

2025年12月10日 第96回運輸政策セミナー
交通サイバーセキュリティ XⅢ
～鉄道分野におけるサイバー攻撃対策と事業継続の取り組み～
宿利会長 開会挨拶

皆様、こんにちは。運輸総合研究所 会長の宿利正史です。

本日の運輸政策セミナーにも、大変多くの皆様にご参加いただきまして、誠にありがとうございます。

当研究所では、2015年度から19年度までの5年間にわたり、交通サイバーセキュリティに関する研究調査を実施するとともに、サイバー攻撃の最新動向と対策を共有するため、実務者をはじめ、経営層や監査役を対象としたセミナーを開催してきました。

その後も、高度化するサイバー攻撃に関する最新情報や知見をアップデートするために、2020年からは交通サイバーセキュリティセミナーを毎年開催しております。本日のセミナーは、当研究所がサイバーセキュリティに関する取り組みを開始した2015年度から数えて通算13回目のセミナーとなります。

さて、地政学リスクが高まり、国際情勢の不確実性が一層増し、他方でAIなどのデジタル技術が進展する中で、サイバーセキュリティに対する脅威が世界的規模で深刻化しております。

2023年7月、名古屋港でランサムウェアを用いたサーバー攻撃により物流の混乱が発生しましたが、今年に入ってからランサムウェア攻撃による被害が相次いでいます。

今年9月にはアサヒグループホールディングスが、ランサムウェア攻撃を受け、基幹システムが停止し、受注・出荷業務などが全面的に停止しました。

続いて10月にはアスクルが、ランサムウェア攻撃を受け、物流システムが停止し、通販サービスが利用できない状態となりました。

これらの障害は他社にも影響し、飲料業界や小売業の一部で販売や配送が停止するなど、サプライチェーン全体に混乱が広がっています。

鉄道、海運、港湾、航空、空港、物流などのいわゆる基幹インフラは、ひとたびサイバー攻撃により機能が停止または低下した場合、国民生活や経済活動

に多大な影響を及ぼすおそれがあります。

これまでのセミナーでは、大手製造業の情報セキュリティ責任者などに登壇いただき、サイバーセキュリティに関する最新動向や対策を共有してきましたが、参加者から交通運輸分野に関連するテーマを扱ってほしいという要望が寄せられていました。そこで今回は、鉄道分野に焦点を当てたセミナーを開催します。

なお、本セミナーでは、政府・国土交通省によるサイバーセキュリティの取り組み、JR 東日本グループにおけるセキュリティ戦略、最新のサイバー脅威と事業継続の取り組みについてご紹介いただきますが、いずれのテーマも、交通運輸・観光分野の方々にとって有益な情報を提供できるものと考えております。

さて、本日のセミナーでは、国土交通省大臣官房政策立案総括審議官の長井 総和様から、株式会社 JR 東日本情報システム ICT 基盤本部セキュリティ対策室次長の関口 義弘様から、そして最後に、先ほどご紹介したサイバーセキュリティ実務の第一人者である名和 利男 様からご講演いただきます。

3名の方の講演の後に、後藤 厚宏 様に今回もモデレーターとなっていていただきまして、各講演の総括とディスカッションを行い、最後に皆様と質疑応答を行います。

すでに皆様にご案内しているとおり、今回のセミナーに参加申込された方々のお手元に、「交通サイバーセキュリティへの理解を促進するための問題集」をご送付しております。また、本日ご参加いただいた皆様の疑問や問題意識などを把握するためのアンケートを実施し、フォローアップ情報をご参加の皆様にお届けする予定です。どちらも名和 利男 様の監修によるものであります。

最後になりますが、本日のセミナーは、一般社団法人交通 ISAC にご後援をいただいておりますことをお伝えします。

本日のセミナーが、ご参加いただいております多くの皆様方にとりまして、真に有益なものとなりますことを期待いたしまして、私の挨拶といたします。

本日は誠にありがとうございます。

以上