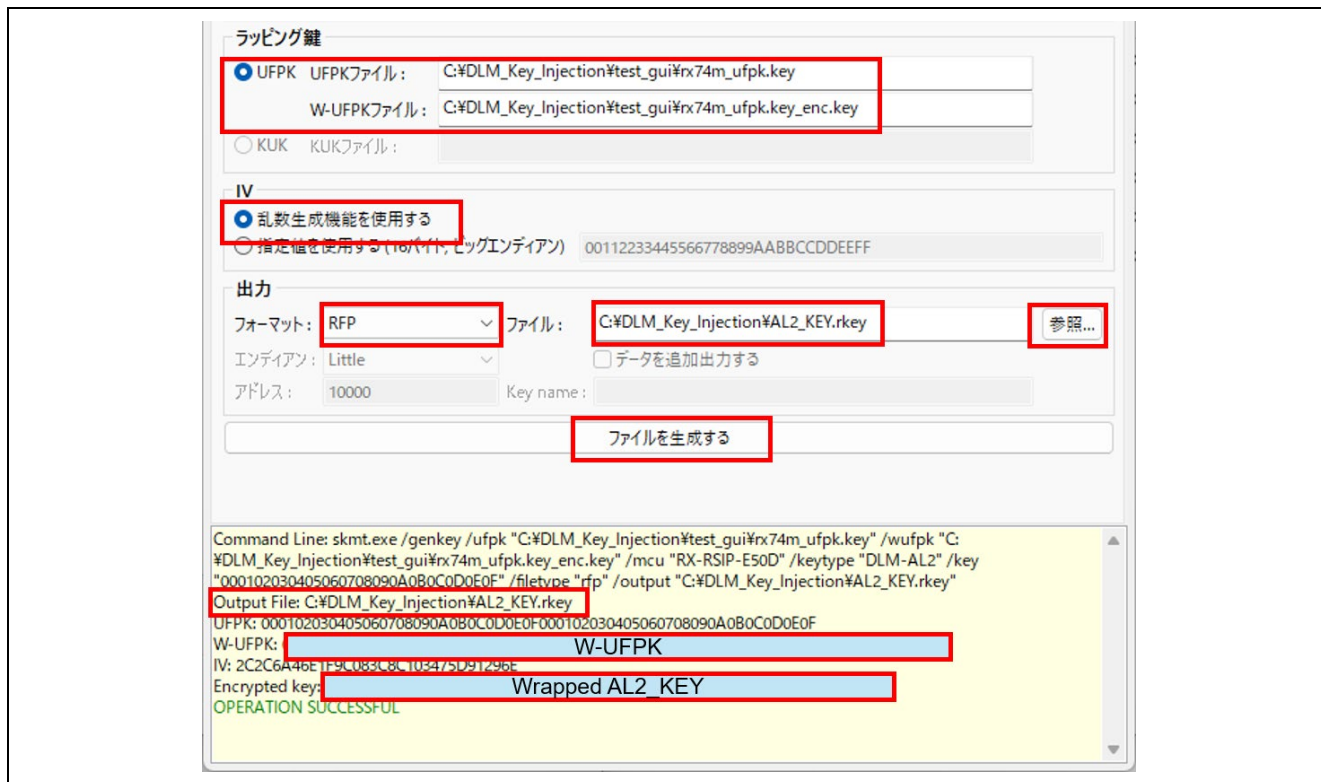


図 3-40 AL2_KEY の RFP 注入ファイルを生成

AL2_KEY は UFPK でラップされます。そして RFP を使用して MCU に AL2_KEY を注入する場合、データに W-UFPK が含まれます。平文の AL2_KEY と UFPK は *.rkey ファイルに含まれていないため、鍵注入時の鍵の機密転送が可能になります。

3.5.2 AL1_KEY のラップ

AL1_KEY のラッピングは、AL2_KEY のラッピングとほぼ同じ手順です。鍵の種類タブで AL1_KEY を選択します。

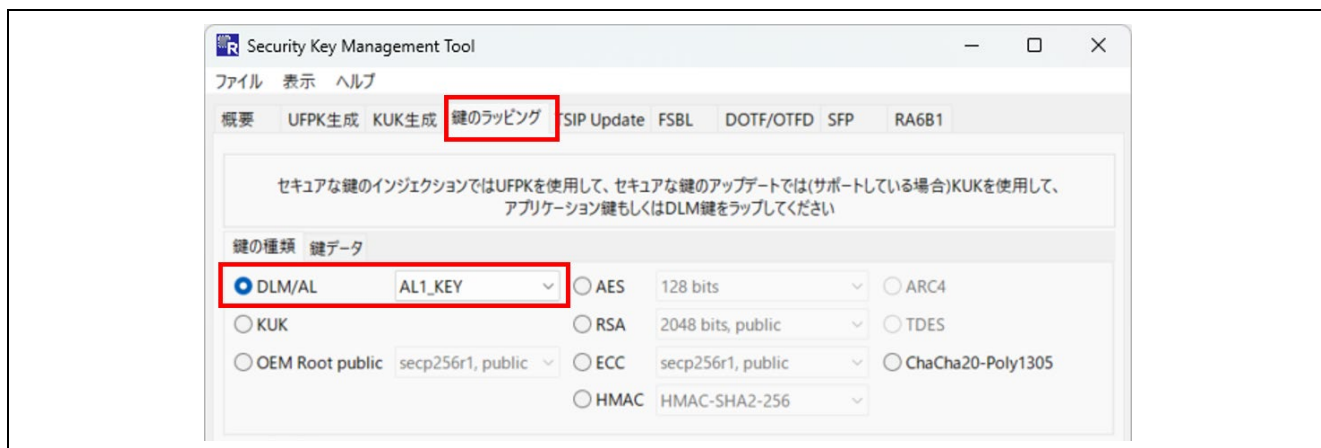


図 3-41 鍵の種類として AL1_KEY を選択

鍵データタブで鍵値のデータを入力します。繰り返しになりますが、この例では、鍵(010102030405060708090A0B0C0D0E0F)を平文として指定します。

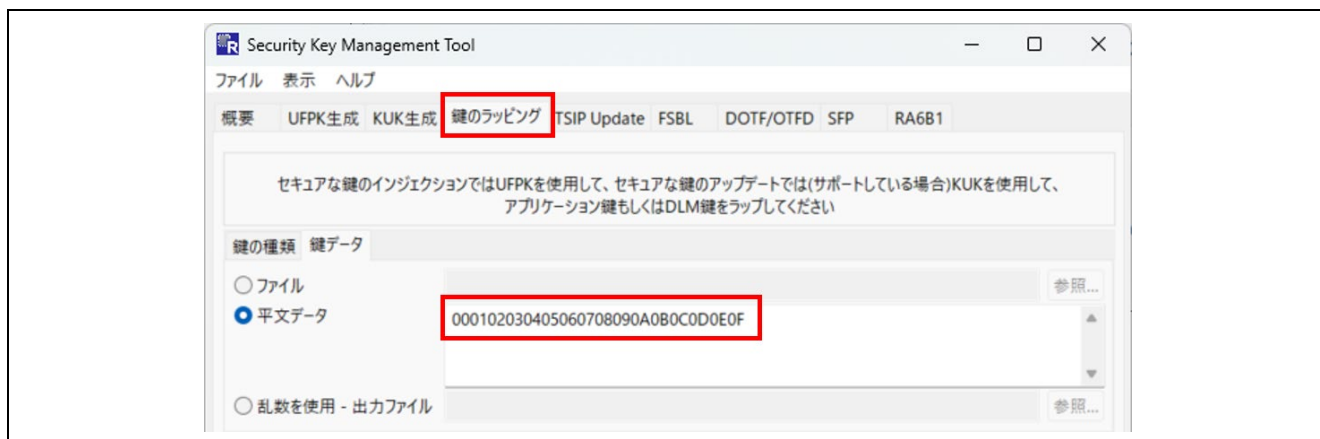


図 3-42 AL1_KEY データを入力

ラッピング鍵セクションで、対応する参照ボタンをクリックして、3.4.2 と 3.4.6 で作成した UFPK と W-UFPK のペアを選択します。IV の乱数生成機能を使用する を選択します。出力セクションで、RFP を選択し、参照ボタンをクリックして出力ファイル名を入力します。

次に、ファイルを生成する ボタンをクリックします。ルネサスキーファイル(AL1_KEY.rkey)が生成されます。

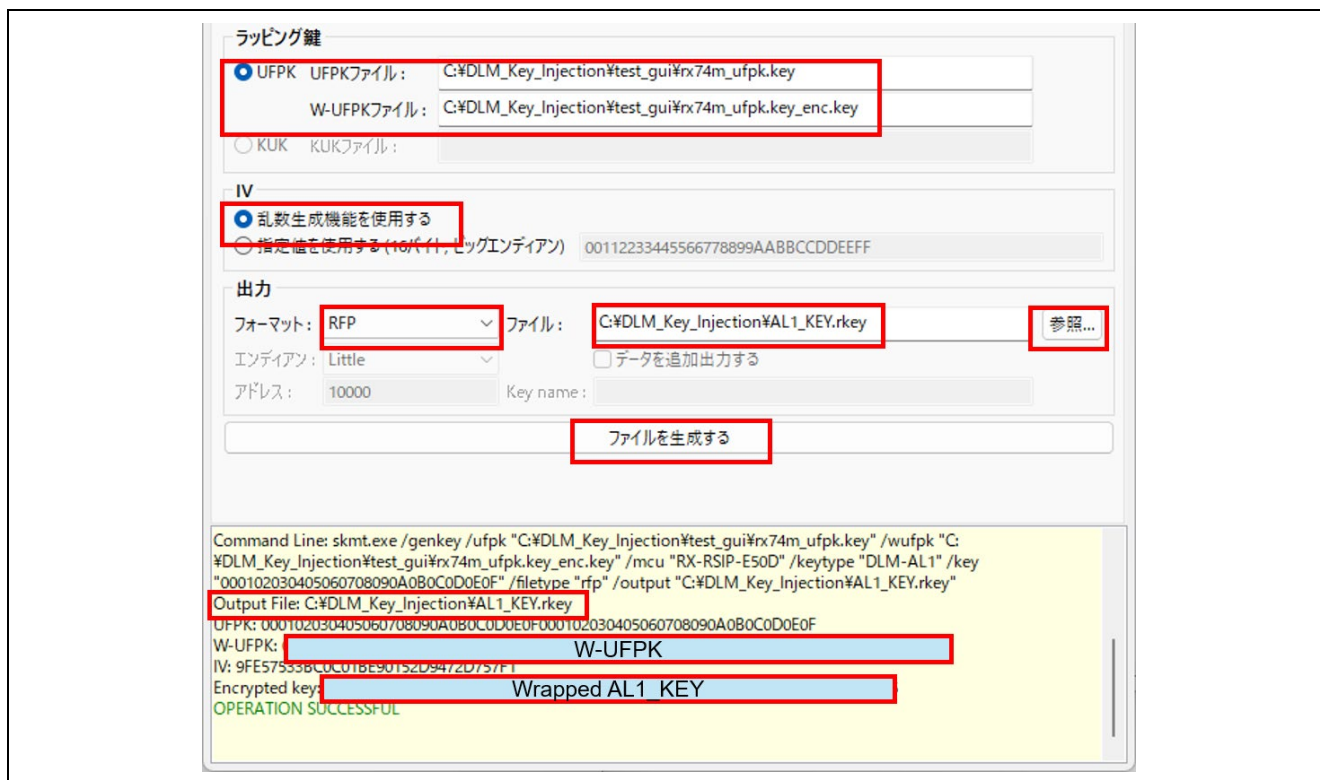


図 3-43 AL1_KEY の RFP 注入ファイルを生成

AL1_KEY は UFPK でラップされます。そして RFP を使用して MCU に AL1_KEY を注入する場合、データに W-UFPK が含まれます。平文の AL1_KEY と UFPK は *.rkey ファイルに含まれていないため、鍵注入時の鍵の機密転送が可能になります。

3.6 RFP を使用した認証鍵の注入

本節では、ALx_KEY 注入を実行する方法を示します。RFP プロジェクトを作成し、ターゲットボードへの接続を確立する方法については、*RFP ユーザーズマニュアル*を参照してください。また、EK-RX74M の SW6-Pin1 および SW6-Pin2 を OFF に設定し、EK-RX74M と PC を USB デバイスケーブルで接続してください。本節では、各状態遷移の主要な構成設定について説明します。

3.6.1 AL2_KEY を注入

AL2_KEY と RMA_KEY は、MCU が AL2 状態の時に注入できます。

注: ALx_KEY の注入は必須ではありません。特定の DLM および特定のデバッグ認証のみが必要な場合、全ての ALx_KEY を注入する必要はありません。どの ALx_KEY を注入すべきかを判断するために、必要な DLM 状態およびデバッグ認証を判断してください。

この例では、3.5.1 で生成した AL2_KEY ルネサスキーファイルを例にしています。RMA_KEY は、一般的な手順で同時に注入することができます。RMA_KEY を使用した RMA_REQ への遷移は、故障解析のために実施する操作であるため、ここでは示しません。

rx74m_dlm_key_inject_rfp.zip を解凍すると、rx74m_dlm_key_inject.rpj が表示されます。RFP を起動し、RFP プロジェクト rx74m_dlm_key_inject.rpj を開き、本項で説明する設定を構成します。

フラッシュオプションタブの **DLM Keys** で、**設定オプションを設定する** に設定します。AL2 Key File 右側の「...」をクリックして、対応する AL2_KEY ファイルを選択します。

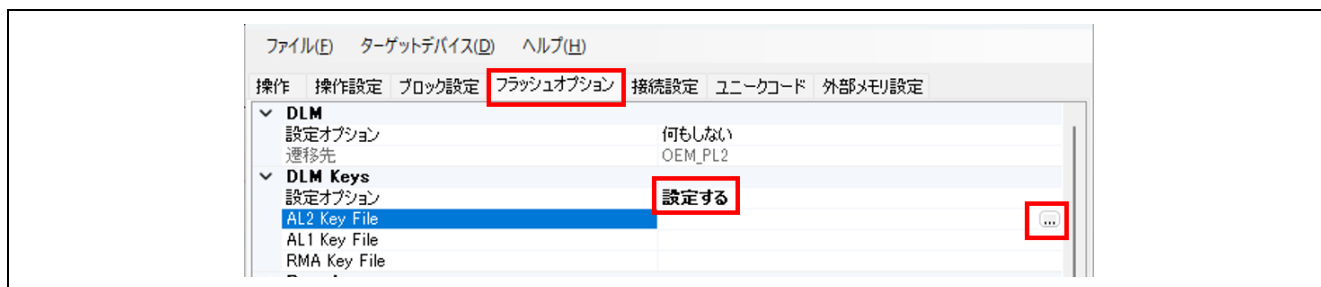


図 3-44 注入する AL2_KEY を選択

前に生成した AL2_KEY.rkey を選択します。



図 3-45 注入する AL2_KEY を選択

操作設定タブで、フラッシュオプション書き込みとフラッシュオプションベリファイを選択します。



図 3-46 書き込みとベリファイ MRAM オプション設定を選択

ALx_KEY とプログラムコードは、同時にプログラムすることも、別々にプログラムすることもできることに注意してください。

操作タブに移動し、セキュリティで保護されたアプリケーションバイナリ(必要な場合)を選択し、スタートをクリックしてデータをプログラムします。

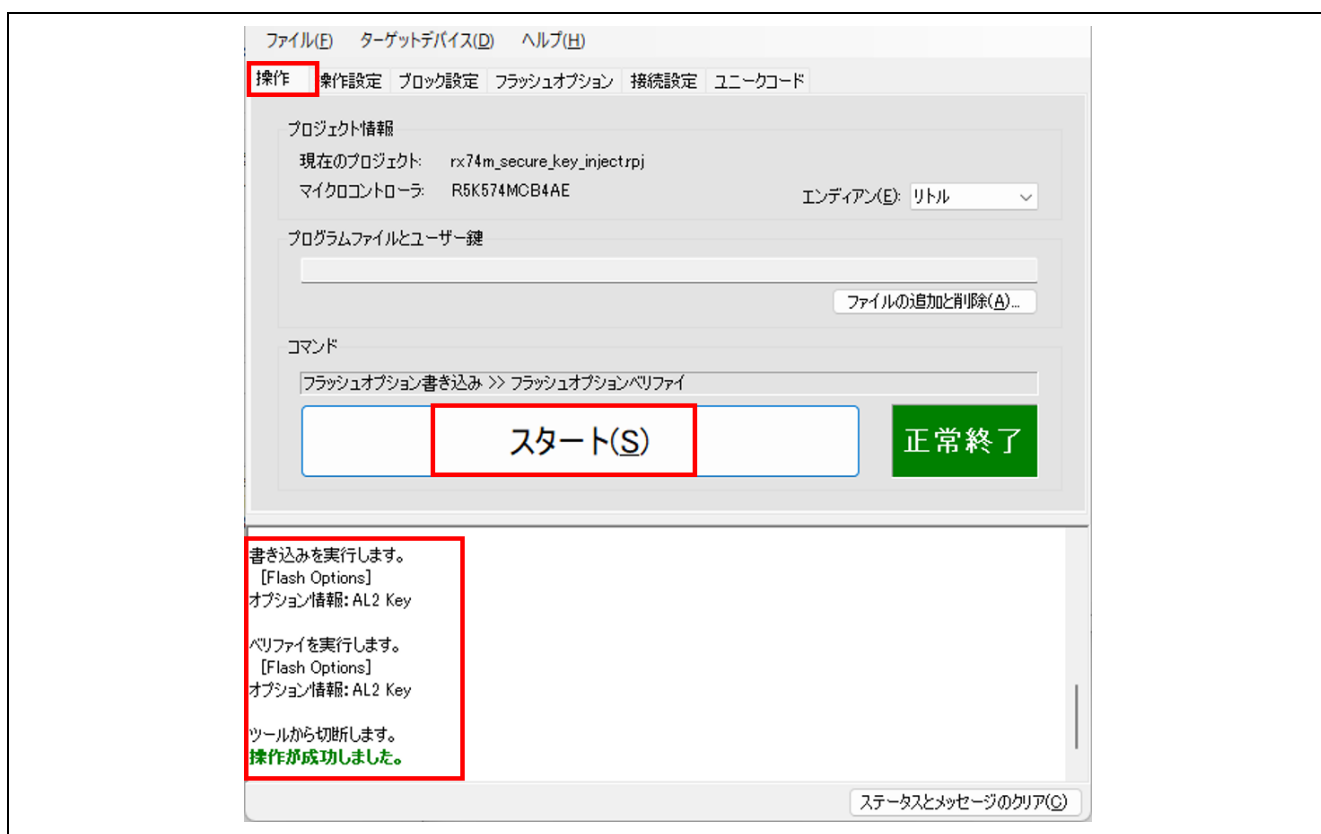


図 3-47 AL2_KEY を注入

3.6.2 AL1_KEY を注入

AL1_KEY は、OEM_PL2 または OEM_PL1 で注入できます。これは、AL2_KEY の注入、未注入にかかわらず注入することができます。

OEM_PL2 で AL1_KEY を注入する場合、AL1_KEY を単独で注入することも、図 3-48 に示すように、フラッシュオプションタブの **DLM Keys** で **AL2 Key File** および **AL1 Key File** を設定し、AL1_KEY と AL2_KEY の両方を注入することもできます。



図 3-48 鍵注入に AL1_KEY と AL2_KEY を含める

操作タブに移動し、スタートをクリックしてデータを書き込みます。

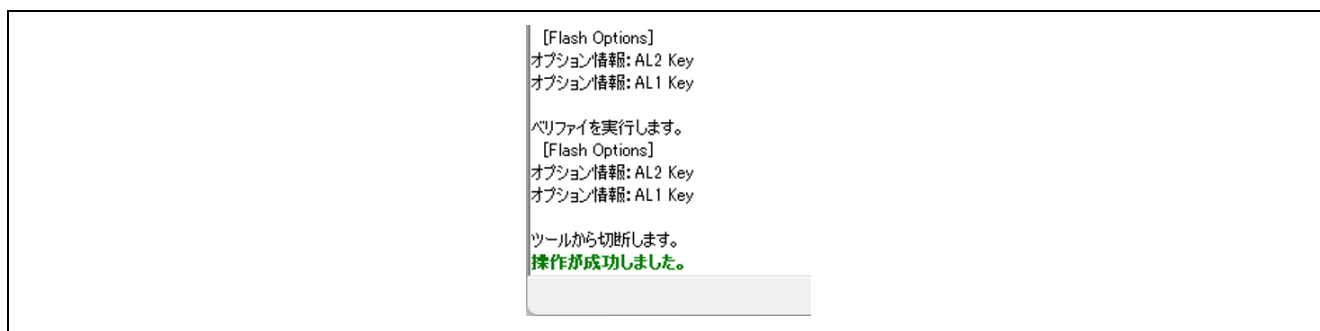


図 3-49 AL1_KEY と AL2_KEY の注入成功

次の例は、OEM_PL1 状態で AL1_KEY を注入する方法を示しています。この場合、図 3-50 に従って OEM_PL1 への遷移を最初に行い、次に図 3-52 に示すように、AL1_KEY のみを注入します。

ターゲットデバイス -> DLM 遷移を選択し、遷移先 DLM ステートを OEM_PL1 に設定して遷移をクリックします。



図 3-50 MCU デバイスライフサイクル状態を AL1 に遷移

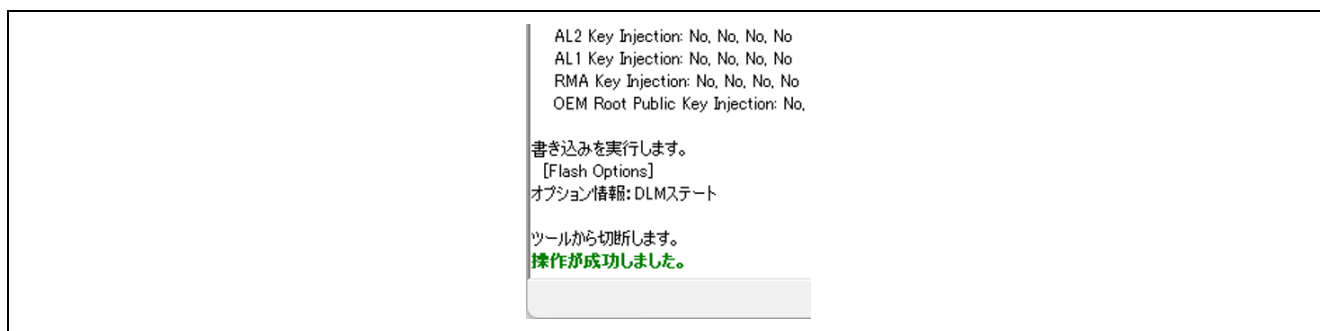


図 3-51 OEM_PL1 への遷移の成功

次に示すように、フラッシュオプションタブの **DLM Keys** で **AL1 Key File** を設定し、AL1_KEY ファイルエントリを追加します。



図 3-52 注入する AL1_KEY を選択

操作タブに移動し、スタートをクリックしてデータを書き込みます。

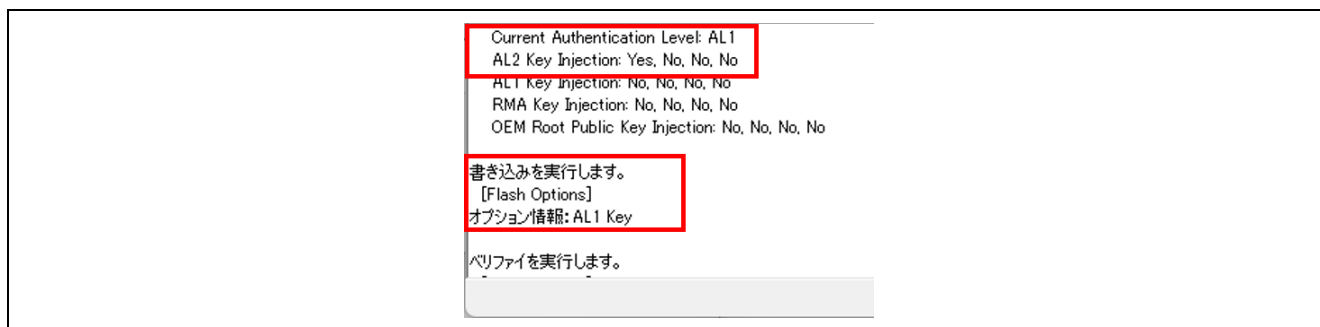


図 3-53 OEM_PL1 の既存 AL2_KEY ありで注入された AL1_KEY

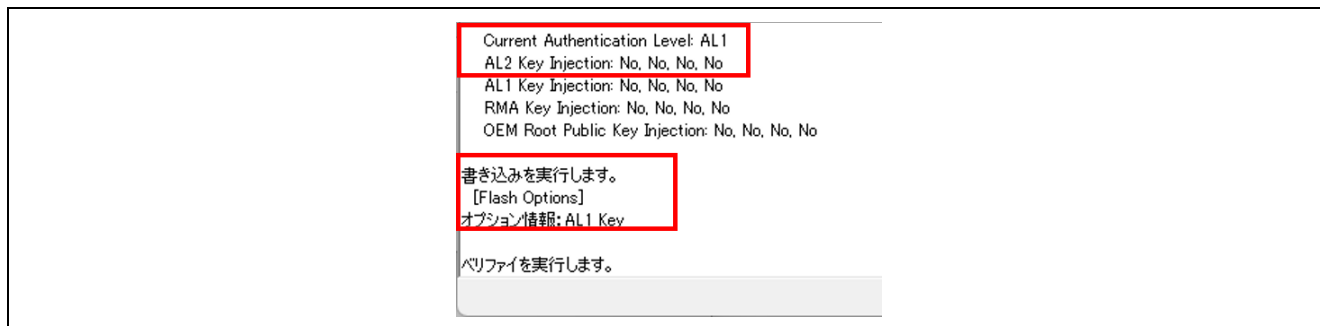


図 3-54 OEM_PL1 の既存 AL2_KEY なしで注入された AL1_KEY

4. 認証レベルと保護レベルの遷移

本章では、RFP と RDPM を使用して DLM 状態遷移を行う方法について説明します。

4.1 認証なしの状態遷移

本節では、DLM(Device Lifecycle Management)の状態、保護レベル(PL)、および認証レベル(AL)を**認証なし**で遷移させる方法を説明します。

これらの遷移は、開発→生産→デプロイまでの一般的なライフサイクルフローを反映しており、遷移するたびにアクセス権限が低下します。なお、EK-RX74M と PC の接続については、3.6 を参照してください。

4.1.1 RFP を使用した認証なしの状態遷移

RFP は、エンドツーエンドの生産工程をサポートします。RFP には、次の機能があります。

- 認証が有効なものと無効なもの全ての状態遷移をサポートします。
- ALx_KEY と RMA_KEY 鍵注入をサポートします。
- 初期化コマンドの無効化をサポートします。これは、デバイスが OEM_PL0 状態で展開され、偶発的な MRAM コンテンツの消去を回避する必要がある場合に望ましいことがあります。**但し、初期化コマンドを無効にすると、再度有効にすることはできません。**
- AL2 および AL1 認証の無効化をサポートします。これは、デバイスが OEM_PL0 状態でデプロイされ、システムのデバッグを無効にする必要がある場合に必要になることがあります。**但し、AL2 認証と AL1 認証を無効にすると、再度有効にすることはできません。**
- LCK_BOOT トランジションへのエントリの無効化をサポートします。これは、デバイスが PL0 状態でデプロイされ、将来的な他の用途のためにデバイスを状態遷移可能な状態にしておきたい場合に必要になることがあります。**但し、LCK_BOOT トランジションを無効にすると、再度有効にすることはできません。**

RFP を使用してデバイスを初期化する場合、**ターゲットデバイス-> デバイスを初期化する** を選択します。

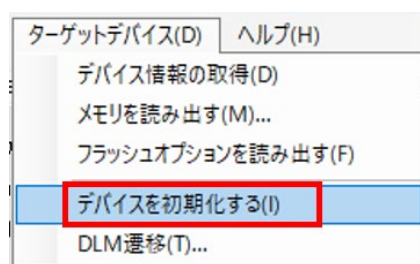


図 4-1 Initialize Device コマンドの使用

PL の遷移は図 4-2 に示すように**ターゲットデバイス -> DLM 遷移**から遷移先の**遷移先 DLM ステート**を選択して実行できます。対応する AL は、PL によって決定されます。

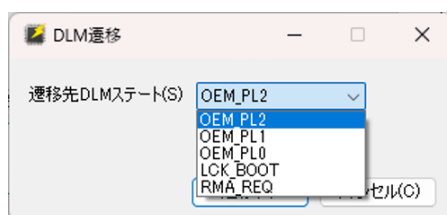


図 4-2 RFP でサポートされる使用可能なライフサイクル状態遷移

初期化コマンドは、次に示すように、フラッシュオプションタブのセキュリティで、設定オプションを設定する、初期化コマンド禁止をはいに選択し無効にできます。**Warning** の表示の通り、この操作を実施した場合、初期化コマンドを有効に戻せません。



図 4-3 初期化コマンドを無効にする

AL2 の認証禁止、AL1 の認証禁止または LCK_BOOT への遷移禁止オプションにはいが選択されている場合も、同様の警告が表示されます。

4.1.2 Renesas Device Partition Manager(RDPM)を使用した認証不要の状態遷移

RDPM は、開発中のデバイスライフサイクル状態管理のために e² studio IDE に統合されたユーティリティツールです。RDPM では、次の機能を実行できます。

- 現デバイスライフサイクル状態の参照
- デバイスの Protect Zone Boundary 設定を参照
- デバイスを OEM_PL2 状態に**初期化**(MRAM が永久に保護されている場合を除く)
- Protect Zone Boundary 設定

e² studio IDE で、**実行-> Renesas Debug Tools -> Renesas Device Partition Manager** を選び開きます。

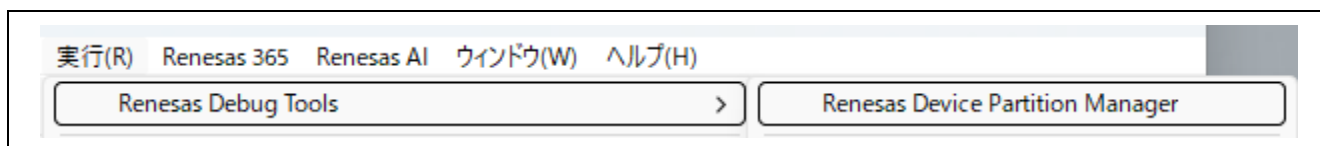


図 4-4 RDPM を開く

図 4-5 は、デバイスを工場出荷時のデフォルトに**初期化**する方法を示しています。**Device Family** を **Renesas RX**、**Initialize device** をオン、および接続方法を選択し、**Run** をクリックします。

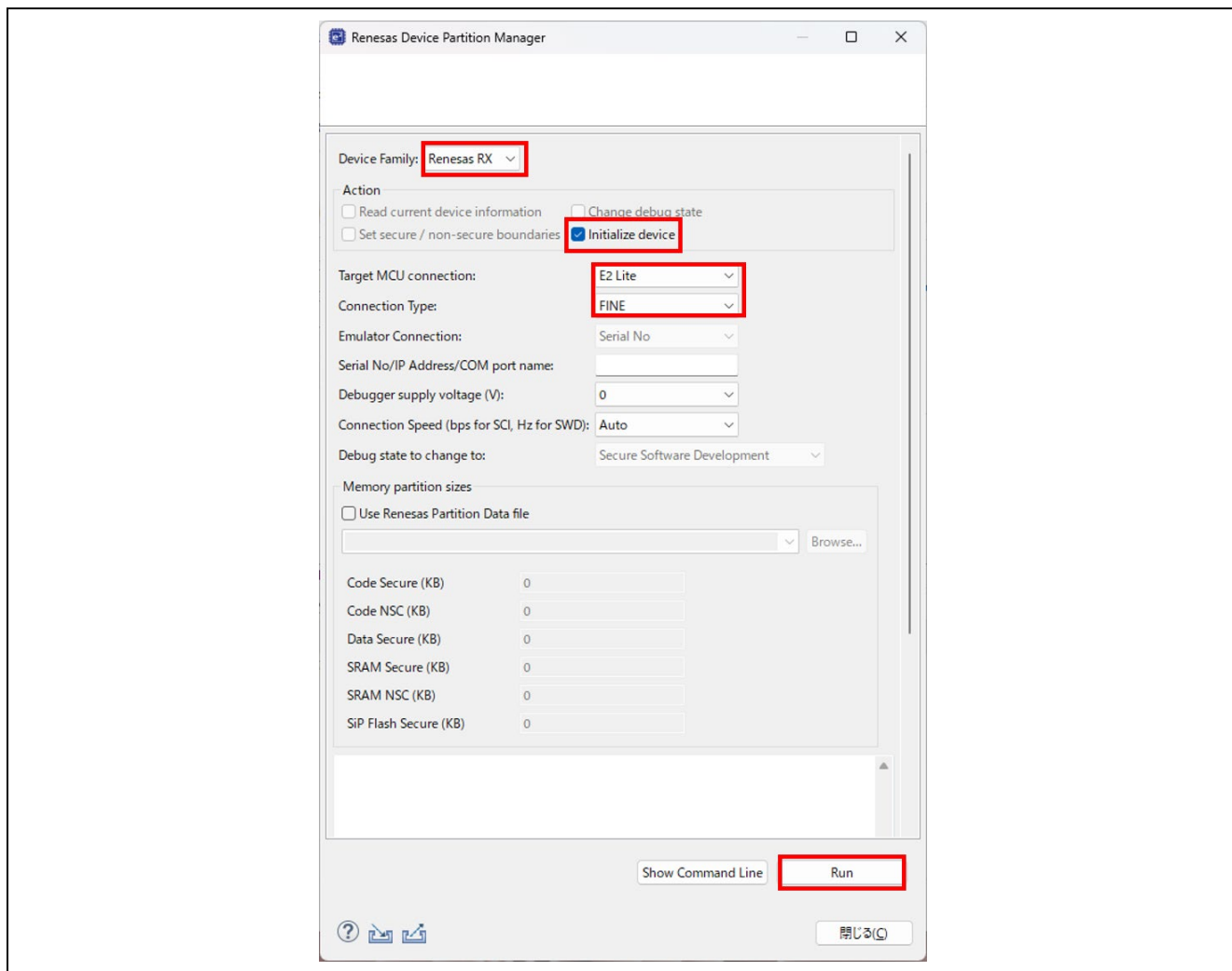


図 4-5 RDPM を使用した RX MCU の初期化

製品開発中、ユーザは通常、保護レベルの遷移(OEM_PL2 から OEM_PL1、OEM_PL1 から OEM_PL0)、およびデバイスの初期化(デバイスメモリを全消去し、保護レベルを OEM_PL2 に設定)に RDPM を使用します。対応する AL は、PL によって決定されます。

RDPM の制限事項

- 認証が必要な遷移はサポートされていません。
- 認証が必要ないデバイスライフサイクル状態への遷移をサポートします。
- 動作には e² studio IDE が必要です。

RX74M において、RDPM を使用する場合、以下の状態が対応します。図 4-6 のように **Debug state to change to** を選択します。

- | | | |
|--|---|---------|
| ● Secure Software Development | → | OEM_PL2 |
| ● Non-secure Software Development | → | OEM_PL1 |
| ● Non-debugging state | → | OEM_PL0 |

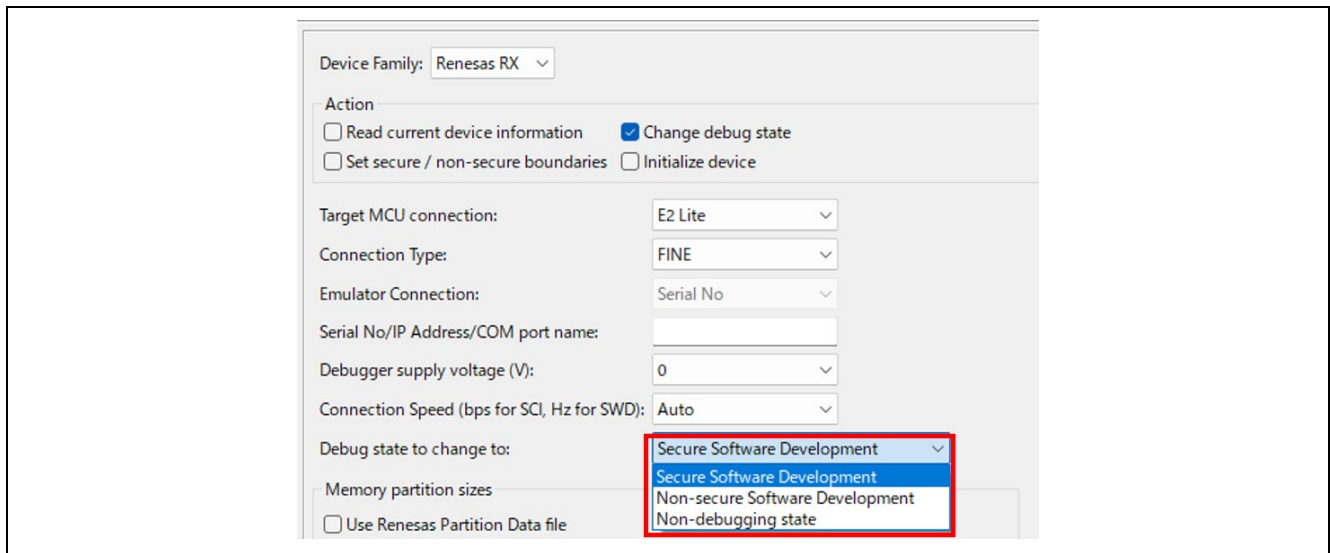


図 4-6 RDPM を使用したデバイスライフサイクル状態の進行

4.2 認証付きの状態遷移

4.2.1 RFP を使用した認証付き遷移

DLM/PL の状態が OEM_PL0 で AL1_KEY が注入されている場合、保護レベルを OEM_PL1 に遷移可能です。

次に、認証付き遷移を実行する手順の例を示します。

1. MCU を OEM_PL2 に初期化します。
2. AL2_KEY と AL1_KEY を注入します。
3. 実施可能な上位権限状態への遷移:

	状態遷移の内容	使用する ALx_KEY	操作例
ケース 1	OEM_PL0 → OEM_PL1	AL1_KEY	ステップ 4 参照
ケース 2	OEM_PL1 → OEM_PL2	AL2_KEY	ステップ 5 参照
ケース 3	OEM_PL0 → OEM_PL2	AL2_KEY	ステップ 5 参照

4. AL1_KEY を使用して OEM_PL0 から OEM_PL1 に遷移します。**ターゲットデバイス-> DLM 遷移**を選択し、**遷移先 DLM ステート**を **OEM_PL1** に設定して**遷移**をクリックします。

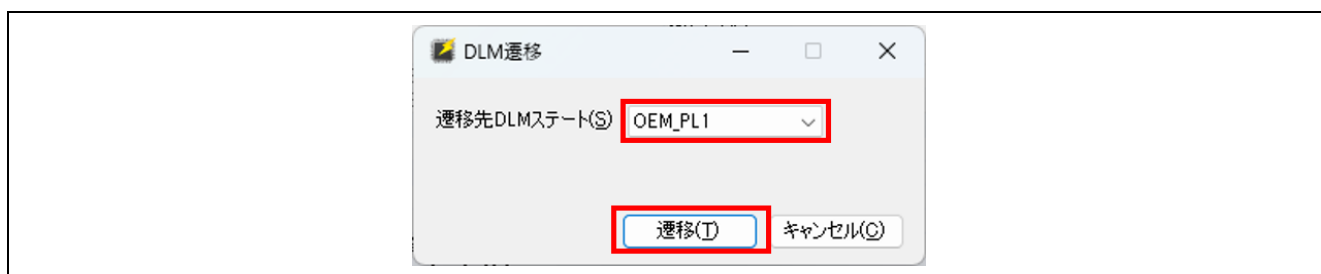


図 4-7 OEM_PL0 から OEM_PL1 への遷移

OEM_PL1 状態に遷移するための AL1_KEY 平文データを入力します。**AL1 Key** に平文鍵を設定し、**OK** をクリックします。必要に応じて、デバイス情報を読み取り、遷移の完了後に結果の状態を確認します。

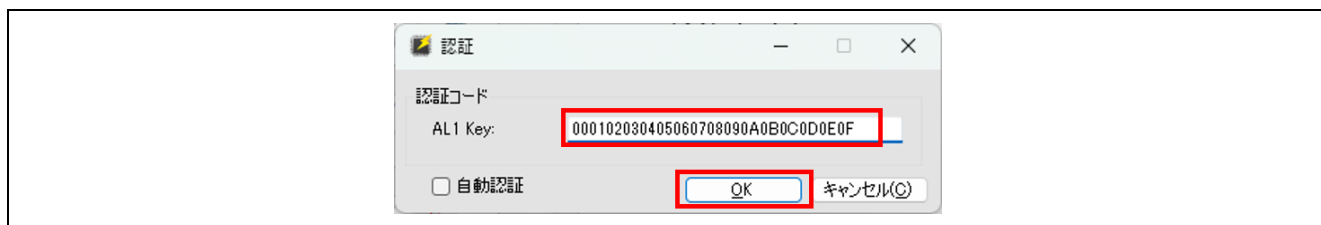


図 4-8 OEM_PL1 へ遷移するために AL1_KEY を提供

5. AL2_KEY が注入されている MCU が OEM_PL1 または OEM_PL0 状態にある場合は、AL2_KEY を使用して OEM_PL1 または OEM_PL0 状態から OEM_PL2 状態に遷移することが可能です。**ターゲットデバイス -> DLM 遷移**を選択し、**遷移先 DLM ステート**を **OEM_PL2** に設定して**遷移**をクリックします。

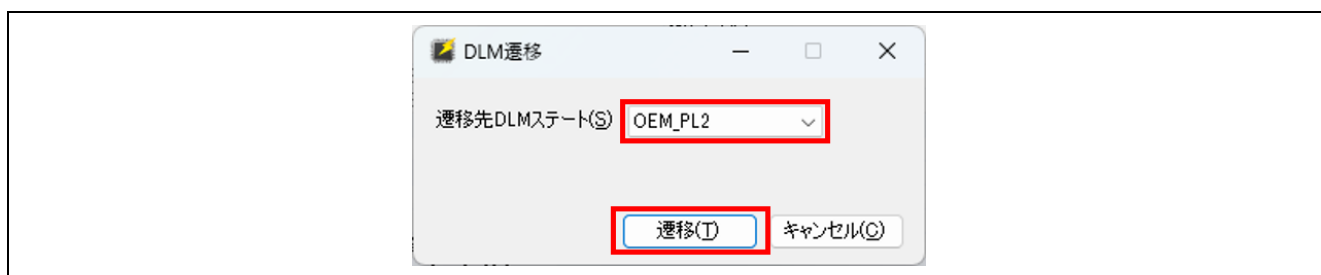


図 4-9 OEM_PL1 から OEM_PL2 への遷移

OEM_PL2 へ遷移するために AL2_KEY 平文データを入力します。**AL2 Key** に平文鍵を設定し、**OK** をクリックします。必要に応じて、デバイス情報を読み取り、遷移の完了後に結果の状態を確認します。

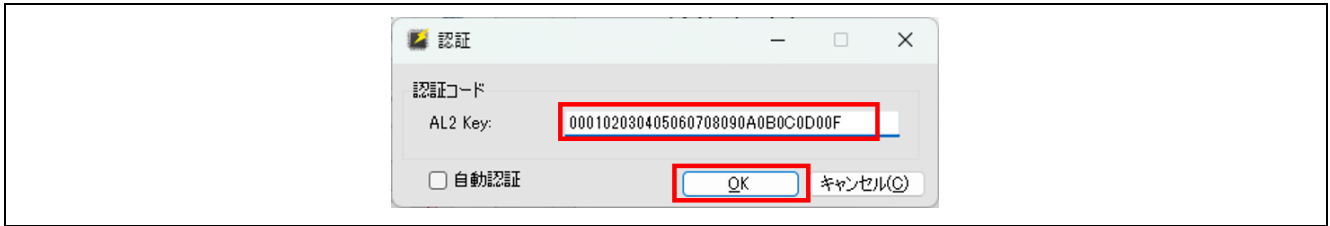


図 4-10 OEM_PL2 へ遷移するために AL2_KEY を提供

4.2.2 e² studio を使用した認証付き遷移

e² studio を使用する場合、保護レベルを変更することはできません。但し、現在のデバッグセッションの認証レベルを変更することで、認証されたデバッグを実行できます。

AL1 から AL2 への認証付き遷移

1. RX74M を OEM_PL2 に初期化します。
2. RFP を使用して RX74M に AL2_KEY と AL1_KEY を注入します。
3. Secure アプリケーションと Non-secure アプリケーションを、2.1 または 2.2 に記載の開発モデルを使用して開発します。この構成では、Non-secure アプリケーションをデバッグすると、Secure アプリケーションと Non-secure アプリケーションの両方がプログラムされ、セキュリティ属性境界が設定されます。
4. Secure アプリケーションと Non-secure アプリケーションをプログラミングし、Non-secure アプリケーションをデバッグするか RFP を使用してセキュリティ属性境界を設定します。
5. デバイスライフサイクルを RFP または RDPM を使用して OEM_PL1 に変更します。
6. Non-secure アプリケーションのデバッグ設定を更新します。
 - セキュリティ属性境界設定の無効化
 - AL2_KEY 平文データ提供により、デバッグ目的で AL2 に遷移

図 4-11 は、本アプリケーションノートで使用されているサンプルの AL2_KEY を使用した設定例です。Debugger -> Connection Settings タブの Protect Zone で、デバイス認証時の認証レベル(AL)を指定する を AL2、認証キーに AL2 平文鍵を設定します。

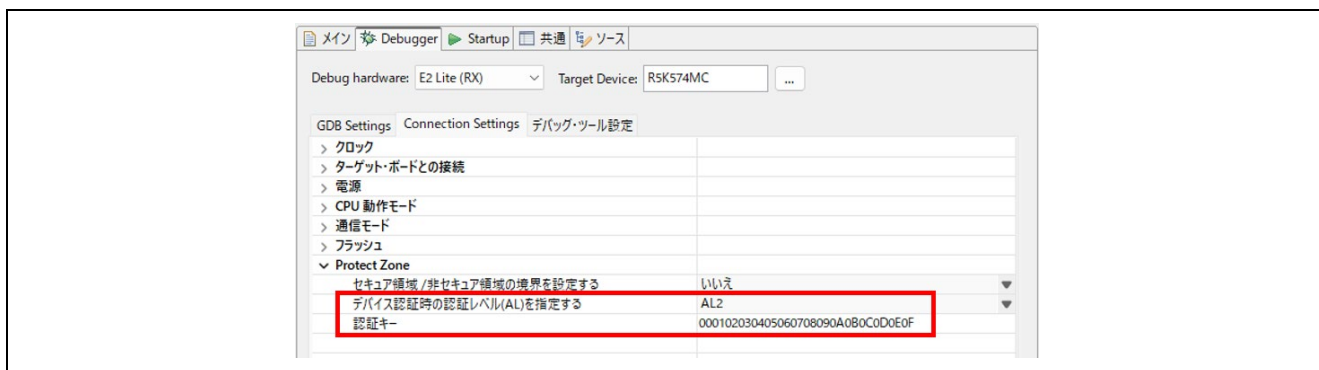


図 4-11 Secure アプリケーションのデバッグと AL2 への遷移

7. 新しい設定の適用と、Non-secure アプリケーションのデバッグはスムーズに進行します。システムは AL2 に遷移するための認証を行い、Secure アプリケーションのデバッグを開始します。この遷移は一時的なものであり、デバッグ接続を終了して電源を投入するとシステムが OEM_PL1 のままになっていることに注意してください。

AL0 から AL1 への認証付き遷移

1. RX74M を OEM_PL2 に初期化します。
2. RX74M に AL2_KEY と AL1_KEY を注入します。
3. Secure アプリケーションと Non-secure アプリケーションを、2.1 または 2.2 に記載の開発モデルを使用して開発します。この構成では、Non-secure アプリケーションをデバッグすると、Secure アプリケーションと Non-secure アプリケーションの両方がプログラムされ、セキュリティ属性境界が設定されます。
4. Secure アプリケーションと Non-secure アプリケーションをプログラミングし、Non-secure アプリケーションをデバッグするか RFP を使用してセキュリティ属性境界を設定します。
5. デバイスライフサイクルを RDPM または RFP を使用して OEM_PL0 に変更します。認証レベルは AL0 になります。
6. Non-secure アプリケーションプロジェクトのデバッグ構成を更新します。
 - Non-secure アプリケーションのみをダウンロードする
 - セキュリティ属性境界設定の無効化
 - AL1_KEY 平文データ提供により、デバッグ目的で AL1 に遷移します。

図 4-12 は、本アプリケーションノートで使用されているサンプルの AL1_KEY を使用した設定例です。Debugger -> Connection Settings タブの Protect Zone で、デバイス認証時の認証レベル(AL)を指定する を AL1、認証キーに AL1 平文鍵を設定します。

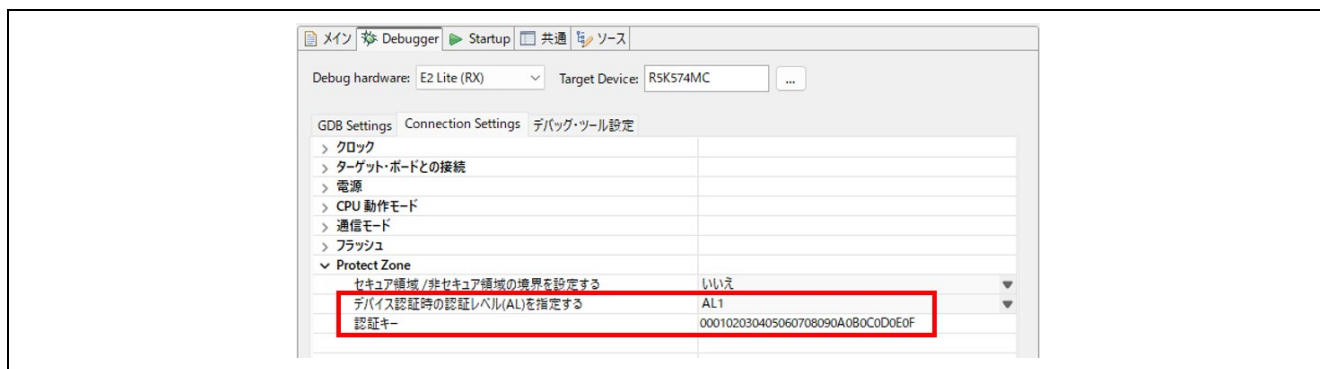


図 4-12 デバッグ中の AL1 への認証付き遷移

7. 新しい設定の適用と、Non-secure アプリケーションのデバッグはスムーズに進行します。システムは AL1 に遷移するために認証を行い、Non-secure アプリケーションのデバッグを開始します。この遷移は一時的なものであり、デバッグ接続を終了して電源を投入するとシステムが OEM_PL0 のままになっていることに注意してください。

5. References

1. RX74M グループ ユーザーズマニュアル ハードウェア編 (R01UH1055)
2. Security Key Management Tool ユーザーズマニュアル (R20UT5349)
3. Renesas Flash Programmer フラッシュ書き込みソフトウェア ユーザーズマニュアル (R20UT5784)

6. ウェブサイトとサポート

RX ファミリの主要な要素について学習し、コンポーネントと関連ドキュメントをダウンロードし、サポートを受けるには、次の URL にアクセスしてください。

RX 製品情報	renesas.com/rx
RX 製品サポートフォーラム	community.renesas.com/mcu/rx
RX Flexible Software Package (FSP)	renesas.com/rx-fsp
ルネサスサポート	renesas.com/support

改訂記録

Rev.	発行日	改訂内容	
		ページ	ポイント
1.00	2026.10.22	-	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、入力信号や入出力ブルアップ電源を入れないでください。入力信号や入出力ブ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くと、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。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、これに限られません。）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た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。