

RZ/G,RZ/V セキュリティ ソリューション概要

ルネサス エレクトロニクス株式会社

免責事項

1. ルネサスエレクトロニクスおよびその関係会社は、本資料に記載された内容（以下「本内容」といいます）の正確性、有用性、確実性その他いかなる保証もするものではありません。本資料に記載された製品の物理的、電気的仕様、特性、ブロック図等は、予告なしに変更することがあります。ルネサスエレクトロニクスおよびその関係会社は、本資料に記載された内容から生じるいかなる損害についても責任を負うものではありません、本資料に記載された情報は、予告なしに変更されることがありますので、あらかじめご了承ください。
2. 記載されている会社名および製品名は、各社の商標または登録商標です。

本書の目的

本書ではRZ/GおよびRZ/V向けセキュリティソリューションとして、どのようなものが提供・準備されているかについて説明します。詳細については下記WEBページよりマニュアルをダウンロードしてください。

RZ MPU Security Package

本書は、下記RZ/GおよびRZ/Vのうちセキュリティ機能を搭載したデバイスを対象にしています。

<対象デバイス>

RZ/G2L, RZ/G2LC, RZ/G2UL

RZ/G2H, RZ/G2M, RZ/G2N, RZ/G2E

RZ/G3S

RZ/V2L

RZセキュリティソリューションのコンセプト

RZセキュリティソリューションは、IoT製品をサイバー攻撃から保護します。



サイバー セキュリティ ソリューション

-Trustzone (Trusted Execution Environment) とセキュアブートを使用して、IoT製品をサイバー攻撃から保護します。



IEC62443 Ready ソリューション

-Secure IPを使用したRZセキュリティ機能は、IEC62443-4-2を取得するのに効果的です。

サイバーセキュリティ ソリューション

セキュリティ機能

提供しているセキュリティ機能一覧です。

下記WEBページより該当デバイスのSecurity Packageをダウンロードし、VLP*に組み込む事で利用可能になります。

詳細はSecurity Packageに含まれているマニュアルを参照してください。

*VLP : Verified Linux Package

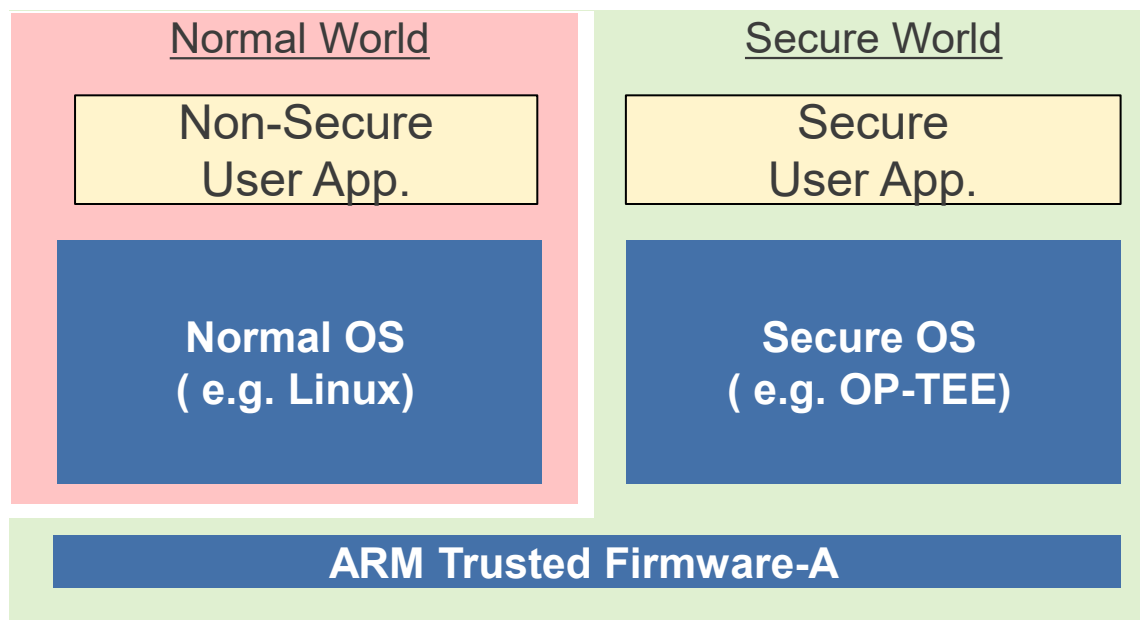
RZ MPU Security Package

機能	説明	使用する機能やツール			
		Mask ROM	Secure IP	Trust Zone	署名付加ツール
Trusted Execution Environment (TEE)	ARM Trust Zoneを用いた隔離実行環境			✓	
セキュアブート	起動時に読み込むプログラムの改ざんを検出	✓	✓	✓	
セキュアブート用署名付加	F/Wに改ざん検出用の署名を付加		✓	✓	✓
セキュアデバッグ	デバッガ接続認証 (認証なし/JTAG認証あり/接続禁止)	✓	✓	✓	

ハードウェア

ARM Trust Zone

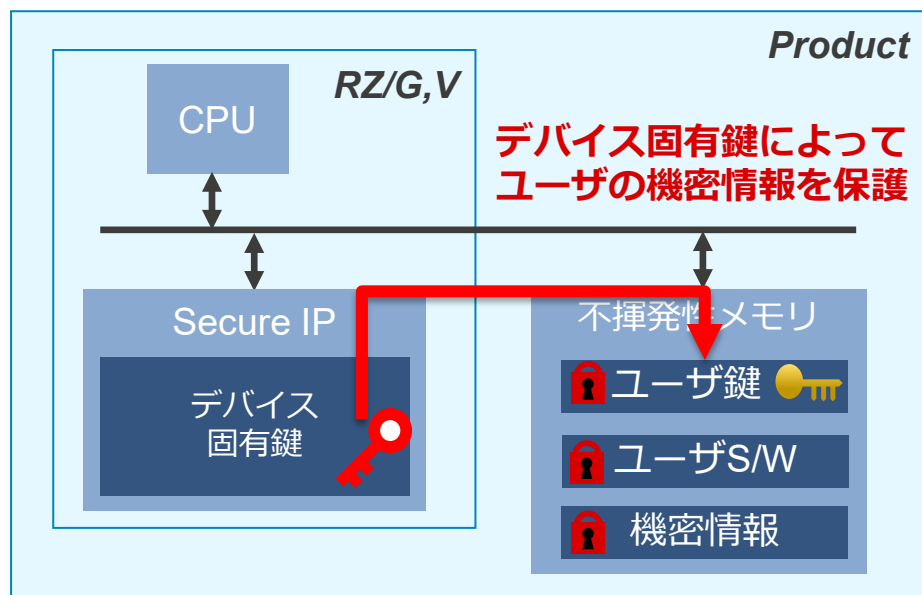
ソフトウェアの実行環境をノーマルワールド（非セキュアな領域）とセキュアワールド（セキュアな領域）に分離し、セキュアな領域を外部アクセスから隔離する事で不正アクセスから保護します。



ハードウェア

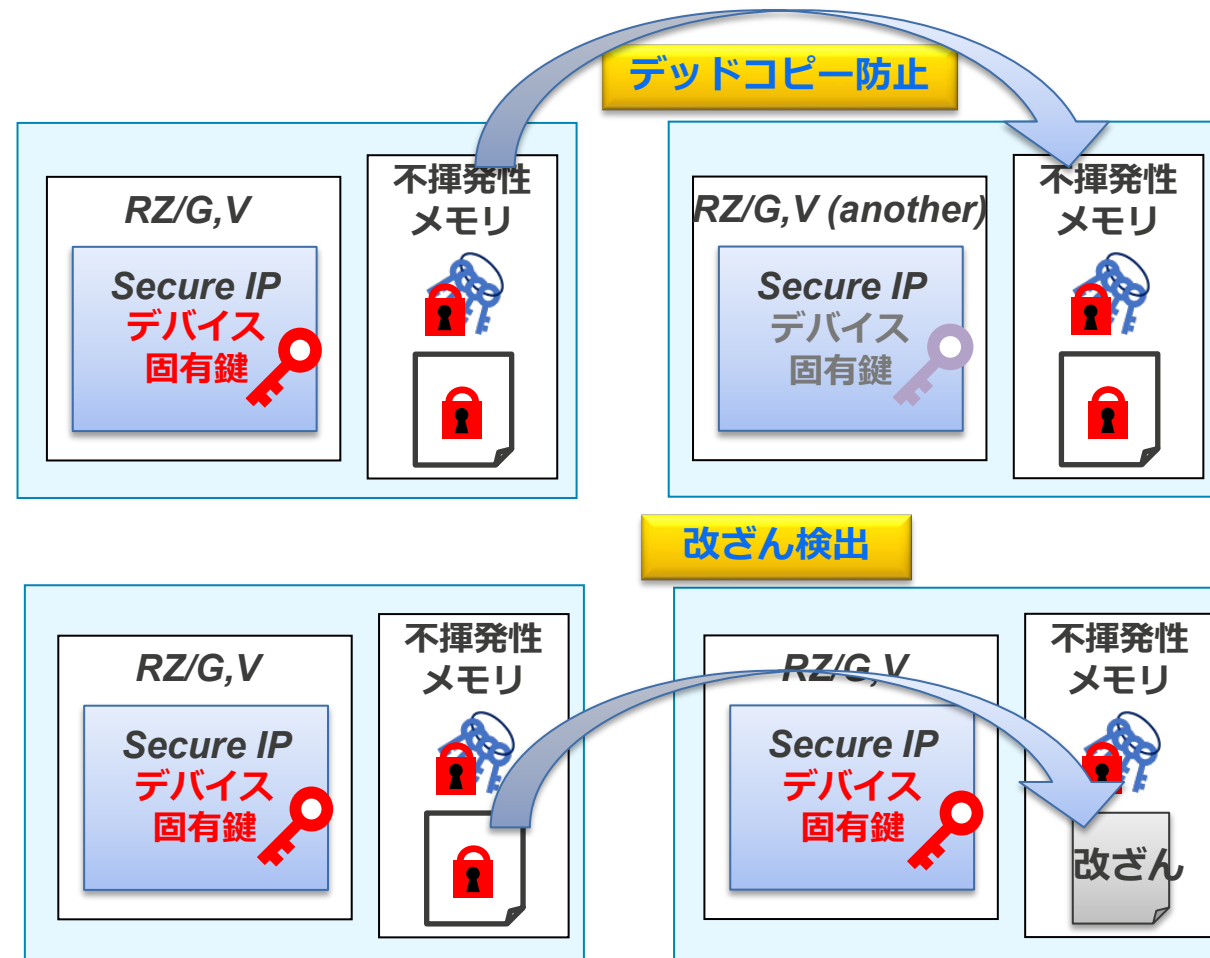
Secure IP

Secure IPの外部からアクセス困難なデバイス固有鍵で重要なデータ（ユーザ鍵、ユーザS/W、機密情報etc.）を暗号化する事で保護します。



なぜ機密を保護できるのですか？

デバイス固有鍵は、ハードウェアメカニズムから派生した一意の値に基づいており、この鍵はSecure IPによってのみ参照されます。



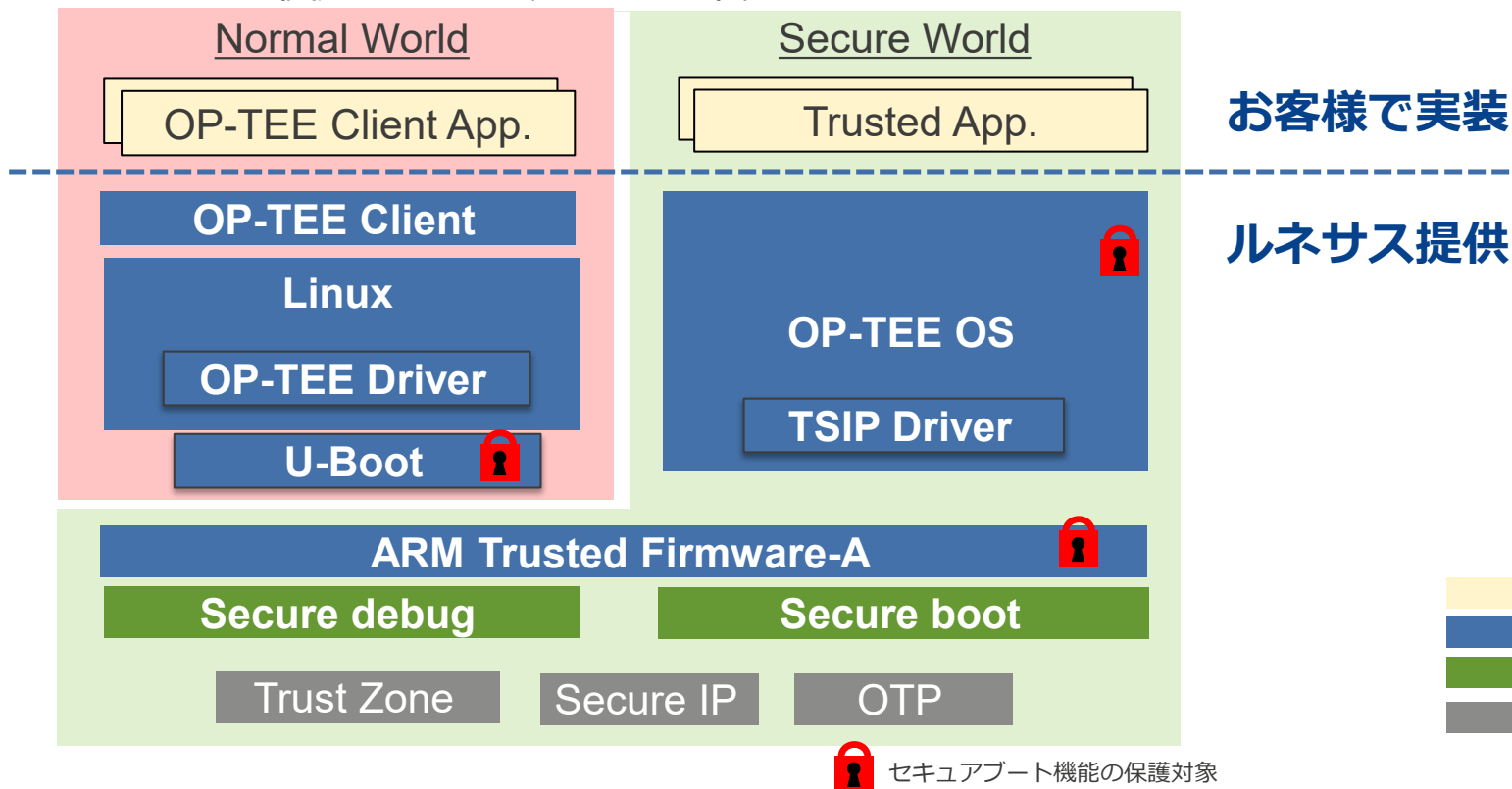
ソフトウェア

Security Package

RZファミリMPU向けに提供しているOS毎にセキュリティパッケージを提供します。

セキュリティパッケージにはセキュリティIPドライバやセキュアブート機能、暗号化/復号API、ARM Trusted FirmwareおよびOP-TEEを使用したリファレンス環境などが含まれます。

OP-TEEを使用したリファレンス環境



サービス

Renesas Key Wrap Service

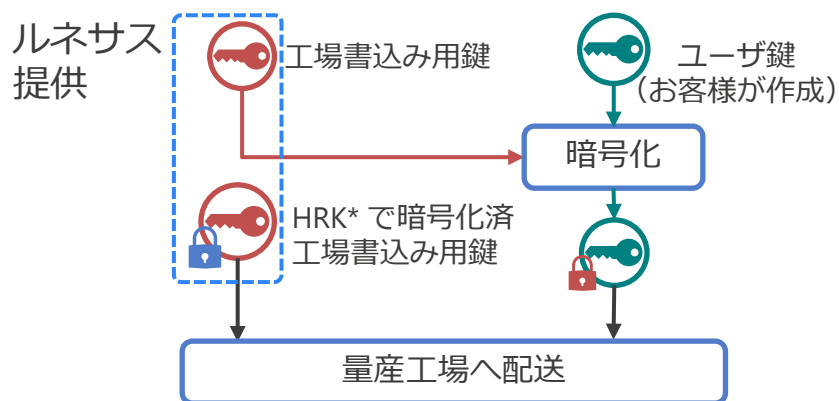
お客様の量産工場での鍵書き込みの安全性をより高めるサービスです。

本サービスを利用することでお客様個別の工場書き込み用鍵(UFPK)* を使用し、ユーザ鍵の漏洩リスクをより低減できます。

<Key Wrap Serviceを利用しない場合>

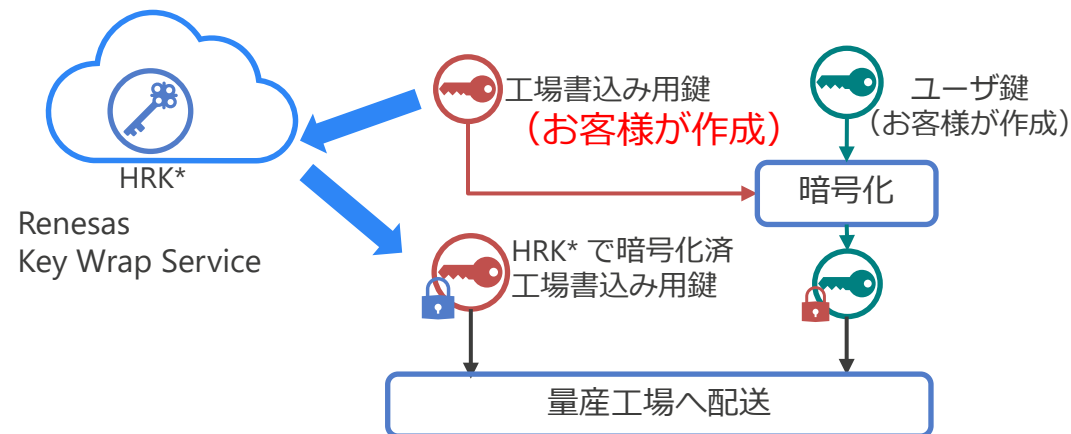
工場書き込み用鍵は**全ユーザ共通**

お客様開発サイト



<Key Wrap Serviceを利用する場合>

工場書き込み用鍵は**お客様個別**



*工場書き込み用鍵(UFPK: User Factory Programming Key) : ユーザ鍵がお客様開発サイトから量産工場に配送されデバイスに書込まれるまでの間、ユーザ鍵を保護する為の鍵

*HRK (Hardware Root Key) : 工場書き込み用鍵を保護する為の鍵

IEC 62443-4-2 READY ソリューション

IEC 62443-4-2 READY ソリューション

デリバラブルズ

弊社RZ/G,V製品をもちいてIEC 62443-4-2を取得するお客様へ、セキュリティ開発と認証にかかる期間／コストを大幅に削減する3つのアイテムを提供いたします。



Linux向け セキュリティパッケージ

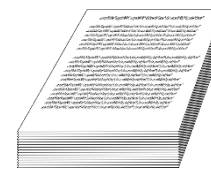
ルネサスでは弊社HPにて、RZ/G, V製品向けセキュリティパッケージを提供しております。こちらに含まれるドライバソフトウェアとライブラリをご使用いただくことにより、IEC62443-4-2の適合性評価で必要なセキュリティ機能を実現することが可能です。

Competitive
point



セキュリティPKG 適合性評価レポート

ISASecure認定の認証機関が発行したLinux向けセキュリティパッケージのIEC 62443-4-2適合性評価レポートを提供いたします。こちらをご使用いただくことにより、アプリケーションが対応すべきセキュリティ要件が一目瞭然となり、調査・設計工程の工数を大幅に削減することが可能となります。



CIP Linux パッケージの 適合性評価レポート

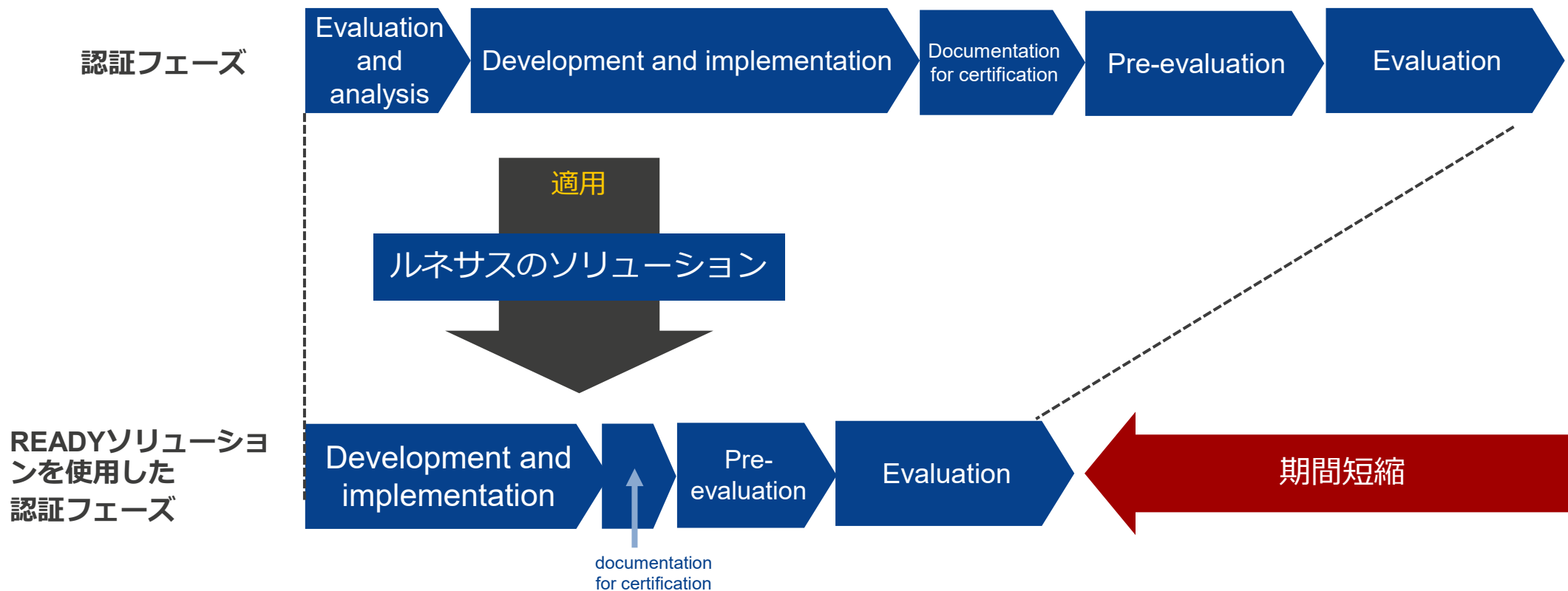
IEC 62443-4-2の多くの要件は、デバイスだけでなく、ソフトウェア全般によって実現する必要があります。[CIPが提供するLinuxパッケージの適合性評価レポート](#)をご使用いただくことにより、お客様はIEC62443-4-2に適合したアプリケーションを効率的に開発／実装することが可能です。

ご要望の方は代理店またはルネサス営業窓口へご連絡ください

IEC 62443-4-2 READY ソリューション

ベネフィット

ルネサスのソリューションを適用することで認証フェーズを大幅に削減



[Renesas.com](https://www.renesas.com)