製品分野別セキュリティガイドライン

車載器編

Ver. 1.01

CCDS セキュリティガイドライン WG

車載 SWG

改訂履歴

版数	改訂日	改訂内容
Ver.1.0	2016/06/08	新規作成
Ver.1.01	2016/06/15	一部改定

■商標について

・本書に記載の会社名、製品名などは、各社の商標または登録商標です。

■おことわり

・本書に記載されている内容は発行時点のものであり、予告なく変更することがあります。

・本書の内容を CCDS の許可なく複製・転載することを禁止します。

目次

1 はじめに

これまで製品業界ごとにセーフティ標準は策定されてきた。一方セキュリティ標準をみると、組織運営に関する標準（ISO27001）と製品設計のセキュリティ評価・認証に関する標準（ISO15408）が策定されており、近年では、重要インフラストラクチャー（社会インフラに欠かせないプラントや施設）の制御システムを対象とした標準（IEC62443）も策定されている状況である。

IoT の普及に伴い、身の回りにある生活機器が様々なネットワーク接続機能をもつことで、製品のセキュリティ懸念は増しているが、IoT 製品やサービスには欠かせないセキュリティ標準がいまだ生活機器に対しては整備されていない状況である。

欧米の動きをみると、各業界のセーフティ標準からセキュリティ標準を検討する動きが各所にみられる。一方、日本においてもセキュリティに関する懸念は顕在化しており、検討すべき、という声は多いが、具体的検討に入っている分野はまだ少ない状況となっている。

このような状況の中で、一般社団法人 重要生活機器連携セキュリティ協議会（CCDS）は設立された。本協議会では、生活機器セキュリティ標準の策定と、その標準に沿っていることを確認・検証した認証プログラムをセットにすることで、ユーザに安心して IoT 製品を使ってもらえる環境を整えることを目標に活動を行っている。

平成 27 年 8 月 5 日には独立行政法人 情報処理推進機構（IPA）が「つながる世界の開発指針検討 WG」を発足させ、国レベルでのセキュリティ検討がスタートした。CCDS も IPA-WG に参画し、CCDS 内でのガイドライン検討結果について提案を重ねてきた。

IPA-WG での検討結果は「つながる世界の開発指針～安全安心な IoT の実現に向けて開発者に認識してほしい重要ポイント」[1]としてまとめられ平成 28 年 3 月 24 日に公表された。IPA の開発指針は分野全体をカバーする共通事項を中心にまとめられた基本的な指針となっているが、CCDS では個々の製品分野において、具体的にセーフティとセキュリティをカバーした設計・開発を進めるために、本分野別ガイドラインを策定した。

IPA 発行「つながる世界の開発指針」については、下記 URL のリンク先を参照。
http://www.ipa.go.jp/sec/reports/20160324.html

1.1　車載器のセキュリティの現状と課題

自動運転、コネクティッドカーなど、車の技術革新は目覚ましく、利便性は急速に向上している。一方で、安心、安全を脅かすサイバー攻撃が拡大しており、ネットワークや車内持ち込みデバイスとつながるクルマが攻撃の対象となることが現実のものとなっている。米国のセキュリティ関連イベント Black Hat 2015 では、Chrysler のコネクテッドカーシステム「UConnect」の脆弱性を狙い JEEP のハッキングに成功した事例が報告された。車載 LAN などを介して ECU に悪意のある偽の信号を送信し、ステアリングやブレーキなどを操作するといった脅威が現実のものになりつつある。

車がハッキングされた際の被害は人命に係るほど非常に甚大であり、開発技術者のみでなく責任者や経営陣がセキュリティに対してどのように取り組んでいくべきかが課題となっている。

これまでネットワーク経由の脅威に直面することを想定していなかった製品が今後は攻撃の対象になり得るため、セキュリティを考慮した製品の企画・開発はもちろんのこと、利用者へのセキュリティ教育も考慮していく必要がある。

1.2　本書のねらいと対象者

本書は車載機器やシステムの開発に関わる企業の開発者を主な対象として、車載機器において適切なセキュリティ対策を実施するための、設計から製品リリース後までに考慮すべき設計・開発プロセスをガイドラインとしてまとめたものである。したがって本書は以下の方を主な対象としている。

1）車載機器やシステムの設計を行う設計者および開発者
2）車載機器やシステムの設計プロジェクトを推進する開発責任者
3）車載機器やシステムの設計プロジェクトに関する予算や人員を決定する意思決定者

また、開発者だけでは対応が難しい経営層の理解や全社的に支援が必要な内容も盛り込み、経営者にも参考にしていただける内容とした。車載機器やシステムの開発時に、IPA でまとめられた「つながる世界の開発指針」と合わせ、本ガイドラインを併用した検討に活用することを想定している。

1.3　略称

本書で使用されている略称について説明する。

表 2-1 略称一覧

略称	名称
A2DP	Advanced Audio Distribution Profile
CAN	Controller Area Network
CCDS	Connected Consumer Device Security council
CSIRT	Computer Security Incident Response Team
CVSS	Common Vulnerability Scoring System
D-Bus	Desktop Bus
DoS	Denial of Service
DSRC	Dedicated Short Range Communications
ECU	Engine Control Unit
ETC	Electronic Toll Collection system
GPS	Global Positioning System
GSM	Global System for Mobile communications
IEC	International Electrotechnical Commission
IoT	Internet of Things
IPA	Information-technology Promotion Agency
ISO	International Organization for Standardization
SWG	Sub Working Group
WG	Working Group

2　車載ガイドラインのシステムモデル

2.1　対象のモデル

対象とする車載システムの範囲を検討するにあたり、図 2-1 を参考にして、接続インターフェースを考えることとした。また、検討の範囲はヘッドユニット周りをモデル化し、そこに接続されているものを基本とする。検討対象のモデル化にあたっては、既に発表されている資料を参考にして検討を行った。参考にした車載システムを図 2-2 に示す。

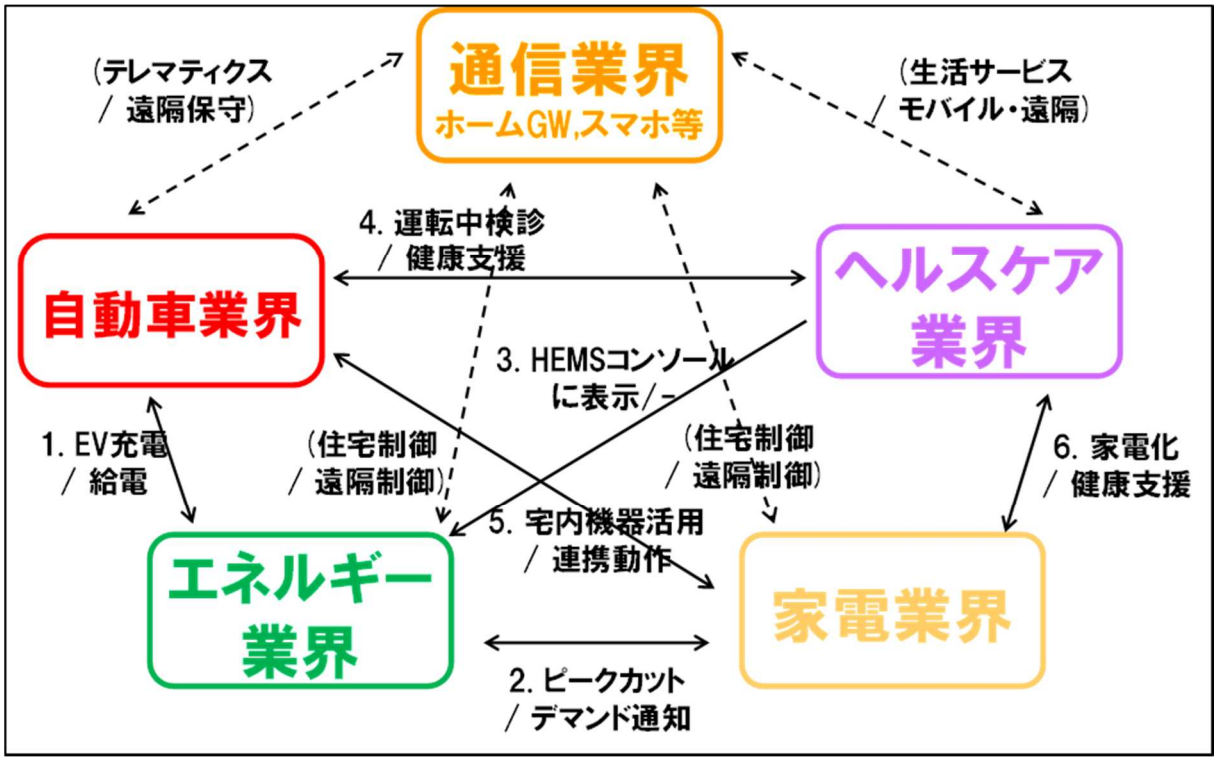
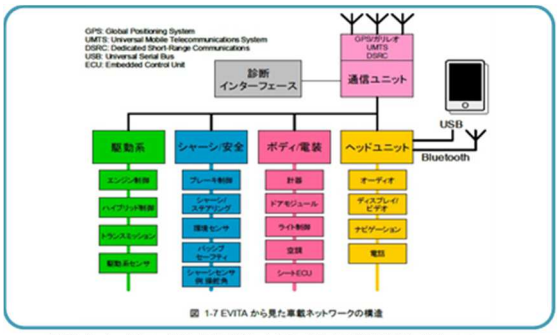
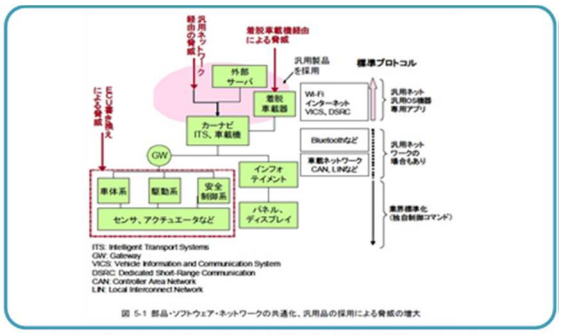


図 2-1 繋がる範囲

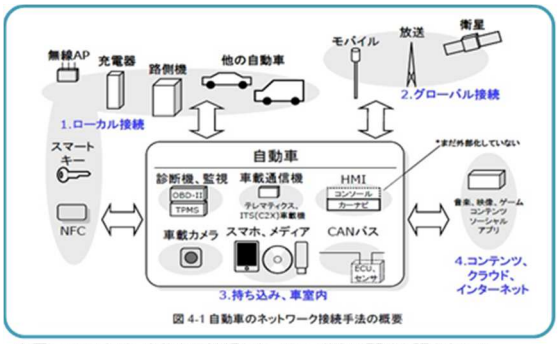
参照：第 2 回セキュリティガイドライン WG 資料より



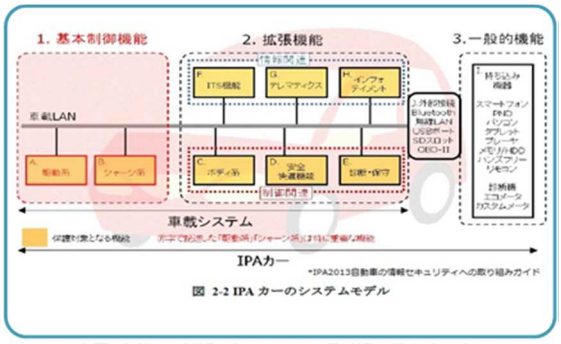
出展:セキュリティ動向と意識向上策に関する調査報告書(IPA)



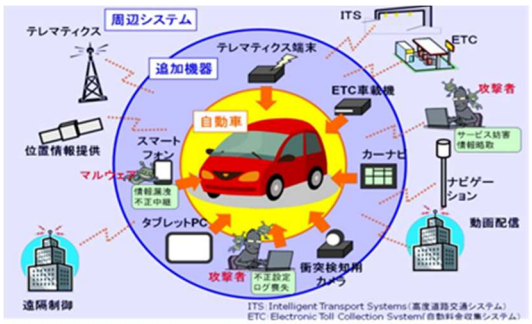
出展:セキュリティ動向と意識向上策に関する調査報告書(IPA)



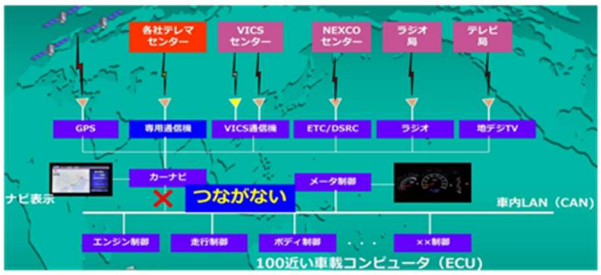
出展: 2011年度 自動車の情報セキュリティ動向に関する調査(IPA)



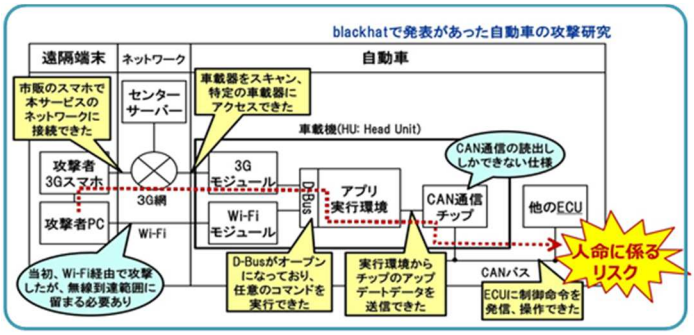
出展:自動車の情報セキュリティへの取り組みガイド(IPA)



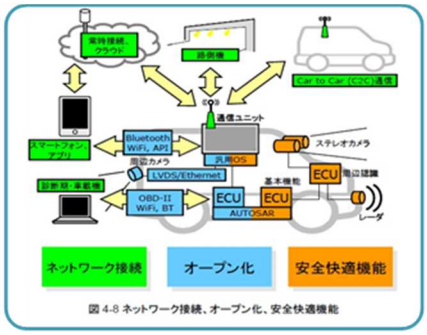
出展:繋がる組込みシステムの脅威とその対策(IPA)



出展:2020年の自動車社会とセキュリティ(インターネットITS協議会)



出展: IPAの第2回つながる世界の開発指針検討WG資料



出展:"繋がる自動車"の動向と関連標準化・セキュリティ(JARI)

図 2-2 車載システムの参考例

2.2　検討対象のシステムモデル

検討対象のシステムモデルを作成することで自動車の機能を整理し、脅威分析を行う際に、攻撃のルートとなる接続インターフェースや、攻撃者から守るべき資産、脅威の発生箇所等をイメージしやすくなる。そこで、前述の対象の範囲を参考にして、車外との接続インターフェースや､車載されるヘッドユニットを中心に､そこに接続される車載機器や、車内持込機器をリストアップし、検討対象のモデルの素案を作成した。

作成した素案をもとに SWG のメンバーでレビューを行い、下記の意見を反映し修正を加えることとした。

・診断用ポート（OBDⅡ）を追加する。
・スマートキーの接続ルートを追加する。
・車外のサーバへのルートを追加する。
・ゲートウェイはセキュリティ機能の入っていないゲートウェイ（CAN GW）としての位置づけで記載する。
・車体系、駆動系、安全制御系の区分けは適切ではないので、ボディ系、パワートレイン・シャーシ系、安全系に改める。
・充電系は対象外とし、図に載せないこととする。

最終的にできあがったモデルを 図 2-3 に示す。

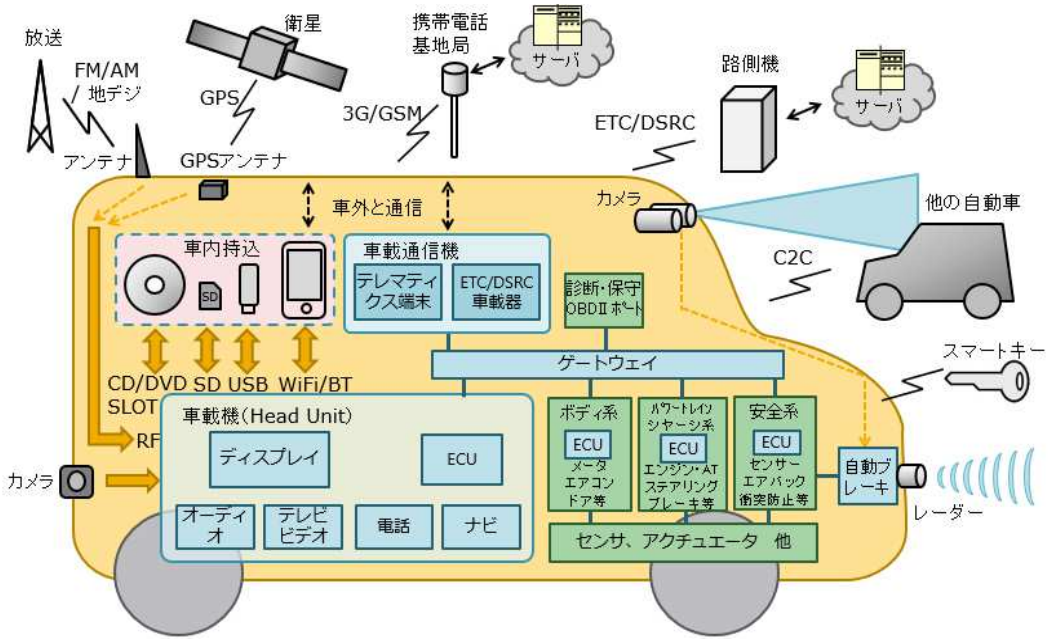


図 2-3 ガイドライン検討のシステムモデル

表 2-1 システム構成要素の説明

名称	説明
車載器	ナビ、オーディオ、車内電話など、ゲートウェイを介して外部と通信を行う装置。
車載通信機	有料道路の料金支払いやITSサービスにおいて路側機と必要な情報を交信、テレマティクス通信、また車車間通信を行うために設置する無線装置。
OBD-Ⅱポート	On-Board Diagnostics, II generation、車載の診断インターフェース
ゲートウェイ	車載システムにおいて二つの異なる通信手段または運用方針を持つネットワーク間の相互通信を行う。
ECU	Electronic Control Unit、自動車に搭載される数々のシステムを電子的に制御するユニット。
ETC	Electronic Toll Collection System、自動料金収受システム。
DSRC	Dedicated Short Range Communications、ITS（高度交通システム）サービスで路側機と交信、また車車間での通信を行う無線通信技術。
C2C	Car to Car Communication、車車間通信。
3G/GSM	第3世代移動通信システム（3rd Generation）／第2世代移動通信システム（Global System for Mobile communications）
GPSアンテナ	衛星から位置情報の通信を受信するアンテナ。
車内持込機器	車載器と有線、無線接続、装着接続によりデータ通信を行う機器。
Wi-Fi	Wi-Fi Allianceによって認定された、無線LANの規格。
BT	Bluetooth、デジタル機器用の近距離無線通信規格。
USB	Universal Serial Bus、コンピュータ等の情報機器に周辺機器を接続するためのシリアルバス規格。
SD	SD Card、携帯機器等で利用されるメモリーカード。
スマートキー	電子データを保持した自動車のキー。無線通信で車載コンピュータとデータ照合を行う。

3 想定されるセキュリティ上の脅威

3.1 車内持ち込み機器

スマートフォン、USB、SD などの持ち込み機器を接続インターフェースにつなげることによって外部からウイルス等の脅威が持ち込まれることが想定される。今後、自動車が連携する外部機器の種類は増加していくため、開発段階からあらゆる脅威に対する対策を講じることが重要になる。

3.2 外部ネットワークからの攻撃

スマートキー、GPS 情報、他の自動車との車車間通信、クラウド上のデータ活用など、外部通信を行うことによって、データの傍受や運転操作の乗っ取りなどの悪意のある攻撃に直面することが想定される。

❒ 遠隔から車載LANに侵入した研究事例

遠隔から車載 LAN に侵入してハンドル操作やエンジンを不正に制御した研究結果が Black Hat 2015 で発表され、対象車種 140 万台のリコールに繋がった事例も出ている。

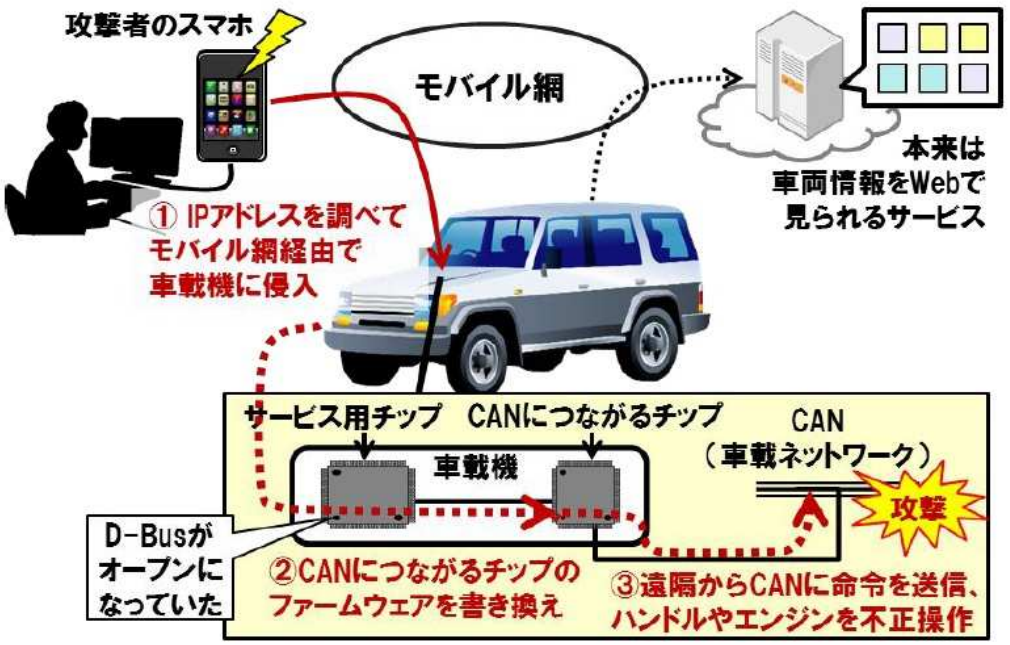


図 3-1 自動車に対する遠隔からの攻撃

3.3　車載器の想定脅威と想定被害

車載器で想定される脅威とその被害について以下に示す。

表 3-1 想定脅威と被害

項番	想定脅威	想定被害
1	外部ネットワーク経由で車載ネットワークに DoS 攻撃	通信機能を必要とする全サービスの利用停止
2	サーバなりすましによる虚偽メッセージの送信	利用者の混乱など
3	ブラウザのバグを利用したストリーミングコンテンツによるシステムのフリーズ	インフォテインメント系サービスの利用停止
4	第三者による受信機を用いた通信メッセージの盗聴	運用管理機関の意図しないサービスへの利用
5	第三者による GPS 信号発生器の悪用による、誤った位置を含むメッセージの配信	誤った位置を含むメッセージ配信による混乱の発生
6	利用者による車載器の悪用や第三者による通信機の利用により他の車載器へのなりすまし	誤った情報を含む走行情報配信による混乱
7	第三者による受信機の利用、利用者による車載器の悪用によって、受信メッセージから個人位置のトレース	個人のプロファイリング
8	3G/LTE 回線から第三者が定常運用時に故意に制御 ECU の制御機能を停止させる	ECU が正常に動作できなくなり車両機能が動作しない
9	スマートフォンなどの Bluetooth 機器からディーラ職員がメンテナンス時に車両状態情報を改ざんする	設定が不正に変更されて意図しない性能変更がなされる
10	SD カードインターフェースから第三者が定常運用時に故意にインフォメーション ECU のインフォメーション機能の誤作動を誘発する	インフォメーション機能が正常に動作しなくなる

4 ライフサイクルのフェーズとセキュリティの取組み

システム開発には計画から開発、運用、廃棄に至るまでのライフサイクルが存在する。そのすべてのフェーズにおいてセキュリティを考慮することが重要である。本章では各フェーズの定義とフェーズごとのセキュリティへの取組みについて説明する。

4.1 ライフサイクルにおけるフェーズの定義

自動車システムのライフサイクルのフェーズは、「企画」、「開発」、「運用」、「廃棄」の 4 つに分類され、提供する製品において十分なセキュリティを確保するには各フェーズにおいて十分な対策を施し、製品のセキュリティ品質を確実なものとする必要がある。

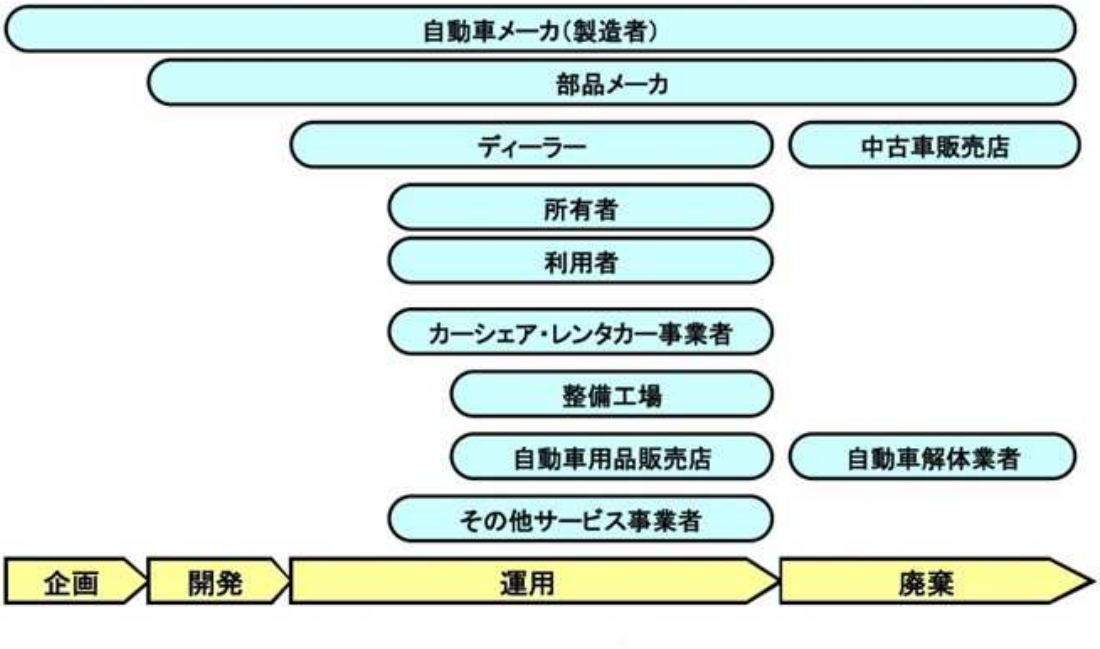


図 4-1 自動車システムのライフサイクル

※参照：IPA 「自動車の情報セキュリティへの取組みガイド」（2013 年）

表 4-1 フェーズの定義

フェーズ	説明
企画	製品のコンセプト、予算、要件定義の策定を行う。
開発	企画フェーズの要件定義を受けて設計・実装・製造を行う。
運用	ディーラから所有者（利用者）に販売され、利用者が使用している期間に、インシデントへの対応、整備、サービス等を行う。
廃棄	所有者が中古車として売却または廃車手続きを行う。

4.2　各フェーズにおけるセキュリティの取組み

本書は自動車システムのライフサイクルにおいて、運用・廃棄フェーズで発生する脅威に対応できる仕組みづくりを企画・開発フェーズで考慮しておくためのガイドラインとしてまとめた。前節で概説したライフサイクルの各フェーズに沿ってセキュリティへの取組み内容を説明する。

また、対策を実施するにはコストがかかることから、開発者だけでは対応が難しいことも多く、経営層の理解や全社的に支援が必要なことも多い。そこで、「企画」、「開発」、「運用」、「廃棄」のライフサイクル全体を通しての基本となる考え方を、「方針」のフェーズとして加え、経営者にも参考にしてもらえるようにした。

各フェーズにおけるセキュリティ取組みの指針一覧を以下に示し以降で説明する。

表 4-2 各フェーズにおけるセキュリティ取組みの指針一覧

フェーズ	項番	項目	取組みの指針
方針	1	基本方針	企業としての基本方針を作りましょう
	2	体制	企業として取り組むための体制を整えましょう
	3	教育	従業員への教育を定期的に実施しましょう
企画・開発	1	評価対象モデル	脅威分析を行う範囲を決めましょう
	2	脅威分析	脅威分析を行い、リスクを把握しましょう
	3	対策の検討	対策を考えましょう
	4	エビデンス	エビデンスを残しておきましょう
	5	設計の関係者	設計者、開発者、あるいは外注者は、信頼しない考え方でやりましょう
	6	評価・検証	セキュリティの評価・検証を行いましょう
	7	未知の脅威への対応	未知の脅威は必ず発生するものだと考えておきましょう
運用	1	取扱説明書	必要なことはすべて取説に書いておきましょう
	2	運用時の使われ方の定義	運用時の使われ方の範囲をきちんと定義しておきましょう
	3	ユーザへの注意喚起	ユーザに異常を気づいてもらえるようにしましょう
	4	アップデート	後からでも対策できるようにしておきましょう
	5	運用の関係者	関係者はすべて信用しないようにしましょう
	6	インシデント情報の共有	インシデント情報を共有し有効に活用しましょう
廃棄	1	難解析化	廃棄フェーズまで考慮した設計をしましょう
	2	初期リセット	初期状態にもどせるようにしておきましょう

4.2.1 方針フェーズ

方針フェーズにおけるセキュリティの取組みを以下に示す。

表 4-3 方針フェーズのセキュリティ取組み

項番	項目	指針	内容
1	基本方針	企業としての基本方針を作りましょう	① コストがかかることなので経営層へ理解を求める。（経営層に理解を求めるためにも、経営層への教育や公的機関による重要性の発信が必要。）
			② 取り巻く脅威の変化に応じて基本方針をアップデートする。
			③ どこまでやっていくのかの指針を検討する。（対策にコストが際限なくかかり製品が作れなくなくならないように、ある程度の指針を決めておく。）
2	体制	企業として取り組むための体制を整えましょう	① 企業によっては、組織横断的な活動となることが考えられるため、当該活動の統括責任者を設置する。
			② 取組みが継続的に運用され繰り返しサイクルで回る仕組みにする。
			③ インシデントレスポンスセンターは通常のお客様相談センターとは別に設置することが望ましい。 （市場における製品挙動に何か問題があった時に、通常のお客様相談センターが受けると、単なる製品の不具合に区分けされ、セキュリティの問題として受け取られない可能性が大きいので、専門のインシデントレスポンスセンターを設けて対応できるようにすることが望ましい。）
			④ 受けたインシデント情報の社内での報告経路・報告方法を決めておく。
			⑤ 今後、製品のセキュリティ関係者向けの資格制度を整備していくことが望ましい。
3	教育	従業員への教育を定期的に実施しましょう	① 基本方針の形骸化を防ぐため、従業員への教育を定期的に実施する。

			② 情報セキュリティの教育は対象者のレベルに応じて、いくつかのグループに分けて行うことが望ましい。 （CSIRT の担当者向け、開発者向け、ユーザ向け、管理者向け、経営者向けで教育の内容が変わるため。）
			③ 従業員がブラックにならないための教育も必要。⇒「4.2.2 企画・開発フェーズ」の項番 5「設計の関係者」の内容②も参照。

4.2.2 企画・開発フェーズ

企画・開発フェーズにおけるセキュリティの取組みを以下に示す。

表 4-4 企画・開発フェーズのセキュリティ取組み

項番	項目	指針	内容
1	評価対象モデル	脅威分析を行う範囲を決めましょう	① 対象のシステムを書く。
			② 想定接続先を書く。
			③ 接続口を明確にする。
			④ 隠れている I/F も全部書く。
			⑤ 網羅的にまず脅威候補をあげる。
2	脅威分析	脅威分析を行い、リスクを把握しましょう	① 最低でも一つの手法を用いて脅威分析をしてみる。できれば複数の評価手法で分析して違いを見てみることが望ましい。 （評価手法によって得意不得意があるので、別な手法でも脅威分析を行ってみるとよい。）
			② 攻撃者のモチベーションや過去の事例の有無をリスク評価に反映させると更によい。 （過去の事例があると攻撃の難易度が下がり、攻撃者のモチベーションが上がる傾向があるため。）
			③ 対策案を考えた後に再度脅威分析を行い、対策の効果を確認することが望ましい。 （対策の妥当性と費用対効果が確認できる。）
			④ インシデントによる企業リスクの評価も行う。

			⑤ 対策を入れると守るべき資産が増えるので、再度それを入れて脅威分析をする必要がある。
3	対策の検討	対策を考えましょう	① 対策案を羅列しておく。
			② 触れる・開けられるという前提で考える。
			③ 鍵管理をどこでやるか、誰の役割にするかを決める。
			④ 侵入経路としてサーバ側への出口のところも検討する。 （車載機器を踏み台として外部への攻撃の事例あり。）
			⑤ 接続される機器やアプリソフトの正当性を確認する。 （車載 SWG での脅威分析では「なりすまし」によるリスク値が高い。）
			⑥ 非正規の I/F 経由によるリスクに対する対策を検討する。
			⑦ 製品のバリューとリスク内容から、開発コストや対策に対する運用コストも考えて、どこまで対策を講じるかを事前に決めて設計に落とし込む。
			⑧ 最終製品を出すところが、全体のシステムとセキュリティの役割分担の方針を決め、下請けは役割分担に見合う条件を設定した上で、セキュリティに関する役割を担うようにすることが必要。
			⑨ 各レイヤー（物理、ネットワーク、アプリケーション）でできる対策案を羅列してみる。
			⑩ コストや仕様の制約で十分な対策が取れない場合、システム全体や上位のコンポーネントでの対策も検討する。
4	エビデンス	エビデンスを残しておきましょう	① 脅威に対するリスク分析と対策の検討結果、講じた対策の有効性や選んだ理由をドキュメントにまとめて残しておく。 （何か起きた時に、当時の実力ではここまではやったが、これ以上のことはわかりませんでしたという、自己責任の範囲を示せる証跡を残しておく。）

5	設計の関係者	設計者、開発者、あるいは外注者は、信頼しない考え方でやりましょう	① 誓約書を書かせる。
			② こういうことをやると人生棒に振るよというような研修で抑制も必要。（守秘義務の順守を求めるだけでなく、外注者への研修もできれば行った方がよい。）
			③ システム全体を知る設計者の数をミニマイズする。
			④ 鍵の管理をしっかり行う。（コストを考えなければ個々の鍵をユニークにする方が強くなる。）
6	評価・検証	セキュリティの評価・検証を行いましょう	① 最低限ファジングツールを使ったテストをするようにする。
			② 評価をするのに IN HOUSE でやる場合も、少なくとも 3rd パーティーのチェックを受けるようにした方が良い。
			③ 第三者によるリスク評価やセキュリティ検証を受けるのが望ましい。
7	未知の脅威への対応	未知の脅威は必ず発生するものだと考えておきましょう	① 考慮すべきことを書き出しておく。
			② 侵入検知や何かおかしな挙動がわかるようにしておくのが望ましい。
			③ 異常を検出した時には、機能を停止させるなど適切な対応がとれるようにしておくのが望ましい。
			④ ログを残し後から解析できるようにしておく。

4.2.3 運用フェーズ

運用フェーズにおけるセキュリティの取組みを以下に示す。

表 4-5 運用フェーズのセキュリティ取組み

項番	項目	指針	内容
1	取扱説明書	必要なことはすべて取説に書いておきましょう	① 免責事項にしてほしいことがあれば、取扱説明書に必ず書いておく。
			② 販売するときは、こういうことを考慮した製品になっていると表示するようにする。
2	運用時の使われ方の定義	運用時の使われ方の範囲をきちんと定義しておきましょう	① 運用時の使われ方の範囲や使用時の前提条件をきちんと定義して運用者に伝える。
3	ユーザへの注意喚起	ユーザに異常を気づいてもらえるようにしましょう	① 不審な機器が接続されている場合や、おかしな挙動を検知した場合に、ユーザに注意をうながす表示をする等の工夫をすることが望ましい。
			② 設定ミスのまま使われない工夫をすることが望ましい。 (ユーザやディーラなどの設定ミスにより、セキュリティが外れたままで使用されることの無いようにする。)
4	アップデート	後からでも対策できるようにしておきましょう	① セキュアにファームウェアをアップデートできる仕組みを講じておく。 (信頼できるサーバからセキュアブートの鍵付きでダウンロードするのが理想。)
			② リモートでアップデートできる仕組みを講じておくと更に望ましい。
5	運用の関係者	関係者はすべて信用しないようにしましょう	① 保守用のマニュアルが流出しても大丈夫なようにしておく。
			② 運用時の関係者に悪い人がいても大丈夫なようにしておく。
6	インシデント情報の共有	インシデント情報を共有し有効に活用しましょう	① 入手したインシデント情報を社内や関係事業者で共有し活用する仕組み作りも必要である。

4.2.4 廃棄フェーズ

廃棄フェーズにおけるセキュリティの取組みを以下に示す。

表 4-6 廃棄フェーズのセキュリティ取組み

項番	項目	指針	内容
1	難解析化	廃棄フェーズまで考慮した設計をしましょう	① 廃棄された基板を解析されても、解析しづらい設計をしておくことが望ましい。 （ツール接続時に認証を求めるのも１つの方法。）
			② ソフトウェアについても簡単に解析できないようにしておくことが望ましい。
2	初期リセット	初期状態にもどせるようにしておきましょう	① 初期状態にリセットできるようにしておく。

5 脅威分析について

5.1 脅威事例の収集

脅威分析を行うにあたり、車載 SWG で先行して検討を進めていた自動車関係の脅威事例の資料を活用することとした。車載 SWG では、国内外の発表文献を調査収集し、約 230 件の既知のインシデント事例を、「対象機器」、「分野固有・共通」、「脅威の分類」、「接続 I/F（侵入ルート）」などのリスク特性で分類し、「攻撃のしやすさ」と「被害の影響度」の評価項目を設定して「リスク値」を評価していた。表 5-1 に車載 SWG でインシデント事例を調査した文献リストを示す。

表 5-1 調査文献リスト

項番	調査文献	URL
1	2010 年度_自動車の情報セキュリティ動向に関する調査報告書, IPA	http://www.ipa.go.jp/files/000014119.pdf
2	2011 年度_自動車の情報セキュリティ動向に関する調査, IPA	https://www.ipa.go.jp/files/000024414.pdf
3	2011 年度自動車の情報セキュリティ動向に関する調査 付録編, IPA	http://www.ipa.go.jp/files/000014165.pdf
4	2012 年度_自動車の情報セキュリティ動向に関する調査, IPA	https://www.ipa.go.jp/files/000027274.pdf
5	Security requirements for automotive on-board networks based on dark-side scenarios, EVITA	http://evita-project.org/Deliverables/EVITAD2.3.pdf
6	自動車－情報セキュリティ分析ガイド_JASO TP15002,自技会	http://www.bookpark.ne.jp/cm/jsae/particulars.asp?content_id=JSAE-tp-15002-PDF
7	運転支援通信システムに関するセキュリティガイドライン, ITS フォーラム	http://www.itsforum.gr.jp/Public/J7Database/p41/ITS_FORUM_RC009V1_0.pdf
8	国内外の自動車の情報セキュリティ動向と意識向上策に関する調査報告書, IPA	https://www.ipa.go.jp/files/000014059.pdf
9	自動車と情報家電の組込みシステムのセキュリティ関する調査, IPA	http://www.ipa.go.jp/files/000013971.pdf
10	自動車のネットワーク化の将来と課題_つながる自動車のセキュリティ, IPA	http://home.jeita.or.jp/page_file/20141009110119_FYXUHuv50O.pdf
11	自動車の情報セキュリティへの取組みガイド, IPA	https://www.ipa.go.jp/files/000027273.pdf

12	車載ネットワークセキュリティの現状, FFRI	http://www.ffri.jp/assets/files/monthly_research/MR201310_Current%20state%20of%20automotive%20network%20security_JPN.pdf
13	車載組込みシステムの情報セキュリティ強化に関する提言, IPA	https://www.ipa.go.jp/files/000034668.pdf

5.2 リスク特性の項目

車載 SWG で収集したインシデント事例を利用して脅威分析を行うにあたり、リスク特性の項目を見直した。当初、車載 SWG で分類に用いていた、「対象機器」、「分野固有・共通」、「脅威の分類」、「接続 I/F（侵入ルート）」の 4 項目に加え、IPA のつながる世界の開発指針検討 WG でリスク特性の分類に用いていた「who 誰がつなげたか」、「whom 何が危害をうけたか」、「where どこで発生したか」の 3 項目を新たに追加した。見直したリスク特性の項目を、表 5-2 に示す。

表 5-2 リスク特性の項目

項番	項目	内容
1	対象機器	脅威に晒されている機器。
2	分野固有・共通	表 5-3 分野固有・共通 参照。
3	脅威の分類	表 5-4 脅威の分類の事例をリストアップ。 その分類基準は以下の通り。 ①利用者の操作に起因するもの。 ⇒“設定ミス／ウイルス感染” ②攻撃者による攻撃手段が明確なもの。 ⇒“盗聴／Dos 攻撃／偽メッセージ／不正中継” ③攻撃者による攻撃手段が不明確、もしくは上記に該当しないが被害を被った場合、以下に該当しているもの。 ⇒“不正設定／情報漏えい／ログ喪失” 上記の①②③に該当しない場合は、“不正利用”とする。
4	接続 I/F（侵入ルート）	表 5-5 接続 I/F（侵入ルート）参照。
5	who 誰がつなげたか	表 5-6 who 誰がつなげたか 参照。
6	whom 何が危害をうけたか	表 5-7 whom 何が危害をうけたか 参照。

7	where どこで発生したか	表 5-8 where どこで発生したか 参照。

■ 分野固有・共通

車載用だけでなく、今後 CCDS がカバーする他の重要生活機器へのツール汎用化を念頭に、本開発に関連する車分野に特化した事例を“分野固有”とし、車分野に関連するものの他の IoT 機器でも起こり得る事例を“共通”として分類を行った。

“分野固有／共通”の判別基準を、表 5-3 にまとめる。“分野固有／共通”のどちらにも該当しない場合は、個別に判断内容を記載した。

表 5-3 分野固有・共通

区分	説明
分野固有	対象が CAN や ECU の場合や、侵入ルートが DSRC や OBD の場合など、車載機器特有の機器や経路が関わっていると判断した場合は、「分野固有」。
共通	対象が車載機であっても、攻撃内容が一般的（フィッシングや Dos 攻撃）だと判断した場合は、「共通」。

■ 脅威の分類

「利用者の操作に起因する脅威」と「攻撃者による干渉に起因する脅威」の分類事例を、表 5-4 に示す。

表 5-4 脅威の分類

脅威	説明
設定ミス	自動車内のユーザインターフェースを介して、利用者が行った操作・設定が誤っていたことによりひきおこされる脅威。 ・インフォテイメント機能で意図しないサービス事業者に個人情報を送付してしまう、テレマティクスの通信の暗号機能を OFF にしてしまい通信情報が盗聴される、等
ウイルス感染	利用者が外部から持ち込んだ機器や記憶媒体によって、車載システムがウイルスや悪意のあるソフトウェア（マルウェア等）等に感染することによりひきおこされる脅威。 ・インフォテイメント機器に感染したウイルスが車載 LAN を通じて更に他の車載器に感染、等
不正利用	なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者に自動車システムの機能を利用される脅威。

	・解錠用の通信をなりすます事により、自動車の鍵を不正に解錠する、等
不正設定	なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者に自動車システムの設定値を不正に変更される脅威。 ・ネットワーク設定を変更し、正常な通信ができないようにする、等
情報漏えい	自動車システムにおいて保護すべき情報が、許可のされていない者に入手される脅威。 ・蓄積されたコンテンツや、各種サービスのユーザ情報が、機器への侵入や通信の傍受によって不正に読み取られる、等
盗聴	自動車内の車載器同士の通信や、自動車と周辺システムとの通信が盗み見られたり奪取されたりする脅威。 ・ナビゲーションや渋滞予測を行うサービスのために自動車から周辺システムに送付される自動車状態情報（車速、位置情報等）が途中経路で盗聴される、等
DoS 攻撃	不正もしくは過剰な接続要求によって、システムダウンやサービスの阻害をひきおこす脅威。 ・スマートキーに過剰な通信を実施し、利用者の要求（施錠・解錠）をできなくさせる、等
偽メッセージ	攻撃者がなりすましのメッセージを送信することにより、自動車システムに不正な動作や表示を行わせる脅威。 ・TPMS（タイヤ空気圧監視システム：Tire Pressure Monitoring System）のメッセージをねつ造し、実際には異常がない自動車の警告ランプをつける、等
ログ喪失	操作履歴等を消去または改ざんし、後から確認できなくする脅威。 ・攻撃者が自身の行った攻撃行動についてのログを改ざんし、証拠隠滅を図る、等
不正中継	通信経路を操作し、正規の通信を乗っ取ったり、不正な通信を混入させる脅威。 ・スマートキーの電波を不正に中継し、攻撃者が遠隔から自動車の鍵を解錠する、等

※参照：IPA　「自動車の情報セキュリティへの取組みガイド」（2013 年）

■ **接続 I/F（侵入ルート）**

脅威が侵入する際のルートを、表 5-5 に示す。

表 5-5 接続 I/F（侵入ルート）

接続 I/F	伝送距離	説明
3G/GSM	(ネットワーク圏内)	デジタル携帯電話の通信方式。
Bluetooth	0～10m	携帯情報機器などで数 m 程度の機器間接続に使われる短距離無線通信技術。
CD	0m	デジタル情報を記録するための光ディスク規格の一つ。
DSRC	0～30m	ITS で用いられる、路側機と走行する車の車載器間の無線通信。
E-コールサービスインターフェース	(ネットワーク圏内)	汎欧州自動緊急通報システム
GPS	受信範囲内	人工衛星を利用して自分が地球上のどこにいるのかを正確に割り出すシステム（Global Positioning System）。
OBD	0m	自動車に搭載されるコンピュータ（ECU）が行う自己故障診断機能（On-Board Diagnostics）。
RF	0～10m	スマートキーや車内通信用のワイヤレス通信。
SD	0m	メモリーカードの一種。
USB	0m	カーナビなどの情報機器に周辺機器を接続するためのシリアルバス規格（Universal Serial Bus）。
VICS	受信範囲内	渋滞や交通規制などの道路交通情報通信システム（Vehicle Information and Communication System）。FM 多重放送と電波ビーコンがある。
Wi-Fi	0～50m	ネットワーク接続に対応した機器を、無線（ワイヤレス）で接続する技術。
センサー	0m	車内センサー
特殊機材	0m	イモビカッターや保守用の専用ツールなど。

■ **who 誰がつなげたか**

IPA の「つながる世界の開発指針検討 WG」で検討中のリスク特性の整理方法にならい、つなげた者を、表 5-6 に示す。

表 5-6 who 誰がつなげたか

脅威	説明
メーカーや関連企業	メーカーが設計時に想定しているつながり。
サービス事業者	メーカーが設計時に想定していないつながり。
ユーザ（意図的）	ユーザによる意図的なつながり。
ユーザ（誤接続）	ユーザによる誤ったつながり。
攻撃者	脆弱性をついたつながり。
偶発的	色々つなげているときの偶発的なつながり。

※参照：IPA　「つながる世界の開発指針」（2016 年）

■ **whom 何が危害をうけたか**

IPA の「つながる世界の開発指針検討 WG」で検討中のリスク特性の整理方法にならい、危害の対象を、表 5-7 に示す。

表 5-7 whom 何が危害をうけたか

脅威	説明
IoT 機能 **（通信、連携、集約等）**	IoT アプリ、通信機能、セキュリティ対策のための機能など。
本来機能　（サーバ、GW、モノ等の機能）	機器やシステム本来の機能、セーフティ対策のための機能など。
情報	個人情報、決済情報、センサーデータなど。
身体や財産	ユーザの身体や財産など。
その他	自動販売機内の商品、ATM 内の現金、本体や部品など。

※参照：IPA　「つながる世界の開発指針」（2016 年）

■ **where どこで発生したか**

IPA の「つながる世界の開発指針検討 WG」で検討中のリスク特性の整理方法にならい、リスク発生箇所を、表 5-8 に示す。

表 5-8 where どこで発生したか

脅威	説明
通常使用 I/F	ユーザ用操作パネル、サービス用有線／無線 I/F、USB 端子など。
保守用 I/F	管理者用操作盤、遠隔管理用通信 I/F、ソフトウェア更新用の USB 端子など。
非正規 I/F	ふさぎ忘れた不要ポート、製造時にのみ使用する USB 端子など。
内包リスク	故障の原因となる欠陥やバグ、攻撃の対象となる脆弱性、故障や悪用で危害を及ぼす機能など。
物理的接触	直接、本体に接触。

※参照：IPA　「つながる世界の開発指針」（2016 年）

6 リスク評価の方法

脅威事例のリスク評価を行うにあたり、自動車関係の参考文献から車載関係のリスク評価手法としてどのようなものがあるのかを調査した。

6.1 ETSIの改良方式

ETSI（European Telecommunications Standard Institute、欧州電気通信標準化協会）のリスク評価は、「発生可能性」と「影響」に分け、それぞれ 3 段階で評価した値の積で、リスク値のクラス分けを行う手法となっている[1]。ETSI の「発生可能性」と「影響」の定義を、表 6-1 に、「リスク値」のクラス分けの定義を、表 6-2 に示す

表 6-1 ETSI の発生可能性と影響の定義

項目	値	ランク	定義
発生可能性	3	likely	脅威に対する十分な備えがなく、攻撃者のモチベーションはかなり高い。
	2	possible	攻撃にそれほど高い技術や努力は必要なく、攻撃者に合理的なモチベーションがあれば起こりうる。
	1	unlikely	最新の知識を用いても技術的に攻撃が難しく、攻撃者のモチベーションも低い。
影響	3	high impact	ビジネスに深刻なダメージを受ける。
	2	medium impact	影響があり無視することはできない。
	1	low impact	ダメージを受ける可能性は低い。

表 6-2 ETSI のリスク値のクラス分け

項目	値(積)	ランク	定義
リスク値	6,9	critical	重大なリスクが発生し最優先で対策が必要。
	4	major	致命的な影響がなくてもメジャーなリスクが発生する可能性がある。
	1,2,3	minor	マイナーなリスクは発生するが、対策を必要とするものではない。

車載 SWG では、リスク評価をするにあたり、発生可能性や影響度だけでなく、攻撃のしやすさ（特に先行事例の有無）や攻撃者のモチベーションを加味して評価を行うのが良いとの意見が出され、車載関係のリスク評価方法の参考文献を調べる中で、ETSI

（European Telecommunications Standard Institute）の改良方式を評価手法の１つとして参考にした。[2]、[3]

この評価手法では、「発生可能性」を「動機」と「技術的困難さ」に詳細化して評価する方法を採用している。「動機」と「技術的困難さ」の定義を、表 6-3 に示す。また、この改良方式では「動機」と「技術的困難さ」から「発生可能性」のランクを定義するので、この改良方式での「影響」の定義と共に、表 6-4 を示す。

表 6-3 ETSI 改良方式の動機と技術的困難さの定義

項目	ランク	定義
動機	High	攻撃する人や組織にとって多くの利益（報酬等）がある。
	Moderate	サービスの混乱（愉快犯等）
	Low	あまり利益は得られない。
技術的困難さ	None	技術的、経済的に容易に攻撃が可能（前例あり）。
	Solvable	理論的には攻撃が可能。
	Strong	理論的、技術的、経済的にも攻撃が大変困難。

表 6-4 ETSI 改良方式の発生可能性と影響の定義

項目	ランク	値	定義
発生可能性	Likely	3	すべての要素が存在する。
	Possible	2	いくつかの要素が存在する。
	Unlikely	1	重要な要素が抜けている。
影響	High	3	利用者やサービスに深刻な影響を与える。
	Medium	2	短期間のサービス停止に陥る。
	Low	1	利用者やサービスに影響を与える。

「リスク値」のクラス分けは ETSI 同様に「発生可能性」と「影響」の評価値の積で行っている.「リスク値」のクラス分けの定義を、表 6-5 に示す。

表 6-5 ETSI 改良方式のリスク値のクラス分け

項目	値(積)	ランク	定義
リスク値	9,6	Critical	対策は必須。
	4	Major	要注意。
	3,2,1	Minor	早急な対策は不要。

また、「動機」と「技術的困難さ」と「発生可能性」の評価値との関係と「影響」の評価値から、「リスク値」のクラス分けをマトリクス的に表したものを、表 6-6 に示す。ETSI 改良方式を用いることで、攻撃者のモチベーションを加味したリスク評価が行えるものと期待できる。

表 6-6 ETSI 改良方式のリスク値の定義

<table>
<tr><th rowspan="2">動機</th><th rowspan="2">技術的
困難さ</th><th rowspan="2">発生可能性</th><th colspan="3">影響</th></tr>
<tr><th>High(3)</th><th>Medium(2)</th><th>Low(1)</th></tr>
<tr><td rowspan="2">High</td><td>None</td><td rowspan="2">Likely(3)</td><td rowspan="3">Critical(9,6)</td><td rowspan="4">Minor(3,2,1)</td></tr>
<tr><td>Solvable</td></tr>
<tr><td rowspan="2">Moderate</td><td>None</td></tr>
<tr><td>Solvable</td><td>Possible(2)</td><td>Major(4)</td></tr>
<tr><td>Low</td><td>Any</td><td rowspan="2">Unlikely(1)</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>Any</td><td>Strong</td></tr>
</table>

6.2 CRSS方式（CVSSの応用方式）[4]

CRSS (CVSS based Risk Scoring System)は、情報システム・装置に対する脆弱性評価で実績のあるリスク評価手法である共通脆弱性評価システム CVSS（Common Vulnerability Scoring System）を応用したリスク評価手法である。

CVSS は FIRST (Forum of Incident Response and Security Teams)で策定され、情報システムの脆弱性に対する評価手法としては、広く利用されている手法だが、車載システムのように脅威による影響が、人体に影響を及ぼすよう甚大なものを想定していない。CRSS では、影響に関するパラメータの区分を、部分的→軽微、全面的→甚大とすることで、車載システムのリスク評価に対応している。

また、CRSS では CVSS の 3 つの評価基準のうち基本値を用いてリスク評価を行っている。CRSS で用いる基本評価値のパラメータを、表 6-7 に示す。基本評価値のパラメータを用いて、以下の式から「影響度」、「攻撃容易性」を求め、「基本値」からリスク値のクラス分けを行う。リスク値のクラス分けの定義を、表 6-8 に示す。

（1）影響度＝10.41×(1－(1－C)×(1－I)×(1－A))

（2）攻撃容易性＝20×AV×AC×Au

（3）f(影響度)＝0(影響度が 0 の場合)、1.176(影響度が 0 以外の場合)

（4）**基本値＝((0.6×影響度)＋(0.4×攻撃容易性)－1.5)×f(影響度)**

表 6-7 基本評価基準 (Base Metrics)

パラメータ	概要	区分	値
AV：攻撃元区分 (Access Vector)	脆弱性のあるシステムをどこから攻撃可能であるかを評価	ローカル	0.395
		隣接	0.646
		ネットワーク	1.0
AC：攻撃条件の複雑さ (Access Complexity)	脆弱性のあるシステムを攻撃する際に必要な条件の複雑さを評価	高	0.35
		中	0.61
		低	0.71
Au：攻撃前の認証要否 (Authentication)	脆弱性を攻撃するために対象システムの認証が必要であるかどうかを評価	複数	0.45
		単一	0.56
		不要	0.704
C：機密性への影響 (Confidentiality Impact)	脆弱性を攻撃された際に、対象システム内の機密情報が漏えいする可能性を評価	なし	0.0
		軽微	0.275
		甚大	0.660
I：完全性への影響 (Integrity Impact)	脆弱性を攻撃された際に、対象システム内の情報が改ざんされる可能性を評価	なし	0.0
		軽微	0.275
		甚大	0.660
A：可用性への影響 (Availability Impact)	脆弱性を攻撃された際に、対象システム内の機能が遅延・停止する可能性を評価	なし	0.0
		軽微	0.275
		甚大	0.660

表 6-8 リスク値のクラス分け

脅威レベル	リスク値 (基本値)
レベルⅢ(重大)	7.0～10.0
レベルⅡ(警告)	4.0～6.9
レベルⅠ(注意)	0.0～3.9

6.3　RSMA方式[4]

RSMA（Risk Scoring Methodology for Automotive system）は、「リスク値」を「影響度」と「発生可能性」のリスクレベル判定表によって決定する方式である。「影響度」は“セーフティ”、“個人情報／プライバシ”、“財産／企業価値”の 3 種類の被害分類に分けた上でレベルを決定する。また、「発生可能性」は“所要時間”、“専門知識”、“TOE の知識”、“機会”、“機器”の 5 つのパラメータから、表発生可能性レベル判定表により大、中、小の 3 段階で判定する。これらを、表 6-9、表 6-10 に示す。リスク値は「影響度」と「発生可能性」からマトリクス的に判定する。表 6-11 に判定表を示す

表 6-9 発生可能性パラメータ

パラメータ	説明	判定基準	
所要時間	脆弱性を識別して悪用するために要する時間	現実的	0
		非現実的	19
専門知識	必要な技術的専門知識	素人	0
		専門家	3
TOE の知識	攻撃対象（TOE）に限定した知識	公開情報	0
		ディーラ、開発・製造者が入手可能な情報	3
		一部の限定された者だけが入手できる情報	7
機会	攻撃対象（TOE）にアクセスする時間及び回数	アクセス不必要 アクセス必要／無制限でアクセス可能	0
		アクセスが必要／回数限定	4
		アクセスが必要／アクセス不可能	19
機器	攻撃に利用するハードウェア及びソフトウェア	市販製品（市販の HW・SW 製品など）	0
		特殊機器（ディーラが所有する製品など）	4
		特別注文品（開発専用の製品など）	8

表 6-10 発生可能性レベル判定表

発生可能性レベル	判定値
大	0～14
中	15～24
小	25 以上

表 6-11 リスクレベル判定表

被害分類	影響度	内容	発生可能性		
			小	中	大
セーフティ	なし	人に影響を及ぼさない	0	0	0
	小	軽症	L	L	M
	中	重症	L	M	H
	大	生命を脅かす	M	H	H
個人情報／プライバシ	なし	個人情報／プライバシでない	0	0	0
	小	単独では、個人の特定が困難な情報	L	L	M
	大	個人が特定できる情報	M	M	H
財産／企業価値	なし	財産／企業価値に影響を及ぼさない	0	0	0
	小	社内への影響だけ（事業への影響：小）	L	L	M
	中	お客様に影響（事業への影響：中）	L	M	H
	大	お客様及び事業に影響（事業への影響：大）	M	H	H

6.4 CCDS改良方式

車載 SWG では、「リスク値」を攻撃の「難易度」とユーザへの「影響度」についてランク付けして判定する方式を用いている。評価項目については、「共通脆弱性評価システム CVSS 概説」の情報を参考とし、初動段階において早期評価および開発を行う事を目的として、基本軸を「難易度」と「影響度」としている。

「難易度」は、攻撃の困難なものから簡単なものへ“S／A／B／C”の 4 段階とし、最も攻撃が容易な C ランクを 10 点とし、脅威度合が大きい程、点数が高くなるよう設定している。またセキュリティが無いものと 1 つでもあるものの点数差を 5 点差と幅を大きく取り、後は 2 点差とし、それぞれ 10／5／3／1 としている。

「影響度」は、“軽微／中程度／重大／破壊的”の 4 段階とし、影響度が最も大きい破壊的を 10 点として同様に数値化を行っている。

数値と内容については以下の表 6-12 に記載する。

表 6-12 攻撃の難易度と影響度の評価値

項目	項目の定義	ランク	ランクの定義	値
難易度	攻撃するために必要な条件（認証が必要、特別な権限が必要など）があるか。	S	複数の条件（認証、特別な権限など）が必要、かつ、ローカルからのみ接続（攻撃）が可能。	1
		A	単一の条件（認証、特別な権限など）が必要、かつ、ローカルからのみ接続（攻撃）が可能。	3
		B	一つ以上の条件（認証、特別な権限など）が必要、もしくは、ローカルからのみ接続（攻撃）が可能。	5
		C	攻撃するための条件が不要、かつ、無線ネットワークからの接続（攻撃）が可能。	10
影響度	攻撃された場合の影響度・影響範囲、二次的被害の影響度・影響範囲がどの程度のものか。	軽微	攻撃を受けてもユーザに影響がないか、もしくは、軽微な表示異常しか発生しない。なおかつ、漏洩する情報も個人を特定できるような情報は漏洩しない。	1
		中程度	攻撃を受けた場合に、ユーザに不利益をもたらす、もしくは、漏洩した情報から個人が特定される。	3
		重大	攻撃を受けた場合に、ユーザに不利益をもたらし、二次的被害も発生、もしくは、漏洩した情報から複数の個人が特定される。	5
		壊滅的	攻撃を受けた場合に、人命に関わるような被害、もしくは、二次的被害が発生する。	10

車載 SWG では、「攻撃者のモチベーション」が高いと脅威のリスクが上がる傾向があるので、「攻撃者のモチベーション」を加味したリスク評価を行うこととした。CCDS の方式をベースに、「攻撃者のモチベーション」を“小／中／大”の 3 段階とし、中の場合はリスク値が 1.25 倍に、大の場合はリスク値が 1.5 倍になるよう設定した。リスク値は下記の式で求める。

リスク値＝（難易度＋影響度）×攻撃者のモチベーション

「攻撃者のモチベーション」の定義を、表 6-13 に、また、リスク値のクラス分けの定義を、表 6-14 に示す。

表 6-13 攻撃者のモチベーションの定義

項目	ランク	定義	値
攻撃者のモチベーション	小	偶発的に発生し攻撃者には何の意図もない。	1
	中	実験や気晴らし、自己顕示などの目的を持つ。	1.25
	大	金銭的な利益を得たり、安全保障に影響を与えるなどの具体的な強い目的を持つ。	1.5

表 6-14 リスク値のクラス分け

リスク値	基準
Low	8 未満
Middle	8 以上 12 未満
High	12 以上 17 未満
Must	17 以上

7 リスク評価の結果

7.1 ETSIの改良方式

「リスク値」のクラス分けを最終的に「発生可能性」と「影響」の評価値の積で行っているため、リスク値が離散的で、更に中間ランクの Major は「4」の場合だけなので、他の方式に比べ Critical（赤色）や Minor（黄色）にばらつき易い傾向がある。表 7-1 に ETSI の改良方式でのリスク評価例を示す。

表 7-1 ETSI の改良方式でのリスク評価例

No	想定脅威	想定被害	対象機器	分野固有共通	脅威の分類	接続 I/F	who 誰がつなげたか	whom 何が危害をうけたか	where どこで発生したか	ETSI の改良方式				
										動機	技術的困難さ	発生可能性	影響	リスク値
1	外部ネットワーク経由で車載ネットワークに DoS 攻撃	通信機能を必要とする全サービスの利用停止	車載器	共通	DoS 攻撃	3G/GSM	攻撃者	IoT 機能	通常使用 I/F	Moderate	Solvable	2	3	6
2	サーバなりすましによる虚偽メッセージの送信	利用者の混乱など	車載器	共通	偽ﾒｯｾｰｼﾞ	3G/GSM	ﾕｰｻﾞ(誤接続)	IoT 機能	通常使用 I/F	Moderate	Solvable	2	2	4
3	ブラウザのバグを利用したストリーミングコンテンツによるシステムのフリーズ	インフォテインメント系サービスの利用停止	車載器	共通	偽ﾒｯｾｰｼﾞ	3G/GSM	ﾕｰｻﾞ(意図的)	IoT 機能	通常使用 I/F	Moderate	Solvable	2	2	4
4	第三者による受信機を用いた通信メッセージの盗聴	運用管理機関の意図しないサービスへの利用	車載器	共通	盗聴	Wi-Fi	攻撃者	情報	通常使用 I/F	High	Solvable	3	1	3
5	第三者による GPS 信号発生器の悪用による、誤った位置を含むメッセージの配信	誤った位置を含むメッセージ配信による混乱の発生	車載器	共通	不正中継	GPS	攻撃者	本来機能	通常使用 I/F	Moderate	Solvable	2	2	4
6	利用者による車載器の悪用や第三者による通信機の利用により他の車載器へのなりすまし	誤った情報を含む走行情報配信による混乱	車載器	共通	不正利用	3G/GSM	ﾕｰｻﾞ(意図的)	情報	通常使用 I/F	Moderate	Solvable	2	2	4
7	第三者による受信機の利用、利用者による車載器の悪用によって、受信メッセージから個人位置のトレース	個人のプロファイリング	車載器	分野固有	情報漏えい	Wi-Fi	攻撃者	情報	通常使用 I/F	High	Solvable	3	1	3
8	3G/LTE 回線から第三者が定常運用時に故意に制御 ECU の制御機能を停止させる	ECU が正常に動作出来なくなり車両機能が動作しない	ECU	分野固有	不正利用	3G/GSM	攻撃者	本来機能	通常使用 I/F	Moderate	Solvable	2	3	6
9	スマートフォンなどの Bluetooth 機器からディーラ職員がメンテナンス時に車両状態情報を改ざんする	設定が不正に変更されて意図しない性能変更がされる	車載器	分野固有	不正設定	Bluetooth	ｻｰﾋﾞｽ事業者	情報	通常使用 I/F	Moderate	Solvable	2	2	4
10	SD カードインターフェースから第三者が定常運用時に故意にインフォメーション ECU のインフォメーション機能の誤動作を誘発する	インフォメーション機能が正常に動作しなくなる	ECU	分野固有	不正利用	SD	攻撃者	本来機能	通常使用 I/F	Moderate	None	3	1	3

Critical(6,9)
Major(4)
Minor(3,2,1)

7.2　CRSS方式（CVSSの応用方式）

CRSS 方式では CVSS のオリジナルに比べ、車載システムのリスク評価に対応するため、「影響度」に関するパラメータ区分を、部分的→軽微、全面的→甚大としている。そのため情報処理に関する影響は軽微に区分され、車両の制御に関する影響は甚大に区分されるので、他方式に比べ「影響度」の数値が高くでない傾向にある。結果的にリスク値もレベルⅢ(重大)（赤色）が少ない。また、同じ脅威事例でも攻撃のルート（3G/GSM、Wi-Fi など）でリスク値が変わるのも特徴の 1 つとなっている。表 7-2 に CRSS 方式でのリスク評価例を示す。

表 7-2 CRSS 方式でのリスク評価例

No	想定脅威	想定被害	対象機器	分野固有共通	脅威の分類	接続I/F	who 誰がつなげたか	whom 何が危害をうけたか	where どこで発生したか	CRSS（CVSS の応用）								
										AV 攻撃元区分	AC 攻撃条件の複雑さ	Au 攻撃前の認証要否	攻撃容易性	C 機密性への影響	I 完全性への影響	A 可用性への影響	影響度	リスク値
1	外部ネットワーク経由で車載ネットワークに DoS 攻撃	通信機能を必要とする全サービスの利用停止	車載器	共通	DoS 攻撃	3G/GSM	攻撃者	IoT 機能	通常使用 I/F	ﾈｯﾄﾜｰｸ	低	単一	7.95	なし	軽微	軽微	4.94	5.46
2	サーバなりすましによる虚偽メッセージの送信	利用者の混乱など	車載器	共通	偽ﾒｯｾｰｼﾞ	3G/GSM	ﾕｰｻﾞ(誤接続)	IoT 機能	通常使用 I/F	ﾈｯﾄﾜｰｸ	低	単一	7.95	なし	軽微	軽微	4.94	5.46
3	ブラウザのバグを利用したストリーミングコンテンツによるシステムのフリーズ	インフォテインメント系サービスの利用停止	車載器	共通	偽ﾒｯｾｰｼﾞ	3G/GSM	ﾕｰｻﾞ(意図的)	IoT 機能	通常使用 I/F	ﾈｯﾄﾜｰｸ	低	単一	7.95	なし	軽微	軽微	4.94	5.46
4	第三者による受信機を用いた通信メッセージの盗聴	運用管理機関の意図しないサービスへの利用	車載器	共通	盗聴	Wi-Fi	攻撃者	情報	通常使用 I/F	隣接	中	複数	3.55	軽微	なし	なし	2.86	1.92
5	第三者による GPS 信号発生器の悪用による、誤った位置を含むメッセージの配信	誤った位置を含むメッセージ配信による混乱の発生	車載器	共通	不正中継	GPS	攻撃者	本来機能	通常使用 I/F	ﾈｯﾄﾜｰｸ	低	なし	10.00	なし	軽微	軽微	4.94	6.42
6	利用者による車載器の悪用や第三者による通信機の利用により他の車載器へのなりすまし	誤った情報を含む走行情報配信による混乱	車載器	共通	不正利用	3G/GSM	ﾕｰｻﾞ(意図的)	情報	通常使用 I/F	ﾈｯﾄﾜｰｸ	低	単一	7.95	なし	軽微	軽微	4.94	5.46
7	第三者による受信機の利用、利用者による車載器の悪用によって、受信メッセージから個人位置のトレース	個人のプロファイリング	車載器	分野固有	情報漏えい	Wi-Fi	攻撃者	情報	通常使用 I/F	隣接	中	複数	3.55	軽微	軽微	なし	4.84	3.39
8	3G/LTE 回線から第三者が定常運用時に故意に制御 ECU の制御機能を停止させる	ECU が正常に動作出来なくなり車両機能が動作しない	ECU	分野固有	不正利用	3G/GSM	攻撃者	本来機能	通常使用 I/F	ﾈｯﾄﾜｰｸ	中	単一	6.83	なし	甚大	甚大	9.21	7.95
9	スマートフォンなどの Bluetooth 機器からディーラ職員がメンテナンス時に車両状態情報を改ざんする	設定が不正に変更されて意図しない性能変更がされる	車載器	分野固有	不正設定	Bluetooth	ｻｰﾋﾞｽ事業者	情報	通常使用 I/F	隣接	低	単一	5.14	軽微	軽微	なし	4.94	4.14
10	SD カードインターフェースから第三者が定常運用時に故意にインフォメーション ECU のインフォメーション機能の誤動作を誘発する	インフォメーション機能が正常に動作しなくなる	ECU	分野固有	不正利用	SD	攻撃者	本来機能	通常使用 I/F	ﾛｰｶﾙ	低	なし	3.95	なし	軽微	なし	2.86	2.11

レベルⅢ(重大)
レベルⅡ(警告)
レベルⅠ(注意)

7.3　RSMA方式

「影響度」は被害分類で区分けして評価するものの、「影響度」の評価値がリスクレベル判定表の 1 つの評価軸となっているため、ストレートにリスク値に反映される。一方、リスクレベル判定表のもう 1 つの評価軸である「発生可能性」は、「所要時間」、「専門知識」、「TOE の知識」、「機会」、「機器」の 5 つのパラメータの評価値の合計によりレベルが決まる方式となっている。他方式に比べ評価パラメータが多く、「影響度」と「発生可能性」の評価パラメータ数のバランスに差がある。表 7-3 に RSMA 方式でのリスク評価例を示す。

表 7-3 RSMA 方式でのリスク評価例

No	想定脅威	想定被害	対象機器	分野固有共通	脅威の分類	接続 I/F	who 誰がつなげたか	whom 何が危害をうけたか	where どこで発生したか	RSMA 方式								
										被害分類	影響度	所要時間	専門知識	TOE の知識	機会	機器	発生可能性	リスク値
1	外部ネットワーク経由で車載ネットワークに DoS 攻撃	通信機能を必要とする全サービスの利用停止	車載器	共通	DoS 攻撃	3G/GSM	攻撃者	IoT 機能	通常使用 I/F	財産・企業価値	中	現実的	専門家	一部の限定者	アクセス不必要・無制限	市販製品	大	H
2	サーバなりすましによる虚偽メッセージの送信	利用者の混乱など	車載器	共通	偽メッセージ	3G/GSM	ユーザ(誤接続)	IoT 機能	通常使用 I/F	財産・企業価値	中	現実的	専門家	一部の限定者	アクセス不必要・無制限	特別注文品	中	M
3	ブラウザのバグを利用したストリーミングコンテンツによるシステムのフリーズ	インフォテインメント系サービスの利用停止	車載器	共通	偽メッセージ	3G/GSM	ユーザ(意図的)	IoT 機能	通常使用 I/F	財産・企業価値	中	現実的	専門家	一部の限定者	アクセス不必要・無制限	特別注文品	中	M
4	第三者による受信機を用いた通信メッセージの盗聴	運用管理機関の意図しないサービスへの利用	車載器	共通	盗聴	Wi-Fi	攻撃者	情報	通常使用 I/F	個人情報・プライバシ	小	現実的	専門家	ディーラ開発製造者	アクセス回数限定	特別注文品	中	L
5	第三者による GPS 信号発生器の悪用による、誤った位置を含むメッセージの配信	誤った位置を含むメッセージ配信による混乱の発生	車載器	共通	不正中継	GPS	攻撃者	本来機能	通常使用 I/F	財産・企業価値	中	現実的	専門家	公開情報	アクセス回数限定	市販製品	大	H
6	利用者による車載器の悪用や第三者による通信機の利用により他の車載器へのなりすまし	誤った情報を含む走行情報配信による混乱	車載器	共通	不正利用	3G/GSM	ユーザ(意図的)	情報	通常使用 I/F	財産・企業価値	中	現実的	専門家	一部の限定者	アクセス回数限定	特別注文品	中	M
7	第三者による受信機の利用、利用者による車載器の悪用によって、受信メッセージから個人位置のトレース	個人のプロファイリング	車載器	分野固有	情報漏えい	Wi-Fi	攻撃者	情報	通常使用 I/F	個人情報・プライバシ	小	現実的	専門家	一部の限定者	アクセス回数限定	特別注文品	中	L
8	3G/LTE 回線から第三者が定常運用時に故意に制御 ECU の制御機能を停止させる	ECU が正常に動作出来なくなり車両機能が動作しない	ECU	分野固有	不正利用	3G/GSM	攻撃者	本来機能	通常使用 I/F	セーフティ	大	現実的	専門家	ディーラ開発製造者	アクセス不必要・無制限	特殊機器	大	H
9	スマートフォンなどの Bluetooth 機器からディーラ職員がメンテナンス時に車両状態情報を改ざんする	設定が不正に変更されて意図しない性能変更がされる	車載器	分野固有	不正設定	Bluetooth	サービス事業者	情報	通常使用 I/F	財産・企業価値	小	現実的	専門家	ディーラ開発製造者	アクセス回数限定	特殊機器	大	M
10	SD カードインターフェースから第三者が定常運用時に故意にインフォメーション ECU のインフォメーション機能の誤動作を誘発する	インフォメーション機能が正常に動作しなくなる	ECU	分野固有	不正利用	SD	攻撃者	本来機能	通常使用 I/F	財産・企業価値	小	現実的	専門家	ディーラ開発製造者	アクセス不可能	特殊機器	小	L

7.4　CCDS改良方式

基本的な評価項目を「難易度」と「影響度」の２つとしているため、簡便にリスク評価をすることができる。また、他方式に比べ、リスク値のランクを４段階としているため、上下にばらつきが大きくでることや、中心化する傾向も緩和されている。攻撃者のモチベーションをリスク値に反映させる工夫もおこなっている。独自方式のため、リスク評価結果の妥当性に懸念があったが、他の３方式と同じ脅威事例を用いてリスク評価を行った結果、方式毎に若干の差はあるものの、同じ傾向を示した。表 7-4 に CCDS 改良方式でのリスク評価例を示す。

表 7-4 CCDS 改良方式でのリスク評価例

No	想定脅威	想定被害	対象機器	分野固有共通	脅威の分類	接続 I/F	who 誰がつなげたか	whom 何が危害をうけたか	where どこで発生したか	CCDS 改良方式			
										難易度	影響度	攻撃者のﾓﾁﾍﾞｰｼｮﾝ	リスク値
1	外部ネットワーク経由で車載ネットワークに DoS 攻撃	通信機能を必要とする全サービスの利用停止	車載器	共通	DoS 攻撃	3G/GSM	攻撃者	IoT 機能	通常使用 I/F	C	重大	中	Must
2	サーバなりすましによる虚偽メッセージの送信	利用者の混乱など	車載器	共通	偽ﾒｯｾｰｼﾞ	3G/GSM	ﾕｰｻﾞ(誤接続)	IoT 機能	通常使用 I/F	C	中程度	中	High
3	ブラウザのバグを利用したストリーミングコンテンツによるシステムのフリーズ	インフォテインメント系サービスの利用停止	車載器	共通	偽ﾒｯｾｰｼﾞ	3G/GSM	ﾕｰｻﾞ(意図的)	IoT 機能	通常使用 I/F	C	中程度	中	High
4	第三者による受信機を用いた通信メッセージの盗聴	運用管理機関の意図しないサービスへの利用	車載器	共通	盗聴	Wi-Fi	攻撃者	情報	通常使用 I/F	B	軽微	中	Low
5	第三者による GPS 信号発生器の悪用による、誤った位置を含むメッセージの配信	誤った位置を含むメッセージ配信による混乱の発生	車載器	共通	不正中継	GPS	攻撃者	本来機能	通常使用 I/F	B	中程度	中	Middle
6	利用者による車載器の悪用や第三者による通信機の利用により他の車載器へのなりすまし	誤った情報を含む走行情報配信による混乱	車載器	共通	不正利用	3G/GSM	ﾕｰｻﾞ(意図的)	情報	通常使用 I/F	B	中程度	中	Middle
7	第三者による受信機の利用、利用者による車載器の悪用によって、受信メッセージから個人位置のトレース	個人のプロファイリング	車載器	分野固有	情報漏えい	Wi-Fi	攻撃者	情報	通常使用 I/F	B	軽微	中	Low
8	3G/LTE 回線から第三者が定常運用時に故意に制御 ECU の制御機能を停止させる。	ECU が正常に動作出来なくなり車両機能が動作しない	ECU	分野固有	不正利用	3G/GSM	攻撃者	本来機能	通常使用 I/F	B	壊滅的	大	Must
9	スマートフォンなどの Bluetooth 機器からディーラ職員がメンテナンス時に車両状態情報を改ざんする。	設定が不正に変更されて意図しない性能変更がされる	車載器	分野固有	不正設定	Bluetooth	ｻｰﾋﾞｽ事業者	情報	通常使用 I/F	C	中程度	中	High
10	SD カードインターフェースから第三者が定常運用時に故意にインフォメーション ECU のインフォメーション機能の誤動作を誘発する。	インフォメーション機能が正常に動作しなくなる	ECU	分野固有	不正利用	SD	攻撃者	本来機能	通常使用 I/F	B	中程度	中	Middle

Must
High
Middle
Low

8 リスク評価の傾向分析

リストアップした脅威事例のリスク評価結果を用いて、「分野固有・共通」、「脅威の分類」、「接続 I/F（侵入ルート）」、「who　誰がつなげたか」、「whom　何が危害を受けたか」、「where　どこで発生したか」の 6 つのリスク特性について項目別の傾向分析を行った。

リスク評価の傾向分析は、リストアップした約 230 件の既知のインシデント事例に対しリスク分析が完了していたことから、CCDS 改良方式のリスク評価の結果を用いて分析を行った。6 つのリスク特性について、それぞれの区分項目毎に Must、High、Middle、Low の件数をカウントすると共に、“リスク値平均”と、それぞれの区分毎の合計件数のうち Must と High の件数の割合を“M&H 比率”として数値化した。これらの数値から区分項目毎のリスク傾向を分析した。

8.1　分野固有・共通の傾向分析

表 8-1 に分野固有・共通の傾向分析を示す。「分野固有」と「共通」の“M&H 比率”に大差はないが、最上位のリスクレベルである“Must”だけの比率で比較すると 46.0%と 24.6%となり、車両の制御に関する影響など車分野に特化した脅威事例を扱う「分野固有」の方が、他の IoT 機器でも起こり得る情報処理に関する事例の多い「共通」に比べると“Must”の比率がはるかに多い。「分野固有」の方がより甚大な影響を与える脅威事例が多いことがわかる。

他の重要生活機器を含めた各分野共通のセキュリティガイドラインやセキュリティ検証基盤を整備していくことは重要なことだが、今後、より甚大な影響を与える脅威に対処していくためには、分野毎のガイドライン策定や分野毎のセキュリティ検証基盤の整備についても、平行してすすめていく必要があると考える。

表 8-1 分野固有・共通の傾向分析

区分	Must	High	Middle	Low	件数計	リスク値平均	M&H 比率	Must 比率
分野固有	80	44	38	12	174	17.0	71.3%	46.0%
共通	14	26	13	4	57	14.5	70.2%	24.6%

8.2　脅威の分類の傾向分析

表 8-2 に脅威の分類の傾向分析を示す。脅威の分類の 10 項目の中で、“M&H 比率”が高い項目は「不正利用」と「偽メッセージ」であった。表 5-4 に示したように、「不正利用」は、なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者に自動車システムの機能を利用される脅威であり、「偽メッセージ」は、攻撃者がなりすましのメッセージを送信することにより、自動車システムに不正な動作や表示を行わせる脅威である。どちらの項目も、なりすましを利用した攻撃であることを考えると、自動車システムの運用フェーズにおいて、なりすましに対する対策の必要性をガイドラインに盛り込み考慮すべきと考える。

また、「設定ミス」は“M&H 比率”は低いが、ユーザの設定ミスが原因でセキュリティが外れた状態のまま知らずに使っている場合があり、セキュリティ上、何でもありの状態となり、大きな脅威につながる可能性があるので注意が必要である。

表 8-2 脅威の分類の傾向分析

区分	Must	High	Middle	Low	件数計	リスク値平均	M&H 比率
設定ミス	2	0	2	0	4	14.8	50.0%
ウイルス感染	14	7	8	0	29	17.3	72.4%
不正利用	33	18	10	2	63	18.1	81.0%
不正設定	3	8	2	2	15	14.4	73.3%
情報漏えい	0	1	1	6	8	7.2	12.5%
盗聴	3	3	2	2	10	13.2	60.0%
DoS 攻撃	21	12	18	3	54	15.1	61.1%
偽メッセージ	17	16	3	0	36	19.7	91.7%
ログ喪失	0	0	0	1	1	7.5	0.0%
不正中継	1	5	5	0	11	12.5	54.5%

8.3　接続I/F（侵入ルート）の傾向分析

表 8-3 に接続 I/F（侵入ルート）の傾向分析を示す。一般的に「OBD」は、ここから攻撃されると弱いと考えられているが、他の侵入ルートより“M&H 比率”が低く出た。これは傾向分析に用いた CCDS 改良方式のリスク評価では、CVSS 方式を参考にした「難易度」の評価を行っているため、ローカルからの攻撃は無線ネットワークからの攻撃よりも「難易度」が高くなり、リスク値が低くでる傾向があるためと考えられる。

一方、遠隔操作できる「3G/GSM」や「Wi-Fi」も一般的にリスク値が高く出ると予想していたが、他の侵入ルートより“M&H 比率”が低く出た。これは車載器を対象とした情報処理に関する脅威事例が多く、「影響度」が“中程度”から“軽微”となり、リスク値が低く出る事例が多かったためと考えられる。

表 8-3 接続 I/F（侵入ルート）の傾向分析

区分	Must	High	Middle	Low	件数計	リスク値平均	M&H 比率
3G/GSM	17	15	12	3	47	16.4	68.1%
Bluetooth	7	3	2	0	12	18.4	83.3%
CD	1	2	0	0	3	20.8	100.0%
DSRC	0	3	0	0	3	15.4	100.0%
E-コールサービスインターフェース	1	2	0	0	3	16.3	100.0%
GPS	4	4	1	0	9	17.4	88.9%
OBD	25	8	11	4	48	16.4	68.8%
RF	13	11	2	2	28	18.3	85.7%
SD	2	0	3	0	5	16.0	40.0%
USB	2	3	4	0	9	14.3	55.6%
VICS	0	3	0	0	3	15.4	100.0%
Wi-Fi	12	11	12	2	37	15.5	62.2%
センサー	2	0	0	0	2	18.8	100.0%
特殊機材	6	5	4	5	20	12.9	55.0%

8.4　who 誰がつなげたかの傾向分析

表 8-4 に who 誰がつなげたかの傾向分析を示す。「サービス事業者」の“M&H 比率”が他よりも高めに出ているが、「サービス事業者」はメーカーが設計時に想定していないつながりのため、もともと脅威事例のユースケースを考えていないし、リスクを想定していない。このためリスク値が高めに出ていると考えられる。

表 8-4 who 誰がつなげたかの傾向分析

区分	Must	High	Middle	Low	件数計	リスク値平均	M&H 比率
メーカーや関連企業	0	0	0	0	0	－	－
サービス事業者	0	5	0	1	6	11.5	83.3%
ユーザ（意図的）	0	10	12	0	22	12.5	45.5%
ユーザ（誤接続）	2	2	2	0	6	15.3	66.7%
攻撃者	92	53	37	15	197	17.0	73.6%
偶発的	0	0	0	0	0	－	－

8.5　whom 何が危害をうけたかの傾向分析

表 8-5 に whom 何が危害をうけたかの傾向分析を示す。「IoT 機能」の“M&H 比率”が他よりも高めに出ているが、この攻撃の特徴は無線ネットワークからの攻撃の場合が多く、「難易度」が低く出るために、リスク値が高めとなる傾向があることである。自動車システムの場合、個人情報や決済情報といった「情報」に危害を与えることよりも、攻撃者は無線ネットワークからの攻撃により、まず「IoT 機能」を不正利用することや乗っ取ることで、ここを足がかりに遠隔操作し、よりリスクの高い脅威を仕掛けてくる可能性が考えられる。今後ますます自動車システムが、他の IoT 機器との接続や連携して動作するような世の中になっていくことを考えると、これらの脅威への対応は必須であると考えられる。

表 8-5 whom 何が危害をうけたかの傾向分析

区分	Must	High	Middle	Low	件数計	リスク値平均	M&H 比率
IoT 機能（通信、連携、集約等）	5	23	2	2	32	15.4	87.5%
本来機能　（サーバ、GW、モノ等の機能）	74	25	31	4	134	17.8	73.9%
情報	14	19	19	10	65	13.7	55.4%
身体や財産	0	0	0	0	0	－	－
その他	1	3	0	0	1	19.5	100.0%

8.6　where どこで発生したかの傾向分析

表 8-6 に where どこで発生したかの傾向分析を示す。「通常使用 I/F」と「保守用 I/F」の“M&H 比率”に大差はないが、最上位のリスクレベルである“Must”だけの比率で比較すると 37.2%と 55.8%となり、「保守用 I/F」の“Must”の比率の方が多い。管理者が操作やソフトウェアの更新に使用する「保守用 I/F」や「非正規 I/F」は、隠されているし公表されていないので攻撃に使われないと想定していると、プロはそこから侵入してくるので、注意する必要がある。

表 8-6 where どこで発生したかの傾向分析

区分	Must	High	Middle	Low	件数計	リスク値平均	M&H 比率	Must 比率
通常使用 I/F	58	55	36	7	156	16.7	72.4%	37.2%
保守用 I/F	29	8	11	4	52	16.6	71.2%	55.8%
非正規 I/F	5	7	3	4	19	13.0	63.2%	26.3%
内包リスク	0	0	0	0	0	－	－	－
物理的接触	1	0	1	1	3	13.8	33.3%	33.3%

9 まとめ

本書は車載器分野を対象としたセキュリティガイドラインとして作成したが、想定される脅威やライフサイクルにおけるセキュリティの取組みなど、他の分野でも応用できるところがあると考えられる。様々な製品の開発プロセスにおいてセキュリティ対策を考慮するにあたり、本ガイドラインを積極的に活用して欲しい。

今後、IoT（Internet of Things）の普及とともに、今までスタンドアロンで機能していた身の回りにある生活機器が、様々な接続機能を持つことで便利になる一方で、これらの機器に対する攻撃が益々増加してくるものと予想される。特に車載システムへの攻撃事例の報告は近年増加傾向にあり、メディアに大きく取り上げられ紹介されることも多く、車のセキュリティに対する関心が急速に高まっている。これらの新しいユースケースや脅威に対応し、セキュリティを考慮した設計・開発を進めていくためには、引き続き下記の見直しをはかる必要があると考えられる。

① 脅威事例のアップデートを行い、脅威分析や対策の検討に反映させる。

② 新しいユースケースに対応したシステムを想定し脅威分析を行うことで、要求仕様と対策を検討する。

また、脅威事例のリスク評価やリスク特性毎の傾向分析から、攻撃者は車内持ち込み機器や、外部ネットワークとの接続部分から侵入し、なりすましなどで乗っ取りを試み、これを足がかりにしてよりリスクの高い脅威を仕掛けてくる可能性があることがわかった。CCDS では分野別セキュリティガイドラインの策定と合わせ、セキュリティ検証基盤形成事業の中で、各社が IoT 機器のセキュリティ評価・検証ツールの開発を進めている。車載器分野でも２種類の評価・検証ツールを開発している。ぜひ、これらの評価・検証ツールを用いて、脅威の侵入口となる可能性の高い車載器とのインターフェース部分から、手始めに検査してみることを強くお勧めする。

最後に本書をまとめるにあたり、車載 SWG のメンバーに多大なるご支援をいただき、謝意を表したい。

10「つながる世界の開発指針」と本書との関係

2016 年 3 月に IPA（独立行政法人情報処理推進機構）から「つながる世界の開発指針」がリリースされた。この指針は、IoT 機器やシステムを開発するメーカーに向けて、従前の安全基準対応だけでなく、セキュリティ対応にも目を向けた開発を実施してもらうため、基本的な実施すべき項目をセキュリティガイドラインとして策定したものである。CCDS からも 4 名の委員が参加し策定に協力した。本書と「つながる世界の開発指針」の策定は、相互に検討状況を共有しながら同時期に進められてきたこともあり、「つながる世界の開発指針」が分野を特定しない IoT に関する業界横断的な指針とすると、本書はそれを受けて策定された車載システムの個別分野に関する指針という位置づけとなる。「つながる世界の開発指針」と本書との対応について表 10-1 と表 10-2 に示す。相互に参照し利用いただきたい。

表 10-1 「つながる世界の開発指針」と本書の対応表 1

「つながる世界の開発指針」			本書での対応箇所	
大項目		指針	章番号	概要
方針	つながる世界の安全安心に企業として取り組む	指針1 安全安心の基本方針を策定する	4.2.1	1項に企業としての基本方針への取り組み内容①～③を記載。
		指針2 安全安心のための体制・人材を見直す	4.2.1	2項に企業として取り組むための体制について内容①～⑤を記載。3項に人材育成に必要な教育について内容①～③を記載。
		指針3 内部不正やミスに備える	4.2.1	3項に内部不正に対する教育として内容③を記載。
			4.2.2	5項に関係者の不正防止対応について内容①～④を記載。
			4.2.3	3項②や5項①に設定ミスやマニュアル流出に対する注意を記載。
			8.2	脅威の分類の傾向分析で、設定ミスに対する注意喚起を記載。
分析	つながる世界のリスクを認識する	指針4 守るべきものを特定する	5.2	脅威分析を行う際のリスク特性にIPAの整理方法にならい「whom 何が危害をうけたか」を採用し、守るべきものを明確化。
			7.1～7.4	守るべきものを特定したうえで脅威事例のリスク評価を実践。
			8.5	何が危害を受けたかのリスク特性について傾向分析を行った結果を記載。
		指針5 つながることによるリスクを想定する	2.2	図2.3に検討のシステムモデルを記載し車載システムの接続箇所を明確化。
			4.2.2	1項でつながるリスクを想定するための内容①～⑤を記載。 3項の対策の検討で③鍵管理、⑥非正規I/Fを検討項目の内容として記載。
			5.2	脅威分析を行う際のリスク特性にIPAの整理方法にならい「who 誰がつなげたのか」「where どこで発生したか」を採用し、つなげた者やつながることによるリスク発生箇所を明確化。
			7.1～7.4	つなげた者やリスク発生箇所を特定したうえで脅威事例のリスク評価を実践。
			8.4、8.6	つなげた者やリスク発生箇所のリスク特性について傾向分析を行った結果を記載。
		指針6 つながりで波及するリスクを想定する	5.2	脅威分析を行う際のリスク特性の中で脅威の分類を示し、つながりで波及するリスクとして「ウィルス感染」「不正利用」「DoS 攻撃」などの脅威分類を掲示。
			7.1～7.4	脅威の分類を明確にしたうえで脅威事例のリスク評価を実践。
			8.2	脅威の分類のリスク特性について傾向分析を行った結果を記載。
		指針7 物理的なリスクを認識する	3.2	図3-1に自動車に対する遠隔からの攻撃事例を記載。
			4.2.4	1、2項に廃棄フェーズでの取組み内容として記載。
			8.5、8.6	遠隔操作や保守用I/F・非正規I/Fからの攻撃に対する注意喚起を記載。

表 10-2 「つながる世界の開発指針」と本書の対応表 2

「つながる世界の開発指針」			本書での対応箇所	
大項目		指針	章番号	概要
設計	守るべきものを守る設計を考える	指針8 個々でも全体でも守れる設計をする	4.2.2	3項の対策の検討の⑨⑩に記載。
			5.2	「where どこで発生したか」の中で外部インターフェース経由のリスク、内包リスク、物理的接触によるリスクを記載。
			7.1～7.4	リスク発生箇所を特定したうえで脅威事例のリスク評価を実践。
			8.2	脅威の分類の傾向分析でなりすましに対する対策の必要性を記載。
			8.6	どこで発生したかの傾向分析で保守用I/F・非正規I/Fからの攻撃に対する注意喚起を記載。
		指針9 つながる相手に迷惑をかけない設計をする	4.2.2	7項に未知の脅威への対応として内容①～④を記載。
		指針10 安全安心を実現する設計の整合性をとる	4.2.2	2項の脅威分析と4項のエビデンスに対応の内容を記載。
			5章～7章	脅威分析のやり方とリスク評価について、4つの手法を用いて評価事例を記載。4.2.2　2項①で複数の評価手法での分析を推奨したり、2項③で対策後の再評価に活用するため記載。
		指針11 不特定の相手とつなげられても安全安心を確保できる設計をする	4.2.2	3項の対策の検討の⑤に記載。ただし正当性の確認だけで、つながる相手やつながる状況によるつながり方の対応までは言及していない。
		指針12 安全安心を実現する設計の検証・評価を行う	4.2.2	6項に評価・検証として内容①～③を記載。
			5章～7章	脅威分析を行う際のリスク特性にIPAの整理方法にならい「who 誰がつなげたのか」「whom 何が危害をうけたか」「where どこで発生したか」を加え、守るべきもの、つながり方、リスク箇所等を明確にした上でリスク評価し、リスク度に応じた対策の検討の必要性を記載。
保守	市場に出た後も守る設計を考える	指針13 自身がどのような状態かを把握し、記録する機能を設ける	4.2.2	7項④にログについての内容を記載。
		指針14 時間が経っても安全安心を維持する機能を設ける	4.2.3	4項にアップデートとして内容①～②を記載。
運用	関係者と一緒に守る	指針15 出荷後もIoTリスクを把握し、情報発信する	4.2.3	6項にインシデント情報の共有として内容を記載。
			9章	今後の課題として脅威事例のアップデートと新しいユースケースに対応した脅威分析の継続の必要性を記載。
		指針16 出荷後の関係事業者に守ってもらいたいことを伝える	4.2.3	2項に運用時の使われ方の定義として内容を記載。
		指針17 つながることによるリスクを一般利用者に知ってもらう	4.2.3	1項に取扱説明書としてユーザーに守ってほしい内容①～②を記 3項にユーザーへの注意喚起として内容①～②を記載。

11「自動車の情報セキュリティへの取組みガイド」と本書との関係

本書を策定するにあたり、IPA（独立行政法人 情報処理推進機構）から 2013 年 3 月に発行された「自動車の情報セキュリティへの取組みガイド」を参照した。「自動車の情報セキュリティへの取組みガイド」と本書との対応について表 11-1 に示す。前章の「つながる世界の開発指針」と本書との対応と合わせ、相互に参照し利用いただきたい。

表 11-1 「自動車の情報セキュリティへの取組みガイド」と本書の対応表

「自動車の情報セキュリティへの取組みガイド」				本書での対応箇所	
章	章題	章番号	内容	章番号	概要
1	はじめに	1.1.	自動車セキュリティの現状と課題	1.1	車載器のセキュリティの現状と課題
		1.2.	本書のねらい	1と1.2	1 はじめにに本書のねらいと1.2章に本書の対象者を記載。
2	自動車システムとセキュリティ	2.1.	自動車システムのモデル	2.1と1.2	2.1 対象のモデルと2.2 検討対象のシステムモデルに記載。
		2.2.	自動車システムにおいて想定されるセキュリティ上の脅威	3.1～3.3	想定されるセキュリティ上の脅威を記載。
		2.3.	脅威に対するセキュリティ対策	–	対策の具体的内容については本書では記載していない。
		2.4.	機能・脅威・対策技術のマッピング	–	対策の具体的内容については本書では記載していない。
3	自動車システムにおけるセキュリティへの取組み	3.1.	自動車システムのライフサイクル	4,1	自動車システムのライフスタイルを引用し記載。
		3.2.	セキュリティの取組みレベルとフェーズ毎の取組み方針	–	フェーズ毎の取組み方針については本書では記載していない。
4	セキュリティへの取組みの詳細	4.1.	マネジメントにおける取組み	4.2.1	方針フェーズの取組みを記載。
		4.2.	企画フェーズにおける取組み	4.2.2	企画・開発フェーズの取組みを記載。
		4.3.	開発フェーズにおける取組み	4.2.2	企画・開発フェーズの取組みを記載。
		4.4.	運用フェーズにおける取組み	4.2.3	運用フェーズの取組みを記載。
		4.5.	廃棄フェーズにおける取組み	4.2.4	廃棄フェーズの取組みを記載。

参考文献

[1] ETSI : Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis. Technical Specification ETSI TS 102 165-1 V4.1.1, 2003.

[2] C. Laurendeau and M. Barbeau : Threats to Security in DSRC/WAVE. ADHOC-NOW 2006, LNCS 4104, pp. 266otocol Harm

[3] ITS 情報通信システム推進会議 : 運転支援通信システムに関するセキュリティガイドライン. ITS FORUM RC-009 1.0 版, 2011.

[4] 公益社団法人自動車技術会 : JASO テクニカルペーパ　自動車－情報セキュリティ分析ガイド, JASO TP15002, 2015.