

**プラットフォームサービスに関する研究会
トラストサービス検討ワーキンググループ
中間取りまとめ(案)**

令和元年6月 24 日

**プラットフォームサービスに関する研究会
トラストサービス検討ワーキンググループ**

目次

はじめに	1
第1章 トラストサービスとは	2
第2章 諸外国におけるトラストサービスの動向	5
第3章 我が国におけるデジタル化に関する政策の概要	8
第4章 個別論点と取組の方向性.....	10
4. 1 リモート署名について	11
4. 2 組織を対象とする認証について	13
4. 3 ウェブサイト認証について.....	16
4. 4 モノの正当性を確認する仕組みについて	18
4. 5 タイムスタンプについて	19
4. 6 データの送達等を保証する仕組みについて	22
おわりに.....	24

はじめに

データは、「21 世紀の石油」とも言われるように、その利活用が国の在り方とその発展に大きな影響を与えることとなり、イノベーションの源泉にもなる。

これまで、人がサイバー空間に存在するデータベースから情報やデータを入手し、分析を行い、「人間が情報を解析すること」で社会的な価値が生まれてきたが、サイバー空間と実空間の高度な融合により、経済発展と社会的課題の解決を両立する Society 5.0 においては、実空間にあるセンサーなどから大量のデータがビッグデータとして収集され、収集されたビッグデータを人工知能 (AI) により解析し、実空間に高付加価値をフィードバックすることで、生活の利便性の向上や産業の高度化を実現することが期待されている。

様々なヒト・組織・モノから発せられ、Society 5.0 の循環の基となるデータを、AI の分析精度向上や様々な領域での活用により新たな価値を生み出すためには、データの量もさることながら質も重要であり、データの有効性を担保するための基盤として、ネット利用者の本人確認やデータの改ざん防止等の仕組みであるトラストサービスが必要不可欠となる。

本ワーキンググループは、「プラットフォームサービスに関する研究会」の下に設置され、我が国におけるトラストサービスの現状と課題を整理し、課題を解決するための方策について検討を行い、今般、これまでの事業者ヒアリングや構成員の意見等を踏まえ、取り組むべき事項の全体像を中間取りまとめとして整理した。

本中間取りまとめをもとに、トラストサービスの重要性について、トラストサービスプロバイダーやシステムベンダーだけでなく、トラストサービスを利用するユーザ企業や個人にも理解や普及が進み、データを安心・安全に、自由に活用できる社会的基盤が構築されることを期待してやまない。

第1章 トラストサービスとは

Society5.0の実現に向けて、サイバー空間と実空間の一体化が進展し、社会全体のデジタル化を進める中、その有効性を担保する基盤として、ネット利用者の本人確認やデータの改ざん防止等の仕組みであるトラストサービスが必要となる。トラストサービスの重要性が高まる背景として、次の二つがあげられる。

(1) 実空間からサイバー空間へ

情報通信技術が急速に進展し、少子高齢化などといった社会課題の迅速かつ柔軟な解決や持続的な経済成長を実現するためには、社会全体のデジタル化を急速に進め、より効率的な社会を実現することが必要不可欠である。

本年、「情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るための行政手続等における情報通信の技術の利用に関する法律等の一部を改正する法律」(令和元年法律第16号。以下「デジタル手続法」という。)が成立し、これまでオンライン化に関して国の行政機関等に認めていた裁量を排除¹して、原則として手続のオンライン化を国の行政機関等に義務付けられることとなった。

デジタル手続法を契機として、現在、実空間において対面や紙を通じて行っているやりとりが、今後サイバー空間においてますます電子的なやりとりに置き換わり、地方・民間を含めた「社会全体のデジタル化」が進展することが想定され、その基盤として、電子データの信頼性の確保が必要となる。

(2) 組織やモノからの情報発信の増大

Society5.0においては、センサーを始めとする様々なモノがネットワークにつながり、これまで人を介在して行われていたデータのやりとりが、モノとモノとの間で自動的に行われるといったこれまでにない形態でデータが流通することとなる。

そのため、正当でないモノがネットワークにつながることや、誤ったデータや改ざんされたデータが紛れ込まないようにデータの真正性を確保した上でデータを流通させる必要があり、ヒトだけではなく、組織やモノの正当性、また、それらから発信されるデータの完全性を確認

¹ 2002年に成立した「行政手続等における情報通信の技術の利用に関する法律(平成14年法律第151号)」においては、行政のオンライン化は義務規定ではなく(「できる規定」)、オンライン化の対象手続は各府省が判断を行うなど一定の裁量を認めていた。

できる仕組みの構築が必要となる。

Society5.0 に向けて、トラストサービスの基盤を活用することが考えられる例として、情報銀行²が挙げられる。情報銀行による個人に向けたサービスが適切に行われるには、各関係者の正当性の確認や、データ流通の過程において改ざん等が行われていないかを担保するデータの完全性の確保が重要となる。

このような社会的背景から、本ワーキンググループの検討に当たって、以下の仕組みについて取り上げた。(図1)

- ① 電子データを作成した本人として、ヒトの正当性を確認できる仕組み(電子署名)
- ② 電子データを発行した法人として、組織の正当性を確認できる仕組み(組織を対象とする認証、ウェブサイト認証)
- ③ IoT³時代における各種センサーから送信されるデータのなりすまし防止等のため、モノの正当性を確認できる仕組み
- ④ 電子データがある時刻に存在し、その時刻以降に当該データが改ざんされていないことを証明する仕組み(タイムスタンプ)
- ⑤ 送信・受信の正当性や送受信されるデータの完全性の確保を実現する仕組み

² 個人とのデータ活用に関する契約等に基づき、パーソナルデータストア (PDS) 等のシステムを活用して個人のデータを管理するとともに、個人の指示又は予め指定した条件に基づき個人に代わり妥当性を判断の上(または、提供の可否について個別に個人の確認を得る場合もある。)、データを第三者(他の事業者)に提供する事業(データの提供・活用に関する便益は、データ活ユーザーから直接的又は間接的に本人に還元される)。

³ Internet of Things の略。「様々な物がインターネットにつながること」「インターネットにつながる様々な物」を指す。

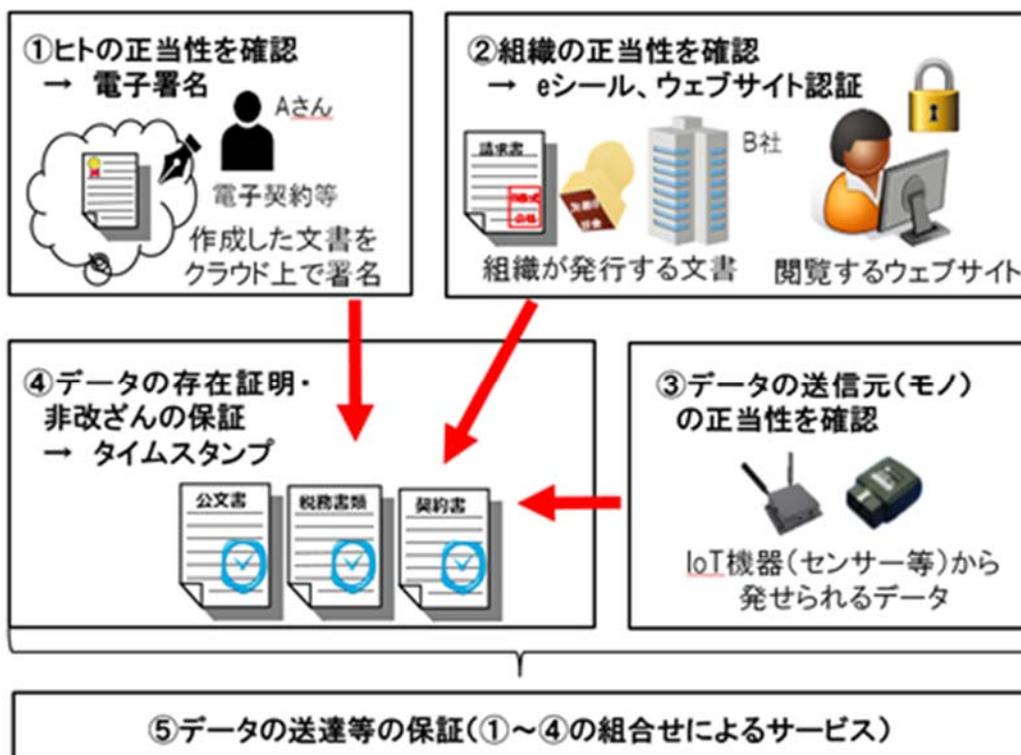


図1 トラストサービスのイメージ

これらトラストサービスに関する課題が整理され、トラストサービスの全部又は一部を多数の事業者等が公平公正に提供することが可能な環境を整備することにより、一部のプラットフォーム事業者がトラストサービスを寡占することなく、健全な市場環境の構築に資することが期待される。

第2章 諸外国におけるトラストサービスの動向

EU は、eIDAS (electronic Identification and Authentication Services) 規則を 2016 年7月に発効した。eIDAS 規則では、一定の要件を満たすトラストサービスの提供者を適格トラストサービスプロバイダーとして規定し、EU 各国はトラストリスト(適格トラストサービスプロバイダーのリスト) (図2)を公開、維持しなければならないとされている。また、eIDAS 規則では、トラストサービス事業者の適合性(技術、運用)を評価・監査する枠組みが規定されている。2019 年1月時点で、EU28 ヶ国において 169 の適格トラスト・プロバイダーが存在しており、EU では、eIDAS 規則の発効以降、トラストサービスの利用が拡大している。

eIDAS 規則には、以下の法的枠組みが規定されている。(図3)

- ① 電子署名(自然人が電磁的に記録した情報について、その自然人が作成したことを示すもの)
- ② タイムスタンプ(電子データが、ある時刻に存在していたこととその時刻以降に改ざんされていないことを示すもの)
- ③ ウェブサイト認証(ウェブサイトが真正で正当な主体により管理されていることを保証するもの)
- ④ e シール(文書の起源と完全性の確実性を保証し、電子文書等が法人によって発行されたことを示すもの)
- ⑤ e デリバリー(データの送受信の証明も含め、データ送信の取扱いに関する証拠を提供するもの)

Web 掲載について確認中

図2 EUにおけるトラストリストの例⁴

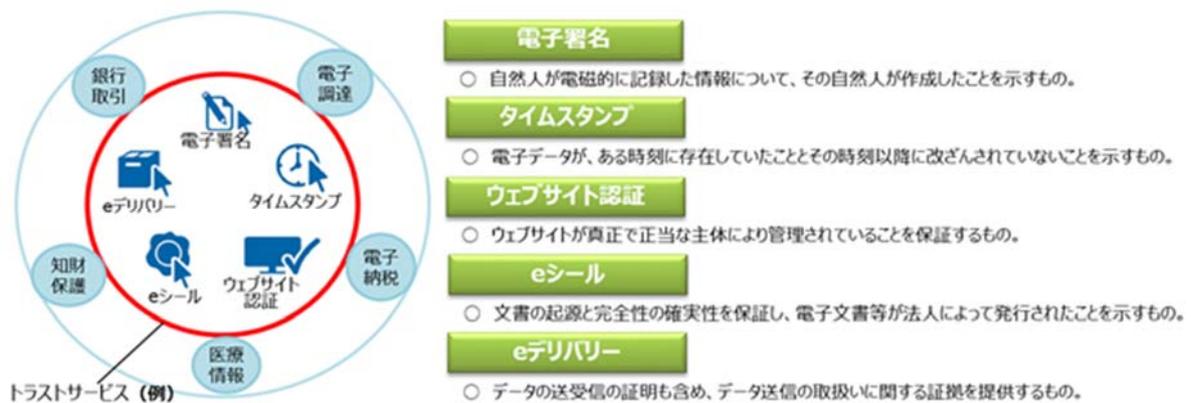


図3 EUにおけるトラストサービスのイメージ⁵

⁴ 各国のトラストサービスプロバイダーが一覧化されている。

<https://helpx.adobe.com/document-cloud/kb/european-union-trust-lists.html>

⁵ ENISA 公表資料をもとに総務省作成。

<https://www.enisa.europa.eu/news/enisa-news/a-digital-europe-built-on-trust>

例えば、エストニアでは、同国の電子政府システムを支える多数のシステムを結ぶ共通システム間連携基盤「X-Road」において、各システム間のデータ送受時に、e シールやタイムスタンプ等のトラストサービスが利用されている。具体的には、政府のデータベースにアクセスして医療記録を確認するときや電子処方箋を入手するとき、税金の申告をするとき、水道・電気等の公共インフラサービスにおいて電子契約を行うときなどに、トラストサービスが利用されている。X-Road には、2019 年1月時点で、2,691 のサービスが接続され、接続事業者数は 1,155 者(民間:651 者、公的機関:504 者)あり、月に1億件程度のアクセスがある。

さらに、PSD2(Revised Payment Services Directive:決済サービス指令)において、決済サービス提供者が金融機関にアクセスする際、適格 e シール等を用いることが求められているなど、eIDAS 規則を適用する法律があることで、デジタル化の推進が図られている。

他方、我が国においては、電子署名及び認証業務に関する法律(平成 12 年法律第 102 号。以下「電子署名法」という。)により電子署名が手書きの署名や押印と同等に通用する法的基盤が整備されているものの、タイムスタンプについては、(一財)日本データ通信協会による民間認定スキーム(タイムビジネス信頼・安心認定制度)が存在するにとどまるほか、他のトラストサービスについては制度的な位置付けがなく、国際的な相互運用性の観点からも、我が国としてのトラストサービスの在り方について検討が必要である。

また、データを国外とやりとりする国民や企業等が、国外での訴訟等においてその真正性や完全性を主張する場面など、国民や企業等が国外での権利実現を図る基盤としても、我が国における法制度に基づくトラストサービスの構築が期待されている。

第3章 我が国におけるデジタル化に関する政策の概要

急速な少子化・人口減少等の我が国が抱える諸課題に対処すべく、データ流通を前提としたデジタル社会を実現することによる社会全体の生産性の向上をさせることを目的とし、2016年に官民データ活用推進基本法(平成28年法律第103号)が制定され、同法において、①行政手続をオンラインにより行うことを原則とするよう国が必要な措置を講ずること、②民間事業者が行う契約の申込みその他の手続をオンラインにより行うことを促進するよう国が必要な措置を講ずることが定められた。

さらに、同法の規定を受け、本年、情報通信技術を活用した行政の推進に関する基本原則及び行政手続を原則としてオンラインにより行うこととするための共通する事項、民間手続のオンライン化の促進に関する施策等を定めたデジタル手続法が成立し、行政手続に係る関係者の利便性の向上、行政運営の簡素化及び効率化並びに社会経済活動の更なる円滑化を図ることで、行政手続のデジタル化が徹底されることとなった。

一方で、民間手続におけるデジタル化については、電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律(平成10年法律第25号。以下「電子帳簿保存法」という。)や、e-文書法(「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律(平成16年法律第149号)」と「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律(平成16年法律第150号)」2法の総称)等により、法令の規定により民間事業者等が行う書面の保存等の手続について、原則全て電子的に行うことが可能となったが、これらの法律の施行から10年以上経過している中、一部民間手続で電子化が進展しているものの、電子データの長期保存に係る信用力を担保する仕組みがないため、保存が義務付けられている書類については、電子媒体と併せて紙で保存されている実態があるなど、書面の作成から保存まで一貫して電子化されていないこと等が課題となっている。

また、電子署名法に基づく認定認証事業者から発行された電子証明書についても、年間35万枚程度の推移にとどまっている。(図4)

以上のことから、民間も含めた社会全体のデジタル化を推進するためには、民間における文書の電子保存の状況等を含めた法律の施行状況を検証し、トラストサービスの活用も含めて、必要な措置を講じることが必要となっている。

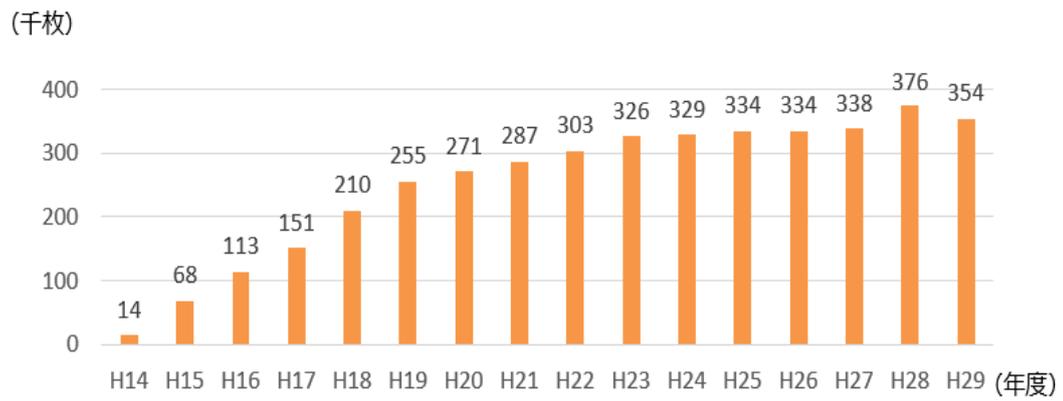


図4 電子署名法に基づく認定認証事業者から発行された電子証明書(有効枚数)

第4章 個別論点と取組の方向性

Society5.0 の実現に際しては、データの起源について(1)誰からのデータであることを保証するヒトを対象にする認証、(2)組織が発行したデータであることを保証する組織を対象とする認証、(3)ネットワークにつながる IoT 機器等のモノからのデータであることを保証するモノの認証の在り方について検討が必要である。こうした認証を行うことは、認証されたヒト、組織やモノがどのようなデータにアクセス可能か、データへの認可をサービスごとに変えることができる仕組みの実現に寄与する。

また、大量のデータが流通する Society5.0 において、データの利用価値を高めるためには、完全性の観点も重要であり、データの存在証明・非改ざん証明の仕組みについての検討が必要である。

さらに、これらの情報の起源や完全性を組み合わせた仕組みや、電子的に長期保存されたデータの真正性を確保できる検証サービスについても検討が必要である。

こうした視点に基づき、本ワーキンググループでは、次の検討事項ごとに課題を整理した。

検討事項1 ヒトの正当性を確認できる仕組み(電子署名)

電子署名については、電子署名法が整備されているものの、クラウド等を活用したりリモート署名など最新の技術に制度が十分に対応しきれていない部分があるため、技術・制度の両面から、対応の方向について検討を行う。

検討事項2 組織の正当性を確認できる仕組み

(1) 組織を対象とする認証(e シール)

請求書、領収書等の企業が発行する文書等に対し、電子的にその企業が発行したことを簡便に保証する仕組みがないことから、その在り方について検討を行う。

(2) ウェブサイト認証

CA/ブラウザフォーラムの定める基準がデファクトスタンダード化していることにより生じている課題への対応について、検討を行う。

検討事項3 IoT 機器等のモノの正当性を確認できる仕組み

IoT 化がますます進展する中、モノのなりすましやデータの改ざん等を防止するため、モノの正当性について検討を行う。

検討事項4 データの存在証明・非改ざんの保証の仕組み(タイムスタンプ)

(一財)日本データ通信協会による民間の認定スキームが存在する中、今後、タイムスタンプの更なる利用拡大に向けて、検討を行う。

検討事項5 データの送達等を保証する仕組み

EU の e デリバリーに相当するような、トラストサービスを利用した新たなサービス創出に向けて、検討を行う。

なお、これらの検討に当たっては、以下の事項に配慮する。

- ・ トラストサービスの仕組みについて、技術的な基準、法律による規制、トラストサービス提供事業者に対する評価・検証体制の確保といった三つの観点から検討する必要がある。
- ・ トラストサービスの実現に当たっては、サイバーセキュリティの三要素である機密性、完全性ととも、利用者が簡便に利用できるような可用性を確保する必要がある。
- ・ 技術革新のスピードに鑑み、最新の技術動向を踏まえつつも、特定の技術に依拠することなく、要件志向で検討する必要がある。
- ・ 技術的な堅牢さや強度だけを追求するのではなく、利用者にとって使いやすいインターフェースやプライバシーデザインにも配慮する必要がある。
- ・ トラストサービスを提供する事業者や利用者にとって過度なコスト負担や不便を強いることが無いようにする必要がある。
- ・ これからの国際的なデータ流通を見据え、EU の eIDAS 規則等との国際的な相互運用性に留意する必要がある。

4.1 リモート署名について

(1) 現状

事業者のサーバに利用者の署名鍵を設置・保管し、利用者がサーバにリモートでログインした上で自らの署名鍵で事業者のサーバ上で電子署名を行うリモート署名については、一定のネットワーク環境があれば、端末を選ばずに電子署名ができるようになるという利便性向上に加え、IC カードの紛失等のリスクが無くなる等のメリットから、利用拡大が期待されているが、電子契約において、契約者が署名をする場合、現状では主に IC カードを用いており、IC カードや端末がある場所でないとう電子署名が行えない状態となっている。

EU では、安全なリモート署名に関する規格や評価制度等も含めて規定され、リモート署名が広く利用されており、例えば、オーストリアでは、2004 年から電子政府に取り組んでお

り、同年の電子政府法⁶で適格電子署名という概念を取り入れ、2009年にリモート署名にも取り組んだ。現在、同国には120万人の適格リモート署名のアクティブユーザが存在している。これはICカードベースの適格電子署名のアクティブユーザ(10万人)の約12倍であり、同国の人口800万人と比しても相当な数と言え、電子手続におけるトラストサービスの進展が見受けられる⁷。

(2) 課題

【課題1】制度的な位置づけが明確ではない

クラウド等を介するリモート署名が本人によるものであることが技術的に担保される場合において、電子署名法第3条⁸に基づく「本人による電子署名」であると言えるか、制度的な位置づけが明確ではない。

【課題2】セキュリティ確保等の技術的な要件が整理されていない

リモート署名サーバの中に格納した本人の秘密鍵を使用する際のアクセス方法についてどのような要件を満たせば、クラウド等を介しても本人による電子署名と言えるのか、技術的な基準が整理されていない。

我が国においてリモート署名のシステムを実装するに当たっては、

- ・ 重要な鍵ペアの安全な管理・利用シーン
- ・ 保証レベルの考え方を踏まえた本人確認の仕組み

など、セキュリティ確保の観点から、顧客に安全性を納得してもらえるレベルの基準策定が必要である。

(3) 構成員からの主な意見

(ア) 一番重要な点は、リモート署名で署名した場合に電子署名法第3条の推定効が働くかという点。「本人による電子署名(符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。)」というところが最大のポイント。

(イ) リモート署名の法律上の課題について、いわゆる二段の推定のうち、一段目の推定

⁶ オーストリア電子政府法

https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2004_I_10/BGBLA_2004_I_10.html

⁷ トラストサービス推進フォーラムによる、A-Trust社へのヒアリング結果に基づく。

⁸ 電子署名法第3条:電磁的記録であって情報を表すために作成されたもの(公務員が職務上作成したものを除く。)は、当該電磁的記録に記録された情報について本人による電子署名(符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。)が行われているときは、真正に成立したものと推定する。

をどのように考えるかが問題。制度的に保障された署名サーバで作成されたことが検証できれば、真正な成立を示すことができる。

(ウ) リモート署名のシステムを実装するに当たっては、本人確認について、保証レベルの考え方を踏まえることが非常に重要であり、セキュリティ確保の観点から何らかの基準が必要。

(エ) リモート署名で重要な論点は、リモート署名サーバの中に格納した本人の秘密鍵にいかにかアクセスするかという点。技術的な水準がどうあるべきかについて JT2A で検討されている。

(オ) リモート署名を使うことで、例えばスマートフォンからの署名にも対応できるようになれば、ビジネスの迅速性が担保できる。

(4) 取組の方向性

クラウド等を介するリモート署名におけるアクセス方法の技術基準については、経済産業省の電子署名法研究会(平成 27 年 12 月～平成 29 年 3 月)での検討を踏まえ、トラストサービスに係る技術関連のガイドライン策定などを行っている日本トラストテクノロジー協議会(JT2A)において議論をしているところであり、当該議論も注視しつつ、並行してリモート署名の電子署名法上の扱いについて、主務省庁において整理することが必要である。

その上で、リモート署名について、特定認証業務と認定認証業務に係る基準の具体化を進めることが必要である。

また、後述する組織を対象とする認証についても、技術的にはクラウド等を活用して署名で行うことが可能であり、組織を対象とする認証の議論も踏まえながら、引き続き、検討を進めていくことが必要である。

4.2 組織を対象とする認証について

(1) 現状

法人が行う契約や申請において、法人代表者や法人代表者から委任された担当者が意思表示をする場合には、実空間では代表印(丸印)や個人印の押印、電子的には電子署名を利用しており、後者については、電子署名法や電子委任状の普及の促進に関する法律(平成 29 年法律第 64 号)といった法制度が整備済であるが、法人が発行する請求書や領収書等の書類については、実空間では社印(角印)で済ませているところ、電子的には組織を対象として認証する仕組みがない。

EU では、組織が発行する電子データについて、eIDAS 規則において当該電子データの

完全性と起源を保証するものとして e シールの法的な効力が認められている。

(2) 課題

【課題1】組織が行う実空間でのやりとりが、サイバー空間では簡便に実現できていない

法人を発行の起源とする文書の真正性を電子的に担保する法的枠組みがないため、法人が発行する請求書や領収書等の書類についても、法人代表者又は法人代表者から委任された担当者の電子署名で処理している場合が多い。このため、

- ・ 受取側にとっては、発行側の担当者の異動、退職後に請求書等の有効性の確認に手間が生じる
- ・ 発行側にとっては、担当者の異動、退職時に電子署名の電子証明書を改めて発行する必要がある
- ・ 書類ごとに自然人による意思表示を示す電子署名は、機械的な大量処理に向かないといった課題が存在する。

【課題2】業務の効率化が十分に進んでいない

法人が発行した請求書や領収書等については、機械発行したものに対して自動的に e シールを付す処理が効率的であるが、我が国においては、紙で発行された請求書や領収書等をスキャナ等により電子化し、保存する形態にとどまっており、電子化のメリットが十分に発揮できていない。

他方、EU では、エストニアにおいて電子処方箋や従業員登記などのサービスを中心に e シールの利用が拡大しているほか、EU 全体としても、決済サービス指令(PSD2)において、金融機関等の決済サービス業者が提供するサービスの決済データを対象に、e シールの利用が義務化されていることから、利用が拡大している。

我が国でも、2023 年 10 月に、軽減税率導入に伴う「適格請求書保存方式」(インボイス制度)の導入が予定されており、仕入額の控除に当たっては、税務署に登録された適格請求書発行事業者が発行した請求書等を保存することが要件とされているところ、仕入れ先が多岐にわたる場合、適格請求書発行事業者の発行した請求書等を個別に確認する事務作業が膨大に発生することが想定される。

適格請求書(インボイス)の電子化と併せて、e シールを活用し、インボイスの真正性を確保しつつ、適格請求書発行事業者であるかを属性として電子的に記載することで、突合、検索、計算などが自動処理可能となり、大幅なコスト削減、効率的で正確な税務処理や納

税手続等の実現が期待されている。

(参考)消費税に係るインボイス制度

消費税法(昭和 63 年法律第 108 号)改正(2016 年 4 月)により消費税の軽減税率制度が 2019 年 10 月から開始されること、複数税率(標準税率 10%、軽減税率 8%)の下で適正な課税を確保する仕組み(仕入れ税額控除の方式)として、2023 年 10 月から適格請求書保存方式(いわゆるインボイス制度)が実施される。

適格請求書とは「売手が買手に対し正確な適用税率や消費税額等を伝えるための手段」であり、一定の事項(取引年月日、消費税率、軽減税率の対象品目である旨等)が記載された書類のこと。

【課題3】 Society5.0 に向けた対応が求められる

現行、パソコンやスマートフォンのアップデートプログラムにコード署名⁹が付されている場合は、OS やブラウザにより検証が実施されているが、Society5.0 時代においては、様々な機器がインターネットに接続される IoT 化が進展することとなり、例えば、これら機器のプログラムをアップデートする場合、コード署名について一般的な OS やブラウザによらない検証が増加すると予測されていることから、そのような際の検証方法について検討が必要である。

また、プログラムをアップデートする際、真正性を確認するに当たっては、自然人の電子証明書を利用した場合、担当者ごとに電子証明書を管理する必要があり、管理コストが高くなることから、組織・法人を対象とする電子証明書を発行するニーズが高まっている。

(3) 構成員からの主な意見

- (ア) ヒトに紐付かない証明書であれば、法人の確認だけで済むため、簡単に審査ができ、コストも低下するため、個人に結びつかなくても成立する領収書の場合、安く証明書を発行することが可能となる。領収書は、機械発行したものに対して自動的に署名がされるような運用が望まれるため、電子署名だとオーバースペックである。
- (イ) 大量に発行する文書に対して使用できることも eシールの大きな魅力。eシールが使えるようになると、電子文書の流通が非常に多くなることが期待されることから、制度化し、経済の発展につなげていくべき。
- (ウ) 訴訟になった場合、社印(角印)だけをもって、会社の文書の成立の真正が認められるかが争点になるだろう。どのようにその文書が作られたかといった周辺の様々な

⁹ プログラムが第三者によって変更されたり改ざんされたりしていないことを証明するために付される署名のこと。

事情も含めて、真正な成立の有無が検討されることになるのだろうと考えられる。

- (エ) eIDAS 規則の前後で大きく利用が伸びているユースケースの一つが、電子インボイスにおけるeシールの活用という分野であり、法的根拠が何も規定されていなかったことが、利用が広まらなかった大きな原因と考えられる。

(4) 取組の方向性

eシールは、請求書・領収書等の企業が発行する文書等の電子化を促進するとともに、従来紙でやりとりしていたデータを機械判読化し自動処理することで、生産性の大幅な向上に寄与することが期待される。

そのため、EUにおいて利用が拡大している実態や今後の我が国における消費税に係るインボイス制度の導入、さらに、Society5.0時代を見据えて、ユーザ企業側のニーズやユースケースを明確化した上で、どのような枠組みでeシールに係るサービスが提供されれば、利用者が安心して利用できるか、制度化も視野に入れて、検討を深めていくことが必要である。

4.3 ウェブサイト認証について

(1) 現状

利用者がウェブサイトを開覧する際、ウェブブラウザでサーバ証明書を確認することにより、そのウェブサイトが正当な企業等により開設されたものであるかどうかを確認することができるウェブサイト認証という仕組みが利用されている。

そのウェブサイト認証のための電子証明書を発行する認証事業者に求められる基準については、認証事業者と米国のウェブブラウザベンダ等からなる団体であるCA/ブラウザフォーラムが定める要件がデファクトスタンダード化されており、当該要件を満たすと認められなくなると、必ずしも直ちにセキュリティ上問題がない場合であっても、ウェブブラウザ上、安全ではないサイトと表示されるおそれがある。

EUでは、eIDAS規則に基づき、一定の要件を満たした適格な認証事業者を公的にリスト化し、当該認証事業者については米国ブラウザベンダに対して安全なものと認めもらえるよう、CA/ブラウザフォーラムに積極的に働きかけを行っている。

また、中国では、独自ブラウザや独自トラストリストを開発し、米国のウェブブラウザベンダに依存しない体制を構築中である。

(2) 課題

CA/ブラウザフォーラムへの関与について検討が必要

CA/ブラウザフォーラムのガイドラインを踏まえ、ブラウザベンダは認証事業者に対して、セキュリティの確保の観点から、

- ・ ポリシーの変更等への迅速な対応
- ・ 認証事業者の運用体制等の透明性の確保
- ・ なりすまし防止等のための証明書発行における確認事項の厳格性の確保

などを要求しており、認証事業者は一方的に求められるそれらの要求に随時対応しなければならず、利用者にとっても短期間で証明書を切り替える必要があるなど、各種コストを要している。

また、法人名の日本語表記は海外の人には読めない、登記簿には英字表記は存在しないなど、日本独自の仕様が CA/ブラウザフォーラムに認められないことがある。そのため、日本の特殊な事情を表明していくことが求められる。

CA/ブラウザフォーラムの運営に積極的に参画しているEUの活動を参考にしつつ、我が国としてもトラストリスト策定に関する検討や、CA/ブラウザフォーラムのガバナンスに戦略的に関与していくことが必要である。

(3) 構成員からの主な意見

- (ア) CA/ブラウザフォーラムなど、積極的に関わることも検討すべき。その場合は、独自の認定基準及び独自トラストリストを作成し、これまで CA/ブラウザフォーラムに関与してきた ETSI(欧州電気通信標準化機構)の活動が参考になる。
- (イ) 国税庁の法人番号の英語表記登録を参照することも含めて制度化を考えることが必要。また、CA/ブラウザフォーラムのガバナンスに積極的に参加し、日本の特殊な事情を表明していくべき。
- (ウ) ウェブサイト認証について CA/ブラウザフォーラムという民間団体の実施基準のみに則って我が国として進めていくか、国として公的なルールを作った上でCA/ブラウザフォーラムと連携するかは、大きな論点。

(4) 取組の方向性

ウェブサイト認証については、CA/ブラウザフォーラムが定める基準に基づき、世界各国で普及しているが、CA/ブラウザフォーラムが定める要件への対応について、日本固有の事情に応じた必要な対策を TSF(トラストサービス推進フォーラム)などにおいて検討・整

理・集約した上で、CA／ブラウザフォーラムのガバナンスに戦略的に関与していくことが必要である。

EU の動向等も踏まえ、我が国としてのウェブサイト認証に関するトラストリスト策定の要否や在り方等について、更に検討を行うことが適当である。

4.4 モノの正当性を確認する仕組みについて

(1) 現状

IoT 機器は幾何級数的に増加しており、民間の調査会社によると、2017 年時点の世界中の IoT 機器は約 275 億個、2020 年には約 400 億個まで増加すると予測されている。2017 年時点ではスマートフォンなどの通信機器が多くを占めているが、今後は自動車・輸送機器分野、医療分野、産業分野で IoT 機器が急速に普及することが見込まれている。

また、IoT 機器の稼働状況などから大量のデータが蓄積され、AI によるビッグデータ解析を活用することで、より高密度のデータの収集・蓄積・解析を通じて社会課題の解決につなげていく Society5.0 においては、モノから発信されるデータの流通量がグローバル規模で飛躍的に増大することとなる。

(2) 課題

【課題1】実装に当たって、機能的制約やコスト面の課題がある

センサーなどの小さな IoT 機器(チップ)に PKI の仕組みを導入することには機能的な制約があるほか、PKI の仕組みを IoT 機器に導入するに当たってのコストも踏まえ、費用対効果の観点からも対象とする機器についての検討が必要である。

【課題2】認証単位等について更なる検討が必要

モノの認証については、ヒトや組織の認証と違い、様々な単位(機器ごとか、製造ロットごとか等)で行うことが考えられ、それぞれの利用実態に応じて柔軟に対応できる仕組みが必要である。

また、IoT 機器の廃棄に関して、データの出所を後で追跡や検証する際には検証用の鍵が必要となるため、廃棄の際の鍵の扱いなどについても検討が必要である。

(3) 構成員からの主な意見

- (ア) PKI を使うのは重いのではないか。ID ベース暗号といった、より軽い方法があるのではないか。
- (イ) コスト面は、アプリケーションとの関係で様々な見方があるため、本ワーキンググループで議論するのは難しいところもある。一方、本ワーキンググループでも既に議論になっている法的根拠やトラストアンカーという観点では、信頼できる発行元をどうやって担保するかという点が一番重要ではないかと考える。
- (ウ) ヨーロッパでは、署名の生成装置についても基準を定め、あるレベル以上のものを使うかどうかで区別をしており、我が国においても、認証局だけではなく、鍵をどう機器の中に組み込むかや、対象となる機器が何かといった点も含めて制度化すべき。
- (エ) e シールは法人が行うものであるため、その法人が管理している IoT 機器のための証明書というものを e シールとは別に考えることも可能だろう。

(4) 取組の方向性

ヒトを起点として発信されるデータだけではなく、Society5.0 時代においては、モノから発信されるデータが利便性の向上や経済活動の生産性を向上させるための基盤となることから、モノの認証の実現は、そのデータの正当性を確保する上で極めて重要である。

特に、重要 IoT 機器については、Society5.0 を実現する上で、デバイスの製造段階からソフトウェアの更新、廃棄までの一連のライフサイクルにおいて「安全」であることが重要であり、PKI 等による認証の仕組みを導入することが考えられるが、モノの認証の具体化に当たっては、e シールとの違いも考慮しながら、コストや機能上の制約等の課題を踏まえ、どのような分野への適用が適切かを整理した上で、引き続き、仕組みの具体化について検討を進めていくことが適当である。

4.5 タイムスタンプについて

(1) 現状

現在は(一財)日本データ通信協会による民間の認定スキーム(タイムビジネス信頼・安心認定制度)により、タイムスタンプ事業者がサービスを提供しており、国税関係の帳簿保存など一部の分野において、利用が進んでいる¹⁰。(図5)

他方、タイムスタンプの制度的な裏付けがないため、民間の認定スキームでは企業の法務部門等で使用を躊躇するケースが存在するなど、上記以外の分野では十分に利用が広

¹⁰ 平成 30 年の発行件数は2億 3,700 万件(対前年比 134%)。

がっているとは言えない。

具体的には、国税関係書類をスキャナ保存する場合には、電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律施行規則(平成10年大蔵省令第43号)において、タイムスタンプの使用が義務付けられているが、建築や医療などの分野においては、ガイドラインにタイムスタンプの使用が記載されているにとどまる中、他の分野では特段のガイドラインがないなど規定のレベルや有無が分野によってバラバラであり、結果として、タイムスタンプの利用の程度もまちまちである。

例えば、建築士法(昭和25年法律第202号)において、建築士の業務として作成した設計図書は15年間保存しなければならないと規定されており、e-文書法により、当該設計図書を電子保存することが可能となっているが、①電子データの真正性を保存期間内にわたって保証する仕組みであるタイムスタンプについて法的な位置づけがない、②タイムスタンプの利用について、民間団体のガイドラインで推奨されるにとどまっている等の要因により、タイムスタンプの導入を躊躇し、設計図書の作成の段階までは電子化が進んでいるが、保存のためだけに紙で印刷しているなど、作成から保存まで一貫した電子化が十分に進んでいない。

また、日本公認会計士協会が発出している通達において、監査法人が上場企業の監査を行う際は原本で確認することが規定されており、監査が終了するまでは原本の破棄はできないという現状がある。その根本的な原因として、電子的に長期保存されたデータの真正性が担保されていないということが考えられる。

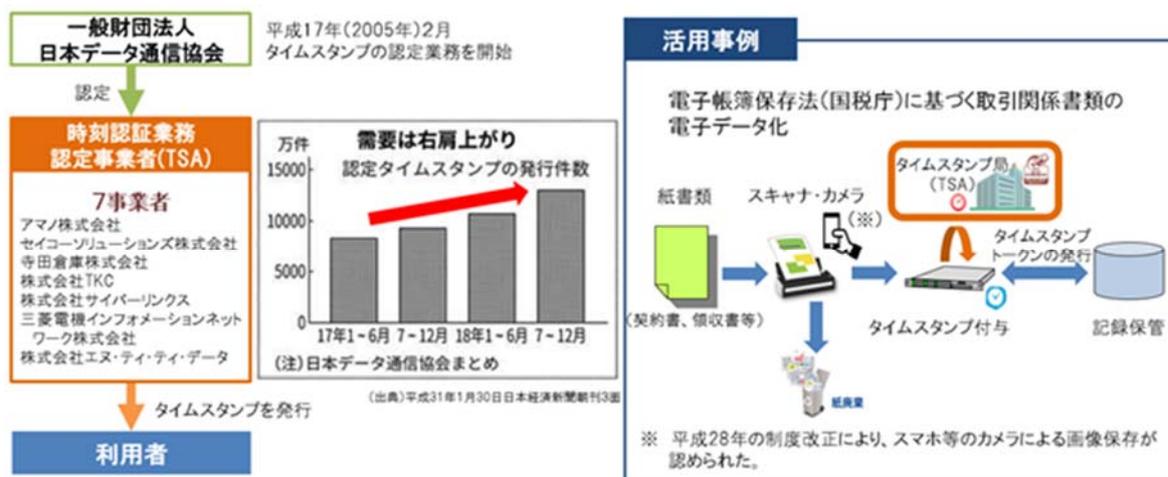


図5 我が国におけるタイムスタンプの利用の現状

(2) 課題

【課題1】 電子化の推進には、長期署名への対応が必要

上記の建築士法に基づく設計図書を始め、法律上長期間の保存を義務付けられている文書や住宅ローンの契約書(最長 35 年)など、長期的な保存を要する文書が様々存在する中で、電子署名の電子証明書の有効期間は5年間であり、電子署名のみでは長期的にデータの真正性を検証することができない。

このような長期にわたって保存が求められる文書について、タイムスタンプを用いた長期署名の枠組みが法的に整備されることで、電子的に長期保存されたデータの真正性が担保され、利用者にとってより安心・安全なサービスの提供につながることを期待される。

【課題2】 廃業の際の対応策が未整備

現行の民間の認定スキームのままでは、タイムスタンプ事業者やタイムスタンプ事業者が電子証明書を発行している認証局の廃局・廃業時の対応が不十分となり、社会的混乱を招くおそれがある。

【課題3】 国際的な相互承認のための公的枠組みが必要

国際的なデータ流通の進展とともに、海外において日本のタイムスタンプの有効性を争われるような場面も増えることが想定される。その際、民間による認定スキームのままでは、証拠として採用されにくくなるおそれがある。

日本のタイムスタンプが、国際的な枠組みにおいて信用のあるものだと認められれば、第三国において訴訟を行う場合でも、証拠として示しやすくなるため、EU を始め、各国と相互運用性を確保する枠組みを構築することが求められる。

(3) 構成員からの主な意見

(ア) 個人向けの住宅ローンでは、貸出期間が 30 年から 35 年が一般的であり、長期署名の枠組みが法的に整備されることで、利用者にとってより安心・安全なサービスが提供でき、サービスの拡大や借入人の利便性向上が期待される。

(イ) 電子帳簿保存法との関係では、法律でデータ保存が認められている一方で、実際には原本が破棄できないという問題がある。監査法人が上場企業の監査を行う際は、日本公認会計士協会が発出している通達において、監査の際は原本で確認することが規定されており、監査が終了するまでは原本の破棄はできないという現状があ

る。

(ウ) 廃業時の失効情報の扱い等について、法律で規定しなければ、タイムスタンプ制度は安定的な制度にはなり得ない。

(エ) (タイムスタンプについて) 法的に担保された規定がないため、電子データを保管するためのシステムを構築するにしても、それなりの規模の投資を必要とする一方、将来的に認められるかどうか不明であることが課題。

(オ) 日本のタイムスタンプが、国際的な枠組みにおいて、信用のあるものだと認められれば、第三国において訴訟を行う場合でも、証拠として示しやすくなるため、EU を始め、各国と枠組みを構築していくべき。

(4) 取組の方向性

2005 年の(一財)日本データ通信協会による民間の認定スキームの開始から 14 年が経過したが、現行の民間認定スキームでは、電子帳簿保存法に基づき、省令でタイムスタンプの使用を義務付けている国税関係書類の電子保存の場面など、その利用は一定の範囲にとどまっているため、今後、他の分野でタイムスタンプの普及が進んでいない原因を分析した上で、タイムスタンプの利用を社会全体に広げるための制度の在り方について、検討を深めていくことが必要である。

その際、海外においてデータの真正性を争う場面が増えることも想定され、EU の eIDAS 規則等との国際的な相互運用性に十分留意することが必要である。

4.6 データの送達等を保証する仕組みについて

(1) 現状

e デリバリーは、送受信者の識別とデータの送受信日時の正確性、送受信データの完全性を保証するものであり、「電子的な書留」に相当するトラストサービスである。例えば、ドイツでは、ドイツテレコムなどによって「De-Mail」サービスが提供されており¹¹、B2C では保険契約事項に関する連絡や株主総会に関する連絡等、B2G では不動産事業者の認可申請や商業登記申請等、C2G では住宅給付申請や税額の査定申請等で使用されている。

また、受信者・送信者個人が特定されるので、フィッシング詐欺やマルウェア配布を防止することにもつながると考えられる。

¹¹ 2019 年3月現在、1,916 組織及び約 100 万アカウントが e デリバリーを利用している。

(2) 課題

e デリバリーは、厳格にヒトや組織の確認がされた送受信者双方が登録して成立するサービスであるが、現時点において、そのようなサービスを利用する送受信者それぞれのニーズが顕在化していない。

(3) 構成員からの主な意見

(ア) 裁判のIT化においては、裁判所から送達したものが確実に相手に到達したことの証明が課題。また、裁判を起こした原告はDe-Mailに登録してもらうことも可能かもしれないが、被告は訴えられて初めて裁判に入ってくるため、De-Mailに登録されていない可能性が非常に高い。

(イ) De-Mailは、受信者・送信者個人が特定されるので、フィッシング詐欺やマルウェア配布を防止することにもつながり、取組を進めるべきと考えるが、個人の特定や個人情報閲覧についてまで、トラストサービスの中で規定して良いかについては検討が必要。

(ウ) 欧州ではGDPRにおいて個人情報に対する取扱いを規定しているように、個人情報保護に係る規定と組み合わせる処理していくのが良いのではないかと。

(4) 取組の方向性

e デリバリーは、現時点においてニーズが顕在化しているとは言えず、電子署名、e シール、タイムスタンプの仕組みを組み合わせるものであることから、e デリバリーの実現に当たっては、今後の我が国におけるトラストサービスの進展を踏まえつつ、ユーザ企業側のニーズやユースケース等について、引き続き、検討を進めていくことが必要である。

また、e デリバリー以外にも、新たなトラストサービスのニーズやユースケースについて、諸外国における動向も踏まえながら、引き続き、検討を進めていくことが必要である。

おわりに

デジタル時代の競争力の源泉であるデータは、21世紀の戦略資源であり、データの自由な流通は、産業活性化・国際競争力の強化に資することから、我が国にとってこれからの成長のエンジンとなる。

その一方で、国境を越えるデータのやりとりが拡大し続けている中、データ流通に関する国際ルールは存在しておらず、国際的なデータ流通網を構築する上で、プライバシーやセキュリティ・知的財産などの安全を確保することは極めて重要な課題となっている。

本年6月8日、9日に日本で開催された G20 茨城つくば貿易・デジタル経済大臣会合においても、日本が提唱した「自由で開かれたデータ流通」と「データの安心・安全」が両輪として機能する「データ・フリーフロー・ウィズ・トラスト(DFFT)」のコンセプトや、デジタル経済におけるセキュリティの確保の重要性について、G20 の議長国として各国の共通理解を求め、閣僚声明に反映された。

また、本年成立したデジタル手続法により、今後、行政手続のデジタル化が徹底されることが期待される一方で、多くの民間手続については、書面の作成から保存まで一貫した電子化が進んでいないことから、今後、民間も含め社会全体として「紙からデジタルへ」を実現するためには、データの信頼性を確保し、安心・安全なデータ流通を支える基盤が不可欠となる。

Society5.0 の実現に向けて、国際的なデータ流通網の構築、我が国におけるデジタル化を進展させるためには、送信元のなりすましやデータの改ざん等を防止する仕組み＝“トラストサービス”が必要であり、ヒトだけでなく、組織(企業が発行する文書等)やモノ(IoT 機器からのセンサー情報の発信等)の正当性も確認できる仕組みが求められる。

本ワーキンググループでは、引き続き、我が国におけるトラストサービスの在り方について、本中間取りまとめの個別の論点に掲げた取組の方向性に基づき、制度の在り方を含めて詳細な検討を進め、関係省庁と連携しながら、具体的な整理を行い、本年 12 月までに最終報告書として取りまとめしていくこととする。