

デジタル庁
日本におけるトラスト基盤の整備に係る調査研究
最終報告書

2022年03月24日

目次

エグゼクティブサマリ.....	2
各章の調査研究の実施概要.....	5
1 我が国のデジタル化におけるトラスト確保の必要性.....	6
1.1 行政分野のデジタル化の実態とトラスト.....	6
1.2 民間分野のデジタル化の実態とトラスト.....	9
1.3 海外におけるトラストを活用したデジタル化.....	12
1.4 Society5.0 実現に向けたトラストの必要性.....	25
2 民間におけるトラスト確保のニーズ.....	27
2.1 個人からのトラスト確保のニーズ.....	28
2.2 企業からのトラスト確保のニーズ.....	32
3 既存トラスト基盤の現状と課題.....	39
4 トラスト基盤普及に向けた課題解決の方策 (案).....	43
5 トラスト基盤の整備・普及による期待効果.....	48
6 今後のロードマップ (案).....	52
7 個別取組の案.....	53
7.1 優先的に取り組むユースケース (案).....	53
7.2 海外連携を目指すトラストサービス (案).....	55
7.3 官民共同規制の在り方 (案).....	55
7.4 アシユアランスレベルの分類 (案).....	61

エグゼクティブサマリ

我が国においては、21世紀のデジタル国家にふさわしいデジタル基盤構築に向け、我が国初となる「データ戦略」及びその具体的な取組の方向性となる「包括的データ戦略」の策定を行っている。その中で、なりすましやデータの改ざんを防ぎ、データ流通基盤の信頼性を確保し、データ社会全体を支えるトラスト基盤の在り方を検討する必要がある。

弊社では貴庁からの「トラスト確保のための実態調査の依頼事項」に沿って日本におけるトラスト基盤に係る調査研究を実施しており、2022年3月に本調査研究の全体成果としてファイナルレポートを提出する予定。本報告書は、中間報告の位置付けとして、デジタル化におけるトラストの立ち位置、トラスト確保のニーズ、既存トラスト基盤の現状と課題から、現時点で考えられるトラスト基盤普及に向けた課題解決の方策、トラスト基盤の整備・普及による期待効果、今後のロードマップを策定し、まとめてある。また個別の取組の案として貴庁から要望のあった優先的に取り組むべきユースケース、海外連携を目指すべきトラストサービス、官民共同規制の在り方、アシユアランスレベルの分類についても調査と整理を実施した。本エグゼクティブサマリでは、まずは要約を記載させていただく。

デジタル化におけるトラスト

我が国のデジタル化の推進に際して、行政分野・民間分野において行政が所管する手続き等だけではなく、各業界の様々な手続き等において、オンライン上の企業や個人の本人確認や、電子データの非改ざん性の担保等、トラスト確保が課題となっている。

行政分野では、年間件数が10万件を超える主要なものでも、厳格な本人確認が必要な申請や、内容の非改ざん性が必要な証明書の交付等は、デジタル化の対象外とされている。また、オンラインで完結できる手続き等でも、電子証明書を擁する者は、利用率が平均1割未満と低水準にある。

民間分野でも、行政が所管する、法的効力(証拠能力)が必要な文書の保存等の一部が、デジタル化の対象外とされている。またその他、B2B取引や、B2B/B2C等の契約、非改ざん性が必要な文書の保存・授受等で、トラストへの懸念がデジタル化の阻害要因となっている。

他方、欧州をはじめとする海外では、官民共同でのトラスト基盤の整備により、「金融」「情報通信」「不動産」「医療」「運輸・物流」等で、日本ではデジタル化されていない手続き等のデジタル化がなされ、その利用率も高い水準となる例も出てきている。

また、我が国では今後IoT (Internet of Things) で全ての人とモノが繋がり、様々な知識や情報が共有され、今までにない新たな価値を生み出す未来社会「Society5.0」の実現による経済発展と社会課題解決の両立を目指している。Society5.0の実現において必須であるIoTを活用した社会システムにおいては、なりすましやデータ改ざん等のリスクがあり、海外では事件化する例も発生する等、危険性も存在している。そこで、Society5.0の実現のためにデータのトラスト確保が必要とされている。

トラスト確保のニーズ

デジタル化におけるトラスト確保のニーズは行政のみならず民間でも業種を問わず存在するが、特に「金融」「不動産」「医療」等の業界は秘匿性の高い情報を多く扱い、情報の取り扱いに関するリスクが非常に高い業界である。従って、これらの業界ではなりすましによる詐欺被害や、法的根拠ともなる文書等の改ざん等の防止、従業員のコンプライアンス遵守強化へのニーズが高く、トラスト確保の必要性が強く認識されている。これらの業界の中で

も、特に企業と個人の両者から、「金融」(送金、貿易金融等)、「不動産」(売買/賃貸契約等)、「医療」(薬剤処方、健診/検査結果発行等)で、「厳格な本人確認(なりすまし防止)」「や」文書等の真正性担保(改ざん防止)等の必要性が、強く認識されている。

また、トラスト確保の必要性は既存の手続き等において発生するのみではなく、Society5.0 実現に向けた新しいデジタルサービスや社会システムについても、「金融」「不動産」「医療」等の業界を中心にその必要性が認識されている。例えば、サービスの利便性や生産性向上に向けた企業間データ共有/IoT化(スマートグリッド、スマート医療等)や、カーボンニュートラルやSDGs達成に向けた商品等のトレーサビリティ確保等の取組で、トラスト確保の必要性が広く認識されている

既存トラスト基盤の現状と課題/課題解決の方策

トラスト基盤の必要性は強く認識されている一方で、その普及は個人/企業共に低い値に留まっている。トラストを確保する仕組みとしては電子署名、eシール、タイムスタンプ、eデリバリー等のトラストサービスが挙げられるが、それぞれの利用率は電子署名(個人25%/企業25%)、eシール(6%)、タイムスタンプ(17%)、eデリバリー(5%)に留まっている。

利用率が低い値に留まっている要因は、個人と企業それぞれに存在する。個人からは「利用場面/メリットの不足」、「知らなかった」、「マイナンバーカードの紛失が心配」、「具体的な使い方を知らなかった」等、企業からは「(電子署名以外)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」、「導入/利用コスト」、「知らない/よく知らない」等が課題の大きな割合を占めているとの意見が挙がっている。

これらの課題を解決し、トラストサービスを普及させるための方策としては、個人/企業からの声として、「普及啓発活動」「モデルケース創出」「ガイドライン等の策定」や、「(電子署名以外の)法的効力(証拠能力)の担保」「国際的な効力(証拠能力)担保(国際連携)」の他、「より堅牢で簡便な方式の確立(生体認証ID等)等」にも要望がある

トラスト基盤の整備・普及による期待効果

トラスト基盤の整備・普及により、様々な業種でトラスト確保によるデジタル化の促進によって「業務量削減」「人為的ミスの回避」や、デジタル/オンラインでの紙・対面以上のトラストの強化による「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。このようなメリットを見込み、自社のデジタル化が進展することを期待する企業は85%存在し、中でも業種共通の「各種契約書類作成」「請求・支払書類作成」と、金融・保険の「銀行口座開設」「為替取引」等のデジタル化への期待が大きい。

具体的にデジタル化によって享受できるメリットは、例えば不動産の売買/賃貸契約では、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「業務量削減」、個人の「手間の削減」に加え、「(“地面師”等の)「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」の効果が見込まれる等である。

なお、これらのトラスト導入によって得られる効果の概算想定規模として、「業務量削減」は約600億時間から約20%、約100億時間が見込まれる他、「詐欺等の犯罪被害防止」100億円(年間の詐欺被害額の40%想定)が見込まれる(「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今回の試算外)。

今後のロードマップと初期案

今後のトラスト基盤の整備・普及に向けて、大きく3ステップのロードマップでの推進を想定する。短期では、現状の規制及び電子システムを前提とした利用促進、モデルケースの創出に注力し、中期ではトラストサービスの法的効力(証拠能力)の強化及びトラストへのニーズの強い業界におけるガイドラインの発行を行う。そして長期的に国際連携の実現と新たな電子システムの稼働を目指す。

なお、短期的に着手する必要があるものに関しては、以上のロードマップや海外先行事例を踏まえ、継続検討を行う必要がある。

優先的に取組むユースケースに関しては、「個人の電子証明書の利用促進に向けたメリット増大」「企業のトラストサービス導入促進に向けたメリットの実証」「課題解決の方策の有効性検証」の3つの目的を踏まえ、実現性/有効性と魅力度(期待効果)の観点から、金融/保険のB2B/Cの手続き等が考えられる。また上記以外にも、法律で定められた帳簿/台帳/記録等の作成・保存などが候補になると考えられる。

また、国際連携を目指すトラストサービスに関しては、企業が行う民間手続き等のうち、海外との取引等があり、相手先の本人確認や情報改ざん防止が必要なものとしては、企業アンケートにおいて幅広い手続き等が挙げられた。それらで必要とされるトラストは「個人の厳格な本人確認」「法人の厳格な本人確認」「文書の非改ざん性・真正性担保」と異なり、その必要に応えるためには、「個人の電子証明書」「eシール」「タイムスタンプ」、及び、それらを組合せた「eデリバリー」何れも、国際連携が望ましいと考えられる。

さらにガイドライン等の策定における、アシュアランスレベルの分類も必要である。トラスト基盤が取り扱う個人の手続/取引情報のセンシティブリティの度合いに合わせた、認証方式のレベル(デジタルIDアシュアランスレベル)を策定し、企業/政府間でやり取りする手続/取引情報の「完全性保証」および「デリバリー」を担当するトラストサービスについては、企業等が参照できるアシュアランスレベルを整理し、各サービス事業者の立ち上げを目指す。

また、官民共同規制の体制構築を行っていく必要がある。トラストサービスを始めとするデジタル基盤の規制の在り方としては、「政府主導型(官中心)」「ハイブリッド型(官民共同)」「民間主導型(民中心)」等がある。我が国のトラスト基盤整備にあたっては、実装上の必要に応じる柔軟性・機敏性を確保する観点から、「ハイブリッド型(官民共同)」が望ましいと考えられる。

各章の調査研究の実施概要

今回の調査研究にあたり、過去の総務省による検討（トラストサービス検討ワーキンググループ、トラストサービスの利用動向に関するアンケート調査の結果等）も踏まえた上で、内閣官房（IT 室）の「行政手続等の棚卸調査」や内閣府の「各府省における書面規制・押印・対面規制の見直し結果」、総務省の「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）」「トラストサービスに関する海外調査」等の分析、文献調査、デスクトップリサーチ、エキスパートインタビュー、及びそれらを踏まえた個人・企業それぞれへのアンケート調査を行った。以下の表では、それぞれの章で使用した参考文献/資料をリスト形式で掲載している。

No.	参考文献/資料	該当章
1	「行政手続等の棚卸結果等」(内閣官房)	1.1 行政分野のデジタル化の実態とトラスト
2	「各府省における書面規制・押印・対面規制の見直し結果」(内閣府)	
3	「各府省の書面を求める行政手続の見直し方針一覧」(内閣府)	
4	外国人技能実習機構ウェブサイト	1.2 民間分野のデジタル化の実態とトラスト
5	「労働力調査 (基本集計)2020 年」(令和 2 年)(総務省)	1.3 海外におけるトラストを活用したデジタル化
6	「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)」(総務省)	
7	「トラストサービスに関する海外調査」(三菱総合研究所 (総務省委託調査))	
8	「Description of the current status and future needs of the Information Architecture and Data Management solutions for the national personalised medicine pilot project」(University of Tartu)	
9	NIST Special Publication 800-63 Revision 3 (NIST)	
10	内閣府ウェブサイト	1.4 Society5.0 実現に向けたトラストの必要性
11	「Connected Car」をめぐる現状等」(総務省)	
12	「『IoT 開発におけるセキュリティ設計の手引き』～「ヘルスケア機器とクラウドサービス」の脅威分析と対策検討～」(独立行政法人情報処理推進機構)	
13	「毎月勤労統計調査全国調査結果原表」(厚生労働省)	5. トラスト基盤の整備・普及による期待効果
14	「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」(総務省)	
15	警察庁ウェブサイト	
16	Gov.UK.com	7.3 官民共同規制の在り方

1 我が国のデジタル化におけるトラスト確保の必要性

1.1 行政分野のデジタル化の実態とトラスト

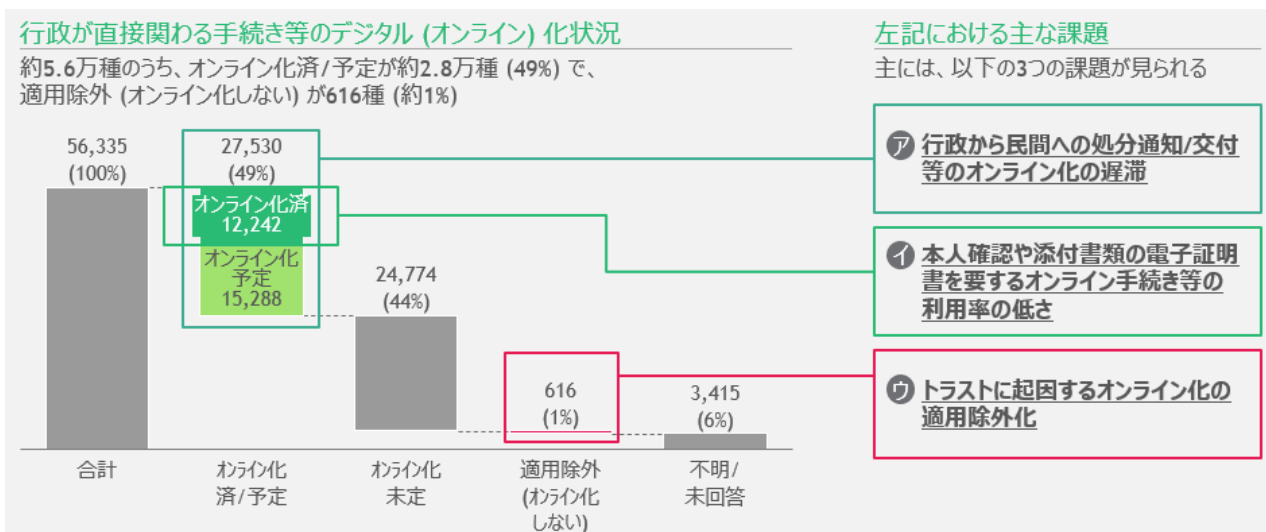
サマリ

行政が直接関わる手続き等は約 5.6 万種存在し、約半分 (49%) でデジタル化 (オンライン化) が進んでいるが、依然として、トラストが阻害要因となってデジタル化できていない または その利用率が低いものが存在する。特に行政から民間への処分通知/交付等は 8 割以上でオンライン完結が実現できておらず、年間 10 万件以上の実施がある規模の大きい手続き等であっても、厳格な本人確認が必要な申請等や、非改ざん性/真正性の担保が必要な証明書等の交付等が、オンライン化の対象外とされている。具体的には、厳格な本人確認が必要な申請等として厚生年金保険の保険料口座振替納付 (変更) の申請、住民基本台帳関連の手続き (転入届 等) が挙げられ、改ざん性/真正性の担保が必要な証明書等の交付として旅券の交付、運転免許証の交付/更新、国外運転免許証の交付、在留カードや乗員上陸許可書等の交付、自動車の保管場所標章の交付等が挙げられる。

一方で、本人確認や添付書類の電子証明書を要さないものでは、平均オンライン利用率が約 3 割であるのに対し、本人確認で電子証明書を要するものでは、平均オンライン利用率は 2 割未満 (約 16%) であり、添付書類に電子証明書を要するものでは同 1 割未満 (約 7%) に留まる等、オンラインでの完結が可能な手続き等であっても、本人確認や添付書類に電子証明書を要するものでは、オンライン利用率が特に低い水準に留まる。

行政分野の手続き等の全体像

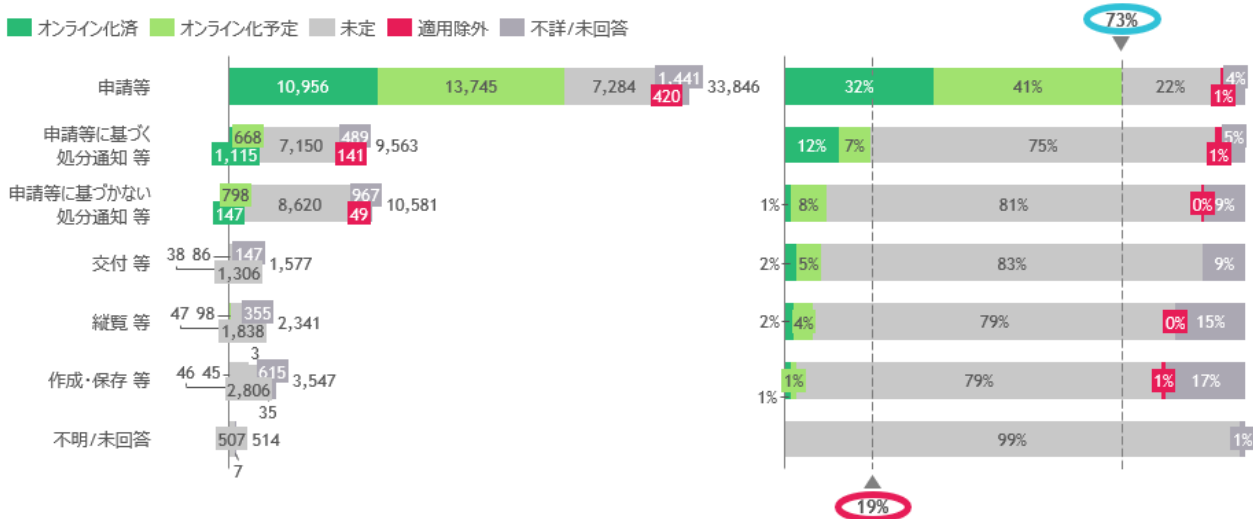
行政が直接かかわる手続き等約 5.6 万種のうち、すでにオンライン化済みの手続き等は約 1.2 万種、今後オンライン化が行われる予定の手続き等は約 1.5 万種存在する。これらを合計した約 2.75 万種の手続きの中には、行政から民間への処分通知/交付等のオンライン化の遅滞や本人確認や添付書類の電子証明書を擁するオンライン手続き等の利用の低さ等の課題が存在している。また、オンライン化が未定の手続き等は約 2.5 万種、オンライン化を適用しない手続き等は 616 種と全体の約 1%程度を占める。



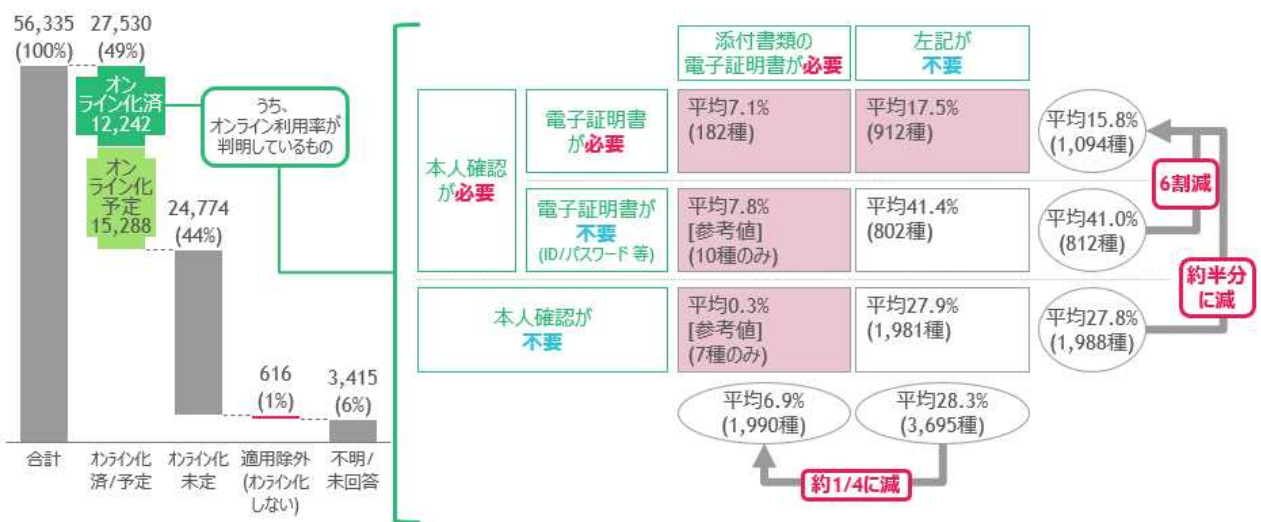
オンライン化済み/オンライン化予定の手続き

オンライン化済み/オンライン化予定の手続きであっても、必ずしもデジタル化率が高いわけではなく、人々がデジタル完結利用を行うことを阻害する課題として、(ア)行政から民間への処分通知/交付等のオンライン化の遅滞、(イ)本人確認や添付書類の電子証明書を要するオンライン手続き等の利用率の低さが挙げられる。

(ア)に関しては、民間から行政への申請等ではデジタル化が進展しており、約7割がデジタル完結可能な手続きになっているものの、それ以外の主に行政から民間への処分通知/交付等ではあまりデジタル化が進んでいるとはいえず、デジタル化率は2割未満の状況である。

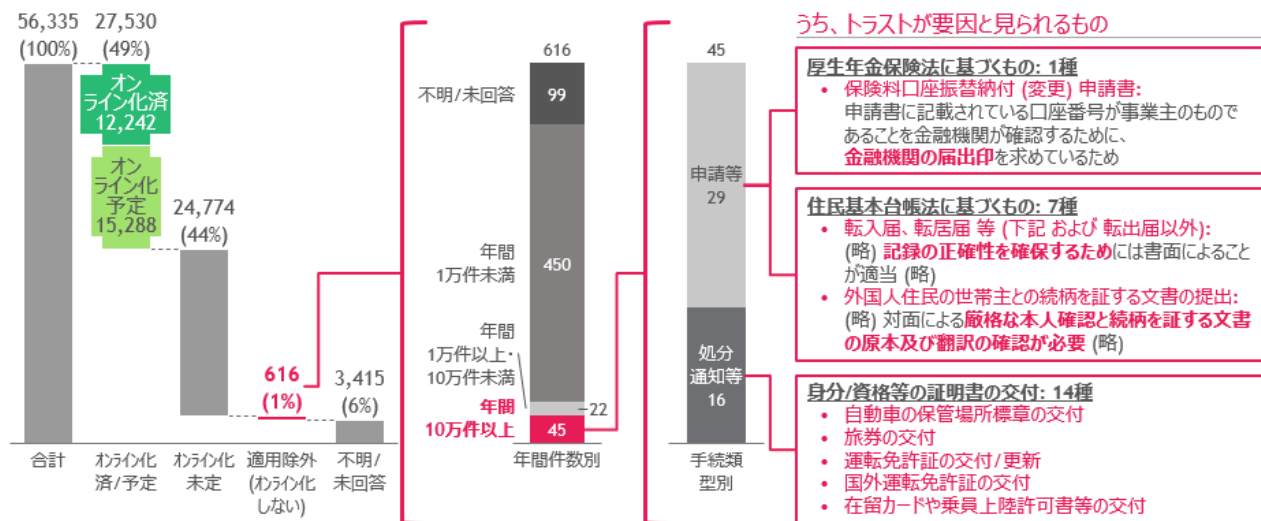


(イ)に関しては、デジタル化がなされている手続き等であっても、本人確認や添付書類で電子証明書が必要な手続き等では双方が不要な手続き等と比較して大きくデジタル化率が低いことがわかった。例えば、本人確認が不要な手続き等と比較すると、電子証明書による本人確認が必要な手続き等では、オンライン利用率が半分程度に減少している。



オンライン化未定の手続き

オンラインの適用を除外されている手続き等の中でも、年間 10 万件以上の手続き件数があるものは 45 種存在し、その中でも金融機関の届出印や厳格な本人確認の必要等、トラストがオンラインの適用除外の要因になっているものが存在する。例えば、「保険料口座振替納付 (変更) 申請書」は、申請書に記載されている口座番号が事業主のものであることを金融機関が確認するために、金融機関の届出印を求めており、オンライン化の適用外となっている。



1.2 民間分野のデジタル化の実態とトラスト

サマリ

民間分野のデジタル化の実態を、行政が所管する手続き等、行政が所管しない手続き等の2つに分け、さらに行政が所管しない手続き等に関しては個人側の視点と企業側の視点の両面からの分析を実施した。

行政が所管する手続き等に関しては、法的効力(証拠能力)が必要な文書の保存等の一部が、デジタル化の対象外とされている。適用除外のもので、年間10万件以上のものはないが、大きく3分類・17種の作成・保存で、規模が不明だが大きい可能性がある。また、オンライン化済みの手続き等の中では、オンライン利用が25%未満のものが2分類・14種存在する。

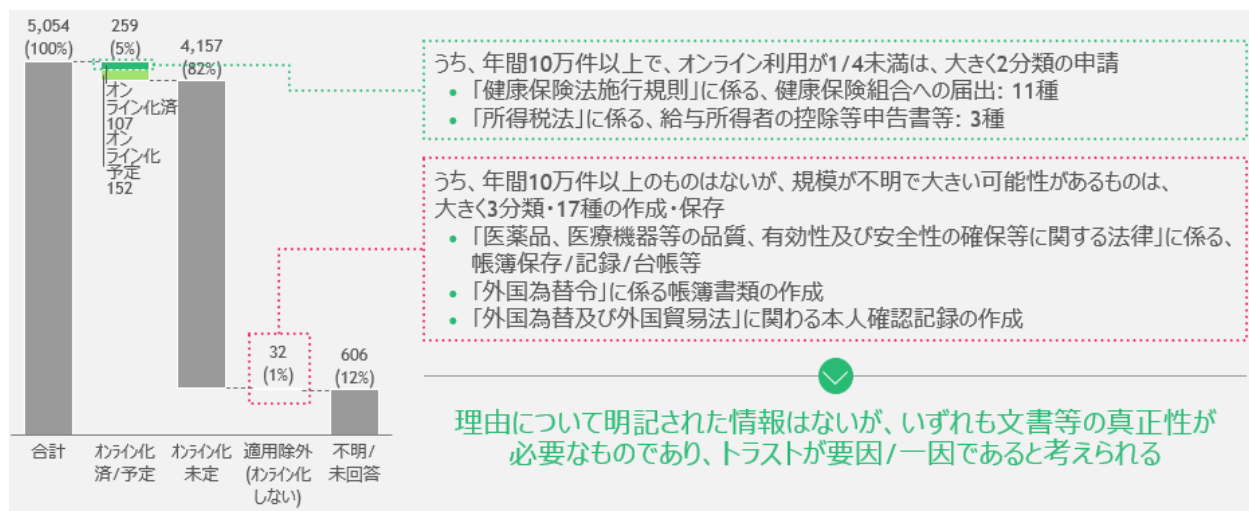
さらに、行政が所管しない手続き等に関しては個人/法人においてオンライン完結による手続き等の実施/導入率は低い水準にあり、トラストへの懸念がデジタル化の阻害要因となっている。例えば個人でトラストが必要と考えられる手続き等で、1年以内に1割以上の人を実施する実施規模が大きいものも含め、デジタル/オンラインでの実施経験率は半分に満たないものがほとんどであり、企業では実施規模が大きい手続き等も含め、実施企業におけるデジタル/オンライン完結の導入率は、いずれも半分未満に留まっている。

行政が所管する手続き等のデジタル化実態

行政が所管する手続き等に関しては、オンライン化済みの手続き等のうち、年間10万件以上でオンライン利用が1/4未満である手続きは大きく2分類14種で、具体的には、①「健康保険法施行規則」に係る、健康保険組合への届出、②「所得税法」に係る、給与所得者の控除等申告書等の2分類である。

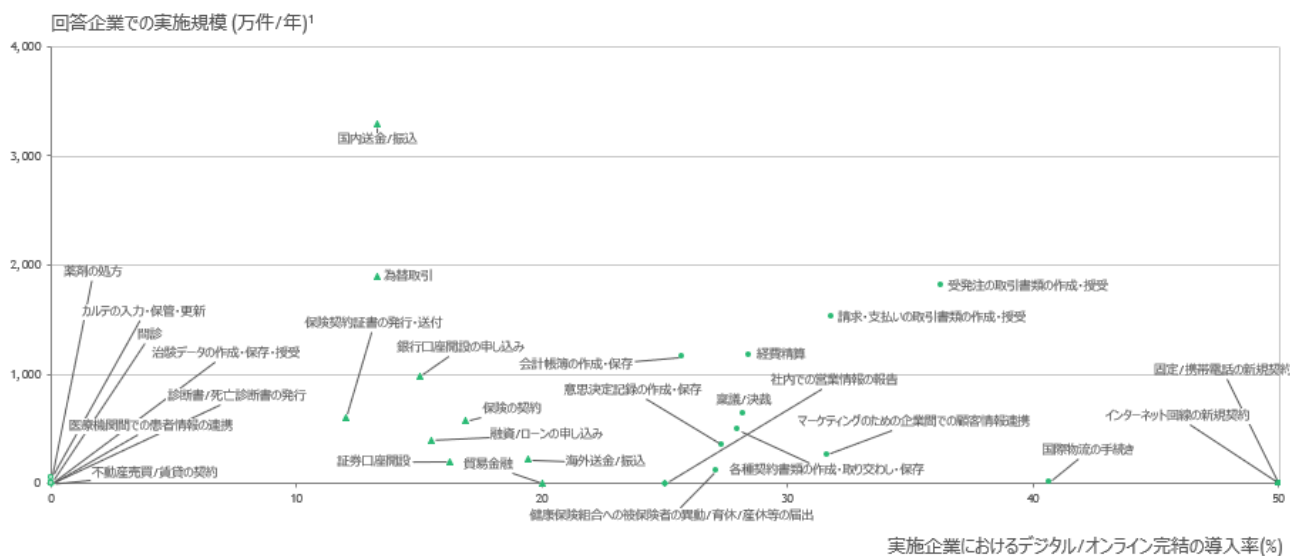
また、オンライン化の適用を除外されている手続き等には年間10万件以上はないが、規模が不明で大きい可能性があるものは大きく3分類・17種存在する。具体的には①「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律」に係る帳簿保存/記録/台帳等、②「外国為替令」に係る帳簿書類の作成、③「外国為替及び外国貿易法」に関わる本人確認記録の作成の3分類である。

以上の手続き等に関しては、いずれも文書等の真正性が必要なものであるため、トラストが要因/一因であると考えられる。

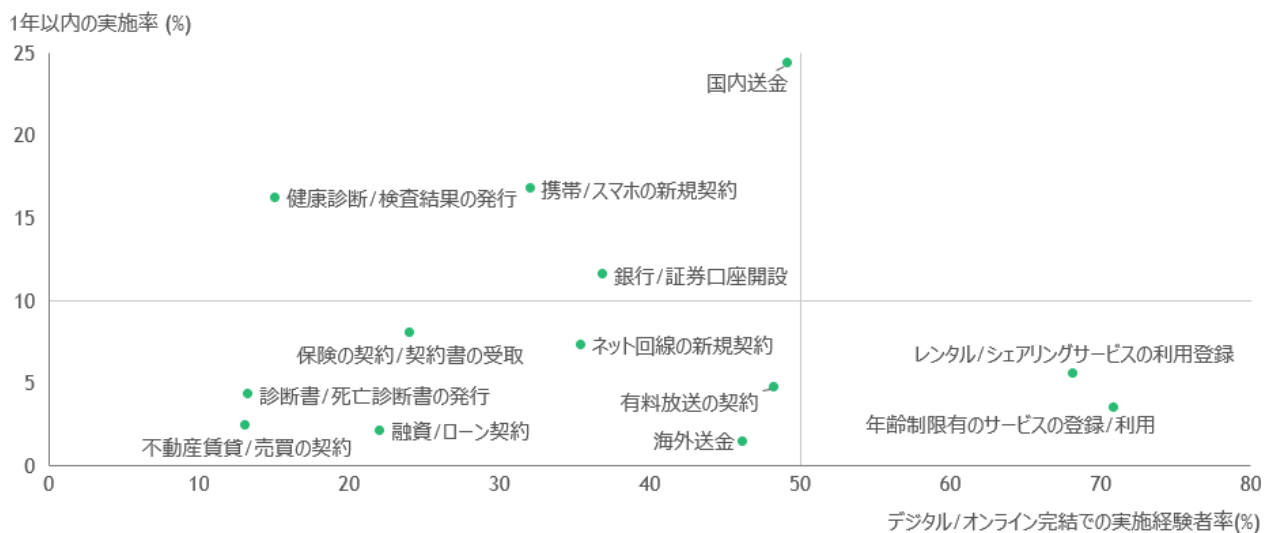


行政が所管しない手続き等のデジタル化実態

行政が所轄しない手続き等の実施規模とデジタル化率を調査した。まず企業側からの視点から、企業における各手続き等の実施規模を縦軸、デジタル/オンライン完結の導入率を横軸として散布図として表すと、実施規模が大きい手続き等も含め、実施企業に於けるデジタル/オンライン完結の導入率はいずれも半分未満に留まった。

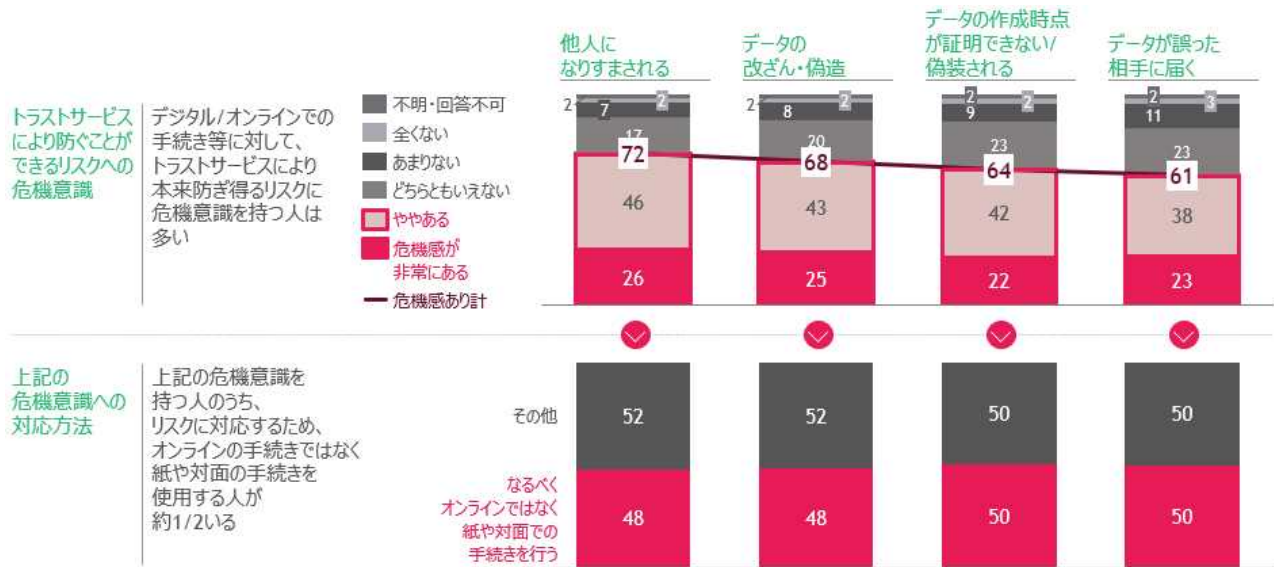


また個人側の視点から、個人の各手続き等を1年以内に実施した割合を縦軸、デジタル/オンライン完結の導入率を横軸として散布図として表すと、1年以内に1割以上の人が実施する実施規模が大きい手続き等も含め、デジタル/オンラインでの実施経験率は半分にも満たないものがほとんどである。

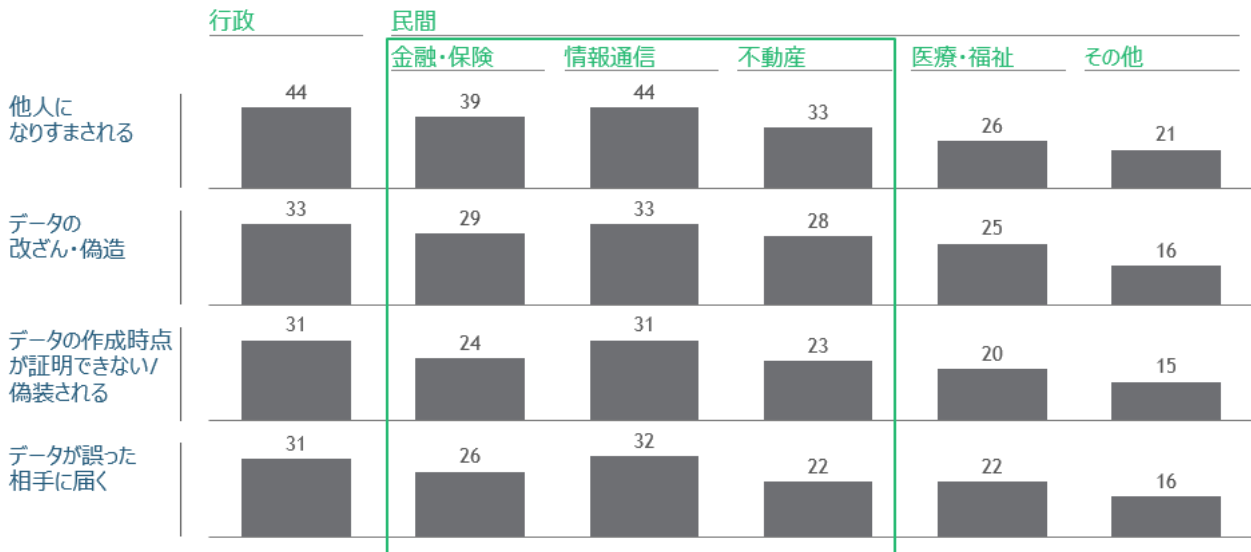


次に、個人を対象としてデジタル/オンラインでの手続き等において、本来トラストサービスによって防ぎ得るリスクへの危機意識と、危機意識を感じた場合における行動を調査した。結果的に、デジタル/オンラインでの手続き等に対して、トラストサービスにより本来防ぎ得るリスクに危機意識を持つ人は多く、さらに危機意識を持った場合にリスクへの対処方法としてオンラインの手続きではなく紙や対面での手続きを使用する人が1/2程度存在することがわかった。この結果より、本来トラストサービスによって防ぎ得るリスクがデジタル/オンラインの手続き等の利用を阻害する

一因となっていることがわかる。



さらに、民間の業界別では特に「情報通信」「金融」「不動産」業界の手続き等へのリスク意識が高い。「金融」「不動産」業界はより秘匿度合いの高い情報を多く扱い、被害が生じた際に大きな損失額が発生するリスクが高い業界であり、また「情報通信」業界は近年フィッシング詐欺や偽装ウェブサイト等の身近なリスクが多く存在する業界であるため、リスク意識が高まっていると考えられる。



1.3 海外におけるトラストを活用したデジタル化

サマリ

我が国において直接かかわるステークホルダーが大きい業種の一部である金融・保険、不動産、医療・福祉、運輸、情報通信等の業種において、欧州や米国をはじめとした海外ではトラストサービスの利用が先行している。この章ではそのような海外のユースケースについて調査を行うと共に、海外でのアシュアランスレベルの調査を実施した。

業種	我が国において直接関わるステークホルダーの規模		海外でトラストサービス利用が先行		
	労働人口	直接関わる相手の規模	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)		✓	
運輸業、郵便業	中 (347万人)	大 (B2C/Bかつ取引相手は全般的)	✓		
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)	✓	✓	
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)	✓	✓	✓
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)		✓	
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)	✓		

また調査の観点として以下を設定した。

分類	調査の観点	詳細
1 各業界サービス	トラストサービスを活用したデジタルサービスのニーズ	各業界におけるサービスニーズとトラスト活用余地を整理 <ul style="list-style-type: none"> 行政手続き分野では、オンライン化による手続きの簡素化とそれに必要となる本人認証のアシュアランスレベルの分類 ヘルスケアやスマートグリッド分野では、業界内での情報流通とそれによる国民サービスの利便性向上や公共性の高いサービスの生産性向上等
2 デジタルID	個人・法人のアイデンティティの運用実態	各業界サービスにおいて、実際にどのレベルのデジタルIDがアイデンティティとして使われているかの整理 <ul style="list-style-type: none"> オンライン化を目指すものはmobile ID/スマートIDの活用状況、及びそれらを補完する多要素認証等の導入状況 企業間取引に関しては法人格のPKIの実態調査
3 トラストサービス	各業界サービスにおいて活用されるトラストサービス及びトラストサービスプロバイダの実態	各業界サービスにおいて、実際にトラストサービスが個人/法人格の証明として使われているかの整理 <ul style="list-style-type: none"> オンライン化を目指すものは電子証明書の発行母体やPKI管理の実態 企業間取引に関してはeスタンプ/eデリバリーの利用状況
4 要素技術/PF	取引連携PF (X-road)、政府・民間CA、個人認証PF、データ統合PF等の適用状況の実態	上記を実現する業界横串でのプラットフォーム適用状況について把握 <ul style="list-style-type: none"> X-Roadは企業間取引のインフラの位置付け、オンライン化含めた個人認証部分の仕組みや運営主体に関する調査 既存トラストサービスプロバイダの運営実態調査 (トラストアンカー)
5 法令/標準	eIDASで規定されるアシュアランスレベル適用実態	各業界サービスがデジタルID/トラストサービスについてどのアシュアランスレベルを求めているかの整理 <ul style="list-style-type: none"> デジタルIDについては認証要素のバリエーションと対面/非対面のレベル トラストサービスに関しては、プロバイダの適合性レベル

エストニアにおける事例

エストニアは近年デジタル化政策を次々と推し進め、世界の中でも「電子国家」として最先端のシステムを導入している国家である。エストニアでは、「住民登録」や「電子投票」等多くの行政手続きがデジタル/オンライン化されているだけでなく、民間分野でも他国に先行してトラストが導入されている。例えば、金融・保険の領域では「銀行口座の開設」、不動産の領域では「不動産売買/賃貸契約」等がデジタル/オンラインで実行できる。

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						その他
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	
厳格な本人確認が必要な申請/手続等	<ul style="list-style-type: none"> 住民登録 電子投票 オンライン化による投票率向上 他国民のID登録 法人登記自由化と誘致ニーズ喚起 					<ul style="list-style-type: none"> 農林水産業、鉱業、建設業、製薬業、電気・ガス等、卸売・小売、畜産業・飲食業等
内容の非改ざん性/真正性が必要な申請/交付/情報授受	<ul style="list-style-type: none"> 租税情報、重要データの国際連携 税務に関する利便性向上、有事対応 教育情報の電子化/一元化 	<ul style="list-style-type: none"> レシート電子化 	<ul style="list-style-type: none"> 不動産情報の電子化/一元化 	<ul style="list-style-type: none"> 処方箋発行の電子化/一元化 ペーパーレス推進、薬処方の利便性向上 PHR等医療情報の一元化 		<ul style="list-style-type: none"> スマートグリッド需要/供給情報の収集とそれによる電力供給最適化
法的証拠能力が必要な文書/記録等の作成・授受・保存		<ul style="list-style-type: none"> レポート電子化 ベンチャー企業の行政当局への報告負担低減 	<ul style="list-style-type: none"> 不動産売買/賃貸契約 不動産登記 			

- ベースは行政手続きの電子化とそれによる利用率の向上
- エストニアの独自ニーズとしては海外IPの誘致ニーズ他国民のID登録、国外法人誘致/GDPの底上げ、ベンチャー企業の当局対応のサポート
- 金融分野は多要素認証による口座開設完全オンライン化

- 公共性の高い業界の取引情報を電子化/一元化するニーズが存在する業界横断での情報参照や手続き(薬処方、専門医紹介)の利便性向上データ収集/分析によるサービス公益性の向上(スマートXX系、CO2削減)
- 認可制のため、民間事業者にデータ提示を義務化する等の強制力が働く
- Eテラリーの半官運営会社がトラストプロバイダーの認可/調達を一元管理

その中でも、特にエストニアで e-Prescription と呼ばれている電子処方箋サービスについて掘り下げて説明する。e-Prescription は、紙の処方箋発行を電子化したものであり、健康保険基金が運営する処方箋システムにデータを統一化し、医療機関と処方箋データをやり取りすることで電子化された処方箋を発行している。この情報のやり取りにおいて、改ざん等の防止のために医療機関はトラストサービスを使用した医療データの登録が義務付けられており、医療機関と処方箋システム間のデータのやり取りにおいては、e シール、タイムスタンプ、e デリバリーの 3 種類のトラストサービスが使用されている。

使用されているデジタル ID のレベルは患者の薬局での薬処方に対してはデジタル ID カードによる対面認証、患者の Web 処方履歴閲覧に対してはカード/Mobile/Smart ID による共通オンライン認証、医者/看護師の識別・資格確認に対しては個人番号が使用されている。

以上のような電子処方箋サービスを実現するために大きく 3 つのプラットフォームを適用している。1 つ目のデータ統合プラットフォームは、健康保険基金が運営する処方箋システムでデータを一元管理するプラットフォームである。2 つ目は個人認証プラットフォームで、患者/医者ポータルへのログインは、共通オンライン認証プラットフォームを利用している。3 つ目は取引連携プラットフォームであり、ポータル/医療機関システム/処方箋システム間の連携制御を行っている。

分類	調査の観点	詳細
1 各業界サービス	トラストサービスを活用したデジタルサービスのニーズ	<ul style="list-style-type: none"> エストニアのヘルスケア業界におけるサービスニーズは? ペーパーレス化の対象として旧来の紙の処方箋発行を電子化(処方箋発行の99%が電子化。再処方方の依頼はEmailやLINE経由) トラスト活用余地は? 健康保険基金が運営する処方箋システムにデータを統一化 医療機関はトラストサービスを使った医療データの登録が義務付け
2 デジタルID	個人・法人のアイデンティティの運用実態	実際にどのレベルのデジタルIDが利用されているか?→国が管理するPKI上で、国民に紐づくデジタルIDを厳格に管理/識別 <ul style="list-style-type: none"> 患者の薬局での薬処方: デジタルIDカードによる対面認証 患者のWeb処方履歴閲覧: デジタルIDカード/Mobile/Smart IDによる、デジタルIDを用いた共通オンライン認証 医者/看護師の識別・資格確認: デジタルIDが使われる →専門医の診察はかかりつけ医の紹介が必要なため、地域診療所ほど電子化が進む
3 トラストサービス	各業界サービスにおいて活用されるトラストサービス及びトラストサービスプロバイダの実態	どのトラストサービスが個人/法人格の証明として使われているか? <ul style="list-style-type: none"> 医療機関⇔処方箋システム間の処方箋データのやり取り ①eシール、②タイムスタンプ、③eデリバリー*の3種類を活用 ※eシールとタイムスタンプを組み合わせることでやり取りの正当性が担保され、eデリバリーが実現
4 要素技術/PF	取引連携PF (X-road)、政府・民間CA、個人認証PF、データ統合PF等の適用状況の実態	上記を実現する業界横串でのプラットフォーム適用状況は? <ul style="list-style-type: none"> データ統合PF: 健康保険基金が運営する処方箋システムでデータ一元管理 個人認証PF: 患者/医者ポータルへのログインは共通オンライン認証PF利用 取引連携PF: ポータル/医療機関システム/処方箋システム間の連携制御
5 法令/標準	eIDASで規定されるアシュアランスレベル適用実態	<ul style="list-style-type: none"> デジタルID 薬処方時: High、ポータル利用時: Substantial トラストサービス ①eシール: 「適格電子証明書付きの高度eシール」または「適格eシール」 ②タイムスタンプ: 「適格タイムスタンプ」 ③eデリバリー: 記載されている資料なし

具体的なサービスの流れは、患者がメールや Skype、電話にて医者へ発行依頼を出し、その後医者が電子的に処方箋を発行し、患者が薬局にて ID カードによる本人認証を行い薬の処方に至るというものである。患者の負担を減らすだけでなく、医者が処方箋を繰り返し発行する手間を減少させることができる等のメリットがあり、エストニア国内では処方箋の 99%が電子的に発行されている。

概要

- ペーパーレス化の対象として、旧来の紙の処方箋発行を電子化
- 処方箋は健康保険基金が運営
- システムにデータを統一化し、エストニア内のすべての処方箋の99%が電子的に発行されている

特徴

- 患者はEmail、Skype、電話で医師に連絡でき、医師は繰り返し発行できるため、都度の診察が不要
- 本人は患者ポータルにて処方情報を参照可能
- 医療機関はトラストサービスを使った医療データの登録が義務付けされている

電子処方箋サービスを利用した薬の処方の流れ

	発行依頼	発行	データ登録	本人確認	データ参照	処方
実施内容	患者が病人で問診・またはメールやラインから医師に連絡	医者がパソコンを操作して電子処方箋を発行	電子処方箋情報をデータベースに登録	薬局にて患者がIDカードによる本人確認を実施	薬剤師が電子処方箋情報管理のデータベースにアクセス	薬を処方(本人は後から患者ポータルにて処方情報を参照可能)
場所	自宅または病院	病院	病院	薬局	薬局	薬局
実施者	患者	医者	医者	患者	薬剤師	薬剤師

また、患者の薬局での薬処方や患者の Web 処方履歴閲覧、医者/看護師の識別・資格確認でデジタル ID を利用している。

患者の薬局での薬処方

概要

カードリーダーを用いたデジタルIDカードによる対面認証

利用イメージ (2011年時)



医者/看護師の識別・資格確認

概要

当該人物が医者/看護師であるかの情報がデジタルIDに紐付けられているため、デジタルIDを利用しての医者/看護師の識別・資格確認が可能

患者のWeb処方履歴閲覧

概要

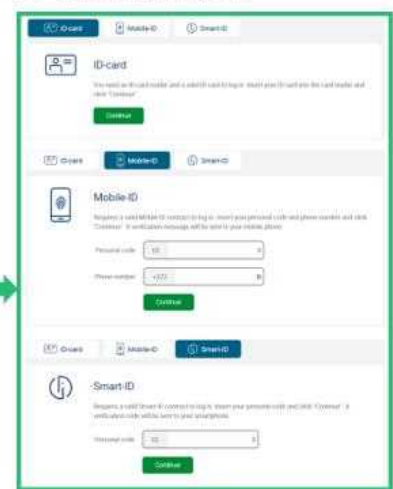
患者ポータルからログインを行うと、シングルサインオンにて認証を行うeサービス本人認証用の別サイトへと遷移

上記サイトでは、IDカード・モバイルID・スマートIDを用いて認証が可能

患者ポータルサイト

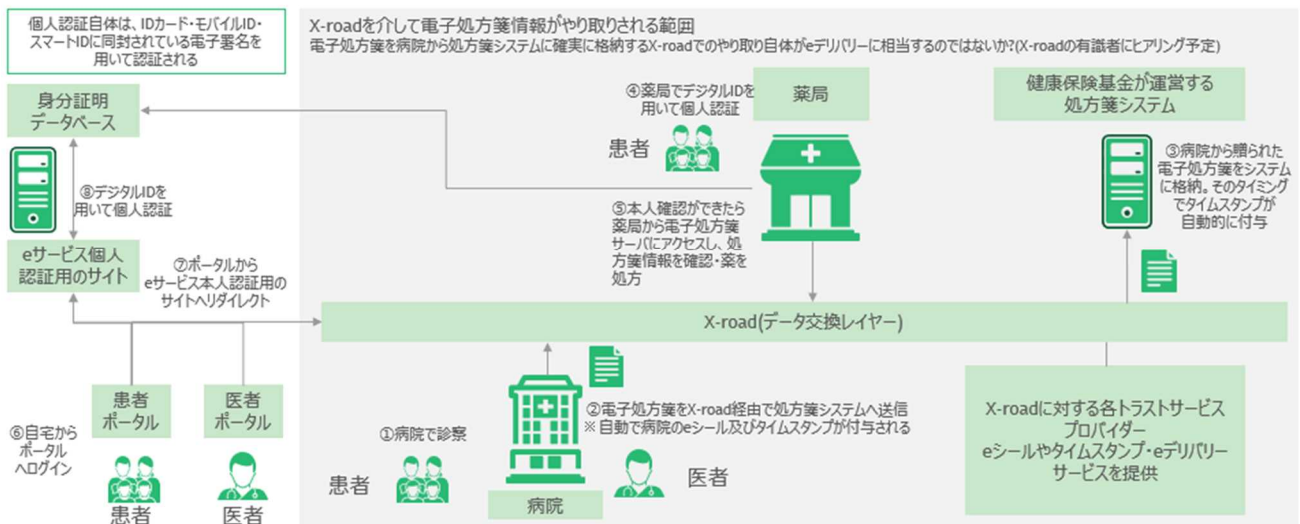


eサービス本人認証用のサイト



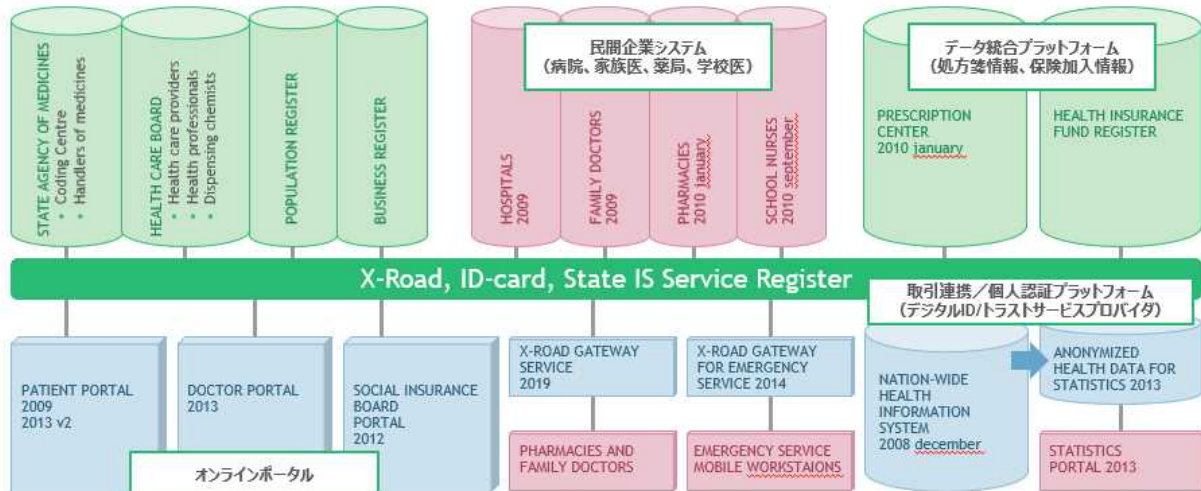
データのやり取りは X-road を介し e シール、タイムスタンプ、e デリバリーの 3 種類を活用されている。

電子処方箋サービスにおけるトラストサービスの関係図



また、エストニアではヘルスケア業界において要素技術/プラットフォームの整備を行っており、処方箋のペーパーレス化に留まらず、PHRの統合、それによるかかりつけ医から専門医への紹介等を電子化している。民間企業(医療機関等)にデータ統合PFへの連携を義務付け、電子化を推進すると共に、データ統合は国民団体が運営・管理することでシステムの普及を行っている。また各システム間の連携(本人確認、文書の正当性保証、文書の確実な送受信等)をHubとなるプラットフォームで一元管理を行っている。

- 処方箋のペーパーレス化に留まらず、PHRの統合、それによるかかりつけ医から専門医への紹介等を電子化
- 民間企業 (医療機関 等) にデータ統合PFへの連携を義務付け、電子化を推進。データ統合PFは国民団体が運営・管理
- 各システム間の連携 (本人確認、文書の正当性保証、文書の確実な送受信 等) をHubとなるプラットフォームで一元管理



Source: [Description of the current status and future needs of the Information Architecture and Data Management solutions for the national personalised medicine pilot project] (University of Tartu) (https://www.sm.ee/sites/default/files/content-editors/eesmargid_ja_tegevused/Personaalmiditsiin/description_of_the_current_status_and_future_needs_of_the_information_architecture_and_data_management_solutions_for_the_national_personalised_medicine_pilot_project.pdf)

さらに、エストニアの電子処方箋サービスに於けるアシュアランスレベルは、eIDAS で定義されているアシュアランスレベルの中でも高度なレベルを達成している。

	サービス名	利用シーン	eIDASで定義されている達成アシュアランスレベル
デジタルID	eID	<ul style="list-style-type: none"> • 患者の薬局での薬処方 • 患者のWeb処方履歴閲覧 • 医者/看護師の識別・資格確認 	薬処方時: High ポータル利用時: Substantial
トラストサービス	eシール	電子処方箋に対する病院の発行元証明	高度または適格
	タイムスタンプ	電子処方箋に対する資料作成時刻・資料をシステムへ格納した時刻の証明	適格
	eデリバリー	電子処方箋を処方箋システムへ確実に格納する際に利用	不明

海外アシュアランスレベルの調査

本調査では、ヨーロッパの eIDAS、アメリカの NIST SP800-63 についてアシュアランスレベルの整備状況を整理している。まず、この 2 つの ID・トラストサービスに、ニュージーランドの ID 管理基準を加えた 3 つに関してアシュアランスレベルの整備有無状況をまとめた。本人確認と認証プロセスがいずれのサービスにも組み込まれている一方、サービス事業者の運営条件、認証情報連携、割当に関しては整備状況に差異が生じている。

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	ニュージーランドの ID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	—	—	✓

まず eIDAS について見ていくが、始めに最初の eIDAS である eIDAS1.0 について述べる。eIDAS1.0 では「Level of Assurance」を 3 段階で定めており、各サービスが管理する情報の Sensitivity によって規定される。各 Level of Assurance によって、デジタル ID を発行するプロセス、デジタル ID による多要素認証パターン、セキュリティコントロール等に差が生まれる。

Level of Assurance	アシュアランスレベルの具体例
Low	サービスへの入会を、個人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	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/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	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。

以上の事例からデジタル ID のアシュアランスレベルに関する論点は、以下の 4 つ程度存在する

- アシュアランスレベルは、現実的な適用ニーズのあるパターンに絞って一次元でレベルを規定するべきか
 - 進め方として、考え得る全パターンの適用ニーズを検証し、最終的に判断するか
- アシュアランスレベルを構成する要素は、①サービス利用登録時の利用者の身元の信用度、②サービス利用時の認証の信用度で良いか
 - NIST で言うと①が IAL、②が AAL 相当となるが、要素の定義に相違はないか? (FAL については別途議論)
- Identity Assurance のレベルを決める要素として、以下の要素以外を想定するか
 - 身元確認のため提示する ID: 公的機関から発行された ID (運転免許証、保険証)、デジタル ID (マイナンバーカード等)
 - 身元の確認方法: サービス事業者による確認、もしくはデジタル ID による確認
 - 非対面/対面: どちらでも、もしくは対面必須

- Authentication Assurance のレベルを決める要素として、以下の要素以外を想定するか
 - 認証の要素数: 単一、もしくは複数
 - 耐タンパー性の確保有無: HW トークン上の PKI アクセスが必須か
 - 個人を特定できる情報の暗号化: 必須、もしくは 不要
 - ◇ FAL のような認証済情報も対象に含めるべきか

Level of Assurance	Identity Assurance (登録時の身元信用度)	Authentication Assurance (認証の信用度)
Low	<ul style="list-style-type: none"> 公的機関から発行されたIDの提示 (リモート/対面問わず) 	<ul style="list-style-type: none"> 単一要素認証 (例: ID or PINコード)
Substantial	<ul style="list-style-type: none"> 公的機関から発行されたIDの提示 (リモート/対面問わず) 登録機関によるIDのペリアイ 	<ul style="list-style-type: none"> 多要素認証 (例: 携帯SIM認証 + PINコード)
High	<ul style="list-style-type: none"> 対面でのID提示と登録機関によるIDのペリアイ 政府発行のソース/ドキュメントによるIDのペリアイ (eID) 	<ul style="list-style-type: none"> 多要素認証 耐タンパー性が確保されたHWトークン上でのPKIアクセス必須 個人を特定できる情報の暗号化

また、適格トラストサービスプロバイダは、1 つ以上の適格トラストサービスを提供し、監督機関より資格を与えられたトラストサービスプロバイダを指す。eIDAS 規則第 20 条に監督/監査要件が定められており、要件は以下等が挙げられる。

- 24 ヶ月に 1 度の適合性評価機関の監査 (監査結果は 3 日以内に監督機関に提出)
- 監督機関はいつでも追加の監査の要求や立ち入り監査を行える
- 監督機関は適格トラストサービスプロバイダに問題があれば適格認定を取り消すことができる

トラストサービス種別	概要	法的効力について
適格	eIDASによって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され、定期的な監査が必要	EU内で有
高度 (電子署名・ eシールのみ存在)	仕様に幅があり各国の電子署名法に合わせられる	電子形式である、適格サービスでないという理由で法的効力が否定されない
通常	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され、事後監査が必要	電子形式である、適格サービスでないという理由で法的効力が否定されない

これに対して、今後 eIDAS1.0 が定めるアシュアランスレベルをベースに、ID/属性情報流通に関する政府 PF 関与強化/下位規則具体化による TSP 普及等、トラストサービスの普及/運営強化に係る規約の制定が盛り込まれた eIDAS2.0 がローンチされる見込みである。

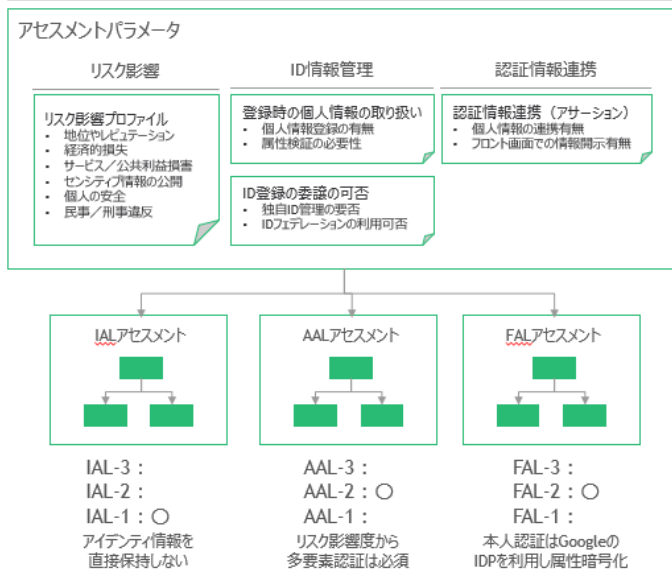
カテゴリ	改正案	詳細
eID	Digital Identity Wallet (EUDIW)	<p>EU内でVoluntaryベースでのデジタルID普及を目指す（2030年までにEU人口の80%カバーが目標） 民間プラットフォーム含めたEU内サービスでの政府共通認証機能の普及率を高め、透明性かつ保証レベルの高い個人情報の管理を実現することが狙い</p> <ul style="list-style-type: none"> 個人識別データ（ID）、属性情報の流通促進のための共通IF化 識別データ/属性の電子証明に関して、ユーザが追跡可能な方法で取得・保管することが義務付け。 （適格電子署名+保証レベルHigh） TSP/QTSP向けの電子証明書発行インターフェース共通化とRelying Partyによる識別データおよび属性証明の要求と確認を義務付け。 サービス事業者への勧告 サービス事業者（RP）が識別データ/属性情報の利用目的を加盟国に通知すること、加盟国は共通認証機能を提供し、データの透明性を保証することが義務付け。
トラストサービス	トラストサービスの拡充	<p>eIDASの対象となるトラストサービスについて以下が拡充される</p> <ul style="list-style-type: none"> 電子台帳 分散台帳/ブロックチェーンに関する法的効果の承認。（データの真正性や時系列的な順序性など） 電子アーカイブ 電子データまたは文書の受領、保存、削除、送信を保証するサービス 属性の電子証明 属性の認証を許可する電子形式の証明（eシールや電子署名のための適格証明書の要件と同等）
その他	下位規則の整備	<p>技術基準等、eIDASが定める法的要件に対する下位規則を具体化。 欧州委員会に対して法律によって下位規則を定めることが義務付け。</p> <p>※欧州のQTSPが遵守すべき基準が明確化。電子台帳に関しては下位規則の整備義務付けは先送り。</p>

また、eIDAS2.0の認証連携に関するアシュアランスレベルと、トラスト下位規則について具体的に述べる。FAL (Federation Assurance Level) と Digital Identity Wallet については、技術面では加盟国が管理するID/属性の電子証明の発行方法や、RP/IDP間のID/属性情報の要求/確認の義務付けを、運営面では各サービス事業者のID/属性情報の利用目的の通知、加盟国のデータ透明性の保証の義務化を行っている。ここでの論点は、Federation (認証連携) に関するアシュアランスレベルとして技術面/運営面での遵守事項を定めるeIDASのアプローチを採用するか、GDPRとも絡み、個人情報保護の観点から政府の関与を強める方針を取るべきかという2点である。

さらにトラストサービスの会規則の整備については、定義されているすべてのトラストサービスに関して、規約発行後12ヶ月以内に下位規約制定の必要性が記載される。ここでの論点は、トラストサービスのアシュアランスレベルとして、技術標準等の下位規則を含めるべきか必要性のみ言及するべきか、必要性に言及する場合、日本国内における運用を見据えてどのトラストサービスまでを義務付けるべきかという2点である。

次にSP800-63-3について言及する。SP800-63-3では、各事業者がリスク影響度や個人情報の取り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する。具体的には、リスク影響とID情報管理、認証情報連携がパラメータとなり、アシュアランスレベルが3段階に分岐する仕組みとなっている。

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ID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IDソリューションへの対応

政府システムにおいてもID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) ID管理/認証はプラットフォームのIDプロバイダ機能へ委譲 (フェデレーション) する

42

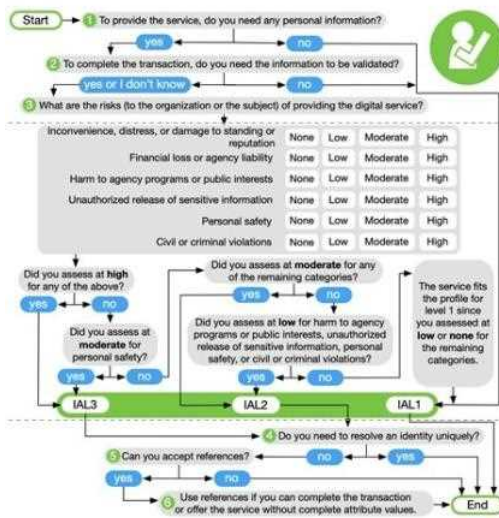
定義内容	定義LoA	LoAの詳細
ユーザ身元確認の確からしさ	IAAL (Identity Assurance Level) SP 800-63A	IAAL.1 身元確認に必要なエビデンスやプロセスの指定なし、自己申告でよい
		IAAL.2 現実世界での存在を示すエビデンスをリモートまたは対面で確認する必要あり
		IAAL.3 物理的な存在を示すエビデンスを対面確認する必要あり。検証担当者は有資格者
ユーザ認証の確からしさ	AAL (Authentication Assurance Level) SP 800-63B	AAL.1 1要素または2要素による認証
		AAL.2 2要素認証、NIST/FIPS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)

それぞれのアシュアランスレベルは、個人情報の取り扱い有無、リスク影響度、フェデレーションの要否に合わせて定義が行われており、適切なアシュアランスレベルが設定されている。

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り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



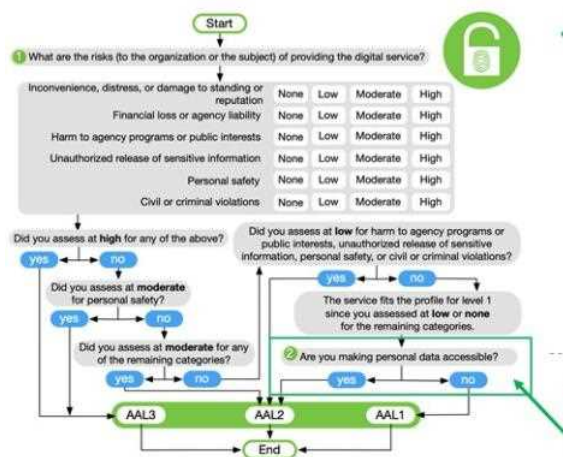
アセスメントの要諦

- **個人情報の取り扱い有無、属性情報等のバリデーション要否**
サービス登録時、個人情報の取り扱いがない場合、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て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（治療を伴う）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、IDリファレンスの可否**
IDの独自管理が不要で、他ソリューションへのID参照が可能であればフェデレーションによるID連携を推奨する。

SP800-63-3 : AALのアセスメントロジック

AALはIALのリスク影響度のアセスメントと同等ロジック+個人情報の取り扱い有無でアシュアランスレベルを決定する

AALのアセスメントフロー



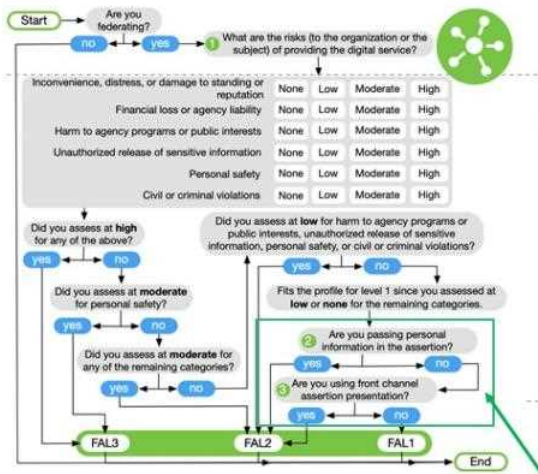
アセスメントの要諦

- **リスク影響度に合わせて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AAL-3相当
 - 上記以外で、個人の安全がModerate（治療を伴う）リスクがある場合AAL-3
 - 上記以外で1項目でもModerateがあればAAL-2
 - 上記以外で以下4項目でLowがあればAAL-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AAL-1
- **個人情報の取り扱い有無**
リスク影響度でAAL-1相当でも、個人情報の取り扱いがある場合は、AAL-2相当とする

SP800-63-3 : FALのアセスメントロジック

主にインシデントが起きた際の被害の「影響度」によって、満たすべきアシュアランスレベルが判断フローに則り決定される

AALのアセスメントフロー

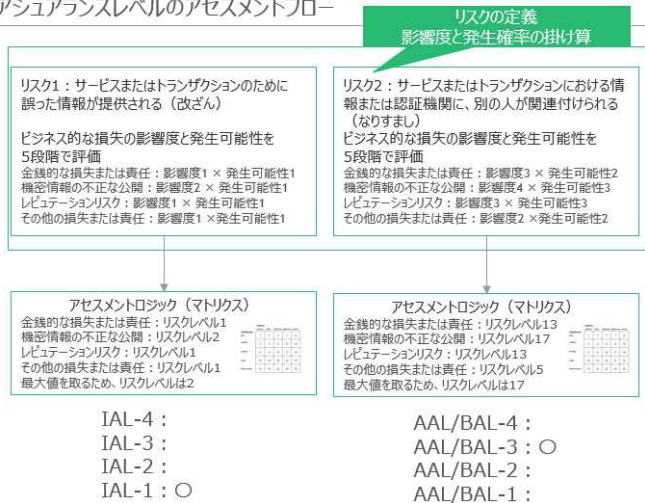


アセスメントの要諦

- **フェデレーションの有無**
フェデレーション前提でない場合は、FALは規定しない
- **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FAL-3相当
 - 上記以外で、個人の安全がModerate（治療を伴う）リスクがある場合FAL-3
 - 上記以外で1項目でもModerateがあればFAL-2
 - 上記以外で以下4項目でLowがあればFAL-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FAL-1
- **アサーション内の個人情報有無、フロントでのアサーション情報表示有無**
リスク影響度でFAL-1となった場合も、アサーション内で個人情報を取り扱う場合、もしくはフロントでアサーション情報を表示する場合はFAL-2

次にニュージーランドのID管理基準について言及する。ニュージーランドのID管理基準では、デジタルID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。また、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。

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

- **想定されるリスクが定義されている**
デジタルID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、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

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



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

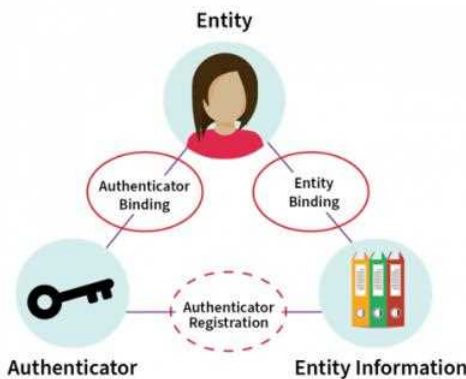
リスクレベルによるアシュアランスレベル評価

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

また、バインディングという概念がニュージーランドの ID 管理基準では定義されているが、これは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である。

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

ニュージーランド政府の ID 管理基準では、情報エビデンスの確からしさ、エンティティ紐付けの確からしさ、ユーザ認証の確からしさ、認証情報連携の確からしさを定義するアシュアランス要素が規定されている。

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

1.4 Society5.0 実現に向けたトラストの必要性

サマリ

我が国が目指す未来社会 Society 5.0 においては、IoT (Internet of Things) で全ての人とモノがつながり、様々な知識や情報が共有され、今までにない新たな価値を生み出すことで、経済発展と社会的課題の解決を両立していくことが目指されている。特に「交通」「医療・介護」「ものづくり」「農業」「食品」「防災」「エネルギー」等の分野が例として挙げられており、今後の実現が期待される一方、IoT を活用した社会システムにおいては、なりすましやデータ改ざん等のリスクがあり、海外で事件化する例も発生している。そのようなリスクを回避するための手段としてトラストサービスの有効性が期待されているため、本調査では Society5.0 に向けたトラストサービスの必要性を整理した。

Society5.0 における新たな価値

まず、Society5.0 の概要を説明する。Society5.0 はこれまでの情報社会 (Society4.0) と比較して生まれた概念である。Society4.0 では人間の情報処理能力の制約や、年齢や障害等による労働や行動範囲による制約、少子高齢化や地方の過疎化等の人口の制約等多数の制約が存在するために、知識や情報が共有されず、分野横断的な連携が不十分であるという問題が存在した。そこで Society5.0 で実現する社会では、IoT ですべての人とモノがつながり、様々な知識や情報が共有され、今までにない新しい価値を生み出すことでこれらの課題や困難を克服することを目指す。

具体的には、「交通」「医療・介護」「ものづくり」「農業」「食品」「防災」「エネルギー」等の分野で Society5.0 の新たな価値を提供することができると考えられている。例えば「交通」の分野では、各自動車からのセンサー情報、天気、交通、宿泊、飲食といったリアルタイムの情報、過去の履歴等のデータベースといった様々な情報を含むビッグデータを AI で解析することにより、「好みに合わせた観光ルートの提供や天気や混雑を考慮した最適な計画が提案され、旅行や観光がしやすくなること」「自動走行で渋滞なく、事故なく、快適に移動すること」「カーシェアや公共交通の組み合わせでスムーズに移動すること」「高齢者や障がい者でも自律型車いすを使って 1 人で移動すること」といったことができるようになるとともに、社会全体としても交通機関からの CO2 排出が削減され、地方の活性化や消費の拡大にもつながるといったような事例が確認されている。



業界

Society 5.0 で期待されるサービス

- 例) 交通 Society 5.0 では、各自動車からのセンサー情報、天気、交通、宿泊、飲食といったリアルタイムの情報、過去の履歴等のデータベースといった様々な情報を含むビッグデータを AI で解析することにより、「好みに合わせた観光ルートの提供や天気や混雑を考慮した最適な計画が提案され、旅行や観光がしやすくなること」「自動走行で渋滞なく、事故なく、快適に移動すること」「カーシェアや公共交通の組み合わせでスムーズに移動すること」「高齢者や障がい者でも自律型車いすで 1 人で移動すること」といったことができるようになるとともに、社会全体としても交通機関からの CO2 排出が削減され、地方の活性化や消費の拡大にもつながることになります。
- 例) 医療・介護 Society 5.0 では、各個人のリアルタイムの生理計測データ、医療現場の情報、医療・感染情報、環境情報といった様々な情報を含むビッグデータを AI で解析することにより、「ロボットによる生活支援・話し相手等により 1 人でも快適な生活を送ること」「リアルタイムの自動健康診断等での健康促進や病気を早期発見すること」「整理・医療データの共有によりどこでも最適な治療を受けること」「医療・介護現場でのロボットによる支援で負担を軽減すること」といったことができるようになるとともに、社会全体としても医療費や介護費等の社会的コストの削減や医療現場等での人手不足の問題を解決することが可能となります。
- 例) エネルギー Society 5.0 では、気象情報、発電所の稼働状況、EV の充放電、各家庭での使用状況といった様々な情報を含むビッグデータを AI で解析することにより、「的確な需要予測や気象予測を踏まえた多様なエネルギーによって安定的にエネルギーを供給すること」「水素製造や電気自動車 (EV) 等を活用したエネルギーの地産地消、地域間で融通すること」「供給予測による使用の最適提案等による各家庭での省エネを図ること」といったことができるようになるとともに、社会全体としてもエネルギーの安定供給や GHG 排出の削減等の環境負荷の軽減を図ることが可能となります。

Society5.0 で必要とされるトラスト

IoT を活用した社会システムやサービスへの期待は高いが、一方でそれらの社会システムやサービスにおいては、なりすましやデータ改ざん等のリスクがあり、例えば交通分野では、「コネクテッドカー」に関して総務省からデータの真正性確保が必要と指摘されている。さらに海外ではすでに事件化する事例も発生している。アメリカでは、医療分野にて「IoT 医療機器」に関してインターネット経由で投与する薬や投薬量を改ざんできる脆弱性が発見され、プエルトリコではエネルギー分野にて「スマートグリッド」に関して、電力使用量データが改ざんされる事件が発生した。これらのリスクに対処するためにトラストサービスが必要であり、IoT を活用した Society5.0 を実現するために必須であると言える。

手続き 分類	BtoB BtoC BtoC/C	BtoC/GtoB BtoC/GtoC GtoB/C	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					その他
	行政	民間	金融・保険	情報通信	不動産	医療・福祉	運輸・郵便	
海外連携が必要なものの	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、変更届出等の申請、運転免許証、国際運転免許証、パスポート、自動車保有管理所事務	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	通学定期券の発行、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、後見届出等の申請、補助金等の請求、年金関連の手続、健康保険関連の手続、防災関連の手続、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)	治療データの作成・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、受発注書の取り交し、契約書の取り交し、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: 企業向けアンケート調査 (n=347, 2021/11/24~12/7実施)

2.1 個人からのトラスト確保のニーズ

サマリ

デジタル/オンラインでの手続き等に対して、「他人によるなりすまし」(72%)や「データの改ざん」(68%)等、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。このリスクに対応するために、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2分の1(49%)存在し、トラストサービスによって防ぎ得るリスクがデジタル/オンラインの手続き等の利用を阻害する一因になっていると言える。そのような背景もあり、トラストサービスによって享受できるメリットを魅力的に感じる人は多く、「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%)等軒並み50-60%程度を占める。さらにトラストが確保されることを前提とすると、現状に比べて、「不動産賃貸/売買の契約」(34%→44%)、「融資/ローン契約」(33%→40%)等、デジタル/オンラインでの手続き等の利用意向は増大することもわかった。

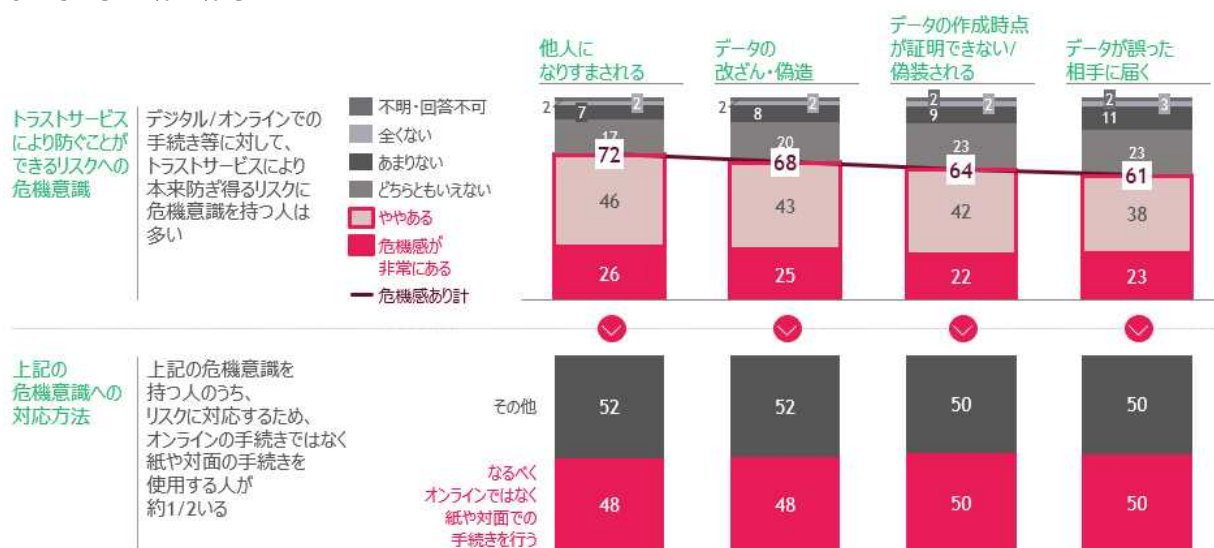
次に、特にトラスト確保のニーズが大きい手続き等についても分析を行った。まずデジタル化できていない手続き等では「選挙での投票」「運転免許証の更新/交付」や、「通学定期券の発行」「住民票関連の申請」「戸籍の届け出」「旅券の交付」等のニーズが大きい結果となった。また現在デジタル化されているものの、トラスト確保によってデジタル/オンライン利用意向が増大する手続き等は「不動産賃貸/売買の契約」「融資/ローン契約」や、「国内送金」「銀行/証券口座開設」「携帯/スマホの新規契約」「健康診断/審査結果の発行」等という結果となった。

さらに、現在実現されていないものの、トラストの確保によって今後実現される可能性のあるサービスの中では、「パーソナルヘルスレコード」(53%)、「遠隔医療/デジタルでの問診」(36%)等のニーズが確認された。

トラストサービスへのニーズ

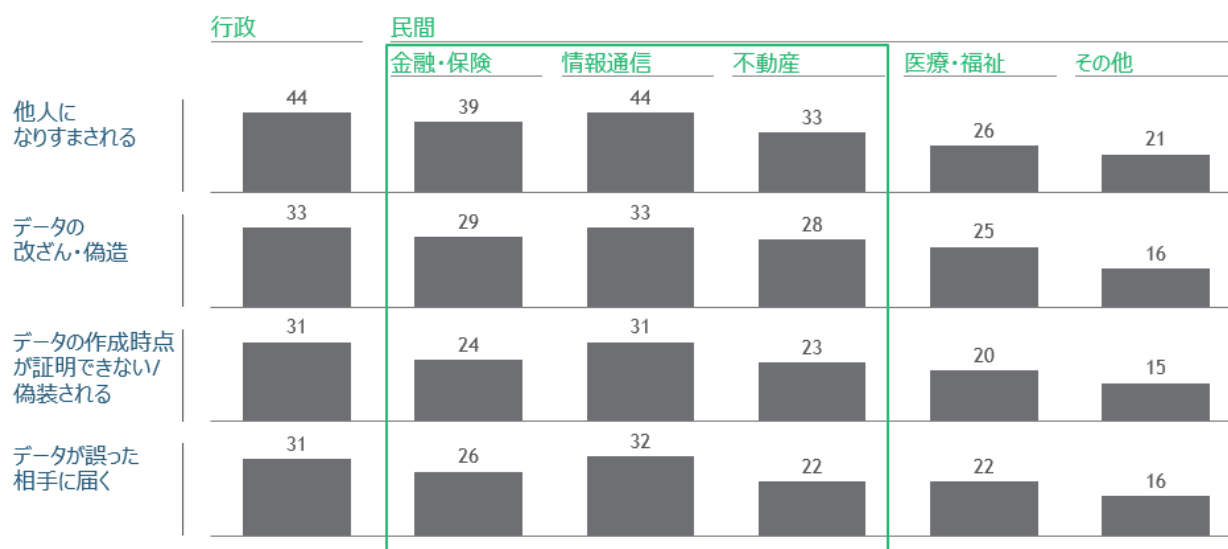
個人を対象としてデジタル/オンラインでの手続き等において、本来トラストサービスによって防ぎ得るリスクへの危機意識と、危機意識を感じた場合における行動を調査した。結果的に、デジタル/オンラインでの手続き等に対して、トラストサービスにより本来防ぎ得るリスクに危機意識を持つ人は多く、さらに危機意識を持った場合にリスクへの対処方法としてオンラインの手続きではなく紙や対面での手続きを使用する人が1/2程度存在することが分かった。この結果より、本来トラストサービスによって防ぎ得るリスクがデジタル/オンラインの手続き等の利用を阻害する一因と

なっていることがわかる。



Source: 個人向けアンケート調査 (n=4,406, 2021/11/19~11/24実施)

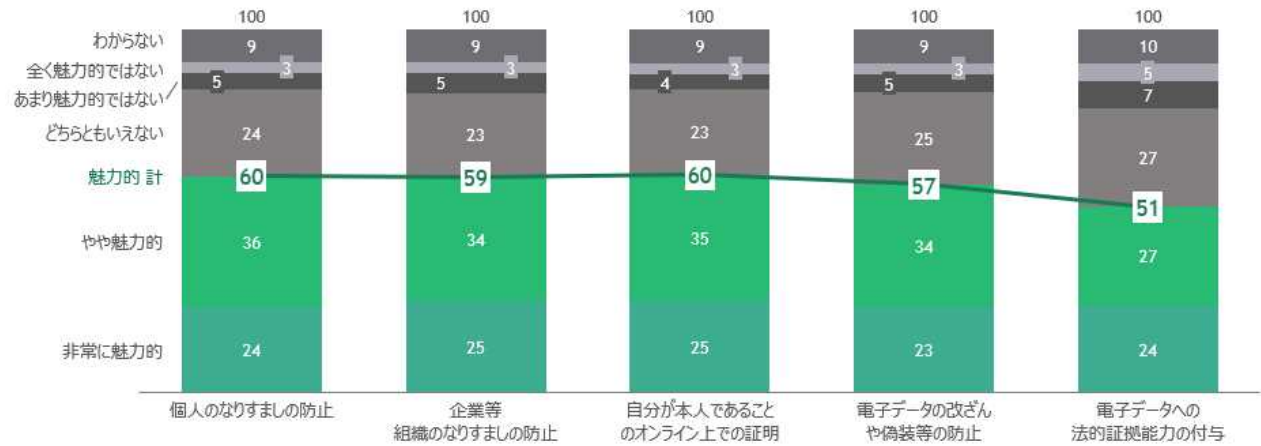
さらに、民間の業界別では特に「情報通信」「金融」「不動産」業界の手続き等へのリスク意識が高い。「金融」「不動産」業界はより秘匿度合いの高い情報を多く扱い、被害が生じた際に大きな損失額が発生するリスクが高い業界であり、また「情報通信」業界は近年フィッシング詐欺や偽装ウェブサイト等の身近なリスクが多く存在する業界であるため、リスク意識が高まっていると考えられる。



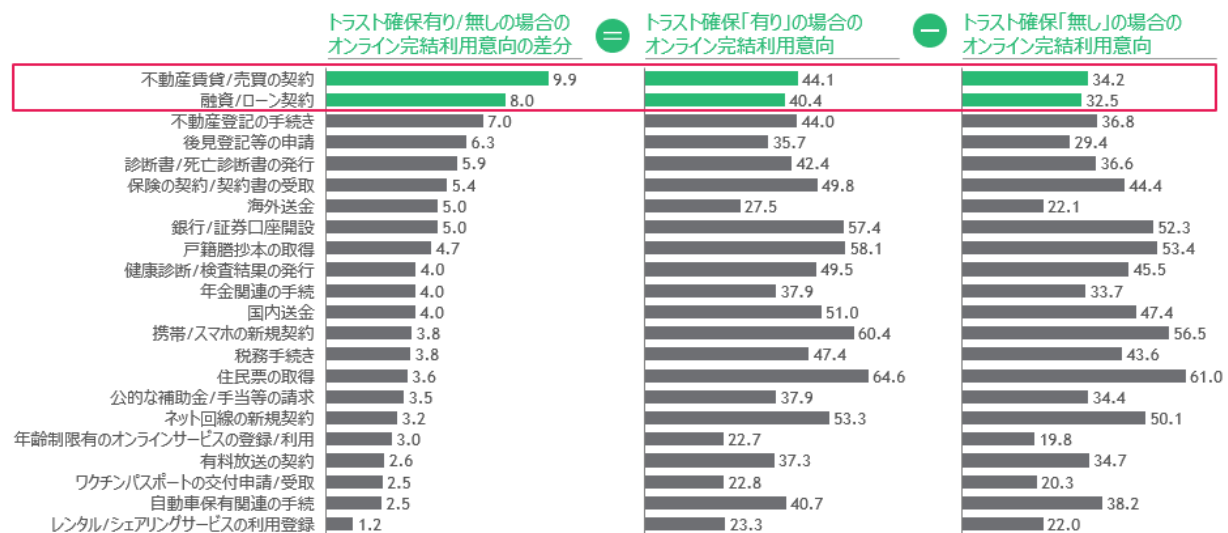
Source: 個人向けアンケート調査 (n=4,406, 2021/11/19~11/24実施)

また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%) 等軒並み 50~60%程度を占めている。

電子証明書等を用いることで実現できるメリットの魅力度



次に、トラスト確保「有り」の場合のオンライン完結利用意向から、トラスト確保「無し」の場合のオンライン完結利用意向を差し引いた値を元に、トラスト確保時のデジタル/オンラインの手続き等の利用意向の強さを分析した。結果的に、すべての手続きでトラスト確保「有り」の場合の方が「無し」の場合と比較してデジタル/オンラインの利用意向は大きくなっており、特に「不動産賃貸/売買の契約」「融資/ローン契約」等で顕著となっている。

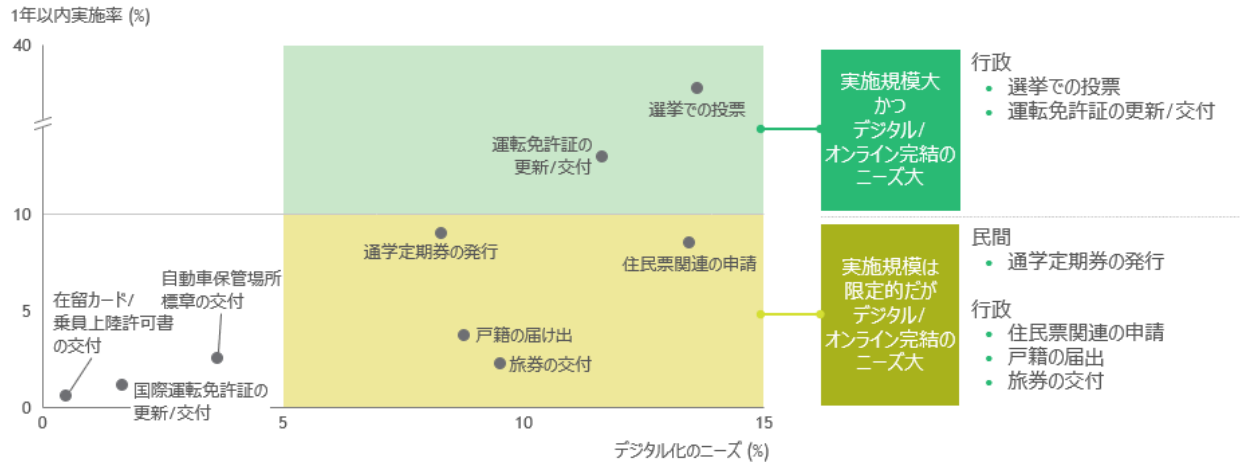


Source: 個人向けアンケート調査 (n=4,406, 2021/11/19~11/24実施)

69

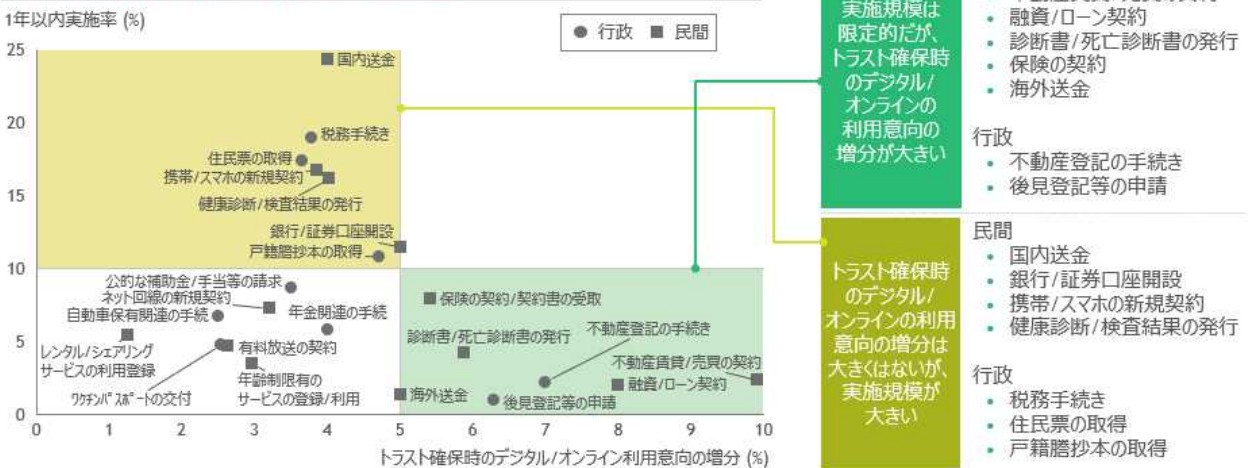
ここからはトラスト確保のニーズがある手続き等を詳しく分析する。まずデジタル化できていない手続き等を対象として、1年以内の手続き実施率を縦軸、デジタル化のニーズを横軸に取った散布図を作成した。この図で右上の緑のセグメントには、実施規模が大きくかつデジタル/オンライン完結のニーズが大きい最も優先的に取り組むべき手続き等が含まれている。具体的には、「選挙での投票」「運転免許証の更新/交付」等が挙げられる。また右下の黄色のセグメントには実施規模は限定的だがデジタル/オンライン完結のニーズが大きい手続き等が含まれており、こちらは規模がそれほど大きくないものの深いニーズが存在する可能性のある手続き等が属していると言える。具体的には、民間では「通学定期券の発行」、行政では「住民票関連の申請」「戸籍の届出」「旅券の交付」等が挙げられる。

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

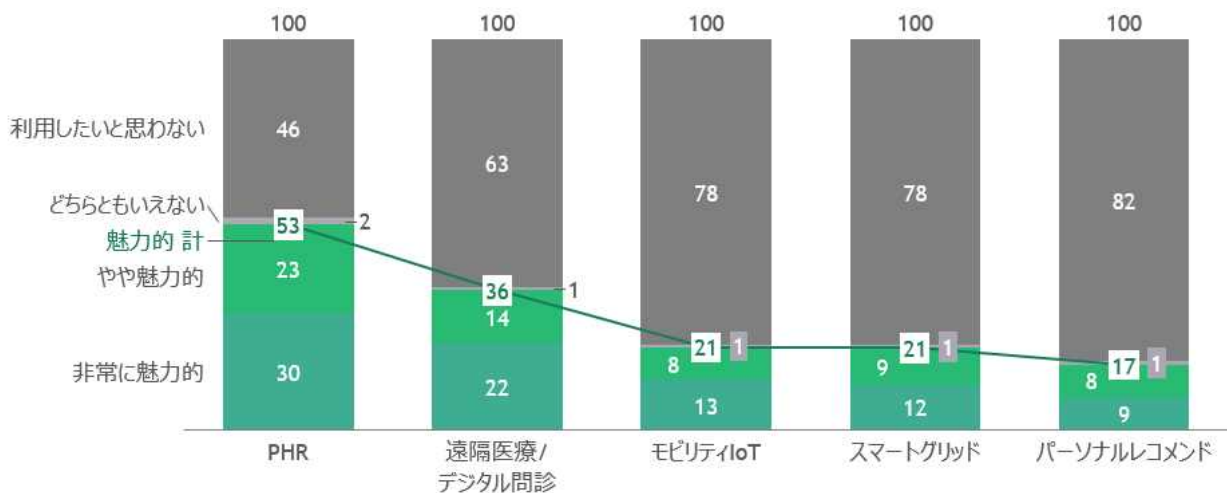


次にデジタル化はされているものの、デジタル化率がそれほど高くはない手続きを対象として、1年以内の手続き実施率を縦軸、トラスト確保時のデジタル/オンライン利用のニーズを横軸に取った散布図を作成した。この図で右下の緑のセグメントには、実施規模は限定的だがデジタル/オンライン利用意向の増分が大きい手続き等が含まれている。具体的には、民間では「不動産賃貸/売買の契約」「融資/ローン契約」等が挙げられる。また左上の黄色のセグメントにはトラスト確保時のデジタル/オンライン利用意向の増分は大きくはないが、実施規模が大きい手続き等が含まれており、こちらはトラスト確保に対するニーズはそれほど深くはないものの、規模が大きいために一定のインパクトを想定できる手続きが属していると言える。具体的には、民間では「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」等が挙げられる。

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



最後に、現在実現されていないものの、トラストの確保によって今後実現される可能性のあるサービスについても分析を行った。「パーソナルヘルスレコード」(53%)、「遠隔医療/デジタル問診」(36%)等のニーズが確認され、医療関連のサービスのニーズが上位を占めた。



2.2 企業からのトラスト確保のニーズ

サマリ

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、リスクそれぞれで最大 5 割近い水準である。またこれらのリスクへの対処法として、トラストサービスによって享受できるメリットに必要性がある企業は、「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 割存在する。さらに、トラストが確保されることで、何らかの手続き等のオンライン/デジタル化を期待する企業は 85%と高い水準で存在する。

次に、特にトラスト確保のニーズが大きい手続き等についても分析を行った。まず行政が所管しておりデジタル化できていない手続き等では「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できた。また現在デジタル化されているものの、デジタル化の期待が大きい手続き等は業種共通の「各種契約書類作成」「請求・支払書類作成」と、金融・保険の「銀行口座開設」「為替取引」「保険契約証書の発行・送付」等であり、中でも「受発注書類作成」「契約書類作成」「請求・支払い書類作成」等が特に大きなニーズがあることがわかった。さらに、トラスト確保によってデジタル/オンライン利用意図が増大する手続き等は「受発注書類作成」「国内送金/振込」「銀行口座の開設」等であった。

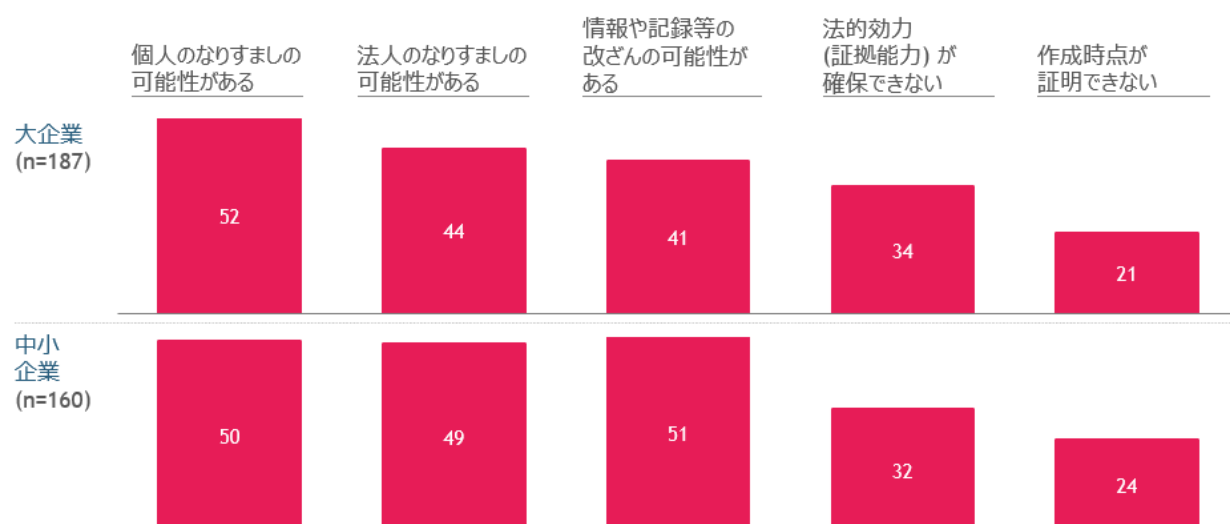
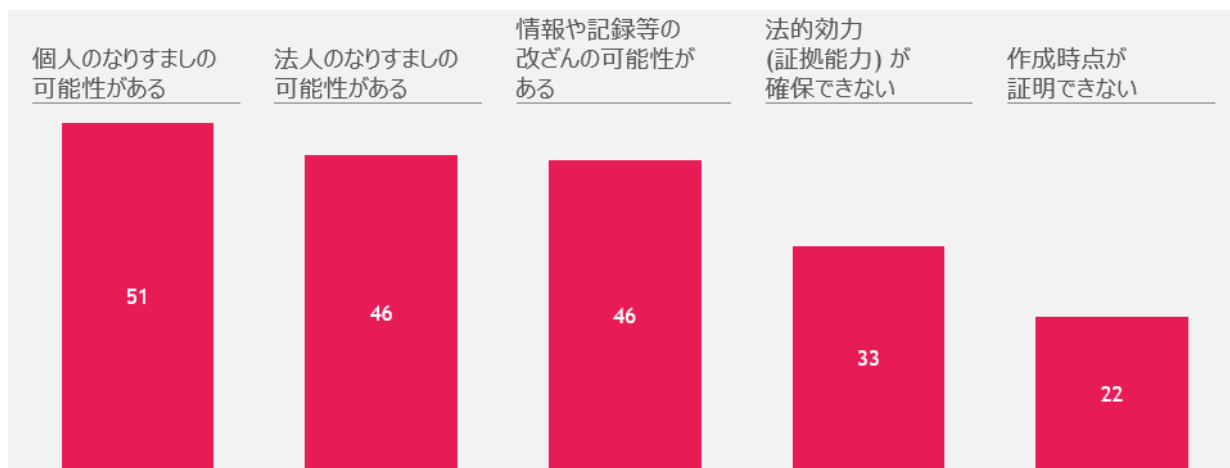
また、企業が行う手続き等の中で海外との取引等があり相手先の本人確認や情報改ざん防止が必要なものとしては、「受発注の取引書類」、「請求支払の取引書類」、「契約書」等の業種共通のものが多く挙げられた。

最後に、現在実現されていないものの、トラストの確保によって今後実現される可能性のあるサービスの中では、「パーソナルヘルスレコード」(16%)、「サプライチェーンのトレーサビリティ」(15%) 等のニーズが確認された。

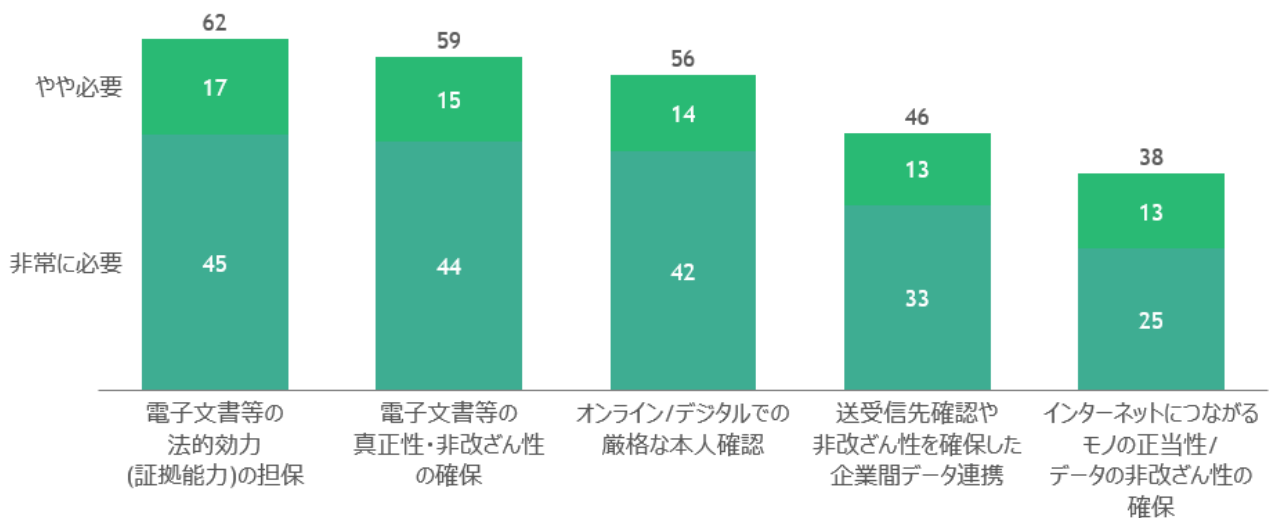
トラストサービスへのニーズ

企業を対象としてデジタル/オンラインでの手続き等において、本来トラストサービスによって防ぎ得るリスクへの危機意識を調査した。結果的に、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対して危機意識を持っている割合は「個人のなりすまし」(51%)、「法人のなりすまし」(46%) 等最大で 5 割に届

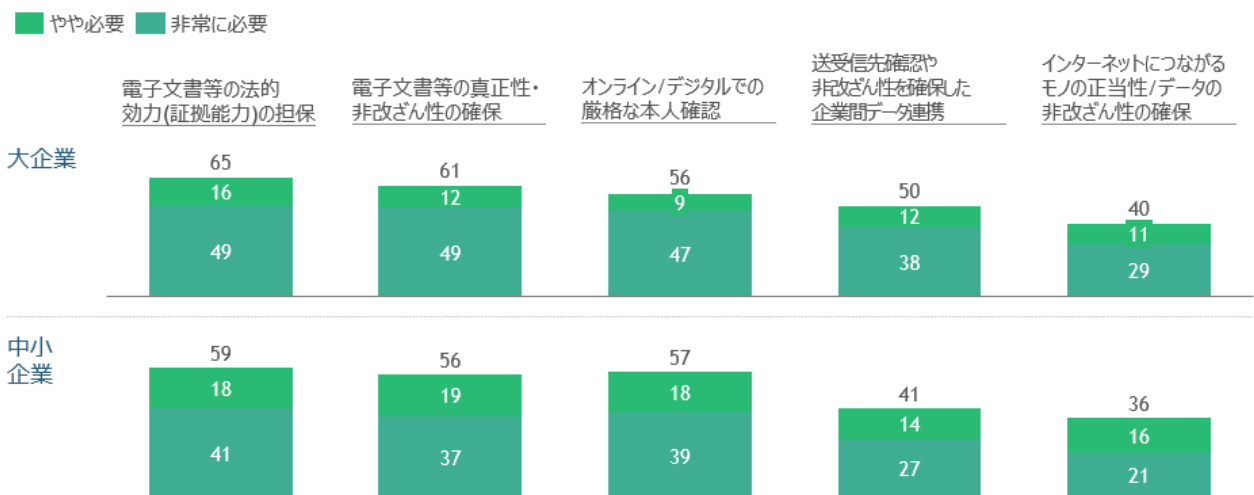
く水準となっている。この結果より、本来トラストサービスによって防ぎ得るリスクがデジタル/オンラインの手続き等の利用を阻害する一因となっていることがわかる。またトラストサービスにより本来防ぎ得るリスクに対して危機意識を持っている割合は、「情報買い残の可能性」について以外に関しては大企業と中小企業で大差はなく、中小企業でも同様に危機意識を持っていることが伺える。



また、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 割の企業が必要であると回答しており、トラストサービスへのニーズが広く存在することがわかる。また、この結果は大企業・中小企業で大差はなく、中小企業であってもトラストサービスへのニーズは強いものだということがわかる。



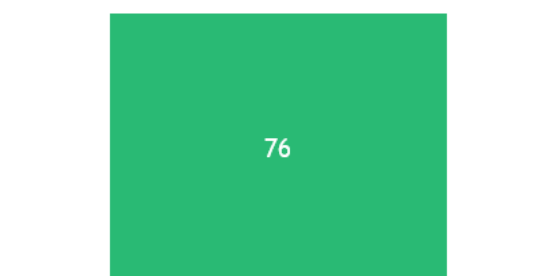
トラストサービスを導入することで実現できるメリットの必要性の程度



以上のようにトラストサービスへのニーズは広く存在し、実際にトラストが確保されることで何らかの手続き等のオンライン/デジタル化を期待する企業は約 8 割に上る。また、オンライン/デジタル化へのニーズは大企業・中小企業で大差はなく、両者同様にオンライン/デジタル化へのニーズが大きいと言える。

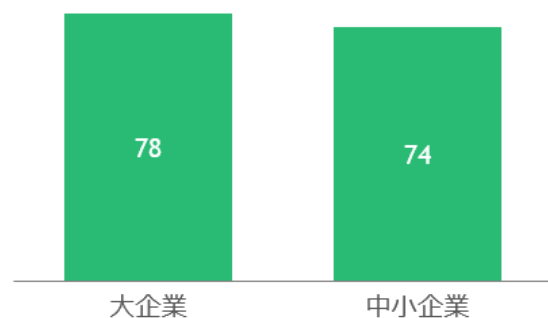
全体

トラストが確保されることで、何らかの手続き等のオンライン/デジタル化を期待する企業は76%



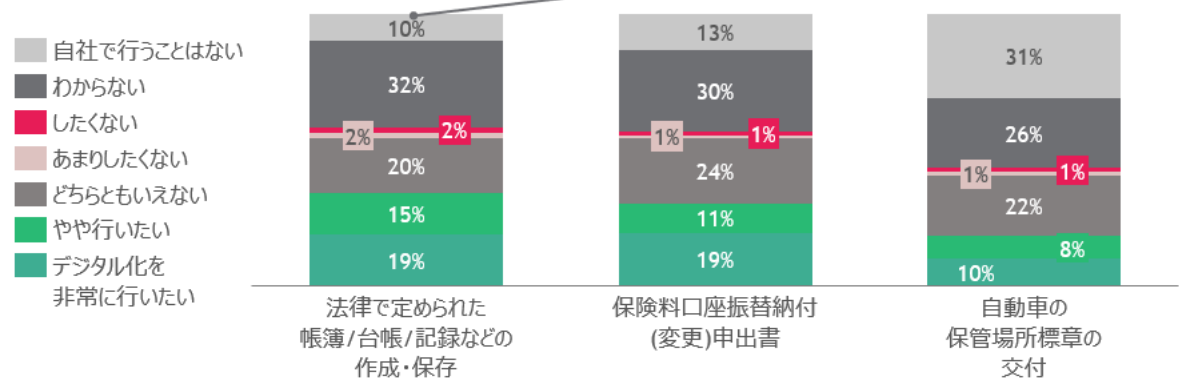
企業規模別

規模別では、「大企業」(78%) が「中小企業」(74%) に比べて多いが、大きな差はない

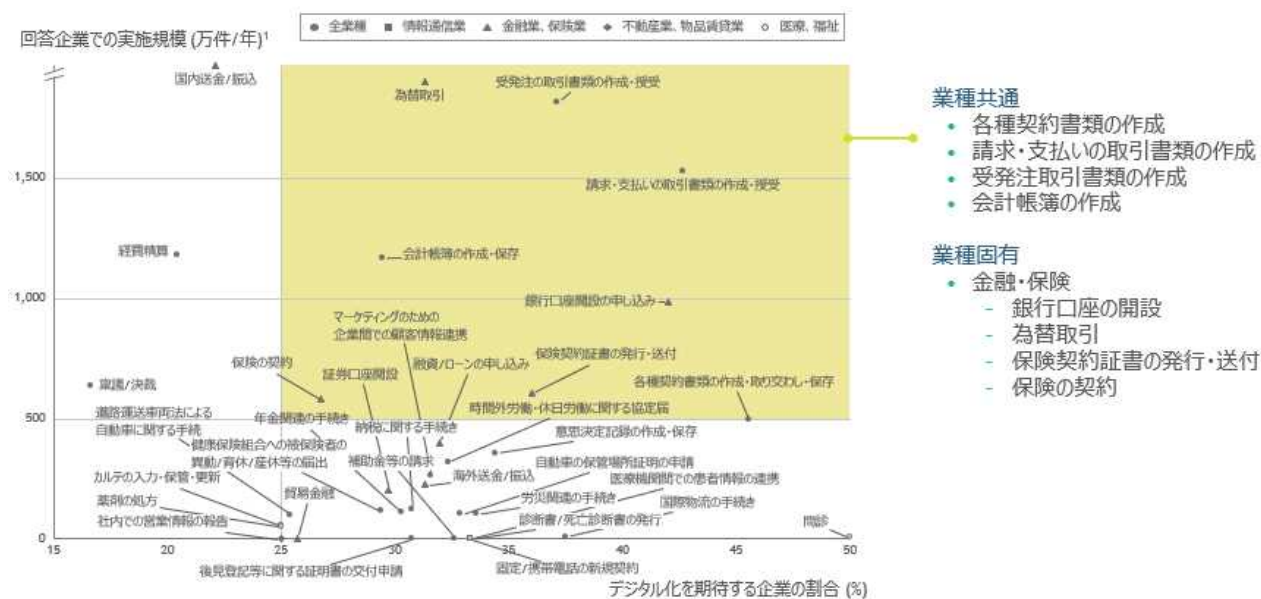


ここからは具体的な手続き等ごとにトラストサービスへのニーズを分析していく。まず行政が所管する未デジタル化の手続き等に関して分析を行う。本セグメントに分類される手続き等は、「法律で定められた文書・帳簿・台帳等の作成・保存」(34%)、「保険料口座振替納付(変更)申出書」(30%)、「自動車の保管場所標章の交付」(18%)でデジタル化の要望を確認することができた。また、デジタル化に対して積極的ではない層もデジタル化に否定的なわけではなく、デジタル化によるマイナスの感情は少ないことが推察される。

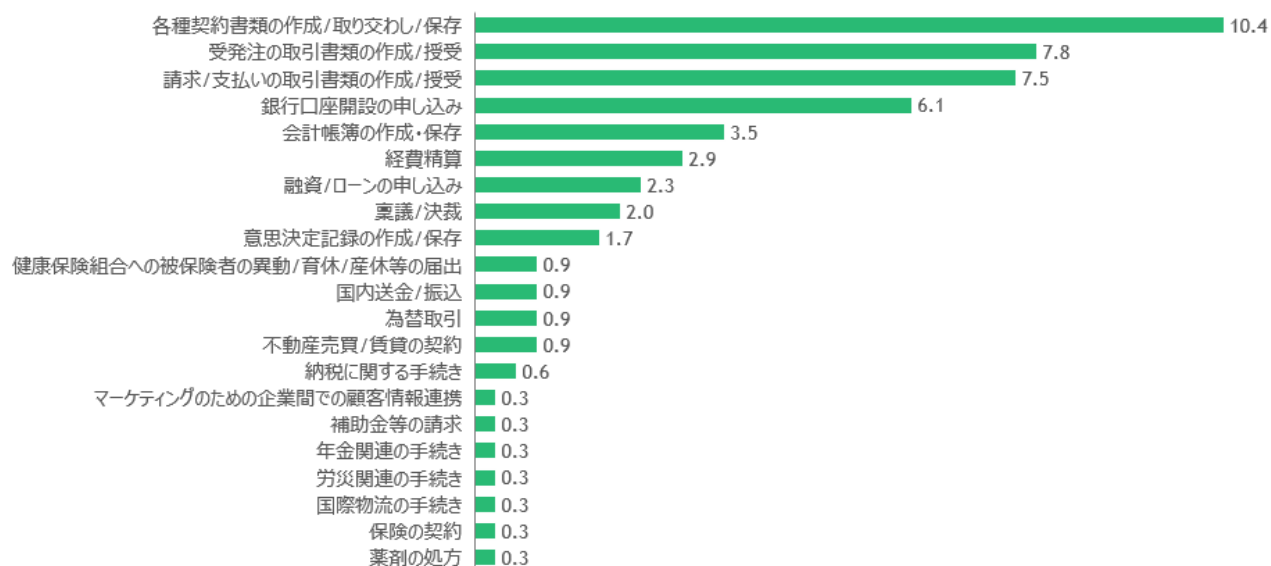
- 労働基準監督署提出物関係
- 保健所提出物関係書類
- 商業登記(株主リスト/個人証明書)
- 外為法上の本人確認記録/個人データ管理台帳/取引時確認記録
- 犯罪収益移転防止法上の本人確認の記録
- 銀行取引開始時に顧客から徴収する本人確認書類
- 医薬品・医療機器等の台帳
- 医薬品・医療機器等の台帳、品質文書の管理台帳、要員の教育記録
- 医薬品GMP関連書類
- 施工体制台帳等



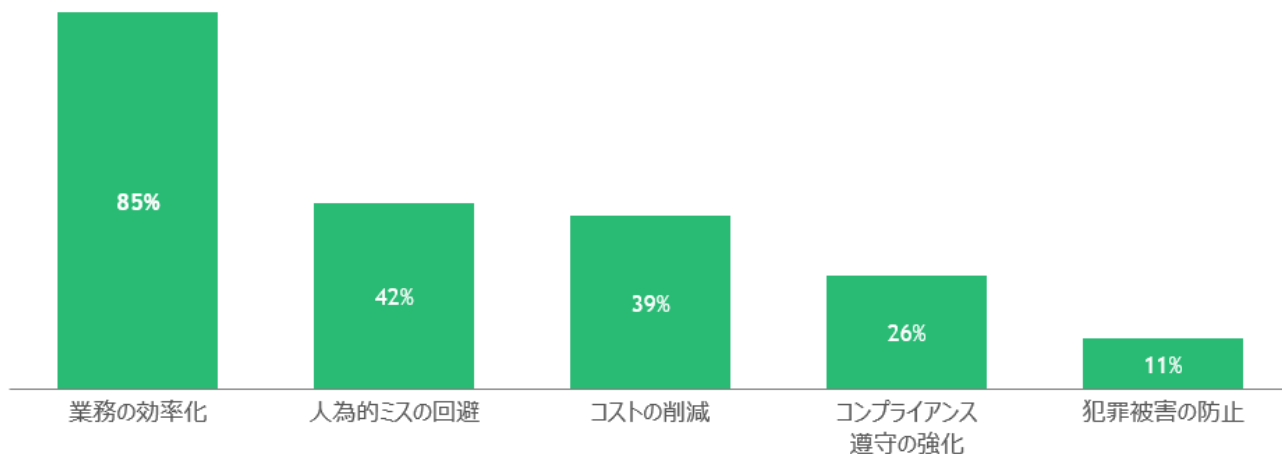
次にデジタル化はされているものの、デジタル化率がそれほど高くない手続きを対象として手続き回数を縦軸、トラスト確保時のデジタル/オンライン利用のニーズを横軸に取った散布図を作成した。この図では、右上の黄色く色づけたセグメントが手続きの実施規模が大きく、同時にデジタル化のニーズも高い手続き等が含まれており、より優先してデジタル化していくべき手続き等に分類できる。具体的には、業種共通の手続きである「各種契約書類の作成」「請求・支払いの取引書類の作成」と、金融・保険の手続きである「銀行口座開設」「為替取引」等が含まれている。



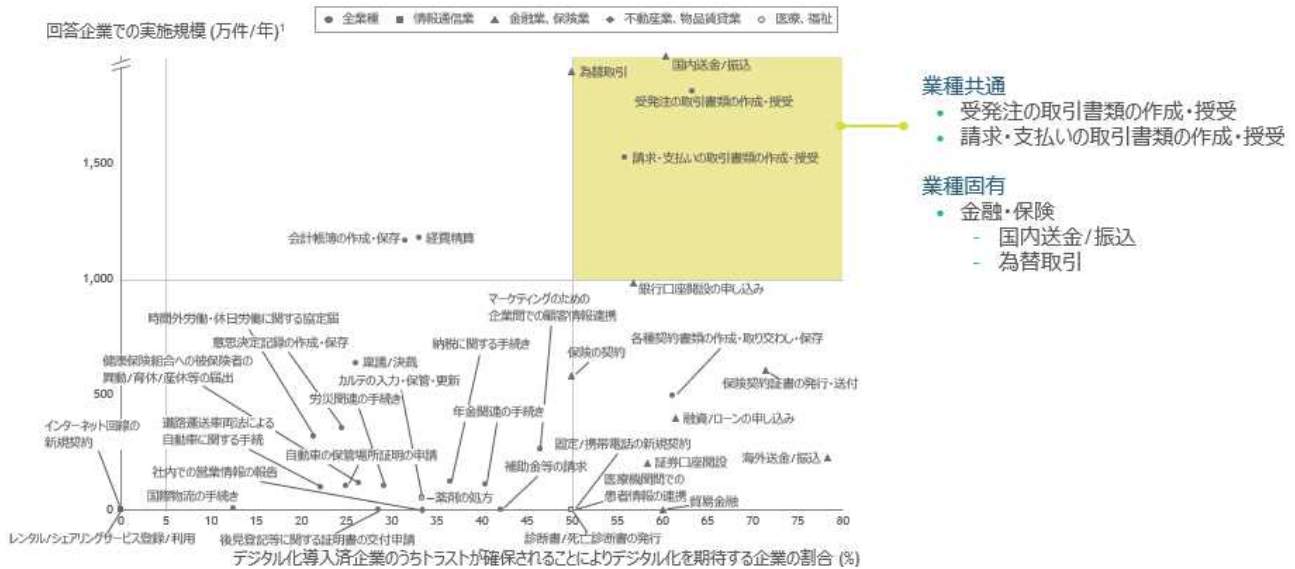
また、これらの手続きに関して、トラスト確保「有り」の場合と「無し」の場合の差分を取り、トラスト確保によってよりデジタル化ニーズが大きくなる手続き等を分析した。結果として、特に「契約書類」「受発注取引書類」「請求・支払い書類」等が特にトラスト確保によってデジタル化ニーズが大きくなる手続きであると言える。



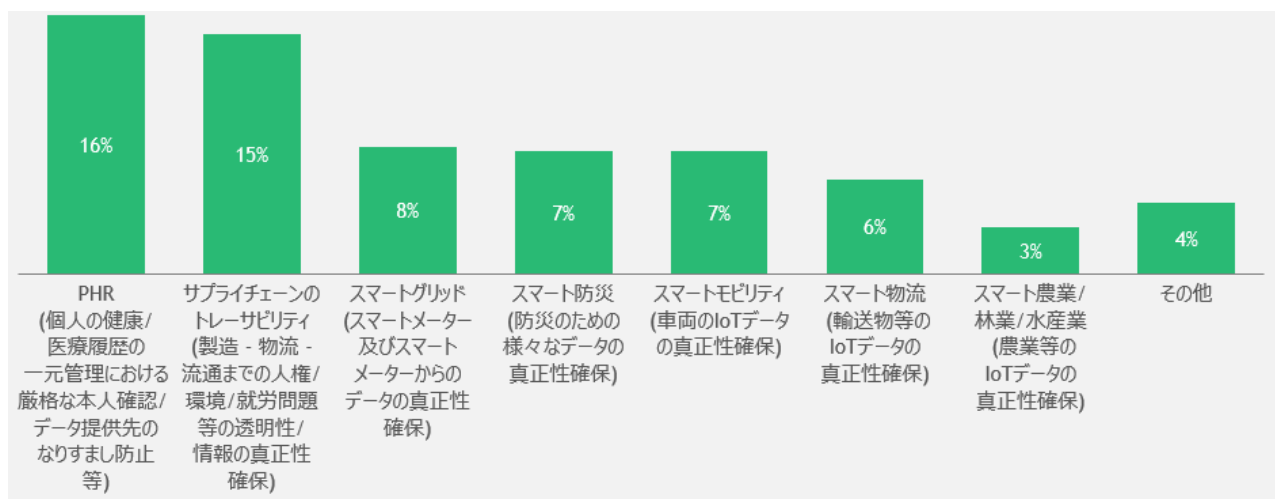
さらに、これまで見てきたようにトラスト確保によるデジタル化が見られる手続き等は数多く存在するが、その中でも最もデジタル化を期待する手続き等に関して、デジタル化による期待効果としては、「業務効率化」(85%)、「人為的ミス回避」(42%)、「コスト削減」(39%)、「コンプライアンス遵守の強化」(26%)、「犯罪被害の防止」(11%)となった。特に業務効率化が大きなメリットとなっているが、全効果に関して期待が集まっていることが分かった。



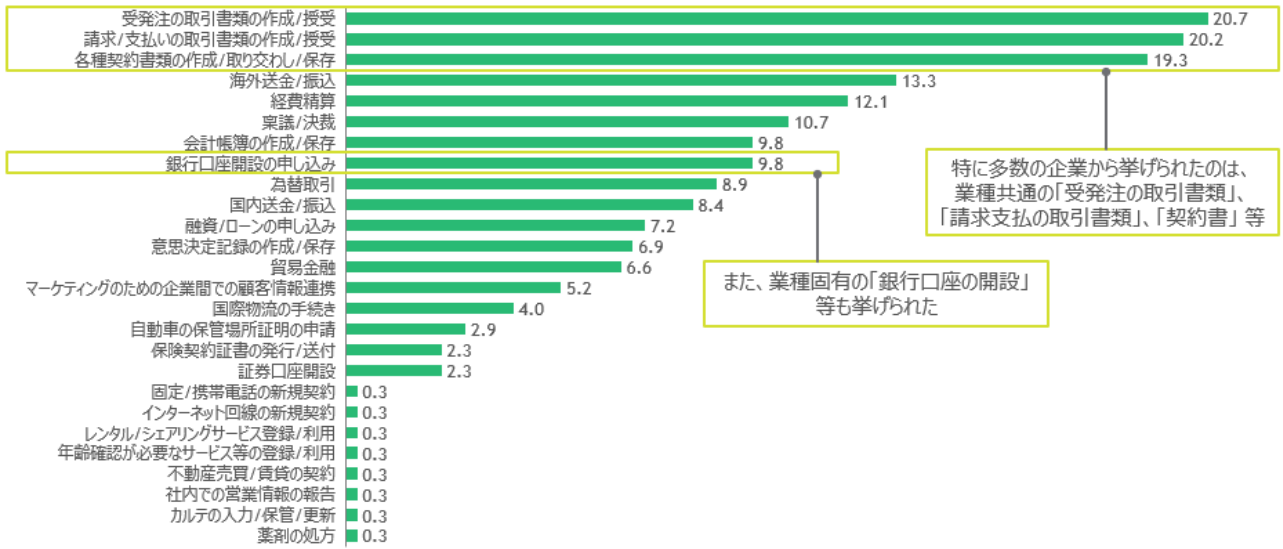
また同様に、デジタル化はされているものの、デジタル化率がそれほど高くない手続き等をデジタルにて実施している企業の手続き等を対象として手続き回数を縦軸、トラスト確保時のデジタル/オンライン利用のニーズを横軸に取った散布図を作成した。この図では、右上の黄色く色づけたセグメントが手続きの実施規模が大きく、同時にトラスト確保時のニーズも高い手続き等が含まれており、より優先してトラストを確保すべき手続き等に分類できる。具体的には、業種共通の手続きである「受発注取引書類」「請求・支払いの取引書類の作成」等や、金融・保険の手続きである「国内送金/振込」「為替取引」が挙げられた。



最後に、現在実現されていないものの、トラストの確保によって今後実現される可能性のあるサービスについても分析を行った。「パーソナルヘルスレコード」(16%)、「サプライチェーンのトレーサビリティ」(15%) 等のニーズが確認された。



さらに、企業が行う民間手続き等のうち、海外との取引等があり、相手先の本人確認や情報改ざん防止が必要なものとしては、業種共通の「受発注の取引書類」、「請求支払の取引書類」、「契約書」等が多く挙げられた。



3 既存トラスト基盤の現状と課題

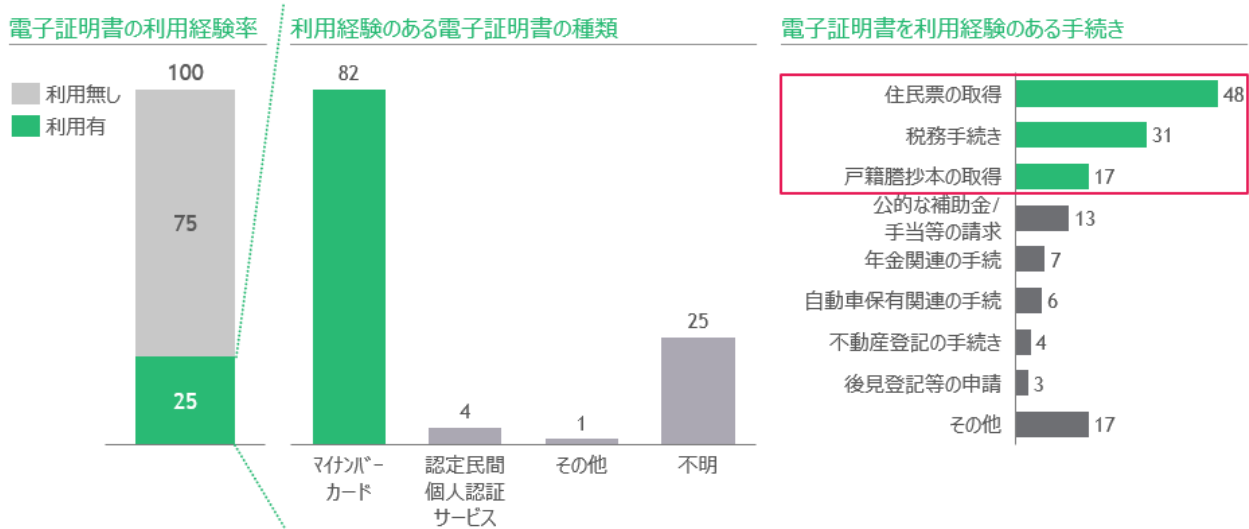
サマリ

まず個人に関しては、現状では電子証明書の利用率は25%に留まり、利用している電子証明書の種類や利用したことのある手続きは限られている。さらに電子証明書を利用した際の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%) 等が多く挙げられる一方、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。

企業に関しても同様にトラストサービスの利用は限定的で、「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%である。さらにトラストサービスの課題は、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。

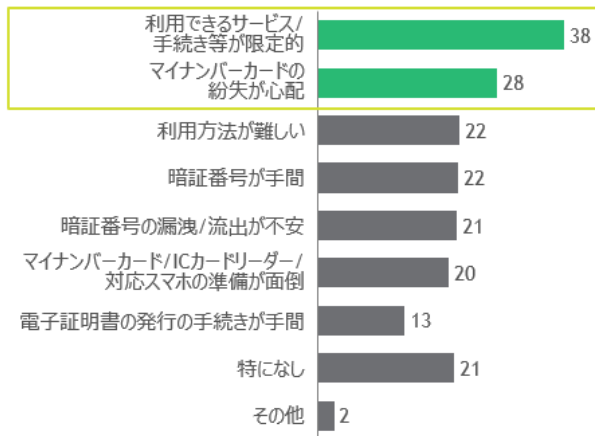
個人におけるトラスト基盤の現状と課題

現状では、個人における電子証明書の利用率は25%に留まり、利用している電子証明書の種類や利用したことのある手続きは限定的である。利用経験のある電子証明書はマイナンバーカードが82%で、他の電子証明書の利用経験を圧倒している。電子証明書を利用経験のある手続きに関しては、「住民票の取得」や「税務手続き」等に集中しており、いずれも電子証明書が一部の限られたケースのみでしか利用されていないことを示している。

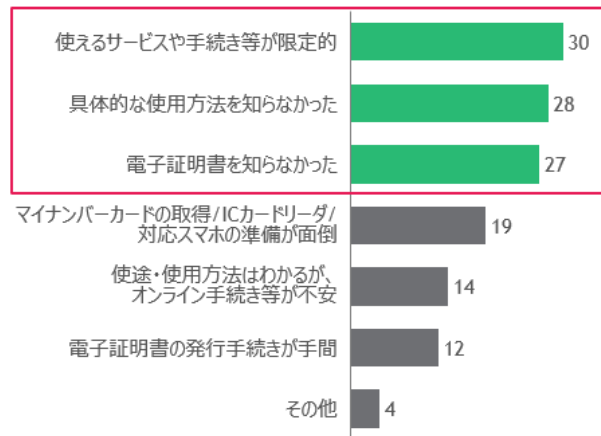


また、電子証明書を利用した際の課題は電子証明書の利用経験者・利用未経験者で異なる。利用経験者/未経験者共に「利用できるサービスが限定的」であることを多く挙げたのに加えて、利用経験者からは「マイナンバーカードの紛失が心配」、利用未経験者からは「認知はしているが使い方を知らない」等が多く挙げられた。

電子証明書の課題 (利用経験者)

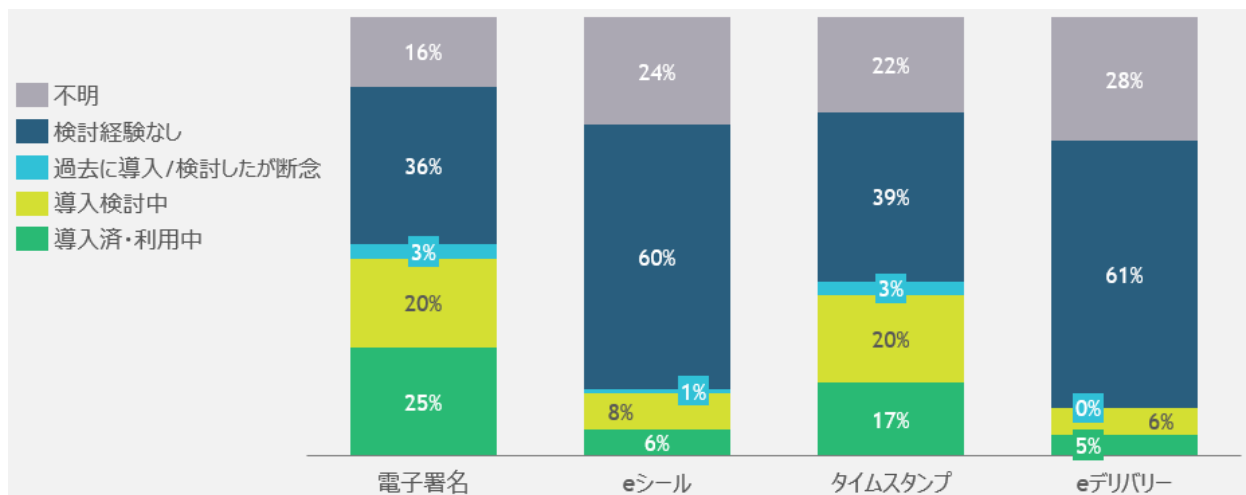


電子証明書の課題 (利用未経験者)



企業におけるトラスト基盤の現状と課題

一方で、企業ではトラストサービスの利用率は、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%であり、いずれも限定的な利用率に留まっている。



また現状のトラストサービスの課題は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。トラストサービス間を比較すると、e シールと e デリバリーは認知度が低いことが大きな課題として見受けられ、利用率が 5%しかないことに大きく影響していると考えられる。

		電子署名	eシール	タイムスタンプ	eデリバリー	
導入済み/ 検討経験あり ・ 検討したが 断念 ・ 検討中 ・ 導入済	法的効力 (証拠能力)の 担保不足	法的効力(証拠能力)の担保不足	-	8	9	5
		国際的な有効性(法的効力)の担保不足	14	5	6	3
	企業間での 共通化の難しさ	業界内の他社と足並みが揃えられない/相手先などが導入しない	24	6	10	5
		他業界の他社と足並みが揃えられない/相手先などが導入しない	21	7	9	3
	事業者/ サービス 選定の難しさ	トラストサービス事業者の選定が困難	14	5	9	3
		適切な方式/トラストサービス選定が困難	12	4	7	2
		サービスの継続性/永続性が不安	16	5	11	3
	導入/ 利用コスト	サービス導入時のコスト	18	4	11	4
		サービス利用時のコスト	15	5	13	4
	利用の手間	効力が切れる前に更新するための工数	11	3	5	2
デジタル化の検討・実施のための工数/人的リソース不足		18	4	10	1	
その他	その他	3	1	3	2	
検討経験なし	認知/ 理解不足	知らなかった/よく知らなかった	9	39	20	48
		知っていたが、これまで必要性を感じたことがなかった	25	19	17	11
	その他	その他	3	3	2	3

また、中小企業を対象とすると課題のほとんどが認知/理解不足であり、ほとんどが検討を行う前の段階にあることがわかる。さらにトラストサービスを導入済みか導入検討を行ったことがある企業を対象を絞ると、全体とは異なり法的効力(証拠能力)の担保も大きな課題の1つに数えられ、また企業間の共通化やコストの課題もより多くの割合の企業が課題だと感じていることがわかった。

		電子署名	eシール	タイムスタンプ	eデリバリー	
導入済み/ 検討経験あり ・ 検討したが 断念 ・ 検討中 ・ 導入済	法的効力 (証拠能力)の 担保不足	法的効力(証拠能力)の担保不足	-	5	4	3
		国際的な有効性(証拠能力)の担保不足	12	4	4	3
	企業間での 共通化の難しさ	業界内の他社と足並みが揃えられない/相手先などが導入しない	13	4	5	4
		他業界の他社と足並みが揃えられない/相手先などが導入しない	12	4	4	3
	事業者/ サービス 選定の難しさ	トラストサービス事業者の選定が困難	8	3	6	3
		適切な方式/トラストサービス選定が困難	8	3	4	2
		サービスの継続性/永続性が不安	9	4	6	2
	導入/ 利用コスト	サービス導入時のコスト	16	4	9	3
		サービス利用時のコスト	10	3	9	3
	利用の手間	効力が切れる前に更新するための工数	8	3	3	2
デジタル化の検討・実施のための工数/人的リソース不足		12	2	4	1	
その他	その他	4	0	1	2	
検討経験なし	認知/ 理解不足	知らなかった/よく知らなかった	11	51	35	59
		知っていたが、これまで必要性を感じたことがなかった	38	20	23	11
	その他	その他	4	3	3	3

Note: 中小企業を対象に分析
Source: 企業向けアンケート調査 (n=347, 2021/11/24~12/7実施)

		電子署名	eシール	タイムスタンプ	eデジパー	
導入済み/ 検討経験あり ・ 検討したが 断念 ・ 検討中 ・ 導入済	法的効力 (証拠能力)の 担保不足	法的効力 (証拠能力)の担保不足	-	51	22	47
		国際的な有効性(法的効力)の担保不足	29	32	16	32
	企業間での 共通化の難しさ	業界内の他社と足並みが揃えられない/相手先などが導入しない	50	42	26	42
		他業界の他社と足並みが揃えられない/相手先などが導入しない	43	43	23	26
	事業者/サービス 選定の難しさ	トラストサービス事業者の選定が困難	30	32	23	26
		適切な方式/トラストサービス選定が困難	26	28	17	21
		サービスの継続性/永続性が不安	34	32	27	26
	導入/利用コスト	サービス導入時のコスト	37	26	28	37
		サービス利用時のコスト	32	32	33	34
	利用の手間	効力が切れる前に更新するための工数	23	23	13	18
		デジタル化の検討・実施のための工数/人的リソース不足	37	26	25	11
	その他	その他	7	4	7	16

4 トラスト基盤普及に向けた課題解決の方策 (案)

サマリ

個人アンケートの結果を踏まえ、個人へのトラストサービス (電子証明書) の普及に向けて、最も優先度高く必要と考えられる方策は、「利用可能なユースケースの拡大」と「認知・理解促進のための (一層の) 啓発活動」である。

「利用可能なユースケースの拡大」に関しては、電子証明書の課題として、利用経験の有無を問わず「利用できる場面の少なさ」が最多 (経験者の 4 割/未経験者の 3 割) であった。また、「あれば利用したい」ものとしても、「オンラインで完結できないものができるようになる」(60%) が同率 1 位で、「民間サービスでの利用場面が増える」(59%)、「オンラインで完結できるものに導入される」(57%) も過半数から挙げられた。

「認知・理解促進のための (一層の) 啓発活動」に関しては、電子証明書の課題として、利用未経験者では「知らなかった」「利用の仕方がわからない」が上記に続き多く(各約 30%)、「あれば利用したい」ものとして、「メリットや利用方法、安全性等について、わかりやすく教えてくれる」(60%) が、上記と同率 1 位であった。

一方、「モバイル ID 方式」「生体 ID 方式」等、現行のマイナンバーカードを利用する方式の見直し/UX 改善も、今後検討が必要な領域である。電子証明書の課題として、利用未経験者では「マイナンバーカード取得や IC カードリーダー/対応スマホ準備の手間/コスト」(約 20%) がユースケースの拡大と認知の拡大に続く課題として挙げられ、利用経験者からは「マイナンバーカード紛失の心配」「暗証番号/パスワードの手間」等 (各約 20%) が挙げられ、大きな課題の 1 つと言える。「モバイル ID 方式」については既に総務省推進中ではある一方、「生体 ID 方式」も実現の可否/是非を含めて今後検討が必要になる可能性がある。

企業へのトラストサービスの普及に向けては、企業アンケート結果と、個人への普及促進のためのユースケース拡大の観点も踏まえ、企業の声として、「あれば導入を前向きに検討したい」有効な施策との回答が多かった「業界ごとの標準化団体設置/ガイドライン策定」や「電子署名以外のトラストサービスの法的効力 (証拠能力) の担保」が優先度高く必要と考えられる方策である。さらに、アンケートの対象を「トラストサービスを導入済み/検討経験あり」の企業に絞った場合には「国際的な相互認証/海外での効力 (証拠能力) の担保」や「用途ごとの必要アシユアランスレベルの明確化」が重要な方策として多く挙げられており、こちらも併せて優先度高く検討すべき方策となっている。最後に、企業間でのトラストサービスの共通化を考えた際、業界内と業界横断の共通化を比較すると、有効な施策・現状の課題いずれもアンケート対象が全体の場合は「業界内」の方が多いものの、「トラストサービスを導入済み/検討経験あり」の企業は「業界横断」の共通化を重要な施策として挙げており、業界ごと/業界間のどちらがより有効なアプローチであるか検討していく必要がある。

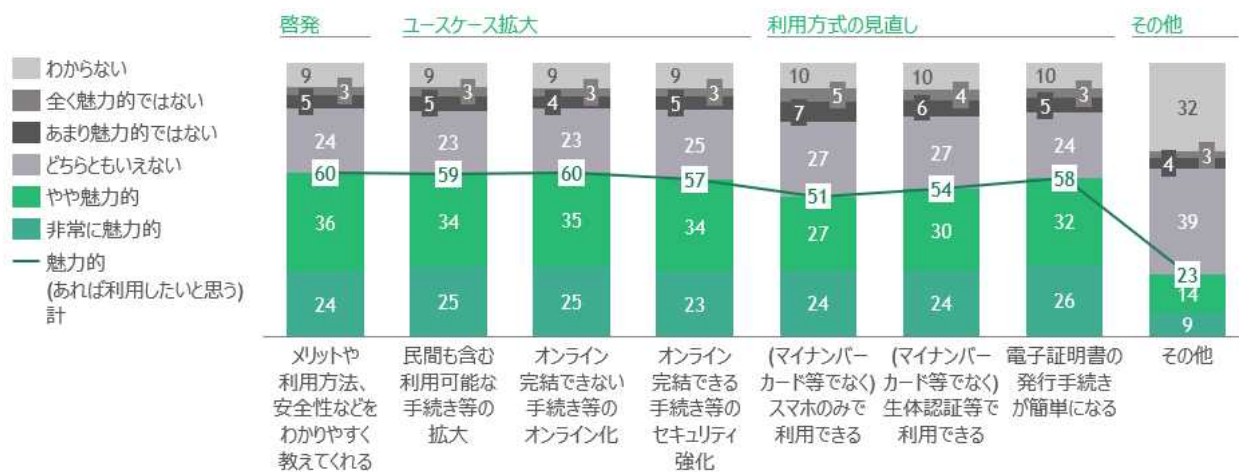
また、アンケートでは有効な方策として比較的多くは挙げられなかったが、個人への普及に向けたユースケース拡大や、課題解決の方策の有効性検証の観点からは必要と考えられる。

なお、「低コストで導入可能な方法の確立」も、「あれば導入を前向きに検討したい」有効な施策として挙げられたが、実現可否・是非は慎重に精査する必要がある。

個人に向けた課題解決の方策

個人に対しての「あれば、電子証明書の利用を検討したい」方策としては、「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の認知拡大」(60%)、「マイナンバーカードを取得した後の、電子証明書の発行手続きが簡単になる」(58%) 等が特に多く挙げられた。いずれの方策も同様に高い

割合が魅力的であるとの回答を行っているが、セグメント別に見ると「啓発」と「ユースケース拡大」のセグメントの方策がより支持を集めており、優先して取り組むべき方策である可能性が高い。

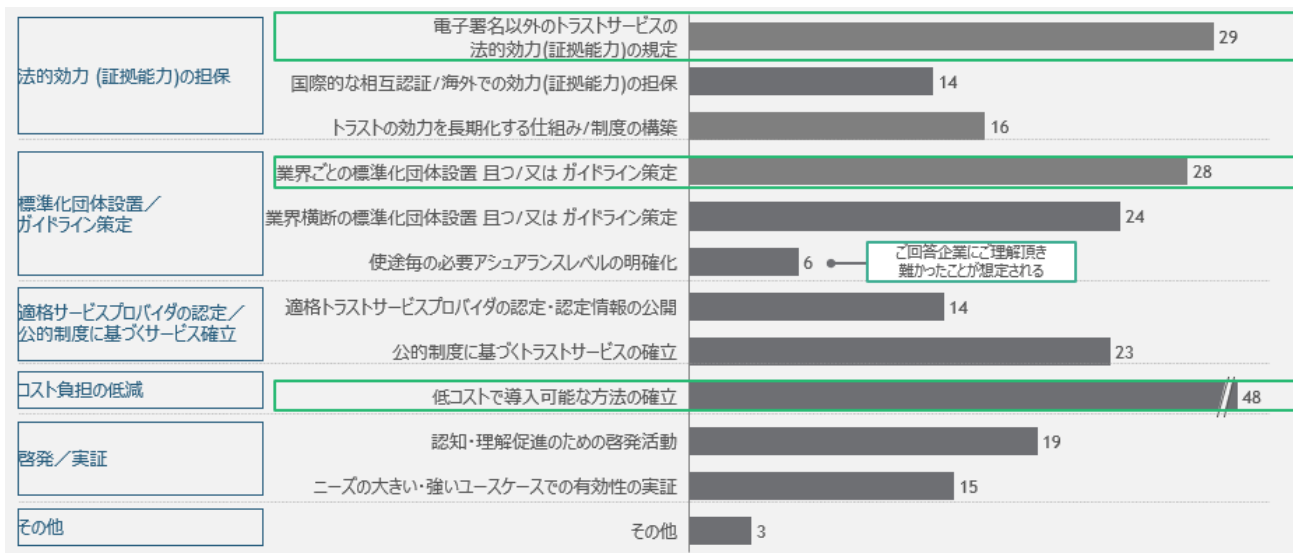


最後に、個人の感じるトラストサービスの課題と、その課題解決のための方策を整理した。課題は「利用だけのメリットがない/使えるものが限られている」「利用の仕方がわからない」「知らなかった」、施策例は「認知・理解促進のための啓発活動 (メリットや利用方法、安全性等をわかりやすく教えてくれる)」「オンライン完結できない手続き等のオンライン化」「民間も含む利用可能なサービス/手続き等の拡大」が、それぞれトップ3に入っていることがわかる。

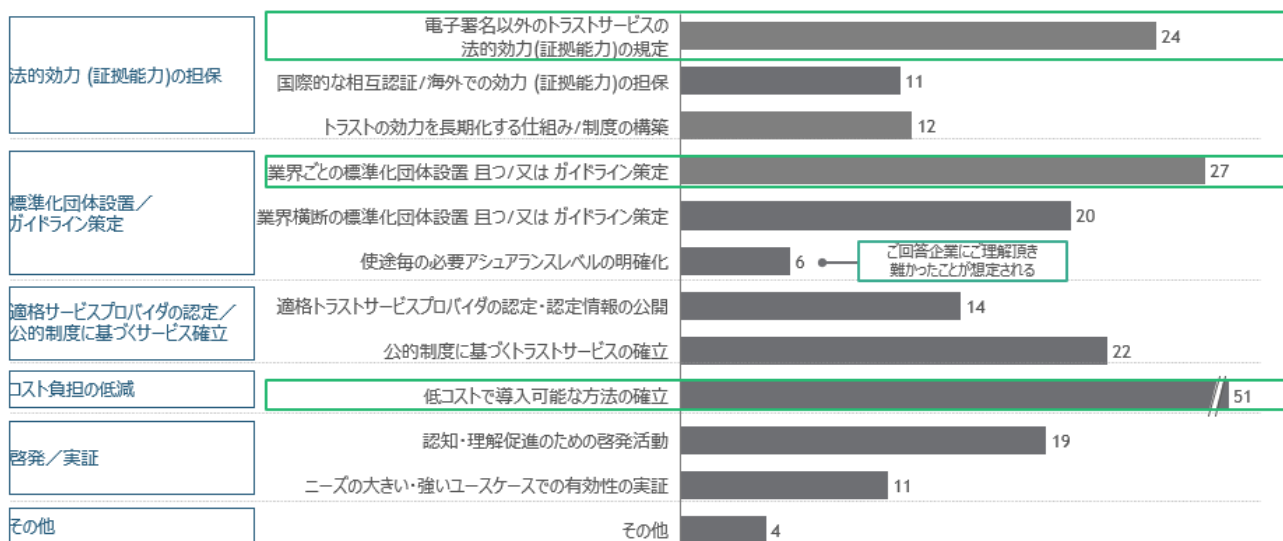


企業に向けた課題解決の方策

企業に対してのトラストサービスの課題を解決するために有効な方策としては、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 かつ/またはガイドライン策定」(28%) が特に多く挙げられ、優先して取り組むべき方策である可能性が高い。また、これは対象を中小企業に限定しても、それほど大きな傾向の差はみられない。



この回答企業にご理解頂き
難かったことが想定される



この回答企業にご理解頂き
難かったことが想定される

また、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に限定すると、「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、一定トラストサービスへの理解が進むと別の課題が大きくなる傾向が見取れる。

法的効力 (証拠能力)の担保	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	15
	国際的な相互認証/海外での効力(証拠能力)の担保	39
標準化団体設置/ ガイドライン策定	トラストの効力を長期化する仕組み/制度の構築	20
	業界ごとの標準化団体設置 目次/又は ガイドライン策定	23
	業界横断の標準化団体設置 目次/又は ガイドライン策定	31
適格サービスプロバイダの認定/ 公的制度に基づくサービス確立	使途毎の必要アシュアランスレベルの明確化	33
	適格トラストサービスプロバイダの認定・認定情報の公開	9
コスト負担の低減	公的制度に基づくトラストサービスの確立	21
	低コストで導入可能な方法の確立	29
啓発/実証	認知・理解促進のための啓発活動	25
	ニーズの大きい・強いユースケースでの有効性の実証	20
その他	その他	2

また、以下にここまでの分析の結果明らかとなった企業の感じるトラストサービスの課題と、その課題解決のための方策を整理している。対象を中小企業のみに限定した場合でも、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への関心の傾向は大きく変わってはいない。



○：電子署名 ○：eメール ○：タイムスタンプ ○：eデリバリ

利用状況 トラストサービスへの課題意識



すでにトラストサービスを導入済みの企業に限定すると、法的効力(証拠能力)の担保不足や、企業間での共通化の難しさが大きな課題となっている。また課題解決の方策としても、「国際的な相互認証/海外での効力の担保(証拠能力)」や「用途ごとの必要アシュアランスレベルの明確化」等が重要な方策となっている。

○：電子署名 ○：eメール ○：タイムスタンプ ○：eデリバリ

利用状況 トラストサービスへの課題意識



5 トラスト基盤の整備・普及による期待効果

サマリ

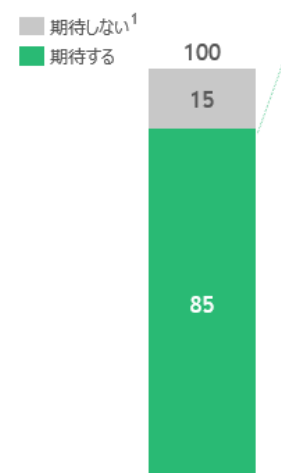
トラスト確保により、自社のデジタル化が進展することを期待する企業は 85%存在し、中でも「不動産売買/賃貸の契約」、「銀行口座開設の申し込み」、「取引書類の作成」等のデジタル化への期待が大きい。トラスト確保によるデジタル化の進展がもたらす効果として期待されるものとして、企業からは、「業務量削減」の他、「人為的ミスの回避」「コストの削減」「詐欺等の犯罪被害防止」「コンプライアンス遵守の強化」等が挙げられている。

なお、これらの期待効果のうち、「業務量削減」と「詐欺等の犯罪被害防止」については効果の概算想定規模を算出しており、「業務量削減」では~100 億時間 (600 万人相当)、「詐欺等の犯罪被害防止」では 100 億円規模の効果が見込まれている。

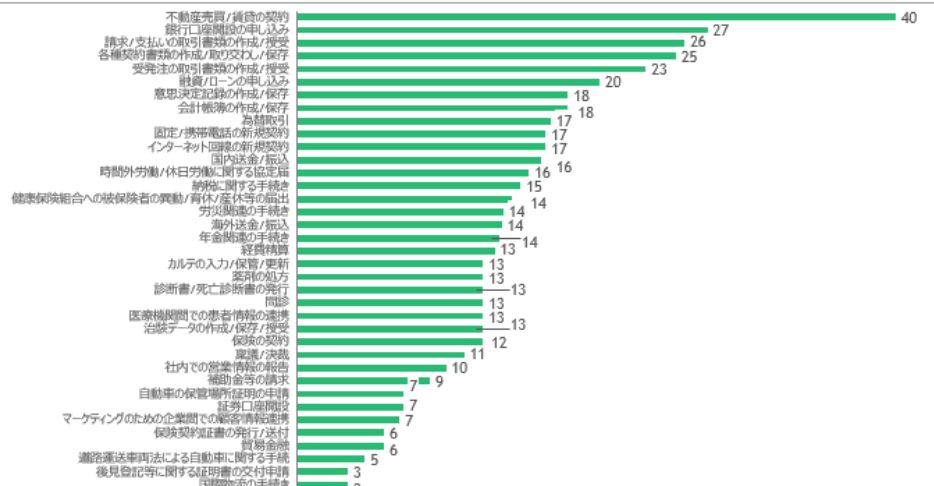
トラスト基盤の整備・普及によって期待される効果

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、ニーズのある手続き等に関しては、概ね 10~25%がデジタル化を期待しており、多くの企業・手続き等のデジタル化が期待されていることが確認された。

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



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。最も多くの期待を集めた効果は「業務量削減」であり、48%もの企業が業務量削減効果を期待している。一方、「詐欺等の犯罪防止」の効果に関しては比較的小さい割合である 6%の企業のみが期待している効果であるが、特に秘匿情報を扱って、金額の大きな取引を行う金融・保険業界や不動産業界に集中して期待効果として挙げられていた。



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が明確にしやすい" (医療)

14%
(347社中の31社)¹



詐欺等の犯罪防止

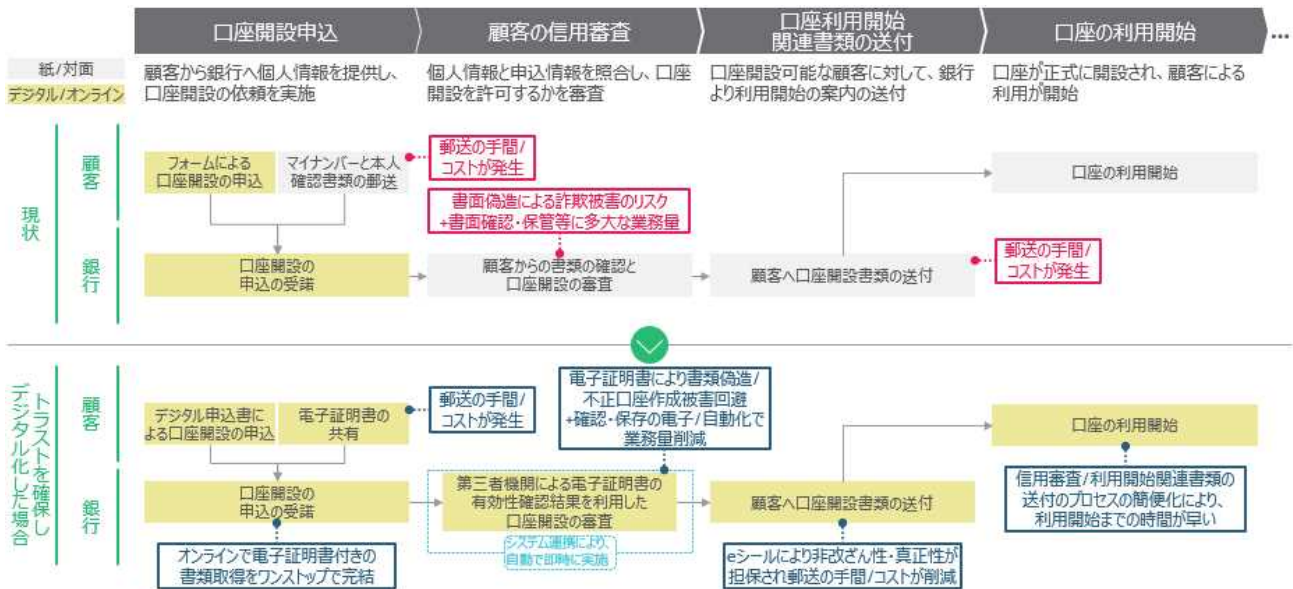
"業界では「地面師」等の詐欺被害が発生した例もあり、書類の改ざん/偽造の防止は重要課題" (不動産)

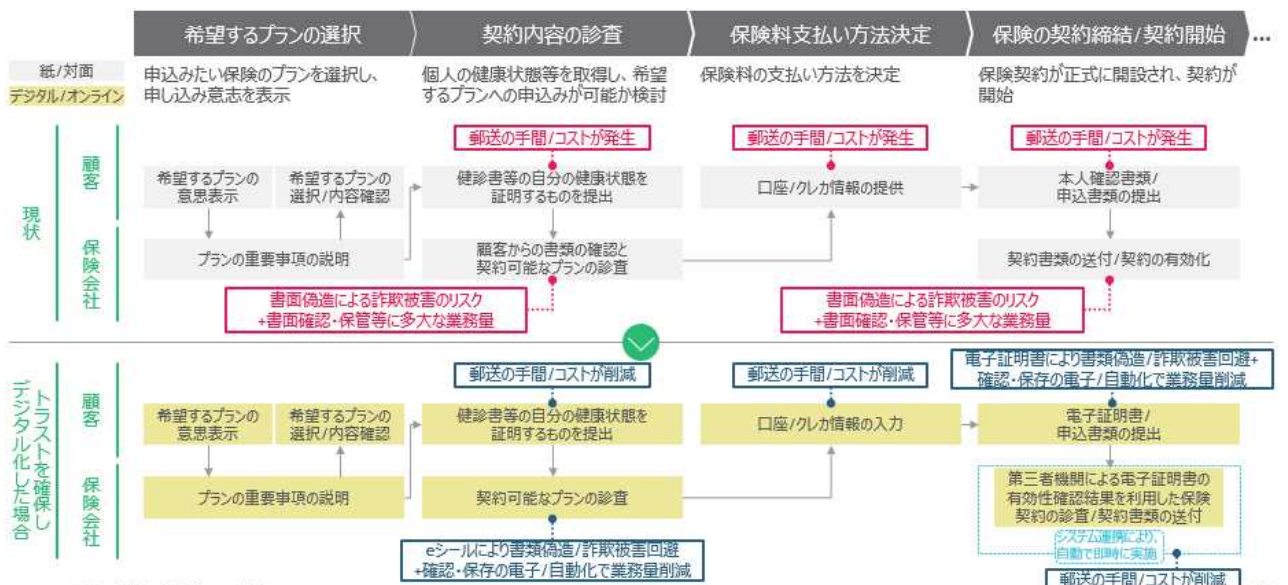
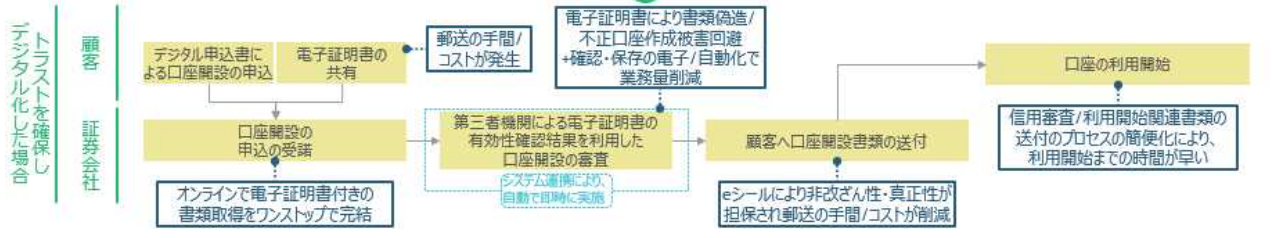
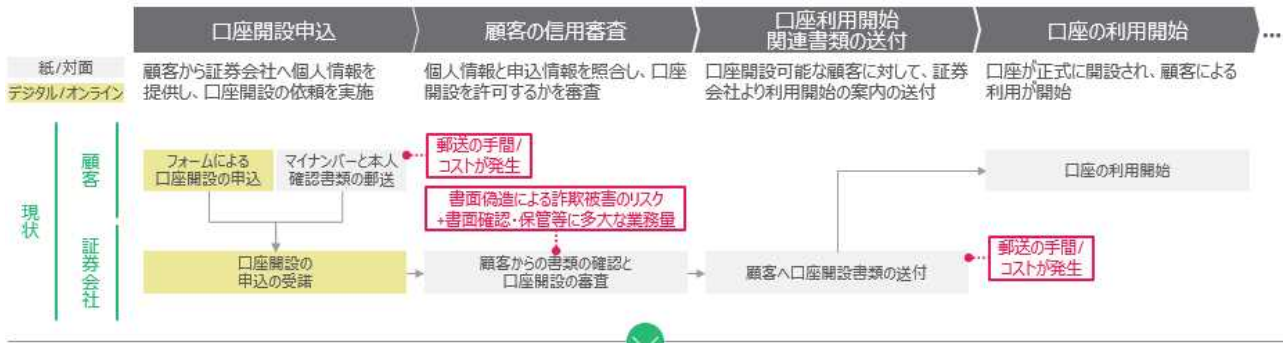
"融資/ローンの申し込みでは顧客の不正申告が考えられ、双方を防ぐことができる" (金融)

6%
(347社中の10社)¹

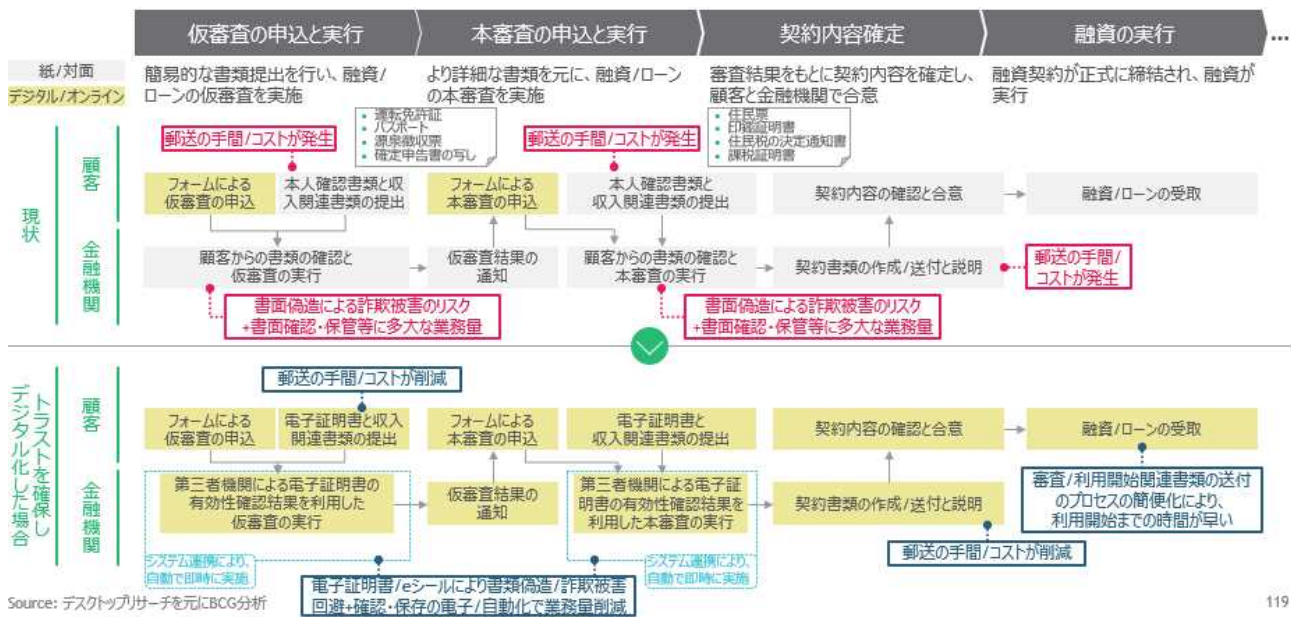
トラスト基盤の整備・普及によって期待される効果の具体例

トラスト基盤が整備・導入されることによって、多くの手続き等のフローが変化し、デジタル/オンライン化がなされることが期待される。デジタル/オンライン化の前後を比較すると、様々な手続き等にて全く同様の効果が見込まれることがわかる。以下に示したのはデジタル/オンライン化ニーズの大きな手続きである「銀行口座の新規開設」「証券口座の新規開設」「保険の契約」「融資/ローンの契約」のデジタル/オンライン化前後の手続きフローの変化を比較したものであるが、いずれの手続きにおいても申込→審査→契約の確認→サービスの開始のフローを辿っており、いずれにおいても企業の「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ことがわかる。





Source: デスクトップリサーチを元にBCG分析



119

トラスト基盤の整備・普及によって期待される効果概算

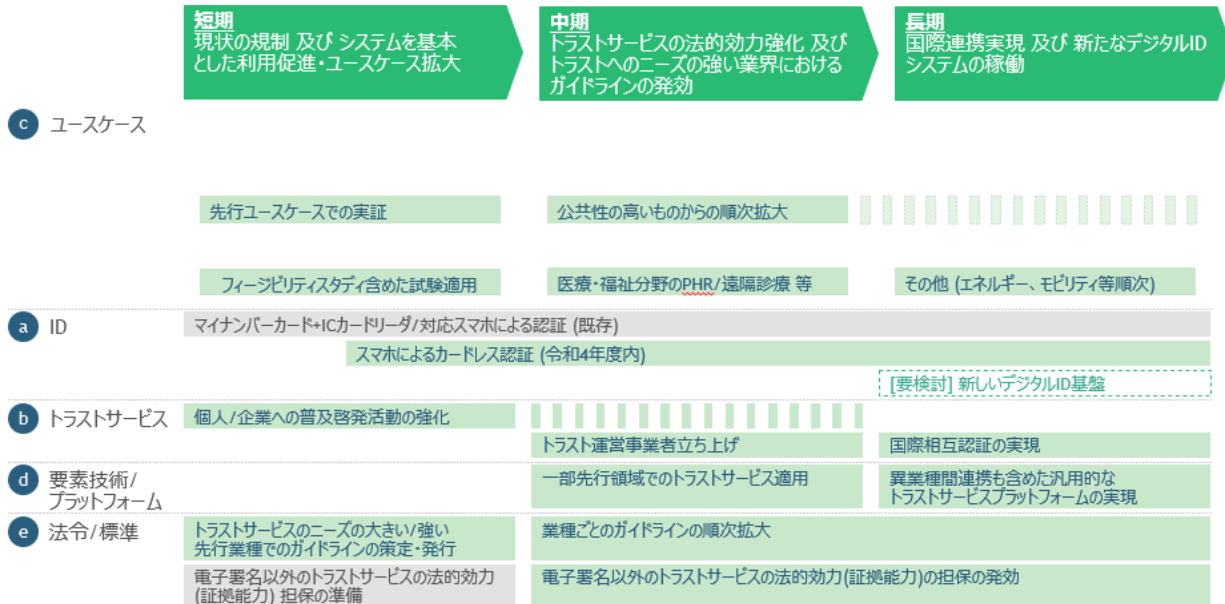
本調査では、トラスト基盤の整備・普及によって期待される効果のうち定量化して効果を算出することが容易な「業務量削減」と「詐欺等の犯罪防止」の期待効果を算出した。それぞれ、現状の規模×トラスト確保による削減率によって、トラスト確保による削減効果を算出した

まず「業務量削減」に関しては、トラスト確保によりデジタル化される企業では、業務量削減が進展するとの前提から効果が期待されるとし、「詐欺等の犯罪防止」に関しては、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との前提から効果を算出した。具体的な算出の式は以下ようになり、「業務量削減」は約 100 億時間規模/年、「詐欺等の犯罪防止」は 100 億円規模/年の効果が期待される。

考え方		期待効果の規模 (概算/粗試算)	
		現状の規模	\times 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)
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を仮置)
			業務時間の削減/効率化 年100億時間規模 詐欺被害額の減少 年100億円規模

6 今後のロードマップ (案)

今後のロードマップとしては、個人及び企業へのトラスト基盤の普及に向けて、新たなトラスト基盤や法制度の整備には時間を要することを鑑み、短期的に実現可能なものから、大きく3ステップでの推進を想定する。



7 個別取組の案

7.1 優先的に取り組むユースケース (案)

サマリ

トラストサービスの普及・拡大において、ユースケースの拡大/実証は、①個人の電子証明書の利用促進に向けたメリット増大、②企業のトラストサービス導入促進に向けたメリットの実証、③課題解決の方策の有効性検証の3つの観点から必要である。ユースケースの拡大/実証のために、直近で優先的に取り組むものとしては、実現性/有効性と魅力度/期待効果の大きさの観点から、以下を選考基準として考慮した。

- 実現性/有効性 (必要条件):
 - 個人/企業から、大きい/強いニーズがある
 - トラストサービス導入以外の課題がなく、既にデジタル化を検討/推進中の未デジタル化のものではない
- 魅力度/期待効果の大きさ (優先条件):
 - ニーズの強さ
 - ◇ 企業で、トラスト確保とデジタル化のニーズが、より大きく/強く、より広く企業のトラストサービス導入促進/実証協力が期待できる
 - ◇ 個人で、トラスト確保のニーズが、より大きく/強く、より多くの個人のトラストサービス利用促進が期待できる
 - スケールの容易さ
 - ◇ 業界団体の力が強い、大手の寡占市場である等の理由で展開が構造的にスケールしやすい



以上の選考基準を踏まえると、最も優先度高く取り組むユースケースは個人・企業の両社でトラスト確保のニーズが大きい「金融・保険」のB2C/Bの手続き等であり、具体的には「銀行/証券口座の開設」「融資/ローンの契約」「保険の契約」等。また次点で優先度高く取り組むユースケースは、必要条件である実現性/有効性に合致する、業種共通の手続き等や、行政が所管する民間手続き等である。具体的には、「法律で定められた帳簿/台帳/記録等の作成・保存」「健康診断結果や診断書の発行」「携帯/スマホの新規契約」等である。

取組内容としては、ユースケースごとの特性に応じ、対象手続き等の所管省庁や業界団体/企業への働きかけ・導入支援、具体的なユースケースにフォーカスした個人への普及啓発活動の強化、業界ごとの標準化団体設置/ガイドライン策定に向けた業界団体等への働きかけ・ガイドライン策定支援等が考えられる。

ユースケース拡大の目的と選定の条件

ユースケースの拡大/実証は「個人の利用促進に向けたメリット増大」「企業の導入促進に向けたメリット実証」「課題解決の方策の有効性検証」の3つが目的である。「個人の利用促進に向けたメリット増大」は、個人が電子証明書を利用しない主要因である「メリットの少なさ」を解消し、「企業の導入促進に向けたメリット実証」は企業がトラストサービスを導入しない主要因である「必要性を感じたことがないこと」を解消し、「課題解決の方策の有効性検証」は「個人に向けた普及啓発活動強化」「企業に向けたガイドライン策定」等の有効性の検証を実現することに対応している。

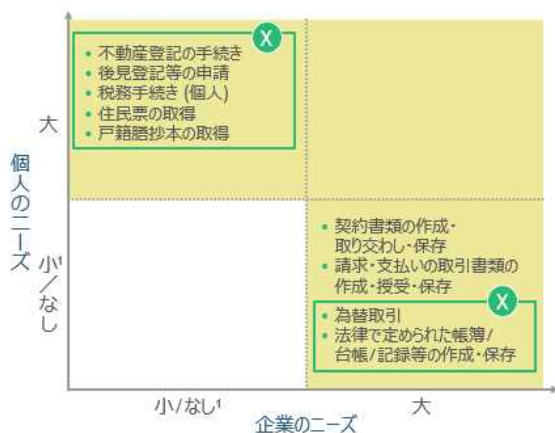
以上の目的の下、優先的に取り組むべきユースケースは、実現性/有効性と魅力度/期待効果の大きさの観点での選定が必要だと考えられる。

		 個人の利用促進に向けた メリット増大	 企業の導入促進に向けた メリット実証	 現状の課題の解決の方策の 有効性検証
A. 実現性/有効性 (必要条件)		個人または企業で、トラスト確保のニーズが比較的大きい/強い (アンケートより)		トラストサービス導入以外の課題がなく、かつ、既にデジタル化を検討/推進中の未デジタル化のものではなく、取組の早期実現性が見込め、有効性がある (アンケートより)
	B. 魅力度/ 期待効果の 大きさ (優先条件)	B-1 ニーズの強さ	トラスト確保のニーズがより大きく/強く、より多くの個人のトラストサービス利用促進が期待できる (アンケートより)	トラスト確保とデジタル化のニーズがより大きく/強く、より多くの企業のトラストサービス導入促進・実証協力が期待できる (アンケートより)
	B-2 スケールの容易さ	展開が構造的にスケールしやすい (業界団体の力が強い/大手の寡占が大きい等)		個人及び/又は企業へのトラストサービス普及に向けた主要な課題解決の方策の有効性をより多く検証できる (アンケートより)

ユースケース仮説と必要な課題解決の方策

先に挙げたように、優先度高く取り組むべきユースケースを必要条件である実現性/有効性が十分ある手続き等に関して、個人のニーズの大きさを縦軸、企業のニーズを横軸として各手続き等をマッピングした。この時、課題解決の方策として検証可能な方策として、B2B または企業内で完結する手続き等や企業が行うべき行政が所管する未デジタル化の手続き等は個人向けの利用可能なユースケースの拡大、認知・理解促進のための啓発活動ができないため、実現性/有効性に差分があるとして、考えられる課題解決の方策が単一か複数化で分けてマッピングしている。結果として、優先度高く取り組むべきユースケースは、個人・企業両社でトラスト確保のニーズが大きく、両者に向けた主要な課題解決の方策を検証可能な、「金融・保険」分野の B2C の手続きが有力である。

単一の主要な課題解決の方策を検証可能



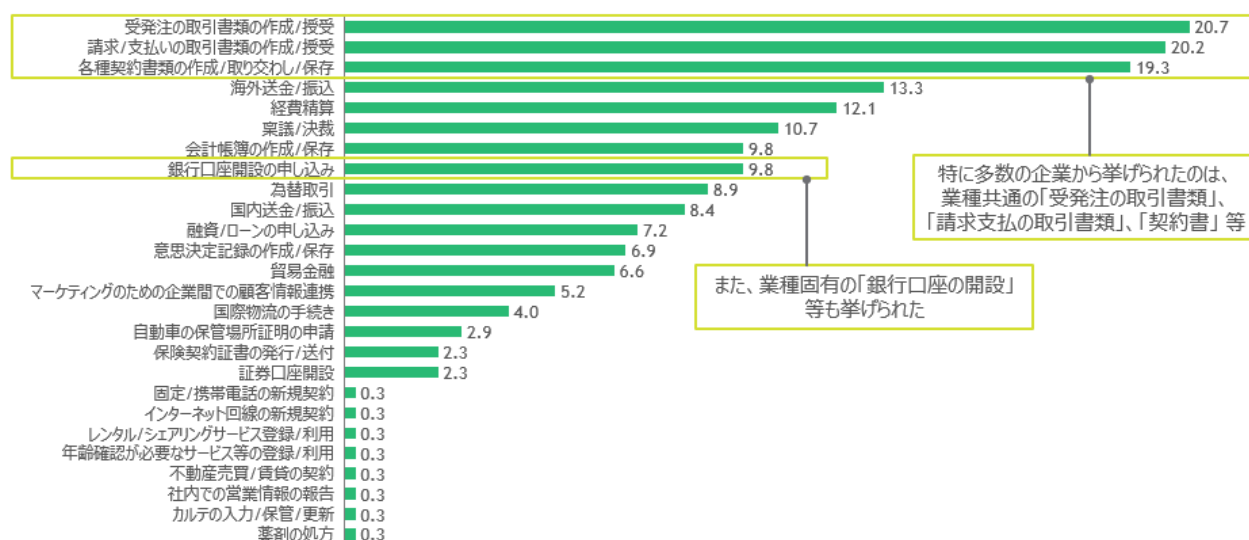
複数の主要な課題解決の方策を検証可能



7.2 海外連携を目指すトラスサービス (案)

企業が行う民間手続き等のうち、海外との取引等があり、相手先の本人確認や情報改ざん防止が必要なものとしては、企業アンケートにおいて幅広い手続き等が挙げられた。特に多数の企業から挙げられた手続き等は、業種共通の「受発注の取引書類」、「請求支払の取引書類」、「契約書」である。また、業種固有の「銀行口座の開設」や「海外送金」等も、上記に次いで多くの企業から挙げられた。

上記の手続き等において、必要なトラスは異なり、「個人の厳格な本人確認」、「法人の厳格な本人確認」、「文書の非改ざん性・真正性担保」と幅広いため、「個人の電子証明書」「eシール」「タイムスタンプ」、またそれらを組合せた「eデリバリー」何れも、海外連携を行っていくことが望ましいと考えられる。



特に多数の企業から挙げられたのは、業種共通の「受発注の取引書類」、「請求支払の取引書類」、「契約書」等

また、業種固有の「銀行口座の開設」等も挙げられた

海外連携が求められる 主なユースケース例

必要なトラス

		個人の厳格な本人確認	法人の厳格な本人確認	文書の非改ざん性/真正性担保
業種共通 の例	受発注の 取引書類		✓	✓
	請求支払の 取引書類		✓	✓
	契約書		✓	✓
業種固有 の例	銀行口座 開設	✓	✓	
トラス確保に必要な トラスサービス		個人の電子証明書	eシール	左記/タイムスタンプ
eデリバリー (上記の組合せ)				

7.3 官民共同規制の在り方 (案)

サマリ

トラスト基盤の構築を推進するにあたって、官庁だけでなく民間の協力を得ることも必要であり、すでに世界各国で先進的にトラスト基盤を導入している国では、官民共同規制の在り方に関して、グローバルには①政府/行政主導型、②ハイブリッド型、③民間主導型の3パターンが存在する。この3パターンの官民共同規制の在り方は、互いに規制のコントローラビリティ/アジリティ、政府/行政の内製化が必要なケイパビリティ、立ち上げに係る期間、普及推進力にトレードオフがある。①政府/行政主導型は、普及速度やフェデレーション等を含め、コントローラビリティやアジリティは高い一方、政府/行政に必要とされるケイパビリティは大きく、立ち上げまでにかかる期間は長い。民間主導型は、政府/行政に必要とされるケイパビリティは限定的で、立ち上げにかかる期間は早い一方、普及は限定的になる可能性があり、コントローラビリティやアジリティも低くなる。ハイブリッド型はいずれも中程度である。

日本におけるトラスト基盤の普及に向けては、これらの特徴を踏まえるとハイブリッド型が望ましいと考える。我が国におけるハイブリッド型の官民共同規制として望ましいと思われるものをコントローラビリティ/アジリティ、政府/行政に必要とされるケイパビリティ、立ち上げ/普及推進の3つの観点から説明する。まずコントローラビリティ/アジリティの観点では、行政/各業界のユースケースを踏まえ、行政トップダウンではなくトラストニーズの優先度を加味した規制/ガイドライン作成を目指すことが望ましいと考える。技術革新や社会ニーズの変化に対しては、情勢に対して規制/ガイドラインを一定程度機動的に更新していく。次に政府/行政に必要とされるケイパビリティの観点では、サービスの設計・開発、運営について、行政内だけで賄う/取り込むことはハードルが高く、運営ガイドライン/認定基準等の会期薬の必要性を示した上で、政府からの委託ではなく民間主導での事業運営を目指すことが望ましいと考える。最後に立ち上げ/普及促進の観点では、トラストに関する認知向上や管轄省庁とタイアップした初期ニーズを満たすサービス実現等、トラストサービス市場形成のための一定の推進力を確保し、早期の普及実現を目指すことが望ましい。

官民共同規制の在り方の類型化

官民共同規制の在り方として、グローバルには①政府/行政主導型、②ハイブリッド型、③民間主導型の3パターンが存在する。それぞれに規制のコントローラビリティ/アジリティ、政府/行政の内製化が必要なケイパビリティ、立ち上げに係る期間、普及推進力にトレードオフが存在し、すでに世界各国で先進的にトラスト基盤を導入している国ではそれぞれのニーズに合わせてどの類型を採用するか決定している。

政府主導型は主にシンガポールやエストニアで採用されている類型であり、政府/政府機関が規制策定およびeTS認証基盤の整備・運用を担当する累計である、民間ベンダーは基板の実装支援または市場展開を部分的に担当する等、トラスト基盤の大部分を政府が担当する。民間主導型は、主にオーストラリアやノルウェー、アメリカで採用されている類型であり、特定民間企業・業界にて既に運用されているデジタルID/eTS基盤を活用する方式を採る。政府はサービス普及推進のための法整備やガイドラインを担当するに留まる。また、ハイブリッド型はEUやイギリス、トラストサービス導入初期のアメリカで採用されていた類型であり、政府/政府機関はガイドライン策定や監査を主に担当する。基板の実装・運用は各ベンダーおよび地方政府が担当する形式で分業を行う。また政府の法規制策定のボードには民間ベンダーの識者を招聘し、早い段階から民間の巻き込みを実施する。

これら3類型を比較すると、政府主導型はアジリティ高く推進できる一方、内製を行うためのケイパビリティを獲得する難易度が高い。具体的には、組織・人材の育成/獲得が必須となる。一方、民間主導は早期実装が可能である者の独自規格化のリスクをはらんでいる。両者ともに大きなハードルがある形になるため、ハイブリッド型を基本として官民が持つケイパビリティ、国内のサービス環境等の条件を複合的に考慮し、官民共同の在り方を模索していく必要がある。

	政府主導型	ハイブリッド型	民間主導型
類型概要	<ul style="list-style-type: none"> 政府/政府機関が規制策定及びeTS認証基盤の整備・運用を担当 民間ベンダーは基盤の実装支援または市場展開を部分的に担当 	<ul style="list-style-type: none"> 規制策定のボードに民間ベンダーの識者を招聘 政府/政府機関はガイドライン策定及び監査を主に担当、基盤の実装・運用は各ベンダー及び地方政府が担当 	<ul style="list-style-type: none"> 特定民間企業・業界にて既に運用されているデジタルID/eTS基盤の活用 政府はサービス普及推進のための法整備、ガイドライン整備を担当
法規制の作成主体	政府	政府	政府
ガイドライン作成主体	政府	官民共同	民間
基盤運営主体	官民共同/民間委託	官民共同/民間委託	民間
主な事例	<ul style="list-style-type: none"> SingPass (シンガポール) <ul style="list-style-type: none"> シンガポールの国民ID及び関連するトラストサービス e-Estonia (エストニア) <ul style="list-style-type: none"> エストニアの国民ID及び関連するトラストサービス 	<ul style="list-style-type: none"> eIDAS (EU) <ul style="list-style-type: none"> EU加盟国共通でeID及びトラストサービスの法的効力を認める規則 GOV.UK Verify (英) <ul style="list-style-type: none"> 国内の民間デジタルID提供企業と連携しトラストサービスを提供 ICANN (米) ※設立時 <ul style="list-style-type: none"> インターネット上の識別子管理及びDNSルートサーバシステムの運用 2016年に民営化し民間主導の運営体制へ変更 Digital Identity Programme (ニュージーランド) <ul style="list-style-type: none"> 政府自ら電子ID基盤を運営しつつ、民間基盤との相互運用に向けた法整備、およびガイドライン作りを推進 	<ul style="list-style-type: none"> Digital ID (豪) <ul style="list-style-type: none"> Australia Postが運営するデジタルIDサービス BankID (ノルウェー) <ul style="list-style-type: none"> 国内主要銀行が展開するデジタルIDサービス PIV-AV (米) <ul style="list-style-type: none"> 航空業界において機材部品やソフトウェアのIDと作業者の個人IDを紐づけた認証管理により業務コスト削減・セキュリティ向上
※ICANNのみ非トラスト領域の事例			
	行政・企業間取引の電子化・トラスト確保 政府IDによるサービス電子化		

Source: BCG分析

156

	政府主導型	ハイブリッド型	民間主導型
事例	<ul style="list-style-type: none"> SingPass (シンガポール) e-Estonia (エストニア) 	<ul style="list-style-type: none"> eIDAS (EU) GOV.UK Verify (英) ICANN (米国) ※設立当初 Digital Identity Programme (ニュージーランド) 	<ul style="list-style-type: none"> Digital ID (豪州) BankID (ノルウェー) PIV-AV (米国)
普及速度	高 トップダウンでの普及推進が可能	中 他類型の中間	低-中 普及速度はサービス自体の普及度に依存
開発速度	低 ケイパビリティ調達や仕様決定に時間要	中 他類型の中間	高 既存トラスト基盤活用のため最短で実装可能
開発・運用費用	高 自前構築のため初期・ランニング費用いずれも割高	中 他類型の中間	低 トラスト基盤の開発・運用は各ベンダーが負担
必要なケイパビリティ	高 組織・人材の育成・獲得が必須	中 他類型の中間	低-中 ベンダー側リソースを活用可能も、監査ケイパは必要
基盤の互換性 ¹	高 仕様を掌握できるため互換性の設計は容易	中 他類型の中間	低 ベンダー側仕様に依存するためロックイン発生リスク
基盤のアジリティ ²	高 一気通貫でガバナンスが効くため機微な対応が可能	低-中 法規制への反映は早い、民間への波及に時間要	中 他類型の中間



前提となる既存法、官民がもつケイパビリティ、国内のサービス環境等条件を複合的に考慮し官民協働の在り方を判断することが肝要

初期案としては、以下のようなものを想定している。

トラストサービス実現に向けたフレームワーク基準の構成 (初期案)

担当機関	基準内容	デジタルIDに係る詳細内容	トラストサービスに係る詳細内容
ポリシー策定者 (デジタル庁)	<ul style="list-style-type: none"> 一般規定 トラストサービスの定義 アシュアランスレベル 下位規則の規定 	<ul style="list-style-type: none"> デジタルIDアシュアランスレベル (IAL/AAL) 個人の身元確認/本人認証におけるリスクレベル 評価とその保証プロセスの定義 	<ul style="list-style-type: none"> トラストサービスの一覧/定義 eシール、タイムスタンプ、分散台帳等 各トラストサービスに関する下位規定の必要性および基準策定の期日の定義
<ul style="list-style-type: none"> 政府/民間事業者間の認証連携に関するインターフェース/運営事項の基準 (FAL相当) 国際相互連携に関するインターフェース/運営事項の基準 (トラストアンカー/トラストドット) 各担当機関間のサービス連携イメージ、各トラストサービスの活用イメージ 			
基準提供者 (トラストフレームワークプロバイダ)	<ul style="list-style-type: none"> 各サービス事業者の運営/監督基準 認定プロセス 審査官の資格認定 	<ul style="list-style-type: none"> 欧州/シンガポールにおいては各加盟国政府によるIDプロバイダサービス提供が前提となる。(国が認定/監査だけでなくサービス提供までの責務を負う) 本取組においても、行政手続きや公共サービス等国民全体を対象としたサービスのための政府が管理するIDの活用を前提とする 具体的なサービスとしては、JPKI/法人ID等マイナンバーと切り離した仕組みの活用を念頭に、トラストサービス事業者と同等の要件を定義し、政府サービスとしてのトラストな運営を実現する。 	トラストサービス事業者が遵守すべき要件 <ul style="list-style-type: none"> 設備要件、技術要件 鍵管理要件 運用要件 監査要件 <div style="border: 1px solid black; padding: 2px; display: inline-block;">手塚教授ご提示のTAL相当</div>
サービス事業者 (トラストサービスプロバイダ)	<ul style="list-style-type: none"> サービス事業運営の方針 個人情報保護方針 	WIP <ul style="list-style-type: none"> トラストIDプロバイダ (マイナンバー) の活用方針、個人情報の利用目的の定義 個人情報の取り扱いに係る基準 (利用許諾等) 	<ul style="list-style-type: none"> 上記基準で定められた運営基準に関する詳細各トラストサービスごとに異なる基準への対応詳細をどう吸収するかが論点
サービス受益者 (各業界団体)	<ul style="list-style-type: none"> 業界横断でのトラストサービス活用範囲の定義 サービス運営方針、各事業者の義務/受益内容の定義 その他レギュレーション 共通インターフェース定義 	WIP <ul style="list-style-type: none"> 各業界で民間事業者で足並みを揃える箇所の定義 トラストサービス事業者との役割分担の定義 	

世界の官民共同規制の事例

政府主導型

事例詳細① : e-Estonia (エストニア)

トラストサービスの法整備から運営まで政府がガバナンスを効かせつつ、基盤の実装は特定少数の民間パートナーと連携し効率的に推進



概要

- 政府機関であるInformation System AuthorityがデジタルIDおよび行政・企業間取引に係るトラスト基盤の開発・運用を主導
- トラスト基盤および周辺サービス設計段階から特定の民間パートナーと協業 (民間から見ると独占的協業)
- 国内法はeIDAS規則に準拠

基本情報

開始年	2002年
利用者数	>130万人
普及率	99%
トラストドットリスト (政府認定)	民間企業2社

提供トラストサービス

デジタルID	○	eシール	○
電子署名	○	eデリバリー	×※
タイムスタンプ	○		

※トラスト基盤事業者が政府プラットフォームとして運営 (X-road)

官民担当ロール

	政府	民間
法的効力の規定	●	○
ガイドライン整備	●	○
トラスト基盤設計	●	○
トラスト基盤開発・運用	○	●
トラストサービス提供	○	●

政府が指針を示しつつ、民間2社と独占的に基盤設計以降で協働

民間ITパートナー



時系列

1994年	Principles of Estonian Information Policy 制定
1996年	e銀行サービス開始
2000年	eTaxサービス開始
2001年	分散データ連携基盤X-Road運用開始
2002年	eIDおよび電子署名サービス開始
2005年	e投票サービス開始
2007年	mobile-IDサービス開始
2014年	e住民サービス開始

政府主導型

事例詳細② : SingPass (シンガポール)



国家デジタル化戦略 (Smart Nation) 8施策のひとつとして、トラスト基盤開発および運用まで政府が主体となって実行

概要

- 政府機関であるGovernment Technology Agency (GovTech)がトラストサービス基盤開発・運用を主導
- 1000以上のデジタルサービス、250以上の政府機関の手続きで利用可能な個人認証サービスを提供

基本情報

開始年	2003年
利用者数	>400万人
普及率	国民の>90%
トラステッドリスト (政府認定)	民間企業8社

提供トラストサービス

デジタルID	○	eシール	○
電子署名	○	eデリバリー	×
タイムスタンプ	×		

民間ITパートナー

- DocuSign, iText, Netrust, Adobe, OneSpan, Dedoco, Tessaract.io, Kofax

時系列

1988年	Electronic Transactions Act 法制定
2003年	SingPass サービス開始
2011年	Electronic Transactions Act 法改訂
2018年	SingPass Mobileをリリース
2020年	Sign with SingPass (電子署名) サービス開始

官民担当ロール



ハイブリッド型

事例詳細③ : ANSSI (フランス)



eIDAS準拠の国内法およびサービスプロバイダー認定ガイドラインを整備し、B2B中心にトラストサービスの利用が普及している。

概要

- 政府機関であるANSSI※がトラストサービス事業者の認定および監査を担当
 - 金融・不動産業界等でのトラストサービス利用が普及 (KYCや公共調達・入札)
 - 業界単位での企業活動の信頼性/トレーサビリティ確保、必要となる技術基盤開発は今後の展望
- ※Agence nationale de la sécurité des systèmes d'information

基本情報

開始年	N/A
利用者数	N/A
普及率	N/A
トラステッドリスト (政府認定)	民間企業27社

提供トラストサービス

デジタルID	○※	eシール	○
電子署名	○	eデリバリー	○
タイムスタンプ	○		

※トラストサービスとは独立したスキームとして構築

民間ITパートナー

基盤未構築のためN/A

時系列

1999年	Electronic Signature Directive 制定 (EU)
2000年	Electronic Signature Act 制定 (仏)
2014年	eIDAS規則制定 (EU)
2014年	Electronic Signature Act 改訂 (仏)

官民担当ロール



事例詳細④ : GOV.UK Verify (英国)



民間IDを用いて政府サービスの登録/認証機能を電子化。当初目標の利用者数に届かずコストメリットが出ない中、民間パートナーの離脱が相次ぐ状況

概要

- 政府機関であるGDSが、規約や運営ガイドライン策定、ファンディングを担当
- 民間IDを活用したID管理コスト削減が目的だが、利用サービスが限定的/Verifyの成功率が低い等の要因で利用者数が伸び悩みコスト負担が高い状況
- 慣習法の国でもあり、政府によるトラストサービス義務化は考えられておらず、あくまでも市場動向に委ねるスタンス

基本情報

開始年	2014年
利用者数	>360万人 (当初目標2500万人)
普及率	~5.4%
トラステッドリスト (政府認定)	民間企業2社

民間主導型

事例詳細⑤ : BankID (ノルウェー)

デジタルIDが国内全銀行で利用できるため高い普及率を達成、今後周辺トラストサービスへの展開に際した官民連携が課題



概要

- 銀行IDをベースに複数の民間サービスを統合し、民間利用率の高い(20-50歳の90%が利用) デジタルIDプラットフォームとして運用
- トラストサービスに係る国内法はeIDAS規則に準拠

基本情報

開始年	2004年
利用者数	430万人
普及率	国民の>74%
トラステッドリスト (政府認定)	N/A

提供トラストサービス

デジタルID	○	eシール	×
電子署名	○	eデリバリー	×
タイムスタンプ	×		

官民担当ロール

	政府	民間
法的効力の規定	●	
ガイドライン整備	●	
トラスト基盤設計	●	
トラスト基盤開発・運用		●
トラストサービス提供		●

2019年より基盤の開発・運用を民間へ移譲

民間ITパートナー



時系列

2014年	パブリックベータ版サービス開始
2016年	サービス実運用開始
2016年	当初9社のIDプロバイダリストから1社脱退
2018年	同リストから更に3社が脱退
2020年	同リストから更に3社が脱退 現在の2社体制に

概要

- 銀行IDをベースに複数の民間サービスを統合し、民間利用率の高い(20-50歳の90%が利用) デジタルIDプラットフォームとして運用
- トラストサービスに係る国内法はeIDAS規則に準拠

基本情報

開始年	2004年
利用者数	430万人
普及率	国民の>74%
トラステッドリスト (政府認定)	N/A

提供トラストサービス

デジタルID	○	eシール	×
電子署名	○	eデリバリー	×
タイムスタンプ	×		

官民担当ロール

	政府	民間
法的効力の規定	●	
ガイドライン整備	●	
トラスト基盤設計	●	
トラスト基盤開発・運用		●
トラストサービス提供		●

官民共同での取り組みは限定的

民間ITパートナー



時系列

2004年	BankIDサービス開始
2014年	BankID Norway AS社設立
2018年	BankID Norge、Vipps、BankAxeptの3社が合併

事例詳細⑥ : Digital iD (豪州)

民間が開発したデジタルID基盤を政府が認定する事例。特定の民間ニーズに即したサービスである反面、普及推進スピードに課題

概要	提供トラストサービス	民間ITパートナー														
<ul style="list-style-type: none"> Australia Postが主導して開発・運営するデジタルID基盤 トランザクションフィーモデルを採用し、サービス利用企業や組織への導入支援や利用料によりマネタイズ 	<table border="1"> <tr> <td>デジタルID</td> <td>○</td> <td>eシール</td> <td>×</td> </tr> <tr> <td>電子署名</td> <td>×</td> <td>eデリバリー</td> <td>×</td> </tr> <tr> <td>タイムスタンプ</td> <td>×</td> <td></td> <td></td> </tr> </table>	デジタルID	○	eシール	×	電子署名	×	eデリバリー	×	タイムスタンプ	×			N/A (自社開発)		
デジタルID	○	eシール	×													
電子署名	×	eデリバリー	×													
タイムスタンプ	×															
基本情報	官民担当ロール	時系列														
<table border="1"> <tr> <td>開始年</td> <td>2018年</td> </tr> <tr> <td>利用者数</td> <td>>400万人</td> </tr> <tr> <td>普及率</td> <td>国民の>2%</td> </tr> <tr> <td>トラステッドリスト (政府認定)</td> <td>民間企業4社 (Australia Postはそのうちの1社)</td> </tr> </table>	開始年	2018年	利用者数	>400万人	普及率	国民の>2%	トラステッドリスト (政府認定)	民間企業4社 (Australia Postはそのうちの1社)		<table border="1"> <tr> <td>2017年</td> <td>サービス開始</td> </tr> <tr> <td>2019年</td> <td>家政府トラステッドリスト認定</td> </tr> <tr> <td>2020年</td> <td>Master Cardと提携し年齢認証サービス開始</td> </tr> </table>	2017年	サービス開始	2019年	家政府トラステッドリスト認定	2020年	Master Cardと提携し年齢認証サービス開始
開始年	2018年															
利用者数	>400万人															
普及率	国民の>2%															
トラステッドリスト (政府認定)	民間企業4社 (Australia Postはそのうちの1社)															
2017年	サービス開始															
2019年	家政府トラステッドリスト認定															
2020年	Master Cardと提携し年齢認証サービス開始															

ハイブリッド型

事例詳細⑦ : Digital Identity Programme (ニュージーランド)



政府自ら電子ID基盤を運営しつつ、民間基盤との相互運用に向けた法整備、およびガイドライン作りを推進

概要	提供トラストサービス	民間ITパートナー																				
<ul style="list-style-type: none"> 政府機関であるDepartment of Internal Affairs (DIA)がトラストフレームワークおよび法整備を主導 18年から官民を巻き込んだパイロットプログラムを実施 将来的に英、豪、カナダのトラストフレームワークの相互運用も構想 英国と同様「ハイブリッド型」での普及推進にあたり、後発の利点を活かした各種工夫を実施 <ul style="list-style-type: none"> 法レベルでのガバナンスを効かせ、eIDに係る本人情報の鮮度と整合性を厳密に管理 eID提供者と利用者間をバイディングし、サービスのアシュアランスレベルを担保 日常に根差したサービスへの活用を前提に、早期からeID利用側企業と調整 今後フレームワーク発効後の実効性検証は必要 	<table border="1"> <tr> <td>eID</td> <td>○</td> <td>eシール</td> <td>×</td> </tr> <tr> <td>電子署名</td> <td>×</td> <td>eデリバリー</td> <td>×</td> </tr> <tr> <td>タイムスタンプ</td> <td>×</td> <td></td> <td></td> </tr> </table>	eID	○	eシール	×	電子署名	×	eデリバリー	×	タイムスタンプ	×			<ul style="list-style-type: none"> RealMe基盤は政府が内製 Trust Framework作成にあたってはITプロバイダ含む民間と協業 								
eID	○	eシール	×																			
電子署名	×	eデリバリー	×																			
タイムスタンプ	×																					
基本情報 (RealMe)	官民担当ロール	時系列																				
<table border="1"> <tr> <td>開始年</td> <td>2013年</td> </tr> <tr> <td>利用者数</td> <td>93万人</td> </tr> <tr> <td>普及率</td> <td>国民の20%程度</td> </tr> <tr> <td>トラステッドリスト (政府認定)</td> <td>作成中</td> </tr> </table>	開始年	2013年	利用者数	93万人	普及率	国民の20%程度	トラステッドリスト (政府認定)	作成中		<table border="1"> <tr> <td>2013年</td> <td>RealMeサービス開始</td> </tr> <tr> <td>2015年</td> <td>に対応</td> </tr> <tr> <td>2018年</td> <td>Digital ID整備に係る2カ年計画をNZ政府が承認</td> </tr> <tr> <td>2020年</td> <td>NZ議会がDigital Identity Trust Frameworkの法制化に賛成</td> </tr> <tr> <td>2021年</td> <td>NZ議会が同Frameworkに係るトラストサービス認証局および運営組織の設置を承認</td> </tr> <tr> <td>2021年</td> <td>同Frameworkに係る法案提出</td> </tr> </table>	2013年	RealMeサービス開始	2015年	に対応	2018年	Digital ID整備に係る2カ年計画をNZ政府が承認	2020年	NZ議会がDigital Identity Trust Frameworkの法制化に賛成	2021年	NZ議会が同Frameworkに係るトラストサービス認証局および運営組織の設置を承認	2021年	同Frameworkに係る法案提出
開始年	2013年																					
利用者数	93万人																					
普及率	国民の20%程度																					
トラステッドリスト (政府認定)	作成中																					
2013年	RealMeサービス開始																					
2015年	に対応																					
2018年	Digital ID整備に係る2カ年計画をNZ政府が承認																					
2020年	NZ議会がDigital Identity Trust Frameworkの法制化に賛成																					
2021年	NZ議会が同Frameworkに係るトラストサービス認証局および運営組織の設置を承認																					
2021年	同Frameworkに係る法案提出																					

7.4 アシュアランスレベルの分類 (案)

サマリ

デジタル ID に関するアシュアランスレベルの分類を考えるにあたって、まずは定義を行うカテゴリに分解し、それぞれに検討を進めていく必要がある。今回は SP800-63-3 等の事例と同様に身元確認 (IAL)、認証プロセス (AAL)、認証情報連携 (FAL) の3つのカテゴリに分解し、それぞれのアシュアランスレベルを3段階もしくは4段階に分割することを考えた。検討の進め方の初期案としては、IALとAALでは身元確認/認証におけるリスクとその保証方法をレベル分けした初期案を策定し、その後ユースケース (利用 ID と確認方法) を継続的に確認し、レベル規定に

反映するという流れを取る。また FAL では、eIDAS が行っているアプローチを踏襲し、技術面/運営面での遵守事項を定めるのが良い可能性があり、議論する必要がある。

	定義カテゴリ	定義内容	アシュアランスレベル		検討の進め方
			Lv	保証レベル内容	
デジタル ID	身元確認 (IAL)	サービス登録時の身元確認の信用度をレベル分けする	IAL.1	身元確認のない自己表明	<p>身元確認/認証におけるリスクとその保証方法をレベル分けした初期案策定</p> <p>↓</p> <p>ユースケース (利用IDと確認方法) を継続的に確認し、レベル規定に反映</p> <p>NISTでは技術標準として Federationのレベルを規定するが、本件では eIDASアプローチを取るべきか?</p>
			IAL.2	非対面確認	
			IAL.3	対面確認 ¹⁾	
	認証プロセス (AAL)	サービス認証時の本人認証の信用度をレベル分けする	AAL.0	認証なし	
			AAL.1	1要素認証	
			AAL.2	多要素認証	
	認証情報連携 (FAL)	認証した情報を別機関に連携する際の認証済情報の信用度をレベル分けする	AAL.3	多要素認証 (ハードウェアトークン有) ²⁾	
			FAL.1	署名付与	
			FAL.2	暗号付与	
			FAL.3	ユーザへ正当性確認可能	

1. 対面確認は何かの方法で検証者としての正当性が認められている検証者が検証するものとする;
 2. 対タンバー性(外部から内部構造や記録されたデータ等を解析、読み取り、改悪されにくいになっている状態)のあるハードウェアトークンとする

身元確認 (IAL) のアシュアランスレベルの定義

身元確認 (IAL) に関する想定リスクとしては、正当な身元確認証明を第三者に不正に利用されてしまうリスクと、身元確認証明が偽造され、なりすまし利用されてしまうリスクが存在する。

アシュアランスレベルの初期案としては以下のように3段階とすることを想定しているが、いくつかの論点が存在する。1つ目は、対面相当オンライン (eKYC) のアシュアランスレベルの定義である。eKYC は対面での確認と同等以上のリスク軽減効果があるため、対面での確認と同様のアシュアランスレベルとして定義することが想定できるため、アシュアランスレベルの表記をどのように設定するか議論する必要がある。ただし、eKYC では Identifier の偽造の可能性は残っている。

2つ目は、発行元保証されている身元証明可能なものを Identifier として、オンライン登録後に対面で確認する場合のアシュアランスレベルの定義である。この場合は偽造リスクを軽減できていないため、IAL-2 とするのが妥当だと思われるが、議論が必要である。ただしこの方式は今後より精度の高い非対面での確認方式に置き換わっていく可能性が高い。

3つ目は、信頼できる機関により電子的に身元証明可能なもの、発行元保証されている身元証明可能なものを Identifier として、オンラインで確認を行う場合の身元確認証明の偽造リスクの評価である。Identifier の偽造耐性の違いが両者で存在するが、第三者に身元を不正利用されるリスクに対する耐性はどちらもなく、レベルを分割するか議論する必要がある。

IAL	Identifier	確認方法	身元確認におけるリスク軽減パターン ¹⁾	
			正当な身元確認証明が第三者に不正に利用されてしまうリスク	身元確認証明が偽造され、なりすまし利用されてしまうリスク
IAL-3	信頼できる機関により電子的に身元証明可能なもの	対面で確認	○	○
	発行元保証されている身元証明可能なもの	対面での有資格者による確認	○	○
		対面相当オンライン (eKYC ²⁾)	○	○?
?	発行元保証されている身元証明可能なもの	オンライン登録後 対面で確認	○	△
IAL-2	信頼できる機関により電子的に身元証明可能なもの	非対面で確認	×	○
	発行元保証されている身元証明可能なもの		×	△
IAL-1	身元確認のない自己表明可能なもの	身元確認なし	×	×

アシュアランスレベルにおける論点

- eKYCは対面での確認と同等以上のリスク軽減効果があるため、対面での確認と同様のアシュアランスレベルとして定義するか? その場合のレベル表記をどうするか? ただし、Identifierの偽造可能性あり?
- 偽造リスクを軽減しきれていないため、IAL-2とするのが妥当か?
※ 本人住所への郵送による本人確認を行っているが、今後より良い非対面での確認方式 (eKYC等) に置き換わっていく想定
- Identifierの偽造に対する耐性の違いはあるが、第三者に身元を不正利用されるリスクに対するはどちらもないため、レベル分け

具体的な各 IAL における Identifier 及び本人確認方法とユースケースの対応は以下ようになる。

IAL	Identifier	確認方法	ユースケース
IAL-3	信頼できる機関により電子的に身元証明可能なもの	対面で確認	マイナンバーカードを使用した対面での申し込み
	発行元保証されている身元証明可能なもの	対面での有資格者による確認	対面での身分証明必須のID/PASSの発行 (e-Tax 等)
		対面相当オンライン (eKYC)	オンラインでの身元証明書上の本人写真とリアルタイム本人画像のマッチング
?	発行元保証されている身元証明可能なもの	オンライン登録後 対面で確認	オンラインでの銀行口座開設→カード受け取り時に本人確認
IAL-2	信頼できる機関により電子的に身元証明可能なもの	非対面で確認	オンラインでのマイナンバーカードリーダーを用いた口座開設
	発行元保証されている身元証明可能なもの	非対面で確認	オンラインでの本人確認書類 (画像アップロード 等) を用いたECサイト会員登録
IAL-1	身元確認のない自己表明可能なもの	身元確認なし	サービス登録時におけるメールアドレスでの通達確認

認証プロセス (AAL) のアシュアランスレベルの定義

認証プロセス (AAL) に関するリスクとしては、盗聴、フィッシング、ハッキング、偽造等が存在する。これらのリスクに対して、認証要素のバリエーションの追加やより堅牢な認証要素の導入を行うことでリスク回避を行うことが一般的である。具体的には、認証要素のバリエーションの追加では単要素認証から複数認証方式へ変更すること、より堅牢な認証要素の導入では耐タンパー性を持つハードウェアトークンの利用や、検証者との認証済保護チャネルの導入を行う等様々なバリエーションが存在する。

アシュアランスレベルの初期案としては以下のように4段階とすることを想定しているが、AAL-3とAAL-2の分類は論点である。より堅牢な認証要素の導入に関しては、想定されるリスクに対して様々なデバイス・認証プロセスの方式がムービングターゲットとして存在し、さらに今後も追加される見込みであるため、AAL-3とAAL-2の分類にお

いて明確な境界線を設けることは難しい、政府発行の PKI 認証を促進するために区分けするか、もしくは区分けしないか等を議論する必要がある。

AAL	認証プロセス	想定リスク及び各本人確認方法によるリスク軽減是非 ^{※2}	
		認証要素のバリエーション	より堅牢な認証要素の導入
AAL-3	多要素認証 (含む耐タンパー性を持つハードウェアトークン) + 検証者との認証済み保護チャネル [※]	複数要素	○
	多要素認証 (含む耐タンパー性を持つハードウェアトークン)	複数要素	△?
AAL-2	多要素認証	複数要素	×
AAL-1	一要素認証	単要素	×
AAL-0	認証なし	無し	×

1 AAL-3とAAL-2の違いをどこまで分けるか?

より堅牢な認証要素の導入に関しては、以下の通り想定されるリスクに対して様々なデバイス・認証プロセスの方式がムービングターゲットとして存在し今後も追加される見込み

- 耐タンパー性を持つハードウェアトークンの利用
- 検証者との認証済み保護チャネルの導入

ムービングターゲットが今後も追加されている中で、どのレベルでAAL-3とAAL-2を区分けするか?政府発行のPKI認証を促進するために区分けするか?もしくは区分けしない等

具体的な各 AAL における認証プロセスとユースケースの対応は以下ようになる。

AAL	認証プロセス	ユースケース
AAL-3	多要素認証 (含む耐タンパー性を持つハードウェアトークン) + 検証者との認証済み保護チャネル [※]	—
	多要素認証 (含む耐タンパー性を持つハードウェアトークン)	ICカード方式・リモート署名利用による申告 ID/PASS+ハードウェアトークンによるワンタイムパスワードによる認証
AAL-2	多要素認証	Smart-ID方式・リモート署名利用による申告 ID/PASS+ソフトウェアトークンによるワンタイムパスワードによる認証
	⋮	⋮
AAL-1	一要素認証	ネット証券口座利用におけるID/PASSによるログイン及び取引時に別パスワード利用サービス利用時におけるID/PASS
AAL-0	認証なし	宅配便の受け取り メールアドレスの送達確認のみ