2021

デジタルトラスト協議会

ルール形成委員会

ホワイトペーパー 第1版

2021年12月7日

デジタルトラスト協議会　ルール形成委員会

内容

I　はじめに 3
II　スコープ：Society5.0 の実現に向けたデジタルトラスト 5
1　背景 5
2　デジタルトラストの定義 5
3　本ホワイトペーパーの構成 6
III　環境状況/状況の変化 7
1　デジタル化が進む中トラストが必要となってくる理由 7
2　各国の状況 9
(1)　米国 9
(2)　EU 11
(3)　国連 12
3　国内の状況 12
4　トラストに関する動向のまとめ 14
IV　デジタルトラスト実現に向けた課題 16
1　デジタルトラストの狙いと社会課題 16
2　デジタルトラストがもたらす効果：堅確化の実現 17
(1)　堅確化実現の例 17
3　実現を目指す世界と課題分析 22
(1)　現状（法人口座開設の例） 24
(2)　デジタル化における課題（法人口座開設の例） 25
(3)　デジタル化移行後の姿（法人口座開設の例） 25
4　デジタルトラスト実現のための技術課題 27
V　解決に向けた機能提言 30
1　TaaS（Trust as a Service）とは 31
2　TaaS の構成 33
3　TaaS の利用イメージ 39
4　TaaS の効果 40
5　TaaS の利便性：高い身元確認レベルの ID のオンライン発行とリモート署名 41
6　TaaS ユースケース 43
(1)　法人の銀行口座開設 43
(2)　請求書の電子化 44
(3)　TaaS 連携形態（分散 TaaS 連携） 46
(4)　政府系システムとベース・レジストリ 47

Copyright 2021 Japan Digital Trust Forum

(5) 国と民、国と自治体のシステムの TaaS による連携.....48
(6) 法人ベース・レジストリ活用による法人活動の確認.....49
(7) 金融機関等での TaaS による情報の連携.....50
(8) 商談・契約活動における交渉経緯の記録.....51
VI 今後の検討事項.....53
1 次期ホワイトペーパーに向けた検討事項.....53
2 社会実装上とるべきアクション.....54

Copyright 2021 Japan Digital Trust Forum

デジタルトラスト協議会 ルール形成委員会 ホワイトペーパー(第１版)

デジタルトラスト協議会 ルール形成委員会

Ⅰ　はじめに

国際社会が持続的な開発目標を目指す上での諸課題を抱えている中、日本政府は AI・5G・IoT 等のデジタル技術をあらゆる産業や社会生活に取り入れ、経済発展と社会的課題の解決を両立していく社会としての Society 5.0[1]の実現を提唱している。

Society 5.0 の実現のため、様々なステークホルダーが協調し、データの国際的な流通を見据えて、欧州 eIDAS 規則[2]など諸外国との調和を前提とした信頼性を担保する仕組みの構築が望まれている。日本政府は、Data Free Flow with Trust(DFFT)[3]として自由で開かれたデータ流通とデータの安心・安全の２つをポイントに取り上げている。

この政策実現は、インターネットによって繋がっていく社会を前提としている。一方で、サイバー攻撃、サイバー犯罪などの悪意ある行為に対し、今までも様々な対策、施策を実行しているが皆無にすることは出来ていない。これからのデジタル社会を形成するうえで、ゼロトラスト[4]を前提とし、デジタル社会で活用されるデータの信頼性を担保した社会構造に変革することが極めて重要である。

デジタル社会で活用されるデータの保護のため、個々のセキュリティ運用の高度化を進めつつ、社会全体で相互に相手の正しさを確認し、安心したデータのやりとりができる環境を整備することが、前述の社会構造の変革の要諦であると考えている。

内閣官房が主導するデジタル・ガバメント閣僚会議[5]や官民を横断した枠組作りであるデ

---

[1] https://www8.cao.go.jp/cstp/society5_0/

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[3] 「デジタル時代の新たなＩＴ政策大綱」、IT 総合戦略本部、2019 年 6 月 7 日決定、https://cio.go.jp/node/2534

[4] 何も信用しない、を前提にセキュリティ対策を実現する考え方。例えば、組織内ネットワークの内部は信用する、組織外ネットワークの外部は信用しない、といったネットワークを分けることを前提とせず、組織内外ネットワークに関係なく信用しないことを前提とし、セキュリティ対策を実現する考え方のこと。

[5] https://www.kantei.go.jp/jp/singi/it2/egov/

Copyright 2021 Japan Digital Trust Forum

ータ戦略タスクフォース[6]などにおいても、Society5.0 における信頼性を担保する中核である「データの信頼性」（トラスト）[7]要件として「サイバー空間とフィジカル空間が高度に融合した Society5.0 を実現するためには、サイバー空間におけるデータが、正しく生成されたもの（主張された通りのもの）であること（真正性）、改ざんされていないこと（完全性）を確保・証明する必要がある。」が挙げられており、データの完全性や、データ連携基盤の信頼性を担保することが極めて大切であると指摘されている。また、コロナ禍においてリモートワーク推進の必要性から、書面・押印廃止、対面規制についての見直しが進むとともに、前述のようなデジタル化における信頼性の担保の在り方の検討が必要とされている。

本ホワイトペーパーは、デジタル化における信頼性の担保を社会課題としてとらえ、社会課題を解決するための技術課題を分析し、解決のための仕組み・仕掛けを提言する。

現状のフィジカル空間では、慣例として各種手続き・契約等を紙の書類と押印により行うことで信頼性を担保している。これらの各種手続き・契約等を Society5.0 や DFFT で必須となるサイバー空間に安心・安全に移行するためには、フィジカル空間とサイバー空間のつながり、サイバー空間どうしのつながりのそれぞれについて、トラストを確保する必要がある。本ホワイトペーパーは、以下の２つの視点から技術課題を分析するとともに、これらを解決するための仕組み・仕掛けとしての Trust as a Service (TaaS)を提言する。

・視点１：フィジカル空間からサイバー空間とのつながり（縦のトラストの確保）
・視点２：サイバー空間のつながりのトラスト（横のトラストの確保）

このような社会課題・技術課題の解決を通じて、様々なステークホルダーが協調し、デジタル化におけるトラストを確保する仕組みの構築と、これらの社会実装をルール形成とともに加速させることがますます重要になると考えられる。その際、データの国際的な流通を見据えて、欧州 eIDAS 規則など諸外国との調和をはかることが必須である。

当協議会では、Society5.0 の実現に向けた基本コンセプトである「デジタルトラスト」の概念を浸透させ、実社会で利活用していくための仕組み・仕掛けとしての Trust as a Service (TaaS)の構築、法制度の整備に向けたルール提言を行うとともに、社会実装と普及を加速する。

---

[6] https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai4/gijisidai.html
https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai7/gijisidai.html

[7] 以下、本書では「トラスト」と呼ぶ

Copyright 2021 Japan Digital Trust Forum

II　スコープ：Society5.0 の実現に向けたデジタルトラスト

1　背景

近年、インターネットが経済や生活に浸透する中で、クラウドサービス、人工知能（AI）、IoT 等によるデータ主導のデジタル社会が到来しつつある。また、新型コロナウイルスは、「新しい日常」の中で、テレワークやリモート会議とともに、書面、押印、対面等の原則の見直しの契機をもたらした。

ビジネスや行政における手続きのオンライン化等のニーズが高まる一方、社会全体としてデジタルの恩恵を享受するためには、紙の世界に慣れ親しんできた人々の心配を取り除き、安心感を与えるとともに、デジタル社会における手続きの最適化を行うことでユーザの利便性の向上を図り、もって社会全体の効率化を実感できる仕組みが重要である。これにはデジタル社会におけるデータに係る信頼性を担保し、安心・安全なデータ流通を担保する社会的な仕組みが不可欠であり、このような社会を目指すための基本コンセプトとして、以下で定義される「デジタルトラスト」を提唱する。コロナ感染の拡大の防止として、個々のサービスのデジタル化・オンライン化も進んできているが、今後 Society5.0 を実現していくには、これらのサービスやシステムが連携し、安心・安全に利用できるために、データ戦略タスクフォースでも述べられているような信頼性の担保が必要となっている。

2　デジタルトラストの定義

データ戦略タスクフォースでは、「信頼性（トラスト）の全体像」として「サイバー空間とフィジカル空間が高度に融合した Society5.0 を実現するためには、サイバー空間におけるデータが、正しく生成されたもの（主張されたとおりのもの）であること（真正性）、改ざんされていないこと（完全性）を確保・証明する必要がある。」と述べられている。これを踏まえたうえで、我々は、Society5.0 実現のための「デジタルトラスト」を、以下のように定義する。

【デジタルトラストの定義】
フィジカル空間とサイバー空間を跨いだ産業や行政等の活動のサービス、手続きおよびデータ連携において、デジタル技術を用い、人・組織・モノ・データ等に対して信頼（トラスト）確保することで、前述のサービス、手続きおよびデータ連携のデジタル化において、堅確性[8]等の効果をもたらすことを指す。信頼（トラスト）確保の具体例としては、ネットワ

[8] 手続き等を堅牢かつ確実な状態にすること

Copyright 2021 Japan Digital Trust Forum

ークを通じた送受信の相手の真正性、データの完全性、などが確保され、当事者および第三者による検証を可能とするとともに、プロシージャ[9]・システムの正当性に関しても当事者および第三者による検証可能性を有すること、などがあげられる。

デジタルトラストの実現には、社会制度とデジタルシステムの両方が必要であり、デジタルトラストを実現するためのデジタルシステムを Trust as a Service(TaaS)と呼び、V 章に詳述する。

本コンセプトは、2021 年 5 月、データ戦略タスクフォース[10]において示された「トラストの枠組みの整備」[11]にも呼応するものであり、「デジタルトラスト」は、Society 5.0 における信頼性（トラスト）を担保するための基本コンセプトとして、官民の連携の下、早急に確立されるべきである。

ここで定義した「デジタルトラスト」は、サイバーセキュリティとは別の視点から、データに係る信頼性の担保を実現することである。これを実現するには、ゼロトラストに基づく対策方法として守るべきデータをクラウドに集約する方法が考えられる。さらに、デジタルトラストを実現することで、DFFT の理念に基づき多くのデータが移動、分散されたシステム上に保管される世界を前提とした、データ連携による新たなイノベーション創造をする社会への移行、および安心・安全なデータ流通を担保することができる。

3　本ホワイトペーパーの構成

本ホワイトペーパーは、Society5.0 にむけてデジタル化が進む中、トラストが必要となる背景と各国のトラストの状況、および「デジタルトラスト」が必要となってくる理由を述べる（第 III 章)。

「デジタルトラスト」の狙い、および「デジタルトラスト」の課題を述べたうえで(第 IV 章)、「デジタルトラスト」実現のためのデジタルシステムとしての解決策である「Trust as a Service(TaaS)」を提言し、実現における課題を述べる（第 V 章)。最後に、本ホワイ

---

[9] 産業活動・サービス・手続き等における目的を実現するための、相互に関連するまたは相互に作用する一連の活動、手順を表す。

[10] https://www.kantei.go.jp/jp/singi/it2/dgov/dai10/siryou_b.pdf

[11] ID の認証やトラストサービスの評価などトラストアンカーの機能整備の他、誰が(主体・意思)、何を(事実・情報)、いつ(時刻)というトラストの要素について、これらが主張されたとおりのものであること(真正性)、改ざんされていないこと(完全性)の確保・証明が必要であるとし、各々の論点を整理し、整理した論点について、関係省庁で解決の方向性を検討開始される旨が記載されている。

Copyright 2021 Japan Digital Trust Forum

トペーパーの今後の課題として、次期ホワイトペーパーに向けた検討課題 および「デジタルトラスト」の社会実装に向けた取るべきアクションを提言する（第 VI 章)。

III　環境状況/状況の変化

1　デジタル化が進む中トラストが必要となってくる理由

世界各国は、デジタル化の進展やイノベーションの推進によるデータ量の増大、AI 技術の向上などを背景に、デジタル社会においてデータが国の豊かさや国際競争力の基盤であると捉え、新たな社会に向けた戦略を策定し強力に推進している。

日本政府は、AI・5G・IoT 等のデジタル技術をあらゆる産業や社会生活に取り入れ、経済発展と社会的課題の解決を両立していく Society 5.0 の実現を提唱している。

このサイバー空間とフィジカル空間を高度に融合させ、データを高度に利活用する Society 5.0 の実現は、従来の産業構造やビジネスに大きな影響を与えると考えられる。例えば、(1)フィジカル空間、(2)フィジカル空間－サイバー空間のつながり、(3)サイバー空間それぞれのレイヤにおいて、次のような変化、影響が生じると予想される。

(1)フィジカル空間

① 業務形態の変化

- 産業活動・サービス・手続き等の目的に応じて、人・組織・モノ等の固定的・静的なつながりから、ダイナミックなつながりに変化(アンバンドリング・リバンドリング[12])
- リモート化・オンライン化への移行
- 上記に伴う、企業・組織間の協業や連携機会の拡大

② サプライチェーンの構造的変化

- ソフトウェア化、ネットワーク化、モジュール化に伴うサプライチェーンの複雑化
- 調達先などのステークホルダーの多様化、サプライチェーンのグローバル化
- 多様化するニーズに応えるため、動的に組み替え可能なサプライチェーンへ進展

③産業構造の変化

- デジタル化、分業化により業種間の参入障壁が低減され、業界再編、異業種融合が進行

[12] 「デジタル市場に関するディスカッションペーパー」、経済産業省、2020 年 1 月 8 日、https://www.meti.go.jp/press/2020/01/20210108002/20200108002-1.pdf

Copyright 2021 Japan Digital Trust Forum

(2)フィジカル空間とサイバー空間のつながり

工場、医療、自動車、建設といった現場で日々蓄積される膨大なデータの利活用が産業競争力強化のカギになる。この利活用をめざし、サイバー・フィジカルの融合が加速し、今後ますますサイバー空間への依存度が高まると考えられる。

① 場所を選ばない働き方・サービスの拡大
- 民間のオンラインサービスの拡大
- デジタル・ガバメント実行計画等、行政等における手続のデジタル化移行

② データの活用による産業競争力強化
- 産業用途、自動車、医療などでIoT機器の急速な増加
- 米国のIIC(Industrial Internet Consortium)やドイツのIndustry 4.0など、サイバー・フィジカル・システムによる産業競争力強化に向けたさまざまな取り組み
- 異業種の新規参入や異なる分野のデータ連携を通じた新たな産業の創出

③ 製造業のサービス事業化
- OSS、3Dプリンタなどにより製品自体はコモディティ化がさらに進み、製造業はデジタル技術、リアルデータを活用し出荷後の保守も含めたサービス事業へシフト

(3)サイバー空間

① 流通するデータ量の増大

さまざまな組織、業種、業界、或いは創出された価値が、その境界を越えてデータでつながる分散環境でのデータ流通の一般化

② サイバー空間におけるリスクの増大
- サイバー攻撃の高度化・複雑化によるリスクの増大
- データ流通の増大によるアタックサーフェス(攻撃対象領域)の増加
- ビジネスメール詐欺など、システムに対する防御だけでは防ぐことができない攻撃の増加

これらの予想される変化、影響を踏まえると、サイバー・フィジカルが高度に融合した、安心・安全なSociety 5.0の実現に向けては以下の(1)～(3)に示したようなリスクが想定される。

(1) サイバー空間の問題が、フィジカル空間、企業の事業活動に深刻な影響を与える可能性が高まる
(2) サイバー空間の拡大に伴って、プライバシーやセキュリティ、データの保護などに関わるリスクが増大する
(3) 組織間、およびマシン間による大量な流通データの連携による、データの発出元や真正性確認の必要性やその自動化要求が高まる

Copyright 2021 Japan Digital Trust Forum

データを有効に利活用することで経済発展と社会的課題の解決を両立しつつ、上記のリスクに対応するには、流通するデータに関するトラストを確保しながら、データを自由に流通させるために必要な国際的なルール作りが不可欠である。
特にデータは組み合わせ、利活用することにより価値が高まるものであるため、単にデータを囲い込むのではなく、業種、業界の垣根を越えて共有可能なエコシステムを構築することが、イノベーション創出に向けて非常に重要である。それを支えるのが、人・モノといった物理的実体に限らず、組織や団体など物理的以外に実存するものを含む実体 （エンティティ）間でトラストを確認する仕組みである。

このため、日本としては、以下の(1)(2)(3)を踏まえ、① データの作成者・発信元の真正性、② データの非改ざん性の確保、③プロシージャ・システムの正当性、等のトラストを確保し、創出される新たな価値を社会に行きわたらせるための仕組みの実現と、その間でデータを安全で自由に流通させることで安心して利活用するための国際的なルール作りをめざすべきと考える。

(1)産業間や組織間のつながり
(2)サイバー空間上に転写、形成される現実社会(デジタルツイン)
(3)サイバー空間上のデータのつながりとデータの取り扱い

2 各国の状況

(1) 米国

連邦政府を中心とした国家安全保障の観点からのトラストサービスに係る技術の標準化や制度が確立されている。

電子認証を幅広くカバーするカードとして FIPS-201(Federal Information Processing Standards Publication 201)に準拠した Personal Identity Verification (PIV) カードが知られている。対面での本人確認、電子認証、電子署名、暗号化、生体認証など、非常に幅広い機能を有し、政府職員に向けて発行されている。民間向けには、PIV-Interoperable (PIV-I) カードが発行される。

電子認証に関するガイドラインとして、アメリカ国立標準技術研究所(National Institute of Standards and Technology, NIST)によって公開された NIST SP 800-63[13]が知られている。政府機関のオンラインサービス等で、重要データへのアクセスなどのために IT システムに

[13] NIST, Digital Identity Guidelines(電子認証に関するガイドライン), https://pages.nist.gov/800-63-3/

Copyright 2021 Japan Digital Trust Forum

対してネットワーク経由でリモートから行うオンライン認証を対象とし、システムへの登録時の本人確認や認証時の保証レベルの要件、目的に応じた保証レベルの選定フローチャートを規定したガイドラインである。

電子認証に関するインフラとして、FPKI(Federal PKI) が知られている。これは電子証明書を使って政府機関同士、関係企業を安全につなげる(認証)基盤であり、数百の認証局(Certification Authorities)から構成される。ブリッジ認証局で他の政府機関や民間組織とつながり、NIST SP800-63 に規定される保証レベルによるポリシーマッピングを行うことで、相互接続を可能にしている。

個人の意思の表明としての電子署名に関する法制度は、1999 年 州レベルの統一法として Uniform Electronic Transactions Act (UETA)が成立、その後 2000 年に、ESIGN Act[14] (Electronic Signatures in Global and National Commerce)として制定されている。ESIGN Act により、あらゆる州でリモート署名や手書きサインのスキャンデータを含む様々な電子署名が手書き署名と法律上同等に扱われるようになった。

国家安全保障に関わる情報分類として、CI(Classified Information)、CUI（Controlled Unclassified Information）と呼ばれる情報の機密性区分が知られている。2009 年 12 月の大統領令 Executive Order 13526 により、機密指定された国家安全保障情報(Classified National Security Information)を対象に CI の分類、保護など、機密指定制度に関する規定が行われ、改定強化が行われた。CUI のコンセプトは 2010 年 11 月の大統領令 Executive Order 13556 によって定義された情報カテゴリである、軍事兵器等、国家安全に関連する製品の生産にサプライチェーンの機密保護を狙ったものである。国立公文書館（NARA）が連邦政府全体に対して CUI 保護の体制の責任を負う。NARA の指示のもとに、NIST が CUI を保護するための基準を NIST SP800-53[15]をもとに、NIST SP800-171[16]として規定した。SP800-53 はセキュリティ管理策のカタログを規定している。SP800-171 は政府調達先である民間を対象にした管理対象外機密情報(Controlled Unclassified Information; CUI)の推奨セキュリティ要件を規定したガイドラインである。

また、フィジカル空間からサイバー空間への移行に関する指針を示すレポートとしては、

---

[14] The Electronic Signatures in Global and National Commerce Act (E-Sign Act), https://www.fdic.gov/regulations/compliance/manual/10/X-3.1.pdf

[15] NIST, Security and Privacy Controls for Information Systems and Organizations（連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策）https://www.nist.gov/privacy-framework/nist-sp-800-53

[16] NIST, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (連邦政府外のシステムと組織における管理された非格付け情報の保護), https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

Copyright 2021 Japan Digital Trust Forum

NIST SP800-207[17] 「ゼロトラスト・アーキテクチャ」が挙げられる。本レポートは、攻撃者は組織内外のいずれのネットワーク上にも存在しうるという「ゼロトラスト」の前提のもと、この前提でサイバー空間上のセキュリティを実現する「ゼロトラスト・アーキテクチャ」を提唱している。本アーキテクチャはサイバー空間上のセキュリティの観点であるが、サイバー空間におけるトラスト確保にも有用な考え方を含んでいると考えられる。

民間の動向としては、民間ベースのデータ流通に対する標準や規制等による社会受容性を持った仕組みの構築や、政府系トラスト制度・基盤（NIST SP800-63 等）を起点とした民間サービスへの展開[18]が行われている。

(2) EU

経済発展の観点からのトラストサービスや制度が確立されている。欧州委員会は 2010 年にデジタル単一市場（Digital Single Market=DSM）戦略を発表、この戦略に伴い、欧州連合(EU)は加盟国間で異なる法律、制度、通信環境などを整備し、1999 年に発出した電子署名指令を廃止し、eID（electronic identification）と電子署名を含むトラストサービスの包括的な統一規則である eIDAS 規則を 2014 年に制定し 2016 年 7 月に発効している。

eIDAS 規則では、身元確認と認証、各種トラストサービスを信頼するための基準や仕組み、そしてトラストサービスを機械的に検証可能とするトラステッドリストの運用を法的に規定している。eIDAS 規則でのトラストサービスは以下が挙げられる。

- 電子署名、e シール、タイムスタンプの生成・検証・照合
- e デリバリーサービスとサービスに関する証明書の生成・検証・照合
- website 認証の証明書の生成・検証・照合
- 各サービスに関する電子署名・e シール・証明書の保存

規則発効時点で、QTSP（適格トラストサービスプロバイダ）事業者数は、151 であったが、2021 年 1 月現在において、200 まで増加している。

最新の状況として、eID やトラストサービスの導入を促進するために、ENISA から 2021 年 2 月に eIDAS 推進報告書が発行されている。このうちのリモートによる本人確認の実態報告書[19]が特に重要と考える。本報告書は、対面での ID Proofing(身元確認)だと面倒かつコロナ禍だと危険という認識のもとに、リモートの ID Proofing に関する調査の方向性を示

---

[17] NIST, Zero Trust Architecture （ゼロトラスト・アーキテクチャ）, https://csrc.nist.gov/publications/detail/sp/800-207/final

[18] EXOSTAR 社など https://www.evaaviation.com/cui-dfars-nist-sp800-171/usaexostar/

[19] Remote ID Proofing https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing

Copyright 2021 Japan Digital Trust Forum

している。これは、eIDAS 規則上はリモートでも容認であるにもかかわらず「対面と同等」という条件が付いており、その解釈がどういうものなのか、不明確な状態と認識されていることに起因している。現在リモート ID proofing に関わっている各国のステークホルダーからアンケートを集め、リモート ID proofing サービスの脅威分析や対策案などの例をまとめ、今後の提言(5 章 3 項)をまとめている。

(3) 国連

UNCITRAL（国際連合国際商取引法委員会）の WG-IV（Electronic Commerce）[20]において、国際間電子取引における eID とトラストサービスの認識に関する規程[21]について、国際的な規定を設定することの議論がされている。

この議論は、2018 年から行われており、直近の 2020 年第 60 回会議において、トラストサービスについては、ほぼ内容が合意されている。モデル法として設定されるか、ガイドラインとして公開されるかは現時点で不明ではあるが、国際的な電子取引を実施するうえで、国連加盟国における指針になると思われる。以下に、関連する文言の定義を記載する。

(d) “Electronic identification”, in the context of IdM services, means a process used to achieve sufficient assurance in the binding between a [subject][person] and an identity.
(g) “Identity management (IdM) services” means services consisting of managing identity proofing or electronic identification of [subjects][persons] in electronic form.
(j) “Identity proofing” means the process of collecting, verifying, and validating sufficient attributes to define and confirm the identity of a [subject][person] within a particular context.
(m) “Trust service” means an electronic service that provides assurance of certain qualities of a data message and includes electronic signatures, electronic seals, electronic time stamps, website authentication, electronic archiving and electronic registered delivery services.
(n) “Trust service provider” means a person that provides one or more trust services.

3 国内の状況

2019 年に行政の推進等に関する法律「デジタル手続法」が施行され、デジタル化 3 原則

[20] https://uncitral.un.org/en/working_groups/4/electronic_commerce
[21] Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services
https://undocs.org/en/A/CN.9/WG.IV/WP.162

Copyright 2021 Japan Digital Trust Forum

（①デジタルファースト、②ワンスオンリー及び③コネクテッド・ワンストップ）を基本原則として明確化する国の行政手続のオンライン化実施が原則とされた。

これまでのデジタル化のように、紙や対面で行っていた手続を単にオンラインでできるようにするというデジタルへの置き換え「Digitization（デジタイゼーション）」ではなく、デジタルを前提とした次の時代の新たな社会基盤を構築するという「Digitalization（デジタライゼーション）」の観点の重要性を強調している。

行政デジタル化のため、2020 年（令和2年）10 月9日にデジタル・ガバメント閣僚会議が組まれ、そこでは「マイナンバー制度及び国と地方のデジタル基盤抜本改善 WG」、「データ戦略タスクフォース」及び「デジタル改革関連法案 WG」が置かれ、具体化・加速化が進められている。

「マイナンバー制度及び国と地方のデジタル基盤抜本改善 WG」では、マイナンバーカードを活用した各種カード等のデジタル化の工程表も作成されており、フィジカル空間をサイバー空間のデータに置き換えるために、サイバー空間でトラストが求められる 3 要素 a)意思表示、b)発行元、c)存在やトラストアンカーの機能など、トラストを確保する包括的な枠組みの確立の必要性が示されている。

「データ戦略タスクフォース」[22]では、「信頼性（トラスト）の全体像」として、サイバー空間フィジカル空間が高度に融合した Society5.0 を実現するためには、サイバー空間におけるデータが、正しく生成されたもの（主張されたとおりのもの）であること（真正性）、改ざんされていないこと（完全性）を確保・証明する必要があると述べられており、サイバー空間での3要素として、意思表示の証明としての「主体・意思」、発行元証明としての「事実・情報」および存在証明としての「存在・時刻」が挙げられている。

「デジタル・ガバメント実行計画」[23]では、「デジタル改革関連法案 WG」において、デジタル化3原則である①デジタルファースト②ワンスオンリー③コネクテッド・ワンストップ、を基本原則として明確化する国の行政手続のオンライン化実施が原則とされ、その中で、デジタル・ガバメント実現のための基盤の整備として、本人確認を目的としたマイナンバーカードや、データ戦略推進を目的としたベース・レジストリ環境の整備が記載されている。

また、データの安心・安全・品質という柱で世界に発信した Data Free Flow with Trust は、プライバシーやセキュリティ・知的財産権に関する信頼を確保しながら、ビジネスや社会課題の解決に有益なデータが国境を意識することなく自由に行き来する、国際的に自由なデータ流通の促進を目指すというコンセプトである。

これらのデジタル化の推進とデータの流通のどちらの流れにおいても、デジタルトラストの実現は急務である。

---

[22] https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai4/siryou1-1.pdf
https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai7/siryou8-2.pdf

[23] https://www.kantei.go.jp/jp/singi/it2/dgov/201225/siryou4.pdf

Copyright 2021 Japan Digital Trust Forum

4　トラストに関する動向のまとめ

米国、EU 各国の動向を表 1 にまとめる。サイバー空間でのトラストに関して、各国とも必要性を認識の上で、オンライン本人認証を起点とした環境整備に向けた提言が始まっているが、包括的な環境整備やアーキテクチャ提言、社会実装およびルール形成はこれからの課題である。

動向比較から考察される日本のトラストの在り方の方向性として、例えば以下が考えられる。

- マイナンバーカードとベース・レジストリの観点で、本人認証や属性情報に関する解決提言
- ベース・レジストリと連携した付加価値の高いトラストの実現
  - 例 1．組織の属性情報をベース・レジストリと連動し、公共入札における競争参加資格の申請時のチェック
  - 例 2. gBizINFO を活用した法人の実在性及び属性情報の確認の自動化
    - gBizINFO（ジービズインフォ）は、経済産業省が運用する国内法人に関する情報提供サイトであり[24]、法人番号が指定されている約 400 万社を対象とし、法人番号、法人名、本社所在地に加えて、府省との契約情報、表彰情報等の政府が保有し公開している法人活動情報を一括検索、閲覧できる。
    - gBizINFO の API は公開されているので、民間のトラストサービスプロバイダが、法人の代表者、法人自体、法人が所有する Web サイト等に対して電子証明書を発行する際に、当該法人の実在性に加えて、所在地、代表者の氏名、役職等の属性情報をオンラインで確認することが可能である。
    - 今後、法人のベース・レジストリとして、法人名（カナ、代替文字、英字）や事業所情報が整備されていく中で、gBizINFO を活用した電子証明書の発行の自動化が期待される。
- 大量な流通データのトラストを自動確認できる国際連携可能な信頼の基点となる情報（トラストアンカー）の開示。

[24] https://info.gbiz.go.jp/index.html

Copyright 2021 Japan Digital Trust Forum

表 1　トラストに関する米国、日本、EU 動向まとめ

項目	米国	日本	EU
関連する法律	-National Commerce Act ：E-SIGN -Uniform Electronic Transactions Act：UETA -USA: Government Paperwork Elimination Act：GPEA -Executive Order 13526, 13556	-電子署名法 -公的個人認証法 -商業登記法 -電子委任状法	eIDAS
国民 ID、ID 管理	SP800-63, FIPS-201, PIV(-I)カード, SSN	マイナンバーカード （公的個人認証の電子証明書）	eID (eID カードは各国単位)
トラストアンカー, Trust Presentation	Federal Bridge CA (FBCA)	-政府ブリッジ CA （機械可読） -官報（対人可読）	Trusted List
監査、認定	- FPKI のポリシー準拠 - NIST SP800-53 の拡張：Cybersecurity Maturity Model Certification（ISMS より厳しく、Level3 まで存在, CUI によるデータ対策＋サイバー対策:CA 監査, NIST SP800-53 の延長だとあるが真偽は不明）	-特定認証業務の認定（電子署名法） -電子委任状取扱業務の認定（電子委任状法） -タイムスタンプ業務の認定 -公的個人認証法の 5 号認定	-eIDAS QTSP -ETSI EN 319 401 （一般ポリシー） -ETSI EN 319 411 （CA のポリシー） -ETSI EN 319 403 （適合性評価機関の基準） -ISO/IEC 17065 （適合性評価機関の基準）
サイバーセキュリティ対策	-NIST Cybersecurity Framework, -SP800-171 , SP800-53	-ISMS -METI サイバー・フィジカル・セキュリティ対策フレームワーク	-ISMS -EU Cyber Security Certification Framework
サイバー空間への移行	NIST SP800-207 「ゼロトラスト・アーキテクチャ」	データ流通基盤や、トラストアンカー等の環境整備が検討されている。	Digital Agenda for Europe デジタル単一市場の実現推進
デジタル化におけるトラストの課題	政府系トラスト制度・基盤を起点としたサービスの産業展開（NIST SP800-63 等）	マイナンバーカードを用いたオンライン認証等の検討はされているが、包括的な整備や、この環境を実現するための機能構成に基づくアーキテクチャは今後。	eIDAS の、適格レベルで求められる対面と同等の本人確認の標準化に対応中。これらへの制度面での対応、および eIDAS の EU 域外との国際相互承認。

Copyright 2021 Japan Digital Trust Forum

Ⅳ デジタルトラスト実現に向けた課題

1 デジタルトラストの狙いと社会課題

II 章で示したように、「信頼性（トラスト）の全体像」として、サイバー空間とフィジカル空間が高度に融合した Society5.0 を実現するためには、サイバー空間におけるデータが、正しく生成されたもの（主張されたとおりのもの）であること（真正性）、改ざんされていないこと（完全性）を確保・証明する必要がある。さらに、利用者負担の少ない導入手段や、組織が個々のシステムを越えてサービスが連携することで手続きが実現されることが必要である。

図 1 は法人の銀行口座開設を想定した書面手続きの事例である。省庁・銀行・企業・手続者との間で様々な書類や証明書を用いた書面手続きにより、銀行口座が開設される。このような組織間サービス連携のデジタル化を安心安全に実現することがデジタルトラストの狙いであり、我々が取り組む社会課題である。

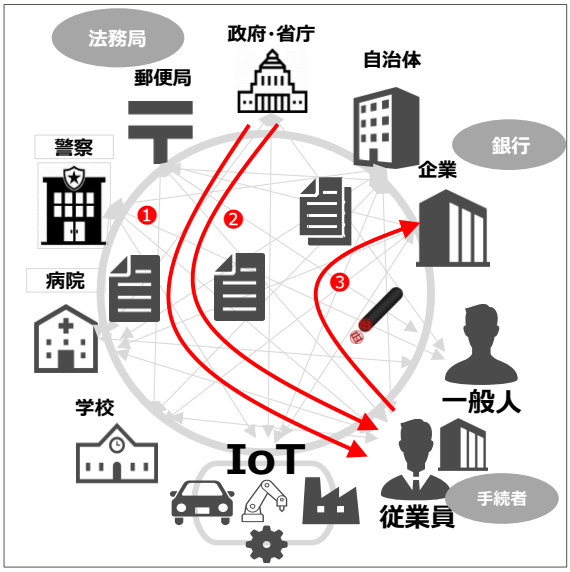


図 1 法人の銀行口座開設の手続き（書面）

Copyright 2021 Japan Digital Trust Forum

2　デジタルトラストがもたらす効果：堅確化の実現

組織が個々のシステムを越えてサービスが連携する手続きを実現するには、この手続きで用いられているデータが重要になる。この理由を、複数組織・企業等をまたがるようなサービス・手続きと、用いられるデータの関係を示した図 2 を用いて説明する。

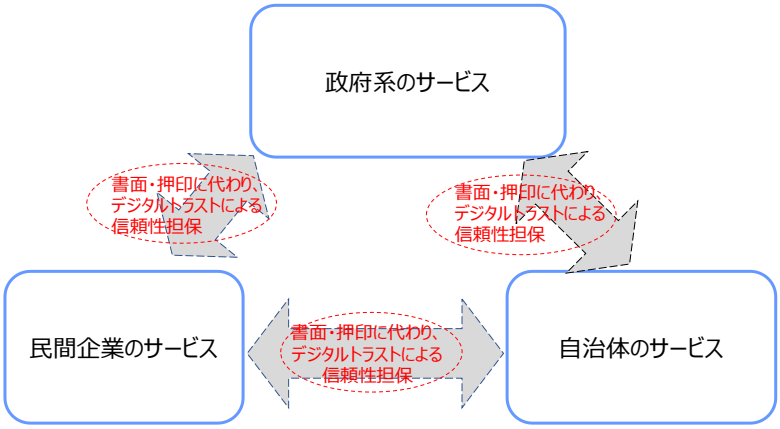


図 2　デジタルトラストによる信頼性の担保と堅確化の実現

図 1 の①～③は、実際の取引では、個別の手続きとしてデジタル化されていると考えられる。その反面、図 2 において、破線の矢印で示した処理がデジタル化されておらず、書面等で、異なるサービスやシステム間をつないでいること考えられる。書面による手続きでは、人間による端末入力や手作業を伴う手順が必要となるため、ミスの発生が避けられない。特に、複雑な入力や作業手順が伴うものではその傾向が高まる。これに対して、デジタル化を進めて人手の作業を無くし、さらに必須として残る手作業についても、利用者にとっての利用容易性を高めたデジタル化により、ミスの発生を低減化することができる。

デジタルトラストの狙いは、このような、書面・押印のデジタル化に伴い置き換わる、データの信頼性の確保およびデジタル化における利用容易性を高めることであり、これによりデジタル化された手続き全体に一定水準の堅牢化・確実化（堅確化）を実現する。

(1)　堅確化実現の例

デジタル化された手続き全体に一定水準の堅牢化・確実化（堅確化）を実現するためには、法的な制度に支えられたトラストサービスによるデータの信頼性の確保だけでなく、人手が関係する手順についても利用可能性を高めることがデジタルトラストして重要であ

Copyright 2021 Japan Digital Trust Forum

る。これを理解するための例として、電子メール等の通信手段を用いた見積書・請求書等のビジネス文書を用いた手続きのデジタル化を説明する。

例えば、現在ビジネスでの主流な通信手段である電子メールには以下の課題がある。

① 送信元の真正性が確保されておらず、正規のメールか、詐欺・フィッシングメールなのか見分けがつけにくい。
② 見積書、請求書などの取引情報を後段の業務システムに自動連携できない。
③ 誤送信のリスクが残り個人情報などの流出などの懸念がある。
④ 送達確認、受領確認の徹底が難しく、また受領通知を受け取っても真正性が確保されないためエビデンスとしては強固なものとみなされにくい。

このような課題を解決するものとして、eIDAS 規則では電子の書留便に相当する e デリバリーサービス（ERDS:Electronic Registered Delivery Service[25]）がトラストサービスの 1 つとして定義されており、様々なビジネス文書をセキュアに送受信可能となっている。ERDS のアーキテクチャは図 3 の 4 コーナーモデル[26]で表される。

[25] ERDS の例としては、e デリバリー、Registered Electronic Mail (REM) Services が知られている。REM の解説は下記の ETSI 文章に記載されており、例えば S/MIME が言及されている。（”Authentication in the REM MSI may rely on the features provided by SASL [i.12], TLS (e.g. certificate-based authentication), S/MIME [i.7] digital signature over the submitted message, or other mechanisms.”）
https://www.etsi.org/deliver/etsi_en/319500_319599/31953201/01.00.00_20/en_31953201v010000a.pdf

[26] Connecting Europe Facility：Introducing CEF eDelivery
https://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/03_eDELIVERY/S02_ERDS_REM_SOLUTIONS_SERVICES/INTRODUCING_CEF_eDELIVERY_RASMUSSEN_EC_DG_DIGIT.pdf

Copyright 2021 Japan Digital Trust Forum

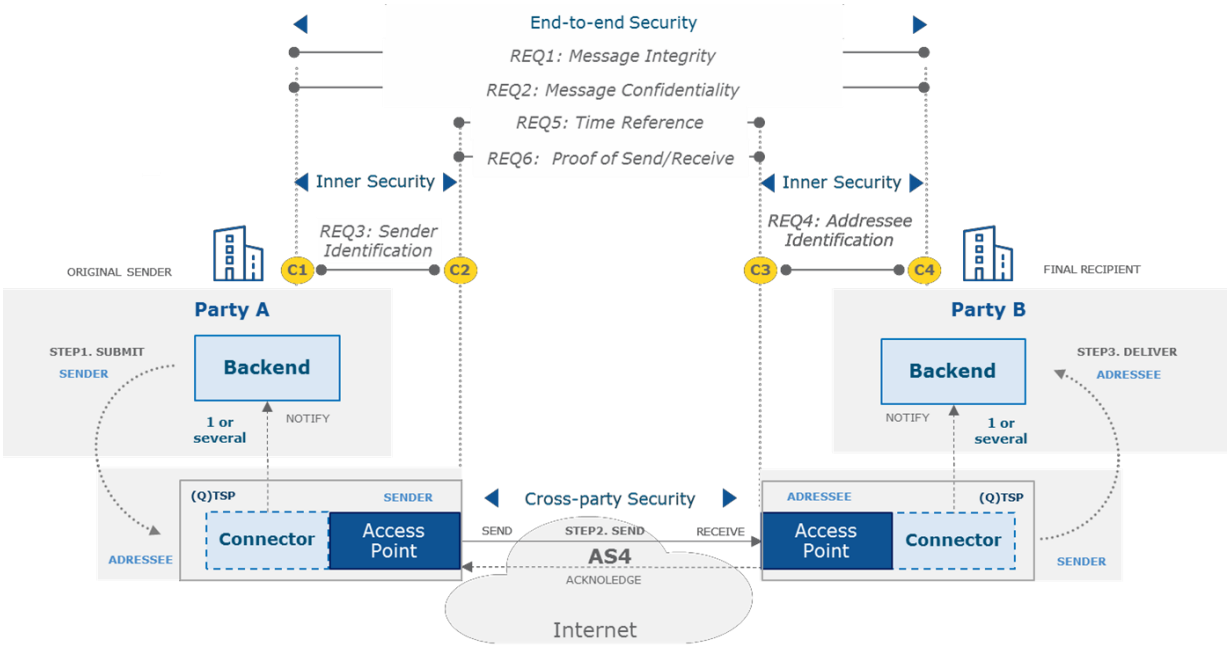


図 3 ERDS(Electronic Registered Delivery Service)のアーキテクチャー

ここでは、送信者の C1 と受信者の C4 との間で、C1 が利用する ERDS が C3、C4 が利用する ERDS が C3 で表されている。

ERDS では、送受信者の認証プロセスや C1-C4 間で End to End のメッセージ文書の真正性確保や C2-C3 間でのメッセージ文書の真正性確保などの要求事項があり e シールまたは電子署名が用いられている。認定された「適格 e デリバリーサービス」である QERDS(Qualified Electronic Registered Delivery Service)では、表 2 の REQ1 から REQ6 の要求事項が規定されている[27]。

取り交わされるメッセージ文書が C1 と C4 間で閉じた使われ方をする場合では C2-C3 間でメッセージ文書に e シールを行うことで確保可能となる(REQ5)。一方、C4 が受信したものを外部に提出が必要な場合は C1-C4 間の End to End のメッセージ文書の真正性確保が必要となる。例えば社員の立替払い精算や保険金請求業務など請求書、領収書の受領者と支払者が異なる場合は C1 が e シールを行うことで C1-C4 間の End to End のメッセージ文書の真正性を確保している(REQ1)。

[27] CEF eDelivery Building Block Version 1.00 Security Controls
Linking eIDAS (Q)ERDS & CEF eDelivery
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Security+Controls+guidance?preview=/82773295/82802571/(CEFeDelivery).(SecurityControls).(v1.00).pdf

Copyright 2021 Japan Digital Trust Forum

このような C1-C4 間の End to End でのメッセージ文書の真正性を確保することで、送受信されたメッセージ文書の完全性、識別される送信者による送信が行われたこと、識別される受信者による受信が行われたこと、QERDS による送信・受信の日付・時刻の正確性さが保証される。請求書、領収書の受領者と支払者が異なる場合でも、立替払い精算や保険金請求業務がデジタル化された場合でもこれらの手続きに堅確性をもたらすことができる。

Copyright 2021 Japan Digital Trust Forum

表 2　eIDAS 規則における適格 e デリバリーサービスの要求事項サマリー

適格 e デリバリーサービスの要求事項	CEF e デリバリーでの解釈	セキュリティ対象領域
REQ1: Message Integrity	メッセージは、送信中に不正に操作されないように保護されなければならない。これは、アドバンスド電子署名/e シールによって保証される必要がある。	End-to-end Security (C1-C4)
REQ2:Message Confidentiality	メッセージは送信時に暗号化する必要がある。	End-to-end Security (C1-C4)
REQ3: Sender Identification	送信者の身元は、認証プロセスおよび/またはアドバンスド電子署名/e シールの使用を介して、高いレベルの信頼性で検証する必要がある。	Inner Security (C1-C2)
REQ4:Addressee Identification	受信者の Identity は、メッセージの配信前に、認証プロセスおよび/またはアドバンスド電子署名/e シールを介して確認する必要がある。	Inner Security (C3-C4)
REQ5: Time-Reference	メッセージを送受信した日時は、アドバンスド電子署名/e シールによって保証された適格タイムスタンプによって示されなければなりません。	Cross-party Security (C2-C3)
REQ6: Proof of Send/Receive	メッセージの送受信者は、メッセージの送受信の証拠を提供する必要がある。これは、タイムスタンプまたは適格ステータスの場合は適格タイムスタンプを用いて、送受信の日時とリンクさせる必要がある。	Cross-party Security (C2-C3)

Copyright 2021 Japan Digital Trust Forum

3　実現を目指す世界と課題分析

現状の多くの手続きにおいては、フィジカル空間のみで紙の書類と押印により信頼性を担保し、企業・自治体間やサービス間をつなぐことが一般的となっている。これらの手続きのデジタル化を進める場合には、前節までに説明した電子署名やタイムスタンプといったトラストサービスにより、個別の組織、個別のサービスごとに、フィジカル空間からサイバー空間にサービスを展開する際のデータのトラストを確保するような仕組みが必要である。このようなデジタル化における課題を分析するためのモデルは、図 4 を用いて表すことができる。

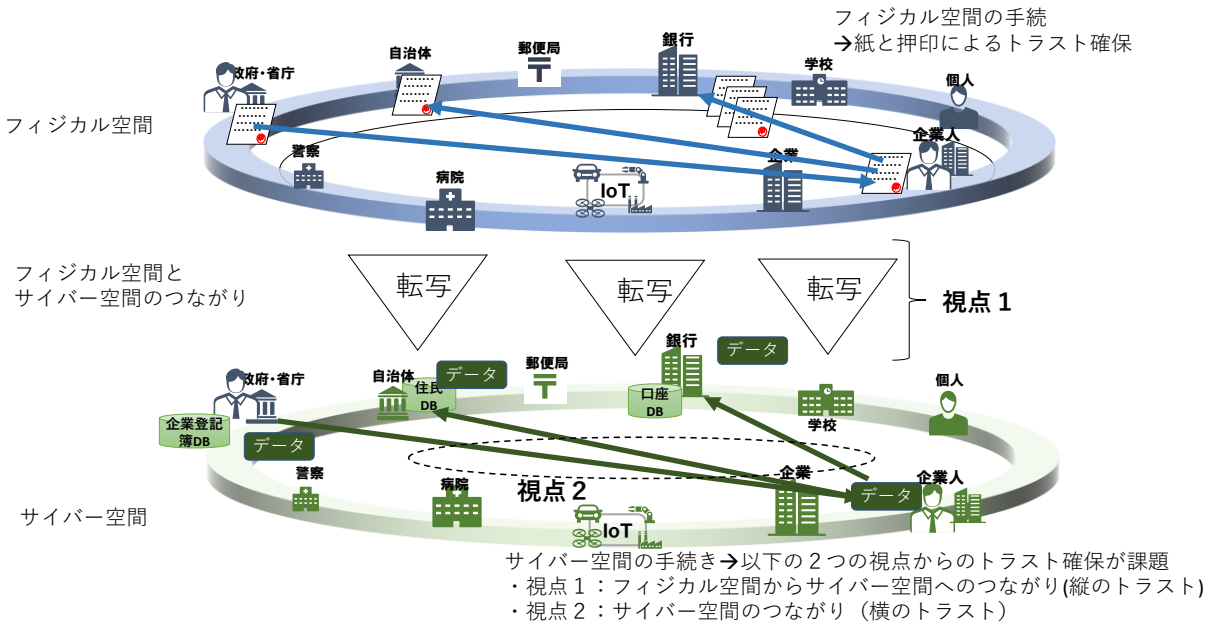


図 4 トラストなデジタル化における課題モデル

図 4 は、手続きのデジタル化における課題モデルを、フィジカル空間、フィジカル空間とサイバー空間のつながり、サイバー空間の３層を用いて示している。フィジカル空間の手続きの場合、紙の書類と押印により信頼性を担保しているが、この手続きをサイバー空間で実現するには、以下の２つの視点からのトラストの確保が課題であると考えられる。

- 視点１：フィジカル空間からサイバー空間とのつながりのトラスト（縦のトラストの確保）

  サイバー空間とフィジカル空間の境界において、要求される情報の正確性に応じて適切な正確さで情報が変換されること、つまり転写機能（「正確な翻訳」という意味も含む）の正確性が必要であり、そのためには以下のような課題を解決する必要がある。

  ➢ フィジカル空間の人・組織・モノに対するサイバー空間の ID 発行と、ID 発行

Copyright 2021 Japan Digital Trust Forum

時のフィジカル空間における実在性確認。

- フィジカル空間の手続きがサイバー空間のシステムにより正しく実現できていることの確認。
- サイバー空間の ID とフィジカル空間の人・組織・モノの対応付け（認証など）
- フィジカル空間の手続きの厳格さに応じて求められる、上記の確認や対応付けに関するルールおよび制度。

- 視点２：サイバー空間のつながりのトラスト（横のトラストの確保）

  データの流通・管理や適切な編集・加工を行うために必要となる対策やそのための仕組みが必要であり、そのためには以下のような課題を解決する必要がある

  - サイバー空間で行われる手続きやデータに関する発行元、時刻、意思確認
  - フィジカル空間で同一の人・組織・モノに対応するサイバー空間の ID 同士の紐づけ[28]
  - フィジカル空間の手続きの厳格さに応じて求められる、上記の確認や紐づけに関するルールおよび制度

以下では、図１で示した法人口座開設を例に、現状の手続き(AsIs)、デジタル化における課題、デジタル化移行後の姿(ToBe)、の順で説明する。

[28] 個人情報保護等、法制度の範囲内での紐づけを指す。

Copyright 2021 Japan Digital Trust Forum

(1)　現状（法人口座開設の例）

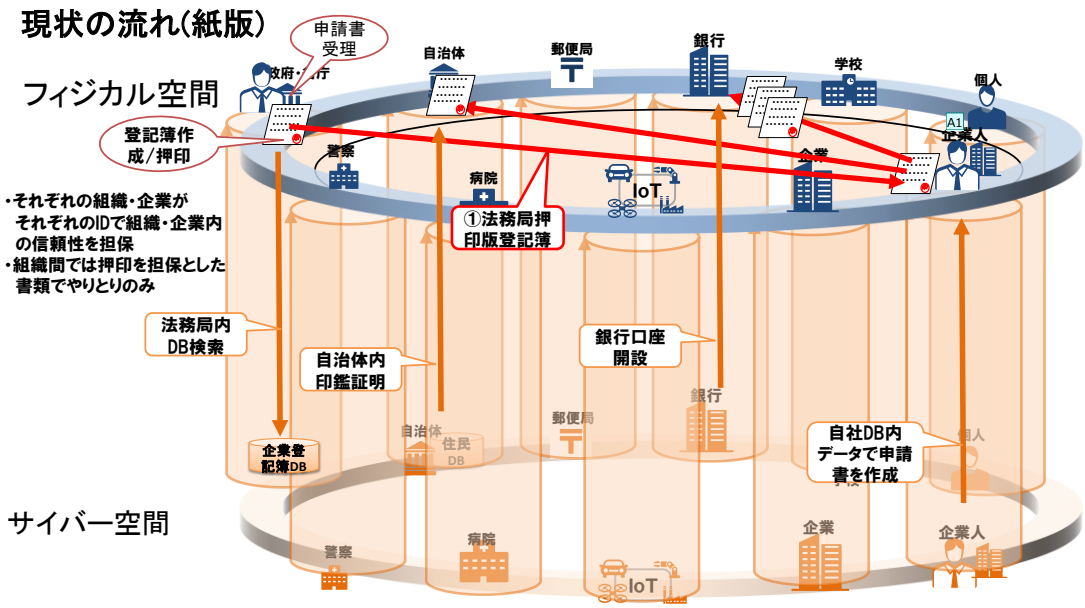


図 5　紙の書類を用いた現状の処理の流れ

図１で例示した法人の銀行口座開設の現状の流れを図 5 に示す。まず、申請する企業では、企業人が自社システムにログインし、自社の DB 等（サイバー空間）を利用して必要な情報を取得し、企業から法務局に商業登記簿謄本（履歴事項全部証明書）および印鑑証明の申請書を紙の書類として提出する（フィジカル空間）。法務局で受理（ここまでがフィジカル空間で処理）されたのち、法務局内の登記簿データベースで検索・確認（これはサイバー空間で処理）される。この結果に基づき、法務局で押印された商業登記簿謄本（履歴事項全部証明書）等は、紙の書類として（フィジカル空間で）申請企業に送付する。また、企業は、入手した証明書類を自社の DB 等（サイバー空間）から取得した会社の定款など、他の書類とともに（フィジカル空間で）、金融機関に提出して法人口座開設を行うことになる。

このように、現代社会においては、各企業・組織等の DB 等のサイバー空間にある情報を利用しつつも、異なる組織間での書類のやり取りは基本的にフィジカル空間で紙の書類としてやり取りされている。現状で、それらを安心・安全なものとして実現しているのは、役所等が発行する押印された書類の真正性が基になっており、そこからのトラストの連鎖であるということができる。

このような各組織内での紙の書類（デジタル空間）とデジタル化された情報（サイバー空間）とを何度も行き来する絡み合った処理は、今後のデジタル化・処理の効率化と大量処理の際のボトルネックとなる。

Copyright 2021 Japan Digital Trust Forum

(2) デジタル化における課題（法人口座開設の例）

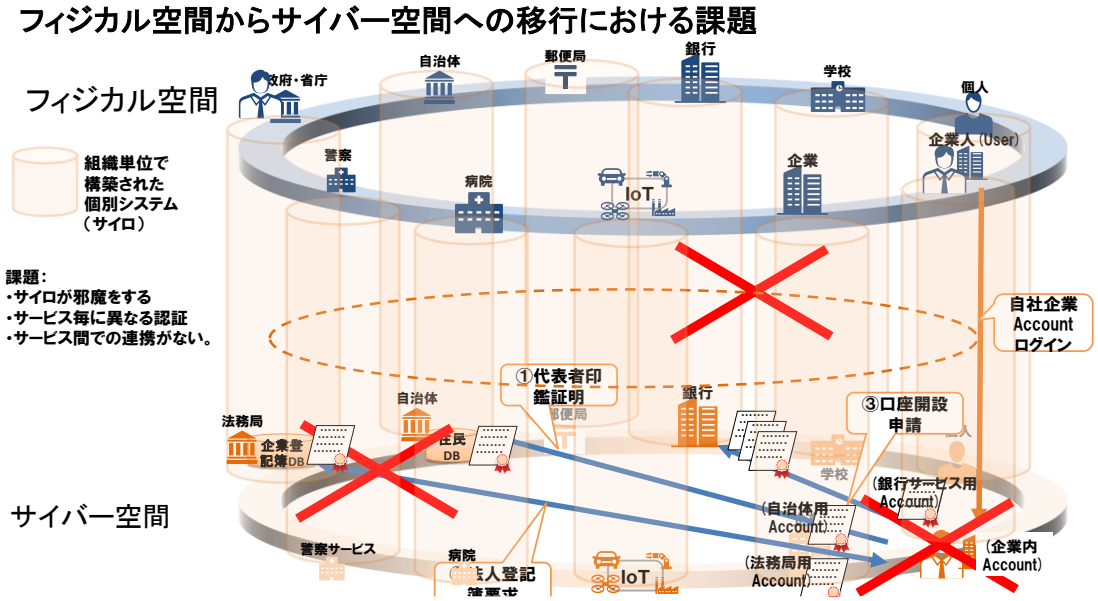


図 6 サイバー空間移行時の課題

図 6 は、現状の紙の書類による手続きをサイバー空間に移す場合の課題を説明する図である。企業から法務局に商業登記簿謄本（履歴事項全部証明書）および印鑑証明の申請をサイバー空間で行おうとする場合、企業や法務局、銀行など各組織単位で構築された範囲（サイロ）で設けられたファイアウオールで閉じたサイロ型の個別システムごとに異なる、ID や ID ごとの権限管理などの整合性などの課題、あるいは、各個別システム間のデータのトラストを確保する仕組みが異なることなどにより、他のサイロ型のシステム間で適切な編集・加工を行うために必要となる対策やそのための仕組みが確立されていないため、データのトラストを相互に確保することは困難である。このため、図 6 の破線で示したような、企業と法務局、企業と銀行というような異なる組織間でのデータの受け渡しをトラストに行うことは現状では困難である。

それぞれのサイロごとに異なる認証、トラストの確保を解決しない限り、サイバー空間での手続きへの移行は困難である。

(3) デジタル化移行後の姿（法人口座開設の例）

これに対し、DFFT、Society5.0 で目指す理想の世界を、図 7 に示す。利用者がフィジカル空間でスマートフォンやパソコンなどから所定の手順に従ってログインし、処理を開始するだけで、サイバー空間内で企業から法務局に対して申請が行われ、法務局から結果がサイバー空間内で届けられる。それと必要な情報とがサイバー空間内の企業から、口座開設を

Copyright 2021 Japan Digital Trust Forum

行う銀行に書類のトラストが確保された状態で申請され、そのトラストを確認した銀行で口座が開設され、再び、サイバー空間内の情報として、企業に通知され、フィジカル空間の申請者は処理の完了を確認できる。つまり、起点としてのフィジカル空間での処理を行うだけで、サーバー空間内で情報のトラストを確保した状態で処理が完結する世界である。

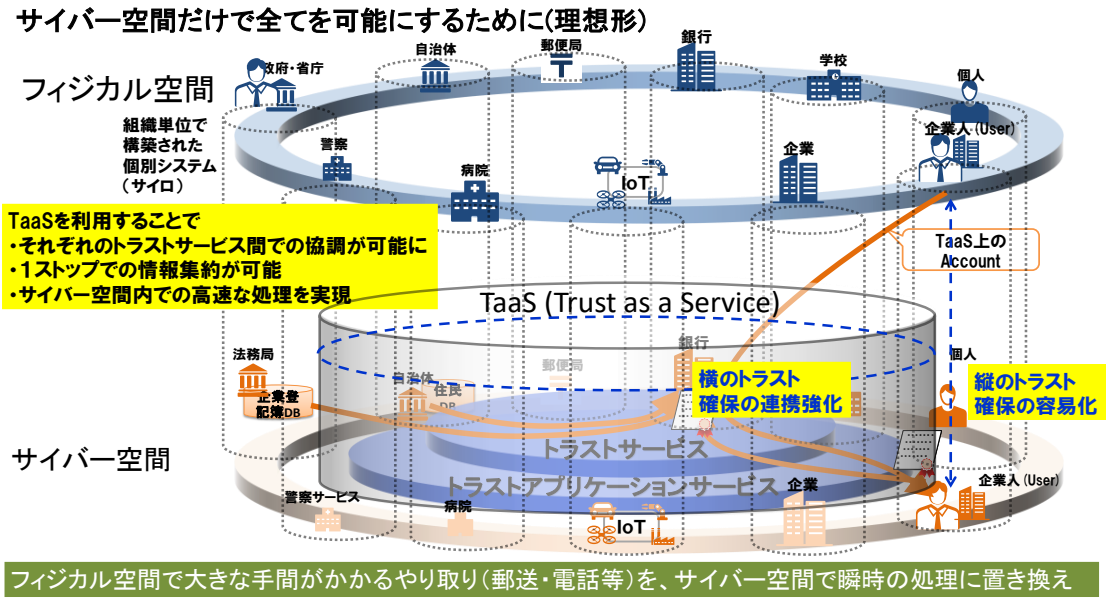


図 7 実現を目指す理想形

このような今後の DFFT、Society5.0 の展開など、一層のデジタル化を進めるためには、新たな２つの仕組みの実現が課題となる。

一つは、フィジカル空間とサイバー空間を真正性の連鎖によりつなぐ専用の仕組みを独自には構築できていないような場合にも、タイムスタンプや電子署名などのトラストサービスを容易に利用できるような仕組みである。(視点１：縦のトラスト確保の容易化)

もう一つは、現状ではフィジカル空間で行われている組織やサービス間の連携をサイバー空間で行うために、個々のサイロ型のトラストの世界から、それらの間をつなぐ世界を実現する仕組みである。(視点２：横のトラスト確保の連携強化)

このような構造(図 7)を実現することにより、ビジネス規模などによる導入の障壁を下げ、誰でも容易にフィジカル空間とサイバー空間をトラストに繋ぎ、利用することが可能となる。従来型の継続利用を可能とするとともに、新規に定義する機能を用いることで、誰もが様々な安心安全に利用可能とし、Society5.0 さらには国境も越えたトラストを実現し、DFFT を実現することを目標とする。

Copyright 2021 Japan Digital Trust Forum

4　デジタルトラスト実現のための技術課題

本セクションでは、前述の技術課題を踏まえつつ、デジタルトラストを実現するための課題を述べる。

図 8 では、サービスは、人・組織・モノ等などの実体（エンティティ）と、プロシージャ・システムの組み合わせで実現されるものとしている。このサービス間で、データの送受信を行うことで、複数組織・企業等をまたがる手続きを実現する技術課題に関するモデルを図 8 は表している。

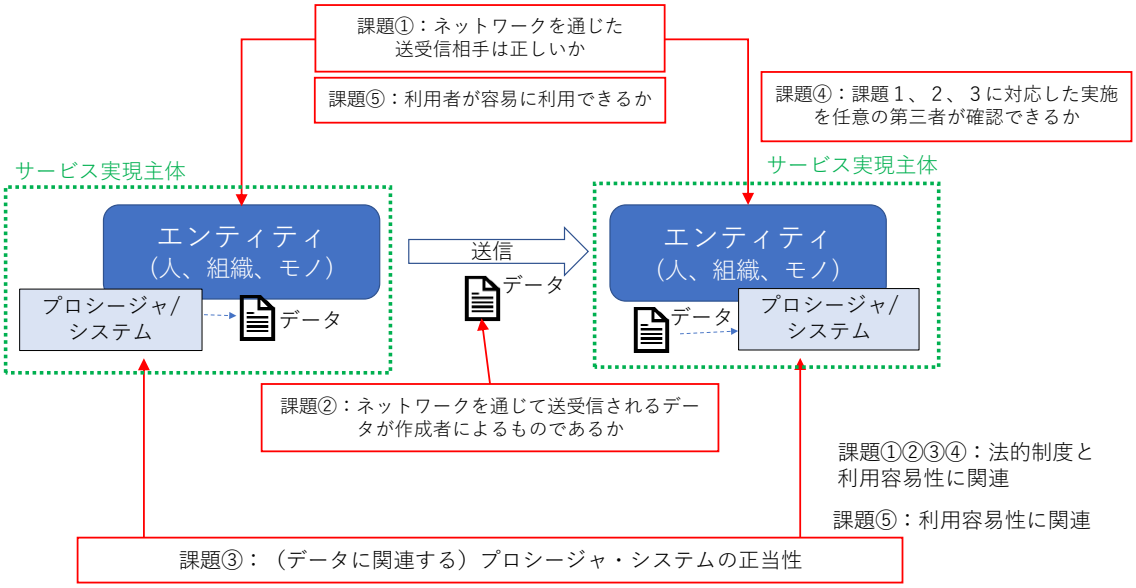


図 8 デジタルトラスト実現のための課題モデル

図 8 は、デジタルトラストの定義である「ネットワークを通じた送受信の相手の真正性、データの完全性、などが確保され、当事者および第三者による検証等を可能とするとともに、プロシージャ・システムの正当性に関しても当事者および第三者による検証可能性を有すること」を実現するためのモデルである。

「何も信じない」ことを前提とするゼロトラストの考え方に基づいてデジタルトラストを実現するにあたっては(1)送受信する相手が意図した相手であるか、(2)送受信するデータが間違いなく送受信されるか、(3)送受信するデータはそもそも正しい生成過程を経たものか、当事者および第三者による検証等を可能とするか、もしくは当事者および第三者による検証可能性を実現するとともに、これらが実現された場合の法制度による有効性を与えることが重要である。

さらに、デジタルトラストの狙いとしては、デジタル化された手続き全体に一定水準の堅牢化・確実化（堅確化）を実現することであり、そのために利用容易性を高めることも重要

Copyright 2021 Japan Digital Trust Forum

である。

利用容易性に対する視点としては、図 9 がある。これは、政府の成長戦略会議 第９回の配布資料[29]に示されたものである。この図には、「to be」として、「人にやさしいデジタル化の推進」とあり、国民と国・自治体、準公共さらには民間との、「徹底した UI・UX／国民向けサービスの実現」とある。これらを実現することが大きな課題のひとつである。

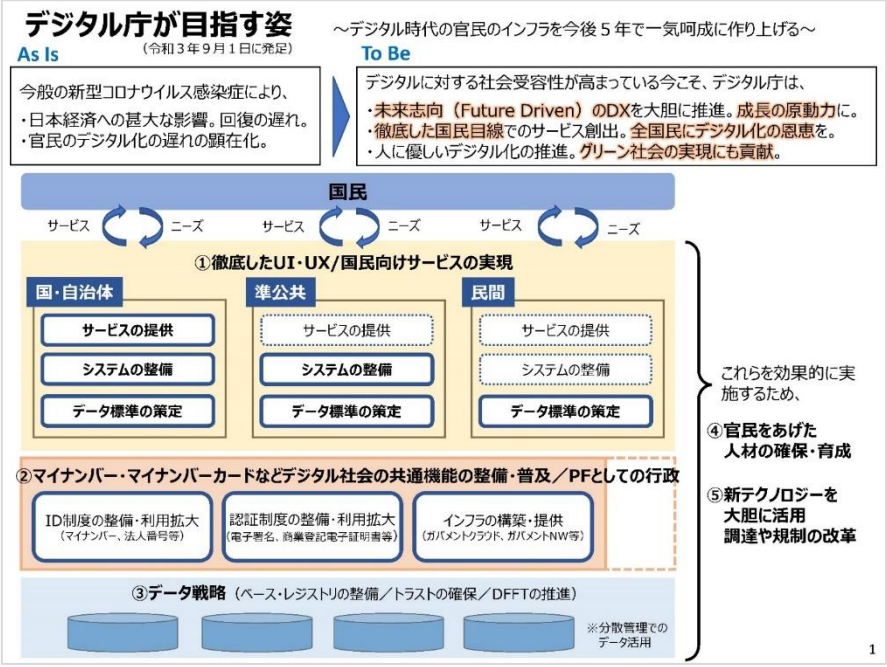


図 9 デジタル庁が目指す姿（成長戦略会議 第９回 資料）

これらを踏まえると、デジタルトラスト実現における技術課題は、図 8 に基づき以下の課題①～⑤のように整理できる。

【課題①：送受信相手は正しいか】

視点１，２両方に対応。

まず、データを送受信するエンティティに着目する。ここで重要となるのは、相互に相手が何者であるか、正当な相手であるかの真正性の確認である。このエンティティの真正性の確保がすべての基本となり、これを前提にデータの受け渡しにまでつながっていく。この真正性を確保する機能の実現が第一の課題である。

---

[29] 内閣官房、成長戦略会議（第９回）、資料４「デジタル社会の実現に向けた取り組み」（令和３年４月１２日）
https://www.cas.go.jp/jp/seisaku/seicho/seichosenryakukaigi/dai9/siryou4.pdf

Copyright 2021 Japan Digital Trust Forum

【課題②：送受信するデータは正しいか】

視点２に対応。

次は、送受信されるデータ自体が、正しいデータで正しく送信され、正しく受信され、送信されたものと一致するものであるかというデータの完全性の確保が第二の課題である。これが確保されないと、当事者間の取引や情報共有を行うことはできない。

【課題③：データに関連するプロシージャ・システムの正当性】

視点２に対応。

三つめは、プロシージャ・システムに関するものである。これは、送受信されるデータに関するプロシージャ・システムの正当性が確保できなければ、サービス・手続き、これらによって実現される産業活動や、そこで創出される価値に信頼をもたらすことができないため、この正当性の確保が第三の課題である。

【課題④：課題①，②と課題③を検証できるか】

視点１，２両方に対応。

デジタルトラストの真価を発揮させるのは、上記の課題①と課題②を解決することで実現される、送受信相手の確認によるエンティティの真正性の確保、エンティティ間で送受信されるデータの完全性の確保を、必要とする任意の第三者にとって検証できるとともに、受信されるデータに関するプロシージャ・システムの正当性に関しても、当事者および任意の第三者による検証可能性を実現することが第四の課題である。

【課題⑤：利用者が容易に利用できるか】

視点１，２両方に対応。

上記の課題①～課題⑤を解決し、多様な利用者・サービス提供者でのデジタルトラスト実現を支える上で不可欠となるのが、利用者にとって容易に利用することができる仕組みの実現が第五の課題である。

Copyright 2021 Japan Digital Trust Forum

Ⅴ　解決に向けた機能提言

Ⅳ章で示した課題を解決するためには、従来のように直接、タイムスタンプや電子署名などのトラストサービスを利用するだけでなく、図 7 のように、フィジカル空間とサイバー空間をトラストの連鎖によりつなぐ新たな仕組みの実現が課題となる。これにより、トラストサービスを直接利用する形でフィジカル空間とサイバー空間をトラストにつないでいた従来からの機能の継続的な利用に加え、従来は十分に利用できていなかったフィジカル空間とサイバー空間をトラストにつなぐ範囲を拡大することを可能とする仕組みの実現を目指す。

この層として新規に提言する部分のみを、より具体的に示すと、図 10 のような構成となる。つまり、従来の個別の仕組みとして作成されていたものに加え、トラスト利用容易化機能、トラストアプリケーションサービス層と、トラストサービス層に整理し、それぞれの役割を明確化することでフィジカル空間とサイバー空間をつなぐ仕組みを新たに定義する。（視点１の解決）

トラスト利用容易化機能を加えることで、トラストアプリケーションサービス層と、トラストサービス層の利用・連携を促進することで、フィジカル空間とサイバー空間をトラストの連鎖によりつなぐ仕組みや、個々のサイロ型のトラストの世界からそれらの間をつなぐ仕組みを提供する（視点２の解決）

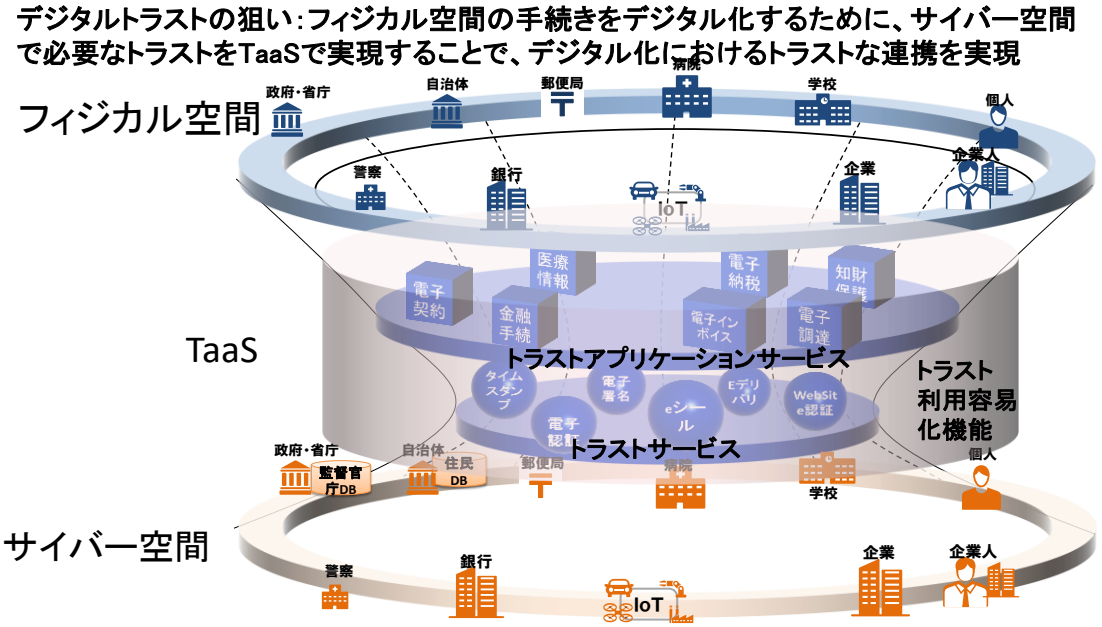


図 10 実現を目指す新たな仕組み：TaaS

Copyright 2021 Japan Digital Trust Forum

これらの 2 つを解決する仕組みを実現することで、利用者が一度ログインしただけで、企業・組織をまたいだ手続きをすべてサイバー空間内で、短時間で効率的に大量の手続きを実現することが可能となり、Society5.0 や DFFT を世の中に広めることが可能となる。これを実現する仕組みとして、我々が提言する TaaS(Trust as a Service)を、以下に説明する。

1 TaaS（Trust as a Service）とは

TaaS (Trust as a Service)とは、IV 章で示したデジタルトラスト実現に向けた課題①から⑤を解決するための手段であり、図 11 のようにサービス型として提供される。TaaS は、課題①～⑤を解決するための機能として、それぞれ解決①～⑤に対応する機能を有する。解決①～⑤の詳細は、V.2 章”TaaS の構成”で述べる。

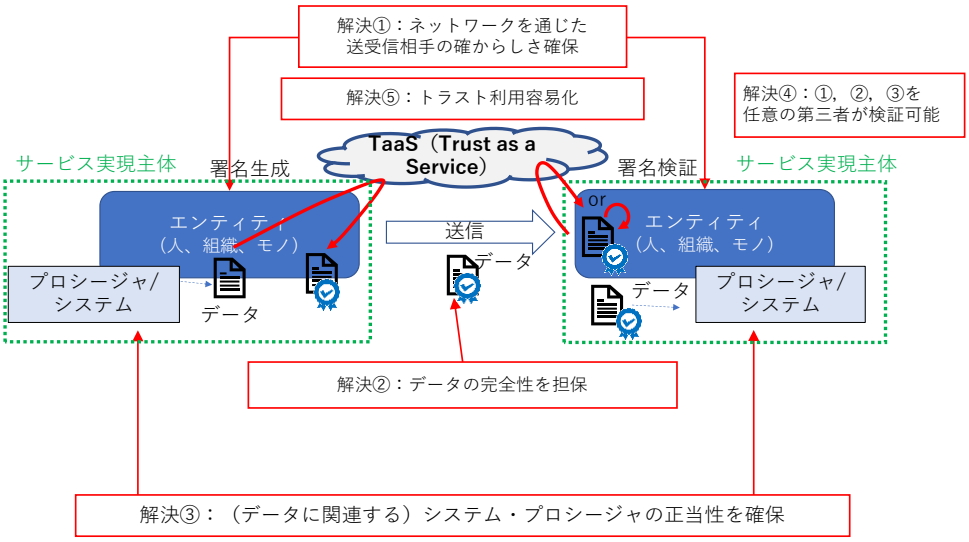


図 11 TaaS(Trust as a Service)によるサービス型のデジタルトラスト実現

TaaS は、デジタルトラストを実現するためのデジタルシステムである。TaaS がどのような効果がもたらすかを、図 12 を用いて説明する。

Copyright 2021 Japan Digital Trust Forum

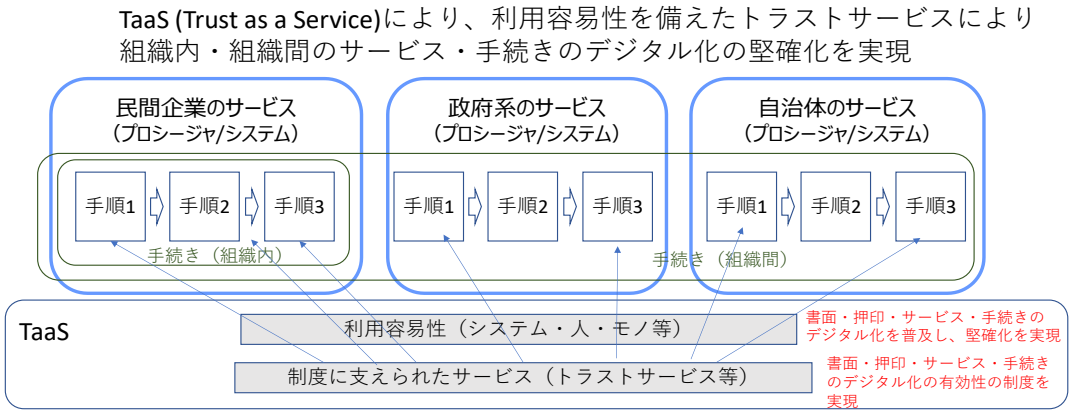


図 12 デジタルトラストを実現するための TaaS

TaaS は、書面・押印・サービス・手続きのデジタル化に伴い置き換わるデータの信頼性の確保、およびデジタル化における利用容易性を高めることであり、これによりデジタル化されたサービス・手続き全体に一定水準の堅確化を実現することを狙う。

前者のデータの信頼性の担保については、書面・押印・サービス・手続きのデジタル化に伴な法的な制度の整備により実現する。制度の有効性はトラストサービス等の法制度に支えられたサービスで担保する。後者の堅確化については、TaaS を利用する組織・システム・人・モノに対して、リモート型サービス等の利用容易性に関する機能を提供することで実現する。

前者によりデジタルトラストの制度的な有効性を担保し、後者によって組織・システム・人・モノにデジタルトラストを広く利用可能とさせることで、TaaS はデジタル化されたサービス・手続き全体に対して、一定水準の堅確化をもたらすデジタルトラストを実現するためのデジタルシステムとしての役割を果たす。

Copyright 2021 Japan Digital Trust Forum

2 TaaSの構成

TaaS の機能構成を図 13 を用いて説明する。TaaS はトラストサービス、利用容易化機能、トラストアプリケーションサービスの3つから構成される。

本書におけるTaaSのトラストサービスとは、サイバー空間でのデータのトラストを実現する電子認証、電子署名[30]、リモート署名、eシール[31]、タイムスタンプ[32]、eデリバリー、Web サイト認証、および 署名検証サービス、等を指す。これらは従来から eIDAS 等で知られるトラストサービスであり、書面・押印のデジタル化に伴う制度的な有効性を支える。

利用容易化機能は、図 11 の解決①～解決⑤を実現する機能であり、TaaS を利用する組織・システム・人・モノに対して、リモート型サービス等の利用容易性を実現することで、堅確性を実現する。利用容易化機能は、トラストサービスと連携することで、制度的な有効性に支えられた堅確性を実現する。

トラストアプリケーションサービスは、電子契約や電子調達等、特定の業務に関連したサービスである。トラストアプリケーションサービスは、トラストサービス、もしくは利用容易化機能と連携することで、トラストアプリケーションで対象とする特定業務に関して、制度的な有効性に支えられた堅確性を実現する。

全てのTaaSの機能は、機能ごとの利用確認において必要となる認証・認可機能を介して、アクセスすることができる。また、すべてのTaaSの機能は、信頼性に関する一定基準を満たすことで、機能の動作に関して一定の保証を与えることができる[33]。

---

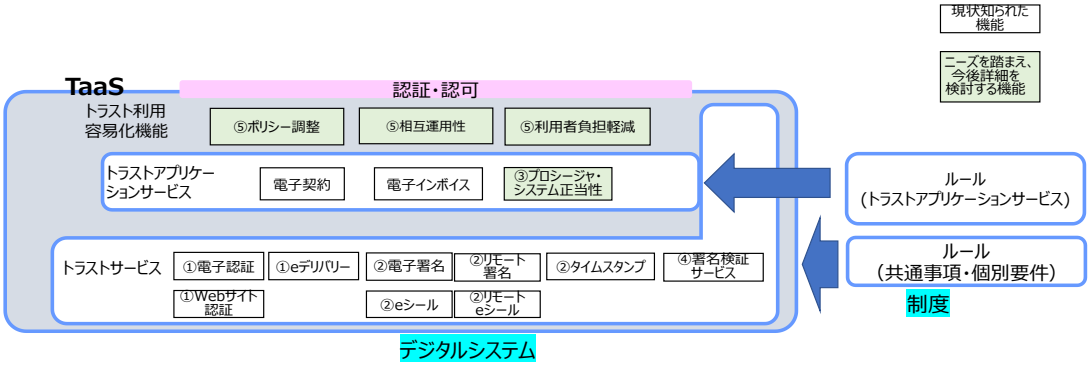
[30] 意思表示としての「主体・意思」を証明

[31] 発行元としての「事実・情報」を証明

[32] 存在としての「存在・時刻」を証明

[33] この一定基準については、国内さらには海外も含めた「信頼性を評価するための基準整備」が不可欠であり、その整備も喫緊の課題である

Copyright 2021 Japan Digital Trust Forum



トラストアプリケーションサービス：トラストサービスの応用サービス
トラストサービス：電子認証、電子署名 、リモート署名、eシール 、タイムスタンプ 、eデリバリー、Webサイト認証、および 署名検証サービス、等を指す
トラスト利用容易化機能：トラストアプリケーションサービス、システム・サービス、および実空間から自らの目的に合わせて、トラストサービスを容易に利用するための補助機能

図 13 TaaS の機能構成

【解決①：相手先信頼レベル確認】

サイバー空間において、データをやり取りする相手を確認する方法として、データ受信者がデータに付与された電子署名を検証することで、データ送信者の確からしさを確保する方法が一般的である。このように、現状はデータ受信者がデータを受信した後にデータ送信者の確からしさを確認する方法のみで、データ送信者視点で相手の確からしさを確保する仕組みが無い。そのため、データ送信者の意図しない相手に対してデータを渡してしまうリスクがある。そこで、課題①の解決に向けて、データ送信者がデータを送信する前にデータ受信者の確からしさを確認する仕組みが必要となる。

例えば、データ送信者がデータ受信者を識別する ID を基に問合せると、データ受信者に対して ID を発行した際のデータ受信者の身元確認保証レベル（Identity Assurance Level、IAL)などからデータ受信者が信頼できるか否かを返すことで相手の確からしさを確認できる、といった方法が考えられる。このような仕組みを API 等によるリモート型のサービスとして提供することで、システムや利用者にとっての利用容易性を向上する。

- 電子認証：サイバー空間の ID に対する実在性確認
- e デリバリー（ERDS)：送受信するデータの完全性、識別される送信者による送信が行われたこと、識別される受信者による受信が行われたこと、QERDS による送信・受信の日付・時刻の正確性さを保証。

Copyright 2021 Japan Digital Trust Forum

【解決②：データ完全性確保】

送受信されるデータが同一のものであり、信頼できるものであることを確保することが必要である。このときにポイントとなるのは、認証されたIDに対して、データ・情報等へのアクセス権限を特定する認可（認可保証）を受けたうえで、送受信されたデータであるか否かということである。また、送信から受信までの間での改ざんがされていないことを確保できるか否かである。この2点を確保する仕組みが不可欠となる。

電子署名でデータの非改ざん性を確保するにあたり、日本において法的根拠となる電子署名法では対象を自然人としており、課題②の解決に向けて、組織やモノが発行するデータの完全性を確保する仕組みを法制度の整備込みで検討する必要がある。また、電子署名を付与するクラウドサービスの観点では、データの完全性を確保する仕組みに必要な電子署名の付与、署名検証等に関するAPIを適切に設けることで、リモート型のサービスとして提供することで、システムや利用者にとっての導入容易性を向上する。

また、ベース・レジストリ等の、情報を保有するシステムと連携して、発行されたIDに関連する属性データをベース・レジストリに格納・参照する際に、ベース・レジストリの情報に対してデータの完全性を確保し、もたらされる情報を利用者が安全に活用することも重要である。このような例については、V章の「6TaaSユースケース」にて後述する。

- 電子署名（リモート署名）：個人によるデータ内容の完全性を確保
- eシール（リモートeシール）：組織によるデータ内容の完全性を確保
- タイムスタンプ：データが存在した時刻に関する完全性を確保

【解決③：プロシージャ・システム正当性】

サイバー空間上のデータでは、「誰が・何を・いつ」作り出したものであるか、を明らかにすることでデータに対するトラストが確保（例えば、データを誰が提供したか、データが改ざんされていないか）されることが必要である。このためには、データが適切なプロシージャで生成されたことを確保する仕組みや、システムを構成するモジュール・コンポーネントの確からしさを保証するための仕組みも必要となる。つまり、「どうやって」作り出したか、を明らかにすることでデータの取扱いプロシージャの正当性を確保することができる。

例えば、複数の組織や企業が関連する手続き、サービス、サプライチェーンやデータの生成手順に複数の人・組織・モノが関係する場合では、関係する人・組織・モノの確からしさだけでは無く、順序も重要となる。例えば、関係する人・組織（主体・意思）・モノ（事実・情報）がデータを操作するたびに電子署名とタイムスタンプ（存在時刻の信頼性）を付与することで、電子署名により本人の確からしさを、タイムスタンプによりデータの操作した時刻を保証することで、プロシージャの正当性を確保する機能である。このような仕組みをAPI等によるリモート型のサービスとして提供することで、システムや利用者に対する導入容易性を向上する。

Copyright 2021 Japan Digital Trust Forum

内閣府・法務省・経済産業省の三省による「押印に関するＱ＆Ａ」（令和２年６月１９日）では、文書の成立の真正を証明する手段を確保するための方法がいくつか例示されている（Ｑ６）。この例示においては、電子署名や電子認証などのサービスはもちろんのこと、継続的取引における「取引先とのメールの送受信記録の保存」や、新規の取引における「文書や契約の成立過程（メールや SNS 上のやりとり）の保存」など、すなわち契約や請求にいたる成立過程が、文書の成立が真正であることの立証手段として示されている。

このＱ＆Ａでは記録を残す方法として、メールの送受信記録や SNS が言及されている。本機能により、文書の成立過程としての文書成立のプロシージャも含めた確からしさのある情報を汎用的に残せることとなり、文書成立の真正を証明するための手段として、より確からしさと利便性の高い手段が選択できることとなる。

上記のように、プロシージャやシステムの正当性確保には様々な方法が考えられるが、詳細はニーズを踏まえて今後検討する。

【解決④：④任意の第三者による検証】

デジタルトラストにおいては、課題①、課題②、課題③を解決する仕組みを使っているか否かを任意の第三者が遠隔から検証出来ることが必要になる。そのため、相手の確からしさ確保の仕組み、データの完全性を確保する仕組み、プロシージャ・システムの正当性を確保する仕組みが使われていることを、検証しようとする任意の第三者が検証可能とする仕組みが不可欠となる。利用者が用いているシステム・サービスに依存しない、データのみを用いた第三者検証により、デジタルトラストで実現する堅確化の水準を一定以上に保つとともに、このような仕組みを、従来型のローカルな検証に加えて、任意の第三者が利用可能な API 等によるリモート型のサービスとして提供することで、組織・システム・人・モノに対する利用容易性を実現する。さらに、任意の第三者が検証可能とすることで、データを生成・送受信・データ利用時点だけでなく、将来の時点でも検証可能となる。これは、サービス・手続きにおけるデータ利用時点だけでなく、データ利用後にも任意の第三者が検証可能とすることで、堅確化の水準をさらに高めることができる[34]。

例えば、①におけるデータ受信者の確からしさに対する検証では、利用者に返された「相手を信頼できるか否か」という結果を判断した根拠を第三者に提示する。この場合、データ受信者の身元確認保証レベル（Identity Assurance Level、IAL)や認証の確からしさを示す当人認証保証レベル（Authenticator Assurance Level、AAL)、といった基準に沿った情報を提示する。組織やモノ、プロシージャ、システムに関しては、国内においてトラストを判断する法的根拠が確立されていないため、まずは法制度の整備が求められる。

---

[34] 長期署名（Long term electronic signatures）等の実現手段が知られている。RFC3126(https://datatracker.ietf.org/doc/html/rfc3126)等で定義

Copyright 2021 Japan Digital Trust Forum

【解決⑤：トラスト利用容易化】

トラストサービスやトラストアプリケーションサービスを導入・運用するための利用容易性[35]を確保することで、トラストを確保したデジタル化の促進普及を実現する。利用容易性を実現するために、多くの利用者にとって共通する課題解決の仕組みを、Trust as a Service として提供することで、トラストを確保したデジタル化における社会全体のコスト最適化の実現を狙う。

現状の検討状況は以下であるが、詳細はニーズを踏まえて今後検討する。

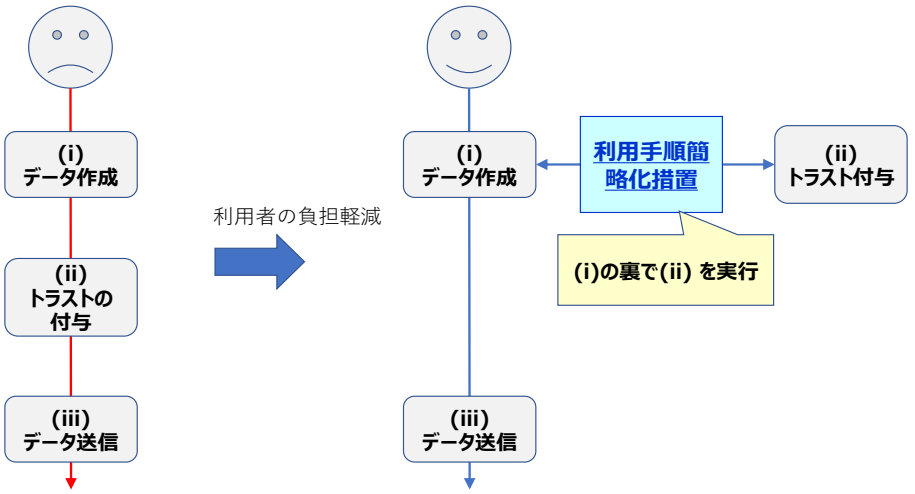
- ポリシー調整： フィジカル空間の手続きの厳格さに応じて求められる、ルールおよび制度に応じたトラストサービス導入を支援する機能検討を深堀することで、利用者にとっての導入負担を軽減する。
  - 複数のトラストサービスを連携して特定の手続きを実現する際に、それぞれのトラストサービスのポリシーの統一化を図る機能を想定している。
- 相互運用性：API、データ、サービスやアプリケーション等の互換性確保による、トラストを確保したデジタル化の促進普及を実現する。
  - サービス間の互換性の例：電子契約を用いた入札に応募したい企業が、自社で利用している電子契約サービスが入札で用いられている電子契約サービスと互換性がない場合、応募できない可能性があり（電子契約の互換性がビジネスに影響）、電子契約に互換性をもたらすためのサービス（例えば、利用者が電子契約に用いる鍵や ID を登録する共通サービス）による課題解決を検討する。
  - サービスとアプリケーションの互換性の例：人や組織等を一意に特定可能な ID・番号の体系が、認証局等のサービスとビジネスアプリケーションで異なる場合、電子署名や e シールの検証結果の正しさをビジネスアプリケーションから判別することができない。人や組織等を一意に特定可能な ID・番号の体系の変換を実現するサービスによる課題解決を検討する。
- 利用者負担軽減：今までも電子署名やタイムスタンプは利用されているが、利用者にとっては(i)データの作成、(ii)トラスト付与[36]（例えば、署名サービスに認証してログイン、同サービスの UI 上で署名するデータを、同サービスにアップロードして署名の意

[35] 内閣官房、成長戦略会議（第９回）、資料４「デジタル社会の実現に向けた取り組み」（令和３年４月１２日）の「人にやさしいデジタル化の推進」にも呼応
https://www.cas.go.jp/jp/seisaku/seicho/seichosenryakukaigi/dai9/siryou4.pdf

[36] 相手の真正性、データの完全性、およびプロシージャ・システムの正当性を確保することを指す

Copyright 2021 Japan Digital Trust Forum

思を示す)、(iii)署名したデータを相手へ提供、の手順が必要で、利用者にとって(ii)の手続の負担を強いるものであった。そこで、利用者が行う普段の業務（例えば、行政に提出する書類の作成）の中で、(i)の裏で(ii)を実行することで、利用者の手順簡略化による負担軽減を実現する。具体的には図 14 に示すように、手続を(i)と(iii)のみにする（(i)の手続の裏で(ii)が実行される）仕組みが不可欠となる。これにより、利用者負担軽減による普及促進と、人的ミスを抑えることで堅確化を実現する。

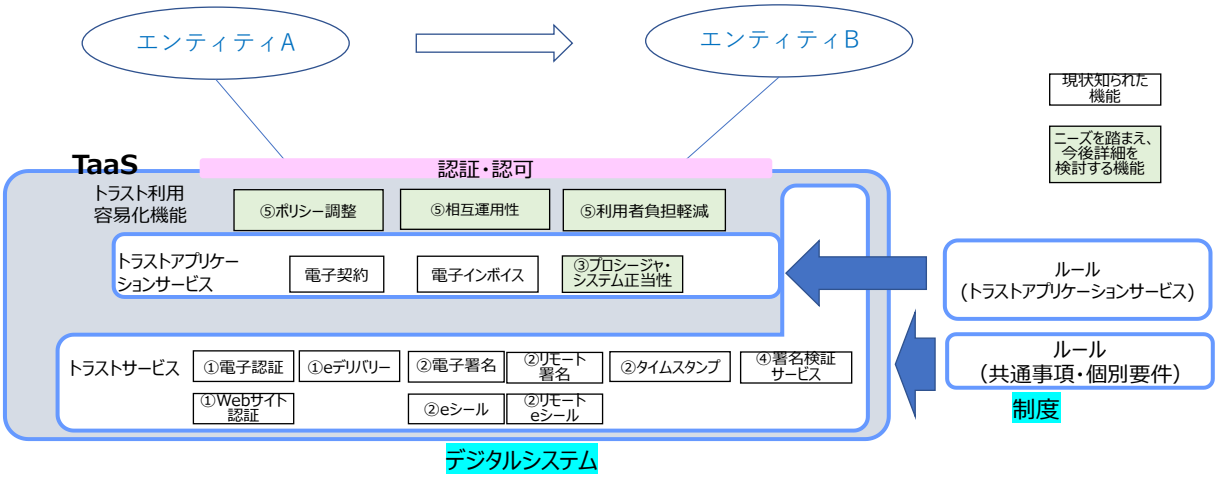


トラスト付与：相手の真正性、データの完全性、およびプロシージャ・システムの正当性を確保することを指す

図 14 利用者負担軽減を実現する仕組み

Copyright 2021 Japan Digital Trust Forum

3 TaaS の利用イメージ



トラストアプリケーションサービス：トラストサービスの応用サービス
トラストサービス：電子認証、電子署名 、リモート署名、eシール 、タイムスタンプ 、eデリバリー、Webサイト認証、および 署名検証サービス、等を指す
トラスト利用容易化機能：トラストアプリケーションサービス、システム・サービス、および実空間から自らの目的に合わせて、トラストサービスを容易に利用するための補助機能

図 15 TaaS の基本的な利用イメージ

TaaS の基本的な利用イメージを図 15 に示す。TaaS を、API 等を介して呼び出すことで、エンティティ A からエンティティ B への署名押印に置き換わるデジタル化としてのデータの送信においてトラストの確保を実現することができる。トラストの確保については、書面・押印のデジタル化に伴う法的な有効性を与えることができるとともに、トラスト利用容易化機能によるものであり、デジタル化された手続き全体に一定水準の堅確化を実現する。

TaaS は、Society5.0 を支えるための、デジタルトラストを実現するためのサービスとしての役割を果たすことから、データ連携基盤や個別業務アプリケーションと連携することが多いと考えられる。データ連携基盤や個別業務アプリケーションと TaaS の連携を図 16 に示す。

データ連携基盤とは、日本政府が Society 5.0 実現のために推進している分野横断でデータを利活用するための基盤であり、広義には官民に関わる様々なステークホルダーが有するデータを連携させ、分野横断でのデータ利活用を可能にするものである。

トラストアプリケーションサービスは、信頼性に関する一定基準を満たすことで、アプリケーションの動作そのもののトラストを確保することができる。これに対し、個別業務アプリケーションは任意のアプリケーションであり、TaaS を利用することで、アプリケーションで取り扱うデータのトラストを確保することができる。

図 16 のような場合において、人・組織・モノ等のエンティティが TaaS を利用するパタ

Copyright 2021 Japan Digital Trust Forum

ーンは、以下の(i)(ii)であり、TaaS の機能ごとに求められる認証・認可を介して、TaaS を利用することができる。どのような利用するパターンが適しているかは、ユースケースごとに異なる。

(i) 直接利用
(ii) 個別業務アプリケーションとデータ連携基盤等のいずれか、もしくはいずれもを介する

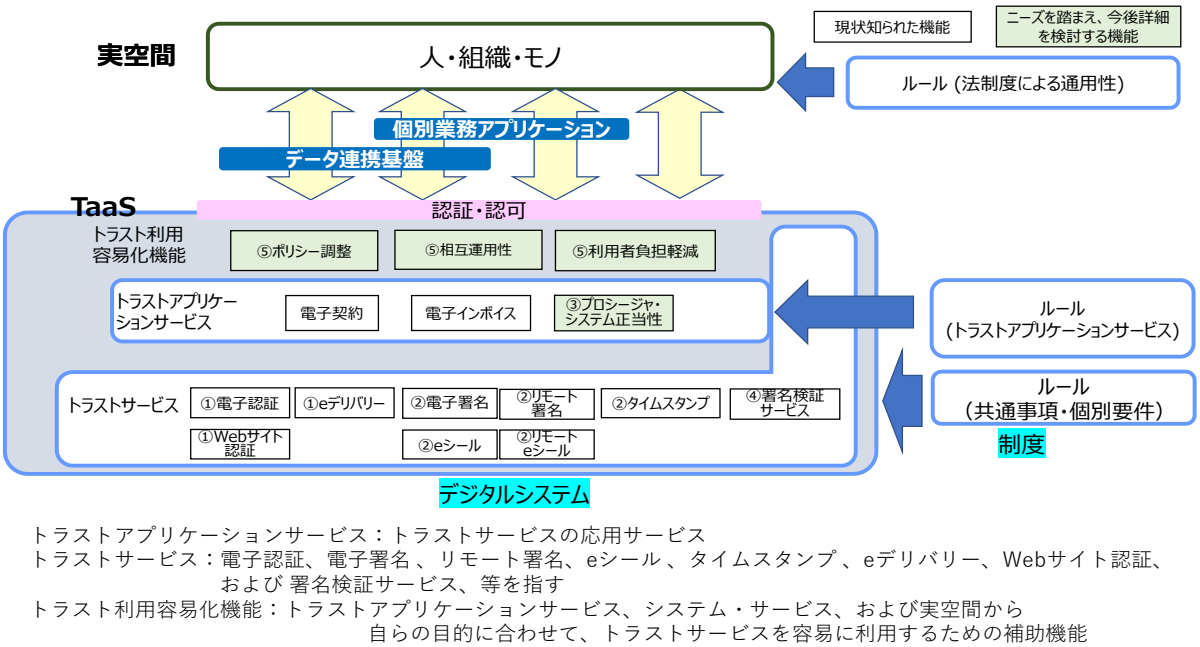


図 16 TaaS の利用イメージ（データ連携基盤・個別業務アプリケーションとの連携）

4 TaaS の効果

- 効果１：堅確化
  手続きに用いられる署名・押印のデジタル化に伴い、相手の真正性・データの完全性の検証、および関連するプロシージャ・システムの正当性に関する検証可能性を、利用容易性が高い TaaS の機能により実現することで、企業や官公庁・自治体の間のサービスや手続きを堅確化することができる。例えば、コネクテッド・ワンストップによる電子手続きや、電子化された請求書がいつ・どの組織によって発行されたかの真正性をオンラインサービスとして容易に確認することができる。
- 効果２：効率化
  従来、書面・電話・ファクシミリ等、物理的手段に依存していた手続きを、デジタル化サービス型として実行する際に、機械可読などを組み合わせ前述の手続きを自動

Copyright 2021 Japan Digital Trust Forum

的に実行可能とすることで、手続き全体の効率化を実現する。例えば、官公庁・自治体・企業が保有するベース・レジストリのデータに関して、データの完全性の検証、およびデータ流通に関連するプロシージャ・システムの正当性に関する検証可能性を、デジタルトラストの実現により担保することで、コネクテッド・ワンストップによる電子手続きや、（ベース・レジストリに格納された登記情報などを用いた）民間のオンラインサービスを効率化することができる。

- 効果３：リスク対応
  組織や人が提供するサービス・手続きが、与えられた業務ルールや契約手順等で規定された正しい手順により実行していることを表明することで、リスク対応を行うことができる。このような考え方は、サプライチェーンにおいて、エンティティやプロシージャ/システムが Trustworthiness[37]を満たしているかの検証に利用できることが期待される。
- 効果４：疑義に関する確認
  企業や官公庁・自治体において、相手方との契約、それにもとづく資金の請求、請求書を受けての支払いといった手順は数多く発生している。さまざまな相手と取引を行う必要のある官公庁・自治体・企業にとっては、中には疑義が生じるものや、係争に巻き込まれるものがあり、それを無くすることはできないのが現実である。デジタルトラストによって、これらの予防策を推進していくことの重要性は言うまでもないが、それと並行して、このような事態が発生してしまった際に備えて、自らがよりどころとする文書（デジタル文書を含む）の成立が真正であることを証明できるようにしておくことが重要となる。

5　TaaS の利便性：高い身元確認レベルの ID のオンライン発行とリモート署名

本ホワイトペーパーでは、高い身元確認保証レベル（Identity Assurance Level, IAL）と利用容易性の実現が、TaaS の普及において重要であると考え、その例を図 17 を用いて説明する。これはリモート ID の身元確認とリモート署名の組み合わせであり、図 17 における(1)(2)(3)の手順をワンストップ、オン・ザ・フライで実現する。これにより TaaS 利用の容易性の大幅な改善が見込まれ、トラストアプリケーションの普及に資すると考えられる。

(1) 利用者はトラストアプリケーションに利用申請
(2) (1)と連動し、CA(Certificated Authority)はマイナンバーカード等によりオンライン

[37] 例えば ISO/IEC JTC 1/WG 13 では、「実証可能・検証可能・測定可能な方法で、ステークホルダーの期待に応える能力である。」と定義したうえで、「ステークホルダーの期待が満たされていることを確かなものにするための検証が必要」であることが記載される。

Copyright 2021 Japan Digital Trust Forum

で本人確認、法人登記情報や国家資格データベースなどのベース・レジストリを確認し組織名義の電子証明書や国家資格属性付き電子証明書をリモート署名サービス内に発行

(3) 利用者はトラストアプリケーションを通じてクラウド上でワンストップによる電子署名が利用可能となる。

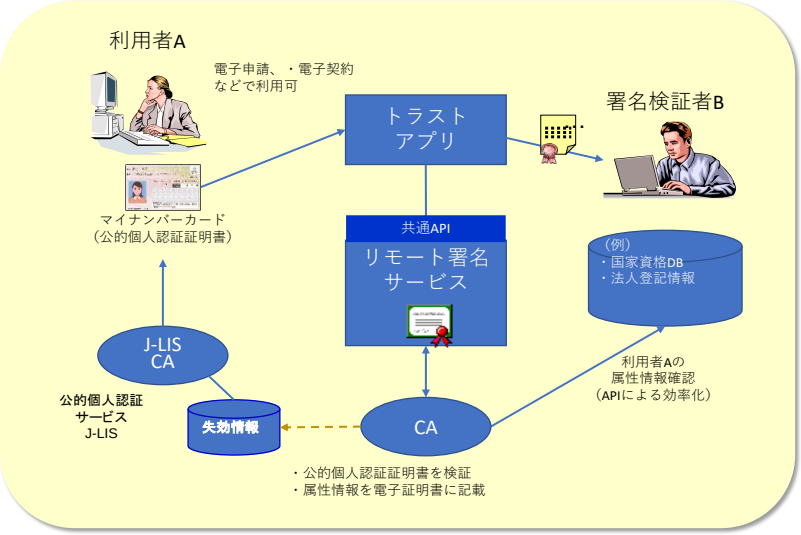


図 17 身元確認レベルと利用容易性の両方を高めた例（リモート署名）[38]

ID のスキームと電子証明書の関係を以下の図 18 に示す。UNCITRAL の"Provisions on the Use and Cross-border Recognition of Identity Management and Trust Service"では、第 1 条の定義の中で、Identity とは特定の目的のために個人を一意に特定できる属性情報のセットとしており[39]、eIDAS 規則でも同様に定義している。TaaS で取り扱う ID＝Identity の最大の特色は、実社会の自然人、組織、機器などに確実に紐づけられ、公開鍵証明書の中に本人の属性情報として書き込まれているため非改ざん性が確保されている。また、ペアとなる秘密鍵で電子署名やオンライン認証を行うことで本人性が担保され、その保証レベルは NIST SP800-63 の IAL（Identity Assurance Level）などを参照し、規定されているものとなる。

---

[38] 「総務省マイナンバーカードの機能のスマートフォン搭載等に関する検討会（第 5 回）」資料 4 より抜粋
https://www.soumu.go.jp/main_sosiki/kenkyu/mynumber_smartphone/02ryutsu02_04000356.html

[39] "Identity" means a set of attributes that allows a person to be uniquely distinguished within a particular context;

Copyright 2021 Japan Digital Trust Forum

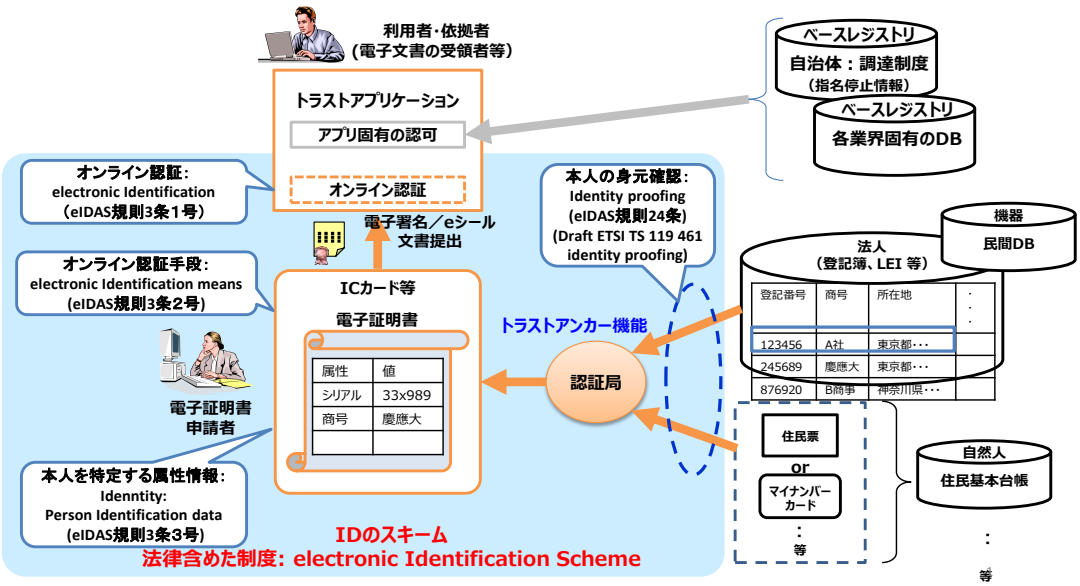


図 18 ID のスキームと電子証明書の関係

一方、一般的な Web における ID の使い方の例では、Google、Amazon、Facebook、Apple などの ID があり、実社会の個人との紐づけは強固ではなく、クレジットカードなどの決済情報を必要に応じて関係づけて利用されている。

6 TaaS ユースケース

TaaS が利用者からどのように利用されるか、TaaS の想定するユースケースについて説明する。

サービス化のために、図 11 の①から④の機能を API 化して、トラストアプリケーションやデータ連携基盤などから共通してアクセスできるようにする。これにより、TaaS をサービスや業種を問わず利用できるクラウドサービスとして提供できる。また、これらの API を工夫することで、利用者が TaaS の複雑な処理を意識せずに利用することを可能とする。

(1) 法人の銀行口座開設

図 1 および図 5 での説明に用いた法人の銀行口座開設手順について、現行の書類等を利用する場合と、TaaS による処理を利用する場合について、整理したものを図 19 に示す。

現行手順では、各種書類は発行元の押印により信頼性を担保され、金融機関に提出される。銀行は書類を受け取り、人が確認する。これを TaaS を使えば、例えば法人が銀行に対し口

Copyright 2021 Japan Digital Trust Forum

座開設依頼をデジタル上で行うと同時に、法人から官公庁に公的情報取得依頼がいき、官公庁から返ってきた法人情報を添えて、口座開設依頼が可能となる。これにより、情報を受け取った銀行は、全て機械可読情報をもとに情報の正確性を人の介在なく判断することが可能となる。官公庁でも銀行でも人の介在不要で正確かつ効率的な処理を実現できる。

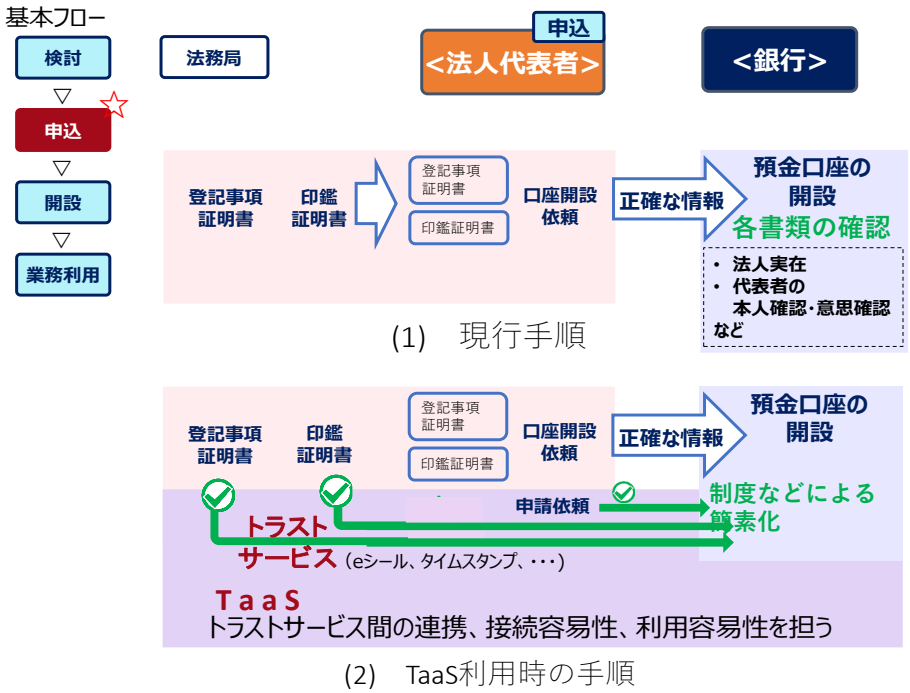


図 19 法人の口座開設手順の比較

(2) 請求書の電子化

図 20 を用いて、請求書の電子化に関する TaaS のユースケースを、①～⑤の機能をどのように利用するかを踏まえて説明する。

Copyright 2021 Japan Digital Trust Forum

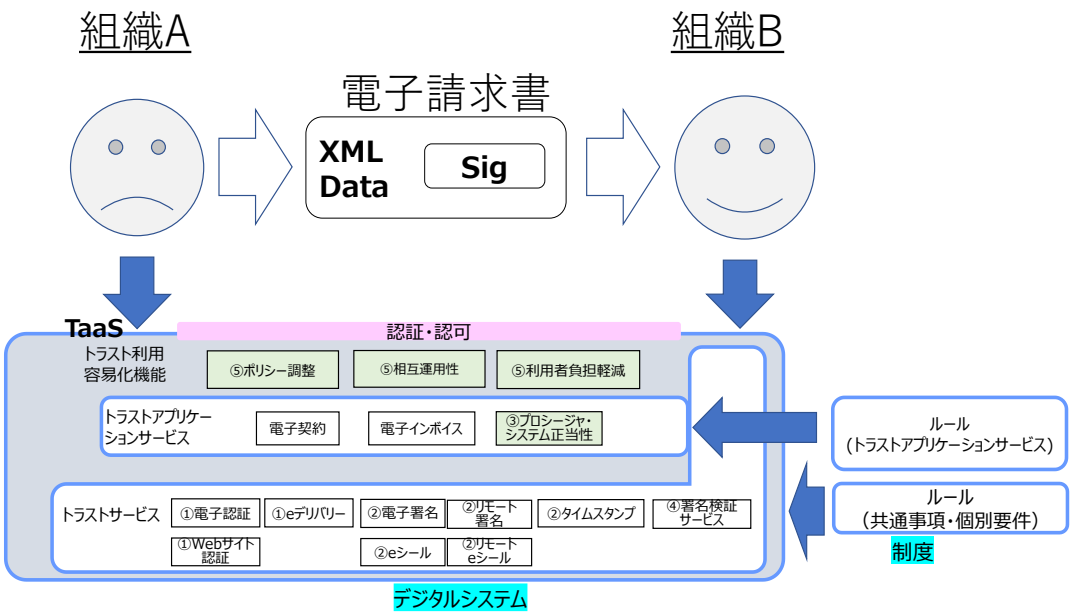


図 20 電子請求書における TaaS のユースケース

図 20 に示したように、請求書は、組織 A の担当者により生成され、組織 B に渡るものとする。電子化された請求書では、例えば XML のようなデータ形式が用いられ、電子署名を組み込むことが可能な仕様となっている場合が多い。このデータ作成および受け渡しにあたり、機能提言した 5 つの観点で、証拠の付与や検証がなされることになる。即ち、(1)誰が関わっているかの確認、(2)データへの改ざんを防止、(3)（組織Aが契約・業務手順の表明を行う場合）どんな手続で作成されたか確認、(4)トラストの根拠の確認。(5)人のスキルに依存しない確認、を実現する。

【もたらされる効果】

TaaS の機能により、組織 A と組織 B の両方にとっての電子請求書の発行・受け取り手続きの堅確化（効果１）、組織 A と組織 B 両方とっての電子請求書の発行・受け取り業務の効率化（効果２）、および組織Aが高額請求を行う場合等において、一定の手順に従い業務を遂行しているかの表明（効果３）を行うことができる。

さらに、このような請求に紐づく支払処理に関して、保険金支払い処理のような場合についても効果がある。例えば、支払者が険サービスに加入している、受け取り者が保険サービスに加入していない場合でも、④により、任意の第三者検証を実現することができるため、同様の効果が見込まれる。

Copyright 2021 Japan Digital Trust Forum

(3) TaaS 連携形態（分散 TaaS 連携）

IV 章の図 1、図 2 で示したように、様々な手続きは、多様な組織のサービスをまたがって成り立っている。これらをデジタル化された手続きとして処理するためには、それぞれが保有するデータを利用しつつ、連携する必要がある。

図 1、図 2 の例を実現する場合の TaaS の実現形態としては、中央集権的に 1 つの TaaS が存在するのではなく、国と民間それぞれに存在する TaaS による連携が必要となる。このような、国と自治体、金融機関の TaaS の（分散 TaaS）連携の全体像を図 21 に示す。

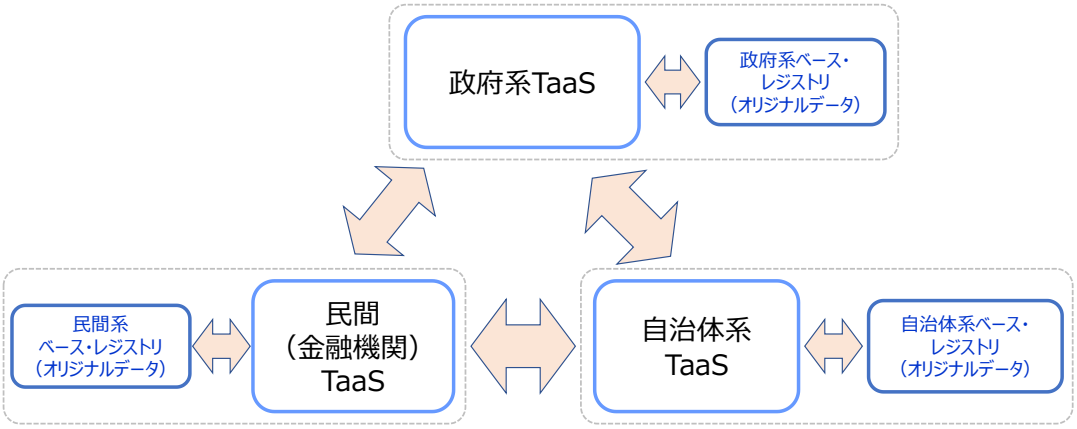


図 21 TaaS 連携形態の全体像

図 21 の全体像を踏まえたうえで、以下では、政府系ベース・レジストリ、自治体系ベース・レジストリとの連携のユースケースを記載する[40]。

---

[40] 各 TaaS、ベース・レジストリは、ベース・レジストリ間の連携を含めて、それぞれの個人情報保護・機密保護を考慮する前提。ただし、複数の TaaS 間連携においては、ベース・レジストリにアクセスする際の個人情報保護・機密保護ポリシーが互いに矛盾した結果により意図しないアクセスを許す、等の事象を発生させないための、マッシュアップ型のサービス（複数のサービスを組み合わせた新しいサービス）としての整合性実現が重要な課題である。

Copyright 2021 Japan Digital Trust Forum

(4) 政府系システムとベース・レジストリ

図 22 を用いて、政府系システムとベース・レジストリを例とした、TaaS の利用形態について説明する。

図 22 では、各種の属性情報を保管する政府系ベース・レジストリと TaaS を連携させている。政府系ベース・レジストリの情報に対して TaaS を介し e シールを行う事で、政府系ベース・レジストリのオリジナルデータから改ざんされていないことを保証することが可能となり、フィジカル空間からサイバー空間への急速な移行に必須となるデジタルトラストを実現する。

また、政府機関から政府系ベース・レジストリへの情報の追加・更新等を行う際にも、TaaS を利用して、正当な申請・手順によるものであることを確認することができる（③プロシージャ・システム正当性に関連）。さらに、ベース・レジストリのデータの発行元（②データ完全性に関連）が改ざんされていないかの完全性（②データ完全性に関連）を確認する。

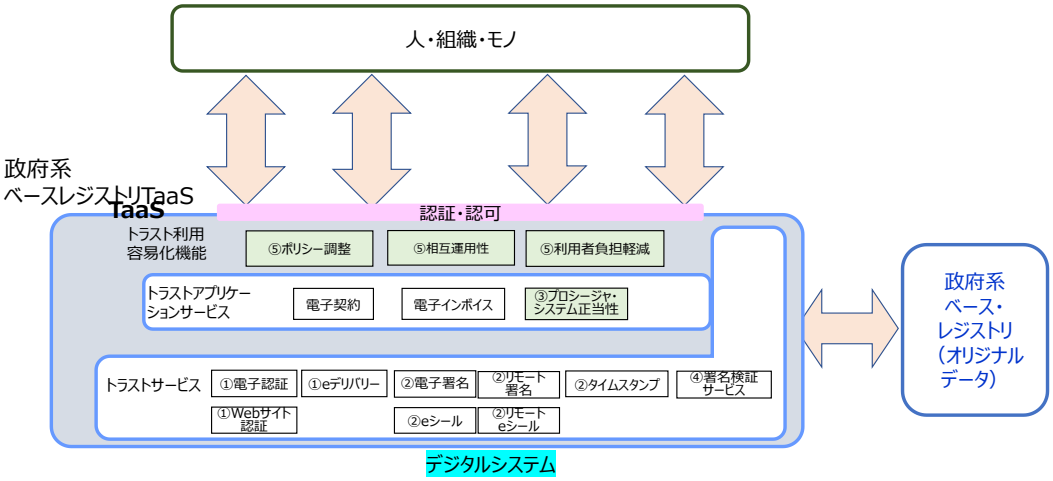


図 22 政府系システムと TaaS の連携

Copyright 2021 Japan Digital Trust Forum

(5) 国と民、国と自治体のシステムの TaaS による連携

図 23 を用いて、民間系 TaaS システムと政府系 TaaS システムと、政府系ベース・レジストリの連携を例とした、TaaS の連携形態について説明する。

TaaS の実現形態としては、中央集権的に 1 つの TaaS が存在するという訳では無く、図 23 のように複数の TaaS が連携する場合が想定される。例えば、複数の政府の TaaS、複数の民間の TaaS がそれぞれ独立して運用され、分散された TaaS 環境によって社会システムが構成されるようになると考えられる。

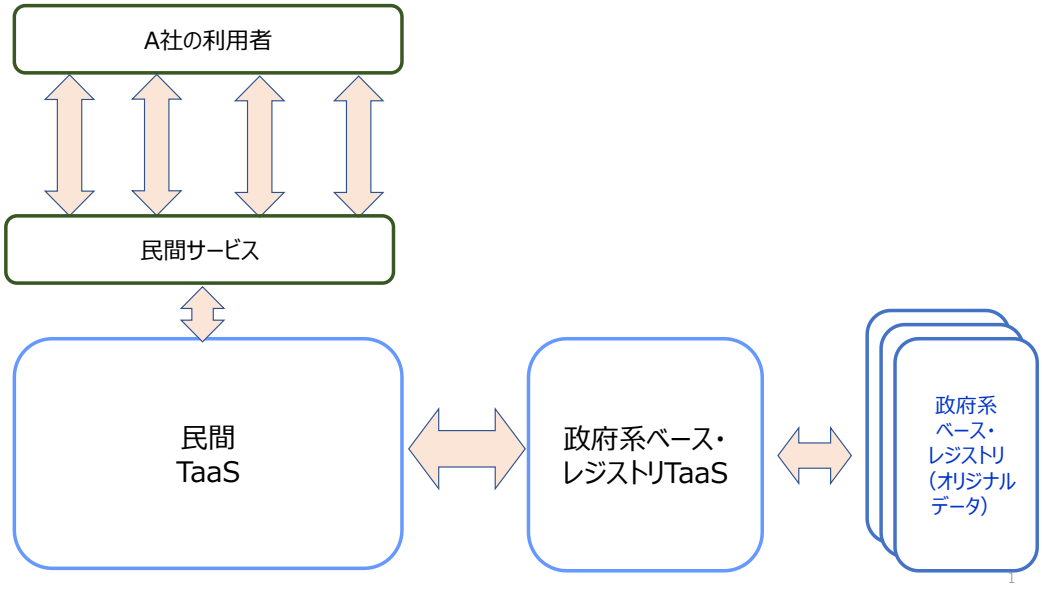


図 23 官と民の TaaS による連携

このような TaaS が分散する環境において、例えば、A 社から政府が保管する情報（例えば政府系ベース・レジストリに格納された情報）に関するリクエストを受けた場合、民間 TaaS が必要に応じて政府系ベース・レジストリ TaaS と連携することで、必要な情報を入手することが可能となる。

Copyright 2021 Japan Digital Trust Forum

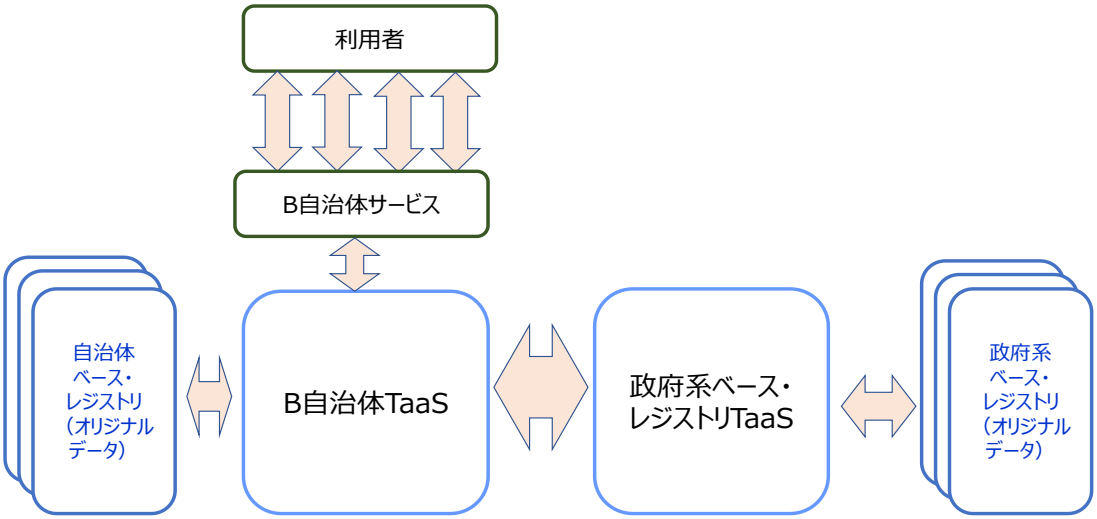


図 24 国と自治体の TaaS による連携

同様の構成は、図 24 のように、国と自治体の間の連携にも適用できる。これにより、国と自治体、それぞれの保有する情報の完全性を保証するとともに、各種手続きの処理の効率・堅確性を提供するコネクテッド・ワンストップのためのデジタルトラストを実現することが可能となる。

(6) 法人ベース・レジストリ活用による法人活動の確認

図 25 を用いて、法人ベース・レジストリ活用による法人活動の確認を行うユースケースについて説明する。TaaS と法人ベース・レジストリが連携し、公開された属性データ（プライバシーマーク、ISO 9000,14000 等）を確認することで、取引相手の実在性確認に加えて、公開された属性データ（プライバシーマーク、ISO 9000,14000 等）、購買手続において用いるデータ等を参照することによる法人活動を確認する基盤を実現することができる。

Copyright 2021 Japan Digital Trust Forum

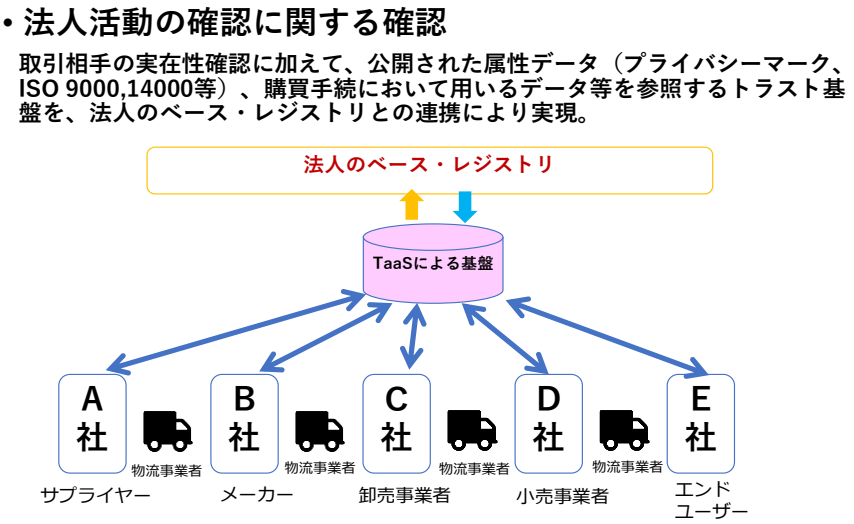


図 25 ベース・レジストリ連携による法人活動の確認

【もたらされる効果】

TaaS の機能により、取引相手の法人に対する疑義の確認を、オンラインサービスにより効率的に実現することができる（効果４、効果２）。さらに、"⑤トラスト利用容易化"を用いながら交渉経緯の記録を行うことで、利用容易性を高めることができ、商談・契約活動の堅確化（効果１）に繋げることができる。

(7) 金融機関等での TaaS による情報の連携

金融機関の融資業務における与信判断など、各種の公的・私的な情報を用いて業務上の判断を実施していく場合がある。

例えば、不動産担保の設定に用いられる不動産登記の情報については、現状、登記情報の電子化は実施されており、登記情報提供サービスによりインターネット経由の参照も可能となっているが、「閲覧」の位置づけであり、紙面の登記事項証明書のように内容を証明するものとはなっていない。ベース・レジストリと TaaS を連携させることにより、本来、情報の確からしさが必要とされている不動産登記情報のデジタルな流通が可能となる。

さらには、年末調整・確定申告内容による所得情報や、反社会的勢力に関する情報等、公的な情報を TaaS と連携させて提供を受けることにより業務判断の確実性の向上させることもできる。

民間同士でも、不動産鑑定の結果や、保証会社との情報連携、結果の通知など、TaaS 連携によりデジタルでの確からしい情報のやりとりの利便性が拡大できる。これらを図 26

Copyright 2021 Japan Digital Trust Forum

に示す。

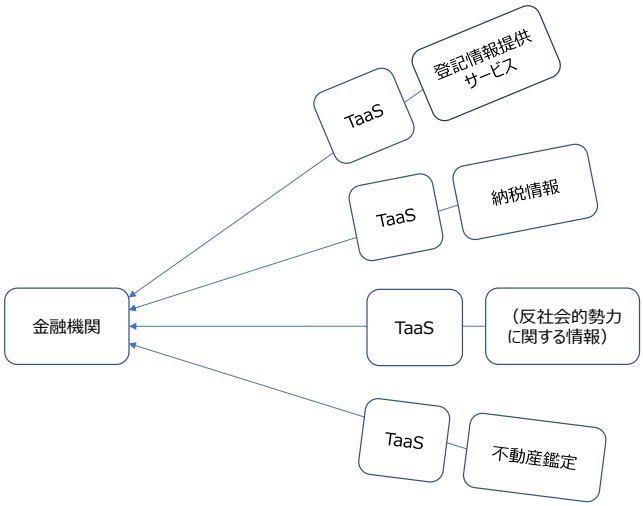


図 26 金融機関等での TaaS による情報の連携

(8) 商談・契約活動における交渉経緯の記録

営業活動から契約締結に至る商談活動においては、交渉過程に合わせて見積書を複数回作成することや、契約条件を見直すことは頻繁に発生する。そのような中、契約の履行に誠実でない懸念がある相手や、管理体制が十分に整っていない相手との契約を進める必要がある場合、自社においては契約の内容に慎重を期すだけでなく、契約に向けた交渉経緯情報を記録することが、契約に至る正当性を主張し、問題発生時のコストと損失の抑制するひとつの対策となる。

TaaS を利用することによって、図 27 のように、交渉経緯情報の作成者や内容の正しさが担保され、第3者からも検証可能となることから、自社の主張を強化することができるとともに、相手方が不当な対応を取ることを牽制する効果を期待することができる。

Copyright 2021 Japan Digital Trust Forum

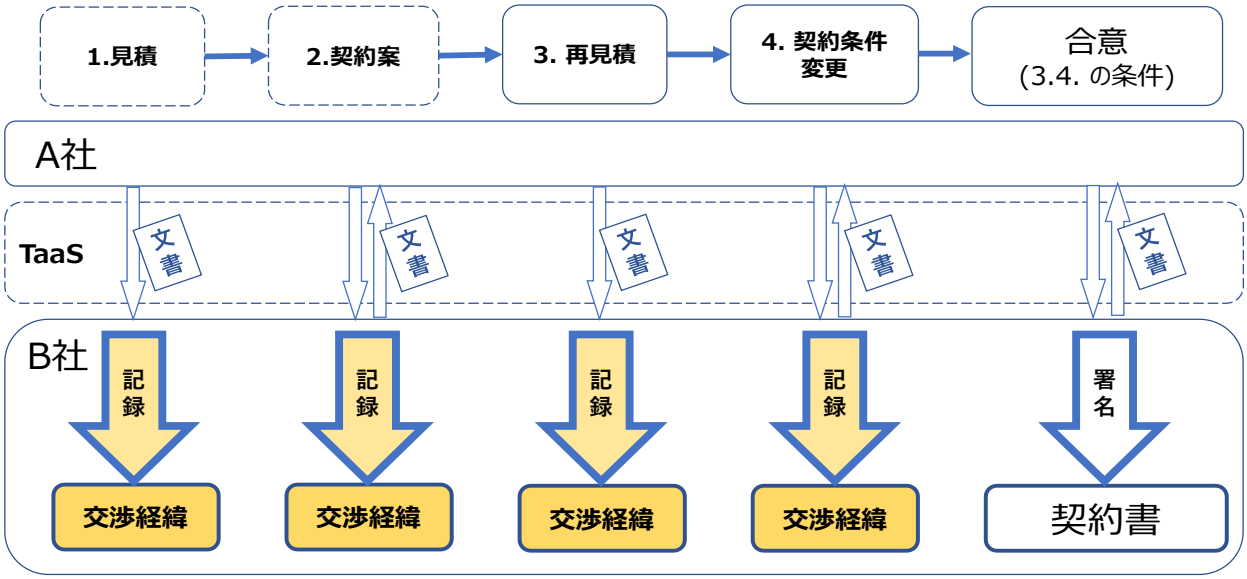


図 27 商談・契約活動における交渉経緯の記録

【もたらされる効果】

TaaS の機能により、B 社にとって、商談・契約活動における交渉経緯の記録により、交渉の経緯に関する疑義の確認（効果４）を実現することができる。さらに、"⑤トラスト利用容易化"を用いながら交渉経緯の記録を行うことで、利用容易性を高めることができ、商談・契約活動の堅確化（効果１）に繋げることができる。

Copyright 2021 Japan Digital Trust Forum

Ⅵ 今後の検討事項

1 次期ホワイトペーパーに向けた検討事項

- 今後は、システム観点をより明確化し、バージョンアップしたホワイトペーパーを出す予定である。普及加速に向けた、ユースケースおよびニーズ発掘を行いたい。
  - Ⅴ章の機能提言を、ニーズを踏まえたうえで検討し詳細化。
    - トラスト利用容易化機能に関する各種解決手段（ポリシー調整、相互運用性、利用者負担軽減）詳細化、等

- TaaSによるデジタル化の信頼性を、組織間、分野間（公共・準公共・民間）、国際連携を踏まえたうえで保証するための要件を、今後検討する予定である。
  - TaaS API に対する認証・認可の在り方：TaaS を利用する人・組織・モノの観点だけでなく、データ保有者のポリシーやデータの性質等を踏まえた認証・認可の在り方を検討する必要がある。
  - TaaS 間で連携する際のトラストアンカーの考え方や API の在り方：異なる組織で運用される TaaS 同士がどのように信頼を築くか、その際に TaaS 間でどのようなデータに対してどのような認可をするか、データ保有者のポリシーやデータの性質等を踏まえて検討する必要がある。

- どのような手続きに対して、どの保証レベルの、トラストアプリケーションサービス、トラストサービスが必要か、今後検討する予定である。

- デジタルトラストを実現する技術変革があっても、それを取り込めるような包括的な枠組みと利用者にとってビジネス継続性の担保できる具体的な方策について今後検討する予定である。

Copyright 2021 Japan Digital Trust Forum

2　社会実装上とるべきアクション

デジタルトラストの社会実装を目指すために、利用環境整備およびルール形成の観点からは、以下が必要である[41]。

● 包括的なトラスト基盤（TaaS 基盤）の制度整備

Society5.0 で高度に融合した人、組織、モノ、システムを繋ぐ多種、大量なデータの完全性を確保し信頼あるデータ連携、データ流通を支えるトラスト基盤の制度に関して、以下の観点で検討することが急務である。

- 各トラストサービスによる意思の証明（電子署名）、発行元証明(e シール)、存在証明（タイムスタンプ）などの効果の法定化
- 各トラストサービス水平横断的な共通要件や個別要件を整理の上、信頼レベルに応じた技術・運用基準等の策定と認定制度の創出
- 上記技術基準を政策と連携し策定、維持、更新する機関の設置
- 大量に流れるトラストを用いたデータの自動検証を可能とする機械可読なトラストアンカーの確認方法（トラステッドリスト）の制度化

普及の観点では、以下の検討が急務である。

● トラストサービスの使いやすさの向上

- ベース・レジストリから発行元証明が確保された形でのデータ取り出し、及びプログラマブルな連携
  （例、法人代表者の属性や法人登記情報等のベース・レジストリ情報を取り出す際にベース・レジストリの運営機関の e シールを付与することにより発行元証明が確保された形のデータ利用が可能となる。また API による取得により後段のシステムとの自動連携による効率化が見込める）
- クラウド型のトラストアプリケーションサービスの普及促進
- TaaS による様々なアプリケーション間のトラストな連携

---

[41] これらの観点は、下記のデータ戦略タスクフォース第一次とりまとめにおける「トラストの枠組み」の論点を踏まえつつ、さらに発展させたものである。
・内閣官房、IT 総合戦略室、データ戦略タスクフォース（第 7 回）、資料 1 、「トラストに関するワーキングチーム-検討状況-」（令和 3 年 5 月 26 日）
https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai7/siryou1.pdf

Copyright 2021 Japan Digital Trust Forum

- トラストサービスの国際相互運用
  - トラストサービスの国際相互運用を可能とするため、法的側面、国による監督・監査、標準技術、トラストアンカーを確認する仕組みの同等性の国際間相互承認
  - 諸外国との調和を目指した国際連携方針・ロードマップの提示

- 認定されたトラストサービスであることを利用者が検証できる技術仕様策定や適格マークの表示独占制度の整備、また、認定トラストサービスを利用する TaaS 登録制度の検討、等

Copyright 2021 Japan Digital Trust Forum