

Trusted Web推進協議会（第2回） 議事概要

1. 開催日時：令和2年12月25日（金）12:30～14:30
2. 開催形式：通信システムを用いた遠隔開催
3. 出席者：

内山 幸樹	株式会社ホットリンク 代表取締役グループCEO
浦川 伸一	日本経済団体連合会 デジタルエコノミー推進委員会企画部会長 損害保険ジャパン株式会社 取締役専務執行役員
太田 祐一	株式会社DataSign 代表取締役
黒坂 達也	株式会社 企 代表取締役
崎村 夏彦	東京デジタルアイディアーズ株式会社 主席研究員
白坂 成功	慶應義塾大学 大学院システムデザイン・マネジメント研究科 教授
武田 晴夫	株式会社日立製作所 技師長
津田 宏	株式会社富士通研究所 セキュリティ研究所 所長
富本 祐輔	トヨタファイナンシャルサービス株式会社戦略企画本部 副本部長
橋田 浩一	東京大学大学院情報理工学系研究科 教授
藤田 卓仙	世界経済フォーラム第四次産業革命日本センター ヘルスケア・データ政策プロジェクト長
増島 雅和	森・濱田松本法律事務所 パートナー弁護士
松尾 真一郎	Research Professor, Computer Science Department at Georgetown University / Head of blockchain research, NTT Research Inc.
三島 一祥	合同会社Keychain 共同創設者
村井 純	慶應義塾大学 教授
安田 クリスティーナ	Microsoft Corp. Identity Standards Architect
4. 議事
 - (1) 意見交換
 - ・アーキテクチャ設計に必要な原則、求められる機能について。
 - ・今後の進め方について
5. 配布資料

資料1	Trusted Web推進協議会討議用資料
参考資料1	Trusted Web推進協議会について

○成田審議官

この年末のお忙しい中、皆様お集まりいただきまして、ありがとうございます。

ただいまより、第2回「Trusted Web推進協議会」を開催させていただければと思います。

まず、今回より、本協議会に東京デジタルアイディアーズの崎村様に御参加いただくことになっております。どうぞ、よろしく願いいたします。

○崎村構成員

よろしく願いいたします。

○成田審議官

それから、本日、内山委員は御都合により、御欠席ということでございます。

それでは、これからの議事進行は、村井座長にお願い申し上げます。

村井座長、よろしく願い申し上げます。

○村井座長

皆さん、おはようございます。座長を仰せつかっている村井でございます。

早速、議事に入りたいと思います。大変重要な議題になっておりまして、いろいろ形になっているということで、それだけに議論の内容も増えているかとは思いますが、よろしく願いいたします。

まず、議論の基になる、討議用として、事務局のほうでまとめた資料でございますので、説明をお願いいたします。

○成田審議官

承知しました。事務局の成田でございます。よろしく願いいたします。

まず、資料の前に、協議会の運営について、一言、お伝えいたします。

本日の会議、それから資料とも、公表とさせていただいております。

それから、本日の会議には傍聴されている方もいらっしゃいます。公開での御議論ということでもありますので、御了承ください。

それから、発言者に御確認いただいた後、議事要旨を公表させていただく予定となっておりますので、その点も御了解いただければと思います。

その上で、今日の資料でございますけれども、今、画面上にも出ているかと思いますが、資料1というパワーポイントに沿って、簡潔に御説明を差し上げたいと思います。

ページめくっていただきまして、2ページ目でございます。

10月に協議会の第1回を開催いただきました後、タスクフォースの皆様には計3回、非常に集中、活発な御議論いただいております。

特に、アーキテクチャーの設計するに当たって必要となる原則についての議論などをいただいております。これは、前回の協議会でも、何らかの原則があるだろうという御指摘も踏まえての御検討を進めてきていただいております。

その際に、これも前回の協議会でも何人かの方から御指摘ありましたけれども、少しこのユースケースなども取り扱いながら、全体としてのアーキテクチャー設計についての議

論を進めるのがいいだろうということで、タスクフォースの皆様には、この下のところに書いている、黄色の2つがありますけれども、ヘルスケアに関するユースケース、これは、いわゆる、本人の方が自らの検査結果を管理しながら、必要な情報提示することで、移動をしたりとか、新たなサービスを受けるといったようなケースを想定したことでの御議論。

もう一つは、コンテンツメディアのユースケースということで、フェイクニュースなどが御指摘されている中で、コンテンツについて明確にしながら、コンテンツについての真偽が判断できるような、そういったユースケースについて御議論いただいております。

次のスライドをお願いいたします。

後ほど、この議論の今までのところの御紹介を簡潔に御説明いたしますけれども、本日の協議会での御議論いただきたい事項でございます。上のほうの四角、黄色の枠の○のところに書いてございますように、この後、年明け以降、また、タスクフォースにおきまして、3月ホワイトペーパーに向けて、年明け以降、Trusted Webの基本アーキテクチャー、そのときの機能であったり等々についての整理の議論に入らせていただくことを考えております。

したがって、今日の協議会の場合には、これまで議論していただいていた原則について、それから、それを踏まえて、必要となる機能、それから、今後の議論になりますけれども、実装の方向性といったようなこと、この3点について、本日、前半で御議論をいただければと思っております。

後半で、今後の進め方ということで、年明け以降のタスクフォースで御議論いただきたいこと等について御議論をいただければと思っております。

次のスライドをお願いします。

これは、非常に字が多くて大変恐縮ですが、適宜拡大していただきながら御覧いただければと思いますけれども、これまでのタスクフォースで御議論いただけてきたものを少しずつサマライズしたものでございます。詳細の内容については、追ってのページにございますけれども、ここで全体像を御説明申し上げたいと思っております。

まず、右上の部分でございますけれども、背景のところの説明でありますけれども、フェイクニュース等、膨大な真偽不明のデータが流通しているような状況にあるということ。

それから、データに基づく正しい判断、それから、IoT等も進むということで、Trustというものがより一層不可欠になってきている。

あるいは、メガプラットフォームあるいは監視社会と言われてきているような、そこにおけるTrustというのが、寡占やプライバシーへの懸念を生み、限界が生じてきているのではないかとこの点。

それから、個人、法人が安心してデータを流通させていく、まさにDFFTということで打ち出しているわけですが、流通させていく上でもTrustというのが重要になるのではないかとこの問題意識。

そうした中で、左側でありますけれども、背景として、あらゆるものでデジタル化、DX

が進む中でのTrustという必要性が、今後、ますます高まっていくだろうということ。

それに対して、インターネットの今の構造上、特定のサービスに依存しない形でのTrustを担保する手段というのが十分に用意できていないのではないかとといったような問題意識でございます。

ちょっと字が小さく、その下に少し書いてありますけれども、Trustということで、ここで考えるTrust、Trustは多義的なわけですが、これは、前回の協議会の資料から抜粋しておりますけれども、事実を確認しない状態で、相手先が期待したとおりにふるまう、信じる場合ということで、前回書かせていただいておりますけれども、今日の議論の中でもこのTrustに定義についても、改めての御議論もあろうかと思っておりますけれども、一応、ここでは、こういう置き方をさせていただきます。

そういう背景を踏まえまして、目指すべき方向性のところでございますけれども、大きく3点書いてございます。

黄色の部分で、特定サービスに依存せず、Trustが担保される仕組みとして、1つは、データの出し手の側に立ったときに、個人、法人がデータをコントロールできて、価値をマネージ、変換できるということ。

それから、データの受け手からすると、データの出し手であったりとか、そこに仲介する人を確認し、その出し手であったり、データそのものについての真正性が担保されているという状態。

そのやりとりにおいて、そのやりとりが正しく行われていることが担保されていると、その辺りが必要な要素になるのではないかとということでございます。

ここも後ほどユースケースに簡単に触れるときにあれですが、ステークホルダーも様々でございますので、ステークホルダーの取り上げ方、つかみ方をどうすればいいのかというのが1つの論点かと思っております。

右側に行ってくださいまして、特にこの部分について、原則のところについて、様々活発に御議論をいただいたわけですが、今までの議論の中で、大体大きくサンライズすると、11個挙がっておりますけれども、幾つかのレイヤーごとに分けて書いております。

まず、一番上の3つでございます。こういった仕組みを作るときの支えるガバナンスです。そして、3つほど書いてあります。

1つは、やはり持続可能なものにしていかなければいけない。その際には、ステークホルダーで、どういった責任分担、インセンティブ設計をするのかと。コンテンツであれば、広告モデルというのがありますけれども、それがサステイナブルになかなかないのではないかとという問題意識は、どういったエコシステムを作っていくのか。その際には、強靱性といったようなことも配慮する必要があるだろうということ。

2つ目、マネジメントプロセス、したがって、そういったエコシステムの中で、どんな形でガバナンスのマネジメントをしていくのかということで、分散・分権と書いています

が、中央集権との組み合わせだと思っておりますけれども、そういったところ。

それから、悪意のある方がいるということの前提でのマネジメントプロセスを組み込む必要があるということ。

それから、トラストアンカーの組み込み。

ここには書いてございませんけれども、やはりシステムを動かすときの運用側面も踏まえた全体設計が要るだろうという御意見も出ておりました。

もう一つ、3点目として、やはり透明性、相互検証可能なことということで、アーキテクチャー、コード等の中身、プロセスがオープンであるということ、相互に検証可能であることということが、ガバナンス上、必要ではないかということでした。

次の下に移っていただきまして、機能、システムとして実装する際の原則に当たるものとして、ユーザー目線という観点で3つ、個人、法人によるコントロールができるということで、持ち運び可能、アクセス容易、個人が特定されない、抹消できるような担保があると。

もう一つは、公益目的でのデータ活用とのバランスをどうするかという観点も必要だろうということがございました。

それから、誰も排除しないユニバーサル性ということで、特に誰もがTrustの程度が理解できるようなUI/UXの設計が必要だろうと。

ユーザー視点として、ユーザー側に選択肢があり、ロックインフリーで、分かりやすいといったようなこと、意思決定が支援されるといったようなことが、御指摘がございました。

システム目線で考えたときの原則として4つほど書いてございます。

今あるもの、既存のものをうまく使いながら、新しいものを付加していこうという発想ではないかということで、継続性ということを掲げさせていただいております。

その際には、やはり、Trust、自律分散だけではなくて、中央集権のものとうまく組み合わせながらという御指摘がございました。

2点目、柔軟性のところに書いてあります。

これは、様々Trustは、いろんなケース、ステークホルダーによって、多様性が必要だろうということ、そういう意味で、柔軟性のあるものにする必要があるだろうということ、マスト・ハブになるものと、ベター・トゥ・ハブになるもの、ベター・トゥ・ハブというものが柔軟に組み合わせられるような仕組みでやっていく必要があるのではないかと。

3点目として、相互運用性ということでもありますけれども、社会システム全体との関係あるいはグローバルとの関係、このグローバルでいきますと、運用、要制度も変わる中で、連携可能なものにする必要があるのではないかとという視点。

4点目として、更改容易性、拡張可能にあることである、これは、中長期にサステイナブルにということでございます。時代に応じて、ゴールなども変わっていく中で、機能拡

張が可能になるような、そういったこと、特にIoTが、これからどんどん広がっていく中では、そういったことにも応用可能なような形にする必要がある。

最後に、相対主義と書いてございますけれども、全てをデジタル化で完結させようということでは、なかなかうまくいかないだろうということで、全てのデジタル化を欲張らない、あるいはリスクをある程度許容しながら、そのような対応も考えていくといったような御指摘がございました。

以上が、原則として、いろいろ御議論いただいた内容でございます。

それを踏まえて、左側に移っていただきまして、下半分で、必要となる機能、このところは、少しまだ議論の時間が足りていないので、これからの議論になりますけれども、今まで出てきたところということで、この3点に対応させて考えたときに、個人、法人へのコントロールということで、コントロールに加えて、全てをコントロールすることも、なかなか難しいという中で、委任可能で、その委任先を監査できるような仕組みも要るのではないかという御指摘もございました。

データの受け手からという視点で申し上げますと、出し手あるいはデータの真正性が確認できるということで、それが把握でき、データのやりとりが記録されて検証可能であること、あるいはステークホルダーに依存しない形での識別子があって、公開可能で、その上で、ステークホルダー固有の属性を必要に応じてひもづけるといった仕組み。

それから、データへのアクセス自体が記録されて検証可能であり、必要に応じて、トラストアンカーに付加ができる。

もう一つ、やりとりの正しさということで、2つ、いろいろ意見が出ましたけれども、ステークホルダーが特定され、それぞれの利害が特定されて、その中で、ステークホルダー間で、ウェブで行う事項について、合意されたゴールを基に、ゴールが実現されているかどうかの評価とフィードバックがなされること、ゴールが動的に修正できること、そういったような仕組みがビルトインされるといいのではないかと。

あるいは、必要に応じて、悪意の者に対して、分権的なガバナンスでブラックリストなどで不正を監視、通知できるような仕組みが要るのではないかとといった御指摘もございました。

最後に一番下、この実装は、まだ、これからの議論でありますけれども、今日の時点でも、今後の検討に当たって考えるべきことを御指摘いただければと思っております。

少しページを飛ばさせていただきまして、12ページ目のスライドまで飛んでいただければと思います。

ごくごく簡単にではありますが、先ほど、冒頭に御紹介しました、2つのユースケースで、どんな題材であったかということの御紹介でありますけれども、この場合は、ヘルスケア、左側におります黒い人のマーク、Aさんが、どこかに渡航しようとする場合に、その検査データを、やや右斜め下のCという検査機関からデータをもらって、右側、Bの渡航先なら渡航先の入管であったり、エアラインだったり、ホテルだったり、それ

を示していく。

その間で、これを伝えるスキームとしてのD、これは、今、スマホアプリを使った仕組みというのが検討されているかと思えますけれども、そんなようなケースで、かつ、ステークホルダーとして右下におりますように、そういうAさんがやってきたその先にいる国民、その国の国民から見てどうなのかといった関心もあろうかと、こういったことのケースについて御議論いただいているということでもあります。

次が、15ページ目のスライドでございます。

こちらのほうがコンテンツのユースケースでございます。こちらでもステークホルダーを中心に簡単に御説明いたしますが、左側Aさん、これがコンテンツを作っているオリジネーターがいらして、右側のBさんが、それを見るという設定でございますけれども、その間で、直接見に行く場合もあるわけですがけれども、このDというのが下におりますけれども、例えば、SNSだったりとか、そういったところを通じて、そこでいろいろ拡散されながら、場合によっては改ざんがあるかもしれないということもある中で、Dを介してBさんが見るといったようなケースもあるだろうということで、その全体の中でのTrustがどうなのか、場合によって、右下におりますEさんのように、誹謗中傷されるような被害に遭うというステークホルダーもいるだろうという視点で、ステークホルダーの目線で、Trustとはどうだろうかという御議論をいただいて、それを抽象と各論を議論させながら、先ほどの原則等を取りまとめて、今までのところをまとめていただいているということでございます。

最後に、少しページを戻っていただきまして、10ページ目を御覧いただければと思います。

後半のほうの議論だと思えますけれども、今後の進め方ということで、左上の黄色の箱でございますけれども、本日の協議会で御議論いただいた後、それを踏まえて、この後、タスクフォースにおいて必要となる機能、基本アーキテクチャーのイメージ、その際の技術、それから、海外の標準化団体、今、皆様に御協力をいただいておりますけれども、海外との関係で、どういうアクションを取っていくべきなのかという話をやりながら、基本アーキテクチャーを固めていきつつ、ロードマップ、アクション、プランを整理して、ホワイトペーパーにまとめていくということを考えてございます。

ぜひ、後半のほうでは、今後やっていくに当たっての海外へのリーチであるとか、実装、技術のところ、ロードマップ等々について、踏まえておくべき点等を御議論いただければと思っております。

あと、ユースケースは、少し個人に根差したユースケースが多かったわけですがけれども、もう一つぐらいできればと思っております、産業分野なのか、その辺り、もう一つやるのであれば、どんなユースケースがいいかといったようなことについても、ぜひ御示唆をいただければと思っております。

私からは、以上でございます。

○村井座長

ありがとうございました。

それでは、御意見をいただきます。

今、御説明があったように、ご議論いただきたいのは、資料1のP4から9のところ、原則等に過不足がないか、機能・実装のイメージについて、委員の皆様から御指摘いただければと思います。

そのほか、どのような議論でもいいです。

それでは、黒坂さんからお願いします。

○黒坂構成員

今、御説明いただきました黒坂でございます。

何で私かと申し上げますと、タスクフォースの座長をやらせていただいている関係だと思えます。

○村井座長

確かに。

○黒坂構成員

ですので、逆に申し上げますと、今日は、実は、皆様から御意見を承って、ぼこぼこにたかれる側になっていると思うので、余り発言するつもりはないのですが、今、事務局からも御説明いただきましたとおり、非常に広範な議論、かつ、一つ一つかなり深掘りの議論を、今、していただいている最中でございます。

4ページのところで整理いただいているのが全体の見取り図になるかと思いますが、ここは、今、御説明いただいたとおり、原則を考えながら、機能も考えながら目指すべき方向性を考えながら、ユースケースを少し意識しながらであります、いろいろぐるぐると話を回しながら、例えば、GitHubであるとか、ウェブサービスのツールも使って、当日、タスクフォース以外のところでも、かなり活発に議論を進めています。

その中で、やはり共通して、この後の議論につなげるところで出てきていることは、やはりTrusted Webと言っている以上、Trustの正体をできるだけ明らかに捕まえにしようということが、タスクフォースで、今、共有されている問題意識かなと思っております。

やはり、そのTrustが社会的価値も含めて、何を我々は求めて、どういう形で実装されるとTrustになるのかということが非常に重要な論点であり、だとすると、4ページの中、あるいは後ほど松尾先生からもあるかもしれませんが、Trustというのは、当然、それを構成するステークホルダーが存在して、ステークホルダーによって見え方が違う瞬間のあるものを、どのようにギャップを埋めていくのかというようなことも出てくる、フィットギャップみたいなことも当然出てきますので、そういったことを考えた上で、最後、アーキテクチャーの手がかりになるものを見つけていこうと。

そこまでの議論の経緯も含めて説明すること、海外に向けて説明し、仲間を集っていくということが、今、ゴールとして意識されていることだと思っております。

ですので、例えば、この4ページ目でいうと、一番下のほうに実装におけるイメージ例というところで、どうしても、今、ディセントライズドアイデンティフィケーションの議論が、世界的に活発に行われていますので、それを意識することは、当然やぶさかではないわけですが、それ以外も含めたアイデンティフィケーションの在り方、あるいはTrustの在り方ということ、もう少し積み重ねて、アーキテクチャーに近づけていこうと考えております。

そういった観点も含めて、今日は、ぜひ、皆様からも御指摘をいただければと思っておりますので、よろしくお願いします。

私からは、以上です。

○村井座長

ありがとうございます。

浦川さん、お願いします。

○浦川構成員

損保ジャパン、経団連の浦川です。

まず、原則の今回の立てつけについて、短期間に非常に分かりやすい整理をしていただきましたことを、改めて御礼申し上げたいと思います。黒坂さん以下、本当にありがとうございました。

その中で、大きく2点だけコメントいたします。

まず、1点目は、今回のTrusted Webは、村井座長もおっしゃっていたように、万人が共通の方向感でやっていけるような流れであるということと、今後、グローバルにどんどん落ちていくということを考えますと、極力分かりやすい整理をしたほうがいいだろうなと思っていますので、用語の洗練化であったり、分類の再確認であったり、そういった精緻化を進めればいいのかと思っています。

原則でいうと細かいですが3か所あります。1つ目は、原則の2のマネジメントプロセス、この言葉は、様々な意味を含んでいるので、例えば、マネジメントメカニズムなどのタイトルがいいかなと。2つ目は、原則の6でユーザー視点とありますが、ユーザー視点という体言止めの表現だと若干分かりづらいので、ユーザー視点での便益の尊重など、文言を工夫いただくとよいと思います。3つ目は、原則の11の相対主義とありますが、よくよく読んでみると、段階的なデジタル実装といった意味に読み取れるので、表現を少しづつ精緻化していくといいのかなと思います。

2点目に、各原則の詳細を拝見しますと、設計上の理念、設計上のコード関連の話、また機能面の話が明らかにまだ入り混じっているように見えます。この辺りも少し議論の中で整理していくといいと思います。例えば、デジタル・デバインドを最大限配慮するとありますが、最大限配慮というのをどう捉えるかとか、あと、ポータブルであることみたいな表現もありますが、これは一体何のポータビリティなのか、というところが1つの例でございます。

私からは、以上です。

○村井座長

ありがとうございました。

それでは、太田さん、お願いします。

○太田構成員

DataSignの太田です。よろしくお願いします。

私からは、今回の資料で気になった点のところに対して、コメントをさせていただければと思います。

まず、1つが、4ページ目の不正を監視、通知できることというところに関してなのですけれども、不正を監視、通知できることということと、個人によるコントロールというところのバランスというか、そこは相反するものだと思っております、そこをどういうバランスにもってくるのかということが、結構1つの大きなポイントだと思っております。

1つ、ユースケースというか、例として考えてみたのが、飲食店の予約サイトとかで、無断キャンセルした人の電話番号を共有するみたいなことが、一時期問題になったかと思うのですが、不正を監視するということは、こういう電話番号共有サイトとかが、分散的に運用されていけばいいのかということ、僕はそうではないと思っております、不正を監視するという部分は、個人のコントロールという意味で、余り好ましくないのではないかと考えています。

こういった予約キャンセルの問題にどう対応するかと考えたときに、店舗側で一定の先払いを必須とするとか、そういう仕組み上の対応で足りるのではないかと考えています。ほかのユースケースでは、どうなるか、そこまで考えてはいないのですけれども、例えば、一定の先払いというところを必須としたときに、むしろ店舗側から、支払い情報を使ってトレースができないような仕組みというのを作っておくことが大事なのではないかと思えます。

ですので、不正を監視という部分に関しては、不正は監視するのではなくて、不正ができない仕組みを整えて対応することが望ましいのではないかと考えています。

一方で、公益目的とデータ活用のバランスというのもあったのですけれども、公益性で、こういう監視的なことが必要な部分というのは、今でいうと、信用情報機関のCICさんとかが例なのなかと思っていて、CICというのは、公益上もビジネス上も必要な仕組みだと、僕も思っているのですが、こちらは、法律に基づいて、ちゃんと指定信用情報機関として、しかるべき手順を踏んで行われているものだと思っております。

ですので、不正の監視という意味では、誰でも監視できてしまうという感じでは絶対なくて、ちゃんとしかるべき法に基づいて、手順を踏んで行われている。

ただ、CICという仕組みも、分散的なガバナンスという意味では足りない部分中央集権的にやっているものだと思いますので、分散的なガバナンスという視点では足りない部分もあるかなと思いますので、もう一つ大事な部分としては、Trusted Webで、分散的なガバナ

ンスというのをどう具体的に実装していくかというのを議論していきたいと思います。

前半は、以上になります。

○村井座長

ありがとうございます。どれも大事なところですね。

それでは、崎村さん、お願いします。

○崎村構成員

よろしくお願いします。

雑多になるのですが、まず、原則について、ユーザー目線、システム目線、留意点となっていますが、これらは、ある意味、ステークホルダーの関心事、コンサーンになっていると思うのです。

そのように考えると、実はステークホルダーは、ここに出ているだけでは足りないと思っています。

例えばの話、レギュレーターのコンサーンなどもあってしかるべきだと思うので、ステークホルダーとして何を想定するかで、アーキテクチャーがぶれますから、このリストアップというのはちゃんとやるべきかなと思っています。

原則要素なのですが、分散と中央集権、ディセントライズ、セントライズと、よく出てくるのですが、これは、実は政治的によく使われる話ですし、実態が何を示すかというのは、実は余り明らかではないので、一旦そういうのから離れて、もう少し考えてみてもいいのかなと思っています。

というのは、トポロジーの話と権利義務の話を分離すべきだからです。SSIみたいな話というのは、前者、トポロジーの話で語られることが多いのですが、実際には後者の話、つまり権利義務の話です。

ホルダーがクラウド事業者であってもコントローラーではなく、プロセッサであれば、同じことが実現できるのです。ですので、ガバナンスの問題なのです。

だから、政治的に使われている言葉や、個別技術名にとらわれるのではなくて、もう少し広く抽象化した形で語るべきではないかなと思っています。

それから、この中に、データの出し手という言葉がしばしば出てきます。これは曖昧です。

データの源泉と中継を担うホルダーとに分離して、きちんと考えるべきかと思います。そうすることによって、整理が進むと思います。

あと、メタデータの話がほとんど出てこないのですが、データとメタデータの信頼性をもっと前面に押し出すべきかなと。

あと、信頼性という観点では、時系列的信頼性の観点が、きっと入っているのだと思うのですが、明示的に出てこないなので、明示化するべきかなと。情報のプロヴェナンスと、メタデータとしての引継ぎ。

あとは留意点なのですが、グローバルなデジタルアイデンティティという、実は、

グローバルなアイデンティファイアととられかねず、そうすると炎上ファクターです。組織にキャプチャーされないアイデンティファイア、ポータブルな、ちょっと日本語が苦手なので、日本語にどう表すかというのがありますが、という言い方にしたほうがいいかなと思います。ちゃんと読むとディレクショナルアイデンティファイアだと、よく分かるのですが、それを読まないで、グローバルなアイデンティティと言われてしまうと、どこでも名寄せが簡単なものと取られる可能性があるのですが、若干注意したほうがいいかなと思いました。

以上でございます。

○村井座長

なるほど、ありがとうございます。

白坂さん、お願いします。

○白坂構成員

ありがとうございます。慶應大学の白坂です。

4点、お話をさせていただければと思います。

まず、1点目が、先ほどの崎村さんのコメントにもつながるのですが、今、想定しているTrusted Webの仕組みのアーキテクチャーではなくて、全体像のアーキテクチャーを可視化したほうがいいかなと思います。

例えば、先ほどのステークホルダーとして、今、ユーザー目線といったときに、ユーザーは誰がいるのみたいなことが、書いていないので分からないですし、例えば、データの出し手、受け手スキームだと、出し手と受け手、その間の3つの構造からしかなく、いように見えるのですが、それでいいのかみたいな議論が、多分、その構造を一回書くと、まさにアーキテクチャーですが、仕組みのアーキテクチャーではなくて、全体像のアーキテクチャーを書くと、そこで簡単に議論ができるようになるので、それがいいかなと思います。

今回見させていただいて、最初に言えばよかったのですが、黒坂さんがリードした、このワーキング、すごいここまで膨大な処理をここまでまとめたのは、本当にすごいなと思って見させていただいていました。

○村井座長

皆さん、僕もそう思いますけれども、皆さんが褒めていくと、褒めるだけで時間が経ってしまうため、褒めるのはやめましょう。

○白坂構成員

はい。では、残りの点で、できれば、なぜという言い方を私はよくするのですが、トレースがちょっと取れるといいかなと、要は、Trustはこう担保できると、このために、このトレースでここに原則があって、この原則からこの機能が出ているみたいなものがどこかで取れると、いいかなと思います。それがあれば、どこを気にしなければいけないのかということが分かってくる。

これにつながってくるのは、階層性だと思っているのですが、今、ここまですごい膨大なインプットから、ここまでまとめられてきたのですが、もうワン整理、もう一つ抽象度を上げる形ができないかなと、そうでないと、ちょっとさすがに、ここはまだ少し複雑過ぎて、ぱっと見、全体どういことをやろうとしているのか見えづらいところがあるので、もう一段階抽象度を上げるところにもっていけると、トレースをもっていけるといいかなというのが3点目です。

最後4点目です。

先ほど、太田さんのコメントの不正のところでも出たのですが、アーキテクチャーで、仕組みで対応するのか、ルールで対応するのか、まさにポートアーキテクチャーの議論でさんざんやられているところなのですが、ここをどう考えるかというのは、どこかで明示的に残しておかないと、結果として、こう考えたから、こっちにしましたと、ここは多分、説明責任上、すごく重要になると思うので、そこは決めるときに、意図的に残すというのをやっていただければと思います。

以上になります。ありがとうございます。

○村井座長

ありがとうございます。

それでは、武田さん、お願いします。

○武田構成員

武田でございます。

この11項は、原則そのもののメッセージも、もちろんあるのですけれども、そのためのプロセスとか、そのときのあるべき性質みたいなものが並列になっているようにも見えまして、それは、それで何とか錬磨していったらどうかということでもあります。

ただし、それと併せて、特にグローバルな場面で、こういう原則を訴求していこうとすると、皆さんもおっしゃっていますように、もっと上位概念を併せて作ってっていくことが大事だなということで、私の理解では、それがこの左半分を書いてあって、目指すべき方向性のところが、そういう上位概念を目指す記述なのかなと理解していました。

これを徹底的に錬磨するというのが大事かなと思ひまして、私なりに少し考えたのですが、ここのTrustの定義が、その上に書いてありまして、そこはそのとおりで、全く異論はございません。

そこで、信じる度合いと書いてあると思うのですけれども、書いてあるように、Trustには主語があって、今回、データの出し手とデータの受け手という二者にされたというのが、そのステークホルダーが大事だということで、それも私は、異論はないのですが、今回、これをもう少しデータの権利を持っている人ということだけではなくて、権利者は別に出していくケースというのものもあるし、あるいはIoTなど、機械同士の通信などもあって、大きな原則にするために、データのセNDERとレシーバーみたいなより一般的な表現にしたらどうかというのが1点。

そのセNDERとレシーバーが何を信じるかということなのですが、セNDERにとっては、自分がデータを出した後も、そのデータをコントロールできることというのが、ここに書かれていまして、これが第1。

第2は、セNDERは、データを出したら、それを価値に変換ができるのだということが第2。

第3が、レシーバーはデータの出し手や改変者が受け取ったデータの真正性やらが確認できることと書いてあるように思いますので、これが本質的だと思いますので、誰が何を信じるかという観点で、この3点が大原則みたいな整理をしてはどうかなと感じました。

その上で、いろんな不十分なケースがあった場合、ワーキング・グループなどにフィードバックして、もんでいただくという進め方はどうかと思ひまして、これを併せて提案させていただきたいと思ひます。

以上です。

○村井座長

ありがとうございました。

それでは、津田さん、お願いします。

○津田構成員

富士通研究所の津田でございます。

何点か、まず、アーキテクチャーを考えるに当たって、やはりTrusted Web、ウェブであるというところが、かなり特徴的だと思いますので、ぜひ、その観点、ユニバーサルで分散的な上に、このTrust層を入れると、そういうところをかなり明確にしていくと良いと思ひます。一見キーワードだけ見ると、ヨーロッパ等のTrustサービスであったりとか、そこら辺で議論されているものと似ているようにも思ひてしまいますので、やはりウェブというのをもう少し前面に出してもいいかなと思ひました。

あと、最初のところで、産業データに対するユースケース、これはぜひお願ひしたいと思ひていまして、やはりパーソナルデータと産業データは、相当性質が違ひておひまして、IoTデータというような観点も入ってまいりますし、秘匿、機密性という観点、特に弊社のような企業では、やはり、そこら辺が非常に気になるところですので、そこもちゃんとBtoBの間で包含できるような、そういう仕掛けになっているといいかなと。

あと、抽象度を上げるという議論もいいとは思ひますが、Trustに関しては、逆にもう少し具体化してもいいのかなという気もいたしました。

後半のユースケースの分析の絵は、私はすごくよくできていると思ひます。あの中で、かなりTrustが、人とかデータの真正性だけではなくて、さらにそのデータがどれぐらい信じられるかであったりとか、幾つかの階層で考えられていると思ひます。Trustというのは多義語で、業界の中の話でも、全然違う意味で使っていたりすることも多いですので、そのところは、逆に具体化してもいいのかなと。

あと、開発系からの要望としては、これはアーキテクチャーなのか、ガバナンスなのか

にもよりますが、プライバシーでPIA (Privacy Impact Assessment) というプロセスがございます。あのようなユースケースを設計する時点(バイデザイン)で、これからTrustも、そういうインパクト・アセスメントが必要ではないかと思っておりますので、そういう開発におけるメソッドロジーみたいなものも併せて提案して、それがグローバルにつながっていくと、システムを作る側としては、ある意味、非常にありがたいなと思っております。

以上です。

○村井座長

ありがとうございます。

それでは、富本さん、お願いします。

○富本構成員

トヨタファイナンシャルサービスの富本でございます。

原則1から11のうち5と9を中心にコメントさせていただきます。

5に関して、誰も排除しないという原則については、誰一人取り残さない、持続可能な社会を目指すSDGsの観点においても、1や2の議論にも通じますが、非常に重要だなと思っております。

一部の組織のみがTrustを発行している現状から、あらゆる個人、事業者が、このTrustの仕組みに参加できるということで、人々のアイデンティティの多様性というものが実現可能になるかなとも思います。

誰でも、許可、追加コストなく参加可能という点では、より具体的な実現性の検討も実は必要なのかなと。

それは、データの真正性、第三者が検証できるようにするためということに、トラストアンカーの在り方、そのTrustの法的有効性、ある程度は、中央集権的な権威性のある仕組みも必要なのかもしれないですし、その点では、現在のインターネットでも、DNSの運用が一定の中央集権性をもとに運用されているように、許可、そして追加されるためのコストは一定発生するのではないかと、それは避けられないかなと思っております。

原則9のほうですが、9番目の相互運用性については、我々トヨタのビジネスとしても、グローバルなサプライチェーンやディストリビューションチェーン、販売店網があります。

その際、ビジネスに合わせてデータの流通も国境をまたぐことが想定されていて、相互運用性については、もちろん重要でございますが、その際に、Trustの有効範囲のグローバル性というのを少し入れていただけるとありがたいと、もちろん書いてありますが、例えば、日本のTrustサービスで担保されたTrust、タイムスタンプとか、電子署名とかであっても、例えば、海外のTrustサービスの運用の仕組みと接続性、必要ななど。

そういった意味では、真正性の証明をグローバルにまたがって行うためには、技術標準だけではなくて、法的な枠組みの連携スキームの構築も必要ななど。

この原則に対して、2つ目で機能ということに関するコメントですが、これは、6番目の原則のユーザー視点にも通じますけれども、人間を中心として考えた場合に、プライバ

シーや真正性の確認はもちろんですが、ユーザーにとって、この仕組みがシームレスに、そして、アンビエントに利用できることというのは、ものすごく重要なのかなと思っています。

いつでも、どこでも意識せずに利用するための機能として、秘密鍵などの鍵管理の仕組みも重要な要素になり得るかなと、我々は思いました。

あわせて、具体的にユーザーが利用する際に、インターフェースのあるブラウザやアプリケーションなどのクライアント側の仕組みも大切な機能で、例えば、証明書やカードやパスワード、そんなものは何も提示しないで、可能な限りテクノロジーを意識しないで、何が後ろで待っているか分からずにも利用できるように、そして、損傷、紛失とか盗難、パスワード忘れなどもID喪失が起きたときに対する検討も入れていくのかなと思います。

以上です。

○村井座長

ありがとうございました。

それでは、橋田さん、お願いします。

○橋田構成員

東京大学の橋田です。

先週タスクフォースがあって、たまたま時間があつたので傍聴をさせていただいたときにも発言をしたのですが、何か一般原理のようなものがあって、そこから、いろいろな提言の内容が導かれるようになっているとぶれないのではないかと思います。

そのとき、例えば、今回の4ページでも、誰も排除しないと、ユーザー視点とかというのは、一般常識から、それはそうだと分かりますけれども、例えば、分散管理がいいのだとか何とかということは、一般の人にぱっと分かるかということ、そうでもないと思うので、一般常識からすんなり理解できるようなロジックがあって、こういうふうに導かれますよという構成になっているのが望ましいのではないかと。

一般原理というのは、例えば、パーソナルデータとか企業のデータは、データ主体がフル活用して、自らにとって価値を最大化できることが望ましいと、これは当然ですね。

一方、プライバシーとか企業秘密の問題があるので、他人が不必要に自分のデータにアクセスするというのは、嫌だねと。しかし、例えば課税とか感染症の拡大防止とかという公共の目的のためには、必ずしも各個人のメリットには直接つながらないようなデータの使い方をしないといけないので、ある程度集中管理が必要ですね。そういうことで、何か一般常識からすると素直に導けるようなロジックが入っているといいのではないかと気がします。

そういう意味からすると、ユースケースは、後で2つ出てきていましたけれども、特に感染症に関連するほうは、ある程度集中管理の必要性も分かっていいのではないかと、そういうユースケースの中で、一般原理から説き起こして、こうなるのが最適ですねという説明が素直に伝わるような形になっているといいと思います。

データミニマイゼーションという考え方がありますがけれども、この資料では最小化という言葉は2か所にしか出てこなくて、1か所がデータミニマイゼーションに近いことを言っています。必要十分なデータへのアクセスはできるけれども、それ以上のことはできないというのが、より分かりやすい言い方だと思いますけれども、そういう一般的な常識で分かるような理屈から素直にみんなが理解できるとなるといいなと思います。

以上です。

○村井座長

ありがとうございます。

それでは、藤田さん、お願いします。

○藤田構成員

世界経済フォーラムの藤田です。

橋田先生と、気持ちとしては同じことを言おうとしているけれども、逆のようなことを一部言うので、こういうのを含めて、「黒坂さん、まとめている人は大変だな、偉いなと褒めたくなる」と、言ってしまうのですが。前回、「ユースケースと、原則を行ったり来たりしたらいいのではないか」という話をしまして、最終的な資料としては、今、橋田先生がおっしゃったように、一般的な話から原則ができていって、その原則を具体化していくと、ユースケースではこうですと説明できるというのが一番いいと思うのですが、一方で、作っていくに当たっては、「ユースケースで想定されているようなことは、こういうことなので、この部分を担保するためには、こういう原則が必要だね」みたいなことから考えて、逆向きに考えることも大事なのかなと思っています。

そういった意味で、ヘルスケアのユースケースについては、タスクフォースのほうでいろいろ検討をいただきまして、CommonPassとか、そういったものを想定したユースケースだと思うのですが、そういったものの中で、例えば、医療の場合だと、医師だとか、専門家がある種Trustされる対象関係者、ステークホルダーであると思うのですが、そういった資格を持っていることによってTrustされているだけとか、あるいは過去の経歴からTrustされるとか、そういったことが、トラストアンカーという形で組み込むという想定なのだろうと思うのですがけれども、その辺の位置づけの仕方みたいなものが、もう少しイメージがわくような、そういう意味では、全体の図みみたいなものが見えているといいのかなというのを1つ思いました。

また、これも白坂先生がおっしゃった話と重なると思うのですがけれども、Trusted Webとして実現しようとしているのがアーキテクチャーで実現できるような話も、設計的に、こういうことができないようになっているから大丈夫ということにするのか、それともレギュレーションとかで、例えば、悪意の人は、入っては来られるのだけれども、悪意に伴うような行動をしたら罰せられるのだとか、そういった外側でのコントロールも入れていくという考えなのかということも出てくるといいなと思っています。

また、原則、大きなレベルでの話でいきますと、Trusted WebでTrustを担保していくと

いう話で書いてあるのですけれども、Trustというのは、いろんな解釈はあると思うのですが、各個人のある種心理的な、そういった信頼=Trustというものというよりは、信頼性、トラストワージネスを担保するために、アーキテクチャーでもやれるような部分、やっている部分というのもあると思うので、先ほどの医師であるという資格とかもそうだと思うのですけれども、信頼性を担保する部分として、こういうところがはっきりと組み込まれていますと、そういった信頼性が担保されている構造の中で信頼できると期待されるのではないのでしょうかという話が、もしかしてあるのかなと思っております。

最後に、公益性の例外みたいな話があったのですが、Trustで考えた場合、本人に、こういうふうに使われるだろうと期待していること以外の使われ方が、例えば、公益の例外だから使われるとか、あなたは嫌がっているかもしれないけれども、あなたの健康のためだからいいのではないかと、パターンリスティックに介入するとか、そういった意図が合致しないような場合でも、一定のロジックに基づいて使われ得るのだというところが書かれていることがいいのかなと思っていて、それが広く「公益」だから良いということになるのかどうかというのは、もう少し検討できるといいのかなと思っています。

以上です。

○村井座長

それでは、松尾さん、お願いいたします。

○松尾構成員

松尾です。

私も黒坂さんと一緒にタスクフォースにいた側の人間なので、どちらかという、たたかれる側のような気がするのですけれども、改めて私が強調したい点を、ここで説明したいと思います。

私自身は暗号学者で、ブロックチェーンとかをよくやっている人間なので、どうしても技術的なことを考えがちなので、今回は、逆にそうではなくて、社会からどういう要請をされるのかという話を集中的に議論しているつもりで、結局我々が議論していることは、やはり村井先生がおっしゃるような、置いてけぼりを作らないデジタル社会みたいなところに通じる場所があり、1つ、独占的な人たちがいることで、置いてきぼりができないようにするというので、いわゆる単一障害というのを作らない、Single Point of Failureを作らないみたいな話というのは重要で、そこで分散みたいな話が出てくると思うのですけれども、ちょうど前回、直前のタスクフォースの日に、グーグルが落ちて、みんながスマート家電が使えなくなる日があったのですけれども、やはり、そういうSingle Point of Failureをどうなくすかということと、もう一つは、完全分散アーキテクチャーは、やはり責任が曖昧になることがよくあって、ブロックチェーンビジネスで、よく責任が曖昧になるというところは、そこなのですけれども、Single Point of Failureをなくすのだけれども、責任が曖昧にならないアーキテクチャーを作るところに、やはり、今、我々が議論しているところの核心があると思っていて、そこをどうするかということ

をずっと議論してきました。

先ほど、崎村さんのコメントにもあったのですけれども、やはりの一番重要なのは、特に責任を曖昧にしないで分散アーキテクチャーを作る意味でいうと、ステークホルダーを特定すること、誰がどういう責任を分かち合っているのかということを確認にすること。

あとは、トラストアンカーは誰なのか、あとは、ビジネスなり、コミュニケーションをとっている人たちが、どういうゴールをもってそのビジネスをやっているのか、そこにはセキュリティとかプライバシーのゴールもあると、つい直近もブラウザから、その情報が抜かれているみたいな話もあったのですけれども、誰が、どうやればセキュリティやプライバシー、あるいはビジネスのゴールを設定しているのかということを確認できることが重要で、あとは、責任をみんなで分かち合うときのインセンティブをどう持つのかということちゃんと議論できないと、幾らブロックチェーンを使っても、あるいは幾ら集中型の管理をしても、ウェブがTrustされないので、そういうウェブとTrustのいろんなビルディングブロックを管理するためのステークホルダー間のアグリーメントの取り方であるとか、そういうところの機能も含めて、それが単に口で言っているのではなくて、マシーンリーダブルになって、形式検証できたりとか、あるいは悪意の話も、私が申し上げたのですけれども、我々がセキュリティの形式検証をするときは、悪い人は何をする人なのか、どういう能力を持っているのかということを含めて形式検証するのですけれども、そういう悪意のモデル化を含めて、マシーンリーダブルにできていることというのが、これから考えていかなければいけないことだと思っています。

以上です。

○村井座長

ありがとうございます。

それでは、次に、三島さん、お願いします。

○三島構成員

Keychinの三島でございます。

1点だけなのですけれども、原則のところ、誰も排除しないユニバーサル性というところについては賛成でございます。

細かいところのほう、タスクフォース様のほうで幾つか詳細を記載されていると思うのですが、念のための確認として、今回、このアーキテクチャーをグローバルに議論するときは、ウェブのつながり方が、完全常設で5Gとかを使えるところもあれば、非常にウィークな接続だったり、オフラインのような状況もあると思うのです。

いわゆるユニバーサルとか、デジタル通貨の議論のときもあると思うのですけれども、自然災害になったり、強靭性、インターネットが接続されない状況とか、オフラインのときとか、またはデータが非同期でしか接続できないときとか、弱いネットワーク、東南アジアの一部の国の人たちとか、アフリカとか、そういう人たちのことは、このTrusted Webの話の範疇に入っているのかどうなのかというのが個人的な疑問ではあったのです。

そういうことを考えると、一部、そういうような人からもグローバルに、パブリックにオープンにしたときに、我々関係ないというようなことが起きないように、そういうインターネット弱者というか、そのような方々に対しての原則というところも、若干細かく追加されてもいいのではないかと思います。

以上です。

○村井座長

ありがとうございました。大変重要なポイントだったと思います。

それでは、安田さん、お願いします。

○安田構成員

マイクロソフトの安田です。

まず、分かりやすさについてコメントされている方がいらっしゃったと思うのですが、まず、相互運用性に関してなのですが、何の相互運用性なのか、いろいろあると思うので、ここをもう少しクリアにできればいいなと思っていて、具体的には、恐らく技術的な相互運用性、セマンティック的な、シンタックス的な言葉の定義のようところ、それに加えてもちろん、リーガル、ガバナンス、オーガナイゼーショナルなところ、そして、かつて、もちろんユーザーのエクスペリエンス的なところにも配慮しなければいけないと思うので、そこら辺がもう少しクリアになるといいのかなと思っています。

また、相対主義に関しましても、少し言葉から連想が難しいなというのは同意でして、先ほど、非同期に関してコメントがありましたけれども、ペーパーといいますか、オフラインシステムとのつなぎ込みについてどう考えるか、もう少し明確にしたほうがいいと思っています、高齢者のような方ですとか、お子さんがいる限りは、恐らく全部デジタルというのは、かなり難しいので、個人的には、デファクトオフラインが残り続けると思うので、そこのつなぎ込みについて議論があってもいいかなと思っています。

また、同じくフィジカルセルフとの関連づけとして、生体認証みたいな視点も必要かなと思っています。

それから、上位概念の話に関連づけまして、キーワードとして、ミニマイゼーションとか、不足しているといったコメントもございましたけれども、同じく幾つか、もう少しハイライトされていていいのかなと、サマリーページですね、コメントには散りばめられているのですが、サマリーページにももう少し反映させていただきたいのが、1つは透明性のような観点、もちろん、世界を意識するにおいて、標準ですとか、規格というところはかなり大事になってくるので、コメントのところには、結構出てきているのですが、サマリーのところに余り見られないので、そこがもう少しほしいなというところでは。

また、ユーザー視点とかがあるのですが、同意といった観点があるといいかなと。

また、個人、法人という視点があるのですが、先ほど、個人と結びつかない業界的なデータといったコメントもあったのですが、デバイスという視点がほしいです。

それから、セキュリティに関しましては、先ほどもコメントがございましたけれども、もう少し、すごく大事なウェブのセキュリティ、かなり大事かつ日本では発展途上なところもあると思うので、ぜひウェブのセキュリティについて研究されているところもございまして、ゼロトラストのような考え方が、もう少しあってもいいのかなと思っています。

一旦、以上です。

○村井座長

ありがとうございます。

それでは、第1ラウンドが終了しました。時間的には間に合いましたので、御協力ありがとうございました。

今、おっしゃっていただいたのはそれぞれすばらしい御意見で、反映させるべき部分がたくさんあるのですが、タスクフォースでやはりこれだけまとめていただいたのと、この網羅性が十分になっていて、これに関して、私が最初にまとめて褒めなかったのも、皆さんが褒め始めてしまったということで、大変反省しております。この第1ラウンドの終わりで、私のほうからも褒めておこうかと思っております。タスクフォースの皆さん、ありがとうございます。

幾つか忘れないうちに言っておきますが、崎村さんをはじめ何人かの方からのご指摘にステークホルダーのことが出てきて、作り手、出し手、受け手だけなのかという話があったと思います。私もそのステークホルダーについて、加工とか、オーソリティーとか、オーディットだとか、さっき出てきた監視、監査、さらにもう一つ言えば、悪い人というのがいると思うのです。こういうステークホルダーを抽象化して浮き上がらせて、最初のほうで言ってしまったほうがいいのではないかなと思うのです。ステークホルダーが、かなり具体的になるのは、このドキュメントの最後、ケーススタディのところなのです。

その前のところで、ステークホルダーのある意味の抽象的な取りまとめができていないのです。

したがって、この辺が少し分かりやすさにつながるかなと思えました。

安田さんがデバイスとおっしゃったけれども、デバイスとの関係もIoTが出てきたときにどうするのか、どういうステークホルダーがデバイスと結びつくかというのは、IoTの議論ではかなりあったかと思うので、それがいいと思います。

また、標準化との関係で、透明性とオープン性というのは、オープンプロセスという言葉で出てくるのです。

やはりいろいろな議論をしていくと、オープンソフトウェアとか、オープンアーキテクチャーそのものが、いかに大切かというのが、今後、展開されるデプロイメントとかに関わってくると思うので、これは後半のところ、申し上げたいと思うのですが、そういう意味では、ここの段階では、透明性とオープンなプロセスという部分に、どこまでオープンソフトウェア、オープンアーキテクチャーが大切かということをはっきりしておいたほうが、今後、すごく役に立つのではないかと思います。これも今後の議論です。

それから、分かりやすさという話が幾つか出てきました。言葉とか、原則とか、これは橋田さんや藤田さんからもご指摘がありましたし、用語のことは、いろいろな方から出てきたけれども、確かに相対主義というのは、これはかなり一般的ではないというか、難しい。苦しいからこう書いたのだとは思うのですけれども、いずれにせよ、それに関連して、成田さんのほうから、ユースケースの3番目などを少し調整できるようなことも含めて考えたらどうかというのがあったと思います。

三島さんからのご指摘に関して、やはり切断時や弱い状況は多々起こるわけで、特に、地震等の災害が起こったときに、地上のインフラがやられて、どうするかというときがあるのです。

ですから、インターネットインクルージョンという、例えば、インターネットにつながっていないような人をどうやってつないでいくかというアクションを、災害時などは必ずやっているのだけれども、そういう視点で、回復力があるという意味なのかもしれないし、そういうアーキテクチャー論はとても大事だと思いましたので、それは私からのコメントとさせていただきます上で、次のラウンドに行きたいと思います。次のラウンドは、説明をしていただいて、さきほど申し上げましたように、反対の順番で行きますから、安田さん、準備しておいてくださいね。

それでは、説明をお願いいたします。

○成田審議官

説明のほうは、先ほども触れましたけれども、改めて確認のためにあれですけれども、10ページ目を御覧いただいて、先ほど少し触れましたけれども、今日いただいたところで、原則とか、4ページ目のところで、もう少しさらに見直していく必要があるかと思えますけれども、今後の展開として、実際の機能のところ、それから基本アーキテクチャーにしていくところの議論が1つの塊としてあろうかと思えます。

それから、先ほど来、お話に出ていましたように、やはり海外に展開していく上で、様々な標準化団体とありますので、今の動向整理をしながら、ここにどう打ち込んでいくかというアクションのところも含めての議論も必要かと思っております。

それと、それを含めたロードマップ、ホワイトペーパーの中の要素として考えたいと思っておりますので、下のほうに、前回の協議会でお示ししましたホワイトペーパーの考えられる検討項目例、記載は項目例と書いていますけれども、そういう意味では、赤線で囲っております、アーキテクチャーの基本ということだと思えますけれども、この具現化をさらに進めるということと、ロードマップ的に技術面、実装面での道筋というのをどう提示できるかということ、それから、必要なアクション、この辺りが、これから年明け以降、皆様に御議論をいただきたいこととございますので、この辺りについて、今後、先ほどのユースケースの追加も含めて、こういうところについて留意したらいいとか、あるいは具体的に実装のときに、こういうことをちゃんと踏まえるべきだとか、海外との関係も含めて、ちょっと幅広なテーマになりますけれども、皆様からの御指摘をいただければと思

ておりますので、ぜひ、よろしくお願い申し上げます。

私からは、以上です。よろしくお願い致します。

○村井座長

ありがとうございます。

それでは、安田さん、お願いいたします。

○安田構成員

はい、覚悟していました、安田です。

まず、アーキテクチャーの具体化においては、ステークホルダー特定といった話があったと思うのですが、コンポーネンツの特定といいますか、明確化も必要な気がしています、何を申し上げているかといいますと、何の話をしているのか、データなのか、アイデンティティーなのか、それこそデバイスなのか、アプリケーションなのか、ネットワークなのか、そこがもう少し、どこでどの話をしているのかというのがクリアになると、アーキテクチャーに移行しやすくなるのかなと思っています。

また、単位といいますか、スケール、どのスケールで考えていくのか、もちろん、最大のSingle Point of Failureがないスケールで考えるのでしょうかけれども、いろんなスケールのアーキテクチャーがあると思うので、そこが1つ重要になってくるかなと。

また、Trustに関しましても、Trustレベルという考え方をここに入れるのか、入れないのか、恐らくTrustレベルにできること、できないことは変わってくると思うので、その視点が少しあると、先ほどオフライン、オンラインみたいな話にもつながってくるのかなと思っています。

また、先ほど、村井先生のほうからオーディットといったお話があったと思うのですが、まさに、この原則どおり運用されているのか、恐らくTrustの源泉が、ベリファイアビリティといいますか、検証可能性なのであれば、その視点があれば、さらに一般的に分かりやすい、かつ、効果のあるところになるのかなと思っています。

また、世界の標準化団体へのアプローチといったコメントがあったと思うのですが、実際、私も幾つか関わらせていただいているのですが、打ち込みに行くといえますか、既にある規格、現在動いている標準で使えるものはどんどん取り入れるのが最初なのかなと。

その上で、現在、ここで日本としてやりたいことと、既にある規格の間にギャップがあれば、どんどんアプローチしていくという、最初からアプローチするというよりかは、そういう3ステップがあったほうがいいのかと思います。

あと、ステークホルダーについて、何かメモを取っていたのですが、覚えていないので、一旦、こんな感じでお願いします。

○村井座長

ありがとうございます。

三島さん、お願いします。

○三島構成員

村井先生がおっしゃったように、ステークホルダーのところと、あと、今後の実装のところの点にも関わってくるのですけれども、さっきおっしゃったデバイスというか、端末というステークホルダーも、どこかで議論に少しずつ入れていってもいいのかなと思ったというところですよ。

例えば、資料の15ページのヘルスケアの図であったとしても、多分、ヘルスのデータを取っているのは、何か、医療機のバイタルデータの端末があって、それを実際に本人のものかと、4ビットのものとかを受けて発信しているところには、多分、スマートフォンなのかタブレットなのか、何らかデバイスが介在しているはずですよ。

今後の議論、データのTrustというか、真正性というのを議論する上では、コンテンツの認知時内容著作権とか、ユーザーのフィンガープリントとかもあると思うのですけれども、一体どのデバイス上で作成されたかというのが分かれば、ある程度、このコンテンツが一時情報であるとか、オラクルであるというのが分かりやすくはなると思うので、そういう視点というの、今後、御議論の中のどこかで追加をいただくと面白いのかなと。

それに加えて、そういうデバイス、例えば、一人が持っているデバイス、私に属しているデバイスは何台あるのかということも管理しようと思えば、今後、議論にできると思うので、そういうユースケースとかも検討の俎上に入っても面白いのかなと思った次第ですよ。

以上です。

○村井座長

ありがとうございます。

全く別のプロジェクトで、総務省と警察が取り組んでいる信号機に5Gの基地局をつけるというものがあるのですけれども、道路は公共空間なのです。もし、そこに何かほかのデバイス、センサーをつけられるとしたら、信号機の制御だけではなくて、例えば、交通量の測定とか、歩いている人が転んでしまったときにどうなるかとか、あらゆることが分かるということ。

実は道路というのは、オーナーのレベルが複雑で、地方自治体のレベルなども違う。そういう縦の多様性を、データアーキテクチャーの中で、何のために使うのか、誰が責任を持って、そのアップデートは誰がするかなどの視点で考えると、非常に複雑になるのです。

今、公共空間の新しいセンサーデバイスが出てくるということを、うまく考えるということとはとても大事だなと、でも難しいけれども。ちょっと余計なことでしたけれども、では、松尾さん、お願いします。

○松尾構成員

私からは、標準化、グローバルアウトリーチの件でコメントさせていただきます。

私も標準化は長いので、ISOもそうですし、BGINみたいなものも始めているので、標準化との関わりは長いのですけれども、まず、ポイントとして、標準化活動をすれば、標準になれば、その技術が使われるというわけでは一切なくて、何かのべき論を押しつけて技術

が使われることは大抵ないのです。

これは、多分、最初はワールドエコノミックフォーラムのイベントに持って行って、その後、いろんな人に使ってもらうための、あるいはグローバルと一緒に協力しながら作り上げていく第一歩だと思うのですけれども、標準化組織というものは、さっき安田さんがおっしゃったとおり、既に確立したものがあって、彼らのやることは決まっています、既存の標準もあるので、正面からとんとんとドアをたたいていったとしても、彼らのスコープに入っていないと、うまくいかないわけです。

多分、重要なのは、組織と同時に、キーマンは誰なのか、それも自分で、一人称でやるのだというインセンティブを持つグローバルなキーマンは誰なのかという特定をして、彼らが、我々が、例えば、ワールドエコノミックフォーラムであるとか、将来いろんなところに提案してくるドキュメントのエディター、著者に日本人だけではなくて、いろんな国の人とか、いろんな異なるバックグラウンドの人たちを入れて、グローバルな共同提案なのだという形にしていかないと、実際に使われるものにならないという意味で、組織と同時に人を特定していくということをしていくことが重要。

ここでは、先ほど来議論になっている、このTrusted Webに関わるステークホルダーは誰なのか、全世界の人なのですからけれども、例えば、うちの年老いた母親が、これを使うのかという観点でいうと、そういう人たちを代表するとか、例えば、シビルソサエティーとか、そういう人たちも巻き込んで、組織と同時に、人をアイデンティファイして、キーマンを探して、この議論に途中からでも入ってもらって、ワールドエコノミックフォーラムであったり、将来いろんなところに出すときに、彼らに著者に入ってもらう、そういうアプローチでやっていくべきなのではないかと思っています。

以上です。

○村井座長

ありがとうございます。

それでは、増島さん、お願いいたします。

○増島構成員

増島でございます。

今、このペーパーに関連してでありますけれども、目的に照らして、この段階で何を書くべきかという発想は、非常に大事だと思います。

あれもこれもとって、いろんなものが出てくるのですけれども、このペーパーで全てが完結することはありませんし、さっき村井先生もおっしゃっていただいたとおり、国の中ですら、いろんなプロジェクトが並行して走っていて、それぞれが、ある意味、関連しているし、ほかの論点、ほかの角度から取り上げているということだと思っています。

我々が今やっているのは、結構長期に見ながらウェブの形を再構築と、こういう中の、まず、日本としての第一弾を整理して、このペーパーを道具にして、いろんな人を巻き込んでいくと、こういう作戦のうちの一部なので、この作戦が成功するような内容は何なの

かという発想がすごく重要で、それは、全てが書き込まれていて、これが正解だと書いてあればいいというものではない、むしろいろんなものが、もう少し余裕、遊びがあって、そこにほかの人たちが、うちのアイデアも、ここにうまくはまるのではないかとか、一緒にできるのではないかとか、思わせるぐらいの粒度のものの方が、目的を達成するという意味では、ペーパーとしてはいいのかなと思います。

ということで、今、イメージとして挙げていただいている項目は、そういう意味では、とてもいいと思いますけれども、書く内容が、余りディテールに入り込まないほうがよいという部分があるかもしれないですし、あれもこれもとつけ加えるという発想ではないほうがいいかなと思いました。

以上です。

○村井座長

ありがとうございました。

それでは、藤田さん、お願いします。

○藤田構成員

何を言おうかなと迷っていたのですけれども、先ほど話したことと、ある種、今度は逆向きみたいな感じになってしまうのですけれども、ユースケースと原則を行ったり来たりということができるといいのかなと思っているところがございまして、ユースケースをベースに原則も考えましょうという話をさっきしましたけれども、今度は、原則からユースケースに、こういったところの肉づけも入れていくといいということも見ていくといいのかなと思っています。

ヘルスケアのユースケースは、CommonPassに関して、特に中心に検討をいただいて、実際に、今、動いているものなので、そこがどういうふうに進んでいるか、タイミングを合わせながらやれるとより効果が大きいいということで、取り上げていただいていると思うのですけれども、一方で、例えば、CommonPassの中でも、デジタルアイデンティティーの部分は、構想としてはあるけれども、なかなか進んでいないみたいな話もあったり、いろいろペーパーレスでどういうふうに対応できるかみたいな話は、まだ、十分な検討ができていないとか、いろんなことがあるので、このTrusted Webのほうから、具体的なユースケースに対して、いろんな角度から、いろんなレベル感で貢献し得るだろうと思っていますので、必ずしも現状のCommonPassに限らず、広く一般的なユースケースの絵になるようにしつつ、いろんなパーツをより膨らませていけるといい部分もあるのかなと思っています。

この標準化とか、今後のステップというのを考えたときに、全体としてのTrusted Webをまるっと何らかの標準に持っていくみたいな、大技みたいなものもあるかもしれないのですけれども、恐らく、パーツ、パーツでの標準化で、現在進んでいるものと、うまく照らし合わせてやっていくということも重要になると思いますし、また、ユースケースを念頭に置いた標準化という話も当然あるかなと思っています。

CommonPassに関しても、ITU等で一部データの出し方のところをしようという話もあっ

たりしますので、どのように国際的なところと協調していくか、連携していくかというところは、いろんな可能性があるのですが、そこら辺をうまく、先ほど増島先生からあったように、時間的に、どのタイミングで、どこまでできるかというのを見ながらやるといいのかなと思っています。

その上で、出口の1つとして効果が出ている世界経済フォーラムとの連携ということでは、4月にGTGSという大きなイベントがあると。そこで、このホワイトペーパーの原案を出して、いろいろ議論をするというのも、すごくいいことだと思いますし、グローバルないろんなステークホルダーを特定できているのであれば、そういったグローバルなステークホルダーがホワイトペーパーとか、ペーパーレベルですぐに関わるというわけではなくても、4月に関わってもらいたいステークホルダーを呼んできて、ぜひ、これから一緒に書きましようという流れを作っていくというのもいいのかなと思っています。

以上です。

○村井座長

ありがとうございます。

橋田さん、お願いします。

○橋田構成員

何人かの方がステークホルダーの話がされていて、デバイスもステークホルダーとして考えてはどうかみたいな話もあったと思うのですが、国際的な場に出て行ったときに、我々としては、こういうステークホルダーが、こういう役割を果たすという枠組みで考えていますというような議論の整理は非常に重要だと思います。

ステークホルダーというのは、名前よりも、むしろどういう役割、例えば、どういうサービスを提供するとか、ここでこうやってもうけるとか、そういう役割によって定義されるわけですが、様々なステークホルダーの役割として、実は、こういうものもあるみたいなことも整理したほうがいいのかと。

例えば、パーソナルデータ等のデータコントローラーは、大抵サービス事業者だったりするわけですが、サービスを個人に提供する、商品を個人に売るという以外に、データポータビリティに対応して、保管しているパーソナルデータを本人に提供する役割も期待されるわけですが、それによって結構もうかったりするような事業モデルの議論もできるといいのではないかと。

GDPRはデータポータビリティ権を明文化していますけれども、データポータビリティが産業創造につながったみたいな話は聞かないですね。それは、本人にデータを渡してももうからないから、みんな真面目にやらないということだと思いますけれども、実はデータコントローラーには、本人にデータを提供してもうけるという道もあるみたいなことが言えるといいのではないかと。

それに関連して、もう一つは、ステークホルダーとしてデバイスがあるならAIもあるのではないかと思います。

この資料にもパーソナルAIエージェントというのが書いてありますがけれども、パーソナルAI以外にも事業者側のAIがいて、それらのAIが不正の検知みたいなことをやるのだけれども、それができるのはAIだけで、人間は生データを閲覧しないというようなことが可能かもしれないと。

また、パーソナルAIエージェントは、本人のデータをフル活用して、かつ、そのデータを他者に開示せずに、本人をアシストする。例えば、購買を支援するとか、本人に働きかけて介入して行動変容させるみたいなサービスを考えると、その価値は結構大きくて、GDPの2、3割いくかもしれないと思うのですが、そこで生み出される価値と言うか収益の一部を、本人にデータを提供したデータコントローラーにも分配するとデータコントローラーは結構儲かるはずですね。

ということで、様々なステークホルダーの様々な役割ということと、ステークホルダーとしてのAIというのはあるのではないかと思います。

以上です。

○村井座長

ありがとうございます。確かにそうですね。

それでは、富本さん、お願いします。

○富本構成員

よろしくお願いします。

それでは、私のほうからは、ユースケースの話と、今後の進め方に対するコメントを申し上げます。

このTrustの仕組みが事業者や個人データの流通を加速して、連携を促すという時点では、SDGsの取組の下支えになる可能性があるようなイメージを持ちました。

そういうユースケースは何かないかなと。例えばですけれども、環境を守るという観点で、サプライチェーンにもつながるかもしれないのですが、複数の事業者間をまたいだCO2排出、環境負荷物質情報の測定ということをしていく、サプライチェーン横断で、ライフサイクル横断でのCO2の排出というようなこともできるのかなと思ったりもします。

また、個人間のほうでも、購買、移動、電力を使ったというような、複数を組み合わせたような形で、CO2排出量の測定とか、それに対するインセンティブみたいなもののユースケースもあるのかもしれないと思いました。

最後になりますが、今後へのコメントとして、今度の春のグローバルテクノロジーガバナンスサミットの発表後は、このTrusted Webの概念を広く認知されることと思います。

その際に、社会実装に向けて実際の事業や利用指針における具体的な実装方法とかも、ぜひその流れの中で、みんながうまく拾ってくれるような仕組みづくりになってくれるといいなと思います。

我々のほうも、ブロックチェーンラボのほうで実証実験をたくさんやっているのですが、その辺で得た知見とかもタスクフォースのメンバーとかに共有させていただいたりしながら、

微力ながら、今後の議論に貢献できたらなと思っています。

以上です。

○村井座長

ありがとうございます。

それでは、津田さん、お願いします。

○津田構成員

津田です。

それでは、ユースケースと進め方、それぞれコメントさせていただきます。

ユースケースに関しましては、案外BtoBの中でも、意外に困った問題があります。例えば、BEC(ビジネスメール詐欺)であったりとか、皆さん何でもメールでやりとりしていますがそのプロトコルにはTrustがないため、それで数兆円の被害になっているみたいなケースもございます。

これなどは、日本だけでやってもしょうがないところもありますので、例えば、そういう分かりやすいケースから、このTrusted Webの効果を示していくというのも、1つの手としてあるのではないかと思います。

進め方ですが、Trusted Webについて、日本としては、DFFTの1つブレークダウンしたとか、一歩先に進めた具体例というのを見せるということが大きいと思います。恐らくTrust系だと欧州の標準化が進んでいると思いますので、ぜひホワイトペーパーで、やはりTrustをバイデフォルトで考えなければいけないというような基本的な考え方を伝えて、このステークホルダーの整理を含めて、まず、議論できるようなことをやるのが、第一歩。その上で、このユースケースを一緒に考えていくというやり方で、DFFTを進めていくというのがよいのではないかと考えました。

以上です。

○村井座長

ありがとうございます。

それでは、武田さん、お願いします。

○武田構成員

武田でございます。

前半の議論は、行為の大原則のようなコンセプトのところ、ルールメイキングの世界でリードすることを目指した議論だったと思うのですが、これとともに、そういう原則の世界になったときに、技術の世界で、実は勝っていたのだという活動が、両輪として走っているということが大事ではないかと思ひまして、今回のラウンドは、そのような議論の場なのではないかと、まさに、前半と後半で、そのように分けられたというのは、非常に分かりやすいかなと思っています。

特に、先ほど来出ているGTGSは、テクノロジーのガバナンスのサミットということで、ダボスと少し違う意味合いを持っていますので、そこで関係のテクノロジーのパネルみた

いなものが作れて、それを日本がリードできるというのが理想的な目標ではないかと思ひまして、これを1つのミッションとして大目標に加えてやっていったらどうかと思ひます。

そのためには、日本のオリジナルで、かつ、できる限りシンプルなテクノロジーのモデルの提案が必要ではないかと思ひまして、そういうことを言うだけではなくて、技術開発の枠組みの1つの案として、私も作って、その中で議論していますので、ごく簡単にお話しさせていただきますと、4つあるのですけれども、第1は、多様なTrustレベルを表せる新しいデータ表現というのがないのかということ。

第2は、そのようなデータ表現にアクセスするための汎用的なインターフェースとは何なのかということ。

第3は、異なるTrustレベルの間で、データの変換をしていくためのロジックというのは、どういうことなのかということ。

第4は、フラットなデータフローからTrustのレベルの構造化された、さっきのデータ表現みたいなものを計算する知識システムの大規模なものになるのではないかとっているのですけれども、そういうものは何なのか。

この4つぐらいを技術の大きな枠組みとして捉えて、少しテクノロジーをガバンしていくという枠組みにしていったらどうかということを考えております。

御紹介まで、以上です。

○村井座長

ありがとうございます。

それでは、白坂さん、お願いします。

○白坂構成員

ありがとうございます。

今後の進め方、特にアーキテクチャーを決めていくところでコメントをさせていただければと思ひます。

今、ユースケースがあって、このユースケースを見ながらと、あと、原則と、この上と下からを両行ったり来たりしながらつないでいくという作業になると思ひますが、具体的な分析作業でやると、基本的には、今、既に考えているものとか、あるものをベースにアーキテクチャーを起こしていくという形に近くなってくるわけですが、あとは、具体的な想定の中で考えていくということになるのですが、これをやっていくときに注意しなければいけないのは、上とつなげるのだという意識だと思ひています。

つまり、原則のなぜこの設計にするのか、このアーキテクチャーになっているかというところをつなげていく、ここの縦の関係性をつないでいこうというのをやっていこうと。

そうすると、基本的にやらなければいけないことが、機能と物理の分離と、我々は言ったりしますが、役割と手段の分離でもいいのですが、こういう役割、つまり、こういう機能が、こう組み合わせるから、ここが目指せるのだと、これが、このユースケースでは、

こういう主体によって行われているみたいな感じの、ここの関係性をちょっと意識しなければいけない。

そのときに、ちょっと気になっていたのは、このホワイトペーパーにどこまで書くかということは、ちょっと個人的には気になりました。

というのは、それは考える過程においてはすごく重要で、多分、説明したりするときにも、最終的には、この原則を実現する、この目的のために、こう考えたから、こういうアーキテクチャーにしたのだというアーキテクチャーデザインのディスクリプションが、多分、必要になってくるわけですがけれども、これを全部書こうとすると、すごく膨大になってしまって、このホワイトペーパーとしては、多分余り意味がない。

でも、一方で、広めていく過程においては、多分、専門家にとっては、ここはすごい重要で、すごい知見になってくると思うので、これを分ける形でいいので、ホワイトペーパーとして出すところと、アーキテクチャーの設計として考えたところというのが、きちんと残されていくと、この活動がすばらしく説得力を持ちながら、いろんなところに広めていけるのではないかと感じております。

以上です。

○村井座長

なるほど、ありがとうございます。

それでは、崎村さん、お願いします。

○崎村構成員

③と④を一緒に話したいと思います。方向性と進め方です。

そこに入る前に、1つ、原則に一瞬戻ってしまうのですがけれども、実は、先だって行われた、12月頭ですけれども、マイデータグローバルカンファレンスで、私、デジタルビーイングの7原則というのをキーノートで発表していて、そこで言ったことは、現在の原則に入っていないものもあるような気がするので、参考にしていただければと思いますので、事務局さんとシェアします。

それで、③と④ですけれども、まず、実装の方向性です。これは、TrustフレームワークとかTrustスキームと僕らの言葉で、ずっと15年とか言ってきたものと近いと思っていて、それは、ツール (Tool) とルール (Rule) のバランス取って~どっちかだけでやるというのは、非常にバランスが悪いので~やると、それぞれ得意なところでやるということなので、実装においても、その辺をちゃんと考えていくとよいと思います。

では、どこから手をつけたらいいかなと思うと、やはりデータがどのように生成されたかです。誰が何の権限を持って、どの基準に従って、どの法律の下でといったようなメタデータをデータと一緒にどうやって送るか、この辺に、まず、着目すると、割とタンジブル (手触り感がでるの) でいいのではないかと思います。

実は、自然人と法人に関してはOpenID Foundationと、IIFですねInstitute of International Financeと、あと、最近はGLEIFですね、Global Legal Entity Identifier

Foundationで進めていて、こういう動きは見ていく必要があるかなと思っています。

これは、松尾先生のキーマンの話と接続していくのですけれども、規格を実装して広く使っていく人を巻き込んでいくというのは重要で、実は、今言った動きには、ドイツの実装者が入っていて、実際に、もう1,000社、銀行、FinTech、トラストサービスプロバイダー(QTSP)などは、それを使って動き始めていて、今、eIDASと接続した形で、Qualified Certificate (適格証明書)だとか、Qualified Signature (適格署名)を発行するのに、もう既に使っていると。

これは、何でこんなに動きが早かったかということ、やはり、ド新規ではなくて、現在使われているものとの接続性を非常に重視しながら進めていったからなのです。ですので、そういった観点は重要かなと。

2分超えてしまいましたけれども、動脈と静脈の話があると思っています、今、私たちは情報流の話ばかりしていますけれども、これは動脈ですね。静脈に当たる金流の話というのは、必ずしなければいけないと思っているので、その辺は考慮に値すると思います。

あと、最後、相互運用性です。相互運用性とふわっと話してしまうのですけれども、特に技術的な点では、実装テストが非常に有用です。実装テストをきちんとやらないと、結局、規格だけあってもつながらなくて、これは1,000社同士でやるといったら、永遠につながらないということになりますから、こういったものは、非常に重要だと思うので、これもホワイトペーパーなどに入るといいなと思っています。

以上です。

○村井座長

ありがとうございます。

今の動脈と静脈の、崎村さんの定義は何でしたか。

○崎村構成員

動脈が、今、私たちがここで話をしている情報の流れです。情報流。

それに対して、静脈の側が、情報が流れると、恐らく何らかの形でお金か、それに類するものが流れると思うのです。これは金流。これは、多分セットになっているので、金流の側を考えないというのは、多分、片手落ちではないかなと思います。

○村井座長

なるほど、分かりました。ありがとうございます。

それでは、黒坂さん、お願いします。

○黒坂構成員

黒坂です。

まず、皆様、タスクフォースの活動に様々な御意見をいただきまして、本当にありがとうございます。

大変過分なお言葉と、私が言うのも変でして、実際に、私は、にこにこしていただけで、多くのタスクフォースメンバーが、非常に活発な議論をしていただいたおかげで、成果が

大量に出てきた状況だと思います。

今日、事務局にも、もちろん多くまとめていただいたので、また、事務局の皆様とも相談しながら、タスクフォースメンバーにできるだけ皆様からいただいたことを、全面的にフィードバックして、さらにブラッシュアップをしていきたいと思っています。

その上で、私が決めるというわけでは、もちろんないのですが、今日いただいた中で、2点だけコメントをさせていただければと思います。

1つは、今後の検討についてなのですが、とりわけ、今、冒頭にも申し上げたTrustの正体を明らかにしていこうというようなことが、それをちゃんと定めた上で、アーキテクチャーを考えていこうというプロセスに、次、入っていくと思っています。

そのときに、やはりTrustを考え上で重要な考え方として、多くの方からステークホルダーをちゃんと明らかにしようという御意見を、今日、いただいたかと思っています。

ステークホルダーを整理する目的を、やはり意識しておいたほうがいだろうなと思っていて、それが、皆様からの御意見にも対応できることになるかなと思っていますが、考えただけでも、例えば、コンポーネントの特定であるとか、それぞれの機能を明確にするであるとか、あるいはコンポーネント間の連携を考える。なおかつ、システム全体への影響、貢献する部分とボトルネックになる部分とあるわけですが、それとか、あるいは連携して作り上げていくがゆえの責任分解、こういったものを考えていくということが基礎になる。

これを明らかにするというのが、ステークホルダーを明らかにすることの、多分、目的になっていると、こういうことを少し留意していきたいと思っています。

あと、標準化、これは検討というよりも、この後のアクションの話になってくると思うのですが、標準化と、どう向かい合うのかというような御意見がたくさんあったかと思っています。

これは、完全に私の私見なので、ほかの御異論もたくさんあるかと思いますが、標準化の目的を、やはりここも考えるべきだろうと思っていて、恐らく市場競争力、すなわちシェアを取っていくというような話だけではなくて、それも最終的に達成できればいいのかもしれませんが、市場に対する影響力であるとか、アクセシビリティ、すなわちリファレンスを示していった、理論の方向づけをしたり、こいつの話は聞いておこうと思ってもらうというところが、まず、出発点ではないかと。

それは、恐らく価値を表現したり、価値観を共有していったりということが非常に重要なアイテムになっていくと思います。

そうすると、誤解を恐れずに言うと、初期の段階では、組織対組織で動くというよりも、個人対個人、つまり、Trusted Webの皆様も含めた検討される方々が、この世界の、この人たちと話すことによって、仲間になってくれるかな、自分の価値観であるとか、分かってくれるかなということを決めていくということが重要ではないかなと思っています。

その営みを、恐らく4月からスタート、4月で決着をつけるのではなくて、4月から連

続的に進めていくというようなことを意識する必要があるかと思っておりますので、ぜひ、そういった観点も含めて、ここがいいよということはもちろんなのですが、この人と絶対に話しておくべきとか、この人が、今、やっていることとジョインしておくべきというようなことも、ぜひ皆様から御指導いただけるとありがたいなと思っております。

長くなりましたが、私からは、以上です。

○村井座長

ありがとうございます。

それでは、太田さん、お願いします。

○太田構成員

太田です。

先ほど、崎村さんの動脈、静脈という話があったと思うのですが、そこに関連して、ユースケースとして、やはり広告というのは必要なのではないかと、ちょっと思いました。

なぜかという、今のウェブのエコシステムというか、お金の流れというのは、広告というところがすごく大きい部分ですので、そのユースケースを考えたいなと思いました。

今、広告の世界では、クッキーは使えないとか、いろいろ規制が厳しくなっている中で、では、IDとして何をしようかという中で、メールアドレスをしようというような方向性になってきています。

それは、今、僕らが考えているTrusted Webとは、ちょっと逆行しているようなものなのではないかというところの懸念がありまして、では、それをこのTrusted Webの考え方で、IDをどうするのか、どういうふうな広告のユースケースで、どう使っていくのかというところを示すというところは、1つ重要な意義があるのではないかと思います。

その上で、IDをどうするか、今後の議論というところにグローバルなデジタルアイデンティティーというのを書いてありますけれども、今のところ、DIDというところをベースに進めていくのかなというイメージではおりますが、ぜひ、その議論として入れていただきたいところに、今、DIDの仕様だったり、W3Cだったり、DIFだったり、やっていると思うのですが、秘密鍵をどうするか問題というところが、いつも僕はつまづいてしまうというか、どうすればいいのだろうかとなってしまっていて、我々も今、DIDをベースとした情報銀行というのを作っているのですが、秘密鍵、実際どうすればいいのかというところで、その秘密鍵を管理するのに、本人に管理してもらうのは、なかなか難しいし、ビットコインのウォレットとかだとキーフレーズとかをメモってもらうみたいなのがあるけれども、それは、ちょっと忘れてしまうし、では、公的個人認証だというと、そこまではないみたいな、そういった部分の議論というのを、今後、広告というところをベースにしつつも、DIDとなったときに、そのDIDは公開が前提というところもあるので、それに全部ひもづいてしまうと、広告事業者は大喜びで、公開されている、このIDで、あれを使って、全部分かるようになるというのでは駄目だと思うのです。そういったユースケースもしつ

かりと議論していきたいと思いました。

以上です。

○村井座長

ありがとうございます。

さっきTrustのレベルという話がありましたけれども、それとも関係するかとおもいました。

浦川さん、お願いします。

○浦川構成員

これまでの議論、非常に有意義だと思います。やはり、インターネット規約と言っても標準化されているのはTCP/IPといったようなプロトコルレベルで、それ以上の部分がほとんど野放しというのが、今回の発端の1つだと思っています。

やはり、レイヤーやカテゴリーを定め、世界の標準を推進したいという思いは同じです。何人かの方もおっしゃっていたとおり、複数の企業がオープンソース化して、どんどん機能追加を誘導し、デファクトスタンダードが取れたら、その分野の業界標準になるという、いわゆる弱肉強食、競争社会でこの20年間のインターネット技術が発展してきたとも言えます。様々な技術要素を一度アラインして、こういうレイヤーで、こういう範囲を規約化したらいいのではないかというようなことを、国際的な場に出すというのは、やはり日本人は得意だと思うし、AIの社会原則についても、そういった動きが今出来つつありますし、グローバルにも結構響くと思うのです。

そのときに、既存の技術と今回出してくる規約は、一体どういうふうにマッピングできるのだろうかということを、国際的な場に持っていけば、いろいろ問われるかと思います。

例えば、APIで企業間の連携をしようとしたときに、現状だと、RESTful APIがデファクトスタンダードになっていますが、今回の規約は、例えば、getとかputとかdeleteとかpostのようなAPIを少し機能拡張して、今のAPIを活かすという形なのか、いや、新しいアクションを追加するという話なのか、そういうレベルで議論に及ぶといいなど。

データコントロールについても、既にGDPRでは英国をはじめ、Opt in / Opt out出来る機能をSaaSで提供している会社が出てきています。この場合、データ認証やデータコントロールについての機能は、今回の規約で整理する機能とどういう差異があるのか。

データ品質ですが、崎村先生がおっしゃっていたのは、データ品質は、今まさにデータエコノミーで、複数の企業間でデータ市場の間でデータ共有をしようとしたときに、やはり、このデータは、どういう品質なのか、範囲とか、欠損値があるのか、鮮度はどうなのかといったようなデータ品質に対する4Vに基づいた標準があると、より流通しやすいとか。

デジタルアイデンティティーは、一丁目一番地という議論がありますけれども、日本の中で議論してしまうと、マイナンバーカードの取り扱いも触れたいところですが、余りジャパンローカルな議論をしても、なかなかグローバルスタンダードにつながりにくいと思います。

このように、それぞれの技術要素に対し、既存の技術の中をどう拡張するのか、追加するのか、どういうレイヤーに属しているのかということ、是非日本が各国各方面の方々に呼びかけて、みんなで作っていきましょうという流れに誘導できるといいのではないかと思います。

以上です。

○村井座長

ありがとうございます。

それぞれ大変貴重な御意見をいただきましてありがとうございました。さらにこの議論を続けることもできるのですけれども、限られた時間ですので、今、お伺いしたことを含めて、今後、皆さんにも検討していただきたいですし、タスクフォースのほうでも詰めていただきたいことを、若干難しい要求も含めて、少しお話ししていこうかと思います。

まず、崎村さんの動脈と静脈のお話で、情報と金流という考え方も、とても重要だと思いました。COVIDの経験により、いろいろなインパクトがあったのですけれども、そのうちの1つに、ドコモのモバイル統計のデータが使われて、人流を表現するというのが、大変頻繁に行われるようになりました。

非常に長い間、センシティブなデータだから、表で使うことはなかったのだけれども、やはり社会的な価値があるデータだという認識ができていないのかなと思うのです。

崎村さんの金流というか、やはりトータルに社会的価値があるということが、データが出たときに対価が戻ってくるということ、どのようにして表現すればいいのかなということも考えていたのですが、それとも関連するのかなと思うので、後でまた、崎村さんの知見を事務局と共有していただくときに考えていただくとありがたいかなと思いました。

それから、やはり、ステークホルダーは、もう少し抽象度を上げながらも、もう少し性格を洗い出したものがあるって、その中で議論があって、その後から、それを適用した形でのケーススタディになると分かりやすいのではないかと思います。さきほどの繰り返しになりますけれども。

そういう中で、デバイスというのもありましたし、AI系のエージェントなどの役割というのも出てくるのかなと思いましたけれども、いずれにせよ、私が重要だと思ったのは、悪い人というステークホルダーです。アタッカーというか、そういう視点を持っていると、そのステークホルダーの中でのブレインストーミングのようなことができるからいいかと思いました。

それと関連して、世界でいろいろな議論をしていると、自分の個人のデータが政府にコントロールされるのは嫌だと、この国もそうなのだけれども、まず、そう思うでしょう。

ところが、一方、さきほどの藤田さんのお話のように、医療というのは、資格を持った人が医療のデータをきちんと扱う、ここにはTrustがあるわけです。

そうすると、このオーソリティーという意味の定義、つまり、政府がデータを取っているのかということ、非常に抵抗感が生じるのだけれども、一定のオーソリティーのレベルと

いうのをどのように定義するのかというのが、やはり元のデザインから入っているべきだ
と思うのです。

つまり、ステークホルダーは明らかにあるわけで、それで、オーソリティーの種類とか、
役割とか、そういうことが出てくるだろうと思うので、その辺りも少し検討していただ
けるとありがたいかなと思いました。必ず政府の役割を明確に、透明にするということは必
要だと思います。

それから、標準化の中で、今回ロックウェルとGTGSの出口、W3C、ISO、こういうところ
ができました。

浦川さんが、日本が世界の中で紹介するのは得意だからというけれども、本当に得意か
という思いもあります。いずれにせよ、非常に大事なことです。

歴史的なインターネットの発展からいうと私はインターネットの世界に国という概念を
入れるのを避けてきたほうなのです。

ところが、そうも言っていられないというのをどのように表現したかという、私達は、
今回のデジタル政策を考えるときに、3段階という言い方を、個人的に初めてしたのです。
まず、国の中の責任をきちんと果たしましょうと。次にそれを基に、共通の言葉で話せる
仲間の国を作りましょう。そして、グローバルガバナンスを考えましょう。この3段階で
いきましょうという提案をワーキング・グループのほうではしたのです。

それが正しいかどうかは別として、そういう意味での責任の在り方と標準化、つまり、
きちんとしたものができているから提案できるのであって、そこをきちんと厳しく考えて、
今の出口を考えましょうということを思いました。

今朝もオードリータンと2人で話していたのです。台湾がどうしてうまくできているの
かというのを探るといふ目的もあって、彼女と話していたのですけれども、やはり、かな
りやり方が分散的なのです。まさに、ここで話していることに非常に近いのです。アーキ
テクチャーを示して、それに基づいてみんなにやらせているのです。だから、とてもスピ
ード感があって、ある意味の多様性もあるのだけれども、非常にうまくいっているケース
が多いと。いろいろ課題もあるというのをお互いに話していたのですけれども、そう思う
と、これは、3月までのタイムラインという期限が出ているのだけれども、大変申し訳な
いのだけれども、ここまできたら、何かプロトタイプの実装のようなことを、ケーススタ
ディベースで、やはりやったほうがいいと思うのです。

できる人はいるでしょう、タスクフォースの中に。だから、ある程度少し並列に、この
実装を進めて、それでお手本ができて、それが実績になって、また標準化とか、そういう
出口につながると。簡単に言えば、スピード感なのです。

このデジタル庁の法律と基本法だって、2、3か月でやってしまったのですから。そう
いう意味で、この議論は、余りに楽しいからずっと続けられるのです。この分野の話、も
う生まれたときからやっているから永遠にやっているのです。けれども、やはりどこかで
スピード感をどうやって作るかという、やはり実装だと思うのです。

ですから、そろそろそういうことが仕掛けられないかと。タスクフォースのメンバーを見てみると、いかにも実装が早そうな方がいるので、何かそういうことを仕掛けられないかと。場合によっては、その開発に費用がかかるなら、事務局と相談すればいいのではないかと思いつつも、何かその辺りを基に、少しケーススタディベースの実装があって、本当にできたのか検証できれば、そこが強くなるのです。

そうすると、日本に強いものがあって、世界に出せて、説得力がある。そんな話になるかなと思いました。

最後に一言だけ、これだけは言うておかなければ気が済まないということがあれば、あと3分ありますから、お伺いしたいと思います。いかがでしょうか。

よろしいですか。

それでは、まだいろいろ事務局のほうもたくさん宿題を抱えていると思いますので、受けていただいて、それを黒坂さんのタスクフォースのほうでも受けとめていただいて、それはさきほど御説明していただいたとおりですので、詰めていただきたいと思います。

それでは、事務局からの連絡をお願いいたします。

○成田審議官

皆様、活発な御議論をいただきまして、本当にありがとうございました。

協議会は、以上でございます。

次回は、協議会自体は3月を予定させていただいておりますが、予定については、また、別途御連絡させていただきます。

それから、今日は、本当にたくさん、また宿題をいただきましたので、これから大変でありますけれども、途中経過、前回もさせていただきましたけれども、協議会の委員の皆様にも、途中途中で状況を御報告したいと思いますので、また、その際にも、いろいろ御知見をいただければと思っております。

私のほうから、事務的な話は、以上でございます。

本当に、この年末のお忙しい中、皆様、お時間を作っていただきましてありがとうございました。

ぜひ、よいお年をお迎えいただきますよう、お祈り申し上げます。誠にありがとうございました。

○村井座長

最後に、一言いいますけれども、本当に率直に言って、このメンバーは、非常に強力な顔ぶれだと思います。本当にありがとうございました。よろしくをお願いいたします。

では、よいお年を。

以上