

## 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10回）

### 議事録

日時：平成29年5月12日(金曜日)10:00～12:00

場所：経済産業省本館17階 第1特別会議室

議題：今後のIT政策の方向性について

○佐野情報経済課長 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10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、議事に先立ちまして資料の確認でございますけれども、本日もiPadを使用いたしまして、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たします。

本日の資料でございますけれども、議事次第をみていただくと書いてございますが、資料1が委員名簿、資料2が今後の情報政策の取り組みの方向性をまとめたもの、資料3が前回、前々回とご議論いただいた、IoTの面的展開の推進に向けての資料でございます。そのほか、参考資料を添付してございます。

iPadの不具合ですとか、資料が掲載されていないなど、問題がございましたら事務局までお声がけをいただければと思います。

本日は、おくれてこられる方はございますが、13名の委員にご出席いただく予定となっております。規定の過半数に達しているということでございます。石黒委員、國井委員、國領委員、西川委員、野原委員、松尾委員、東原委員は、ご都合によりご欠席となっております。

本日は、2名の方に代理出席いただいております。西川委員の代理としまして、株式会社Preferred Networksの丸山宏様。それから、東原委員の代理としまして、JEITAの常務理事の川上様にご出席を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 ありがとうございます。本日もよろしくお願いいたします。

それでは、本日は事務局から今後の情報政策の方向性、及びIoTの面的展開の推進に向けてという資料を用意していただいておりますので、これをご説明いただいて、皆様に

自由討議を行っていただくという運びになっておりますので、よろしくお願いいたします。

事務局の方、よろしくお願いいたします。

○佐野情報経済課長　それでは、資料2をごらんいただければと思います。今後の情報政策の取り組みの方向性を全体図をまとめたものでございまして、2ページ目をごらんいただきますと、目次でございまして、

3ページからが課題と今後の取り組みの方向性を整理してございますけれども、4ページをごらんいただければと思います。

まず、基本的な認識でございますけれども、I o Tの進展に向けて我が国が抱える課題ということで、これまで実証事業等行ってまいりましたが、いよいよ本格的な社会実装を進めていくフェーズへと移行していく段階にあるのではないかとございまして、

したがって、本格的な社会実装を進めていくために、データ流通の仕組みの構築、I o Tの実ビジネスへの実装、人材の問題、サイバーセキュリティの問題、それぞれについて新たな取り組みが求められているのではないかとございまして、

5ページ目をごらんいただきますと、今後の取り組みの方向性でございます。これまで基盤整備を中心に取り組んでまいりましたが、いよいよリアルなビジネスの展開を促進していくということで、I o T市場の創出ですとか新しいビジネス、面的普及にさらに力を入れていくとございまして、

6ページをごらんいただきますと、具体的な取り組みということで大きく3つに分けてございまして。1つ目はI o Tなリアルな社会実装を進めていくために、データ流通や利活用の環境整備をしていく、I o Tビジネスの面的展開を図っていく、新たな競争領域の担い手をしっかりと育成していく。大きな2つ目としては、サイバーセキュリティ対策の強化。3つ目としては、I T人材育成の強化でございます。

7ページをごらんいただきますと、こういった取り組みを進めるに当たりまして、Connected Industriesという旗印をもとに私どもは進めてまいりたいと思っております。ことしの3月にドイツでC e B I Tの展示会がございまして、日本企業から118の出展をいたしまして、総理、世耕大臣が出席いたしました。C e B I Tの場を通じまして、さまざまなものがつながり合って新しい付加価値を生み出していく産業のあり方として、Connected Industriesということで内外に発信しているところでございまして、

8ページ目をごらんいただきますと、Connected Industriesを通じて日本の勝ち筋をつくっていくということでございます。事業所、工場等、電子データ化が進んでおります

けれども、それぞればらばらに管理され連携されていないという中で、さまざまなものをつなげて課題解決を図っていく。事業所間、部門間、人とロボット、人と人、さまざまなものをつなげていき、技術革新、生産性向上、技能伝承などの課題解決を図っていき、これを日本の新しい強みにつなげていこうということでございます。

9 ページがConnected Industriesのコンセプトを整理したものでございます。下をみていただきますと、技術の変化として、第4次産業革命がございまして、これを受けて産業のあり方が変化してくるわけでございます。先ほど申し上げたようなさまざまなものがつながり合って新しい付加価値を生み出していき、従来独立、あるいは対立関係にあったものが融合して変化していき、新しいビジネスモデルが生まれてくる。こういう産業のあり方をConnected Industriesと定義しております。

こういった産業のあり方が、人間中心で課題解決をして、一番上にございますけれども、Society5.0、スマート社会につながっていくということでございます。

10ページから具体的な取り組みを整理したものでございまして、11ページ、まずIoTのリアルな社会実装に向けての取り組みということでございます。

12ページをごらんいただきますと、IoTのリアルな社会実装を進めていくために大きく3つございまして、データ流通の利活用の環境整備、面的展開、新たな競争領域の担い手がございます。

具体的に13ページからそれぞれについて整理してございます。まず、データ流通の利活用の環境整備でございます。

14ページをみていただきますと、ゴールイメージということで、企業、産業、国家の壁を越えてさまざまなデータを掛け合わせることで付加価値を出して、日本型の新たな連携の仕組みを実現していこうということです。

課題と対応の方向性は、その下に簡単に整理してございます。パーソナルデータについては、個人起点のデータ流通の仕組みを実現して、社会受容性を高めることで、パーソナルデータ活用を次の局面へつなげていこうということでございます。

企業が保有するさまざまなデータについては、各企業内でなかなか外に出ないこともございまして、これにつきましては、企業間の契約締結の促進を通じまして、データの連携を進めていこうということでございます。

3つ目でございます。データ取引を仲介するプラットフォームが登場しておりますけれども、プラットフォーム間の連携を図っていく必要があるということで、最低限共通で整

備する事項を整理して、データ取引市場を拡大していこうと。

国際的なデータ流通の円滑化でございます。日EUなどでの対話を継続しまして、必要な制度整備を推進していく。

公的データのオープン化でございます。官民の継続的な対話を通じまして、民間ニーズを踏まえて公共データ開放をしっかりと推進していく。

行政手続のIT化につきましては、デジタルデータのみで完了する手続を実現していこうというのが基本的な方向性でございます。

15ページがこれまでの取り組みとこれからの取り組みを工程表的に整理してございます。パーソナルデータの活用につきましては、匿名加工ガイドラインですとかカメラ画像のガイドブックの策定等を行ってまいりましたけれども、実証事業等を通じまして、個人起点のデータ流通を可能とする具体的なプロジェクトを生み出していこうということでございます。

事業者間のデータ流通につきましては、個別の企業のお悩み相談ということで、データ流通促進ワーキンググループの活動を通じて企業の懸念を解消していこうということでございます。先ほど申し上げたBtoBのデータの利用権限に関しましては、契約ガイドラインを5月いっぱい策定しまして、それを分野別に具体化して落とし込んでいこうということでございます。

データ取引市場間の連携でございます。データ流通プラットフォーム間の連携に関する基本的な事項を整理して既に公表してございます。これを実際に民間の取り組みに落とし込んで、取り組みを後押ししていこうということでございます。

国際流通は、その下の(5)となります。日EUの間では対話を継続しながら、国際的なデータフリーフローの実現につなげていこうということでございます。

下の(6)でございます。官民データ活用推進法に基づきます計画を策定しつつ、重点分野を指定して、オープンデータを図っていくということ。

行政手続の観点では、法人インフォメーションを構築しまして、これとベンチャー支援プラットフォームと連携していくことで、ワンスオンリーの手続を実現しようということで進めていこうということでございます。

16ページ以降に今申し上げたことを具体的に書いてございます。16ページが先ほど申し上げたPDSとか情報銀行の話、17ページが個別の事例の蓄積の話、18ページがデータ利用権限に関する契約ガイドラインの中身について書いてございます。19ページもそうです。

20ページがカメラ画像利活用ガイドブックの概要ということで、ご参考まででございます。

21ページがデータ流通プラットフォーム間のAPIによる相互連携の取り組みについて書いてございます。

22ページが国際的な越境移転、23ページが日EU間のジョイントプレスステートメントのポイントを書いております。

24ページからが公共データの開放についての取り組みを記載してございます。

25ページが具体的な事例ということで、JAXAが保有しています衛星データのオープン化を進めていこうという話、その次のページが行政機関がもっていますバイオデータをオープン化していくという話、その次が省エネ法に基づきますデータを使いやすい形で提供していこうということで、事例としてつけ合わせてございます。

28ページが法人インフォメーションとベンチャー支援プラットフォームを連携させまして、ワンスオンリーの手続につなげていこうという取り組みを書いております。

29ページからが2つ目のIoTビジネスの面的展開をどう促進していくかということを整理してございます。

30ページをみていただきますと、課題の整理ということで、徐々に新しいサービス、ビジネスモデルが登場してきておりますけれども、まだ実際の社会実装は十分に進んでいないということで、IoT推進ラボの取り組みを通じまして、さらなる先進的なビジネスの発掘を実証していく。

地域において、まだなかなか実装が進んでいないということでございますけれども、地方版IoT推進ラボの先進事例をさらに創出して横展開をしていく。

新しいビジネスモデルについては、既存の法制度でなかなか判断できないグレーゾーンがございまして、こういったグレーゾーンにつきましても、電子商取引の準則、グレーゾーン解消制度などを通じまして、新技術導入の足かせとなり得るような法解釈を明確化していくということでございます。

その下は、実証事業はなかなか社会実装に結びつくためのサイクルがまだ確立していないということでございまして、既に導入化になったソリューションにつきましても、さまざまな政府の制度に組み込んでいって面的な普及を促進していこうということで、これは後に資料3でご説明します。

31ページがそれらの取り組みの線表でございまして、IoT推進ラボについてはいろいろ

やってきておりますけれども、プロジェクトの発掘自体を課題解決型、コンテスト方式にシフトしていこうと考えてございます。

その下の(2)でございます。さまざまな実証を行っておりますが、その実証を通じて具体的なプロジェクトを創出、制度整備に向けた課題を抽出していくことを進めていくということでございます。

地域への展開でございます。地方版 I o T 推進ラボを通じました創出支援のほか、現在、国会に提案しております地域未来投資促進法案に基づいて、個別プロジェクトをしっかりと重点的に支援していくということでございます。

時代に即したルール整備ということで、電子商取引の準則を毎年度改定しておりますけれども、AIによる契約責任論ですとか、仮想通貨、ブロックチェーンをめぐる法的論点など、新しいテーマについてルール整備を検討していこうということでございます。

I o Tの面的展開としては、後ほど資料3でまたご説明します。

32ページからが今申し上げたことを具体的に書いてあるということでございます。32ページが I o T 推進ラボの話、33ページからは実証の話でございます。外国人のおもてなし実証事業、34ページが健康・医療データの実証事業の話、35ページがスマートホームの実証事業の話ということでございます。

36ページからが地方版 I o T 推進ラボの概要でございます。37ページからが具体的な地域の類型、38、39ページが具体的な事例で、40ページが先ほど申し上げた地域未来投資促進法案を通じました地域の I o T 実装推進でございます。

41ページが電子商取引準則によります新しい課題に対するルール整備についてまとめてございます。

42ページからが新しい競争領域の担い手をどう育成していくかということでございます。43ページをみていただきますと、今後、我が国の強みとなり得る新しい領域について、プレーヤーをどう育成していくかということでございます。

その課題と対応の方向性についてでございます。ブロックチェーン、実証実験等進んでおりますけれども、まだシステム導入は進んでいないということで、具体的な分野を特定しまして、必要なルール整備とあわせて実装を推進していく。

シェアリングエコノミーでございます。規制の問題等ございますが、地域でのシェアリングシティーの事例創出、グレーゾーン解消制度を通じた規制改革支援等を推進していこうということでございます。

まだクラウドの利活用が企業においても十分に進んでいないということで、クラウド投資促進を通じましたIT投資構造、人材配分の改革につなげていきたいということでございます。

行政システムにおいて民間のクラウドサービスの活用が少なく、政府調達を活用しました先進的なサービスの育成がなかなかされていないということで、政府によるセキュリティ認証などの制度創設によりまして、民間サービスの活用を促進していくということでございます。

IoTの進展に伴いまして、データ量の爆発的増加によって今後デバイスを含むエッジ側の付加価値が向上していくと考えておりまして、それに対して分散型のアーキテクチャの実現に向けた技術開発の強化でございます。

44ページがそれを線表にまとめたものであります。

45ページがブロックチェーンの取り組み、46ページがシェアリングエコノミーに関する取り組み、47ページがクラウド投資促進に関する取り組み、48ページがクラウドサービスを政府調達する場合の認証制度をつくらうということについての取り組みで、49ページが今アメリカでありますFedRAMP制度と同様の認証サービスを導入できないかということで整理したものでございます。

50ページからは、田中デバイス室長から簡単に。

○田中デバイス室長 50ページからご説明申し上げます。

今、技術開発を強化しようということを事務局から申し上げておりますけれども、現状の認識でございます。ハードウェアのメガトレンドと申し上げますと、皆さんご案内のとおり、60年後半、70年からムーア則ということで、最初は1年半でしたけれども、2年に一度、半導体の密度が倍になるということでございます。このトレンドがほぼ28ナノぐらいを目途に経済的には終わってきたというような、今まで放っておいても性能も上がって価格も下がるという状況の中で、ハードウェアのトランジスタのコストはそんなに下がらなくなってきてしまっているという状況。

それから、機械学習、深層学習といいますような、大量のデータを用いて、そこから特徴を抽出して、それで自動的に、ある種、機械的にプログラミングしていくという新しいソフトウェアのコーディングの考え方が実際に使われるようになってきた。ご案内のとおり、IoT、たくさんのデバイスが常につながっているという新しい時代に入ってきているという状況の中で、技術的には非常に大きな変遷期にあるのではないかという認識をも

っております。

こういう非連続な時期に当たりまして、国としても産学官一体で新しい革新的技術開発を強化していくべきだと思っておりますし、その際にベンチャーとかスタートアップを機動的にやっていく。新しい節目を迎えて、そうした新しい力も使いながらやっていくことが必要ではないかと思っております。

そのときに、エッジとクラウドの関係でございます。次のページでございます。これは本小委員会の下にございます分散戦略ワーキンググループで議論された内容を改めてでございますけれども、まさにエッジ側、それからフォグといわれています層につきまして、特に自動車、ロボティクス、こうしたものが強い我が国の状況をうまく活用して、現在の構造の変革につなげるチャンスを考えていこうという大きな方向でございます。

1つ、革新的な技術開発で、どういうことがあるのかということで、52ページに簡単に例を紹介させていただいております。エッジ側のお話、とはいってもクラウド側もでございますし、少し長い話として非連続な次世代の話、ポストノイマンという新しい形の形態についても視野に入れて考えていこうと考えております。

その際に、実際の事例でございます。53ページに出ておりますけれども、海外の企業でございます。ご案内のとおり、機械学習、深層学習に使われているG P G P Uと申しますN V I D I Aのもの、これは実際にエッジ側にも少しずつ入り始めているという状況です。日本のベンチャー企業でございますけれども、L e a p M i n d。新しい先端的な取り組みとして、N E Cが東京大学や阪大とブレインモルフィックのチップを考えていこうという少し先の取り組みもこうした形で始まっているものがございます。

セキュリティにつきましても、実際にいろいろな動きが54ページに出てきている状況でございます。

その際に、少し後半申し上げましたけれども、ベンチャーとかスタートアップとか、これまで既存の事業と少し技術的な変節を迎えていることを考えますと、特に市場規模が黎明期におきましては必ずしも大企業の既存ビジネスにはミートしていない状況もございます。そうしたときに、新しいI o Tコンセプトをもつようなテクノロジーのスタートアップをどのように国の力、経済の力としてうまく活用していくかというのが非常に重要であるかと思っております。その際に、彼らの規模をスケールアップしていくためには、プルーフ・オブ・コンセプトを示すような手伝いをやって、それで彼らのアクティビティーを加速していくことが重要であろうかと思っております。特にハードウェアの場合、P o C

にはそれなりのコストがかかりますので、テクノロジー、アイデアはあっても、なかなかこの谷を越えることができないということもございます。この辺の支援、環境整備も、研究開発も含めた中で考えていければいいかと思っております。

以上でございます。

○師田サイバーセキュリティ課長　それでは、56ページ以降、サイバーセキュリティについてご説明させていただきます。

まず、57ページ目をごらんください。ゴールイメージとしまして、重要インフラ、産業インフラ等のサイバーセキュリティ対策の強化、I o T製品・サービスのサイバーセキュリティ強化ということで、サイバーの防衛力を高めることがまず大きな1つの目的でございます。加えまして、今度はサプライサイドとしてのサイバーセキュリティの産業化を図り、競争力確保を目指します。大きくこの2つのゴールを目指すのがサイバーセキュリティのゴールだと思っております。

これに向けまして、5つの課題と対応の方向性を整理してございます。

1つ目が、組織のリーダーが率先してサイバーセキュリティ対策に取り組む。これは経営者にしっかり認識していただいて、自社の取り組みを進めていただくということで、これに向けた対策としまして、重要インフラにおけるペルトレーションテストなども含むリスク評価の推進。さらには、サイバーセキュリティ経営ガイドラインなどの啓発でございます。さらには、企業における投資を促進するための保険の普及とか予算などについても検討していくというのが1つ目の課題でございます。

2つ目が、人材が不足しているということで、人材育成をしっかりやっていくということでございます。

3つ目が、インシデント情報などの攻撃情報、予兆情報の迅速な共有ということで、1つの会社がやられた情報をシェアすることで、ほかの防衛力を上げていくという情報収集、分析体制整備をするというのが3つ目でございます。

4つ目が、I o Tに対する対策ということで、I o Tセキュリティガイドラインの普及啓発とか国際標準化などでございます。

5つ目が、産業化、産業競争力強化でございます。

おめくりいただきまして、58ページ目がスケジュールになっておりまして、今の5つを整理してございます。

59ページ目、重要インフラにおける対策強化でして、青の四角の中のまず1つ目で、オ

リ・パラ2020年に向けまして、重要インフラにつきましては、NISCとも協力しながら、2018年度までに重要インフラの分野の全てでリスク評価を実施していくことにしてございます。

さらに2つ目としては、経営ガイドラインの策定でございます。

3つ目として、投資を促進するための保険の普及、予算などについて実施していくものでございます。

おめくりいただきまして、60ページ目がサイバーセキュリティの経営ガイドラインでして、これは2015年、一昨年12月に策定しまして、昨年12月に改定しました経営者の認識すべき3原則、さらには経営者が担当幹部に指示すべき重要10項目をまとめたというものがございます。さらに、中小企業向けのガイドラインを昨年11月に策定してございます。

61ページ目、今度は青い四角の中の2つ目の点になりますけれども、特にこれは中小企業向けになります。中小企業向けのガイドラインを実施して、セキュリティ対策を実施していることを自己宣言した企業に対しましては、SECURITY ACTIONマークというのを付与いたしまして、これを付与した人については、サイバー保険の保険料割引制度というのをことしの4月につくったものでございます。サイバー保険の割引は、まさに今月以降提供される予定でございますけれども、このようなところも活用しながら、各企業のサイバーセキュリティ投資を促していきたいと思っているものでございます。

62ページ目は人材育成でありまして、これは今年4月にIPAに産業サイバーセキュリティセンターを設置いたしました。これは当省所管の電力、ガス、鉄鋼、石油、化学、自動車といった業種に加えまして、他省庁が所管されております鉄道、ビル、空港、放送、通信、住宅といった業界からも幅広く研修生を受け入れまして、約80名が1年間のコースを7月からスタートしますけれども、トレーニングなどを受けていただくという予定にしてございます。ここで実際に重要な人材を育て、これが各業界に戻って行って、各社のサイバーセキュリティ対策に貢献していくことを期待しているものでございます。

63ページ目は、情報収集、分析、共有でございます。まず1つ目は、独法に対する監視、監査、原因究明調査が2016年のサイバーセキュリティ基本法の改正によりIPAが実施することになったのが1つ目。

2つ目としましては、来年の秋にサイバーセキュリティ基本法の見直し期限が来ることを踏まえまして、2020年を見据えて重要インフラを中心にしました分野横断的な情報収集の仕組みをとりまとめて構築していく予定にしてございます。

3つ目は、分野ごとの情報共有体制です。右下の絵にありますように、青色が全部で12分野あるのです。重要インフラ分野の中で、例えばI S A CであるとかI P AのJ—C S I Pという青いところは分野別の情報共有体制が既存であったのですが、黄色のところは、例えば医療、水道、物流、航空、鉄道は今まで分野別の共有の仕組みがなかったものです。これにつきましても、今般、各省とも調整しまして、I P Aに加盟していただく方向で調整していくということで、民間における重要インフラの全ての分野に分野別の情報を組み入れていくことにしてございます。

4ページ目、I o Tセキュリティガイドラインの国際標準化でありまして、これは青い四角の2つ目をごらんいただければと思います。昨年7月に総務省とも共同しまして、I o Tのセキュリティガイドラインを策定いたしました。これを国際標準にしていくことで今取り組みを進めてございます。実際に本年の4月にI S O / I E CのJ T C 1 / S C 27のWG 4というところに新規案件として今登録してございまして、具体的な国際標準案を作成しております。これを10月を目途に提案して、2019年までに国際標準化を実施していきたいと考えているものでございます。

5ページ目、サイバーセキュリティの産業化であります。これは今、三輪委員に委員長を務めていただいておりますビジネス化研究会でも具体策に取り組んでございますけれども、信頼性向上を図るということで、日本企業の競争力を高めるために、対応の方向性として、一定の品質を備えたセキュリティ製品・サービスの認定をすることで、質の高い製品・サービスを洗い出しまして、こういうところに政府における調達であるとか、企業の投資促進が向かうような制度、これは税制なども含めて今検討しているところでございます。

以上、サイバーセキュリティに関する説明でございました。

○滝澤情報処理振興課長　　続きまして、ラスト・バット・ノット・リストということで、簡潔に人材育成の取り組みをご紹介します。

67ページをごらんいただけますでしょうか。ゴールイメージでございます。第4次産業革命による産業構造の変化に対応するためには、産業界のニーズを反映して、実践的な人材育成パッケージを推進することが重要だと考えております。具体的には、必要なI T・データスキルを習得できる教育、人材育成の仕組みをしっかりと整備していくことを、質、量ともに人材を拡充するためにやっていきたいと考えております。

課題と対応の方向性、4つございます。

1つ目は、まず産業界から求められるITスキルが十分に可視化されていないのではないかということで、教育機関からの人材供給のミスマッチが生じている現状に対しまして、ITスキル標準を設定以来、初めて抜本的に改訂いたしまして、今後求められる能力等を明確化していこうと考えております。

それから、技術進展のスピードが非常に速くて、スキルが陳腐化してしまいますので、社会人の学び直しのアクセスが非常に難しくなっております。ここにつきましては、経済産業大臣が民間企業なども含めて提供する講座を認定する制度を創設いたしまして、第4次産業革命に対応した人材育成を推進することをやっていきたいと思っております。

2020年から小学校でもプログラミング教育が必修化されます。教育機関でいろいろと対応が進んでおりますけれども、当然、産学官連携して取り組むことが非常に重要でございます。未来の学びコンソーシアムということで、総務省も一緒になりまして文科省さんと経産省ともに産学官連携となって取り組むためのコンソーシアムをことし1月に立ち上げております。産学連携をしっかりとやっていきたいと思っております。

それから、非連続的なイノベーションを創出する突出した能力をもつ人材が非常に重要でございます。本日お越しになっておりませんが、西川さんも実は私どもがやっております未踏事業のOBでございます。こういった若い才能を発掘するための取り組みをしっかりと強化していきたいと思っております。

おめくりいただきまして、68ページが全体像でございます。

1つ目は、先ほど申し上げました2002年につくりましたスキル標準を初めて抜本的に見直しまして、ことしの4月7日にITSS+ということで、セキュリティとデータサイエンスの分野を追加して発表させていただきました。これからユーザー企業の皆様も含めまして、新しい技術開発のやり方なども含めて、スキル標準を抜本的に拡充することをやっていきたいと思っております。

2つ目、情報処理安全確保支援士というのをスタートさせていただきました。4月1日に4,170人が登録されてございまして、2020年に3万人ということで、非常に野心的な目標でございますけれども、掲げて、しっかりとセキュリティ人材の育成をやっていきたいと思っております。

先ほどご紹介しました経済大臣の認定制度でございます。こちらも講座の認定に向けました具体的な検討を開始してございまして、来年4月に新しい認定講座をスタートして、ボリュームゾーンの皆様方にしっかりとITスキルを身につけていただく、そういった機会

を提供できるように頑張ってもらいます。

外国人材につきましても、トランプ政権が非常にビザを絞っているということで、私たちはチャンスだと考えておりまして、7月をめどにインドにミッション団を派遣して、実務レベルの協議を開始して、11月に予定されております日印ジョイントワーキンググループを通じまして、政府レベルでもしっかりとインドの人材を吸収することに取り組んでまいりたいと思っております。

未踏の人材でございます。先ほど申し上げましたように、未踏、非常に優れた人材が輩出されております。1,650人ぐらいOBがいるのですけれども、その中でも起業技術が非常に高いということがございます。3割が起業しております。未踏アドバンストということで、起業人材を育成するための取り組みは抜本的に強化すると考えておりますし、個別の自動車などの分野につきましても、いわば天才と業界との掛け合わせもトライアルしていきたいと思っております。

プログラミング教育につきましても、先ほど申しましたように、官民コンソーシアムを通じて産学連携でしっかり支援していくことでやろうと思っております。

個別のものについては、69ページ以降でございます。スキル標準の見直しにつきましては、セキュリティ領域やデータサイエンスの領域を追加すると、4月7日に公開させていただきました。これからアジャイル型開発のような新しい開発手法なども含めまして、新スキル標準の検討を継続していこうと思っております。

70ページでございます。今回、セキュリティデータサイエンスを4月7日に追加させていただきましたけれども、単に追加するだけではなくて、研修事業者ですとか教育機関の皆様方がこういったものに基づいて教育のコンテンツを提供していただけるように、しっかりとコンテンツの充実を図っていきたいと思っております。

71ページでございます。情報処理技術者試験は50年の歴史、40万人が受検する国家試験でございますけれども、2016年から情報セキュリティマネジメント試験を創設するなどの不断の見直しを行っております。ことしからは情報処理安全確保支援士という新しい国家資格もスタートしておりまして、登録セキスペと呼んでいますけれども、2020年までに3万人を目指してしっかりと頑張ってもらいたいと思っております。

72ページでございます。第4次産業革命のもとの人材をしっかりとボリュームゾーンも含めて育成するということが、IT・データ分野を中心に、社会人向けの教育訓練の講座を大臣に認定いただきまして、そちらに対してしっかりサポートする支援を考えており

ます。こういった制度の詳細が固まり次第、厚生労働省さんにおいて検討いただきまして、厚生労働省のもっております専門実践教育訓練給付金の対象にさせていただくことを考えておりまして、こちらの対象になりますと、上限7割、168万円という非常に大きなサポートを個人の方に対してできるということで、ボリュームゾーンの皆様方にITのスキルを身につけていただいて、スキルの転換を図っていただくことの礎にしたいと思っております。

73ページ、先ほど申し上げました外国人IT人材の獲得でございます。7月にインドにミッション団を派遣して、実務レベルの協議を開始することを考えております。

74ページ、未踏人材でございます。先ほど申し上げましたように、西川さんも含めて非常におもしろい方々が発掘されている事業でございますので、こちらの事業を拡充いたしまして、起業につなげていくといった取り組みを抜本的に強化していきたいと思っております。

セキュリティ・キャンプでございます。こちらは三輪委員に非常にお世話になっておりまして、高度人材、サイバー攻撃に適切に対応するためにも、若年層のセキュリティ人材の発掘、裾野をしっかりと拡充していこうということで取り組んでおります。累計で581名が受講していますけれども、実はキャンプの修了者の中には、ラスベガスで開催されているDEFCONで大人に交じって参加して優勝したという非常に優秀な方も発掘されておりまして、こういった取り組みを抜本的に強化していきたいと思っております。

76ページ、プログラミング教育でございます。先ほど申し上げましたように、2020年から小学校でもプログラミング教育が必修化されます。未来の学びコンソーシアムで、総務省、文科省、経産省も一緒になって、産学官で一体となって教育環境を整備することをやっております。あわせて、EdTechということで、旧態依然とした教育現場をテクノロジーの力で革新していくことに取り組んでいきたいと思っております。

次のページをごらんいただきますと、ことしの11月にSXSWeduというのがありますけれども、毎年オースティンで開催される全米最大の教育イベントがあります。こちらを日本にも輸入して、多くの関係者の方に集まっていただいて、意見交換をしていただいて、体験をしていただくというような取り組みができないかということで、これも検討中でございますけれども、さまざまな取り組みにチャレンジしていきたいと思っております。

以上でございます。

○佐野情報経済課長　　続きまして、78ページから参考まででございます。きょう、小笠

原課長にも来ていただいておりますが、総務省と経済産業省との連携について、既に公表させていただいておりますけれども、さまざまな分野で連携していこうということで、今、具体的な検討を進めているということでございます。

続きまして、資料3をあけていただければと思います。前回、前々回からご議論いただいてきたI o Tの面的展開についてでございます。

まず、2ページ目を開いていただけますでしょうか。前回もご議論いただきましたけれども、改めてコンセプトを整理したものでございまして、社会実装可能なフェーズになってきたI o Tソリューションについて、制度への組み込みまでを見据えまして、データエビデンスでしっかりと評価しまして、一体的に導入していくサイクルを構築して、あわせて社会課題の解決を図っていこうということでございます。それによりましてI o Tの面的展開を進めていこうということでございます。

海外の事例を参考までにつけさせていただいております。3ページが欧州の緊急時自動通報システムの搭載の義務化の例、4ページがイギリスのスマートメーター義務化の例、5ページがアメリカにおきます自動ブレーキの導入の自主協定の例ということで、海外でも各分野ではいろいろな動きが出てきているということでございます。

6ページ以下が、前回もご議論させていただきましたけれども、さまざまな分野で既に社会実装可能なソリューションがいろいろ出てきておりまして、個別分野でそれぞれ検討が進められております。今後、自動車の例えば安全装置、ものづくりに関するシミュレーション開発等々、さまざまな分野でソリューションがあると考えてございます。

7ページが土木、インフラ、8ページが保育、医療、9ページがバックオフィス、行政等、さまざまな具体的なソリューションがあるということでございます。

10ページが面的展開を実現するためのサイクルで、段階があるわけでございますけれども、技術の発掘の段階、実証による性能評価の段階、11ページ、インセンティブ付与を保険とか税などによりまして導入を促進していく段階、4段階目としまして、制度に組み込んでいく、これは導入の義務化とか補助金の交付要件化でございます。

各ソリューションによっていろいろな段階がございますけれども、その段階に応じて措置を講じていくということで整理してございます。

12ページが保険の例であります。

13ページでございます。こういったI o Tの面的展開を各分野ではそれぞれ取り組みの検討が進められてきておりますけれども、戦略的に進めていくために、本年度中をめどと

しまして、以下のようなスキームの構築ができないかということでありまして、民間から提案を募集しまして、それに基づいて評価をし、どれだけ効果があるかをデータエビデンスに基づいて精査いたしまして、担当省庁へ検討を要請するという一方で、個別のさまざまなソリューションの面的展開を図れないかということでございます。

14ページからがそれを行うに当たりまして、各ソリューションが実際にどれだけインパクトがあるのかというデータエビデンスで数字を整理しまして、その効果に基づいて導入を判断していくことが重要だと思っております。これはあくまでも例でございますけれども、自動車分野、行政分野、介護分野、建設分野、こういったそれぞれの分野で具体的な数字を出して取り組んでいくことが必要であると思っております。

資料3については以上でございます。

○村井委員長　　どうもありがとうございました。

2つの資料を説明していただきましたので、ここから自由討議となります。今説明していただいたように、1つは情報政策の方向性という非常に大きな方向性に関する話です。2つ目はI o Tの面的展開とあって、実はI o Tファーストとして議論していただいていた内容になっています。

順番は一つずつ分けてもいいのですが、I o Tの面的展開は、どのようにしてI o Tを具体的に進めればよいかということですし、前者のほうは、それを含めた経済産業省の情報政策全般の方向性だと思いますので、それぞれどの箇所かを指摘していただきながら、自由に議論していただければと思います。いつものように、ご発言は札を立ていただき、お気づきの点からどんどんご発言いただければと思います。よろしく願いいたします。

では、岡村さん、お願いします。

○岡村委員　　今回、I o Tを機に、利活用とセキュリティという、アクセルとブレーキの両面を同時にやらなければならないという点で非常に難しい部分だと思います。特に解釈及び立法、つまり制度整備は非常に重要な課題だと思います。従来から個人情報の利用ルールについては法整備もそれなりになされてきています。これに対して、法人情報、特に信用情報などにかかわるものについて、どこまでどう利活用することができるのか、よく相談を受けるのですが、そのルールは意外にはっきりしていません。金融庁さんだったか、研究会を開催して一定限度、検討作業をされているようですけれども、最終的なルール化には至っていないような状況です。そういう面では、民間事業者は利活用したいのだ

けれども、どこまでしていいのか、非常に不安に駆られています。やはりそれを取り除くために基準を明確化する形で進めなければいけないのではなかろうかと存じます。

それから、標準化あるいは共有化の中で1つ課題になりますのは、実際の作業をしてみますと、意外なところで問題が出てまいります。例えばかつて問題になったのが、外字の共通化でした。特に住基外字がある、常用漢字表外字がある、他にもあれこれ外字があるという形で、国の省庁レベルでも統一が図れていなかったような状況を、何とかIPAフォントを外字でつくるといふことである程度解決してきたわけです。これも国レベルで一定の共通化を強制しないと、民間に普及してもらいたくても、なかなか進まないだろうと。ISO/JISの水準の整備をさらに進めていただくこととともにお願いしたいところでございます。

それに関連して、書式のひな形フォーマットなどもある程度国等々も含めて共通化していただかないといけません。例えば自治体レベル1つにしても、全然それぞれが違うので、なかなかデータの共有がしにくい部分がありますので、やはり共通化をお考えいただかなければいけませんし、実際に帳票のフォーマットが著作権紛争で裁判沙汰にまでなった事件もありますので、この点の共通化も1つの課題になるのではなかろうかと思えます。

他面で、セキュリティについて少しだけ申し上げます。先ほども出てまいりましたけれども、やはり自主的な取り組みに任せるところも大事ですが、ある程度限界があることも否めません。今、IoT、あるいはAI化が進む中で、例えば車載システム1つにしても、ある意味どんどんブラックボックス化をしているような状況でございます。前にも少し他の会議で申し上げたところではありますけれども、各種業法に基づく検査制度の基準を省令などで決定される際に、基準の内容についてIoTセキュリティをビルトインした形へとアップグレードして、ある程度猶予期間をもたせることで無理がないようにやっていただくことで対応できるはずです。このような形で脆弱性をなくしていくような形の努力が必要なのではなかろうかと思えます。

それに関連して、これだけ組み込みのためだけの制度というシステムが普及してまいりますと、やはりソフト、ハードの垣根が一種のフュージョン化するということは先ほどのお話の中にも出てきたのです。そうすると、製造物責任法のあり方にしても、これまでソフト、ハード2分論をしていたものが、かなり変わったような状態になっていく。他方で、この技術革新の激しい中で10年間という長期の責任を負うべき期間に耐えられるのかどうかという問題も出てきますので、それも含めてやはり制度整備をさらに強化を検討い

ただきたいと思います。

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した。

それでは、横塚さん、お願いいたします。

○横塚委員　　私から、情報政策の方向性という観点で、ここに書いていないテーマを2点お話しまして、ぜひ検討をお願いしたいと思います。

1つ目は、人材の問題です。Connected Industriesというコンセプトに基づいて、これからの新しいビジネスというのは、会社を越えて、あるいは業種を越えて、いろいろな枠を越えて新しい価値をつくっていくビジネスとなるのです。これをつくっていくに当たりましては、全体を構想していく力、あるいは全体を俯瞰していろいろな技術やいろいろな会社さんの特徴を生かして組み合わせしていく力が非常に重要になってまいります。これはITスキルとは全然違う能力でして、学術的にはシステムズ・エンジニアリングとか、システム・オブ・システムズとかというようではございますけれども、この力が実は日本は民間を含めてかなり弱いと痛感しております。個別の現場力は強いわけではございますけれども、全体を構想していく力を日本全体で強化していかないといけないのではないかという観点で、産業界、あるいは大学も含めて、全体を構想していく力は特にビジネスをつくる上では非常に重要なので、ここをどう力を入れてやっていくかをご検討いただきたいのが1点目です。

2つ目は、法制度の問題です。施策にもいろいろ書いてございましたけれども、人材もやはり流動化することは非常に重要で、いろいろな会社を渡り歩くような人材がいろいろなことを思いついたり多様化していくわけで、欧米並みな人材の流動化も日本にぜひ進めていくべきではないかと考えます。

そう考えたときに一番ネックなのは、企業が解雇するという制度が今日本の場合には条件が余りにも厳しいので、そろそろ解雇をもうちょっと柔軟にできるような制度に変えていくことが、人材にとっても企業がいろいろな形で生まれ変わっていく状況にあわせても、ぜひとも必要な時代が来たのではないかとということで、ぜひご検討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した。

それでは、唯根さん、お願いします。

○唯根委員　　私も2点お願いがございます。

まず、人材の育成なのです。きょうのご提案の中に、幼児教育の部分、今生まれたお子さんたちはオギャーと産まれて自己を意識したときから既にこういうITを使っていますので、この方々の幼児教育部分からみていただきたい。それは情操教育的な分野も視野に入れておいていただきたい。なぜかという、私などでも感じるのですが、機器がうまく使えなかったり電源が入らなかったときのITロス症候群的ないらいらですとか不安感ですとか、そういうものへの対応なども早い段階で対策をとっておいていただけないかという点も併せて、こういう人材育成の面もお考えいただきたいと思います。

それから、法制度について、ビジネスの電子商取引の準則の改定についてご提案いただいているのですが、これも犯罪面というか、今私たちが使っている中で、いろいろなその中の仕組みを悪用して消費者が犯罪に巻き込まれてしまうようなケースも多々出てきております。直近では、現金というか紙幣をネットで販売されるとか、未成年者の犯罪組織的な集団がマネーロンダリングのために、振り込め詐欺や何かのお金を集めていたりするとかいう事件もあると聞いたりしますので、こういう分野での電子商取引のルール視野というか、警察との連携も含めて、総合的な法律の見直しというか、ルール整備についてもお考えを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。立っている札が尽きました。

喜連川先生、ありがとうございます。

○喜連川委員　　遠慮深いので、皆さんが発言されなくなってからでないとお話できないのです（笑声）。

最近、政府で申し上げているのは、リアクティブからプロアクティブにしてくださいというのがメッセージでございます。例えば民が既に膨大な開発投資をしている領域を政府が考える場合、そこには既に大きなアウェアネスが存在しているわけですから、むしろ、そこを飛び越えたところ、つまりプロアクティブというのは、これから起こるか起こらないかわからないぐらいのところに対してどのように介入していくのが一番重要なのではないかと考えています。

ことしの連休中、することがないので、トランプさんのおかげで大きくサブスクライバーが上がったというニューヨークス・タイムズを読んでいますと、6年間の懲役というものを米国の裁判所がソフトウェアで決めたと書いてあるわけです。なかなかいいのは、AIで決めたとはいまだ書いていないのです。アルゴリズムとソフトウェアで決めたと書いて

ある。人生の犯罪のための懲罰をソフトウェアで決めた。これをどうしてくれるのだといったときに、結局、住民サイドからどうなっているのと問うても、会社は原則ディスクロージャーしなかった。しかし、裁判所はそれを最終的には是とした。なぜかという、人間よりコンピューターのほうがよくいろいろな情報をきちっと整理できるからだ。だけれども、やはり違和感が残るのです。

つまり何がしたいかという、これはいわゆるデジタル・トランスペアレンシーの話になってきます。この問題は、裁判だけではなくて、いろいろなサービス全てに対して適用される可能性がありまして、こういう問題をどう整理するかは、ほとんどまだ考えられていない。その辺を政府がしっかりと見据えることが私は重要ではないかという気がしています。

ちょっと誤解があるといけませんけれども、きょうご用意いただいた資料が不適切とか何とかとっているのではなくて、リアクティブなポジションも必要です。だけれども、それに加えてプロアクティブなポジションをぜひ入れていただきたいということです。例えば、それに関連して、きょうの中に全然入っていなかったと思うのですが、Alexaをどう考えるのかというのがあります。言葉をグーグルがとりました。しかし、ボイスを全部アマゾンがとったとすると大変です。今、車の中に入ろうとしています。完全にオープンですから、全てただです。そうすると、ありとあらゆる、ユーザーのインターフェースがあれになったときに、産業のインパクトは圧倒的に大きいです。つまり一歩先をみたときに、どう考えるのが重要です。

もうちょっとへんちくりんな例でみますと、前回もいったか忘れてしまいましたけれども、中国で1円で自転車乗り放題というのがあるではないですか。あれを、私、何で日本のアントレプレナー道場みたいな、ああいうことを学生が考えないのかということです。それはやはり大陸法なのか、英米法なのかというところで、そもそもどんなところにも自転車を乗り捨てていいのかというところがバックプレッシャーになっているような気がするのです。そういう法的な枠組み、つまり、まずゲームを変えなければ勝てないのではないかというのを感じておりまして、まだいろいろありますけれども、その辺をまず考えていただくとありがたいと思います。

最後に一言申し上げますと、内閣府の下の日学が安全保障のアナウンスメントを掲げました。セキュリティが議論されていますが、大学の先生をお招きしながら研究するときに、安全保障をどう考えるのかをどこかでやらないと、スムーズにいかなくなる時代になった

というのは非常に大きな変化だと思います。

以上です。

○村井委員長　　ありがとうございました。

根本さん、お願いします。

○根本委員　　簡単に。医療への踏み込みを今後もう少し強める必要があるのだろうと思います。一番メインストリームのところなので、そこへの言及はしていてもいいのではないかというのが一点です。

もう一点は、例えば資料3の13ページあたりでも、民間からの提案募集を待っているいろいろな施策を講じていきますという形の展開になっているわけなのですが、官民データの基本法ができた段階で、原則が完全に転換していることを忘れてはならないと思います。行政府そのものにおいて、全ての事務を電子化するという義務が行政府側に課されているのだということを恐らく法律を書いた人たちは意図していたはずでございまして、少なくとも経産省は、省のやり方として、ここまでやったのだというところを各省にみせていただくような政策展開が必要ではないか。民間からの提案募集をみて、評価委員会でやりますというのではなくて、省側でもやりますというトラックをもう1つつくっていただけると、全体が進みやすくなる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した。

それでは、有賀様、お願いいたします。

○有賀委員　　きょういただいた資料で、実は私が一番違和感があるのは、冒頭の5ページの図があるのです。左の図を右にもっていくのだとおっしゃっているのですが、そもそもこれはIT産業が拡大していくようなイメージで、これは違うのではないかと思うのです。新しいIoT産業をつくりかえる感じで物が動いているのに、何だか知らないのですが、従来型の延長線上みたいなイメージがどうしてもある。そもそもやっている人種が違うと思うのです。これは皆さん百も承知なのだけれども、絵を描くところになってしまう。ここら辺から改めていかないと、物は変わらないのではないかと思うのです。

当然、そうすると育成方法も違う。それから、最近、ベンチャーを育てていると、結局新しいビジネスモデルのシステム化を相談する相手がいないのです。大手のS I e rなどをもっていても、例えば中堅中小企業のベンチャーは相手にしてくれない。では、中堅中小のソフトウェアハウスにもっていきと、いっていることが理解できないからろくなものをつくってくれない。今2つ、3つ立て続けにトラブっているのを私みたいなのがトラブ

ルシュートしているという状況が発生しています。

これはもともと昨年、一昨年ぐらいで議論した、例の25対75の話に決着するのではないかと思うのです。そもそも論として、自分たちがやりたいことをきちっと定義して、自分たちで実現できるという人材がいなかったことがすごく大きいと思うのです。だから、去年あたりは、最低でも50：50にもっていきましょうという議論をここでしたと思うのです。それに対応して、今回その辺が何か配慮されているかという、申しわけないのだけれども、非常に寂しいなど。

例えば、72ページあたりに第4次産業革命スキル習得講座の認定制度をつくろうという話で、これは私、すごくいいと思うのです。むしろ、本当は情報処理技術者試験制度などは全部民に移してしまっていて、これこそきちっとした試験制度にするぐらいの画期的なことをやらないと、人も育たなければ産業構造も変わらないのではないかという気がして仕方がないのです。

やはり従来型の産業構造を壊そうとすると、漸進でちょっとずつ進んでいっても変わらないです。何かぱっと変えないと。だから、例えば人材育成のところなど、一番それをやりやすいと私は思いますので、全体的なトーンでおっしゃっていることは非常にいいとは思いますが、そういうキーポイントのところでは何か1つ2つ、ぐさっと刺さるようなものをやはりやっていかないと、変わらないかという気はいたします。

以上です。

○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　私からは、22ページの越境データ移転について簡単にコメントさせていただきたいと思います。データの越境流通は、個人情報保護法の世界で以前からずっと問題になっておりまして、今回の個人情報保護法改正によって一定の対応がなされたと理解しております。個人情報保護委員会も、EUや米国などとの協力対話を進めている状況があります。

EUが去年の4月に一般データ保護規則という新しい個人情報保護法を採択しまして、新しいルールをつくっているところです。

その中に、EUから第三国にデータを移転するときに、欧州委員会が第三国の保護レベルが十分か否かを判断する仕組みがあります。この制度は1995年データ保護指令から一般データ保護規則に引き継がれているわけですので、日本についても十分性認定を受けるか否

かが以前から議論されています。ただ、日本が仮に充分性を申請するという話になった場合には、欧州委員会から評価を受けるという仕組みに入り込むことになります。その関係で意見交換を行うと書いてある22ページの越境データ移転の話の中では、充分性の議論に引きずられ過ぎないようにすることが重要ではないかと思います。

あわせて、国内の関係省庁、それから協力対話を進めている個人情報保護委員会との連携もぜひ行っていただきたいと考えているところです。

EUとの関係では、越境データ移転の充分性の話だけではなくて、市民に対してサービスを提供している事業者に対して、EUの規則がかかってくるという越境適用の問題があります。その場合には、どの程度の日本の事業者がEUのルール適用を受け得るのかが明確ではないという点ではありますが、EUのデータ保護法制には越境データ移転以外の問題があると申し上げておきたいと思います。

ただ、逆にEUのルールの中にはデータポータビリティの仕組みという自由な情報流通を促すような規定もありますので、日本に存在しない規定の示唆を受ける可能性もあるかもしれないと考えております。

以上です。

○村井委員長　ありがとうございます。

それでは、澤谷さん、お願いいたします。

○澤谷委員　資料2の14ページパーソナルデータ匿名加工制度の創設についての質問です。ここでは個人を特定しないビッグデータについて売買をしていくことを中心に行い、個人を特定するようなディープデータのほうで実際にサービスの恩恵を受けるような部分については今回は行わないということです。今回はビッグデータを中心とした匿名加工したデータを売買する市場をつくることで効果があると思うのですけれども、そういったデータを使った価値のあるサービスをつくり上げるところで実際には本当は価値が出てくると思われま。なので、この2つを分けて片一方だけを進めることは、余り効果がないのではないかと思います。そのためには、まずパーソナルデータのオーナーシップの議論を避けてはいけないと思うのです。データは誰のものかといったことを避けていくと、あやふやになってしまって、昔、音楽業界で起こったようなグレーゾーンの話になってしまうのではないかと危惧します。

データの利活用権限に関する契約ガイドラインというのが昨日送られてきて、電車の中で読みながら来ました。この5ページに、データは無体物であるので、所有権の対象では

ないので、今回は所有権なしで使っていこうと書いてあります。そうだからこそ、今、そこに立ちどまって、そのデータのオーナーシップは誰なのかを議論することが必要なのではないかと思います。データ活用のためのルールづくりから、個人から発生したデータがどういったところで何に使われているという、EUで定められたGeneral Data Protection Regulation（一般データ保護規則）のようなルールづくりをやはり議論を並行していくことが重要です。匿名化したデータのための市場をつくることだと、片手間ではないかと思います。

○村井委員長　ありがとうございます。

どうぞ、岡村さん。お願いいたします。

○岡村委員　今の問題に私なりにお答えしますと、今、経済産業省の知財室でIoT、あるいはAIに即したデータ保護のあり方ということを別途検討しております。そろそろ中間報告が公表されたはずですが、座長を私が仰せつかっておりますもので、それはそれで粛々と進めなければなりませんけれども、諸外国に先立ってやるということ、また、EUはデータベース保護指令が現実に必ずしも成功をおさめておりませんので、それを踏まえて、新たな時代に即した情報のオーナーシップというか、保護のあり方を検討しておりますので、またそれについても有益なご意見などをお寄せいただきますようお願いする次第です。

○村井委員長　ありがとうございます。

それでは、川上さん、お願いいたします。

○東原委員代理（川上）　データの利活用が話題になっておりますので、その点についてまず申し上げたいと思います。

冒頭、岡村先生から法人間のデータの利活用についてのお話がありました。不安を感じている人がたくさんいるという趣旨のお話がありましたし、準備いただいた資料にも、手探り状態であるという記述があったと思いますが、現場は多分そういう状況だと思います。

そういう中で、カメラ画像活用ガイドブックを作成いただいたり、契約ガイドラインを検討いただいているのは大変ありがたいことと存じますが、現場の状況によっては、個人のデータで行われているものと同様に、特に中小企業などを念頭におきますと、法人向けの情報銀行もご検討いただければと考えますので状況をみつつ、是非ご検討いただければ

と存じます。

もう一点申し上げたいのは、今回、面的展開という形で整理していただいたのは、大変わかりやすくなったと思います。その際に、いろいろ政策ツールとして予算とか保険について言及がございました。やはりもう1つの手段としての税制の活用は、お考えをいただきたいと思います。特に攻めのIoT投資の促進が重要になると思いますので、資料にもありますが、例えば、クラウド投資を促進することのインセンティブとして税制優遇を図るというように、ぜひ税制の活用もお考え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、砂田さん、お願いいたします。

○砂田委員　3点あります。

最初は、Connected Industriesで、これは非常にいいコンセプトだと思います。いろいろな産業や分野がつながって新たな価値を生み出そうとするとき、やはりどうしてもそれぞれの分野を所管する官庁や公的機関の連携も必要になります。そこで、ぜひConnected Governmentといいますか、それを並行して進めていただければと思います。

その意味で、IoTで経産省と総務省が連携するのはとてもいいニュースですけれども、ほかにも連携を広げてできるだけ政策の一貫性を高めてほしい。たとえば、先ほど人材の流動性の話が出ましたが、そのためには、やはり社会保障のあり方も見直す必要が出てくると思われま。また、データ活用について、規制改革政策とIoT政策のそれぞれから出てくる方針や取り組みは整合性の取れたものであるべきでしょう。新しい産業創造も視野に入れた政府の新たな役割を考えると、政府全体で一貫したデジタル化政策を持つことの重要性が高まっているというのが1点目です。

2点目が技術開発、イノベーションのところ。ちょっと古い話で恐縮なのですが、私は以前に経産省の情報政策の歴史を研究したことがありまして、そのときに気づいたことは、日本政府は市場でメジャーになり始めた技術の開発に予算を集中して振り向けてきたということです。コンピューター開発は米国より遅れて始まり、当初はキャッチアップを目標としてきたから仕方がないという気もします。しかし、今日に至るまで、なぜ米国は次々とIT市場で新しいゲームチェンジを起こすことができ、日本はできないのか。それは、米国政府がまだメジャーになっておらず誰も強い関心を払っていないような技術であっても、幅広く開発を支援し調達も行ってきた、そういう技術政策が一つの大きな要因な

のではないかと思います。

ですので、先ほど新しいデバイスの開発といったお話がありましたけれども、ハードだけではなく、とりわけ今後はソフトの新しい技術、特に今メジャーではない技術を育てていくことがイノベーション政策として大切であるような気がいたします。

最後に、人材のところですか。つい最近IPAが発行したIT人材白書を見ても、IT人材の7割強がIT業界で働き、ユーザー企業は3割弱にとどまっています、米国などと比べてその割合が逆転している状況は大きく変わっていません。情報工学専攻の学生は、ユーザー企業に就職したくないと言っています、なぜと聞くと、活躍できるかどうかわからないからと答えます。IT企業のほうが、ITの技術をもっていれば活躍できるのではないかと学生は考えているのです。ただ、まだ一部かもしれませんが状況は変わりつつあり、デジタル化がもたらす大変革に気づいているユーザー企業はデータサイエンティストをどんどん採用しようとしています。もはや中途採用では確保できないから、新卒を採るのが最近の状況のようです。ユーザー企業自体の意識変革がまず必要ですし、そういう変化が起こっていることを学生に対して広報活動などを通じて知らせていくことも大切だと思っています。

以上です。

○村井委員長 丸山さん、お願いします。

○西川委員代理（丸山） 今のユーザー企業の話で、すごくそうではないかという気がするのです。恐らくITの黎明期、60年代とかは、ユーザー企業がとにかくCOBOLを書ける人を採用していたという時代があって、それから水平分業の産業構造になっていったと思うのです。今、いわゆるデータサイエンス系で同じことが起きているような気がします。ですから、いずれそれがまた水平分業になるのだと思うのですけれども、今、データサイエンス系の人ユーザー企業に吸い込まれている状況かという気がします。

それとは別に、セキュリティに関して2つだけ申し上げたいのです。

1つは、ハードウェアトロイという概念があって、半導体チップは今どうやってつくるかということ、ほとんどが外部のIPを買ってきて組み合わせるような、私もよくわからないのですけれども、そういう外部から買ってきた設計回路の中にトロイの木馬が入っているというタイプの攻撃があるようです。

実は私どももハードウェアチップをつくっております、物理設計をしてくださる海外の会社なのですけれども、いってみたら、そういうことはほとんど気にされていないので

す。それで、実は早稲田大学に戸川先生という方がいらっしゃって、そこの方々が比較的先進的な仕事をされているように思います。もし、これは日本の安全保障に対して極めて重要なことでございますし、そこで競争力がとれるのであれば、1つ考えてもいい領域かという気がします。

セキュリティの2番目は、すぐに競争力になるかどうか分からないのですが、海外のセキュリティベンダーの方々はインテリジェンスということをしします。情報共有で脆弱性の情報の共有とか、あるいはインシデントの情報の共有はIPAさんが非常に真剣にやってくださって、非常によい仕組みができておりますが、実はどちらかというところ、これは政治的に難しいのかもしれないですが、ポテンシャルなアタッカーが次に何をやるかという情報収集をすること、敵が何をやるかということがインテリジェンスなのですが、海外のベンダーはそれを真面目にやっているところがあります。我々、日本でやるべきかどうかは私はよくわからないのだけれども、一応、どこかで頭の隅に入れておいたらいいのではないかと気がいたします。

以上でございます。

○村井委員長　ありがとうございます。

松本さん、お願いします。

○松本委員　私自身の意見をいう前に、直前に丸山さんからお話に出ましたハードウェアトロイについて、これはハードウェアトロージャンとか、マリジャスハードウェアともいわれていますが、この件について少しだけコメントさせてください。

まずハードウェアトロイについては、既に我が国でもSIPのプロジェクト等いろいろなところで私も含めて頑張って研究を行っていますので、ぜひさらなるご支援をお願いしたいところです。

一方で、我が国の内部で半導体の製造をしている企業は、どのようにしてしっかりやっているかを外部に対して示していくのが重要です。それから、設計自体を日本国内で行っていて、製造を海外に委託するときに、海外でしっかりと管理を行っている会社は、製造委託先の会社の一技術者が何か悪い気を起こして、おかしな回路を追加するといったことがもしありますと、製造を受託した会社は業務をやっていけなくなるので、ハードウェアトロイがそのようにして仕掛けられるということはなかなか考えにくいのですが、そのような恐れがある場合には、委託元の会社においてハードウェアトロイが含まれていないことを確認できるようにしないとイケません。

さらに、半導体の分野によって、例えば無線モジュールに関しては、我が国のメーカーがリーダーシップをとれない状況にあり、ほとんど海外製という場合があります。もし、そもそも製造会社が属する国の政府レベルの関与があって、何かの機能を含まないと輸出が許可されないというケースもあると聞いております。したがって、そういう状況では盗聴機能が仕込まれている可能性のある半導体しか使えないという状況となり得ますので、相当気をつけなければいけないということかと思えます。

半導体においてまぎらわしいのは、今現在は、仕様書に無い機能がないように見える回路が、将来何かあった場合に対処できるように備えて仕様書にない機能を実は含んでいるなど、悪意ではないのですけれども、ユーザー側からみるとよくわからない回路が入っているというケースもあるようです。このような場合と本当にマリシャスなケースを区別するというのは難しいみたいです。以上がハードウェアトロイについての補足です。長くなりました。

それでは、私が申し上げたかった点2つに移ります。

1つ目は、パーソナルデータの活用の中で、いろいろ個人情報保護法等、あるいはそれから派生したルールが整備されてきて、活用できるようになってきたと思うのですけれども、個々の分野で匿名加工をこのようにすべきだ、というところがあります。そのような規定も整ってきているかと思うのですが、その中で高度な暗号化という言葉があり、その高度な暗号化が何を意味するかがはっきりしていないようで、困っている方々がたくさんいらっしゃいます。したがって、こうすればよいとか、どのように対処すればよいとかを早めに決めてあげることが必要なのではないかと考えます。

第2点目は、IoTも関係するのですが、民間企業間のデータの自動的な連携、流通に関しては、事務局ご提示の資料でも整理していただいております。まだなかなか難しいというところではありますが、これは事例をみつけていくというよりは、もう少しドライブをかけた何らかの施策が必要になってくるのではないかと考えます。それから、国際的にもヨーロッパ、アメリカが主導権を握ろうとして強力に動いておりますので、我が国がどのような立場で臨むべきかという部分はまだ暗中模索のような感じではありますものの、何とか切り開いていかなければいけない課題が非常に多いのではないかと考えます。

以上です。

○村井委員長　ありがとうございます。

では、岡村さん。

○岡村委員 何回も済みません。先ほどの点に関して、ハードウェアトロージャンの問題もありますけれども、私が外部理事をやっていますJPCERT/CCでは、むしろいわゆる産業機器のセキュリティを保つためセキュアコーディングをどう進めるかということで、いろいろな大手企業に対して働きかけをしております。つまり、保守という発想はあっても、セキュリティという発想が、そういう産機のメーカーさんには必ずしも十分でないことが少なくありませんので、大変脆弱なものができる一方、例えばスマメに代表されるように、各家庭に端末として配置されるというような性格のものであるため、いつでも、どこからでも、誰からでも大変攻撃しやすいような状態が、そうした脆弱性が残ることで悪用される恐れがあります。そのような観点からチップの脆弱性をなくするという観点でI o Tを乗り切ることも重要な視点として1つご認識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。

石井さん、お願いします。

○石井委員 先ほどから匿名加工情報のお話が出ておりますが、今回の資料で出ているケースとといいますのは、匿名加工情報を使わないケースと理解しております。そうであるならば、匿名加工情報を使うものではないという前提での資料のつくり方をさせていただいたほうがよろしいかと思えます。

匿名加工情報に関しては、個人情報保護委員会から加工基準のガイドラインはやユースケースを取り上げたレポートが出ておりますけれども、まだ実運用の問題が残されているかと思えます。匿名加工情報を使うニーズ、それから具体的な場面がもしあるのであれば、別途資料を追加していただくほうがよろしいのではないかと思えます。

以上です。

○村井委員長 ありがとうございます。

三輪さん、よろしくお願いします。

○三輪委員 一応、セキュリティが専門ですので、セキュリティで自分がかかわっているものが多いので、自分で意見すると自分に返ってくるだけなので、どうかなと思って余りいわなかったのです。

サイバーセキュリティ経営ガイドラインについて、ここでも何回か言及されて、参考にもなって記されているのですけれども、経営ガイドラインというのがそれなりに世の中の的にもかなり意識されてきているところではあるのです。この中の資料に置くと、普及啓発

を進めるといふ表現にとどまっているので、サイバーセキュリティ経営ガイドラインをもう少し強く押し出す工夫がここに書き込まれているといいと思いました。

以上です。

○村井委員長　ありがとうございます。今一通りお話ししていただいたので、幾つか私の方で気づいた点をお話しさせていただこうと思います。

幾つか抜けているところをご指摘いただきまして、ありがとうございました。そういう視点でいうと、さきほど喜連川先生が最後におっしゃったリアクティブ、プロアクティブというのはそのとおりだと思います。

国の安全保障との関係が学術会議の件もあり、2つ考えなければならないことがあるかと思えます。1つは、前にもお話ししたかもしれないけれども、サイバーセキュリティとサイバーディフェンスという2つの使命を考えると、トップはそれぞれミッションが違います。ところが、イメージとしては2つの大きなピラミッドが重なり合っているようなもので、トップのコマンドは明らかに違うのですが、オペレーションやインフラのようなところは共通点があります。その全体像をきちんと定義しておいて、それぞれの関係が各レベルでどうなっているのかを明らかにすることが重要です。例えばオペレーションとして重要インフラを担っているというのは、両方に関係することがあります。また、コマンドとしてトップの使命がどういう形でどういう判断をしていくのかに関しては連携をしなければいけない。

このような全体構造の定義ですけれども、経済産業省は当然サイバーセキュリティに関しての産業的な責任があるかと思えますが、国全体としてはその両方の責任があって、この問題がなかなか難しいといっているといつても何も進まないのです。サイバーセキュリティとサイバーディフェンスに関してきちんと定義して、役割を考えていく場所が必要だという議論がほかの国ではありますが、日本ではあまり議論する機会も場所もなかったように思います。ご専門の方がいらっしゃるのので、このあたりをどのように進めればいいのかを含めてお考えいただければと思います。

もう1つが、これも余り言及されないのですけれども、アメリカでのネットニュートラルティー（インターネットの中立性）の動きをみていると、トランプ政権になってからがらりと変わりそうな感じがしますが、まだわかりません。ただ、さきほど松本先生がご指摘されたように、将来使うためにいろいろとデータを取り、後からそのデータにアクセスできるようにしておくような回路は、確かにハードウェアの中に沢山あるのです。それが

そもそもハードウェアトロージャン（トロイの木馬ウイルス）なのかという議論はあるのだけれども、これは通信機器の中でいうと、やはりネットニュートラル、すなわち業界が何をどこまで見て・変えていいかという議論になる。DPI(Deep Packet Inspection)のような技術は発展してきており、実際に使われていることも、使うとよいサービスができることもわかっているのだけれども、別の使い方もできるのではないかという議論は多くあるのです。

ネットニュートラルティーの判断は、アメリカではFCCが行うけれども、ISPがこれをやっていいとか、データセンターではこれをやってはいけないとか、ユーザーに対してこういうサービスをしなければいけない等、それに依存して、誰が何をできるかが変わってくるのではないかと思うのです。

つまり、サイバーセキュリティとネットニュートラルティーの議論は、かなり関係が深いのですが、サイバーセキュリティの議論をするときにネットニュートラルティーの議論をしましょうということは余りいわれてはいません。さきほどのハードウェアの発注のお話で、設計したものを発注して、戻ってきたものに何か仕掛けられているというようなことを心配し始めると切りがなく、何かそれをチェックするようなことができるのかもしれないですが、それに加えてこのような議論も必要かと思いました。

もう1つだけ気がついたところを申し上げておくと、製造物責任に関して、さきほど岡村さんにおっしゃっていただいたと思います。要するにハードウェアをつくっていくときに、世の中には既にチェック機構があり、その中にサイバーセキュリティや個人情報のことを組み込んでいくことで、ルールの横の調整のようなことができるのかと思います。

それから、幼児教育は唯根さんにおっしゃっていただいたけれども、先生と親がアクセスに関しての定義ができる仕組みをもった子供向け携帯電話が最近売れ始めたというお話を伺いました。子供向け電子教科書のマーケットはアメリカでは結構発展しており、調べると、やはり子供達を守るためにアクセスを管理するような発想が入り込んでいることがありまして、こういうところも確かに考えていかなければいけないところかと思いました。

今どなたも名前の札を立てていただいていたので、少し余計にお話ししました。  
○夏野委員　おくれてきて、済みません。1点、オープンデータについてなのですが、オープンデータで今政府が持っているデータをどのように開放するかという議論が各省で進んでいると思うのですが、これにつけ加えて、今後センシングするものとか、今後整備するものがいっぱい各省であると思うのです。例えば河川につけているセンサーの

話とか、トンネルとか、ああいうところにつける。そういったものも、最初の設計時から後に開放することを想定したAPIの設定とか、そういうのをマニフェストすることは無理だと思うのですけれども、働きかけをここに1つ入れておいていただくといいかと。特にほかの省庁ですね。特に文科省とか、ぜひそういうのを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。私は内閣のデータ流通環境整備検討会オープンデータワーキンググループの主査でもあるので、申し上げておくと、今、各省庁がデータベースをつくる際、基本的にはオープンデータにしないと予算がつかないよう、政府CIOがチェックをする仕組みになっているのです。デバイス等の情報まではいっていないけれども。税金でデータベースをつくるといたらオープンデータを検討しなければならないので、それは一歩前進なのです。

確かに、センサーからのデータや、さきほどお話がありましたJAXAのデータなどは、これから大変役に立ちます。先日、シリコンバレーの話聞いていたら、NASAのデータを使って空から農作物の状態を把握して、それを分析すると、農作物の生育状態や病気がわかるという、NASAのデータの農業利用の例がありました。そういう意味ではいろいろな産業にまたがった貢献ができるのではないかと思います。

そのほかいかがでしょうか。では、喜連川先生。

○喜連川委員　安全保障の問題は非常に深く、原則今回の決定はオフenseに対する技術はだめというのは当たり前なのですが、ディフェンスも明確になったわけです。コンピューターというのはそもそも弾道計算から始まっていますから、ジェニユイン、軍事技術ですと。これ、嫌だといったとき、コンピューターなしの世界になりますけれども、それでいいのですかという話をいろいろ根源的に世論をつくっていく必要がある時代になってきているのではないかという気がいたします。それが1点。

それから、先ほど来、データの話が出ていますけれども、知財本部長の中でようやく一応整理がなされているわけです。一言でいいますと、データは財産権が認められないということで、対処策としては不競法の改正。もう1つは、これは非常に重要なのですけれども、経産省で情報大航海プロジェクトで100億円以上を投入していただいたおかげで、データの解析が著作権の制限規定に入った経緯があります。これのおかげで、いわゆる解析、ラーニング、学習のためのデータセットに対しては著作権を制限できるというところまで何とか解釈をしようというところが現行のぎりぎりのラインだと理解しています。

ただ、私の論述は、大学で、あるいは最近だと中学生もそうかもしれないのですけれども、

教えるときはプログラムとデータしかない。つまりデータはコンピューターサイエンスにとって物すごく大きなエンティティで、そのデータが不正競争防止法、トレードシークレットというのでまとめられるのは、データで生涯を送ろうとしている一研究者としてはすごく切ない。コンピューターサイエンスでなくても、私の人生このデータという研究者は山のようにいるのです。そうすると、法律屋さんからの論拠は、日本だけで法制度をつくっていても、そんなもの何の役にも立ちません、グローバルにみんなが共有しないと法律は意味がないのです。そのとおりなのです。

したがって、ショートタームの法的なリアクトと、でも、ロングタームにみると、どう考えてもおかしいので、そこはいろいろと国際協調しながら、自然な枠組み、これはぜひ日本がリーダーシップをとっていただければと思っております。

きょうは皆さん発言するのが嫌なのか、時間が有り余る。1つの理由は、こんなにたくさん資料をつくられるからではないかと思うのです（笑声）。東大の学生でもこんなもの咀嚼できないのではないか。

最後が教育のことです。先ほどのまともな人材が育っていないのではというご意見は、私もそのとおりだと思っています。これも5月の連休、暇で、じっと新聞をみていましたら、インフォシスがアメリカで雇用を創出するといったときに、アメリカのニュースでは結構おもしろい情報を出してしまして、インドのプログラマーを調べてみると、これはインドが発言しているところがおもしろいのですが、まともにロジックを考えてしっかりプログラムできるのは、5%以下しかいないとのこと。1回日本も、しっかりしたクオリティを測ってみてもいいのではないかという気がしますので、その辺をお考えいただくのが重要かというのが1つ。それから、最近の中で一番おもしろいかと個人的に思っていますのは、やはり一番最後にありましたE d T e c hでして、アメリカで1時間の講義をつくるのに7,000時間をかけますというのが最近聞いてきておもしろいなと思いました。7,000時間を投入すると、完璧に落ちこぼれはないということです。そうすると、そこら辺のそこそこの先生は要らなくなり、このコンテンツで全て用が足りることになります。結構すごい教育革命になる可能性があります。ここがビッグデータなのです。つまり、この子が落ちこぼれるとか迷ったというデータを全て上げていくと、ほぼホールカバレッジになるところになります。

ただ、ややこしいのは個人情報です。ゲイツ財団も100ミリオンぐらい捨てているわけです。こういうレギュレーションの問題も、ぜひ真剣にお考えいただく必要があって、個

保法の研究と同じように、学生、あるいは子供の将来に対してよかれと思いながらデータ解析をすることと、先ほどの村井先生のネットニュートラリティーの話と似ているのですが、今技術の境目が非常に難しいです。政府の場でしっかりご検討いただきたいと思います。

ありがとうございました。

○村井委員長　ありがとうございました。

それでは、松本さん、お願いします。

○松本委員　先ほどのセンサーからのデータというお話があったので、前回も少し申し上げたつもりなのですが、データの品質、あるいは信頼性をどうやって確保するかという課題の中に、センサーそのものがだまされないことに係る重要な課題があると思っております。

「計測セキュリティ」という言葉であらわされている領域なのですが、例えば自動車が前方に何か障害物があると認識して自動ブレーキをかけるとか、そのほか、自動走行においては、さまざまなセンサーからのデータを集約して、高度な判断が行われなければなりません。あるいは、ビッグデータ処理においても、たくさんのセンサーからのデータを集めてきて処理をするわけです。そもそもの入り口のデータが多少狂っていても大丈夫であるように処理は工夫されるとしても、丸っきりだまされてしまうようなことに関しては問題があります。このような問題の存在は指摘されているのですが、まだ研究が十分に進んでいない状況ですので、いずれ大きな課題になるであろうと思われれます。ぜひこのような観点も入れておいていただけるとよろしいかと思います。

○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　先ほど喜連川先生がおっしゃった点なのですが、ご安心いただきたいのは、既存の営業秘密の枠を飛び越えて、どこまで保護できるかということで頑張って検討作業を日本が世界に先駆けてやろうという形でやっております。ただ、いろいろな意見があるのも事実で、調整をしつつ進めているところが現状でございます。

その前の話に戻るのですが、実はちょうど2003年ころに、土居範久先生が中心になられて「情報セキュリティ総合戦略」を経済産業省で策定しましたが、その際にナショナルセキュリティという観点を入れるべきではないかという議論があったと思います。その点では多少は先見の明があったのかと思います。ただ、セキュリティというよりはイン

テリジェンスというようなものとの境界線みたいな状態になっているのも事実ではなからうかと思えます。

ところが、この間も、ある中小の公的団体の方とお話をしていましたら、セキュリティはどうしておられるのかと尋ねると、事務室に裸のままサーバーが置いてあると。クラウドも使っていないという程度だと。C I O、C I S Oを誰がやっているのですかと聞いたら、その団体のナンバー 2 の幹部ですと。その幹部は技術がわかるのですかと。沈黙されておられましたけれども、どういう理由からですかと聞いたら、やはり要は人、物、金を動かそうとすると、幹部クラスに担当させざるを得ないのだと。また、なかなか専門家を雇うだけの余裕がないのだということをおっしゃって、納得したわけではないのですけれども、それなりになるほどなと思った次第です。そういうギャップが現実にあることもご認識いただければと存じます。よろしく申し上げます。

○村井委員長　　ありがとうございました。

丸山さん、どうぞ。

○西川委員代理（丸山）　　面的展開について、一言だけ申し上げたい。そもそもファーストよりは面的展開のほうが非常によくわかるかなという気がいたします。

I o T が適用できる領域は物すごくいっぱいあると思うのですが、私はどちらかというと機械学習のほうが専門で、今、深層学習のテクノロジーは、実は適用できる領域が物すごくいっぱいあって、いわゆるローハンギングフルーツだらけなのです。これを誰が早くとりにいくかがすごく大事なのですが、その際に、面的展開でおっしゃっているような事例の収集とか、

そういうことが大事だと思います。

さらに事例をベストプラクティスの形で体系化することが極めて重要で、さっきの話に戻りますけれども、1960年代にソフトウェア危機といわれて、そのときにソフトウェア工学というのができたと聞いていますが、同じように、機械学習工学のようなディシプリンがこれから必要なのではないかと思います。ですから、こういう国の取り組みの中で、ベストプラクティスが体系化できれば、それをベースに機械学習工学のようなものをリードできるのではないかという気がいたします。

以上です。

○村井委員長　　ありがとうございました。

それでは、有賀さん。

○有賀委員 先ほど喜連川先生のお話を聞いて思い出したのですけれども、制度的には2019年度から専門職大学がスタートするわけです。その例示の中でもIT人材育成というのは一番先に挙がっているわけです。この人材育成の中で、それはどう取り組むのかというのは、やはりこれは考えておかなければいかんことではないか。770校もあってろくな人材が出てこない現状にさらに大学をつくって、コードをかけるやつが7%いればいいのですけれども、1、2%もいかなかったら、これは何のために制度をつくったかということで、しかも従来型の各種学校の延長線上になるのか、それともいわゆる高等専門学校の非常に熱心な連中がプロ的に育っていく延長線上でいくのか、これによっても人材供給源としては非常に違ったものになってくるだろう。この中には、そこにまだ触れられていないので、先ほど村井先生がおっしゃったように、欠けている部分の1つかなと思ったものですから、発言いたしました。

○村井委員長 ありがとうございます。

夏野さん。

○夏野委員 これ、いろいろな政策が入っていて非常にいいと思いますけれども、面的に展開していくと、絶対穴が出てくると思うのです。その穴をどうやって発見するかが、結構抜け落ちるところがこれから将来的に出てくると思うのです。一方で、ユーザーから見ると、こんなところでこんな変なデータのオープン形式になっているけれども、こんなものでは使えないと思っても、いうところがないのです。なので、これは経産省につくるのか、内閣府につくるのかわからないですけれども、消費者庁みたいな存在。つまりここがこんなことになって、これはおかしいのではないかというのを受け付けるような窓口みたいなものをつくって、そこでリスト化したものを各省庁で潰していくみたいなことをやはり制度化したほうがいいのではないかと思います。

ちなみに、この間、恐ろしいことがわかったのですけれども、渋谷区役所の不動産課はメールを受け付けられないのです。東京都の都税事務所は、インターネット上のメールは、職員同士のクローズドなものしか使えない、つまりインターネットではないということなのです。そんなのがこの2017年にあること自体がめちゃくちゃで、書類1つPDFで送りますといたら、うちは受け取れないのですというわけです。では、それをどこに文句をいったらいいのだろうというと、ないのです。なので、そういう全体的にそれを受け付けるところをどこかにつくるといいと思いました。

先端事例からプリミティブ事例まで。

○村井委員長　　ありがとうございます。

それでは、時間も大体まいりました。活発にたくさんのご意見を出していただきまして、ありがとうございました。

本日は、今後の情報政策の方向性と、I o Tの面的展開の推進についてご議論いただきました。幾つかの方向性は、新しい知恵が必要で、先手を打っていかなければいけないとか、少し先を見てやらなければいけないことがあるというのは方向性としていいと思います。

一方では、インデックスがやはり必要だと思うのです。さきほど海外の話も出ていましたけれども、私も先日、北京へ行って驚きましたが、自転車全部3色のシェアリングバイクになっているのです。海外ではいろいろ進んでいるところもありますので、そういうものを含めてグローバルなインデックスをつくり、それできちんと評価をしていくことが、行政では常に重要かと思いましたが、このあたりも考えていただきたいということだと思います。

そのほか、いろいろなご意見をいただきましたけれども、事務局でよく検討していただき、またこの次へ続けていければと思います。

それでは、安藤局長からご挨拶をお願いいたします。

○安藤商務情報政策局長

今、皆様方の話を聞いて、ちょっと2点だけ気づいた点を申し上げたいと思います。

前申し上げたと思いますが、やはり我々の仕事の仕方は、ユースケースを発掘して褒めるのですけれども、下手すると褒め殺しにしてしまったり、褒めた後、放置状態にして、後は野となれ山となれになってしまうというケースがすごく多かったと思うのです。そういうことの1つの反省で、やはり社会に展開して何ぼのものだということをもう少し考えなくてはならない。それがファーストという言葉から面的展開ということだったと思います。

きょう、あまり個別具体的な事例はご紹介していませんが、医療分野への展開です。やはり最後は、いろいろな診療報酬体系とか、そっちのほうへの制度へ落としていくことを、世界の技術を使ってどう証明していくのかということのコンビネーションとして、制度に展開して全国に落としていくことが大事だと思っております。

他方、そういう議論をやっておりますと、前も別の場でご議論させていただいたかもしれないのですけれども、本当にどういう社会の実態があって、ニーズがあるのかを掘り込

んでおかなければいけないという議論になってくるわけです。ところが、これは我々のような想像力の乏しい人間がやってしまうと、物すごく陳腐な世界観にとどまってしまっているのではないかという反省があるわけです。

先ほど前半にお話があったみたいに、少し待っていただきたいと。現実はずっと飛んでいるのではないかというところの認識が、私たちの創造力が乏しいと、本当にニーズはあるのだろうと思って掘り込んでみていってしまうと、産業構造の変化が全くみえていないところに焦点を当てたような議論を展開しているのかということが時々自己反省みたいになってくるわけでありまして。

したがって、やはりもっと創造力をもちながら考えなければいけないと思いながら、そういうことの裏返しとして、ぐさりとする話とか、手のついていない分野にもっとチャレンジしろと。経団連さんから、民間の提案を待つまでもなくというお話もいただいているわけでありまして、我々からむしろ率先してプロアクティブな領域に一手を打っていくことがやはり必要かと改めて感じました。

それをまた行政ツールに展開していくと、やはり制度というものは、ご案内のとおり、いろいろな世の中の主体の人たちは物すごく固定的に捉えているわけです。税法一つとってもそうです。補助金もそうだと思うのですけれども、責任主体がしっかりとした法人格として存在して、そこにその人たちの役割がおのずと決まってしまうわけです。製造物責任といっても、製造者と消費者がおのずと色分けされてしまっているというのがあるわけでありまして、現実はそのほとんど溶けている状況なので、そういうものに対して行政手段を展開していく場合は、これまでの行政ツールのあり方をかなり考えていかないと、発想は最大限頑張ったとしても、具体的にやっていく施策がピンを外れてしまうことがあるのではないかという感じがしております。

それと、サイバーセキュリティの関係でいろいろお話がございました。まさに大変重要なご指摘だと思っております。きょう、私どもはここでご紹介する立場にありませんが、先ほどのいろいろな周辺状況も含めて、今、内閣官房を中心として、村井先生などはインナーでやっておられるけれども、少しこれまでは入り込めなかった領域もいよいよ検討しようかとなっているのではないかと仄聞させていただいております。

それで、きょう、センターという話をちょっとご紹介させていただきました。センターは、どんがらをつくるというだけではなくて、攻撃側、防衛側にかなりしっかりとロールプレーをやろうと思っております。攻撃側の方の知見は最大限生かした実践に近い演習

を相当重点的にやろうと思っています。ですから、1年ぐらいかかってしまうわけであり  
ます。

そうすると、攻撃側の方の意見も聞いていると、やはり一番最小コストで一番簡単な攻  
撃の仕方をするのが基本というわけですから、余り机上の空論で難しい侵入の仕方を考え  
るのではなくて、先ほどのような形で、実はUSBを差し込むこととか、国家が関与した  
ような、連中たちからすると、先ほどのネットの世界でもありませんけれども、攻撃もリ  
アティーをできるだけ念頭に置いて、重要インフラの皆さん方に実践に近いような形で  
研修させていただきたいということを思って始めます。試行錯誤の繰り返しになっていく  
と思います。

その中で、いろいろなことをやはり制度の中にビルトインしてセキュリティを重視して  
いく中で、実は一番の悩みは、私たちの能力の問題があるわけです。これまでは電力とか  
ガスの保安規定は、何ボルトとか、何メートルか、圧力とか、電圧が書いてあった世界で  
済んだわけですがけれども、そこにサイバーが入ってくるとなってくると、法の執行をやる  
我々、あるいは現場がこの世界を熟知していないと制度の設計も執行もできないとなっ  
ております。実は経産省の中でも今そういう問題意識のもとで、地方局等々も含めて、サイ  
バーを念頭にしっかりと置いたインフラ整備のための法整備の執行のあり方を、どうい  
う手だてを講じていかなければいけないのかも含めて検討させていただいております。

また皆様方のいろいろご指導、ご鞭撻を賜ればと思っておりますので、よろしくお願  
い申し上げます。

○村井委員長　　どうもありがとうございました。

それでは、委員の皆様のご非常に活発なご議論をありがとうございました。これをもちま  
して、産業構造審議会商務流通情報分科会の第10回情報経済小委員会を閉会させていた  
だきたいと思っております。どうもありがとうございました。

――了――