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）

調査報告書

令和 4 年 2 月

慶應義塾大学 SFC 研究所

目次

1. はじめに

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 ver 1.0[1]」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。

1.1. Trusted Web ホワイトペーパ 1.0

これまでの Trust の仕組みの上でのデータのやりとりにおいて確認・検証できる領域が狭く、事実を確認せずに、プラットフォーム事業者等を信頼せざるを得ない状況であった。また、データを紐づける識別子の仕組みもプラットフォームもサービス事業者に強く依存するものであった。

この状況に対し、Trusted Web では、特定のサービスに依存せずに、データのコントロールや合意形成の仕組み を取り入れ、検証できる領域を拡大し、Trust(相手が期待した通りに振る舞う度合い)を高めることが出来るような新し

---

[1] Trusted Web ホワイトペーパ 1.0
https://www.kantei.go.jp/jp/singi/digitalmarket/trusted web/pdf/documents 210331-2.pdf

い Trust の枠組みを現行のインターネットの上に重ね合わせるオーバーレイアプローチによって実現しようというものである。

Trusted Web ホワイトペーパ 1.0 では、ユーザーがデータへのアクセスをコントロールでき(Identifier 管理機能)、相手やデータに関する信頼を第三者によるレビューも含めて検証でき(Trustable Communication 機能)、双方の意思を反映した動的な合意形成(Dynamic Consent 機能)とそのプロセスやその後の履行状況を検証できる(Trace 機能)フレームワークを、マルチステークホルダーによるガバナンスでこれを支える形で実現しようというものである。

本調査では、Trusted Web ホワイトペーパ 1.0 での議論から、その実現に向けて一歩進めるために、国際標準化に向けた技術関連調査ということで、3 種類のユースケースについての議論を有識者の協力を得て進めるとともに、Trusted Web 技術に関連する標準について調査し、Trusted Web 実現に向けての今後の課題を整理すると共に必要となる標準策定について検討するものである。

1.2. 本調査研究の進行全体について

本調査研究は大きく分けて (1) 技術開発調査、および、(2) 標準化動向調査の二つの部分にわけられる。(1) 技術開発調査は、プロトタイプ及びユースケース分析を主体としている。(2) 標準化動向調査については、プロトタイプ及びユースケースで用いられる技術を中心に、デジュール標準及びフォーラム標準の標準化の状況を概観する形とした。

1.2.1. プロトタイプ及びユースケース分析についての調査

調査は Trusted Web 推進協議会タスクフォース内に設置された 3 個の検討小グループを通し、会合にてフィードバックを得ながらユースケースとしてまとめる作業を行った。それぞれの小グループについては、Trusted Web 推進協議会第 4 回会合の資料[2]にて公開されている。

サブグループは、以下の三点をとりあげ、ユースケース調査を行った。

---

[2] 第 4 回 Trusted Web 推進協議会 討議用資料
https://github.com/TrustedWebPromotionCouncil/Documents/blob/master/20211026 第 4 回 Trusted Web 推進協議会/01 当日資料/02 資料 1 第 4 回 Trusted Web 推進協議会 討議用資料.pdf

(1) 「個人」のスキル・実績等の転職時におけるやりとり

(2)「法人」の補助金申請における行政庁との情報のやりとり

(3)「モノ」の付加価値の訴求につながる情報のやりとり（サプライチェーンにおけるデータ流通）

3 つのサブグループは、事業期間中に会合を複数回行いつつ、ユースケース文書としてまとめるように進めた。事業期間中に、(1)「個人」サブグループは 5 回、(2)「法人」サブグループは 2 回、(3)「モノ」サブグループは 5 回の会合を行い、有識者による領域に特化した知見をまとめるとともに、Trusted Web 技術をどのように適用することができるか議論を進めた。

また、「個人」のグループはプロトタイプの開発を並行して行った。

それぞれの成果については、サブグループでの議論は Trusted Web ホワイトペーパ 2.0 の内容として反映される。また、プロトタイプはオープンソースとして公開される予定である。

1.2.2. 標準化動向調査

プロトタイプで用いられている技術を中心として、デジュール標準及びフォーラムで関連する技術について調査またはインタビューを行い、まとめた。

Trusted Web で中核となる技術は公開鍵暗号によるデジタル署名に関連する技術である。これらの技術のうち、近年注目を集めており、Trusted Web 技術を下支えする柱となる技術として、World Wide Web Consortium (以下 W3C) で検討・標準化されている Verifiable Credentials (VC) および Decentralized Identifiers (DID) 技術について、関連動向を含めてまとめるとともに、適用における課題についてまとめた。さらに、日本において国際を視点とした活用で重要な Verifiable Credentials の多言語化の議論について検討・提案し、具体的に Verifiable Credentials ワーキンググループの Verifiable Credentials 2.0 に向けた作業アイテムとしてチャータに取り込むことに成功している。これらの経緯についてもまとめた。

2. 国際標準化に向けた技術関連調査

2.1. 技術開発調査 -

2.1.1. ユースケースの検討と分析

Trusted Web 推進協議会のタスクフォースの議論から、個人に纏わる情報、法人と補助金、産業における情報という 3 つのサブグループが組成され、議論を開始した。これらのうち、個人に纏わる情報はプロトタイピングも行う形で進めてきた。

以下、現在検討課程にあるユースケースの議論について、現時点での議論から抜粋する。議論は進行中であるため、それぞれの項目について今後修正がある可能性がある。それぞれのユースケースは、今後まとめられた上で、Trusted Web での議論の基礎となる。

2.1.1.1. 個人に纏わる情報

背景

昨今のデジタル化の進展や COVID-19 の影響により、企業の採用プロセスのデジタル化が急速に進展している。こうした中で、就職・転職活動を行う個人にとっては、自らの機微な属性情報の取扱いに対する懸念やリスクが高まっている。

一方、人口減少や人材需給逼迫の下、採用難が広がる中、採用企業にとっては、採用時のミスマッチを回避すべく、信頼できる情報を得るニーズが高まっている。このような中、人材を採用する際に、採用企業は応募者本人が作成する履歴書や職務経歴書の内容の確認に加え、応募者の現職または前職の同僚や上司に対し、応募者本人の実績や勤務状況に偽りがないかの確認を行う、リファレンスチェックを実施するケースも増えてきている。しかしながら、採用企業からすると、応募者本人やリファレンス提供者について、本人確認や、現職・前職企業の在籍確認などを行うにはハードルが高く、確認手法の信頼性の担保には課題がある。また、応募者やリファレンス提供者の機微な属性情報については、採用企業にとっても、その取扱いに対する信頼性を高め、これら関係者が安心して自らの情報を提供できる環境を整えることが求められている。そのため本ユースケースでは、応募者、リファレンス提供者、採用企業が「事実の確認をしない状態で、相手先が期待したとおりに振る舞うと信じる」に足りる情報のやりとりを検証する。

議論しているペインポイント

- 転職先 / 採用企業側

応募者、リファレンス提供者が本人であることの確認が容易ではない。
応募者、リファレンス提供者が現・前職企業に在籍していること・いたことの確認が難しい。
応募書類やリファレンス内容が改ざんされていないかの検証ができない。
応募者の意図しない情報を受け取ってしまうかもしれない。
応募者やリファレンス提供者から、属性情報の取扱いについて不安を持たれている懸念がある。

- 応募者側
  本人確認のために、応募とは直接関係の無い情報を開示する必要がある。
  応募書類やリファレンス内容が改ざんされていないか確認ができない。
  応募者本人が自らの情報の開示内容、開示先がコントロールできない。
  応募書類やリファレンス内容を誰がいつ参照したかを確かめられない。
  応募時に提供したデータの撤回ができない。
  情報が目的外利用や意図しない第三者に提供される可能性がある。
- リファレンス提供者側
  リファレンスの内容が応募者本人や転職先企業以外に知られてしまうかもしれない。
  リファレンス内容を誰がいつ参照したかを確かめられない。

効果を期待できるポイント

応募者本人が転職先企業に直接応募情報を送ることで、目的外利用や意図しない第三者に提供される可能性を最小限に抑え、本人確認情報や在籍確認情報などを Verifiable Credentials（以下、VC）として渡すことで、転職先企業側の本人確認や在籍確認のコストを抑えることができる。また、応募者本人やリファレンス提供者が転職先企業に対して、必要な情報のみ Identifier に紐づけて提供することとし、VC への一次アクセスを制御できるようにすることで応募者本人は、開示先をコントロールし参照履歴も確認することができる。更に、採用企業において、例えば情報を取得する際の同意や、取得した情報を目的外利用していないことの証明・担保が容易になることにより、情報の取扱いに対する信頼性を高め、これら関係者が安心して自らの情報を提供できる環境を整えることができる。

本ユースケースにおける特異な点

本人と転職先企業だけではなく、リファレンス提供者もエンティティとして参加することにより、本人と転職先企業の二者間のデータのやりとりだけでなく、リファレンス提供者も含め、どの情報を誰に見せるかを厳密にコントロールする必要がある。また、本人確認情報に加え、現・前職における在籍確認の証明も必要となる。

2.1.1.2. 法人と補助金

背景

中小企業等が補助金等を行政に対し申請する際、申請書とともに様々な提出書類を提出する。申請書は企業が用意するが、提出書類として国や中小企業支援機関によって一定のお墨付きを与えられた書類を用意し申請書とともに提出する。現状では、申請書自体の形式が補助金によって異なるので、それに合わせて手作業により情報を入力したり、他の文書から文字情報としてコピーする必要がある。ここには間違いが入り込む余地があるとともに、手間がかかる。提出書類については、確からしさを容易に確認できない場合があり、実際に改ざんされた決算申告書を用いた不正補助金申請の事例報告がある。

本ユースケースでは、令和 4 年度 1 月 20 日募集を開始した、事業再構築補助金の第 5 回公募[3]の情報を元に、法人が通常枠での補助金額 3000 万円を越える申請を行う場合に限定して議論する。

議論しているペインポイント

- 補助金の募集及び受付をする受付機関、申請者、申請に関係した情報を扱う業者等のステークホルダー間でやりとりされる情報の書式がまちまちである
- 提出された書類が改ざんされているかどうかの検証には相当の作業が必要である
- 申請者にとって申請が受理されたかどうか確信をもてない

効果を期待できるポイント

「信頼できる情報」を組み合わせる事によって、情報が改ざんされていないことと情報がどのように誰によって確認されたのかを明らかにできる。これら

[3] https://jigyou-saikouchiku.go.jp/

の事実に頼ることで、法人の補助金申請における申請者と補助金受付組織の負担を軽減でき、補助金交付の迅速化が可能となるとともに、不正補助金申請の削減が見込まれる。

本ユースケースにおける特異な点

- 申請者の営業についての情報に関与するエンティティとの連携によって実現されている
- 既存の GPKI、gBizID、jGrants 等の既存の事業者のためのサービスを適用できる

2.1.1.3. 産業: サプライチェーンにおける化学物質管理

背景

各国・地域において、製品に含有される有害性の高い物質（REACH (Registration, Evaluation, Authorization and Restriction of Chemicals) 規則で言えば、高懸念物質（SVHC: Substances of Very High Concerns）として規制）等の化学物質の製造・輸入や使用等に関する法規制がある。我が国においても、化学物質の審査及び製造等の規制に関する法律（昭和四十八年法律第百十七号、以下、化審法という。）により、化学物質の製造、輸入、使用等を規制している。また、環境の保全上の支障を未然に防ぐために、特定化学物質の環境への排出量の把握等及び管理の改善の促進に関する法律（平成十一年法律第八十六号、以下、化管法という。）により、事業者による化学物質の自主管理の改善を促している。欧州では、REACH 規則により化学物質の登録、評価、許認可、制限、情報伝達等を規制している。また、電気・電子機器については特に RoHS (Restriction of Hazardous Substances Directive) 指令により特定有害物質の使用等を制限している。

本ユースケースでは、これらの規制への対応のためにサプライチェーンにおける化学物質の含有量や使用量の管理についての 4 つのシナリオとそのペインポイント、要求事項、Trusted Web 技術の適用可能性を議論する。

現状のサプライチェーンにおける化学物質管理方法として、我が国の電気・電子機器の製造において広く利用されている chemSHERPA[4]を利用した情報共有を元に議論する。

---

[4] ChemSHERPA
https://chemsherpa.net

議論しているペインポイント

化学物質管理の現状と想定されるシナリオにおける課題と議論するペインポイントを以下のとおりまとめ、各課題・ペインポイントについて詳説する。

- 営業秘密の保持
- 開示範囲の制御
- 既存規制・新規制への対応
- 製造現場の 4M（Man: 人、Machine: 機械、Method: 方法、Material: 材料）変更への追従
- 企業・データの ID 管理
- データの信頼性の担保
- 中小企業のフォロー
- 規制当局への報告
- プロセスで使用される化学物質
- 化学反応により伝達されたものから変化する化学物質
- 販売後の問い合わせ対応
- 販売終了後の対応

効果を期待できるポイント

目的を達成するにはデータの信頼性が重要である。現状のワークフローでは、契約により一定のデータの信頼性を確保している（債務不履行や不法行為による損害賠償請求権などによりデータの改ざんをけん制している）が、ミスや 4M 変更による報告漏れなどが発生しうる状況となっている。一方で、すべての情報を開示することは、製造方法や調達情報等の営業秘密の保持の観点から許容できない。

そこで、「営業秘密の保持」や「開示範囲の制御」を実現しながら、「データの信頼性」を担保出来る仕組みが実現できれば、このような 4M 変更への追従や規制当局への報告、さらには販売後の問い合わせ対応、販売終了後の対応も実現可能となりうる。

本ユースケースにおける特異な点

- 営業秘密を取り扱うため、開示内容・開示範囲の制御が必要である点
  - ➢ データの中身だけでなく、流通過程（サプライヤー情報など）も秘匿する必要がある
- データの信頼性を担保するために検証可能である点

- データの流通過程を秘匿しながら、検証のための情報（信頼）を伝搬する必要がある

2.2. 標準化動向調査

プロトタイプ開発及びユースケース分析を踏まえ、「Trusted Web」の技術仕様を確立していくにあたり、①互換性・品質の確保、②安心・安全の確保、③利便性向上、といった観点から標準を目指した取組が期待される。本章では、そうした標準化の取組について、想定される具体的な方策を検討する。

まず、Trusted Web 標準化の検討に際し、「標準の類型」を以下を参照して定義する。

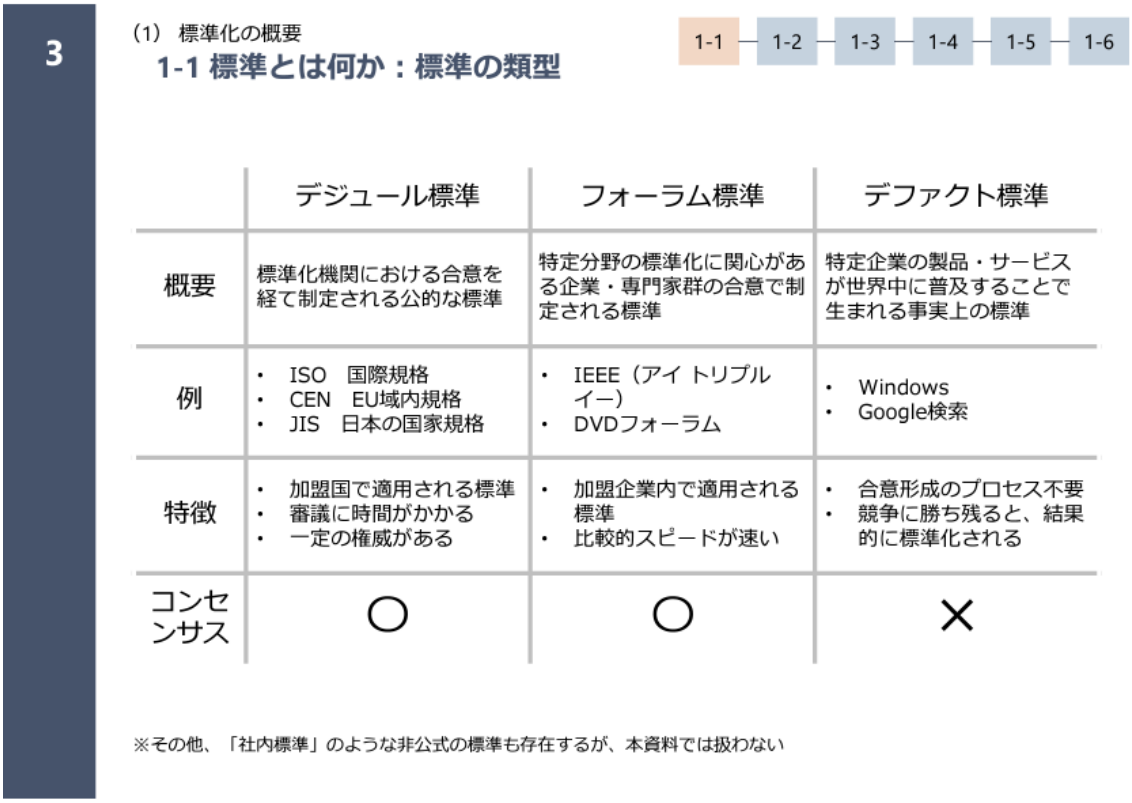

図1 標準の類型[5]

このうち、Trusted Web は特定の企業・団体の利益を目指した製品・サービスではなく、広く社会一般で利用されることを目指した技術であることから、デジュール標準及びフォーラム標準によるアプローチが望ましい。

---

[5] 出所 標準化ビジネス戦略検討スキル学習用資料（経済産業省）
https://www.meti.go.jp/policy/economy/hyojun-kijun/katsuyo/business-senryaku/pdf/001.pdf

デジュール標準及びフォーラム標準は、一定のメンバーの合意を得て規格（仕様書）を制定し、規格を普及させる営みが必要となる。すなわち、前述の図にもあるように、コンセンサス（合意形成）が不可欠となる。

デジュール標準は、代表的な技術標準策定団体（SDO - Standards Development Organization)として、ISO/IEC が挙げられる。ISO/IEC は、各国委員会における検討（随時開催）を経て、各国委員会が一堂に会する国際委員会（年 2 回程度開催）において合意形成が諮られる。そのため、標準化が成立した際は、各国の国内標準化も進展しやすく（我が国で言えば ISO/IEC 標準が JIS 標準として定められる等）、より社会全般に普及しやすく、また一定の権威も認められる。

しかしながら、前述の手続きを経るため、審議に時間を要する。実際、ISO/IEC 標準の場合、00.準備（国内調整）、10.提案（国債規格案の提案）、20.規格開発（WG 内での検討）、30.委員会（TC/SC 内での投票）、40.照会（全加盟国への意見照会）、50.承認（最終国際規格案の正式投票）、60.発行（国際規格の発行）というプロセスを経ることになる（さらに発行後に 90.レビューというステージもある）。そのため、すべてのプロセスを通じて 5 年程度を要することも少なくない。またそれぞれのプロセスにおいて、当事者の利害が一致しない場合、標準化が不成立または当初の目的と異なる妥協を余儀なくされるリスクも存在する。

一方フォーラム標準は、予め利害が一定程度一致したメンバーによって構成されることが多いため、デジュール標準に比べて迅速に検討が進められる可能性があるとされる。しかしながら実際には、フォーラム標準においてもそのフォーラムのポリシーによっては、利害の調整に多くの交渉を要することが少なくない。

たとえばインターネット技術の標準化を担う IETF は、ネットワーク上を流れるデータの取扱いをプロトコルとして策定することを目的とした SDO である。その際、仕様の合意形成はラフコンセンサス（暫定合意）とし、ランニングコード（コンピュータプログラムによる実装）を重んじる文化が醸成されている。そのため仕様に関する検討は比較的迅速に進められるが、実装を終えて製品・サービスとして提供される際には、インターオペラビリティ（相互接続・相互運用性）を確保するための改善が必要となるため、製品・サービスを提供した後も開発を漸次継続することが求められる。

また WWW 技術の標準化を担う W3C は、Web 上の技術、ブラウザ API、あるいはアプリケーション層における抽象度の高いデータモデルを対象とする SDO である。そのため、特に Web ブラウザを実装する事業者・団体の利害が直接的に衝突しやすいことから、W3C で標準化を進めるには、取組に精通したメンバーによる検討・交渉や、W3C 内で利害が一致する他グループとの協調が欠かさない。

こうした標準の類型とそれぞれの特徴や課題を念頭に、Trusted Web を実現するために必要となる要素技術に着目すると、現時点ですでにデジュール標準では ISO と IETF、フォーラム標準では W3C といった SDO で標準化が進められている。

本委託事業ではこのうち、W3C と ISO における Trusted Web 技術展開に関連した動向と今後とりうる方向性について調査した。以下の節で、W3C 及び ISO それぞれについてまとめる。

2.2.1. W3C Decentralized Identifiers (DID)標準と Verifiable Credentials(VC)標準の概観

2.2.1.1. デジタルアイデンティティとその発展

デジタルアイデンティティとは、人に対応するサイバー空間中で識別可能な自己像のことである。ISO 24760-1 では、「実体を構成する属性の集合」と表現されている。我々が常日頃用いているインターネット上のサービスにログインして操作を行う。この操作はユーザ実体とサービスの中のデジタルアイデンティティを結びつける操作と言える。

ユーザ識別子とパスワードの組み合わせによるサービスへのアクセスは、インターネット以前より広く用いられている手段であり、発展してきた。Christopher Allen の整理[6]に頼るならば、以下の四段階の発展に整理できる。

- フェーズ 1 : 中央集権型アイデンティティ
  (単一の、あるいは、階層化された管理権限域によるコントロール)
  例: ドメイン名システム(DNS)、公開鍵認証局(X.509 PKI CA)
- フェーズ 2 : フェデレーションされたアイデンティティ
  (複数の管理権限域間の連合によるコントロール)
  例: Liberty Alliance, Microsoft Passport
- フェーズ 3 : ユーザ中心のアイデンティティ
  (複数の権限域にまたがる個人または管理者によるコントロール)
  例: 複数のコミュニティでの議論から育っていった、様々な標準: OpenID (2005), OpenID 2.0 (2006), Open ID Connect (2014), OAuth (2010), FIDO (2013)
- フェーズ 4 : 自己主権型アイデンティティ
  (複数の権限域にまたって個人がコントロール)
  例: Decentralized Identifiers (DIDs)[7]

現時点では、サービス提供事業者がサービス提供の一環として提供するデジタルアイデンティティが広く用いられている。サービス提供業者のサービス自体と直接的に結びつき、当該サービスを提供するために必要なユーザに紐付いた属性情報を収集、保持し活用する。

---

[6] 出展 The Path to Self-Sovereign Identity
http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereereign-identity.html

[7] Decentralized Identifiers (DIDs) v1.0, W3C Proposed Recommendation 03 August 2021, https://www.w3.org/TR/2021/PR-did-core-20210803/

提供業者によっては、上に示した「ユーザ中心のアイデンティティ」で実現されたプロトコルを用い、サービス間の壁を乗り越えて同じデジタルアイデンティティを活用出来る。このようなデジタルアイデンティティを提供できるサービスプロバイダを Identity Service Provider(IdP)、IdP からデジタルアイデンティティのサービス提供を受けるものを Relying Party(RP) と呼ぶ。IdP～RP 連携基盤においては、サービスの壁を越え、ユーザの許可に従って、IdP は RP に対して属性情報を開示する。

2.2.1.2. デジタルアイデンティティにおける課題

インターネット上のサービスは、デジタルアイデンティティの活用によって成長してきた。一方、慶応義塾大学 SFC 研究所ブロックチェーンラボのディスカッションペーパ[8]や、Trusted Web 推進協議会[9]のホワイトペーパ v1.0 で議論されているように、ユーザーから収集された属性情報はユーザの様々な活動によって生み出されるデータは、事業者において、ユーザからの実質的な合意を伴わない形で、集約・統合・利用されているという懸念がある。いうまでも無く、デジタルアイデンティティはユーザに結びついた情報を直接的得るための手段の一つとなっている。

このようなサービス提供状況に加え、デジタルアイデンティティがサービス提供業者によって直接的にコントロールされているという問題がある。サービス提供業者の管理下にあるデジタルアイデンティティは、サービス提供業者に生殺与奪が握られている。サービス提供業者からアカウント停止されるといった事案は、良く耳にする問題であると言える。更に、そのユーザに結びついたデジタルアイデンティティに紐付いた属性情報も、一定の保護がされているとはいえ、制御権をサービスプロバイダに与えているという問題がある。

2.2.1.3. 自己主権型デジタルアイデンティティ

前節で述べたような課題から、いわゆる自己主権型アイデンティティ（Self-Sovereign Identity)についての議論や設計、関連した標準化が行われるようになってきた。自己主権型デジタルアイデンティティとは、誰にも依存せずに自身で制御可能なデジタルアイデンティティのことである。

---

[8] ニューノーマル時代における人間の社会活動を支える情報基盤の在り方とデジタルアイデンティティの位置づけ, 慶應義塾大学 SFC 研究所 ブロックチェーン・ラボ
https://kbcl.sfc.keio.ac.jp/TR/global-digital-Identity-for-new-normal/

[9] Trusted Web 推進協議会
https://www.kantei.go.jp/jp/singi/digitalmarket/trusted web/index.html

現時点で定義が完全に定まっているとは言えないが、一例として、Christopher Allen による十基本原則[10]を以下に示す:

- 実在: ユーザは独立した存在である。決してデジタルだけでは存在しえない
- コントロール: ユーザーは、自分のアイデンティティ、秘匿性あるいは顕名性を望みに応じてコントロールできなければならない
- アクセス: ユーザは自身のデータへのアクセスができなければならない　門番は存在せず、隠されるものが一切ない
- 透明性: システムとアルゴリズムはオープンかつ透明性が確保されなければならない
- 永続性: アイデンティティはユーザーが望の望みに応じ長期にわたり用いることができなければならない
- 可搬性: アイデンティティに関する情報とサービスはユーザによって移動可能でなければならない
- 相互接続性: アイデンティティは、越境を許す等、可能な限り広く利用できるようにすべきである
- 同意の自由: ユーザーは、自分の個人情報がどのように使用されるかの同意について自由であるべきである
- 最小化: アイデンティティについての主張の開示は最小にとどめるべきである
- 保護: 個々のユーザの権利は、強権を持つ者から保護されなければならない

2.2.1.4. Decentralized Identifiers (DID) と Verifiable Credentials(VC)

Decentralized Identifiers (以下、DID) は、W3C の同名ワーキンググープによって標準化が進められている標準であり、属性情報と紐付けられていない「限り無く無色の」アイデンティティを実現できる。Verifiable Credentials (以下、VC)は、同じく W3C の同名ワーキンググループによって標準化された、属性情報を第三者に証明してもらうためのデジタル証明書の標準である。双方ともデータモデルの標準であり、何らかの API 等のプロトコルを決めているものではない。

---

[10] Self-Sovereign Identity: Ideology and Architecture – Christopher Allen – Webinar 51
https://ssimeetup.org/self-sovereign-Identity-why-we-here-christopher-allen-webinar-51/ (CC BY-SA 4.0)

DID は分散システム志向のシステムであり、このデータモデル標準に従った”method”とよばれる実装を用意することによって利用できるようになる。この実装をどのように行うかによって、様々な特性　これには技術的な特性だけでなく、ガバナンスの上での特性を含む　をもったデジタルアイデンティティを実現できる。

DID を「限り無く無色」と表現したが、DID 対し、属性情報を VC によって紐付けることによって、色づけすることが可能である。また、どのような VC を紐付けるか、提供するかによって、属性情報に対する繊細なプライバシを実現できるところに特徴がある。たとえば、VC にゼロ知識証明などの技術を組み合わせることより個人情報の「選択的最小開示」を実現できる。

既存のデジタルアイデンティティシステムが、単一のシステムで属性情報を集中的に管理するのに対し、DID と VC によるシステムは、属性情報をユーザの手元で管理し、必要に応じて組み合わせて用いることができる。すなわち、属性情報をバンドルして扱っていた従来型のシステムに対し、属性情報のアンバンドルとリバンドルを可能としたシステムということもできる。

DID は VC は並行しながら、以下のような発展過程を辿ってきている[11]

- 2014 - W3C WebPayment Group での議論が発端[12]
- 2015 - XDI.org での議論継続[13],
  第一回 Rebooting Web Of Trust (RWOT1) [14] でのホワイトペーパ “Decentralized Public Key Infrastructure”[15]
- 2016 - RWOT2 でのホワイトペーパ: “Requirements for DIDs” [16]
- 2017 - RWOT3 でのホワイトペーパ:
  “DID (Decentralized Identifier) Data Model and Generic Syntax 1.0 Implementer’s Draft 01”[17]

---

[11] Decentralized Identifiers (DIDs) v1.0, Appendix D. Acknowledgements (Editor’s Working Draft), https://w3c.github.io/did-core/#acknowledgements

[12] Web Payments Community Group Telecon Minutes 2014-05-07, https://web-payments.org/minutes/2014-05-07/#topic-1

[13] XDI.org Registry Working Group Charter, https://docs.google.com/document/d/1EP-KhH60y-nl4xkEzoeSf3DjmjLomfboF4p2umF51FA/edit

[14] Rebooting Web of Trust, https://www.weboftrust.info

[15] Decentralized Public Key Infrastructure, https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/dpki.pdf

[16] Requirements for DIDs, *https://github.com/WebOfTrustInfo/rwot2-id2020/blob/master/final-documents/requirements-for-dids.pdf*

W3C Credentials Community Group[18] の作業に統合

- 2019 - W3C Decentralized Identifiers Working Group による標準化開始[19]

---

[17] DID (Decentralized Identifier) Data Model and Generic Syntax 1.0 Implementer's Draft 01, https://github.com/WebOfTrustInfo/rwot3-sf/blob/master/final-documents/did-implementer-draft-10.pdf

[18] W3C Credentials Community Group, https://www.w3.org/community/credentials/

[19] W3C Decentralized Identifiers Working Group, https://www.w3.org/2019/did-wg/

2.2.1.5. Decentralized Identifiers 標準

Decentralized Identifiers (DID) v1.0[20]は、識別子にまつわるデータモデル標準であり、周辺技術との組み合わせで自己主権型のアイデンティティを実現できる。複数の方式(メソッド)で実装され、メソッドにより、ブロックチェーン技術を下支えにするものも、しないものもある。

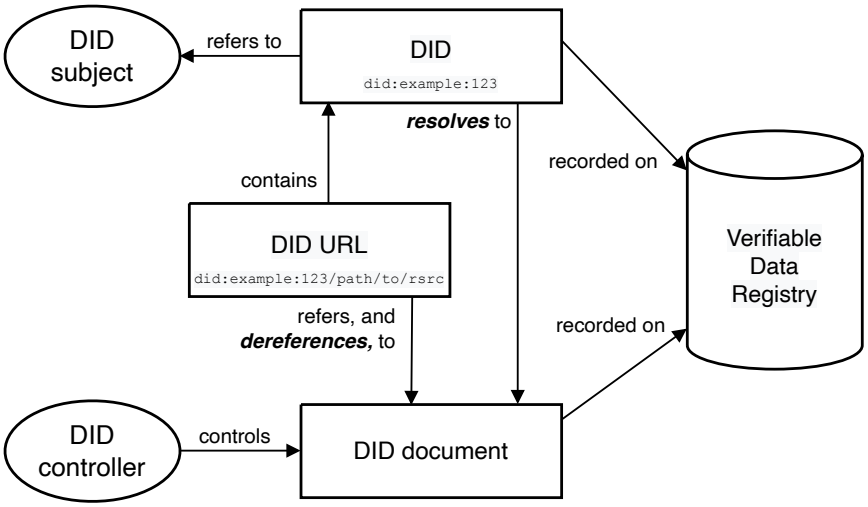

図2 Overview of DID architecture and the relationship of the basic components[21]

DID の標準では、DID の識別子自身、DID で指し示されている対象、DID から導き出せる DID 自身についての情報を示す DID document、DID 自身のコントローラ（すなわち DID Document の更新権限をもつ）、DID を活用したリソースロケータである DID URL が定義されている。DID document は、DID をキーとして発見可能な形で Verifiable Data Registry というデータベースに保持される。

---

[20] Decentralized Identifiers (DIDs) v1.0, W3C Proposed Recommendation 03 August 2021, https://www.w3.org/TR/2021/PR-did-core-20210803/

[21] Decentralized Identifiers (DIDs) v1.0, W3C Proposed Recommendation 03 August 2021 より。

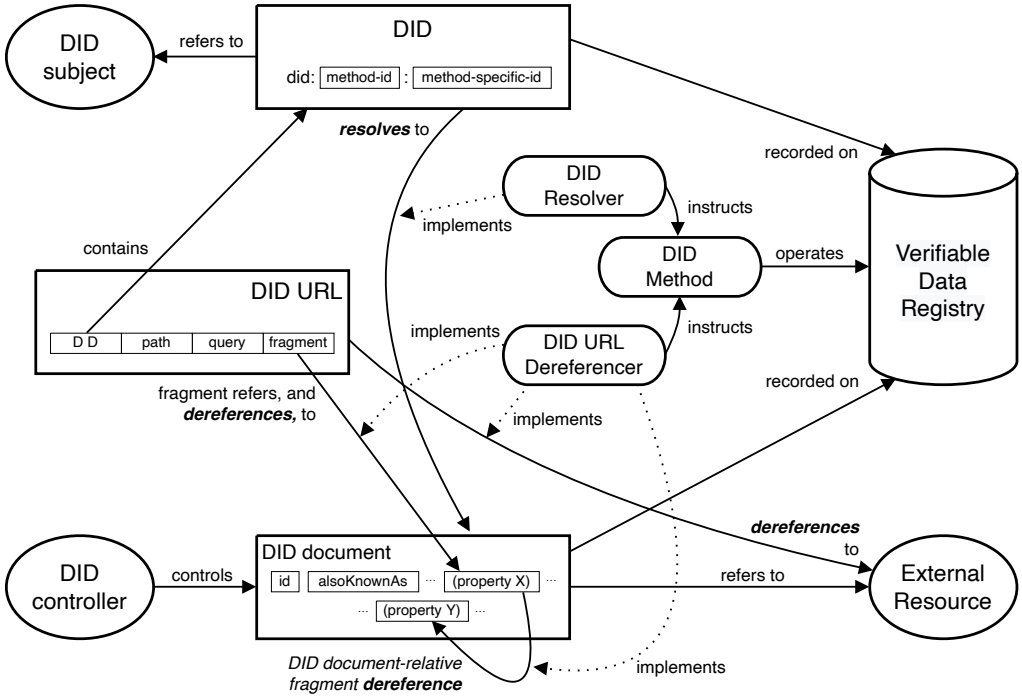

図3 Detailed overview of DID architecture and the relationship of the basic components[22]

実装状況

DID の使用中で特別な意味を持つ名前については、DID Specification Registry[23]に登録することにより名前の衝突をさけている。DID method も、このレジストリに登録することになっている。本文書作成時点(2022/2/19)では 113 種類の Method が登録されている。

様々なインターネットで用いられているフォーラム標準においては、複数の実装の存在が要件になっている。DID の標準化にあたっても同様のプロセスがとられており、仕様項目毎に最低 2 個の実装が登録されることが期待されおり、実装されない仕様については最終的な仕様から削除された。DID 標準はデータモデルであるので、実装（具体的には Method 実装）のデータモデルの正当性を確認するためのテストスートが準備され、テストレポートが公開されている[24]。テストレポートの最新版には 47 個の実装の結果が記録されている。

---

[22] Decentralized Identifiers (DIDs) v1.0, W3C Proposed Recommendation 03 August 2021 より。

[23] DID Specification Registries, 13. DID Methods
https://www.w3.org/TR/did-spec-registries/#did-methods

[24] DID Core Specification Test Suite and Implementation Report, 29 November 2021
https://w3c.github.io/did-test-suite/

2.2.1.6. DID とプライバシ

DID は単一のユーザが多数用い、自由に使い分けができるようになっている。DID は、DID 自身を伝える対象、組み合わせる VC 等に応じて、対象ごとに都度作成 (pair-wise) で使われることが前提となっている。DID および DID document に含まれる情報に、個人識別情報(PII)を含めるだけでなく、個人識別に繋がる可能性のある情報が含まれないように、注意深く検討、仕様化（必要に応じた注意書き）などが行われている。特に、DID 仕様の §9. Security Considerations、§10. Privacy Considerations は、デザイン上の思想が表現されている

2.2.1.7. 標準化過程と公式の反対意見表明

DID 仕様は 2021 年 8 月に勧告提案(Proposed Recommendation)として公開されたが、その後、Google, Apple, Mozilla の三者によって反対意見が表明されている。反対意見については W3C のワーキングルグープの公式反対意見の FAQ ページ[25]にまとめられているが、反対意見の中核部分は以下の 3 点である。

- インターオペラビリティ: データモデルを超えた部分におけるインターオペラビリティが欠落している
- 非中央化(Decentralization)の仕様と表現されているが、非中央化されていないのではないか
- 特定のブロックチェーンベースのメソッドを用いる場合のエネルギー消費の懸念

2.2.1.8. DID Rubrics

DID は、自己主権型の識別子にまつわるデータモデル標準であり、周辺技術との組み合わせで自己主権型のアイデンティティを実現できる。DID の具体的な実装仕様は DID Method 毎に規定される。たとえば、どのように「Decentralize」されるのかは、Method のデザイン毎に異なる。さらに、“decentralization” という概念の共通した定義さえ困難であることが明らかになった。

このことから、DID Method は様々な特性を持ちうるようにデザインされており、DID を用いるシステム設計者は、これらの特性を考慮しつつ Method を選択する必要がある。

---

[25] DID Working Group Formal Objection FAQ
https://www.w3.org/2019/did-wg/faqs/2021-formal-objections/

システム設計者による DID Method の選択を支援するための文書として DID Rubrics[26]が用意されている

2.2.1.9. Verifiable Credentials 標準

Verifiable Credentials は、検証可能な資格証明書である。さまざまな「証明書」のデジタル化手段として適用出来る。デジタル署名技術を用いい、発行者(Issuer)により対象者(Subject)が特定の条件を満たしている事を保持者(Holder)が示すことができるというデータモデル標準である。データモデルに加え署名アルゴリズムと署名の形式を選択し、適用することで実装できる。

(VC 図)

現時点で v1.0 が W3C で標準化されており、まもなくマイナーチェンジを伴った v1.1 がリリースされる *VC*[27]。後の節で述べるように更新版である v2.0 の策定がまさにこれから始まるところで、2〜3 年の時間をかけて標準化されてゆく。

先に述べたように、証明書中には、発行者、対象者、保持者というデジタルアイデンティティ、あるいは、デジタルアイデンティティに相当するものを指示する必要がある。すなわち、デジタルアイデンティティ技術との連携が必須である。

2.2.1.10.Verifiable Credentials 2.0

Verifiable Credentials 1.0 は 2019 年 11 月に 2 年程度の作業の後に勧告されている。DID の標準化と関わっているメンバが重なっていることもあり、2021 年 11 月に DID v1.0 の勧告提案が完了したのを機に VC 2.0 に向けた議論が始まっている。

2022 年 2 月中旬の段階で、新しいチャーターの策定作業が進行中[28]であるが、本報告書の他の章で説明するように、多言語化の仕組みを取り入れる事が決定している。

他に、以下の作業項目が決定済みである:

- 検証可能な証明書データモデルの旧バージョンで見つかった誤りに対処

---

[26] DID Method Rubric v1.1, W3C Group Note 19 November 2021
https://www.w3.org/TR/did-rubric/

[27] Verifiable Credentials Data Model v1.1, W3C Recommendation 09 November 2021
https://www.w3.org/TR/vc-data-model/

[28] PROPOSED Verifiable Credentials Working Group Charter
https://w3c.github.io/vc-wg-charter/

- クレデンシャル、プレゼンテーション、および証明のデータモデル
- データモデルのレジストリ
- 既存の暗号プリミティブを利用した証明の表現と検証のためのアルゴリズム

チャータが承認されてから 2 年間の作業期間になる見込みである。

多言語化は、VC 1.0 の仕様に Example として現れているので、一見して標準化されているように思えるが、実は言語選択の部分などを含め、国際化という意味でも標準に含まれていない。そのため、本委託事業期間中に慶応から提案[29]を行った。

2.2.1.11.DID/VC における課題

本節では、DID/VC 活用における課題を示す

インターオペラビリティ

DID や VC は抽象的なデータモデルとして定義されており、これらを実際に使うには JSON, CBOR, XML といったデータモデルの表現形式と、それらに対する署名の表現形式、加えて署名アルゴリズム[30]を組み合せる必要がある。

現時点で、VC のデータモデルと署名の表現形式として、JSON[31]と JSON Web Token[32]を組み合わせる方式と、JSON-LD[33]と Linked Data Proof[34]を組み合わせる方式の二つの方式があり、これらの間には相互互換性が無い。W3C ではこれ

---

[29] Issue#19, Standardization of Multilingual Support
https://github.com/w3c/vc-wg-charter/issues/19

[30] The Security Vocabulary, Draft Community Group Report 22 December 2021
https://w3c-ccg.github.io/security-vocab/

[31] The JavaScript Object Notation (JSON) Data Interchange Format
https://datatracker.ietf.org/doc/html/rfc8259

[32] JSON Web Token (JWT)
https://datatracker.ietf.org/doc/html/rfc7519

[33] JSON-LD 1.1, A JSON-based Serialization for Linked Data, W3C Recommendation 16 July 2020
https://www.w3.org/TR/json-ld/

[34] Data Integrity 1.0, Draft Community Group Report 12 February 2022
https://w3c-ccg.github.io/ld-proofs/

らのうちの一つを選択するということは行われないと見込まれるので、現時点では、必要に応じて選択するか両方式に対応した形での実現が必要である。

さらに、VC をどのようにやり取りするかというトランスポートの視点では、様々な方式が取りえる。たとえば、VC を Issuer からどのように発行し、Holder が受け取り保持するのか、そして、Holder がどのように Verifier に提示するのかについては、VC 技術の適用領域によって最適な方式が異なり、複数の方式が提案されているのが現状である。さらに、DID/VC を実装し提供している DID/VC 基盤ソフトウエアの設計思想により大きく異なる部分でもあり、適用方式によって基盤ソフトウエアを選択する必要があったり、逆に、基盤ソフトウエアを選択することによって適用方法に制約を受けるのが現状である。今後、選択の幅が広がって行くと考えられるが、より選択の幅を広げられるようなソフトエア基盤は標準の整備が必要であると言える。

Method の選択と適用

DID は、Method の実現方法によって、提供される DID の性質が大きく異なるものになりうる。たとえば、did:key[35]を用いる場合は DID の文字列自体が公開鍵を示しており、背後に Verifiable Data Registry を必要としない。did:ethr[36]の場合は Ethereum を基盤として過程はしているが、事実上 Ethereum のアドレスなので、ブロックチェーンに書き込む事もできるが、書き込まずにも利用が可能である。さらに、did:web[37]は Web サーバに鍵を置く事を仮定しているので DNS や Web 技術に依存している。

これらの比較から分かるように、ブロックチェーンでなければ実装出来ないということもなく、様々な技術を組み合わせて Method を実現できる。

一方、DID 技術を用いるユーザの立ち場でいうならば、いずれかの Method を選択するか、自分で構築するかということになる。選択するためには選定のための基準を定めて選ぶことになるが、この際に役に立つのが、先に示した DID Method Rubric[38]という文書である。

---

[35] The did:key Method v0.7
https://w3c-ccg.github.io/did-method-key/

[36] ETHR DID Method Specification
https://github.com/decentralized-Identity/ethr-did-resolver/blob/master/doc/did-method-spec.md

[37] did:web Method Specification, 20 December 2021
https://w3c-ccg.github.io/did-method-web/

[38] DID Method Rubric v1.1, W3C Group Note 19 November 2021
https://www.w3.org/TR/did-rubric/

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。

従って、適用領域（ドメイン、あるいは業界）毎に、グローバルに認知され共通に用いられるスキーマの合意が、グローバルな連携には欠かせない。そして、この時に、このスキーマが国際化されているだけでなく、多言語化されていることが重要である。

大学における学歴証明を一つとってみても、これを実現するのは困難である。W3C の CCG でも議論されている[39]が、日本と米国の間に限ってさえ、そもそも学歴についての考え方が異なり、それにともなってデータモデルも異なるので、双方に対応した形で整えるのは困難と考えられる。

医療系でいうと、コロナワクチン証明書は Smart Health Card[40]標準に従った形式が一つの形式として用いられており、Verifiable Credential 準拠の形式となっているが、Smart Health Card は HL7[41]という国際的に活用が進む医療情報形式である。しかし、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と考えられ、それ故、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思える。

このようなことから、スキーマの国際的な統一は極めて困難な事であると言えるため、VC 技術がグローバルに有用となるためには、何らかの技術的な対応を含めた工夫が必要であると考えられる。

---

[39] vc-ed
https://w3c-ccg.github.io/vc-ed/

[40] SMART Health Card
https://smarthealth.cards

[41] HL7 Standards
https://www.hl7.org

既存のトラストフレームワークとの連係

発行されている DID が、対象者が保持するものであるかを確認するためには、確認する場でのコントローラの存在確認をするか、DID に Verifiable Credential をあわせる必要がある。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[42]に依拠する Web PKI や日本であるなら GPKI[43]、DNS[44]と DNSSEC[45], JSON Web Key[46,47]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” [48]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

先のドメイン知識とスキーマの項で説明したように、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と考える。データレベルでの

---

[42] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
https://datatracker.ietf.org/doc/html/rfc5280

[43] 政府認証基盤(GPKI)
https://www.gpki.go.jp

[44] RFC 1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION
https://datatracker.ietf.org/doc/html/rfc1035

[45] RFC 4033: DNS Security Introduction and Requirement
https://datatracker.ietf.org/doc/html/rfc4033

[46] JSON Web Key (JWK)
https://www.rfc-editor.org/rfc/rfc7517

[47] JSON Web Signature (JWS)
https://www.rfc-editor.org/rfc/rfc7515

[48] TLS DNSSEC Chain Extension
https://datatracker.ietf.org/doc/html/rfc9102

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。

今回の事業期間中に、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[49]。

提案の骨子としては、1. 文字列として表現出来るプロパティにおいて、複数の言語による表記を並行して記載できるようにする、2. 複数言語をサポートするために、マッピングテーブルを VC の外に置きつつもデータ一貫性を保てる実装とする、3. イメージなどリソースデータも言語によって選択可能とする、という 3 点である。

現時点で提案が受け入れられ、多言語化対応の作業が今後正式に始まる予定である。

セキュリティ

本報告書では詳細には触れないが、セキュリティ視点での様々な対策が必要であることは論を待たない。さらに、DID/VC を用いた自己主権型のデジタルアイデンティティシステムにおいては、エンドユーザ自身がアイデンティティを管理するための「アイデンティティウォレット」を管理する必要があり、この視点でのセキュリティの確保が重要であり、今後十分な検討が進められる必要がある。

---

[49] Issue#19, Standardization of Multilingual Support
https://github.com/w3c/vc-wg-charter/issues/19

2.2.2. ISO/IEC

ISO における Trusted Web に関連した技術の標準化について、Trusted Web 推進協議会及び同タスクフォースに参加し、なおかつ ISO の国内審議団体に参加して国際的に検討に参加している以下の有識者にヒアリングを行った。また調査担当者である黒坂達也（慶應義塾大学）も、かつて ISO/IEC JTC1 SC27 WG5 のメンバーとして以下の有識者と協働しながら標準化の検討に従事していたことを付記しておく。

氏名（敬称略）	所属
崎村 夏彦	東京デジタルアイディア株式会社エグゼクティブパートナー/主席研究員
佐古 和恵	早稲田大学基幹理工学部情報理工学科教授
松尾 真一郎	Research Professor, Computer Science Department at Georgetown University Head of blockchain research, NTT Research Inc.

表1 ヒアリングに御協力頂いた有識者

有識者ヒアリングを行った結果、まず Trusted Web に関連した技術について、大まかには以下の通りに分類できることが示された。

- ブロックチェーン技術
- アイデンティティマネジメント技術
- 関連する情報管理手法

具体的には、前項（W3C）で説明した通り、DID 及び VC が中核的な要素技術であり、いずれも自己主権型アイデンティティ（Self-Sovereign Identity）を構成する要素である。その上で、それらに関する検討は、主に以下の 2 委員会において検討されていることが明らかになった。

① ISO/TC 307（ブロックチェーンと電子分散台帳技術に係る専門委員会）
② ISO/IEC JTC 1/SC 27（情報セキュリティ、サイバーセキュリティとプライバシー保護に関する小委員会）

次項において、それぞれの検討状況を説明する。

2.2.2.1. ISO/TC 307 の標準化動向と協調可能性

ISO/TC 307（以下 TC 307）は、ISO において第 307 番目に設置された専門委員会（Technical Committee）である。2016 年の設立当初の P メンバー（Participating member）はオーストラリア、カナダ、中国、デンマーク、フィンランド、フランス、ドイツ、イタリア、日本、韓国、マレーシア、ノルウェー、英国。また O メンバー（Observing member）は、アルゼンチン、オーストリア、ベルギー、中国、インドネシア、イラン、アイルランド、オランダ、シンガポール、スロバキア、南アフリカ、スペイン、スウェーデン、スイス、タイ、米国が参加している（P メンバー、O メンバーいずれもアルファベット順）。また我が国における国内審議団体は、一般財団法人日本情報経済社会推進協会が担当している。

当該 TC では、ブロックチェーンと電子分散台帳におけるシステム、アプリケーション、ユーザ間の互換性やデータ交換をサポートする国際標準化活動が行われており、以下のような構造で検討が進められている。

REFERENCE	TITLE	TYPE
ISO/TC 307/AG 1	SBP Review Advisory Group	Working group
ISO/TC 307/AG 2	Liaison Advisory Group	Working group
ISO/TC 307/AG 3	Digital currencies	Working group
ISO/TC 307/AHG 2	Guidance for Auditing DLT Systems	Working group
ISO/TC 307/AHG 3	Representation of physical assets as non-fungible tokens (NFT)	Working group
ISO/TC 307/CAG 1	Convenors coordination group	Working group
ISO/TC 307/JWG 4	Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Security, privacy and identity for Blockchain and DLT	Working group
ISO/TC 307/SG 7	Interoperability of blockchain and distributed ledger technology systems	Working group
ISO/TC 307/WG 1	Foundations	Working group
ISO/TC 307/WG 2	Security, privacy and identity	Working group
ISO/TC 307/WG 3	Smart contracts and their applications	Working group
ISO/TC 307/WG 5	Governance	Working group
ISO/TC 307/WG 6	Use cases	Working group
ISO/TC 307/WG 7	Interoperability	Working group

図4 ISO TC307 STRUCTURE [50]

具体的には、ブロックチェーン技術を DLT（分散型台帳技術）として定義し、関連する用語の定義、デジタル通貨や NFT（ノンファンジブルトークン）としての要件、スマートコントラクトとしての要件、セキュリティ・プライバシー・アイデンティティに関する検討、各種ユースケースの検討等を行っている。

[50] 出所 ISO サイト: TECHNICAL COMMITTEES ISO/TC307 Blockchain and distributed ledger technologies- https://www.iso.org/committee/6266604.html

これらのうち、DLT に関する検討は、ISO/TC 307 N713（＝ISO/NP 7603）Decentralized Identity standard for the identification of subjects and objects（主体と対象を識別するための非中央集権型アイデンティティ標準規格）という N 文書として編さんされている。具体的には、定義されたアーキテクチャ群全体でアイデンティティを管理するための高品質なブロックチェーンと DLT システムのコストと時間の効率的な開発を提供するために開発者をサポートすることを目的に、ブロックチェーンと DLT システムの設計の中で、検証可能なクレデンシャル（VC）と連携して、主体（法人と自然人）および対象、また資産の分散型かつ自己主権的な識別の設計と使用のための規格として定めている。この規格において、ISO のみならず、W3C、GLEIF、IETF、ITU、IEEE などの他の標準化団体、DIF、TOIP、Kantara Initiative などの非標準化グローバルコンソーシアムから入手できる識別規格を参照している。

一方、DLT の検討は、ISO 以外のブロックチェーン・コミュニティとは、必ずしも検討が整合していないとの指摘が、TC 307 のメンバーである松尾氏からあった。たとえば DLT は Distributed Ledger Technology の略だが、ブロックチェーン・コミュニティは当該技術概念を表現する際には Distributed ではなく Decentralized を用いる。これはブロックチェーン・コミュニティが中央集権的なものの対義語として、時に社会変革の有力なツールとしての価値を表現することを目的とすることが少なくないことと関係しており、その場合は単なる技術的特徴である Distributed（分散）ではなく、非中央集権と訳されることの多い Decentralized という用語が使われることが多いことからもうかがえる。

これは Trusted Web の標準化を検討する際に重要な示唆を含んでいる。すなわち、Trusted Web の標準化の目的として、単に技術手段の提供を目指すのか、そうではなく Web という社会インフラとも言えるシステム及びそれを構成する技術を刷新することによる社会変革を目指すのかが問われることになるからである。

仮に前者、つまり技術手段の提供を指向するのであれば、TC 307 との協調は標準化の手段の一つとして妥当である可能性がある。しかし後者を目指すとしたら、TC 307 との協調だけでは必ずしも十分ではない。むしろその場合は、ブロックチェーン・コミュニティや、TC307 自体もリエゾンしている、ISO 以外の SDO、すなわち W3C、GLEIF、IETF、ITU、IEEE などの他の標準化団体、DIF、TOIP、Kantara Initiative などの非標準化グローバルコンソーシアム等との協調が必要となる。

また関連して松尾氏からは、海外の様々なブロックチェーン・コミュニティと連携した検討を進めている経験を踏まえ、明示的なリエゾン先として示される SDO はさておき、それ以外のブロックチェーン・コミュニティは、ISO TC 307 の動向をほとんど認識していない（認識する意向もない）可能性が高い、との指摘もあった。そのため、そうしたコミュニティの中で TC 307 の動向に

関心を払う者はごく少数であると考えられるため、Trusted Web の標準化活動に投入できる資源（とりわけ人的資源）に制約がある場合、TC 307 への取組を戦略的に劣後させる可能性も視野に入れるべきだとの提案もあった。

2.2.2.2. ISO/IEC JTC 1/SC 27 の標準化動向

ISO/IEC JTC 1/SC 27（以下 SC 27）は、1990 年に ISO/IEC JTC 1 によって設置された。SC27 は、セキュリティ技術分野の標準化を担当していた SC20 のうち、秘密鍵技術（WG 1）、公開鍵技術（WG 2）、データ暗号化プロトコル（WG 3）が解散となったことを受けて結成されたものである。この組織変更により、SC 27 は SC 20 の作業を引き継ぐだけでなく、IT セキュリティ技術の他の分野にも範囲を拡大することに成功し、現在は Sub Committee ではあるが多岐にわたる検討を進めている。

2021 年 7 月に策定された SC27 STANDING DOCUMENT SD11:2021(2)[51]によると、SC27 のスコープとして、「情報セキュリティ、サイバーセキュリティ、プライバシー保護に関する規格の策定」と規定している。これには、セキュリティとプライバシーの両方の側面に対処するための、以下のような一般的な方法、技術、ガイドラインが含まれる。

- セキュリティ要求の把握方法
- 情報及び ICT セキュリティの管理、特に情報セキュリティ管理システム（ISMS）標準、セキュリティプロセス、セキュリティ管理及びサービス
- 暗号化及びその他のセキュリティメカニズム（情報の説明責任、可用性、完全性及び機密性を保護するためのメカニズムを含むが、これらに限定されない）
- セキュリティ管理支援文書（用語集、ガイドライン、セキュリティ構成要素の登録手順など）
- アイデンティティ管理、バイオメトリクス、プライバシーのセキュリティ
- 情報セキュリティマネジメントシステム分野の適合性評価、認定、監査要件
- セキュリティ評価基準及び方法論

SC27 は以下に図示する構造で作業グループ（WG）等が設置されている。

---

[51] SC27 STANDING DOCUMENT SD11:2021(2) - Overview of SC 27 Structure, Members and Work Programme https://www.din.de/resource/blob/78920/3b04211f9d8da787812569c5ab97be94/sc27-sd11-work-programme-data.pdf

REFERENCE	TITLE	TYPE
ISO/IEC JTC 1/SC 27/AG 1	Management Advisory Group	Working group
ISO/IEC JTC 1/SC 27/AG 2	Trustworthiness	Working group
ISO/IEC JTC 1/SC 27/AG 3	Concepts and Terminology	Working group
ISO/IEC JTC 1/SC 27/AG 5	Strategy	Working group
ISO/IEC JTC 1/SC 27/AG 6	Operations	Working group
ISO/IEC JTC 1/SC 27/AG 7	Communication and Outreach (AG-CO)	Working group
ISO/IEC JTC 1/SC 27/CAG	Chair's Advisory Group	Working group
ISO/IEC JTC 1/SC 27/JWG 6	Joint ISO/IEC JTC1/SC 27 - ISO/TC 22/SC 32 WG : Cybersecurity requirements and evaluation activities for connected vehicle devices	Working group
ISO/IEC JTC 1/SC 27/WG 1	Information security management systems	Working group
ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms	Working group
ISO/IEC JTC 1/SC 27/WG 3	Security evaluation, testing and specification	Working group
ISO/IEC JTC 1/SC 27/WG 4	Security controls and services	Working group
ISO/IEC JTC 1/SC 27/WG 5	Identity management and privacy technologies	Working group

図5 ISO/IEC JTC1 SC27 STRUCTURE [52]

WG は 1～5 が設置されており、それぞれの関係は以下のように整理されている。

[52] 出所 ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection https://www.iso.org/committee/45306.html

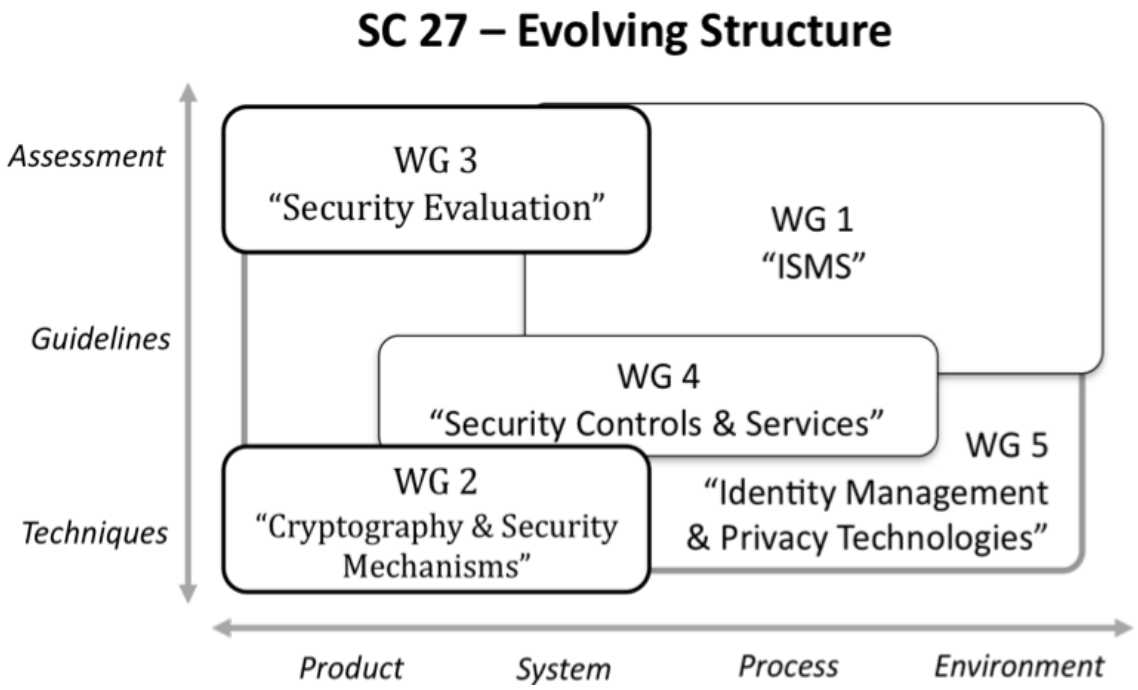

図6 SC27 Evolving Structure [53]

このうち、Trusted Web に関係する WG は、WG 5（Privacy, Identity management and Biometrics：プライバシー、アイデンティティ管理とバイオメトリクス）が最も妥当である指摘が、すべての有識者から示された。有識者のうち崎村氏と佐古氏、また前述の通り調査主体である黒坂達也は、いずれも WG 5 のメンバーとして国際的な標準化活動にも従事しており、また SC 27 全体の状況も把握していることから、その指摘は妥当だと考えられる。

WG 5 は、大きくは以下の 3 項目で構成されている。

- アイデンティティ管理
- プライバシー
- バイオメトリクス

WG 5 全体において多くの参照元となる重要な標準は、ISO/IEC 29100:2011（プライバシーフレームワーク）である。この標準は 2017 年 6 月に JIS X

[53] 出所 ISO/IEC JTC1
https://jtc1history.wordpress.com/isoiec-jtc-1-subcommittees-2/sc-27-r2013/

9250:2017（プライバシーフレームワーク（プライバシー保護の枠組み及び原則））として我が国でも発行された。この ISO/IEC 29100:2011 を軸として前述の 3 項目の位置づけを整理したのが以下の図である。

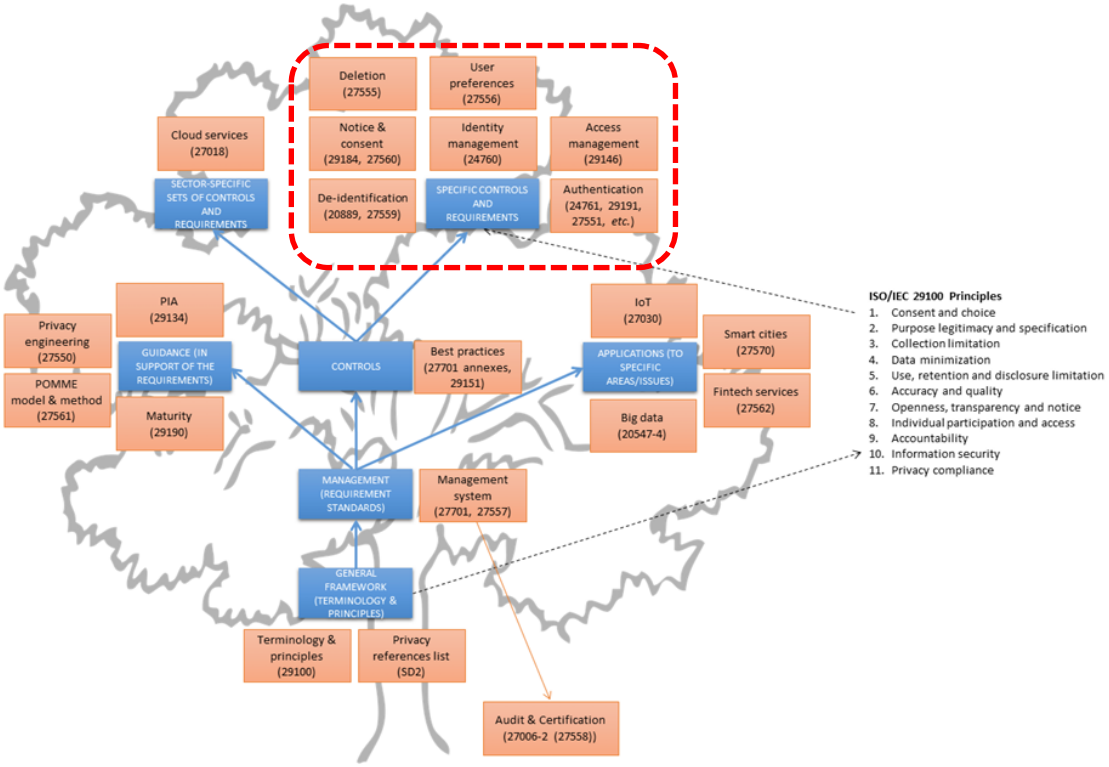

図 7 ISO/IEC JTC 1/SC 27/WG 5 N2732 （WG 5 SD1 Roadmap）[54]

このうち Trusted Web に直接関係するものは、図において赤破線で示した「アイデンティティ管理」の領域だと考えられることから、これらの項目について概要を説明する。まずアイデンティティ管理領域の全体構成を以下の図で示す。

[54] 出所 ISO/IEC JTC 1/SC 27/WG 5 N2732（WG 5 SD1 Roadmap）※赤破線は筆者記入
https://www.din.de/resource/blob/259644/c93dd96ef5f9c690f86cf93443bbbb4f/sc27wg5-sd1-data.pdf

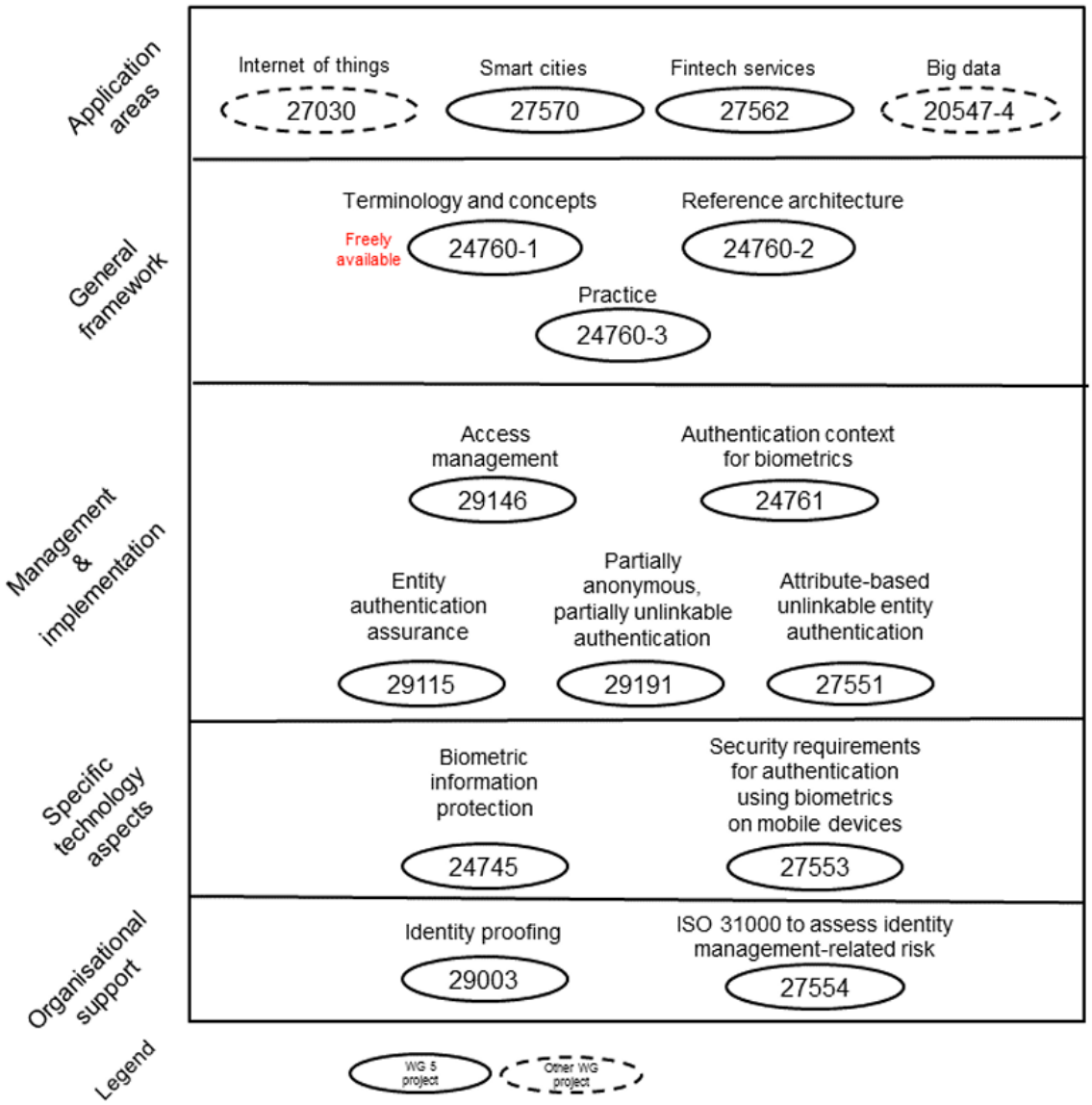

図8 ISO/IEC JTC 1/SC 27/WG5 N2732（WG 5 SD1 Roadmap）[55]

このうち、General framework として位置づけられている ISO/IEC 24760 シリーズが他の標準の参照元となっているため、このメンテナンスが大きな対象となる。ISO/IEC 24760 シリーズは、情報システムがビジネス、契約、規制、および法的な義務を満たすための情報システム管理を実現する目的で、アイデンティティ管理の基本概念と運用構造を規定する。

[55] 出所 ISO/IEC JTC 1/SC 27/WG5 N2732（WG 5 SD1 Roadmap）
https://www.din.de/resource/blob/259644/c93dd96ef5f9c690f86cf93443bbbb4f/sc27wg5-sd1-data.pdf

ISO/IEC 24760-1:2019（IT セキュリティとプライバシーーアイデンティティ管理のフレームワーク：パート１ 用語と概念）[56]は、情報処理システムが一般に、接続された人、機器、ソフトウェアなどのユーザに関するさまざまな情報を収集し、その情報に基づいて意思決定を行うことから、多くの組織にとって、ID 情報の適切な管理は、組織のプロセスのセキュリティを維持するために不可欠であるという認識の下で、2011 年に初版が発行され、2019 年に改訂された。

特に、個人にとって正しいアイデンティティ管理はプライバシーを保護するために重要なものであると規定し、アイデンティティ管理の用語及び概念を規定し、同分野における共通理解を促進することを目的に編さんされた。具体的には、このようなアイデンティティに基づく判断が、アプリケーションやその他のリソースへのアクセスに関わるものであり、アイデンティティベースの決定を行うシステムを効率的かつ効果的に実装する必要性に対処するため、個人、組織、または個人もしくは組織の代理として動作する情報技術コンポーネントを特徴付けるのに役立つデータの発行、管理、および使用のためのフレームワークを規定している。

また ISO/IEC 24760-2:2015（IT セキュリティとプライバシーーアイデンティティ管理のフレームワーク：パート２ 参照アーキテクチャと要件）[57]は、前述の ISO/IEC 24760-1:2019 と共通の目的を有しつつ、主要なアーキテクチャ要素およびそれらの相互関係を含むアイデンティティ管理システムのための参照アーキテクチャを定義している。これらのアーキテクチャ要素は、アイデンティティ管理の配備モデルに関して記述されており、システムの展開および運用に関与する利害関係者の目的を 満たすことができるように、その設計および実装の要件を規定している。特に、アイデンティティ情報の処理に関連する他の国際標準の実装、特に前述した ISO/IEC 29100 シリーズ（以下参照）のための基礎を提供することを意図している。

- ISO/IEC 29100, Information technology — Security techniques — Privacy framework
- ISO/IEC 29101, Information technology — Security techniques — Privacy reference architecture
- ISO/IEC 29115, Information technology — Security techniques — Entity authentication assurance framework
- ISO/IEC 29146, Information technology — Security techniques — A framework for access management

[56] https://www.iso.org/standard/77582.html

[57] https://www.iso.org/standard/57915.html

これらISO/IEC 24760シリーズを基礎に、管理と実装、個別技術、ユースケース等の検討を全般に進めているが、現在ISO/IEC 24760-2の改訂作業が始まったところである。具体的には、ISO/IEC 24760-2.2としての発行を目指した検討が進められており、2021年7月に30.60（投票締切、コメント終了）まで至ったものの差し戻され、2022年1月時点では30.20（CD study ballot initiated）という状況にある。

このほかアイデンティティ管理領域では、ユーザ認証の標準であるISO/IEC 29115（Entity authentication assurance framework）について、多要素認証等の技術動向の反映や、前述のISO/IEC 24760-1:2019との整合やISO/IEC 24760-2の改訂を念頭においた改訂の検討が進んでいるが、Trusted Webの標準化とは現時点では直接的には関係が薄いと考えられる。

2.3. 今後の戦略 - 標準化活動への展開

本節では、標準化活動への展開可能性についてまとめる。

2.3.1. W3C および IETF における提案活動の可能性

今回のユースケースにおける議論を進める過程で、Trusted Web ホワイトペーパ 1.0 で議論した 4 つの機能 (Identifier, Trustable Communication, Dynamic Consent, Trace) の整理をもう一段進める必要があることが明らかになっている。

一方、Verifiable Credentials についての調査の過程で特定した課題のうちのいくつかは、Trusted Web を実現するためにも解決しなければいけないことでもある。今回の調査研究の成果から、以下のように整理できる。

A 群) 今回のユースケースの議論で、対象領域を絞りつつ、議論をできた課題:

- 既存のトラストフレームワークとの連係
- ドメイン知識とスキーマ
- 国際化と多言語化

B 群) Trusted Web の実現のために広く議論され、標準化された上で、デプロイされる必要がある課題:

- インターオペラビリティ
- ドメイン知識とスキーマ
- 国際化と多言語化
- トランスポート
- セキュリティ

これらのうち B 群については、一部は既に議論を始めているものもあり、各 SDO でも課題として認識されているものもある。これらの整理を、ホワイトペーパ ver 2.0 の策定過程で整理し、対外的に発信してゆくことが重要であろう。

Verifiable Credentials を中心とした取り組みは、W3C においては主には特定のアプリケーションに寄らない、抽象度の高いデータモデルについての議論である。従ってデータモデルに関連した部分については W3C での議論が自然である。

また、データ自身をどのようにやり取りするのかというトランスポートの視点では、Internet Engineering Task Force (IETF)にて標準化を進める必要もあり、実際、Verifiable Credentials に関連した標準化の一部は IETF で行われている。

2.3.2. 各対象アプリケーション領域におけるデータモデルの標準化

一方、データモデルにおけるドメイン知識についての議論にあるように、適用対象となる業界毎に扱うデータは異なり、業界内でデータモデルが整っている業界もそうでない業界もある。また、仮に国内での業界標準があったとしても、国際的に共通したデータモデルが存在しない場合もある。すなわち、業界毎にデータモデルの成熟度にはばらつきがあるのが実情である。しかし、高度かつグローバルなデータ流通を志向するのであれば、データモデルは適用するアプリケーション領域ごとにグローバルスタンダードとして整える必要がある。そのような整備が進まない限り、Trusted Web によってデータの正しさが検証できたとしても、十分な効果は得られないであろう。従って、Trusted Web を適用するためには、業界によっては、データモデルの共通化を合わせて進める必要があり、Trusted Web の適用自身がデータモデル共通化を後押しする形にできる可能性はあるだろう。

2.3.3. ISO/IEC JTC 1/SC 27 WG 5 との協調可能性

前項で示した通り、Trusted Web との協調可能性を探る上で ISO/IEC JTC 1/SC 27 において優先的な対象となるのは WG 5 であり、特にアイデンティティ管理領域が直接的な働きかけの対象となると考えられる。当該領域では前述の通り、現在 ISO/IEC 24760-2 の改訂作業が開始されたところである。

このため、ISO/IEC 24760-2 の改訂作業に参加することで協議・提案する可能性について、崎村氏と佐古氏に確認したところ、以下のような指摘があった。

- 可能性の有無でいえば、可能性はある。
- しかし Trusted Web が現時点でそこまで技術的に成熟していないことから、よほど ISO/IEC 24760-2 の改訂作業で特定された課題に対して Trusted Web が直接的な解決策とならない限り、受け入れ可能性は低い。
- また、現状では Trusted Web がどのようなものかを理解してもらえていない状況のため、まず理解を踏まえて協調してもらうための「仲間作り」から始めるべきである。
- そう考えると、差し戻しにより 30.20（CD study ballot initiated）の段階にあるものの、検討はすでに進んでおり、あまり現実的とはいえないかもしれない。

このような見通しは、崎村氏と佐古氏、また TC 307 の委員である松尾氏も含め、ISO におけるデジュール標準の位置づけ自体が社会的に変化しつつあるという、以下のような認識に基づくものでもある。

- ISO による標準は、今日においても権威としての位置づけを保っていることは事実である。
- 一方でデジタル技術の対象が極めて広範囲に広がり、またそれらが細分化されて社会に深く浸透し、さらに技術革新の速度が高速化したことで、技術開発に従事するエンジニアにとっての標準化の意味や価値は変化してきている。
- 特にアイデンティティ管理のような領域はシステムの規模が極めて大きくなりやすいことから、ISO のような「表の標準化機構」だけでなく、実装との橋渡しをするような「ブリッジ役としての機構・団体」が存在するのではないか。

実際にこうした認識は、前述した通り、ISO TC 307 において W3C や Kantara Initiative と連携していること、また ISO/IEC JTC 1/SC 27 WG 5 において取組が複雑化していることなどからも裏付けられる。その上で、そうした認識を踏まえつつ、Trusted Web が目指しているのが、仮にインターネットや Web 技術を社会インフラとして機能しうるものにするための改善なのだとしたら、ISO だけでなくこうした「ブリッジ役としての標準化」を担う存在との連携の模索も期待される。

2.3.4. デジュール標準化の取組に向けたインプリケーション

ISO をはじめとしたデジュール標準による Trusted Web に関連した技術の標準化について、現時点を総合すると、ISO TC 307 よりも ISO/IEC JTC 1/SC 27 WG5 が期待される。また、より具体的には、WG 5 の中でも「アイデンティティ管理」領域での取組が対象として考えられる。

当該領域においては、まず ISO/IEC 24760-2 の改訂作業が進んでおり、こうした既存の検討に関与する方法が考えられる。また、新たに PWI（Preliminary Work Item：予備業務項目）を起こして、NWIP（New Work Item Proposal：新業務項目提案）を進めていくという、標準化のプロセス通りの手順により進めていくという方法もありうる。特に Trusted Web が DID/VC のような新たなアイデンティティ管理技術に関連していると考えるのであれば、後者の方法についても検討の余地はあるといえる。

一方で、こうしたデジュール標準化の伝統的なアプローチについては、以下のような論点に基づき、その合理性を評価する必要がある。

- 時間が大幅にかかることをどのように評価するか
- 将来にわたって標準化にどの程度の（人的）資源を割けるか
- デジュール標準の社会的位置づけが変化する中で Trusted Web の目指す世界観や関連する技術のコミュニティとの整合が取れるか

こうした論点の評価においては、①Trusted Web そのものの目的、②Trusted Web の標準化の目的、③Trusted Web そのものとその周辺のケーパビリティ、④関連する標準化活動の状況、等を定めることが求められることから、標準化に係る戦略や作戦の具体化に向けて、今後 Trusted Web 推進協議会における検討で何らかの合意を図ることが強く期待される。

一方、こうした検討を進める上で、デジュール標準と実装の間をつなぐ役割を担う機関との連携を模索することは、戦略や作戦の如何に関わらず有益であることが、有識者から示唆された。特にこうした機関との協議や連携は、デジュール標準の様々な局面や、フォーラム標準等にも参加しており、あらゆる標準化における協調先の開拓、いわゆる「仲間作り」そのものであると考えれば、Trusted Web の戦略や作戦を問わず、必要な取組となる。具体的には、以下のような機関が挙げられた。

機関名	拠点となる地域	概要
NIST	米国	National Institute of Standards and Technology：米国立標準技術研究所。米国政府機関で利用される情報セキュリティ技術等の標準化を行う、商務省傘下の機関。ISO/IEC JTC 1/SC27 WG 5 等の米国の国内審議団体でもある。
MITRE	米国	米国の連邦政府が資金を提供するセキュリティ分野の非営利組織であり、R&D センターと官民のパートナーシップを通じて、国の安全性、安定性、福祉に関する事項に取り組んでいる。NIST の連邦研究開発センター（Federally funded research and development center：FFRDC）の運営主体でもある。
ENISA	欧州	European Network and Information Security Agency：欧州 ネットワーク情報セキュリティ機関。ネットワークと情報に関する欧州の中心的な機関で、 EU 加盟国や民間の部門と緊密に連携することにより、サイバーセキュリティ対策を向上するためのアドバイスや提言を行う。 また、国家情報セキュリティに関する EU の政策と法案の開発や実施もサポートする。
Kantara Initiative	米、欧、豪、日	アイデンティティ管理に関する技術仕様と推奨事項を提言する非営利団体。崎村氏は主要メンバーの一人でもある。

表 2 連携を想定すべき機関