第４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１月25日（火）16:30-18:15

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
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
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
杉　眞里子　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）
袖山 喜久造　SKJ総合税理士事務所　所長
高岡　文訓　金融庁　監督局　総務課　監督管理官　※代理出席
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）
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「インキュベーションラボ・プロジェクト「サービスに応じたデジタル本人確認ガイドラインの検討」」、資料３「欧州eIDAS規則におけるアシュアランスレベル」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。

・当サブワーキンググループの目的は、トラストを確保してDXの具体的な推進方策を検討することである。アシュアランスレベルというのは、それに加わってくる条件である。DXでは、データの相互運用性と自動処理が重要で、設備としてはAPI接続性とデータ形式の相互運用性を確保するためには、仕様を決めて、継続的テストを行うためのテスト環境を提供するなどが必要になり、そこに認証と証明のアシュアランスレベルが入ってくる。したがって、データの相互運用性のも本サブワーキンググループで議論するべき。

・資料１の４ページ目については、トラストアシュアランスレベルとなっているが、トラストサービスアシュアランスレベルのほうが正確。

・資料１の10ページについては、AAL.3でハードウェアベースが必須のような書き方になっているが、ここでいうハードウエアは、NIST SP800-63では、FIPS 140-2の要件を満たすハードウエアという意味。資料には、FIPS 140-2で規定されている要件を列記するか、FIPS 140-2を参照できるようにすべき。脅威ベースで考えるのは実務上重要である。資料では、ハードウェアベースと検証者なりすまし耐性の要件があることが記載されているべき。

・身元確認や認証プロセスのレベルの議論において、基本的な考え方は、国際標準があるので、SC 27などの国際の場でやるべき。

ユースケースについては、偽造証明書の提示、認証機の貸借など問題になっているケースがある。日本においては、証明書の非改ざん性の確認が非常に難しいという問題もと見ておくべき。

BindingやFederationが重要なのは論を待たない。貸借の問題もBindingの話と密接に関係している。リモートのeKYCは、認証情報連携の話。ただ、国のレベルで決めていけるかは疑問で、標準化団体に委譲して、Interoperabilityが取れるところで議論すべき。

・資料２について、ニュージーランドを参考にするのは良い。ISO/IEC 29003のエディタ

ーをしていた人が基準策定していて、ISO/IEC 29003の議論が反映されている。（発表中）民間のデジタル本人確認ガイドラインが無いという話だったが、ISOの基準を実質化するというアプローチもある。ISO/IEC29003も、ISO/IEC 29115も改定が必要な時期になっており、エディターの引受手がいない状態なので、逆に手を挙げるのも良い方法である。発表中挙げられているユースケースは、おそらく行政機関における身元確認や認証における身元確認だが、実際に確認すべき属性はユースケースによって異なる。第１ステップとして、確認すべき属性をリストアップするべき。基本情報は、アプリオリにこういった基本情報が必要というわけではないので、ユースケースごとに考えるべき。(参考)
レベル区分については、脅威ベースで書き換えたほうが良い。国際基準等に合わせて、本来はどうでなければならないけれども、日本ではできないから、このように妥協していというように、あるべき論を考えていったらいい。

・資料３について、eIDAS1.0が成功だったのかの総括は必要。EU Digital Identity Wallet(DIW)の定義についての情報いただきたい。電子文書に関するArticle46が重要というのはその通り。

・eIDASには、eIDに関する規定とトラストサービスに関する規定がある。eIDAS2.0が出るに当たって、欧州でeIDAS1.0が十分な法律だったのか調査が行われている。eIDについては、全体でカバーできているEU市民の割合は６割に届かなかった。eIDAS規則では、全EU市民に対してeIDを配り、皆がオンラインで色々なサービスを利用でき、その認証にeIDが使える又は国を跨いだ認証ができるようになるという目標は達成できなかった。う保証レベルのLow、Substantial、Highの基準も規則で示されていたが、その評価方法は、曖昧なまま運用が進んでいた。eIDAS2.0でEU DIWを各EU市民に配ることで、普及率100％を目指すことになっている。
トラストサービスに関しては、アンケート調査で、約70％がeIDAS規則によってトラストサービスが普及し、その結果、コスト削減、時間削減、行政手続簡略化につながる効果を実感しているという結果がある。一方、eIDAS1.0では、技術基準があくまで国家標準としての採用であって、法律と技術基準の紐付けが明確でなかったので、例えばリモートで身元確認をする要件等に国によってばらつきがあるところでは課題があった。
さらに、分散台帳、ポータブルアイデンティティーといった新たな概念が出てきており、eIDAS2.0では、トラストサービスを拡充しなければいけないことになった。
属性証明に関わる部分は、eIDAS1.0でDXに完全に資することになったわけではない。eIDAS規則が定めているトラストサービスというのは、基本的な信頼性しか保証していない。例えば、誰がそれに署名したかというレベルの信頼性のようなこと。私がある文書に署名して、eIDAS1.0が認めている領域というのは、“確かに私がその文書に署名したこと”を保証するだけ。私がどういう学位を持っていて、どういう属性の人なのかというと

ころまでは保証できていない。今回、規制産業の通信、教育産業、航空産業において、属性情報の信頼性も保証してほしいという要望があり、eIDAS2.0では、単なる自然人の保証だけではなく、属性証明という新しいトラストサービスを入れることによって、分野ごとに要求される属性情報に対する信頼性も保証しようという枠組みになっている。

eIDAS1.0は完全に成功した法律ではないものの、過半数の人が賛成していて、より時代に資するサービスを追加して、対応しようとしているということが現状。

EU DIWは、スマートフォン上のアプリとして発行されているeIDの検証結果等をアプリの中に入れ込み、それぞれがSelf-Sovereignな形で自分のアイデンティティとして、Relying Partyに対して提供できる形になっている。

・国際的にIdentificationアシュアランスレベルの議論が進んでいるのはその通りだが、日本では確実なベースレジストリーとしての戸籍や住民票、登記があるので、IALのレベルは、そういった確実なベースレジストリーとの関係がどこまでしっかりしているかを一つの考え方として示していくべき。

トラストサービスのアシュアランスレベルは非常に重要。このフォーラムでは、これまでIAL、AALなどを先行して議論しているが、IDプロバイダーだけを見ても、そこのプロバイダーがしっかりしているかどうかは、当然に重要。

アシュアランスレベルの基準を考えていく上での見方として、トラストサービスの種別によらず、共通的な要件と個々の種類のトラストサービスにおける要件を分けて洗い出していく必要がある。セキュリティで言うと、組織要件、人的要件、物理要件は恐らくトラストサービスの処理によらないで決まってくる。それに対して、技術要件に関しては共通的なものもある。この辺りをしっかり整理することが、トラストサービスのアシュアランスレベルを考えるときに重要。

機動性については、法令、告示で決めていくのはやりづらいので、規格を決めていく専門的な組織を設定して、ここで規格策定をするべき。

・eIDAS Article26について、電子文書の通用性について、電子的な形式であるというだけの理由で否定されないということが言われている。国によっては、「法令によって定められている場合を除き」と書いてある。法令によって、こういうものは紙でなければいけないと制限を加えると、この条文の意味がなくなってしまう。ここは例外がないということが重要。

・Identificationのアシュアランスレベルについて、日本国内で検討するのであれば、日本の現状に対してどう適用するべきかということを議論するべき
・初期は具体のユースケースが必要。まず行政、ガバメントセクターから実施するべき。スモールスタートをして、自分たちで物を進めていくということを鑑みて、行政の領域か

らユースケースとして具体化していくのがあるべき姿。

・トラストサービスの定義を明確にしないで話をしているところがあるので、何を指しているのか明確にして、今後、議論できるようにすべき。

・資料３について、eIDASの中で、B2Bの普及率について、どのぐらいの成功、失敗のような話があったが、eIDASだと国と国との間のことを考えがちになってしまうが、実際に民民での利用は偏りがあって、真ん中ぐらいの領域が割と使われますというようなこの辺の課題感みたいなものがあったら、教えていただきたい。
EU DIWについては、スマートフォンアプリで実装されるというお話だったのですが、時期を御存じだったら。

・B2Bに関して、統計データがない。認証局の目線からいうと、市場規模や売上げは、eIDAS以後は３倍ぐらいになっている。そのうちの大体２割から３割が適格トラストサービス。大部分は適格ではない領域での普及が進んでいることが言える。
EU DIWのスケジュール感については、欧州委員会からのオフィシャルな情報では、10月30日に欧州委員会からツールボックスと言われるEU DIWの設計案や、技術基準が示される形になっている。

・電子的な形式であるというだけの理由で否定されないということについて、例外をなくすことに対して賛成。まず行政から始めていくことに対しても賛成する。

・住所、氏名、生年月日（の開示）が前提になって本人確認をするところに違和感がある。電子契約をするときに両者が合意していることをどう相手を認証してとりもつかというITサービス企業の話を聞いたときに、相手の生年月日を聞いて、それをパスワードとして登録して、相手が自分の生年月日を入れると、そのデータをもらえるようなサービスが実際に使われていると聞いた。本人確認のために生年月日を提出しろと言っている人が、その生年月日を使って他のところにログインできてしまうというという問題が出てくると懸念する。ベースレジストリーをベースにして、マイナンバーカードを持っていることだけで、それ以外の詳細な情報は見せずとも、民間でうまく回るような認証サービスが検討できたら良い。

・足元で実際に実現していきたいユースケースは、行政の手続等を使っていけばいいが、将来的に求められるトラストのスコープだと対応ができないケースがある。データの相互運用性、B2Bのユースケース、複数企業での共同でデータを利用した共同開発を行う際のデータ利用の同意確認のユースケースまで考えていくべき。

・ユースケースで一番使われるところからスモールスタートでやることは理解できるが、ここのサブワーキンググループでは全体を網羅し、戦略的にどういうステップで進めていくかという議論とするべき。

・資料２について、DADCが提案する民民手続の分類手法は違和感がなかったが、IALのレベル分けを５段階で行っているところ、このような5段階のレベル分けを作成しているそもそもの目的への質問がある。

法的効果のような形で、例えばeIDASの枠組みで言うと、三つぐらいのレベルで取り扱うのが実務では使いやすいが、レベル分けをしたものが、最終的に法的な効果に結びつくようなことまで意図してIALのレベル分けをされているか、それとも全体的に物事を考えていく際の尺度として整備しておくと、今後の議論が非常に容易になるということでやっているのか伺いたい。

・資料３について、eIDASの下における加盟国間における相互承認のフレームワークは分かるが、今後、我が国でトラストサービスのアシュアランスレベルを考えていく場合、EUとの間で相互認証みたいなことを考えていかなければならない場合もあり得るとすると、むしろ加盟国間ではなくてEU域外の国々との相互承認が考えられ、その際に基準がどうなっているかが日本にとっては大事だと思うが、その辺りについては議論がされているのか。

例えば、UKはBrexitでEU加盟国ではなくなっているが、UKとの関係では、EUは何か相互認証的な枠組みを用意しておかなければならない状況になっているはずなので、その意味で、EU域外の国々との相互認証の枠組みは議論があってもしかるべき。

・日本はかなり確実なベースレジストリーが存在している。アメリカには戸籍はないし、印鑑証明のようなものがある国もあまりないだろうと思われる。一方、英米法では口頭のものは証拠にならないといったルール（パロール・エビデンス・ルール）等があり、その意味で、eIDASの中でArticle46の電子形式であるという理由だけで、証拠としての能力を否定されないことは理解できるが、日本だとおよそ証拠としての能力を否定されるものは存在しないので、この部分は日本に当てはめても、そのままでは議論の出発点にならない。日本で存在している確実なベースレジストリーを前提とした上で、どうなるかというところから話を進めていくのが効率的ではないか。

・５段階が適切なのかどうか、ここはまだ議論の余地がある。一方で、本人確認のレベル分けのゴールは２点あり、１点目は、自分で決められるというところ。主に確認する主体が事業者であることが多いので、現在考えている手法は、法令に手法が記載されているも

のを中心に集めております。今、民間を見渡しても、オリジナルな手法はあまりない。強いて言うなら、公的身分証をリアルタイムに所持していることを確認しながら撮影すること、後は法令に定義がある手法となっています。オリジナルが出てきていないというのはどうしてかというと、自分たちはどのレベルが必要で、どういう手法で確認すればいいのかということに対して指針がないから。そういう意味で、まず自分で決めるための足がかりに対して、材料を御提供したい。

２点目は、相互運用性。それぞれの事業者が自社のユーザーの本人確認を行うと、恐らく他の事業者に本人確認自体を頼ることもあるし、自社が本人確認したユーザーが認証連携、情報連携で他の事業者に対して連携していく世界が考えられる。そのときに、相手側にあなたはどのレベルで確認しているか、我々が要求しているレベルに合っているかが問われるようになってくる。

・相互運用性ということでいった場合、片方は電子と関係ない世界の人もいると思うので、例えば実印と印鑑証明を持っている人がいる場合、そのような人はこの中の手法でいくとどこに当てはまるのか。４／４とか、３／４とか、そういう世界なのかもしれないと思うが、DXと関係ないような形の本人確認、当人認証をされたものとの対応関係をきちんと考えておいた方がよい。実印プラス印鑑証明というような、デジタルの世界ではないものについても、この中に落とし込んでいくおつもりか。

・情報連携、認証連携を考えたときに、一旦はデジタルに写し取られるタイミングがあるのではないかと考えている。オフラインからオフラインの情報連携も考えられるかもしれない。確認したときの手法なり、そのときの材料、エビデンスというのは、アナログなものかもしれないが、それがデジタル上で確認されて、何らかの認証子を持った状態から連携が始まるケースが圧倒的に多い。そういう意味で、一旦デジタルに写し取られて、デジタル、デジタルで考えていくというのがいいのではないか。

・EU域外の件について、UKに関しては、ブレグジット以後、UKはeIDAS規則の相互承認の傘から抜けている。各加盟国の適格トラストサービスは、トラステッドリストという形で、エクセル形式で公開されている。リストはEUコミッションが管理しているリストオブトラステッドリストで管理されているのが、リスト上の最後のイギリスのトラステッドリストは、2021年１月１日付の発行になっており、１年以上前のトラステッドリストがそのまま載せられている。

ブレグジット以後、イギリスではeIDAS規則をそのまま国内法に書き写した法律を施行した。トラステッドリストとは別に、イギリスのトラステッドリストが存在します。ただ、イギリスの国内法において運用されているトラステッドリストであり、EUとのリンクが切れてしまっている。

一方で、第三国、EU域外との相互承認の枠組みについて、eIDAS1.0にはArticle14で、EU域外国との連携について、EU連合と第三国との協定をもって適格トラストサービスの相互承認を行いますと書かれています。

その際の条件が二つあり、一つ目は、第三国の適格トラストサービスが欧州の適格トラストサービスと同等の要件を充足していることが保証されていること。例えばセキュリティ要件であったり、ポリシー要件は、eIDASで定めているトラストサービスの要件と同じレベルと示すことが必要。もう一つは、第三国の国内法において認められている国内の適格トラストサービスと同等の法的効力がEUの適格トラストサービスにも与えられること。

この二つの条件を満たしていれば、イギリスの適格トラストサービスが欧州の適格トラストサービスと同等だと欧州域内でも認められると書かれている。ただ、あくまで第三国と欧州連合との協定があることが前提になる。

・国際相互認証は、必ずやデジタルトレードの関係で出てくる。個人情報保護法においても、GDPRと日本の個人情報保護法を同等レベルにして、相互連携を図った。同じ現象がこの分野でも起きるのではないか。EUとは、G to Gの関係で条約的なレベルで相互認証を結んでいかないと、国際連携できないものになるのではないか。そのときの日本の環境をどう整備していくかということを含めて、考えていかないといけない。

・日本はマイナンバーカードが配られていて、国民全員がもらえる状況にある。在留マイナンバーカードでは、電子署名用電子証明書も入っていて色々な手続きができる。ゼロから別のものを作るのではなく、マイナンバーカードを活用する視点も必要。

マイナンバーカードは、対面での引渡しということになっていることが、アシュアランスレベルのトップを担保する構造になっている。そういうところをきちんとこのグループから打ち出していく必要がある。まずマイナンバーカードがあり、その派生として利便性の高い、カジュアルに扱えるものを考えて行くべき。

スマホに信頼の起点を置くというのは危険。スマホは、買換え、紛失、壊すリスクがある。普通のデータだったら移せばいいのですけれども、耐タンパーモジュールを入れてしまうと、書き込みはできても、読み出せない。そうすると、電子証明書が全部どこかへ行ってしまうことが起きる。総務省内で公的個人認証、利用者証明書をスマホでも使えるようにするための方法の議論をしているが、マイナンバーカードから取り出せないので、利用者証明用の電子証明書は２枚、スマホ用とマイナンバーカード用と両方出す話になっている。そういうことも念頭に置きながら、現実的なほうを目指さないと、実装が難しい、又はコストが高いものが出来上がるのではないかということを懸念する。

・eIDAS Article46は、法制審議会の中で民事訴訟のIT化ということが議論されている。結局、証拠能力、訴訟の話については、民訴法から考えることなので、この場で

Article46の話を打ち出すのではなく、法制審議会の動向を見守るべきではないか。

・eIDASで、国家間で相互承認した例があったら教えていただきたい。

・レベルの話をしているが実際にレベルだけで役に立つかというと、微妙。いつ誰がどこでどうやって確認したかというメタデータを流してあげることが重要。

・Article46は、縫製審議会の専門家の議論を見守るべきかもしれないが、こういう場からも、ニーズがあるという叫びを上げていくことは必要。

・EU域外との国際相互承認は、eIDASの枠組みにおいて現時点で無い。欧州委員会の資料には、既にそういう議論が進んでいる国として幾つか挙がっている。ただ、正式なアナウンスはされていない。

・例えばレベル３で認証しましたということを送るだけでは、結局、実際にもっと細かいデータも一緒に引き渡してもらわないと受け取り側が困るというのがある。そういったところも念頭に置いておく必要がある。

・アシュアランスレベルを整理していくだけではなく、アトリビュート、受け渡し方なども含めて、非常に多岐にわたる議論をしなければ、使えるIDにならない。

ここ何か月か、スマホ搭載の実験と費用の最適化も取り組んできた。民間のユースケースで利用者証明が広がっていかない理由は、アトリビュートが取れないから。シリアルナンバーと紐づく氏名、住所の情報を取るためには、住基ネットにつなぐか自治体の住民システムにつなぐ必要がある。ところが、そこにつなげる者は限られており、デジタル庁がシステムを整備するだけでなく、住基法で認められるかというハードルがある。

昨年12月にワクチンパスポートの発行を始めたが、本来は利用者証明用電子証明書を使いたいところ、住基法においていわゆる接種証明書の発行というのは認められないので、アトリビュートが取れないため、券面入力補助アプリから12桁のマイナンバーを引き抜いて、これを当てるということをワクチンパスポートではやった。技術的にはナンセンスだが、PINの入力を１回にしたいということで、こうせざるを得なかった。

設計の際の技術的な理想と、現実の制約条件がある中でのインプリメンテーションを揃えていくのは大変なことであり、トラストにおいても、リアリティーの中で、ここをこうしてくれれば、世の中がよくなるというところをしっかりと伝えていく必要がある。当然世界の潮流、グローバル化の流れを意識して、海外との相互運用をどうしていくかということも考えていくべき。

我が国の中において、信頼できるデータの流通をやろうとしても、課題は山積。契約書

では準拠法を書くので、インターオペラブルでなくても、国の閉じた中でトラストをやり取りできないわけではないが、今後、DFFTを真剣にやっていこうとすると、流通していくデータに対して、どういうふうにトラストを確保するかを含めて、広いトラストのスコープの中で、グローバル化している現実と向かい合わなければならなくなっている。

今、デジタル臨調と絡んで世の中をデジタル化していくためにどのようにしていかなければいけないかは、重要なイシューとして、岸田政権として取り組んでいる。デジタル臨調において、しっかりとトラストの話を盛り込んでいこうとしたならば、アシュアランスレベルについても議論を深めていきながら、昨年から議論いただいていたユースケースのところにもう一回戻ってくる、あるいは我々は社会にどういうインパクトを与えなければならないのか、そういう議論に立ち返って議論することになる。引き続き御支援と闊達な議論をお願いできればと思います。よろしくお願いします。

・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８日11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