

## 産業構造審議会 商務流通情報分科会 情報経済小委員会（第7回）

### 議事録

日時：平成27年12月7日(月曜日)16：00～17：30

場所：経済産業省本館17階 国際会議室

議題：（1）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に関する対応

（2）その他

#### ○佐野課長

それでは、定刻になりましたので、ただいまから、産業構造審議会商務流通情報分科会第7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、まことにありがとうございます。

まず、議事に先立ち、資料の確認をいたします。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。ご協力をよろしくお願いいたします。

本日の配布資料は、座席表、議事次第のほか、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に関する対応」、資料3としまして、「試験ワーキンググループの設立について」ということでございます。それから、参考資料としまして、「IT利活用ビジネスに関するルール整備WGについて」でございます。

iPadの不具合ですとか資料が掲載されていないなど問題ございましたら、事務局の方までお声がけをお願いいたします。

本日は12名の委員にご出席をいただいております。規定の過半数11名に達しております。あらかじめご連絡をいただいた有野委員、石井委員、石黒委員、岡村委員、國井委員、國領委員、根本委員、松尾委員、横塚委員は、ご都合によりご欠席となっております。

それでは、ここからの議事の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

ありがとうございます。どうぞよろしくお願いいたします。

これより議事に入るわけですが、5月に本委員会でもとめた報告書に基づいて、これまで、データ利活用、サイバーセキュリティに関する法制度等の課題について議論をしてきました。ここまでの議論を踏まえて、IoT推進コンソーシアム、法制度の検討を大分進捗させていただいたという状況になっております。したがって、本日、国会との関係での法制度に関する議論を賜って、今後の法案作成などに反

映させていただくという会議になっております。どうぞよろしくお願いいたします。

それでは、「I o T 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に関する対応」について、資料 2 に基づき事務局から説明していただいて、その後、自由討議をさせていただきたいと思います。それでは、説明をお願いいたします。

○佐野課長

それでは、事務局のほうから資料 2 に基づきまして説明をさせていただきます。

先ほど委員長からご発言があったように、5 月にレポートをまとめまして、それに基づき、I T 利活用、セキュリティ等の施策について具体的に進めてまいりました。

I T 利活用について、後ほどご紹介しますが、I o T 推進コンソーシアムを総務省と共同で 10 月に立ち上げ、関連施策の展開を進めてまいりました。また、内閣官房の I T 室で、I T 利活用新法（仮称）に向けた検討を進めてきております。その中で、これまで、この審議会でもご審議賜った事項について反映することを検討しているところでございます。

それから、大きく 2 つ目、セキュリティについて、セキュリティの関係での法制度整備ということで、「2 - 1 セキュリティ対策強化に向けた制度整備」、「2 - 2 情報処理安全確保支援士（仮称）制度の創設」、「2 - 3 ソフトウェア脆弱性情報の公表の方法・手続の整備」についてご説明いたします。それから、運用については、「2 - 4 サイバーセキュリティ経営ガイドライン（案）」としまして、今準備を進めておりますサイバーセキュリティ経営ガイドラインについて、ご説明いたします。

以上について、本日ご審議を賜ればと考えております。

1 - 1（1）「I o T 推進コンソーシアムについて」、企業、業種の枠を超えまして、産学官で利活用を促進するために、民主導の組織として I o T 推進コンソーシアムが設立されました。一番下をみていただきますと、総務省、経済産業省共同で取り組んでおります。会長には、村井委員長をお願いしているところでございます。総会の下に 3 つ組織がございまして、1 つが技術開発 WG（呼称：スマート I o T 推進フォーラム）でございまして、ネットワーク等の I o T 関連技術の開発・実証、標準化を行う機関でございます。2 つ目に、I o T 推進ラボでございまして、先進的なモデル事業の創出や案件ベースの規制改革などの環境整備を行う組織でございます。それから、3 つ目に専門 WG としまして、セキュリティ、プライバシー関連の専門家が集まって議論していく場をつくるということにしております。

ページを 1 枚おめくりいただきますと、前の I o T 推進ラボの活動の紹介ということで、10 月 30 日に開催された第 1 回 I o T 推進ラボの報告をいたします。支援委員会の加盟企業の半数程度が外資系企業であり、オープンな運営をさせていただいております。

この I o T 推進ラボの中には 3 原則として、成長性・先導性、波及性（オープン性）、社会性を掲げております。こちらの 3 原則に基づきまして、個別の I o T プロジェクトを発掘・選定しまして、企業連携・資金面・規制面から徹底的に支援するということと、大規模な社会実装に向けた規制改革などの環境整備を行うということをミッションとしております。

「支援内容」をご覧くださいますと、企業連携を促進し、資金と規制両面から集中的に支援していくということで、今後は案件の公募を実施する予定にしております。

なお、「第 1 回（10 月 30 日）の意見の概要」としまして、とにかく I o T ビジネスは圧倒的にスピードであるという意見がございました。日本は手続等で非常に面倒な国ということで、事業の候補地にあがらない状況がございました。一方で、技術力等で社会的ニーズをもっておりまして、潜在的なチャンスは多数ございます。海外企業が日本でビジネスをするためには、どんな規制があっても、1 年以内には先鋭的な実証が開始できるようなスピード感、リーダーシップによる環境整備が必要である、こういった意見をいただいているところでございます。

4 ページをご覧ください。この I o T ラボに集まりつつある取組事例ということで 5 つの事例を記載させていただきます。1 つ目にロボットタクシーという会社につきまして、2020 年に無人のタクシー事業の実現を志向しているということでございます。それから、エクスメディオという会社につきまして、スマホを通じて送られた患部の写真をもとに、ディープラーニングで皮膚病の診断支援をするシステムを開発しているベンチャー企業でございます。それから、セーレンについて、47 万通りの生地、デザインから顧客が選んで、世界で 1 着のオーダーメイド服を自動的に生産するシステムを展開しているということでございます。

それから、ドローンによる施工管理ということで、エアロセンスという、あるいはコマツで取り組んでおりますけれども、ドローンで土木現場を 3D モデル化して、建機を自動制御するとか、あるいは建設現場を上空から撮影して、高層ビルの鉄骨の施工状況を検査する、こういったプロジェクトが出てきております。

それから、カスタマイズ健康サービスということで、日常の運動量などの健康データと健診データを組み合わせることで、カスタマイズされた健康生活、習慣病の予防サービスを提供する会社としてテルモが挙がってきております。

それぞれ、規制、ルール面での課題があるところでございまして、こういった障害となる規制、あるいはルール形成について、この I o T ラボの中でサポートしていくことが期待されているということでございます。

次の 5 ページをご覧ください。11 月 5 日に「未来投資に向けた官民対話」が開催されました。I o T をテーマとしまして、I o T 推進ラボの座長であります富山和彦さんと民間企業の 3 社から、I o T のビジネスの取組についてプレゼンを行ったところでございまして、そうした民間企業からは、自動運転、ドローン配達・施工管理、A I の医療診断支援システムに関する規制等の課題が示されたところでございます。

出席者につきましては、富山和彦さんのほかは、ZMPの谷口社長、アメリカのアマゾンのポール・マイズナー副社長、それからセーレンの川田会長にご出席をいただきました。

6ページ目をご覧ください。その官民対話の中で、企業から示された課題に対しまして、その場で安倍首相より具体的な指示が示されました。大きく4つ指示が出ておりまして、第1に「自動走行」について、2020年には無人自動走行による移動サービスや高速道路での自動運転ができるように、2017年までに必要な実証を可能とすることを含めて制度やインフラを整備するという方向性が示されたところでございます。

第2に「ドローン」について、早ければ3年以内に、ドローン物流を可能とすることを目指しておりまして、直ちに「官民協議会」を立ち上げ、その場で来年夏までに対応方針を策定するという方向性が示されたところでございます。

第3に「電波」について、ドローン等の制御・データ通信を広域で可能とするために、来年夏までに、使用できる周波数帯の拡大、出力アップなど、新たな電波利用の制度を整備することとされたところでございます。

第4に「健康医療」について、3年以内に人工知能を活用した医療診断支援システムを医療の現場で活用できるように、来年春までに医療診断支援ソフトウェアの審査に共通して活用できる新たな指針を公表することとされたところでございます。早速、このIoT推進ラボの案件の障害となっている規制やルール形成に関して具体的な指示が出たということでございます。

次に、7ページをご覧ください。内閣官房IT室におきまして、IT利活用に関する制度整備を検討しているところでございます。通称、IT利活用新法として、内容は大きく2つございます。1点目に、安全・安心にITを活用して情報を共有・利用する制度の設立のため、代理機関の創設を予定しております。2点目に、いわゆるシェアリングエコノミーに対応した制度整備を行うこととしておりまして、現在、検討中でございます。

情報の利活用制度につきましては、情報を保有する会社が情報収集を行う事業者へ情報を提供し、事業者はその情報を元に、ビッグデータ分析をし、人工知能やアルゴリズムの精度向上に役立てる。そして事業者は、その成果を、情報を保有する会社に提供するという仕組みを、政府があらかじめ一定の要件のもとに事業者を認定することで運用を図るものがございます。

事業者認定の要件として、安全管理措置を実施しているか、広域目的にかなうかどうか、あるいは事業継続性があるのか等を検討しております。認定後、仮に要件に沿っていない場合には、担保措置として、報告徴集や立入検査、改善命令等を講ずるという制度でございます。

具体的な対象事例として、自動運転向けの3D地図の更新・配信をするためのデータ収集や、医

療情報の収集・分析により治療を高度化する等が想定されております。これまで、この情報経済小委員会の中でも、データ利活用についてご審議いただきましたが、内閣官房 I T 室で検討している代理機関のスキームに反映できるよう、現在、検討しているところでございます。

次にセキュリティについて、「セキュリティ対策強化に向けた制度整備」ということで、本年の 6 月に公表された日本年金機構における個人情報流出事案を踏まえまして、9 月にサイバーセキュリティ戦略が閣議決定されました。それに基づいて政府機関全体の対策の抜本的強化を図ることになっております。

具体的には、下の図をご覧くださいと、従来、政府の監視対象というものは中央省庁がベースでありましたが、それが独立行政法人等にも対象の拡大を検討しております。経産省でもこの対象拡大に伴い、I P A の知見を活用することが検討されております。また、専門人材の拡充やソフトウェアの脆弱性情報の共有体制を整備するため、法改正を含めた所要の措置を検討しているところでございます。

9 ページにつきまして、この情報処理安全確保支援士という名前はまだ仮称でございますが、当制度の創設につきまして具体的に記載しております。セキュリティ対策強化に向けた専門人材数は国全体で不足しているという現状を踏まえ、現在、I P A や民間団体にセキュリティの試験というものが複数実証されております。しかし、人材の所在が見える化されておらず、日進月歩のセキュリティ知識を適時・適切に評価できるものとなっております。したがって、最新のセキュリティに関する知識・技能を備えた高度かつ実践的な人材の国家資格である本制度の創設を検討しているところでございます。

具体的には、2 点ございます。1 点目に、専門人材が見える化して活用できる環境整備をするために、有資格者に対して独占的に情報処理安全確保支援士（仮称）という肩書きの使用を許可する。さらに、民間企業が人材を活用できるように登録簿を整備いたします。

2 点目に、技術進歩が早いサイバーセキュリティ分野では、知識などが陳腐化するおそれがあるということで、したがって、有資格者の継続的な知識・技能の向上を図るために、講習の受講を義務化いたしまして、義務に違反した者は登録が取り消されるという更新制を導入するというところで考えております。

3 点目に、民間企業が安心して人材を活用できるようにするためには、厳格な秘密保持が必要であるということで、業務上知り得た秘密の保持義務を措置することにしております。

10 ページをご覧ください。「ソフトウェア脆弱性情報の公表の方法・手続の整備」についてです。本件も、ソフトウェアの脆弱性に起因する被害、情報漏えいが深刻化しているということで、これまでの情報経済小委員会でご議論いただいております。例としてクライスラーの例を提示させていただきましたが、こうした悪影響を未然に防ぐために、現在、I P A がソフトウェアの脆弱性について情報収集しまして、利用者への公表を行っているところでございます。しかし、これは事実上やっておりますので、ソフトウェアの開発者から公表の同意が得られない場合には、運用上、情報を無理やり公表ということが難しいケースがご

ございます。したがって、法令に基づく手続を定め、その手続に則って、このソフトウェアの脆弱性の情報を公表する制度を整備しようというものでございます。

1 1 ページをご覧ください。「サイバーセキュリティ経営ガイドライン（案）」についてです。サイバー攻撃対策は経営課題として重要なものに関わらず、日本企業では対策が経営問題として考えられていないという現状を踏まえ、企業経営者を対象として対策を推進するためのガイドラインを策定しようというものでございます。

本ガイドラインでは3原則というものを定めております。1つ目に、経営者自身がリスクを認識して、リーダーシップによって対策を進める。2つ目に、自社のみならず、ビジネスパートナーを含めた対策を講じる。3点目に、平時及び緊急時のいずれにおきましても、情報の開示など適切なコミュニケーションをとるという3点について

また、本ガイドラインの重要項目といたしまして、大きく4つに整理しております。

1つ目が、リーダーシップの表明と体制の構築ということで、サイバーセキュリティリスクを認識して体制構築を指示するということでございます。2つ目に、P D C A サイクルの仕組みをつくって、経営者も適時状況を把握し、サイバーセキュリティのリスクを適切に管理するというところでございます。それから3点目に、対策に必要な予算、人材等を確保して、リスクを踏まえた事前の対策をしっかりと講じておくということでございます。最後に4点目に、緊急時の対応体制の整備と演習の実施、それから経営者の説明準備などによって、サイバー攻撃を受けた場合に備えた準備を行うということでございます。

現在、本ガイドラインについては、パブコメを募集中でございます。

それから最後、1 2 ページでございますけれども、「I T 人材に関する検討」といたしまして、年度末にかけて I T 人材の需給に関するアンケート調査を実施するということと、個別のテーマごとに有識者へのヒアリングを行い、今後報告書をまとめていきたいと思っております。

実施内容は、I T 人材需給のマクロ推計をまず行うということ。それからセキュリティ人材や、I o T 関連の新たなビジネス分野で必要とされる人材について、アンケート調査を実施して詳細な需給推計を行っていきたくて考えております。さらに、この調査結果を踏まえまして I T 人材の確保に関する研究会を立ち上げて、今後、我が国にとって必要なスキルをもつ I T 人材を、どのように確保していくのか、ということにつきまして検討を深めてまいります。

以上が、5月のレポートに基づいて、その後、この情報経済小委員会でご審議を賜って、具体的な施策に展開している事項でございます。

私からは以上です。

○村井委員長

ありがとうございました。

それでは、今ご説明いただいた内容に関連した議論をしていただきます。議論の内容は多岐にわたっておりますが、タイトルは「データ利活用施策及びサイバーセキュリティに関する対応」ということで、決めていただきたい内容というのは、この法律に関係があるところ、セキュリティ関係の I P A の人材の件と脆弱性の条文の公表の仕方、この 2 点に集約した内容でございます。

そのほかの前後の話も含めていただいて結構ですので、I o T 社会に向けたデータ利活用及びセキュリティに関してということでご議論いただければ幸いです。

それでは、ネームプレートを立てていただき、私が指名した後マイクを押して御発言いただき、話し終わったらネームプレートを元に戻すという形をお願いしたいと思いますので、よろしくお願いいたします。どなたからでも結構です。どうぞ。

では、夏野さん。

○夏野委員

1 点質問させていただきたく、9 ページの情報処理安全確保支援士制度についてなのですが、支援士制度自身の創設は非常に意義あることだと思うのですが、これまでのこのあたりの国家資格って、大体が、余り実践経験ない人が一生懸命勉強して、資格をとったらどこかに就職して、やっと使いものになるのが 3 年後みたいなのが多いような気がします。この制度も同じように、これから情報処理の安全、セキュリティ絡みの仕事に就きたいという若者を中心として、意思のある人がまずこの資格をとり、そこから経験を積むというタイプのものなのか、あるいは、ある程度経験ある人だけが受けられる試験として、経験に基づいているんな見識があって、その見識を試すような試験にしてオーソライズしていくような試験体制なのか、どちらにするのでしょうか。僕は実は後者のほうがいいのではないかと非常に思っております。免許だけもっている人を増やしてもあまり意味がないと思うので、後者のほうがいいと思っています。

それからもう一つ、もし後者であって、しかも人数がそんなに莫大に、とりあえず何か学部やマスターを出て、勉強すればとれるような資格でないのだとすれば、名前をもっと偉そうにするか、もっと格好よくするか、どちらかにしてほしいですね。支援士とかいうと、なんかちょっと権威も格好よさもないので。

以上 2 点です。

○村井委員長

ありがとうございます。ほかにご意見があれば先に伺っておきましょう。

喜連川先生、お願いします。

○喜連川委員

ネーミングに関しては私も夏野委員と全く同じで、ちょっと I T っぽくないなという感じがします。

それはともかくとしまして、スピード感のある規制改革に関して、今、内閣府でも議論されていると思いますが、いわゆる環境に伴う対処をどうするかということだけでなく、環境の変化を含んだような法体系、いわゆるフェアユースみたいなものはもっと積極的に入れないと、とにかくレスポンスに、リアクティブに動くことになってしまうと思うのですね。著作権法の改正として、例えば検索エンジンに類する何とかの場合は、とか一般化して緩めることも考えておられるのですけれども、そんなことはどうでもよくて、そもそも日本にとってみると、検索エンジンのビジネスそのものをとられたことのほうがはるかに大きいわけですね。ですから、ちょっとした法体系のリラクゼーションというものの以前に、もっと根源的な、自由度がとれるような、方策こそが必要なのではないかなというのを最近強く感じる次第です。

それから 2 番目は、そこに幾つか事例がありまして、自動走行、ドローン、電波、健康医療みたいなものあるのですけれども、これがどのようにして決まったかわからないですけれども、もっと根源的に、今一番はち切れそうなのはやはりエデュケーションのような気がするのですね。こういうものは個人情報にも関連しますし、著作権法にも関連しますし、非常にホットなのですけれども、これだけ少子化が進むだけでいかに有能な子供たちを未来に向けて育てていくかというのはぜひお考えいただければありがたいのと、もう一つは、今回の鬼怒川でもそうですけれども、圧倒的に早くディザスターリカバリーが我が国はできているのですが、あれはもう完璧に商売になる話ですので、そういうものがやや抜けていて、自動走行とかドローンとか、誰でも考えるようなことが出ている、というまた怒られてしまうのですけれども、もうちょっと違うところの目線もあつたほうがいいのかと思います。

それから最後に、1 2 ページに I T 人材育成についての記載がございますけれども、実は日本学術会議では情報学委員会で学部学生の IT 教育という観点で参照基準というのを今決めているのですけれども、資料にどのように必要なスキルをもつ人材を確保していくのかというのが書かれているのですけれども、そもそも必要なスキルって一体何なのかというところがやはりまず指針として必要になってくると思うのですね。これがサプライサイドの大学サイドとデマンドとしての企業サイドが欲しいスキル——スキルとっていいかどうかかわからないのですけれども、その辺が若干マッチしてないところが、我が国にとってみたときの不具合感が出ているのかなという気がしまして、そもそもどういう人材が欲しいのかというところの根底的なコミュニケーションをアカデミアと産業界で何かうまくできればありがたいなと思ってまして、今からちょうどアブループしていくフェーズでもありますので、ぜひそういう場をもっていただければ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。

それでは、水嶋さん、お願いします。

○水嶋委員

今回の I o T 推進コンソーシアム、I o T 推進ラボが設立されたというのは非常に意義があると思いますので、我々、J E I T A のほうも一生懸命参加させていただきたいと思っています。

そんな中で、7 ページのところに、「I T を活用して円滑に情報を共有・利用する制度整備」という形で挙がっております。その中に公益目的をという要件がございますが、これをあまり限定的に運用してしまいますと本来のデータの利活用という目的が逆に制限されてしまいます。従いまして、できるだけ要件を工夫していただいて、広く本当にデータ活用できる実体感のある制度に仕上げさせていただきたいと存じます。

更に、ご検討頂いているような事例に加え、医療情報等では本人を特定した情報を収集・提供する必要が出てくると思いますので、そのような場合の利活用の促進についてもお考え願いたいと存じます。また、是非ともスピーディー感をもって法整備をすすめていただきたいと思います。2 番目は、先日、欧州議会国際貿易委員会のラング委員長とお話をさせていただく機会がございました。今、E U と日本の間では、情報の流通に関して制約がありますが、データの利活用の推進をすすめていこうとすると、国境を越えたデータの利活用という目線が必要になってくるだろうと思っています。これは国と国との政府間での解決が非常に重要となってまいりますので、せつかく I o T の推進ラボが国際的にオープンな組織でございますので、この辺、本当に国際間の国を越えたデータの利活用という観点での方針を今後しっかりと定めていただきたい。特に先進国だけでなく東南アジア諸国も含めて政府間の協議をしっかりと進めていただきたいと思います。

最後に、今回の資料の中にはないのですが、オープンソース、あるいは組込みも含めた各種ソフトウェアを今後はこういう取組の中で組み合わせて活用していくことになっていきますので、例えばインタフェースの標準化とか動作性等を評価できるような何か共通の基盤というものも必要ではないかと考えております。次のステップになるのでしょうけれども、ご検討いただければと考えております。

いずれにしても、スピードが大事ですので、非常に疑心暗鬼に手探りで進めるということから、できるだけ早く、我々の基準となるような枠組みを決めていただいて進めさせていただいたらと思っています。

以上です。

○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

10ページのソフトウェア脆弱性情報の公表関連の話なのですが、ちょっとよくわからないのは、「法令に基づく適切な方法・手順に則り、その社会的影響に応じ、脆弱性の情報を公表する制度」というのですが、その制度に従うのは誰なのかというあたりについては、今現状ではどのようにお考えなのでしょうか。つまり、世界中でいろんな人がいろんな活動をしていて、どんどん勝手に脆弱性が公表されてしまう状況の中で、どのようにして健全化を図るかという課題があるのはよくわかるのですが、どうされようとしているのかということをご質問したいのですが、いかがでしょうか。

○渡邊課長

現状は法律に基づく制度ではなくて、通達に基づく制度ということになっております。基本的にはプログラムを開発した人が同意をしないと公表しないという制度になっています。

ただ、現実問題としては、なかなか同意がとれないケースや、そもそもその開発者に連絡がとれないケースがありまして、ただ、そういう場合であっても、放置しておくリスクがどんどん高まる場合があります。したがって、放置した場合と放置しなかった場合、どちらがリスクが大きいのか、国民にとってマイナスダメージが大きいのかということの評価、比較考量して、それで公表するかどうかを決めるという制度を法令に基づいてやりたいという話です。

○松本委員

わかりました。そうすると、現在、IPAがヘッドクォーターになって回している制度に関して、それをより実効ある形にしていきたいというようなタイプの事柄なのですね。

ただ、そこを手直すること自体は意義があると思うのですが、もうちょっと広く捉えないと焼け石に水的な感じのところがあるかなとは思っております。その辺、非常に難しいのですが、つまり、ある種、まじめに届け出がなされたら、それを評価して、関係者に連絡をとって、対策がとられたら開示するというようなものを組織的に行うというアクティビティは非常にいいと思うのですが、そこに参画している人はどのぐらいの割合なのかなあと。世の中でそういう脆弱性を発見したりした場合に、どのぐらいの方がそこに行って、その制度があっ

たことによってどのぐらい健全に世の中が回ってきたのかというあたりがなかなか難しいなとは思っております。どうすればいいかという意見をもっているわけではないですが。

以上です。

○村井委員長

ただ、これは本日の意思決定の一項目なので、今の点、もう少しわかりやすく説明していただいたほうがいいかなと思います。今、松本先生がご指摘いただいた部分を含めて、今までの状況をご存じでない方もいらっしゃるので、今までの状況と、これからどのようになるのかということをお願いします。

○渡邊課長

現状を申し上げますと、実はプログラムの脆弱性の多くは、開発事業者が自ら気づいて、自ら修正し、公表するのが一般的です。ただ、そうではない例が、過去10年間で二千数百件ほど、IPAに通報が寄せられております。そのうち、開発者が見つかり、開発者に修正の依頼の対応をして、解決した例が1,000件ほどあります。つまり、積み残しているものが1,000件ほどあるということです。今後、この1,000件の中でも、粘り強く交渉を続けていけば、何件かは公表できるようになるかもしれません。

他方で、今、開発者に連絡とれてないケースというのが200件弱ありまして、これについては、現在の制度では恐らく公表できずに、そのまま置いておかれるということになると思います。そこにもし重大なリスクがあれば問題ですので、その公表ができないかという、メインはそういう話になります。

ただ、今一度申し上げますが、同意がとれなかったら何でも公表するわけではなくて、要は、対策がとられてないのに脆弱性だけを公表するというのはかえって危ないケースが考えられますから、公表する場合としない場合とどちらがリスクが大きいかということ、専門家も交えてその場で比較考量して、評価をして公表するという形をとろうと思っています。

それから開発者の多くは海外にいるということを踏まえて、海外でも同様の取組をやっている機関がありますので、そういう機関との横の連携も考えていきたいということでもあります。

いずれにしても、今までは通達に基づいてIPAが独自にやっていたという部分もあるのですけれども、これからもう少し法律に基づいてきちんと、どのように公表するかしないか等をきちんと決めていきたいと思っております。専門家を交えて検討していくということは今までと同じですけれども、引き続き、より詳細に検討していきたいと考えています。

○村井委員長

もし違ったら課長のほうで補足していただくとして、私の理解では、実質的に開発者が直していく場合、例えば I P A に通報が来て、開発者に連絡が行き、直すというルートがあるのですけれども、セキュリティに関心のある人が自主的に穴を発見して、I P A に報告するというのはいいことなのですよ。その脆弱性を利用して悪いことするよりは。そういった意味で、ホワイトハッカーまでいかないですけれども、発見したらすぐに運用している人、或いは I P A に報告するという、いわば正義感で行動する人が最近ふえていて、I P A にもそういう人が沢山集まってきている状況があります。

ただ、I P A には非常に多岐にわたるソフトウェアに関する報告が集まってくるため、対応がスムーズにいかない場合もあります。なぜならば、開発者が大手のソフトウェアベンダー等に限られないからです。脆弱性情報の公表というのは、同じソフトウェアもっている人がどのようにして安全なオペレーションができるようにサポートができるかということにつなげていくためのものですので、この橋渡しをやっていけるような体制をきちんと整えることが必要です。私はこのように理解していますけれども、大体それでよろしいですか。

○松本委員

現状の今の問題点を解決するために、法令に基づいて新しくバージョンアップすること自体は非常に好ましいことだと私も思います。ただ、そこに、例えば I P A に連絡していたのだけれども、最近はしたくなくなつたという人たちもいるということは事実で。つまり、お蔵入りしてしまうから。まじめにやればやるほど、連絡がとれないとかいうことであつたり、あるいは案件が非常に難しくてなかなか対応してもらえないということになつてしまうと、せっかちな人が多いものですから、勝手に公表してしまうという方向に行つてしまつてはいけませんので、その辺、うまい仕組みをつくらないといけないのかなと思います。

以上です。

○村井委員長

わかりました。そうすると、課題としては一緒ですよ。

○松本委員

はい。課題としては。あと、世界的にたくさんいるので、I P A に通報といいますか、届け出してこない人のほうが圧倒的に多いわけですよ。

○村井委員長

ありがとうございます。

それでは、野原さん、お待たせしました。

○野原委員

2点あって、1点、質問なのですけれども、7ページにある代理機関のイメージについて、もう少し具体的なイメージを教えてくださいということなのですが、例えばシェアリングエコノミーを重ねると、例えば民泊をマッチングするようなマーケットプレイスを運営するような事業者は認可制にしましょうとかということがいわれているわけですね。ウーバーのような白タク的なプラットフォームを行う事業者は認定した事業者しかできないようにしようということのかなと思いつながりていたのですけれども、この場合、代理機関はどこまでをそういう認可しなくてはいけない対象として考えるのかとか、あるいはそのときの条件というのは何なのかというあたりで、先ほど、公的も公益目的でなくてもという話があったのですが、ここが広がるということはむしろ許認可の制度が厚くなっていくことのような気がして、むしろなくてもできるような範囲ができればそれはそれでいいのかなという気もするのですけれども、そのあたりの趣旨と範囲についてちょっと教えていただきたいと思えます。

○佐野課長

7ページの資料につきまして、紛らわしくて申し訳ありませんでした。内閣官房のIT室で検討しているシェアリングエコノミーの内容と、代理機関とはまた別の制度でありまして、代理機関のほうは個人情報に関するものであり、シェアリングエコノミーはまた別の制度でございます。今検討している方向性としては、例えばAirbnb（エアビーアンドビー）のような民泊のプラットフォームに一定の規制といいますか、届け出等をかけるかわりに、その下に連なっている各個人について、通常は許認可をとらなくてはいけないのですが、その規制緩和とセットで検討しているということでもあります。規制としては変わらないのですが、トータルでプラットフォーム側がある程度責任を負うことによって、その連なる個人の手続作業が緩和されるような、方向で検討しているということでもあります。

○野原委員

そうかなとも思いつつ聞いたのですけれども、ということは、代理機関が範囲とする、どういうときにこの代理機関が動くのかという、対象事例が幾つか書いてあって、確かにとても機密情報を扱わなくてはいけないとか、あるいは何社も出てくるというよりは、代表してそういうことをやってほしいというような事業については拳がっているようにもみえるのですけれども、それをどのように考えると思えばいいのでしょうか。

○佐野課長

代理機関については、例として、医療情報がございまして、複数の医療機関でもっている医療データをこの代理機関に提供して、情報集約して、そこでビッグデータ分析をしていくことが検討されています。

それから2つ目、想定されているものとしては、7ページの「対象事例」にも書いてありますけれども、自動運转向けに走行画像を各社が撮っているものを1カ所に集めて、ビッグデータ分析をして、人工知能のアルゴリズムの精度を上げていくような研究開発を行うとかいうものが想定されております。

○野原委員

今既にそういう関連の事業者っていて、開発をどんどん続けているわけですが、今はもちろんそういうことは関係なく自由にできると思うのですが、それはある時点で認可を受けないとそういう関連の開発ができなくなるということでしょうか。

○佐野課長

この資料にまだ明確に書いていないのですが、今検討されていますのは、個人情報情報を第三者に提供するときには、原則、同意をとらなくてはなりません。しかし、現実問題、なかなか同意をとることは難しい場合がございます。したがって、単に規制強化というよりは、代理機関にデータを提供するときには、その同意をとらなくてはいけない規制をある程度緩和することが必要ではないかというようなことで検討されております。その段階は規制緩和ということになると思います。

○村井委員長

ありがとうございました。この件は、さきほど、喜連川先生や水嶋さんがおっしゃったことと関連があるかと思えます。つまり、データを使わせるためにルールをつくるということなのです。ルールをつくってしまえば使えるだろうというのは、近ごろ始まったある制度のやり方に少し似ているところがありますよね。つまり、進めるためにルールをつくる。ルールをつくと、それに縛られることはないのかというのが、水嶋さんがさきほどおっしゃったようなお話で、それから、そもそも進めるために自由度を失ってはいけないというのが喜連川先生がおっしゃった部分だと思います。

皆さんが心配されているのはその部分かなと思います。7ページに書いてあるやり方は、あまりに前に進まないで、政府がお墨付きを与えるメカニズムで推進させましょうという考え方に、哲学的には近いのではないかと思います。そうすると、そのやり方の洗練度が低ければ、おっしゃったような、使いにくいとか、結局やりにくいということが起こってしまわないかという心配も出てくると、こういうあたりがポイントかと思えます。

この件は内閣官房で進められていますが、今ここでこうやって紹介していただいたということは、経産省の政策の中での責任がやはりあるとお考えいただいていると思います。ルールづくりには洗練度があって、新しいものが生まれてきたときの自由度の確保や、喜連川先生はリアクティブという言葉でおっしゃいましたけれども、新しいことがどんどん起こってきたときに、あらかじめリスクを予想してとめるということを繰り返していると、時にはそれが新しいものを生み出すことの障害になるのではないかといった懸念もありますので、そのあたりが洗練されたものになるということは、ぜひ経産省もかかわって検討していただくというのがいいのではないかと私は思いました。

○野原委員

今のことに関連して、そのあたりがもう少し何か意図が伝わるような書き方をする必要はあるのかなあと。これだとよく分からないという気もしまして、ちょっと質問という形で明確にできればなと思いました。それは先ほどの、IT戦略室との役割分担ということ以前に、そもそもこの代理機関の位置づけというか、何のために存在して、それがどういうことをなし遂げたいと思っているかという、この代理機関がある事業者を認可することによって個人が情報を出しやすくするというのをいっているわけですよね。普通だと抵抗があるかもしれない情報を。

○村井委員長

両方でしょうね。出すほうも安心して出せる、なぜならお墨つきがついている、こういうメカニズムですから。そして、使うほうも安心して使える、こういうことだと思います。

○野原委員

確かに、どうやって書くかと考えるとそれはそれで難しいなという気もするのですが、もう少し、何かこのページに書いてあることというのはわかりやすくする必要はあるのかなという気がします。

以上です。

○佐野課長

まだ検討中の段階でございまして、少し曖昧な書き方になってしまったのですが、おっしゃったように、データを収集して分析するのはもちろん自由なので、認定は必ず受けなければいけないということにはならないということでもあります。ただ、認定を受けるとある種のお墨つき効果のようなものがあって、データが集めやすくなるということが1つと、あと、データを実際に集めようとしたときに、同意をとらなければいけないという

手続が厳しいときに、そこを一部緩和する措置を講じようというのがこの今検討しているコンセプトということになります。おっしゃったように、当然、規制強化にはつながらないような形でしっかり取り組んでいきたいと思っています。

○村井委員長

三輪さん、お待たせしました。

○三輪委員

三輪です。よろしくお願いします。

8ページ以降に、セキュリティの話題がありますが、きょうの時点で何かいっても間に合わない感じはあるのですが、I o Tにおけるセキュリティというのは、先ほど、例えばクライスラーの例とか出されましたけれども、例えば車の中に積まれている膨大なコンピュータネットワークに関する脆弱性に対する問題については、メーカーさんと一言でいっても、実際には車メーカーだけでなく、その配線、ネットワークをやっているメーカー、チップをつくっているメーカー等、多くの会社に関与しております。そういったいろんなところのベンダーがつくったものが組み合わさって、自動車一台ができあがりますよね。

I o Tというのは今後進んでいくなかで、これと同じようなことが、例えば、私もちょっとかかっていますが、スマートメーターなんかもそうですし、軒下にIPアドレス振られて通信をしたりするわけですよね。そういったものに対するセキュリティというのは、技術的なものというのをもっと深くやはり追求する必要があると思っています、つくる側がきちんとつくりましょう、あるいはつくりなさいという枠組みがそもそもあり、でも、本当にできているか調べる第三者機関というのがあり、そのようにしていかないと、今のインターネットの世界だと、今のサーバとかソフトウェアの世界だと、さっきの脆弱性届け出制度みたいなもので、あとバグハンターというのがいて、それで生業立てている人がいたりとかいう世界でなんか回りそうな気もするのですが、自動車であるとか、例えばドローンが乗っ取られるであるとか、そのようなもの、医療情報なんかも、この話題では、厚労省でないのであれですけれども、もっと技術的にどんどん深く追求していく必要がともあると思っています、今のままだと、利活用のところについては非常に具体的にパワフルに進んでいるのですが、セキュリティは、例えば、それぞれの施策については、私もこれは大抵かかっているのを否定するものでももちろんないですけれども、I o T社会のセキュリティということになると、もっと技術的な面、例えば脆弱性は届け出ではだめで、もっと積極的に検査、あるいは発見する仕組みというのは必要ですし、そのあたりはIPAという組織としてできる仕組みに多分なっていないと思いますので、そういったものを、特にただ機関だけつくってもだめだと思いますので、当然、産学連携で英知を集中して、実際、スマートメーターはそのようにやろうとい



うことで動いてはいるのですが、そういった取組がこの施策の中にどれかあるといいなあとちょっと思ったのと、最後に、12ページに人材の調査というので、ここにまたセキュリティ人材も調べると書いているので、一応簡単にちょっと釘を刺しておく、これは関係者の人には何百回とっているのですが、セキュリティ人材は足りてますかと経営者に聞くと、セキュリティは、いや、足りてないなどと答えます。その数を数えたら20万人です。これはよくある話なのですからけれども、でも、その後、「雇いますか」という質問をすると、誰も雇うとわかないという。だから、不足してないのですよね。

そのこと自体が問題なのだというので、サイバーセキュリティ経営ガイドラインとかが出てきているのですが、アンケートのときにはぜひ、先ほど冒頭、どなたかご質問でおっしゃっていましたが、足りない人材の類型化をしっかり行って、セキュリティ人材というのは経営者にちゃんともの申して、予算を分捕ってくる人もセキュリティ人材だとももちろん思いますし、技術的にすごい方々もそうですし、もともとSE屋がしっかりしてないと話にならないので、そのあたりもそうですし、いろんなところにセキュリティを高める人材が必要なのわけですからけれども、その類型化をせずに、単にセキュリティ人材足りていますかとか、ホワイトハッカーいるよねとか、そういう議論にまた戻らないように、ぜひアンケートするときには分類をちゃんと行って、それから採用する気があるのかということもあわせて聞い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。大変重要な点だと思いました。

では、澤谷さん。

○澤谷委員

データ利活用の価値を受容する者としての観点で3つ申し上げます。

2ページ目にありますI o Tコンソーシアムでは、外資を含む多くの企業が入っているということですが、この中にも受容者であるユーザーが加わる必要があるではないでしょうか。特にシェアリングエコノミーを目指した新しいサービスをつくっていく場合にはユーザーの意見を酌み取る仕組みが必要だと思います。その一つがI o T推進ラボなのかと思いますが、このあたりにうまく、アメリカ・ヨーロッパ等の先進事例や地域の新しいサービスを取り込むような仕組みがあるといいと思います。

次に7ページの代理機関について、今までのご議論では公益的なサービスに対するデータを集める役目をなすということとなっています。それとともに、もう一方の考え方としては、個人のデータを個人が主体となり活用する方法もあると思います。色々な形態のビジネスが今後出てくることが考えられますので、制

度で規定される内容が明確に書かれ、想定外のビジネスが排除されないようにすることが重要だと思います。

最後に人材の12ページのITスキルについて、今後ますます重要になってくると思われます。今まで会社・オフィスの中で使われていたITが、家でも、地域コミュニティでも使われ、ITがないのと使うのでは全く生産性が変わってくるということを考えると、使えるIT技術者を育てていくことが必要だと思います。

例えば、Make Universityが行っているように企業のエンジニアを積極的に教員として迎えて実践的なスキルをつけるような仕組みも必要だと思います。そのときには、今まである文部科学省制度の教員資格等を含め、IT人材・それを育てる人材に関して検討も考えていただければと思います。

以上です。

○村井委員長

ありがとうございます。

それでは、唯根さん、お願いします。

○唯根委員

ありがとうございます。

もう三輪委員からもご意見として出たのですが、12ページについて私も1点だけ。IT人材については、利用者、国民全てがIT人材と言えるので、最低限必要なスキルというのはどこまでなのか、生まれたときからITに触れている子供たちに、どこまでが自分自身で守らなければいけないセキュリティの分野なのか、少なくともそれがわかるようなところはぜひ示していただきたいと思います。それでないと消費者教育も行えないという状況です。お願いいたします。

○村井委員長

どうぞ、西川さん、お願いします。

○西川委員

2点ほど。

まず、前半部分のIoT推進のところなのですが、日本が世界に先駆けて社会変革を起こすところがあるのですが、このどういう分野を支援するのか、どういう分野に注力するのかというのは、

日本が本当に勝てる領域にきちんとフォーカスすべきなのかなとは思いますが。

例えば、先週、ロボットの展示会がビッグサイトであったのですが、私もそこにファナックと一緒にブースを出していたのですが、日本の人もそれなりに訪れることは訪れるのですが、どちらかというと海外の競合がかなり来ていて、ほかに、私自身、I Tの展示会とか出して、そういうことって余りない。ロボットの分野というのは本当に世界中が日本の技術に注目しているところなど、その強みというのは、日本が強い、勝てる領域というのはいろいろあると思うので、そういうところをきちんと選定していく必要があるのかなと。若干、自動運転だとカドローンというのは北米が先行している点というのはあるのかなと思うので、要は規制緩和やルールの整備だけではなくて、技術的にも勝てる領域というのを選んでいかないと、きちんと勝ち抜くことはできないのかなと思います。

もう一点、セキュリティの部分なのですが、これは、今、人が何とかするという視点であると思うのですが、これがI o Tと混ざってくると、先ほどのお話にもありましたように、要はサイバーの空間だけに閉じなくなっていくと。これからセキュリティの主戦場というのは間違いなくI o Tの領域になっていくと考えると、どうやってその仕組みとしてセキュリティを担保していくのかというのをきちんと考えていかないといけないのかなと。

例えば自動車の領域とかいうのは、恐らく個々の車だけのセキュリティを高めてもだめで、車同士がうまく協調して何かテロに近いことを起こしてしまうとか、そういうことが起こり得ると、インフラとも協調していかないといけない。そうすると、個々の会社だけで対応するというのは無理で、そのような仕組みを国が支援するという事は必要になってくるのかなと思います。

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

今の西川さんのご意見と大分重なるのですが、I o T推進ラボで実施するプロジェクトは、やはり日本が強みを発揮できるもの、ダントツにこれは日本だと思えるような技術や応用分野が含まれるといいなと思っています。そういう観点から、私もロボットに注目しています。フィンランドにゼンロボティクスという会社があります。ロボットとA Iを組み合わせる産業廃棄物の分別を行うシステムを開発・販売しているのですが、同社にヒアリングする機会がありました。そこでうかがったのは、欧米ではロボットといえば人間の雇用が失われるというイメージがとても強く、まずそこが議論になるのだけれど、日本はそうではない、ロボットに関し

て抵抗がなくウェルカムな市場であるという点で世界でも珍しい国だということです。同社はすでに日本市場にも進出していて、第1号機の納入も決まったそうです。一方、日本の技術、とくに筋力が衰えた人をサポートするロボットスーツは海外からも注目されています。日本は、ロボット開発の技術力だけでなく、その応用に関する考え方でも世界に発信していけるものをもっているのではないかと思います。その強みを生かすということを考える必要があると思います。

また、喜連川先生がおっしゃったように、災害対策であるとか環境問題であるとか、日本が強い分野の中で何か出てくるとおもしろいかなと思っております。応用分野については、早く実用化できる分野の見極めという視点も大切です。例えば、自動運転車の開発は人命に関わりますので、エラーをできるだけなくし、技術の精度を高める必要があるでしょう。それに対して、先ほど紹介したゴミの分別のようなものであれば、100%完璧なシステムではなく多少エラーが生じたとしても大した問題ではありません。むしろ早く実用化したほうが社会的利益は大きいとも言えます。防災、環境といった日本が得意とする分野で、精度をそれほど高めなくてもすぐに実用化にもっていけるものを考えるということは重要であると考えます。

最後にもう一点なのですが、これは澤谷さんおっしゃったのですけれども、個人のデータを個人がもつことの可能性について、私ももっと考えたほうが良いような気がしています。フィンテックのような銀行とか証券とか、いろんなところと取引しているデータを自分をもって第三者の会社に助言をもらうとか、いろいろな発展がヘルス分野でもあるかもしれません。そこはさらに検討すべき課題と思っています。

以上です。

#### ○村井委員長

ありがとうございます。

皆様に、大変貴重なご意見、ご指摘をいただきました。さきほどのレギュレーションの件はありましたけれども、砂田さんと喜連川さんがご指摘された、災害からのリカバリー等、日本が本当に強い領域で、IoTあるいはデータをうまく利用していくということも大変重要な使命だと感じました。そこはほかの国にはまねできないようなことがあるかと思います。それから、喜連川先生がおっしゃっていましたが、セキュリティ人材について、産学で認識がマッチしていないということは、三輪さんにおっしゃっていただいている人材の、「不足しているの？」という、必ず不足しているというけれども、じゃあ「雇うの？」という雇わないと、こういう話とも関係があって、それをとても大事なポイントとして考えているわけです。その産学のマッチしていないことをマッチさせるような議論する場所があるのかとか、そういうこともご指摘いただきましたので、それに関しては、議論がきちんとできる体制はつくっていただけるのではないかと思いますので、そのこともぜひ進めることができるのではないかと思います。

それから、推進ラボの会議には色々な方が参加されているので、国際的なデータがどうやって国境を越えて利用できるのか。これも水嶋さんからご指摘あったと思いますけれども、そのようなことも、どこまでができて、できないのか。今、データローカライゼーションという、国の中に納めなければいけないという議論が世界のあちこちで出ておりますが、一方では、そのデータの適正な利用ということに関しては、それに対するやみくもなルールができるというのもこれは課題になっていますので、この解決に取り組まなければいけないということでございます。

もう一つは、セキュリティの件で、最初に夏野さんについていただいたのですが、どういう教育をするのか、どういう資格をとるのか。資格にしていくというのはかなり踏み込んだ話で、以前の会議で三輪さんがそういうことをおっしゃったので、それに関して動いていくのは大事ですけれども、少なくとも本当に必要な人材がどのようにできてくるのかということをはきちんと定義しなければいけないだろうということがあります。

それから、私がもう一点気がついたのは、三輪さんのおっしゃった I o T の、技術的には複雑になっているが、だんだんインターネットにつながっているものが通信するようになってきているという点について、これは私も少し実感があります。I o T が始まったころはそれぞれのやつが T C P / I P を使わなくても、ローカルなところで分離されていればいいというので結構議論が進んでいたのですが、今はエンドシステムまでインターネットにつながってくるというモデルが多くなってきている。

一方では、頼りないハードウェアというのがあり、暗号化の機能などが省かれるおそれもあるわけです。そのあたりを含めてご指摘の点があったと思うのですが、これはやはり基準をつくらなければいけない。評価基準のようなものをつくっていくというのはどこでも大事なことで、企業そのものの評価基準もつくらなければいけないし、今ご指摘があったようなハードウェアとか、つながってくるものの評価基準もつくらなければいけないのですが、基準やクライテリアをつくるというのは、産官学が一緒になって行なうべきと、かなりコストの高いプロセスなのです。基準を議論して決めていく、あるいは評価基準や物差し、インデックスを決めていくというのは、

アメリカの状況を見てみると、新しいことが起こってくると、それが何であるかを見極めるための、やはり調査研究みたいなことに予算がついていて、それで基準をつくっています。I o T 関連で、各省庁を見てみると、例えば経済効果はどうなるのか、どういうところが変わるのかというのは、みんな海外のデータをもってくるのです。それから、シンクタンクでつくられたデータをもってきて、役所のデータとして、それに基づいて、だから進めるといってしまう。

これはやはり国として非常におかしくて、データをこの国で取り、そのデータに基づいた基準があり、それに対して、この基準を満たしているか、日本はほかの国よりもすぐれているか等の判断やレーティングができるようになる。この基準づくりにコストをかけていないのです。これはこの国の行政の特徴だと思います。評価

軸に対する投資。こういうのはいつもそう思っていたのですけれども、1つ三輪さんをお願いしたいのは、スマートメーターができてくると、その横展開のようなことができるかもしれません。そうだとすると、この問題に非常に有効ではないかと思います。そのほかにも実は重要な鍵はI o Tにあるのです。データを使うためにガイドラインをつくり、そのデータの匿名化プロセスをつくり、それに従って有効にデータが使えるねという研究や実験は沢山されているのですから、それを今度は外に出してほかの分野で使えるようにするというのはいかがでしょうか、そのあたりの評価基準づくりというのも大変重要ではないかと思いました。貴重なご意見、ありがとうございました。

それでは、発言していただいている有野さんをお願いしていいですか。

○有野委員

はい。ありがとうございます。

1点だけちょっと質問させていただきたいのですが、11ページのサイバーセキュリティ経営ガイドラインですけれども、サイバー攻撃リスクは経営課題でもありますし、我々にとってもリスク、労働組合としてもその認識は必要だと思っているのですが、我々も経営サイドといろんな話を進める中でこの視点を大事にしたいと思うのですが、ガイドラインが、今、パブコメ中だというお話がありましたけれども、期限的にはどれぐらいを目指して発表されようとしているのか。あと発表の仕方、決めているのであればちょっと教えていただきたいなという2点でございます。

○瓜生室長

ガイドラインですけれども、12月1日から2週間程度でパブコメの期間をとっておりまして、その後、パブコメの中身を分析した結果を踏まえまして、年内には公表という形でやりたいと思います。あくまでガイドラインですので、強制ではなくて、ガイドライン。公表する形で実際使っていただくということを想定しております。

○村井委員長

よろしいでしょうか。

どうもありがとうございます。それでは、本日の議題は、サイバーセキュリティに関する法制度の2つの点でございますので、今の議論をもちましてこちらに関してはご了承いただいで進めさせていただくことよろしいでしょうか。

(「異議なし」の声あり)

それでは、ご指摘のことを踏まえて進めていただきたいと思います。

それでは続きまして、その他の議題ということで、事務局から資料3と参考資料に基づいて、試験ワーキンググループの設立、及び、IT利活用ビジネスに関するルール整備WG、今後の方針という説明をお願いいたします。

○佐野課長

資料3をご覧くださいと思います。「試験ワーキンググループの設置について」というペーパーでございます。この情報経済小委員会の下には、後ほど出てきますIT利活用のルール整備WGと、それからIT人材WG、2つこれまでございましたけれども、これに加えて、新しい試験ワーキンググループというものを新たに設置したいという議案でございます。

長々書いておりますけれども、要すれば、これまで人材WGの中で、今回のこの法案、法制度の中身の一つであります国家資格制度を検討してきたところでございますけれども、今後、この国家資格制度について具体的にどういった形で試験を実施していくのか、試験の内容などにつきまして実務的な検討を行う必要がございます。そのために必要とされる専門性も少し異なるものですから、別途、WGを立ち上げたいということでございます。

今後の予定ということで、年度内をめどといたしまして、3～4回程度審議を行いたいと考えております。

28年度以降につきましては、引き続き、この情報経済小委員会などの検討結果を踏まえて、また必要な検討を行っていきたいと考えてございますけれども、まずはこの試験ワーキンググループを設置したいということでございます。

続きまして参考資料をご覧ください。この情報経済小委員会の下にIT利活用ビジネスに関するルール整備WG、従来からございましたけれども、電子商取引等の準則というものがございますけれども、これは毎年、このWGを開いて改訂の検討を行っているところでございまして、今年度も12月11日にそのルール整備WGを開きまして、2月に開いて、パブリックコメントを経て、春に改訂版の電子商取引の準則というのを定めていきたいと考えてございます。

私からは以上でございます。

○村井委員長

それでは、今のご説明に関して何かご質問、ご意見等ありますでしょうか。

それでは、本日の議題は以上ということでございますけれども、私から1点実はありまして、本日も説明いただいたことは大変重要なことでございまして、また、さきほど松本委員からご質問があったような、例えばIPAの制度に関するご説明等については、委員の方もお忙しいのだけれども、もう少し前提となる状況

をわかった上で議論したほうがいいのではないかという印象を少しもっていますので、私自身の責任も重々感じておりますけれども、運び方として、ほかの省庁との関係もあると思うのですけれども、ぜひ十分なお説明もお願いして進めていただきたいなと思いましたが、よろしくお願いします。

それでは、安藤局長からご挨拶をお願いしたいと思います。

#### ○安藤局長

ちょっと遅れて来まして、大変失礼いたしました。

皆様方、本当に熱心にご議論いただきまして、次の通常国会目指して、今ご説明したような法案をしっかり仕上げたいと思っております。ただ、具体的な制度は、今のお話にあるように、例えば試験制度1つとりましても、これからまさに皆様方のご知見を生かしてつくっていかねばいけないということであります。

せっかくですので、個別に出たお話について私見を申し上げると、セキュリティの試験制度についてもっと格好いい名前にすると。これはもうおっしゃるとおりでありまして、ぜひ皆様方も、候補をいただければ幸いです。併せて英語表記も行い、世界に通じる名称にしていきたいと思っております。

それと、一体どういうレイヤーの技術者を狙っていくのかというそこについては、先ほどの夏野さんのお言葉をおかりすれば、後者を狙っていきます。それと関連して三輪さんのお話、あるいは喜連川さんのお話にもありましたけれども、人材の話は抽象的な議論をするつもりはありません。具体的に、どういったスペックの人間がどれぐらいのボリュームで、何年までに必要となるか、ということを検討してまいります。

ただし、その後は、行政だけでできる話ではなくて、いわば社会経済システムの中に消化していかねばなりません。ガイドライン一本つくればそれで問題が解決できるわけではないと思っておりますので、さまざまな手段で、例えば、産業ごと、あるいは企業ごとに、あるべき体制検討し、さらに、このセキュリティのエキスパート試験に合格した人を何人ぐらい配置すべきとことがわかるようなものにしていきたいと思っております。

そういう意味で、経営ガイドラインはかなり中身が抽象的でありますけれども、これは誰に向けてガイドラインとして発出させていくのかということが大事だと思っております。これはまさに、技術的な内容ではなくて、経営者の皆さんにこの問題を最低限考えていただきたい、まさに経営としてのサイバーセキュリティということをご認識いただくようなものにしていきたいと思っております。

それと、IoT推進ラボの扱うテーマ、先ほどごらんいただきましたもの、あれはこの一例でございます。まさに災害対応、あるいは保安、あるいは安全の確保、このようなところに日本のかなり強みがあると思っております。今後、年明け以降、具体的に選定させていただくプロジェクトについては、まさに日本発で世界に展開されるようなソリューションモデルを提供していけるようなものをぜひ選ばせていただきたいと思っております。



ます。そういう意味では、日本が直面している課題はむしろ地方が直面している課題でありますので、そういう意味で、地域発の世界へのソリューションモデルみたいなものが出てくると大変おもしろいと思っております。

先ほどの個人情報のところはなかなかお話しにくいテーマでありますので、村井先生も大変お気遣いいただきながらお話をされていたということであると思っておりますけれども、これまでは少なくとも、ご本人の同意が得られないと、およそ第三者機関というのが個人情報を扱えなかったという世界の中で、いかに大多数の方々に迷惑をおかけしないようにしながら少しでも進めていかなければいけないのかということの、いわば試みだのご理解いただければと思います。

ただ、村井先生が最後におっしゃられましたように、さまざまな検討状況について、途中経過や議論の経過を、今後機会があればぜひご提供させていただいて、ご議論いただくに当たって事前のインフォメーションをご提供させていただくようなご議論の仕方をお願いしたいと思っております。

と申し上げながら、一応この情報経済小委員会、5月にとりまとめていただいて、それで8月から再開していただいて、今回、きょうのご議論で一応の一くくりをさせていただければと思っております。ただ、釈迦に説法でございますが、課題はまだ山積しておりますし、課題が日進月歩でございますので、またいつでも、皆様方のご知見をおかりできれば幸いです。また、こういった公式の場ではなくても、私どもにご指導、ご鞭撻をいただければ幸いです。

それをこの場をおかりいたしましてお願い申し上げまして、簡単でございますけれども、御礼のご挨拶にえさせていただきます。どうもありがとうございました。

#### ○村井委員長

どうも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、5月のレポート、そして一旦の区切りということで本日を迎えましたので、委員長として私からも、皆さんに非常に大切な議論をしていただいたこと、心から感謝申し上げます。どうもありがとうございました。

それでは、本日の産業構造審議会商務流通情報分科会第7回の情報経済小委員会を閉会させていただきます。どうもありがとうございました。

——了——