Supported by 日本財団 THE NIPPON FOUNDATION

運輸政策研究機構　2016.5 No. 3

研究調査報告書要旨

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

１．研究の目的

2020 年東京オリンピック・パラリンピック競技大会の開催が決定したが、過去のオリンピックでは幾度となくテロの標的になっており、特に近年急増しているサイバー攻撃は大きな脅威となっている。一方、期間中に多くの人の移動を担う鉄道、航空などの交通分野では、一般的に独自回線やクローズドシステムを運用しており、現在までサイバー攻撃の大きな被害の発生はないが、今後は GPS や電波を利用した運行制御、IC カードの料金収受の運用が拡大している交通機関に対するサイバーテロの脅威も十分に考えられ、仮に発生すると被害が甚大になる恐れがある。

これまで交通機関に特化したサイバーテロ、サイバー攻撃に関する研究は非常に少ない。本研究では、専門家、関係省庁、事業者を委員とする検討委員会を設置し、サイバー攻撃に関する国内外の事例の収集・分析、交通事業者のサイバーセキュリティに対する取組みの実態調査などを実施し、我が国の交通分野におけるシステムの脆弱性を明らかにすることを目的とした。

２．研究の内容と結果

本研究は、「重要インフラの情報セキュリティ対策に係る第３次行動計画」に示された重要インフラ 13 分野に指定されている「鉄道」「航空」を対象に、以下の内容を実施した。

(1)　事例調査と分析

近年の国内外におけるサイバー攻撃の事例とその被害について、「一般事例」「交通機関関連事例」「ビッグイベント事例」について収集及び整理し、サイバー攻撃の傾向や今後の動向を分析した。

その結果、交通機関はサイバー攻撃の標的の一つである可能性が高いと判断でき、交通機関のクローズドネットワークに対する攻撃の可能性もあることがわかった。交通分野においてもサイバー攻撃やサイバーテロの脅威を正しく捉え、適確な対策を講じていく必要があるほか、攻撃事例は少ないものの、被害に気付いていない可能性も考えられ、既に侵入されていることを想定したセキュリティ対策や、内部犯行への対応も必要であることがわかった。

(2)　外国調査

欧州では主に鉄道分野、米国では航空分野を中心とした交通関係の諸機関、組織、民間企業を対象としてヒアリング調査と実態調査を実施した。

欧州と米国の両調査とも、クローズドならばシステムやネットワークは安全ということは無く、システムである以上は何らかの脆弱性を抱えているという前提で対策が行われていることを改めて確認した。また、従業員のバックグラウンドチェックなどを徹底し、内部犯行への対応や多層防御を実施しているとの知見も得られた。さらに、欧米のサイバーセキュリティ体制については、欧州では国の機関に権限と責任がしっかりと委譲されていることなど、米国では情報共有のフレームワークである ISAC（Information Sharing and Analysis Center）の枠組みの実態やその設立背景などについて把握することができた。

(3)　交通分野におけるセキュリティに対する意識調査

交通分野における事業者の情報セキュリティ、サイバーセキュリティへの取り組み状況について現状を把握するため、アンケート調査等を実施した。

その結果、交通分野のサイバーセキュリティに対する組織体制について、人数ならびにスキル面で不足を感じていること、個別システムのセキュリティ

対策を検討・実施する所管部門とサイバー攻撃に関する情報収集の担当部門が異なる傾向が見られること、セキュリティパッチの適用や脆弱性検査の実施が進んでいない状況などが明らかになった。また、被害を想像しにくい攻撃や脅威については事業者の意識が低くなる傾向が確認された。これは、「クローズドシステムはインターネットからの脅威とは隔離されており、安全である」という間違った認識の結果、交通分野のサイバーセキュリティに対する意識が必ずしも高くないことにもつながると考えられる。

(4) システムの脆弱性評価・検証

事業者にご協力いただき、実際のシステムに対してペネトレーションテストを実施した。

ペネトレーションテストは、対象となるシステムに対して模擬的に攻撃を行うテストであり、対象システム上に存在する脆弱性を検出し、ネットワークやシステムへの侵入やシステムの停止などに繋がる可能性があるかを検証するものである。対象システムは、運輸事業者の運行系システム群で、前提としてクローズドネットワークに対して内部からアクセスできる環境（建物や居室への侵入、内部犯行、マルウェア感染等）にあるという条件で実施した。

その結果、致命的な問題はなかったものの、保守用ネットワークという限られた利用者あるいは利用環境において、運用や設定に不備があったため意図的に侵入が可能であることが確認できた。

昨今の IT システムにおけるセキュリティ対策はシステム上の対策に重きが置かれており、今回のような運用・設定の不備を突いた攻撃が行われた場合の防御と検知は難しいと考えられる。しかし、今後はネットワーク、各製品の様々な Web アプリケーション、開発体制、運用体制、各種ポリシーの策定、開発委託業者の管理など、あらゆる点において適切な情報管理、脆弱性の管理、対策が必要となることがわかった。

(5) 関連する調査等の整理

鉄道に関しては韓国の鉄道関連事業者を狙った一連のサイバー攻撃事例の調査結果、航空に関しては情報セキュリティ大学院大学内の Aviation security 研究会の調査研究を整理した。

(6) 脅威シナリオと求められるセキュリティ対策

サイバー攻撃の類型化と、サイバー攻撃に係る交通網システムが有する特徴を整理し、交通網へのサイバー攻撃のシナリオを想定するとともに、想定シナリオに基づいたセキュリティ対策について、本研究の検討委員会にご参画いただいた名和委員よりご寄稿いただいた。

３．おわりに

平成 28 年に入ってサイバー空間に関する情勢はより深刻になっており、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。

本研究は 2 か年計画で進めており、初年度は、サイバー攻撃やサイバーテロに対する脅威について、幾つかの角度から事例や実態を用いて正しく把握することができた。2 年目は、国や事業者がその脅威とどのように向き合い、どのように対策を施していくべきかについて、引き続き研究を進めていく予定である。

この成果が関係者の皆様のサイバーセキュリティに対する意識の発展への一助となり、それぞれの組織において対策の導入や見直しに向けた第一歩を踏み出すきっかけになれば幸甚である。

報告書名：
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（資料番号 270119）
本文：Ａ４版　276 頁

報告書目次：

【担当者名：西村潤也】

【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。】