産業構造審議会　商務流通情報分科会
第6回　情報経済小委員会　議事録

○佐野課長

定刻でございますので、ただいまから、産業構造審議会商務流通情報分科会第６回情報経済小委員会を開催したいと思います。

本日は、ご多忙な中お集まりいただきまして、まことにありがとうございます。

まず、議事に先立ちまして資料の確認をさせていただきます。

本日もｉＰａｄを使用しましてペーパーレスで審議を進めてまいります。ご協力よろしくお願いいたします。

本日の配付資料でございますけれども、座席表、議事次第、配付資料一覧のほか、資料１としまして情報経済小委員会の委員名簿、資料２としましてＩｏＴ社会に向けたデータ利活用施策及びサイバーセキュリティ戦略を受けた今後の対応、それから、参考資料が２つございまして、セキュリティ人材の確保に関する研究会中間報告、データに関する取引の推進を目的とした契約ガイドライン、以上でございます。

ｉＰａｄの不具合や、資料が掲載されていないなど、何か問題がございましたら、事務局までお声がけをお願いいたします。

本日は15名の委員にご出席いただいており、過半数11名に達しております。有野委員、喜連川委員、國井委員、國領委員、夏野委員、西川委員におきましては、ご都合によりご欠席となっております。

なお、本日は、総務省の情報通信政策課の小笠原課長にご同席をいただいております。どうぞよろしくお願いいたします。

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

おはようございます。それでは、進めさせていただきたいと思います。本日は、お忙しいところお集まりいただきまして、ありがとうございます。

本日の議題は、ＩｏＴ社会に向けたデータ利活用の施策及びサイバーセキュリティ戦略を受けた今後の対応が１つ目、２つ目がセキュリティ人材の確保に関する研究会の報告、そして、その他となっております。自由討議の時間は60分ほどとられているようでございます。それでは、進めていきたいと思いますので、よろしくお願いします。

○佐野課長

資料２をごらんください。１枚めくっていただいて、２ページ目をお開きいただければと思います。

前回、ＩｏＴ社会に向けて利活用とセキュリティの２点について、さまざまなご議論をいただいたところでございます。本日は、引き続きデータ利活用環境整備、そのうちＩｏＴ、ビッグデータ、ＡＩに関するビジョンの策定と戦略的取り組みについて、それからパーソナルデータのさらなる活用に向けた取り組みについて、ご議論いただければと思っております。

さらに、セキュリティ強化ということで大きく５点ございます。ＩＰＡの業務の監査の関連、ソフトウエアの脆弱性の関連、重要インフラのセキュリティ対策の関連、国際連携の関連、最後にサイバーセキュリティの専門人材の国家資格制度の創設について有賀委員から中間報告をいただきます。

３ページ目をごらんください。まず１点目としまして、ＩｏＴ、ビッグデータ、ＡＩに関するビジョンの策定と戦略的取り組みについてです。

下の図をみていただきますと、さまざまな分野で革新的な産業モデルを創出していく必要があるということで、例えば自動走行技術を活用した新たなサービスの創出として自動タクシーとか自動物流等がございます。こうした産業モデルを創出していくために具体的な取り組みをさまざまな分野で動かしていかなければならないということで、官民で規制改革と新たな規格形成を目指して、分野ごとに実証的な取り組みを推進してまいります。また、ベンチャーなどのＩｏＴを活用した先駆的なチャレンジを支援してまいります。この両面をあわせて進めていくことが重要であると考えているところでございます。

このための民間主導の枠組みとしまして、ＩｏＴ推進コンソーシアム（仮称）というものを検討しているところでございます。これは関係省庁連携をし、総務省とも一体的に取り組んでまいりたいということで、今具体的に検討、調整をしているところでございます。

これら具体的な取り組みを支える中長期的な羅針盤としまして、ＩｏＴ、ビッグデータ、人工知能の進展を踏まえた2030年の新産業構造ビジョンの策定を開始したところでございます。これは産業構造審議会の新産業構造部会で議論を開始したところでございます。

次の４ページ目をごらんください。ＩｏＴ推進に向けた実証を支えるものとして、経産省としては来年度の概算要求で技術開発と実証を合わせて 138.6億を要求させていただいているところでございます。そのうち、各分野に関する実証事業を書いておりますが、実証事業で約60億の概算要求をさせていただいているところでございます。具体的な分野としましては、製造プロセス、モビリティ、医療・健康、流通、インフラ、行政等のさまざまな実証事業につきまして予算要求をしているということでございます。

次に５ページ目をお開きいただければと思います。2030年に向けた新産業構造ビジョンの検討を開

始いたしましたが、９月17日に第１回を開催しております。検討事項としましては、ＩｏＴ、ビッグデータ、人工知能等がもたらす産業構造、就業構造、経済社会システム全体の変革がどうなるのか、そのインパクトがどうなるのか、海外のプレイヤー等がどう動いていくのか。それから具体的な処方箋として政府、民間企業、個々人はどういう対応を進めていくのかということにつきまして、あるべき姿、ビジョンをまとめていこうということで検討を開始したところでございます。

次は６ページをごらんください。パーソナルデータのさらなる活用に向けた取り組みでございます。先般、個人情報保護法が改正されまして、個人情報の利活用のための基盤が整備されたところでございます。今後具体的な制度設計を進めていく必要がございます。さらに、この個人情報を含めましたデータの利活用のためには、データを提供する個人と、情報を取得する事業者との信頼関係を構築しながら事業者の実質的な取り組みを進めていく必要があると思っております。また、個人の権利を実質的に侵害する可能性が低いと考えられる場合で匿名化などが現実的に難しいと考えられるケースについても今後対応、検討していくことが必要であると考えているところでございます。

個人情報保護法上、これまで必ずしも規程が明確でなかったために企業の活動が萎縮していた部分がございまして、個人情報の範囲が明確でないとか、匿名化の程度が明確でないとかというような課題がございました。この課題に対して、今回の個人情報保護法の改正によって、対応済みになりました。しかし今後は、具体的な運用を明確にしていく必要がございます。

それから、事業者の自主的な対応を促進していくべきという課題について、事業者と消費者との信頼関係をどのように構築をし、また、分野による特殊事情にどう対応していくかという課題がございますが、これにつきましては、昨年10月にオンライン上で同意を取得する場合のガイドラインを経産省で策定したところでございます。こういった取り組みを進めていくということと、分野に応じてさまざま自主的なルールを形成していくことが重要であろうと考えております。

①の課題の２つ目でありますけれども、プライバシーデータに限りませんが、データ流通の契約慣行がまだ十分でない中で、どのようにデータ流通を促進していくかという課題について、データ取引の促進のためのガイドライン策定を検討しております。今回、そのガイドラインを参考資料２として掲載させていただきました。

それから、下の③、さらなる個人情報の利活用のために検討すべき課題について、個人の権利を実質的に侵害する可能性は低いと考えられるものの、同意取得や匿名化が現実的に難しいと考えられるケースがございます。この課題をどう整理していくのかということについて検討が必要であると考えております。

７ページをお開きいただきますと、さらなるデータ利活用を検討すべきケースという具体例を書かせていただいておりますが、不特定多数の人に同意をとることが現実的ではない場合についてです。例えば、

駐車場内で自動駐車を制御する人工知能エンジンの開発を行うようなケースの場合に、さまざまな駐車場に設置されている防犯カメラのデータを大量に読み込んで、駐車場の枠線やロープを識別するという高度解析システムの開発が行われているところでございます。この場合、防犯カメラに人の顔が映っている等、個人情報ということでどうしても萎縮してしまうところをどうするのかという課題がございます。

下の②でありますけれども、最終的には匿名加工処理をされるわけでありますが、分析段階では個人情報であるほうが精度が高い場合について、例えば、別々の機関が保有している事故車の損傷データと事故車のドライバーの負傷状況を掛け合わせることで車の損傷状況を把握して、ドライバーの損傷程度を自動的に検証して救急手段を選択するような、緊急サービスの改善に用いられるケース等にどう対応していくのかということでございます。

８ページは、先ほど申し上げた事業者と消費者との信頼関係構築のための取り組みということで、昨年10月にオンラインサービスにおける通知と同意・選択のためのガイドラインを策定して、今、国際標準化を進めているところでございます。

各分野の自主ルールの策定を進めていく必要があるということで、ＨＥＭＳのデータ活用のプライバシーマニュアルを今策定中でございます。

次の９ページをごらんください。先ほど申し上げた、データを事業者間で取引する場合の契約ガイドラインというのを策定しておりまして、各事業者の方々、それから法務関係者に意見をお聞きした上で、データに関する取引を行う場合の契約の検討項目としてどういった項目に留意すべきか、という参考資料として整理いたしました。

10ページに現行の個人情報保護法の概要、11ページに本年９月に成立しました改正個人情報保護法の概要をつけております。大きなポイントは、１つ目に個人情報の定義の明確化、２つ目に匿名加工情報という新しい枠組みが整備されたという２点でございます。それから、個人情報保護委員会に現行の主務大臣の権限が一元化されるというところでございます。

12ページをごらんください。セキュリティの関連でございます。９月４日にサイバーセキュリティ戦略が閣議決定されましたが、それを踏まえた取り組みを整理いたしました。政府機関を守る取り組みについて、１点目に、国による監視、監査、調査の対象を独立行政法人と一部の特殊法人等に拡大していきます。２つ目といたしまして、左真ん中の箱でございますけれども、重要インフラを守る取り組みということで、情報共有体制の強化、サイバーレスキュー隊の派遣、ガイドラインとして制御系の対策に関するガイドラインの策定ということが盛り込まれているところでございます。

右側の企業を守る取り組みでございますけれども、経営ガイドラインの策定は、この委員会でもこれまでご議論いただいたところでございます。それから、ＩｏＴシステムのセキュリティに関する制度整備・技術

開発、普及啓発活動の実施について、これらを支える基盤整備のための取り組みということで人材の育成が課題とされているところでございました。若年層の優秀なセキュリティ人材の早期発掘イベントの拡充、突出した能力をもつ若年層の人材を発掘・育成。情報処理技術者試験を活用しまして実践的な能力を適時適切に評価できる資格制度の創設。ソフトウエアの脆弱性に関して、開発者の同意がない場合も必要に応じ公表。政府系ファンドを活用してセキュリティ企業の競争力強化を図る。幅広い分野で国際協力体制を確立しましてサイバー空間の安全を確保していく。こういうさまざまな取り組みが盛り込まれたところでございまして、きょうは特に、このうちの制度と書かれている部分についてご議論いただければと考えてございます。

次に13ページをごらんください。サイバーセキュリティ対策強化に係るＩＰＡの業務でございます。下の表をみていただきますと、①セキュリティ対策の基準・ガイドラインをつくる、それから、②対策の実施を確認（監査）、③不正アクセスをみつける（監視）、④事故対応・原因究明（調査）、⑤情報収集・分析・発信・知見の提供・人材育成と大きく５つございますけれども、サイバーセキュリティ本部（ＮＩＳＣ）の業務としましては、この５つにつきまして国の行政機関についてこれまでやってきておりましたが、この②から④のところについて対策強化が必要であるとされたところでございます。一方、ＩＰＡは民間企業の①、④、⑤のところを実証してきたところでございますが、真ん中の独法等に関するＮＩＳＣの対策強化に当たりましてＩＰＡの知見を活用しようということでございます。

14ページをごらんください。ソフトウエア製品の危険性に関する情報の公表というところでございます。現在、ＩＰＡを窓口としましてソフトウエア製品の脆弱性について情報を収集して、開発者と調整した上で公表しましてユーザへの注意喚起を行っているところでございます。一方で、開発者との調整で同意が得られないケースや、必ずしも脆弱性には当てはまらない危険性情報の取り扱いについては、定められていないということでございまして、こうしたソフトウエア製品における脆弱性等の危険性情報に関しまして公表手続などの取り扱いを明確化していくことが必要であると考えております。

15ページをごらんください。重要インフラのセキュリティ対策についてです。重要インフラにつきましては、ＮＩＳＣが策定いたしました第３次行動計画に基づきまして取り組みを推進しているところでございます。経済産業省の取り組みとして、標的型攻撃の情報共有、制御機器の認証、研究開発などの対策を複合的に推進しているところでございます。これにつきまして、さらなるサイバー情報共有イニシアティブの体制強化が必要ではないかということで、ＩＰＡが重要インフラ等につきまして情報共有の構築をし、各社と秘密保持契約を結んで情報収集、解析、共有等を実施しているところでありますが、こうした体制強化をどのように図っていくかの検討が必要であります。

16ページをごらんください。国際連携の取り組みでございます。政府、民間機関等のさまざまなレベル

での国際連携を推進していくということについて、政府機関間の連携、民間専門機関間の連携、大きく２つございますけれども、政府機関間の連携としましては、ＮＩＳＣ等によります日米サイバー対話ですとか、日ＡＳＥＡＮの情報セキュリティ対策会議等、政府間の連携を行っているところでございます。民間の専門機関間の連携としましては、ＪＰＣＥＲＴが日本の窓口となりまして世界 100ヵ国の窓口と連携をし、サイバー攻撃に対して共同対処を実施しているということでございます。また、ＡＳＥＡＮを中心としまして現地の指導とか、ＯＪＴによりますＣＳＩＲＴの構築も支援してございまして、こういった国際連携を推進していく必要があるということでございます。

次の17ページでございますけれども、有賀委員のほうから、先日行いましたセキュリティ人材の確保に関する研究会の報告をいただければと思っております。

以上でございます。

○村井委員長

ありがとうございました。

それでは、引き続きまして、先日のセキュリティ人材の確保に関する研究会の報告を有賀委員からお願いいたします。

○有賀委員

では、御報告いたします。まず、お手元の参考資料１、セキュリティ人材の確保に関する研究会の中間報告をまとめて掲示してございますので、ご参考にしていただければ幸いです。資料２の17ページ、情報セキュリティ人材の育成確保について（中間報告）をごらんください。

８月から９月にかけまして、極めて短期間でございましたけれども、委員の方はかなりインテンシブにやっていただきまして中間報告をまとめました。概略は、一番上の箱にありますように、まず、実践的な能力を適時適切に評価できる試験制度の充実を図るという、改訂2015年の日本再興戦略に盛られました良質な情報セキュリティ人材を供給するということでいろいろ討議をいたしました。結論として、情報セキュリティスペシャリスト試験をベースにした登録制度の創設を目指す方向がよいのではないかということになりました。登録制度では、更新制度や登録簿の公開等によりまして、実践的な能力など質を担保するとともに、実務経験者や過去の試験合格者などへの門戸拡大によりまして量も確保していくという、質、量両方を確保しようということで計画を練っております。

それから、これは後ほど説明いたしますが、主にユーザ企業を対象に、現在、ＩＰＡで情報セキュリティマネジメント試験を新たに導入するということで、その準備が進んでいるということでございます。より詳細

には、左側下の枠をごらんいただきたいのですが、研究会の検討の中で、今後必要となる情報セキュリティ人材像というのを、この下の３つのポツにあるような形で分類いたしまして、それを明確にした上で、その育成確保の方策を策定しております。

まず、１つは、ホワイトハッカーのような高度なセキュリティ技術者。これは、人材の発掘、育成に関する取り組みを継続、改善していくということで、やっていくしかないということでございます。

２番目には、ユーザ企業の事業部門や情報システム部門において、自社の情報セキュリティ技術者と連携して情報セキュリティの確保を管理する人材。これに関しましては、かなり喫緊のニーズがございまして、かつ人数の確保も必要だということで、新たに情報処理技術者試験制度の中に情報セキュリティマネジメント試験というものが導入されるということで準備をしております。現在聞いておりますところは、できるだけ早く、来期の早々にも実施されるということで準備をされるということであります。

３つ目の分類といたしまして、ユーザ企業やベンダ企業の情報システムを設計、開発、運用する担当者として必要な情報セキュリティに関する高度な知識、技能を身につけた人材。これに関しましての確保と育成でございますが、これが今回の研究会の中間報告の骨子でございます、情報セキュリティスペシャリストの登録制度ということでまとめております。

登録制度の概要につきましては、私も長年試験を作成したり、まとめたりしておりますけれども、試験制度45年の間で登録制度でございますとか、それを更新制度で統括するのは多分初めての経験でございます。まずは、主な登録制度の対象者としては、情報セキュリティスペシャリスト試験の合格者を中心に取り上げたいと考えております。過去、試験を何回かやっておりますけれども、現在、情報セキュリティスペシャリスト試験合格者だけで申し上げますと３万数千人、その前身でございます情報セキュリティアドミニストレータですとかテクニカルスペシャリスト（情報セキュリティ）ということで合格されている方を合計いたしますと、全部で６万数千人おります。

これに対する登録制度をつくり、かつ、更新制度として最新の専門的な知識・技能の習得でありますとか資質の維持・向上を図る。それから、規模的には2020年度ぐらいを目安に３万人超の規模ぐらいで登録・更新制度を回していきたい。それから、３年ごとに更新をする。それから、当然のことでございますが、登録者の活用に関する施策を実施するということでございます。更新の主な要件といたしましては、情報セキュリティスペシャリスト試験の一部――多分、午後の試験ぐらいになると思いますが――を再受験していただいて合格していただく、もしくは、最新の知識や技能に関する講習の受講の実績を積んでいただくというようなことで更新を図っていくことになると思います。

それから、登録制度でございますので、登録簿の公開を図りたいと考えておりまして、できますれば業務経歴等による検索機能等も含めた登録簿を公開し、情報セキュリティ人材の利活用が促進される、

もしくは確保が図れるということに貢献するような仕掛けにしたいと考えております。

登録者に関しましては、当然、コミュニティをつくることをやっていただき、最新のインシデント情報の提供でありますとか、コミュニティ参加者同士の切磋琢磨、教育訓練ということで資質の維持・向上を図っていただくというようなことを考えております。

このようなことが参考資料１にまとめられております。この会議で一応、基本的にご了解いただいた上で、具体的に仕組みをつくる、運用方針などを詰めるということで早期の実現を目指したいと思っておりますので、改めてそのためのワーキンググループ等をつくりまして推進していきたいと考えている次第でございます。

私のご説明は以上でございます。

○村井委員長

ありがとうございました。

それでは、今、２つのご説明をいただいたわけですけれども、ここから先は自由討議で進めていきたいと思いますので、ご自由な発言をお願いいたします。発言がある方はネームプレートを立てて教えていただければと思います。よろしくお願いします。それでは、岡村さん、お願いします。

○岡村委員

まず、資料２の６ページ以降の個人情報保護法の話でございますが、今般の改正の特徴というのは、政令あるいは規則などに委任されている事項が大変多うございます。施行自体は将来に委ねられている部分が個人情報保護委員会の部分を除けば多いわけですけれども、大体、産業界というのは、ご存じのとおり、法律が改正されれば施行を待たずして先取りして運用しようとする傾向がございます。また、実際に非常にコンプラ意識が日本企業は強うございます。つきましては、政令、規則などについて迅速に進めていただくことによって、できるだけ産業界がストップしないようにご対応をお願いしたいということであります。

さらに、その具体的なものとして、識別符号という概念が個人情報の明確化の中にございますけれども、例えば、今後自動車の車載システムなどによるいろいろなサービスの拡張というのは日本の産業の１つになろうかと存じます。余りにも識別符号が広く定められると、せっかく規制緩和が目的であるにもかかわらず使い勝手が非常に悪くなりますので、ひとつ、識別符号の範囲を定めるに当たっても必要最小限のものということで、規制が過剰にならないようにお願いしたいと思います。

次に、セキュリティに関する問題が12ページ以降に書いてございますけれども、例えば先ほどの車載シ

ステムを前提にしますと、電波が飛んでくるとか、元のデータが間違っていたとか、電波が遮られる、あるいは車載システムなどのメンテが悪かった、いわゆるバグ等々がありますので、法的な責任分岐点をどうするかということが制度的には非常に重要になってこようかと思います。この範囲はどこが責任をもつ、こちらの範囲はどちらが責任をもつということを明確化していただきたいということであります。

それとともに、その中でもＩｏＴということになりますと制御系が大変重要になります。私が外部理事を務めておりますＪＰＣＥＲＴでも制御系に関するセキュリティを非常に推進しているところでございますので、なお一層、この点についてご注意をいただいて政策を促進するようにしていただきたいと存じます。

ソフトウエア製品の脆弱性情報などの公表に関しても非常に困っているところでございますが、実際には最後通告をすると何とか公表してくれるというようなことで、現場では大変苦労しているというように聞いているところでございます。

それから、16ページの国際的な関係の問題でありますけれども、これは、途上国のセキュリティ水準を上げるお手伝いをするということが、当該途上国が踏み台になるなどしてループホールになる可能性がありますので、それを避けるためには非常に重要なことであり、ひいては、我が国の国益にも資することだと思われますので、この対策についても、なお一層力を入れていただければと存じます。

最後に、セキュリティ人材に関して申し上げます。第１に、国際的な他の試験との整合性などをどう図っていくかということで、我が国の国民が海外的に通用しやすいような状態をおつくりいただくということも検討していただく必要があるのではないかと存じます。それから、登録制度を公開するという形になりますと、登録者のセキュリティが、特にトップガンといわれる方々の場合には、いつどういうことになるのか非常に不安であるというような声も伝わってきておりますので、公開方法を検討いただくというような形でお願いしたいと思います。でないと登録を控えられるような状態に萎縮してしまうということになると困るからでございます。

一例を挙げますと、我々弁護士の制度の場合には、本人の申告によって自宅は隠す、公開しないというような措置をとることで、いわゆる身の危険を守るというような制度が確立しておりますので、そうした公開方法をさらにご検討いただければと思います。長くなりましたが、以上です。

○村井委員長

ありがとうございます。横塚さん、お願いいたします。

○横塚委員

横塚でございます。セキュリティに関して２点コメントしたいと思います。まず１つ目は、この中間報告

のペーパーにあるホワイトハッカーのような高度情報セキュリティ技術者、トップガンですけれども、なかなかここに書けないのかもしれませんが、継続的に取り組みをするということしか書いていないのです。いろいろな形で外国からアタックされた時に、本当に守り切れるのかというのが日本国家の重要な問題かと存じます。日本には、そういったエンジニアが３人しかいないとか１人もいないとか、いろいろ噂話が流れておりますけれども、相当大勢のハイレベルなトップガンをどうつくっていくか、これは非常に緊急の課題だと思いますので、しっかりやっていただきたいというのが１つでございます。

２つ目でございますが、この間、習近平とオバマとの会談でサイバー攻撃の話が出ていましたけれども、狙われた瞬間になかなか守っていけないというのがアメリカの企業でも相当あったということでございますが、日本の重要インフラはしっかりＩＰＡ等々で守っていただくとしても、一般的な企業、あるいは中小企業、自治体、そういったところが狙われたときに、個人情報だけでなく商品、あるいは製品に関するいろいろな機密の情報が盗まれるということが行われているようで大変不安であります。そういった中小企業、自治体等々の情報漏えいをどう防いでいくかということにつきましては、セキュリティ人材を育成していくこともベースとしては重要ですけれども、急ぎどのような対応をしていくのかという観点に立ちますと、例えば日本ナショナルクラウドみたいな頑丈なクラウドサービスをつくって、その中に中小企業なり自治体なりのシステムを入れていくとか、直接的に外部から守るということをもう少し積極的に考えるべきではないかと感じております。

以上でございます。

○村井委員長

ありがとうございます。それでは、根本さん、お願いします。

○根本委員

データ利活用とサイバーセキュリティについてそれぞれ２点ずつ申し上げたいと思います。

まず、データの民間での利活用の話で岡村先生から幾つかご指摘がございましたものに加えまして、個人情報保護法の中での行政と民間の取り扱いの違いについて再度指摘させていただきたいと思います。

総務大臣に一元化されたという形にはなっておりますが、主務大臣への委任可能という制度体系でございまして、この部分は相変わらず心配が非常に強くございます。運営のほうの話になりますが、ぜひご配慮をお願いできればと思っております。

それから、７ページの②「最終的には匿名加工するが、分析段階では個人情報である方が精度が

高い場合」に示された例は極めて重要でございます。こういった具体例を取り扱いますときに、やはり行政サイドにおけるデータの取り扱い規則と民間サイドにおけるデータの取り扱い規則が異なっているという現状は非常に大きな障害になりますので、ぜひ解消に向けた作業をお願いしたいと思っております。

セキュリティ人材育成の仕組みづくりのところで、試験や講習などに関してさまざまなお話がございました。まさかとは思いますが、１ヵ所に集めて全部行うなどという仕組みにはならないことを祈っております。オンラインで全部済むように願うばかりでございます。

セキュリティ関係についての２点目でございますけれども、横塚様から、守り切れる堅牢なシステムというお話がございました。ただ、幾ら堅牢なシステムをつくりましても必ず中に入られてしまいますので、入られたときの対処をどうするかも重要でございます。入られたときに強いシステムについても、ぜひご検討お願いできればと思っております。

以上でございます。

○村井委員長

ありがとうございます。松本先生、お願いします。

○松本委員

松本です。まず、パーソナルデータの活用に向けた取り組みというところで、個人情報について匿名化の方法を明らかにして、こういうものを適用すればよい、このようにできますというようなことが整備されてきたのは非常に好ましいと思うのですけれども、資料の８ページを見ますと、右側のところで、匿名加工情報に係る作成方法等につき、消費者の意見を代表する者、その他の関係者の意見を聞いて個人情報保護指針が作成されるよう努めるべきと定められたということなのですが、そのときに技術的に、こういう体系があって、これを使えばよろしいとか、これではだめだとかという、メニュー化されている状況を整備しないといけないのではないかと思うので、そちらもしっかりとやるべきではないかと考えます。

関連いたしまして、匿名化ではないのですけれども、パーソナルデータ、あるいは個人情報等を暗号化して蓄えておくということにつき、暗号化しても個人情報のままであるというようなところがあり、諸外国では暗号化すればレベルが違ったものだと考えられ、それでもよいということになるケースもあるわけですが、我が国ではまだそこが整備されていないと聞いております。ぜひ暗号化の効果もしっかりと把握し、暗号化を制度的に位置付けて使えば、パーソナルデータの活用がさらに発展させられるかと思われますので、その辺の整備が必要かと思います。

それから、サイバーセキュリティ対策強化でＩＰＡの業務というところ、13ページあたりにありますけれど

も、前回も私は申し上げたのですが、ＩＰＡに優秀な人材が集まるようにうまくすべきではないかと。今、外堀りを埋めているといいますか、このようにしてＩＰＡが頼りになる存在であるということにすると、ＩＰＡ自体をどのように変えていかなければいけないかという話につながるだろうというシナリオなのかもしれないのですけれども、現状はＩＰＡ職員は研究活動は原則できないわけでありまして、自由な発想で、世の中にアピールしていけるような個人の能力を高められる自由な研究活動を一部認める、しかし、定められた業務はしっかりとやらなければならないというような形にしていきますと、さらによい人が継続的にＩＰＡにぜひ行って活躍したいというようにできるのではないかと考えます。

あと、一言。サイバーセキュリティ人材を確保するということで、ご検討ありがとうございます。非常によろしいかと思うのですけれども、皆様がお使いの言葉で「トップガン」という言葉があるのですが、ちょっと誤解があるようで、対外的には恥ずかしいので、もうそろそろ使うのをやめたほうがいいのではないかと。「トップガン」というのは養成所の名前でありまして、人、個人を指していません。嫌われ役で申し上げました。

以上です。

○村井委員長

ありがとうございます。人材の件は松本先生にお聞きしたいことがあるのですけれども、もし後で時間があればお話ししますので、よろしくお願いいたします。石黒さん、お願いいたします。

○石黒委員

3点ございます。

まず、民間企業は、成長のために機会とリスクのバランスをとりながら経営するものなのですが、私の感覚として、日本企業の場合はグレーのものがあるとそこはなかなか踏み出さないという文化的なものというか、特に大企業はなかなかリスクをとれないということで成長の機会を逸しているというのが、今の、特にインターネットビジネスにおける日米格差につながっていると思います。

ここで１つこの場をお借りしてお願いしたいのですが、そもそも政府方針としてアメリカ政府が新しいビジネスのリスクに対してどんな方針をとっているかということを１度検証していただきたいと思います。

私もこれまでこういった委員会で７、８年同じような発言をしてきていますが、アメリカ政府の方針というのは、新しいものが出てきたときに、当初は規制をせず、産業界がどんどん成長できるよう、ある意味野放しにしているように見えます。具体的な例ですとGoogleが書籍をコピーしはじめても、政府としての介入は最小限にとどめているとか、各州で課税する売上税がｅコマースを課税するかについても、私からみるとビジネスが大きくなるまで敢えて放置していたように思えるのです。Uber、AirBnB、無人走行なども

同様で、新しいビジネスやシステムも非常に緩い形で進めさせておいているように見えます。

一方で、ハッカー対策とかセキュリティ対策などにおいては、日本の比ではないほど厳しくしている部分もあり、私の知る限りではシリコンバレーにコンピュータサイエンスの中でも天才級の人が集まっている企業がありまして、そことＮＡＳＡが組んで、大きな、非常にシリアスな問題を企業と政府が一緒に解決しているというようなところがあります。

私の狭い知識、経験の中での話になるのですが、米国政府は非常に両極端な方針をとっているように思えます。一方は成長を加速させながら他方では引き締めるという方針に見えます。しかしながら、これはあくまでも私個人の経験や知識によるものであり、本当にそうなのかというのは一度検証する必要があると考えています。

そもそもアメリカ政府がこういった俯瞰的な方針をもって実際にどういった行動をとったのかとか、アメリカ政府はインターネットが始まって以来こういう方針をとってきました、こういう場面ではこういったことをしてきましたみたいなことを一度調査いただきたい、それがありますと、判断が非常にしやすいと思うのです。

究極的には政府の大方針も変わっていかないと、また、民間の文化も変わっていかないと根本的に解決できない問題があると思いますので、そういったところの情報も、難しいとは思うのですけれども、政府側から示していただきたいなというのが私の何年か委員をやらせていただいてのお願いです。

あと２つは小さいところなのですけれども、ソフトウエアの脆弱性というところで、開発者と直接話をしながら、というお話がありました。これは企業が特定されている場合はいいのですが、オープンソースソフトウェアに代表されるように、開発者の特定も難しいような動きになっていて、今後、ＩｏＴや外部サービス連携ということになるとさまざまな企業やシステムが複雑に絡み合うことが想像されます。

そのようになる時代に、どんな形でソフトウエアの開発者の方と進めていかれるかというところを決めておいたほうがいいと思います。

３つ目は、先ほど横塚委員から海外からのハッキングというご発言がございましたけれども、それは本当にそのとおりだと思いますし、国際的な脅威に対してどういった取り組みができるかということを示して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。日米のいろいろな構造の違いについてのご質問でしたので、後で議論が切れたところで少し対応するようにしましょう。それでは、松尾委員、お願いいたします。

○松尾委員

まず、人材育成の話がセキュリティ関連でいろいろ出ておりまして、それ自体は非常に重要なことだと思います。一方で、使う側として人工知能を活用できる人材の育成というのも同時に極めて急いでやる必要があるのではないかと思っております。

２点目が、個人情報の整備というあたりは本当にどんどん進めていただければと思っておりますが、先ほど松本先生からありましたように匿名加工情報の中身がすごく重要で、そこがどういったあたりになるのかというところを詰める必要があるのではないかと思っております。

３点目は、少し漠然とした話になってしまうのですけれども、個人情報周りの話をいろいろ聞くにつけ、私なりに思うところがあって、どういうことかというと、そもそも個人の情報を守りたいという話とそれを活用したいという話が実はブレーキとアクセルの関係になっていて、それを両方一緒に踏んでしまっている気がするのです。何かといいますと、例えば人工知能で技術が進むと何が起こるかというと、少ない情報、少ないサンプルでも非常に自由度の高いモデルが同定できるようになるわけです。それは逆にいうと個人の情報を暴いてしまうことができるようになると。それは技術の進歩としては必然的にそうなるわけです。一方で個人情報を守る立場としては、そうしてはいけないとなるので、より情報を出さないべきだというようになって、そうすると、技術が進めば進むほど出せる情報がますます少なくなってくるという、何かよくわからないことになってくる。

私は、本来これはどのように解決すべきかというと、恐らく、この人は信用できるから情報を出してもいいのだという、それは対企業の場合は法人という人格に対して信頼を与えて消費者がその情報を提供しているわけで、それがGoogleなりAmazonなりという非常に大きな法人であればそれがいろいろなものに転用されてもいいというように考えると、データ活用における新しい法人格のような、少し違った概念をつくり出さない限りは、本質的にブレーキとアクセル両方を踏んでしまっているという問題が解決しないのではないかと思っております。当面やらないといけないことは、前に進めていかないといけないというのはそのとおりで、ここに示していただいていることは非常にすばらしいと思うのですけれども、一方で長期的にはそういうことも考えていく必要があ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。それでは、水嶋さん、お願いします。

○水嶋委員

今回のプレゼンテーションでビジョンを策定して、将来像をまとめて、必要な体系、あるいは制度整理、人材育成をやっていこうというのは非常に意義のあることだと思っております。前回も述べさせていただきましたが、今、国民の皆さんにＩｏＴ、あるいはビッグデータの利活用のメリット、それによりもたらされる世界観というものが本当に伝わっているのか、ということを少し疑問に思っております。

こういう取り組みについては、メリット側と、今のお話にもありましたようにリスク、あるいはデメリット側の問題が常に両天秤にあるわけで、そうするとメリット側のものをしっかりとご理解いただかないと一定のリスク、あるいはデメリットに対する割り切りの線引きができないのではないのかなと思っております。ぜひメリット側の、どういう世界観が来るのかということを国民の皆さんに十分理解していただけるよう、そのために実証プロジェクト等をしっかりと実施して進めていただきたいと存じます。

また、規制の改革のところにつきましても、国土交通省であったり、厚生労働省であったり、いろいろな関係省庁にかかわる問題が出てまいりますので、この辺の連携について、しっかりととっていただけるような体制をお願い致します。

ちなみに、ＪＥＩＴＡにおきましても今回、ＣＰＳ社会実装検討タスクフォースを設置いたしましたが、どのような実装プロジェクトに取り組んでいくことがいいのかという検討を進めております。自動走行を用いた物流や医療・ヘルスケア、また、ホームネットワークの活用による効率的エネルギーの利用といったことについて具体的な提案を経済産業省にしていきたいと考えております。

その裏返しになりますが、今回のデータの利活用について、個人情報保護法ということで、もちろん本人の同意を得ることが重要ではありますが、利活用を進めるためには、１つの組織にとどまらず複数の法人とか研究機関が共有していくことが必要になってまいります。この場合に、どこまで匿名化の加工をすれば横方向に流通してもいいのか。単純にその法人なり機関が使うということだけではなくて、横方向の連携のためにはどの程度の匿名の加工をすればいいのかというようなことは、我々としては非常に悩ましいところではないかなと思います。守秘義務、あるいは匿名化というところにつきまして、これも国民の皆さんに理解をいただけるような基準を示す必要があるのではないでしょうか。片方でメリットといいますか、夢のある社会の構築を明確にイメージしていただくとともに、そのためには一定の匿名化や守秘義務の線引きをして、それでご理解をいただくといったような取り組みが必要なのではないかと思っております。

また、単純に個人の情報ということではなくて交通機関の運行状況、渋滞状況、いわゆる公的なデータについては皆さんへの共有、あるいは事業者間取引での促進といったものについて進めていただけるようにお願いしたいと思っております。特に政府機関が保有するデータを率先して皆さんに提供していただ

けるような仕組みづくりをお願いしたいと思っております。

セキュリティの話なのですけれども、セキュリティは、非常に悩ましい問題です。いかに個人のデータなどを保護していても、セキュリティが一旦破られれば大した意味もなくなるというような危険性もございます。今日もいろいろお話がありましたが、セキュリティ人材育成等セキュリティ対策をぜひ迅速に進めていただけますようお願い致します。

また、国際連携のお話もございましたが、我が国のカウンターパートとなり得るだけの力といいますか、そういうものを我が国にもたせるということが非常に重要だと思っております。いろいろな機関でやっていただくこともいいかとは思うのですが、何よりも世界に冠たるサイバーセキュリティ産業と人材をつくるということが、このカウンターパートたり得る我が国の目指すべきものだろうと思っております。また、前回申し上げたことでもありますが、政府調達の機会を通じて、セキュリティ産業の育成を進めていただくことをお願いしたいと思っております。

以上でございます。

○村井委員長

ありがとうございます。三輪さん、お願いいたします。

○三輪委員

三輪です。よろしくお願いします。3 点あるのですけれども、これも繰り返しいっていることなのですが、日本においてセキュリティ対策が進まない大きな理由は、誰もやりたくないからですよね。やらない理由というのは、最近の標的型攻撃に関していえば、全く気づかないし公表義務もないし、だったらみつけないほうがいいよねといって今は何もしないほうが得なのです。いろいろな経緯があって公開しないといけないところがた偶然報道されているだけで、水面下ではとんでもない数の事案が実際に起きているのです。でも、ほとんど世には出てこない。例えば特定個人情報においては、特定個人情報の取り扱いの端末に関する操作ログの記録であるとか、それを定期的に監視するとか、それに対する漏えいとかがあった場合、あるいはおそれがある場合にも届けないといけなくなっていって、場合によっては速やかに公表というところまで明確に書き込まれています。

そういうことからすると、特定個人情報ほどではないにしても、企業においてもマルウェアは感染した段階で公表というか、届けるとかしない。マルウェアというのは情報が漏れたことはほぼわからないのです。今のフォレンジック技術をもってしても、何が漏れたかはわからないのです。そういうことからすると、感染した段階で基本的には向こうは入ってきているのだから何もしていないわけがないので、一定期間の通信があれ

ば、それは出ていったに決まっている。何が出ていったかは確定できないけれども、その中にある情報はもっていかれたに決まっているわけなので、その段階での届け出、公表、あるいは、もともとそれを監視する義務というのをどこかに課さないと、経営者として取り組まないと思います。

今、日本において個人情報について敏感なのは、やはり届け出義務があるから。私はそれが一番大きいかと思うのです。でも、マルウェア感染に関していえば、漏えいを確定させることは難しいことなので、実際に届けることもないし公表することもないというのがずっと繰り返されています。日本の全ての企業にこれを当てるのは不可能だと思いますので、重要インフラであるとか、政府に関係のある重要な企業であるとか、そういうところにはこういったものを義務化していくのは必要ではないかと思います。特に、漏えいが確定したらではなく、あるいはシステムが破壊されたり止まったりしたという障害ではなく、マルウェアが侵入した段階で届け出義務があるようにしてほしいと思いました。

○村井委員長

侵入……

○三輪委員

無理だというのは、よくわかっていていっています。

○村井委員長

つい口を挟んでしまったのだけれども、つまり侵入の段階は全てのメールにあり得るのですよね。侵入してしまうと感染の疑いが非常に高くなる。

○三輪委員

そういう意味では感染という段階ですよね。

○村井委員長

そうですね。侵入というのはメールを受け取ったらということですよね。

○三輪委員

私もそこまで敏感にいっていないです。全て感染して外への通信が確認された場合という定義でいいと思います。

２番目に、制御系ということからすると、一番抜け落ちているのがＰＯＳシステムというのは金融のようで金融でなかったり、その辺、結構抜け落ちたままになっていて、日本が大規模な攻撃を受けていないのは奇跡にしか過ぎなくて、ここは経産省だから、これは金融だから関係ない、というようにみるのか、実際、ネットワーク構成においてはオープンな中に置かれているので、金融の網にはかかっていないと私は思っているのです。なので、ＰＯＳシステムについては早急に手を打たないと危険だと思います。

３番目に、今回ファンドは関係ないのですけれども、話題ではないことになっているのですが、一応つけ加えておくと、このままいくと政府系ファンドでお金だけばらまいて終わりにならないようにするためにも、投資した会社においては必ず政府関係、経産省だけでもいいですけれども、関連組織での調達というのを必ずつけてあげてほしいなと思いました。

以上です。

○村井委員長

ありがとうございます。それでは、石井さん、お願いいたします。

○石井委員

パーソナルデータのさらなる活用に向けた取り組みのところでコメントを申し上げたいと思います。既にご指摘のあるところとも重なっておりますけれども、６ページの③さらなる個人情報の利活用のために検討すべきものというところの欄に、個人の権利を実質的に侵害する可能性は低いと考えられるものの、同意取得や匿名化が現実的に難しいと考えられるケースがあるというように書いてあります。これに対処するためには、着地点としては別法をつくってみたり、次の改正を待ったりするといったことが必要になってくるであろうと考えられます。

大量のデータを収集して分析するときには、現状、同意スキームが効かなくなっている、同意スキームが合わなくなっているという問題があります。他方で、法制度は同意を前提につくられているというところが問題の根本にあると考えております。

仮に別法や次の改正を待つことを考える場合には、幾つか論点が出てくると思われます。例えば、今回の個人情報保護法の改正は民間を対象にしたものになっておりますけれども、行政や自治体が保有するもの、研究開発関係ですと国立大学法人が保有をするようなものについても分野横断的に解決する必要があるということが１点目です。2点目として、7頁の記載を拝見しますと、今回の民間の個人情報保護法の改正に関しては、病歴や犯罪に関する経歴が入ると要配慮個人情報の規制がかかってくる可能性があるということです。

匿名加工については、ほかの先生方からもご指摘がありますけれども、仮名データが含まれるかどうかという点を含め、ある程度解釈を待つ必要があるかもしれないということです。3点目として、公益目的、例えば事故の防止、犯罪の予防、医学の向上といった全体的な社会の利益を上げていくようなものにおいては、データの利活用を進めるべきと考えられますが、他方で、目的外に使われないように委員会の監督が及ぶようにしなければならないといった問題もあったりします。これらについて、ある程度時間をかけて論点を砕いて検討していく必要があるであろうと考えられます。

以上です。

○村井委員長

ありがとうございます。有賀さん。

○有賀委員

私も先ほどの石黒さんの話の、政府の話の逆に民間版もやるべきだと思うのです。ここで議論するのは難しいテーマなのですけれども、経営者の頭の切りかえをどうするかというのがすごく大きい問題だと思うのです。より具体的に申し上げれば、先ほどトップクラスの人材をどうするのだというのですけれども、いないわけではありません。極端にいえば活用されていない。大体そういう人たちは、ちょっと変人ですから、むしろ大人しくしていて、仕事をやれといったらやってしまうわけで、そうすると青い銀行ですとか、隣の上場する銀行のレガシーな仕事をやらせたほうが真面目にやります。そういう人間を活用する場が、結局変なところに行ってしまうわけです。処遇も当然悪い。

こういうところを経営の立場で改めない限りは、そちらのほうが儲かりますから、レガシーなものを開発させたほうがいいわけです。この辺をどうするかというのはすごく大きな問題だと思います。

それから、最近非常におもしろい分析をやりました。、私は実はＩＴコーディネーター協会の理事をやっているものですから、ＩＴコーディネーターの方々が自分の会社でどんなブラウザを使っているか調べました。そうしましたら、何とＩＥ６ですとか、７ですとか、８がメインなのです。ＩＴ関連の企業の、しかも、具体的に申し上げたくはないのですけれども、ＪＩＳＡの会員ですとか、ＪＥＩＴＡの会員ですとか、経団連の会員が山のように、しかも超有名な会社がずらっと並んでいるのです。せめてＩＴ関連企業のトップぐらいは、その辺について少し頭を切りかえてほしいなというのが非常に強く感じました。IE８でさえも既に脆弱性が指摘されていて、パッチが当たることはもうないといわれているわけですから、幾ら何でもひどいなと。だから、そういう立場の方が今日みたいな議題を協議しても無駄かなと。

その辺、私は非常に強く感じていまして、これはどうやってプロモートしていくかというのは、すごく難しい

問題なのですけれども、先ほどの人材の登録、更新よりずっと難しい問題です。でも、これは皆さん本当に真剣に考えないとなりません。先ほどの政府全体のコンセプトのつくり方などは私はすごくすばらしいと思っていますけれども、経営そのもののつくり方が全然違っていて、ＩＴ関係で勝とうと思ったら、そこら辺を上回るようなコンセプトでいかない限りは勝てない。そこは、ここにおいでになる、政府も考えないといけないかと思いますが、委員の方でもお考えにならないといけないのかなと、この分析をみて強く感じた次第です。

○村井委員長

ありがとうございます。澤谷さん、お願いします。

○澤谷委員

４つあります。まず、ページ４のプラットフォーム技術開発については、インターナショナルな取り組みとして海外の企業と協業し、日本の強みを出していくことを期待します。

次に、新しい社会システムの推進では、雇用をつくり出すことも戦略の１つとして考えていただければと思います。GAFA（Google、 Apple、Facebook、Amazon）等、ＩＴベースの企業がトヨタの何倍もの時価総額の企業に育っています。実際に第３次産業の中でもＩＴベースの企業が雇用を生み出しているということを考えると、ぜひアクセルを踏むことをやっていただければと思います。

３番目に、ＣＳＲを企業で実施してきましたが、これからＣＳＶ（クリエイティング・シェアード・バリュー）、ともに価値を企業も社会のためにつくっていくということが重要になってくると思います。データは、目的によって活用は良くも悪くもなります。企業が新しい社会的な価値をつくることを支援していただければと思います。

４番目に、若い人ももうちょっとフォーカスしたほうがいいのではないかと思います。2030年のビジネスを考える場合に、そこで活躍している30代から40代は今15歳から25歳です。産まれたときからデジタルがあって、デジタルネーティブといわれる彼らは、私たちが考えるよりも違うやり方で価値創造をしていくと思われます。そういったことを考えますと、15年先の戦略をつくる場合には、中心になるであろう若い世代の声を聞いていくことが重要だと思います。

以上です。

○村井委員長

ありがとうございました。砂田さん、よろしくお願いします。

○砂田委員

２点あります。１つは、先ほど来、ビッグデータやパーソナルデータの活用のメリットをしっかり強調すべきだというご意見がありましたが、私もそれは大変重要だと思っております。かつて、情報通信白書の情報セキュリティに関する調査で、実際の被害にあったことはないにもかかわらず不安を感じる人が多いのが日本の特徴という結果が出ておりました。メリットとデメリットの両方を理解することが不安解消へとつながるように思います。とくにメリットへの理解を高めるためには、まずは政府自らが実際にビッグデータを活用して、消費者や企業にとって有益な情報を提供することに力を入れていくことが大切ではないかと思っています。

たとえば、韓国のＫＩＨＡＳＡ（Korea Institute for Health and Social Affairs：韓国保健社会研究院）という政府系シンクタンクでは、４年分のSNSのビッグデータ分析に基づいてゲーム中毒の子供をいかに減らせるかを分析したり、検索エンジンで入力されるキーワードから自殺者を減らすにはどうしたらいいかを分析したりして、政策提言を行っています。日本でも国土交通省はすでに自動車のドライバー向けに有益な情報を提供していますが、センサー収集データをより充実させることで、その情報内容をさらに豊かにしていくこともその一つでしょう。経済産業省でも近年の急成長企業のデータを分析するなど、企業向けに有益な情報提供をさらに強化できると思います。行政機関とデータの関係といえば、個人情報保護が大きな論点になっていますが、それだけでなく、行政自らがビッグデータやパーソナルデータの先進ユーザになっていくこと、そしてデータ活用の効果や利点をしっかり発信していただくことが重要と思っています。

もう１点は、ＩｏＴの実証実験です。従来とは大きく違って、産業が再定義されるということをベースに考えていただくとよろしいかなと思っています。伝統的な自動車産業はトップクラスの大手自動車メーカーを中心にした産業構造となっていますが、それがモビリティサービス産業として再定義されていくと、パーソナルモビリティやモビリティ情報サービスなど新たなベンチャーも出てくるでしょう。プレイヤーが多様になるだけでなく、パワーシフトが起こる可能性もあります。たとえば、自動車のドライバーや各種移動サービスの利用者といったユーザが発信する情報の価値が高まるので、ユーザのパワーは強くなるでしょう。そういった新規参入のビジネスや新しいサービスのユーザなども含めた実証実験を考えていただくといいかなと思っております。

また、産業の再定義が進むプロセスでは、新たな産業クラスターがつくられていくような気がします。農業ですと、農地が作物の生産だけではなくて、農業情報を発信する拠点としての役割が大きくなるでしょう。製造業においても、モノづくりの中小企業、町工場のクラスターで、単に下請の部品をつくっているだけではなくて、３Dプリンターを利用する個人向けに新たにモノづくりの情報を発信する拠点になる可能性が

あるわけです。そういった新しい産業のイメージのもとで実証実験、新しい試みをしていただければと考えています。

以上、２点です。

○村井委員長

ありがとうございました。野原さん、先にお願いします。

○野原委員

１点だけ申し上げて、もう１つは所感を申し上げたいと思います。

サイバーセキュリティ戦略が９月４日に閣議決定されて、それを踏まえて、経産省がしっかりと取り組んでいこうと思っていらっしゃるサイバーセキュリティ関連の施策がとりまとめられていると理解しています。13ページ以降の論点として上げられている課題については、具体的で適切に取りまとめられていると思うのですけれども、12ページの中の「政府系ファンド等の活用」という項目については、もう少し書き方を変えていただけないだろうかと思います。

趣旨は、サイバーセキュリティ関連の施策は、資料にあるように政府機関を守る取り組み、重要インフラを守る取り組み、企業を守る取り組み、関連した基盤整備というように、いわゆるユーザの組織を守る取り組みとして全体像の枠組みが捉えられているわけですけれども、それだけでなく、関連サービスや、ツール、体制、ノウハウを提供するサイドのセキュリティ産業があるわけで、その部分がしっかりと成長・充実しないと守ることはできないと思うのです。

そういう意味で、この項目は、できれば「セキュリティ産業の振興」とか、「セキュリティ企業の競争力強化」等より大きな概念を前に項目として出して、そのうちの１つの取り組みとして政府系ファンド等の活用もあるという位置づけの記載にしていただきたいと思います。このように頭にこの項目があると、それ以外の施策はないというようにも読めますし、そのあたりのセキュリティ産業の振興策を、特に経産省さんのほうでは取り組んでいただきたいと思いますので、その点、この紙のスタンスを変え、このアウトプットの中でもそうしたことに踏み込んでいただきたいと思います。それが１点です。

あともう１点は、この10年ぐらい経産省さんの委員会ですとか他の政府の委員会や政策会議にも多数参加させていただいていますが、とても気になっているというか、問題だなと思うのは、政策の検討や策定の手順が、いわゆる従来の方法論にとどまっているというか、経済成長期の間に培われた、基本的には今ある産業をそのまま延長線上で成長させるための政策を検討する枠組みになっていると思うのです。

そのために枠組みとして既存の大手プレイヤー方々が中心に集まって、あるいは業界団体もできてき

ちんと整備されてきた段階の産業の人が集まって、そして少し先の未来を検討すると。そこから出てきた声を要約して、調整して、できる範囲で方法論を政策として落とし込んでいくということをやっていると思うのですけれども、これに限界があるのだと思うのです。

いろいろな方が、若い世代の声をきちんと聞かないといけないとか、ベンチャーを育成しないといけないとか、私も一生懸命、考えつく限り、その都度いろいろ発言をしてきたわけですけれども、これだけ社会環境の変化が激しく、市場動向、ユーザーニーズ、そして競争環境が変化し、経済・産業界のありようが大きく変わっていくというような時代背景の中で、高度経済成長期に培われた枠組みではいけないのではないかと思います。そういう意味でも、こういう場も使ってどういう形の議論をすればいいのか、あるいはどういう形で官僚の方々が動いてくだされればいいのか考えていただきたいと思います。

先ほど石黒委員からも示唆に富んだ発言がありましたけれども、ああした日米の比較分析をして、その結果報告書がまとまって、次の人が来たらそれを忘れてしまうということではなくて、そこで出た知見をもとにちゃんと政策検討の枠組みを変えるということに落とし込んでいかないといけないと思います。ぜひそうした政策検討のあり方も一緒に考えながら新しいやり方をみつけていただければと思います。

○村井委員長

ありがとうございました。では、岡村さん。

○岡村委員

岡村でございます。手短に申し上げます。先ほど三輪さんがおっしゃったことですけれども、私が現場をみると、けっこう暗たんたる状況だと思います。感染していることがわからない、感染していることを告げてもどうしていいかわからない、これが実情だと思っております。というか、そのようにみてまいりました。

大企業中心であるということはわかりますけれども、中小企業にアウトソーシングをすることで産業界が成り立っていることも事実でございます。重要インフラ、基幹だけに目を当てずに、そういうところへ目を当てているときには、むしろ今のようなＩＴ系の、いわゆるベンチャー企業であればともかく、それ以外の企業の場合にはパラダイムシフト的な考え方で不要不急ならばインターネットに接続しないぐらいの方向でいかないと間に合わない。現に中小、自治体に関しては今度の番号通知の関係でそういう方針が一部打ち出されているところでもございます。

あるいは、インターネットにつなぐ必要があるのであれば、早い話、責任ある、かっちりした事業者に預けてしまうということで責任の移転をする。現実に国立大学法人はこの数年ほどの間にすごい勢いで外部の事業者へ委託するということで、自前で管理するというところからかなり変わってきている。もちろん端末

管理は必要になるわけですけれども。

ということで、私がもう１点だけ申し上げたかったのは、日本を支える中小企業については、優しいセキュリティということで、必要でなければつなげない、つまりインターネットから切断するということを考えてもいいだろうし、接続する必要があるのであれば責任の移転というセキュリティ用語でいうところの概念に従って安心できるところに預けてしまう。それぐらいのパラダイムシフトを考えないといけないだろうと。そうして初めて、そこからつながる重要インフラ等々が守れるような状態になるだろうということで、セキュリティの観点からももうそろそろ考え方を根本的に改めたほうがいいのではないか。そのために中小企業庁などで啓発活動とか、そうした動きをしていただきたいということをつけ加えさせて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。では、石黒さん。

○石黒委員

ジャストアイデアですが、私が間違っていたら先生方にご指摘いただきたいのです。セキュリティ人材なのですが、学術関係ともう少し密接な連携をとったらどうかと思っていて、具体的にはポスドクの方の活用というのはどうなのでしょうか。――他の会議で、今ポスドクの方が物すごく余っていらっしゃるという議論がありました。

しかし、殊この分野、セキュリティは民間にも人材がいないし、恐らくかなり高度なことをやられていると思いますので、ポスドクの方の活用というのはあるのではないかなと感じました。

○村井委員長

期待していただいてありがとうございます。ただ、セキュリティのポスドクが余っているということはないような気がしますけれども。松本さん。

○松本委員

今全然足りなくて、全部出払っています。

○村井委員長

先ほど、私は逆のことを松本さんにお伺いしようと思っておりました。現在、セキュリティ関係の人材が

非常に必要なため、かなりの予算が割り当てられています。そうすると、この国全体で本当に必要なところでの取り合いが起こっているような気がしています。文科省のセキュリティのプログラムも、ＡＩも似たようなところがあるかもしれません。

基本的には、いいと思うのです。要求があって、予算がつく領域だからこそ取り合いが起こるのだけれども、そうすると例えば重要な役割を担うＪＰＣＥＲＴから人材を引っこ抜くようなことになってしまうといけないでしょう。何となく、松本先生のような業界のリーダーが、ある程度全体を俯瞰してバランスをとらなければいけないということがあるのではないかと思っています。

リーダーが八面六臂で働くのは当たり前なのだけれども、少し配置を考えなければいけないですよね。ＡＩの領域も同様ですが、今、研究として全体の動きは進んでいるのだけれども、いい人材を最適配置するという努力も要るような気がするのですが、どうでしょうか。

○松本委員

そのとおりだと思います。基本的に、普通の技術を使ってモノをつくる人が常識としてセキュリティのことがわかっていないとシステム、製品、サービスがつくれない。明らかなのですけれども、今まで後回しにされてきてしまったというところはあります。

大学等でもその辺のキャッチアップといいますか、昔からやっているグループはずっとやっているのですけれども、パイが小さいので人数は少ししかいなかったというところで今足りないという状況があると思うのですが、今ここにいらっしゃる団体の中のリーダー格の会社でも、本当に中枢でセキュリティを仕切れる方は何人かしかいらっしゃらないという状況があり、我々およびのセキュリティ分野の同僚のところにも、よいドクターコース修了候補者の人や、さっき石黒さんがおっしゃったような形でポスドクの方で当社に来ていただける方は「いませんか」というようにたくさんお声掛けいただきます。そうすると、セキュリティを専攻した若手は、自分たちが生き延びないといけませんので、チャンスがあれば飛びついてしまうということになります。つまり、ある意味で力があるといいますか、魅力的な先がどんどんそういう人材を獲得していくことになります。

問題は政府系とか国全体で最適化ということがあると思うのですけれども、これは競争だと思いますので、いかに魅力ある条件で雇用ができるかとか課題です。加えてセキュリティ人材だというのでとがった人がよくいまして、そういう人が外部から助っ人で企業に入ってきても、もともとそこで頑張っている方々とカルチャーが違って衝突が起きてうまくいかないケースが非常に多いいので、中で育てることも含めていかないといけないと思います。

ですから、常識として、教養としてセキュリティ分野の力を相当もった人たちをつくっていくというのが教育機関系の課題としてはあると思っております。このような先が長い話も、即戦力ということで今すぐに役立

つ人が圧倒的に足りないことを解決する方策とともに、長い時間をかけて地道にパラレルにやっていかないといけないと考えます。

○岡村委員

最後に端的に申し上げますと、先ほど国立大学法人が外部委託を始めたということを申し上げましたけれども、ある有名国立大学の大型電算機センターで運用の中心を１つ世代前にやっていた２人は、１人はおられる。もう１人は国立の研究機関におられるというような状態で、ブリーダー的な役目で大型電算機センターのお守りをやっている人間が大学におられたわけですが、外部委託で吹っ飛んでしまうと、ブリーダー役が物すごく手薄になっているということだけ指摘しておきます。

○村井委員長

岡村さん、外部委託と人材育成の問題はいろいろ難しいですよね。松本さん、どうぞ。

○松本委員

ついでに申し上げれば、横浜国立大学もそのような形なのですが、ネットワークとかセキュリティとか暗号をやっている研究拠点では、唯一自前での管理もやっておりまして、そこが事故を起こすと大変なことになるのですが、やはりかなり気を遣って自分たちでメンテをしていかなければ身につかない力ということはどうしてもありまして、かつリアリティーがないとだめなので、ちょっとした演習とかでは余り効果がないという悩みはあります。

でも、そういうことを地道にやっている方々は日本全国にそれなりにはおりますので、そういう人たちを核として、人材を大学等でもきちっと育てていかないといけないと考えます。

○村井委員長

岡村さんの先ほどのお話は半分諦めのように聞こえるところもありますが、中小企業もインターネットにつながらないと事業が発展しませんし、人材が少ないのはわかっていますが、やはり育てることを諦めてはいけないと思うのです。そのためにどうすればいいのかということですけれども、そこには、本日の議論の中に、三輪さんがおっしゃったような、ある意味の仕組みとして人を育てるであるとか、石黒さんの会社の中でポスドクをやっているなら３倍の給料を出すとか、前回話題になったＣＳＩＲＴを全ての組織をつくり、監査のメカニズムをつくるというお話もありました。このようなことを、マーケットでも東証でも役所でもいいと思いますけれども、強制力を持った仕組みとしてつくることによって、それぞれの組織に人材を育てていく必要

があると思います。

やはりそれぞれの組織において、セキュリティに対する意識レベルが上がり、それを担う人材が全ての組織にいなければなりません。前回出たＣＳＩＲＴは全ての組織にあり、そのレポート体系があって、例えばＪＰＣＥＲＴがそのネットワークの中心だとすれば、そこからある意味の監査のようなメカニズムが社会の中にできるとか、そのようなことも必要かなとセキュリティでは思いました。

ちなみに、時間をオーバーしていますが、もう１点だけ。ＩｏＴの推進に関して、皆さんのお話を伺って出てきたのは、リスクと利点、つまりポジティブインパクトとネガティブインパクトがはっきりいってよくわからないということだと思うのです。確かにそのとおりで、これはいろいろなことを言う方がいますし、そもそもビッグデータ、クラウド、ＡＩ、ＩｏＴ――全てを複合してＩｏＴといっているようなところですので、データを使うということだけはどうも間違いないようです。

そうすると、プレイバシー等の問題が出てきますが、私が思うのは、先ほどの石黒さんのお話とも関係があるのだけれども、ＩｏＴのインパクトとして、ネガティブもポジティブもあり、これの定量化の話がないですよね。こういうことをやるときには、例えば経済効果等、やはりある程度の目標値をつくって、それを修正できる定量的なインデックスが普通はあるでしょう。これが今はないのです。

アメリカの研究者と話をしていると、その調査のためにシンクタンクや大学に予算をつけているのです。ポジティブインパクトは何か、リスクは幾らになるか、うまくいったらどれだけの経済効果があるか、先ほど松尾さんがおっしゃったような形でＡＩの研究が進化したらどれだけのインパクトが出てくるかなど、そういう調査を研究者本人ではなくてもいいけれども、専門家が調査して、あるいはきちんとしたヒアリングをして、定量的な目標値を出すという研究自体に大きな研究費がついているのです。しかし、この国は、このような研究費がないのです。

いずれにせよ、先ほど有賀さんがおっしゃったように民間の経営の問題もあるでしょうし、行政の問題も、法制の問題もあると思います。それぞれの点で、過去の分析結果は出していただけるといいかと思います。ただし、この話は未来の話ですから、もしかしたらゲームチェンジかもしれない。そうすると、そのときの予想はそれなりにコストをかけて調査をして、目標値を定量的に把握しておく必要があるのではないかと思います。それが前半の話です。

セキュリティの話はたくさんのことがありますが、三輪さんがおっしゃったような、ある程度の強制力を持った方法を考えて、全体的にその新しいやり方でセキュリティに対する意識改革や人材の問題に手を打たないと、使命を果たしたといえない時期に来ている気がいたします。それでは、事務局から連絡をお願いいたします。

○佐野課長

次回の日程でございますけれども、１ヵ月後の10月30日をめどに今調整をしておりますが、開催が決まり次第皆様にご連絡をさせていただきたいと思いますので、引き続きどうぞよろしくお願い申し上げます。

以上です。

○村井委員長

それでは、委員長不手際で時間をオーバーいたしまして、申しわけございません。会議は以上でございます。

――了――