鉄道分野におけるサイバーセキュリティ対策要件の動向予測

中央大学　国際情報学部　准教授　松崎　和賢

1．はじめに

本研究では、鉄道分野におけるサイバーセキュリティに関する国際的な動向を踏まえ、国内鉄道事業者やメーカーに関係する事項を整理した。その上で、国内の鉄道事業者の今後のサイバーセキュリティ対策に資する情報を提示した。

本研究の貢献は二つに大別できる。一つは諸外国で実施されている鉄道分野に関するプロジェクトから、特に注目すべきプロジェクトや文書を特定したことである。もう一つは、国内鉄道事業者やメーカーにとってそれらの情報をどう活用すべきかを示したことである。

諸外国のプロジェクトは、(1) 既存の情報セキュリティや産業制御システムセキュリティの国際標準を鉄道分野に落とし込むこと、(2) 既存の情報セキュリティ製品を運行管理システムや信号システムに適用すること、(3) セーフティとセキュリティの共存のあり方を検討すること、について過年度までに調査研究を進め、欧州標準規格である CLC/TS 50701 にその成果を集約しつつある。この欧州標準規格は国際標準規格である IEC 文書の原型となることが予想される。

諸外国においては、インシデント発生時の報告義務に迅速に対応するための組織論の研究が今後隆盛になると見込まれる。その一方で、鉄道分野の既存のシステムに対する攻撃を実証する事例等もあり、事業者のシステムごとのリスクアセスメントに基づく対応をしていくことが望まれる。本研究では、この際のリスクアセスメントに資する情報を過去のプロジェクト等から整理している。

以下、調査研究の背景、注目事例、考察について記載する。既存プロジェクトの内容等、調査の詳細は報告書本編に記載する。

2．調査研究の背景

本研究を実施するに至る背景について本章で述べる。2.1 節では、諸外国で報告されたサイバーセキュリティインシデントを挙げる。2.2 節では欧州において対策検討が進む根拠となる法制度の動向について整理する。2.3 節では、国内の鉄道分野における最近の関連動向を記載する。

2．1　諸外国でのインシデント

- 2009 年、ポーランド (Lodz)[1]、トラックポイントを、改造したテレビリモコンで 14 歳の少年が操作。路面電車 4 台が脱線、12 人が負傷した。
- 2011 年、米国 (unnamed railroad located in the Pacific Northwest)[2]、遠隔からコンピュータを制御され、信号が二日間停止。運行遅延が発生した。

1　https://www.theregister.co.uk/2008/01/11/tram_hack/
2　https://www.wired.com/2012/01/railyway-hack/

- 2014 年、韓国 (Seoul Metro)[3]、北朝鮮のハッカーが、ソウル地下鉄の従業員 60 名のコンピュータに侵入。運行管理系には到達していない。
- 2016 年、米国 (San Francisco Municipal Transportation Agency)[4]、ランサムウェア (HDDCryptor malware の亜種) に 2,112 台の PC が感染、券売機使用不可。改札を開放して無料で乗車可能となった。
- 2016 年、英国、2016 年に英国の鉄道網が 4 つの主要なサイバー攻撃に曝されたとダークトレース社が公表。同社は、英国の民間企業であり、鉄道網のセキュリティ監視も実施している。
- 2017 年、ドイツ (Chemnitz 駅等) 2017 年 5 月 12 日にドイツのケムニッツの主要鉄道駅で WannaCry マルウェアの影響を受け、情報表示装置にエラーが表示される。
- 2017 年、スウェーデン (Sweden Transport Administration)[5]、同機関へのサービス提供事業者である TDC 社と DGC 社に対する Distributed Denial-of-Service (DDoS) 攻撃を受け、運行遅延及び運休が発生した。
- 2018 年、デンマーク (DSB)[6]、DDoS 攻撃を受け、券売機、アプリ、ウェブサイト、小売店 (7-Eleven) からの発券が不可となった。

２．２　諸外国の法制度・標準

2019 年に UNIFE(Union des Industries Ferroviaires Européennes: 欧州鉄道産業連合) が公表した文書“UNIFE VISION PAPER ON DIGITALISATION”の中でサイバーセキュリティをこれからの鉄道分野における 5 つの主要な領域 [7] の一つとして挙げている。これには欧州の法制度や標準機関の動向が関係している。

２．２．１　ネットワークおよび情報システムのセキュリティに関する EU 指令（NIS 指令）[8]

EU 各国は、EU 指令に対して各国で独自に実装をする。鉄道分野のサイバーセキュリティに関して影響のある指令として、NIS 指令 (2016 制定、2018 施行) がある。NIS 指令は、サイバー攻撃（情報流出）に対して、システムが完全性を維持することと、実効性のあるプロトコルを有することを指示している。鉄道を含む重要インフラ事業者向けのサイバーセキュリティ基準のベースラインを設定する意味を持つ。

EU 加盟国は 2018 年 5 月 9 日までに NIS 指令の国内法制化が求められていた。

２．２．２　各国の例：英国政府による業界へのガイダンス[9]

英国では、鉄道システムの所有者に「誤動作や疑わしい活動を確実に検出できるように監視システムを導入する」こと等を求めるガイダンスを発行している。

---

3 https://www.securityweek.com/north-korea-suspected-hacking-seoul-subway-operator-mp
4 https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware
5 https://www.bleepingcomputer.com/news/security/ddos-attacks-cause-train-delays-across-sweden/
6 https://www.itgovernance.eu/blog/en/danish-rail-network-dsb-hit-by-cyber-attack
7 “five major areas – Big Data; Cybersecurity; Artificial Intelligence; New Mobility Services and the Digitalisation of the Freight Logistics Chain”
8 EU, EU 2016/1148, http://data.europa.eu/eli/dir/2016/1148/oj
9 Department for Transport, "Rail Cyber Security Guidance to Industry", February 2016

2．2．3　欧州電気標準化委員会 (CENELEC) による EN 規格[10]

EU の標準機関である CENELEC では、2017 年 7 月に TC9X/WG26 を設立した。目的は、鉄道分野における情報セキュリティに関する技術仕様 (Technical specification) の策定である。実態としては、制御システムセキュリティの国際標準である IEC 62443 をベースとして作成をしている。当初の予定では、2020 年 2 月に TS 発行であったが、スケジュールが遅延して現在 (2020 年 3 月) に至っている。

2．2．4　IEC/TC9/AHG 20 の活動

IEC-ACSEC (International Electrotechnical Commission - Advisory Committee on Security: 情報セキュリティ諮問委員会) から求められている IEC Guide 120 “Security aspects – Guidelines for their inclusion in standards”への対応を鉄道分野の TC9 として行うために 2018 年に AHG 20 が設立された。鉄道分野の国際標準文書について情報セキュリティの記載の必要性や記載方法について見直しが行われている。結果として情報セキュリティについて一貫した形での国際標準規格の改定が見込まれる。

2．3　国内の動向

- 2017 年、内閣サイバーセキュリティセンターが「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」を公表した。2018 年には「重要インフラ分野における情報セキュリティ確保に係る安全基準等策定指針（第 5 版)」を策定した。
- 2019 年、上記指針の改定を受け、国土交通省が「鉄道分野における情報セキュリティ確保に係る安全ガイドライン」の改訂版 (第 4 版) を公表した。用語や平仄を合わせる他、『国民生活及び社会経済活動に影響を与える重要インフラサービス障害が発生した場合、国土交通省へ情報連絡を行う』と明記する等の更新があった。これは英国のガイダンスと同様に、サイバーセキュリティの被害を受けた後の報告を求める内容である。
- 2020 年、一般社団法人「交通ＩＳＡＣ（アイザック)」が設立 (4 月 1 日) される。IT 部門と OT(鉄道) 部門の連携に関する WG 等に鉄道事業者も参画している。

3．注目事例

3．1　最近終了したプロジェクト

- CYRail: CYBERSECURITY IN THE RAILWAY SECTOR、2016-2018、EU の鉄道分野における研究基金である Shift2Rail と、同じく EU の研究基金である Horizon 2020 の双方から支援を受けているプロジェクト。鉄道インフラを狙う脅威の分析を実施している。既存の検知技術（製品）の検証も実施している。また、サイバー攻撃に対する被害の緩和計画、対策を定義している。運行管理システムのプロテクションプロファイルを作成して、新しい鉄道インフラの「セキュリティ バイ デザイン」(設計時からセキュリティを考慮する）を進める。
- CIPSEC: Enhancing Critical Infrastructure Protection with innovative SECurity framework、2016-

10 CLC/TC 9X/WG 26 IT-Security / Cybersecurity in the railway sector
https://www.cenelec.eu/dyn/www/f?p=104:14:1639550872240101::::FSP_ORG_ID,FSP_LANG_ID:2336555,25

2019、Horizon 2020 の支援を受けているプロジェクト。CIPSEC の主な目的は、最先端の異種セキュリティ製品を統合して、CI の IT（情報技術）および OT（運用技術）部門に高レベルの保護（脅威の検出、特定、軽減）を提供する統合セキュリティフレームワークを作成することである。複数分野によるパイロット試験を実施したが、そのうちの一つに鉄道分野を含む。ドイツの鉄道事業者 DB の関連会社が対応した。

- Shift2Rail - X2Rail-1、2017-2019、Shift2Rail には、5 つの Innovation Programmes (IP) があり、IP2 に X2Rail-1 project が含まれる。 X2Rail-1 には technical workpackages (WP) が複数あり、WP8 が Cyber Security for railways となっている。"IEC 62443 AS CYBERSECURITY FRAMEWORK FOR RAILWAY”としており、IEC 62443-3-2 にて定義されているリスク分析手法の鉄道分野への適用等を実施している。

３．２　現在進行系、将来のプロジェクト

以下のプロジェクトが、今後欧州の鉄道分野におけるサイバーセキュリティの研究を牽引すると考えられる。

- HASELNUSS、2017-2020 Ministry of Education and Research (BMBF)
- Shift2Rail - 4SecuRail、2019-2021
- Shift2Rail - X2Rail-3、2019-2021 (X2Rail-5、2021-)

３．３　未公開・公開文書

- PD CLC/TS 50701 Railway Applications – Cybersecurity、2020、CENELEC TC9X WG26 が策定中。この文書が鉄道分野の RAMS 規格の際と同様に国際標準になる可能性を有する。
- Guidelines for Cyber-Security in Railways[11]、2018、UIC (International Union of Railways) 名義で発行されたガイドライン。ARGUS (Availability and Security Challenges of Open Networks aiming of their use in signalling of railways) プロジェクトの成果の一部を刊行。鉄道分野で ISO 27000 およびその他の一般的な規範を適用する方法のガイドとなっている。
- Gordeychik、Sergey、Cyber Resilience of Railway Signaling Systems、2019、著名なハッカーグループ SCADA StrangeLove 主幹による文書。同氏は、日本最大級のセキュリティ国際会議 CODE BLUE の技術セッションでもプレゼンを過去に実施している。鉄道分野の国際標準には明示的に書かれない、鉄道分野のシステムの脆弱性を指摘している。

４．考察

鉄道分野におけるサイバーセキュリティ研究の傾向を把握するために、米国 NIST が発行するサイバーセキュリティフレームワークとの関係を図 1 にマッピングした。過年度までのプロジェクトでサイバーセキュリティ活動の上流（図の左側）である ID (Identify: 青)、PR(Protect: 紫) 及び DE(Detect: 橙) についてはカバーされており、その成果が TS 50701 にも影響を与えると考えられる。一方、最近始まったばかりのプロジェクト (4SECURail) では RS(Response: 赤) に軸足を移しており、一つの新し

11　http://www.shop-etf.com/en/guidelines-for-cyber-security-in-railways

い傾向と捉えられる。欧州や日本で緒に就いた ISAC(アイザック、Information Sharing and Analysis Center) 、具体的には ER-ISAC(European Rail) や交通 ISAC においてもインシデントレスポンス、情報共有、監督官庁への報告については議論されるものと考えられる。

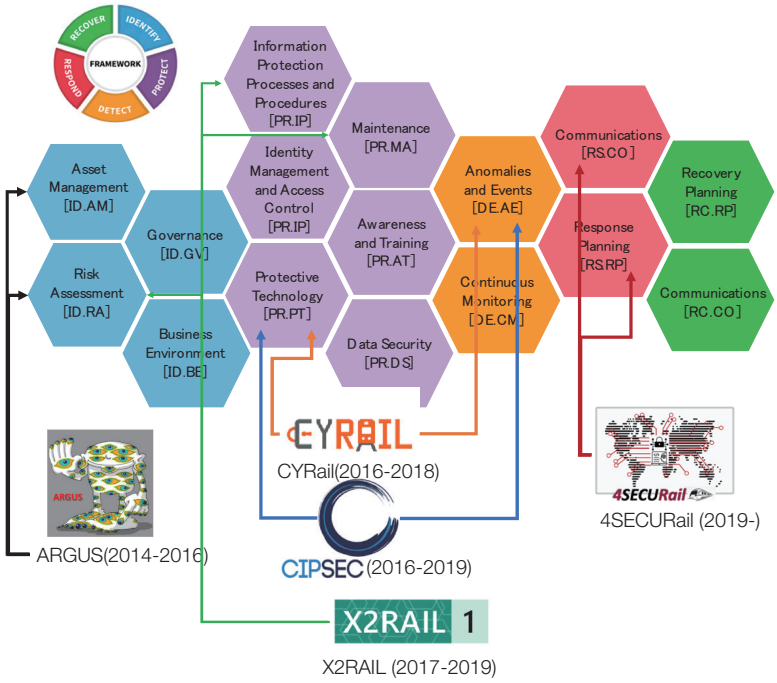

図１　鉄道分野のサイバーセキュリティ研究プロジェクトの傾向：セキュリティインシデント対応フェーズへ　(出典 : NIST Cybersecurity Framework に基づき著者作成)

以下、既存プロジェクトの傾向と、これから国内の鉄道事業者やメーカーに求められる行動を挙げる。

４．１　既存プロジェクトの傾向

- 情報セキュリティの国際標準である ISO 27000 と制御システムセキュリティの国際標準である IEC 62443 を鉄道分野に適用する。
- 侵入検知システム (IDS) 等、情報系のセキュリティ製品を適用する。
- セーフティとの共存に対する検討を実施する。例えばセキュリティ要件に、IEC 62280 に準拠することと記す。

４．２　これから求められる行動

- 監督官庁への報告要件を満たすためのインシデントレスポンスのあり方の検討
- 鉄道部門のシステム全体に対するリスクアセスメントと対策
- 標準規格等の文書と実システムの構成の違いを考慮した上での検討