ホワイトペーパー

Arm® TrustZone® を使用したシステム開発のメリット

2020 年 11 月

概要

バッテリ駆動のワイヤレス温度センサから高出力の産業用モータ制御まで、さまざまな電子機器を開発するメーカーにとって、セキュリティ対策は重要で広範囲にわたる課題です。最終製品の安全性を確保するということは、単に暗号鍵やパスワードへの攻撃をブロックするだけではありません。アプリケーションの動作をつかさどるソフトウェアは重要な知的財産であり、それがコピーされないように保護することや、侵入されたデバイスを経由して他のシステムを制御し悪用されることも防ぐ必要があります。

デジタルセキュリティでは、暗号鍵と暗号アルゴリズムを使用して、さまざまなシステムリソースや機能へのアクセスを保護します。そうしたセキュリティ機能を動作させるには十分な処理性能が必要です。また、システム内のクリティカルな部分は、それ以外のアプリケーション部から分離しておき、他のシステムによるアクセスから保護される必要があります。

このシステム分離の考え方はセキュリティ対策の重要な要素ですが、豊富な機能が高度に統合された昨今のプロセッサシステムで実現することは、大きなチャレンジといえます。

このホワイトペーパーでは、Arm® TrustZone® を使ってシステム全体のセキュリティを実現するアプローチを紹介します。そして、ルネサスの 32 ビットマイクロコントローラである Renesas RA ファミリに、TrustZone がどのように実装されているかについても解説します。Renesas RA ファミリは、Arm® Cortex®-M マイクロコントローラアーキテクチャをベースとし、低電力動作から高性能動作まで、広範囲に最適化された 4 シリーズを展開しています。

システム分離の必要性

今日、ほとんどの組込みシステムが他のデバイスやアプリケーションと繋がっています。有線や無線によって接続された、IoT デバイスなどに代表されるインターネット・コネクテッド・デバイスはいたるところに設置されていますが、その多くはセキュリティ攻撃に対して非常に脆弱です。IoT デバイスの多くは、ローカルゲートウェイを経由して、または直接クラウドにアクセスします。たとえば、製造工場内の環境センシングエッジノードは、ローカルまたはクラウドのリソースに定期的にアクセスし、分析に必要な温度、湿度、他の環境パラメータを送信します。この環境パラメータはプロセス制御アプリケーションによって解析され、プラント内の暖房や換気システムといった別のエッジノードに送信されて、暖房や換気システムが稼働します。この際、アプリケーションコードは通信認証を行い、データの暗号化や復号化を行うために、機密データと暗号鍵にアクセスします。もし、このような方法でデータを処理するアプリケーションと同時に、別のアプリケーションが動作して周辺機能がアクセスできる状態になっているとしたら、同時にこのエッジノードは、侵入攻撃が可能な状態になってしまいます。

暗号鍵にアクセスしてセキュリティプロセスを処理するアプリケーションは、他の無関係なコードから完全に分離されている必要があります。特に、多くの侵入攻撃はデバイスのブートプロセス中を標的にするため、ブート処理を含む最下位の物理層での分離が重要です。

Arm TrustZone テクノロジは、シングルコアデバイスのハードウェア領域を2つの異なる独立した環境に分離するための効率的な組み込みメカニズムを提供します。1 つは通常のコード実行に使用され、もう 1 つは完全に分離されたセキュアな領域を必要とするコード実行に使用されます。図 1 を参照してください。

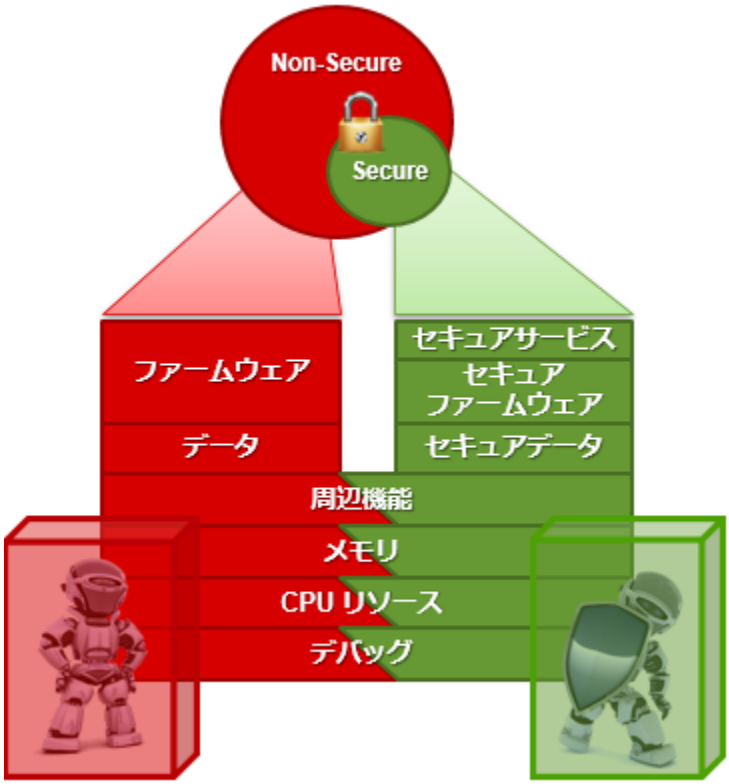


図 1. Arm TrustZone によるマイクロコントローラの一部機能をハードウェア的に分離するコンセプト

Arm TrustZone とは

Arm TrustZone には 10 年以上の歴史があります。当初は Cortex®-A クラスのアプリケーションプロセッサのセキュリティ拡張機能として導入されました。Cortex-A マイクロプロセッサでは、2 つの別個に分離された環境（セキュアワールドまたはトラステッドワールドと、ノン・セキュアワールドまたはノーマルワールド）で、別々のオペレーティングシステムを使用することが出来ます。TrustZone が Cortex-M33 マイクロコントローラコアで利用できるようになったのはごく最近のことです。マイクロコントローラは、マイクロプロセッサと比較してリソースの制約が非常に多く、Cortex-M シリーズへの TrustZone 実装は Cortex-A と微妙に異なっており、パフォーマンスと電力効率のオーバーヘッドが低減されています。すべてのマイクロコントローラベンダーが TrustZone を実装しているわけではないので、ソフトウェアやツールに関連したエコシステムはまだ発展途上です。

Arm TrustZone は、トラステッド実行環境の代表例で、データ、サービス、および特定のメモリ領域を、セキュアワールドとノーマルワールドに分離することができます。セキュアワールドで何を実行するかについては非常に柔軟性があり、秘密鍵やファームウェア、セキュリティ関連ルーチンを置くことが多いですが、ビジネス上機密性が高いライブラリやアルゴリズムといった知的財産も保護することができます。TrustZone は、ノーマルワールドのソフトウェアがセキュアワールドのソフトウェアやリソースへアクセスすることをブロックします。セキュアワールド

内では、その領域内すべてのリソースにアクセス可能です。ノーマルワールドとセキュアワールドの間のアクセスは、ノンセキュア・コーラブル・ベニア（NSCV）によって管理されます。図 2 を参照してください。NSCV は、ノーマルワールドのコードがセキュアワールドのサービスを呼び出すためのアクセスポイントとして機能します。

図 2. ノンセキュア・コーラブル・ベニア（NSCV）が、ノーマルワールドからセキュアワールドのサービスにアクセスできるアクセスポイントとして機能

TrustZone が提供する分離機能により、攻撃者がよく狙う重要なコンポーネントへの攻撃界面を大幅に削減し、組み込みデバイスのセキュリティ評価を簡素化できます。Arm TrustZone のオリジナル仕様では、この分離機能がフラッシュメモリと RAM に対応しています。しかし、ダイレクトメモリアクセス（DMA）やデータトランスファーコントローラ（DTC）などのバスマスタには対応していません。また、周辺機能や外部端子へのアクセスも分離されていません。したがって、GPIO などの外部端子や周辺機能に対する様々な攻撃に対してマイクロコントローラは脆弱なままになります。

Renesas RA ファミリが対応する Arm TrustZone

Renesas RA ファミリマイクロコントローラにおけるシステム分離のアーキテクチャは、上述した Arm v8-M TrustZone に加えて、いくつかの重要な機能強化を行っています。図 3 を参照してください。RA ファミリでは、この TrustZone の機能を使うか使わないかはユーザの選択次第ですが、現在のコネクテッドワールドにおいては、この機能を活用し、自信と安心を持って IoT エンドポイントやエッジノードを安全に展開されることを強くお勧めします。ルネサスは、すべてのアプリケーションにおいて、柔軟で堅牢なセキュリティ機能の提供が今こそ必要だと認識し、Arm TrustZone のアプローチをさらに前進させ、組み込みシステムの将来ニーズを見据えた安全なシステム分離の仕組みを提供しています。

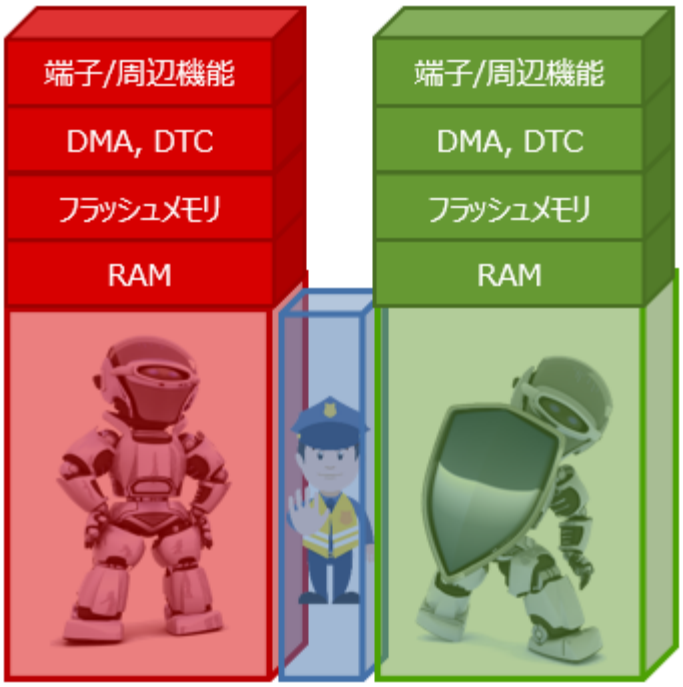


図 3. Renesas RA ファミリ Cortex-M33 マイコンコントローラにおける TrustZone の実装イメージ

RA ファミリ Cortex-M33 マイクロコントローラにおける TrustZone 実装では、DMA や DTC などのメモリアクセスからもセキュアコードやセキュアデータのコピーを防止しています。また、すべての周辺機器と IO ピンにも TrustZone が適用され、すべての外部インターフェイスにおける出力オーバーライドや入力の盗聴を防止します。

セキュリティメモリ保護ユニットからの更なる進化

Arm Cortex-M で TrustZone が利用できるようになる以前から、ルネサスはコネクテッド・デバイスのセキュリティの重要性を認識しており、セキュリティメモリ保護ユニット（MPU）を搭載したマイクロコントローラを提供してきました。セキュリティ MPU は、TrustZone のようなシステム分離機能に対応していないプロセッサのセキュリティを強化する方法です。しかし、要求仕様や求められるセキュリティ機能によっては、さらなる機能強化が必要な場合がありました。ルネサスは、Arm TrustZone を実装することで、ルネサス RA ファミリラインナップのシステム分離機能、セキュリティ機能をさらに進化させました。図 4 を参照してください。

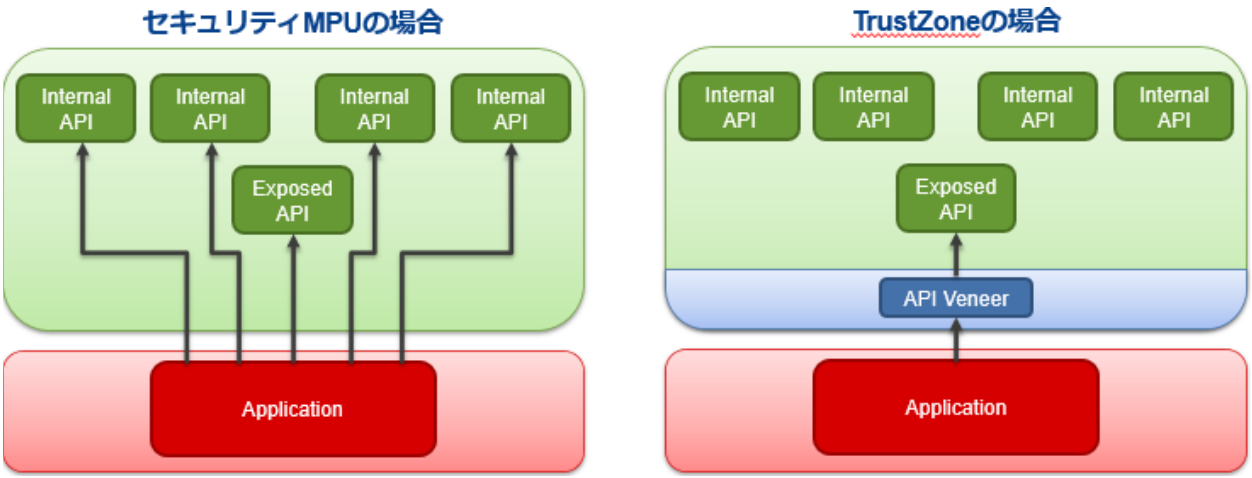


図 4. ノーマルワールドからセキュアワールドの API へのアクセス比較
セキュリティ MPU の場合（左）と RA の Arm TrustZone の場合（右）

セキュリティ MPU の場合、アプリケーションは論理的に API にアクセスできます。この際に API へのアクセスを制限する方法はありません。公開している API が特定のセキュリティ機能を含む場合や、ビジネス上の機密性が高いアルゴリズムへのアクセスを行う場合を考えてみてください。 図 4 に示すように、セキュリティ MPU の場合、セキュアワールド内の API へのアクセス方法に制限はありません。API ルーチンがどこにあるのか、どんなパラメータを使用するのかがわかってしまえば、その API ルーチンが使用可能です。推奨されるアクセス方法ではありませんが、ノーマルワールドのコードから、セキュアワールドの特定のサブルーチンにアクセスすることができてしまうのです。一方で、TrustZone を使用すると、公開された API を介したセキュアワールド内の API へのアクセスは、ハードウェアによって制御されます。ノーマルワールドのアプリケーションコードは、ノンセキュア・コーラブル・ベニアを経由してでしかアクセスできません。よって、ノーマルワールドのアプリケーションコードが API 内のサブルーチンに直接アクセスするメカニズムは物理的に不可能です。

同様の例は、コードの誤用を防ぐことについても言えます。図 5 を参照してください。

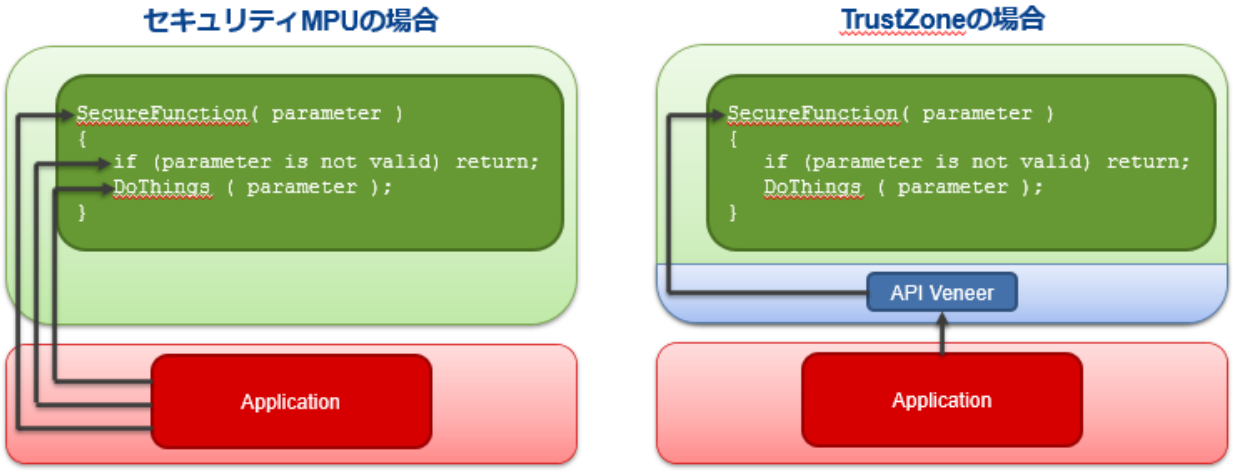


図 5. Arm TrustZone によるコードの誤使用防止

セキュリティ MPU の場合、非セキュアアクセスでも、特定のアドレスにジャンプすることにより、正式なエントリポイントがバイパス可能となります。これは、コードの誤使用であり、それが偶然であれ故意であれ、防ぐ手立てはありません。もし、開発者が、ノンセキュアコードで、正式なエントリポイントをバイパスして、有用な関数のエントリポイントに直接ジャンプすることで得られるパフォーマンスや操作上の利点があることに気付いた場合、セキュリティ MPU には、そういった行為を防止する術はありません。TrustZone を使用した場合、セキュアコードへのアクセスが正しい方法となるよう、ハードウェアで制御されます。ノンセキュアコードは、唯一のエントリポイントである API ベニヤを介してのみセキュアコードにアクセスします。この方式であれば、セキュアコードを物理アドレスを使用してダイレクトに呼び出す行為を禁止することができます。

ルネサスによる TrustZone 実装では、外部インターフェイスや端子への無制限なアクセスも禁止しています。ノンセキュアコードによる、端子への直接の読み取りや書き込みを防止しすることで、盗聴やなりすましを防止しています。

アプリケーションの API アクセスを制限し、コードの誤使用を防止し、外部インターフェイスへのアクセスを監視することで、攻撃者が利用できる潜在的な攻撃対象領域を限定しています。

TrustZone のユースケース

Arm TrustZone が提供するノンセキュア環境とセキュア環境の分離機能には、さまざまなユースケースが考えられます。このセクションでは、IP 保護、コード分離、および Root Of Trust（信頼の基点）の保護の 3 つの利用例を紹介します。

IP 保護

モータ制御アルゴリズムなどの特殊なアルゴリズムの開発には時間と労力がかかるため、アルゴリズム開発者がこの IP を違法にコピーされる脅威から保護したいと考えることは理に適っています。アプリケーションの柔軟性を維持しながら、これを実現する 1 つの方法として、アルゴリズム開発者がマイクロコントローラのセキュア領域にアルゴリズム IP を事前にプログラムし、アプリケーションがそのアルゴリズムにアクセスするための API を提供することが考えられます。図 6 を参照してください。

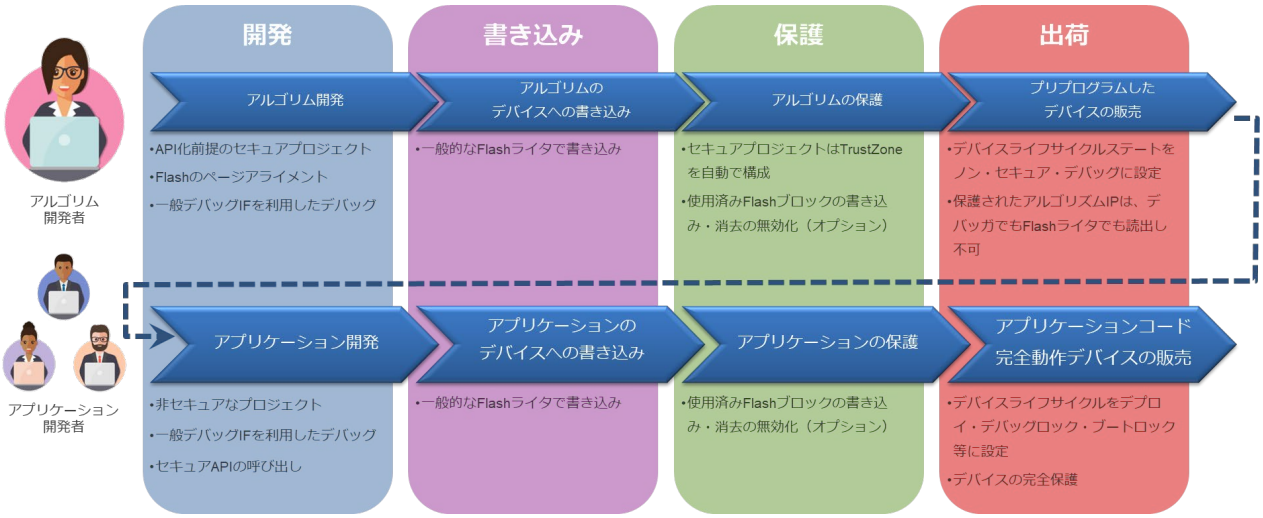


図 6. アルゴリズム IP を事前にプログラムし、TrustZone を用いてアプリケーションから保護するユースケース

アルゴリズムをセキュアワールドにプログラムし、アルゴリズム IP が書き込まれたメモリブロックの変更および消去を無効にします。アルゴリズム開発者は、アルゴリズム IP を書き込んだチップを不正アクセスや著作権侵害から完全に保護した状態で、アプリケーション開発者に販売することができます。一方、アプリケーション開発者はノーマルワールドを利用してアプリケーションコードを開発、NSCV を介して事前にプログラムされているアルゴリム IP に自由にアクセスすることもできます。

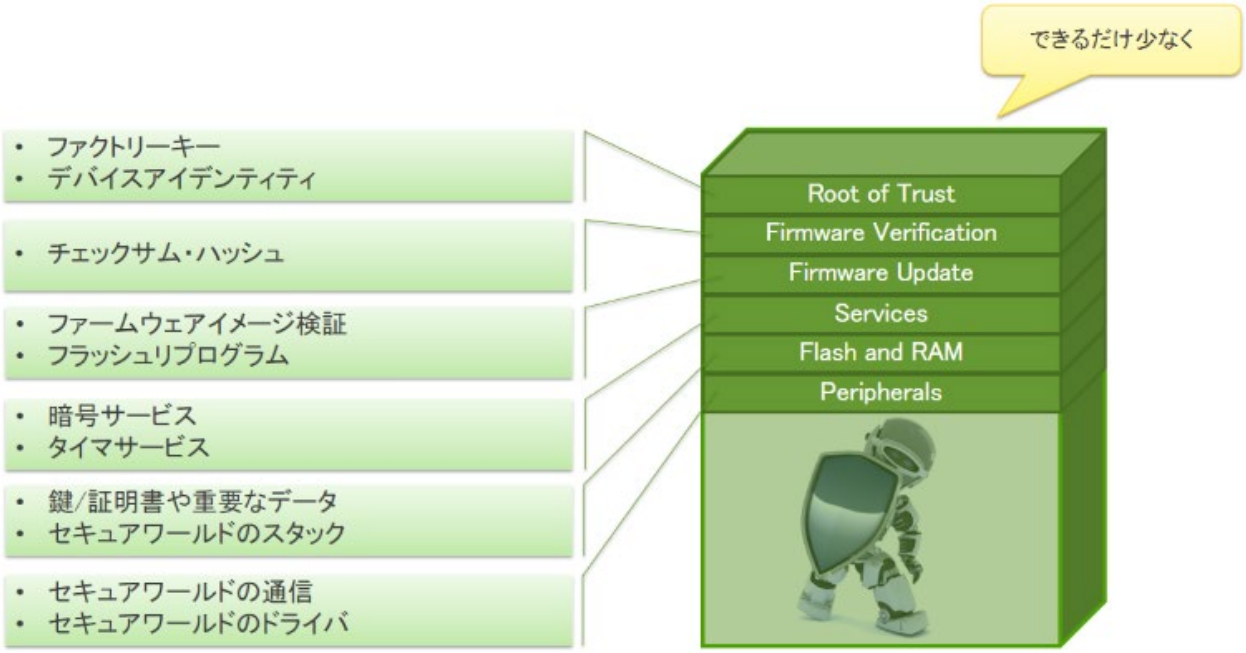
コード分離

TrustZone によるコード分離の優れた利用例として、欧州のスマートメーター規格が挙げられます。欧州計量器規制(MID)において、測定および請求金額の計算に使用する部分のアプリケーションコードは認証取得が義務付けられています。この規制に該当する部分のプログラムコードは、スマートメーターアプリケーションの他の部分から分離されている必要があります。現在、これを実現する唯一の方法は、2 つのマイクロコントローラを使用し物理的に分離することです。この場合、認証プロセスは簡素化されますが、追加部品によるコスト増、消費電力の増加、余計な PCB スペースが必要になっています。

ここに新たなアプローチとして、ArmTrustZone を使用した論理的に分離する方法が考えられます。規制に該当するすべての認証済みコードはセキュアワールドに配置し、認証を必要としない残りのコードはノーマルワールドに配置します。

Root Of Trust(信頼の基点)の保護

デバイスの信頼の基点(RoT: Root of Trust)は、ここを基点として構築されるすべてのセキュリティの基盤となります。RoT には、工場出荷時に設定された秘密鍵、認証済みファームウェア、デバイス ID、および起動時のチェックサム計算に必要な資格情報が含まれています。上位層のセキュリティ障害が原因でデバイスが危険にさらされた場合、RoT からやり直すことができますが、RoT が侵害された場合、RoT を基点としたすべてのセキュリティは信頼を失います。よって、すべての RoT 要素はセキュアワールドに保持することを強くお勧めします。図 7 を参照してください。



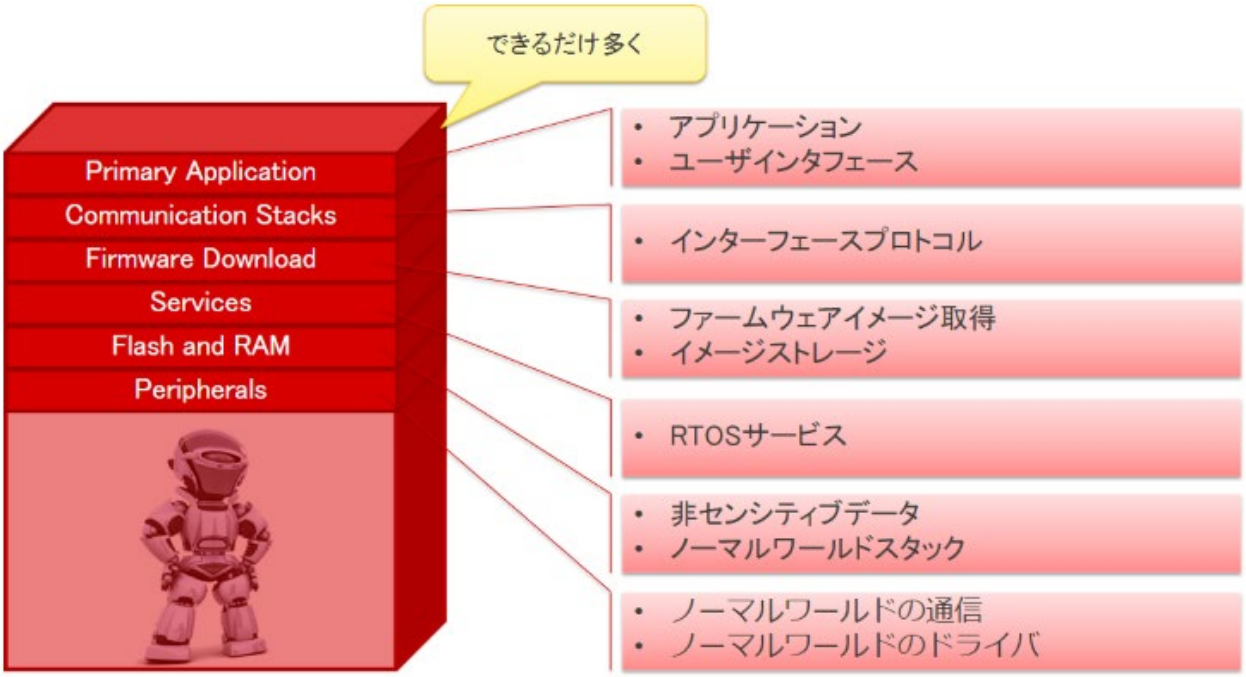


図 7. Arm TrustZone による信頼の基点（RoT: Root of Trust）の保護

Renesas RA ファミリ Cortex-M33 マイクロコントローラ

Renesas RA ファミリ Cortex-M33 は、Arm v8-M TrustZone テクノロジを採用した Arm Cortex-M33 コア搭載のマイクロコントローラです。暗号アクセラレータが強化された Secure Crypto Engine と TrustZone によってセキュアエレメント機能を実現できます。 セキュリティ関連機能として、高度な鍵のマネジメント、改ざん検出、および電力解析耐性機能なども備えます。 アプリケーションコード用に最大 1MB のフラッシュメモリ、エラー訂正（ECC）を備えた SRAM を内蔵しています。周辺機能としては、静電容量式タッチセンシングコントローラ、イーサネット、USB 2.0 フルスピード、SD ホストインタフェース、および SPI インターフェイスなどが搭載されています。

RA ファミリを採用したセキュア IoT アプリケーション開発には、利便性の高いエコシステムである Flexible Software Package (FSP)をご利用いただけます。FSP には、FreeRTOS を採用しており、BSP、HAL ドライバに加えて、コネクティビティやセキュリティ、グラフィックスなどのミドルウェアをご用意しています。GitHub から無償で入手してご利用いただけます。

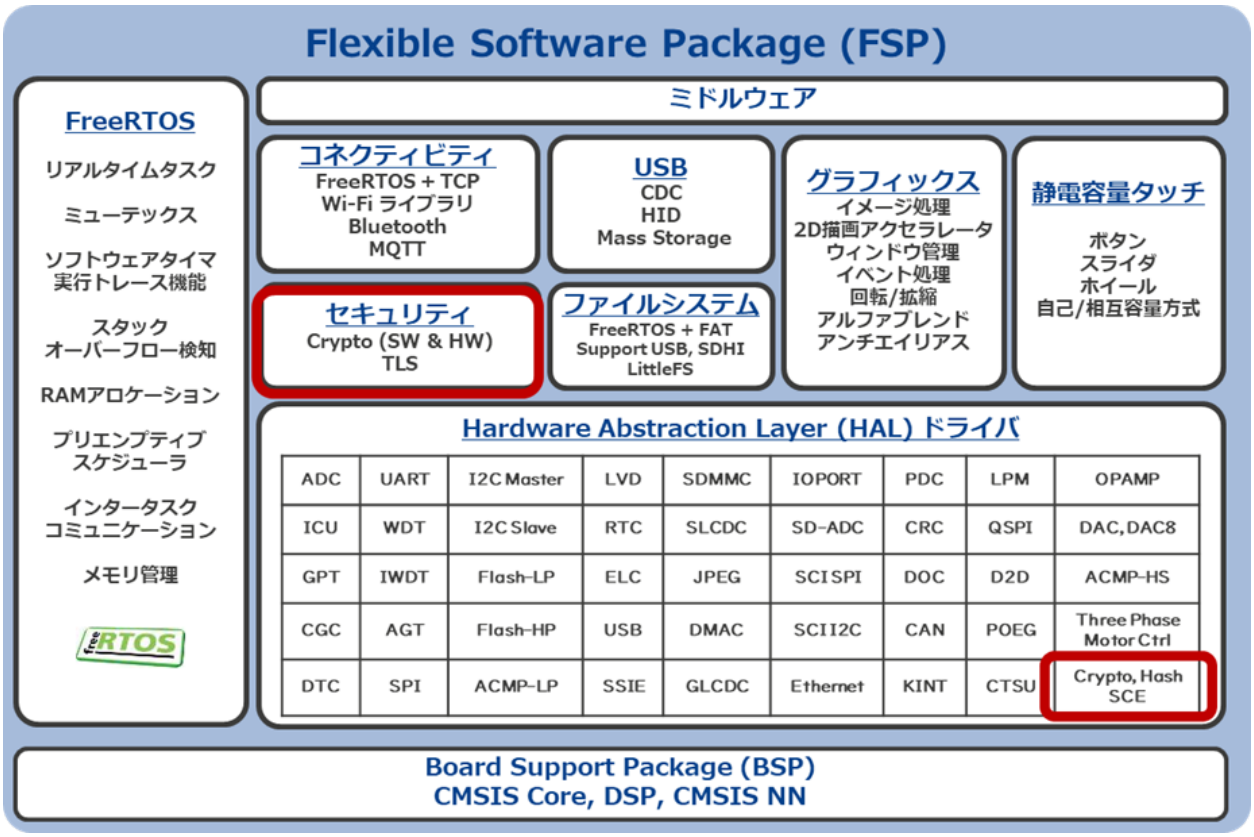


図 8. FSP 機能の概要

また、ルネサス RA パートナエコシステムには、RA ファミリを採用した開発に有用な、さまざまなパートナベンダ製のソフトウェア製品やハードウェア製品をリストアップさせていただいています。FSP に加えてこうしたパートナ製品を活用することで、IoT アプリケーションの開発を加速することが可能です。

結論

Renesas RA ファミリ Cortex-M33 マイクロコントローラは、Cortex-M33 コアの高い性能と、先端 40nm プロセスによる低消費電力を両立させたマイクロコントローラです。コードやデータ、IP 資産の論理的なシステム分離を必要とするさまざまな産業および民生アプリケーションを構築するための理想的なプラットフォームです。 RA ファミリの TrustZone 実装では、RAM やフラッシュメモリのみならず、周辺機能や端子、ダイレクトメモリアクセスなどのバスマスタにも適用し、機能をさらに強化しています。

詳細情報

1. RA6M4 製品情報
2. RA4M3 製品情報
3. RA パートナエコシステム

4. Flexible Software Package (FSP)
5. RA ファミリの MCU
6. Arm® TrustZone®