ホワイトペーパー

# IoT デバイスに求められる安全なインターネット通信機能

Brad Rex、シニアプロダクトマーケティングマネージャー、ルネサスエレクトロニクス社 IoT インフラストラクチャビジネスユニット

2020 年 1 月

## 概要

インターネット接続されたデバイスを包括的に保護することが、これまで以上に重要になってきています。しかし、1つのソリューションで全てに対応可能なインターネットセキュリティはありません。組込みシステムは、システムごとにそれぞれ異なる仕様や要求が存在し、各システムのすべての脆弱性を保護できる万能ソリューションはありません。組込みシステム開発では、開発コストや納期を守りつつ開発手法や取込む機能の優先順位などのバランスを取る必要があります。このホワイトペーパーでは、インターネット通信セキュリティについて複数の保護方法を検証し、その正しい実装方法について説明します。

## 増大する脅威の状況

今や日々の生活でもっともありふれたものと言えるコーヒーカップやピルケースまでインターネットやクラウド接続される時代です。これは、日々の生活環境の多くが潜在的なセキュリティ攻撃の対象になっていることを意味します。インターネット接続されたデバイスに対するサイバー攻撃がより強力で悪意を持つようになると、ハッカーやマルウェアによってほぼすべの生活シーンが危険にさらされる可能性があります。

インターネット経由のすべての通信を保護するためには、組込みシステムにセキュリティ機能を付加し、その機能やデータを保護することが、今日のシステム開発の最重要課題となっています。

重要なポイントは、組込みセキュリティは後付けで考えることはできないということです。セキュリティ機能は、企画段階から計画的に設計する必要があります。セキュリティ機能の後付けも可能かもしれません。しかし、こういった方法はコストの大幅な増加を招きます。さらに、セキュリティの脆弱性によっては、最悪、製品のリリース後にセキュリティ欠陥が露呈し、それに適切に対処できない場合があります。

ここで必要なことは、ハードウェアとソフトウェアの両方に対応した最新セキュリティ技術を活用し、インターネット通信を多層・包括的に防護できる首尾一貫したセキュリティ戦略です。

## 安全な通信技術

インターネット経由のデバイス間通信を十分に保護するためには、複数の保護層が必要となります。多くのセキュリティ脅威からデバイスを保護するためには、ハードウェアによってキー生成を行ってデバイス ID を保護する必要があります。デバイス ID は、開発したデバイスに生成し組込まれるとき、十分信頼できる方法で安全に内部フラッシュに保存される必要があります。

堅固なデバイス ID を確立することで、すべてのデバイスを一意に識別し認証することが可能です。強力なデバイス ID を獲得できれば、組込みシステムのさまざまなセキュリティ要件に対応でき、製品化したデバイスが相互接続されたときに安全に認証と識別を行うことが可能となります。

一意のデバイス ID を生成する方法として、最も簡単な方法がシリアル化です。例えば、製品のシリアル番号を使用する方法やデバイス ID の連番化です。一方、非対称暗号化手法で生成するデバイス ID は、より強力なセキュリティと幅広い用途を提供することができます。

**キーベースの暗号化**：暗号化されたデバイス ID を作成する最初の手順は、キーの生成です。キーは、デバイス内で生成する方法と、安全な施設で生成しデバイス内に注入する方法があります。デバイスキーが生成または注入されると、認証局（CA）がデジタル証明書を発行します。CA は、パブリック（クラウドに配置）またはプライベート（オンプレミスに配置され、通常は安全なサーバーでホストされる）のいずれかです。デバイス ID を作成してデバイスにプログラムしたら、デバイス ID（キーと認証）が消去または再プログラムされるのを防ぐために、「セキュアコード」のみがアクセスできるセキュアメモリ領域に安全に保存する必要があります。

非対称暗号アルゴリズムは、公開鍵と秘密鍵の作成が必要で、デジタル証明書による認証を提供する公開鍵インフラストラクチャ（PKI）と呼ばれる暗号化手法の一部です。公開キーは誰にでも公開できますが、秘密キーは公開キーで暗号化されたデータを復号化する当事者だけが知っている必要があります。

セキュリティで保護された単一 ID を持つデバイスがネットワークに接続された場合、他の同様に識別されたデバイス、サービス、およびユーザーと認証を行い、**信頼**を確立し、その信頼できるメンバー同士で、暗号化されたデータや情報を安全に送信や交換ができるようにする必要があります。**プライバシー**保護は、一意のデバイス ID のもう 1 つの利点です。ネットワーク上で交換されるデータに個人情報、機密情報、財務情報が含まれる場合、何らかの規制に準拠する必要があります。デバイス ID を使えばセキュリティで保護されたデータ送信が可能となります。デバイスの**整合性**は、デバイス自身と信頼が確立したチャネルを通るデータ、その両方に適用されます。 デバイス自身の整合性は、デバイスが「自分自身が正しい存在である」ことを証明することから始まります。 強力なデバイス ID を使うことで、デバイスは正統であることが保証され、偽造品を減らし企業のブランドを保護します。

**転送中のデータの保護**： デバイス ID は、安全な製品、安全な製造、安全な通信の基盤です。しかし、ネットワーク上を移動するデータの安全性には、別のセキュリティが必要です。

**トランスポート・レイヤー・セキュリティ（TLS）**は、コンピューターネットワーク上で通信セキュリティを提供する暗号化プロトコルです。 新たな脅威に対応するために、より強力なセキュリティ対策を行う新規格が次々とリリースされます。TLS は、非対称暗号化と対称暗号化の両方の技術を使用して、暗号化と復号化の速度を犠牲にすることなく高度なセキュリティを提供します。 そして、下記の機能を提供することにより、2 つのアプリケーション間通信のプライバシーと信頼性を提供します。

- **暗号化**：アプリケーション間通信で交換されるメッセージは、データ暗号化に使用される対称暗号化手法を使用して暗号化され、接続がプライベートになるようにします。
- **認証**：証明書ベースのメカニズムを使用して、ID を検証します。
- **整合性**：接続の信頼性とメッセージの整合性を確保するために、メッセージ認証コード（MAC）メカニズムによって、メッセージの改ざんと偽造を検出します。

**データ・トランスポート・レイヤー・セキュリティ（DTLS）**は、データグラムベースの通信を保護し、盗聴や改ざんを防ぐために設計された通信プロトコルです。 TLS プロトコルをベースとし、同様レベルのセキュリティを提供します。DTLS は、Web ブラウジング、メール、インスタントメッセージング、VoIP 等で使用できます。 DTLS は、TLS

がトランスミッション・コントロール・プロトコル（TCP）を使用するのに対し、ユース・データグラム・プロトコル（UDP）を使用します。ただし、DTLS は TLS よりもオーバーヘッドが低く、低遅延でタイムセンシティブな伝送に適しています。DTLS は、JavaScript API を利用するブラウザ間リアルタイム・コミュニケーション（WebRTC）に使用されるセキュリティプロトコルの 1 つです。

## セキュア IoT とクラウド通信

モノのインターネット（IoT）とクラウドコンピューティングの急成長により、デジタル通信の安全性確保にも新しい要求が出てきました。

IoT システムは、センサーやアクチュエーターなど色々な技術を結集したスマートデバイスで構成され、それらがお互いにインテリジェントにリンクして、モノや人の新しい形態の通信を実現します。IoT デバイスが連携して動作を行う過程で、IoT デバイスは大量のデータを生成し、クラウドコンピューティングは、データが目的デバイスまで移動する経路を提供し、また IoT デバイスでは到底処理できない計算処理を実行します。

IoT システムの適用分野には、スマートホーム、スマートシティ、ウェアラブルデバイス、e ヘルス、農業、エネルギー管理等があります。これらのスマートネットワークは、情報を収集・分析し、人間の補助なしで意思決定を行うことも可能です。このような便利な IoT の利用形態が普及すると、IoT システム内に悪意のある非認証デバイスが持ち込まれる可能性が生じます。こういった存在が与える影響を考えると、デジタル通信のセキュリティ保護は非常に重要な要求事項となっていきます。しかし、IoT ネットワークのセキュリティ要件（機密性・整合性・認証）は、IoT デバイス上で稼働するアプリケーションに大きく依存し、リソースが制限された IoT デバイスやネットワークでは、従来の認証や暗号化手法が使えない場合があります。

IoT デバイスがクラウドサービスを使用するためには、認証およびプロビジョニングされる必要があります。現在、ほとんどのクラウドプロバイダーは、ハイパー・テキスト・トランスファー・プロトコル（HTTP）、メッセージ・キュー・テレメトリー・トランスポート（MQTT）、およびコンストレインド・アプリケーション・プロトコル（CoAP）を組み合わせてデータ通信を行っていますが、セキュアなデータ送信を行うために、デバイスの資格情報に対して生成された、もしくはオフラインによって生成された、プロビジョニング証明書とキーを用いた TLS/DTL を使用します。

**HTTP** は、World Wide Web で使用される基本的なプロトコルです。HTTP は、Web ブラウザとサーバーとの通信用に設計されましたが、他の目的にも使用できます。ただし、HTTP はもともと平文転送用に設計されたので、盗聴や中間者攻撃に対して脆弱でした。そこで、ハイパーテキスト・トランスファー・プロトコル・セキュア（HTTPS）が HTTP の拡張機能として導入され、コンピューターネットワークおよびインターネットを介した安全な通信に使用されています。HTTPS は TLS 暗号化で HTTP を強化し、ネットワークデバイス間で交換されるすべてのデータが双方向で暗号化されるようになっています。

これは、PKI（パブリック・キーインフラストラクチャ）と X.509 証明書を使用して、暗号化キーペアを信頼できるデバイス、個人、企業、および Web サイトの ID に添付することで実現されます。HTTPS Web サイトによって提示された証明書が公的に信頼された認証局によって署名されている場合、ユーザーは Web サイトの ID が信頼された第三者によって検証されたことを保証できます。各キーペアには、セキュリティで保護された秘密キーと、任意に配布可能な公開キーが含まれます。秘密鍵はデコーダとして機能し、メッセージの所有者が公開鍵で暗号化したメッセージを復号化するために使います。送信者は、メッセージにデジタル署名する方法として秘密鍵を使用することもできます。インターネット自体は安全ではないネットワークですが、暗号化システムはネットワーク内で安全な接続を確立します。

ほとんどの IoT デバイスにとって、HTTP プロトコルは、余計なデータ量が多く重すぎます。また、リクエスト・リスポンス応答速度は、なかなか高速化できません。**MQTT** は、HTTP に比べはるかに軽量で、オープンで使いやすいクライアント/サーバー・パブリッシュ/サブスクライブ形式のメッセージング・トランスポート・プロトコルです。MQTT は、センサーノードや制約の多い IoT デバイス、低帯域幅、高遅延、または信頼性の低いネットワーク向けに設計されています。MQTT のこういった特性により、M2M（Machine-to-Machine）や IoT デバイス同士の通信など、小さなコードフットプリントが必要な環境や、ネットワーク帯域幅が厳しい環境での使用に最適です。MQTT は TLS をサポートし、実装後はクライアントとブローカー間で完全に通信を暗号化して、移動中のデータをハッカーが傍受するのを防ぎます。

**CoAP** は、制約のある IoT ノードやネットワークで使用するための特別な Web 転送プロトコルです。このプロトコルは、スマートエネルギーやビルディングオートメーションなどの M2M アプリケーション向けに設計されています。CoAP のデータ転送は UDP トランスポートベースで、転送データの保護に DTLS セキュリティ方式を使用します。

## コネクテッドデバイス保護の課題

MQTT と CoAP は両方とも IoT の特殊用途として提案されました。一般的なセキュリティプロトコルをサポートしていますが、正しく保護されていないと簡単に攻撃される可能性があります。これらのプロトコルに基づいたネットワークは、下記に示すセキュリティ脅威に脆弱である点を注意して下さい。

**DDoS 攻撃（ディストリビューテッド・デナイアル・オブ・サービス攻撃）**：サイバー攻撃の最も一般的で破壊的な形態の 1 つで、インターネットのトラフィック洪水をターゲットに引き起こし、ターゲットサーバー、サービス、またはネットワークの通常運用を妨害します。この攻撃が始まると、システムやネットワークがシャットダウンし、許可されたユーザーは、データまたはサービスにアクセスすることが出来ません。この攻撃は通常、ハッカーがネットワーク化された何千ものデバイスを操って、ターゲットサーバーに対してメッセージ送信の一斉攻撃を仕掛ける方法です。この結果、サーバーはその対応にコンピュータリソースを使い果たしハングアップしてしまいます。セキュリティが不十分な IoT デバイスは、こういった DDoS 攻撃の道具として使われることがよくあります。その典型例が、2016 年 10 月にインターネットの大部分がダウンした Dyn サーバー・アッタクです。この時は、セキュリティカメラやデジタルビデオレコーダーなどのネットワークデバイスがハッキングされ攻撃の道具として利用されました。

**TCP SYN フラッド攻撃**：DDoS 攻撃のもう 1 つの形式である TCP SYN フラッドは、クライアントとサーバー間の 3 方向 TCP ハンドシェイクを操作して、未完了の接続ポートオープン要求を出してターゲットサーバーを停止させます。攻撃者は、トランザクションを完了することなく初期接続要求（SYN）パケットを繰り返し送信することにより、ターゲットサーバーで利用可能なすべてのポートを占有し、他への応答を無効化します。（注1）

**Slowloris（スローロリス）攻撃**：さらに別のタイプの DDoS 攻撃である Slowloris は、攻撃者が 1 台のマシンを使用して、ターゲットサーバーに同時に多数の HTTP 要求を開きそれを保持することで、ターゲットサーバーを停止させる攻撃方法です。HTTP は同時接続に使用できるスレッド数に上限が設定されています。ターゲットサーバーはリクエストが完了するまで一定時間待機しますが、攻撃側はリクエスト完了を行わず、同様のリクエストを多発させる手法で、サーバーの最大接続数を埋めてしまいます。これにより、サーバーは新しいサービスに対応できなくなってしまいます。

**安全でない MQTT**：MQTT は本質的に安全ではありませんが、MQTT 接続を保護するためのメカニズムがいくつかあります。例えば、単純なユーザー名とパスワードの組み合わせや TLS などを使って、MQTT 上のメッセージに暗号化されたパイプを設置する方法です。MQTT では、MQTT ブローカーまたはサーバーがセキュリティ制限をかけている場合もあり、またクライアントノードは個別に構成する必要があることに注意して下さい。これだけでもかなり複雑なのですが、センサー機能しかない単純なクライアントでは、セキュリティ機能を実装できるような余

裕すらない場合があります。IoT システム全体のセキュリティを計画するときに、MQTT クライアントのセキュリティ機能をどの程度にするのか十分検討しておく必要があります。

**安全でない CoAP**：CoAP のセキュリティへの懸念事項は MQTT のセキュリティの懸念事項に似ていますが、不適切に CoAP ノードを展開した場合、その影響はより深刻化します。CoAP のサイズや速度のアドバンテージは、DTLS セキュリティ等を追加すると、無くなってしまうので、特定の公開インフラストラクチャは、そういったセキュリティ実装の必要性を無視しています。その結果、インターネット上に数千もの安全でないデバイスが設置されてしまっています。TCP と UDP の違いにより、セキュリティ保護されていない CoAP デバイスは、最大 51,000 倍で DDoS 攻撃に悪用される可能性があります。（注 2）

ここで注意して頂きたいのは、MQTT の問題はプロトコルではなく、多くの MQTT ネットワークで誤ったセキュリティ設定がされているか、もしくはセキュリティなしで動作しているという事実です。特に小規模組織で展開されているスマートホームや IoT ネットワークでは、MQTT 通信を保護するためのセキュリティ実装や構成方法が、顧客や IoT ベンダーまかせになっている場合がよくあります。

パスワード無しの MQTT サーバーがインターネット上で公開されている事例をよく見かけます。こういったサーバーは、ハッカーにとっては関連するスマートホームやビジネスに侵入するための格好の餌食です。さらに、MQTT の 1 対多のサブスクリプションアーキテクチャは、MQTT サーバーへのアクセス権取得はネットワーク内のすべてのデータアクセス権を取得することを意味します。
サイバー犯罪者は、こういった仕様の欠陥や脆弱性を簡単に悪用して、偵察、秘密データの盗難、DDoS 攻撃を行うことができます。

## 脅威が内在するインターネットでの IoT デバイスの保護

多くのリスクが潜み無防備なデバイスを狙うサイバー犯罪者が待ち構えるインターネットへ、IoT 製品を投入するために堅牢なセキュリティを確保することは、経験豊富な開発者がいたとしても多くのマンパワーと十分な開発期間が必要です。組込みデバイスをベースとする IoT 製品に包括的・必要十分なセキュリティ機能を提供するには、複数のプロトコルとセーフガードが必要であり、これらが連携して多層レベルでセキュリティを提供できるソリューションが求められます。

ルネサスは数十年にわたって組込みセキュリティのリーダーであり、今日のコネクテッド製品のセキュリティへの高まるニーズに対応できるベストポジションに立っています。 ルネサスは、組込みセキュリティに対して様々なアプローチでソリューションを提供することが可能です。それは、幅広い組込み製品に対して包括的なセキュリティを提供するための多層的開発インフラストラクチャを提供できるからです。

Renesas Synergy™プラットフォームは、包括的に認定された開発プラットフォームで、Synergy Software Package（SSP）形式の量産可能な品質グレードのソフトウェアやファミリ間展開・シリーズ間ピン互換 MCU が含まれています。これらの MCU には、複数レベルでセキュリティパッケージが提供され、テストプラットフォームで統合され動作テストも完了しています。このような開発環境を提供できる 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の上に構築されることを保証します。

さらに、新しいルネサス RA ファミリの MCU は、Arm Cortex-M コアとルネサスのクラス最高の組込みシステム周辺機能 IP を組合わせて、プラットフォームの柔軟性を高めたオプションを提供します。RA のフレキシブルソフトウェアパッケージ（FSP）は、FreeRTOS 上に構築され、最適化された HAL ドライバー、ベースラインソフトウェアプラットフォーム、および関連ミドルウェアの構成で提供されます。FSP は柔軟性を重視した設計により、開発ユーザーは、各種ミドルウェアと必要なライブラリを簡単に自分のシステムに組込むことができます。

Synergy プラットフォーム MCU と RA MCU は、Secure Crypto Engine（SCE）と呼ばれる統合暗号サブシステムが組込まれています。SCE は、業界標準の暗号化アルゴリズム、キー生成、そして True Random Number Generator（TRNG）のためのハードウェアアクセラレータです。さらに、Synergy プラットフォームと RA FSP のどちらも、PKI（パブリック・キー・インフラストラクチャ）をサポートしています。

ユーザー開発環境においては、開発プラットフォームは簡単・安全にクラウド接続できる必要があります。Synergy SSP は、組込み MQTT および TLS モジュールを使用してクラウド接続をサポートし、Synergy クラウド接続アプリケーションは、Amazon Web Services（AWS）、Google Cloud、Microsoft Azure などの主要クラウド環境への安全な組込み接続を提供します。RA FSP も同様の機能を提供し、Arm エコシステムソフトウェアが活用できます。

## 結論

IoT デバイスソリューションに包括的かつ緻密なセキュリティを提供するには、複数レベルで防衛可能な連携型統合テクノロジーが必要です。ルネサスは、デバイス、サービス、およびネットワークを深層レベルまで保護できるさまざまなソリューションを提供することにより、IoT デバイスを保護するという課題に取り組む組込み開発ユーザーを支援します。

詳しい情報は、当社のウェブサイトをご覧ください。

## 参考資料


[1] Hacked Cameras Were Behind Friday's Massive Web Outage

[2] In-the-Wild DDoSes Use New Way to Achieve Unthinkable Sizes

[3] RA Family of 32-bit Arm Cortex-M MCUs
RX Family of 32-bit MCUs
Synergy Platform of 32-bit Arm Cortex-M MCUs + qualified software