VECTOR



はじめてのAUTOSAR SecOC

車載通信に必要なセキュリティー機能とは

発行元：ベクター・ジャパン株式会社
ベクター・ジャパン株式会社の書面による許可なしに、本書の内容を転載、複製、複写することを禁じます。
記述されている内容は予告なく変更されることがあります。

©Vector Japan Co., Ltd.

VECTOR

目次

1. はじめに 02

2. 自動車にサイバーセキュリティーが必要になった背景 03

なぜ自動車にサイバーセキュリティーが必要になったのか？ 03

なぜ車両内部のネットワークにもサイバーセキュリティーが必要なのか？ 04

サイバー攻撃から安全を確保するためには？ 05

3. 安全を確保するための暗号技術 06

暗号の基礎技術 06

メッセージ認証子とデジタル署名 07

メッセージ認証子の仕組み 08

メッセージ認証子の特長 09

4. AUTOSAR SecOCの仕組み 10

AUTOSAR SecOCの概要 10

再送攻撃対策用カウンター：Freshness Value 11

SecOCのMAC生成アルゴリズム 12

参考：PDU (Protocol Data Unit)について 13

5. まとめ 14

はじめてのAUTOSAR SecOC

1. はじめに

インターネットなど外部のネットワークと通信する自動車には、サイバーセキュリティーが求められます。実際に自動車に対するハッキング事例も報告されています。

自動車に対するハッキングは、乗車している人や周囲を走行する自動車の安全への脅威となります。もし、自動車の制御を担っているECUが遠隔操作されるようなことがあれば、非常に危険です。そのため、自動車にはサイバーセキュリティー対策が必要です。

ECUの遠隔操作を防ぐためには、車載通信、すなわち車両内部のECU間の通信にもセキュリティーが必要になります。自動車に必要なセキュリティー機能は多岐に渡りますが、本資料ではこの車載通信に関するAUTOSAR規格であるSecOC (Secure Onboard Communication)について、必要となった背景からセキュリティーを確保する仕組みまでを解説していきます。

2.自動車にサイバーセキュリティーが必要になった背景

なぜ自動車にサイバーセキュリティーが必要になったのか?

自動車のエレクトロニクス化が進むにつれ、自動車は車外のネットワークと通信するようになりました。インターネットなど、車外のネットワークとの通信が可能となると、外部からサイバー攻撃を受ける可能性が出てきます。ここでいうサイバー攻撃とは、具体的には遠隔操作を指します。

車外ネットワークと接続しない車両の場合、所有者や車両そのものに危害を加えるには、直接車両に近づく必要があります。車両に物理的に近づいて行われる犯罪は古くからあり、また現在でも（手口の高度化などはあるにしても）変わらず発生しています。攻撃者の目線で考えたとき、車両に直接近づくことができるのであれば、サイバー攻撃のように知識やスキルが必要なうえ、手間のかかる手段をとる必要はなく、その攻撃手段も多様です。

一方、車外ネットワークに接続可能な車両の場合、攻撃者は遠隔地からの攻撃ができるようになります。そのため、遠隔攻撃を実現させるための準備作業にコストがかかったとしても、実際の車両に近づく必要がないなど、実行するメリットが出てきます。

遠隔攻撃に対する防御として、第一に外部と通信する出入口をしっかり守る必要があります。これは企業や家庭などのイントラネットと同様で、通常はファイアウォールの設置などを行い、内部と外部のネットワークを分けることで内部のネットワークを守ります。

本資料では、車両内で内外のネットワークを分断するECUのことをGateway（ゲートウェイ:GW、以下GW）と呼称します。前述のとおり、自動車サイバーセキュリティーにおいて、「GWを堅牢にする」ことが重要なポイントの一つになります。

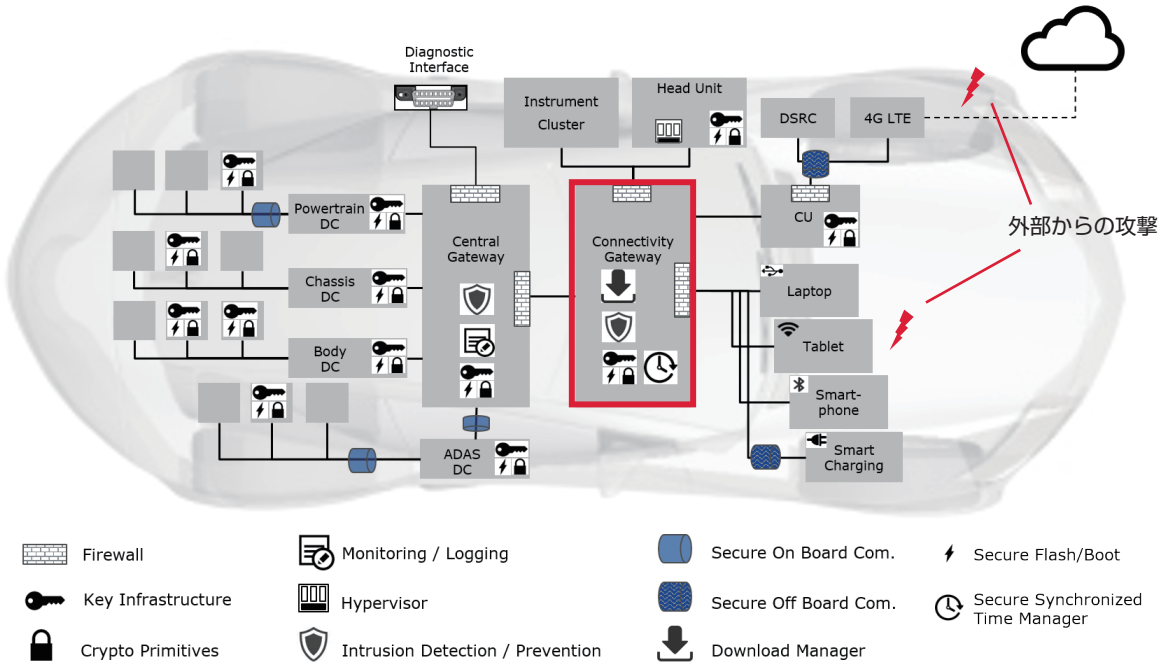

図1:車両のアーキテクチャーの模式図
赤枠のGateway（GW）にて車両の内外のネットワークを分断しています

なぜ車両内部のネットワークにもサイバーセキュリティーが必要なのか?

いくらGWを堅牢に作っても、100%防御できるシステムを作ることはできません。実際、ITの分野ではサイバー攻撃により内部のネットワークに侵入され、企業の機密情報などが盗まれる事件が数多く発生しました。また、自動車の分野でも市販されている車両のGWが外部から乗っ取られ、車両内部のCANバスまで侵入された事例があります。

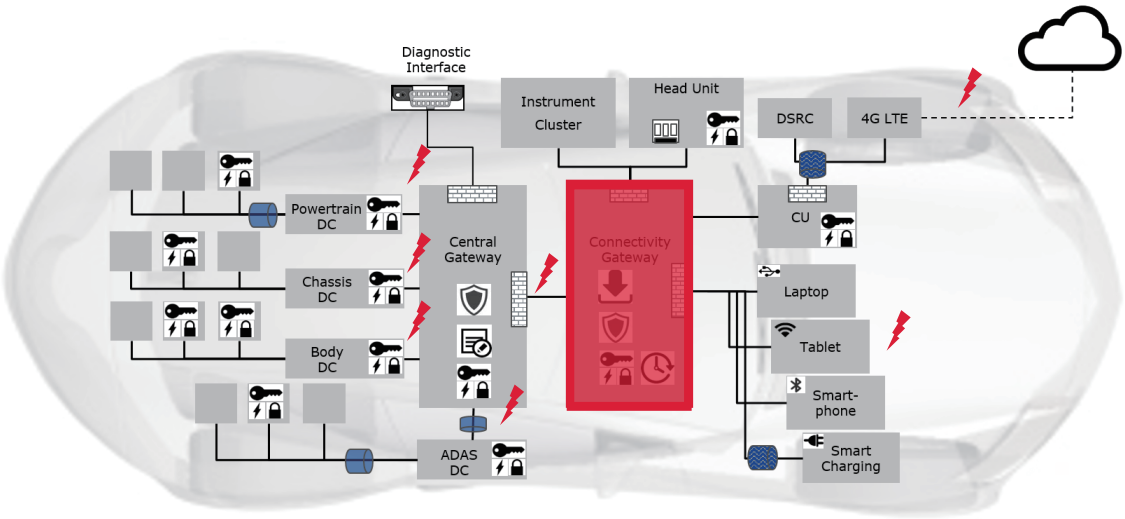

図2:GWが乗っ取られ、車両内部のCANバスが攻撃にさらされているイメージ図

特に注目を浴びた事例を以下にご紹介します。

> 2015年:車外からの遠隔攻撃で走行中にワイパー動作やエンジン停止　⇒　結果、リコール

> 2016年:走行中のハンドル遠隔操作

上記2つの事例はアメリカで行われたもので、どちらも同一の車種に対して実施されました。これらの事例はホワイトハッカーと呼ばれるセキュリティー研究者による実証実験で、遠隔操作の様子が動画で公開されたため、多くの注目を集めました。現在でもインターネットでこれらの動画を閲覧することができます。実際に動画を見てみると分かりますが、2016年のハンドル遠隔操作の事例が仮に公道において犯罪目的で実行された場合、大きな事故につながる危険があります。

サイバーセキュリティーはIT業界で先行していたため、一般的にセキュリティーとはプライバシーや財産を守るため、と考えられることが多いのですが、自動車におけるサイバーセキュリティーは運転手や同乗者の安全と直結します。そのため、自動車のサイバーセキュリティーではプライバシーや財産の保護よりも、まず人命を守ることを考えなければなりません。

サイバー攻撃から安全を確保するためには？

サイバー攻撃から安全を確保するために、実際に行われたハッキング手口について考えます。左記に紹介した事例では、大まかに以下の手順で遠隔操作を実現しています。

Step1：GWに攻撃を仕掛け、GWを乗っ取る
Step2：その後、乗っ取ったGWが接続しているCANバス経由で対象のECUに不正なメッセージ（例：急ハンドルを切るよう命令）を送りつけ、遠隔操作する

上記2つのステップのうち、1つでも防ぐことができれば安全を確保することができます。Step1については前述のとおり、GWをより堅牢にしていく必要があります。Step2については、CANバスに接続しているECUが不正なメッセージを破棄することができれば安全を確保することができます。

不正なメッセージには以下の2つの例があります。

不正メッセージの例	CANにおける実現方法
なりすまし	本来、他のECUが送るべきCAN IDのメッセージを、乗っ取ったGWから不正な値を乗せて送信
メッセージの改ざん	CANバス上に流れるメッセージの特定bitを反転させ、不正な値とする （単純にはビットエラーとなるためうまく行かないうえ、ビット反転用のHWが必要となる）

攻撃者の目線から考えると「なりすまし」は比較的容易に実現できる一方、「メッセージの改ざん」は実現のハードルが高いものとなります。そのため、多くの場合、CANの不正なメッセージは「なりすまし」を指します。

CANプロトコルやその拡張であるCAN FDなど、車載ネットワークのプロトコルには不正なメッセージを検知する仕組みはありません。そのため、不正メッセージを検知できるような仕組みを別途追加する必要があります。

3. 安全を確保するための暗号技術

暗号の基礎技術

前章にて、車載ネットワークのセキュリティーを確保するために必要な対策は、不正なメッセージを検知し、棄却する機能であることが分かりました。

車載通信に不正メッセージ検出機能を取り入れるため、セキュリティーに関して先行しているIT業界の既存技術から使えるものを探します。

以下に、暗号技術における6種類の基礎技術を示します。

暗号技術	主な用途
暗号	メッセージを暗号化。機密性の確保に必要
鍵配送プロトコル	共通鍵暗号用の鍵を配送するための仕組み
(暗号学的)ハッシュ関数	改ざん検知や、他の技術の基盤として利用
メッセージ認証子	改ざん検知、ユーザー認証など
デジタル署名	改ざん検知、ユーザー認証、否認拒否など
(暗号学的)擬似乱数生成	他の暗号技術の基盤として利用

上記の暗号技術の中で有名なのは「暗号」です。狭い意味の「暗号」である暗号化は、盗聴対策の技術であり、車載通信のデータを秘匿する必要がある場合には有効ですが、今回の不正メッセージ検出とは用途が異なるため使用できません。

不正メッセージの検出には「改ざん検知」と「ユーザー認証」の機能が必要となります。この2つを満たすことができる技術は、上記の表の赤枠で示した2つで、「メッセージ認証子」と「デジタル署名」になります。

メッセージ認証子とデジタル署名

「メッセージ認証子」と「デジタル署名」の2つの技術について、一般的な特長を簡単にまとめると以下のようになります。

	メッセージ認証子	デジタル署名
基盤技術	共通鍵暗号	公開鍵暗号
計算量	小さい	大きい
認証に使用するデータ量	小さい	大きい
鍵管理	通信相手が増えるほど鍵が増加	通信相手数に因らず一定
通信相手	同じ鍵を共有する相手と通信	不特定多数と通信

車載通信の場合、ECUの計算リソースが大きくないため、計算量は十分に小さい必要があります。デジタル署名はメッセージ認証子と比べて計算時間が数百倍かかるといわれており、ECU間の通信に利用するには不向きです。同様に、車載通信で扱えるデータ量も小さいため、デジタル署名を使って通信する際に必要となる大きな認証用データをやり取りするのは現実的ではありません。

一方、メッセージ認証子のデメリットとして、通信相手が増えるほど管理すべき鍵が増加し、鍵の管理コストが高くなる、という点があります。しかし車載通信に適用する際、同じネットワークでは同じ鍵を共有するなど、運用方法でカバーできる部分もあるため、大きな問題とはなりません。

よって、車載通信に不正メッセージ検出機能を取り入れるには、メッセージ認証子の技術を使うことが最も適切であることが分かります。

メッセージ認証子の仕組み

ここから、メッセージ認証子の仕組みについて解説していきます。

メッセージ認証子は略して、MAC (Message Authentication Code)と呼ばれます。

共通鍵暗号を応用しているため、事前に送信者と受信者で鍵を共有していることが前提になります。本資料では、この鍵のことをMAC鍵、または単に鍵と呼称します。鍵の共有方法についてはメッセージ認証子とは別の技術で実現しますが、本資料の範囲を超えるため記載はいたしません。ご興味のある方は暗号技術や鍵配送などに関する書籍等を参照してください。

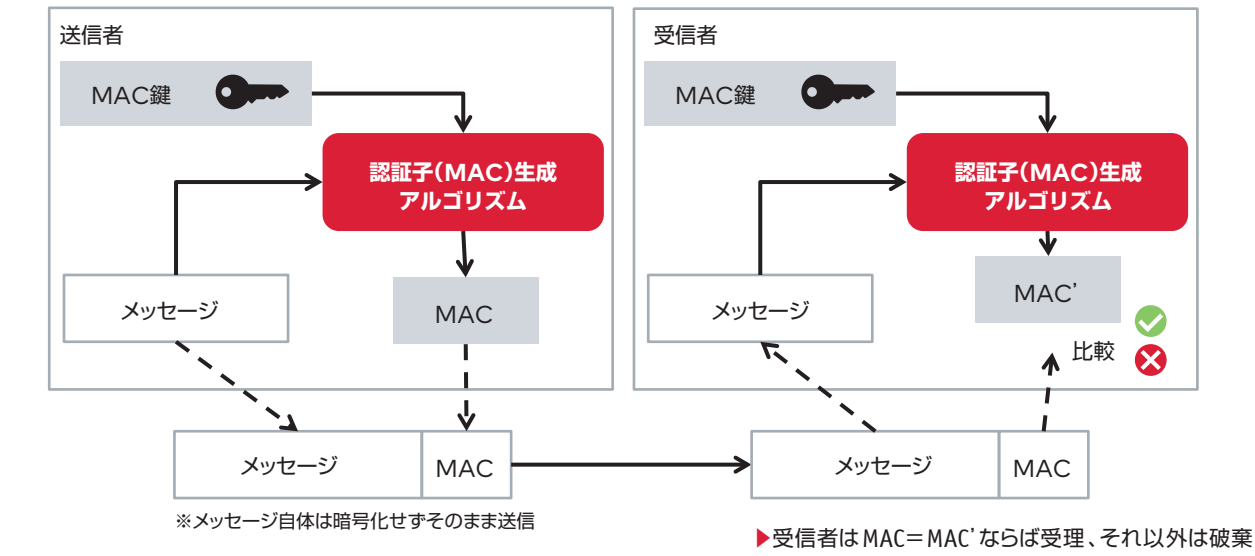

図3：メッセージ認証の仕組み

メッセージ認証の仕組みは以下のとおりです。

Step1：送信者がメッセージとMAC鍵をMAC生成アルゴリズムに入力し、MACを生成します。

Step2：送信者はメッセージを平文（暗号化せずそのままの状態)で、後ろにMACを付加して送信します。

Step3：受信者は受け取ったメッセージと自分の持つMAC鍵をMAC生成アルゴリズムに入力し、MAC'を生成します。

Step4：受信者が生成したMAC'と、送信者から受け取ったMACが完全一致した場合は、メッセージを受理します。そうでない場合はメッセージを破棄します。

「メッセージ」の中身についてはどのようなものでもかまいません。

上記の前提として、MAC生成アルゴリズムは入力となる「メッセージ」と「MAC鍵」が同じだった場合、まったく同じMACを出力します。そうでないと受信者が受理できないためです。またMAC生成アルゴリズムは、生成したMACと入力メッセージが多数あったとしてもMAC鍵が容易に推測できないアルゴリズムとなっています。

上記の仕組みにより、正しいMAC鍵を持たない送信者は正しいMACが生成できないため、受信者は不正なメッセージを検知できるようになります。

メッセージ認証子の特長

メッセージ認証子の特長を簡単にまとめると、以下のとおりとなります。

> 機密性なし

メッセージ認証子はメッセージが正しい送信者から送信され、改ざんされていないことを保証するための技術であり、盗聴対策の技術ではありません。そのため、メッセージ認証子単体では通信内容は盗聴可能です。盗聴対策も必要な場合は、暗号も組み合わせる必要があります。

> 送信者を厳密には特定できない

メッセージ認証子の受信者は「正しいMAC鍵を持っている送信者が送信したか否か」のみを判別します。たとえば、5つのECUで同じMAC鍵を共有している場合、「その中の1つのECUが送信した」ということまでは判別できますが、5つの中から送信者を特定することはできません。

ただ、本章にて議論している対策としては、そこまで特定する必要はありません。上記の例で送信者を特定したい場合には、鍵をそれぞれのECUで異なるものを使用するか、デジタル署名が必要になります。

> 鍵の配送と管理が重要

メッセージ認証子は正しい送信者、受信者だけが同じMAC鍵を共有していることが前提となります。メッセージ認証子を用いた通信を開始する前に、鍵の共有を安全に行う必要があります。また鍵の配送完了後も、鍵を適切に保存しておく必要があります。鍵情報が漏れてしまうとメッセージ認証子の前提条件が崩れてしまい、防衛の効果はすべて失われてしまいます。

特に複数のECUで同一の鍵を共有している場合、仮に、管理がずさんなECUがあり、そこから鍵が漏れると、鍵を共有するすべてのECUが危険にさらされることになります。そのため、鍵の管理はすべてのECUで正しく行う必要があります。

> 再送攻撃対策が重要

再送攻撃（Replay attack）とは、ネットワークに送信されるデータを盗聴して記録しておき、所望のタイミングで再送する攻撃です。過去の送信データであればMACも含めて判明しているため、MAC鍵を持たなくても「なりすまし」を実現できます（※MAC生成アルゴリズムは、入力データとMAC鍵が同じであれば必ず同じMACを生成するため）。

車載通信の場合、たとえば以下のような攻撃が考えられます。

過去のアクセル全開時のデータを記録しておき、危険なタイミングでなりすまして送信します。受信ECUは再送攻撃時に送信されるMACの値が正しいためメッセージを受理してしまい、アクセル全開の指示を実行し、運転手や同乗者が危険にさらされます。

そのため、メッセージ認証子の利用時には、運用するシステムに応じて個別に対策を立てる必要があります。

次章では、AUTOSAR SecOCでどのように再送攻撃対策を行っているかについて、具体的に解説していきます。

4.AUTOSAR SecOCの仕組み

AUTOSAR SecOCの概要

AUTOSAR SecOCは、メッセージ認証子をベースに作られた、車載ネットワーク用のセキュリティー技術です。SecOCはAUTOSAR 4.2.1（2014年）よりAUTOSAR仕様に追加されています。

SecOCの仕組みは以下の図のようになっており、メッセージ認証子の仕組みをベースに作成されていることがわかります。

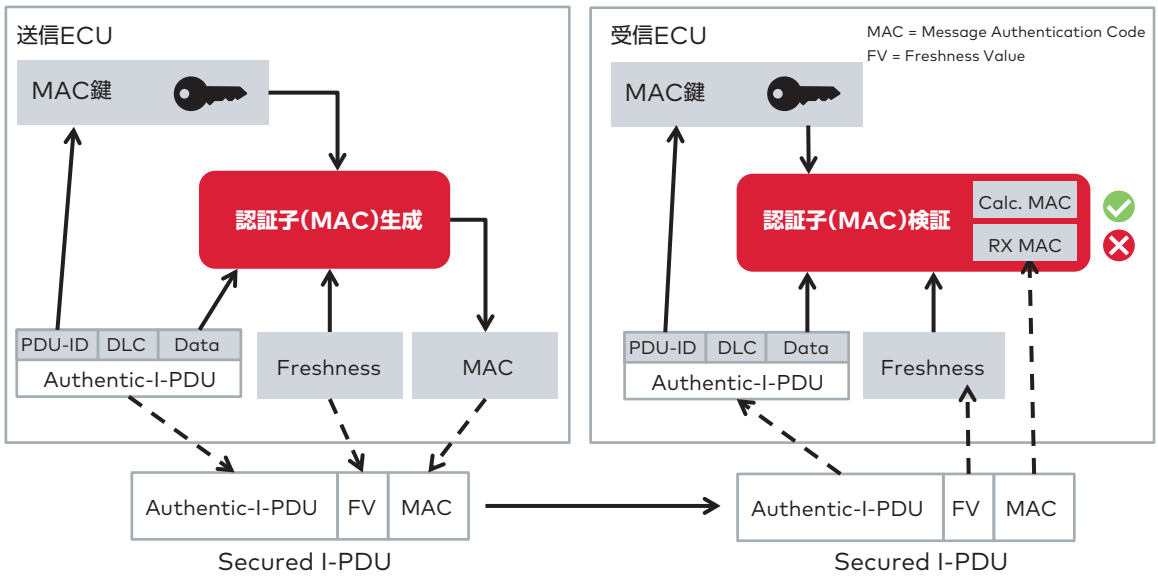

図 4：SecOC の仕組み

SecOCはメッセージ認証子の仕組みをベースにして作成されているため、その特長がそのまま当てはまります。つまり、正しいMAC鍵を持っている送信者だけが正しいMACを生成でき、受信者はMAC検証を行うことで不正メッセージを判別します。

メッセージ認証子と異なる点は、MAC生成アルゴリズムへの入力にFreshness Valueと呼ばれるデータが追加されていることです。本資料では、このFreshness ValueをFVと呼称します。FVは、再送攻撃を防ぐために追加されたカウンターで、次ページで詳しく解説します。

再送攻撃対策用カウンター：Freshness Value

メッセージ認証子における再送攻撃対策として、以下のような運用が一般的です。

> MAC生成時に入力となる「メッセージ」が常に異なる値となるよう、カウンター値（シーケンス番号やタイムスタンプ、セッション番号など）を付加する

> 受信者は過去に送信されたカウンター値が付加されたメッセージを受理しないようにする

再送攻撃を防ぐために上記に沿ってSecOCに規定されたカウンターがFVとなります。

図4ではFVをMAC生成アルゴリズムに直接入力していますが、実際には「メッセージ」のデータ末尾に付加して計算を実行しています。つまり、メッセージ認証子の仕組みのうえでは「メッセージ」とだけ定義されていたデータについて、SecOCでは「保護対象データ」と「FV」に分割した、と考えることができます。この保護対象データのことを図4ではAuthentic-I-PDUと記載しています。保護対象データには、ECUが使用する制御データが格納されています。

上記のとおり、メッセージ認証子における再送攻撃を防ぐためには、メッセージ送信ごとに値が異なるカウンターがあればよく、シンプルなカウンターでも複雑なものでもかまいません。

SecOCにおけるFVも同様で、再送攻撃を防ぐために付加し、古い値の受信時は破棄するということのみが規定されており、具体的な値の変化についてはOEMの仕様次第となっています。そのため、OEMによってFVが類似していることもあれば、まったく違う形式のこともあります。

図5に、FVの一例としてAUTOSAR仕様に記載されているJASPARプロファイルにおけるFVの構造を示します。

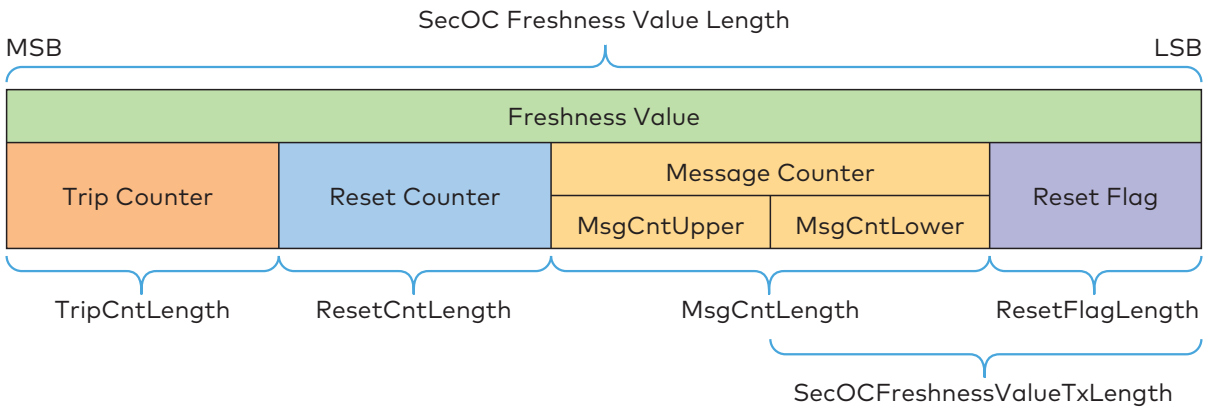

図5：FVの一例

※ AUTOSAR CP Release 4.3.1 RfC77782 V6 より抜粋

SecOCのMAC生成アルゴリズム

SecOCで使用されるMAC生成アルゴリズムについてもOEM次第ではありますが、通常CMAC/AES-128が使われます。CMAC/AES-128はMAC生成のアルゴリズムとして非常に優秀で、SecOC以外でも広く使われています。

> AES (Advanced Encryption Standard)

アメリカで2001年に規定された国家標準暗号です。アルゴリズムは公募で選ばれ、日本でも電子政府推奨暗号となっています。AES-128は鍵長が128bitで、他にAES-192、AES-256があり、将来的にも利用可能な拡張性があります。現在ではさまざまな場面で採用され、2030年以降も十分に安全であると考えられています。

> CMAC (Cipher-based MAC)

アメリカ政府推奨の認証子生成アルゴリズムです。高い安全性と計算効率の高さを両立し、また任意長のメッセージを扱うことが可能です。内部の暗号アルゴリズムにAES-128を利用した場合については、送信用にMACを切り取ったときの偽造確率について研究機関にて検証され、結果が公開されています。そのため車載通信用にMACを切り取って送信する場合の安全性も事前に確認することができます。

一方、誤った使い方をした場合、安全性が低下することがあります（認証暗号でCTRモードとの併用など）。

参考：PDU (Protocol Data Unit)について

AUTOSAR SecOCでは、取り扱うデータはPDUとなります。ここではPDUについて簡単にご紹介します。詳細についてご興味のある方は、AUTOSAR仕様や関連書籍等を参照してください。

PDUは、実際に制御に用いる値であるシグナル（=アプリケーション層）と、（データリンク層の）フレームとの間に入る、抽象的なレイヤーとなります。PDUが間に入ることで、シグナルとフレーム（=バスプロトコル）を切り離すことができます。

なお、PDUはAUTOSARによって作られたわけではありません。AUTOSARにより、以前から存在したPDUの考え方が仕様に取り入れられています。

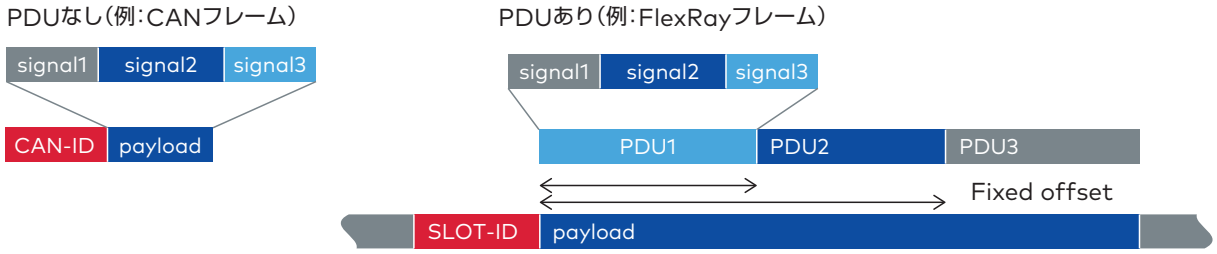

図 6：PDU の有無による、シグナルとフレームの関係の違い

CANについてもPDUを導入し、シグナルとフレームを分離することが可能です。

PDUの導入には、以下のようなメリットがあります。

> ソフトウェアの再利用促進
> PDU単位で転送処理やプロパティー定義（PDU単位の送信周期定義など）を行うことで、伝送効率を向上
> シグナルのグループ化

このうち、最初の「ソフトウェアの再利用促進」は特に重要で、AUTOSARスローガン：“Cooperate on standards – compete on implementation”（標準化においては協力 – 実装／利用にて競争）に沿っており、ソフトウェアに属するシグナルをハードウェアに属するフレームから切り離すことができるようになる、という意味を持ちます。

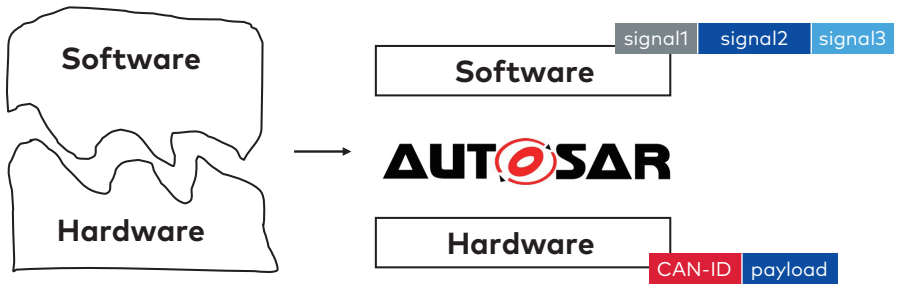

図 7：シグナルとフレームを切り離し、ソフトウェアの再利用を促進

5. まとめ

これまで解説してきたように、車外のネットワークとつながる自動車にとって、サイバーセキュリティーは安全に直結する重要な要素となっています。特に、走る、曲がる、止まるといった自動車の基本機能に関わるECUが遠隔操作されれば、運転手や同乗者、周囲を走行する車両等が危険にさらされることになります。

これを防ぐために、ECUは外部から注入される不正なメッセージに対して防衛手段を持つ必要があります。AUTOSAR SecOCはメッセージ認証子とFVを利用することで不正メッセージを検知し、遠隔操作を防ぎます。

以上、AUTOSAR SecOCの基礎知識として策定の背景からセキュリティー確保の仕組みまでを解説しましたが、いかがでしたでしょうか。本資料で解説した基礎知識が、車載ネットワーク開発に携わる、もしくは今後携わっていくエンジニアの方々の一助となれば幸いです。

[This page intentionally left blank.]

[This page intentionally left blank.]

VECTOR

www.vector.com/jp/ja/