Copyright© 2022 The Institute of Electronics,
Information and Communication Engineers

SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

サイバーキルチェーンに基づく車両における攻撃行動把握手法の検討
A Study on Attacker Behavior Detection in Vehicles using Cyber Kill Chain

福田 國統* 三好 孝典* 濱田 芳博* 礒山 芳一* 上田 浩史†
Kunito Fukuda, Takanori Miyoshi, Yoshihiro Hamada, Yoshikazu Isoyama, Hiroshi Ueda

キーワード 車載セキュリティ，サイバーキルチェーン，侵入検知

あらまし

現在の車両では，安全性，運動性，快適性を高めるために，多くの電子制御ユニット（ECU）を利用している．一方，車両に対するサイバー攻撃が報告され，それらに対応するセキュリティ手法が多数提案されてきた．

また，それらのセキュリティ手法を各国や組織が制定した場合，それらの仕様への対応が車両の開発に負担となると懸念された．そこで，国際的な法規としてUNECE が自動車基準調和世界フォーラム（WP.29)において，車両に対するサイバーセキュリティ法規基準(UNR155)を制定した．この中で，型式認証を得るには車両におけるセキュリティ対策は必須となっている．

一般的に IT 機器と比較して，車両製品寿命は長く，市場流通後に未知の脅威や脆弱性への対応が必要となる．そのため，未知の脅威による被害の拡大を抑えるために，多層防御の実現が必須となっている．

車両での多層防御を実現するために，攻撃者が目的を達成するまでの一連の行動(サイバーキルチェーン)を把握し，行動ごとに対応する必要がある[1]．しかし，近年の車両は，従来の車両内に閉じていた制御用の車載ネットワークが，サービス向上のため，公衆無線や，Wi-Fi，Bluetooth などの車外の IT 通信網へ接続されている．そのため，従来の IT 向けに作成されたサイバーキルチェーンでは，車載システムでの攻撃者の行動を理解することが困難である．

本稿では，攻撃者の行動を把握し，その一連の行動を分断するための緩和策の実施を目的とし，侵入検知やログ分析による脅威情報から，攻撃者の攻撃行動を把握する図 1 に示すフローを提案した．また，アタックサーフェイスが異なる 10 種の車両攻撃事例を分析して，サイバーキルチェーンの整理を行うとともに，攻撃行動を把握するために必要な脅威情報を得るため，必要となる検知機能について検討した．

今後は，本論で整理を行ったサイバーキルチェーンでのサイバー攻撃事例に対する網羅性を高めるとともに，図 1 の行動把握フローを支援するシステムの構築を進める．

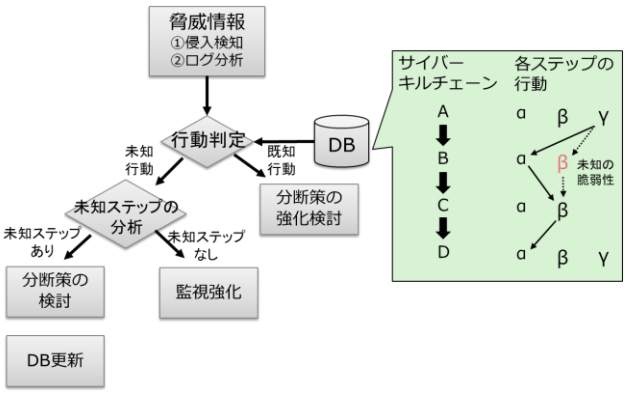

図 1 攻撃行動を把握するフロー

参考文献

[1] Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." Leading Issues in Information Warfare & Security Research 1.1 (2011): 80.

* 住友電気工業株式会社 〒554-0024 大阪市此花区島屋 1-1-3
SUMITOMO ELECTRIC INDUSTRIES, LTD. 1-1-3, Shimaya, Konohana-ku, Osaka, 554-0024, Japan
† 株式会社オートネットワーク技術研究所, 〒 510-8503 三重県四日市市西末広町 1 番 14 号 AutoNetworks Technologies, Ltd. 1-14 Nishisuehiro-cho, Yokkaichi, Mie,510-8503, Japan