博士学位論文

内容の要旨及び審査結果の要旨

第 54 号

2024 年 9 月

京　都　産　業　大　学

はしがき

本号は，学位規則（昭和 28 年４月１日文部省令第９号）第８条の規定による公表を目的とし，令６年３月 16 日 17 日に本学において博士の学位を授与した者の論文内容の要旨及び論文審査結果の要旨を収録したものである。

学位番号に付した甲は学位規則第４条第１項によるもの（いわゆる課程博士）であり，乙は同条第２項によるもの（いわゆる論文博士）である。

目　　次

課程博士

氏名（本籍）	川西　康之（兵庫県）
学位の種類	博士（先端情報学）
学位記番号	甲先　第６号
学位授与年月日	令和６年９月 21 日
学位授与の要件	学位規則第４条第１項該当
論文題目	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
論文審査委員	主　査　井上　博之　教授
	副　査　秋山　豊和　教授
	〃　林原　尚浩　教授

論文内容の要旨

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 チェロキー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 インベ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元に、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、より実際的なものとなっている。

さて、セキュリティ設計におけるリスク分析についての課題は 4 つあり、(1) 時間・コスト・リソース総量の節約、(2) 時間やコストの面でネックとなるセキュリティ専門家の判断に依存し過ぎない分析手法の実現、(3) 脅威抽出における網羅性の担保、および(4) 分析対象のシステムの実情に沿った適切な分析、である。セキュリティ設計を開発者が主体的に進められ、分析の抜け漏れを防ぎつつ効率良く実施でき、かつ分析対象の実情に沿ったリスク分析が求められる。

本研究ではリスク分析手法に着目し、上記 4 つの課題を解決できるリスク数値化手順を研究してきた。まず課題(3)の解決には、脅威を攻撃の入り口、目的地、および資産の組合せでリストアップすることで網羅性を担保する「資産コンテナ方式」を考案した。次に課題(1)(2)の解決には、資産コンテナ方式により詳細な分析が必要な重要脅威だけふるいにかける「2 ステップリスク分析」を提案した。そして、課題(4)の解決には、「資産コンテナ方式」と「2 ステップリスク分析」に適し、かつ自動車システム特有の領域や観点に沿って、より精密な差別化が可能なリスク数値化手法の研究を行った。

本論文で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)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提案手法、「RSS-CWSS_CPS」における研究をまとめた。そしてリスク数値化手法「RSS-CWSS_CPS」がサイバーフィジカルシステムにおける脅威を検知する際にどういった観点を重視しているか、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を行った。最後にケーススタディを踏まえ、CAN インベ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実情に沿った分析結果が出せることが確認できた。

論文審査結果の要旨

本博士学位論文は、自動車システムにおけるサイバーフィジカルシステムのセキュリティ設計におけるリスク分析についての課題の整理と、それらの解決のための手法を提案し、そして実際の攻撃に適用し評価を行っている。まず脅威を攻撃の入り口、目的地、および資産の組合せでリストアップすることで網羅性を担保する資産コンテナ方式を考案し、次に資産コンテナ方式により詳細な分析が必要な重要脅威だけふるいにかける 2 ステップリスク分析を提案している。そして、資産コンテナ方式と 2 ステップリスク分析に適し、かつ自動車システム特有の領域や観点に沿って、より精密な差別化が可能なリスク数値化手法の研究を行うことで、CWSS 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提案手法 RSS-CWSS_CPS における研究をまとめている。そしてリスク数値化手法 RSS-CWSS_CPS がサイバーフィジカルシステムにおける脅威を検知する際にどういった観点を重視しているかについて、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を行っている。また、近年問題になっている CAN インベ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適用することで本攻撃も

重要脅威として抽出されることを確認し、提案したリスク数値化手法の有効性を明らかにしている。以上より、本博士学位論文は学術的かつ社会的に有用で価値ある研究である。

本提案手法による具体的成果は次の 3 点に集約される。1 点目は、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 RSS-CWSS_CPS を考案したことである。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、分析対処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という利点を持つ。2 点目は、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ことである。CRSS と RSS-CWSS_CPS の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。3 点目は、ケーススタディで得られたデータを元に、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の違いや、実際の数値のばらつきを評価したことである。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 との関連性についても触れ、メトリック TI と BI を用いることにより影響度の評価をより細かく行えるなど、資産コンテナ方式に基づいた功率の良いリスク分析手法を行える可能性についても言及している。

以上の本博士学位論文にもとづき、2024 年 7 月 12 日にオンラインで副査の秋山教授と林原教授による予備調査会を実施した。その後、予備調査会で頂いた複数の指摘事項に基づき博士学位論を修正し、2024 年 8 月 7 日(水)3 限に 15 号館 15102 セミナー室で先端情報学研究科博士学位論文公聴会を実施した。公聴会の参加者からの提案手法および評価結果に対する活発な質疑応答を通して、先端情報学分野における当該研究の新規性および有用性がより明確になり、今後の研究の発展性も検討できた。また、審査として提出された学術成果より、本研究の主な学術成果としては、電子情報通信学会の英文論文誌 A および IEEE Access での計 2 本のジャーナル論文採択であり、専門分野の査読者における国際的な客観的評価がなされており学術成果は十分といえる。なお、研究科が定める学位審査基準「本審査を開始するまでに、学術雑誌、又は国際会議で査読付き研究論文を２報以上発表」を満たしている。

以上、先端情報学研究科博士学位論文公聴会および学外専門分野研究者の査読による学術成果を踏まえ、博士学位論文として十分な内容を有すると判断し、審査委員全員の一致で本博士学位論文調査結果は合格と判定する。