経済産業省委託事業

Trusted Webの国際標準化に向けた調査 概要

鈴木茂哉

慶應義塾大学大学院政策・メディア研究科 特任教授
慶応義塾大学SFC研究所ブロックチェーン・ラボ 副所長（技術統括)
WIDEプロジェクトボードメンバ

2022/3/15

Trusted Webの国際標準化に向けた調査

- 令和３年度産業標準化推進事業委託費
  （戦略的国際標準化加速事業：ルール形成戦略に係る調査研究Trusted Webの国際標準化に向けた調査）

- 慶応義塾大学SFC研究所で受託

- 事業期間: 2021/12/10 〜 2022/2/25
- 報告書は経済産業省から公開予定

事業目的

- COVID-19を契機に社会全体のデジタルトランスフォーメーション（ＤＸ）が加速 し、サイバーとフィジカルが融合していく中で、様々な社会活動のデジタル化が進む「デジタル社会」に移行している。しかしながら、フェイクニュースやプライバシーリスク等の様々な課題が顕在化し、“一握りの巨大企業への依存”でも、“監視社会”でもない第三の道を模索することが必要となっている。このような中で、デジタル社会の基盤として発展してきたインターネットとウェブでは、データの受け渡しのプロトコルは決められているが、Identity管理も含め、データ・マネジメントの多くはプラットフォーム事業者など各サービスに依存し、かつサイロ化され、外部からの検証可能性が低く、「信じるほかない」状況となっている。
- こうした中、2020年６月のデジタル市場競争会議における「デジタル市場競争に係る中期展望レポート」の提言を受け、データ・フリー・フロー・ウィズトラスト（DFFT）の具現化も視野に、2020年10月、内閣官房において「Trusted Web推進協議会」が発足し、2021年３月には、「Trusted Webホワイトペーパーver1.0」がとりまとめられた。ここで提唱されている「Trusted Web」の実現により、現在インターネット上では行うことができていない、Identity管理に係る外部からの検証可能性が高められることで、データそのものやデータ主体の真正性・信頼性の向上、それによるデータ流通の質的向上、ひいてはインターネットにおける安全で信頼できるデータ流通基盤の整備、また、必ずしも一部のプラットフォーム事業者に依存することのない、さまざまな新しい関連サービスの創出が期待される。
- **本調査においては、「Trusted Web」のアーキテクチャーを構成する、Identity管理をはじめとする機能の具体的な技術仕様の検討及び必要なルール形成戦略の策定を行う**

- 国際標準化に向けた技術関連調査
  - 技術開発調査
  - 標準化動向調査
  - ルール形成戦略策定
- 検討グループ運営
- 事業報告書作成

ユースケース分析

- 3個のサブグループの議論（承前）
  - 個人
  - 法人
  - モノ

標準化動向調査 (1)

- 標準化団体 (Standard Development Organizations - SDOs) についての類型とTrusted Webの関係

- デジタルアイデンティティについての議論
  - 発展経緯、問題点、自己主権型の登場
- Decentralized Identifiers (W3C)
  - 実装状況

標準化動向調査 (2)

- Verifiable Credentials (W3C)
  - v1.0
  - v2.0 の今後

- DID/VC における課題

- ISO/IEC における関連議論の現状整理
  - ISO/TC 307
  - ISO/IEC TC 1/SC 27

- 今後の戦略

DID/VC活用における課題

- インターオペラビリティ
- Methodの選択と適用
- **ドメイン知識とスキーマ**
- **既存のトラストフレームワークとの連係**
- **国際化と多言語化**
- セキュリティ
- **トランスポート**

ドメイン知識とスキーマ

- Verifiable Credentials は、受け取り検証する側が求める情報を、発行する側が、受け取り側が解釈できるような形式で提供する必要がある。先の節で示したようなインターオペラビリティ上に加え、**それぞれの適用領域（ドメイン）毎に合意されたスキーマを用いてデータが用意されている必要がある。**さらに、**それらの情報が国内にとどまるのでは無く、グローバルにやり取りされるような場合は、グローバルに合意されたスキーマである必要**がある。
- コロナワクチン証明書はVCに基づいたSmart Health Card標準に従った形式が一つの形式として用いられているSmart Health CardはHL7という国際的に活用が進む医療情報形式を用いている
- 一方、HL7は各国国内で用いるのに十分なレベルでの国際化はされているが、国を跨いで使われるような多言語化まではされていないため、海外から日本国内への留学生が取得するようなケースでの対応に苦慮しているように見える

既存のトラストフレームワークとの連係

- Verifiable Credential自身の**発行者の確からしさを確認するためには、何らかの方法で信頼の起点を確保し、発行者が署名時に用いた公開鍵に至るまでの信頼の連鎖を確保する必要がある**
- **求める確からしさに応じて、必要な信頼の起点と信頼の連鎖の選択が必要である**
- **要素技術としては、X.509 PKI に依拠するWeb PKIや日本であるならGPKI 、DNS とDNSSEC , JSON Web Key に、HTTP/TLS等の組み合わせ**であろう。これらの選択と組み合わせは現時点においても、**かなりの自由度で組み合わせが可能**である。求められる確からしさに応じて組み合わせることになる。
- さらに、TLSのエンドポイント認証へのDNSSECの適用である “TLS DNSSEC Chain Extension” が実験されている。これを含め他組み合わせの検討により、**必要な証明書あるいは署名の数を減らせる可能性がある。**

国際化と多言語化

- データレベルでどのような言語で書かれていてもデータとして納められる国際化と、複数の言語を同一データの中で記述できる多言語化は必須である
- **データレベルでの国際化と多言語化を達成するには、データモデルのレベルにおける国際化と多言語化が必要**である。
- **現在最新のVC 1.1データモデルでは、示された例において一見多言語化がサポートされているように見える部分があるが、この部分は標準化されていない**
- 国際化についてはUTF-8を用いるのが基本となっているので一定レベルで達成出来ている。従って、VC標準における国際化が必須である
- **事業期間中に、VC 2.0データモデル標準化に向けてのワーキンググループチャータの組成がタイミングよく行われていた。このため、本委託事業期間中に慶応から提案を行った**

トランスポート

- 確認済みのデータをどのようにやりとりするのか
- やりとりするために、デジタルアイデンティティをどう活用するのか
- etc..

- 例
  - ウォレットからの提示
    - 人材ユースケース
      - 本人に纏わる情報の提示
      - リファレンス情報の提示
    - 法人ユースケース
      - 様々な書類のやりとり