

博士論文  
令和6年度

自動車等サイバーフィジカルシステムの  
特定の領域や観点に合わせた  
セキュリティ設計におけるリスクの分析手法に関する研究

京都産業大学大学院  
先端情報学研究科  
博士後期課程 3 年  
186258  
川西 康之

Doctoral Thesis  
FY2024

Studies on risk analysis methods in security design that takes into  
consideration fitting to specific areas or viewpoints of  
cyber-physical systems such as automotive systems

By  
Yasuyuki Kawanishi  
186258  
Faculty of Frontier Informatics  
Graduated School of  
Kyoto Sangyo University

**Abstract:** This research is concerned with improving the efficiency of security design methods for cyber-physical systems, mainly targeting automotive systems. Due to the introduction of ICT (Information and Communication Technologies), automotive systems in recent years have become cyber-physical systems that require countermeasures not only from a safety perspective but also from a security perspective. Cyber-attacks can be carried out on these systems using the same means as ICT systems, and the results of these attacks can lead to accidents. Since the successful control takeover experiment by hacking the Jeep Cherokee in 2015, the vulnerabilities in automotive systems can bring serious impacts, and a cyber-attack on automotive system such as the actual theft of vehicles by CAN invader is a problem. In response to this situation, there is an urgent need to implement security designs for automotive systems like those for ICT systems.

A Security design is a process of creating system specifications for security as well as functionality and safety. First, based on a system model that organizes functions and data flows from system specifications, functions and data that should be protected are identified as assets. Next, evaluate the degree of the risk based on the attack feasibility and the severity of damage to the asset caused by the cyber-attack. Then, a decision is made as to whether to avoid, reduce or accept the risk, and a countermeasure policy is determined. Finally, the security requirements are identified, which are necessary to realize the countermeasures and incorporate them into the design specifications. Guidelines such as JASO TP15002 (2015) and ISO/SAE 21434 (2021) define the procedures for performing these tasks during system development. These are based on standards for assessing the vulnerability of IT products, and use methods that incorporate perspectives such as safety, financial, operational, and privacy to evaluate the attack feasibility and the severity of damage sustained on automotive systems. Moreover, the latter also stipulates recurrent risk management such as re-evaluating security risks after product release more practically.

One of the issues in risk analysis of such security design concerns the validity of the analysis. In other words, there is a need for a risk quantification method that can perform appropriate analysis according to the actual situation of the system being analyzed. The CAN invader mentioned above is a cyber-attack that uses a wired connection to the in-vehicle network, and in the past, it was thought to be difficult to attack because it required intruding into the car and wiring work. However, there was a communication line connected to important functions just after the front bumper was removed, and an attack that exploited this was successful. A quantification method that can predict such risks is required.

In this paper, I examined a risk quantification method that allows for more detailed differentiation in accordance with the areas and perspectives specific to cyber-physical systems, and I applied the software vulnerability evaluation standard CWSS (Common Weakness Scoring System) to cyber-physical systems. I proposed it as RSS-CWSS\_CPS that was applied to the metric evaluation criteria and customized the metric evaluation criteria. Then, I clarified what aspects this method emphasizes when quantifying risk through a detailed analysis of partial differentiation of the CWSS calculation formula for each metric and evaluated direct access attacks on automotive systems such as the CAN Invader. Although direct access attacks are effective for cybercrime, conventional risk quantification methods have shown that the risk is lower than attacks via long-distance wireless communication. However, this method also identified direct access attacks as important threats, confirming that this risk quantification method can perform evaluations that are consistent with the actual situation of the system being analyzed.

**Keywords:** In-vehicle security, security design, risk analysis, TARA, ISO/SAE 21434, JASO TP15002, CWSS, CVSS.

**概要:** 本研究は、自動車システムを主なターゲットとした、サイバーフィジカルシステムのセキュリティ設計手法の効率化に係る研究である。近年の自動車システムは ICT(Information and Communication Technologies: 情報通信技術)の導入により、ICT システムと同様の手段でサイバー攻撃が実施でき、その攻撃の結果が事故につながるなど、単にセキュリティのみならずセーフティの観点でも対策が必要なサイバーフィジカルシステムとなっている。2015 年の Jeep Cherokee のハッキングによる制御乗っ取り実験の成功以来、自動車システムの脆弱性がもたらしうる深刻な影響が予測され、近年でも CAN インバーダーによる車両盗難が現実に行われるなど、自動車システムへのサイバー攻撃が問題となっている。そのような情勢を受け、自動車システムにおいても ICT システム同様のセキュリティ設計を行うことが急務となっている。

セキュリティ設計は、機能やセーフティと同様に、セキュリティに関してシステム仕様を作るプロセスである。まずシステム仕様書から機能やデータフローを整理したシステムモデルを基に、守るべき機能やデータを資産として抽出する。次に資産への攻撃のしやすさや攻撃により受けた損害の深刻度からリスクの大小を評価する。そしてリスクを回避・軽減するのか受け入れるのかなど取り扱いを決め、対策方針を決定する。最後に対策方針を実現するために必要なセキュリティ要件を洗い出し、設計仕様に盛り込む。これらの作業をシステム開発時に行う手順を定めたのが、JASO TP15002(2015 年)や ISO/SAE 21434 (2021 年)のようなセキュリティ設計ガイドラインである。これらは IT 製品の脆弱性評価を行う標準をベースに、安全、金銭、運用、プライバシーなどの観点を盛り込んだ手法により、自動車システムに対する攻撃容易性や受けた損害の深刻度を評価する。さらに後者は製品リリース後のセキュリティリスクの再評価などの回帰的なリスクマネジメントについても定めており、より実地的なものとなっている。

そうしたセキュリティ設計のリスク分析における課題のひとつは分析の妥当性に関するものである。つまり分析対象のシステムの実情に沿った適切な分析ができる、リスク数値化手法が必要となっている。前述の CAN インバーダーは車載ネットワークへの有線接続によるサイバー攻撃であり、従来は車への侵入と配線作業が必要で攻撃が困難とされていたものである。しかしフロントバンパーを剥がしたすぐ先に重要機能に繋がる通信線が配線されていたため、これを悪用した攻撃が成功してしまった。このようなリスクも予見する数値化手法が求められる。

本論文では、サイバーフィジカルシステム特有の領域や観点に沿って、より詳細な差別化が可能なリスク数値化手法の検討を行い、ソフトウェアの脆弱性評価基準 CWSS(Common Weakness Scoring System)をサイバーフィジカルシステムに適用し、メトリックの評価基準をカスタマイズした手法 RSS-CWSS\_CPS を提案した。そしてこの手法がリスクを数値化する際にどういった観点を重視しているかを、CWSS の計算式についてメトリクスごとに偏微分する詳細分析で明らかにし、CAN インバーダーに代表される自動車システムへのダイレクトアクセス攻撃について評価した。ダイレクトアクセス攻撃は実際にサイバー犯罪に有効であるにも関わらず、従来のリスク数値化手

法では遠距離無線通信経由の攻撃と比べリスクが低いとされていた。しかし本方式ではダイレクトアクセス攻撃も重要脅威として抽出され、このリスク数値化手法が分析対象のシステムの実情に沿った評価が行えることが確認できた。

**キーワード:** 車載セキュリティ, セキュリティ設計, リスク分析, TARA, ISO/SAE 21434, JASO TP15002, CWSS, CVSS.

# 目次

第 1 章	はじめに .....	1
1.1	背景 .....	1
1.2	セキュリティ設計と本論文の範囲 .....	3
1.2.1	セキュリティ設計の役割と手順 .....	3
1.2.2	本論文の範囲 .....	4
1.3	課題 .....	5
1.3	本論文の目的と貢献 .....	6
1.4	本論文の構成 .....	7
第 2 章	準備・関連研究 .....	8
2.1	セキュリティ設計における各要素 .....	8
2.2	自動車システムのセキュリティ設計 .....	9
2.2.1	セーフティクリティカルシステムにおけるセキュリティ .....	9
2.2.2	JASO TP15002 .....	11
2.2.3	ISO/SAE 21434 .....	11
2.2.4	セキュリティ設計手順比較 .....	13
2.3	脆弱性評価基準 .....	14
2.3.1	CVSS(Common Vulnerability Scoring System) .....	14
2.3.2	CWSS(Common Weakness Scoring System) .....	19
2.4	自動車システムで特徴的なエントリーポイント: ダイレクトアクセス攻撃 .....	24
2.5	むすび .....	25
第 3 章	資産コンテナ方式, および 2 ステップリスク分析の考案 .....	27
3.1	セキュリティ設計手順効率化の試み .....	27
3.2	資産コンテナ方式と 2 ステップリスク分析 .....	27

3.3 ケーススタディ例 .....	30
3.4 その他先行研究 .....	36
3.4.1 自動車以外の対象システムの検討 .....	36
3.4.2 過去に検討したリスク数値化手法 .....	39
3.4.2.1 RSS-CWSS .....	39
3.4.2.2 RSS-CVSSv3 と Q-RSMA .....	42
3.5 むすび .....	43
第4章 ダイレクトアクセス攻撃を検知可能なリスク数値化手法 .....	45
4.1 背景と研究動機 .....	45
4.2 本章における研究の目的と貢献 .....	46
4.3 ダイレクトアクセス攻撃の評価における従来手法の問題 .....	47
4.4 CWSS をベースとした新たな提案手法: RSS-CWSS_CPS .....	48
4.4.1 RSS-CWSS_CPS の計算式 .....	48
4.4.2 RSS-CWSS_CPS におけるメトリックの定義 .....	50
4.4.3 RSS-CWSS_CPS によるダイレクトアクセス攻撃の評価 .....	52
4.4.4 RSS-CWSS_CPS のメリット .....	53
4.5 ケーススタディおよび手法の効果の分析 .....	54
4.5.1 自動車システムの分析対象モデル .....	54
4.5.2 リスク数値化手法 .....	58
4.5.3 各メトリックのマッピング .....	58
4.5.4 ダイレクトアクセス攻撃の分析に RSS-CWSS_CPS を用いることの優位性 .....	62
4.5.5 ダイレクトアクセス攻撃に対する評価結果の比較 .....	63
4.5.6 エントリーポイントの優先度の比較 .....	67
4.5.7 ケーススタディにおける結論 .....	68

4.6 ディスカッション .....	69
4.6.1 2ステップリスク分析に有利なリスク値のばらつき .....	69
4.6.2 中長期的なリスクの解釈 .....	70
4.6.3 リスク評価後のプロセス .....	70
4.7 むすび .....	71
第5章 ISO/SAE 21434 TARA におけるリスク数値化手法 .....	72
5.1 背景と研究動機 .....	72
5.2 本章における研究の目的と貢献 .....	75
5.3 ISO/SAE 21434 TARA で用いられている従来手法 .....	75
5.4 従来手法 CVSS-based approach の問題 .....	78
5.5 ISO/SAE 21434 TARA における、資産コンテナ方式と RSS-CWSS_CPS の適用 .....	79
5.5.1 資産コンテナ方式と RSS-CWSS_CPS の第4章からの変更点 .....	80
5.5.2 RSS-CWSS_CPS を適用することのメリット .....	80
5.6 RSS-CWSS_CPS によるケーススタディ .....	81
5.6.1 自動車システムの分析対象モデル .....	81
5.6.2 資産定義と損害を受けることでの影響度の分析 .....	83
5.6.3 脅威シナリオの抽出 .....	84
5.6.4 攻撃経路の分析と攻撃容易性の算出 .....	84
5.6.5 リスク値の算出と考察 .....	90
5.7 ケーススタディの結果から見た提案手法の優位性 .....	91
5.7.1 エントリーポイント別の攻撃容易性の傾向の変化 .....	91
5.7.2 資産が損害を受けることでの影響度におけるバイアス .....	93
5.8 むすび .....	96
第6章 おわりに .....	97



6.1 本研究で得られた成果 .....	97
6.2 今後の課題 .....	97
6.2.1 リスク値が適度にばらつくようにしたい .....	98
6.2.2 分析対象をどこまで詳しく定義し評価するか .....	98
謝辞 .....	99
Acknowledgements .....	100
参考文献 .....	101
Appendix A 重要脅威リスト（第 4 章および第 5 章の補足） .....	106
A.1 重要脅威リスト(4.5.5 項) .....	107
A.2 重要脅威リスト(5.6.5 項) .....	111
著者研究業績 .....	115
図目次 .....	116
表目次 .....	118

# 第 1 章 はじめに

## 1.1 背景

情報通信技術(ICT: Information and Communication Technology)やセンサ、アクチュエータなどの発達により、いわゆるサイバーフィジカルシステムが登場した。これは実世界の情報をセンサネットワークで電子データに変え、サイバー空間を形成する ICT システムでデータ処理を行い、算出されたデータを基に実世界のアクチュエータの制御を行うなど、実世界での物理的な事象とサイバー空間での情報を取り持つことで成り立つシステムである。サイバーフィジカルシステムは発電所などの重要インフラ、工場、航空機、鉄道など、様々な分野で運用されているが、自動車もその一つである。

近年の自動車システムでは、カメラ、センサ、アクチュエータなど、様々な機能を持つ車載 ECU (Electronic Control Unit: 電子制御ユニット)が搭載されており、これらが車載ネットワークで相互に結びつくことで走行やドライブアシストなどの高度な機能を実現している。また車載インフォテインメント(IVI: In-Vehicle Infotainment)やテレマティクス(Telematics)用途の車載 ECU もあり、インターネットやクラウドのような車外ネットワークと連携し、ナビゲーションやソフトウェア自動アップデートなどのサービスを受けることもできる。このように、車載ネットワークと車外ネットワーク 2 つのサイバー空間があり、センサ、アクチュエータなどで自動車を取り巻く実世界に影響を与え、ドライバーや周囲の道路利用者に恩恵を施している。

しかしその一方で、サイバー空間で生じた悪影響が実世界に波及してしまうリスクも生じた。車載ネットワークや車外ネットワークを形成する ICT システムへのサイバー攻撃の結果が実世界で事故を引き起こしうることは、2015 年の Miller と Valasek による Jeep Cherokee の実車をハッキングした制御乗っ取り実験の事例[1]で示されている。以来、自動車システムへのサイバー攻撃がもたらしうる実世界への深刻な悪影響への対策が課題となっている。そのような情勢を受け、自動車システムにおいてもセーフティのみならず ICT システム同様のセキュリティ対策を設計仕様書の段階で盛り込む工程を入れることが急務となっている。この工程がセキュリティ設計(Security Design)であり、本研究のテーマである。

自動車システムのサイバーセキュリティにおける開発ガイドライン ISO/SAE 21434[2]に掲載されている、開発 V 字モデルを図 1 に示す。セキュリティ設計はこの図左上の“Chapter 9 Concept”に該当する。これは図下側の“Chapter 10 Product Development”で具体的な機能の実装に入る

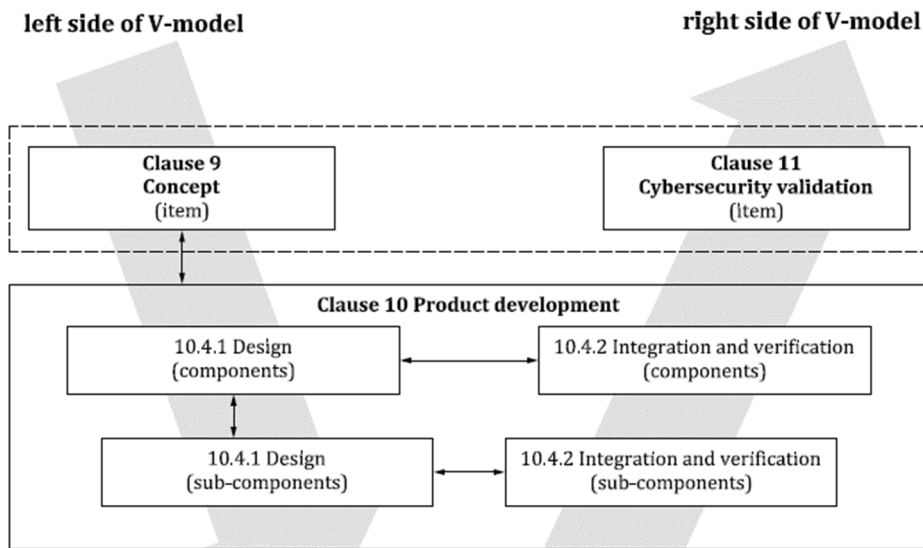


図1: 製品開発における開発V字モデル[2]

Figure 1: The V-model of Product Development Activities [2]

前に、システム仕様書から分析対象のモデルを構築してリスクを分析し、実装が必要なセキュリティ要件を策定する作業である。

この自動車システムのセキュリティ設計については、自動運転関連の定義を含め、ここ数年で関連する法整備、標準化などが進められている。国連自動車基準調査世界フォーラム作業部会 29 (WP.29: United Nations world forum for harmonization of vehicle regulations Working Party 29) は、自動車システムに対するサイバーセキュリティの様々なリスクやそれらを管理する仕組み (CSMS: Cyber Security Management System) を定めた法規 UN-R155 [3] および自動車システムにおけるソフトウェアアップデート機能とそれを管理する仕組みを定めた UN-R156 [4] の、2 つのサイバーセキュリティ法規を制定した。自動車業界においても自動運転に関連したものを含め、新しいガイドラインが公開されている。主要メーカー11 社が 2019 年に公開した自動運転車のセーフティとセキュリティに関する開発、テストおよび評価を実施するためのフレームワーク“Safety First for Automated Driving, 2019” [5]、ENISA が 2020 年に公開したスマートカーのセキュリティに関するグッドプラクティスを定義したレポート“Good practices for security of Smart Cars” [6]、米国運輸省が 2020 年に公開し、セキュリティの重視とプライバシーの保護について言及したガイドライン “Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0” [7]、などである。

欧州でセキュリティチップやスマートカードなどの認証に用いられているコモンクライテリア (CC: Common Criteria) [8] も、権威のあるセキュリティ認証基準であり、現在これを用いた認証手法として EUCC スキーム (Common Criteria based European candidate cybersecurity certification

scheme) [9] が策定中である。コモンクライテリアの自動車システムへの適用に関しては、2019 年に Maliatsos らがコモンクライテリアのセキュリティ要件をコネクテッドカーに適用する試みについて研究発表[10]を行っている。

## 1.2 セキュリティ設計と本論文のスコープ

### 1.2.1 セキュリティ設計の役割と手順

まずセキュリティ設計について説明する。セキュリティ設計とは図 2 にあるように、前述の開発 V 字モデルにおいて最初に着手する、左上のプロセスである。具体的には製品がまだ出来上がっていない時点で、システム仕様書を基にセキュリティ仕様書を作成する以下のような作業である：

- **フェーズ 1(システムモデルの作成):** システムの構成要素(各コンポーネント/機能モジュールのネットワーク構成図, それぞれが持つ機能と情報)と情報フローを図にし, 機能や情報の概要やライフサイクルを定義する。
- **フェーズ 2(脅威の抽出):** システムが攻撃者からサイバー攻撃を受ける可能性を, 脅威として洗い出す。
- **フェーズ 3(脅威分析とリスクアセスメント):** 脅威が持つセキュリティリスクを評価 (定量化)し, どのように対処するかを検討する。
- **フェーズ 4 (セキュリティ対策のゴール策定):** セキュリティ対策方針を決めるなど, システムをどう保護していくのか, あるべき姿を策定する。

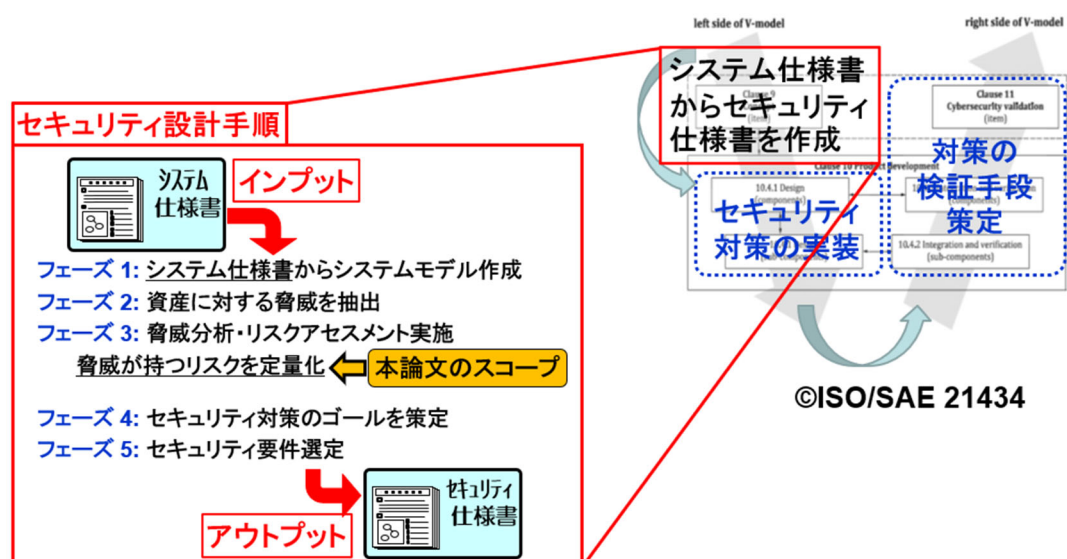


図2: セキュリティ設計の製品開発における役割とその手順

Figure 2: Role and Procedure of Security Design  
in Product Development

- フェーズ 5(セキュリティ要件の選定):セキュリティ対策を実現するために必要なセキュリティ要件を選定し(該当する標準があればそれに従う), セキュリティ仕様書を完成させる。

### 1.2.2 本論文のスコープ

本論文のスコープは, 上記フェーズ 3 で実施する脅威分析において脅威の持つリスクを定量化する, リスク数値化手法に係る研究である。図 3 にあるような自動車システムを簡略したモデルを用いて, リスク数値化手順について説明する。

図 3 上段のように, CGW(セントラルゲートウェイ), ITS, テレマティクス, およびその他の機能それぞれについてひとまとまりにしたものを機能モジュールとして黄色地緑字のボックスを置く。そして CGW, ITS, テレマティクスが持つ通信インタフェースをエントリーポイントとして白地に青字のボックスを置く。そしてメンテナンス機器, 料金所, サーバといった車外の通信相手を橙色地黒字

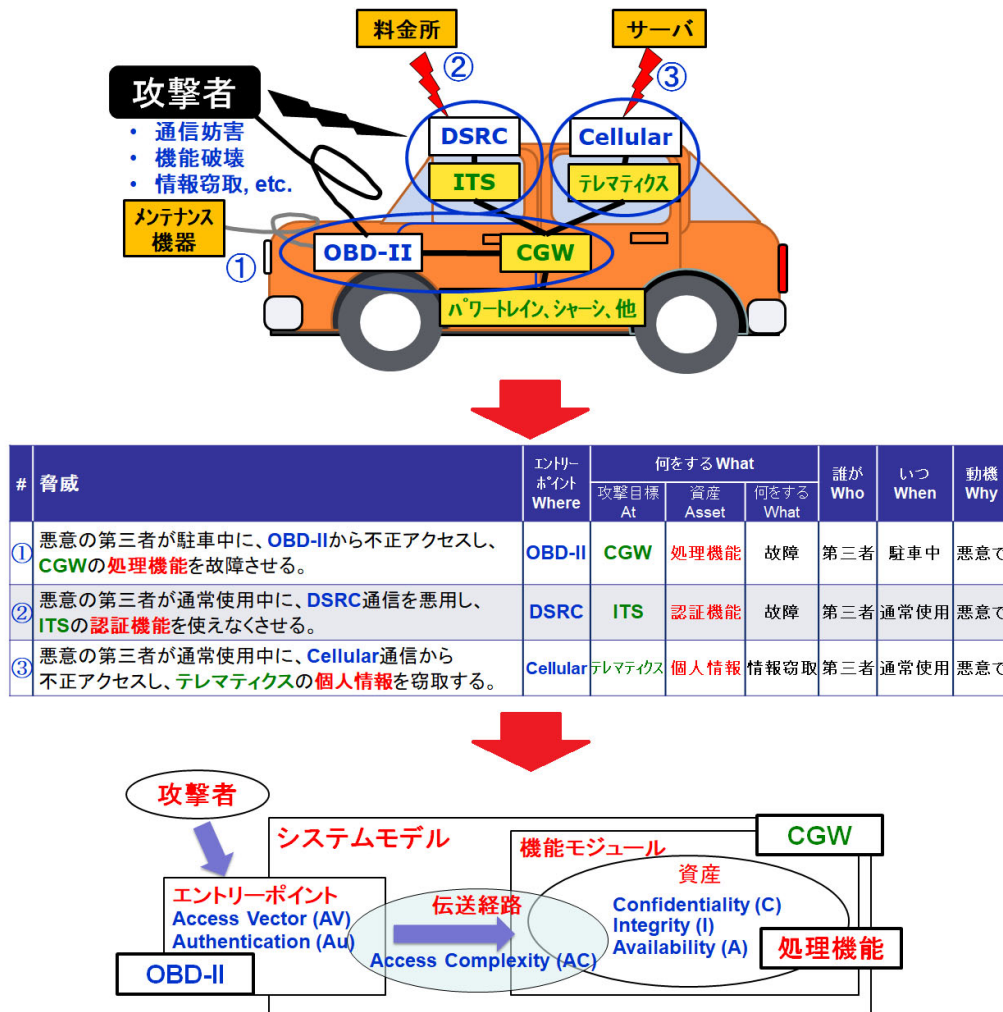


図3: 脅威の定式化とリスクの数値化

Figure 3: Formulation of Threat and Risk Quantification

のボックスを置く。最後に攻撃者として黒地白字のボックスを置き、各ボックス間を通信経路に応じて線を結ぶ。これが説明のため簡略化した自動車システムのモデルである。

次にこのモデルを基に脅威を書き出したのが図3中段の表である。基本的に脅威は5W法、即ち5つの“W”である“Who(誰が)”, “When(いつ)”, “Where(どこから)”, “Why(どういう意図で)”, “What(何を)”を用いて記述するが、モデル図があることで“What”を攻撃目標“At”と攻撃対象の資産“Asset”を具体的に補うことができる。図3上段のモデルにある①②③はそれぞれ脅威を指すが、青字のエントリーポイント、緑字の攻撃目標、赤字の攻撃対象の資産を表に書き出すことで他の脅威と区別することができる。

そして脅威の“What”, “At”および“Asset”を中心にトポロジーを簡略化したものが図3下段の図である。これに対してリスク数値化手法のメトリックを割り当てて、リスクの定量化を行う。これが一連のリスク数値化手順である。

脅威①を例に挙げると、この図の“What”, “At”および“Asset”はそれぞれ「OBD-II」, 「CGW」および「処理機能」を割り当てることができる。リスク数値化手法として2.3.1項で後述する

CVSS (Common Vulnerability Scoring System)を例に、前述の脅威①に対して、メトリックの割り振りと評価について説明すると以下ようになる:

- OBD-II は通信インタフェースを評価するメトリック AV (Access Vector) により有線通信であることを評価され、認証の可否を評価するメトリック Au (Authentication)により認証が不要なことを評価される。
- CGW は OBD-II ポートを持つので、攻撃の複雑さを評価するメトリック AC (Access Complexity) により不正アクセスによる攻撃が容易であることを評価される。
- 処理機能は資産の完全性と可用性が侵されると損害が生じることを、メトリック I (Integrity) と A (Availability)により評価される。
- 最後に脆弱性評価基準 CVSS の計算式(2.3.1項で後述)を用いることにより、リスク値が算出される。

本研究のスコープであるリスク数値化手法とは、この例のようにシステムモデルから脅威を抽出し、脅威の持つリスクを定量化するプロセスである。次節で本研究の課題をまとめる。

## 1.3 課題

以上のように、自動車システムの開発者が機能安全など従来からのセーフティに加え、セキュリティの観点でリスク分析と対策を検討する、「セキュリティ設計」を盛り込むことが求められている。

そして自動車ならではの特定の条件や観点に沿った攻撃リスクを分析し対応することも必要となっている。

たとえば、2021 年の日本において、CAN インベーター[11]と呼ばれる、ダイレクトアクセス攻撃による高級車窃盗事件が起きたが、これは車載ネットワークへの有線接続によるサイバー攻撃であり、従来は車への侵入と配線作業が必要で攻撃が困難と思われたものである。

このことは同じサイバーフィジカルシステムに対する同様の攻撃でも、工場と自動車では事情が異なり評価も変える必要があることを示している。工場システムでは入室制限やカード認証などで、イントラネットに物理的にアクセスすることが極めて困難である一方で、自動車システムでは CAN インベーターで露見したように、フロントバンパーを剥がしたすぐ先に重要機能に繋がる通信線が配線されている場合もある。そのため、分析対象のシステムの実情に沿った、適切なリスク分析が課題となる。

本研究はセキュリティ設計のプロセスのうち、脅威をいくつかの観点からリスクを評価し数値化する、いわゆるリスク数値化手法に着目し、自動車システムを主に対象とした、サイバーフィジカルシステムのリスク分析における「分析対象のシステムの実情に沿った、適切なリスク分析の実現」を課題とする。

## 1.3 本論文の目的と貢献

本論文の目的と貢献はセキュリティ設計におけるリスク分析手順で課題を解決できる、新たなリスク数値化手法を提案し、サイバーフィジカルシステムのシステムの解釈に知見を与えることである。具体的には、ソフトウェアの脆弱性評価基準のひとつである CWSS(Common Weakness Scoring System)[12]をベースに、サイバーフィジカルシステムの物理的/論理的構造の解釈を考慮した、新しいリスク数値化手法の提案とその効果の考察を行う。

前提として、筆者は開発者が行うセキュリティ分析手順の効率化について検討を行っており、2017 年の論文[13]で、自動車技術会(JSAE)のセキュリティ設計ガイドライン JASO TP15002 [14]で用いる手法として、「資産コンテナ方式」および「2 ステップリスク分析」というアプローチを提案しており、本論文ではこのアプローチで行ったケーススタディの結果を基に、提案するリスク数値化手法の有用性を分析した。これらアプローチについては 3 章で説明する。

また、リスク数値化手法の考案は当初前述の JASO TP15002 をベースに進めていたが、2023 年にこれが ISO/SAE 21434 に置き換わる形で廃止となった。そのため、ISO/SAE 21434 への移行と共に本提案手法の適用を行い、本提案手法が課題を解決し、JASO TP15002 および ISO/SAE 21434 双方のリスク分析において有用であることを確認した。JASO TP15002 や

ISO/SAE 21434 では、CVSS(Common Vulnerability Scoring System)[15]のような IT 製品の脆弱性を評価する手法と ISO/IEC 18045 [16]のような CEM (Common Methodology for Information Technology Security Evaluation)による攻撃の可能性(Attack Potential)を評価する手法の 2 通りがリスク数値化手法として挙げられているが、本研究では前者を比較対象とし、既存手法に対する優位性を論じた。これらは第 4 章および第 5 章で述べる。

## 1.4 本論文の構成

第 2 章で準備として、セキュリティ設計概論、セキュリティ設計ガイドラインの JASO TP15002 および ISO/SAE21434 の紹介、リスク数値化に用いる CVSS や CWSS の脆弱性評価基準、および本論文の課題に係るサイバー攻撃であるダイレクトアクセス攻撃について述べる。

第 3 章では課題であるリスク数値化を適用するリスク分析のアプローチとして筆者が過去に提案した、「資産コンテナ方式」および「2 ステップリスク分析」の紹介を主に、本論文の研究に関連する先行研究について説明する。

第 4 章では、課題を解決する手段として CWSS をベースとしたリスク数値化手法 RSS-CWSS\_CPS を提案する。そして JASO TP15002 のリスク分析手順を用いたケーススタディを通じ、TP15002 の従来手法である CVSS ver.2 でのリスク数値化結果と比較した、提案手法の優位性を論じる。

第 5 章では第 4 章に引き続き RSS-CWSS\_CPS を ISO/SAE 21434 のプロセスに適用し、ISO/SAE21434 の従来手法である CVSS-based approach でのリスク数値化結果と比較した。そして課題解決の確認とともに、提案手法の優位性を論じる。

最後に第 6 章で課題が解決したかどうか、結論と今後の課題を述べる。



## 第2章 準備・関連研究

本章では準備として、セキュリティ設計における各要素、セキュリティ設計ガイドラインの JASO TP15002 および ISO/SAE21434 の紹介、リスク数値化に用いる CVSS や CWSS の脆弱性評価基準、および本論文の課題に係るサイバー攻撃であるダイレクトアクセス攻撃について述べる。

### 2.1 セキュリティ設計における各要素

まず、セキュリティ設計における各要素について説明する。前述のように、セキュリティ設計ではシステム仕様書からセキュリティ要件を盛り込んだセキュリティ仕様書を作成する。システム仕様書から脅威の分析を終えるまでに必要な情報とそれらの関係を示したものが図 4 である[13]。図中の各要素について説明する。

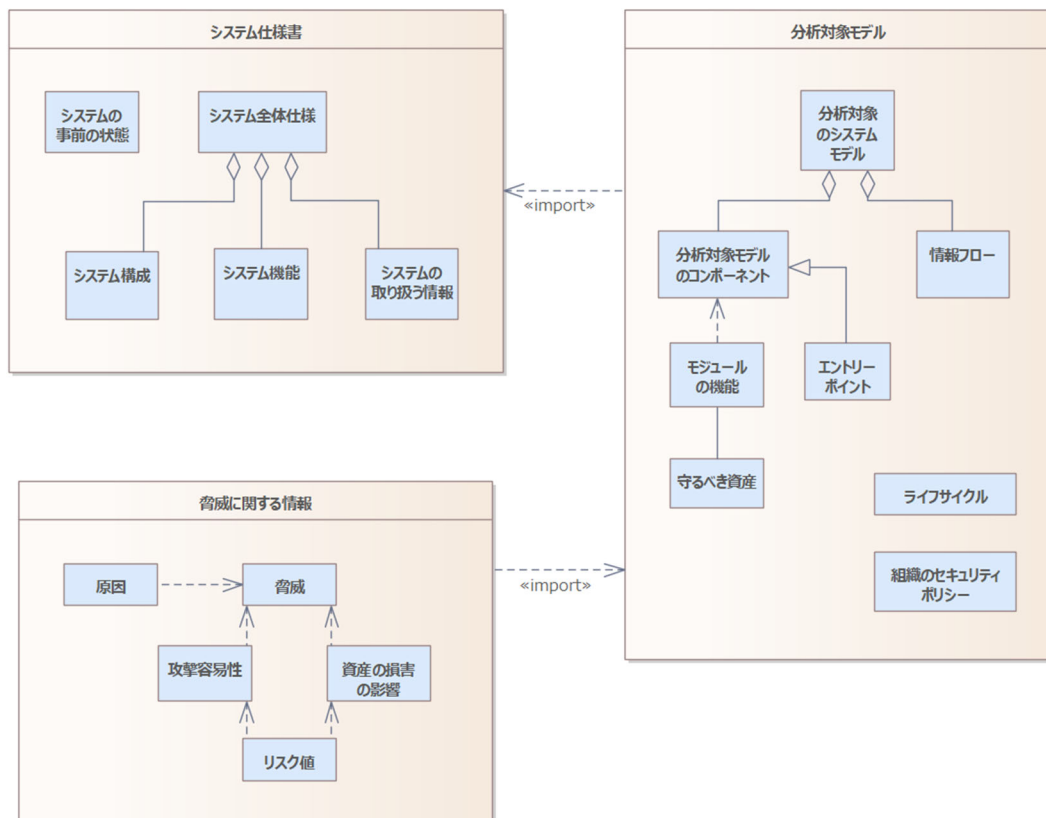


図4: セキュリティ設計における各要素の論理的関係

Figure 4: Logical Relationship between Each Element of The Security Design Process

**システム仕様書:** システム仕様書には、システムの構成(物理的/論理的なネットワーク構成図)、システム機能、システムの取り扱う情報、システム内部での状態が定められている。

**分析対象モデル:** システム仕様書から抽出した情報を整理したシステムモデルである。システム構成の中に含まれる個々のコンポーネントや機能モジュール、機能、および情報を、システム仕様書から逸脱しない範囲で抽象化を行うことは可能であり、後段の脅威抽出における作業量を適度に抑えるために必要である。そして内部のコンポーネントごとの機能やコンポーネント間の情報フローがシステム仕様書に準拠した正しい流れになっていることを確認し、守るべき資産(機能、情報)を整理する。また脅威の成否に影響を与える前提条件として、システムのライフサイクルや組織のセキュリティポリシーを確認する。

**脅威に関する情報:** 分析対象モデルから抽出および分析評価を行った結果、得られる情報である。脅威に関しては、コンポーネントや機能モジュールが所有する資産に対しサイバー攻撃が成功して、資産に損害を受けることで利用者や製造者などのステークホルダーに影響を及ぼしうる事象を抽出する。この脅威を基に、サイバー攻撃が成功してしまう原因を攻撃経路や攻撃手段の観点から分析し、資産の損害の影響をいくつかの観点から考察することで、攻撃容易性と資産が損害を受けることでの影響度を得る。そしてリスク数値化手法を用いてリスク値を算出する。

自動車システムのセキュリティ設計ガイドラインである、JASO TP15002 および ISO/SAE 21434 では、図 4 に沿ったセキュリティ設計手順を定義している。

## 2.2 自動車システムのセキュリティ設計

次に、自動車システムにおけるセキュリティ設計ガイドラインの成り立ちについて説明し、JASO TP15002 と ISO/SAE 21434 におけるセキュリティ設計手順について説明する。

### 2.2.1 セーフティクリティカルシステムにおけるセキュリティ

自動車システムはサイバーフィジカルシステムである以前にセーフティクリティカルなシステムである。よってその開発プロセスは、セーフティの問題を扱う標準 ISO 26262 [18] に従ってきた。セーフティクリティカルなシステムでは、安全性の分析と設計のいくつかの方法論が確立されていた[19][20][21][22][23]が、当初セキュリティは考慮されていなかった。しかしその後、情報通信技術(Information and Communication Technologies: ICT)を導入したサイバーフィジカルシステムとしての側面を持つようになると、セキュリティのさまざまな分析および設計手法が情報技術において提案されるようになった [24][25][26][27][28][29][30][31][32]。自動車システム以外の分野でも、セーフティとセキュリティの関係が考慮されるようになっており、例えば、鉄道制御システム

[33][34]や航空電子機器[35], 産業制御システム[36][37]などの分野でも, セキュリティに関連する研究が行われてきた。

こうした中で, 自動車システムにおけるセキュリティのガイドラインとして 2016 年に SAE が公開したものが SAE J3061[38]である。前述の JASO TP15002(2015 年公開)はセキュリティがスコープであったが, J3061 はシステムにおけるセーフティとセキュリティの関係性を図 5 のように示している。この図では, セキュリティクリティカルシステムはセーフティクリティカルシステムよりも範囲が広いこと, システムセーフティ工学の要素とシステムセキュリティ工学の要素は部分的にオーバーラップすることを示している。そのため自動車システムのセキュリティ設計ガイドライン ISO/SAE 21434 においては, セーフティとセキュリティ両面について考慮するよう定められている。この標準では, 第 15 章 TARA(Threat Analysis and Risk Assessment: 脅威分析とリスクアセスメント)の手順において, サイバー攻撃をもたらす脅威と攻撃の結果により道路使用者が受けるセーフティ/セキュリティ上の損害を受けることでの影響を具体的に記したものを「ダメージシナリオ」として, サイバー攻撃による脅威を記した「脅威シナリオ」とは分けて定義している。

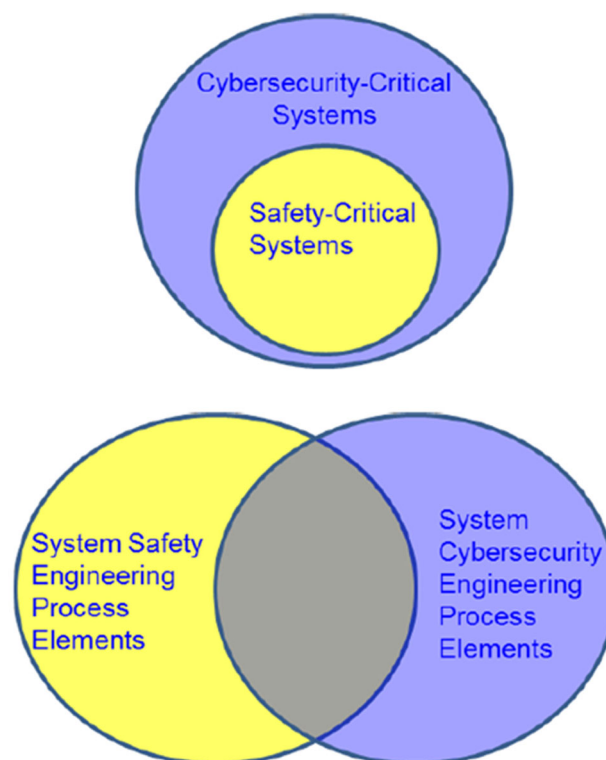


図5: SAE J3061で定めたセーフティとセキュリティの関係 [38]

Figure 5: Relationship between Safety and Security in SAE J3061 [38]

### 2.2.2 JASO TP15002

JASO TP15002 は 2015 年に自動車技術会(JSAE)が公開し、2023 年に ISO/SAE 21434 に引き継ぐ形で廃止となった、自動車システムのセキュリティ設計ガイドラインである。これはセキュリティ設計をスコープとし、サイバー攻撃の脅威に対する対策をコモンクライテリアのセキュリティ要件に落とし込むためのガイドラインである。システムをモデル化し、リスク分析後に策定したセキュリティ対策方針からコモンクライテリアのセキュリティ要件を選定するところまでの手順を以下の 5 フェーズに定めている:

- **Phase 1: 評価対象(TOE: Target of Evaluation)定義:** システムの構成要素(各コンポーネント/機能モジュールのネットワーク構成図, それぞれが持つ機能と情報)と情報フローを図にし, 機能や情報の概要やライフサイクルを定義する.
- **Phase 2: 脅威分析:** 対象システムの情報セキュリティ課題(攻撃者からサイバー攻撃を受ける可能性)を脅威として洗い出す.
- **Phase 3: リスク評価:** 脅威に伴うセキュリティリスクを適切に評価し, 詳細を分析する. 脆弱性評価基準を基にした CRSS および RSMA が, 具体的なリスク評価手順として Appendix D に例示されている.
- **Phase 4: 対策方針策定:** セキュリティリスクを緩和する対策方針を検討し策定する.
- **Phase 5: セキュリティ要件の選定:** それぞれのセキュリティ対策方針に対し, コモンクライテリアのセキュリティ機能要件(SFR: Security Functional Requirement)とセキュリティ保証要件(SAR: Security Assurance Requirement)の中から選定し結びつける.

### 2.2.3 ISO/SAE 21434

ISO/SAE 21434 は, SAE J3061 や JASO TP15002 などの自動車システムのセキュリティ設計ガイドラインに代わるものとして, 2021 年に公開された. ISO/SAE 21434 では自動車システムのセキュリティに関して, 設計時のリスク分析や要件の策定(ただし, こちらは JASO TP15002 のようにコモンクライテリアのセキュリティ要件とは指定されていない), および製品リリース後の継続的なリスクマネジメントを実施するためのガイドラインを提供する. セキュリティ設計は本標準の第 9 章(前出の図 1 左上のプロセス)に該当し, JASO TP15002 同様の分析対象のモデル化による脅威抽出, リスク分析, 対策のためのセキュリティ要件抽出を行う. リスク分析のプロセスは TARA(脅威分析とリスクアセスメント)と呼ばれ, 別途第 15 章で詳細な手順が定義される. そこでは「ダメージシナリオ」に基づくサイバー攻撃により資産が受ける損害の影響度と「脅威シナリオ」に基づく攻撃容易性の 2 つの軸でリスクを評価する.

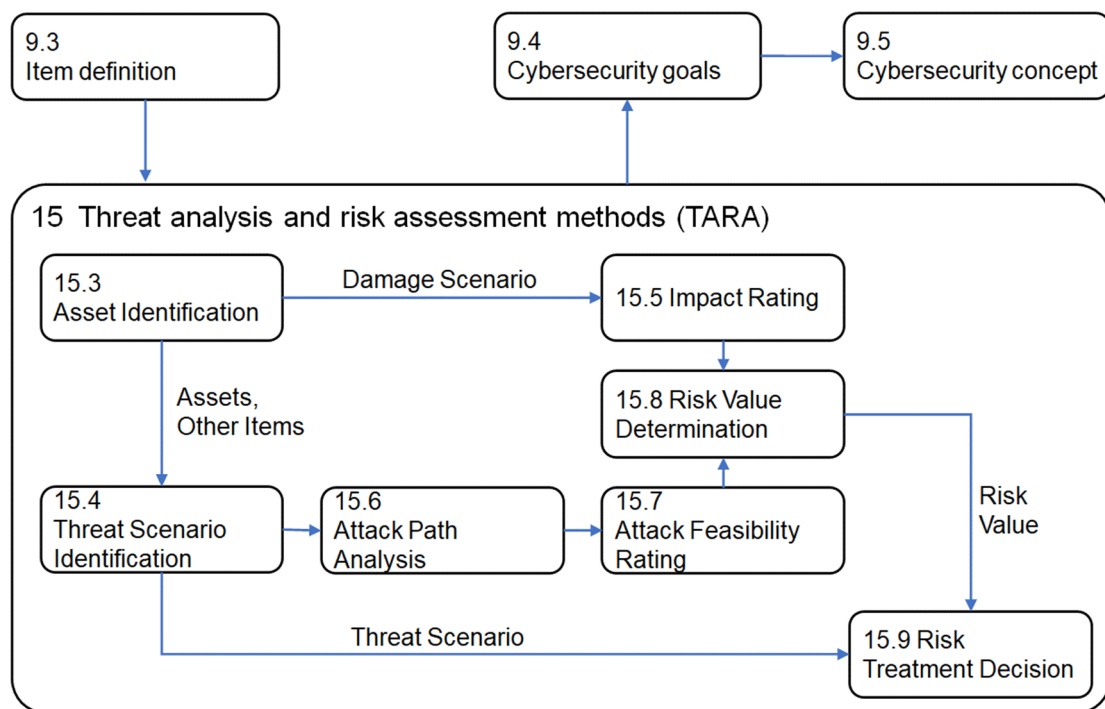


図6: ISO/SAE 21434のブロックダイアグラム  
Figure 6: Block Diagram of ISO/SAE 21434

「脅威シナリオ」「ダメージシナリオ」の2つの軸のプロセスを追いやすくするため、TARAのブロックダイアグラムを図6に示す。このブロックダイアグラムに従い、以下のような脅威の抽出と脅威の持つリスクを評価し、対策の要否を検討するプロセスが示されている。

第9章および第15章で定められた、ISO/SAE 21434におけるセキュリティ設計の手順を以下に示す。作業手順としては、9.3節でシステム仕様書からアイテムを定義し、15章の各手順を進めて抽出した脅威にどう対応するかを決めてから、9.4節のセキュリティゴールの策定と9.5節のコンセプトレベルの対応をまとめるようになっている：

- **アイテム定義(9.3節):** 分析対象のシステムおよび周辺環境をシステム仕様書からモデル化(システム構成図の作成、機能やデータの定義を実施)し、TARAのインプットとする。
- **資産の識別(15.3節):** まずシステムの持つ機能やデータについて、サイバーセキュリティ領域(例えば機密性、完全性、可用性)から見て、守らなければならないものを資産としてリストに計上する。
- **損害の評価(15.5節):** 脅威により資産が損害を受けた時に、その結果「車両または車両の機能に關与し、道路利用者に影響を与える悪影響」が何であるかをダメージシナリオとして定義し評価する。個々の資産が損なわれることでの悪影響(損害を受けることでの影響度)は、S, F, O, P( Safety: 安全, Financial: 金銭, Operational: 運用, および Privacy: プライバシ

一)の4つの観点から見た,4段階の深刻度(Severity: “Severe”, “Major”, “Moderate”, および “Negligible”)で決定される.

- **脅威シナリオの識別(15.4 節):**「ダメージシナリオが実現する,1つ以上の資産のサイバーセキュリティ領域が侵害される潜在的な原因」を,脅威シナリオとして抽出する.
- **攻撃経路の分析と攻撃容易性の評価(15.6 節および 15.7 節):**脅威シナリオの攻撃経路(および手法)を分析し,攻撃者から見た攻撃容易性を評価する.
- **リスクの数値化とリスクへの対処(15.8 節および 15.9 節):**上記で評価された資産の損害と攻撃容易性からリスクを数値化し,個々のリスクへの対処(回避,軽減,移転,および受容)を決定する.
- **サイバーセキュリティゴール(9.4 節):**TARA の分析結果を受け,脅威のリスクを低減するものについては対策としてサイバーセキュリティゴール(Cybersecurity goals)を,脅威をそのまま保持するものについては保持していても大丈夫だと示す根拠としてサイバーセキュリティクレーム(Cybersecurity claims)を策定する.
- **サイバーセキュリティコンセプト(9.5 節):**サイバーセキュリティゴールを分析対象のシステムやその周辺環境に適用するための具体的なシステム要件を定義し,それらについて完全性,正確性,一貫性の観点で評価する.

## 2.2.4 セキュリティ設計手順比較

セキュリティ設計手順に関して,ISO/SAE 21434 と JASO TP15002 との流れを比較したものが図 7 である.以下のように3点違いがあるものの,基本的な手順は図 4 のセキュリティ設計プロセスに従ったものであり,本研究で扱うリスク分析までの実施内容は同様である.

- ISO/SAE 21434 では攻撃経路の攻撃容易性と資産の損害による影響を個別に評価するよう,手順を定義しているが,JASO TP15002 では明確には分けられていない.だが,前者においても,攻撃経路における攻撃容易性および資産の損害に係るインパクトはリスク値を算出するまでの中間評価的なものであり,リスク数値化手法の個々のメトリックをそれぞれ攻撃経路と資産の損害に割り振ることで代用できる.したがって両者の標準において任意のリスク数値化手法を適用することが可能である.
- ISO/SAE 21434 の 15.9 節のリスクへの対処は,JASO TP15002 には該当するフェーズが無い.これは ISO/SAE 21434 では ISO31000[40]で定義されたリスクアセスメントを組み入れているためと思われる(このパートは本研究のスコップ外である).
- ISO/SAE 21434 9.5 節のサイバーセキュリティコンセプトは製品開発のフェーズで必要な機能要件の基になるコンセプトが得られれば良いので,JASO TP15002 のフェーズ 5 のように

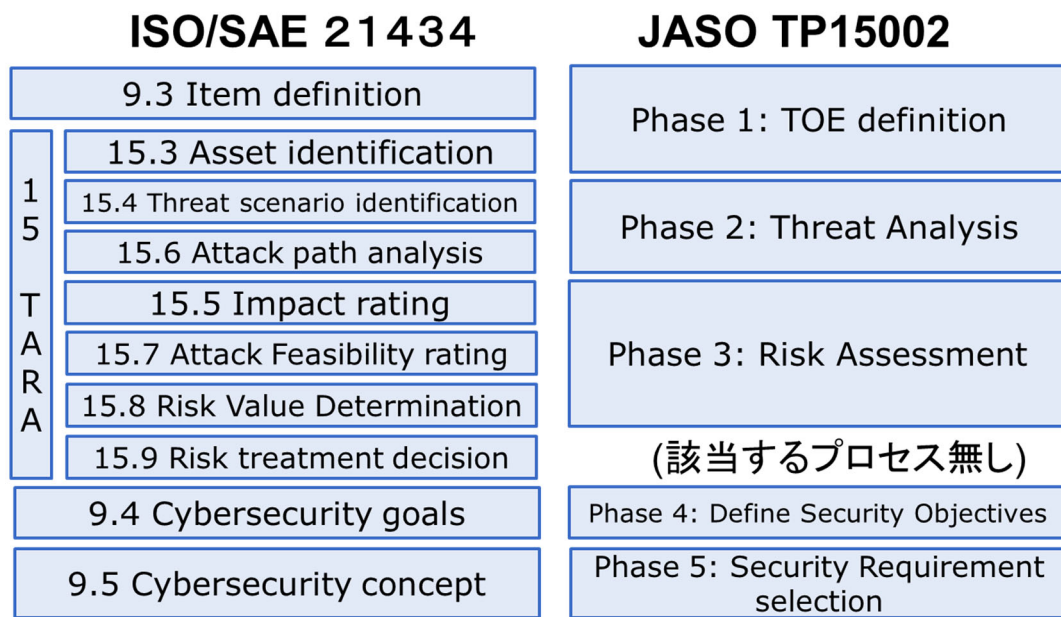


図7: ISO/SAE 21434とJASO TP15002 との手順比較

Figure 7: Procedure Comparison between ISO/SAE 21434 and JASO TP15002

コモンクライテリアのセキュリティ要件の選定は必須ではない(このパートも本研究のスコープ外である)。

以上のように、リスク数値化手法に係る本研究はどちらの標準にも適用可能である。

## 2.3 脆弱性評価基準

そして、本論文でリスク数値化手法のベースとして用いる、脆弱性評価基準について説明する。本研究では JASO TP15002 や ISO/SAE 21434 で用いられている CVSS をベースとした従来手法に対し、これに代わる新しい手法として CWSS をベースとしたリスク数値化手法を提案する。

### 2.3.1 CVSS(Common Vulnerability Scoring System)

CVSS は、JASO TP15002 や ISO/SAE 21434 など攻撃容易性を評価するのに利用される、脆弱性評価基準の 1 つである。ISO/IEC 18045 [16]での Attack Potential 評価手法のような攻撃者の資質や環境からリスクを分析する方式と異なり、パラメータ(メトリック)は攻撃を受ける側のシステム仕様から割り出せるもので構成されている。

CVSS は現在 Ver.4.0[41]が最新であるが、2023 年 11 月に公開されたばかりであり、自動車システムなどのサイバーフィジカルシステムに適用された関連研究も現時点ではないため、本研究

では Ver.4.0 はスコープ外とした。ここでは標準や関連研究で用いられた Ver.2, Ver.3.0, および Ver.3.1 に関してのみ言及する。

JASO TP15002 では CVSS Ver.2[42]の基本値をリスク値に用いた CRSS(CVSS based Risk Scoring System)を用いている。計算式を式(1-1)～(1-4)に、メトリックの定義およびランクを表 1 に、それぞれ示す。

$$\text{影響度} = 10.41 \times \{1 - (1 - C) \times (1 - I) \times (1 - A)\} \quad (1-1)$$

$$\text{攻撃容易性} = 20 \times AV \times AC \times Au \quad (1-2)$$

$$f(\text{影響度}) = 0(\text{影響度が } 0 \text{ の場合}), 1.176(\text{影響度が } 0 \text{ 以外の場合}) \quad (1-3)$$

$$\text{リスク値 } R_r = \{(0.6 \times \text{影響度}) + (0.4 \times \text{攻撃容易性}) - 1.5\} \times f(\text{影響度}) \quad (1-4)$$

式(1-1)～(1-4)および表 1 の各メトリックについて補足する:

- 個々のメトリックの値は大きいほど攻撃に有利, もしくは攻撃を受けることでの資産のダメージが深刻であることを定めている。
- 式(1-1)の影響度, 式(1-2)の攻撃容易性, 共にメトリックの値が大きいほど大きな値を取り, 式(1-4)のリスク値  $R_r$  もリスクが大きいほど大きな値を取るようになっている。
- リスク値  $R_r$  は 0～10 の値を取るようになっており(負の値は 0, 10 を越える値は 10 とする), 値が大きいほどリスクが高いと評価される。

**表 1: CVSS Ver.2 のメトリックとランク [42]**

**Table 1: Metrics and Ranks of CVSS ver.2 [42]**

Metric	Concept	Rank(Value)
Access Vector (AV)	This metric reflects how the vulnerability is exploited.	N (1.0) A (0.646) L (0.395)
Access Complexity (AC)	This metric measures the complexity of the attack required to exploit the vulnerability once an attacker has gained access to the target system.	L (0.71) M (0.61) H (0.35)
Authentication (Au)	This metric measures the number of times an attacker must authenticate to a target in order to exploit a vulnerability.	N (0.704) S (0.56) M (0.45)
Confidentiality Impact (C)	This metric measures the impact on confidentiality of a successfully exploited vulnerability.	C (0.660) P (0.275) N (0.00)
Integrity Impact (I)	This metric measures the impact to integrity of a successfully exploited vulnerability.	C (0.660) P (0.275) N (0.00)
Availability Impact (A)	This metric measures the impact to availability of a successfully exploited vulnerability.	C (0.660) P (0.275) N (0.00)



- Access Vector (AV)については、攻撃の侵入口であるエントリーポイントの観点で分類する。例えば、N(“Network”)はセルラーなどの遠距離無線通信、A(“Adjacent”)は Bluetooth などの近接無線通信、L(“Local”)は OBD-II などの有線接続による通信で分類する。表1にあるように、値は N, A, L の順に大きく、攻撃に有利とみなされている。
- Access Complexity (AC)については、攻撃成立までの手間の数を決める要素で分類する。例えば、エントリーポイントから侵入後にいくつかのモジュールを経由するかで AC を決める場合、エントリーポイントから侵入した機能モジュールを攻撃するなら L(“Low”), さらに内部の通信路を経由して隣接する機能モジュールを攻撃するなら M(“Middle”), さらに先の機能モジュールを狙うなら H(“High”)と、攻撃目的を達成するまでにかかった攻撃の数や手間に応じてランクを決定する。表1にあるように、値は L, M, H の順に大きく、攻撃に有利とみなされている。
- Authentication (Au)は AC と別に設けてあるので、AC のランク判定に認証は含めない。目的の機能モジュールに到達するまでに必要な認証回数が複数の時は M(“Multiple”), 1 回の時は S(“Single”), 認証不要の場合は N(“None”)と判定される。表1にあるように、値は N, S, M の順に大きく、必要な認証回数が少ないほど攻撃に有利とみなされている。
- Confidentiality Impact (C), Integrity Impact (I), および Availability Impact (A)については、資産である機能および情報の気密性、完全性、および可用性が損なわれた場合の影響について、影響が部分的である場合の P(“Partial”), 甚大である場合の C(“Complete”), もしくは影響なしの N(“None”)と判定している。表1にあるように、値は C, P, N の順に大きく、攻撃された場合の資産の影響度、資産が損なわれると悪影響が大きいとみなされている。

次に、ISO/SAE 21434 第 15 章 TARA で攻撃容易性を評価する際に用いる手法の 1 つ、CVSS-based approach では Ver.3.1 の攻撃容易性の計算式(2-4)が使用されている。

CVSS Ver.3 および Ver.3.1 では、システムの仮想化やサンドボックス化などが進んできていることから、メトリック UI や S の取り扱いなど、コンポーネント単位で評価する場合を考慮した仕様となっている。計算式を式(2-1)～(2-7)に、メトリックの定義およびランクを表 2 に、それぞれ示す。

$$\text{調整前影響度} = 1 - (1 - C) \times (1 - I) \times (1 - A) \quad (2-1)$$

$$\text{影響度(スコープ変更なし)} = 6.42 \times \text{調整前影響度} \quad (2-2)$$

$$\text{影響度(スコープ変更あり)} = 7.52 \times (\text{調整前影響度} - 0.029) - 3.25 \times (\text{調整前影響度} - 0.02)^{15} \quad (2-3)$$

$$\text{攻撃容易性} = 8.22 \times AV \times AC \times PR \times UI \quad (2-4)$$

影響度がゼロ以下の場合:

$$\text{基本値} = 0 \quad (2-5)$$

影響度がゼロよりも大きい場合:

スコープ(S)変更なし(Scope = “U”):

$$\text{リスク値 } R_r = \text{RoundUp1}(\min [(\text{影響度} + \text{攻撃容易性}), 10]) \quad (2-6)$$

スコープ(S)変更あり(Scope = “C”):

$$\text{リスク値 } R_r = \text{RoundUp1}(\min [(1.08 \times (\text{影響度} + \text{攻撃容易性})), 10]) \quad (2-7)$$

Ver.3.1[15]と Ver.3[43]との違いは AV の定義の厳密化, 計算式実装の際の Roundup 関数の定義の変更(バグ修正)であり, 計算式に変更は無い。

式(2-1)～(2-7)および表 2 の CVSS Ver.3 および Ver.3.1 のメトリックについて, Ver.2 との違いと合わせて以下に補足する:

- 個々のメトリックの値は大きいほど攻撃に有利, もしくは攻撃を受けることでの資産のダメージが深刻であることを定めている。

**表 2: CVSS Ver.3 および Ver.3.1 のメトリックとランク [15]**

**Table 2: Metrics and Ranks of CVSS Ver.3 and Ver.3.1 [15]**

Metric	Concept	Rank (Value)
Attack Vector (AV)	This metric reflects the context by which vulnerability exploitation is possible.	N (0.85) A (0.62) L (0.55) P (0.2)
Attack Complexity (AC)	This metric describes the conditions beyond the attacker’s control that must exist in order to exploit the vulnerability.	L (0.77) H (0.44)
Privileges Required (PR)	This metric describes the level of privileges an attacker must possess before successfully exploiting the vulnerability.	(if S=C/if S=U) N (0.85/0.85) L (0.62/0.68) H (0.27/0.5)
User Interaction (UI)	This metric captures the requirement for a human user, other than the attacker, to participate in the successful compromise of the vulnerable component.	N (0.85) R (0.62)
Scope (S)	The Scope metric captures whether a vulnerability in one vulnerable component impacts resources in components beyond its security scope.	U C
Confidentiality (C)	This metric measures the impact to the confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability.	H (0.56) L (0.22) N (0)
Integrity (I)	This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.	H (0.56) L (0.22) N (0)
Availability (A)	This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.	H (0.56) L (0.22) N (0)

- 式(2-2)の影響度, 式(2-4)の攻撃容易性, 共にメトリックの値が大きいほど大きな値を取り, 式(2-2)および式(2-3)のリスク値  $R_r$  もリスクが大きいほど大きな値を取るようになっている。
- 式(2-6)および式(2-7)は後述するメトリック  $Scope(S)$ に関する式で, 本論文では使用しない。
- リスク値  $R_r$  は 0～10 の値を取るようになっており, 値が大きいほどリスクが高いと評価される。
- Attack Vector (AV)については, Ver.2 の Access Vector に該当するメトリックで, ランクは N, A, L に加え, P(“Physical”)が追加された。これは L(“Local”)よりもさらに物理的にコンポーネントにアクセスし, 秘密情報の情報窃取や書き換えを行う攻撃手段に該当するものとして定義されている。表 2 にあるように, 値は N, A, L, P の順に大きく, 攻撃に有利とみなされている。
  - AV が “Physical”に該当する攻撃の例は, 文献[9]の “Annex 7: Application of Attack Potential to Smartcards and Similar Devices”の“5 Examples of Attack Methods”における, “5.1 Physical Attacks”, “5.5 Side-channel Attacks”などの攻撃事例に詳しい。
  - “Physical”の適用範囲には USB などインタフェースを持ち比較的アクセスしやすい攻撃も例示されているが, 攻撃のためにコンポーネントの電気部品のつけ外しが必要など, 自動車運用中での攻撃が困難な攻撃も含まれる。
  - 本研究における自動車システムのリスク数値化手法に CVSS Ver.3 および CVSS Ver.3.1 を用いる場合, AV をこの “Physical”には選ばないものとした。USP や SD カードのようなインタフェースを持つエントリーポイントは “Local”と判定する。
- Attack Complexity(AC)は, Ver.2 の Access Complexity(こちらも略称は AC)に該当するメトリックで, ランクが L(“Low”)と H(“High”)の 2 つになり粗くなっている。“High”については侵入後のシステムの挙動の偵察など, 攻撃に先駆けた準備行動が必要な場合に適用するものとなっている。本研究では引き続き, 自動車システム侵入後に経由するモジュールの数を判定基準に用いている。表 2 にあるように, 値は L, H の順に大きく, 攻撃に有利とみなされている。
- Privileges Required (PR)は CVSS Ver.2 の Authentication (Au)に該当するが, 単なる認証の回数という Au よりも特権レベルの概念の導入を行い, より柔軟な解釈ができるようになっている。本研究では引き続き, 自動車システム侵入後に必要とする認証の数を判定基準に用いている。例えば権限昇格が不要なら N, ユーザーかゲストレベルの権限でいいなら L, 管理者レベルの権限が必要なら H などのように評価する。表 2 にあるように, 値は N, L, H の順に大きく, 攻撃に有利とみなされている。
- User Interaction (UI)は CVSS Ver.3 および CVSS Ver.3.1 で加わったメトリックで, 攻撃が成功するために必要とする, 被害者となる自動車ユーザーが起こす何らかのアクションの有無

を評価する。表 2 にあるように、値は N, R の順に大きく、ユーザーのアクションに関係なく攻撃できる方が攻撃に有利とみなされている。

- 例えば GNSS を模した偽の装置から誤った位置情報を自動車に与える攻撃を考える場合、この攻撃が有効になるのは、ユーザーの判断ミスが誘発されうる状況もしくは自動運転中という条件は必要である。この場合に UI は R(“Required”)と評価される。
- Scope (S)は、CVSS Ver.3 および CVSS Ver.3.1 で加わったメトリックで、脆弱性を突いて攻撃が成功したコンポーネントが他のコンポーネントのリソースにも権限を持ち影響を与えていて、攻撃成功により本来意図したよりも大きな損害が発生しうる可能性を判定する。
  - 本研究における自動車システムのリスク数値化手法に CVSS Ver.3 および CVSS Ver.3.1 を用いる場合、システムの抽象度の関係でコンポーネントの関係をそこまで込み入ったものと想定していないため、基本的に U(“Unchanged”)と判定している。
- Confidentiality Impact (C), Integrity Impact (I), および Availability Impact (A)については、CVSS Ver.2 と同様に資産である機能および情報の気密性、完全性、および可用性が損なわれた場合の影響について判定している。影響が部分的である場合の L(“Low”), 甚大である場合の H(“High”), もしくは影響なしの N(“None”)と判定している。表 2 にあるように、値は H, L, N の順に大きく、攻撃された場合の資産の影響度、資産が損なわれると悪影響が大きいとみなされている。

CVSS はソフトウェアの脆弱性評価基準であるが、関連研究においてもシステムのセキュリティ分析に適用されているケースがある。例えば[44]では CVSS Ver.2 をエネルギー分野のスマートグリッドシステムに適用し、および[45]では CVSS Ver.3 を自動車システムに適用し、セキュリティ分析を行っている。

### 2.3.2 CWSS(Common Weakness Scoring System)

CWSS[12]は、CVSS とは異なる観点で脆弱性を分析する脆弱性評価基準で、2015 年に ITU-T にて標準化されている[46]。計算式を式(3-1)～(3-5)に、メトリックの定義およびランクを表 3 に、それぞれ示す。

$$\text{リスク値 } R_w = S_{\text{Base}} \times S_{\text{Surface}} \times S_{\text{Env}} \quad (3-1)$$

$$\text{基本値: } S_{\text{Base}} = 4 \{f(TI) \cdot (10TI + 5(AP + AL) + 5FC) \cdot IC\} \quad (3-2)$$

$$\text{エントリーポイントの評価: } S_{\text{Surface}} = \{20(RP + RL + AV) + 20SC + 15IN + 5AS\} / 100.0 \quad (3-3)$$

$$\text{環境の評価: } S_{\text{Env}} = \{f(BI) \cdot (10BI + 3DI + 4EX + 3P) \cdot EC\} / 20.0 \quad (3-4)$$

$$\text{影響度の補正式: } f(x) = 0(\text{if } x=0), 1(\text{otherwise}) \quad (3-5)$$

式(3-1)～式(3-5)および表 3 の CWSS の各メトリックについて補足する:

- 個々のメトリックの値は大きいほど攻撃に有利, もしくは攻撃を受けることでの資産のダメージが深刻であることを定めている.
- 式(3-2)の SBase, 式(3-3)の SSurface, 式(3-4)の SEnv, 共にメトリックの値が大きいほど大きな値を取り, 式(3-1)のリスク値  $R_w$  もリスクが大きいほど大きな値を取るようになっている.
- リスク値  $R_w$  は 0～100 の値を取るようになっており, 値が大きいほどリスクが高いと評価される.
- 各メトリックは程度に応じたランクを持つが, それらとは別にデフォルト値 D(“Default”), 不明 UK(“Unknown”), 適用外としてメトリックを使わない時の NA(“Not Applicable”)およびそれ以外のカスタム判定として任意の値を与える Q(“Quantified”)を持つ. 本論文では使用しないメトリックがある場合に対し NA を使用する以外, これらのランクは使用しない.
- Technical Impact (TI)は, 攻撃が成功した場合の制御の乗っ取りなど, 直接的な影響を評価する. 程度に応じて C(“Critical”), H(“High”), M(“Medium”), L(“Low”), および N(“None”)のランクで判定する. 表 3 にあるように, C, H, M, L, N の順に値が大きく, 攻撃を受けた際の影響が大きいとみなされている.
- Acquired Privilege (AP)は, 攻撃が成功した時に攻撃者が得られる権限を評価する. 特権レベルに応じて A(“Administrator”), P(“Partially-Privileged User”), RU(“Regular User”), L(“Limited / Guest”)および N(“None”)で判定する. 表 3 にあるように, A, P, RU, L, N の順に値が大きく, 攻撃が成功した場合の攻撃者のメリットが大きいとみなされている.
- Acquired Privilege Layer (AL)は, 攻撃が成功した時に攻撃者が特権を得られるシステムレイヤを評価する. レイヤに応じて A(“Application”), S(“System”), N(“Network”)および E(“Enterprise Infrastructure”)で判定する. 表 3 にあるように, A=E, S, N の順に値が大きく, 攻撃が成功した場合の攻撃者のメリットが大きいとみなされている.
- Internal Control Effectiveness (IC)は, アーキテクチャ, 設計, または実装を通じてソフトウェアに明示的に組み込まれた制御, 保護メカニズム, または緩和策について評価する. 保護機能の有無や強さに対して, N(“None”), L(“Limited”), M(“Moderate”), I(“Indirect”), B(“Best-available”), および C(“Complete”)で判定する. 表 3 にあるように, N, L, M, I, B, C の順に値が大きく, 攻撃が有利とみなされている.
- Finding Confidence (FC)は, 脆弱性に関するレポートを検証した結果, 信憑性があるかを評価する. 脆弱性が正しいとする T(“Proven true”)の他, 部分的に正しい LT(“Proven locally true”), 誤りとする F(“Proven false”)で判定する. 表 3 にあるように, T, LT, F の順に値が大きく, 攻撃が有利とみなされている.

表 3: CWSS のメトリックとランク [12]

Table 3: Metrics and Ranks of CWSS [12]

Metric	Concept	Rank (Value)
Technical Impact (TI)	The potential result that can be produced by the weakness, assuming that the weakness can be successfully reached and exploited.	C(1.0), H(0.9), M(0.6), L(0.3), N(0.0)
Acquired Privilege (AP)	The type of privileges that are obtained by an attacker who can successfully exploit the weakness.	A(1.0), P(0.9), RU(0.7), L(0.6), N(0.1)
Acquired Privilege Layer (AL)	The operational layer to which the attacker gains privileges by successfully exploiting the weakness.	A(1.0), S(0.9), N(0.7), E(1.0)
Internal Control Effectiveness (IC)	the ability of the control to render the weakness unable to be exploited by an attacker.	N(1.0), L(0.9), M(0.7), I(0.5), B(0.3), C(0.0)
Finding Confidence (FC)	the confidence that the reported issue is a weakness that can be utilized by an attacker	T(1.0), LT(0.8), F(0.0)
Required Privilege (RP)	The type of privileges that an attacker must already have in order to reach the code/functionality that contains the weakness.	N(1.0), L(0.9), RU(0.7), P(0.6), A(0.1)
Required Privilege Layer (RL)	The operational layer to which the attacker must have privileges in order to attempt to attack the weakness.	A(1.0), S(0.9), N(0.7), E(1.0)
Access Vector (AV)	The channel through which an attacker must communicate to reach the code or functionality that contains the weakness.	I(1.0), R(0.8), V(0.8), A(0.7), L(0.5), P(0.2)
Authentication Strength (AS)	The strength of the authentication routine that protects the code/functionality that contains the weakness.	S(0.7), M(0.8), W(0.9), N(1.0)
Level of Interaction (IN)	the actions that are required by the human victim(s) to enable a successful attack to take place.	A(1.0), T(0.9), M(0.8), O(0.3), H(0.1), NI(0.0)
Deployment Scope (SC)	Whether the weakness is present in all deployable instances of the software, or if it is limited to a subset of platforms and/or configurations.	A(1.0), M(0.9), R(0.5), P(0.1)
Business Impact (BI)	The potential impact to the business or mission if the weakness can be successfully exploited.	C(1.0), M(0.9), M(0.6), L(0.3), N(0.0)
Likelihood of Discovery (DI)	The likelihood that an attacker can discover the weakness	H(1.0) M(0.6) L(0.2)
Likelihood of Exploit (EX)	the likelihood that, if the weakness is discovered, an attacker with the required privileges/authentication/access would be able to successfully exploit it.	H(1.0) M(0.6) L(0.2), N(0.0)
External Control Effectiveness (EC)	the capability of controls or mitigations outside of the software that may render the weakness more difficult for an attacker to reach and/or trigger.	N(1.0), L(0.9), M(0.7), I(0.5), B(0.3), C(0.1)
Prevalence (P)	How frequently this type of weakness appears in software.	W(1.0), H(0.9), C(0.8), L(0.7)

- Required Privilege (RP)は、攻撃に必要な権限レベルを評価する。特権レベルに応じて A(“Administrator”), P(“Partially-Privileged User”), RU(“Regular User”), L(“Limited / Guest”)および N(“None”) で判定する。表 3 にあるように、AP とは逆に N, L, RU, P, A の順に値が大きく、攻撃が有利とみなされている。
- Required Privilege Layer (RL) は、攻撃に必要な権限のシステムレイヤを評価する。レイヤに応じて A(“Application”), S(“System”), N(“Network”)および E(“Enterprise Infrastructure”) で判定する。表 3 にあるように、A=E, S, N の順に値が大きく、攻撃が有利とみなされている。
- Access Vector (AV)は CVSS の AV と同様、攻撃の侵入口、エントリーポイントの観点进行评估する。エントリーポイントに応じて、I(“Internet”), R(“Intranet”), V(“Private network”), A(“Adjacent network”), L(“Local”), P(“Physical”) で判定する。表 3 にあるように、I, R, V, A, L, P 順に値が大きく、攻撃が有利とみなされている。
  - CVSS Ver.3 や Ver.3.1 とは定義が異なり、“Physical”の定義が USB, CD, マウスやキーボードなどの、インタフェース経由でのアクセスも対象としている。そのため、本研究の自動車システムのリスク分析で CWSS を用いる場合、P も使用している。
- Authentication Strength (AS)は、CVSS Ver.2 の Authentication (Au)や CVSS Ver.3 および Ver.3.1 の Privileges Required (PR)に該当する、認証の強さを評価する。本研究では CVSS と同様、必要な認証の回数に応じて S(“Strong”), M(“Moderate”), W(“Weak”), および N(“None”) で判定する。表 3 にあるように、N, W, M, S の順に値が大きく、攻撃が有利とみなされている。
- Level of Interaction (IN)は、CVSS Ver.3 および Ver.3.1 の User Interaction (UI)に該当する、攻撃が成功するために必要とする、被害者となる自動車ユーザーが起こす何らかのアクションの有無や程度を評価する。アクションの有無や程度に対して、A(“Automated”), L(“Typical/Limited”), M(“Moderate”), O(“Opportunistic”), H(“High”), および N(“No Interaction”) で判定する。表 3 にあるように、A, L, M, O, H, NI の順に値が大きく、攻撃が有利とみなされている。
- Deployment Scope (SC)は CVSS Ver.3 および CVSS Ver.3.1 の Scope(S)と類似したメトリックで、攻撃のもととなるソフトウェアの脆弱性がシステムに含まれるコンポーネントに波及する範囲を評価する。範囲に応じて A(“All”), M(“Moderate”), R(“Rare”), および P(“Potentially reachable”) で判定する。表 3 にあるように、A, M, R, P の順に値が大きく、攻撃を受けた際の影響が大きいとみなされている。
- Business Impact (BI)は、攻撃が成功した場合のビジネスもしくはミッションに関する潜在的な影響を評価する。程度に応じて C(“Critical”), H(“High”), M(“Medium”), L(“Low”), およ

び N(“None”)のランクで判定する。表 3 にあるように、C, H, M, L, N の順に値が大きく、攻撃を受けた際の影響が大きいとみなされている。

➤ 脆弱性の評価において CVSS には無い、金銭(Financial)に関するメトリックである。

- Likelihood of Discovery (DI)は、攻撃に用いる脆弱性の見つけやすさを評価する。程度に応じて H(“High”), M(“Medium”), および L(“Low”)で判定する。表 3 にあるように、H, M, L の順に値が大きく、攻撃に有利とみなされている。
- Likelihood of Exploit (EX)は、攻撃の可能性がどれだけあるかを評価する。程度に応じて H(“High”), M(“Medium”), および L(“Low”)で判定する。表 3 にあるように、H, M, L の順に値が大きく、攻撃に有利とみなされている。
- External Control Effectiveness (EC) は、攻撃者が弱点に到達したり、引き起こしたりするのをより困難にする可能性がある、ソフトウェアの外部での制御または緩和の機能について評価する。保護機能の有無や強さに対して、N (“None”), L(“Limited”), M(“Moderate”), I(“Indirect”), B(“Best-available”), および C(“Complete”)で判定する。表 3 にあるように、N, L, M, I, B, C の順に値が大きく、攻撃に有利とみなされている。
- Prevalence (P)は、攻撃に用いられる脆弱性について起きる頻度や認知度を評価する。程度に応じて、W(“Widespread”), H(“High”), C(“Common”), および L(“Limited”)と判定する。表 3 にあるように、W, H, C, L の順に値が大きく、攻撃に有利とみなされている。
  - 本研究における自動車システムのリスク数値化手法に CWSS を用いる場合、システムの前提として想定するのが困難であるため、基本的に NA(“Not Applicable”)と判定している。

CWSS はメトリックの数が多く、細かいランク分けも行えるため、個々の脅威に対して CVSS よりきめ細かな数値の差を与えることができることに特徴がある。また自動車システムのセキュリティ標準である ISO/SAE 21434[2]や SAE J3061[38]と同様に、資産が損害を受けることでの影響度を金銭 (Financial)の観点で評価できるメトリック Business Impact(BI)を持つ。

筆者が 2018 年に発表した論文 [47]にて、JASO TP15002 と CWSS を組合せた手法 RSS-CWSS で産業制御システムのコンポーネントであるデータロガーのリスク分析を行い、リスクの細かな差別化が出来ていることを確認した。そしてその後の本研究にてさらに改良した手法 RSS-CWSS\_CPS を導入している。



## 2.4 自動車システムで特徴的なエントリーポイント:

### ダイレクトアクセス攻撃

最後に、自動車システムの攻撃手法である、ダイレクトアクセス攻撃について説明する。

サイバーフィジカルシステムは自動車、鉄道、航空機、船舶、工場、重要インフラなど多くの分野で運用されており、自動車システムはそのひとつであるが、他のシステムと比べてシステム外からの物理的なアクセスが行いやすいという特徴がある。例えば工場における産業制御システムでは、工場内部の制御機器のある OT(Operational Technology)エリアのネットワークへのサイバー攻撃を防ぐため、ID カードでの認証システムや外部からの機器持ち込み制限など、技術的にも環境的にも内部への侵入対策を何重にも施すことが可能である。また、米国国土安全保障省が 2015 年に公開した、“Seven Strategies to Defend ICSs” [48]でも、OT と外部との通信も可能であればデータダイオード(伝送路の一部を電気/光、光/電気の信号変換器を介して光ファイバーとし、片方の光ファイバーを除去することで通信を物理的に一方向にする装置で、実際に市販されている)を使用し物理的に隔離することで、サイバー攻撃の可能性を根本的に排除する対策すら検討されている。こういったケースに比べ自動車システムでは、物理的に直接車載ネットワークに不正な機器を接続するなどの、ダイレクトアクセス攻撃が行いやすい。これには以下のようないくつかの技術的/環境的な理由がある:

- 車種によっては、重要な機能に係る ECU に繋がる配線が自動車の表層を走っており、外部から容易にアクセスできる場合がある。大規模な高級自動車窃盗団が行った CAN インベーターによる盗難事件がその一例で、2021 年の日本で立件された[11].
  - 図 8 は、CAN インベーターの攻撃手口を図示したものである。被害を受けた自動車の前方バンパーを外した所にドアロック解除とエンジン始動を可能にする重要な ECU に繋がる CAN バスがあったとされ、ここに不正な CAN メッセージを送信できる機器を接続することで、ドアロックの解除とエンジン始動が行えた。
- 認証や暗号化がなされておらず、プロトコルが解析されている CAN バスのようなレガシーネットワークを用いており、不正なメッセージの挿入などの攻撃に弱い。CAN バス経由で ECU に実施できる攻撃ではバスオフ攻撃[49]がある。
  - CAN のプロトコルを悪用したもので、不正な CAN メッセージをタイミングよく送ることで送信エラーのカウントを操作し、狙った ECU をシャットダウンさせる攻撃である。
  - CAN FD と SecOC[50]のような、MAC 認証を用いたなりすまし防止策も登場している。

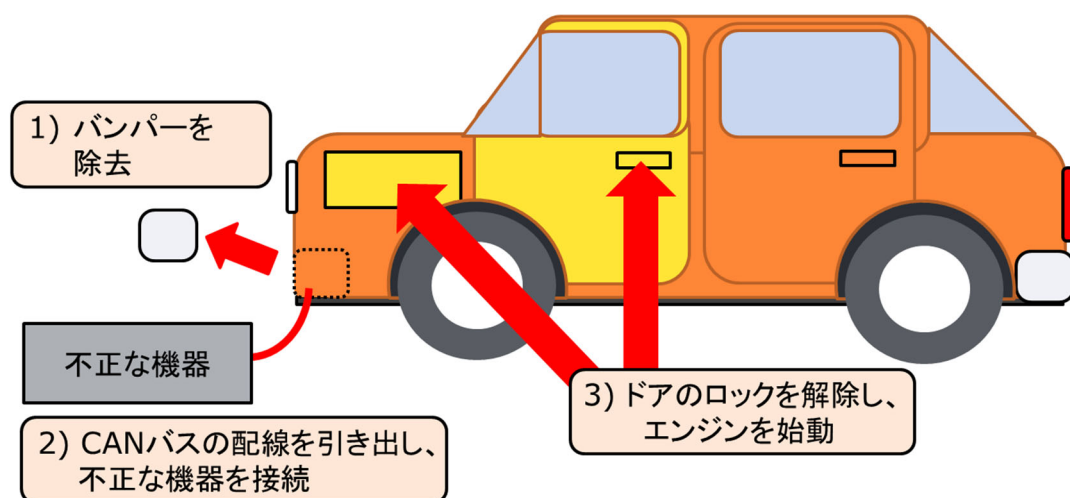


図8: CANインバーダーによる自動車盗難の手口

Figure 8: Car Theft Techniques Used by CAN Invader

- コンシューマ向け機器であるため流通台数が多く、リバースエンジニアリングの機会に恵まれている。

2011 年頃、まだ Miller らがサイバー攻撃による自動車システムの乗っ取り[1]を実証する以前の Checkoway らによる研究 [51]では、ダイレクトアクセス攻撃が行えるような状況であるならブレーキの配線を切るなどもっと直接的な攻撃を行えるから、サイバー攻撃のエントリーポイントとして考えるのは現実的ではないという見解があった。また、2.3 節で説明した CVSS Ver.2 でリスクを評価した場合でも、ダイレクトアクセス攻撃のような物理的に車載ネットワークに接続する方法はスコアが低かった。しかし CAN インバーダーのような攻撃が現実には犯罪に利用されていることを考えると、ダイレクトアクセス攻撃の脅威の持つリスクは実際にはもっと高く評価されるべきなのではと考えられる。

リスク分析によりこのダイレクトアクセス攻撃が検知できるかについて考察し、より実際の局面に即した評価ができるリスク分析手法を検討したいというのが、本研究の動機の 1 つである。

## 2.5 むすび

本章では、本論文における研究内容を述べる準備として、セキュリティ設計概論、セキュリティ設計ガイドラインの JASO TP15002 および ISO/SAE21434 の紹介、リスク数値化に用いる CVSS や CWSS の脆弱性評価基準、および本論文の課題に係るサイバー攻撃であるダイレクトアクセス攻撃について説明した。

まずセキュリティ設計について手順、必要な情報を、成果物に関して整理した。システム仕様書から分析対象のシステムモデルを作る際に必要な情報とその関係性を図示し、システム仕様書から抽出すべき情報、分析評価モデル作成のために必要な情報、およびそれらから導出する脅威やリスクに関する情報について説明した。

次に、サイバーフィジカルシステムであると同時にセーフティクリティカルシステムでもある自動車システムにおける、セキュリティ設計標準の成立に至る経緯と関連研究を示し、セキュリティ設計ガイドライン標準である JASO TP15002 と ISO/SAE 21434 を紹介した。そして両標準におけるセキュリティ設計の手順を比較し、両者に大きな違いはなく本研究を適用できることも示した。本研究では当初 JASO TP15002 をベースとしていたが、これが ISO/SAE 21434 に置き換わる形で廃案となり、後半は ISO/SAE 21434 をベースに研究を進めた。

そして、リスク分析でリスクの重大さを数値化する手法として用いられる、脆弱性評価基準について CVSS(Ver.2, Ver.3.0 および Ver.3.1)および CWSS を紹介し、リスク計算式とメトリックについて詳細を説明した。本論文では CWSS に着目し、これをベースとしサイバーフィジカルシステムのリスク分析を行う、新しいリスク数値化手法を考案する。そして提案手法の詳細な分析と、従来手法として用いられている CVSS との比較を行う。

最後に、自動車システムにおけるダイレクトアクセス攻撃について説明し考えを述べた。他分野のサイバーフィジカルシステムと比較し、物理的にシステム内部にアクセスしやすく、暗号化されておらずプロトコルも解析済であるレガシーなネットワークが残されている自動車システムでは、実際にそれらを悪用したインシデントが発生している。このダイレクトアクセス攻撃における脅威は、従来手法ではリスクが低いものと考えられ評価基準も低くみなされていたが、本研究ではこのリスクを適切に評価しようと試みる。

## 第 3 章 資産コンテナ方式, および 2 ステップリスク分析の考案

本章では、課題であるリスク数値化を適用するリスク分析のアプローチとして筆者が過去に提案した、「資産コンテナ方式」および「2 ステップリスク分析」の紹介を主に、本論文の研究に関連する先行研究について説明する。本手法は筆者の 2017 年の論文 [13] でアイデアとして提案し、さらにその後の論文 [17][52] で本手法に適用するリスク数値化手法を検討している。本手法は、攻撃経路の網羅性を意識しつつ、攻撃被害者側の情報のみで評価を行うための脅威の定義手法である。

### 3.1 セキュリティ設計手順効率化の試み

序章でも述べたが、JASO TP15002[14]や ISO/SAE 21434[2]などのセキュリティ設計ガイドラインを実際の作業手順に落とし込む際に、効率化が課題となる。

考えられる脅威は全て検討し、合理的に定めた基準でリスクを分析してその評価結果を第三者にも納得できるよう作成するというのがセキュリティ設計ガイドラインであるが、実際にこれらを作業手順に落とし込む場合にギャップが存在する。

製品開発において、セキュリティを考慮した設計を行う場合に、なるべく工数やコストを増加させたくないというのが動機であり大前提である。そしてそのためにはリソース運用を最適化し、精査のためにセキュリティ専門家を外注してコストを増やすのは極力避け、なるべく自社の開発者だけで行ったセキュリティ設計が網羅性や合理性を持つように作業手順を考えたい。これが効率化を求める動機である。

本研究の前提として、脅威抽出における網羅性を担保しつつ、開発者が比較的少ない工数でリスクを分析しやすくするために、脅威を表す観点を絞るアプローチとして検討したアイデアが、「資産コンテナ方式」および「2 ステップリスク分析」である。

### 3.2 資産コンテナ方式と 2 ステップリスク分析

資産コンテナ方式はガイドライン JASO TP15002 のフェーズ 2 にて脅威を記述する手法として用いられている、5W 法を改良した手法である。5W 法とは 1.2 節でも挙げた、脅威を 5 つの

“W”, 即ち“Who(誰が)”, “When(いつ)”, “Where(どこから)”, “Why(どういう意図で)”, “What(何を)”で記述する手法であるが, これら 5 つのパラメータの組み合わせになるため脅威の数が膨大(～数千件)になりうるのと, これらパラメータが網羅性を担保する上で定義が不明瞭という課題があった。例えば“Where”はどこを指すのか, “Why”は攻撃被害者側からは判断しづらい攻撃者のモチベーションや技術に係る, “What”は攻撃手段や攻撃の影響などが考えられ, それぞれ解釈の余地が広すぎるためである。

考案した資産コンテナ方式ではこのような 5W 法の問題を踏まえ, 観点を整理し解釈の範囲を限定することで, 網羅性の担保をはかった手法である。具体的には攻撃を受ける側が情報として持っている, システム内の伝送経路と守るべき資産を以下のように観点に振り分ける。

- “Where”はエントリーポイント, システムと外部を繋ぐインタフェースのひとつ。
- “What”の内容から以下の 2 つの観点を抽出する。
  - “At”: 攻撃の到達する機能モジュール(機能を実現する, ひとまとまりのサブシステム)。
  - “Asset”: 上記機能モジュールの持つ, セキュリティ上守るべき資産。
- “Where”と“At”の組み合わせで攻撃経路の最短経路を定義する。

図 9 がこの脅威の捉え方を図示したものである。図の点線の四角が分析対象のシステムと外部環境との境界線, 赤い丸がエントリーポイント(“Where”), システム内の黒い丸が攻撃目標の機能モジュール(“At”), 黒丸の中の黒い四角が守るべき資産(“Asset”)である。エントリーポイントから機能モジュールに至る矢印が攻撃経路を示しており, これは“Where”と“At”の組合せで決定できる。

攻撃者は資産の容れ物である機能モジュール(“At”)から手を入れて資産を奪うもしくは損害を与えようとしていると考える手法であるので, 「資産コンテナ方式」と呼称した[13]。これは攻撃を受ける側から見た情報のみで 5W 法よりシンプルに脅威を定義する手法であり, “Where”と“At”と“Asset”の組み合わせを総当りさせることで, 少なくとも「攻撃経路と対象の資産との組合せを網羅する」という観点で想定しうる脅威を検討したと主張できる。

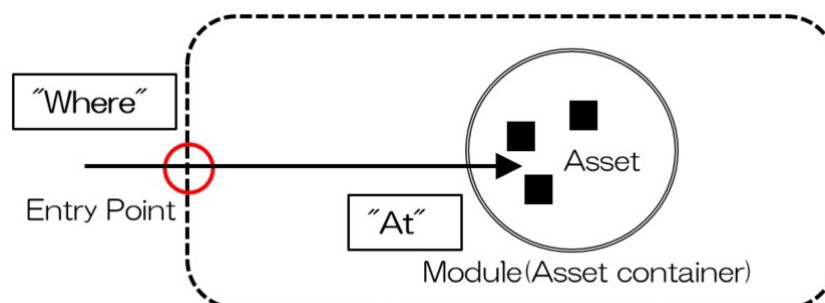


図9:アイデア: 資産コンテナ方式による脅威の捉え方

Figure 9: Idea: How to Interpret the Threat by Asset Container Method

これら 3 つの要素は網羅性の主張に必要であるが、それ以外の要素、すなわち“Who”, “When”, “Why”, および“What”の残りの詳細が不要というわけではなく、最終的な攻撃要因の分析には必要な情報である。そのため資産コンテナ方式に合わせ、脅威の 5W の定義については以下のように 2 段階の手順で行う。これを「2 ステップリスク分析」と呼称する。

- ステップ1: 脅威を“Where”と“At”と“Asset”の組み合わせで定義する。
- ステップ2: ステップ 1 の脅威について, “Who”, “When”, “Why”, および“What”に関する残りの詳細な内容を定義する。  
追加する観点に応じてひとつの“Where”と“At”と“Asset”の組み合わせに対し, 複数の脅威を定義しても良い。

資産コンテナ方式と 2 ステップリスク分析を併用した 5W の定義手順を, JASO TP15002 や ISO/SAE 21434 の脅威抽出に適用する場合, 以下の 3 つのメリットがある:

- まず作業手順の観点から, セキュリティ評価作業をより形式化できる。特に脅威の定義を 2 つのタスクに分けることで作業の最適化が可能である。
  - 例えば“Where”, “At”および“Asset”を定義した段階で, CVSS などの攻撃容易性と資産の損害のインパクトを評価する脆弱性評価基準ではリスク値を算出することが可能である。
  - ステップ 1 でリスクの数値化が可能であるので, この時点で重要と思われる脅威をふるい分けし, ステップ 2 の定義を優先的に行うことで, 対策検討などの以降の手続きを時間とリソースに合わせ効率良く進めることができる。
- 次にセキュリティ設計の成果物の観点から見ると, 本方式は脅威の説明から曖昧さを取り除くことができるため, 脅威分析結果の可読性を向上させることができると考える。
  - 観点を“Where”, “At”および“Asset”に絞り込むことで, 明確な判断基準を開発者間での議論で詰めやすい。
- そして, 資産コンテナ方式を用いることで, 少なくとも「攻撃経路と対象の資産との組合せを網羅する」という観点から想定しうる脅威を検討したと主張できる。

以上により, これらの手法はセキュリティ設計における効率化の課題解決に向けたアプローチとして有用であると考えており, 本論文の研究の主題である第4章, 第5章のケーススタディで前提として使用している。

### 3.3 ケーススタディ例

本節では筆者の論文 [13]における自動車システムのケーススタディを交え、資産コンテナ方式の具体的な運用について説明する。なおここで例示する自動車システムモデルのネットワーク構成図における各要素、インタフェース、および資産の名称に関しては、第 4 章および第 5 章で使用する自動車システムモデルに合わせ名称を変更している。

まずシステム仕様書を基に、分析対象のネットワーク構成図を作成する。図 10 が文献[13]でケーススタディとして使用したコネクテッドカーの分析対象モデルである。点線の四角がシステムと外部環境との境界線であり、システム内の実線の丸が各機能モジュールを、システム外部の丸がシステム外の通信相手や環境を指す。丸の間を結ぶ実線は通信路であり、線に添えられた名前は通信規格を指す。そして実線と点線と交わったところにある赤い丸は、システム外から見たエン트리ポイント、即ち通信インタフェースである。

図 10 の各要素について補足する。

システム内の各機能モジュール:

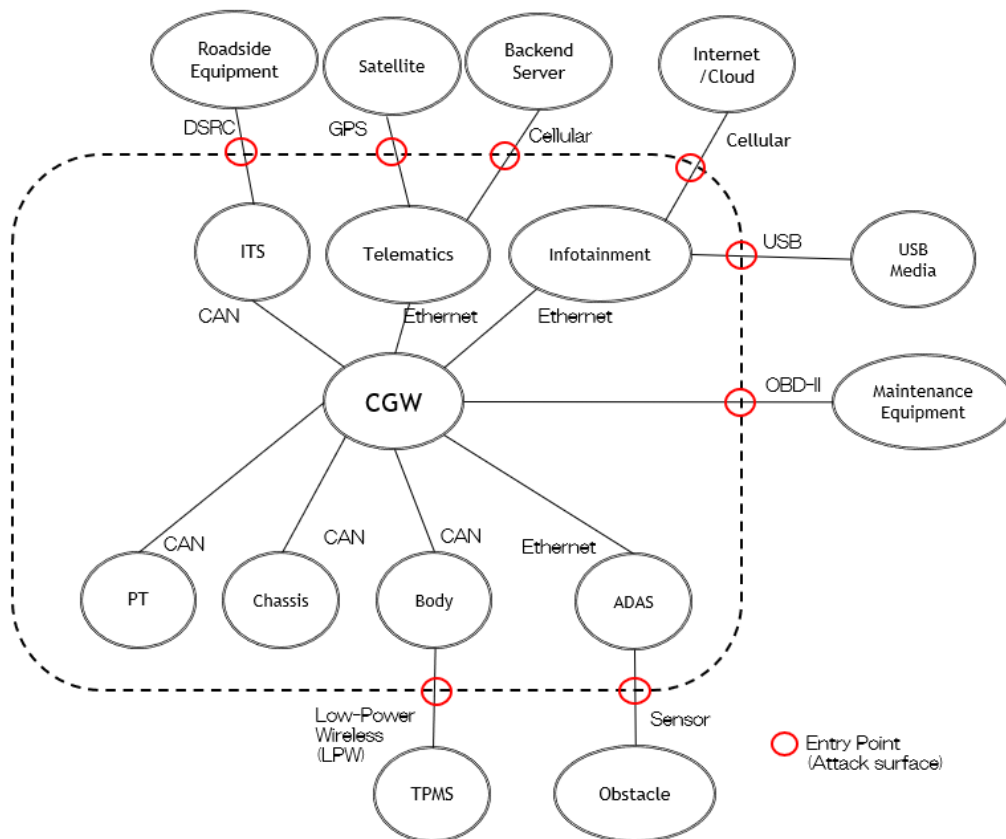


図10: コネクテッドカーの分析対象モデル

Figure 10: Target Model for Evaluation: Connected Car

- **PT(Power-Train):** エンジンなど, 駆動系 ECU をまとめた機能モジュール.
- **Chassis:** ブレーキなど, シャーシ系 ECU をまとめた機能モジュール.
- **Body:** ドアロックなど, ボディ系 ECU をまとめた機能モジュール.
- **ADAS:** 運転補助機能など, ADAS (Advanced driver-assistance systems: 先進運転支援システム) 系 ECU をまとめた機能モジュール.
- **ITS:** ITS など, V2X(Vehicle to X)通信を行う ECU をまとめた機能モジュール.
- **Telematics:** バックアップサーバなどとの通信を行う, テレマティクス系 ECU をまとめた機能モジュール.
- **Infotainment:** ナビゲーションシステムやエンターテイメント系アプリの提供など, インフォテインメント系 ECU をまとめた機能モジュール.
- **CGW(Central Gateway):** CAN バスと Ethernet ネットワークを接続しデータを変換, CAN バス間での通信タイミングを調整などを行う機能モジュール.

#### エントリーポイント:

- **Low-Power Wireless (LPW):** TPMS と通信を行う近接無線通信インタフェース. なお文献[13]で分析対象モデルを検討するにあたり, TPMS の持つセンサ情報が駆動系 ECU と連携するのではないかと考え, LPW のインタフェースを Power-Train に設けていた. しかし現在 TPMS は Body 系の ECU として分類されているため, 本論文では LPW のインタフェースを Body 系に移動させている.
- **Sensor:** 障害物レーダー/センサ.
- **DSRC:** Roadside Unit(RSU)と通信を行う遠距離無線通信インタフェース.
- **GPS:** GPS を受信し位置情報を取得する遠距離無線受信インタフェース.
- **Cellular:** 携帯電話通信などの遠距離無線通信を用いる通信インタフェース.
- **USB:** USB メモリなどを接続するための物理インタフェース.
- **OBD-II:** OBD-II などを使用した, CGW に対して車内にあるコネクタを介してダイアグメツセージを受ける物理インタフェース.

#### システム外の通信相手や環境:

- **TPMS:** Tire Pressure Monitoring System, タイヤ空気圧センサ.
- **Obstacle:** 障害物.
- **Roadside Equipment:** 路側機もしくは他の自動車.
- **Satellite:** GPS 衛星.
- **Backend Server:** ファームウェアやアプリをダウンロードしたり, データを保存したりするバックエンドサーバー.



- **Internet/Cloud:** アプリのダウンロードや Web ブラウジングに利用する, インターネットもしくはクラウドサービス.
- **USB Media:** USB をインタフェースとするメモリーデバイスなど.
- **Maintenance Equipment:** メンテナンス用診断機器.

次に, 各機能モジュールが持つ機能や情報のうち, 改ざん, 情報漏洩などのサイバー攻撃から守らねばならないものを「守るべき資産(Asset to be protected)」として洗い出す. 表 4 が図 10 の事例における機能モジュールと守るべき資産のリストである. 研究初期のモデルのため, 機能モジュールの持つ通信機能をリストに含めていないなど, リストに不備があるが, その後の研究で不足する資産を補うこととなった. 以下資産の内容について補足する:

- **Control function:** 自動車に対し, 各機能モジュールに応じた制御を行う機能.
- **Auth. function:** 無線通信の確立や利用者の機能モジュールへのアクセスの際に行う認証機能.
- **Auth. information:** 各認証機能に必要な, パスワードなどの認証情報.

表 4: 機能モジュールおよび資産のリスト

Table 4: The List of Function Modules and Their Assets

#	Module name	Function	Assets to be protected	C	I	A
1	PT	Control functions for driving vehicle related to Engine, Motor, Fuel, Battery, Transmission, etc.	Control function		✓	✓
2	Chassis	Control functions for operating vehicle related to Brake and Steering.	Control function		✓	✓
3	Body	Control functions for operating vehicle body equipment related to Door lock, Air conditioner, Lights and Blinker.	Control function		✓	✓
			Control input data		✓	
			Sensor information		✓	
4	ADAS	Automatic brake, Lane-keeping control, Inter-vehicle distance control, etc. Functions which bring safety and comfort working together other vehicle control functions.	Control function		✓	✓
			Sensor information		✓	
5	CGW	Functions for integration and transformation of Ethernet and CAN communication. At the same time, it acts as fault diagnosis port, OBD (On-Board Diagnostics) -II.	Control function		✓	✓
			Flow/Storage data		✓	
6	ITS	Functions via roadside-to-vehicle or vehicle-to-vehicle communication, ETC, ITS (Intelligent Transport System), etc.	Auth. function		✓	✓
			Auth. information	✓	✓	
			Control information		✓	✓
7	Telematics	Functions for remote control services. For example, collection service of location information, remote door-lock service, remote lighting-on service, etc.	Auth. function		✓	✓
			Auth. information	✓	✓	
			Personal information	✓	✓	
			Request to server		✓	✓
			Vehicle status information	✓	✓	
8	Infotainment	Functions for information and entertainment. For example, car navigation system, audio equipment, key-less entry system, etc.	Auth. function		✓	✓
			Auth. information	✓	✓	

- **Sensor information:** TPMS からのタイヤ空気圧の情報, またレーダーやセンサから取得され ADAS 機能モジュールで利用される, 障害物や他車に関する情報.
- **Control input data:** Body 系の制御信号(ドアロック解除など).
- **Flow/Storage data:** CGW で処理する車載ネットワーク内の通信データ.
- **Communication function:** ETC 決済など, ITS の路側機との通信機能.
- **Personal information:** テレマティクスのサービスで必要なユーザーの個人情報.
- **Request to server:** Download Center/Server との通信機能.
- **Vehicle status information:** 自動車の診断データ, 位置情報, 周囲との通信結果など.

守るべき資産それぞれにおいては, 資産の何が損なわれると問題になるのか,

C(Confidentiality: 機密性), I(Integrity: 完全性), および A(Availability: 可用性)の観点にチェックを入れておく.

資産コンテナ方式では, エントリーポイントが“Where”, 機能モジュールが“At”, 各機能モジュールがそれぞれ持つ資産を “Asset”とし, 実現可能な組み合わせを全て脅威として計上する. 組み合わせはこれらを乗算した数となるため, あまり数が膨大にならないよう, 適度な抽象化を心がける必要がある. 目安としては, 機能モジュールが 10 個を越えない程度に抽象化を行えると良い.

表 5 が資産コンテナ方式に基づいた脅威の記述である. この表のようにまず左の 3 列の “Where”, “At”, および “Asset”について記述するのを第 1 ステップとし, 残りの “Who”, “When”, “Why”, および “What”の残りの詳細な内容を記述するのを第 2 ステップとする.

例えば表 5 の 1 行目, 脅威#1 であるが, 第 1 ステップで「OBD-II から侵入し, 駆動系(Power-train)機能モジュールの制御機能(Control function)を攻撃する脅威」と定義し, 第 2 ステップで「保守員がメンテナンスの際に不用意に故障させてしまう」を定義する. これにより「保守員がメンテナンスの際に OBD-II を使った際に, 駆動系機能モジュールの制御機能を不用意に故障させてしまう脅威」が出来上がる.

第 2 ステップでの残りの観点の内容記述に関しては, リスク値の算出を優先し後回しにする. 理由としては以下の通りである:

- 文献[13]で用いている CVSS では, これらの観点だけでリスク値を算出できるため.
- 同じ “Where”, “At”, および “Asset”の組でも残りの観点の組み合わせが複数考えられる場合があるため, 精査を行うならまずリスク値を求めて, 値の大きい重要脅威から着手するのが効率良いと思われるため.

- 例えば先程の脅威#1 の第 2 ステップにて「保守員がメンテナンスの際に不用意に故障させてしまう」の他に「悪意の第三者が駐車中に故意に故障させてしまう」という観点を付け加えることが可能だが、攻撃容易性や資産が受ける損害の影響は変わらない。であれば、この部分の精査は後回しにしてもよいと思われる。

表 6 が、資産コンテナ方式の 3 つの観点から CVSS のリスク値を求めた例である。“Where”と“Att”の観点でシステムへの侵入口と攻撃経路を推定できるため、AV, AC, Au の攻撃容易性 (AE: Attack Ease)を、“Asset”の C, I, A から資産が損害を受けることでの影響度 (EF: Effect

表 5: 資産コンテナ方式に基づく脅威の記述

Table 5: Threat Description based on Asset Container Method

#	Where	Att	Asset	Who	When	Why	What
1	OBD-II	PT	Control function	Maintenance staff	maintenance	Negligibly	cause malfunction
5	LPW	PT	Control function	Outsider	regular use	Deliberately	cause malfunction
9	DSRC	PT	Control function	Outsider	regular use	Deliberately	cause malfunction
28	Cellular	Chassis	Control function	Outsider	regular use	Deliberately	cause malfunction
29	Cellular	Chassis	Control function	Outsider	regular use	Deliberately	cause malfunction
30	USB	Chassis	Control function	Outsider	regular use	Deliberately	cause malfunction
45	LPW	ADAS	Control function	Outsider	regular use	Deliberately	cause malfunction
47	DSRC	ADAS	Control function	Outsider	regular use	Deliberately	cause malfunction
49	Cellular	ADAS	Control function	Outsider	regular use	Deliberately	cause malfunction
56	OBD-II	CGW	Control function	Outsider	regular use	Deliberately	cause malfunction
59	LPW	CGW	Flow/Storage data	Outsider	regular use	Deliberately	write wrong data
60	DSRC	CGW	Control function	Outsider	regular use	Deliberately	cause malfunction
62	Cellular	CGW	Control function	Outsider	regular use	Deliberately	cause malfunction
65	Cellular	CGW	Flow/Storage data	Outsider	regular use	Deliberately	write wrong data
66	USB	CGW	Control function	Outsider	regular use	Deliberately	cause malfunction

表 6: 資産コンテナ方式に CVSS を適用した例

Table 6: Example of Applying CVSS to Asset Container Method

#	Where	At	Asset	AV	AC	Au	AE	C	I	A	EF	Risk Value
103	Cellular	Telematics	Auth. information	N	L	S	8.0	Complete	Complete	None	9.2	8.5
104	Cellular	Telematics	Personal information	N	L	S	8.0	Complete	Complete	None	9.2	8.5
62	Cellular	CGW	Control function	N	M	S	6.8	None	Complete	Complete	9.2	7.9
58	LPW	CGW	Control function	A	M	S	4.4	None	Complete	Complete	9.2	6.6
60	DSRC	CGW	Control function	A	M	S	4.4	None	Complete	Complete	9.2	6.8
64	Cellular	CGW	Control function	A	M	S	4.4	None	Complete	Complete	9.2	6.8
24	USB	PT	Sensor information	L	H	S	1.5	None	Complete	None	6.9	3.8
42	USB	Body	Control input data	L	H	S	1.5	None	Complete	None	6.9	3.8
37	Cellular	Body	Control function	N	H	S	3.9	None	Partial	Partial	4.9	3.6

Factor)を、そして両者を総合したリスク値をそれぞれ得ることができる。例えば表 6 の 1 行目、脅威#103 は以下のようにそれぞれの値が算出される:

- 「Cellular(遠距離無線通信インタフェース)から侵入し、Telematics 機能モジュールの認証情報 (Authentication Information)を攻撃する脅威」である。
- 遠距離無線通信は車との距離に依存しないため、通信インタフェースの中では最もカジュアルに攻撃が可能である。エントリーポイントの攻撃容易性を決めるメトリック AV は攻撃容易性が最も有利な N(“Network”: 数値は 1.00)と判定される。
- Telematics 機能モジュールの持つインタフェースから侵入し、同機能モジュール内の資産を攻撃するので、攻撃の複雑さを示すメトリック AC は程度が容易な L(“Low”: 数値は 0.71)と判定される。
- 認証の回数を示すメトリクス Au は認証 1 回を示し攻撃容易性が中程度な S(“Single”: 数値は 0.56)と判定される。
- 資産は外部サーバとの通信に必要な認証情報で、機密性および完全性の損失は OEM データや個人情報の流出などの重大なインシデントに繋がりがかねない。従って資産の損害の影響は {C, I, A}={ “Complete”, “Complete”, “None”}で、数値にすると {C, I, A}={0.66, 0.66, 0.00}である。
- C, I, A の数値を式(1-1)に代入することで、攻撃容易性=8.0 を得る。
- AV, AC, Au の数値を式(1-2) に代入することで、影響度=9.2 を得る。
- 式(1-3)により、影響度がゼロでないので、f(影響度)=1.176 を得る。
- 式(1-1)～(1-3)を式(1-4)に代入することより、基本値(リスク値)は 8.5 と判定される。

このように、“Where”, “At”, および“Asset”の 3 つの観点で絞り込むことにより、脅威の攻撃経路と守るべき資産、さらに脅威のリスクを一括整理することができる。そのことにより、速やかに分

析の優先順位などの作業方針を決めることができ、時間や人的リソースに応じた効率の良い作業が行える。

### 3.4 その他先行研究

JASO TP15002 および資産コンテナ方式に関して筆者は、2017 年の論文 [13]の他に応用研究として、2018 年の論文 [47]および 2019 年の論文[17]では他ジャンルのシステムへの適用、リスク数値化手法の検討を行っている。以下、次章から述べる本論文の研究に関連する先行研究について説明する。

#### 3.4.1 自動車以外の対象システムの検討

分析対象に関しては、文献[47]で産業制御システム向け機器であるデータロガーを、文献[17]で自動車システムの応用分野であるドローンシステムを、それぞれ対象としたモデルを作成し分析した。

図 11 が文献[47]で用いたデータロガーの分析対象モデルである。各要素について補足する。

システム内の各機能モジュール:

- **Control:** Network Interface からの通信データを取得し、ログデータとして Storage へ転送する。また HMI とシリアル通信を行い、必要な情報を提供する。
- **Network Interface:** Ethernet 通信で Information Control Server や HMI と通信し、データロガーの情報を提供する。また Modbus Serial 通信で各 PLC と通信を行い、ステータスを取得する。
- **Storage:** Control が仲介したログデータを保存する。

エントリーポイント:

- **Serial:** 暗号化されていないシリアル通信。
- **Modbus Serial:** PLC(Programmable Logic Controller)向けで使用される、暗号化されていないシリアル通信。
- **Ethernet:** 暗号化されていない Ethernet 通信。

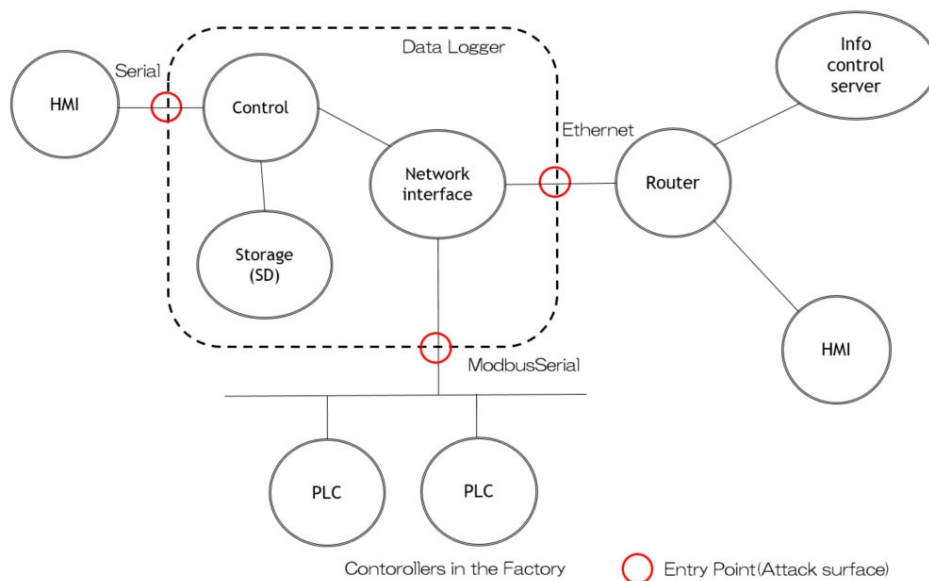


図11: データロガーの分析対象モデル

Figure 11: Target Model for Evaluation: Data Logger

システム外の通信相手や環境:

- **HMI:** データロガーと通信するための PC と通信ソフトウェア.
- **Router:** ルーター/ハブ.
- **Information Control Center:** データロガーのログの収集を行う.
- **PLC:** フィールド機器.

一方文献[17]では, 図 10 同様のコネクテッドカーのモデルを参考に, 図 12 のようなドローン(トイドローン規模の小型のもの)の分析対象モデルも分析した. 各要素について補足する.

システム内の各機能モジュール:

- **CPU (Flight Controller):** ドローンの飛行制御を行う.
- **Camera:** 映像を記録するカメラ.
- **Position Sensor:** 機位センサ.
- **GPS:** GPS 衛星からの電波を受信し, 位置情報を取得する.
- **Storage:** カメラ映像, ドローンのステータスを記憶する.
- **Transceiver (Network Interface):** スマートフォンなどのコントローラと無線通信を行う.
- **Li-Po Battery:** 駆動用バッテリー.

エントリーポイント:

- **Optical wave:** カメラが撮る映像.
- **Electromagnetic wave/Supersonic wave:** 機位センサが受信する電磁波と超音波.

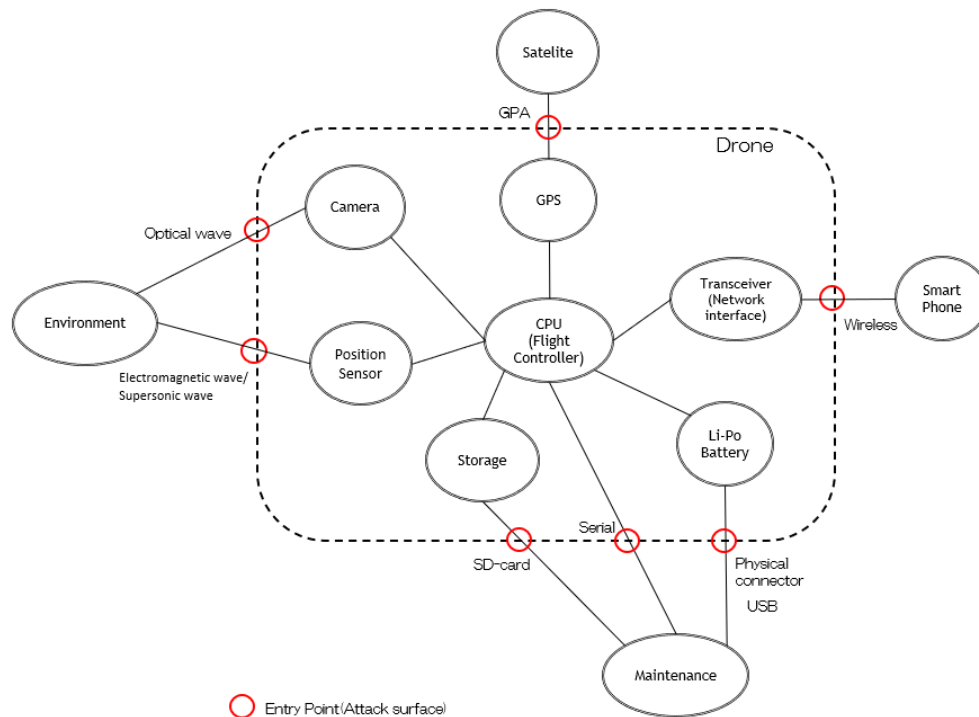


図12: ドローンの分析対象モデル

Figure 12: Target Model for Evaluation: Drone

- **GPS:** GPS 電波を受信する遠距離無線通信インタフェース.
- **Wireless:** スマートフォンなどのコントローラと通信する中～長距離無線通信インタフェース.
- **SD card:** 映像データなどを SD カードに保存し取り外せる物理インタフェース.
- **Serial:** 診断やメンテナンスに用いるシリアル通信インタフェース.
- **Physical connector/USB:** 電池の充電及び電池状態の確認に用いるインタフェース.

システム外の通信相手や環境:

- **Environment:** 撮影対象や機位を測定するための地球環境.
- **Satellite:** GPS 衛星.
- **Smart Phone:** スマートフォンなどの無線コントローラ.
- **Maintenance:** メンテナンス機器やバッテリー充電器.

これら自動車システム以外のサイバーフィジカルシステムにおいても、物理的もしくは論理的に機能モジュールを分けることができ、ネットワーク構成図と守るべき資産を割り当てることができれば、資産コンテナ方式を適用できる分析対象モデルを構築できることを確認した。

### 3.4.2 過去に検討したリスク数値化手法

また文献[17]および[47]では、CVSS 以外の脆弱性評価基準でも資産コンテナ方式を適用できないか、筆者はリスク数値化手法を検討した。

#### 3.4.2.1 RSS-CWSS

文献 [47]は、CWSS を JASO TP15002 フェーズ 3 のリスク数値化手法に適用しようと試みた最初のケースで、2.3.2 項の式(3-1)～(3-5)を用い、CWSS のメトリックを資産コンテナ方式に適用する試みを行っている。この時のリスク数値化手法は RSS-CWSS (Risk Scoring System based on CWSS)としているが、次章で述べる本研究のリスク数値化手法である RSS-CWSS\_CPS(Risk Scoring System for Cyber Physical System based on CWSS)とは使用するメトリックとランクの選定基準が異なる。表 7 が RSS-CWSS で選択した CWSS のメトリックである。文献[47]では CWSS の 16 のうち 6 つを固定値とし、10 個のメトリックの適用を試みた。以下のメトリックについては細かいランク付けが困難で、以下の理由により一律に同じ値を使用している。しかし本研究(第 4 章以降)では、再度メトリックのランク付けルールを見直し、異なる運用を行っている(大体的方針は 2.3.2 項に記載)。

- **Acquired Privilege Layer (AL):** 機能モジュールに資産という粒度で攻撃容易性や資産への損害の影響を見ていたため、レイヤが異なることで影響が異なるなどの違いを判断するのは困難であったため、一律で A(“Application”)とした。
- **Internal Control Effectiveness (IC):** システムの持つ保護機能は想定せず、一律に N(“None”)とした。
- **Finding Confidence (FC):** セキュリティ設計段階では正確な脆弱性情報は持ち得ないため、一律に T(“Proven True”)とした。
- **Level of Interaction (IN):** ユーザーのアクションで状態がセンシティブに変化するようなユースケースを想定していないため、一律に N(“None”)とした。
- **Deployment Scope (SC):** システムの抽象度の関係で波及範囲が予測できないため、中間的な値の R(“Rare”)とした。  
➤ 2.3.2 項でも述べたが、最終的に NA(“Not Applicable”)とすることとした。
- **Prevalence (P):** 攻撃に用いられる脆弱性について起きる頻度や認知度を評価するが、こちらもセキュリティ設計段階では正確な脆弱性情報は持ち得ないため、一律に最もリスクが高く判定される W(“Widespread”)とした。

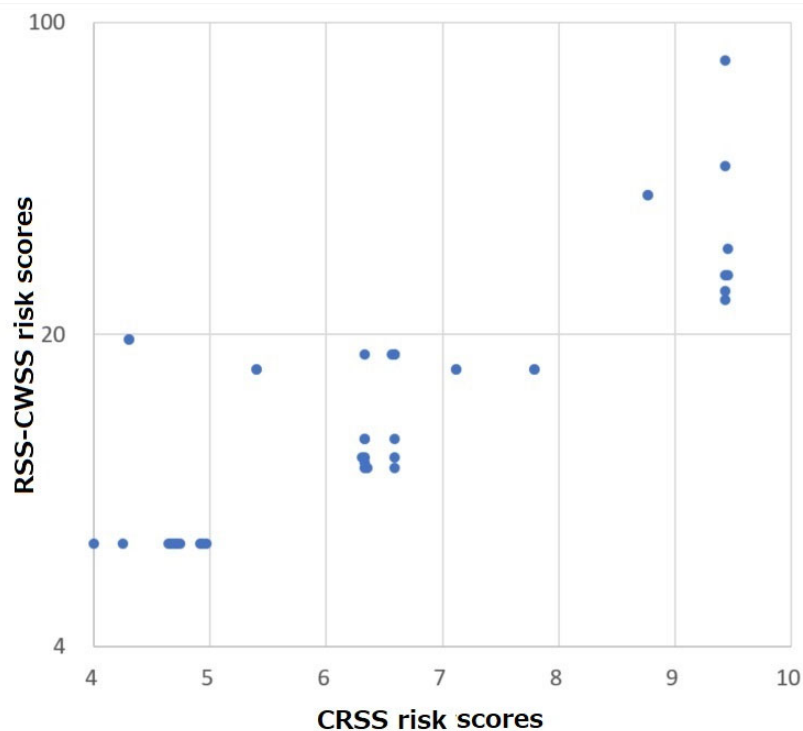


そして、CRSS(前述の CVSS ver.2 を用いた JASO TP15002 のリスク数値化手法)に対し、RSS-CWSS を用いることでリスク値の分布の違いを比較することで、CWSS を用いるメリットを把握し、次の研究につなげる目処をつけた。

表 7: RSS-CWSS で採用した CWSS のメトリック

Table 7: Metrics of CWSS used in RSS-CWSS

Metric	Concept	Used in RSS-CWSS
Technical Impact (TI)	The potential result that can be produced by the weakness, assuming that the weakness can be successfully reached and exploited.	✓
Acquired Privilege (AP)	The type of privileges that are obtained by an attacker who can successfully exploit the weakness.	✓
Acquired Privilege Layer (AL)	The operational layer to which the attacker gains privileges by successfully exploiting the weakness.	Fixed to A(1.0)
Internal Control Effectiveness (IC)	the ability of the control to render the weakness unable to be exploited by an attacker.	Fixed to N(1.0)
Finding Confidence (FC)	the confidence that the reported issue is a weakness that can be utilized by an attacker	Fixed to T(1.0)
Required Privilege (RP)	The type of privileges that an attacker must already have in order to reach the code/functionality that contains the weakness.	✓
Required Privilege Layer (RL)	The operational layer to which the attacker must have privileges in order to attempt to attack the weakness.	✓
Access Vector (AV)	The channel through which an attacker must communicate to reach the code or functionality that contains the weakness.	✓
Authentication Strength (AS)	The strength of the authentication routine that protects the code/functionality that contains the weakness.	✓
Level of Interaction (IN)	the actions that are required by the human victim(s) to enable a successful attack to take place.	Fixed to A(1.0)
Deployment Scope (SC)	Whether the weakness is present in all deployable instances of the software, or if it is limited to a subset of platforms and/or configurations.	Fixed to R(0.5)
Business Impact (BI)	The potential impact to the business or mission if the weakness can be successfully exploited.	✓
Likelihood of Discovery (DI)	The likelihood that an attacker can discover the weakness	✓
Likelihood of Exploit (EX)	the likelihood that, if the weakness is discovered, an attacker with the required privileges/authentication/access would be able to successfully exploit it.	✓
External Control Effectiveness (EC)	the capability of controls or mitigations outside of the software that may render the weakness more difficult for an attacker to reach and/or trigger.	✓
Prevalence (P)	How frequently this type of weakness appears in software.	Fixed to W(1.0)



**図13: RSS-CWSSとCRSSのリスク値分布の比較**  
**Figure 13: Comparison of Risk Value Distribution**  
**between RSS-CWSS and CRSS**

図 13 は、同じ分析対象モデル(データロガー)のリスク分析を行った際のリスク値の分布を CRSS と RSS-CWSS とで比較したグラフで、横軸が CRSS のリスク値の分布、縦軸が同じ脅威を RSS-CWSS で評価した時のリスク値の分布を示す。このグラフにおいて点が個々の脅威であり、以下の状況が確認できる。

- 点の分布が右肩上がりである。これは CRSS でリスクが高いと評価された脅威は、RSS-CWSS でもリスクが高いと評価されていることを示す。
- 複数の点が縦に並んでいる場合、同じ CRSS リスク値を取る複数の脅威があるが、RSS-CWSS では異なる値に区別されつつ評価されていることを示す(ケース 1)。
- 複数の点が横に並んでいる場合は、同じ RSS-CWSS リスク値を取る複数の脅威があるが、CRSS では異なる値に区別されつつ評価されていることを示す(ケース 2)。
- ケース 1 は CRSS リスク値が 6 以上のリスクの高い脅威について起きている。
- ケース 2 は逆に、CRSS リスク値が 4～5 の付近、すなわちリスクの低い脅威について起きている。

以上により, CRSS に対し, RSS-CWSS は重要脅威に対して細かい区別をつけた(リスク値の分布を滑らかな)評価を行うことができ, 資産コンテナ方式に基づく 2 ステップリスク分析(3.2 節)における重要脅威のふるい分けが行いやすくなることを示した.

#### 3.4.2.2 RSS-CVSSv3 と Q-RSMA

また文献[17]においても同様に, リスク数値化手法の検討を行った. こちらのベースは脆弱性評価基準 CVSS Ver.3 および RSMA(Risk Scoring Methodology for Automotive systems)である.

CVSS Ver.3 をベースにした RSS-CVSSv3 の計算式は, 2.3.1 項の式(2-1)~(2-7)と同一なので割愛する.

RSMA(Risk Scoring Methodology for Automotive systems)は, JASO TP15002 で挙げられていたリスク数値化手法である. 攻撃容易性の評価を ISO/IEC 18045 [16]を簡略したもの, 資産が損害を受けることでの影響度の評価を安全(Safety), 個人情報/プライバシー(Personal info./Privacy), および資産/企業の価値(Prop./Corp. Value)の 3 つで評価しており, 配点などの細部は異なるが, ISO/SAE 21434 TARA の Attack-potential based approach と類似している.

Q-RSMA の計算式を式(4-1)~(4-3)に示す. Q-RSMA は RSMA においてマトリクスで数値を決めている箇所を計算式に置き換え, 小数点以下の値を出してリスクを細分化できるようにしたものである.

$$\text{Q-RSMA Score} = \text{Occurrence Possibility} \times \text{Effect Factor} / 100.0 \quad (4-1)$$

$$\text{Occurrence Possibility} = \max [ \{ 34.0 - (\text{Time required} + \text{Expert knowledge} + \text{TOE knowledge} + \text{Opportunity} + \text{Device}) \}, 0.0 ] \quad (4-2)$$

$$\text{Effect Factor} = \text{Vval} \quad (4-3)$$

$$\begin{aligned} \text{where } \text{Vval} = & 0.0 \quad (\text{if } V = \text{None}), \\ & 10.0 \quad (\text{if } V = \text{Small}), \\ & 20.0 \quad (\text{if } V = \text{Medium}), \\ & 30.0 \quad (\text{if } V = \text{Large}), \end{aligned}$$

$$\begin{aligned} \text{and where } V = & \{ \text{None, Small, Medium, Large} \} \quad (\text{if Damage affects Safety}) \\ & \{ \text{None, Small, Large} \} \quad (\text{if Damage affects Personal info. /Privacy}) \\ & \{ \text{None, Small, Medium, Large} \} \quad (\text{if Damage affects Prop. /Corp. Value}) \end{aligned}$$

式(4-1)~式(4-3)は本論文では使用しないので, 各メトリックについてのみ補足する:

- **Time required(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」で 0, 「非現実的」で 10.

- **Expert knowledge(専門知識):** 必要な技術の専門知識。「素人」で 0,「専門家」で 3.
- **TOE knowledge(TOE の知識):** 攻撃対象に限定した知識。「公開情報」で 0,「ディーラー、開発・製造者が入手可能な情報」で 3,「一部の限定されたものだけが入手できる情報」で 7.
- **Opportunity(機会):** 攻撃対象にアクセスする時間及び回数。「アクセス不必要/アクセスが必要だが無制限でアクセス可能」で 0,「アクセスが必要だが回数設定あり」で 4,「アクセスが必要だがアクセス不可能」で 19.
- **Device(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」で 0,「特殊機器(ディーラーが所有する製品など)」で 4,「特別注文品(開発専用の製品など)」で 8.
- **Safety:** 安全への影響. “None”(0.0), “Small”(10.0), “Medium”(20.0), “Large”(30.0).
- **Personal info. /Privacy:** 個人情報/プライバシーへの影響. “None”(0.0), “Small”(10.0), “Large”(30.0).
- **Prop. /Corp. Value:** 財産/企業価値への影響. “None”(0.0), “Small”(10.0), “Medium”(20.0), “Large”(30.0).

RSS-CVSSv3 および Q-RSMA については、文献[17]で CRSS との比較評価を行っている。図 8 のコネクテッドカーでの RSS-CVSSv3 と CRSS との比較では、CVSS ver.3 でメトリック AV(ver.2: Access Vector, ver.3: Attack Vector)のランクが 3 から 4 に増えた際に、有線のエントリーポイント(Local)と無線のエントリーポイント(“Network”, “Adjacent”)との値の格差が狭まったため、本来不利な有線である OBD-II 経由での攻撃のリスクが重要脅威に上がったことが述べられている。一方 Q-RSMA では手法の評価基準が Attack potential によるものであり、資産コンテナ方式の組合せとリスク値との相関が弱い結果となっている。

また両者に共通して、資産の損害による影響度を評価するメトリクスやランク数が多い割に影響度の値が同じものが多く、ばらつきが少ないことが述べられている。この問題に関しては本研究でも継続して考察しており、詳細は第 5 章で述べる。

### 3.5 むすび

以上、本論文の研究の前提で用いている「資産コンテナ方式」というアイデアについて、ケーススタディを交えメリットと課題について述べた。詳細な脅威分析を行う前に資産コンテナ方式で脅威を “Where”, “At” および “Asset” の 3 つの観点で定義することで、攻撃脅威と攻撃対象の組合せを網羅しつつ、観点を絞ることで開発者間の議論により明確な判断基準を定めやすいというメリットがある。

また、資産コンテナ方式だけでリスク値を出せることを利用し、まず資産コンテナ方式を進め、その後他の観点での脅威の肉付けを行うという「2ステップリスク分析」についても述べた。脅威の定義のプロセスを分けることで、先にリスク値を出してスコアの高い重要脅威をふるい分けしておき、重要脅威を優先的に2ステップ目の詳細分析に回すようにするなど、セキュリティ設計におけるリスク分析手順の効率化をはかることが可能である。

また本章では、リスク数値化手法としていくつかのリスク数値化手法を考案し評価したが、そのうちの1つであるRSS-CWSSでは、リスク値が適度に滑らかに分布し、個々の脅威がわずかでも区別できることで、2ステップリスク分析を用いた効率化に有利に働く可能性があるという、本論文の研究に繋がるヒントを得た。

## 第 4 章   ダイレクトアクセス攻撃を検知可能な リスク数値化手法

本章では、本論文の研究における課題、「分析対象のシステムの実情に沿った、適切なリスク分析の実現」を解決するために、自動車システムなどのサイバーフィジカルシステム向けのリスク数値化手法にフォーカスした研究[52][53]について述べる。自動車システムのリスク数値化手法としては前述した CVSS Ver.2 を用いた CRSS(CVSS based Risk Scoring System)が従来手法として用いられていたが、近年 CAN インベーターなどの犯罪に悪用されたダイレクトアクセス攻撃も検知すべく、CWSS を適用した RSS-CWSS\_CPS を提案した。そしてケーススタディを通じて提案手法の優位性やメカニズムについて考察を行った。

### 4.1 背景と研究動機

本章の研究の背景として、近年のサイバーフィジカルシステムが急速に普及し、これに対するサイバー攻撃のリスクを正しく評価し対応を考える必要が出たことがある。重要インフラ、工場、自動車などの制御システムに ICT(Information and Communication Technologies: 情報通信技術)が適用されたものがいわゆるサイバーフィジカルシステムであるが、このシステムでは、ICT 側と物理世界側それぞれが相互に影響を及ぼし合う。したがって ICT 側へのサイバー攻撃の結果が事故などの物理世界での破壊や損傷をもたらすことも、物理世界からの不正なアクセスでシステムの ICT 側の情報などに損害をもたらすことも双方起こりうる。これらはサイバーフィジカルシステムならではの新たなリスクである。例えば、2017 年 12 月に中東の石油化学施設が緊急停止したインシデントは前者であり、マルウェア Triton が施設の安全計装システム(SIS: Safety Instrumented System)へ感染することで緊急停止したというものである。もしさらに攻撃が進んだ場合、故障や爆発、火災などの大惨事が発生する可能性があった[54]。

これらの新たなリスクに対処するために、法整備と標準化が急速に進められてきた。例えば自動車業界では、国連自動車規制調和世界フォーラム作業部会 29 (WP.29)による法整備で UN-R155 [3]および UN-R156[4]が成立し、セキュリティ開発ガイドラインの ISO/SAE 21434 [2]が公開されたことは既に述べた。また産業制御システムの業界においても、ISA99 と IEC/TC65/WG10 の共同開発による ISA/IEC 62443[55]が公開され、現在においてもベンダー、

システムインテグレータ、経営者それぞれに向けたガイドラインと評価基準について整備が進められている。

さらに、自動車システムに対するダイレクトアクセス攻撃がある。これは 2.4 節で触れた CAN インバーダーによる高級自動車盗難事件が典型で、犯罪の有効手段として認知されるようになった。しかし、セキュリティ設計のリスク分析においてこの攻撃を検知し評価できるかという疑問があった。ダイレクトアクセス攻撃はサイバーフィジカルシステム内の有線ネットワークに直接不正な機器を接続するなど物理的にアクセスし、情報窃取や制御乗っ取りなどの攻撃を加えるというものである。一般的にはインターネットなどの広域ネットワーク経由の方がよほどカジュアルに攻撃できるのに、自動車システムではなぜこの攻撃が犯罪の手段として成立するのか、特有の事情があるのではと興味を引かれた。

ダイレクトアクセス攻撃というエントリーポイントについては、前述のように Checkoway らの分析 [51] で言及されている。本文献においては、OBD-II のようなメンテナンスポートは別として、このようなダイレクトアクセス攻撃は現実的ではないというものであった。車載ネットワークに接続できるほど近寄れるのなら、ブレーキのワイヤーを切断するなど、サイバー攻撃に頼らずとも効果的な攻撃ができるのではないかというのがその理由であった。しかし近年では、車載ネットワークの CAN バス経由で内部の ECU を停止に追い込むバスオフ攻撃[49]など、自動車分野を中心にダイレクトアクセス攻撃に関する研究が行われており、2021 年には CAN インバーダーを用いた高級車盗難が立件され現実のものとなった [11]。この事件で用いられたサイバー攻撃の詳細な手順は明らかになっていないが、自動車のバンパー下の配線がイモビライザーなどドアロックの解除やエンジン始動に関わる ECU が属するドメインを構成する CAN バスの一端であったのではと推察される。

以上のように、ICT 側のシステムと ECU などの物理側のフィールド機器が相互接続され連動するサイバーフィジカルシステムにおいては、通常の ICT システムやソフトウェアを対象とした従来の脆弱性評価基準では想定されていない状況があり、セキュリティ設計のリスク分析においてはそのまま評価基準の定義通り適用するだけでは正しい分析が行えていないのではないかと思います。そのためサイバーフィジカルシステムの物理的な境界などの ICT システム単体では無い観点について考え、脆弱性評価基準のメトリックやランクの選定基準をサイバーフィジカルシステム向けに見直すことで解決を図れるのではというのが、本章の研究における動機である。

## 4.2 本章における研究の目的と貢献

本章はそれまでの章の前提を踏まえ、課題「分析対象のシステムの実情に沿った、適切なリスク分析の実現」を解決するための、サイバーフィジカルシステムの実情である特定の領域または

観点に適合したリスク数値化手法を考案することを目的としている。本来はソフトウェア向けに開発された脆弱性評価基準に物理世界側の構造や境界などの特徴を解釈できる観点を加味することで、サイバーフィジカルシステムのリスクを適切に分析することに貢献する。

本章では、ICTシステムではあまり注目されないがサイバーフィジカルシステムでは実際に被害が出ているケースとして、自動車システムへのダイレクトアクセス攻撃に着目し、これを検知できるCWSSベースのリスク数値化手法を考案し、ケーススタディで従来手法であるCRSSとの比較を行った。

## 4.3 ダイレクトアクセス攻撃の評価における従来手法の問題

前章で述べた資産コンテナ方式が適用可能な従来のリスク数値化手法としては、JASO TP15002で示されたCRSSがあるが、この手法では課題「分析対象のシステムの実情に沿った、適切なリスク分析の実現」の観点から不十分ではないか、具体的にはダイレクトアクセス攻撃が見落とされるのではないかという懸念があった。

2.3.1項で説明したCRSSの計算式(1-1)～(1-4)を以下に再掲する:

$$\text{影響度} = 10.41 \times \{1 - (1 - C) \times (1 - I) \times (1 - A)\} \quad (1-1)$$

$$\text{攻撃容易性} = 20 \times AV \times AC \times Au \quad (1-2)$$

$$f(\text{影響度}) = 0(\text{影響度が0の場合}), 1.176(\text{影響度が0以外の場合}) \quad (1-3)$$

$$\text{基本値} = \{(0.6 \times \text{影響度}) + (0.4 \times \text{攻撃容易性}) - 1.5\} \times f(\text{影響度}) \quad (1-4)$$

CRSSの攻撃容易性の計算式は式(1-2)であるが、攻撃容易性を決めるメトリックがAV、AC、およびAuの3つであり、そのうちエントリーポイントの攻撃容易性を評価しているのはAV(Access Vector)である。ダイレクトアクセス攻撃については、AVの値が最も低い“Local”である。攻撃者は攻撃対象の施設に侵入し、接続可能なポートを探す必要があり、状況によっては配線などの工作も必要のため、遠距離無線通信もしくは近接無線通信に比べリスクがかなり低いとみられると解釈される。そのためACやAuで多少の優位性があってもAVが“Local”である不利に差し引かれ、遠距離無線通信など他のエントリーポイントからの攻撃の脅威に比べてリスクは低いとみなされていると考えられる。

しかし2.4節で述べたようなCANインバーダーの事例のように、自動車システムにおけるダイレクトアクセス攻撃はもはや非現実的ではない。工場や重要インフラの現場では、カード認証を必要とする禁止エリアを設定するなど、ダイレクトアクセス攻撃を阻止する仕組みを設置するのは容易であるが、自動車ではリソースも限られそこまでの対策は行われていない。よって車載ネットワ



ークへのダイレクトアクセス攻撃は工場へのそれよりもリスクが高いと考えられる。しかし上記のように、CRSSでは、ダイレクトアクセス攻撃のリスク値は低くなる可能性が高い。

となれば、メトリックAVと別の観点でダイレクトアクセス攻撃を評価できればよいのであるが、それに対応できそうなメトリックがAC(Access Complexity)しかない。これは攻撃の複雑さに関する評価基準であるが、“Low”、“Middle”、および“High”の3ランクしか持っておらず、これらのランク間の数値の差はAVの“Local”の不利を覆すほど大きくはない。また何をもってランクを決定するのか、多くのエントリーポイントや攻撃経路を持つと思われる自動車システムを評価するには非常に曖昧かつ粗いメトリックである。

以上のように、従来手法であるCRSSの問題は、自動車システムのような特定の分野でのサイバーフィジカルシステムに対するダイレクトアクセス攻撃のリスクを正しく評価するにはメトリックが少なく問題もあることであった。資産コンテナ方式の“Where”、“At”、“Asset”の3つの観点での評価に合うのがCRSSのメリットであるが、このメリットを維持した上でサイバーフィジカルシステムの物理的な構造での攻撃容易性の違いを評価できるような、新しいリスク数値化手法が必要であった。

## 4.4 CWSS をベースとした新たな提案手法: RSS-CWSS\_CPS

### 4.4.1 RSS-CWSS\_CPS の計算式

新しいリスク数値化手法のベースに着目したのがCWSSであり、RSS-CWSS\_CPSと命名した。3.4.2項でも述べたように、CWSSをベースとしたリスク数値化手法は[47]でもRSS-CWSSという手法で試みたが、本章の研究で新たに考案したRSS-CWSS\_CPSは、メトリックの選定をより明確化し、サイバーフィジカルシステムの物理的/論理的な構造を解釈する。表8が表7同様CWSSで用いたメトリックの一覧で、式(5-1)～(5-5)が計算式である。

計算式は式(3-1)～(3-5)に使用せず固定値とするメトリックの値を代入した計算式である。また、リスク値のスケールをCVSSに合わせ、式(5-1)で最大値100から10に落としている。

$$\text{リスク値 } R_w = S_{\text{Base}} \times S_{\text{Surface}} \times S_{\text{Env}} / 10.0 \quad (5-1)$$

$$\text{基本値: } S_{\text{Base}} = 4 \{f(\text{TI}) \cdot (10\text{TI} + 15) \cdot \text{IC}\} \quad (5-2)$$

$$\text{エントリーポイントの評価: } S_{\text{Surface}} = \{20(\text{AV} + 2) + 5\text{AS} + 35\} / 100.0 \quad (5-3)$$

$$\text{環境の評価: } S_{\text{Env}} = \{f(\text{BI}) \cdot (10\text{BI} + 3\text{DI} + 4\text{EX} + 3) \cdot \text{EC}\} / 20.0 \quad (5-4)$$

$$\text{影響度の補正式: } f(x) = 0(\text{if } x=0), 1(\text{otherwise}) \quad (5-5)$$

表 8: RSS-CWSS\_CPS で採用した CWSS のメトリック

Table 8: Metrics of CWSS used in RSS-CWSS\_CPS

Metric	Concept	Used in RSS-CWSS_CPS
Technical Impact (TI)	The potential result that can be produced by the weakness, assuming that the weakness can be successfully reached and exploited.	✓
Acquired Privilege (AP)	The type of privileges that are obtained by an attacker who can successfully exploit the weakness.	Not used Fixed to NA(1.0)
Acquired Privilege Layer (AL)	The operational layer to which the attacker gains privileges by successfully exploiting the weakness.	Not used Fixed to NA(1.0)
Internal Control Effectiveness (IC)	The ability of the control to render the weakness unable to be exploited by an attacker.	✓
Finding Confidence (FC)	The confidence that the reported issue is a weakness that can be utilized by an attacker	Not used Fixed to NA(1.0)
Required Privilege (RP)	The type of privileges that an attacker must already have in order to reach the code/functionality that contains the weakness.	Not used Fixed to NA(1.0)
Required Privilege Layer (RL)	The operational layer to which the attacker must have privileges in order to attempt to attack the weakness.	Not used Fixed to NA(1.0)
Access Vector (AV)	The channel through which an attacker must communicate to reach the code or functionality that contains the weakness.	✓
Authentication Strength (AS)	The strength of the authentication routine that protects the code/functionality that contains the weakness.	✓
Level of Interaction (IN)	The actions that are required by the human victim(s) to enable a successful attack to take place.	Not used Fixed to A(1.0)
Deployment Scope (SC)	Whether the weakness is present in all deployable instances of the software, or if it is limited to a subset of platforms and/or configurations.	Not used Fixed to NA(1.0)
Business Impact (BI)	The potential impact to the business or mission if the weakness can be successfully exploited.	✓
Likelihood of Discovery (DI)	The likelihood that an attacker can discover the weakness	✓
Likelihood of Exploit (EX)	The likelihood that, if the weakness is discovered, an attacker with the required privileges/authentication/access would be able to successfully exploit it.	✓
External Control Effectiveness (EC)	The capability of controls or mitigations outside of the software that may render the weakness more difficult for an attacker to reach and/or trigger.	✓
Prevalence (P)	How frequently this type of weakness appears in software.	Not used Fixed to NA(1.0)

#### 4.4.2 RSS-CWSS\_CPS におけるメトリックの定義

RSS-CWSS\_CPS は 3.4.2 項で述べた RSS-CWSS の延長ではなく、CWSS のメトリックを新たに解釈し直したリスク数値化手法である。CWSS の各メトリックについては 2.3.2 項で述べたが、ソフトウェア脆弱性評価基準をそのままシステムのリスク評価にあてはめるのは困難であり、適用外のメトリックを除外し、一部のメトリックにおいては解釈をサイバーフィジカルシステムに合わせて変更するなどの改良が必要であった。リスク数値化手法 RSS-CWSS\_CPS を考案するにあたり、元の CWSS から変えた部分がある。以下、それらについて補足する:

##### **CWSS からそのまま適用するメトリック:**

- Technical Impact (TI), Business Impact (BI), Access Vector (AV), および Authentication Strength(AS)は、CWSS での定義や評価基準をそのまま継承させて RSS-CWSS\_CPS で使用することとした。
- Likelihood of Discovery (DI)も評価基準をそのまま継承するが、RSS-CWSS\_CPS 適用において定義を「攻撃に用いる脆弱性の見つけやすさを評価する」から「攻撃の際にターゲットとして見つけやすい資産に対する脅威であるかを評価する」と読み替えることとした。
  - 例えばエントリーポイントから侵入した機能モジュールが持つ資産は、その機能モジュールに隣接する他の機能モジュールの資産よりは見つけやすく狙いやすいため、前者が攻撃されるリスクを H(“High”), 後者を M(“Medium”)と評価するなど、ランクに差をつける。

##### **サイバーフィジカルシステムの解釈のために重要視し、解釈の変更を行ったメトリック:**

- Internal Control Effectiveness (IC)は、アーキテクチャ、設計、または実装を通じてソフトウェアに明示的に組み込まれた制御、保護メカニズム、または緩和策について評価する。  
RSS-CWSS\_CPS ではこれをシステム内部におけるネットワーク構造にも拡張させ、「攻撃を困難にする物理的または論理的構造」とした。
  - 例えば認証の有無に関わらず、経由する機能モジュールの数に応じてランクを 1 段階下げ、侵入後に経由する機能モジュールが多いほど攻撃容易性が下がるようにする。
- External Control Effectiveness (EC) は、攻撃者が脆弱性に到達し、使用するのをより困難にすることが可能な、ソフトウェアの外部での制御または緩和の機能について評価する。  
RSS-CWSS\_CPS ではこれをシステムの物理的境界として拡張した解釈を行い、「アクセスを困難にするエントリーポイント」とした。
  - 例えば、アクセスするために何らかの追加の認証が必要だったり、筐体を剥がしたりコネクタを作るなどの物理的な工作を必要とするなど、面倒な作業が必要なエントリーポイントに対してそうでないものよりランクを高くする。

- Likelihood of Exploit (EX)は、攻撃の可能性がどれだけあるかを評価する。  
RSS-CWSS\_CPS ではエントリーポイントの AV の評価を補足する目的で、エントリーポイントの評価に適用する。
  - 近接無線通信だと、通信距離が限定されるため、システムの運用により通信が繋がる時間的なウィンドウが異なるため、そうした違いを解釈するために使用する。
- IC, EC, EX の 3 つは、それぞれ攻撃の複雑さを解釈するメトリックであり、CVSS Ver.2 の Access Complexity (AC), CVSS Ver.3 および Ver.3.1 の Attack Complexity (AC)に相当する。

#### 適用外としたメトリック:

- 権限に関するメトリック, Acquired Privilege (AP), Acquired Privilege Layer (AL), Required Privilege (RP), および Required Privilege Layer (RL)は NA(“Not Applicable”)とした。
  - ソフトウェアの脆弱性を評価する際には意味のあるメトリックであるが、システムレベルの抽象度で設定するには適していないメトリックである。
- Finding Confidence (FC)は NA(“Not Applicable”)とした。
  - 脆弱性に関するレポートの信憑性を評価するメトリックであるが、システムの評価に使用するには適していないメトリックである。
- Level of Interaction (IN)は NA(“Not Applicable”)とした。
  - 被害者となる自動車ユーザーが起こす何らかのアクションの有無や程度を評価するものであるが、システムレベルの抽象度によっては具体的なアクターを想定するのが困難である。
  - EX でも同様のことを考慮しているので、そちらで評価を行うこととした。
- Deployment Scope (SC)は NA(“Not Applicable”)とした。
  - 脆弱性がシステムに含まれるコンポーネントに波及する範囲を評価するメトリックであるが、システムの評価に使用するには適していないメトリックである。
- Prevalence (P)は NA(“Not Applicable”)とした。
  - 脆弱性について起きる頻度や認知度を評価するメトリックであるが、未知の脅威の評価に使用するには適していないメトリックである。

#### その他留意事項:

- 式(5-1)～(5-5)で使用する各メトリックに与えるランクは、デフォルト値 D(“Default”), 不明 UK(“Unknown”), およびそれ以外のカスタム判定として任意の値を与える Q(“Quantified”)は使用しない。
  - 特に Q を使うには根拠のある明確な基準を考える必要があり、今後の課題とする。

#### 4.4.3 RSS-CWSS\_CPS によるダイレクトアクセス攻撃の評価

RSS-CWSS\_CPS を資産コンテナ方式と組み合わせてハードウェアシステムのリスク分析に使用する場合に、各メトリックを“Where(エントリーポイント)”, “At(攻撃目標の機能モジュール)”, および“Asset(機能や情報などの資産)”のどの観点で評価すればいいかを図示したものを図 14 に示す. このように資産コンテナ方式の各観点においてランク値を定めた.

また, RSS-CWSS\_CPS においてダイレクトアクセス攻撃の評価に用いられる, 攻撃容易性を決める重要な 5 つのメトリックを表 9 に示す. ダイレクトアクセス攻撃は各メトリックの観点で以下のように評価される:

- **Internal Control Effectiveness (IC):** “At”に該当する機能モジュールが, エントリーポイントを持たないなどの理由でいくつかの機能モジュールを経由しないと到達できないものでも直接アクセスできるので, IC の観点でのダイレクトアクセス攻撃のリスクはより高くなる.
- **Access Vector (AV):** 無線通信と比べ攻撃者がより近くに接続しに行かなければならないので, AV の観点でのダイレクトアクセス攻撃のリスクはより低くなる.
- **Authentication Strength (AS):** 認証が不要とみなせるので, AS の観点でのダイレクトアクセス攻撃のリスクはより高くなる.

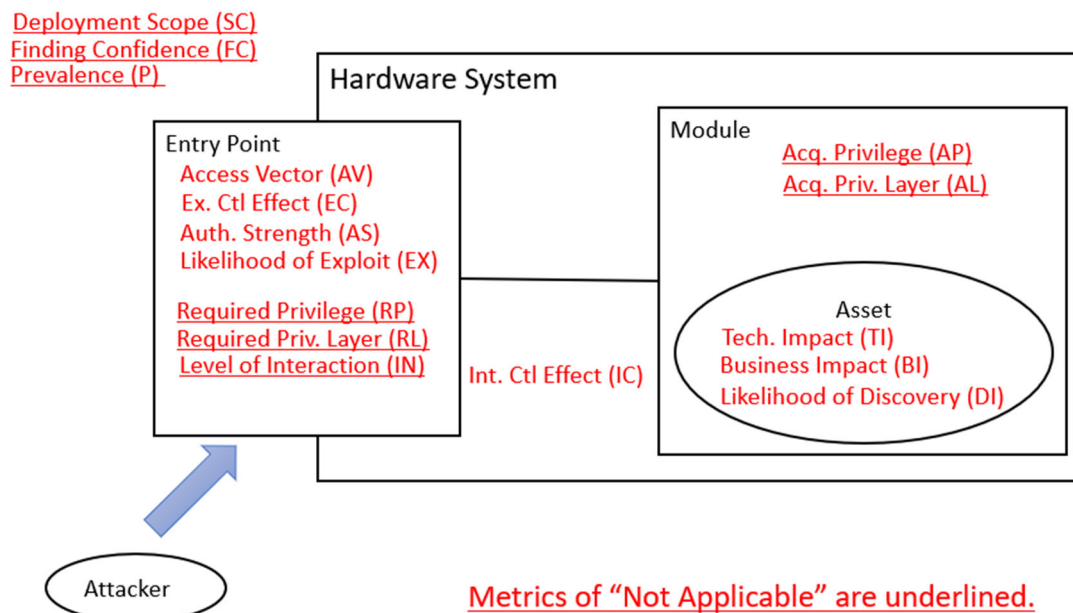


図14: 資産コンテナ方式におけるRSS-CWSS\_CPS各メトリックの評価箇所

Figure 14: Evaluation Points for Each RSS-CWSS\_CPS Metric  
of The Asset Container Method

表 9 RSS-CWSS\_CPS でダイレクトアクセスの評価に用いられる CWSS メトリック

Table 9 CWSS Metrics Used in RSS-CWSS\_CPS for Direct Access Attacks

Metric	Expected Results in RSS-CWSS_CPS
Internal Control Effectiveness (IC)	It may be <b>Higher</b> risk for some modules because the attacker can directly attack them even if they can only be reached via other multiple modules.
Access Vector (AV)	It may be <b>Lower</b> risk than that via other wireless communication because the attacker needs to get closer to connect.
Authentication Strength (AS)	It may be <b>Higher</b> risk because the attacker can gain access without authentication.
Likelihood of Exploit (EX)	It may be <b>High</b> risk as well as via long-distance wireless communication because the attacker can gain access at any time.
External Control Effectiveness (EC)	It may be <b>High</b> risk as well as via long-distance wireless communication because there are no restrictions on the connection to in-vehicle network

- **Likelihood of Exploit (EX):** CAN インベーターにおけるバンパー裏の配線にアクセスするなど短時間で行える攻撃であれば、攻撃を行う機会は十分確保できる。EX の観点でのダイレクトアクセス攻撃のリスクは長距離無線通信同様に高くなる。
- **External Control Effectiveness (EC):** CAN インベーターにおけるバンパー裏の配線から重要な機能モジュールへアクセスできるのであれば、通信線を探して工作する程度の手間は僅かで、攻撃が露見するリスクが減り問題とならなくなるので、EC の観点でのダイレクトアクセス攻撃のリスクは長距離無線通信同様に高くなる。

特に IC と EC については本来、ソフトウェアの脆弱性を軽減するための内部および外部のメカニズムであったが、これらをサイバーフィジカルシステムのハードウェア構造と物理境界として解釈することで、システムの解釈に柔軟性を与えている。

#### 4.4.4 RSS-CWSS\_CPS のメリット

最後に、CVSS に代わり CWSS をリスク数値化手法に用いた、RSS-CWSS\_CPS の 2 つのメリットについて述べる:

- 資産が損害を受けることでの影響度を評価するにおいて、CWSS は CVSS よりもきめ細かいランクの組み合わせを選べる (表 2 の C, I, A それぞれのランク数, および表 3 の TI, BI それぞれのランク数を参照). TI と BI にはそれぞれ 5 つのランクがあるが, C, I, および A はそれぞれ 3 つのランクしかない. また CWSS では TI と BI は組み合わせられるが, CVSS では機能に関する資産は I と A, 情報に関する資産は C と I の組み合わせし

か用いない。そのため RSS-CWSS\_CPS で選べる影響度の組み合わせは  $5 \times 5 = 25$  通りあるが、CRSS では  $3 \times 3 = 9$  通りのみである。

- B) 攻撃容易性に関するメトリックに関しても、CWSS は CVSS より資産コンテナ方式に適するメトリックを多く持ち、ランク数も多い。そのためこちらも CWSS は CVSS よりもきめ細かいランクの組み合わせを選べる(こちらも表 2 の AC のランク数、および表 3 の IC, EC, EX それぞれのランク数を参照)。実際、CWSS の IC, EC, および EX にはそれぞれランク数が 6, 6, および 4 であり、攻撃の複雑さを判定するメトリックのランクの組み合わせは  $6 \times 6 \times 4 = 144$  であるが、CVSS だと AC のみで 3 通りのランクしか選べない。

## 4.5 ケーススタディおよび手法の効果の分析

本節では、考案した RSS-CWSS\_CPS について自動車システムのリスク分析のケーススタディを行う。ここで一旦、本論文の研究目的および本節で実施することをまとめる。

- 本論文の研究目的は、課題「分析対象のシステムの実情に沿った適切な分析」について、サイバーフィジカルシステムのひとつである自動車システムのダイレクトアクセス攻撃の検知という問題を解決することで、課題解決のための考察を行う。
- 前節では、自動車システムへのダイレクトアクセス攻撃が従来のリスク分析では検知しづらいという問題を解決するために、RSS-CWSS\_CPS を考案した。本節では自動車システムのケーススタディを通じて実際に対するリスク評価を行い、従来手法である CRSS とのリスク値の違いを比較する。そして「分析対象のシステムの実情に沿った適切な分析」という目的での RSS-CWSS\_CPS の有用性を述べる。

4.5.1 項では、自動車システムを分析対象モデルとして定義する。4.5.2 および 4.5.3 項では、RSS-CWSS\_CPS のメトリックとランクのマッピング結果を示す。4.5.4 項では、ダイレクトアクセス攻撃の検出にどのメトリックが有効であるか考察する。4.5.5 項ではケーススタディで分析した 2 つの脅威を例に取り、RSS-CWSS\_CPS と CRSS の分析結果の違いを確認しつつ、各手法のメトリックがどのようにダイレクトアクセス攻撃の評価に寄与した違いを見せたか具体的に分析する。4.5.6 項では、各手法のエントリーポイントごとに、関連する脅威のリスク値が取る傾向を比較する。最後に 4.5.7 項でケーススタディにおける結論を述べる。

### 4.5.1 自動車システムの分析対象モデル

自動車システムの分析対象モデルは Liu らの研究[56]で想定された CGW(Central Gateway)を含むネットワークストラクチャを基に、Ethernet ネットワークを追加して定義した。図 15 が分析対象

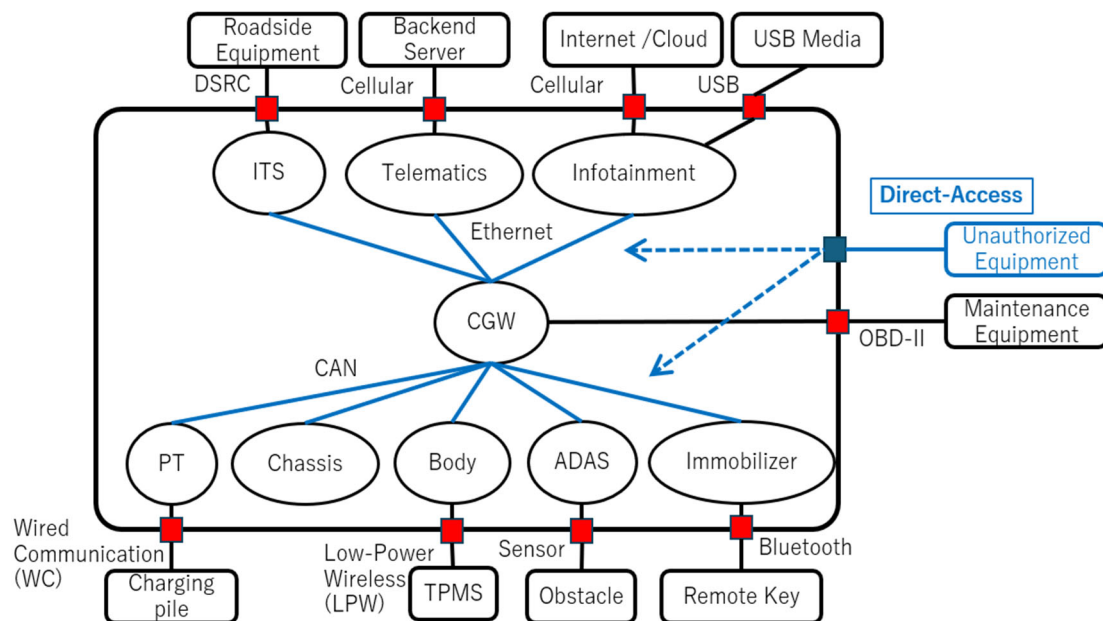


図15: 分析対象システムとしての自動車システムのシステム構成  
**Figure 15: System Configuration of Automotive System as a Model to be analyzed**

モデルのシステム構成図である。これは 3.3 節で述べた文献[13]の自動車システムモデルの発展形で、一部機能モジュールとエントリーポイントを追加削減したものになっている。各要素について以下に補足する:

システム内の各機能モジュール:

- **PT(Power-Train):** エンジンなど、駆動系 ECU をまとめた機能モジュール。
- **Chassis:** ブレーキなど、シャーシ系 ECU をまとめた機能モジュール。
- **Body:** ドアロックなど、ボディ系 ECU をまとめた機能モジュール。
- **ADAS:** 運転補助機能など、ADAS (Advanced driver-assistance systems: 先進運転支援システム) 系 ECU をまとめた機能モジュール。
- **Immobilizer:** リモートキーによるエンジン始動を行う機能モジュール。
- **ITS:** ITS など、V2X(Vehicle to X)通信を行う ECU をまとめた機能モジュール。
- **Telematics:** バックアップサーバとの通信を行う、テレマティクス系 ECU をまとめた機能モジュール。
- **Infotainment:** ナビゲーションシステムや Web ブラウザ、エンターテインメント系アプリの提供など、インフォテインメント系 ECU をまとめた機能モジュール。
- **CGW(Central Gateway):** CAN バスと Ethernet ネットワークを接続しデータを変換、CAN バス間での通信タイミングを調整などを行う機能モジュール。



#### エントリーポイント:

- **Low-Power Wireless (LPW):** TPMS と通信を行う近接無線通信インタフェース. 文献 [52][53]では, 文献[13]同様の考えで LPW のインタフェースは PT 機能モジュールに設けられていたが, 本論文では現在の運用に合わせ TPMS を Body 機能モジュールに移動させ, 分析し直したリスク値を用いた再評価を行っている.
- **Wired Communication (WC):** Charging Pile との電源供給兼有線通信インタフェース.
- **Sensor:** 障害物レーダーやセンサ.
- **Bluetooth:** Remote Key と通信を行う近接無線通信インタフェース.
- **DSRC:** Roadside Unit(RSU)と通信を行う近接無線通信インタフェース.
- **Cellular:** 携帯電話通信などの遠距離無線通信を用いる通信インタフェース.
- **USB:** USB メモリなどを接続するための物理インタフェース.
- **OBD-II:** OBD-II などを使用した, CGW に対して車内にあるコネクタを介してダイアグメツセージを受ける物理インタフェース.
- **Direct-Access:** 通信ポートやコネクタなどへの, ダイレクトアクセス攻撃のエントリーポイント. 図 13 では点線矢印で表現しているが, 任意の機能モジュールに直接アクセスできる通信インタフェースとみなす.

#### システム外の通信相手や環境:

- **TPMS:** Tire Pressure Monitoring System, タイヤ空気圧センサ.
- **Charging Pile:** 充電ステーションの接続ケーブル.
- **Obstacle:** 障害物.
- **Remote Key:** リモートキー.
- **Roadside Equipment:** 路側機もしくは他の自動車.
- **Backend Server:** ファームウェアやアプリをダウンロードしたり, データを保存したりするバックエンドサーバー.
- **Internet/Cloud:** アプリのダウンロードや Web ブラウジングに利用する, インターネットもしくはクラウドサービス.
- **USB Media:** USB をインタフェースとするメモリーデバイスなど.
- **Maintenance Equipment:** メンテナンス用診断機器.
- **Unauthorized Equipment:** ダイレクトアクセス攻撃に使用する不正な機器.

各資産について表 10 にまとめる. 以下, 詳細を補足する:

- **Control Function:** 自動車に対し, 各機能モジュールに応じた制御を行う機能.

表 10: 機能モジュールおよび資産のリスト

Table 10: The List of Function Modules and Their Assets

#	“At”	“Asset”	#	“At”	“Asset”
1	PT	Control Function	7	ITS	Ex-Comm. Function
		Charging Function			Auth. Function
		In-Comm. Function			Auth. Information
2	Chassis	Control Function			In-Comm. Function
		In-Comm. Function			Personal Information
3	Body	Control Function	8	Telematics	Ex-Comm. Function
		In-Comm. Function			Auth. Function
		Ex-Comm. Function			Auth. Information
		Sensor Information			Remote Service App.
4	Immobilizer	Auth. Function			In-Comm. Function
		Auth. Information			Personal Information
		Ex-Comm. Function			Location Info / Status
		In-Comm. Function			
5	ADAS	Control Function	9	Infotainment	Ex-Comm. Function
		In-Comm. Function			Auth. Function
		Sensor Function			Auth. Information
		Sensor Information			In-Comm. Function
6	CGW	Data Processing			Navi App.
		Diagnostic Function			Entertainment App.
					Personal Information

- **Charging Function:** 充電機能.
- **Ex-Comm. Function:** エントリーポイントを使った, システム外部との通信機能.
- **In-Comm. Function:** 車内ネットワークを使った, システム内部の機能モジュールとの通信機能.
- **Sensor Function:** センサ機能およびセンサを制御しデータを受け取る機能.
- **Sensor Information:** センサからの情報. Body 機能モジュールのものは TPMS からのデータ, ADAS 機能モジュールのものは Sensor からのデータ.
- **Auth. Function:** 無線通信の確立や利用者の機能モジュールへのアクセスの際に行う認証機能.
- **Auth. Information:** 各認証機能に必要な, パスワードなどの認証情報.
- **Data Processing Function:** CGW のデータ処理機能.
- **Diagnostics Function:** 診断機能.
- **Personal Information:** 個人情報, 自動車システム外の認証情報なども含む.
- **Remote Service App.:** Telematics が提供する遠隔サービスのアプリケーション.
- **Location Info. / Status:** 位置情報, 車両ステータスなど.
- **Navi App.:** ナビゲーションアプリなど, Infotainment が提供する運転サポートサービスのアプリケーション.

- **Entertainment App.:** ナビゲーションアプリなど, Infotainment が提供する娯楽サービスのアプリケーション.

## 4.5.2 リスク数値化手法

4.4 節で定義したリスク数値化手法 RSS-CWSS\_CPS を用いて, 脅威のリスクを評価する. 計算式は式(5-1)～(5-5)(再掲)を使用した:

$$\text{リスク値 } R_w = S_{\text{Base}} \times S_{\text{Surface}} \times S_{\text{Env}} / 10.0 \quad (5-1)$$

$$\text{基本値: } S_{\text{Base}} = 4 \{ f(\text{TI}) \cdot (10\text{TI} + 15) \cdot \text{IC} \} \quad (5-2)$$

$$\text{エントリーポイントの評価: } S_{\text{Surface}} = \{ 20(\text{AV} + 2) + 5\text{AS} + 35 \} / 100.0 \quad (5-3)$$

$$\text{環境の評価: } S_{\text{Env}} = \{ f(\text{BI}) \cdot (10\text{BI} + 3\text{DI} + 4\text{EX} + 3) \cdot \text{EC} \} / 20.0 \quad (5-4)$$

$$\text{影響度の補正式: } f(x) = 0(\text{if } x=0), 1(\text{otherwise}) \quad (5-5)$$

## 4.5.3 各メトリックのマッピング

脅威のリスク値を算出するために, 資産コンテナ方式に基づく “Where”, “At”, および “Asset” の組み合わせに応じて, CWSS の各メトリックにランクを割り振った. 表 11～14 がマッピング結果である. 以下補足する:

**表 11 の TI, BI, DI のランク付けに関して:**

- 自動運転は想定しない. ADAS は運転サポートのみで, 最終的には操縦者が判断する.
  - 操縦機能に関わる PT と Chassis, およびエンジン始動に関わる Immobilizer の 3 つの機能モジュールが持つ資産の TI と BI は高めに判定している.
- 各機能モジュールは基本的に独立して動くものと考えており, 連携は弱め.
  - 各機能モジュールの In-Comm. Function や CGW が持つ資産の TI と BI は相対的に低めに判定している.
- 個人情報の情報漏洩は他システムでの使い回しなどで波及範囲が大きい可能性があり, また企業の信用に関わる重要な資産である.
  - Personal Information の BI は C (“Critical”) と判定している.
- 攻撃に用いる脆弱性の見つけやすさは, エントリーポイントに直接関係する資産>エントリーポイントを持つ機能モジュールが持つ資産>エントリーポイントを持たない機能モジュールが持つ資産, の順とみなす.
  - DI の判定はこの順で H>M>L と判定する.

表 11: 資産に対する TI, BI, および DI のランク

Table 11: Ranks of TI, BI, and DI for Each Asset

#	“At”	“Asset”	TI	BI	DI	#	“At”	“Asset”	TI	BI	DI
1	PT	Control Function	C	C	L	7	ITS	Ex-Comm. Function	H	H	H
		Charging Function	C	C	L			Auth. Function	M	H	H
		In-Comm. Function	H	H	L			Auth. Information	H	H	H
2	Chassis	Control Function	C	C	L			In-Comm. Function	M	L	M
		In-Comm. Function	M	L	L			Personal Information	L	C	H
3	Body	Control Function	H	H	M	8	Telematics	Ex-Comm. Function	H	H	H
		In-Comm. Function	H	H	M			Auth. Function	M	M	H
		Ex-Comm. Function	C	C	H			Auth. Information	H	H	H
		Sensor Information	H	M	H			Remote Service App.	M	M	H
4	Immobilizer	Auth. Function	C	C	H			In-Comm. Function	M	L	M
		Auth. Information	H	H	H			Personal Information	L	C	H
		Ex-Comm. Function	C	C	H			Location Info / Status	L	M	M
		In-Comm. Function	C	C	M						
5	ADAS	Control Function	H	L	M	9	Infotainment	Ex-Comm. Function	M	M	H
		In-Comm. Function	M	L	M			Auth. Function	L	M	H
		Sensor Function	H	M	H			Auth. Information	M	H	H
		Sensor Information	H	M	H			In-Comm. Function	M	L	M
6	CGW	Data Processing Function	H	H	H			Navi App.	L	M	H
		Diagnostic Function	M	L	M			Entertainment App.	L	L	H
								Personal Information	L	C	H

- ダイレクトアクセス攻撃を想定する場合、エントリーポイントを持たない機能モジュールが持つ資産も直接攻撃できるので、MとLの差が縮まることを考慮すべきかもしれない。ただ、ダイレクトアクセス攻撃は、通常のエントリーポイント経由の攻撃と比べてノウハウが少ない可能性も考え、本研究ではこの序列を変えないことにした。

表 12 および表 13 の, IC, AV, AS, EX のランク付けに関して:

- IC のランクは、経由する機能モジュールの数に応じて決定する。
  - 本来の IC のランクの定義は考慮せず、「エントリーポイントから侵入した機能モジュール」>「CGW」>「CGW を挟んで反対側にある機能モジュール」、の順で N>L>I と判定する。
  - エントリーポイントが OBD-II の場合は、「CGW」が N、「CGW 以外の隣接する機能モジュール」が L。
  - エントリーポイントがダイレクトアクセスの場合は、「ネットワークプロトコル(Ethernet, CAN Bus)が同じ機能モジュール」が N、「プロトコルが異なる機能モジュール」は CGW 経由でのアクセスとみなして L とする。
- AV のランクについては、USB や WC が P に対し、ダイレクトアクセスは OBD-II と同等の L と判定している。これは Ethernet や CAN Bus のネットワークに任意の不正なパケットやメッセージを送り込めるなど、USB や WC などのエントリーポイントより攻撃の自由度が高いことを考慮している。
- AS は M(“Moderate”)か N(“None”)かの 2 択で判定している。

表 12: 攻撃経路に対する IC, AV, AS, および EX のランク(1 of 2)

Table 12: Ranks of IC, AV, AS, and EX for Each Attack Route (1 of 2)

#	“Where”	“At”	IC	AV	AS	EX	#	“Where”	“At”	IC	AV	AS	EX
1	Cellular of Telematics	PT	I	I	M	H	28	LPW	PT	I	A	N	L
2		Chassis	I	I	M	H	29		Chassis	I	A	N	L
3		Body	I	I	M	H	30		Body	N	A	N	L
4		Immobilizer	I	I	M	H	31		Immobilizer	I	A	N	L
5		ADAS	I	I	M	H	32		ADAS	I	A	N	L
6		CGW	L	I	M	H	33		CGW	L	A	N	L
7		ITS	I	I	M	H	34		ITS	I	A	N	L
8		Telematics	N	I	M	H	35		Telematics	I	A	N	L
9		Infotainment	I	I	M	H	36		Infotainment	I	A	N	L
10	Cellular of Infotainment	PT	I	I	M	H	37	Bluetooth	PT	I	A	M	L
11		Chassis	I	I	M	H	38		Chassis	I	A	M	L
12		Body	I	I	M	H	39		Body	I	A	M	L
13		Immobilizer	I	I	M	H	40		Immobilizer	N	A	M	L
14		ADAS	I	I	M	H	41		ADAS	I	A	M	L
15		CGW	L	I	M	H	42		CGW	L	A	M	L
16		ITS	I	I	M	H	43		ITS	I	A	M	L
17		Telematics	I	I	M	H	44		Telematics	I	A	M	L
18		Infotainment	N	I	M	H	45		Infotainment	I	A	M	L
19	DSRC	PT	I	A	M	M	46	USB	PT	I	P	N	M
20		Chassis	I	A	M	M	47		Chassis	I	P	N	M
21		Body	I	A	M	M	48		Body	I	P	N	M
22		Immobilizer	I	A	M	M	49		Immobilizer	I	P	N	M
23		ADAS	I	A	M	M	50		ADAS	I	P	N	M
24		CGW	L	A	M	M	51		CGW	L	P	N	M
25		ITS	N	A	M	M	52		ITS	I	P	N	M
26		Telematics	I	A	M	M	53		Telematics	I	P	N	M
27		Infotainment	I	A	M	M	54		Infotainment	N	P	N	M

- EX はダイレクトアクセス攻撃においては、2.4 節で述べた CAN インバーダーの事例のように、自動車の配線などの物理的な脆弱性を利用して素早く攻撃することができると仮定し、H(“High”)としている。

表 14 の、EC のランク付けに関して:

- EC はダイレクトアクセスのみ N(“None”)とし、他は L(“Limited”)とした。多くのエントリーポイントは認証やフィルタリングなどの既存の対策があることを想定し、ダイレクトアクセス以外のエントリーポイントは攻撃容易性を下げるように判定している。
- OBD-II についてはダイアグ機能対応など CGW が行うため、ここ経由の CAN メッセージには何らかのフィルタリングがなされていると仮定し、L としている。

表 13: 攻撃経路に対する IC, AV, AS, および EX のランク(2 of 2)

Table 13: Ranks of IC, AV, AS, and EX for Each Attack Route (2 of 2)

#	“Where”	“At”	IC	AV	AS	EX	#	“Where”	“At”	IC	AV	AS	EX
55	OBD-II	PT	L	L	N	H	82	WC	PT	N	P	N	L
56		Chassis	L	L	N	H	83		Chassis	I	P	N	L
57		Body	L	L	N	H	84		Body	I	P	N	L
58		Immobilizer	L	L	N	H	85		Immobilizer	I	P	N	L
59		ADAS	L	L	N	H	86		ADAS	I	P	N	L
60		CGW	N	L	N	H	87		CGW	L	P	N	L
61		ITS	L	L	N	H	88		ITS	I	P	N	L
62		Telematics	L	L	N	H	89		Telematics	I	P	N	L
63		Infotainment	L	L	N	H	90		Infotainment	I	P	N	L
64	Direct-access via Ethernet	PT	L	L	N	H	91	Sensor	PT	I	A	N	M
65		Chassis	L	L	N	H	92		Chassis	I	A	N	M
66		Body	L	L	N	H	93		Body	I	A	N	M
67		Immobilizer	L	L	N	H	94		Immobilizer	I	A	N	M
68		ADAS	L	L	N	H	95		ADAS	N	A	N	M
69		CGW	N	L	N	H	96		CGW	L	A	N	M
70		ITS	N	L	N	H	97		ITS	I	A	N	M
71		Telematics	N	L	N	H	98		Telematics	I	A	N	M
72		Infotainment	N	L	N	H	99		Infotainment	I	A	N	M
73	Direct-access via CAN Bus	PT	N	L	N	H							
74		Chassis	N	L	N	H							
75		Body	N	L	N	H							
76		Immobilizer	N	L	N	H							
77		ADAS	N	L	N	H							
78		CGW	N	L	N	H							
79		ITS	L	L	N	H							
80		Telematics	L	L	N	H							
81		Infotainment	L	L	N	H							

表 14: エントリーポイントに対する EC のランク

Table 14: Ranks of EC for Each Entry Point

#	“Where”	EC
1	Cellular of Telematics	L
2	Cellular of Infotainment	L
3	DSRC	L
4	LPW	L
5	Bluetooth	L
6	USB	L
7	OBD-II	L
8	Direct-access via Ethernet	N
9	Direct-access via CAN Bus	N
10	WC	L
11	Sensor	L

#### 4.5.4 ダイレクトアクセス攻撃の分析に RSS-CWSS\_CPS を用いることの優位性

自動車システムへのダイレクトアクセス攻撃が、いくつかの理由により産業制御システムなどと比べて非現実的と言われるほど不利ではないということは既に述べた。これは自動車システムへのダイレクトアクセス攻撃におけるセキュリティ設計の課題「分析対象のシステムの実情に沿った適切な分析」の「分析対象のシステムの実情」の部分である。CWSS は、分析システムの物理的/論理的構造を解釈してこの課題に対処する点で、CVSS Ver.2 よりも有利である。

サイバーフィジカルシステムのエントリーポイントと物理的/論理的ネットワーク構造に基づいて攻撃容易性を評価する場合、CVSS Ver.2 では AV, AC, および Au の 3 つのメトリックで評価するが、RSS-CWSS\_CPS では IC, AV, AS, EX, および EC の 5 つのメトリックを用いる事ができる。その特徴とダイレクトアクセス攻撃における有利不利については表 9 とともに 4.4.3 項で述べた。IC と EC という、本来はソフトウェアの脆弱性を軽減するための内部および外部のメカニズムを定義するメトリックをサイバーフィジカルシステムのネットワーク構造と物理的境界として解釈することで、システムへの攻撃容易性の解釈に柔軟性を与えている。

メトリックの数だけでなく、RSS-CWSS\_CPS でのこれらのメトリックの重みも CRSS のそれとは異なる。表 15 は、1 つのメトリックの値を 0.1 変更し、残り全てのメトリックに 1.0 を代入した場合のリスクスコアの変動量を示している。要するにリスク計算式を 1 つのメトリックで偏微分して傾きを見た。エントリーポイントに関連するメトリックについて見ると、CRSS のメトリック AV と Au の変動量はそれぞれ 0.941 である。それに対して RSS-CWSS\_CPS のメトリック AV と AS の変動量は 0.2 と 0.05 であり、その変動量は CRSS のメトリックの 1/4 以下と小さい事が分かる。一方、CRSS の攻撃の複雑さに関するメトリック AC の変動量は 0.941 であるのに対し、RSS-CWSS\_CPS のメトリック IC および EC の変動量はいずれも 1.0 である。したがって、攻撃の複雑さの変化による変動量は RSS-CWSS\_CPS の方が CRSS よりも若干大きいものの、その差はエントリーポイントでの違いほど明らかではないことも分かる。

表 15: 攻撃容易性に関連するメトリックが 0.1 変動した場合のリスク値の変化量

Table 15: Amount of Change in Risk Score When Metric Related to  
Attack Feasibility Fluctuates by 0.1

Change of $R_w$ calculated by RSS-CWSS_CPS				
AV	AS	IC	EC	EX
0.2	0.05	1.0	1.0	0.2
Change of $R_r$ calculated by CRSS				
AV	Au	AC		
0.941	0.941	0.941		

以上のように、RSS-CWSS\_CPS は CRSS と比較して、エントリーポイントの違いを決め手とするような重み配分をしておらず、攻撃の複雑さを解釈するメトリックが多いことを含め、多くの要素で他の要素も含めた総合的な判断を行うようにしている手法になっていると思われる。このことがダイレクトアクセス攻撃などの実情に合っているのではないかと考える。

#### 4.5.5 ダイレクトアクセス攻撃に対する評価結果の比較

4.3 節では、自動車システムに対するダイレクトアクセス攻撃が、他の無線通信経由の攻撃に比べ低リスクであると考えられてきたことは述べた。本節で実施したケーススタディでは RSS-CWSS\_CPS を考案し、この新しい手法が実際に評価結果を変えるかどうかを確認する。具体的には 2 つの脅威の比較を CRSS, RSS-CWSS\_CPS 双方の手法でそれぞれ行い、ダイレクトアクセス攻撃とそれ以外の攻撃のリスク値の関係が新しいリスク数値化手法よりどう変わったかについて説明を行う。

まずそれぞれのリスク数値化手法による評価結果を表 16 と表 17 に示す(抜粋していないデータは Appendix A の表 A.1～A.4 参照)。比較する 2 つの脅威のうち、1 つは遠距離無線通信 (Cellular) からの Telematics 機能モジュールの外部通信機能 (Ex-Comm. Function) に対する脅威である脅威#63 であり、もう 1 つはダイレクトアクセス攻撃からの同じく Telematics 機能モジュールの外部通信機能に対する脅威である脅威#215 である。CRSS では脅威#63 が 7.95、7 点以上の重要脅威であるのに対し、脅威#215 は 6.59、中程度の脅威であると評価されている。それに対し RSS-CWSS\_CPS では、脅威#63 が 8.13 に脅威#215 が 8.21、共に重要脅威と判定されつつ、僅かだが順位が逆転している。本項では両者の比較を行い、リスク値に差が現れたメカニズムを明らかにする。



表 16: CRSS により抽出された重要脅威(抜粋)

Table 16: Important Threats Extracted by CRSS (excepted)

#	"Where"	AV	AC	Au	C	I	A	Rr
63	Cellular of Telematics	N	M	S	None	Complete	Complete	7.95
64	Cellular of Telematics	N	M	S	None	Complete	Complete	7.95
65	Cellular of Telematics	N	M	S	Complete	Complete	None	7.95
66	Cellular of Telematics	N	M	S	None	Complete	Complete	7.95
68	Cellular of Telematics	N	M	S	Complete	Complete	None	7.95
69	Cellular of Telematics	N	M	S	Complete	Complete	None	7.95
109	Cellular of Infotainment	N	M	S	None	Complete	Complete	7.95
110	Cellular of Infotainment	N	M	S	Complete	Complete	None	7.95
112	Cellular of Infotainment	N	M	S	None	Complete	Complete	7.95
114	Cellular of Infotainment	N	M	S	Complete	Complete	None	7.95
386	LPW	A	M	N	None	Complete	Complete	7.34
387	LPW	A	M	N	None	Complete	Complete	7.34
388	LPW	A	M	N	None	Complete	Complete	7.34
...	...	...	...	...	...	...	...	...
215	Direct-access via Ethernet	L	L	N	None	Complete	Complete	6.59

表 17: RSS-CWSS\_CPS により抽出された重要脅威(抜粋)

Table 17: Important Threats Extracted by RSS-CWSS\_CPS (excepted)

#	"Where"	TI	IC	AV	AS	BI	DI	EX	EC	Rw
274	Direct-access via CAN Bus	C	N	L	N	C	H	H	N	9.00
279	Direct-access via CAN Bus	C	N	L	N	C	M	H	N	8.46
215	Direct-access via Ethernet	H	N	L	N	H	H	H	N	8.21
277	Direct-access via CAN Bus	H	N	L	N	H	H	H	N	8.21
63	Cellular of Telematics	H	N	I	M	H	H	H	L	8.13
65	Cellular of Telematics	H	N	I	M	H	H	H	L	8.13
198	Direct-access via Ethernet	C	L	L	N	C	H	H	N	8.10
270	Direct-access via CAN Bus	C	N	L	N	C	L	H	N	7.92
272	Direct-access via CAN Bus	H	N	L	N	H	M	H	N	7.69
203	Direct-access via Ethernet	C	L	L	N	C	M	H	N	7.61
360	OBD-II	H	N	L	N	H	H	H	L	7.39
239	Direct-access via Ethernet	H	L	L	N	H	H	H	N	7.39
286	Direct-access via CAN Bus	H	L	L	N	H	H	H	N	7.39
94	Cellular of Infotainment	H	L	I	M	H	H	H	L	7.31
350	OBD-II	C	L	L	N	C	H	H	L	7.29
211	Direct-access via Ethernet	M	N	L	N	H	H	H	N	7.18
269	Direct-access via CAN Bus	H	N	L	N	H	L	H	N	7.17
194	Direct-access via Ethernet	C	L	L	N	C	L	H	N	7.13
110	Cellular of Infotainment	M	N	I	M	H	H	H	L	7.11
388	LPW	C	N	A	N	C	H	L	L	7.11
162	Bluetooth	C	N	A	M	C	H	L	L	7.03

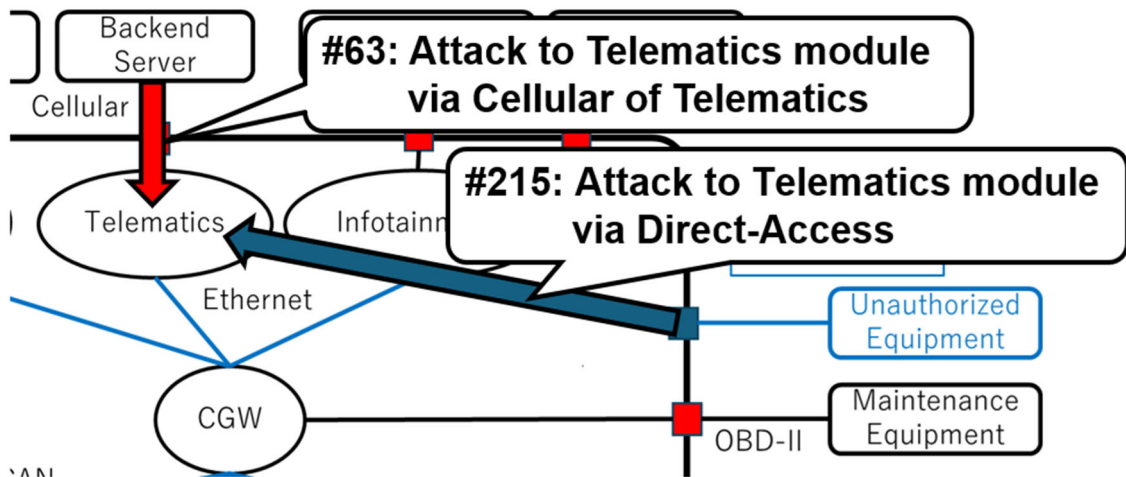


図16: ケーススタディにおける2つの脅威の比較

Figure 16: Comparison of Two Threats in The Case Study

図 16 は, 図 15 の 分析対象モデルの右上部分の Telematics 機能モジュール付近の拡大図である. 図中の赤い矢印は 脅威#63 の攻撃経路を示しており, Cellular をエントリーポイントとして侵入し, Telematics 機能モジュールをターゲットとして攻撃する脅威である. 一方青い矢印は, Ethernet ネットワークへのダイレクトアクセスを介して侵入し, 同じく Telematics 機能モジュールをターゲットとして攻撃する脅威#215 を示す.

脅威#63 と脅威#215 の比較結果を表 18 に示す. メトリックによる重みの違いを解析するために, メトリックのランクの下に代入する数値を併記した. 各資産が損害を受けることでの影響度は, RSS- CWSS\_CPS の一連のメトリック {TI, BI, DI}, および CRSS の {C, I, A} によって定義される. 資産が損害を受けることでの影響度については, RSS-CWSS\_CPS における脅威#63 と脅威

表 18: 2 つの脅威のリスク値の比較 (RSS-CWSS\_CPS & CRSS)

Table 18: Comparison of Risk Values on Two Threats  
(RSS-CWSS\_CPS & CRSS)

	Quantified by RSS-CWSS CPS								
#	AV	AS	IC	EC	EX	TI	BI	DI	Rw
63	I	M	N	L	H	H	H	H	8.13
	1.0	0.8	1	0.9	1.0	0.9	0.9	1.0	
215	L	N	N	N	H	H	H	H	8.21
	0.5	1.0	1.0	1.0	1.0	0.9	0.9	1.0	
	Quantified by CRSS								
#	AV	Au	AC			C	I	A	Rr
63	N	S	M			N	C	C	7.95
	1.0	0.56	0.61			0.00	0.66	0.66	
215	L	N	L			N	C	C	6.59
	0.395	0.704	0.71			0.00	0.66	0.66	

#215 の {TI, BI, DI} の組がそれぞれ {0.9, 0.9, 1.0}, CRSS における {C, I, A} の組が {0.00, 0.66, 0.66} であった。同じ資産が対象なため、資産が損害を受けることでの影響度については、いずれの手法においても脅威#63 と脅威#215 の評価結果に差異は無い。

よってリスク値に差異が生ずる原因は、エントリーポイントと攻撃経路によって割り当てられた他のメトリックの組、つまり第 3 章で述べた資産コンテナ手法の “Where” と “At” の組の解釈の違いである。対応するメトリックの組はそれぞれ、RSS-CWSS\_CPS の {IC, AV, AS, EX, EC}, CRSS の {AV, AC, Au} である。

双方のメトリック AV は、エントリーポイントの有利性を決定する。RSS-CWSS\_CPS における脅威#63 の AV の値 1.0 は脅威#215 の 0.5 より大きく、CRSS でも脅威#63 の AV の値 1.0 は脅威#215 の 0.395 より大きい。これは双方の評価基準が「脅威#63 は遠距離無線通信経路でカジュアルに攻撃できるため、脅威#215 より攻撃されるリスクが大きい」と判定していることを意味する。

RSS-CWSS\_CPS のメトリック AS と CRSS のメトリック Au は、それぞれの値の大きさによってエントリーポイントの認証の強さを決定する。RSS-CWSS\_CPS における脅威#63 の AS の値 0.8 は、脅威#215 の 1.0 より小さく、CRSS における脅威#63 の Au の値 0.56 は、脅威#215 の 0.704 より小さい。これは、「認証機能があるため、脅威#63 は脅威#215 よりリスクが小さい」と判定している。

攻撃経路の特徴を表すメトリックは、RSS-CWSS\_CPS では {IC, EC, EX} の組、CRSS では AC のみである。このケーススタディでは、RSS-CWSS\_CPS のメトリック EC と CRSS のメトリック AC のみが異なる。RSS-CWSS\_CPS のメトリック EC はシステム外部における物理的特性の強さを評価するが、CRSS の AC は攻撃の複雑さを曖昧に評価する。RSS-CWSS\_CPS における脅威#63 の EC の値 0.9 は脅威#215 の 1.0 より小さく、CRSS における脅威#63 の AC の値 0.61 は脅威#215 の 0.71 よりも小さい。これは「車載ネットワークに直接接続する方が容易なので、そうでない脅威#63 は脅威#215 よりもリスクが小さい」という意味である。特に RSS-CWSS\_CPS ではメトリック EC により「物理境界の脆弱性を突くことにより攻撃が用意になるか否か」という、より具体的な判定基準が付加される。

以上のように 2 つの脅威のリスク値を、RSS-CWSS\_CPS と CRSS の双方を使って算出した。CRSS で定量化した結果、この自動車システムが持つ合計 494 個の脅威のうち、脅威#63 ( $R_r = 7.95$ ) が最も高いリスク値を持つ 1 位で、脅威#215 ( $R_r = 6.59$ ) は 22 位であった。一方 RSS-CWSS\_CPS で定量化した場合は、脅威#63 ( $R_w = 8.13$ ) が 23 位、脅威#215 ( $R_w = 8.21$ ) が 9 位となった。このように、ダイレクトアクセス攻撃による脅威#215 は、ネットワーク経由の脅威#63 に比べてメトリック AV の値が低いものの、RSS-CWSS\_CPS を用いたリスク分析ではそのことだけで低リスクとは判断されず、脅威#63 と共に重大な脅威であると判断された。

この結果は、4.5.4 項で挙げた表 15 の変化量の観点から以下のように説明できる：

- CRSSにおいて、脅威#63と比較した脅威#215の各メトリックの値は、AVで0.605低く、Auで0.144高く、ACで0.1高い。これらの差に各メトリックの0.1あたりの変動量を乗算して合計すると、脅威#215のリスク値が脅威#63のリスク値よりも  
 $(0.605-0.144-0.1) \times 0.941/0.1 = 3.82$  だけ低くなると予測できる。
- 一方、RSS-CWSS\_CPSでは、脅威#63と比較した脅威#215の各メトリックの値は、AVで0.5低く、ASで0.2高く、ECで0.1高い。CRSSの場合と同様、これらの差に各メトリックの変動量を乗算して合計すると、脅威#215のリスク値が脅威#63のリスク値よりも  
 $-0.5 \times 0.2/0.1 + 0.2 \times 0.05/0.1 + 0.1 \times 1/0.1 = 0.1$  だけ高くなることが予想できる。
- したがって変動量で計算すると、脅威#215のリスク値は、CRSSでは脅威#63のリスク値より3.82低くなるが、RSS-CWSS\_CPSでは0.1高くなると分析できる。実際には他のメトリックとの相互作用により、これらの値はそれぞれ「1.36低くなる」と「0.08高くなる」と縮退するが、脅威#215と脅威#63の順序の逆転について計算式から定量的に導き出すことができる。

自動車システムへのダイレクトアクセス攻撃に対しては4.4.4項で述べたメリットBがあり、4.5.5項および表15に示すようにエントリーポイントの重みが軽いため、RSS-CWSS\_CPSによるリスク数値化はダイレクトアクセス攻撃をうまく評価できると思われる。

スコアの高い重要脅威を優先するなど、リスク値に応じて脅威をどのように区別し対処するかは、セキュリティ設計におけるリスク分析の方法論として議論の余地がある。しかし、RSS-CWSS\_CPSはセキュリティ専門家の認識を広げ、ダイレクトアクセス攻撃に注意を払うようにすることに成功したと考える。実際、CRSSでは7点に届かなかった中程度の脅威が、RSS-CWSS\_CPSでは重要脅威として評価された。この結果は重要な成果である。

以上のように、RSS-CWSS\_CPSはセキュリティ設計の課題「分析対象のシステムの実情に沿った適切な分析」を解決した。特定の領域および観点について、メトリックの解釈を適切に定義することで、脅威の特定が実現した。

#### 4.5.6 エントリーポイントの優先度の比較

本項では、2つのリスク数値化手法によってどのエントリーポイント経由の攻撃が高リスクと評価されているかを比較する。まず分析対象モデルの11個のエントリーポイントを通信距離ごとに4つのカテゴリに分類した：

- ネットワーク (長距離無線): Cellular
- 近接 (中距離): LPW, Bluetooth, DSRC
- ローカル (短距離): OBD-II, Direct-access
- その他: USB, WC, Sensor

表 19: エントリーポイントの優先度の比較

Table 19: Comparison of Priority on Entry Points

Classification of Entry Point	Rank First Appeared	
	RSS-CWSS_CPS	CRSS
Network (Cellular)	23	1
Adjacent (LPW, Bluetooth, DSRC)	72	11
Local (OBD-II, Direct-Access)	1	22
Other (USB, WC, Sensor)	111	122

次に RSS-CWSS\_CPS と CRSS において、各カテゴリの脅威が上位から数えて最初に出現する順位を比較し、その結果を表 19 に示した。従来手法である CRSS では、「ネットワーク」経由の脅威が 1 位、「近接」が 11 位、「ローカル」が 22 位、「その他」が 122 位であった。4 つのカテゴリは、CRSS のメトリック AV のランク  $N > A > L$  の順で、通信距離が長くなるほど上位にランク付けされる傾向があった。一方 RSS-CWSS\_CPS では「ローカル」経由の脅威が 1 位、「ネットワーク」が 23 位、「近接」が 72 位、「その他」が 111 位となった。4 つのカテゴリの順序は、必ずしも RSS-CWSS\_CPS のメトリック AV のランク  $N > A > L > P$  の順序には沿わない結果であった。

これは前項で述べた、RSS-CWSS\_CPS と CRSS のメトリックの重み配分の違いによるものと思われる。RSS-CWSS\_CPS では、通信距離が必ずしも攻撃での優位性をもたらすわけではなく、ネットワーク構造や物理的境界など、システムに関連する他の要素がリスク評価に作用している。その結果、「ローカル」よりも遠くて有利なはずの「近接」が、Immobilizer のインタフェースに用いられている Bluetooth の様に、その認証手段のため攻撃の機会が限られる分、攻撃の可能性を評価するメトリック EX で「ローカル」に比べてリスクが低く評価されるなど、通信距離以外の特性が出ているように考える。

#### 4.5.7 ケーススタディにおける結論

RSS-CWSS\_CPS は、従来手法である CRSS で検知できていた脅威に加え、ダイレクトアクセス攻撃も高リスクとして検知できることを確認した。RSS-CWSS\_CPS は、サイバーフィジカルシステムのネットワーク構造や物理的境界を解釈するための 2 つのメトリックを備えており、セキュリティ設計の課題である「分析対象のシステムの実情に沿った適切な分析」を解決する有用な手法だと思われる。

またケーススタディを通じて、2 つのリスク数値化手法を定量的に比較した。CRSS にはエントリーポイントに関して遠距離通信ほど有利というバイアスがあったが、RSS-CWSS\_CPS は必ずしも距離だけで判断しない手法であり、それらの違いがリスク値に現れたことを確認できた。RSS-CWSS\_CPS がダイレクトアクセス攻撃を検知できたのもその違いによるものと思われる。

## 4.6 ディスカッション

本節では、効果的なセキュリティ設計のための今後の研究における、いくつかの検討事項をまとめる。

### 4.6.1 2 ステップリスク分析に有利なリスク値のばらつき

CRSSと比較したRSS-CWSS\_CPSのリスク値の傾向として、RSS-CWSS\_CPSリスク値の分布がCRSSリスク値のそれよりも滑らかというのが挙げられる。この傾向は、資産が損害を受けることでの影響度の分布において顕著である。図17は、双方の手法で影響度に関係しないメトリックを定数(最大値)にして算出したリスク値のヒストグラムの差を示している。CRSSとRSS-CWSS\_CPSの計算式は同じではなく、RSS-CWSS\_CPSは影響度だけを取り出すことは出来ないが、影響度に関連しないメトリックを固定値にして横軸のスケールを合わせることで、影響度のばらつきは評価できる。CRSSのヒストグラムはピークが非常に尖っていて複数ある一方で、RSS-CWSS\_CPSのヒストグラムは緩やかなヒストグラムを取る。

この結果は4.4.4項で述べたメリットAを可視化したものであり、この特性がリスク値全体の分布にも影響を与えていると考えられる。リスク値の適切な分散という特徴は、リスクアセスメントにおける優先度の高い脅威の選別に役立つと考える。

実際のセキュリティ設計の現場では、時間、予算、およびリソースが限られ、脅威全体の分析を実施できない場合がある。その問題に対し提案したのが第3章の2ステップリスク分析である。これを利用して、リスク値によって重要脅威のみを詳細に分析する方針を立てた場合、ヒストグラムのこの特性は有利になる可能性がある。例えば「全体の上位○○%のみ詳細分析に進める」という方針を立てた場合、各脅威のリスク値が適度に分布しているとスクリーニングしやすい。

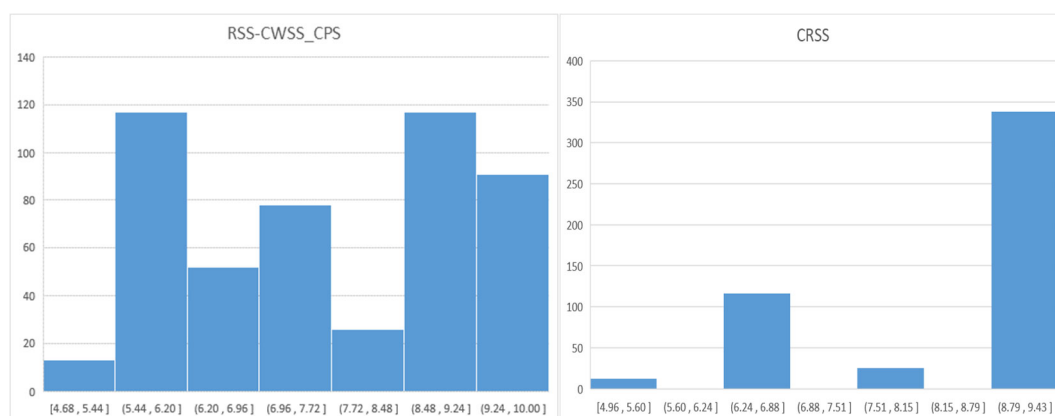


図17: 影響度スコアのヒストグラムの比較

Figure 17: Comparison on Histogram of Impact Score

JASO TP15002 や ISO/SAE 21434 などのガイドラインでは、脅威のスクリーニングについては規定されていない。しかし近年の製品開発期間は短縮化される傾向にあり、今後製品ライフサイクルにおいて定期的なリスク評価が導入されるなど、製品開発を取り巻く環境が変化すると思われる。時間、コスト、およびリソース節約目的で、このような手法がセキュリティ設計とリスクアセスメントに実装することが求められるようになるだろうと考える。

#### 4.6.2 中長期的なリスクの解釈

攻撃に関連するリスクを定量化する際、一部のリスクは適切に解釈することが困難である。攻撃それ自体が持つリスクもそのひとつである。例えば、「一度攻撃手法が確立され広まってしまうと、次回以降攻撃が容易になってしまうリスク」のように、発見されることでリスクを底上げしてしまうリスクである。このようなリスクにおいても、課題「分析対象のシステムの実情に沿った適切な分析」が求められる。

RSS-CWSS\_CPS により、このような「中長期的な」リスクを読み解くことが可能になると期待している。RSS-CWSS\_CPS における以下の 4 つのメトリックは、攻撃手法自体の影響をある程度解釈できると考える：

- **TI:** 脆弱性を悪用した場合の技術的な影響を評価するメトリックであり、攻撃手法が蔓延した際のリスクの大きさを評価できる可能性がある。
- **BI:** 現在のビジネスやミッションへの影響を評価するメトリックであるため、攻撃手法の蔓延による回避策への対応コストの大きさも評価できると考える。
- **DI:** 脆弱性の見つけやすさ評価するメトリックであり、攻撃手法が普及した際にその攻撃に続く次段の攻撃に対する脆弱性が発見されやすくなった場合に、攻撃容易性の向上を評価できる可能性がある。
- **EX:** 攻撃の可能性を評価するメトリックであり、攻撃手法の普及により攻撃が増加した時期を特定することが可能だと考える。

CWSS に基づく RSS-CWSS\_CPS を適用する際にこれらのメトリックの解釈を考慮することで、リスク評価の精度や説明性が向上できるのではないかと考え、今後の課題としたい。

#### 4.6.3 リスク評価後のプロセス

本研究で提案した 2 ステップリスク分析で将来的に追加したい手順は、前述した脅威のスクリーニングである。脅威を資産コンテナ方式で確実に網羅しつつ、詳細分析に入る前にリスク分析で重要でない脅威を除外することである。

実際、ケーススタディで示した脅威の数は 494 で、それぞれに 10 程度 のシナリオがあるように思われる。具体的な手法を含めた詳細な脅威の想定には高度なセキュリティの専門知識と経験が必要となるため、セキュリティ専門家への依頼を含め、限られたリソースで適切な分析を行うためにはスクリーニングが必要だと思われる。

詳細分析には資産の機密性、完全性、および可用性に応じて Microsoft の STRIDE を適用することで攻撃シナリオのバリエーションを増やす一方で、適度な抽象化のし直しで類似するシナリオを統合して攻撃シナリオの総数を削減するなど、詳細分析の作業量をコントロールすることも必要である。この後段の方法論の確立は今後の研究課題である。

## 4.7 むすび

本章では、セキュリティ設計における課題である「分析対象のシステムの実情に沿った適切な分析」を解決するため、リスク数値化手法の比較検討を行った。従来手法である CVSS Ver.2 ベースの CRSS に対する別のアプローチからの解決策として、CWSS をベースとして一部のメトリックの定義を再検討することで、新しいリスク数値化手法である RSS-CWSS\_CPS を考案した。RSS-CWSS\_CPS は、攻撃被害者所有の情報のみを使用してリスク値を算出する、資産コンテナ方式に適用しつつ、分析対象モデルのネットワーク構造や物理的境界を持つサイバーフィジカルシステムのリスク、特に自動車システムへのダイレクトアクセス攻撃のリスクを算出できる。

また、ダイレクトアクセス攻撃の検出に焦点を当てた自動車システムのリスク評価のケーススタディを実施した。そして従来の手法でも検出できた重要脅威に加え、ダイレクトアクセス攻撃も検出できることを確認した。

さらに CRSS と RSS-CWSS\_CPS の 2 つの方法を比較し、メトリックの重み配分を比較分析するなど定量的な評価を行い、ダイレクトアクセス攻撃が検出できる根拠を示した。RSS-CWSS\_CPS は、ICT システムの特性だけでなく、サイバーフィジカルシステムの物理的/論理的構造や境界をより柔軟に定量化するのに適切かつ十分なメトリクスとランクを備えていると考える。



# 第 5 章 ISO/SAE 21434 TARA における リスク数値化手法

本章では第 4 章に引き続き、リスク数値化手法である RSS-CWSS\_CPS について、これを ISO/SAE 21434 に適用し課題解決の優位性を比較検証した研究 [39]について述べる。

2021 年に発行された ISO/SAE 21434 は、自動車システムのリスク分析において、既存の標準での手法をミックスさせた分析手法を用いている。2023 年に JASO TP15002 が廃止となることが決まったため、ISO/SAE 21434 の脅威分析とリスクアセスメント(TARA: Threat Analysis and Risk Assessment)のプロセスに、JASO TP15002 ベースで考案した資産コンテナ方式や RSS-CWSS\_CPS の適用することを検討した。

## 5.1 背景と研究動機

第 4 章でも触れたが、国連 WP29 により成立した UN-R155[3]および UN-R156[4]や 2021 年に公開されたガイドライン ISO/SAE 21434[2]など、自動車システムのサイバーセキュリティに関する法整備や標準化が進み、セキュリティ設計に関してもアップデートが必要となったという背景がある。

ISO/SAE 21434 は自動車のサイバーセキュリティ管理に関連する用語、目的、要件、ガイドラインを提供する国際標準であり、ある程度具体的な脅威分析とリスクアセスメント (TARA) のプロセスや要件が本文に盛り込まれている。この標準では、脅威に対する攻撃容易性と攻撃が成功した結果資産が損害を受けることでの道路利用者への影響度が定義されており、それぞれ攻撃経路と手段を分析する脅威シナリオと、資産が損害を受けた場合に起きることを分析するダメージシナリオで、それぞれ攻撃容易性と損害を受けることでの影響度に紐づけるようになっている。プロセスを確認するため図 6 を再掲する。

また図 18 は、ISO/SAE 21434 での各用語の関係図であるが、赤枠で囲った部分で、脅威シナリオが資産のサイバーセキュリティ領域を危殆化するもので、脅威シナリオが実現することで道路使用者に影響を与える内容がダメージシナリオであることを示している。

2.2.3 項で前述したように、ISO/SAE 21434 第 15 章が TARA の手順を定義したもので、脅威シナリオから攻撃容易性を、ダメージシナリオから資産が損害を受けることでの影響度を導出する具体的な指標を示している：

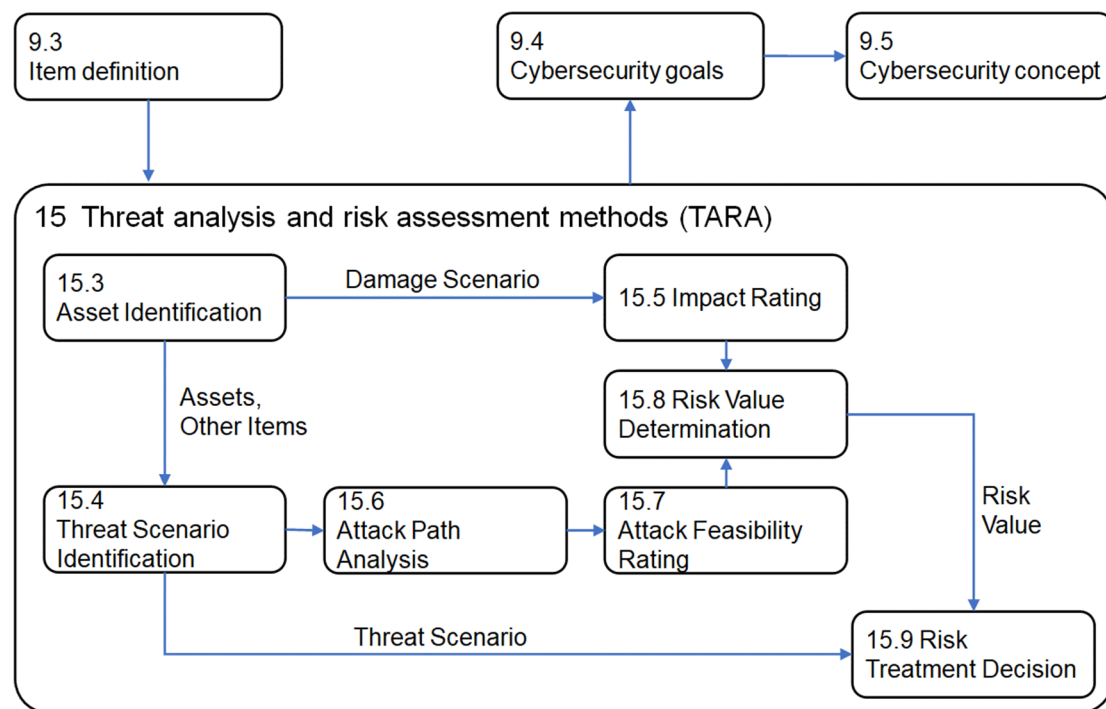


図6: ISO/SAE 21434のブロックダイアグラム(再掲)

Figure 6: Block Diagram of ISO/SAE 21434 (Reposted)

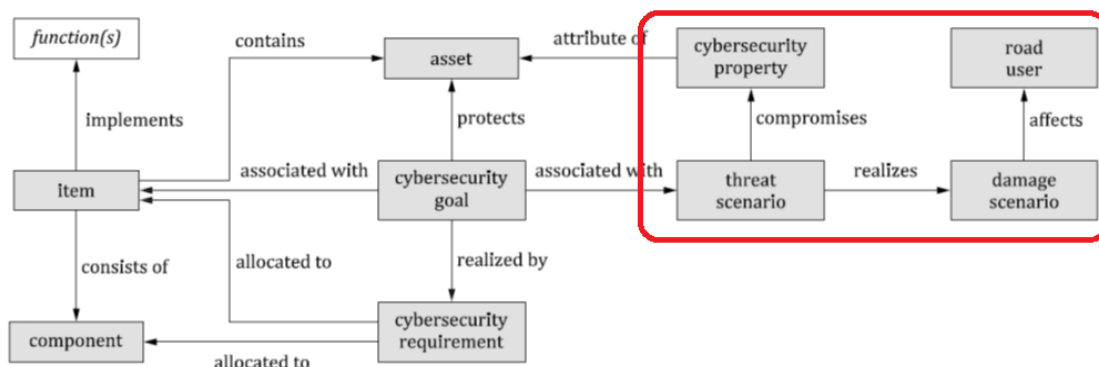


図18: 脅威シナリオとダメージシナリオの関係 [2]

Figure 18: Relationship between Threat Scenario and Damage Scenario and Other Terms [2]

- 脅威シナリオの攻撃経路や攻撃手段から攻撃容易性を評価するために、以下の3つのアプローチを推奨している:
  - Attack potential-based approach: 攻撃手段に要する時間, 攻撃者の持つ技術や攻撃対象に対する知識など, 攻撃者側の情報を基に分析するやり方.
  - CVSS-based approach: CVSS Ver.3.1 の攻撃容易性の計算式である, 式(2-4)を用いたやり方.

- Attack vector-based approach: エントリーポイントの種別を“Network”, “Adjacent”, “Local”, および“Physical”の 4 つに分け, これだけで評価するやり方.
- ダメージシナリオの資産が損害を受けることでの影響度は, S(Safety: 安全), F(Financial: 金銭), O(Operational: 運用), および P(Privacy: プライバシー)の観点で, “Severe”, “Major”, “Moderate”, および“Negligible”の 4 段階で評価する.

これに対して, 本研究で考案した資産コンテナ方式を上記 TARA プロセスに適用することを試みるにあたり, 2 つの懸案事項があると分かった:

- 攻撃容易性評価のために推奨される 3 つのアプローチは, 以下のように扱う:
  - Attack potential-based approach は攻撃者側の情報を基にした分析手法だが, それだと特定の攻撃手段に対する詳細分析が可能な反面, 攻撃被害者側の情報から攻撃経路の網羅性を担保する資産コンテナ方式とは抽象度が異なり適用が困難である.  
Attack Potential の分析手法については ISO/SAE 18045 [16]で確立した手法であるが, 上記の理由により本章の研究ではスコープ外とする.
  - CVSS-based approach に関しては, CVSS Ver.3.1 のメトリック AV, AC, PR, および UI を用いるが, 資産コンテナ方式で運用するのに以下のような問題がある.
    - ✧ CVSS Ver.2 同様, メトリック AV(Attack Vector)によるエントリーポイントの評価の影響が大きい問題がある.
    - ✧ 攻撃の複雑さを評価するメトリック AC(Attack Complexity)のランク数が CVSS Ver.2 よりさらに減り(3→2), 攻撃経路を評価する観点としては粗い.
    - ✧ 攻撃の複雑さに寄与すると思われるメトリック UI(User Interaction)が加わったものの, 攻撃の成否にユーザーのアクションが必要かどうかを判定するこのメトリックはダイレクトアクセス攻撃を評価する観点としては関係性が低い. またランク数も 2 であり, ランク間の値の差も小さいため, リスク値への寄与が小さい.
    - ✧ 本章の研究での比較対象とするが, 上記 3 つの問題により評価の精度の面で劣り, かつリスク値に対するメトリック AV の影響が大きいままであると思われる.
  - Attack vector-based approach に関しては, エントリーポイントだけでしか攻撃容易性を評価できず, CVSS-based approach 以上に評価が粗くなると思われるので, これも本研究ではスコープ外とする.
- 資産が損害を受けることでの影響度を S, F, O, P の観点で 4 段階に評価するとあるが, 複数の観点での影響度が想定された場合の 4 つの要素間の関係が定義されていない.

本論文における研究動機は, ISO/SAE 21434 TARA においても RSS-CWSS\_CPS を適用し, 上記懸案事項が解決した上で優位性を確認したいというものである.

## 5.2 本章における研究の目的と貢献

本章での研究の目的と貢献は、ISO/SAE 21434 TARA において RSS-CWSS\_CPS の適用を提案し、それにより課題「分析対象のシステムの実情に沿った、適切なリスク分析の実現」を解決することである。

CWSS には資産コンテナ方式に適したメトリックが多数あり、その中には ISO/SAE 21434 TARA の CVSS-based approach で採用されている CVSS よりも詳細な評価に影響を与えるものもある。例えば CVSS では攻撃の複雑さに関連するメトリックは AC のみであるが、CWSS では IC, EC, および EX を用いてより具体的な観点から評価を行える。CWSS を用いた RSS-CWSS\_CPS は、TARA での攻撃容易性を正確に分析するのに貢献できると考える。

本章では文献[40]に基づき、攻撃容易性の判定に CVSS-based approach を用いた ISO/SAE 21434 TARA プロセスへ資産コンテナ方式と RSS-CWSS\_CPS を適用し、自動車システムにおけるリスク分析のケーススタディを通じて貢献を検証した。第 4 章での比較研究[53]で比較対象となった CRSS は CVSS Ver.2 を用いていたのに対し、ISO/SAE 21434 TARA の CVSS-based approach では CVSS Ver.3.1 を用いているので、改めて CAN インバーダーなどのダイレクトアクセス攻撃についても検知に違いがあるかどうか確認した。

また、ISO/SAE 21434 TARA における、資産が損害を受けることでの影響度を S, F, O, P の観点で 4 段階評価を行うが、これに関しても 4.6.1 項のディスカッションで述べたような影響度のばらつきに関する問題が起きる可能性がある。CWSS のメトリックには金銭(Financial)の観点からのリスクを判断するメトリックである BI(Business Impact)があり、これと TI(Technical Impact)を組み合わせたものを S, F, O, P の代わりに使うことで、この問題も解決できる可能性がある。こちらについても本章のディスカッションで言及する。

## 5.3 ISO/SAE 21434 TARA で用いられている従来手法

本章で従来手法として扱う、ISO/SAE 21434 TARA における CVSS-based approach を含めたリスク値の算出手順について説明する。ISO/SAE 21434 第 15 章の TARA については 2.2 節でも触れたが、本章の研究での比較のため、リスク値の計算手法について改めて説明する。ISO/SAE 21434 TARA のリスク値は、攻撃容易性、損害を受けることでの影響度、そしてリスク値をそれぞれ ISO/SAE 21434 Annex F, Annex G, および Annex H を基に導出する。

**攻撃容易性(Attack feasibility rating)の導出:**

$$\text{攻撃容易性} = 8.22 \times AV \times AC \times PR \times UI \quad (2-4)(\text{再掲})$$

表 20: Table G.8 — CVSS exploitability mapping の例 [2]

Table 20: Table G.8 — Example CVSS exploitability mapping [2]

Attack feasibility rating	CVSS exploitability value
High	2.96 - 3.89
Medium	2.00 - 2.95
Low	1.06 - 1.99
Very low	0.12 - 1.05

- 計算式は式(2-4)であるが、ISO/SAE 21434 ではメトリック AV の値を V, メトリック AC の値を C, メトリック S を U(“Unchanged”)とした場合のメトリック PR の値 P, そしてメトリック UI の値を U と定義している。
- 攻撃経路や手段について表 2 に基づいて AV, AC, PR, および UI のランクを定める。
- 式(2-4)の計算結果を ISO/SAE 21434 Annex G に掲載の Table G.8(表 20)を参照し、攻撃容易性を “High”, “Medium”, “Low”, および “Very low” のいずれかに決定する。

**影響度(Impact rating)の導出:**

- 資産が損害を受けた影響をダメージシナリオとして記述する。
- ISO/SAE 21434 Annex F の Table F.1～F.4(表 21～24)を基に、S, F, O, および P の観点から、それぞれの影響度を “Severe”, “Major”, “Moderate”, および “Negligible” から選ぶ。

表 21: Table F.1 — Safetyの影響度の例 [2]

Table 21: Table F.1 — Example safety impact rating criteria [2]

Impact rating	Criteria for safety impact rating
Severe	S3: Life-threatening injuries (survival uncertain), fatal injuries
Major	S2: Severe and life-threatening injuries (survival probable)
Moderate	S1: Light and moderate injuries
Negligible	S0: No injuries

表 22: Table F.2 — Financialの影響度の例 [2]

Table 22: Table F.2 — Example financial impact rating criteria [2]

Impact rating	Criteria for financial impact rating
Severe	The financial damage leads to catastrophic consequences which the affected road user might not overcome.
Major	The financial damage leads to substantial consequences which the affected road user will be able to overcome.
Moderate	The financial damage leads to inconvenient consequences which the affected road user will be able to overcome with limited resources.
Negligible	The financial damage leads to no effect, negligible consequences or is irrelevant to the road user.

表 23: Table F.3 — Operationalの影響度の例 [2]

Table 23: Table F.3 — Example operational impact rating criteria [2]

Impact rating	Criteria for operational impact rating
Severe	The operational damage leads to the loss or impairment of a core vehicle function. EXAMPLE 1 Vehicle not working or showing unexpected behavior of core functions such as enabling of limp home mode or autonomous driving to an unintended location.
Major	The operational damage leads to the loss or impairment of an important vehicle function. EXAMPLE 2 Significant annoyance of the driver.
Moderate	The operational damage leads to partial degradation of a vehicle function. EXAMPLE 3 User satisfaction negatively affected.
Negligible	The operational damage leads to no impairment or non-perceivable impairment of a vehicle function.

表 24: Table F.4 — Privacyの影響度の例 [2]

Table 24: Table F.4 — Example privacy impact rating criteria [2]

Impact rating	Criteria for privacy impact rating
Severe	The privacy damage leads to significant or even irreversible impact to the road user. The information regarding the road user is highly sensitive and easy to link to a PII principal.
Major	The privacy damage leads to serious impact to the road user. The information regarding the road user is: a) highly sensitive and difficult to link to a PII principal; or b) sensitive and easy to link to a PII principal.
Moderate	The privacy damage leads to inconvenient consequences to the road user. The information regarding the road user is: a) sensitive but difficult to link to a PII principal; or b) not sensitive but easy to link to a PII principal.
Negligible	The privacy damage leads to no effect or, negligible consequences or is irrelevant to the road user. The information regarding the road user is not sensitive and difficult to link to a PII principal.

表 25: Table H.8 — Risk matrixの例 [2]

Table 25: Table H.8 — Risk matrix example [2]

		Attack feasibility rating			
		Very low	Low	Medium	High
Impact rating	Severe	2	3	4	5
	Major	1	2	3	4
	Moderate	1	2	2	3
	Negligible	1	1	1	1

リスク値の導出:

- ISO/SAE 21434 Annex H に掲載の Table H.8 (表 25)を基に, Attack feasibility rating の列と Impact rating の行が交差するところの数値をリスク値とする.

## 5.4 従来手法 CVSS-based approach の問題

本章では, 前述した従来手法 CVSS-based approach においても前章と同様に, 課題「分析対象のシステムの実情に沿った, 適切なリスク分析の実現」の観点から不十分ではないかという懸念があった. この懸念となる問題は以下の 2 つである:

- α) 攻撃容易性評価手法の比較対象である CVSS-based approach は, 第 4 章で比較した CRSS 同様, ネットワーク経由の攻撃を優先する傾向があると思われる. しかし実際には, 自動車システムへのダイレクトアクセス攻撃など, ネットワークを介さない攻撃が用いられ効果を挙げている場合がある.
- β) 資産が損害を受けることでの影響度について, 評価方法の詳細が表 21~24 のように定められているものの, 複数の観点で異なる影響度が挙げられた場合どう判断するかについては未定義である. 単純に「S, F, O, P で一番大きく評価された影響度を選ぶ」とする場合, 色々検討しても最終的には影響度は 4 段階のどれかに縮退してしまい, 影響度の大きさを分類するには不正確に思える. 特に自動車システムの場合, 金銭(Financial)の観点での影響は単独ではなく, 他の要素と絡めて評価するのが妥当と考えるが, そこが明確でない.

問題 α とは, 前章の従来手法である CRSS と同様, エントリーポイントの攻撃容易性を評価するメトリック AV(CVSS Ver.3.1 では “Attack” Vector と名称を変更)の結果が支配的なことで, これはそれ以外の要素を評価するメトリックが不十分であるというものである. 前章でも述べたが, メトリック AV 以外で攻撃容易性を評価できるものは, 攻撃の複雑さを評価するメトリック AC(こちらも Ver.3.1 では “Attack” Complexity と名称を変更)があるが, CRSS では 3 ランクであったのが,

CVSS-based approach ではさらに 2 ランクに減少しており, 評価が粗く変わっている. 新たに被攻撃者の行動が攻撃の成否に影響が出るかを判定するメトリック UI (User Interaction) が追加されたものの, こちらも 2 ランクに過ぎず, かつ物理的境界とは関わりが薄いメトリックである. そのため, 多くのエントリーポイントや攻撃経路を持つと思われる自動車システムの攻撃経路や物理的境界を評価するにはこの手法も不十分である.

問題  $\beta$  においては, 影響度を最終的にどう判断するかが ISO/SAE 21434 では明記されていないことが特に大きいと考える. 各観点の影響度を比較して一番大きなものを選ぶか, 観点ごとに重み付けをして合算するか, Annex H のケーススタディでもこの点には触れられていない.

後者の合算方式としては, HEAVENS security model [57] では, S と F の影響度を O と P の影響度の 10 倍の値となるよう合算し, Impact Level (IL) を求めている. また, Püllen らの研究[58]でも, 乗客の安全性 (PS), 運行制限 (OL), 金銭の損失 (FL) の 3 つの観点による影響値も評価する際に, VSL, いわゆる統計的寿命の価値[59]に基づいて, PS が比較的大きな値になるように重み付けしている.

## 5.5 ISO/SAE 21434 TARA における, 資産コンテナ方式と RSS-CWSS\_CPS の適用

本研究では前節での問題を解決するために, 資産コンテナ方式と RSS-CWSS\_CPS を組合せたアプローチを試みた. 前者手法は攻撃被害者の視点のみからリスクを評価するアプローチであり, 後者手法は前章の研究でも導入した, 分析対象のシステムの実情に沿った適切な分析を行えるリスク数値化手法である.

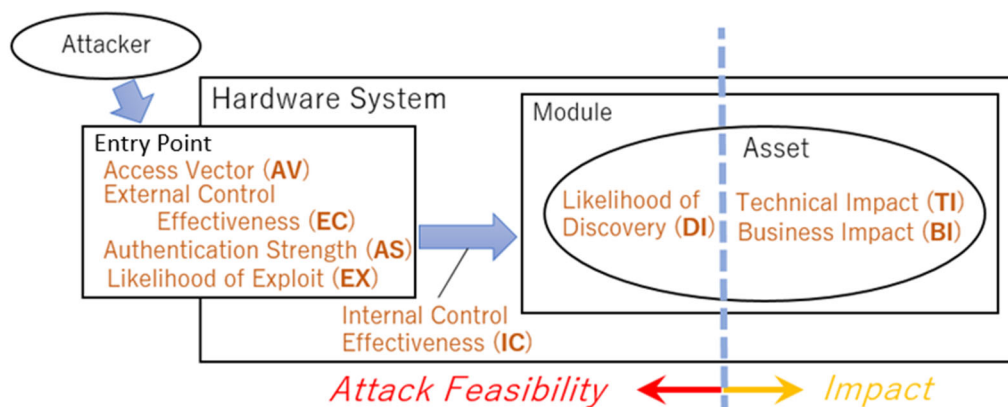


図19: RSS-CWSS\_CPSメトリックと資産コンテナ方式  
Figure 19: RSS-CWSS\_CPS Metrics  
and Asset Container Method



表 26: TARAで使用するCWSSメトリック

Table 26: CWSS Metrics Used for TARA

CWSS	Belongs to	Used for What in TARA
TI	“Asset”	Impact Rating (damage scenario)
BI		
DI		
AV	“Where”	Attack Feasibility Rating (attack path)
AS		
EX		
EC		
IC	“Where” & “At”	

### 5.5.1 資産コンテナ方式と RSS-CWSS\_CPS の第 4 章からの変更点

資産コンテナ方式および RSS-CWSS\_CPS の詳細に関しては第 3 章および第 4 章で示した。ここでは本章の研究で行った変更点について説明する。

図 19 は、資産コンテナ方式の概要図で、RSS-CWSS\_CPS で用いるメトリックを “Where (Entry Point: エントリーポイント)”, “At (Module: 攻撃目標の機能モジュール)”, および “Asset(Asset: セキュリティ上守るべき資産)” に割り振っている。内容は 4.4 節の図 14 と同様のものであり、割り振るメトリックやその判定基準も同一である。

本章の研究での第 4 章からの変更点は、メトリック DI (Likelihood of Discovery) の扱いで、資産に基づくメトリックであるものの、ISO/SAE 21434 TARA の評価では攻撃容易性を判定する観点とした。資産が損害を受けることでの影響度の評価には TI (Technical Impact) および BI (Business Impact) の 2 つのみを用いる。ISO/SAE 21434 TARA に RSS-CWSS\_CPS を適用するにおいて、資産コンテナ方式のそれぞれの観点の評価にどの CWSS メトリックを割り当てるのか、またどの CWSS メトリックの評価結果が攻撃容易性と資産が損害を受けることでの影響度に反映されるのか、表 26 にそれらの関係を示す。

### 5.5.2 RSS-CWSS\_CPS を適用することのメリット

この手法を用いるメリットを以下に示す。詳細は後節で、ケーススタディの結果を経てディスカッションで説明する:

- CVSS ベースのアプローチよりも複雑な方法で分析対象モデルのネットワーク構造や物理的境界を解釈することが可能であり、ネットワークを介した攻撃が必ずしも有利ではなく、システムの実情に合っている。
- CWSS を使用して、TI および BI の複数のメトリックで資産の評価を保証することにより、資産が損害を受けることでの影響度をより詳細に評価できる。金銭(Financial)での観点として

の Business Impact (BI) は、多くの場合攻撃が起きた時の直接的な影響である Technical Impact(TI)と密接に関連しているため、S(安全), F(金銭), O(運用), および P(プライバシー) の間で 1 つの観点のみを選択するより現実的に影響度を定量評価できる。

## 5.6 RSS-CWSS\_CPS によるケーススタディ

本節では、典型的な自動車システムを分析対象モデルとし、ISO/SAE 21434 TARA における提案手法の効果を確認する。なお、本ケーススタディで使用する表では、リスクの比較を理解しやすくするために、各メトリックのランクの代わりに数値を記入している。

### 5.6.1 自動車システムの分析対象モデル

図 20 が分析対象モデルである。通信相手として GPS の追加とエントリーポイントの名称が一部変更されたので、以下に補足する:

システム内の各機能モジュール:

- **PT(Power-Train):** エンジンなど、駆動系 ECU をまとめた機能モジュール。
- **Chassis:** ブレーキなど、シャーシ系 ECU をまとめた機能モジュール。
- **Body:** ドアロックなど、ボディ系 ECU をまとめた機能モジュール。

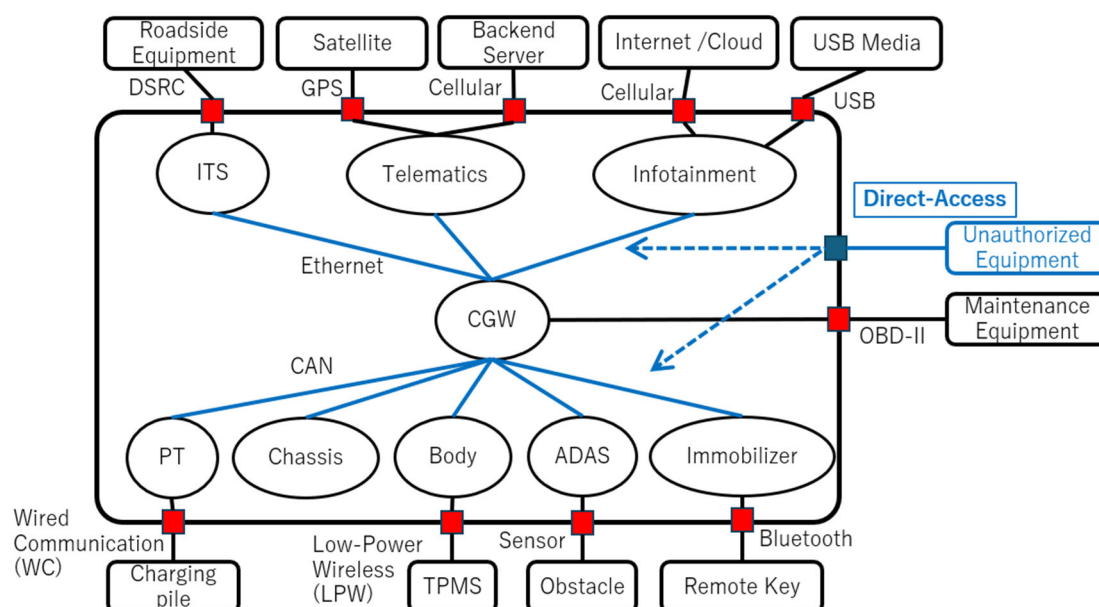


図20: 分析対象システムとしての自動車システムのシステム構成 (2)

Figure 20: System Configuration of Automotive System  
as a Model to be analyzed (2)

- **ADAS:** 運転補助機能など, ADAS (Advanced driver-assistance systems: 先進運転支援システム) 系 ECU をまとめた機能モジュール.
- **Immobilizer:** リモートキーによるエンジン始動を行う機能モジュール.
- **ITS:** ITS など, V2X(Vehicle to X)通信を行う ECU をまとめた機能モジュール.
- **Telematics:** バックアップサーバとの通信を行う, テレマティクス系 ECU をまとめた機能モジュール.
- **Infotainment:** ナビゲーションシステムや Web ブラウザ, エンターテインメント系アプリの提供など, インフォテインメント系 ECU をまとめた機能モジュール.
- **CGW:** セントラルゲートウェイ. CAN バスと Ethernet ネットワークを接続しデータを変換, CAN バス間での通信タイミングを調整などを行う機能モジュール.

#### エントリーポイント:

- **Low-Power Wireless (LPW):** TPMS と通信を行う近接無線通信インタフェース. 文献 [40]でも文献[13]同様の考えで LPW のインタフェースは PT 機能モジュールに設けられていたが, 本論文ではこれまでのケーススタディと同様に TPMS を Body 機能モジュールに移動させ, 分析し直したリスク値を用いた再評価を行っている.
- **Wired Communication (WC):** Charging Pile との電源供給兼有線通信インタフェース.
- **Sensor:** 障害物レーダーやセンサ.
- **Bluetooth:** Remote Key と通信を行う近接無線通信インタフェース.
- **DSRC:** Roadside Equipment(路側機や他の自動車など)と通信を行う近接無線通信インタフェース.
- **GPS:** GPS を受信し位置情報を取得する遠距離無線受信インタフェース.
- **Cellular:** 携帯電話通信などの遠距離無線通信を用いる通信インタフェース.
- **USB:** USB メモリなどを接続するための物理インタフェース.
- **OBD-II:** OBD-II などを使用した, CGW に対して車内にあるコネクタを介してダイアグメッセージを受ける物理インタフェース.
- **Direct-Access:** 通信ポートやコネクタなどの, ダイレクトアクセス攻撃のエントリーポイント. 前章の図 15 同様, 図 20 でも点線矢印で表現しているが, 任意の機能モジュールに直接アクセスできる通信インタフェースとみなす.

#### システム外の通信相手や環境:

- **TPMS:** Tire Pressure Monitoring System, タイヤ空気圧センサ.
- **Charging Pile:** 充電ステーションの接続ケーブル.
- **Obstacle:** 障害物.

- **Remote Key:** リモートキー.
- **Roadside Equipment:** 路側機もしくは他の自動車.
- **Satellite:** 位置情報を提供する GPS 衛星.
- **Backend Server:** ファームウェアやアプリをダウンロードしたり, データを保存したりするバックエンドサーバー.
- **Internet/Cloud:** アプリのダウンロードや Web ブラウジングに利用する, インターネットもしくはクラウドサービス.
- **USB Media:** USB をインタフェースとするメモリーデバイスなど.
- **Maintenance Equipment:** メンテナンス用診断機器.
- **Unauthorized Equipment:** ダイレクトアクセス攻撃に使用する不正な機器.

各資産については表 10 のものを継承しているので省略する.

### 5.6.2 資産定義と損害を受けることでの影響度の分析

まず自動車システム内の資産を定義し, それぞれのダメージシナリオを考慮し, メトリック TI および BI)の値を決定する. 表 27 に各資産における TI と BI の取る値を示す. 例えば「PT 機能 モジュールの制御機能」資産は, 「資産の誤作動もしくは予期せぬ機能停止は, 道路利用者の安全, 金銭, および運用の観点で影響が大きいと同時に, TI, BI ともに重大な損害として 1.0 と設定される」と評価される. また各ダメージシナリオの S, F, O, P の観点からの組み合わせは {S, F, O}もしくは{S, F, O, P}で, 必ず金銭(Financial)の観点が含まれることも示している.

本研究では自動車システムは所有者や利用者だけでなく, 周辺環境の道路使用者にも影響を与えるサイバーフィジカルシステムであると考えており, そのため S, F, O, P の観点のうち金銭の

表 27: 資産に対するTI, BIの値およびS, F, O, Pの観点

Table 27: Values of TI and BI and S, F, O, P Perspectives for Each Asset

#	"At"	"Asset"	TI	BI	SFOP Attributes	#	"At"	"Asset"	TI	BI	SFOP Attributes
1	PT	Control Function	1.0	1.0	S, F, O	7	ITS	Ex-Comm. Function	0.9	0.9	S, F, O, P
		Charging Function	1.0	1.0	S, F, O			Authentication Function	0.6	0.9	S, F, O
		In-Comm. Function	0.9	0.9	S, F, O			Authentication Information	0.9	0.9	S, F, O, P
2	Chassis	Control Function	1.0	1.0	S, F, O			In-Comm. Function	0.6	0.3	S, F, O
		In-Comm. Function	0.6	0.3	S, F, O			Personal Information	0.3	1.0	S, F, O, P
3	Body	Control Function	0.9	0.9	S, F, O	8	Telematics	Ex-Comm. Function	0.9	0.9	S, F, O, P
		In-Comm. Function	0.9	0.9	S, F, O			Authentication Function	0.6	0.6	S, F, O
		Ex-Comm. Function	1.0	1.0	S, F, O			Authentication Information	0.9	0.9	S, F, O, P
		Sensor Information	0.9	0.6	S, F, O			Remote Service App.	0.6	0.6	S, F, O, P
4	Immobilizer	Authentication Function	1.0	1.0	S, F, O			In-Comm. Function	0.6	0.3	S, F, O
		Authentication Information	0.9	0.9	S, F, O, P			Personal Information	0.3	1.0	S, F, O, P
		Ex-Comm. Function	1.0	1.0	S, F, O, P			Location Info. / Status	0.3	0.6	S, F, O, P
		In-Comm. Function	1.0	1.0	S, F, O			Ex-Comm. Function	0.6	0.6	S, F, O, P
5	ADAS	Control Function	0.9	0.3	S, F, O	9	Infotainment	Authentication Function	0.3	0.6	S, F, O
		In-Comm. Function	0.6	0.3	S, F, O			Authentication Information	0.6	0.9	S, F, O, P
		Sensor Function	0.9	0.6	S, F, O			In-Comm. Function	0.6	0.3	S, F, O
		Sensor Information	0.9	0.6	S, F, O			Navi App.	0.3	0.6	S, F, O, P
6	CGW	Data Processing Function	0.9	0.9	S, F, O			Entertainment App.	0.3	0.3	S, F, O, P
		Diagnostics Function	0.6	0.3	S, F, O			Personal Information	0.3	1.0	S, F, O, P

表 28: 脅威シナリオのリスト (抜粋)

Table 28: List of Threat Scenarios (Excepted)

#	Simplified Threat Scenario		
	“Where”	“At”	“Asset”
1	DSRC	PT	Control Function
101	GPS	Telematics	Ex-Comm. Function
201	Bluetooth	Immobilizer	Auth. Information
301	Direct-access via CAN Bus	Infotainment	In-Comm. Function
401	WC	ITS	Auth. Function

観点は常に考慮する必要があると考える。CWSS ではメトリック TI は安全, 運用, およびプライバシーの側面を評価し, メトリック BI は金銭の観点を評価できるので, 自動車システムのリスク分析に適していると考ええる。

### 5.6.3 脅威シナリオの抽出

次に, 攻撃者がどのように資産に到達するかを記述する脅威シナリオを定義する。これには資産コンテナ方式に従い, “Where(どこから)”, “At(どこ)”, および“Asset(何の資産を攻撃するか)”という観点を組み合わせて攻撃経路を記述する。表 28 は脅威シナリオの組み合わせの例である。この段階では, これらの観点のすべての組み合わせについて書き出す。例えば脅威#1 は「DSRC インタフェースから侵入し, PT 機能モジュールの制御機能を攻撃する脅威シナリオ」を示す。

### 5.6.4 攻撃経路の分析と攻撃容易性の算出

次に, 表 24 で示した各脅威シナリオに CWSS のメトリックのランクを割り振る。例えば, 脅威#1 「ITS 機能モジュールの DSRC インタフェースから侵入し, ITS 機能モジュールや CGW を介して PT 機能モジュールの制御機能を攻撃する脅威シナリオ」は, 次のように評価する。

- 複数の機能モジュールを中継して PT 機能 モジュールを攻撃するのは比較的攻撃しづらい (IC=“Indirect”=0.5)
- DSRC は近接無線通信インタフェースである(AV= “Adjacent network”=0.7)
- ITS モジュールへのアクセスには認証が必要である (AS=“Moderate”=0.8)
- DSRC 通信を行う場合, 路側機を偽装するなど送信元の場所が限定されたり, 非攻撃者が攻撃を受ける状況が限られるなどで攻撃の可能性が限定される (EX=“Medium”=0.6)
- DSRC 通信インタフェースは, 一定の対策を考慮されている (EC=“Limited”=0.9)
- PT 機能モジュールはエントリーポイントを持たないモジュールであり, その制御機能は深く侵入した後に見つけ出す必要があり, 非常に手間がかかる(DI=“Low”=0.2)

このようにして各メトリックのランクが決定され、#1 の脅威が攻撃容易性の観点から比較的风险が低いと判断できるようになる、ただし RSS-CWSS\_CPS では、攻撃容易性と資産が損害を受けることでの影響度を個別に定量化することはできないため、リスク値は次項で決定される。

攻撃容易性の 6 つのメトリックは表 26 にある IC, AV, AS, EX, EC, および DI である。表 29～31 にそれぞれの攻撃経路に割り振った各メトリックの値を示す。

表 29: 攻撃経路に対する IC, AV, AS, EX, および EC のランク(1 of 2)

Table 29: Ranks of IC, AV, AS, EX, and EC for Each Attack Route (1 of 2)

#	“Where”	“At”	IC	AV	AS	EX	EC	#	“Where”	“At”	IC	AV	AS	EX	EC
1	Cellular of Telematics	PT	0.5	1.0	0.8	1.0	0.9	28	DSRC	PT	0.5	0.7	0.8	0.6	0.9
2		Chassis	0.5	1.0	0.8	1.0	0.9	29		Chassis	0.5	0.7	0.8	0.6	0.9
3		Body	0.5	1.0	0.8	1.0	0.9	30		Body	0.5	0.7	0.8	0.6	0.9
4		Immobilizer	0.5	1.0	0.8	1.0	0.9	31		Immobilizer	0.5	0.7	0.8	0.6	0.9
5		ADAS	0.5	1.0	0.8	1.0	0.9	32		ADAS	0.5	0.7	0.8	0.6	0.9
6		CGW	0.9	1.0	0.8	1.0	0.9	33		CGW	0.9	0.7	0.8	0.6	0.9
7		ITS	0.5	1.0	0.8	1.0	0.9	34		ITS	1.0	0.7	0.8	0.6	0.9
8		Telematics	1.0	1.0	0.8	1.0	0.9	35		Telematics	0.5	0.7	0.8	0.6	0.9
9		Infotainment	0.5	1.0	0.8	1.0	0.9	36		Infotainment	0.5	0.7	0.8	0.6	0.9
10	GPS	PT	0.5	1.0	1.0	1.0	0.9	37	LPW	PT	0.5	0.7	1.0	0.2	0.9
11		Chassis	0.5	1.0	1.0	1.0	0.9	38		Chassis	0.5	0.7	1.0	0.2	0.9
12		Body	0.5	1.0	1.0	1.0	0.9	39		Body	1.0	0.7	1.0	0.2	0.9
13		Immobilizer	0.5	1.0	1.0	1.0	0.9	40		Immobilizer	0.5	0.7	1.0	0.2	0.9
14		ADAS	0.5	1.0	1.0	1.0	0.9	41		ADAS	0.5	0.7	1.0	0.2	0.9
15		CGW	0.9	1.0	1.0	1.0	0.9	42		CGW	0.9	0.7	1.0	0.2	0.9
16		ITS	0.5	1.0	1.0	1.0	0.9	43		ITS	0.5	0.7	1.0	0.2	0.9
17		Telematics	1.0	1.0	1.0	1.0	0.9	44		Telematics	0.5	0.7	1.0	0.2	0.9
18		Infotainment	0.5	1.0	1.0	1.0	0.9	45		Infotainment	0.5	0.7	1.0	0.2	0.9
19	Cellular of Infotainment	PT	0.5	1.0	0.8	1.0	0.9	46	Bluetooth	PT	0.5	0.7	0.8	0.2	0.9
20		Chassis	0.5	1.0	0.8	1.0	0.9	47		Chassis	0.5	0.7	0.8	0.2	0.9
21		Body	0.5	1.0	0.8	1.0	0.9	48		Body	0.5	0.7	0.8	0.2	0.9
22		Immobilizer	0.5	1.0	0.8	1.0	0.9	49		Immobilizer	1.0	0.7	0.8	0.2	0.9
23		ADAS	0.5	1.0	0.8	1.0	0.9	50		ADAS	0.5	0.7	0.8	0.2	0.9
24		CGW	0.9	1.0	0.8	1.0	0.9	51		CGW	0.9	0.7	0.8	0.2	0.9
25		ITS	0.5	1.0	0.8	1.0	0.9	52		ITS	0.5	0.7	0.8	0.2	0.9
26		Telematics	0.5	1.0	0.8	1.0	0.9	53		Telematics	0.5	0.7	0.8	0.2	0.9
27		Infotainment	1.0	1.0	0.8	1.0	0.9	54		Infotainment	0.5	0.7	0.8	0.2	0.9

表 30: 攻撃経路に対する IC, AV, AS, EX, および EC のランク(2 of 2)

Table 30: Ranks of IC, AV, AS, EX, and EC for Each Attack Route (2 of 2)

#	"Where"	"At"	IC	AV	AS	EX	EC	#	"Where"	"At"	IC	AV	AS	EX	EC
55	USB	PT	0.5	0.2	1.0	0.6	0.9	82	Direct-access via CAN Bus	PT	1.0	0.5	1.0	1.0	1.0
56		Chassis	0.5	0.2	1.0	0.6	0.9	83		Chassis	1.0	0.5	1.0	1.0	1.0
57		Body	0.5	0.2	1.0	0.6	0.9	84		Body	1.0	0.5	1.0	1.0	1.0
58		Immobilizer	0.5	0.2	1.0	0.6	0.9	85		Immobilizer	1.0	0.5	1.0	1.0	1.0
59		ADAS	0.5	0.2	1.0	0.6	0.9	86		ADAS	1.0	0.5	1.0	1.0	1.0
60		CGW	0.9	0.2	1.0	0.6	0.9	87		CGW	1.0	0.5	1.0	1.0	1.0
61		ITS	0.5	0.2	1.0	0.6	0.9	88		ITS	0.9	0.5	1.0	1.0	1.0
62		Telematics	0.5	0.2	1.0	0.6	0.9	89		Telematics	0.9	0.5	1.0	1.0	1.0
63		Infotainment	1.0	0.2	1.0	0.6	0.9	90		Infotainment	0.9	0.5	1.0	1.0	1.0
64	OBD-II	PT	0.9	0.5	1.0	1.0	0.9	91	WC	PT	1.0	0.2	1.0	0.2	0.9
65		Chassis	0.9	0.5	1.0	1.0	0.9	92		Chassis	0.5	0.2	1.0	0.2	0.9
66		Body	0.9	0.5	1.0	1.0	0.9	93		Body	0.5	0.2	1.0	0.2	0.9
67		Immobilizer	0.9	0.5	1.0	1.0	0.9	94		Immobilizer	0.5	0.2	1.0	0.2	0.9
68		ADAS	0.9	0.5	1.0	1.0	0.9	95		ADAS	0.5	0.2	1.0	0.2	0.9
69		CGW	1.0	0.5	1.0	1.0	0.9	96		CGW	0.9	0.2	1.0	0.2	0.9
70		ITS	0.9	0.5	1.0	1.0	0.9	97		ITS	0.5	0.2	1.0	0.2	0.9
71		Telematics	0.9	0.5	1.0	1.0	0.9	98		Telematics	0.5	0.2	1.0	0.2	0.9
72		Infotainment	0.9	0.5	1.0	1.0	0.9	99		Infotainment	0.5	0.2	1.0	0.2	0.9
73	Direct-access via Ethernet	PT	0.9	0.5	1.0	1.0	1.0	100	Sensor	PT	0.5	0.5	1.0	0.6	0.9
74		Chassis	0.9	0.5	1.0	1.0	1.0	101		Chassis	0.5	0.5	1.0	0.6	0.9
75		Body	0.9	0.5	1.0	1.0	1.0	102		Body	0.5	0.5	1.0	0.6	0.9
76		Immobilizer	0.9	0.5	1.0	1.0	1.0	103		Immobilizer	0.5	0.5	1.0	0.6	0.9
77		ADAS	0.9	0.5	1.0	1.0	1.0	104		ADAS	1.0	0.5	1.0	0.6	0.9
78		CGW	1.0	0.5	1.0	1.0	1.0	105		CGW	0.9	0.5	1.0	0.6	0.9
79		ITS	1.0	0.5	1.0	1.0	1.0	106		ITS	0.5	0.5	1.0	0.6	0.9
80		Telematics	1.0	0.5	1.0	1.0	1.0	107		Telematics	0.5	0.5	1.0	0.6	0.9
81		Infotainment	1.0	0.5	1.0	1.0	1.0	108		Infotainment	0.5	0.5	1.0	0.6	0.9

表 31: 資産に対する DI のランク

Table 31: Ranks of DI for Each Asset

#	"At"	"Asset"	DI	#	"At"	"Asset"	DI
1	PT	Control Function	0.2	7	ITS	Ex-Comm. Function	1.0
		Charging Function	0.2			Authentication Function	1.0
		In-Comm. Function	0.2			Authentication Information	1.0
2	Chassis	Control Function	0.2			In-Comm. Function	0.6
		In-Comm. Function	0.2			Personal Information	1.0
3	Body	Control Function	0.6	8	Telematics	Ex-Comm. Function	1.0
		In-Comm. Function	0.6			Authentication Function	1.0
		Ex-Comm. Function	1.0			Authentication Information	1.0
		Sensor Information	1.0			Remote Service App.	1.0
4	Immobilizer	Authentication Function	1.0			In-Comm. Function	0.6
		Authentication Information	1.0			Personal Information	1.0
		Ex-Comm. Function	1.0			Location Info. / Status	0.6
		In-Comm. Function	0.6				
5	ADAS	Control Function	0.6	9	Infotainment	Ex-Comm. Function	1.0
		In-Comm. Function	0.6			Authentication Function	1.0
		Sensor Function	1.0			Authentication Information	1.0
		Sensor Information	1.0			In-Comm. Function	0.6
6	CGW	Data Processing Function	1.0			Navi App.	1.0
		Diagnostics Function	0.6			Entertainment App.	1.0
						Personal Information	1.0

一方, CVSS は攻撃の実現可能性を計算するために 4 つのメトリックを使用する. 表 32~35 にそれぞれの攻撃経路に割り振った各メトリックの値と攻撃容易性の計算結果を示す.

RSS-CWSS\_CPS は攻撃容易性の評価に 6 つのメトリックを使用し, また 1 つのメトリックに割り振ることのできるランクの数も多いので, それぞれの攻撃経路での攻撃容易性に細やかな差別化を行うことができる. 図 21 が RSS-CWSS\_CPS について資産が損害を受けることでの影響度の部分の変動を TI と BI を固定値とすることでゼロにした値と, ISO/SAE 21434 TARA の CVSS-based approach で CVSS Ver.3.1 の式(2-4)を計算した値, それぞれのヒストグラムである. 4.6.1 項と同様, 計算式の違いで RSS-CWSS\_CPS と CVSS-based approach とで取る値の範囲が前者は 2.72~9.00, 後者は 1.18~3.89 と異なるが, 攻撃容易性に関連しないメトリックを固定値にして横軸のスケールを合わせることで, 攻撃容易性の分布の傾向を見ることができる.

これを見ると, CVSS-based approach の値の分布が低い値で偏っているのが分かる. 実際, 表 32~35 の結果を見ると, 右の CVSS-based approach の攻撃容易性のヒストグラムは “Low” が大多数でその次が “Medium”, “High” は 1 件のみで “Very low” はゼロであった. それに比べると RSS-CWSS\_CPS の値は比較的高い値にも分布しており, 脅威の差別化はより明確に行われているように思われる.

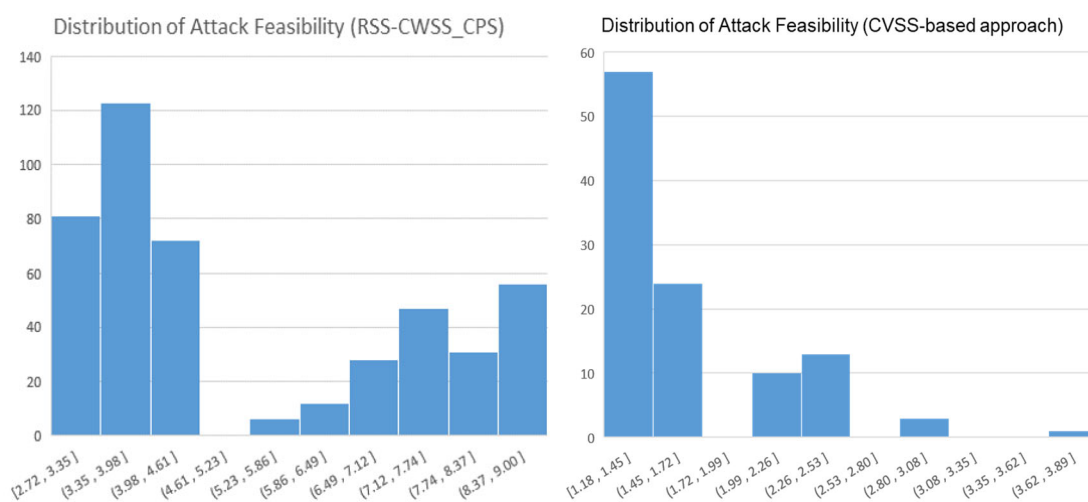


図21: 攻撃容易性のヒストグラム比較

Figure 21: Histogram Comparison on Attack Feasibility



表 32: 攻撃経路に対する CVSS Ver.3.1 の攻撃容易性分析(1 of 4)

Table 32: Attack Feasibility of Attack Routes by CVSS Ver.3.1 (1 of 4)

#	“Where”	“At”	AV	AC	PR	UI	CVSS exploitability	Attack feasibility
1	Cellular of Telematics	PT	0.85	0.44	0.62	0.85	1.62	Low
2		Chassis	0.85	0.44	0.62	0.85	1.62	Low
3		Body	0.85	0.44	0.62	0.85	1.62	Low
4		Immobilizer	0.85	0.44	0.62	0.85	1.62	Low
5		ADAS	0.85	0.44	0.62	0.85	1.62	Low
6		CGW	0.85	0.44	0.62	0.85	1.62	Low
7		ITS	0.85	0.44	0.62	0.85	1.62	Low
8		Telematics	0.85	0.77	0.62	0.85	2.84	Medium
9		Infotainment	0.85	0.44	0.62	0.85	1.62	Low
10	GPS	PT	0.85	0.44	0.85	0.85	2.22	Medium
11		Chassis	0.85	0.44	0.85	0.85	2.22	Medium
12		Body	0.85	0.44	0.85	0.85	2.22	Medium
13		Immobilizer	0.85	0.44	0.85	0.85	2.22	Medium
14		ADAS	0.85	0.44	0.85	0.85	2.22	Medium
15		CGW	0.85	0.44	0.85	0.85	2.22	Medium
16		ITS	0.85	0.44	0.85	0.85	2.22	Medium
17		Telematics	0.85	0.77	0.85	0.85	3.89	High
18		Infotainment	0.85	0.44	0.85	0.85	2.22	Medium
19	Cellular of Infotainment	PT	0.85	0.44	0.62	0.85	1.62	Low
20		Chassis	0.85	0.44	0.62	0.85	1.62	Low
21		Body	0.85	0.44	0.62	0.85	1.62	Low
22		Immobilizer	0.85	0.44	0.62	0.85	1.62	Low
23		ADAS	0.85	0.44	0.62	0.85	1.62	Low
24		CGW	0.85	0.44	0.62	0.85	1.62	Low
25		ITS	0.85	0.44	0.62	0.85	1.62	Low
26		Telematics	0.85	0.44	0.62	0.85	1.62	Low
27		Infotainment	0.85	0.77	0.62	0.85	2.84	Medium

表 33: 攻撃経路に対する CVSS Ver.3.1 の攻撃容易性分析(2 of 4)

Table 33: Attack Feasibility of Attack Routes by CVSS Ver.3.1 (2 of 4)

#	“Where”	“At”	AV	AC	PR	UI	CVSS exploitability	Attack feasibility
28	DSRC	PT	0.62	0.44	0.62	0.85	1.18	Low
29		Chassis	0.62	0.44	0.62	0.85	1.18	Low
30		Body	0.62	0.44	0.62	0.85	1.18	Low
31		Immobilizer	0.62	0.44	0.62	0.85	1.18	Low
32		ADAS	0.62	0.44	0.62	0.85	1.18	Low
33		CGW	0.62	0.44	0.62	0.85	1.18	Low
34		ITS	0.62	0.77	0.62	0.85	2.07	Medium
35		Telematics	0.62	0.44	0.62	0.85	1.18	Low
36		Infotainment	0.62	0.44	0.62	0.85	1.18	Low
37	LPW	PT	0.62	0.44	0.85	0.85	1.62	Low
38		Chassis	0.62	0.44	0.85	0.85	1.62	Low
39		Body	0.62	0.77	0.85	0.85	2.84	Medium
40		Immobilizer	0.62	0.44	0.85	0.85	1.62	Low
41		ADAS	0.62	0.44	0.85	0.85	1.62	Low
42		CGW	0.62	0.44	0.85	0.85	1.62	Low
43		ITS	0.62	0.44	0.85	0.85	1.62	Low
44		Telematics	0.62	0.44	0.85	0.85	1.62	Low
45		Infotainment	0.62	0.44	0.85	0.85	1.62	Low
46	Bluetooth	PT	0.62	0.44	0.62	0.85	1.18	Low
47		Chassis	0.62	0.44	0.62	0.85	1.18	Low
48		Body	0.62	0.44	0.62	0.85	1.18	Low
49		Immobilizer	0.62	0.77	0.62	0.85	2.07	Medium
50		ADAS	0.62	0.44	0.62	0.85	1.18	Low
51		CGW	0.62	0.44	0.62	0.85	1.18	Low
52		ITS	0.62	0.44	0.62	0.85	1.18	Low
53		Telematics	0.62	0.44	0.62	0.85	1.18	Low
54		Infotainment	0.62	0.44	0.62	0.85	1.18	Low

表 34: 攻撃経路に対する CVSS Ver.3.1 の攻撃容易性分析(3 of 4)

Table 34: Attack Feasibility of Attack Routes by CVSS Ver.3.1 (3 of 4)

#	“Where”	“At”	AV	AC	PR	UI	CVSS exploitability	Attack feasibility
55	USB	PT	0.55	0.44	0.85	0.85	1.44	Low
56		Chassis	0.55	0.44	0.85	0.85	1.44	Low
57		Body	0.55	0.44	0.85	0.85	1.44	Low
58		Immobilizer	0.55	0.44	0.85	0.85	1.44	Low
59		ADAS	0.55	0.44	0.85	0.85	1.44	Low
60		CGW	0.55	0.44	0.85	0.85	1.44	Low
61		ITS	0.55	0.44	0.85	0.85	1.44	Low
62		Telematics	0.55	0.44	0.85	0.85	1.44	Low
63		Infotainment	0.55	0.44	0.85	0.85	1.44	Low
64	OBD-II	PT	0.55	0.44	0.85	0.85	1.44	Low
65		Chassis	0.55	0.44	0.85	0.85	1.44	Low
66		Body	0.55	0.44	0.85	0.85	1.44	Low
67		Immobilizer	0.55	0.44	0.85	0.85	1.44	Low
68		ADAS	0.55	0.44	0.85	0.85	1.44	Low
69		CGW	0.55	0.77	0.85	0.85	2.52	Medium
70		ITS	0.55	0.44	0.85	0.85	1.44	Low
71		Telematics	0.55	0.44	0.85	0.85	1.44	Low
72		Infotainment	0.55	0.44	0.85	0.85	1.44	Low
73	Direct-access via Ethernet	PT	0.55	0.44	0.85	0.85	1.44	Low
74		Chassis	0.55	0.44	0.85	0.85	1.44	Low
75		Body	0.55	0.44	0.85	0.85	1.44	Low
76		Immobilizer	0.55	0.44	0.85	0.85	1.44	Low
77		ADAS	0.55	0.44	0.85	0.85	1.44	Low
78		CGW	0.55	0.77	0.85	0.85	2.52	Medium
79		ITS	0.55	0.77	0.85	0.85	2.52	Medium
80		Telematics	0.55	0.77	0.85	0.85	2.52	Medium
81		Infotainment	0.55	0.77	0.85	0.85	2.52	Medium

表 35: 攻撃経路に対する CVSS Ver.3.1 の攻撃容易性分析(4 of 4)

Table 35: Attack Feasibility of Attack Routes by CVSS Ver.3.1 (4 of 4)

#	“Where”	“At”	AV	AC	PR	UI	CVSS exploitability	Attack feasibility
82	Direct-access via CAN Bus	PT	0.55	0.77	0.85	0.85	2.52	Medium
83		Chassis	0.55	0.77	0.85	0.85	2.52	Medium
84		Body	0.55	0.77	0.85	0.85	2.52	Medium
85		Immobilizer	0.55	0.77	0.85	0.85	2.52	Medium
86		ADAS	0.55	0.77	0.85	0.85	2.52	Medium
87		CGW	0.55	0.77	0.85	0.85	2.52	Medium
88		ITS	0.55	0.44	0.85	0.85	1.44	Low
89		Telematics	0.55	0.44	0.85	0.85	1.44	Low
90		Infotainment	0.55	0.44	0.85	0.85	1.44	Low
91	WC	PT	0.55	0.77	0.85	0.85	2.52	Medium
92		Chassis	0.55	0.44	0.85	0.85	1.44	Low
93		Body	0.55	0.44	0.85	0.85	1.44	Low
94		Immobilizer	0.55	0.44	0.85	0.85	1.44	Low
95		ADAS	0.55	0.44	0.85	0.85	1.44	Low
96		CGW	0.55	0.44	0.85	0.85	1.44	Low
97		ITS	0.55	0.44	0.85	0.85	1.44	Low
98		Telematics	0.55	0.44	0.85	0.85	1.44	Low
99		Infotainment	0.55	0.44	0.85	0.85	1.44	Low
100	Sensor	PT	0.55	0.44	0.85	0.85	1.44	Low
101		Chassis	0.55	0.44	0.85	0.85	1.44	Low
102		Body	0.55	0.44	0.85	0.85	1.44	Low
103		Immobilizer	0.55	0.44	0.85	0.85	1.44	Low
104		ADAS	0.55	0.77	0.85	0.85	2.52	Medium
105		CGW	0.55	0.44	0.85	0.85	1.44	Low
106		ITS	0.55	0.44	0.85	0.85	1.44	Low
107		Telematics	0.55	0.44	0.85	0.85	1.44	Low
108		Infotainment	0.55	0.44	0.85	0.85	1.44	Low

しかし 5.4 節で予想した, CVSS-based approach における問題  $\alpha$  については, 表 32~35 の結果を見る限り必ずしもネットワークが圧倒的に有利とはなっていないように思われた. 上記 4 枚の表の結果では, ネットワークのエントリーポイントである Cellular と Direct-Access による CVSS exploitability value は前者の値が大きいものの, 共に評価は “Medium” であった. おそらく CVSS が Ver.2 から Ver.3 以降に上がった際にメトリック AV のランク間の値の差が “Network” と “Local” で 1.000 と 0.395 であったのが 0.85 と 0.55 に差が縮まった影響だと思われる.むしろ値の分布が偏っているのはメトリック AV のせいだけではなく, 5.4 節の問題  $\alpha$  で言及したように, 攻撃の複雑さを評価するメトリック AC のランクが 3 から 2 に減ったことが大きいように思われる. CVSS-based approach は CRSS よりエントリーポイントの属性が支配的という状況は緩和されたものの, 引き続き図 21 のように, 攻撃容易性の評価においてメトリックが適切に使われていないという問題が残っている.

### 5.6.5 リスク値の算出と考察

以上のように 8 つの CWSS メトリックが決定されたので, RSS-CWSS\_CPS に基づいて式(5-1)~(5-5)によりリスク値  $R_w$  を算出する. 式(5-1)~(5-5)を再掲する:

$$\text{リスク値 } R_w = S_{\text{Base}} \times S_{\text{Surface}} \times S_{\text{Env}} / 10.0 \quad (5-1)$$

$$\text{基本値: } S_{\text{Base}} = 4 \{f(TI) \cdot (10TI + 15) \cdot IC\} \quad (5-2)$$

$$\text{エントリーポイントの評価: } S_{\text{Surface}} = \{20(AV+2) + 5AS + 35\} / 100.0 \quad (5-3)$$

$$\text{環境の評価: } S_{\text{Env}} = \{f(BI) \cdot (10BI + 3DI + 4EX + 3) \cdot EC\} / 20.0 \quad (5-4)$$

$$\text{影響度の補正式: } f(x) = 0(\text{if } x=0), 1(\text{otherwise}) \quad (5-5)$$

表 36 は, 脅威シナリオとそのリスク値のリストを抜粋したものである(抜粋していないデータおよび CVSS-based approach での分析結果は Appendix A の表 A.5~A.8 参照). GPS やセルラーなどのネットワークを介した攻撃に加え, 第 4 章でも述べたダイレクトアクセス攻撃も脅威となる攻撃の上位にランクインしている事が確認できる.

ちなみに, 脅威 #1 のリスク値は 3.35 で, 本ケーススタディで抽出された 456 件の脅威中 249 位の低リスク脅威としてランク付けされている. これは資産が損害を受けることでの影響度を決めるメトリクス TI と BI の値が大きいにもかかわらず, 攻撃の実行容易性を決定するメトリックの値が低いことが原因であると考えられる. 脅威 #20 も脅威 #1 と同じ DSRC 通信経由の脅威であるが, これは ITS 機能モジュール内の車外通信機能への脅威(DI=1.0)であり, 複数の機能モジュールを経由するいわゆる踏み台攻撃を必要としない(IC=1.0)ため, より危険な脅威と判定されたのだと思われる. その結果, 脅威 #20 ( $R_w=6.99$ , 47 位) のリスク値は脅威 #1 を上回っている.

表 36: 脅威シナリオとリスク値 (抜粋)

Table 36: List of Threat Scenarios and Risk Values (excepted)

#	Rank	“Where”	CWSS Metrics for RSS-CWSS_CPS								
			Attack Feasibility						Impact		Rw
			IC	AV	AS	EX	EC	DI	TI	BI	
274	1	Direct-access via CAN Bus	1.0	0.5	1.0	1.0	1.0	1.0	1.0	1.0	9.00
101	5	GPS	1.0	1.0	1.0	1.0	0.9	1.0	0.9	0.9	8.21
63	14	Cellular	1.0	1.0	0.8	1.0	0.9	1.0	0.9	0.9	8.13
322	25	OBD-II	1.0	0.5	1.0	1.0	0.9	1.0	0.9	0.9	7.39
350	43	LPW	1.0	0.7	1.0	0.2	0.9	1.0	1.0	1.0	7.11
200	45	Bluetooth	1.0	0.7	0.8	0.2	0.9	1.0	1.0	1.0	7.03
20	47	DSRC	1.0	0.7	0.8	0.6	0.9	1.0	0.9	0.9	6.99
170	100	USB	0.9	0.2	1.0	0.6	0.9	1.0	0.9	0.9	5.68
434	101	Sensor	1.0	0.5	1.0	0.6	0.9	1.0	0.9	0.6	5.60
381	108	WC	1.0	0.2	1.0	0.2	0.9	0.2	1.0	1.0	5.44
...	...	...	...	...	...	...	...	...	...	...	...
1	249	DSRC	0.5	0.7	0.8	0.6	0.9	0.2	1.0	1.0	3.35

## 5.7 ケーススタディの結果から見た提案手法の優位性

本節では、ケーススタディの結果から見える本研究の手法の優位性について説明する。あくまで一実施例であるものの、本研究のアイデアは 5.4 節で述べた 2 つの問題を解決し、具体的な分析を進めることでいくつかの知見が得られるように思われる。

### 5.7.1 エントリーポイント別の攻撃容易性の傾向の変化

5.4 節の問題  $\alpha$  で述べたように、ISO/SAE 21434 TARA における攻撃容易性の分析を行う際に CVSS-based approach を用いる場合、第 4 章の研究で比較対象とした CVSS Ver.2 をベースにした CRSS と同様、ネットワーク経由の攻撃が有利になる傾向があると考え、別のアプローチである RSS-CWSS\_CPS の適用を提案した。5.6.4 項で得られたケーススタディの結果(表 32～35)を見る限りではエントリーポイントが GPS であることを除いては、攻撃容易性は “Medium” がせいぜいで、エントリーポイント間での大きな差は見られなかったが、本項では第 4 章と同様の観点から、本方式がこの問題を解決していることを確認する。

表 37 では、エントリーポイントを 4 つのカテゴリに分類し、それぞれ ISO/SAE 21434 の CVSS-based approach と RSS-CWSS\_CPS の間で、エントリーポイントの攻撃容易性を比較し、各カテゴリのエントリーポイントが上位から数えて最初に出現する順位を比較した。4.5.6 項における表 19 の比較はリスク値で行ったが、ISO/SAE 21434 TARA でのリスク値は計算式ではなくマトリクスで

表 37: エントリーポイントの優先度の比較

Table 37: Comparison of Priority on Entry Points

Entry Point	First Appeared in 456 threats	
	CVSS-based approach	RSS-CWSS_CPS
Network (Cellular, GPS)	1	1
Adjacent (LPW, Bluetooth, DSRC)	8	88
OBD-II, Direct-Access	27	1
Other (USB, WC, Sensor)	213	105

算出する整数値であり、細かな比較が困難であったため、表 37 の比較ではカテゴライズ前の攻撃容易性の数値で比較を行った。

- ネットワーク (長距離無線): Cellular, GPS
- 近接 (中距離): LPW, Bluetooth, DSRC
- ローカル (短距離): OBD-II, Direct-access
- その他: USB, WC, Sensor

ISO/SAE 21434 TARA CVSS-based approach では、エントリーポイントにおいて、ネットワーク、近接ネットワーク、ダイレクトアクセス、およびその他の順に脅威のリスクが高く、攻撃が有利であると評価される。一方提案手法では、ネットワークとダイレクトアクセスの脅威が最上位で、その他の脅威が続く。そのため、攻撃者と攻撃対象との距離が長くても必ずしも有利とは限らない。

第 4 章では、RSS-CWSS\_CPS と CRSS のリスク値を比較し、RSS-CWSS\_CPS においてはエントリーポイントが決定的な要素ではないと述べた。そして根拠として、RSS-CWSS\_CPS のメトリックの重み付けが CVSS Ver.2 のそれと異なることを指摘した。本項ではこれらの主張に基づき、CVSS Ver.3.1 に基づく CVSS-based approach についてもメトリックの重み付けを RSS-CWSS\_CPS と比較した。

表 38 は、攻撃容易性に関連するメトリックが 0.1 変動した時に、残り全てのメトリックを 1.0 に設定した場合のリスク値の変動量(いわばリスク数値化式の偏微分)を示している。エントリーポイントに関する CVSS-based approach のメトリクス AV と PR の変動はともに 0.822 と、CRSS の 0.941 より重みが少なくなったものの、RSS-CWSS\_CPS のメトリクス AV, AS の変動は 0.2, 0.05 と 1/4 以下とさらに小さい。

一方 CVSS-based approach の攻撃の複雑さに関するメトリック AC による変動量は 0.822 であるのに対し、RSS-CWSS\_CPS のメトリック IC および EC による変動量はいずれも 1.0 と重みはやや大きくなった。しかし表 2 と表 3 から明らかなように、AC が 2 ランクのメトリックであるのに対し、IC や EC はそれぞれ 6 ランクのメトリックであるため、最終的なリスク値の結果に極端に支配的になることは無いと思われる。

表 38: 攻撃容易性に関連するメトリックが 0.1 変動した場合のリスク値変化量

Table 38: Amount of Change in Risk Value When the Metric Related to Attack Feasibility Changes by 0.1

Change of Rw calculated by RSS-CWSS_CPS				
AV	AS	IC	EC	EX
0.2	0.05	1.0	1.0	0.2
Change of Rr calculated by CRSS [51][52]				
AV	Au	AC		
0.941	0.941	0.941		
Change of E calculated by CVSS-based approach				
AV	AC	PR	UI	
0.822	0.822	0.822	0.822	

したがって 5.4 節の問題  $\alpha$  は, 5.6.4 項のケーススタディ最後で述べたように AV だけでなく AV と AC 両方のメトリックの問題だと再確認されたものの, 最終的にこの問題が RSS-CWSS\_CPS で解決されたことが計算式の分析によっても確認できた. この結果は, CWSS が攻撃容易性の解釈の面で柔軟であり, セキュリティ設計における課題「分析対象のシステムの実情に沿った適切な分析」を解決できていることを示している.

## 5.7.2 資産が損害を受けることでの影響度におけるバイアス

5.4 節の問題  $\beta$  は, 資産が損害を受けることでの影響度の評価において, 安全(S), 金銭(F), 運用(O), およびプライバシー(P)をどう関連付けて扱うかという問題である. ISO/SAE 21434 TARA では, これらの観点をどう組み合わせで影響度を算出するかが明記されていない. 本項では RSS-CWSS\_CPS を用いた提案を示す.

まず, ISO/SAE 21434 TARA における資産が損害を受けることでの影響度を評価する観点(S, F, O, P), CVSS の資産に関するメトリック(C, I, A), および RSS-CWSS\_CPS のメトリクス (TI と BI) の関係を確認する. 表 39 は ISO/SAE 21434 TARA における S, F, O, P の観点が各手法のどのメトリックに対応するかを示す. CVSS の C (機密性), I (完全性), および A (可用性) のメトリックは, S, F, O, P 観点の S, O, P に近い観点を持っているが, F に対応する観点は含まれない.

表 39: 各観点・メトリックの関連性

Table 39: Relevance of Each Perspective/Metric

SFOP Perspectives	Impact metrics in	RSS-CWSS_CPS
Safety	Integrity (I) and Availability (A)	The combination of Safety, Operational and Privacy impacts can be evaluated to Technical Impact
Operational	Availability (A)	
Privacy	Confidentiality (C)	
Financial	No applicable metric	Business Impact

一方, RSS-CWSS\_CPS を使用する場合, S, O, および P の 3 つの観点は 1 つのメトリック TI だけで評価する必要があるが, F はメトリック BI により評価できる。

上記のように S, O, および P の観点を単一のメトリック TI で評価する必要があるものの, 次の 2 つの理由から RSS-CWSS\_CPS が有利であると考えられる:

- 1) CWSS でメトリック TI と BI の関係が十分考慮され標準化されているため, 信頼性がある。
- 2) メトリック TI だけでも, ダメージシナリオの安全, 運用, およびプライバシーの観点での影響を十分に評価できる。

理由 2) の根拠は, 5.4 節で言及した HEAVENS security model [57]での Impact Level(IL)の考え方にあるように, 運用およびプライバシーの観点からの損害は安全や金銭のそれに比べて比較的軽微であるのではないかということにある。図 22 に HEAVENS security model での S, F, O, P 観点での値配分の違いを示す。メトリック TI は “Critical”, “High”, “Medium”, “Low”, および “None” の 5 ランクを選択できるものの, これひとつで各々 4 ランクを持つ S, O, および P の組み合わせに比べて定量化における影響度の区別の点で弱いのではないかという懸念があった。しかし実際にケーススタディを実施し, 資産が損害を受けることでの影響度で取る値のヒストグラムを比較してみると, TI 単独でも遜色ない結果が出ている。

図 23 のヒストグラムは, ケーススタディのデータを基に各観点での資産が損害を受けることでの影響度の取る値の分布をヒストグラムにしてみたものである。4.6.1 項や 5.6.4 項のヒストグラム分析と同様に, 影響度だけを取り出せない計算式もあるため取る値の範囲がそれぞれ異なるが,

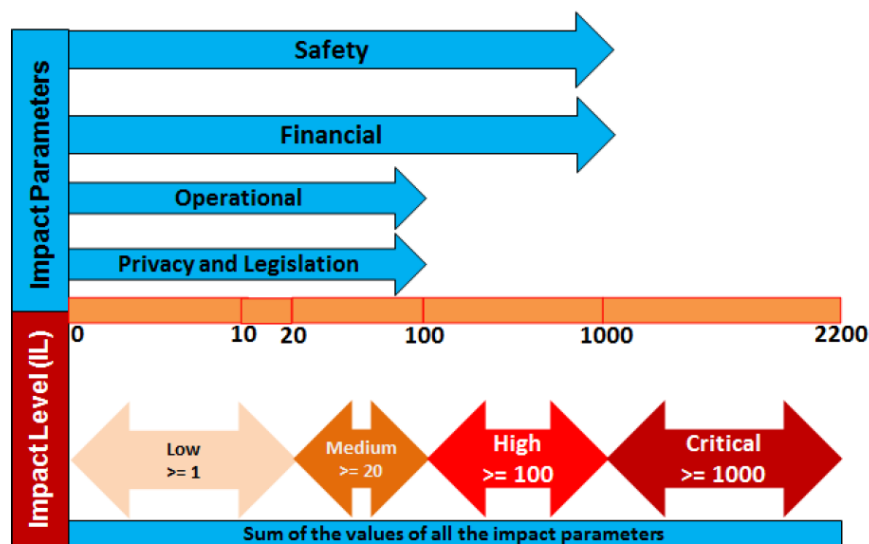


図22: HEAVENS security modelにおける  
インパクトレベルとパラメータの考え方 [57]

Figure 22: Impact Parameters and Impact Level  
in the HEAVENS security model [57]

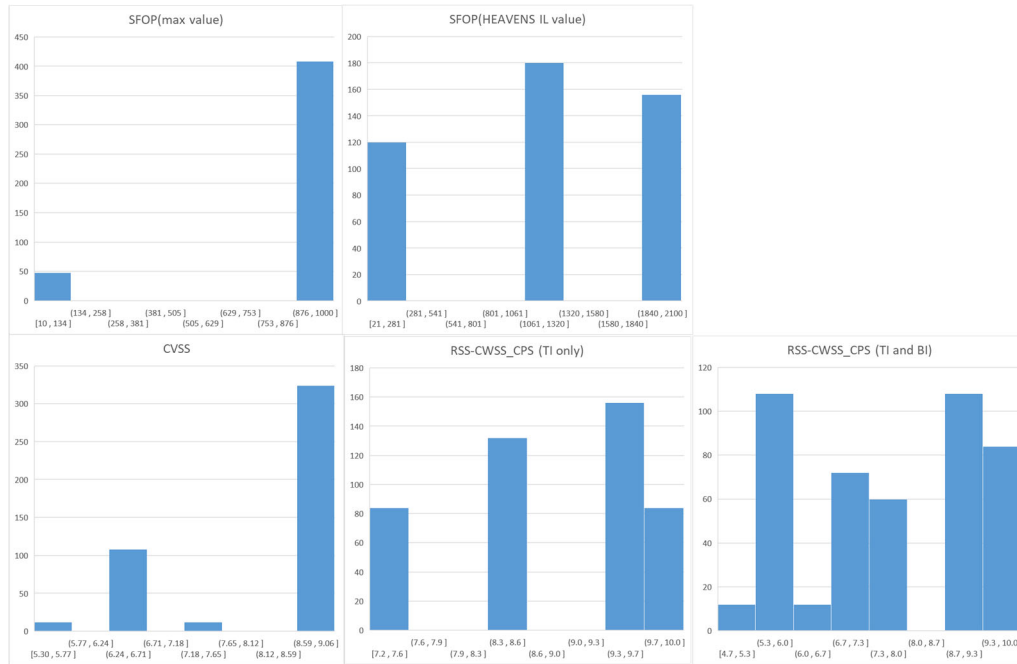


図23: 資産が損害を受けることでの影響度のヒストグラム比較

Figure 23: Histogram Comparison on Impact Rating

影響度に関連しないメトリックを固定値にして横軸のスケールを合わせることで、影響度間の分布の違いを見ることができる。

上段が ISO/SAE 21434 TARA の Impact Rating での影響度の値で、左がダメージシナリオで S, F, O, P を評価した際に最も大きな深刻度(Severity)が出たものを選んだ場合の影響度の分布、右が HEAVENS security model の IL で採用されている、S, F, O, P で重みを変えて合算する方法で算出した影響度の分布である。左のように最大値を選ぶ方法だと深刻度が “Severe” になりがちで、影響度の分布は偏る傾向にある。

次に下段は左から CVSS の C, I, A で評価した影響度、CWSS の TI のみで評価した影響度、CWSS の TI と BI の両方で評価した影響度、それぞれの値の分布である。CWSS は攻撃容易性と影響度を分けて算出できないため、この場合 5.6.4 項 図 21 の攻撃容易性のヒストグラム評価の時の逆で、攻撃容易性の部分の変動を TI と BI 以外のメトリックを固定値とすることでゼロにした値を使用している。

これらのヒストグラムを比較すると、ISO/SAE 21434 TARA で用いられている S, F, O, P の観点からの影響度は CVSS の C, I, A での評価と同程度に影響度を最大に評価しがちであり、個々のダメージシナリオの影響度をうまく区別できていないように思われる。その点 RSS-CWSS\_CPS ではメトリック TI 単独での評価によっても、影響度の分布の偏りが緩和されており、さらに TI と BI の両方で評価することで、影響度の分布の偏りが大幅に改善されていることが分かる。5.4 節の問題 β に関してはどれが正解かは今後分析するケースを増やして考えていく必要があるが、本研究で提唱する資産コンテナ方式に基づく2ステップリスク分析を適用し重要脅威のスクリーニングを



行うという目的で考えると、攻撃容易性や資産が損害を受けることでの影響度の2つの評価値は偏りが少なく分布しているのが望ましい。したがって RSS-CWSS\_CPS での影響度評価の分布が最も偏りが少なかった以上、問題  $\beta$  を解決するために RSS-CWSS\_CPS のメトリック TI と BI で影響度を分析することを提案する。

## 5.8 むすび

本章では第4章に引き続き RSS-CWSS\_CPS を ISO/SAE 21434 のプロセスに適用し、ISO/SAE21434 の従来手法である CVSS-based approach でのリスク数値化結果と比較した。

RSS-CWSS\_CPS のベースとなった CWSS は課題の解決に加え、“Financial”すなわち金銭の観点からの損害を評価するメトリック BI を持ち、ISO/SAE 21434 TARA の Impact Rating での影響度の評価に用いられている観点である S, F, O, P に対しても効果的な評価が行えるという優位性が確認できた。

後者に関しては、ISO/SAE21434 TARA プロセスにおいて資産が損害を受けることでの影響度の評価に用いられている S, F, O, P の観点と RSS-CWSS\_CPS のメトリック TI, BI との関連性に着目し、メトリック TI と BI を用いることにより S, F, O, P 観点よりも影響度の評価をより細かく行える可能性についても述べた。

## 第 6 章 おわりに

本論文ではセキュリティ設計における「分析対象のシステムの実情に沿った適切な分析」という課題を抽出し、自動車システムへのダイレクトアクセス攻撃の事例を挙げ、この攻撃のリスクを新たな観点から評価できるリスク数値化手法 RSS-CWSS\_CPS を考案し、提案及び評価を行った。

### 6.1 本研究で得られた成果

本研究で得られた成果を以下に示す：

- ソフトウェアの脆弱性評価基準である CWSS に物理的/論理的なネットワーク構造や物理的境界を解釈する観点を加えることにより、サイバーフィジカルシステムのリスク分析を行えるリスク数値化手法 RSS-CWSS\_CPS を考案した。
- ダイレクトアクセス攻撃の前提条件を設定し、これに RSS-CWSS\_CPS を自動車システムの分析対象モデルに適用したケーススタディを行うことで、既存のリスク数値化手法である CRSS や ISO/SAE 21434 TARA の CVSS-based approach との比較評価を行うことで、ダイレクトアクセス攻撃を検知できることを確認した。
- ケーススタディで得られたデータを基に、計算式の解析やデータの統計分析を行うことで、RSS-CWSS\_CPS と既存手法とで重要視している観点的違いや、実際の数値のばらつきを評価した。

### 6.2 今後の課題

本論文の研究に関連する、リスク分析手法に関する研究のゴールとして、「資産コンテナ方式と 2 ステップリスク分析を適用し、重要脅威を優先的に抽出しておき、それらを優先的に詳細分析することで効率良く対策を導出したい」というものがある。本論文で述べたリスク数値化手法はこのゴールを実現するための主要な技術である。それには大きく分けて 2 つの課題があり、十分な検討がなされていないものは第 4 章および 5 章のディスカッションで述べた他、ここで追記する。

### 6.2.1 リスク値が適度にばらつくようにしたい

これは 4.6.1 項, 5.6.4 項, 5.7.2 項などで言及しているが, リスク値が適度にばらつくことは, 2 ステップリスク分析で重要脅威を優先的に抽出する際に重要なファクターである. リスク値の分布でどこかで一線を引いてそれ以上の値の脅威だけを先に詳細分析にかけたいという時に, リスク値が同点で固まるとうまく線を引くことができず, 結局全部分析すると労力が大して変わらなくなってしまうことになる.

図 21 や図 23 上段のヒストグラムを見ると分かるように, ISO/SAE 21434 TARA の分析手法では, 攻撃容易性や影響度の値が数箇所に固まって分布する傾向があった. これは前述のリスク値が同点で固まってしまい, 重要脅威だけふるいにかけたい時にうまく線を引くことができない状態である. それに対し RSS-CWSS\_CPS を用いた攻撃容易性と影響度の分布は滑らかで適度にばらついているので, 脅威をふるいにかける目的に適っていると言える.

### 6.2.2 分析対象をどこまで詳しく定義し評価するか

資産コンテナ方式を用いる場合, 攻撃経路と資産の組み合わせで脅威を網羅しようとするため, 粒度(抽象度)の関係でうまく適用できないメトリックがある. RSS-CWSS\_CPS で使用しなかった CWSS の IN(Level of Interaction)や ISO/SAE 21434 TARA の CVSS-based approach における UI(User Interaction)など特定のシチュエーションにのみ適用可能なメトリックがそうで, これらが細かく区別できるようにシステムをモデル化した場合, 脅威を網羅する組み合わせは “Where”, “At”, および “Asset” の組み合わせだけでは不足する.

4.6.2 項で触れた「中長期的なリスクの解釈」もそうで, これは CVSS Ver.3.1 の S(Scope)や CWSS の SC(Deployment Scope)などのメトリックで解釈する内容であるが, 現在と近未来を網羅する抽象度が不明瞭で, 組み込むのが難しい. これらはひとつの攻撃手段が明らかで, それを評価するのであれば問題なく想定できるが, これから設計しようというシステムで未知の脅威を網羅し, 限られたリソースで効率良くリスク分析を行うにはどの程度の粒度が適切なのか, という想定が難しい. 本研究において, これに関する指標を定めるのも今後の課題である.

# 謝辞

本論文は、筆者が京都産業大学大学院先端情報学研究科先端情報学専攻博士後期課程に在籍中の研究成果をまとめたものです。博士論文を提出するに当たって、多くの方にご指導、ご助力を頂き、深く感謝しております。特に、井上博之教授には指導教員として本研究の実施の機会を与えて頂き、その遂行にあたって終始、ご指導を頂きました。ここに深謝の意を表します。また、本学位論文審査の副査である秋山豊和教授ならびに林原尚浩教授には草稿をご精読頂き論文の質向上に資するたくさんのコメントを頂きました。ここに感謝の意を表します。

以上の方々をはじめとして、研究を進めるにあたり、多方面にわたり筆者を支えてくださった関係各位に、心から感謝申し上げます。特に国立研究開発法人 産業技術研究所 住友電工一産総研サイバーセキュリティ連携研究室のメンバーである吉田博隆博士、西原秀明博士、相馬大輔博士、山本秀樹氏、そして畑洋一副室長には、国際会議発表やジャーナル投稿にあたり共著者として多くの知見を与えてくださり、感謝を申し上げます。

# Acknowledgements

This paper summarizes my research results while I am enrolled in the doctoral course in the Department of Advanced Informatics, Graduate School of Advanced Informatics, Kyoto Sangyo University. I am deeply grateful to many people for their guidance and assistance in submitting my doctoral thesis. In particular, I would like to thank Professor Hiroyuki Inoue for giving me the opportunity to conduct this research as my supervisor, and for his guidance throughout the process. I would like to express my deepest gratitude. In addition, I would like to thank the assistant examiners for this dissertation, Professor Toyokazu Akiyama and Professor Naohiro Hayashibara, who carefully read the draft and provided many comments that helped improve the quality of the thesis. I would like to express my gratitude here, too.

I would like to express my sincere gratitude to all the people mentioned above and others who supported me in many ways as I carried out my research. Especially, I sincerely thank the members of the SEI-AIST Cyber Security Cooperative Research Laboratory of the National Institute of Advanced Industrial Science and Technology (AIST), Dr. Hirotaka Yoshida, Dr. Hideaki Nishihara, Dr. Daisuke Souma, Mr. Hideki Yamamoto and Mr. Youichi Hata, Deputy Director, for providing me with much knowledge as co-authors for international conference presentations and journal submissions.

## 参考文献

- [1] C. Miller and C. Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” Black Hat USA 2015, (2015).
- [2] ISO/SAE, “ISO/SAE 21434: Road vehicles - Cybersecurity engineering,” (2021).
- [3] United Nations, “UN Regulation No. 155, Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system,” (2021).
- [4] United Nations, “UN Regulation No. 156, Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system,” (2021).
- [5] M. Wood, et al., “Safety First for Automated Driving, 2019,” <https://group.mercedes-benz.com/documents/innovation/other/safety-first-for-automated-driving.pdf>, (accessed 2024-02-29), (2019).
- [6] ENISA, “Good practices for security of Smart Cars,” (2019).
- [7] U.S. Department of Transportation, “Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0,” (2020).
- [8] ISO/IEC, “ISO/IEC 15408: Information technology - Security techniques - Evaluation criteria for IT security -,” (2009).
- [9] ENISA, “Cybersecurity Certification - EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS -,” Version 1.1.1, (2021).
- [10] K. Maliatsos, C. Lyvas, P. Pantazopoulos, C. Lambrinoudakis, A. Kanatas, M. Gay, and A. Amditis, “Standardizing Security Evaluation Criteria for Connected Vehicles: A Modular Protection Profile,” 2019 IEEE Conference on Standards for Communications and Networking (CSCN), (2019).
- [11] “Nearly 20% of Lexus LX SUVs stolen in Aichi Prefecture,” The Asahi Shinbun, 2021-07-06, <https://www.asahi.com/ajw/articles/14378293/>, (accessed 2024-02-29)
- [12] Common Weakness Enumeration, “Common Weakness Scoring System (CWSS),” [https://cwe.mitre.org/cwss/cwss\\_v1.0.1.html](https://cwe.mitre.org/cwss/cwss_v1.0.1.html), (accessed 2024-02-29).
- [13] Y. Kawanishi, H. Nishihara, D. Souma, and H. Yoshida, “Detailed Analysis of Security Evaluation of Automotive Systems Based on JASO TP15002,” Dependable Smart Embedded Cyber-physical Systems and Systems-of-Systems (DECSoS), (2017).

- [14] Society of Automotive Engineers of Japan, “JASO TP15002: Guideline for Automotive Information Security Analysis,” (2015).
- [15] FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST), “Common Vulnerability Scoring System (CVSS), Common Vulnerability Scoring System v3.1: Specification Document,” <https://www.first.org/cvss/v3.1/specification-document>, (accessed 2024-02-29).
- [16] ISO/IEC, “ISO/IEC 18045:2022, Information technology — Security techniques — Methodology for IT security evaluation,” (2022).
- [17] Y. Kawanishi, H. Nishihara, D. Souma, H. Yoshida, Y. Hata, “A Comparative Study of JASO TP15002-Based Security Risk Assessment Methods for Connected Vehicle System Design,” *Security and Communication Networks*, vol. 2019, Article ID 4614721, 35 pages, (2019).
- [18] ISO, “ISO 26262: Road vehicles – Functional safety,” (2011).
- [19] IEC, “IEC 61025 Fault tree analysis (FTA),” (2006).
- [20] IEC, “IEC 60812 Analysis techniques for system reliability-Procedure for Failure modes and effects analysis (FMEA and FMECA),” (2006).
- [21] IEC, “IEC 61882 Hazard and operability studies (HAZOP Studies)-Application guide,” (2001).
- [22] C. A. Ericsson, “Hazard Analysis Techniques for System Safety,” John Wiley & Sons, (2015).
- [23] N. G. Leveson, “Engineering A Safer World: Systems Thinking Applied to Safety,” MIT Press, (2011).
- [24] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, “Introducing OCTAVE allegro: improving the information security risk assessment process,” *Tech. Rep. CMU/SEI-2007-TR-012*, (2007).
- [25] D. G. Firesmith, “Common concepts underlying safety, security, and survivability engineering,” *Tech. Rep. CMU/SEI-2003-TN-033*, Software Engineering Institute, (2003).
- [26] “Microsoft Security Development Lifecycle(SDL): Threat Modeling,” <https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling> (accessed 2024-02-29).
- [27] B. Schneier, “Attack Trees: modeling security threats,” *Dr. Dobb’s Journal*, vol. 24, no. 12, pp. 21–29, (1999).

- [28] B. Kordy, S. Mauw, S. Radomirovic, and P. Schweitzer, “Foundation of Attack-Defense Trees,” in *Proceedings of the International Workshop on Formal Aspects in Security and Trust*, Springer, (2010).
- [29] A. Roy, D. S. Kim, and K. S. Trivedi, “Attack countermeasure trees (ACT): Towards unifying the constructs of attack and defense trees,” *Security and Communication Networks*, vol. 5, no.8, pp. 929–943, (2012).
- [30] G. Sindre and A. L. Opdahl, “Eliciting security requirements with misuse cases,” *Requirements Engineering*, vol. 10, no. 1, pp.34–44, (2005).
- [31] J. P. McDermott and C. Fox, “Using abuse case models for security requirements analysis,” in *Proceedings of the 15th Annual Computer Security Applications Conference*, IEEE Computer Society, pp. 55–64, Phoenix, Ariz, USA, (1999).
- [32] T. Okubo, K. Taguchi, H. Kaiya, and N. Yoshioka, “MASG: Advanced misuse case analysis model with assets and security goals,” *Journal of Information Processing*, vol. 22, no. 3, pp. 536–546, (2014).
- [33] UK Department for Transport, “Rail Cyber Security Guidance to Industry,” (2016).
- [34] K. Netkachova and R. E. Bloomfield, “Security-Informed Safety,” *The Computer Journal*, vol. 49, no. 6, pp. 98–102, (2016).
- [35] RTCA, “DO-326A Airworthiness Security Process Specification,” (2014).
- [36] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, “A survey of approaches combining safety and security for industrial control systems,” *Reliability Engineering & System Safety*, vol. 139, pp. 156–178, (2015).
- [37] S. Kriaa, “Joint Safety and Security Modeling for Risk Assessment in Cyber Physical Systems,” *Université Paris Saclay*, (2016).
- [38] SAE, “SAE J3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,” (2016).
- [39] Y. Kawanishi, H. Nishihara, H. Yoshida, H. Yamamoto and H. Inoue, “A Study on Threat Analysis and Risk Assessment Based on the “Asset Container” Method and CWSS,” in *IEEE Access*, vol. 11, pp. 18148-18156, (2023).
- [40] ISO, “ISO 31000:2018, Risk management — Guidelines,” (2018).
- [41] FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST), “Common Vulnerability Scoring System (CVSS), Common Vulnerability Scoring System v4.0: Specification Document,” <https://www.first.org/cvss/v4.0/specification-document>, (accessed 2024-02-29).



- [42] ITU-T, “ITU-T X.1521(04/2011): Cybersecurity information exchange, Vulnerability/state exchange, Common vulnerability scoring system,” (2011).
- [43] ITU-T, “ITU-T X.1521(03/2016): Cybersecurity information exchange, Vulnerability/state exchange, Common vulnerability scoring system 3.0,” (2016).
- [44] J. Ko, S. Lee, Y. Lim, S. and Ju, T. Shon, “A Novel Network Modeling and Evaluation Approach for Security Vulnerability Quantification in Substation Automation Systems,” *IEICE Trans. Inf. & Syst.*, 2013, Vol. E96-D, Issue 9, pp. 2021-2025, (2013).
- [45] E. Ando, M. Kayashima, and N. Komoda, “A Proposal of Security Requirements Definition Methodology in Connected Car Systems by CVSS V3,” 2016 5th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI), (2016).
- [46] ITU-T, “ITU-T X.1525: Cybersecurity information exchange, Vulnerability/state exchange, Common weakness scoring system”, (2015).
- [47] Y. Kawanishi, H. Nishihara, D. Souma, H. Yoshida, and Y. Hata, “A study on quantitative risk assessment methods in security design for industrial control systems”, 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), (2018).
- [48] US Department Homeland Security (DHS), “Seven Strategies to Defend ICSs,” (2015).
- [49] K. Iehira, H. Inoue, and K. Ishida, “Spoofing attack using bus-off attacks against a specific ECU of the CAN bus,” 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), (2018).
- [50] AUTOSAR, “Specification of Secure Onboard Communication Protocol (R23-11),” (2023).
- [51] S. Checkoway et al., “Comprehensive Experimental Analyses of Automotive Attack Surfaces,” *USENIX Security Symposium* 2011, (2011).
- [52] Y. Kawanishi, H. Nishihara, H. Yoshida, and Y. Hata, “A Study of The Risk Quantification Method focusing on Direct-Access Attacks in Cyber-Physical Systems,” 2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), AB, Canada, 2021, pp. 298-305, (2021).
- [53] Y. Kawanishi, H. Nishihara, H. Yamamoto, H. Yoshida, H. Inoue, “A Study of The Risk Quantification Method of Cyber-Physical Systems focusing on Direct-Access Attacks to In-Vehicle Networks,” *IEICE Trans. Fundamentals* E106.A (3) pp.341-349, (2023).

- [54] A. D. Pinto, Y. Dragoni, and A. Carcano, "TRITON: The First ICS Cyber Attack on Safety Instrument Systems," Black Hat USA 2018, (2018).
- [55] ISA/IEC, "ISA/IEC 62443: Security for Industrial Automation and Control Systems," (2007-).
- [56] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions," IEEE Network, vol. 31, Issue 5, pp. 50–58, (2017).
- [57] M. Islam, et al., "Deliverable D2- Security Models. HEAVENS Project," Version 2.0, (2016).
- [58] D. Püllen, N. Anagnostopoulos, T. Arul and S. Katzenbeisser, "Safety Meets Security: Using IEC 62443 for a Highly Automated Road Vehicle," The 39th International Conference on Computer Safety, Reliability and Security (SafeComp 2020), (2020).
- [59] U.S. Department of Transportation, "U.S. DoT: Revised departmental guidance 2016: Treatment of the value of preventing fatalities and injuries in preparing economic analyses," (2016).

# Appendix A 重要脅威リスト (第 4 章および第 5 章の補足)

本文第 4 章および第 5 章における論点から外れるため、本編では抜粋とした脅威分析の結果をここで掲載する。

## A.1 重要脅威リスト(4.5.5 項)

表 16 および表 17 のオリジナルデータとして、全脅威 494 件中上位 70 件程度の脅威を表 A.1 ～A.4 に示す。

表 A.1: CRSS により抽出された重要脅威(1 of 2)

Table A.1: Important Threats Extracted by CRSS (1 of 2)

#	"Where"	"At"	"Asset"	AV	AC	Au	C	I	A	Rr
63	Cellular of Telematics	Telematics	Ex-Comm. Function	N	M	S	None	Complete	Complete	7.95
64	Cellular of Telematics	Telematics	Auth. Function	N	M	S	None	Complete	Complete	7.95
65	Cellular of Telematics	Telematics	Auth. Information	N	M	S	Complete	Complete	None	7.95
66	Cellular of Telematics	Telematics	Remote Service App.	N	M	S	None	Complete	Complete	7.95
68	Cellular of Telematics	Telematics	Personal Information	N	M	S	Complete	Complete	None	7.95
69	Cellular of Telematics	Telematics	Location Info / Status	N	M	S	Complete	Complete	None	7.95
109	Cellular of Infotainment	Infotainment	Auth. Function	N	M	S	None	Complete	Complete	7.95
110	Cellular of Infotainment	Infotainment	Auth. Information	N	M	S	Complete	Complete	None	7.95
112	Cellular of Infotainment	Infotainment	Navi App.	N	M	S	None	Complete	Complete	7.95
114	Cellular of Infotainment	Infotainment	Personal Information	N	M	S	Complete	Complete	None	7.95
386	LPW	Body	Control Function	A	M	N	None	Complete	Complete	7.34
387	LPW	Body	In-Comm. Function	A	M	N	None	Complete	Complete	7.34
388	LPW	Body	Ex-Comm. Function	A	M	N	None	Complete	Complete	7.34
20	DSRC	ITS	Ex-Comm. Function	A	M	S	None	Complete	Complete	6.81
21	DSRC	ITS	Auth. Function	A	M	S	None	Complete	Complete	6.81
22	DSRC	ITS	Auth. Information	A	M	S	Complete	Complete	None	6.81
24	DSRC	ITS	Personal Information	A	M	S	Complete	Complete	None	6.81
162	Bluetooth	Immobilizer	Auth. Function	A	M	S	None	Complete	Complete	6.81
163	Bluetooth	Immobilizer	Auth. Information	A	M	S	Complete	Complete	None	6.81
164	Bluetooth	Immobilizer	Ex-Comm. Function	A	M	S	None	Complete	Complete	6.81
165	Bluetooth	Immobilizer	In-Comm. Function	A	M	S	None	Complete	Complete	6.81
208	Direct-access via Ethernet	CGW	Data Processing Function	L	L	N	None	Complete	Complete	6.59
209	Direct-access via Ethernet	CGW	Diagnostic Function	L	L	N	None	Complete	Complete	6.59
210	Direct-access via Ethernet	ITS	Ex-Comm. Function	L	L	N	None	Complete	Complete	6.59
211	Direct-access via Ethernet	ITS	Auth. Function	L	L	N	None	Complete	Complete	6.59
212	Direct-access via Ethernet	ITS	Auth. Information	L	L	N	Complete	Complete	None	6.59
214	Direct-access via Ethernet	ITS	Personal Information	L	L	N	Complete	Complete	None	6.59
215	Direct-access via Ethernet	Telematics	Ex-Comm. Function	L	L	N	None	Complete	Complete	6.59
216	Direct-access via Ethernet	Telematics	Auth. Function	L	L	N	None	Complete	Complete	6.59
217	Direct-access via Ethernet	Telematics	Auth. Information	L	L	N	Complete	Complete	None	6.59
218	Direct-access via Ethernet	Telematics	Remote Service App.	L	L	N	None	Complete	Complete	6.59
220	Direct-access via Ethernet	Telematics	Personal Information	L	L	N	Complete	Complete	None	6.59
221	Direct-access via Ethernet	Telematics	Location Info / Status	L	L	N	Complete	Complete	None	6.59
223	Direct-access via Ethernet	Infotainment	Auth. Function	L	L	N	None	Complete	Complete	6.59
224	Direct-access via Ethernet	Infotainment	Auth. Information	L	L	N	Complete	Complete	None	6.59
226	Direct-access via Ethernet	Infotainment	Navi App.	L	L	N	None	Complete	Complete	6.59
228	Direct-access via Ethernet	Infotainment	Personal Information	L	L	N	Complete	Complete	None	6.59
246	Direct-access via Ethernet	CGW	Data Processing Function	L	L	N	None	Complete	Complete	6.59
247	Direct-access via Ethernet	CGW	Diagnostic Function	L	L	N	None	Complete	Complete	6.59
248	Direct-access via Ethernet	ITS	Ex-Comm. Function	L	L	N	None	Complete	Complete	6.59

表 A.2: CRSS により抽出された重要脅威(2 of 2)

Table A.2: Important Threats Extracted by CRSS (2 of 2)

#	"Where"	"At"	"Asset"	AV	AC	Au	C	I	A	Rr
249	Direct-access via Ethernet	ITS	Auth. Function	L	L	N	None	Complete	Complete	6.59
250	Direct-access via Ethernet	ITS	Auth. Information	L	L	N	Complete	Complete	None	6.59
252	Direct-access via Ethernet	ITS	Personal Information	L	L	N	Complete	Complete	None	6.59
253	Direct-access via Ethernet	Telematics	Ex-Comm. Function	L	L	N	None	Complete	Complete	6.59
254	Direct-access via Ethernet	Telematics	Auth. Function	L	L	N	None	Complete	Complete	6.59
255	Direct-access via Ethernet	Telematics	Auth. Information	L	L	N	Complete	Complete	None	6.59
256	Direct-access via Ethernet	Telematics	Remote Service App.	L	L	N	None	Complete	Complete	6.59
258	Direct-access via Ethernet	Telematics	Personal Information	L	L	N	Complete	Complete	None	6.59
259	Direct-access via Ethernet	Telematics	Location Info / Status	L	L	N	Complete	Complete	None	6.59
261	Direct-access via Ethernet	Infotainment	Auth. Function	L	L	N	None	Complete	Complete	6.59
262	Direct-access via Ethernet	Infotainment	Auth. Information	L	L	N	Complete	Complete	None	6.59
264	Direct-access via Ethernet	Infotainment	Navi App.	L	L	N	None	Complete	Complete	6.59
266	Direct-access via Ethernet	Infotainment	Personal Information	L	L	N	Complete	Complete	None	6.59
267	Direct-access via CAN Bus	PT	Control Function	L	L	N	None	Complete	Complete	6.59
268	Direct-access via CAN Bus	PT	Charging Function	L	L	N	None	Complete	Complete	6.59
270	Direct-access via CAN Bus	Chassis	Control Function	L	L	N	None	Complete	Complete	6.59
272	Direct-access via CAN Bus	Body	Control Function	L	L	N	None	Complete	Complete	6.59
273	Direct-access via CAN Bus	Body	In-Comm. Function	L	L	N	None	Complete	Complete	6.59
274	Direct-access via CAN Bus	Body	Ex-Comm. Function	L	L	N	None	Complete	Complete	6.59
276	Direct-access via CAN Bus	Immobilizer	Auth. Function	L	L	N	None	Complete	Complete	6.59
277	Direct-access via CAN Bus	Immobilizer	Auth. Information	L	L	N	Complete	Complete	None	6.59
278	Direct-access via CAN Bus	Immobilizer	Ex-Comm. Function	L	L	N	None	Complete	Complete	6.59
279	Direct-access via CAN Bus	Immobilizer	In-Comm. Function	L	L	N	None	Complete	Complete	6.59
284	Direct-access via CAN Bus	CGW	Data Processing Function	L	L	N	None	Complete	Complete	6.59
285	Direct-access via CAN Bus	CGW	Diagnostic Function	L	L	N	None	Complete	Complete	6.59
305	Direct-access via CAN Bus	PT	Control Function	L	L	N	None	Complete	Complete	6.59
306	Direct-access via CAN Bus	PT	Charging Function	L	L	N	None	Complete	Complete	6.59
308	Direct-access via CAN Bus	Chassis	Control Function	L	L	N	None	Complete	Complete	6.59
310	Direct-access via CAN Bus	Body	Control Function	L	L	N	None	Complete	Complete	6.59
311	Direct-access via CAN Bus	Body	In-Comm. Function	L	L	N	None	Complete	Complete	6.59
312	Direct-access via CAN Bus	Body	Ex-Comm. Function	L	L	N	None	Complete	Complete	6.59
314	Direct-access via CAN Bus	Immobilizer	Auth. Function	L	L	N	None	Complete	Complete	6.59
315	Direct-access via CAN Bus	Immobilizer	Auth. Information	L	L	N	Complete	Complete	None	6.59
316	Direct-access via CAN Bus	Immobilizer	Ex-Comm. Function	L	L	N	None	Complete	Complete	6.59
317	Direct-access via CAN Bus	Immobilizer	In-Comm. Function	L	L	N	None	Complete	Complete	6.59
322	Direct-access via CAN Bus	CGW	Data Processing Function	L	L	N	None	Complete	Complete	6.59
323	Direct-access via CAN Bus	CGW	Diagnostic Function	L	L	N	None	Complete	Complete	6.59

表 A.3: RSS-CWSS\_CPS により抽出された重要脅威(1 of 2)

Table A.3: Important Threats Extracted by RSS-CWSS\_CPS (1 of 2)

#	"Where"	"At"	"Asset"	TI	IC	A	AS	BI	DI	EX	EC	Rw
274	Direct-access via CAN bus	Body	Ex-Comm. Function	C	N	L	N	C	H	H	N	9.00
276	Direct-access via CAN bus	Immobilizer	Auth. Function	C	N	L	N	C	H	H	N	9.00
278	Direct-access via CAN bus	Immobilizer	Ex-Comm. Function	C	N	L	N	C	H	H	N	9.00
312	Direct-access via CAN bus	Body	Ex-Comm. Function	C	N	L	N	C	H	H	N	9.00
314	Direct-access via CAN bus	Immobilizer	Auth. Function	C	N	L	N	C	H	H	N	9.00
316	Direct-access via CAN bus	Immobilizer	Ex-Comm. Function	C	N	L	N	C	H	H	N	9.00
279	Direct-access via CAN bus	Immobilizer	In-Comm. Function	C	N	L	N	C	M	H	N	8.46
317	Direct-access via CAN bus	Immobilizer	In-Comm. Function	C	N	L	N	C	M	H	N	8.46
208	Direct-access via Ethernet	CGW	Data Processing	H	N	L	N	H	H	H	N	8.21
210	Direct-access via Ethernet	ITS	Ex-Comm. Function	H	N	L	N	H	H	H	N	8.21
212	Direct-access via Ethernet	ITS	Auth. Information	H	N	L	N	H	H	H	N	8.21
215	Direct-access via Ethernet	Telematics	Ex-Comm. Function	H	N	L	N	H	H	H	N	8.21
217	Direct-access via Ethernet	Telematics	Auth. Information	H	N	L	N	H	H	H	N	8.21
246	Direct-access via Ethernet	CGW	Data Processing	H	N	L	N	H	H	H	N	8.21
248	Direct-access via Ethernet	ITS	Ex-Comm. Function	H	N	L	N	H	H	H	N	8.21
250	Direct-access via Ethernet	ITS	Auth. Information	H	N	L	N	H	H	H	N	8.21
253	Direct-access via Ethernet	Telematics	Ex-Comm. Function	H	N	L	N	H	H	H	N	8.21
255	Direct-access via Ethernet	Telematics	Auth. Information	H	N	L	N	H	H	H	N	8.21
277	Direct-access via CAN bus	Immobilizer	Auth. Information	H	N	L	N	H	H	H	N	8.21
284	Direct-access via CAN bus	CGW	Data Processing	H	N	L	N	H	H	H	N	8.21
315	Direct-access via CAN bus	Immobilizer	Auth. Information	H	N	L	N	H	H	H	N	8.21
322	Direct-access via CAN bus	CGW	Data Processing	H	N	L	N	H	H	H	N	8.21
63	Cellular of Telematics	Telematics	Ex-Comm. Function	H	N	I	M	H	H	H	L	8.13
65	Cellular of Telematics	Telematics	Auth. Information	H	N	I	M	H	H	H	L	8.13
198	Direct-access via Ethernet	Body	Ex-Comm. Function	C	L	L	N	C	H	H	N	8.10
200	Direct-access via Ethernet	Immobilizer	Auth. Function	C	L	L	N	C	H	H	N	8.10
202	Direct-access via Ethernet	Immobilizer	Ex-Comm. Function	C	L	L	N	C	H	H	N	8.10
236	Direct-access via Ethernet	Body	Ex-Comm. Function	C	L	L	N	C	H	H	N	8.10
238	Direct-access via Ethernet	Immobilizer	Auth. Function	C	L	L	N	C	H	H	N	8.10
240	Direct-access via Ethernet	Immobilizer	Ex-Comm. Function	C	L	L	N	C	H	H	N	8.10
267	Direct-access via CAN bus	PT	Control Function	C	N	L	N	C	L	H	N	7.92
268	Direct-access via CAN bus	PT	Charging Function	C	N	L	N	C	L	H	N	7.92
270	Direct-access via CAN bus	Chassis	Control Function	C	N	L	N	C	L	H	N	7.92
305	Direct-access via CAN bus	PT	Control Function	C	N	L	N	C	L	H	N	7.92
306	Direct-access via CAN bus	PT	Charging Function	C	N	L	N	C	L	H	N	7.92
308	Direct-access via CAN bus	Chassis	Control Function	C	N	L	N	C	L	H	N	7.92
272	Direct-access via CAN bus	Body	Control Function	H	N	L	N	H	M	H	N	7.69
273	Direct-access via CAN bus	Body	In-Comm. Function	H	N	L	N	H	M	H	N	7.69
310	Direct-access via CAN bus	Body	Control Function	H	N	L	N	H	M	H	N	7.69
311	Direct-access via CAN bus	Body	In-Comm. Function	H	N	L	N	H	M	H	N	7.69

表 A.4: RSS-CWSS\_CPS により抽出された重要脅威(2 of 2)

Table A.4: Important Threats Extracted by RSS-CWSS\_CPS (2 of 2)

#	"Where"	"At"	"Asset"	TI	IC	AV	AS	BI	DI	EX	EC	Rw
203	Direct-access via Ethernet	Immobilizer	In-Comm. Function	C	L	L	N	C	M	H	N	7.61
241	Direct-access via Ethernet	Immobilizer	In-Comm. Function	C	L	L	N	C	M	H	N	7.61
360	OBD-II	CGW	Data Processing Function	H	N	L	N	H	H	H	L	7.39
201	Direct-access via Ethernet	Immobilizer	Auth. Information	H	L	L	N	H	H	H	N	7.39
239	Direct-access via Ethernet	Immobilizer	Auth. Information	H	L	L	N	H	H	H	N	7.39
286	Direct-access via CAN bus	ITS	Ex-Comm. Function	H	L	L	N	H	H	H	N	7.39
288	Direct-access via CAN bus	ITS	Auth. Information	H	L	L	N	H	H	H	N	7.39
291	Direct-access via CAN bus	Telematics	Ex-Comm. Function	H	L	L	N	H	H	H	N	7.39
293	Direct-access via CAN bus	Telematics	Auth. Information	H	L	L	N	H	H	H	N	7.39
324	Direct-access via CAN bus	ITS	Ex-Comm. Function	H	L	L	N	H	H	H	N	7.39
326	Direct-access via CAN bus	ITS	Auth. Information	H	L	L	N	H	H	H	N	7.39
329	Direct-access via CAN bus	Telematics	Ex-Comm. Function	H	L	L	N	H	H	H	N	7.39
331	Direct-access via CAN bus	Telematics	Auth. Information	H	L	L	N	H	H	H	N	7.39
56	Cellular of Telematics	CGW	Data Processing Function	H	L	I	M	H	H	H	L	7.31
94	Cellular of Infotainment	CGW	Data Processing Function	H	L	I	M	H	H	H	L	7.31
350	OBD-II	Body	Ex-Comm. Function	C	L	L	N	C	H	H	L	7.29
352	OBD-II	Immobilizer	Auth. Function	C	L	L	N	C	H	H	L	7.29
354	OBD-II	Immobilizer	Ex-Comm. Function	C	L	L	N	C	H	H	L	7.29
211	Direct-access via Ethernet	ITS	Auth. Function	M	N	L	N	H	H	H	N	7.18
224	Direct-access via Ethernet	Infotainment	Auth. Information	M	N	L	N	H	H	H	N	7.18
249	Direct-access via Ethernet	ITS	Auth. Function	M	N	L	N	H	H	H	N	7.18
262	Direct-access via Ethernet	Infotainment	Auth. Information	M	N	L	N	H	H	H	N	7.18
269	Direct-access via CAN bus	PT	In-Comm. Function	H	N	L	N	H	L	H	N	7.17
307	Direct-access via CAN bus	PT	In-Comm. Function	H	N	L	N	H	L	H	N	7.17
191	Direct-access via Ethernet	PT	Control Function	C	L	L	N	C	L	H	N	7.13
192	Direct-access via Ethernet	PT	Charging Function	C	L	L	N	C	L	H	N	7.13
194	Direct-access via Ethernet	Chassis	Control Function	C	L	L	N	C	L	H	N	7.13
229	Direct-access via Ethernet	PT	Control Function	C	L	L	N	C	L	H	N	7.13
230	Direct-access via Ethernet	PT	Charging Function	C	L	L	N	C	L	H	N	7.13
232	Direct-access via Ethernet	Chassis	Control Function	C	L	L	N	C	L	H	N	7.13
110	Cellular of Infotainment	Infotainment	Auth. Information	M	N	I	M	H	H	H	L	7.11
388	LPW	Body	Ex-Comm. Function	C	N	A	N	C	H	L	L	7.11
162	Bluetooth	Immobilizer	Auth. Function	C	N	A	M	C	H	L	L	7.03
164	Bluetooth	Immobilizer	Ex-Comm. Function	C	N	A	M	C	H	L	L	7.03

## A.2 重要脅威リスト(5.6.5 項)

表 36 のオリジナルデータ, および ISO/SAE 21434 TARA CVSS-based approach の分析結果として, 全脅威 456 件中上位 80 件程度の脅威を表 A.5～A.8 に示す.

**表 A.5: RSS-CWSS\_CPS により抽出された重要脅威(1 of 2)**

**Table A.5: Important Threats Extracted by RSS-CWSS\_CPS (1 of 2)**

#	"Where"	"At"	"Asset"	IC	AV	AS	EX	EC	DI	TI	BI	Rw
274	Direct-access via CAN Bus	Body	Ex-Comm. Function	1.0	0.5	1.0	1.0	1.0	1.0	1.0	1.0	9.00
276	Direct-access via CAN Bus	Immobilizer	Authentication Function	1.0	0.5	1.0	1.0	1.0	1.0	1.0	1.0	9.00
278	Direct-access via CAN Bus	Immobilizer	Ex-Comm. Function	1.0	0.5	1.0	1.0	1.0	1.0	1.0	1.0	9.00
279	Direct-access via CAN Bus	Immobilizer	In-Comm. Function	1.0	0.5	1.0	1.0	1.0	0.6	1.0	1.0	8.46
101	GPS	Telematics	Ex-Comm. Function	1.0	1.0	1.0	1.0	0.9	1.0	0.9	0.9	8.21
103	GPS	Telematics	Authentication Information	1.0	1.0	1.0	1.0	0.9	1.0	0.9	0.9	8.21
246	Direct-access via Ethernet	CGW	Data Processing Function	1.0	0.5	1.0	1.0	1.0	1.0	0.9	0.9	8.21
248	Direct-access via Ethernet	ITS	Ex-Comm. Function	1.0	0.5	1.0	1.0	1.0	1.0	0.9	0.9	8.21
250	Direct-access via Ethernet	ITS	Authentication Information	1.0	0.5	1.0	1.0	1.0	1.0	0.9	0.9	8.21
253	Direct-access via Ethernet	Telematics	Ex-Comm. Function	1.0	0.5	1.0	1.0	1.0	1.0	0.9	0.9	8.21
255	Direct-access via Ethernet	Telematics	Authentication Information	1.0	0.5	1.0	1.0	1.0	1.0	0.9	0.9	8.21
277	Direct-access via CAN Bus	Immobilizer	Authentication Information	1.0	0.5	1.0	1.0	1.0	1.0	0.9	0.9	8.21
284	Direct-access via CAN Bus	CGW	Data Processing Function	1.0	0.5	1.0	1.0	1.0	1.0	0.9	0.9	8.21
63	Cellular of Telematics	Telematics	Ex-Comm. Function	1.0	1.0	0.8	1.0	0.9	1.0	0.9	0.9	8.13
65	Cellular of Telematics	Telematics	Authentication Information	1.0	1.0	0.8	1.0	0.9	1.0	0.9	0.9	8.13
236	Direct-access via Ethernet	Body	Ex-Comm. Function	0.9	0.5	1.0	1.0	1.0	1.0	1.0	1.0	8.10
238	Direct-access via Ethernet	Immobilizer	Authentication Function	0.9	0.5	1.0	1.0	1.0	1.0	1.0	1.0	8.10
240	Direct-access via Ethernet	Immobilizer	Ex-Comm. Function	0.9	0.5	1.0	1.0	1.0	1.0	1.0	1.0	8.10
267	Direct-access via CAN Bus	PT	Control Function	1.0	0.5	1.0	1.0	1.0	0.2	1.0	1.0	7.92
268	Direct-access via CAN Bus	PT	Charging Function	1.0	0.5	1.0	1.0	1.0	0.2	1.0	1.0	7.92
270	Direct-access via CAN Bus	Chassis	Control Function	1.0	0.5	1.0	1.0	1.0	0.2	1.0	1.0	7.92
272	Direct-access via CAN Bus	Body	Control Function	1.0	0.5	1.0	1.0	1.0	0.6	0.9	0.9	7.69
273	Direct-access via CAN Bus	Body	In-Comm. Function	1.0	0.5	1.0	1.0	1.0	0.6	0.9	0.9	7.69
241	Direct-access via Ethernet	Immobilizer	In-Comm. Function	0.9	0.5	1.0	1.0	1.0	0.6	1.0	1.0	7.61
94	GPS	CGW	Data Processing Function	0.9	1.0	1.0	1.0	0.9	1.0	0.9	0.9	7.39
322	OBD-II	CGW	Data Processing Function	1.0	0.5	1.0	1.0	0.9	1.0	0.9	0.9	7.39
239	Direct-access via Ethernet	Immobilizer	Authentication Information	0.9	0.5	1.0	1.0	1.0	1.0	0.9	0.9	7.39
286	Direct-access via CAN Bus	ITS	Ex-Comm. Function	0.9	0.5	1.0	1.0	1.0	1.0	0.9	0.9	7.39
288	Direct-access via CAN Bus	ITS	Authentication Information	0.9	0.5	1.0	1.0	1.0	1.0	0.9	0.9	7.39
291	Direct-access via CAN Bus	Telematics	Ex-Comm. Function	0.9	0.5	1.0	1.0	1.0	1.0	0.9	0.9	7.39
293	Direct-access via CAN Bus	Telematics	Authentication Information	0.9	0.5	1.0	1.0	1.0	1.0	0.9	0.9	7.39
56	Cellular of Telematics	CGW	Data Processing Function	0.9	1.0	0.8	1.0	0.9	1.0	0.9	0.9	7.31
132	Cellular of Infotainment	CGW	Data Processing Function	0.9	1.0	0.8	1.0	0.9	1.0	0.9	0.9	7.31
312	OBD-II	Body	Ex-Comm. Function	0.9	0.5	1.0	1.0	0.9	1.0	1.0	1.0	7.29
314	OBD-II	Immobilizer	Authentication Function	0.9	0.5	1.0	1.0	0.9	1.0	1.0	1.0	7.29
316	OBD-II	Immobilizer	Ex-Comm. Function	0.9	0.5	1.0	1.0	0.9	1.0	1.0	1.0	7.29
249	Direct-access via Ethernet	ITS	Authentication Function	1.0	0.5	1.0	1.0	1.0	1.0	0.6	0.9	7.18
262	Direct-access via Ethernet	Infotainment	Authentication Information	1.0	0.5	1.0	1.0	1.0	1.0	0.6	0.9	7.18
269	Direct-access via CAN Bus	PT	In-Comm. Function	1.0	0.5	1.0	1.0	1.0	0.2	0.9	0.9	7.17
229	Direct-access via Ethernet	PT	Control Function	0.9	0.5	1.0	1.0	1.0	0.2	1.0	1.0	7.13



表 A.6: RSS-CWSS\_CPS により抽出された重要脅威(2 of 2)

Table A.6: Important Threats Extracted by RSS-CWSS\_CPS (2 of 2)

#	"Where"	"At"	"Asset"	IC	AV	AS	EX	EC	DI	TI	BI	Rw
230	Direct-access via Ethernet	PT	Charging Function	0.9	0.5	1.0	1.0	1.0	0.2	1.0	1.0	7.13
232	Direct-access via Ethernet	Chassis	Control Function	0.9	0.5	1.0	1.0	1.0	0.2	1.0	1.0	7.13
148	Cellular of Infotainment	Infotainment	Authentication Information	1.0	1.0	0.8	1.0	0.9	1.0	0.6	0.9	7.11
350	LPW	Body	Ex-Comm. Function	1.0	0.7	1.0	0.2	0.9	1.0	1.0	1.0	7.11
200	Bluetooth	Immobilizer	Authentication Function	1.0	0.7	0.8	0.2	0.9	1.0	1.0	1.0	7.03
202	Bluetooth	Immobilizer	Ex-Comm. Function	1.0	0.7	0.8	0.2	0.9	1.0	1.0	1.0	7.03
20	DSRC	ITS	Ex-Comm. Function	1.0	0.7	0.8	0.6	0.9	1.0	0.9	0.9	6.99
22	DSRC	ITS	Authentication Information	1.0	0.7	0.8	0.6	0.9	1.0	0.9	0.9	6.99
234	Direct-access via Ethernet	Body	Control Function	0.9	0.5	1.0	1.0	1.0	0.6	0.9	0.9	6.92
235	Direct-access via Ethernet	Body	In-Comm. Function	0.9	0.5	1.0	1.0	1.0	0.6	0.9	0.9	6.92
275	Direct-access via CAN Bus	Body	Sensor Information	1.0	0.5	1.0	1.0	1.0	1.0	0.9	0.6	6.91
282	Direct-access via CAN Bus	ADAS	Sensor Function	1.0	0.5	1.0	1.0	1.0	1.0	0.9	0.6	6.91
283	Direct-access via CAN Bus	ADAS	Sensor Information	1.0	0.5	1.0	1.0	1.0	1.0	0.9	0.6	6.91
317	OBD-II	Immobilizer	In-Comm. Function	0.9	0.5	1.0	1.0	0.9	0.6	1.0	1.0	6.85
315	OBD-II	Immobilizer	Authentication Information	0.9	0.5	1.0	1.0	0.9	1.0	0.9	0.9	6.65
324	OBD-II	ITS	Ex-Comm. Function	0.9	0.5	1.0	1.0	0.9	1.0	0.9	0.9	6.65
326	OBD-II	ITS	Authentication Information	0.9	0.5	1.0	1.0	0.9	1.0	0.9	0.9	6.65
329	OBD-II	Telematics	Ex-Comm. Function	0.9	0.5	1.0	1.0	0.9	1.0	0.9	0.9	6.65
331	OBD-II	Telematics	Authentication Information	0.9	0.5	1.0	1.0	0.9	1.0	0.9	0.9	6.65
203	Bluetooth	Immobilizer	In-Comm. Function	1.0	0.7	0.8	0.2	0.9	0.6	1.0	1.0	6.53
106	GPS	Telematics	Personal Information	1.0	1.0	1.0	1.0	0.9	1.0	0.3	1.0	6.48
252	Direct-access via Ethernet	ITS	Personal Information	1.0	0.5	1.0	1.0	1.0	1.0	0.3	1.0	6.48
258	Direct-access via Ethernet	Telematics	Personal Information	1.0	0.5	1.0	1.0	1.0	1.0	0.3	1.0	6.48
266	Direct-access via Ethernet	Infotainment	Personal Information	1.0	0.5	1.0	1.0	1.0	1.0	0.3	1.0	6.48
287	Direct-access via CAN Bus	ITS	Authentication Function	0.9	0.5	1.0	1.0	1.0	1.0	0.6	0.9	6.46
300	Direct-access via CAN Bus	Infotainment	Authentication Information	0.9	0.5	1.0	1.0	1.0	1.0	0.6	0.9	6.46
231	Direct-access via Ethernet	PT	In-Comm. Function	0.9	0.5	1.0	1.0	1.0	0.2	0.9	0.9	6.45
68	Cellular of Telematics	Telematics	Personal Information	1.0	1.0	0.8	1.0	0.9	1.0	0.3	1.0	6.42
152	Cellular of Infotainment	Infotainment	Personal Information	1.0	1.0	0.8	1.0	0.9	1.0	0.3	1.0	6.42
305	OBD-II	PT	Control Function	0.9	0.5	1.0	1.0	0.9	0.2	1.0	1.0	6.42
306	OBD-II	PT	Charging Function	0.9	0.5	1.0	1.0	0.9	0.2	1.0	1.0	6.42
308	OBD-II	Chassis	Control Function	0.9	0.5	1.0	1.0	0.9	0.2	1.0	1.0	6.42
201	Bluetooth	Immobilizer	Authentication Information	1.0	0.7	0.8	0.2	0.9	1.0	0.9	0.9	6.35
18	DSRC	CGW	Data Processing Function	0.9	0.7	0.8	0.6	0.9	1.0	0.9	0.9	6.29
310	OBD-II	Body	Control Function	0.9	0.5	1.0	1.0	0.9	0.6	0.9	0.9	6.23
311	OBD-II	Body	In-Comm. Function	0.9	0.5	1.0	1.0	0.9	0.6	0.9	0.9	6.23
237	Direct-access via Ethernet	Body	Sensor Information	0.9	0.5	1.0	1.0	1.0	1.0	0.9	0.6	6.22
244	Direct-access via Ethernet	ADAS	Sensor Function	0.9	0.5	1.0	1.0	1.0	1.0	0.9	0.6	6.22
245	Direct-access via Ethernet	ADAS	Sensor Information	0.9	0.5	1.0	1.0	1.0	1.0	0.9	0.6	6.22
21	DSRC	ITS	Authentication Function	1.0	0.7	0.8	0.6	0.9	1.0	0.6	0.9	6.12

表 A.7: ISO/SAE 21434 TARA CVSS-based approach により  
抽出された重要脅威(1 of 2)

Table A.7: Important Threats Extracted  
by ISO/SAE 21434 TARA CVSS-based approach (1 of 2)

#	"Where"	"At"	"Asset"	Impact	Attack Feasibility	Risk Value
101	GPS	Telematics	Ex-Comm. Function	Severe	High	5
102	GPS	Telematics	Authentication Function	Severe	High	5
103	GPS	Telematics	Authentication Information	Severe	High	5
104	GPS	Telematics	Remote Service App.	Severe	High	5
105	GPS	Telematics	In-Comm. Function	Severe	High	5
106	GPS	Telematics	Personal Information	Severe	High	5
20	DSRC	ITS	Ex-Comm. Function	Severe	Medium	4
21	DSRC	ITS	Authentication Function	Severe	Medium	4
23	DSRC	ITS	In-Comm. Function	Severe	Medium	4
63	Cellular of Telematics	Telematics	Ex-Comm. Function	Severe	Medium	4
64	Cellular of Telematics	Telematics	Authentication Function	Severe	Medium	4
65	Cellular of Telematics	Telematics	Authentication Information	Severe	Medium	4
66	Cellular of Telematics	Telematics	Remote Service App.	Severe	Medium	4
67	Cellular of Telematics	Telematics	In-Comm. Function	Severe	Medium	4
68	Cellular of Telematics	Telematics	Personal Information	Severe	Medium	4
77	GPS	PT	Control Function	Severe	Medium	4
78	GPS	PT	Charging Function	Severe	Medium	4
79	GPS	PT	In-Comm. Function	Severe	Medium	4
80	GPS	Chassis	Control Function	Severe	Medium	4
81	GPS	Chassis	In-Comm. Function	Severe	Medium	4
83	GPS	Body	In-Comm. Function	Severe	Medium	4
84	GPS	Body	Ex-Comm. Function	Severe	Medium	4
85	GPS	Body	Sensor Information	Severe	Medium	4
86	GPS	Immobilizer	Authentication Function	Severe	Medium	4
88	GPS	Immobilizer	Ex-Comm. Function	Severe	Medium	4
89	GPS	Immobilizer	In-Comm. Function	Severe	Medium	4
90	GPS	ADAS	Control Function	Severe	Medium	4
91	GPS	ADAS	In-Comm. Function	Severe	Medium	4
92	GPS	ADAS	Sensor Function	Severe	Medium	4
93	GPS	ADAS	Sensor Information	Severe	Medium	4
94	GPS	CGW	Data Processing Function	Severe	Medium	4
96	GPS	ITS	Ex-Comm. Function	Severe	Medium	4
97	GPS	ITS	Authentication Function	Severe	Medium	4
99	GPS	ITS	In-Comm. Function	Severe	Medium	4
107	GPS	Telematics	Location Info. / Status	Major	High	4
111	GPS	Infotainment	In-Comm. Function	Severe	Medium	4
112	GPS	Infotainment	Navi App.	Severe	Medium	4
113	GPS	Infotainment	Entertainment App.	Severe	Medium	4
149	Cellular of Infotainment	Infotainment	In-Comm. Function	Severe	Medium	4
150	Cellular of Infotainment	Infotainment	Navi App.	Severe	Medium	4
151	Cellular of Infotainment	Infotainment	Entertainment App.	Severe	Medium	4
200	Bluetooth	Immobilizer	Authentication Function	Severe	Medium	4

表 A.8: ISO/SAE 21434 TARA CVSS-based approach により  
抽出された重要脅威(2 of 2)

Table A.8: Important Threats Extracted  
by ISO/SAE 21434 TARA CVSS-based approach (2 of 2)

#	"Where"	"At"	"Asset"	Impact	Attack Feasibility	Risk Value
101	GPS	Telematics	Ex-Comm. Function	Severe	High	5
102	GPS	Telematics	Authentication Function	Severe	High	5
103	GPS	Telematics	Authentication Information	Severe	High	5
104	GPS	Telematics	Remote Service App.	Severe	High	5
105	GPS	Telematics	In-Comm. Function	Severe	High	5
106	GPS	Telematics	Personal Information	Severe	High	5
20	DSRC	ITS	Ex-Comm. Function	Severe	Medium	4
21	DSRC	ITS	Authentication Function	Severe	Medium	4
23	DSRC	ITS	In-Comm. Function	Severe	Medium	4
63	Cellular of Telematics	Telematics	Ex-Comm. Function	Severe	Medium	4
64	Cellular of Telematics	Telematics	Authentication Function	Severe	Medium	4
65	Cellular of Telematics	Telematics	Authentication Information	Severe	Medium	4
66	Cellular of Telematics	Telematics	Remote Service App.	Severe	Medium	4
67	Cellular of Telematics	Telematics	In-Comm. Function	Severe	Medium	4
68	Cellular of Telematics	Telematics	Personal Information	Severe	Medium	4
77	GPS	PT	Control Function	Severe	Medium	4
78	GPS	PT	Charging Function	Severe	Medium	4
79	GPS	PT	In-Comm. Function	Severe	Medium	4
80	GPS	Chassis	Control Function	Severe	Medium	4
81	GPS	Chassis	In-Comm. Function	Severe	Medium	4
83	GPS	Body	In-Comm. Function	Severe	Medium	4
84	GPS	Body	Ex-Comm. Function	Severe	Medium	4
85	GPS	Body	Sensor Information	Severe	Medium	4
86	GPS	Immobilizer	Authentication Function	Severe	Medium	4
88	GPS	Immobilizer	Ex-Comm. Function	Severe	Medium	4
89	GPS	Immobilizer	In-Comm. Function	Severe	Medium	4
90	GPS	ADAS	Control Function	Severe	Medium	4
91	GPS	ADAS	In-Comm. Function	Severe	Medium	4
92	GPS	ADAS	Sensor Function	Severe	Medium	4
93	GPS	ADAS	Sensor Information	Severe	Medium	4
94	GPS	CGW	Data Processing Function	Severe	Medium	4
96	GPS	ITS	Ex-Comm. Function	Severe	Medium	4
97	GPS	ITS	Authentication Function	Severe	Medium	4
99	GPS	ITS	In-Comm. Function	Severe	Medium	4
107	GPS	Telematics	Location Info. / Status	Major	High	4
111	GPS	Infotainment	In-Comm. Function	Severe	Medium	4
112	GPS	Infotainment	Navi App.	Severe	Medium	4
113	GPS	Infotainment	Entertainment App.	Severe	Medium	4
149	Cellular of Infotainment	Infotainment	In-Comm. Function	Severe	Medium	4
150	Cellular of Infotainment	Infotainment	Navi App.	Severe	Medium	4
151	Cellular of Infotainment	Infotainment	Entertainment App.	Severe	Medium	4
200	Bluetooth	Immobilizer	Authentication Function	Severe	Medium	4

# 著者研究業績

## 学術論文誌

- (1) 文献[53] Y. Kawanishi, H. Nishihara, H. Yamamoto, H. Yoshida, H. Inoue, “A Study of The Risk Quantification Method of Cyber-Physical Systems focusing on Direct-Access Attacks to In-Vehicle Networks,” IEICE Trans. Fundamentals E106.A (3) pp.341-349, (2023).
- (2) 文献[39] Y. Kawanishi, H. Nishihara, H. Yoshida, H. Yamamoto and H. Inoue, “A Study on Threat Analysis and Risk Assessment Based on the “Asset Container” Method and CWSS,” in IEEE Access, vol. 11, pp. 18148-18156, (2023).

## 国際会議(査読あり)

- (1) 文献[52] Y. Kawanishi, H. Nishihara, H. Yoshida and Y. Hata, “A Study of The Risk Quantification Method focusing on Direct-Access Attacks in Cyber-Physical Systems,” 2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCCom/CyberSciTech), AB, Canada, 2021, pp. 298-305, (2021).

## 国内会議(査読なし)

- (1) 川西 康之, 西原 秀明, 吉田 博隆, 山本 秀樹, 井上 博之, “ネットワークレイヤと物理的構成を考慮したソフトウェア定義型自動車を構成するゾーンアーキテクチャのリスク分析,” 2024 年暗号と情報セキュリティシンポジウム(SCIS2024), (2024).

# 図目次

図 1: 製品開発における開発 V 字モデル	2
図 2: セキュリティ設計の製品開発における役割とその手順	3
図 3: 脅威の定式化とリスクの数値化	4
図 4: セキュリティ設計プロセス各要素の論理的関係	8
図 5: SAE J3061 で定めたセーフティとセキュリティの関係	10
図 6: ISO/SAE 21434 のブロックダイアグラム	12, 73
図 7: ISO/SAE 21434 と JASO TP15002 との手順比較	14
図 8: CAN インバーダーによる自動車盗難の手口	25
図 9: アイデア: 資産コンテナ方式による脅威の捉え方	28
図 10: コネクテッドカーの分析対象モデル	30
図 11: データロガーの分析対象モデル	37
図 12: ドローンの分析対象モデル	38
図 13: RSS-CWSS と CRSS のリスク値分布の比較	41
図 14: 資産コンテナ方式における RSS-CWSS_CPS 各メトリックの評価箇所	52
図 15: 分析対象システムとしての自動車システムのシステム構成	55
図 16: ケーススタディにおける 2 つの脅威の比較	65
図 17: 影響度スコアのヒストグラムの比較	69
図 18: 脅威シナリオとダメージシナリオの関係	73
図 19: RSS-CWSS_CPS メトリックと資産コンテナ方式	79
図 20: 分析対象システムとしての自動車システムのシステム構成(2)	81
図 21: 攻撃容易性のヒストグラム比較	87

図 22: HEAVENS security model におけるインパクトレベルとパラメータの考え方	94
図 21: 資産が損害を受けることでの影響度のヒストグラム比較	95

# 表目次

表 1: CVSS Ver.2 のメトリックとランク	15
表 2: CVSS Ver.3 および Ver.3.1 のメトリックとランク	17
表 3: CWSS のメトリックとランク	21
表 4: 機能モジュールおよび資産のリスト	32
表 5: 資産コンテナ方式に基づく脅威の記述	34
表 6: 資産コンテナ方式に CVSS を適用した例	35
表 7: RSS-CWSS で採用した CWSS のメトリック	40
表 8: RSS-CWSS_CPS で採用した CWSS のメトリック	49
表 9 RSS-CWSS_CPS でダイレクトアクセスの評価に用いられる CWSS メトリック	53
表 10: 機能モジュールおよび資産のリスト	57
表 11: 資産に対する TI, BI, および DI のランク	59
表 12: 攻撃経路に対する IC, AV, AS, および EX のランク(1 of 2)	60
表 13: 攻撃経路に対する IC, AV, AS, および EX のランク(2 of 2)	61
表 14: エントリーポイントに対する EC のランク	61
表 15: 攻撃容易性に関連するメトリックが 0.1 変動した場合のリスク値の変化量	62
表 16: CRSS により抽出された重要脅威(抜粋)	64
表 17: RSS-CWSS_CPS により抽出された重要脅威(抜粋)	64
表 18: 2 つの脅威のリスク値の比較(RSS-CWSS_CPS & CRSS)	65
表 19: エントリーポイントの優先度の比較	68
表 20: Table G.8 — CVSS exploitability mapping の例	76
表 21: Table F.1 — Safety の影響度の例	76

表 22: 表 22: Table F.2 — Financial の影響度の例	76
表 23: 表 23: Table F.3 — Operational の影響度の例	77
表 24: Table F.4 — Privacy の影響度の例	77
表 25: Table H.8 — Risk matrix の例	78
表 26: TARA で使用する CWSS メトリック	80
表 27: 資産に対する TI, BI の値および S, F, O, P の観点	83
表 28: 脅威シナリオのリスト (抜粋)	84
表 29: 攻撃経路に対する IC, AV, AS, EX, および EC のランク(1 of 2)	85
表 30: 攻撃経路に対する IC, AV, AS, EX, および EC のランク(2 of 2)	86
表 31: 資産に対する DI のランク	86
表 32: 攻撃経路に対する CVSS Ver.3.1 の攻撃容易性分析(1 of 4)	88
表 33: 攻撃経路に対する CVSS Ver.3.1 の攻撃容易性分析 (2 of 4)	88
表 34: 攻撃経路に対する CVSS Ver.3.1 の攻撃容易性分析(3 of 4)	89
表 35: 攻撃経路に対する CVSS Ver.3.1 の攻撃容易性分析 (4 of 4)	89
表 36: 脅威シナリオとリスク値 (抜粋)	91
表 37: エントリーポイントの優先度の比較	92
表 38: 攻撃容易性に関連するメトリックが 0.1 変動した場合のリスク値変化量	93
表 39: 各観点・メトリックの関連性	93
表 A.1: CRSS により抽出された重要脅威(1 of 2)	107
表 A.2: CRSS により抽出された重要脅威(2 of 2)	108
表 A.3: RSS-CWSS_CPS により抽出された重要脅威(1 of 2)	109
表 A.4: RSS-CWSS_CPS により抽出された重要脅威(2 of 2)	110
表 A.5: RSS-CWSS_CPS により抽出された重要脅威(1 of 2)	111
表 A.6: RSS-CWSS_CPS により抽出された重要脅威(2 of 2)	112



表 A.7: ISO/SAE 21434 TARA CVSS-based approach により抽出された重要脅威(1 of 2)

113

表 A.8: ISO/SAE 21434 TARA CVSS-based approach により抽出された重要脅威(2 of 2)

114