第1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12月7日（木）16:00～18:00

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	遠藤 典子	慶應義塾大学 グローバルリサーチインスティテュート 特任教授
	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
	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
	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
	中村 修	慶應義塾大学環境情報学部 教授
	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）事務局からの説明

・テクノロジーベースの規制改革推進委員会の開催等について

（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）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の開催について

資料２　テクノロジーベースの規制改革推進委員会 構成員

資料３　テクノロジーベースの規制改革推進委員会 運営要領

資料４　「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４別紙１　技術カタログ運用タスクフォースの開催について

資料４別紙２　技術解説記事「ドローン、3D点群データ等の技術がもたらす効果とミライ」

○須賀参事官　時間となりましたので、第１回「テクノロジーベースの規制改革推進委員会」を開催します。

このたび、デジタル行財政改革会議の発足に伴いデジタル臨調が発展的に改組されたことにより、デジタル臨調及びその下の作業部会は本年 10 月に会議体としては一旦廃止されることとなりました。しかしながら、デジタル臨調と作業部会で行ってきた取り組みは大変重要であることから、デジタル庁において承継し、継続的に行っていくという整理がなされました。先日、作業部会が改組された「デジタル関係制度改革検討会」が新たに第１回として開催されたところです。

本日の委員会は、その会議の下で最初の開催となりますところ、開催回数について改めて第１回とさせていただいています。引き続き、横断的な規制の見直しに活用可能なデジタル技術の精査、安全性や実効性が確認されたデジタル技術の他の規制エリアへの適用可能性等の検討を行うことを目的とし、委員会を続けてまいります。

構成員はこれまでと同じメンバーの方々にご参加いただくこととしています。引き続き、どうぞよろしくお願いいたします。また、会の運営についてもこれまで同様に、議事録や会議の資料については原則公表という扱いにさせていただければと思います。

今、申し上げたことについてはお手元の資料１～３にそれぞれ関連の規程などをお配りしています。また、この委員会の座長については、引き続きデジタル庁シニアエキスパートの江崎浩先生にお願いしたいと思っています。それでは江崎座長、ご挨拶をよろしくお願いいたします。

○江崎座長　江崎でございます。先ほど須賀様からご説明がありましたように、これまでの会議体の組織編成からデジタル庁のほうに「デジタル関係制度改革検討会」として改組するという形になりました。そのため、本委員会も第１回となりますが、基本的には同じ内容、同じ体制で作業を進めていくと理解しておりますので、引き続き私が座長ということでお認めいただければと思います。円滑かつ効果的に議論を進めていく運営に、是非ご協力いただければと思います。どうぞよろしくお願い申し上げます。私からの挨拶は以上です。

○須賀参事官　どうもありがとうございます。それでは以降の議事進行を江崎座長、どうぞよろしくお願いいたします。

○江崎座長　それでは、議事を進めたいと思います。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説明をお願いします。

○須賀参事官　資料４について、説明いたします。冒頭に委員会の概要、テクノロジーベースの規制改革をどのように全体として進めてきたかということを掲載しており、次のページが目次です。今回もテクノロジーマップ、技術カタログ、コンソーシアム、そして技術検証の事業について、それぞれの進捗と今後の課題の定点報告をさせていただきます。

まず１つ目の技術検証事業の進捗です。技術検証は、第１期、第２期、第３期に分けて、それぞれ簡単なところから少しずつ仕様書を固め、検証していただける事業者を決めてその事業者を公表し、順次、検証事業が各地で始まっています。例えば、南極の環境でドローンを飛ばしての点検精度を検証するために、雪の北海道での検証などを始めています。

今回、第３期の公募分についての７事業を含めて新たに事業者の公表に至りました。こちらで私たちデジタル庁が旗を振って各省と一緒に技術検証を行う事業については、全ての事業者が出そろったことになります。

右下の類型２がグレーになっているのは、類型２の中には６つの保安規制条項がぶら下がっていましたが、２度公募しても１件も提案が出なかったためです。それを含めて第３期の公募分についてはいくつかの条項について、事業者から検証の提案をいただけませんでした。提案をいただけなかったことについては原因究明をしっかり行ってまいります。現時点では 32 事業が採択され、予算を使いながら技術検証事業が順次開始に至ったという報告をさせていただきます。

次のページからは、各類型のそれぞれの事業者がどの法令についてどのような検証をどのような技術を使って行うことになったかを、規制所管省庁と完全に合意ができた内容でお示ししています。

実は、この検証事業の中身がいずれも非常におもしろいため、検証事業をやっていただく事業者の代表者にお集まりいただいて対談していただき、デジタル庁のホームページにてそれを記事にすることを始めています。第１弾の記事がホームページに公表されたところです。お手元に別紙２という形でその原稿をお配りしています。お時間があればぜひ記事に目を通していただけるとありがたく思います。

13 ページでは、事業が成立しなかったものをまとめてお示ししています。類型２の６条項はすべてだめでしたが、それ以外に類型４、５、10 については経済産業省、国土交通省、環境省に、それぞれこの条項はこの類型に当てはまるということで非常に前向きにご協力いただいたのですが、こういう技術が使えるのではないかという提案はいただけなかった、という状態になっています。

第３類型に集中したことに象徴されますが、定期検査や点検をデジタル完結するという難易度の高いものが多かったこと、定期点検の対象物が地上の見やすいところにあるのではなく、地下、地盤面下にあったり、一般の家庭や船舶などにあったりと、センサーやカメラを設置して常時監視することはなかなかやりづらい業務が多いことが特徴です。

右下に小さく書いていますが、該当項目を足し上げると、今回デジタル庁で 460 条項について技術検証の成立を目指しましたが、そのうち 8.9%に当たる 41 条項が不成立だったという形になっています。

次のページで不成立となった原因分析をしています。なぜ成立しなかったかというところから、非常に大きな知見を得られる可能性があると思っているためです。私たち事務局として持っている仮説は４つです。まず１つ目に、技術があるなら使ってほしいと規制当局は思っていても、実は技術自体が存在しない可能性です。２つ目に、技術自体はあっても技術成熟度が低いという可能性があると思います。１と２は同じようなことかもしれません。それに対して３つ目に、技術自体はあっても規制当局が期待しているほどの精度が出ないことも含めて十分な性能基準を満たす技術になっていないか、あるいは私たちが公募する時に、満たして欲しい基準の設定や説明が十分具体的にできなかった可能性です。４つ目は、公募が第３期になって開始が遅れたため、時間がない、あるいは人手が足りないといった、技術の有無とは別の理由があった可能性を考えています。

私たちは不成立となった8.9%を大事にし、この仮説を深掘りしたいと思っています。まず、技術自体があっても私たちが探索しきれていないとするともったいないため、技術や製品情報の調査を独自にやってまいりたいと思っています。一方で、私たちの募集の仕方が十分に具体的でなかった可能性を踏まえ、技術保有事業者になぜ応募しなかったか、どうすれば応募したかといったアンケートやヒアリングを実施し、公募の課題も含めて洗い出したいと考えています。何か分かってきたらまたご報告させていただきます。

続いて２つ目の論点、テクノロジーマップです。こちらは長きにわたりこの委員会で議論していただきましたが、ついに10月６日にデジタル庁のホームページに、法令に基づいて公表するテクノロジーマップ第１弾をアップすることができました。資料16ページの画像はデジタル庁のホームページのスクリーンショットです。このページが私たちの関連の取り組みの中では最大のアクセスをいただいています。

17ページからは実際に公表しているテクノロジーマップのバリエーションを示しています。簡略版が２種類あり、１つ目は、法令とは関係なく管理対象毎に分類して縦軸に設定しています。２つ目は、法令担当の方に分かりやすいように規制の類型に寄せて縦軸を整理しています。当面はこの２種類を維持することになりましたので、両方を提示しています。可読性が高くなるように少し大くくり化したものが簡略版の２つのバージョンで、委員会で議論する際にお見せしていたのは19，20ページにある非常に細かいものです。今はデジタル庁のホームページのスペックの問題で検索機能は付けられていないのですが、今後はもう少しインテリジェントに自分たちで軸を選んだり、検索をかけたりといった表示調整ができるようにしたいと考えています。

最後に21ページについてです。テクノロジーマップは現在使っていただける技術類型をマッピングしたものをホームページに公表していますが、先ほど申しました通り、技術はないが欲しいというエリアは、技術検証に手が挙がらなかった類型があることからも存在しそうだということが分かってきました。技術代替に向けて課題が残っている領域、活用可能性がある領域、検証が完了した領域といった3種類くらいのテクノロジーマップを出していけるとよいのではないかと思っています。現時点では活用可能性が検証しなくてもあると分かっているものだけが出ている状態ですが、技術代替に向けた課題があり、むしろ募集したい領域についてのマップも作りたいと思いますし、技術検証を精力的にやっていただいている結果を何らかの形で反映したマップが作れればよいと考えています。以上がテクノロジーマップについての報告です。

続いて技術カタログについてです。それぞれのマップからカタログに飛べるように作っていきたいと考えていますが、この委員会において、まずは技術検証を要しない情報から先行的にカタログを整備しますという説明をさせていただいてきました。

現時点で検証事業を実施しているのは、1,043条項のうちデジタル庁が460、各省が590あり、それ以外の8,600条項については技術検証を経ずとも既にテクノロジーがあるので使って構わないと規制当局が言っている条項です。それらについてカタログを順次整備しています。

第３回までに分けてカタログ公募を実施し、以降、第４回、第５回と続けていく予定です。これも後ろに行けば行くほど難易度が高くなる募集ですので、どのような応募要領を作るか、どこを聞くかということで事務局は苦労しています。第１回と第２回のカタログ公募については既に終了しました。第１回ではセキュリティの問題などは聞かずに公募しておりましたので、事業者

に追加で回答をいただきました。講習・試験については27件を載せていたうち、17件に追加の情報提供に応じていただき、カタログに掲載しています。

それに対して第２回の往訪閲覧・縦覧は相当に難しかったようで、応募自体が７件、さらに規制当局が要求する「のぞき見防止機能」を満たす製品やサービスの応募は１件もなく、ここはポテンシャルエリアということかと思っています。

サイバーセキュリティ管理については、この委員会で質問事項をもっと増やそうという議論をしていただきました。実際に事業者から、どう書けばよいか分からないという質問が最も多かったのがこのサイバーセキュリティの追加の質問でしたが、その中でも記載していただいたものがカタログとして出ています。

カタログで出していただいた情報を踏まえて私たちが得ている所感としては、サイバーセキュリティ管理に関して第三者認証を取っている、あるいは国内外のガイドラインに準拠している、もしくは独自の脆弱性検査を実施している場合が大半ですが、それは組織や企業のレベルで行っているものがほとんどで、製品やサービス単位で認証を取得しているものは少ない印象です。それから、技術を使って損害が生じた時に日本において責任財産を持っているかという質問を追加しており、損害賠償の上限規定についてはほとんどの企業から回答がありましたが、担保資産が日本にあるかどうかについてはほとんどの企業が非公開となっています。このあたりについても課題があれば、後でコメントをいただきたいと思います。

27ページは、現在カタログ公募を行っている第３回公募の２つの類型についてのまとめです。広域的に自然環境などの利用状況を確認したり、災害時の被害を把握したりといったことをデジタルで行う技術と、事業場の管理や業務状況の確認を実地で調査しているものをデジタル完結できないかという内容です。スマートグラスなどがここで出てきます。公募の締切りは12月22日ですが、順次タスクフォースで精査していただき１月以降にカタログとして出していきたいと思っています。

続いてコンソーシアムについてです。８月４日にRegTechコンソーシアムを立ち上げ、10月27日に「RegTech Day」というキックオフイベントを開催しました。皆さんのご協力をいただき、本当にありがとうございました。RegTech Dayには大変多くの方々に参加していただきました。
我々が目指すのはSlackのコミュニティに入っていただく方を増やすということでしたが、「RegTech Day」の開催によって申込者が少し非連続に伸びています。

ただ、本当はここからより一層参加者を増やしていかなければならないのですが、その後は伸び悩んでいることから、コミュニティとしてどう盛り上げるかに課題があると認識しています。

次のページは「RegTech Day」の開催報告です。リモートの配信イベントとして、登壇者には現地に集まって議論していただきました。参加者からは、何をしているかやっと分かったというような肯定的なコメントをたくさんいただいています。

「RegTech Day」の開催前後に様々な広報をしており、デジタル庁のオウンドメディアの取材も含めていくつかの記事が出ています。

次のページは参加者のアンケートです。満足度は基本的に高めであり、様々な属性の方にご参加いただくことができたと思っています。

次に今後の方向性です。「RegTech Day」当日の視聴者数は450名近くとなり、延べの視聴回数は1,000回近いということでたくさん見ていただけたと思う一方で、豪華なメンバーで開催してコンソーシアムへの参加を呼びかけたわりには、コンソーシアムへの参加者が少なかったことは課題だと思っています。私もコンソーシアムのSlackに入っていますが、私の立場でも何を言えばよいか困るような過疎の状態になっています。これからコンテンツをしっかり詰めて、活気のあるコミュニティに仕上げていきたいと思っています。

次のページは「RegTech カフェ」です。「RegTech Day」のような大きなイベントをそれほどたくさんやるつもりはなく、むしろ現場で困っていることや検証事業でどんな課題が見えてきたかといった細かい気づきがそれぞれ非常におもしろいため、勉強会のようなものをオンラインで続々と開催したいと思っています。「RegTech カフェ」の第1弾は12月20日（水）からオンライン開催したいと思っていますので、ご参加いただけるようでしたらQRコードからアクセスをお願いします。

次のページは以前に説明したもののアップデートとなりますが、今後も様々なイベントを仕込みながら活動してコミュニティを盛り上げていきたいと思っていますので、どうぞよろしくお願いします。

最後に、今後のスケジュール等についてお話しします。約1年前に、RFIということでアナログ規制の見直しに活用可能性のあるデジタル技術について幅広く情報提供の依頼をさせていただきました。その時には、年末年始の募集だったにもかかわらず大変多くの応募をいただきました。応募したがその後どうなっているかという問い合わせも複数いただいていますので、どのように使われているか、どのように使っていきたいかをまとめました。

まず、テクノロジーマップをつくるにあたって、どのような製品が実際に存在するかという情報として参照させていただきました。さらに技術カタログについても、RFIで提供していただいた情報の中からカタログに当てはまると事務局で判断したものについて、掲載してもよいかどうか個別に企業に問い合わせました。講習・試験に1社、往訪閲覧・縦覧に2社、第3回の広域把握・実地調査に29社が該当しますが、カタログに移行していただく調整をしています。

技術検証については、想定される技術について規制当局にイメージを持っていただき、それを仕様書に落とすという作業がありました。その際の想定技術としてRFIの情報を参照しています。検証事業の実施事業者を公募しているのでぜひ応募してほしいというお願いも個別にしています。

また、応募していただいた方とは今後も接点を持ちたいということで、コンソーシアム、「RegTech Day」を含めたイベントについての情報を随時、プッシュでお届けしています。今後もこういった情報提供にしっかりご恩返しできるように、無駄にしないようにしていきたいと思っています。

テクノロジーマップ整備事業の今後のスケジュールですが、第1弾のマップを10月に出し、その後は随時更新としています。その中でマップにバリエーションを出すというタスクがあり、来年にはポテンシャル領域のマップという形で出せたらよいと思います。

カタログは5回に分けて公募して公表してきましたが、これらは検証の必要がない分野です。技術検証を行ったエリアについても、随時カタログへの掲載を始めることになると思っていま

す。その間、RegTech コンソーシアムを関係者の皆さんが直接つながっていただけるコミュニティにしていく活動を続けていきます。本年も大変お世話になり、どうもありがとうございました。
○江崎座長　どうもありがとうございました。別紙などの説明は行わなくてよいでしょうか。
○須賀参事官　別紙２はすでにネットに公表しているインタビュー記事で、ぜひ読んでいただきたいと思って提供しました。別紙１はすでにご議論いただきましたが、カタログに載せる前にスクリーニングをかけるために技術カタログ運用タスクフォースを設置し、稼働を始めていることの報告です。
○江崎座長　ありがとうございました。それでは、これからの時間は意見交換となります。ご質問、ご意見等があればいただきたいと思います。発言したい方はチャットに名前を書き込むか、挙手機能でお知らせください。よろしくお願いします。
○中村構成員　技術検証の運用性のような部分についてはどのようにお考えですか。９割の技術検証事業が採択されて具体的に動き始めていて、10%は応募がなかったという説明がありました。私もこの 10%はとても大事だと思いますが、その中で具体的に手が挙がらなかった背景には、例えば検査などの実際の業務をする人たちの運用性があると思います。テクノロジーとしては存在しても、実際の運用はなかなか難しいので手を挙げられないというようなことについては、今回、デジタル庁として何か考慮されていますか。
○須賀参事官　ぜひ仮説に組み込んで検証したいと思いますが、今すでに実証を始めている類型の中にも、やればできるが遠隔で指示するのは面倒といったコメントがありました。運用性にはそのようなことも含まれるのかと思います。資格を持っている人が現地に行かなくてもリモートで「もう少し右下を見たい」といった指示を出し、現場の人がカメラを向けたりドローンを近づけたりといったことが技術としてはできても、現地で見たほうが早いというようなコメントもいただいています。そのようなことから、手が挙がらなかったというより、検証してみてやはり面倒だとなる部分があるように思っていました。そのあたりはどうでしょうか。
○中村構成員　私も具体的な話ではないのですが、検査などでは資格を持つ人が作業しなければいけないといった状況があると思います。そのような状況になった時に、資格を持つ人が高年齢になっていて、新しいテクノロジーを入れるよりも自分が見てサインするほうが早いというような背景があって応募がなかったのではないでしょうか。すなわち、テクノロジーとしてアナログかデジタルかではなく、検査の仕方などでの問題、例えば有資格者は誰で、誰が何をしなければいけないかという運用を含めた形で今回は検証できるのでしょうか。それとも、既存のルールに従う形でデジタル技術が使えるかどうかだけを検証するのでしょうか。そこに大きな違いが出てくるのではないでしょうか。
　すなわち、それぞれの検査項目といった本質的なやり方や、免許を持つ人がどのような形で携わらなければいけないかというところまで含めて変えていく必要があると思います。今回はそこまで踏み込んでいないということですか。
○須賀参事官　これから原因分析をしていきますので、そのような可能性もぜひ含めたいと思います。有資格者が現地に行かなくてよいだけで、最終的には有資格者が見て判断することに頼って検査していることは変わらないとすれば、それはデジタル完結の１つ手前のフェーズにある可

能性もあり、だからこそより難しい面があるのではないかと思います。エンドトゥーエンドで有資格者の人的な関与をなくすような方向で検討しないと技術が入っていかない可能性もあり得ると思いますので、その点も含めて分析したいと思います。
○中村構成員　その辺が大事だと思いますので、よろしくお願いします。
○江崎座長　As Is から To Be に行きたいけれど、その途中の段階もあったりするので悩ましいところです。もう１つは法律や規制を技術に合わせてどう変えていくかというところも重要な仕事だということのご指摘だったと思います。ありがとうございます。登構成員、書き込みをいただいておりますが、その説明も含めてご発言いただけますか。
○登構成員　現行の技術カタログの公募フォームの内容を確認し、気づいたことがあります。応募フォームに設問を追加したほうがよいのではないかと思いますので、提案させていただきます。

ポイントを申し上げると、応募技術の中に個人情報を扱うサービスがあると思います。個人情報を扱うサービスで、かつ外国のパブリッククラウドをシステム基盤として利用している製品の応募もあると思いますが、個人情報が漏洩することを防ぐ措置がなされているかどうかについて今のフォームの入力項目だけでは不安なケースがあります。あらかじめ重要な点は設問に入れておくことがよいと思います。

具体的に追加したほうがよいという設問は、個人情報が保管されることになるサービスに限定して生じるものです。まず情報が保管されるのはオンプレかクラウドか、日本国内か国外かということを記入してもらうべきです。さらに、利用されているパブリッククラウドサービスの名前を書いてもらうべきです。ここまではそれほど難しくないのですが、肝心なのは、保存される個人情報が暗号化されているとしても、暗号化されたデータが、日本国の司法審査を経ずに外国国家による外国法に基づき強制捜査またはデータが取られる恐れがある場所にあるかどうかを確認することです。

ここからさらに、暗号化の強度の確認や、外国の政府がデータを取れるとしたら、暗号鍵も外国の政府が勝手に取れる状態になっていては暗号化の意味がないため、別の場所に保管しているかということの確認をするとよいと思います。

最後に、日本国の司法審査を経ずに強制的に取得される可能性を技術的にどのように予防しているか、その具体的な措置を書いてもらいます。これはどのように書けばよいか分からない人がいるので、いくつか記入例を設けておくイメージです。

このような設問を入れなければならないと考えた理由を示します。ヨーロッパでは 2018 年頃から問題になっていることですが、ヨーロッパはいろいろな個人情報保護の法規制をつくっています。今ヨーロッパ各国が問題にしている代表的な課題は、米国政府の「米国クラウド法（CLOUD Act)」という法令への対処です。これはヨーロッパでは個人情報保護上の問題になっています。米国クラウド法のポイントは、この技術カタログへの応募者が利用している米国のパブリッククラウド事業者は、契約上はデータを勝手に見ないとなっていたとしても、米国政府の権限でその約束を上書きしてデータが勝手に米国政府に提出されてしまう大変に強い法律であることです。

米国クラウド法の元では、米国の州政府や連邦政府が捜査令状あるいは行政召喚状をパブリッククラウド事業者に出すと、たとえそのデータが日本にあっても、アメリカなどから遠隔でコピ

ーされてしまうというリスクがあります。これが問題なのは、司法妨害や裁判所侮辱罪といった刑罰が科されるので、日本の顧客を保護したいとアメリカのクラウド事業者が思ったとしても、従わなければならないと思われることです。

これについては日本でも国会答弁があり、2019 年 6 月に「個人情報保護法における、法律に基づき他人にデータを渡すことを例外的に許容する規定のうち『法令に基づく場合』(同法規 27 条１項１号）の『法令』というのは、『日本の法令』に限定する」というのが政府見解答弁です（「米クラウド法と個人情報保護法上の対応に関する質問主意書」第 198 回国会衆議院内閣総理大臣答弁第 227 号)。したがって、米国クラウド法に基づいて米国政府がいつでもデータを取得できてしまう状態に置いているということは日本の個人情報保護法の例外的な除外理由にならず、個人情報保護法の 23 条の「データの漏洩を防止する措置」が講じられていないと認定されるリスクがあると思います。

ここまでは当たり前の話ですが、ほとんどの人はそれを認識した上でクラウド上に置くデータは暗号化されていると思います。もし、応募データに、暗号化されていないと書いてあったり、されていても例えば AES256 で暗号化していると書いてあったりするだけで、その暗号化がクラウド事業者のサービス基盤の機能としての暗号化なのか、事業者が独自に暗号化しているかの区別がフォームを見ただけではできないため、個別に問い合わせが必要となります。

クラウドサービス事業者の行う暗号化には２種類あります。第１に鍵がクラウド事業者のデータとして保存されている形式ですが、これでは意味がありません。第２に鍵をクラウド外に保存する方式があります。第２の方式による保護が確実になされているかどうかを見る必要があるため、設問に入れるほうがよいと思います。

最後に、米国クラウド法のことを書くとなると、日本政府と米国政府のパートナーシップは非常に重要であり、米国クラウド法に注目することは信頼関係を損なうおそれがあります。そのため、設問の中では「米国クラウド法」のように「米国」を名指しすることは避け、「外国の法律」と一般化した表現を用いたほうがよいと思います。

これらの設問には、応募者の技術者であれば新しいアイディアを考案することなく答えられ、それほど負荷は生じないと思います。以上です。

○江崎座長　説明と提案をありがとうございます。これについて他の構成員の皆様からご意見等はございますか。個人情報の保護は非常にセンシティブというか難しい問題になっていますが、ご指摘の政府によるオーバーライドの権限が出てきているので、ローカライゼーションをしっかりした上で、かつ鍵管理がしっかりできていないといけないという指摘と要望ということですね。データマネジメントが専門の方から何かご意見等はございますか。

○荻野構成員　私は、サイバーセキュリティに関する技術カタログの応募時のヒアリング内容を事務局と一緒に作成しています。急場しのぎというのは否めないところで、サプライチェーンリスクについてヒアリングしなければいけないのですが、企業の方々に分かって頂けるような言葉で聞かなければいけないということと、専門家がいないとなかなか書けないような質問になっていること、また、設問の内容が NIST で出しているサプライチェーンのガイドラインのサマリーを書いただけの状況になっています。もう少し現実的な内容にしていく必要があり、技術カタログでは応募企業がどんな脆弱性試験をやっているか、どのような認証を取っているかといった形

で、分かりやすく修正を加えていくべきだと思います。時間を優先してしまったので、今後は、もう少し修正していきたいと思っています。一般の方にも分かるように書かなければいけないと思っていますので、事務局と一緒にやっていきたいと思っています。

○江崎座長　中村構成員、発言されますか。

○中村構成員　たぶん荻野構成員の言っていることと同じで、相手のレベルがいろいろなので、登構成員が言われたような形での設問は、どちらかというとデフォルトがYESになるような設問にしていただいていると思います。「米国」を「外国」と変えてしまうと逆に、中国や韓国のことも、ヨーロッパのことも考えなければいけないというように、皆さんが想像を膨らませてしまうと思うのです。

僕がコメントしたのは「～を推奨する」というような言い方にして、そうでない場合にはそれぞれの項目についてディスクライブしてほしいという書き方のほうが分かるのではないか、分からない人にとっては、推奨されたことをそのままやるというほうが楽なのではないか、と思いました。

○江崎座長　他にご意見はありますか。これを100%やろうとするとかなり難しい、しかもサプライチェーンでやらなければいけないということになると、ほぼ作業はできなくなることも懸念されるので、落とし所をどうするかというのは難しいところです。これはそのあたりをきちんと意識した形で今後のエンハンスメントというか修正等を進めていくのが現実的ということになるでしょうか。登構成員、どうですか。

○登構成員　まさにそうです。「外国」と書くと混乱するのではないかという意見をいただきましたが、これは、データの法規が日本国内にあるかそれ以外かを聞くことにより、日本のほとんどの事業者は日本国内のクラウドサーバーを借りているので、中国かヨーロッパかと迷うことはたぶんないのではないかと思いました。

次に、江崎座長からご指摘のあった、サプライチェーンを含めると対策が難しいのではないかという話は、私はそう思いません。標準的な機能として暗号鍵を事業者側のサーバーに置くといったことがありますし、もしそういうものがないクラウドを使っていても、クラウドの中で動くIaaSであればディスク上の暗号化、データベースの暗号化があり、SaaSのようなものであれば格納するデータの暗号化の機能があります。また、応募の内容を見て、大体の場合は暗号化していると答えているのであれば、サプライチェーン全体を考えて意味不明な状態ではないことを維持するのはそれほど難しいことではないのではないかと思いました。

○江崎座長　クラウドに関しては、特に大手のクラウドはそういうトランスペアレンシーをしっかり出しているのですが、そうではない機器が実はたくさん存在していて、そういうものはなかなかクラウドのようなトランスペアレンシーは確保できていない状態と認識しています。クラウドであればおっしゃる通り、それほど手間はかからないし、そういう機能を特に大手のクラウドは提供していると認識しています。

○登構成員　まさにそう思います。クラウドではなくオンプレミスの場合に、かつそれが日本国内であって自社または委託会社が管理・支配している場合には暗号化する必要はなく、外国国家がそれを押収することは物理的に不可能です。オンプレミスの場合は、日本国の司法審査を経ずに外国国家が取得する可能性は元々ないので、それ以降の設問にもすべてNOと答えることができ

ます。小規模なサーバーをデータセンターなどに置いているケースは、オンプレミスかつ日本国内を選択すればよいので、それほど心配ないのではないかと思います。

大手の米国のクラウド事業者の場合には暗号化の仕組みがありますから、そのどれを選定しているかを書けばよいということです。小規模な日本のレンタルサーバー会社のようなところを考えますと、われわれは、そういうところを応援しなければなりませんが、そのサービスを使う場合も、クラウド事業者等の第三者が管理・支配する装置または機能の一部であり、データの保管場所が日本国内のみとなっている場合に当てはまります。そういった小規模な事業者は米国クラウド法の管轄にそもそも当てはまらないので、強制取得のリスクはないのではないかと思います。日本の会社であれば通常はそうだと思います。

例外として、日本の小さなクラウドサーバーに見えるものが、実はアメリカにも同一法人が拠点を持っている場合には、アメリカの拠点に米国が最低限の接触という概念で命令を下すことがあります。そういう限定的な場合については、日本の司法審査を経ずして外国法に基づきデータの強制捜査あるいは取得されるリスクがないかどうかを日本のクラウドサービス会社に聞かなければいけないのですが、それほど多くないのではないかと思います。オンプレミスと日本国内であればそれほど重大なリスクはなく、たいていの場合はできる事柄ではないかという感想を持ちました。

○江崎座長　単純にサーバーを利用しているだけではないような IoT デバイスが入る、あるいは違うシステムが入ってくると、機器自体がクラウドの別のところと知らない間に話しているということがありますので、そのあたりは荻野構成員のチームで考慮しているというように認識しています。中村構成員が書いていたように、「こういう形を推奨する」という形が現実的かもしれないですね。

○登構成員　テクノロジーマップ及び技術カタログで何かを推奨することは新たな挑戦に見えるのではないかと思います。仮にプライバシーの問題について推奨の構成を書くとなると、その他にも安全性や可用性について推奨することが出てきて、それを記述していったならば、ついには情報学の教科書が一揃いできてしまうのではないかと思い大変です。特にプライバシーの問題については、他の問題と比べて大きな看板を掲げる必要は今のところはないというか、推奨ガイドラインを書く必要ないのですが、ご指摘の通り、どう書けばよいか分からないという場合があります。それは設問のフォーム上に注釈としてカンニングペーパーのような感じで回答例を記載しておけば、何も考えていなかった人もそれを読んで理解できるのではないかと考えます。

○江崎座長　ありがとうございます。中村構成員から、記入ガイドがあればよいのではないかという意見をいただいているので、そのあたりについては関係する方々で議論しながら方向性をつくり、可能であればこの委員会でもう一度相談して進めるという形が適切ではないかと思います。事務局として何か回答はありますか。

○須賀参事官　座長がおっしゃった形で進めたいと思います。大変貴重なご指摘をいただいたと思う一方で、中村構成員もおっしゃっていましたが、今の設問でも難しいということで質問が殺到しています。記入する人のリテラシーと、さらにそれを読んで調達する人のリテラシー、この中には政府の職員も入ってきますが、その二段階のハードルがあります。両方にとってその項目が何を意味し、何に気をつけなければいけないかということが即座に分かる UI を実現したいと思

っています。応募のハードルがどんどん上がっていくことのないようによくご相談しながら、ご指摘いただいた点に対応できる方法を考えたいと思いますので、よろしくお願いします。
○江崎座長　まさにサイバーセキュリティのところは非常に厄介で、レベルも非常にばらばらの領域ですからかなり力を入れていかなければいけない領域ということだと思います。ありがとうございます。他にご意見、ご質問等はありますでしょうか。小川構成員、お願いします。
○小川構成員　２点あります。今お話のあったクラウドにも少し触れたいと思います。我々のように財務データや当局向けのレポート、コアデータの生成過程にクラウドを使う場合は、サードパーティリスクというリスクカタログに当てはめ、そこをどのように担保するかということで、まず一義的にSOCレポートを必ず入手することになっています。
SOCレポートには３つあり、１は財務省ですが、２はセキュリティの多様性、機密保持、プライバシー、インターブリッジといったことですので、まずそれをもらいます。これは通常、クラウドを使っているようなベンダーではほとんどの人が理解できるので、それをもらうというのが１つだと思います。
それをもらうだけでは弱く、サードパーティのクラウドから問題が起こるケースが非常に多いので、「これだけではだめ」というのが今の潮流です。中のスコープがきちんとカバーされているかどうか確認することが企業のコアデータについては求められています。
クラウドで国内か国外かというのは絶対的な要件と思いますが、その次にクラウドの信頼性があります。サイバーセキュリティのみならず、SOCは十分な内部統制があるかということを評価した第三者評価のレポートですので、ベンダーであればある程度分かっていると思います。昨今は最新の技術でクラウドを使うケースが非常に多く、企業自体はスタートアップだったとしてもクラウドは大手を利用するケースがありますので、そのあたりが１つのポイントになると思います。
もう１つは別の話で、RegTechコンソーシアムについてです。非常によい取り組みだと思いますし、今回の取り組みの中では情報収集の重要なチャネルの１つと思います。このコンソーシアムをこれからよい議論の場にしていくというお話に賛成です。私もこのコンソーシアムを宣伝したいと思い、いろいろな民間企業のエグゼクティブと話していますが、その中でいくつかの課題をいただいています。
期待される参加者はどういうベネフィットを得られるかということがあります。デジタル庁としては、こうすればもっとよくなるという意見を広く募ることが大きな目的だと思いますが、参加する側はどういう情報を得られるか、もしくは自分たちの活動にベネフィットがあるかというところが見えにくいという意見を聞きました。
技術保有事業者にはスタートアップのような企業もあれば、例えば規制対象事業者として大手の民間企業もあると思います。それぞれに求めるベネフィットは違うと思うので、ある程度の仮説を立て、どういう形でやっていけば参加者が満足できるかということはもう少しブレークダウンし、ステークホルダー別に分析してもよいと思います。
例えば、ピッチランをやっていくという説明がありましたが、UKのFCAは「テック・スプリント」ということで、民間の橋渡しとして当局側がサンプルデータを準備してハッカソンに民間企業を巻き込み、その成果を広く公表しています。民間のスタートアップは、その場で自社の技術

が公表されることは非常に大きなメリットになるので、多くの会社が手を挙げています。ピッチランをどういう形で組んでいくかということも重要だと思います。

それから、規制を受ける側の企業もテクノロジーを探し求めています。例えばコンダクト・リスク・モニタリング、トランザクション・モニタリング、データ改ざん、あるいは棚卸しの客観性ということでドローン、これは我々監査法人もすでに使っています。そういったところにも技術をどんどん入れて、人員とコストの削減を目的にデジタル化していくという大きな潮流があります。そういったところにデジタル庁の今回の取り組みによって参考となる技術が提供できれば、彼らも多く入ってきて、そこでどのようにトラストを実現していくかという民間企業側からの意見も吸い上げることができると期待されますので、RegTech コンソーシアムをいかに有効に運用していくかということに期待しています。

○江崎座長　２つの重要なお話をいただき、ありがとうございます。事務局から回答はありますか。

○須賀参事官　資料４の 35 ページに、我々の妄想も含めて各ステークホルダーに対してベネフィットやバリューを提供するためのイベントや仕掛けをマッピングしてみました。そういう意味では「RegTech Day」は始めの告知、Slack コミュニティの存在を知ってもらうという目的で開催しましたが、それだけでは Slack に常駐していただけるわけではないというのが現時点の状況と思います。ピッチランもうまく仕込む必要があると思いますし、技術検証でどういうことをやっているかという記事の配信、カフェでの勉強会など、いくつかを積み重ねながら何がお役に立つかということの試行錯誤をぜひやっていきたいと思っています。それぞれのイベントの仕込みについては、計画した段階でまた相談させていただきご知見を賜りたいと思います。ありがとうございます。

○江崎座長　たぶん小川構成員がおっしゃったのは、皆さんが PR できそうなスライドがあるとやりやすいということもあるように思いました。

○須賀参事官　コンソーシアムのチラシのようなもの、QR コードが入っているようなものでしょうか。ホームページにも QR コードは入れていますが、フライヤーなどがよいでしょうか。アイディアがあればいただければと思います。

○江崎座長　小川構成員、いかがですか。

○小川構成員　おっしゃる通りだと思います。私はこの案件に関わっているのでよく理解していますが、新しい人たちをどんどん巻き込んでいくには、ぼんやりした絵なのか、すごく細かいものなのか、民間企業が入るには人員やコストを割くことになりますので、それなりのベネフィットをもっと分かりやすく示してほしいと思います。コンソーシアムに入ることでどういうことが起きていくのか、何が期待されるのかということを提示していくのは重要なプロセスだと思います。非常に期待していますので、よろしくお願いします。

○江崎座長　事務局への宿題ということですね。

○須賀参事官　ありがとうございます。デジタル庁のホームページをあまり見ていただけないのです。そこにいろいろ書いているつもりですが、書き方の問題でしょうか、PR がうまくないということだと思いますが、デジタル庁本体の広報チームにも手伝ってもらい連携して工夫したいと思います。

○江崎座長　川端構成員が書き込んでいるのはまた違う話のようですが、ご発言いただけますか。
○川端構成員　「RegTech Day」の開催についてはできるだけ役員クラスの知人がいるところや仕事の中で関係先に話して、参加していただいたりしたのですが、その上で応募のハードルは高いと言われました。その理由が大企業とスタートアップでは違っていたので、そのことを共有したいと思います。
大企業の場合、こういった応募に関して法務的な部門を通さないといけないため、応募までの時間が足りないということでした。また、新しい取り組みやデジタル化の取り組みについては、コンソーシアムといった形で他企業と連携しながらやっているものが多いので、応募にあたってもいろいろな会社を説得しなければいけないということがあるようです。そういった意味で応募のハードルが高いということで、リードタイムが欲しいということだろうと思います。
それからスタートアップは、非常に興味があるのですぐ応募するという返事があったものの、スタートアップは他社と組んでいることが多く、いざとなると相手企業の合意を取ることがなかなか難しいと聞いています。スタートアップのコンソーシアムのようなところに声をかけると、応募が少し進むのではないかというアドバイスをいただきました。応募に関するフィードバックをお伝えしたいと思いました。
○江崎座長　ありがとうございます。実際にやろうとすると合意を取らなければいけないプレイヤーが多いということがあり、苦労しているところがあるということだと思います。少し応募しやすいような形を考えるというのが宿題になるかと思います。岡田構成員、ビジネスチャンスが見えないのでなかなか応募しないのではないかという趣旨で書いていただいているようですが、ご発言いただければと思います。
○岡田構成員　先ほどの応募がなかったということについて、別にエビデンスがあるわけではなくて個人的な印象ですが、まず１つはカーボンニュートラルの影響で石油産業や大手のプラントは縮小傾向にあるところがわりと増えてきているので、こういうところにデジタルで参入してもビジネスチャンスはないのではないかということがあります。未来の産業構造を考えて、これからより広がっていくようなところはデジタル化するところに入りやすいと思いますが、縮小傾向にある業界では何か工夫をしないと規制改革だけではデジタル技術の導入にはなりにくいのではないかと思います。
もう１つ、船舶はパターンが多いので、１つの方式や技術では手に負えないのではないかという気がします。定期検査の詳細を吟味しないと明確には分からないですが、船舶関係の業務への新技術導入は非常に難しいと思っています。おそらく、船舶における検査などの業務を調べれば調べるほど、儲からない、つまりビジネスモデルが見つからないという気もします。技術があるかないかという以前に、ビジネスとして成り立つのかということを考えることが大事です。ビジネス環境が整っていない業界において、新技術を積極的に導入したいのであれば、たとえば成長産業と組み合わせる、税制優遇などの特例化を行うなど、新しい動きの呼び水になるようなものを考えていかないとうまくいかないという感じがします。
テクノロジーマップの中に産業界の特性も盛り込み、規制改革だけでは背中を押しにくい場合には何らかの支援を行う形にしなければいけないと思います。

○江崎座長　ありがとうございます。他人任せではなく、産業界が自主的に取り組むための機会になればという感じもあるかと思いますが、そういう問題意識を持っている方からすると、ここに載っていないような話が出てくるようにできれば建設的にもなるでしょうか。
○岡田構成員　そうですね。それもありますし、検査などを技術に任せて、もし間違っていた場合に誰が責任を取るかということへの不安も少なくありません。「計測は自動、最終判断は人」とするのか、「計測から最終判断まで機械やAIが行う」という技術の形式だけではなく、使用者責任・製造者責任など責任をどう分担するのかが見えないことは技術導入の障壁になるでしょう。皆が疑心暗鬼になっている事柄についてきちんと答えていくことも大事です。ITに関する理解度はまだまだ低く、よく分かっている人が社内には少ししかいないという会社も少なくありません。２番手、３番手なら安心して導入できるでしょうが、１番手ではできないという事業者・自治体がほとんどです。１番手の引き受け手をうまく見いだす仕組みも大事と思います。
○江崎座長　それはデジタル臨調の進め方の本質的なところになるので、ここの実務部隊も意識する必要はあります。もう１つ上のほうで、産業界の意識をどう変えるかということのトリガーをどう引け受けるかという話をしていただくとよいかもしれません。
○須賀参事官　規制当局の側から、技術があるなら使ってほしいとせっかく言っていただいているので、もったいないという気持ちがあって、こういう表になっています。確かに岡田構成員がおっしゃったように、そもそも市場がないとか事業性が見通せないといったことも仮説の中に入れておくべきと思いました。ありがとうございます。
○江崎座長　ただ、それで固まってしまうと非効率的かつ最悪の10年になってしまう危険があるので、考えなければいけないと思います。中垣構成員、いかがでしょうか。
○中垣構成員　岡田構成員の内容とほぼ同じですが、私が関係している電気事業法という類型５について思っていることをお話しすると、まさに行ったほうが早い状況だと思われます。電気主任技術者、発電機であればタービンやボイラーの主任技術者がいて、訪問して点検します。一般家庭でも何年かに１回、例えば４～５年に１回、電気保安協会の人が来たりすると思います。
　１件当たりの頻度が４～５年に１回ということになるので、対象は多いのですが一般化しにくく、そこにカメラを設置しても投資回収できないビジネスモデルになります。デジタル完結型のセンサー・カメラ設置というと、電気関係では定点で常時監視して変化を見ることに向いている技術なので、そのあたりは応募がなかった理由だと思います。あとはほとんど岡田構成員と同じです。
○江崎座長　ありがとうございます。そのトリッキーなところを越えられるかということについては、既存のインフラとこれからつくるところ、チャレンジャブルにコストダウンしてつくってしまうところが出てきていることに対しどうするかということも含めた話になるかもしれません。他にご意見等はございますか。平本構成員、お願いします。
○平本構成員　意見というか感想として、14ページの有効な提案がなかったところに対して検討するのはとてもよい取り組みだと思います。今後の結果に非常に期待しています。
　あとはコミュニティに関してですが、コンソーシアムのところにカフェとピッチの話がありますが、僕たちはオープンデータをやっていた時に規制に近いような壁にぶつかることがよくありました。その時に、規制を持っている側と要望している側が集まって議論するラウンドテーブル

をやったりしました。そういうことをすると、規制の背景などについて書面でやるより少し細かい話が議論できてお互いにメリットがあると思います。解決策があるといったことをその場で話せますし、そういう理由があったのかということで納得感もあるので、いろいろなパターンがあると思いますがそういうものもやっていくとよいと思います。どうもありがとうございました。
○江崎座長　ありがとうございます。大変に建設的なご意見ですが、事務局はいかがですか。
○須賀参事官　ぜひやりたいと思っています。仕様書を作っていく段階では規制所管省庁に本当に細かいところまで教えていただいて作っているので、ぜひそれを皆さんにも伝えてほしいという思いが私たちにもあります。権限があるからこそ、おもてに出てきて話していただくことはハードルがなかなか高いのですが、そういう場も実現できたらよいと考えています。
○江崎座長　ぜひ経験者である平本構成員にご協力いただければと思います。
○平本構成員　分かりました。
○江崎座長　他にご意見等はございますか。無いようでしたら、今日は１回目で進捗の報告がメインだったと思いますし、サイバーセキュリティのところは扱いにくいというか非常に難しい問題でありながら、いくつかの解法、新しいご提案を登構成員などからいただけたと思います。クリティカル情報に関する取扱いはすでに信販等で行われているというインプットもいただいたと思います。
　よろしければ、本日の議事は以上とさせていただきたいと思います。最後に事務局より次回の委員会についてご説明をお願いします。
○須賀参事官　本日はどうもありがとうございました。次回の委員会の開催は、事務局より改めてご連絡をさせていただきます。また、本日の議事は、後日、事務局からご出席いただいた皆様に議事録の案のご確認をさせていただいた上で、デジタル庁 HP で公表させていただきます。委員会資料につきましても、特段のご異議がないようでございましたら原則全てデジタル庁 HP に公開させていただきたいと存じます。本日は、ご参加いただきましてどうもありがとうございました。
○江崎座長　ありがとうございます。それでは、以上をもちまして、本日の委員会を閉会したいと思います。ご参加いただきどうもありがとうございました。