RX65N グループ
産業機器向けセキュアアップデートソリューション
スタートアップガイド

R01AN4506JJ0100
Rev.1.0.0
2018.12.19

要旨

本書は産業機器向けセキュアアップデートソリューション（以下、本ソリューション）を導入する際に必要な情報を記載したアプリケーションノートです。

本ソリューションは、アップデート対象機器（対象機器が導入されている工場など）を外部ネットワークに接続して行うのではなく、現状広く行われている保守員を介したアップデートを、セキュアに行えるようにしたソリューションです。

本ソリューションを用いて、お客様がプログラムを開発する際の具体的な実装方法については、ソリューション実装ガイド（R01AN4507JJ0100）を参照してください。

本ソリューションのプログラムを含む提供パッケージは、ルネサスマイコンをご採用/ご採用予定のお客様に提供させていただいています。お取引のあるルネサスエレクトロニクス営業窓口か、下記窓口にお問い合わせください。（https://www.renesas.com/jp/ja/support/contact.html）

動作確認デバイス

RX65N グループ

目次

1. 概要

1.1 はじめに

本書では、産業機器向けセキュアアップデートソリューションの概要と、使用する各ツールの操作方法について説明します。

1 章ではセキュアアップデートソリューションの概要を説明します。

2 章で各ツールの操作方法を説明します。

1.2 特長

現状の産業機器へのファームウェアアップデートは図 1-1 に示すように、保守員が記録媒体に保存されたプログラムを用いてアップデート対象機器を書き換える方法が主流です。しかし、この方法にはファームウェアの情報漏えいや改ざん、保守員のヒューマンエラーによる誤った機器へのアップデートやアップデート漏れ等のリスクがあります。

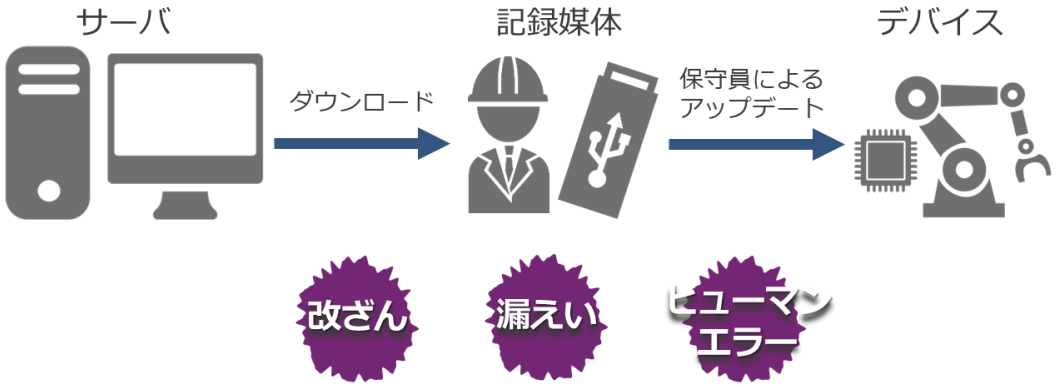

図 1-1 現状のファームウェアアップデートのイメージ

本ソリューションでは図 1-2 に示すように、数学的に安全性が証明された高信頼性プロトコル（特許出願済み）を採用することにより、これらのリスクを回避することができます。高信頼性プロトコルが備えるファームウェアの暗号化とメッセージ認証機能により、ファームウェアの情報漏えいや、改ざんを防ぎます。また、アップデート管理機能により誤った機器へのアップデートやアップデート漏れ等の保守員のヒューマンエラーを防止することが可能です。

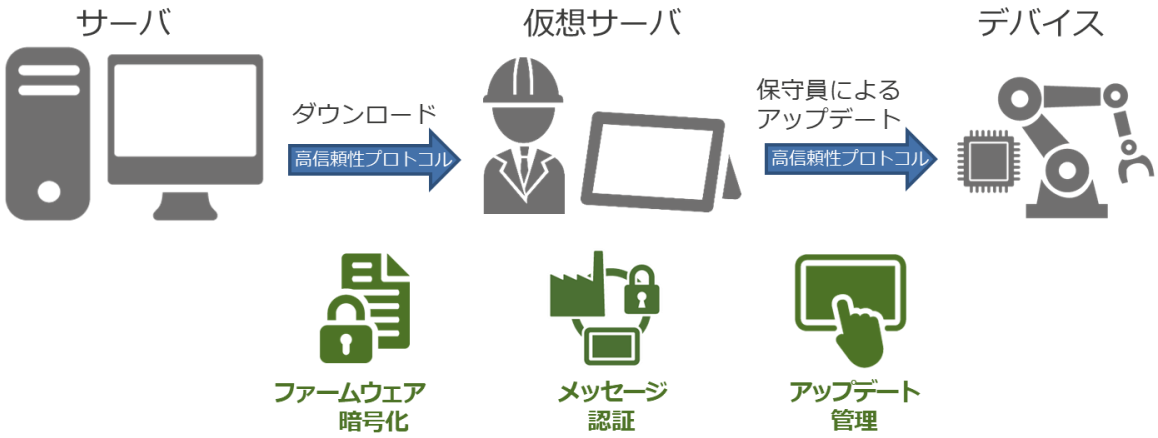

図 1-2 本ソリューションのファームウェアアップデートのイメージ

1.3　機能

本ソリューションには、大きく分けて量産用ファームウェア生成・書き込み機能とファームウェアアップデート機能があります。

量産用ファームウェア生成・書き込み機能は、設計・量産時にファームウェアアップデートに必要なデバイス側の準備を行う際に使用する機能です。

ファームウェアアップデート機能はフィールドでのアップデートを行う際に使用する機能です。

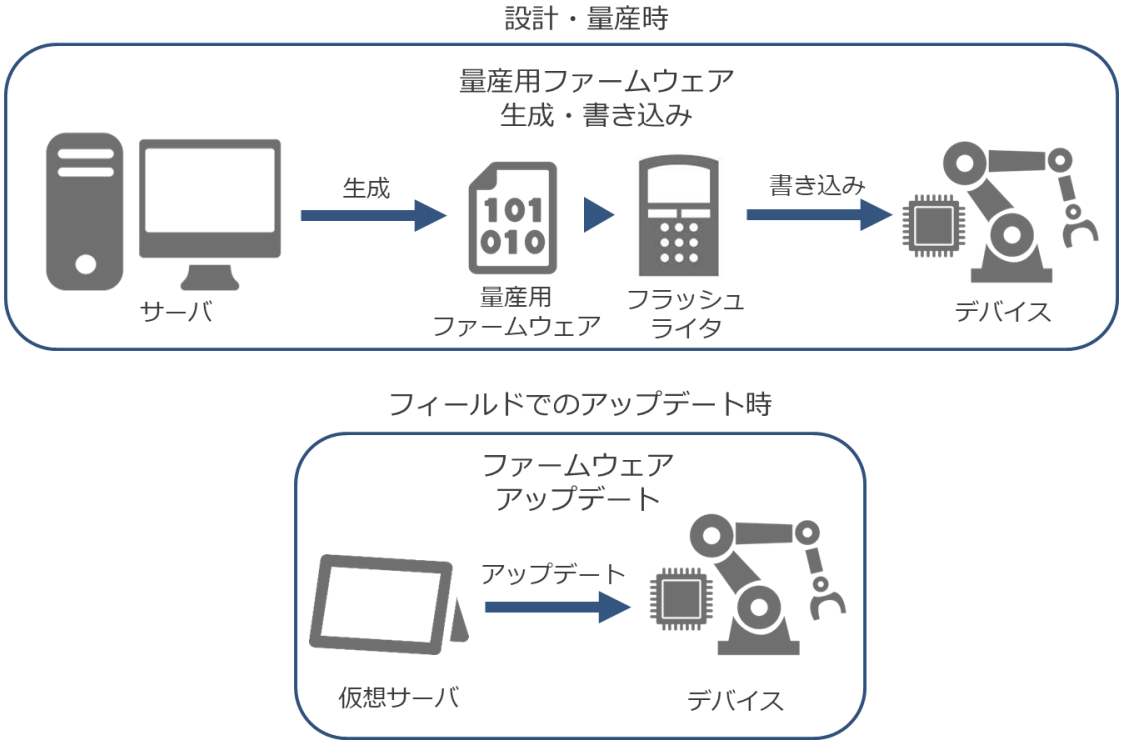

図 1-3 本ソリューションの機能

＜量産用ファームウェアの生成・書き込み機能＞

本機能には、ファームウェアアップデートを行うために必要なデバイス側の準備（鍵のインストールおよび、ユーザプログラム、アップデートプログラムの書き込み）をまとめて行える量産用ファームウェアの生成および書き込みを行う機能があります。

また、書き込まれた個々のデバイスから管理するために必要の情報を取得し、サーバ側にフィードバックする機能もあります。

＜ファームウェアアップデート機能＞

本機能には、仮想サーバを使いアップデート対象機器のファームウェアをセキュアにアップデートする機能があります。

また、アップデート状況を管理する機能もあります。

＜セキュリティ機能＞

暗号機能のアルゴリズムは AES の CBC モードを使用します。

メッセージ認証機能のアルゴリズムは CMAC を使用します。

1.4　提供パッケージ

本ソリューションで提供するパッケージの内容一覧を表 1.1 に、パッケージに含まれるソフトウェアのファイル構成を表 1.2 に示します。

表 1.1　パッケージ内容一覧

名称			説明
産業機器向けセキュアアップデートソリューションパッケージ			本パッケージには RX65N 用プログラムおよび Windows GUI ツール、ドキュメントが含まれます。
	PCツール	鍵生成ツール	ファームウェアアップデートで使用する鍵の生成
		ファームウェア管理ツール	ファームウェアの管理および量産用ファームウェアの生成
		アップデート管理ツール	ファームウェア管理ツールと連携しデバイスへのファームウェアアップデート実施
		ユニーク ID 読み出しツール	デバイス毎のユニーク ID 情報を読み出しユニーク ID 情報ファール生成
		PG-FP6 制御用マクロ	フラッシュプログラマ（PG-FP6）を制御するためのターミナルソフト用のマクロ
	デバイス	RX65N 用ファームウェアアップデートプログラム	ファームウェアアップデートプログラムとサンプルアプリを含むプロジェクト一式
		RX65N 用セキュアブートプログラム	RTOS 版または Non OS 版の RX65N 用セキュアブートプログラム(モトローラ S レコードフォーマットファイル)
	ドキュメント	スタートアップガイド	本ソリューションの概要およびツール類の操作方法に関するドキュメント
		ソリューション実装ガイド	本ソリューションを使ったファームウェアアップデートの実装方法に関するドキュメント

表 1.2 パッケージに含まれるソフトウェアのファイル構成

ファイル名	説明
¥¥Secure_firmware_Update¥Key_generator	
Secure_Firmware_Update_Key_Generator.exe	鍵生成ツール
Secure_Firmware_Update.mdb	ファームウェア管理用データベース
¥¥Secure_firmware_Update¥Firmware_Manager	
Secure_Firmware_Update_Firmware_Manager.exe	ファームウェア管理ツール
Secure_Firmware_Update.mdb	ファームウェア管理用データベース
¥¥Secure_firmware_Update¥Update_Manager	
Secure_Firmware_Update_Update_Manager.exe	アップデート管理ツール
Secure_Firmware_Update_Update_Manager.mdb	アップデート管理ツール用データベース
¥¥Secure_firmware_Update¥UID_Reader	
Secure_Firmware_Update_UID_Reader.exe	ユニーク ID 読み出しツール
¥¥Secure_firmware_Update¥FlashProgramer	
rx65n_write.ttl	PG-FP6 を制御するターミナルソフト用のマクロ
¥¥Secure_firmware_Update¥RX65N¥nonOS_rx65n_secure_boot	
nonOS_rx65n_secure_boot.mot	Non OS 版セキュアブートプログラム（ファームウェア生成用）
nonOS_rx65n_secure_boot_debug.mot	Non OS 版セキュアブートプログラム（デバッグ用）
¥¥Secure_firmware_Update¥RX65N¥rx65n_secure_boot	
rx65n_secure_boot.mot	RTOS 版セキュアブートプログラム（ファームウェア生成用）
rx65n_secure_boot_debug.mot	RTOS 版セキュアブートプログラム（デバッグ用）
¥¥Secure_firmware_Update¥RX65N¥nonOS_rx65n_app_prog	
Non OS 版 プロジェクト一式	Non OS 版 RX65N 用ファームウェアアップデートプログラム
¥¥Secure_firmware_Update¥RX65N¥rx65n_app_prog	
RTOS 版 プロジェクト一式	RTOS 版 RX65N 用ファームウェアアップデートプログラム
¥¥Secure_firmware_Update¥document	
r01an4506jj0100-rx65n.pdf	スタートアップガイド
r01an4507jj0100-rx65n.pdf	ソリューション実装ガイド

1.5　参照資料

本ソリューションで参照する資料を表 1.3 に示します。

表 1.3　マニュアル一覧

ドキュメント名	資料番号	リビジョン
産業機器向けセキュアアップデートソリューション スタートアップガイド	R01AN4506JJ0100	Rev.1.00
産業機器向けセキュアアップデートソリューション ソリューション実装ガイド	R01AN4507JJ0100	Rev.1.00
PG-FP6 V1.01 フラッシュメモリプログラマ ユーザーズマニュアル	R20UT4254JJ0100	Rev.1.00
Key Wrap サービス 操作マニュアル	―	Rev.1.03

1.6　ソリューション構築に必要な機材

本ソリューションを構築するために必要な機材を表 1.4 に示します。

表 1.4　必要機材一覧

名称	説明
鍵生成ツール用 Windows PC	鍵生成ツールを運用する Windows PC 注 1,2 です。
ファームウェア管理ツール用 Windows PC	ファームウェア管理ツールを運用する Windows PC 注 1,2 です。
アップデート管理ツール用 Windows PC	アップデート管理ツールを運用する Windows PC 注 2 です。
フラッシュライタ制御用 Windows PC	フラッシュライタ制御用の Windows PC 注 2 です。
フラッシュメモリ書き込みツール	量産用ファームウェアをデバイスに書き込む際に使用します。フラッシュメモリ書き込みツールの指定はありません。 ただ、フラッシュプログラマ（PG-FP6）であれば、提供パッケージに含まれる PG-FP6 制御マクロを使い、プログラムの書き込みとユニーク ID 情報の読み出しを一度に行うことができます。 PG-FP6 はルネサス製のフラッシュプログラマです。 (https://www.renesas.com/ja-jp/products/software-tools/tools/programmer/pg-fp6.html)
サンプルアプリ動作確認用ボード （Renesas Starter Kit+ for RX65N-2MB（Trusted Secure IP 搭載））	本ソリューションパッケージに含まれるサンプルアプリが動作するボードです。 Renesas Starter Kit+ for RX65N-2MB（Trusted Secure IP 搭載） （https://www.renesas.com/jp/ja/products/software-tools/boards-and-kits/renesas-starter-kits/renesas-starter-kitplus-for-rx65n-2mb.html） 本ソリューションを構築する上で必須となる機材ではありません。
ルネサス Key Wrap サービス	本システムは、ユーザが使用したい鍵をデバイス内に秘匿されている鍵を使い、ルネサスにて暗号化するサービスです。これによりデバイスへの鍵インストールを安全に行うことができます。 詳細は“Key Wrap サービス 操作マニュアル”を参照してください。

注 1）鍵生成ツールとファームウェア管理ツールは同じ PC で運用することが可能です。これにより必要な PC の台数を減らせるだけでなく、同じ PC の同じディレクトリで運用することにより鍵情報の同期（“2.2.6 鍵情報の同期”を参照）の手間を省くことができます。

注 2）各ツールは Windows10 環境で動作を確認しております。Windows10 以外の環境でご利用は、各自の判断で実施ください。

1.7　システム構成

本ソリューションのシステム構成を説明します。

1.7.1 に量産用ファームウェア生成・書き込みのシステム構成を、1.7.2 にファームウェアアップデートのシステム構成を示します。

システム構成に登場するサーバとは、本ソリューションで提供されているファームウェア管理ツールをインストールした Windows PC を指し、仮想サーバとは、アップデート管理ツールをインストールした Windows PC を指します。

1.7.1　量産用ファームウェア生成・書き込みのシステム構成

量産用ファームウェア生成・書き込みには、鍵の生成、量産ファームウェアの生成、デバイスへの量産ファームウェアの書き込み、デバイス管理に使用するユニーク ID 情報取得等があり、サーバ／フラッシュプログラマ／デバイスにより構成されます。

鍵を生成する際のシステム構成を図 1-4 に示します。

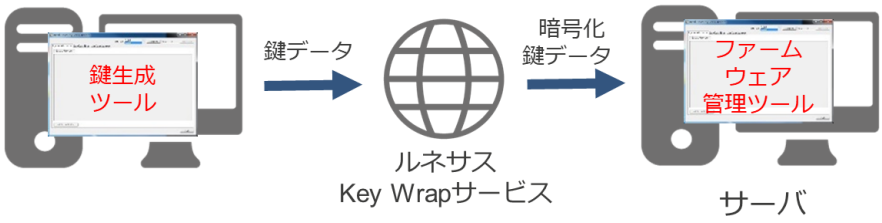

図 1-4 鍵生成のシステム構成図

量産ファームウェアを生成する際のステム構成を図 1-5 に示します。

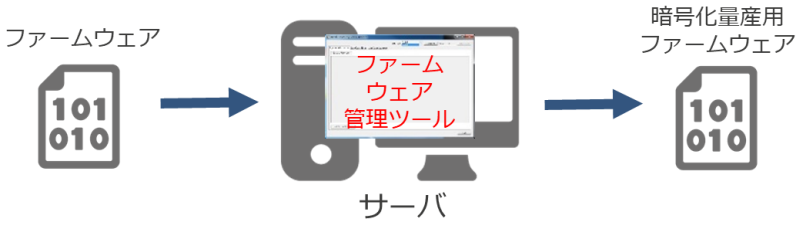

図 1-5 量産ファームウェア生成のシステム構成図

デバイスに量産ファームウェアを書き込む際のシステム構成を図 1-6 に示します。

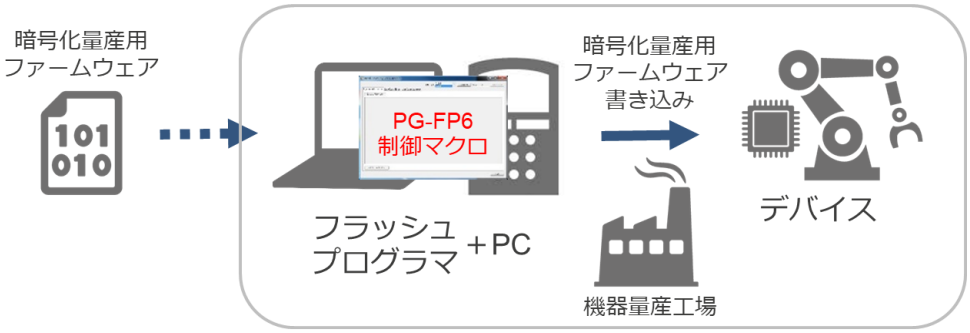

図 1-6 量産ファームウェア書き込みのシステム構成図

デバイスの管理に使用するユニーク ID 情報を取得する際のシステム構成を図 1-7 に示します。

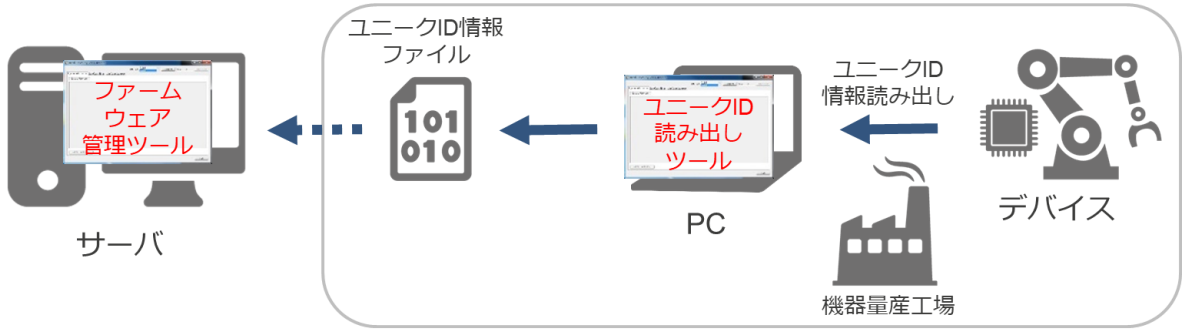

図 1-7 ユニーク ID 情報のフィードバックのシステム構成図

量産用ファームウェア生成・書き込みの詳細は“1.8 量産用ファームウェア生成・書き込みの流れ”を参照してください。

1.7.2　　ファームウェアアップデートのシステム構成

ファームウェアアップデート機能は、サーバ／仮想サーバ／デバイスにより構成されます。ファームウェアアップデートのシステム構成を図 1-8 に示します。

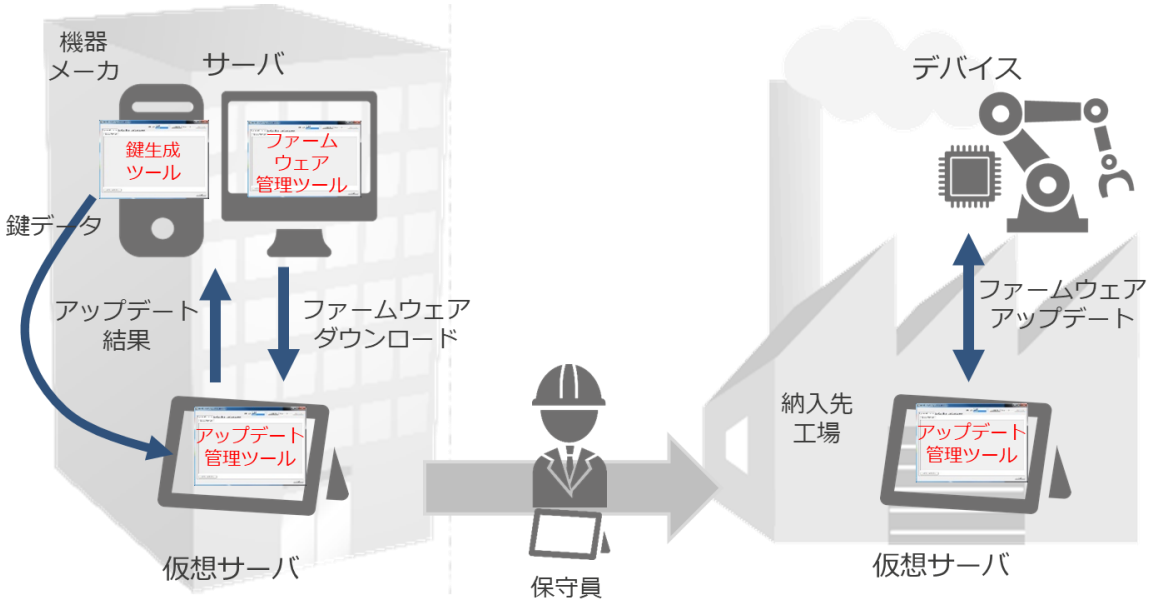

図 1-8 ファームウェアアップデートのシステム構成図

ファームウェアアップデートの詳細は“1.9 ファームウェアアップデートの流れ”を参照してください。

1.8　量産用ファームウェア生成・書き込みの流れ

量産用ファームウェアの生成およびデバイスへの書き込みのフローを図 1-9 に示します。

フローの詳細に関しては、図内に記載されている番号（①～⑧）と同じ番号の説明文を参照してください。また、操作方法の詳細に関してはフロー内に記載している章を参照してください。

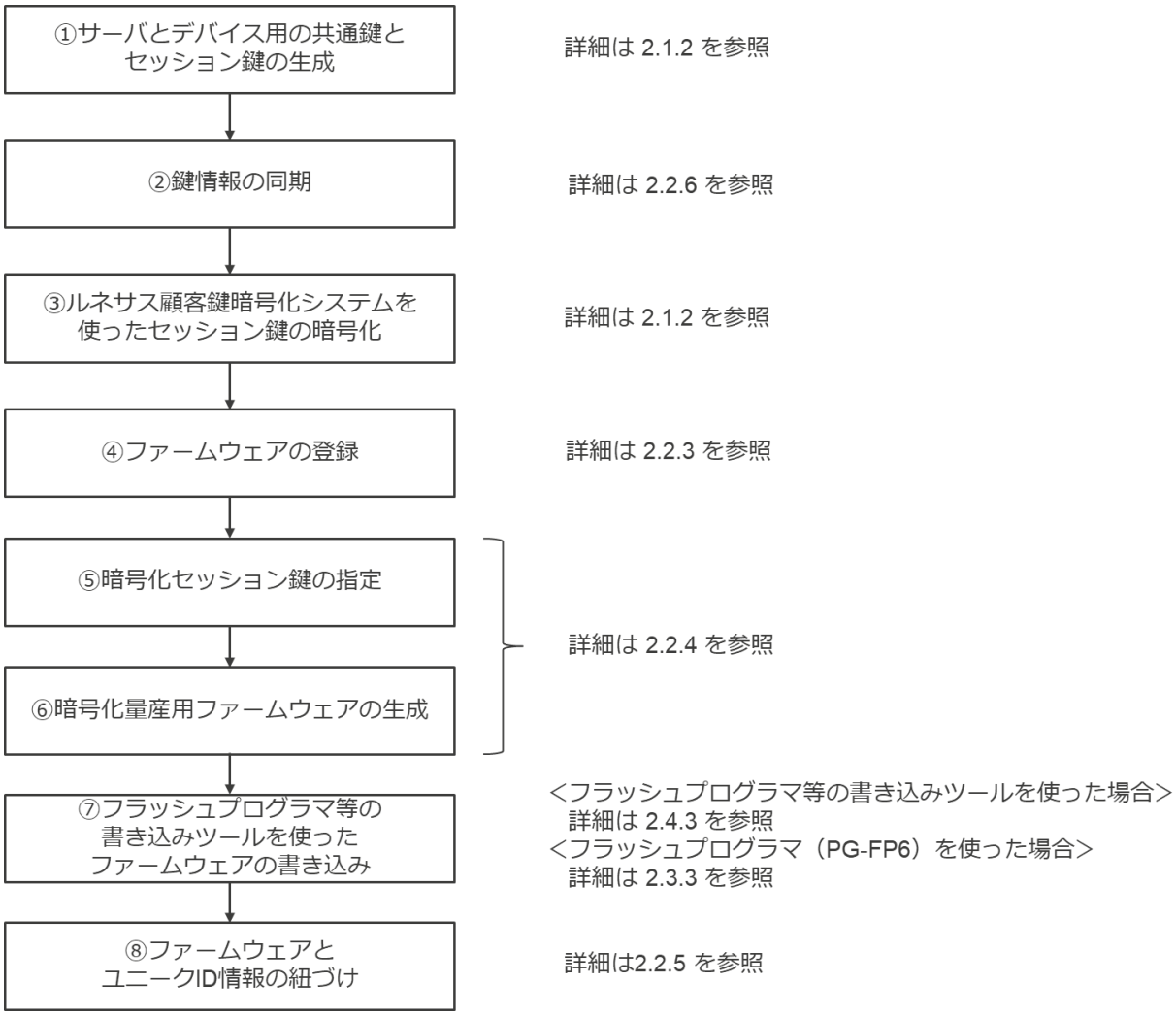

図 1-9 量産用ファームウェア書き込みフロー

量産用ファームウェアの生成およびデバイスへの通常の書き込みのイメージを図 1-10 に、点線部分に関して、PG-FP6 による書き込みのイメージを図 1-11 に示します。

イメージ図の詳細に関しては、図内に記載されている番号（①～⑧）と同じ番号の説明文を参照してください。

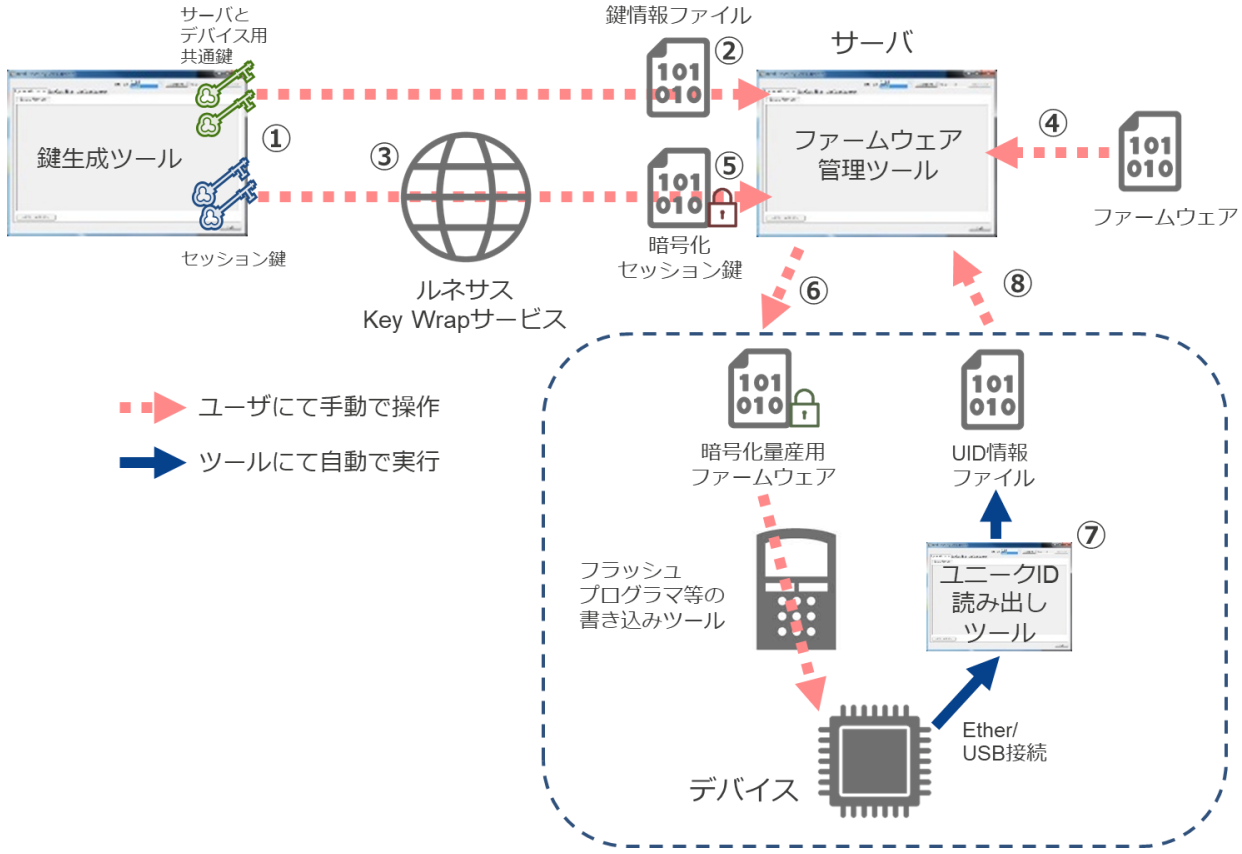

図 1-10 量産用ファームウェアの生成およびデバイスへの書き込みのイメージ

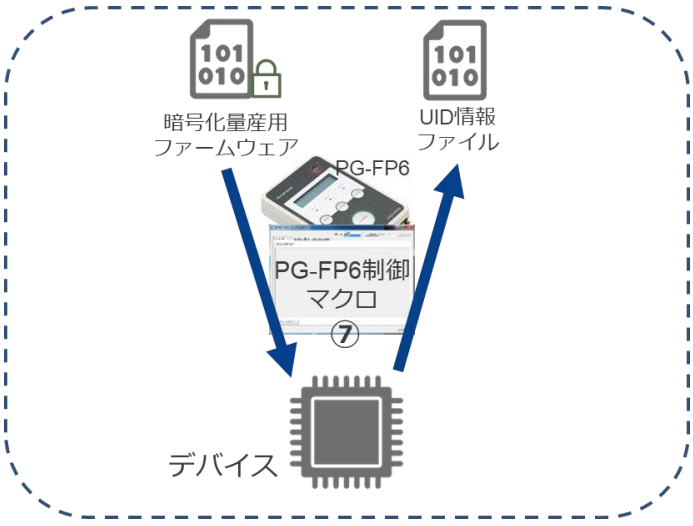

図 1-11 PG-FP6 による書き込みのイメージ

① サーバとデバイス用の鍵生成

鍵生成ツールを使いサーバとデバイスで使用する共通鍵を生成します。

鍵生成ツールに製品名（Products）を入力することにより、サーバとデバイスで使用する共通鍵（2 個）と、共通鍵を暗号化するためのセッション鍵（2 個）を生成します。

共通鍵はセッション鍵で暗号化され、その他の情報とまとめて鍵情報ファイルが生成されます。セッション鍵はそのままバイナリファイルとして出力されます。

② 鍵情報の同期

生成された鍵情報ファイルをファームウェア管理ツールに同期します。

鍵情報ファイルが出力されたディレクトリを、ファームウェア管理ツールが管理している鍵情報に上書きし鍵情報を同期させます。

（鍵生成ツールとファームウェア管理ツールを、同一 PC の同じディレクトリで運用することにより、鍵情報の同期作業を省くことができます）

③ ルネサス Key Wrap サービスを使ったセッション鍵の暗号化

ルネサスの Key Wrap サービスを使い、①で生成したセッション鍵を暗号化します。

④ ファームウェアの登録

ファームウェア管理ツールに、製品名（Products）とバージョン情報を指定し、ファームウェアを登録します。

⑤ 暗号化セッション鍵の指定

③で暗号化されたセッション鍵をファームウェア管理ツールに指定します。

⑥ 暗号化量産用ファームウェアの生成

ファームウェア管理ツールを使い、④で登録されたファームウェアをサーバとデバイスで使用する鍵で暗号化し、暗号化量産用ファームウェアを生成します。

⑦ フラッシュプログラマ等の書き込みツールを使ったファームウェアの書き込み

＜フラッシュプログラマ等の書き込みツールを使った場合＞

フラッシュプログラマ等の書き込みツールを使い、⑥で生成した暗号化量産用ファームウェアをデバイスに書き込みます。

デバイスを再起動させ暗号化された状態のファームウェアを復号します。

デバイスとユニーク ID 読み出しツールがインストールされた PC を Ether ケーブルまたは USB ケーブルで接続します。

ユニーク ID 読み出しツールを起動し、デバイスからユニーク ID 情報を読み出し、ユニーク ID 情報ファイルが生成されます。

＜フラッシュプログラマ（PG-FP6）を使った場合＞

PG-FP6 を使い、⑥で生成した暗号化量産用ファームウェアをデバイスに書き込みます。書き込みは、パッケージで提供される PG-FP6 制御マクロを使い PG-FP6 を制御し行います。マクロでの制御の流れは以下の通りです。

・デバイスに暗号化量産用ファームウェアを書き込む

・デバイスを再起動することにより、書き込まれたプログラムが自動的に暗号化された状態の量産用ファームウェアを復号しフラッシュに書き込む

・デバイス毎のユニーク ID（UID）を読み出し、ユニーク ID 情報ファイルを生成

⑧ ファームウェアとユニーク ID 情報の紐づけ

⑦で生成したユニーク ID 情報ファイルをファームウェア管理ツールに登録し、ファームウェアとユニーク ID を紐づけます。

1.9　ファームウェアアップデートの流れ

ファームウェアアップデートの全体の流れを図 1-12 に示します。

フローの詳細に関しては、図内に記載されている番号（①～⑥）と同じ番号の説明文を参照してください。また、操作方法の詳細に関してはフロー内に記載している章を参照してください。

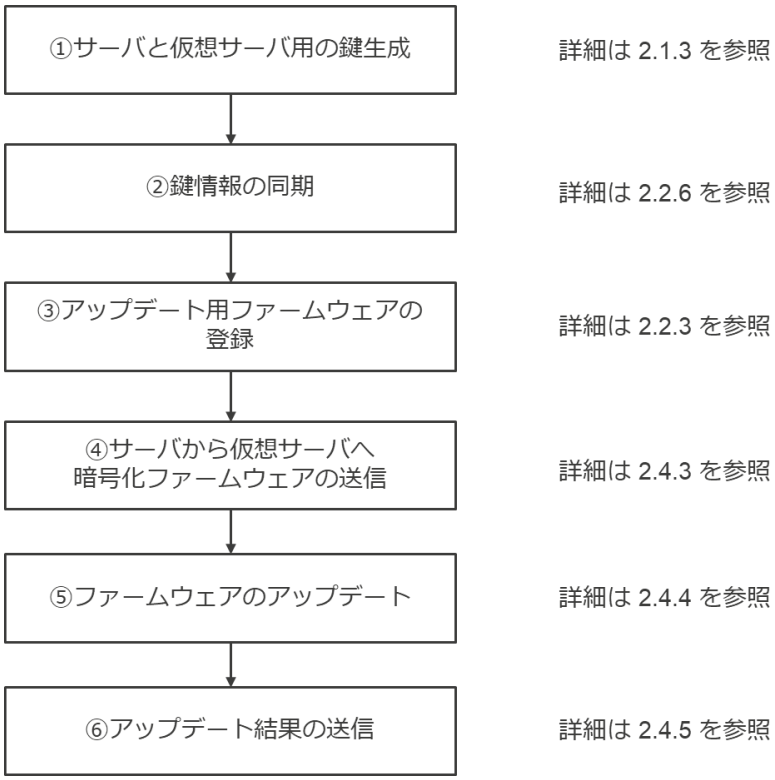

図 1-12 ファームウェアアップデートのフロー

ファームウェアアップデートのイメージを図 1-13 に示します。

イメージ図の詳細に関しては、図内に記載されている番号（①～⑥）と同じ番号の説明文を参照してください。

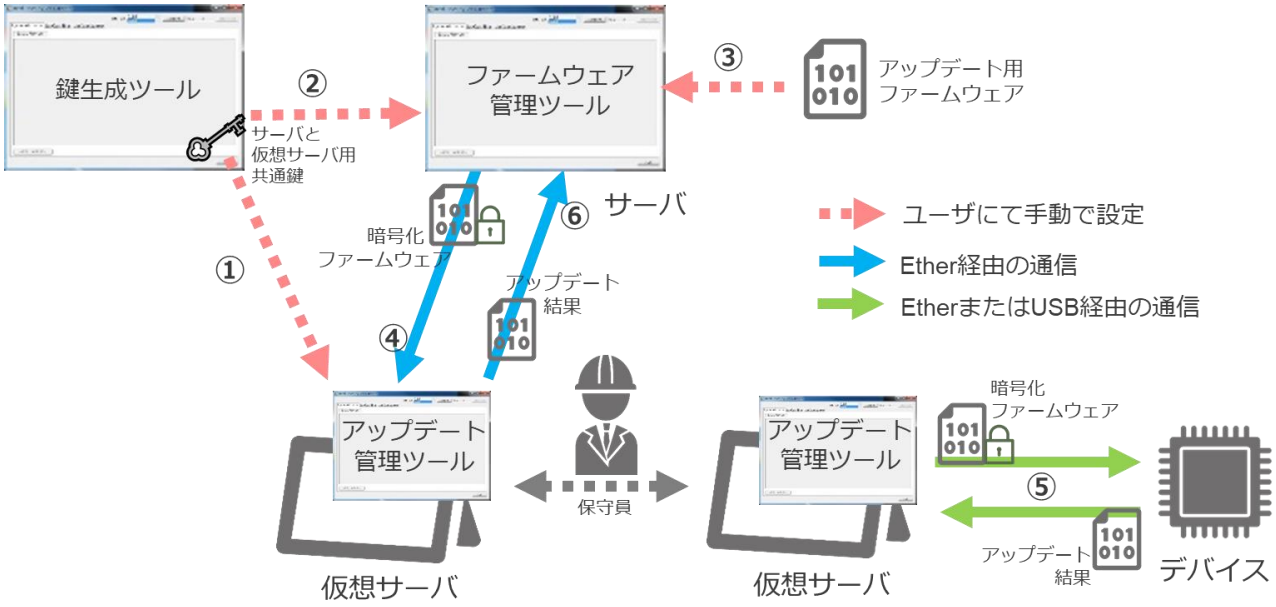

図 1-13 ファームウェアアップデートのイメージ

① サーバと仮想サーバの鍵生成

鍵生成ツールを使いサーバと仮想サーバで使用する共通鍵を生成します。

鍵生成ツールにアップデート管理ツール用 ID（指定範囲：1～65,535）を入力し、サーバと仮想サーバ用の共通鍵を生成します。

また、同時に鍵情報ファイル（バイナリファイル）が出力されるので、このファイルを使って仮想サーバに鍵情報のコピーが必要です。

② 鍵情報の同期

生成された鍵情報ファイルをファームウェア管理ツールに同期します。

生成された鍵のバイナリファイルが出力されているディレクトリを、ファームウェア管理ツールが管理している鍵情報に上書きし鍵情報を同期させます。

(鍵生成ツールと、ファームウェア管理ツールを同一の PC の同じディレクトリで運用することにより、鍵情報の同期作業を省くことができます)

③ アップデート用ファームウェアの登録

ファームウェア管理ツールに、製品名（Products）とバージョン情報を指定し、アップデート用ファームウェアを登録します。

④ サーバから仮想サーバへ暗号化ファームウェアの送信

仮想サーバとサーバを接続し、アップデート管理ツールで製品名を指定してサーバへファームウェアの送信要求を送信します。

その要求を受けサーバから仮想サーバへファームウェアを暗号化して送信されます。

ファームウェアの送信完了後、仮想サーバとサーバとの接続を解除してください。

⑤ ファームウェアのアップデート

仮想サーバとデバイスを接続し、アップデート管理ツールを使いデバイスのファームウェアアップデートを行います。仮想サーバとデバイス間で以下の処理を行います。

・仮想サーバとデバイスの相互の認証を実施

・仮想サーバからデバイスへ暗号化されたファームウェアを送信

・デバイスのファームウェアアップデート結果を仮想サーバに送信

・アップデート管理ツールでアップデート結果を GUI 上に表示

ファームウェアアップデート完了後、仮想サーバとデバイスの接続を解除してください。

⑥ アップデート結果の送信

仮想サーバとサーバを接続し、アップデート管理ツールを使用してファームウェアアップデートの結果をファームウェア管理ツールに送信します。

ファームウェア管理ツールでは取得したアップデート結果を GUI 上に表示します。

2. 各ツールの使い方

2.1 鍵生成ツール

本章ではセキュアアップデートで使用する鍵生成ツールについて説明します。

鍵生成ツールの機能は以下の通りです。

・サーバとデバイス用の共通鍵とセッション鍵の生成

・サーバと仮想サーバ用の共通鍵の生成

・サーバとデバイス用の共通鍵をセッション鍵で暗号化したデータの生成

2.1.1 鍵生成ツールのセットアップ

セキュアアップデートソリューションパッケージで提供されている以下のファイルを、鍵生成ツールを運用する Windows PC の任意のディレクトリにコピーしてください。

（鍵生成ツールは、ファームウェア管理ツールと同一の PC の同じディレクトリにコピーして運用することにより、鍵情報を同期する手間を省くことができます。その際、データベースファイル（Secure_Firmware_Update.mdb）はファームウェア管理ツールのファイルを使用してください）

Secure_Firmware_Update_Key_Generator.exe Secure_Firmware_Update.mdb

2.1.2 サーバとデバイスで使用する共通鍵の生成

サーバとデバイスで使用する共通鍵（2 個）と、共通鍵を暗号化するためのセッション鍵（2 個）を生成する方法を以下に示します。

サーバとデバイスの共通鍵は、1 製品（Products）に 1 セットの鍵を生成して管理します。

鍵に紐づくデバイスは、全て同じファームウェアによりアップデートが行われるため、アップデートの管理を分けたい場合には、異なる製品としてツールに登録してください。

① 鍵生成ツールを運用する Windows PC で、Secure_Firmware_Update_Key_Generator.exe を起動してください。

② Generate Device Key タブを選択し、[Products]の入力 BOX に製品名を入力してください。

ここでは例として“RX65N”と入力していますが、実際はお客様で使用したい任意のプロダクト名を入力してください。

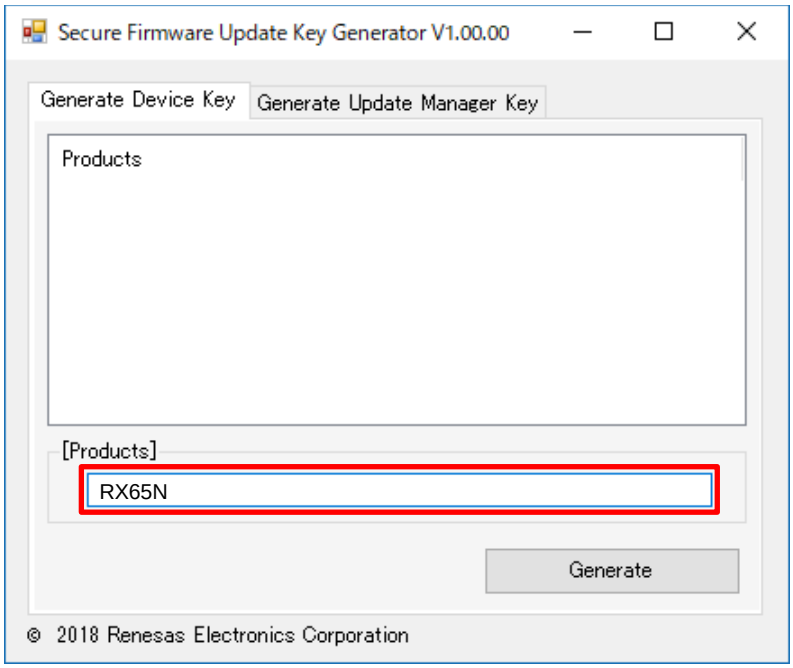

図 2-1 製品名入力 GUI イメージ

③ Generate ボタンを押してください。鍵が生成されます。

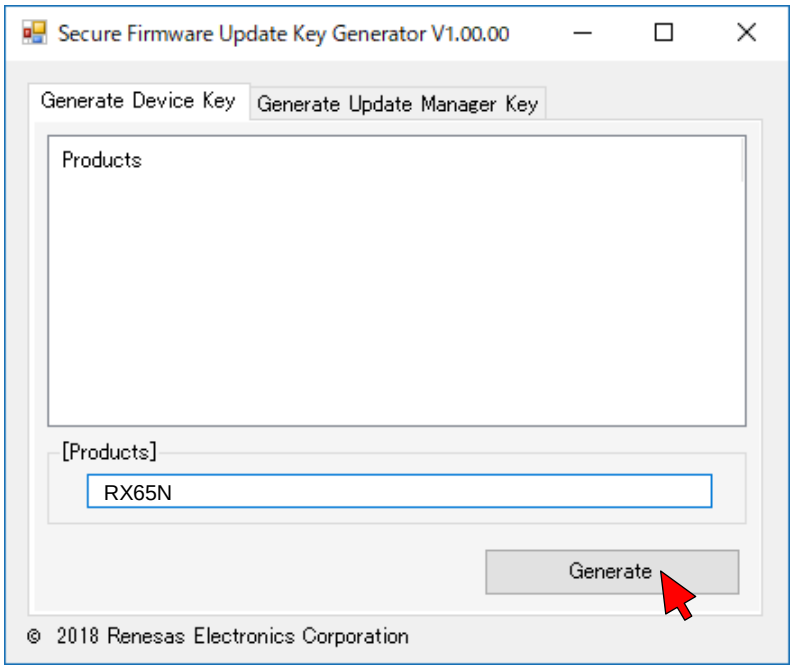

図 2-2 サーバとデバイス用鍵生成 GUI イメージ

鍵データは鍵生成ツールを起動したディレクトリの直下に以下のように生成されます。

¥KEY_FOLDER¥*products*¥*products*_session_key_MSK1.key
¥KEY_FOLDER¥*products*¥*products*_session_key_MSK2.key
¥KEY_FOLDER¥*products*¥*products*.dat

products：[Products]に入力した製品名

④ 上記③で生成した鍵（*products*_session_key_MSK1.key、*products*_session_key_MSK2.key）を、ルネサス Key Wrap サービスに送信して、RX65N 用に暗号化されたデータを取得してください。

2.1.3 サーバと仮想サーバで使用する共通鍵の生成

サーバと仮想サーバで使用する共通鍵の生成方法を以下に示します。

サーバと仮想サーバの共通鍵は、仮想サーバ毎に 1 セットの鍵を生成して管理しています。そのため複数の仮想サーバがある場合は、それぞれの仮想サーバ用に鍵を生成しください。

仮想サーバはそれぞれ異なる UMID を設定する必要があります。異なる仮想サーバに同じ UMID を設定し運用するとサーバでの管理に問題が発生するため、仮想サーバ毎に必ず異なる UMID を設定してください。特に問題がなければ、仮想サーバ毎にシリアルに番号を設定することをお勧めします。

① 鍵生成ツールを運用する Windows PC で、Secure_Firmware_Update_Key_Generator.exe を起動してください。

② Generate Update Manager Key タブを選択し、[UMID]の入力 BOX にアップデート管理ツール用 ID（指定範囲：1～65,535）を入力してください。（アップデート管理ツール用 ID は複数指定可能*注 1 で仮想サーバ毎に ID が被らないように指定してください）

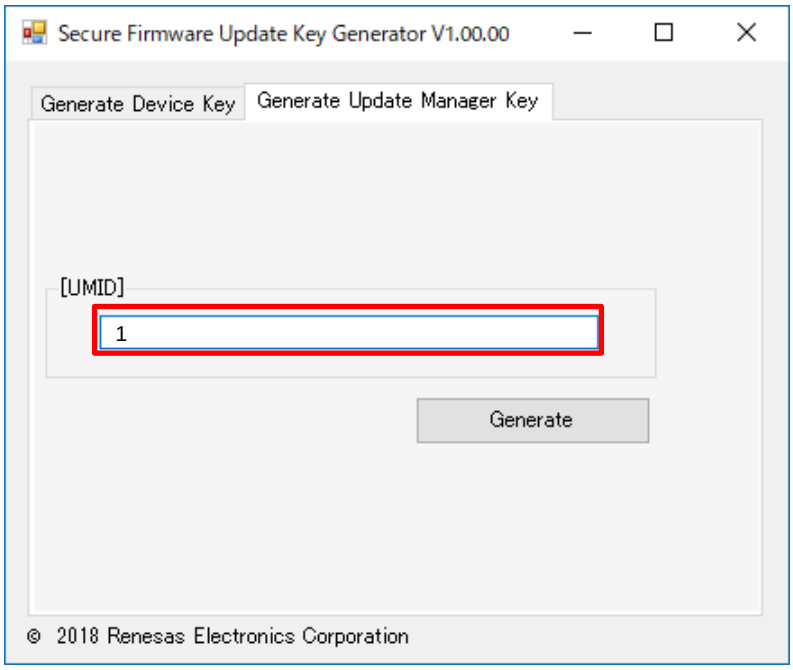

図 2-3 アップデート管理ツール用 ID 入力 GUI イメージ

③ Generate ボタンを押してください。鍵が生成されます。

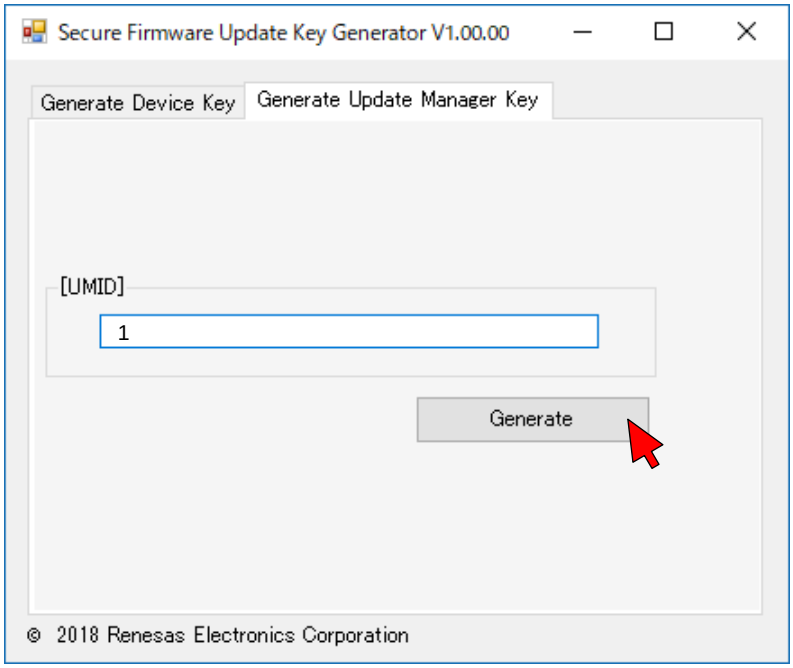

図 2-4 サーバと仮想サーバ用鍵生成 GUI イメージ

鍵データはツールを起動したディレクトリの直下に以下のように生成されます。

¥KEY_FOLDER¥UMSK¥*umid*¥UMSK.bin

umid：[UMID] に入力したアップデート管理ツール用 ID

④ 生成された UMSK.bin を、仮想サーバとして運用する Windows PC のアップデート管理ツール（Secure_Firmware_Update_Firmware_Manager.exe）が格納されているディレクトリにコピーしてください。

注 1）ID の指定方法として、“,”区切りによる複数指定と、“-”による範囲指定が可能です。入力解釈は表 2-1 を参照してください。

表 2-1 ID の入力解釈

入力例	解釈
␣	入力エラー
␣1	1
1,␣2	1,2
1-	入力エラー
-3	入力エラー
1␣2	12
1,1,2	1,2
1,	入力エラー
,1	入力エラー
1,,2	入力エラー
1-2-3,4	入力エラー

2.2　ファームウェア管理ツール

本章ではセキュアアップデートで使用するファームウェア管理ツールについて説明します。

ファームウェア管理ツールでは、ファームウェアの登録とアップデート状況の管理、仮想サーバへのファームウェアの送信、送信するファームウェアの暗号化と署名生成などを行います。

また、量産用ファームウェアの生成およびデバイス毎のユニーク ID の取り込みを行います。

ファームウェア管理ツールの機能は以下の通りです。

・アップデートするファームウェアの登録

・ファームウェアの暗号化と署名生成

・量産用ファームウェアの生成

・デバイスのユニーク ID 取り込み

・仮想サーバへのファームウェアの送信

・ファームウェアアップデート結果の取得

・ファームウェアアップデート状況の管理

・鍵生成ツールで生成された鍵情報の同期

2.2.1　ファームウェア管理ツールのセットアップ

セキュアアップデートソリューションパッケージで提供されている以下のファイルを、ファームウェア管理ツールを運用する Windows PC（サーバ）の任意のディレクトリにコピーして使用してください。

（ファームウェア管理ツールは、鍵生成ツールと同一の PC の同じディレクトリにコピーして運用することにより、鍵情報の同期をする手間を省くことができます。その際、データベースファイル（Secure_Firmware_Update.mdb）はファームウェア管理ツールのファイルを使用してください）

Secure_Firmware_Update_Firmware_Manager.exe Secure_Firmware_Update.mdb

2.2.2　ファームウェア管理ツールの初回起動時の対応

ファームウェア管理ツールを Windows PC にコピーした後、初回起動時に「Windows セキュリティの重要な警告」のポップアップが出ますので、全てのチェックボックスをチェックし アクセスを許可する(A) ボタンを押してください。

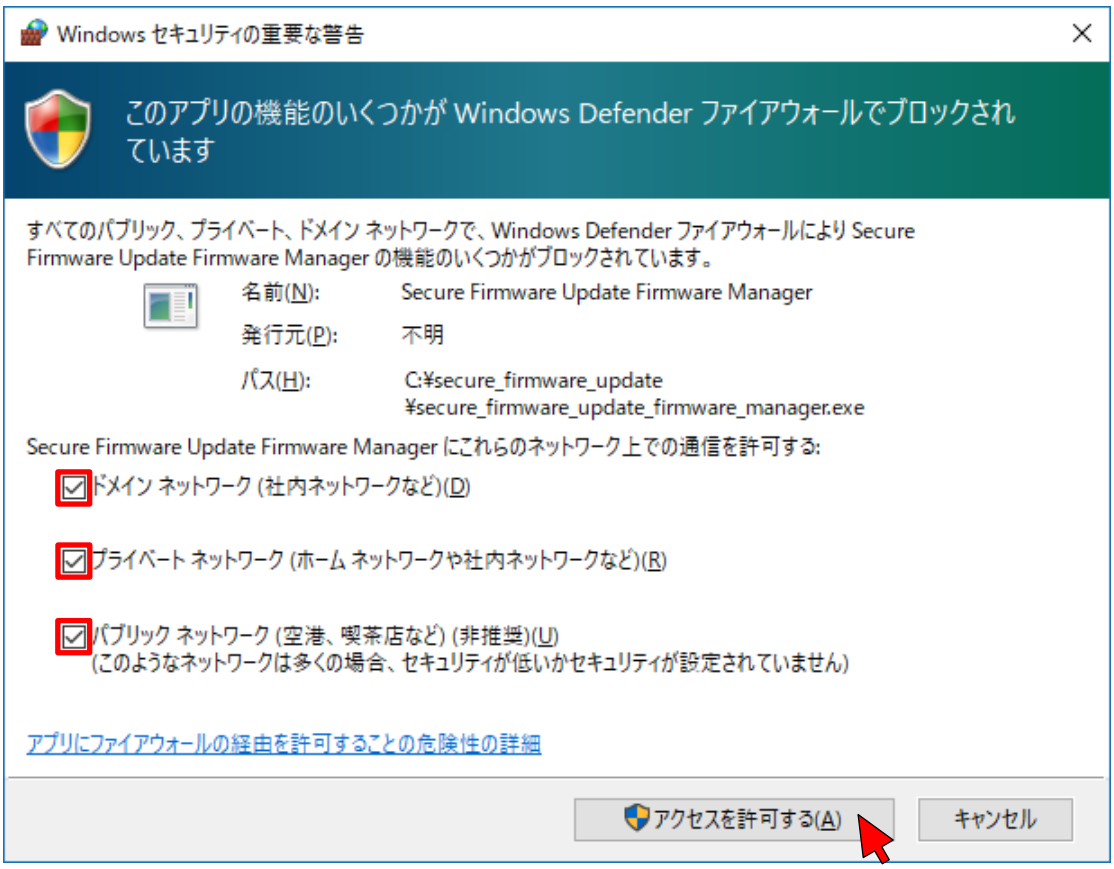

図 2-5 アクセス許可 GUI イメージ

2.2.3　ファームウェアの登録

デバイスのファームウェアの登録方法を以下に示します。

登録する際は、事前にデバイスとサーバ用の共通鍵がファームウェア管理ツールに登録されていなければなりません。“2.1.2 サーバとデバイスで使用する共通鍵の生成”を参照してください。

① Secure_Firmware_Update_Firmware_Manager.exe を起動してください。

② Register Firmware タブを選択し、Products/Version ウィンドウから製品名を選択してください。
選択すると、[Products]の表示 BOX に選択した製品名が反映されます。

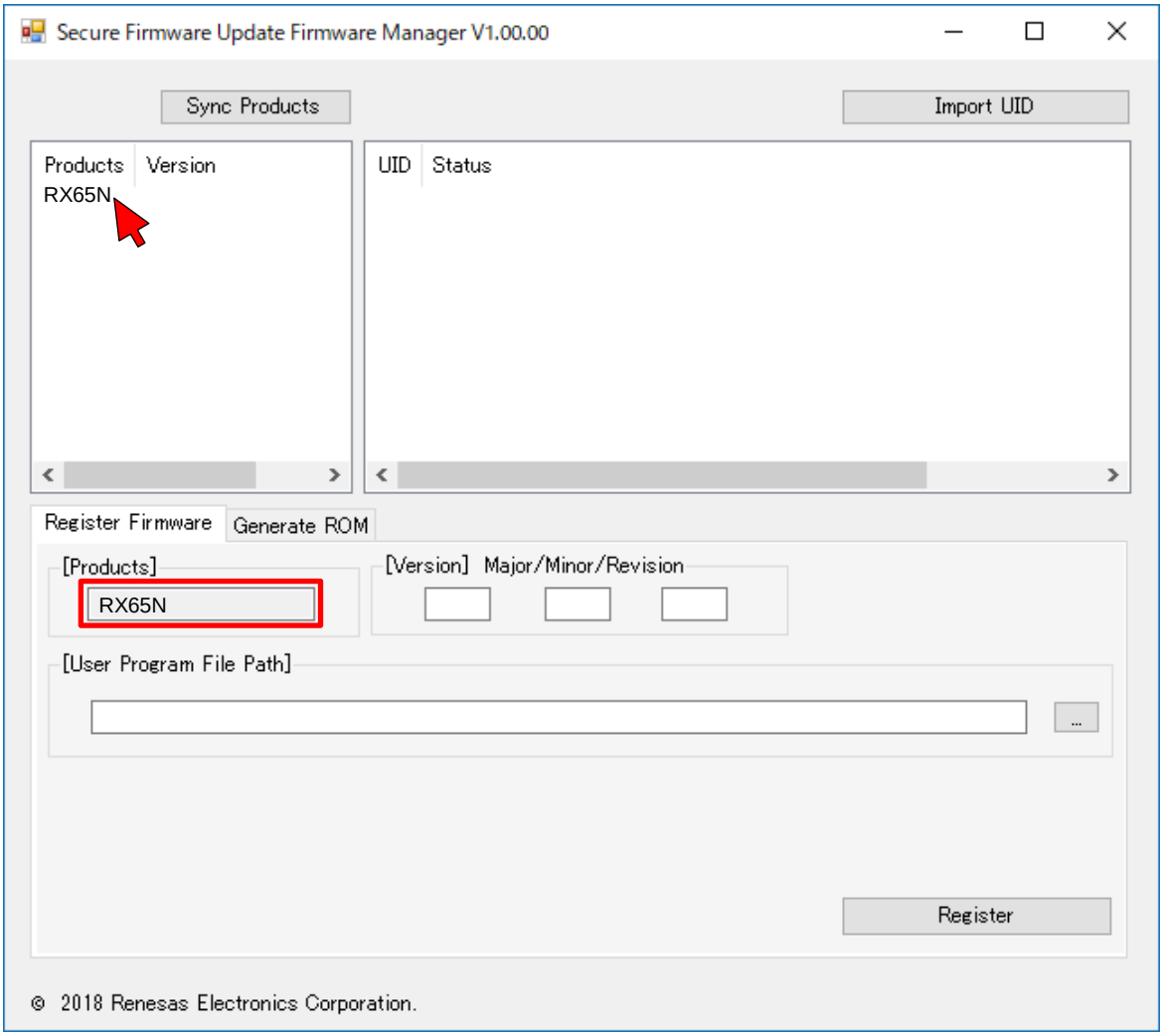

図 2-6 サーバと仮想サーバ用鍵生成 GUI イメージ

③ [Version]の入力 BOX に登録するファームウェアのバージョンを入力し、[User Program File Path]の入力 BOX にファームウェアのパスを登録してください。

バージョンの Major・Minor・Revision は 0~255 の範囲で入力可能です。ファームウェアのバージョンは必ず、現在登録されているバージョンよりアップしたバージョンを登録してください。

本ソリューションではバージョン情報に基づきデバイスのファームウェアをアップデートするため、バージョン情報がダウンして登録された場合は入力エラーとなります。

例）1.0.0 → 1.0.1　入力可能

1.1.0 → 1.0.1　入力エラー

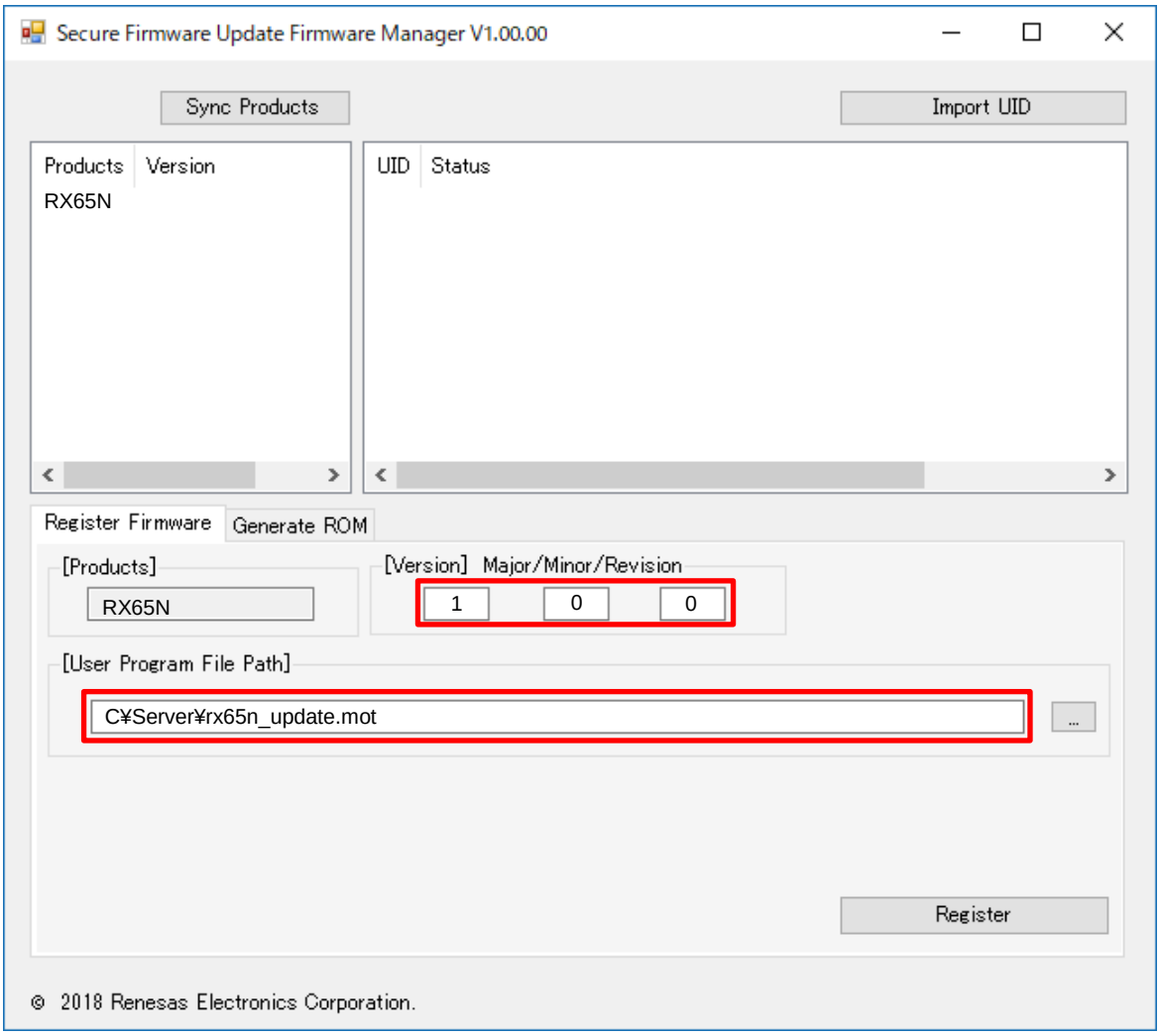

図 2-7 バージョンとユーザプログラムファイルパス設定 GUI イメージ

④ Register ボタンを押してください。

ファームウェアが登録され、Version 情報が更新されます。

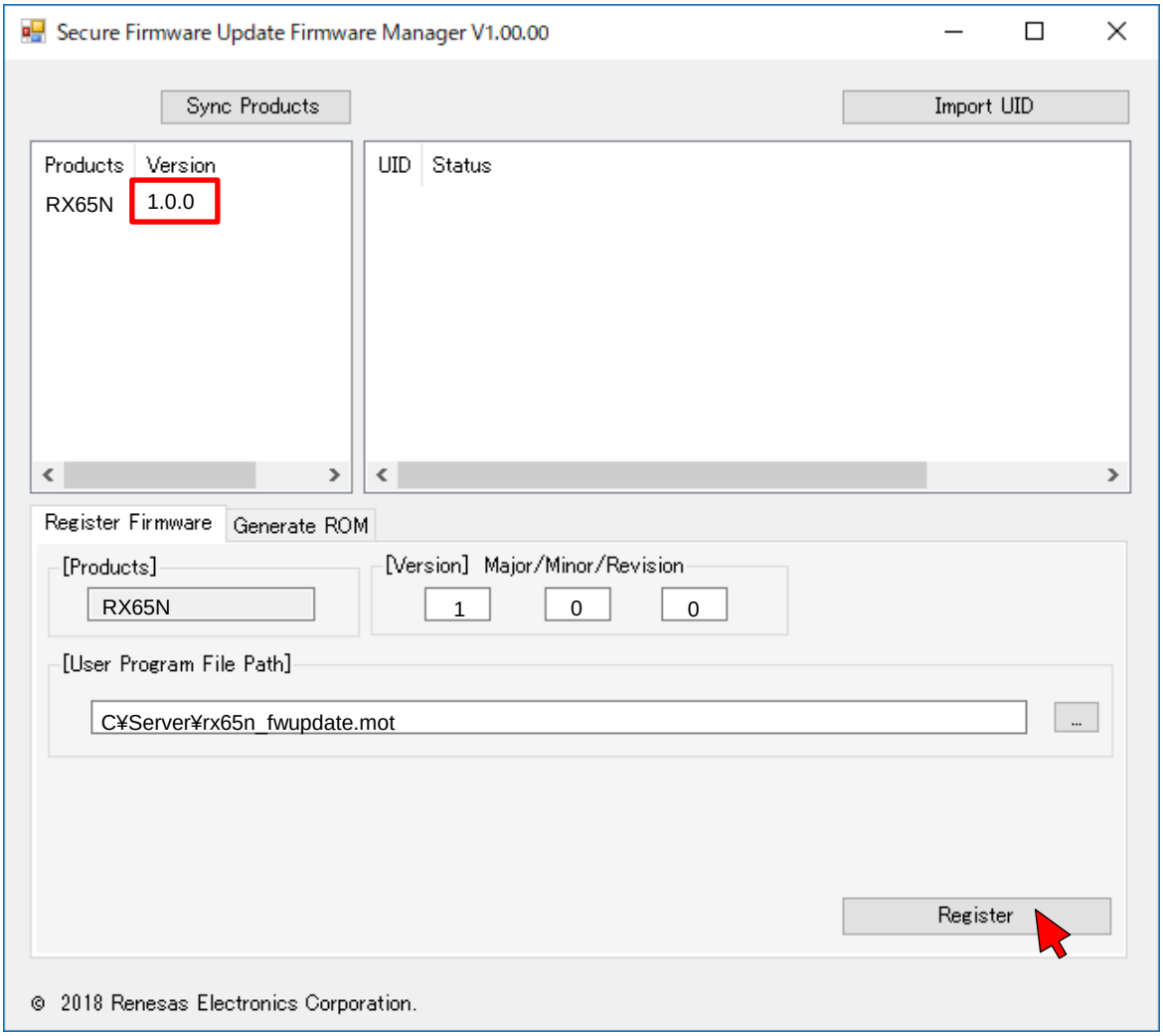

図 2-8 ファームウェア登録 GUI イメージ

2.2.4　量産用ファームウェアの生成

量産用ファームウェアの生成方法を以下に示します。

① Secure_Firmware_Update_Firmware_Manager.exe を起動してください。

② RTOS 版または Non OS 版のセキュアブートプログラムの何れかをファームウェア管理ツールと同一のディレクトリにコピーしてください。（Non OS 版の場合は nonOS_rx65n_secure_boot.mot から rx65n_secure_boot.mot にリネイムしてコピーしてください）

```
Secure_Firmware_Update_Firmware_Manager.exe
Secure_Firmware_Update.mdb
rx65n_secure_boot.mot　←　RTOS 版または Non OS 版のセキュアブートプログラムの何れかをコピーしてください。
```

③ Generate ROM タブを選択し、Products/Version ウィンドウから製品名を選択してください。
選択すると、[Products]と[Version]の表示 BOX に選択した製品名とバージョンが反映されます。

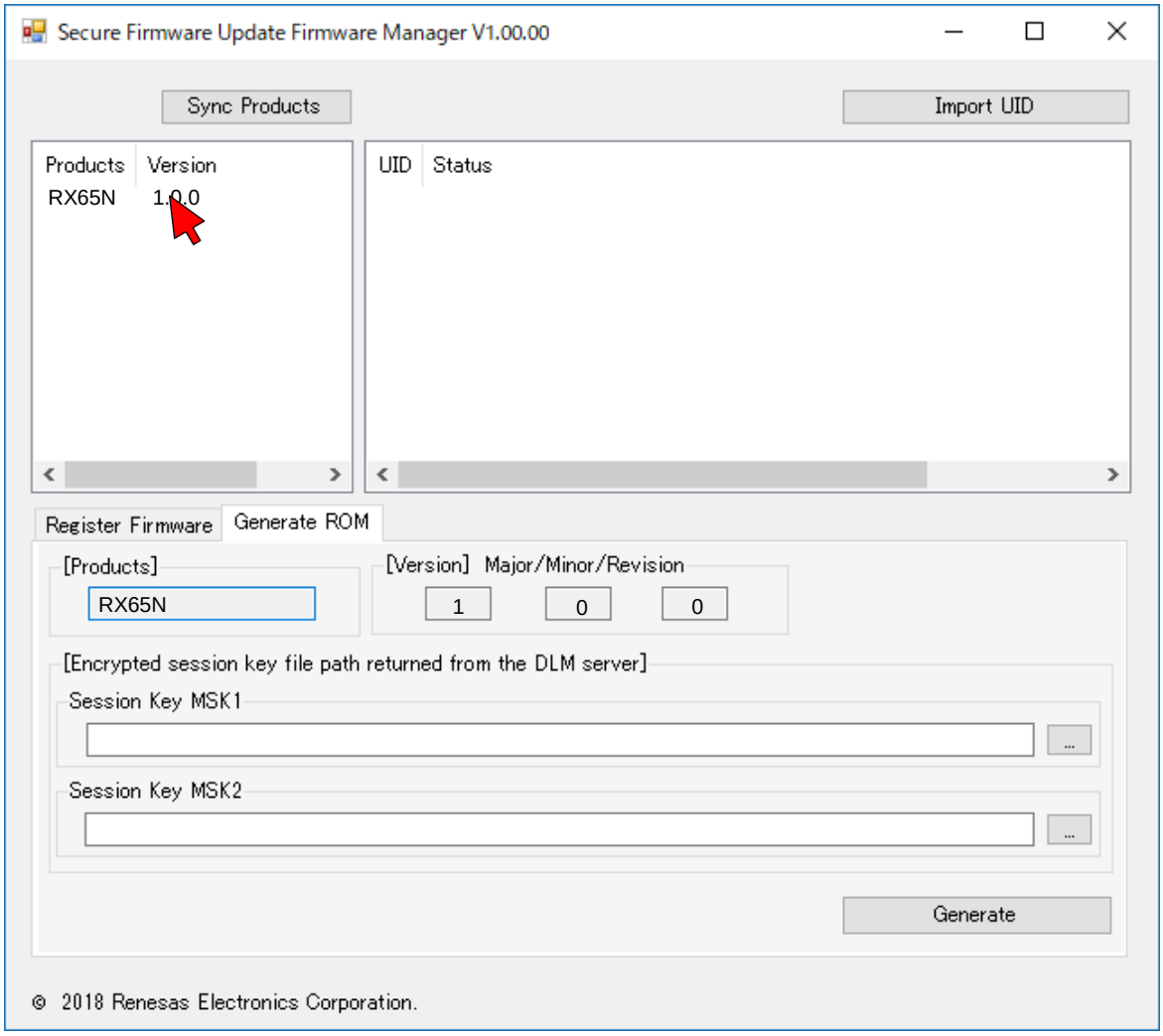

図 2-9 製品名選択 GUI イメージ

④ [Encrypted session key file path returned from the DLM sever]の Session Key MSK1 と Session Key MSK2 の入力ボックスに、“2.1.2 サーバとデバイスで使用する共通鍵の生成”で生成し、Key Wrap サービスを使用し RX65N 用に暗号化したセッション鍵データのファイルパスを登録してください。

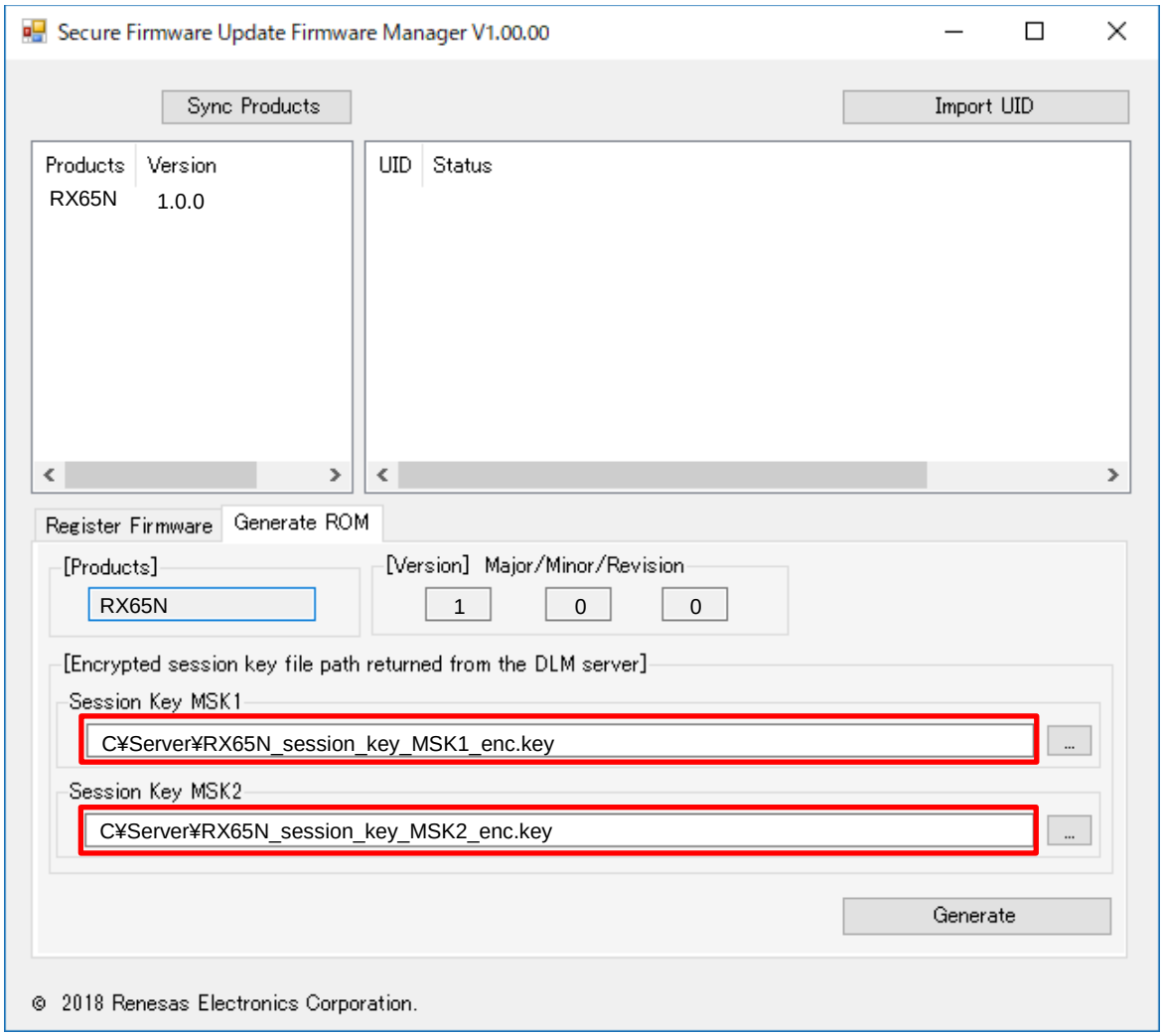

図 2-10 インストール鍵データ登録 GUI イメージ

⑤ Generate ボタンを押してください。

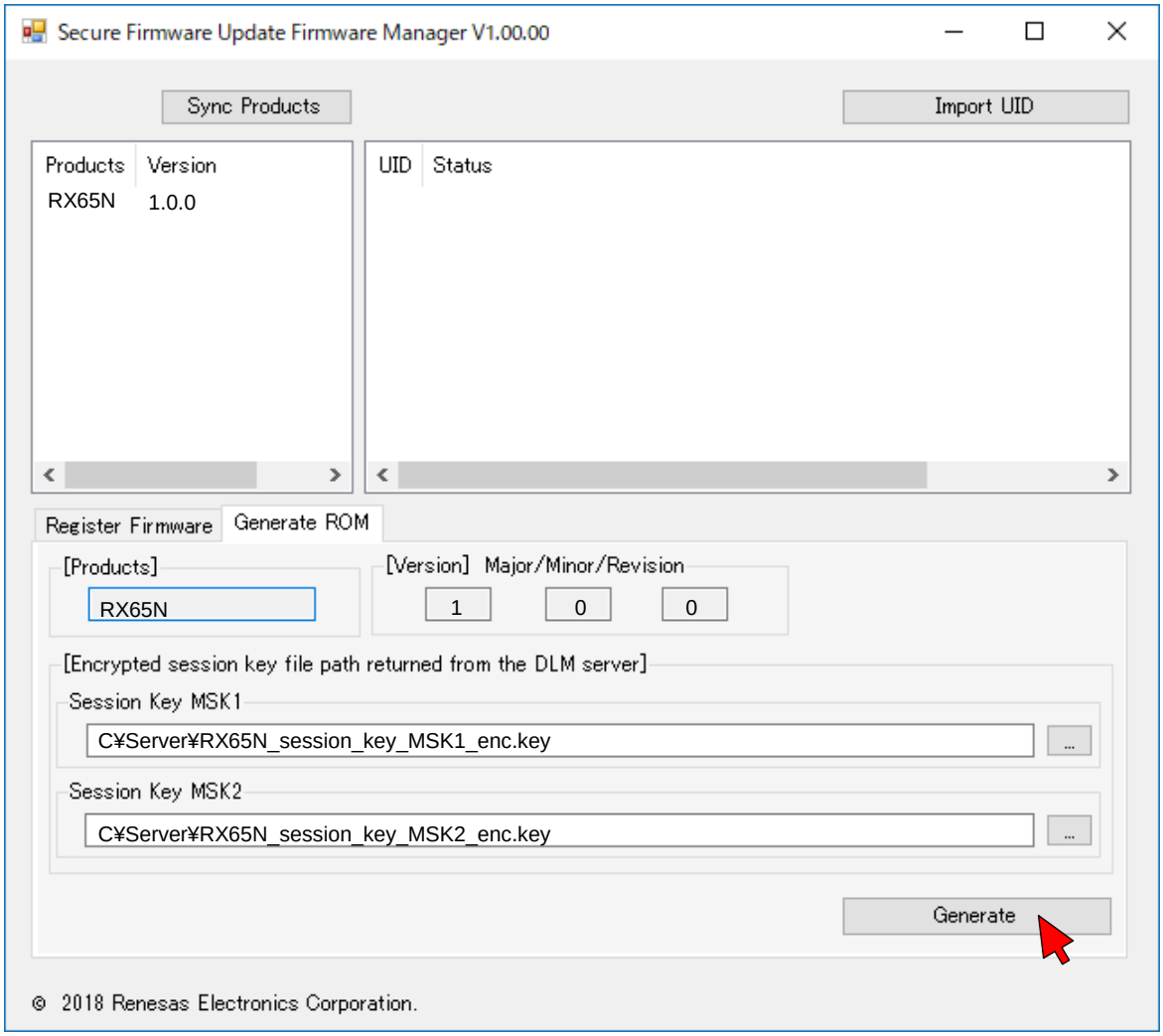

図 2-11 量産用ファームウェア生成 GUI イメージ

量産用ファームウェアはツールを起動したディレクトリの直下に以下のように生成されます。

¥*products*_*version*_ROM_RELEASE.mot

products：生成したファームウェアの製品名

version：生成したファームウェアのバージョン番号

2.2.5　ファームウェアとユニーク ID 情報の紐づけ

量産用ファームウェアをデバイスに書き込む際に生成されるユニーク ID 情報ファイル（uid.csv）をファームウェア管理ツールに登録し、ファームウェアとユニーク ID 情報との紐づけ方法を以下に示します。

ユニーク ID 情報の詳細は“2.3.2 ユニーク ID の読み出し”または“2.4.3 PG-FP6 制御マクロを用いたファームウェア書き込みとユニーク ID 読み出し”を参照ください。

① Secure_Firmware_Update_Firmware_Manager.exe を起動してください。

② Import UID ボタンを押してください。

ファイル選択画面が表示されますので、ユニーク ID 情報ファイル（uid.csv）を選択してください。

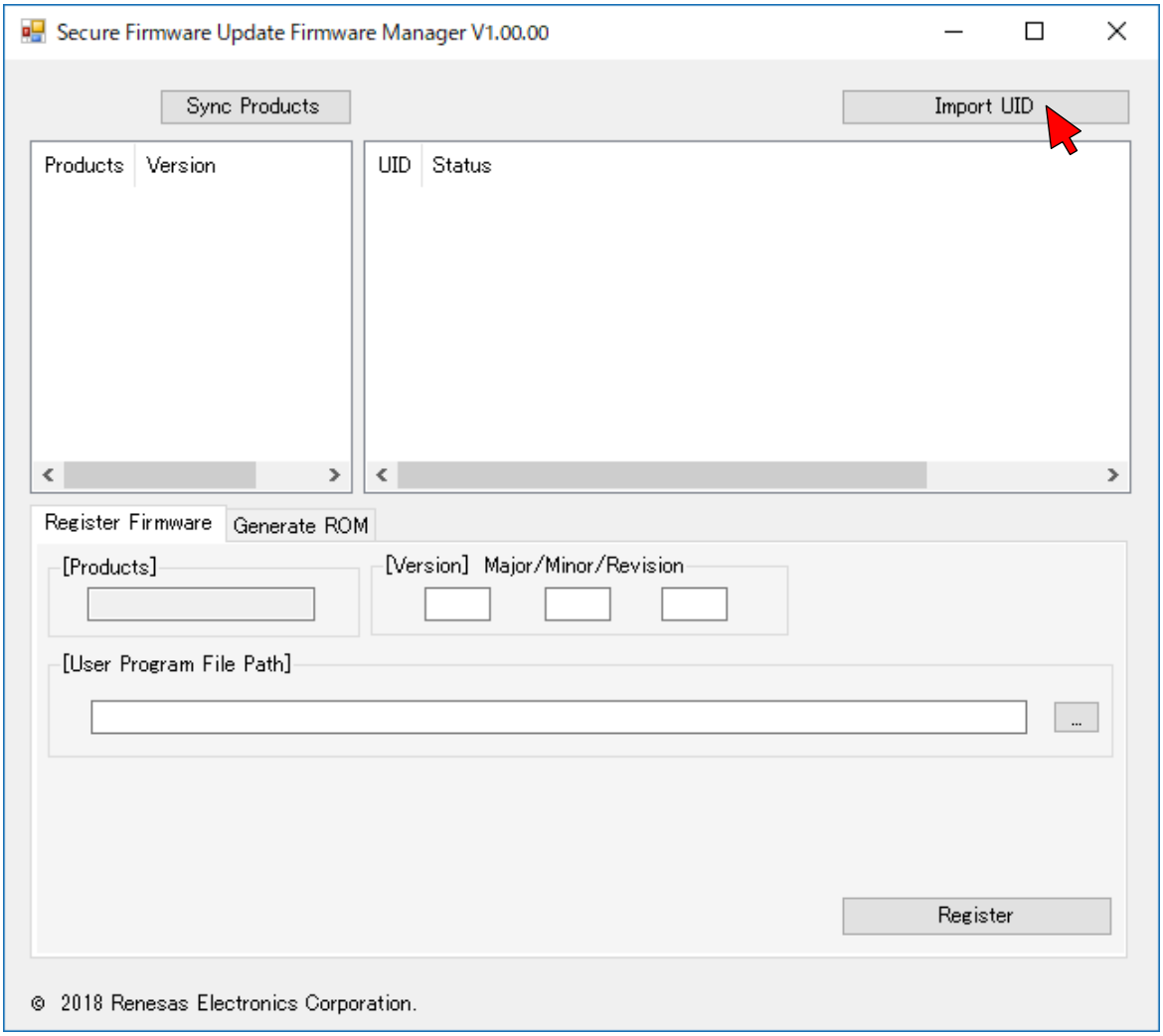

図 2-12 ユニーク ID 情報取り込み GUI イメージ

③ 製品毎のユニーク ID 情報が取り込まれ、情報表示に反映されます。

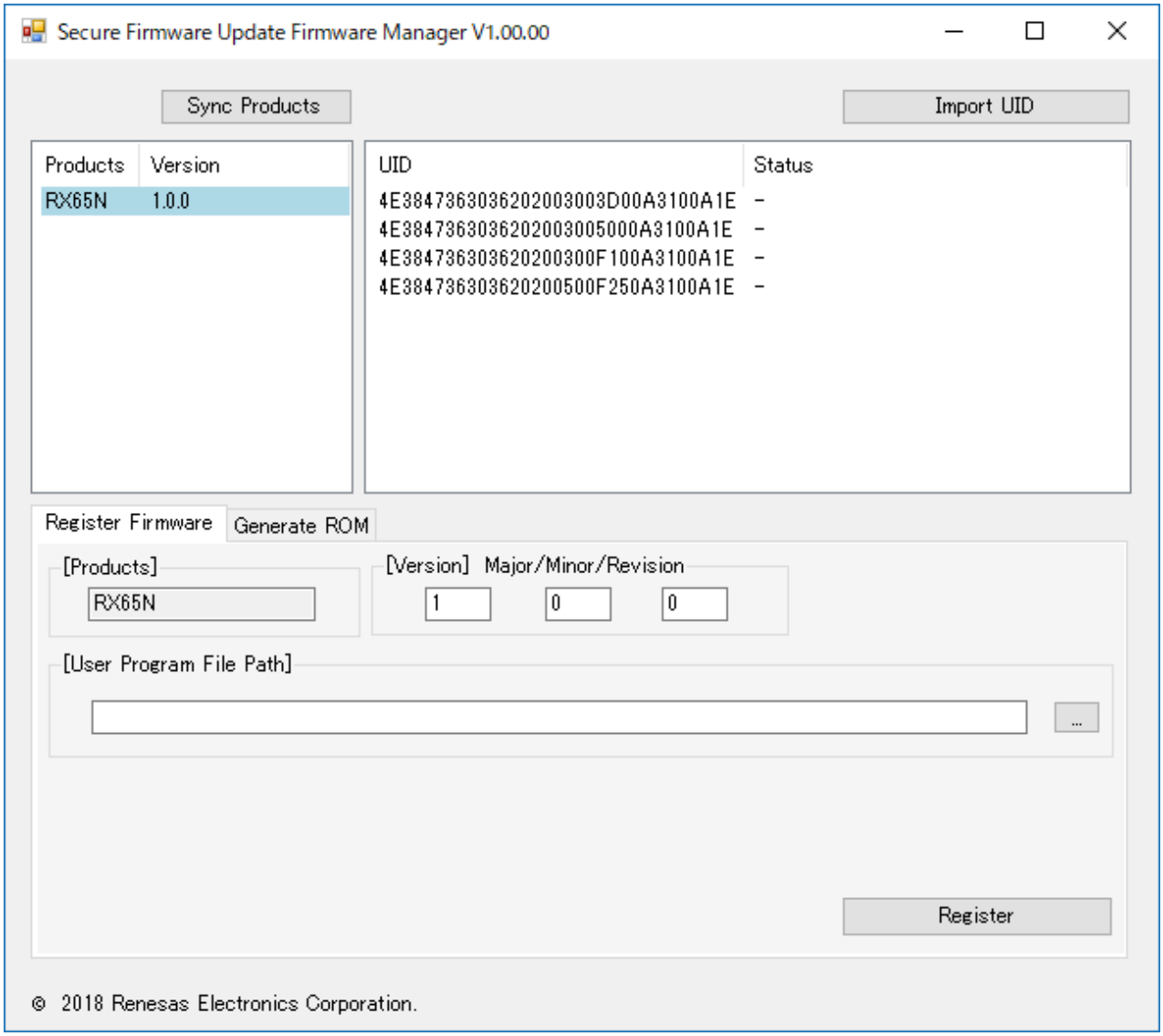

図 2-13 ユニーク ID 情報反映後 GUI イメージ

2.2.6　鍵情報の同期

鍵生成ツールで生成した鍵情報をファームウェア管理ツールに取り込み同期する方法を以下に示します。

鍵生成ツールとファームウェア管理ツールを、異なる PC や異なるディレクトリで運用している場合、鍵生成ツールで生成した鍵情報を、ファームウェア管理ツールに取り込む必要があります。

鍵生成ツールで生成した鍵情報（特定のディレクトリ）を、ファームウェア管理ツールにコピーして同期させることにより、鍵情報を両ツール間で同期させます。

具体的には、鍵フォルダ内の鍵ファイルとファームウェア管理ツールのデータベースファイルを検索し、新しく鍵が増えている場合、データベースファイルに鍵の情報を反映させます。

① 鍵生成ツールで生成した鍵情報が置かれている、KEY_FOLDER フォルダ以下をコピーしてください。

¥KEY_FOLDER

② ファームウェア管理ツールの実行ファイルが置かれているディレクトリに、先ほどの KEY_FOLDER フォルダを貼り付けてください。（コピーする際は必ず鍵生成ツールからファームウェア管理ツールへコピーしてください）

③ Secure_Firmware_Update_Firmware_Manager.exe を起動してください。

④ Sync Products ボタンを押してください。

KEY_FOLDER フォルダの内容を検索し、鍵情報をファームウェア管理ツールに同期します。

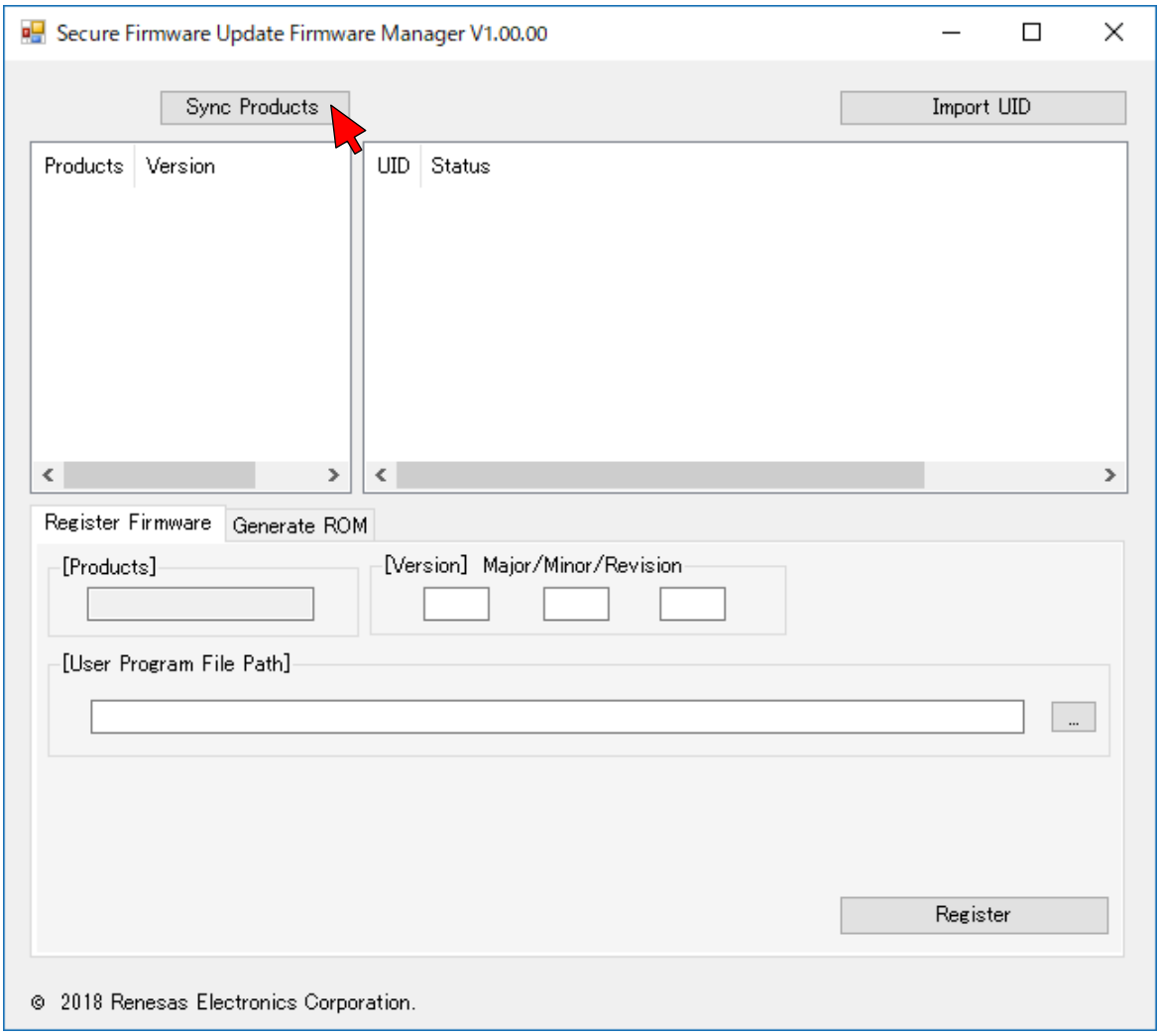

図 2-14 鍵情報の同期操作 GUI イメージ

2.2.7　ファームウェアアップデート状況の管理

ファームウェア管理ツールでのファームウェアアップデート状況の表示について説明します。

ファームウェアアップデートの状況は GUI の情報表示領域に表示されます。

情報表示領域に表示される情報は次の内容です。

① 製品名（Products）

② バージョン（Version）

③ 機器 ID（UID）

④ アップデート状況（Status）

アップデート状況の表示内容を以下に示します。

⑤ ファームウェアの登録済みの状態。（Status=“－”）

⑥ ファームウェアアップデートの正常完了。（Status=“Success”）

⑦ ファームウェアアップデートの失敗。（Status=“Failed”）

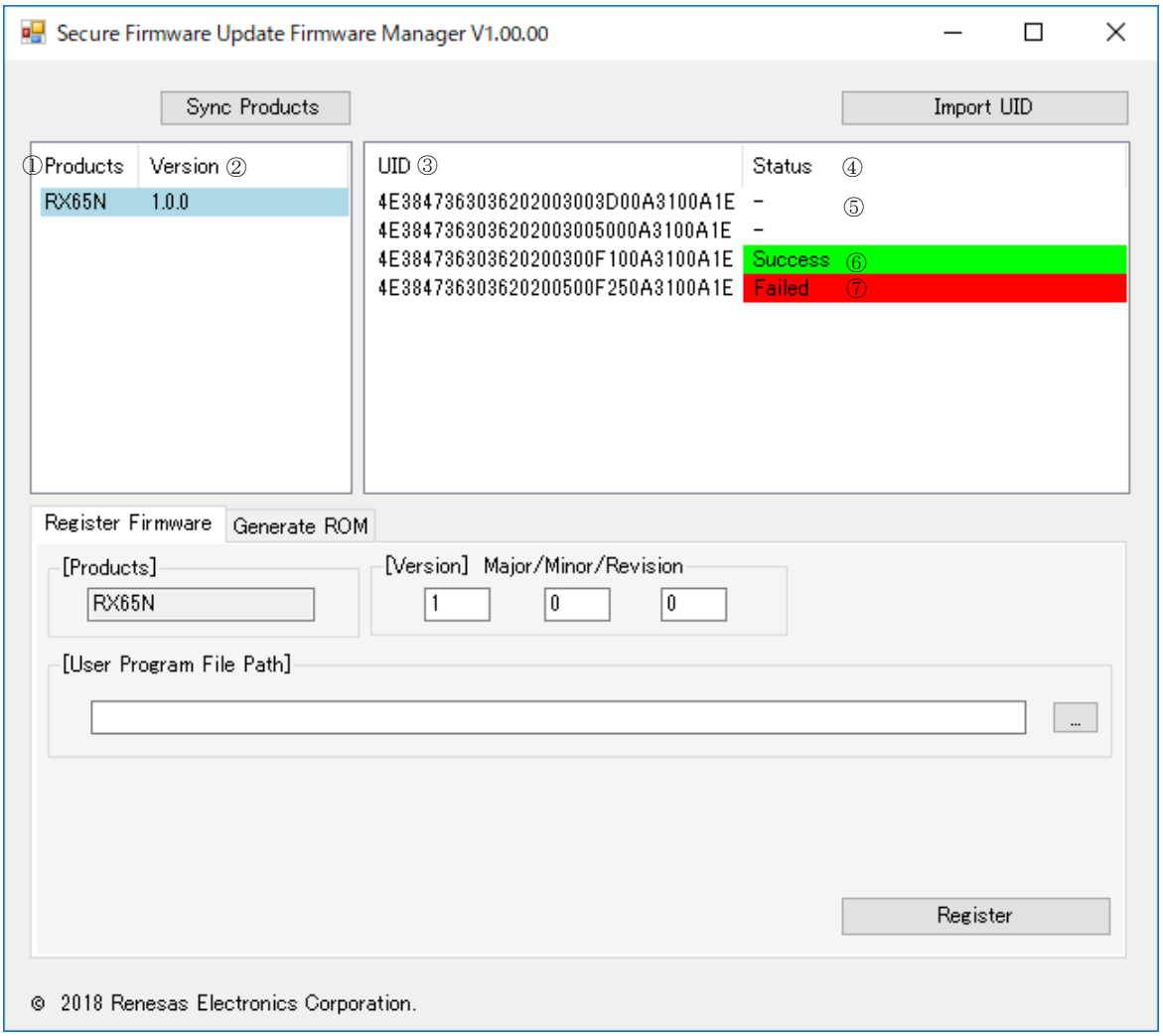

図 2-15 ファームウェアアップデート状況の GUI イメージ

Failed 表示は、ファームウェアアップデートに失敗したことを表しています。

原因はファームウェアデータの破損または、デバイス側のフラッシュメモリの問題が考えられます。

対応としては再度サーバから仮想サーバにファームウェアをダウンロードしアップデートを行ってください。それでも Transfer failure と成る場合は、デバイスのフラッシュメモリに問題があると思われますのでデバイスの交換等を検討してください。

2.3　ユニーク ID 読み出しツール

本章では、フラッシュメモリ書き込みツール等を使い、“2.2.4 量産用ファームウェアの生成”で生成した量産用ファームウェアを書き込んだデバイスから、ユニーク ID を読み出す方法を説明します。

なお、フラッシュプログラマ（PG-FP6）をお使いの場合は FP6 マクロを使用することにより、書き込みからユニーク ID 読み出しの一連の作業を一度に行うことができます。詳細は“2.4PG-FP6 制御用マクロ”を参照ください。

ユニーク ID 読み出しツールの機能は以下の通りです。

・デバイスからのユニーク ID の読み出しとユニーク ID 情報ファイルの生成

2.3.1　ユニーク ID 読み出しツールセットアップ

セキュアアップデートソリューションパッケージで提供されている以下のファイルを、ユニーク ID 読み出しツールを運用する Windows PC の任意のディレクトリにコピーして使用してください。

Secure_Firmware_Update_UID_Reader.exe

2.3.2　ユニーク ID の読み出し

デバイスのユニーク ID を読み出す方法を以下に示します。

デバイスのユニーク ID を読み出す際には、事前にフラッシュライタ等を使用し量産用ファームウェアをデバイスに書き込んでおいてください。

① ユニーク ID 読み出しツールをインストールした PC とデバイスを Ether ケーブルまたは USB ケーブルで接続してください。

② ユニーク ID 読み出しツール（Secure_Firmware_Update_UID_Reader.exe）を起動してください。

③ デバイスの電源を入れ、ファームウェアアップデートが可能な状態にしてください。フラッシュ書き込み後の初回起動時は、ファームウェアの復号等を行うため立ち上がるまでに少し時間がかかります。

④ ＜デバイスと Ether ケーブルで接続した場合＞

Interface の選択 BOX で Ether を選択してください。

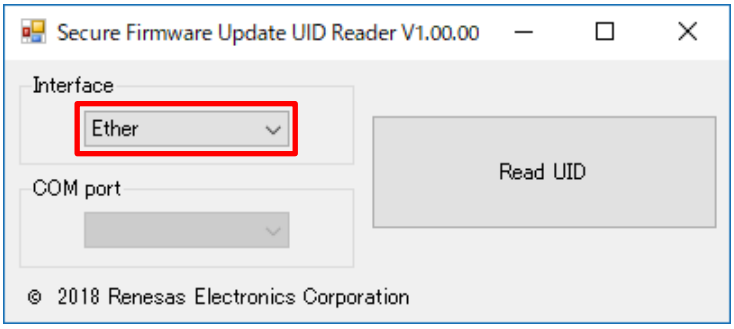

図 2-16 Ether 接続設定の GUI イメージ

＜デバイスと USB ケーブルで接続した場合＞

Interface の選択 BOX で USB を選択し、COM Port の選択 BOX で USB ケーブルが接続されている COM ポート番号を選択してください。（COM ポートは USB ケーブル接続時に自動で割り振られますので、割り振られた COM ポートをデバイスマネージャー等で確認し選択してください

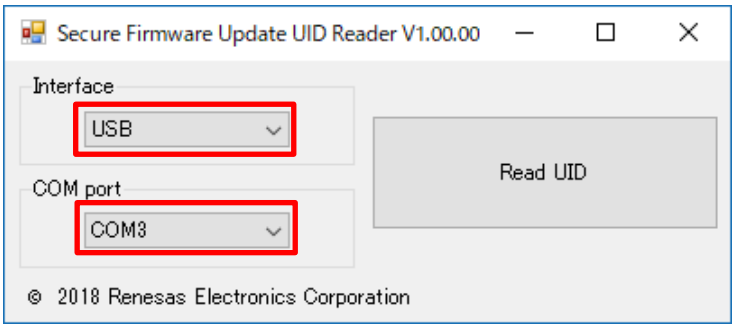

図 2-17 USB 接続設定の GUI イメージ

⑤ Read UID ボタンを押してください。

接続されているデバイスのユニーク ID が読み出されます。

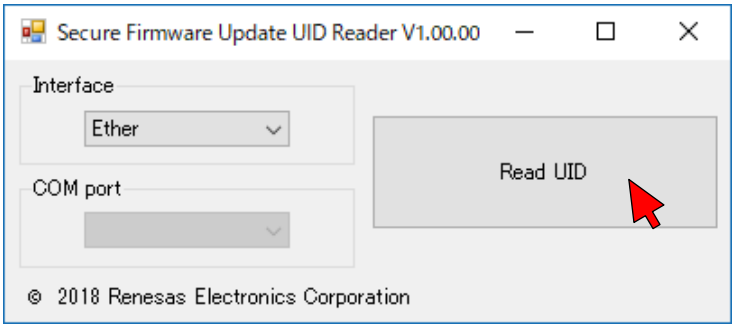

図 2-18 ファームウェアアップデート操作の GUI イメージ

読み出されたユニーク ID 情報が、ユニーク ID 読み出しツールの実行ファイルと同じディレクトリに CSV ファイル（uid.csv）として保存されます。

uid.csv

⑥ 生成されたユニーク ID 情報をファームウェア管理ツールに登録し、ファームウェアとそのファームウェアが書き込まれた機器のユニーク ID 情報を紐づけます。

ファームウェア管理ツールへの登録は“2.2.5 ファームウェアとユニーク ID 情報の紐づけ”を参照してください。

2.4　PG-FP6 制御用マクロ

本章では、PG-FP6 をターミナルソフトのマクロ機能で制御し“2.2.4 量産用ファームウェアの生成”で生成した量産用ファームウェアを、デバイスに書き込みユニーク ID の読み出しを行う方法について説明します。

本章では、PG-FP6 の制御のために、ターミナルソフトとして PG-FP6 添付の FP6 Terminal とフリーソフトウェアの Tera Term を使用します。

PG-FP6 および FP6 Terminal の詳細は PG-FP6 のユーザーズマニュアル（PG-FP6 V1.01 フラッシュメモリプログラマ ユーザーズマニュアル R20UT425JJ0100）を参照してください。

Tera Term の詳細は https://ttssh2.osdn.jp/index.html.ja を参照してください。

ターミナルソフトのマクロ機能を使った PG-FP6 制御機能は以下の通りです。

・デバイスへのファームウェア書き込み

・デバイスからのユニーク ID の読み出しとユニーク ID 情報ファイル生成

2.4.1　PG-FP6 の初期化

PG-FP6 の初期化方法を以下に示します。

① PG-FP6 と PC を接続し、FP6 Terminal を起動してください。

PG-FP6 と PC の接続方法および FP6 Terminal のセットアップの詳細は PG-FP6 のユーザーズマニュアル(R20UT425JJ0100)を参照してください。

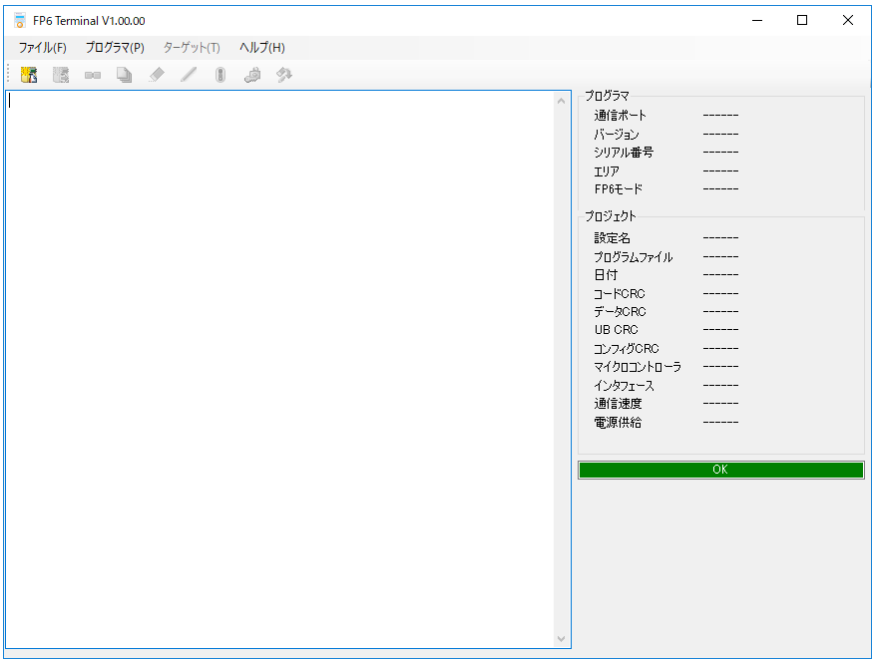

図 2-19 FP6 Terminal の GUI イメージ

② FP6 Terminal のファイル(F)→セットアップ(S)→新規(N)で新しいセットアップファイルの作成を開始します。設定情報を下記のように設定し、OK ボタンを押してください。

・ファミリ：RX

・グループ：RX65N

・ターゲットマイコン：R5F565NE (Dual mode)

・設定名：任意

・作成場所：任意

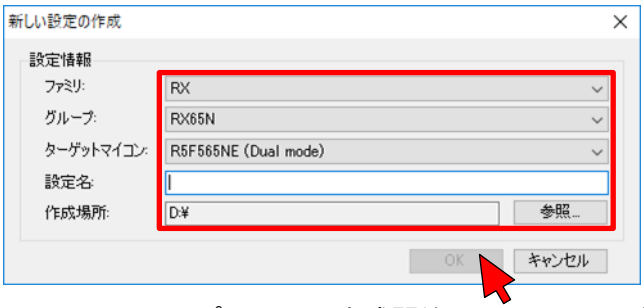

図 2-20 セットアップファイル生成開始の GUI イメージ

③ プログラムファイルタブを選択し、“2.2.4 量産用ファームウェアの生成”で作成した量産用ファームウェアを設定してください。

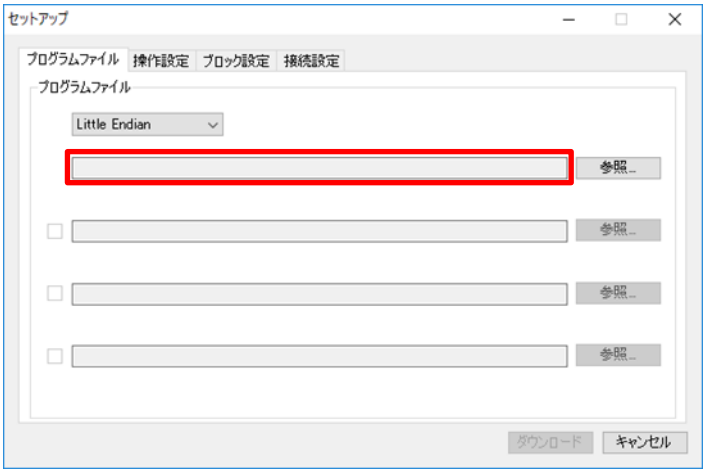

図 2-21 プログラムファイルタブの GUI イメージ

④ 操作設定タブを選択し、コマンドの「ベリファイ」の項目にチェックを入れ、書き込みとベリファイオプションの「0xFF で補完する」の項目のチェックを外してください。

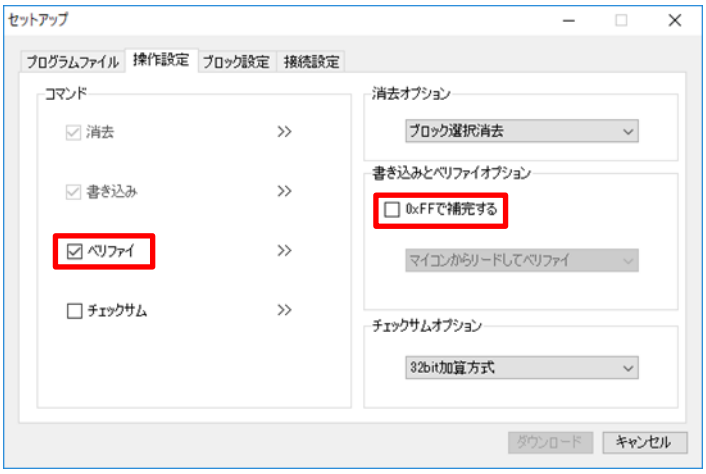

図 2-22 操作設定タブの GUI イメージ

⑤ ブロック設定タブは初期状態のまま変更しません。

図 2-23 ブロック設定タブの GUI イメージ

⑥ 接続設定タブを選択し、切断時のモード端子設定を「リセット端子を Hi-z」に設定してください。

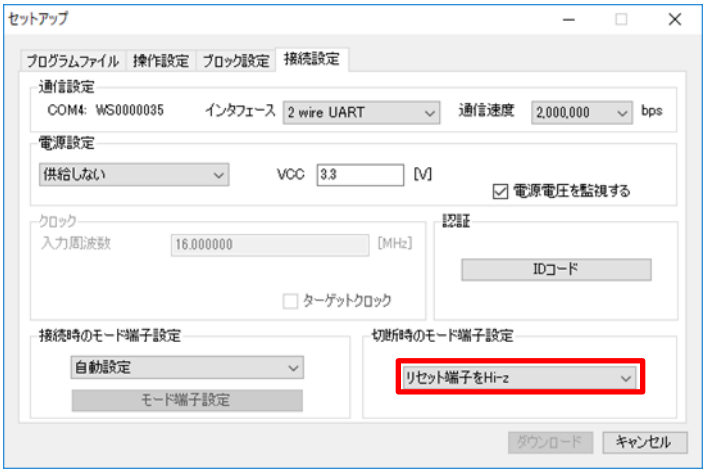

図 2-24 接続設定タブの GUI イメージ

⑦ セットアップの各タブの設定が完了したら、ダウンロードボタンを押してください。セットアップファイル（.pr5、.esf ファイル）が生成され、③で指定した量産用ファームウェアが PG-FP6 にダウンロードされます。

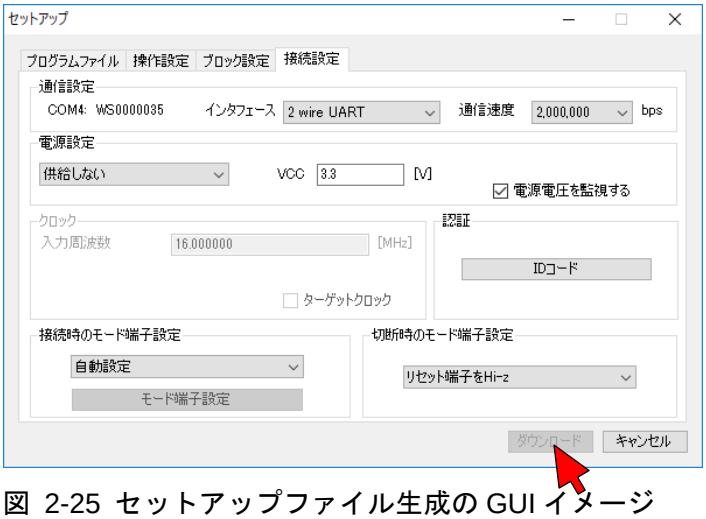

図 2-25 セットアップファイル生成の GUI イメージ

2.4.2 PG-FP6 制御マクロのセットアップ

セキュアアップデートソリューションパッケージで提供されている以下のファイルを、PG-FP6 制御用 Windows PC の任意のディレクトリにコピーして使用してください。

rx65n_write.ttl

2.4.3 PG-FP6 制御マクロを用いたファームウェア書き込みとユニーク ID 読み出し

PG-FP6 と Tera Term のマクロ（rx65n_write.ttl）を使用し、量産ファームウェアファイルをデバイスに書き込む方法について説明します。

① PG-FP6 と PC を接続し、PG-FP6 の電源を入れてください。

② PG-FP6 とデバイス（RX65N）を接続し、デバイスの電源を入れてください。

③ Tera Term を起動してください。

Tera Term のセッティング等の詳細は https://ttssh2.osdn.jp/index.html.ja を参照してください。

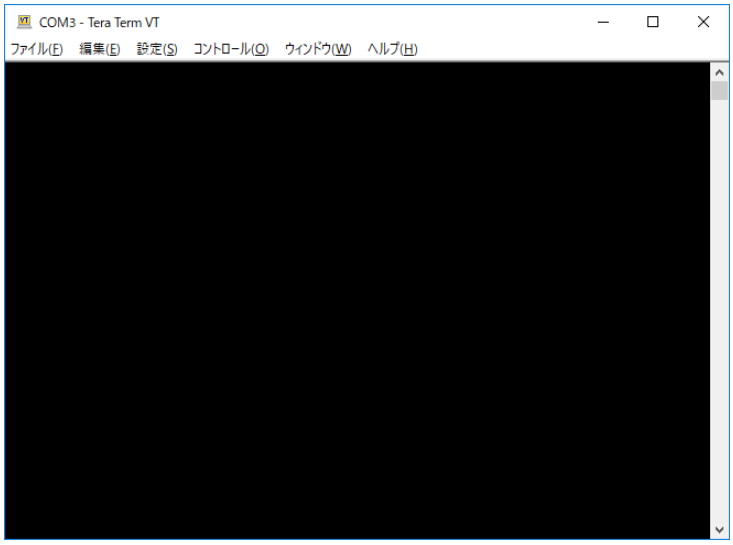

図 2-26 Tera Term の GUI イメージ

④ Tera Term の通信設定を以下のように設定してください。

・ポート：USB ケーブルが接続されている COM ポート番号を選択
（COM ポートは USB ケーブル接続時に自動で割り振られますので、割り振られた COM ポートをデバイスマネージャー等で確認し選択してください））

・ボーレート：9600bps

・データ：8bit

・パリティ：none

・ストップ：1bit

・フロー制御：none

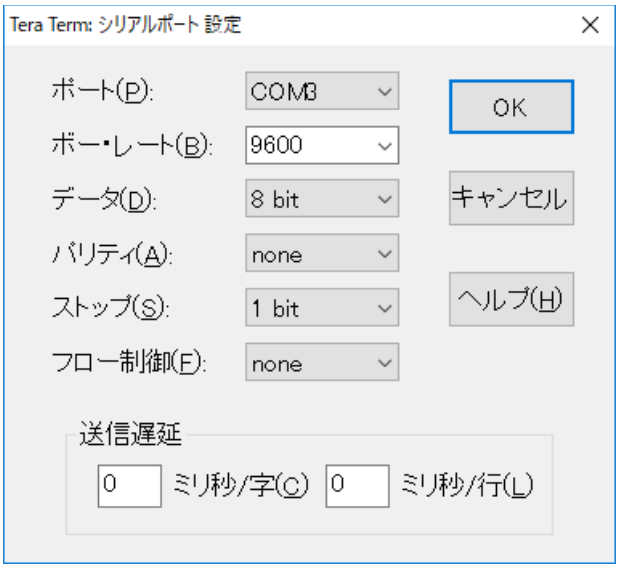

図 2-27 TeraTerm 通信設定の GUI イメージ

⑤ Tera Term でコントロール(O)→マクロ(M)で実行するマクロファイル（rx65n_write.ttl）を選択してください。

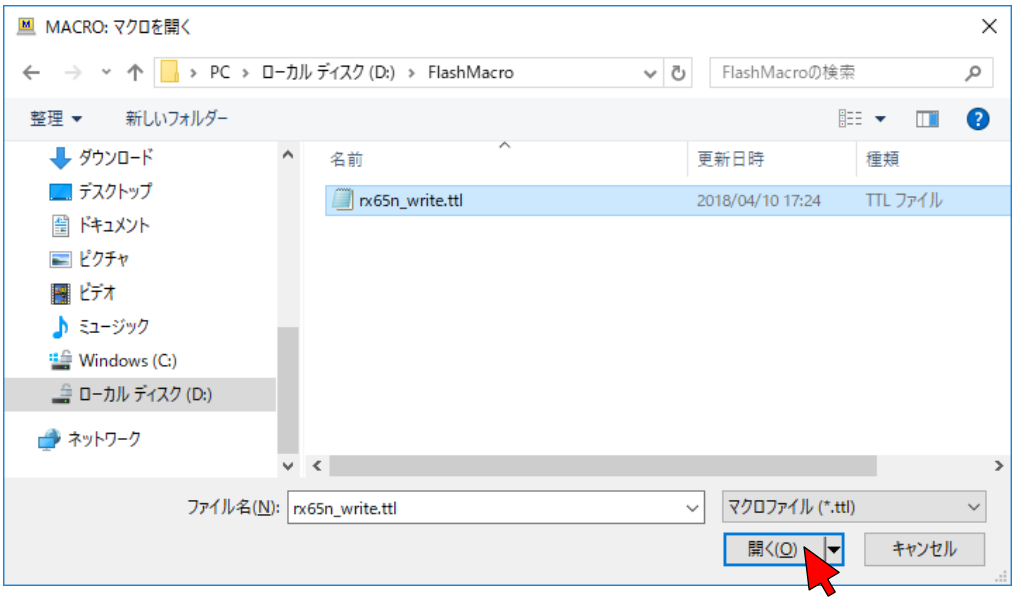

図 2-28 マクロファイル選択の GUI イメージ

⑥ マクロの表示に従いデバイスへの書き込みを行います。

⑦ 書き込み終了後にデバイスのユニーク ID 情報が読み出され、選択したマクロファイルと同じディレクトリに CSV ファイル（uid.csv）として保存されます。

uid.csv

⑧ 生成されたユニーク ID 情報をファームウェア管理ツールに登録し、ファームウェアとそのファームウェアが書き込まれた機器のユニーク ID 情報を紐づけます。

ファームウェア管理ツールへの登録は“2.2.5 ファームウェアとユニーク ID 情報の紐づけ”を参照してください。

2.5　アップデート管理ツール

本章ではセキュアアップデートで使用するアップデート管理ツールについて説明します。

アップデート管理ツールでは、サーバからのファームウェアダウンロードと、デバイスへのファームウェアアップデート、サーバへのファームウェアアップデート結果の送信、ファームウェアアップデート状況の管理を行います。

アップデート管理ツールの機能は以下の通りです。

・サーバへのファームウェアの送信要求とファームウェアのダウンロード

・仮想サーバとデバイス間の相互認証とデバイスへのファームウェア送信

・デバイスからのファームウェアアップデート結果の受信

・サーバへのファームウェアアップデート結果の送信

・ファームウェアデータの消去

・ファームウェアアップデート状況の管理

2.5.1　アップデート管理ツールセットアップ

セキュアアップデートソリューションパッケージで提供されている以下のファイルを、アップデート管理ツールを運用する Windows PC（仮想サーバ）の任意のディレクトリにコピーして使用してください。

また、“2.1.3 サーバと仮想サーバで使用する共通鍵の生成”で生成した共通鍵（UMSK.bin）を同じディレクトリにコピーしてください。

Secure_Firmware_Update_Update_Manager.exe Secure_Firmware_Update_Update_Manager.mdb UMSK.bin

2.5.2　　アップデート管理ツールの初回起動時の対応

アップデート管理ツールを Windows PC にコピーした後、初回起動時に「Windows セキュリティの重要な警告」のポップアップが出ますので、全てのチェックボックスをチェックし アクセスを許可する(A) ボタンを押してください。

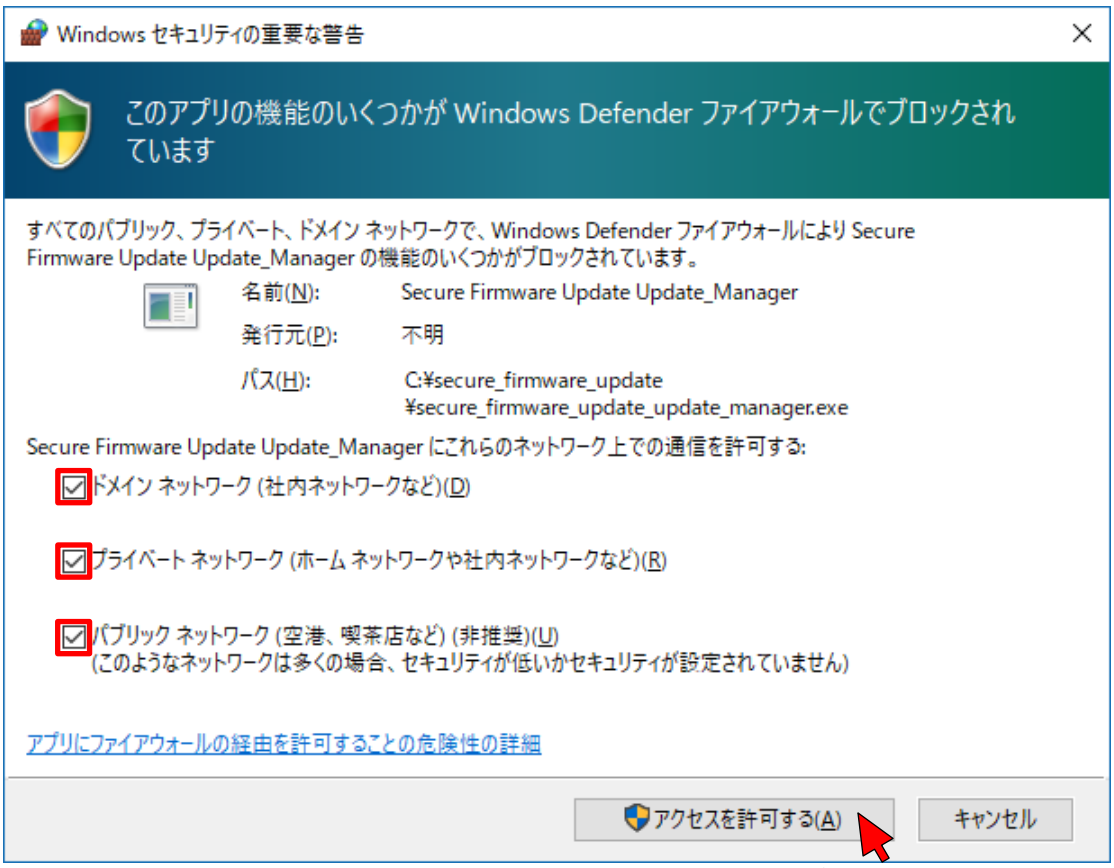

図 2-29 アクセス許可 GUI イメージ

2.5.3　　ファームウェア管理ツールからファームウェアをダウンロード

サーバからファームウェアをダウンロードする方法を以下に示します。

① サーバと仮想サーバを Ether ケーブル（同一サブネットでのネットワーク接続）で接続してください。

② サーバのファームウェア管理ツール（Secure_Firmware_Update_Firmware_Manager.exe）を起動してください。

③ 仮想サーバのアップデート管理ツール（Secure_Firmware_Update_Update_Manager.exe）を起動してください。

④ Connect to Server タブを選択し、IP Address の入力 BOX にサーバの IP アドレスを設定してください。

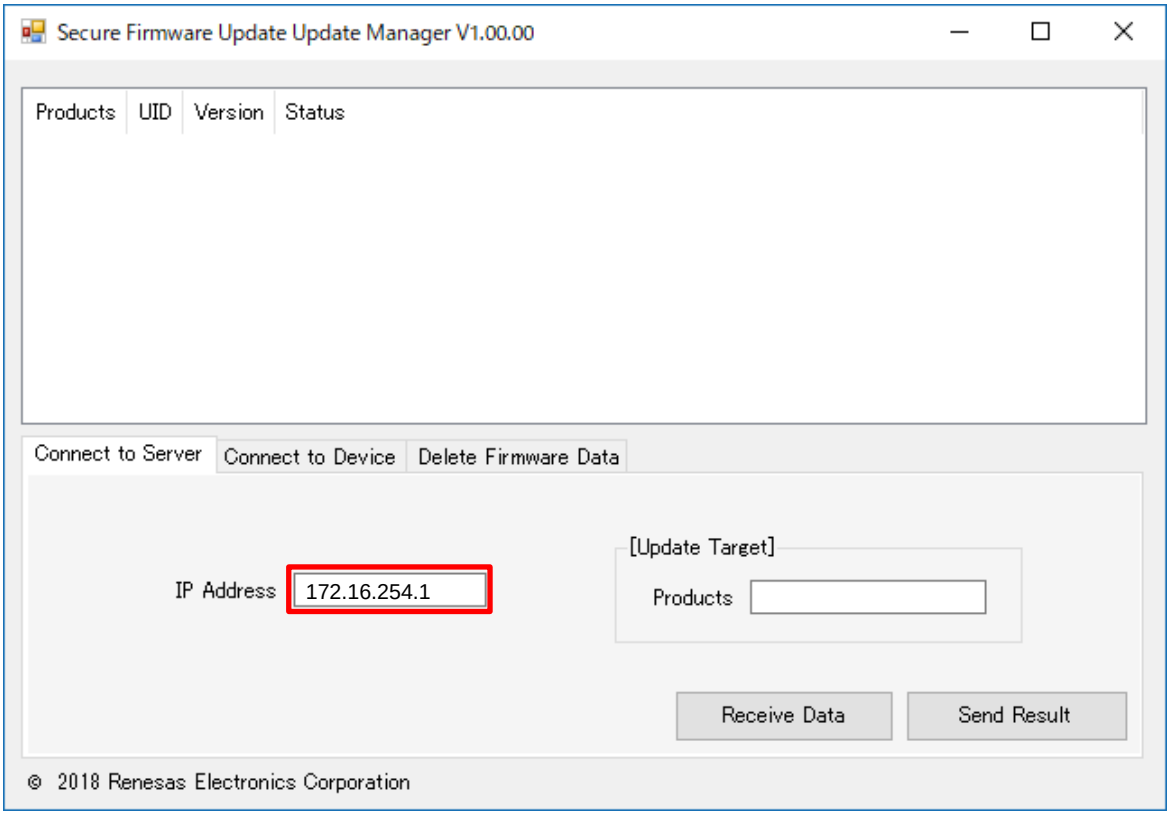

図 2-30 サーバの IP アドレス設定の GUI イメージ

⑤ [Update Target]の入力 BOX にアップデートしたいデバイスの製品名を入力してください。

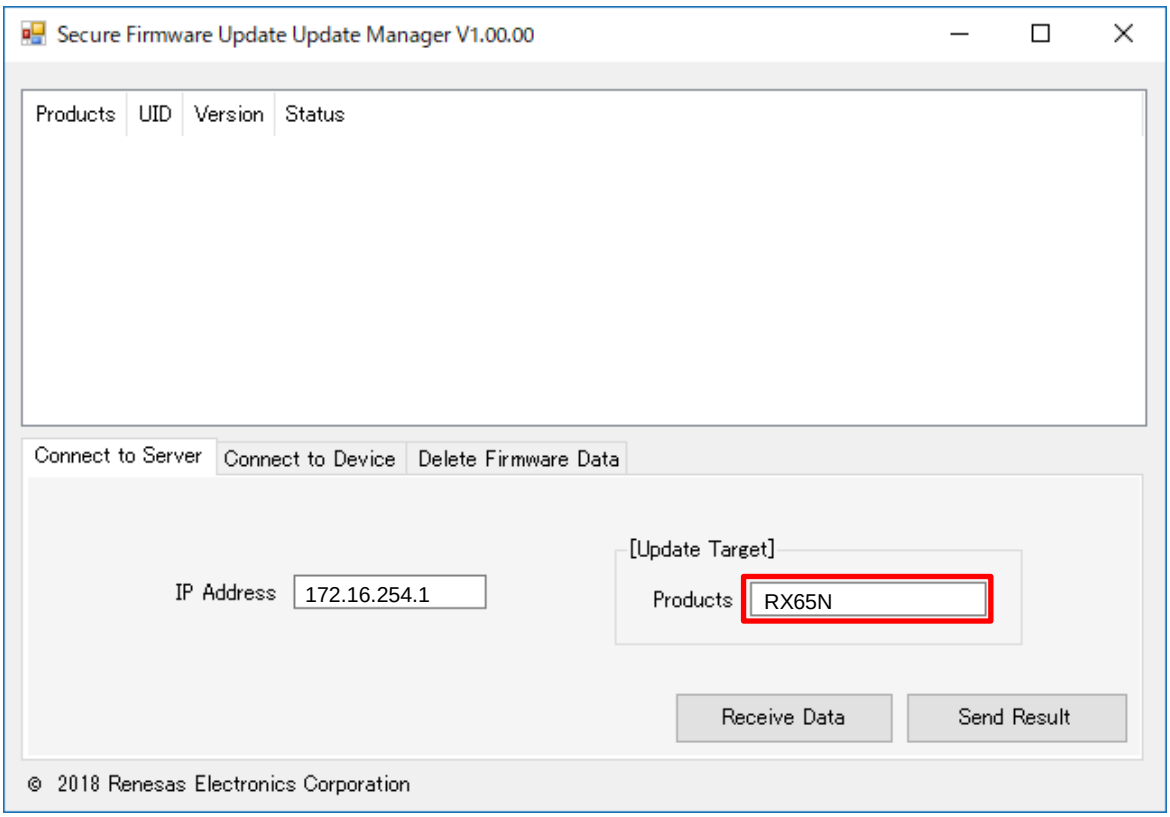

図 2-31 アップデートの製品名入力の GUI イメージ

⑥ Receive Data ボタンを押してください。

サーバから仮想サーバへファームウェアのダウンロードを開始します。

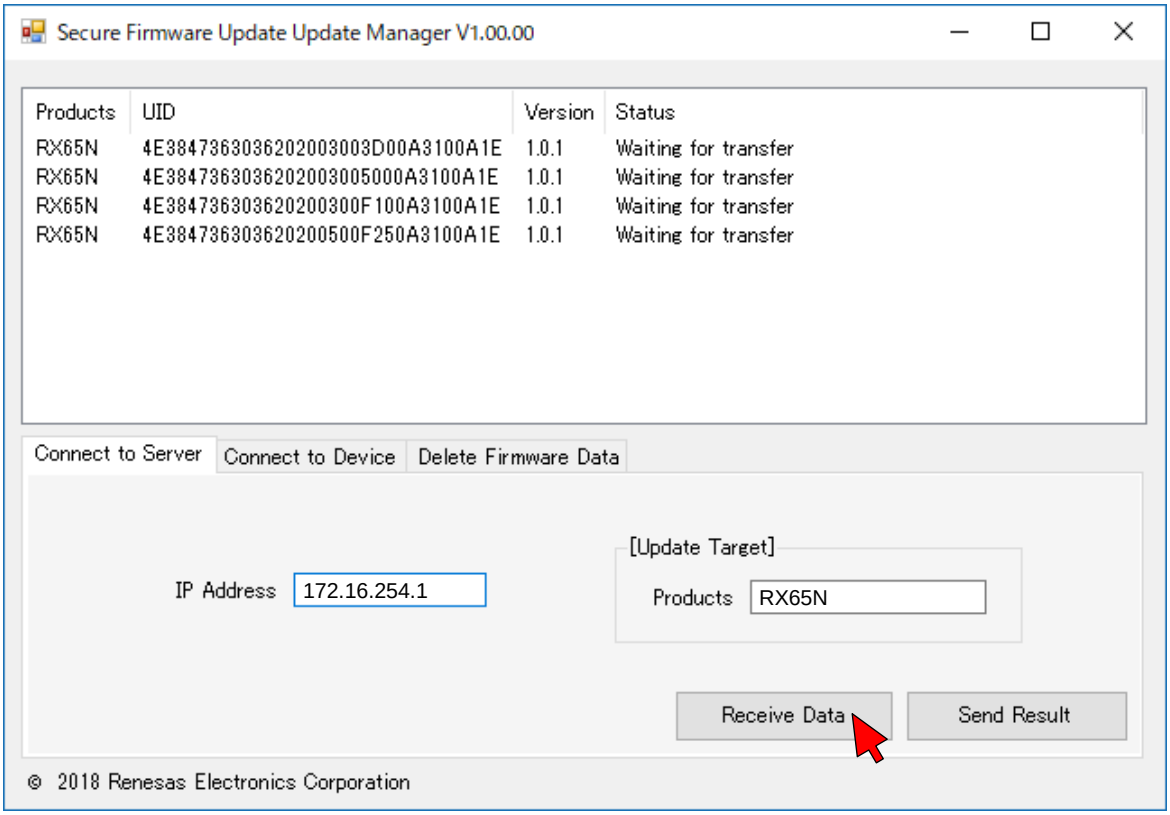

図 2-32 ファームウェアダウンロード操作の GUI イメージ

2.5.4　デバイスへのファームウェアアップデート

デバイスのファームウェアアップデートを行う方法を以下に示します。

デバイスのファームウェアアップデートを行う際は、事前にアップデートするファームウェアをサーバからダウンロードしておいてください。ダウンロード方法は、“2.5.3 ファームウェア管理ツールからファームウェアをダウンロード”を参照してください。

① 仮想サーバとデバイスを Ether ケーブルまたは USB ケーブルで接続してください。

② 仮想サーバのアップデート管理ツール（Secure_Firmware_Update_Update_Manager.exe）を起動してください。

③ デバイスの電源を入れ、ファームウェアアップデートが可能な状態にしてください。

④ Connect to Device タブを選択してください。

＜デバイスと Ether ケーブルで接続した場合＞

Interface の選択 BOX で Ether を選択してください。

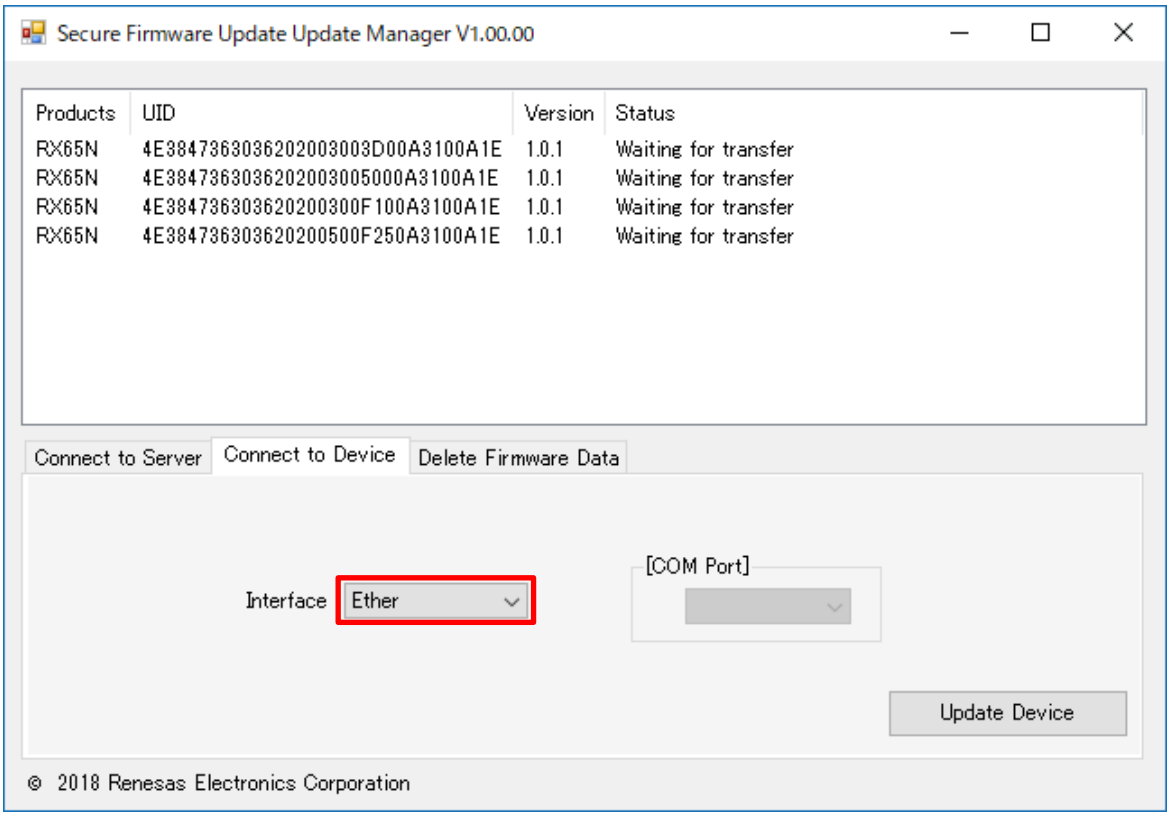

図 2-33 Ether 接続設定の GUI イメージ

＜デバイスと USB ケーブルで接続した場合＞

Interface の選択 BOX で USB を選択し、COM Port の選択 BOX で USB ケーブルが接続されている COM ポート番号を選択してください。（COM ポートは USB ケーブル接続時に自動で割り振られますので、割り振られた COM ポートをデバイスマネージャー等で確認し選択してください）

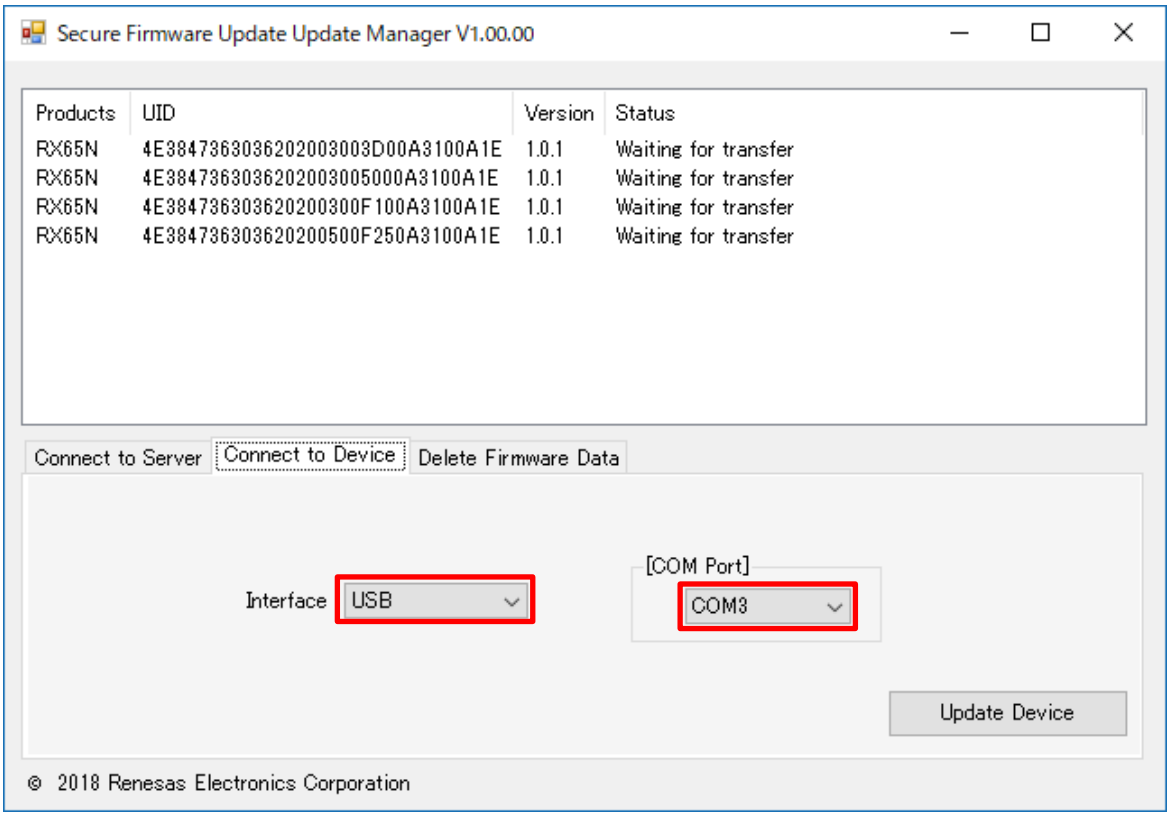

図 2-34 USB 接続設定の GUI イメージ

⑤ Update Device ボタンを押してください。

デバイスのファームウェアアップデートが開始されます。

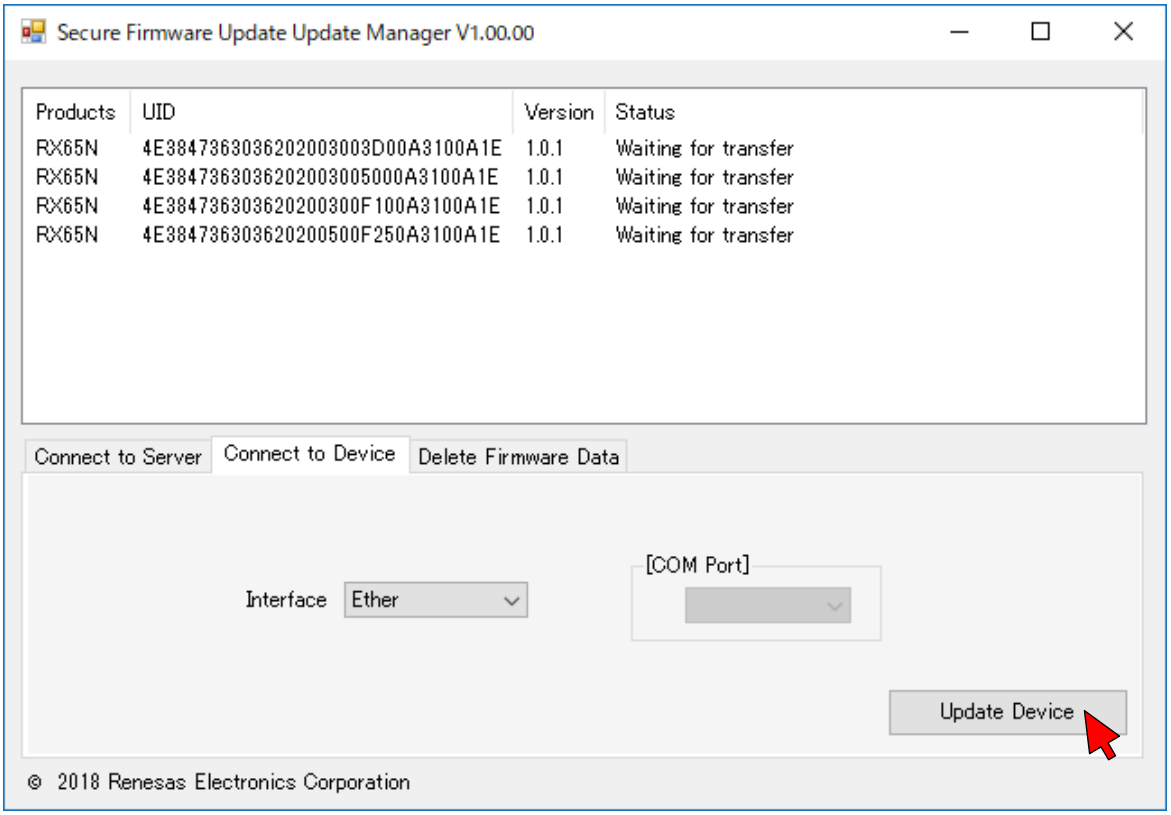

図 2-35 ファームウェアアップデート操作の GUI イメージ

2.5.5　サーバへのファームウェアアップデート結果送信

デバイスのファームウェアアップデート結果をサーバに送信する方法を以下に示します。

① サーバと仮想サーバを Ether ケーブル（同一サブネットでのネットワーク接続）で接続してください

② サーバのファームウェア管理ツール（Secure_Firmware_Update_Firmware_Manager.exe）を起動してください。

③ 仮想サーバのアップデート管理ツール（Secure_Firmware_Update_Update_Manager.exe）を起動してください。

④ Connect to Server タブを選択し、IP Address の入力 BOX にサーバの IP アドレスを設定してください。

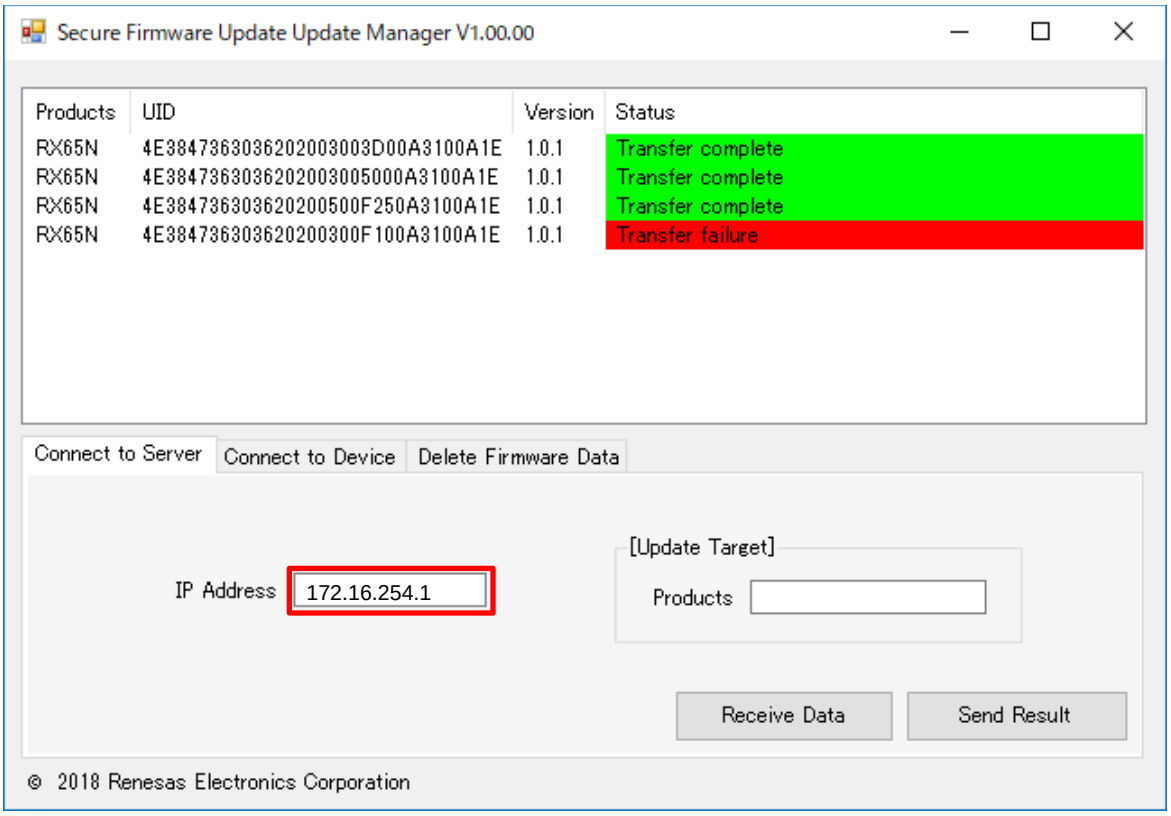

図 2-36 Ether 接続設定の GUI イメージ

⑤ Send Result ボタンを押してください。

仮想サーバからサーバにファームウェアアップデート結果が送信されます。

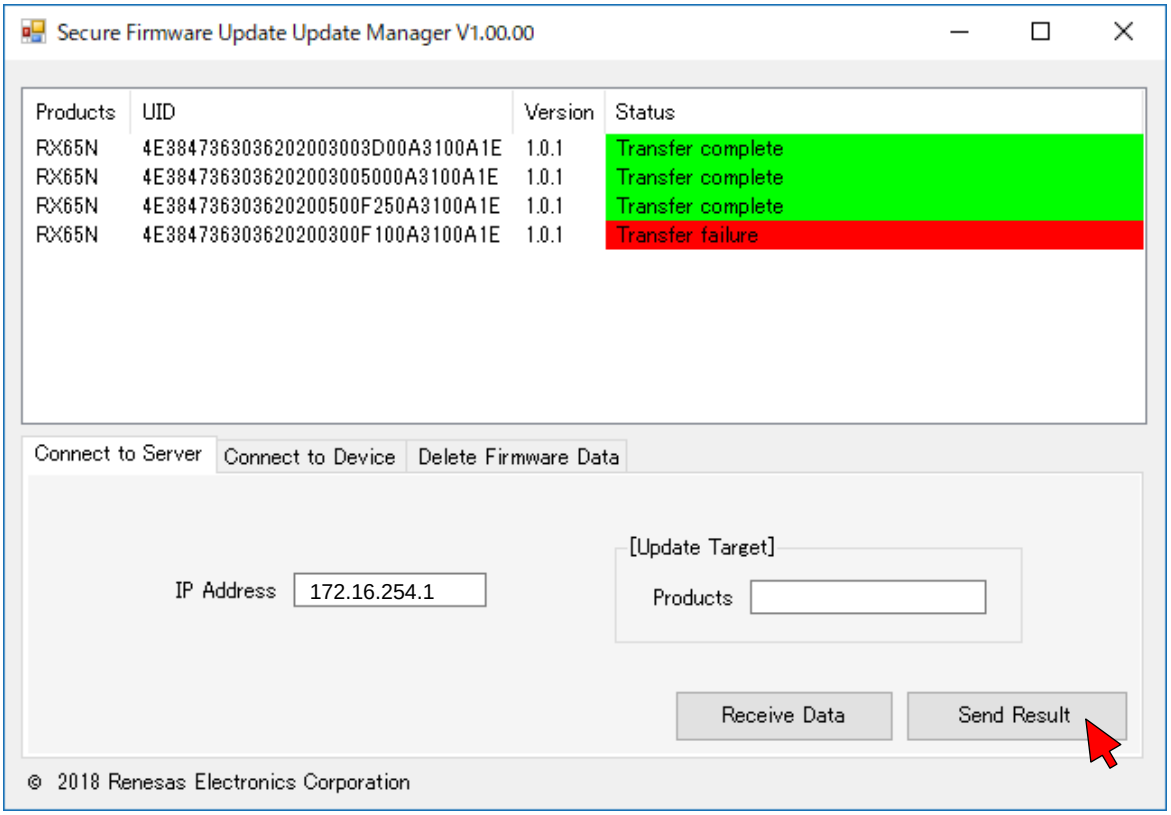

図 2-37 ファームウェアアップデート結果送信操作の GUI イメージ

2.5.6　ファームウェアデータの消去

仮想サーバに保持しているファームウェアデータを消去する方法を以下に示します。

サーバへ未送信のアップデート結果情報がある場合は、その情報は消去されません。サーバへのファームウェアアップデート結果の送信および、同じ製品名で異なるバージョンのファームウェアをダウンロードした際に消去されます。

① 仮想サーバのアップデート管理ツール（Secure_Firmware_Update_Update_Manager.exe）を起動してください。

② Delete Firmware Data タブを選択し、消去したいファームウェアの製品名をリストから選択してください。選択すると Products の入力 BOX には自動で入力されます。

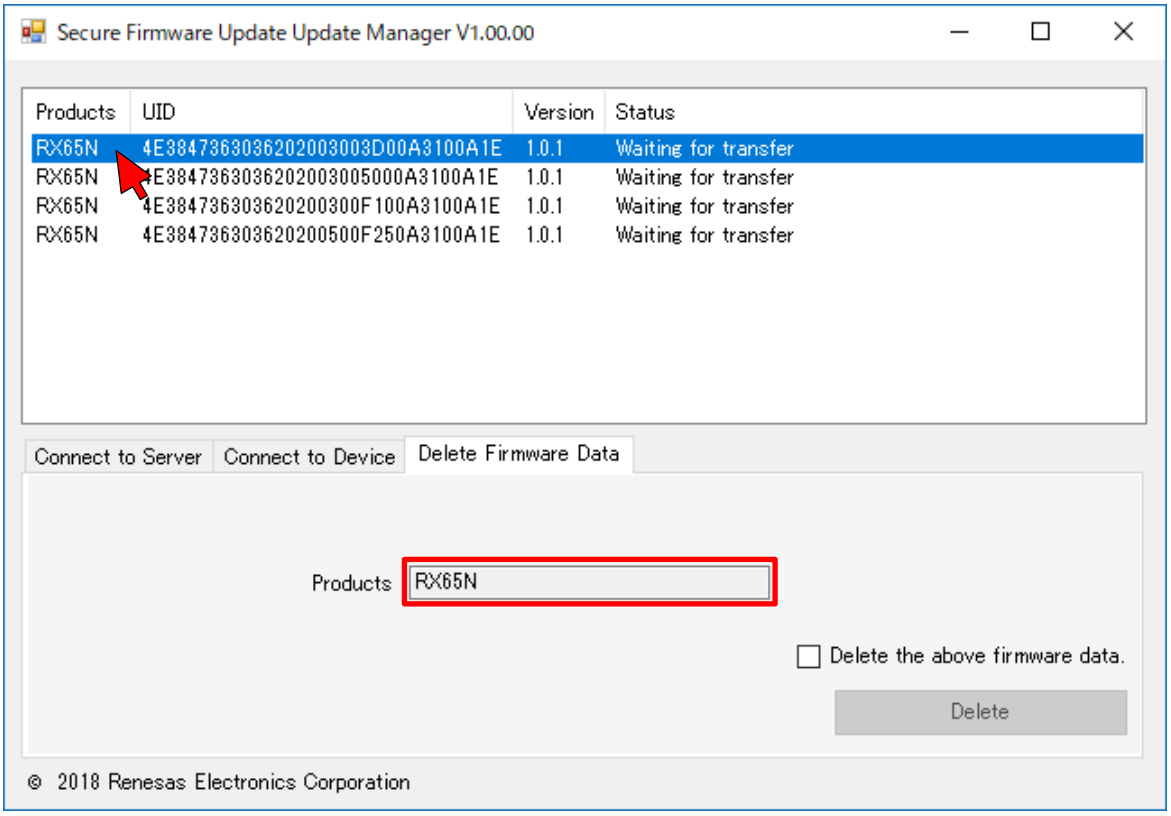

図 2-38 消去する製品名（Products）の指定操作の GUI イメージ

③ 消去するファームウェアの製品名（Products）が決定したらチェックボックスをチェックしてください。

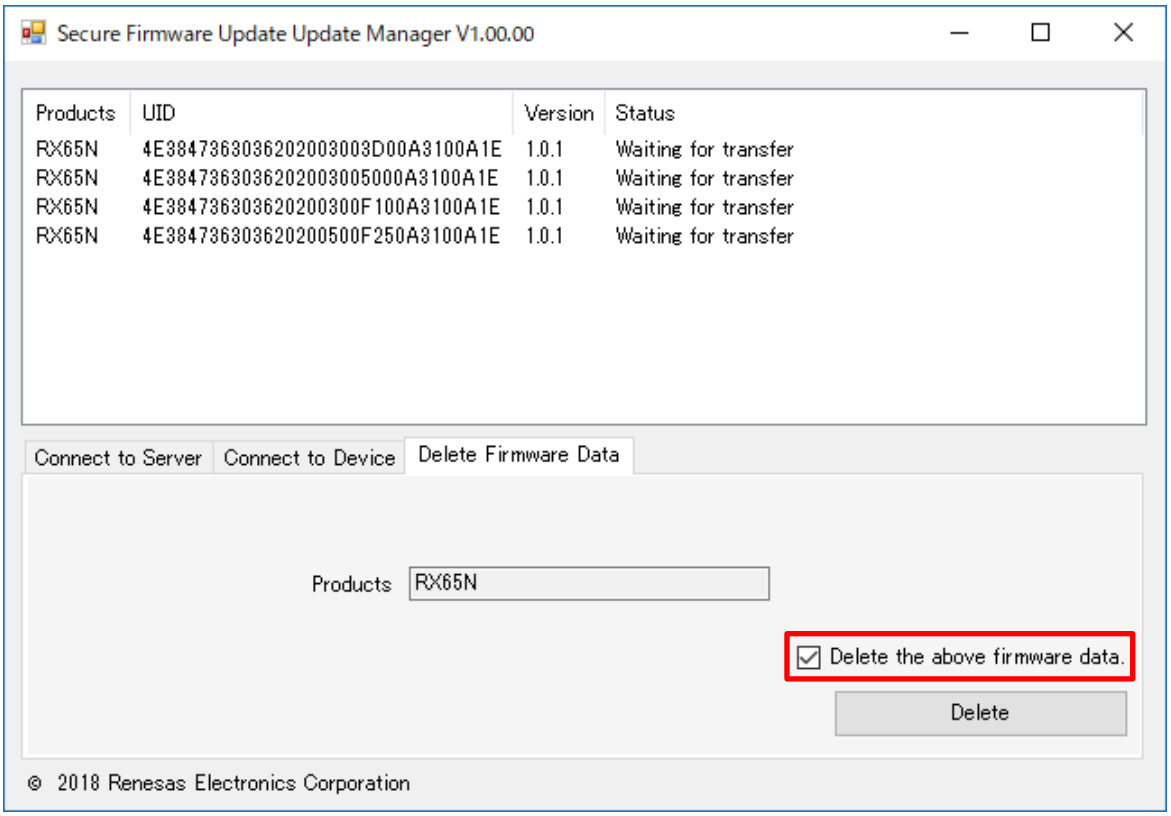

図 2-39 消去する製品名（Products）の再確認操作の GUI イメージ

④ Delete ボタンを押してください。選択した製品名のファームウェアデータが消去されます。

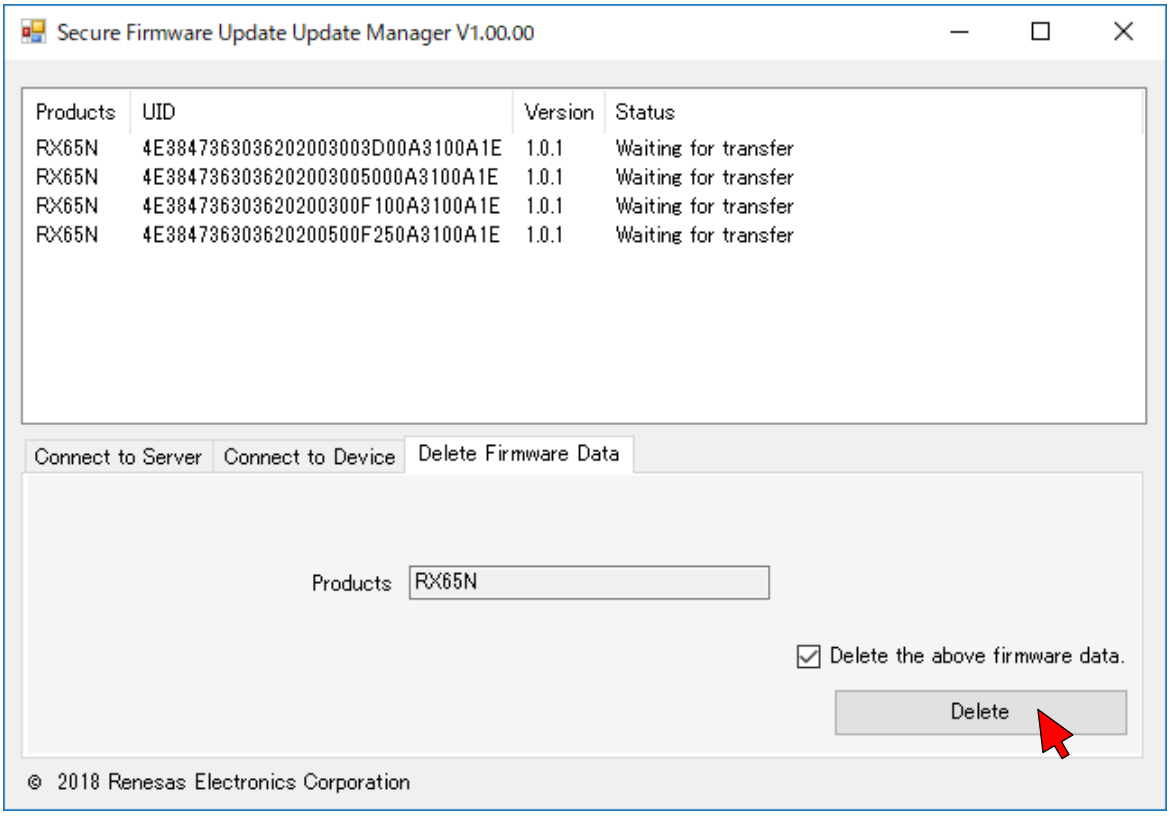

図 2-40 ファームウェア消去操作の GUI イメージ

但し、サーバへ未送信のアップデート結果情報がある場合は、その情報は消去されませんので、“2.5.5 サーバへのファームウェアアップデート結果送信”を参考にサーバへのアップデート結果を送信してください。

2.5.7　　ファームウェアアップデート状況の管理

仮想サーバでのファームウェアアップデート状況の表示について説明します。

ファームウェアアップデートの状況は GUI の情報表示領域に表示されます。

情報表示領域に表示される情報は次の内容です。

① 製品名（Products）

② 機器 ID（UID）

③ バージョン（Version）

④ アップデート状況（Status）

アップデート状況の表示内容を以下に示します。

⑤ ファームウェアアップデート待ち状態。（Status=“Waiting for transfer”）

⑥ ファームウェアアップデート正常終了。（Status=“Transfer complete”）

⑦ ファームウェアアップデートの失敗。（Status=“Transfer failure”）

⑧ ファームウェアアップデートで通信エラーや内部エラー、鍵のエラーや NACK 送信等により発生。（Status=“Transfer abort”）

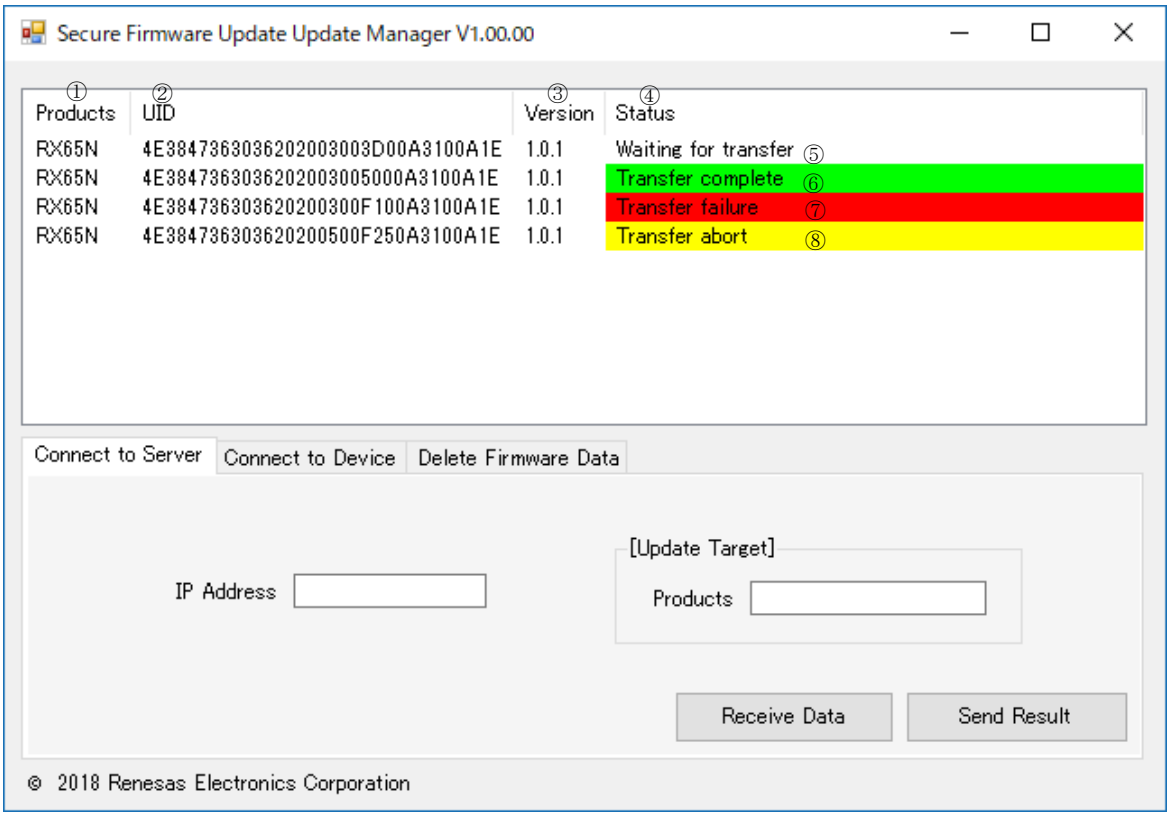

図 2-41 ファームウェアアップデート状況の GUI イメージ

Transfer abort 表示はファームウェアアップデートが中断されたことを表しています。

原因は仮想サーバとデバイス間の通信の問題および、デバイスの内部エラーがあると考えられます。

対応としては機器の接続等を確認し再度ファームウェアアップデートを行ってください。

Transfer failure 表示はファームウェアアップデートに失敗したことを表しています。

原因はファームウェアデータの破損または、デバイス側のフラッシュメモリの問題が考えられます。

対応としては再度サーバからファームウェアをダウンロードしアップデートを行ってください。それでも Transfer failure と成る場合は、デバイスのフラッシュメモリに問題があると思われますのでデバイスの交換等を検討してください。

参考　MIT ライセンス

本ソリューションのアップデート管理ツールには MIT ライセンスの FtpServer および sockets-for-pcl ソフトウェアが含まれています。

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/contact/

改訂記録

Rev.	発行日	改訂内容	
		ページ	ポイント
1.00	2018/12/19	54	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. 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」にしたが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、製品型名毎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、個々の製品毎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)

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 エレクトロニクス株式会社　〒135-0061　東京都江東区豊洲3-2-24（豊洲フォレシア）

■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：https://www.renesas.com/contact/

Colophon 6.0