製品分野別セキュリティガイドライン
車載器編　v2.0

平成29年5月29日

CCDS セキュリティガイドラインWG
車載 SWG

目次構成

CCDS

章	節	項		章	節	項	
1			はじめに	6			リスク評価の方法
	1.1		車載器のセキュリティの現状と課題		6.1		ETSIの改良方式
	1.2		本書のねらいと対象者		6.2		CRSS方式（CVSSの応用方式）
	1.3		略称		6.3		RSMA方式
2			車載ガイドラインのシステムモデル		6.4		CCDS改良方式
	2.1		対象のモデル	7			リスク評価の結果
	2.2		検討対象のシステムモデル		7.1		ETSIの改良方式
3			想定されるセキュリティ上の脅威		7.2		CRSS方式（CVSSの応用方式）
	3.1		車内持ち込み機器		7.3		RSMA方式
	3.2		外部ネットワークからの攻撃		7.4		CCDS改良方式
	3.3		車載器の想定脅威と想定被害	8			リスク評価の傾向分析
4			ライフサイクルのフェーズとセキュリティの取組み		8.1		分野固有・共通の傾向分析
	4.1		ライフサイクルにおけるフェーズの定義		8.2		脅威の分類の傾向分析
	4.2		各フェーズにおけるセキュリティの取組み		8.3		接続I/F（侵入ルート）の傾向分析
		4.2.1	方針フェーズ		8.4		who 誰がつなげたかの傾向分析
		42.2	企画・開発フェーズ		8.5		whom 何が危害をうけたかの傾向分析
		4.2.3	運用フェーズ		8.6		where どこで発生したかの傾向分析
		4.2.4	廃棄フェーズ	9			まとめ
5			脅威分析について	10			「つながる世界の開発指針」と本書との関連
	5.1		脅威事例の収集	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
	5.2		リスク特性の項目	12			「IoTセキュリティガイドライン」と本書との関係
							参考文献

1. 現状と課題

１．車載器セキュリティの現状

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。Black Hat 2015で報告されたJEEPのハッキング成功事例など、車載器への攻撃の脅威は拡大している。

２．車載器におけるセキュリティ対策の必要性

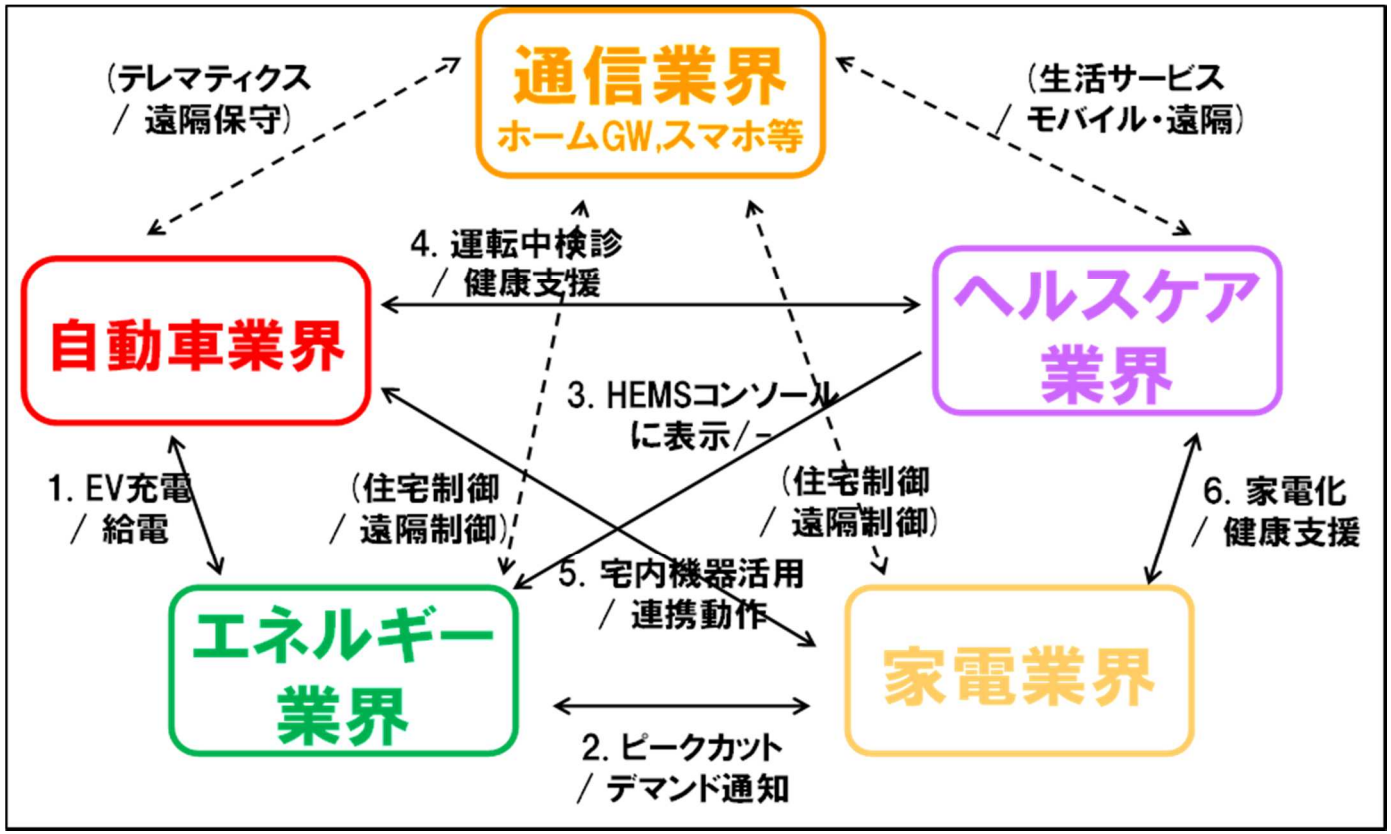
車がハッキングされた際の被害は人命に係るほど非常に甚大であり、開発技術者のみならず責任者や経営陣がセキュリティに対してどのように取り組んでいくべきかが課題となっている。

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。

2. システムモデル–その1–

■ つながる範囲検討の参考モデル

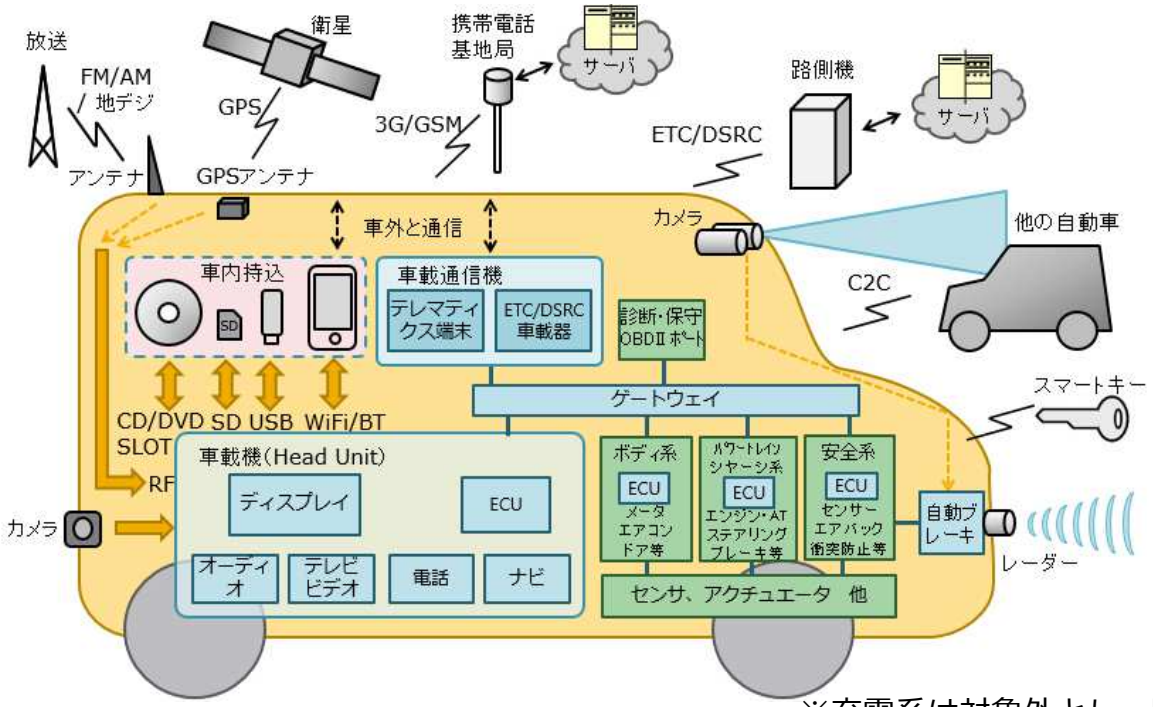
対象とする車載システムの範囲を検討するにあたり、下図を参考にして、接続インターフェースを考えることとした。また、検討の範囲はヘッドユニット周りをモデル化し、そこに接続されているものを基本とする。検討対象のモデル化にあたっては、既に発表されている資料を参考にして検討を行った。



2. システムモデル–その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。



※充電系は対象外とし、図に載せないこととする。

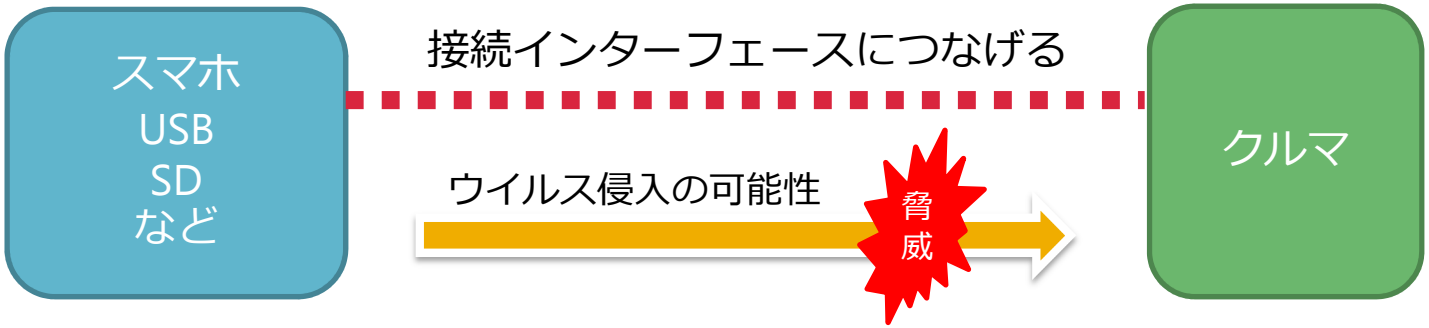
2. システムモデル–その3–

■システムモデルの構成要素

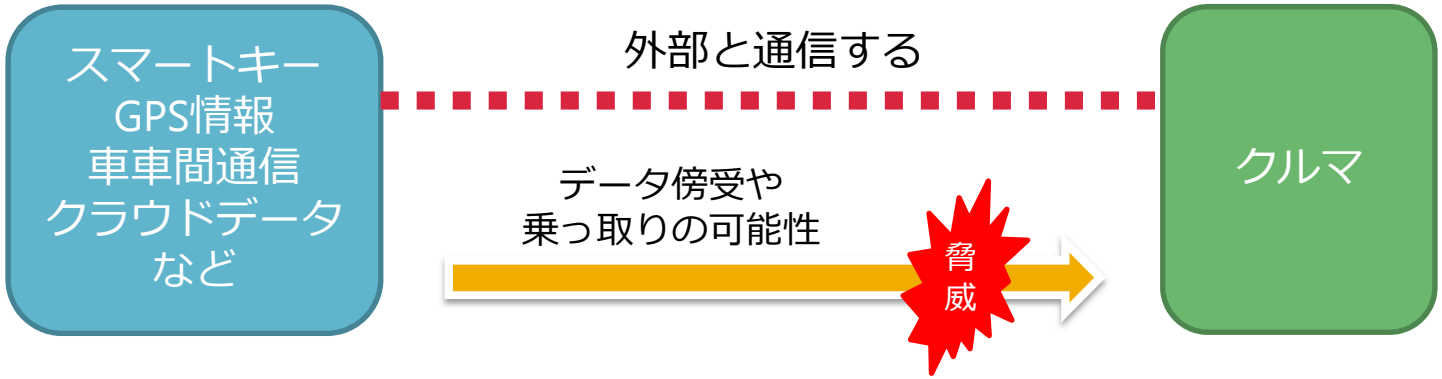
項番	構成要素	機能
1	車載器	ナビ、オーディオ、車内電話など、ゲートウェイを介して外部と通信を行う装置。
2	車載通信機	有料道路の料金支払いやITSサービスにおいて路側機と必要な情報を交信、テレマティクス通信、また車車間通信を行うために設置する無線装置。
3	OBD–Ⅱポート	On-Board Diagnostics, II generation、車載の診断インターフェース
4	ゲートウェイ	車載システムにおいて二つの異なる通信手段または運用方針を持つネットワーク間の相互通信を行う。
5	ECU	Electronic Control Unit、自動車に搭載される数々のシステムを電子的に制御するユニット。
6	ETC	Electronic Toll Collection System、自動料金収受システム。
7	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。
8	C2C	Car to Car Communication、車車間通信。
9	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）
10	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。
11	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。
12	Wi-Fi	Wi-Fi Allianceによって認定された、無線LANの規格。
13	BT	Bluetooth、デジタル機器用の近距離無線通信規格。
14	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。
15	SD	SD Card、携帯機器等で利用されるメモリーカード。
16	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. 想定される脅威–その1–

■車内持ち込み機器

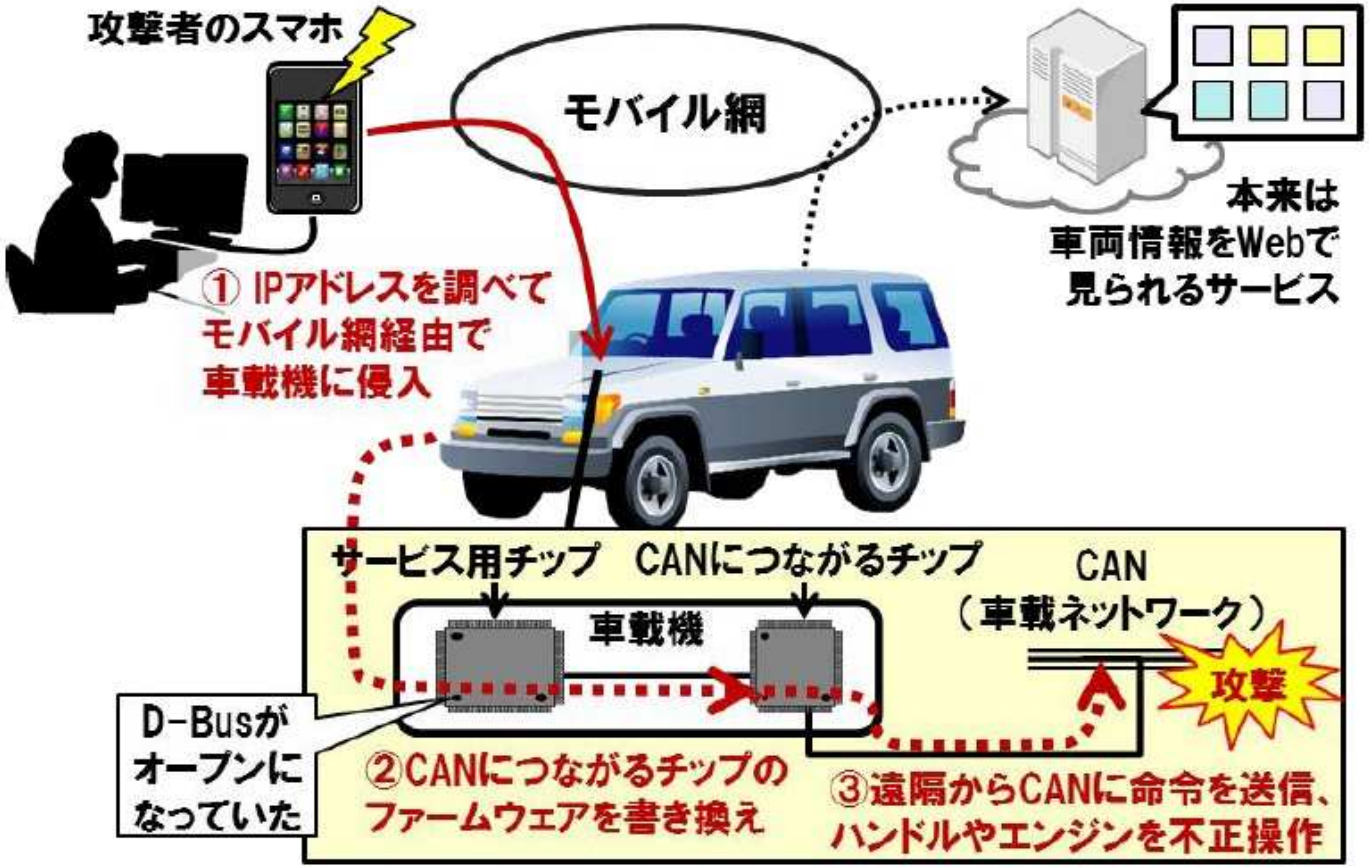


■外部ネットワーク



3. 想定される脅威–その2–

■遠隔から車載LANに侵入した研究事例（Blackhat 2015での発表事例）



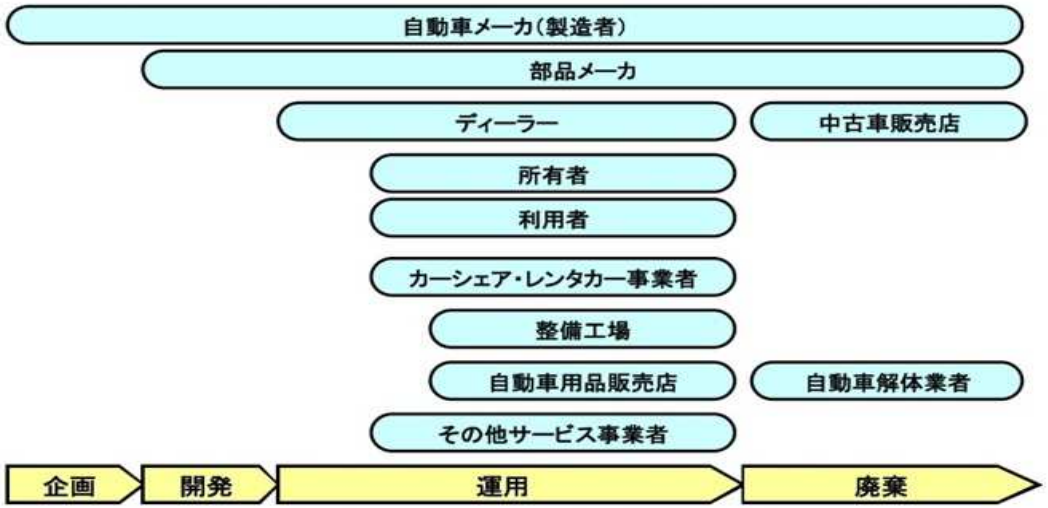
3. 想定される脅威–その3–

■想定される脅威と被害

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の通信機の利用による路側機のなりすまし（路側機なりすまし	誤った情報を含むメッセージ配信による混乱
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

■自動車システムのライフサイクルにおける4つのフェーズ



フェーズ	説明
企画フェーズ	製品のコンセプト、予算、要件定義の策定を行う。
開発フェーズ	企画フェーズの要件定義を受けて設計・実装・製造を行う。
運用フェーズ	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。
廃棄フェーズ	所有者が中古車として売却または廃車手続きを行う。

経営者にも参考にしてもらえるよう、これらにライフサイクル全体を通しての基本となる考え方を「方針フェーズ」として加えた。

4. 各フェーズの取組み–その1–

各フェーズにおけるセキュリティの取組み指針を以下に示す。

■方針フェーズ

項番	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。⇒「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. 各フェーズの取組み–その2–

■企画・開発フェーズ

項番	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。

4. 各フェーズの取組み–その3–

■企画・開発フェーズ（続き）

項番	指針	内容
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。）

4. 各フェーズの取組み–その4–

■企画・開発フェーズ（続き）

項番	指針	内容
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 セキュリティの評価・検証を行いましょう	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. 各フェーズの取組み–その5–

■運用フェーズ

項番	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こう	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. 各フェーズの取組み–その6–

■廃棄フェーズ

項番	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–その1–

■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	参照☞「（1）分野固有・共通」
3	脅威の分類	脅威の分類の事例をリストアップ。 参照☞「（2）脅威の分類」 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／ウィルス感染” 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）	参照☞「（3）接続I/F（侵入ルート）」
5	who 誰がつなげたか	参照☞「（4）who 誰がつなげたか」
6	whom 何が危害をうけたか	参照☞「（5）whom 何が危害をうけたか」
7	where どこで発生したか	参照☞「（6） where どこで発生したか 」

5. 脅威分析について–その2–

（1）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」。

（2）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
ウィルス感染	利用者が外部から持ち込んだ機器や記憶媒体によって、車載システムがウィ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ィルスが車載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

5. 脅威分析について–その3–

（2）脅威の分類（つづき）

脅威	説明
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

5. 脅威分析について–その4–

（3）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。

5. 脅威分析について–その5–

（4）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。

（5）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。

5. 脅威分析について–その6–

（6）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、サービス用通信I有線／無線/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。

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

1）ETSIの改良方式

ETSI（European Telecommunications Standard Institute、欧州電気通信標準化協会）のリスク評価法をベースに、「発生可能性」を「動機」と「技術的困難さ」に細分化して評価し、これに「影響」の評価を行い、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

2）CRSS方式（CVSSの応用方式）

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。

3）RSMA方式

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。

4）CCDS改良方式

CCDS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。

7. リスク評価の結果–その1–

同一の脅威事例を４つの手法を用いてリスク評価した結果を以下に示す。

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。

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

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

7. リスク評価の結果–その2–

2）CRSS方式（CVSSの応用方式）

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

レベルⅢ(重大)
レベルⅡ(警告)
レベルⅠ(注意)

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

7. リスク評価の結果–その3–

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、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

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	偽ﾒｯｾｰｼﾞ	3G/GSM	ﾕｰｻﾞ(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	偽ﾒｯｾｰｼﾞ	3G/GSM	ﾕｰｻﾞ(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・ﾌﾟﾗｲﾊﾞｼ	小	現実的	専門家	ﾃﾞｨｰﾗ開発製造者	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	ﾕｰｻﾞ(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・ﾌﾟﾗｲﾊﾞｼ	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	ﾃﾞｨｰﾗ開発製造者	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	ｻｰﾋﾞｽ事業者	情報	通常使用I/F	財産・企業価値	小	現実的	専門家	ﾃﾞｨｰﾗ開発製造者	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	ﾃﾞｨｰﾗ開発製造者	ｱｸｾｽ不可能	特殊機器	小	L

7. リスク評価の結果–その4–

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

Must
High
Middle
Low

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

8. リスク評価の傾向分析–その1–

4つのリスク評価方法のうち、**CCDS改良方式のリスク評価の結果を用いて傾向分析**を行った結果を以下に示す。「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。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”、Mustの件数の割合を“Must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。

（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%

「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。

8. リスク評価の傾向分析–その2–

（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%

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。「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。“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になってしまうことも考慮する必要がある。

8. リスク評価の傾向分析–その3–

（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%

「OBD」は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。CCDS改良方式では、CVSS方式を参考にした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。

8. リスク評価の傾向分析–その4–

（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	–	–

「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。

8. リスク評価の傾向分析–その5–

（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%

「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。

8. リスク評価の傾向分析–その6–

（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%

「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。

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、車載システムへの攻撃事例の報告が増えてくるものと考えられる。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。

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。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。

10. 「つながる世界の開発指針」と本書との関係

■「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。

10. 「つながる世界の開発指針」と本書との関係

■「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が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。

10. 「つながる世界の開発指針」と本書との関係

■「つながる世界の開発指針」と本書の対応表3

「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
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を記載。 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

■「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。

12. 「IoTセキュリティガイドライン」と本書との関係

■「IoTセキュリティガイドライン ver1.0」と本書の対応表１

「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	
大項目	指針	内容	章番号	概要
方針	指針１ IoT の性質を考慮した基本方針を定める	要点1. 経営者がIoT セキュリティにコミットする	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。
			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。
		要点2. 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	指針２ IoT のリスクを認識する	要点3. 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。
		要点4. 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。 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。
			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。

12. 「IoTセキュリティガイドライン」と本書との関係

■「IoTセキュリティガイドライン ver1.0」と本書の対応表２

「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	
大項目	指針	内容	章番号	概要
分析	指針２ IoT のリスクを認識する	要点5. つながりで波及するリスクを想定する	5.2	脅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。
		要点6. 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。
		要点7. 過去の事例に学ぶ	4.2.3	6項に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の必要性を記載。
			5.1、8章	国内外の発表文献を調査収集した約230件の既知のインシデント事例を用い、リスク評価の傾向分析結果を記載。
設計	指針３ 守るべきものを守る設計を考える	要点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。
		要点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。

12. 「IoTセキュリティガイドライン」と本書との関係

■「IoTセキュリティガイドライン ver1.0」と本書の対応表３

「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	
大項目	指針	内容	章番号	概要
設計	指針３ 守るべきものを守る設計を考える	要点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。
		要点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。
		要点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。
構築・接続	指針４ ネットワーク上での対策を考える	要点13. 機器等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。
		要点14. 機能及び用途に応じて適切にネットワーク接続する	4.2.2	3項の対策の検討の⑩に、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検討を記載。
		要点15. 初期設定に留意する	4.2.3	4項にソフトウェアアップデートについて内容①～②を記載。
		要点16. 認証機能を導入する	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。
			4.2.2	3項の対策の検討の⑤に接続される機器やアプリソフトの正当性の確認を記載。

12. 「IoTセキュリティガイドライン」と本書との関係

■「IoTセキュリティガイドライン ver1.0」と本書の対応表４

「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	
大項目	指針	内容	章番号	概要
運用・保守	指針５ 安全安心な状態を維持し、情報発信・共有を行う	要点17. 出荷・リリース後も安全安心な状態を維持する	4.2.3	4項にアップデートとして内容①～②を記載。
		要点18. 出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える	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。
			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。
		要点19. 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を記載。 3項にユーザーへの注意喚起として内容①～②を記載。
		要点20. IoT システム・サービスにおける関係者の役割を認識する	4.2.2	3項の対策の検討の⑧に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ることを記載。
		要点21. 脆弱な機器を把握し、適切に注意喚起を行う	4.2.3	3項にユーザーへの注意喚起として内容①～②を記載。