

属性証明の課題整理に関する有識者会議(第1回) 議事要旨

1. 日時

令和7年10月23日(木)10:00-12:00

2. 場所

デジタル庁会議室及びオンライン

3. 出席者

(委員)

板倉陽一郎委員、笠井玲子委員、國領二郎委員、崎村夏彦委員、瀧俊雄委員、中村素典委員、富士榮尚寛委員、松尾真一郎委員、松本泰委員、横田明美委員、若江雅子委員(欠席)

4. 議事概要

(1) 議論前提に関する主な意見

- 全体的にリスクの話にフォーカスし過ぎてしまっているのではないか。リスクのないユースケースを洗い出し、そこから社会実装を進める道もある。
- 現場の運用でダメージコントロールが可能な場合はリスクを受容することもあり、高いリスクのケースだけを考えるよりは、非常にリスクの低いケースも検討が必要ではないか。
- 架空のものでも構わないので、詳細化されたユースケースが題材としてあれば、それぞれの観点で検討範囲、リスクの考慮範囲が議論しやすい。

(2) 論点1に関する主な意見

論点1-1) 公的なユースケース(特にリスクが高い個人向けのもの)を念頭におくと、その推進に向け、適切な技術面・運用面の対策を促すには何が必要か?(例:ガイドライン等)

- すべてのクレデンシャルにおいて Holder Binding をしなければならないのか、バインドの強度がそれほど強くなくても機能するケースもあると思うので、腑分けするところから始めるのが良い。縛る方向ばかりではない議論にしていけると良い。
- 公的なものであればエコシステムは機能すると思うが、民間の場合、法制度の縛りが無くてもエコシステムが機能するかは疑問がある。縛りが無くても機能することが望ましいが、法制度が必要なフェーズがいつなのかも検討すべき。例えば民間による寡占が問題視される場合は、認定制度などが必要なのではないか。
- ハードローによる規制も検討対象に含めるべきではないか。既存の法律での対応も提案されているが、個人情報保護法で DIW の全てのプライバシーリスクに対応することは難しいと思われる。
- 選択的開示やデジタル完結が、市民、行政に大きなメリットがあることがわかるよう議論を進めるべき。そのため必要であれば、今すぐ必要とまでは思わないが、法令改正を躊躇わないでほしい。
- Can-Be として法令改正不要なものを進めたい意図は理解するが、To-Be として目指す方向性の議論が必要ではないか。極論、資格は全て VC を利用するよう強制力を持たせる一括法などもありだと考える。

- Wallet Provider は現状では多くの情報を取得・利用が可能である。今後プラットフォーム事業者による寡占が生じた場合、本来の目的と異なる一定の用途への利用を禁じる必要は出てこないか。
- この仕組みは最低線のセキュリティ水準の底上げが必要だが、サプライチェーンにおけるセキュリティ確保等では、優越的地位の濫用とならないよう留意が必要。
- まだまだ VC への理解が得にくい状況であり、普及活動や利用シーンの盛り上げといったことも必要ではないか。

論点1-2) 上記手法案の対象範囲や位置付けはどうあるべきか？

- ガイドラインをゴールとすることは良いと思うが、そのガイドラインを Verifier や Issuer が遵守して運用していることが、人の目だけでなく、AIエージェントなど機械的にも判別出来るような仕組みも目指すべき。
- 究極的には紙を無くしていく、デジタルファーストを目的としていることは明記すべき。
- 実装主体が国、自治体、民間と異なるため、目線を合わせて実装される必要がある。ガイドラインがどのように活用されるか、ある程度見越して作成する必要がある。
- 攻撃者は法律を無視して一番効率的に攻撃手法を考えるため、一番緩い人が攻撃されないように、一番緩い人がちゃんとやるように設計をしていく必要がある。
- 議論の対象が、オンライン提示のみではなく対面での提示も含めているのであれば、対面提出時の検証機器も、リスクや利用者を絞る上で重要な観点となるのではないか。
- 運用を拡大していくためには、VC を受け入れる側の体制や、どういうものを受け入れるのかという考え方もガイドラインで示すべきではないか。
- 選択的開示が可能だとしても、本人に対して、十分かつ簡潔に提示させる情報の必要性を示せないという意味がない。情報提供先である Verifier が要求するものが適切か、というデータミニマイゼーションがなされているのかも、ユーザーは判断できない。情報銀行の認定制度を参考に、要求時の表示方法等、そのような観点もガイドラインに含めるべきではないか。

論点1-3) 技術 WG で特に議論すべき論点はなにか？

- 利用シーンをもう少し細かく考えていかないと、リスク分析や技術検討における議論が進みにくい。例えば、記載内容の正しさのみ検証する場合もあれば、記載されている本人が提示できることも含めて検証する場合もある。提示時点のみ有効性を検証するのか、提示後一定時間が経過した後も有効性を確認する必要があるのか、個人の識別子を仮名化して紐づかないことを求めるケースもあれば、紐づいていても良いケースもある。
- ユースケースは重要だと思う。ユースケース次第で関係するステークホルダーが変わるので。例えば欧州では官官はバックオフィス連携するとしているが、フロントで連携した方がいい場合もあるかもしれない。そして今できることをやることと、将来どうなるかというのは、両方考える必要がある。
- 今年度、網羅的なガイドラインを作成することは困難だろう。まずはどのようなパターンがあるのかという全体像を示し、そのうち利便性が高く、早めに手を付けるべき分野にフォーカスして議論を進めていくのが良い。