第79回運輸政策セミナー（オンライン開催）

2021/11/17（水）14：30〜17：00

# 交通サイバーセキュリティ

## 〜DXが進展する企業経営への新たな脅威とリスクコントロール〜

**開催概要**

DX（デジタルトランスメーション）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やオンライン等の進展，安全保障環境の変化など，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，多様化しており，個人情報や機密情報の漏洩，不正送金，工場出荷停止などの事案のほか，海外においては社会インフラを狙った事案も発生しています．

社会のデジタル化が進む中で，経済活動の発展や安全・安心な暮らしの確保を実現していくためには，企業における個別セキュリティ対策の強化はもとより，サプライチェーン全体での対策など，環境変化に対応したサイバー攻撃に対する対策が求められています．

本セミナーにおいては，近年のサイバー攻撃の特徴や企業が抱える課題，政府の新たなサイバーセキュリティ戦略，交通分野に求められる対策などについてご講演を頂きました．

なお，当研究所では，2015年度から5年にわたり，「鉄道，航空・空港分野のサイバーセキュリティに関する調査研究」を実施してきましたが，今回のセミナーはこれを踏まえ，新たな取組みを行うキックオフとして開催しました．

**1. 基調講演**
**DX with Cybersecurity**
**〜デジタル活用の拡大と大規模サイバーセキュリティ災害への“備え”〜**

**講師　後藤厚宏**
情報セキュリティ大学院大学　学長・教授

社会経済活動においてIoTやクラウド等のデジタル技術を広く活用するDX（デジタル改革）の恩恵を享受するためには，サイバーセキュリティの確保を同時並行で進めることが極めて重要となる．

DXの進展によりサイバー攻撃の被害がフィジカル空間まで拡大し，社会経済活動に大きな被害をもたらすようになった．Solar Winds社へのソフトウェアサプライチェーン攻撃では，Microsoft社やCisco社，官公庁などのシステムが乗っ取られた．近年，企業機密の漏洩，製品や部品への不正機能の混入などの事案が発生しており，グローバルサプライチェーン全体での対策強化などが求められている．Colonial社へのランサムウェア攻撃では安全性を確保するために社会インフラである石油パイプラインを停止した．この結果，ニューヨークのガソリン価格が急騰した．公共交通機関において運行（運航）システム以外がサイバー攻撃を受けた場合であっても安全性を確保するために運行（運航）を停止する場合もある．

急速なデジタル化によりインターネット，クラウド，IoTなどへのデジタル依存度が高まっている．米国のクラウド事業者の上位3社が，3日〜6日間事業停止した場合の被害金額は69億＄〜147億＄になると2018年にLloyd's社が試算している．この試算では政府，産業界，市民生活に至るまで広範囲に被害をもたらすことが分かっている．

こうしたことから，社会全体のデジタル化を進める上での「備え」が必要となる．具体的には，サイバー攻撃の被害ハザードマップを作成し，国全体を俯瞰した被害シミュレーションとリスク分析を実施した上で，レジリエンス向上策を検討する必要がある．さらに，データ流通時のプロヴァナンス確保，レジリエンス確保のためのクラウドなどの分散利用，復旧や保守のためのエッセンシャルワーカーの確保，国家としてのサイバー脅威インテリジェンスの強化，CPS（Cyber Physical Systems）における脆弱性DBや国産技術として保持すべきサイバー技術に関する検討などが必要となる．

**2. 講演**
**新たなサイバーセキュリティ戦略について**

**講師　吉川徹志**
内閣サイバーセキュリティセンター　副センター長
（内閣審議官）

新しい「サイバーセキュリティ戦略」が2021年9月28日に閣議決定された．この戦略は3年毎に見直され，前回は2018年7月に閣議決定された．今回東京オリパラの状況を踏まえることになったので9月の閣議決定になった．東京オリパラでは大会運営に影響を与えるようなサイバー攻撃は確認されなかった．東京オリパラの開催に備え，2016年からリスクアセスメントや演習を実施してきた．また，大会期間中のインシデントに備えるために情報共有プラットフォームやサイバーセキュリティ対処調整センターを運用した．

今回のサイバーセキュリティ戦略では，デジタル改革の推進，新型コロナによるテレワークの進展，国家の関与が疑われる攻撃の脅威などサイバー空間を取り巻く課題認識を踏ま

え，「Cybersecurity for All〜誰も取り残さないサイバーセキュリティ〜」という目的のもとに3つの方向性を示した．

1つ目の「DXとサイバーセキュリティの同時推進」では，経営層の意識改革，地域・中小企業におけるDX with Cybersecurityの推進等を具体的な施策としている．

2つ目の「公共空間化と相互連関・連鎖が進展するサーバー空間全体を俯瞰した安全・安心確保」では，安全・安心なサイバー空間の利用環境の構築，デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保，ナショナルシーサート機能の強化等を具体的な施策としている．

3つ目の「国際社会の平和・安定及び我が国の安全保障への寄与」では，自由・公正かつ安全なサイバー空間の確保，我が国の防御力・抑止力・状況把握力の強化等を具体的な施策としている．

**講演**
**「企業利益を損なう結果を招くサイバー脅威」への対策のあり方**

**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

我が国におけるサイバーセキュリティ対策は企業活動を考慮したものが少なくなっている．企業は「営利を目的で事業を行う経済主体」であることを踏まえると，サイバー攻撃から企業利益をどう守っていくのかということが焦点となる．

Twitter社のハッキング事件は甚大な被害をもたらした．これは経営層のサイバー攻撃に対する最新動向に関する認識不足，経営層のセキュリティコントロールに対する強固なリーダーシップの不足などが要因となっている．

日本の多くの経営層は，サイバー攻撃のリスクを単なるIT技術の問題と考えていることから，ITスキルの高い人材の採用やコンプライアンス強化など，小手先の手段で問題が解決できると考えている．しかし，サイバー攻撃から企業利益を守るためには，最新のサイバー攻撃の脅威に適応した包括的なサイバーリスクマネジメントに基づいたセキュリティコントロールが極めて重要となる．

包括的なサイバーリスクマネジメントを実施するには，CSIRTやITセキュリティ部門の権限が組織内だけでなくグループ企業にまで及んでいる必要がある．また，CISOがサイバーセキュリティに関する知識や能力を有しているとともに，自らのリーダーシップにより統治を行うことが重要となる．包括的なサイバーリスクマネジメントを実現するためにはセキュリティに対する投資やヒューマンリソース確保など経営層のリーダーシップが不可欠となる．

**3. 主な質疑応答**

**山内弘隆**
運輸総合研究所所長

Q：ロイズ社のセキュリティ版ハザードマップと同様のものが他にもあるのか．

A：現在調査中である．参考事例として，ロイズ社から電力停電の被害に関する分析が出ている．また米国などでサイバー攻撃がクラウドに及ぼす影響に関する分析がある．個別の分析はあるがハザードマップになっていない．

Q：サイバーリスクに対して企業として取組むべき優先事項は何か．

A：どういう企業から部品調達や保守サービスの提供を受けているのか．サプライチェーン全体を俯瞰した上でリスクの洗い出しと対策の見直しを行うことが優先事項の一つとなる．

A：企業経営上，守るべき情報について洗い出しを行うとともに，その情報が攻撃を受けた場合のビジネスリカバリープランを立てることも重要となる．

Q：IoT機器のパスワードを初期設定のまま使用することでサイバー攻撃を受けるケースが多くなっているが，これをシステム的に防止することは可能か．

A：IoT機器についてパスワードが初期設定の状態のままで使用することができない技術的な仕組みはすでに確立されている．制度的には消費者向けのIoT機器を対象に本年（2021年）イギリスにおいて法的な義務付けが提案された．

A：単純なパスワードや初期設定の状態で使用しているIoT機器について，一定の規律のもと検知して利用者に伝える取組みを情報通信研究機構がサービス・プロバイダと連携して行っている．これは東京オリパラ対応を見すえた期間限定事業であったが，継続的な事業の実施について現在議論している．

Q：ランサムウェア対策についてのプラットフォームなどを用いた対策はあるのか．

A：NISCでは重要インフラグループに対してランサムウェアに関する注意喚起などを行っている．また，「ストップ！ランサムウェア」の特設ページを設けて注意喚起や関係機関の取組みなどについて情報共有を行っている．

Q：東京オリパラで得られた知見やノウハウの活用について具体例を知りたい.

A：東京オリパラのレガシーとしての今後の政策展開について有識者を交えた議論を行っており，年末に報告書を取りまとめる予定である．東京オリパラ開催中の対処や関係機関との調整，リスクアセスメントなどが柱になると考えている.

Q：サイバーセキュリティ保険は考えられるか.

A：サイバーセキュリティ保険は日本でもすでに商品化されている．国によって補償の範囲が異なり，日本ではサイバー攻撃を受けた際の初期対処に関する補償が中心となっている．また，中小企業向けには「サイバーセキュリティお助け隊制度」において安価な掛け金で保険などを提供している.

A：海外のサイバー保険では，ランサムウェアの身代金支払いに対するオプションなどもある．海外では短期成果主義となっていることから経営リスクを極小化するために補償の範囲が広くなっている.

Q：企業間のセキュリティレベルの差異を埋める方策はないか.

A：企業間のセキュリティレベルの差異を分析する手法が定着していない．自社のセキュリティレベルを高める努力を行い，それを自己評価し公開することが重要である.

本開催報告は主催者の責任でまとめています.

https://www.jttri.or.jp/events/2021/semi211117.html