# 車両サイバーセキュリティの未来（7）

## 製造フェーズにおけるセキュリティ対策

PwC コンサルティング合同会社　マネージャー　納富 央
PwC コンサルティング合同会社　シニアアソシエイト　澤 謙太

## 製造フェーズにおけるセキュリティ対策

これまで、製造工場では独自のネットワークや制御系システムの設備が用いられていたものの、それでもマルウェアなどによるセキュリティ被害は発生していました。さらに近年では、スマートファクトリーのようなIoT化が進み、さまざまな機器が製造工場のネットワークに接続しています。また、システム自体に汎用的なOSやアプリケーションが用いられることが増えています。このような環境の変化により、マルウェアのターゲットとなるなどセキュリティリスクがより高まっているのです。

また、車両がネットワークに接続されたことで、通信の暗号化やメッセージ認証のような暗号技術の利用が広がりました。その影響で、暗号技術において重要な役割を果たす暗号鍵を、内部に保管しなければならないECU（Electronic Control Unit）が増えてきました。この暗号鍵は製造工場で厳重に管理し、漏えいや改ざんがないことを常に保証する必要があります。

さらに、国際規格であるISO/SAE 21434とともに重要であり、今後の法律化が見込まれている

“Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA”においても、製造フェーズを含む開発のライフサイクル全体においてCSMS※1の実施が求められており、今後は法律・国際規格の上でも製造工場におけるセキュリティ活動が必須になると考えられます。

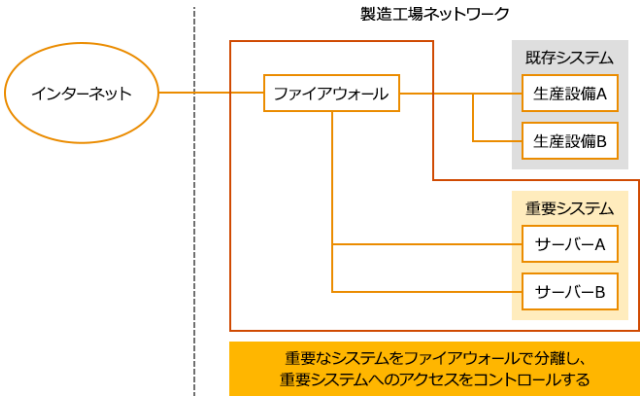
このように、工場のIoT化・車両機能の進化・法律・国際規格といったさまざまな面から製造フェーズにおけるセキュリティ活動の必要性が高まっています。

## 製造工場の各設備で必要なセキュリティ対策とは

これまで工場の生産設備は外部のネットワークにつながることが少なく、セキュリティ対策が十分に実施されていないケースもあると考えられます。そのような設備をそのまま外部のネットワークにつないでしまうと、セキュリティ強度の弱い生産設備が攻撃の対象となってしまいます。ネットワーク全体がセキュリティ上の危険にさらされるため、各生産設備やネットワークへのセキュリティ対策が必要です。

しかし、全ての設備を同じレベルでセキュアにすると、作業量やコストが膨大になってしまいます。そこで、ネットワークを分離し、ネットワーク同士の接続にはファイアウォールなどでアクセスを制御し、各設備にそれぞれ必要なセキュリティ対策を施すことで、効率的なセキュリティ管理を実現します。

図表1：重要システムへのアクセスコントロール例




## より強固な対策が必要な暗号鍵管理システム

通信の暗号化やメッセージ認証などには暗号鍵と呼ばれるデータを用います。この暗号鍵は、攻撃者に不正に入手されると、暗号化通信の解読や車両のなりすましにつながるため、生産設備や車両内で安全に保管するなど厳重に管理する必要があります。

暗号鍵は車種や車両1台1台ごとに別の鍵を使うことが想定されるため、その際には暗号鍵と車両やデバイスをひもづけて管理し、デバイス内に暗号鍵を書き込むための管理システムが必要となります。前述のとおり、この暗号鍵は漏えいすると車両に対して大きなインパクトを与えてしまうため、暗号鍵を取り扱うシステムは、通常の生産設備よりも高いレベルでのセキュリティ強度を確保することが必要です。

**鍵管理システムのセキュリティ対策例**

- サーバールームへの入室管理などの物理セキュリティ強化
- 多要素認証などを用いたシステムへのアクセス制御強化
- HSM※2による暗号鍵の管理
- 鍵管理に関連するシステムのログ監視強化

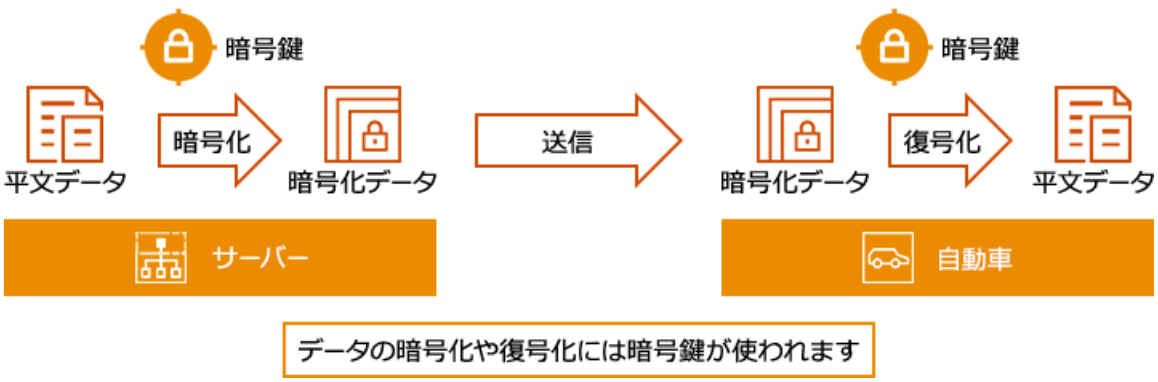
このように、鍵管理システムではより強固なセキュリティ対策が必要となります。既存のシステムと鍵管理システムが同一ネットワーク上で混在している環境では、それら全てを同じレベルのセキュリティ強度にしなければ、最もセキュリティ強度が低いシステムに対して攻撃が行われ、同一ネットワーク上の鍵管理システムが危険にさらされることになります。そのため、前述したようなネットワークの分離とアクセスコントロールを行い、それぞれのシステムにおいて必要十分なセキュリティ構成にすることが重要となります。

今後、ますます重要となってくる製造フェーズでのセキュリティ対策と暗号鍵管理について考察を行いました。第8回では製造した製品出荷後に必要となるセキュリティ活動について考察します。

※1 CSMS：Cyber Security Management Systemの略、産業用オートメーションおよび制御システムを対象としたセキュリティを管理する仕組み

※2 HSM：Hardware Security Moduleの略、データセンターなどにおいて暗号鍵のような重要なデータを保管するためのセキュアなハードウェア

図表2：暗号化処理の概要





**お問い合わせ**

PwCコンサルティング合同会社
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel : 03-6250-1200（代表）　Mail : jp_cyber_inquiry@pwc.com



© 2019 PwC. All rights reserved.  PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.  This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.