Report of the Sub-working Group for Trust-Assured Digital Transformation

July 29, 2022

デジタル庁
Digital Agency

Table of Contents

Executive Summary

"The Sub-working Group for Trust-Assured Digital Transformation (DX)" was established under the Data Strategy Promotion Working Group on October 25, 2021, to discuss measures for digital transformation while assuring trust under the provisions of paragraph 4 of "Convening of the Data Strategy Promotion Working Group" (Selection of the Chair of the Digital Society Promotion Council on September 6, 2021). Over a total of 11 sessions, this Sub-working Group carried out its discussions divided into the three main pillars consisting of finding trust needs and issues through fact-finding surveys and expert interviews, discussions on trust assurance, and trust implementation use cases and the implementation scheme. This report summarizes the discussions by this Sub-working Group, opinions of members and observers, and the future direction.

I. Trust needs and introduction issues

- **Scope of discussion**
  - The concept of "trust" which is expected in DFFT needs further clarification going forward. Regarding the scope of "trust services," we will start working on assuring trust in terms of the authenticity and tamper resistance possessed by paper in the digital realm as well.
  - Regarding focus areas for assuring trust, "administrative agencies" will independently promote the utilization of trust services in its procedures and transactions. When the government promotes utilizing trust services, it is imperative to devise measures to advance the utilization of trust services by small to medium-sized enterprises, which account for the majority of Japanese enterprises. Moreover, because transactions and procedures in the private sector are also important in DX, electronic transactions and procedures in the private sector must be explored at the same time.

- **Fact-finding surveys on trust assurance**
  - Fact-finding surveys shows that there is a need for trust services in use cases primarily in the industry/fields of "government," "finance/insurance," "telecommunications," "real estate," "medicine/welfare," and "transportation/postal services."
  - The introduction issues with trust services highlighted issues including the difficulty of vendor/service selection ("not sure which trust service vendor would be appropriate to use, etc.") in addition to the lack of recognition of

trust services and the difficulty of aligning actions between companies to introduce trust services.

- Regarding use cases in foreign countries, we examined the utilization of eID and trust services for information exchange and personal authentication in Estonia's electronic prescriptions and discussed issues with their application in Japan.
- Based on the “Administrative Procedures and Other Inventory Surveys (Cabinet Secretariat (IT Office)),” we analyzed the current situations of digitalization in procedures involving the government. While digitalization is making progress in applications from the private sector to the government in each ministry and agency, we found that progress is limited in other areas which consist primarily of disciplinary notification/delivery, etc. from the government to the private sector.

- **Opinions from experts**
  - Regarding trust services which are needed in front line, utilization examples, and issues concerning internal and external introduction/penetration, the sub-working group heard opinions from experts of “auditing,” “taxation,” “finance,” and “trust service provider.”
  - The sub-working group heard opinions from experts regarding the “examination progress of electronic seals” and the “competence of evidence of electronic agreements” as policy and legal issues in trust services, and discussed future improvements and the direction of discussions.

II. Discussions of trust services based on fact-finding surveys

- **Organization of the assurance levels.** The fact-finding surveys found there is a need to select the appropriate services in consideration of the risks and convenience as well as cope with problems in digital procedures which differ from those in analog procedures to adopt trust services, we discussed the organization of the identification assurance levels as well as the standards for evaluating the trustworthiness of trust services and the conformity assessment.

- **Promotion of the utilization of trust services in administrative procedures**. The Special Commission on Digital Administrative Reform formulated digital principles and has been discussing the review of “regulations requiring face-to-face meetings and documentation in official certificates, course, and viewing” and other requirements to promote “digital completion.” Because the utilization of trust

services is effective when reviewing regulations, trust services should be proactively utilized.

- **Promotion of the utilization of trust services in the private sector.** In order to incorporate diverse opinions about online contracts and procedures in the private sector, we should discuss trust service policies in multi-stakeholder model. The operation of a multi-stakeholder model requires a mechanism for fair discussion so that it is not influenced by the interests of a specific party, a mechanism to encourage the participation of stakeholders in the discussion, and a way to ensure efficient operation. Moreover, in order to promote e-seals in private sector, we should deepen discussions on policymaking of electronic seals.
- **Key principles of trust policy:** The Sub-working Group established key principles of trust policy (international interoperability, technical neutrality, etc.), which follow the "digital principles" for structural reforms in order for the multi-stakeholders including the government to follow the principles when considering policy making of trust services

III. Actions required for implementing trust

- **Promote digital completion in government:** The government is playing a central role in discussing the technology standards and utilization policies of trust services used in official certificates and will provide input aiming for June 2025 (FY 2025), which is the intensive reform period for regulatory reviews by the Special Commission on Digital Administrative Reform. At the same time, based on the request of Ibaraki Prefecture to utilize electronic signatures based on job responsibility electronic certificates issued by private sector certificate authorities, we will discuss how trust services in which public institutions are involved should be in terms of developing an environment in which users can easily verify the validity of a signature, support for international standard specifications, and continuous updating of technology standards, etc. In addition, we will proceed discussions on enabling local governments to utilize trust services and to issue disciplinary notifications and other documents online.

- **Establish a community to discuss with diverse stakeholders**: As topics relating to transactions and procedures between private sector entities, a diverse set of interested parties should participate and discuss issues pertaining to

"private-sector's online transactions and procedures," "support for remote signatures and electronic seals based on Act on Electronic Signatures and Certification Business and updating of technology standards," and "guidelines for use cases based on needs from industries." With regard to "trust service layer," which consists of the basis for trust assurance infrastructure, it is important to clarify technical standards which have already been established internationally in order to be referred in Japan and to seek to harmonize standards. In the long run, as the requirements of "digital completion" become clear, it will be necessary to explore the needs of trust services and usage environment of trust services.

- **Develop a policy of electronic seal:** Since the need for issuer related certification will increase in online transactions and procedures, we should support the initiative by the Ministry of Internal Affairs and Communications aimed at the establishing standards and conformity assessment based on the "Guidelines Pertaining to Electronic Seals" issued by the ministry in order to evaluate the reliability of private sector's electronic seal services

- **Promote internationally harmonized rulemaking**: Regarding identification assurance levels, we should provide input to the Digital Agency Technology Advisory Committee and utilize it in discussions concerning identity verification in administrative procedures. Development regarding identity verification levels in the private sector should continue to be discussed within the multi-stakeholder model based on the DADC study results. In addition, we will also continuously discuss the Digital Identity Wallet with international interoperability. Furthermore, while exploring market needs of trust services with international interoperability, we will also take into account international trends of "standards and conformity for the evaluation of trust service reliability" and continue to discuss "standards and conformity for the evaluation of trust service reliability" .

  In proceeding with these studies, discussions on the multi-stakeholder model should refer to international standards and should be conducted in collaboration with experts and specialized institutions so that standards, which will be created in the multi-stakeholder model, can be disseminated overseas. In addition, we will clarify the concept of trust aimed at the promotion of DFFT with the goal of introducing it at the G7 in 2023.

1. Introduction

As a new form of society following the hunter gatherer society (Society 1.0), agrarian society (Society 2.0), industrial society (Society 3.0), and information society (Society 4.0), Japan is aiming for Society 5.0 as a "human-centric form of society which balances economic development and the resolution of social issues through systems that merge cyberspace and physical space to a high degree[1]." Moreover, as privacy and security issues are becoming more apparent due to digitalization, Japan proposed the concept of "Data Free Flow with Trust (DFFT)" in 2019 to promote free data distribution across national borders.

Despite proposing the type of vision described above, it became clear during the response to COVID-19 that the development of a digital infrastructure for the generation, distribution, and utilization of data in government was insufficient in Japan. Accordingly, the Digital Agency was established in September 2021 with the goal of "a society in which services can be selected according to individual needs and diverse forms of happiness can be realized through the utilization of digital technologies[2]." To realize the type of society that the Digital Agency aims to achieve, the Special Commission on Digital Administrative Reform chaired by the Prime Minister was established in November 2021 for the purpose of conducting structural reforms such as review regulations and systems that are not premised on digital technologies and began to promote the integrated digitalization of government regulations and administration based on the digital principles[3].

Regarding the establishment of a trust framework, the "Trust Related Working Team" was founded in April 2021 under the Data Strategy Task Force in the Digital Government Cabinet Meeting. Within the "National Data Strategy"[4] issued by the Cabinet in June 2021, the main points directed at the establishment of a trust base which would become the infrastructure for data utilization and application were organized, and it was decided that the order of discussions should be clarified after analyzing the needs with respect to trust services for the purpose of realizing Society 5.0 and promoting DFFT. Against such a backdrop, the "Sub-working Group for Trust-Assured Digital Transformation (DX) " was established under the Data Strategy Promotion Working Group within the Digital Agency in order to discuss digital

---

1 Cabinet Office, Society 5.0

2 Digital Agency, "Priority Plan for the Realization of a Digital Society (Text)" No. 1 Introduction ~ Purpose of the Priority Plan ~ (p. 1),
(December 24, 2021)

3 Digital Agency, "Priority Plan for the Realization of a Digital Society (Text)"No. 5 Basic Digitalization Strategy (pp. 21 - 23)

4 Cabinet Secretariat IT General Strategy Office, "National Data Strategy (digital.go.jp)"

transformation while assuring trust directed at the implementation of the “National Data Strategy.”

Taking a look at individual initiatives within the establishment of trust base, the “provisions regarding the certification of time authentication businesses” (2021, Ministry of Internal Affairs and Communications Public Notice No. 146) were enacted in June 2021, and a national authorization system for the time stamp was newly established. Through relationships with foreign countries, the Japan-EU digital partnership was launched at the Japan-EU Summit on May 12, 2022, which is increasing the importance of mutual cooperation between Japan and other countries regarding trust such as the continuation of a pilot project initiative aimed at interoperability between trust services, an initiative aimed at determining the equivalence between Digital COVID Certificates, and the coordination of continuous information exchange regarding the Digital Identity Wallet.[5]

For the purpose of implementing the “National Data Strategy,” this Sub-working Group identified the trust service needs and introduction issues through fact-finding surveys and expert interviews, studied the assurance of trust based on fact-finding surveys, and organized future trust implementation use cases and the promotion system. This report summarizes the results of discussions by this Sub-working Group and the direction of future discussions.

5 Digital Agency, “Japan-EU Digital Partnership” (May 12, 2022)

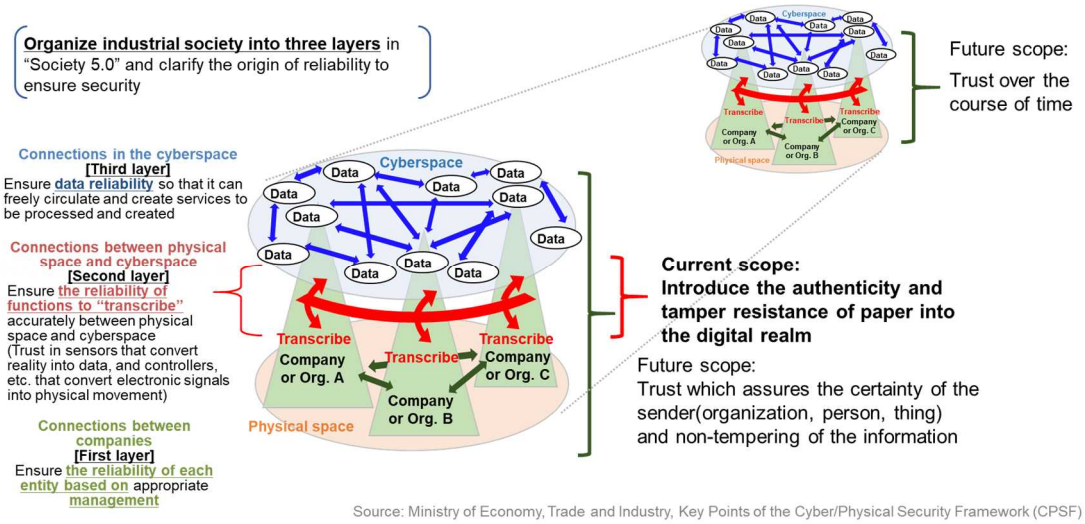
2. Scope of discussion

2.1 Scope of trust services

"Trust" constitutes an integral part of DFFT (Data Free Flow with Trust), which has become an essential element for maximizing the value of data to the fullest extent. Today, "trust" is used in various situations. It is hard to unequivocally define "trust", because the meaning differs according to each context. In discussing policies of trust-assured digital transformation in this Sub-working Group, the members attempted to organize an overall perspective of trust (Document 1) as well as organize the main theme and scope involved with data trust and the issues (Document 2) to clarify what kind of "trust" should be assured. In particular, regarding the overall perspective of trust (Document1), some members pointed out that trust assurance mechanism could be discussed by classifying "application layer," which provides trust services based on users' needs and "trust service layer," which provides authenticity and tamper resistance as an infrastructure. Considering the argument, the sub-working group tried to have elaborate discussions on trust service needs and introduction issues, trust services policy issues, identification assurance levels, and standards and conformity assessments for evaluating the reliability of trust services.

Through discussion, we learned that in aiming for Society 5.0, "trust" is a concept that possesses different shades of meaning according to various fields, subjects, and objectives. The members voiced the opinion that ensuring "trust" should include not only ensuring online the authenticity (the creator, sender, or time of existence matches what is described) and tamper resistance as paper assures, but also ensuring data truthfulness (data contents are correct, including the fact that the data is not fabricated, etc.), the accuracy of the sender (organization, person, thing) information, and the longitudinal trust over a long period of time (Figure 1). At the same time, trust services that are currently being used or assumed to be in use to assure the procedural side of things, and it has been pointed out that data truthfulness should be handled by the base registry. Accordingly, because the clarification of "trust" in DFFT requires further discussion, this report does not provide a definition of "trust". To leave room for future expansion of the scope of "trust," we started the discussion from of trust services to assure the authenticity and tamper resistance of paper in the physical space in cyberspace as well. In addition, when establishing comprehensive trust framework, it was pointed out that we should discuss criteria of technical standards of "trust service layer" by clarifying elements necessary to assure trust based on use cases.

(Figure 1) Items that should be assured through “trust”



Source: Ministry of Economy, Trade and Industry, Key Points of the Cyber/Physical Security Framework (CPSF)

2.2 Definition of trust services

“Trust services” have been defined in various reports and rules in Japan and overseas. For example, the “Study Group on Platform Services, Final Summary of the Trust Service Study Working Group” explains that trust services “are a system which verifies the correctness of people, organizations, and data, etc. on the Internet to prevent tampering, impersonation of the sender, etc.[6]” The rules of Europe’s eIDAS define trust services as follows based on a presumption of specific services.[7]

eIDAS Article3 Definition
(16) ‘trust service’
“an electronic service normally provided for remuneration which consists of:
(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
(b) the creation, verification and validation of certificates for website authentication; or
(c) the preservation of electronic signatures, seals or certificates related to those services;”

6 Ministry of Internal Affairs and Communications “Study Group on Platform Services, Final Summary of the Trust Service Study Working Group”p. 2 (February 7, 2020)
7 eIDAS2.0 is in the proposal stage, but the ‘electronic attestation of attributes,’ ‘the electronic archiving of electronic documents,’ ‘the management of remote electronic signature and seal creation devices,’ and ‘the recording of electronic data into an electronic ledger’ have also been added.

The United Nations Commission on International Trade Law (UNCITRAL), a United Nations organization which discusses the harmonization of commercial transaction rules across many countries provides the following definition.

> "Trust service" means an electronic service that provides assurance of certain qualities of a data message and includes the methods for creating and managing electronic signatures, electronic seals, electronic time stamps, website authentication, electronic archiving and electronic registered delivery services;[8]

The ISO/IEC DIS 27099 Information Technology - Public key infrastructure - Practices and policy framework defines "trust services" as "electronic service which enhances trust and confidence in electronic transactions."

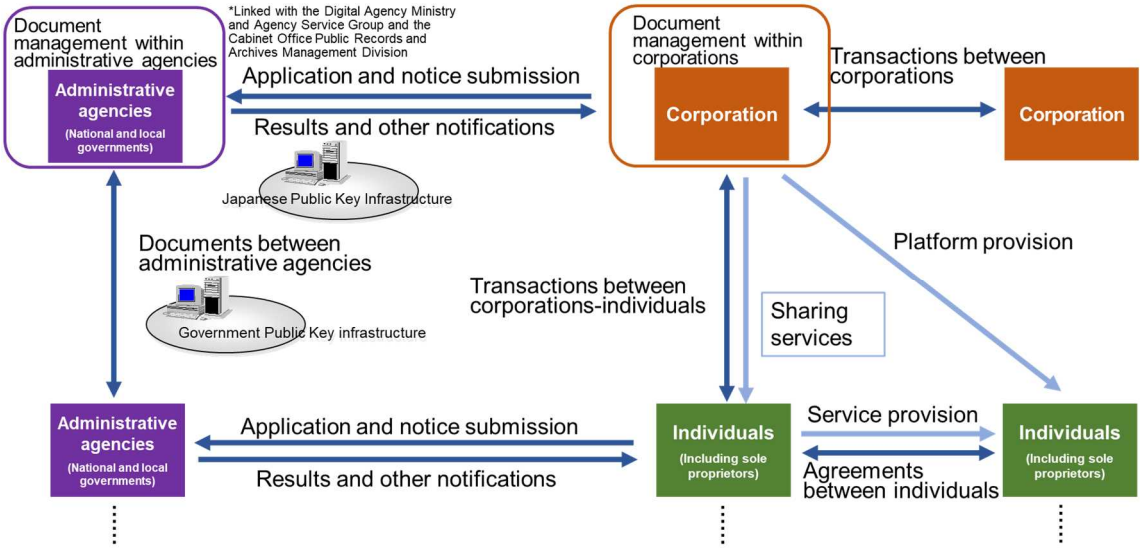
2.3 Stakeholders involved in trust

In order to understand stakeholders involved in trust and help discuss which part of trust we assure in policy making, we visualized the major users involved in trust and the mutual relationships among them. (Figure 2)

Figure 2 shows an overall picture of the major users, "administrative agencies," "corporations," and "individuals", as well as examples of the procedures and transactions among them. Moreover, due to the provision of platforms by corporations and the creation of sharing services through which individuals provide services to each other in recent years, procedures and transactions for sharing services are also described.

8 United Nations Commission on International Trade Law(Fifty fifth session) Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services

(Figure 2) Overall picture of users involved in trust



2.4 Focus Areas

In organizing the overall picture of users involved in trust, some members expressed the opinion that as a result of large enterprises requesting that Small to Medium Enterprises (SMEs) use Electronic Data Interchange (EDI) and other systems from their own companies in the computerization of SMEs[9], such enterprises that were required to support multiple EDI systems had no choice but to conduct their business on paper so as to be able to support any system. Hence, it is important to consider SMEs as main players when it comes to ensuring trust. In addition, members expressed the opinion that “administrative agencies” should be the first party to proactively promote the utilization of trust services.

Accordingly, the Sub-working Group will first focus on promoting the use of “trust service” by “administrative agencies” including electronic issuance of official documents that assure authenticity in the procedures and transactions. We should place an emphasis on devising ways for SMEs to adopt trust services, which account for the majority of Japanese companies, when the government promotes the utilization of trust services. Moreover, because transactions and procedures in the private sector are also important in DX, electronic transactions and procedures in the private sector shall be discussed at the same time.

9 The Small and Medium Enterprise Agency, “https://www.chusho.meti.go.jp/sme_english/index.html”

3. Trust assurance needs and issues

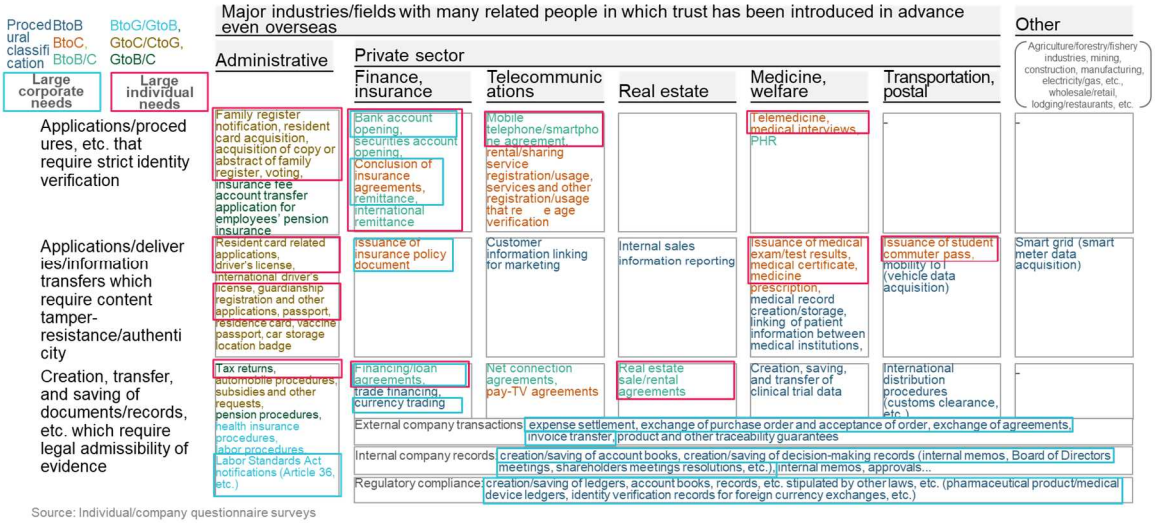
3.1 Fact-finding surveys on trust assurance

Regarding the current situations and needs for trust assurance of service users of administrative, private-sector, and other services, surveys of company/individuals and research into overseas precedents, etc. were carried out.

Use cases in each field which have needs to assure trust

When companies were asked about procedures, etc. which require identity verification of the other party or tempering prevention in fact-finding surveys, it was verified that there is a need for trust services in use cases primarily in the industry/fields of “government,” “finance/insurance,” “telecommunications,” “real estate,” “medicine/welfare,” and “transportation/postal services” (Figure 3).

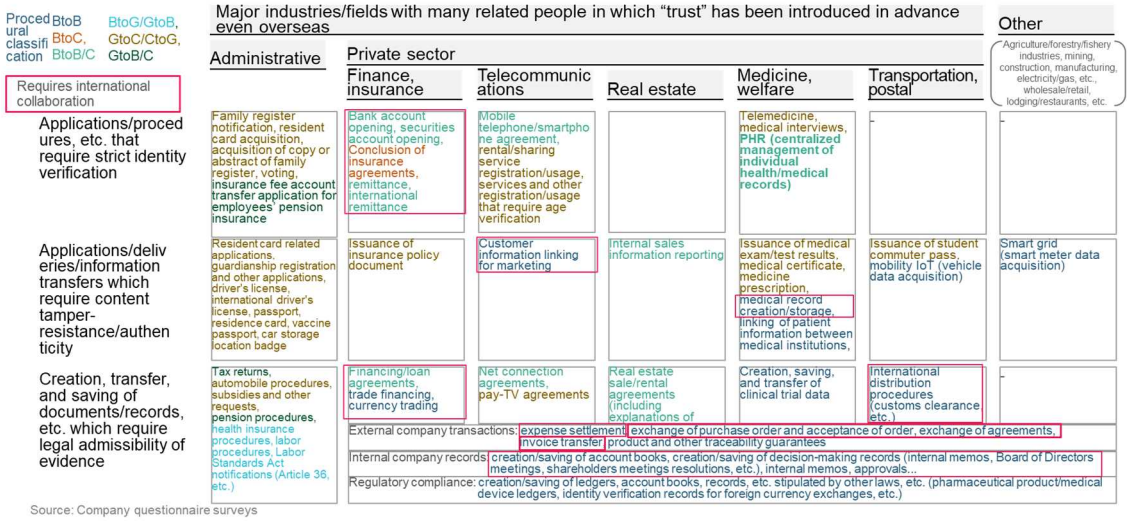
(Figure 3) Major use cases in which the need to assure trust has been verified



Source: Individual/company questionnaire surveys

Examples of trust service use cases which require international collaborations include external company transactions that are common to industries (purchase order and acceptance of order, agreements, invoices, etc.) and procedures that are specific to “finance, insurance” and other industries (Figure 4).

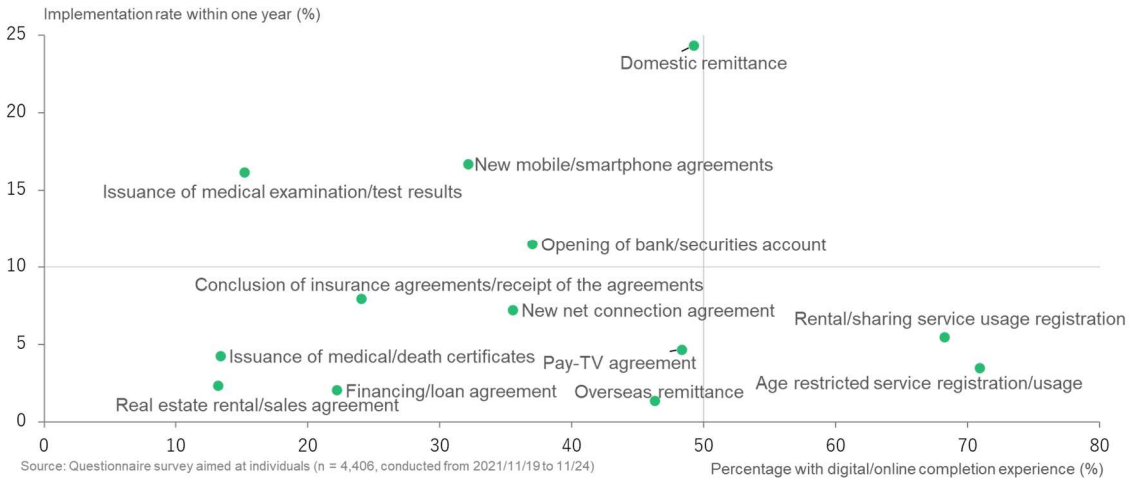
(Figure 4) Procedures, etc. which require international collaborations



Source: Company questionnaire surveys

In most of the procedures by individuals, the percentage of people who experienced implementing such procedures digitally/online was less than half in procedures for which trust services are thought to be effective. In particular, procedures implemented by 10% or more of the survey subjects in the past year (domestic remittance, new mobile/smartphone agreements, issuance of medical examination results, and the opening of bank/securities accounts), an experience rate of the digital/online implementation of these procedures was less than half (Figure 5).

(Figure 5) Use cases in individual procedures for which trust services are believed to be effective

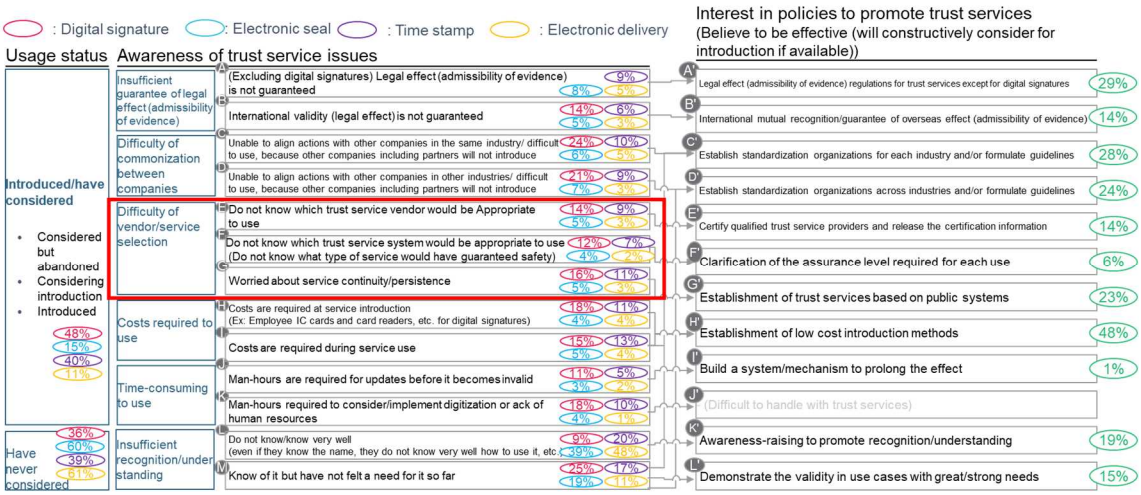


Source: Questionnaire survey aimed at individuals (n = 4,406, conducted from 2021/11/19 to 11/24)

Trust service introduction issues

The awareness of issues with trust services by companies included the difficulty of vendor/service selection (“do not know which trust service vendor would be appropriate to use, etc.”) in addition to the lack of recognition of trust services and the difficulty of aligning actions between companies to introduce trust services (Figure 6).

(Figure 6) Awareness of trust service issues (all companies)



Note: Each percentage is the ratio with respect to all respondents (N = 347). The total for those who “have introduced/have considered” and “have never considered” excludes the “do not know” results, so it does not reach a 100% total. Arrows are written in locations which are not based on a clear analysis result but are believed to have a deep relationship.
Source: BCG analysis from company questionnaire surveys

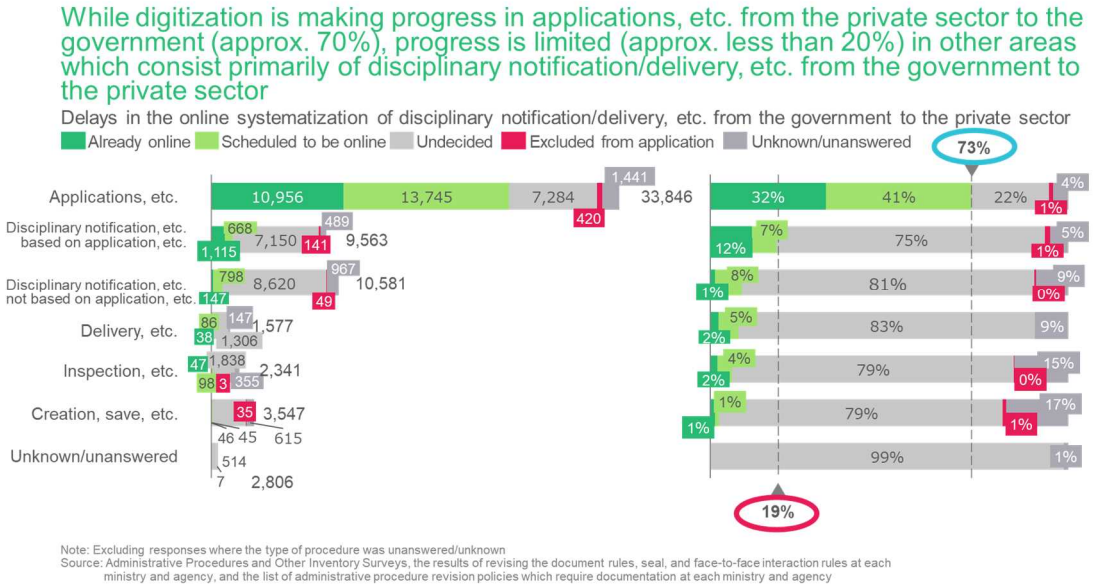
In terms of the “interest in policies to promote trust services,” “legal effect (admissibility of evidence) regulations for trust services except for electronic signature” and “awareness-raising to promote recognition/understanding” were cited in the results of this company survey. As pointed out in “2.4 Focus areas,” because it is necessary for SMEs to be able to use trust services, the members expressed the opinion that guidelines for introduction, low-cost trust service design, auditing, and operational structures are required to enable SMEs to consider convenience and cost aspects.

3.2 Analysis of digitalization in administrative procedures

Based on the “Administrative Procedures and Other Inventory Surveys (Cabinet Secretariat (IT Office)),” we analyzed the current situations of digitalization in “procedures that the government is directly involved,” “private sector procedures that

the government has jurisdiction over," etc. While digitalization is making progress (approx. 70%) in applications, etc. from the private sector to the government in the procedures of each ministry and agency, findings showed the fact that progress is limited (less than approx. 20%) in other areas which consist primarily of disciplinary notification/delivery, etc. from the government to the private sector (Figure 7).

(Figure 7) Disciplinary notifications from the government to the private sector/online systematization delays



Note: Excluding responses where the type of procedure was unanswered/unknown
Source: Administrative Procedures and Other Inventory Surveys, the results of revising the document rules, seal, and face-to-face interaction rules at each ministry and agency, and the list of administrative procedure revision policies which require documentation at each ministry and agency

Main opinions from members

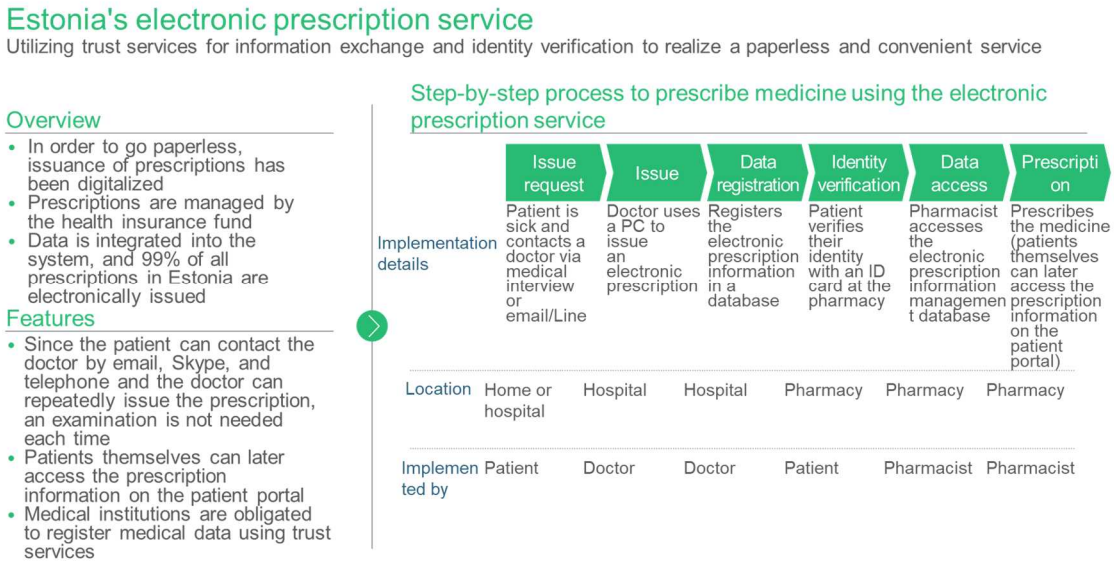
- The problem is that it is extremely low in digitalization of delivery documents. It is important to significantly raise the ratio of online delivery documents from the government to the private sector to become familiar with online and computerized forms of trust. Process reform must also be rapidly advanced within administrative organizations.
- While digitalization has progressed in applications, etc. from the private sector to the government, there is still significant room for improvement in many areas in terms of the ease-of-use of digital applications, etc.

3.3 Use cases in foreign countries

This Sub-working Group examined the utilization of digital ID and trust services in Estonia's electronic prescriptions and discussed the issues with their application in Japan.

In Estonia's electronic prescriptions, the patient contacts the doctor by email or other means, the doctor issues the electronic prescription, and registers the electronic prescription information in a database. The patient uses their ID card at the pharmacy for identity verification. The pharmacist accesses the database, references the electronic prescription data, and prescribes the medicine. The digital ID is used for identity verification of the patient at the pharmacy, browsing the web history, and doctor/nurse identification and qualification verification. The exchange of electronic prescription data is carried out through X-Road, and trust services such as electronic seals, time stamps, and electronic delivery, etc. are utilized. (Figure 8).

(Figure 8) Estonia's electronic prescription service



Use of eID in the Estonian Electronic Prescription Service

The eID is used in prescribing medicine for a patient at the pharmacy, browsing the prescription history on the web by the patient, and for doctor/nurse identification and qualification verification

Prescribing medicine for a patient at the pharmacy

Overview

In-person authentication with an eID card using a card reader

Usage example (as of 2011)

Doctor/nurse identification and qualification verification

Overview

Because the information as to whether the person concerned is a doctor/nurse is tied to the eID, it can be used to identify and verify the qualifications of a doctor/nurse

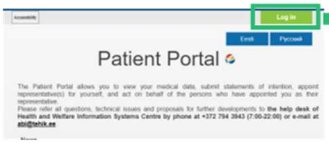
Web browsing of the prescription history by the patient

Overview

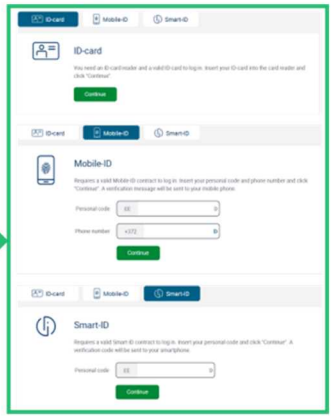
When logging into the patient portal, the user is transferred to a separate site for e-services personal authentication which authenticates with a single sign-on

ID cards, mobile IDs, and smart IDs can be used for authentication on the site above

Patient portal site



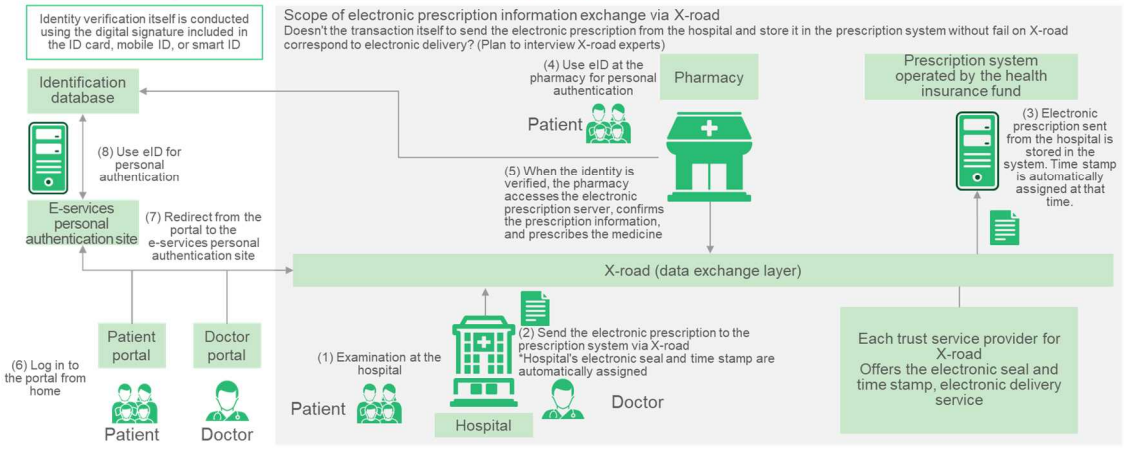
E-Services personal authentication site



Trust Services in Estonia's Electronic Prescription Service

Data exchanges utilize electronic seal, time stamps, and electronic delivery through X-road

Relationship diagram for trust services in the electronic prescriptions service



Source: Desktop research

Primary opinions from the members included that the potential utilization of identity verification and trust services in electronic prescriptions in Japan should be treated in a proactive manner. For example, a member expressed, “Electronic prescriptions are an example of implementing a service which uses authentication based on legally recognized trust services and eID which is the equivalent of official personal authentication. It is a domain which requires a high assurance level due to the fact that it handles serious personal information in the form of medical information, and it is the direction that Japan should head in.” Moreover, “there should be a mechanism to

prevent the prescribing of multiple doses of medicine through illegal sales of electronic prescriptions such as performing identity verification when the medicine is picked up." When managing electronic prescriptions, a member pointed out for a concern, "If in principle the identity of the patient is not verified when issuance of a prescription is requested, there may be a chance to issue a prescription that no one could pick up."

3.4 Opinions of experts

Trust assurance needs and issues presented by experts

Regarding trust service related front line needs, utilization examples, and issues concerning internal and external introduction/propagation, the Sub-working group heard opinions from experts on "auditing," "taxation," "finance," and "trust service providers" . The following describes the presentations and primary opinions of experts by referring to their presentation materials. (For more details, see the expert presentation materials in Appendix A (Document 3 - Document 13)

Auditing services

- Through the development of trust base, business efficiency, fraud prevention effects, and the visualization of control will advance through the ease of access to digital evidence. In addition, there is a need to promote continuous audits utilizing abnormal journal entry detection, data analysis, etc.
- There are issues to be addressed that data standardization is not progressing and no supporting measures beneficial in proportion to the cost of trust service introductions, thorough encryption key management, ensuring the reliability of electronic certificates, improving the understanding of trust service systems.

(Document 3 "Trust Service Needs and Issues in Company Business Process Reform and the Digital Transformation of Auditing Services")

Taxation related services

- In the consumption tax invoice system, the issuance of data for an eligible invoice is recognized. As electronic invoices permeate, there will be a need for an origin certification system (electronic seal) in the digital realm like a company seal stamped on a paper invoice.
- In the digital transformation of taxation related services of companies, hindrances to the adoption of electronic transactions include corporate cultures that do not wish to change their customs, a significant burden of investment to

computerize workflow systems, and the inability to obtain the cooperation of business partners.

- In particular, the significant burden of system investment and the complication of conforming to the Electronic Account Books Preservation Act are factors that make SMEs persist to use paper documents. To advance the computerization of all companies and build a trust-assured digital society, consideration must be given to further deregulation of laws and ordinances as well as reducing system introduction costs and cost of electronic signature usage and others.
  (Document 4 “Issues in the Digital Transformation of Taxation Related Services”)

Financial services

- Computerization is progressing at appropriate fields in bank such as account opening procedures and loan agreements, etc. for individuals. Meanwhile, the progress of computerization has been slow in financing agreements and account opening procedures for corporations due to requests for original copies of submitted documents and anti-money laundering related procedures. Moreover, checks and paper-based procedures play a central role in commercial paper transactions. There is significant room for the utilization of electronic seals in the area of corporate business.
- In the introduction of trust services to customer-facing procedures for banking services, there are issues such as the burden of genuine proof in the establishment of an agreement (ensuring legal stability), the assurance of contract procedures by a legitimate authority in corporate transactions is insufficient, service introduction costs (system investment burden, ROI), insufficient awareness of trust services, concerns about security, and the burden of a smooth transition from the current situation, etc.
  (Document 5 “Electronic Certificate Needs and Issues”)

Electronic financing agreement services

- While electronic signatures are aimed at natural persons, the fact that juridical persons (corporations) sign loan on deed and other financing transaction agreements is an issue when it comes to introducing electronic signatures.
- In order to tie the electronic signatures used by individuals to actions based on corporate decision-making, we have taken a way that the corporation nominates an individual as an authorized person and an electronic contract holder pertaining to a financing agreement in a service application. Moreover,

the sales manager directly hands over the notification of the initial PIN code to enable the ID to assure the identity of the electronic signature.

- Future issues include establishing a reliable way to notify the user of the initial PIN code to activate the ID in a non-face-to-face setting and improving convenience and productivity for both the customer and the bank through the promotion of digitalization and the introduction of electronic contracts throughout the entire financial industry that are not just limited to individual banks.

  (Document 6 “Electronic Financing Agreement Services Being Deployed by Sumitomo Mitsui Banking Corporation”)

Primary opinions about electronic financing agreement services

- When using electronic certification in transaction reliability, it is important to analyze the process flow end-to-end and clarify the requirements when it comes to assuring the validity.
- When conducting international transactions, it is important to have international arrangements in place for the trust chain representation within companies and corporations.

Role of the “electric stamps display on electronic documents”

- The fact that many people feel that a document is official when looking at a stamped document has become ingrained in our lifestyle habits. A stamp is thought to have the effect of making people believe that the individual’s intentions and the document’s completeness have been visually verified, and perhaps there is room to utilize electronic stamps in the digital realm as well.
- Electronic stamps are a tool that people are used to using and that have a certain legal foundation, but their reliability (threat resistance) is lacking. On the other hand, electronic signatures are highly reliable, but they still cannot be said to have a generally high degree of recognition. The adoption of trust services will be promoted by fulfilling both needs of being a familiar tool with high reliability.
- In terms of the interface, the stamps fall under the internal company rules during the transaction, and in some aspects it is difficult to change the operation itself. In regard to new technologies, familiar interfaces are effective as a way to curtail costs for internal system design and internal propagation as well as labor.

(Document 7 “History of Electronic Stamps and Their Role in Electronic Agreements”)

Primary opinions about the “stamp seal display on electronic documents”

- Building trust in a way which is only visual using images of stamps and signatures may be misleading. Methods for displaying technical validation results to users in an easy to understand manner in trust services must be discussed as a set together with assurance levels. In Japan, the trust service validation methods differ according to each service. In the EU, they have developed a trust infrastructure called a trusted list and trust anchors within the eIDAS regulations, and the European Commission operates a service that can validate trust services that are legally valid. They have also developed a library for validation under open source and provide a public validation infrastructure as published[10].
- While there are certified authentication services, etc. in authentication services and reliability assurance frameworks which tie together users and signatures, what is the situation with linking user reliability in witness-type electronic signatures and NFT stamps? Witness-type electronic signatures must be properly positioned in the assurance levels of trust services.
- Electronic stamp systems may also be valid in internal company business processes.
- Regarding the statement that a registered seal proves identity with “the trust of the government,” this issue should be cleared up, because in reality people think that trust for the stamping process and the process to hand over a document are included.
- It is important to discuss how to get people to accept the recognition of authentic documents in the digital world.

Trust service providers

Global DX solution provider

- From the perspective of providing electronic signature services globally, we observed points of improvement in the EU eIDAS regulations such as the harmonization of personal information protection, technical standards, interoperability, and security levels between each country and issues aimed at the adoption of digital ID solutions.

[10] Digital Signature Service version : 5.10.1 - 2022-04-08

(Document 8 “Current State and Issues in Trust Services as Recognized by SAP”)

Electronic certificate service providers

- An introduction to case studies about the use of electronic certificates (graduation certificates, business formulated, vehicle registration documents, PCR test result reports)

  (Document 9 “Case Studies of Using Electronic Certificates in GlobalSign”)

Cloud-based electronic signature service providers

- The reason why the high volume, rapid commercial transactions that stamping supported were not digitized through the Act on Electronic Signatures and Certification Business is because the trust level settings, which were increased more than expected by said act, did not conform to user needs.
- In order to realize the digital principles based on such past reflection, we must increase the number of “just right trust” choices and have the Digital Agency lead that adoption.
- We would like to have the cloud-based electronic signature services that are already attracting the support of foreign and domestic users positioned as “standard” in the new trust legal system.

  (Document 10 “The Need to Promote the Adoption of Cloud-based Electronic Signature Services Which Support the ‘Digital Principles’”)

Primary opinions about cloud-based electronic signature service providers

- Regarding the uniqueness of processes indicated in the Q&A of Article 3 of the Act on Electronic Signatures and Certification Business, what level of uniqueness are cloud-based electronic signatures trying to ensure? Are there any thoughts about officially announcing the IAL and AAL levels in the future?
- Although the type of signature in which the parties concerned sign is explained as not having strong backing, based on the number of certificates issued for certified authentication services, that type of signing also includes non-certified authentication services as well, so taking this type of signing as not being adopted because of the lack of adoption of certified authentication services may be misleading.

- Regarding the pie chart showing the “Share of Electronic signature Systems Selected by Global Corporate Users (Estimate),” consideration must be given to the fact that this is the result of a survey conducted among customers by the corporate members of the Cloud-based Electronic signature Service Council.

Expert opinions of policy issues of trust services

In addition to receiving input from experts regarding the “Progress of discussions on policymaking of electronic seals” and the “Competence of evidence of electronic agreements” as policy and legal issues in trust services, we discussed future improvements and the direction of discussions. The following describes the presentations and primary opinions of experts.

Progress of discussions on policymaking of electronic seals

- The electronic seals which the Ministry of Internal Affairs and Communications explored are limited to seals issued by organizations. These electronic seals mechanisms for verifying that the issuing entities and corresponding documents have not been tampered with.
- Regarding the standard for measures to assure the reliability of the issuer certification, the electronic seal levels are divided into a light level which only needs to prove that it has not been tampered with, a level that can conclusively assure who issued it, and a level that assures a higher standard of reliability. The reliability levels are separated in order not to prevent the low-level certifications from spreading.
- Regarding identifiers for specifying those that must issue an electronic certificate for electronic seals, we should discuss a comprehensively expressible method (OID: Object Identifier) including organizations, individuals, data, and other existing IDs and numbers so as not to later reduce the flexibility.
- Regarding the HSM equipment on the certification authority side of electronic seals, the current FIPS140-2 Level 3 or ISO/IEC 15408 EAL4+ should be adopted. FIPS140-1 is still referenced under the standards of the Act on Electronic Signatures and Certification Business. We should explore update mechanism in order to support the current version of the standard.
  (Document 11 “Progress of Discussions on Policymaking of Electronic Seals and Future Issues and Needs”)

Primary opinions about policymaking of electronic seals

- (Regarding the procedure to issue electronic certificates pertaining to electronic seals) there is an awareness of the issue that it is indeed difficult for large companies to have a representative operate the procedure. The issue should be discussed so that the operation can be simplified.
- Because the same certificate is copied when you want to use an electronic seal with server-side scaling, Derived Credentials become important. There needs to be a way that is institutionally permitted for the receiving side to follow the certificate chain and be able to verify the validity by signing the key that is generated within a company through the certificate from the certification authority.
- Regarding Derived Credentials, it is important to discuss whether identity verification using a key issued in advance is recognized when conducting identity verification online.
- Methods should be devised so that users do not need to have electronic certificates/secret keys for use with electronic seals for each service.
- In the European electronic seal PoC, they are validating a framework aimed at international mutual recognition. As internationally-authorized traceability assurances are being required in SDGs, environment, and human rights frameworks, perhaps it can be said that a framework needs to be developed.
- In order to make it possible for the people to carry out online-based transactions with a sense of security, it is essential that electronic seals be developed with legal backing. In today's world of rapid technological progress, legal disciplines should be minimized, but under the current situation of rampant phishing scams, it is extremely important to be able to legally verify as a "trust" infrastructure whether the other party that is conducting an online-based transaction is the true organization that was authorized.

Competence of evidence of electronic agreements

- Because it is easy to impersonate or falsify an electronic agreement, the verification of identity and completeness is important. Electronic signatures do not necessarily need to be used in effectively establishing an electronic agreement, but in practical terms the electronic signature levels need to be separated according to the level of reliability that is required.

- Regarding electronic agreements, there is a need to use electronic signatures, etc. with the appropriate level in the verification of identity and completeness in consideration of the risks and convenience.
- It is believed that the development of the legal environment required for the adoption of electronic agreements is almost complete. As to whether the requirements in Article 2, paragraph 1 and Article 3, Q&A of the Act on Electronic Signatures and Certification Business announced by the government are satisfied, as a problem of application, there is a need to select the appropriate service according to the application by utilizing legal experts while having the parties to the agreement and the electronic agreement platform providers perform a self check.

(Document 12 “Validity of Electronic Agreements”)

Primary opinions about the evidential power of electronic agreements

- Standards need to be created according to the level. Regarding remote signatures and witness-type interest, because there are no clear standards for service stability and certification and conformity audits are also not ready, it may be the case that users or judges cannot make decisions.
- Regarding the creation of trust level standards, the standards which differ from the equivalent of unregistered seals and other aspects of the analog world are required.
- The levels should be classified not only by the “means” but also be studied on a “threat resistance” basis in accordance with SP800-63-3B.
- Discussion is required not only about the process but also about the level that is equivalent to an authority which issues an ID or credential.
- As a standard which is established by the enforcement regulations of Article 2 of the Act on Electronic Signatures and Certification Business, there are concerns as to whether it is appropriate to write as much as the encryption algorithm and bit length amid rapid technological progress.
- Regarding the “two stage presumption” in the Civil Proceedings Act, Article 228, paragraph 4, the thinking which is applied in the case of witness-type electronic signatures must be clarified according to each process. In particular, regarding the case where the “stage one presumption” (if there is an imprint of the individual’s stamp, it is presumed that it was stamped

according to the individual's wishes[11]) is computerized, it must be discussed going forward as it has not been yet discussed so far.

- Regarding the "sufficient standard uniqueness" in the Q&A[12] of the Act on Electronic Signatures and Certification Business, Article 3, it would be easy for users to understand if there were several illustrations in addition to two factor authentication.
- Because decisions regarding trust also include technical details, the judgment of technical experts is also required in addition to legal judgment.
- The interoperability of "specified authorization services" and the means to achieve it should be studied going forward.

Possibility of utilizing electronic seals in computerization and the institutional issues

- In utilizing trust services, the standard computerized form must be indicated at the same time as the discontinuation of systems that require paper or document delivery.
- In the application steps, procedural regulations exist that require the originality of the agreement, etc. From the perspective of assuring the "originality" and "authenticity," there are many areas in which computerization can be promoted through the utilization of electronic seals in cases such as the cases which require the submission of the original when issuing a certificate, cases which require the submission of the original on paper as the original is a paper document, and cases which require assuring the authenticity of the contents of the agreement, etc. officially issued by an organization.
- In particular, there are many aspects in import/export transactions where overall computerization is being promoted by assurining the authenticity with authorized certificates, and other electronic seals that include not only the export side but also agreements required for importation, written pledges by importers, and invoices for importation. In addition, inefficient, paper-based aspects remaining in trade transactions will disappear, and the industry overall will be broadly streamlined. Through advances in the computerization of trade transactions, manual verification work will be systematized, and infrastructure will be developed for the systematic detection of "Trade Based Money

[11] Cited from p. 69 of the "Electronic Agreement Textbook ~Fundamentals to Introduction Examples~ Third Edition" (Hiroshi Miyauchi (author))

[12] Ministry of Internal Affairs and Communications, Ministry of Justice, Ministry of Economy, Trade and Industry, "Q&A Regarding Electronic Agreement Services That Perform Encryption, etc. With the Service Provider's Own Signature Key Based On The User's Instructions (in relation to the Act on Electronic Signatures and Certification Business, Article 3)" (September 4, 2020)

Laundering (TBML),” which will also be beneficial in terms of Japan’s AML measures.

(Document 13 “Trust Service Use Cases and Restrictive Systems”)

4. Studies for the assurance of trust

The sub-working group carried out following discussions based on trust assurance needs and issues in introductions of trust services that were identified through fact-finding surveys and opinions from experts.

4.1 Organization of the identification assurance levels

The fact-finding surveys found issues in introducing trust services including the “selection of trust service businesses/services according to the application” and the “difficulty of aligning actions between companies regarding the use of trust services.” We found there is a need to select the appropriate services in consideration of the risks and convenience as well as a need to address problems in the online procedures of digital completion that differ from the analog world. We organized the identification assurance levels and discussed standards and conformity assessments for evaluating the reliability of trust services.

Understanding cases in foreign countries

- We examined the assurance level rules and approach to standards in the eIDAS regulations, NIST SP800 63-3, and the New Zealand government’s Identification Management Standards in order to help select an appropriate assurance level for each use cases i. (Document 14 “Assurance Levels in Europe’s eIDAS,” Appendix C Overseas Precedents Regarding Assurance Levels)
- Regarding the eIDAS regulations, it was pointed out that while a certain evaluation has been obtained about the effects of digitalization through the adoption of trust services and the systemization of eID and trust services for the purpose of promoting a European digital integration market, the issues concerning the effects, efficiency, and adoption of eID and trust services are being reviewed. Based on these issues, the EU is addressing these issues through the development of an EU Digital Identity Wallet and the preparation of lower regulations for trust services, etc. aimed at eIDAS2.0. (Document 15 “eIDAS2.0 and EUDIW”)

Organization of the identification assurance levels

Approach for discussion

- The basic approach should be to reference existing international standards and then consider the realization of identity verification utilizing these standards according to the actual situation in Japan where a base registry is prepared and public personal authentication certificates for Individual Number Cards and electronic certificates for commercial registrations are available.
- Authentication information linking and allocation should also be considered as part of the identification assurance levels.

Ideas and use cases of assurance level

In addition to the approach being indicated below, the sub-working group tried to organize a mapping with use cases as shown in Figure 9.

- Because Individual Number Cards are issued by qualified personnel who are local government officials after verifying a person's identity in-person, the level exceeds the equivalent of IAL3. As a result, it can be said that the in-person verification that the person on the Individual Number Card and the face photograph match and the signature using the digital certificate of the Individual Number Card are equivalent to IAL3.
- In situations other than the issuance of an Individual Number Card, it may be possible to make everything electronic as in the "Maebashi ID" of Maebashi City (Gunma Prefecture) to replace the identity verification with a electronic signature using an Individual Number Card.[13] In that case, the question of whether a photo of the person in question truly needs to be matched with a real-time image of the person will become a point of discussion.
- The matching of a person's photo with a real-time image of the person has two different objectives which are physically tying the image to an Authenticator and detecting the use of an Authenticator by someone other than the person in question, so these objectives should be discussed separately.
- As users can easily register in the COVID-19 vaccination certificate app using an Individual Number Card, the usability and cost of the ID Proofing have been improved.
- A mechanism that can link identification and administrative data needs to be developed.
- If identity verification is required more than necessary in private sector services, it will have the negative effect of causing the number of service subscribers to

[13] In fact, dependence-based identity verification is carried out in the EU. This is carried out not only under eIDAS QS but also appears in the issuance of a certificate of eligibility through trust services based on a digital transfer of verified identity information performed by German banks at the counter, etc. and the resulting implementation of an eligible signature, etc.

decrease, so diverse identity verification choices such as eKYC are required in addition to the Individual Number Card. Regarding use cases of online identity verification in private sector services, the identity verification methods were divided by level, and an initiative status report was obtained from the Digital Architecture Design Center (DADC) about the approach to selecting identity verification methods according to risk and how to proceed with guideline formulation.

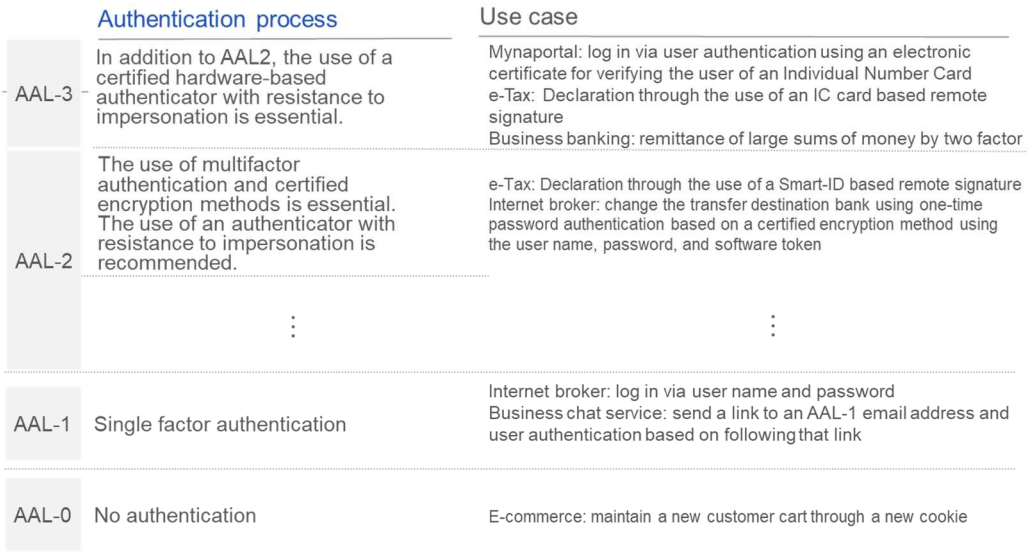
(Document 16 “Incubation Lab Project ‘Service-specific Digital Identity Verification Guidelines’”)

(Figure 9) Use case mapping within IAL

IAL	Identifier	Identity verification method	Use case
IAL-3	Item that can be electronically identified through a trustworthy institution	Verified face-to-face	Face-to-face application using an Individual Number Card
		Non-face-to-face	Digital signature using an Individual Number Card
	Item that is assured by the issuer and can be identified	Verified face-to-face by a qualified person	
		Face-to-face equivalent online (eKYC)	Online matching of an individual's identification card photo and a real time image of the person
	⋮	⋮	⋮
?	Item that is assured by the issuer and can be identified	Verify face-to-face after online registration	Open a bank account online -> identity verification at card pickup
IAL-2	Item that can be electronically identified through a trustworthy institution	Verified without face-to-face contact	Open an account online using an Individual Number Card reader
	Item that is guaranteed by the issuer and can be identified	Verified without face-to-face contact	Online EC site member registration using identity verification documents (image upload, etc.)
IAL-1	Can be self-asserted with no identity verification	No identity verification	Confirm notification at an email address during service registration

*Face-to-face also includes remote face-to-face (supervised remote)

AAL and Use Case Mapping Proposal



	Authentication process	Use case
AAL-3	In addition to AAL2, the use of a certified hardware-based authenticator with resistance to impersonation is essential.	Mynaportal: log in via user authentication using an electronic certificate for verifying the user of an Individual Number Card e-Tax: Declaration through the use of an IC card based remote signature Business banking: remittance of large sums of money by two factor
AAL-2	The use of multifactor authentication and certified encryption methods is essential. The use of an authenticator with resistance to impersonation is recommended.	e-Tax: Declaration through the use of a Smart-ID based remote signature Internet broker: change the transfer destination bank using one-time password authentication based on a certified encryption method using the user name, password, and software token
⋮	⋮	⋮
AAL-1	Single factor authentication	Internet broker: log in via user name and password Business chat service: send a link to an AAL-1 email address and user authentication based on following that link
AAL-0	No authentication	E-commerce: maintain a new customer cart through a new cookie

Future direction

- The approach to identification assurance levels and use cases organized by this Sub-working Group needs to be input into the “Guidelines Concerning Online Identity Verification Methods in Administrative Procedures”[14] review by the Special Commission on Digital Administrative Reform.
- It is important to organize assurance levels not only in administrative procedures but also in private sector services. We should discuss further the architecture development regarding identity verification levels within the multi-stakeholder model based on the DADC study results.
- We will also continuously discuss the Digital Identity Wallet with international interoperability as a method for identity verification and the digitalization of qualification procedures as Decentralized Identity and Self-Sovereign Identity have been paid attention globally in a way that does not depend on the platform providers.

[14] Digital Agency “Guidelines Concerning Online Identity Verification Methods in Administrative Procedures” (February 25, 2019)

4.2 Discussion on standards and conformity assessments for evaluating the reliability of "trust service layer"

Direction of discussions

- Thinking about standards and conformity assessments for evaluating the reliability of "trust service layer " is also important in ensuring the trust of ID providers, and the discussion was conducted because there was an opinion that trust service standards should be created in anticipation of international interoperability.
- As a trust service business operation policy, there was a proposal from the members to organize the organizational requirements, equipment requirements, technology requirements, key management requirements, operation requirements, audit requirements, etc. as common trust service standards and individual standards, which are to be organized as the "trust service assurance levels." (Document 17 "Trust Service Assurance Level Approach")
- At the same time, it was pointed out by members that the standards and conformity assessments for evaluating the reliability of " trust service layer" include a wide range of arguments and details that should be assured.

Issues in discussions

In discussing standards and conformity assessments for evaluating the reliability of "trust service layer", the following discussions were held about the issues and conditions which should be fulfilled.

- **Role of the state**:
  - In the case where the state assures the highest level of standards and conformity assessments for evaluating the reliability of "trust service layer", it would be challenging under the current system for the state to continue to maintain the latest specifications and assure the audit system. For example, because the Act on Electronic Signatures and Certification Business certification standards are stipulated in the enforcement rules and guidelines etc., they are difficult to maintain in conformance with the latest international technical standards. Therefore, one direction is to refrain from writing the technical standards in the

provisions and instead reference international standards to lessen the burden on the state, which will enable the realization of a more effective policy.

- Legally speaking, the trust assured with trust services is a “presumption,” and because contrary evidence to deny presumed facts is allowed, a 100% guarantee is not sought as a state for presumed facts.

- **Formulation work**:
  - If we are to envision technical standards which are at the same level as those standardized by the European Telecommunications Standards Institute (ETSI) and European Committee for Standardization (CEN), some ingenuity is required to curtail the work based on existing standards and prevent a massive amount of work.

- **Subject:**
  - As the question of what is legitimate differs depending on the use case, we need to clarify what legitimacy we are discussing instead of the assurance levels.

- **Relationships between the axes**:
  - The identification assurance levels and trust service assurance levels should be turned into parameters with no interdependency.

- **Audit requirements:**
  - In the audit systems of certified business operators, it is important to link the metadata and provide the operational transparency through AI-based automatic inspections instead of conducting audits at a single point in time.
  - While it is understandable for the audit requirements to be part of the certification procedure, it feels out of place for them to be part of the assurance levels.

- **International interoperability**: to deepen the discussion going forward, facts which should be verified as a precondition and terminology that should be common knowledge were cited.
  - We need to clarify the barriers and reasons why there are no countries with mutual recognition of eIDAS outside of the EU and verify the

feasibility of doing so before discussing.

- "Cross-border agreements" came up as a type of transaction which requires international interoperability, but agreements state the governing law, so international interoperability may not be required.
- When it comes to assuring international interoperability, it may be the case that the trust services of one's own country can be used even if the governing law is the law of the other country. On the topic of governing law, if for example the governing law is Japanese law, because even foreign companies would be judged based on Japan's laws, a need would emerge for foreign companies to also use Japan's trust services. Conversely, if European law is the governing law, Japanese companies would have to use European trust services instead of Japanese trust services. There was the opinion that since agreements state the governing law, international interoperability is not necessarily needed. However, even if the governing law was stipulated, international interoperability is actually needed when thinking about evidentiality and other issues.
- After developing a common understanding of the term "mutual recognition," we should clarify what it is aimed at, what it is related to, and with what countries (regions) mutual recognition should be studied.
- With the goal of assuring international interoperability, we should reference the compliance with international standards and related standards (ISO/IEC 27000 Series, CAB/F baseline requirements, ETSI and CEN standards, and Webtrust auditing standards, etc.) before regulating requirements for institutions conducting assessments of conformity with these standards for each trust service in reference to international standards (ISO/IEC 17065, ETSI EN 319 403, etc.)
- The domestic trust services must be verifiable overseas as well as to the assurance level at which they are positioned. Therefore, the establishing a validation infrastructure according to international standards will also be required.

- **Assurance of mobility:**
  - Each standard should be formulated as an independent technology standard referenced by laws and ordinances.
  - The establishment of an expert organization to continuously formulate and update standards in proportion to technology advancement,

international standards, and the social environment must be studied.

- **Compliance with the existing system:**
  - In deepening the discussion of trust services, discussion of reviews of laws relating to electronic signatures and authorization services (including the utilization of international technical standards) cannot be avoided.
  - In order to promote the effective utilization of electronic signatures and electronic seals, etc., the presumed effect and other legal effects must be studied in regard to highly reliable trust services typified by certified authorization services.

- **Usability:**
  - The universality of electronic documents shall not be denied only for the reason that they are in an electronic format and in this regard exceptions should not be allowed by law.
  - Standards development and mechanisms for indicating to users in an easy to understand manner (release of certified trust services in a machine readable format, information validation based on the corresponding trust services) what level a trust service meets must be studied.

- **Interoperability:**
  - To ensure digital interconnectivity and operability, the provision of a validation infrastructure and the passing of the corresponding tests must be confirmed on a timely basis to verify that technical compliance.

Future direction

Because there are a wide range of details that should be assured and there are many issues that should be considered during formulation, we will advance the discussion about standards and conformity assessments for evaluating the reliability of “trust service layer” based on international discussions and changes in the external environment.

4.3 Promoting trust services in government administration

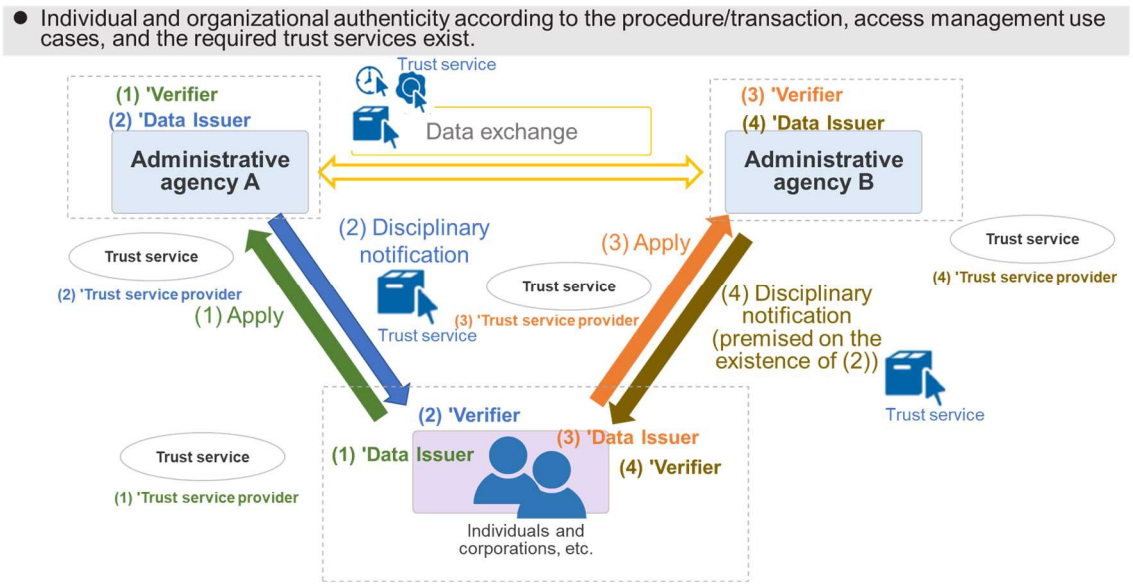
Regarding what is provided by trust services, members expressed opinion that we should first discuss trust services that assure authenticity and tamper resistance possessed by paper in cyberspace as well. In addition, it was revealed in fact-finding surveys of trust assurance that the need for trust was high in the administrative field.

At the same time, the Special Commission on Digital Administrative Reform was launched in the government, and the digital principles for structural reforms were formulated. As completing all procedures online becomes a principle with regard to procedures and services that require documentation, visual inspection, residency, and on-site participation in realizing “digital completion” within the digital principles, the Commission has been discussing “regulations requiring in-person documentation for official certificates, course, and viewing ” and other reviews.

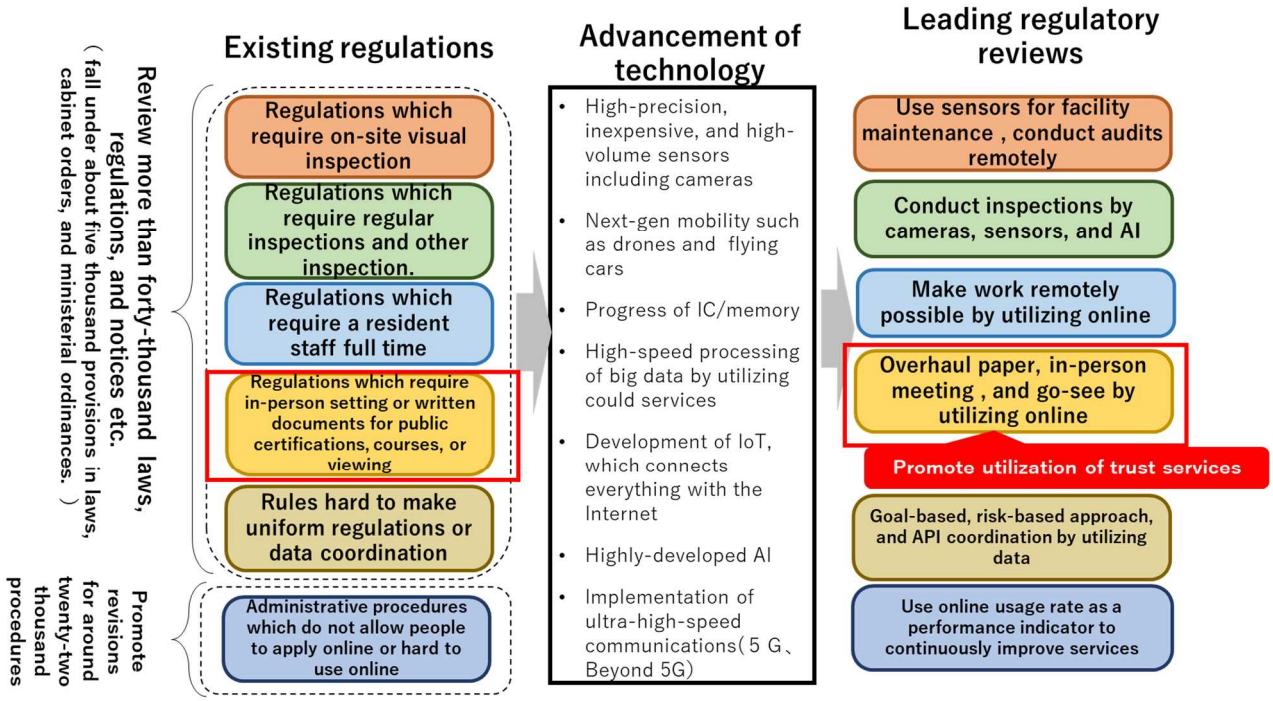
When it comes to “digital completion,” trust services are required which assure the authenticity of the time of existence of individuals and organizations (including the identification of authorities within organizations) and the resistance to tampering of data according to the procedure and transaction. Because the utilization of trust services is effective when reviewing the regulations above, trust services will be proactively used as a means of realizing “digital completion”. Specifically, the government will play a central role in discussing the technology standards and utilization policies of trust services used in official certificates and will provide input aiming for June 2025 (FY 2025), which is the intensive reform period for regulatory reviews by the Special Commission on Digital Administrative Reform.

At the same time, based on the request of Ibaraki Prefecture to utilize electronic signatures based on job position electronic certificates issued by private sector certificate authorities, there is a need to discuss trust services in which public institutions are involved in terms of issues such as developing an environment in which users can easily verify the validity of a signature, support for international standard specifications, and continuous updating of technology standards, etc. In addition, we will proceed with the discussions so as to enable local governments to utilize trust services and be able to issue more smoothly disciplinary notifications and other documents online.

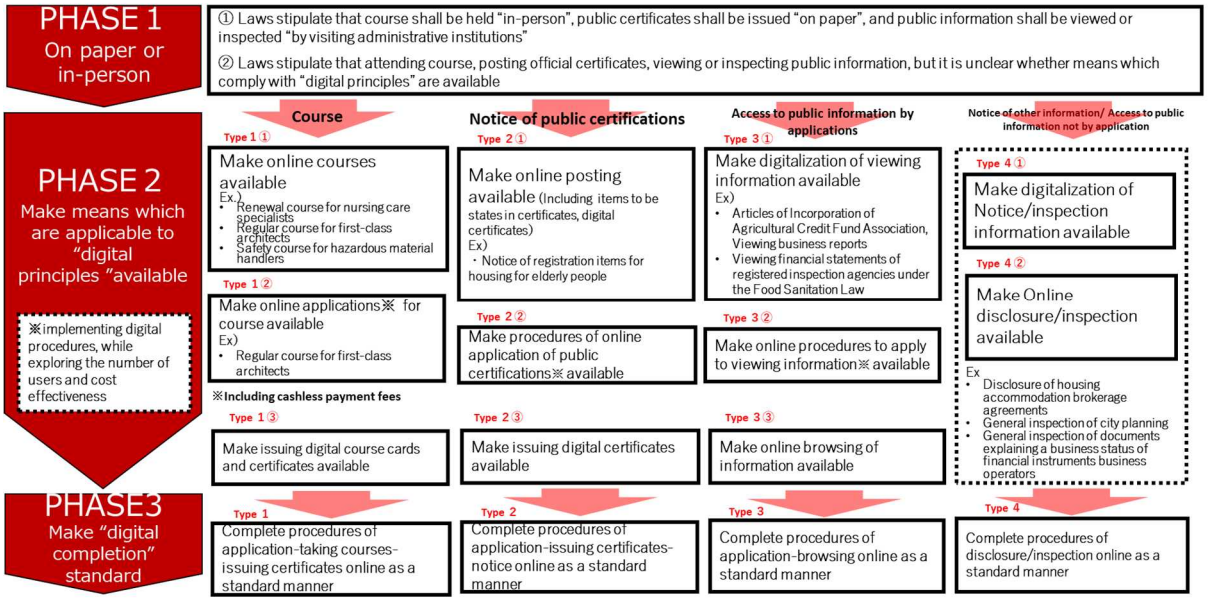
(Figure 10) Image of utilization of trust services to enable digital completion



(Figure11) Approach to review regulations based on the digital principles for structural reforms



(Figure12) Types and phases of regulations regarding written notices, in-person course, on-site viewing (In detail)



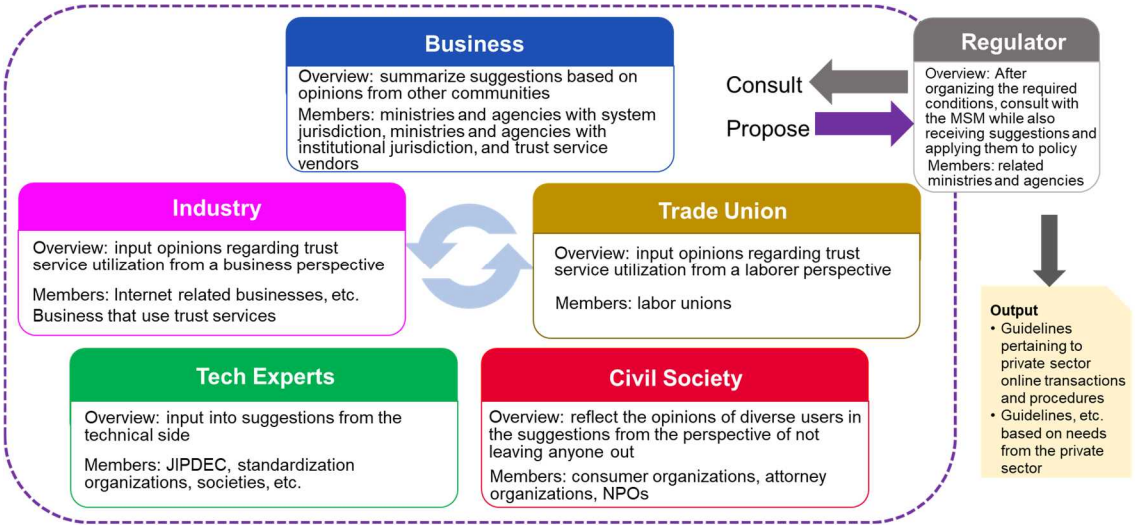
By having the government speedily promote the utilization of trust services in administrative procedures, the goal is to provide trust services that can be referenced for trust service utilization in the private sector under the multi-stakeholder model.

4.4 Promoting trust services in private sector

Discussion in the multi-stakeholder model

In order to address the issues which came up in the fact-finding surveys, a multi-stakeholder discussion about online agreements and procedures, etc. in the private sector will be carried out to incorporate the viewpoints of diverse participants from the perspective of realizing and utilizing easy-to-use trust services as technological progress advances (Figure 13).

(Figure 13) Multi-stakeholder model aimed at realizing and utilizing trust services



Agenda to be addressed in the multi-stakeholder model

Since the multistakeholder model should deal with issues that private sector companies will feel that their participation is meaningful, discussion topics of the multi-stakeholder discussions may include, for example, the “private sector online transactions and procedures,” “support for the Act on Electronic Signatures and Certification Business remote signatures and electronic seals and the updating of technology standards,” and “guidelines for use cases regarding needs from industries.” In addition, agenda items in the multi-stakeholder model going forward must be based on the trust assurance needs identified in the fact-finding surveys.

Moreover, some members expressed opinions that the multistakeholder should limit the scope of discussions to just practical handling and best practices which does not fit into legal matters in order to form opinions together.

Multi-stakeholder model utilization example (1) Disocclusions of remote signature and electronic seal technology standards

Advisory agenda

- What are the electronic signature technical standards required for the “sufficient standard uniqueness” as a measure to indicate that an electronic document is something pertaining to the user’s creation in the Act on Electronic Signatures and Certification Business (Article 3 Q&A definitive)?
- Organize the conformance of the technical standards of the Act on Electronic Signatures and Certification Business with overseas standards
- Organize the positioning of electronic seals in the Code of Civil Procedure and the Act on Electronic Signatures and Certification Business

Interested parties

- Business operators: trust service providers, JDTF, Cloud Electronic signature Service Council, Fintech Association of Japan, Japan Blockchain Association, etc.
- Industrial world: Internet related businesses, businesses that use trust services
- Experts: JIPDEC, JT2A, jurists, other standardization organizations, trust related societies, etc.
- Consumers: consumer organizations, attorney organizations, NPOs
- Laborers: labor unions
- Government: Digital Agency, Ministry of Justice, Ministry of Internal Affairs and

Multi-stakeholder model utilization example (2): Hearing of opinions regarding trust services in which public institutions are involved

Advisory agenda

Improvement issues in trust services in which public institutions are involved

- (development of an environment that allows users to easily verify the validity of signatures, support for international standard specifications)
- Organize arguments such as private sector service utilization and trust model changes as well as the division of roles and lines of responsibility between the government and private sector

Interested parties

- Business operators: Digital Agency, Ministry of Internal Affairs and Communications, J-LIS, trust service providers, JDTF, Cloud Electronic signature Service Council, Fintech Association of Japan, Japan Blockchain Association, etc.
- Industrial world: Internet related businesses, businesses that use trust services
- Experts: JIPDEC, JT2A, jurists, other standardization organizations, trust related societies, etc.
- Consumers: consumer organizations, attorney organizations, NPOs
- Laborers: labor unions
- Government: Digital Agency, Ministry of Justice, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, local governments

Considerations in the management of the multi-stakeholder model

System for fair discussion

To ensure transparency, the members participating in the multi-stakeholder model shall be recruited in an open entry manner and use a discussion format that ensures flexibility. At the same time, because the trust services are involved in transaction and procedural trust, where care is needed to make sure not to be influenced by the interests of a specific party, care is needed to make sure that the discussion is not influenced only by those who wish to participate in the discussion by their own choice. On this point, regarding those who should participate in the discussion as stakeholders, it has been pointed out that government and other neutral parties that act in an advisory capacity should approach stakeholders to participate in the discussion and lead the discussion.

Moreover, it has been pointed out that to prevent only the opinions of a specific stakeholder from having a large impact, a system needs to be devised whereby opinions are solidified within each community and then the representatives of each community comment on the opinions of the community that they represent.

System to encourage participation in the discussion

In order to encourage participation by the relevant parties in the multi-stakeholder model, a member was of the opinion that we should incorporate a system to visualize discussion contributions such as retaining a record of participant contributions on the Digital Agency's web site. At the same time, because "trust" involves the reliability of procedures and transactions conducted by various people, some members were of the opinion that instead of leaving the discussion up to the lead of those who voluntarily contribute, consideration to prevent the overall discussion from being influenced by the statements of a specific interested party is essential. Moreover, discussions on the multi-stakeholder model should refer to international standards and should be conducted in collaboration with experts and specialized institutions so that standards, which will be created in the multi-stakeholder model can be disseminated overseas.

Efficient operation

Because decision-making takes time with multiple stakeholders, there were those of the opinion that the issues should be separated into issues to be studied in a top-down manner led by the government and issues to be advanced in a bottom-up manner by listening to the opinions of the stakeholders with the policies advanced by the government to be made accessible in the multi-stakeholder model as well. Moreover,

there was the opinion that the multiple stakeholders are essentially an advisory body, and the government should have the final authority regarding the details proposed by the multi-stakeholder model.

Furthermore, regarding the agenda topics studied with the government taking the lead, opportunities should be established to listen to the opinions of a diverse stakeholder model in the multi-stakeholder model from the viewpoint of promoting trust services that are easy for many people to use.

The points mentioned above shall be considered in the operation of the multi-stakeholder model, and a deeper discussions of the decision-making and other forms of rule design will be carried out while advancing the discussions on the agenda topics in the multi-stakeholder model utilization example.

4.5 Key principles of trust policy

From the viewpoint of exploring policy for trust services, it is important to discuss with diverse stakeholders without being biased toward experts and some businesses, to consider the conformity with international standards and regulations while aiming for trust services that are easy for private sector businesses to adopt and consider the relationships with private sector businesses involved in trust services including platform companies with global influence. Moreover, as a Japan-EU digital partnership, which was launched on May 12, 2022, mentions the continuation of a pilot project initiative aimed at interoperability for trust services, the mutual cooperation between each country has become more important than ever.

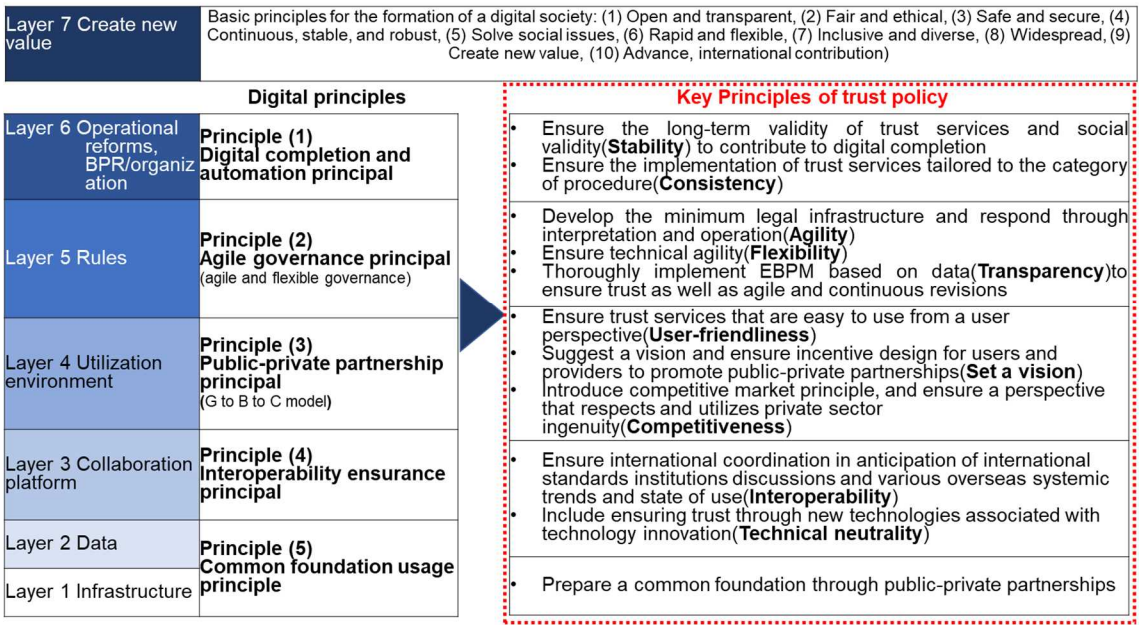
The Priority Plan for the Realization of a Digital Society (Cabinet decision on December 24, 2021), within the specific measures concerning the National Data Strategy, says that the “the Digital Agency will establish basic ideas for the framework for assuring trust(trust policy) by FY 2022.”[15] In the sub-working group, the members proposed (1) Setting a vision (design of the incentives (disincentives) for both the users and providers), (2) stability (assurance of long-term validity and social validity), (3) minimality (minimize policies to find in a top-down manner), (4) and flexibility (assurance of technical and economic agility) as elements that should be considered in the formulation of the trust policies. (Document 18 “Arguments Concerning Policy Formulation to Realize Trust Assurance in Service Provision”)

To establish principles for multiple stakeholder participants including the government

[15]Digital Agency, “Priority Plan for the Realization of a Digital Society (Text)” (1) Realizing a Framework to Assure Trust (p. 35), (December 24, 2021)

to discuss policies relating to trust, it is considered that trust policy, which fulfils characteristics described in figure 14, should be established. The Sub-working group organized the characteristics in which the basic approach of the framework for assuring trust should satisfy as the “key principles of trust policy” in a way that supports “digital principles” (Figure 14)

(Figure 14) Key principles of trust policy



Some members pointed out that the adoption of trust services by society will lead to further stability in judicial decisions, the frontline ease-of-use should be considered in the adoption of trust services, and careful attention should be paid to the discussions within the United Nations Commission on International Trade Law (UNCITRAL) in discussing international interoperability.

The key principles of trust policy shall support the “digital principles” for structural reforms, Society 5.0, DX, and DFFT, and should be utilized as principles when discussing policies for establishing trust base in the Digital Agency and multi-stakeholder model. With regard to technical standards which have already been established internationally, it is important to clarify technical standards that should be referred to in Japan and seek to harmonize standards. In the long run, as the requirements of “digital completion” become clear, it is necessary to explore the needs of trust services and usage environment of trust services.

5. Action Required

To implement trust assurance, we should discuss both “application layer,” which provides trust services that meet the needs of users and “trust service layer,” which provides infrastructure that assures authenticity and non-tampering. Regarding the “trust service layer,” it is considered that we could explore technical standards based on use cases. Hence, by coordinating with the Special Commission on Digital Administrative Reform and creating a community to discuss trust services’ policies with diverse stakeholders, both the government and private sector will reflect opinions of diverse stakeholders and will implement trust assurance as follows.

5.1 Promote administrative digital completion

The government will play a central role in discussing the technology standards and utilization policies of trust services used in official certificates and will provide input aiming for June 2025 (FY 2025), which is the intensive reform period for regulatory revisions by the Special Commission on Digital Administrative Reform. At the same time, considering the request of Ibaraki Prefecture to utilize electronic signatures of job position electronic certificates issued by private sector certificate authorities, we will discuss trust services operated in which public institutions are involved in terms of issues such as developing an environment in which users can easily verify the validity of a signature, support for international standard specifications, and continuous updating of technology standards, etc. We should also proceed with discussions so as to enable local governments to utilize trust services and be able to issue more smoothly disciplinary notifications and other documents online. As a use of trust services, the government should deepen use cases of trust services, explore a framework of trust assurances, and expand its efforts to utilize trust services to private sector.

5.2 Establish a community where diverse stakeholders discuss trust

In order to incorporate diverse opinions about online agreements and procedures, etc. in the private sector, a community for discussion with multi-stakeholders will be established. The operation of a multi-stakeholder model requires the establishment of a system for fair discussion so as not to be influenced by the interests of specific stakeholders, a system to encourage the participation of stakeholders in the discussion, and a system to carry out efficient operation.

Discussions in a multi-stakeholder model relating to transactions and procedures between private sector entities should consider, for example, topics such as the “issues pertaining to private sector online transactions and procedures,” “support for the Act on Electronic Signatures and Certification Business remote signatures and electronic seals and the updating of technology standards,” and “guidelines for each use case regarding needs from the business world.” As for the “trust service layer”, since it is the basis for assuring trust, stakeholders in multi-stakeholder model will be expected to discuss necessary technical standards etc. based on use cases. Considering that so-called “cloud-based electronic signatures” have been spreading online market, we should keep in mind to create criteria which do not hamper private sector’s creativity, new services, and technical innovations, based on users’ needs for trust. In the first place, with regard to technical standards which have already been established internationally, it is important to clarify technical standards etc. that should be referred to in Japan and seek to harmonize standards. In the long run, as the requirements of “digital completion” become clear, it will be necessary to explore the needs of trust services and improve usage environment of trust services.

5.3 Develop an electronic seal policy system

Regarding time stamps, a national certification system has been operated, and in regard to electronic seals, the guidelines pertaining to standards required by certification authorities to assure reliability have been provided. Because it is anticipated that the need for certifications from issuers will increase in online transactions and procedures going forward, we should support the initiative by the Ministry of Internal Affairs and Communications aimed at the formulation of standards and conformity assessment to evaluate the reliability of electronic seal private sector services based on the “Guidelines Pertaining to Electronic Seals” announced by the ministry.

5.4 Promote internationally harmonized rule-making

Regarding identification assurance levels, we should provide input to the Digital Agency Technology Advisory Committee and utilize it in discussions concerning identity verification in administrative procedures. Development regarding identity verification levels in the private sector should continue to be studied within the multi-stakeholder model based on the DADC study results. In addition, we should continuously explore the Digital Identity Wallet which has international interoperability

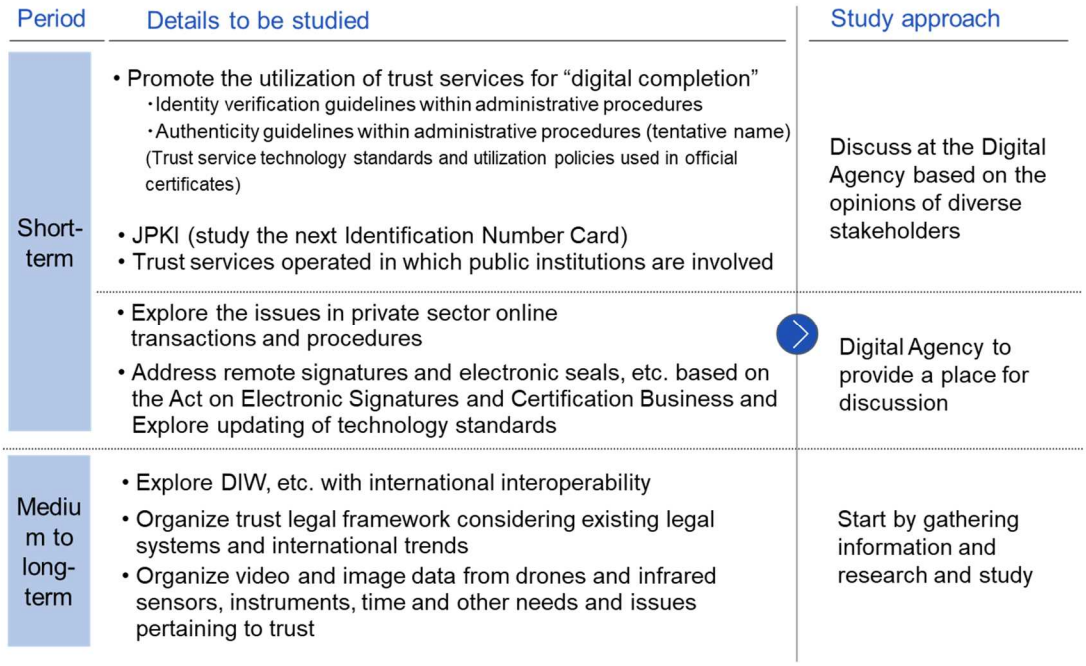
based on the fact that it is attracting global attention as a method for disclosing attributes under one's own control in such a way that Decentralized Identity and Self-Sovereign Identity (SSI) do not depend on the platform. Furthermore, while digging deeply into the market needs of trust services that are required to have international interoperability, we will also take into account trends of "standards and conformity for the evaluation of trust service reliability" in foreign countries and continue to designate "standards and conformity for the evaluation of trust service reliability" as an issue for study going forward.

In proceeding with these studies, discussions on the multi-stakeholder model should refer to international standards and should be conducted in collaboration with experts and specialized institutions so that standards, which will be created in the multi-stakeholder model can be disseminated overseas. In addition, we will clarify the concept of trust aimed at the promotion of DFFT with the goal of introducing it at the G7 in 2023.

5.5 Implementation scheme

Regarding the framework of discussions aimed at establishing trust base, based on the following, after dividing it into the characteristics to be studied with the government taking the lead and topics for which the government should provide a place for discussion, it should be divided and promoted as (1) short-term trust service implementation (promotion of the utilization of trust services aimed at digital completion (revision of identity verification guidelines in administrative procedures, creation of authenticity guidelines in administrative procedures (tentative), the utilization of trust services in which public institutions are involved)) and (2) medium to long-term trust base establishment (the Digital Identity Wallet with international interoperability, organization of a trust legal system based on the existing legal system, etc.) (Figure 15)

(Figure 15) Promotion system conclusion（Main agenda items）



6. Conclusion

Regarding arguments aimed at establishing trust base, in the “National Data Strategy” it says that, “the related industries and agencies will cooperate and study the arguments with a focus on the Digital Agency and aim for implementation in the early 2020s. Because these arguments are wide-ranging, it is important to analyze the needs with respect to the trust services and clarify priorities.”[16] When the needs were assessed through fact-finding surveys and experts in this Sub-working Group, it was revealed that there are needs for trust assurance in online procedures and transactions in a wide range of industry types/industries including the government.

A certain degree of progress on the arguments summarized in the National Data Strategy was seen through discussions in this Sub-working Group. For example, regarding the “creation of a certification scheme,” because it was learned from fact-finding studies and expert interviews that the need for issuer related certification is expected to increase in online transactions and procedures, further systematization of electronic seals is now being studied. Regarding the “establishing trust base,” the fact that “key principles of trust policy” to act as guidelines for the approach were created in the study of policies pertaining to trust by multiple stakeholders including the government was important as a precondition for the creation of trust infrastructure. In addition, facts which should be verified as a precondition and terminology that should be common knowledge in Japan and overseas were pointed out to deepen the discussion regarding “international mutual recognition” going forward. Moreover, the “Japan-EU Digital Partnership” was launched during this Sub-working Group, and the fact that an initiative aimed at interoperability of trust services between Japan and the EU was stipulated is beneficial to contribute to mutual understanding between Japan and the EU for mutual recognition. As the “remote signature and electronic seal technology standards” and other topics are discussed within the multi-stakeholder model going forward, discussions about “certification standards” are expected to deepen. Even when looking at foreign countries, the creation of standards for online identity verification by governments and the utilization of ID and trust services are advancing along with the increase in online procedures and transactions. Because it is extremely important as the G7 host country in 2023 that Japan lead the process to flesh out DFFT and promote the utilization of trust services directed at the realization of “digital completion” in the Special Commission on Digital Administrative Reform, discussions aimed at the establishment of trust infrastructure will continue to be advanced going forward.

---

16 Cabinet Secretariat IT General Strategy Office, ”National Data Strategy (digital.go.jp)”

Finally, the key principles of trust policy were created in this Sub-working Group in line with the “digital principles” based on the fundamental approach which came up from the experts during the meetings. The trust policies will be fleshed out in parallel with the adoption of the trust services. Based on the use cases, we will continue to discuss framework which assures trust within the government and multi-stakeholder model.

Members and observers

(Members)

	Yo Ota	Partner, Nishimura & Asahi
	Nat Sakimura	Executive Fellow, Tokyo Digital Ideas Co., Ltd.
	Kazue Sako	Professor, School of Computer Science and Engineering, Waseda University
◎	Satoru Tezuka	Professor, Faculty of Environment and Information Studies, Keio University
	Soshi Hamaguchi	Senior Researcher, Keio University SFC Research Institute
	Tatsuya Hayashi	Director, LocationMind Inc.
	Hiroshi Miyauchi	Attorney, Miyauchi & Mizumachi IT Law Firm
	Kazuya Miyamura	Partner, PricewaterhouseCoopers Aarata LLC
	Shin Takamura	Counselor to the Chief Cyber Security Officer, Ministry of Internal Affairs and Communications
	Toshiyuki Dote	Director of the Commercial Affairs Division, Civil Affairs Bureau, Ministry of Justice
	Shuji Okuda	Director, Cybersecurity Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry

(Observers)

Osamu Ijichi	Head of the Time Business Certification Center, Information and Communication Security Division, Japan Data Communications Association
Takayuki Idaka	Medical Information Technology Counselor, Research and Development Division, Health Policy Bureau, Ministry of Health, Labour and Welfare
Osu Ota	Chairman, Public Relations Department, Japan Digital Trust Forum
Hirohisa Ogawa	Chairman of the Steering Committee, Japan Trust Technology Association and Senior Researcher,Cyber Security Strategy Group, Digital Innovation Division, Mitsubishi Research Institute, Inc.
Mikio Ogawa	Director of Administration and Payment Systems, Japanese Bankers Association
Tetsuro Okuno	Assistant Section Chief, General Affairs Section, Pharmaceutical Safety and Environmental Health Bureau, Ministry of Health, Labour and Welfare

Seiji Kaneko	Adviser, General Affairs Section, Pharmaceutical Safety and Environmental Health Bureau, Ministry of Health, Labour and Welfare
Hiroaki Komatsu	Partner, Tokyo IT Audit Department, KPMG AZSA LLC
Soichi Sato	Director of Policy, Japan Association of New Economy
Tatewaki Sato	Council Secretariat, Cloud-based Electronic signature Service Council
Koichi Shibata	Senior Manager, DX Services Planning and Coordination Department, Seiko Solutions Inc.and Department Chairman, Planning and Management Subcommittee, JAPAN Trust Service Forum
Kenichiro Shimai	Deputy Head, Office of Medical Information Technology Promotion, Research and Development Division, Health Policy Bureau, Ministry of Health, Labour and Welfare
Masaki Shimaoka	Research Engineer, SECOM Intelligent Systems Laboratory
Kikuzo Sodeyama	Director, SKJ Tax Accounting Office
Kazukiyo Toyoshima	Managing Director, DigitalBCG Japan
Yuji Nakasu	Vice-president, Government Public Relations, SAP Japan Co., Ltd.
Hiroshi Nakatake	Representative, Japan office, Global Legal Entity Identifier Foundation (GLEIF)
Takayuki Ogura	Director, System Corporate Sales Department, Shachihata Inc.
Akira Nishiyama	Special Member (Representative, Future Trust Lab), Certification Authority Conference
Eiji Nozaki	General Affairs Section Chief, Supervisory Bureau, Financial Services Agency
Akihide Higo	Project Owner, Digital Identity Verification Project Team, Digital Architecture Design Center (DADC) Incubation Lab, Information-technology Promotion Agency
Tomoaki Misawa	Partner, PricewaterhouseCoopers Aarata LLC
Toru Yamauchi	Executive Director and Director of the Digital Trust Evaluation Center, Japan Institute for Promotion of Digital Economy (JIPDEC)
Mitsuo Wakameda	Data Strategy WG Chief Examiner, Digital Economy Promotion Committee Planning Subcommittee, Keidanren

(Digital Agency (Secretariat))

Director General Masanori Kusunoki and Deputy Director General Shusaku Indo of the Digital Society Common Function Group, etc.

(Written in order of the Japanese alphabet, names listed without honorifics, ◎ Chief Examiner)

Appendix A

有識者からの発表資料

資料１

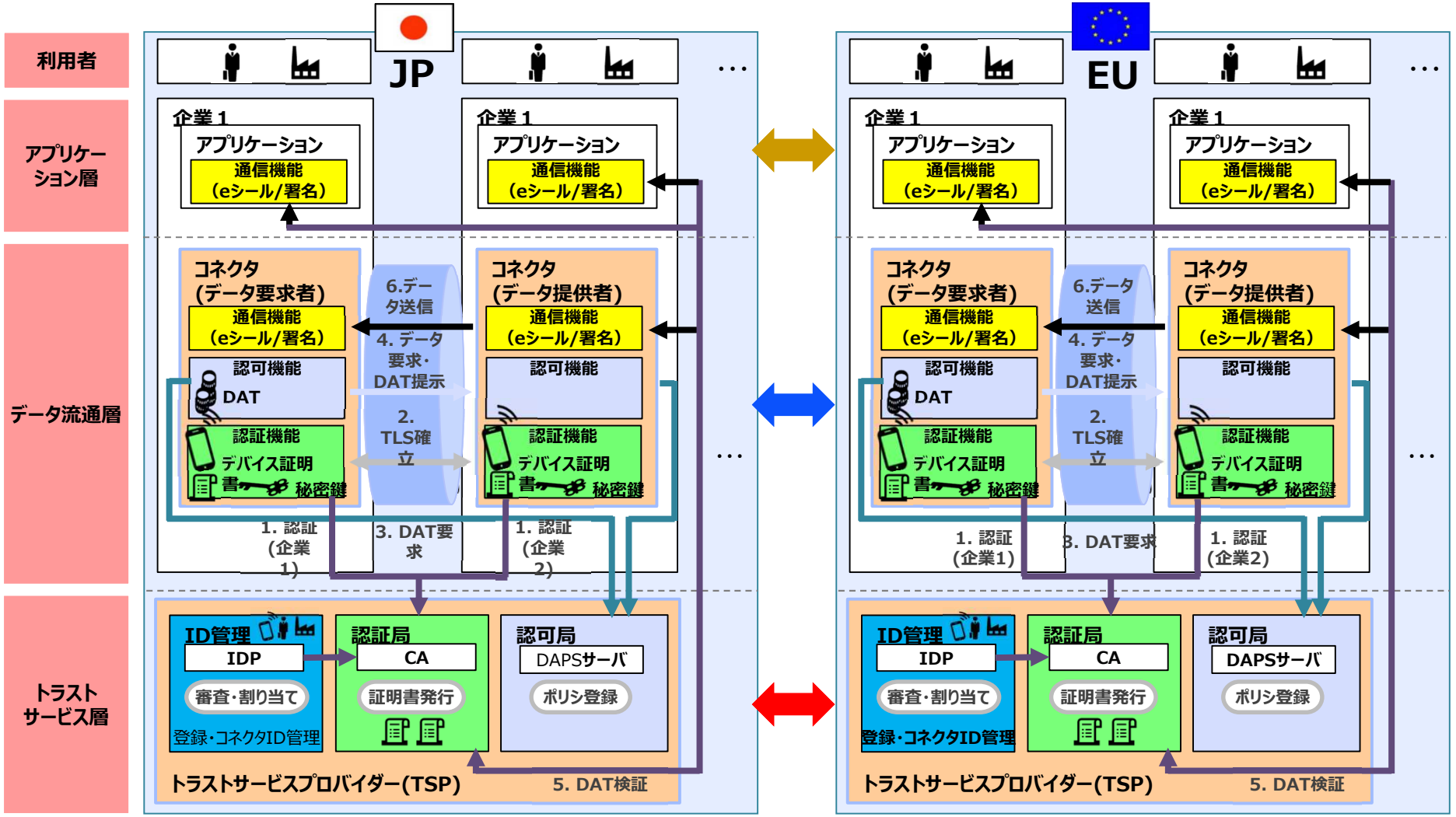
トラストを確保したDX推進SWGにおける
トラストの全体像

2021年11月18日

慶應義塾大学
手塚　悟

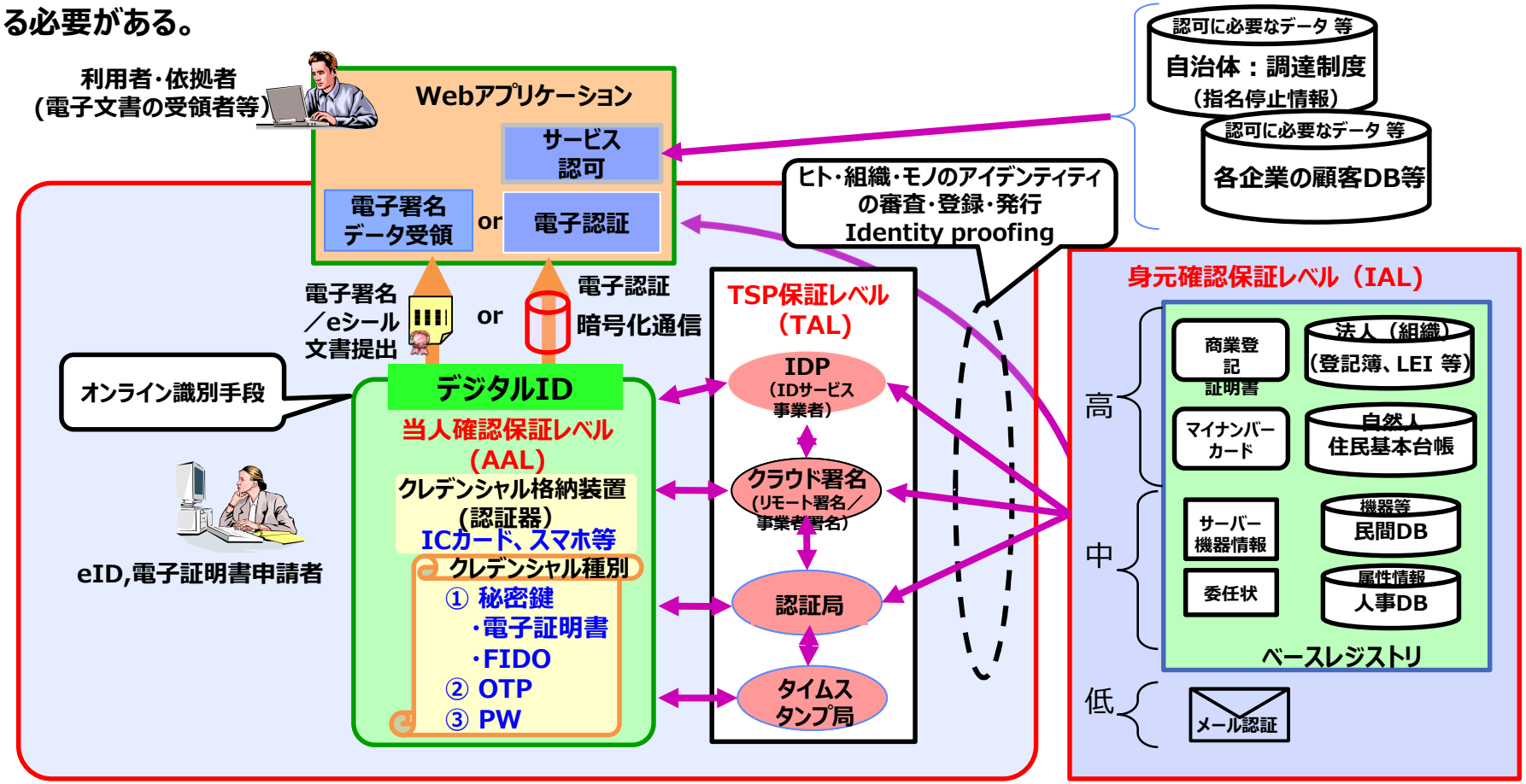
アプリケーションサービスとトラストサービスの関係

- GAIA-X/IDSAとトラストサービスの連携例
- トラストサービスは、eIDAS基準、GAIA-X/IDSA自主基準のどちらも利用可能



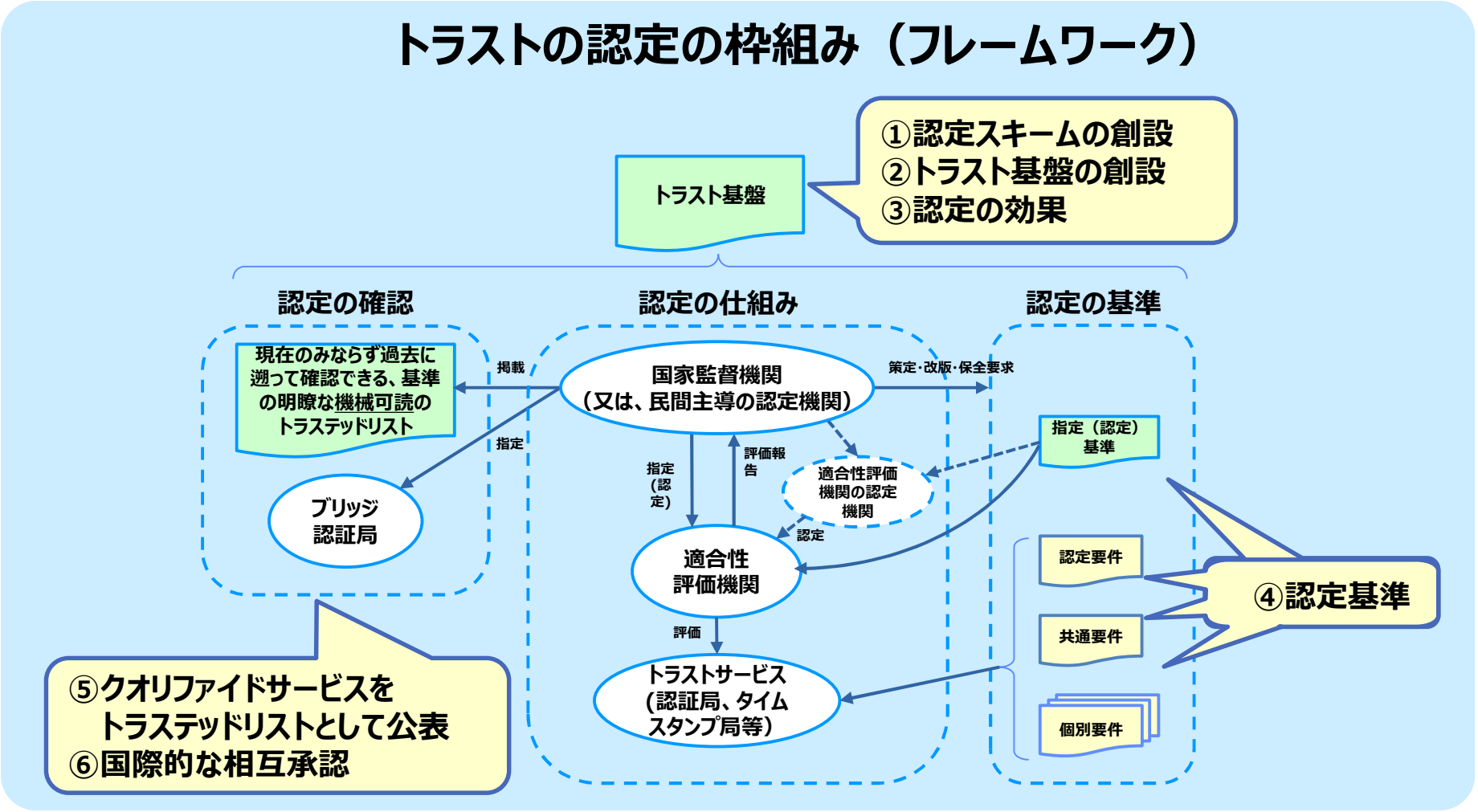
トラストの全体像

- トラストのレベルは、身元確認(IAL)、クレデンシャルの強度(AAL)、トラストサービス事業者の信頼度(TAL)で決定され、手続き記録の真正性（証拠力）が求められる程度で電子署名もしくは電子認証が選択されうる。
- 従来は業務アプリケーション毎の判断で本人を確認しクレデンシャル（パスワード等）を発行し利用者を特定していたが、社会的混乱を防ぐためベースレジストリと紐づけたデジタルIDをトラストサービス事業者から発行するスキームの創設が重要となる。
- そのためにはデジタルIDの保証レベルや、デジタルIDを発行するトラストサービス事業者に求められる保証レベルを検討する必要がある。



トラストの認定の枠組み

- トラストの認定の枠組みの検討
- 認定基準の策定が重要



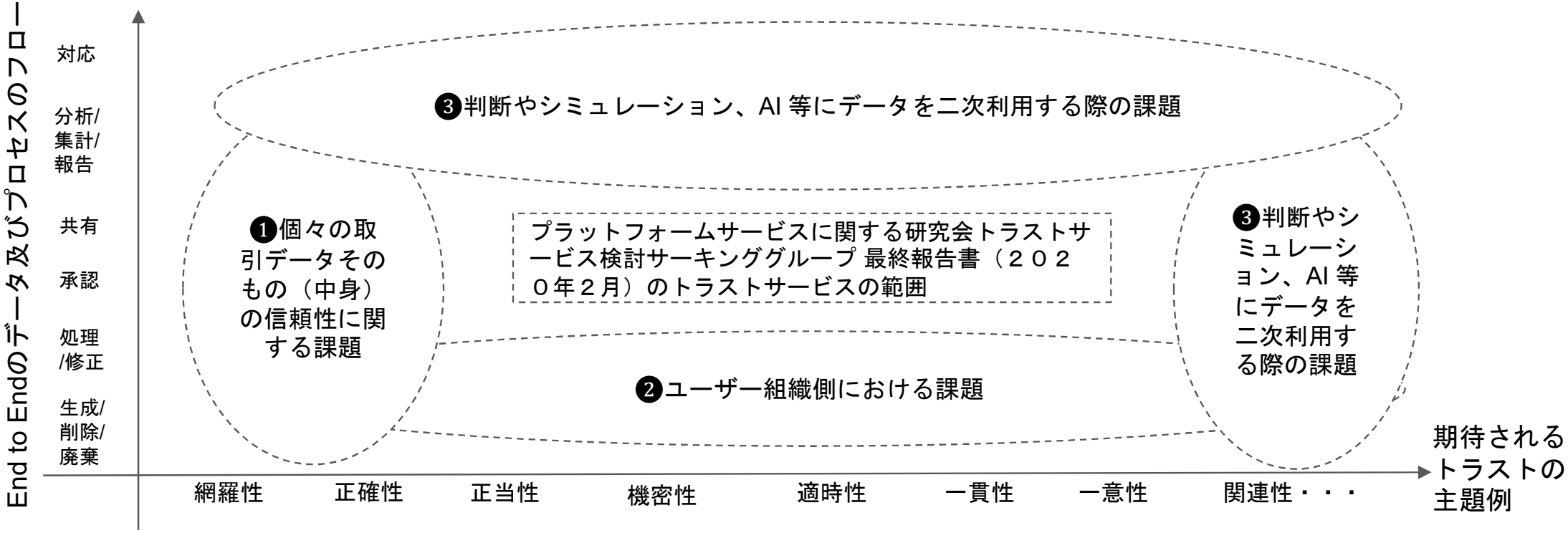
資料２

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

2022年2月25日
PwCあらた有限責任監査法人
パートナー　宮村　和谷

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

【プロセスレベル】



【エンティティレベル】

❹アジャイルガバナンス、チェンジコントロール、サードパーティートラスト（もしくはサプライチェーンガバナンス）等に関する課題

※本イメージ図は、正確かつ網羅的な整理図ではなく、課題認識のイメージを共有する目的で記載した不正確さや抜け漏れを含むものですのでその点ご承知おきください。

資料３

デジタル庁
「トラストを確保したDX推進サブワーキンググループ」

企業の業務プロセス変革及び監査業務のDX化におけるトラストサービスのニーズ、課題について

2021年11月18日

有限責任 あずさ監査法人
小松 博明

Agenda

トラストサービス活用によるメリット

ケース1：証憑へのアクセス

ケース2：不正防止

ケース3：統制状況の見える化

業務及び監査における電子的証跡の活用

データを活用した監査イメージ

継続的モニタリング及び継続的監査

制度推進に際しての課題

資料上の意見に関する部分については、作成者の私見であることをあらかじめお断りいたします。

トラストサービス活用によるメリット

テーマ	内容	参照先
証憑へのアクセス	証憑の信頼性を容易に確かめることができる。それによって、業務も効率化する。	ケース1
不正防止	改ざん防止に有効であるため、不正防止に効果が期待できる。	ケース2
統制の見える化	証跡に電子的な承認記録を残すことで、統制の見える化が期待できる。	ケース3

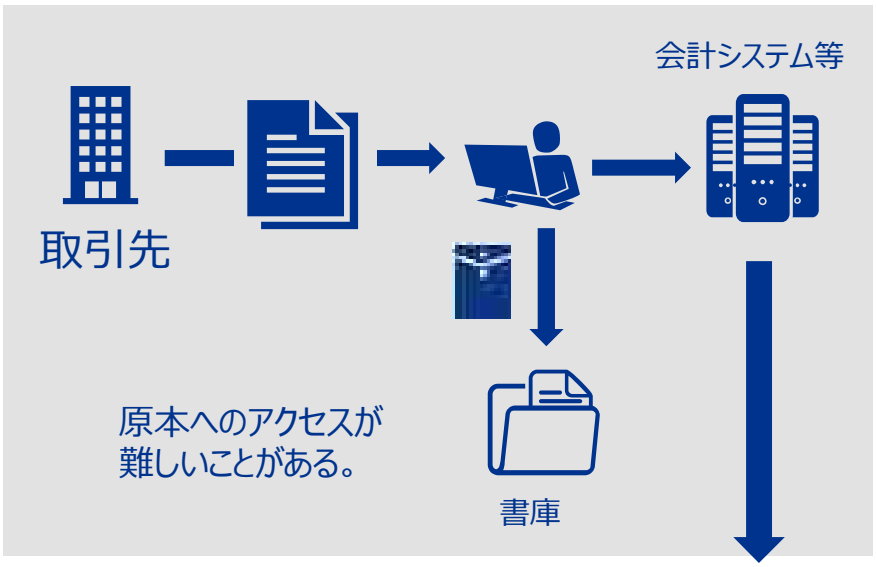
上記に加え、電子化される範囲が広がることでデータを活用した新しい取り組みにつながる。

- 電子データ化した外部証跡を利用することで、効果的・効率的な業務・監査が期待できる。
- 企業の業務プロセスや監査プロセスにデータを活用した仕組みをシステム的に組み込むことで、継続的モニタリングや継続的監査が期待できる。

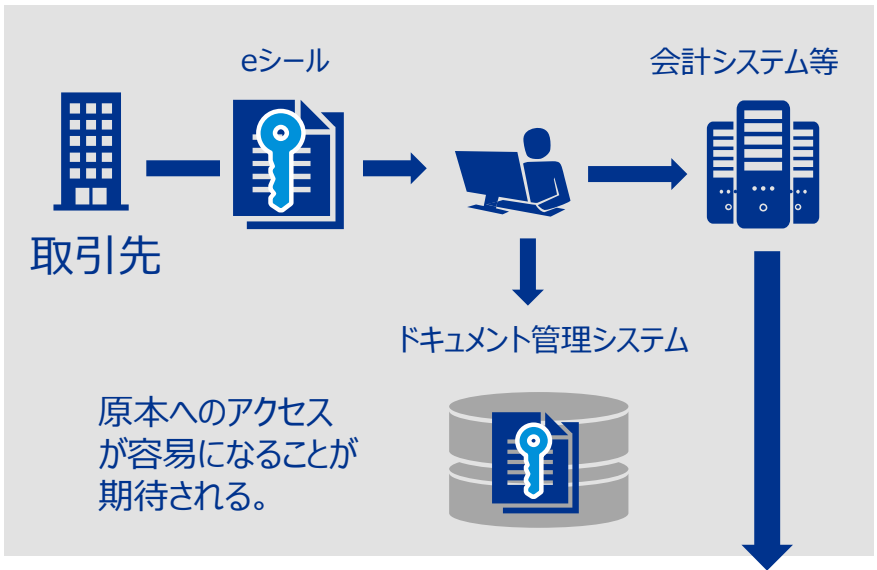
ケース1：証憑へのアクセス

■ **監査手続において外部証跡との突合を実施するのに際し、証憑の原本へのアクセスが容易になる。**

従来のケース



今後想定されるケース



✓ 全国にある拠点に保存されている、外部倉庫にある、管理者が不在など、アクセスが難しいことがある。よって、

① 経理部門へ証憑を依頼してから入手までに相当の時間を要したり

② 他の代替手続に変更することで、追加時間を要したりすることがある。

eシールの効果

① 証憑の入手が容易になることで効率化が図られる。

② 原本を直接確かめることができるため、心証を得やすい。

①② 企業内部（経理部門や監査部門など）の業務も効率化する。

ケース2：不正防止(1/2)

■ **不正の手口となる証憑の改ざんや偽造の防止効果が期待できる。**

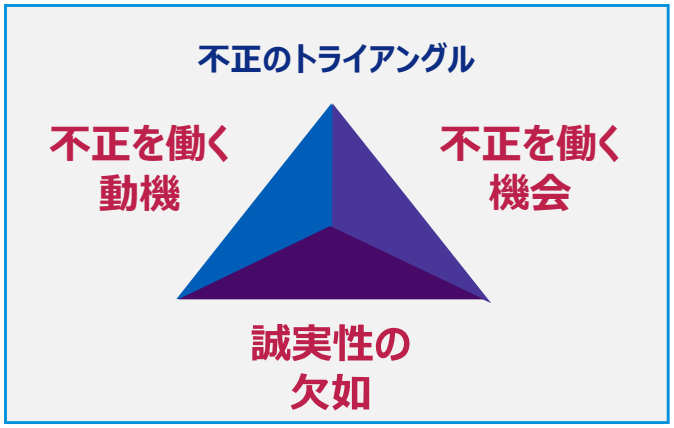
不正事案発生 → 不正調査開始 → 調査報告書報告

不正調査報告書を閲覧すると、証憑の偽造を手口とする不正案件が散見される。

証憑を偽造した不正手口（代表的な実例）

- ✓ 会社には、売上計上に必要な証憑類は整っていたが、証憑類は全て偽造されたものであった。
- ✓ 担当者が関係する書類について、印鑑等を偽造して取引を行っていた。
- ✓ 実態のない会社との取引として証憑は全て偽造されていた。
- ✓ 販売先代理先と共謀して偽造の注文書を発行させて、運送会社とも共謀して出荷案内書兼物品受領書を偽造して発行していた。

これらの不正事例を踏まえて、



監査人側

監査品質向上へつなげる。※

企業側

不正を働く機会を減らす取組み

偽造や改ざんができないような仕組みとして活用することも。

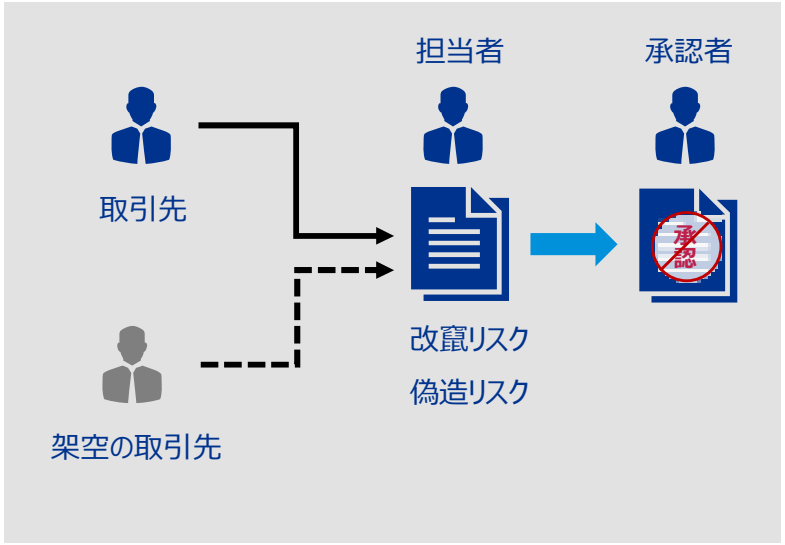
不正防止の統制整備方法には様々な方法が考えられるが、ｅシールはその一つの手段として有益と考えられる。

※日本公認会計士協会では、監査業務の改善に資することを目的に、調査事案を踏まえた提言を取りまとめて会員に配布している。

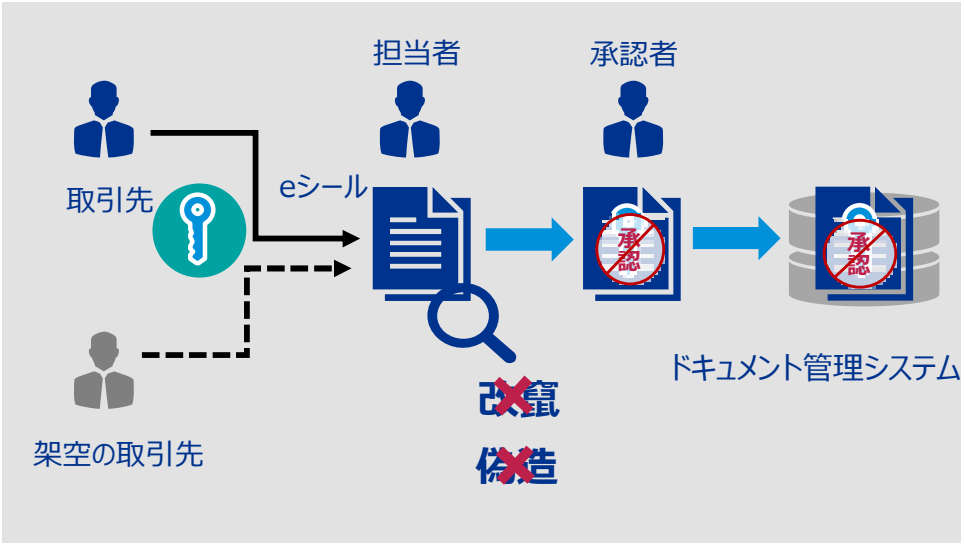
ケース2：不正防止(2/2)

■ 改竄リスクや偽造リスクの低減効果

従来のケース



今後想定されるケース



紙資料における改竄・偽造リスク

前ページの事例をまとめると、

① 担当者ベースでの証憑類の偽造・改竄

② 実態のない会社の架空取引の証跡作成

③ 取引先との共謀による証憑の偽造

e シールの効果

① 取引先からの証憑は改竄されていないことが分かるため、承認者がレビューし易い。

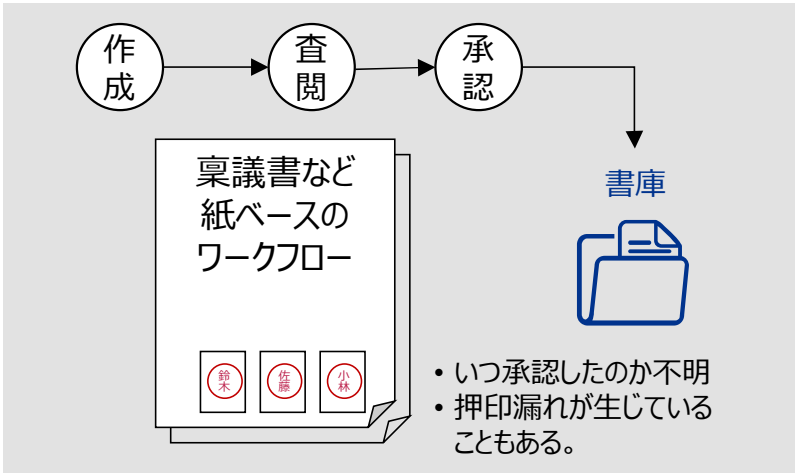
② 認証局が身元を確かめた公開鍵（証明書）によるため、架空の証憑による不正の防止が期待できる。

③ 共謀防止には難しい一面があるが、利用者権限が明確であれば不正調査等において、責任の所在が分かり易い。

ケース3：統制状況の見える化

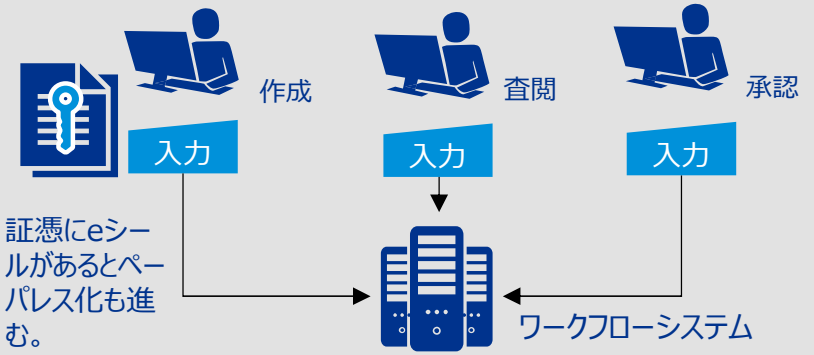
■ **紙ベースでの承認プロセスをシステムによるワークフローにすることで、プロセスを見える化する。見る化すると→監査で心証が得やすい。 企業側もルールを徹底させやすい。**

従来のケース



今後想定されるケース

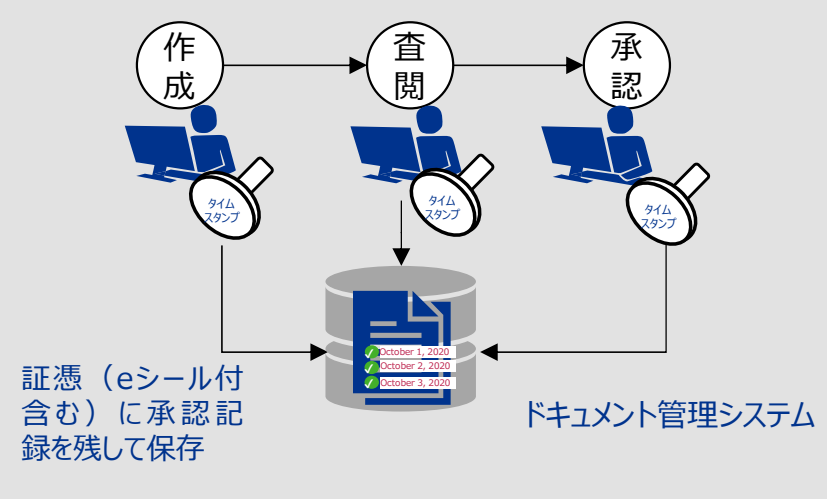
リモート環境構築のため、システムによるワークフローに変更していく流れが想定されるが、タイムリーな変更は難しいかもしれない。



紙ベースの場合、いつ承認されたのか曖昧になるケースがある。ワークフローシステムはこの点について有効であるが、すべての業務に対応することは難しいことが想定される。

eシールとタイムスタンプ※によるワークフローの構築

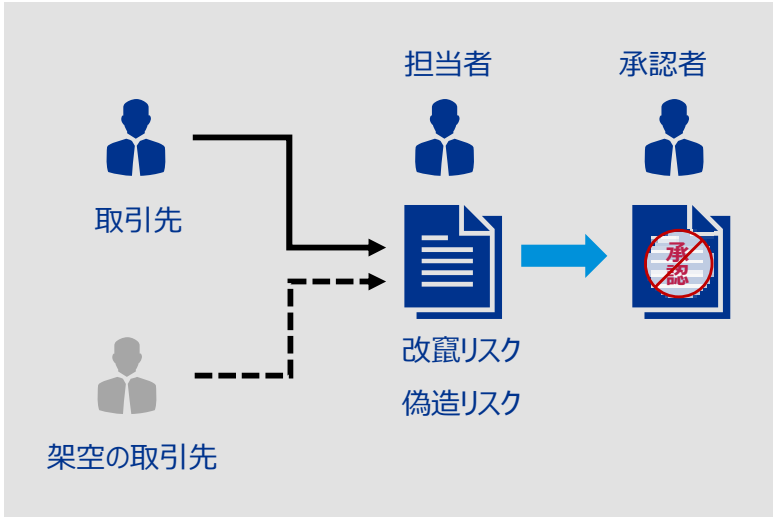
- 原本性のあるeシール付証憑をメールベースで回覧するワークフローも想定される。ただし、承認を行う端末（PC）の時刻が正確でないリスクが想定される。
- タイムスタンプを併用すれば、正確な承認日が残せるほか、重要な証跡の長期保存も可能となる。 ※電子署名含む

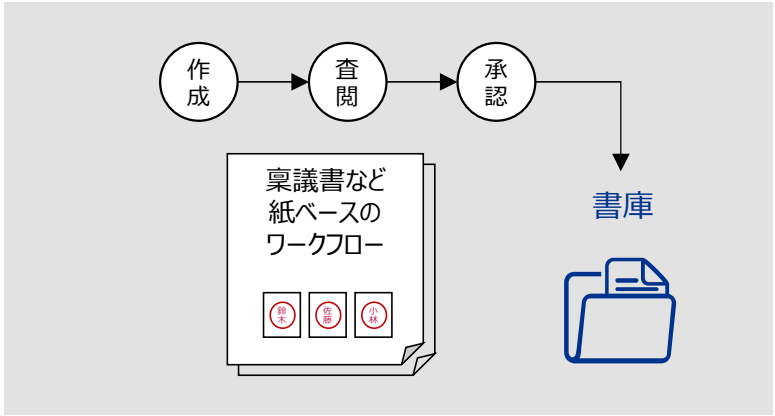


業務及び監査における電子的証跡の活用(1/2)

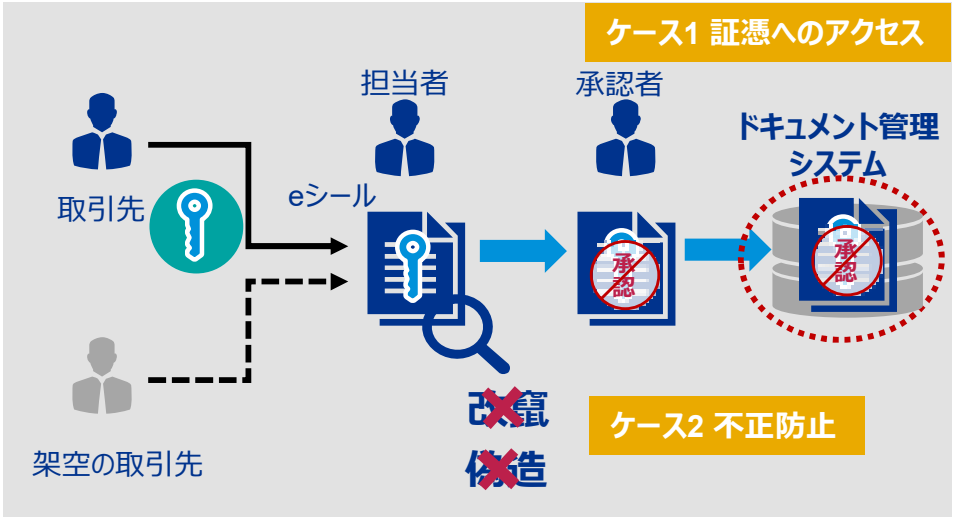
■ **紙ベースの証跡から電子的証跡に変遷することで、データを活用した監査が促進される。**

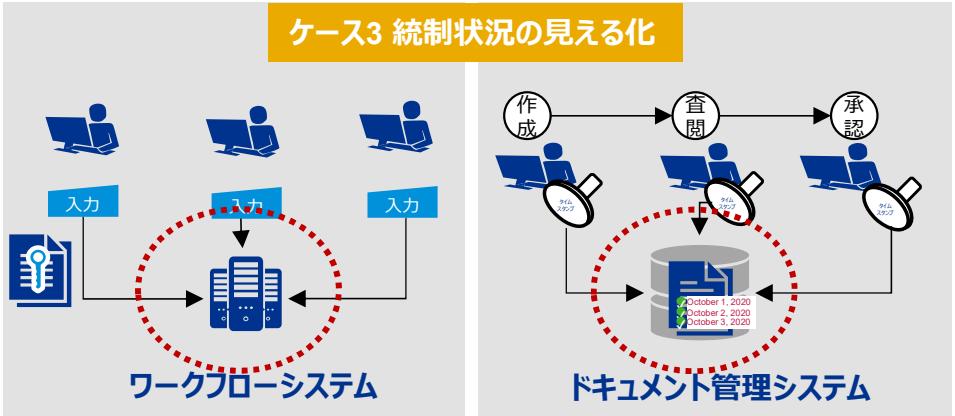
従来のケース





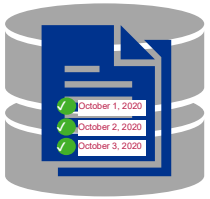
今後想定されるケース





業務及び監査における電子的証跡の活用(2/2)

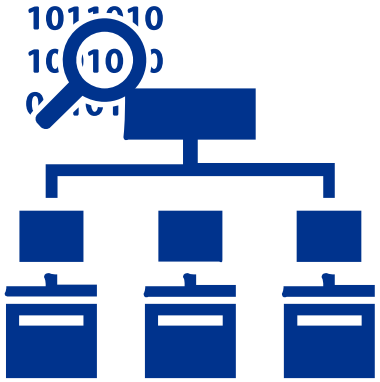
ドキュメント管理システム



ワークフローシステム

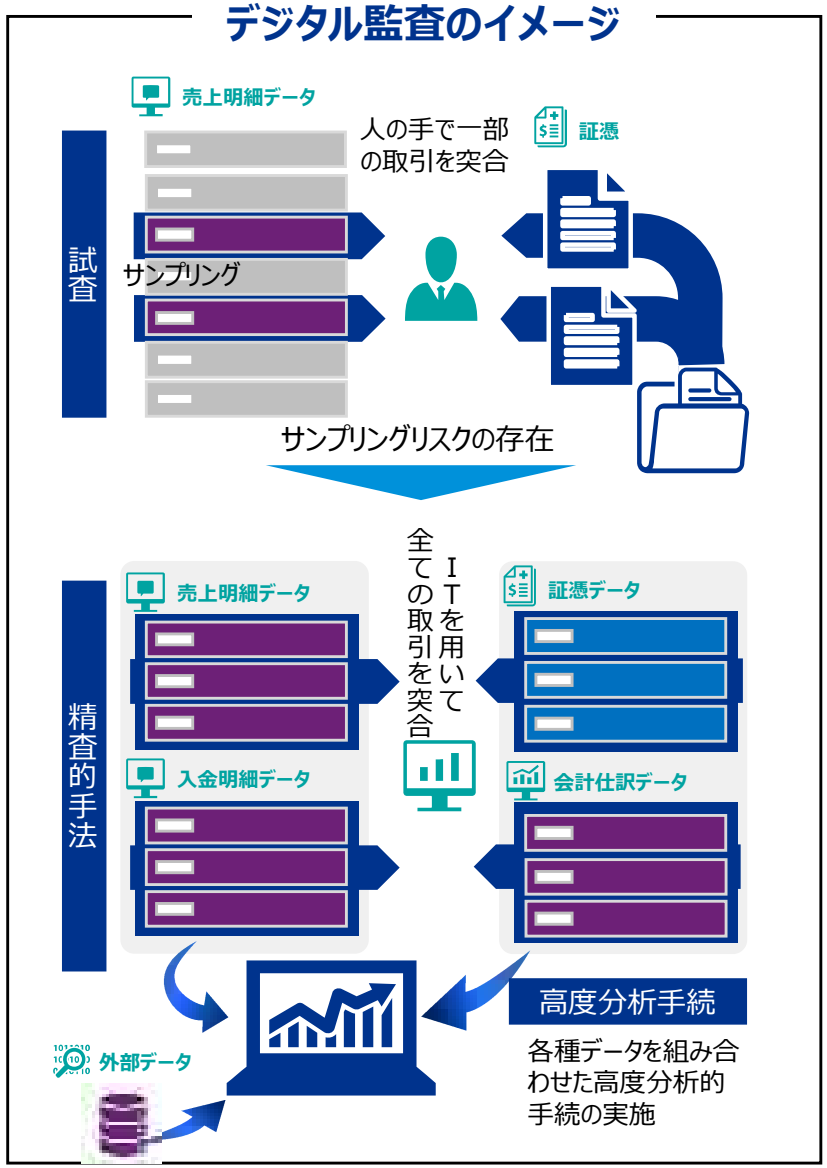
信頼性の高い監査証拠の多くは、紙ベースによる資料であった（信頼性の高い外部証拠をデータとして入手できるケースは現状多くない。）。

電子証憑※を読み取って自動処理に繋げ効率化を図る。
※eシール付きPDFによる請求書など



信頼性のある外部データを基礎に、データを活用したモニタリングや監査が促進される。

データを活用した監査イメージ



データを活用した監査の具体例

利用するデータの信頼性を事前に確かめておくことが求められるため、トラストサービスの活用は有益

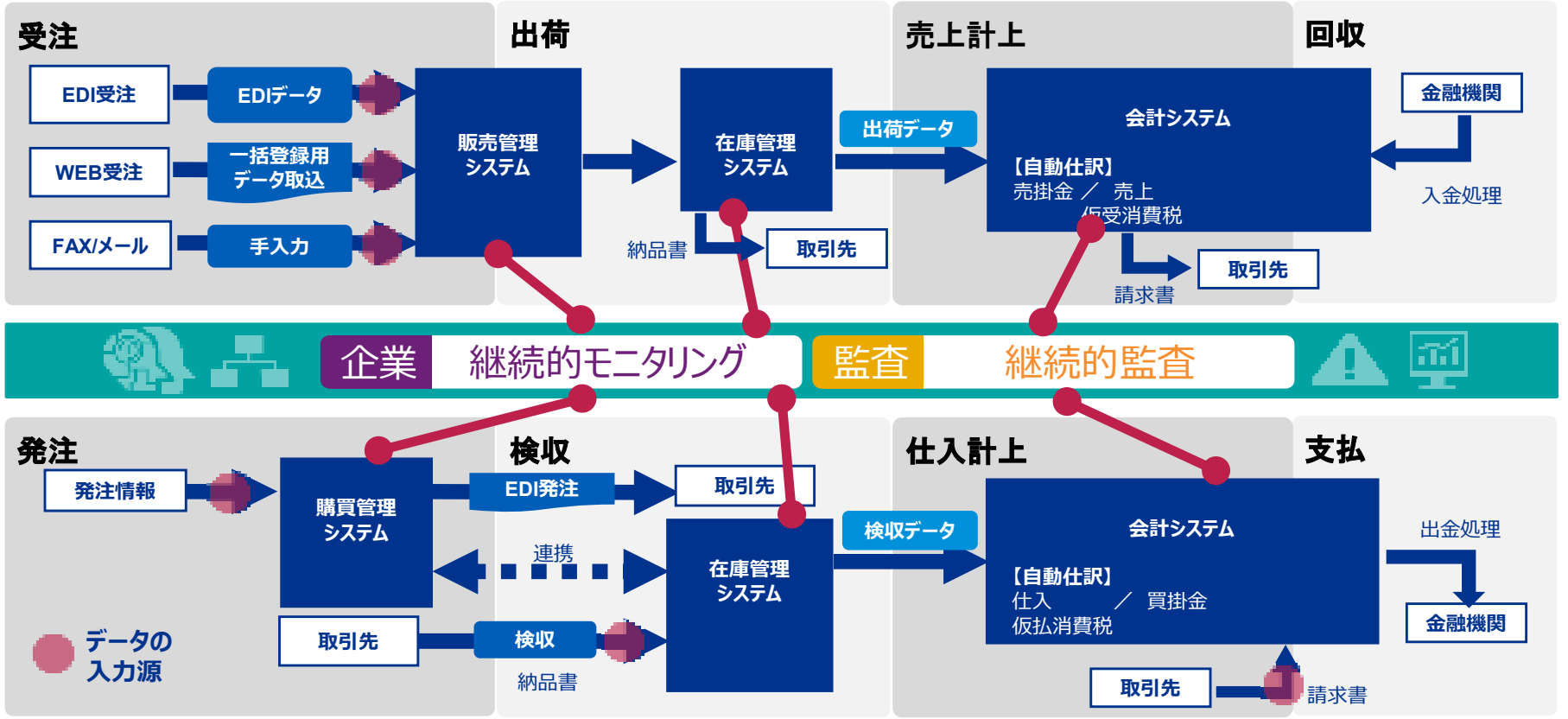
- **仕訳データを蓄積し、異常仕訳を検知**
- **子会社等も含む蓄積された財務データに基づく分析**
- **リスクシナリオに基づいて、異常値を検知する分析モデルの適用**
- **各業務プロセスのイベントログデータを蓄積・可視化し改善ポイントを分析するプロセスマイニング**

上記のロジックや機能をシステム的に組み込むことで、継続的モニタリング（経営の高度化）や継続的監査（監査の高度化）が可能になる。

継続的モニタリング及び継続的監査

- ✓ 各基幹システムのデータを継続的に収集し、一定のロジックに基づきデータを分析するツール等を導入し、適時にアラートを発信
- ✓ データの入力源についての信頼性を担保する仕組みとして一般的には人的又はシステムによる内部統制が構築されるが、トラストサービスの活用は有益※(不正データが混在するリスクの低減、アラートが生じた場合の証憑への遡及容易性 など)

※ 設定内容により多数のアラートが発生するが、フォローするためには、原始証憑まで遡る必要がある場合が多い。



制度推進に際しての課題(1/3)

トラスト基盤の構築・普及により新しい取り組み（システム化による自動処理、データ活用にる業務/監査の高度化など）によるメリットが生まれるが、以下のような課題が考えられる。

項目	課題	参考
データ標準	• 自動化によるメリットを目的としてシステム化を進めるためには、データ仕様が明確になっていることが必要になる。なお、異なる業界でも流通する普遍的なデータ標準（帳票様式）が望ましい。 • 電子証憑にメタデータが付与され、効率的に読み込むことができることが望ましい。	• 紙資料を取り込んだPDFをRPAにより読み込んで自動検証に繋げる取り組みは可能であるが、基礎証憑のフォーマット形式やPDFへの変換精度によって、識別できないことがある。 • CAAT（Computer Assisted Audit Techniques）ツールやERPパッケージに、読取機能や改ざん検知機能などが付与されると多くの人が活用しやすくなる。 • トラスト基盤と直接関連するものではないが、データ標準化の観点として、ISO21378（監査データ標準化の国際規格）がある。
コスト	• システム化を行うためには、コストに見合った便益がないと難しい。 • 一部の業務に係る証票が電子化されている状況では、システム変更のコストに見合わないことが想定される。 • 大きな投資ができない企業でも活用できるように、ERPやクラウドベンダーなどが対応できると望ましい。	• 大企業はサプライチェーンの中で定型取引についてはEDIの活用が進んでいる。非定型の取引についてもシステム化するには、コストメリットがあるかが重要な要素になる。 • 電子取引は、電子帳簿保存法に基づく電磁的記録の保存のための措置への対応が必要になるが、データの有効活用を推進するメリットを感じさせる支援策があると有益。

制度推進に際しての課題(2/3)

項目	課題	参考
暗号鍵の管理、承認手続	• 暗号鍵が不正に流出しないように管理を徹底する必要がある。 • 企業側の利用者権限ルールの明確化、厳格な運用が必要になると考えられる。 • 幅広い証憑において利用可能となるが、物理的な社印と管理方法が異なるため、従来のルールで良いか検討が必要と考えられる。	• 暗号鍵を各利用者の個別管理に委ねる対応は、不正利用のリスクが高まる要因となるため、（組織規模によるが）集中管理が望ましい。 • USBやPCに保存する場合は、耐タンパー性の考慮は必須になるが、PC交換が難しい場合やUSBなどの物理管理を避けたい場合も想定される。 →集中管理のための専用設備の投資や鍵の管理方法を考慮すると、業務委託やクラウドサービスの活用は有益なものになると考えられる。
証明書の信頼性の確保	• 認証局のセキュリティの確保、証明書のインテグリティの確保のための制度作りが必要 • 外部委託やクラウドサービスを活用する場合は、その委託先やクラウドベンダーのセキュリティや処理のインテグリティの確保も必要	• 認証局のセキュリティや証明書のインテグリティに関する評価制度は、既存の他の制度が存在するため、それらが参考になる。規制やガイドラインが重複しないような調整が望まれる。 • eシールの活用も踏まえて請求書発行プロセスを外部に委託する場合は、財務報告の主要なプロセスであることから、SOC1/SOC2などの外部評価があることが望ましい。

制度推進に際しての課題(3/3)

項目	課題	参考
制度理解の推進	• 企業の業務担当者、内部監査人、外部監査人（監査法人等）の、当該仕組みの理解促進が必要であり、そのための教育訓練が必要になる。 • 各種団体が推進に関与する体制があるとより望ましい。	• 日本公認会計士協会では、複数の関連する研究報告等を公表している。ｅシール制度が確定していない状況があり、利用者側の立場としての理解度向上に向けた研修などの取り組みは不足している。

日本公認会計士協会が公表している関連した研究報告

（2013/7/30）研究報告43号
「電子的監査証拠～入手・利用・保存等に係る現状の留意点と展望～」

（2016/3/28）研究報告48号
「ITを利用した監査の展望～未来の監査へのアプローチ～」

（2016/12/26）研究報告50号
「スキャナ保存制度への対応と監査上の留意点」

（2019/1/31）研究報告52号
「次世代の監査への展望と課題」

（2021/7/30）研究報告56号
リモートワークに伴う業務プロセス・内部統制の変化への対応（提言）

リモートワーク環境下における課題等がまとめられている。
トラスト基盤の構築はいくつかの課題に対して有効なものとなる（監査証跡の信頼性確保など）

（2021/9/9）研究報告58号
リモートワークを俯瞰した論点・課題（提言）

ｅシール等について紹介。
日本公認会計士協会としても、リモートワーク実施のために、トラストサービスの枠組みによる電子データの信頼性保証の体系的な取り組みが求められる旨を提言

資料４

デジタル庁：トラストを確保したDX推進サブWG

「税務関連業務のDX化の課題について」
～改正電子帳簿保存法による対応～

SKJ総合税理士事務所
所長・税理士　袖山 喜久造

民間企業等の税務関連業務のDX推進上の課題について

1. 業務においての取引書類

会社が行う業務で取引先とやり取りする取引書類は、ほぼ税法(特に法人税法や消費税法)で保存が必要な書類となります。取引書類は税法等で保存義務が規定され、税法等の規定による保存が必要となります。

2. 取引書類の社内処理

取引において取引先に発行又は受領する書類は、社内において必ず処理が必要です。会社内の業務処理を書面で行うか、データで行うかにより業務効率、適正性が異なってきます。書面処理は各担当者の属人的能力に依存します。データ処理の場合にはシステムにおいて一定程度の適正性や確実性が担保可能であり、業務効率も向上することになります。

3. 社内処理の電子化の課題

①取引書類をデジタルデータに変換する必要(発行元が作成したデータを活用)
②社内処理をデータ処理が可能となるワークフローシステムの導入が必要(DXの活用)
③社内システムに取引情報を入力する必要(DXの活用)
④取引書類データは、電子帳簿保存法の入力や保存要件を満たす必要(電帳法要件を満たしたシステム導入)
⑤税務関連帳簿書類を法定期間保存する必要(安全性のあるストレージ)
⑥重要な取引書類については、データの真正性を確保する必要(改ざん等の防止)
⑦取引書類の授受をデータで行う場合には、発行元の証明が必要(角印に代わる措置)

4. 電子化の阻害要因

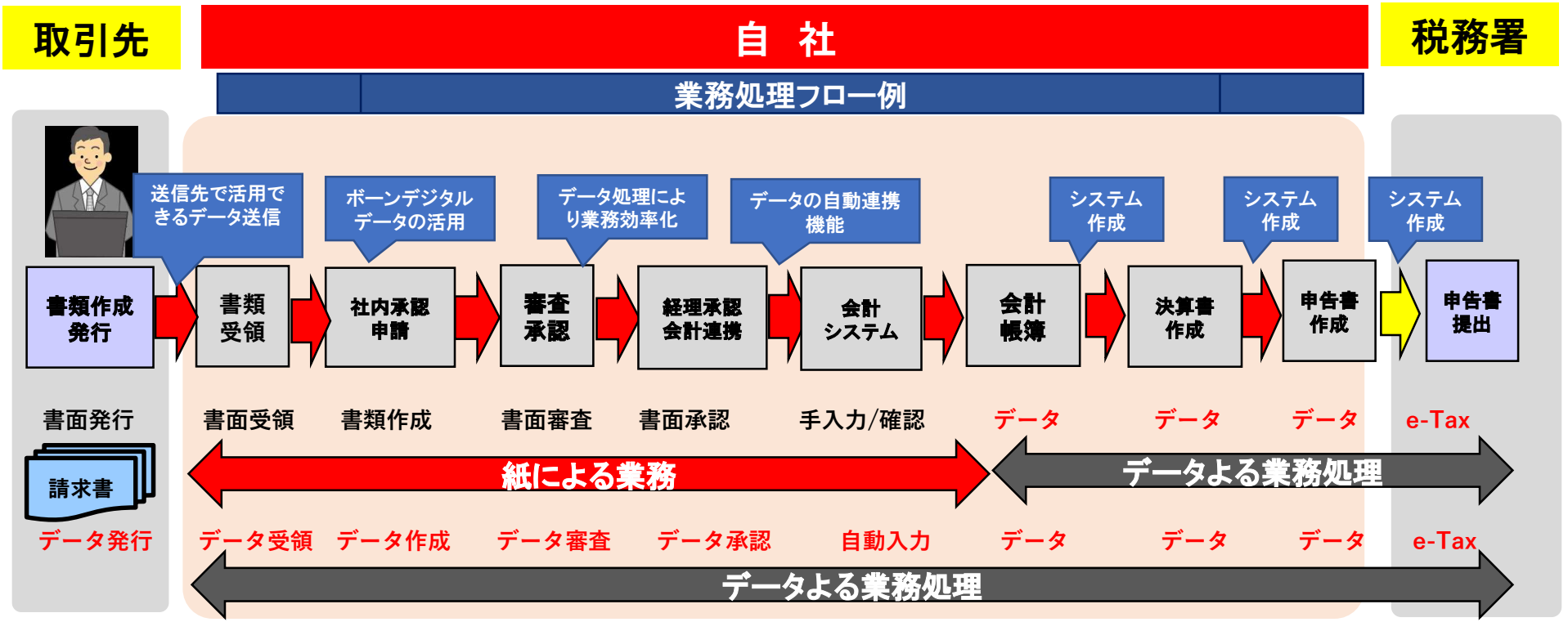
①電子化するためのコスト(特に中小企業も利用できるパッケージやソリューションが必要)
②取引先の協力が得られない(取引書類のデータ発行や受領の理解をどのように得るか)
③誤送信リスクや発行元の信用ができない(専用システムの利用や信頼できる認証局による電子証明書が必要)
④電子化の利便性が感じられない(社内処理は一気通貫でデジタル化を進める必要)
⑤現在のやり方を変えたくないという社内風土(トップダウンで業務改革を行う風潮を醸成する)

民間企業等の税務関連業務のDX推進上の課題について

5. 税務関連業務の電子化

法人税、消費税法の税務申告においては、電子申告が義務化(資本金1億円超の法人等)され、申告時には申告書類はデジタル化されている。また、ほとんどの企業において会計帳簿はデータで作成されているが、社内処理は依然として書面で行う方法が定着している。

書面処理をデータ処理に変更することは、社内運用のリスクがあり消極的な企業が多いことは事実である。

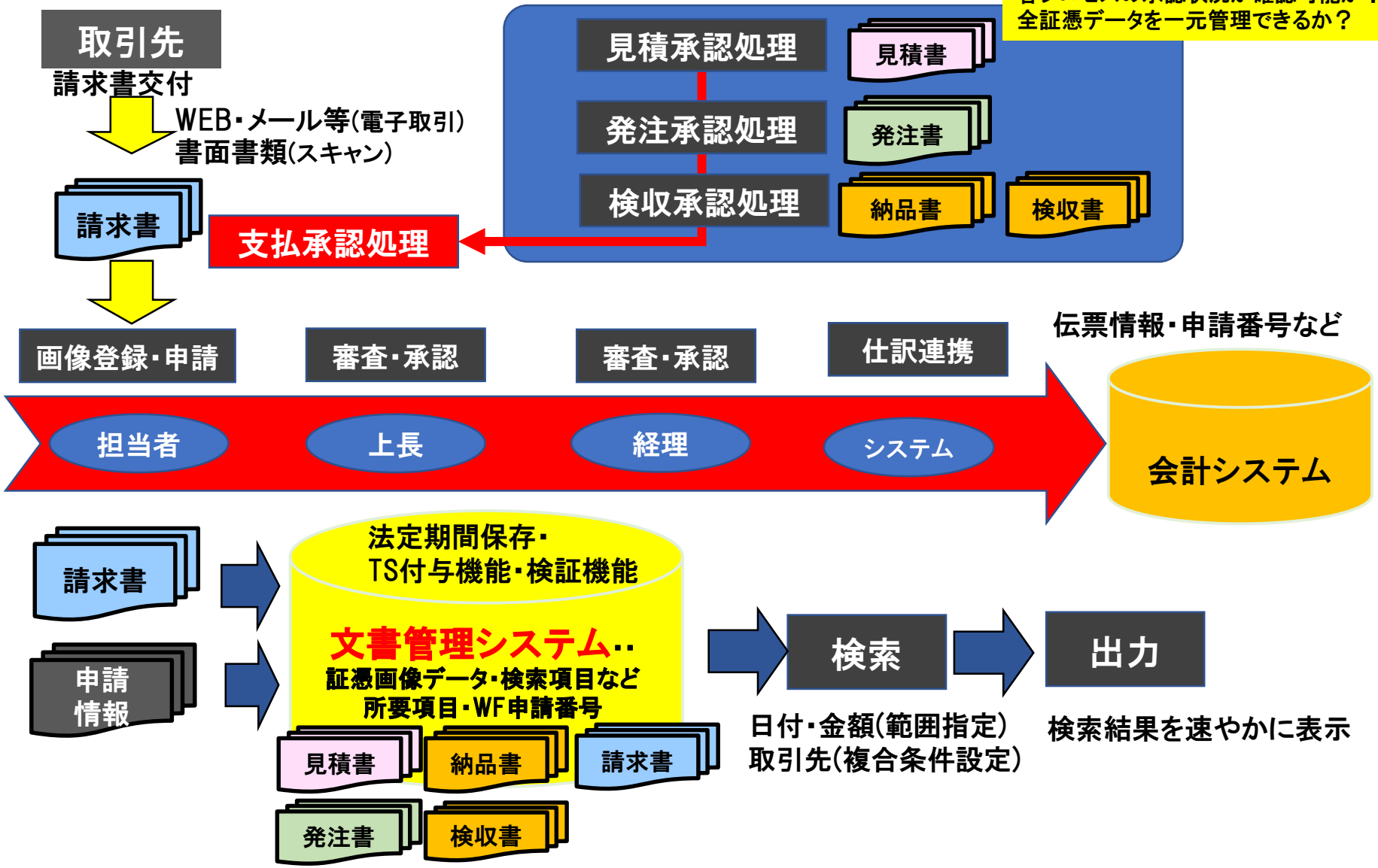


税法関連帳簿書類等の電子化関係法令

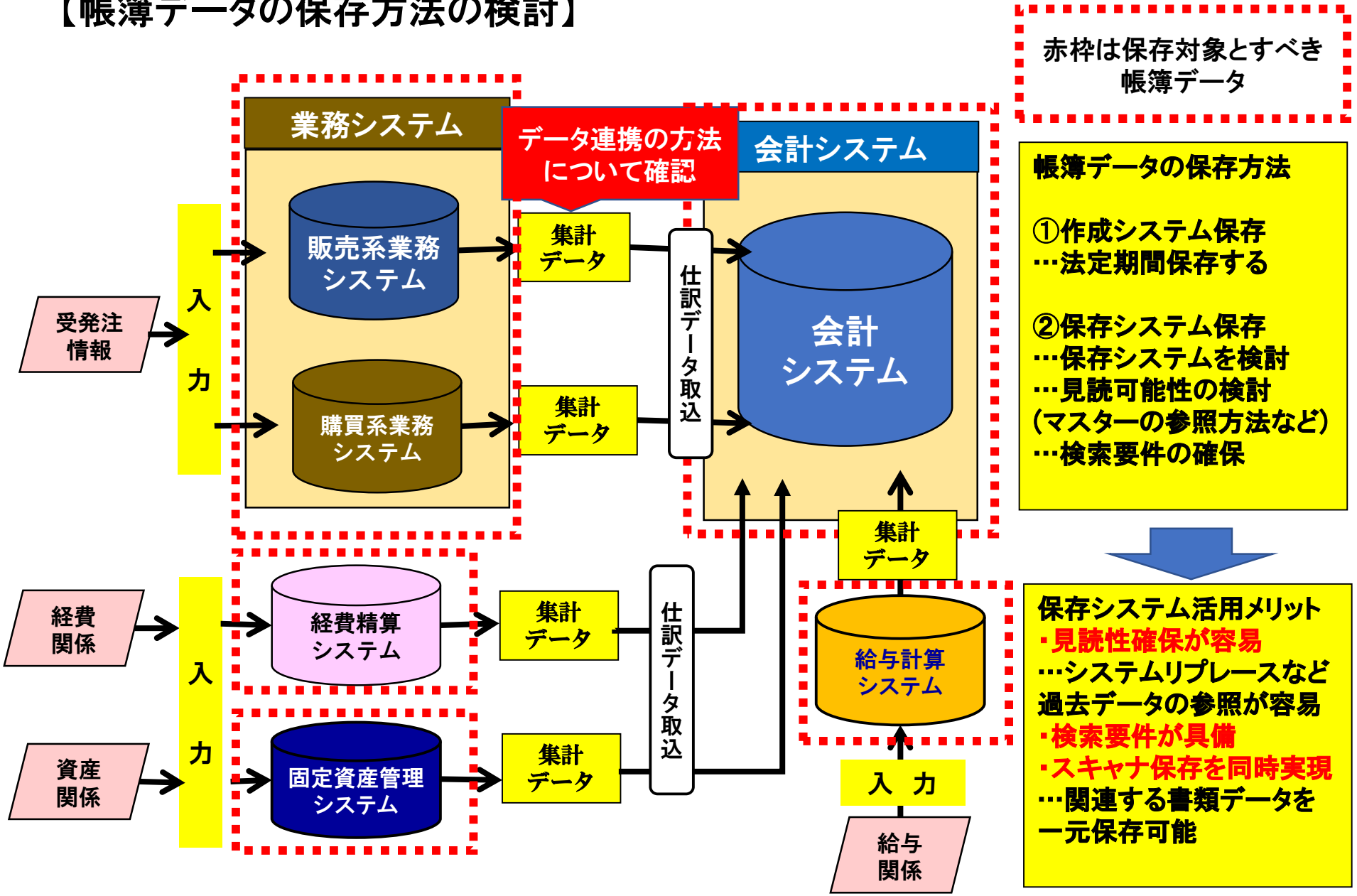
	国税関係帳簿	国税関係書類			電子取引
		決算関係書類	取引書類		
			自社発行の控え	取引先から受領	国税関係書類以外の書類
説明	資産・負債・資本の金額に影響を及ぼす一切の取引を記録	決算に際して作成される書類	取引に関して相手先に交付した書類の控え	取引に関して相手先から受領した書類	取引に関し電磁的方式で授受される取引情報
授受種別	--	ー	書面	書面	電磁的記録
保存方法	書面	書面	書面	書面	電磁的記録
保存義務規定	税法	税法	税法	税法	電帳法
帳簿書類の種類例示 電子取引例示	仕訳帳	貸借対照表	見積書控	見積書	EDI取引
	総勘定元帳	損益計算書	契約書	契約書	電子契約書
	その他の帳簿	キャッシュフロー計算書	注文書控	注文書	メールデータ
	現金出納帳・当座預金元帳・手形帳・売掛金元帳・買掛金元帳・他債権債務事項・有価証券・固定資産台帳・繰延資産・他固定資産・売上帳・他収入金額・仕入帳・他経費に関する事項	株主資本等変動計算書	送付書控	送付書	メール添付書類
		付属明細書・個別注記表	納品書控	納品書	WEB請求書
		実地棚卸表	請求書控	請求書	WEB領収書
		勘定科目組換表	領収書控	領収書	FAX
		その他決算整理作成書類	その他取引書類控	その他取引書類	その他授受された取引データ
関連条文(法人・所得) (保存義務関係規定例) 所得税又は法人税の納税義務者若しくは消費税の保存義務者	法人税法第126条第1項(青色)・同法第4条の2第1項(連結)・同法第150条の2第1項(普通)				電帳法第7条 同法規則第4条第1項
	法規則第59条第1項第1号他	法規則第59条第1項第2号他	法規則第59条第1項第3号		
	法規則別表20	法規則第56条・57条			
	所得税法第148条第1項(青色申告者)				
	法規則第57条～第64条・規則別表1				
消費税法関連条文例 (令和5年10月以降)	消費税法第30条第7・8項	ー	消費税法第57条の4	消費税法第30条第7項・9項	
	同法令第49条第1項～第3項		同法規則第70条の10	同法規則第49条第4項～9項	
電子化関連法令 (データで保存する場合の関連規定)	電帳法第4条第1項	電帳法第4条第2項	電帳法第4条第2・3項	電帳法第4条第3項	
	同法規則第2条第1・2項(一般)	同法規則第2条第3項	同法規則第2条第3項(データ)	同法規則第2条第4～7項(スキャナ)	
	同法規則第5条第1～5項(優良)		同法規則第2条第4～7項(スキャナ)		
	作成データ保存	作成データ保存	作成データ保存・スキャナ保存	スキャナ保存	授受データ保存
保存データ形式	テキスト形式	テキスト形式・画像(PDF等)	テキスト形式・画像(PDF等)	画像(PDF等)	授受された形式(原則)

改正電帳法による電子化の検討
【請求書処理の電子化例】

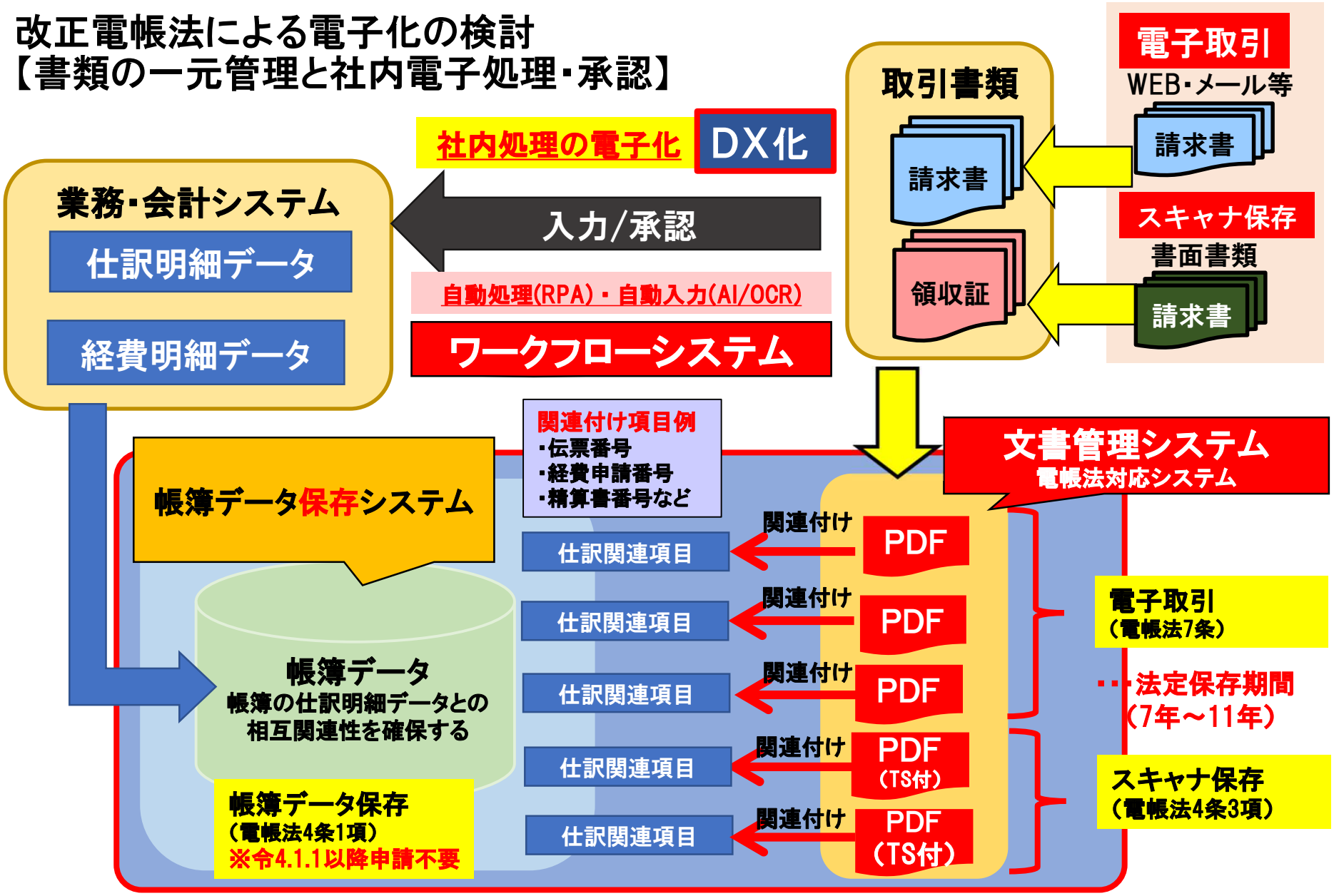
ワークフロー機能
全業務が同一システムで処理可能か？
各プロセスの承認状況が確認可能か？
全証憑データを一元管理できるか？



改正電帳法による電子化の検討
【帳簿データの保存方法の検討】

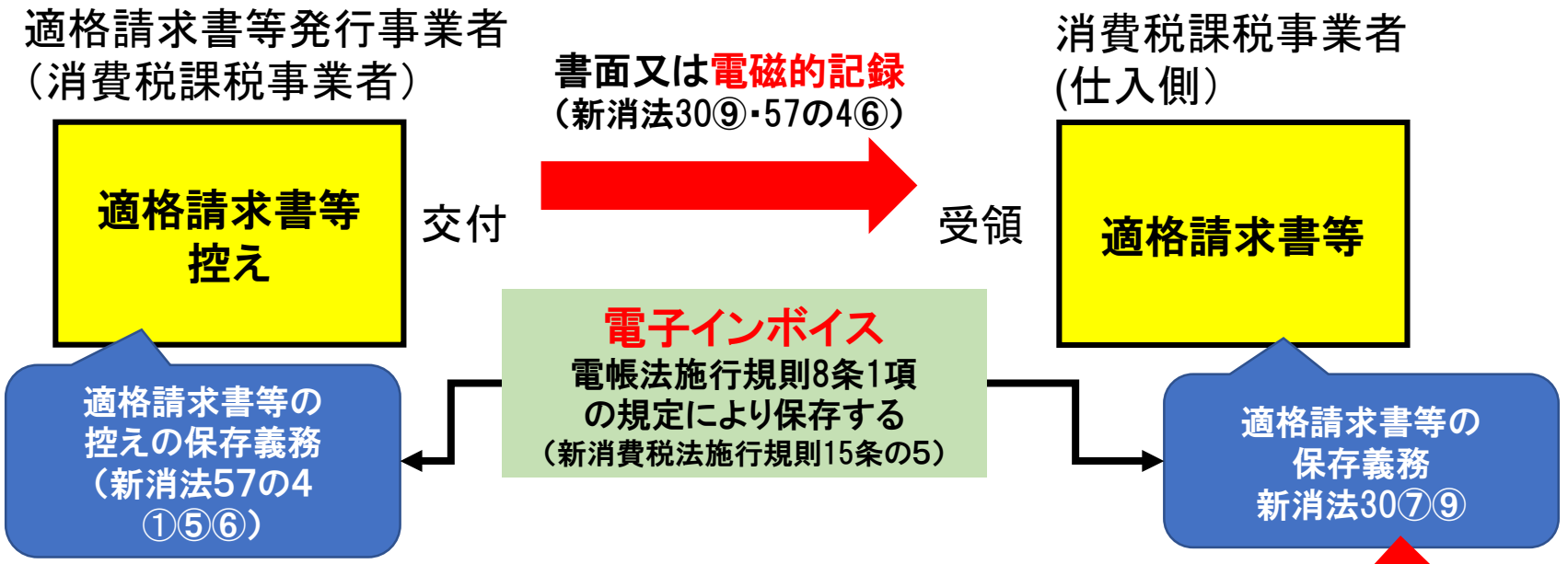


改正電帳法による電子化の検討
【書類の一元管理と社内電子処理・承認】



※JIIMA認証されたシステムを推奨。

インボイス制度の電子化による対応
【適格請求書等の保存義務規定】



適格請求書登録申請手続き
令和3年10月1日～令和5年3月31日
所轄税務署に届け出書の提出が必要

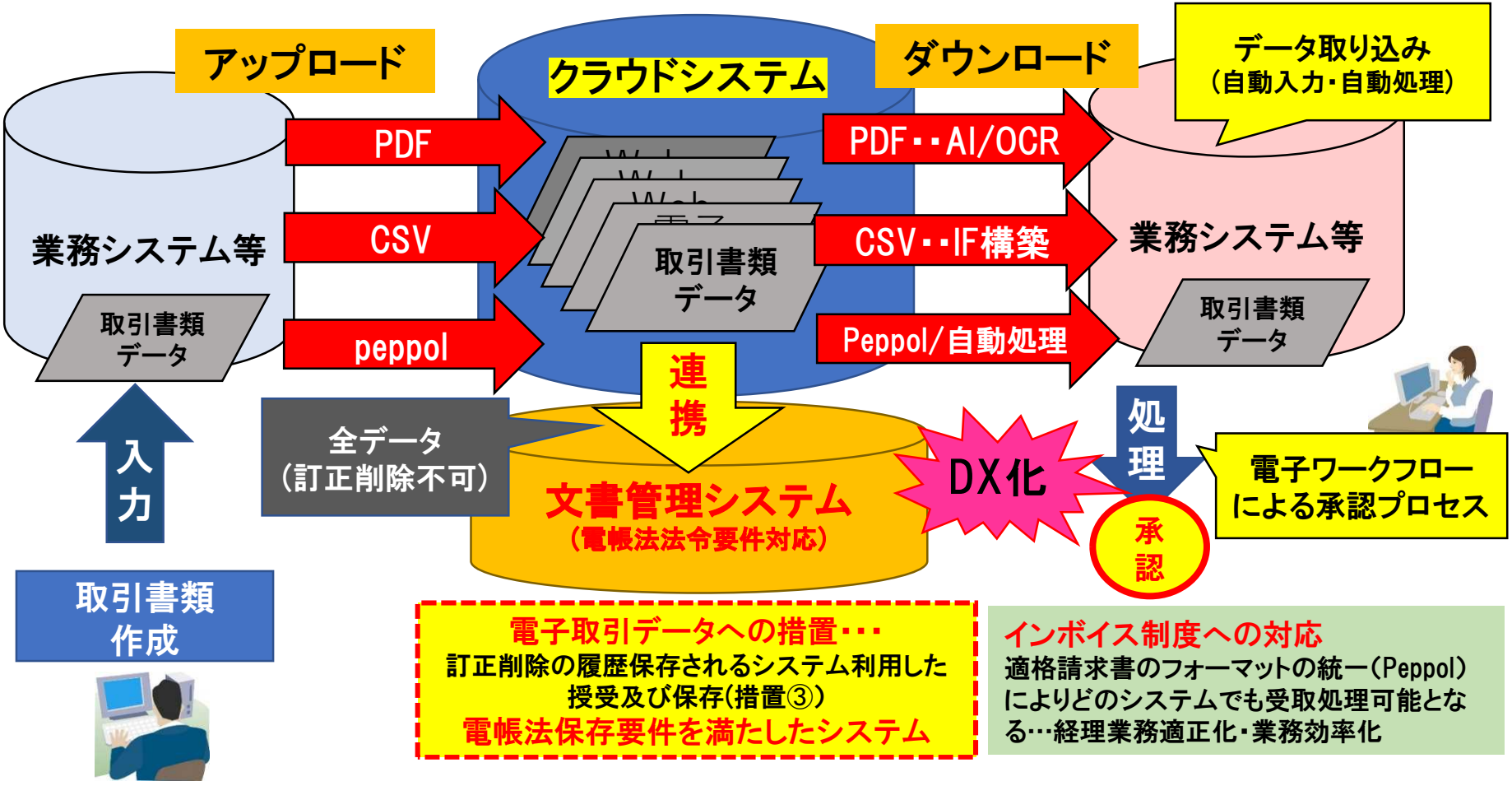
インボイス制度の対応事項
・消費税率ごとの区分経理
・適格請求書発行事業者登録簿の確認業務
・適格請求書の保存

インボイス制度導入で変更されている点

①書面だけでなくデータで発行・受領・保存が可能
②発行者の請求書控の保存が義務付け
③すべての適格請求書の保存が必要
…現在は3万円未満の支払金額の場合の請求書の保存は必須ではない
④電子インボイスは書面保存しても仕入れ税額控除は可能

インボイス制度の電子化による対応
【クラウドを活用した取引書類授受とDXの検討】

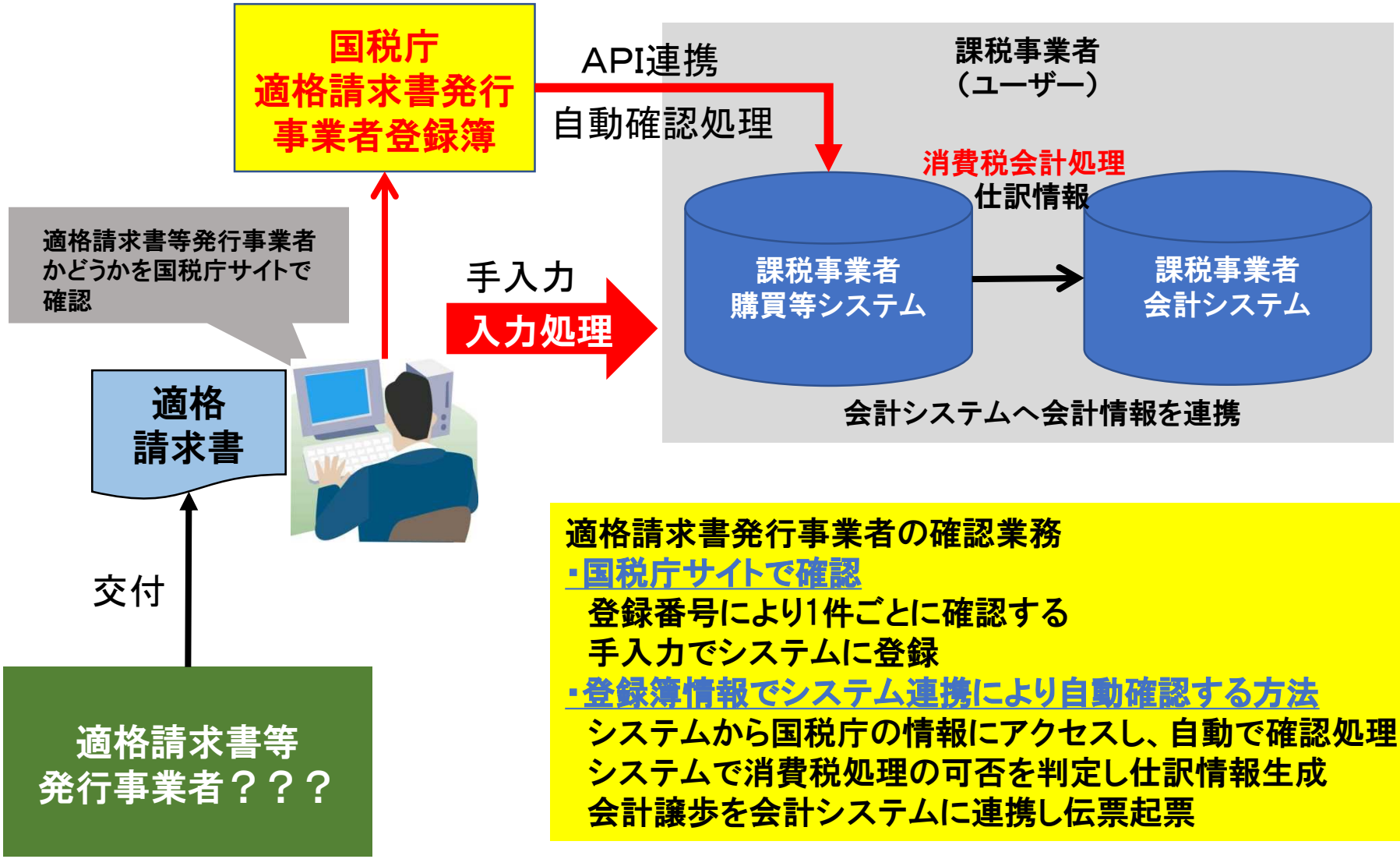
クラウドにより電子取引データの授受及び保存する場合のポイント
- 授受するデータを全て保存でき、電帳法対応ができていること
- 保存期間中クラウドで保存する(クラウドから自社サーバにデータ移管することも可能)
- 取引データの入力や処理において、送受信データを活用できるか



電子取引データへの措置・・・
訂正削除の履歴保存されるシステム利用した授受及び保存(措置③)
電帳法保存要件を満たしたシステム

インボイス制度への対応
適格請求書のフォーマットの統一(Peppol)によりどのシステムでも受取処理可能となる…経理業務適正化・業務効率化

インボイス制度の電子化による対応
【適格請求書発行事業者の確認方法】



適格請求書発行事業者の確認業務

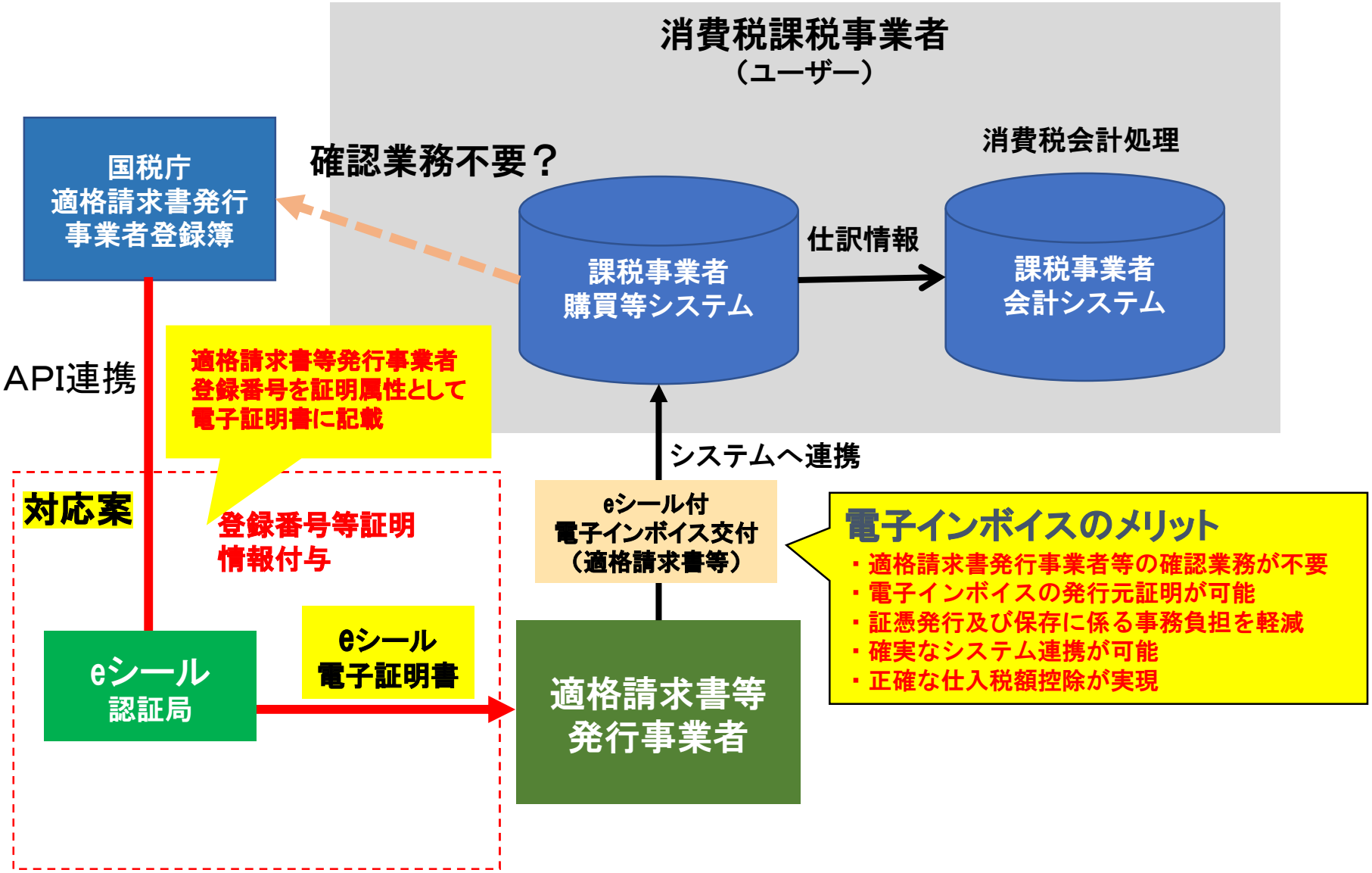
・国税庁サイトで確認

登録番号により1件ごとに確認する
手入力でシステムに登録

・登録簿情報でシステム連携により自動確認する方法

システムから国税庁の情報にアクセスし、自動で確認処理
システムで消費税処理の可否を判定し仕訳情報生成
会計譲歩を会計システムに連携し伝票起票

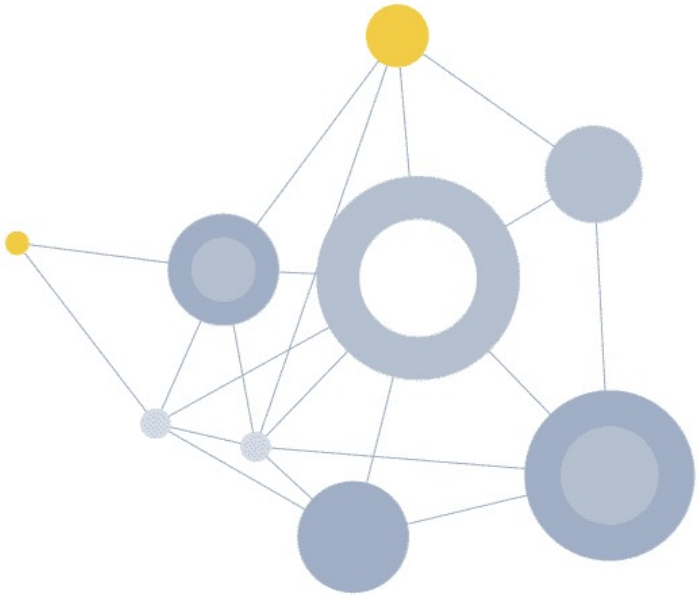
インボイス制度の電子化による対応
【eシール(日本版)の活用】



SKJ総合税理士事務所
所長・税理士　袖山　喜久造
税理士　龍　真一郎　　税理士　坂本　真一郎
千代田区神田須田町1－2－1カルフール神田ビル8階
☎03－3525－4688（代表）
HP：http://tax-wave.com/

資料５

電子証明書ニーズと課題について



18th November 2021

中武　浩史
GLEIF Japan

Agenda

1. 銀行における電子化の現状
2. 海外におけるe-シールの活用事例
3. 普及に向けての課題
4. 今直面する課題：具体的事例

1. 銀行における電子化の現状

- インターネットバンキング（個人・法人）、税公金収納、個人向け新規口座開設、個人向けローン契約等、相応の分野で電子化は進展
- 業務別では、法人融資契約（まだ窓口が主体、提出書類が電子でない）、法人口座開設（実質的支配者の確認等AML/CFT等に課題）といった法人契約に関わる分野の電子化は必ずしも進んでいない
- 手形は電子債券に移行が進む一方、小切手・その他証券（株式配当金領収書等）はまだまだ
  - 電子化で残された法人業務（小切手・領収書等含）エリアはeシール活用の余地大

JBA JAPANESE BANKERS ASSOCIATION 一般社団法人 全国銀行協会

各銀行が提供する個別サービス

ステージ	銀行における取引事例	電子化に向けた課題	目指すべき姿・対応の方向性
大部分の銀行が電子化サービスを提供しており多くの顧客が利用している	・個人インターネットバンキング	・顧客側に使い勝手への不満・懸念がある（対面の方が分かり易い） ・顧客側にセキュリティへの懸念がある	・更なる利便性向上・UI/UXの改善を図る ・全銀協としてセキュリティ対策を横展開
大部分の銀行が電子化サービスを提供しているが、利用する顧客は限定的	・法人インターネットバンキング ・ZEDI ・でんさい ・税公金収納	・顧客側のコストや使い勝手への懸念（特に、取引数が少ないとコストに見合わない）	・顧客への周知により、利用者拡大を図る ・更なる利便性向上を図る ・中小企業に対する国の支援策の活用等も検討し、金融取引の電子化推進を図る
一部の銀行が電子化サービスを提供している	・個人向け新規口座開設 ・個人向けローン契約	・顧客側のオンライン手続（特に本人確認）の使い勝手の悪さへの不満・懸念がある ・銀行側にも、開発コストに見合う利用者拡大への不安がある ・銀行側のセキュリティへの不安がある	・一部の銀行で提供されている先進事例の業界横展開による導入促進を図る ・顧客への周知により、利用者拡大を図る
銀行からの電子化サービスの提供が限定的	・法人との新規取引開始 ・法人代表者変更手続 ・法人融資契約 ・担保契約	・法的証拠能力に懸念がある ・事業者側のIT環境・体制が未整備であるため、銀行側に開発コストに見合う利用者拡大への不安がある ・法令による制約（不動産担保取引等）、がある	・一部の銀行で提供されている先進事例の業界横展開による導入促進を図る ・面前での自署・捺印、書面交付等を原則とする監督指針の柔軟な運用についても協議させていただきたい

JBA JAPANESE BANKERS ASSOCIATION 一般社団法人 全国銀行協会

各銀行が提供する個別サービス（銀行界と関係当事者の皆さまと協働して解決したい課題）

取引内容	現状	電子化に向けた課題	解決に向けた取組み・対応案
・監査法人残高証明書	・監査法人から依頼のある残高証明書は書面で郵送	・電子化のルート構築 ・フォーマットの統一	・日本公認会計士協会と協議のうえ、具体化について検討中
・配当金領収証	・配当金領収証を窓口で受付し、現金を支払う ・銀行間で交換に回している	・振込へのシフトが進まない ・関係者が複数関与しており推進が難しい	・紙の削減、振込での受取シフトついて関係団体（ゆうちょ銀行、信託協会、日証協、全国株懇連合会）と協議中
・定額小為替証書	・定額小為替証書をゆうちょ銀行で購入、銀行間で交換に回している	・行政手続きに必要であり法改正が必要	・キャッシュレス推進協議会におけるロードマップに掲載された ・行政の改革、法改正が必要
・収納企業経由の口座振替の電子化	・収納企業経由の口座振替の電子化	・事業者の協力が必要	・口座振替など収納企業経由で受付する手続の電子化に向けた事業者への協力要請
・マンション管理組合口座の印鑑レス	・印鑑を前提とした法規則となっており、マンション管理組合口座の印鑑レスを推進する際に論点となる	・マンション管理会社の不正防止を主な目的とし、適正化法施行規則では管理組合口座の印鑑管理について明記あり	・マンションの管理の適正化の推進に関する法律施行規則第87条の見直しが必要
・店頭窓口におけるタイムスタンプ導入促進	・国税関係書類のスキャナ保存にあたり、スキャニングや電子取引の改ざん防止のため、認定事業者発行のタイムスタンプ付与が必要	・タイムスタンプはシステムランニングコストが大きく、導入障壁が高い	・電子帳簿保存法の見直しが必要 ・タイムスタンプに代わる安価な方式を選択可とする（例：日本標準時刻と同期する社内タイムサーバの活用など）
・電子帳簿保存の柔軟化	・銀行が保管する国税関係帳簿書類を中心として電子帳票のデジタル化が進まない	・イメージデータ保存方式で保管する電子帳票では、国税関係帳簿書類に係る電子帳簿保存法要件を満たさない	・電子帳簿保存法の見直しが必要 ・国税関係帳簿書類についても「電子帳票システム」によるイメージデータ保存で可とする

出典；金融庁　金融業界における書面・押印・対面手続の見直しに向けた検討会　令和２年８月19日　第5回　全国銀行協会発表資料より

2. 海外におけるe-シールの活用事例

1) 欧州　eIDAS指令の元での（スペイン・イタリア）等の事例

- 法人税申告でのeシール利用義務
- UBLフォーマットを用いた公的セクターへのインボイスへのeシール付与義務
- その他電子書類手続き
  - 雇用契約、サービス契約、SLA、発注書等契約の発行と受諾

2) 香港の事例

- USBないしソフトウエア形式で組織に対しての電子証明書発行（eシール+電子署名的位置？）
- 主に貿易取引の通関申告等での利用を目的に20年以上前から運用

  - 香港では手数料の観点で主に利用が多い電子小切手発行の裏付けとして活用（携帯で電子小切手発行が可能）

  - 日本の手形小切手電子化検討の中で、小切手は８割を占める。オンラインバンキングへの移行が主軸であるが、より簡便で安価な香港の手法は普及に向けた良い参考になる

3. 普及に向けての課題

- 「文書（契約書）の成立の真正」の立証負担 、法人取引における正当な権限者による契約手続の確保が、銀行業務の対顧客手続き電子化にあたり最初にあげられる課題
- その他コスト面で、個別企業での維持にはコスト高となるシステムの投資負担、利用者サイドでの利用料・システム投資負担も課題
- 単純な周知不足の解決や、特に中小企業を中心とした手厚い導入・運用サポートも必要
  - 安価で導入しやすい形での実現手段の工夫、税制等インセンティブと十分なサポート体制の構築は必須

No.	項目	詳細
1	法的有効性	成立の真正の立証方法が煩雑ないし、判例も少なく、 立証に成功するかどうかの不安材料が企業サイドの懸念材料 また法人取引における正当な権限者による契約手続の確保
2	コスト負担	企業サイドでは個別企業での維持にはコスト高になるシステム投資負担とそのROI、利用者サイドでは利用料や利用にあたってのシステム投資負担が課題（非課税枠や補助金等工夫）
3	ITリテラシー	特に中小企業において使い方がわからず抵抗感
4	セキュリティに対する不安	安全性について、わかりやすい形で示す必要性
5	そもそも知らない	効果も含めた十分な宣伝活動
6	現状からの移行負担	既存サービス業者からのスムーズな移行への考慮

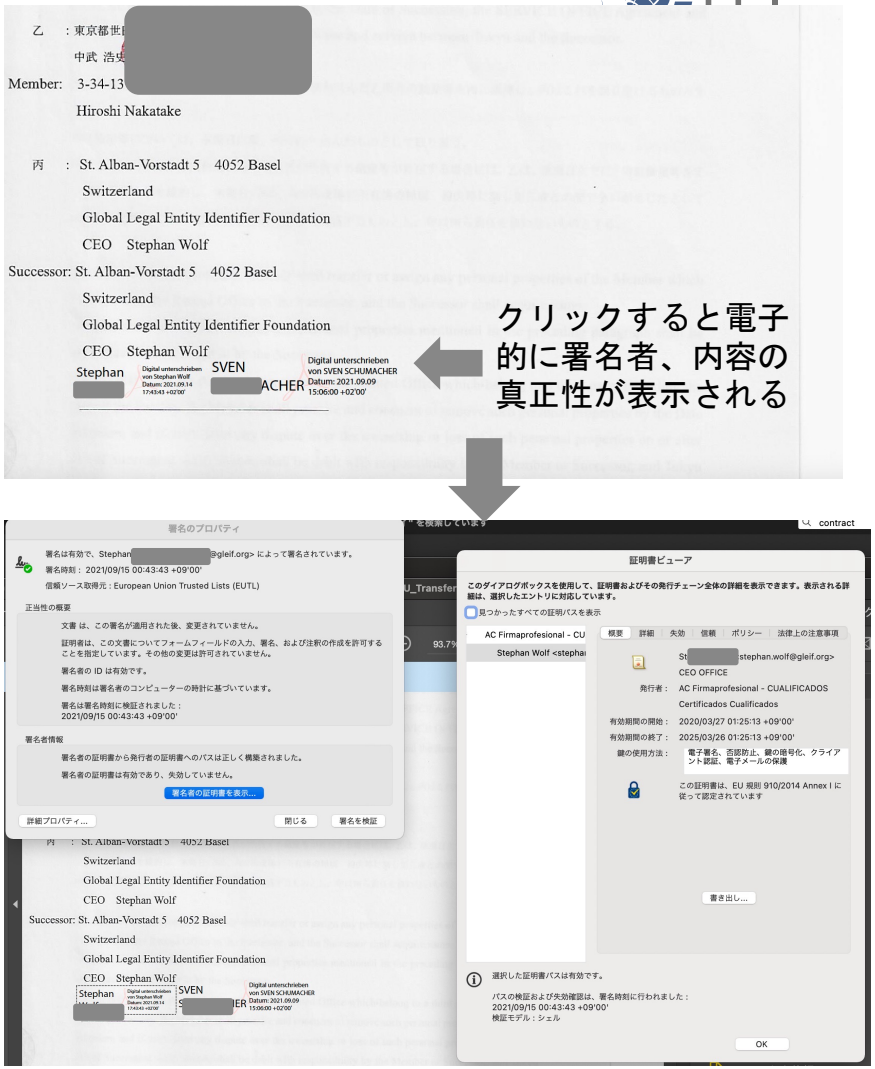
4. 今直面する課題；具体的事例

日本ーEU間での契約締結

1. 日本の不動産契約に欧州企業が調印
2. 欧州ではeIDAS配下、電子署名、eSeal付与が標準であり電子的に署名
3. 日本企業側では直筆でのサイン、署名の登記証明を要求
4. 更に欧州企業が何者か、登記事項含めた情報も要求
5. 欧州ではデジタル上で確認されるものが全てであり、法的にも有効

- **<u>eシールでの電子的有効性が担保され、LEIで企業情報にもアクセスし、信用の補完が必要な典型的事例</u>**

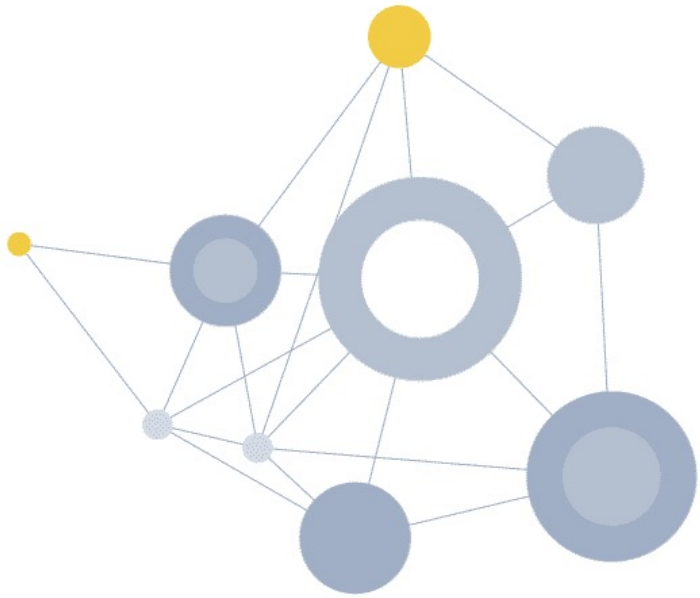
実際の契約書署名欄



Limitations

- This presentation contains confidential and proprietary information and/or trade secrets of the Global Legal Entity Identifier Foundation (GLEIF) and/or its affiliates, and is not to be published, reproduced, copied, or disclosed without the express written consent of Global Legal Entity Identifier Foundation.

- Global Legal Entity Identifier Foundation, the Global Legal Entity Identifier Foundation logo are service marks of Global Legal Entity Identifier Foundation.



資料６

三井住友銀行で展開中の融資電子契約サービスについて

2021年12月13日

一般社団法人全国銀行協会
（株式会社三井住友銀行事務統括部上席推進役）
楠　俊樹

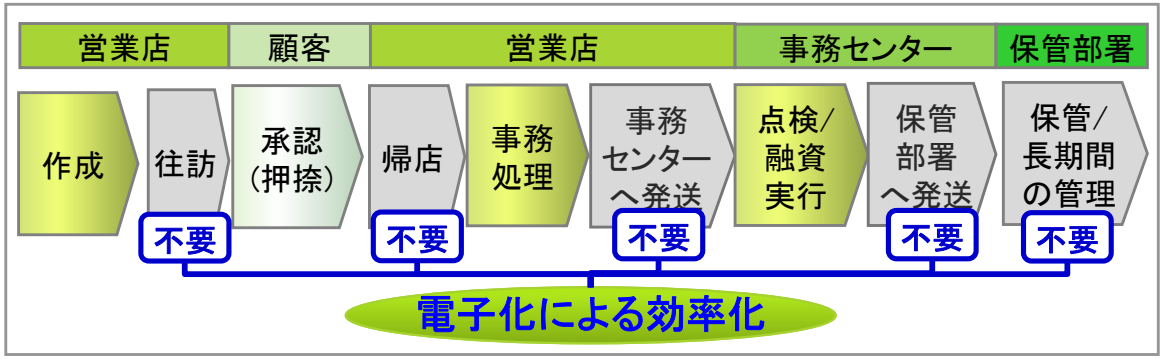
SMBC
三井住友銀行
SUMITOMO MITSUI BANKING CORPORATION

融資電子契約サービスについて

SMBC 三井住友銀行

- **電子署名法準拠の当事者署名型電子署名**を活用し、**融資の契約プロセスを電子化**
- お客さまは**銀行への往訪や書類への記入・押捺なく契約締結**が可能

融資業務フロー

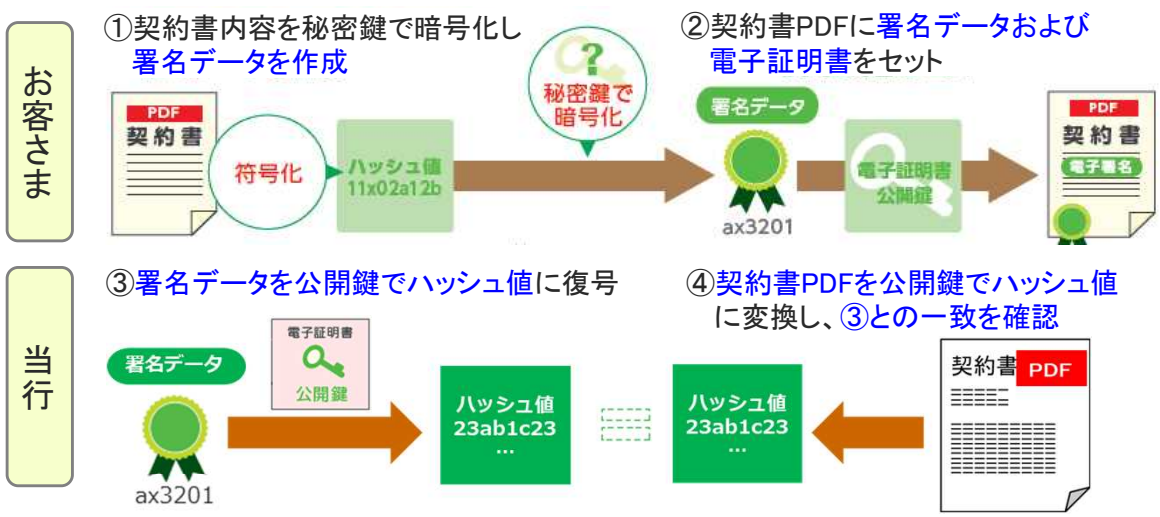


効果

お客さま
- 銀行への往訪が不要
- 契約書への記入・印鑑押捺が不要
- 融資を受けるまでの期間短縮

当行
- 契約書の授受レスに伴い、顧客からの相談や提案に割ける時間が増加
- 契約書の点検効率化や保管レス

電子署名スキーム

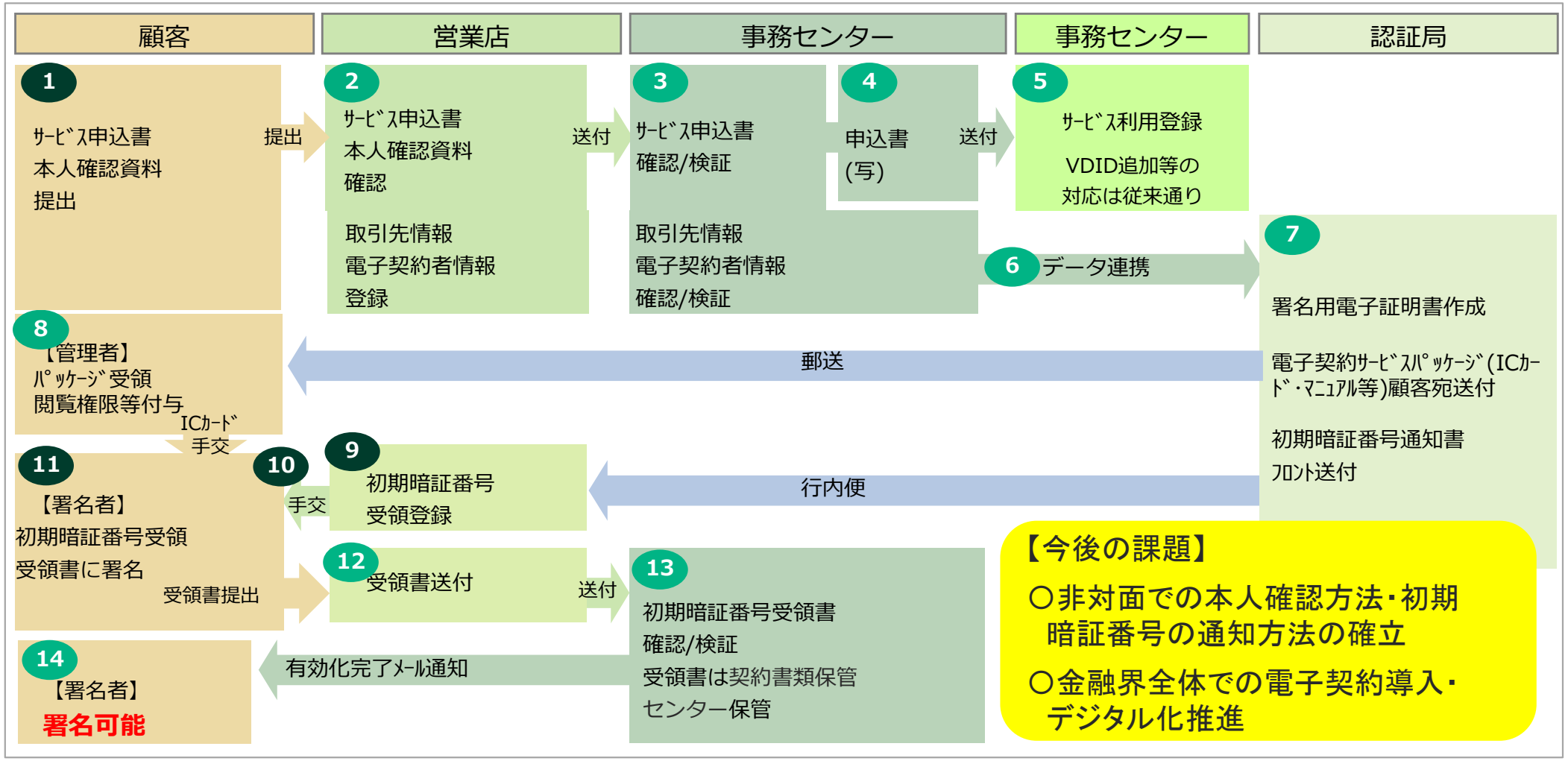


【図表】取引実績

電子契約サービス申込と電子証明書交付フロー

SMBC 三井住友銀行

- 課　題：電子署名法は自然人が対象。一方、証書貸付などの融資取引の契約者は法人。
- 解決策：**法人の融資契約権限者として電子契約を行う個人（電子契約者）を特定**することで、法人取引に適用（融資契約権限者を申込書にて明確化）⇒下図 1
- 解決策：IDを有効化するための「初期暗証番号通知書」を**電子契約者に手交**⇒下図 9 10 11



資料７

第２回 トラストを確保したDX推進サブワーキンググループ （2021年12月13日 Mon.）

電子印鑑の歴史と
電子契約におけるその役割について

２０２１年１２月１３日

シヤチハタ株式会社

システム法人営業部 部長　小倉 隆幸

Shachihata

電子印鑑、開発の理由

電子印鑑、開発の理由

社内に息づく、“自己否定”の精神
～スタンプ台から浸透印へ、そしてデジタルスタンプへ～

- **１９９５年、創業以来初 のソフトウェアをリリース**
- **「PCで作成するのに、承認印を捺すためだけに印刷する」**
  こんな無駄を省くため、開発を手がけた

電子印鑑システム「パソコン決裁」

電子印鑑、開発の理由

社内に息づく、“自己否定”の精神
～スタンプ台から浸透印へ、そしてデジタルスタンプへ～

- **１９９５年、創業以来初 のソフトウェアをリリース**
- 「PCで作成するのに、承認印を捺すためだけに印刷する」
  こんな無駄を省くため、開発を手がけた

→ **いち早く対応、ノウハウを蓄積**

電子印鑑システム「パソコン決裁」

時代背景と法整備の推進

進む法整備と電子印鑑の歴史

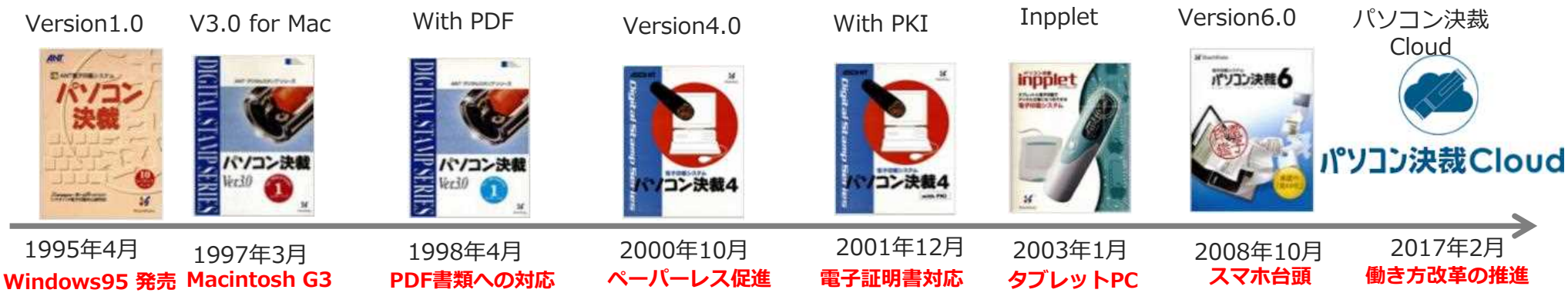
■**1998年7月施行：電子帳簿保存法**

■**2001年4月施行：電子署名法**

■2001年4月施行：IT書面一括法

■2005年4月施行：e文書法

➢ 共に進化し続けて25年



進む環境変化と電子印鑑の歴史

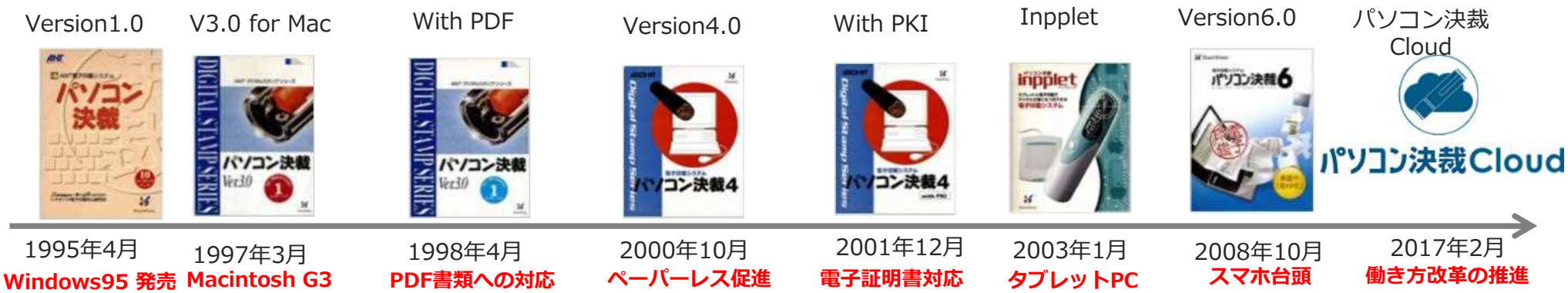
■2003年：家庭向け光回線が登場

■2008年：iPhoneが日本で発売を開始

■**2017年：働き方改革の推進**

■**2020年：リモートワーク普及、クラウドが定着**

- 共に進化し続けて25年



進む環境変化と電子印鑑の歴史

■2003年：家庭向け光回線が登場

■2008年：iPhoneが日本で発売を開始

■2017年：働き方改革の推進

■2020年：リモートワーク普及、クラウドが定着

→ 法整備だけでは進まず、
せざるを得ない状況下で動く

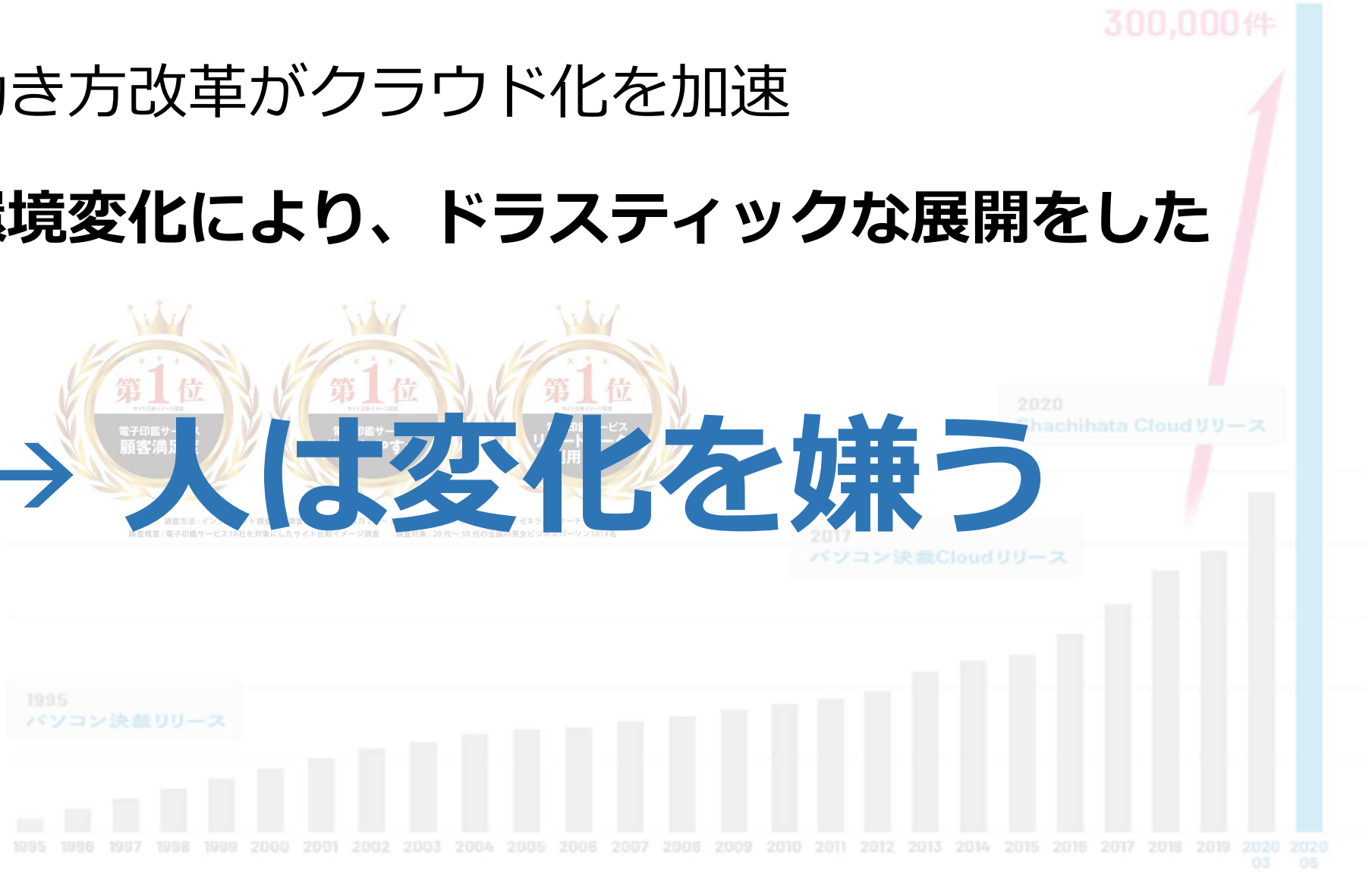
在宅勤務推進がリモートワークに大きく影響

- 電子印鑑の普及は法整備の影響が少なかった
- 働き方改革がクラウド化を加速
- **環境変化により、ドラスティックな展開をした**

調査方法：インターネット調査　調査期間：2021年3月2日～3日　アンケートモニター提供元：ゼネラルリサーチ
調査概要：電子印鑑サービス10社を対象にしたサイト比較イメージ調査　調査対象：20代～50代の全国の男女ビジネスパーソン1014名

在宅勤務推進がリモートワークに大きく影響

- 電子印鑑の普及は法整備の影響が少なかった
- 働き方改革がクラウド化を加速
- **環境変化により、ドラスティックな展開をした**



→人は変化を嫌う

印鑑の役割について

法的効力は「実印」と同等の「認印」

本人性と完全性、それぞれの証拠能力について

本人性

実 印 → 役所に対する信頼

■ **役所が本人であることを証明**してくれる

認 印 → なつ印に対する知識

■ **たぶん本人であるだろう**という判断

完全性

実印・認印

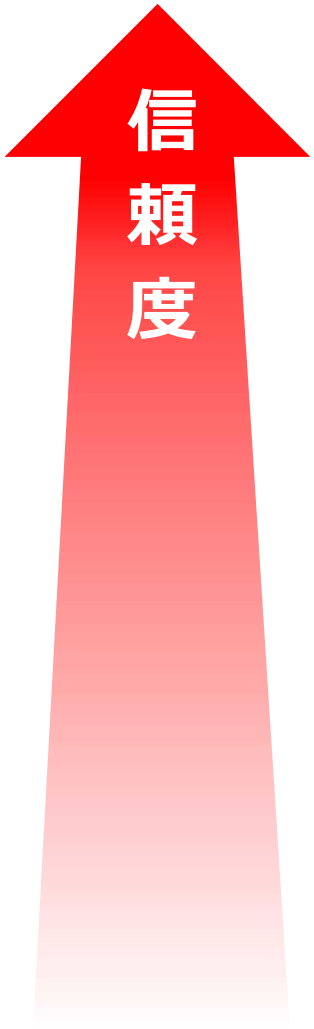
■ **それぞれ、文書の偽造や改ざんはないと判断**

- **民事訴訟法第228条**
  本人等の署名・押印がある場合、真正に成立したものと推定
- **最高裁S39.5.12判決**
  本人等の印章により押印された事実が確定された場合、反証がない限り、本人の意思に基づいて成立したものと推定

→ **「二段の推定」という通説**

法的効力について

信頼された機関により、本人性の信頼があがる「実印」



実 印

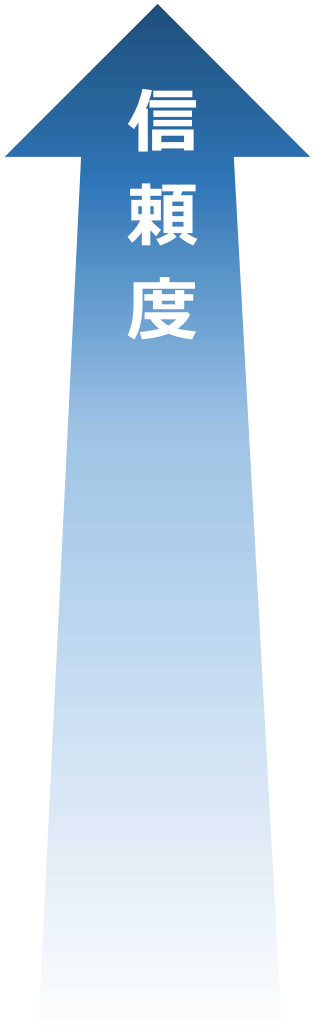
- 役所等に届けている印章を指す
- 印影が印鑑証明と同じなら本人の意思であると推定
- 裁判になったときの証拠能力が高い

認 印

- どこにも届けていない印章を指す
- 法的効力自体は実印と同等
- 裁判になったときの証拠能力は実印より低い

署名、捺印、それぞれの信頼性について

書類の完全性について、実印も認印も問わない



- 「署名」および「捺印」してある文書
- 「記名」および「捺印」してある文書
- 「捺印」してある文書
- 「署名」してある文書

民法での境界線

- 「記名」してある文書

※署名とは自筆により、記名とはパソコン等により名前を書くことを指す

印鑑の役割って？

「印鑑」が果たす役割

＝本人の「**意思**」と、書類の「**完全性**」とを

視覚的に確認できる

印鑑の役割って？

「印鑑」が果たす役割

＝本人の「**意思**」と、書類の「**完全性**」とを

視覚的に確認できる

一般に「決裁＝押印」の概念が定着

参考）未来を担う子供達に影響！？　“仮面ライダーリバイス“

“悪魔と契約する仮面ライダー”

仮面ライダーリバイスでは、悪魔との契約に「ハンコ」が使われており、
ハンコが「意志を決定するもの」であることが、広く視聴者に布教されている

出典：石森プロ・テレビ朝日

電子契約における電子印鑑

電子印鑑は法的効力がある？

それぞれの証拠能力について

電子印鑑の効力は？

＝認印と同様の効力がある

本人性

認 印

- たぶん本人であるだろうという判断 → なつ印に対する知識

「たぶんその人が捺したのだろうの判断」に基づく

実 印

- 本人であることを確認
- 役所が本人であることを証明してくれる → 役所に対する信頼

裁判になったときの証拠能力は低い

完全性

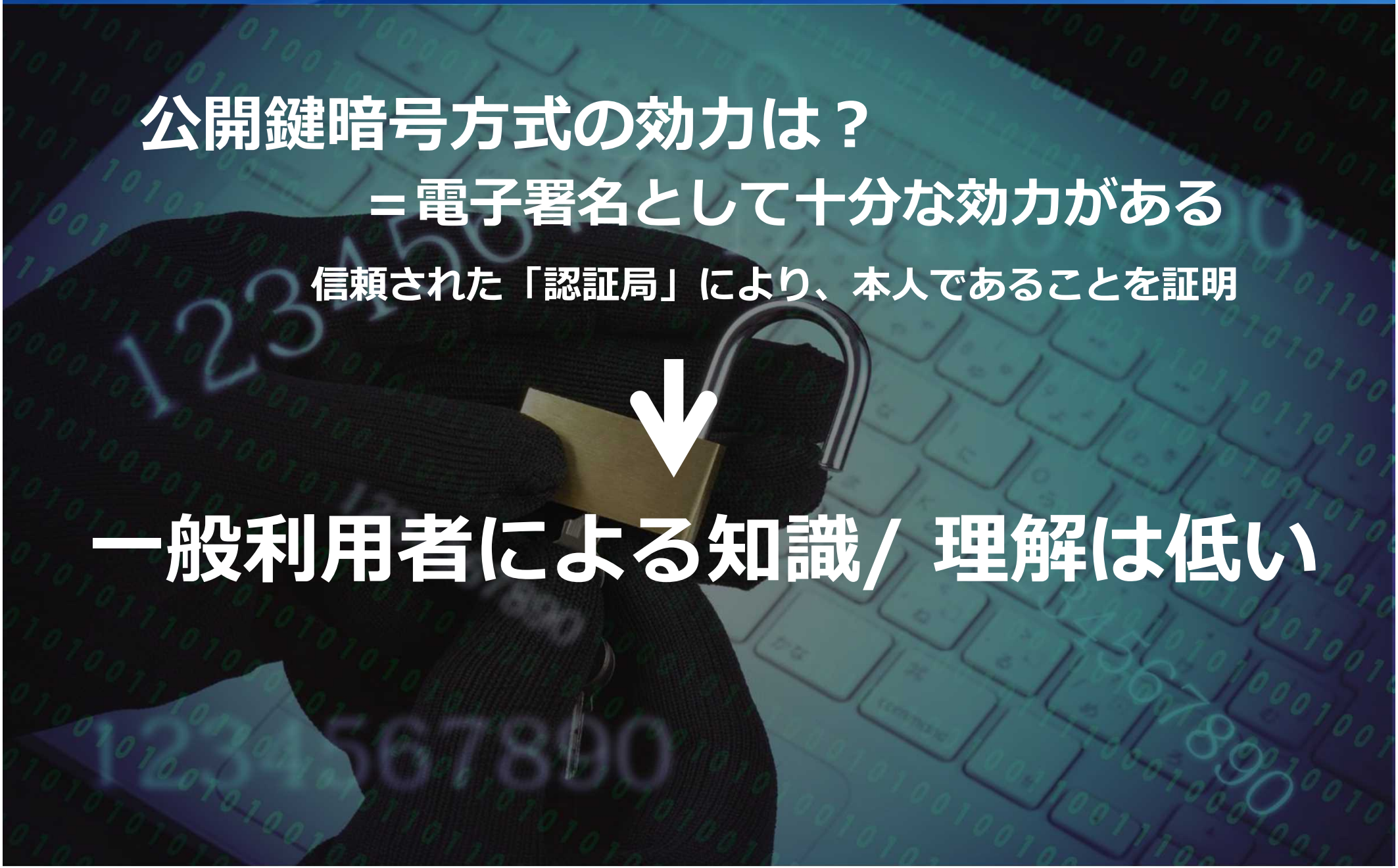
認印・実印

- 文書の偽造や改ざんはないと判断

※ **「二段の推定」という通説**

- **最高裁S39.5.12判決**
  本人等の印章により事実が確定された場合、反証がない限り、本人の意思に基づいて成立したものと推定
- **民事訴訟法第228条**
  本人等の署名・押印がある場合、真正に成立したものと推定

一方、公開鍵暗号方式だけによる電子契約では、



公開鍵暗号方式の効力は？

＝電子署名として十分な効力がある

信頼された「認証局」により、本人であることを証明

↓

一般利用者による知識/ 理解は低い

利用者にとって使いやすいツールとは？

使い慣れたツールで
署名できることが一番嬉しい

“技術は文化を超えられない” by Tom Gonser

貴方なら、どちらの文書を受け取りたいでしょう?

■署名済み文書（捺印済み）

注　文　請　書

平成　2009 年　　1 月　　15

社 様

月28日

鯱旗工務店
〒 103-0001
東京都中央区日本橋
TEL　03-3663-9658
FAX　03-3666-6235

鈴木太郎

■署名済み文書

注　文　請　書

平成　2009 年　　1 月　　15

電子印鑑株式会社 様

納　　期 2009年2月28日
納 品 場 所
支 払 条 件
弊 社 担 当 鈴木

鯱旗工務店
〒 103-0001
東京都中央区日本橋小伝馬町１－５
TEL　03-3663-9658
FAX　03-3666-6235

“NFT電子印鑑”という提案

- **「実印」に寄せる人々の信頼性**

  市区町村に登録された印鑑であるという、高い信頼度
  長年に渡るユーザ体験が作り上げた、高い信頼性

- **現状における電子署名での課題**

  書類だけでは署名付与の判断がつけにくい
  利用者にとって「署名した」という実感が湧かない

- **「実印」に最も近い、NFT印鑑**

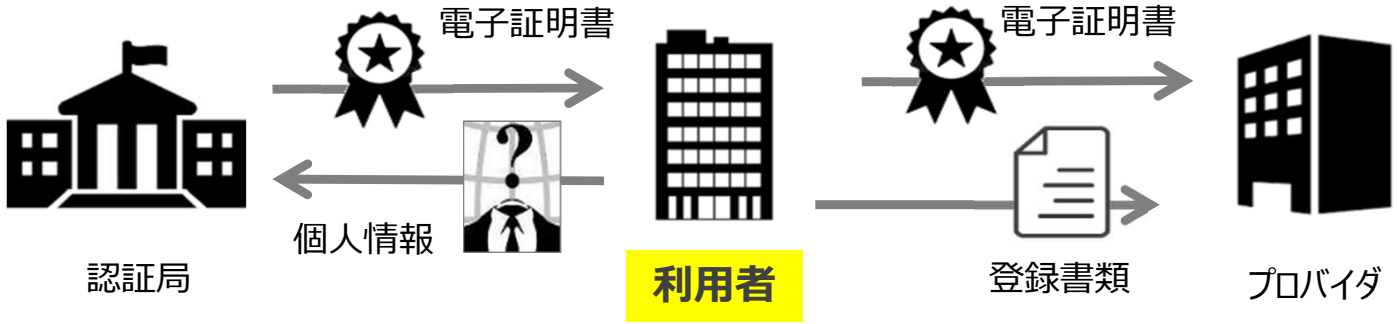
  NFTを活用した「唯一無二」の印鑑であること
  個人情報は印鑑と結び付けられている
  生体認証を使った厳格な本人認証

Shachihata Cloud

立会人型署名を補完できる、“NFT印鑑”

当事者型署名

- 本人の電子証明書を使っており、本人認証に優れている
- 一方、証明書取得の手間、管理コストが高く、広く普及させづらい



立会人型署名 ＋ NFT印鑑

- 立会人型署名に個人情報を持つNFT印鑑を追加
- 取得の手間、管理コストが低く、広く普及させやすい

最終章

Shachihata

資料８

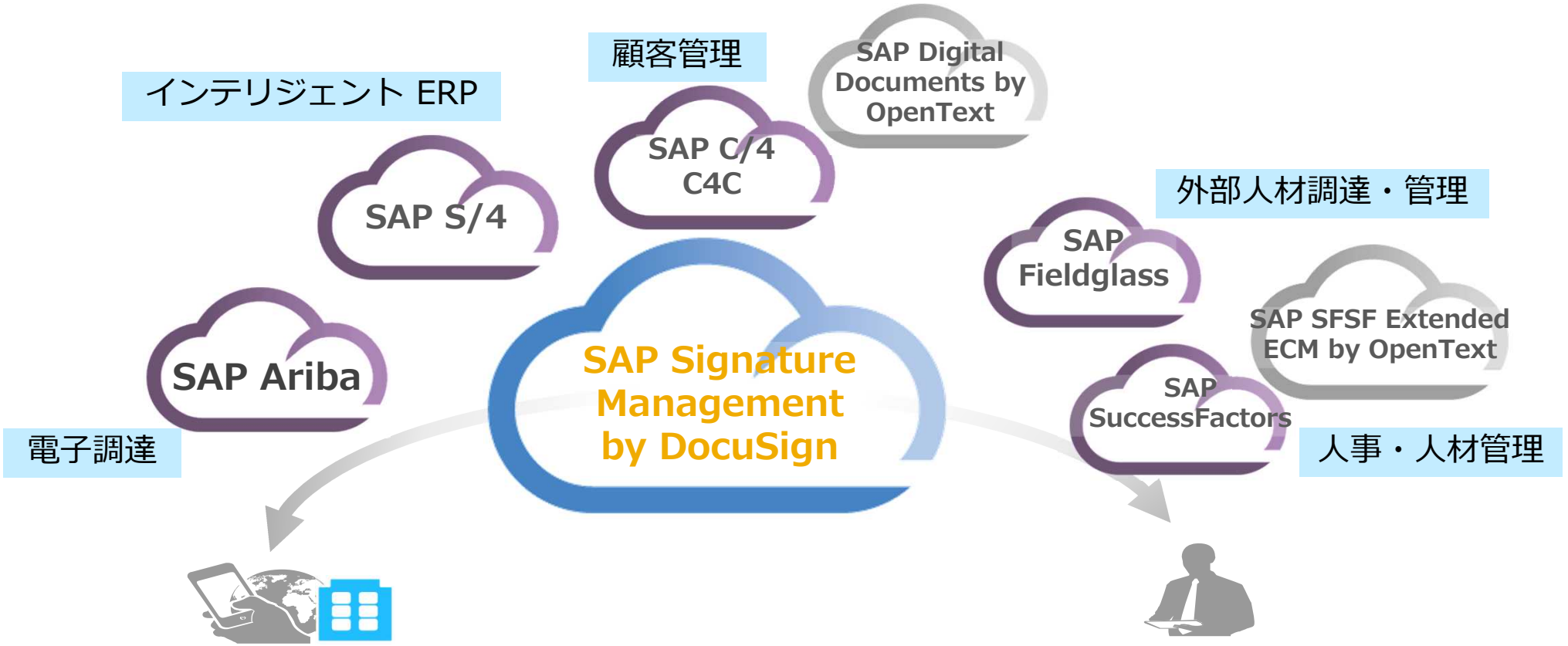
SAPが認識するトラストサービスの現状と課題

2021年12月27日

SAPジャパン株式会社
バイスプレジデント 政府渉外
中須 祐二

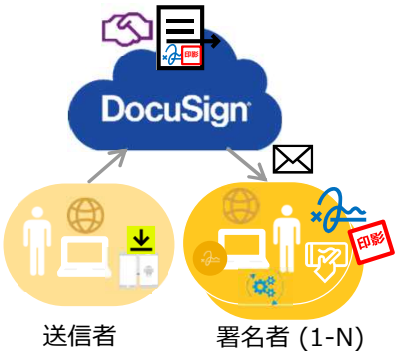
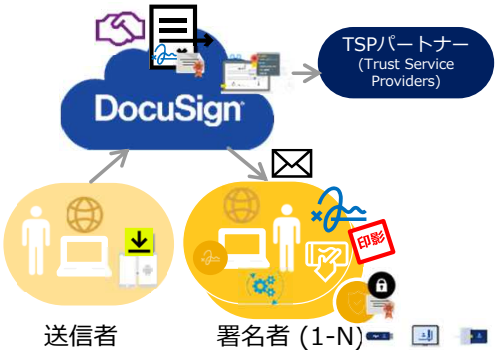
THE BEST RUN SAP

SAPは幅広い業務領域において電子署名ソリューションを提供（DocuSign, OpenTextとの連携）



SAPが対応する署名方式（DocuSignとの連携）

合意文書の内容・種別に応じて選択できる複数の署名方式オプション

署名方式	DocuSign eSignature	DocuSign EU Advanced/ DS Express	署名書保有の証明書/ TSPパートナー連携
システム構成 イメージ			
署名型式	立会人型 電子署名	立会人型 デジタル署名 (電子証明書利用)	当事者型 デジタル署名 (電子証明書利用)
当事者の意思確認	ユーザー認証で当事者の意思を反映	ユーザー認証で当事者の意思を反映	付された電子署名が当事者の意思を反映
当事者本人の確認	当事者本人の確認は送信者が実施	当事者本人の確認は送信者が実施	当事者本人の確認は第三者である 認証局(登録局)が実施
当事者の意思と 非改ざん性	電子署名が付された合意文書と 証跡を記録した完了証明書で 当事者の意思、ドキュサインの電子署名で 非改ざん性を保証	デジタル署名が付された合意文書と 証跡を記録した完了証明書で 当事者の意思、ドキュサインの電子署名で 非改ざん性を保証	デジタル署名が付された合意文書単体で、 当事者の意思と非改ざん性を保証 (完了証明書は補足資料)

EUの現行ルール ー eIDAS規則（2014年）

- 加盟国が、公共サービスへの安全なアクセスを可能にするデジタルIDシステムを市民や企業に提供する義務や、EUの国境を越えた利用を確保する義務は含まれていない。このため、国によって適用にばらつきがある。
- 欧州委員会が相互運用性のためのオープンソースフレームワークを提供。
- デジタルID:

  9つの指針：ユーザーの選択、プライバシー、相互運用性とセキュリティ、信頼性、利便性、ユーザーの同意と管理の均整、相手の認識、グローバルな拡張性
- 3種類の電子署名を定義: 標準電子署名 (Standard)、高度電子署名 (Advanced)、適格電子署名(Qualified)

  * 取引の種類毎に必要な署名の種類は、各EU加盟国の国内法で定めらる

第一次調査結果

トラストサービス：利用可能性と利用率、各国のセキュリティレベルの同等性、監督活動の調和

eID：実装の弱さ、市民への普及率の低さ、相互運用性の難しさ、ユーザーの利便性の低さ、通知プロセスの複雑さ、公共サービスに限定

SAPが認識するEUでの改善点（eIDAS)

- 各国間のハーモナイゼーション:
  - 「個人情報」が各法域で事実上同じ意味で理解されることを保証
  - 各国の技術基準の不一致を避ける
  - 相互運用性とセキュリティレベル
- すべての国民や企業が利用可能なデジタルIDソリューションの使用を希望または選択するとは限らず、また国民にオプトアウトする法的権利が与えられているため、普及に懸念（不信の文化）
- データ保護 ー 重要課題
  - データ保護とプロファイリングの経済的・社会的影響
  - 法律の執行度と罰則による十分な抑止力の有無
  - 産業界にとって負担となりうる要件:
    - 技術的実現と標準化
    - 情報が収集された後、その使用を管理するための効果的な技術的メカニズム
    - 中心となるIDシステムのユーザー・エクスペリエンス

Thank you.

THE BEST RUN SAP

資料９

GlobalSignにおける電子証明書の利用事例

GMOグローバルサイン株式会社
伊藤健太郎

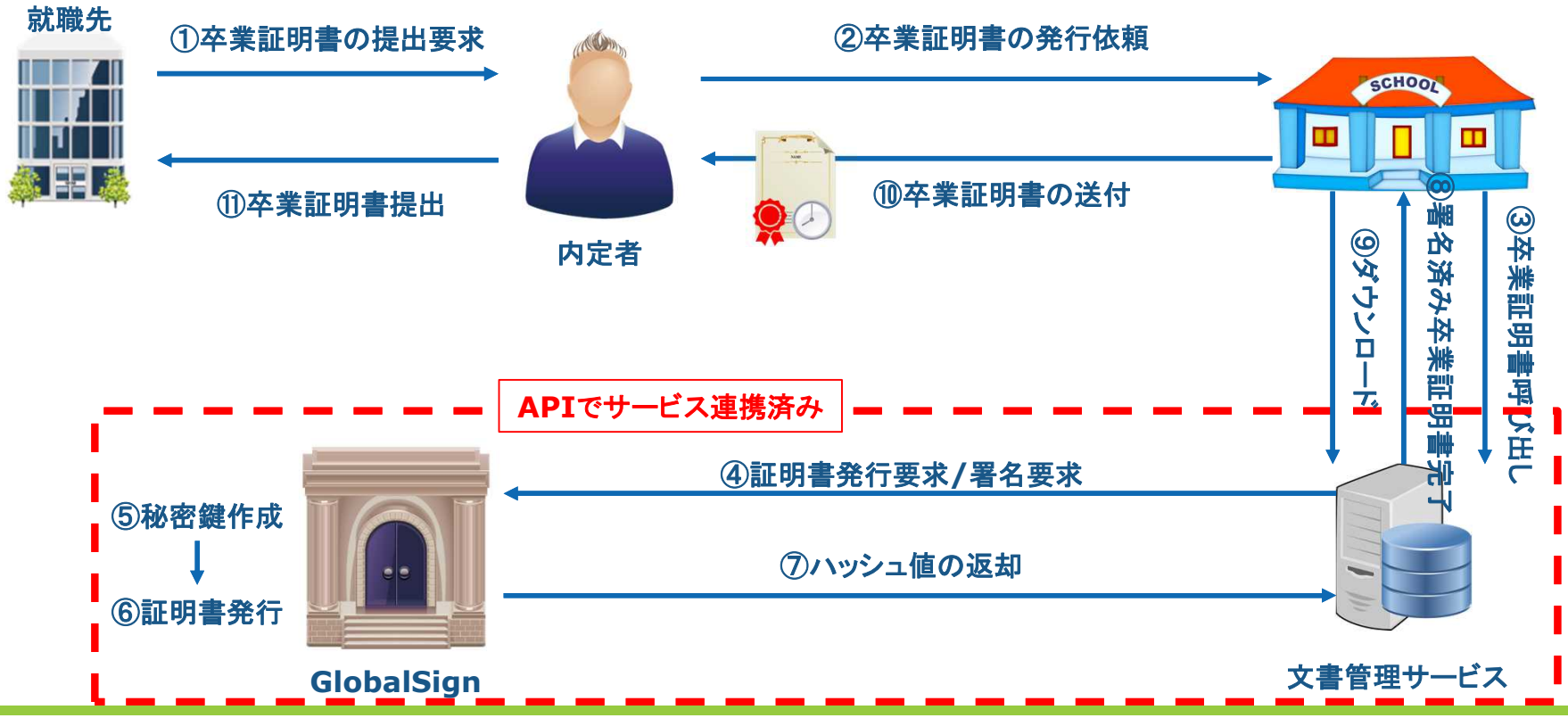
February 8, 2022

GlobalSign by GMO

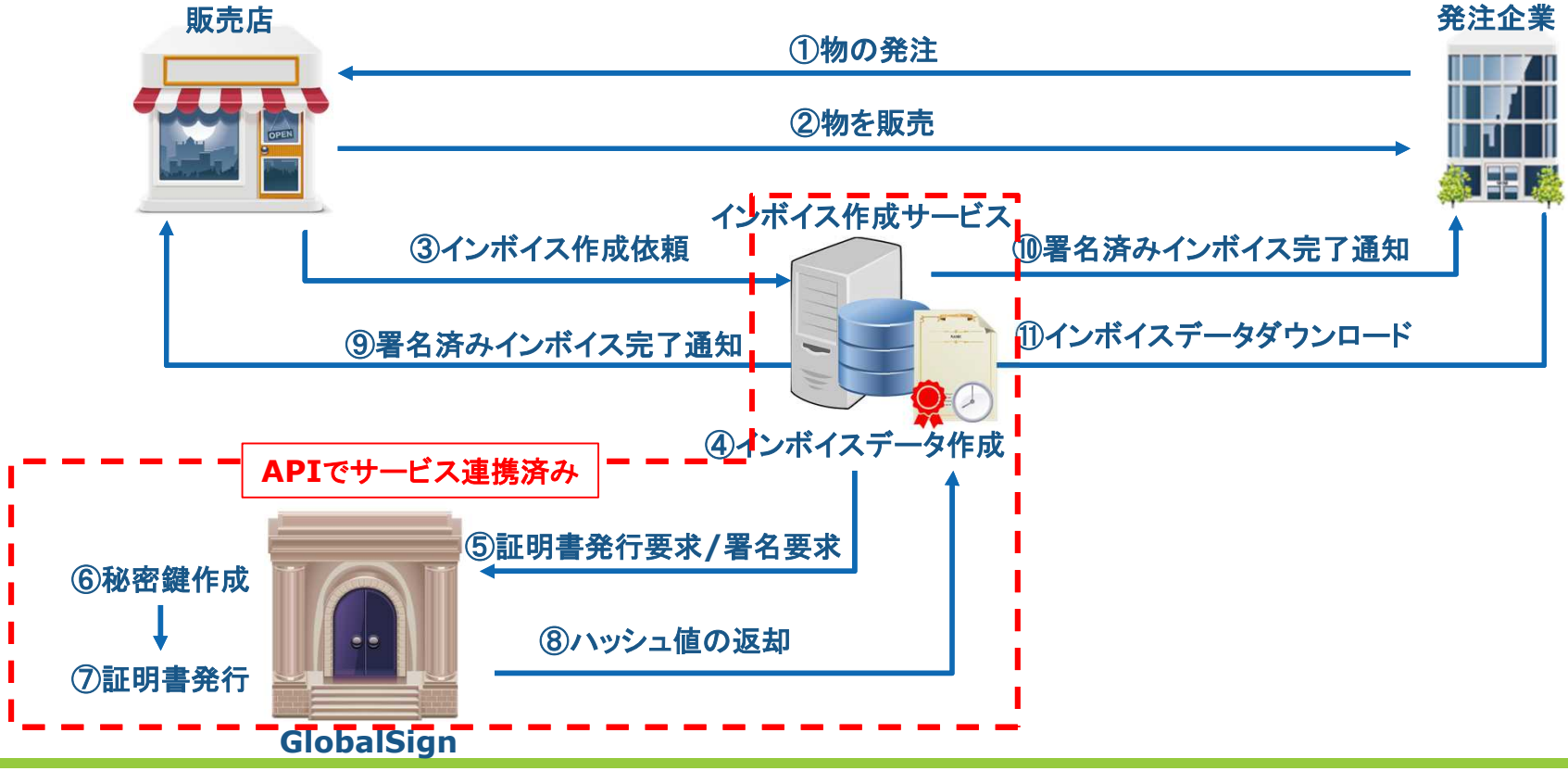
GlobalSignで発行している電子証明書の利用シーンについて、以下4点のご紹介を差し上げます。

①卒業証明書への署名
②帳票関係への署名
③車両登録書類への署名
④PCR検査結果報告書への署名

①卒業証明書への署名

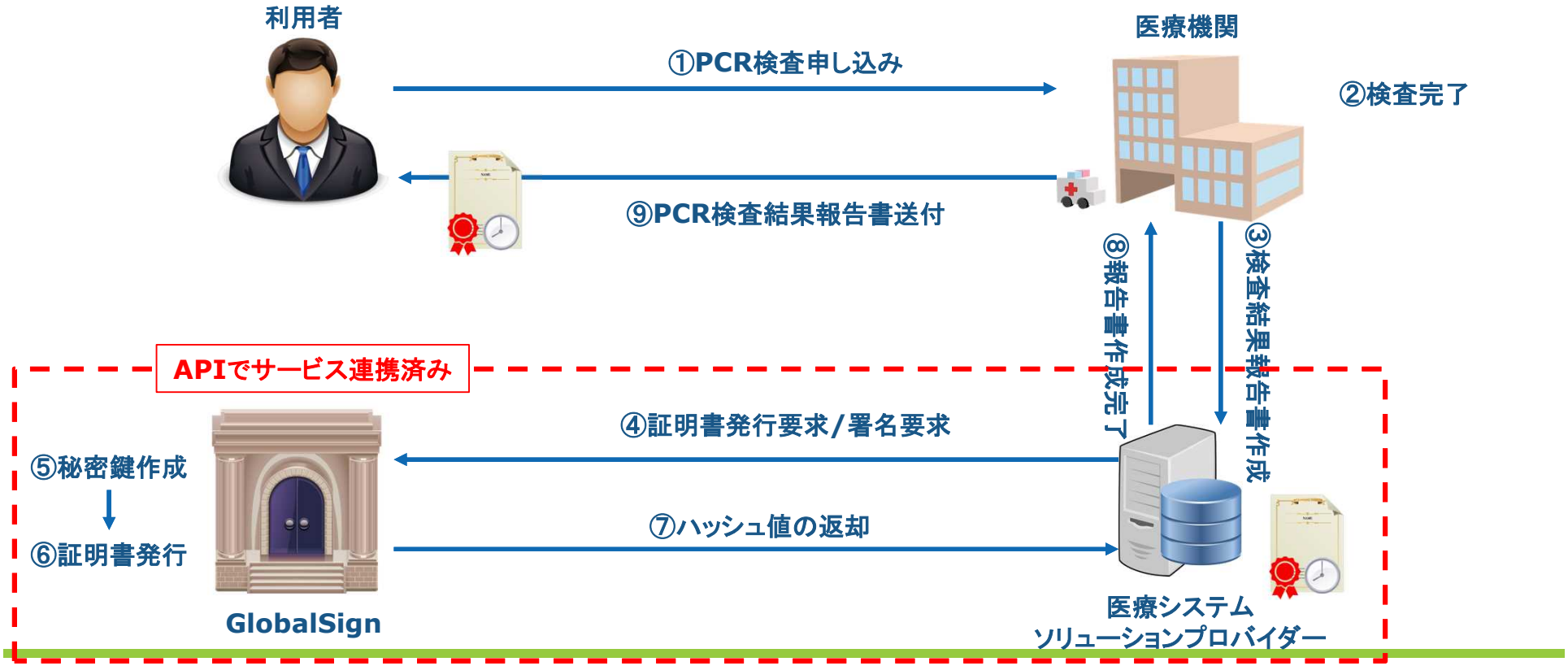


②帳票関係への署名



③車両登録書類への署名

④PCR検査結果報告書への署名



GlobalSignのプロダクトにおける電子証明書発行数及び署名回数

GlobalSign by GMO

電子証明書発行数及び署名回数

Confidential

公開資料なし

最後に

- 今回ご紹介をさせていただきました事例で利用がされている証明書は、EUのQualifaied Certificates（QC）ではありません。
  あくまでも弊社のQC以外のプロダクトから発行した「組織用証明書」を利用した署名（eシール）の事例となります。
- その他に証明書を利用した署名事例では、「納税申告」や「FDA申請」などの活用もあります。

ご清聴ありがとうございました

GMOグローバルサイン株式会社

〒150-0043

東京都渋谷区道玄坂1-2-3　渋谷フクラス

https://jp.globalsign.com/

資料１０

トラストを確保したDX推進サブワーキンググループ
第3回　提出資料

「デジタル原則」を支える クラウド型電子署名サービス 普及促進の必要性

2021年12月27日

クラウド型電子署名サービス協議会
代表理事　橘 大地

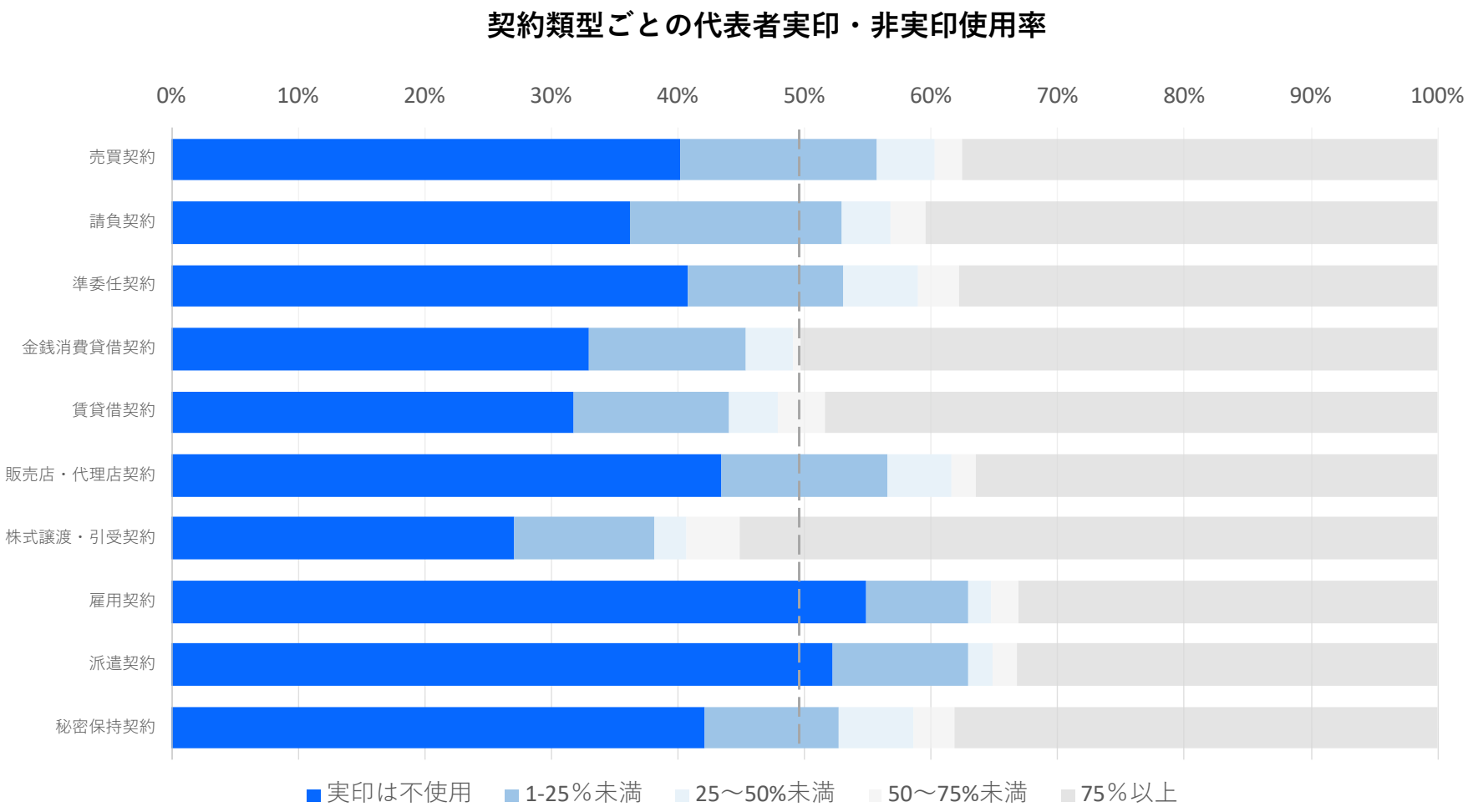
デジタル庁および本SWGの皆様にお伝えしたいこと（サマリー）

- 押印が支えた大量・迅速な商取引が、電子署名法の制定によってもデジタル化されなかったのは、同法の上振れしたトラストレベル設定がユーザーニーズに即していなかったことが原因

- そうした過去の反省を踏まえデジタル原則を実現するためには、「ちょうどよいトラスト」の選択肢を増やし、その普及をデジタル庁がリードすることが必要

- すでに国内外のユーザーの支持を集めるクラウド型電子署名サービスを、新しいトラスト法制において「スタンダード」と位置付けていただきたい

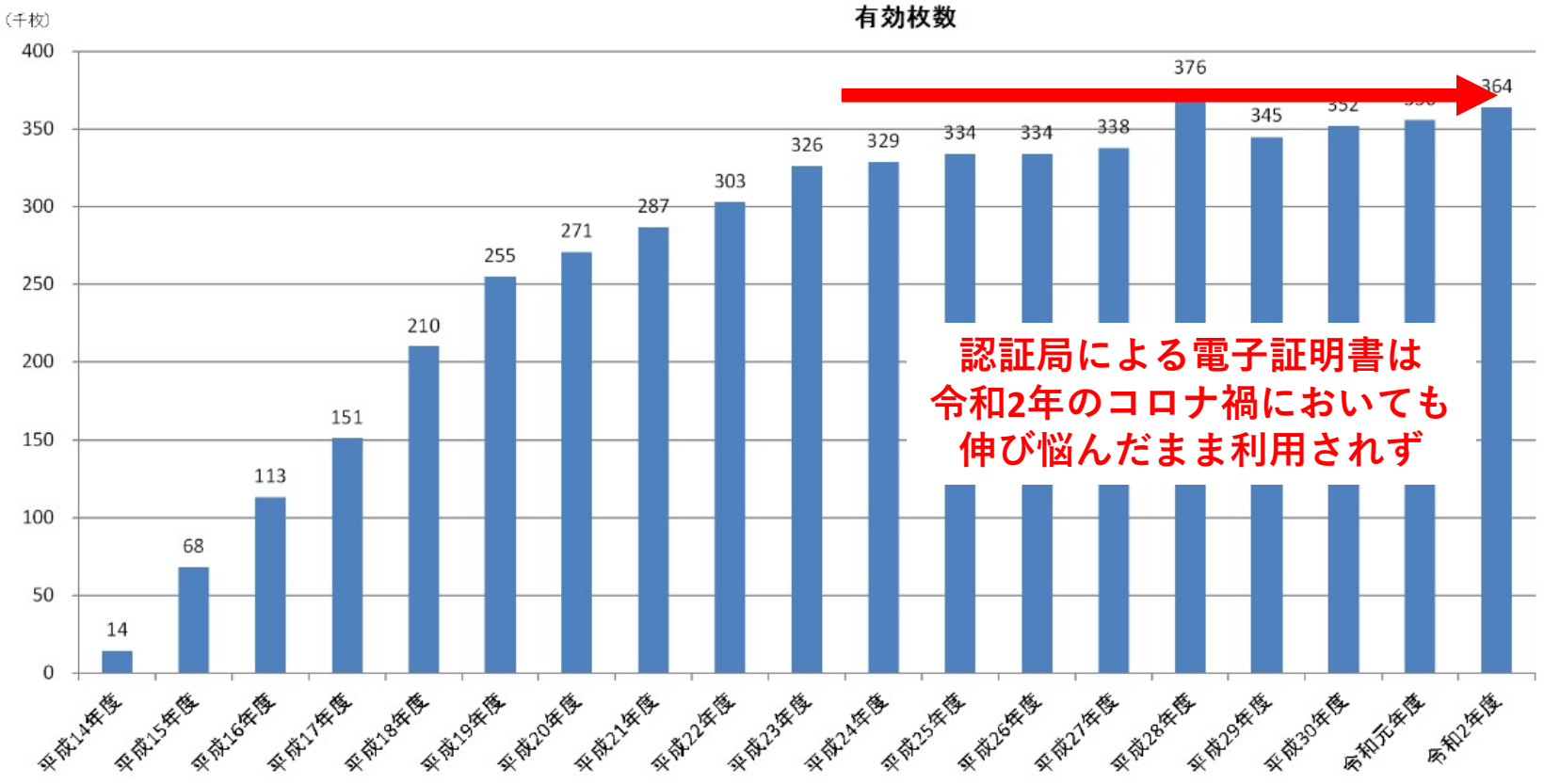
企業の押印実務においては、実印を使用せず、非実印を活用することで大量かつ迅速な商取引を実現している実態がある



2021年12月当協議会実施「紙の契約書に押印する実印／非実印の使い分けに関するアンケート」（n=489）

平成12年には当事者署名型を高度なトラストと位置付けた電子署名法が制定されたが、この10年ユーザーの支持は広がっていない

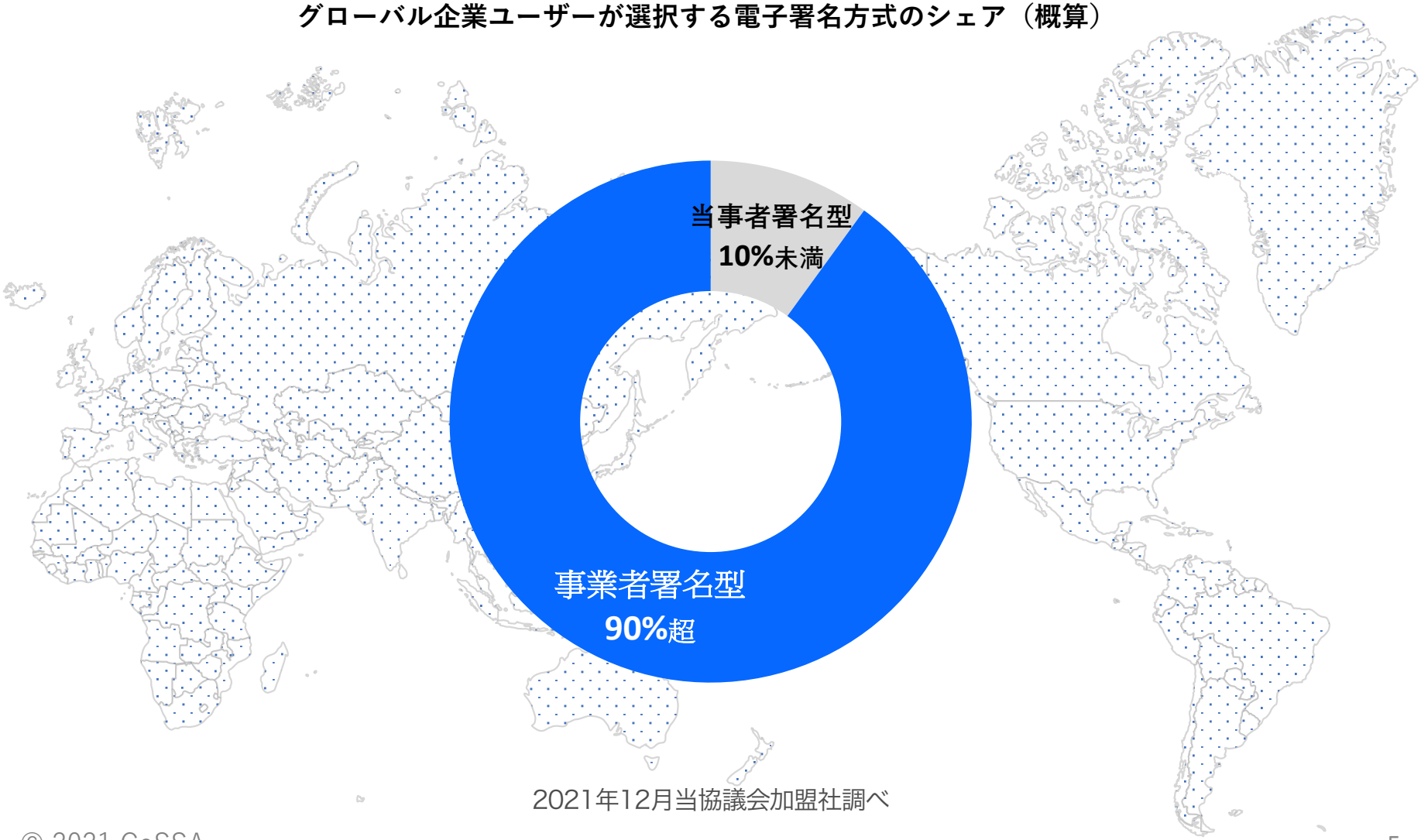
認定認証業務（民間認証局）から発行された電子証明書の推移



総務省2021年調査　https://esac.jipdec.or.jp/designated-investigative-organization/index.html

EUをはじめ当事者署名型が法制化されている諸外国においても、ユーザーがこれを選択・利用するケースは限定的

グローバル企業ユーザーが選択する電子署名方式のシェア（概算）



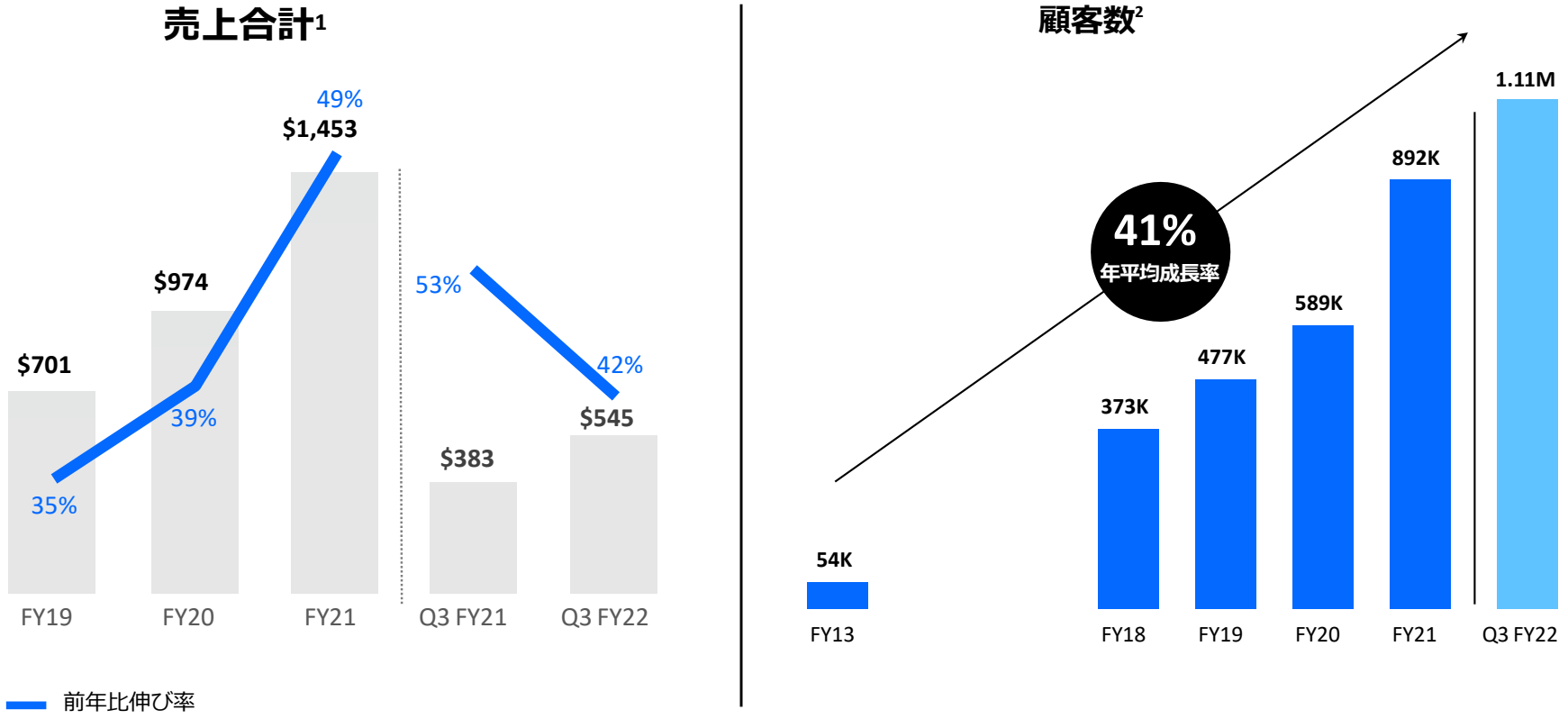
2021年12月当協議会加盟社調べ

一方、事業者署名型は「ちょうどよいトラスト」として企業に受け入れられ、近年の日本では数少ない成長産業の一つとなっている

（図表）構成員限り

グローバルでも、電子署名サービスのスタンダードとして、事業者署名型の利用が急速に拡大している

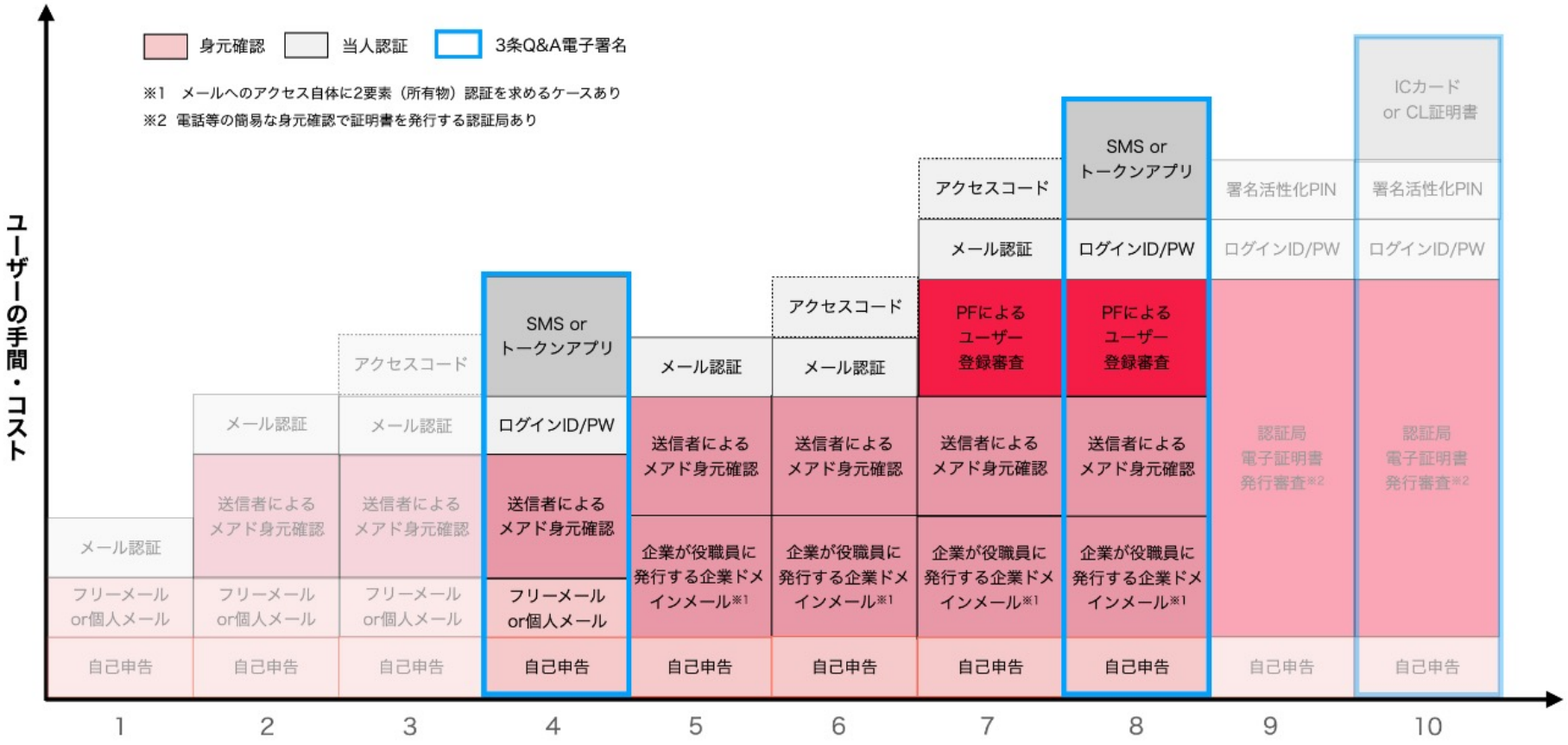
Docusignのグローバル売上合計・顧客数推移



(1) Fiscal years ended January 31 and fiscal quarters ended October 31. $ in millions.
(2) For the fiscal years ended January 31 and the fiscal quarter ended October 31, 2021.

UI・UXと安全性がバランスした「ちょうどよいトラスト」の選択肢を増やすために、クラウド型電子署名の普及促進が必要

電子契約における本人確認手法（身元確認・当人認証）の一覧



経済産業省「オンラインサービスにおける身元確認手法の整理に関する検討報告書」を参考に当協議会にて作成
https://www.meti.go.jp/press/2020/04/20200417002/20200417002-1.pdf

クラウド型電子署名サービスを、新トラスト法制において「スタンダード」と位置付けていただきたい

クラウド型電子署名サービス協議会　参画7社
（2021年12月現在）

Appendix

- 2021年12月当協議会実施
  紙の契約書に押印する実印／非実印の使い分けに関するアンケート

- クラウド型電子署名普及を支持するユーザーからの定性コメント

実印／非実印の使い分けに関するアンケート　回答者属性

・業種

業界	回答数	%
IT	97	20.0%
製造	69	14.2%
サービス業	62	12.8%
卸売	30	6.2%
建設	28	5.8%
士業	27	5.6%
運輸	18	3.7%
不動産	16	3.3%
小売	15	3.1%
情報通信	15	3.1%
人材	12	2.5%
福祉	10	2.1%
広告	8	1.6%
教育	9	1.9%
外食	6	1.2%
金融	7	1.4%
電気・ガス・水道	6	1.2%
医療	6	1.2%
公共機関	5	1.0%
メディア	4	0.8%
リース	0	0.0%
保険	0	0.0%
その他	35	7.2%

・従業員数

従業員規模	回答数	%
1-14名	160	32.9%
15-99名	138	28.4%
100-499名	104	21.4%
500－1999名	52	10.7%
2000名以上	32	6.6%

・役職

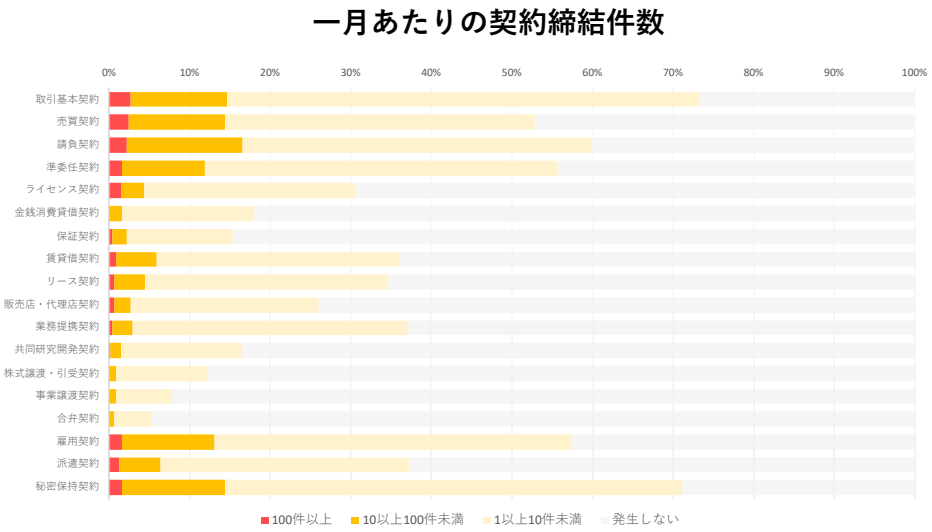
役職	回答数	%
代表・役員	176	36.1%
部長	83	17.0%
課長	98	20.1%
一般社員	130	26.7%

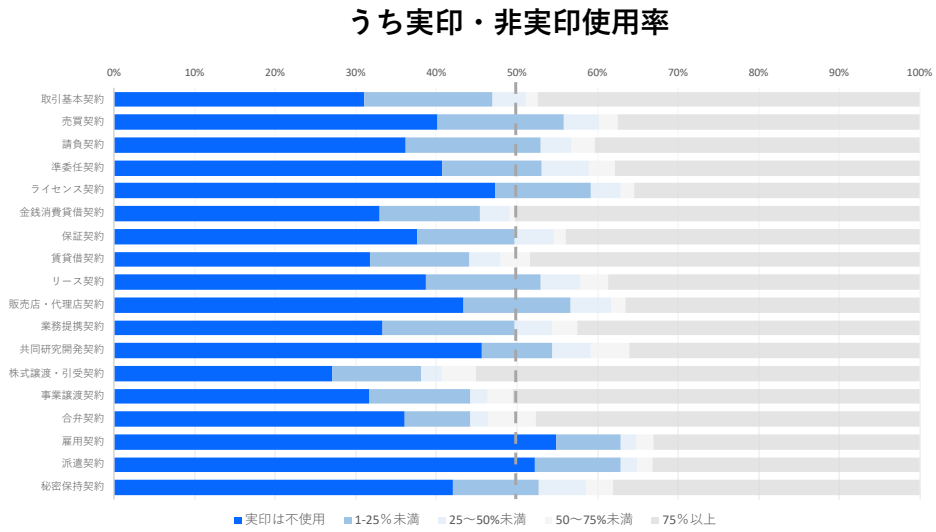
・押印業務への関与度合い

押印業務への関与度合い	回答数	%
契約書等への押印権限を持ち、自ら契約書等に押印する作業もしている	216	44.4%
契約書等への押印権限を持つが、押印作業は担当者に代理させている	33	6.8%
契約書等への押印権限はないが、権限者に代わって押印作業している	145	29.8%
契約書等への押印権限はなく、押印作業にもほとんど関与していない	92	18.9%

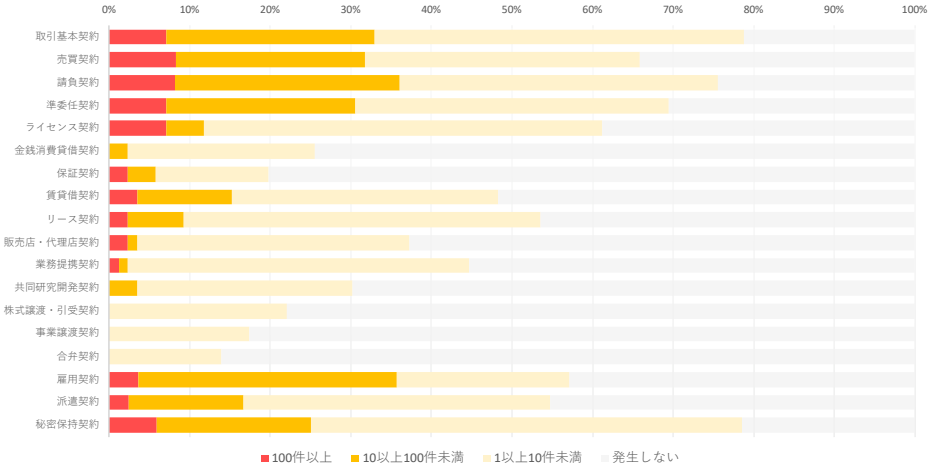
実印／非実印の使い分けに関するアンケート　— 全回答者 vs 従業員数500名以上

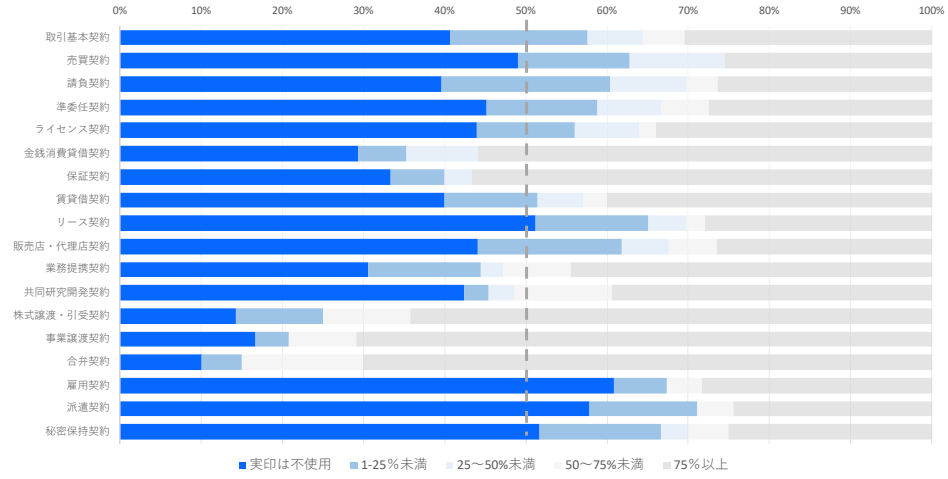
全回答者





うち従業員数500名以上





クラウド型電子署名普及を支持するユーザーからの定性コメント

「UI・UXがカギ」

- 電子署名に関して当社の利便性・経済性は高まり、**契約行為の負荷が減った**と感じる。実際に操作を経験した従業員の多くもそう感じているようだ
- 電子契約は**シンプルなUIで誰でも感覚的に使えるように**してほしい。マニュアルを見ないと進められないような形だと難しい
- 中小の事業者にはデジタル対応を専門で担う人材はいないので、**素人でも分かる仕組み**づくりをしてほしい
- 使いやすく、法人だけでなく**個人の利用も念頭においたもの**が良い

「上振れのトラスト法制は不要」

- **徒に現場が窮屈になるだけのような法制化は避けて**欲しい
- 法ありきのトップダウン型で電子署名を普及させることは、関連法規の整序がなされていない以上、**トラストサービスの法制化のみでは普及しない**と考えている
- 電子署名やタイムスタンプの**認定認証事業者が少なく利用料もそこそこするため、中小企業では導入するだけで負担**
- 当社は、契約印を用意することで、**実印を押す機会を制度的に減らし**ている

「デジタル原則徹底に期待」

- 電子契約を義務化もしくは原則化し、**税務上などなんらかのインセンティブを付与して**いただきたい。
- 長年染み付いている**押印神話は啓蒙や啓発活動によって変わるものではない。**政府主導で強制力を持って一気に進めていくしかない
- **個人事業主の方も導入せざるを得ない状況に**しないと、法人と個人事業主での乖離が生まれてしまう

「官公庁の率先垂範が必要」

- とてつもなく便利です。ぜひ**官公庁、自治体等において、物理印との利用選択を提出側にて指定できるように**していただくと、より普及すると思います
- **自治体との契約が一番印鑑種類指定や紙への押印要望が多い**ので、押印等のデジタル化を率先して進めてほしい
- **政府がまず電子契約を率先**して推奨し、民間企業に対する啓蒙活動を
- **法務局関連が押印不要に**なれば全て楽
- **法務局に電子署名による組合契約では登記を受理してもらえず**、毎回その目的の為だけに製本・押印しており不便

―専門家からの評価―

- クラウドサインをはじめとするクラウド型電子署名サービスでは、クラウドネイティブな時代に求められる利便性・ユーザ視点に立ったアクセスビリティ・強固なセキュリティ・証拠化など法的観点にも配慮したサービス提供がなされています。情報セキュリティと法の専門家の立場から、**当事者署名型の電子署名と比較しても企業ユーザーにとって十分に利用価値のあるものと評価**しており、こうした新しいサービスの普及に向けた制度構築支援をデジタル庁に望みます。
（TMIプライバシー＆セキュリティコンサルティング株式会社　代表取締役弁護士 大井哲也様・取締役弁護士 寺門峻佑様）
- クラウド型電子署名サービスは優れたUXを備えており、これらサービスを駆使する企業が増えてきていることを日々実感しております。また、弊所でも使用するケースが増えてきておりますが、クラウド型電子署名であることに起因するトラブルは特段なく、クライアント様に使用の推奨を行うこともございます。日常的に契約業務に携わる弁護士として、**クラウド型電子署名サービス普及という潮流は非常に歓迎すべきものと捉えており**、行政の支援による一層の普及を強く望んでおります。
（弁護士法人ネクセル総合法律事務所　代表弁護士 成川弘樹様）

資料１１

デジタル庁
トラストを確保したDX推進サブワーキンググループ（第２回）

eシール政策の検討状況と今後の課題・ニーズ

令和３年12月13日

総務省　サイバーセキュリティ統括官付
参事官　　高村　信

eシールに係る指針の策定

➢ 意見募集（意見募集期間：R3.5.1～6.4）の結果を踏まえ、我が国のeシールにおける信頼の置けるサービス・事業者に求められる技術上・運用上の基準等について整理した**「eシールに係る指針」を令和３年６月25日に公表。**

eシールに係る指針の概要

- 我が国におけるeシールの定義は、「電子文書等の発行元の組織等を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組み」とする。
- 発行元証明の信頼性を担保するための措置の水準に応じて、eシールのレベル分けを行う。
  - レベル1：上記eシールの定義に合致するもの
  - レベル2：一定の技術基準を満たすもの
  - レベル3：レベル2に加えて、十分な水準を充たしたトラストアンカー※1によって信頼性が担保されたもの（組織等の実在性の確認の方法や設備のセキュリティ要件等について、十分な水準を満たし、第三者のお墨付きがあるもの）
- eシール用電子証明書の発行対象となる組織等は、法人、個人（主に個人事業主を想定）、権利能力なき社団・財団、その他任意の団体等とする。

※1　インターネットなどで行われる、電子的な認証の手続きのために置かれる基点のこと。本指針においては、信頼性の起点となる認証局を想定。

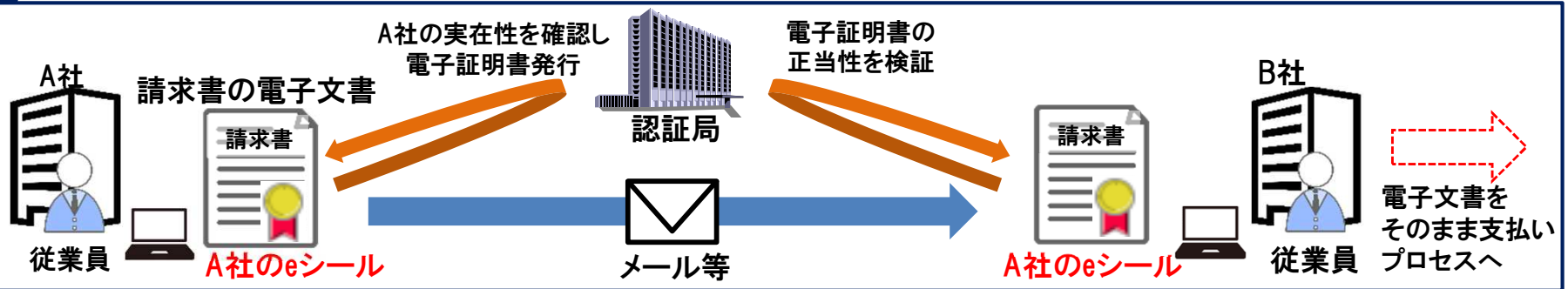
レベル3のeシールの基準となる要件（抜粋）

- ○ eシール用電子証明書の発行の際には、当該組織等の代表者の意思による申請に基づき、当該組織等の実在性を公的な情報（登記情報等）に裏付けられたエビデンスで確認すること。
- ○ eシール用電子証明書のフォーマットは、国際標準としても規定されているITU-T X.509を用いること。
- ○ 認証局の秘密鍵は、一定の厳しい要件を満たしたHSM※2によって厳格に管理されること。
- ○ 利用者の秘密鍵は、利用者自身で管理することとするが、認証局から利用者に対する説明事項として、秘密鍵の管理に係る事項（秘密鍵の管理は厳格に行うこと）を規定すること。

※2　Hardware Security Module の略。耐タンパー機構による物理的な安全性が確保された鍵管理機能を備えた暗号処理装置。

eシールのイメージ

【主なユースケース】
- 契約に紐付いて発生する書類
- 組織等が公開する情報（IR関連資料、広報資料等）
- 組織等が発行する証明書（各種証明書、各種保証書等）



参考

令和3年4月8日　IT総合戦略本部　データ戦略TF
第1回　トラストに関するワーキングチーム　配布資料

組織が発行するデータの信頼性を確保する制度に関する検討会取りまとめ

令　和　３　年　６　月

サイバーセキュリティ統括官室

はじめに

- Society5.0においては、実空間とサイバー空間が高度に融合し、**実空間での紙や対面に基づく様々なやりとりを、サイバー空間においても電子的に円滑に実現**することが求められる。

- その実現のためには、データを安全・安心に流通できる基盤が不可欠であり、**データの改ざんや送信元のなりすまし等を防止**する仕組みである**トラストサービスの重要性が高まっている**。

- 我が国におけるトラストサービスの在り方については、**2019年１月に**「プラットフォームサービスに関する研究会※1」の下に**「トラストサービス検討WG※2」を立ち上げ、**約１年間検討を進め、**2020年２月に最終取りまとめ**を実施した。

- トラストサービスの１つである**eシールは、**EUにおいて「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」と定義されているが、我が国では新しいサービスであることから、**一定程度国が関与し**つつも、基本的には民間の自主的な仕組みにより、e シールを提供するサービスの立上げやその導入が促進されるよう、信頼の置けるサービス・事業者を認定する民間の仕組みの創設に向け、**信頼の置けるサービス・事業者に求められる技術上・運用上の基準や認定の仕組みに関する検討を進めることが適当**であるとトラストWGの最終取りまとめで提言された。

- 当該提言を受け、**2020年４月に「組織が発行するデータの信頼性を確保する制度に関する検討会」を設置**し、**我が国におけるeシールの在り方について、検討**を進めてきた。

- 本取りまとめは、**我が国におけるeシールの在り方について、**国内の類似制度や国際的な整合性等を踏まえながら各検討事項についての**方向性等を取りまとめたもの**。

※1　総合通信基盤局長及びサイバーセキュリティ統括官共同開催。プラットフォーム事業者による利用者情報の適切な取扱いの確保の在り方等を検討
※2　サイバーセキュリティ統括官主催の研究会。

eシールの目的

- 新型コロナウイルス感染拡大に伴って、テレワークの推進が一層求められており、インターネット上で官民のあらゆるやり取りを完結する要請が高まるなか、トラストサービスの1つであるeシール（電子文書の発信元の組織を示す目的で行われる暗号化等の措置）がその重要な役割の一端を担うことが期待されている。
- eシールの活用によって、データ発行元の組織を簡便に確認できるようになり、これまで紙で行われていた書類等の企業間のやり取りを電子的に安全に行えるようになる。また、意思表示を伴わないことから、機械的に迅速・大量にeシールを行うことができるため、業務効率化や生産性向上が期待される。
- これまで本検討会では、eシールが有効だと考えられるユースケースについて、ヒアリングや提案募集等を通じて深掘りを行ってきた。
- デジタル・ガバメント閣僚会議 データ戦略タスクフォース※にて取りまとめられた「包括的データ戦略」においても、我が国におけるトラストを担保する包括的な枠組みの必要性が示された。

※　内閣官房情報通信技術（IT）総合戦略室及び内閣府政策統括官（科学技術・イノベーション担当）にて庶務を処理。主査は内閣総理大臣補佐官。

主なユースケースの例

- 見積もりから請求・支払プロセスまでの経理関係業務や契約に紐づいて発生する書類
- 組織が公開する情報（決算短信、ニュースリリース 等）
- 組織が発出する証明書（レポート、在職証明書、保証書 等）
- 監査手続において、外部証跡を入手及び確認する必要のある資料
- 行政と民間との間でやり取りされる証明書・報告書

データ戦略タスクフォースでの議論

➢ **「事実・情報」：発行元証明**

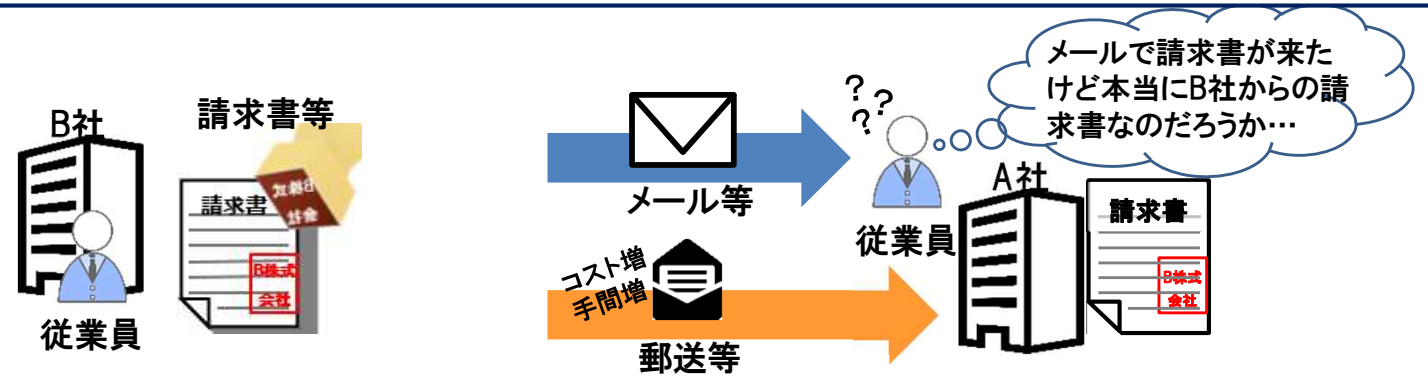
自然人、**法人や事業所などの「組織」**、さらには IoT 時代において爆発的に増大する「機器」が存在するという事実と、当該機器**が発行する情報等の信頼性を担保するためには、発行した自然人・組織・機器が信頼できるか、その発行方法が信頼できるのか、当該事実・情報が作成しようとした通りのものかなどの証明（発行元証明）が必要**である。

（データ戦略一次取りまとめ 令和2年12月21日 デジタル・ガバメント閣僚会議決定）

eシールの仕組み

- eシールとは、電子文書の発信元の組織を示す目的で行われる暗号化等の措置（技術的には電子署名と同じ仕組み）。
- 個人名の電子署名とは異なり、<u>使用する個人の本人確認が不要</u>であり、領収書や請求書等の経理関係書類等のような<u>迅速かつ大量に処理するような場面</u>において、<u>簡便にデータの発行元を保証することが可能</u>。
- eシールの活用により、<u>データ発行元の組織を簡便に確認</u>できるようになり、これまで紙で行われていた<u>書類等の企業間のやり取りを電子的に安全に行える</u>ようになり、従来の郵送の手間やコストの削減による業務効率化や生産性向上が期待される。

従来



B社は請求書等に会社印（角印等）を押印し、取引先（A社）に送付

請求書等を受け取ったA社は、B社の角印を確認し、請求書等の発行元がB社であることを確認

eシール

B社は請求書等のデータにB社のeシール（電子証明書は認証局が発行）を行い、メール等でA社に電子的に送付

請求書等のデータを受け取ったA社は、データに行われたB社のeシールを確認（検証）し、請求書等データの発行元がB社であることを確認

検討に当たっての主な観点

１．国内の類似制度との整合性

- 同じトラストサービスの1つである電子署名法上の電子署名との関係性
- 商業登記に基づく電子認証制度上の電子署名との関係性　等

２．国際的な整合性

- EU等の諸外国の仕組み・制度との整合性
- ISO等国際標準との整合性　等

３．eシールの普及・利用促進

- eシールの利用者視点で、わかりやすいeシールの目的・用途
- eシール用電子証明書発行事業者視点で、参考となるeシールの仕組みや技術基準　等

組織が発行するデータの信頼性を確保する制度に関する検討会

- eシールについて、ユースケースの具体化や有効性の検証を行うとともに、サービス提供者の認定の基準やそれに基づく民間の認定の仕組みを検討するために有識者検討会を開催。
- 学識経験者、会計関係、トラストサービス提供事業者、評価機関、経済団体（利用企業）等で構成。

1．構成員

	新井　聡	NTTネオメイト ITビジネス本部 プラットフォームサービス推進本部 電子認証サービス担当 主査
	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
	岡田　勲	日本電気株式会社 サイバーセキュリティ戦略本部 主席事業主幹
	小川　博久	日本トラストテクノロジー協議会 運営委員長
	小木曽　稔	一般社団法人新経済連盟 政策部 部長
	小田嶋　昭浩	電子認証局会議 事務局
	堅田　英次	東京海上日動火災保険株式会社 IT企画部 次長 兼 企画グループ 課長
	小松　文子	長崎県立大学 副学長
	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
	柴田　孝一	トラストサービス推進フォーラム　企画運営部 会長
	渋谷　秀人	富士通株式会社　政策渉外室 シニアエキスパート
	袖山　喜久造	SKJ総合税理士事務所 所長
（座長）	手塚　悟	慶應義塾大学 環境情報学部 教授
	中田　秀明	公益社団法人日本文書情報マネジメント協会 法務委員会 委員長
	中村　信次	株式会社日立製作所 公共イノベーションビジネス推進本部 公共戦略企画部 部長
	濱口　総志	慶應義塾大学SFC研究所 上席研究員
（座長代理）	宮内　宏	宮内・水町IT法律事務所 弁護士
	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
	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 主査 株式会社日本総合研究所 リサーチ・コンサルティング部門 上席主任研究員

（オブザーバー）　内閣府、内閣官房、法務省、財務省、金融庁、経済産業省

2．スケジュール

eシールの仕組みの全体像（例）

eシールの仕組み（例）

② eシール用電子証明書の発行対象となる組織等の範囲はどうあるべきか

⑤ eシール用電子証明書を発行するための認証局の鍵ペアを生成・保管する暗号装置の基準はどうあるべきか

1．eシール用電子証明書発行依頼

3．鍵ペアの生成
電子証明書発行

暗号装置

③ 組織等の実在性・申請意思の確認はどうあるべきか

2．組織の実在性・申請意思確認

利用者

A社

eシール用証明書
発行事業者
（認証局）

eシール用
電子証明書

4．eシール生成装置の送付

管理

④ 電子証明書の記載事項はどうあるべきか

公 Signature
eシール用
電子証明書

秘
A社の
秘密鍵

eシール生成装置

証明書
失効リスト

A社の従業員

eシール
生成装置

⑤ eシールを生成する装置の基準はどうあるべきか

確認

検証者
（依拠者）

6．eシールが行われたデータの送付

データ
（領収書等）

eシール

① 日本版eシールにはどのような要素が必要か

5．eシールの実施

eシールが行われた
データ
（領収書等）

7．eシールの検証

我が国におけるeシールの検討事項の全体像

我が国におけるeシールの在り方について、主に検討すべき事項は以下のとおり。

① eシールに求められる要素

② eシール用電子証明書の発行対象となる組織等の範囲

③ 組織等の実在性・申請意思の確認の方法

④ eシール用電子証明書の記載事項

⑤ 設備（認証局側の暗号装置、利用者側のeシール生成装置等）の基準

⑥ その他（一定の技術基準（リモート方式、CRL（失効リスト）等）等）

eシールの定義

確認事項

- 我が国におけるeシールの定義はどうあるべきか。

方向性

- 我が国におけるeシールの定義は以下のとおり。
  - **発行元証明**： 電子文書等の発行元の組織等を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組み。

デジタル・ガバメント閣僚会議（第10回）（令和2年12月21日）「データ戦略タスクフォース第一次とりまとめ」（P29）から抜粋

c)eシール
eシールとは、**電子文書等の発行元の組織を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組み**であって、発行元が個人に限らず組織となることもある。我が国においては、eシールに関する公的な仕組みは現状存在していないものの、一部の企業において、組織名の電子証明書としてe シールの導入が進んでいる。

同とりまとめ（P31）から抜粋

b)「事実・情報」:発行元証明
自然人、法人や事業所などの「組織」、さらにはIoT 時代において爆発的に増大する「機器」が存在するという事実と、当該機器が発行する情報等の信頼性を担保するためには、発行した自然人・組織・機器が信頼できるか、その発行方法が信頼できるのか、当該事実・情報が作成しようとした通りのものかなどの証明（発行元証明）が必要である。

eIDAS規則 Article3

‘electronic seal’ means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity;（「eシール」とは、データの起源と完全性を保証する為に電子データに添付又は論理的に関係している電子形式のデータをいう;）

【参考】議論であがった主な意見（抜粋）

- eシールの定義を発行元証明とすることに賛同。
- eシールと電子署名の違いを明確にし、使う側がどちらを使えばいいのかを明確にわかるようにした方がよい。

① eシールに求められる要素

検討事項

- eシールの用途等にあわせて、レベル感を分けて検討することが必要か。

方向性

- 我が国におけるeシールは以下のようにレベル分けを行う。

レベル3：レベル2に加えて、十分な水準※1を満たしたトラストアンカー※2によって信頼性が担保されたeシール（発行元証明として機能することに関し、第三者によるお墨付き（将来的には国による認定制度等の要否を検討）があるものを想定）

主な用途例：国際取引等における証憑類、法的に保存義務が課されているデータ、排他的独占業務とされている士業の証明書等

レベル2：一定の技術基準を満たすeシール（技術的には発行元証明として十分機能することが確認できるもの）

主な用途例：行政手続における提出書類※3、民民の契約に関連する書類、IR関連資料等の公開情報等

レベル1：裸のeシール（eシールの定義（P8参照）には合致するが、レベル2の要件を満たす保証がないもの）

主な用途例：民民における企業間で日常的にやり取りされる電子データ全般、発行元を担保したい情報等

注） eシールのレベルを判別するための呼称については将来決定することが必要。

今後、eシールは発行元証明として様々なユースケースでの使用が期待される。

例えば、国際取引等における証憑類に使用する場面においては、当該eシールについて国際的な整合性を求められることが想定され、行政手続における提出書類等に使用する場面においては、当該eシールが一定の水準を満たしていることを求められることが想定される。

一方、eシールの普及・利用拡大の観点では、例えば、日常的に企業間でやりとりする資料等にeシールを行ったり、個人事業主や中堅・中小企業等においてeシールを活用する場面においては、低コストで簡便に利用できるeシールのニーズも想定される。

また、EUにおいては、eシール、先進eシール、適格eシールと3つのeシールが定められており、用途やeシールの効力に応じてそれぞれのeシールが使い分けられている。

これらに鑑みて、我が国におけるeシールは、用途や活用場面に応じてレベル分けを行い、利用者自身である程度選択的にeシールを利用できるようなフレームワークにすることが適切だと考えられる。

※1 組織等の実在性確認の方法、電子証明書のフォーマット、認証局におけるセキュリティ要件等の一定の水準
※2 インターネットなどで行われる、電子的な認証の手続きのために置かれる基点。信頼性の起点となる認証局を想定。
※3 用途によっては、レベル3が必要となるケースも考えられる

【参考】議論であがった主な意見（抜粋）

- eシールは必ずしも完璧なものである必要はなく、例えば印鑑では印鑑登録しているものに限定していることもあれば、緩いものが使われることもあり、レベル分けされたeシールがあるのはいいこと。
- 用途等にあわせてeシールをレベル分けすることに賛同。
- eシールの法的効果として、「組織から発出されたことが推定できる」といったことを規定できるといいのではないか。

① eシールに求められる要素

【参考】各ユースケースとeシールのレベルとの関係性の一例

	分類① 契約関係	分類② 組織が公開する情報	分類③ 組織が発出する証明書	分類④ 官民間のやりとり	分類⑤ 監査関係	分類⑥ その他
高 発出元証明による信頼性担保の必要性 低 レベル3	• 領収書 • 請求書 • 【契約書】 • 見積書	• 気象データ • IR関連資料 • 広報資料	• 資格証明書（排他的独占業務とされている士業等）等 • 商工会議所が発行する貿易関係書類 • 健康診断結果証明書	• 法令上保存義務のある書類（国税関係等） • 国への各種申請書類等	• 監査の合格証明書 • 残高証明書	
レベル2	• 納品書 • 受領書	• 【会社法に定める議事録】 • デジタル名刺	• 生産者証明書 • 在学、卒業証明書 • 機器測定データ • 機器の保証書、ライセンス証書	• 請負、委託業務の成果物		
レベル1		• 企業間でやりとりされる一般的なデータ	• 加工証明書		• 企業文書	• 情報連携基盤・クラウド環境等でやり取りされるデータ

【 】内は、本来、意思表示を目的とする“電子署名”が馴染むと考えられるユースケース

主に機械的に大量に発行するものにeシールの活用が期待

② eシール用電子証明書の発行対象となる組織等の範囲

検討事項

- eシール用電子証明書の発行対象となる組織等の範囲は以下のどこまでを含めることが適切か。
  - 法人、個人事業主、権利能力なき社団・財団、その他の団体等の組織
  - 事業所・営業所・支店・部門等の組織内の細かい単位
  - その他（組織に所属する個人、機器等）

方向性

- **eシール用電子証明書の発行対象は、法人 、個人（主に個人事業主を想定）、権利能力なき社団・財団、その他任意の団体等の組織**とする。
- それよりも粒度の細かい、**事業所・営業所・支店・部門単位や、担当者**（意思表示を伴わない個人）**、機器については、電子証明書の任意のフィールドである拡張領域に記載**することができることとする。

eシール用電子証明書の発行対象については、対象とする組織自体の範囲や組織内のより細かい区分を含むかどうか等について検討が必要となる。

対象とする組織自体の範囲については、eシールの普及・利用拡大の観点から、発行対象の実在性を認証局が確認できることを前提に、法人に限定せず幅広い対象を含めることが適当だと考えられる。

他方、発行対象として組織内の事業所等を含むかどうかについては、含めることに対するニーズもあるが、認証局においてその実在性等を確認することが極めて困難である（確認できる内容に限界があり、信頼性にも課題がある）ことや、当該発行対象自体に変更（例えば、事業所統合・廃止や部署名の変更等）が生じた場合、その都度電子証明書の再発行が必要となることが想定され、利便性が著しく低下してしまう可能性があるといった課題があげられる。

なお、EUにおいては、発行対象は法人であり、事業所や営業所といった細かい単位や機器等については、電子証明書の任意のフィールドである拡張領域に記載可能になっている。

これらを踏まえて、eシール用電子証明書の発行対象は、法人 、個人（主に個人事業主を想定）、権利能力なき社団・財団、その他任意の団体等の組織とし、事業所や営業所といった細かい単位や組織に所属する個人や機器等については、電子証明書の任意のフィールドである拡張領域に記載することができることとすることが適切だと考えられる。

【参考】議論であがった主な意見（抜粋）

- eシールは発出元の証明であるということを考慮すると、 発行対象は法人（組織）とするのがいいのではないか。
- 発行対象として、事業所等まで含めることが望ましいが、組織の体制とeシールの紐付きが強固になってしまうと、組織の体制の変更等に伴って電子証明書の更新が頻繁に発生し、eシールの利便性の低下に繋がる可能性がある。

② eシール用電子証明書の発行対象となる組織等の範囲

検討事項

- eシール用電子証明書の発行対象を特定するための識別子はどうあるべきか。

方向性

- eシール用電子証明書の発行対象を特定するための**識別子については、既存のID・番号も含めて包括的に表現可能な方式**（OID：Object Identifier（オブジェクト識別子）等）**を軸として今後検討**することが必要。

eシール用電子証明書には、発行対象の組織等を一意に特定可能な識別子が必要となる。

その識別子については、eシール用電子証明書の発行対象である組織等を一意に特定可能なID・番号体系が我が国で既に存在していれば、そのID・番号体系を活用することが望ましいと考えられるが、我が国では官民どちらにおいても複数のID・番号体系が共存している状態（参考：P13）であり、発行対象を網羅的に管理可能な識別子として使用可能なID・番号体系が現状存在していない。

また、そのような識別子（番号体系）をベースレジストリとして整理していくことも考えられるが、その整理には別途多大な時間を要することが想定され、データ戦略タスクフォース等他の検討の場で議論されていることも考慮すると、我が国におけるeシールの在り方を検討する本検討会での議論の対象外だと考えられる。

これらに鑑みて、eシール用電子証明書の発行対象を一意に特定可能な識別子については、既存のID・番号も含めて包括的に表現可能な方式（OID：Object Identifier（オブジェクト識別子）等）を軸として今後検討することが必要であると考えられる。

【参考】議論であがった主な意見（抜粋）

- 今後、インボイスでeシールが活用されることを考慮すると、公的なデータベース（識別子）として適格請求書発行事業者登録番号も検討の余地があるのではないか。

② eシール用電子証明書の発行対象となる組織等の範囲

【参考】発行対象と既存の番号体系（一例）

【凡例】 ◎：全てに付番（悉皆性）　○：基本的には付番可　△：一部に付番可　ー：付番対象外

			法人番号	会社法人等番号	企業コード				その他
					TDB企業コード	TSR企業コード	D-U-N-S® Number	LEI※1	
eシール用電子証明書を発行する対象	組織・団体等	法人	◎	◎	○	○	○	○	―
		権利能力なき社団・財団	○	―	○	○	○	―	―
		その他任意の団体	―	―	○	○	○	―	―
		個人事業主	―	―	○	○	○	○	―
		その他の個人	―	―	―	―	―	―	マイナンバー、運転免許証、旅券番号 等
拡張領域に記載する対象	その他	事業所・営業所・支店・部門等	―	―	―※2	―※3	△※4	―	―
		担当者	―	―	―	―	―	―	社員番号 等
		機器	―	―	―	―	―	―	型番、シリアルナンバーの組合せ 等

（ヒアリング等の結果に基づき、事務局にて一例として整理）

※1　Legal Entity Identifier：　取引主体識別コード。金融商品の取引を行う当事者（法人、ファンド等）を識別するための国際的な番号。

※2　別体系で保持。

※3　日本国内に存在する事業所には TSR 企業コードは付与せず、事業所コードを付与。なお、事業所コードは単独では発番せず、TSR 企業コードに必ず付随する。

※4　事業所単位で付番。日本企業の場合、同一ビル内や事業所内にビジネスユニットが複数存在する場合、D-U-N-S®Numberを発番できるのは 1 箇所のみとなる。

③ 組織等の実在性・申請意思の確認の方法

検討事項

- レベル3のeシール用電子証明書の発行の際には、どのような手続・手段で確認することが必要か。

方向性

- 組織等の**実在性の確認については、登記事項証明書や第三者機関データベース等で行い、申請意思については、電子署名、押印、署名等で行うことが必要**。ただし、当該申請者（電子署名、押印、署名等をした者）が間違いなく当該組織の代表者又は代表者から委任を受けた者（委任状等によって委任を受けていることを確認できる場合に限る。）であることを確認できることが必要。
- **レベル3のeシール**の電子証明書の発行にあっては、**組織等の実在性の確認に用いるエビデンスが公的な情報に裏付けられたもの**であることが必要。

eシールは発行元証明であることから、架空の組織等のeシールやなりすましのeシールの流通を防止するため、eシール用電子証明書を発行する際には、発行対象の組織等が間違いなく実在していること（実在性）を確認し、かつ、発行申請が間違いなく当該組織に在籍する適切な権限を有した者（法人であれば代表者）によって行われたこと（申請意思）を確認する必要があると考えられる。

実在性の確認については、客観的に判断可能な情報である登記事項証明書や第三者機関が管理するデータベース等による確認が想定され、申請意思の確認については、当該組織等に在籍する適切な権限を有した者による電子署名や押印、署名等による確認が想定される。（詳細はP16参照）

ただし、レベル3のeシール用電子証明書の発行にあっては、十分な水準を満たした組織等の実在性の確認を行う必要があるため、実在性の確認は商業登記情報等の公的な機関が管理する情報に裏付けられたものであることを求めることが適切だと考えられる。なお、将来的には、データ戦略タスクフォース等他の検討の場で議論されているベースレジストリを活用して実在性の確認が行われることが望ましいと考えられる。

【参考】議論であがった主な意見（抜粋）

- 組織の確認に際しては、確認コストも見据えて優先順位付けが必要。公的な書類やデータベースで確認することは認証局にとって手間のかからない方法になる一方、実地調査はコストが高くなってしまう。
- 第三者機関データベースは、それがしっかり管理・構築されているかを確認しその扱いについてランク付けが必要ではないか。

③　組織等の実在性・申請意思の確認の方法

検討事項

- 登記よりも小さい単位（事業所・営業所・支店・部門等）については、当該組織の代表者による宣言の結果を尊重することが適切か、または認証局が事業所等の実在性を直接確認することが適切か。
- 機器は事業所・営業所・支店・部門等と同様に扱うか。

方向性

- 組織等よりも細かい粒度である、<u>事業所・営業所・支店・部門等や担当者、機器の実在性の確認については、組織の代表者の宣言の結果を尊重</u>することとし、<u>認証局はその結果に基づいて記載</u>することが適当。

eシール用電子証明書の任意のフィールドである拡張領域に記載可能な事業所・営業所・支店・部門等や担当者、機器等の実在性の確認について、認証局がそれらの実在性について何らか適切に確認した上で記載することが望ましいものの、確認の方法・程度によっては認証局による確認コストが大きくなり、ひいてはeシールのサービス利用料にも影響が及ぶことが想定され、eシールの普及・利用拡大の観点からも課題があると考えられる。

あくまでもeシール用電子証明書の発行対象は組織等であり、事業所・営業所・支店・部門等や担当者、機器等は、任意の拡張領域に記載されるということを踏まえると、認証局に対して、事業所・営業所・支店・部門等や担当者、機器等の実在性を確認することまで求める必要はないと考えられる。

したがって、事業所・営業所・支店・部門等や担当者、機器等の実在性の確認については、組織の代表者の宣言の結果を尊重することとし、拡張領域への記載事項については発行対象である組織等が一義的な責任を負うことが適当だと考えられる。

【参考】議論であがった主な意見（抜粋）

- 組織の確認として、事業等の細かい単位まで網羅的に認証局が確認することは、多大な負担となり、困難ではないか。
- 認証局が組織のどこまで確認するかという問題よりも、その記載した情報に誰が責任を持つかが重要。代表者が宣言していることを認証局が確認するという方法と、認証局においても何らか一定の事業所等の確認をするという方法がある。前者であれば、その事業所等の情報をeシールの証明書に記載することに果たしてどれだけの意味があるのかということについて検討が必要。後者であれば、一定の責任が認証局に出てくるが、それにどれだけ意味が出てくるのかは検討が必要。
- 組織の確認については、認証局側ですべき確認と第三者機関（TDBやTSR等）で行っている確認との切り分けを明確に整理すべきではないか。

③ 組織等の実在性・申請意思の確認の方法

方向性

- eシールに係る電子証明書の発行の手続きの整理の一例は以下の表のとおり。
  - ➢ 第三者機関データベースにて組織等の実在性確認を行う場合、レベル3にあっては商業登記情報等の公的な機関が管理する情報と照合されたものであることが求められる。

（★）はデジタルで行える手続

	組織等の実在性の確認	組織（代表者）の意思の確認	組織の代表者の在籍の確認
レベル3	• 商業登記電子証明書による電子署名が行われた利用申込（★）		
	• 登記事項証明書	• 申込書への押印（代表印に係る印鑑証明書が添付されている場合に限る）	
	• 第三者機関が管理するデータベース*（商業登記情報等の公的な機関が管理する情報と照合されたものに限る。）*（★）	• 代表者のマイナンバーカードの署名用電子証明書又は認定認証業務に係る電子証明書等による電子署名が行われた利用申込（★）…① • 申込書への代表者の署名又は押印…②	【甲： 意思の確認が①の場合】 • 第三者機関が管理するデータベース*（商業登記情報等の公的な機関が管理する情報と照合されたものに限る。）*に登録されている代表者の住所と電子証明書に記載されている代表者の住所の一致の確認（★） 【乙： 意思の確認が②、又は甲で確認できない場合】 • 第三者機関が管理するデータベース*（商業登記情報等の公的な機関が管理する情報と照合されたものに限る。）*に登録されている電話番号等を通じた代表者本人に対する当該申請の有無の確認
レベル2	• 第三者機関が管理するデータベース※（★）		【丙： 意思の確認が①の場合】 • 第三者機関が管理するデータベース※に登録されている代表者の住所と電子証明書に記載されている代表者の住所の一致の確認（★） 【丁： 意思の確認が②、又は丙で確認できない場合】 • 第三者機関が管理するデータベース※に登録されている電話番号等を通じた代表者本人に対する当該申請の有無の確認

※ 定期的に更新され、信頼できるデータソースとしてみなされるデータベース

④ eシール用電子証明書の記載事項等

検討事項

- eシール用電子証明書に記載すべき事項として何が考えられるか。
- eシール用電子証明書のフォーマットはどうあるべきか。
- eシールのレベルに応じて記載事項を検討する必要があるか。

方向性

- **レベル2及びレベル3のeシール用電子証明書のフォーマットはITU-T X.509**を使用する。
- 電子証明書には、**発行対象となる組織等の公式名称、当該組織等を一意に特定可能な識別子、有効期間、公開鍵、署名アルゴリズム、eシール用電子証明書の発行者、eシールのレベルを判別可能な情報、その他属性情報（営業所、事業所、機器等）等を記載**することとする。なお、レベル2で第三者（当該eシールサービスについて技術基準等を満たしているか否かの評価を行う機関）による評価を受けている場合は、評価を行った当該第三者機関を拡張領域に記載することを可能とする（レベル3の場合は、制度上明確化された認定主体であるため記載は自由）。レベル3、レベル2に関わらず、記載項目は変わらない。

レベル2及びレベル3のeシール用電子証明書のフォーマットについては、国内の類似制度（電子署名法における認定認証業務の電子証明書、商業登記電子証明書）や国際的な整合性に鑑みて、ITU-T X.509を使用することが適切だと考えられる。

eシール用電子証明書に記載すべき事項としては、発行元を示すための組織等の公式名称、当該組織等を一意に特定可能な識別子をはじめとして、電子証明書の有効期間、公開鍵、署名アルゴリズム等があげられる。

また、レベル2のeシールについては、例えば第三者による評価を受けたeシールが今後登場することも想定されるが、レベル3のeシールは認定主体が制度上明確である一方、レベル2のeシールはそもそも制度上の位置づけが明確でないため、当該eシール用電子証明書の検証時に当該eシールが第三者（当該eシールサービスについて技術基準等を満たしているか否かの評価を行う機関）による評価を受けたeシールであることが判別できるように拡張領域に記載することを認めることが信頼性確保の観点からは適切だと考えられる。

【参考】議論であがった主な意見（抜粋）

- eシール用電子証明書のフォーマットとして、X.509を採用することには異論なし。
- 発行対象を一意に特定可能な識別子は記載する必要がある。

④ eシール用電子証明書の記載事項等

【参考】eシール用電子証明書（ITU-T X.509）の記載の一例

	フィールド名	値（サンプル）
基本領域	バージョン	V3
	シリアルナンバー	WWWWWWWWW
	署名アルゴリズム	sha256RSA/sha512RSA
	署名ハッシュアルゴリズム	sha256/sha512
	発行者	**発行者を識別する情報**
	有効期限の開始時刻	Monday, January 5, 2020 5:00:00 PM
	有効期限の終了時刻	Thursday, January 5, 2022 5:00:00 PM
	サブジェクト	**発行対象となる組織等の公式名称、当該組織等を一意に特定可能な識別子等**
	公開鍵	RSA (2048bit)
	公開鍵パラメータ	05 00 …
拡張領域	認証機関アクセス情報	[1]CA証明書のURL [2]OCSPのURL
	サブジェクト鍵識別子	YYYYYYYYYY
	QCステートメント	**eシールのレベルを判別可能な情報等**
	証明書ポリシー	[1]0.4.0.194112.1.1/0.4.0.194112.1.3 [2] http://xxxxxxxxxxxxxx
	サブジェクト別名	**「事業所・営業所・支店・部門名、担当者、機器」や「組織等の和文商号」等**
	CRL配布ポイント	http://xxxxxxxxxxxxxxxCA.crl
	基本制約	Subject Type = End Entity
	鍵使用目的	Non-Repudiation (40)

注） 下線太字は具体的な記載方法について、今後検討が必要な項目

⑤ 設備の基準（認証局側の暗号装置）

検討事項

- レベル3のeシールにおける、認証局側の設備であるHardware Security Module（HSM※1）の基準はどうあるべきか。

※1 耐タンパー機構による物理的な安全性が確保された鍵管理機能を備えた暗号処理装置

方向性

- <u>レベル3のeシールにおける認証局側のHSMの基準は、</u>基本的には<u>電子署名法を準用</u>することとする。
- ただし、技術基準は現行化（FIPS140-2 レベル3相当）することを前提とし、念頭に置くレベルはFIPS140-2 レベル3相当もしくは、ISO/IEC 15408のEAL4+相当（プロテクションプロファイルは別途検討が必要）とする。

注）電子署名法の現行の基準はFIPS140-1 レベル3相当

認証局の秘密鍵は、例えば悪意のある第三者に盗まれて悪用された場合、当該認証局の発行するeシール用電子証明書の信頼性が著しく損なわれてしまい、当該認証局からeシール用電子証明書の発行を受けた全ての組織等に影響が及んでしまうため、認証局の秘密鍵はHSM等で厳格に管理されることが必要となる。

eシールにおける認証局の秘密鍵の管理の重要性については、同じトラストサービスの1つである電子署名の認定認証業務における認証局の秘密鍵の管理と同等だと考えられるため、認証局の秘密鍵の管理に係る具体的な基準については、電子署名法の認定認証業務で規定している基準を準用することが適切だと考えられる。

ただし、国際的な整合性も踏まえて、電子署名法の基準は現行化すること※2を前提とし、念頭に置くレベルはFIPS140-2 レベル3相当もしくは、ISO/IEC 15408のEAL4+相当（プロテクションプロファイルは要検討）を求めることが適切だと考えられる。

※2 電子署名法の現行の基準はFIPS140-1 レベル3相当であるが、理想的には現状の脅威に対抗できる要件が必要であり、例えば、現時点においてはFIPS140-2 レベル3相当にアップデートすることが望ましいとのご意見があった。

【参考】議論であがった主な意見（抜粋）

- 国内の類似制度や国際的な通用性に鑑みて、ISO/IEC 15408（コモンクライテリア）のEAL4+又はFIPS140-2 レベル3を求めることが適当ではないか。
- 現状の日本の認証局の数を考えると、HSMの基準として日本独自のプロテクションプロファイルを作成するのはコストがかかり過ぎるので、望ましくない。ISO/IEC 15408は国際相互認証されており、プロテクションプロファイルはそのためにあるので、それを適用するのがよいのではないか。
- 電子署名法と同等の基準を設けるということでよいと思う。現状の電子署名法の規定では、特定の認証取得製品に限定しておらず、FIPSでもISO/IEC 15408でも使用できるような記載になっているため、同じような記載でいいのではないか。その上で、実際にどのような製品（FIPS認証製品なのか、ISO/IEC 15408認証製品なのか、その他の認証製品なのか等）を使っていくかは別の議論。
- 電子署名法の基準を準用するということでよいと思うが、電子署名法の現行の基準はFIPS140-1 レベル3相当であるため、まずはFIPS140-2 レベル3相当にアップデートすることが必要ではないか。

⑤ 設備の基準（認証局側の暗号装置）

【参考】HSMについて

- HSMとは、耐タンパー機構による物理的な安全性が確保された鍵管理機能を備えた暗号処理装置。

～電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針～（抜粋）

注） FIPS140-1 レベル3の基準がベースになっていることに留意

2. 暗号装置関係

(1) 規則第4条第4号に規定する「専用の電子計算機」（以下「暗号装置」という。）とは、発行者署名符号の漏洩、破損、消失等の事象の発生を可能な限り低い確率に抑えるための以下の機能を備えたものをいう。

ア 暗号化されていない状態の暗号符号や認証データ等、保護されていない形式の重要なデータに係る暗号装置への入出力が行われるインタフェースが存在する場合は、そのインタフェースは他のデータの入出力を行うインタフェースとは物理的に独立したものであること。

イ 暗号装置は、以下の機能を有するものであるとともに、暗号装置の操作者ごとに機能ごとの権限の有無が特定されているものであること。

(ｱ) 操作者機能: 暗号化、署名等、通常の暗号化機能を実施するための機能

(ｲ) 管理者機能: 暗号装置自体の初期化、署名符号などの重要パラメータの投入等、暗号装置を管理するための機能

ウ 発行者署名符号等のデータの盗難を回避するため、暗号装置は、以下のいずれかの物理的なセキュリティ対策が講じられていること。

(ｱ) 暗号装置が IC チップ単体からなる場合、IC チップが強固で除去困難な材質の不透明なコーティングで覆われていること。

(ｲ) 暗号装置にカバーが施されている場合、物理的な侵入行為に対し、暗号装置の機能の停止、内部データの無効化等の耐タンパ対策が講じられていること。

(ｳ) 暗号装置の筐体に排気用スリットもしくは空孔が存在する場合、それらは十分小さく、かつ、検出されずに筐体の中をプローブされることを防止する対策が講じられていること。

エ 暗号装置に係る発行者署名符号の管理に関し、以下の措置が講じられていること。

(ｱ) 暗号装置内で発行者署名符号の生成を行う場合、安全な擬似乱数生成アルゴリズムを用いるものであること。

(ｲ) 暗号装置への発行者署名符号の入出力を行う場合には、以下のいずれかの方式であること。

① 発行者署名符号は暗号化された上で入出力されること。

② 発行者署名符号を2つ以上の構成要素に分割して入出力を行う場合は、暗号装置に対して直接行うこととし、発行者署名符号の各構成要素に対する操作者の認証が行われること。また、発行者署名符号の各構成要素は、暗号装置内で分割、結合されること。

(ｳ) 発行者署名符号を暗号化されていない状態で暗号装置内に保管する場合は、外部からアクセスできない仕組みとすること。

(ｴ) 発行者署名符号を廃棄する際には、発行者署名符号その他のセキュリティパラメータを無効化する機能を有すること。

(2) 省略

⑤　設備の基準（利用者側のeシール生成装置）

検討事項

- レベル3のeシールにおける、利用者側のeシール生成装置の基準を求めることが適切か。
- 求める場合、その基準はどうあるべきか。

方向性

- 当面は、一定の基準を満たしたeシール生成装置を用いることを認定の要件とはしないことが適当。ただし、第三者機関による認証を受けたeシール生成装置（以下、「認証eシール生成装置」という。）を用いてもよい。
- また、認証eシール生成装置を使用していないにも関わらず、認証eシール生成装置を使用していると誤認させる表示は禁じる。一方、国際的な整合性の観点から、認証eシール生成装置を用いている場合、当該eシールが認証eシール生成装置を用いて行われていることを検証者が判断可能な仕組みとすることが適切。
- なお、国際的なやりとりにおいて、諸外国がQSCD等の認証eシール生成装置を求める場合は、我が国におけるQSCD等の認証eシール生成装置で秘密鍵を管理して行われたeシールが、海外でも認められるための仕組み（工夫）について今後検討が必要。

利用者の秘密鍵が悪意のある第三者に盗まれた場合、利用者の意図しないところでeシールが悪用されることが想定され、EUの適格eシールにおいては、利用者の秘密鍵を耐タンパー性を備えた適格eシール生成装置（QSCD）に格納して利用することを求めている。

他方、利用者の秘密鍵は認証局の秘密鍵とは異なり、盗まれて悪用された際の影響はeシール用電子証明書の発行を受けた組織等に限定され、認証局から利用者への秘密鍵の受け渡しを安全かつ確実に行えば、その先は利用者側の管理の問題という考え方もできる。

なお、意思表示のために使用され、推定規定が法定されている電子署名であっても、署名生成装置に関する規定が設けられていない。

これらを踏まえて、当面はeシールにおいても、一定の基準を満たしたeシール生成装置を用いることを認定の要件とはしないことが適当だと考えられる。

ただし、国際的な整合性の観点から、認証eシール生成装置が必要となる場面も将来的には想定されることから、認証eシール生成装置を用いてもよいこととし、認証eシール生成装置を用いて行われたeシールであるかどうかを検証者が判断できる仕組みとしておくことが適切だと考えられる。

なお、電子署名法含め、将来的に利用者側の生成装置に関してセキュリティ上の問題が生じた場合には、改めて生成装置の要否について検討が必要。ただし、仮に生成装置を求めることになった場合は、現状の電子署名法の認定基準の強化（これまで認められていたものが認められなくなる）となる点に留意が必要。

⑤　設備の基準（利用者側のeシール生成装置）

～前ページからの続き～

【参考】議論であがった主な意見（抜粋）

- 日本でも少なくともQSCD相当のものを使用して耐タンパ性能が確保されたところで秘密鍵が管理されるよう規程の整備が必要ではないか。Society5.0やDFFTを実現していく上で、データを自動で検証して処理し、更にそのデータが自動処理されていくということを想定していくと、検証時に秘密鍵が適切な環境で保護されているかどうかを確認できる必要がある。レベル3のeシールでQSCDを求めるかどうかは別の議論になるが、EUのQCステートメントのように、少なくとも検証時において、QSCDを使用していることがわかるような制度にした方がいい。
- 電子署名法とのバランスが重要である一方、EUとの相互運用の関係もあるので非常に難しい問題。商業登記や法的効力のある電子署名法でも署名生成装置は規定されておらず、また、実世界でも実印の管理については規定がないため、QSCDの規定は設けないという考え方が1つある。電子署名には推定効というものがあるが、eシールがそれ以上の効力を持つことは考えられないのでeシールにのみQSCDを求めるというのは全体のバランスを欠くのではないか。
- QSCDの規定を設ける場合、QSCDの使用/未使用によってeシールの効力にどれだけ違いが出るのかについては、レベル2、3問わずeシールには現段階では法的効力がないことを考えると、EUの適格として通用するかどうかではないか。
- 選択肢としては、電子署名法でもeシールでも両方QSCDを求めるか、あるいは両方求めないか、という2択になるのではないか。両方求める場合は、現状規定のない電子署名法は規制強化になってしまうことが懸念される。他方、両方求めない場合はEUと相互運用を目指す際に課題となる。従来の我が国の法制度の中での秘密鍵等の管理は本人に任されていて本人の責任であるという考え方を維持するのであれば、QSCDは必須にしないが、秘密鍵等の管理の方法として、QSCDを使用する方法もあるということやEUとやりとりする際のオプションとして使用することをガイドライン等に記載するのはどうか。
- eシールの普及という観点では、国内での申告や申請等に利用するということでレベル2の世界で考え、レベル3については欧州等の諸外国との相互運用に値する他国に恥じない基準にすることが適切ではないか。
- EU等の諸外国との相互運用の観点も重要であるが、QSCDの規定を設ける場合は実際の企業側の運用と基準がどうフィットするのかについても検討が必要ではないか。

⑤　設備の基準（認証局側の暗号装置の管理）

検討事項

- レベル3のeシールにおける、認証局側のHSMの管理に係る基準はどうあるべきか。

方向性

- <u>レベル3のeシールにおける認証局側のHSMの管理に係る基準は、基本的には電子署名法を準用することとする。</u>

認証局のHSMの管理については、秘密鍵を管理しているというその重要性に鑑みて、HSMが配置される部屋への入出場に係る基準、HSMに対する不正アクセス防止に係る基準、災害対策に係る基準等が一般的に求められると考えられる。

eシールにおける認証局のHSMの管理の考え方については、同じトラストサービスの１つである電子署名の認定認証業務における認証局のHSMの管理の考え方と同等だと考えられるため、認証局のHSMの管理に係る具体的な基準については、電子署名法の認定認証業務で規定している基準を準用することが適切だと考えられる。

【参考】議論であがった主な意見（抜粋）

- 電子署名法の認定認証業務で要求している基準と同等の基準を求めることが適切ではないか。

⑤　設備の基準（認証局側の暗号装置の管理）

【参考】電子署名法の認定認証業務におけるHSMの管理に係る規定

～電子署名及び認証業務に関する法律施行規則第４条第１項（抜粋）～

（認証設備室への入出場の管理に関する規定）

１　申請に係る業務の用に供する設備のうち電子証明書（利用者が電子署名を行ったものであることを確認するために用いられる事項（以下「利用者署名検証符号」という。）が当該利用者に係るものであることを証明するために作成する電磁的記録をいう。以下同じ。）の作成又は管理に用いる電子計算機その他の設備（以下「認証業務用設備」という。）は、入出場を管理するために業務の重要度に応じて必要な措置が講じられている場所に設置されていること。

（認証業務用設備へのアクセス等の管理に関する規定）

２　認証業務用設備は、電気通信回線を通じた不正なアクセス等を防止するために必要な措置が講じられていること。

（認証業務用設備の作動権限等の管理に関する規定）

３　認証業務用設備は、正当な権限を有しない者によって作動させられることを防止するための措置が講じられ、かつ、当該認証業務用設備の動作を記録する機能を有していること。

４　HSM自体の基準のため省略

（災害対策に関する規定）

５　認証業務用設備及び第一号の措置を講じるために必要な装置は、停電、地震、火災及び水害その他の災害の被害を容易に受けないように業務の重要度に応じて必要な措置が講じられていること。

注）　これらの規定は、HSMに限らず、認証業務用設備全般についての規定であることに留意

⑤　設備の基準（利用者側の秘密鍵の管理）

検討事項

- レベル3のeシールにおける、利用者側の秘密鍵の管理に係る基準はどうあるべきか。
  - ①　1つの秘密鍵を複数人で共同で使用することを禁じるか。
  - ②　又は、利用者側で秘密鍵を複製し、複数人がそれぞれ管理して使用することを禁じるか。
  - ③　又は、同一の組織等に対して複数のeシール用電子証明書（及び秘密鍵）を発行することを禁じるか。

方向性

- 利用者の秘密鍵の管理は発行対象である組織等の管理に委ねることとする。
- ただし、認証局から利用者に対する説明事項として、秘密鍵の管理に係る事項（秘密鍵の管理は厳格に行うこと（複製は望ましくない等））を規定することが適切。

利用者の秘密鍵の管理次第では、当該秘密鍵が漏えいして悪用される懸念があることから、秘密鍵の管理は厳格に行われる必要がある。他方、仮にeシールに係る認定制度ができた場合でも、利用者側が所持している秘密鍵（生成装置に格納している場合は生成装置）の具体的な管理の在り方に関して、フレームワーク上で何らか利用者側に義務を課すことは困難であることが想定される。

電子署名法の認定認証業務においては、利用者の秘密鍵の管理に係る直接的な規定はないが、認証局に対する要求事項として、秘密鍵は十分注意を持って管理する必要がある旨を利用者に説明することが規定されており、秘密鍵の管理は利用者に委ねられている。

EUの適格eシールにおいても、秘密鍵（適格eシール生成装置）の管理は法人の管理下にあることが規定されているのみ（ただし、適格eシール生成装置を用いるため、秘密鍵の複製は不可）となっている。

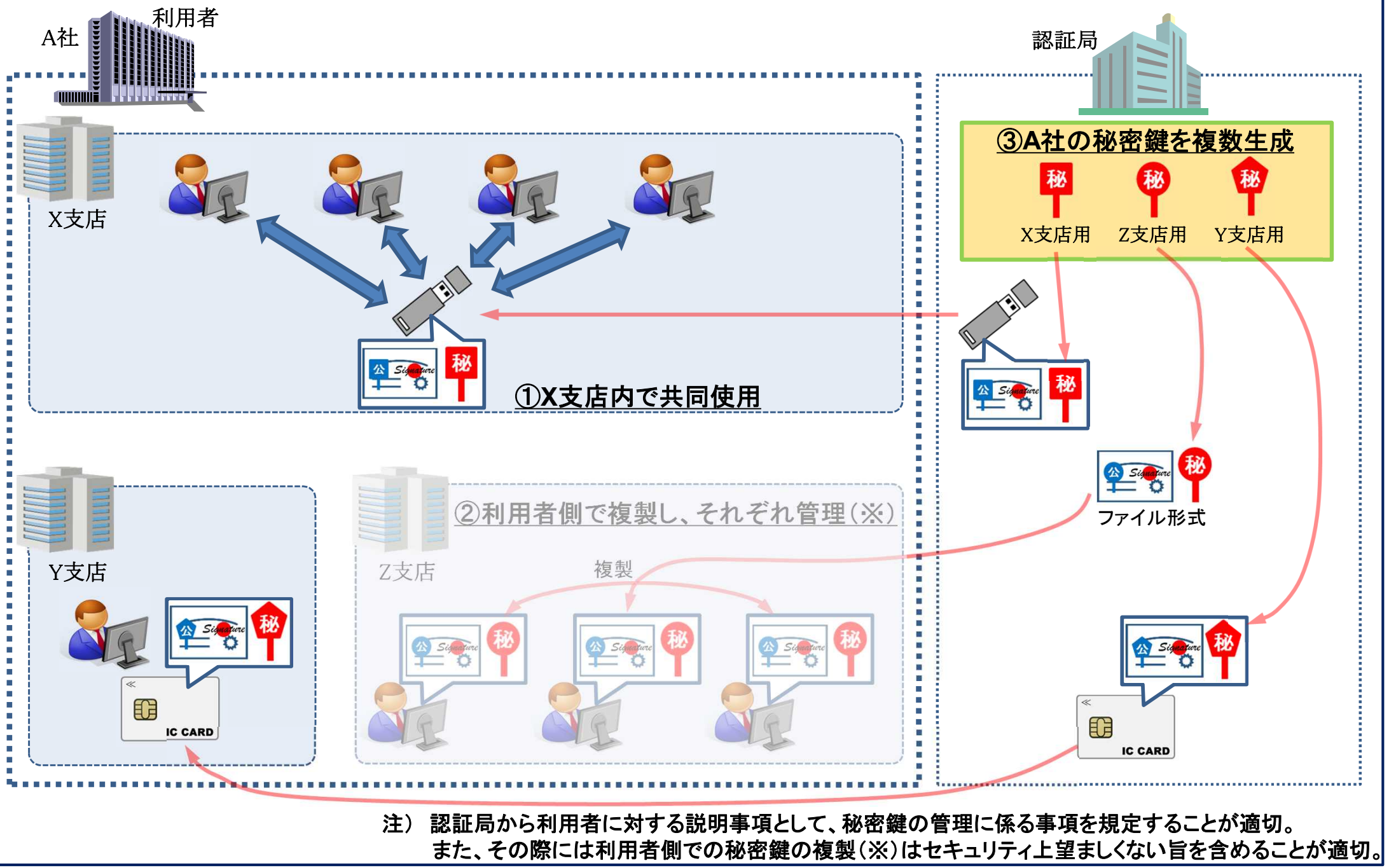
これらに鑑みて、利用者の秘密鍵の管理は発行対象である組織等に委ねることが適切だと考えられる。ただし、認証局から利用者に対する説明事項として、秘密鍵の管理は厳格に行うこと（複製は望ましくない等）を規定することが適当だと考えられる。なお、秘密鍵の管理が利用者に委ねられ、利用者側での複製が望ましくないことを考慮すると、当然、認証局側での利用者の秘密鍵の複製も望ましくない。

【参考】議論であがった主な意見（抜粋）

- EUでは法人の管理下にあることが求められており、電子署名法でも実質的には同じルールになっているため、特段の要件は不要ではないか。
- QSCDを求めない以上、ファイル形式で利用者に秘密鍵を渡すことも可能であるため、ユーザー側でも複製ができてしまうことになると思うが、特にレベル3のeシールにあっては、利用者の秘密鍵を利用者側で複製できるのは望ましくないのではないか。
- 利用者の秘密鍵の管理については、少なくとも認証局から利用者への重要事項説明として規定するべきではないか。
- 有事の際のバックアップを考えると、利用者側での秘密鍵自体の複製ができないと困るのではないか。
- 利用者の秘密鍵の複製については、同一の組織に複数のeシール用電子証明書（及び秘密鍵）を発行することで対応可能。

⑤　設備の基準（利用者側の秘密鍵の管理）

【参考】利用者側の秘密鍵の管理の一例



注）　認証局から利用者に対する説明事項として、秘密鍵の管理に係る事項を規定することが適切。
また、その際には利用者側での秘密鍵の複製（※）はセキュリティ上望ましくない旨を含めることが適切。

⑤　設備の基準（利用者側の秘密鍵の管理）

【参考】電子署名法の認定認証業務における認証局から利用者への説明事項に係る規定

～電子署名及び認証業務に関する法律施行規則～（抜粋）

第六条　法第六条第一項第三号の主務省令で定める基準は、次のとおりとする。

一　利用申込者に対し、書類の交付その他の適切な方法により、電子署名の実施の方法及び認証業務の利用に関する重要な事項について説明を行うこと。

～電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針～（抜粋）

第八条　規則第六条第一号に規定する利用申込者に対して説明を行うべき事項とは、次の各号に掲げる事項を内容として含むものとする。

一　認定認証業務においては、虚偽の利用の申込みをして、利用者について不実の証明をさせた者は、法第四十一条の規定により罰せられること。

二　電子署名は自署や押印に相当する法的効果が認められ得るものであるため、**利用者署名符号については、十分な注意をもって管理する必要があること。**

三　利用者署名符号が危殆化（盗難、漏えい等により他人によって使用され得る状態になることをいう。以下同じ。）し、又は危殆化したおそれがある場合、電子証明書に記録されている事項に変更が生じた場合又は電子証明書の利用を中止する場合においては、遅滞なく電子証明書の失効の請求を行わなければならないこと。

四　認定認証業務に係る電子証明書を使用する場合における電子署名のためのアルゴリズムは、認証事業者が指定したものを使用する必要があること。

⑥　その他（eシールを大量に行う際の処理）

検討事項

- レベル3のeシールにおいて、複数の対象データに一括でeシールを行うことを認めるか。

方向性

- レベル3のeシールにおいて、複数の対象データに一括でeシールを行うことを認めることが適当。

eシールにおいては、業務効率化の観点から、ローカル/リモート方式に限らず機械的に複数の対象データ（例えば領収書等）に対して一括でeシールを行うことに対するニーズがある。

一括処理について、我が国における実空間での手続では、複数の対象文書（例えば委嘱状等）に対して、まとめて処理（決裁・押印）することは一般的に実施されている。

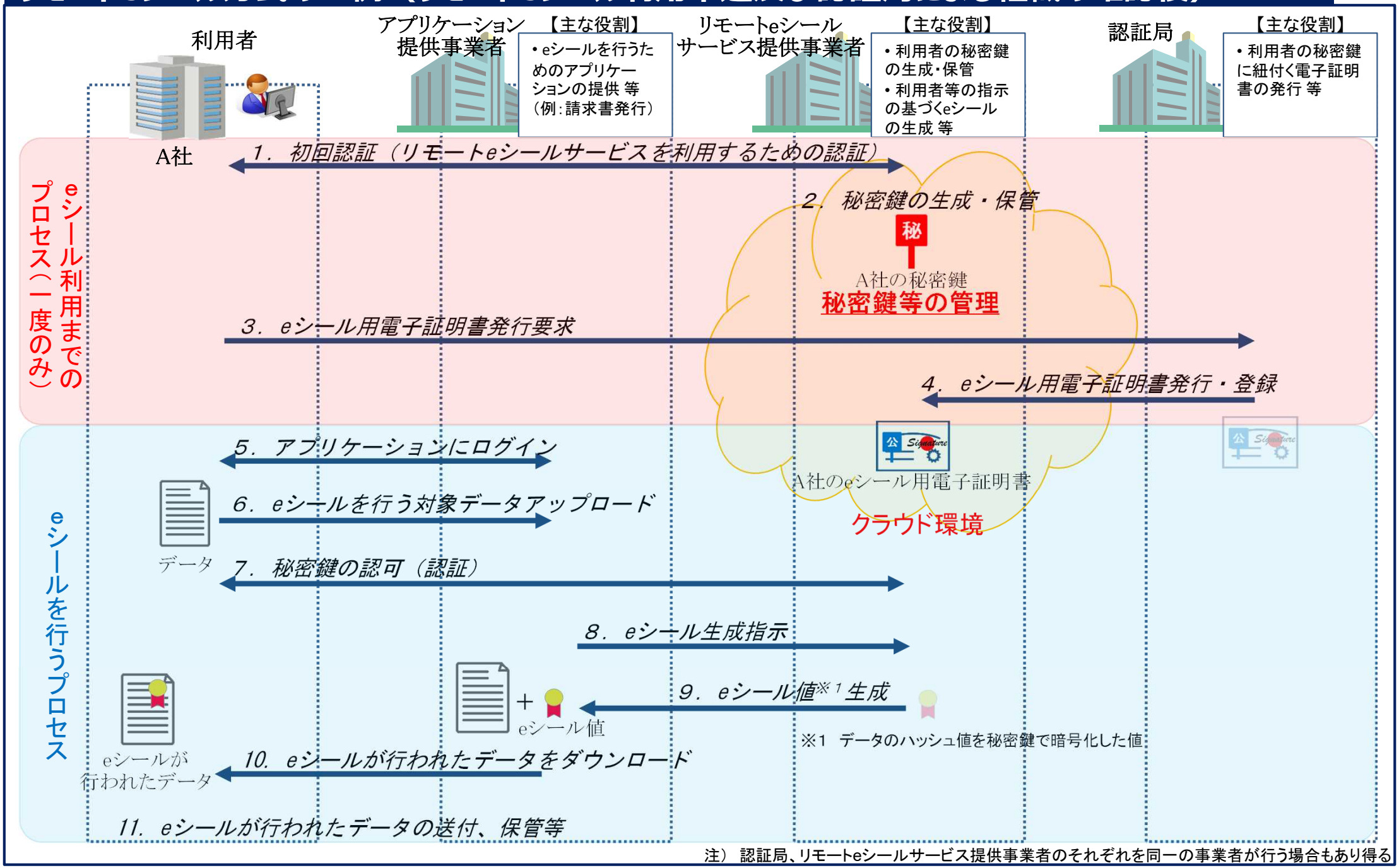
また、EUの適格eシールにおいては、ローカルeシールについては特段の規定がないが、リモートeシールについてはCENの技術基準において、複数の対象データに一括で署名（eシール）指示することが認められている。

eシールの普及・利用促進の観点や国内における実運用、EUの制度を踏まえ、そもそもeシールは意思表示を伴わず、発行元証明にとどまるということに鑑みて、レベル3のeシールであっても、複数の対象データに一括でeシール行うことを認めることが適当だと考えられる。

ただし、一括でeシールを行う際には、当然利用者が指定したデータのみにeシールが行われることが求められることから、利用者が対象データに対してeシールを行う指示を行って以降、他のデータが紛れ込むことがないことはeシールサービス側で担保する必要がある。

⑥ その他（リモート方式）

リモートeシール方式の一例（リモートeシール利用申込及び認証局による組織の確認後）



注） 認証局、リモートeシールサービス提供事業者のそれぞれを同一の事業者が行う場合もあり得る

⑥ その他（リモート方式）

ローカルeシール方式の一例（ローカルeシール利用申込及び認証局による組織の確認後）

【主な役割】
・利用者の秘密鍵の生成
・利用者の秘密鍵に紐付く電子証明書の発行 等

利用者

A社

認証局

eシール利用までのプロセス（一度のみ）

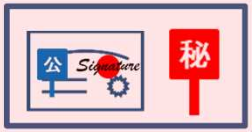
1．秘密鍵の生成

A社の秘密鍵

2．eシール用電子証明書発行

A社のeシール用電子証明書

eシール生成装置



秘密鍵等の管理

3．秘密鍵及びeシール用電子証明書、（eシール生成装置）の送付

eシールを行うプロセス

4．対象データにeシールを実施（秘密鍵の認可（PIN入力等）及びeシール値生成）

eシールが行われたデータ

5．eシールが行われたデータの送付、保管等

⑥　その他（リモート方式）

検討事項

- リモートeシールサービス提供事業者が利用者の秘密鍵を管理し、利用者がそのリモート環境にある秘密鍵にアクセスしてeシールを行う方式であるリモートeシールについて、レベル3のリモートeシールを行う際にはどのような認証が必要か。

注1）なお、ローカルeシールでは、利用者自ら秘密鍵を管理していることに留意。

方向性

※　日本トラストテクノロジー協議会（JT2A）が作成したリモート署名に関する技術的な基準を示したガイドライン

- **レベル3のリモートeシールにおいては、少なくとも利用認証**（eシールを行うことができる権限者（リモートeシールサービスへの登録者）であることを認証するための認証）と**鍵認可**（実際にeシールを行うために利用者の秘密鍵を利用できる状態にすること）**を別に求めることが適切**。
- ただし、上記の**鍵認可の場面で複数要素認証（例えば、所持認証＋知識認証）までは要求しない**。

注2）レベル2のリモートeシールは、利用認証と鍵認可を別々に行わなくてもよい。

ローカルeシールにおいては、一般的に利用者自身が管理している秘密鍵をPINコード等によって鍵認可を行い、eシールを行う形式が想定される。

ローカルeシールにおける認証を踏まえると、利用者の秘密鍵を利用者自身で管理するのではなく、リモートeシールサービス提供事業者が管理するリモートeシールにおいては、まずは利用者の秘密鍵が保管されているリモートeシールサービス提供事業者のクラウド環境等にアクセス（以下、「利用認証」という。）し、その後、鍵認可を行ってeシールを行う必要があると考えられる。

なお、リモート署名ガイドライン※のレベル2（電子署名法における認定認証業務と同等の信頼性を想定）においては、サービス提供を受けるための利用認証と秘密鍵（署名鍵）を利用するための鍵認可を分けて行い、かつ鍵認可は複数要素認証を行うことを要求している。

また、EUの適格eシール（リモート方式）においては、リモート署名ガイドラインのレベル2の要件に加えて、鍵認可はISO/IEC 15408（コモンクライテリア）の認証（プロテクションプロファイル：EN 419 221-5）を取得した署名活性化モジュールにて行うことを要求している。

他方、電子署名は意思表示であり、我が国でもEUでも推定規定があるのに対し、eシールは発行元証明にとどまり、我が国では現状は推定規定もないことに鑑みて、レベル3のリモートeシールを行う際には、利用認証と鍵認可（単要素認証でも可）を別に求めることで十分だと考えられる。

【参考】議論であがった主な意見（抜粋）

- レベル3のリモートeシールにおいて、組織によっては鍵認可の際は複数要素認証であったとしても単純な認証だけでは認められないことも考えられ、よりレベルの高いもの（例えばVPNを使ったシステム間連携等）を要求する可能性もある。

⑥　その他（リモート方式）

検討事項

- レベル3のリモートeシールにおいて、eシールを行う際の鍵認可で使用する知識要素（PINコード等）等の認証要素の管理はどうあるべきか。
  - 利用者のみが管理することを求めるか。
  - リモートeシールサービス提供事業者やアプリケーション提供事業者が管理することも認めるか。

方向性

- **認証要素の管理は基本的には利用者が行う**こととし、eシールとしての用をなさないレベル3のeシールの生成、流通を防止するため、**レベル3のeシールをリモートで行う事業者（リモートeシールサービス提供事業者）のサービスについては、一定の基準（認証要素は利用者本人が管理すること等）を設ける**ことが適切。

リモートeシールにおいて、仮に利用者の秘密鍵を管理しているリモートeシールサービス提供事業者が認証要素も管理して、利用者に断りなくeシールを行うことができる可能性がある場合は、そもそも認証要素としての意義が失われ、eシールを行った利用者、すなわち発行元が誰であるかの判断ができなくなる可能性が想定され、基本的には認証要素は利用者のみが管理することが望ましいと考えられる。

加えて、eシールの場合には、eシールが行われたデータを受け取る者（例えば領収書の受領者）には、リモートeシールサービスの利用について協議を受けられない蓋然性が高い（電子署名の場合には、文書の名義人間で、どのような方式を取るかの合意があるため、リモート署名サービスの利用について、双方の合意があるとみなす余地がある）。

このため、仮にレベル3のリモートeシールにおいて、eシールを行う際の鍵認可で使用する認証要素の管理が適切に行われない可能性がある場合には、信頼性が損なわれたレベル3のeシールが存在・流通してしまうことが想定され、制度の安定性そのものに影響を与えかねないと考えられる。

なお、EUにおいては、認証要素の管理は法人に委ねられ、アプリケーション提供事業者が管理することも否定はされていない一方、リモート署名ガイドラインにおいては、利用者本人のみが秘密鍵（署名鍵）を活性化（鍵認可）できることを要求している。

これらを勘案し、認証要素の管理は基本的には利用者が行うこととし、eシールとしての用をなさないレベル3のeシールの生成、流通を防止するため、レベル3のeシールをリモートで行うする事業者（リモートeシールサービス提供事業者）のサービスについては、一定の基準（例えば認証要素の管理は不可とする等）が必要になると考えられる。なお、当然認証要素をアプリケーション提供事業者が管理することは望ましくない。

【参考】議論であがった主な意見（抜粋）

- リモートeシールサービス提供事業者に関しては、一定の基準が必要ではないか。

⑥ その他（失効に係る事項）

検討事項

- 利用者において、eシール用電子証明書の失効要求ができる者の範囲はどこまでとすることが適切か。
  - eシール用電子証明書の発行を求めることができる者に限定する。
  - 上記に加えて、当該eシールを行う権限を有する者でも可とする。
  - 当該eシール用電子証明書の発行を受けた組織等に属する者であれば誰でも可とする。

方向性

- 失効要求できる者は電子証明書の発行を要求できる者（法人であれば代表者又は代表者から委任を受けた者）に限定することが適切。

電子証明書と自然人の紐付けが1対1である電子署名とは異なり、eシールは1つのeシール用電子証明書を組織等の中の複数人が使用することが想定されるため、当該eシール用電子証明書の失効を要求できる者の範囲をどこまでとするかについて検討が必要となる。

その範囲については、①eシール用電子証明書の発行を求めることができる者に限定するか、②それに加えて当該eシールを行う権限を有する者でも可とするか、③当該eシール用電子証明書の発行を受けた組織等に属する者であれば誰でも可とするか、が主な選択肢としてあげられるが、失効要求は、eシール用電子証明書の発行申請と同様に意思表示が必要であると考えられることから、失効要求できる者は電子証明書の発行を要求できる者（法人であれば代表者又は代表者から委任を受けた者）に限定することが適切だと考えられる。

【参考】議論であがった主な意見（抜粋）

- 失効要求ができる者は、基本的には代表者もしくは委任を受けた者といった制限をかけるのがよいのではないか。

資料１２

NISHIMURA & ASAHI

デジタル庁　第2回トラストを確保したDX推進SWGプレゼン資料

電子契約の有効性について

2021年12月13日（月）

西村あさひ法律事務所
弁護士・ニューヨーク州弁護士
太田　洋

NISHIMURA & ASAHI

I Executive Summary

（書面契約と異なった）電子契約の特殊性

NISHIMURA & ASAHI

- データ時代には、認証と改ざん防止が重要
  - なりすましが容易
  - 改ざんが容易

⇒ 電子契約の有効性・内容の正確性に脆弱性

- DXには、データへの信頼（トラスト）が確保されていることが大前提
- 電子契約への信頼

① 本人性確認

- 電子契約の現実の作成者と表示されている作成者の同一性が確認されていること

② 完全性確認

- 電子契約のデータが改ざんされていないことが確認されていること

電子契約の有効性を考える上での前提

NISHIMURA & ASAHI

- 電子契約についての一般的な法的定義はない
  - ⇒ ここでは仮に「書面ではなく、電磁的記録のみによって締結される契約」としておく
  - ⇒ 電子署名を用いなくとも、電子契約は成立し得る（ex. eメールのやりとりやLINEでのチャットのやりとりでも「電子契約」は成立し得る）

- 電子契約にはレベルがある
  - 口頭合意による契約に相当するもの ≒ eメールのやりとり/LINEのトークでのやりとり
    - ⇒ 裁判所に「最終的」かつ「確定的」な合意ではない（それ故、法的拘束力がない）と判断されるリスク
    - ⇒ サイン頁をPDF化してメールで交換する実務があるが、当該実務は自署された書面契約が存在することを前提
  - 三文判の印影が顕出されているだけの書面契約に相当するもの ≒ 3条署名が付された電子契約 ≒ ①当事者署名型で、（特定認証等のない）2条署名が付され、秘密鍵が適正に管理された電子契約/②事業者署名型のうち当事者指示型で、2要素認証等が確保され、2条署名が付された電子契約
    - ⇒ 三文判が顕出されているだけの書面契約でも、「二段の推定」は効く（最高裁判決が存在）
  - 認印・銀行（手彫り）の印影が顕出された書面契約に相当するもの ≒ ①当事者署名型で、特定認証された2条署名が付され、秘密鍵が適正に管理された電子契約/②事業者署名型のうち当事者指示型で、2要素認証等が確保され、2条署名が付された電子契約
  - 実印（印鑑証明付き）の印影が顕出された書面契約に相当するもの ≒ 当事者署名型で認定認証（準ずるものを含む）された2条署名が付され、秘密鍵が適正に管理された電子契約

電子契約が裁判上「証拠」となるために何が必要か

NISHIMURA ASAHI

- （書面の）文書を証拠とするためには、「文書の成立が真正」であることを証明しなければならない（民訴法228条1項）
  - ＝ 文書を証拠として提出する者が、当該文書の作成者であると主張している者（作成名義人）の意思に基づいて作成されたこと
  - ＝ 作成名義人の印影がその者の印章と一致⇒当該印影は作成名義人の意思に基づくものと事実上推定（判例）【第1段の推定】⇒文書の成立の真正が法律上推定（民訴228Ⅳ）【第2段の推定】
- 電子文書を証拠とするためにもその「電子文書の成立が真正」であることを証明する必要
  - ※ 3条推定効：その電子文書が真正に成立したものと推定する効果
  - ＝ 電子文書を証拠として提出する者が、当該文書・契約の作成者であると主張している者（作成名義人）の意思に基づいて作成されたこと
  - ＝ 作成名義人の電子署名がその者の秘密鍵によって生成されたことが検証⇒当該電子署名は作成名義人の意思に基づくものと事実上推定（実務法曹の多数説）【第1段の推定】⇒電子文書の成立の真正が法律上推定（電子署名法3条）【第2段の推定】
  - ※ 3条Q&Aは、事業者署名型のうち当事者指示型（⇒これで2条署名には該当）のものでなされた電子署名が、作成名義人の秘密鍵によって生成されたものと検証されるために必要な条件は、「他人がなりすますことができないという『固有性』を有すると評価できること」であることを明らかにしたもの
  - ⇒ もっとも、3条Q&Aがカバーしているのは「当人認証」までであり、電子契約プラットフォームを利用した者＝作成名義人であること（身元確認）は別途確認・確保される必要あるが、これは内部統制の問題
- 「文書の成立の真正」の証明方法
  - ⇒ もっとも、上記の民訴228条4項・電子署名法3条の推定規定のルートを経由しなくとも、「（電子）文書の成立の真正」を（他の証拠により）直接立証することは常に可能

わが国における電子契約を巡る法的環境整備

NISHIMURA & ASAHI

クラウド型電子署名プラットフォームの利用を含め、電子契約の普及についての法的環境整備はほぼ完了

⇒ ①2020年7月17日付け総務省＝法務省＝経済産業省「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ&A」（「2条1項Q&A」）及び②2020年9月4日付け総務省＝法務省＝経済産業省「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ＆A（電子署名法第3条関係）」（「3条Q&A」）により制度整備は完了

⇒ 後は、個々の事業者が自己の責任において、利用するクラウド型電子署名プラットフォームが、上記の2条1項Q&A及び3条Q&Aの要件を満たしているかを（適宜弁護士等も活用しながら）セルフ・チェックして、用途に応じた適切なサービスを取捨選択して利用していくべきステージ

用途に応じて適切なフォーマットの電子契約を選択することが重要

- 本人性確認と完全性確認は、リスクと利便性を考慮して、適切なレベルに設定することが重要
- いずれの電子署名を利用して電子契約を締結するかは、安全性、コスト、利便性を勘案して判断すべき

⇒ 見積書、注文書、請書のような取引基本契約を前提とした個別契約や、NDAのような定型的契約は、通常は、事業者署名型のうち当事者指示型の3条署名を利用すれば十分であろう。見積書、注文書、請書等の一方当事者の意思表示を示すものについては（3条推定効によらず文書の成立の真正は直接立証する前提で）「電子印鑑」（2条署名には該当する前提のもの）サービスを利用することもあり得る

⇒ 取引基本契約等の重要な契約や、M&Aに関する契約については、件数も限られていると考えられ、事業者にとっての重要性も高いので、自署された書面契約（の存在を前提にサイン頁をPDF化してメールで交換して成立を確認する実務）を用いたり、当事者署名型で認定認証（準ずるものを含む）された2条署名（秘密鍵は適正に管理する前提⇒3条署名に該当）を付した電子契約を用いることが、今後も多いものと思われる

NISHIMURA & ASAHI

II Reference

電子契約・電子文書に関する近時の政府見解

NISHIMURA & ASAHI

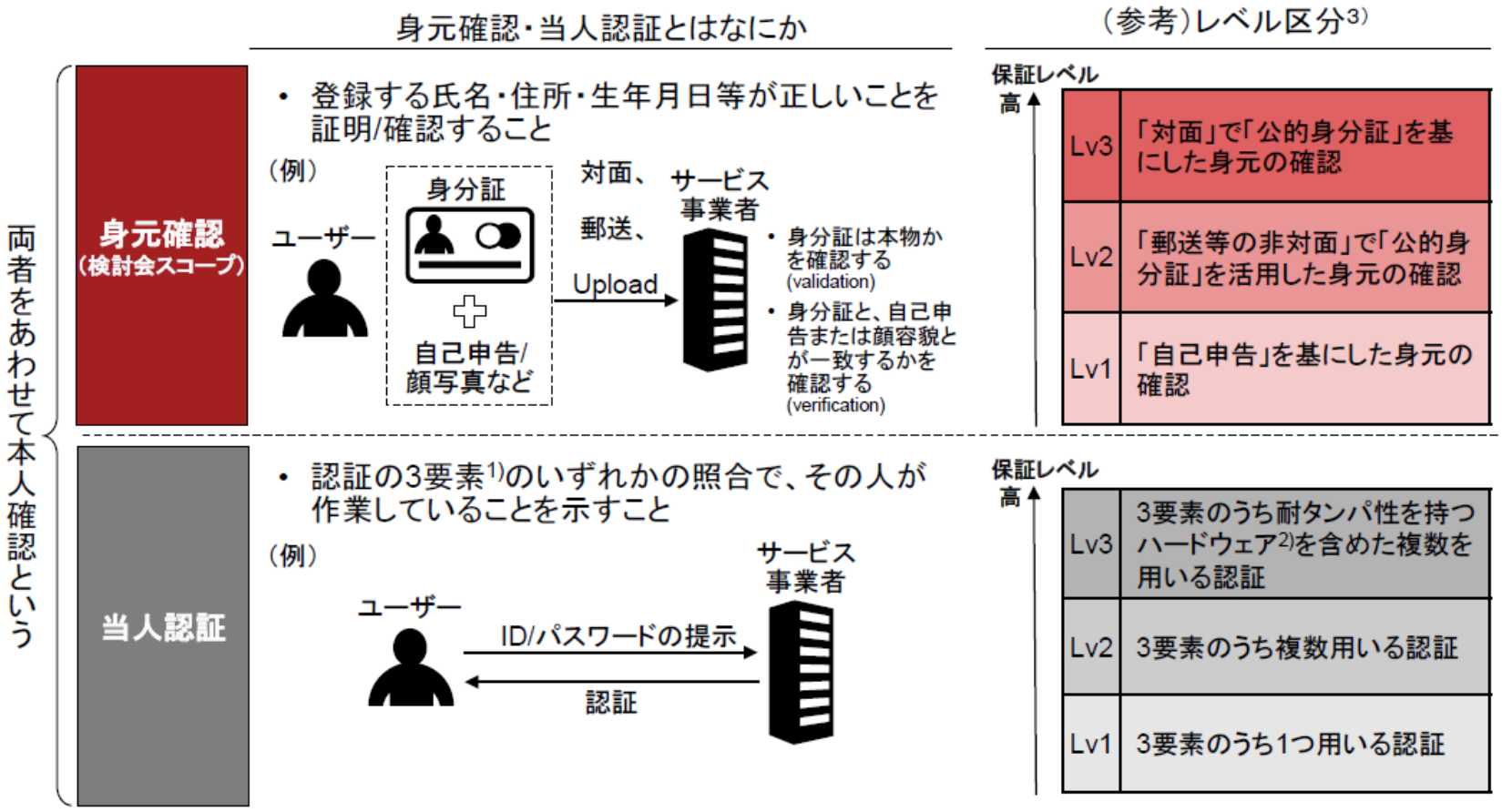
- 第10回成長戦略ワーキング・グループ資料1-2「論点に対する回答」(法務省、総務省、経済産業省提出資料)（2020年5月12日）（「3省論点回答」という）
- 第10回成長戦略ワーキング・グループ資料2-1「論点に対する回答」（2020年5月12日）(法務省提出資料)
- 内閣府＝法務省＝経済産業省「押印についてのQ&A」（2020年6月19日）（「押印Q&A」という）
- 規制改革推進会議「規制改革推進に関する答申」（2020年7月2日）16頁以降
- 総務省＝法務省＝経済産業省「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ&A」（2020年7月17日）（「2条1項Q&A」）
- 総務省＝法務省＝経済産業省「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ＆A（電子署名法第3条関係）」（2020年9月4日）（「3条Q&A」）

本人確認とは

NISHIMURA & ASAHI

1.「身元確認」の「当人認証」との区別

「身元確認」は、ユーザー当人の実在性を確認し、「当人認証」は、ユーザーの行為を確認する。通常両方の組み合わせを通じて「本人確認」が行われている。

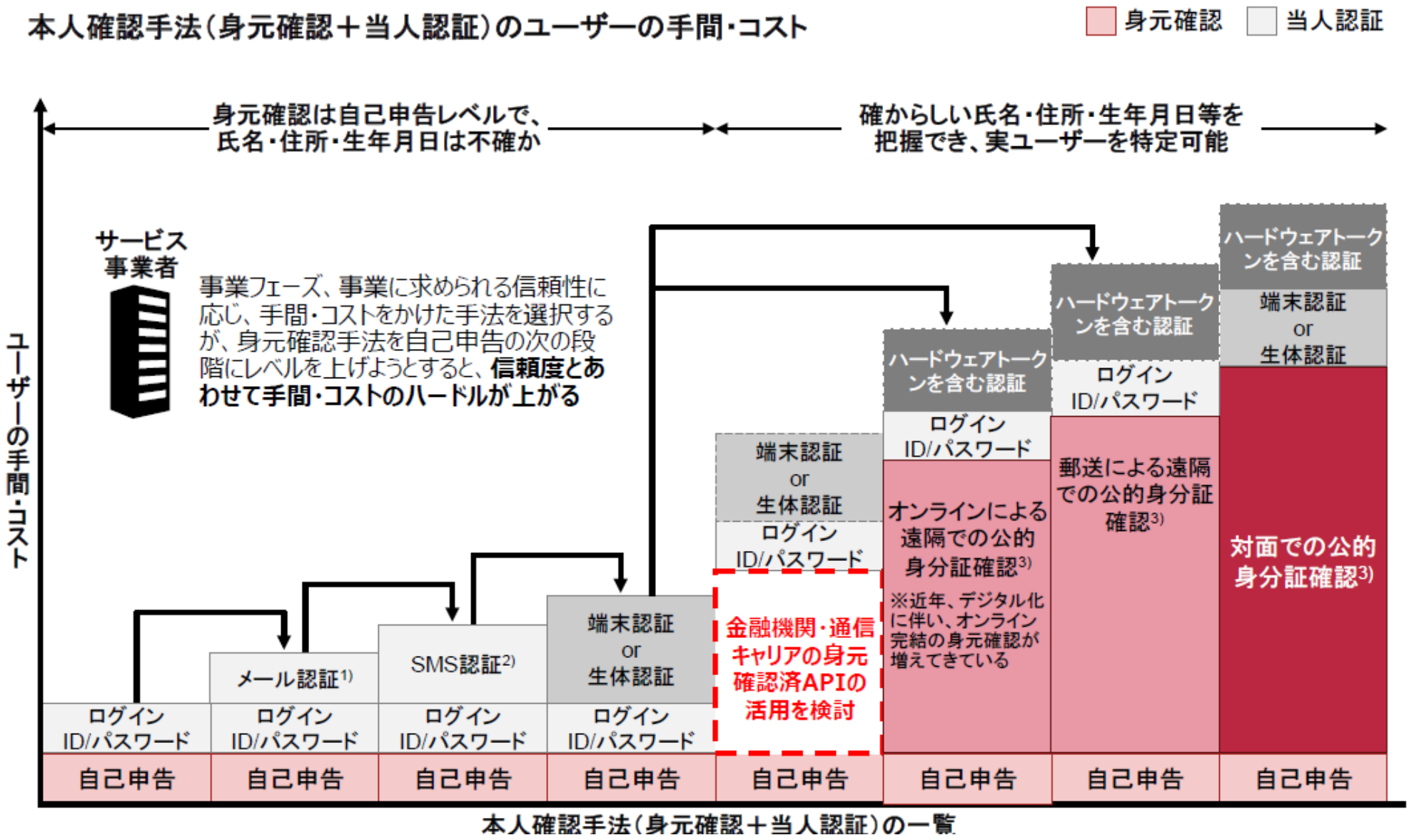


1)認証要素は「生体」（顔・指紋など）・「所持」（マイナンバーカードなど）・「知識」（パスワードなど）に分かれる
2)マイナンバーカードなど、内部の情報に対する不正な読み出しが困難である物理装置
3)「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（2019年2月CIO連絡会議決定）のレベル区分

出典：経済産業省他「オンラインサービスにおける身元確認手法の整理に関する検討報告書」

本人確認とは

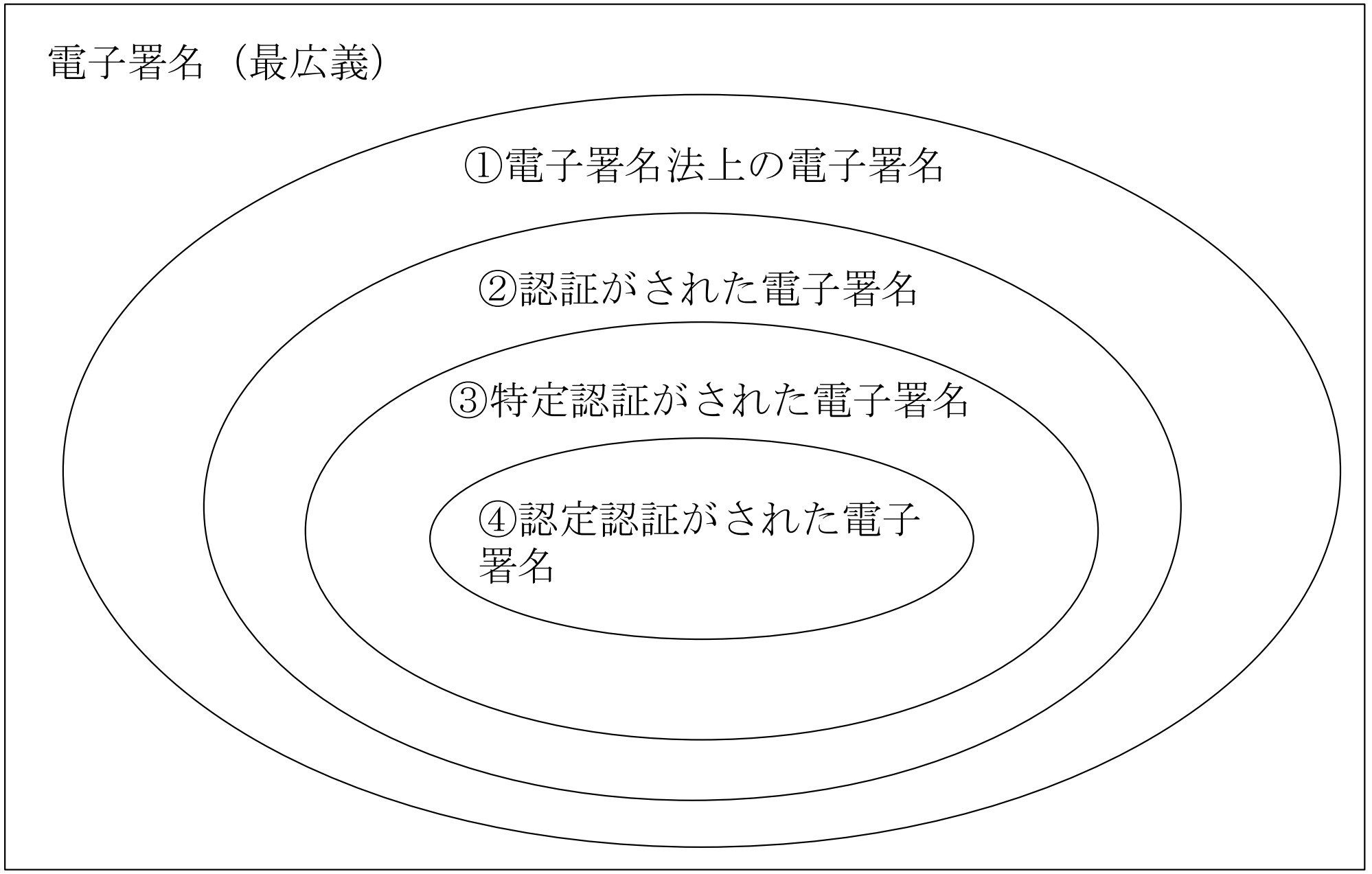
NISHIMURA & ASAHI



出典：経済産業省他「オンラインサービスにおける身元確認手法の整理に関する検討報告書」

電子署名の種類

NISHIMURA & ASAHI



出典：高林淳＝商事法務編『電子契約導入ハンドブック〔国内契約編〕』（商事法務、2020）102頁

電子署名法上の電子署名(2条署名)

NISHIMURA & ASAHI

電子署名

電磁的記録に記録することができる情報について、以下の要件を満たした「措置」

① 電磁記録に記録された情報が、当該措置を行った者の作成に係るものであることを示すためのものであること（本人性）

② 電磁記録に記録された情報について改変が行われていないかどうかを確認することができるものであること（非改ざん性）

- 身元確認は必要とされていない
- 当人認証は必要とされていない
- 印鑑でいうと三文判を含む

認証された電子署名

NISHIMURA & ASAHI

■ 認証業務

認証業務を行う者が、利用者が電子署名を行ったものであることを確認するために用いられる事項（公開鍵暗号方式では検証に用いる公開鍵）が当該利用者に係るものであることを証明する業務（電子署名法2条2項）

⇒ 電子証明書の発行（通常）

- 当人認証は必要とされている
- 身元確認は必要とされていない
- 認証業務は第三者である必要は無い
- 認証業務に資格は不要

特定認証された電子署名

NISHIMURA & ASAHI

- 特定認証業務

  電子署名のうち、その方式に応じて本人だけが行なうことができるものとして、電子署名法施行規則2条に定める基準に適合する電子署名について行なわれる認証業務（電子署名法2条3項）

- 電子署名法施行規則2条に定める基準

  電子署名の安全性が以下のいずれかの有する困難性に基づくもの

  ①ほぼ同じ大きさの二つの素数の積である2048ビット以上の整数の素因数分解

  ②大きさ2048ビット以上の有限体の乗法群における離散対数の計算

  ③楕円曲線上の点がなす大きさ224ビット以上の群における離散対数の計算

  ④前三号に掲げるものに相当する困難性を有するものとして主務大臣が認めるもの

  ← 認証業務と同じ＋暗号が解読困難

  手彫りの印鑑と類似

認定認証された電子署名

NISHIMURA & ASAHI

- 認定認証事業者

  主務大臣が、設備・本人確認の方法・業務体制等が一定の認定基準を満たしている特定認証業務を行なう事業者について、認定をする制度によって認定された事業者（電子署名法4条）

- 認定認証事業者は、公的身分証等による身元確認を行なうことが求められる（電子署名法6条1項2号、電子署名規則5条）

- 認定をうけた認証事業者は、電子証明書等に認定を受けていることを表示することができる（電子署名法13条）

・ 印鑑だと、実印＋印鑑証明書と類似

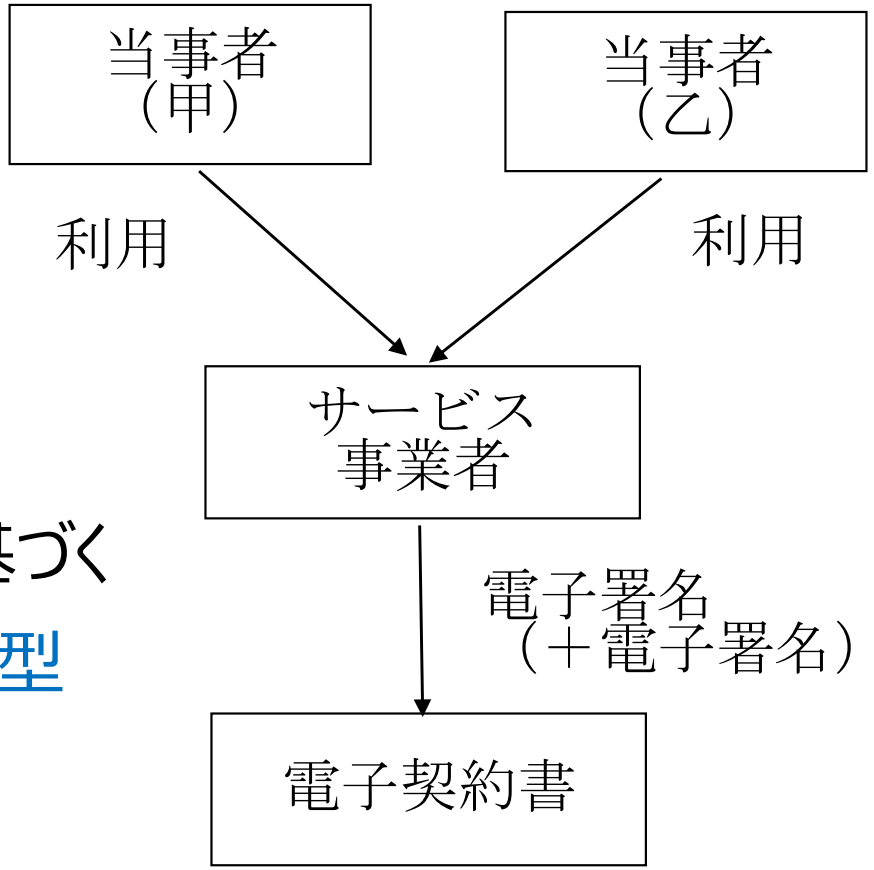
事業者署名型(立会人型)の電子署名とは

NISHIMURA & ASAHI

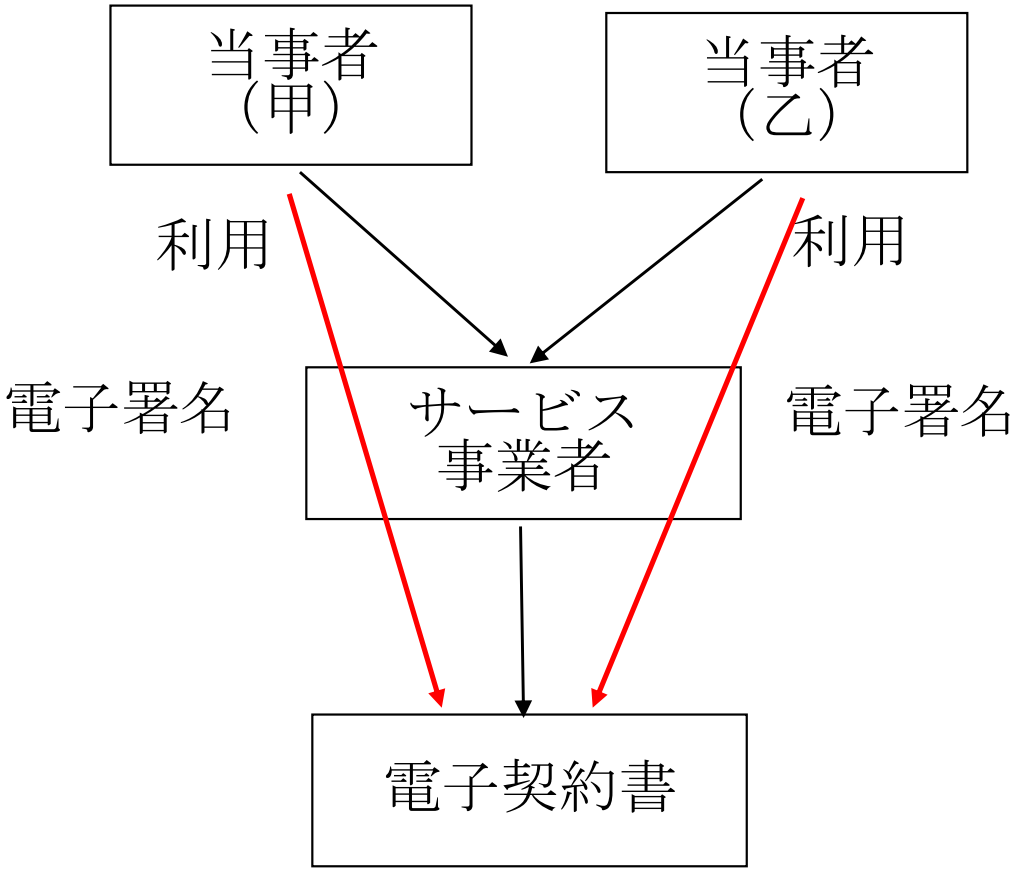
- サービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービス

- 様々な名称
  - 立会人型
  - 事業者署名型
  - クラウド型

⇒ このうち利用者の指示に基づくものが次頁の当事者指示型



当事者指示型の電子契約プラットフォームを利用した電子契約



仕組みの面からの電子署名の分類

NISHIMURA & ASAHI

- 基本形としての当事者型と事業者型（立会人型）
  - 当事者が自分が保有・管理する電子署名(署名鍵＝秘密鍵)を自ら付すのが当事者型
  - 当事者が利用するクラウド型サービス提供事業者が、当該事業者の電子署名(署名鍵＝秘密鍵)を付すのが事業者型（立会人型）

- 当事者型と事業者型（立会人型）それぞれの変形版
  - 事業者型（立会人型）のうち、事業者が、当事者の指示を受けて当該事業者の電子署名(署名鍵＝秘密鍵)を付すのが当事者指示型
  - 当事者が、認証局を運営するクラウド型サービス提供事業者から認証を受けた自らの電子署名(署名鍵＝秘密鍵)を、当該事業者にクラウド上で管理して貰い、必要な場合に当該事業者のプラットフォームを利用して、リモートで当該電子署名を自ら付すタイプ（クラウド利用当事者型）も存在

リモート署名の電子署名(2条署名)該当性

NISHIMURA & ASAHI

- サービス事業者による電子署名（リモート署名による電子署名）が、当事者による電子署名といえるか？

  ⇒ 2条1項Q＆A

  利用者が作成した電子文書について、サービス提供 事業者自身の署名鍵により暗号化を行う…サービスであっても、技術的・機能的に見て、サービス提供事業者の意思が介在する余地がなく、利用者の意思のみに基づいて機械的に暗号化されたものであることが担保されていると認められる場合であれば、『当該措置を行った者』はサービス提供事業者ではなく、その利用者であると評価し得る

2条1項Q＆A

NISHIMURA & ASAHI

- 「電子署名法第2条第1項第1号の『当該措置を行った者』に該当するためには、必ずしも物理的に当該措置を自ら行うことが必要となるわけではなく、例えば、物理的にはＡが当該措置を行った場合であっても、Ｂの意思のみに基づき、Ａの意思が介在することなく当該措置が行われたものと認められる場合であれば、『当該措置を行った者』はＢであると評価することができるものと考えられる。
- このため、利用者が作成した電子文書について、サービス提供 事業者自身の署名鍵により暗号化を行うこと等によって当該文書の成立の真正性及びその後の非改変性を担保しようとするサービスであっても、技術的・機能的に見て、サービス提供事業者の意思が介在する余地がなく、利用者の意思のみに基づいて機械的に暗号化されたものであることが担保されていると認められる場合であれば、『当該措置を行った者』はサービス提供事業者ではなく、その利用者であると評価し得るものと考えられる。
- そして、上記サービスにおいて、例えば、サービス提供事業者に対して電子文書の送信を行った利用者やその日時等の情報を付随情報として確認することができるものになっているなど、当該電子文書に付された当該情報を含めての全体を１つの措置と捉え直すことよって、電子文書について行われた当該措置が利用者の意思に基づいていることが明らかになる場合には、これらを全体として１つの措置と捉え直すことにより、『当該措置を行った者（＝当該利用者）の作成に係るものであることを示すためのものであること』という要件（電子署名法第２条第１項第１号）を満たすことになるものと考えられる。」

電子署名法3条

NISHIMURA & ASAHI

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（これを行うために必要な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。

①電子署名

②本人による

③これを行うために必要な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。

本人＝電磁的記録に記載された思想を表現した者

事業者署名型のうち当事者指示型を利用した署名の3条署名該当性

- 利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに3条推定効の適用はあるか？
  - ◆ 3条Q＆A

⇒ 当該サービスが十分な水準の固有性を満たしていること（固有性の要件）が必要

※ 〔利用者の指示に基づき、利用者が作成した電子文書について、サービス提供事業者自身の署名鍵による暗号化等を行う電子契約サービス〕が電子署名法第３条に規定する電子署名に該当するには、更に、当該サービスが本人でなければ行うことができないものでなければならないこととされている。そして、この要件を満たすためには、問１のとおり、同条に規定する電子署名の要件が加重されている趣旨に照らし、当該サービスが十分な水準の固有性を満たしていること（固有性の要件）が必要であると考えられる

固有性の要件とは？(1)

NISHIMURA & ASAHI

- 固有性の要件

⇒ 暗号化等の措置を行うための符号について、他人が容易に同一のものを作成することができないと認められること

⇒ そのためには、当該電子署名について相応の技術的水準が要求されることに

※ 電子署名法第３条に規定する電子署名について同法第２条に規定する電子署名よりもさらにその要件を加重しているのは、同法第３条が電子文書の成立の真正を推定するという効果を生じさせるものだからである。すなわち、このような効果を生じさせるためには、その前提として、暗号化等の措置を行うための符号について、他人が容易に同一のものを作成することができないと認められることが必要であり（以下では、この要件のことを「固有性の要件」などという。）、そのためには、当該電子署名について相応の技術的水準が要求されることになるものと考えられる。したがって、電子署名のうち、例えば、十分な暗号強度を有し他人が容易に同一の鍵を作成できないものである場合には、同条の推定規定が適用されることとなる

固有性の要件とは？(2)

NISHIMURA & ASAHI

- 固有性の具体例

①利用者とサービス提供事業者の間で行われるプロセス

②サービス提供事業者内部で行われるプロセス

⇒いずれにおいても十分な水準の固有性

◆プロセス①：利用者が２要素による認証を受けなければ措置を行うことができない仕組みが備わっているような場合

◆プロセス②：暗号の強度や利用者毎の個別性を担保する仕組み例：システム処理が当該利用者に紐付いて適切に行われること

電子署名法3条の推定効の意義(1)

- 推定効の意味
  - 通説：証拠評価にかかる法則を法律上規定した法定証拠法則
    - 証明責任は相手方に転換されない
    - 相手方からの反証が可能
  - 文書の記載内容が、立証主題である事実の証明に寄与する程度（実質的証拠力）は別問題

電子署名法3条の推定効の意義(2)

NISHIMURA & ASAHI

- 推定効の意味

①立証責任の転換を定めた法律上の推定の規定ではなく、相手方からの反証が許される法定証拠法則に過ぎない

②文書の成立の真正を直接立証することも可能

③推定効が認められれても、文書の記載事項・内容が真実であることまでが保証されるものではない

⇒3条推定効は一定の意義を有するが、その機能・意味を過大評価しないことが必要

プレゼンター略歴等

NISHIMURA & ASAHI

太田　洋

Yo OTA

西村あさひ法律事務所
パートナー弁護士

Tel: 03-6250-6285(直通)
Fax: 03-6250-7200
y.ota@plus.nishimura.com

1991年　東京大学法学部卒、
93年　第一東京弁護士会弁護士登録、
2000年　ハーバード･ロー･スクール修了（LL.M）
01年　米国NY州弁護士登録
01年～02年　法務省民事局参事官室（商法改正担当）
03年1月　西村あさひ法律事務所パートナー
13年4月～16年3月　東京大学大学院法学政治学研究科教授

オンライン名刺

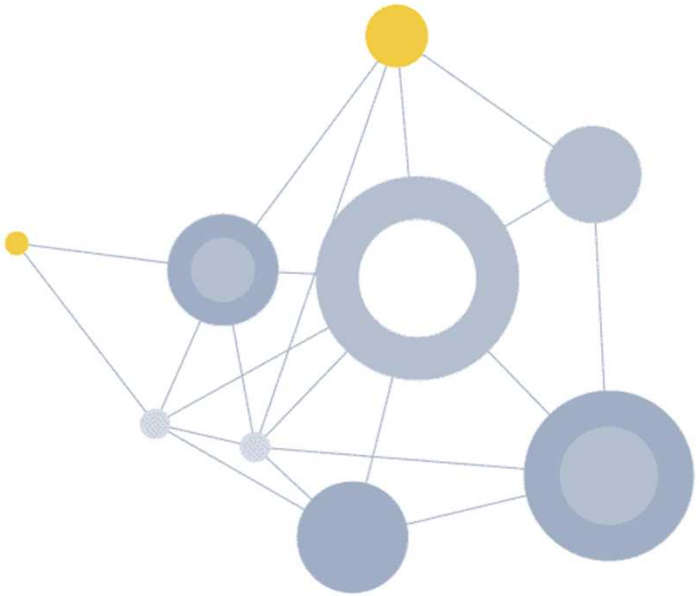
現在、**西村あさひ法律事務所　パートナー弁護士**
（株）リコー社外監査役、日本化薬（株）社外取締役、（公財）ロッテ評議員、日本取締役協会幹事、同協会コーポレート･ガバナンス委員会副委員長、経済産業省「デジタル経済下における国際課税研究会」委員、デジタル庁「トラストを確保したDX推進サブWG」構成員

主な著書等

『バーチャル株主総会の法的論点と実務』（共編著、商事法務、2021）、『令和元年会社法改正と実務対応』（共編著、商事法務、2021）、『デジタルエコノミーと課税のフロンティア』（共編著、有斐閣、2020）、『社外取締役の教科書』（共著、中央経済社、2020）、『個人情報保護法制大全』（編著、商事法務、2020）、『M&A･企業組織再編のスキームと税務〔第4版〕』（編著、大蔵財務協会、2019）、『M&A法大全（上）（下）〔全訂版〕』（編著、商事法務、2019）、『社債ハンドブック』（共編著、商事法務、2018）、『新株予約権ハンドブック〔第4版〕』（共編著、商事法務、2018）、『種類株式ハンドブック』（共編著、商事法務、2017）、『経済刑法』（共著、商事法務、2017）、『会社法実務相談』（共編著、商事法務、2016）、『企業取引と税務否認の実務』（大蔵財務協会、2015）、『クロスボーダー取引課税のフロンティア』（共編著、有斐閣、2014）、『タックス･ヘイブン対策税制のフロンティア』（共編著、有斐閣、2013）、『移転価格税制のフロンティア』（共編著、有斐閣、2011）、『新しい持株会設立･運営の実務』（共編著、商事法務、2011）、『M&A法務の最先端』（共編著、商事法務、2010）ほか多数

資料１３

トラストサービスのユースケース及び制約となる制度について



第５回トラストを確保したDX推進サブワーキンググループ
2022年2月8日（火）

Global Legal Entity Identifier Foundation (GLEIF)
Managing Director, 日本代表
中武　浩史

Agenda

1. トラストサービスのユースケース、他の政策との関係上想定されるニーズ
2. ユースケース実現に対する商慣習等の制約、課題
3. ユースケース実現の制約となる法令・制度関係
4. 制度・手続改革のポイント：「原本性」「真正性」
5. 「原本性」「真正性」の担保で電子化が促進されるエリア
6. 制度化による効果のまとめ

1. トラストサービスのユースケース、他の政策との関係上想定されるニーズ

- 総務省において、トラストサービスのユースケースと制約事項につき提案募集を実施（令和2年）
- 広範なユースケースが提案された他、慣習・制度含めた制約事項について整理された
- トラストサービスは、将来的なものも含め、他の政策との関係上も必要となる備え

トラストサービスのユースケース

○ 見積もりから請求・支払プロセスまでの**経理関係業務**や**契約関係の書類**（契約書、保険申込書、電子製造指示書、電子設計変更指示書等）等**企業内外のデータのやり取り**に関する業務において、**データの信頼性確保や業務効率化**の観点から、**eシールの使用ニーズが大きい**。

○ 企業が消費者や投資家等外部の関係者に向けて**組織が公開する情報**（アニュアルレポート、決算短信、ニュースリリース等）や**組織が発出する証明書**（保険会社、士業団体、教育機関、企業等が自社顧客・関係者に対し契約内容、資格、学歴・受講歴、所属状況等を証明するために発行する書面（**保険証券、資格証明書、卒業証明書、修了証書、在職証明書等**））に発行元の証明とデータの改ざん防止のため、**eシールを付与すべき**とのニーズが大きい。

○ **監査手続**における納品書・受領書・請求書等の外部証跡の入手・確認や**行政と民間との証明書・報告書等のやり取り**に関し、現在政府を挙げて取り組んでいる書面規制、押印、対面規制の見直しの流れを踏まえつつ、**ユースケースについて更なる深掘り**の余地があるのではないか。

他の政策との関係上想定されるニーズ

- 行政サービスデジタル化
  - ✓ エストニアの例でもわかるとおり、各種行政・病院・民間サービス業者等複数の組織との連携が必要になり、サービスの信頼性担保の為にも、申請組織とのデータ授受の仕組みがないと安心して利用できない（個人に紐つく電子署名ではない）
- 決済サービス事業者等、各種認定事業者の市場への参入
  - ✓ 欧州の例でもある通り、市場の開放を行い、マーケットの活性化を促進する一方で、安心した事業者とのデータ流通の仕組みを備えることは前提として必須
- 国際的取引での活用
  - ✓ 貿易取引等国を跨ぐ民間取引における信頼性の担保（欧州、米国、中国等）

出典：総務省　令和２年７月３日　サイバーセキュリティ統括官室　トラストサービスのユースケースに関する提案募集の結果

2. ユースケース実現に対する商慣習等の制約、課題

- 慣習・制度含めた制約事項あり。特には制度上紙や書面交付を求めるものは依然存在
- 紙の制度廃止と同時に電子化の標準形もある程度示すことは必須

ユースケース実現の制約となる規制・制度・手続・慣習等

○既存のトラストサービスの制度については、**電子署名の使い勝手の改善**に関する意見や、**タイムスタンプの国際的な通用性**に関する意見があげられた。

○eシールについては、**制度整備が必要**といった意見や**電子証明書に記載する標準的事項を定める必要**があるといった意見、eシールの発行**申請時の組織の実在性確認の仕組みが必要**といった意見があげられた。

○**行政手続き**や**自治体との契約**が、印鑑や紙ベースでのやりとりとなっていることから、**電子化していくための制度整備**を求める意見があげられた。

○**企業間のやりとり**及び**企業内のプロセス（社内規定等）**において、**押印や書面交付を求めている**という**民間の商慣習**があげられた。

○トラストサービスの利便性を高めるために、企業間における**データ連携のためのデータ様式の標準化が必要**、**トラストサービスを自動付与・検証するシステム**（会計ソフト等）**側の工夫が必要**という意見があげられた。

商慣習等を電子化していく上での課題

- 現状でも電子証明書は公共・民間問わず文書や手続きによって利用されてはいるが、対象文書や手続によって利用できる電子証明書が統一されておらず明らかに非効率
- 過去文書含めた継続性の観点は民間を超えた標準化は必須。また、電子署名業者も様々であり、電子署名法に基づく認定制度がさらに有効に働く工夫も必要。
- 効率的かつ安全・安心にデータ流通が行える基盤作りが当WGの趣旨。利用されていないから制度が不要なのではなく、制度が整備されていないから利用されていない面あり

出典：総務省　令和２年７月３日　サイバーセキュリティ統括官室　トラストサービスのユースケースに関する提案募集の結果

3. ユースケース実現の制約となる法令・制度関係

- 紙媒体での作成・提出が義務、申請書への押印を求めるような法的制度等が存在
- 電子化を担保する制度、国際的やりとりでデータの真正性を担保する制度も必要

分類④　法令、制度関係

【既存の法制度に対する意見・要望】
・**民事訴訟法上訴状や準備書面は紙媒体での作成が義務**
・**民法の**債権譲渡の対抗要件である**『確定日付のある証書』にタイムスタンプが含まれないことが課題**
・**地方自治体と民間の電子契約**においては、実態的に**民間の電子契約サービスが使えなくなっている**（地方自治法施行規則、総務省関係法令に係る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施行規則）
・**公的機関の入札・契約に係る多数の手続き書類**について**印刷・製本・押印が求められる**
・**犯罪収益移転防止法**の規程により、**法人の印鑑証明や登記事項証明を提出が必要**
・会社登記の全登記類型について、取締役会議事録が取締役全員の実印押印でなく認められるよう電子署名に使用する電子証明書の要件が限定されないようにするなどの改正が必要（**商業登記法、商業登記規則**）
・法令上書面作成が要求されている契約がある（**定期建物賃貸借契約（借地借家法第38条）**等）

【新たな法制度等に向けた意見・要望】
・**公的証明書等**に関して**電子的に発行する制度が存在しない**
・**電子文書保管**に関する、**一定の効果を担保するような指針がない**
・**有価証券性のある貿易書類（船荷証券等）の電子化**を担保する**制度がない**
・国際的なやりとりにおいては、関係国の間で共通の法的スキームが求められ、**電子化された貿易書類に対して法人が電子署名**を行い、当該**電子データの真正性を担保する制度が必要**

【官民間のやりとりに関する意見】
・厳格な根拠法令はないが、**法人が自治体に対して各種証明書等の発行を申請**する際には、**申請書へ押印が求められている**
・**就労証明書や休業証明書の発行**が必要な制度において**紙媒体の提出が求められる**

出典：総務省　令和２年７月３日　サイバーセキュリティ統括官室　トラストサービスのユースケースに関する提案募集の結果

4. 制度・手続改革のポイント：「原本性」「真正性」

- 申請手順の中で契約書等の原本ないしその写の提出を求めている手続きが存在
- 有価証券のように唯一無二である必要はないが、「原本（ないし原契約）と同一である確認」が要件
- eシール活用で「原本性」と「真正性」の担保がなされ、真のデジタル化が促進される

（例）役務取引許可申請（外為令別表）、輸出許可申請（輸出令別表第一）
https://www.meti.go.jp/policy/anpo/kanri/sinsa-unyo/sinnseisyo-tenpsyorui-itiran/tenp24fy/tenpD6.html

「契約書等及びその写し 輸出者から最終需要者までの一連の契約書等及びその写しを提出すること。（注3）原本を提出する場合は当該原本の写しを併せて提出するものとし、原本を提出せずに写し を提出する場合は原本証明書（別記１（ナ））を併せて提出するものとする。なお、原本につ いては、内容確認の後、申請者に返却する。」

・原本契約書を一旦提出、もしくは写の場合は「原本証明書」を提出する必要
・海外との契約自体も電子化が進む中で、原本性と契約の真正性を確認する為に「紙」の提出が必要
・eシールを付与した契約を電子的に提出することで、紙はなくなり、真正性も担保される

同様に例えば「地方公共団体における書面規制、押印、対面規制の見直しについて」（総行行第１６９号総行経第３５号　令和２年７月７日）においても、見積書等、後日紙の原本を求めているものが複数存在。
https://www.soumu.go.jp/main_content/000749491.pdf

5. 「原本性」「真正性」の担保で電子化が促進されるエリア

- その他eシールにより電子化が促進され、紙の流通がなくせるエリアは多数存在
  ① 「原本性」「真正性」担保の観点で、証明書類発行の際等に原本提出を求めているケース
  ② そもそも大元の書類が紙である故に、紙で原本提出が必要なケース
  ③ 組織として正式に発行し、契約等内容の真正性担保が必要なもの

①の具体例
商工会議所が発行するインボイス証明発行に必要なインボイス
検査会社等が発行した書類を除き、書類上に「COPY」表記のあるものは認証不可
オリジナル（原本）のみが認証対象
→電子化された場合、原本は紙でなくなり真正性を電子的に担保するものが必要になる

②の具体例
通関電子化の中での税金関連書類（原本提出等要否判断のためのＮＡＣＣＳコード一覧）

③の具体例
保険契約、卒業証明書、資格証明書、在籍証明書等

6. 制度化による効果のまとめ

- 輸出入取引全般を見て、例に上げた輸出サイドのみならず、輸入で必要な契約書、輸入者の誓約書、輸入時のインボイス、授権証明書等eシールで真正性を担保することで全体の電子化が促進されるものが多数存在。
- 同様の動きにより、貿易取引の中で残存していた「紙」による非効率部分が解消し、広く産業全体に対して効率化される効果は大きい
- また、貿易取引の電子化が進展することで、マニュアルでの検証作業がシステム化され、近時アンチマネーロンダリング対策上課題とされ注目されている「トレードベースマネーロンダリング（Trade Based Money Laundering, TBML）をシステム的に検知する基盤が整備され、日本としてのAML対策上も有意義
- 貿易取引のみならず、原本提出を求められる分野はeシールで電子化が促進され、単独では効果が見えづらい各種提案されたトラストサービスのユースケースも、本件制度化の結果として効果を享受し、デジタル化社会推進の礎となる

資料１４

欧州eIDAS規則における アシュアランスレベル

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

2022年1月25日

慶應義塾大学SFC研究所

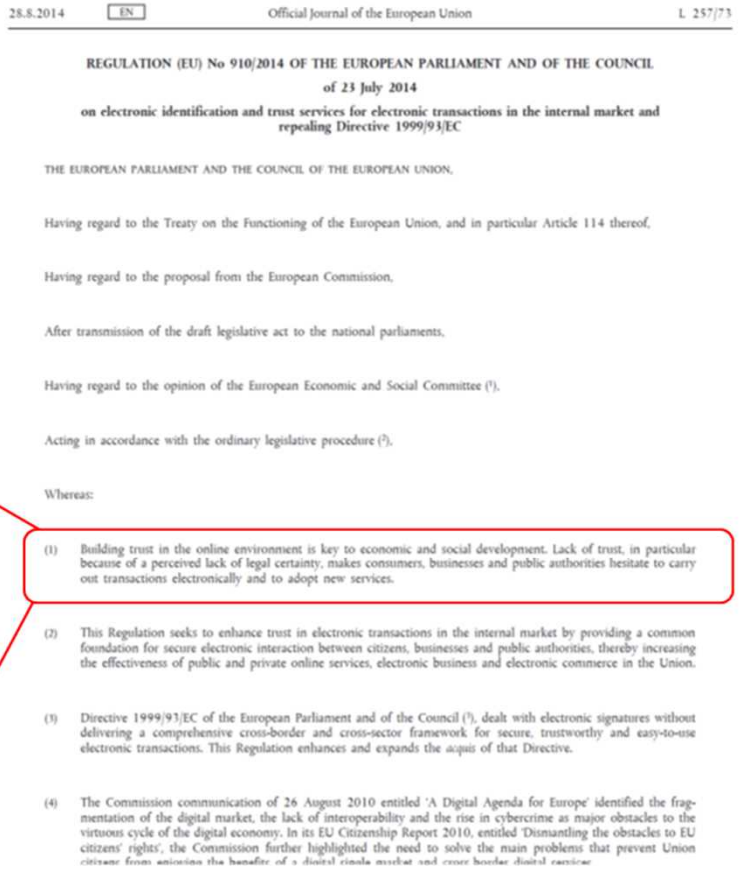
上席所員　濱口 総志

eIDAS(electronic Identification and Authentication Service)規則*

- eIDAS規則の2つの目的
  - 欧州DSM(Digital Single Market)戦略
  - トラストサービスの普及による経済発展の促進

Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.

（和訳）オンライン環境における信頼の構築は経済と社会の発展の鍵である。信頼の欠如、特に法的安定性の欠如が消費者、企業、公的機関に電子取引や新たなサービスの採用を躊躇させている。



28.8.2014 EN Official Journal of the European Union L 257/73

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.

(2) This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

(3) Directive 1999/93/EC of the European Parliament and of the Council (3), dealt with electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. This Regulation enhances and expands the *acquis* of that Directive.

(4) The Commission communication of 26 August 2010 entitled 'A Digital Agenda for Europe' identified the fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as major obstacles to the virtuous cycle of the digital economy. In its EU Citizenship Report 2010, entitled 'Dismantling the obstacles to EU citizens' rights', the Commission further highlighted the need to solve the main problems that prevent Union citizens from enjoying the benefits of a digital single market and cross-border digital services

*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=CELEX%3A32014R0910

eIDAS(electronic Identification and Authentication Service)規則*

- eIDの加盟国間相互承認フレームワーク
  ➡eIDのアシュアランスレベルについて3段階（low, substantial, High）を規定

- トラストサービスの法的効力を規定
  ➡2段階の法的効力
  ①トラストサービスは電子形式、適格トラストサービスでない理由で法的効力が否定されない
  ②適格トラストサービスは法的効力が推定される
  ➡トラストサービスの第三者評価フレームワーク
  適合性評価機関による評価と監督機関による適格ステータスの付与

*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=CELEX%3A32014R0910

eIDのアシュアランスレベル

Low, Substantial, Highの要件はCIR (EU)2015/1502*に規定されている。

eIDAS2.0におけるEUDIW(EU Digital Identity Wallet)は保証レベルHighとされている。

保証レベル	身元確認	eIDの機能	認証メカニズムの想定攻撃能力
Low	身元確認書類を所持していると見做すことができる	単要素認証	強化基本(Enhanced-Basic), EAL1～3
Substantial	身元確認書類の所持を確認及び、身元確認書類の有効性確認	二要素認証	中(moderate), EAL4
High	顔写真等の生体情報を含む身元確認書類の所持を確認及び、身元確認書類の有効性確認	二要素認証＋対タンパ性	高, EAL4+

CIR(EU)2015/1502*より抜粋

*COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

現在までの通知状況①

	Member State	Title of the scheme	eID means under the scheme	Level of assurance	Status	Date	OJEU
Austria	Austria	ID Austria		High	PRE-NOTIFIED	27 Sep 2021	
Belgium - eID	The Kingdom of Belgium	Belgian eID Scheme FAS / eCards	Belgian Citizen eCard Foreigner eCard	High	NOTIFIED	27 Dec 2018	2018/C 464/08
Belgium - Itsme	The Kingdom of Belgium	Belgian eID Scheme FAS / Itsme®	itsme® mobile App	High	NOTIFIED	18 Dec 2019	2019/C 425/06
Croatia	Republic of Croatia	National Identification and Authentication System (NIAS)	Personal Identity Card (eOI)	High	NOTIFIED	07 Nov 2018	2018/C 401/08
Czech Republic	Czech Republic	National identification scheme of the Czech Republic	CZ eID card	High	NOTIFIED	13 Sep 2019	2019/C 309/09
Czech Republic (Mobile eGovernment Key, mojeID)	Czech Republic	National identification scheme of the Czech Republic	Mobile eGovernment Key (MEG), mojeID	Low, Substantial, High	PRE-NOTIFIED	27 Sep 2021	
Denmark	Kingdom of Denmark	NemID	Key card (OTP) Mobile app Key token (OTP) NemID hardware Interactive Voice/Response (OTP) Magna key card (OTP)	Substantial	NOTIFIED	08 Apr 2020	2020/C 116/05
Estonia	Republic of Estonia	Estonian eID scheme: ID card Estonian eID scheme: RP card Estonian eID scheme: Digi-ID Estonian eID scheme: e-Residency Digi-ID Estonian eID scheme: Mobiil-ID Estonian eID scheme: diplomatic identity card	– ID card – RP card – Digi-ID – e-Residency Digi-ID – Mobiil-ID – Diplomatic identity card	High	NOTIFIED	07 Nov 2018	2018/C 401/08
France	French Republic	French eID scheme "FranceConnect+ / The Digital Identity La Poste"		Substantial	PEER REVIEWED	02 Feb 2021	
Germany	Federal Republic of Germany	German eID based on Extended Access Control	National Identity Card Electronic Residence Permit eID Card for Union Citizens and EEA Nationals	High	NOTIFIED	26 Sep 2017	2017/C 319/03 2020/C 432/07
Italy - eID	Republic of Italy	Italian eID based on National ID card (CIE)	Italian eID card (Carta di Identità elettronica)	High	NOTIFIED	13 Sep 2019	2019/C 309/09
Italy - SPID	Republic of Italy	SPID – Public System of Digital Identity	SPID eID means provided by: • Aruba PEC SpA • Namirial SpA • InfoCert SpA • In.Te.S.A. SpA • Poste Italiane SpA • Register.it SpA • Sielte SpA • Telecom Italia Trust Technologies S.r.l. • Lepida SpA	Low, Substantial, High	NOTIFIED	10 Sep 2018	2018/C 318/02 amended by 2018/C 344/09, 2019/C 309/09
Latvia	Latvia	Latvian eID scheme (eID)	eID karte eParaksts karte eParaksts karte+ eParaksts	Substantial, High	NOTIFIED	18 Dec 2019	2019/C 425/06
Lithuania	Republic of Lithuania	Lithuanian National Identity card (eID / ATK)	Lithuanian National Identity card	High	NOTIFIED	21 Aug	2020/C 276/02

現在までの通知状況②

			(eID / ATK)			2020	
Luxembourg	The Grand Duchy of Luxembourg	Luxembourg national identity card (eID card)	Luxembourg eID card	High	NOTIFIED	07 Nov 2018	2018/C 401/08
Malta	Malta	Identity Malta	Maltese eID card and e-residence documents	High	PEER REVIEWED	04 Mar 2021	
Norway	Norway	eID-gateway "ID-porten"	Buypass ID, BankID		PRE-NOTIFIED	27 Sep 2021	
Portugal - Cartão de Cidadão	The Portuguese Republic	Cartão de Cidadão	Portuguese national identity card (eID card)	High	NOTIFIED	28 Feb 2019	2019/C 75/04
Portugal - Chave Móvel Digital	The Portuguese Republic	Chave Móvel Digital	Digital Mobile Key	High	NOTIFIED	08 Apr 2020	2020/C 116/05
Portugal - Sistema de Certificação de Atributos Profissionais	The Portuguese Republic	Sistema de Certificação de Atributos Profissionais	Professional Attributes Certification System		PRE-NOTIFIED	30 May 2018	
Slovakia - eID Scheme	Slovak Republic	National identity scheme of the Slovak Republic	Slovak Citizen eCard Foreigner eCard	High	NOTIFIED	18 Dec 2019	2019/C 425/06
Spain	The Kingdom of Spain	Documento Nacional de Identidad electrónico (DNIe)	Spanish ID card (DNIe)	High	NOTIFIED	07 Nov 2018	2018/C 401/08
Sweden	The Kingdom of Sweden	Swedish eID (Svensk elegitimation)	BankID Freja eID	Substantial and High	PEER REVIEWED	14 Dec 2020	
The Netherlands (DigiD)	The Kingdom of the Netherlands	DigiD	DigiD Substantieel DigiD Hoog	Substantial, High	NOTIFIED	21 Aug 2020	2020/C 276/02
The Netherlands (DTF/eHerkenning)	The Kingdom of the Netherlands	Trust Framework for Electronic Identification (Afsprakenstelsel Elektronische Toegangsdiensten)	Means issued under eHerkenning (for businesses)	Substantial, High	NOTIFIED	13 Sep 2019	2019/C 309/09

トラストサービスの法的効力

項目	法的効力
電子文書（Art.46）	**電子文書は、その法的効力及び法的手続きにおける証拠としての能力を、それが電子形式であるという理由だけで否定されない。**
電子署名（Art.25）	1.電子署名は、それが電子形式である、又は適格電子署名の要件を満たさないという理由だけで、法的効力及び法的手続きにおける証拠としての能力を否定されない。 **2.適格電子署名は、手書き署名と同等の法的効力をもつこと。** 3.ある加盟国で発行された適格証明書に基づく適格電子署名は、他のすべての加盟国においても適格電子署名として認められる。
eシール（Art.35）	1.eシールは、その法的効力及び法的手続きにおける証拠としての能力を、それが電子形式である、又は適格eシールの要件を満たさないという理由だけで否定されない。 **2.適格eシールは、適格eシールがリンクするデータの完全性及びデータの起源の正確性を推定することができる。** 3.ある加盟国で発行された適格証明書に基づく適格eシールは、他の全ての加盟国で適格eシールとして認められる。
タイムスタンプ（Art.41）	1.タイムスタンプは、その法的効力及び法的手続きにおける証拠としての能力を、それが電子形式である、又は、適格タイムスタンプの要件を満たさないという理由だけで否定されない。 **2.適格タイムスタンプは、それが示す日時の正確性とその日時を結びつけたデータの完全性に関する推定を享有する。** 3.ある加盟国で発行された適格タイムスタンプは、他の全ての加盟国で適格タイムスタンプとして認められる。
eデリバリー（Art.43）	1.eデリバリーサービスを利用して送受信されたデータは、その法的効力及び法的手続きにおける証拠としての能力を、それが電子形式である、又は、適格eデリバリーサービスの要件を満たさないという理由だけで否定されない。 **2.適格eデリバリーサービスを利用して送受信されたデータは、データの完全性、識別された送信者によるデータの送信、識別された宛先者による受信、適格eデリバリーサービスで示されたデータの送受信の日時の正確性に関する推定を享有する。**

トラストサービス(電子署名)のレベル毎の技術基準、第三者評価フレームワーク

<table>
<tr><th rowspan="2">eIDAS規則における区別</th><th rowspan="2">法的効力</th><th colspan="3">技術基準</th><th rowspan="2">第三者評価のフレームワーク</th></tr>
<tr><th>電子署名種別</th><th>身元確認要件</th><th>秘密鍵の保護</th></tr>
<tr><td rowspan="6">適格トラストサービス

トラストサービス</td><td rowspan="6">推定される

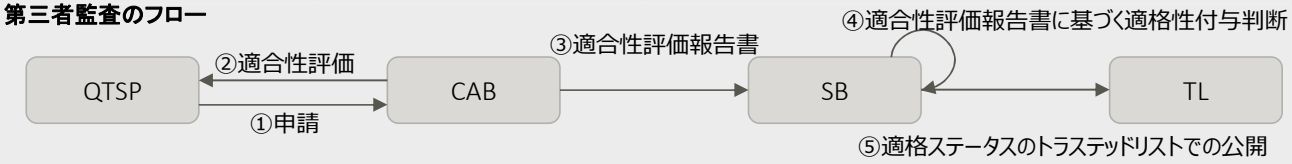
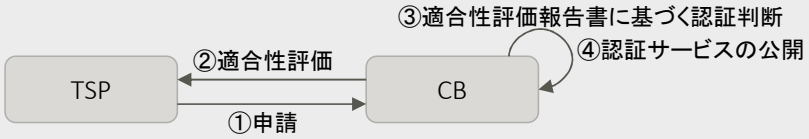
否定されない</td><td>適格電子署名、適格eシール（QCP-n-qscd, QCP-l-qscd）</td><td rowspan="2">F2F, eID(substantial以上)、適格証明書及び同等の方式</td><td>QSCD(Qualified Signature/Seal Creation Device)</td><td rowspan="2">eIDAS規則（適合性評価機関の評価結果に基づく監督機関による適格性の付与）</td></tr>
<tr><td>適格電子証明書に基づく先進電子署名(QCP-n, QCP-l)</td><td>利用者の環境で保護</td></tr>
<tr><td>先進電子署名(NCP+)</td><td rowspan="3">F2F及び同等の方式</td><td>SCD(Secure Crypto Device): ISO/IEC 15408 EAL4+ 或いは FIPS 140-2 level 3</td><td rowspan="3">任意の適合性評価或いは自己宣言</td></tr>
<tr><td>先進電子署名(NCP)</td><td rowspan="2">利用者の環境で保護</td></tr>
<tr><td>先進電子署名(LCP)</td><td>本人確認資料に基づく確認</td></tr>
<tr><td>その他の電子署名(PKI以外)</td><td>N/A</td><td>N/A</td><td>N/A</td></tr>
</table>

QCP: Qualified Certificate Policy　　LCP: Lightweight Certificate Policy
NCP: Normalized Certificate Policy　　F2F: Face to Face

技術基準：ETSI EN 319 401, 411-1, 411-2

総務省 組織が発行するデータの信頼性を確保する制度に関する検討会（第8回）富士通株式会社提出資料より

監査監督のフレームワーク

eシールのレベル	ポリシー	第三者監査	認証機関	監督機関	ステータスの公開方法	スキーム
適格eシール、適格証明書に基づく先進eシール	QCP-l, QCP-l-qscd	**CAB** eIDAS規則が定める適合性評価機関 (Conformity Assessment Body)	**SB** eIDAS規則が定める監督機関 (Supervisory Body)	**SB** eIDAS規則が定める監督機関 (Supervisory Body) 事前／事後監督	**TL** トラステッドリスト (Trusted List)	eIDAS規則
		第三者監査のフロー 				
先進eシール	LCP, NCP, NCP+	**CB** 認定機関から認定を受けた認証機関 （Certification Body）	**CB** 認定機関から認定を受けた認証機関 (Certification Body)	**SB** eIDAS規則が定める監督機関 (Supervisory Body) 事後監督*	認証機関のWeb	ETSI認証
		第三者監査のフロー 				

- QTSPはeIDAS規則で定められている適合性評価を受け、トラステッドリストで適格ステータスが公開される必要がある。
  QTSP：Qualified Trust Service Provider（適格トラストサービスプロバイダ）
- TSP(LCP, NCP, NCP+)にとって、第三者監査や認証は必須ではなく、先進eシールにも第三者監査や認証は必須ではない。
  一方で先進eシール、eシール共に監督機関による事後監督の対象とはなっている。

eIDAS2.0とNIS2(Network and Information Security Directive 2)

- NIS2においてトラストサービスプロバイダはデジタルインフラの一つとして位置付けられており、サイバーセキュリティリスク管理及びセキュリティ事故報告の義務を負うことが示されている。

  2021年11月26日付けの最新案*1では；
  ➡適格トラストサービスプロバイダは不可欠主体（Essential Entity）として事前、事後監督*2の対象
  ➡トラストサービスプロバイダは、中小企業*3であれば重要主体(Important Entity)として事後監督の対象となり、中小企業*の規模を超える場合は不可欠主体として適格トラストサービスプロバイダと同様に事前、事後監督の対象となっている。

*1 Interinstitutional File: 2020/0359(COD) Brussels, 26 November 2021 (OR. en) 14337/21
*2 事前監督: サービス開始前に要件の充足を確認　　事後監督：事故/違反発生時の立ち入り等
*3 COMMISSION RECOMMENDATION 2003/361/EC における中小企業(SME)の定義（従業員250名未満、売上50Mユーロ未満等）

適格トラストサービスが要求される領域

NIS2* (70bisaa)では「*特定のサイバーセキュリティリスク管理措置への準拠を証明するために、加盟国は不可欠主体及び重要主体に対して、eIDAS規則に基づく適格トラストサービスまたはeIDスキームの利用を要求することができる*」とされている。

Annex Iに記載されている不可欠主体及び重要主体

- エネルギー(電気、オイル、ガス、水素等)
- 輸送(航空、鉄道、海運、交通)
- 銀行
- 金融市場インフラ
- ヘルス
- 飲料水
- 下水
- デジタルインフラ
- ICTサービス管理
- 行政機関
- 宇宙

Annex IIに記載されている不可欠主体及び重要主体

- 郵便、クーリエ
- 廃棄物管理
- 化学
- 食品
- ヘルス
- 製造
- デジタルプロバイダ

* Interinstitutional File: 2020/0359(COD) Brussels, 26 November 2021 (OR. en) 14337/21

まとめ

- EUはeIDAS規則及びNIS2によって、デジタルインフラとしてトラストサービス及びeIDを整備し（ようとし）ている。
  - 制度化と技術基準、事前/事後監督
  - 行政機関及び規制産業における適格トラストサービスの利用を促進

- 一方で、B2B等において広く用いることができるレベルのトラストサービスについても、技術基準と民間第三者評価のフレームワークを整備されており、利用者が必要なトラストサービスを正しく選択できる環境を構築されている。

資料１５

eIDAS2.0とEUDIW

第７回 トラストを確保したDX推進サブワーキンググループ

2022年3月22日

慶應義塾大学SFC研究所

上席所員　濱口 総志

eIDAS規則の評価

参考資料

- Evaluation Report (2021年6月3日)
- Staff Working Document (2021年6月3日)
- Briefing from European Parliament (2022年3月7日)

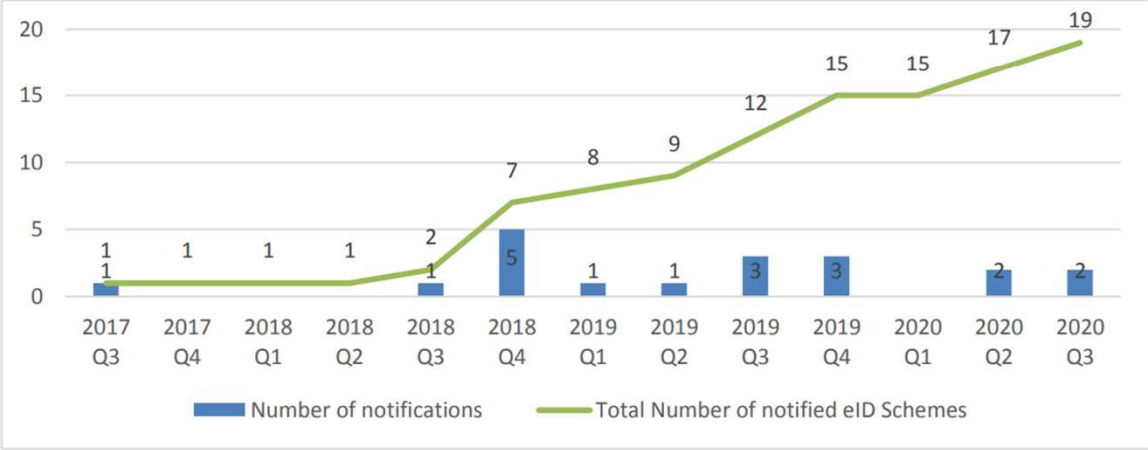
*1 COM(2021) 290 final “REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)”
*2 SWD(2021) 130 final “COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)”
*3 Revision of the eIDAS Regulation Findings on its implementation and application

Evaluation Report(評価報告書) 概要

評価項目	eID	トラストサービス
効果 (目的に対してどれ程効果が得られたか)	○相互承認を共通目的としたeIDスキームの加盟国間ネットワーク構築に寄与 ×相互承認可能なeIDスキームが限定的でEU市民の59% ×eIDASノードの限定的な稼働、国境を越えた認証時のエラー	○責任、立証責任、法的効果、トラストサービスの国際的側面に関する法的確実性を確立 ×利用率に加盟国間、トラストサービス種別間で差がある ×技術的中立性を重視した結果、加盟国間での解釈の違い等が生じた
効率性	△定量評価ではコストが利益を上回る（利益の定量化が困難）	△定量評価ではコストが利益を上回る（利益の定量化が困難） ＋TSPは市場拡大、DSMによる利益を享受
関連性 （ニーズ、課題等と目的の関連性）	×範囲が限定的すぎる（通知されたeIDスキームの公共サービスでの受け入れ）	×EUの多くのセクターの法律にeIDAS規則への言及があるにもかかわらず、eIDAS規則はまだ特定の分野（例：教育、銀行、旅行、航空）のニーズに応えられていない。 ×最新の技術動向に対応できていない
一貫性	○通知とピアレビューに基づくeIDの相互承認のための一般的に首尾一貫したシステム ×LoAを達成するための技術的要件に関する共通理解の不足 ×データ最小化の原則に対応できていない	○一貫した監督システムを提供 ×加盟国間で認められる本人確認方法に差がある ×適合性評価機関の義務、責任、能力に関する十分な説明がないこと
付加価値	○規則を廃止することは、eIDASに依存している他の立法分野への断片化と否定的な結果につながるだろう △規則の枠組みを一部修正することで、EUの付加価値を高めることができる（民間セクターによる信頼できる政府のeIDの使用を促進し、公共および民間セクターが提供する特定の属性やクレデンシャルを交換するための枠組みを定義することなど）。	○共通の法的枠組みを提供し、市場の断片化を減らし、その利用を増加させた ○トラストサービスを利用することで、行政はサービスの近代化・デジタル化を図り、証拠をデジタルで発行することができるため、行政の負担を軽減すること可能に ×各国の解釈や国内法の矛盾に起因する障壁がまだ残っており、トラストサービスの利用を制限している。

出典： COM(2021) 290 final “REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)”

eIDスキームに関する統計データ



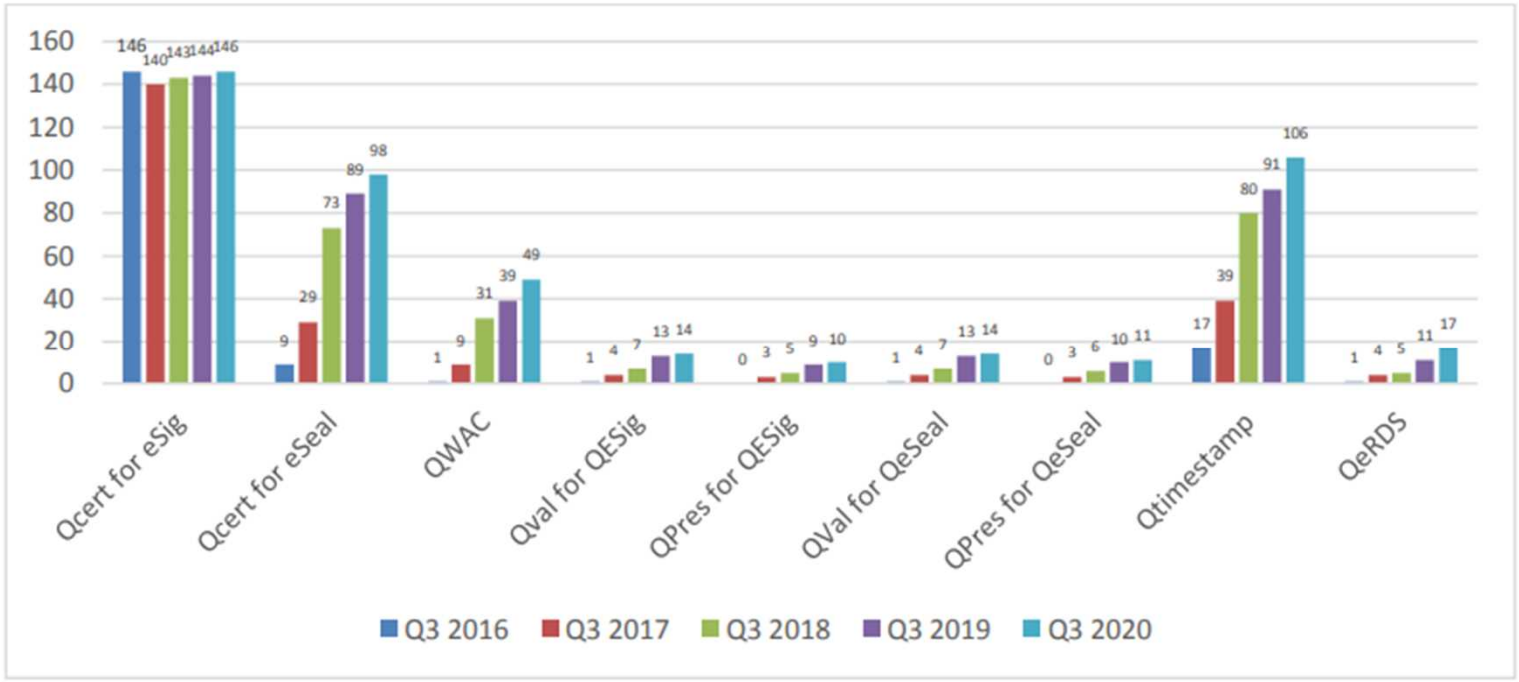
通知済みeIDスキーム数の推移

加盟国間の認証トランザクション数の推移

	2017	2018	2019	2020
Receiving		2	9866	48005
Sending	917	4043	4772	14756
Total nbr of transactions	917	4045	14638	62761

出典： SWD(2021) 130 final “COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)”

適格トラストサービス数の推移



出典： SWD(2021) 130 final “COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)”

eIDAS対応に関する費用及び効果に関するアンケート調査結果

ステークホルダー	初期費用	経常管理費	技術関連費用	利益
政策立案者（政府）	40,000 – 2,300,000 (8)	10,000 – 500,000 (7)	30,000 - 650,000 (9)	N/A
eID提供者	10,000 – 4,500,000 (3)	100,000 – 2,000,000 (4)	30,000 - 650,000 (3)	N/A
eIDサービス提供者	55,000 – 230,000 (3)	25,000 – 1,000,000 (3)	N/A	N/A
認定機関、監督機関、適合性評価機関	N/A	0 – 1,550,000 (23)	N/A	N/A
適格トラストサービスプロバイダ	50,000 - 10,000,000 (19)	3,000 – 4,750,000 (17)	N/A	0 – 20,000,000 (9)
トラストサービスプロバイダ	N/A	3,000 – 4,750,000 (17)	N/A	10,000 (2)

＊本文中には、全体的なデータのばらつきと、各値のサンプル数から、データ分析には注意が必要であると明示されている。　単位：EURO　()内は有効回答数

出典： SWD(2021) 130 final “COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)”

QTSPへのアンケート結果

項目	割合		金額
初期費用：800,000€			
	管理費用（例：管理、業務書類作成、監査手続き、適合性評価、その他）	45％	360,000€
	技術コスト（技術、物的資産への新規投資、コンサルティング、資格)	50％	400,000€
	その他	5％	40,000€
経常費用：750,000€			
	管理費用	40％	300,000€
	技術コスト	35％	262,500€
	OCSPその他保管費用	5％	37,500€
	セキュリティ事故発生時の通知にかかわる費用	10％	75,000€
	その他	10％	75,000€
利益：2,711,000€			

TSPへのアンケート結果

項目	割合		金額
経常費用：750,000€			
	管理費用	40％	300,000€
	技術コスト	35％	262,500€
	OCSPその他保管費用	5％	37,500€
	セキュリティ事故発生時の通知にかかわる費用	10％	75,000€
	その他	10％	75,000€
利益：10,000€			

eIDAS2.0*

●EU Digital Identity Wallet(EUDIW)

全欧州市民が利用可能なeIDの枠組み整備

●トラストサービスの拡充

電子アーカイブ（e-Archiv）、電子台帳（e-Ledger）、属性の電子証明（e-Attestation of Attribute）、リモート署名（シール）生成装置の管理（the management of remote eSig/eSeal creation devices）

●下位規則の整備

技術基準を指定する下位規則の整備をEU委員会に義務付け

*Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (SEC(2021) 228 final) - (SWD(2021) 124 final) - (SWD(2021) 125 final)

eIDAS規則の課題とeIDAS2.0

評価項目	eID	トラストサービス
効果 (目的に対してどれ程効果が得られたか)	○相互承認を共通目的としたeIDスキームの加盟国間ネットワーク構築に寄与 ×相互承認可能なeIDスキームが限定的でEU市民の59% ×eIDASノードの限定的な稼働、国境を越えた認証時のエラー EUDIWで対応	○責任、立証責任、法的効果、トラストサービスの国際的側面に関する法的確実性を確立 ×利用率に加盟国間、トラストサービス種別間で差がある ×技術的中立性を重視した結果、加盟国間での解釈の違い等が生じた 下位規則の整備で対応
効率性	△定量評価ではコストが利益を上回る（利益の定量化が困難）	△定量評価ではコストが利益を上回る（利益の定量化が困難） ○TSPは市場拡大、DSMによる利益を享受
関連性 （ニーズ、課題等と目的の関連性）	×範囲が限定的すぎる（通知されたeIDスキームの公共サービスでの受け入れ） EUDIWで対応	×EUの多くのセクターの法律にeIDAS規則への言及があるにもかかわらず、eIDAS規則はまだ特定の分野（例：教育、銀行、旅行、航空）のニーズに応えられていない。 ×最新の技術動向に対応できていない トラストサービスの拡充で対応
一貫性	○通知とピアレビューに基づくeIDの相互承認のための一般的に首尾一貫したシステム ×LoAを達成するための技術的要件に関する共通理解の不足 ×データ最小化の原則に対応できていない EUDIWで対応	○一貫した監督システムを提供 ×加盟国間で認められる本人確認方法に差がある ×適合性評価機関の義務、責任、能力に関する十分な説明がないこと 下位規則の整備で対応
付加価値	○規則を廃止することは、eIDASに依存している他の立法分野への断片化と否定的な結果につながるだろう △規則の枠組みを一部修正することで、EUの付加価値を高めることができる（民間セクターによる信頼できる政府のeIDの使用を促進し、公共および民間セクターが提供する特定の属性やクレデンシャルを交換するための枠組みを定義することなど）。 EUDIWで対応	○共通の法的枠組みを提供し、市場の断片化を減らし、その利用を増加させた ○トラストサービスを利用することで、行政はサービスの近代化・デジタル化を図り、証拠をデジタルで発行することができるため、行政の負担を軽減すること可能に ×各国の解釈や国内法の矛盾に起因する障壁がまだ残っており、トラストサービスの利用を制限している。 下位規則の整備で対応

出典： COM(2021) 290 final “REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)”

eIDAS2.0における EUDIW

- 希望する全EU市民、在留者、企業が利用可能

各加盟国は、本規則の発効から12か月以内にEU Digital Identity Walletを発行すること （Art.6）
>3つのオプション：加盟国による発行（by member states）/加盟国の委任による発行
(under mandate from a member states)/加盟国による承認
(independently but recognized)

- EUの公的及び民間デジタルサービス利用における本人確認or属性の証明に利用

- 自己主権型（Self Sovereign Identity）

個人識別データ（PID）及び属性の電子証明（EAA）を透明性のある、ユーザが追跡可能な方法で、安全に、要求及び取得、保管、選択、組み合わせ、共有する

- 適格電子署名（QES）をサポート

- 保証レベル：High

EUDIWの利用

1. 公的オンラインサービス

2. 強固なユーザ認証を要求する民間サービス

金融、社会保障、通信等の強固なユーザ認証が法或いは契約によって求められているサービス

3. 大規模オンラインプラットフォーム（Digital Service Act）

DSAで定義される大規模オンラインプラットフォームではユーザからの要請に従ってEUDIWによる認証を受け入れなければならない（Art. 12b）

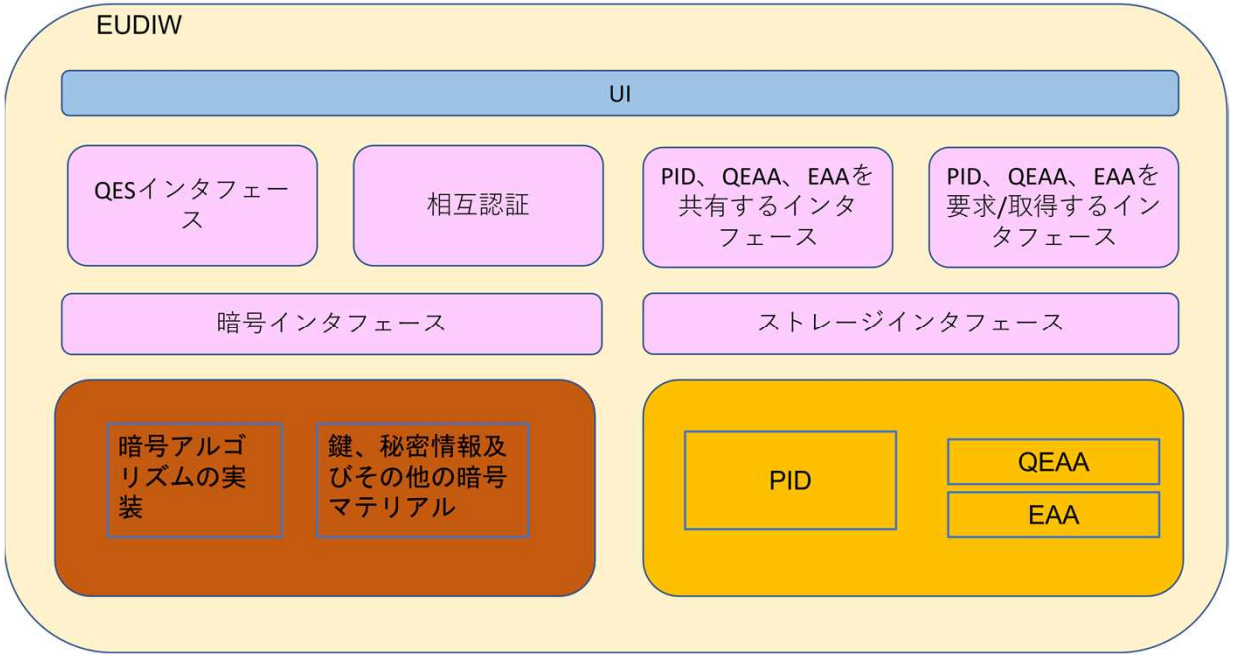
4. その他のオンラインサービス

行動規範(Code of Conduct)を策定し、推奨することで、他のオンラインサービスにおいてもEUDIWが受け入れられるように委員会が奨励、推進する

EUDIW

参考資料

- European Digital Identity Architecture and Reference Framework (2022年2月22日)



各機能の要件

機能	Shall	May
UIの要件	• ユーザに“必要な”情報を表示する機能 -GDPR -QES -使用履歴 -EUDIWトラストマーク等	• “Constraint”コード • EAAの検証 • 特定の属性情報の共有に関する制限と警告
QESインタフェース	複数の実装オプション ①EUDIWがQSCDとなる ②ローカルQSCDと併用 ③リモートQSCDへのインタフェース	
相互認証(mutual authentication)	• オンライン/オフラインでの相互認証 • EUDIW－第三者間の相互認証	• 利用者の認証
暗号機能	• 今後の技術規格、実施法の要件を充足する暗号方式及び暗号機能 RPへの認証、EAA及びPIDの認証、EUDIWの認証、リモートQSCDのアクティベーション（リモート署名時）/QC及び鍵（ローカル署名時）、リ モートストレージへのアクセス、センシティブデータの保管	RPへの仮名認証(pseudonymous authentication)
暗号マテリアル管理	アルゴリズムの十分な強度（SOG-ISカタログへの掲載）	機密度に応じたSWあるいはHWによる管理機能のサポート
信頼できる環境		追加の信頼性が必要な場合におけるTEEあるいはSE（リモートあるいはローカル）の利用
PID（個人識別データ）の保管	ローカルでの保管あるいは、リモートストレージへのポインターをローカルで保管	ストレージ間のデータのコピー、同期、移動
PID、属性の証明（EAA）の要求と取得	• PIDの要求と取得機能 • EAAの要求と取得機能 • PID、EAA及び関連暗号マテリアル（秘密鍵等）の削除機能	識別/認証プロセスにおけるAuthoritative Sourceへの依拠（公的身分証やCivil Registry）
PID、属性の証明の共有	• オンライン/オフラインでの共有	
ユーザ認可	• セキュリティとプライバシーバイデザインを保証した認可メカニズム • 正当な利用者による当該行為への認可の保証 • QSCDによる署名認可の保証 • 2要素認証（LoA High）	

Briefing from European Parliament

- 欧州理事会

加盟国はeIDAS2.0を前向きに受け止め、その野心的なレベルを賞賛している。しかし、IDスキームを導入する期限については懸念が示された。（規則発効後12ヶ月以内）

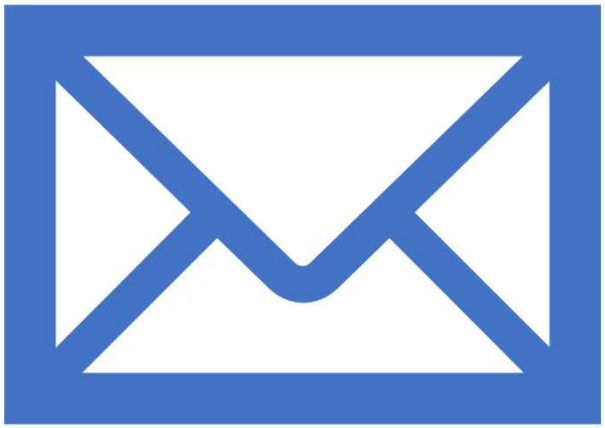
- 経済社会評議会

eIDAS2.0を歓迎し、ユーザーが自分自身のデータを管理し、データへのアクセスを決定し、どのような情報を共有するかを選択できるようにするユーザー中心のアプローチを支持。

- 地域委員会（CoR）

欧州理事会と同様。

出典： Revision of the eIDAS Regulation Findings on its implementation and application



ご清聴いただきありがとうございました

ご質問等ございましたら

s.hamaguchi@cosmos-corp.comまでご連絡ください

資料１６

Digital Architecture Design Center

IPA Better Life with IT

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」

2022年1月25日

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

本日のアジェンダ

1. 本インキュベーションラボの背景と目的
2. オンラインの身元確認手法のレベル分けについて
3. リスクに応じた本人確認手法選択の考え方について
4. ガイドラインの策定に向けた進め方について

参考

本日のアジェンダ

1. **本インキュベーションラボの背景と目的**
2. オンラインの身元確認手法のレベル分けについて
3. リスクに応じた本人確認手法選択の考え方について
4. ガイドラインの策定に向けた進め方について

参考

採択時の目的

- 目的

日本の産業や生活を、グローバルに通用するデジタル本人確認のガイドラインが普及した、サービス提供者と利用者双方の安全性、利便性が両立した環境にする。このことにより、Society5.0に根差した市場拡大及び国際競争力に資する。

- 目標

サービスに応じたデジタル本人確認のガイドライン及び技術を、世界の動向を踏まえて整備し、広く普及させる。

- デジタル本人確認におけるガイドライン整備の意義

- 身元確認手法の、より精緻な整理
- どのようなサービスであればどのレベルの身元確認手法を選択する必要があるかの整理

このふたつを行うことが重要である。

【活動のスコープ（赤枠内）】

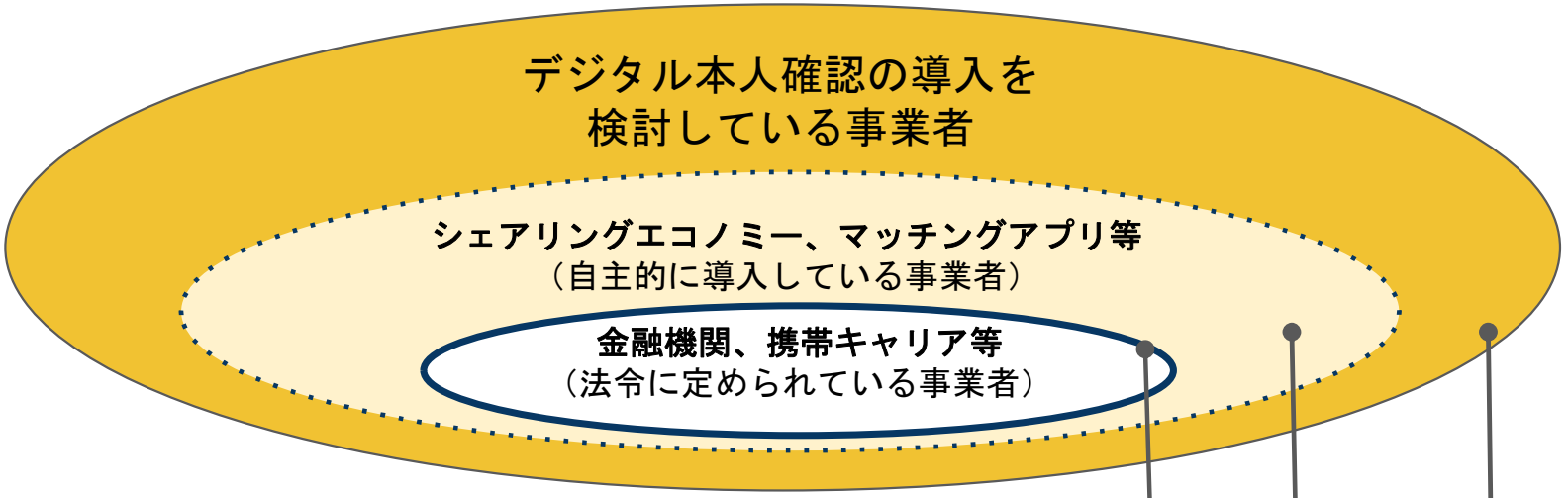
サービスの種類	サービス提供者の種類		利用	ガイドラインの現状
	管理責任	実行責任		
行政サービス、行政手続	行政機関、自治体・省庁及び関連組織	行政機関、自治体・省庁及び関連組織	個人 法人	あり 「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」
民間委託、コラボレーション	行政機関、自治体・省庁及び関連組織	企業、個人事業主	個人 法人	なし 但し「行政手続き～」に従うことが適当。管理責任者の基準において、実行責任者が実行するため。
民間サービス	企業、個人事業主	企業、個人事業主	個人 法人	**大部分に存在しない** **身元確認/当人認証の保証レベル判定方法、保証レベルに応じた手法例が必要**

・個人の民間サービス利用をスコープとする。

・既にガイドラインが定められている「行政手続き」は取り扱わない

ガイドラインを策定する趣旨

レベルは違えど、「本人確認手法が分からない」が共通の課題



課題

- 法令に多くの手法が定められているが、安全性や利便性の**違いが分からない。**
- 導入済みの手法が自社のサービスに**最適な手法か分からない。**
- 対面手続に代わる手続として、**どの手法をどのように導入するのか分からない。**

求められる対応

①身元確認手法の保証レベルの整理

↓

②サービスに応じた本人確認手法の提案

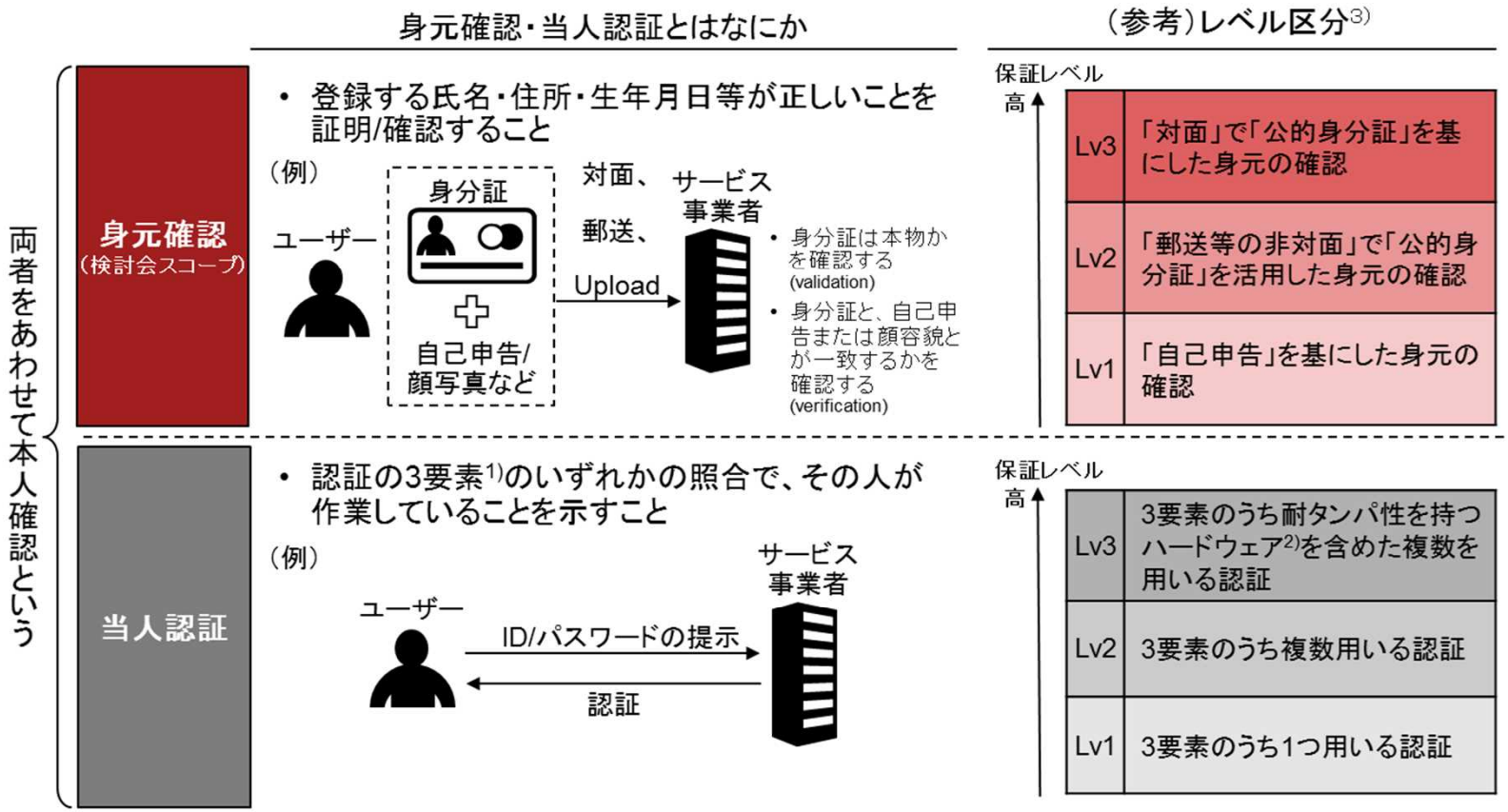
本日のアジェンダ

1. 本インキュベーションラボの背景と目的
2. **オンラインの身元確認手法のレベル分けについて**
3. リスクに応じた本人確認手法選択の考え方について
4. ガイドラインの策定に向けた進め方について

参考

オンラインの本人確認は身元確認と当人認証からなる

身元確認と当人認証の違い



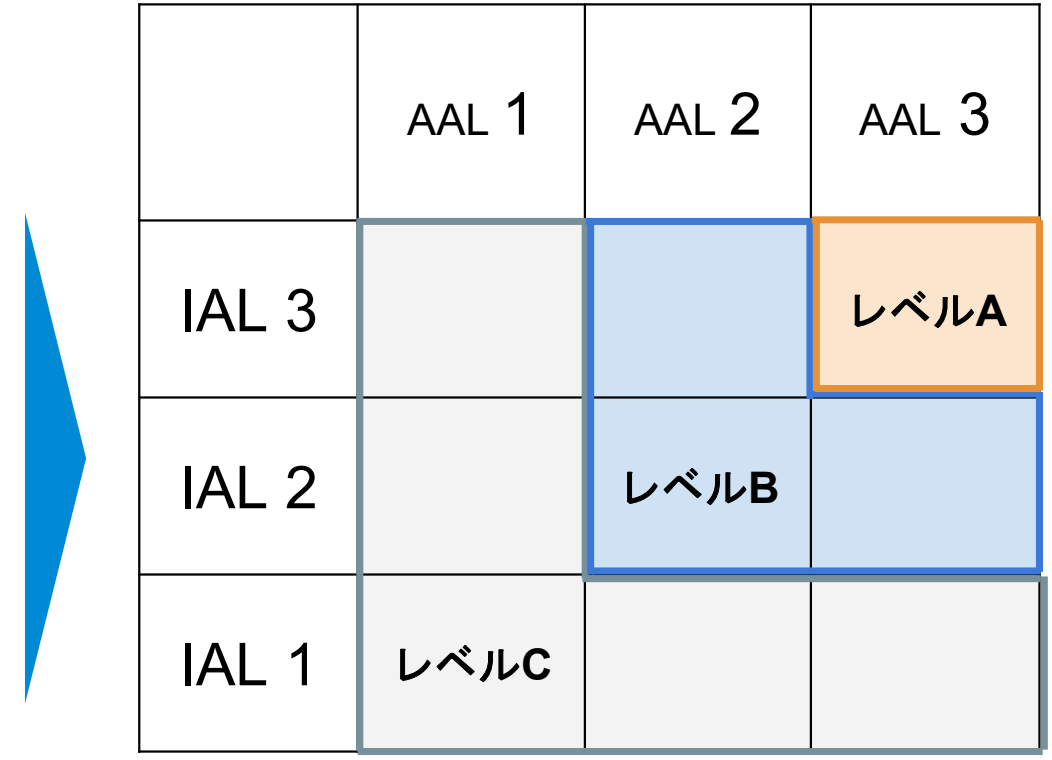
1)認証要素は「生体」（顔・指紋など）・「所持」（マイナンバーカードなど）・「知識」（パスワードなど）に分かれる
2)マイナンバーカードなど、内部の情報に対する不正な読み出しが困難である物理装置
3)「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（2019年2月CIO連絡会議決定）のレベル区分

本人確認の現状　レベル分表作成についての参考：デジタル本人確認の保証レベルと手法例の根拠

IAL・AALのいずれかのレベルが低ければ、本人確認手法のレベルも下がることから、
サービスリスクに応じてIAL・AALを選択する必要がある

身元確認と当人認証の保証レベル

必要な保証レベル		オンラインによる手法例
IAL	AAL	
レベル３ 対面での身元確認	**レベル３** 耐タンパ性が確保された ハードウェアトークン	**レベルA**
レベル２ 遠隔又は対面での身元確認	**レベル２** 複数の認証要素	**レベルB**
レベル１ 身元確認のない自己表明	**レベル１** 単一又は 複数の認証要素	**レベルC**



出所：各府省CIO連絡会議 (2019)「行政手続きにおけるオンラインによる本人確認の手法に関するガイドライン」より作成

本人確認の現状　本人確認手法について

本人確認手法をマトリクスに配置したところ「レベルB」に集中しており、法令内でもばらつきがみられる。

身元確認レベル（IAL） ＼ 当人認証レベル (AAL)	認証なし	レベル1 単要素認証	レベル2 2要素認証	レベル3 2要素認証 (耐タンパを含む)
レベル3 対面確認				・犯収法ワ (犯収法規則6条1項1号) ・公的個人認証
レベル2 郵送・リモート確認		・公的身分証以外の身分証のアップロード ・公的身分証のアップロード ・犯収法ホ (犯収法規則6条1項1号) ・口座連携(犯収令13条1項1号)	・公的身分証以外の身分証のアップロード ・公的身分証のアップロード ・犯収法ホ (施行規則6条1項1号) ・口座連携(犯収施行令13条1項1号) (※1) ・身元確認のAPI連携(銀行API/キャリアAPI) (※1) ・犯収法ヘ (犯収法規則6条1項1号) ・犯収法ヲ (犯収法規則6条1項1号) ・民間APIサービスB (※1)	・犯収法ヘ (犯収法規則6条1項1号) ・犯収法ヲ (犯収法規則6条1項1号) ・身元確認のAPI連携(キャリアAPI) (SIM利用) (※1)
レベル1 自己申告		・身分証に基づかない自己申告での登録	・身分証に基づかない自己申告での登録	

凡例　レベルC　レベルB　レベルA

※1　アカウント作成後は身分証不要

本人確認の現状　オンラインサービスにおける本人確認について

本人確認を実施しているオンラインサービスについてもマトリクスの「レベルB」に集中。
【課題】自社サービスに応じた適切な本人確認手法を選択するためには、**レベルに応じた細分化が必要**

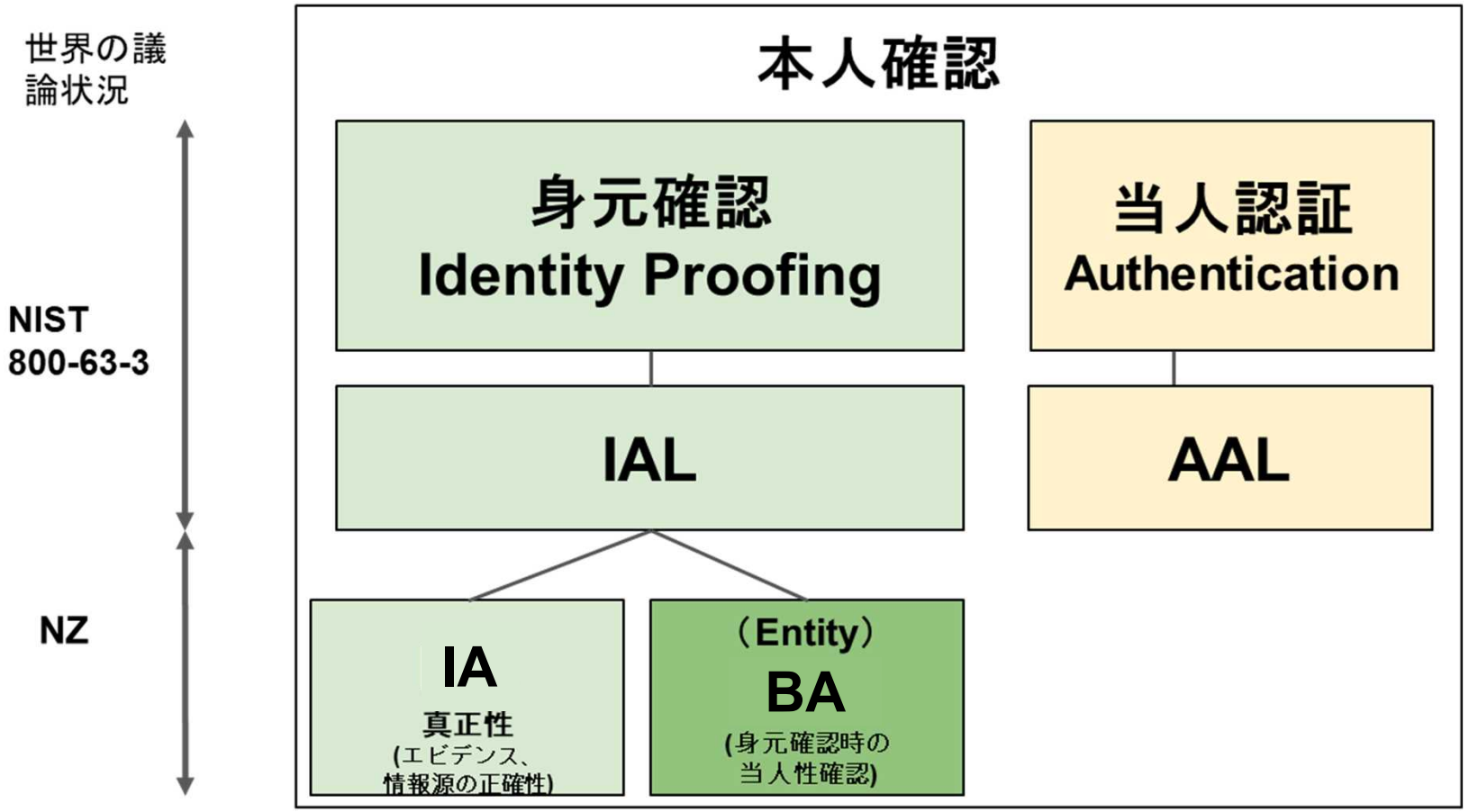
身元確認レベル（IAL） ＼ 当人認証レベル (AAL)	認証なし	レベル1　単要素認証	レベル2　2要素認証	レベル3　2要素認証 (耐タンパを含む)
レベル3 対面確認			・古物商A (※1) ・犯収法の特定事業者 (※1) ・携帯電話事業者 (※1) ・シェアリングエコノミーA社 (※2)	・犯収法の特定事業者 ・携帯電話事業者(※1) ・電子サインA (※1)
レベル2 郵送・リモート確認		・マッチングアプリ ・シェアリングエコノミーB社	・犯収法の特定事業者 (※1) ・携帯電話事業者 (※1) ・古物商B (※1) ・シェアリングエコノミーB社 (※2) ・マッチングアプリ (※3) ・たばこ会員登録 (※3) ・公営ギャンブル (※3) ・eMAFFプライム (オンライン本人確認) (※4) ・gBizプライム (郵送) (※4) ・引越し (※4)	・電子サインA (※1) ・口座開設 (ネット完結) (※2) ・たばこ会員登録 (※3) ・公営ギャンブル (※3)
レベル1 自己申告		・gBiz・eMAFF (エントリー) ・電子サインC (※1)	・電子サインB (※1)	

凡例	レベルC	レベルB	レベルA

※1　法令に基づく
※2　自主的取組
※3　自主的取組 (年齢確認のみ)
※4　行政

＜参考＞ニュージーランドにおけるレベル分け（概要）

身元確認時の「当人性」の確認を含めてIALを整理する動きが見られ始めている。



活動状況　IAL細分化

- IALの細分化に当たり、ニュージーランドのBALの概念を導入
- チーム内で複数回議論を重ね、マトリクス、および手法のマッピングを一旦、完成
- 現在、外部有識者と意見交換し、助言に対しての対応を検討中

  エビデンスに対する支配権、管理権限の観点も必要／リスク（具体的な例示が必要）、UXを考慮した手法の選択する旨の説明が必要 等

手法	DADC IAL (Information Assurance Level)	DADC BAL (Entity Binding Assurance Level)	再考後の DADC IAL (Identity Assurance Level)
公的個人認証による署名用電子証明書＋電子署名付契約書	4	4	**4**
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影	3	4	**3** 調整中
顔写真のある公的身分証のICチップ読み取り／顔写真のある公的身分証の撮影撮（表・裏・厚み）＋法律に基づく身元確認済のAPI連携（銀行など）	3	4	
顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影	3	4	
認定認証事業者による電子証明書＋電子署名付契約書	3	3	
法律に基づく身元確認のAPI連携（銀行API、携帯キャリアAPI等）	3	3	
公的身分証のリアルタイム撮影	2	2	**2**
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）	1	2	**1**
身分証確認なし（自己申告＋eメール、SNSログイン等）	0	0	**0**

【参考】ニュージーランドの新しいInformation Assurance

IAレベル	要求事項(レベルごとに差分があるもののみ抜粋)
4	情報の正確性 ・RPは、**権威ある情報源**であるか、または**権威ある情報源と連続的に同期したリンクを持つエビデンス**を選択しなければならない。 エビデンスの質 ・信頼できる通信チャネルを介してシステム的に識別され、アクセスされる証拠に基づいて品質を設定しなければならない。 コントロール ・RP は詐欺対策技術を適用しなければならない。
3	情報の正確性 ・RP は、**少なくとも権威のあるソースのコピーである証拠**を選択しなければならない。 エビデンスの質 ・RPは、手動で特定された証拠に基づいて品質を決定しなければならず、また、 **再現するために独自の知識を必要とする物理的なセキュリティ機能**を含まなければならない。 コントロール **・RPは詐欺対策技術を適用すべきである。**
2	情報の正確性 ・RPは、少なくとも作成時に権威あるソースのコピーを参照した証拠を選択すべきである。 エビデンスの質 ・RP は証拠を「額面通り」に受け取らなければならない。
1	情報の正確性 ・RPはエンティティを証拠として用いるべきである。 エビデンスの質 ・RPはそのエンティティを証拠として受け入れなければならない。

【参考】ニュージーランドの新しいEntity Binding Assurance

BAレベル	要求事項(レベルごとに差分があるもののみ抜粋)
4	エンティティと情報との関係の確立 **・RP は、バイオメトリクス要素を、知識または所有のいずれかのバインディング要素タイプで使用するか、または同等以上の保証レベルの既存の認証機関またはクレデンシャルを使用しなければならない。** 詐欺対策技術 ・RPは不正防止技術を適用しなければならない。 エンティティバインディングの再確認 ・認証イベントに生体認証要素が含まれていない限り、少なくとも5年に1回RPはこの管理を実施しなければならない。
3	エンティティと情報との関係の確立 ・RP は、**最低でも 2 種類の結合要素、**または保証レベルが同等以上の既存の認証機関やクレデンシャルを使用しなければならない。 詐欺対策技術 **・RP は詐欺対策技術を適用すべきである。** エンティティバインディングの再確認 ・認証イベントに生体認証要素が含まれていない限り、少なくとも5年に1回RPはこの管理を実施しなければならない。
2	エンティティと情報との関係の確立 ・RP は、**最低でも 1 種類の結合要素**を使用するか、同等以上の保証レベルの既存の 認証子またはクレデンシャルを使用しなければならない。 エンティティバインディングの再確認 ・少なくとも5年に1回行うべきである。
1	エンティティバインディングの再確認 ・少なくとも5年に1回行うべきである。

ニュージーランド/IALの要件を参考にしたDADC/IALの考え方

NZレベル	1	2	3			4			DADC IAL (Information Assurance Level)
	IA3.03	IA3.03	IA3.03	IA4.02	IA4.03	IA3.03	IA4.02	IA4.03	
	依拠当事者が、各情報の検証に必要な情報アシュアランス（IA）のレベルに合った適切な証拠を選択すること	依拠当事者が、各情報の検証に必要な情報アシュアランス（IA）のレベルに合った適切な証拠を選択すること	依拠当事者が、各情報の検証に必要な情報アシュアランス（IA）のレベルに合った適切な証拠を選択すること	依拠当事者が、使用できないような登録状態（一時停止、取り消し等）の証拠があるかを確認すること	依拠当事者が、可能な限り不正行為対策技術を適用すること	依拠当事者が、各情報の検証に必要な情報アシュアランス（IA）のレベルに合った適切な証拠を選択すること	依拠当事者が、使用できないような登録状態（一時停止、取り消し等）の証拠があるかを確認すること	依拠当事者が、可能な限り不正行為対策技術を適用すること	
	依拠当事者はエンティティーを証拠として使用すべきです。	[SHOULD]権威ある情報源のコピーを参照した証拠	[SHOULD]権威ある情報源のコピーである証拠	[SHOULD]証拠発行者又は同等のサービス・プロバイダーに登録状態を確認	[SHOULD]不正行為対策技術を適用	[MUST]権威ある情報源である証拠、又は権威ある情報源と継続的に同期したリンクを持つ証拠	[MUST]証拠発行者又は同等のサービス・プロバイダーに登録状態を確認	[MUST]不正行為対策技術を適用	
チーム内で検討した補足条件 / 手法					以下のいずれかを満たせば〇 1.認定事業者による電子署名 2.犯収法要件に準拠 3:キャリア網+暗証番号認証 / FIDO認証等を利用する			以下のいずれかを満たせば〇 1.認定事業者による電子署名 2.犯収法要件に準拠 3:キャリア網+暗証番号認証 / FIDO認証等を利用する	
公的個人認証による署名用電子証明書＋電子署名付契約書						〇	〇	〇	**4**
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影			〇	×	〇	×	×	〇	**3**
認定認証事業者による電子証明書＋電子署名付契約書			〇	×	〇	×	×	〇	**3**
顔写真のある公的身分証のICチップ読み取り／顔写真のある公的身分証の撮影撮（表・裏・厚み）＋法律に基づく身元確認済のAPI連携（銀行など）			〇	〇	〇	×	〇	〇	**3**
顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影			〇	×	〇	×	×	〇	**3**
公的身分証のリアルタイム撮影		〇	〇	×	×	×	×	×	**2**
法律に基づく身元確認のAPI連携（銀行API、携帯キャリアAPI等）			×	〇	〇	×	〇	〇	**3**
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）	〇	×	×	×	×	×	×	×	**1**
身分証確認なし（自己申告＋eメール、SNSログイン等）		×	×	×	×	×	×	×	**0**

ニュージーランド/BALの要件を参考にしたDADC/BALの考え方

NZレベル	1	2	3		4		DADC BAL (Entity Binding Assurance Level)
		BA3.02	BA3.02	BA3.06	BA3.02	BA3.06	
	なし	依拠当事者が、以下の紐づけ要素タイプを用いて、要求される紐づけのアシュアランスのレベルと整合する紐づけ方法を選択すること	依拠当事者が、以下の紐づけ要素タイプを用いて、要求される紐づけのアシュアランスのレベルと整合する紐づけ方法を選択すること	依拠当事者が、可能な場合に詐欺対策技術を適用すること	依拠当事者が、以下の紐づけ要素タイプを用いて、要求される紐づけのアシュアランスのレベルと整合する紐づけ方法を選択すること	依拠当事者が、可能な場合に詐欺対策技術を適用すること	
		[MUST]最低でも 1 種類の紐づけ要素を使用するか、同等以上のアシュアランスレベルの既存のオーセンティケーター又はクレデンシャルを使用	[MUST]最低でも 1 種類の紐づけ要素を使用するか、同等以上のアシュアランスレベルの既存のオーセンティケーター又はクレデンシャルを使用	[SHOULD]不正行為対策技術を適用	[MUST]最低でも 1 種類の紐づけ要素を使用するか、同等以上のアシュアランスレベルの既存のオーセンティケーター又はクレデンシャルを使用	[SHOULD]不正行為対策技術を適用	
チーム内で検討した補足条件 / 手法				以下のいずれかを満たせば○ 1.認定事業者による電子署名 2.犯収法要件に準拠 3:キャリア網+暗証番号認証 / FIDO認証等を利用する	対面で証明書を渡してる事が保証でき、それが確実に確認出来る場合（ICチップ読取り）に○。	以下のいずれかを満たせば○ 1.認定事業者による電子署名 2.犯収法要件に準拠 3:キャリア網+暗証番号認証 / FIDO認証等を利用する	
公的個人認証による署名用電子証明書＋電子署名付契約書	—				○	○	4
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影	—				○	○	4
認定認証事業者による電子証明書＋電子署名付契約書	—		○	○	×	×	3
顔写真のある公的身分証のICチップ読み取り／顔写真のある公的身分証の撮影撮（表・裏・厚み）＋法律に基づく身元確認済のAPI連携（銀行など）	—				○	○	4
顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影	—				○	○	4
公的身分証のリアルタイム撮影	—	○	×	×	×	×	2
法律に基づく身元確認のAPI連携（銀行API、携帯キャリアAPI等）	—		○	○	×	○	3
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）	—	○	×	×	×	×	2
身分証確認なし（自己申告＋eメール、SNSログイン等）	—	×	×	×	×	×	0

DADCが提案する民民手続におけるIAL

手法	DADC IAL (Information Assurance Level)	DADC BAL (Entity Binding Assurance Level)	再考後の DADC IAL (Identity Assurance Level)
公的個人認証による署名用電子証明書＋電子署名付契約書	4	4	**4**
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影	3	4	
顔写真のある公的身分証のICチップ読み取り／顔写真のある公的身分証の撮影撮（表・裏・厚み）＋法律に基づく身元確認済のAPI連携（銀行など）	3	4	**3**
顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影	3	4	調整中
認定認証事業者による電子証明書＋電子署名付契約書	3	3	
法律に基づく身元確認のAPI連携（銀行API、携帯キャリアAPI等）	3	3	
公的身分証のリアルタイム撮影	2	2	**2**
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）	1	2	**1**
身分証確認なし（自己申告＋eメール、SNSログイン等）	0	0	**0**

今回の整理における IAL間の外形的な違い

・現況確認の有無

・確認対象の有無
・偽造等不正対策の有無

・保有確認の有無

・身分証の有無

新たな手法の検討の必要性

手法	再考後の DADC IAL (Identity Assurance Level)
公的個人認証による署名用電子証明書＋電子署名付契約書	4
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影	3
顔写真のある公的身分証のICチップ読み取り／顔写真のある公的身分証の撮影撮（表・裏・厚み）＋法律に基づく身元確認済のAPI連携（銀行など）	
顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影	
認定認証事業者による電子証明書＋電子署名付契約書	
法律に基づく身元確認のAPI連携（銀行API、携帯キャリアAPI等）	
公的身分証のリアルタイム撮影	2
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）	1
身分証確認なし（自己申告＋eメール、SNSログイン等）	0

既存手法の要件を足し引きすることで、
◈新たな手法の確立
◈新たな手法のIALの明確化
が容易となる

IALが明確な手法の選択肢が広がり、**各事業者が、サービス内容やユーザの特性などを踏まえて、適切な手法を選択しやすくなる**

本日のアジェンダ

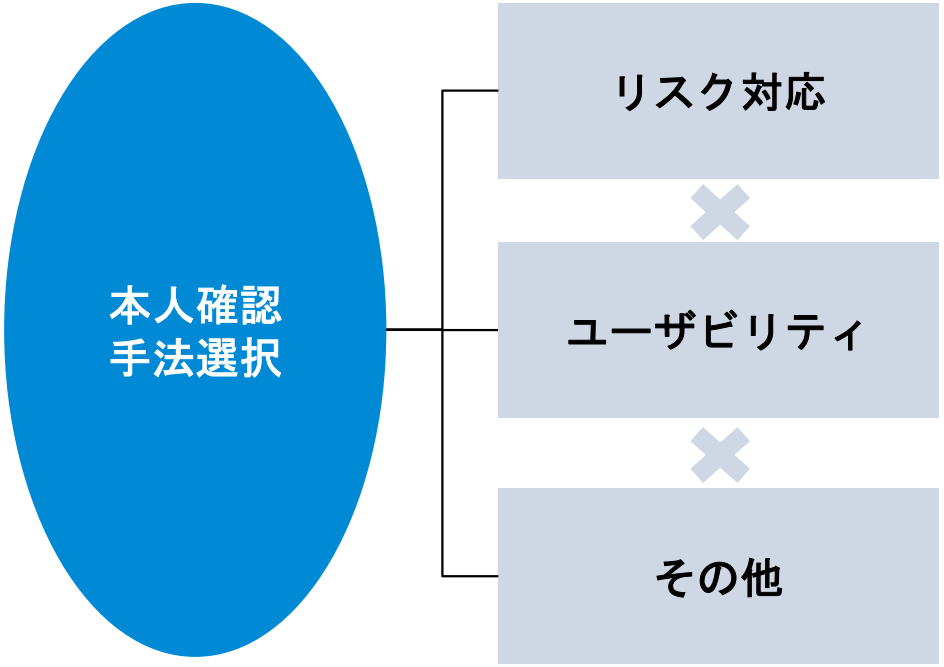
1. 本インキュベーションラボの背景と目的
2. オンラインの身元確認手法のレベル分けについて
3. **リスクに応じた本人確認手法選択の考え方について**
4. ガイドラインの策定に向けた進め方について

参考

事業者は、どのように本人確認手法を選択しているか

ラボチームの行ったヒアリングによると、
各事業者は、①リスク対応と②ユーザビリティを重視した上で、コストや事業者の信頼度も踏まえ、
本人確認手法を選択している

本人確認手法の選択軸



ヒアリングでの事業者からの主なコメント

- オンラインで完結できる手法を選択した
- 依頼者が起こすトラブルを回避したい
- 偽造身分証を防ぎたい

- セキュリティを強化するとユーザーのハードルが上がるが、サービスが使われないと意味がない。本人確認を強固に行うことで、利用者のハードルがどれだけ上がるかのバランスで手法を決めた

- コストとのバランスを見ながら（身分証の偽造を検知するという）目的を達成できる手法を選択した
- 当社の求める目的に過不足ない適切な手法を提示してくれた(eKYCサービス事業者の信頼度)

本インキュベーションラボにおける検討事項

本インキュベーションラボでは、「リスクに応じた本人確認手法を選択できる」という目的を踏まえ、
まずはリスクに関して、事業者が捉えているリスクレベル等について調査・整理した

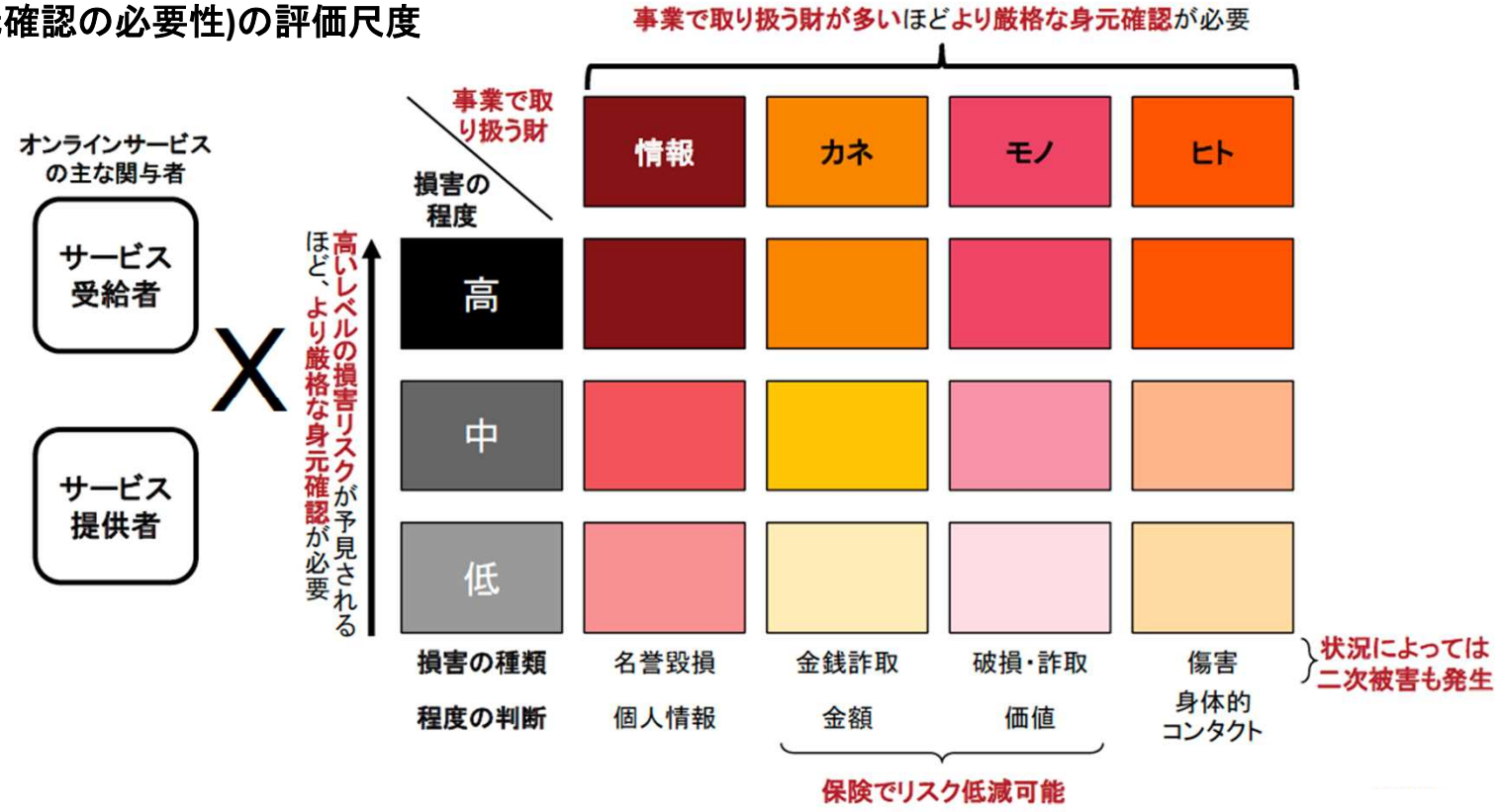
検討事項の整理

本人確認手法の選択軸	論点	検討の方向性
リスク対応	● 事業者がどのようなリスクを抱えて、本人確認で対応しているか ● 本人確認で対応できている点、できていない点 等	**本インキュベーションラボで検討を開始**
ユーザビリティ	● ユーザーにとっての負荷をどう整理するか ● 既存の手法をユーザビリティの視点でどう整理するか	手法のレベル整理を行った後、議論すべき論点
その他	● コストについては、各eKYC事業者の競争領域で、ガイドライン等では対象外 ● eKYC事業者の信頼度については、認証制度等も考えられるが、本ラボのスコープ外と思料	コストは、各事業者判断。事業者の認証等は将来的な課題

前回研究会におけるリスクの整理

経済産業省「オンラインサービスにおける身元確認に関する研究会」では、リスク評価の際には、事業で扱う財とその内容や関与者、保険/補償の有無、二次被害の可能性、等を踏まえた被害程度を見積る必要性が指摘された

事業リスク(身元確認の必要性)の評価尺度

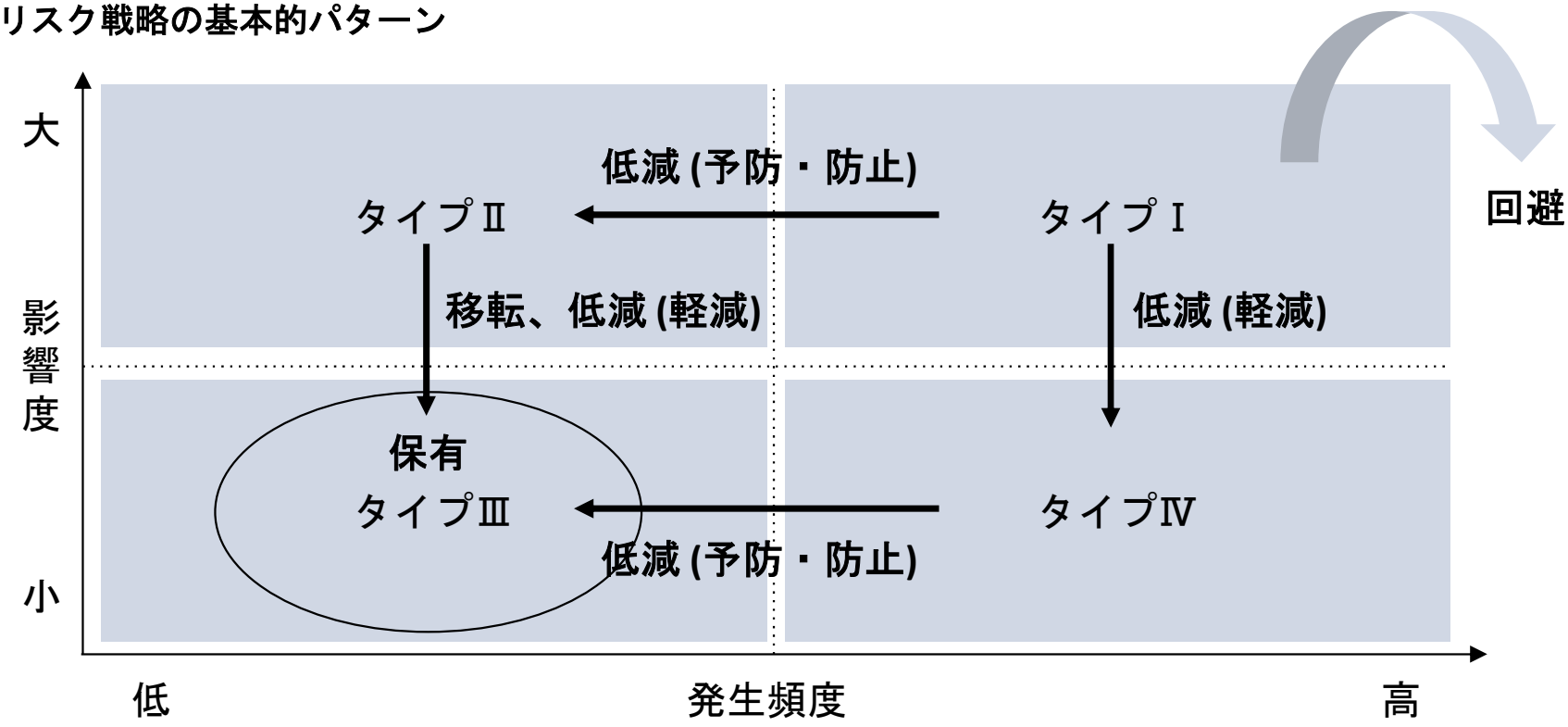


出所：経済産業省 (2020)「オンラインサービスにおける身元確認手法の整理に関する検討報告書」より

ヒアリングにおける示唆・事業リスクに関する整理

一般的にリスクマネジメントでは、各リスクを影響度と発生頻度のリスクマップ上にプロットし、各社が優先順位をつけて適切なリスク戦略を選択している。「リスクに応じた本人確認手法の選択」をガイドライン化するためには、リスク評価・リスク戦略等の手法を参考に「リスクの標準化」が課題となる

リスク戦略の基本的パターン



リスク戦略の例

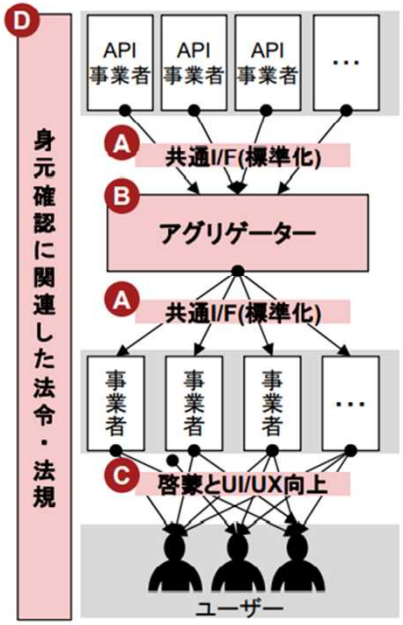
- 移転:
  損害保険
- 低減(予防・防止):
  本人確認
- 低減(軽減):
  サービスごとに立案
- 回避:
  事業撤退

出所：経済産業省 (2005)「先進企業から学ぶ事業リスクマネジメント実践テキストー 企業価値の向上を目指して ー」より

ヒアリングにおける示唆・ユーザビリティについて

本人確認を実施することによるUXの悪化を懸念する意見も得られた。
リスク対策と、ユーザビリティ確保の両立を実現する必要がある。

（参考）「オンラインサービスにおける身元確認に関する研究会」で提示されたアグリゲーターを設置する案



ステークホルダーと論点

論点詳細

A どの標準化動向に、どこまで合わせていくか
- 国際標準、先行プレイヤー等のどの基準にあわせていくか
- 合わせる場合はどこまで合わせていくか

B アグリゲーターの必要性と、どこまで任せるか
- 官、民どちらが行うか、民で行う場合の競争環境をどう考えるか
- APIを取りまとめるだけなのか、ユーザー情報のアグリゲートまで行うのか
- e-KYC事業者等の認定の仕組みが必要ではないか
- 産業毎・アグリゲーター毎の相互接続性を担保できるようにすべきではないか
- データ連携技術で、実装としての共通I/F化が必要ではないか

C UI/UXを向上し、どう利便性向上を図るか
- 国際標準、先行プレイヤー等のどの基準にあわせていくか
- 事業者間の協調及び、ユーザーへの普及をどうやって推進するか

D 身元確認に関連した法令・法規は、それぞれどのように整合しているか

(参考)
標準化・アグリゲーター設置のメリット

- 対象
  - オンラインサービス等の身元確認を活用する事業者
  - 身元確認API事業者
- 効果
  - 開発、接続、カバレッジ、オペレーション等が全て効率化される
    - API・データの仕様を詳細レベルで揃え、共通I/Fで事業者へ提供
    - 複数の身元確認API提供者を束ねて、ユーザーカバレッジが向上
    - 身元確認API業者と事業者との契約・請求業務が一本化される

(参考)
中長期的な検討事項

- マイナンバーカードとの連携、保険証や資格情報[1)]との連携、在留外国人のデジタルアイデンティティの活用、更には海外での活用等の観点も考慮をしておくことが必要か

出所：経済産業省 (2020)「オンラインサービスにおける身元確認手法の整理に関する検討報告書」より

本日のアジェンダ

1. 本インキュベーションラボの背景と目的
2. オンラインの身元確認手法のレベル分けについて
3. リスクに応じた本人確認手法選択の考え方について
4. **ガイドラインの策定に向けた進め方について**

参考

ガイドライン策定に向けた進め方

サービスに応じた本人確認手法の提案に向けて

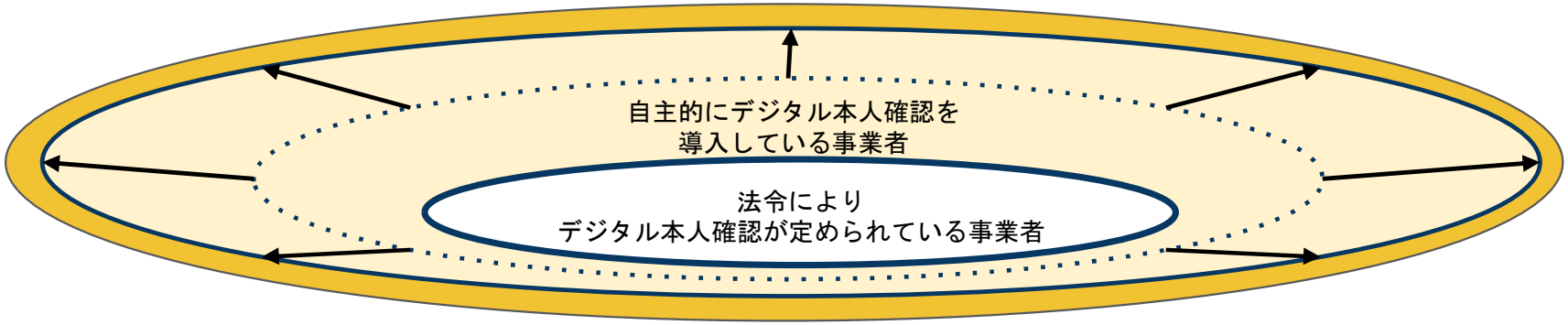
検討内容	① 身元確認手法 の保証レベルの整理	② リスク対応 ユーザビリティの検討
進捗	ニュージランドの基準参考に DADC　IAL案を策定	ヒアリングを実施し、 リスクについて検討開始
今後の 予定	専門家の意見を交え IAL案を確定	幅広い事業者から意見を収集 し、考え方を整理

ガイドラインの策定

ガイドライン策定後の社会

ガイドラインの策定

「分からない」課題が解決し、デジタル本人確認の普及が促進



ガイドライン策定後は下記のニーズが高まることが想定される

ガイドラインのアーキテクチャに基づき、
技術革新に対応した新たな手法

ガイドラインに沿って、的確な手法を
提案する「信頼できるID Provider」

本日のアジェンダ

1. 本インキュベーションラボの背景と目的
2. オンラインの身元確認手法のレベル分けについて
3. リスクに応じた本人確認手法選択の考え方について
4. ガイドラインの策定に向けた進め方について

参考

海外動向調査

- 海外動向についてネットを中心に調査
- スウェーデン、シンガポール、イギリス、ドイツ、エストニア、インドの６ヵ国
- 各国「サービス概要」、「利用状況」、「普及または失敗した背景」、「留意すべき日本との違い」についてまとめました。
- 本人確認も含まれますが、主にデジタルIDを中心とした各国の全体的な取り組み状況についてとなります。

海外動向調査

#	国名	区分	サービス名	サービス概要 （取り組みの概要）	利用状況 （結果や現状）	普及または失敗した背景	留意すべき日本との違い （文化、風習、国民性…）
1	スウェーデン ・人口：約1,022万人（2018年11月，スウェーデン統計庁） ・面積：約45万平方キロメートル（日本の約1.2倍）	民間主体	Bank ID ・口座開設時に付与 ・IDはパーソナルナンバーと紐づく	2003年に開始。 運営主体は、銀行７行のコンソーシアム。 国の関わり：2004年、電子政府のオンライン申告や申請手続きに使用するデジタルIDに選定される。パーソナルナンバーに紐付けられており、オンラインで各種申請や手続きを行う際の本人認証手段として、Bank IDが利用されている。 2009年、国税庁がBankID利用者の優遇税制を設け利用拡大。BankIDによる電子署名には、法的拘束力がある。	・登録者数：820万人（2019年）人口普及率80%以上。 ・対応可能なサービス：公共サービス：確定申告、各種行政手続、病院関連の手続き等 ・民間サービス：銀行取引、決済サービス、電子商取引、ポイントサービス等 ・BankIDの電子署名は、eIDASのルールを遵守する電子署名法に基づく法的効力のある署名	**普及のきっかけは、2010年にモバイルBank IDが導入され利便性が高まったこと。2012年にはモバイルP2P決済サービス「スウィッシュ(Swish)」の認証手段にBank IDが使われたことで、一気に利用が広がる。**	・パーソナルナンバー（日本のマイナンバーに相当）開始年：1947年 ・ナンバーから生年月日と出生地が一目瞭然。元々ナンバーを使う機会が多く、国民の抵抗感が低い ・高い透明性と国への信頼：公的機関における個人情報の取り扱いの適正性については、独立機関が監督。希望者に対しては公的機関の保有する自己に関する情報を毎年提供し、官庁間や官から民への情報提供ルールが法令で規定されているなど、透明性の高い仕組みが構築されている。 ・国民の プライバシー意識：センシティブな情報の対象範囲が狭い。収入や納税額もオープン。

海外動向調査

#	国名	区分	サービス名	サービス概要 （取り組みの概要）	利用状況 （結果や現状）	普及または失敗した背景	留意すべき日本との違い （文化、風習、国民性…）
2	シンガポール ・人口：約569万人（うちシンガポール人・永住者は404万人）（2020年） ・面積：約720平方キロメートル（東京23区と同程度）	政府主体	National Digital Identity（NDI） SingPass	・国が主導してNDI（国家デジタル認証）と呼ぶ官民共通のデジタルIDスキームの開発・普及を推進している。 ・NDIは、識別子となる個人登録番号（NRIC番号）と既存の公的認証システム「SingPass」、個人情報の登録・利用の一元化サービス「MyInfo」を基盤とし、市民が単一のデジタルIDで官民のサービスを利用できる共通認証プラットフォームの構築を目指すプロジェクトである。	SingPass/My Infoという既存のサービスは、70の政府機関が提供する160のデジタルサービスの認証基盤として活用されている。今後は民間企業も個人認証のためにNDIプラットフォームを利用できるようになる予定である。 ・SingPassに実装されたクラウドベースの顔認証は、生体認証スキャンによって得られたユーザーの顔データを政府に保管されたデータベースと照合することで、本人確認を行う。政府機関だけでなく、銀行・保険などの民間企業に対しても開放しており、インターネットバンクの新規利用申し込みに必要な本人確認手続きにも利用されている。	**2018年にスマートフォンの生体認証を利用するSingPass Mobileが始まり、2019年には公的身分証明書（NRICカード）を見せなくても本人確認と必要な個人情報を提供可能とするSG Verifyが導入された。** 企業は、独自のインフラやシステムを構築しなくても、政府が提供するNDIの共通APIや各種ツールを使って認証基盤を導入することが可能となり、コスト削減や安全性の強化に繋がる。	・シンガポールのスマートネイション構想は、わが国が推進するソサエティ5.0と類似する点が多く、先行事例として位置づけることができる。

海外動向調査

#	国名	区分	サービス名	サービス概要 （取り組みの概要）	利用状況 （結果や現状）	普及または失敗した背景	留意すべき日本との違い （文化、風習、国民性…）
3	イギリス ・人口：6,680万人（2019年） ・面積：24.3万平方キロメートル（日本の約3分の2）	政府主体	GOV.UK Verify	2016年に公共サービスの共通認証プラットフォーム「GOV.UK Verify（Verify）」が導入された。オンラインで公共サービスを利用するにあたり、政府の認定を受けた複数のIDプロバイダーのなかから、利用者自身が使用する認証サービスを選択する仕組み	Verifyは当初の計画通りには普及が進んでいない。	普及が進んでいない理由として、**ユーザーエクスペリエンスが不十分であることや、関係する省庁が必ずしも協力的ではないこと、民間サービスプロバイダーの求める要件を満たすものではないことなどが指摘されている。**政府は、2019年に省庁横断的にデジタルIDを推進する組織を設置し、Verifyに代わる新たなデジタルIDの在り方を検討している。	**・識別子となる統一的な国民番号がないことが課題として指摘されている**
4	ドイツ ・人口：約8,319万人（2020年9月、独連邦統計庁）	民間主体	Verimi	業界横断型の連合で消費者データのプライバシーを優先し、FacebookとGoogleの二大覇権に対抗することを目指している。 従来のプラットフォーマーと異なり、参加企業が集めたデータをどう使うかをユーザーの選択に委ねている。ユーザーが同意しない限りデータは広告や外部企業に使われることはない。	自動車メーカーのダイムラー（Daimler）や保険大手のアリアンツ（Allianz）、ドイツ銀行（Deutsche Bank）も参加している。ドイツの航空会社ルフトハンザ（Lufthansa）や通信会社のドイツテレコム（Deutsche Telekom）、ITセキュリティ会社のブンデスドルクレイ		

海外動向調査

#	国名	区分	サービス名	サービス概要 （取り組みの概要）	利用状況 （結果や現状）	普及または失敗した背景	留意すべき日本との違い （文化、風習、国民性…）
5	エストニア ・人口：約133万人（2021年）日本の約9分の1 ・面積：4.5万平方キロメートル（日本の約9分の1）	政府主体	・Mobile-ID（SIMカード） ・Smart-ID（アプリ）	・Mobile-IDは身分証明書法で本人確認手段として定められているモバイル端末を利用するSIMカード ・Smart-IDはモバイル端末で利用するアプリ 「世界で最も先進的なデジタル社会」と名付けられたエストニアは、政府サービスの99%がオンラインである	・2002年エストニア政府はエストニア版マイナンバーカード「e-IDカード」を国民に配布し、従来は役所に訪問しなければ不可能だった本人確認をオンライン上で可能にした。現在エストニアでは99%の行政申請がオンラインで可能であり、連携したサービスも2,700を超える。 ・結婚、離婚、不動産の手続き以外は全部オンラインでできる。	e-IDカードにも不便な部分は指摘されてきた。e-IDカードで認証を行うためには、カードリーダーを持ち歩き、物理的なカードで認証させなくてはならず、導入当初は利用者からの不満も多かった。**そこで誕生したのが「デジタルIDアプリ」だ。初回登録時にe-IDカードを認証し、アプリと紐付けることで公的身分証による本人性を担保する。それによって、毎回カードリーダーでe-IDカードを読み取る不便さがなくなり、利便性が向上した。現在は国民の35%が「デジタルIDアプリ」を利用している。**	“国の規模”が小さい

海外動向調査

#	国名	区分	サービス名	サービス概要 （取り組みの概要）	利用状況 （結果や現状）	普及または失敗した背景	留意すべき日本との違い （文化、風習、国民性…）
6	インド	政府主体	国民IDシステム「Aadhaar（以下アドハー）」	NECの技術が基盤となっているアドハーは、インドの固有識別番号庁（UIDAI）によって登録が進められている生体認証IDシステムで、国民の名前や住所、生体情報を収集して管理する。システムに登録された国民1人ひとりに12桁の数字からなるIDを発行し、役所などの公共機関や銀行はこの固有のIDを使って社会保障の受け取りや銀行口座開設の本人確認をスムーズに行うことができる。	・2009年から導入された国民IDシステム「Aadhaar」。既に12.3億人以上が登録し、公共福祉サービスが効率的に支払われるようになり、不正行為も激減した。 ・指紋、顔、および虹彩認証を組み合わせた、超高精度なマルチモーダル生体認証。 **・インドのデジタルID普及割合は銀行口座保有者の割合と比例して増加しており、口座を保有できることが1つのデジタルID普及のドライバーになったと考えられる。**2008年時点では人口の4%程度しかIDを持っていなかったが、2018年には10億人以上がIDを保有するようになった。	「デジタル化」されたIDシステムによって、国民が、公共サービスや福祉支援、金融サービスを公平に享受できるようになっている。またインドの成長の足かせとも言われ、長年にわたって深刻な問題となっていた汚職や不正が減ったことで、政府はこれまでに124億ドル（約1.37兆円）の不正支出をなくすことに成功している。 iSPIRT(非営利団体)によれば、企業がユーザーデータから利益を得ていることが問題なのではなく、ユーザーが自分のデータから恩恵を得られないことが問題であるとしている。このため、銀行口座とデジタルIDの紐づけやデータ接続を個人に管理できる環境を提供することで、ユーザーが自分のデータを適切に生かして企業からメリットを得やすくしている。	・10億人をこえる市民に対していかに効率的に行政サービスを提供するかという観点からデジタルテクノロジーの導入を進めた。 ・整備が必要なのは、市民が行政に対して提供したデータを、どの機関に、そこまで共有するかを確認する機能や、行政側からの通知を一元的に受ける機能の提供。個人情報の保護とワンスオンリーを同時に実現するには、事故データの共有先を管理できる機能が欠かせない。

海外動向調査まとめ

- スウェーデンやシンガポール、エストニアの例から、デジタルIDがスマートフォンに搭載され物理的なカードを使わずに本人確認が行えることでユーザーの利便性が高まり、一気に普及していくケースがみられた。

- デジタルIDや本人確認サービスの一極集中について、スウェーデンでは、①単一IDプロバイダーへの過度の依存はリスク、②イノベーションや品質、価格面での競争が不在、③移民や銀行口座のない個人などが排除、などの問題点が指摘されている。また、シンガポールでも中央集権型のシステムであるためトラブルが発生すると機能不全となる事態や、民間企業の採用が想定通りに進むか、といった課題がある。

- イギリスでは、2000年代に入ってテロ対策や犯罪予防等の観点から、厳格に本人確認できる手段として国民IDカードの導入が議論され、IDカード法が成立したものの、費用対効果やプライバシー侵害等が問題視され、政権交代とともに同法は廃止された。この代替策として、2016年に公共サービスの共通認証プラットフォーム「GOV.UK Verify（Verify）」が導入された。政府の認定を受けた複数のIDプロバイダーのなかから、利用者自身が使用する認証サービスを選択する仕組みであるが、Verifyは当初の計画通りには普及が進んでいない。その理由として、ユーザーエクスペリエンスが不十分であることや、関係する省庁が必ずしも協力的ではないこと、民間サービスプロバイダーの求める要件を満たすものではないことなどが指摘されている。政府は、2019年に省庁横断的にデジタルIDを推進する組織を設置し、Verifyに代わる新たなデジタルIDの在り方を検討している。もっとも、識別子となる統一的な国民番号がないことが課題として指摘されている。

- シンガポールのCODEX等、階層化されたアーキテクチャーを前提にデータ層・サービス層を分離した立体的な階層構造で構築、民間にも広く開放している。

海外動向調査 主な参考ソース

- 「行政をハックしよう」吉田 泰己(著)　ぎょうせい
- 日本総研「デジタル時代の社会基盤「デジタルID」」
  https://www.jri.co.jp/MediaLibrary/file/report/jrireview/pdf/11717.pdf
- エストニアの電子証明書等について（総務省）
  https://www.soumu.go.jp/main_content/000731090.pdf
- ドイツのパブリッシャー、共通ログインで「異業種」連携：FacebookとGoogleの2強に対抗
  https://digiday.jp/publishers/german-publishers-joining-forces-duopoly/
- インド13億人の「生体認証」国民IDに、知られざる日本企業の貢献
  https://wisdom.nec.com/ja/collaboration/2019051701/index.html
- GAIN DIGITAL TRUST
  https://gainforum.org/GAINWhitePaper.pdf

資料１７

トラストを確保したDX推進SWG
トラストサービスのアシュアランスレベルの考え方

2022年2月8日

慶應義塾大学
手塚　悟

トラストを確保したDX推進SWGスケジュール（案）

2021年12月末

- トラストスコープで集中的にニーズやユースケースを検討する範囲特定
- 電子化できる手続・取引の主要事例

2022年3月末

- トラスト実態調査分析結果に基づく対応検討
- IDのアシュアランスレベル整理
- トラストサービスのアシュアランスレベル整理

2022年6月末

- トラストポリシー基本方針
- ユースケース選定
- 報告書とりまとめ（日・英）

出典：第1回トラストを確保したDX推進SWG資料1

トラストサービスのアシュアランスレベルにおける主な論点案

1 アシュアランスレベルの基準

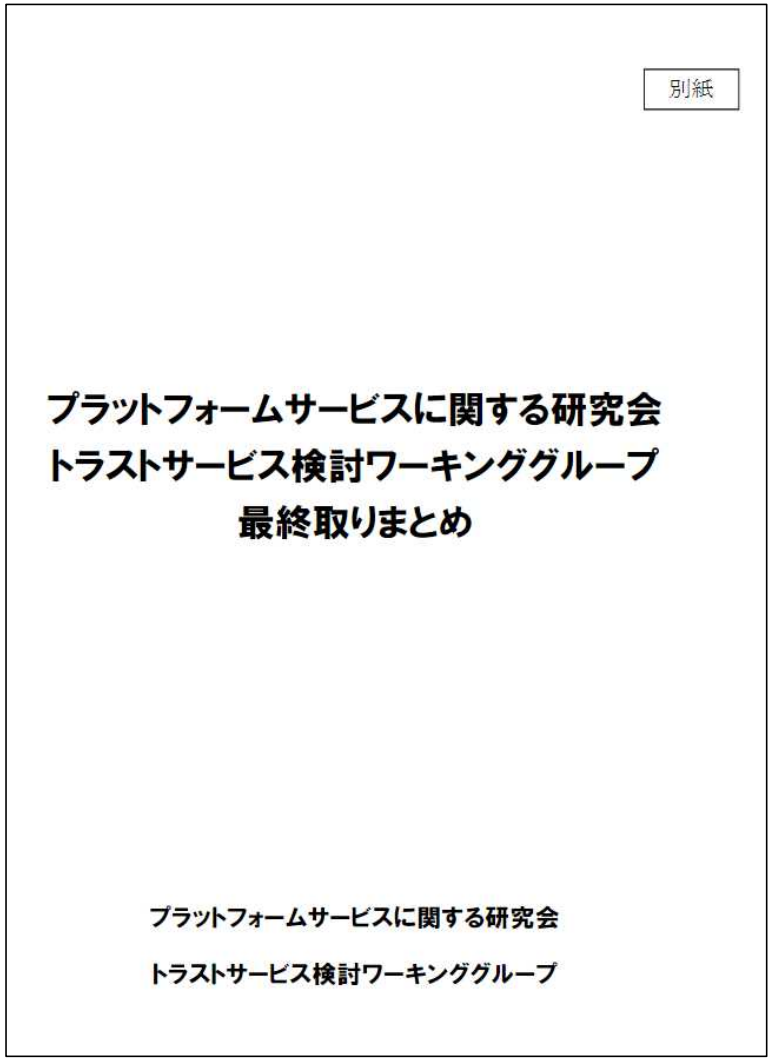
- トラストサービスのアシュアランスレベルに関して、どのような基準が考えられるか
- 考慮すべき要素（トラストレベルの担保、国際的な通用性、ユーザーへのわかりやすさ等）
- 具体的なユースケースにおける検討

2 機動性の確保

- 技術進化に対応した柔軟な見直しが求められる中、機動性の確保するための考え方
- トラストアシュアランスレベルの策定/運営の在り方

出典：第4回トラストを確保したDX推進SWG資料1

トラストサービスの定義（１）



別紙

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
最終取りまとめ

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

はじめに

サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）、Society5.0。

このような Society5.0 として実現される社会においては、ICT 機器の爆発的な普及や、AI の能力の飛躍的な増大とその活用に伴うビッグデータの分析・利活用の進展、すべての人とモノが繋る IoT (Internet of Things)等の社会実装が進み、社会のあらゆる場面でデジタル革命が浸透することで、今までにない、新たな価値が生み出されることが期待される。

Society5.0 の中核となるデータ駆動型社会（Data-driven society）では、良質、最新、正確かつ豊富なリアルデータが価値の源泉となり、経済社会活動を支える最も重要な糧となることが見込まれる。これは、とりもなおさず、経済社会を支える中核的な要素としてのデータの重要性が飛躍的に増大することを意味する。

このような様々な可能性を秘めるデータ駆動型社会においては、そのバックボーンとなるデータの真正性やデータ流通基盤の信頼性を確保することが極めて大切となる。そのためには、インターネット上における人・組織・データ等の正当性を確認し、改ざんや送信元のなりすまし等を防止する仕組み（トラストサービス）の実現に向けて、包括的な検討を加えることが必要となってくる。

また、海外に目を転じてみれば
に、その基盤を支えるために包括
うな国際的な動向も見据えながら
とが必要である。

このような状況を背景に、本ワーキンググループが「プラットフォームサービスに関する研究会」の下に設置された。本ワーキンググループは、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最終取りまとめとして整理した。

インターネット上における人・組織・データ等の正当性を確認し、改ざんや送信元のなりすまし等を防止する仕組み（トラストサービス）

出典：総務省　プラットフォームサービスに関する研究会　最終報告書（2020年2月）別紙
https://www.soumu.go.jp/main_content/000668595.pdf

トラストサービスの定義（２）

- 各種トラストサービスのイメージ

（ア）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（個人名の電子証明書）

（イ）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

（ウ）電子データを発行した組織として、組織の正当性を確認できる仕組み
→eシール（組織名の電子証明書）

（エ）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確認する仕組み
→ウェブサイト認証

（オ） IoT 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
→モノの正当性の認証

（カ）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
→eデリバリー

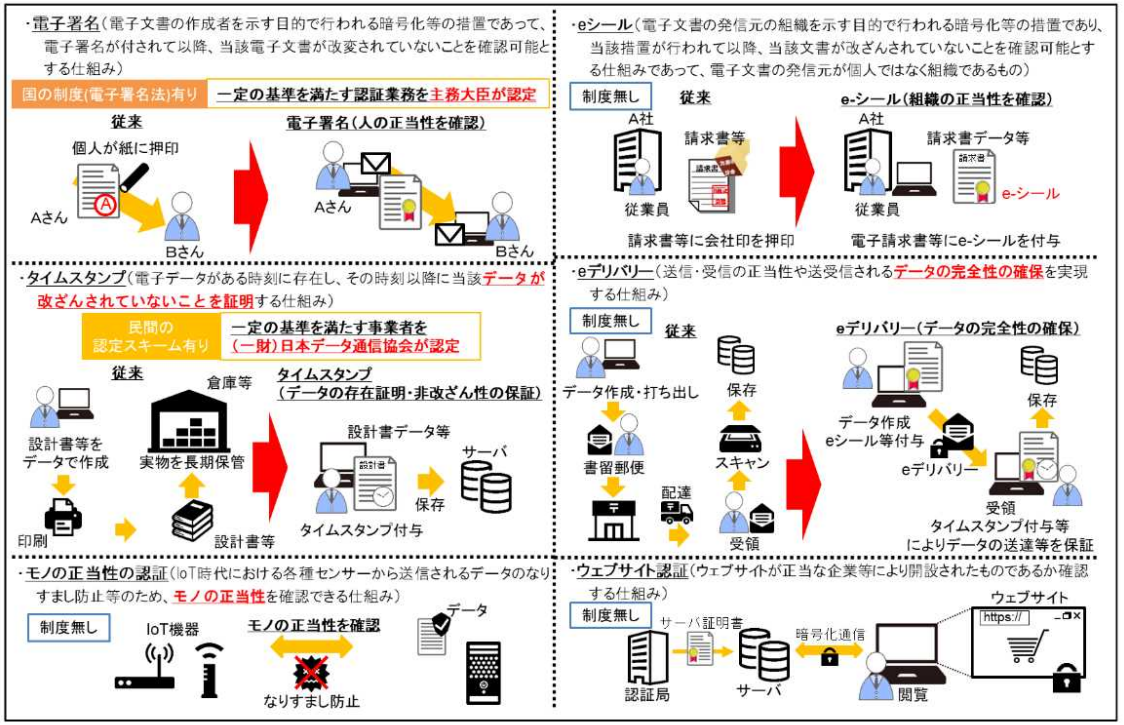
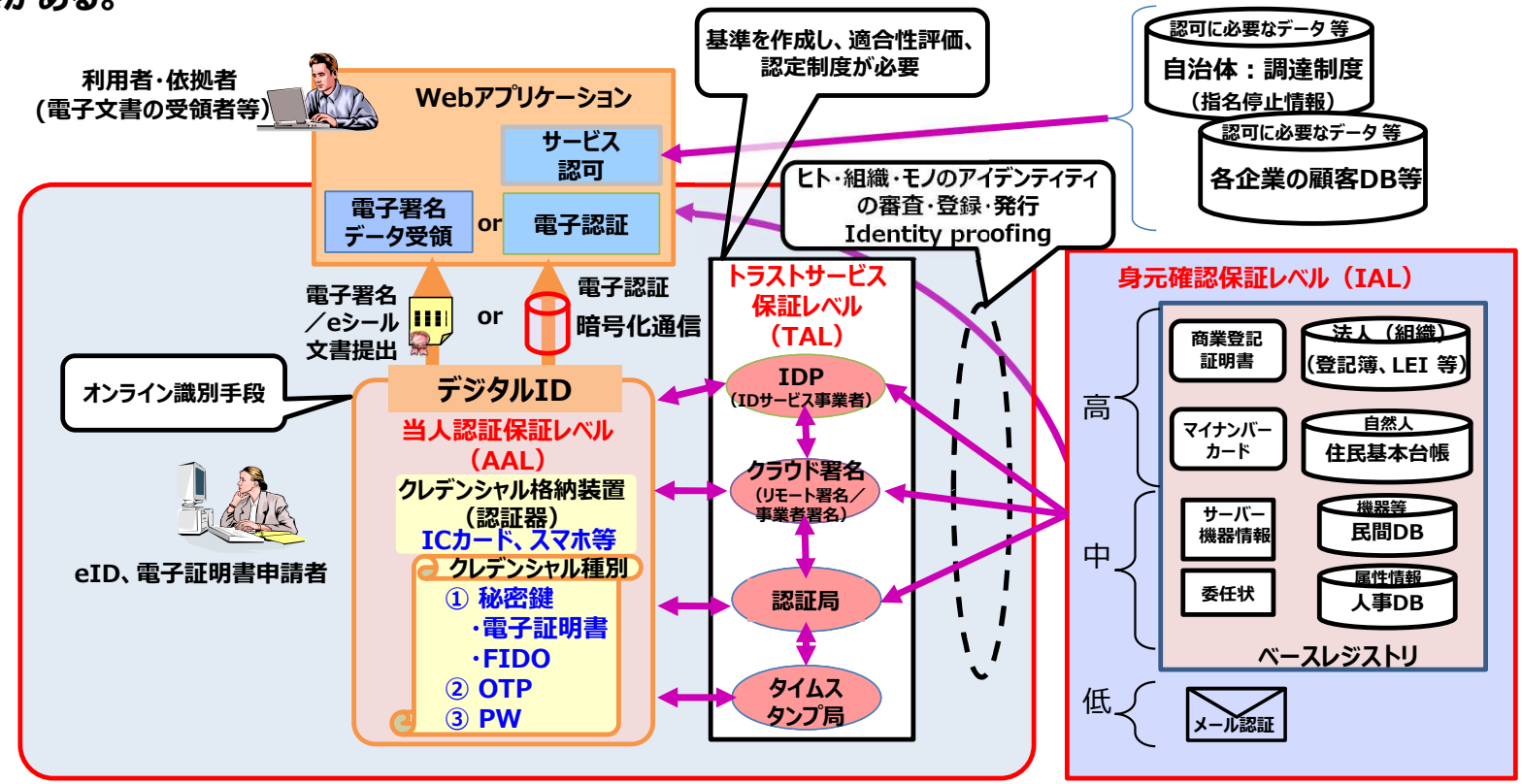


図 1 各種トラストサービスのイメージ

出典：総務省 プラットフォームサービスに関する研究会 最終報告書（2020年2月）別紙
https://www.soumu.go.jp/main_content/000668595.pdf

トラストの全体像（１）

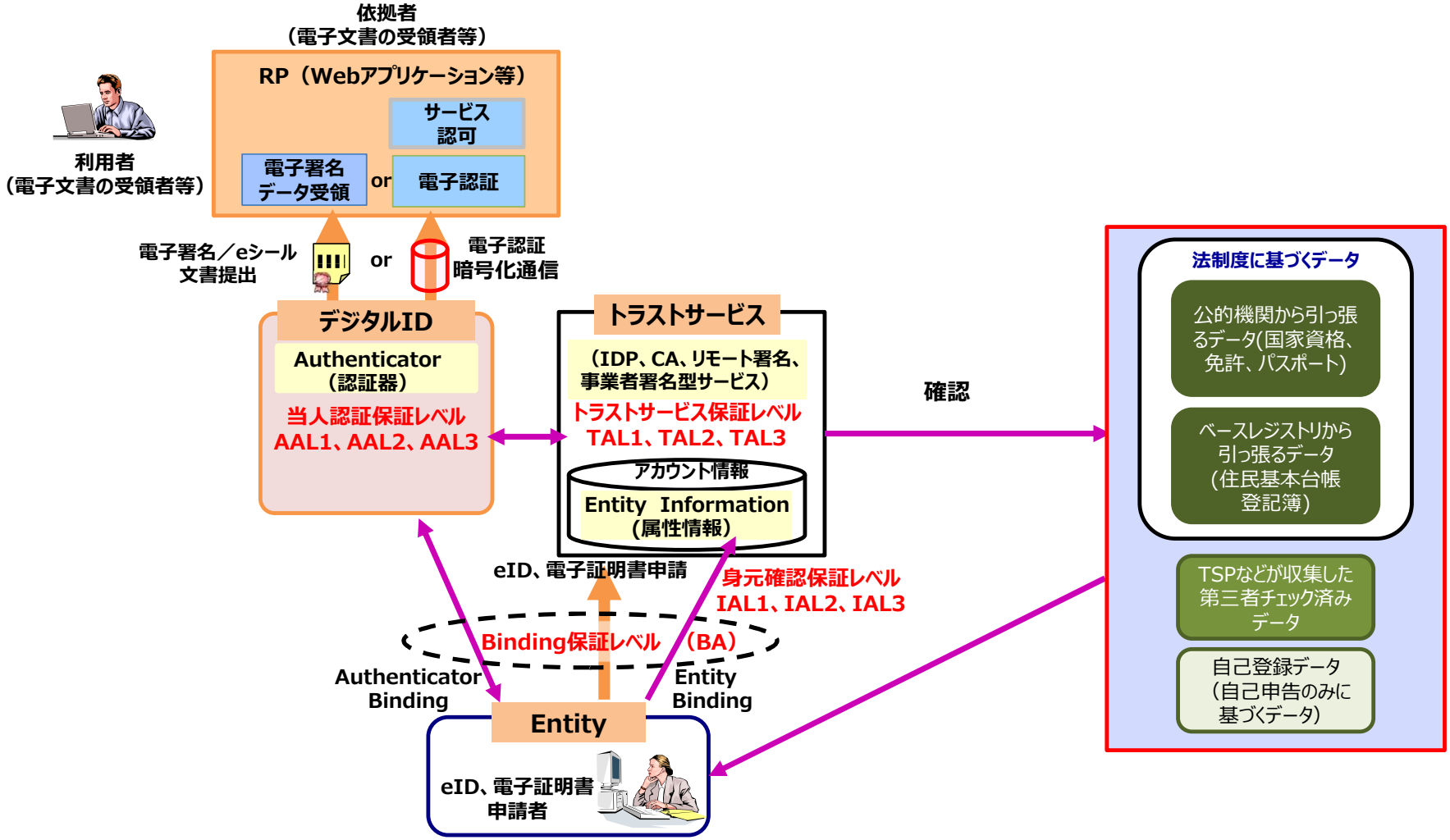
- トラストのレベルは、身元確認（IAL）、当人認証（クレデンシャル）の強度（AAL）、トラストサービスの信頼度（TAL）で決定され、手続き記録の真正性（証拠力）が求められる程度で電子署名もしくは電子認証が選択されうる。
- 従来は業務アプリケーション毎の判断で本人を確認しクレデンシャル（パスワード等）を発行し利用者を特定していたが、社会的混乱を防ぐためベースレジストリと紐づけたデジタルIDをトラストサービスから発行するスキームの創設が重要となる。
- そのためにはデジタルIDの保証レベルや、デジタルIDを発行するトラストサービスに求められる保証レベルを検討し認定制度を創設する必要がある。



出典：第1回トラストを確保したDX推進SWG資料5

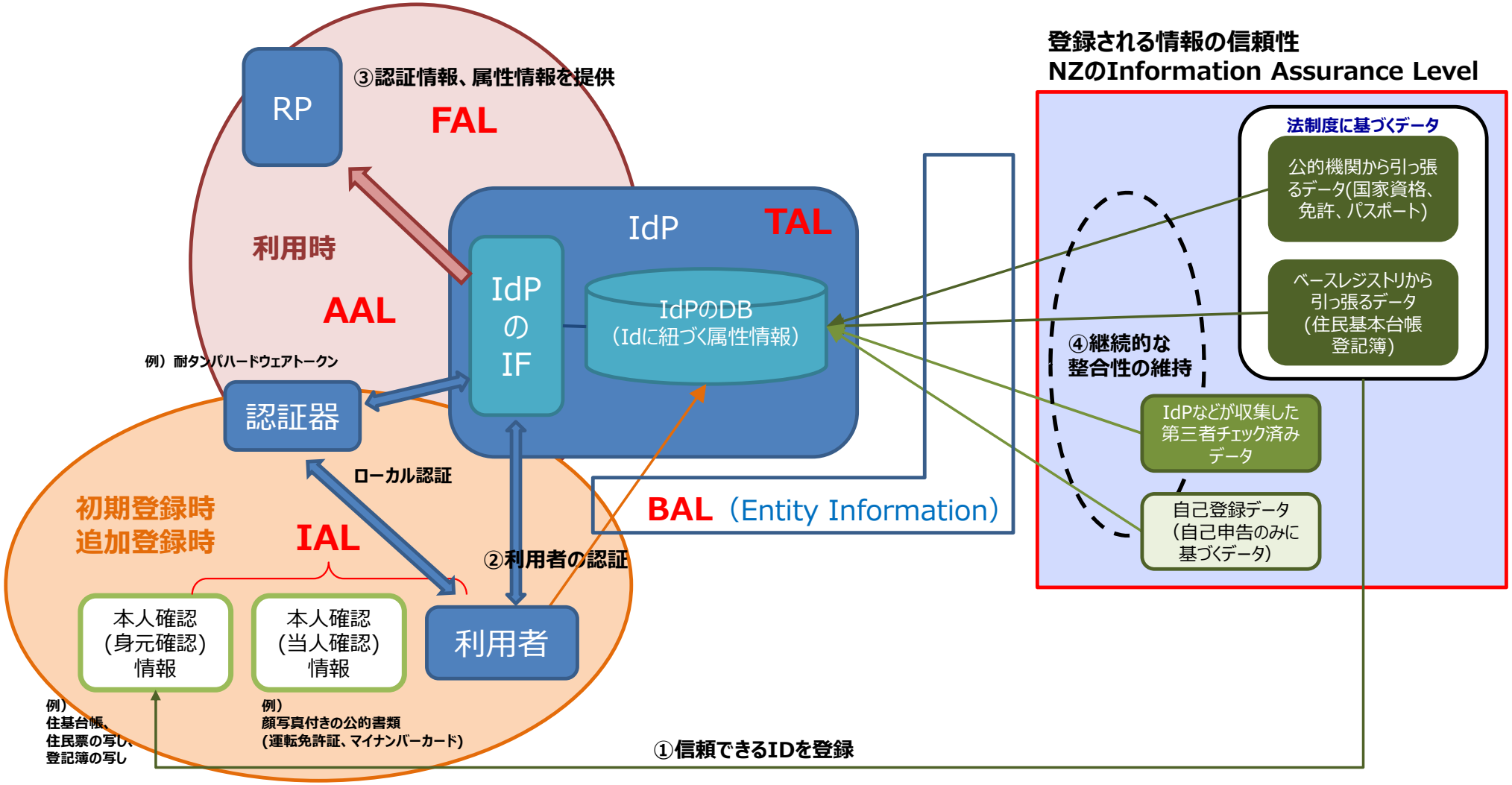
トラストの全体像（２）

●トラストサービスのアシュアランスレベルの全体像におけるBinding 保証レベルの位置づけ



IDPにおける各アシュアランスレベルの考え方

●Entity Informationの正確性のライフサイクルを通じた維持（属性情報変更の反映等）が重要



論点1：アシュアランスレベルの基準

- トラストサービスのアシュアランスレベルに関して、どのような基準が考えられるか

● トラストサービス事業者（IDプロバイダー、クラウド署名サービス※、認証局、タイムスタンプ局等）の運営ポリシーをトラストサービスアシュアランスレベル（TAL：Trust service Assurance Level）として整理すべきである。
  - 組織要件（組織の責任）
  - 設備要件（ファシリテイ要件）
  - 技術要件（暗号技術等）
  - 鍵管理要件（適格署名生成装置等）
  - 運用要件（複数人による相互牽制）
  - 監査要件（内部監査、外部監査、適合性監査、認定）
  - その他

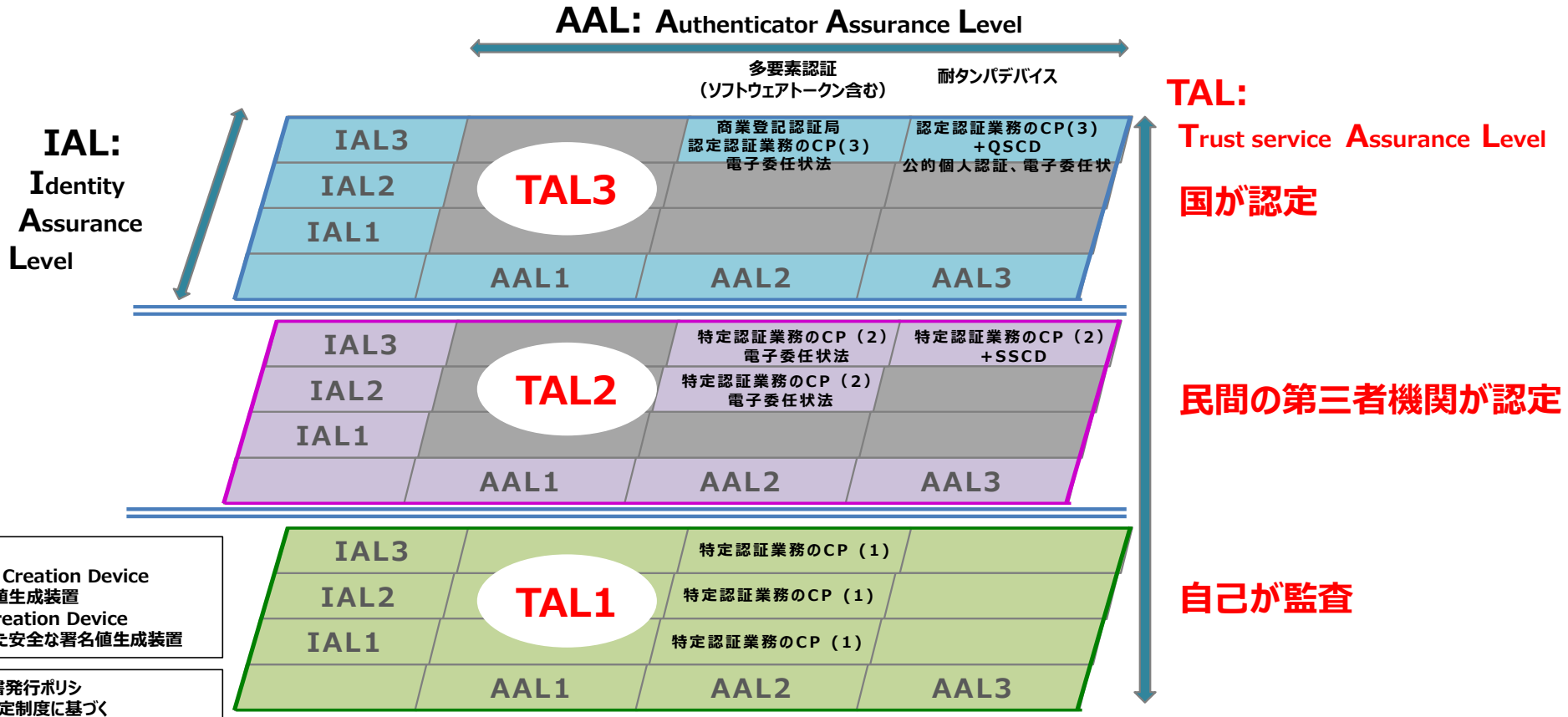
● これらをトラストサービスに共通する基準、個別の基準として整理し、TAL1、TAL2、TAL3のアシュアランスレベルを定義する。それぞれの認定主体としては以下を想定する。

  TAL3：国が認定
  TAL2：民間の第三者機関が認定
  TAL1：自己が監査

※　当事者の署名鍵によるリモート署名サービスおよび利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービス（令和2年7月17日　主務三省Q&Aより）

論点1：アシュアランスレベルの基準

- アシュアランスレベルの基準はIAL、AAL、TALの組み合わせから構成される。（下図は認証局を例にしたイメージ）
- IDプロバイダー、クラウド署名サービス、認証局、タイムスタンプ局等に対してユースケースに応じた基準を作成すべき。



耐タンパデバイス
QSCD：Qualified Signature Creation Device
国により認定された署名値生成装置
SSCD：Secure Signature Creation Device
国際規格により認定された安全な署名値生成装置

CP: Certificate Policy 証明書発行ポリシ
認定認証業務のCP (3)：国の認定制度に基づく
特定認証業務のCP (2)：信頼できる民間の監査制度に基づく
特定認証業務のCP (1)：上記以外の認証業務

論点1：アシュアランスレベルの基準

- 考慮すべき要素（トラストレベルの担保、国際的な通用性、ユーザーへのわかりやすさ等）

● トラストレベルの担保
  - ニーズと基準や制度との整合性を担保する必要がある。
  - 各トラストサービス固有の脆弱性に対する「脅威耐性」ベースでの検討が必要である。
    （例:同じ設備要件でもトラストサービスにより対象やレベルが異なる）

● 国際的な通用性
  - 国際的な基準との整合性や関連基準の参照をする。
    （ISO/IEC 27000シリーズ、CAB/F baseline requirement、ETSIやCEN規格、Webtrust監査基準、等）
  - 適合性評価機関の国際的な整合性確保
    各トラストサービスに対し上記基準への適合性評価を行う機関の要件を国際標準（ISO/IEC 17065、ETSI EN 319 403など）を参考に規定する。

● ユーザーへの分かりやすさ
  クオリファイド(TAL3)、アドバンスド(TAL2)等、どのレベルを満たしたトラストサービスであるか、利用者にとってわかりやすい仕組みの検討が必要である。
    （認定トラストサービスの機械可読な形での公開や、署名検証など当該トラストサービスに基づく情報（署名値やタイムスタンプトークンなど）の検証などの利用時にどのレベルのトラストサービスであるかユーザーが分かる形の基準策定）

論点２：機動性の確保

- 技術進化に対応した柔軟な見直しが求められる中、機動性の確保するための考え方

● 各基準は法令から参照される独立した技術規格として策定されるべきであり、変化する技術進化や国際標準に対応したメンテナンス性が確保される必要がある。

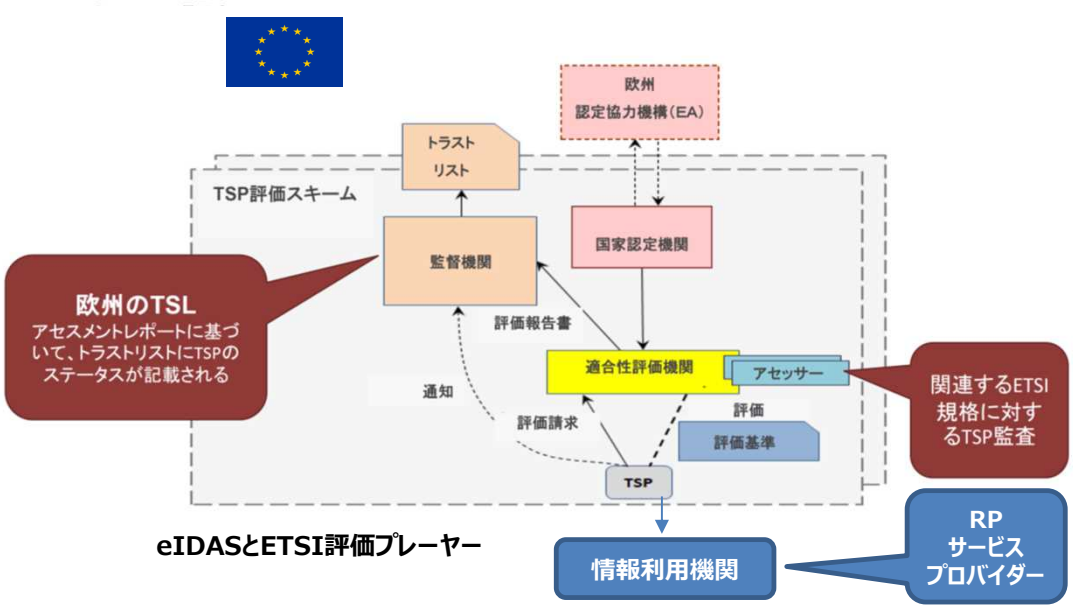
- トラストアシュアランスレベルの策定/運営の在り方

● 各基準は諸外国の標準などを参考に国の関与の下に、トラストサービスフレームワークに対応してクオリファイドレベル(TAL3)とアドバンスドレベル(TAL2)等に応じて作成することが必要である。

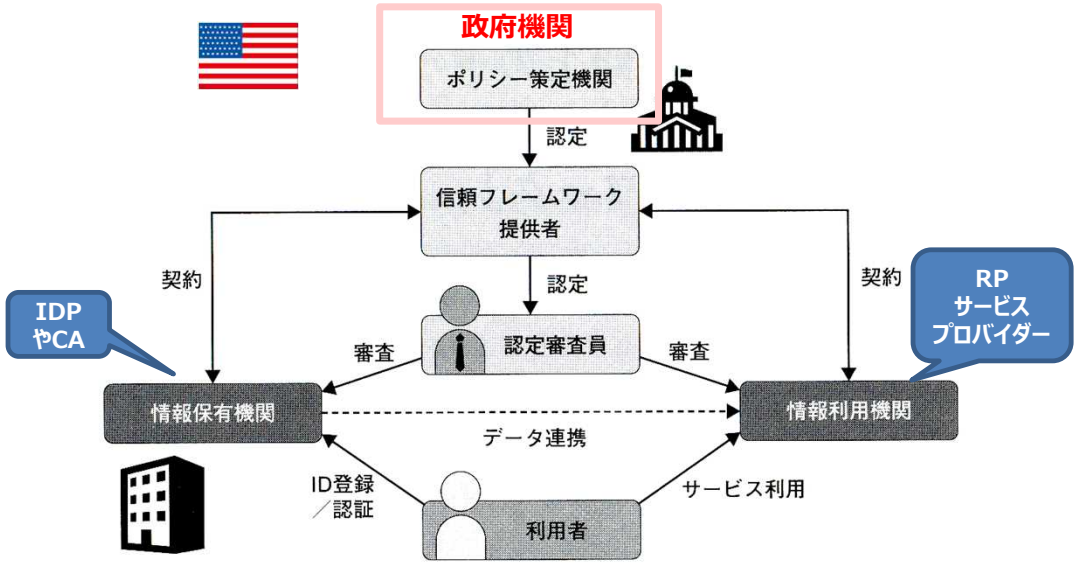
● 変化する技術進化や国際標準をウオッチし適時、適切に基準のバージョンアップを行う体制、運営の在り方の検討が必要である。

海外のトラストフレームワーク

●欧州、米国のトラストフレームワークを比較すると、そのポリシーは両者とも国(政府）主導により策定されている。



eIDASとETSI評価プレーヤー



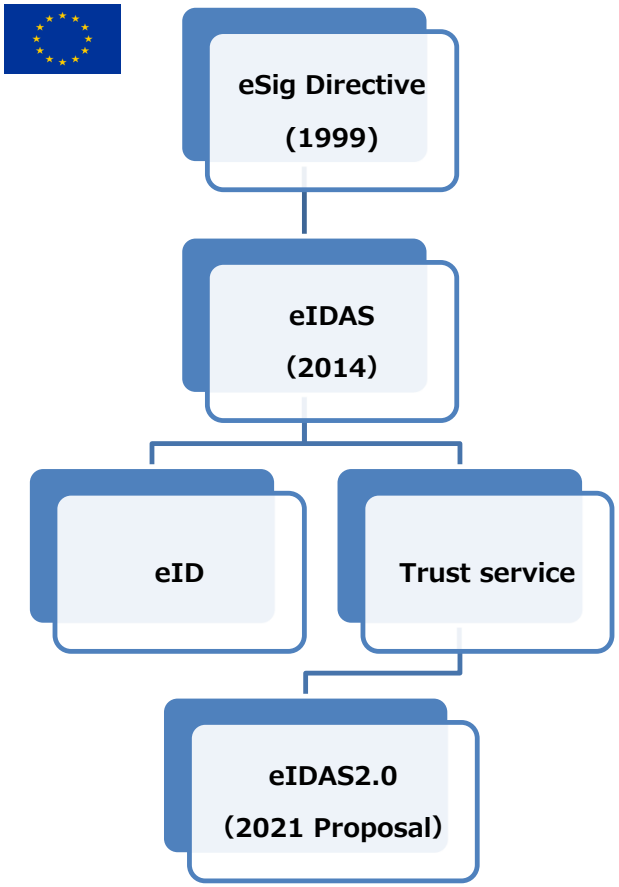
図表 9-1　アイデンティティー・トラストフレームワークの構成
出所：山中進吾『信頼フレームワーク最新動向』（2011）を基に筆者

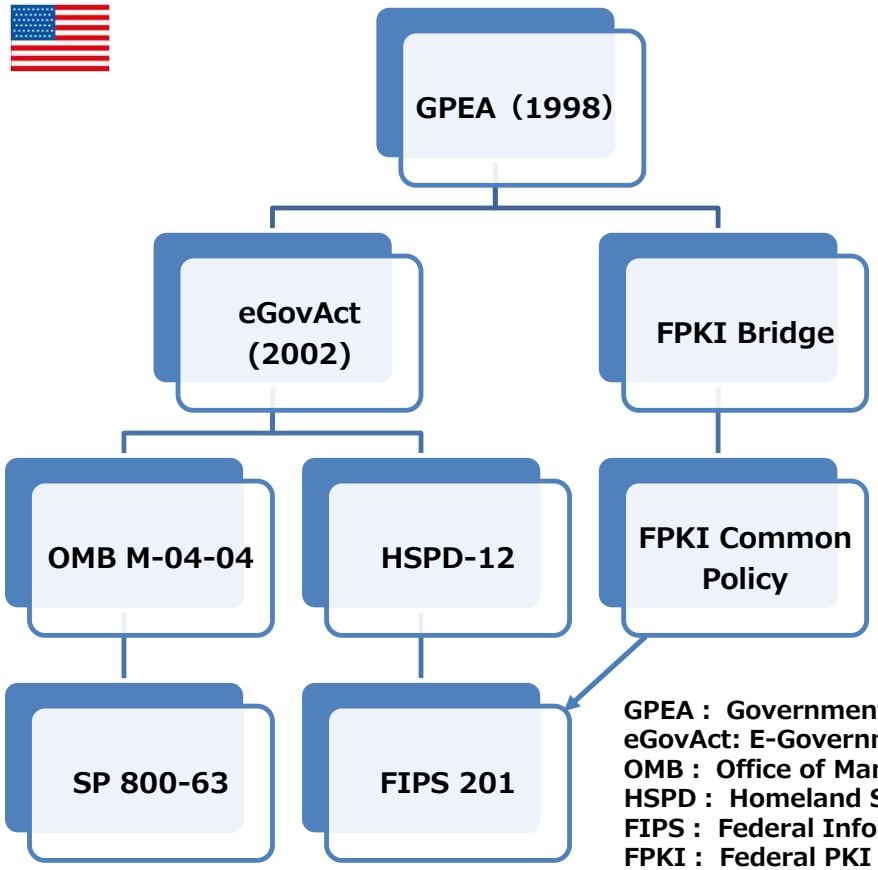
TUViT Clemens Wanko
Audits based on ETSI CP for qualified TSP and global recognition
Japan-Europe Internet Trust Symposium
July 4 th , 2017 を参考に追記

崎村夏彦,「デジタルアイデンティティー」,日経BP,2021年7月20日 を参考に追記

海外の制度化プロセスの事例

●欧州、米国の制度化プロセスを構成する法制度やポリシー、技術基準の概要は、以下となっている。





GPEA： Government Paperwork Elimination Act
eGovAct: E-Government Act
OMB： Office of Management and Budget
HSPD： Homeland Security Presidential Directive
FIPS： Federal Information Processing Standards
FPKI： Federal PKI

主な国際的なトラストフレームワークの比較表

Table 4: Comparison between the trust frameworks (based on (Hamaguchi, 2016))

	ETSI	WEBTRUST	eIDAS	FPKI	ISO 27000
Law	Supports eIDAS Regulation	N/A	eIDAS Regulation	e-Government Act of 2002	N/A
Objective	Technical interoperability and trusted third party assessment	Technical interoperability and trusted third party assessment	Legal recognition of electronic trust services	Identity management and trust across organizational, operational, physical and network boundaries	Information security
Governor	ETSI Board	N/A	EU Committee	CIO Council	
Harmonization Body	ETSI ESI	PKI Assurance Task Force	FESA	N/A	
Accreditation Body	National Accreditation Bodies	CPA Canada	NAB	FPKI Policy Authority	National Accreditation Bodies
Conformity Assessment Body	CAB accredited to EN 319 403	Same as above	Conformity Assessment Body	FPKI Certificate Policy Working Group	Conformity Assessment Body
Supporting Technical Standards	ETSI Standards, CA/B Forum: BRG, EVCG + NetSec	WebTrust Criteria	ETSI Standards, CEN Standards	NIST SPs, FIPS 201, FPKIPA Documents	
Assurance to be achieved	Best Practices and Legal Compliance	Best Practices	Legal Compliance	Technical Compliance, Interoperability with FPKI system	Technical Compliance to Management Requirements

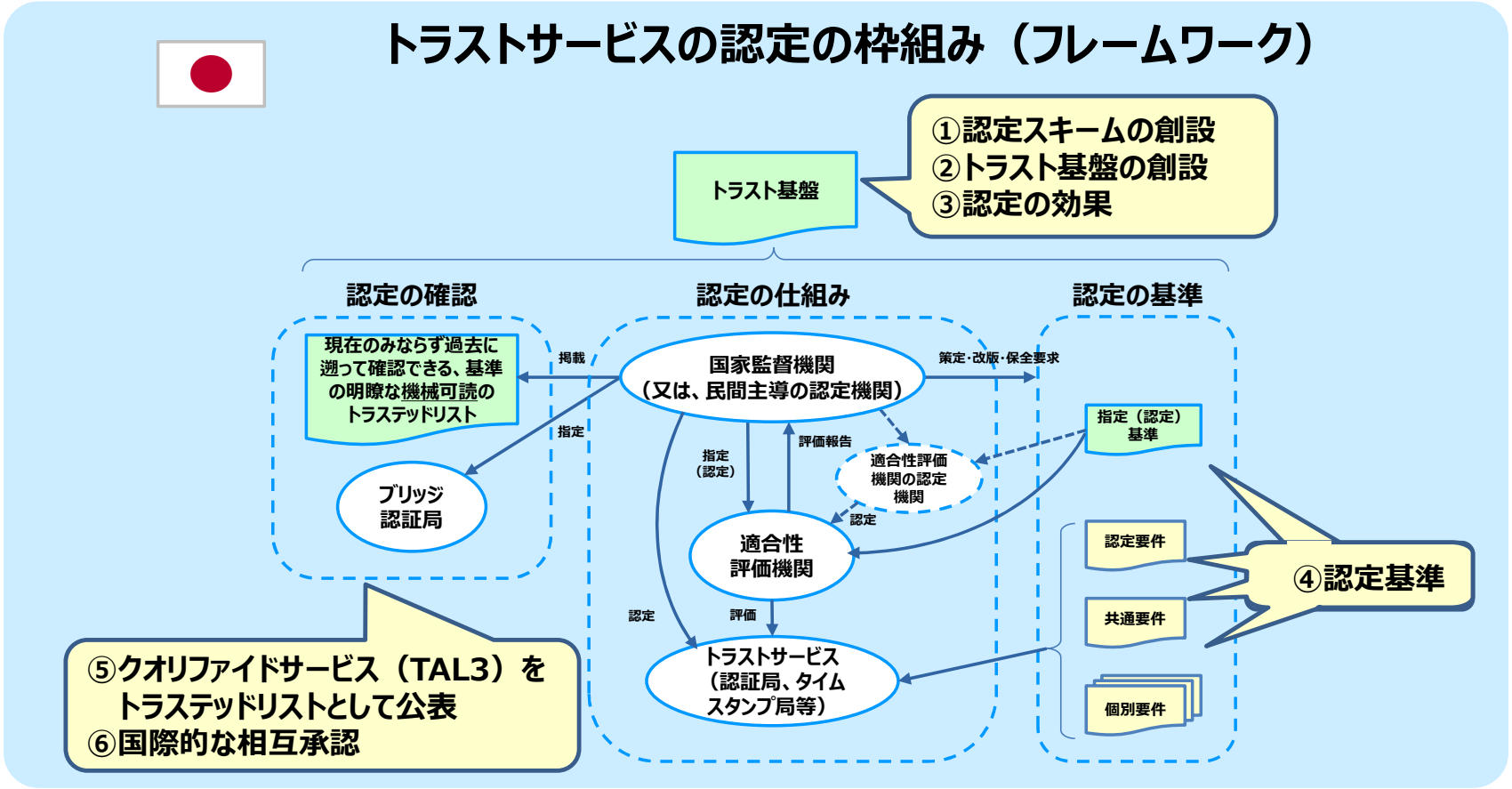
https://www.enisa.europa.eu/publications/towards-global-acceptance-of-eidas-audits

日・EU・米国のトラストフレームワークの比較表

	EU	米国		日本（案）	備考
当局	欧州委員会	米国国土安全保障局	Federal CIO Council	デジタル庁	欧州も米国も政府機関
レギュレーション	eIDAS	FISMA NIST SP800-63	e-government Act Common Policy root CA	トラストポリシー	欧州は法で規定、米国は国立機関で規定
トラストフレームワークプロバイダ	EU 各加盟国	Kantara Initiative（KI）	Certipath Bridge CA	民間TFP（TAL3は国に限る）	欧州は各加盟国、米国は政府機関または民間団体
審査基準	ETSI,CEN 規格群 ・ETSI EN 319 401（一般ポリシ） ・ETSI EN 319 411-1（証明書発行者のポリシ） ・ETSI EN 319 421（タイムスタンプ局のポリシ） 等	KI Identity Assurance Framework（IAF）およびService Assessment Criteria（SAC）	CBCA CP	官民共同スキームによる策定（国が一定関与）	欧州は欧州委員会の指示の下、標準化団体で策定 米国は政府機関または民間団体で策定
認定審査機関	適合性評価機関（CAB）のAssessor	KI Accredited Assessors	Assessor	適合性評価機関等	欧州は認定機関から適合性評価機関としての認定を取得、米国はフレームワークによって異なるが自己宣言型も認められている
公表	トラステッドリスト	トラストレジストリ	FBCA	トラステッドリストおよびBCAのハイブリッド	欧州はトラステッドリスト、米国はFBCA及びリスト方式

トラストサービスの認定の枠組み

- TAL3に関するトラストサービスの国による認定の枠組みを検討すべきである。

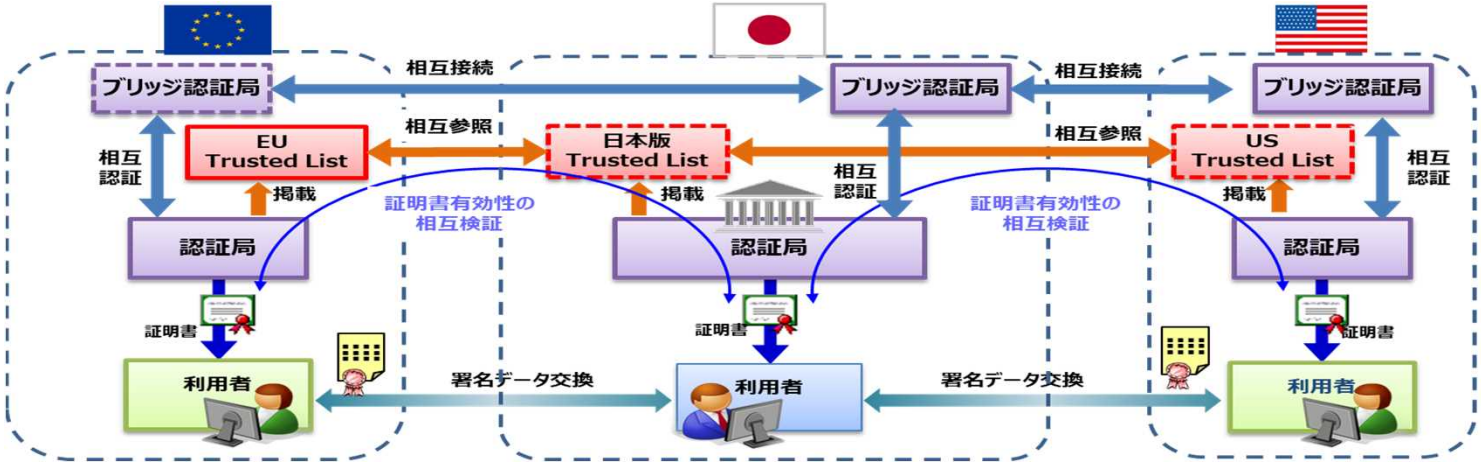


出典：第7回データ戦略タスクフォース資料1を参考に追記

トラストに関する国際的な相互承認

●国際間の利用者が相互に適格性を確認できるように、以下の項目の同等性などを検討し、相違点を補完することが必要である。

	項目	論点	国際相互承認のために必要な施策
1	法制度	論点① トラスト基盤の創設 論点② 国（又は、民間機関）による認定フレームワークの創設 論点③ 認定の効果	・トラストサービスの認定に係るフレームワークの同等性 ・国（又は、民間機関）による認定フレームワークの確立 ・トラストサービスの効果の同等性
2	監督・適合性評価	論点④-4 適合性評価機関の適合性	・適合性評価機関の要件の同等性 ・指導・監督の仕組みの確立
3	技術標準	論点④-1 トラストサービスプロバイダの共通要件 論点④-2 認証局の要件 論点④-3 タイムスタンプ局の要件	・技術標準の作成・維持の体制の整備 ・技術標準の同等性に関する検討
4	トラストアンカー間の接続の仕組み	論点⑤ クオリファイドサービスをトラステッドリストとして公表	・トラステッドリスト方式とブリッジ方式の併用



出典：第7回データ戦略タスクフォース資料1

資料１８

サービス提供におけるトラスト確保を実現するポリシー策定の論点

LocationMind株式会社 取締役
株式会社パロンゴ 取締役

林 達也

2022/2/8「トラストを確保したDX推進SWG #5」

ご提案 (Recap)

- 「先ず、隗より始めよ」
- 行政手続き(Government Sector)におけるサービスで実際に試す
- スモールスタート可能なユースケースを選ぶ(G2B or B2G)のはどうか
- 「トラストサービス」の定義を行う

背景

■ **eIDAS 1.0は、日本で暮らすうえでは影響を受けるものではなかった**
- 議論として参考になった側面は大きく、偉大な先行者
- 一方、EUという国と国をまとめる必要がある特殊な状況下で求められる取り組み
- 実際には、背後にISO等の国際的な標準を引くことで技術的な裏打ちとしていた

■ **NIST標準は、アメリカの政府調達を主眼としており、軍事も含めた包括的なもの**
- 我々は深い洞察をせず、NIST標準を文脈を意識しないで多くの参考にしてしまった
- 彼らもまた先行者であり、我々はeIDASと同じようにNISTも参考にした
- (もちろん、他の多くの国際標準も)

■ **今まで、我々は後手であった点が多分にある**
- もちろん、先行しているケースもあるが…

民間では自分はよく「(先行)事例病」と呼んでいます

■ **では、我々が、本来汗をかくべき部分はどこなのか**
- 日本に固有の状況において必要な補足・補遺・補正を行うべきではないか
- なぜ、『海外のものはすごい』となってしまうのか
- 『日本版XYZ』のようなアプローチはそもそも適切なのか

現状

- 2022年2月において我々は、デジタル庁が発足し、EUはeIDASは2.0と言い出し、NIST SP800-63-4の登場が近づき、大多数の人々がスマートフォンを常時携帯し、マイナンバーカードの改定も議論される、という『潮目』の時期にいる
- コロナ禍において人類の活動のオンライン化は促進され、物理的な制約を如何にしてデジタル化し、オンラインで実現するかが焦点となった
- 政府だけでなく民間でも、国内・国際ともに、Identity Proofing (KYC)やAuthentication/Authorization、Notice and Consent、パーソナルデータ、データの流通や真正性、等々が重要視されるようになった

今まさに社会的環境条件が大きく変わりつつある

小さくても手を動かすべき時期

補足：ID Proofing / KYC関係の国内活動

■ デジタル庁
- トラストSWG(本WG)
- 「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」(2019年2月25日)
  - 改定の要望・必要性が高く、取り組むべき(本項にはバイアスがかかっています)

■ IPA 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
- 経済産業省「オンラインサービスにおける身元確認に関する研究会」の実質的な後継プロジェクト

■ OpenID Foundation Japan KYC WG

■ JNSA「オンライン身元確認(eKYC)金融事例調査報告書」

■ etc...

前提整理

■ **本SWGでいう「トラストサービス」の定義をきちんと行うべき**
- 「eIDAS 日本語版」、ではおそらくないだろう
- では一体なんなのか、どこまでが範囲なのか
- その目的は何か？ -> ユースケース？

■ **民間との接合をどこまで視野に入れるのか**
- その是非はさておき、立会人型で十分、という社会実態をどう捉えるべきか
- アメリカに近しいIT業界や、欧州に近しい自動車等製造業の差異
- 領域は違うが、「個人情報保護」や「プライバシー」の分野も、同じく各国を睨むことになっているのが民間の実態

■ **純粋な政府主導のサービスは、そう簡単には社会受容されない**
- 民間の方がはるかに進んでおり、護送船団のような発想はもう終わっている
- 代替手段があって、価値があれば(要件を満たせば)そちらが使われる
- ただし、罰則などがあれば別

■ **サービスそのもので担保されなくても、商習慣や契約等で実態としてカバーされているものは多い**
- 日々の生活がかかっている以上、これは当然
- そこに大きなペインポイントがあるか？

トラストサービスの位置づけ

■ DXを推進するとはなにか
- 目的は何をどう変えることなのか

■ 何のためのトラストサービスか
- トラストサービスは、サービスであり手段
  - 正確には、今まで本SWG等で議論されているインフラやコンポーネントに近いサービスは、その一定の汎用性から手段である
- 「なんにでも使える魔法のトラストサービス」はおそらく存在しない

■ UXがひどくても、コストが高価でも、どうしてもそれでないと実現できないサービス
- -> 多くのひどい(行政)サービスの山
- 問題から、競争原理の一定の価値が見いだされるところ
- 是非はさておき、現在の「なんとかTech」の興隆はこの点にある

■ 実態実務で使われているが、細部の詰めが甘いサービスを、適正に変えていく要素
- 慣習や長期的視点、消費者保護など、民間ではおろそかにされやすい、せざるを得ない側面を指摘し、強化を促す
- e.g.)「既知であったことの証明」「発案者であることの証明」「犯罪収益移転防止」

「トラスト」の特性と本質

■トラストの特性

- 本来は技術の話ではない
- 社会制度の大きな一部
- 一朝一夕には変えられないもの
- 時間をかけて得られるもの
- 認知の問題
- 社会受容性を伴う

■トラストの本質

- 「醸成」できるようなものなのか
  - ▸ 本来、個々人や主体が自然発生的に生じるものではないか
- それを踏まえた上で、それを社会制度として補強する
- 仮に「裏打ち」をするのであれば、「保証」も担保しなくてはならない
- 制度と技術の構成要素の話をすると混乱する

トラストSWGにおける、制度と技術の区別

■ トラストサービス

- デジタルテクノロジーを如何にして社会的にトラストしてもらえるようにするか
- 「技術的な」側面から、それを満たす条件や運用形態、あり方を論じている
- 専門性が高く、変化の速い、まだまだ試行錯誤が必要な未知の領域
- (他国は、一周目を終えて二周目に入ろうとしている…?)

■ トラストに関する制度

- 古くから存在し、事象をどう捉えるかを常に入念に検証せずとも、「複雑性を縮減」(ルーマン)するために、いわば「決め打ち」をするための外縁を定める行為
- 人間同士、村同士、村と人、等々、「関係性」の連鎖を「容易には改ざんし難い」要素で定めていく
  - それでも、トラストは100%ではなく、一定の確度でしかないと多くの人は認識している
  - そして、そのトラストは裏切られることもある(技術としてのトラストとの意識差がある)
- 社会生活を営む中で法律や制度として定める必要があるものの中に、トラストの要素は数多く存在する
  - 人類がこれをうまくできているかは別の問題
  - ただし、これは経験値によるラフコンセンサスの中から、いわばデファクトとして社会制度化されているように思える

参考：トラスト・信頼の難しさ

■「信頼を考える: リヴァイアサンから人工知能まで」(小山 虎著)

■本書で取り扱われる主な対象領域

- 経済学
- 心理学
- 社会心理学
- 社会学
- エスノメソドロジー
  - (「人々の – 方法論 (ethno-methodology)」)
- 動物行動学
- 哲学
- etc...

トラストの「正しい」連鎖

■ マイナンバーカードやベース・レジストリを活かす
- これらは大きな努力によって実現してきた「トラスト」
- おそらく、社会的には登記関係なども同様
- これらのデジタル化がこの瞬間の重要な転換要素

■ 信頼できる点から点への連鎖
- Root of Trustであり、これは例えばベース・レジストリだが…
- ひとつの重要要素は「不変性」

■ 正しい連鎖を作るには「要件」が必要

■ ただし、ポリシーで求めるべきは「正しい連鎖」の実現、評価方法までであって、要件はきちんと時代(四半期レベルの変動)と技術に合わせて変更可能な社会制度であるべき

トラストサービスが目指すべき目的

■ **トラストサービス(未定義)は、暗黙の裡に以下の仮定をおいている**
- Xをトラストサービスだと認めるYによって、Xはトラスト可能だとされる
- それを聞いたAは、自分にとってのY、またはそれに類する(と推測する)なにかへの信頼と近しいものとして、Xをトラストする
- 信頼を複雑性の縮減と捉えるならば、トラストサービスを定義し制度化することは、対象に対する入念な検証を行わずとも利用していいことを明確化することに他ならない

■ **トラストサービスの定義の必要性**
- どういう目的の手段として信頼し利用できるサービスなのかを明確化することに他ならない
- それを使えば無条件で安心できるサービス…?

■ **トラストサービスが目指すべき目的は何なのか**
- 手段や部品だけを用意しても、使われなくては意味がない
- 毎日使うものなのか? 土地売買のような時にのみ使うものなのか?
- ユースケースの明確化が必要
  - e.g.) 国家間の調印行為のデジタル化等

■ **トラストするという行為は、長期的に保証されることと同義**
- インターネット社会はまだまだこれは難しい事象

個の観点で実現されて欲しいこと (ID/認証及びID Proofingの観点で)

■ オンライン上の本人手段の確立
- 攻撃に耐性があること
- 文脈ごとのデファクトスタンダード
- まだまだ成熟していない途上の状態

■ オンライン上で選択可能なペルソナによる、選択的属性開示可能なID/認証の仕組み
- デジタル社会の共通機能として、まだまだ端緒にも至れていない

■ マイナンバーカードの位置づけは非常に難しいと感じる
- 日々、人生を揺るがすレベルのクレデンシャルを持ち歩くのか
- 失くした時の恐怖心もあるが、一方、持ち歩いたら実はとても便利になる可能性もある
- さらにスマートフォンに搭載されたらどうなってしまうのか
  - もしかしたらUXによりスマホ版マイナンバーカードは豊かになるかもしれない

目的に合わせた適切なレベルの利用

■ なんにでも最高レベルのものを使えばいいわけではない
- 「実印相当」等の物理世界の既存制度の比喩表現をデジタルテクノロジーに適用するのは個人的にはとても不適切だと思うが、それであっても「なんにでも実印は捺さない」だろう
- 何をどうやって担保するのか、Single Point of Failureにならないか、リスクはどうあるのかを考えるのはとても重要

■ レベルは高ければいいわけではなく、使い分けられることこそが重要
- 大は小を兼ねない

■ 高いレベルのものを定義することで、そこから下位のレベルのものを作り上げることが可能

■ エコシステム全体のコストとベネフィットを計算しなくてはならない
- これを数値として明確化できる材料を提示するのはポリシーの役目
- 仮定として、トラストサービスを民間が運営するのであれば、費用対効果が一定程度明確ではなくては成立しない
  - Web PKIやタイムスタンプ認証局での学びを活かす必要がある
  - 我々はいまだ、放棄ドメインの再利用にすら対応が出来ていない

■トップダウンの必要性

- 発展途上の場合、サービスの定義をゼロから国が主導して実施する必要があった
- EUの各国をまとめあげるのは事実上困難であり、EUデジタル単一市場など、強制的にトップダウンで実施する「必要性」があった
- 問題のある認証技術や本人確認手法では社会全体に問題が波及するため、問題のある部分を、必要に応じて変更するよう定義してきた

■ボトムアップの必然性

- デジタルの世界において、政府よりも民間が先を走っていることは避けがたい事実
- トップダウンでなにが言えるほど、我々はリソースを正しく投じていない
  - これは今から少しずつ手を付けるべき、だが…
- 現状は、民間のデファクトスタンダードが社会を動かしており、政府が行う役割は「コストであってもやらなくてはいけない最低限の対策」

Small StartとBig Picture

Small Start (実務主導)

- 先ず、きちんと我々で実績を積み重ねることが重要
- 日本としてSmallな検証を進めていくべき
  - 絵にかいた餅ではなく、実利のあるDFFTへの道
  - この瞬間、正に始めるべき議論
  - 良い面も悪い面も含めて、日本の特殊性をもとに話をするべき
- 正しくTransformationすべきものは山ほどある
- これを進めることで、トラストサービスに求められる最低限のポリシーとその体制についての知見が一定程度明確になると思われる

Big Picture (技術主導)

- マイナンバーカードの普及が一般的となり、スマートフォンの保有が当然のことになっている状況下で、Small Startした実績からフィードバックしつつ、大きなフレームの議論は、数歩先の未来を想定してゼロベースで検討すべき
- 極限の安全性を考えるならば、厳しい条件下でのみ要求される実務はなにで、どう運用するのかを明確にする必要がある
- そしてなにより、それをどう普及させ、スケーラビリティを得るのか
  - これは、上位のレベルのものが、より日常的に使いやすい下位のレベルのものを生み出すことにもつながる
- 最終的には、広く社会に受け入れられるかが評価のポイント

DXサービスに寄与するトラスト確保を実現するポリシー策定の検討課題

■ 最小限、サービス提供者に求めなくてはいけないことはなにか
- 資本金？上場？事業継続性？
- 100年持つサービスがどれだけあるのか
- 100年持たないトラストサービスに意味があるのか
- (少なくとも行政サービスは形態を変えても正しく継続し、正しく終わることが期待できる可能性は高い＝信頼？)
- 持たないのであれば、どうすればいいのか
  - サービスが提供するものが短期間に収まればよい？

■ インセンティブとディスインセンティブ
- 使う理由が必要
- 信頼を損なう行為には厳しい罰則を
  - 例えば売り上げのx%など
  - 1億円程度では防止にならない領域は多々ある

■ トラストサービスにおいて政府や制度でなければ出来ないことはなにか
- 我々はeIDASがなくても経済活動を行っているし、Web PKIもInternetも国家には依存していない
- 一方、個人情報保護法のように、法や制度で守られることが重要なものがある

ポリシー作成における要素・要点(私見)

■ **方向性**
- ブレない方向性の提示、趣旨、あるべき姿の提示
- 利用者と提供者それぞれへのインセンティブとディスインセンティブ

■ **安定性**
- 長期間の有効性
  - 持続性と経済性
- 社会的有効性(裁判?)

■ **最小性**
- トップダウンで定義するポリシーの内容は、最小限のものが望ましい
  - 本SWG構成員からも同論の意見があったと認識
  - エンジニア的観点として、個人的には、法律等にbit長やアルゴリズムを書くことはナンセンスだと考える

■ **柔軟性**
- 技術的・経済的アジリティを確保するために必要な要素として、変化を受け入れ可能にしておくことは重要

Appendix B

BCG BOSTON CONSULTING GROUP

トラストサービスに関する アンケート実態調査の報告

デジタル庁

トラストサービスのニーズ及び現状等 (インタビュー・アンケート結果より)

トラストサービスのニーズ

「行政」に加え「民間」でも、業種を問わず、オンライン手続きへのリスクヘッジのために、トラストサービスへのニーズがある

- デジタル/オンラインでの厳格な本人確認 (他人になりすまされるリスクの回避)
- データの改ざん防止・真正性の担保 (データの改ざん／偽造リスクの回避)
- データの法的効力の担保 等

中でも、トラストサービスのニーズが大きく・強いのは、上記のうち、
「業種共通」の社外取引等のほか、「金融」「情報通信」「不動産」「医療」「運輸」で業種固有のもの

- 業種共通：「受発注」、「契約」、「請求」 などの社外取引、「会計帳簿」などの社内取引
- 業種固有：
  - 金融：「銀行/証券口座の開設」、「為替取引」、「保険の契約」、「融資/ローン契約」、「為替取引」等
  - 情報通信：「携帯電話の契約」等
  - 不動産：「不動産売買/賃貸契約」等
  - 医療：「健診/検査結果の発行」、「診断書の発行」等
  - 運輸：「通学定期の発行」等

トラストサービスの現状の利用率、課題意識、今後のトラストサービスの基盤整備・普及に向けて考えられる施策例への関心

現状のトラストサービスの利用率は以下の通り

- 企業: 電子署名:25%、eシール:6%、タイムスタンプ:17%、eデリバリー:5% (アンケートにご回答頂いた民間企業内)
- 個人: 電子署名 25%

トラストサービスの導入/利用における課題としては、以下が多く挙げられた

- 企業:「認知/理解不足」(知らなかった 等) 、「法的効力 (証拠能力)の担保不足」、「企業間での共通化の難しさ」
- 個人:「認知/理解の不足」(知らなかった/使い方がわからない 等)、「利用場面の不足」 等

今後のトラストサービスの基盤整備・普及に向けて考えられる施策例への関心("あれば前向きに導入検討したい"もの)は、以下が多く挙げられた

- 企業：低コストで導入可能な方法、標準化団体の設置/ガイドライン策定、電子署名以外の法的効力(証拠能力)の担保、使途毎の必要アシュアランスレベルの明確化、国際的な相互認証/海外での法的効力(証拠能力)担保
- 個人：認知・理解拡大に向けた普及啓発活動(わかりやすく教えてくれる)、ユースケース拡大による利用メリット増大 等

個人 企業

「行政」および民間の「金融・保険」「情報通信」「不動産」「医療・福祉」「運輸・郵便」や、業種共通の手続き等で幅広く、トラスト確保や、トラスト確保したDXのニーズが確認された

トラスト確保や、トラスト確保したDXのニーズのある主なユースケース

手続き分類 BtoB BtoC, BtoB/C / BtoG/GtoB, GtoC/CtoG, GtoB/C

企業のニーズが大きいもの / 個人のニーズが大きいもの

関連する人が多く、海外でも先行してトラストが導入された主な業種／分野

	行政	民間 金融・保険	情報通信	不動産	医療・福祉	運輸・郵便	その他（農林水産業、鉱業、建設業、製造業、電気・ガス等、卸売・小売、宿泊業・飲食業 等）
厳格な本人確認が必要な申請/手続等	戸籍の届け出、住民票の取得、戸籍謄抄本の取得、投票、厚生年金保険の保険料口座振替申請	銀行口座の開設、証券口座の開設、保険の契約、送金、国際送金	携帯電話/スマホの契約、レンタル/シェアリングサービス登録/利用、年齢確認が必要なサービス等の登録/利用		遠隔医療、問診、PHR	-	-
内容の非改ざん性/真正性が必要な申請/交付/情報授受	住民票関連の申請、運転免許証、国際運転免許証、後見登記等の申請、旅券、在留カード、ワクチンパスポート、自動車保管場所標章	保険契約証書の発行	マーケティングのための顧客情報連携	社内での営業情報の報告	健診/検査結果の発行、診断書の発行、薬の処方、カルテの作成・保管、医療機関の間での患者情報の連携、	通学定期の発行、モビリティIoT(車両のデータ取得)	スマートグリッド(スマートメーターのデータ取得)
法的証拠能力が必要な文書/記録等の作成・授受・保存	税務申告、自動車関連の手続、補助金等の請求、年金関連の手続、健保関連の手続、労災関連の手続、労働基準法関連の届出（36協定等）	融資/ローンの契約、貿易金融、為替取引	ネット回線の契約、有料放送の契約	不動産売買/賃貸契約	治験データの作成・保存・授受	国際物流関連の手続き (通関 等)	-

社外取引：経費の精算、受発注書の取り交わし、契約書の取り交わし、請求書の授受、商品等のトレーサビリティ確保

社内記録：会計帳簿の作成・保存、意思決定記録の作成・保存 (稟議、取締役会決議、株主総会決議など、稟議・決裁 …

規制対応：他の法律等で定められた台帳・帳簿・記録等の作成・保存 (医薬品・医療機器の台帳、外国為替取引の本人確認記録 等)

Source: 個人アンケート調査/企業アンケート調査

企業

海外取引があり、本人確認や文書/データの非改ざん性/真正性が必要なものとしては、業種共通の社外取引(受発注書、契約書、請求書等)や、「金融・保険」他の業種固有の手続き等が、挙げられた

海外取引があり、本人確認やデータの非改ざん性/真正性が必要な手続き等　(アンケート速報を踏まえた現時点まとめ)

手続き分類　BtoB　BtoG/GtoB,　BtoC,　GtoC/CtoG,　BtoB/C　GtoB/C

海外連携が必要なもの

関連する人が多く、海外でも先行してトラストが導入された主な業種／分野

	行政	民間						その他
		金融・保険	情報通信	不動産	医療・福祉	運輸・郵便		農林水産業、鉱業、建設業、製造業、電気・ガス等、卸売・小売、宿泊業・飲食業 等
厳格な本人確認が必要な申請/手続等	戸籍の届け出、住民票の取得、戸籍謄抄本の取得、投票、厚生年金保険の保険料口座振替申請	銀行口座の開設、証券口座の開設、保険の契約、送金、国際送金	携帯電話/スマホの契約、レンタル/シェアリングサービス登録/利用、年齢確認が必要なサービス等の登録/利用		遠隔医療、問診、**PHR (個人の健康/医療履歴の一元管理)**	-		-
内容の非改ざん性/真正性が必要な申請/交付/情報授受	住民票関連の申請、後見登記等の申請、運転免許証、国際運転免許証、旅券、在留カード、ワクチンパスポート、自動車保管場所標章	保険契約証書の発行	マーケティングのための顧客情報連携	社内での営業情報の報告	健診/検査結果の発行、診断書の発行、薬の処方、カルテの作成・保管、医療機関の間での患者情報の連携、	通学定期の発行、モビリティIoT (車両のデータ取得)		スマートグリッド (スマートメーターのデータ取得)
法的証拠能力が必要な文書/記録等の作成・授受・保存	税務申告、自動車関連の手続、補助金等の請求、年金関連の手続、健保関連の手続、労災関連の手続、労働基準法関連の届出 (36協定等)	融資/ローンの契約、貿易金融、為替取引	ネット回線の契約、有料放送の契約	不動産売買/賃貸契約 (含 重要事項説明、登記 等)	治験データの作成・保存・授受	国際物流関連の手続き (通関 等)		-

社外取引：経費の精算、受発注書の取り交わし、契約書の取り交わし、請求書の授受、商品等のトレーサビリティ確保

社内記録：会計帳簿の作成・保存、意思決定記録の作成・保存 (稟議、取締役会決議、株主総会決議など)、稟議・決裁 …

規制対応：他の法律等で定められた台帳・帳簿・記録等の作成・保存 (医薬品・医療機器の台帳、外国為替取引の本人確認記録 等)

Source: 企業アンケート調査

アウトライン

1. トラストサービスのニーズ及び現状 についての業種/分野別エキスパートインタビュー
2. 企業/個人へのアンケート調査実施概要
3. 企業向けアンケート結果の分析
4. 個人向けアンケート結果の分析
5. トラスト基盤の整備・普及による期待効果

デジタル化の期待インパクト（直接関わるステークホルダーの規模）と、トラストサービスの先行普及の可能性（海外での例）から、(行政以外の)5業種を選定し、先行ヒアリングを実施

（参考）ヒアリング対象とする業種の選定

業種	デジタル化の期待インパクト: 直接関わるステークホルダーの規模			トラストサービスの先行普及の可能性: 海外でトラスト利用が先行			優先調査
	労働人口		直接関わるユーザー規模	欧州	米国	中国	
農業，林業	小	(200万人)	小 (基本的にB2Bかつ取引相手は限定的)				
漁業	小	(13万人)	小 (基本的にB2Bかつ取引相手は限定的)				
鉱業，採石業，砂利採取業	小	(2万人)	小 (基本的にB2Bかつ取引相手は限定的)				
建設業	中	(492万人)	小 (基本的にB2Bかつ取引相手は限定的)				
製造業	大	(1,045万人)	小 (基本的にB2Bかつ取引相手は限定的)				
電気・ガス・熱供給・水道業	小	(32万人)	大 (B2C/Bかつ取引相手は全般的)				
情報通信業	中	(240万人)	大 (B2C/Bかつ取引相手は全般的)		✓		a
運輸業，郵便業	中	(347万人)	大 (B2C/Bかつ取引相手は全般的)	✓			b
卸売業，小売業	大	(1,057万人)	中 (B2C/Bかつ取引相手は限定的)				
金融業，保険業	小	(166万人)	大 (B2C/Bかつ取引相手は全般的)	✓	✓		c
不動産業，物品賃貸業	小	(140万人)	大 (B2C/Bかつ取引相手は全般的)	✓	✓	✓	d
学術研究，専門・技術サービス業	中	(244万人)	小 (基本的にB2Bかつ取引相手は限定的)	✓	✓		
宿泊業，飲食サービス業	中	(391万人)	大 (基本的にB2Cかつ取引相手は全般的)				
生活関連サービス業，娯楽業	中	(235万人)	大 (基本的にB2Cかつ取引相手は全般的)				
教育，学習支援業	中	(339万人)	中 (基本的にB2Cかつ取引相手は限定的)		✓		
医療，福祉	大	(862万人)	大 (基本的にB2Cかつ取引相手は全般的)		✓		e
複合サービス事業	小	(51万人)	中 (B2C/Bかつ取引相手は限定的)				
サービス業（他に分類されないもの）	中	(452万人)	中 (B2C/Bかつ取引相手は限定的)	✓			

Source: 厚生労働省「労働力調査（基本集計）2020年」(令和2年)、総務省「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 最終取りまとめ (案)／三菱総合研究所 (総務省委託調査)「トラストサービスに関する海外調査」

金融では、特に「融資/ローン契約」「貿易金融」「為替取引」「口座開設」「送金」「国際送金」等でニーズがありそう。他方で、普及には取引先の理解醸成が必要

(参考)トラストサービスへのニーズ: 金融 (業界エキスパートへのヒアリング)

トラストサービスのニーズ

「融資/ローン契約」、「貿易金融」、「為替取引」、「口座開設」、「送金」「国際送金」などは、特にトラストサービスのニーズがありそう。中でも、「**貿易金融」や「国際送金」では、海外連携**も必要となる

- **「融資/ローン契約」**: 個人は勿論、法人でも、あまり**デジタル化が進んでいない**
  - オンライン契約システムを使おうという動きはあるが、**相手側**、特に中堅・中小企業**が承諾しない**ことが多い
- **「貿易金融」**: 例えば皮革製品を輸入する場合、書類が高さ1mになる程で、**最も電子化の必要があるものの一つ**
  - その書類のOCRによる電子化は既に試みられているが、データ化されれば、トラストサービスも必要になるだろう
  - 特に、相手先が海外のマイナーな金融機関の場合等には、データの改ざん防止なども求められるだろう
- **「為替取引」**: 主に国内の事業会社が外国通貨に変える際など、"**紙の契約書の塊**"になっている
- **「口座開設」**: 口座の開設時には**厳格な本人確認が必要。大手銀行なら、年間数十万件ぐらい**はある
  - 既にeKYCはあるが、オンラインで送られた本人と身分証の写真の確認は人力で行っており、**膨大な人手**を要しているため、その削減のニーズがある
- **「送金」「国際送金」**: **送金先が反社会的勢力でないことを確認**する(AML/アンチマネーロンダリング)ため、**膨大なコスト**を要している (年間数十億円以上)
  - 海外事業から撤退する要因にもなっており、これが容易に出来るようになるならば、大いにニーズはある

なお、証書の発行などは、保険ではあるだろうが、銀行ではあまり多くはない

トラストサービス導入／普及に向けた課題等

そもそもデジタル化の阻害要因として、**取引先の中堅・中小企業**で**判子への信頼とオンライン化への不安**が強いことが大きい

- 中堅・中小企業の社長には、「**判子**を自分が管理していれば、契約などの際には**必ず自分のところに来る**」という安心感と、逆に「オンラインでのやり方だと、**社員が勝手にやってしまうのでは**ないか」という不安がある
- 上記に対して、オンラインのやり方であっても、**経営者の不安を解消**することが出来れば、拡がっていく可能性があるのでは

Source: エキスパートインタビュー

貿易金融や(法人)口座開設等に関しては、マネーロンダリング防止(AML)や制裁国・資金凍結者への送金／物資供給防止のための、KYCCやデューデリジェンスが必要だが、顧客の法人の融資元／出資元等の支配者関係チェック等のドキュメントワークの負荷が高く、トラスト確保だけでなく、その共同化なども求められる

(参考)トラストサービスへのニーズ: 金融 (業界エキスパートへのヒアリング)

トラストサービスのニーズ

- **「貿易金融」**
  - 貿易金融も**架空取引等、マネーロンダリングの温床**となる。トラストサービスによる発行元証明のニーズが存在
  - 不正取引という意味では、**北朝鮮やイラン等、制裁国・資金凍結者への送金／物資提供を隠す手段**となっている。グローバル化している邦銀に対してアメリカ当局から指摘・罰金が入ることも多い
- **「KYCC」**：法人口座開設時に**法人格の確認事項として、反社チェック等のドキュメントワーク負荷が高い**
  - 口座を開設する法人の融資元／出資元等支配者関係をチェックする必要があり、各銀行のドキュメントワークとなっている。
- **「Continuous Due Diligence」**：KYCCに加えて年次レベルで既顧客のデューデリを実施。定常的なドキュメントワーク負荷の原因となっている。
  - 各顧客（法人／個人）含めて3段階くらいにスコアリング。警視庁からくるブラックリストを受入れ。

トラストサービス導入／普及に向けた課題等

トラストサービスの価値である発行元証明／電子ドキュメントの信頼性に加えて、顧客の信用チェックにかかるドキュメントワークに関する共同化ニーズがある

Source: エキスパートインタビュー

情報通信では、通信回線やオンラインサービスの登録・利用時の本人確認/年齢確認ニーズ。他方、(他業種も含め)導入・利用のコストは障壁になることが見込まれる

(参考)トラストサービスへのニーズ: 情報通信 (業界エキスパートへのヒアリング)

トラストサービスのニーズ

オンラインでの厳格な「本人確認」や「年齢確認」にはニーズがありそう。
例えば、**「携帯電話/スマホの新規契約」**や**「インターネット回線の新規契約」**のほか、
「年齢制限があるオンラインサービスの登録/利用」「レンタル／シェアリングサービスの利用登録」などが挙げられる

- **「携帯電話の新規契約」「インターネット回線の新規契約」「レンタル／シェアリングサービスの利用登録」**:
  - 厳格な本人確認が必要とされており、それが簡単になるならば、ニーズはありそう
- **「年齢制限があるオンラインサービスの登録/利用」**:
  - 現状は、厳しい法規制等もなく、実態として緩やかな運用になっているが、本来は必要
  - 例えば、一部のスマホゲームや、オンラインでの酒類の販売、宝くじ販売なども年齢確認が必要だが、現在は、ほぼ自己申告だけになっているケースも多い

なお、マーケティングのための企業間での顧客データ共有等では、あまりトラストサービスのニーズはないのでは

- 正確なデータは必要だが、企業にとっては自社のマーケティングのために行うもので、データを改ざんする動機がない

トラストサービス導入／普及に向けた課題等

トラストサービスの導入にあたっては、**導入や利用のコスト**が課題になる可能性がある

- 民間で、事前に本人確認・年齢確認された顧客データを使い、他社に対して、オンラインでの本人確認や年齢確認の機能を提供している企業もある
- 但し、そのためとして企業から利用料金を得られているわけではなく、決済など、他の有料B2Bサービスに付帯するものとして提供している

Source: エキスパートインタビュー

不動産では「賃貸/売買の契約」や「社内での営業報告」、業種共通の「社内決裁/稟議」、「請求」等でニーズが見込まれる。普及には対面・紙以上の信頼性への理解醸成が鍵か

(参考)トラストサービスへのニーズ: 不動産 (業界エキスパートへのヒアリング)

トラストサービスのニーズ

古い業界慣習が根強く、全般的にデジタル化は遅れている。
本来、**「不動産賃貸/売買の契約」**のデジタル化・詐欺の防止や、**「社内での営業報告」**の改ざん防止、
また、他業界とも共通するが**「社内決裁/稟議」**や、社外への**「請求」**などで、トラストサービスへのニーズがあるはず

- **「不動産賃貸/売買の契約」:**
  - 事業者側は重要事項説明などの紙がなくならず、入居者側は戸籍謄本などの準備の手間が大きい
  - 一方で、紙であるが故に偽造できてしまう側面もあり、"地面師"の詐欺被害の事件が近年でも起きている
- **「社内での営業報告」:**
  - 営業目標 (例:住宅展示場の来場者数など) に対する報告で、数割レベルの実績の改ざんが常態化している
  - 本社側では、適切な営業管理が出来ていない認識はあるが、根治する対応が取れていない
- **「社内決裁/稟議」:**
  - (企業にもよるが) 古い業界慣習が根強く、稟議やワークフローが紙・捺印のままになっている
  - 精神論的だが、どの部署の誰に責任があるのか、責任の所在を明確にするための「血判状」のような側面もある
- **「請求」:**
  - 賃貸物件オーナーなどへの請求で、依然として大量の紙を使用しており、効率化の余地が大きい

営業が、営業個人としての差別化("武器")として、顧客情報を隠したがることが問題

トラストサービス導入／普及に向けた課題等

「対面・紙よりも電子証明の方が信頼・信用できる」という認識作りが最も必要ではないか

- 依然として、「対面での紙・判子が一番信用できる」という"神話"が不動産業界には根強い
- 「対面・紙以上に、電子証明の方が信用できる」ということが確り理解されれば、使われていく可能性は十分あるのでは

Source: エキスパートインタビュー

医療では「健診/検査結果」「診断書」等のデジタル化時の改ざん防止や、今後の「遠隔診療」「PHR」等での本人確認などでニーズが見込まれる。地域・事業者横断の連携が課題

(参考)トラストサービスへのニーズ: 医療 (業界エキスパートへのヒアリング)

トラストサービスのニーズ

既存の紙・対面のデジタル化に加えて、今後進展・拡大が期待される遠隔診療やデータヘルス関連の取組でも、トラストサービスへのニーズがある

- 既存の紙・対面のデジタル化では、既に電子化を進めている**「カルテ」**や**「薬の処方」**に加え、**「健診/検査結果」「診断書」**などにニーズがある
  - **「薬の処方」**: 非改ざん性と本人確認が重要で、現在は基本的に紙。電子化に向け厚労省で推進中
  - **「カルテ」**: 電子化が法的に認められるようになって以来、進んでいるが、非改ざん性が必要
  - **「健診/検査結果」**: 保険契約や資格認定などにも用いられるため、非改ざん性が必要
  - **「診断書」**: 非改ざん性が必要で、現在は紙ベース
- 今後拡大が期待されるものとしては、**「遠隔診療」「(デジタルでの)問診」**や**「PHR」**、**「医療機関等の間での患者情報の連携」**などにニーズがある
  - **「遠隔診療」「(デジタルでの)問診」**: 患者の厳格な本人確認が必要
  - **「PHR」**: 機微情報を多く含むため、利用者の厳格な本人確認が必要。また、本人の許諾に応じて、医療機関や企業などにデータを提供することが見込まれているが、その開示先のなりすまし防止も必要
  - **「医療機関間の患者情報の連携」**: 非改ざん性の確保や、発信元・送付先を確認した確実な送達が必要
    - 例えば、海外で撮影したX線写真を日本の医療機関に共有して診療・治療を行うなど、**国際連携**もある
- また**「治験データ」**は、薬の認可のベースとなるもので、非改ざん性の担保が必要

トラストサービス導入／普及に向けた課題等

現在でも、一部で個々にはトラストサービスが導入されているが、**地域や事業者を横断する連携**が課題

- 例えば、患者が東京の病院や大阪の病院に移る際に、それぞれが地域内でトラストサービスやデータ連携の仕組みを導入していても、地域間で仕組みが分断されているため、紙の紹介状が必要になっている

上記のために、政府によるものなど、**公的な認証基盤**が使えると良いのでは

Source: エキスパートインタビュー

物流/小売/製造業では、川上の小売や製造業も巻き込んだトレーサビリティ確保による配送の需給最適化やCO2削減、盗難やマネロン等不正対応、サプライヤーの信用創造・保険リスク低減 等

(参考)トラストサービスへのニーズ: 物流/小売/製造業 (業界エキスパートへのヒアリング)

トラストサービスのニーズ

消費者が買った商品が消費者の手元に届くまでの情報をトラッキングすることで、製造／小売／物流に関わる以下のようなリターン／ベネフィットが期待できる

- 物流：ドライバー不足など需給ミスマッチに対する抜本対策、盗難紛失への対応
  - 物流単体での需給ミスマッチ解消は難しく（国交省推進のモーダルシフト等含め）、メーカー共同配送や小売データを使った需要予測高度化等の抜本対策が望まれている
- **政府：マネロン解消、商品単位でのCO2排出／水質汚染の見える化（カーボンニュートラル等）**
  - 使途不明金の追跡。商品単位でのCO2排出量／水利用量の見える化で消費者意識向上
- **融資／保険リスク評価：取引の可視化によるサプライヤー信用創造／拡大、保険会社リスク評価の正確性向上**
  - 取引実績（トランザクション）を積み上げることによる各企業の与信力向上／リスク評価の正確性向上
- **その他：人権に関するデューデリジェンス**
  - 生産現場では外国人労働者の強制労働（一定期間工場に張り付け）等があり、アメリカ当局から日本への批判の的となっている。将来的には不買運動等にも繋がるレピュテーションリスク

製造／小売／物流各社で自主的な取り組みが進むが本来は**業界横断テーマ**
→ネスレ等は自前のブロックチェーンで川上の情報を取得。小売事業者は各商品のタグとトレース情報を紐づけ中。

トラストサービス導入／普及に向けた課題等

公共性の高い金融やヘルスケアに比べると業界としてトラスト活用による自主透明性の難易度が高い
→**取引参加企業の裾野が広く**、認可制というよりNPO活用等による草の根の不正監視が現実解となっている。
→人権よりも生産性維持が優先されてしまっている状況

とはいえ物流の需給ミスマッチの解消は喫緊課題、人権やカーボンニュートラル等レピュテーションリスクが顕在化し始めているので遠くない将来、トラスト確保を含むトレーサビリティ確保が望まれる

Source: エキスパートインタビュー

アウトライン

1. トラストサービスのニーズ及び現状 についての業種/分野別エキスパートインタビュー
2. 企業/個人へのアンケート調査実施概要
3. 企業向けアンケート結果の分析
4. 個人向けアンケート結果の分析
5. トラスト基盤の整備・普及による期待効果

先行ヒアリングも踏まえた上で、企業/個人へのアンケート調査を実施

アンケート調査の実施概要

実施目的

トラストを確保したDX推進の検討のご参考とするため、企業/個人の現状やニーズ等を把握する

- トラストを確保したDXが求められる手続き等(≒トラストサービスのユースケース)
- トラストサービスの現状の利用状況、課題、及び、必要な方策

実施概要

	企業アンケート	個人アンケート
対象	国内企業 • 全国、企業規模・業界問わず	国内個人 • 全国、10代~70代以上・男女
実施方法	オンラインアンケート • 業界団体等にメール・電話等で協力依頼を行い、ご協力頂けた業界団体の加盟企業に回答依頼	オンラインアンケート
有効回答数	347社 (12月7日時点) • 245業界団体に協力依頼 • ３３団体のご協力で、加盟企業(計 約11万社)にご依頼頂いた	4,406人 • 電子証明書の利用あり/なしで均等割付し、分析時に電子証明書の利用率でウェイトバック (重み付け)
調査期間	2021年11月24日~12月7日	2021年11月19日~11月24日
主な調査項目	• 基本属性 • トラストを確保したDXのニーズ • トラストサービスの導入/検討状況 • トラストサービスへの課題意識 • デジタル完結を実現するための検討への関心　等	• 基本属性 • トラストを確保したDXのニーズ • トラストサービスの導入/検討状況 • トラストサービスへの課題意識 • デジタル完結を実現するための検討への関心　等

企業

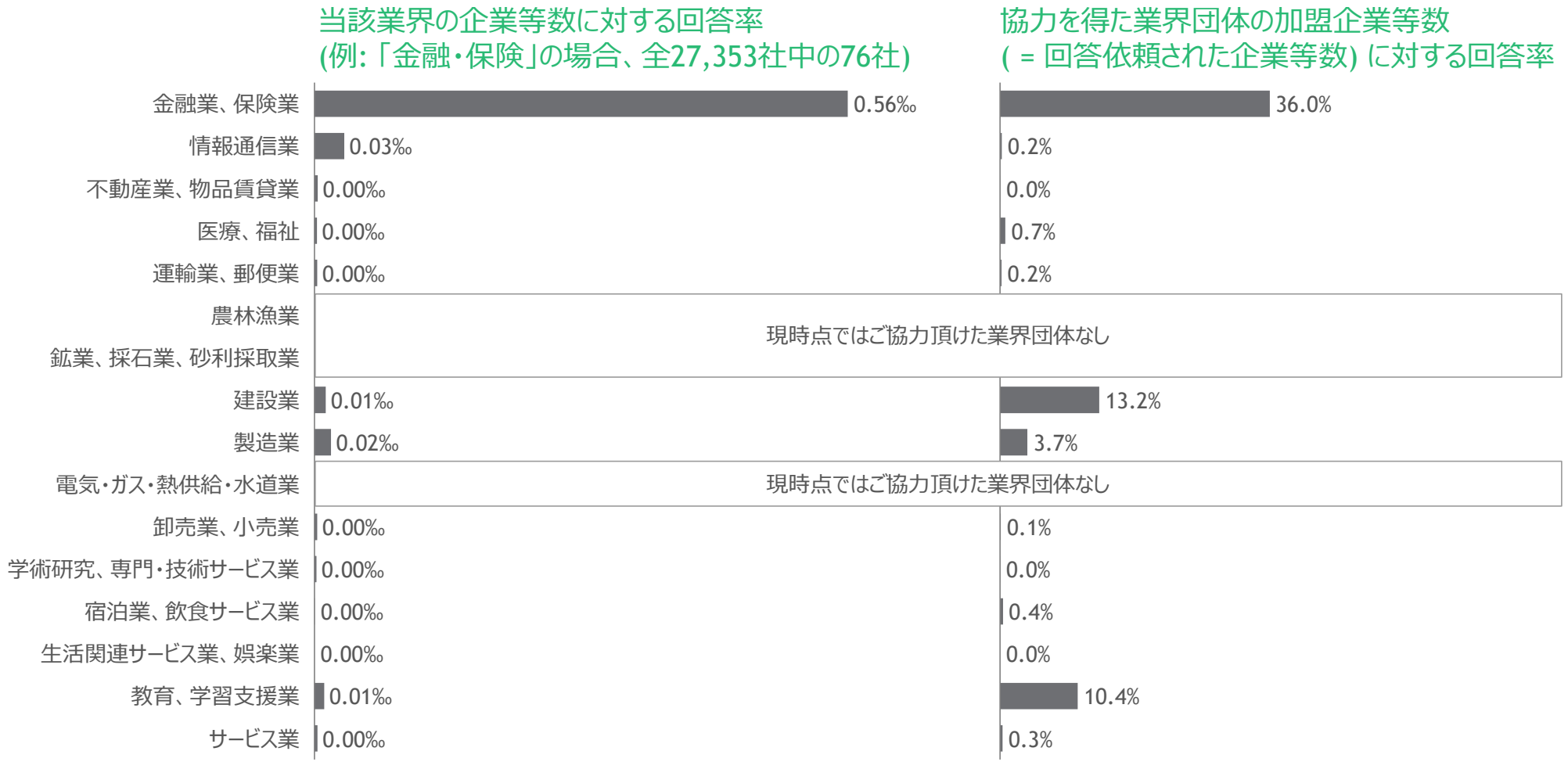
245の業界団体(加盟企業 計44万社)に依頼し、調査終了時点で 33団体(加盟企業 計11万社) の協力を得て、347社に回答を完了して頂いた

業種		企業等数	協力可			協力検討中		協力不可	
調査項目	細目		団体数	所属企業等数	回答数	団体数	所属企業等数	団体数	所属企業等数
金融業、保険業		27,353	3	425	153	3	497	5	411
情報通信業		38,218	3	5,378	12	6	983	3	563
不動産業、物品賃貸業		278,732	2	33,058	10	1	158	2	99,313
医療、福祉		276,248	3	1,114	8	19	9,201	6	2,388
運輸業、郵便業		64,662	3	1,048	2	3	338	5	2,601
農林漁業		24,883	0	0	0	0	0	5	3,660
鉱業、採石業、砂利採取業		1,294	0	0	0	1	33	1	49
建設業		409,536	3	370	49	10	33,370	6	18,898
製造業		366,065	7	1,746	64	23	4,543	16	5,157
電気・ガス・熱供給・水道業		1,013	0	0	0	8	9,158	3	284
卸売業、小売業		794,837	2	23,004	25	5	13,420	2	319
学術研究、専門・技術サービス業		173,944	1	40,625	4	7	72,281	5	223,510
宿泊業、飲食サービス業		446,485	1	244	1	8	40,093	2	2,768
生活関連サービス業、娯楽業		341,559	1	5,500	0	2	5,708	1	5,500
教育、学習支援業		105,841	1	106	11	4	1,895	1	0
サービス業(複合サービス業、サービス業(他に分類されないもの))		235,472	3	2,290	8	2	320	2	52,006
計		3,586,142	33	114,908	347	102	191,998	65	417,427

Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

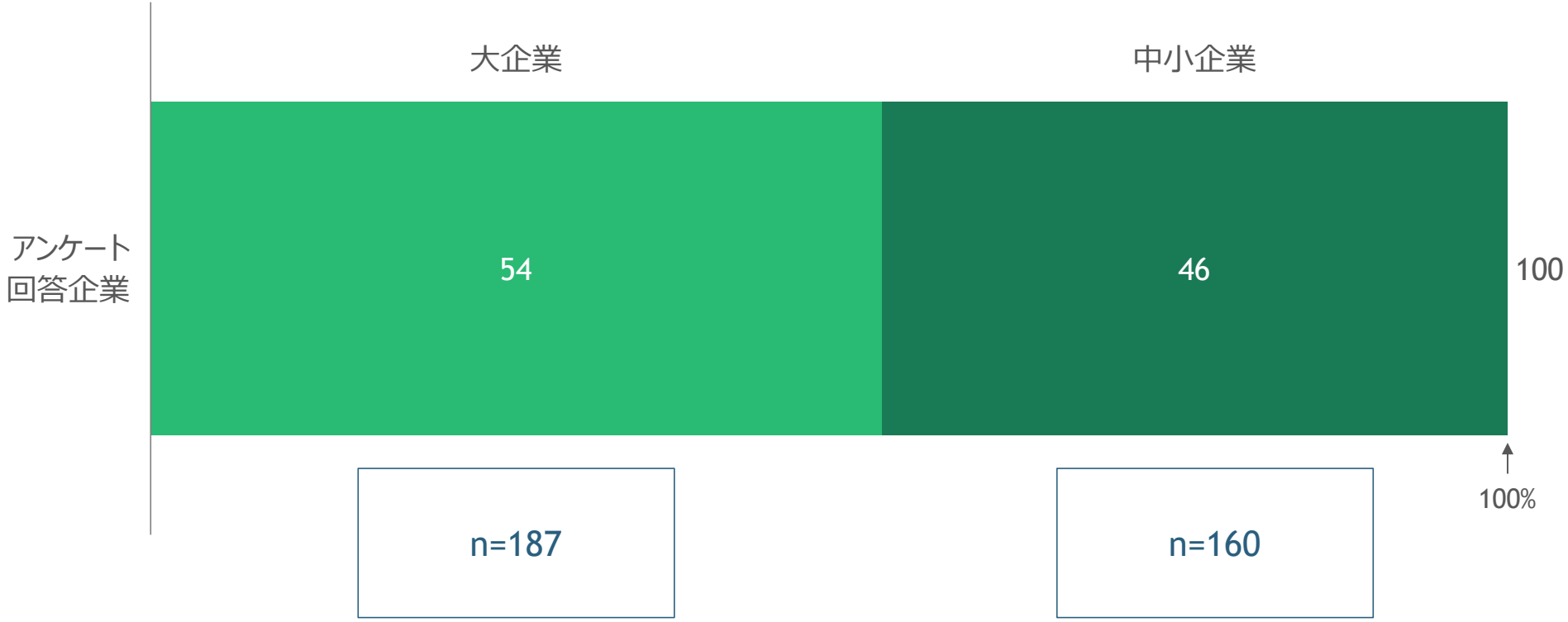
企業

(参考) 業種別の回答率は、金融・保険が突出



Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

(参考) 企業規模別では、大企業と中小企業でほぼ半々



Note: 大企業の定義は業種ごとに異なり、卸売業では資本金1億円以上かつ従業員数100人以上、サービス業では資本金5,000万円以上かつ従業員100人以上、小売業では資本金5,000万円以上かつ従業員50人以上、その他の業種では資本金3億円以上かつ従業員300人以上
Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

アウトライン

1. トラストサービスのニーズ及び現状 についての業種/分野別エキスパートインタビュー
2. 企業/個人へのアンケート調査実施概要
3. 企業向けアンケート結果の分析
4. 個人向けアンケート結果の分析
5. トラスト基盤の整備・普及による期待効果

企業

企業向けアンケート結果

現状のトラストサービスの課題と方策

企業におけるトラストサービスの利用は、依然として限定的

- 利用率は、「個人の電子証明書」25%、「eシール (企業の電子署名)」6%、「タイムスタンプ」17%、「eデリバリー」5%

現状のトラストサービスの課題は、各トラストサービス毎に異なるが、全体に「認知/理解不足」が特に多く、
導入済み/検討経験ありの企業の中では「企業間での共通化の難しさ」や「導入/利用コスト」が多い

課題解決の方策として、有効な(あれば導入を前向きに検討する)ものとして、コスト負担の低減以外では、
「電子署名以外のトラストサービスの法的効力 (証拠能力)規定」(29%)、「業界ごとの標準化団体設置 かつ/又は ガイドライン策定」(28%)
が特に多く挙げられた

(補足1) 民間分野のデジタル化の実態 (企業視点)

実施規模が大きい手続き等も含め、実施企業におけるデジタル/オンライン完結の導入率は、いずれも半分未満に留まる

- 実施規模の多い手続き等は、業種共通の「受発注の取引書類の作成・授受」、「請求・支払書類の作成」や、
  業種固有で金融・保険の「国内送金/振込」、「為替取引」、「銀行口座開設」 等
- 他方で、そのデジタル/オンライン完結の導入率は、「受発注の取引書類の作成・授受」(36%)、「請求・支払書類の作成」(32%)、
  「国内送金/振込」(13%)、「為替取引」(11%)、「銀行口座開設」(15%) 等限定的

(補足2) 印鑑・署名等への意識

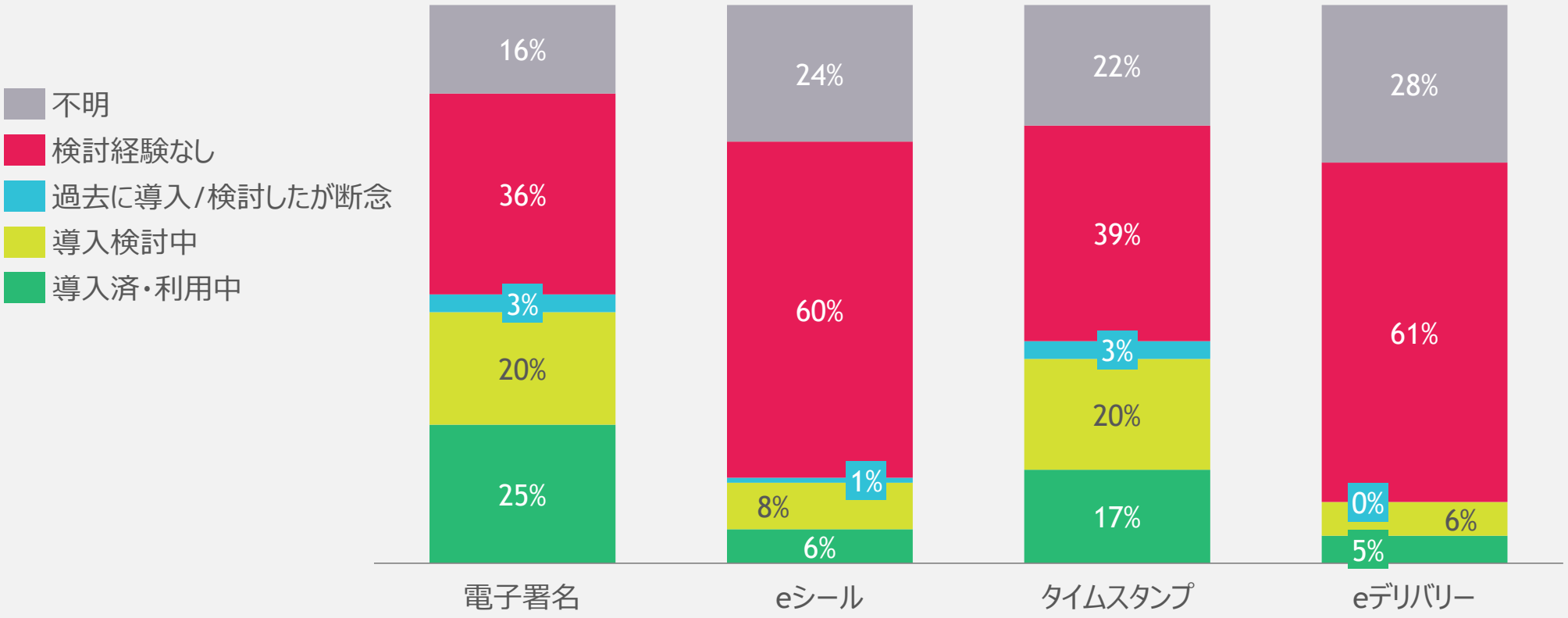
社外取引では認印が圧倒的に多い一方、社内手続では会計帳簿の作成・保存を除いて、認印、自著署名、チェックが多い

- 上記のうち、社内基準や規定によるものは40%~50%程度で、業界/自社の慣習によるものは45%程度

使用側としても受取側としても、法的効力 (証拠能力)の認識は、実印は4~6割以上の一方、認印や自著署名では2割未満に留まる

企業

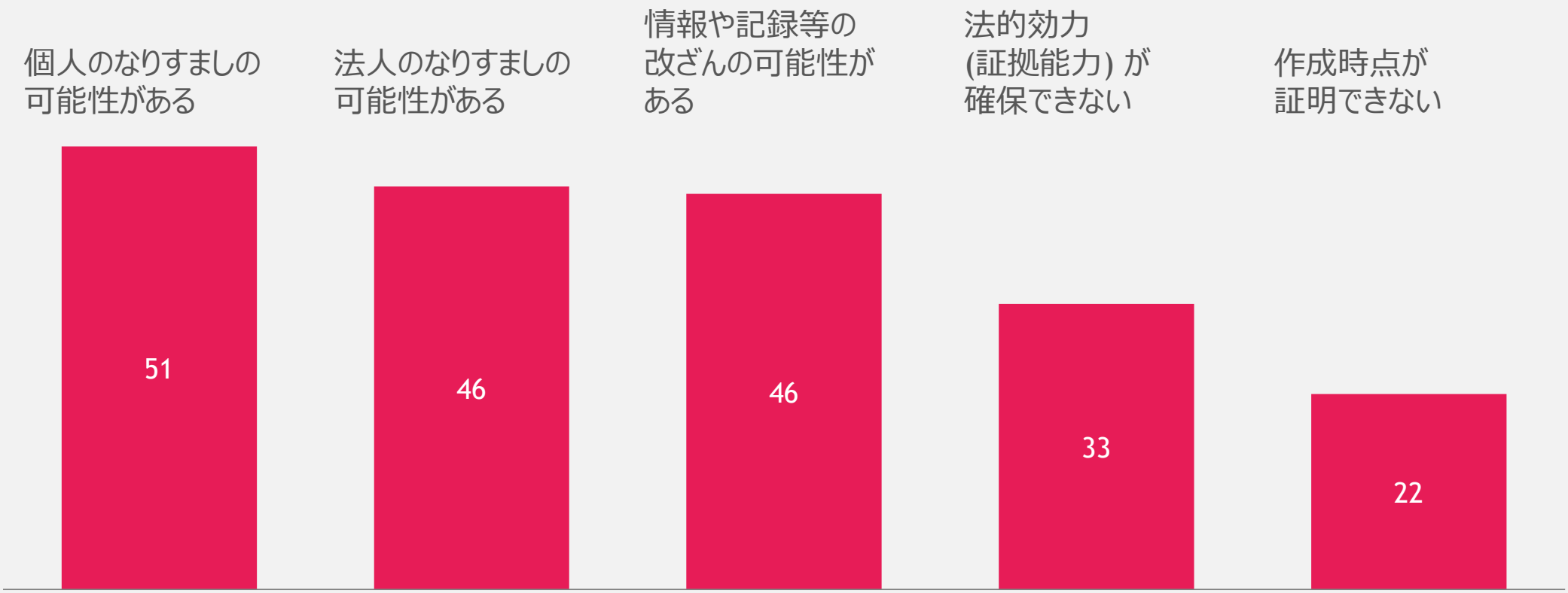
トラストサービスの利用は、電子署名25%、eシール6%、タイムスタンプ17%、eデリバリー5%



Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業

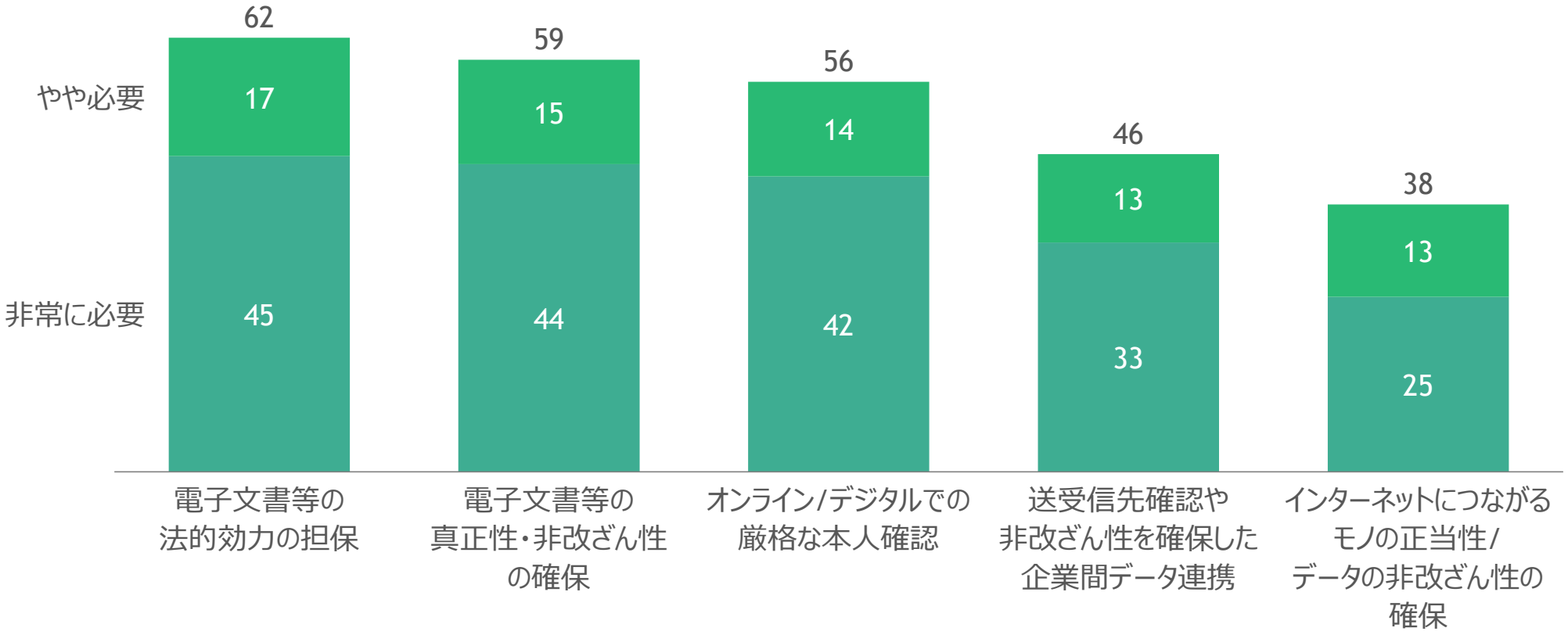
デジタル/オンラインでの手続き等に対し、本来トラストサービスにより防ぎ得るリスクに危機意識を持つ企業は、「個人のなりすまし」(51%) や「法人のなりすまし」(46%) 等、～5割水準



Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業

トラストサービスによって享受できるメリットに対しては、「電子文書等の法的効力 (証拠能力) 担保」(62%)、「電子文書等の真正性・非改ざん性の確保」(59%) 等、約6割の企業が必要との回答

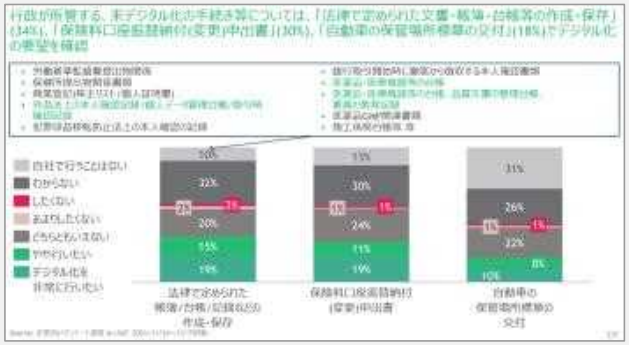


Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

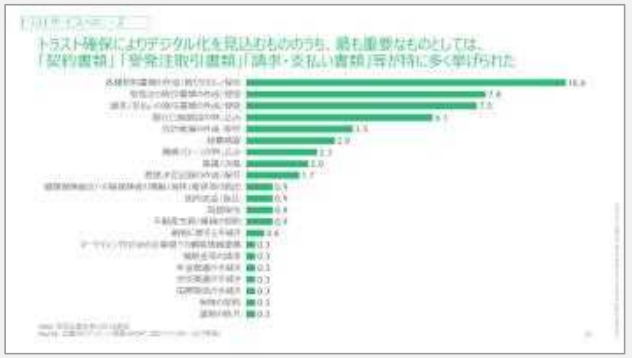
企業

トラスト確保/それによるデジタル化のニーズがある手続き等は、行政が所管する未デジタル化のもの、トラスト確保によるデジタル化の見込みが大きいもの、デジタル化済でトラスト確保が必要なものの3点から把握

行政が所管する未デジタル化のもの



トラスト確保によるデジタル化の見込みが大きいもの



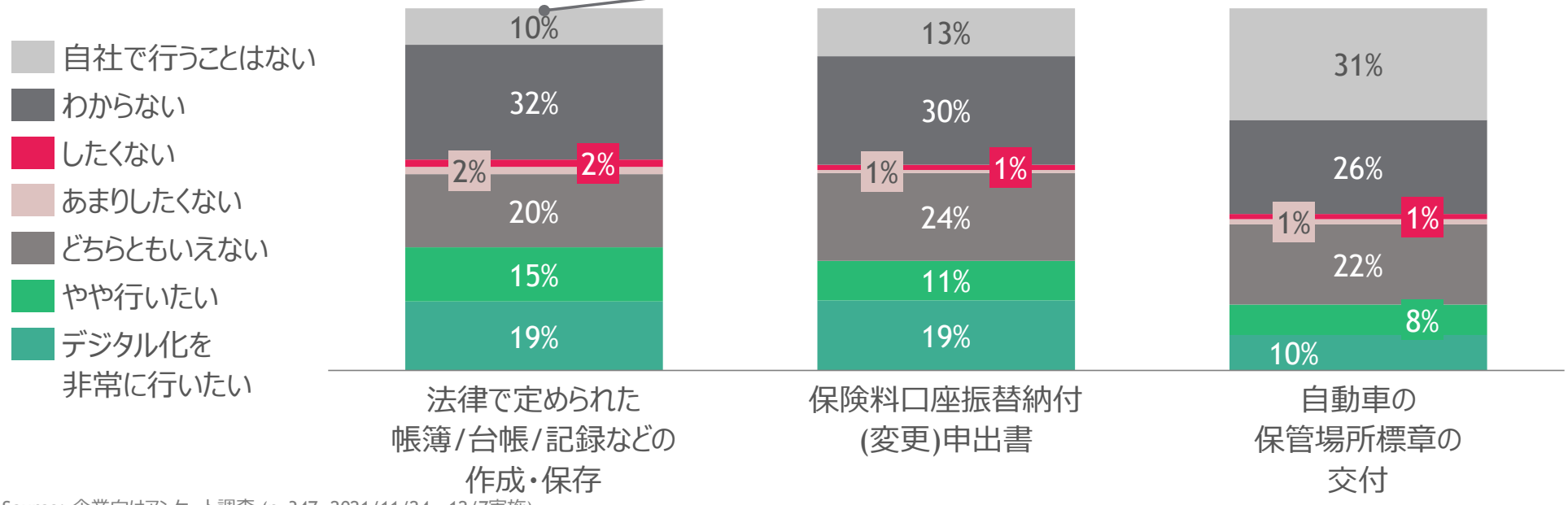
デジタル化済でトラスト確保が必要なもの

Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業

行政が所管する、未デジタル化の手続き等については、「法律で定められた文書・帳簿・台帳等の作成・保存」(34%)、「保険料口座振替納付(変更)申出書」(30%)、「自動車の保管場所標章の交付」(18%)でデジタル化の要望を確認

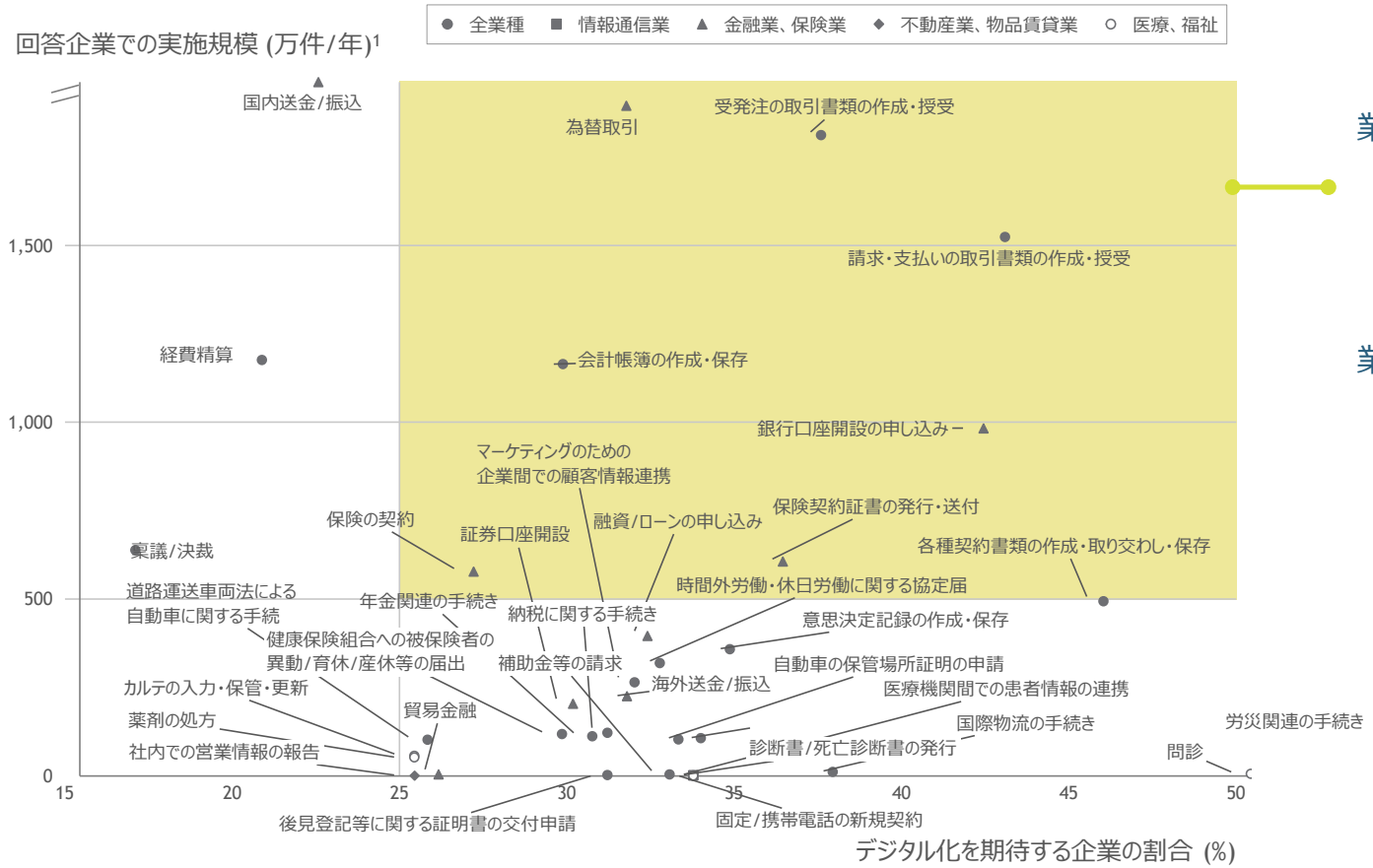
- 労働基準監督署提出物関係
- 保健所提出物関係書類
- 商業登記(株主リスト/個人証明書)
- 外為法上の本人確認記録/個人データ管理台帳/取引時確認記録
- 犯罪収益移転防止法上の本人確認の記録
- 銀行取引開始時に顧客から徴収する本人確認書類
- 医薬品・医療機器等の台帳
- 医薬品・医療機器等の台帳、品質文書の管理台帳、要員の教育記録
- 医薬品GMP関連書類
- 施工体制台帳等 等



Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業

トラスト確保によるデジタル化の期待が大きいものは、業種共通の「各種契約書類の作成」「請求・支払いの取引書類の作成」と、金融・保険の「銀行口座開設」「為替取引」等



業種共通

- 各種契約書類の作成
- 請求・支払いの取引書類の作成
- 受発注取引書類の作成
- 会計帳簿の作成

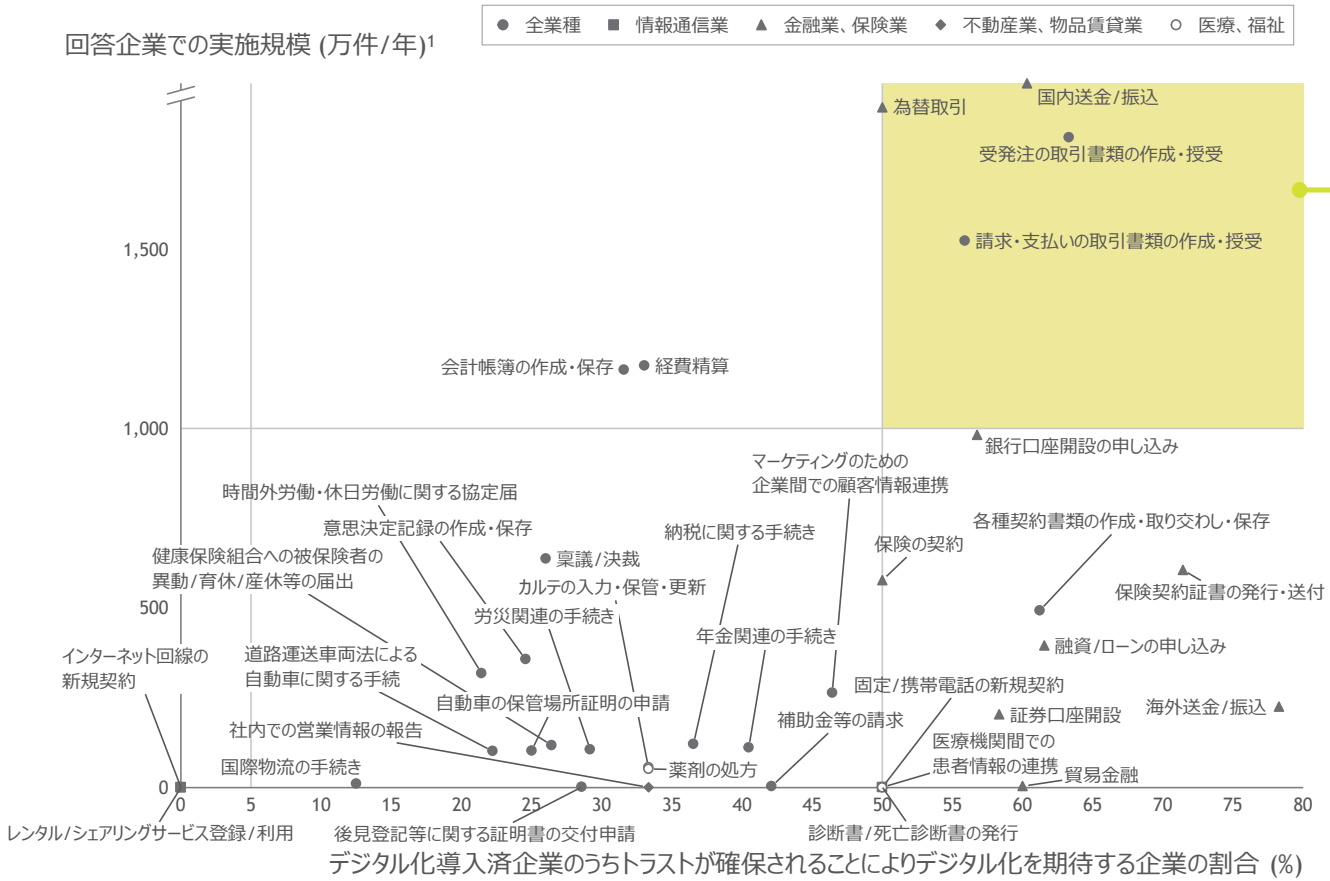
業種固有

- 金融・保険
  - 銀行口座の開設
  - 為替取引
  - 保険契約証書の発行・送付
  - 保険の契約

1. 実施ありと回答した企業数に、実施規模を乗じた値
Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業

デジタル化済でトラスト確保が必要なものは業種共通の「受発注取引書類」「請求・支払いの取引書類の作成」等や、金融・保険の「国内送金/振込」「為替取引」が挙げられた



業種共通
- 受発注の取引書類の作成・授受
- 請求・支払いの取引書類の作成・授受

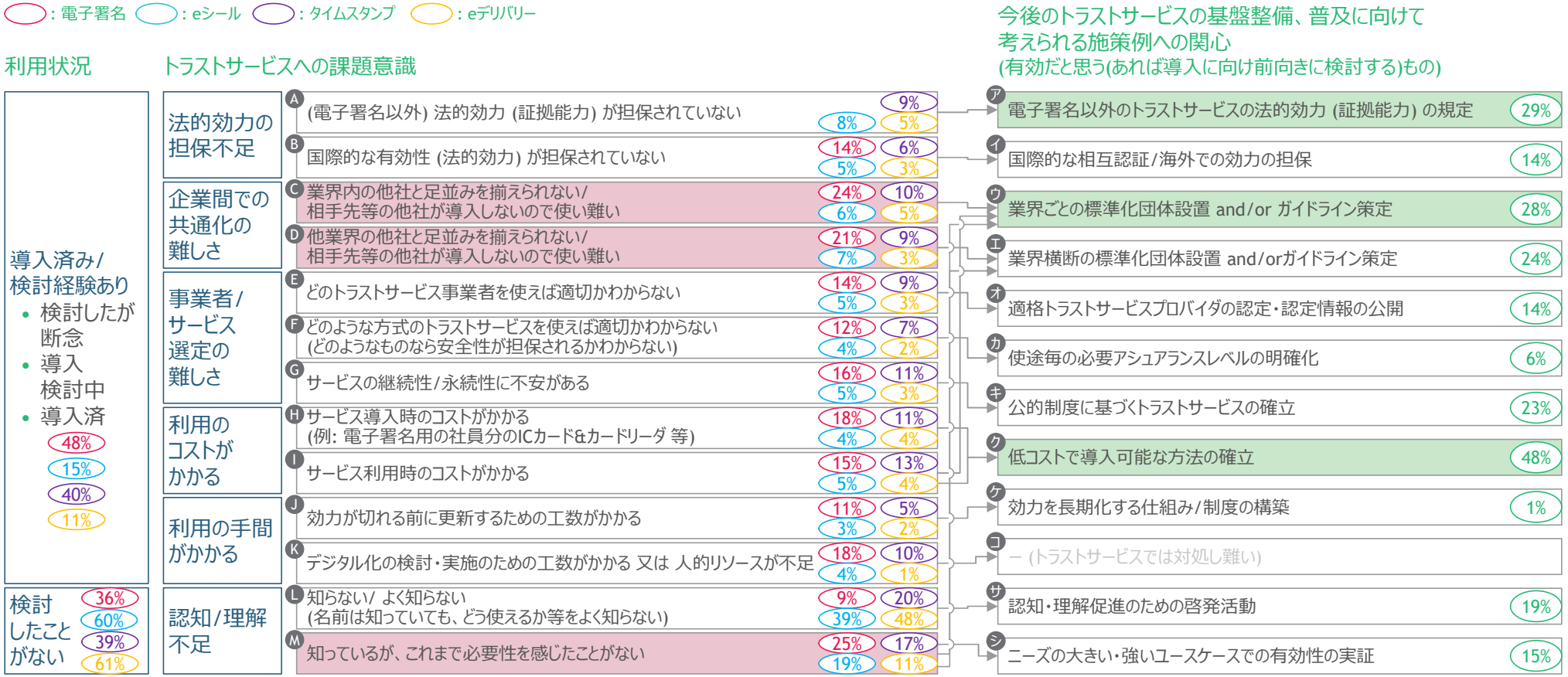
業種固有
- 金融・保険
  - 国内送金/振込
  - 為替取引

1. 実施ありと回答した企業数に、実施規模を乗じた値
Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業

全体としては、トラストサービスの課題意識として「企業間での共通化の難しさ」や「認知/理解不足」が多く、今後考えられる施策例への関心は、「低コストで導入可能な方法」「法的効力(証拠能力)の規定」「業界ごとの標準化団体設置/ガイドライン策定」がトップ3

トラストサービスへの課題意識、今後のトラストサービスの基盤整備・普及に向けて考えられる施策例への関心



Note: それぞれの割合は、全回答者 (N=347)に対する割合。導入済み/検討経験ありと検討したことがないの合計は、「わからない」を除くため、合計100%にならない
矢印は明確な分析結果に基づくものではないか、関係性が深いと考えられる箇所に記載
Source: 企業アンケートよりBCG分析

企業 (中小企業)

中小企業では、トラストサービスの課題意識として「認知/理解不足」が特に多く、今後考えられる施策例への関心は、「低コストで導入可能な方法」「法的効力(証拠能力)の規定」「業界ごとの標準化団体設置/ガイドライン策定」がトップ3 (全体同様)

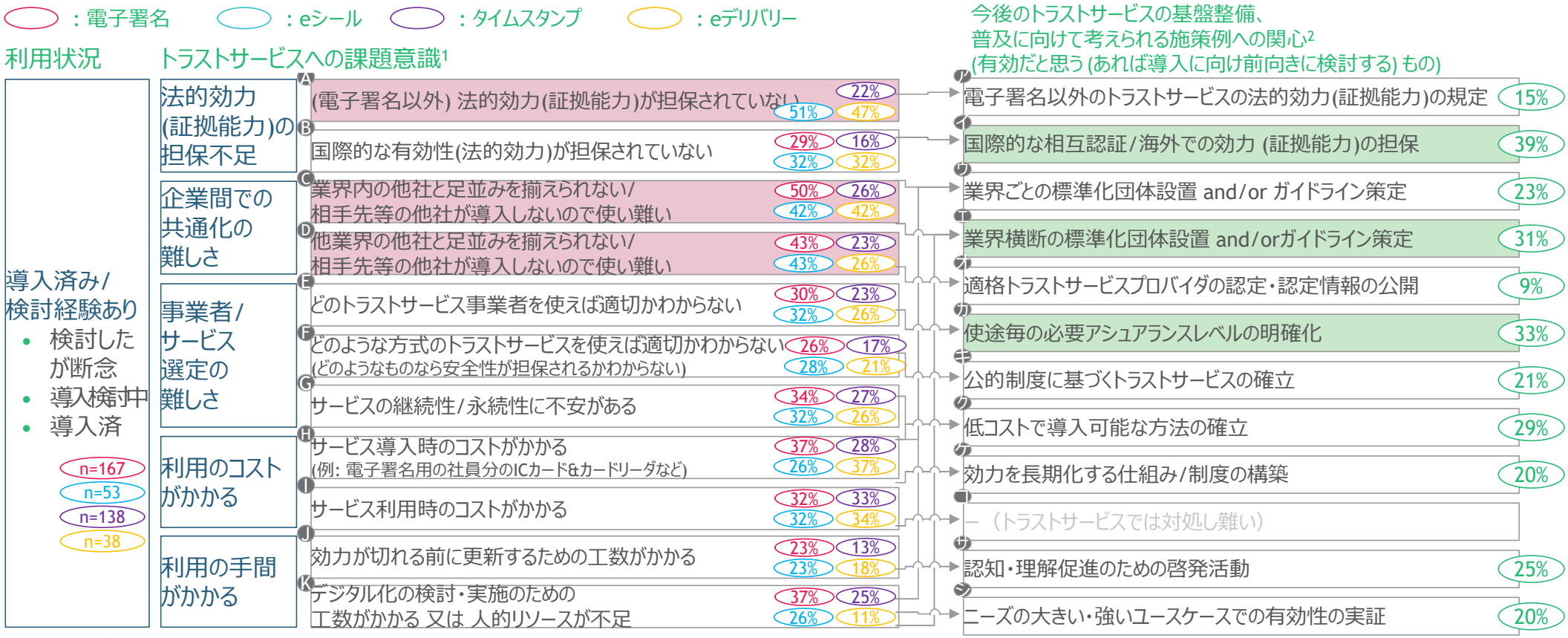
トラストサービスへの課題意識、今後のトラストサービスの基盤整備・普及に向けて考えられる施策例への関心 (中小企業)

Note: それぞれの割合は、中小企業の回答者 (N=160)に対する割合。導入済み/検討経験ありと検討したことがないの合計は、「わからない」を除くため、合計100%にならない
矢印は明確な分析結果に基づくものではないが、関係性が深いと考えられる箇所に記載
Source: 企業アンケートよりBCG分析

企業 (導入済み または 検討経験ありの企業)

導入済み/検討経験ありの企業では、トラストサービスの課題意識として「法的効力(証拠能力)の担保不足」と「企業間での共通化の難しさ」が多く、今後考えられる施策例への関心は「国際的な相互認証/海外での法的効力(証拠能力)の担保」「使途毎の必要アシュアランスレベルの明確化」「業界横断の標準化団体設置/ガイドライン策定」がトップ3

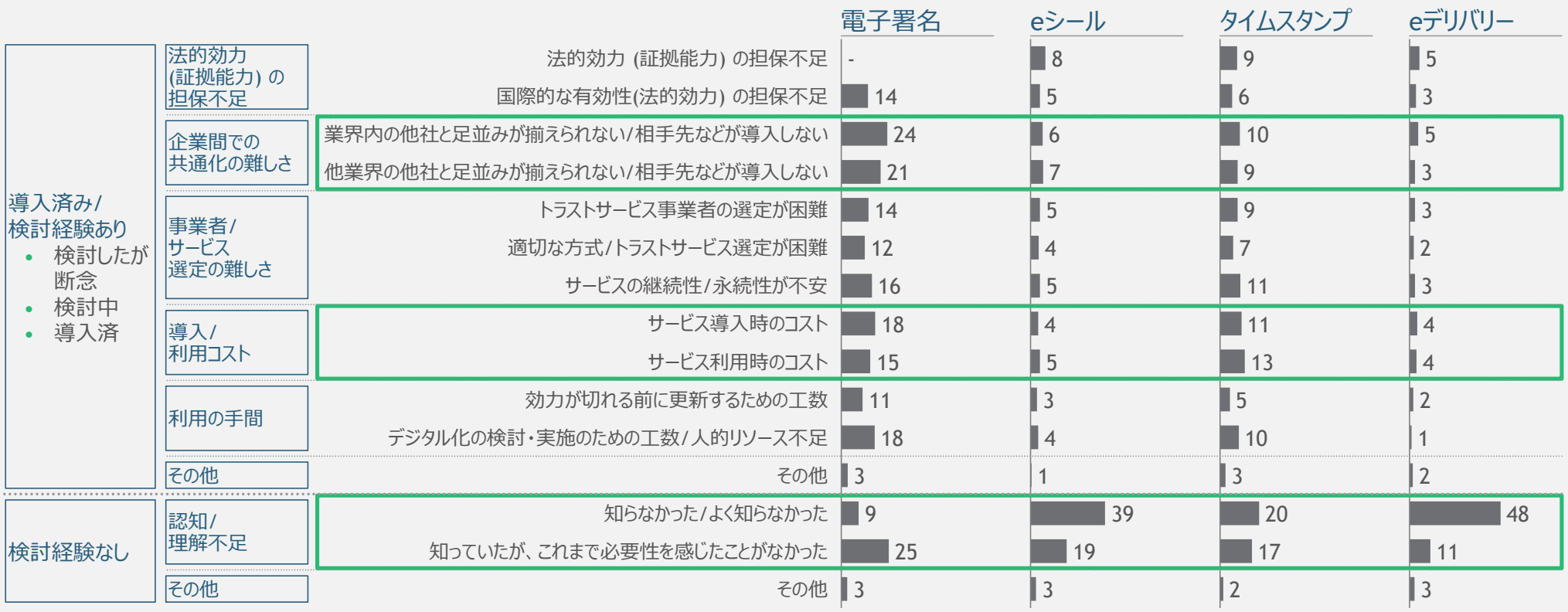
トラストサービスへの課題意識、今後のトラストサービスの基盤整備・普及に向けて考えられる施策例への関心 (導入済み/検討経験あり)



1.トラストサービスの課題で示している割合は、導入済み/検討経験ありの回答者に対する割合 (n数は図中に記載)。また、
2.課題解決の方向性で示している割合は、一つ以上のトラストサービスを導入済み/検討経験ありの回答者に対する割合 (n=204)
Note: 矢印は明確な分析結果に基づくものではないが、関係性が深いと考えられる箇所に記載
Source: 企業アンケートよりBCG分析

企業

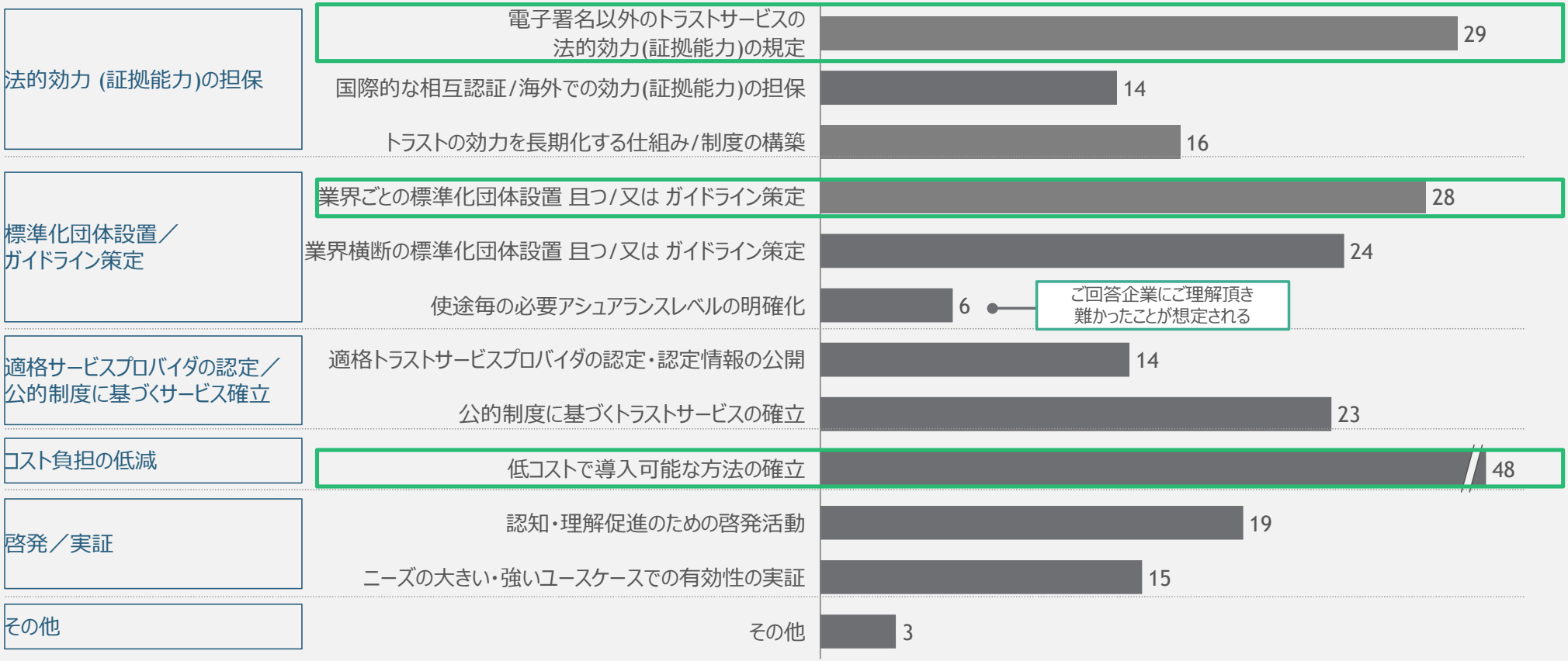
トラストサービスの課題は、各トラストサービスごとに異なるが、全体に「認知/理解不足」が特に大きく、導入済み/検討経験ありの企業の中では「企業間での共通化の難しさ」や「導入/利用コスト」が多く挙げられた



Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業

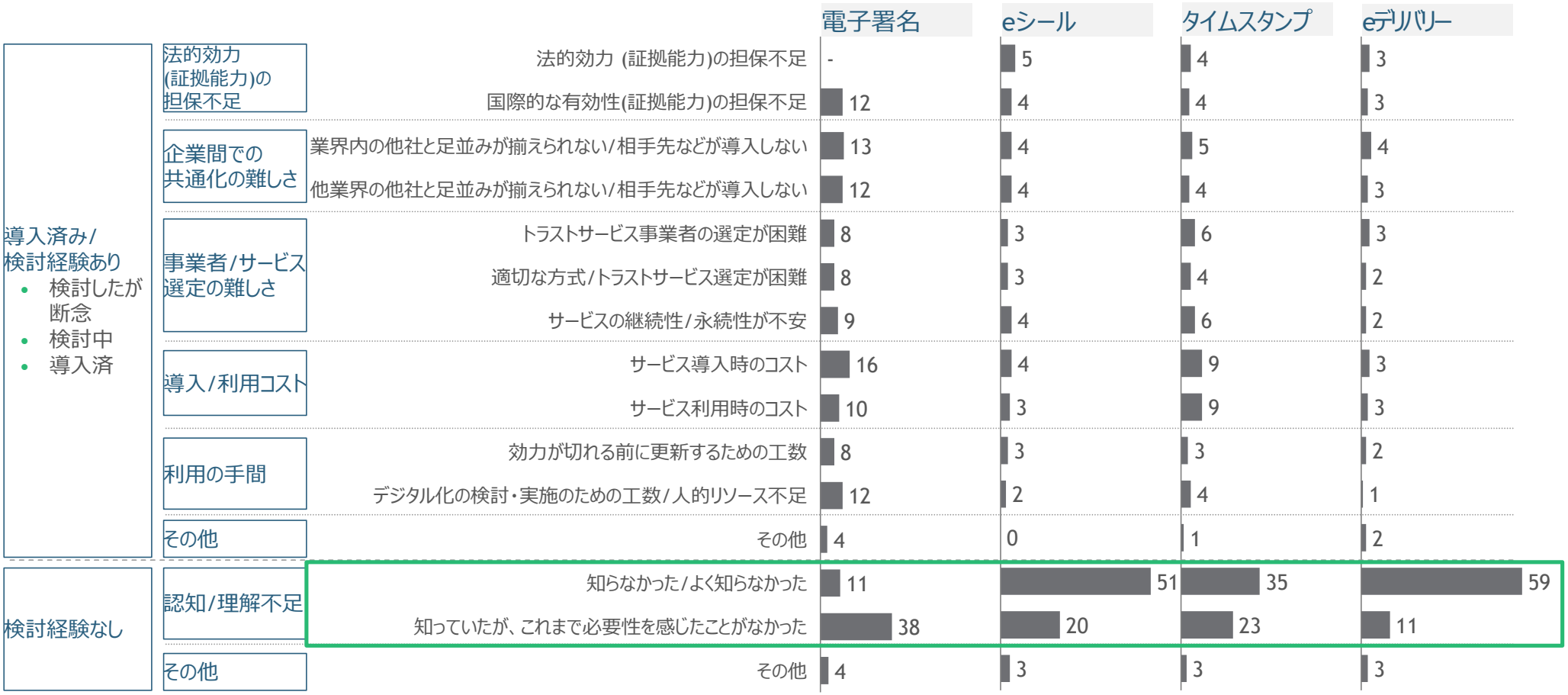
課題解決の方策として、有効な(あれば導入に向け前向きに検討する)ものとして、コスト負担の低減以外では、「電子署名以外のトラストサービスの法的効力(証拠能力)の規定」(29%)、「業界ごとの標準化団体設置 且つ/又は ガイドライン策定」(28%)が特に関心を集めた



Note: 数値は全企業数に対する回答企業割合を記載
Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業 (中小企業)

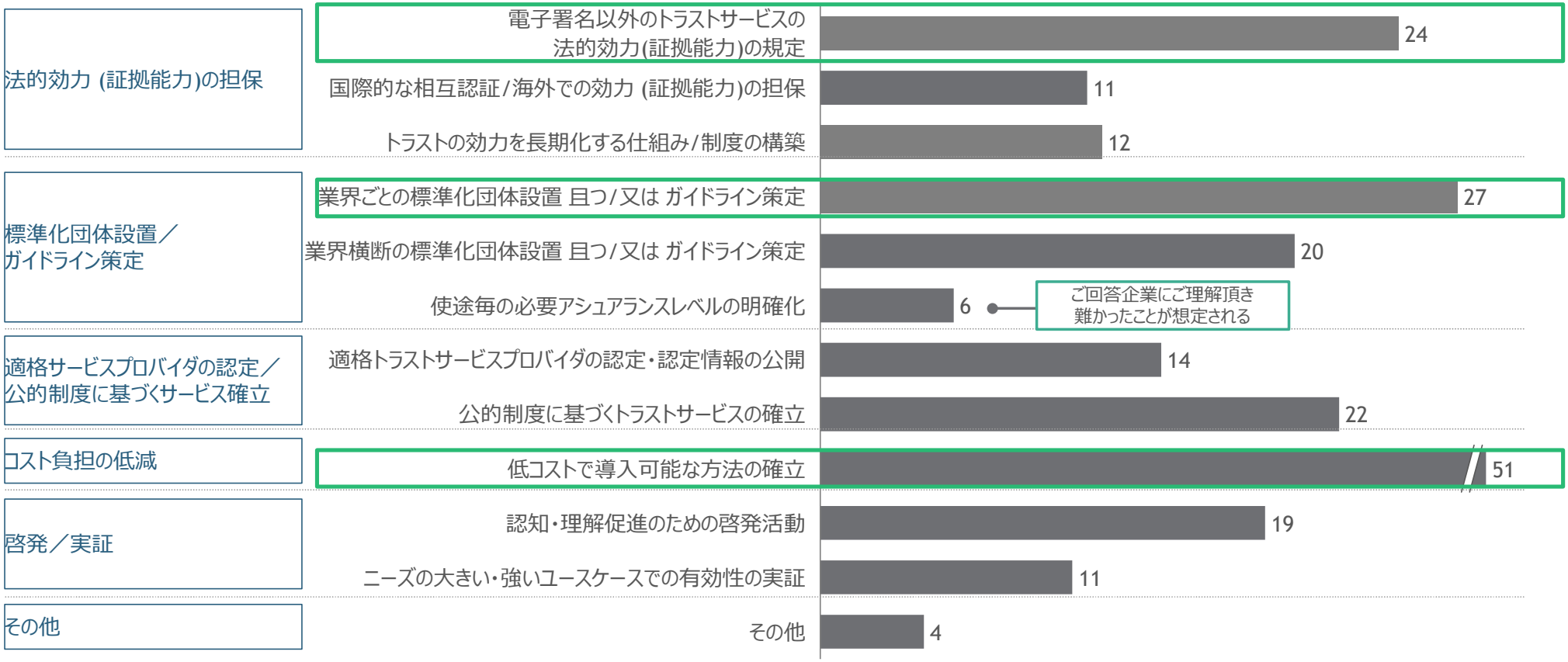
(参考) 中小企業では、認知/理解不足が非常に多く挙げられた



Note: 中小企業 (n=160)を対象に割合を計算
Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業 (中小企業)

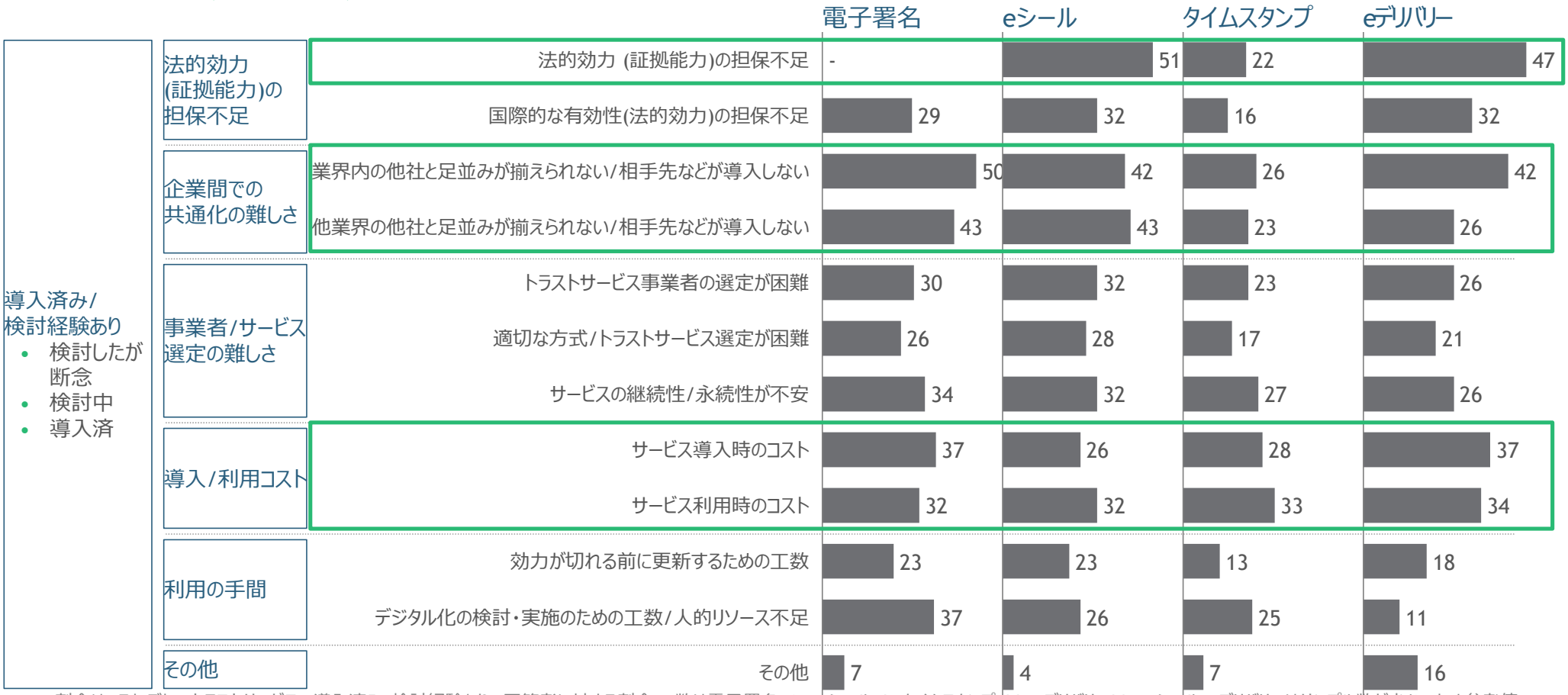
(参考) 有効なものとしては、全体と同様、コスト負担の低減以外では、「電子署名以外のトラストサービスの法的効力(証拠能力)の規定」(24%)、「業界ごとの標準化団体設置 且つ/又は ガイドライン策定」(27%)が特に多く関心を集めた



Note: 中小企業 (n=160)を対象に割合を計算
Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業 (導入済み または 検討経験ありの企業)

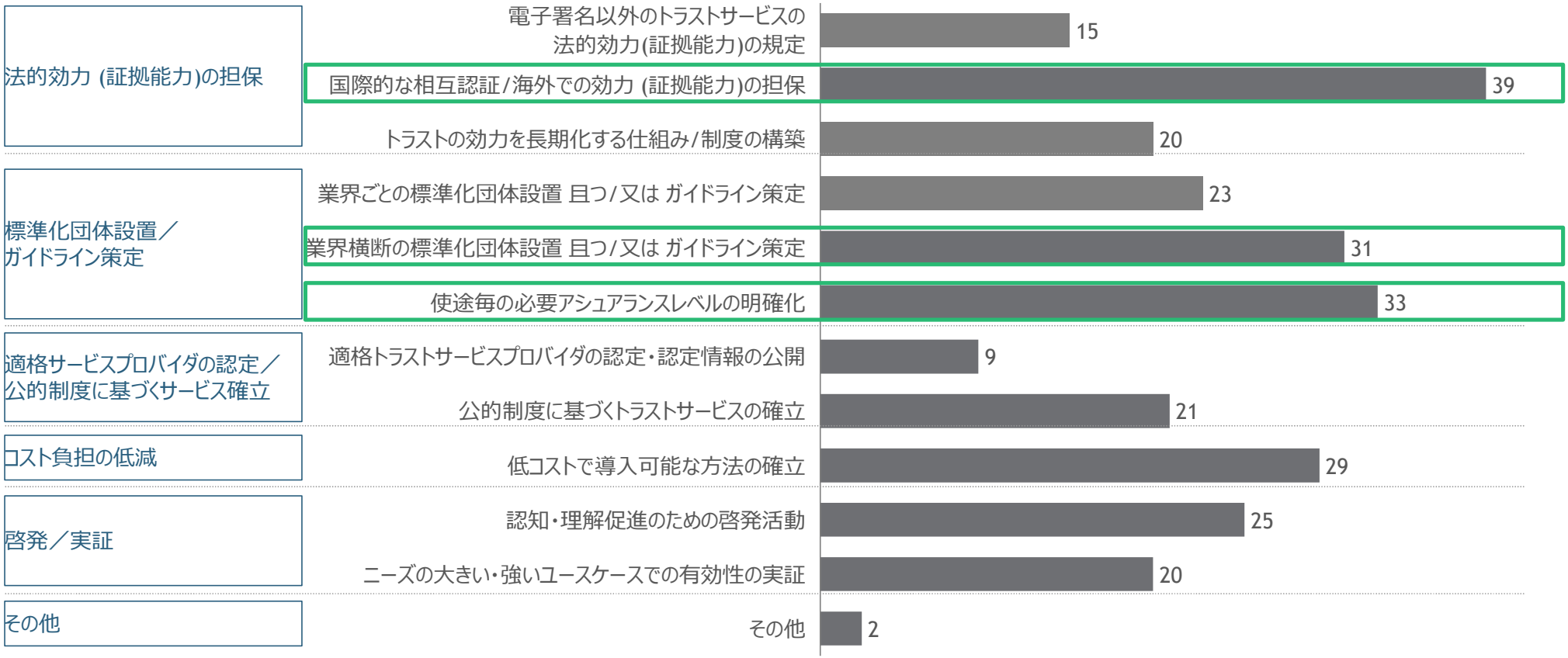
(参考) それぞれのトラストサービスを導入済み/検討経験ありの企業が感じている現状のトラストサービスの課題は、各トラストサービス毎に異なるが、全体に「導入/利用コスト」や「企業間での共通化の難しさ」が大きく、eシールとeデリバリーでは「法的効力(証拠能力)の担保不足」も課題として多く挙げられた



Note: 割合は、それぞれのトラストサービスの導入済み/検討経験ありの回答者に対する割合 (n数は電子署名167、eシール53、タイムスタンプ138、eデリバリー38)。eシール・eデリバリーはサンプル数が少ないため参考値
Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業 (導入済み または 検討経験ありの企業)

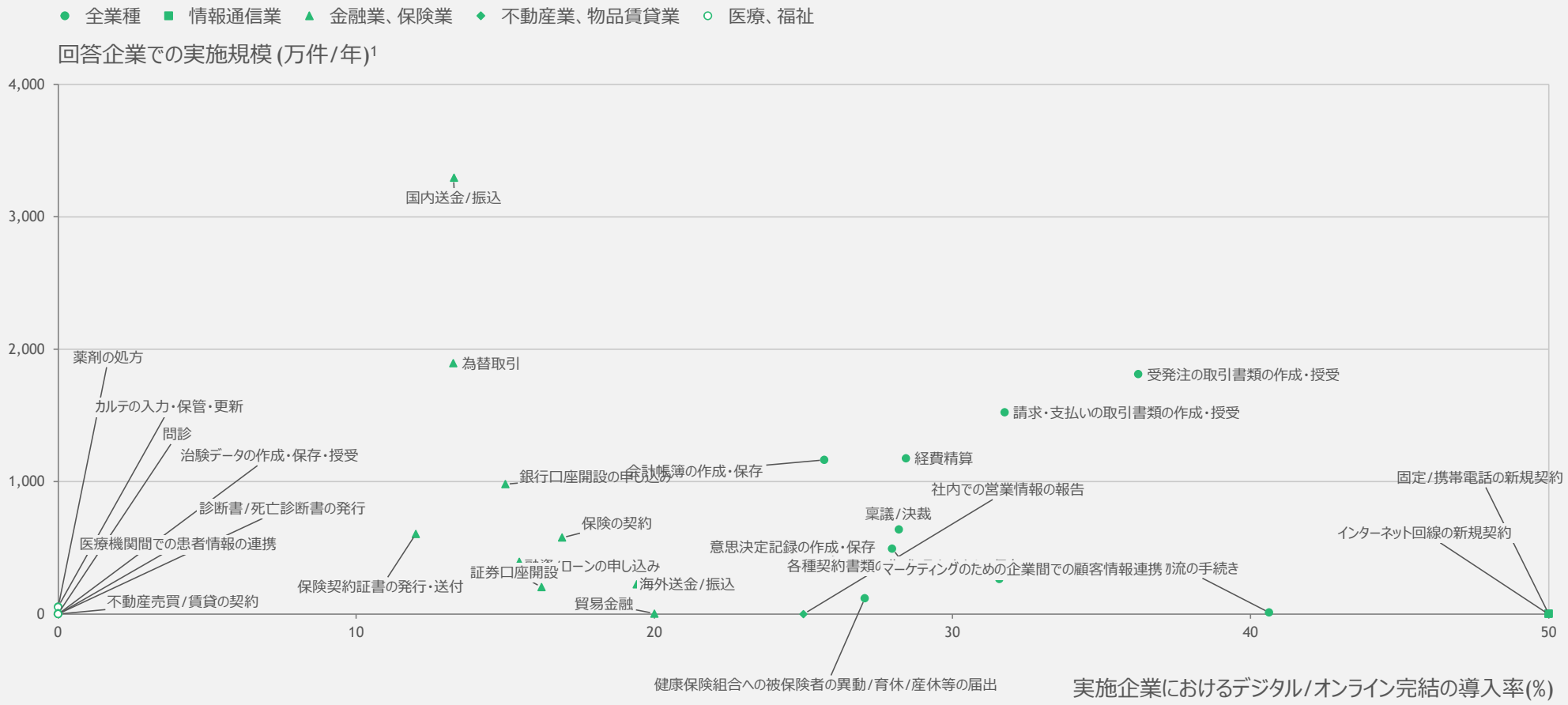
(参考) いずれかのトラストサービスを導入済み/検討経験ありの企業では、「国際的な相互認証/海外での効力 (証拠能力)の担保」(39%)、「アシュアランスレベルの明確化」(33%)「業界横断の標準化団体/ガイドライン」(31%)等が課題として多く挙げられた



Note: 割合は、一つ以上のトラストサービスを導入済み/検討経験ありの回答者に対する割合 (n=204)
Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業 民間分野のデジタル化の実態 (企業視点)

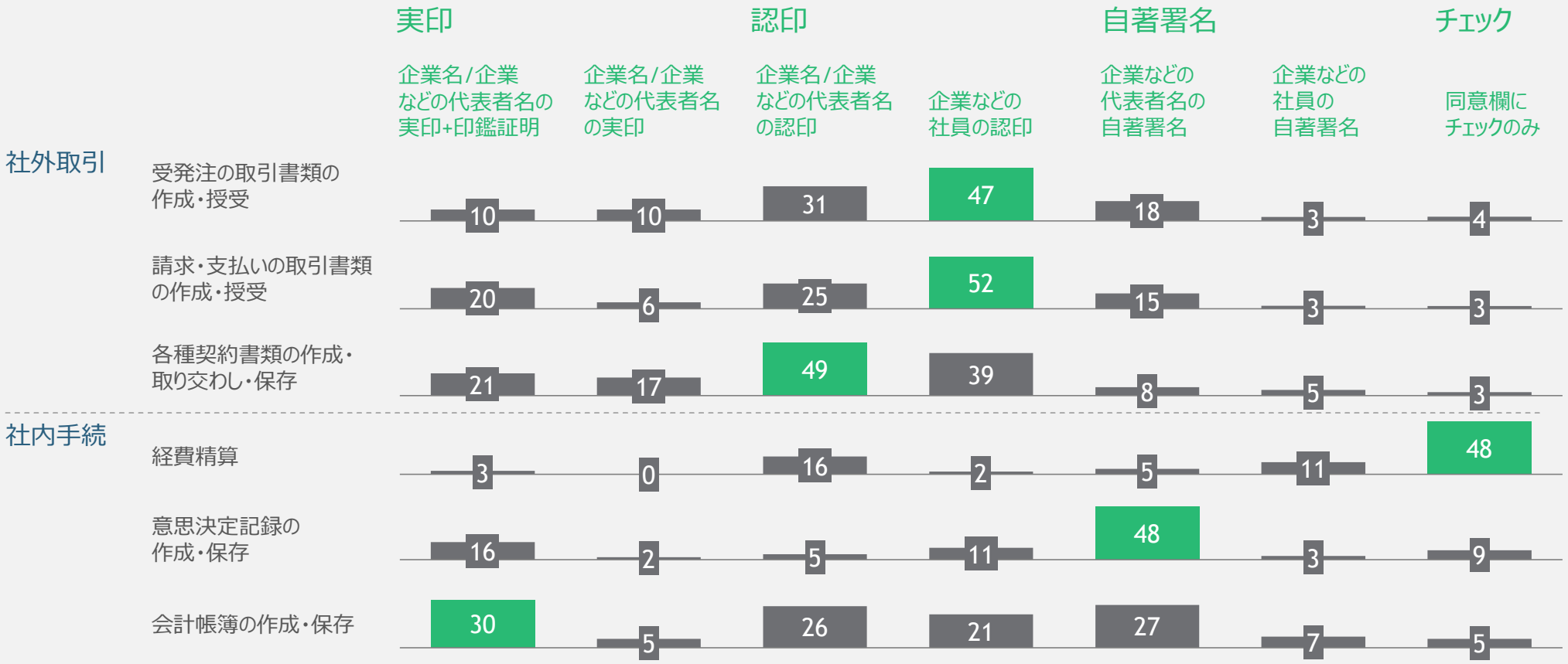
実施規模が大きい手続き等も含め、実施企業におけるデジタル/オンライン完結の導入率は、いずれも半分未満に留まる



1. 実施ありと回答した企業数に、実施規模を乗じた値
Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業 印鑑・署名等への意識

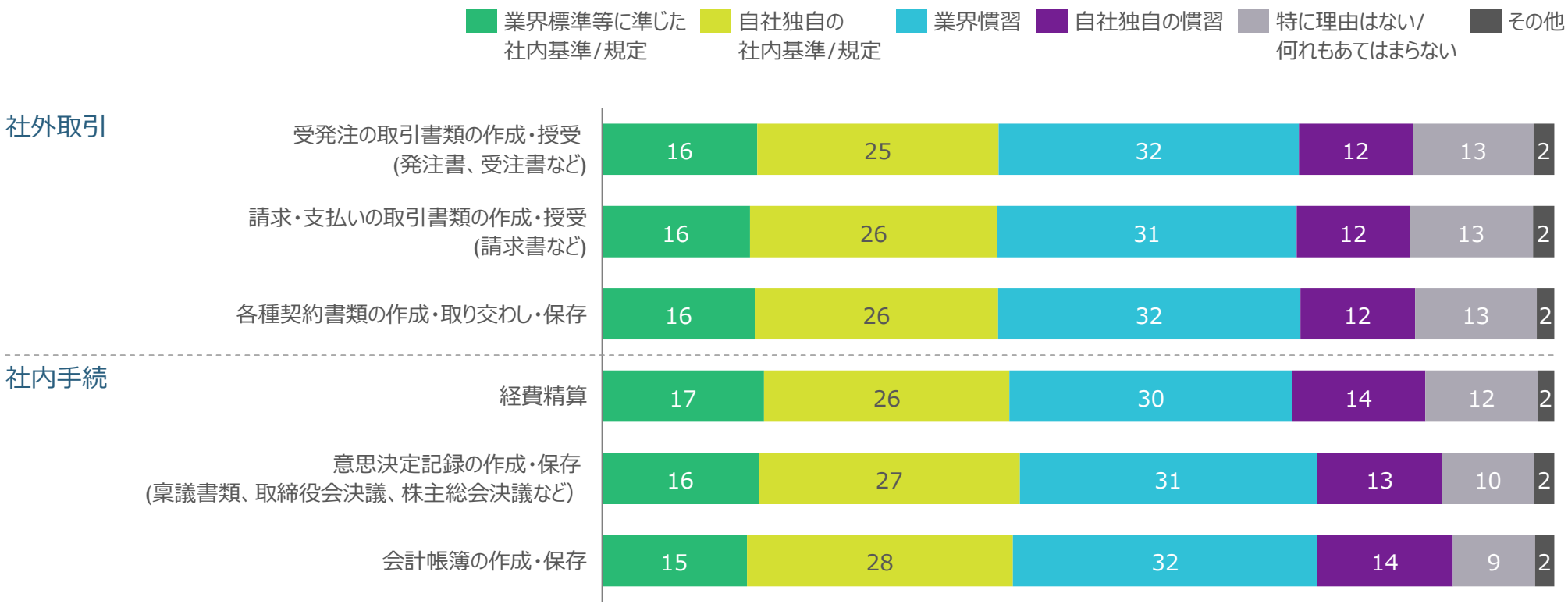
手続き等ごとに使用しているものとしては、社外取引では認印が圧倒的に多い一方、社内手続では会計帳簿の作成・保存を除いて、認印、自著署名、チェックに分散している



Note: 数値は全企業数に対する回答企業割合を記載
Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業 印鑑・署名等への意識

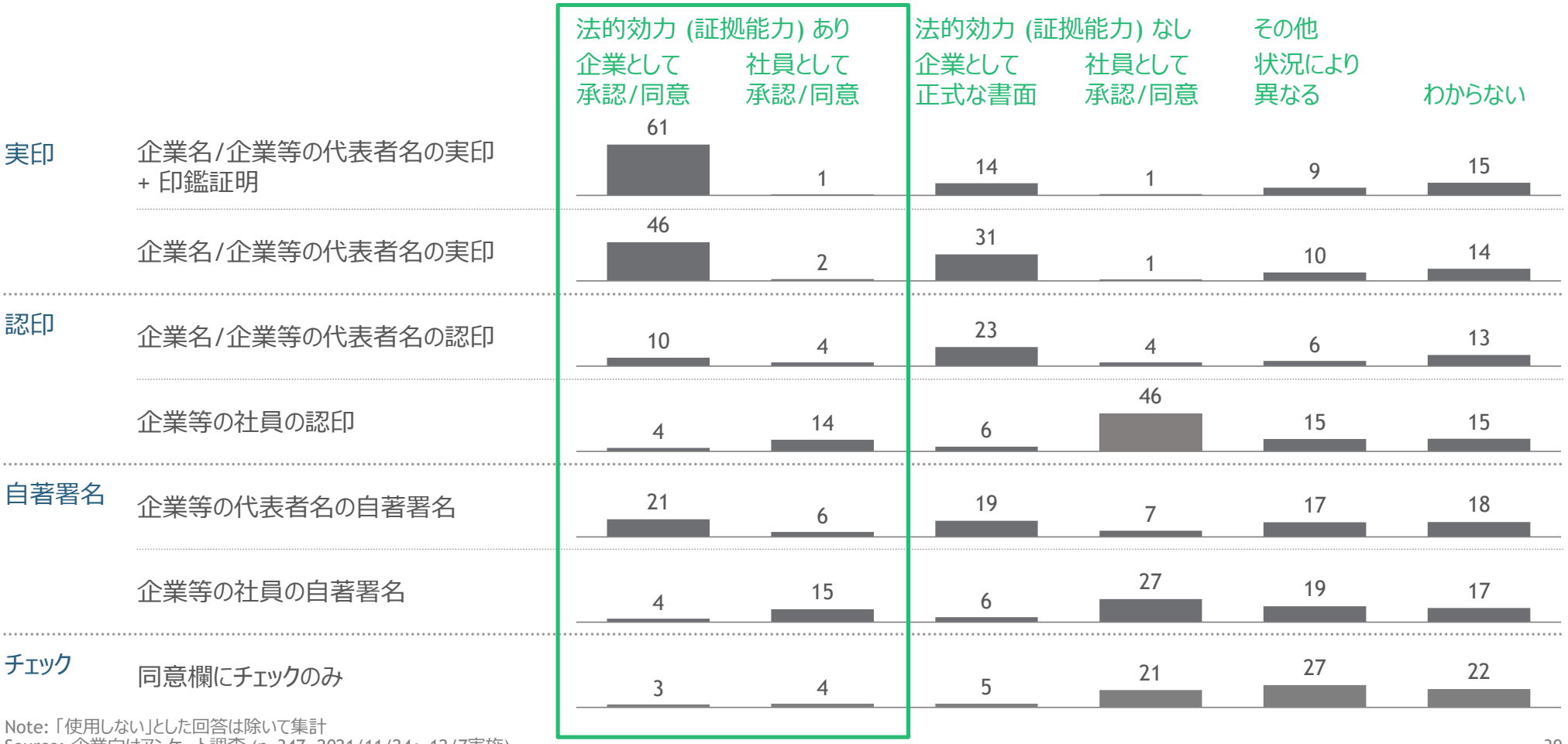
印鑑・署名等の使用根拠は何れも、業界標準等に準じた社内基準や規定は2割未満で、業界慣習が3割前後で最も多く、自社独自の社内基準/規定が3割弱で続く



Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業 印鑑・署名等への意識

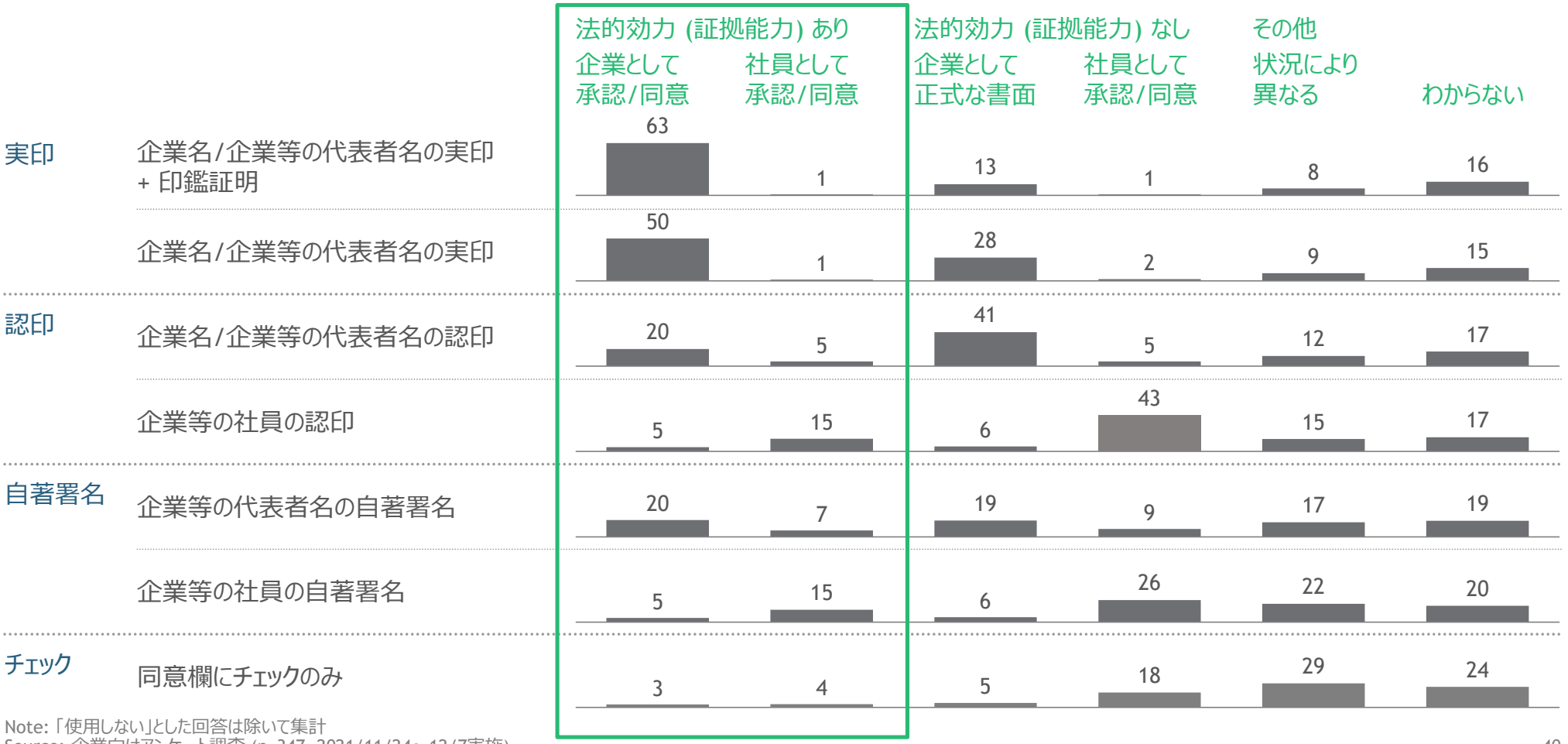
使用側として、法的効力 (証拠能力)の認識は、実印は4~6割以上の一方、認印や自著署名では、その比率は~2割程度以下に留まる



Note:「使用しない」とした回答は除いて集計
Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

企業 印鑑・署名等への意識

受取側として、法的効力 (証拠能力)の認識は、実印は4~6割以上の一方、認印や自著署名では、その比率は~2割程度以下に留まる



Note: 「使用しない」とした回答は除いて集計
Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

アウトライン

1. トラストサービスのニーズ及び現状 についての業種/分野別エキスパートインタビュー
2. 企業/個人へのアンケート調査実施概要
3. 企業向けアンケート結果の分析
4. 個人向けアンケート結果の分析
5. トラスト基盤の整備・普及による期待効果

個人

個人向けアンケート結果

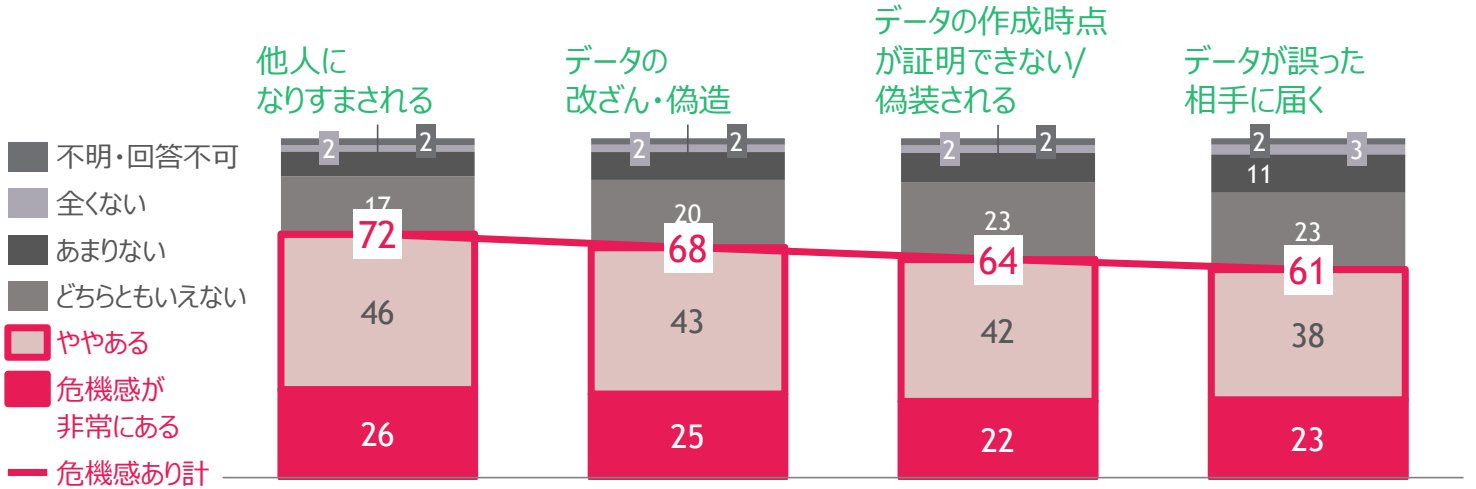
トラストサービスの現状の利用率、課題意識、デジタル完結実現のための検討への関	現状では、個人における電子証明書の利用率は25%留まる。 電子証明書の利用に対する課題は、利用経験者と未経験者で異なるが、 利用経験者からは「利用できるサービスが限定的」(38%)、「マイナンバーカードの紛失が心配」(28%)などが多く挙げられ、 利用未経験では「認知はしているが使い方を知らない」(28%)や「使えるサービスや手続きが少ない」(30%)が多い 上記にして、どのようなことがあれば電子証明書を利用したいかを聴取したところ、 "あれば、電子証明書の利用を検討したい"ものとしては、 「民間を含めた使用できるサービス/手続きの拡大・オンライン化」(59-60%)、 「利用した場合のメリット・使い方や安全性等のわかりやすい周知」(60%) 等が挙げられた
(補足1) 民間分野のデジタル化の実態 (個人視点)	トラストが必要と考えられる手続き等で、1年以内に1割以上の人が実施する実施規模が大きいものも含め、 デジタル/オンラインでの実施経験率は半分に満たないものが殆ど
(補足2) 印鑑・署名等への意識	印鑑・署名等について、使用側としても受取側としても、「法的効力 (証拠能力)を伴う承認または同意の証明」の認識は、 実印+印鑑証明でも半分を下回り、認印や署名では2~3割に留まる

個人

デジタル/オンラインでの手続き等に於いて、本来トラストサービスにより防ぎ得るリスクに危機意識を持つ人は多く、デジタル/オンラインの手続き等の利用を阻害する一因となっている

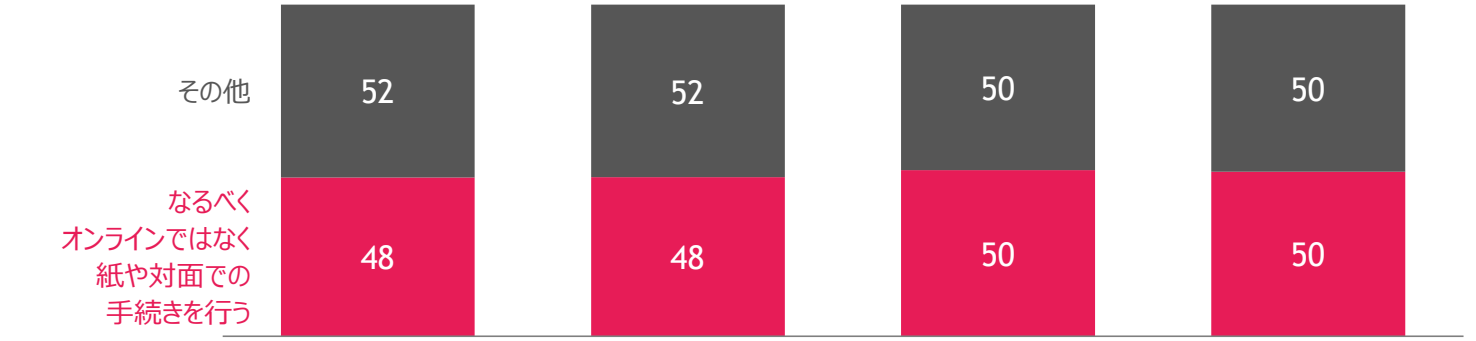
トラストサービスにより防ぐことができるリスクへの危機意識

デジタル/オンラインでの手続き等に対して、トラストサービスにより本来防ぎ得るリスクに危機意識を持つ人は多い



上記の危機意識への対応方法

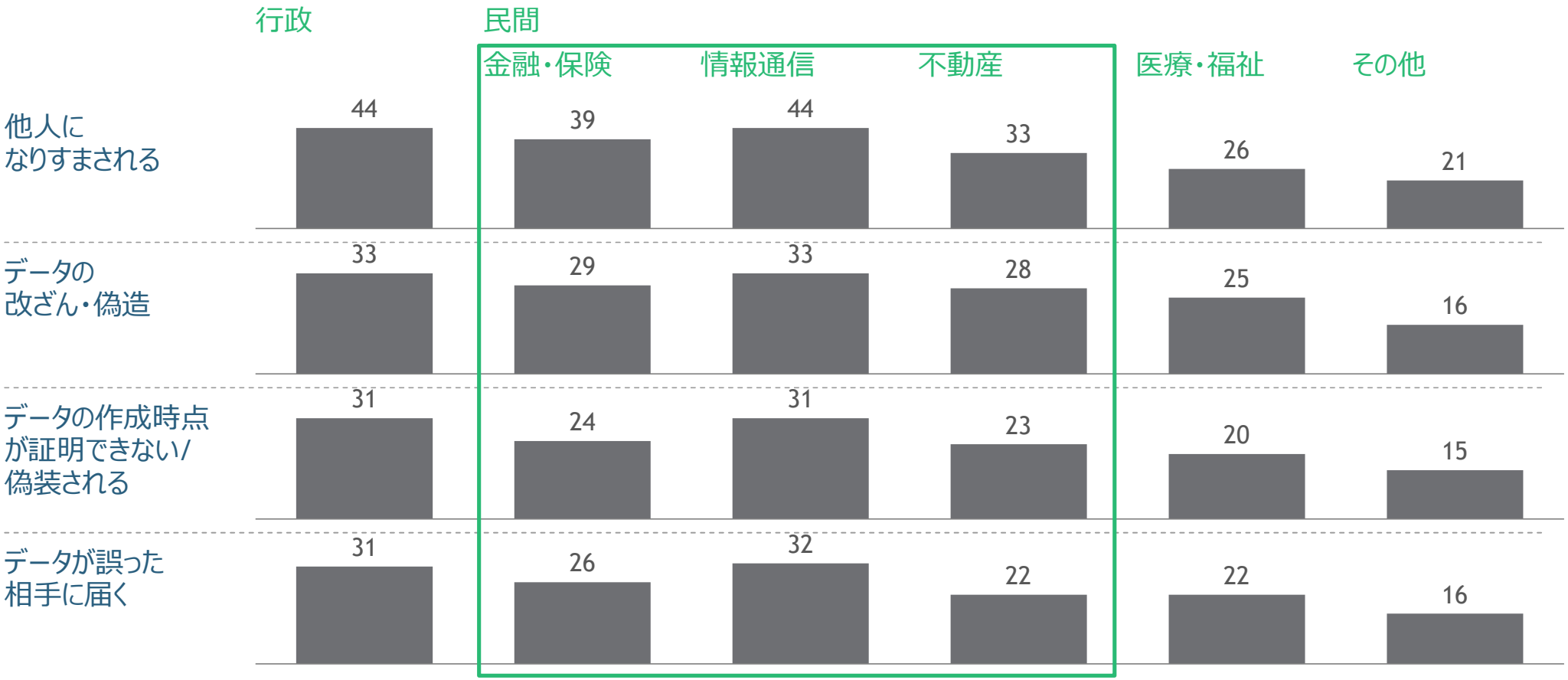
上記の危機意識を持つ人のうち、リスクに対応するため、オンラインの手続きではなく紙や対面の手続きを使用する人が約1/2いる



Source: 個人向けアンケート調査 (n=4,406、2021/11/19～11/24実施)

個人

民間の業界別では特に、「情報通信」「金融・保険」「不動産」の手続き等へのリスク意識が高い

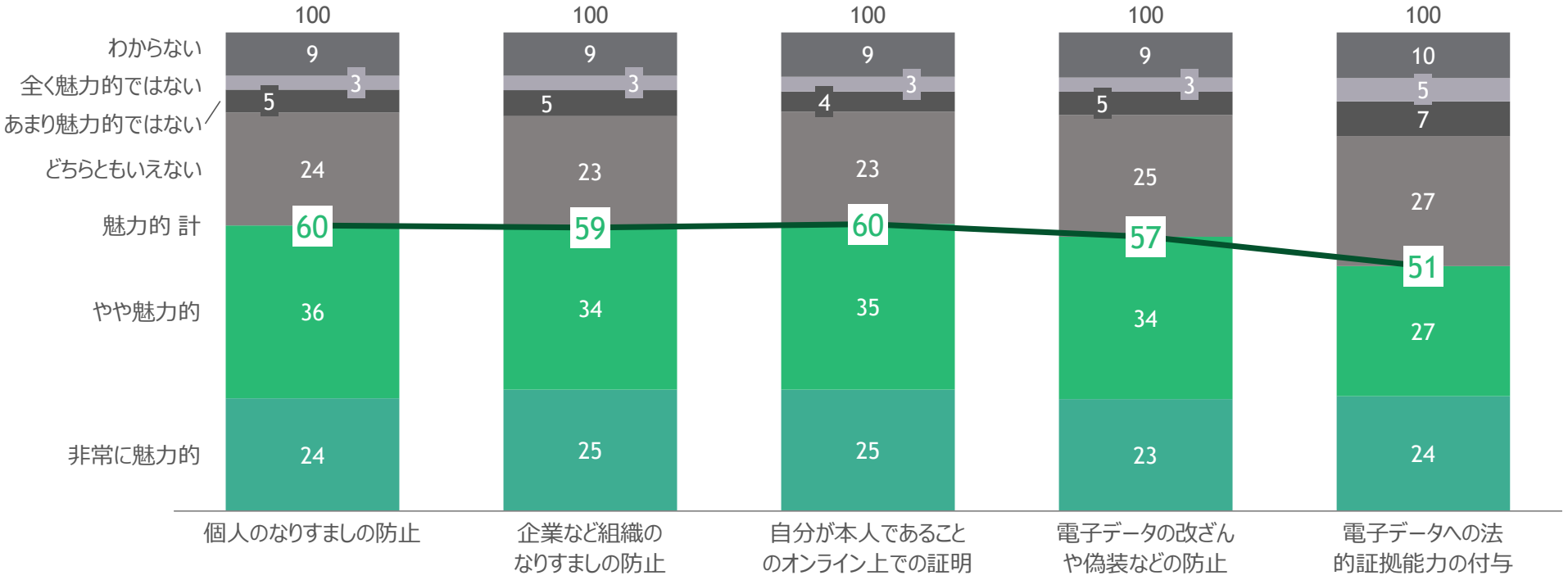


Source: 個人向けアンケート調査 (n=4,406、2021/11/19～11/24実施)

個人

トラストサービスによって享受できるメリットに魅力を感じる人は、「個人/組織のなりすましの防止」(60%)、「自分が本人であることのオンライン上での証明」(60%)など50-60%程度を占める

電子証明書などを用いることで実現できるメリットの魅力度

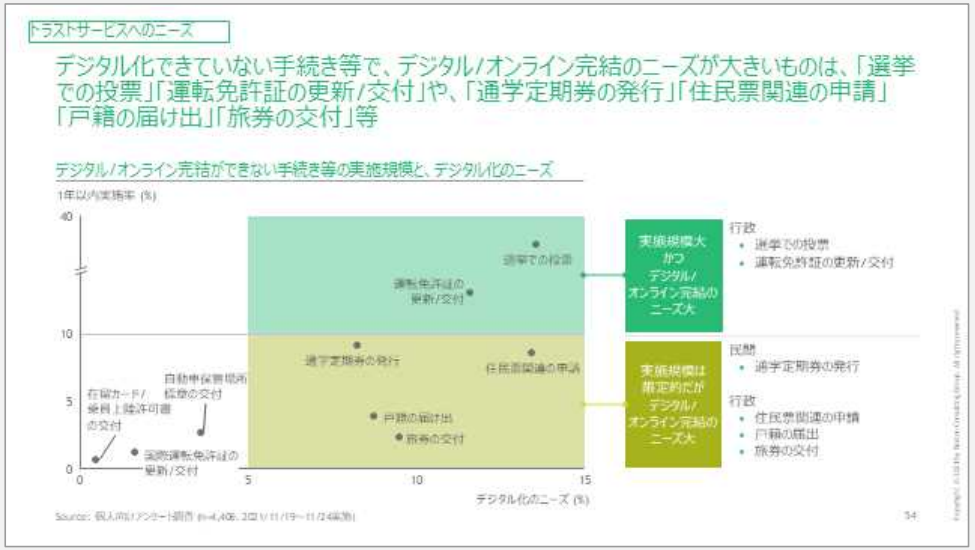


Source: 個人向けアンケート調査 (n=4,406、2021/11/19～11/24実施)

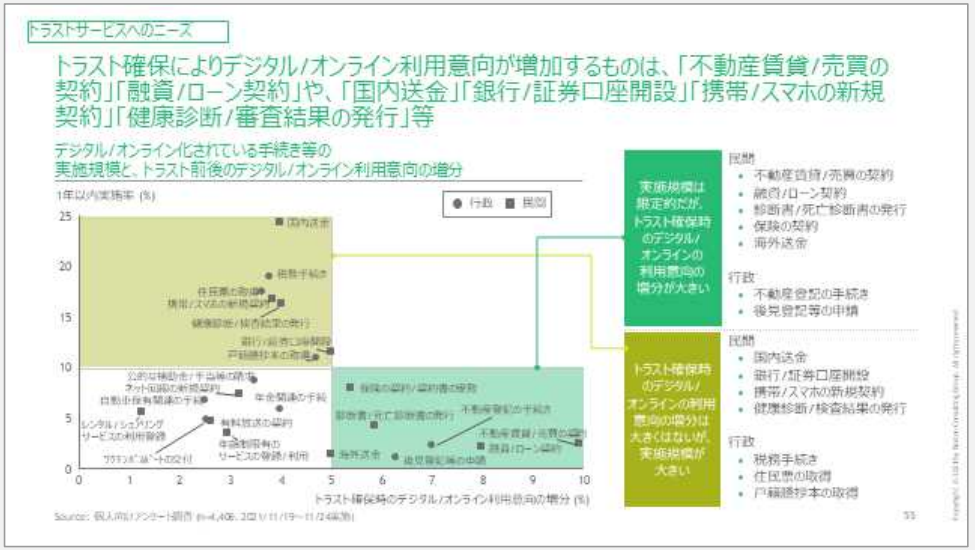
個人

トラスト確保のニーズがある手続き等には、デジタル/オンライン完結ができないがそのニーズが大きいものと、トラストの確保によりデジタル/オンライン利用意向が高まるものがある

トラストで解決できる課題によりデジタル化できていない手続き 等



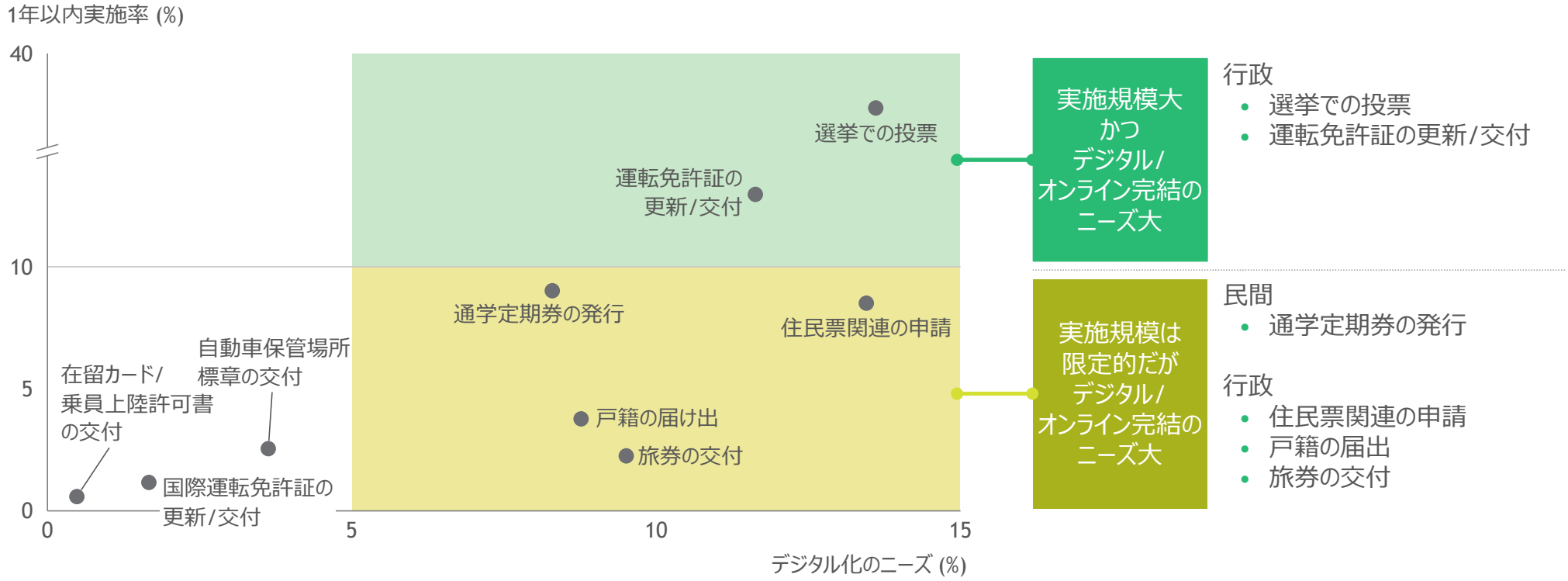
デジタル化されているがトラストの確保によりオンライン移行が高まる手続き 等



個人

デジタル化できていない手続き等で、デジタル/オンライン完結のニーズが大きいものは、「選挙での投票」「運転免許証の更新/交付」や、「通学定期券の発行」「住民票関連の申請」「戸籍の届け出」「旅券の交付」 等

デジタル/オンライン完結ができない手続き等の実施規模と、デジタル化のニーズ

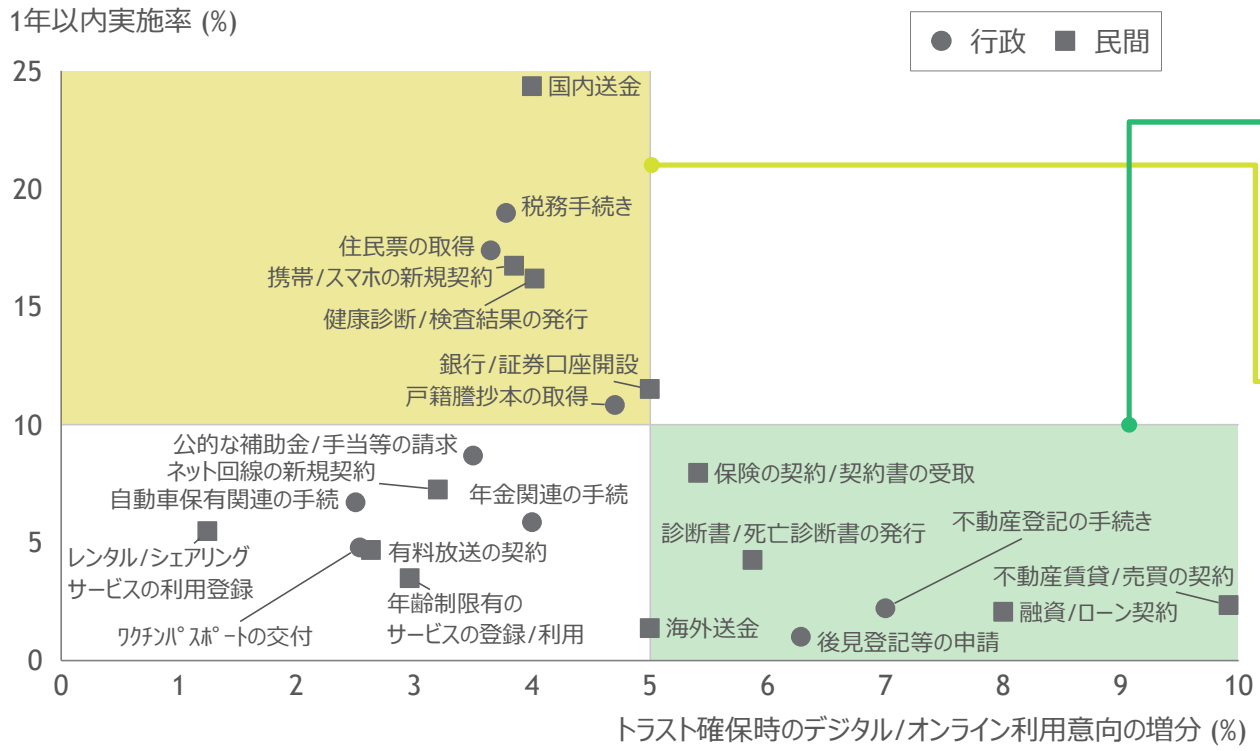


Source: 個人向けアンケート調査 (n=4,406、2021/11/19～11/24実施)

個人

トラスト確保によりデジタル/オンライン利用意向が増加するものは、「不動産賃貸/売買の契約」「融資/ローン契約」や、「国内送金」「銀行/証券口座開設」「携帯/スマホの新規契約」「健康診断/審査結果の発行」等

デジタル/オンライン化されている手続き等の実施規模と、トラスト前後のデジタル/オンライン利用意向の増分



実施規模は限定的だが、トラスト確保時のデジタル/オンラインの利用意向の増分が大きい

民間
- 不動産賃貸/売買の契約
- 融資/ローン契約
- 診断書/死亡診断書の発行
- 保険の契約
- 海外送金

行政
- 不動産登記の手続き
- 後見登記等の申請

トラスト確保時のデジタル/オンラインの利用意向の増分は大きくはないが、実施規模が大きい

民間
- 国内送金
- 銀行/証券口座開設
- 携帯/スマホの新規契約
- 健康診断/検査結果の発行

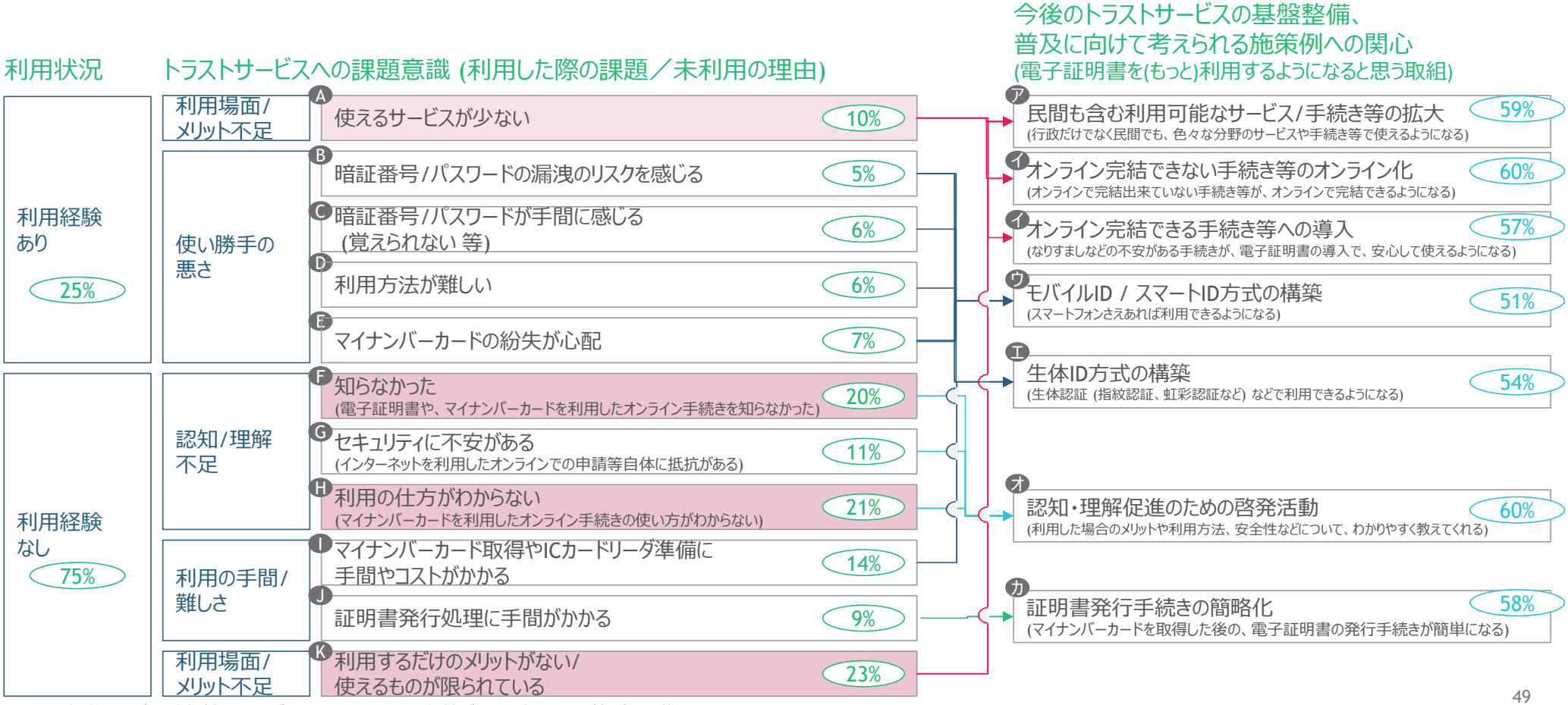
行政
- 税務手続き
- 住民票の取得
- 戸籍謄抄本の取得

Source: 個人向けアンケート調査 (n=4,406、2021/11/19～11/24実施)

個人

利用経験ありは25%で、課題は「利用するだけのメリットがない/使えるものが限られている」「利用の仕方がわからない」「知らなかった」、施策例は「認知・理解促進のための啓発活動 (メリットや利用方法、安全性などをわかりやすく教えてくれる) 」「オンライン完結できない手続き等のオンライン化」「民間も含む利用可能なサービス/手続き等の拡大」が、それぞれトップ3

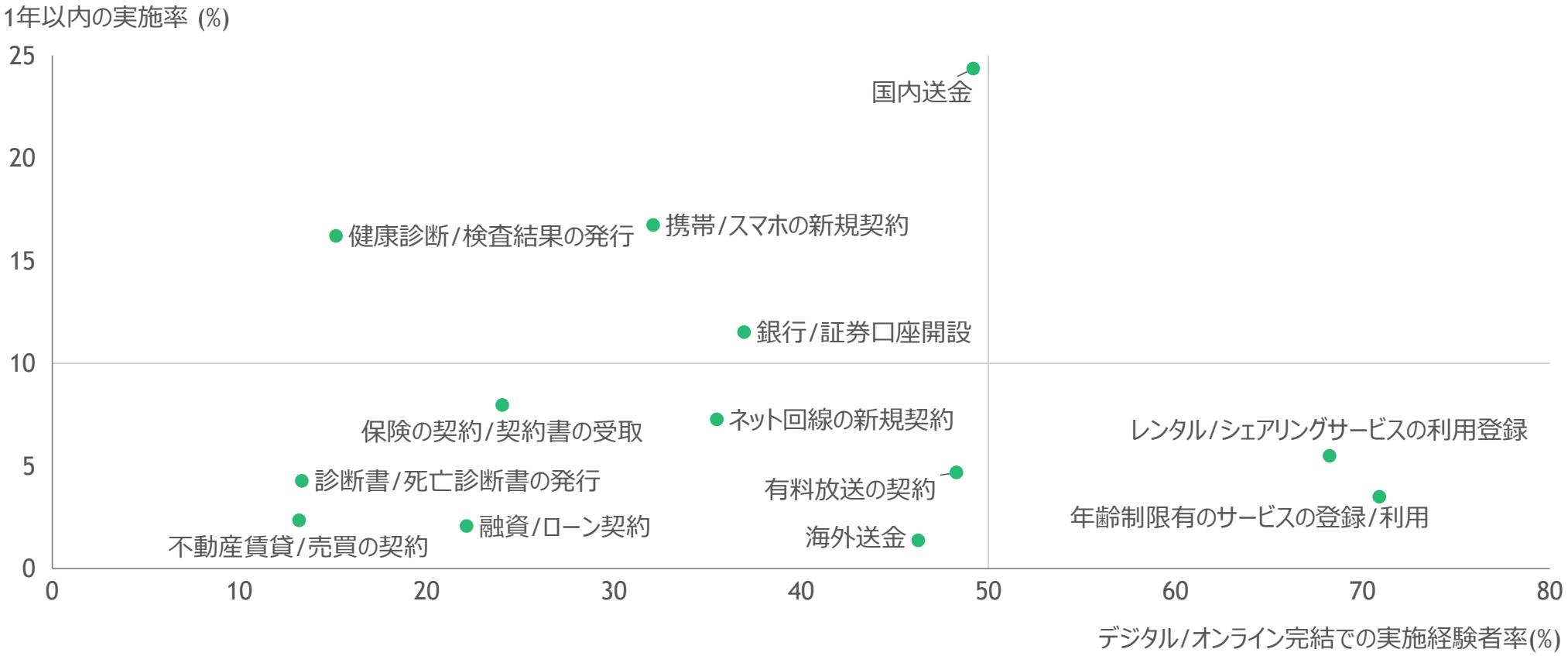
トラストサービスへの課題意識、今後のトラストサービスの基盤整備・普及に向けて考えられる施策例への関心 (個人)



Note：矢印は明確な分析結果に基づくものではないか、関係性が深いと考えられる箇所に記載
Source: 個人アンケートよりBCG分析

トラストが必要と考えられる手続き等で、1年以内に1割以上の人が実施する実施規模が大きいものも含め、デジタル/オンラインでの実施経験率は半分に満たないものが殆ど

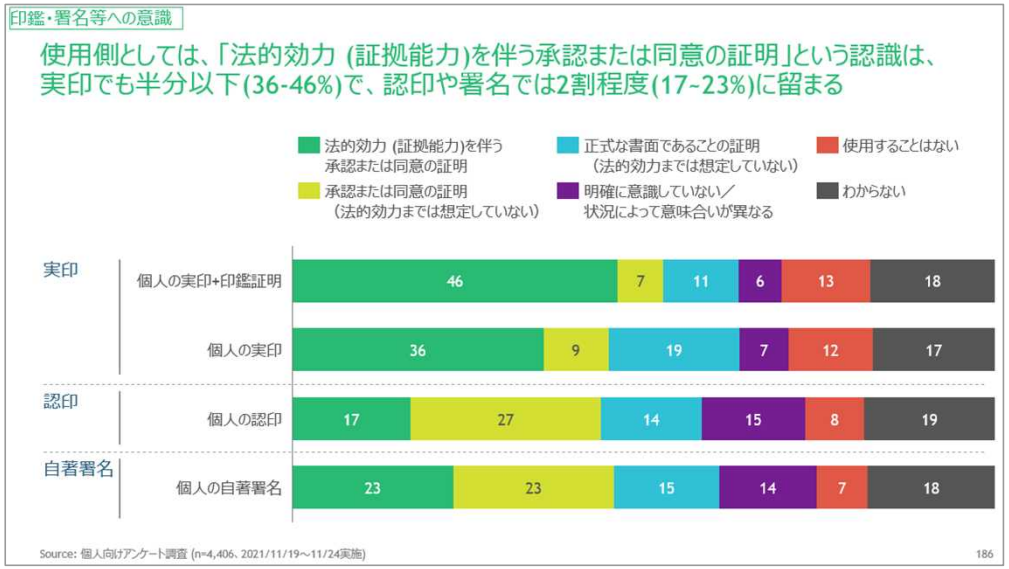
例: 国内送金、携帯/スマホの新規契約、銀行/証券口座開設、健康診断結果の発行 等

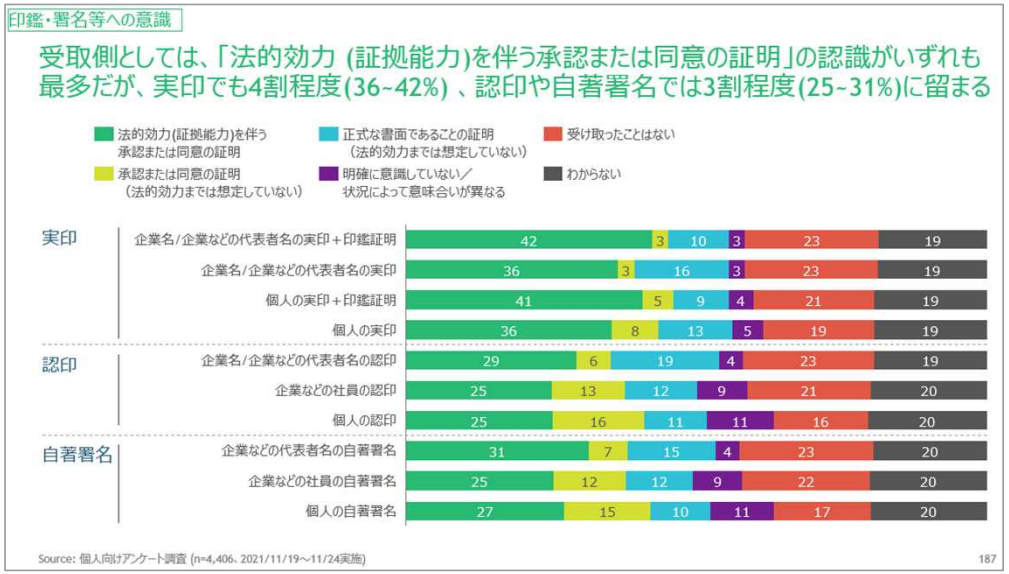


Source: 個人向けアンケート調査 (n=4,406、2021/11/19～11/24実施)

個人 印鑑・署名等への意識

印鑑・署名等について、使用側としても受取側としても、「法的効力 (証拠能力)を伴う承認または同意の証明」の認識は、実印+印鑑証明でも半分を下回り、認印や署名では2~3割に留まる

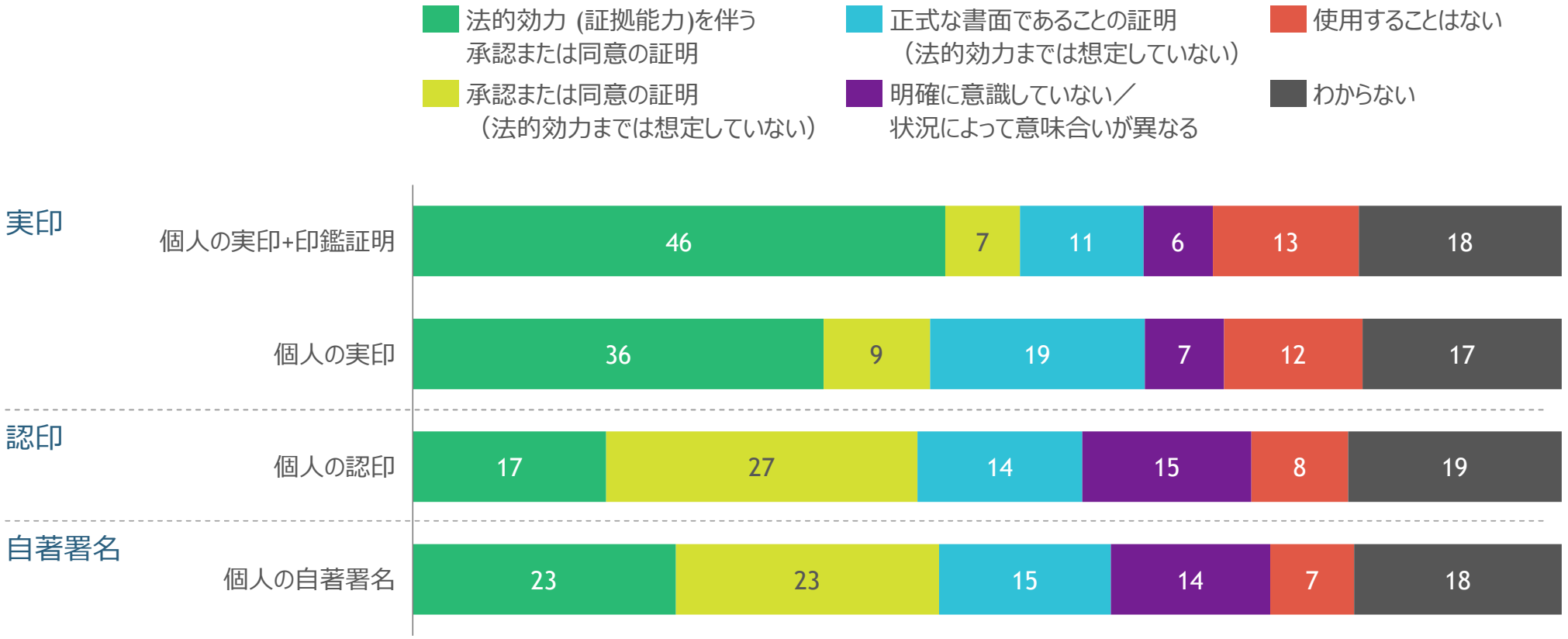




Source: 個人向けアンケート調査 (n=4,406、2021/11/19～11/24実施)

個人 印鑑・署名等への意識

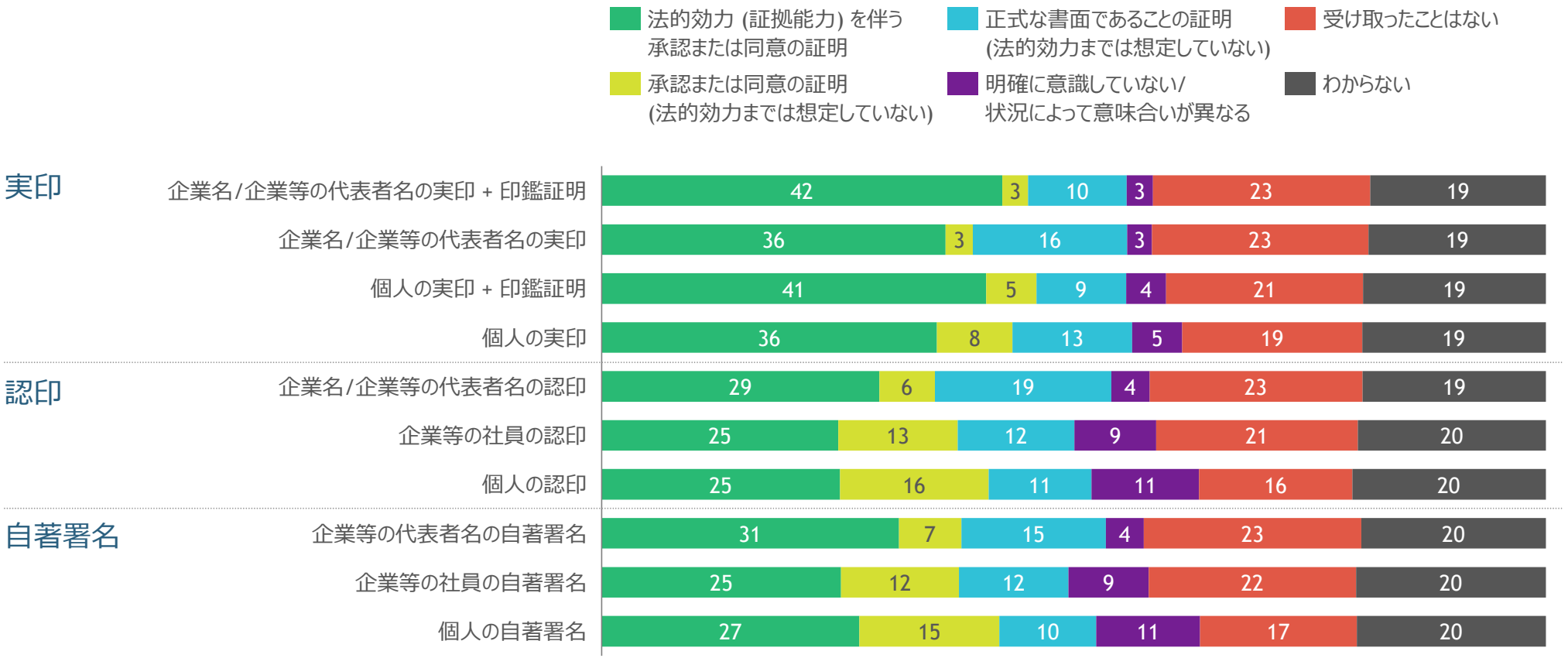
使用側としては、「法的効力 (証拠能力)を伴う承認または同意の証明」という認識は、実印でも半分以下(36-46%)で、認印や署名では2割程度(17~23%)に留まる



Source: 個人向けアンケート調査 (n=4,406、2021/11/19～11/24実施)

個人 印鑑・署名等への意識

受取側としては、「法的効力 (証拠能力) を伴う承認または同意の証明」の認識がいずれも最多だが、実印でも4割程度 (36~42%)、認印や自著署名では3割程度 (25~31%) に留まる



Source: 個人向けアンケート調査 (n=4,406、2021/11/19～11/24実施)

アウトライン

1. トラストサービスのニーズ及び現状 についての業種/分野別エキスパートインタビュー
2. 企業/個人へのアンケート調査実施概要
3. 企業向けアンケート結果の分析
4. 個人向けアンケート結果の分析
5. トラスト基盤の整備・普及による期待効果

トラスト確保によるデジタル化の期待効果の見積り/イメージ具体化 (まとめ)

トラスト基盤の整備・普及により、トラスト確保によるデジタル化の促進や、デジタル/オンラインでのトラストの強化が果たされ、
「業務量削減」「人為的ミスの回避」「詐欺被害等の犯罪防止」「コンプライアンス遵守強化」等の効果が期待されている

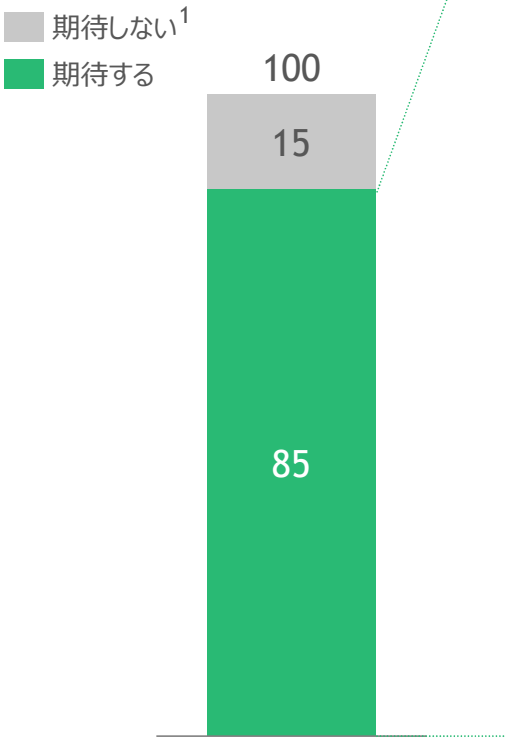
- トラスト確保により、自社のデジタル化が進展することを期待する企業は85%あり、
  中でも「不動産売買/賃貸の契約」、「銀行口座開設の申し込み」、「取引書類の作成」等のデジタル化への期待が大きい
  - 中でも、海外と取引があり、トラストサービスでも海外連携が必要と考えられるものとしては、「各種取引書類等の作成/授受」「銀行口座開設の申し込み」「海外送金/振り込み」等が挙げられる
  - 上記で、海外取引がある企業では、各手続き等の10%~40%程度を占める

- 上記により期待される効果として、企業からは、「業務量削減」の他、「人為的ミスの回避」「コストの削減」「詐欺等の犯罪被害防止」「コンプライアンス遵守の強化」等も挙げられている
  - 例えば、銀行口座の新規開設では、従前は紙による本人確認/利用開始案内を前提としていたが、トラストを確保しながらデジタル化されることによって、企業の「業務量/郵送コスト削減」、「書面偽造による不正口座作成等の犯罪被害防止」や、職員による不正防止での「コンプライアンス遵守の強化」、また個人の「手間の削減」「手続きの迅速化」の効果が見込まれる

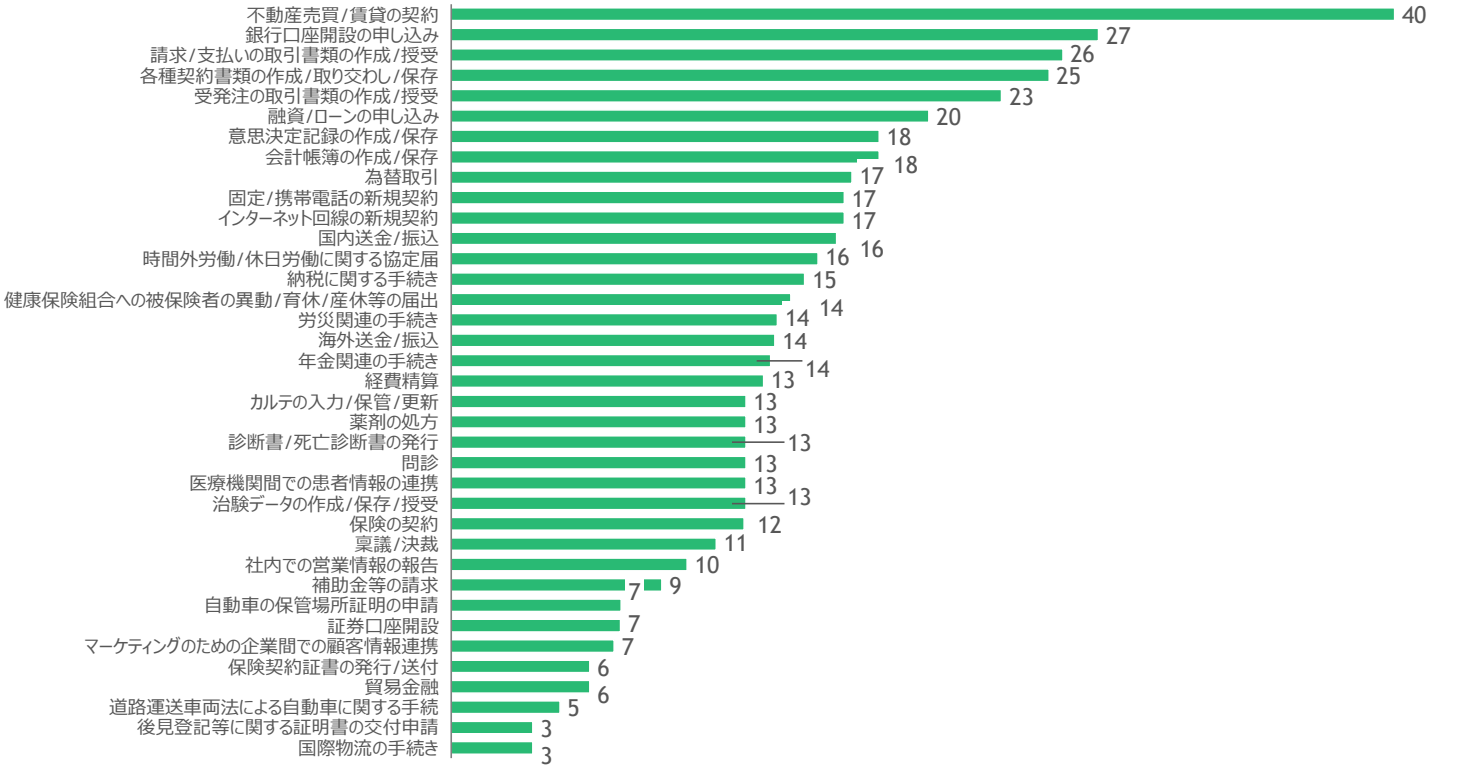
- なお、上記効果の概算想定規模としては、「業務量削減」では~100億時間 (600万人相当) の削減が見込まれる他、
  「詐欺等の犯罪被害防止」100億円規模が見込まれる

トラスト確保により、自社のデジタル化が何らかの手続きにおいて進展することを期待する企業は85%あり、ニーズのあるものに関しては概ね10~25%がデジタル化を期待

トラスト確保によるデジタル化を期待するか否か



各業種のトラスト確保時における、手続きごとのデジタル化を期待する割合



1. トラストが導入された場合にデジタル化された手続きを使用したいと回答した割合を期待すると記載
Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施)

トラストを確保したデジタル化による期待効果として、企業からは「業務量削減」「人為的ミスの回避」の他、「コストの削減」「詐欺等の犯罪被害防止」「コンプライアンス遵守の強化」等も挙げられた

業務量削減

" 例えば個人の口座開設時等、現状のeKYCでは、裏側の作業を膨大な人手で行っており、その削減にはニーズがある" (金融)

" テレワークが主のため、紙面確認で出社する必要がない" (不動産)

48%
(347社中の166社) [1]

人為的ミスの回避

" 現状、会計帳簿の作成・保存は目視で行っているが、ミスが起こる可能性があり、この改善が行える" (建設)

" 経費の自動計算が行われ、ミスの可能性が減少する" (小売)

24%
(347社中の43社) [1]

コストの削減

" 紙の保管コストや人件費が削減できる" (金融)

" 郵送コストが削減できる" (製造業)

" 契約書の回収は直接出向く場合が多く、このコストが削減できる" (教育)

22%
(347社中の36社) [1]

コンプライアンス遵守の強化

" 営業現場からの業績成績の水増し報告/改ざん防止が長年の課題" (不動産)

" 時間外労働・休日労働の管理に関して、法的な基準を守れているか明確にしやすい" (医療)

14%
(347社中の31社) [1]

詐欺等の犯罪防止

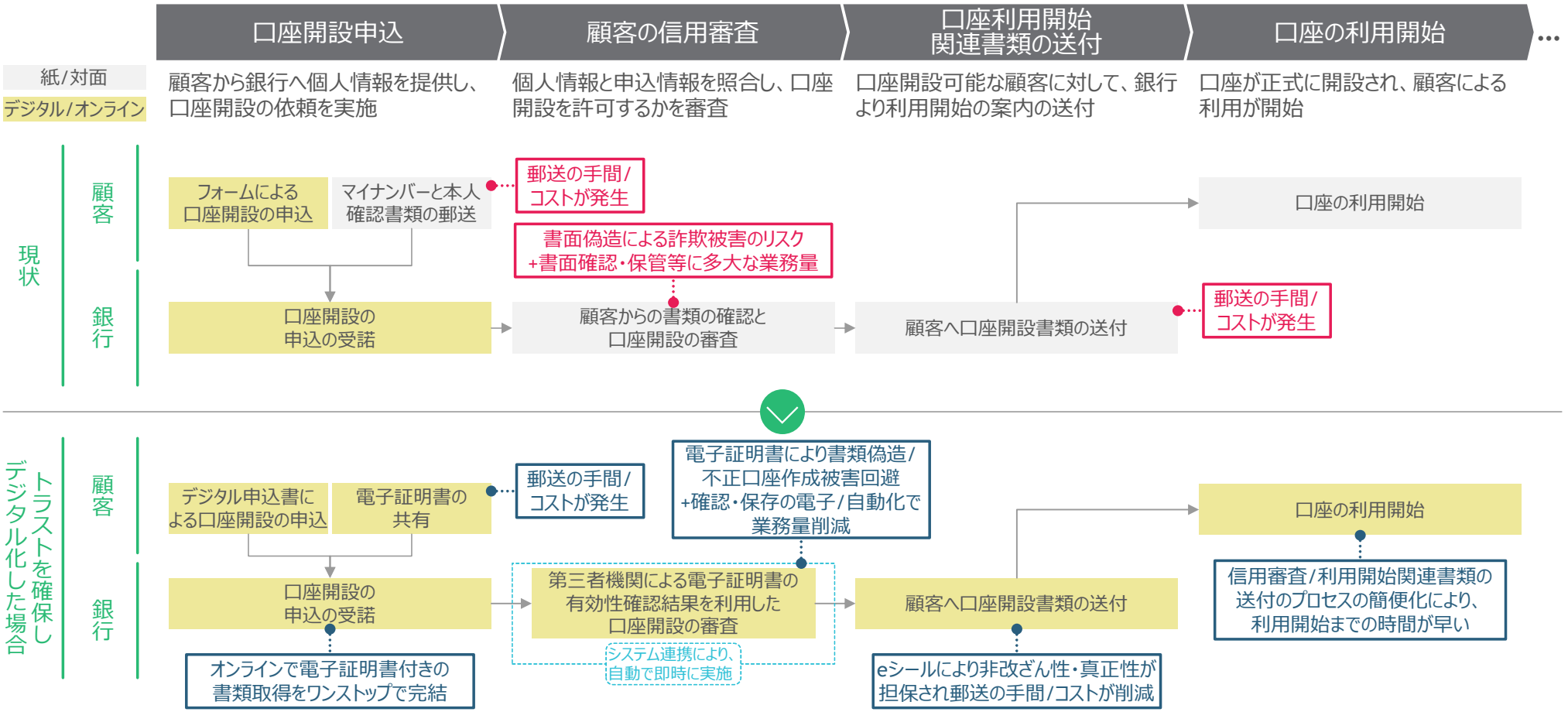
" 業界では「地面師」等の詐欺被害が発生した例もあり、書類の改ざん/偽造の防止は重要課題" (不動産)

" 融資/ローンの申し込みでは顧客の不正申告が考えられ、双方を防ぐことができる" (金融)

6%
(347社中の10社) [1]

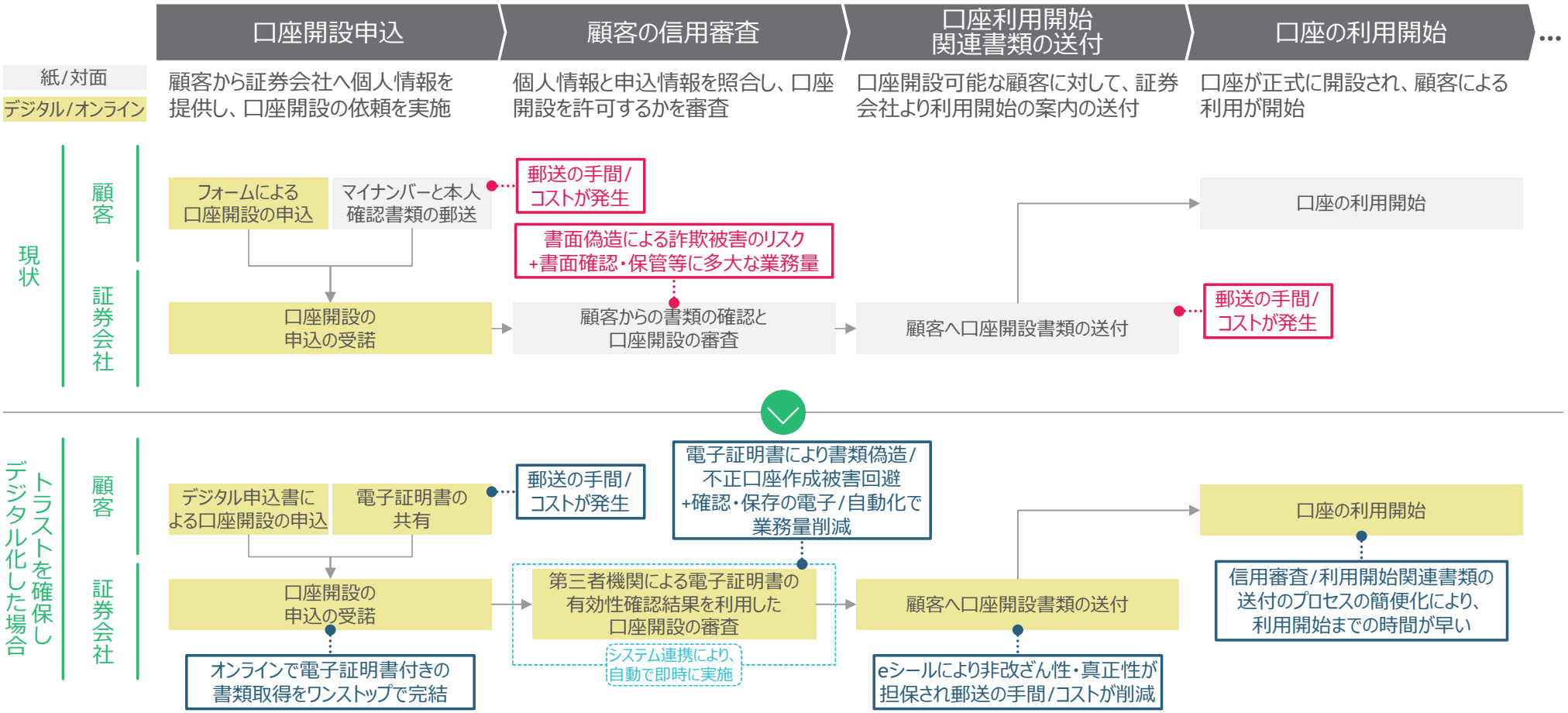
1. トラスト確保によるデジタル化の必要が最も高いものについて、そのデジタル化により見込まれる効果として挙げられた割合
Source: 企業向けアンケート調査 (n=347、2021/11/24～12/7実施); エキスパートインタビュー

銀行口座の新規開設では、従前は紙による本人確認/利用開始案内を前提としていたが、トラストを確保しながらデジタル化されることによって、企業の「業務量/郵送コスト削減」、「書面偽造による不正口座作成等の犯罪被害防止」や、職員による不正防止での「コンプライアンス遵守の強化」、また個人の「手間の削減」「手続きの迅速化」の効果が見込まれる



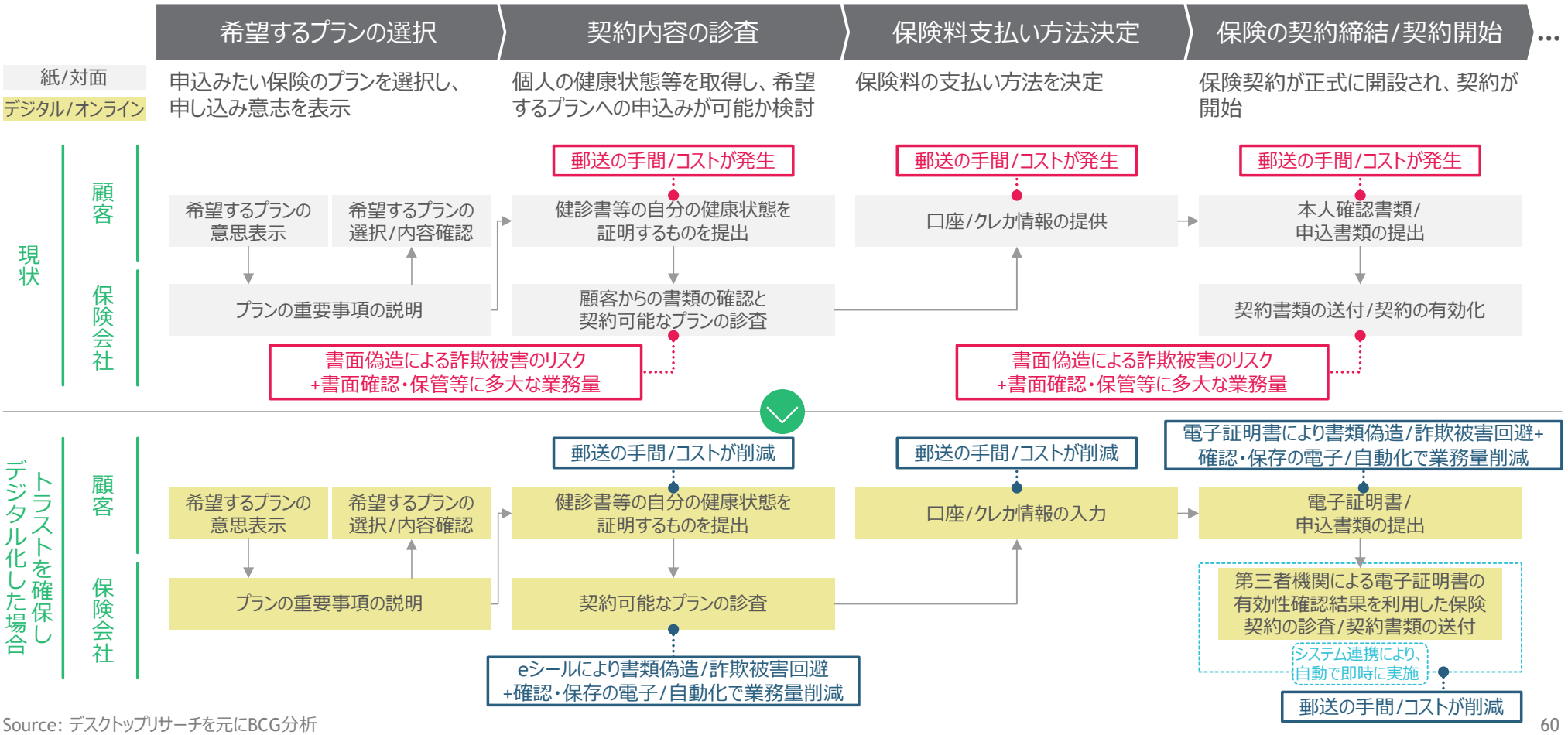
Source: デスクトップリサーチを元にBCG分析

証券口座の新規開設では、従前は紙による本人確認/利用開始案内を前提としていたが、トラストを確保しながらデジタル化されることによって、企業の「業務量/郵送コスト削減」、「書面偽造による不正口座作成等の犯罪被害防止」や、職員による不正防止での「コンプライアンス遵守の強化」、また個人の「手間の削減」「手続きの迅速化」の効果が見込まれる



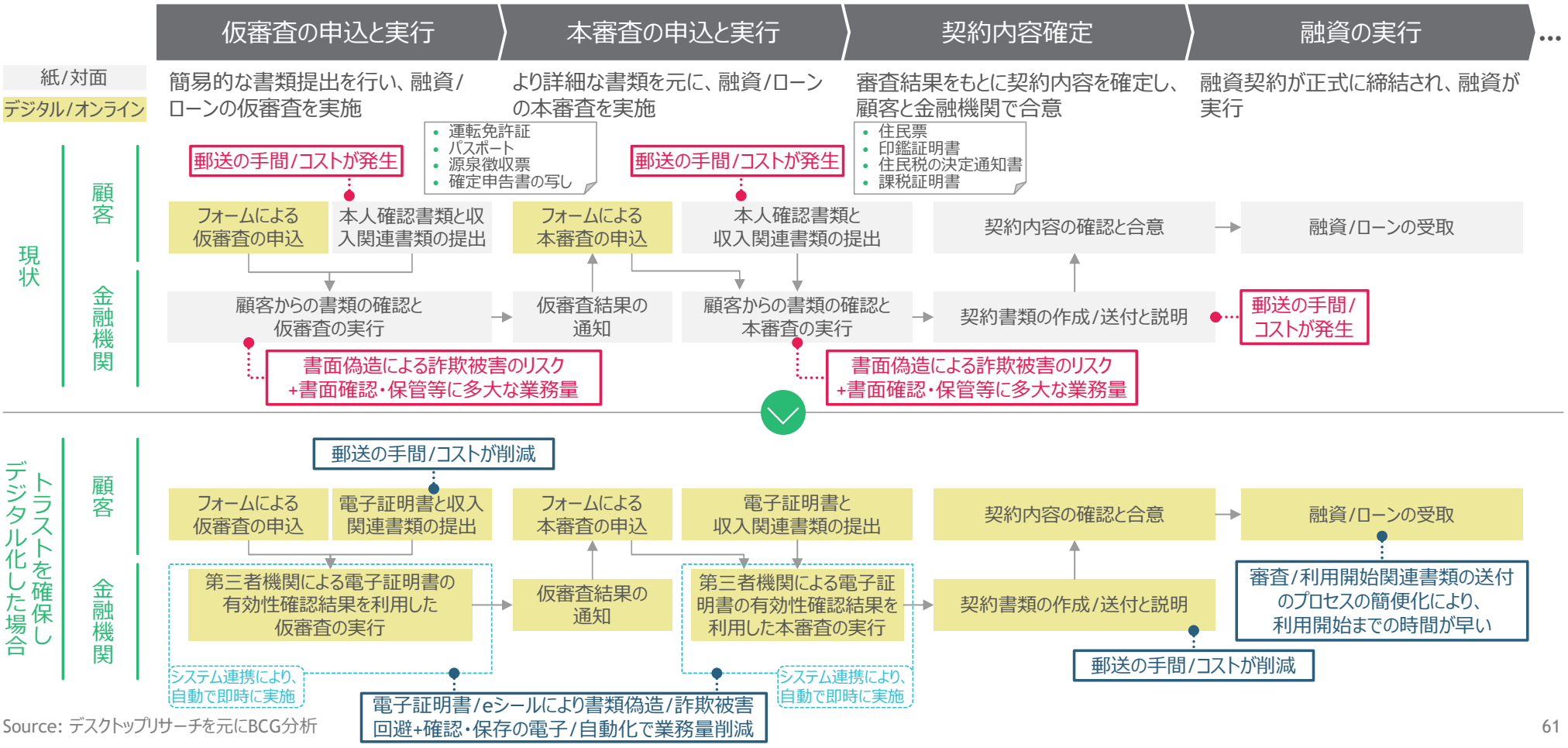
Source: デスクトップリサーチを元にBCG分析

保険の契約では、従前は紙・対面を前提としていた一連の手続きフローが、トラストを確保しながらデジタル化されることによって、企業の「業務量/郵送コスト削減」、「書面偽造による詐欺等の犯罪被害防止」や、職員による不正防止での「コンプライアンス遵守の強化」、また個人の「手間の削減」「手続きの迅速化」の効果が見込まれる



Source: デスクトップリサーチを元にBCG分析

融資/ローンの契約では、従前は紙・対面を前提としていた一連の手続きフローが、トラストを確保しながらデジタル化されることによって、企業の「業務量/郵送コスト削減」、「書面偽造による詐欺等の犯罪被害防止」や、職員による不正防止での「コンプライアンス遵守の強化」、また個人の「手間の削減」「手続きの迅速化」の効果が見込まれる



Source: デスクトップリサーチを元にBCG分析

効果の概算想定規模としては、「業務量削減」では最大で年100億時間規模の労働時間の削減/効率化、「詐欺等の犯罪被害防止」では100億円規模の詐欺被害額の削減を見込む (初期的・規模の粗試算)

	考え方	期待効果の規模 (概算/粗試算)			
		現状の規模	× トラスト確保による削減率 (仮想定)	= トラスト確保による削減効果	
業務量削減	トラスト確保によりデジタル化される企業では、業務量削減が進展 (企業により業務量は異なるため、過去の総務省検討を援用し粗試算)	トラスト確保によるデジタル化を見込む企業の業務時間 **年600億時間規模** (令和元年の業種別の業務時間とアンケートでのトラスト確保によりデジタル化を見込む企業率を乗じて粗試算)	デジタル化による業務時間の削減 **約20%** (過去の総務省での検討における業務効率化の試算より仮置)	業務時間の削減/効率化 **年100億時間規模**	
詐欺等の犯罪防止	個人/企業の電子証明書による本人確認が普及することで、特殊詐欺やフィッシング詐欺等のなりすましや文書偽造の詐欺被害が減少する (利用側としてと同程度、受取側としても確認するようになる)	なりすまし等の詐欺被害 **年300億円規模** (令和2年の特殊詐欺の被害額285億円 + 令和元年のフィッシング詐欺被害額25億円の合算を仮置)	個人の電子証明書の普及 **約40%** (アンケートでの電子証明書の今後の利用意向[1]を仮置)	詐欺被害額の減少 **年100億円規模**	

1. 「現状の規模」は基本的に個人を対象とするものが対象のため、個人の今後の利用意向をアンケート結果を使用。アンケート上で聴取したのは回答者自身の利用意向(何らかの施策に対して、非常に魅力的(あれば電子証明書を利用したい)と回答した割合)だが、同利用意向者は受取手としても電子証明書等を認識し・確認するようになる可能性があると想定して、規模感の参考として仮置。なお、同値は60代/70代以上では42~43%程度で、年代が低いほど高く、最大の10代で56%~になる

Note: 人為的ミスの回避・コンプライアンス遵守の強化は定量化し難いため、またコスト削減については過去の総務省検討において検討されており、業務量同様のアンケートベースのアップデートは困難なため、割愛

Source: 厚生労働省「毎月勤労統計調査全国調査結果原表」、総務省「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最終取りまとめ」、警察庁ウェブサイト、アンケート調査

Appendix C

Identificationのアシュアランスレベルにおける海外の先行事例

海外におけるIdentificationアシュアランスレベルの状況

定義カテゴリ	定義内容	各国の整備有無状況（内容の差異は存在）		
		eIDAS	NIST SP800-63	NZの Identification 管理基準
本人確認（IAL※1）	本人確認方法の確からしさをレベル分けする	✓	✓	✓
認証プロセス（AAL※1）	認証プロセスによって認証強度をレベル分けする	✓	✓	✓
トラストサービス事業者の運営条件	トラストサービスの提供元が信頼できる機関であるかどうかを定めた要件を満たすかどうかによってレベル分けする	✓	–	–
認証情報連携（FAL※1）	認証した情報を別機関に連携する際の連携方法の確からしさをレベル分けする	–	✓	✓
割当（Binding※2）	RP(Relying Party)が個人や組織といったエンティティをエンティティの情報に割り当てたり、エンティティを認証プロバイダーに割り当てるプロセスの堅牢性をレベル分けする	–	–	✓

※1 SP800-63-3 におけるアシュアランスレベルの定義名を記載
※2 ニュージーランドのIdentification管理基準におけるアシュアランスレベルの定義名を記載

eIDAS：Electronic Identificationアシュアランスレベル

electronic identificationのアシュアランスレベルを３つのレベルに規定している。

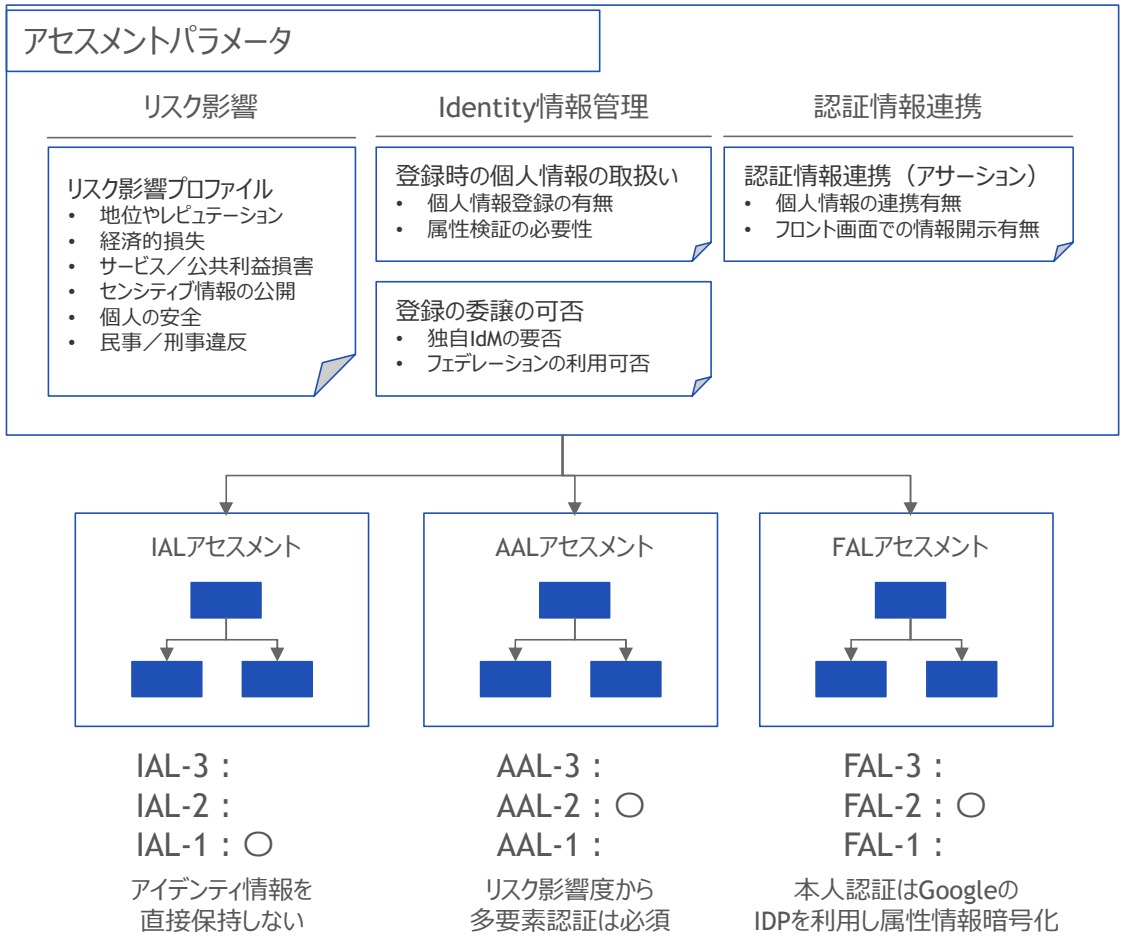
LoA	概要	具体例
Low	• 個人の身元に対して限定された程度の信頼度を提供。Identityの誤用又は改ざんリスクを減らすことを目的 • eIDAS仕様外の簡易なトラストサービス • トラストサービスプロバイダによって提供。事後監査が必要	サービスへの入会を、本人がウェブページを通じてセルフで行うケース。 本人性確認等は実施しない。
Substantial	• 個人の身元に対してSubstantialレベルの信頼度を提供。Identityの誤用又は改ざんのリスクを大幅に減らすことを目的 • 仕様に幅がある	サービスへの入会において、個人のアイデンティティ情報の提示が必須とするケース。 サービス利用時に、ユーザID／パスワード認証、および多要素認証（SMSへのワンタイムパスワード送付等）を必要とする。
High	• 個人の身元に対してSubstantialのアシュアランスレベルを備えた電子識別手段よりも高い信頼度を提供。Identityの誤用又は改ざん防止を目的 • 厳密に守るべき要件やポリシーが定められている • 適格トラストサービスプロバイダによって提供。定期的な監査が必要	サービスへの入会において、有人・対面による本人確認を必須とするケース。 サービス利用時の認証は、国民IDカード等スマートカードの利用を必要とする。

Source:eIDAS – The Ecosystem (EUROPEAN COMMISSION)(https://www.eid.as/), eIDAS Levels of Assurance (LoA) (Connecting Europe Facility)(https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Levels+of+Assurance)

SP800-63-3：基本的な考え方

各事業者がリスク影響度や個人情報の取扱い有無等をインプットに、適切なアシュアランスレベルを選択する基準を提示

アシュアランスレベルのアセスメントフロー



アセスメントの意義／効果

- **ビジネス／セキュリティ／プライバシーのための適切なリスクマネージメントの実現**

  各サービス事業者が、サービスが取り扱うIdentityのリスク影響度を６カテゴリで定義し、規定された共通のアセスメントロジックによりアシュアランスレベルを個別に選択できるようにする。

  例）本来必要とされるレベル以上のアシュアランスを実現するため、コスト増大するようなケースを抑止する。

- **マイクロサービス化されたIdentity ソリューションへの対応**

  政府システムにおいてもIdentityソリューションは単一ベンダーが全機能を提供するモノリシックなものとは限らない。

  分散マイクロサービスによるアイデンティティ管理／認証連携を前提とするアシュアランスレベル選択を可能とする。

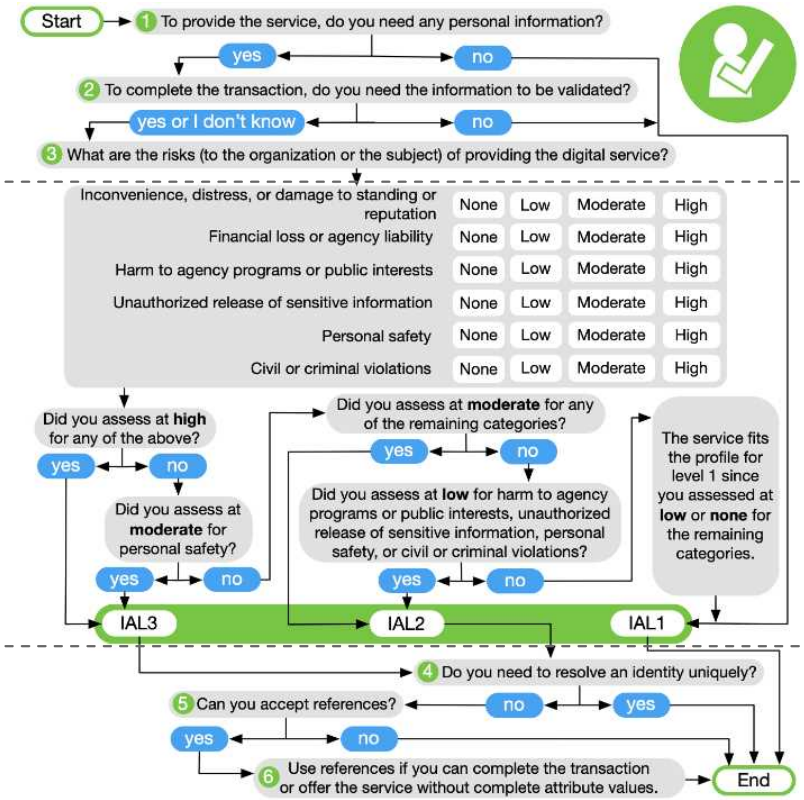
  例）Identity Management／認証はプラットフォーマーのIDP機能へ委譲（フェデレーション）する

Source:NIST Special Publication 800-63 Revision 3 (NIST)(https://pages.nist.gov/800-63-3/sp800-63-3.html)等を元に作成

（参考）SP800-63-3：IALのアセスメントロジック

リスク影響度に加えて個人情報の取扱い有無やアイデンティティの独自管理の要否を加味し、LoAの選択肢を増やしている

IALのアセスメントフロー



アセスメントの要諦

- 個人情報の取扱い有無、属性情報等のバリデーション要否

  サービス登録時、個人情報の取扱いがない場合、ある場合も属性情報のバリデーションが必要ない場合はIAL1を許容する。

- リスク影響度に合わせたアシュアランスレベル決定
  - 6項目のうち一つでもHighがあればIAL-3相当
  - 上記以外で、個人の安全がModerateリスクがある場合IAL-3
  - 上記以外で 1 項目でもModerateがあればIAL-2
  - 上記以外で以下4項目でLowがあればIAL-2
    （サービス／公共利益損害、センシティブ情報の公開、個人の安全、民事／刑事違反）
  - 上記以外はIAL-1

- アイデンティティの独自管理の要否、Identityリファレンスの可否

  Identityの独自管理が不要で、他ソリューションへの参照情報が可能であればフェデレーションによるIdentity連携を推奨する。

Source:NIST Special Publication 800-63 Revision 3 (NIST)(https://pages.nist.gov/800-63-3/sp800-63-3.html)

SP800-63-3：アシュアランスレベル定義

各事業者がリスク影響度や個人情報の取扱い有無等をもとに、ユーザーの身元情報、ユーザー認証、連携方法の確からしさからアシュアランスレベルが定義されている

定義内容	定義LoA	LoAの詳細	
ユーザ身元確認の確からしさ	IAL（Identity Assurance Level）SP 800-63A	IAL.1	身元確認不要、自己申告の登録でよい。メールアドレスの到達確認など
		IAL.2	識別に用いられる属性をリモートまたは対面で確認する必要あり
		IAL.3	識別属性を対面で確認する必要があり。検証担当者は有資格者
ユーザ認証の確からしさ	AAL（Authentication Assurance Level）SP 800-63B	AAL.1	1要素または2要素による認証
		AAL.2	2要素認証が必須。2要素目の認証手段はソフトウェアベースも可能
		AAL.3	2要素認証が必須。2要素目の認証手段はハードウェアベースが必須
連携方法の確からしさ	FAL（Federation Assurance Level）SP 800-63C	FAL.1	アサーション（RPに送るIdPでの認証結果データ）への署名
		FAL.2	FAL.1に加え、対象RPのみが復号可能な暗号化
		FAL.3	FAL.2に加え、Holder-of-Key アサーションの利用（ユーザごとの鍵とIdPが発行したアサーションを紐づけてRPに送り、RPはユーザがそのアサーションに紐づいた鍵を持っているか（ユーザの正当性）を確認）

Source:NIST Special Publication 800-63 Revision 3 (NIST)(https://pages.nist.gov/800-63-3/sp800-63-3.html)

SP800-63-3：アシュアランスレベル一覧

各事業者がリスク影響度や個人情報の取扱い有無等をもとに、ユーザーの身元情報、ユーザー認証、連携方法の確からしさからアシュアランスレベルが定義されている

定義内容	定義LoA	LoAの詳細	
ユーザ身元確認の確からしさ	IAL（Identity Assurance Level）SP 800-63A	IAL.1	身元確認不要、自己申告の登録でよい。メールアドレスの到達確認など
		IAL.2	識別に用いられる属性をリモートまたは対面で確認する必要あり
		IAL.3	識別属性を対面で確認する必要があり。検証担当者は有資格者
ユーザ認証の確からしさ	AAL（Authentication Assurance Level）SP 800-63B	AAL.1	1要素もしくは2要素による認証
		AAL.2	2要素認証、NIST/FIPSで認可された暗号化手法の利用が必須
		AAL.3	AAL2に加えて、ハードウェアベースおよびなりすまし耐性を持つ認証子の利用が推奨
連携方法の確からしさ	FAL（Federation Assurance Level）SP 800-63C	FAL.1	アサーション（RPに送るIdPでの認証結果データ）への署名
		FAL.2	FAL.1に加え、対象RPのみが復号可能な暗号化
		FAL.3	FAL.2に加え、Holder-of-Key アサーションの利用（ユーザごとの鍵とIdPが発行したアサーションを紐づけてRPに送り、RPはユーザがそのアサーションに紐づいた鍵を持っているか（ユーザの正当性）を確認）

Source:NIST Special Publication 800-63 Revision 3 (NIST)(https://pages.nist.gov/800-63-3/sp800-63-3.html)

SP800-63-3：AALに関する要求詳細

	認証要素に関する要求	Hardware-based authenticator	verifier impersonation resistance
SP800-63-3における Requirement Type※	AAL２以上では、二要素認証および FIPS/NISTで認可された暗号化手法が要求される。 AAL3では加えてフィッシングやOTP侵害等に対応するハードウェア認証子の利用をしなければならない(shall use)とされる	• FIPS 140 validation 認証子や暗号化デバイスに加えて、認証者、フィジカルセキュリティに関して、FIPS 140-2に規定されるレベルを満たすことが要求される	• verifier impersonation resistance フィッシング等のなりすましに対する耐性 PKIを使った認証要求者とのチャネル確立等 • verifier compromise resistance 認証処理への侵害に対する耐性 生成したOTPを盗まれるリスクへの対応等
AAL.1	either single-factor or multi-factor authentication using a wide range of available authentication technologies	• Level 1: Government agency verifiers	要求しない
AAL.2	Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required	• Level 1: Government agency authenticators and verifiers	要求しない
AAL.3	（AAL2の要求に加えて）shall use hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device may fulfill both these requirements.	• Level 2 overall: MF Authenticators • Level 1 overall: verifiers and SF Crypto Devices • Level 3 physical security: all authenticators	**要求する**

※Permitted authenticator types、Reauthenticationなどその他要件も定義されているが、本スライドでは要求一覧より主要な要求事項を抜粋して掲載

FIPS 140-2に規定される要求レベル

4. SECURITY REQUIREMENTS

This section specifies the security requirements that shall be satisfied by cryptographic modules conforming to this standard. The security requirements cover areas related to the design and implementation of a cryptographic module. These areas include cryptographic module specification; module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; and design assurance. An additional area concerned with the mitigation of other attacks is currently not tested but the vendor is required to document implemented controls (e.g., differential power analysis, and TEMPEST). Table 1 summarizes the security requirements in each of these areas.

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

NZ政府Identification管理基準：基本的な考え方

各事業者がリスク影響度とリスク発生可能性をインプットに、適切なアシュアランスレベルを選択する基準を提示

アシュアランスレベルのアセスメントフロー

リスクの定義
影響度と発生確率の掛け算

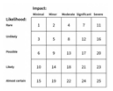
リスク1：サービスまたはトランザクションのために誤った情報が提供される（改ざん）

ビジネス的な損失の影響度と発生可能性を5段階で評価
金銭的な損失または責任：影響度1 × 発生可能性1
機密情報の不正な公開：影響度2 × 発生可能性1
レピュテーションリスク：影響度1 × 発生可能性1
その他の損失または責任：影響度1 ×発生可能性1

リスク2：サービスまたはトランザクションにおける情報または認証機関に、別の人が関連付けられる（なりすまし）

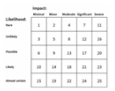
ビジネス的な損失の影響度と発生可能性を5段階で評価
金銭的な損失または責任：影響度3 × 発生可能性2
機密情報の不正な公開：影響度4 × 発生可能性3
レピュテーションリスク：影響度3 × 発生可能性3
その他の損失または責任：影響度2 ×発生可能性2

アセスメントロジック（マトリクス）
金銭的な損失または責任：リスクレベル1
機密情報の不正な公開：リスクレベル2
レピュテーションリスク：リスクレベル1
その他の損失または責任：リスクレベル1
最大値を取るため、リスクレベルは2



IAL-4：
IAL-3：
IAL-2：
IAL-1：〇

アセスメントロジック（マトリクス）
金銭的な損失または責任：リスクレベル13
機密情報の不正な公開：リスクレベル17
レピュテーションリスク：リスクレベル13
その他の損失または責任：リスクレベル5
最大値を取るため、リスクレベルは17



AAL/BAL-4：
AAL/BAL-3：〇
AAL/BAL-2：
AAL/BAL-1：

アセスメントの意義／効果

- 想定されるリスクが定義されている
  Identificationに関する想定リスク（改ざん／なりすまし等）が定義されており、各リスク発生時のビジネス／セキュリティの影響度がパラメータ化されている
- 発生確率が考慮されており、リスク影響度の発生期待値を見たより現実的なリスクアセスメントとなっている
  リスク影響度とリスク発生可能性をそれぞれ5段階で評価することで、適切なアシュアランスレベルを精度を高く選択できる。（発生確率も見ることで、ほぼ起こりえないリスクに対してコスト高なアシュアランスレベルを選択しないよう工夫されている。）
- バインディング
  人を身元確認のための情報や認証プロバイダーのユーザーID/PASS等の認証子に関連付けるプロセスを指す。なりすましリスクの低減に加えて、本人情報の鮮度／整合性を担保することを目指す

Source: Identification management (digital.govt.nz)(https://www.digital.govt.nz/standards-and-guidance/identification-management/)等を元に作成

NZ政府Identification管理基準：リスク及びアシュアランスレベル

リスク影響度とリスク発生可能性をレベル分けし、マトリクス表を用いて総合的にリスクレベルとアシュアランスレベルを判断

リスク影響度とリスク発生可能性のレベル分け

ビジネス的な損失の影響度と発生可能性を5段階のレベルで評価

ビジネス的な損失

- 金銭的な損失または責任
- 機密情報の不正な公開
- レピュテーションリスク
- その他の損失または責任

リスク影響度

- Minimal
- Minor
- Moderate
- Significant
- Severe

リスク発生可能性

- Rare
- Unlikely
- Possible
- Likely
- Almost certain

マトリクス表によるリスクレベル評価

以下のマトリクス表を基に、各ビジネス的な損失のリスクレベルを評価

Likelihood:	Impact: Minimal	Minor	Moderate	Significant	Severe
Rare	1	2	4	7	11
Unlikely	3	5	8	12	16
Possible	6	9	13	17	20
Likely	10	14	18	21	23
Almost certain	15	19	22	24	25

リスクレベルによるアシュアランスレベル評価

算出されたリスクレベルの最大値及び以下の表を基に、アシュアランスレベルを評価

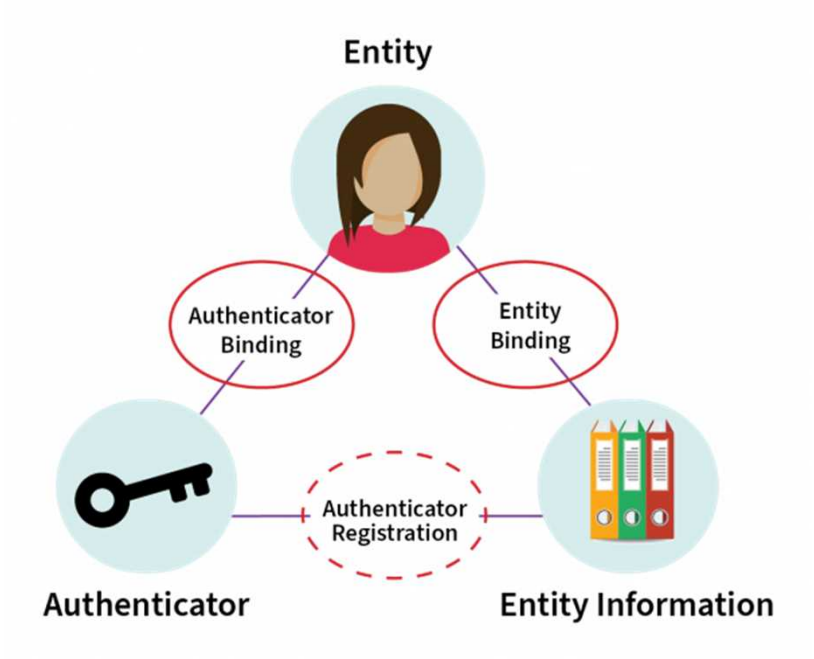
リスク1	リスク2	対応するアシュアランスレベル
1–3	1–3	Negligible — Level 1
4-6	4-10	Low — Level 2
7-19	11-19	Moderate — Level 3
20-25	20-25	High – Level 4

Source: Identification management (digital.govt.nz)(https://www.digital.govt.nz/standards-and-guidance/identification-management/)

（参考）NZ政府Identification管理基準：バインディング

人を正当な情報及び認証子に関連付けるプロセスを指し、なりすましリスクを考察するための概念

バインディングイメージ図



バインディングとは？

- 概要
  Entity（人）をEntity Information（本人確認書類から読み取れる個人情報など）に関連付けたり、EntityをAuthenticator（認証プロバイダーなど）に関連付けるプロセスを意味する
  バインディングには、認証と同様に、知識要素、所有要素、生体要素が使用される

- 実施タイミング
  バインディングは、主には登録時だが、それだけではなく、エンティティ情報の存続期間中のさまざまな時点で実行される
  - Entity InformationがEntityに紐ついていない時（出生登録、割り当てられていないプリペイドカードなど）
  - 新しいAuthenticatorを追加する時
  - BindingのAssurance Level を上げる時
  - Entity Informationが漏洩している可能性があり、再紐付けが必要な時

- Assurance Levelの表現意義
  バインディングのAssurance Levelを定義することで、主には登録時の身元確認のなりすましに加え、上記のユースケースにおけるEntityとInformation、Authenticatorとの関連付けるへのリスク低減の強弱を表現する

Source: https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/binding-assurance-standard/

NZ政府Identification管理基準：アシュアランス要素の規定

定義内容	定義	LoAの詳細	
情報エビデンスの確からしさ	Information Assurance	IAL.1	エビデンスはエンティティの自己主張である
		IAL.2	エビデンスは信頼できるソースのコピーの一部を参照している
		IAL.3	エビデンスは信頼できるソースのコピーであり、品質・有効性が保証されている
		IAL.4	エビデンスは信頼できるソースそのものであり、品質・有効性が保証されている
エンティティ紐付けの確からしさ	Binding Assurance	BAL.1	バインディングのための情報が提供されているが条件はなし＋整合性の維持
		BAL.2	1要素以上の認証子をバインディングに使用＋整合性の維持
		BAL.3	2要素以上の認証子をバインディングに使用＋整合性の維持や不正対策技術等の要件
		BAL.4	生体要素含む2要素以上のバインディングを紐付けに使用＋整合性の維持や不正対策技術等の要件
ユーザ認証の確からしさ	Authentication Assurance	AAL.1	1要素認証
		AAL.2	1要素認証＋認証子保有者の義務に関する規約の発行義務等の要件
		AAL.3	生体要素を含む1要素認証、または2要素認証
		AAL.4	生体要素を含む2要素認証
認証情報連携の確からしさ	Federation Assurance	なし	

Source: Identification Management Standards (**https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/**)を元に作成

NZ政府Identification管理基準：アシュアランス要素の規定

定義内容	定義	LoAの詳細	
情報エビデンスの確からしさ	Information Assurance	IAL.1	エビデンスはエンティティの自己主張である
		IAL.2	エビデンスは信頼できるソースのコピーの一部を参照している
		IAL.3	エビデンスは信頼できるソースのコピーであり、品質・有効性が保証されている
		IAL.4	エビデンスは信頼できるソースそのものであり、品質・有効性が保証されている
エンティティ紐付けの確からしさ	Binding Assurance	BAL.1	バインディングのための情報が提供されているが条件はなし＋整合性の維持
		BAL.2	1要素以上の認証子をバインディングに使用＋整合性の維持
		BAL.3	2要素以上の認証子をバインディングに使用＋整合性の維持や不正対策技術等の要件
		BAL.4	生体要素含む2要素以上のバインディングを紐付けに使用＋整合性の維持や不正対策技術等の要件
ユーザ認証の確からしさ	Authentication Assurance	AAL.1	1要素認証
		AAL.2	1要素認証＋認証子保有者の義務に関する規約の発行義務等の要件
		AAL.3	生体要素を含む1要素認証、または2要素認証
		AAL.4	生体要素を含む2要素認証
認証情報連携の確からしさ	Federation Assurance	なし	

Source: Identification Management Standards (**https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/**)を元に作成

デジタル庁
Digital Agency