October 5th, 6th, 2017

Cyber3 Conference Tokyo 2017 Summary

開催概要

開催日	2017 年 10 月 5 日（木）、6 日（金）
会　場	慶應義塾大学三田キャンパス
主　催	日本経済新聞社、日経 BP 社
共　催	慶應義塾大学サイバーセキュリティ研究センター 独立行政法人情報処理推進機構 国立研究開発法人情報通信研究機構
協　力	一般社団法人日本サイバーセキュリティ・イノベーション委員会（設立準備中）
企画協力	PwC Japan グループ 世界経済フォーラム（WEF）
本会議座長	齋藤ウィリアム浩幸（内閣府参与、経済産業省参与）
後　援	サイバーセキュリティ戦略本部、総務省、外務省、文部科学省、経済産業省、防衛省、警察庁、個人情報保護委員会、一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)、駐日英国大使館、在日フランス大使館、駐日イスラエル大使館経済部経済貿易ミッション、オランダ王国大使館、シンガポール共和国大使館、米国大使館商務部、INTERPOL、InterNational Cyber Security Center of Excellence (INCS-CoE)＝慶應義塾大学、東京大学、早稲田大学、東京電機大学、情報セキュリティ大学院大学、九州大学、スタンフォード大学、ノースイースタン大学、メリーランド大学ボルチモアカウンティ校、ハーバード、マサチューセッツ工科大学、カーネギーメロン大学、ジョージア工科大学、デラウェア大学、ケンブリッジ大学、インペリアル・カレッジ・ロンドン、ユニバーシティ・カレッジ・ロンドン、ロンドン大学ロイヤル・ホロウェイ校、クイーンズ大学ベルファスト

Executive Summary and Proposal

今年の Cyber3 のテーマは「2020 and beyond」。東京 2020 オリンピック・パラリンピック競技大会（以下、「東京 2020 大会」）を契機とした将来のサイバーセキュリティのあるべき姿を議論した。Cyber3 では、グローバルや日本の産官学のマルチステークホルダーが集まり、各自の領域を超えて新しい時代に向けた議論を実施した。今回は人材育成も主なテーマの 1 つであった。また、今年は慶應義塾大学サイバーセキュリティ研究センターが主催する第 5 回サイバーセキュリティ国際シンポジウムも同時に開催した。

- Society5.0（IoT 等のテクノロジーでサイバー空間と物理空間が高度に融合される超スマート社会）を実現するためには、様々なデジタルトランスフォーメーションを推進するとともに、それに伴うセキュリティに係る組織的な対応を強化する必要がある。

- サイバーリスクが拡大しており、サイバー攻撃に企業単独で対応することには限界がある。特に中小企業ではサイバーセキュリティの専門家を採用することは難しいため、政府の積極的な支援のもと、産学官が一体となった対応を図る必要がある。

- 更なる高度なサイバー攻撃を受ける可能性もあるため、攻撃者の動機・意図の分析結果に基づくプロアクティブな対抗策の検討・共有に向けた脅威情報管理の取組や事業継続計画（BCP）等を考慮した組織としてのレジリエンスを考える必要がある。

- サイバーセキュリティにはリーダーシップの発揮と情報共有の仕組が求められる。Cyber3 の議論を通して、今後の取組へ繋げていくことが重要である。

Background

1972 年のミュンヘンオリンピックは、物理的なセキュリティを見直すきっかけとなったと言われているが、東京 2020 大会はサイバーセキュリティの確保が不可欠である。サイバー攻撃の高度化・巧妙化に対して、国の政策、企業経営者の認識の向上ともに、官公庁や企業による官民連携及び各国間のコラボレーションが求められる。

安倍首相・米国トランプ大統領との会談、安倍首相・英国メイ首相との共同声明でも、サイバーセキュリティの問題が取り上げられている通り、米国・英国においてサイバー空間における国際的なパートナーシップの重要性は非常に高まっている。

信頼できるサイバー空間の構築には、各国間のパートナーシップに加え、政府・産業界との官民連携が不可欠である。英国ではサイバーセキュリティセンター（NCSC）を政府主導で立ち上げ、官民・国内外のパートナーシップのもと、現在では 100 以上の業界団体に対してサイバーセキュリティに関する情報共有を行っている。

政府がリーダーシップをとり、産官学の間で連携を行い、国際的な広がりのもとで、ベストプラクティスを共有していくことがサイバー対策として重要である。

Connect Track

Connect Track では、あらゆるモノがインターネットにつながる IoT の普及によって、様々なリスクが生じるため、どのようにサイバーセキュリティを確保するかが議論された。

IoT が普及すると、異なるシステムの連携による仮想的な統合システム（System of Systems）が構築され、今までの情報システムとは異なり、デバイス、ネットワーク、プラットフォーム、サービスの各レイヤーにセキュリティ対策が必要となる。このセキュリティ対策においては、「脆弱性対策に関する体制の整備」、「研究開発の推進」、「民間企業等におけるセキュリティ対策の促進」、「人材育成の強化」、「国際連携の推進」の 5 つの柱をマルチステークホルダーの協力により一体的に推進することが効率的である。

サイバーセキュリティでは、「レジリエンス」を考えなければならない。従来の考えとは異なり、問題発生を予防するより、発生した問題状況からどのように復旧を図っていくかに力点を置いた概念が重要となる。日本ではリスクゼロが良いとする文化があるが、サイバーセキュリティにおいては、ゼロリスクということはあり得ない。セキュリティインシデントを防ぐことは当然重要であるが、その後の対策展開、さらにその共有こそがより重

要である。

金融分野では現在 Open API が注目を浴びている。Open API の利活用は安全性と利便性を両立して実現する必要がある。金融機関・Fintech 事業者や利用者それぞれの用途・目的に応じた安全なアクセスを実現するセキュリティレベルが担保されなければならない。Open API の成功に向けたキーワードは、「確実なアクセスコントロール」、「関係者によるコミュニティの確立」、「規制やガバナンスの強化」の 3 点である。

「Society 5.0」では、データベースやサービスレイヤーを統合し、新たな価値やサービスを創出する。ビッグデータ、AI、サイバーセキュリティ等がこれらのテクノロジー基盤となる。世界では「インダストリー4.0」が用いられるが、日本では「人」にフォーカスするため「Society 5.0」を用いている。データドリブンな原理に基づくため、データの機密性、可用性、完全性はもちろんのこと、データ間の整合性も重要になる。

Society 5.0 では、人、データ、デバイスは全てオブジェクトとして捉えており、これらがオブジェクトとして認証されるメカニズムのもとで、初めてシステム全体の信頼性が確保される。Secure by Design や Privacy by Design というアーキテクチャー、アクセス権限をコントロールするルール等を構築する必要がある。

AD（自動運転車）、EV（電気自動車）、CC（コネクテッド・カー）の 3 つを組み合わせることで非常に高いレベルのモビリティ・サービスが実現可能となる。モビリティの進化のみに目を奪われるのではなく、あらゆるビジネスセグメントが連結して展開される利便性の高いサービスを開発していく必要がある。安心・安全に対する高い意識を持ち、車を含めた高品質な社会インフラを誇る日本では、自動運転車の核であるディープラーニングについても厳しいチェックを受けるだろう。しかし、このような環境で研鑽を積むことが、日本をこの分野のリーダーたらしめ、競争力のある生活に密着したテクノロジーを生み出す原動力となるのである。

Crime Track

Crime Track では、サイバー犯罪の動機や目的、官と民それぞれの役割と責務に焦点を当て議論を行った。議論の中では主に「実行可能な脅威情報の収集メカニズムの構築」、「官民連携の信頼関係の構築」の 2 つの必要性が指摘された。

サイバー犯罪は常に進化しており、サイバー空間と現実世界（Real World）を融合させた犯罪も増えてきている。一方、意識啓発はまだ不足しており、対策や協力も強化する必要

がある。攻撃者目線に立ち、各組織にとって実行可能なサイバー脅威情報の分析・共有を行っていくことが求められている。

サイバー攻撃者は、オンライン犯罪者、ハクティビスト、テロリスト、国家等、様々な動機や目的を持っている。サイバー攻撃の裏に「誰が」いるのかだけではなく、「なぜ」、「何を」、「どうやって」攻撃してくるのかという背景も特定する必要がある。

企業の経営層は、個人情報漏えい、事業停止、物理的損害等のサイバー犯罪の深刻さを理解し、適切にリスクアセスメントを実施しなければならない。IT 部門に依存するのではなく、適切な予算をセキュリティ人材やサイバー保険等に配分すべきである。

サイバーセキュリティにおいて、政府の役割や責任を拡大すべきという議論があるが、企業は法規制や業界ガイドラインには自らが準拠するための準備をしなければならないことを認識すべきである。政府は、情報共有や研究を推進するための重要な役割を果たすことができる。

産官学が信頼関係を構築することが重要である。政府は、法規制や制裁を設定することができるだけではなく、民間企業とプロアクティブに情報を共有することができる。より高度な情報共有が求められており、実行可能な脅威情報や期待する結果を具体化する必要がある。

サイバーセキュリティとは、本質的にはテクノロジーでなく、政策や施策に係るものであるが、そこにギャップが生じている。特に日本では、Society 5.0 を目指している一方で、政策が追い付いていない。IoT 時代の最初のオリンピックを東京で開催できるため、政府や民間企業は法規制やサイバーセキュリティを提供するための絶好の機会ととらえるべきである。

Security Track

Security Track では、技術（人工知能；AI）、法規制、人材育成の 3 つの観点で、サイバーセキュリティについて議論した。

AI は、ログ監視において発生するアラート等を効果的に絞り込む異常検知の分野等で、セキュリティアナリストの作業負荷を低減し、本来求められる専門性の高い分析活動に注力することを可能とするためのツールとして既に活用されている。また、アラートを発見した後のオペレーションプロセスにも活用用途がある。

サイバー攻撃を検知するためのログ監視水準は、今後より高度化することが想定されるため、AI やディープラーニングの重要性も高まることになる。AI やディープラーニングを有効活用するためには、技術アルゴリズムに精通し、セキュリティアナリストと双方向にコミュニケーションできる AI 専門家の存在が不可欠である。

日本では新たな技術が登場した場合、ルールのフィージビリティを検討するより、規制の適用を優先する傾向があるが、もっと自発的に技術の活用を阻害しないルール作りに関与すべきである。

Secure By Design を要件としたシステム開発においては、要件定義だけではなく、テスト環境もこれを担保しなければならず、コストとセキュリティのバランスが重要になってくる。セキュリティ要件を充足した組織によるセキュアな製品の開発・製造を担保するセキュリティクリアランス制度が今後必要になる。

データ保護に係る法律は各国で様々に整備されているため、国境を越えてデータが移動する時、その正当性を判断することが難しい状況である。直近でのプライバシー規制では 2018 年に施行される EU の GDPR があるが、認知度は依然として低く、完全に準拠している企業は少ない。

日本企業は、個人情報の範囲に生体認証情報、運転免許証、クッキー情報や IP アドレス情報も含まれることがあり、地域や国によって個人情報の定義が異なることを認識しなければならない。

プライバシー規制対応では、ビジネス要件の整理、プライバシー影響評価、プライバシーバイデザインが重要なポイントであり、オーナーシップを持つ人材を経営層に配置すること、予算の適切な配分を行うことが重要である。

日本では最高情報セキュリティ責任者（CISO）は兼任する方が多い。CIO はアクセラレーターだが CISO は抑制者であるべきであり、CISO が CIO を兼務することは本来の役割の上で適切ではない。企業によって、組織体系は異なるが、セキュリティポリシーの中で責任範囲を明確にしておく必要がある。

Next Actions

経済産業省では、2020 年以降の経済発展や国民生活の向上を見据え、「Connected Industries 東京イニシアティブ 2017」を先日発表した。人、モノ、技術、組織等が様々につながることにより新たな価値創出を図る「Connected Industries」の概念の実現に欠かすことができないのがサイバーセキュリティであり、企業においては安心・安全にデータの利活用を行えるようにすることが重要である。また、経済産業省と IPA 産業サイバーセキュリティセンターは、米国国土安全保障省や ICS-CERT との共同のサイバー演習を始め、欧米のトップレベルの専門家との連携を進めており、今後も継続して協力を行っていく。

重要インフラへのサイバー攻撃は、サイバー分野だけで対策を考えるのではなく、グローバルな問題としてあらゆる国レベルで話し合い、連携をしていくことが必要である。既にサイバーセキュリティは、技術的な課題ではなく、国家安全保障や政策・戦略に関する課題となっている。サイバーセキュリティの確保のためには、新しい制度、新しい法律の制定が必要となっている。また、セキュリティとプライバシーの相反関係、イノベーションとセキュリティの相反関係を解決する必要がある。

全ての ICT 施策において、サイバーセキュリティは基礎になる。東京 2020 大会に向けて、確実に脅威は存在し拡大していくため、対策を取っていかなければいけない。テクノロジーの変化は 1 年単位で発展する。東京 2020 大会まであと 3 年であることを考えると、3 世代、4 世代先となるため、誰も将来を明確に予測することはできない。よって何よりも、人と組織の成熟度を高めることが重要である。

東京 2020 大会は、IoT や自動走行といった新しいショーケースが社会に浸透した状態で実施される初めてのオリンピックであり、リスク評価やセキュリティ対策を実施することが重要である。オリンピックのような世界的なイベントは、攻撃者にとっても魅力的なマーケティングチャンスでもある。開催を妨害することで、攻撃スキルを宣伝することが可能なため、こうしたリスクも視野に含めた対策検討が求められる。

政府が注力するテーマは、次の 5 つである。「IoT のライフサイクル全体を見渡した対策」、「産学連携による研究開発を通したセキュリティ知見の拡充」、「民間企業へのセキュリティ投資奨励」、「人材育成の強化」、「国境を越えたサイバー攻撃に対する国際連携」である。

サイバー空間・物理空間が融合された Society5.0 の実現にはサイバーセキュリティが不可欠である。サイバーセキュリティの確保のためには、政府と民間企業が信頼関係を構築することが重要である。また、最適な政策の意思決定を行うためには、専門家や研究者の関

与も必要である。現在、サイバーセキュリティの専門家が不足しているが、人材は重要な要素であるため、人材育成を強化しなければならない。

サイバーセキュリティ対策の力点は、データの機密性から、データの完全性・可用性へ移行し始めている。攻撃者がどのような意図で、どのような行動を実施するのかという想像力を活かして最適な防御方法を考えなければならない。

直近一年でも、フェイクニュースによる選挙への影響、国家支援を受けたとされるランサムウェアによるサイバー攻撃、Equifax のデータ漏えい、金銭的利益を得るための金融市場操作等が発生している。仮に 5 年後も同義の＜サイバー＞カンファレンスが開催されているようであれば、現在とは全く違ったテーマや課題を議論しているであろう。

Documentation:

pwc Urban Connections