TTCに寄せて

分散型アイデンティティを公共財として実現するための標準形成

～TTC会長表彰を受賞して～

SPRIN-D(ドイツ連邦 飛躍的イノベーション機関)
安田　クリスチーナ

1．はじめに（Introduction）

国際的な技術標準の世界では、進展は通常、年単位ではなく数十年単位で測られる。そのような文脈の中で、過去5年間、私はOpenID FoundationのDigital Credentials Protocols Working Groupの共同議長を務め、OpenID for Verifiable Credentialsに関する3つの最終仕様（OpenID4VP、OpenID4VCI、HAIP）のエディタを担当し、さらにIETF RFC 9901（Selective Disclosure for JSON Web Tokens）の著者として活動してきた。また、W3C Verifiable Credentials Working Groupの共同議長を務めたほか、ISO/IEC JTC 1/SC 17のWG10およびWG4においてモバイル運転免許証（mDL）関連の標準化に参加し、W3C Digital Credentials APIにも貢献してきた。

私がデジタル・アイデンティティ及びその標準化に取り組み始めた原点は、NGOにおける現場での活動にあった。私が2016年から2022年の間に運営していたNGOでは、バングラデシュの難民やザンビアのシングルマザーといった周縁化された人々に対し、分散型アイデンティティを用いて本人性や信頼性を証明できる手段を提供し、それまでアクセスできなかった機会やサービスへの道を開くことを目指していた。こうした取り組みを通じて、デジタル・アイデンティティは本質的に公共財であり、誰にとってもアクセス可能で、かつ実用的でなければならないという信念が、私の中で確かなものとなった。

インターネットそのものに地理的な境界が存在しない以上、インターネット上のデジタル・アイデンティティもまた、国境によって制限されるべきではない。このように国境、分野、実装をまたいで機能させるためには、デジタル・アイデンティティは個別最適化された断片的な解決策に依存することはできない。その基盤となるインフラは、堅牢な国際技術標準の上に構築される必要がある。

同時に、NGOでの現場経験は、当時の標準化の状況がその理想に大きく及んでいないことも明確に示していた。ある領域では標準そのものが存在せず、別の領域では既存の標準があまりにも複雑で、実験的な環境を超えて展開することが事実上不可能であった。私自身が実施したパイロットプロジェクトを通じて学んだのは、デジタル・アイデンティティにおいて最も難しいのは「一度動くことを証明すること」ではなく、使いやすさやプライバシーを損なうことなく、デバイス、ベンダー、法域を超えて繰り返し機能させることである、という点であった。

デジタル・アイデンティティは公共財であるという確信と、それを支える標準が実用段階に達していないという現実が重なり合い、私は現場での実装から、標準そのものを作る側へと軸足を移す決断をしたのである。

同時に、私がデジタル・アイデンティティの分野に関わり始めた当初、この分野は非常に強く二極化していた。一方には、自己主権型アイデンティティ（Self-Sovereign Identity）を支持し、分散化を重視し、ブロックチェーン技術を探求しながら、既存のフェデレーテッド・アイデンティティ・システムを特にプライバシーの観点から強く批判する人々がいた。他方には、すでに数百万、あるいは数十億規模で運用されているシステムで使われる標準を策定してきた実務家がおり、新しいアプローチの多くは大規模運用の現実を十分に理解していないと見なされていた。この分断は非常に深く、「クレデンシャル」という用語の定義といった基本的な概念ですら、継続的な議論の対象となっていた。

私は最初から、この二つの立場の中間に身を置くことになった。一方ではNGOを運営し、自己主権型アイデンティティのプロトタイプを構築し、ユーザー主導や分散化の新しいモデルを試していた。他方では、AccentureやMicrosoftといった、グローバル規模でアイデンティティ・システムを構築・運用してきた企業に所属し、新しいデジタル・アイデンティティの考え方をどのように現実のシステムへ落とし込めるか

を模索していた。両方の世界を間近で見たことで、実装が容易で、かつスケール可能な標準がなければ、どちらのビジョンも成功し得ないという事実を無視することはできなかった。

2．分散型アイデンティティを支える中核的標準（Core Standards Underpinning Decentralized Identity）

分散型アイデンティティ・システムでは、複数の異なる役割が相互に関与する。Issuer（あるいはProvider）は、ユーザーの属性（本人確認情報、資格、権利など）を表明するクレデンシャルを生成し、署名する信頼された主体である。これらのクレデンシャルは、ユーザー（Holder）が管理する認証済みアプリケーションである Wallet に保存される。ユーザーが自身について何かを証明する必要がある場合、Wallet が関連するクレデンシャル情報を Verifier（Relying Party）に提示する。これらのやり取りを支えるのがトラストモデルであり、Issuer、Wallet、Verifier がどのように認証・認可され、鍵、証明書、メタデータに対する信頼がどのように確立されるかを定義する。このモデルにおける重要な変化は、ユーザーデータが Issuer から Verifier へ直接流れるのではなく、ユーザー自身がいつ、どのようにデータを共有するかを制御する点にある。

このモデルを実際に、かつエコシステム横断で機能させるためには、Issuer、Wallet、Verifier 間の相互運用性を確保する必要がある。当時、この課題を包括的かつ広く採用された形で解決する標準は存在していなかった。そのため私は、Issuer–Wallet 間および Wallet–Verifier 間の相互作用を規定するプロトコルと仕様の策定に標準化活動を集中させ、大規模なデジタル・アイデンティティ・システムを構築するための強固で持続可能な基盤を築くことに注力した。

この取り組みの直接の成果が、OpenID for Verifiable Credential Issuance（OpenID4VCI）および OpenID for Verifiable Presentations（OpenID4VP）である。OpenID4VCI は、Issuer

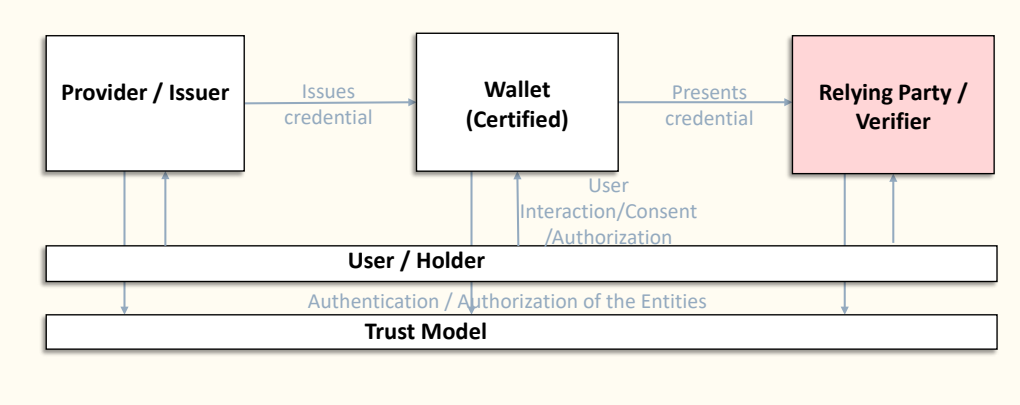

図１　分散型アイデンティティ　エコシステムの概要

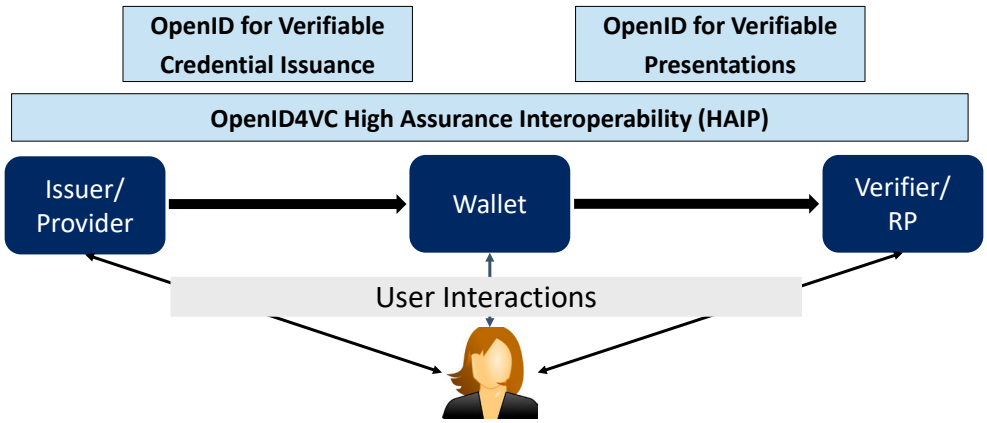

図２　OID4VC: OpenID for Verifiable Credentials プロトコル群

がクレデンシャルを安全にユーザーの Wallet に発行する方法を定義し、OpenID4VP は、Verifier がクレデンシャルの提示を要求し、Wallet がそれをオンラインで標準化された相互運用可能な形で提示する方法を定義している。

次の課題は、これらのプロトコル上でやり取りされるクレデンシャル形式であった。W3C Verifiable Credentials Data Model（VCDM）は、分散型アイデンティティ向けに設計された最初のクレデンシャル形式であったが、VCDM の定義する複数の表現形式は難しいトレードオフをもたらした。JSON-LD と Data Integrity（旧 Linked Data Proofs）はリンクドデータの利点を提供する一方で、容易に複雑化するリスクがある。一方、JWT ベースのクレデンシャルははるかに実装しやすいものの、選択的開示をサポートしていなかった。

ここで、選択的開示は妥協できないプライバシー要件であった。BBS+ 署名を用いて JSON-LD VCDM クレデンシャルで選択的開示を実現しようとする取り組みも進められていたが、このアプローチはプラットフォームやエコシステムを越えてスケールさせるのは難しいことが明らかになった。このギャップこそが、私が Selective Disclosure for JSON Web Tokens（SD-JWT）の策定を主導するきっかけである。目的は、mdoc など他のクレデンシャル形式と競合するためではなく、実装容易性と強固なプライバシー保証を両立する、シンプルな JWT ベースのクレデンシャル形式を実現することだった。

OpenID4VCI、OpenID4VP、SD-JWT はすでに、相互運用性、セキュリティ、プライバシーが重要となる実運用環境で採用されている。欧州デジタル・アイデンティティウォレット（EUDIW）のエコシステムでは、OpenID4VCI によりクレデンシャルが認証済みウォレットに発行され、OpenID4VP によって公的・民間双方の Verifier に対するオンライン提示が可能となっている。SD-JWT は、必要最小限の属性のみを開示する選択的開示を実現するために、こうしたシナリオで活用されつつある。政府発行の身分証明にとどまらず、金融分野での本人確認や強固な認証、教育分野での学位・証明書の発行と検証、企業やプラットフォームにおける従業員クレデンシャルなど、幅広い領域で採用が進んでいる。これらの分野において、OpenID4VCI、OpenID4VP、SD-JWT の組み合わせは、発行・保持・提示を一貫して支える共通の標準基盤を提供している。

3．OpenID4VC の成功を支えた要因（Key Factors Behind the Success of OpenID4VC）

OpenID4VCI および OpenID4VP の設計にあたっては、いくつかの設計原則が成功に大きく寄与した。最も重要な原則の一つは、「必要性が明確な場合を除き、新たなプロトコル群をゼロから定義しない」という点である。当時、他の提案の多くは独自設

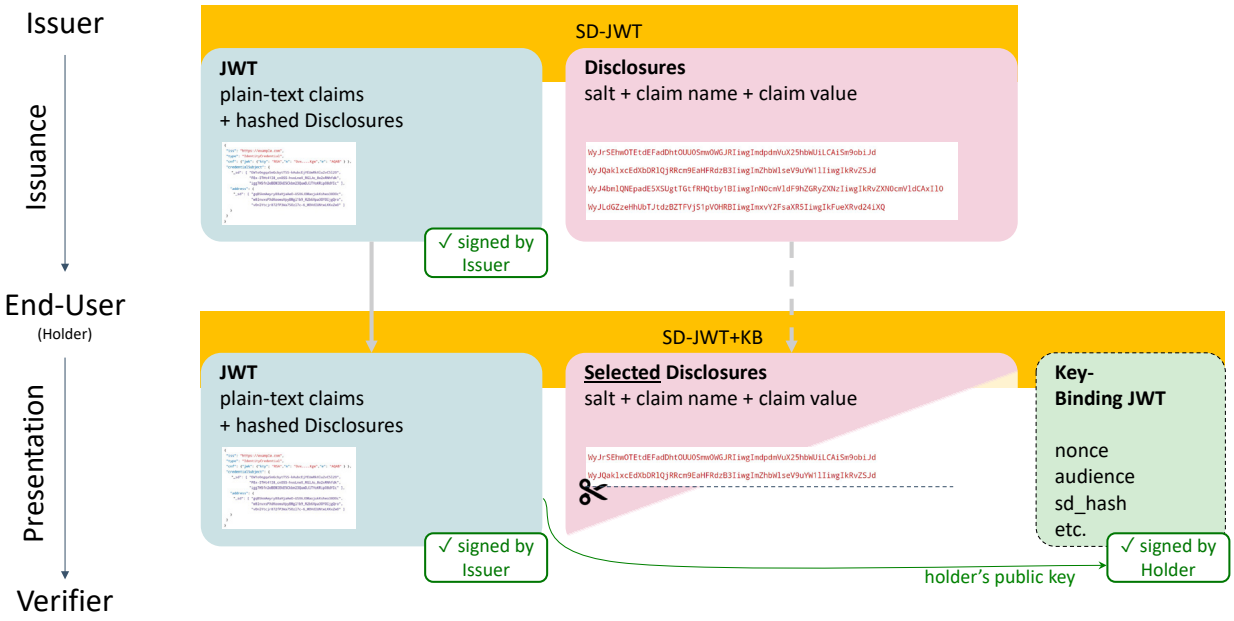

図３　SD-JWT の選択的開示の概要

計の新規プロトコルに依存しており、それはセキュリティ保証を難しくし、採用の障壁を大きく高めていた。これに対し、OpenID4VCI と OpenID4VP は、OAuth2.0 や OpenID Connect といった、すでに広く展開され十分に理解されている標準の上に意図的に構築された。その結果、成熟したセキュリティ特性、実装経験、既存の開発者エコシステムを継承しつつ、検証可能クレデンシャルという新たなユースケースを拡張として実現することができた。

もう一つの重要な設計判断は、単一のクレデンシャル形式に収束していなかった現実を前提とした点である。ISO/IEC 18013-5 の mdoc、IETF の SD-JWT、W3C Verifiable Credentials など、各エコシステムは異なるアプローチに投資していた。特定の形式を「勝者」として選ぶのではなく、プロトコルをクレデンシャル形式非依存とすることで、Issuer、Wallet、Verifier が複数形式を並行してサポートできるようにした。この分離により、コアとなるプロトコルを変更することなく、エコシステムが時間とともに進化する余地が確保された。

暗号鍵管理およびトラスト管理についても、同様の考え方が採用された。分散型アイデンティティ・システムは暗号鍵操作に大きく依存するため、Issuer、Wallet、Verifier が署名検証のための正しい公開鍵を取得し、それらの鍵に対するトラストを確立できることが不可欠である。しかし、すべてのユースケース、プラットフォーム、規制環境に適合する単一の仕組みは存在しない。そこで OpenID4VCI と OpenID4VP では、実装者が自ら選択した鍵管理・トラストモデルを組み込めるよう、明確な拡張ポイントを定義した。この柔軟性により、強いセキュリティ要件やポリシー要件を満たしつつ、組織や国境を越えた相互運用が可能となった。

OpenID4VP の中核には、Verifier が要求するクレデンシャル要件を正確に表現するためのクエリ言語が存在する。設計初期には、Decentralized Identity Foundation で策定された Presentation Exchange を採用した。これにより、提示要件表現そのものではなく、OpenID4VP および OpenID4VCI の拡張性、セキュリティ、プロトコル全体の構造設計に注力することができた。

しかし、実装が進むにつれて、当初のアプローチが不必要に複雑であり、採用を妨げているという一貫したフィードバックが実装者から寄せられた。このフィードバックを真摯に受け止め、設計を見直し、実運用のニーズにより適合した形へとクエリ機構を再設計した。その結果、表現力とセキュリティを維持しつつ、実装の敷居を大きく下げる、よりシンプルで扱いやすいモデルが実現した。この経験は、標準設計において、理論的な正しさだけでなく、開発者体験に根ざした実用性がいかに重要であるかを改めて示した。

OpenID4VCI や OpenID4VP についてよく見られる誤解の一つに、「そのままで完全に相互運用できるはずだ」という期待がある。前述の通り、これらのプロトコルは、異なるクレデンシャル形式、トラストモデル、セキュリティ要件、規制環境に対応するため、高い柔軟性を意図的に備えて設計されている。この柔軟性は大きな強みである一方、相互運用性を確保するにはプロファイルが必要となる。プロファイルは、仕様中の選択肢のうち、実装において必須とすべき要素を明確に定義するものである。

この課題に対応するために策定されたのが High

Problem		Solution
A lot of entirely new Protocols. (Hard to get security right, steep learning curve)	⇒	Building upon currently widely used protocols: OAuth 2.0 and OpenID Connect. (Secure, already understood)
No clear winner among Credential Formats	⇒	Designing a protocol agnostic to the Credential Formats.
No one way to do key management.	⇒	Designing a protocol agnostic to the key management mechanism.
Participating entities cannot typically establish trust upfront, using traditional mechanisms.	⇒	Flexibility in Trust Management. Third Party Trust.

4

図４　特定した課題とその解決方法

Assurance Interoperability Profile（HAIP）である。HAIP は、特に政府発行クレデンシャルのような、高いセキュリティ水準を要求するユースケースを満たすための制約と要件を定義している。これは OpenID4VP 及び OpenID4VCI の唯一のプロファイルであることを意図したものでもなく、将来の革新を妨げるものでもないが、現時点で最も重要かつ要求の厳しいユースケースに対する具体的で実装可能な基準を提供するものである。HAIP は、汎用仕様と特定の政策主導エコシステムをつなぐ橋渡しとして、オープン標準がどのように拡張性と実運用性を両立できるかを示している。

プロファイルの必要性は、しばしば相互運用性の欠如と誤解される。しかし私はこれを成熟の指標だと捉えている。汎用プロトコルは可能性の空間を定義し、プロファイルは独立したチームが一貫して実装できる具体的な運用モードを定義する。重要なのは、プロファイルを明示的かつ検証可能な形で定義し、実際の展開要件と整合させることである。

4．調和への道（Path to Harmonization）

ここで、OpenID4VP と ISO/IEC 18013-5 の設計目標および適用範囲の違いが、どのようにして標準化団体間の緊張を生み、並行して進んでいた取り組みがより広範な相互運用性の課題へと発展していったかを認識することが重要である。

この緊張の根底には、プロトコル設計思想の違いがあった。ISO は、単一のクレデンシャル形式である mdoc に特化し、オフライン提示を主な想定としたプロトコルを開発し、即時に利用可能な相互運用性を提供した。その結果、クレデンシャル形式、リクエスト／レスポンス構造、NFC や BLE といった安全な接続確立手段が密接に結合された設計となった。一方、前述の通り、OpenID4VP は当初からクレデンシャル形式非依存で、オンライン提示を想定し、HTTPS/TLS といった既存のインターネット上の安全な通信基盤を利用する形で設計されている。

この違いは、ISO において mdoc のオンライン提示をサポートする必要が生じた際に、より顕在化した。その際、OpenID4VP を採用するのではなく、ISO の作業部会は既存のプロトコルを拡張する道を選択した。OpenID4VP を待つべきか、独自に仕様を公開すべきかが議論された結果、「断片化は悪いことではない」という前提のもと、ISO 独自の拡張仕様が公開された。一方で OpenID4VP は独立して進化を続け、最も収束が求められる局面で、二つのアプローチが併存する状況が生まれた。

この断片化は、主要なプラットフォームベンダーの一つがが ISO 定義のプロトコルのみを実装し、OpenID4VP をサポートしなかったことで、さらに強化された。この選択は、技術的な合意や標準化団体間の合意を通じたものではなく、単独な実装判断によって、事実上どちらか一方を優位に位置付ける結果となった。さらに、ある政府による大規模な初期展開が、この実装選択を前提として本番導入に踏み切ったことで、その影響は決定的なものとなった。こうして、標準化団体間の設計上の相違は、実装者、エコシステム、利用者全体に影響を及ぼす、構造的な相互運用性の問題へと発展した。

しかし近年、このプロトコル層における断片化は望ましくないという共通認識が形成されつつある。この動きは、もともと mdoc に強く結合していた ISO/IEC 18013-5 を SD-JWT といった追加のクレデンシャル形式に対応させる必要性が生じたことも一因である。これを受け、両作業部会のメンバーが対等な立場で議論し、将来的なプロトコル調和を検討するための新たな場が設けられつつある。私は、この取り組みが真の収束に向けた意味のある一歩となり、調和が確かな成功への道を歩み始めていることに、心から希望を抱いている。

5．標準の採用（Adoption of Standards）

「もし SD-JWT が mdoc より先に発明されていたら、世界を制していただろう。しかし現実はそうではない。」この言葉は、標準の採用がいかに複雑で偶然性に左右されるかを象徴するものとして、今も私の心に残っている。

仕様の採用を最終的に決定づける要因は何かという問いは、非常に興味深い。先行者であることは確かに有利に働くことがあるが、それは信頼できる代替案が現れるまでの間に限られることも多い。開発者体験、ドキュメントの品質、価値を明確に伝える能力も、仕様が実装・維持されるかどうかに大きく影響する。規制もまた採用を左右し得るが、それは強制ではなく、関係するコミュニティ、産業、利用者の合意を反映したものであるべきである。

私が得た最も重要な学びの一つは、多くの点で標準は、市場経済における製品と本質的に変わらないとい

うことである。標準は市場の中に存在し、注目と採用を巡って競争し、可視性、支持活動、調整努力によって形作られる。

この現実は、標準の採用が純粋に技術的な問題ではないことを意味する。複数の設計が技術的に成立し得る場合でも、エコシステムは「最も実装しやすく、説明しやすく、組織内で正当化しやすい」ものに収束する傾向がある。この事実はオープン標準の価値を否定するものではないが、標準が公共財であり続けるためには、ガバナンスと開放性が極めて重要であることを示している。

だからこそ私は、標準の採用は最終的に市場によって決まるべきであり、単一の企業や支配的な主体によって決定されるべきではないと考えている。幅広い実装と合意によってではなく、一社の判断によって仕様の採否が事実上決まってしまう状況には、強い問題意識を抱いている。誰かが「いずれ他のすべての参加者もこの選択に従うだろう」と想定することは、オープン標準が共有され、協働によって作られるという理念そのものを損なう。標準は、避けられないから採用されるのではなく、選ばれるからこそ成功すべきなのである。

とはいえ、現実の制度設計や政府調達の文脈では、この原則が必ずしもそのまま適用されているとは限らないのも事実である。歴史的な経緯や制度上の慣行から、標準の技術的成熟度や実装実績よりも、従来から参照されてきた枠組みや形式的な位置づけが重視される場合も少なくない。その結果として、実装者の視点から見ると、より完成度が高く、実運用に即した仕様が存在していても、それが十分に評価されないまま、別の選択がなされることがある。こうしたギャップは、標準の採用が持つ本来の目的、相互運用性を高め、選択肢を広げ、公共の利益に資すること、を損なうおそれがあるため、今後は出自や慣行だけでなく、実装可能性や運用実績を含めた多面的な観点から標準を評価する姿勢が、より一層求められると考えている。

6．日本と分散型アイデンティティ標準（Japan and Decentralized Identity Standards）

国際的な標準化コミュニティと密接に協働する中で、地域ごとの標準化への関わり方の違いを観察する機会を得た。日本は長年にわたり国際標準化に深く関与しており、日本の専門家は高い技術力と長期的なコミットメントを一貫して示している。また、TTC で表彰されている方々を含め、明確に発言し、議論や成果に積極的な影響を与えている個人が存在することも事実である。

一方で、日本からの参加全体としては、発言や立場表明が控えめになる傾向も見られる。その結果、重要な意思決定が形成される局面において、本来共有されるべき視点が十分に表明されないことがある。これは意見や考えが存在しないからではなく、公開の議論の場で十分に可視化されないためである。進行の速い標準化プロセスでは、沈黙はしばしば同意として解釈され、方向性に影響を与える機会が失われることもある。

また、日本国内で選択されている技術的な賭けが、グローバルな潮流と異なる場合があることも観察された。例えば、W3C Verifiable Credentials Data Model に対する関心は依然として高いが、他の多くのエコシステムでは、実装フィードバックに基づき、よりシンプルで展開しやすいアプローチへと移行している。これらの違い自体に正解・不正解はないが、前提が大きく乖離すると、他地域で開発されたシステムとの整合性が難しくなるという結果を伴い得る。

7．成功する標準の条件（How Successful Standards Look Like）

私が関わってきたすべての標準に共通して言える成功要因がいくつかある。第一に、「単純なものを単純に保つ」ことは利便性の問題ではなく、持続可能性の問題である。一般的な利用経路を過度に複雑化する標準は、理論的にいかに洗練されていても、採用コストを高め、実装を阻害する。これと密接に関連するのが、拡張ポイントを本当に多様性が避けられない箇所にのみ導入するという規律である。柔軟性が必要な部分では拡張を許容しつつ、コアとなる相互作用は明確で安定し、理解しやすい状態を保つことが重要である。

そして何よりも、成功する標準は実装者との継続的な対話によって形作られる。実装フィードバックは後付けの確認ではなく、主要な設計入力である。曖昧さ、不必要な複雑性、現実の運用では成り立たない前提は、実装を通じて初めて明らかになることが多い。実際、インターフェースの簡素化や仕組みの見直し、設計判断の再考といった重要な改善は、現場でシステムを構築・運用する人々からのフィードバックによってもたらされてきた。たとえ強く信じていた前提であっても見直す姿勢こそが、仕様を「正しい文書」から「使われる標準」へと変える鍵である。

私はまた、仕様を最終化することの重要性を強く実感するようになった。欧州では、ドラフト段階の仕様が最終化前に実装を義務付けられるという、非常に特殊で困難な状況が生まれた。ドラフトである以上、実装フィードバックに基づいて破壊的変更が入ることは避けられない。大規模展開が依存する複数の仕様の著者として、私は標準を安定した状態に導く責任を強く感じていた。この厳しいスケジュールを乗り越えられたのは、議論、レビュー、プルリクエストに並外れた時間と労力を注いだ、少数の献身的な人々の存在があってこそである。

8．標準化団体（SDO）で効果的に貢献するために（How to Effectively Contribute in the SDOs）

これまでの経験を通じて学んだのは、標準化活動で効果的に貢献するためには、技術的専門知識だけでは不十分だということである。仕様の中核に関与し、その進化を追うためには技術力が不可欠である一方、標準化の成果を組織の実際のニーズや制約と結びつけるためには、ビジネス的な理解も必要となる。さらに重要なのが、政治的・対人的スキルである。標準は交渉と妥協、説得の積み重ねによって前進し、核心的な目標を見失うことなく多様な利害を調整する能力が、成果を左右する。

ワーキンググループの議長を務めることは、同一組織内のチームを管理することとは本質的に異なる経験であった。昇進や評価といった強制力は存在せず、進捗はすべて自発的な貢献に依存する。議長の役割は、参加者の動機を引き出し、信頼を築き、限られた時間と異なる優先順位を持つ人々の間で妥協を促すことである。公平性と技術的誠実さを保ちながら前進することは、プロセスであると同時に一つの技である。

また、４～５の標準化団体に同時に関わる立場にあったことで、標準化団体間の複雑な階層構造と相互依存関係を深く理解するようになった。分散型アイデンティティは、複数の SDO が並行して仕様を策定し、それらが密接に相互運用する必要がある、数少ない分野の一つである。これらの関係を調整するには、謙虚さ、継続的な調整、組織の壁を越えて協働する姿勢が不可欠であり、単一の組織や視点だけではこの課題を解決できないことを改めて実感した。

標準化の現場を進む中で、個人の属性が経験に与える影響についても触れずにはいられない。年齢、出身、性別のいずれか一つだけでも、発言の受け取られ方や立ち位置に影響を及ぼすことがあるが、若く、アジア出身であり、かつ女性であるという複数の要素が重なったとき、その難しさはより顕著になると感じた。現在の標準化コミュニティは、こうした属性を持つ参加者を多数想定して形成されてきたものではなく、そのことが無意識の前提として作用する場面も少なくない。

こうした環境の中で、過小評価されたことが、結果として目標に向けて準備し、進めるための時間と余地を与えてくれた場面もあった。この経験を通じて、年齢や性別、背景に左右されず、能力と誠実さを重んじる協力者を見極め、信頼関係を築く力が磨かれたと感じている。

9．謝辞（Thank You）

最終的に、標準化活動は人によって成り立っている。コミュニティ自体は小さいが、卓越した専門性、強い意見、長い記憶を併せ持つ人々が集まっている。貢献の評価は必ずしも均等でも形式的でもなく、影響の大きさに比例して可視化されるとは限らない。それは容易ではないが、同時に、各個人の内発的動機と、共に形作る成果への責任の重要性を思い起こさせる。

私はこの分野で、極めて経験豊かで思慮深い多くの方々から学び、導いていただいた。とりわけ日本は、私の思考に深い影響を与えた第一線の専門家を数多く輩出している。崎村夏彦氏、富士榮尚寛氏、鈴木茂哉氏、岸上順一氏、そして村井純氏から受けた指導と助言は、私の標準化への姿勢と、対立ではなく橋を架けることで前進するという信念を形作る上で決定的な役割を果たした。

また、Torsten Lodderstedt 氏には、心からの感謝を捧げたい。彼は常に卓越した議論の相手であり、知的誠実さと先入観にとらわれない対話に開かれた姿勢を持つ、かけがえのない協力者であった。この取り組みのすべての段階において、彼の支援と関与は不可欠なものであった。