土屋大洋（つちや もとひろ）
慶應義塾大学大学院政策・メディア研究科教授

遠藤信博（えんどう のぶひろ）
審議員会副議長／情報通信委員長／日本電気会長

野田聖子（のだ せいこ）
総務大臣／衆議院議員

中西宏明（なかにし ひろあき）
副会長／情報通信委員長／日立製作所会長

根本勝則〈司会〉（ねもと かつのり）
常務理事

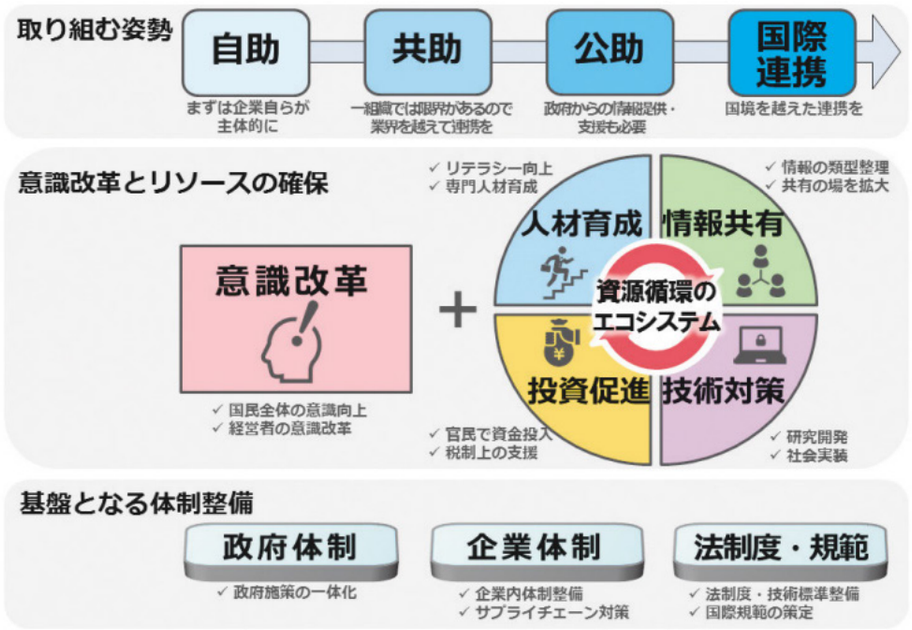
サイバー空間とフィジカル空間の融合による新たな社会「Society 5.0」。あらゆるモノ・コト・サービスがネットワークでつながり、データの活用が飛躍的に進むことにより、さまざまな社会的課題が解決される。そんな輝かしい未来が到来する。一方で、サイバー攻撃の対象が増加し、対策を急がなければあらゆる情報が窃取され、事業の停止や物理的障害までもが引き起こされてしまう。安心・安全なSociety 5.0を実現するためには、サイバーセキュリティに万全を期さなければならない。2年後の2020年に東京オリンピック・パラリンピックを控えた今、関係者の連携のもと対策強化に国を挙げて取り組むことが喫緊の課題となっている。

そこで本座談会では、野田聖子総務大臣を迎え、Society 5.0時代におけるサイバーセキュリティのあり方、対策強化に向けた産学官それぞれの役割と連携について議論する。

◆座談会◆
Round-table Discussion

サイバーセキュリティ
—新たな時代の安心・安全

図表1　サイバーセキュリティ対策の全体像



Society 5.0時代におけるサイバーセキュリティ

根本　まず、Society 5.0の推進を提唱されてきた中西副会長より、そのコンセプトやサイバーセキュリティとのかかわりについて、お話しいただけますか。

Society 5.0の「ネガティブ面」が、サイバーセキュリティ問題

中西　私たちの生活に関する情報、社会インフラなど、あらゆるものがデータ化され、そうして蓄積されたデータが「知恵の源泉」として新たな価値を生み出していく――これが、今起きているデジタル化の大きな波です。

　ただ、デジタル化というと、データがオープンになることで「プライバシーがなくなる」と不安を感じる人もいるでしょうし、AIやロボティクスの進展で「仕事がなくなるのでは」と心配している向きもあるでしょう。新しい世界をつくろうと変革していくとき、そこにはポジティブな側面とネガティブな側面、両方が生じてきます。

　デジタル化のポジティブな側面をとらえて、日本あるいは世界全体が抱える社会的課題を解決しようというのが、Society 5.0の大きなゴールです。先が見えない時代だからこそ、そのゴールをコンセプトとして共有しておくことが、とても大切です。それがSociety 5.0の重要なポイントです。国内外から続々と賛同が寄せられていることが、関心と期待の大きさを物語っています。そして、今や、現政権の成長戦略の大きな柱に位置付けられています。

　一方、ネガティブな側面をどうマネージしていくのかも大きな課題です。その典型例が、サイバーセキュリティ問題ではないでしょうか。あらゆるインフラをデジタル化して制御し、そこから生活者のメリットを引き出していくIoT（Internet of Things）の世界では、サイバー攻撃によって深刻なダメージを受けるリスクが今まで以上に高まります。

　デジタル化のメリットを享受する一方で、そうした大きなリスクにも対峙していかねばならない、これが私たちの置かれている現状なのです。

サイバー空間、個々のネットワークの双方がセキュアであるために

遠藤　あらゆるモノがつながることでデータを収集し、それを質の高い情報へと仕上げ、さらに新しい価値をつくり上げる。これがIoTの世界です。

　言い換えると、私たちは、個人も、企業も、IoTの世界にコネクトしていかなければ、そこから価値を取り出すことができません。そのとき、サイバー空間そのもの、私たちが価値をつくり上げる場所、そのどちらも「セキュアな」状態でなければならない。ここがポイントです。

　共通空間、それにつながる個々のネットワークがセキュアな状態を確保するために、絶えず努力していく必要があります。そのための技術をいかに開発し、人材をどのように育成し、共有していくか、といったことが課題になってきます。

　当然ながら、一個人、一企業の努力で解決できるものではありません。国としてどうするか、という極めて大きな課題ですし、国境を越えて国同士の連携のなかで答えを見いだしていくべきものでもあると思っています。

根本　野田大臣は、総務大臣として「IoTセキュリティ総合対策」を取りまとめ、推進する一方で、自民党「サイバーセキュリティ対策推進議員連盟」（以下、議連）の幹事長としても、長年にわたって活動してこられました。どのような経緯で取り組まれるようになったのか、お話しいただけますでしょうか。

パラリンピックの成功とサイバーセキュリティ

野田　昨年8月の総務大臣就任までの約3年間、私が集中的に取り組んでいた課題が2つあります。1つがパラリンピックで、もう1つがサイバーセキュリティ。この2つは、実は深くつながっているのです。

　オリンピックには注目が集まりますが、それに比べて、パラリンピックへの社会的な関心はまだまだ低い。それではダメ、啓発活動を進め、ムーブメントをしっかりつくり出さなければ、ということで、党内にワーキングチームを立ち上げ、議論を始めました。

　そのなかで、「聖子さん、肝心なことを忘れているよ、パラリンピックの成功とは何よりも、参加した選手から監督、コーチ、応援団に至るまで、みんなが安心・安全に過ごし、無事に帰国することだよ」とのご指摘をいただきました。サイバー攻撃は、リオ大会でも、その前のロンドン大会でも、大会期間中に集中します。東京大会に向けて、一番やらなくてはならないことなのに、議論がすっぽりと抜けていた。それがサイバーセキュリティだったわけです。そこで、有志を集めて勉強会を始めました。

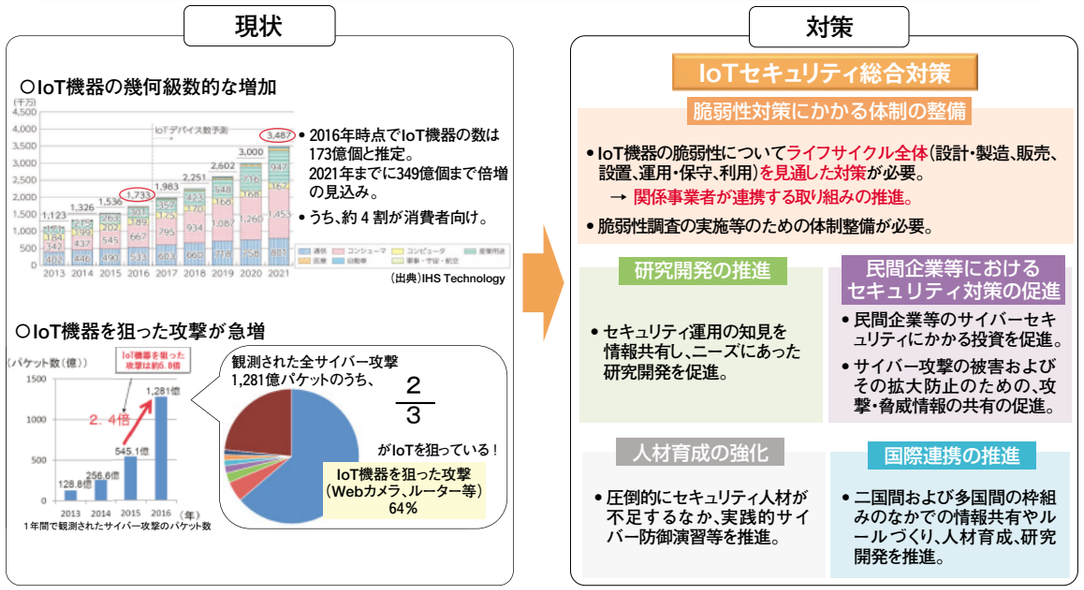
根本　なるほど。それが議連の発足につながるのですね。

野田　ええ。党にも、IoT、AI、第4次産業革命やSociety 5.0に伴走するようなかたちで議連や戦略会議があります。そこでは、中西副会長がおっしゃったポジティブな話、どれだけ価値を生むか、どれだけ雇用が増えるか、といった話は弾むのですが、それを支えるサイバーセキュリティの議論が進んでいないことに不安を感じたのです。

　そこでまず、議連として提言書をつくりました。大会期間中、相当数のサイバー攻撃が予想されるが、その対策として、ヒト・モノ・カネがまったく足りていない状況である、と警鐘を鳴らしたのです。一番の課題は人材でした。トップガンと呼ばれるセキュリティ対策をけん引する人材がいないこと、ホワイトハッカーに対する理解、そうした有為の人材

図表２　IoTセキュリティ総合対策（2017年10月公表）の推進

○　IoT機器の普及に伴い、IoT機器を狙ったサイバー攻撃が急増。
○　総務省では、昨年10月に「IoTセキュリティ総合対策」を策定し、必要な施策を推進。



提供：総務省

の活用が進んでいないことなどを挙げて、先進国のサイバー攻撃に対する備えと比較して、日本は、さまざまな阻害要因があって立ち遅れていることを世に示しました。

それから総理官邸に向かい、安倍総理に提言を直接お見せしました。すると、実は総理も以前からサイバー攻撃を危惧されていて、「大会は、同盟国などにサポートしてもらい、突貫工事で乗り切ろう。ただ、今後、Society 5.0を推進するとき、その面の対策が講じられていることが前提条件になるのだから、継続的に取り組まなければならない」とおっしゃいました。

その後、自分なりにコツコツと議連での活動を続けてきましたが、図らずも総務大臣となりましたので、これ幸いとばかりに、政府内外の皆さんのお尻をたたくのではなく、プッシュするかたちでがんばってまいりました（笑）。おかげさまで、かなり理解が広まり、いろいろなことが変わってきたと感じているところです。

根本　大臣から、東京大会を乗り切るには同盟国などのサポートが不可欠だというお話もありましたが、国際政治や安全保障の観点からサイバーセキュリティを研究されている土屋先生は、サイバーセキュリティ確保に向けたあり方は、今後どのようになっていくとみておられるでしょうか。

東京オリンピック・パラリンピックをハッカーたちの「晴れ舞台」にしない

土屋　政治家の先生を前にしてはばかられますが、政治学を専門にしていると、どうしても人間をネガティブに見る癖がつきます。例えば、大臣が本日お持ちになった資料「ＩｏＴセキュリティ総合対策（２０１７年10月公表）の推進」を見れば、ＩｏＴ機器を狙った攻撃が急増していることがわかります。つまり、悪いことを考える人の方が成長率が高いわけです。ここが非常に問題だといえます。

よく「サイバー攻撃は地球の裏側から来る」「いつ来るかわからない」といったことがいわれます。でも、そうではなくて、やはり地政学上のリスクと結び付いているのです。サイバー犯罪は別として、意図的に狙ってくる攻撃には何らかの理由があります。確かにリオ大会でもサイバー攻撃はありましたが、それほど深刻な問題は起こりませんでした。その理由は明確です。当時のブラジルは国内にさまざまな問題を抱えていたのですが、国際的な問題は少なかったのです。

東京の場合はどうでしょうか。今、平昌大会の開催にあわせ、表面的には落ち着いて見えるものの、裏ではたくさんのサイバー攻撃が行われていることが検知されています。北朝鮮に見せかけながら、ロシアがオリンピック関連サイトにサイバー攻撃をかけたと報道されています。ロシア選手の参加が認められなかったことへの報復とみられています。日本が近隣諸国との間で地政学的なリスク、テンションを抱えている以上、東京大会が狙われることは当然、想定しておかなければならないでしょう。

野田大臣がおっしゃるとおり、オリンピック・パラリンピックは非常に狙われやすいのです。悪者ハッカーたちにとっては「晴れの舞台」ですから。

野田　ハッカーたちのオリンピックみたいになってしまったら、困りますね。

土屋　そうです。やはり目立ちますから、「あいつはすごい」と評判が立つ。悪名ですけどね。それが一種のシグナルとなり、われもわれもと名乗りを上げる。パフォーマンスとして実行する人たち、市場を混乱させてもうけようとする人たち、あるいは政治的な思惑から「日本に恥をかかせたい」と考えている人たち、実にさまざまです。そうしたいろいろな動機が交錯するなか、大量のサイバー攻撃が行われるわけです。

また、現在この領域は「スパイの世界」、つまり、各国のインテリジェンス機関が主たる役割を担う世界です。米国であればＮＳＡ（国家安全保障局）、英国であればＧＣＨＱ（政府通信本部）が、サイバー防衛の最前線に立っていますが、日本にはカウンターパートとなる組織がありません。

いろいろな法制上の理由がありますが、それでは、米国に頼ればよいのか、英国が助けてくれるのか。「情報共有すればよい」と言う人もいますが、情報は交換するものであって、一方的にもらえるものではありません。「日本は何をくれるのか」と聞かれたときに、私たちが持っている知見を提供できなくてはいけないのです。ここは、早急に対策を講じる必要があります。

私も東京大会は、この問題に国民の目が向く非常に良いきっかけになると思っています。一方で、２０２０年以降の日本のことも考えておかなくてはいけません。そのための方策を、今考えることが大切だと思います。

野田　土屋先生のご指摘のとおり、ＩｏＴ機器の増加に伴い、これらを狙ったサイバー攻撃が急増しています。そこで、総務省では、昨年10月に「ＩｏＴセキュリティ総合対策」を策定し、必要な施策を推進しているところです。

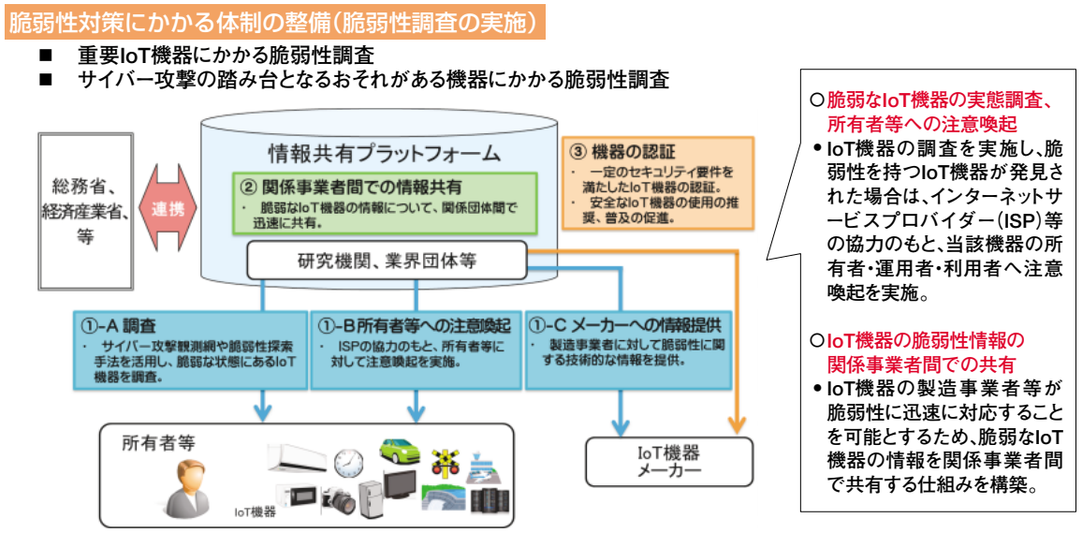
私たちとしては、ＩｏＴ機器の脆弱性について、ライフサイクル全体（設計・製造、販売、設置、運用・保守、利用）を見通した対策が必要だと考えていて、体制整備を急いでいます。すでに昨年９月から実態調査も開始しており、その結果を関係事業者と共有していくつもりです。その先に、日本発のＩｏＴ機器認証制度を構築できれば、「日本製品は安心・安全だ」という認識が広まって、付加価値の向上に貢献できるのではないかと思っています。

また、東京大会を１つの契機にしたいというのは、私たちも同じ思いです。サイバー空間では、「島国」という日本の地政学的なメリットがなくなるのだ、という意識を国民の皆さんに持っていただくことが大切です。

その鍵となるのは、やはり人材育成だと思っています。私は勉強会を始めた当初から、

図表３　脆弱性対策にかかる体制の整備（脆弱性調査の実施）

○ すでに流通しているIoT機器のセキュリティ対策については、昨年９月から、脆弱なIoT機器の実態調査を開始。
○ 関係事業者間での情報共有を通じて、対策の強化につなげていきたい。



提供：総務省

セキュリティ人材が圧倒的に不足していることに危機感を抱いていました。ＮＩＣＴ(National Institute of Information and Communications Technology：情報通信研究機構)に設置された「ナショナルサイバートレーニングセンター」では今、東京大会の適切な運営に向けたセキュリティ人材の育成のために、大会開催時を想定した模擬演習「サイバーコロッセオ」を実施しています。

サイバーセキュリティ人材の育成

根本　野田大臣から人材育成のお話がございましたが、遠藤副議長は、サイバーセキュリティ人材の育成について、どのようなお考えをお持ちですか。

才能ある子どもたちが活躍できる環境づくりを

遠藤　大臣のおっしゃるとおり、セキュリティ人材は圧倒的に不足しています。ある調査によると、情報セキュリティに従事する技術者は20数万人であるのに対し、中小を含めた企業数は約３８０万社で、１社に１人どころか、まったく足りていないのが現状です。

一般家庭から企業まで、セキュアな環境をつくろうと考えたときに、まず、どのように守っていくのかというコンセプトを持つことが大切です。それをベースに、どんな人材が、どのくらい不足しているのかを見定め、育成していくことが必要だと思います。

実際のサイバーアタック数を見ると驚くような数字で、例えば、マルウェアは毎月新たに約１０００万件がつくられるといわれています。当社でもサイバーセキュリティのサービスを提供していますが、対応している約１０００件弱のネットワークで、１日に約２億のイベントが検知されるという状況です。

もちろん、それらすべてを人が見ているわけにはいかないので、ＡＩを入れるなどして絞り込むのですが、それでも最後はやはり、人が対応します。そのために、どのくらいの人数がいればリアルタイムで処理できるようなお考えをお持ちですか。

になってくるのかといったことも、人材育成の基本的なコンセプトとして考えておく必要があります。

もう１つ重要なのは、国民全体のリテラシーを上げることです。日常生活で、「ネットワークにアクセスするときは機器をセキュアな環境に置かなければいけない」ということが、「食事のときにお箸を使う」というのと同じくらい、当たり前になることが望ましいと思っています。そうなるように教育、啓発を進めていくことが必要です。

また、若い人たちの能力を、より早い段階から開発していくための教育システムも重要です。15～20歳の若者によるＩＴ関連の犯罪は、他の年齢層と比べて非常に高いという統計もあります。高いＩＴスキルがあっても、それをまっとうなかたちで発揮できる場がないことが問題なのではないでしょうか。能力がある人が早い段階から高度な教育を受けられる仕組みが必要です。

当社では、サイバーセキュリティに関するサマーキャンプを開催していて、参加者の最年少は10歳です。参加にあたって誓約書に署名してもらおうとしたら、彼は、そこに書いてある漢字が読めない。小学校４年生なので当たり前の話なのですが、プログラミングの能力は大人を凌駕している。ＩＴの領域は、学校で教わらなくても、自分でどんどん学ぶことができるのです。そうした子どもたちがいかに共有するか、といったことが課題だったわけですが、もはやそれでは不十分です。自分たちのオペレーションで閉じてしまうのではなく、社会の仕組みまで考えて連携し、さらに社会全体を守るにはどうすればよいかという考え方を持たなければいけない時代なのだと思っています。

なお、現在、ＩＰＡ(Information-technology Promotion Agency, Japan：情報処理推進機構)のなかにある「産業サイバーセキュリティセンター」において、ＯＴとＩＴ、双方のスキルを持った人材を育成するプログラムが提供されています。

根本　土屋先生、大学教育あるいは国際連携といった観点から、お願いします。

サイバー空間をめぐる２つのグループの対立

土屋　私は大学におりますから「大学で何とかしろ」という声はよく耳にします。ですが遠藤副議長のお話からわかるように、大学に入ってから教育したのでは、もう遅いですね。そもそも、先ほどの小学校４年生のような子が飛び級で進学したいと思っても、今の教育制度では、なかなかできない。

うちの学部では、数学と小論文と情報科の非常にクリティカルなところまで来ている。

初期には、業界単位でインシデント情報を

社会インフラを守る「ＯＴ人材」が不可欠

中西　東京オリンピック・パラリンピックが開催されている日本を思い描いてみたとき、列車や飛行機など、交通機関をはじめとする社会インフラが、デジタル化された仕組みのなかで動いていて、そこを狙われた場合、深刻なダメージを受けることは明らかです。まあ、そういうことをしゃべると、狙う人が出てくるので、あまり言いたくはないのですが。

そうなると、もう１つ違う教育が必要になってきます。というのも、例えば実際に列車はどう動いているのか、その仕組みを理解したうえで守らなくてはいけないからです。これはもう、サイバー空間のなかで完結する話ではありません。私たちは、これをＯＴ(Operation Technology)と呼んでいます。

実際、ウクライナでは２０１５年から16年にかけて、マルウェアによるサイバー攻撃で、大規模な停電が何度も起きています。これらは、土屋先生がおっしゃる政治的な意図で行われた攻撃です。生活の生命線である社会インフラが、こうした攻撃で脅かされるという

図表4　セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

○ セキュリティ人材の不足の早急な解消は、政府にとって重要課題。
○ 総務省では、NICTに組織したナショナルサイバートレーニングセンターにおいて人材育成を実施。

① 国の行政機関、地方公共団体、独立行政法人および重要インフラ事業者等に対するサイバー攻撃について、実践的な防御演習を実施（CYDER）
② 2020年東京オリンピック・パラリンピック競技大会の適切な運営に向けたセキュリティ人材の育成（サイバーコロッセオ）
③ 若手セキュリティエンジニアの育成（SecHack365）

提供：総務省

3つの科目で入学できるコースを設置しています。今、情報科は、中学校でも高校でも、ほとんど重視されておらず、余った時間で受講する科目のようになっている。これでは情報リテラシーは上がらないし、特殊な能力を持った子が救われません。初等中等教育から変えていく必要があると思っています。

では大学は何をやっているかと申しますと、国際連携でいえば、いろいろな大学と提携したり、国際会議の場でサイバーセキュリティの現場からお話を伺ったりといった取り組みを進めています。昨年は、中西副会長にも講演していただきました。

一方、国際政治の情勢から見ると、日米英豪に欧州諸国を加えたグループと、中国、ロシア、中東、その他の国々からなるグループとに分かれてしまうため、対話ができないという状況です。

後者の主張は、こうです。サイバー空間は非常に荒れていて、そのため膨大な数の攻撃が連日行われている。だから、政府が責任を持って対処すべきであり、そのための国際条約をつくらなければならない。発展途上国にとって非常に魅力的な主張であり、「そのとおり」と考えている国は少なくありません。

これに対して、日本を含む前者のグループは、サイバー空間は自由な表現の場である、だから政府が関与するべきではない、という立場です。過剰な規制をもたらすような条約は、自由な情報の流通を阻害するという考え方で、今のところ、こちらの主張の方が分が悪い。

これまで、国連サイバーGGE（Group of Governmental Experts：政府専門家会合）で議論していたのですが、昨年7月に決裂し、報告書をまとめられませんでした。これは、非常にショッキングな出来事で、サイバー外交というものが機能しなくなりつつあることを示しています。

その結果、昨年後半から起きていることはこうです。OSCE（Organization for Security and Cooperation in Europe：欧州安全保障協力機構）という冷戦時代につくられた国際的な枠組みがあるのですが、ここでサイバーセキュリティの議論が始まりました。あるいは、ARF（ASEAN地域フォーラム）に日米露中が入っての議論も始まっています。サイバー空間がボーダーレスであるにもかかわらず、地域ごとに議論が進められるという、ちょっと歪な状況になってきているといえるでしょう。

そうしたなかで、今、日本が一生懸命進めているのが、ASEANへの支援です。日ASEANのサイバーセキュリティ協議は、もう長い間続けられていますが、そこに日本政府の関係者、あるいはJPCERTコーディネーションセンターをはじめ政府の支援を受けて能力構築を行っている機関の職員が、ASEANやアフリカの国々へ赴いて、支援を行っています。

主に現地の若い人材を育てていますが、その世代が将来、日本のために貢献してくれることが期待されます。そうしたかたちでの国際連携が進んでいることは、とても重要なことだと思います。

根本　大臣、お三方のお話を聞いての感想はいかがでしょうか。

従来の能力観にとらわれない人材育成を

野田　サイバーセキュリティのサマーキャンプに参加している小学生のお話は、とても示唆的ですね。NICTのナショナルサイバートレーニングセンターでも若手セキュリティエンジニアの育成（SecHack365）を行っていますが、最年少の参加者は、やはり10歳です。

私の息子は7歳になったばかりで、重度の知的障がいがありますが、スマートフォンは達人です。SNSで特定の人物をピックアップして、自分が貼り付けた写真を送ったりしている。私たちは普通、何かの機器を使うとき、まず説明書を読んで、それに従って扱い方を覚えていくわけですが、スマートフォンは、年齢に関係なく、いきなりできてしまう。

そうしたところにもICT（情報通信技術）の「すごさ」を感じますし、私たち大人が、これまでの能力観を変えなくてはいけないと思いますね。

むしろ一番リテラシーが必要なのは、中小企業の経営者かもしれません。ICTとか、セキュリティとかいうだけで、はじめから敬遠してしまう。その人たちがどこに逃げるかというと、保険です。自分たちで身を守ることをあきらめて、被害にあったら保険で補填してもらえばよい、という流れが、この国にできてしまうと、Society 5.0が世界的に信用されなくなります。そこは、経団連が率先して経営者の方々の意識を変えていただけるとありがたいなと思っています。

海外との連携についてですが、先進国のなかでも、IoTの脆弱性に着目したのは、日本が一番早かったと思っています。世界各国のユニークな取り組みを互いに紹介し合うことで、情報共有や人材交流を進めていきたいですね。土屋先生が指摘されたように、情報をもらうばかりではダメ。自分たちからオープンにして、世界の役に立っていく姿勢が大切です。

国内に「ICT-ISAC Japan」という民間団体があります。これまで、官民連携のプロジェクトを一緒に進めてきていますが、ここに窓口になってもらって、海外との情報共有もしっかり進めていきたいと考えています。また、現在、法律改正によってIoTの脆弱性対策に取り組むことを考えていますが、今後は、産学官が連携して、情報共有や対策に取り組んでいくことが必要です。総務省としては、人材を含め、そのための枠組み、受け皿をつくっていかなければならないと思っています。

遠藤　当社は、総務省の「ASEAN諸国におけるサイバー防御能力の向上に向けた実践的演習のモデル事業」の一環として、2015年度からタイ、マレーシアなどのASEA

2020年の東京パラリンピック成功に向けた取り組みを進めるなかで、サイバーセキュリティの重要性を認識し、自民党「サイバーセキュリティ対策推進議員連盟」を立ち上げた。現在は、総務大臣として「IoTセキュリティ総合対策」を推進している。サイバーセキュリティは安全保障の問題であり、国家として国民を守らなければならないという思いで取り組んできた。これからも国会議員の課題認識を高めつつリテラシー向上に努めていくが、経済界からの応援を期待している。

（野田聖子）

経営者の意識を変えていくために

根本　野田大臣から、中小企業経営者のリテラシーを上げることが課題であるとのご指摘がありました。経団連として協力できる部分もあろうかと思いますが、中西副会長、いかがでしょうか。

情報のフラットな共有が不可欠

中西　中小企業の生産性を上げることが、日本の経済力強化の政策において、かなりのポーションを占めていることは間違いありません。しかしながら、そもそも、中小企業、大企業という分類が今や成り立たなくなっているのではないでしょうか。

　デジタル化が進むと、サプライチェーンそのものがフラットになり、情報共有は、サプライチェーンが活き活きと動くための前提条件となります。情報のフラットな共有を放棄してしまうと、日本の産業構造そのものの脆弱性に直結しますので、危機感を持たなければいけません。

　そう考えたときに、「小さい企業では情報担当者をアサインできませんよ」というところから始まって、あれもできない、これもできない、ないないづくしになってしまっては先がない。そうならないよう、例えば中小企業を対象にしたクラウドを上手に使って、そこでセキュアなネットワークを構築するような、お金をかけない技術、仕組みをつくっていく必要があると思います。

野田　例えば「ICT寺子屋」みたいなものをつくって、経営者の皆さんに参加してもらうといった方法もありますね。先ほど大学生になってからでは手遅れだというお話もありましたけれど（笑）。でも、サイバーセキュリティは経営戦略上必須の課題だ、ということを理解してもらうために、いろいろなかたちで支援していきたいと思っています。

根本　中小企業の話が出ましたが、大企業の経営者は大丈夫なのでしょうか。

企業におけるセキュリティに対する認識

遠藤　大企業の経営者は、だいぶ痛い目に遭っていますからね。

中西　3年前に経団連でサイバーセキュリティの話をしたら、「それはテクノロジーの話だから…」という方や、「うちはそれほどオンラインにつながっていないから…」という方が、かなりおられました。ところが、この3年でガラッと変わりましたね。

野田　本当ですか。それは良いニュースですね。

N各国の政府サイバーセキュリティ関係機関を対象に、サイバー演習を実施しています。経済界としてもASEANとのこの面での関係構築を重視していますので、非常に意義のある事業だと思っています。

野田　総務省は、非常に地道な活動をしている役所なのですが、自分たちのPRが苦手なところがありますので、そうおっしゃっていただけるのは、とてもありがたいです。

変革によって新たな世界が誕生するとき、ポジティブな側面とネガティブな側面が必ず生まれる。前者がSociety 5.0実現による社会的課題の解決であるとすれば、後者の典型例はサイバーセキュリティ問題である。東京オリンピック・パラリンピックでは、交通機関をはじめとする社会インフラへの攻撃が想定される。ITのみならずOTのスキルをも備えた人材育成が急務である。ここ3年の間に、経営者の認識も大きく変わってきた。官民連携のもとサイバーセキュリティ対策を推進していきたい。

（中西宏明）

ね。

中西　昨年、経団連の会長・副会長の間でサイバーセキュリティをテーマに重点的に議論をしようということになりました。ベンダーや通信業界の方だけが発言して終わりかな…と予想していたら、なんと私たちがしゃべる暇がないくらい（笑）。

　ただ、意識の高まりには手応えを感じているのですが、これをアクションに移さなければ、どうしようもない。単なるコストではなく、投資として考えて、お金を使って、人を育てるというところまでやらなくてはいけません。当然、この取り組みは、今日動けば明日に成果が得られるというものではなく、一方で、敵は日々進歩しているので、継続的にやっていく必要があります。果たしてそこまで意識が変わってきたのかどうかについては、あまり自信はありません。

遠藤　いや、かなりいいところまで来ていると思いますよ。日本の大企業は、すでにサイバー攻撃の対象になっていますから、意識せざるを得ません。

中西　当社にしても、2～3年前までは、入らせない、データを流出させない、という2点を重点に考えていました。最近のアタックは、例えばWannaCryのようなものは、何の目的かわからないけれど、とにかくファイルを破壊していく。入らせない、流出させない、というクライテリア（判断基準）では防衛になりませんね。

土屋　「若者がこの分野に入っていかないのは、キャリアパスがないからだ」とよくいわれます。セキュリティ担当者が出世して、社長になるかというと、その可能性は低い、とみられているのです。そもそもセキュリティというのは、破られたら怒られるけれど、破られなければ「よくやった」で終わってしまうようなところがあります。そうした認識も変わりつつあるのでしょうか。

中西　そういう側面も多少残ってはいるけれど、かなり変わってきたと思います。少なくとも、セキュリティ人材を世代ごとに育てていくことが必須の経営課題である、ととらえられるようになってきました。

土屋　では、学生には堂々と「セキュリティをやりなさい」と言えますね。

中西　そう思います。

野田　ぜひ学部を新設してください（笑）。

根本　先ほど大臣からいわゆる「トップガン」の話がありましたが、そこはどうなのでしょうか。

日本で「トップガン」を育成できるか

遠藤　トップガンの育成は非常に難しいですが、トップガンの2つ下ぐらいのレベルであれば、教育でなんとかなります。そこから先は個々人の突き詰め方次第です。自分で興味を持って学んでいくことになりますね。ただ、教育で育成することが可能な層をケアするだけでも、大きな効果が期待できます。

野田　トップガンは、ICT技術はもとより、OTがわかっていないとダメですね。アタックをどう止めるかについては、事業全体にか

意図的なサイバー攻撃は、必ず地政学上のリスクと結び付いている。近隣諸国との緊張関係を抱える日本は、東京オリンピック・パラリンピックが狙われることを想定し、対策を講じる必要がある。ハッカーたちの「晴れ舞台」にしてはならない。初等中等教育など早期に人材を育成する取り組みが必要だ。政府の過剰な関与を望まない日米英等のグループと、国際条約などによる規制強化を主張する中露・中東諸国等のグループとの間で国際協議が二極化することを懸念している。日本は、ASEANとの協議など、各国・各地域との関係構築を急がなければならない。（土屋大洋）

遠藤　世界的に見ると、軍が教育機関になっているケースが多いですね。

野田　やはり早いうちから目を付けるのですよ。

遠藤　例えば、イスラエルは高等教育の段階で、数学などいくつかの学科で優れている人を、強制的に軍の教育機関に入れると聞きました。

中西　そこの出身者がベンチャー企業の経営者になっています。だから、キャリアパスがきちんとあるといえるわけです。

対策強化に向けた各主体の役割と連携

根本　野田大臣にお伺いします。人材育成やリテラシーの向上を含め、サイバーセキュリティ対策を推進するうえで、政府の役割と体制については、どのようにお考えでしょうか。

「サイバーセキュリティ統括官」を新設

野田　総務省内に情報セキュリティ政策局を創設するという議論がありましたが、今の行革のなかでは難しいですね。そもそも横断的にかかわる問題なので、私は庁レベルの組織が必要だと思っています。

　とはいえ、企業の皆さんのカウンターパートとして、総務省内に「サイバーセキュリティ統括官」を新設することにしました。そこに来ていただければ、ある程度のことは解決できるし、協力もできる体制になります。後は、審議官を置き、専門の参事官を複数置くことで、「局」という名称こそ付いていませんが、局以上の働きができると思っています。

標準化に向けた合意形成の努力が必要

遠藤　スタンダーダイゼーション（標準化）は、絶対に必要です。ただ、スピード感をどう入れ込んでいくかが課題になっていると思います。

　例えば、EUは個人データの保護に関して、非常に厳格な制度を全域で適用しようとしていますし、中国も独自の規制を設けています。日本や米国は、ある程度自由度を守っていこうというスタンスです。ある領域に関しては非対称性が出てきてしまっているなかで、共通的なスタンダードを構築していくのは、かなり難しい状況になっています。

　スタンダーダイゼーションは、国益を含めた議論になってきます。すでにベースがあるなかで、その上に組み上げていくには、高いレベルで合意を形成し、方向感をつくっていく努力が必要です。いずれにせよ、絶対にやかわる意思決定ができる人でなければ判断ができない。それをどうやって育てていくのか、エンジニアを自衛官にするのか、まだ日本では方向性が定まっていません。米国では、かなり若いうちに選抜されるようですが、日本の場合、教育システム自体を見直さないと難しいでしょうね。

IoTの世界では、サイバー空間と個々のネットワークの双方がセキュアな状態であることが求められる。現在、セキュリティ人材は圧倒的に不足している。明確な対処方針のもと、人材の育成・確保を図っていく必要がある。同時に、国民のリテラシーを高める取り組みやSociety 5.0を担う若い世代を育てるための教育システムの構築も必須である。当社では、総務省による事業の一環として、ASEAN諸国での人材育成も行っている。引き続き産学官の連携、国際的な協調・協働を進めたい。（遠藤信博）

らなくてはならないことだと思っています。

根本　土屋先生、いかがでしょうか。

情報共有における言語問題を日本の技術力で解決せよ

土屋　情報共有をしようというときに、今までは、担当者が紙に打ち出して、相手に渡すというようなことをやっていたと思います。当然それは時代遅れで、機械と機械が直接対話できるような仕組みをつくらなければならないでしょう。

　そのための標準化がとても重要で、例えば「日本の金融業界で、こういうインシデントがありましたが、米国ではどうですか？」と聞くときに、コンピューターが自動で受け答えして、担当者に見えるようにする必要があります。このときに課題となってくるのは、言語です。日本から出ていくインシデント情報が日本語で書かれていては、コンピューター同士の対話が成立していたとしても、生身の人間である相手には理解不能です。

　日立なり、NECなりが、そこの工夫に取り組むことは、国際社会に対するとても重要な貢献になります。例えば、ASEANの国々で話されている多様な言語について、自動的に友好国間で共有できるようなシステムができると、Society 5.0における日本の素晴らしい貢献になるのではないでしょうか。

中西　とても素晴らしいチャレンジになると思います。インターネットでは、英語と中国語が二大言語ですから、日本語にスティックしていると、情報共有の限界に直面してしまいます。

　先ほど大臣が話されたIoT規格のスタンダードも、大きな動きです。例えば、政府調達のなかで納入要件のところにまで入ってくれば、一気に進むと考えられます。

　そうしたことをすべて見渡した、体系的なアプローチができる体制をつくっていかなければ、日本はどんどん取り残されてしまうと危惧しています。

オープンかつ柔軟な姿勢で諸外国との関係構築に努めたい

野田　20年前、私が小渕政権で郵政大臣を務めていた時に、日本のIT政策がスタートしました。当時も標準化をめぐって、規制的な欧州と自由を優先する米国の間で確執がありました。日本は、その境に立って右往左往していたわけですが、現在も同じ状況が続いているのだろうと思います。

　ただ、日本国内は人口減少で内需が縮小していくのですから、外需にシフトしていくなかで、土屋先生が指摘された言語の問題もしかりですが、とにかく閉鎖的にならず、オープンな姿勢で、諸外国との関係構築に努めなければならないと思っています。

　標準化に関して、これまで日本はかたくなになってしまうところがありましたが、これからはもっと柔軟な対応が求められます。時には「褐」のように、さまざまなことに対応できるしたたかさが必要かもしれません。

　内需が先細りするなかで外需獲得に突破口を見いだそうということも、Society 5.0のコンセプトの1つだとするならば、今まで考え

撮影：工藤裕文

てこなかったようなことに答えを出していかなければいけない、と痛感しています。

中西　20年前と大きく異なっているのは、中国のプレゼンスです。特に、移動通信分野で「5G」の世界がやってくるわけですが、この面で大きな影響力を持つ中国の動向に左右されるとみています。だからこそ、日本が自らの立ち位置を明確にして、世界にメッセージを発信していく必要があると思います。

野田　おっしゃるとおりです。

根本　では、最後に本日の議論を総括して、遠藤副議長よりお願いします。

サイバーセキュリティは安全保障の問題である

遠藤　やはりサイバーセキュリティは「国でしっかり守る」という考え方が重要です。その意味で、官民が一体となって方向性を定めるような体制が整ってきたことをとてもうれしく、心強く思っています。

　政府内でも各省庁、各部署によって役割分担があろうかと思いますが、サイバーセキュリティはボーダーレスな領域です。その観点からいえば、部署によってプライオリティが異なってはならないと思います。

　「サイバーセキュリティは、すべてのプラットフォームである」という認識を共有しつつ、産学官が連携して取り組みを推進していくことを、心から願っています。

野田　私も同じ思いです。先ほどお話ししたとおり、サイバーセキュリティの勉強会を立ち上げたころは、なかなか周囲の理解が得られず、孤独な世界を漂っている心持ちでおりました。国会では、目に見えない課題は議論になりません。そういう政治的欠如の状態からスタートしたわけですが、経団連のなかでもサイバーセキュリティの議論が盛り上がっているというお話を聞き、大変心強く思っています。

　遠藤副議長が指摘されたとおり、サイバーセキュリティは安全保障の問題です。私は、「安全保障なのに予算が付いていないのはおかしい、国民を守る気がない国家にしてはいけない」という思いで取り組んできました。これからも国会議員に働きかけ、議員の課題認識を高めつつ、リテラシー向上に努めていきます。ぜひ経済界の皆さんからもハッパをかけていただけたら、うれしく思います。今日は素晴らしい応援団に恵まれた思いです。ありがとうございました。

根本　われわれ経団連としても、大臣の思いをしっかりと受け止めて、サイバーセキュリティの推進に取り組んでいきたいと思います。本日は貴重なご意見をありがとうございました。

（2018年2月14日　帝国ホテルにて）