SCIS 2022 2022 Symposium on Cryptography and Information Security
On-line, Jan. 18 – 21, 2022
The Institute of Electronics, Information and Communication Engineers

サイバーフィジカルシステムの効率の良いセキュリティ設計のための リスク分析手順の検討

Examinations of risk analysis procedures for efficient security design of cyber-physical systems

川西 康之*† 西原 秀明† 吉田 博隆† 山本 秀樹*†
Yasuyuki Kawanishi Hideaki Nishihara Hirotaka Yoshida Hideki Yamamoto

あらまし ICT システムと物理世界に影響を及ぼすデバイスが相互接続され連動する，サイバーフィジカルシステムが世の中に普及するようになった．このシステムには，ICT システムへの攻撃が波及させる物理的な影響，物理面でのセキュリティの弱さなど，より多くのリスクを想定したセキュリティ設計が必須である．我々は自動車業界のガイドライン JASO TP15002 をベースに，サイバーフィジカルシステムのセキュリティ設計手順の効率化を進めてきた．特に自動車分野においてはダイレクトアクセス攻撃の分析を進め， ICT システムの脆弱性評価基準である CWSS がベースの，サイバーフィジカルシステムの物理的な境界を解釈した新しいリスク数値化手法を提案した．本稿では，我々の DECSoS2017 会議論文，CyberSciTech2018 会議論文，CyberSciTech2021 会議論文等で発表した，セキュリティ設計手順において我々の検討してきた課題，および加えた観点についてまとめ報告する．

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，TP15002，CWSS

1 本論文の課題

我々は自動車業界のガイドライン JASO TP15002 をベースに，ガイドラインで書かれていない部分を埋める，効率の良いセキュリティ設計手順を研究してきた．以下の 4 つがセキュリティ設計において，解決しなければならない課題である．

- **脅威の網羅性担保**
- **作業の属人化解消**
- **時間，コスト，リソース使用の最適化**
- **特定の領域や観点へのフィッティング**

2 課題の解決手法

まず，脅威を網羅的に抽出する手法として，攻撃を受ける側が把握できる資産と攻撃可能性のみで脅威を記述する，「資産コンテナ方式」という手法を考案した．

次に，脅威のリスクを数値化しふるいにかけるプロセスを入れた 2 ステップリスク分析手法(図 1)を考案し，属人化解消とコストの節約を実現した．

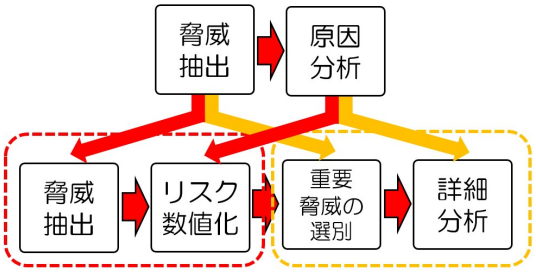

図 1: 2 ステップリスク分析

そして，特定の領域や観点へのフィッティングのために，既存のリスク数値化手法のカスタマイズを行うことを提案した．自動車システムに不正な機器を接続するダイレクトアクセス攻撃を事例として検証した．

3 まとめ

従来手法では検知が難しかった自動車システムにおけるダイレクトアクセス攻撃を例に，システムの物理的境界を乗り越えた攻撃を的確に評価できるリスク数値化手法 RSS-CWSS_CPS を考案した．そして脆弱性評価基準 CWSS に基づくこの手法が上記攻撃を適切に検知できることを，ケーススタディを通じ示した．

* 住友電気工業株式会社，〒541-0041 大阪府大阪市中央区北浜 4-5-33, Sumitomo Electric Industries, Ltd., 4-5-33 Kitahama, Chuo-ku, Osaka, Osaka 541-0041, Japan.
† (国研) 産業技術総合研究所住友電工―産総研サイバーセキュリティ連携研究室，〒563-8577 大阪府池田市緑丘 1-8-31, SEI-AIST Cyber Security Cooperative Research Laboratory, AIST, 1-8-31 Midorigaoka, Ikeda, Osaka 563-8577, Japan.