第6回 テクノロジーベースの規制改革推進委員会 議事録等

（開催要領）

１．開催日時：令和5年9月11日（月）10:00～12:00

２．場　　所：オンライン開催

３．出席構成員：

座　長	江崎 浩	デジタル庁 シニアエキスパート
構成員	岡田 有策	慶應義塾大学理工学部管理工学科 教授
	小川 恵子	EYストラテジー・アンド・コンサルティング株式会社 バンキングキャピタルマーケットリーダー レグテックリーダー パートナー 公認会計士
	荻野 司	一般社団法人重要生活機器連携セキュリティ協議会 代表理事
	加藤 真平	東京大学大学院情報理工学系研究科 特任准教授
	川原 圭博	東京大学大学院工学系研究科 教授
	川端 由美	ジャーナリスト 戦略イノベーション・スペシャリスト
	島田 太郎	株式会社東芝 代表執行役社長 CEO
	鈴木 真二	公益財団法人福島イノベーション・コースト構想推進機構 福島ロボットテストフィールド 所長 東京大学未来ビジョン研究センター 特任教授
	染谷 隆夫	東京大学大学院工学系研究科 教授
	豊田 啓介	東京大学生産技術研究所 特任教授
	中垣 隆雄	早稲田大学理工学術院創造理工学部 教授
	永井 歩	アスタミューゼ株式会社 代表取締役社長
	根本 勝則	一般社団法人日本経済団体連合会 参与
	登 大遊	独立行政法人情報処理推進機構 サイバー技術研究室 室長
	平本 健二	独立行政法人情報処理推進機構 デジタル基盤センター センター長

（議事次第）

１．開会

２．議事

（１）構成員の変更について

（２）事務局からの説明

・「テクノロジーベースの規制改革」の進捗及び当面の進め方

（３）岡田構成員からの説明

・公共サービスにおける技術戦略 イノベーション・マネジメント

「第一期 SIP の経験を踏まえて」

（４）経済産業省 商務情報政策局 サイバーセキュリティ課からの説明

・経済産業省のサイバーセキュリティ政策について

（５）意見交換
３．閉会

（資料）
資料１　テクノロジーベースの規制改革推進委員会 構成員
資料２　「テクノロジーベースの規制改革」の進捗及び当面の進め方
資料３　公共サービスにおける技術戦略 イノベーション・マネジメント 「第一期 SIP の経験を踏まえて」
資料４　経済産業省のサイバーセキュリティ政策について

〇須賀参事官　時間となりましたので、第６回目のテクノロジーベースの規制改革推進委員会を開会いたします。今回も構成員の皆様にはオンラインでご参加をいただいております。後半にまとめて意見交換の時間を設けておりますが、これまでと同様、Webex のチャットを活用して、説明の最中などでも随時、皆様からのご意見、ご質問お願いいたします。

それでは、これ以降の議事進行につきまして、江崎座長にお願いしたいと存じます。よろしくお願いいたします。

〇江崎座長　皆様、おはようございます。それでは議事に入らせていただきます。第６回の議事といたしましては、今お見せいただいた議事次第のとおりです。まず、事務局から本委員会の構成委員の変更についてご報告させていただきます。続いて、同じく事務局から、テクノロジーベースの規制改革の進捗及び当面の進め方についてご説明させていただきます。次に、岡田構成員から、公共サービスにおける技術戦略イノベーション・マネジメント「第一期 SIP の経験を踏まえて」に関してお話しいただきます。その後、経済産業省商務情報政策局サイバーセキュリティ課から、経済産業省のサイバーセキュリティ対策についてお話しいただきます。最後に本日の議題全てに関しての皆様方からのご自由なご発言、ご質問、ご意見等の交換の時間とさせていただきます。

それでは、まず事務局から、本委員会の構成員の変更についてご報告をお願いいたします。

〇須賀参事官　資料１をご参照ください。今回より、今年新たに立ち上がった独立行政法人情報処理推進機構デジタル基盤センターのセンター長になられました平本健二様に構成員として新たにご参加いただくことになりました。平本様、今後どうぞよろしくお願いいたします。ご報告は以上です。

〇江崎座長　平本様はデジタル庁でも仕事をしていますけれども、またご一緒に仕事をすることになります。よろしくお願いします。ご挨拶等は、質問等の中でお話しになるときに、簡単に自己紹介をしていただければと思います。

続きまして、テクノロジーベースの規制改革の進捗及び当面の進め方についてのご報告を事務局からお願いいたます。

○須賀参事官　続きまして、資料2です。いつもどおり、テクノロジーベースの規制改革のこれまでの検討の進捗と今後の進め方についてご報告させていただきます。

1枚めくっていただきまして、ここは委員会の概要、次のページは全体像を復習のためにお付けしております。次のページが議題です。これまで5回にわたりいろいろご議論いただきました。1つ目は、技術検証について、第1弾から第3弾に分けて公募を行うと申し上げておりました。いずれも実施に至りましたのでそのご報告です。

2つ目が、テクノロジーマップの縦軸と横軸について、いろいろとご議論いただいていました。この形で当面進めたいということで、今回成案をお諮りしたいと思います。

3つ目が技術カタログです。特に一番大きいのが、今回経済産業省サイバーセキュリティ課からもプレゼンをいただきますが、サイバーセキュリティ関係のカタログ掲載項目を追加したほうがよいのではないかというご指摘をいただきまして、そちらのご提案をさせていただきます。その追加を踏まえまして、今後どういった形でカタログの公募を随時行っていくかについてもご報告いたします。

最後に、コンソーシアムの運営を開始しておりますので、そのご報告と、最初のイベントとなるRegTechDayの日程も含め、今回ご提案させていただきたいと思います。

まず、技術検証事業のお話です。前回までにご報告しましたとおり、1万のうち1043条項に関して技術検証が必要と規制所管省庁がおっしゃっていました。それらをまとめていきますと14の検証類型に大ぐくり化できることが分かってきました。その14の類型に沿いまして、各府省庁連名で実証に入っていただく手続きを調整しておりました。連名となっている府省庁の中には、前回ご報告したとおり、自治体から代表して大分県に入っていただいて一緒にやっております。対象の条項数は、国の条項数の隣に記載の括弧の中が大分県の条項数となっております。全体としてかなりたくさん相乗りいただいている類型と、結局、単品でやらざるを得ないところがある状況となっています。

第1期の技術検証公募として一番始めに公募要領を書いた赤色の5類型については、既に技術検証の担い手の公募が終了しており、実証にこれから入ってまいります。第2期をブルー、第3期を黄色で示しています。いずれも6月から8月にかけて公募を実施したところです。

次のページからが類型、技術検証の概要、その対象となる法令の具体的な条項、そして実際に性能をテストする技術が具体的にはどういったものかの一覧表です。各類型について、まずはこういう性能を確認してほしいという詳細な仕様書を各規制所管省庁と調整し、それを公募しました。現在、検証を主導していただける事業者の公募が終了した段階です。ここから事業者と規制所管府省庁の方と対話していただいて、具体的な進め方の詳細をかためて、順次、実際の検証に入っていくことになります。非常にコストのかかるプロセスですけれども、1つ1つ大変丁寧に各府省庁にもおつき合いいただいて進めております。

第1弾、第2弾は前回までにご説明したので飛ばしまして、11ページからが第3弾で、最後にまとまったものです。公募期間が8月4日から25日という夏に実施させていただきました。例えば、類型2は非破壊検査の技術を使って、地盤面下や接触不可能な場所に存在するような設備の定期点検を求める規制について、技術代替ができないかという検証に臨んでいただきます。類型

4 は、施設の内外にある設備や機器の不備、劣化の有無を目視で確認するように求める規制について、センサーで代替ができないかというものの一部を対象にしております。

次のページから、IoT やセンサーを活用して設備の作動状況の定期点検を行うことについて技術代替ができないかということ、類型 10 が、大気や水質等の環境情報について、採取した試料に基づいた定期検査を常時点検に置き換えていけないかということにチャレンジしていただきます。

次に詳しいご報告ができるのは、こういう検証を始めましたという段階になり、しばらくお時間をいただければと思います。

次のページからがテクノロジーマップについてです。14 ページになりますが、まず縦軸です。もともと見慣れたテクノロジーマップは、右下に書いているとおり、縦に 7 類型と我々が申し上げているアナログ規制の代表格を並べました。それについて共通の機能を書き出して、どういった機能に対してどういったテクノロジーの代替可能性があるかを大ざっぱにマッピングしてまいりました。

次のページですけれども、規制の構造については前回ご説明したとおり、規制の目的があり、その目的を果たすためにどういった機能をどういった手段で満たしていくかという構造になっています。その構造がそのままマップに表現できるように、規制目的と、その規制を達成するための手段が一覧になるようにします。

次のページは規制の基本的な構造です。非常におもしろいことが分かってきました。デジタル臨調で抽出した 1 万条項の全数分析を三菱総研にしていただきましたところ、あらゆる規制がほぼ同じ構造になっていることが分かってきました。まず、規制の目的が一番上にあり、一番下に規制の管理対象、安全を確保したい対象などがあります。この管理対象に関する情報、データを誰かが取得します。それが健全な状態なのか、劣化しているのか、さびているのか、ひび割れしているのか、そういった情報を誰かが取得します。そしてその取得した情報を誰かに伝えます。次はこのピンクの判断主体という人たちが入ってきて、この状態がまずい状態なのかの判断をします。この判断結果が、次の対応主体に伝達されます。伝達された対応主体が、その判断に基づいて早く補修をしなければいけないなら瞬時に補修に入るなど、事態に対処していきます。同じ主体が幾つかの役割を果たす場合ももちろんあります。基本的には全ての規制はこのように、データを取得して、判断なり、対応なりをしていくというループを回すことを求めていることが分かってきました。

次のページです。この規制の基本構造を踏まえますと、テクノロジーマップの横軸は、IPO モデルに従って、インプット、プロセス、アウトプットと整理するのがよさそうです。すなわち、まずは管理対象のデータを取得し、セキュアに遠隔地に流し、伝達する。そして、その次のフェーズとして判断する。その判断に従って、最後のアウトプット、対処、対応をしていく。こういった構造にしますと、おおむね全ての規制がうまくプロットできるだろうと考えております。

次のページが、各要素の条文上の記載率を 1 万条項に対して全数チェックしてみていただいたものです。要は、何のデータを誰がとって、どのように判断、伝達していくのか、それぞれの要素をどのぐらい条文上読み取れるのかということをチェックしていただきました。赤い色、暖色系は記載率の高いもので、緑に近いものがほぼ条文上は読み取れないという意味です。例えば管

理者に特定の場所の状況を資格者が確認するようにと求めているような規制がありますが、具体的にどういった場合にどのように対応するのかは、試験の内容で恐らく確認をされているので、規制の条文を見てもそれは読み取れないということです。分析の結果、表の左側の管理対象や判断に関する情報の一部については、条文の文言上確認可能、あるいは類推可能なものが多かったということがわかりました。

以上の構造を踏まえまして、19 ページからが縦軸の考え方です。従来のテクノロジーマップは、規制所管省庁の方にも分かりやすいように、アナログ規制のキーワード 7 項目、7 類型を縦軸に置いていました。これを修正してより網羅性を高めようというときに、先ほどの規制の構造に従いますと、最も記載率の高い「管理対象」を主軸に大きく類型化していくのがよさそうです。一体何の管理対象についてどういうデータを取得しなさいと条文に書いてあるのか、それはどんな判断や対応を期待してのことなのか、そういった順番で整理をしていこうというのが縦軸のパターン 1 です。

縦軸のパターン 2 については、従来案のように規制類型のキーワードにひもづいていたほうが、規制所管府省庁はご自身の見るべき場所が見つけやすいというご意見がありました。そこで引き続きその構造も維持するということで縦軸パターン 2 にしております。当面、パターン 1、2 を維持しながら、前回難しいご指摘もいただいて、今、事務局で悩んでいるところですが、いろいろな追加のパターンも検討していきたいと思っているところです。

次のページからが、この縦軸のパターンに合わせますと、こういったマップになるというものです。ネット上で見ていただく想定で、1 枚の紙に収めることを想定していないので、非常に見にくくなっております。何らか表としてお出しする際には、もう少し大ぐくり化をして、皆様が見る気が起きるようなものにしたいと思っておりますが、拡大して見ていただくと、各部分がかなり精緻につくられていると思います。現時点で把握している技術情報を、ご提案した縦軸・横軸にプロットすると、こういったマップになっていきます。

さて、テクノロジーマップでそれぞれのプロットされたテクノロジーの裏にあるべきものが技術カタログということなります。23 ページからはカタログの話で、1 つ目はサイバーセキュリティの話です。

技術カタログをつくるプロセスですが、こういった分野に適応可能そうなテクノロジーを教えてくださいと分野を限って公募を何度かかけていくことにしておりました。カタログ掲載情報は技術保有機関から提案いただき、いただいたものについてはその製品、サービスが既に調達可能な状態でマーケットインしているかという最低限のチェックだけをデジタル庁が行い、すぐにカタログに掲載して、スピード重視で表に出していくというのがもともとの私たちのご提案でした。今回新しく 24 ページで、青字で示していますけれども、「公募結果の事前確認」というプロセスを追加したいと思います。ご提案いただいた製品、サービスがお勧めするに足りるものなのかという観点でのチェックをやはりするべきだろうというご意見が多くあったことをふまえ、提供された製品やサービスの情報について、「技術カタログ運用タスクフォース」という場を設置いたしまして、そこでサイバーセキュリティやサプライチェーンリスクについて最低限の確認をしていただいてから、カタログとして掲載するという形に変更させていただきたいと思っております。

具体的には、次のページです。サイバーセキュリティやサプライチェーンリスクの状況は刻々と動いていきますので、常にこのやり方でというよりは、グローバルにも国内にも随時状況を見ながら運用を変えて柔軟にやっていくということになります。もともと、カタログに掲載される製品やサービスは、採用して何かが起きてしまった場合、デジタル庁でその結果責任まで負うことは難しいので、調達される方にしっかりと確認してほしいということで、それを規約に明示させていただく予定です。他方で、デジタル庁が法令に基づいて整備するテクノロジーマップの裏にひもづくカタログとして、デジタル庁のホームページにおいてこのカタログは公表されますので、最低限の信頼確保、提供情報の充実を図るべきであるということで、以下の取組を追加で実施させていただけたらと思います。

1つ目が、この委員会の下に、先ほど申し上げました「技術カタログ運用タスクフォース」を設けまして、技術カタログ公開前に、応募された入力情報の確認を行っていただきたいと思います。そのメンバーは、座長の承認を得て決定しますが、非公開とさせていただきたいと思います。

それから、技術を公募する際にカタログの掲載項目としてたくさん質問を用意していますが、その中によりサイバーセキュリティやソフトウェアサプライチェーンリスクに対応した項目を充実させるために、追加をしていくこともお諮りをしたいと思います。具体的には、個人データの保護について、保管場所はどこなのか、暗号化対策をしているのか、裁判管轄権はどこなのかといった情報を少なくとも聞くべきであろうというご提案もいただいております。それから、ソフトウェアのサプライチェーンリスクについては、ソフトウェアの特性、その特性を踏まえたセキュリティ対策をどのようにやっているかということを聞いていければと思います。

次のページですけれども、追加項目の考え方は、1つでも漏れていますとそこがセキュリティホールになってしまうということで、なるべく包括的な何らかのガイドライン、世の中に通用しているものに準拠したいと思います。日本のセキュリティ対策も含め、アメリカのNIST、国立標準技術研究所が出している重要なソフトウェアの定義及びその使用に当たっての5つのセキュリティ対策、それからソフトウェアの検証において推奨される11の最低基準というものが世の中一般に通用し参照されているということです。それを踏まえながら、応募者の入力のしやすさに配慮しながら最低限の項目を選定させていただきました。

次のページから4ページにわたりまして、具体的な追加項目のリストを載せています。

それから次は、ソフトウェアの検証に関する具体的な実施状況の確認です。いずれもチェックリストで確認いただけるように、なるべく配慮したつもりです。座長からも「サプライチェーンリスクに関して全体的にちゃんとカバーしているのかということを常に確認するべき」というご指摘をいただきましたので、その一覧表を整理しました。応募される段階ではまだ技術を使うことが決まっているわけではありませんので、さすがにそこまでは聞かないでよいというものは聞かないという判断をさせていただいております。この辺りも、コメントいただけるようであればぜひお願いいたします。

以上、このようにセキュリティの質問項目を充実させる作業を進めておりましたため、第2回のカタログ公募は往訪閲覧・縦覧ということでもう決まって質問リストも用意していましたが、しばらく実施を待っておりました。32ページになりますが、この第二弾カタログ公募をやっと9

月中に、以上のセキュリティ対策の項目を追加した形で実施したいと思っております。公募を行った後に、カタログを公表していけるのは10月以降になるかと思っております。カタログの質問内容自体は、セキュリティ部分以外は前回から変わっておりません。

第3回以降も続々とカタログの整備を進めていきます。技術検証も行い、その結果技術代替が可能だと分かったら、その後に規制を見直していただきます。そこからやっと技術の調達が可能になるということで、技術検証を要する類型は少し時間がかかりますので、技術検証はもういらない、技術があれば使ってよいと言われている部分を重点的に、まずはカタログ整備をしていきたいと思っております。

その観点から、33ページになりますが、左側に技術検証を要する条項が書いてあります。デジタル庁が取りまとめて実施をする技術検証と、各府省庁が独自で技術検証をやっていただくことになっているものがあり、その2つが技術検証を要する1043の条項です。それ以外の、右側の、技術検証が不要な、1万条項のうち大半の約8600条項について、カタログの整備を先行していくということを考えております。

次のページから記載されている第3回以降のカタログ公募に向けましては、新しくつくった縦軸に合わせて、1万の条項を全部プロットするという苦行を三菱総研にやっていただいております。その成果を生かして、公募についてもそれぞれの類型ごとにまとめてやっていければと思っています。準備が早く進みそうなのが、例えば目視です。施工、経年劣化、安全措置対策の状況などを目視や見張りで確認しなさいと言っているような規制の類型です。それから、主に屋外の環境の広域な利用状況や被害などについて、ドローンを飛ばすなどして把握しなさいと言っているような規制類型です。また、事業上の管理や業務状況などを実地調査などで確認しなさいと言っているような組織管理の類型です。この3つが、第3回で技術カタログの公募に入れられるのではないかと思います。

少し遅れまして、第4回と第5回でやっていくことになるかもしれないのが目視以外の規制です。施工や経年劣化の状況などを目視以外の手段で確認していくというものです。それから、カタログの類型の中で最後のものは測定や分析で、管理対象物をどのように網羅するかが課題です。いろいろなものの測定や分析が規制によって求められていますので、どう類型化して情報提供を求めていくのがよいかという整理が必要です。これは少し後回しにしつつ、順次カタログ公募も始めさせていただければと思います。35ページからは、テクノロジーマップのリストにカタログの公募類型をそれぞれ位置づけてみましたものです。

最後になります。40ページ以降がコンソーシアムの運営開始、RegTechDayのお話です。RegTechコンソーシアムは、何度かお話ししていますが、このマップやカタログというものを通じていつまでもデジ庁が真ん中に入って情報のつなぎをするのではなく、マップやカタログのステークホルダーである技術保有機関、規制所管省庁、規制の対象機関の皆様が直接、随時、必要な情報を共有していただける関係を構築できればという思いから、緩やかなコミュニティをつくっていきたいということでご提案しているものです。

41、42ページですけれども、このコンソーシアムでは関係者のネットワーク化、情報提供、学習の機会、最先端ではどういったテクノロジーがアンロックされつつあるのかなどについて必要に応じて学習していただける場があればと考えております。

次のページですが、RegTech コンソーシアムはひっそりと運営を開始しておりまして、既に、何のイベントも打たないうちから、100 名以上の方からご登録いただいております。コンソーシアム自体はコミュニティですので、Slack を立ち上げまして、そこでいろいろな議論を深めていただけるように場をご用意しております。このコンソーシアムの立ち上げイベントを RegTechDay と名付けて、今年の 10 月 27 日金曜日 13 時から 15 時、オンラインで開催したいと思っております。アナログ規制の見直しで経済効果が 3.6 兆円という数字も出てきておりますけれども、そもそもアナログ規制とはどういうものがあるのか、今後どういった技術が使えるようになるのか、あるいは今どういった技術検証をやっているのかなど、気軽に情報収集していただけて、関係者につながっていただけるようなイベントになればと思っております。委員の皆様にも、ぜひこの時間は押さえておいていただければ、今後いろいろなご相談を事務局からさせていただけてありがたいです。

45 ページがコンソーシアムの活動スケジュールです。前回もお示ししましたが、日程などを入れてアップデートしているものです。この RegTechDay を皮切りに、勉強会やピッチコンテスト、マッチングイベントなども引き続き企画していきたいと思っております。

最後の 46 ページが今後のスケジュールです。マップは夏に公表することが決まっております。夏も終わりの 9 月ですけれども、マップを何らか第 1 弾として、縦軸・横軸がやっと決まりましたので、お出ししていきたいと思っています。それから、技術カタログも先ほど申し上げたように、第 1 弾、第 2 弾の公募に続きまして、先ほど類型化したような形で続々と公募をかけて公表していきたいと思っております。技術検証は産みの苦しみのフェーズですけれども、事業者がやっと決まりましたので、その方々にこれから続々と技術検証を行っていただきます。そして、その合間に、コンソーシアムでコミュニティをつくり、盛り上げていくという形で進めたいと思います。

以上、事務局からのご報告でした。

○江崎座長　どうもご報告ありがとうございました。幾つか既に皆様方からご質問したいことがあるかとは思います。先にあと 2 つのプレゼンテーションをいただいた後に、最後にまとめて皆様方からのご意見、ご質問等を受けることにさせていただければと思います。事務局は大分苦労して作業を進めてきているということがお分かりいただけたのではないかと思います。

それでは、続きまして岡田構成員から、「公共サービスにおける技術戦略イノベーション・マネジメント　第一期 SIP の経験を踏まえて」ということで、ご説明お願いいたします。

○岡田構成員　本日はお時間いただきましてありがとうございます。

私は第 1 期の SIP のところでインフラ維持管理という、今もお話がありましたけれども、土木関連の新技術の導入のところでサブ PD として、特に出口管理のところでの仕事に 4 年間ぐらい入っていました。最初の 1 年間は別のところも入っていましたので、後ろの 4 年間、実際に開発された技術に対してのアウトプットの支援もさせていただきました。

その中において、最後のページに書いたような 4 つの事柄が、特に出来上がった技術を表に出すところで非常に苦労した部分です。今もカタログのことを含めて事務局側からお話がありましたけれども、我々が思っていたところも随分よくなったという感じもしています。少し重なると

ころもあるかとは思いますけれども、気になったところを、前回のSIP1期のときの経験を踏まえて、お話しさせていただければと考えております。私のいろいろな経験を含めてお話ししたい事柄ということで、このスライドで最後に整理し、まとめてお話しさせていただきます。

もともとインフラ維持管理というところで始まった理由は、2ページの左上のところです。実際に日本の中に、例えば橋は70万橋、トンネルは1万という数であるわけです。けれども、85%は地方自治体が持っているものです。ということは、いわゆる有料ではないです。そうすると、それに対する維持管理はどういうお金で払うかというと、いわゆる税金で払うことになるわけです。その税金が、実際にストックの量に対して見合う税収になっているかというと、もうそういうふうにはなってきていないということは、10年以上前から言われ始めてきています。笹子トンネル事故などもありましたように、インフラの維持管理をしっかり行っていかないと、社会安全にも非常に影響してくるということが言われておりました。実際には維持管理もできない橋が増えてきていて、トリアージというような言い方をしている自治体も出ています。本当に悪くなったら通行止めにして、使うのをやめましょうというやり方しかないものも出始めている現状です。

そういうことを踏まえまして1期SIPインフラが2010年から始まっています。このSIPインフラの中において新しい技術を開発して、ここでもお話になっていますけれども、いわゆるデジタル技術を中心にしながら、こういった社会的問題に対応しましょうということで、およそ60のチームが技術を開発して進んできた状態です。

ただ、それが進んでいる途中でも、2018年のジェノバの事故があります。実際にこういった町なかのインフラでも、通行規制などができずになかなか維持管理が進んでいないとこういう状態になってしまいます。このようにインフラ事故というのは世界各国で起こり続けている状態です。また、そのことが実際に社会生活にも大きな影響を与えるところが出てきていますので、非常に喫緊の課題として進んできているかと思います。

一方で、その技術というものを考えるときに、3ページですが、これはよく出てくるMOPのグラフです。横軸がTRLです。最近はBRLという言い方も出てきていますけれども、いわゆる技術水準を上げていくところです。実際に大学や研究所で行われているのは、この左側の基礎研究、応用研究と言われている部分が中心的になります。実際に今のSIPの場合も、公募の段階で入ってくる研究というのは、大体この辺りの優れた研究を選ぶことになるわけです。実際に出口ということになると、この一番右側の実用化、事業化という、いわゆるTRLの7、8、9辺りを狙ったものが必要になるわけです。

ただ、この辺りのところは、実際に大学もそうですし、いわゆる理研や産総研などの研究者もそうですが、研究者の日常的な活動ではなかなか直接的にそこを考えて行うということは、特に今から10年ぐらい前ではほとんどないような状態でした。そうした中において、最近ではこうした実用化・事業化を最終目標にしなさいと言われていますので、そこにいかなければいけないわけです。しかし、各研究チームにここまで行けとただ言ったところで、行けないというのが現状でした。先ほど出ていたような実証実験などもそうです。そのことも含めて、こういった研究開発から実用化・事業化に関しては、各開発チームにお任せ、これが条件ですと言っても、なかなかうまく動かないというのが現実です。実際には事務局側でこの辺りのTRLを上げていくという

ところを支援する必要性が出てきたのが、大体SIPの2年目ぐらいの後半から出てきた大きな問題点です。その辺りから、事務局の中において、SIPの技術のいわゆる社会実装化を支援するための様々な取組を、実際にプロジェクトチームの中心のところで行っていたわけです。

その中において、いわゆるアウトプットのこともよく出てきますけれども、4ページに示すビジネスモデルというものを考えるときに、よく出てくるのはB to BやB to Cになるわけです。とにかく、いいものを作れば売れる、いいものを作れば人が買ってくれる、あとはこれまでよりもコストを下がればいい、というような形で商品開発を行うことはよくあります。先ほど実際にインフラの場合には有料ではない橋やトンネルが多いというお話をしました。実際にそれを使うお金のもとが税金だということになると、いわゆるB to BやB to Cとは違います。

一番下にB to Gと書いてありますけれども、こういったビジネスモデルの中で問題を解いていかなければいけないところが出てきました。端的な言い方をすると、例えば自治体などでは単年度決算ということがよく出てきます。そうすると、維持管理のように中長期にわたっての予算を考える中において、今、例えば100万円払うと10年間安くなりますよということは、頭では分かっても、いわゆる担当の方は、私の権限ではできませんという形になります。このように、中長期の考え方を受入れてもらえにくいところが非常に大きな問題点として出てきました。コストカットという場合が典型例ですけれども、今年のコストが下がるということに関しては非常に喜んでもらえます。けれども、将来のコストを下げるために今、投資しましょうというような考えは、理屈は分かってもらえても、実際になかなか財布を開いてもらいにくいというところが出てきます。

また、もう1つ大事な点は機能要件です。実際には発注要件も考えればいい。これができればいいというところは出てきますけれども、実際に機能要件も立てておかないと、言葉は悪いですけれども、「安かろう・悪かろう」が選ばれてしまうことになってしまいます。ですから、実際には性能発注をある程度してもらうようなことを考えないと、いいものが買ってもらえなくて安いものが買われてしまうということになってしまいます。新技術導入の人たちの、ある意味インセンティブや途中でのやる気というものが損なわれてしまうことも多くありました。そういうことがあるので、B to Gという言い方をしていますけれども、こういったいわゆる一般的な地方行政のあり方をそのまま勉強するというよりは、地方行政のあり方も含めて、こういった新技術の導入の仕方を見据えて、いろいろな意味で導入の仕方に工夫を与えていくことが大事なのではないかというところが出てきたわけです。

それからは、実際に新技術を導入したときに、SIPのところでも最初は普通に技術の内容でというところで研究開発者たちがつくった内容のカタログをつくりました。ただ、これは非常に評判が悪かったようです。いわゆる学会の予稿集のような形になっていて、専門家でないと分からない、難しい用語があってよく分からないものでした。例えば地方行政の人たちから見たときに、何がいいのか、何ができるようになったのか、これまでと何が違うのかよく分からないなどと言われました。

ということで、見出しのように売り物とセールスポイントを書き、どういうところができますという形で、実際に読み手の立場に立ったやり方というのをつくり直していきました。ただし、これは研究者に全部やってくださいというのはなかなかできません。そういうことに長けた人た

ちによってチームを再構成して、カタログの内容やコンテンツを見直しました。さらにはユーザーの声、実際に現場の実証実験などで得られた声を入れていったわけです。

例えば、腐食の状態を検査で見るというものに関しても、実際最初に提案されたものとは別に、それを見たある行政で、例えば公園で犬の放尿によって電柱が腐食したところが出てきているというような自治体からの別のニーズがあり、それを使ってうまくいったということも出てきました。実際に実証の中において、いろいろな意味で活用方法や可能性も出てきます。そういったことも見ながら、どういったところで使えるということもいろいろ入れるというところでアップデートする形もとっていきました。

マルチコプタ、いわゆるドローンもいろいろな技術が出てきますし、いろいろな特徴が出てきます。ドローンの中において、目視点検しなくてもカメラで画像を撮って、このぐらいができるというのは簡単に見せられます。実際に橋の話になってくると、例えば風に対してこれは強い・これは弱い、海ならば強い・山ならばこれが強い、というような形で、様々な形でドローンにもいわゆる得意不得意というものが実際には出てきます。そういった長所・短所をしっかり見せながら、ある意味合わせ技で実際に検証していくようなこともやらないと、特に大きな橋などで言えば、ドローン１体で全部をカバーできるというのはなかなかできません。新技術の組合せのようなものをモデル化していくことも必要になってきました。

トンネルの中で実際に車が走りながら、いわゆるレーザーによって全体の状態を見るというもの、トンネル内の腐食状況や空洞状況なども把握できる装置もあります。これは本当に早い段階から出来上がったのですが、実は大きな問題点は、実際に似たようなものを中国が造ったことです。中国の中で走らされてしまったということで、非常に国際競争力が落ちてしまったということにもつながっていきました。もちろん、性能的にはこちらのほうがいいわけですけれども、先ほど言いましたように性能要求や性能発注をしっかりしておかないと、ちょっとしたバッタものの技術が入ってきてしまうとそこに負けてしまうということも出てきてしまいます。しっかりと新技術を支援していくために、新技術の性能をしっかりと評価し、それが性能発注できるような流れにもっていかないと、いいものを作った人が割をくうというしんどいところが出てくるわけです。

レーザー打音ということで、映像を撮るものではなくて、レーザーの発する音を分析する装置もあります。今、SIP2 期や 3 期のところも含めて、非常に成果が上がってきている技術です。ただ、こういったものに関しても、先ほど言いましたように、実際に使っていくためにはどのぐらいの状態でどういうところなら使えるのかというようなことも含めて、単なる技術の実証だけではなくて、どういったところでこのような技術を使うマーケットがあるのかというところも含めて見せていかなければ、なかなかうまくいかないということがあります。

同じような例として、トンネル内で打音も映像解析も全部一緒にするというものもあります。ガイドフレームにいろいろな計測器をつけるということで開発されたものです。道路の真ん中を車で走りながら測定できるものは、交通規制をするので大変だという話がありますが、このシステムでは交通規制が不要なので、新技術として非常にレベルが高いと我々も最初は推していたのですが、実際にこれを使うとなると、警察から前例がないと言われます。規制がなくても大丈夫といっても、何かあったら困るから結局規制してほしいというような形になってしまい、ある意

味売りが減ってしまうことにもなってしまいました。いわゆる前例がないとなかなか使ってもらえないところがあるので、実証実験をするのはいいのですが、実証実験が実験施設になってしまいますと、実際の現場の中では最初というところは怖がってやらないということにもなります。いわゆる実験場で使うだけではなく、どこかちゃんとした場所で使っていく、協力的な自治体を見つけて、まずはそこで実績をつくるということも、汎用化する上では非常に大事な点です。

衛星からレーザーを使って、実際に地盤沈下の状態を測るというものもあります。飛んでいる衛星で情報をとり、それを解析するということで、早いうちから実装化できたわけです。ただ、1つ大きな問題点になったのは、とられたデータが誰のものか、また特に地盤沈下になっていると、これが表に出ると非常に社会不安を誘発するという話にもなってきます。実際には、この企業との契約に基づくデータは、そのインフラの人たちがしっかり持って表に出さないというような形で進んできたということになります。こういうふうにデータがクローズ化されてしまいますと、例えばAIなどへの学習データとしては使えないということになってきます。こうしてとったデータを含めて、将来的な学習に使っていくということはなかなかしにくいということにもなってきます。

ドローンでとったデータもそうですけれども、どうしても維持管理のデータとなると、クローズにしたいというところも依然としてあります。データのオープン化、あるいはデータの一部、本当の完全なオープン化ではなくて、あるところまでオープンにするなど、取得したデータのオープン／クローズの範囲というところを見てあげないと、どうしても安全に寄り過ぎるとクローズになりやすく、オープンにしたくないという心理が働いてしまいます。実際にデジタル技術としては、いわゆる効果半減のようなことになってくるところは否めません。ですから、そういったところで実際にとられたデータをどこが管理して、どこがしっかりと活用していくのかという、先ほどコンソーシアムの話もありましたけれども、そういうところも含めてデータのオープン化というところを考えていくことが大事です。

ということで、今、幾つかの技術を紹介しました。そういった技術の出口を考えていくすう勢もありました。これらの技術に対して、ステージゲートの中でも実際に技術の評価だけではなくて、今お話ししたような出口の評価、最初に話したTRLの評価も併せて行っていきました。実際にやってみておもしろかったのは、6ページの右上のところです。開発技術と出口戦略というのは、あまりリンクしないのではないかと最初は思っていました。実際にステージゲートとして3年目の終わりに評価をして、本当にこれはそれぞれ30人ずつぐらいの人たちが評価をしましたけれども、それらの平均値をとったグラフです。実際に見てみると、開発技術と出口は非常にリンクしています。やはりTRLのレベルが上がってくると、実は開発技術の評価が上がります。どちらが先か分かりませんけれども、そういうことになるので、技術としてのレベルアップ、いわゆる国際競争力を高めるということは、実は国際技術力を高めることにもなっていたのではないかと思われます。実際に研究者としては、TRLの5ぐらいで興味を失うのではないかと思われていました。しかし、こういったところをしっかり見せることによって、TRLを上げることによって、研究者としてのブレークスルーも起こってくるのだということも、もう少しいろいろな意味で研究者のインセンティブにもっていってもいいところとして、出てきました。

それから、先ほど言いました技術の最終的な出どころは地方自治体が多くなるわけです。地方自治体の中においてつくった技術をどのように支援していくのか考えた場合に、我々としては地域の大学に、いわゆるメインプレーヤーになってもらおうという形で話をつくっていきました。実際に、霞が関や関東圏などの人たちや大学がいってしまうと、やはりいろいろな意味で評価されないところが出てきました。地方自治体の中においては、地方大学との連携等もしっかり見ています。そういったところの連携をしっかり考えてもらい、また、一番大事なのは技術の伝承というよりも技術の維持管理です。技術がそのときは新しくても、どうしても劣化してしまいます。だから、その技術のいわゆる維持管理、それから、技術を使うための人材育成が重要です。こういった2点の中において、地域の大学はメインプレーヤーとして非常に大事なのではないかと考えています。我々としては最終的にSIPが終わった後にも、こういった地域の大学の人たちにしっかりメインプレーヤーとして頑張っていただきたいということで、現在の土木学会を中心にしながら、地域の大学ネットワークの中で、そういった新技術の導入や推奨を進めてもらっています。

そういう中において我々が考えたのが、もともと今言いましたように地域の大学はこういった自治体とつながって、様々な形で人材育成や技術伝承、インフラの維持管理をしておりました。そういったところに対して、今回、7ページに示しますようにSIPインフラというところでいろいろな技術が出てきますけれども、そのまま持っていくと嫌がられます。昔、酒屋さんがセブンイレブンになったような形で、各地域大学の中にSIPインフラという形でのチームの中に入ってもらう。そういうネットワークの中で、地域大学の人たちが自分たちの技術も、こういったSIPで開発された技術も、また、国交省の中で紹介された技術も、いろいろな形でそういった技術の紹介というイベントを地域大学主催でやってもらうということを考えて進めていきました。

さらにそういった中において、8ページに示しますようにコンサル会社や地場産業などが興味をもってもらったものに対して、ビジネス支援も含めた形で進めていくということを行っていったわけです。

鳥取県のベタ踏み橋と言われているところで、いろいろなドローンを使ったりカメラを使ったり、組合せ技で評価をするということで、実証実験を行っていきました。この実証実験で一番よかったことは何かというと、なかなか現場で使ってもらえないところに、1回とにかく現場で使ったということが出てくると、これらの商品に対していわゆる社会的認知というものが上がることです。こういった形で使ってくれる場所が見つかったということは、SIPサイドとしては非常によかったと思っています。また、現場で実際に使うことによって、幾つかの技術が他のインフラのところでもどんどん使ってもらえるような状態に向かったということです。

以上、お話ししましたように、最後のページになりますが、データをオープンにするということは非常に大事です。どこまでオープンにするのかについては注意しないと、やはりもともとのインフラを持っている方や設備を持っている方から見ると、非常に不安感が出てきます。実際には設備のものだと思っているところも非常に強いです。ですから、この辺りのデータのオープン化というところも併せて将来的には考えていく必要があるでしょう。それらのところに対して、地域行政を含めて見ていくことが大事かと思います。

先ほど検証という話がありましたけれども、その先には認証ということが大事になってきます。やはり、誰かがお墨付きを与えないと、できるということだけだと、今言いましたようになかなか一発目としては使いにくいということになってきます。完全な認証とまではいきませんけれども、大丈夫だというお墨付きをどの程度まで与えるのかというのが、技術を証明できるためには1つ大事な点になってくるでしょう。

同じような意味で、特にAIや自動化が入ってくると、では、何かあったときには誰が責任をとるのか。それは使用者なのか製造者なのかという非常に微妙なところが残り続けることは事実です。こういった法整備やリテラシー教育というところも必要になってくるかと思います。

また、技術のメンテナンスや人材育成というところは、この後、技術の継続性においては非常に大事になってきます。そういった中において、地域の大学や地域の産学連携支援といった形で、地域全体を盛り立てていくところも併せて見ていくことが、技術を広げていくのにつながるかなと考えています。

今日は第1期SIPのところで私が経験した事柄を含めて情報提供ということでお話をさせていただきました。駆け足で短いところもありましたけれども、以上で終わります。どうもありがとうございました。

○江崎座長　岡田構成員、どうもありがとうございました。建築関係、SIPでご経験されたところを非常に明確に、明瞭に、コンパクトにお示しいただきましてどうもありがとうございます。今回の事務局の進捗のところも、そういう観点で少し最初のほうでおっしゃったとおりで、まだまだ抜けているところがあるということが、やはり先生のご経験からあるのではないかということだと思います。後半の質疑応答のところで、またいろいろご示唆、ご意見をいただければと思います。ありがとうございました。

それでは3つ目、今日の最後の説明になります。経済産業省商務情報政策局サイバーセキュリティ課の塚本様から、経済産業省のサイバーセキュリティ政策についてのご説明をお願いいたします。

○塚本課長補佐　本日はお時間をいただきましてありがとうございます。経済産業省サイバーセキュリティ課で課長補佐をしております塚本と申します。本日は経済産業省で行っておりますサイバーセキュリティ政策、特にガイドラインやそういったところを中心にご説明をさせていただきます。先ほどデジタル臨時行政調査会事務局の発表資料にもありましたサイバーセキュリティの部分で、何かしら連携や参考にしていただける部分もあるかと思います。そういった部分を中心にご説明させていただければと思います。

本日の目次はこのような形となっております。最初に諸外国の動向をご紹介させていただいた後、2番目に、主に経済産業省がどのような取組、特にガイドラインの作成や制度づくりなどでどういったことをしているか、そういったところをご紹介させていただければと思います。具体的にはIoTのセキュリティ、ソフトウェアのセキュリティ、制御系IoTのセキュリティ、データの取扱いセキュリティについてご紹介できればと思います。

まず、諸外国の動向として、米国です。米国は2023年3月に米国のサイバー戦略を公表したところです。本日のテーマとも関連する部分ですと、第3の柱の3.2にIoT、3.3にソフトウェアが

あります。米国はIoTで言えば、今、セキュリティラベリングプログラムを開発しているところです。後でご紹介いたします。3.3のソフトウェアの部分は、米国はかなりベンダに対する責任を今後強めていくような見込みです。この戦略の中にも、ソフトウェアを保護するための合理的な予防措置を講じなかった事業者に対しては、何かしらの責任を負わせることを開始しなければならないと書いています。それを担保する方策として、ソフトウェア製品とサービスの責任を確立する法律を策定するということが明記されているところです。アメリカは、このようにソフトウェアのベンダに対する規制、いわば責任を問うような方向にどんどんいくのではないかと思っております。　先ほど少し触れましたIoTのラベリングスキームです。

こちらは今年の8月にFCCが公表したものになります。任意のラベリング制度としてスタートしていく見込みで、その内容や考え方について、今パブリックコメント中です。9月25日までというところです。上の青いところの4点目にあるとおり、2024年後半の運用開始を目指しているところです。

こちらは、少し時間をさかのぼりまして、2021年に発令された大統領令です。これはかなりアメリカの中で大きな影響力を及ぼしております。その中のテーマの1つとして、ソフトウェア・サプライチェーンのセキュリティ向上があります。これが書かれていて、2021年、22年、現在というように、様々な取組がアメリカでなされているところです。こちらはタイムラインで、どういったことがあったかのご参考です。

次のページで、OMBは各省庁に対して、重要なソフトウェアを実装するとことを要求する覚書が結ばれています。また、OMBはNISTやCISAに対して、重要なソフトウェアをしっかり更新することを要求しています。

NISTはいろいろなガイドラインをつくっております。その1つとして、SSDFと呼ばれるセキュアなソフトウェアを開発するためのフレームワークをつくっております。主に組織の準備やソフトウェアの保護、安全なソフトウェアの開発、脆弱性への対応の4本の柱からなっておりまして、その手法から具体例まで書かれています。このガイドラインが発行されていますけれども、これを行政機関のOMBが取り込んで、SSDFの活用の覚書を結んでおります。内容としましては、ソフトウェア使用前にSSDFの実装の適合性を証明する自己適合証明書の取得をソフトウェアベンダへ要求する、要するに、政府機関が調達するソフトウェアについては、SSDFに適合しているかどうかをベンダの自己証明でいいので出してほしいということです。ガイドラインを一部規制化するような形です。その覚書は、これは手続面ですけれども、更新されております。

次はEUです。EUもいろいろ動いていますし、アメリカよりも規制度合いが強いように動いているかと思います。下の3点目の「加えて」というところですけれども、EUサイバーレジリエンス法（CRA）がかなり重要な動きだと思います。

2025年後半の施行ですけれども、具体的には、まず、デジタル要素を備えた全ての製品が対象ということです。医療機器等一部の例外はありますけれども、基本全てのデジタル製品が対象になる規制です。このデジタル製品に対して、SBOM作成や更新プログラムを提供する際のセキュリティ要件への適合等について、製品の重要度に応じて自己適合宣言あるいは第三者認証を求めていくということが書かれています。罰則ありということで、最高は1,500万ユーロまたは売上高の2.5%以内です。認証取得以外にも報告義務化やいろいろな規制がかかるわけですけれども、

それに違反したら、かなり高額な罰則もついているという法律です。これが今議論中で、早ければ2025年後半に適用されるというところです。

こちらは先ほど申し上げたデジタル製品の類型の参考です。あとは英国を載せております。3点目の「また、」から始まる部分ですけれども、これもIoT製品に対するセキュリティ対策の義務化を求める法律の検討が進められているところです。こちらには、その他の国々や州も含めてどのようなことがなされているかを一覧に書いておりますので、参考です。

このようにして諸外国はIoTやソフトウェアのセキュリティについて規制を強めているところです。経済産業省も、これからご紹介するいろいろなガイドラインを作成するところです。ガイドラインはなかなか法的に拘束力がないので、いかにしっかり担保していただけるような取組をできるか、規制化を進めていけるかというところも重要だと思っています。まさしく本日の議論に挙がっているようなデジ臨様の取組においても反映していただくことが、しっかりIoTのソフトウェアセキュリティが進む1つのレバレッジになるのではないかと考えております。

では、引き続きまして経済産業省の取組をご紹介させていただきます。経済産業省のサイバーセキュリティ政策は、産業界全般にサイバーセキュリティ対策を行っていただくこと、あるいは、何か起きた時に迅速に復旧していただくお手伝いをすること、あとは人材育成等、いろいろなことをしているところです。先ほど諸外国の動きもありましたけれども、あのような動きと対応して、どういう制度をつくっていこうとしているのか、この辺について本日、ご紹介できればと思っております。

産業サイバーセキュリティ研究会の中で、大きくは検討していまして、ワーキンググループに分かれて具体的な検討を進めているところです。これが経済産業省のサイバーセキュリティ政策の検討体制です。

ワーキンググループの下で、いろいろなサブワーキンググループやタスクフォースに分かれています。WG1の中で、大きくまず我々の考え方の根幹のところを議論していたのがサイバー・フィジカル・セキュリティ対策フレームワーク、CPSFと呼んでいます。一言でいえば、世の中を因数分解すると現実空間の層、サイバー空間、あとは現実空間とサイバー空間の間の層の3層に分かれるという構造、そして、それらの中に位置する構成要素はソシキ、ヒト、モノ、データ、プロシージャ、システムという6つの構成要素に分解することができます。これらの構成要素がルート・オブ・トラストとして信頼性が保たれたものであって、かつ、信頼性の保たれた連携がなされていれば、世の中のセキュリティは保たれる。そういった価値観、概念を提唱しています。これらは概念過ぎるので、それをブレークダウンしたようなフレームワークやガイドラインをつくっているところです。　これは、いろいろなガイドラインをつくっているという参考です。

次に、具体的なIoTセキュリティ関連です。まず背景として、IoT機器は現在2023年に358億台ですが、右肩上がりで増え、2024年にはほぼ400億台に達する見込みです。総務省の調査によれば、観測している不正な通信の3分の1はIoT機器を狙ったものであります。また、我が国においてもセキュリティ事件・事故によるIoT機器やOTシステムの一時停止を25%の企業が経験しているとの調査もあり、多くの企業にとってIoTはセキュリティリスクの一つであると思われます。

様々なことをやっていますが、まず紹介するのはIoT適合性評価制度検討です。先ほど紹介したように、アメリカではラベリングプログラムを開始しました。説明を省略しましたが、ドイツ、フィンランド、シンガポールなどもIoTのラベリングスキームを開発しています。そのようなラベリングスキームを日本でもつくる必要があるだろうということで、昨年11月に検討会を立ち上げ、IoT製品に対する任意のラベリングスキームをつくるべしということで中間報告を取りまとめ、現在も検討を進めています。

総務省が、一部、技術基準においてIoTの規制を行っていますが、そこでは機器が限られ、必要最低限の規制が書かれているところです。本検討内容としては、消費者用IoTも含め、より広範なIoTを対象にしています。また、IoTに応じてリスクレベルがあるので、リスクに応じたラベリング制度をつくることを考えています。

スキームとしては、IPAと協力しようと考えています。後ほど紹介しますが、IPAには今CC認証を行っているJISEC認証制度がありますが、CC認証のみならず広範なIoT機器を対象にできるようなものに拡張できないかと考えています。IoT製品ベンダがいますが、彼らがつくるIoTに対して何かしらの評価を受けていただく、あるいは、リスクが低いものについては自己評価も可能とするスキームにしたいと考えています。それによって何かしらのセキュリティ要件をこれから定めるので、それに適合しているかどうかをチェックし、適合しているようであればIPAに申請し、IPAからそのラベルが貼られる、そのようなスキームを考えています。

CC認証、JISEC認証は、狭義のJISEC認証をより発展させ、☆1、☆2、☆3、☆4のようないくつかのリスクレベルに応じてラベルを貼れる制度をつくれないかと考えています。☆1は、低レベルのリスクに対応するということで、最低限の基準を設けています。☆が上がるほど、より広範な脅威や、より深刻度の高い脅威に対してのラベルを貼るというイメージです。このような制度を検討していきたいと思っていますし、また、先ほど紹介した米国、あるいはEUなど、諸外国と連携して、相互認証を取るような形で制度を構築していきたいと考えています。このような制度が仮にできた暁には、先ほどデジ臨の事務局から紹介のあったセキュリティチェックに入れてもらうことが考えられるのではないかと思います。

続いて、SSDFと近い取組ではありますが、IoT機器等の開発時のセキュリティ向上を目指したガイドラインも策定しています。

昨年度、実証実験的に74社・155製品のIoT機器に対してペネトレーションテストなど、様々な検証を行ってみました。その結果、155製品に対して4,789件の脆弱性が検出され、脆弱性に対策していくことの必要性も改めて感じました。その脆弱性の80%はソフトウェアのバージョンが古いなど、プリミティブな脆弱性であったことから、開発時における対策はしっかり行うことによって大部分の脆弱性が潰せるのではないかと思いました。

したがって、開発時にセキュリティ対策を行うようなガイドとして、特に中小企業は知見も人材も乏しいので、中小企業に主眼を置いて中小企業が分かりやすいガイドを作成しました。詳細は割愛しますが、体制を構築する、セキュリティポリシーを作成する、設計の段階からしっかりセキュリティを考慮する、リリース時にセキュリティ検証を行うことを想定して開発・設計する、といったことを書いています。これらを見て、もし必要なところがあれば、先ほどのチェックリストに設けることも一案ではないかと思います。要するに、ソフトウェアを納入する会社

が、どれほどセキュリティを意識した開発ができているかということの参考にはなるのではないかと思います。

次は IoT-SSF、IoT セキュリティ・セーフティ・フレームワークです。先ほど説明した IoT ラベリング制度、適合性評価制度、あるいは開発時のガイドラインも、IoT を出荷する際のセキュリティを担保するものですが、IoT が現に使用されている空間においても、どれだけラベリングを貼ろうが、開発時にチェックしようが、新たな脆弱性は出てくるだろうし、攻撃者も狙ってくるので、リスクは使用中も当然、生じるわけです。その使用中のリスクをいかに管理するかという、より大局に立ったフレームワークになっています。

詳細は後で説明しますが、IoT 機器のリスクを見る軸として、1 つ目は、回復困難性の度合いです。すなわち、IoT で人がけがをするリスクもあるので、それを回復性と呼んでいます。仮に亡くなった場合には回復できませんので、回復困難度は高いところにマッピングするといった具合です。軽傷であれば治るのでリスクは低くなります。それを横軸に置いています。2 つ目は、経済的影響の度合いです。IoT が工場のラインに搭載されていたと仮定して、それが止まってしまったら 1 日停止して数億円の被害が出ることも考えられます。どれほど経済的な影響が出たかという指標を縦軸に置いています。この縦軸、横軸で機器のリスクを、定性的にではあるが、マッピングすることができるということを、まず提案しています。

こちらは 3 次元になりますが、そのおのおののマッピングされたリスクを管理していく考え方には、第 1 から第 4 の観点があると思っています。第 1 は設計時の考慮で、そこから第 4 にいくに従って、より社会でリスクを分け合うような観点が増えてきます。第 4 になると、IoT 保険のようなものに入る必要があります。様々な観点からリスクを分け合うことが考えられるのではないかということを示したフレームワークになります。

様々なユースケースをつくって紹介しています。簡単に一連の紹介をすると、物流倉庫にある AGV によって自動ピッキングされるというケースを想定すると、このフレームワークではステークホルダーを整理することも謳っておりますので、AGV のステークホルダーとしては、製造業者、システムインテグレータ、物流事業者がいます。こういったステークホルダーがいるという整理、それらの者にとってどういうリスクがあるのかという整理、それらのリスクはシステムベースでいうとどこに起きるのかという整理、それらをステークホルダー間でしっかり共有することを示しているフレームワークです。そのリスクを低減するためにどのような対策を行うかという考え方を示しています。おのおののステークホルダーにおいて対策を自主的にやってほしいというフレームワークです。

事務局の説明資料に対して一つ考えられるのは、セキュリティのチェックリストにこの IoT-SSF も含んだような自己適合届出のようなことをすると、申請者が自主的にリスク低減策をステークホルダーと分け合って管理できているか否かということもあるかもしれません。そのように考えられるのではないかと思います。

次にソフトウェアセキュリティです。先ほどの検討体制の中で、経済産業省の審議会やソフトウェア TF で議論していますが、まず OSS（オープン・ソース・ソフトウェア）の管理に関する事例集を作っています。

一番はSBOMに着目しています。先ほどEUではSBOMが義務化されるといったことが書いてありましたが、SBOMはソフトウェアの部品構成表です。OSSが世の中にあふれていますが、ある人によれば、95%はオープン・ソースから引っ張ってきてアプリケーションが構成されているようです。オープン・ソースもTier1、Tier2、Tier3、Tier4があり、コンポーネントを組み合わせて1つのアプリケーションをつくっていると思っています。えてしてそれが管理できておらず、脆弱性の管理ができていない、また脆弱性に基づいて攻撃を受けたとしても原因の特定が遅れてしまうことにつながりかねないという課題があります。したがって、ソフトウェアを構成するコンポーネントが、誰がつくったもので、バージョンがいくつで、どのような脆弱性があるのか、内訳を管理するものがSBOMです。これが、ヨーロッパでもアメリカでも期待が高まっている脆弱性管理の手法です。

経済産業省としてはこれも推していきたいと考え、昨年度は自動車業界、医療機器業界、ソフトウェア業界と協力して実証を行っています。Tierが広いので、どう分け合えば効率的に脆弱性を管理できるかという実証を行ってきました。それらの実証を踏まえ、今年7月に「ソフトウェア管理に向けたSBOMの導入に関する手引」を策定しました。SBOMの活用に向けて、その体制構築、SBOMをどう作成するか、SBOMを関係者とどう共有するかといった運用にわたる考え方や手続を書いた手引であり、それを公開しています。

今年も実証を行っており、SBOMは脆弱性をいかに管理するかというツールですが、当然、日々様々な脆弱性が出てきて、それらはNVDや日本ではJVNでどんどん登録されていくわけです。これらのデータベースとSBOMのソフトウェアが自動的に連携すると、JVNで上がった脆弱性は自動的にSBOMにも反映され、ソフトウェア開発者やTier1、Tier2の関係者が一様に脆弱性を把握、管理することができるということで、そのような脆弱性の紐づけ実証も行っています。

先ほどもソフトウェアの管理に関するチェックリストがあり、どこまで厳しくするかによりますが、SBOMをどこまで考慮できているかということも考慮事項の一つになるのではないかと思っています。

参考として、SBOMはアメリカ、EUなど一国、一地域のみならず、Quadのような多国間の枠組みでも問題意識の議論がされています。今年5月に行われた首脳宣言の一文書の中にはサイバーセキュリティがあり、そのうちの一つにソフトウェアセキュリティに関する共同原則があります。その中には、SSDFに書いてあったようなこと、中でもSBOMも書かれており、これらの対策の重要性、脆弱性管理の重要性、SBOMを使う重要性が、Quadのような多国間の枠組みでも議論されています。

続いて、OTセキュリティです。工場SWGというものを我々は持っており、江崎先生が座長を務めていますが、昨年1月に設置し、議論を重ねて、昨年11月にガイドラインを公表しました。工場も多種多様で、これさえすればよいというものはなかなか示せないですが、このガイドラインでは、工場の規模、構成する機器・システム、構成する人員の人数・能力を把握して体制を構築し、工場が達成したい価値を守るためにどういう対策をしなければならないのかを立案すべしという価値観を提示し、またそれらができるようなプロセスを提示しています。

これも昨年11月に公開して、今、多くの人に使われており、工場は多種多様ですし、対策は業界ごとに違う部分はあるかと思うので、業界ごとの対策が進むような仕掛けをしていきたいと思っています。

最後は、データセキュリティ関連です。先ほど紹介した第3層TFは、データがやりとりされる際にどのようなステークホルダーがいて、おのおのはどうデータを保有して、それに対してどういうリスクがあるのかということを定性的に整理するようなフレームワークです。

データマネジメント・フレームワークと呼んでいますが、例えば小売業のPOSデータだとすれば、まず販売データはレジに登録され、1日の売上を集計すると物理店舗のパソコンに集約されます。それがさらに集約されてエリアごとのデータになります。そういったデータの流れや、おのおののデータの状態、これを属性と呼んでいますが、データがどこにどういう状態であるのかをまず整理します。「場」と書いていますが、それが個人情報保護法のような法律に抵触するかもしれません。例えば、個人情報として秘匿されない形でデータが受け渡されると個人情報保護法違反になるかもしれません。あるいは、データが受け渡される過程で脆弱性があれば、ネットワーク上で侵入されて、個人情報の漏洩やデータの漏洩につながる可能性があります。そのようなセキュリティ上のリスクもあります。データがどういう状態にあり、どこにリスクがあるか、それがどう管理されているかということを定性的に表すようなフレームワークも作成しています。このようなデータの取扱いに関してリスクを把握することも、先ほどデジ臨の事務局からデータの扱いについても紹介がありましたので、参考になる部分ではないでしょうか。

このような形で、デジタル臨時行政調査会事務局が進めていこうとしている部分に協力できるようなガイドラインやフレームワークを構築していますので、その検討の一つの材料になればと思っています。大変駆け足でしたが、ご静聴ありがとうございました。

○江崎座長　ご説明ありがとうございました。非常に多様な議論が進められており、具体的なガイドライン、ラベリングの話も進められているということなので、デジタル庁での検討との整合性を取った形で進めなければいけないということになるでしょう。また、先ほどの岡田構成員から説明のあった経験とも非常に関連する点が多かったのではないかと思います。

○江崎座長　今日ご用意しました説明に関しては終了しましたので、以後は本日のメインの主題である意見交換の時間とします。本日の議論に関して、あるいは今後の委員会における議論の進め方、今後のプレゼンテーションの機会のリクエスト等に関して、構成員の皆様からご意見、ご質問等があればお願いします。

○島田構成員　本日の議論を拝聴しまして、私が当初から懸念していたところではありますが、スピード重視はもちろん継続されると思いますが、コンテンツに対する責任をチェックするというのは、今までの方針から転換したものだと私は非常にポジティブに受け取っています。実際に公開されたものを誰かが一定程度チェックすることは非常に重要だと思います。ただ、チェックする人は公開しないというのは気になる点です。そういう意味では、SIPの岡田構成員からの説明にもあったように、そのように準備して、努力して、用意して、結局採用されないことは、民間企業ではよくある話です。規制を改革することを考えているということであれば、本来はこういった目的、目標値をクリアすれば採用するということを規制官庁からコミットすることが重要

ではないかと思います。努力した結果、結局はしごが外されていくようなことがあると、実際に規制の改革は進んでいかないのではないかと思います。
○江崎座長　特にトランスペアレンシーについて、公開しないことで伏魔殿になってしまうのではないかというご指摘、ご心配だと思いますが、先に事務局から回答をお願いします。
○須賀参事官　資料 2 の 25 ページですが、TF を設け、ある程度チェックを強化することについては、島田構成員からもご賛同いただきましたが、他方でそのメンバーを非公開にすることは問題ではないか、つまり、よく分からない理由でカタログに載らないものが増えていくのではないかというご懸念の表明をいただきました。その点については、可能であればまず非公開で始めて、どのくらいの割合で落ちてしまうのかというデータについては、この場で皆様にも共有し、その割合が妥当な水準なのか、落とし過ぎ、絞り過ぎなのかということは見ていただいた上で、やり方がまずいということであれば、すぐに改めていくというようなアジャイルなやり方ができないかと思います。
　非公開にする理由は、構成員の先生方に何らかの圧力がかかってしまうような事態は望ましくないということです。構成員を務めていただける方の人材プールが非常に小さいので、その先生方に辞退されてしまうとこの仕組み自体が持続可能とならないことから、まずは事務局の側に責任が重い形で始められないかというご提案ですが、いかがでしょうか。
　もう一点、技術検証したときの規制所管省庁側のコミットというご指摘については、今回、技術検証を行うことによって、規制所管省庁は普通の調達事案と比べると既に深くコミットしてくれていると思っています。仕様書の中に、具体的にどういった機能・性能を確認したいのかということをかなり細かく書いています。その中で、今まで言語化されていなかったことがされている部分もあると思います。岡田構成員から指摘があったように、性能をしっかり見ないと、安かろう・悪かろうの技術が入ってきて、正直者がばかを見るということになり得ますが、そこについてかなり言語化が進んできた面もあります。他方で、難しいのは、規制自体は所管省庁が直しても、技術を調達するのは規制所管省庁とは限りません。規制所管省庁が自身で所管している下位団体が調達するような場合には、ぜひ調達までつなげてほしいということは、我々からしっかりとお願いしていこうと思います。他方で、規制が開放されることによって、規制をコンプライアンスする側の企業が実際は調達に踏み出すということでありますと、規制所管省庁としては、その技術はぜひ採用してもらって構わないというシグナルを出す、一歩踏み出すことを多とするというコミュニケーションをしてもらうことが、我々からすると最大限お願いできることだと思っています。その辺りも、技術検証をした結果、テクノロジーが実際にいつ採用されたのかというところまでフォローアップしながら、策を練っていきたいと思っています。よい知恵があればぜひアドバイスをいただければと思います。
○島田構成員　その意味では調達の公平性もあると思うので、認定制度が鍵ではないかと思います。
○江崎座長　トランスペアレンシーに関しては、プロセス、データを出していくということが大きな方針です。チェックする人の非公開性に関しては、ハイブリッドの形になることももしかするとあるかもしれない、という説明でした。

○平本構成員　今回からの参加です。よろしくお願いします。私はデジタル基盤センターにおり、今まで齊藤アーキテクチャ・センター長が出ていたのですが、より技術に寄せようということで参加することになりました。

今回資料を拝見しまして、マップが非常に充実しており、テクノロジーが一覧化されていてすばらしいと思いました。

実は我々IPAは以前からテクノロジー・レファレンス・モデルという技術カタログや、OSSiPediaという形でOSSのカタログなどを作った経験がありますので、そこからお話をします。技術カタログはスタートのときには勢いがあるが、フィードバックを受けながらやらないと、技術が広がって維持するのが大変になるので、その運用のサイクルをきちんと考えることが重要と思いました。

そのときに感じた点が2点あります。こういう技術を見ると、製品を出している企業はどのような会社なのかと思うことがあります。法人番号からgBizINFOなど企業情報が見られるサイトに飛べる、あるいは、類似技術が多くあるものでは、上に出ているものがいつも同じだと公平性の問題を指摘されることもあるので、複数の種類のソートの仕方をつくる、そういう工夫も必要なのではないかと思います。

それと、先ほどフィードバックの話をしましたが、テクノロジーマップに事務局で追加していくこともあると思いますが、一般の技術企業、技術者から提案やフィードバックをもらって直していくという仕組みも必要なのではないかと思いました。

○江崎座長　大変貴重な経験の話と、運用を続けていくことについて留意しなければいけないという示唆をいただきました。

○登構成員　今日の資料を拝見して、充実してきたと思いました。一つ、セキュリティについてコメントがあります。詳しくは、説明を聞きながら作成したPDFがあるので、それで説明します。※末尾の【構成員からのチャット等でのコメント】に記載

25ページに、入力させる情報として、個人情報の保護、セキュリティに関する項目で、裁判所の管轄権の話がありました。これについてコメントがあります。セキュリティというのは単にサイバー空間上、安全だと言っているだけではなく、日本の行政組織、日本の会社、そこにデータを預ける国民、顧客の観点から見て、実体法上の何らかの安全の担保がある必要があります。そうしないと、単なる抽象的な概念に終わってしまうと思います。

25ページの先ほどの部分はすばらしく、なぜあれを入力させるかという趣旨は3つあると考えています。ベンダ企業の欠陥、漏洩、サービス停止によるデータの取り出し不能など、債務不履行が起きるリスクを把握すること、起きたときにどのように法的対処を日本人ができるかを常に考えること、起きた場合に賠償義務をベンダに負わせることで、賠償をしなくて済むようにベンダが大変な注意を払って日本人のデータを保管するという状況を実現することによって問題を遮ること、この3つが趣旨だと理解しました。

そうすると、(2)にあるように、重要なデータは個人データにとどまらないと思います。「個人」と限定的に書くと誤解を招くので、「個人データを含めた全ての取扱い業務データを保護対象とする」と書いたほうが、個人以外はそれほど重要ではないということにならないので、よいのではないかと考えます。

(3)に書いたことは、裁判管轄権の所在国は確かに重要ですが、それに加えてよく見落とされるのは、適用される準拠法です。管轄権と準拠法は全く違う概念だと思います。たとえ日本の裁判所に管轄権があると書いてあっても、○○国○○州法を適用すると書いているケースがあります。これはユーザーに予期せぬ不利益を与えるので、管轄権とともに準拠法も書くべきだと思います。

(4)は、よくある話ですが、外国ベンダ系の製品を日本人に売るときに、本社が売っているのか、日本の子会社が売っているのか、よく分からないことがあります。例えばGというブランドのすばらしいクラウドサービスを使おうとすると、「G合同会社」という東京都A区の法人か、「G・クラウド・ジャパン」という東京都B区の法人か、アメリカのデラウェア州にある「G LLC」なのか、ユーザーはよく分からず、Gというブランド力で、安全だろうということで利用を開始してしまうのではないかと思います。海外企業で重要なブランドがあるときには、彼らが保証してくれているから安全だろう、取締役の個人財産も含めて補償してくれるだろうと、安心してGのサービスを使うが、彼らはとても賢いので、日本で大規模なデータが同時に多発漏洩したときに、その過失の損害賠償を全員が同時に賠償請求をしてきても払わなくていいようにリスク隔離をし、日本の小さな会社の責任財産の範囲でしか賠償しなくてもいいような工夫をしていることが、海外ベンダにはよくあります。そういうときに大変な被害をこうむるのは日本人なので、日本の官公庁や民間企業がカタログに載っているサービスを契約しようとするときに、誰が契約の相手先であるか、ブランド名ではなく「○○株式会社」、「米国○○LLC」のように明記することを義務づける必要があるのではないかと思います。

(5)は、いくらそれを明記して、日本の○○社と書いてあっても、その○○社が外国の本社の財産とは無関係で、○○社で賠償に充てる財産があまりないとなると、日本の裁判所でいくら裁判しても取れるものが日本にはないということで意味がなく、ユーザーは泣き寝入りになります。ただ、ユーザーは泣き寝入りになっても、あらかじめサイバー保険等の手段に入ればいいのです。ですが、その場合、ユーザー企業やユーザー役所は、いくらの金額の保険をかけるか、そもそも保険に入るリスクがあるか否かを把握する必要がありますから、そのためには掲載される海外ベンダが日本においてこのくらいの信用担保があるという金額を、自己申告でもいいし、秘密だという場合、入力しなくてもいいということでもいいので、入力が任意で秘密だとしていれば、十分警戒して契約するのでサイバー保険に入るだろうから、入力欄があることには価値があると思います。

最後に、大規模な障害が同時に発生したときにユーザーは賠償を求めますが、よくよく約款を見ると、最後の1年分を上限とする、特別損害は一切補償しないなどと細かい字で書いてあります。ところが、役所や民間企業の担当者がそれを読み込むのは事実上、困難です。技術カタログを読んで対応を決めるときに補償の範囲は極めて重要な要素になります。約款を読むのは難しいので、経営判断のためにもこれを簡略化し、事業者の自己申告値として、上限を1～2行程度で記入することを、国際裁判管轄権を記載させる欄と同じような簡単さでもいいので、ぜひ追加してほしいです。事業者にとっても、自社のサービスが安心であることを謳うのもよいことであり、日本のユーザーにとっても安心料を把握できるのでよいことだと思いました。以上、走り書きですがコメントを送付しました。

○江崎座長　ありがとうございました。基本的にはコンプリメンタリーな情報を出し、ただ、強過ぎるとコンプライアンスのオーバーヘッドが増えてしまうことを気にしなければいけないです。事務局から反応はありますか。
○須賀参事官　ご指摘のとおりだと思います。必須の項目にするのか、任意の項目にするのかを検討した上で、いずれも対応したいと思います。改めてそこはご相談させていただきます。何か損害が生じたときの賠償を海外企業に求めていくことが難しいという論点をしっかりアドレスしていくこと、約款を全部読み込むのが事実上難しいという問題についてこのカタログが貢献する余地を見いだしていただき、大変ありがたく思います。
○染谷構成員　１つコメントと１つ質問をしたいと思います。
まず事務局へのコメントとしては、最初の質問にもありましたが、技術カタログ運用 TF メンバーが非公開ということについてです。普通こういうものの決定は、個人のリスクというよりは委員会全体でその責任を共有するものなので、非公開である必要性は必ずしもないのではないかと思いました。また、非公開というと皆引っかかって、なぜだろう、重要な決定をする際の透明性は大丈夫かということが不安になるのに対して、メンバーの公開のタイミングや内容などを適切に管理すれば、わざわざここで非公開にしなくても十分適切に運用できるのではないかと感じました。
もう一つは、岡田構成員のプレゼンについて、SIP における現場に寄り添った活動を続けてこられたことに感銘を受けました。その中で最後に言及のあった、地域の大学という項目で、地域の産学連携を支援することが解決に向けて非常に重要だということは、心から共感するところです。いい話でしたが、実際には簡単ではないところもあると思いますので、課題とそこに向けた解決策、あるいは、今日はデジタル庁も出席しているので、行政に向けた要望などがあればぜひ伺いしたいと思いました。
○江崎座長　前半は事務局から簡単に、後半は岡田構成員からお願いします。
○須賀参事官　確かに我々もメンバーを「非公開」とするのはかなり踏み込んだ提案だと思いつつ、何らか構成員をお守りする工夫をしなければいけないと思っていました。公表のタイミングを重要な意思決定が終わった後にすることなども含めて柔軟に判断し、いずれにしても重要な意思決定に関わった方が未来永劫ブラックボックスではないという状態は担保することによって、意思決定に関わる方のインテグリティを担保していくことも重要だと思いましたので、ご提案を踏まえてこの方針は見直したいと思います。
○岡田構成員　地域の大学に関しては、言うと台なしになるかもしれませんが、一番大事なところは、それをやってくれそうな人をどう見つけてくるかということになると思います。ただ、私の経験で言うと、基本的に定年した名誉教授は割とやってくれます。つまり、現役の先生はまだ研究などで主に働いているので、プラスアルファでこういうことをしてもらうのはなかなか難しいです。一方で、定年しても皆まだ元気なので、そういう方々が逆に若い博士の学生などにやっていこうと言うと、一生懸命やってくれます。
総務省や内閣府の地域創生などの予算を逆に地域の人たちと取りに行くなど、様々な形で国の予算の取り方も支援すると、それも含めて取りに行くという形で出てくると思います。デジタルの技術開発といった金の取り方ではなく、地域創生などを組み合わせることによって、うまく他

の予算も取れます。実際に取りに行くのは大学だけではなくとも、産学連携すると取りやすい予算もあるので、そこをうまく指導することをどこかがやれるといいのではないかと、個人的には思いました。

土木の場合には土木学会でやっていますが、そういうコンソーシアムを支援することが必要で、単に直接的なものではなく、間接的なところの環境設定がうまくできると、動いてくれるのではないかと思います。それさえあれば、やりたいと思っている人は意外に多かったと感じます。

○江崎座長　まさにテクノロジーマップのような成功事例を見せること、その中にシニア人材を使うということだと理解しました。最初の質問に関しては、「検討する」というのは役人的な「やらない」ということではなく、公開する方向で方法を具体的に考えるという回答という理解でよろしいですか。

○須賀参事官　そのように対応したいと思います。

○鈴木構成員　東京大学の鈴木ですが、福島ロボットテストフィールド所長という立場でこちらには参加しています。

前回か前々回に参加したときにお願いしたのですが、先ほど岡田構成員の話にもありましたように、技術といってもそのレベルに応じて段階がありますので、出来上がったものだけをカタログ化しなくても、テクニカル・レディネス・レベルの、まだ低いが可能性のあるものも、カタログという形で紹介するのもいいのではないかとお願いしました。そのときにテクニカル・レディネス・レベルがどのくらいのものか、見る人が認識できるように、項目をつくるとよいのではないかと思いました。

今日の話を聞いて、リスク・ベースドとパフォーマンス・ベースドという話が根底にはあるのではないでしょうか。検証が必要のないものもあるという話もあり、それはリスクが低いからということだと思いますが、福島ロボットテストフィールドでドローンを飛ばす際のリスクマネジメントのガイドラインをつくりました。世界的に国連の専門機関である ICAO の WG がつくった SORA というリスクアセスメントのガイドラインがあり、それを日本の環境に合わせてつくり直したところがあります。リスクが低いものは自己宣言でいいわけですが、リスクが中程度以上になると、第三者評価を求めて、それがないと本当に大丈夫かどうかということが客観性に欠けることになります。

したがって、今後、第三者評価をリスクの高い検査に使うときに、どのように機能させていくのかといったところの検討もぜひ進めていただければと思います。パフォーマンス・ベースドなので、ここで出された新しい技術がそれ自体を要求するわけではなく、それは一つの事例ですので、様々な手法があり得る中で、どのように組み合わせて使っていくかを考えなければいけないと思います。リスクの低いものに関しては自己宣言でいいですが、リスクが高いと、それが本当に大丈夫かどうかについては、第三者の検証が必要になるのではないでしょうか。そのような検証機構をつくるという話も先ほど岡田構成員からございましたが、日本の中でそういうものがまだ成熟していない段階で、どのように第三者認証を構築していくのかについての検討も必要ではないかと思いました。

○江崎座長　本質的なレベルによってラベリングとサーティフィケーションというレベルがあるというご指摘が改めて鈴木構成員からありました。
○須賀参事官　鈴木構成員には福島のテストフィールド類型3で、検証自体もお世話になることになっています。また、先生が企画されている様々な場に我々事務局が出席してご説明する場を設けていただき、本当に感謝しています。
TRLに関しては、先生のご指摘を踏まえて既にカタログの項目に追加していますが、そのまま入れると書けない人も多いのではないかと考えまして、今の時点では分かりやすさ重視で、研究段階、実証中、販売段階と3つに大ぐくり化しています。それがまとめ過ぎかどうかについても何らかご指摘があればお願いしたいと思います。
もう一つ、ご議論が出ています、検証だけではなく、その後のラベリングから始まる認証やお墨付きの話です。経済産業省サイバーセキュリティ課からのプレゼンを伺っても思ったのですが、餅は餅屋なので、何でもデジタル庁、デジタル臨調で、自前主義でやらずに、新しくできる制度にどのように我々が乗っていけるか、それによって制度自体のエンフォースメントに我々が貢献するという側面もあると思いますので、認証、お墨付きの機能がこれからできていくようであれば、いの一番に我々がそれに乗らせていただくことを考えたいと思います。現在進行中の議論だと思いますが、しっかり追っていきたいと思います。
○鈴木構成員　先ほどのTRLのレベルについては、最初は、研究中、開発中、商品化されたものというぐらいの大まかな項目が書かれていれば、皆様、認識するのではないかと思うので、それを入れていただきありがとうございます。
認証については、ご説明のとおり、デジタル庁がそこまでやるということではなく、それを扱う業界団体のようなものが中心になって、またアカデミアとともに進めていくことだと思うので、デジタル庁としては、そういう動きを誘導するようなメッセージをこれからも出し続けていただければと思います。よろしくお願いします。
○江崎座長　スケーラビリティを考えたときに、ここだけでやるという形ではないということを意識するようにということだと理解しました。
○中垣構成員　岡田構成員のご講演が非常に参考になりました。個別の質問で恐縮ですが、データの所有権の課題です。スマート保安プロモーション委員会でも常に問題になりますが、見逃し率と誤認率で、特に見逃し率は致命的になることも多いので、検出を緩めようとすると今度は誤認も増えてしまうということで、データの質の向上のために、機器開発者はリリース後に良質な機械学習の教師データが欲しいと思われます。しかし、それがインストールした客先の場合、許諾が必要となり、様々な制約条件で開示されない場合が多々あります。それについての対応として、何かいい事例はございませんでしょうか。
○岡田構成員　事例になるかどうか分かりませんが、先ほどの地域大学のところで言うと、地域の中に実際にはインフラセンターなど、土木の先生方が外とつながる形で人材育成のセンターをつくっているところがいくつかありました。そういったところで自治体のデータを集めて、そこでクローズにする。実際に使いたいところは、そこに入ってその大学と包括連携のようなものを結ぶと使えるようにしましょう等、技術を使うところもそこに入ってもらう形で、ローカルなネットワークをつくったところで、そのネットワークの中でのオープン化はできると思います。例

えばそれを使った自治体の中では、市のデータも含めて全部取るという形で、県の中で全部使えますし、そこに行ったら使えるという形も取れたりしました。

最初は、それこそ自治体の話で言うと、市のデータを県は使えないというような話になっていて、そのままで自治体に任せると、簡単に言うと、つながりがないから駄目ですとか、県と市の仲が悪いから駄目ですとか、昔の談合の話があるからあそことは組みたくないなど、そういう下世話な話も出てきたりします。だから、先ほど言った、地域の大学の中に収めようと言うと、ある程度担保ができることも含めて周りの人たちが安心できるので、地域の大学の中のセンターの中にそういったデータを集めるところをつくる、そしてそのセンターが全部使うわけではなく、そことコンソを組めばそこに入っている企業も使える形になれば、対外的な経済安全保障も含めて組めるのではないかと思いますし、実際にそれでいくつかうまくいっているところもあります。その意味で地域の大学のセンターをうまく活用するというのが一つの方法ではないかと思っています。

○中垣構成員　今の回答が次の質問の回答にも関係するかと思いますが、フロントランナーとなる方の消極性があり、前回、アンケートでもお示ししましたが、どこかで実績があればうちもやろうとなりますが、逆に、新技術が初めて実装段階にあるようなときには、開発段階でリスクを取ってまでボランタリーなフィールド試験を提供する人はいないです。そのよい克服策はないかということですが、それも大学が絡めば可能だということでしょうか。

○岡田構成員　実際に自治体で、大学の研究者で来ていたような人たちがいることもあるので、非常にローカルな人脈で追いかけると、意外にそういう人がそこでキーマンで動いていることが見えてきます。あるいは、市長の特別補佐で、どこかの市の副市長扱いで技官をやっている人がいると、その人を使ってやってみるとこんなことができているという話が出てきます。あるいは、技術でもそういう形で見てみる、またローカルな人脈で見ていくと、意外に自治体にいくつか出てくることもあります。また、イベントに積極的によく来る課長をつかまえると、やりたいということを言ってくることもあります。だから、先ほど言ったリモートのウェブ会議ばかりするのではなくて、実際にリアルな会議をすると、話を聞きたいと言って来てくれる人がいるので、その人に声をかけるとやりたいという形になってきます。逆に、デジタルであればあるほど、会やイベントをリアルにやって、そこで興味のある人をつかまえるのが、地方行政で言うと手ではないかと思っています。

○中垣構成員　参考になりました。

○江崎座長　ニュートラリティを持っているところを上手に使っていくことに関しての知見でした。

○川端構成員　チャットにコメントしたもの全てを話す時間がないので、重要なところをお伝えします。※末尾の【構成員からのチャット等でのコメント】を参照

資料２で従来の法整備の分析や解析が把握されていて納得しました。法整備の順序立てがよく分かりました。一方で、デジタル化するよさもこれからのアドオンになると思うのですが、従来の法整備はこうであったという解析と同時に、デジタル化するとこうあるべきということが必要ではないかと思いました。例えば、問題があったところへの迅速な対応が従来の法整備で求められるところでしたが、デジタル化になると予防保全、ミティゲーションのデータが取れたりでき

ると思います。壊れてしまったところを検査する、その検査の目的や手法を定義するというのが従来の法整備だったと思いますが、例えばセンサーなどが発達しているので、センサーや測定データの共有や、場合によっては測定データからプラットフォームへのフィードバックもできるので、今後の法整備の際にそれが推進できる形が付け加えるとよいのではないかと思いました。

したがって、従来の法解析だけではなく、今後、将来に向けては、少子化で作業者が少なくなりますし、また、壊れたところを検査するのはお金もデータもかかります。例えば建築現場では、BIM の導入などにより、BIM は設計する手法が簡単になるだけではなく、今後の予防保全や検査に対して設計データを使っていけるよさもあるので、そういった法整備ができると BIM の導入も進むのではないかと思います。

次の資料 3 につながりますが、インフラのモニタリングなどは、できてしまったところに対して壊れたところをモニタリングするだけではなく、センサーを入れていくことが、特に土木工事などでは予算がきつい中でやっていくとき、現在予算をつけるときに新しいセンサーなどを積極的に導入するような仕組みになっていませんが、予防保全のテクノロジーを推進できるような法整備になっていると、そのようなことが推進できるのではないかと思います。

資料 2 と 3 についてはそういうところが関連しているかと思います。

また、他の構成員からも再三ご指摘があったように、規制と調達は非常に難しい部分があります。民間業者の場合、技術確立の段階の PoC に人もコストもかかる中でせっかく参加しても、調達においては承認されたもののコストは下がるので、そこで違う業者が入ることが往々にしてあります。入札が予算ありきになるのは当たり前のことではありますが、民間業者の PoC 段階までの参加の腰が引けることになりかねないので、そこのバランスを取るような仕組みができるとよいのではないかと思いました。

最後のところはアイデアがなくて申し訳ないですが、資料 2 と 3 についての指摘を反映してもらえるとうれしいです。

○江崎座長　時間が来てしまいましたので、川端構成員、荻野構成員からチャットに書き込んでいただいたものを議事録にしっかり載せていただきたいです。

○須賀参事官　小川構成員は大丈夫でしたでしょうか。

○小川構成員　時間がなければチャットに記載します。

○江崎座長　では、チャットあるいはメール等でいただき、確実に議事録に載せるということで対応します。

○小川構成員　承知しました。※末尾の【構成員からのチャット等でのコメント】に記載

○江崎座長　この 3 件について須賀参事官から簡単に反応はありますか。

○須賀参事官　いずれも貴重なご指摘ですので、対応を考えて、また修正案についてご相談させていただきます。

○江崎座長　時間の取りまとめが不手際で申し訳ありませんでしたが、本日の議事に関してはここまでです。

○江崎座長　最後に事務局から次回の委員会等に関する説明をお願いします。

○須賀参事官　次回の委員会はまた追って日程などをご連絡いたします。議事録や資料の扱いについては従前と同様です。本日もありがとうございました。
○江崎座長　大変建設的な、本質的なご意見等いただき、本当にありがとうございます。
「検討します」というのは、役人の「やらない」ということではなく、いただいたご意見を反映させることになると思いますので、引き続き支援をお願いします。本日は、どうもありがとうございました。

（了）

【構成員からのチャット等でのコメント】
○登構成員
事務局資料 『第 6 回テクノロジーベースの規制改革推進委員会 「テクノロジーベースの規制改革」の進捗及び当面の進め方』 に関するコメントです。
P.25 『サイバーセキュリティ・サプライチェーンリスクへの追加対応』の入力項目のうち「②入力項目にサイバーセキュリティやソフトウェアサプライチェーンリスクに対応した項目を追加する」（目的は、「技術カタログ利用者の適切なリスク判断等を支援するため」と明記されている。）について。
そもそも、「セキュリティ」（security）という言葉は、「(安全の）担保」という意味が強いことばと思います。単に安全と言っているだけでなく、安全性に対する担保を把握することが、リスク管理上必須です。

(1) 本施策の趣旨は、製品・サービス供給元会社が債務不履行（欠陥、データ漏えい、サービス停止によるデータ取り出し不能等）を引き起こすセキュリティ上のリスクについて、
(a) そのリスクを把握すること。
(b) 実際に問題が発生した場合にユーザー組織が取り得る法的措置の範囲を把握すること。
(c) 万一、回復不能な損害が生じた場合の損害賠償義務が十分に果たされる状況を確実化することにより、事業者が自主的に相当な注意を払って製品・サービスを供給したくなる状況を実現し、よって問題の発生確率を軽減させること。
を実現する点にあると思います。

(2) そうすると、まず、事業者の責任により発生し得るセキュリティ上の侵害は、「個人データ保護」のみに限定される合理性はなく、むしろ「個人データ」と限定的に表記することは誤解を招き不利益と思います。そこで、「(個人データを含めた）すべての取扱い業務データの保護」とするべきと思います。

(3) 次に、「裁判管轄権の所在国」に加えて、「適用される準拠法」をも入力項目に追加すべきと思います。「裁判管轄権」と「準拠法」とは、全く異なる概念で、両方とも等しく重要と思います。(約款などに、たとえ、日本の裁判所に管轄権があるとして安心していても、準拠法が国外法であると書いてあるケースがあります。この場合、日本の裁判所は、たとえ被害ユーザーが日本

人であっても、その国外法を適用して裁判しなければならず、日本人ユーザーにとって極めて不利な結果を招くためです。そのリスクはあらかじめユーザーによって把握される必要があります。）

(4) すべてのベンダの製品・サービスについて、日本人ユーザーに対する、契約相手となる「法人名」を明確に識別できるように、「法人名の正式名称と法人設立国」を記載することを必須とする必要があると思います。その理由を、以下で説明します。

外国系のベンダの場合、本社が外国にありますが、そこが直接販売する場合もあり、あるいは、日本に支店があったり、子会社があったり、代理店があったりと、さまざまなパターンがあります。この場合、ユーザー（債権者）との契約上、製品・サービスの提供元（債務者）が一体誰なのか、導入前に明確でない問題があります。（たとえば、「G 社」としか書かれておらず、「G合同会社（東京都Ａ区の法人)」であるのか、「Ｇ・クラウド・ジャパン合同会社（東京都Ｂ区の法人)」であるのか、「G LLC（米国デラウェア州法の法人)」であるのか、ユーザーにはよく分からず、「G」はブランド力が高いからまあ安全だろう、と、あいまいなまま申し込んで利用開始してしまう、という具合です。）

すなわち、海外企業の場合、日本人ユーザーは「大規模な責任財産を有する、世界的信用のある米国 〇〇 社（複数名の外国人お金持ちの人が取締役をやっており、究極的には、会社に加えて、それらの取締役の個人財産をも追求できるはず)」と取引していると誤認していても、実は、「小規模な責任財産しかない、日本の関連会社 〇〇 社で、資力が十分でない取締役しかいない」と取引していないことがあるのです。

さらに、海外企業はとても賢いので、日本人の多数のユーザーのデータに対して、同時期に大規模なデータ漏えいを過失によって発生させてしまった場合など、同時に賠償請求がなされても日本の小規模な会社の財産の範囲でのみしか賠償せず、本社に影響が生じないような法的工夫（リスク隔離）で防衛がなされている場合がよくあります。日本人ユーザーとしては、担保があると思っていても、実は無担保だった、ということがよくあります。このような誤認から、ユーザーを保護する必要があります。もちろん、「名ばかり法人」をフロントとしているならば、看板貸しなどで責任追及ができる場合がありますが、それはとても限定的な場合で、その立証責任はユーザーにあり、ハードルはとても高く、ユーザーは、かなり不利と思います。

現代では、データの機密性や可用性が極めて重要な財産となっています。ユーザーは、自組織や国民等に権利がある貴重なデータ本体やデータの処理（重要な財産）を委ね、代金に引換えてセキュリティという「債務」を事業者に負ってもらうわけです。

他人に重要な財産を委ねるときは、契約先の相手方の信用資力や担保の有無などを慎重に調べるのが普通だと思います。リスク管理には、これが必須です。他人にお金を貸す場合とまったく同じです。

このように、特に多数の子会社等が複合している海外企業においては、「一体誰が、日本人ユーザーとの契約上の債務者となるのか」明確に判別できることが、各ユーザーにおいて、信用資力や担保をそれぞれ独自に調査する上で、必須と思います。

(5) (4)に関連して、前記(c)を実現するため、取引先となる法人が日本国内にどの程度のどのような担保的な資産を有しているのか、を自己申告で入力・記載することを求めるべきと思います。

多数の日本ユーザーが同時にある外国ベンダの日本法人を経由してサービスを利用しているときで、サービスに脆弱性などの過失があり全部データが流出したとき、全員がその会社に賠償を請求することになります。

日本の行政機関や民間機関などで、国民や顧客の大量のデータを有している場合、それを海外系ベンダが原因で漏えいさせたとき、日本組織は、国民や顧客から、国家賠償や民事損害賠償を求められ、それは払わないといけないのに、いくら日本に裁判管轄権があったとしても、日本にあまり財産がなければ、当該ベンダの子会社法人は損害賠償の支払いはできないので、その原因となった海外系ベンダから補償が得られず（裁判で勝っても、お金がなければもらえない)、ほとんどの額についてユーザーが泣き寝入りとなってしまいます。

このような場合は、ユーザーは予めサイバー保険などに入っておく必要があります。しかし、保険の必要／不要や入るべき金額をユーザーが適切に把握するためには、ユーザーが利用する海外系ベンダの日本国内における担保的財産の額を把握しておく必要があります。

このようなリスク管理のため、日本における担保的責任財産の概要・状況を自己申告で入力させることが必要と思います。これは、入力は必須とせず、「非公開」とすることも認めることでも良いと思います。この場合、ユーザーとしては、「信用が非公開の会社であるので、十分警戒して契約し、サイバー保険にも入っておこう」と認識することができるので、それでも価値があると思います。

(6) 最後に、ユーザデータ等が事業者側の過失によって漏えい・破損・取り出し不能となった場合の損害にかかる、製品／サービスの契約の約款上における、事業者側の損害賠償額の上限規定の概要を、１、２行程度でよいので、明記させるべきと思います。

たいていのユーザーは、「十分に補償してもらえる」と信用していますが、実際に約款をよく読むと「最後の料金支払の１年分を上限とする。特別損害は一切補償しない。」などと記載されています。ユーザーは細かい約款を読まず契約し、実際に問題が発生した時に泣き寝入りになります。ユーザー側では、前記のようなサイバー保険加入や、データの分散・暗号化・マルチクラウドの利用といった対策が可能ですが、そのリスク管理をどの程度の度合いまで行なうべきか経営判断するためには、前記のような、賠償の上限額の有無またはその内容を簡潔に知ることができる必要があります。

ユーザーが約款を細かく読むのは実質的に難しく、また解釈リスクも生じるので、カタログに掲載する側の事業者の自己申告値として、賠償責任の上限の決定方法の概要（１、２行程度）を自己申告で記入してもらうべきと思います。

○荻野構成員

サイバーセキュリティにける事項とソフトウェアに関するサプライチェーンにおける事項は重なる部分があります。今回の事務局資料については、それぞれ独立して項目を出されています。

応募する方、掲載する方に適切に記載して頂くためにも、整理する必要があると思います。(26ページから31ページ）また、網羅性を確認する資料（32ページ）についても再確認すべきかと思います。

○川端構成員

資料2について：従来の法整備の解析については、よく把握された内容で素晴らしく思います。一方で、デジタル化する良さも反映したほうがいいように思います。問題があった時への迅速な対応だけではなく、予防保全についても推進する枠組みが必要に思います。また、共有の加速、プラットフォームへのF/Bもデジタル化の良さなので、その点も盛り込めると良いかと思います。

資料3について：インフラモニタは特に、現在すでに待ったなしに思います。予防保全のテクノロジーの推進ができるような法整備が必要に思います。 規制と調達については、技術確立の段階のPoCまでと、その後の量産について、調達の自由度を変えてもいいかと思います。初期のテクノロジー開発と承認には相応のコストがかかりますが、普及段階になると入札予算ありきになってしまうので、民間事業者の腰が引けることもあるためです。

○小川構成員

本日、発言の機会がありませんでしたので、最後に座長のご指示の通り、こちらに記載いたしますので、皆様への展開と、掲載のほどよろしくお願いします。

本日、3点コメントさせていただきたく思います。

まず、「最低限のチェック」の動的モニタリングの必要性についてです。「最低限のチェック」については、当方も同じく大きな一歩であると評価しています。一方で、テクノロジーは日進月歩で進化するため、一度評価したあとに高度化、更新されることが、容易に想定されます。この場合、当然サプライチェーンにも影響を及ぼす可能性があります。また、テクノロジーを提供する会社のオーナーなどが変更になる、買収されるなどの変化もリスクに影響を及ぼす可能性があります。こうしたリスクの変化に対する、変更管理含めた動的評価、モニタリングの仕組みも併せて導入するべきと考えています。

次に、先ほど岡田先生もおっしゃっていましたが、各自治体、規制所管省庁の購買プロセスにおいて、必要十分な性能要求を理解するに足りる知見の醸成プログラムが必要性ではないかと考えています。性能要求に関する十分な知見がない場合、価格面のみで決定されます。これは民間でもよくあることで、その結果、適切な購買の最終意思決定まで結びつかない、購買後後戻りし、結果としてコストが大きく超過するなどの要因になりえます。各自治体、規制所管省庁側における性能要求水準の維持を担保する、法的、性能、技術的リテラシー、知見の向上トレーニングプログラムも必要なのではないかと考えています。

最後に、今回の規制対応技術、いわゆるRegTechや、Trusted Dataについて、民間側への的確な還元プロセスも視野に入れる必要があると思っています。これにより、今回の取り組みが、社会全体のコスト削減により多く貢献するものと考えています。

RegTechについて、当方も2015年より研究を進めています。米国シリコンバレーでFinTechという競争領域が台頭し、多くのキャピタルが米国に流れ始めた事象を、英国当局は非常に危機感を覚えた。そこで注目したのがRegTechでした。われわれは、RegTechの醸成度合いを、段階的に分類していますが、最初のレベルが、RPAなどによる規制レポート等の自動化や、コンプライアンスリスクのビジュアル化分析で、次がコグニティブ技術、AIによるリスク評価、判断の補助、例えばアンチマネーロンダリングにおける疑わしき者をコグニティブ技術で一時分類するなどといった技術が挙げられます。

そして、非競争領域であるRegTechの醸成度としてもっとも高く分類されるのが、規制対応テクノロジーやデータを共有するコンソーシアム化です。当時、例えばKYC（Know Your Customer）のプラットフォームの構築について民間数社で検討がなされました。しかし、誤った場合だれが責任を負うのか、だれが開発維持コストを負担するのかなど、異なる利害関係の中で多くの難しい課題に直面しています。その結果、民間のみでの限界を学び、国に対する期待が大きくなった経緯があります。

今回の国のコミットは、こうした点からも非常に価値があると感じています。ここで取り上げられるテクノロジーが、民間企業のコンプライアンス対応として利用されれば大きく社会的コストを下げることに貢献すると大いに期待しています。また今回生成されるTrusted Dataは、適切にオープン化されることで、新たなビジネスを創造し、スタートアップ企業を創出することに寄与すると考えています。

今回新たに発足するRegTechコンソーシアムについては、テクノロジーマップのために情報収集するだけではなく、より具体的に民間側への還元手法も含んで議論していただくことを期待しています。

○豊田構成員

本日のミーティングでは時間がなくなったので、かつ今回のより具体性が高まった本題とは少し外れるところなので、あえて発言はしなかったのですが、あえて一点加えさせてください。

これまでのこうした動きでは、どうしても日本の多様な企業や自治体等と内部調整するのに疲弊してそれらの調整で終わってしまい、より国際的な標準化、特に欧州や米国との広域での協調を戦略的に組み込み得ている成功例が少ないように思います。

個別の内部調整を始めるのに先立ってより巨視的な視点での海外の動きをしっかりリサーチしつつ、それらと協調するもしくは戦略的にその先を取りに行くような活動にも、しっかりと予算をつけていくべきように思います。日本の国内での標準化がグローバルスタンダードの中での局所通になってしまわないような視点の提供は、民間企業では行い難く、全部の網羅は無理としても、政府が先導して戦略的領域を抽出し、調査および協調予算をつけていくような事例はあっても良いように感じています。

本日もSIPの話がありましたが、あれなども社会実装がままならないという事のもう一つ先に、仮に実装が進んでも国際標準が取れないという問題が潜在的に待ち構えていると思いますので、そこへの問題提起も今の時点で行っておくべきかと思いました。

あくまで補足的な意見になりますが、議事録に加えていただけると幸いです。引き続きどうぞよろしくお願いいたします。

以上