産業オートメーション機器におけるセキュリティ技術動向

― RA Family / RX Family / RZ Family と Security ソフトウェアスタック実装アプローチ ―

古城 隆, wolfSSL Japan 合同会社, 技術統括

小関 敬祐, Staff Engineer, Functional Safety & Security Core Tech/EP Core Technologies, Renesas Electronics Corporation

1. はじめに

産業オートメーション機器を取り巻く環境は大きく変化しています。従来は閉域ネットワークでの運用が前提でしたが、近年はクラウド連携や遠隔監視の普及により、外部ネットワーク接続を前提とした設計が求められています。これに伴い、セキュリティの対象は通信、起動、更新、鍵管理を含む製品ライフサイクル全体へ広がっています。さらに、欧州の Cyber Resilience Act（CRA）、日本の JC-STAR、米国の U.S. Cyber Trust Mark といった各国のサイバーセキュリティ対策の制定に伴い、組込み機器においても設計・開発段階から市場投入、更には EoL までライフサイクル全体で幅広いセキュリティ設計の配慮が強く求められるようになっています。加えて、PQC (Post-Quantum Cryptography) への移行という暗号技術の世代交代も進みつつあり、10 年から 20 年といった長期運用が求められる産業用途機器では、将来の暗号リスクを見据えた開発・設計が求められています。しかし実際には、多くの産業機器において以下の課題が顕在化しています：

- OTA 未実装により、出荷後の脆弱性対応が困難
- デバイス認証や証明書管理が個別実装で破綻しやすい
- CRA など新規制への対応コストが増大
- 長期運用を前提とした暗号更新の設計が不足

これらの課題は、出荷後に顕在化した場合、製品回収やサービス停止といった大きなビジネスリスクにつながる可能性があります。本稿では、主に PLC、産業用ロボット、ゲートウェイなど産業機器に求められるセキュリティ要件を整理し、リスク低減、認証コスト削減、市場投入スピードの加速を軸に、Renesas の RA/RX/RZ Family と wolfSSL 社の wolfSSL / wolfBoot などのセキュリティソフトウェアスタックを組み合わせた実装アプローチについて解説します。

2. 産業オートメーション機器を取り巻く環境

2.1 閉域ネットワーク前提からの転換

従来の産業機器は、工場内の閉じたネットワークで運用されることが一般的であり、外部からのサイバー攻撃リスクは限定的であると考えられてきました。しかし近年では、クラウド接続、遠隔監視・保守、装置の分散配置などの要因により、ネットワーク環境の前提そのものが変化しています。これにより、産業機器もインターネットに直接または間接的に接続される存在となり、サイバー攻撃の対象となる可能性が高まっています。

2.2 装置内・非接続環境への拡張

セキュリティ対策が必要なのは、ネットワーク通信だけではありません。装置内のユニット間通信、USB や SD カードを使った保守経路、ファームウェアの不正書き換えなども重要な攻撃経路となり得ます。
そのため、ネットワーク接続の有無にかかわらず、機器単体として信頼性を確保できる設計が求められています。

2.3 規制・認証・調達要件の変化

近年、各国・各地域でインターネットに直接的・間接的に接続する組込み機器に対するセキュリティ規制やセキュリティ評価・表示制度（ラベリング制度）の整備が進んでいます。これらは、出荷時点の安全性だけでなく、出荷後の更新や脆弱性対応を含む継続的なセキュリティ確保を重視している点が特徴です。

欧州 CRA

欧州 **CRA（Cyber Resilience Act）**は、デジタル要素を持つ製品に対する包括的なサイバーセキュリティ規制です。欧州市場で流通するデジタル製品の安全性を高めるとともに、製品ライフサイクル全体を通じて安全性を維持し、利用者がそのセキュリティ特性を把握しやすくすることを目的としています。

CRA では製造ベンダに対して、リスク評価に基づく以下のような要求が課されます。

- セキュア・バイ・デザイン／デフォルト

- 製品出荷時に既知の脆弱性を残さないこと
- 脆弱性ハンドリング体制
- 安全なセキュリティ更新
- 技術文書・適合性評価
- サポート期間の明示
- 重大インシデントと悪用中の脆弱性の報告

これらの要件が示すように、CRA は出荷時の安全性だけでなく、製品の想定使用期間を通じて脆弱性を管理し、安全に修正・更新を継続できることを求めており、製品アーキテクチャと運用体制の両方に影響します。そのため、産業機器においても、起動時の真正性確認（セキュアブート等）、安全なソフトウェア更新（OTA 等）、デバイス認証、アクセス制御、鍵・証明書の管理、長期的な脆弱性対応を含む製品ライフサイクル全体を意識したセキュリティ設計が重要になります。

こうした要件は、顧客の調達条件やサプライチェーン要求、セキュリティ監査にも反映されつつあります。

日本 JC-STAR

日本では、**JC-STAR**（Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements）が、IoT 製品のセキュリティ機能を共通基準で評価・可視化するラベリング制度として運用されています。本制度は、ETSI EN 303 645 や NISTIR 8425 などと整合しつつ、インターネットと通信可能な幅広い IoT 製品を対象に、調達者や利用者が製品のセキュリティ水準を把握しやすくすることを目的としています。

JC-STAR は、単に暗号機能の有無を評価する制度ではなく、初期設定、更新、認証・アクセス制御、脆弱性対応、廃棄時の配慮など、製品ライフサイクル全体のセキュリティを重視しています。適合基準は★1～★4 の 4 段階で構成され、★1 は製品共通の最低限の要件、★2～★4 は製品類型や利用用途に応じたより高い要件です。★1・★2 は自己適合宣言、★3・★4 は第三者評価を前提とし、適合製品には QR コード付きラベルが付与されます。JC-STAR は日本国内の制度ではありますが、その考え方は欧州 CRA や U.S. Cyber Trust Mark とも共通点が多く、また、政府調達や民間調達での活用、海外制度との相互承認も視野に入れており、今後は国内の調達要件やサプライチェーン要求への影響がさらに広がる可能性があります。

米国 U.S. Cyber Trust Mark

米国では、**U.S. Cyber Trust Mark** が、無線対応のコンシューマ IoT 製品を対象とするサイバーセキュリティラベリング制度として整備が進められています。製品のセキュリティ機能を可視化し、安全な IoT 製品を市場で識別しやすくすることを目的とし、ラベルは QR コードと組み合わせて、サポート期間、ソフ

トウェア更新やセキュリティパッチの提供状況などの詳細情報を確認できる仕組みも検討されています。制度の基準は、NISTIR 8425 に基づくベースライン要件を土台としており、認証、更新、データ保護、セキュア通信、脆弱性開示などが重視されています。製品ライフサイクル全体で継続的にセキュリティを管理するという考え方は、CRA や JC-STAR と共通しています。本制度は、現時点では産業機器を直接の対象としていませんが、「インターネットに直接的・間接的に接続する組込み機器には継続的セキュリティ管理が必要である」という方向性を市場全体に示す制度として重要な意味を持っており、今後の調達要件や市場要求として波及する可能性があります。

2.4 規制が求める実装要件

欧州の CRA、日本の JC-STAR、米国の U.S. Cyber Trust Mark は、制度や対象市場は異なるものの、いずれも製品ライフサイクル全体でのセキュリティ確保、出荷後の脆弱性対応、安全な更新、デバイス認証・識別、セキュリティ情報の可視化と説明責任などを重視している点で共通しています。

産業機器で特に重要となる実装要件は次のとおりです。

- 起動時の真正性確認（セキュアブート等）
- 安全なソフトウェア更新（OTA 等）とロールバック防止
- デバイス認証、アクセス制御、鍵・証明書のライフサイクル管理
- 脆弱性対応体制、ログ取得、インシデント対応
- 長期サポートとセキュリティ情報の管理・提示

重要なのは、これらを個別の機能としてではなく、相互に連携するアーキテクチャとして設計することです。具体的には、セキュアブート、TLS/DTLS、デバイス認証、OTA、鍵管理などが一体となって機能する必要があります。また、SBOM、サプライチェーン管理、長期的な脆弱性監視、インシデント報告義務など、設計・調達から出荷後の運用・保守に関わる要求も強まっています。

3. 新しい脅威とセキュリティ技術の変化

3.1 長期運用と暗号寿命

産業機器は、10 年から 20 年といった長期間で運用されるため、現在は安全とされている暗号方式であっても、将来的には計算能力や解析技術の進歩によって、安全性を維持できなくなる可能性があります。そのため、セキュリティ設計では、特定の暗号アルゴリズムに依存せず、将来的に暗号方式を変更可能な構造を備えておくことが重要となります。

TLS をはじめとするセキュリティプロトコルでは、この課題に対応するため、設計段階からアルゴリズムの柔軟性（Crypto-agility）が考慮されています。例えば、以下のような仕組みにより、新しい暗号方式への移行を可能としています。

- 暗号スイート（Cipher Suite）によるアルゴリズムの組み合わせ選択
- 鍵交換方式、署名方式、ハッシュ関数の切り替え
- プロトコルバージョンの更新（TLS 1.2 から TLS 1.3 への移行 など）

一方、産業機器では、暗号スイートの固定化や鍵・証明書更新機能の未実装、ファームウェア更新の制約などにより、この柔軟性を十分に活用できていないケースもあります。このような設計では、長期運用中にセキュリティリスクが顕在化する可能性があります。そのため、長期運用と暗号寿命を考慮し、以下の要素をあらかじめ組み込むことが重要です。

- 鍵ローテーションおよび証明書更新の仕組みの実装
- セキュアなファームウェア更新（OTA）による機能拡張
- 暗号アルゴリズムの将来更新を前提とした設計
- プロトコルバージョンおよび暗号スイートの柔軟な選択

さらに、量子計算機の発展を見据え、PQC (Post-Quantum Cryptography) への移行も重要な検討事項となります。これは単なる暗号アルゴリズムの置き換えではなく、鍵サイズの増大や計算特性の変化を考慮した、システム設計全体の見直しを伴うものです。

暗号技術は固定的なものではなく、時間とともに変化することを前提に設計する必要があり、特に長期間運用される産業機器においては、新たな脅威へ継続的に対応できる設計そのものが、セキュリティの重要な要素となります。

3.2 PQC

PQC（Post-Quantum Cryptography）は、量子コンピュータによる攻撃に対しても安全性を維持することを目的とした暗号方式群です。従来の公開鍵暗号（RSA や楕円曲線暗号）は、量子アルゴリズム（特に Shor のアルゴリズム）により効率的に解読される可能性が指摘されており、長期的な安全性に課題があるとされています。これに対し PQC は、格子問題やハッシュベース署名など、現時点で量子計算機でも効率的に解くことが困難と考えられている数学問題に基づいて設計されています。

PQC アルゴリズムの標準化動向

PQC はすでに研究段階を超え、標準化と実装のフェーズに移行しています。米国国立標準技術研究所（NIST）は、長年にわたる選定プロセスを経て、以下のアルゴリズムを標準として策定しました。

- ML-KEM（旧 Kyber）：鍵共有・鍵カプセル化（KEM）

- ML-DSA（旧 Dilithium）：格子ベースデジタル署名
- SLH-DSA（旧 SPHINCS+）：ステートレス階層ハッシュベースデジタル署名

これらは、それぞれ NIST FIPS 203、204、205 として標準化されており、すでに実装・評価が進められています。また、これら以外の PQC アルゴリズムについても、標準化に向けた検討が引き続き進められています。

既存プロトコルへの適用（TLS など）

PQC は単独利用だけでなく、TLS など既存のセキュリティプロトコルへの統合も進んでいます。従来方式を一度に置き換えるのではなく、従来アルゴリズムの鍵長を引き上げて安全性を補強しつつ、鍵交換では ECDHE と ML-KEM、署名では ECDSA と ML-DSA を組み合わせたハイブリッド構成を導入することで、既存システムとの互換性を維持しつつ、量子耐性を段階的に付加する構成が採用されつつあります。この考え方は、TLS の複数共有秘密の結合、証明書の複数署名（ハイブリッド証明書）、ファームウェア署名における二重署名などに展開されており、既存システムとの互換性を保ちながら段階的に PQC を導入できる仕組みとして注目されています。

3.3 証明書および PKI の対応状況

PQC の導入は、通信プロトコルだけでなく、証明書や PKI 基盤にも影響を及ぼします。現在の X.509 証明書では、新しい署名アルゴリズム（ML-DSA など）の OID 定義に加え、鍵サイズや証明書チェーン全体のサイズ増大といった課題があります。このため、従来署名と PQC 署名を併用するハイブリッド証明書や、中間証明書での段階的移行、プロトコルレベルでのサイズ最適化といった対応が進められています。特に産業機器では、通信帯域、フラッシュ容量、起動時間への影響を考慮した設計が必要になります。

証明書・鍵管理の高度化

従来の産業機器における鍵管理は、単一の共有鍵や固定証明書に依存する比較的単純な構成が一般的でした。しかし、クラウド接続や長期運用、規制対応が求められる現在では、こうした単純なモデルでは対応が難しくなっています。そのため、以下のような高度な証明書・鍵管理が求められています。

証明書チェーンによる信頼モデル

従来は、単一の公開鍵や自己署名証明書に依存する構成も多く見られましたが、現在では、ルート CA（Root of Trust）、中間 CA（発行と運用の分離）、デバイス証明書から成る階層型の信頼モデルが導入されはじめています。この構造により、ルート鍵の長期保護、中間鍵のローテーション、デバイス単位で失効管理が可能になります。産業機器においては、特に製造時に書き込まれるルート信頼アンカーと、運用中に更新される証明書を分離して管理することが重要です。

デバイス固有鍵（Device Identity）

近年では、すべてのデバイスが一意の鍵を持つことが前提となっています。これにより、デバイス単位での認証が可能になるだけでなく、不正機器の排除やトレーサビリティの確保にもつながります。実装面では、製造時に鍵を生成・書き込む、あるいはチップ内でユニークな鍵値を生成したうえで、これをハードウェア Root of Trust に格納し、鍵を外部に出すことなく署名や復号処理を実行できる構成が重要になります。

鍵ローテーションとライフサイクル管理

鍵は一度設定して終わりではなく、ライフサイクル全体を通じて管理する必要があります。具体的には、定期的な証明書更新に加え、鍵漏洩時の迅速な置き換えや、RSA から ECC、さらに PQC へといったアルゴリズム更新も見据えた運用が求められます。これを実現するには、OTA による証明書更新機構、セキュアストレージによる鍵保護、更新失敗時のロールバック制御などを組み合わせた仕組みが重要になります。

4. 産業機器に求められる基本セキュリティ要件

産業機器に求められるセキュリティは、通信の保護、起動の保護、更新の保護、鍵の保護、脆弱性対応の 5 つの観点で整理できます。

4.1 通信の保護

- TLS/DTLS による暗号通信
- 認証および完全性の確保

通信の保護は、外部ネットワークと接続される産業機器において最も基本的な要件です。TLS/DTLS により通信の機密性（盗聴防止）と完全性（改ざん検出）を確保するとともに、サーバ認証やクライアント認証により通信相手の正当性を確認します。特に産業用途では、装置同士の相互認証（mTLS）や、長期運用を前提とした証明書管理が重要となります。また、暗号スイートやプロトコルバージョンを柔軟に更新できる設計（crypto-agility）も求められます。

4.2 起動の保護

- セキュアブート
- ファームウェアの真正性確認

起動の保護は、機器が「正しい状態で動き始めること」を保証する仕組みです。セキュアブートにより、起動時にファームウェアの署名を検証し、改ざんされたコードの実行を防ぎます。このとき、信頼の起点

となるルート鍵（Root of Trust）をハードウェア内に保持し、検証処理をソフトウェアから切り離すことが重要です。これにより、攻撃者がソフトウェアを書き換えた場合でも、不正な起動を防止できます。

4.3 更新の保護

- セキュア OTA
- ロールバック防止

産業機器では、脆弱性対応や機能改善のためにファームウェア更新が不可欠です。セキュア OTA（Over-The-Air）により、遠隔から安全に更新を配布・適用できる仕組みを構築します。更新データには署名を付与し、適用前に検証を行うことで、改ざんされたファームウェアの導入を防ぎます。古い脆弱なバージョンへの巻き戻し（ロールバック）を防止するため、バージョン管理やカウンタを用いた制御も重要です。

4.4 鍵の保護

- 安全な鍵格納
- ライフサイクル管理

鍵はセキュリティの根幹となる資産であり、その保護は極めて重要です。デバイス固有鍵や証明書秘密鍵は、ソフトウェアから直接参照できない形でハードウェア内に安全に格納し、外部に漏洩しないよう保護します。鍵は製造時の生成・書き込みから、運用中の更新・失効、廃棄に至るまでライフサイクル全体で管理する必要があります。長期運用を前提とする産業機器では、鍵ローテーションやアルゴリズム更新への対応も重要な設計要素となります。

4.5 脆弱性対応

- 更新体制
- インシデント対応

近年の規制では、製品出荷後の脆弱性対応能力が強く求められています。脆弱性が発見された際に、迅速に修正パッチを提供し、安全に適用できる体制が必要です。また、インシデント発生時には、ログ取得や状態確認、影響範囲の特定ができる仕組みも重要になります。単にアップデート機能を持つだけでなく、「継続的に安全性を維持する運用能力」そのものがセキュリティ要件の一部となっています。

重要なのは、これらを個別機能ではなく相互に連携した仕組みとして設計することです。たとえば、セキュアブートで信頼できるソフトウェアを起動し、TLS で安全に通信し、OTA で安全に更新し、鍵管理でその基盤を支えるといった一連の流れで機能する必要があります。

また、脆弱性対応は製品メーカー単独の取り組みだけで完結するものではなく、採用するソフトウェアコンポーネントのサプライヤによる継続的なサポート体制も重要になります。例えば wolfSSL は、CRA への全面対応を発表しており、長期的な脆弱性管理、CVE 対応、構造化された脆弱性レポート受付、協調的な開示プロセス、長寿命製品向けの保守オプションを提供する方針を示しています。これにより、製品メーカーは自社製品のライフサイクル全体にわたるセキュリティ維持を、ソフトウェアスタックのサポート体制と組み合わせて実現しやすくなります。産業機器のセキュリティは、単一の機能ではなく、システム全体として成立するアーキテクチャ、体制として捉えることが重要です。

5. 実装モデル

本章では、産業オートメーション機器における今後のセキュリティ実装モデルを、ハードウェアセキュリティ機能とソフトウェアスタックの観点から整理します。

5.1 ハードウェア実装モデル

実装モデルの進化

従来の組み込み機器では、ハードウェアセキュリティ機能は主に暗号処理を高速化するハードウェアアクセラレータとして提供されてきました。これは処理負荷の軽減には有効でしたが、鍵の生成・書き込み・更新を信頼の起点として一貫管理する仕組みは限定的でした。しかし、システム全体の信頼性は、鍵をどのように保護し制御できるかに大きく左右されます。セキュアブート、更新時の正当性確認、デバイス認証などにおいて、前提となる鍵が信頼できなければ十分な安全性を確保できません。このため近年では、暗号処理の高速化だけでなく、鍵を Root of Trust として確立し、ソフトウェアと連携してシステム全体のセキュリティを実現することが求められています。

Renesas の RA/RX/RZ Family に搭載しているセキュリティエンジン(RSIP/TSIP/SCE)*は、単なる暗号アクセラレータではなく、鍵の安全な生成・書き込み・更新の支援、Root of Trust の基盤を提供するセキュリティ機構を実現しており、外付けセキュリティ部品を追加することなく、 統合的なセキュリティ機能を実装可能です。

Renesas セキュリティエンジンは、主に以下の機能を提供します。

- Root of Trust
- 鍵の安全な管理（生成・書き込み・更新）
- ハードウェア暗号処理
- ライフサイクル管理を支える基盤機能

これにより、設計負荷の低減、BOM コストの削減、消費電力の最適化を図りながら、 産業機器に求められる高度なセキュリティ要件を効率的に満たすことができます。これらの基盤機能をソフトウェアと組み合わせることで、セキュアブート、認証、通信保護、ソフトウェア更新、鍵ライフサイクル管理といったシステムレベルのセキュリティを実現できます。その結果、ハードウェアとソフトウェアの協調により、製品全体として一貫した信頼性を確保することが可能となります。

＊RSIP：Renesas Secure IP, TSIP：Trusted Secure IP, SCE：Secure Crypto Engine

Root of Trust の確立

Renesas のセキュリティエンジンは、デバイス内に信頼の起点（Root of Trust）を提供します。これは、デバイス固有の鍵や識別情報を保護し、それらを信頼の基盤として利用できるようにするものです。この Root of Trust により、起動時のファームウェア検証、デバイス固有 ID や鍵に基づく認証、セキュアな鍵導出などの処理における信頼の基盤を確立できます。

鍵の安全な管理

Renesas のセキュリティエンジンでは、平文鍵を外部に露出させることなく利用することができます。鍵はハードウェア固有鍵で保護された状態で格納され、暗号処理もセキュリティエンジン内部で完結します。このような仕組みにより、鍵の読み出しやコピーの防止、鍵の露出リスクの低減、ソフトウェア侵害時の影響範囲の限定、サイドチャネル攻撃に対する耐性向上などといった効果が期待できます。

ハードウェア暗号処理

Renesas のセキュリティエンジンは、AES、RSA、ECC などの暗号処理をハードウェアで実行する機能を備えています。これにより、ソフトウェアのみで暗号処理を実装する場合と比べて、高速な暗号処理、CPU 負荷の軽減、消費電力の低減、タイミング攻撃などに対する耐性向上といった利点が得られます。さらに、wolfSSL などのソフトウェアスタックと連携することで、TLS 通信における鍵操作や暗号処理を安全かつ効率的にオフロードすることが可能になります。

ライフサイクル管理の支援

Renesas のセキュリティエンジンは、製造から運用、廃棄までのライフサイクル全体を通じたセキュリティ運用を支える基盤です。鍵をハードウェア側で安全に扱うことで、製造時の鍵書き込みやプロビジョニング、運用中の鍵更新、廃棄時の機密情報消去といった対策をハードウェアレベルで実装することが可能です。このように、Renesas のセキュリティエンジンは、単なる暗号アクセラレータではなく、Root of Trust を中核に、製品ライフサイクル全体を通じた継続的なセキュリティを支える基盤として位置づけられます。

5.2 ソフトウェア実装モデル

ハードウェア Root of Trust や暗号アクセラレータは、鍵の保護や暗号処理の安全性を高める上で重要な役割を果たします。一方で、実際の製品においては、通信プロトコル、証明書処理、ファームウェア検証、OTA 更新制御などをソフトウェアとして実装する必要があります。

産業機器のセキュリティ実装では、ハードウェアセキュリティ機能とソフトウェアスタックを適切に組み合わせることが重要です。

wolfSSL 社および製品概要

wolfSSL 社は、組み込み機器および IoT 向けのセキュリティソフトウェアを提供するネットワークセキュリティ専門ベンダです。同社は、サイズ、速度、移植性、標準準拠を重視した組み込み向けセキュリティライブラリを提供しており、技術サポートやコンサルティングも行っています。

wolfSSL 社の代表的な製品として、TLS/DTLS 通信を実現する **wolfSSL**、およびセキュアブートとファームウェア更新を実現する **wolfBoot** があります。関連製品として、wolfSSH、wolfMQTT、wolfTPM、wolfHSM なども用意されており、リモートアクセス、軽量メッセージ通信、TPM 連携、鍵管理基盤を補完します。これらのコンポーネントを組み合わせることで、通信、認証、デバイス管理、セキュアストレージ、ライフサイクル管理を含む、統合的なセキュリティアーキテクチャを構築することが可能になります。これらは、リソース制約のあるマイコン環境や RTOS 環境を想定して設計されており、産業機器、IoT 機器、車載、医療機器など、長期運用が求められる分野で利用されます。

本稿において、wolfSSL/wolfBoot は、Renesas の RA/RX/RZ Family に搭載されているセキュリティエンジンと連携して、通信、起動、更新、鍵管理を統合的に実装するためのソフトウェアスタックとして位置付けられます。

wolfSSL：TLS/DTLS、証明書、PQC、セキュリティエンジン連携

wolfSSL は、組み込みシステム向けに設計された軽量な SSL/TLS ライブラリです。C 言語で実装され、組み込み、RTOS、リソース制約環境を対象としており、TLS/DTLS によるセキュア通信を実現します。

産業機器における wolfSSL の主な役割は、外部システムやクラウド、保守端末、装置間通信に対して、安全な通信経路を提供することです。具体的には、次のような機能を担います。

- TLS/DTLS による暗号通信
- サーバ／クライアント認証
- X.509 証明書検証
- mTLS による装置間・デバイス対クラウド認証
- 暗号スイートやプロトコルバージョンの柔軟な選択

- PQC およびハイブリッド鍵交換への対応
- ハードウェア暗号アクセラレータとの連携

特に産業機器では、通信相手がクラウドサービスだけでなく、保守端末、ゲートウェイ、他の制御機器など多岐にわたります。そのため、単に通信を暗号化するだけでなく、証明書を用いて通信相手を確認し、不正な機器やサーバとの接続を防ぐことが重要です。

また、長期運用される産業機器では、暗号アルゴリズムや証明書の更新が必要になる場合があります。wolfSSL のような TLS スタックを用いることで、プロトコルバージョン、暗号スイート、証明書検証方式をソフトウェアとして更新・拡張でき、Crypto-agility を確保しやすくなります。

さらに、PQC への移行を見据えた場合、TLS におけるハイブリッド鍵交換や PQC 署名アルゴリズムの導入が重要になります。wolfSSL は PQC 対応を進めており、既存の TLS/DTLS 通信基盤に対して、将来的な暗号方式の拡張を行うための選択肢となります。

Renesas セキュリティエンジンと連携する構成では、秘密鍵や暗号処理をできるだけハードウェアに委譲し、wolfSSL は TLS プロトコル処理、証明書処理、セッション管理を担います。このような構成により、ハードウェアレベルで鍵を安全に保護しつつ、TLS クライアント認証や暗号通信を実現することが可能になります。

wolfBoot：セキュアブート、署名検証、OTA、ロールバック防止

wolfBoot は、組み込みシステム向けのセキュアブートローダであり、ファームウェア認証とファームウェア更新機構を提供するポータブルなセキュアブートローダとして位置付けられています。
産業機器における wolfBoot の主な役割は、以下の通りです。

- 起動時のファームウェア署名検証
- 改ざんされたファームウェアの実行防止
- 署名付きファームウェア更新の適用
- OTA または任意の通信経路による更新への対応
- 更新失敗時の復旧制御
- ロールバック防止
- 複数鍵や鍵更新を見据えた検証構成

wolfBoot は、起動時およびファームウェア更新受信時に署名を検証し、信頼できるファームウェアだけを実行対象とします。検証または認証できないイメージは起動しません。

また、産業機器では、脆弱性修正や機能改善のために、出荷後もファームウェアを安全に更新できることが重要です。更新時には、受信したファームウェアが正当な署名を持ち、改ざんされておらず、既知の脆

弱性を含む旧版へ戻らないことを確認する必要があります。wolfBoot は、OTA を含む任意の転送経路で受信したファームウェアの署名を検証し、バージョン情報に基づくロールバック防止にも対応します。これにより、CRA や JC-STAR などが求める安全な更新、脆弱性対応、出荷後のセキュリティ維持を支える実装基盤となります。

Renesas 製セキュリティエンジンとの役割分担

Renesas の**セキュリティエンジン**と **wolfSSL / wolfBoot** を組み合わせる場合は、ハードウェアとソフトウェアの責務分担が重要です。具体的にはセキュリティエンジン(ハードウェア)とソフトウェアの連携をすることで、長期運用サポート、CRA 対応の現実解に繋がります。

セキュリティエンジンでは、主に以下を担います。

- Root of Trust の提供
- 秘密鍵やデバイス固有鍵の保護
- 暗号演算のハードウェア実行
- 鍵導出や鍵利用の制御
- ライフサイクル管理の支援

一方、wolfSSL / wolfBoot は、主に以下を担います。

- TLS/DTLS プロトコル処理
- 証明書検証と通信相手認証
- セキュアブートの制御
- ファームウェア署名検証
- OTA 更新フローの制御
- ロールバック防止
- 暗号アルゴリズムやプロトコルの将来更新

この構成では、秘密鍵は可能な限りセキュリティエンジン内でのみ扱い、wolfSSL / wolfBoot は必要な暗号操作をハードウェア機能として利用します。これにより、秘密鍵をソフトウェアから直接扱わない設計が可能になります。具体的には、通信時は wolfSSL が TLS/DTLS と証明書検証を担当し、起動・更新時は wolfBoot が署名検証、バージョン確認、ロールバック防止を制御します。Renesas セキュリティエンジンは各場面で鍵保護と暗号処理を担い、運用中も製品ライフサイクル全体の信頼基盤となります。

このように、Renesas セキュリティエンジンは信頼の基盤として鍵と暗号処理を保護し、wolfSSL / wolfBoot はその上で通信・起動・更新の具体的なセキュリティ機能を実装します。その結果、産業機器に

求められる通信、起動、更新、鍵保護、脆弱性対応を統合的なセキュリティアーキテクチャとして実現できます。

5.3 運用・コンプライアンス支援モデル

CRA をはじめとする近年のセキュリティ規制では、製品にセキュリティ機能を実装するだけでなく、出荷後も継続的に脆弱性を管理し、必要に応じて修正を提供し、その対応状況を説明できることが求められます。したがって、産業機器のセキュリティ実装では、通信、起動、更新、鍵管理といった技術機能に加えて、運用・保守・文書化を含めたコンプライアンス支援体制も重要になります。

wolfSSL は、2026 年 3 月に欧州のサイバーレジリエンス法（CRA）への全面対応を発表し、同社製品を通じてコネクテッドデバイスおよび組み込み機器向けの CRA セキュリティ要件を支援する方針を示しています。発表では、CRA が求めるセキュアな開発プロセス、脆弱性管理、市場投入後の保守責任に対して、wolfSSL の組み込み向けセキュリティコンポーネントと長期サポートにより対応することが説明されています。

具体的には、wolfSSL は以下のような領域で CRA 対応を支援します。

セキュア通信およびデータ保護

TLS 1.3／DTLS 1.3 による通信データの暗号化、認証付き暗号、最新の暗号スイート、リソース制約環境に適した構成オプションを提供します。

強固な暗号技術とセキュアな鍵管理

AES、RSA、ECC、EdDSA、PQC アルゴリズムを含む暗号プリミティブに対応し、セキュアエレメント、TPM、HSM などのハードウェアベースの鍵保護との統合を支援します。また、規制対象市場向けに FIPS 140-3 認証済み暗号モジュールも提供しています。

ファームウェア整合性とセキュアブート

wolfBoot により、起動時のファームウェア検証、OTA を含む認証済みファームウェア更新、ロールバック保護を支援します。これにより、不正または脆弱なファームウェアの実行を防ぐ基盤を提供します。

脆弱性管理および協調的な開示

CRA では市場投入後の保守が重要な柱となります。wolfSSL は、構造化された脆弱性レポートの受付、協調的な開示プロセス、CVE 追跡、迅速な修正支援、長寿命製品ライフサイクルに合わせた保守オプションを提供します。

透明性および SBOM 対応

CRA では、サプライチェーンの透明性と脆弱性追跡のため、ソフトウェア部品表（SBOM）の維持が重視されます。wolfSSL は、外部依存を最小限に抑えたソフトウェアコンポーネント、明確なコンポーネントトレーサビリティ、セキュアな構成とライフサイクルメンテナンスを支援する文書化を通じて、SBOM ベースのコンプライアンスを支援します。

このように、wolfSSL / wolfBoot は、暗号通信やセキュアブートといった個別機能を提供するだけでなく、CRA で求められる製品ライフサイクル全体のセキュリティ維持を支援するソフトウェア基盤として位置付けられます。Renesas セキュリティエンジンと組み合わせることで、通信、起動、更新、鍵管理、脆弱性対応、文書化を含む統合的なセキュリティアーキテクチャを構築しやすくなります。

6. 将来動向とまとめ

産業オートメーション機器に求められるセキュリティは、今後さらに高度化・長期化していくと考えられます。従来は通信の暗号化や固定鍵による認証、出荷時の安全性確保が中心でしたが、今後は長期運用、クラウド連携、OTA 更新、規制対応を含め、運用期間全体で安全性を維持する仕組みが求められてきています。今後重要になると考えられる技術動向として、証明書チェーン化、遠隔アテステーション、PQC 対応などが挙げられます。

6.1 証明書チェーン化と信頼モデルの高度化

今後は、認証モデルとして、ルート CA、中間 CA、デバイス証明書による階層型の信頼モデルが一般化すると考えられます。これにより、デバイス単位での認証、証明書失効管理、鍵ローテーション、サプライチェーン単位での管理が可能になります。また、製造時に書き込まれる Root of Trust と、運用中に更新される証明書・鍵を分離して管理する構成も重要です。この信頼モデルは、通信認証に加え、OTA 更新、デバイス管理、クラウド連携、遠隔保守を支える基盤となります。

6.2 遠隔アテステーション

遠隔アテステーションは、「正しいデバイスであること」に加え、「現在も正しい状態で動作していること」を外部から確認する仕組みとして注目されています。起動時に検証されたファームウェア情報、ソフトウェア構成、デバイス識別情報などを署名付きで提示することで、クラウド側は健全性確認や改ざん機器の排除、不正ファームウェアの検出、ゼロトラスト型のアクセス制御を行えます。近年は、DICE（Device Identifier Composition Engine）や EAT（Entity Attestation Token）など軽量機器向け技術の整備も進んでおり、セキュアブートで構築した信頼チェーンを通信やクラウド連携に拡張する流れが広がっています。

6.3 PQC 対応と暗号移行

量子コンピュータの発展に伴い、PQC への移行も重要な課題となります。現在は、TLS におけるハイブリッド鍵交換や PQC 署名アルゴリズム、ハイブリッド証明書などの実装・評価が進められています。
一方で PQC 導入はアルゴリズム置き換えだけではなく、鍵・証明書サイズ、通信量、メモリ使用量への影響を伴います。そのため、産業機器では通信帯域、フラッシュ、RAM、起動時間、消費電力を含めた最適化と、crypto-agility を前提とした設計が重要です。量子計算機の実用化時期には不確実性がある一方、「現在取得された暗号化通信を将来復号する」いわゆる **Harvest Now, Decrypt Later** のリスクも指摘されています。そのため、長期保護が必要な産業システムでは、今後 PQC 移行(crypto-agility)を前提とした設計が重要になると考えられます。

6.4 統合型セキュリティアーキテクチャへの進化

今後の産業機器では、通信、起動、更新、鍵管理、デバイス認証、アテステーション、脆弱性対応を個別に実装するのではなく、統合的なセキュリティアーキテクチャとして設計することが重要です。特に、ハードウェア Root of Trust、セキュアブート、TLS/DTLS、OTA、証明書管理、アテステーション、PQC などを連携させ、製品ライフサイクル全体を通じて継続的に信頼性を維持できる構成が求められます。このように、今後の産業オートメーション機器では、「出荷時に安全」ではなく、「運用期間を通じて継続的に信頼できる」ことを実現する統合型セキュリティアーキテクチャがますます重要になっていくと考えられます。

Renesas および wolfSSL は、本稿で紹介したセキュリティアーキテクチャを評価可能なリファレンス実装および評価キットを提供しています。具体的な設計や適用については、担当営業または Web フォームよりお問合せください。

wolfSSL 社について

wolfSSL Inc.は、スピード、サイズ、移植性、機能、標準への準拠にこだわった組み込み向けセキュリティライブラリを提供するネットワークセキュリティ専門ベンダです。セキュリティライブラリを製品として提供するほか、技術サポートやコンサルティングも行っています。

自社の専門エンジニアが独自開発した SSL/TLS 製品と暗号ライブラリは、政府機関、自動車、航空宇宙などの高度なセキュリティデザインをサポートします。航空宇宙では RTCA DO-178C レベル A 認証、車載向けでは MISRA-C をサポートしており、2004 年の創業以来世界各国で 2,000 社を超えるカスタマーに採用されています。

また、2024 年 7 月には wolfCrypt 暗号ライブラリが世界初の SP800-140Br1 準拠の FIPS 140-3 認証を取得しました。お客様への FIPS 140-3 認証取得代行サービスも提供しており、10 年の経験と多くの実績があります。

wolfSSL Inc.は米国ワシントン州シアトルに本社を置き、モンタナ州ボーズマン、オレゴン州ポートランドなどに拠点があります。

wolfSSL Japan 合同会社の技術サポートセンターでは、日本人専任スタッフによるサポートサービス、カスタマイズサービスなどを提供しています。

wolfSSL 会社情報

wolfSSL Inc.	本社所在地：Edmonds Way, Suite C-300, Edmonds, WA 98020 USA 代表者：Larry Stefonic 設立：2004
wolfSSL Japan 合同会社	本社所在地： 〒108-6028 東京都港区港南 2-15-1 品川インターシティーA 棟 28F 代表者：須賀 葉子 設立：2018 年 https://www.wolfssl.jp/
事業内容	ネットワークセキュリティと関連ソフトウェアテクノジーの開発、提供、サポート
特徴	ライセンスモデルとして、無償のオープンソースと有償商用ライセンスのデュアルライセンスを特徴としています。オープンソース版によりお客様に十分な技術検討の機会を提供する一方、商用版ライセンス、サポートにより長期安定した技術開発の提供、高い専門性を持つ技術者による製品・技術開発の継続性を実現します。

問い合わせ先： info@wolfssl.jp

(Rev.1.0 Mar 2020)

本社所在地

〒 135-0061 東京都江東区豊洲 3-2-24
（豊洲フォレシア）
https://www.renesas.com

商標について

ルネサスおよびルネサスロゴはルネサス エレクトロニクス株式会社の商標です。すべての商標および登録商標は、それぞれの所有者に帰属します。

お問合せ窓口

弊社の製品や技術、ドキュメントの最新情報、最寄りの営業お問合せ窓口に関する情報などは、弊社ウェブサイトをご覧ください。
http://www.renesas.com/contact/

Doc Number: R01WP0034JJ0100