第５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２月８日（火）11:00-12:51

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
佐古　和恵　早稲田大学　基幹理工学部情報理工学科　教授
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
佐藤　秀紀　経済産業省商務情報政策局サイバーセキュリティ課企画官　※代理出席

（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「トラストサービスのアシュアランスレベルの考え方」、資料３「GlobalSignにおける電子証明書の利用事例」、資料４「トラストサービスのユースケース及び制約となる制度について」、資料５「サービス提供におけるトラスト確保を実現するポリシー策定の論点」についてプレゼンテーション。

・自由討議において、主に以下の発言。

・Identificationのアシュアランスレベルにおいてマイナンバーカードを用いた署名を位置づけるとしたら、(NIST基準では)AAL3となるだろう。現在の「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」には、日本の固有の状況が必ずしも含まれていない。当サブワーキンググループで検討を行い、このガイドライン改訂に打ち込んでいくような活動が望まれる。

契約書は準拠法を書くのでInteroperabilityは必ずしも必要ではないという意見があったが、準拠法を定めたとしても、実際に証拠性などを考えるときにはInteroperabilityは要るのではないか。例えば日本法が準拠法になった場合に、欧州やアメリカの会社でも日本の法律に基づいて判断すると、外国の会社も日本のトラストサービスを利用する必要が出てくると考えられる。逆に、欧州の国の法律が準拠法なら、日本の会社は日本のトラストサービスではなくEUのトラストサービスを使うことが必要になってくる。Interoperabilityを確保すれば、相手の国の法律が準拠法であっても、自分の国のトラストサービスが利用できると考えている。

茨城県庁からの要望について、個別の法令や条例で電子署名や電子証明書を規定すると、それぞれに対応しなければいけないので利用者に大きな負担が生じる。統一のレベル分けをデジタル庁あるいはその他政府機関などの規格を制定していくような機関で決め、各法令や条例で参照していく方法を取るべき。個別の法令で基準を決めていくと、その判断が明らかでないような場合に、グレーゾーン解消制度を使うようなことになりかねないのは、望ましい状況ではない。LGPKI、地方公共団体の職責証明書等がなかなか使えない理由は、AATLに載っていないからだが、LGPKIについても、ポリシーの公表や第三者監査などを実施する方向でパブリックの利用を広めていくべき。

トラストアシュアランスレベルの策定に当っての詳細の議論は、当サブワーキンググループの下に、分科会を設置して、レベルの策定についての案を分科会で策定するべき。

・Identificationのアシュアランスレベルの議論においては、IALやAALといった基準以外に、IdP(Identity Provider)そのものの評価のフレームワークが整備されていく必要

がある。米国の場合は、Open Identity Exchangeを通してトラストフレームワークプロバイダーを認定する枠組みを政府が準備していた。また、行政手続におけるガイドラインだけでなく、ガイドラインの民間での位置づけや有効活用方法についても考えていく必要がある。

紙や対面のプロセスのデジタル化だけでなく、Society5.0やDFFTの実現に向けて、流通、自動処理されていくデータの信頼性については、必ず誰がそのデータをつくったのか、あるいはその誰というのは自然人、法人なのか、いつのデータなのか、その完全性が保証されているのかどうかについて、一定の保証レベルのものを自動で検証できる基盤が必要であり、そのためにもこのトラストサービスの整備が必要不可欠。

茨城県庁からの要望について、電子証明書について、共通の要件で定められているほうが望ましい。LGPKIについて、AATLに入っていないという現状は、国際的な技術基準のケースや相互承認に対して注力を陥ってきた現れ。例えば、EUのQuantified Trust Serviceであれば、自動的にAATLに入っており、Adobe製品、Adobe Reader等で検証可能な署名として表示されているのに対し、日本のLGPKIがAATLに入っていなくて、茨城県庁では民間の証明書を使わざるを得ない状況になっているというのは不本意。これからはLGPKIを含め、諸外国と比較して妥当な運用になっているかどうか十分検証していくべき。

トラストサービスのアシュアランスレベルについては、IALやAALといったものが当てはまらないトラストサービスもある。トラストサービスアシュアランスレベルの基準には、別の場を設けて集中的に議論を煮詰めていく必要がある。一方で、詳細な技術基準について、例えば欧州のETSIやCENで標準化されている技術基準と同レベルのものを想定するのであれば、ゼロから整備していくというのは非常に膨大な作業量になるので、既にある基準、ETSIやウェブトラスト、その他基準をベースにISO化の提案等、作業をショートカットしていくような工夫も必要。

・Adobeには、AATLに登録されている古いGPKIの証明書を新しい証明書に更新してもらえないかと交渉したが、Adobeでは、2017年６月に技術要件が変わり、ルート証明書の鍵長が3072ビットになったため、鍵長がその基準でないと難しいという話があった。LGPKIも交渉したらしいが、ルート証明書の鍵長が問題となって登録に至っていないらしい。認証局は鍵更新が５年に一度あるため、次回の更新を見据えてAATLの登録を検討して参りたい。それまでは、今年９月に誰でも検証できるようなツールをGPKI側から提供する予定にしている。

・ｅシールについて、ワクチンパスポートを数百万枚提供しており、かなり大規模な事例として実装している。ワクチンパスポートというInteroperabilityが求められる事例において課題となったのはトラストフレームワークであり、これはWHOが整理しようとしてできなかった。EUの方式はEU Digital Green Certificate Gateway (DGCG)でトラス

トフレームワークを規定し、ICAOに関してはパスポートのトラストフレームワークに乗っかる形で実現し、スマートヘルスカードについては、公開鍵をデータ上のURIとして記載し、ドメインのトラストの上に乗っかる形態で実装した。マイナンバーカードが最高レベルの認証手段であるべきか、最高レベルというのをどう定義するか疑問がある。現在でも、2048ビットのRSA暗号やシリアル番号の付番の方法を含め、必ずしも現代的なPKIになっていない。LGPKIのInteroperabilityに関しても御指摘があったが、GPKIでウェブトラストのCA/Browser Forumの基準を満たすことがでず、アプリケーションCAの運用を止め、原則としてSSLのサーバー証明書は民間のものを利用するというような結論に至った過去の事例もある。欧米と比べて我が国におけるトラストに対する投資は十分ではなかった。このような状態で何とか運用している中、我が国のトラストサービスが世の中のニーズに見合っていない実情もあることから、我が国のトラストサービスが社会的な責任を果たしていくためにはどうやって体制強化をしていくかというところも考えないといけない。

トラストアシュアランスレベルでは、全体のトラストレベルを議論しているとすると、NIST SP800 63-2のLevels of Assuranceの考え方との関係はどう考えているのか。

・トラストアシュアランスレベルでは、国の監督機関、適合性評価機関、認定の仕組みが必要ということ。適合性評価機関を国が認定するということで、以下は適合性評価機関がトラストサービスを運用しているプロバイダーの設備をチェックする。電子署名法での認定認証事業を監査しているJIPDECと同じような役割になっている。JIPDECは、指定調査機関なので、立てつけ方は別だが、認定ということで民間がもっとフレキシブルに複数の適合性評価機関が動いていくということで検証していく。それを実際にやるにおいては、認定の基準を国で定めていくことになる。今、電子署名はそれに近い形で、認定認証事業自体はやっている。急に日本に新たなものを導入するというわけではなくて、今までも電子署名で近い形のものをやっていたので、より広い範囲でそういうことができるようにしていったらどうか。

・トラストサービスとそのアシュアランスレベルの議論にあたっては、今まで主として議論をしてきた 1. 認証・認可、タイムスタンプに関わるトラストサービス及びそれを提供するサプライチェーンと、2.各種データそのものの流通・処理を行うサプライチェーンを区別して議論した方がよい。いままで話をしてきている 1.トラストサービスでサポートできる 2.で流通・処理されるデータの信頼性は、正当性、完全性等の限られた主題やスコープに限られるものであり、デジタル原則でのデジタル完結・自動化原則で必要となってくる、2.データの流通そのもののサプライチェーンで求められるデータの信頼性は、今まで議論をしてきた 1. のサービスで提供できる正当性、完全性、タイムスタンプ（適時性等）のみならず、正確性、網羅性も必要になるだろう。トラストサービスのス

コープやアシュアランスレベルを考える際、主題を明確にして、主題やスコープから外れているものは、利用者側で自ら信頼を担保する必要があることになる。トラストサービスのスコープやアシュアランスレベルの議論にあたっては、ユーザーサイドで担保しなければならないトラスト部分をクリアにして取り組む必要がある。DFFTやデジタル原則等を目的として制度設計を検討していくうえでは、カバーできる主題やスコープが、正当性、完全性に限られたものなのか、正確性、網羅性まで含めたものなのか、また2. データの流通そのもののサプライチェーン上どのスコープをカバーできるものなのかを切り分けて考えていくべき。

・認定事業者の認証は、レベル分け以上に運用がどうされているのかとそれをどう監査するかが重要。一時点での監査は過去のものになる。運用上では、受け取り手は、それがいつされたのかというメタデータをリスク管理のために必要とする。単にレベルがどうのという話ではない。

アメリカでも国の認定があるという話があったが、ICAMという連邦機関による利用のための認定なのでこれは当然。それでは、民間での認定基準の活用はどうなっているかというと、あまりうまくいっていない。主要な事業者にそっぽを向かれてしまったため。そこまで考えて制度設計する必要がある。

トラストサービスのレベル策定にあたっては、色々なものを入れ込まない方がいい。Identification、Authentication、AuthorizationやClaim verificationは全部分け、独立に考える必要がある。トラストサービスのアシュアランスレベルで担保したいものについては、時間がたった後のトラストも担保する観点が必要。Identificationアシュアランスレベルとトラストサービスアシュアランスレベルは直交する概念なので、混ざらないようにしたほうがいい。運用に対する透明性をいかにして担保していくかが重要。

・身元確認や認証プロセスの考え方について、「行政手続におけるオンライン本人確認の手法に関するガイドライン」を参照することで対応可能ではないか。トラストを議論していく中で、行政でどのようにやっているかということが、民間でのトラストサービスを考える場合も出発点になっていくはず。

茨城県からの要望に関しては、GPKIやLGPKIがAATLに載っていないこと自体が大問題。デジタル庁の方から検証ツールを別途配付するみたいな話があったが、ユーザーの観点からすると、GPKIにのみ別途検証ツールが必要になっていることだと、より一層デジタル化が進まない原因にもなり得る。デジタル原則で今後政府としてデジタルの方向に舵を切っていくからには、民間のユーザーの立場からすると、AATLに載っているということが使いやすさの一つの大きな基準になっている。できるだけ早期にGPKIもLGPKIもAATLに載るような形にしてほしい。

トラストサービスのアシュアランスレベルの基準の中で、監査要件が入っているのは疑

問。これはやや性質が異なるのではないか。アシュアランスレベルとしては、確保されるべき実体は何かという話（実体要件論）と、それが確保されているかどうかということを検証、認定する際の手続の話（検証・認定手続論）とは分けて考えたほうが分かりやすい。監査要件は、認定の際にこういう監査をしなければいけないという認定手続の中に入ってくるのであれば理解ができるが、アシュアランスレベルそのものの中に監査要件が入ってくるというのは違和感がある。

・TALについて、基準に合致しないものでも電子であることをもって否定されないようにすべきというのが前回までの議論と理解しており、自己が監査すらしていないレベルとして、TAL0も入れるべき。

トラストのアシュアランスレベルで担保したいものについて、総務省で類似の議論を重ねてきている中で、紙が自然に持っている証明機能をデジタルに持ち込むというのがまず大前提で、その上で、誰が発出者なのかを区別する際に、経済産業省で議論されているサイバーフィジカルセキュリティフレームワークの中で、エンティティーととされているヒト・モノ・ソシキが必要になる。今後、制度論を考えていくときに、モノが発出者としてトラストに将来入ってくる可能性があることを留保する必要がある。何を証明したいかについて、サイバーフィジカルセキュリティフレームワークだと、データ、プロシージャ、システムが要素として挙がっているが、eIDASや電子署名法等で定義されているものは人の意思、事実、時刻、いつからの３つが挙がっている状態という認識である。

茨城県の要望書については、法律上、公務員だけが文書を成立に関して特殊な扱いをされていることが、国の場合は官職証明書、地方公共団体の場合には市職責証明書がある理由になっている。GPKIやLGPKIについては、日本政府は、ブリッジ認証局で全部の電子証明書が統合される形で運用されており、このブリッジ認証局のルート証明書がAATLに載るようデジタル庁にて取り組んでいただくべき。

IALについては、長期的には、自然人を確認したいのか、YouTuberの誰々ですということを確認できればいいのかというユースケースを念頭に置いて制度の議論をするべき。

マイナンバーカードで署名することがIAL3相当の認証になるという話については、前橋市でスマートシティの流れの中で、「まえばしID」が発行され、マイナンバーカードでの電子署名を起点として、別のIDを振るということをやられている。これをやるために、先般、デジタル庁で認定認証事業者を新たに認定されたはずであり、このような、マイナンバーカードについている電子証明書を直接使うのではなく、そこから起点としてつくられた確認されたものを便利使いしていくというケースは、全体の仕組みとして念頭に置いておいたほうがいい。

・トラストサービスは、「インターネット上における人・組織・データ等の正当性を確認し、改ざんやなりすまし等を防止するしくみ」と定義されているが、何をもって正当かと

いうのが、ユースケースあるいはサービスによって異なるのではないか。レベル分けも重要だが、何の正当性を確認したサービスを提供しているのかということが重要ではないか。例えば、PCR検査結果への署名がある時、検証する側が、これは誰の公開鍵（検証鍵）で確認できるのかとか、それが本当に医療機関なのか名前から分かるのかとか、など、、何をもって正当としているのか、いろいろな解釈ができてしまう。

原本性と真正性というキーワードについては、紙だから原本性と真正性が必要なのであり、デジタルデータに関してもこれらの２つのキーワードが必要なのか悩ましい。

・PCR検査については、ワクチンパスポートでも悩んだ点で、アプリ一つでこの人が安全だと分かるようにしてほしいというニーズがあったのだが、PCR検査の精度が結構ばらばらであり、中々認められないという中でまだ実現できていない。この研究会も、ずっとユースケースからスタートして議論をしてきており、それぞれのユースケースにおいて求められるトラストとは何なのかというところに本日の議論でもかなり引き戻された部分があった。そういった議論を積み上げていく中で、本当に信頼できる社会をつくっていくために必要な要件が整理されてくると、これからつくるべきものというのも見えてくるのではないか。

・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頂くこと、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、構成員の皆様に内容を確認いただいた後に公表させて頂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２月25日15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