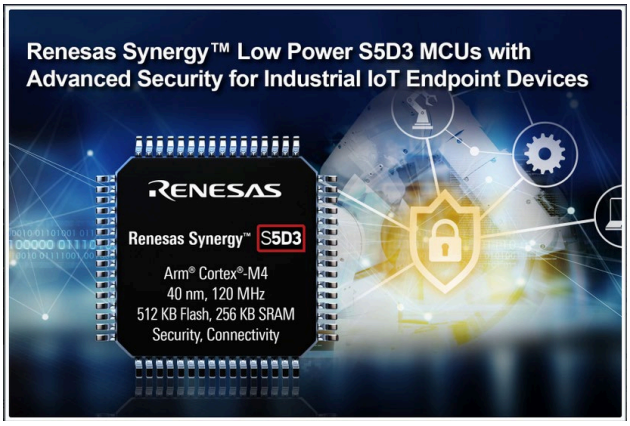
ホワイトペーパー

無数の IoT デバイスを安全かつスケーラブルに管理するには

2019 年 2 月

概要



Internet of Things（IoT）のアプリケーションにおいて、包括的できめ細かなセキュリティを確保するには、さまざまな困難を伴います。 Renesas Synergy プラットフォームは、この困難を解決するための特徴的なハードウェアとソフトウェアを備えています。例えば、遠隔地にある生産設備での安全な製造手段を確保したり、大事なファームウェアに含まれる知的財産を保護したりといった、IoT デバイスやネットワークを保護したいという要求に対応することができます。S5D3 MCU は、Renesas Synergy MCU の最新製品として開発され、Renesas Synergy プラットフォームのポートフォリオを拡充するとともに、このクラスのデバイスでは既存のソリューションをはるかに凌駕するセキュリティ機能を提供しています。 汎用品である S5D3 MCU は、魅力的な価格で高度な機能を提供し、IoT システム内のエンドポイントデバイスにおいて、高度でスケーラブルなセキュリティ管理を可能にします。

IoT におけるセキュリティ課題

ほんの数年前まで、エレクトロニクス製品は現在のようにインターネットに接続されていませんでした。よって、アプリケーション開発者は開発した製品のセキュリティについて、あまり心配する必要はありませんでした。しかし最近は、電球や玩具、家電製品などの簡単な電化製品でさえも、IoT デバイスとしてインターネットやクラウドに接続されています。セキュリティに対する要求は、パスワードとファイアウォールで事足りていた時代から比べると、大きく変わりました。 サイバー攻撃からデータと機能を守るために、IoT デバイスにセキュリティ機能をもたせることは、開発者にとって後回しにできない最も重要な検討事項のひとつになりました。これを実現するためには、ハードウェア・ソフトウェアの両面からアプローチする必要があります。

セキュリティに対する脅威がより強力で悪意のあるものになるにつれ、セキュリティ規格も絶えず進化し、また複雑なアプリケーションになれば複数の規格に対応していく必要があります。そのため、デバイスの互換性や柔軟性が阻害される可能性があります。製品開発の多くのケースにおいて、高いセキュリティ機能を求める結果、高いコストや消費電力の増加を引き起こし、最終製品の市場競争力に影響を与えてしまう事例が起き始めています。

そのため、IoT 製品では次のような特有の課題に対処する必要があります。

- 製造時の IP 盗難、製品のクローン化、過剰生産などの脅威からの知的財産の保護
- 重要インフラのシャットダウンや損傷、けがや事故を引き起こす可能性のある不正行為に対する防御
- 重要情報のプライバシーと機密性を保証するため、転送中／休止中のデータ保護
- 安全なブート管理と ROT（Root-of-Trust：信頼の基点）など、堅牢なシステム基盤の構築
- エンドポイントから有線または無線ネットワーク、そしてクラウドへの通信と接続の保護

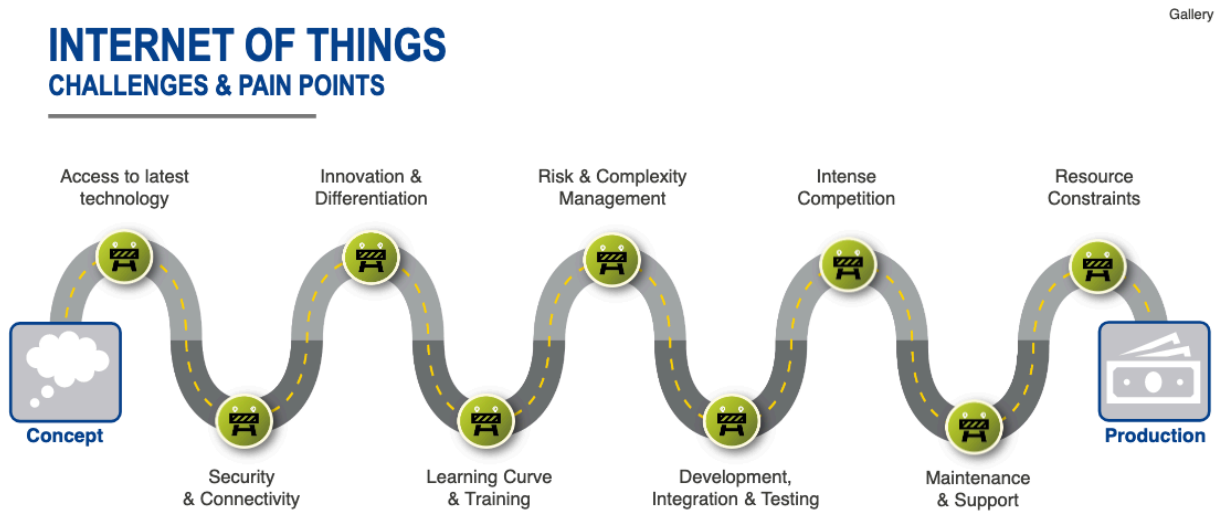


図 1. IoT 製品開発は企画から製造まで長い道のりをたどるため、市場への投入遅延やコスト増などに影響する

これらのセキュリティ課題を解決するためには、最新技術を適用したハードウェアとソフトウェアを備えるプラットフォームベースの開発手法が有効です。この手法により、さまざまな脅威に対する包括的なセキュリティ機能を実装することができます。

ハードウェア面では、このプラットフォームには以下のような機能が必要です。

- デバッグインタフェースを攻撃経路として利用されないような、保護されたデバッグ アクセス機能
- 共通鍵暗号および公開鍵暗号の双方の処理を高速化でき、 さらに高速にハッシュ関数処理が可能なセキュリティ暗号エンジン
- セキュリティ鍵を生成し、その鍵が暗号化されていない状態で露出されないよう、セキュアに隔離できる機構を持つこと。そして、各デバイスが固有の鍵を生成／保持することにより、固有のデバイス ID を持てること。これはデバイスの安全な供給と大規模展開に不可欠です。
- フラッシュメモリおよび RAM 上の任意の領域を、不正または意図しない読み取り、または書き込みのアクセスから保護する安全なメモリアクセス機構。 機密性の高いコードやデータは、通常のコードやデータと区別し、安全な領域に隔離でき、また OTP Flash（One-time-Program Flash）領域を構成し、一度書き込まれたデータの変更を防ぐ仕組みが必要です。

ソフトウェア面では、このプラットフォームには以下のような機能が必要です。

- 実績のあるアプリケーション フレームワークと標準 API を備え、統合・最適化された商用グレードのソフトウェア

- ハードウェアがサポートするセキュリティ機能や暗号機能を使いこなすための HAL ドライバ API
- マイクロコントローラとそれに接続された外部機器や、ネットワークとの間での認証やセキュア通信、重要な機密データやプログラムを、暗号化して格納するためのハイレベルで抽象的な API を備えた、暗号アルゴリズムのソフトウェアライブラリ
- TLS、MQTT、HTTPS などの主要な通信プロトコルやトランスポート、そして様々なクラウドとの接続に必要な固有のプロトコルへの対応。これにより、開発者は低層ミドルウェアとネットワーク スタックのインテグレーションに時間を費やす必要がなくなり、これらのプロトコルのライセンスやコストに対処する必要もなくなります。

以上のようなハードウェアとソフトウェアの要件を備えるマイクロコントローラ・プラットフォームは、IoT デバイスの開発者にとって、次のようなメリットがあります。

- 開発チームが API レベルでアプリケーション・ソフトウェアの開発を開始でき、開発期間の短縮が可能
- 主要なセキュリティ機能やコネクティビティ機能、その他周辺機能をインテグレートしたソフトウェアを使用することにより、従来ソフトウェアのインテグレーションに要していた時間やソフトウェアに支払っていたロイヤリティ／ライセンス費用を削減可能（TCO : Total Cost of Ownership の大幅な削減）
- セキュリティへの対応をはじめとして、日々変化する市場要求への煩雑な対応を軽減し、導入／参入障壁を下げられる

ハードウェアとソフトウェアを高度に統合したマイクロコントローラ・プラットフォームは、組込み機器の生産時における安全なプログラミングも可能にします。サプライチェーンのグローバル化や複雑化が進む昨今は、どのような製造環境下や生産サイクルにおいても、製品の完全性や信ぴょう性を維持するために、しっかりとしたセキュリティ管理と、不断の努力が必要になります。

Renesas Synergy のセキュリティ機能

Renesas Synergy プラットフォームは、各種ソフトウェア、スケーラブルな MCU ファミリ、および開発ツールを含む、完全かつ品質テストをおこなったシステムソリューションです。 この包括的で実証済みのプラットフォームを使うことで、開発チームは API レベルですぐにアプリケーション開発を開始できるため、何ヶ月もの時間と労力を節約できます。 MCU を搭載する製品開発向けに最適化されており、開発者は独自に製品革新を進めることに時間を費やすことができます。

Renesas Synergy プラットフォームは、これから示すような様々な機能を統合した、幅広いセキュリティ機能に対応しています。

セキュアデバイス ID：強力なデバイス ID を確立することで、それぞれの IoT デバイスを一意に識別および認証し、接続された他のデバイスやサービス、ユーザーとの間で、安全で暗号化された通信を保証します。このデバイス ID は、さまざまな IoT セキュリティ要件に対応します。

- **信頼の確立**：デバイスをネットワークに接続する際、他のデバイスやサービス、ユーザーとの認証と信頼の確立が必要になります。 信頼が確立されると、デバイスやユーザー、サービスは安全に通信し、暗号化されたデータや情報を交換することができます。
- **プライバシー**：IoT デバイスの増加に伴い、より多くのデータが生成、収集、共有されます。これらのデータには、個人情報や機密情報、財務情報などが含まれることがあり、通常これらは安全に保管されなければならず、時には法令順守を求められます。デバイス ID によって接続デバイス相互の認証と識別が行われます。

- **完全性**：IoT システム内のデバイスやシステム間で送受信されるデータには完全性が求められます。 デバイスの完全性は、「そのデバイスが確かに間違いなくそのデバイスである」ことを証明することから始まります。 固有のデバイス ID により、そのデバイスが確かに正当なものとして保証されることで、偽造品を減らし企業のブランドを守ることができます。データの完全性は見過ご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において、送られた情報の真贋や、品質の信頼性は極めて重要です。

Renesas Synergy プラットフォームでは、MCU に搭載しているセキュリティ暗号エンジン（SCE）を使用して一意のデバイス ID を生成する機能など、多彩な鍵生成機能を提供しています。また、生成したデバイス ID はセキュリティ・メモリ・プロテクション・ユニット（Security MPU）とフラッシュ・アクセス・ウィンドウ（FAW）を使用して、MCU 内部のフラッシュメモリに安全に保存できます。

デバイス ID を作成する最初の手順は鍵の生成です。 鍵は Renesas Synergy MCU の内部で生成することも、外部の安全な施設で生成して Renesas Synergy デバイスに注入することもできます。デバイス鍵が生成または注入されると、認証局（CA：Certification Authority）と呼ばれる機関がデジタル証明書を発行します。CA は、パブリック（クラウドのどこか）またはプライベート（私設設備内にあり通常はセキュア・サーバーで運用）のいずれかです。デバイス ID が作成され、Renesas Synergy デバイス上への書込みが行われたのちは、盗難や破壊から安全に管理される必要があります。これは、コードフラッシュ（フラッシュメモリのコード領域）および SRAM 内に、Security MPU および FAW 機能を使用して、4 つのセキュア領域を設定することによって実現されます。これらのセキュア領域へのアクセスは、「セキュアコード」からしか行うことができません。FAW 機能は、コードフラッシュのアドレス範囲をレジスタで設定して使用され、この範囲設定は消去および再設定が可能です。ここで FAW の範囲外に設定されたアドレス空間は、一度プログラムすると変更できない One-Time-Program Flash として使用できます。この機能により、デバイスの識別情報（鍵と証明書）が消去または再プログラムされることを防ぐことができます。

セキュアコード領域には、セキュアデータ領域で作業することだけが許可されている API も含まれています。この領域には、セキュアコード以外のコードからのアクセスや内容の変更はできません。Security MPU の設定は、リセットベクタがフェッチされる前に読み取られて適用されるため、プログラムコードが実行される前に設定されます。またこの Security MPU の設定は、出荷前に FAW 機能（ワンタイムプログラマブル FPSR ビットを使用）を使用してロック可能なので、以降に変更されることはありません。

Renesas Synergy MCU が提供するメモリ保護機能は、デバイス識別アプリケーションに不可欠な各種の機密データの中でも、セキュア ブートコードやデバイス証明書、鍵などを格納するために使用できます。

休止中データの保護

IoT やクラウド産業の急速な進展に伴い、デジタルデータセキュリティは企業秘密と個人のプライバシーを保護する際の最優先事項となっています。休止中データとは、デバイス間やネットワーク間で積極的に移動していないデータのことを意味します。組込みシステムでは、保護されるべきデータは揮発性データストレージ（MCU の内蔵 SRAM または外部 SDRAM）または不揮発性データストレージ（MCU の内蔵フラッシュメモリ、外部 QSPI メモリ、外部 EEPROM など）に格納されています。

Renesas Synergy MCU は、休止中データを脅威から守るために、データアクセス制御、認証スキーム、CPU やバスマスタからの読み取り／書き込み保護機能、ライトワンスアクセス保護機能などを提供します。さらに、Renesas Synergy MCU は、セキュアではないソフトウェアアクセスからセキュリティに関する周辺機能の制御を無効にする機能も提供しています。

データアクセス制御：デバイスへのコネクティビティ要求が高まり、組込みシステムの複雑さが増すにつれ、潜在的な攻撃対象も増えていきます。セキュアデータへのアクセスを制御することにより、攻撃対象を効果的に減らしシステムのセキュリティを高めることができます。

Renesas Synergy プラットフォームは、以下のデータアクセス制御を提供しています。

- **リードプロテクション**：フラッシュメモリや SRAM に存在する機密データまたは機密コードには、読み取り権限が付与されたソフトウェアのみが、それらにアクセスできるように、リードプロテクションを設定できます。 Security MPU には、リードプロテクション領域を設定する機能があります。

- **ライトプロテクション**：悪意を持って変更または消去されることから機密データを保護することも重要です。Renesas Synergy MCU のメモリオプション設定を使用して、揮発性および不揮発性データを書き込み禁止にして不正な変更を防ぐことができます。

- **リード／ライトプロテクション**：この機能により、マルウェアや IP 盗難といった攻撃に対応することができます。内部フラッシュデータの場合、Renesas Synergy MCU が提供するリード／ライトプロテクション機能は次の 2 つです。

    - Security MPU によって設定されたフラッシュメモリや SRAM 上のセキュア領域は、非セキュアコードからのリード／ライトアクセスを無効にすることができます。

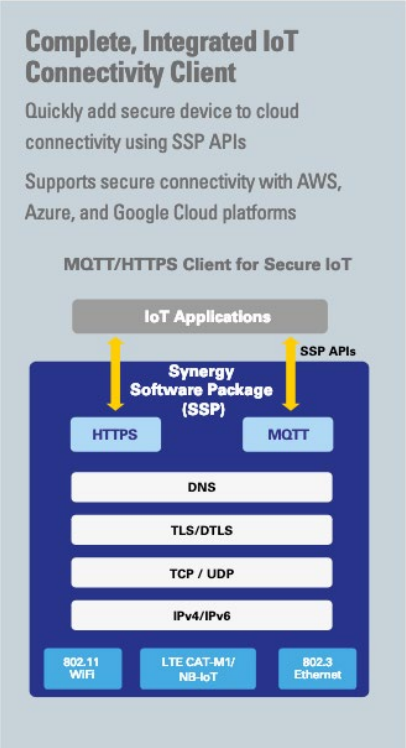
    - Security MPU と FAW を共に使用することで、設定したフラッシュメモリ領域内の機密データをセキュアコード、非セキュアコード双方からのリード／ライトアクセスから保護することができます。

- **ライト・ワンスプロテクション**：一部の利用ケースにおいては、機密性の高い休止中データは、デバイスの寿命が尽きるまで、アクセスや改ざんから保護される必要があります。たとえば、セキュア ブートローダは製品が寿命を迎えるまで不変でなければなりません。 データが内蔵フラッシュに常駐する使用方法では、FAW 機能を用いて、初回の書込み以降に改竄されないように保護することができます。

- **ライト・ワンス＆リードプロテクション**：ライト・ワンスプロテクションされたデータは、さらにリードプロテクションすることもできます。セキュアコードだけがアクセスできるように、ライト・ワンスプロテクションされたフラッシュデータにリードプロテクションを設定することができます。

クラウドへのセキュアな接続

IoT は、モノや人との間に複数の新しい通信形態をインテリジェントにリンクする、幅広く様々なテクノロジで構成されています。デバイスはネットワークに接続して、センサーを用いて収集した環境情報を提供し、他のシステムからのアクセスを許可し、世の中の色々な場所でアクチュエーターを動かす、などをしています。その過程では、IoT デバイスは膨大な量のデータを生成し、クラウドコンピューティングは希望する目的地にデータを転送できるよう、経路を提供します。



Renesas Synergy プラットフォームは、Amazon Web Service（AWS）、Google Cloud、Microsoft Azure などの主要なクラウド環境へのセキュアな組み込み接続機能に対応しています。SSP（Renesas Synergy™ Software Package）に備えた MQTT および TLS を使用してクラウド接続を行います。

MQTT プロトコル：MQTT（Message Queuing Telemetry Transport）は、非常に軽量・オープンで使いやすいクライアント・サーバーのパブリッシュ・サブスクライブ型のメッセージング転送プロトコルです。MQTT は、低帯域幅、高レイテンシ、不安定なネットワーク環境や、メモリや処理能力に制限のあるデバイスに用いることに適した設計がされています。こうした特性により、MQTT は、マシン間通信（M2M）や IoT に類する通信、コードサイズに制限がある場合や、ネットワーク帯域幅が貴重な場合など制約の多い環境下での使用に最適です。

TLS プロトコル：TLS（Transport Layer Security）プロトコルとその前身である SSL（Secure Sockets Layer）は、コンピュータネットワーク上での通信セキュリティを提供する暗号化プロトコルです。TLS/SSL プロトコルは、2 つの通信アプリケーションの間でのプライバシーと信頼性を提供します。そして、次のような基本的な機能を有しています。

- **暗号化**：通信アプリケーション間で交換されるメッセージは、接続がプライベートであることを保証するために暗号化されています。AES などの共通鍵暗号がデータの暗号化に使用されます。
- **認証**：デジタル証明書を使用して通信相手の身元を確認するためのメカニズムです。
- **完全性**：メッセージの改ざんや偽造を検出するメカニズムにより、接続の信頼性を保証します。SHA（Secure Hash Algorithm）などの MAC（Message Authentication Code）により、メッセージの完全性を保証します。

セキュア ブートマネージャ

Renesas Synergy の セキュア ブートマネージャは、安全でスケーラブルな製造を可能にする機能を提供します。ファームウェアの改変、海賊版やクローン製品といった脅威から守ると同時に、開発者は遠隔地にある生産施設や実際のフィールドにおいて、Renesas Synergy MCU のフラッシュメモリに信頼性の高いファームウェアを確実かつ安全にプログラムできます。

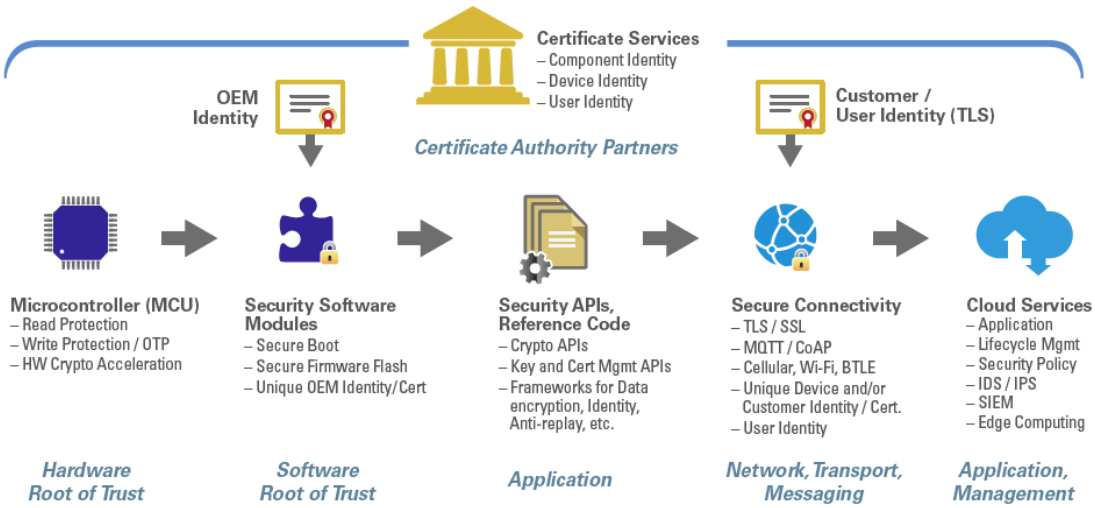


図 2. 製品のライフサイクル全体にわたって ROT（Root-Of-Trust：信頼の基点）保護機能を提供します。

Renesas Synergy MCU とセキュア ブートマネージャの組み合わせにより、固有のデバイス ID、ハードウェアで保護された鍵、セキュア ブートローダ、セキュア フラッシュ・アップデートモジュール、そして各種暗号機能の API を通じて、強力な ROT（Root-Of-Trust: 信頼の基点）を提供します。 セキュア ブートマネージャには以下が含まれます。

- ファームウェアのマスタリング（デジタル署名）用ツール
- ブートローダ、証明書、および鍵をダウンロードする機能
- 許可された MCU にのみアプリケーションファームウェアを書き込む機能

最初の作業ステップは、安全が確保されたセキュア プログラミングセンターで、対象の Renesas Synergy MCU に固有の ROT をインストールすることから始まります。この ROT とは、ルネサスが提供するセキュア ブートマネージャと、ファームウェア・マスタリングツールによって生成された独自の ROT で構成されています。このマスタリングツールは承認されたファームウェアに署名して暗号化し、セキュア ブードローダーはマスタリングツールによって署名されたファームウェアのみをロードします。ROT は、セキュア プログラミングシステムの安全な接続により事前にロードされ、データを安全に保存し使用方法も厳しく管理できます。

ROT は鍵と共にセキュア プログラミングシステムにセットされた個々の MCU に書き込まれ、それにより各 MCU に安全で一意の ID を与えます。次の作業ステップは、マスタリングツールを使用して、事前にデジタル署名および暗号化された認証済みファームウェアをインストールすることです。プログラミングシステムはファームウェアを MCU へ書き込み、最初のステップでインストールされた ROT がファームウェアを検証し、復号してフラッシュ メモリに書き込みます。最後の作業ステップで、FAW 機能によりセキュア ブートローダが変更されないようにロックします。こうして信頼できるファームウェアのみを起動し、不変の ROT として機能します。

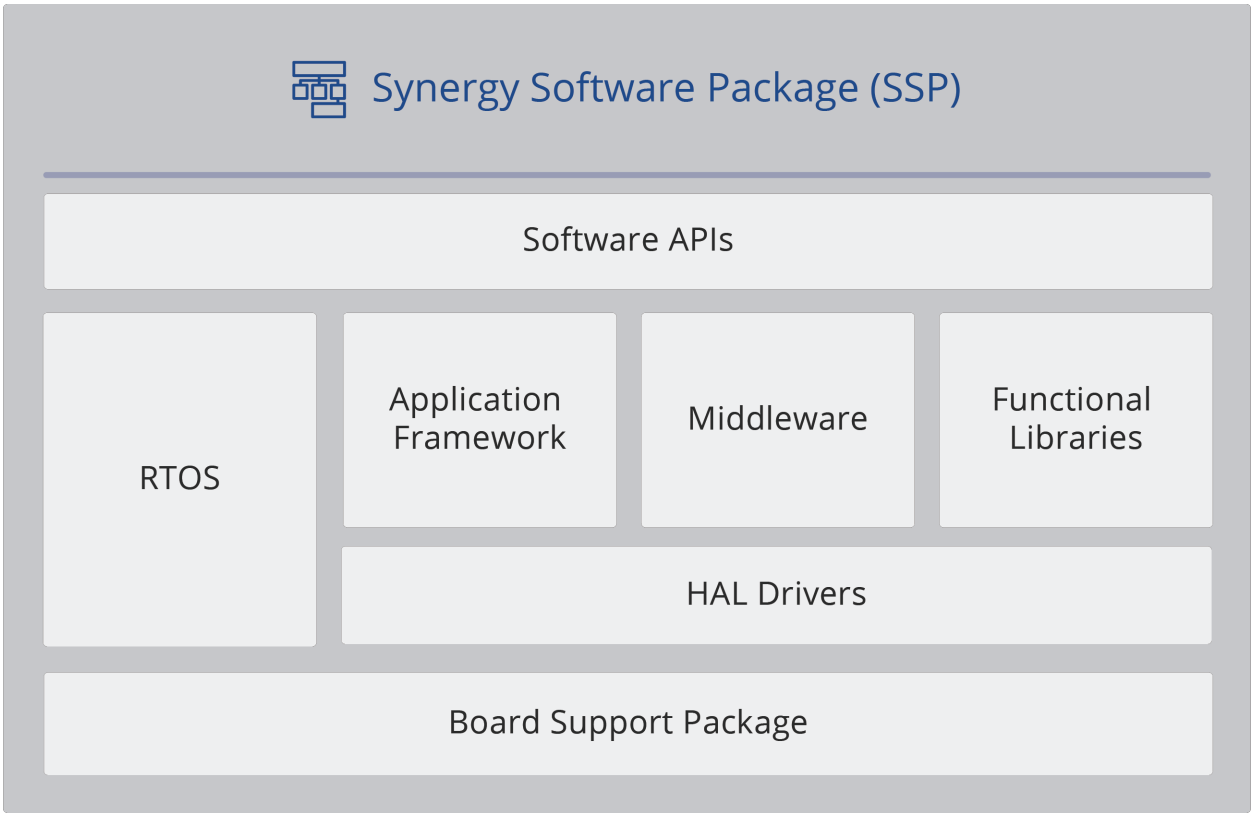
こうしてプログラムされた Renesas Synergy MCU は、OEM または契約製造施設に出荷され、そこで MCU は最終製品に組み込まれる回路基板に取り付けられます。市場に投入された後もこのチップ内の ROT が機能し、ファームウェア更新の際にも、ファームウェアの検証や復号化を行い、正しいファームウェアのみ安全にフラッシュメモリに書き込まれます。

Renesas Synergy ソフトウェアパッケージ

Renesas Synergy ソフトウェア・パッケージ（SSP）は、Renesas Synergy プラットフォームの為に開発、最適化され、更に品質認定を受けたソフトウェアを提供します。SSP には、高機能なリアルタイム・オペレーティングシ

ステム（RTOS）や各種ミドルウェアスタック、ライブラリ、ハードウェアを抽象化する低層 HAL ドライバ、そして実績あるシステムレベルの API を提供するフレームワークなどが含まれます。SSP の階層化アーキテクチャにより、開発者は共通のフレームワーク API を使用、あるいは必要に応じて MCU のデバイスドライバ層を直接制御することで、また時には MCU のレジスタを直接設定することで、アプリケーション開発ができます。

Renesas Synergy プラットフォームでは、2 種類のソフトウェア統合開発環境（ルネサスの自社開発環境である e² studio および IAR Embedded Workbench™ for Renesas Synergy）を追加のライセンス費用やロイヤリティの支払いをすることなく使用することが出来ます。



ルネサスはソフトウェア開発ライフサイクル全体をカバーする国際規格 ISO / IEC / IEEE 12207 に従って SSP を開発しています。SSP のすべての要素は、この規格に従って定義・テストされており、量産品質を確認しています。

ルネサス S5D3 MCU のご紹介

S5D3 MCU は、Renesas Synergy MCU の最新製品として開発され、魅力的な価格でありながら高度な機能を提供し、IoT システム内のエンドポイントデバイスに特に適しています。40nm プロセスをベースに、高性能な Arm ® Cortex®-M4F コアと、内蔵フラッシュメモリと SRAM の比率が 2 対 1 となるメモリ、実績のある各種周辺機能をバランスよく搭載しています。この S5D3 MCU も、Renesas Synergy ソフトウェアパッケージによってサポートされており、従来同様 e² studio と IAR Embedded Workbench for Renesas Synergy の 2 種類の統合開発環境（IDE）を無制限に使用することが可能です。デバイス評価やソフトウェア開発にすぐに着手できるように、ターゲットボードも同時にリリースされています。S5D3 MCU は汎用マイコンとして幅広い用途に利用可能ですが、なかでも産業オートメーションやビルオートメーションなどの分野における IoT アプリケーションにおいて、高度なセキュリティとエンドポイント管理機能を提供できます。

S5 シリーズ MCU は高性能・高集積な MCU で、豊富なコネクティビティ、グラフィックスエンジン、高精度なデータ収集に対応するアナログ インタフェースを複数備えたシリーズであり、S5D3 MCU はその 1 つとして製品化されました。高度な暗号アルゴリズム用のハードウェア アクセラレータにより、強力なセキュリティとセーフティ機能も提供します。メモリや周辺機能のバリエーションも豊富でピン互換性があり、製品開発を加速するための開発キットも準備しています。

S5D3 MCU の登場により、S5 シリーズ MCU に魅力的なコストの製品が新しくラインナップされました。S5D3 MCU は、従来の S5 シリーズの性能や堅牢なセキュリティは必要なものの、グラフィック アクセラレータやイーサネット接続などの機能を必要としないアプリケーション向けに設計された汎用 MCU です。40nm プロセスの採用により、CPU 動作時の消費電力を効率的に低減でき、モニタリング データを継続的に収集する IoT アプリケーションに最適です。S5D3 MCU は、512 KB のコードフラッシュ、8 KB のデータフラッシュ、および 256 KB の SRAM を搭載し、バランスの良いメモリ配分になっています。また魅力的な価格と高効率な動作により、IoT システムのエンドポイントデバイスの高度でスケーラブルなセキュリティ管理に最適です。主な用途としては、産業オートメーション、ビルディングオートメーション、システムおよび機械制御、スマート電力メーターのネットワーク制御や OA ソリューションのシステム制御に適しています。

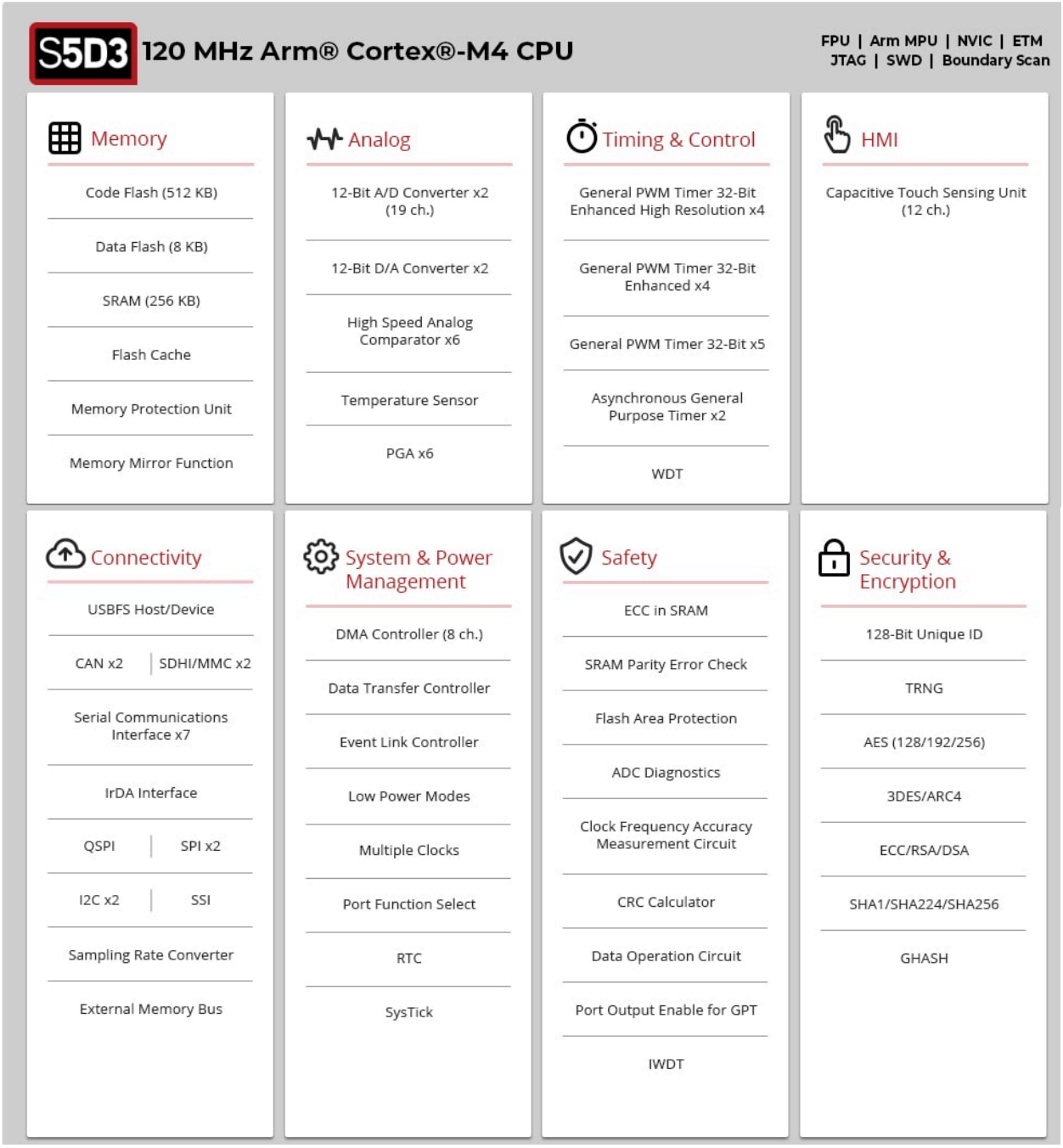


図 3：S5D3 MCU グループのブロック図

S5D3 の特徴

外部セキュリティ専用チップを必要としないワンチップ統合セキュリティ：S5D3 は、MCU に集積されている高度な機能を組み合わせることで、首尾一貫した ROT セキュリティを提供します。S5D3 に搭載された暗号エンジンであるセキュリティ暗号エンジン（SCE7）は、このクラスの MCU を使ったソリューションをはるかに超えるセキュリティ機能を実現しています。SCE7 は MCU 上の独立したサブシステムで、専用の制御ロジックによって管理・保護されています。鍵を各 MCU 固有の ID で暗号化したラッピング鍵は、機密情報の漏洩を防ぎます。

SCE7 には、鍵の生成機能を備えた ECC、RSA、AES、3DES、SHA、TRNG などのハードウェア アクセラレータも組み込まれています。また、MCU 内のフラッシュメモリ上に、書き込み禁止のブートコードとデータ（ルート鍵、コンフィギュレーション）を用意します。 これにより、コードの改ざんや複製、リバース エンジニアリングなどを防ぐことができます。Security MPU は、セキュア メモリ領域を確保し、信頼できるコードと信頼できないコードやデータの分離をハードウェアレベルで可能にします。

大容量の SRAM を搭載しさまざまな通信スタックに対応可能：IoT 環境ではアプリケーションに、堅牢なコネクティビティを備えることが不可欠です。十分な量のペイロードを転送できる通信スタックを動作させ、さらに通信パフォーマンスの向上や BOM コストの削減には、大容量の内蔵 RAM が必須となります。そのため、S5D3 MCU では、組込みマイコンとしては珍しく、内蔵フラッシュメモリと SRAM の比率が 2 対 1（512 KB：256 KB）のメモリ構成を提供しています。

まとめ

Internet of Things（IoT）のアプリケーションにおいて、包括的できめ細かなセキュリティを確保するには、様々な機能が連携し多様なセキュリティを実現できる、高度に統合・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、IoT デバイスとネットワークを保護するという要件を満たすために、ROT を構築し、その上に特徴あるハードウェアとソフトウェアのセキュリティ機能を提供しており、安全でスケーラブルな製造と知的財産の保護に貢献します。S5D3 MCU は IoT システム内のエンドポイントデバイスにおいて高度でスケーラブルなセキュリティ管理を可能にする MCU です。