Supported by 日本財団 THE NIPPON FOUNDATION
運輸総合研究所 2018.5 No. 3
研究調査報告書要旨

サイバー攻撃に対する人材育成に関する調査研究報告書・サイバー攻撃に対するセキュリティ情報共有組織(ISAC)の構築に関する調査研究報告書

１．研究の目的

近年急増しているサイバー攻撃は、2017 年度に発生した「WannaCry」と呼ばれる身代金攻撃（ランサムウェア）に代表されるように、世界規模で拡大しており、我が国にとっても大きな脅威になりつつある。海外ではこうした鉄道及び航空分野[注1)]へのサイバー攻撃も散見されており、仮に 2020 年東京オリンピック・パラリンピック開催期間中にサイバー攻撃が発生した場合、甚大な影響を及ぼすおそれがある。

こうした中で、鉄道及び航空分野では、サイバーセキュリティ人材の不足が懸念されている。平成 27 年度に実施した鉄道、航空事業者への意識調査[注2)]では、鉄道及び航空分野の事業者の７割以上が人材育成に課題があると回答があり、同分野においても、サイバー攻撃に対応できる人材の育成が急務となっている、一方で、サイバー攻撃は、日々攻撃手法が進化しているため、近年、金融などの分野では業界全体でセキュリティ情報を共有する情報共有組織（ISAC）が立ち上がり活動を行っているとともに、国土交通省においても交通分野での同組織の立ち上げに向け検討が行われている。

以上を踏まえ、本事業では 2020 年東京オリンピック・パラリンピックに向けて、我が国の鉄道及び航空分野の事業者におけるサイバーセキュリティ体制の強化に資することを目的として、サイバー攻撃に対する人材育成、セキュリティ情報共有組織（ISAC）の構築に関する調査研究を実施した。

２．研究の内容と結果

(1) サイバー攻撃に対する人材育成に関する調査研究

鉄道/航空の安全・安定輸送に資するサイバーセキュリティ対策の手引き

平成 28 年度に鉄道/航空の安全・安定輸送に資するサイバーセキュリティ対策の手引き[注3)]を作成した。この手引きを実践する人材を育成することを目指し、事業者がサイバーセキュリティ人材を育成する際に参考となるカリキュラムの作成を行った。

カリキュラムの作成の前提条件となる、求められる人材像として、①インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、適切に対応できる人材、②サイバー攻撃に対処（原因究明、復旧など）する専門機関と連携して、インシデント対応ができる人材と定義した。また、これを踏まえ、本カリキュラムの育成対象者は、事業部門のシステムを維持管理する人材とした。

前提条件の検討結果を踏まえ、国内外の人材育成カリキュラム事例収集や机上演習の実施結果など

をもとに学習内容を検討し、カリキュラムを作成した。講座にはサイバーの攻撃の現状やサイバーセキュリティで必要となるネットワークの知識、サイバー攻撃対策、インシデント対応などを選定した。

同カリキュラムは、鉄道及び航空分野に特化した内容を目指し、学識経験者や鉄道及び航空分野の事業者からなる検討委員会での検討を経て作成したものであり、鉄道及び航空分野の事業者がサイバーセキュリティ人材を育成する際の参考資料として実務に役立つ内容とすることができたと考える。

(2)　サイバー攻撃に対するセキュリティ情報共有組織（ISAC）の構築に関する調査研究

国内のセキュリティ情報共有組織、米国 Aviation ISAC 等へのヒアリングを実施し、情報収集、分析、提供等の現状、ベストプラクティスや課題などについて把握した。また、鉄道及び航空事業者の IT/運輸部門へのアンケート調査を実施し、セキュリティ情報の入手と社内等への情報展開、ISAC への課題やニーズを把握した。さらに、セキュリティ情報の共有体制が進んでいる米国（Aviation ISAC、ST- ISACS、ISAO 等）、欧州（EA-ISAC、EU Rail ISAC 等）のセキュリティ情報組織について、情報共有の仕組み、運用実態、運用時の工夫などにて文献調査を実施するとともに、2016 年リオデジャネイロオリンピック・パラリンピックなどでの情報共有の取組みについて把握を行った。

上記調査で把握された内容をもとに、情報共有を確立するためのガイドラインである NIST SP 800-151、ISAC の発展策について取りまとめられた ENISA ISACs Cooperative Models を参考に ISAC のあるべき姿として、鉄道・運輸分野における ISAC の設計（基本方針、組織構成、構築手順、規約案等）を行った。

ISAC 構築時に踏まえなければならない要件として①情報共有の目的の定義、②共有情報と情報源の特定、③情報共有規則の確立、④会員制度の制定、⑤事務局の決定について取りまとめた。さらに ISAC の機能として検討すべき事項について、①情報分析の実施、②ISAC を活性化させるための活動、③情報共有の評価などについて取りまとめた。

ヒアリングやアンケート調査などから把握された既存 ISAC や事業者等での情報共有の取り組みを ISAC の設計（基本方針、組織構成、構築手順、規約案等）に反映させることで、ISAC の構築や情報共有活動を行う際の参考資料として実務に役立つ内容とすることができたと考える。

３．おわりに

サイバー空間に関する情勢は日々深刻になっており、その攻撃方法も日々進化している。2020 年の東京オリンピック・パラリンピックに向けて、わが国に対するサイバー攻撃の脅威は一層深刻化すると考えられる。

サイバー攻撃に対する人材育成に関する調査研究では、人材育成カリキュラムと教材（簡易版）の作成を行うとともに、セキュリティ情報共有組織（ISAC）の構築に関する調査研究では、ISAC のあるべき姿を提言としてまとめた。

我が国の鉄道及び航空分野の事業者におけるサイバーセキュリティ体制の強化の参考資料となれば幸いである。

注1)本調査研究における「航空事業者」は、航空輸送事業者及び空港運営事業者を想定している。

注2) 日本財団助成事業：「平成 27 年度東京オリンピック・パラリンピックに向けた交通機関へのサイバーテロ対策に関する調査研究報告書」（一財）運輸政策研究機構、平成 28 年 3 月）

注3) 日本財団助成事業：「平成 28 年度東京オリンピック・パラリンピックに向けた交通機関へのサイバーテロ対策に関する調査研究報告書」（一財）運輸総合研究所、平成 29 年 3 月）

報告書名：
サイバー攻撃に対する人材育成に関する調査研究
（資料番号 290003）
本文：A 4 版　170 頁

報告書目次：

サイバー攻撃に対するセキュリティ情報共有組織（ISAC）の構築に関する調査研究

（資料番号 290004）

本文：A４版　139 頁

報告書目次：

【担当者名：吉澤智幸、深作和久】

【本調査は、日本財団の助成金を受けて実施したものである。】

一般財団法人運輸総合研究所

〒105-0001　東京都港区虎ノ門 3-18-19　虎ノ門マリンビル

TEL ： 03-5470-8405　FAX ： 03-5470-8401