RENESAS synergy™

Renesas Synergy™ のセキュリティポートフォリオが産業分野およびIoT（Internet Of Things）における脅威に対する包括的な保護を提供

高度なセキュリティ機能によって、組み込みシステムエンジニアの悩みを解決する

今日、140億台もの機器がインターネットに接続されていると予測されています。さらに、2020年までにはその数は500億台に達することが見込まれており、IoT市場はますます大きなビジネスチャンスとなります。しかし、それは同時に重大なセキュリティリスクが発生することも意味しています。どうしてなのでしょうか？重要なことは、今日、インターネットに接続されている70％以上の機器が、セキュリティ対策が不十分で、常に何らかの脅威にさらされるリスクを抱えている状況にあるということです。Open Web Security Application Project（OWSAP）の最新の報告から、この問題の深刻さを伺い知ることができます。

2015年8月

以下のような状況が報告されています。

- 60%：認証の脆弱性などユーザーインタフェースに問題がある機器
- 70%：暗号化されていないネットワークサービスを利用している機器
- 70%：外部から侵入して個人情報を盗み取ることが容易な機器、クラウド、モバイルアプリケーション
- 80%：堅牢なパスワード設定を要求していない機器、クラウド、モバイルアプリケーション

ネットワークに接続される機器とシステムの増加に伴い、セキュリティ保護に対する潜在的リスクおよびその影響はより深刻なものになっていきます。たとえば、製造工場がサービス妨害攻撃（DoS攻撃）または分散型サービス妨害攻撃（DDoS）のターゲットになると、生産システムの処理に過度な負荷がかかり、重要な処理を行うことができず、生産ラインがストップする恐れがあります。また、ネットワークの接続先である温度監視・制御システムがDoS/DDoS攻撃され、システムオペレーターへの通知またはオペレーターからの指令がブロックされた場合、厳しい温度管理を必要とする工場の冷却システムに重大な影響を及ぼすことになるでしょう。同様に、DoS/DDoS攻撃が、道路交通制御システムに侵入した場合、交通インフラに大きな影響を及ぼすことになります。さらに、国家の安全保障においては、その影響は深刻です。現に米国国家安全保障局（NSA：National Security Agency）は、2014年、米国は現実的にはサイバー空間で戦闘状態にあり、ハッカーがすでにシステム内に潜入していることを認めています。米軍幹部による、米国の電力システムおよび金融業界を機能不全にするだけの能力を持つ国家も存在するという報告もあります。

個人ユーザーという観点から言えば、私たち消費者はネットワークに接続された機器を使用する機会が増えるにつれて、よりセキュリティ機能の脅威にさらされている状況にあるといえます。たとえば、乳幼児用の監視モニター、血糖値測定器、ペースメーカーなど、ネットワークに接続されている多くの医療機器を私たちは使用しています。もし、これらの医療機器がネットワークを通じて攻撃を受けた場合、機器を使用できなくなるだけでなく、外部から侵入されたことにより不適切な量の薬品が投与される危険があるなど、私たちの健康そのものに重大な影響を及ぼすことになります。自宅からネットワークに接続する機会が増えるにつれて、ハッカーに個人情報を盗まれる危険も、今後は急速に高まっていくでしょう。

この問題の深刻さを理解するために、お客様に「IoTで最も深刻な脅威となりうるのは何か」と尋ねました。次の6項目がIoTに対する脅威として捉えられているということがわかりました。

- 信頼できない契約製造業者がソフトウェアまたはファームウェアのクローニングを行う。あるいはMicrocontroller Unit（MCU）または製品のセキュリティ設定のクローニングを行う
- ハッカーが純正のファームウェアをインストールする段階でマルウェアに置き換え、製品を破壊する
- 特にセキュリティパラメーターが暗号化されずにやり取りされた場合、ハッカーがファームウェアのインストール中に盗み見て攻撃する
- システムファームウェアが物理的に保護されていない場合、外部からセキュリティパラメーターが抽出されてしまい、プライバシーへの脅威となる
- 外部からアドオンプログラムを使用して情報を改ざんしたり盗もうとしたりする
- ハッカーが単純なソフトウェアアップデートセッションを利用して、ファームウェアをマルウェアと置き換えようとする

Renesas Synergyプラットフォームを構築していくにあたり、すぐに明確になったことがありました。それは、Renesas Synergyプラットフォームを中心に構築した機器のセキュリティを確実かつ安全なものにするためには、このような脅威すべてに対応する必要があるということです。製品ライフサイクルのすべての段階でこれらの脅威から機器を守るためのセキュリティ機能をプラットフォームに組み込まなくてはならないということ

です（セーフティクリティカル機能およびサービスについては別途レビューを行う予定です）。

ルネサスは、すべてのアプリケーションにおける潜在的な脅威に対応するため、かつてないほどのセキュリティ機能を備えた統合ハードウェア / ソフトウェアプラットフォームを開発しました。新しいセキュリティ機能の多くは、外部から攻撃される可能性が比較的低いハードウ ェア側に実装されています。たとえば、Renasas Synergy MCU が製造される際は、128 ビットの固有 ID が割り当てられ、アプリケーションを保護し、プロビジョニングをサポートするキーの生成に使われます。従来の擬似乱数生成器に比べて大幅な改善を加えた Renesas Synergy の乱数生成器は、最新の NIST SP 800-90 規格を満たし、MCU 暗号アクセラレーターおよびキー生成器に密接に統合されています。

Renesas Synergy のすべての MCU（S1、S3、S5、および S7 シリーズ）では、対称暗号アクセラレータ、HASH、真性乱数生成器、JTAG アクセス制限機能を備えています。Renesas Synergy においてハイエンドに位置づけられる S7 シリーズおよび S5 シリーズでは、非対称暗号、非対称キー生成、およびキーの安全な保管のためのアクセラレータも内蔵しています。Renasas Synergy のセキュアメモリ保護ユニット（MPU：Memory Protection Unit）は、認証済みユーザーのみによるメモリ特定領域へのアクセス許可を保証するために使用されます。

Renasas Synergy プラットフォームは、システムの整合性および可用性を保証するにあたり、重要な役割を果たします。たとえば、多くの接続されたシステムの整合性においては、ステークホルダーを分離することが重要になります。Renesas Synergy MCU で利用できるセキュア MPU では、セッションキーやユーザーデータを機器のデータから分離し、システムが構成データ向けに別のサンドボックスを作成できるようにすることで、ユーザーが複数のステークホルダーを同時に操作できるようにします。

Unique ID	True Random Number Gen	Crypto HASH Functions	Symmetric Key Crypto	Asymmetric Key Crypto	Secure Key Storage	Read-Out Protection
Security Software Library						

Threat	S7	S5	S3	S1
Product cloning	Best	Best	Better	Good
Product disruption with malware injection during update	Best	Best	Better	Good
Eaves-dropping during update	Best	Best	Better	Good
Privacy threat by firmware/data exposure	Best	Best	Best	Good
Add-on program to damage or steal	Best	Best	Best	Limited

Renesas Synergyセキュリティ保護

Renesas Synergyプラットフォームには多くのセキュリティ機能を備えています。

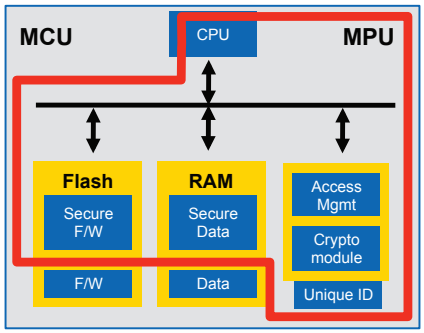
製品ライフサイクル全体での保護

ID 盗難のリスクは、MCU が機器設計チームの手を離れた直後の製造段階から始まります。たとえば、設計チームが血糖値測定器を作っているとします。もし、契約製造業者に悪意があれば、著作権のあるアルゴリズムの逆行分析を行って血糖値測定器の MCU を偽造し、競合他社に売る可能性があります。このような製品のクローニングは、製品の売上・収益に悪影響を与える脅威となります。低品質の機器が市場に出回り、そうとは知らずにクローン製品を購入した購入者に対するサポートの問題が生じると、元の製造メーカーの評判に傷をつける恐れもあります。

Renesas Synergy MCU では、革新的な機能を組み込んで各デバイスの認証方法を刷新し、クローニングに対する脅威を徹底して抑えます。Renesas Synergy MCU を使用するエンジニアは、製造プロセスの初期段階でルネサスまたは他社製のキーインジェクションサービスを使用するオプションを選択できます。キーインジェクションは、実質的に独自の識別子または出生証明書を MCU に割り当てます。早期にキーインジェクションを行うことにより、コードをデバイスにロックすることができます。以降、コードのチェックサムは既知の値でなければ認証されません。

Enable a Certifiable Root of Trust

- Measures and verifies software boot chain
- Performs device authentication
- Protects cryptographic keys



Secure Key Provisioning and Generation

- Keys can be provisioned prior to manufacturing to secure devices
- Generate keys via integrated Asymmetric Key Generation Unit
- Keys held in secured and isolated memory

ソリューション：早期および安全なIP保護

キーインジェクションサービスおよび認証可能なRoot of Trustなどの新しい機能が、製品のクローニングに対して確固たる防御となります。

独自の識別子が製造プロセスの初期段階に割り当てられると、MCU の ID を盗むことが難しくなります。Renesas Synergy S7 シリーズは、MCU 上でキーの保管および生成を行うことが可能な数少ない MCU の 1 つです。

ルネサスが製品のクローニングに対応するために Renesas Synergy プラットフォームで提供するもう一つの機能は、認証可能な Root of Trust です。Root of Trust はセキュリティの基礎となり、その他のセキュリティコンポーネントはこの上に構築されます。たとえば、セキュアファームウェア、データ、アクセス管理、暗号化モジュール、デバイス固有 ID など、オペレーティングシステムが信頼し、リセット直後に操作できなくてはならない組み込みシステムの主要なコンポーネントです。

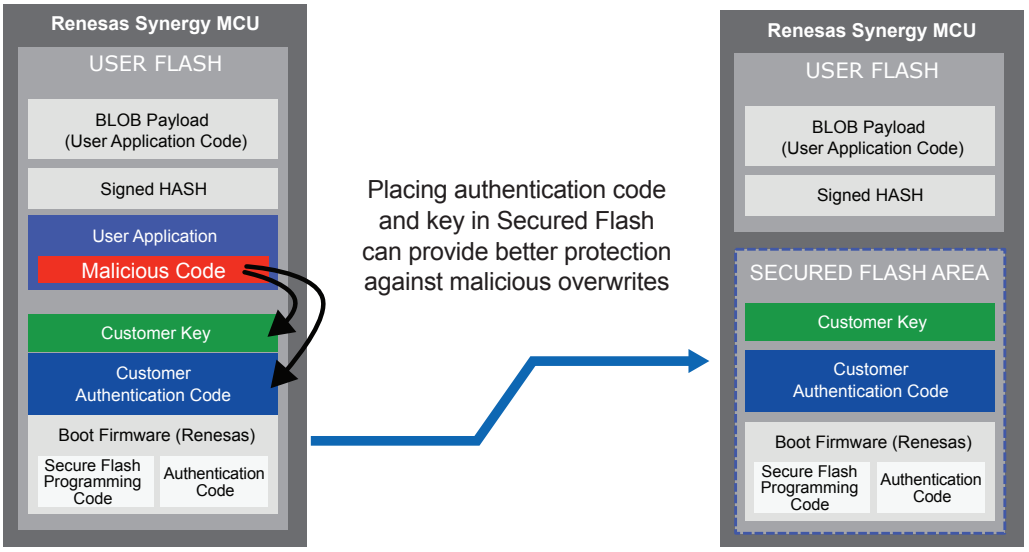
Root of Trust は、主に 3 つの役割を果たします。第一に、ソフトウェアブートチェーンを測定および検証できなくてはなりません。このため、システムブートチェーンの下で独立して存在する必要があります。第二に、Root of Trust は暗号化キーを保護しなくてはなりません。Root of Trust のキーは、早期にそして安全にプロビジョニングされる必要があります。Renesas Synergy プラットフォームの早期キーインジェクション、安全なストレージ、および JTAG アクセスの制限により、これらの要件が必ず満足されます。第三に、Root of Trust は、機器の認証を行う必要があります。Renesas Synergy プラットフォームは、非対称キー生成器、非対称暗号アクセラレータ、真性乱数生成器、および対象暗号エンジンによりこの役割を果たします。

IoT 機器がフィールドにインストールされると、すべてのリモートパッチ、ソフトウェアアップデート、またはライフサイクルのメンテナンスルーチンが潜在的な脅威となります。これらの各機能はリモートで、かつ安全に実行されなくてはなりません。悪意のある改ざんから保護するため、Renesas Synergy プラットフォームは、コードとそのキーを MCU の安全なオンチップフラッシュメモリ領域に配置する認証済ブート機能を備えています。

従来の MCU は、ユーザーの認証コードをユーザーフラッシュに割り当てたに過ぎません。そのため、コードは上書きされる可能性があります。Renesas Synergy プラットフォームでは、JTAG アクセスを制限し、MPU の安全なフラッシュ領域で認証コードを保護するため、ハッキングが難しくなります。ユーザーフラッシュセキュリティロードの残りはそのままです。BLOB ペイロードは、信頼できるソースからもたらされたことを証明する署名済み HASH によりアップデートされる可能性が高く、追加物がないことを保証するために予想サイズ（HASH）も示されます。

Renesas Synergy の認証ブート機能は、デバイスがダメージを受けそうな場合、継続的に保護されることを保証することにより、プロダクトライフを延ばします。ダメージを受けそうなことが確認された場合、認証ブートは適切に確認された所有者のみにデバイスのアップデートを許可します。アップデートはサーバーが署名およびコードを検証した場合にのみ許可され、ソフトウェアを旧バージョンにロールバックすることはできません。

インストール後の環境において、ネットワークに接続された機器またはシステムのユーザーは、常にハッカーによる脅威にさらされることになります。たとえば、ハッカーがスマートホームに侵入した場合、個人情報が盗まれ、ネットワーク上の機器の正常な動作に影響を与えます。同様に、スマートファクトリーが攻撃を受けた場合、製品の生産が遅れる、ストップするなど、壊滅的なダメージを受けることになります。



Subject to Change

ソリューション：認証ブート

認証コードおよびキーを安全なフラッシュに配置することにより、Renesas Synergyの認証ブート機能は製品の寿命を伸ばします。

ハッキングからデバイスを保護するために、Renasas Synergy プラットフォームは、3 つの主要なセキュリティ機能を追加しました。信頼できるコードのライブラリ、サンドボックス、そして ThreadX® RTOS です。信頼できるコードのライブラリは、入力と通信を制約することでバッファーのオーバーフローおよびコードのインジェクションを回避します。たとえば、暗号化および安全なブートコンポーネントは、入力のサブセットのみを有効にし、感染を制御します。

サンドボックスは、Renasas Synergy プラットフォームが攻撃を受けている間でも可用性を保つための機能です。システムがオペレーティングシステムおよびアプリケーションの異なる面を分離できるようにします。基本的には、統合 MPU を使用して、特権を持つアプリケーションのみがアクセスできる領域、および通信が可能な領域にオンチップメモリを分離します。このセグメント化により、ユーザーはスーパーバイザーモードとユーザーモードを作成し、ユーザーモードにおける問題がスーパーバイザーモードに影響しないようにできます。さらに、サンドボックスを利用してメモリ領域を読み取り不能またはプリント不能にすることができます。いったん分割された後にアプリケーションで問題が起きた場合（サービス妨害攻撃など）、MCU はハードウェアでフラグを立ててシステムをリセットします。これが攻撃に対する防御となります。

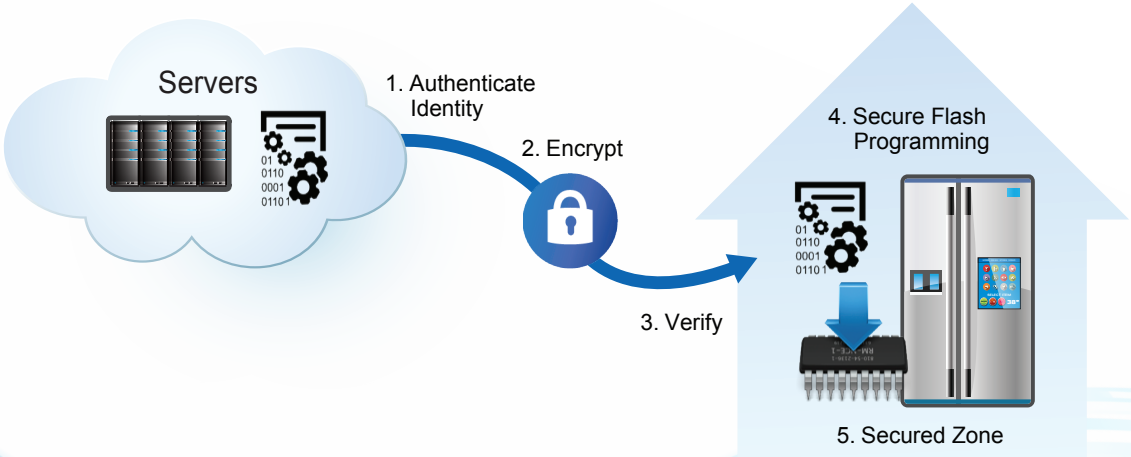
さらに、Renesas Synergy プラットフォームは業界で実績が証明されている RTOS、Express Logic 社の ThreadX® を使用しており、セキュリティ上のメリットを飛躍的に向上しています。何万人ものユーザーに長年使われてきたオペレーティングシステムとして、ThreadX® は堅牢なセキュリティ基準に基づいて、開発、チェック、そして認証されているという安心感があります。

ファームウェアの保護

製品ライフサイクルにおける開発段階と製造段階において、組み込みシステムはファームウェアにおいて特に脆弱です。ネットワークに接続された機器の最大のメリットは、ファームウェアを遠隔地からリモートでアップデートできるということですが、同時に、この機能は脆弱性ともなりえるものです。典型的な例が自動車の製造ラインです。自動車の製造ラインの MCU がファームウェアによりコントロールされ、マルウェアを注入されたとします。このような場合、製造ラインだけでなく、生産される自動車の性能そのものがダメージを受け、さらに自動車を運転する私たち消費者の生命に関わる事態に発展する可能性さえあります。

Renesas Synergy プラットフォームは、5 段階の認証ファームウェア管理プログラムを利用して、このような攻撃から保護します。1）ID 認証ファームウェアアップデートサービスのデジタル認証と ID 確認をします。Renesas Synergy プラットフォームでは、独自の ID キーセキュアストレージ、非対称暗号化、および非対称キー生成器など、複数の技術を利用してコミュニケーションチャネルを認証します。2）暗号化バイナリがダウンロード中に改ざん・遮断されないように、真性乱数生成器および HASH を備えたセキュア暗号エンジン、トランスポートレイヤーセキュリティ（TLS）接続を使用します。Renesas Synergy プラットフォームが高性能な暗号処理を実現できるのは、セキュア暗号エンジンが、真性乱数生成器、対称暗号アクセラレータ、非対称暗号アクセラレータ、HASH アクセラレータ、ストリーム解読アクセラレータ、セキュアキーストレージなど、多数の重要な機能を統合しているからです。Root of Trust に近いセキュア暗号エンジンの近くにある真性乱数発生器は、ソフトウェアイネーブルではなく、より小さいセッションキーをサポートするため、外部からの攻撃を受けにくくなっています。

3）検証統合 HASH 技術を使用して、ダウンロードされたバイナリがサーバ上のソースバイナリと同じであることを確認します。4）セキュアフラッシュプログラミングセキュア暗号エンジンを使用して認証されたバイナリのみをプログラムします。5）安全な領域の確保フラッシュ上のバイナリを保護するため、システムはセキュア MPU および制限付き JTAG アクセスを使用して安全領域を作ります。



ソリューション：認証されたファームウェア管理

Renesas Synergyプラットフォームには多くのセキュリティ機能を備えています。

結論

産業分野および IoT 市場では、組み込みシステムエンジニアが今まで直面したことがないセキュリティ上の問題にさらされています。製品のクローニングから盗み見攻撃、そしてアドオンプログラムやファームウェアの置き換えまで、エンジニアは新しいレベルの脅威に対応する必要があります。この市場で生き残るための鍵は、エンジニアが製品ライフサイクル全体でデバイスを保護するために最適なプラットフォームを選択し、投資することです。

Renesas Synergy プラットフォームは、包括的かつ堅牢なセキュリティ機能をハードウェアとソフトウェアにおいて提供することにより、長期にわたる製品の品質を保証します。お客様が安心して製品開発できるように、ルネサスは常に最新のセキュリティリスクに対応しながらソリューションを提供し続けていきます。