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

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。ルネサスは、組込みIoT機器の開発において、下記6つのセキュリティ課題を克服する必要があると考え、それぞれの課題に対して組込みIoT製品のセキュリティを確保するための方法をご提供いたします。ルネサスは、ハードウェアとソフトウェア双方に最新の技術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実現するプラットフォームを提供しています。既に使われている開発プラットフォームの維持や新規構築を柔軟に選択し、実績あるRenesas MCU、周辺機能を引き続き活用しながら、Arm Cortex-Mコアの広範なエコシステムを利用いただけます。

IOTの
セキュリティ課題

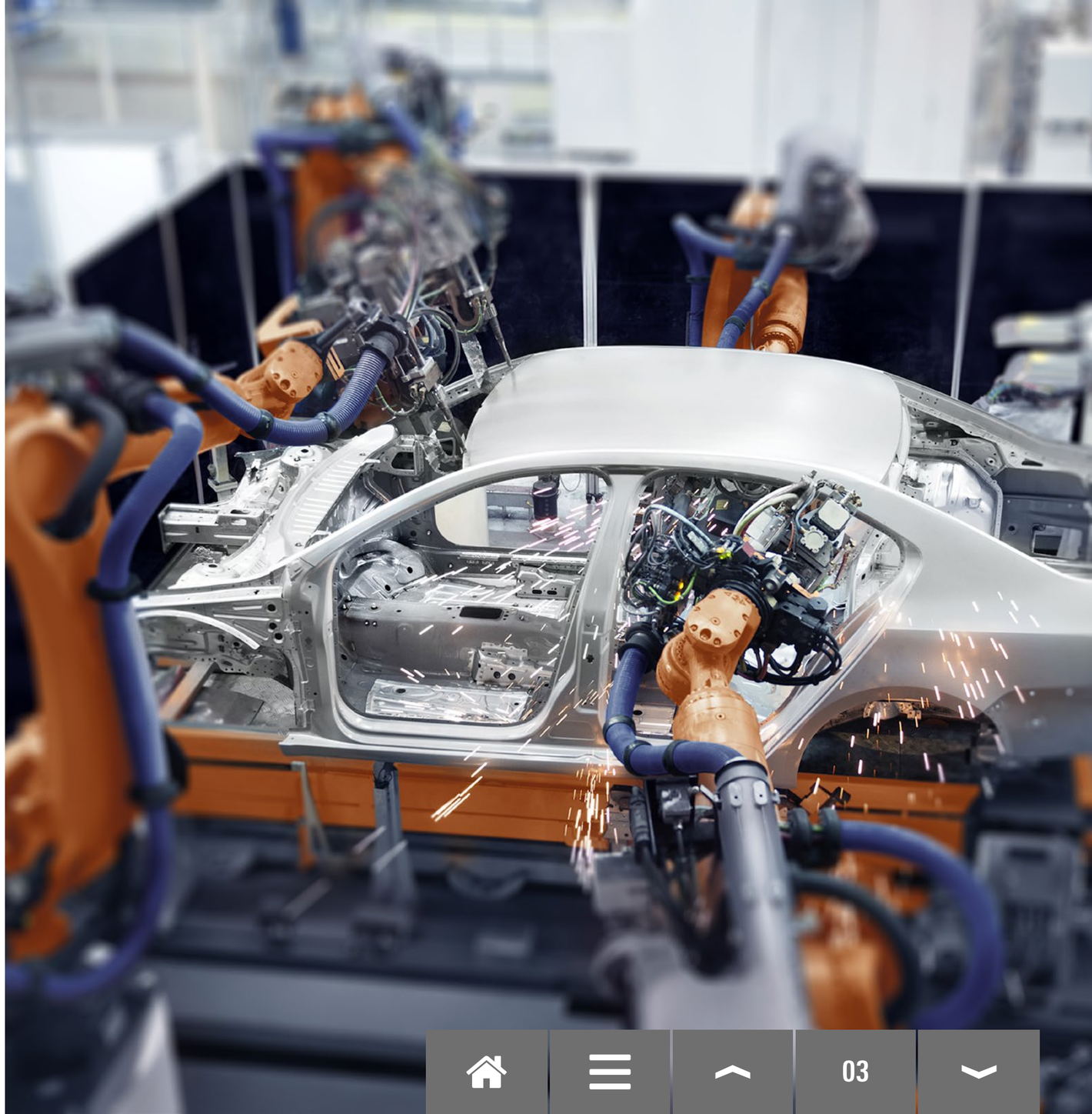
2020年までに世界全体で、およそ310億台の機器がIoT（Internet of Things）化される見通しですが、その多くはセキュリティ管理が不充分で、ハッキングに対して無防備な状態にあります。これほど多くの組み込みシステムが脆弱性を抱えたまま設計されているのはなぜなのでしょうか。最大の理由は、エンジニアが組み込みアプリケーションやデバイスに、セキュリティ対策を施す際に直面する膨大な課題や複雑な手続きが、開発の大きな課題となっていることです。エンジニアは日々巧妙化する脅威環境に通じていなければならない上、絶えず進化するセキュリティ基準も満たさなければなりません。同時に、複雑なアプリケーシ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。

> 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。

本eBook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eBook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. 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

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ごされるか、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。

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。セキュリティ対策は、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。

- 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サポート**。
- アプリケーションソフトウェアを構築可能な次を含む一体型ソフトウェアプラットフォーム：**互換性のある統合スタック、各種ライブラリ、HALドライバ、必要に応じてリアルタイムOS（RTOS）**。

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多層的なアプローチにより、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Synergy Software Package (SSP)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。

さらに、新登場のRenesas RAファミリは、より柔軟なプラットフォームで、Arm Cortex-Mコアとルネサスの持つ業界最高水準の周辺機能IPを組合せてご利用いただけます。RAファミリが提供するFlexible Software Package (FSP)には、FreeRTOS上に構築された基本ソフトウェアモジュール、各種ミドルウェア、最適化HALドライバなどが含まれています。FSPは文字通り柔軟性をコンセプトに設計されており、ミドルウェアやライブラリを自由に選択でき、システムに簡単に組み込むことが可能です。

SynergyプラットフォームとRA MCUには、Secure Crypto Engine（SCE）という統合暗号化モジュールが内蔵されています。SCEモジュールは、市場で広く使用されている暗号化アルゴリズム（RSA/ECC/DSA/AES/SHA）、キー生成機能、True Random Number Generator（TRNG）機能などをハードウェアで高速処理します。キーバインディング処理は、MCU固有のキーラッピング機能によって実行されます。これにより、各MCU専用のキーが暗号化されるため、ラッピングを実行した個々のMCUのSCEモジュール内でのみキーにアクセスできます。SCEは外部から隔離された専用RAMを内蔵しており、プレーンテキスト・キーはCPUがアクセス可能なバスに公開されることはありません。MCUは厳格なアクセス制御プロトコルによってのみアクセス可能ですが、もしこれに違反してアクセスした場合、アクセス保護回路によってSCEをロックします。MCUには、セキュリティメモリ保護ユニット（SMPU）とフラッシュアクセスウィンドウ（FAW）も組み込まれています。これらは、セキュアな不変ブートコード、証明書、およびその他の機密データを保存するために使用されます。SCEをMCU固有のキーラッピング機能と組み合わせて使用することで、非セキュアメモリでもセキュアストレージとして使用可能です。

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 SSP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。 RA FSPは、Armエコシステムソフトウェアを活用することで、同様の機能を提供可能です。

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。ルネサスMCUの柔軟なブートマネージャ（Boot Manager）は、遠隔地にある製造施設で、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。

> 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。

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。

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複数層にわたるハードウェアとソフトウェアを選ぶことです。

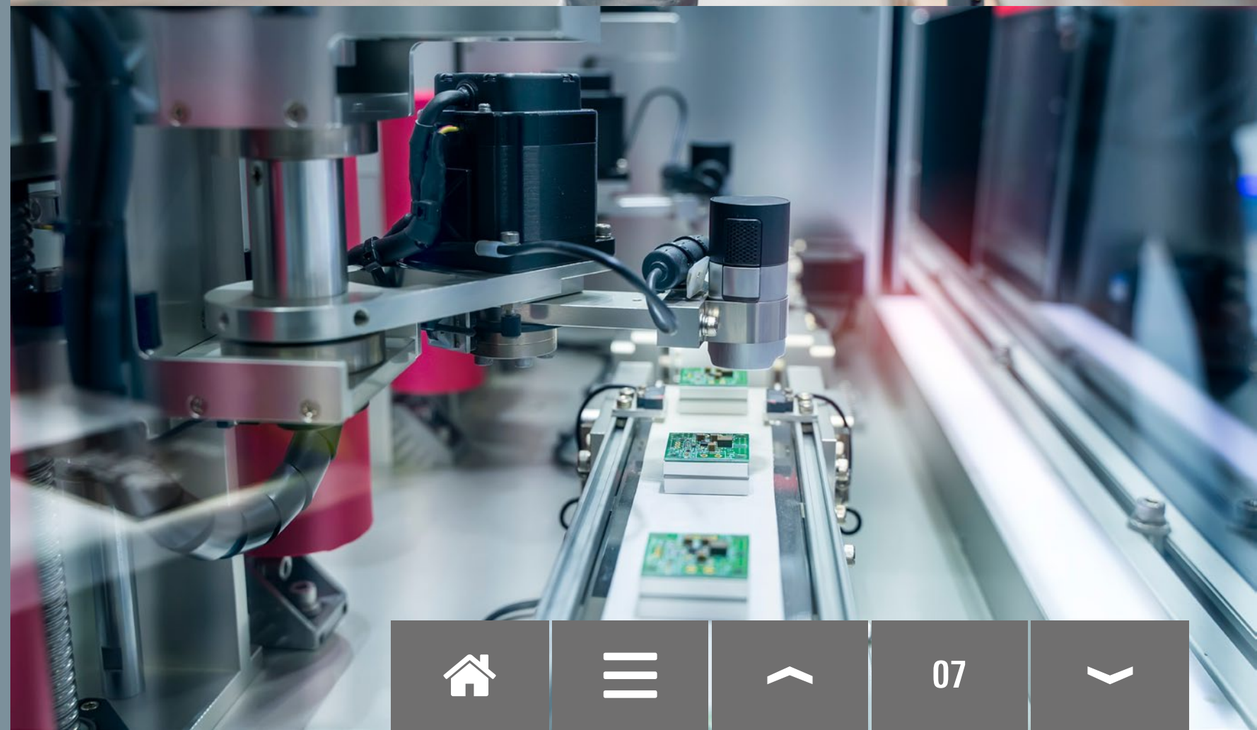
Synergyプラットフォームを用いれば、セキュアなアプリケーションを作成するのに最新の関連プロトコルやセキュリティ対策をすべて学ぶ必要はありません。Synergy Software Packageは、セキュアなコネクテッド組み込みシステムの開発に伴う複雑な機能や手続きを簡素化します。このソフトウェアでは、フラッシュとSRAMのメモリ領域がセキュア化されるため、読み取り／書き込み保護されたコードを作成・保存することができます。これにより、一時鍵（temporal key）や秘密鍵、その他の機密データを保存するのに使用できるカスタマイズ可能なメモリ領域を作成できます。

SynergyプラットフォームとRA FSP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。

> セキュリティを簡素化できるため、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複数層にわたるハードウェアとソフトウェアを選びます。

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。

新登場のRAファミリMCUは、既存インフラストラクチャの再利用や拡張に柔軟に対応可能なため、アプリケーションに必要な機能を的確・効率的に拡張できます。SCEの高度なセキュリティ機能を活用し、さまざまな製品に対応した独自のプラットフォームを構築可能です。RAファミリを使用されるお客様は、世界中のArm開発者の豊富な知識と経験が反映されたArmエコシステムソフトウェアとソリューションを簡単に組み込むことも可能です。



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。SynergyとRA MCUの強力なデバイス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。

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 とRA 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 とRA 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、必要があります。

> 組み込みIoT設計のセキュリティ対策は、課題が多く時間を要する作業です。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ます。

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。

新しいRA MCUをベースに設計される場合、ルネサスのセキュリティIPや組込み周辺IPの専門性と同時に、イノベーション・サポート・セレクションを促進するArmの広範なエコシステムの恩恵も受けることができます。

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？

システム開発を開始する前に、MCUソリューションを選択してください。セキュリティ開発を十分にサポートできる高度な統合プラットフォームを提供するものか、或いは、いろいろなサードパーティのソリューションやリソース、その他のビルディングブロックを提供できるエコシステムを持ったものか、というところがポイントです。

プラットフォームベースのアプローチは、複数層にまたがったセキュリティ機能が提供され、それらが連携して機能します。この連携が重要です。さもないと、開発したシステムのバリエーションに依存した色々なセキュリティプロトコルの弱点を突いてハッカーが侵入し、悪意のあるエージェントソフトウェアにその脆弱性を利用される可能性があるためです。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として標準化されていない場合、これは大きなリスクとなります。

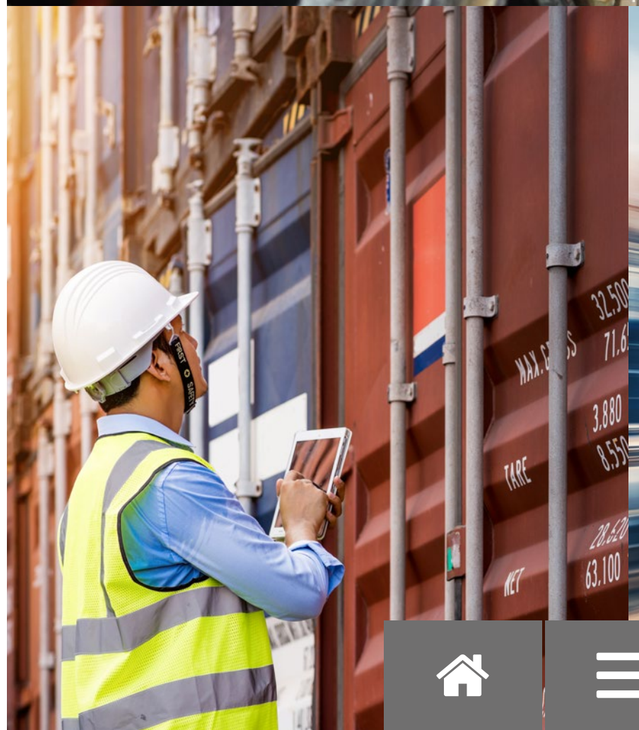
高度なセキュリティ保護を備えた、包括的で完全に統合化された開発プラットフォームは、設計のセキュア化を可能な限りシンプルかつ容易に行えるものにします。プラットフォームにすでに組み込まれた主要ソフトウェア、一連の機能群、スタック、ドライバと統合化済みのフレームワークを選べば、低層階の開発の繰り返しから解放され、その分、製品の差別化に寄与する機能や能力の開発に集中できます。

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。

Synergyプラットフォームを活用することで、開発リソースを消費者ニーズにマッチする独自機能の開発に集中させ、急速に変化するIoT市場動向に遅れることなく製品投入が可能になります。

RAファミリのMCUは、Arm Cortex-Mコアと業界最高水準のセキュリティIPと周辺機能を内蔵し、総合的なセキュリティ保護を可能とする高度な機能を提供します。さらに、いろいろなサードパートナーや数多くのリソースからなるArmエコシステムを活用することで、市場で現在求められている複数層にまたがるセキュリティ機能を備えた革新的なシステムを開発するためのノウハウや技術サポートが入手可能です。

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。特定のセキュリティ規格やユニークな機能を開発するために信頼できるサードパーティに外部委託できる場合には、開発期間を短縮し、自社独自機能にリソースを集中し最終製品を更に強化できます。



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色々なソリューションを提供し、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 MCU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。

CONTACT US

Web: renesas.com/support/contact