

第7回トラストを確保したDX推進サブワーキンググループ議事概要

1. 日時：令和4年3月22日（火）15:00-16:51

2. 場所：Web会議による開催

3. 出席者：

(構成員)

太田 洋	西村あさひ法律事務所	パートナー弁護士
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
手塚 悟	慶應義塾大学環境情報学部	教授【主査】
濱口 総志	慶應義塾大学SFC研究所	上席所員
林 達也	LocationMind株式会社	取締役
宮内 宏	宮内・水町IT法律事務所	弁護士
宮村 和谷	PwCあらた有限責任監査法人	パートナー

高村 信	総務省	サイバーセキュリティ統括官付	参事官
希代 浩正	法務省民事局商事課	補佐官	※代理出席
奥田 修司	経済産業省商務情報政策局	サイバーセキュリティ課長	

(オブザーバー)

伊地知 理	一般財団法人日本データ通信協会	情報通信セキュリティ本部	タイムビジネス認定センター長
井高 貴之	厚生労働省 医政局	研究開発振興課	医療情報技術参与 ※代理出席
太田 大州	デジタルトラスト協議会	渉外部会長	
小川 博久	日本トラストテクノロジー協議会	運営委員長	兼 株式会社三菱総合研究所 デジタル・イノベーション本部 サイバー・セキュリティ戦略グループ 主任研究員
小川 幹夫	全国銀行協会	事務・決済システム部長	
奥野 哲朗	厚生労働省 医薬・生活衛生局	総務課	課長補佐 ※代理出席
小倉 隆幸	シヤチハタ株式会社	システム法人営業部	部長
金子 聖治	厚生労働省 医薬・生活衛生局	総務課	指導官 ※代理出席
小松 博明	有限責任あずさ監査法人	東京IT監査部	パートナー
佐藤 創一	一般社団法人新経済連盟	政策部長	
佐藤 帯刀	クラウド型電子署名サービス協議会	協議会事務局	
柴田 孝一	セイコーソリューションズ株式会社	DXサービス企画統括部	担当部長 兼トラストサービス推進フォーラム 企画運営部会 部会長
島井 健一郎	厚生労働省 医政局	研究開発振興課	医療情報技術推進室 室長補佐 ※代理出席
島岡 政基	セコム株式会社IS研究所	主任研究員	
袖山 喜久造	SKJ総合税理士事務所	所長	
豊島 一清	DigitalBCG Japan	Managing Director	
中須 祐二	SAPジャパン株式会社	政府渉外	バイスプレジデント
中武 浩史	Global Legal Entity Identifier Foundation (GLEIF)	日本オフィス	代表
西山 晃	電子認証局会議	特別会員 (フューチャー・トラスト・ラボ)	代表
野崎 英司	金融庁 監督局	総務課長	
肥後 彰秀	独立行政法人情報処理推進機構 (IPA)	デジタルアーキテクチャ・デザインセンター (DADC) インキュベーションラボ	デジタル本人確認プロジェクトチーム プロジェクトオーナー
三澤 伴暁	PwCあらた有限責任監査法人	パートナー	
山内 徹	一般財団法人日本情報経済社会推進協会	常務理事・デジタルトラスト評価センター長	
若目田 光生	一般社団法人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	データ戦略 WG 主査

(デジタル庁 (事務局))

デジタル社会共通機能グループ 楠 正憲グループ長、犬童 周作グループ次長 他

4. 議事要旨：

- ・事務局より、資料1「事務局説明資料」について説明。
- ・有識者より、資料2「eIDAS2.0とEUDIW」、についてプレゼンテーション。
- ・会合欠席の佐古構成員からの意見を事務局より発表。

- ・自由討議において、主に以下の発言。

・資料2の14ページでEUDIWの機能の概要を書いているが、デプロイの部分に関して、安全な経路でどうやってユーザーに届けるかというところがトラストに重要になってくる。ここの部分の記述等があったらお教えいただきたい

マルチステークホルダー・プロセスにおいて、レビューを行い、 이슈や問題を集めるというプロセスが必要。これらを集めることで、実際にどういうふうにこれを改善していくのかというサイクルが回せる。マルチステークホルダーモデルで重要なのは、透明性とオープンネスである。最近では、日本政府でもGitHubの利用を推進できている状況になってきている中で、関連文書、 이슈、プルリクエストを広くオープンに公表していくことでマルチステークホルダー・プロセスを回していくのを、デジタルのツールの力で最小化し、効率よくオープンに実施できるのではないか。

・今、公開されている資料の範囲では関連の記載は無い。EU DIWはスマートフォン上のアプリとして実装するという事も決定されていない。これまでEUの法律というのは、その技術的な実装から中立性を持って書かれてきているので、今の段階ではまだこの実装で行くという書き方はされていない。それが無いことにはデプロイについても議論にならない。

・資料2の4ページ、加盟国間の認証トランザクション数が2020年で6万件と少ない数字となっているが、国内で閉じているトランザクションが入っておらず、国をまたぐトランザクションが少ないからという理由からか。今の段階ではインターオペラブルにならず、Walletの信頼性をどうやって確保していくのかというのは難しい問題になると思っているが、その辺りは検討されているのか。

資料1の事務局資料のほうに関して、マルチステークホルダーモデルのCivil Societyに企業だとか企業団体が入っているのは違和感がある。OECDでもCivil SocietyとBusinessは分けている。OECDでは、トレードユニオン、労働者、Businessを分けてやっているなので、その辺は考えたほうがいい。Business Ownerは、サービスプロバイダという別の言葉に言い換えた方が良い。Tech CommunityとCivil Societyに並ぶような形でBusinessという枠で、考えようによってはトレードユニオンみたいな枠も作ったほうがいい。Regulatorもマルチステークホルダーの点線の中に一部かかるべき。マルチステー

クホルダーには評価とトランスペレンシーが重要。透明性とトラストというのは非常に近いところに密接に関係しているので、その透明性をどのように確保していくのか。ログを確保するなどを考えていくというのが必要。

- ・統計データは、全加盟国間のトランザクションを示しているわけではない。かつ、加盟国間の認証トランザクション数になっており、国内の認証トランザクションではない。例えば、オランダにおいてルクセンブルクのeIDが使われたような数だけを加算している。それでも、数としてはそんなに多くないというのが現状。eIDのeIDASの評価結果の中にもあったとおり、範囲が狭過ぎた。59%の市民しか最大でもカバーできない通知されたスキームしかないにもかかわらず、国境を越えたサービスで、かつ、公共サービスでしか受けられないとなると、多分、国境を越えて公共サービスにアクセスしたい人の数がそもそも限定的で、かつ、その中でeIDを持っている人の数が限定的だということで数が少ないということは、この評価報告書の中でも示されているとおり。

ウォレットの信頼性に関する御質問は、まだ技術的にどうやってその信頼性を保証するのかということとは書かれていないが、法案上は、EUの各加盟国の専門家が集まって、さっきのArchitecture and Reference Frameworkといったような、いわゆる機能要件レベルのものを書いている。その後、技術基準が作られている。技術基準が作られた後に、今、EUのサイバーセキュリティーフレームワークというものが設計されてきているが、そちらのほうでEU Digital Identity Walletのセキュリティー認証を行うということが法律案では書かれている。

- ・事務局資料のマルチステークホルダーモデルについては、いただいたご意見を踏まえた形で次回までに修正させていただく。

- ・事務局資料では、マルチステークホルダーモデルでは、処分通知、公的な証明書等に割と注力していくことになる感じを受けた。GPKI、LGPKIの最新化や公文書の真正性の確保という意味でのタイムスタンプ・eシールも重要だが、社会全体でDXを考えたときに、公文書が最も重要だとは思っていない。むしろ、DXの主たる領域というのは、BtoBやBtoCになるのではないか。そういった領域では、電子取引のDXがすごく重要で、そのためには、電子署名法の見直しやリモート署名とか立会人型署名という、クラウドで署名するようなものについての基準を固めていく必要がある。

そういう意味で、政府システムでの本人確認ということで電子契約と資料に書かれているが、政府調達における電子契約というふうに政府調達に限定する必要はなく、もっと広く電子契約を考えるのが妥当。

なお、仮想通貨取扱業者が高額の仮想通貨を持っていながら、あまりそのセキュリティ的な基準というものが一般的には言われておらず、その結果、すごく巨額なものが流通し

たという事件も起こっている。これを他山の石として、トラストを確保したDXの推進に関して考えていく必要があるのではないか。特に、立会人型の電子署名を含む、電子署名についての身元確認の在り方や、一昨年、2020年9月4日の政府Q&Aで示された、立会人型電子署名サービスのプロセスの固有性についても、判断基準をしっかりと策定していくことが必要。これが国全体としてのDX推進のために不可欠な状況。

そういう点から、このマルチステークホルダーモデルというのは、政府のシステムに関する提言をするものかのように見えるが、実際には民間を含めたトラストの枠組みの検討や、法制度の検討も必要。ここについて、事務局の考えを伺いたい。

それから、ここのBusiness Ownerに書かれているサービス運営企業とはどういうものか。これが国のシステムだけを相手にするのだったら、デジタル庁などになるが、民間だとこのBusiness Ownerはサービスプロバイダになると考えてよいか。

・一点目については、マルチステークホルダーモデルというのは、資料の例1、例2で挙げたものに限るものではなく、民間での手続や取引に関しても想定しているが、まず、事務局として案をお示しする中で、具体的な例示をするに当たって、まずデジタル庁でマルチステークホルダーモデルを運営していけそうなところということで、例示を挙げた。

二点目については、各コミュニティの構成員に関しては、もう少し案を詰めていく必要があるが、民間手続・取引の案件においては、サービス運営企業というのは、例えば、トラストサービスプロバイダになるのではないかと現時点では考えている。

・事務局が例に挙げているGPKIの技術基準の最新化や公文書における技術基準は国が決めればいいのであって、色々なところから意見を聞くというのは、パブリックコメントを使って吸い上げるべきであり、敢えてマルチステークホルダーモデルを使う必要はないのではないか。eIDASでも技術基準についてまで本当にマルチステークホルダーモデルで決めているのか。例えば、濱口構成員の発表の資料の中でもeIDAS2.0の下位規則の整備について触れられているが、ここでも技術基準を指定する下位規則の整備をEU委員会に義務づけということになっているので、そういう意味では、これはEU委員会が責任を持って決めるということになっていて、必ずしもマルチステークホルダーモデルで決めているのではないか。さらに、マルチステークホルダーモデルは、我が国の法体系の中では、個人情報保護法の53条にあるような形で、認定個人情報保護団体の指針の策定にマルチステークホルダーモデルが取り入れられているのだが、個人情報保護法の場合には、非常に様々な利害を持つ様々な関係者がいるので、そういう微妙な利害関係を持つ関係者の納得を得られるようなものを作り上げるために、このマルチステークホルダーモデルを用いていると理解している。しかし、今挙がっているような、例1、例2の技術基準というのは、技術基準の話なので、これをマルチステークホルダーで議論するというのは違和感がある。

実際、ICANNやIETFが例として挙げられていたが、インターネットはある意味で政府がない世界での技術基準を議論していく場なので、ICANNやIETFでマルチステークホルダーモデルが使われているのは、ある種の専門家の村の中で決めているような話で違和感がないが、今回の話の中で、Civil Societyの中に消費者団体や弁護士会を入れてはどうかということがあったが、あまり弁護士会でこんなことができるとはあまり思えない。

事務局資料の中での、国際的な相互通用性を持ったID Walletの仕組みをどうするかというところは、これは多少、マルチステークホルダーモデルにもなじむかもしれないと思うが、処分通知、公的な証明書とか、政府システムでの本人確認は政府で決めればよい話で、これはマルチステークホルダーモデルが関わって議論しだすと、議論は収れんしない。しかも全員のコンセンサスが必要ということになると、いつまでたっても決まらないし、迅速性が著しく損なわれるのではないか。

・資料2の9ページ目で、技術基準を指定する下位規則の整備を欧州委員会に義務づけていることを説明している。下位規則では、eIDAS2.0の法的な要件は、下記の技術基準を充足したときに要件を充足しているとみなすと書かれているので、基本的には既に作られている技術基準のリストを下位規則という形で指定している形になる。実際の技術基準自体は、欧州標準化団体であるETSI、CEN、CENELECの3団体のうち、基本的にはCENとETSIから技術基準が参照されている。ETSIとCENそれぞれで、恐らく、標準化のプロセスは異なってきており、ETSIの標準化のプロセスでいうと、基本的にはETSIというのは民間の会員制の標準化団体になっている。例えば、最近ではGoogleがたくさん投票権を持って、ETSIの欧州の標準化でもかなり強い意見を持ち始めている。ただ、欧州標準化団体というのは、基本的に一般私企業がたくさん投票権を持っていて強い力を発揮して技術基準を作るようなことを許していない。なので、実際にはその上に欧州規格としての投票プロセスがある。その中で、各加盟国の実際の投票、加盟国1票という形で投票を行って、欧州規格として成立する形になっているので、いかに企画、立案の段階で一般の私企業が、民間企業が自分に有利な形で投票したとしても、実際の欧州標準としてはそういったことがまかり通らないようなプロセスになっている。ただ、それが、この事務局資料で示されているマルチステークホルダーモデルと同等のレベルのマルチステークホルダーかという疑問である。ただ、このeIDASのフレームワークの中で、基本的には技術基準に関して、標準化団体に標準化を委ねている。ただし、採用する技術基準に関しては最後、加盟国の投票をもって承認している。最後、下位規則の整備という形で下位規則を作って、法律によって作られた技術基準を指定していくところは欧州委員会が行っている。公的なプロセスとしては入っていない。基本的にはパブリックコメントという形で意見を受け付けている。ETSIの中にも技術的なことに詳しい弁護士が入っており、IT系に強いことを武器にいろいろビジネスを広くやられている方が標準化団体のほうにも入ってきているので、一応、弁護士や法曹関係者の意見というのも反映された形で技術基準が作られている。

- ・資料2のトラストサービスの拡充というところでe-Ledgerを記載していたが、どのようなユースケースが欧州で想定されているのか。

- ・いわゆる分散台帳のこと。法案自体には分散台帳とは書かれていないが、法案の序文のほうに技術の進化例、ブロックチェーンだとかディストリビューテッド・レジャー、分散台帳というのが出てきているので、それに対応しなければいけないということが書かれている。その法的効力は、分散台帳に記載される時系列データの真正性を保証するということになる。実際にどういったサービスモデルがあるのかについては、例えば、Digital Identity Walletがスマートフォン上に実装されたという仮定でお話すると、Self Sovereign Identityのように自己主権型のアイデンティティを達成しようとした場合に、検証をする都度、どこかのサービスプロバイダにそのウォレットの中のIDが真正なIDであるかどうかという問合せが行くような形の実装だと、誰がいつ何に対して自分の認証を行ったかというデータがトレースされてしまうようなことが起きる。それを実際にどういった形で実装すればよいのかといったときに、この分散台帳を使う。分散台帳でそのIDの発行した記録を分散台帳のほうに記載しておいて、検証する側は分散台帳のほうに見にいて、そのIDがいつ発行されて真正なものであるかどうかという検証結果を見に行くようなプロセスを経ることで、自己主権型のいわゆるその機能の一部を実装できるのではないかということが議論されている様子。

- ・eIDAS2.0では、IoTに対してのID、台帳は考慮されているのか。

- ・eIDAS1.0では、機器から出てくるデータ、例えば、画像の写真の真正性をeシール用の証明書でデジタルサインすることで保証することが検討されていた。ただ、日本で検討しているような、その機器自体の証明書というよりは、あくまでその機器がどこかの法人で製造した、管理している、運用しているという情報と紐づけた形での証明書の運用をe想定していたようである。

- ・マルチステークホルダーモデルについて、技術基準だけでなくコンテキストを踏まえてトラストが確保される現状を踏まえ、DFFTのTを担うということが書いているが、これを考えた場合、やはり技術基準だけでないと考えている。そうなのであれば、DFFTのユースケースの中のどこに関するユースケースで、それに関するまさに技術基準なのか、もうちょっと広いコンテキストも含めての何なのかというところが、全体のマップの中で分かれば、マルチステークホルダーモデルを適用すべきなのか、また、誰をステークホルダーとして設定すべきなのかというのが変わってくるのではないか。

・いただいたご意見を踏まえて、マルチステークホルダーモデルで議論する内容やスコープについて検討したい。

・ETSIだけでなく、ETSI、CEN、ISOの関係も見ておく必要がある。マルチステークホルダーということに関して言うと、ISOの側も結構、OECDのようにステークホルダーを分けているわけではないが、参加はできるような格好になっている。弁護士や、Civil Society的な感じの方もいらっしゃる様子。

・もしマルチステークホルダーモデルを採用するのであれば、ルールを明確にしていかないと、有識者会議の構成と明確な差異というのがあまりできないのではないかと。それぞれのコミュニティの権限や責任、それぞれが作る成果物のモデル上の正式な位置づけをルールとしてまとめる、また、その構成員の選定方法についても公平な形でルール化することが重要。これに関して、政府が決めればよいのではないかとこの御指摘もあったが、ICANN、IETFと同等のレベルのマルチステークホルダーモデルというのは、今回の件に関しては不要なのではないか。マルチステークホルダーモデルに関してレベル感があって、ISOでやっているようなレベルのマルチステークホルダーモデルなのか、ICANNでやっているようなマルチステークホルダーモデルなのかというところがあると思うが、必要なレベルのものを議論していけばよいのではないかと。

公文書におけるタイムスタンプ・eシールのニーズを踏まえ、これらの技術基準で何を定めるべきかということについては、仮にこれが公文書に押すタイムスタンプ、あるいは公文書につけるためのeシールの技術基準という形で策定されたとしても、例えば、NISTのSP 800-63で約63年のようにこのタイムスタンプやeシールの技術基準というの、公文書のための基準と言ったとしても、民間は参照することになると思うので、そういったことも念頭に置いて技術基準を検討していく必要がある。

・Identificationのアシュアランスレベルについては、ユースケースをこのワーキングが示すというのは間違いと考える。どの程度の確認に当たるのかを定性的に示した上で、ユースケースサイドがレベルを選択できるようにすべきである。

今後の検討体制について、事務局資料で示しているマルチステークホルダーモデルでは、必要条件を誰が定めるのかというのが抜けている。Regulatorサイドが、求める必要条件を入力しないと、議論するだけ無駄ということになる。今、この場で議論していることも、電子署名、要するに実印に代わるものをどうしますかという議論をしているのであり、そういった要求条件を出してくれないといけないのではないかと。あと、Business Owner、Tech Community、Civil Societyというのが、慣れていない人には違和感があるので、サービスの提供者、利用者技術を分かっている人など、日本語で書くべき。

ICANNやIETFの事例が出ているが、インターネットのマルチステークホルダーモデルは、

提言側の方が声大きいことに留意すべき。Civil Societyが要求条件を突きつける側なので、ここで考えているマルチステークホルダーモデルとは異なる考える。つまり、インターネットの世界でプライバシーを要求するのは、Civil Societyの人である。それに対して、今の日本の社会の状況で言うと、面倒くさいからプライバシーの要件を緩くしろというのがCivil Societyから来るため、条件の設定の仕方を間違えるとぐちゃぐちゃになると考えている、

利用者という意味でいくと、ここのCivil Societyの中の企業にユーザー企業が入ってくるのは特に違和感はない。

資料2で属性の話が出ていたが、欧州では属性の話は今後やるということになっているということなので、この場で何度か議論に上がりかけたその資格の話は、欧州の様子見ということも含めて、今、この段階で、この場で結論を出ようと頑張らないほうがよいのではないか。

・濱口構成員の発表をお伺いして、ヨーロッパの議論というのが、足元で今提供しているものがどのように使われているかというところをレビューした上で次の手を打っていることが理解できた。こういった姿勢というのは、本来、我が国においても極めて重要である。今の電子署名法の運用がどうなっているかや、クラウド署名がどういう使われ方をしているかみたいな話もあったが、これらの議論を踏まえて、これから足りないところをどうインプラブしていく必要があるかという議論をしなければならないと考えた。EUのDigital Identity Walletに関しても、これをiOSでAndroidがどんどん対応してくるのであれば上手に相乗りできるかなと思っていたのだが、どうやらもうちょっと時間がかかりそうで、それを待って何かやるということよりは、ちゃんと日本は自分たちで考えて主体的にやっていき、そのときに各国がどういった要件を満たそうとしているのかを横目で参考にしていくというのが、現実的なところなのだろうと感じた。

また、事務局から御提案させていただいたマルチステークホルダー・プロセスについて、大変多くの御議論をいただいた。未熟なところもあるが、これをどういう形できちんと回し得る、納得が得られるものにしていくかというところで、ぜひ引き続き御指導いただきたい。民間も入ったユースケースや、新しいものの方がより必要性が高いという思いもありつつ、実際にやっていこうと思うと、サービスプロバイダはかなり汗をかいていく必要のある話であり、デジ庁としては自分たちが最初に汗をかきますよというところまでは決断できている中で、一体どこまで民間のサポートをきちんといただきながら回していけるかというところは非常に大きな課題であろうと思っている。

そういったことも含めて、あと3か月できっちりとアウトプットを出していきたいと考えている。引き続き御指導のほど、よろしく願いしたい。

・会議資料は、デジタル庁ウェブサイトにてこの後公表させていただくこと、追加の意見

及び質問は事務局まで連絡の上、事務局で今後の運営の参考とすること、議事要旨は、構成員の皆様の内容を確認いただいた後に公表させていただくこと等を事務局より説明。

・次回のサブワーキンググループの会合は、令和4年4月8日(金)16時00分よりオンライン開催予定であることを事務局より説明。

以上