第６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25日（金）15:00-16:44

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
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「データトラストにかかわる主題とスコープ、課題の整理イメージ」、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。

・資料２において、❶（個々の取引データそのもの（中身）の信頼性に関する課題）、❷（ユーザー組織側における課題）、❸（判断やシミュレーション、AI 等にデータを二次利用する際の課題）とマップし、中央に本サブワーキンググループでのトラストサービスの範囲を書いているが、トラストサービスにおいて、❶、❷、❸のどの部分から手をつけるべきか。

・❷に該当する課題は、一定程度、❶に当たる部分もカバーされている。ここをデジタル化していくのは簡単なので、さっさとやればいい。新規にプロセスや業務を作らなくてはならないものについては、データの網羅性、正確性は重要になる。それを別個に手作業でやるとかユーザーに個別に担保させるのは辛い。法人間のデータの共有や二次利用も、ユースケースとして考えておかないと、企業側が法人として持ち得たデータをどのように、どこまで流通させていいのか、契約での規定では促進されないので、トラストで担保した上でできることが、法人間でのデータの共有の上で必要。

・❶について、信頼性を保証するのか、どうやって保証するのかということを考えると、取引データの作成者、作成するまでのプロセスに関わったモノや人、組織の属性情報、組織内の責任者の承認、公的資格保持ということをもって、受領者が、そのデータに紐づく個人や組織、装置の属性情報を検証し、リスクを受け入れる形になる。

安全試験を行う中で、試験に用いる測定器のデータの正確性について、「正確性」ではなく「不確かさ」という言葉を用いる。不確かさが十分な範囲に収まっていることを、校正を通じて保証する。これをデジタルの世界で実現しようとすると、測定器が、いつ、誰に校正された測定器か、校正を行った人が認定を取っている機関かどうかという属性情報を校正器に紐づけ、校正器から出るデータに対して、校正器のデータを受け渡していくというような形が考えられる。最終的にはそのデータの信頼は、データに関わる機器、人、組織の属性情報のセットによって保証される。その観点では、資料２の点線の四角で囲まれた領域について、現行のeIDAS1.0だったものが、欧州ではこの四角の枠が左に寄ってきている。eIDAS2.0においては、今まで、自然人、法人の実在性等にデータをひもづけることを、信頼の保証の限度としたが、属性認証という新しいトラストサービスを生んだことにより、その人が資格者なのか、財政的なバックグラウンドを持っているか、どうい

った法人に紐づいているかの属性情報まで、トラストサービスというスコープの中で提供できるようになった。データの正確性に関しては、属性情報のセット、時系列的な紐づきによって信頼されると考えて行くと、少しずつこの四角が広がってきている。

・　いよいよ検討会も終盤に入ってきて、ここで何をアウトプットとして出すのか、大事なタイミングとなった。電子署名法制定から20年近く経ち、ｅシールやタイムスタンプを実務上しっかりとやらなくてはいけない一方、制度上の位置は微妙なところもある。非常に技術進歩が早い領域において、最新の技術を適切に活用していくことを目指すにあたり、トラストアンカーの信頼性だけではなく、データの中身も含めて、DFFTまで考えたときに求められるトラストというのは、20年前と比べると相当範囲が広がっている。ぜひシステム全体、あるいは社会としてのトラストをどういう実現していけるか御検討いただきたい。

・トラストサービスにコンテンツを含まない方が良い。トラストサービスは、手続面を保証するものであり、内容の真実性はベース・レジストリが担うべき。例えば、内容証明郵便は、いつ、どこに届いたかというところだけを示すものであり、内容が正確であることは保証しない。トラストサービスというのは、内容証明郵便のようなものである。例えば、電子証明書を発行するときの認証局で身元確認をするが、これはベース・レジストリに載っているということを確認すればよい。内部処理、機器の内容をトラストで確保する場合、業種、サービス、機器ごとに基準を整備していく必要があり、共通的なトラストサービスとはならなくなるため、これがコンテンツは含まない方が良い。

トラストサービスは、第三者に対してある事実を証明するために用いられるもの。現在の電子署名法は、いわゆる「二段の推定」の一段目に相当する電子署名のデータが現実に存在したときに、そこから、電子署名と法律上言われている電子署名の処理はどのように導き出せるのかとか、そのときに電子証明書はどういう役割を果たすのかの整理が十分でない。ｅシールとかタイムスタンプについてもまだやるべきことがある。個々のトラストサービスについて、第三者に証明するという意味合いから効力を考えていく必要がある。

トラストサービスのユースケースを検討する際、GtoB、をメインにするのは疑問がある。例えば、民事訴訟法228条４項、電子署名法３条は、公文書を対象から外しているため、ユースケースとしては疑問がある。社会的にも、電子取引は広く利用されており、今後の拡大も見込まれているサービス。トラストサービスの考え方を見いだしていく上では、BtoBとかBtoCのユースケースをメインに検討するのが必要。

・中小企業が多く関わる形でユースケースを特定して、そこに必要なトラストサービスを検討していく必要がある。行政機関間のデータ交換においても、トラストサービスが使われ、行政機関Ａに保持されている個人・法人データが、行政機関Ｂでワンスオンリーの原

則等で使われるのであれば、いつ、どの行政機関によって、どういった目的で使われたのか、トラストサービスを使うことで、法的に保証される形で透明性を確保できるのではないかと考えている。

・トラストサービスアシュアランスレベル策定における課題について、トラストサービスアシュアランスレベルが構成員の間で合意が取れていないが、国の役割について、トラストサービスのアシュアランスレベルの最も高いレベルについて、国としての関わり方も色々あり得る。最高レベルに電子署名法における認定認証業務相当のものが想定されるのであれば、我が国の重要なデジタルインフラとしてトランスサービスを位置づけ、国がそのフレームワークのガバナンスに関わることが必要不可欠となる。標準の策定や監査そのものについては、民間が行うかフレームワークそのものの運営についても民間が行うモデルもあり得る。例えば、仕様の承認、監査機関の承認、フレームワークそのものを民間が運営するのであれば、フレームワークの承認等の最終的に意思決定には、国が関与すべき。

・デジタル原則においては、自動化原則を実現するために、人が介在しない部分でのトラストをどう確保するのかの議論を深めなければならない。コンテンツの中身はトラストサービスで確保しない場合、データ流通の枠組みをサービスとみなした場合、サービス、コンテンツで、データ基盤という線引きが難しくなる。

・現段階で、データの信頼性まで国の制度で固めるというのは、やり過ぎと考える。今は技術が進展する中で、市場がトライアンドエラーを行っている段階である。「国の役割」で「国が最新の仕様をメンテナンスし続け、監査する体制が確保できない可能性がある」との考えについては、監査は可能と考える。その一方で、最新の仕様をメンテナンスし続けるのが難しいケースがあるというのは指摘の通り。例えば、電子署名法では、秘密鍵を収めるICカードの規格について古い規格を引用しているままであり、このように仕様を最新に維持し続けるのは大変である。このような問題を解決するために、電気通信事業法において、電気通信事業者の役務としてドメイン名電気通信役務を追加した際に、DNSサーバの運用者に対しての技術基準を規定する際、元々国際的な水準を決める者がICANNという外国に設立されたNPOであり、その水準を省令・告示で引用することのハードルが高かったこともあり、「ドメイン名電気通信役務を提供する電気通信事業者は、その設備に関する国際的な標準に適合するように維持しなければならない」という特殊な規定をおいた。そういうやり方をすることで、最新の国際標準に合致するようなものにしていくということは、論理的には可能である。

・IALにおけるユースケースについて、マイナンバーカードの発行は、自治体職員、すなわち有資格者が対面で確認し、さらに本人性も極限まで確認した上での発行を行っている

ため、IAL3よりさらに上のレベルといえる。その結果、マイナンバーカードを持っており、マイナンバーカードが本物であるということが確認できた上で、顔写真と本人が一致することを対面でもって確認したもの、又はマイナンバーカードの電子証明書を使った署名がなされているものはIAL3に相当するということではないか。マイナンバーカードの発行ではIAL-3を超えるレベルでの本人確認を行っているからこそ、マイナンバーカードの発行以外のところでは、例えばマイナンバーカードを用いた電子署名を使って本人確認に代えるという「まえばしID」のように、全て電子にしてしまうことは可能ではないか。そうすると、本人の写真とリアルタイムの本人の画像マッチングが本当に要るのかということが一番大きな論点になる。写真とリアルタイム画像の照合が不要であれば、特殊なアプリケーションを使わなくても、マイナンバーカードの電子証明書であるということが確認でき、そのパスワードを入力できるのであれば、物件と知識で本人確認ができたとしていいのかどうか、という議論に収れんしていくのではないか。

・トラストサービスアシュアランスレベルの制定について、このレベルを、誰がどのように使うことを想定して決めるのかというところに、この委員の中もばらばらである。それが明確になると、どういうレベルがあったらいいのかという議論ができると考える。

・デジタル化に求められている要件について、紙ベースでは、本人確認のために４情報を使うことを前提に法律がつくられてきた。しかし、その方式もリスクがあり、提出先の内部犯行で、個人が本人確認のために提出した情報が不正利用されてしまう場合が散見されている。デジタル化された場合、そのリスクが大きくなる可能性があるのではないか。一方で、マイナンバーで電子化されることによって、技術的に住所を開示しなくても、本人の一意性や法人の一意性が担保できる。今までデジタル化される前に必須とされていた４情報や、法令で文書に住所と名前を記述というようなところも、デジタル庁を中心に見直していただき、プライバシーリスクも解消できるというところを目指していただきたい。

・特定のトラストサービスを強制的に利用せざるを得ない状況ではなく、利用者が幾つかのトラストサービスを選べるような状況を目指すべき。そのときに、トラストサービス自身が、トラストワージーであるということを、利用者側が検証できるようになっていると良い。それは技術を使うこともありますし、制度的に、これはトラストワージーだと思えるということがあると良い。

・現在、本サブワーキンググループで話している中身が、拡散してしまっている。トラストサービスアシュアランスレベルの基準で担保すべきものということで、現状の担保だけでなくて、将来的な担保として、ソシキ、ヒトに限らず、モノに関するものも担保することができるようにするとか、時間経過後のトラストの話も将来的には考えていかなければ

いけないため、今、トラストサービスやトラストアシュアランスレベルを考えるときに、将来こういったものに拡張していった場合の拡張性の余地を残しておくことといったことは非常に重要だが、まずは現状の担保のところの議論を固めてからにしないと、全体的に議論が収れんしないと危惧する。その観点からは、どこまでのトラストを求めるかについて、ベース・レジストリ以外の世の中にあるものについて、内容的真実性が絶対的に担保されているというものは無いように思う。トラストが人々の信頼を基礎に置いたものだということからすると、我が国は法治国家なので、最後は、裁判所に行った場合にどうなるかということに帰着する。今の日本の民事訴訟法は、基本的に成立の真正のところまでを規律するに止まっており、内容的真実性については、様々な間接証拠から裁判官が自由心証で認定していくという構造になっているので、トラストサービスを考える上でも、判断やシミュレーション、AI等にデータを二次利用する場合の課題まで含めた形でトラストサービスを議論しようとすると、あまりに広大無辺になってしまう。そういう意味では、手続的な側面に絞って、どういうものがあれば、まさにその人、その組織が、いつの時点でやったものだということが言えるかという点に絞って議論をするのが、現段階においてはいいのではないか。

・トラストアシュアランスレベルについて、現在、抽象的なところで議論しているが、電子契約プラットフォームや、運転免許の申請、パスポートの申請などの個別のユースケースを取り上げ、どこまでの技術や事業レベルがそろえば、TAL2なりTAL3なりに相当するものになるかということを議論し、それぞれにベースラインが定まれば、相当程度、民間企業や一般の人たちもイメージがつかみやすくなって、具体的なトラストサービスを使って、デジタルの世界に取引を全部移し替えるような形で、社会のデジタル化が進むのではないか。

・このサブワーキンググループのDX推進という目的から考えて、トラストサービスの普及を進めるべき。中小企業等にとって、コストが低いとか、体感としての安心安全があることが普及のポイントになる。先ほど、GtoBはユースケースとしてどうかという意見があったが、安心安全のためには、政府がやっているからというのが重要。普及を促すという点では、GtoBのユースケースは外せない。

・信ずるに値するかは最終的に受取手の人が判断するもの。こういう最高レベルのだというようにラベルがついているから信じられるというものではない。レベルが３だから、受取を強制するというのは、行政機関に対してはいいと思うが、民間にはいろいろ難しいところがある。

・トラストサービスサービスに対する要件について、継続的検証がされているものという

のが重要。自動テストがずっと行われているとか、任意の人がテストできるとか、ログがずっと取られており、それを見ることができるとか、そういった類いの継続的検証、Continuous Authenticationを要件の中に入れるべき。

・先ほど、スコープが発散していっているのではないかという話があったが、むしろ、そうではなくて、現在混在して議論されているものを分解している。例えば電子署名は、実は紙という媒体を持っている真正性、非改ざん性を担保するような性質、それから、署名と記名・捺印みたいな、発出者の真正性を推定するための性質、それから、紙は改ざんしたら分かるとか、あと、紙自身の安定性とか、そういうところに依拠する、時間経過後でも検証が割とできるとか、そういった性質を文書みたいなものは持っている。それを、我々はITの世界に入ってくると一緒に議論しがち。今言った３つの性質でのトラストは、結局最終的には鍵管理の問題に帰着しており、その鍵の検証性をどのように担保していくか、鍵がリボークされていないか、どのように発見するかという話に帰着している。なので、トラストサービスの要件といろいろ言っているが、鍵の検証性、鍵の管理性を、私たちはいろいろな側面から話しているのではないか。

・TALについて、一番上のレベルでこういう要件が必要ということを言いつつ、それを誰が認定したかだけでレベルが分かれていることが問題である。世の中のほとんどのものはこのような技術的要件を満たしている必要がない。IALについて、IAL3より上をつくるべきだということを申し上げたのと同じように、TALもほとんどのものが、よりレベルが低いTAL0でいいというメッセージを出していかないと、変な話になるのではないかなと懸念する。例えば、AAL0でも、宅配便の受取は、ドアの鍵を持っているとか、結構レベルが高い。確実性という意味で、ほとんどのものは、もっと緩いTALを設定していいということを強くメッセージしないといけない、マイナンバーカードを全国民持っているはずという建前に立ち、何でもかんでもマイナンバーカードで電子署名してくださいという世の中になってはならない。

・IALといっても、本質的には、サービスによって確認しなくてはいけない属性は異なる。Identityは属性の集合なので、サービスとして確認しなくてはいけない属性をまず決めなくてはいけない。それがどういうレベルで確認されたかという話で、鍵の所有、鍵のコントロールだけを確認すればいいサービスはたくさんある。そういったことにちゃんと配慮してやるというのが必要。世の中のかなりのサービスにおいては、こういったもの、ほとんどノーケアでもいいようなものが多い。いきなり高いレベルのものだけを許すみたいな印象を持たれると、結局広がらないおそれが強いので、そこに対しては十分配慮する必要がある。誰がやったかというのだけで判断されるみたいな印象を持たれるような書き方も戒めるべき。

・少なくとも今回のサブワーキンググループで自分たちが議論しているスコープは決めなくてはいけない。第２層のところに限定する、加えて属性に関する保証も入れていくというところで、資料２の真ん中の四角の領域に加えて、属性を入れていくことに賛成と表明する。

・トラストサービス事業者が備えるべき要件について、UNCITRALとの関係でProvisions on the Use and Cross-border Recognition of Identity Management and Trust Servicesの草案が出ていて、ずっとこれについてUNCITRALで議論をされているが、これが将来、モデル法になることが想定されている。この草案の中では、23条に、トラストサービスの信頼性判断の要件が列挙されている。このUNCITRALにおけるトラストサービスの信頼性判断の要件として挙げられているものでは、組織要件、監査要件に関係するものが多く、業務規程、ポリシー、国際基準、手続、業界標準、ハードウエア、ソフトウエアのセキュリティ、財務的、人的資源、それから、独立主体による監査、監督主体や認可主体などによる信頼性に関する言明等々である。UNCITRAL草案の23条に出てくるような要素は、いずれ国際的にトラストサービスについて相互に認証していくような場合に、トラストサービス事業者の信頼性との関係で出てくるはずなので、これを念頭に置いた議論をすべきである。

・トラストは内容的真正性と手続的真正性の両面がある。内容的真正性については、このサブワーキンググループで検討するのは非常に広い範囲になり、ある意味アプリケーションに依存してくる話になる。このサブワーキンググループで手続的真正性のスコープが見えてくれば、後はどういう順番で検討していくかという方法論の話となる。その中で、電子契約、運転免許証、パスポートなどのユースケースを検討しながら、実際に、具体的なところへ落とすとすればアシュアランスレベルというものを見ていくことになる。さらにそこから基準というものを見ていく、というようなステップを踏んでやっていくということではないか。この検討会の６月までであり、全てをやり切れるかは難しいのではないか。事務局で、本サブワーキンググループのスコープと今後の進め方、スケジュールを整理していただきたい。

・データの真正性そのものを扱うかどうかは、相当難しい議論である。このサブワーキンググループは、デジタル庁において、DFFTの“T(Trust)”の部分を担うものであるため、そこに対する一定の答えを示していく必要がある。もともとこの会議では、ユースケースにフォーカスをしていた。実社会のユースケースにおいては、詳細の技術基準だけでトラストを実現するのではなく、コンテクストを踏まえて、中身とやり取りの中で、信頼を確保しているものもある。そうすると、中身を見ることが難しいか簡単かということではな

く、トラストを実現していくために全てをかっちり決めたほうが実現しやすいのか、それとも、中身に踏み込んだほうがやりやすいこともあるのかという問題に帰着する。実際には、アプリケーションまで見ると様々な範囲で社会のトラストが実現されているということと、どのように折り合いをつけていくのかを考えていく必要がある。専門家がきちんと技術的に詰めていくということも大事だが、社会から受け入れられるものにしていくためには、消費者とか事業者も巻き込んで議論をしていくということが大事だとも各方面からご指摘いただいている。

これまで20年、様々なことをやっていく中で、e-Japanのときの電子署名法の取組、2010年のオンライン手続のための電子認証ガイドラインは、どちらかというと、アメリカのNISTSP800-63に近いようなアプローチだった。隗より始めよという意味で、国としてどういう立場でこれをやるのかというところで、たまたまアメリカ型のアプローチだったという部分もある。一方、欧州のようにレギュレーションとして整備をしていくというやり方もある。それぞれ様々な面があって、異なる背景の中で必要性に基づいて行われてきたことなので、EUのQualified signatureがどのように使われているかや、eIDAS2.0のDigital Identity walletでどういうことを考えているのか、SP800-63-4のドラフトの議論にもキャッチアップしながら、国として何をやらなくてはいけないのかということをデジタル庁として考えていくタイミングになっている。非常に短い期間で広範にわたることを議論いただいているため、６月までに細かい基準まで作れるか厳しいところではあるが、デジタル庁が始まってから、年末に重点計画を出しているとは言え、実質的に最初の結果がこの夏に結実をしていくので、ぜひ５年、10年の指針となるようなレールを敷けていければと考えているので、引き続き宜しくお願いしたい。

・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３月22日(火)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