ルネサスMCUを活用したファームウェアアップデートソリューションの提案

～お客様のサイバーセキュリティリスク低減のために～

2026 APR REV.5.00
EMBEDDED PROCESSOR & CONTROLLER SOLUTION MARKETING DEPT
EMBEDDED PROCESSING MARKETING DIVISION
EMBEDDED PROCESSING PRODUCT GROUP
(EP/EPMD/EPMSM)

ルネサス エレクトロニクス株式会社

目次

はじめに：ファームウェアアップデート市場ニーズの増加

IoT化の加速に伴い**ファームウェアアップデートソリューションの需要増加**が見込まれます

様々な機器がIoT化されてインターネット（クラウド）に接続される時代

総務省 令和7年度版情報通信白書※1では、世界の IoT 製品数は2025 年には 467 億台、2026 年には 522億台程度に上ると報告されています。2024年のIoTデバイス数は令和6年の予測（418億台）を上回る420億台に上り、機器のIoT化は更に加速しています。

IoT 製品数の増加に伴い、IoT 製品の脆弱性を狙ったサイバー脅威も増加

日本を含む各国は IoT 製品のセキュリティ確保に向けた取り組みに注力しています。日本セキュリティ要件適合評価及びラベリング制度(JC-STAR)、米国U.S. Cyber Trust、欧州 サイバーレジリエンス法(通称：CRA)などがその代表例です。

→上記背景から、IoT製品の代表例とされるGateway等の**インターネットに直接繋がる機器のOTA**(Over-the-Air)に加えて、**直接繋がらない機器においてもファームウェア更新のニーズ**が増えてくることが予想されます。

本プレゼン資料では、**インターネットへの接続有無に関わらず、IoT製品/組込み機器に必須となるMCU向けファームウェアアップデートソリューション**をご紹介します

※1 総務省｜令和7年版 情報通信白書｜データ集 ※2 総務省｜令和6年版 情報通信白書｜データ集

組込み機器におけるファームウェアアップデートの必要性

サイバーセキュリティ規制法が整備される中、**ファームウェアアップデート機能の実装**は、
IoT製品・組込み機器の市場投入後からEoLまでの一環したライフサイクル管理の必須要件となります。

市場ニーズ

➢ サイバーセキュリティ規制の対策

各国のサイバーセキュリティ規制法への対処が急務。

➢ 信頼とブランド価値の維持

IoT製品や組込み機器は長期間の安定・正常動作が求められ、
製品出荷後の機能追加やセキュリティ脆弱性の対処が必須。
持続的なアプリケーション更新機能がお客様の信頼確保と
企業のブランド価値を持続。

➢ 長期運用を支えるアップデート基盤の強化

製品運用ライフが長期化する中、
最早アップデート機能無しでは
差別化が困難な時代に突入。
サイバーセキュリティ対策が
企業競争力維持に直結。

ファームウェアアップデートの役割

➢ ファームウェアの安全性確保

署名検証によりファームウェア更新時の**完全性**を確認し、
改ざんを防止します。

➢ セキュアブートとファームウェア更新

電源投入後のセキュアブート、市場投入後の機能追加や
脆弱性対策のファームウェアアップデートで、サイバー
攻撃のリスクを最小化し、製品の**可用性**を持続します。

➢ 鍵管理と暗号化技術

鍵管理と暗号化を組み合わせて
データの**機密性**を保持します。

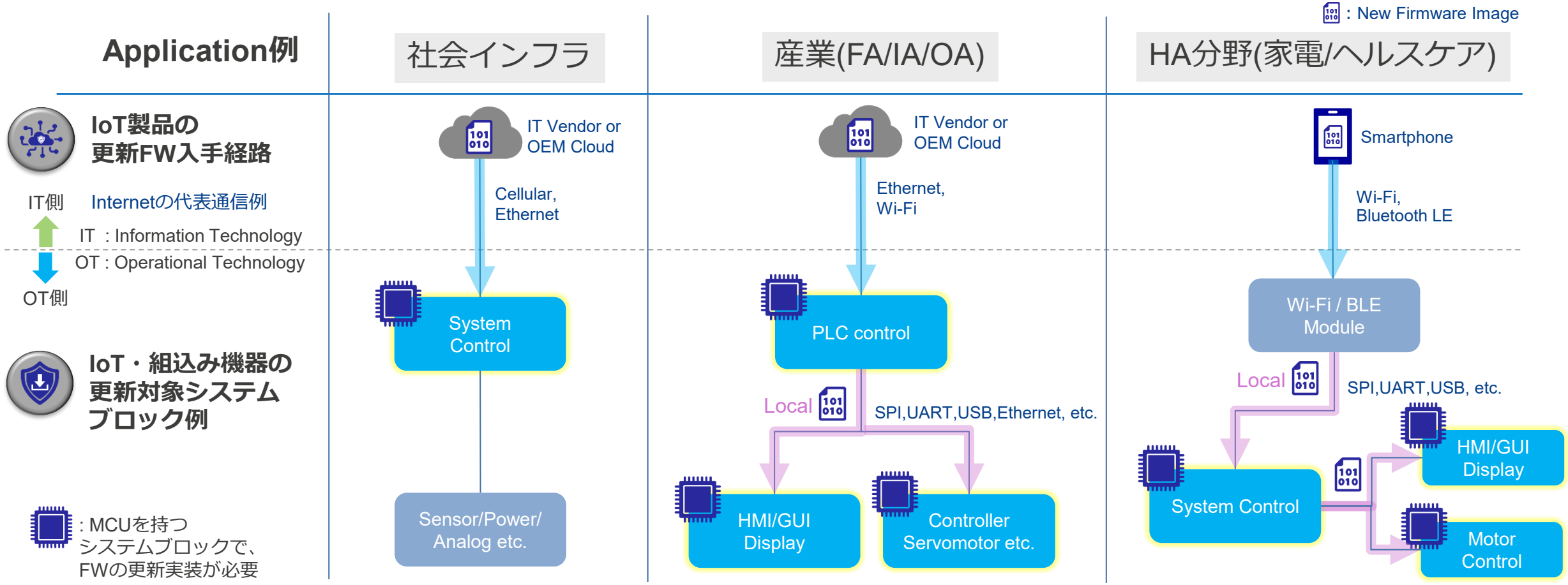
ファームウェアアップデート*が求められるAPPLICATIONシステム構成例

*: Secure Bootも含む

Firmware Update

IoT デバイスやデジタル製品の一般的なアプリケーションにおけるファームウェアアップデートの実装例

: New Firmware Image



RENESAS MCUを活用した ファームウェアアップデートソリューション

FW UP : Firmware Update
OSS : Open-Source Software
SKMT : Security Key Management Tool
TSIP : Trusted Secure IP
RSIP : Renesas Secure IP
SCE : Secure Crypto Engine

MCUファミリ毎の特長やセキュリティエンジンを活かして、最適なFW UP制御方式を提供

“ FW UP モジュール “ ソリューション		内容	“ MCUboot “ ソリューション		
RX Family	**RL78** Family	対象MCUファミリ	**RA** Family without Security Engine	**RA** Family with Security Engine	**RX** Family with Security Engine
FW UP モジュール		ドライバ名	**MCUbootモジュール**		
ソフトウェア暗号ライブラリ		署名検証方法	ソフトウェア暗号ライブラリ	セキュリティエンジン（by TSIP / RSIP / SCE）	
ECDSA P-256, SHA256		署名検証方式	**ECDSA P-256/P-384, RSA 2048/3072, ML-DSA-44/65/87**	**ECDSA P-256/P-384, RSA 2048/3072**	**ECDSA P-256, RSA 2048**
平文形式		署名検証用”公開鍵”の格納形式	**平文**形式	**ラップ**形式* or **平文**形式	**ラップ**形式*
リニアモード - **半面更新**方式 リニアモード - **全面更新**方式 デュアルモード - **デュアルバンク**方式		Flash ROM構成で選択可能な更新方式	リニアモード - **スワップ**方式 リニアモード - **上書き** 方式 リニア or デュアルモード - **DirectXIP** 方式		
FW UP ソリューション章 参照		詳細	MCUboot ソリューション章 参照		

*： SKMTでラッピングした署名検証用公開鍵を作成し、キーインストール用のサンプルを使って格納

注：対応内容（署名検証方式、更新方式等）は、MCUやセキュリティエンジンの有無によって異なります。詳細は、各ソリューション章とアプリケーションノートをご確認ください。

RX & RL78向け
ファームウェアアップデート（FW UP）モジュール
ソリューション

ファームウェアアップデートの役割と実装ステップ

お客様が鍵ペアをご用意、Renesasはツールやドライバで安全な署名・FW更新を支援します

Firmware Update

ファームウェアアップデートに必要な「順序」に沿った「実装」を実現するソリューション

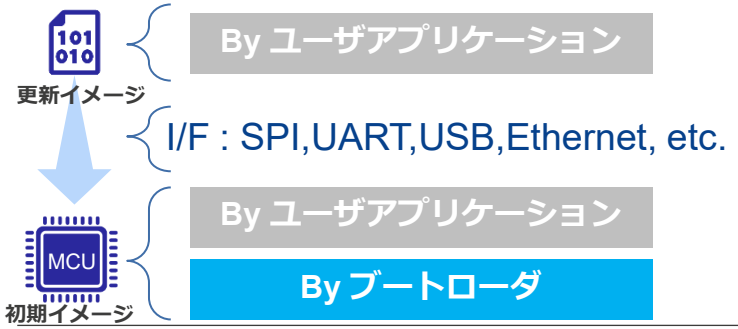
ファームウェアアップデートの 順序

①通信インタフェースを介して
更新イメージを MCU に取り込む

②更新イメージをMCU内蔵フラッシュ
に書き込む

③更新イメージの正当性を検証する

④更新イメージを有効化する



ファームウェアアップデートの 実装

ブロックの色分け：お客様にご準備いただく工程／ルネサスがサービス提供する工程

1. ファームウェアイメージの作成

- ✓コード署名のための鍵ペア (秘密鍵,公開鍵) を生成
- ✓ブートローダ と ユーザアプリケーション の統合
- ✓コード署名検証データの生成・付与

2. ファームウェアアップデートの実行

- ✓更新イメージをMCUに取り込むための通信制御
- ✓更新イメージの内蔵フラッシュへの書き込み
- ✓コード署名検証で更新イメージの正当性検証
- ✓更新イメージの有効化

コード署名検証のアルゴリズムは**楕円曲線暗号(ECDSA)方式による ECDSA NIST P-256** および **SHA256（HASHのみ)**に対応しています。

鍵ペアの生成
本サンプルソフトでは**OpenSSL(OSS)ツールを利用してサンプル鍵を生成**しています

ルネサス提供

更新FWのイメージ生成ツール
Renesas Image Generator

＋

FW UPモジュール

＋

ブートローダ

＋

ユーザアプリケーション

ルネサス製ファームウェアアップデート（FW UP）モジュールの特徴

Firmware Update

FW UPモジュールを実装することで、容易にファームウェアアップデート機能の組込みが可能！

ルネサス提供

更新FWのイメージ生成ツール
Renesas Image Generator

＋

ブートローダ サンプル

＋

FW UPモジュール

＋

ユーザアプリケーション

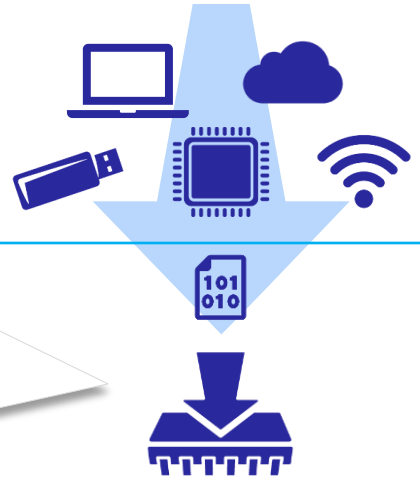
事前準備：プログラムのmotファイルおよび鍵ペアを作成

Renesas Image Generatorで**署名付き更新イメージ***を生成

101
010

* OpenSSLで鍵ペアや署名情報を生成

いずれかの方法で更新イメージをインプット



様々な入力経路 でファームウェア更新可能！
（ UART / SPI / USB / Ethernet 等の通信インターフェース経由等）

お客様のご要望に沿った**様々な通信インターフェース**で更新ファームウェアイメージを取得できる設計

MCUに応じた３つの更新方式に対応！

1. デュアルモード：**デュアルバンク方式**
2. リニアモード　：**半面更新方式**
   - ファームウェア更新に失敗しても容易に復旧可能
3. リニアモード　：**全面更新方式**
   - 小メモリフットプリントMCUでのファームウェア更新が可能
   - 外部フラッシュをバッファとして使用する方式にも対応

署名検証による安全なファームウェア更新を実現！

セキュアブート機能によるファームウェアの正当性検証（**ECDSA NIST P-256 および SHA256**）に対応

FW UPモジュールを使ったシステム構成例

FW UPモジュールは、様々な”プライマリデバイス”を経由したファームウェア更新に最適です

様々なユースケースに対応

: New Firmware Image

スタンドアローン
（機器単体で動く製品）

家電　計測機器

空調機など
“ **対** “ になるシステム

室外機 (ODU)
↓
室内機 (IDU)

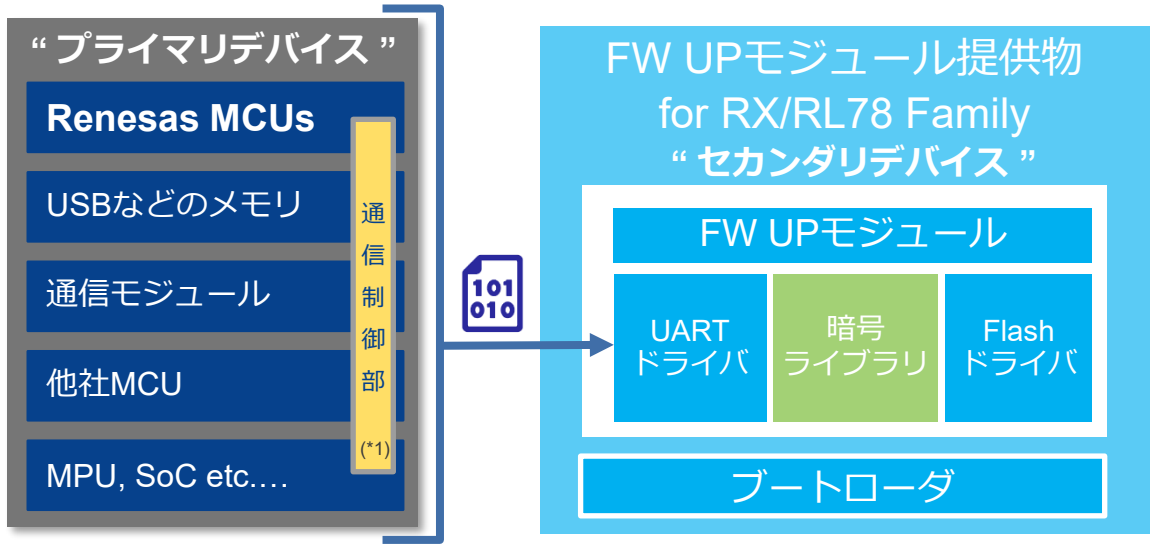
産業系システム
（制御用デバイスと接続された複数のデバイスで構成されるシステム）

制御デバイス
(プライマリデバイス)

セカンダリデバイス　セカンダリデバイス　セカンダリデバイス

FW UPモジュール対応製品：**RXファミリ**　：全マイコン
RL78ファミリ：RL78/G22, RL78/G23, RL78/G24, RL78/L23

シリアル通信でファームウェアを取得



(*1) : ファームウェアアップデート通信モジュール（RX, RL78）を提供

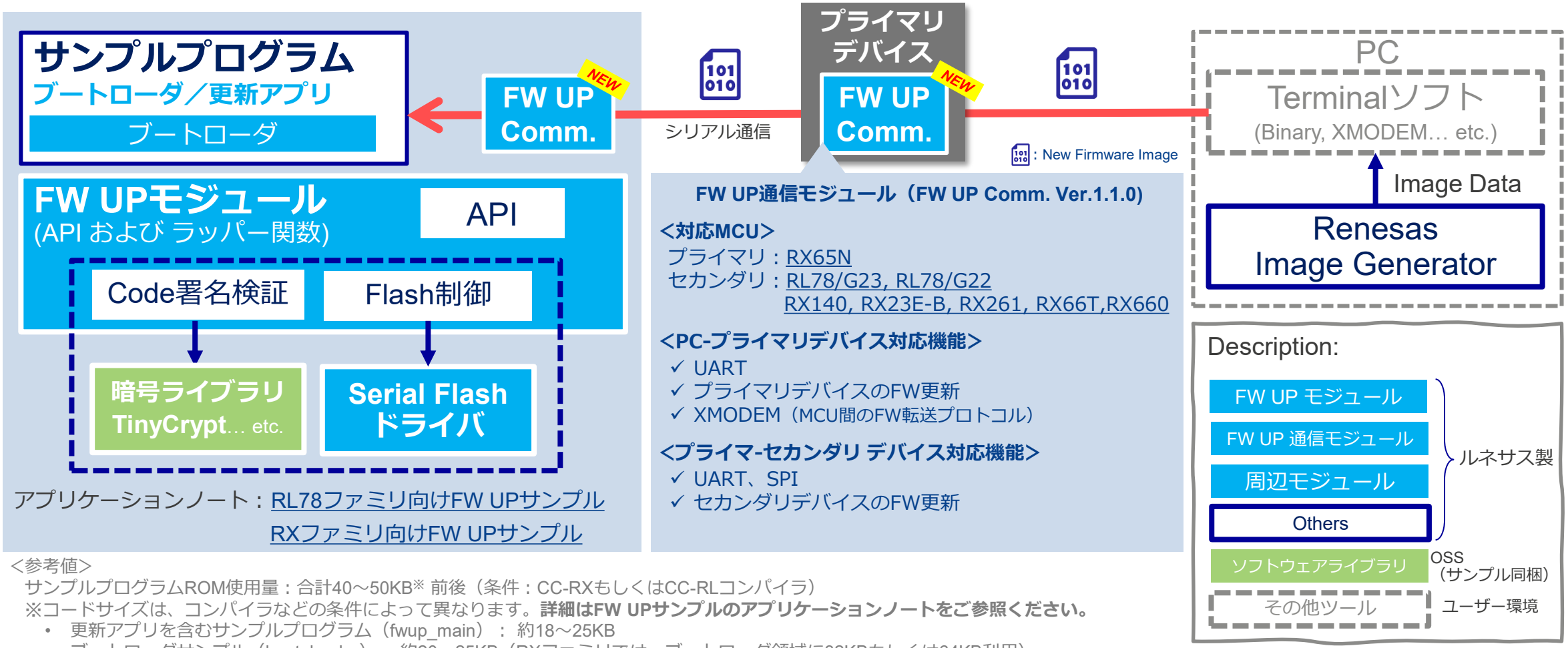
アプリケーションノート

RXファミリ向けFW UPサンプル

RL78ファミリ向けFW UPサンプル

“FW UPモジュール”を使用した“セカンダリデバイス”更新システム構成例

➢ “セカンダリデバイス” の ファームウェアアップデート



アプリケーションノート：RL78ファミリ向けFW UPサンプル
RXファミリ向けFW UPサンプル

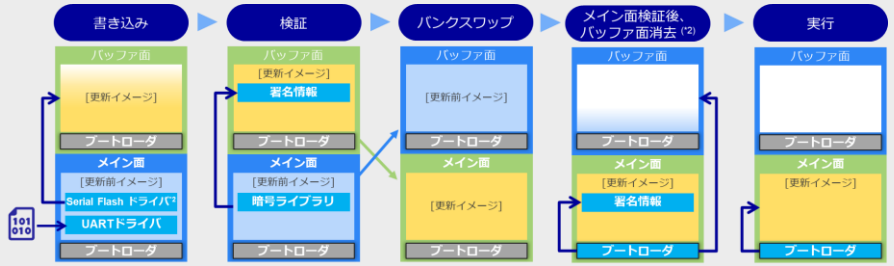
<参考値>
サンプルプログラムROM使用量：合計40～50KB※ 前後（条件：CC-RXもしくはCC-RLコンパイラ）
※コードサイズは、コンパイラなどの条件によって異なります。**詳細はFW UPサンプルのアプリケーションノートをご参照ください。**
- 更新アプリを含むサンプルプログラム（fwup_main） ： 約18～25KB
- ブートローダサンプル（boot_loader） ： 約20～25KB（RXファミリでは、ブートローダ領域に32KBもしくは64KB利用）

製品に応じて選べるアップデート方式
各方式のサンプルプログラムで開発をサポート！

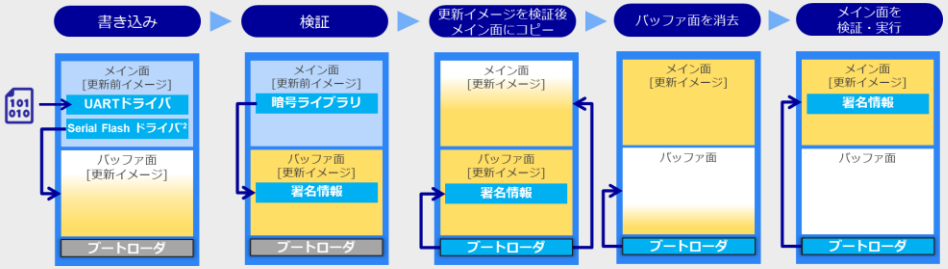
MCUに応じた３つの更新方式に対応！

<サンプルプログラム>
RX : #R01AN6850 / Sample Zip
RL78 : #R01AN6374 / Sample Zip

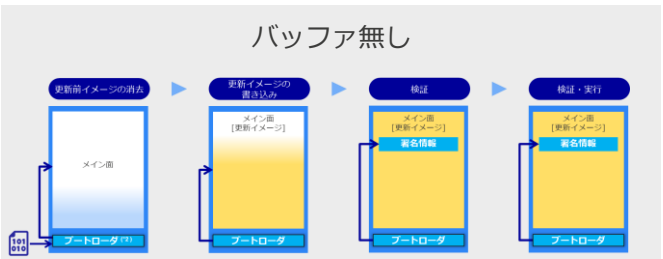
1. デュアルモード：デュアルバンク方式*のアップデート動作

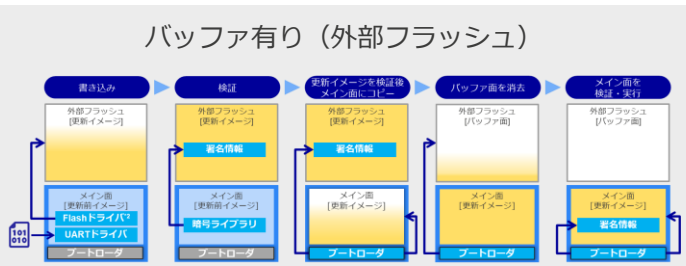


2. リニアモード：半面更新方式*のアップデート動作



3.リニアモード：全面更新方式*のアップデート動作





各モードおよびデバイス対応表

Flash Product	4MB	2MB	1.5MB	1MB	768KB	512KB	384KB	256KB	128KB	96KB	64KB
RX130	-	-	-	-	-	L	L	L	L	-	-
RX140	-	-	-	-	-	-	-	L	L	-	-
RX231/230	-	-	-	-	-	L	L	L	L	-	-
RX23E-A	-	-	-	-	-	-	-	L	L	-	-
RX23E-B	-	-	-	-	-	-	-	L	L	-	-
RX24T	-	-	-	-	-	L	L	L	L	-	-
RX261	-	-	-	-	-	L	L	L	-	-	-
RX26T	-	-	-	-	-	DB/L	-	L	L	-	-
RX65N/651	-	DB/L	DB/L	L	L	L	-	-	-	-	-
RX66N	DB/L	L	-	-	-	-	-	-	-	-	-
RX66T	-	-	-	L	-	L	-	L	-	-	-
RX660	-	-	-	L	-	L	-	-	-	-	-
RX671	-	DB/L	DB/L	L	-	-	-	-	-	-	-
RX72M	DB/L	L	-	-	-	-	-	-	-	-	-
RX72N	DB/L	L	-	-	-	-	-	-	-	-	-
RX72T	-	-	-	L	-	L	-	-	-	-	-
RL78/G22	-	-	-	-	-	-	-	-	-	-	L
RL78/G23	-	-	-	-	L	L	L	L	L	L	-
RL78/G24	-	-	-	-	-	-	-	-	L	-	L
RL78/L23	-	-	-	-	-	DB/L	-	DB/L	L	L	L

DB ： デュアルバンク機能を使用したFW UP対応製品 (1. デュアルバンク方式)
L ： リニアモードでのFW UP対応製品 (2.半面更新方式／3. 全面更新方式)
- ： 対象外
赤字 ： サンプルプログラム対応製品（サンプルプログラムはZipとして提供）

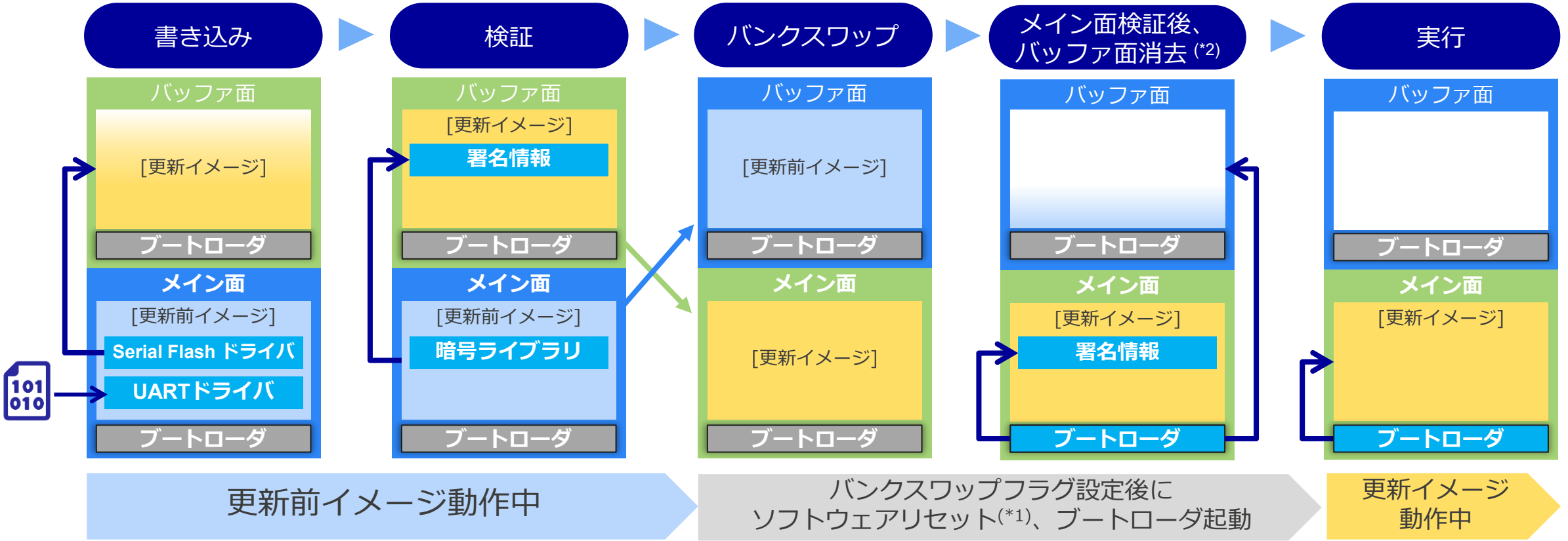
注) RXファミリ用リニアモードの全面更新方式（バッファ有り）のデモプロジェクトは、デュアルバンク対応製品向けには提供しておりません。対応は可能ですので、必要な場合はメモリ配置の近い製品のデモプロジェクトを参考に検討ください。

* 更新方式名はRL78向けアプリケーションノートと一部表記が異なります。
1.は「デュアルバンク（２バンク）方式」、
2.は「半面更新方式（バッファ面は内部フラッシュ）」、
3.は「全面更新方式（バッファ無し）」「全面更新方式（バッファ面は外部フラッシュ）」を指します。

1．デュアルモード
デュアルバンク方式：正常動作

ユーザアプリケーションを止めたくない機器には
デュアルバンク対応製品を使った
デュアルバンク方式がお勧め！

デュアルバンク対応製品では、メイン面のプログラムを実行中に更新イメージを書き込み可能！
バンクスワップ機能により実行するプログラムのアドレス配置管理が不要！



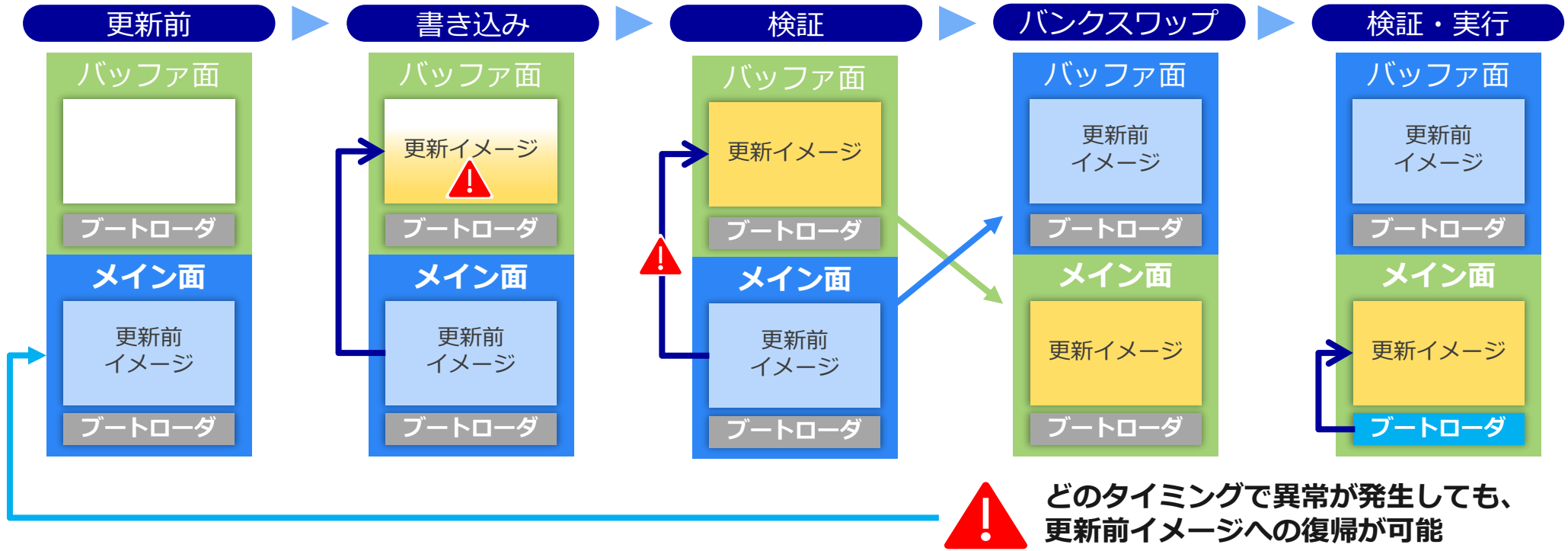
*1 : ソフトウェアリセットによる初期化対象は、各マイコンのハードウェアマニュアルの『リセット章』をご参照ください。
*2 : デモプログラムでは、バッファ面の消去を行っておりません。ロールバックの対策等で、更新前のイ メージを消去する必要が有る場合は、バッファ面のイメージの消去処理を追加してください。

1．デュアルモード
デュアルバンク方式：異常発生時の動作

電源遮断／署名検証失敗によりファームウェアアップデートに失敗した場合、
更新前のイメージを起動してファームウェアアップデートをやり直すことが可能

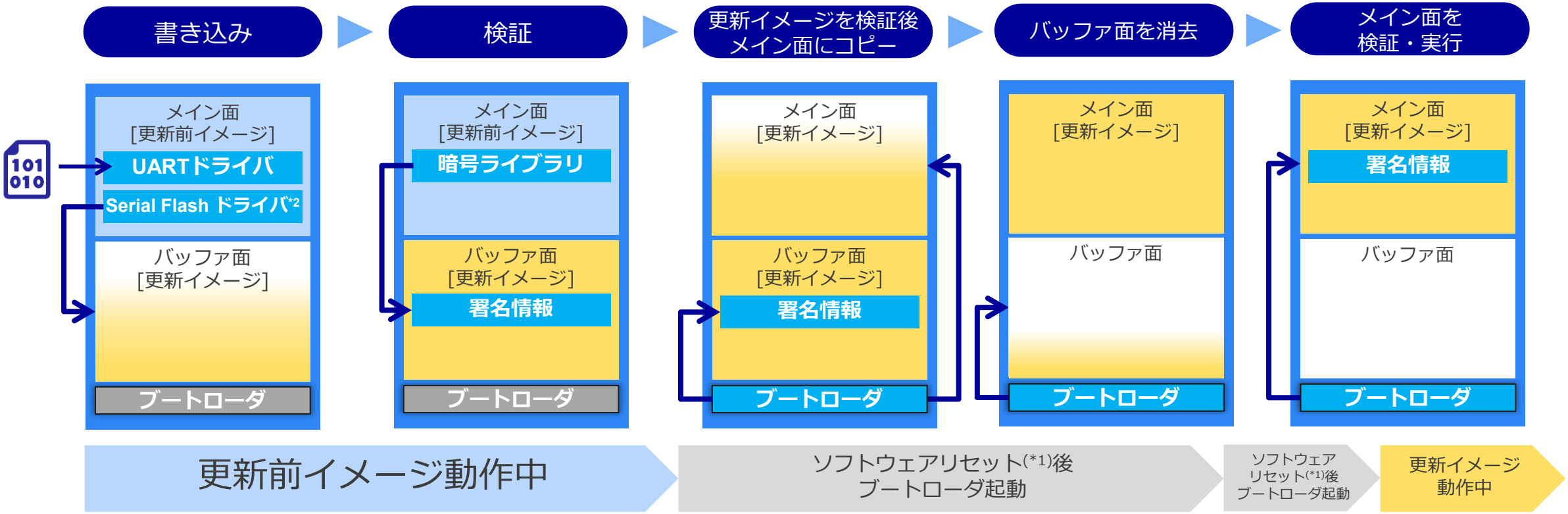
バッファ面	無効	無効	有効	有効
メイン面	有効	有効	有効	有効

緑文字：起動可能な状態／**黒文字**：起動不能な状態



2．リニアモード
半面更新方式：正常動作

デュアルバンク非対応製品でも、半面更新方式を使用することで
更新前イメージを保持した状態でファームウェア更新が可能



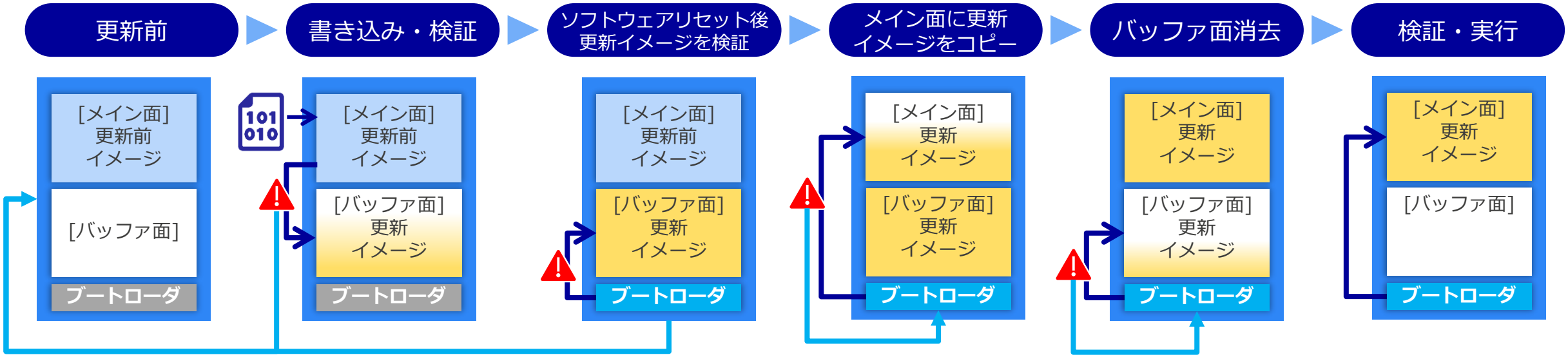
*1 : ソフトウェアリセットによる初期化対象は、各マイコンのハードウェアマニュアルの『リセット章』をご参照ください。
*2 : Serial Flashドライバでの書き込み処理はRAMで実行されます。詳細は各ファミリ（RX、RL78）のSerial NOR Flash Memory制御モジュールのアプリケーションノートをご参照ください。

2．リニアモード
半面更新方式：異常発生時の動作

電源遮断／署名検証失敗などによりファームウェアアップデートに失敗した場合、
更新前のイメージを起動してファームウェアアップデートをやり直すことが可能

メイン面	有効	有効	無効	有効	有効
バッファ面	無効	無効	有効	無効	無効

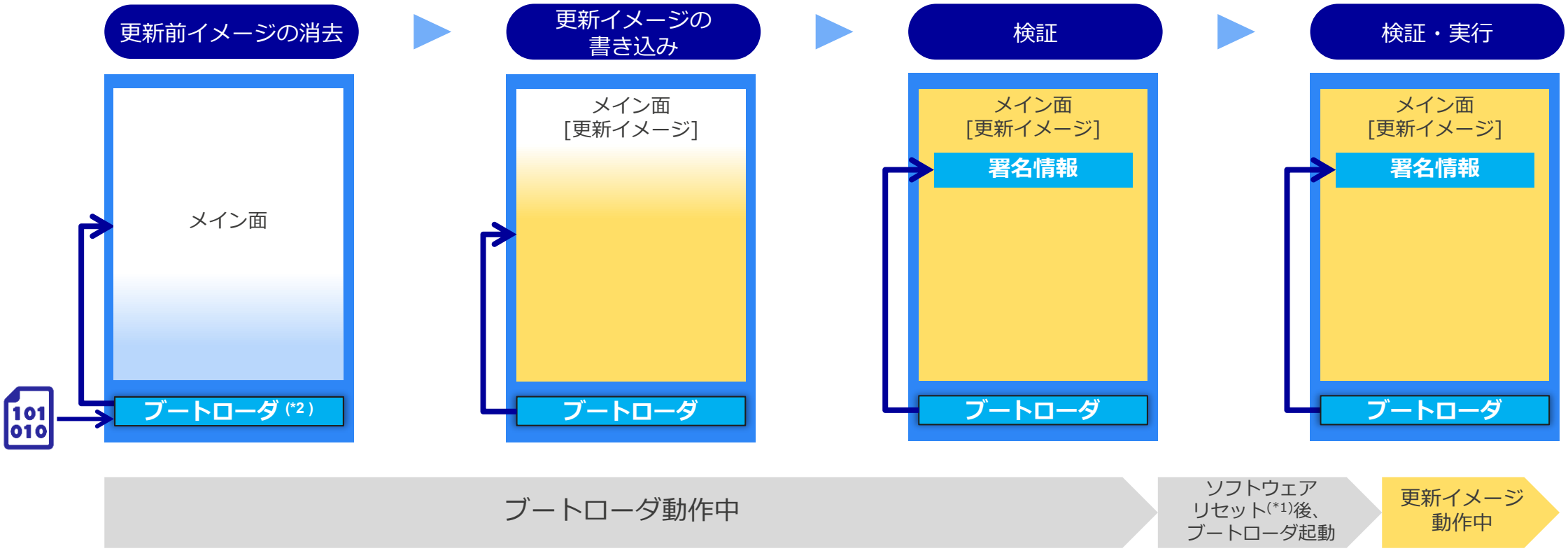
緑文字：起動可能な状態／**黒文字**：起動不能な状態



**常にどちらかの面に有効なイメージが存在し、
異常発生時に復帰が可能**

3．リニアモード
全面更新方式（バッファ無し）：正常動作

ROMサイズの小さな製品でも、
全面更新方式を使用することでファームウェアアップデートを実装可能！



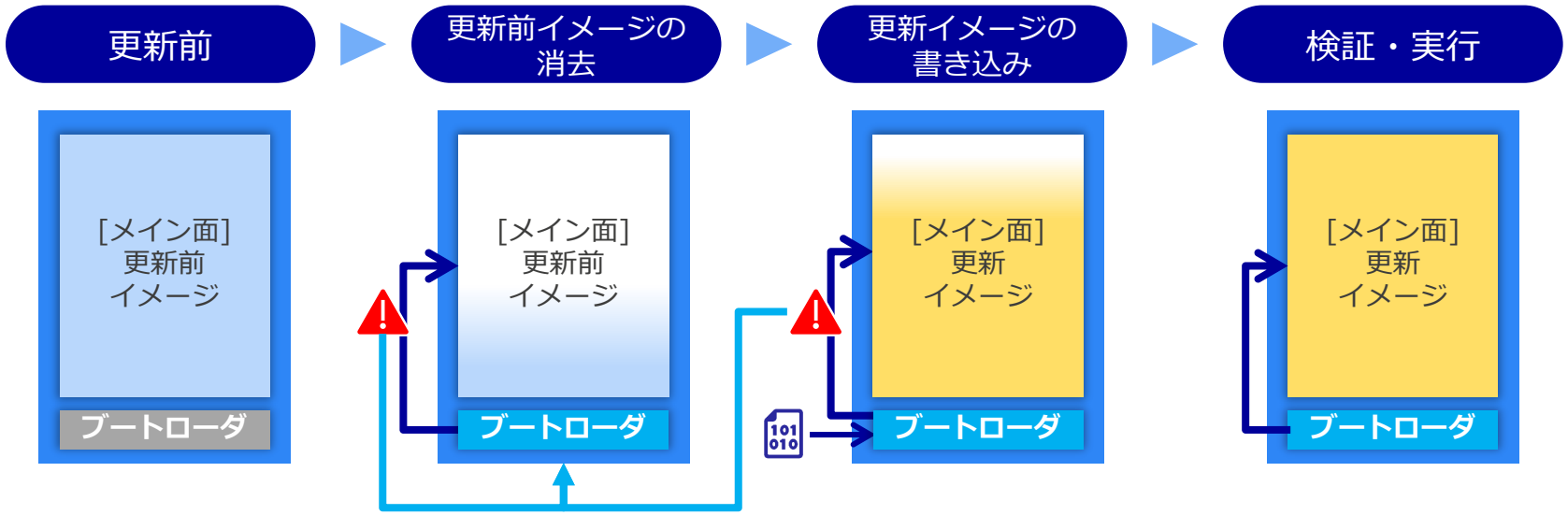
*1：ソフトウェアリセットによる初期化対象は、各マイコンのハードウェアマニュアルの『リセット章』をご参照ください。
*2：デモプログラムのブートローダは、更新イメージの取得にUART通信を利用しています。お客様の利用したい通信方式に応じて変更いただく必要があります。
*3：ブートローダのFlash書き込み処理はRAMで実行されます。詳細は各ファミリ（RX、RL78）のSerial NOR Flash Memory制御モジュールのアプリケーションノートをご参照ください。

3．リニアモード
全面更新方式（バッファ無し）：異常発生時の動作

全面更新方式（バッファ無し）では、ファームウェアアップデートに失敗した場合、
ブートローダの機能を使ってファームウェアアップデートを再実行

メイン面	有効	無効	無効	有効

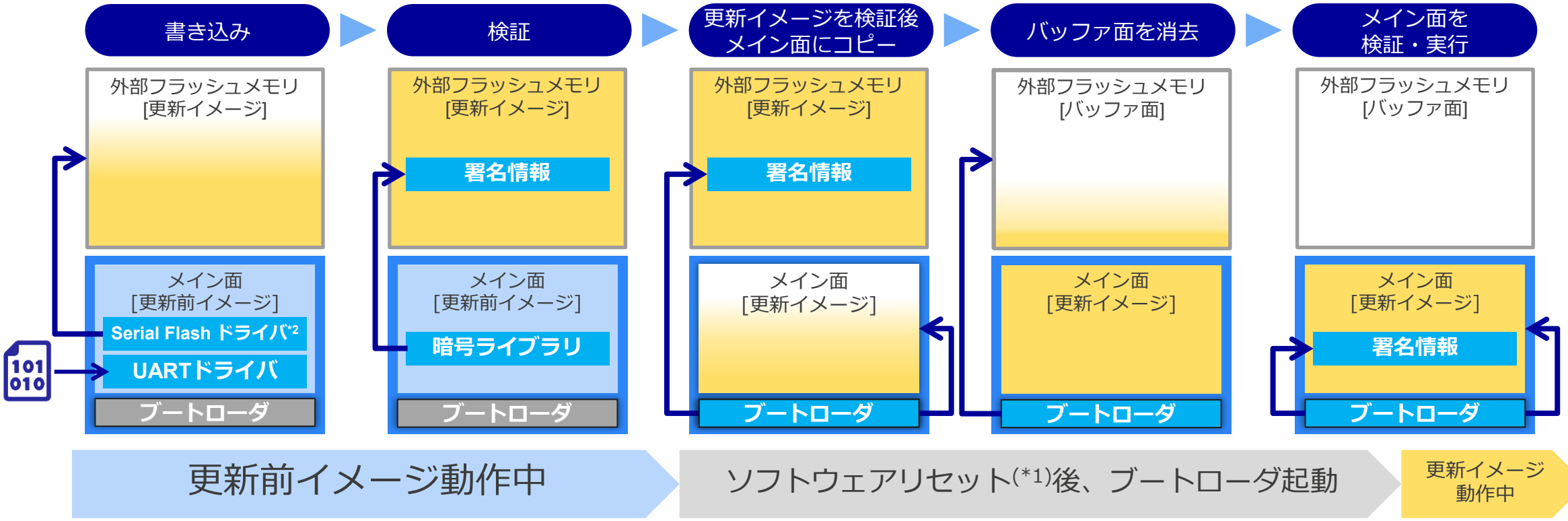
緑文字：起動可能な状態／**黒文字**：起動不能な状態



ファームウェアアップデートに成功するまで、
処理を繰り返します

3．リニアモード
全面更新方式（バッファ有り）：正常動作

外部フラッシュメモリを使用することで、メイン面の更新前イメージを保持したまま
更新ファームウェアの取得が可能！



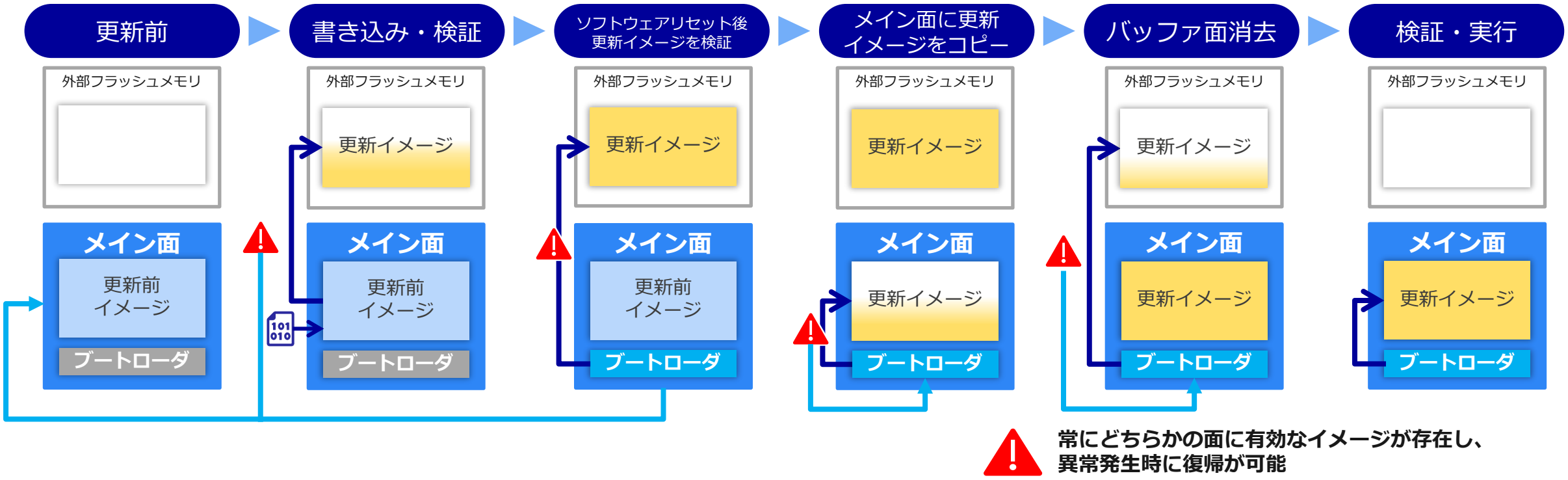
*1 : ソフトウェアリセットによる初期化対象は、各マイコンのハードウェアマニュアルの『リセット章』をご参照ください。
*2 : 外部フラッシュへの書き込み処理の詳細は、各ファミリ（RX、RL78）のSerial NOR Flash Memory制御モジュールのアプリケーションノートを参照ください。

3．リニアモード
全面更新方式（バッファ有り）：異常発生時の動作

電源遮断／署名検証失敗などによりファームウェアアップデートに失敗した場合、
更新前のイメージを起動してファームウェアアップデートをやり直すことが可能

外部フラッシュメモリ（バッファ面）	無効	無効	有効	無効	無効
メイン面	有効	有効	無効	有効	有効

緑文字：起動可能な状態／**黒文字**：起動不能な状態



常にどちらかの面に有効なイメージが存在し、
異常発生時に復帰が可能

署名検証による安全なファームウェア更新を実現！

Renesas Image Generatorで出来ること：署名付き初期イメージおよび更新イメージの生成

Renesas Image Generatorで『ファームウェアへの署名』や『ブートローダとの結合』を容易に実現

1. お客様の事前準備

署名検証方式：**ECDSA NIST P-256の場合**
お客様ご自身で下記のデータを生成します

ECDSA 署名用の鍵ペアを生成

鍵生成ツール

公開鍵

秘密鍵

公開鍵と**秘密鍵**の鍵ペアを生成
当社サンプル鍵ペアは、OpenSSL(OSS)で生成しています

ファームウェアの作成

e² studio

アプリケーション 

ブートローダ 

アプリケーションと**ブートローダ**の
ソースコードに署名検証用 公開鍵を埋め込む

motファイルの生成

e² studioで各.motファイル生成

アプリケーション.mot

ブートローダ.mot

2. Renesas Image Generatorが実行

事前準備したファイルをインプットするだけで、
初期イメージを簡単に生成できます

ヘッダアドレス情報の作成

Renesas Image Generatorは、対象MCUデバイスのアドレス情報を含むパラメータファイルを用いて、ヘッダアドレス情報を**RSU**として作成

RSUヘッダアドレス情報

※**RSU**＝Renesas Secure Updateでルネサス独自のデータ方式でmotファイルよりサイズが軽量で、通信量を抑制します

コード署名情報を付与

秘密鍵(Pvt.)を用いて、RSUヘッダアドレス情報とアプリケーション.motに署名を付与

RSUヘッダアドレス情報

アプリケーション.mot

＋ 

署名用

コード署名情報を付与

3. 初期イメージの生成完了

Renesas Image Generatorが
RSU, アプリケーション, ブートローダを統合して、
初期イメージ(.mot)を生成します

➢ **初期イメージ(.mot)**

RSUヘッダ署名情報
（0x200バイト）

RSUヘッダアドレス情報
（0x100バイト）

アプリケーション
プログラムのデータ

ブートローダ
（コードフラッシュのデータ）

4.以降、更新イメージ（.rsu）の生成

Renesas Image Generatorで同様に生成可能
詳細な手順・実際の運用はアプリケーションノート（RX, RL78）をご参照ください。

RA & RX 向けMCUboot ソリューション

ファームウェアアップデートの役割と実装ステップ

お客様が鍵ペアをご用意、Renesasはツールやドライバで安全な署名・FW更新を支援します

ファームウェアアップデートに必要な「順序」に沿った「実装」を実現するソリューション

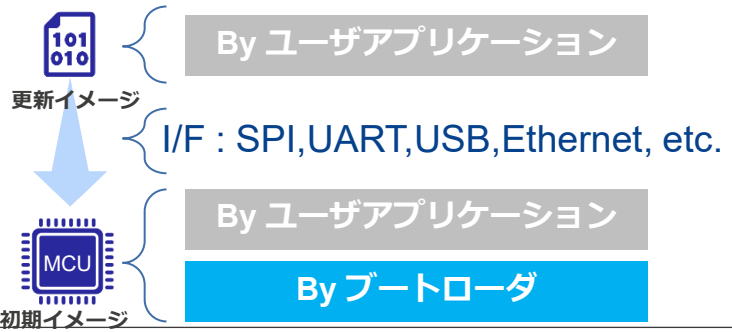
ファームウェアアップデートの 順序

①通信インタフェースを介して
更新イメージを MCU に取り込む

②更新イメージをMCU内蔵フラッシュに
書き込む

③更新イメージの正当性を検証する

④更新イメージを有効化する



ファームウェアアップデートの 実装

ブロックの色分け：お客様にご準備いただく工程 / ルネサスがサービス提供する工程

1. ファームウェアイメージの作成

- ✓コード署名のための鍵を生成
- ✓イメージを暗号化するための鍵を生成
- ✓ブートローダとユーザアプリの統合
- ✓イメージの暗号化、コード署名検証データの生成

2. ファームウェアアップデートの実行

- ✓更新イメージをMCUに取り込むための通信制御
- ✓更新イメージ復号, MCU内蔵フラッシュへ書込み
- ✓コード署名検証による更新イメージの正当性検証
- ✓更新イメージの有効化

※コード署名検証のアルゴリズムはMCUによって異なります。

鍵ペアの生成
本サンプルソフトではOpenSSL(OSS)ツールを利用してサンプル鍵を生成しています

ルネサス提供

MCUboot
“imgtool”

＋

MCUboot

＋

ユーザアプリケーション

セキュリティエンジン* 内蔵MCUを用いてセキュアなファームウェアアップデートを実現する “ MCUboot “ ソリューション

＊：TSIP/RSIP/SCE

ルネサス製セキュリティエンジン* を活用して暗号処理性能の向上とセキュアな鍵管理の両立を実現！

■ MCUboot (OSS)

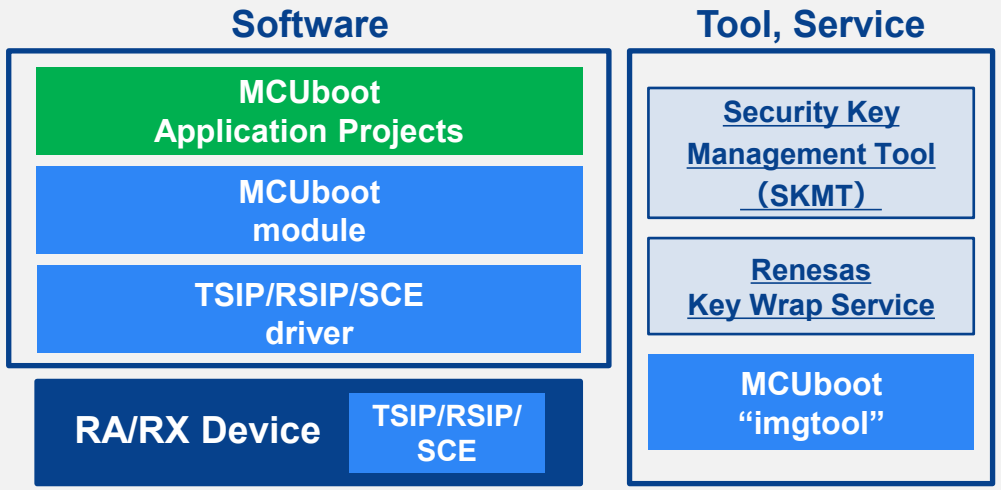
- ✓ 32-bit MCU向けの**セキュアブートローダ**
- ✓ ブートローダとシステムフラッシュのインフラストラクチャ標準化を目的とした**オープンソースソフトウェア**
- ✓ 様々なハードウェアやOSと統合できる柔軟な設計
- ✓ IoTオペレーティングシステムの主要なブートローダ

参考：MCUboot | mcuboot
GitHub - mcu-tools/mcuboot: Secure boot for 32-bit Microcontrollers!

■ セキュリティエンジン（TSIP / RSIP / SCE）

- ✓ **署名検証による安全なFW更新**
- ✓ **暗号処理能力の向上**
  Renesas MCU搭載のセキュリティエンジンを利用することで、**処理速度の向上、消費電力の削減、負荷の軽減** が可能
- ✓ **鍵データの保護**
  署名検証や復号に使われる鍵は、**ラッピングして保存**
- ✓ **セキュアな鍵の管理**
  Renesas提供の**SKMT**や**Renesas Key Wrap Service** により セキュアな鍵インジェクションをサポート

Renesas Deliverables



TSIP：Trusted Secure IP, RSIP：Renesas Secure IP, SCE ：Secure Crypto Engine

対応デバイス

RAファミリ：RA4, RA6, RA8 のセキュリティエンジン搭載品
RXファミリ：RX261, RX65N, RX651, RX66N, RX671, RX72M, RX72N

RAおよびRX MCUbootソリューションの機能と構成

セキュリティエンジン*1 と連携した MCUboot moduleでセキュアなファームウェアアップデートを実現

*1 : TSIP/RSIP/SCE

署名検証：セキュリティエンジン(TSIP/RSIP/SCE)

起動時ファームウェアの署名検証
MCU起動時にファームウェアの正当性を確認

更新ファームウェアイメージの署名検証
すべての更新ファームウェア受信後*に正当性を確認
* 更新ファームウェアイメージを暗号化している場合、復号処理を含む

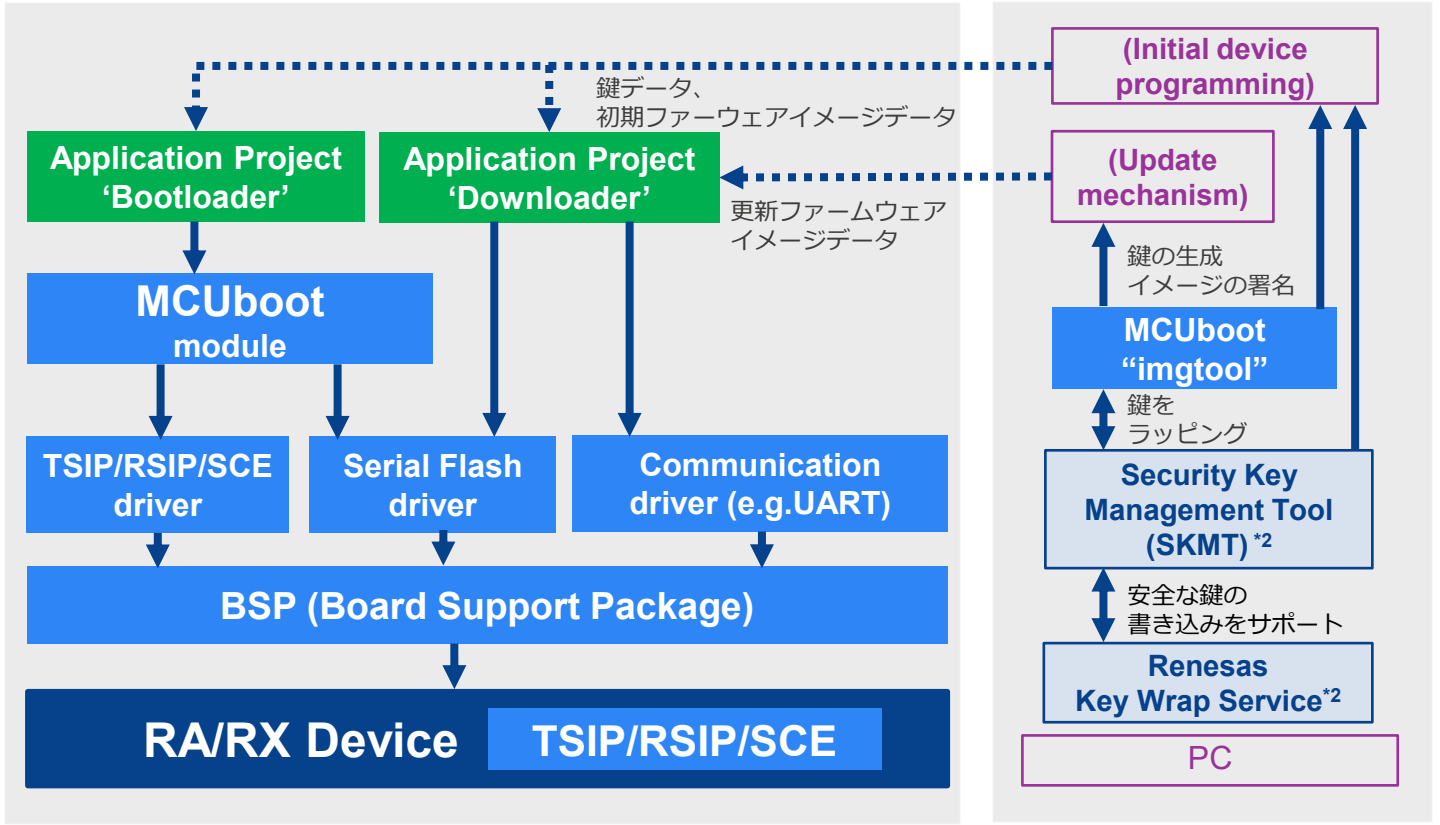
署名検証方式

RA	RX
[SCE/RSIP搭載品] ECDSA NIST p256 + SHA256 ECDSA NIST p384 + SHA384 RSA 2048 + SHA256 RSA 3072 + SHA256	[RSIP搭載品] ECDSA NIST p256 + SHA256 [TSIP搭載品] ECDSA NIST p256 + SHA256 RSA 2048 + SHA256

使い方ガイドとサンプルプログラム

・MCUbootモジュールガイド（RA FSP / RX FIT）
・サンプルプログラム（ルネサスWebページに掲載）

ブートローダーおよびデモアプリケーションのシステム構成



*2 : SKMT is required for Protected Mode only

本ページはRAファミリのみ対象です

セキュアなFW UPを実現するMCUbootソリューション

ルネサス製セキュリティエンジンが非搭載品では、ソフトウェア暗号ライブラリ（FSP MCUboot module）で実現！

■ MCUboot (OSS)

- ✓ 32-bit MCU向けの**セキュアブートローダ**
- ✓ ブートローダとシステムフラッシュのインフラストラクチャ標準化を目的とした**オープンソースソフトウェア**
- ✓ 様々なハードウェアやOSと統合できる柔軟な設計
- ✓ IoTオペレーティングシステムの主要なブートローダ

参考：MCUboot | mcuboot, GitHub - mcu-tools/mcuboot: Secure boot for 32-bit Microcontrollers!

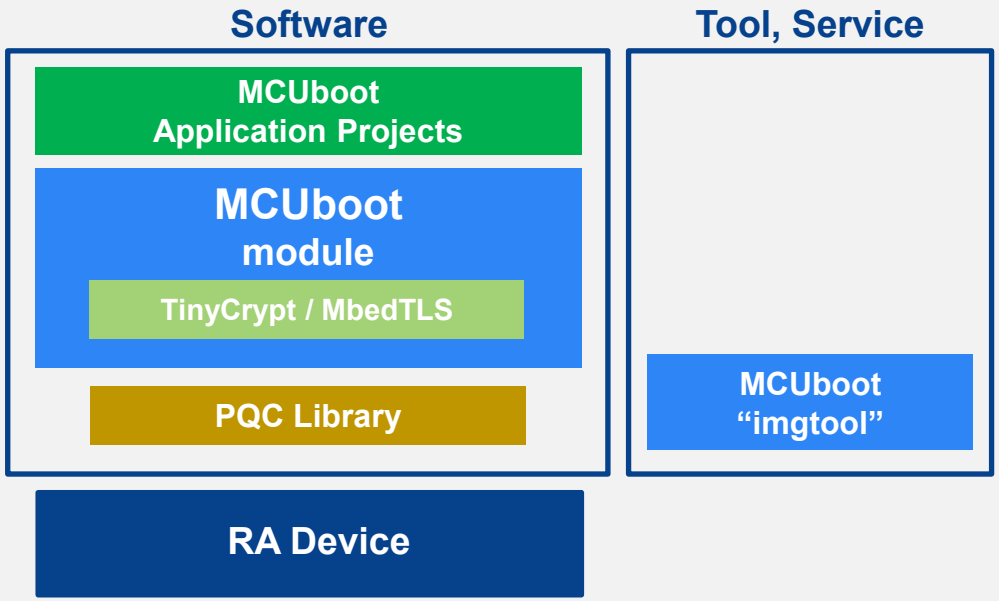
■ ソフトウェア暗号ライブラリ（FSP MCUboot module）

- ✓ **署名検証による安全なFW更新**
  セキュアエンジン**非搭載**のRAファミリMCU群では、
  FSPのソフトウェア暗号ライブラリを利用することで実現可能
- ✓ **PQC（耐量子暗号）にも対応** NEW
  NIST(米国国立標準技術研究所) では2035年以降に上市するDigital製品のPQC対応を推奨。RA/FSP MCUbootではv6.4.0以降でPQCを利用可能。

<ソフトウェア暗号ライブラリ>

- RA0, RA2シリーズ　：MCUboot の **TinyCrypt** を利用
- RA4, RA6, RA8シリーズ　：MCUboot の **MbedTLS** を利用
- RAファミリ　：ルネサス製の**PQC Library**を利用

Renesas Deliverables



対応デバイス

RAファミリ：RA0, RA2, RA4, RA6, RA8の全シリーズ
RXファミリ：-（セキュリティエンジン非搭載製品では、ファームウェアアップデートモジュールをご利用ください）

本ページはRAファミリのみ対象です

RA MCUbootソリューションの機能と構成

暗号ソフトウェア FSP MCUboot module でセキュアなファームウェアアップデートを実現

署名検証：ソフトウェア

起動時ファームウェアの署名検証
MCU起動時にファームウェアの正当性を確認

更新ファームウェアイメージの署名検証
すべての更新ファームウェア受信後に正当性を確認

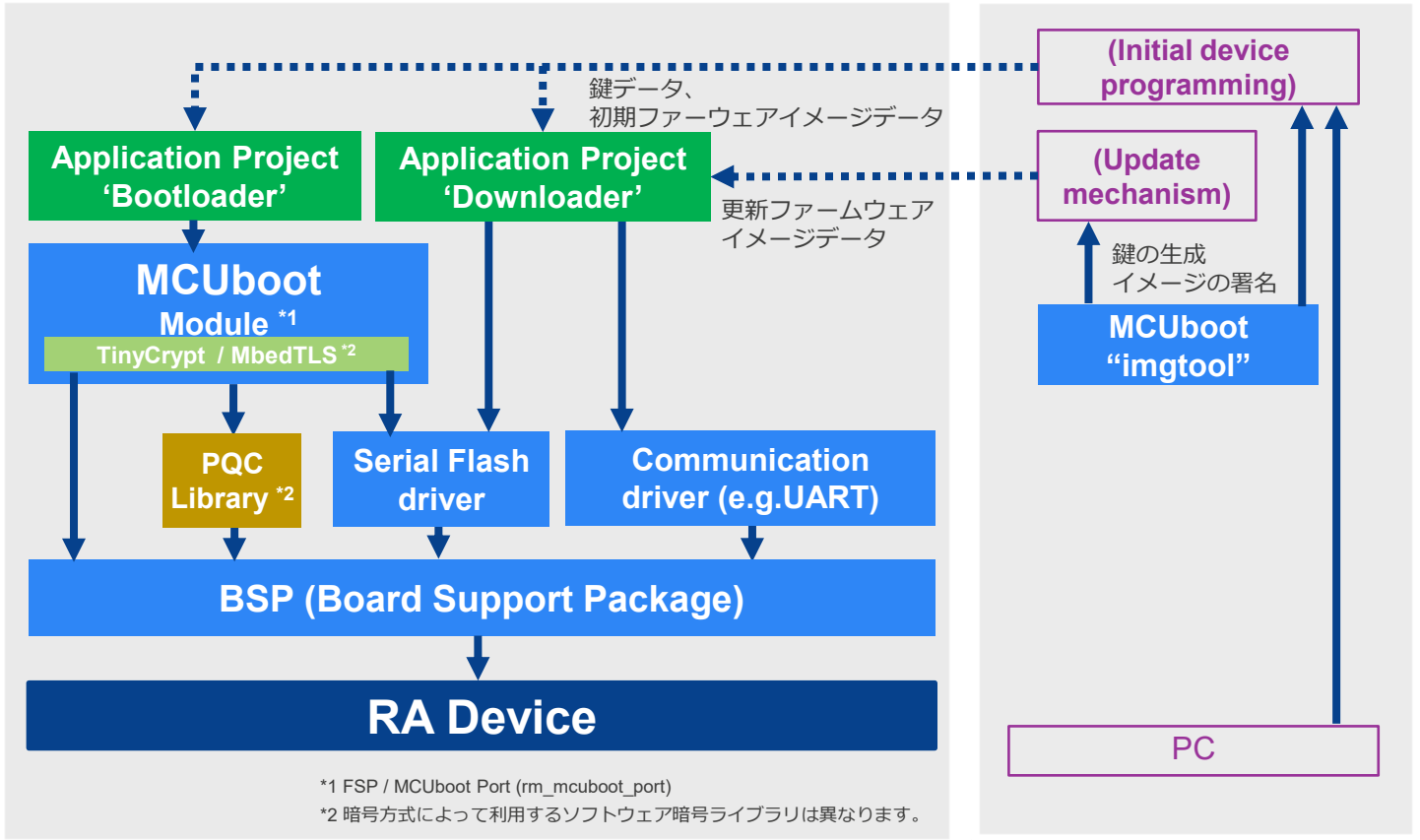
署名検証方式

RA	RX
➢ **RA0, RA2 (TinyCrypt):** ECDSA NIST p256 + SHA256 ➢ **RA4, RA6, RA8 (MbedTLS):** ECDSA NIST p256 + SHA256, ECDSA NIST p384 + SHA384, RSA 2048 + SHA256, RSA 3072 + SHA256 ➢ **RAファミリ (PQC Library) :** ML-DSA-44/65/87	- セキュリティエンジン非搭載品では、ファームウェアアップデートモジュールをご利用ください

使い方ガイドとサンプルプログラム

・MCUbootモジュールガイド（RA FSP）
・サンプルプログラム（ルネサスWebページに掲載）

ブートローダーおよびデモアプリケーションのシステム構成

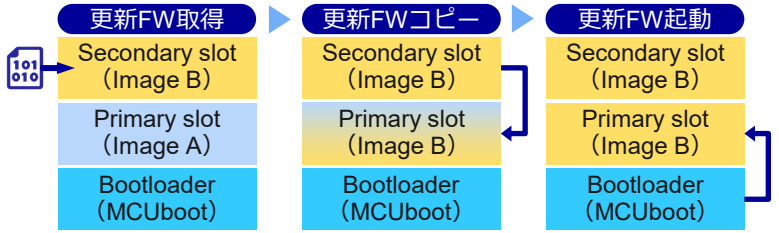
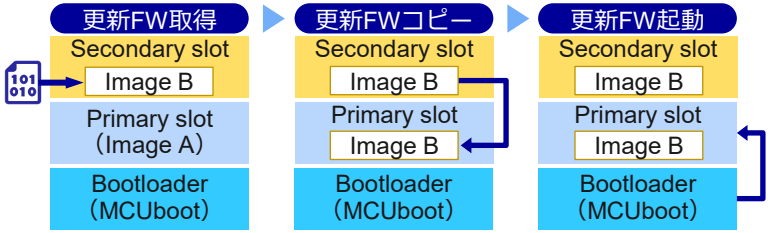
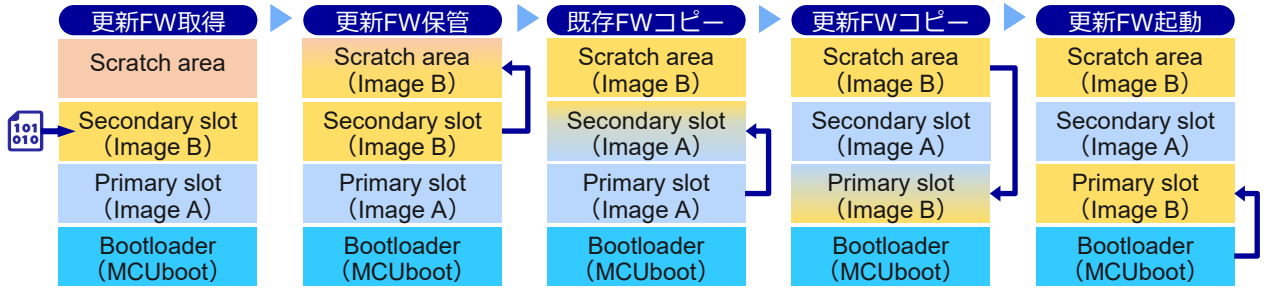
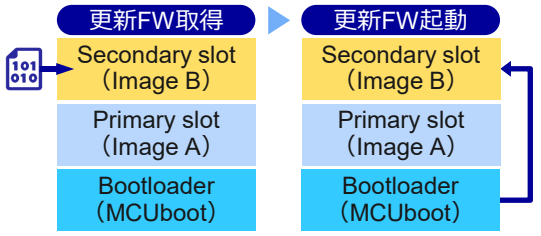
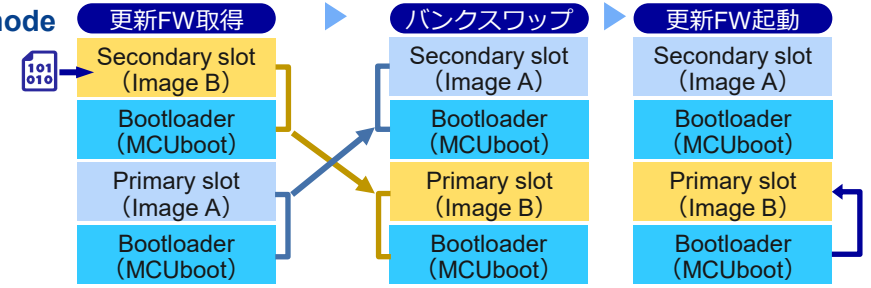


*1 FSP / MCUboot Port (rm_mcuboot_port)
*2 暗号方式によって利用するソフトウェア暗号ライブラリは異なります。

RA & RX MCUboot ファームウェア更新方式

更新FWの取得処理は、Primary slotのユーザアプリケーションの中（Flash ROM上）で実行されます。ただし、Linear mode時のFlash書き換え処理はすべてRAM上で実行されます。

お客様システムのユースケースに応じてMCUbootの各アップデート方式を選択可能！

更新方式	更新手順	特徴およびメリット
Overwrite Only Method	**Overwrite Only (Linear mode)**  Secondary Slot 全体を Primary slot全体にコピー **Overwrite Only Fast (Linear mode)**  更新FWサイズのデータのみSecondary slot からPrimary slotにコピー	✓ 省メモリフットプリント ✓ 更新イメージを直接上書き ✓ 更新イメージ暗号化可能
Swap Method	**Linear mode** 	✓ 更新イメージの暗号化可能
DirectXIP Method	**Linear mode**  **Dual mode** 	✓ コピーなどのデータ移動不要で高速なアップデートが可能

MCUbootは更新ファームウェア作成時に定義したバージョン情報確認と署名検証を行い、常に最新の更新ファームウェアイメージを起動します

Renesas.com

付録：
ファームウェアアップデート関連ソリューションのご紹介

IOT製品でのファームウェアアップデートにも最適なRENESAS MCU

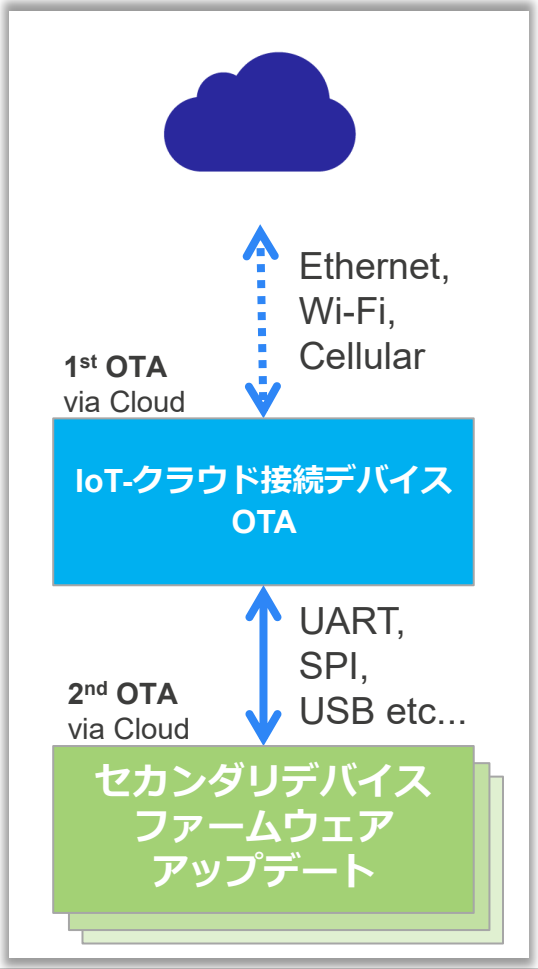
Renesas IoT Cloud

クラウドを経由したOTA（Over the Air）によるファームウェアアップデートにも対応！

MCU Family	セカンダリデバイス ファームウェア アップデート	IoT-クラウド接続デバイス OTA
RENESAS RA	RA0, RA2, RA4 Series Non-RTOS	RA6, RA8 Series MQTT / OTA / TLS / TCP/IP*1, Fleet Provisioning (Coming soon) FreeRTOS
RENESAS RX	RX100/200 Series Non-RTOS	RX65N MQTT / OTA / TLS / TCP/IP*1 / Fleet Provisioning FreeRTOS
RENESAS RL78	RL78/G22, RL78/G23, RL78/G24, RL78/L23 Non-RTOS 本資料で紹介	RL78/G23 MQTT / OTA / FreeRTOS *2

*1 : Ethernet(MCU) Only

*2 : これらコンポーネントをRL78/G23(max ROM 768KB, RAM 48KB)でご利用いただく場合、お客様アプリでご利用可能なRAMサイズが10KB未満になる可能性があります。



ファームウェアアップデート関連ソリューション一覧

		RX	RL78
セカンダリデバイス ファームウェアアップデート	ファームウェアアップデートモジュールサンプルコード	✓ RX Family Firmware Update module Using Firmware Integration Technology Application Notes - Sample Code	✓ RL78/G22, RL78/G23, RL78/G24, RL78/L23 Firmware Update Module
	ファームウェアアップデート通信モジュール	✓ RX ファミリ ファームウェアアップデート通信モジュール Firmware Integration Technology	✓ RL78/G22, RL78/G23 ファームウェアアップデート通信モジュール
IoT-クラウド接続デバイス OTA	セカンダリデバイスOTAファームウェアアップデートサンプルコード	✓ RX65Nグループ FreeRTOSを用いたAmazon Web ServicesによるセカンダリデバイスのOTAアップデートサンプルコード	✓ RL78/G23 FreeRTOSを用いたAmazon Web ServicesによるセカンダリデバイスのOTAアップデートサンプルコード
	OTAファームウェアアップデートサンプルコード	✓ RXファミリ Amazon Web Servicesを利用したFreeRTOS OTAの実現方法(202406-LTS版)	✓ Getting Started Guide for Connecting Amazon Web Services in Wi-Fi Communication: RL78/G23-128p Fast Prototyping Board + FreeRTOS
	開発支援ツール	✓ ファームウェアアップデート向け開発支援ツール QE for OTA	

ワイヤレスモジュールを活用した ファームウェアアップデート関連ソリューション一覧

		RX	RL78
Wi-Fi	Wi-Fi DA16600モジュール MCUファームウェア アップデート コマンドを利用	✓ RX Family AWS Cloud Connectivity for MCU Firmware Update Over-the-Air on RX65N Cloud Kit Board with Wi-Fi DA16600 Application Note | Sample Code	✓ RL78/G23 AWS Cloud Connectivity for MCU Firmware Update Over-the-Air on RL78/G23-128p Fast Prototyping Board with Wi-Fi DA16600 | Sample Code
Bluetooth LE	Bluetooth LE DA14535/DA14531モジュールの Renesas SUOTAサービスを利用	✓ RX Family Renesas Firmware Update Over the Air (FOTA) Sample Program With Bluetooth Low Energy DA14535/DA14531 Application Note | Sample Code	✓ RL78 Family Renesas Firmware Update Over the Air (FOTA) Sample Program With Bluetooth Low Energy DA14535/DA14531 Application Note | Sample Code

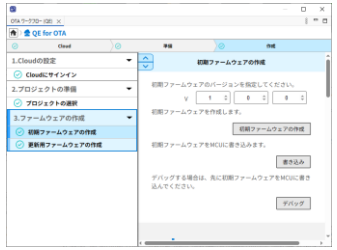
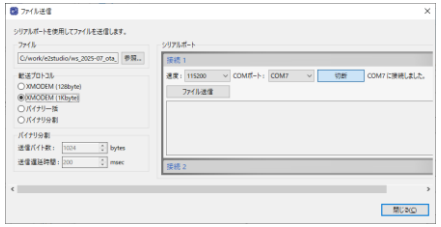
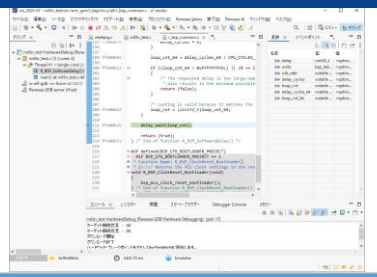
ファームウェアアップデート向け開発支援ツール QE for OTA

Over the Air （OTA）から<u>ローカルアプリケーションの更新</u>まで、
様々なシステム構成でのファームウェアアップデートを簡単なGUI操作だけで実現！

クラウドサービス（AWS）連携の有無		アップデート対象		アップデート方式		
クラウドあり	クラウドなし	プライマリ	セカンダリ	デュアルバンク方式	半面更新方式	全面更新方式
Wi-Fi / Ethernet	シリアル通信	FreeRTOS / non-OS	non-OS	Bank0 main Bank1 buffer	Single Bank main buffer	Single Bank main

Quick and Effective tool solution

1台のOTAに必要な操作時間を約86%削減、スムーズなPoC開発をサポート！

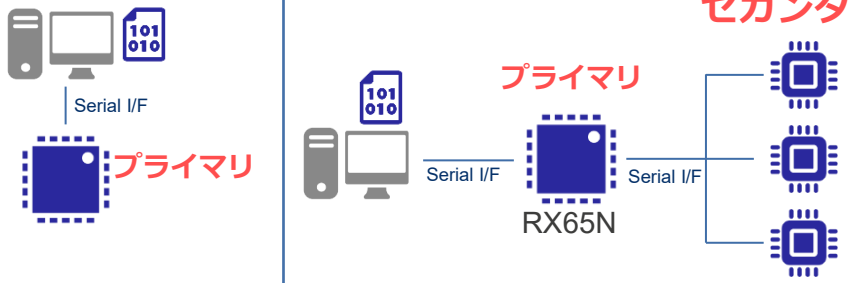
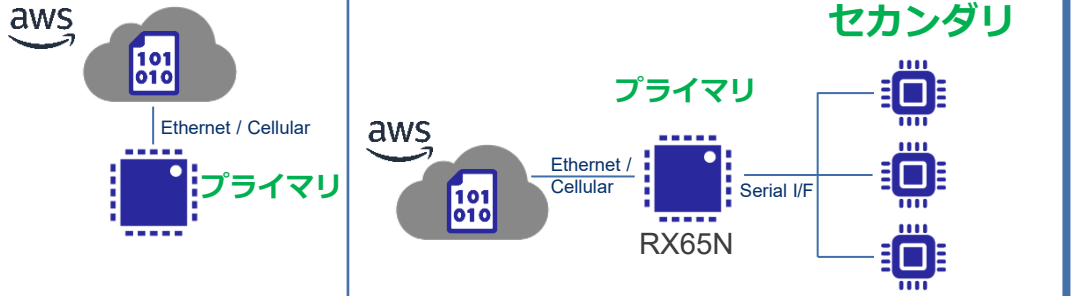
QE for OTA

ファームウェア、ブートローダの作成 → 署名検証用情報の生成・組み込み → ファームウェアアップデートの実行 → デバッグ

QE FOR OTA
対応デバイス一覧

QE for OTA

< 詳細情報>
- QE for OTA: Development Assistance for Cloud
- Firmware Update module

	クラウドを経由しないファームウェアアップデート			クラウド経由のOTAファームウェアアップデート		
						
FW UP対象	プライマリ	プライマリ	セカンダリ	プライマリ	プライマリ	セカンダリ
サポートデバイス	**<RA>** RA6M4, RA6M5 **<RX>** RX ファミリ – 全シリーズ **<RL78>** RL78/G22,G23,G24,L23	**<RX>** RX65N	**<RX>** RX23E-B, RX66T, RX660, RX261, RX140 **<RL78>** RL78/G23	**<RA>** RA6M5 **<RX>** RX65N **<RL78>** RL78/G23	**<RX>** RX65N	**<RX>** RX23E-B, RX66T, RX660, RX261, RX140 **<RL78>** RL78/G23
RTOS有無	non-OS	FreeRTOS, non-OS	non-OS	FreeRTOS	FreeRTOS	non-OS
更新方式	**< RA, RX >** デュアルバンク方式 **< RL78 >** 半面更新方式	**<RX>** 半面更新方式	デュアルバンク方式※1 半面更新方式 全面更新方式	**< RA, RX >** デュアルバンク方式 **< RL78 >** 半面更新方式	デュアルバンク方式	デュアルバンク方式※1 半面更新方式 全面更新方式
通信方式	シリアル通信※2			**< RA, RX >** Ethernet **< RL78 >** Cellular		シリアル通信※2

：更新FW置き場

※1：デュアルバンクモード対応製品のみ　※2：MCU間の通信には「ファームウェアアップデート通信モジュール (RX, RL78)」を使用