

2024年12月13日 第94回運輸政策セミナー

交通サイバーセキュリティ XII

～交通運輸分野における基幹インフラサービスの安定的な提供に向けた持続
可能なサイバーセキュリティ体制の構築について～

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、当研究所においてサイバーセキュリティに関する取り組みが開始された2015年度から数えて通算12回目のセミナーとなります。

2021年から昨年まで3回実施した交通サイバーセキュリティセミナーでは、本日ご登壇いただく情報セキュリティ大学院大学学長の後藤 厚宏 様に毎回モデレーターを務めていただいています。また、同じく本日ご登壇いただく株式会社サイバーディフェンス研究所専務理事の名和 利男 様には、皆様の疑問や問題意識に関するフォローアップ情報を監修していただき、ご参加の皆様にお届けしてきました。

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。

昨年7月には名古屋港において、ランサムウェアを用いた攻撃により、物流の混乱が発生しました。今年に入ってから、出版会社、情報処理会社、医療機関、報道機関などで、ランサムウェア攻撃による被害が相次いでおり、警察庁などから注意喚起が出されています。

また、米国では本年2月に、サイバーセキュリティー・インフラセキュリティー庁、

国家安全保障局、連邦捜査局から米国の重要インフラへの環境寄生型攻撃に対する共同勧告が出されました。この攻撃は、コンピュータにインストールされている正規のツールを駆使して攻撃を行うことから、攻撃検知が難しくなっており、新たな脅威となっています。

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し、または低下した場合には、国民生活や経済産業活動に多大な影響を及ぼすおそれがあります。

こうしたことから、交通運輸分野における基幹インフラサービスの安定的な確保を図るために、サイバー攻撃に関する最新動向を踏まえたサプライチェーン対策とレジリエンスのあり方、持続可能なサイバーセキュリティ体制の構築をテーマとして、本日のセミナーを開催することといたしました。

すでに皆様にご案内しているとおおり、今回のセミナーに参加申込された方々のお手元に、「サイバーセキュリティに関する理解を促進するための Q&A 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。

さて、本日のセミナーでは、国土交通省大臣官房サイバーセキュリティ・情報化審議官の山下 雄史様から、株式会社東芝研究開発センター・サイバーセキュリティ技術センター・セキュリティ技術部長の古川 文路様から、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。

最後になりますが、本日のセミナーは、鉄道、航空、空港、物流の4分野のサイバーセキュリティに関する協議や情報共有を行う一般社団法人交通 ISAC にご後援をいただいておりますことをお伝えしておきたいと思っております。

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。