サイバーセキュリティ（ハードウェアセキュリティモジュール）

昨今、デジタル技術の急激な発展に伴い、自動車業界では AD、ADAS の開発、コネクティッド化が進んでいますが、利便性が向上する一方、それはセキュリティ上の脅威に晒されることを意味しています。各企業様においてはサイバー法規（ISO 21434）対応が急務となっているものの、慣れない用語や専門技術に頭を悩ませている方も多いのではないでしょうか。今月のメルマガではセキュリティ技術を支える HSM について述べてみたいと思います。

HSM（Hardware Security Module）は、暗号鍵の保管や生成、暗号化、ハッシュ化を担うモジュールであり、HSMを内蔵したマイコンが各社からリリースされています。HSMが内蔵されていない一般的なマイコンでセキュリティにかかるこれらの処理をまかなう場合、負荷が重くなってしまうばかりでなく、攻撃者から鍵を解析されやすいというリスクが生じてしまいます。さっそく本題に入りたいところではありますが、HSM の機能を説明するためには、いくつかの事前知識が必須となるため、セキュリティの基本技術について触れていきたいと思います。

鍵

鍵はバイナリーデータであり、規則性を持たない値が良いとされています。セキュリティの生命線であり、送信したいデータ（平文）の暗号化を行う際は、この鍵を使用します（図 1）。一般的に暗号化アルゴリズムは公開されているもの（AES128 等）であるため、鍵を盗まれてしまうと全てのセキュリティ機能が無効化されるといっても過言ではありません。

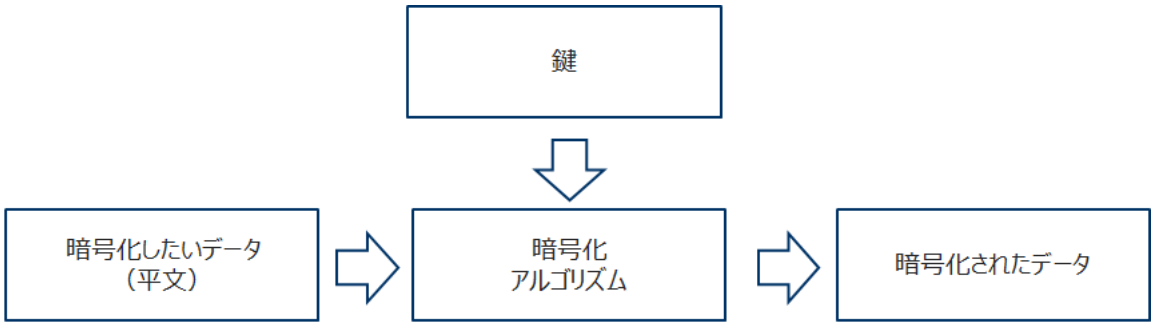

図 1　暗号化の流れ

対称鍵と非対称鍵

暗号化と復号に同じ鍵を用いる「対称鍵」方式と、異なる鍵を用いる「非対称鍵」方式があります。前者は内部ネットワーク（CAN 等）で用いられることが多く、後者は不特定のノード間でやり取りを行う（インターネット、V2X 等）場合に使用されます。非対称鍵方式においては、暗号化用の鍵は外部に「公開」し、復号用の鍵は外部に漏洩しないよう厳重に管理されることになります。暗号化用の鍵を盗んだとしても、暗号化したデータは受信側のノードが厳重に管理している復号用の鍵でしか復号できないため問題は生じません（図 2）。尚、復号用の秘密鍵で暗号化を行う場合（デジタル署名）もありますが本稿では割愛します。

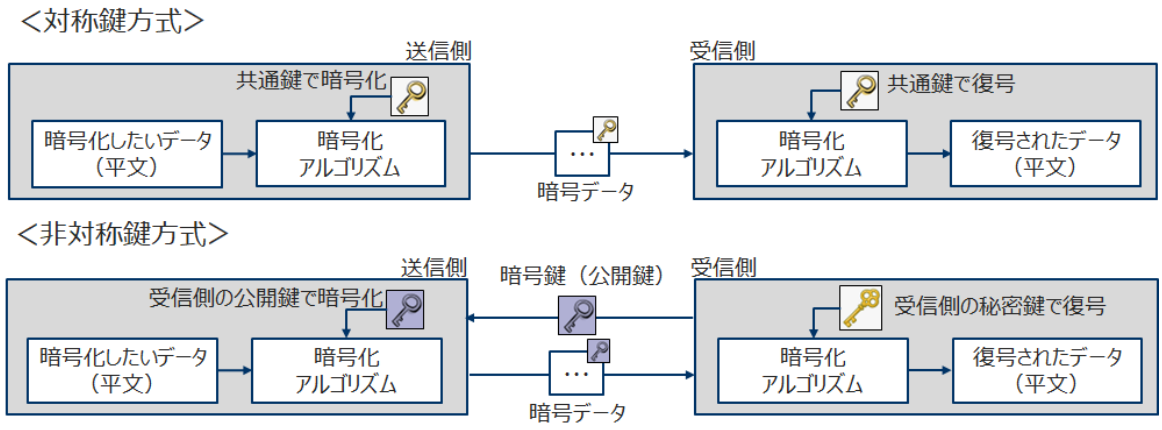

図 2 対称鍵と非対称鍵の違い

ハッシュ

ハッシュは送信したいデータ（平文）をハッシュ関数（SHA2 等）によってユニークな値に変換したもので、元データとは全く異なるほぼ「唯一の値」となり、1bit 変えただけでも全く異なる値になる性質をもっています。また、暗号化とは違って不可逆であり、復号することはできません。この特性を利用して、改ざんの防止に用いられています。送信側はデータとデータのハッシュ（図 3 ハッシュ 1）を送信、受信側は受信したデータを用いてハッシュに（図 3 ハッシュ 2）に変換し、受信したハッシュ 1 とハッシュ 2 を比較します。両者が合致していればデータは改ざんされていないと判断できるという理屈です。

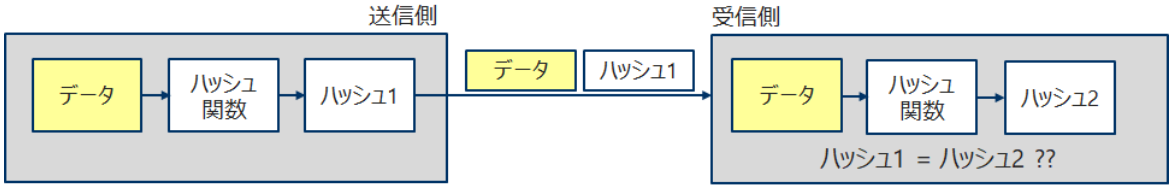

図 3 ハッシュ化と比較の流れ

耐タンパ性

通常のマイコンの場合、メモリダンプによる鍵の読み出しや、マイコンの物理信号（電圧、消費電流等）から統計的に鍵を類推するサイドチャンネル攻撃、IC の樹脂が壊されチップ内の鍵情報を直接解析されてしまう物理攻撃に対する耐性（耐タンパ性）が不十分であり、秘密情報が不正に盗まれやすいものとなっています。

HSM は秘密に管理すべき情報を格納し、鍵など秘密情報は外に出力することなく内部で暗号化、ハッシュ化等の演算を行います。限られたインタフェースによりメモリダンプを防ぎ、サイドチャネル攻撃に対しては意図的に消費電流を変更できる機能、物理攻撃に対しては樹脂を剥がされると光によって記録が消去される機能を備えた製品もあります。このように耐タンパ性に優れた HSM ですが、搭載する機能については基本的に EVITA（E-safety Vehicle Intrusion Protected Applications）プロジェクトによって策定されたハードウェア規格で定められた 3 つのレベル（表 1）に準拠して開発されており、用途によって使い分ける必要があります。今後さらにセキュリティ対策が求められることが想定されているため、これを期に導入を検討してみてはいかがでしょうか。

Full　　：外部と通信するためのデバイス（TCU）

Medium ：セントラルゲートウェイ、ヘッドユニットなど
Light　　：エンド ECU

項目	Full	Medium	Light
不揮発性メモリ 揮発性メモリ	搭載	搭載	オプション
セキュア CPU	搭載	搭載	無
対称暗号化	搭載	搭載	搭載
非対称暗号化	搭載	無	無
ハッシュ	搭載	無	無
乱数生成	真性	真性	疑似

表 1 HSM のレベルと機能

トレーニング（ISO 21434 自動車サイバーセキュリティ）のご案内

弊社では ISO 21434 のトレーニングの開催を 6 月に予定しています。車載 ECU システム開発（システム／ハードウェア／ソフトウェア）を担当するエンジニアが、これから ISO 21434 に対応したプロセス及びセキュリティ設計を実施して行くために、規格の要求事項にはもちろんのこと、鍵管理をはじめとするセキュリティに関する基本事項の学習や TARA の演習を通じて解説します。貴社にてプライベート開催も実施可能です。是非、ご受講をご検討ください。

2024/5/14 山田 毅

【トレーニングのお申し込みページ】
ISO/SAE 21434 サイバーセキュリティ概論トレーニング：2024 年 6 月 20 日
https://biz3.co.jp/publictraining/3675

ISO/SAE 21434 サイバーセキュリティ実践～エンジニアリング編～：2024 年 6 月 21 日
https://biz3.co.jp/publictraining/6200