エグゼクティブサマリーと提言

- あらゆるものがデジタル化され、インターネットに接続されると、サイバー犯罪などの脅威（Internet of Threats）が激増する。サイバーセキュリティの確保のためには、業界連携、官民連携、国際連携が不可欠である。

- マルチステークホルダー間の連携を推進するために、情報共有のインセンティブを設けるとともに、Need to Share のマインドセットを浸透させ、円滑にサイバーに関する脅威情報を共有する仕組み構築が求められる。

- 政府機関には、国際的なルールの整備、法規制やガイドラインの整備や推進など、サイバー空間に関するフレームワークを構築することが求められる。

- 各企業には、自らの責任としてサイバーセキュリティに取り組む自助努力が求められる。そのためには、セキュリティマインドをもった企業経営が必要である。経営者は、サイバーセキュリティ対応を「費用」ではなく「投資」と位置づけ、サイバーリスクを適切に把握し、効果的な投資判断することが求められる。

- 企業規模に関わらずセキュリティ対応を推進するために、大企業が中心となり子会社や関連会社、および中小企業などのサプライチェーンにもセキュリティを浸透させていく必要がある。

- セキュリティ人材が質的・量的に不足しているため、社会のニーズにあった人材の底上げ、およびグローバルで通用する人材の育成が必要である。AI などのテクノロジーにより、人材不足を補うことも検討すべきである。また、経営層と現場とのコミュニケーションを円滑にするため、サイバーに関するリスクを技術用語ではなく、ビジネス用語で対話することが求められる。

- 高い品質（ジャパンクオリティ）などを活かした日本独自・日本発の第4次産業革命を興すことは可能である。これを実現するために大きなモメンタムを起こさないといけないが、企業の自助努力では限界があるため、政府がリーダーシップを発揮する必要がある。東京 2020 大会を契機として、産官学が協力して、成長戦略を推進していく必要がある。

背景

Cyber3 conference は、データの支配が進む世界的な環境の変化を受けて、マルチステークホルダーがサイバーセキュリティに関連する課題を協議する場を提供する。相互接続性（Interconnectivity）の増大がもたらす影響、この接続性の変化に伴うサイバー犯罪の増加、そしてセキュリティ面の課題という、互いに密接に関連する 3 分野について議論した。

自動運転車の登場に伴い、車車間通信および車とスマートフォンなど他の機器との通信に配慮する必要がある。異なる種類のモノが通信を行う場合、責任範囲を明確に定義しセキュリティを確保する必要がある。日本政府はサイバーセキュリティ戦略、および「安全な IoT システムのためのセキュリティに関する一般的枠組み」を策定した。これは、各業界向けの標準的なメタフレームワークであり、関係諸国とともに同枠組みを国際基準として提案していく予定である。

産業構造・社会構造のグローバルな変化がデジタル技術の導入を促しており、政府は、技術だけでなく運用ノウハウを重視して、こうした広範な課題に対処する統一的アプローチとして超スマート社会（Society 5.0）を提唱している。IoT の急激な拡大は、社会が大きく依存するライフラインに数多くの新たなサイバー脅威をもたらす。日本経済団体連合会は、この分野で政府の活動に貢献するサイバーセキュリティ強化のための政策提言を行った。

Connect Track

インターネット接続された世界には、大きなチャンスと同時に甚大なリスクがある。官民提携を通じてのみこれらを解決し、リスクへの理解を深めることができる。また、技術変化のスピードは飛躍的に進化する傾向があるため、今後 5～10 年で計り知れない変化が生じることに注意する必要がある。

ビジネスの最前線での自動運転車の問題として、自動運転車の性能評価基準の確立、公的/社会的インフラの構築、法規制やガイドラインの策定などが挙げられる。ドライバーの責任で運転するレベルの自動走行については、インフラがすぐに整備されるだろう。だが、システムが完全に制御するレベルの自動走行に関しては、国内のみならず国際的な議論が必要になる。IT 業界の取り組みをお手本として、自動車業界は独自のセキュリティ要件を策定すべきである。AI システムの信頼性・正確性という意味では、自動車メーカーやサービス提供者の責任範囲を明確化することも課題である。

IT と OT（Operational Technology）のリスクの違いを、明確にする必要がある。特に OT は、物的被害による経済的損失のリスクだけでなく人の命が危険にさらされるリスクも伴う。サイバーセキュリティ保険市場はまだ発達しておらず、この分野には対処すべき課題が多く残る。データ管理の法規制は国や地域によって異なる。これは困難な分野であり、地域毎に環境に応じた独自の政策を実施しているため調整が十分実施されていない。様々な地域において、行動に対する責任から身を守る方法を考える必要がある。想定されるリスクに伴う費用と、そのリスク軽減に必要な投資を評価すべきである。社会的インフラに影響が生じるおそれがある分野では、このニーズを考慮に入れねばならない。

現在の IoT 分野は機能性が重視され、セキュリティが軽視されている。そのため攻撃対象領域が爆発的に増えている。スマート都市に移行している国もあるため、砂上の楼閣ではとの懸念がある。セキュリティを含め、IoT の標準化が必要である。安全な IoT は国際的な競争の中で強固な立場をもたらし、持続可能な経済成長の実現を可能にするため、これは成長への投資とみなすことができる。IoT の未来には、セキュリティ専門家の育成とユーザーの基礎知識拡充に向けた教育が欠かせない。サイバーセキュリティは我々の国と子どもたちに影響を与えるリスクであるとの市民の意識啓発を通じて、情報共有に関する慣行や考え方を変えていく必要がある。

企業は、ビッグデータを活用して生産性を高め、新たなビジネスチャンスを作り出す可能性はあるが、これを実現するために大きなモメンタムを起こさないといけない。この分野は、企業の自助努力では限界があるため、政府がリーダーシップを発揮する必要がある。また、インターネットの黎明期には多くの企業が新しいアイデアを競って実装したように、AI やビッグデータを民間企業が早期に実装（Implementation）する必要がある。例えば、将来的にはビッグデータと AI を利用して新たな保険サービスを開発することも可能である。既に、電力会社のガスタービンのビッグデータ（500GB/日）分析を通じて、故障を予測できるようになった。ビッグデータの利活用により、疑わしい異常な活動の検出を含め多様な分野で正確な予測を行える。企業内では自動化できる多くのポジションが AI に取って代わられ、人間の操作者の必要

性が減っている。日本のビッグデータ/AI ソリューションを輸出する際は、高い品質（ジャパンクオリティ）が有効な結果を導き出し、重要な差別化要因のひとつになる。日本型の組織構造（現場の権限の大きさ）も、日本の強みになっている。ネットからビッグデータを集めるには、規範と標準化が必要になる。

CrimeTrack

CrimeTrack では、サイバー脅威に関する状況認識強化に向けた情報共有、集団的防御の強化、法執行能力の強化といった前回の Cyber3 conference の成果を基盤として議論を行った。脅威の急激な進化に応じて、対策も進化させねばならない。有用な情報の共有を阻む障害を分析する必要もある。

サイバー犯罪の大半が国境を越えたものであるため、国際協力が欠かせない。サイバーリスク管理のため、現在システムセキュリティ監査などの重要性が高まってきている。政策的対応と「個人情報」の内容を検討する必要がある。アウトソーシングなどにより内部攻撃のリスクが高まっているため、内部の攻撃から企業を守るためのベストプラクティスも実施しなければならない。サイバー犯罪の進歩に合せ、サイバーセキュリティの対策基準やガイドラインを定期的に見直す必要がある。基幹インフラが含まれる場合も多いため、サイバーセキュリティと国家安全保障は密接に結びついている。政府はこの点に注意を払うべきである。金融機関は最も重要な基幹インフラのひとつであるため、大手においては比較的高い水準で対策がなされている。しかし、中小の金融機関においては、そうしたレベルに達していないところも散見され、早急な対応が望まれる。新技術が開発されてから対応すると遅すぎるため、新たな技術やリスクへの対応策を事前に検討しておかねばならない。

サイバー攻撃者の能力と官民のセキュリティ慣行の間に大きなギャップが存在している。犯罪者には、犯罪者コミュニティの信頼関係を活かして情報を手に入れる能力がある。他方で政府・民間部門のサイバーセキュリティ管理は得てして細分化し縦割り方式で運営されており、多くのサイバー犯罪は記録に残されない。加えてレガシーIT は、更改と防御が非常に難しい。権力の分散が起きており、国家アクターから非国家アクターに権力が移っている。民間部門のレジリエンスを高めるため、民間での連携・情報共有に向けた自発的な枠組みや仕組みが求められる。

サイバー脅威に対抗する上で、ベストプラクティスに関する情報共有が業界全体にメリットをもたらすことに、ほとんどの企業が賛同している。企業間のビジネス競争を繰り広げる一方で、脅威に関する情報は積極的に共有を望んでいる。脅威情報を共有するベンダーが増えれば、業界全体のメリットも大きくなる。セキュリティ面では、業界を越えてソリューションに一貫性がある場合が多い。だが、そのセキュリティソリューションを使いやすいものにすることが課題である。トラストアンカーが重要であり、アンカーの考え方を標準化する方法について議論する必要がある。また、ルール義務化やそのための国際的な合意形成の方法についても、継続して議論する必要がある。

AI とロボティクスの進化により、現在はロボットが自律的に情報を収集し発信できる。サイバー世界と現実世界の境界が消えた。今では、サイバーテロや物理的なテロを通じて電力供給を止めることができる。サイバー技術を利用できる強者と、利用できない弱者の間にギャップが生まれるだろう。インターネットとサイバー技術に関しては、国家は既に弱者になっている。

SecurityTrack

セキュリティトラックでは、サイバー攻撃の増大化・巧妙化による影響を踏まえ、サイバーセキュリティにおける課題について議論した。

近年世界で起きた数々のインシデントから、何が起きても不思議はなく、想定外の出来事に驚いてはらならないことが分かる。未来は予測できないが、インシデントが発生した際に文化・言葉の違いが意志疎通の問題につながらないよう準備しなければならない。攻撃の隙を作らないため、様々な課題に対し明確な当事者意識が必要になる。対策の多くを民間部門が実施する必要があり、信頼の問題が生じるため、早い段階で信頼関係を築かねばならない。関係構築に加え、ギャップを発見するためテストとリハーサルを行う必要がある。オリンピック・パラリンピック競技大会は、特定の期日と共通の目標に基づき適切な対応に注力する格好の機会である。オリンピック・パラリンピック競技大会の開催まで、

既に準備を進めている攻撃者には長い時間があるが、防御する側は時間が足りない。基本的に攻撃側が勝つことを、忘れてはならない。

データと情報が持つ価値が、サイバー犯罪の動機になる。従ってサイバーセキュリティ管理では、人・プロセス・テクノロジーをバランスよく制御する必要がある。人の面では、適切な人材の雇用、その人材の適正を評価する仕組みの構築、質の高い社員の維持などが必要となる。プロセスでは良いマニュアルを作成すれば、新たな人材の教育や監査時のトレーサビリティに活用できる。技術的改善のため日常的に積極的な取り組みを行う必要があるため、国際基準を守るだけでは足りない。

セキュリティでは組織により必要なスキルが異なるため、事業内容と容認可能なリスクの程度を把握しなければならない。役員が、様々な課題に対し正しい判断を下す能力を身につけることが重要になる。日本のトレーニングプログラムは、判断より知識を重視している。意志決定には一定の知識が必要だが、判断力を独立したスキルとして培う必要がある。経営陣には、付随リスクへの不安から新たな技術の導入を拒む傾向がある。だが他方で、新技術の導入なしに競争力を維持するのは難しい。

グループ企業の場合、セキュリティに充てる予算とマンパワーが会社によって異なる。しかしながら、風評リスクはグループ全体に関係し、一番脆弱な会社のセキュリティ水準がグループ全体のセキュリティレベルになる。情報セキュリティの管理法とインシデントへの速やかな対応法を理解するには、事業内容と企業の組織構造、ベンダーを理解することが重要になる。明確な方針に基づく優れたコーポレートガバナンスも欠かせない。このコーポレートガバナンスは、社内各部門のセキュリティ方針実施に向け効果的な構造に支えられる一方、各部門のニーズに応じて方針を調整する柔軟性も備えていなければならない。どの企業もサイバー防衛を独力で行うのは難しいため、外部との連携が欠かせない。企業がどこまでリスクを容認できるか、そのリスクへの対処にどの程度のコストを負担する用意があるかは、経営判断である。経営陣と明確な対話を交わし、データ漏洩が事業に与える影響とリスクの大きさを理解させて支持をとりつける必要がある。経済産業省は 2015 年、子会社・ベンダーのサイバーセキュリティ対策を定めた「サイバーセキュリティ経営ガイドライン」を発表した。このガイドラインは、セキュリティ担当チームが対策の必要性を経営陣に納得させる上で大いに役立った。サイバーセキュリティは投資だというメッセージが記載されたことも、非常に好ましい。だがこれはガイドラインなので、ガイドラインに基づく対応の実施を義務づけるものではない。

次のアクション

IoT（モノのインターネット）はプラスの面もあるが、デバイスを接続することで犯罪者がスマートなサイバー犯罪に移行するため、リスクも多い。これを「Internet of Threats（脅威のインターネット）」と呼ぶ人もいる。IoT をターゲットにしたマルウェア（悪意のあるソフトウェア）は、新たな攻撃ベクトルであり、インターネットの大部分を麻痺させる DDoS 攻撃に利用されている。サイバー攻撃の関係者（役者）となるのは、ハクティビスト（テロリスト）、オンライン犯罪者、国家、ハッカー集団である。金融機関や口座からのデジタル窃盗のほか、ランサムウェア事件も急速に拡大している。PC やスマートフォンのみならず、インターネット対応テレビやスマートデバイスはランサムウェアに対して脆弱である。インターポールのシンガポール総局（INTERPOL Global Complex for Innovation）は、レジリエンスに重点的に取り組むため設置されたもので、情報の共有化改善を目標として、INTERPOL と連携する民間セクターからの専門家を配属している。「知る必要性（Need to Know）」から「共有する必要性（Need to Share）」へと思考を変化させることは、サイバーのリスクに対応する上で、不可欠なプロセスである。日本では、同じインシデントであっても、データ盗難ではなく、データ流出と呼ぶ傾向があり、マインドセットを変える必要がある。

経営層がサイバーセキュリティに対する明確な意識を持ち、管轄機関へのインシデント報告の他、犯罪防止、検知、減少に適切な人材とリソースを割り当てる必要がある。特に、「3 つの C（Collaboration：協働、Cooperation：協力、Coordination：調整）」を中心とした取り組みが求められる。

サイバーセキュリティは、複雑かつ重大な現象であり、公共・民間企業の上層部は、どのようにこの問題に取り組むかは重大な課題である。日本では、役員（取締役会）をトレーニングするというコンセプトは一般的ではないが、意識の低さやこうした分野に対する準備不足に関して、役員室の中に危機感が必要なのではないだろうか。

会社役員育成機構（NACD）では、サイバーリスク概要取締役会ハンドブックを作成しているが、これは企業を狙ったサイバーセキュリティのリスク意識に対する重要な原則を記載したものである。サイバーセキュリティには「正解」はないが、「正しいプロセス」ならある。サイバーセキュリティに対しては、管理が不可欠だが、IT だけでなく、法務や人事の代表者が加わる必要がある。取締役会は、総合的なリスク評価フレームワーク（サイバーセキュリティを含むがこれに限定されない）が必要である。

基本的な内容は、全て経済産業省のサイバーセキュリティ経営ガイドラインにまとめられている。データ保護法令には、国境をまたぐ複雑な問題がある。一部の企業では、CSIRT に十分な人的リソースを配置することも可能であるが、こうした措置は一般的ではない。データは、デジタル経済にとって石油のようなもので、21 世紀に向けて石油の流出を防ぐ方法を学ばなければならないのである。

外交戦略から見たサイバーセキュリティ

重要なインフラへの攻撃を含めたサイバー攻撃の増加によって、ありとあらゆる国が影響を受ける可能性があり、その結果が国民の命を左右する危険性もある。サイバー攻撃の被害は、毎年、数百または数千億ドルに上ると見られ、急激に増加している。サイバー攻撃は誰が攻撃を行っているのか判別することが困難であるため、攻撃者にとって有利な状況だと言える。つまり、各国政府が協力しなければ、この脅威に対応することは不可能だろう。サイバー空間における法の支配を確立するための国際的な対話が進められており、現段階での最適なアプローチとして、既存の国際法の適用が検討されている。国連は、サイバー空間における国際法の適用や責任ある国家の行動規範について話し合うべく、政府専門家会合（GGE）を立ち上げている。今後は、これまでの GGE で合意された報告書の内容を、多くの国が履行できるよう、GGE に参加していない国も含めて包括的に理解を広げていくことが必要である。国連テロ対策委員事務局（CTED）は、包括的なテロ対策法の施行を監視する権能を持つ。テロリストによる重要なインフラへの攻撃は、多数の国民に被害を及ぼすもので、自らの活動の露出を最大限に増やすための手段として利用される。こうした攻撃を防ぐには、セキュリティ対策だけでなく、検察当局の仕組みも強化する必要があり、デジタル証拠を保全するための国際法を整備しなければならない。自国のインフラを守るために適切な措置を行うとともに、他国のインフラが攻撃されている時には適切な支援を行うべきであるなど、適正な規範を定める話し合いが進められている。G7 伊勢志摩サミットでもサイバーが取り上げられ、さらに話し合いを進展させるために作業グループの設置が合意された。信頼醸成のために、さまざまな二国間協議も行われている。また、サイバーセキュリティの領域において脆弱な国の能力構築を行うことも重要である。この問題は、一つの国だけでは解決が望めないためである。

アジアにおけるリーダーとして日本が取るべき行動

昨年の 1 月、日本でサイバーセキュリティ基本法が施行され、内閣サイバーセキュリティセンター（NISC）が中心機関となった。しかし、日本年金機構への攻撃に伴い、サイバーセキュリティにおける政府機関の対策活動は不十分だという認識を深めることになり、その結果 NISC による監視活動の範囲が拡大された。また、各省庁の審議官レベルでサイバーセキュリティの新しい役職が設けられることになった。各主要産業を担当している経済産業省は、この分野において特に本格的な措置を取ってきた。その一つが「サイバーセキュリティ経営ガイドライン」の策定である。

IoT、ビッグデータ、AI は、日本が社会の変化を乗り越えるために不可欠である、第四次産業革命を支えるもので、日本の経済発展の鍵を握っていると言っても過言ではない。しかし、昨年のサイバー攻撃の件数は、5 秒に 1 回発生している計算になる。つまり、サイバーセキュリティは、国の成長戦略において不可欠であり、政府はこの分野における管制塔として、サイバーセキュリティ戦略本部を設置したのである。

2015 年 9 月、サイバーセキュリティ戦略が改定されたが、これによって、セキュリティ対策を投資と考える民間企業の経営層、質量の両方におけるサイバーセキュリティ分野の人材育成、またサイバー攻撃からの国家と一般市民の保護の重要性が浮き彫りになった。今年の 8 月、情報セキュリティ対策のための統一規範が変更され、重要インフラに対する行動計画の見直しを行っている。伊勢志摩で行われた G7 サミットでは、各国首脳は安全なサイバースペースの構築に協力することで合意した。また、ASEAN では、ASEAN 諸国の提携関係を強化する姿勢を明らかにしている。

G7 首脳会談などの大規模なイベントの準備を進める際、この分野における急速な変化を考えると、過去のインシデントを振り返るだけでは有効とは言えない。むしろ、準備の段階から、直近の数ヵ月間に起こったことを慎重に監視する方が有効だろう。東京 2020 大会を開催するにあたり、日本は起こり得るインシデントを想定し、具体化する必要があり、あらゆる分野における人々の経験を共有する幅広い情報共有の枠組みを作らなければならないだろう。

2020 年は、IoT が試される年にもなるだろう。IoT システムにはセキュリティを実装する必要があり、経済産業省と総務省は協力し、IoT にセキュリティゲートウェイ機能を実装する方法を開発する必要がある。産業システムに関しては、従来からのセキュリティ対策を適用するのは非常に難しく、情報システムとは異なるシステムとしてルールを適用していくための想像力が必要になるだろう。サイバーセキュリティ全体のレベルを向上させると同時に、企業が脅威の潜在的な影響を特定し、分析できるようにするとともに、サイバーセキュリティ対策がコストではなく、発展と安定性に対する投資とみなされるように、民間セクターの能力向上を図る必要がある。