2024. 12. 13（金）14：00～16：30
運輸総合研究所２階会議室 及び オンライン配信（Zoomウェビナー）

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～

主催：一般財団法人 運輸総合研究所　後援：一般社団法人 交通ISAC

1．開会挨拶

宿利　正史
運輸総合研究所 会長

2．講演

サイバー安全保障に関する政府の検討状況やサイバーセキュリティに関する国土交通省の取組

山下　雄史
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

社会インフラを支える製造業におけるサプライチェーンセキュリティの取組 ～サイバーレジリエンスの向上に向けて～

古川　文路
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

対策から組織戦略へ：脅威の変化に応じた持続可能なセキュリティ体制の構築

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

3．パネルディスカッション

モデレーター
後藤　厚宏
情報セキュリティ大学院大学 学長／教授

山下　雄史
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

古川　文路
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

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

4．閉会挨拶

大髙　豪太
運輸総合研究所 主席研究員／事務局長

開催趣旨

冒頭、宿利会長は開会挨拶において「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、本日は通算12回目のセミナーとなります。

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します。」と述べました。

セミナーの概要

■講演①　サイバー安全保障に関する政府の検討状況やサイバーセキュリティに関する国土交通省の取組

山下 雄史　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

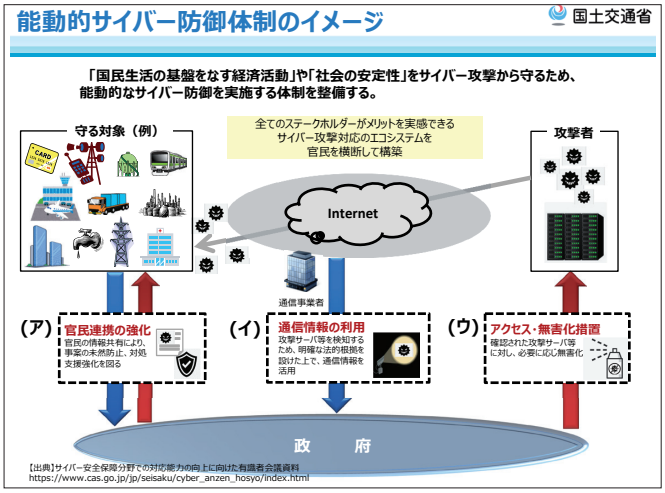
本日は、サイバーセキュリティを取り巻く情勢、能動的サイバー防御、国土交通省の取組についてお話しする。

サイバーセキュリティの重要性について、石破総理は所信表明演説の中で、サイバー安全保障分野での対応能力を向上させるための法案を可能な限り早期に国会に提出すべく、検討をさらに加速することを表明した。これは2022年12月に閣議決定された国家安全保障戦略の中で、サイバー攻撃への危機管理が明確に記述されたことによると考えている。

国家を背景とした重要インフラに対する攻撃が行われ、軍事目的遂行のための手段としてさらに洗練された攻撃が行われる可能性が高いことが指摘されている。

能動的サイバー防御は、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために導入され、今後必要な措置の実現に向け検討を進めることになっている。サイバー安全保障分野での対応能力の向上に向けた有識者会議が2024年６月に設置され、11月に（1）官民連携の強化、（2）通信情報の利用、（3）アクセス・無害化等に関する提言がなされた。

国土交通省では、省内のセキュリティ対策だけでなく、国土交通省が所管する独立行政法人に対してもセキュリティ対策の支援を行っている。また、国土交通省が所管する重要インフラ分野に関する「情報セキュリティ確保に係る安全ガイドライン（2024年４月）」の改定が行われた。このガイドラインでは、重要インフラ事業者における情報セキュリティに係るリスクへの必要な備えや、有事の際の適切な対処等を規定している。また、最高情報セキュリティ責任者が、重要インフラ防護の目的、目指す方向、情報セキュリティ対策において守るべき対象等を明らかにし、情報セキュリティへの取組姿勢を情報セキュリティ方針として規定することなどを盛り込んだことがポイントとなる。さらに、中小企業に対しても、サプライチェーンの観点から自主的にサイバーセキュリティ確保に取組むことが重要であることから、2024年度末を目途に自組織のセキュリティ対策に関する自己点検チェックリストを改定する予定である。



能動的サイバー防御体制のイメージ（山下審議官の講演資料）

最後に航空、空港、鉄道、物流の重要インフラ事業者等が中心となって設立された交通ISACは、平時はセキュリティ対策についての情報交換等を行い、有事の際は迅速に情報共有ができる仕組みとなっている。交通ISACが交通分野全体のセキュリティの中枢としてリーダーシップを発揮していくと考えている。

■講演②　社会インフラを支える製造業におけるサプライチェーンセキュリティの取組～サイバーレジリエンスの向上に向けて～

古川 文路　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

製造業の視点から見たサプライチェーンに起因するリスクとして主に、サプライチェーンからの情報漏洩リスク、サプライチェーンからの不正侵入リスク、サプライヤーの停止による事業継続リスク、ソフトウェアを通じたサプライチェーンリスクの４つが挙げられる。このようなリスクに対応するために、経済安全保障推進法には基幹インフラ役務の安定的な提供の確保に関する制度が設けられている。重要インフラ事業者の特定重要設備については、それぞれの所管官庁に、調達に関する情報やそのリスク管理措置をまとめた計画書を提出しなければならず、その作成のためにはサプライチェーン全体での対策が必要となる。

EUのサイバーレジリエンス法は、製造業者に対してデジタル要素を持つ製品等のセキュリティに関するリスクアセスメントや脆弱性の管理、インシデント報告などを求めるものとなっている。また、この法律に違反した場合、高額な制裁金が課せられる。

東芝グループでは、インシデントの影響を最小化し、早期回復、事業継続を可能とするサイバーレジリエンス戦略を実施している。東芝グループにおけるサプライチェーンセキュリティに関する主な取組について以下のとおり紹介する。

1）セキュリティガバナンス運用体制の構築　東芝では、サイバーセキュリティリスクをガバナンスする東芝サイバーセキュリティセンター（東芝SIRT）を設置し、グループ全体に対して一貫したセキュリティ対策を実施できるようにしている。

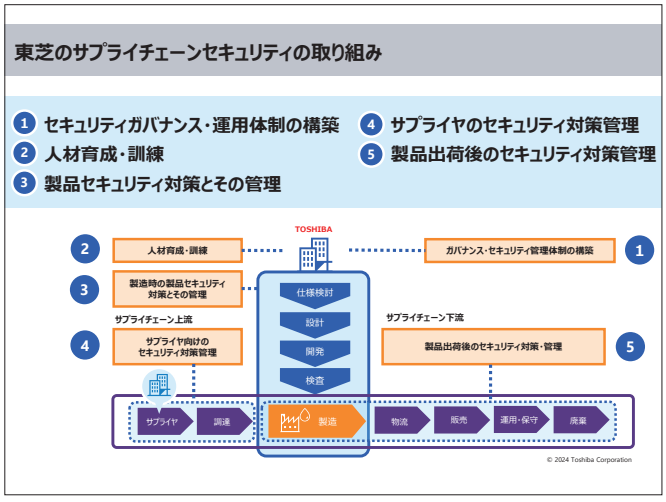
2）人材育成・訓練　セキュリティ対策を進めるためには、社員の意識向上、人材の育成、サプライチェーン全体のリテラシーの向上が重要となる。経営層、グループ社員、取引先の社員の３層に分けて人材育成カリキュラムに基づく教育訓練を推進している。

3）製品セキュリティ対策とその管理　製品の開発の各フェーズにおいて確認すべき事項をまとめたグループ共通のガイドラインや製品セキュリティチェックリストを整備している。また、東芝SIRTのメンバーが事業部でワークショップを行い、ガイドラインの普及と啓発に努めている。

4）サプライヤーのセキュリティ対策管理　製品開発に携わる取引先に対して、具体的なセキュリティ要望事項を定めたセキュリティ品質保証ガイドラインに基づく自己点検や攻撃リスクを客観的に評価するアタックサーフェス調査を実施するとともに、相談窓口の設置やセミナーの開催を通じたリテラシー向上に努めている。

5）製品出荷後のセキュリティ対策管理　SIRT支援システムにより脆弱性ハンドリングを可視化し、インシデント発生時は、東芝SIRTとグループ会社のPSIRTが連携し迅速な対応を目指している。

東芝グループからの情報発信として、毎年６月頃にサイバーセキュリティ報告書を発行している。また、四半期毎のCISO会議の開催、社外の専門家による勉強会を開催するとともに、サイバーセキュリティに関して情報交換や業界団体等での講演活動や教育、啓発活動も積極的に行っている。



東芝のサプライチェーンセキュリティの取組（古川部長の講演資料）

■講演③　対策から組織戦略へ：脅威の変化に応じた持続可能なセキュリティ体制の構築

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

本日のセミナーでは、脅威の変化に応じた持続可能なセキュリティ体制の構築についてお話ししたい。

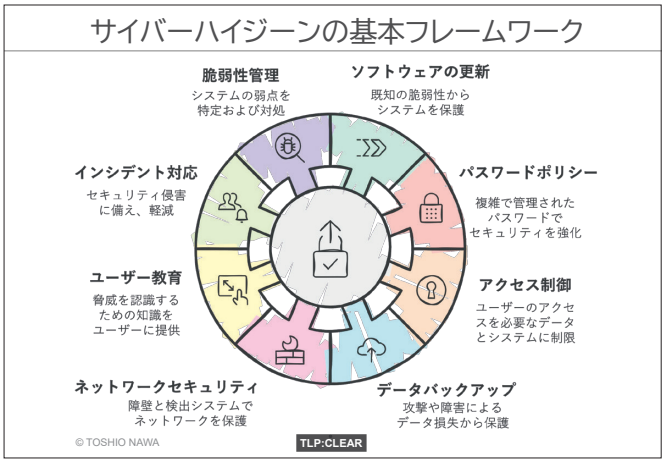
近年、AI駆動型サイバー攻撃が増加している。この攻撃は、攻撃ターゲット毎に高度にカスタマイズした攻撃を大規模に行うマスカスタマイゼーション、人間の認知や反応を超えた攻撃速度、機械学習モデルの活用により予測困難性を有している。具体的には、①高度な音声や映像の偽造による攻撃、②環境に適応し進化する自立型マルウエア攻撃、③高度に洗練されたDDoS攻撃、④AIシステムを標的とした攻撃、⑤未知の脆弱性の早期発見による攻撃などが可能となる。

こうしたことから防御側も人間をサポートするAI補助型のセキュリティオペレーションの導入、従来の事後対応型から予防防御型セキュリティアプローチへ移行、相互に学習・適応するエコシステムの導入*1）等が必要となる。

さらに、AI駆動型サイバー攻撃に対して、経営層や戦略的意思決定者が組織全体の長期的な目標や方向性等を包括的に定める組織戦略を示し、これに基づきサイバーハイジーン*2）を実践することが重要となる。AI駆動型サイバー攻撃への脅威に対応するための組織戦略について主なものは以下のとおりとなる。

①機械学習を活用したセキュリティの強化	②ゼロトラストアーキテクチャの重要性
③多層防御戦略の再構築	④脅威ハンティングの進化
⑤インシデントレスポンスの高度化	⑥セキュリティオーケストレーションの実施
⑦人材育成とスキル開発	⑧法的・倫理的課題への対応
⑨サプライチェーンセキュリティの再考	⑩新たなクラウドセキュリティへの対応
⑪量子コンピューティングがもたらすAIサイバーセキュリティへの影響	

近年、高度化したサイバー攻撃が増加し、攻撃手法も多様化していることから、予防的対策、インシデント対応計画、定期的なトレーニング、知見の共有などが重要となる。



サイバーハイジーンの基本フレームワーク（名和専務理事の講演資料）

■パネルディスカッション

【総括】

後藤 厚宏　情報セキュリティ大学院大学 学長／教授

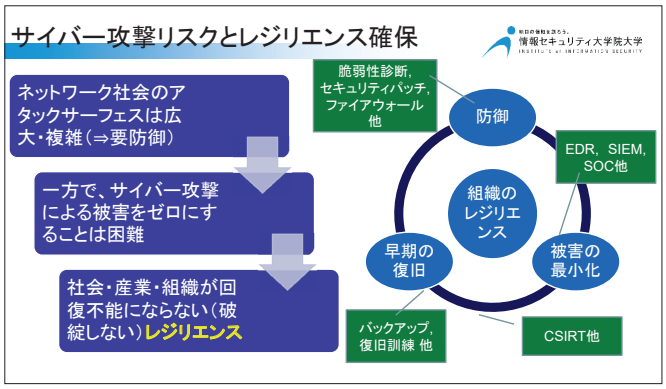
被害の波及と増幅という視点からサプライチェーンへの攻撃を見ていきたい。昨年（2023年）発生した名古屋港のランサムウェア攻撃事案では、船舶37隻、コンテナ約２万本に影響が生じ、中京地区の自動車やアパレル産業に大きな被害を及ぼした。また、自動車の主要部品を生産するベンダーへのサイバー攻撃では、完成車１万３千台の生産が停止した。米国のソーラーウィンズ社へのサイバー攻撃では、米国政府機関や企業など

*1）複数のセキュリティ防御システムやツールが連携し、互いに情報を共有しながら学習し新たな脅威に対応するセキュリティ体制
*2）日常的に実行すべき基本的なセキュリティ対策の集約であり、システム防御の強化するためのベストプラクティス

1万8千組織に影響をもたらした。クラウドストライク社へのサイバー攻撃では、ウィンドウズシステムを導入している850万台のPCが影響を受け、その影響でデルタ航空では航空機の運航が停止した。Log4jの脆弱性に対する攻撃では数えきれない被害が生じている。

サプライチェーン攻撃は、調達から出荷まで広範囲に波及被害を及ぼすことから経営的視点でリスクをみる必要がある。また、産業全体でみた場合、川上産業から川下産業まで波及被害が及ぶことから政策視点でリスクをみる必要がある。

ネットワーク化により無限に広がったアタックサーフェスをしっかり防御することが重要となるが、どんなに対策を講じてもサイバー攻撃のリスクを完全に排除することは難しくなっている。こうしたことから、サイバー攻撃を受けても社会や産業、組織が復旧・回復できるレジリエンスが重要となる。



サイバー攻撃リスクとレジリエンス確保（後藤学長の講演資料）

【ディスカッション】

（後藤学長）

サプライチェーンのリスクと対策についてお聞きしたい。

（古川部長）

サプライヤーがリスクを自分ごととして捉え、ガイドラインやルールの実践を徹底することが重要となる。サプライヤーに対して説明会の実施や、自己点検だけでなくアタックサーフェス調査による検証等を行っている。

（後藤学長）

ランサムウェア対策としてバックアップが一般的となっているが、バックアップからの復旧訓練はあまり行われていない。

（名和専務理事）

演習を通じて把握された課題を、誰が、いつまでに、どこまで改善するのかを明確にし、次の演習までに着実に改善していくことが重要となる。日本の公的機関が実施している演習は、単年度開催となっているので、この流れができない。

（後藤学長）

企業では利益を優先するあまり、セキュリティが軽視されることもあるが如何か。

（名和専務理事）

金融機関では内部統制を行うためにスリーラインモデルを採用している。第一線は業務計画、第二線はリスクマネジメントとなる。視点が異なる二つのラインでそれぞれ検討し、最終的に経営課題として議論する必要がある。

（山下審議官）

サイバー攻撃も災害と同様に捉えていく必要があるのではないか。災害では、詳細なシナリオに基づき訓練を行い、訓練で把握された課題は改善策として反映される。サイバー攻撃による被害の復旧対応は専門的な知識や技術が必要になるが、国民生活への影響は災害と共通する部分もあるのではないか。

（後藤学長）

サイバー攻撃の場合、法律が整備されていないため、自衛隊、警察、自治体などの関係者が動きづらいという意見もある。

（山下審議官）

災害対策法では対象となる災害の名称が明記されている。同法の対象になると災害救助法に基づき救助活動や食料支援などが行われる。

（後藤学長）

資金や人材が限られる中小企業のサイバー対策をどうするべきか。

（古川部長）

リスクがどこに存在するのか分からないというサプライヤーもあるので、リテラシーの向上に資する取組を強化する必要がある。

（名和専務理事）

資金がないとセキュリティソリューションを導入することができない。東京都中小企業振興公社では、サイバーセキュリティ対策促進助成金制度がある。他の地方自治体や公的機関でも同様の制度がある。「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築について」が公正取引委員会から出されている。

（後藤学長）

自動車産業は裾野が広がっていることから、下請け事業者の意見などを取込み、ガイドラインを制定・改訂している。持続可能なサイバーセキュリティ体制の構築について如何か。

（名和専務理事）

欧州の事例として、サプライチェーン攻撃の殆どがIDとパスワードの窃取から始まることから、これを強固なものにするなど管理を徹底すること、セキュリティパッチを迅速に適用するなど脆弱性管理を厳格に行うこと、企業のトップが自らの言葉で繰り返し注意喚起を行うことが重要である。

（古川部長）

サプライチェーンセキュリティは、１社だけでは実現できず、産業界全体で取り組む必要がある。政府のセキュリティ施策の実効性を高めるために、ガイドラインや基準を政府や重要インフラ事業者の調達要件に組み込むことや、施策を評価するための認証制度などの仕組みが必要。こうした取組みは、企業側のコスト増につながるので、政府の支援や何らかのコスト負担の仕組みが求められる。

（名和専務理事）

米国や欧州では、官側がリーダーシップを発揮し、存在感を示すことが成功の要因となっている。

（山下審議官）

官民の情報連携を円滑に行うために、人的な要素は重要であるが、それだけに依存しない仕組みを構築することも重要となる。交通分野では、交通ISACがあるので官民連携のあり方について意見を伺っていきたい。

当日の講演資料等は運輸総合研究所のWEBページでご覧いただけます。
https://www.jttri.or.jp/events/2024/semi241213.html