産業構造審議会　商務流通情報分科会
第5回情報経済小委員会

○佐野課長

それでは、定刻になりましたので、産業構造審議会商務流通情報分科会第5回情報経済小委員会を開催いたします。

本日は、ご多忙の中お集まりいただきましてありがとうございます。

まず議事に先立ち、資料の確認をさせていただきます。

本日は、iPadを使用し、ペーパーレスで審議を進めてまいりたいと思います。

本日の配付資料は、座席表、議事次第のほか、資料1の委員名簿、資料2の論点ペーパー、資料3の今後の予定の3つでございます。併せて参考資料として、第4回の情報経済小委員会を踏まえて、5月に公表した中間取りまとめとその概要を掲載しております。

本日は15名の委員にご出席いただいておりまして、規定の過半数11名に達しております。

なお、石黒委員、國井委員、國領委員、夏野委員、根本委員、松尾委員は、ご都合によりご欠席となっております。また、一般社団法人日本経済団体連合会常務理事の根本委員の代理で、産業技術本部上席主幹・吉田一雄様に本日はご出席いただいております。また、このたび、一般社団法人電子情報技術産業協会会長にシャープ株式会社取締役会長の水嶋繁光様が着任されたことに伴いまして、新たに委員にご就任いただいております。

それでは、ここからの議事進行は村井委員長にお願いしたいと思います。

○村井委員長

皆さん、こんにちは。それでは、議事を進めさせていただきます。よろしくお願いいたします。

議事に先立ちまして、安藤商務情報政策局長からご挨拶をお願いいたします。

○安藤局長

このたび、7月31日付で富田の後に商務情報政策局長になりました安藤と申します。よろしくお願い申し上げます。

IoTや人工知能などの発展によって、産業構造から社会構造が広く変わりつつあります。前回の小委員会第4回では、皆様方の各方面からの知見を出していただきながら中間取りまとめをさせていただいて、まさに官民を挙げてチャレンジしていこうではないかという方向性をご確認いただいたという認識をさせていただいております。

まさにデータをしっかりととって、そのデータをうまく分析して、それをさまざまなシステムにフィード

バックしていく。こういったデータ駆動型社会の到来が現に動いているわけでございます。こういった社会におきましては、新たなビジネスがどんどん生まれているわけでございますけれども、従来型のモデルにしがみついていては、あっという間に陳腐化していってしまうということは宿命の時代になってきたと思っております。

我が国といたしましても、世界の潮流に乗り遅れずに一歩でも二歩でも先んじなければいけない。まさに今の安倍政権の成長戦略の中でこういった分野が大変注目されているのはご案内のとおりでございます。肝心なことは、これを具体化していかなければいけないということだと認識しております。

こちらの委員会でもう1つご議論いただきたいのは、サイバーセキュリティの問題でございます。ご案内のとおり、年金機構の問題が大きくクローズアップされておりますが、これは氷山の一角ではないかと危惧しているわけでございまして、類似の事象、あるいはさらにそれを上回る事象の脅威に日本は今さらされていると私どもは思っております。2020年の東京オリンピック・パラリンピック、祝福すべきイベントに育てていかなければいけないわけでございますけれども、これがまた海外からのアタックの誘引になってしまうということもあり得るのではないかと思っております。

こういった、いわゆるデータ駆動型社会における利活用の側面とセキュリティの側面について、これからさらに具体策、論点等々を含めまして、先生方のご知見を改めて拝借させていただきたいということで、村井先生にお願いいたしまして、招集していただいたということでございます。

今後、何回かまた皆様方のご意見をいただくようにお願い申し上げまして、簡単ではございますが、私のご挨拶にかえさせていただきます。よろしくお願いいたします。

○村井委員長

ありがとうございました。

今、局長からお話がありましたように、今まで4回にわたり小委員会を開催して、中間取りまとめという形でまとめていただきました。今回は、前回の議論の中からデータの利活用及びセキュリティについて社会の中でどのように進めていくか、ということを抽出し、議論を深めて参ります。では事務局作成の資料をもとに、ご説明を伺ったあと、自由討議に移りたいと思います。よろしくお願いいたします。

○佐野課長

事務局でございます。資料2をご覧下さい。本日ご議論いただく論点につきまして、事務局であらかじめ整理させていただいたものでございます。

まず、2ページ目をご覧下さい。昨年12月から4回にわたり審議をいただきまして、それを踏まえ

て5月に中間取りまとめを行ったところでございます。

中間取りまとめでは、大きく3つの方向性をご提示いたしました。1番目に、制度を変える。新しいビジネス創出のための制度環境を整備していくということでございました。

2番目に、チャレンジを促す。企業間連携によって新しい産業モデルを生み出す、あるいは企業がチャレンジする環境を抜本的に強化していくということでございます。

3番目に、基盤を整備していく。本日のテーマの多くが含まれておりますが、サイバーセキュリティの対策、人工知能を含めました研究開発の強化、それから人材の確保強化ということでございました。

次の3ページ目をご覧下さい。今回の討議事項でございます。これまで委員会でご議論いただいて、中間取りまとめをまとめたわけでございますが、先ほど紹介したそれぞれについて、必要な施策の具体化を図っているところでございます。今後、この委員会におきましては、それぞれの施策の進捗状況の報告をいたしますとともに、一部の論点につきまして、さらに深掘りをして議論を深めていただければと思っております。

深掘りが必要な論点として、事務局で整理したものが下に赤字で書いてある部分でございます。データの利活用で論点2つ、セキュリティの関係で大きく論点4つでございます。ユーザー、ベンダー、あるいはユーザーとベンダー共通のそれぞれ論点がございます。その論点のほか、後ほど経過報告をさせていただければと思います。

5ページ目をお開きいただければと思います。データを活用した産業モデル創出の戦略的展開でございます。前回まとめた中間取りまとめにおきましても、付加価値の源泉があらゆる産業でデータの利活用に移行していき、産業構造が大きく変化していくのではないか。このために新たな産業モデルの創出を加速化していくことが必要ではないかというご議論でございました。

これを実現していくために、重要分野ごとの課題や状況に応じまして将来像を共有して、民間ベンチャーの先駆的なチャレンジの支援と官民での規制改革や新たな規格形成を目指した実証的な取り組みを展開して、革新的な産業モデルの創出を行っていくべきではないかという論点でございます。下の図は、今申し上げたところを図にしてあります。

6ページ目をご覧下さい。AI等の技術深化をにらんだデータの収集・分析を促進する仕組みの構築でございます。データの有効な利活用には、従来からデータの収集、蓄積が重要でございましたけれども、人工知能等の開発競争の激化によりまして、その重要性、緊急性が一層増しているところでございます。

日本におきましては、さまざまな主体、企業ですとか行政機関等にデータが一定程度は蓄積されておりますけれども、その蓄積量は企業によっては限定的であったり、分散されていたりと、統合

的な解析はなかなかできずに、データが有効に活用されていないのではないかという問題意識でございます。したがって、AI等を活用しましてビッグデータ解析を進めて、より高度な成果を得ていくためには、プライバシーにも配慮しながら、分散したデータの分野を超えた統合、解析を促進する仕組みを構築していくべきではないかという論点でございます。

下に西川委員のPreferredの会社概要を記載させていただきましたが、国内でも他社と連携をして、人工知能の開発を進めているベンチャーも出てきているところでございます。

7ページをご覧下さい。サイバーセキュリティに関する論点でございます。こちらはユーザー側のサイバーセキュリティの論点でございますけれども、左下のグラフをみていただきますと、インシデントの報告受付数は年々増加傾向にあるところでございまして、手口も巧妙化しているところでございます。さらに、IoT社会が進展してきますと、脅威自体も増大してくるということでございまして、政府関係機関、企業への標的型サイバー攻撃によりまして、大量の情報漏えい事案も発生しているところであります。一方で、企業規模に応じまして、具体的にどの程度のレベルの対策を講じればよいかというのが必ずしも明らかでないという課題がございます。

したがいまして、今後、政府機関、独立行政法人、特殊法人については、総合的な対策強化を図りつつ、その対策の不断の見直しが必要ではないか。重要インフラ事業者、民間企業においては、それぞれの特性を踏まえながらセキュリティ対策を促す取り組みを推進すべきではないかという論点でございます。併せて、現行のセキュリティ対策の概要ということで簡単に整理させていただきました。

8ページご覧下さい。標的となりやすい機関等の対策強化についてでございます。経済社会活動の基盤である機能やサービスを提供して、支障が生じると重大な悪影響が生じる可能性がある政府機関や重要インフラなどのセキュリティ強化が重要でございます。

左下のグラフをみていただきますと、セキュリティインシデントの発生状況としまして、政府・公共、教育、電気・ガス・水道、金融、医療・福祉に対するインシデントが過半数を占めているところでございます。

したがいまして、標的となりやすい機関の対策強化に当たりまして、独立行政法人、あるいは府省庁と一体となって公的業務を行う特殊法人なども国の行政機関に準ずる対策を講ずるなど、国全体として対策強化すべきではないかということでございます。

その中でもIPAにおいて、従来から政府、独法、企業等に対する支援、ガイドラインの策定、情報提供ですとかサイバーレスキュー隊による支援、サイバー情報共有イニシアチブの運営等を行って参りました。こうしたIPAの知見、経験を生かして積極的に貢献していくべきではないかという論点で

ございます。

9ページ目をご覧下さい。重要インフラの対策強化についてです。2020年の東京オリンピックを控え、重要インフラ事業者のセキュリティ対策の強化が重要ということでございます。ロンドンオリンピックにおきましては、開会式の直前に電力網を対象としたサイバーテロの予告があって、開会式での照明システムへのDOS攻撃が40分間続くなど、サイバー攻撃のリスクが高まったという事例もあったところでございます。

したがいまして、重要インフラ事業者に対しまして、平時における情報共有体制を強化するとともに、緊急時におけます被害拡大を防ぐことが重要でございます。平時、緊急時、それぞれのセキュリティ対策の実効性を高めることを検討すべきではないかという論点でございます。

併せて、現行の重要インフラに関する取り組みを簡単に紹介させていただいております。重要インフラ事業者みずからの責任で行うセキュリティ対策に対して、政府として支援を実施していくという施策で、現行13分野が指定されております。情報通信、金融、航空、鉄道、電力、ガス、政府、科学、クレジット、石油、物流、医療、水道等となっているところでございます。

10ページ目をご覧下さい。企業のセキュリティ対策強化についてです。これはこれまでの委員会でもご議論がありましたが、我が国において、経営層のセキュリティ意識が低いことが課題でございます。

積極的にセキュリティ対策を推進する経営幹部がいる企業は、グローバルに比較すると低いという結果になっております。また、サイバー攻撃の予防は取締役レベルで議論すべきか、という問いに対して、日本は国際的にみて低いという結果になっております。さらに、中小企業におきましては、セキュリティ対策に割く余力が少ないという課題がございます。

したがいまして、民間のセキュリティ経営の基準となりますガイドラインの整備を加速すべきではないかということでございます。また、経営層が主導してセキュリティ対策を積極的に強化する企業が市場から評価される枠組みとしまして、第三者認証制度を確立するなど、経営層のセキュリティ意識の向上を促していく必要があるのではないかということでございます。さらに、中小企業におきましては、専門家が企業内にいないということも踏まえまして、よりわかりやすい丁寧な支援を進めていくべきではないかという論点でございます。

11ページをご覧下さい。論点4でございます。ソフトウエア製品・IoT製品の安全性・信頼性強化についてです。IoTが進む中で、ソフトウエアの欠陥等が与える社会的影響がさらに増大していく中で、あらゆるものがインターネットにつながることで、ソフトウエアの単体を超えてシステム全体での安全性、信頼性を検証していくことが重要になってきているところでございます。

これまでソフトウエアの脆弱性については経産省で規定を定めて、情報収集、開発者との調整、公表などの規定を整備してきたところでございます。一方で、脆弱性だけではなくて、データの外部通信の問題、システム障害等のソフトウエアリスク、それからシステム開発、運用におけます取引の安全性確保の問題も課題になっているところでございます。

ソフトウエアの安全性・信頼性上の問題として3点挙げさせていただきました。脆弱性につきましては、今年の7月にアメリカの自動車メーカーのリコール問題があったり、データの外部通信についても2013年にある企業による日本語入力システムからの外部サーバーへの送信の問題もあったりと、世界中で問題が発生しているとことでございます。3番目のバグにつきましても、今年の4月にアメリカの金融情報会社の取引システム障害による事例があったということでございます。

したがいまして、こうしたソフトウエア製品、IoT製品、システム開発等の広範な安全性、信頼性上の問題につきまして、リスク情報の取り扱い制度や安全基準、ガイドラインなどの整備を行っていくべきではないかという問題意識でございます。

下にソフトウエア脆弱性の取り扱いフローと書いてございますけれども、平成16年に経産省の告示で定めて、IPAを窓口としまして情報収集等の取り扱いが行われているところでございます。

12ページをご覧下さい。共通の課題でございますけれども、セキュリティ人材の能力評価制度のあり方についてです。日本企業のセキュリティ対策において不足している人材は約8万人といわれておりまして、さらに、セキュリティ対策に現在取り組んでいる人材のうち16万人がスキル不足ということで試算されております。ユーザー側、ベンダー側双方でセキュリティ人材の育成、登用、活用を進めていくことが重要でありまして、このためにはセキュリティ人材の能力を評価する仕組みが必要ではないかということでございます。

したがって、情報処理技術者試験を改革しまして、必要とされる人材像に基づいた試験創設、常に能力を評価、担保できる更新制の仕組みの導入が必要ではないかという問題意識でございます。

人材像をみていただきますと、情報セキュリティマネジメント人材でございますけれども、来年春に新しい試験の導入を予定してございます。実際に安全な情報システムをつくる人の資格ということで情報セキュリティスペシャリスト人材ということでございます。特に高度化するサイバー攻撃、ITの技術革新などの動向を踏まえまして、セキュリティ対策のアップデートを常に図っていく必要があるのではないかということで、登録更新制の導入等によりまして、能力を適時適切に評価できる試験制度の充実に向けた検討を行う必要があるのではないかということでございます。

13ページをご覧下さい。その他の論点ということで、サイバーセキュリティ産業の成長産業化につ

いてです。国内の情報セキュリティツール市場、あるいはサービス市場の規模は増加傾向にございまして、今後この需要が一層増加することが見込まれているわけでございます。

一方で、こうした激しい変化に対する機動性が求められておりますので、革新的な新規事業、技術開発に挑戦するベンチャー企業などの活性化が重要であるということでございます。このために、サイバーセキュリティ産業の成長産業化を図っていくに当たりまして、政府系のファンドなどを活用した投資などによりまして、国内外で大規模に活躍できるベンチャー企業等の振興が必要ではないかという論点でございます。

以上が論点の紹介でございますけれども、幾つか経過報告をさせていただければと思います。

15ページをご覧下さい。先ほどの論点5でセキュリティ人材あり方についての論点を紹介いたしましたけれども、8月から研究会を設置いたしまして、具体的な専門的な制度の検討を行っているところでございます。その結果、9月上旬ころまでに取りまとめて、情経小委の関係会議体に報告するということにしております。

16ページをご覧下さい。情報経済小委員会の中間取りまとめにおきまして、企業間連携の中核拠点を創設していくことにしておりまして、その経過報告でございます。簡単にコンセプトをまとめておりますけれども、革新的なプロジェクトを創出して、必要な規制改革の提言とルール形成を行って、グローバルかつ業界横断的な企業間連携の促進、それから投資への企業マインドの変革をねらいとしまして、チャレンジ促進のための規制改革の提言を行っていく機能、それからセキュリティ、プライバシー等の基盤整備を行っていく機能、IoTプロジェクトの発掘、実現を行っていく機能をあわせもった新しい枠組みを検討しているところでございます。

17ページをご覧下さい。市場を活用したIT経営の推進でございますけれども、今年の5月28日に東証と連携して、攻めのIT経営銘柄を選定したところでございます。この銘柄選定の過程の中で、東証に上場しております全企業を対象としてアンケート調査を行いましたところ、210社から回答がございました。右の図をみていただきますと、ROEが高い8%の以上の企業につきましては、積極的にIT活用の体制をとっているといった特徴が確認されたところでございます。

18ページをご覧下さい。研究開発の関係でございますけれども、本年5月に産業技術総合研究所に人工知能研究センターが設置されたところでございます。国内外のすぐれた研究者技術を集結して、ビッグデータを活用しました研究人材育成を推進しております。

最後、19ページでございます。これも研究開発絡みでありますが、IoT推進に不可欠な技術開発、先進モデル創出ということでございまして、IoTの高度なデータ利活用を実現するために、センサー側でのデータ処理技術を初めとしましてデータの収集、蓄積、解析技術といった分野横断的な活

用可能な基盤技術の研究開発を推進していくことにしております。

端末側で高度なデータ処理を行う情報収集システムのための無給電データ収集端末や、超大容量、高速の読み書き可能なデータストレージ、AI専用の計算機、サイバー攻撃から守るための検知、予測、防御技術といったものを研究開発にて検討しているところでございます。

それから、モビリティや製造・工場、行政・インフラなどのさまざまな分野におけるデータを活用した先進モデルを創出していこうということで、課題となる規制制度、民間企業のビジネスモデル、商慣習をあわせて見直しながら行政、民間企業のデータ利活用を推進していく先進モデルを進めていこうということを検討しているところでございます。

以上が経過報告でございますけれども、本日は、先ほど申し上げた論点1から論点6までを中心にご議論いただければと考えております。

事務局からの説明は以上です。

○村井委員長

ありがとうございました。それでは、ここからは自由討議ということで残りの時間を進めたいと思いますので、いつものように、ご意見のある方は名札を立てていただいて、できるだけ立った順にこちらからご指名させていただきたいと思いますので、よろしくお願いします。

議論が、IoTのデータ利活用とセキュリティがありますけれども、どちらも関連する内容はご遠慮なく混ぜていただいて、データ利活用からセキュリティへ移行する形で議論を進めて参りましょう。

○横塚委員

横塚でございます。3点申し上げたいと思います。

まず、論点1、2のデータ利活用のあたりでございます。データを活用した新しい産業モデルの創出ということは、まさにビジネスそのものでございまして、CAOではなくてビジネスリーダー、あるいは経営者そのものがテクノロジーを使って自分のビジネスをどうイノベーションしていくかという動きになりますので、ビジネスリーダーがマインドを変えていく、あるいはデジタルテクノロジーについて理解を深めていく、そういう施策が重要な施策になっていくのではないかと思います。

日本の経営者におきましては、テクノロジーに関して自分のことと理解していない経営者も多いものですから、そういう施策が必要ではないかというのが1点です。

2つ目ですけれども、データ利活用という観点で少し問題だと思っているのは、固有名詞を出さないとわかりづらいので、実は私、東京海上出身なのですけれども、上場大企業の多くが今、社内でどんな感じでパソコンを使っているかという観点でみてみますと、まず、電車に乗ってなくしたらいけないので、パソコンは基本持ち歩かない。社内の端末におきましてもいろいろなアクセス規制があ

って、例えばフェイスブックにはアクセスできないとか、いろいろなサイトには行かないような形でがんじがらめのセキュリティがかかっておりまして、これではデータ利活用のインフラが全然整っていない。現状に物はあるのだけれども、ややtoo muchなセキュリティの誤解みたいなところから、そんなことが実際に多くの企業で運用されております。

ですから、例えば、A企業とB企業とC企業の3つが一緒になって新しい何かをつくっていこうとしたときに、3人が会わないで1つのウエブサイトか何かでいろいろ議論し合おうとしても、社内の端末にアクセス規制が入っていて、なかなかそういうことができないような状態になっているのです。これは民間の問題ではありますけれども、そういったことを改善していって、メリハリのついたセキュリティ対策をとることが産業政策上非常に重要だと思いますので、セキュリティに絡めて各企業の中のデータ活用のインフラ整備の部分についても着目していく必要があるのではないかと思います。

3点目は、サイバーセキュリティのことでございます。ご案内のとおり、サイバーセキュリティは国家と国家との戦争に近いような厳しい戦いになっている様相を呈しております。したがって、世界で戦える超一流のトップガンのエンジニアを育成していくことが日本国にとって非常に重要ではないかと感じております。

そういう意味でいうと、超一流のトップガンが日本の中に何人いるのかというと、非常に限られた数しかいないのではないかと思います。防衛省、警察、あるいは経済産業省一体となって日本のトップガンのエンジニアをどう育成していくか。これはお金をかけてでも絶対やっていかないといけないことではないかと思うのです。東京オリンピックの例が出ましたけれども、例えば東京オリンピックでいきなり電子時計をハッキングされて、100メートル予選で7秒台が出たら、もう東京オリンピックは終わりになってしまいますので、そういったものがしっかり守れるようなエンジニアを育成していくことが必要だと思うのです。

そういうトップエンジニアがそんなに数多くいないということになりますと、上場企業一社一社がそういうエンジニアを会社の中に育成していく、抱えていくということは、自主的にはかなり難しい話になってくると思いますので、重要インフラだけでなく一般的な企業も含めて、日本としてサイバーセキュリティからどう守っていくのか、そういう検討も必要ではないかと思っております。

以上です。

○村井委員長

ありがとうございました。野原さん、お願いします。

○野原委員

本日は、少し早めに途中で退席させていただくので、早目に発言させていただきます。また、明日内

閣のサイバーセキュリティ戦略本部があり、同様なコメントをしたいと思っているので、今日はサイバーセキュリティに関連して4点コメントしたいと思います。

まず、先ほどのお話にもありましたが、年金機構への標的型攻撃に限らず、官民問わず日本の組織がターゲットとなるサイバー攻撃のリスクが非常に増加しています。また、来年は伊勢志摩サミットがありますし、2020年には東京オリンピック・パラリンピックもあるので、日本をターゲットにしたサイバー攻撃のリスクが非常に高まっていることは皆様もよくご存知のとおりです。　それを踏まえて本日資料でも論点3で、政府、重要インフラ、民間企業全体のサイバーセキュリティ対策を積極的に強化拡充し、体制も充実するということをうたわれているわけで、それについては大変重要なことだと思いますし、しっかりと進めていただきたいと思っています。それがまず1点目です。

しかしながら、セキュリティ対策は、ただ積極的に強化拡充するだけではうまく働かず、セキュリティと利便性、使い勝手とのバランスをとることが重要だと思います。セキュリティリスクが高まっているため、政策を検討する場で、対策の強化拡充については議論が活発に行われますが、利便性、使い勝手という課題は軽視されがちで、結果として話題になりにくいから吹き飛んでしまうようなところもなきにしもあらず、かと思います。

例えば年金機構のインシデントの場合、ガイドラインでは個人情報をネット非接続の環境下に置くことになっていますが、実態としては業務上の使い勝手がよくないということもあるのか、あちこちの部署で個人情報を必要な部分だけを自分のPCに置く、あるいは共有サーバーに置いていたということが起こっており、これが情報漏えいの1つの原因になっています。現場の実態とガイドラインとに乖離があったということが今回の事件につながった側面があります。担当者のセキュリティ意識の醸成が足りなかったかもしれませんが、業務の使い勝手を改善すれば、ガイドラインとの乖離が防げたかもしれないと思います。

したがって、経産省でやられる政策、例えば経営層へのガイドライン検討の構築に際して、使い勝手とセキュリティを両立させることを配慮していただきたいと思います。その点をしっかりと進めていただきたいというのが2点目です。

3点目について、先ほど横塚委員もおっしゃいましたが、民間でも官でもセキュリティ対策を重視した結果、現場の使い勝手がよくない状況が見受けられます。その状況を改善するために、セキュリティツールやソフト、サービスの使い勝手を向上していくことも重要だと思います。認証の仕方や、暗号化の仕方、パスワード管理の方法等、充分な機能は提供されていますが、その使い勝手までは充分な配慮がなされていないのではないかと思います。

この要因として、ツール導入の決裁権者とユーザーとが別であるため、決裁権者はセキュリティ機

能とコストを比較して選択するということが起こりがちで、現場での使い勝手への配慮が充分でないということも起こりやすい状況にあるかと思います。

そういう状況を踏まえた上で、セキュリティ関連のサービス事業者、ツール開発事業者に向けて、使い勝手向上へのモチベーションができるような仕組みを考えていただきたいというのが3点目です。

最後は、セキュリティ産業の育成、拡充が重要だということです。IoTやビッグデータ、AIといった新技術が進展する中で、サイバーセキュリティに必要な技術も変わっていきます。新しいツールデバイスやサービスを開発・提供するベンチャー等の創出、新事業領域の創出が重要だと思います。

その意味で、今回、論点3の最後にその他として書いてありますが、その他的扱いではなく、セキュリティ産業の育成、拡充策をしっかり検討いただきたいと思います。

以上です。

○村井委員長

ありがとうございました。それでは、三輪さん、お願いします。

○三輪委員

三輪です。よろしくお願いします。私は、多分セキュリティということで呼ばれていると思うので、きょうは論点がとても多くて、今書いてみたら6つくらいあるので、早口で手短に行きます。

論点3(2)標的となりやすい機関ということで、グラフが出ているのですけれども、これをこのように紹介されると、政府とか教育機関、大学といったところが攻撃を受けやすいと誤解すると思うのですが、これはJPCERTで把握しているインシデントの数なので、必ずしも攻撃の数とは一致しないのです。よくインシデントが発生しやすいところは当然、攻撃数が多く換算されます。なので、これをもってサイバー攻撃の過半数が上記機関だ、というのは、数字としておかしいと思います。

実際、日本の国力ということを考えたときに、攻撃を受けやすい、あるいはちゃんと守らなければいけないものの一つに、製造業が入るかと思います。知的財産をどれだけ守るか。そこに対する攻撃も非常にたくさん来ている。ところが、大分進んではきているのですけれども、日本の製造業の方は、それがもっていかれたから何なのとか、それで直接何もないじゃないという反応が多くて、敏感な会社もあるのですけれども、言い方を変えればおおらかな会社も非常に多くて、そういった製造業、ここでいう企業37%というところが本来のターゲットになっているのではないかと思います。

そういう意味では、3(2)でいくと、やるべき対策は、平時から情報共有をすることだと思います。もともと今のサイバー攻撃はみえないということが最大のポイントなので、いかに攻撃に気づいていくかのほうが大事なのです。年金機構のサイバー攻撃の場合も、今回はNISCからの連絡があり偶然気づいただけで、もし連絡がなかったら多分今ごろ誰も知らないと思うのです。そういうことから考え

ると、いかにセキュリティの監視が大事かということだと思います。

なので、セキュリティの監視というところを平時からしっかりやるところを義務づけていかないと気づかない。JPCERT、あるいはNISCから指摘がなければやらなくていいという雰囲気が今あるので、そうではないようにすべきであると思います。

次が論点3(4)、ユーザー側企業のセキュリティ対策として、資料の後ろにITの利活用をやっている会社のランキングがついていたと思うのですけれども、同じようにセキュリティの強度だって頑張っている企業をランキングしてしまえばいいではないですか。最下位を公開するわけではないので、トップ20ぐらいだったら公開してしまってもいいと思うし、もともとそういうのに参加しないという企業は、それはそれで構わないので、そういったセキュリティ強度を見える化してランキングづけするということは、それが認証制度であろうが何であろうが構わないのですけれども、必要かと思います。

次に、論点4、IoT等に関しては、脆弱性発見の報奨金という制度を導入すべきだと思いますし、それをほぼ義務化ぐらいまでもっていったほうがいいと思います。一部の企業、例えばGoogleや、国内だとサイボウズ等報奨金を出しており、それを目的に自分の時間を割いて脆弱性をみつけて指摘し、それを周囲が賞賛し、またそれがモチベーションになるというのが今うまく働き始めているので、そういった報奨金というのは、ほぼ義務づけたほうがいいかと思います。あるいは、バグハンターの育成に努めれば、当然ながら、さっきいわれたセキュリティ人材、トップガンの育成にもほぼ直接的につながると思います。

次に論点5について、ここでのポイントは、こういう人を必置するという義務化がどこまでできるかだけだと思うのです。これだと個人のモチベーションだけで試験をとらせようというだけの話にしかなっていないように思えます。それだけだと誰も動かないので、必ずその資格をもった人を企業に1人置き、その人がシステムの発注をする、あるいはその人がプロジェクトの真ん中にいる、というように明示的に何らかの対策を行い、それを必置すればよいかと思います。もちろん急には無理だと思うので、徐々に浸透させ、必ず置く形にもっていくように方向性を示すべきだと思います。

最後に論点6ですが、単純にベンチャーにお金を出そうといっても絶対にうまくいかないので、政府関係機関や特殊法人での積極的な活用が必要かと思います。お金だけ投資されても企業は絶対に成長しません。ベンチャーが成長する一番のもとはお客さんです。いかに実際に使われて、そこでバグが出たり文句をいわれたりしながら、初めてそこで成長します。特にアメリカなどでは、政府関係機関での積極的採用をすることで、あっという間にベンチャーが成長します。

かつ、今私も実際自分の会社をやっていて思うのですけれども、今一番の悩みは人がとれないことです。それは私の知っている同じセキュリティ業界のほかの会社の人もみんなパンクしていて、仕事

はあり余っているのですけれども、逆に人がとれないのです。セキュリティ業界に来ようという人がそもそもいないし、かつとろうと思っても小さい会社だと誰も来てくれません。人材確保というところが最大のネックで、資本とか以前の話です。

なので、国としてベンチャー企業の育成に背中を押しているということで、例えば経産省がそういうベンチャーを集めて、就職活動フェアみたいなものをやってくれると、お墨つきがついていて、学生や中途採用であっても夢がもてるのではないかと思いました。

以上です。

○村井委員長

ありがとうございました。有野さん、お願いします。

○有野委員

電機連合の有野でございます。私からは1点です。

やはり論点1が我々にとって非常に大事なところです。ITの活用が産業構造を大きく変化させると一言書いてありますけれども、本当に具体的にどうなっていくのか。将来像の共有が大事だと書かれてあるとおり、どういう社会になるかをしっかり共有しておかないと、それぞれかかわる分野でどう論議をしたらいいか分かりません。

先日行われた電気産業にかかわる労働組合の世界会議では、ドイツの労働組合がインダストリー4の労働に対する影響について論議をしておりました。IT化が進むくらいのことで実はそれほど変化がない、とのことです。今までの構造改革だと企業内、あるいは少なくとも産業内で何とか対応してきたのですが、恐らくもっと広い、あるいはもっとグローバルとの関係になって、これが雇用にどう影響してくるのかとか、働き方への影響とか、格差の問題とか、今から対応を考えておかなくてはいけないのではないかというぼやっとしたイメージ論議しかできていないのです。

そういった意味では、ぜひ具体的モデルを積極的に出して議論を広め、深めることが必要だと思っていますので、ぜひ論点1を積極的に進めていただければありがたいと思います。

以上であります。

○村井委員長

ありがとうございます。石井さん、お願いします。

○石井委員

筑波大学の石井です。

資料2の2ページ目で情報経済小委員会の中間取りまとめの方向性の1で制度を変えるという記載がありまして、その中で法制度の見直しなども書かれていますが、その関係の討議事項として、

論点2が深掘りされていくのでないかと理解しております。

論点2の6ページを拝見すると、AI等を活用したビッグデータ解析を進め、より高度な成果を得るためにはプライバシーに配慮しつつ、分散したデータの分野を超えた統合、解析を促進する仕組みを構築するべきと書いてあります。確かにデータが有効に活用されていないという現状があるとして、さまざまな研究開発の中で、例えば病気の予防ですとか治療ですとか、交通事故の防止などの社会の安全性を高めるといった公益性のある利用の仕方をするということでしたら、その利活用の必要性は認められるというように考えております。

他方、その方法を具体的にどうするのかということを考えた場合には、プライバシーへの配慮も考える必要がありますので、個人情報保護法の改正法との関係で、新しい制度的な例外をつくることになる可能性もあると考えております。

その場合には、法律にどのように書き込むのかという点において、目的や要件、執行の点などさまざまな課題が出てくることになります。深掘りをしていく際には、ここではごく簡単にしか申し上げませんでしたが、制度的な例外を設けるのであれば、どのような論点が出てくるのかということを具体的に出した上で、慎重に検討していくということもあわせて必要になってこようかと考えられます。

以上です。

○村井委員長

ありがとうございました。岡村さん。

○岡村委員

まず、論点1、2の関係でございます。先ほど、具体像が見えないという発言がございましたが、私が勝手に考えるのは、少子高齢化する中で国内にノウハウを蓄積しつつやっていくということになると、二番煎じ、三番煎じになる危険性があるかと思います。クラウドを使ったIoTのコントロール等、そういう細かい技術は日本人が一番得意なはずですから、ノウハウを国外に逃がさないようにして蓄積していくというスタイルからすれば、そういう方向性が最も考えられるのではないかという気がいたしました。

それからセキュリティの関係について、私はJPCERT理事もしていますが、今般、JPCERT等々の通報がいろいろ事件を発覚させているようでございますが、まず今の問題は、侵入されたかどうかもわからないというのが、企業であったり自治体であったりする。それから、侵入されましたよということをJPCERTがいったところで、どう対応していいかわからないというのも事実である。これは先ほど三輪委員がおっしゃった考え方ともかなり一致すると思います。

そうしますと、それに対する処方箋として、企業等の自助努力と国のサポートが車の両輪になる

のではなかろうか。自助努力という面では、今、CSIRT協議会をやっている関係もございまして、CSIRTをつくりたいという団体が多いという状態です。この間、NISCの補佐官もされている電機大学の佐々木先生とお話ししていて、「なんちゃってサート」では困るという言葉が飛び出したのですけれども、とりあえずつくろうということの限度ではいいわけですが、なかなかノウハウが蓄積されないので、そうしたCSIRT協議会などの立ち位置というか重要性が、先ほどのサポートという意味も含めてより重要になってくるだろうと思われますので、もう少しこういう組織づくりということについても、経済産業省としてお力をお入れいただければと感じるわけでございます。

あと1つ、情報セキュリティマネジメント人材ということを12ページのような形でおつくりになることは非常にいいことだと思います。

ただ、ここで注意しなければならないのは、余り閾値を高くしてしまうと、結局少数の人材しか集まらないというような状態になりますので、中高年齢者にも敷居の低い、徐々にレベルアップし、スキルを磨きやすいような形のグレード制をつくって、企業の性格とか規模に応じたものに対応する人材を生み出せるようにお願いしたい。

そうでないと、結局、きょうの資料の中にも出てまいりましたけれども、委託の連鎖であるとか、委託先の小規模企業がループホールになっていることは昔と変わりありませんので、そこを埋める必要があるということも大変重要なことではないか。

それと同様に、中高生ぐらいでも興味がある人間はそこから進んでいけるような、まさに若年層からマネジメント人材の育成ができるような形にしていただきたい。いずれは、例えばNIIに入っていただくとかという形で高度な人材に育っていっていただきたい。そのためにも低いところから、だんだんグレード的に始めるという形をご用意いただければと存じます。

以上です。

○村井委員

ありがとうございました。それでは、澤谷さん、お願いします。

○澤谷委員

3点です。最初の論点1、2につきましては、新しいビジネスをつくり上げるときには、やはりトライアル・アンド・エラーで失敗がつきものだと思います。そういった意味では、フェイルファースト、失敗から学ぶといったことを積極的にできるような形で進められればと思います。

その場合に、ビジネスのリーダーが技術のデジタル化社会に向けて技術の最低限のことを身につけていくといった方向性、もう1つは、テクノロジーのリーダーが視野を広げ、ビジネスまでわかるといった方向性があると思いますので、両方ともやってみる。どちらかというと、テクニカルリーダーがビ

ジネスマインドを広げるようなリーダーが海外をみても多いのではないかと思いますので、そちらの方向も考えていければと思います。

2つ目に、フェイルファーストをする場合には、そもそもセキュリティをどのようにデザインするか。ガイドラインとか運営といったレベルから、ポリシーをどうやって設計して、どこまで許容するのか。コンティンジェンシーとしてどこまでプランとして含めておくのかといった、セキュリティのデザイン人材といったものが必要なのではないかと思います。そういったデザインをした上でマネジメント人材、あるいは技術のスペシャリティー人材が生きてくるのではと思います。

最後に、セキュリティを使うのはシステムと実際に人であるといったことを考えますと、一般ユーザーのセキュリティリテラシーを上げていくことが重要であると思います。その場合には、企業内だけではなく、小学生から。携帯電話をもつようになったら、そういったセキュリティの最低限のことを理解していくといったことが必要なのではないかと思います。

以上です。

○村井委員長

ありがとうございます。有賀さん、お願いします。

○有賀委員

1つご報告と2、3ご意見を申し上げたいのですけれども、1つは、先ほどご紹介がありましたようにセキュリティ人材の確保に関する研究会、今、私が座長でやらせていただいておりまして、進行中でございます。8月後半ないし9月頭までにはセキュリティ人材の技術的なレベルの確保でありますとか、それの登録、更新等を含めた担保をどうするかというようなことについて、論点をまとめてご報告したいと考えております。

それから、きょうの論点を通してどの論点というよりも、ちょっと気になりますのは、この委員会、どちらかといえば今回は利活用側に相当振って議論をしているという認識なのですが、コアテクノロジーの技術開発だとか先進モデルの創出ということは書いてはあるのですけれども、もうちょっとそこら辺を具体的に詰めておく必要があるかなと。

具体的に申し上げれば、ネットワークあたりでも、例えば今、ソフトウエアディファインドでもって全然変わってくるとか、組み込みソフトもIoTの世界になると一番主役でありますから、その辺の話だとか、情報セキュリティはもちろんですが、あとビッグデータでデータベースに関して意外と研究が進んでいない気もしますので、そういうことだとか、それから、産研にAIのセンターをおつくりになりましたけれども、AI関係だとかロボティクス、この辺はターゲットを定めてかなり具体的に述べておかないとまずいかなという気がしました。

2番目は、制度についてもう少し本格的に。例えば重要インフラ等へのICTの利活用に関して、規制という言葉は余りよくないかもしれないのですけれども、どこまできちんとしたルールづけをするかということを単なるガイドラインレベルの努力目標でやりなさいということだけで本当にいいのかというところが非常に気になります。この辺は特に経産省、エネルギー関係ですとかインフラ関係を統括しておられるので、いわゆる重要インフラの安全性を確保するために単なるセキュリティだけではなくて、中に入っているソフトだとかシステムを含めてどうするのだということを相当具体的に詰める必要がある気がいたします。

もう一点は、論点全体がどちらかというと大きい会社を相手にしたような論点が多いのですけれども、ベンチャーではネットワークですとかウエブとか最新のテクノロジーを活用して、結構身軽な商売をどんどん立ち上げている。こういうものが将来GoogleだとかAmazonだとかという形に育っていったら非常にうれしいのですけれども、スタートアップをいかにうまく育てるかということ。大きい会社をどうするかというのもあるのですけれども、小さいスタートアップをどこまででかくするかというのも作戦をもって取り組んでおかなければいけないのではないか。

この3点がご報告です。

○村井委員長

ありがとうございました。それでは、松本さん。

○松本委員

松本です。

まず、論点2から行きたいのですけれども、AI等の新しい技術を使っていろいろな仕掛けがでてくるといった点で、セキュリティとも絡むのですが、AIを使ってセキュリティを強化するという話はいろいろ出てきていて、実際に使われていたりもするのですけれども、逆に、攻撃側のAIが、AIで守っている側をだますこともあるのです。

小さな例ですと、指紋認証のシステム等のうち、ある種のAI的パターン認識的な技術を使ってボトムアップ的に組み立てられてきたものについて、ある種の脆弱性があることが10年以上前から指摘されています。それから解釈を拡げていきますと、やはりAI対AIの戦いとなってきますので、そういった観点も必要なのかなと考えます。

それから、論点3にも入るのですけれども、今そこにある危機に対してどう対処するかという話があろうかと思います。三輪委員もおっしゃっていましたけれども、観測が非常に重要でして、例えば私どもも大学でマルウエアに感染したIoT機器からの攻撃を選択的に検出するようなハニーポットを作ってみますと、世の中で知られていない、特定されていないマルウエアがたくさん存在しており、あっと

驚くような装置がインターネットにつながっていて、特に管理用の通信がのっとられてマルウエアに感染して、ほかのIoT機器を（例えばDoS）攻撃をしていたりするという実態が明らかになってきています。新しく技術を開発して良いシステムを作って、弱いIoT機器を置きかえていくということが必要なのですが、一体どうやってそれをやったらよいのだろうと考えると絶望的な感じがします。

つまり、今、既に広まってしまっている弱い機器をどうやって駆逐して強いものにしていくのかということが1つ大きな課題であろうかなと思います。この意味では、先ほどのじっくりいくという戦略に対しては、セキュリティの新しい技術を開発して、それを積極的に取り入れていくことに対してインセンティブをもたせるような方法があるのかなと考えます。

それから、現場対応に関しては、例えばIPAでもサイバーレスキュー隊といった形で初動体制に対して貢献するようなことがあって非常に評判がよいと伺っていますけれども、人手不足なのではないかと思われるので、今後どうやってそのような実務レベルで戦力になるよい人を集めてくるのかというところが必要かと思います。

例えばIPAには研究員という名称の職員がたくさんいますが、IPAは研究してはいけないというルールになっているらしくて、ちょっと不思議な感じがしているのです。例えば研究とか、本来定められた業務以外の遊びといいますか、何か新しいことを考えてみようというようなことについても、何パーセントかは仕事としてやってよろしいという条件にすると、かなりよい人が多数来て、定着するのではないかと思いますので、そういった仕掛けも産総研だけではなくて、IPAといった現場に近いところでも取り入れられるといいのではないかと考えます。

ちょっと長くなって恐縮ですが、もう2つお話しさせてください。1つは、新しい技術を開発していく際に、積極的、能動的に調べると情報が得られそうだが、攻撃技術だと受け取られた場合、観測しているつもりでも捕まってしまうということがあり得ます。

つまり、研究開発をする側、セキュリティ技術を開発する側が安心して開発できるような仕掛け、制度が必要かと考えます。リバースエンジニアリングの問題なども同じように考えられます。

最後ですが、ソフトウエアないしセキュリティ技術を含めてよい製品をつくって、どう広めていくかということについては、三輪委員がおっしゃっていたように、やはり政府系が大口ユーザーになり、需要が見込まれ使われるのだということにして、安くよい技術が手に入るような環境と整え、それを政府系以外でもみんなで使えるようにしていくという作戦がよいのかなと考えます。

以上です。

○村井委員長

ありがとうございます。水嶋さん、お願いします。

○水嶋委員

本日初めて参加させていただきます、新しくJEITAの会長に就任いたしましたシャープの水嶋でございます。よろしくお願いいたします。

いろいろご意見ございました。重複があってもいけませんので、シンプルにお話しさせていただきます。

まず、今回、中間取りまとめ、改めて私も、勉強させていただきました。CPSによるデータ駆動型社会の実現というのは、我が国にとって非常に重要な課題であることはJEITAといたしましても認識しております。

7月にCPS社会実装検討タスクフォースをJEITAの中に立ち上げまして、会員企業に加えて関係する団体、あるいは先ほどからお話が出ている産総研の人工知能研究センターなどの研究機関などにも参加いただきまして、IoT社会の実現に向けた取り組みをどう進めていくかという検討に着手しております。今後、その成果についてもこういう場でお話しさせていただきたいと思っております。

今後はやはりデータの収集とその使い道が課題になるかと思います。例えば個人情報とリンクしているようなデータであった場合、個人情報をいかに保護しつつデータを提供いただけるかという部分については、データの利活用が社会的利益に大きくつながっているのだということを国民の皆さんに十分理解していただく必要があるかと思います。リスクの議論ばかりが表に出てしまうと、データを提供いただけないとか、あるいは制約がたくさん加わりますと、収集されたデータが十分な利活用に結びついていかないということがございます。

得られたデータは誰のものだという議論も片方でございまして、持っているデータの所有権はどこにあるのかという議論も含めて、利活用に向けた国民理解の促進、コンセンサスを作っていくということに、政府として実証プロジェクトを通じて具体的な例として示していただくことも必要ではないかと思っております。どこまで匿名性を確保すれば、あるいはどこまで生データを加工したデータであればいいのかといったような基準のようなものを議論していただいて、明確にしていただきたいと思っております。

卑近な例で、当社が今やっている例で申し上げて失礼ですけれども、当社はテレビをつくっており、テレビの視聴データは、それこそ秒刻みで何百万台から、全てとることができます。このデータをどう使うかというときに、大きな悩みがございます。非常に有用なデータですけれども、実際、活用していく上において、個人情報をいかに保護していくかというところが大きな悩みであるということが現場で起こってくるのではないかと思います。

また、個人だけではなくて産業全体で各企業が自分たちの持っているデータを提供していただ

かなければいけないわけです。けれども、そのデータは各企業にとって非常に大きな知的財産なわけです。例えば車メーカーが、自分たちの売った車がどういう走行状況にあるかというのは、その車メーカーが全部ためてあるわけです。これは非常に大きな経営資源ですけれども、これを提供していただかないと、他の産業、他の企業で有為に活用できない。このようなところにどういうガイドラインを設けていくのか、あるいはその所有権と価値に対する商的な流通をどう考えるのかということは非常に重要と思っております。そのためにも、国民理解の促進というのが1つのキーワードになると思っております。

セキュリティにつきましては、皆さんがおっしゃるように非常に大きなリスクです。人は、リスクを背負うぐらいならメリットは別になくてもいいと思いがちなので、メリットを示すとともに、リスクのミニマイズのためにどう取り組むか。リスクはゼロにはならないので、メリットとしっかり天秤にかけながら導入を図っていくということの理解をいただくものだと思っております。

セキュリティの議論は、専門家の皆様がされましたが、セキュリティのインシデント情報の共有化については、本当にタイムリーかつ漏れがない状態で、どのように制度を実現していくかということは非常に重要だと思っております。この辺について必要な手立てをぜひスピード感をもって進めていただきたいと思います。

最後に、セキュリティの高さが商品なり製品なりサービスなりの価値であるという認識を広めていただく必要があると思います。そのために例えば今、政府調達においてもISO／IEC15408に基づく認証取得を義務づけていないのですが、政府調達、あるいはいろいろなところでの調達にこのセキュリティに対する認証取得を必須条件とするといったような取り組みに先行的に取り組んでいただく必要があるのではないかと思います。セキュリティのレベルが高いということが、その商品のサービスなり価値につながっていくという仕組みづくりを考えていただく必要があるのではないかと思います。

以上でございます。

○村井委員長

ありがとうございます。唯根さん、お願いします。

○唯根委員

ユーザーというか、消費者として発言させていただきます。

利活用については、論点2でプライバシーへの配慮という点で、また、サイバーセキュリティについて、こういった国の取り組みについて、私たち消費者は何も知らないで、ネットを便利に使っているユーザーが殆どなので、ぜひ情報提供していただく手だても考えていただきたいです。今回の論点は、国民への周知というか理解を前提として考えていただきたいというところをぜひご検討いただきた

いと思います。

また、三輪委員がおっしゃっていたように、バグハンターのような形というのは、少しでも関心をもっている消費者であれば参加できるわけですから、そういう点では個人でも一人一人が参加できるのではないか、そういう資質のある方をみつける手段としても、こういう取り組みを早い段階でわかりやすく情報提供して、広報というか啓発も含めて考えていただきたい。教育の分野にも広がるかもしれませんし、そこも含めてご検討いただきたいと思います。

以上です。

○村井委員長

ありがとうございます。砂田さん、お願いします。

○砂田委員

論点1、2について、先端的なテクノロジーを使いながら新しい産業モデルやビジネスモデルを創出していこうということを考えるときに、テクノロジーとビジネスの視点に加えて、より人間とか社会の視点というのが重要になってきていると感じております。

私は、情報システム学会の一会員として、同学会が掲げている「人間中心の情報システム」という考え方に興味を持ち、それに関連した研究を行っています。そのような立場から申し上げますと、AIの技術進歩によって人の仕事が奪われるといった議論が現在盛んに行われていますが、そういう論点だけではなくて、人とテクノロジーの協働や共創のあり方であるとか、人間や社会が抱える課題の解決を支援するテクノロジーといったことを考えていくことが大切だと考えます。その中から新しいビジネスや産業が生まれてくると思います。そういう意味では、ヒューマニティーの未来とかソサエティーの未来を構想することがますます重要となりますので、産業政策の中にもそういった視点を含めていただきたいと考えています。

それと、サイバーセキュリティに関しては、既にご発言いただいたことと重なりますが、公共調達の条件やガイドラインに入れていくことを検討してはいかがでしょうか。他にも、情報セキュリティ投資に対する減税などの政策ツールを活用することで、投資を活発にさせ、セキュリティ産業の成長を促していくことが大切だと思います。とくに公共調達においては、ベンチャー企業が開発した新技術を導入しやすくするなど、イノベーション促進型の調達を通じて先進的なユーザーを増やしていくことがきわめて重要です。そのためには前例のない調達が行われやすい仕組みづくりや、調達においてもリスクがあっても挑戦しようとする人を評価する制度を整える必要があると思います。

あと、サイバーセキュリティのトップガン育成に関してもお話が出ておりましたが、それを聞いて私は2014年11月に韓国のソウル女子大学を訪問した時のことを思い出しましたので、ご参考までに紹介

いたします。情報セキュリティ教育に力を入れている同大学では、これまでに女性のセキュリティ・コンサルタントを輩出しています。しかし、それだけでなく、ホワイトハッカー育成を目的として中学生・高校生を対象とした「情報保護英才教育院」を運営しています。韓国では、さまざま分野で大学が国や自治体と組んで英才教育のプログラムを運営しているのですが、これもその一環で、土曜日や夏休みを使って教育が行われ、費用は全額国が負担しています。情報保護英才教育院は全国に4か所あるそうで、同大学はそれを初めて設置したことで注目されました。国の支援だけでなく、ホワイトハッカーが勤務する情報セキュリティ会社も協力していますし、さらに、数学、情報セキュリティ、教育心理、人間教育の4つの学会も関わっていると聞きました。まさに産官学の連携に加え、異なる学問領域の連携で英才教育が行われているわけです。

最後に、先ほども申し上げましたが、テクノロジーとビジネスの未来を考える場合にも、情報技術に関連した人材育成を考える場合にも、人間や社会に関わる幅広い領域の専門知識を動員して、それらを結び付けていくことが重要な時代になったということを改めて強調しておきたいと思います。

以上です。

○村井委員長

ありがとうございます。岡村さん、どうぞ。

○岡村委員

先ほど、松本委員を初め複数の委員から法制度の問題が出ましたので、手短に申し上げておきます。

法制度とセキュリティを考えるときには、例えば個人情報保護法20条以下であるとか、今度の番号利用法にも入っておりますけれども、must doという意味で、セキュリティを図らなければいけませんという規定がある一方で、例えば労働基準法とか労働契約法を守らなければ、つまり一定の要件を守らなければモニタリングができないという意味で、セキュリティの対応策を講じる際に遵守しなければならない法令があるという側面があります。

その両方がどうも皆さんにわかりにくいような状態でこれまで来ていましたので、情報セキュリティ政策室で数年前に情報セキュリティの準則というのをつくりました。ところが、それから今申し上げた番号利用法を初め新たな法律ができたり、あるいは改正されたりしております。

どうも日本企業というのは、よくも悪くもコンプライアンスに注力するところがありますので、そうした準則づくりをいま一度リニューアルするということが企業のセキュリティ意識を高めるとともに、円滑な情報セキュリティの対策を講じるために必要であると考えます。

以上です。

○村井委員長

ありがとうございます。それでは、吉田さん、お願いします。

○吉田様（根本委員代理）

本日、代理で出席させていただいておりますが、幾つか発言させていただきます。

まず、論点3（4）（ユーザー側）企業のセキュリティ対策強化については、日本再興戦略2015にも記されているところでございますが、経団連としては、今年2月17日に「サイバーセキュリティ対策の強化に向けた提言」を公表し、その中で、サイバーセキュリティの確保は企業の信用の維持や事業の継続に関わる重要な課題であるとした上で、サイバーセキュリティを技術上の問題だけではなく経営上の重要課題として位置づけ経営層の意識改革を図ることや、経営層の強力なリーダーシップのもとCISO（Chief Information Security Officer:最高情報セキュリティ責任者）の設置など組織の改革や人材の育成などに努め業種間の分野横断的な情報の交流や意見交換なども進めることなどを産業界の取組みとして掲げております。

こうしたなか、論点3（1）に「◆企業規模等に応じて具体的にどの程度のレベルの対策を講じればよいか必ずしも明らかではない。」といった課題についても認識しているところでございます。同ページの右下に、自発的対策の促進、ガイドライン等による情報提供、人材育成支援（IPA）と、民間企業における現行のセキュリティ対策の概要を記していただいておりますが、こうしたセキュリティ対策の強化に向けた取組みを進めるにあたっては、引き続き業種・業態や事業規模等に応じて、経営判断の中で対策を講じることができる枠組みを維持していただきたいと考えております。

一方で、現在、企業でマイナンバー制度の実務導入への対策が進んでおりまして、経団連においても実務導入の円滑化に向け、実務担当者の方が集まり、具体的な実務をイメージしながら、どのような対策をとればよいかといった点について、政府の関係者の方と意見交換を行う会合などの機会を設けさせていただきながら、一つ一つ対策を講じているところでございます。マイナンバー制度については、厳格なルールがある中で、それらを遵守するためにどうすればよいかということと同時に、いかにヒューマンエラーを減らすかということも重視されているところでございます。こうしたなか、セキュリティ対策への意識についても高まりを見せておりますので、サイバーセキュリティ対策の議論が国で大きく取り上げられてきますと、民間企業の意識もさらに高まってくるであろうということを申しあげます。

次に論点1に関しまして、データの一層の利活用について、でございます。2ページ「情報経済小委員会中間取りまとめ（概要）」の方向性1として「制度を変える」ということを大きく掲げていただいておりますが、この点については、引き続き最も重視していただきたいと考えております。経済活動

のプレイヤーが自身の経営判断で、事業戦略の中で創意工夫をしながら新しいビジネスを展開することができる制度整備を推進していただきたいと考えております。

また、制度整備にあたっては、ITを用いて生産性を向上するという観点も重要視しております。例えば、現在、経済産業省や財務省において、電子帳簿保存法に関係するルールを緩和し、領収書等をスマートフォンで撮影した画像を用いて経費申請することを認めることで企業内に紙の原本を保存しなくてよいとするよう制度を変更することを検討されているという報道もございます。経団連も若干意見を出させていただいているところですが、これが実現しますと、従来、営業担当者が会社に戻り会社の建屋の中にあるスキャナ機器を用いて領収書等をスキャンしていたものが、例えば出張先のビジネスホテルの部屋からスマートフォンで撮影して会社の経理担当に申請することが可能となり、業務効率化や原本保管コストの削減が期待できます。

一方で、会社の管理外にある状況下でデータを作成することになるため、そのデータの信頼性や行為の信頼性をどのように確保するのかというのは非常に重要な課題であると認識しております。

ITを活用することで新たに出来るようになることを実際のアクションにつなげていくためには、ほかの関連する制度についても検討が必要な場合があり、「制度を変える」というテーマの中には、そうした観点も含まれていると考えているところでございます。引き続きIT、それからデータをさらに活用して社会が高度化していけるように、制度の見直しや事業者の自由度についても、セキュリティの強化とあわせてご勘案いただければと思います。

以上でございます。

○村井委員長

ありがとうございます。西川さん、お願いします。

○西川委員

私からは、論点1と2に関してコメントをさせていただければと思います。

ここではデータを活用するというところで、データの収集や分析を促進するという論点が書かれていると思うのですけれども、今、データを活用するという文脈だと、多くの企業は今あるデータをどう活用するかというところに焦点を当てていると思うのですが、それだけではなくて、データを活用して応用の機会をふやしていくためには、データの収集方法そのものから進化させていく必要があるということをコメントさせていただきたいと思います。

特に我々、今、自動運転・ADASの分野に取り組んでいるのですけれども、そこでは、要は今あるセンサーを活用するだけではなくて、どうすればより高度な制御ができるようになるのかというところをセンサー技術と密接に関わって取り組んでいるところでありまして、また、例えば産業用ロボットの

データ分析においても、要はセンサーをつけ過ぎるとコストが高くなってしまうので、今、センサーはそれぞれのロボットにそんなについているわけではないのです。ただ、今後、プレディクティブメンテナンスとかをもっと精度よくやっていくためには、センサーをどこに置けばいいのか、どういう情報をとればいいのかというところから設計し直さないと、今ある情報だけではなかなか難しい局面も出てくるのかなと。

それを実現するためには、単にデータ分析をするようなベンチャーとデバイスをもっている大企業が組むだけではだめで、もっとデータのとり方からともに議論していけるようなパートナーシップを築いていく必要があるのではないか。

そうではなくて、なかなかそこが融合できないような関係だと、うまい形で連携というのは組めないのではないかと思うので、そういう点も強味を生かすというところでは、論点に含めていただけると幸いでございます。

以上になります。

○村井委員長

ありがとうございます。喜連川さん、お願いいたします。

○喜連川委員

最近日経に記事を書かせていただきました。いままでご議論があったように、AI、即ち人工知能で職業がなくなるという話はあちこちであって、やや食傷気味ではないかという気がしまして、完璧に技術だけにフォーカスする時AIと呼ぶ分野で何が起こっているのかというのを書きましたが、結構いろいろな反応がありました。その中で非常にアグリーされたのは、今のAIが大きな変化感を与えているのは、完璧にビッグデータである。つまり、賢くみえる原因はデータであるということに対して、そのとおりですと皆さんおっしゃっていただきまして、逆にいうと、データがないと何もできない時代に入ったということです。

という時代に、今度、このデータはスカなデータでもいいのですかというとそうではなくて、やはりいいデータでないといけない。いいデータというのは、先ほど西川委員もおっしゃった通り、データをどうアクワイアするかということと、どう品質を担保するかという観点からすると、ただではなく、とても大きなレイバーを投入しなければいけないのです。先ほどビジネスモデルがみえないというようなことをおっしゃったのですけれども、まずはこの時代の変化に対する意識改革が根源的にかなり重要なのではないかという気がいたします。

先ほどCPSの話がJEITAの水嶋会長からも経産省からもありましたが、CPSというのは、ある意味で極めてデータ中心に王道で考える。つまり、従来の制御という世界から脱却し、データとしての

プログラムをどうフュージョンさせるかという意味で極めて王道で、逆に今後の方向としましてはここしかないのではないかと思っていますので、ぜひ頑張っていただければと思います。昔、私の師匠が第5世代をやられて、経産省は第5世代に対していろいろとご批判があるのかもしれないですけれども、ゆっくりと非常にいい成果が今出てきていると私は思うのです。それぐらい長い目でみていただくことも重要だと思います。

第2点は、ソリューションを上側にもってきたときに、引っ張ってこなければいけない技術がすごくふえているような気がするのです。単一のテクノロジーで出口につながるということもなくはないのですけれども、そうではなくて、いろいろな要素技術をプルするようなことが必要になってくる。

そのときに、これは毎回申し上げて申しわけないのですけれども、地味な大学の研究をぜひうまく活用していただきたいと思います。大学には結構とがったすごいものをもっている先生がおられるのですけれども、大学の入試でもそうなのですが、私は通る、通ったという学生は必ず落ちるのです。通っているかどうかわからないという控え目な学生が通るのです。研究者でも同じで、できる研究者になるほど控え目なのです。だから、世の中にあまり見えない。そういう人をうまく活用するような場をつくる、今後日本を強くするためにはマルチプレーヤーの連携が極めて必須ではないかと私は考えます。

最後にセキュリティについてです。最近、米国も新しい施策、NSCIというものを出しておられると思うのですけれども、大体ほとんどがクラシファイですから、セキュリティの議論はこういう平場で一体何を議論すればいいのかよくわからないのが実情です。私どものSINETは、来年度4月からいろいろな方々のご支援で、北見から沖縄まで全国を100ギガで結びます。多分これは日本の中で一番パワフルなネットワークになります。これは大きな大学は全て結んでいますし、大きな研究所もみんな結んでいますので、ありとあらゆるトラフィックは補足できます。そういう意味では、セキュリティの視点からみたときに大学の資産がどれだけあるかといわれると、必ずしもクリティカルではないという議論もありますが、産学連携の深い情報もあります。

こういうところでセキュリティをオペレーショナルにどう守るか。先ほどどこかでご議論があったかと思いますけれども、個々の企業でやることなどほとんど不可能だということと同じことが大学にも起こっていまして、小さな大学ではセキュリティの対策を丁寧にやれません。日本中でどうオペレートするかということ。日本中でどうやって人材を育成するかということもNIIでやろうとしていますので、ぜひいろいろご協力させていただければ大変ありがたいと思います。

以上でございます。

○村井委員長

ありがとうございます。

一通り全ての委員の方からお話を伺ったようでございます。委員長も発言する時間がありそうなので、皆さんのご意見を伺った上でのコメントを申し上げたいと思います。

まずは最初のデータの利活用なのですが、おっしゃるように、データがあるということが世の中のいろいろな変革を生むということですが、一方で、どなたもおっしゃっていたのは、データをそもそも使っていいのか否かという点です。

この点、何度か申し上げておりますが、まだガイドラインをつくる前の段階だと思います。イノベーティブでクリエイティブなデータを使って新しい産業が生まれてくる状況を考えたとすると、これは事後承諾というか、調整機構のようなものをつくっておくのがいいのではないか。つまり、ADRのような、事後調整の仕組みです。

何か起こることが決まっているときはガイドラインでかなり詰められるのだけれども、粗々のガイドラインプラス、そういった調整機構があれば、使い方と目的を透明にしてデータが使えます。そのような仕組みができないかというのを、私はこの場で何度か申し上げましたが、なかなかうまくいかないようです。

やはりここから生まれてくるものの新しさというのは、わからないことも沢山あって、そこに挑戦していきたいのだから、だとすると事前に決めることができません。したがって、おびえて使わないではなくて、ここまできちんと準備したのだから、とりあえず使って始めなさいということができないのかということです。インターネットではそういうことをやってきたのです。岡村先生にもお世話になりながらそういう仕組みをつくったと思いますので、そういうことはできないのかなと思いました。

つまり、クリエイティブなことが沢山起こるという期待があるということなのです。そうだとしたら、勇気をもって、リスクを多少とりながらビジネスが進められる環境を整備するということだと思いますので、今のは例ですが、そういう環境があるのが重要だろうということが1点です。

それから、セキュリティ関係について。義務づけなければだめだと三輪委員もおっしゃったし、松本委員のご発言もある意味そういうことに関係があると思うのですけれども、日本の企業がセキュリティに対してある義務づけをするというのは、政府調達などはある程度縛りがかけられるのかなと思いますが、CSIRTをつくるというのは、ぜひ進めたほうがいいと思います。

○岡村委員

今、法制度が余りに横に広がり過ぎていて、もう全体像がみえないような状態なのです。まず、ずらっと並べてみて、粗々でどんな状態なのかをみた上で、制度的に足りないもの、あるいは行き過ぎなものをうまく最適化していく必要がある。そのためにも、その前提として、まずは今どうなっているの

ですかと全体像をわからなければいけないというのが1つ。

それと、セキュリティを講じる際に、例えば派遣の人間から誓約書をとっていいかどうかという些末な論点で時間をとられているのです。そういう無駄時間といっては失礼ですけれども、そういうことはないようにしたいという趣旨です。

○村井委員長

CSIRTを義務づけるというのはできないのですか。

○岡村委員

何を義務づけるのですか。

○村井委員長

要するに、セキュリティ・レスポンス・チームというものを各企業の中でつくるということです。それを連携しましょうと。CSIRT（Computer Security Incident Response Team）を各企業の中につくってください、あるいは政府の組織にもつくってください、つくったものをネットワーク化するという仕組みはCSIRT協議会などでできているわけでしょう。

○岡村委員

これまでのスタイルでいけば、個人情報保護法であるとか番号利用法で非常に粗々の、安全管理措置を図りなさいという義務を抽象的にかけておいて、ガイドラインの中で具体的にこういうことが必要ですよ、あるいはこういうことが望ましいですよという形で書くということはありました。

○村井委員長

要するに義務づけというのを政策としてどういう形で進められるのかということだと思うのです。なかなか難しいところもあるけれども、できることもあるはずです。インシデントのレポートを各組織できちんと把握しておいて、それが全体的に収集できる、あるいはJPCERTで一箇所に集約できるとか。そうだとすると、集約点が経済産業省の守備範囲なので、そういった意味でのオペレーションとして、あるいは施策として何かできるのではないかというのが1点。

もう一点は、トップガンというお話が出ていて、やはりセキュリティの研究はこわいところがあって、研究としてオーソライズしてくれるとか、そういう仕組みで何かできるといいと思うのだけれども、それは差し障りがあるから置いておきます。

発見報奨金というのは、海外ではかなりいろいろなところでやっているようだけれども、なぜ日本ではできないのですか。これは三輪委員。

○三輪委員

やっているところはやっています。

○村井委員長

なるほど。これは、例えば国などがやってはいけないのですか。

○三輪委員

日本で進まない理由は、例えばサイボウズさんなどがうまく回っているのは、脆弱性をみつけてくれてありがとうというのを素直にいえる珍しい日本人なのです。日本のほかの企業はそんなことできなくて、脆弱性がみつからないほうがいいねとみんな思っているし、それがみつかると欠陥ととられてしまう。

例えばそれが家庭に配っているルーターだったりすると、下手すると製品の回収問題であったりとか、欠陥だと国民が騒ぐとか、そういったマイナス面のイメージが強いので、できればこっそりみつけて誰にもいわないで報告してほしいと思っていたりとか、そこの恥の文化とそれを攻める文化があるからではないかと思います。

○村井委員長

そうすると、経済産業省のホームページの脆弱性を発見したら報奨金を出すということを経済産業省がやるということはできないのですか。

○三輪委員

いいと思います。例えば、恥という部分については、発見者もお互い公開しない。その上でちゃんと報奨金だけは出るというのでも日本的にはいいと思うのです。

○村井委員長

つまり、トップガン養成みたいなことにはプラスになるのではないかと思うのです。

○三輪委員

すごくなります。

○村井委員長

仕組みとして、できる人が勇気をもってやるというのは、今の三輪委員のお話ですと有効なのではないかと思われます。

私の研究室にいるセキュリティの学生は、そういう貢献をしようと思って一生懸命頑張って、攻撃できるかとか、穴がないかとか、人のところを調べたりしているのだけれども、一歩間違えると攻撃者と間違えられるというところなので、リスクと背中合わせなのですが、研究だとか報奨金だとか、何かそういう仕組みをつくって、やれることはあるのではないかという気がいたしました。

時間はまだ少しあるようですので、もし何か言い残したことがあればお願いします。喜連川先生、どうぞ。

○喜連川委員

最初に委員長がおっしゃったことは、村井先生だけではなくて私もあちこちで何遍もいっているのですが、うまく動かないです。1つのロールモデルはODIなような気がします。

この間、英国大使館が非常に丁寧に物事を進められて、随分お越しになられるのですけれども、英国にも来てくださいとかといわれて行きますと、やはりODIやデジタルキャピタルトなど頑張っておられます。会場では、最初に必ずリーガルが出てこられます。すごく上等なスーツとすごく上等なネクタイをつけられたリーガルが必ず一番に出てこられる。

結局、データの利活用というものを考えたときに、どこまで活用していいのか、どこまで他人のデータを利用していいのかという権利関係から何から全然わからないので、そこをODIがコーディネートすると同時に、小さなエンジェルマネーみたいなものを用意するという構造を彼らはうまく使っているのではないかと思います。そんな極端に大きなお金は入れていないです。

原則、現在のITを少し萎縮させる、一歩踏み出せない日本の今の姿というのは、どこまでやっていいという何かのし紙をもらわないと一歩進めないという構図は、まさに村井先生がおっしゃるとおり私もずっとそう思っていまして、そういう組織をおつくりいただけると、相当カンフル剤として有効ではないか。ぜひそれは頑張っていただきたいと思います。

○村井委員長

ありがとうございます。そのほか、いかがでしょうか。

○岡村委員

ODR、ADR関係で一言申し上げます。

既に電子商取引の準則関係では、消費者保護との関係でADRの制度を経産省の委託事業で動かしておられますので、そういうフレームワークは既に前例があるということ。

それから、喜連川先生がおっしゃったODRについては、ドメイン名紛争で既に世界知的所有権機関、あるいは日本の弁理士会連合会の連合でつくった組織などがODRで動いておりまして、うまく機能していると聞いておりますので、それはそれで非常に達見ではなかろうかと存じます。

○横塚委員

この議論は公開と書いてありますけれども、セキュリティ対策をこれから詰めていくに当たって、本当に公開していいのかもう一度ご検討いただいたほうがいいのではないかと思うのです。

○佐野課長

今後の審議いかんによっては、そこのルールについても柔軟に対応してまいりたいと思います。

○村井委員長

それでは、よろしいでしょうか。冒頭申し上げましたように、きょうは自由討論ということで、特に落としどころは考えずに議論していただいたと思います。どうもありがとうございます。

お気づきになったことは後でまた事務局にフィードバックしていただけると、今の会議の扱い等も含めまして、今後の参考にさせていただいて進めていきたいと思います。

本日の議論はここまでとさせていただきたいと思います。それでは、熱心なご議論、どうもありがとうございました。会議は以上でございます。

――了――