第86回運輸政策セミナー

2022/9/26（月）15:00～（会場・オンライン併用開催）

交通サイバーセキュリティ

～安全保障環境の変化やDXの進展等を踏まえた経営層の役割～

開催概要

DXの進展，新型コロナウイルス感染症の拡大に伴うテレワークの一般化など，サイバーセキュリティを取り巻く環境の変化を背景に，サイバー攻撃は高度化，多様化していることを踏まえ，当研究所では，昨年11月7日に運輸政策セミナーを開催しました．

今回は，ウクライナ情勢などその後の更なる安全保障環境の変化や経済安全保障法制の整備等を踏まえ，質の高い情報提供と意識喚起を行い，交通分野の官民の取り組みをさらに一歩進めることを目的として，運輸政策セミナーを開催します．具体的には，交通分野の取り組みの方向性，経営層の意識改革に関する課題と現場経験に基づくアドバイス，報道ではわかりにくいサイバーセキュリティの最先端の状況などについて講演，質疑応答を行いました．

●ウクライナ情勢で発生した「重要インフラサービス」へのサイバー攻撃のレビューと得るべき教訓

ロシアによるウクライナ侵攻「以前」,「直前と直後」,「以降」において，ウクライナとロシアの重要インフラ事業者およびそのサプライヤー等にさまざまな種類のサイバー攻撃の発生が観測されました．その中で，日本の重要インフラ事業者が理解すべき「脅威アクター（攻撃者）がとった戦略・戦術・手順」を簡潔にレビューします．そして，それらから得られた教訓等を示した上で，経営者自らが従来のセキュテリィ対策のあり方を大きく変革させていかなければならない必要性と重要性について講演しました．

●重要インフラのサイバーセキュリティ対策に係る国土交通省の取り組みについて

2022年6月17日に新たに策定された「重要インフラのサイバーセキュリティに係る行動計画」（サイバーセキュリティ戦略本部）を踏まえ，新行動計画で特に強調されているポイントを説明するとともに，これを踏まえて政府及び国土交通省が現在取り組んでいる施策の概要と今後について，また，事業者の注目すべき取り組みとして，一昨年に発足した交通ISACのこれまでの活動と今後の課題等について講演しました．

●CASEに向けたサイバーセキュリティ対応について

自動車産業はCASE（Connected，Autonomous，Shared & Service，Electric）に象徴される様に新領域での技術革新が進む中で大きな変革期を迎えています．一方で，こうしたCASEの進展に伴い，クルマや生産施設などへのサイバーリスク対策も大きな課題になっています．デンソーでは，クルマを安心・安全にご利用いただくため，サイバー攻撃から守る技術を開発し，確実に搭載すべく独自の仕組み構築を行っています．今回のセミナーではCASEにおけるサイバーセキュリティ対策，さらに工場や生産ラインなどへのセキュリティリスクと対策について講演しました．

●サイバー攻撃の脅威に備えるために経営層がなすべきこと
―セキュリティ体制の構築に向けた取組みからの示唆―

DXの進展等によりサイバーセキュリティの一層の強化が求められています．またDXの活用により大量の顧客情報等を活用した商品やサービス開発が可能となったことから個人情報保護の必要性がこれまで以上に高まっています．今回のセミナーでは，サイバーセキュリティ・情報セキュリティを高めるための社内体制の構築，情報セキュリティ部門が担う役割，経営層が踏まえるべき点について講演しました．

講演①
ウクライナ情勢で発生した「重要インフラサービス」へのサイバー攻撃のレビューと得るべき教訓

講師：名和利男
株式会社サイバーディフェンス研究所専務理事／
上級分析官

ウクライナ侵攻前に機密情報搾取や継続的な攻撃を実施するための情報収集を目的としたサイバー攻撃が各国政府機関や企業等に対して行われた．侵攻直前には，ウクライナ政府機関などのITシステムがマルウェア「WhisperGate」などによる攻撃により破壊された．また，ウクライナ政府機関のウェブサイトが改ざんされ，国家分断を目的としたメッセージが表示された．ウクライナ侵攻直後には，衛星通信を含めた情報通信機能への機能破壊の試みが行われ，一部でインターネットが繋がりづらい状況となった．また高い検知回避力を持つサイバー攻撃により，高電圧変電所を含めたウクライナの重要インフラに対する侵害攻撃の試みが発生した．

今回の侵攻ではロシア国内のプロパガンダによる影響を受けたと見られるKillnetなどのハクティビストがサイバー攻撃の一翼を担っている．

こうした中で日本企業の課題は，①情報収集能力の欠如によるサイバー攻撃に対する状況認識の獲得が困難，②サイバーセキュリティに関する業務の担当部門へ丸投げ，③インシデント立ち向かうための「態勢」不足等となる．ウクライナ侵攻で

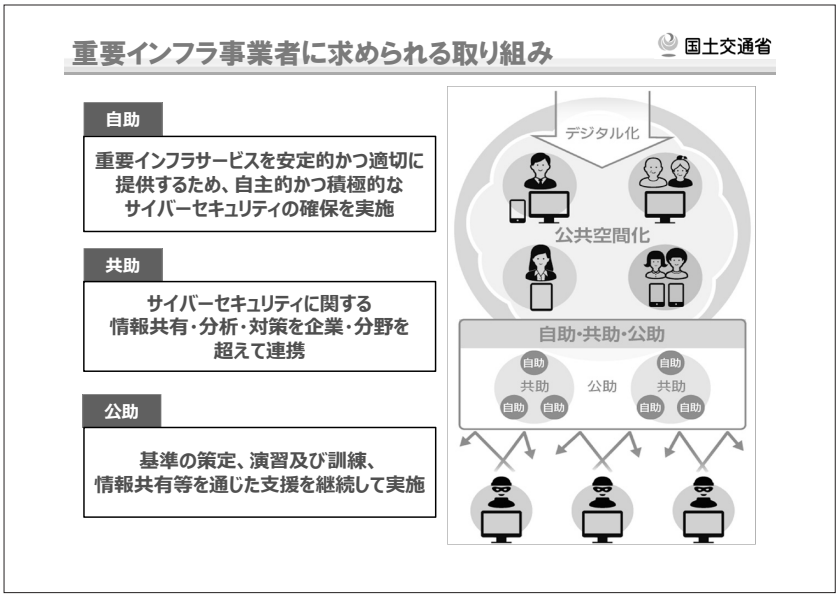
はロシアやハクティビストによる多様なサイバー攻撃が同時多発的起こった．また，有事発生の前には，極めて高度なサイバースパイの活動が活性化していたとみられており，経営層においてはこうしたことを理解し対策の強化に努めて頂きたい．

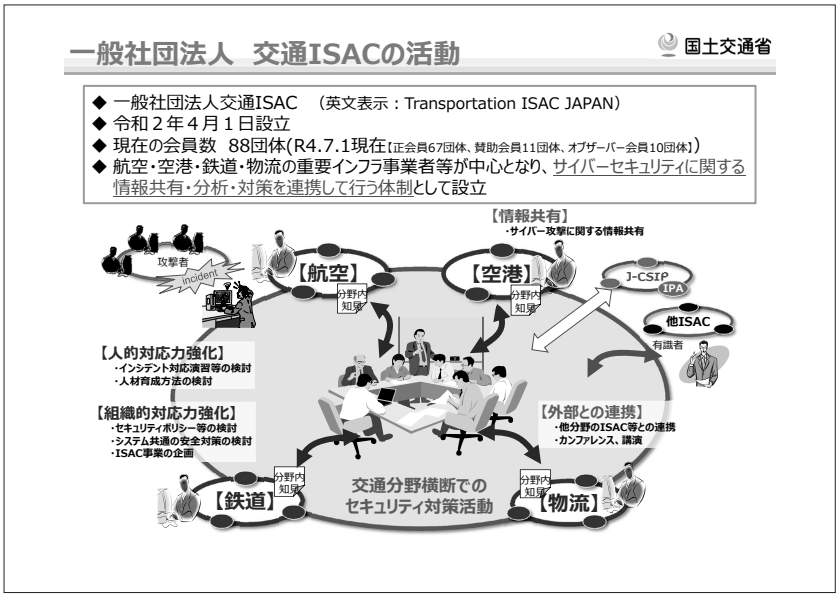
講演②
重要インフラのサイバーセキュリティ対策に係る国土交通省の取り組みについて

講師：髙杉典弘
国土交通省サイバーセキュリティ・情報化審議官

重要インフラの防護に関する法体系として，令和4年6月17日に「重要インフラのサイバーセキュリティに係る行動計画」が策定された．行動計画の基本的な考え方としては，経営層，CISO，戦略マネジメント層，システム担当者を含めた組織全体での対応を一層促進するということが最重要項目として記載されている．

重要インフラ事業者に求められる取り組みとして，自助・共助・公助に基づき，皆で力を合わせてサイバーセキュリティ対策に取組む必要がある．この中の共助とは，「サイバーセキュリティに関する情報共有・分析・対策を企業・分野を超えて連携」するものと定義されており，業界内での情報共有・連携の取組みの推進を図る組織として，ISAC（Information Sharing and Analysis Center）がある．交通分野においても，令和2年4月に一般社団法人交通ISACが設立されており，現在88団体が加盟している．我が国を取り巻く状況というのは非常に緊迫しているところもあり，一部の鉄道事業者のHPが閲覧しにくい状況があったが，外部からの情報共有は非常に有用であり，同日中に復旧した．こうしたことから交通ISACの活動の有用性を改めて感じることができた．交通ISACに加入していない事業者の方々におかれては加入について是非検討していただきたい．





講演③
CASEに向けたサイバーセキュリティ対応について

講師：平永敬一郎
株式会社デンソー情報セキュリティ推進部
製品セキュリティ室長

クルマがインターネットに接続することで便利性や安全性が大きく向上する一方で，サイバー攻撃の機会も増大する．こうしたことから国連法規UNR155が2021年1月に発効し，車両型式法規として，国内では既に施行済みであり，順次適用車両が拡大されている．

製品セキュリティを推進するために，企画段階でリスクアセスメントを行い，市場投入後もPSIRT（Product Security Incident Response Team）が脆弱性の監視・分析や品質問題対応等を実施している．今後，技術面では車両SOC（Security Operation Center）で検知された情報がPSIRTにも共有される．

クルマは脆弱性に対して長期間に亘る対応が必要となることから，業界を挙げての対応が必要となる．その際，取引先の管理（責任分担決めや能力評価）が法規としても求められており，サプライチェーン全体でのセキュリティ確保が課題となっている．

またCASEと呼ばれるConnected（コネクティッド），Autonomous/Automated（自動化），Shared（シェアリング），Electric（電動化）の進展により，セキュリティだけではなく，プライバシー侵害リスクも高まることから，Privacy by Designに基づき企画段階からプライバシーに配慮したものづくりを行う必要がある．

講演④
サイバー攻撃の脅威に備えるために経営層がなすべきこと　～セキュリティ体制の構築に向けた取組みからの示唆～

講師：斉藤宗一郎
株式会社資生堂情報セキュリティ部長（CISO）

自社のビジネスを理解することが非常に重要となる．どういう事業を展開し，何を守る必要があるのかということを明確にし，それらに紐づく情報資産やデータの所在や管理方法など，全体像を具体的な把握しなければ，情報セキュリティを経営課題として捉えることができない．

情報セキュリティを取り巻く外部環境として，サイバー攻撃の頻度の増大や攻撃手法の高度化，インシデント対する社会的なインパクトが高まる中で，内部環境として不安定で流動的なセキュリティ対策についての優先度，慢性的な予算不足，セキュリティ人材の不足等が課題となる．このような中で，コロナ禍で加速した働き方改革が今後も常態化することが考えられる．社内への入退室管理や警備員配備といったオフィスのファシリティ投資と同じように，安心・安全にテレワークを実現させるデジタルファシリティへの投資を拡充していくことが必要になる．

情報セキュリティを経営課題にするためには，目標達に着目したKPI（Key Performance Indicator）からリスクに着目したKRI（Key Risk Indicator）へ切り替え，なりすましを防ぐためのサイバーインテリジェンスの活用やグループ会社のサイバー防衛力の客観評価のためのサイバーリスクスコアの活用，セキュリティの自己点検のサプライチェーン全体への適用，セキュリティ人材の育成などが挙げられる．

総括と質疑応答

コーディネーター
後藤厚宏
情報セキュリティ大学院大学学長・教授

パネリスト
名和利男
株式会社サイバーディフェンス研究所専務理事 / 上級分析官
高杉典弘
国土交通省サイバーセキュリティ・情報化審議官
平永敬一郎
株式会社デンソー情報セキュリティ推進部製品セキュリティ室長
斉藤宗一郎
株式会社資生堂情報セキュリティ部長（CISO）

講師の皆様からサイバーセキュリティは経営問題であり，経営者の責任において対策を実施しなければならないという強いメッセージがあった．

私の方から三つの論点を提示したい．一つ目は，事業停止による被害の連鎖について，コロニアルパイプライン社ではランサムウェアによるサイバー攻撃を受けた．同社は安全を確保するためにパイプラインを停止したことから，ニューヨークでガソリン価格が高騰するなどの大きな被害をもたらした．

二つ目は，サイバー防御の「公助」について，米国で2022年3月に立法化されたCIRCIA（Cyber Incident Reporting for Critical Infrastructure Act of 2022）では，サイバー攻撃を受けた重要インフラ事業者が報告する見返りとして，米国安全保障省の下部機関であるCISA（Cybersecurity and Infrastructure Agency）が救済することが明記された．

三つ目は，ソフトウェアサプライチェーンについて，米国のセキュリティ企業であるソーラーウィンズ社へのサイバー攻撃により，連邦政府機関をはじめ民間企業1万7,000社が被害を受けた．この事件を契機として，NSA（National Security Agency），CISAなどにおいてソフトウェアのサプライチェーン対策に関する詳細なチェック項目を盛り込んだガイダンスが出された．

最後に米国連邦証券取引委員会において，サイバーセキュリティのリスク管理，戦略，ガバナンス等の開示に関する法案が承認される予定である．

こうした動きと三つの論点を踏まえ，安全保障環境の変化やDXの進展等を踏まえた経営者の役割という観点で登壇者からコメントを頂きたい．

＜回答＞

名和専務理事/上級分析官

諸外国におけるサイバー防御の「公助」について，米国国土安全保障省のCISA（Cybersecurity and Infrastructure Security Agency）や国防省のDC3（Department of Defense Cyber Crime Center）では民間企業からの報告に対してフォレンジック調査の支援や対策に資する助言の提供等を実施している．また，英国諜報機関GCHQ（Government Communications Headquarters）に設置されたNCSC（National Cyber Security Centre）も同様な支援を行っている．

この背景には，ビジスネ環境に直接的かつ即時的に影響を与える安全保障環境やDX進展において，多くの企業は，想定されるサイバー脅威に備えるべき対策を十分にできていない．そのため，他の国家は，企業において発生したインシデントによる被害を軽減させることを目的とした「公助」を積極的に行っている．しかし，日本にはこのようなものはない．そのため，経営層は，インシデント発生時において，他国の企業の経営層より高いレベルで，被害を軽減させるための強いリーダーシップを発揮できるようにしておく必要がある．

髙杉サイバーセキュリティ・情報化審議官

交通ISACの加盟は88団体となっている．加盟していない企業等に理由を聞いたところ，経営者が交通ISACのことを知らないという指摘があった．セキュリティについて全体的な底上げを図ることが重要であることから，交通ISACへの加入についてお願いに行く予定である．

平永室長

ロシアによるウクライナ侵攻により，当初，欧州企業を中心にロシアからの撤退が進んだ．“市民自治を尊重する欧州市民社会で，「言論の自由」や「法の支配」の原則を無視する地域との経済交流は制限されるべきである，という流れが生まれた”とするレポートもある．今後も企業経営において，安全かつ速やかにサプライチェーンを切替える，という厳しい判断がなされる可能性を念頭に置く必要がある．平時の段階から，取引先の可視化を行って，代替手段を確保しておくことが重要であると考えている．

また，ソフトウェアのサプライチェーンでは，米国を中心にSBOM（Software Bill Of Materials）の検討が政府を中心に進んでおり，国内でも経産省を中心に議論されている．個社の知的財産権の問題もあるが，有事の際にはセキュリティレベルを下げSBOMを共有するような“共助”の議論が進むことを期待したい．

斉藤部長

サプライチェーンが複雑化するなかで，脆弱性のあるコードが書き込まれた部品をグローバル規模でチェックする作業が大変であったことからSBOMの整備を進める必要がある．

ランサムウェアに感染したら，直接攻撃者と交渉するという人がまだいる．ランサムウェアによる脅迫は犯罪であるので，反社会的勢力とどう向き合うのかという経営問題として，公助的な見方が広まれば良い．

＜質疑応答＞

Q　サプライチェーンについて，どの範囲まで確認する必要があるのか悩ましい．サプライチェーンの可視化が重要あることは理解しているが，ゴールがどこになるのか分からない．

A　公開情報をインテリジェンスに活用するOSINT（Open Source Intelligence）という方法を用いてリスクを洗い出し，リスクの大きさからサプライチェーンの範囲を検討する方法がある．「ゴール」を見出すには，サプライヤーにおいて発生するリスクを定量的に見積もることで得るべきである．これ以外の方法はないと考える．これを実現するためのソリューションとして，IT-VRM（Vender risk Management）と言われる，OSINT手法などを活用して委託先などを継続的にモニタリングしてリスクの評価，緩和，修復を行うことができるようになっている．

A　業界として遵守するべきガイドラインや項目をしっかり定め，契約に織り込み，サプライチェーンの連鎖で着実に基本事項を実施していくことが重要と考えている．但し，より下部の組織への要件の伝達は難しく，取引先で実施が困難なケースやセキュリティ体制が十分に確認できないこともある．個社だけでなく，業界としての遵守事項の整備やレベルアップについて，ISAC（Information Sharing and Analysis Center）等も通じ，啓蒙や教育を行うなど，底上げをしていくことが重要と考えている．

A　自社のビジネスをよく理解し，何がどの程度ビジネスに影響を与えるのかというリスク分析を実施した上で，大きなインパクトのあることころは責任関係を含めて広い範囲を可視化することが重要となる．

本開催概要は主催者の責任でまとめています．

https://www.jttri.or.jp/events/2022/semi220926.html