資料5

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