ホワイトペーパー

組み込み IoT 設計におけるセキュリティ課題を解決するソリューション

2019 年 8 月

概要

組み込み IoT 設計のセキュリティ対策は、熟練の開発者でも、課題が多く時間を要する作業です。以下では、主な 6 つのセキュリティ課題に対し、ルネサスは、プラットフォームベースのアプローチを提案しています。ハードウェアとソフトウェア双方に最新の技術進歩を取り入れた多層的な保護を施すことで、徹底的（in-depth）かつ包括的な防御機構を提供するというものです。

IoT のセキュリティ課題

2020 年までに世界全体で、およそ 310 億台の機器が IoT（Internet of Things）化される見通しですが、その多くはセキュリティ管理が不充分で、ハッキングに対して無防備な状態にあります。これほど多くの組み込みシステムが脆弱性を抱えたまま設計されているのはなぜなのでしょうか。最大の理由は、エンジニアが組み込みアプリケーションやデバイスに、セキュリティ対策を施す際に直面する膨大な課題や複雑な手続きが、開発の大きな課題となっていることです。エンジニアは日々巧妙化する脅威環境に通じていなければならない上、絶えず進化するセキュリティ基準も満たさなければなりません。同時に、複雑なアプリケーションの中には複数の規格への対応が要求されるものもあり、これはデバイスの互換性やフレキシビリティの妨げになります。多くの開発シナリオでは、高レベルのセキュリティ機能ほどコストがかかり消費電力も増えるため、エンドデバイスの市場性にも悪影響を及ぼしかねません。

本ホワイトペーパーでは、組み込みシステムエンジニアが最もよく直面する 6 項目のセキュリティ課題を取り上げ、安全なデバイスやサービス、システムをいち早く市場に届けるために、セキュリティ設計ワークフローの簡素化・効率化に役立つ洞察と最適な回答を提供します。

本ホワイトペーパーで検討した、組み込みシステムエンジニアの抱える 6 つのセキュリティ課題を以下に示します。

1. 2019 年はどのようにデバイスのセキュリティ対策を行えばよいか？
2. 製品を不正コピーから守るにはどうしたらよいか？
3. どうすればセキュリティを簡素化できるか？
4. 多様なセキュリティの脅威からデバイスを守るにはどうしたらよいか？

5. セキュリティの専門家ではないが、安全な製品をつくりたい。知っておくべきことは？

6. セキュリティ対策はベンダーのソリューションやサポートを活用し、自身のリソースを最終製品の差別化に集中させるにはどうしたらよいか？

課題 1——2019 年はどのようにデバイスのセキュリティ対策を行えばよいか？

数年前までは、アプリケーション開発者が製品のセキュリティを心配する必要がありませんでした。なぜなら、デバイスやアプリケーションは現在のようにネットワークに接続されていなかったからです。今日では、最も基本的なアイテムでさえ——照明から、乳幼児監視モニター、医薬品の容器に至るまで——インターネットやクラウドに接続されています。こうしたアイテムのセキュリティは見過されるか、気づいたときには手遅れである場合が多くなっています。

2019 年は、IoT アプリケーションをサイバー脅威から守ってデータや機能を保護することが、開発者にとって極めて重要な関心事となります。セキュリティは、ハードウェアとソフトウェアレベルの両方でデバイスに最初から組み込まれていなければなりません。プラットフォームベースのセキュリティアプローチは、ハードウェアとソフトウェアの両方で最新のセキュリティ技術を活用し、多層的な防御機構を構築することで、徹底的かつ包括的な保護を提供します。

ハードウェア面の効果的なセキュリティ対策には、以下を盛り込む必要があります。

- 鍵（key）が暗号化されていない状態でアクセスできないようにする安全な鍵管理（key management）。デバイスは、真にセキュアなデバイス固有 ID（device-unique identity）やプロビジョニングを実現するために、秘密鍵（private key）を含む種々の鍵を安全に生成・保存できなければなりません。

- デバイス上での暗号化動作（cryptographic operation）を加速するハードウェア暗号化アクセラレーション（hardware-accelerated encryption）、ハッシュ化、真性乱数発生器（true random number generation）。こうしたハードウェアのサポートは、暗号化に要する時間と労力を節約します。

- RAM やフラッシュメモリの特定領域を不正アクセスから保護するための安全なメモリアクセス。分離されたメモリ領域は、機密のコードやデータを非セキュア（non-secure）コードやデータから分離し、ライトワンス（write-once）保護メモリは、コードやデータを改ざんや再プログラミングから保護します。

- デバッグやプログラミングへのアクセスの保護。これにより、ハッカーがデバッガやプログラミングインターフェースを攻撃ベクトルとして利用するリスクが減ります。

ソフトウェア面の効果的なセキュリティ対策には、以下を盛り込む必要があります。

- 検証済みのアプリケーションフレームワークと標準 API を搭載し、統合化・最適化された商用グレードのソフトウェア。

- ハードウェアのセキュリティ機能への容易なインターフェースを提供するドライバレベルの API。

- マクロレベルのセキュリティ機能、「ルートオブトラスト」（信頼基点）、信頼できるソースやコードを認識する能力をはじめ、多様なセキュリティ機能を提供する、API コレクションを備えた暗号ライブラリ。

- Hypertext Transfer Protocol Secure（HTTPS）や Transport Layer Security（TLS）、その他のクラウド専用プロトコルなど、一般的な通信プロトコルやトランスポートのための組み込みサポート。

ルネサスは、組み込みセキュリティのトッププロバイダとして数十年の実績があり、今日のコネクテッド〔ネットに接続〕製品群におけるセキュリティニーズの高まりに応える万全の体制を整えています。ルネサスは、組み込みセキュリティへのプラットフォームベースのアプローチにより、さまざまな組み込み製品に高度なセキュリティ保護を提供する多層的な開発インフラを市場に提供しています。

例えば、Renesas Synergy™プラットフォームは、さまざまなレベルでセキュリティを提供するために、あらかじめ組み込まれ、検証された、プロダクショングレードのソフトウェアとスケーラブルでピン互換のマイクロコントローラユニット（MCU）ファミリを含む、包括的かつ品質保証された（qualified）開発プラットフォームです。Synergy プラットフォームは、IoT アプリケーションが安全で堅牢な技術基盤上に構築されることを保証します。

Synergy プラットフォームは、セキュア暗号化エンジン（Secure Crypto Engine: SCE）モジュールによって、複数の鍵生成（key generation）オプションを提供しています。SCE は、ハードウェアベースの独特な暗号化デバイス ID を生成します。この ID は、セキュリティ MPU（Security Memory Protection Unit: SMPU）とフラッシュアクセスウィンドウ（Flash Access Window: FAW）を使用して、内部フラッシュ（internal flash）に安全に保存することができます。これらのメモリ保護機能は、セキュアブートコード、デバイスの電子証明書／鍵、その他の機密データの格納にも使用可能です。加えて SCE は、機密情報――セキュアでない場所にあるものも含め――がリスクにさらされるのを防ぐためのセキュアな鍵保管（key storage）も提供します。鍵の隔離は、MCU に固有の鍵のラッピング（key wrapping）によって確保されます。これは、MCU ごとに個別に鍵を暗号化するため、ラッピング鍵にアクセスできるのは、その鍵をラッピングした MCU の SCE モジュール内においてのみとなります。

セキュアな暗号化エンジン

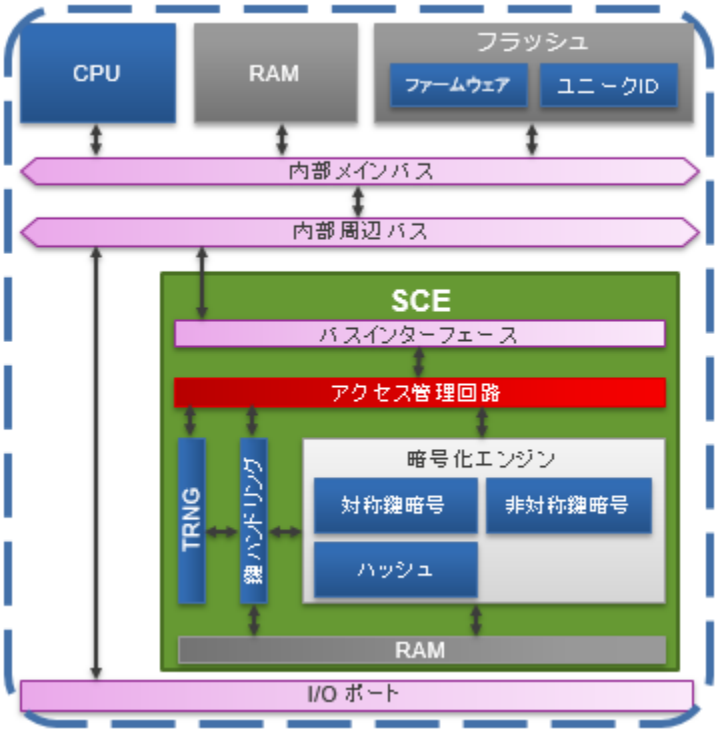

図 1: MCU 内の隔離されたサブシステムであるセキュア暗号化エンジン（出典：ルネサスエレクトロニクス）

加えて、開発プラットフォームは、クラウドにも安全かつ容易に接続できなければなりません。IoT アプリケーションがますます複雑化し、〝セーフティクリティカル〞〔安全性の確保が重要視される〕になるにつれ、必要なデータ処理能力も加速度的に増大しています。こうしたシステムは、IoT データの演算やストレージのためのハイパースケールなインフラを確保するに当たって、クラウドコンピューティングへの依存を増しており、クラウドへの安全な接続が不可欠となっています。Synergy MCU は、組み込み MQTT と TLS モジュールによって、クラウド接続をサポートします。Synergy Cloud 接続アプリケーションは、Amazon Web Services（AWS）、Google Cloud、Microsoft Azure をはじめ、主要なクラウド環境へのセキュアな組み込み接続を提供します。

課題 2——製品を不正コピーから守るにはどうしたらよいか？

自社製品の模倣品が市場に出回るのを防ぐには、自社製品が簡単にクローンを作成できないようにすればよいでしょうか。そのためには、デバイスに独自の機能を組み込む必要があります。

グローバルなサプライチェーンでは今、全製造環境とサイクルを通じて、製品の完全性（integrity）や真正性（authenticity）を確保するために、注意力の向上やセキュリティの強化が求められています。

その方法の一つが、安全な製造サプライチェーンを通じて信頼性のあるデバイスを提供することで、知的財産へのリスクを軽減し、生産工程の完全性（integrity）を維持することです。Synergy セキュアブートマネージャ（Secure

Boot Manager）は、遠隔地にある製造施設で、Synergy MCU フラッシュメモリに認証されたファームウェアを確実かつ安全にプログラミングできる、ファームウェアのセキュアなフラッシュ書き込みソリューションを提供します。これにより、ファームウェアの海賊版の作成、改ざん、不正に複製されたハードウェアへのインストールを防止できます。

Synergy セキュアブートマネージャは、独自の ID、ハードウェア保護キー、セキュアブートローダ、セキュアフラッシュ更新モジュール、そして、MCU ハードウェアと連動する暗号化された API を通じて、強力な「ルートオブトラスト」（信頼基点）を実現します。「ルートオブトラスト」は、安全なネットワーク接続によって、プロセッシングユニットの作成やセットアップを行うための大容量プログラマシステムにあらかじめインストールされます。セットアップされたチップはデータを安全に保存し、その利用を厳重な管理下に置きます。

Renesas Synergy セキュアブートマネージャ

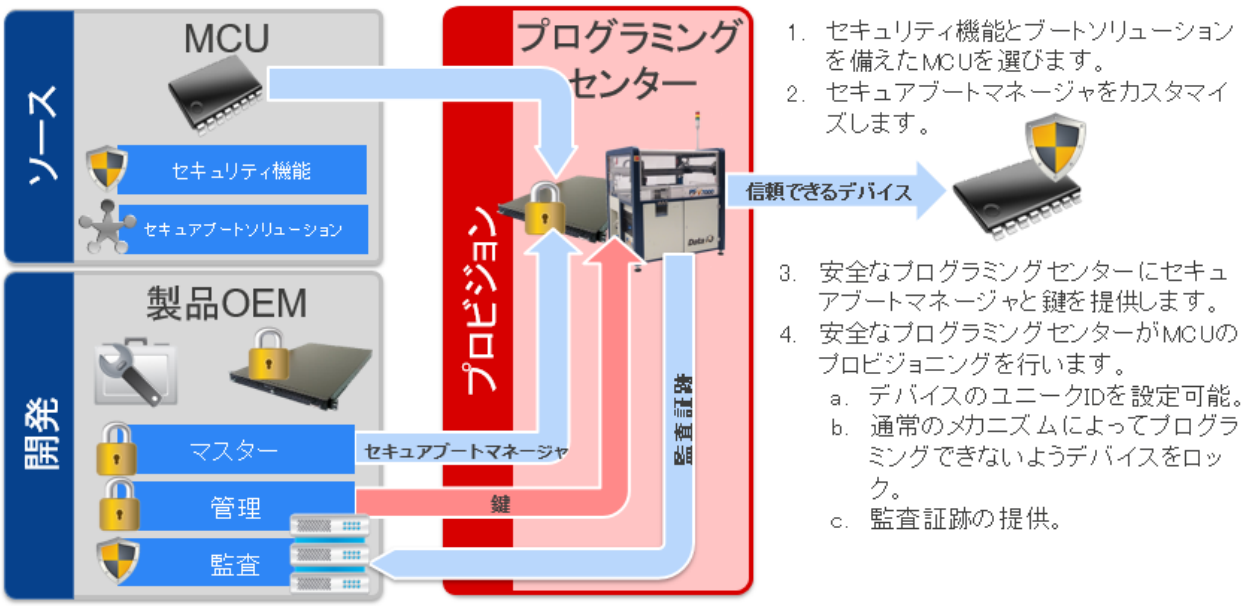

図 2: Renesas Synergy セキュアブートマネージャはファームウェアのセキュアなフラッシュ書き込みソリューションを提供
（出典：ルネサスエレクトロニクス）

いったん市場に出荷された後、ファームウェアのアップデートが必要な場合は、チップ上の「ルートオブトラスト」が、フラッシュメモリ書き込み前にファームウェアの認証や複号を行うため、認証ファームウェアを Synergy MCU のフラッシュメモリに安全にアップデートすることができます。すべての動作は、Renesas Cloud 接続ソリューションによって信頼性が確保されたセキュアなクラウドインフラを通じて、安全にプロビジョニングされます。

一部の Renesas パートナーも、ソリューションやサービスのセキュアなプロビジョニングやプログラミングをサポートしており、合理的なコストでの製造セキュリティの提供に努めています。

課題 3——どうすればセキュリティを簡素化できるか？

組み込みデザイン向けに高度な階層化（layered）セキュリティを設計するのは複雑で時間がかかります。短期間で多くの成果を得る方法の一つは、最新のセキュリティ技術やプロトコルがあらかじめ組み込まれている開発プラットフォームを選ぶことです。Synergy プラットフォームを用いれば、セキュアなアプリケーションを作成するのに最新の関連プロトコルやセキュリティ対策をすべて学ぶ必要はありません。

Synergy Software Package は、セキュアなコネクテッド組み込みシステムの開発に伴う複雑な機能や手続きを簡素化します。このソフトウェアでは、フラッシュと SRAM のメモリ領域がセキュア化されるため、読み取り／書き込み保護されたコードを作成・保存することができます。これにより、一時鍵（temporal key）や秘密鍵、その他の機密データを保存するのに使用できるカスタマイズ可能なメモリ領域を作成できます。

Synergy プラットフォームは、公開鍵基盤（public key infrastructure: PKI）——電子証明書による認証を行う暗号方式——と、事前共有鍵（pre-shared key: PSK）——ピア間で事前に設定した共有鍵が一致した場合に認証される暗号方式——の両方をサポートしています。PSK は簡易な暗号方式であり、少数のユーザのアクセス制御などに適切な保護レベルを提供できます。これに対し PKI は、ユーザの認証、電子証明書の作成・配布・維持・管理・取り消しが行える非対称鍵暗号方式であり、導入や運用管理はより複雑になります。公開鍵と秘密鍵の二つの対となる鍵を用いる PKI は、セキュリティのより高い暗号モデルとされており、一般に大規模な暗号化システムにおける認証に使用されます。

Synergy プラットフォームは、ハードウェアのセキュリティ機能や暗号化機能とのインターフェースが容易に構築できる標準 API を搭載し、最適化されたコマーシャルグレードのソフトウェアを提供しています。アプリケーションフレームワークは、アプリケーションコードと低層階のドライバ間の統一インターフェースによって、わずらわしいワイヤレスドライバの統合を簡素化・効率化します。こうした〔ドライバ〕レベルの抽象化によって作業の複雑さが大幅に軽減し、ネットワークスタックを統合、必要に応じてドライバのスイッチアウトやドロップインを行うことも容易になります。

課題 4——多様なセキュリティの脅威からデバイスを守るにはどうしたらよいか？

今日のサイバー脅威環境（cyberthreat landscape）には、さまざまな悪意あるエージェントやリスクが蔓延しています。悪用〔システムの脆弱性を攻撃するコードやプログラム〕や攻撃手段は、至るところで保護されていないものを待ちかまえています。多様なセキュリティの脅威からデバイスを守るには、ハードウェアベースの鍵生成によってデバイス ID を保護する必要があります。こうした ID は、内部フラッシュに安全に保存され、信頼を確立するのに活用されるほか、設計に追加して、ターゲットアプリケーションに設定されることで、高度なプライバシーを提供します。

強力なデバイス ID の確立によって、個々の IoT デバイスを一意的に識別し（singularly identified）、唯一のものとして認証することが可能となります。これにより、各デバイスは個別にセキュリティ保護され、他の保護されたデバイスやサービスとの暗号化された通信を行うことができます。強力なデバイス ID は、以下の機能の提供により、何重ものセキュリティ保護を通じて、さまざまなセキュリティの脅威を防ぎます。

- **信頼**。デバイスはネットワークに接続されると、他のデバイスやサービス、ユーザとの間で信頼を確立するために真正性を保証して、暗号化されたデータや情報を安全にやりとりできるようにしなければなりません。「信頼」は、デバイスを適切に認証して、それが真正のデバイスであり、偽装されたものでないことを保証することから始まります。

- **プライバシー**。IoT ネットワーク内でキャプチャされ、共有されるデータや情報には往々にして、機密データや個人データ、金融取引に関するデータが含まれています。こうしたデータは、機密かつ安全に管理して、規制コンプライアンスにも対応しなければなりません。セキュリティで保護されたデバイス ID は、IoT デバイスやシステムが共有データにアクセスする際に、データの機密性を保証する要となります。

- **完全性**。ネットワーク内で共有されたデータが改ざんされていないことを保証することは、階層化セキュリティのキーエレメントです。データの「完全性」は見過されがちな要件ですが、コネクテッドデバイスやシステムは、伝送される情報の「真正性」(信頼)、「機密性」(プライバシー)、「完全性」に依存しています。

Renesas Synergy MCU SCE ハードウェアセキュリティ機能(シリーズ別)

	機能		Key Wrap	NIST CAVP	S7	S5	S3	S1
IDおよび鍵交換(非対称)	RSA	鍵生成、署名/検証[1]	Y	Y[5]	1024/2048/4096	1024/2048/4096		
	ECC[4]	鍵生成、ECDSA, ECDH[2]	Y	WIP	NIST P192/P224/P256/P384	NIST P192/P224/P256/P384		
	DSA	署名/検証			L:2048/1024, N:256/226/160	L:2048/1024, N:256/226/160		
プライバシー(対称)	AES	ECB, CBC, CTR	Y	Y	128/192/256	128/192/256	128/256	128/256
		GCM		Y	128/192/256	128/192/256	128/256	
		XTS, CCM			128/256	128/256	128/256	
	3DES	ECB			192	192		
		CBC			192	192		
		CTR			192	192		
データの完全性	Hash	GHASH		Y	Y	Y	Y	
		SHA1/224/256		Y	Y	Y		
	TRNG	DRBG-AES-128によるハードウェアエントロピー		Y	Y	Y	Y	Y
	Unique ID				Y	Y	Y	Y
データの保護	MPU	Arm、バスマスター、バススレーブ			Y	Y	Y	Y
	MPU	セキュリティ				Y	Y	Y[3]
	FAW	プログラム/消去保護			Y	Y	Y	Y
	SCE	暗号化モジュール			SCE7	SCE7	SCE5	
	SCE	鍵実装および鍵ラップ			Y	Y	Y	

[1] 4096 bits Verify, Encrypt only
[2] Via Scalar Multiplication
[3] Not available on the S124
[4] SSP v1.5.0 required for low-level drivers
[5] SSP v1.6.0 required for low-level drivers

図 3: Synergy プラットフォームで利用可能な Renesas Synergy MCU(出典: ルネサスエレクトロニクス)

デジタルデータのセキュリティも、多様なセキュリティの脅威を防ぐ上で最優先事項の一つとなります。保存〔休眠〕データ(data at rest)とは、デバイス間やネットワーク間を移動中(in motion)ではないデータを指し、こうしたデータは通常、SRAM や不揮発性ストレージに保存されています。Synergy MCU は、読み取り保護、書き込み保護、読み取り/書き込み保護、ライトワンス保護といったデータアクセス制御によって、こうした保存データをセキュア化します。保存データへのアクセスを制御することで、攻撃面〔攻撃の入口〕(attack surface)が減り、システムのセキュリティが高まります。

さらに、市場に出荷された Synergy MCU は、遠隔操作で更新できるため、常に最新のサイバー脅威に対応可能です。

課題 5——セキュリティの専門家ではないが、安全な製品をつくりたい。知っておくべきことは？

組み込みデバイスをベースにした製品に包括的かつ徹底的なセキュリティ対策を施すには、多様なプロトコルやセーフガードを備え、それらが連携してさまざまなレベルでセキュリティを提供する、高度に統合化・最適化されたプラットフォームが必要です。

Renesas Synergy プラットフォームは、ハードウェアとソフトウェアの独自の組み込みセキュリティ機能一式を備えた完結した開発環境を提供するため、開発者はスタートから優位に立てます。これらのセキュリティ機能は、組み込みデバイスや IoT ネットワークのセキュリティ保護の要件を満たす、共通の「ルートオブトラスト」を構築します。さらに、このプラットフォームは、セキュアかつスケーラブルな製造フローや知的財産保護を確保する能力も備えています。

専用ウェブサイトにはアプリケーション・プロジェクトのライブラリもあり、開発者は、エンド・ツー・エンドのセキュリティソリューションの構築に向けたステップ・バイ・ステップのインストラクションやガイダンスを利用できます。

加えて、Renesas コミュニティやアライアンスパートナーの大規模かつ堅固なエコシステムのサポートを利用できるのも大きな魅力です。トレーニングを受け認定された設計サービスパートナーのネットワークが、設計サイクルのすべての段階をサポートし、あなたの設計やビジネスゴールの実現を後押しします。Renesas パートナーを活用すれば、開発のスピードアップが図れる上、セキュリティソリューションの開発に高度な知見をもたらすことができます。

課題 6——セキュリティ対策についてはベンダーのソリューションやサポートを活用し、自身のリソースを最終製品の差別化に集中させるにはどうしたらよいか？

開発に着手する前に、設計のベースには、さまざまなレベルで万全なセキュリティを提供する一連の機能群が高度に統合化されたプラットフォームを備えた MCU ソリューションを選択してください。組み込みデバイスにおける設計やセキュリティプロトコルのバラツキがハッカーの侵入を許す弱点となれば、悪意あるエージェントが、こうした設計の脆弱性を利用する恐れがあります。これは特に、MCU のハードウェア、ソフトウェア、通信スタック、ドライバが完全に統合されたフレームワークに標準化されていない場合に、重大なセキュリティリスクとなります。

高度なセキュリティ保護を備えた、包括的で完全に統合化された開発プラットフォームは、設計のセキュア化を可能な限りシンプルかつ容易に行えるものにします。プラットフォームにすでに組み込まれた主要ソフトウェア、一連の機能群、スタック、ドライバと統合化済みのフレームワークを選べば、低層階の開発の繰り返しから解放され、その分、製品の差別化に寄与する機能や能力の開発に集中できます。

さらに、活動的で包括的なパートナーのエコシステムを擁するソリューションプロバイダを選ぶことも重要です。特定のセキュリティ機能または機能群の開発を信頼できるエキスパートに外部委託するという選択は、時間の節約になる上、最終製品の性能強化にもつながります。

Renesas Synergy プラットフォームは、量産グレードのソフトウェア、ピン互換のスケーブルな MCU ファミリ、アプリケーションフレームワーク、機能的なライブラリ、HAL（Hardware Abstraction Layer）ドライバ、高度なソフトウェアツールや開発用キットを含む、包括的かつ品質保証された開発プラットフォームです。Synergy プラットフォームは、ア

プリケーションがセキュアで堅牢な技術基盤の上に構築されることを保証します。高度かつ多層的なセキュリティ対策が施されており、各デバイスは一意的に識別され、認証されることで、他のデバイス、サービス、ユーザ間でのセキュアな通信を確保します。

ルネサスを選べば、強固なセキュリティがプラットフォームに組み込まれているため、設計者は貴重な時間とスキルをセキュリティに関わる開発に費やす必要がなく、その分、急速に変化する IoT マーケット機会や消費者需要に対応するためのより高レベルの課題やイノベーションに集中できます。ルネサスによってあらゆる機能があらかじめ組み込まれ、検証され、品質保証されているため、アプリケーションソフトウェアの開発は API レベルからすぐに開始でき、開発期間と労力の大幅な短縮につながります。

加えて、開発者はRenesasパートナーの専門的知見も活用できます。高度なスキルや経験を有するパートナーが、あなたのチームをサポートし、特定のセキュリティ機能または機能群の開発をバックアップします。

結論

ルネサスは、ハードウェアとソフトウェアのセキュリティ保護における最新のブレークスルーを活用し、多層的なセキュリティ機構を施すことで、徹底的かつ包括的な保護を実現するプラットフォームベースのセキュリティアプローチを提供し、組み込みシステムエンジニアが設計のセキュリティ課題に対処するのを全面的にサポートします。Renesas Synergy プラットフォームは、共通の「ルートオブトラスト」を構築し、IoT デバイスやサービス、ネットワークを深いレベルでセキュア化し、製品ライフサイクル全般にわたってセキュアかつスケーラブルな製造フローと知的財産保護を約束します。