企業はどう適応するべきか？
デジタルアイデンティティ標準の
高度化がもたらすビジネスチャンス

目次

はじめに

インターネットやデジタルサービスが急速に発展しています。プライバシーを守りつつ、安全にサービスを利用できる環境が求められる中、デジタルアイデンティティの適切な管理は、個人および企業が持続可能なデジタル社会を築くために欠かせない条件となっています。

ただ、デジタル空間で人や物を他と区別し、アクセス権をコントロールしながらデータ利活用を実現するデジタルアイデンティティに求められる要件は、セキュリティやコンプライアンス要件が複雑化する中で高度化し続けています。

このような課題がある中、グローバルではデジタルアイデンティティ関連の標準仕様も進化しており、それを取り入れることは、生産性の向上、システム間の互換性とインターフェースの整合性、そして信頼性と安全性の強化に重要な役割を果たしています。

本レポートでは、標準仕様が進化する中で生じる、実装に必要な観点の漏れや拡張性の欠如といった課題に対処するために、企業が標準仕様に精通した上で設計や開発を進めることの重要性について、具体的な事例を交えて説明します。

また、ビジネスの効率性や競争力をどのように高めるかを考察し、企業が新しい標準仕様を取り入れることで得られるチャンスについても提案します。

独自仕様で実装することの課題・リスク

独自仕様の実装は、思わぬ問題を招くことがある。この章では、独自仕様の実装に関連する課題とリスク例（図表1）をいくつか列挙する。

（1）セキュリティとプライバシーの考慮漏れ

独自仕様のシステムでは、セキュリティとプライバシーの課題が見落とされがちである。世界中の有識者によって作成されレビューを経た標準仕様に比べ、個別に設計されたものは、検討に必要な観点の漏れなどからくるセキュリティホールを内包するリスクが高く、脅威に対する迅速な対応が困難だからだ。そのまま利用を続けた場合、データ漏洩やプライバシー侵害のリスクが増大し、信用を失う可能性がある。

（2）相互運用性の欠如によるビジネス障壁

独自の仕様でシステムを開発した場合、異なるシステム間での連携が難しく、変化のペースが早いビジネス環境で重大な障壁となり得る。互換性がないために、データや業務プロセスが効率的に統合されず、企業間の協業が滞るためである。この結果、事業の展開に影響を及ぼし、場合によっては新しい機会を逃し、ビジネスの柔軟性が損なわれるおそれがある。

（3）拡張性の制限とその影響

独自の仕様で開発されたシステムは、設計が特定の目的や環境に固有のものであるため、長期的な拡張性に欠ける場合がある。このため、ビジネス環境の変化に対応できず、アップデートや機能追加が困難になることで、システムの陳腐化を招きかねない。また、新たなニーズに即応できず、競争力が低下し、企業の成長を妨げる可能性がある。そのため、関係システムとの連携方式やデータ構造については、特に留意が必要だ。

（4）コストの増加と市場競争力の低下

カスタムソリューションの開発や維持には、多大なコストが伴う。独自仕様のシステムは、特殊なスキルやリソースが必要となり、運用コストが膨らむ一方で、ニーズに対する素早い適応が難しくなる。このため、他社との競争において劣勢となり、市場競争力の低下を招きかねない。

図表1：標準仕様のメリットと独自仕様の課題

標準仕様を使用するメリット		独自仕様の課題・リスク
• 最新の標準プロトコルや規格がシステムの防御力を強化 • プライバシー保護の透明性を向上	セキュリティとプライバシー	• 非標準的なシステムはセキュリティホールを内包する可能性が高い
• 異なるシステム間でのデータ共有やプロセス連携が円滑 • グローバルでの市場展開が容易	相互運用性	• システム間の連携が難しく、ビジネスの柔軟性が損なわれるおそれがある
• 他の開発者や企業との間で一貫性を持ち、新しい機能やサービスを追加しやすい	拡張性	• 独自仕様は特定目的に固有で、拡張性に欠ける場合がある
• 開発と運用のコスト削減、規制順守の容易化	コスト	• 独自開発は特殊なスキルやリソースが必要。維持コストも膨らみやすい

出所：PwC作成

標準仕様の高度化がもたらすベネフィット

(1) セキュリティ、プライバシー、コンプライアンスの強化

最新の標準プロトコルや規格は、セキュリティとプライバシーを強化するための堅ろうなフレームワークを提供する。標準化されたセキュリティプロトコルは、最新の攻撃や脅威に対応するために継続的に更新され、システム全体の防御力を強化する。プライバシーの保護に関しても、標準化されたガイドラインはデータ管理の透明性を向上させ、利用者の信頼を獲得する手助けをする。

さらに標準仕様は規制順守を考慮していることが多く、規制対応における考慮漏れリスクを低減する。

(2) 相互運用性の向上による企業間連携、グローバル展開の可能性

標準化への準拠は、システム間の相互運用性を向上させる。これにより、異なるシステム・プラットフォーム間でのデータ共有やプロセスの連携が円滑になり、企業間の協業が促進される。さらに、国際的な標準仕様に準拠することで、グローバルでの市場展開が容易になり、競争力が向上する。グローバルで統一されたオペレーションを実現し、事業のスケールアップにも有用である。

(3) 標準化による拡張性の確保

標準仕様を採用することで、システムの拡張性が大幅に向上する。標準化された技術やプロトコルは、他の開発者や企業との間で一貫性を持つため、新しい機能やサービスを容易に追加できる。これにより、新しい技術を取り入れやすくなり、迅速な対応が可能となる。また、標準化された環境は、長期的なメンテナンスの負担を軽減し、将来の拡張計画に柔軟に対応できる基盤を実現する。

(4) コスト削減と市場参入の柔軟性

標準化を採用することは、開発と運用のコスト削減につながる。標準仕様は広く認知され、多くの開発者が精通しているため、独自開発に比べて人材やリソースのコストを抑えられる。また、市場参入に際しても、標準仕様に基づく製品は規制の順守が容易であり、新たな市場のニーズに柔軟に対応できる。標準化は、迅速かつ効率的な市場参入を実現し、コスト効果の高い競争力強化も可能にする。

具体的な標準仕様規格の紹介

ここからは、デジタルアイデンティティ関連の主な標準化団体と標準仕様を具体的に紹介する（図表2）。

（1）デジタルアイデンティティ関連の主な標準化団体

デジタルアイデンティティ分野では、多様な国際標準化団体が技術仕様やガイドラインを策定し、相互に補完しながら標準化を進めている。

● ISO／IEC

情報技術・セキュリティ分野の国際標準規格を策定。ISO／IEC 24760（アイデンティティ管理フレームワーク）やISO／IEC 29115（保証レベル）など、基盤となる概念定義や枠組みを提供している。また、ISO／IEC 18013-5（モバイル運転免許証）などの開発も行っている。

● ITU-T（国際電気通信連合・標準化部門）

国際的な電気通信標準（勧告）を策定する国連専門機関の一部。通信ネットワーク、セキュリティ、ID管理など幅広い分野の技術標準を定め、各国や企業の相互運用性を促進している。

● W3C（World Wide Web Consortium）

ウェブ技術の標準化団体。近年は分散型アイデンティティ技術に注力し、DID（分散型識別子）やVC（検証可能なクレデンシャル）の標準化を推進。VCデータ構造1.0（2019年勧告）、DIDコア1.0（2022年勧告）、VCデータ構造2.0（2025年勧告）などを策定している。

● FIDO Alliance

パスワードに依存しないフィッシング耐性のある認証技術の業界標準を策定。近年は主要プラットフォームと連携し、「パスキー」の普及を推進している。

● IETF（Internet Engineering Task Force）

インターネット技術の標準化フォーラム。OAuth 2.0やJOSEファミリー（JWT／JWS／JWE／JWP）など、デジタルアイデンティティ関連プロトコルを策定・更新。OAuth 2.1やSD-JWTなどの新仕様も策定中。

● OIDF（OpenID Foundation）

2007年設立の非営利団体。セキュアで相互運用可能なアイデンティティ標準（OpenID Connect、FAPI、OpenID for Verifiable Credentials, Shared Signal Frameworkなど）を策定。OpenID Connectは数十億人に利用されている。

これらの組織は、それぞれの観点からデジタルアイデンティティ基盤の構築に貢献している。なお、標準化団体ではないが、以下のような組織の発行するガイドラインも大きな影響力を持っている。

● 経済協力開発機構（OECD）

政策面での指針を提供。2023年には「デジタルアイデンティティのガバナンスに関する勧告」を採択し、ユーザー中心、包括性、ガバナンス、相互運用性の重要性を強調。法的拘束力はないものの、各国の政策に影響を与えている。

● 米国立標準技術研究所（NIST）

産業と科学技術の革新を支えるための標準とガイドラインを策定する米国商務省の機関。サイバーセキュリティ、暗号、デジタルIDなどの分野で広く採用される技術文書を提供。

● デジタル庁

政府のデジタル化推進を担う行政機関で、行政サービスのDXやデジタル基盤の整備を統括。マイナンバー制度やデジタルID、ガバメントクラウドなどの政策を推進し、官民の連携も支援。

図表2：デジタルアイデンティティ関連の標準化・ガイドライン策定を進める主な組織

組織名	活動内容
ISO／IEC	情報技術・セキュリティ分野の国際標準規格を策定。ISO／IEC 24760（アイデンティティ管理フレームワーク）、ISO／IEC 29115（エンティティ認証保証レベル）、ISO／IEC 18013-5（モバイル運転免許証）などがある。
ITU-T	国際的な電気通信標準を策定する国連専門機関の一部。通信ネットワーク、セキュリティ、ID管理など幅広い分野の技術標準を定め、各国や企業の相互運用性を促進。
W3C	ウェブ技術の標準化団体。分散型アイデンティティ技術に注力し、DID（分散型識別子）、VC（検証可能なクレデンシャル）などの標準化を推進。
FIDO Alliance	パスワードに依存しない認証技術の業界標準（FIDO2：WebAuthn／CTAP）を策定。主要プラットフォームと連携し「パスキー」の普及を推進。
IETF	インターネット技術の標準化フォーラム。OAuth 2.0、JOSEファミリー（JWT／JWS／JWE／JWP）などを策定・更新。OAuth 2.1やSD-JWTなどの新仕様も策定中。
OpenID Foundation	2007年設立の非営利団体。セキュアで相互運用可能なアイデンティティ標準（OpenID Connect、FAPI、OpenID for Verifiable Credentialsなど）を策定。数十億人に利用されるOpenID Connectや昨今EUデジタルIDウォレットで採用されたOpenID4VC/VPなどが有名。
OECD	政策面での指針を提供。「デジタルアイデンティティのガバナンスに関する勧告」を採択。ユーザー中心、包括性、ガバナンス、相互運用性の重要性を強調。法的拘束力はないが政策に影響。
NIST	サイバーセキュリティ、暗号、デジタルIDなどの分野で広く採用される技術文書を提供。産業と科学技術の革新を支える標準とガイドラインを策定する米国商務省の機関。
デジタル庁	政府のデジタル化推進を担う行政機関。マイナンバー制度、デジタルID、ガバメントクラウドなどの政策を推進し、デジタル基盤の整備や官民の連携を支援 。

出所：各組織の情報を基にPwC作成

(2) デジタルアイデンティティ関連の主な標準化の状況(図表3)

● OAuth 2.0／OpenID Connect(認可・認証)

1. 概要

(1) OAuth 2.0：インターネットにおける認可プロトコル(IETF RFC 6749)。第三者アプリに限定的なアクセス権を与える仕組み。アクセストークンを用い、パスワードを渡さずに安全な権限委譲を実現する。API連携やSSOの基盤として広く普及。

(2) OpenID Connect(OIDC)：OAuth 2.0ベースの認証プロトコル(OIDF、2014年策定)。IDトークン(JWT形式のユーザー識別情報)を追加し、クライアントが本人認証と属性情報を取得可能に。ソーシャルログインや企業内SSOの事実上の標準。多くの国の「国民ID基盤」も採用する。

2. 技術内容

OAuth 2.0はネットワーク上の資源にアクセスするための権限を表すアクセストークンなどを発行。OIDCは、アクセスしてきているのが誰なのかを表すIDトークンを発行。またUserInfoエンドポイントというAPIアクセスのためのアクセストークンも発行するため、ログイン後、随時最新の属性を取得することができる。追加属性も取得可能。動的クライアント登録、Logout仕様など拡張も多数。

3. 進展状況

IETFでOAuth 2.1の標準化が進行中(2025年RFC化見込み)。これまでの十数年で積み重なってきたセキュリティ上のベストプラクティスを統合。

4. 意義

現代のウェブ・モバイル認証基盤の根幹。ソーシャルログイン、企業内SSO、金融API連携(Open Banking)などビジネスエコシステムを支える。セキュリティ面でもトークンベース認証は重要。最近ではAI Agentにおける認証・認可での利用検討も始まっている。

5. 国内外の動向

(1) 国外

グローバル標準としてSNS、金融、政府サービス、医療など多様な分野で採用。各国政府の市民ID連携にも利用。IETFとOIDFが連携し拡張仕様を策定。

(2) 国内

広く普及。大手IT企業がOpenIDプロバイダーを運用。行政サービスでも利用。課題はレガシーシステムからの移行や中小サービスでの実装ミス対策(ガイドライン充実、認定制度活用)。

● VC（W3C VC Data Model 2.0、IETF SD-JWT VC、OID4VCI／VP／SIOPv2など）

1. 概要

証明書類をデジタル化し、改ざん検知可能かつ検証可能な形で表現する枠組み。ユーザーが自身の資格情報を保持・提示でき、中央集権的な認証局への都度問い合わせが不要。署名技術と標準データ構造で実現。

2. 主要な標準

（1）W3C VC Data Model：VCの基本データ構造とプロトコルを定義。Issuer／Holder／Verifierモデル、クレームへのIssuer署名、Holderによる保持者拘束、検証手順などを規定。1.0版（2019年勧告）、2.0版（2025年勧告）が発行されている。

（2）IETF SD-JWT VC：VC表現フォーマットの一つ。Selective Disclosure JWT（SD-JWT）技術でクレームの選択的開示（最小限開示）を実現。JSON形式で既存技術と親和性が高い。IETFで標準化進行中。

（3）OpenID for Verifiable Credentials（OID4VC）：OAuth2を用いてVCの発行・提示を行う仕様群（OIDF策定）。

1 OID4VCI（Issuance）：OAuth2フローでVCをウォレットに発行。特定のVC形式に依存しない柔軟性を持つ。

2 OID4VP（Presentation）／SIOPv2（Self-Issued OP v2）：VCの提示・検証。専用言語DCQLを使ったVerifierからの要求とHolderからの提示フローを定義。ユーザー中心の分散型IDエコシステム形成を可能に。

3. 意義

デジタル世界での信頼性の高い資格情報交換を実現。個人が一元管理し選択的に提示可能（eKYC、資格証明など）。発行者の負荷軽減。改ざん検知可能でオフライン検証も可能。SD-JWT-VCなどによるプライバシー保護（最小限開示）。

4. 国内外の動向

（1）国外

EUの「ヨーロッパデジタルIDウォレット」構想（eIDAS 2.0）で技術基盤として参照。米国でもデジタル運転免許証や学歴証明プラットフォームなどで活用。W3C／OIDF／IETFが協調し、標準策定と実装促進。

（2）国内

政府の「Trusted Web推進協議会」とデジタル庁が社会実装を検討。金融分野のeKYCの高度化、大学卒業証明の電子化などで実証実験を実施。課題は発行主体間の調整、法制度整備、VCウォレット普及策。国際標準との整合性の確保の他、プライバシーと利便性のバランスも論点。官民で国際標準への準拠の方向で動きが一致しており、関心が高まっている。

● ISO／IEC 18013-5 モバイル運転免許証（mDL）

1. 概要

ISO／IEC 18013-5は、モバイルデバイス上のmDL／mdocを安全かつ相互運用可能な形で実装・検証するための国際的なインターフェース仕様を確立することが目的。利便性の向上、偽造防止、プライバシー保護（選択的開示）、国境を越えた利用を実現し、保有者の同意に基づいた近接通信（デバイスリトリーバル）やサーバー経由（サーバーリトリーバル）で情報を提示・検証するプロセスを規定することで、ユーザー中心のデジタル身分証明を目指す。

2. 技術内容

mDL／mdocの安全性と相互運用性を確保するため、データ構造にCBCR（Concise Binary Object Representation）エンコーディングとMSO（Mobile Security Object）、暗号化・署名にCOSE（CBOR Object Signing and Encryption）やPKI、発行者・デバイス認証メカニズム、そして近接通信（NFC、BLE、Wi-Fi Aware、二次元コード）やセッション暗号化といった特定の技術要素を規定。これらの技術は連携してデータの完全性・真正性・機密性を保ち、選択的開示を実現するが、リーダー認証が必須でない点など、実装上の課題が指摘されている。

3. 進展状況

2021年9月に発行されたISO／IEC 18013-5（近接通信向け）に続き、オンライン利用を標準化する技術仕様書ISO／IEC TS 18013-7が2024年10月に発行された。標準化はISO／IEC JTC 1／SC 17／WG 10が主導し、AAMVA（北米）やEUDI Wallet（EU）などの地域実装ガイドライン、NISTなどによるパイロット、主要OS ベンダーの対応といったエコシステムの発展とともに、規格の実用化と普及が進んでいる。

4. 背景

ISO／IEC 18013-5の開発は、世界的なデジタルトランスフォーメーションとスマートフォンの普及を背景に、物理的な証明書の紛失・偽造リスクやプライバシー課題、そして初期のデジタル免許証における相互運用性の欠如といった問題に対応する必要性から生まれた。セキュリティ強化、プライバシー保護、利便性向上、国際的な通用性への社会的な要請が、この標準化の取り組みを推進した。

5. 意義

ISO／IEC 18013-5に基づくmDL／mdocは、利用者には利便性とプライバシー向上、検証者には信頼性の高い本人確認と業務効率化、発行機関にはセキュリティ強化とコスト削減、そして相互運用性の確保という多大な利点をもたらす。これにより、信頼できるデジタルアイデンティティのエコシステムを構築し、安全なオンラインサービスや新たなデジタル社会基盤の実現に貢献することが期待される。

6. 国内外の動向

（1）国外

ISO／IEC 18013-5／7はモバイルIDのグローバル標準として世界的に採用が進んでおり、特に米国では多数の州が導入しTSAが空港で受け入れ、EUではEUDI Walletの必須技術として位置づけられている。オーストラリア、カナダ、韓国など他の国々でも関心が高く、大手OSベンダーなどのプラットフォーム事業者の対応も普及を後押ししており、特に政府発行IDにおいて主要選択肢化しつつある。

（2）国内

2025年3月からマイナンバーカードと運転免許証を一体化する「マイナ免許証」制度が開始されているが、これは警察共通基盤を活用したカード中心のアプローチであり、mDLではない。一方で、デジタル庁や一部民間企業、研究機関では、国際標準仕様であるISO／IEC 18013-5（mdoc／mDL）を用いた実証実験が活発に行われており、スマートフォンに搭載されるカード代替電磁的記録ではこの国際標準が採用される見込みである。

● FIDO2（WebAuthn／CTAP、パスキーなど）

1. 概要

パスワードを代替する強力な認証仕様群（FIDO Alliance／W3C策定）。中核はWebAuthn（W3C標準API）とCTAP2（認証器-クライアント間プロトコル）。デバイス認証（指紋、顔など）と公開鍵暗号でログイン。サーバーには公開鍵のみ登録。

2. パスキー（Passkey）

パスワードの代わりに、公開鍵暗号方式によって安全かつ簡単にログインできる新しい認証方法。ユーザーアカウントにひも付き、デバイスロック操作でログイン可能。複数デバイス間で同期可能。ユーザー名やパスワード、二要素コードの入力は不要。鍵は送付先のOrigin（Scheme、Host、Portの組み合わせ）に関連づけられており、正しいOriginにしか認証情報（署名鍵で署名した情報）を送らないのでフィッシング耐性が高い。

3. 背景

FIDO Alliance（2012年設立）が「パスワードのない世界」を目指し策定。WebAuthnはW3C勧告。CTAP2はFIDO規格。パスキー普及促進や認定プログラムを展開。

4. 意義

フィッシングやパスワード漏洩リスクを大幅低減。従来の二段階認証よりユーザー体験が向上し、セキュリティと利便性を両立。サービス提供者もパスワードリセットやアカウント乗っ取り対応の負担を軽減。

5. 国内外の動向

（1）国外

アップル、グーグル、マイクロソフトなどが自社エコシステムでパスキー対応を進め、2023年頃からグローバルで実装本格化。金融機関なども導入。FIDO AlliancのPasskey Pledgeに多数参加。各国政府も注目。

（2）国内

主要ウェブサービスや携帯キャリア、一部銀行が導入・検討。課題は一般ユーザー認知度、企業での既存認証基盤との統合。既存パスワードを廃止する真のパスワードレス化への移行も課題。利用者教育とシステム改修が重要。

● デジタル庁 DS-500／DS-511（日本の本人確認指針）

1. 概要

デジタル庁策定の「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」（DS-500）。行政手続きのデジタル化において必要な本人確認基準、手法、リスク評価手順などを規定。NIST SP 800-63-3などを参照し作成された。2021年公開。2024年度に大幅改定作業を実施。適用範囲を対面や行政手続外にも拡大し、デジタルID全般を対象に。名称を「行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン」に変更、文書番号もDS-511に。フェデレーションなども視野に。2025年3月に改定方針公開、2025年度中の正式改定を目指す。

2. 技術内容

（1）DS-500

NIST SP 800-63-3に倣い、「身元確認保証レベル（IAL）」と「認証保証レベル（AAL）」でリスクに応じた手法を選定。手法例（公的個人認証、銀行口座確認など）やリスク評価方法を記載。

（2）DS-511（改定検討）

DS-500を大幅改定して、フレームワークを「デジタルIDの保証レベル」体系へ再構築。最新脅威（Deepfakeなど）や技術（生体認証精度向上）を反映。分散型ID／VCへの言及も期待（改定案資料に「クレデンシャルプロバイダ」「クレデンシャルの提示要求」などの用語あり）。

3. 意義

国内行政サービスで統一的な本人確認基準を提供。サービス間の基準ばらつきを抑制し、ユーザー体験の一貫性を向上。民間サービスeKYC実装時の参考にもなり、国内全体の水準向上に寄与。

4. 国際的位置づけ

後述するNIST SP 800-63やISO／IEC 29115を踏襲し、保証レベル体系は国際標準と整合。他国からも注目。

5. 国内動向

法的拘束力はないものの、システム調達要件などに組み込まれ、実装が進む（パスポート申請オンライン化など）。課題はガイドラインの難解さ、実務への落とし込みを支援、新技術への迅速な対応。改定後のDS-511普及と民間連携が重要。

図表3：デジタルアイデンティティ関連の主な標準化の状況

OAuth 2.0 ／ OpenID Connect	概要		インターネットにおける認可・認可プロトコルを連携するフェデレーションと呼ばれる技術。第三者アプリに限定的なアクセス権を与える。
	主要な標準		OAuth 2.0：権限を表すアクセストークンを発行する認可プロトコル。 OpenID Connect：OAuth 2.0上にIDトークンと呼ばれるユーザー識別情報を加えたもの。最新の属性取得やログアウト仕様など拡張機能が多数。
	進展状況		OAuth 2.1の標準化が進行中。AI Agentにおける認証・認可での利用検討も開始。
	意義		分散アーキテクチャが必要なウェブ・モバイル認証基盤の要。ソーシャルログインや企業内SSO、金融API連携などを支える。セキュリティ面でも重要。
	動向	国外	多様な分野でグローバルに採用。
		国内	広く普及し、行政サービスにも導入。
VC	概要		証明書をデジタル化し、改ざん検知と検証可能な形で保持・提示。
	主要な標準		W3C VC Data Model：VCの基本データ構造とプロトコルを定義 OpenID for Verifiable Credentials（OID4VC）：OIDC／OAuth2を用いてVCの発行・提示を行う仕様群（OIDF策定）。 ① OID4VCI（Issuance）：OAuth2フローでVCをウォレットに発行 ② OID4VP（Presentation）／SIOPv2（Self-Issued OP v2）：VCの提示・検証。専用言語DCQLを使ったVerifierからの要求とHolderからの提示フローを定義。
	意義		信頼性の高い情報交換とプライバシー保護を実現。
	動向	国外	EUのeIDAS 2.0では技術基盤として参照され、米国でもデジタルIDの活用が進む。W3C、OIDF、IETFが協調し標準策定を推進。
		国内	政府の「Trusted Web推進協議会」や、デジタル庁によるeKYC・卒業証明電子化の実証が進行中。課題は発行主体調整、法制度、VCウォレット普及策、国際標準とプライバシー・利便性のバランスなど。

モバイル運転免許証（mDL）	概要		モバイルデバイス上のmDL／mdocを安全かつ相互運用可能な形での連携を実現。偽造防止、プライバシー保護（選択的開示）などへの配慮もされており、国境を越えた利用、ユーザー中心のデジタル身分証明を実現。
	主要な標準		ISO／IEC 18013-5。mDL／mdocの安全性と相互運用性を確保するため、データ構造（CBOR）とMSO（Mobile Security Object）、暗号化・署名にCOSEとPKI、発行者・デバイス認証メカニズム、近接通信（NFC, BLE, Wi-Fi Aware, QRコード）やセッション暗号化といった特定の技術要素を規定。
	進展状況		2021年9月に発行されたISO／IEC 18013-5（近接通信向け）に続き、オンライン利用を標準化する技術仕様書 ISO／IEC TS 18013-7が2024年10月に発行。
	背景		グローバルなデジタルトランスフォーメーションの要請。
	意義		利便性、プライバシー、信頼性を向上し、セキュリティ強化とコスト削減、相互運用性を確保。デジタルIDエコシステムの構築に貢献。
	動向	国外	ISO／IEC 18013-5／7は米国やEUをはじめグローバルに採用され、政府発行IDの主要選択肢として位置づけられ、各国・地域で関心が高まる。
		国内	2025年にマイナンバーカードと免許証を統合する「「マイナ免許証」制度を導入。デジタル庁はISO／IEC 18013-5を用いたモバイルIDの実証実験を進行。
FIDO2	概要		パスワード代替の強力な認証仕様群（FIDO Alliance／W3C策定）。中核はWebAuthn（W3C標準API）とCTAP2（認証器-クライアント間プロトコル）。
	主要な標準		パスキー。 主要OSベンダーが推進するFIDO認証資格情報。ユーザーアカウントにひも付き、デバイスロック操作でログイン可能。複数デバイス間で同期可能。ユーザー名／パスワード／二要素コード入力が不要。
	背景		FIDO Allianceが策定。
	意義		フィッシングやパスワード漏洩リスクを大幅低減。従来の二段階認証よりユーザー体験が向上し、セキュリティと利便性を両立。サービス提供者もパスワードリセットやアカウント乗っ取り対応の負担軽減。
	動向	国外	主要メガテックなどが自社エコシステムでパスキー対応を進め、2023年頃からグローバルで実装本格化。金融機関なども導入。各国政府も注目。
		国内	主要ウェブサービスや携帯キャリア、一部銀行が導入・検討。課題は一般ユーザー認知度、企業での既存認証基盤との統合。
デジタル庁DS-500／DS-511	概要		行政手続デジタル化のための本人確認基準を定義。NIST SP 800-63-3を参照。2021年に公開し、2024年度に改定に向けた検討を実施。対面・行政手続外も対象。名称変更し、2025年に改定方針公開。2025年度中に正式改定を目指す。
	主要な標準		DS-500はNIST基準を踏まえたリスク対応手法を設定し、これを発展させたDS-511では最新の脅威や技術を反映したデジタルID保証レベルの再構築を検討。
	技術内容		IALとAALを基にした手法を選定。
	意義		国内行政で統一的な本人確認基準を提供し、ユーザー体験を向上。eKYC実装の参考となり、国内全体の水準向上に貢献。
	国際的位置づけ		後述するNIST SP 800-63やISO／IEC 29115を踏襲し、保証レベル体系は国際標準と整合。他国からも注目。
	国内動向		法的拘束力はないが、システム調達要件などに組み込まれ、実装が進む（パスポート申請オンライン化など）。課題はガイドラインの難解さ、改定後のDS-511普及と民間連携。

出所：公表されている情報を基にPwC作成

● その他関連規格

1. NIST SP 800-63

米国連邦政府向けデジタルアイデンティティガイドライン（2025年改訂［第4版］）。IAL（身元確認）、AAL（認証手段強度）、FAL（フェデレーション連携時の保護）の3指標で定義。リスクに応じた強度設計が可能。

2. ISO／IEC 29115

電子認証のエンティティ保証フレームワーク国際規格。保証レベルをLoA1（最低）～LoA4（最高）の4段階で規定。身元確認と認証プロセスの強度で段階設定。各国のデジタルIDフレームワークの参照基準（欧州eIDAS「低・中・高」もおおむね対応）。現在改訂版を作成中。日本からもDS-511の知見などを提供する予定。

日本のガイドライン（DS-500／511）もNIST／ISO体系を参考に、保証レベル（IAL／AAL）を定義。eKYCガイドラインなども整合。国際的な保証レベル相互認証が将来重要に。国際標準準拠の枠組み整備はクロスボーダーID連携に不可欠。

上記のように多くの標準化団体や政府当局が昨今のニーズの変化や、規制への対応、セキュリティへの配慮が施された標準の策定を進めている。

サービスを実装する際は、これらを抑えておくことが、現状を守り、戦略的にビジネスを進めていく上で、極めて重要である。

新規にサービスを開発する場合は、これらの標準のいずれか、もしくは複数を抑えるのはもちろん、現状サービスの設計と照らし合わせてFit&GAP分析を行い、不足している要件の洗い出しに活用することも、ビジネスを守り、拡大していく上で有効だろう。

3. 量子コンピュータ時代への備え

デジタルアイデンティティ分野では、量子コンピュータの脅威に対する準備も始まっている。2024年にNISTが最終標準化したML-KEM（旧Kyber）、ML-DSA（旧Dilithium）などの耐量子暗号アルゴリズムの採用検討が各標準化団体で進められている。企業は現在のシステム設計において、将来のPQC（Post-Quantum Cryptography）移行を考慮した暗号アルゴリズムの抽象化レイヤーを設けるなど、移行コストを最小化する準備を進めることが推奨される。

標準への準拠がもたらすビジネスチャンス

ここでは、標準仕様への準拠が企業にもたらすビジネスチャンスについて紹介する。

(1) 新たな市場機会の発見および参入スピードの確保

標準化動向を知ることで、新たな市場機会を見つけることが可能だ。例えば欧州では、上述のVerifiable Credentials仕様が国際的に標準化されると同時に、企業間で相互接続テストが行われている。これにより、企業は新しいサービスを開発しながら、相互接続性の懸念なくエコシステムを拡大する機会を得られる。このような標準に基づく新技術の導入と協力関係の構築は、市場における存在感を高め、新たな商機をもたらすことが期待される。

(2) 競争優位性の確立

標準化を採用することは、企業の競争優位性を強化する有力な手段となる。標準規格に従うことで、システムの互換性が確保され、より迅速かつ効率的な製品・サービスの提供が可能になる。これにより、他社との差別化を図ることができ、市場におけるポジションを強固なものとする。

(3) イノベーション促進による長期的成長

標準化は、イノベーションを促進し、企業の長期的な成長を後押しする。標準仕様に基づいた開発は、一貫した品質と安定性を保証し、新たなアイデアや技術をスムーズに取り入れる土壌を整える。これにより、企業は新しい製品やサービスの開発に柔軟に対応でき、技術革新を取り入れたソリューション提供を行えるようになる。標準化は、グローバルな市場へのアクセスを容易にし、新しいアイデアを世界中で展開するための支援にもなる。

事例の紹介

国際的に議論され標準化されている内容は、一般的に非常に高度で配慮が行き届いている。これらへの理解が及ばない実装ミスの例をいくつか列挙する。

(1) セキュリティに関する考慮漏れ

ID連携を基にした認証システムとして導入したが、最初は標準仕様からいくつか逸脱していた。これにより、情報漏洩やクロスサイトリクエストフォージェリ攻撃のリスクを招く可能性があった。特に、認証情報が漏れる設定や、ユーザー情報を適切に処理しない部分が課題とされた。標準仕様からの独自の解釈や実装があり、他のシステムとの連携には注意が必要だ。

(2) 責任分解の混同

デジタルアイデンティティの管理では、ユーザー、アプリケーション、リソースオーナー、認証事業者などの役割を明確に区分し、それぞれが知るべき情報のみを扱うよう実装する必要がある。

例えば、認証事業者とアプリケーション事業者が異なる場合、認証事業者はクレデンシャルであるIDやパスワードを管理するが、アプリケーション事業者はそれらを知るべきではない。したがって、アプリケーション側でIDやパスワードを直接入力させない実装が求められる。やむを得ずこのような実装をする場合、セキュリティガバナンスの強化などが必要だ。

(3) 採用プロトコルの判断間違い

OpenID ConnectとSAML（Security Assertion Markup Language）は、どちらもID連携を実現する技術として広く利用されている。一般的には、インターネット上で、OpenID Connectは消費者向けアプリケーションに、SAMLは企業向けアプリケーションに適しているとされることが多い。しかし、実際にはOpenID Connectも企業向けアプリケーションで活用されており、場合によってはSAMLよりも有利な選択肢となり得る。これらの標準技術は、その特性と用途を正確に理解する必要がある。正確な比較を行うことで、最適なID管理戦略を構築できるだろう。

(4) 拡張性を欠いたデータ構造

消費者向けサービスでは、消費者からのデータ取得に際し、その目的を正確に消費者へ説明し、同意を取得することで初めてデータが保管可能となる。企業が複数のサービスを提供し、各サービスで異なるデータを取得する場合には、同意もサービスごとに個別に取得する必要があるため、目的を複数管理できるようデータ構造を設計しておくことが求められる。また、サービス変更に伴い同意を取り直す場合、目的のバージョン管理をしておくことも欠かせない。ISO／IEC TS 27560:2023 Privacy technologies・Consent record information structureという規格では、そうした状況に対応するための考え方が整理されているため、実装者は理解しておくべきだ。

実際の適応戦略

企業が国際標準に効果的に対応するためには、開発プロセスから専門家の活用、そして社員教育までを組み合わせた包括的なアプローチが求められる（図表4）。以下に、その具体的な戦略を解説する。

（1）国際標準の専門家を企画・開発体制に含める

国際標準化に対応するためには、外部の専門家の力を借りることも有効だ。特に複雑な標準や新しい分野での経験が不足している場合、外部の知見者に依頼することで、標準への理解と適合を加速化できる。これらの専門家の下で具体的なプロジェクトにおける標準の実装を行い、その結果を基に今後の社内プロセスを改善する。これにより、標準対応能力の向上と、より高度な国際基準への準拠を実現できる。

（2）国際標準に基づいた設計・開発プロセス

国際標準に基づいた設計および開発プロセスを構築するには、標準の要件を的確にプロジェクトに反映させるためのアプローチを確立する必要がある。まず、プロジェクトマネジメントに標準の要件を組み込み、それに基づくガイドラインを策定する。具体的には、取り込むべき標準仕様を明確にし、要件定義の初期段階から組み入れ、デザインレビューやコードレビューにチェックリストとして使用する。また、開発プロセスの各フェーズで標準適合性を確認するメカニズムを導入し、継続的なモニタリングとフィードバックループを構築する。さらに、組織内の各部門と効果的にコミュニケーションを図り、標準の理解と適用が一貫して行われるようなチーム文化を育むことも重要である。

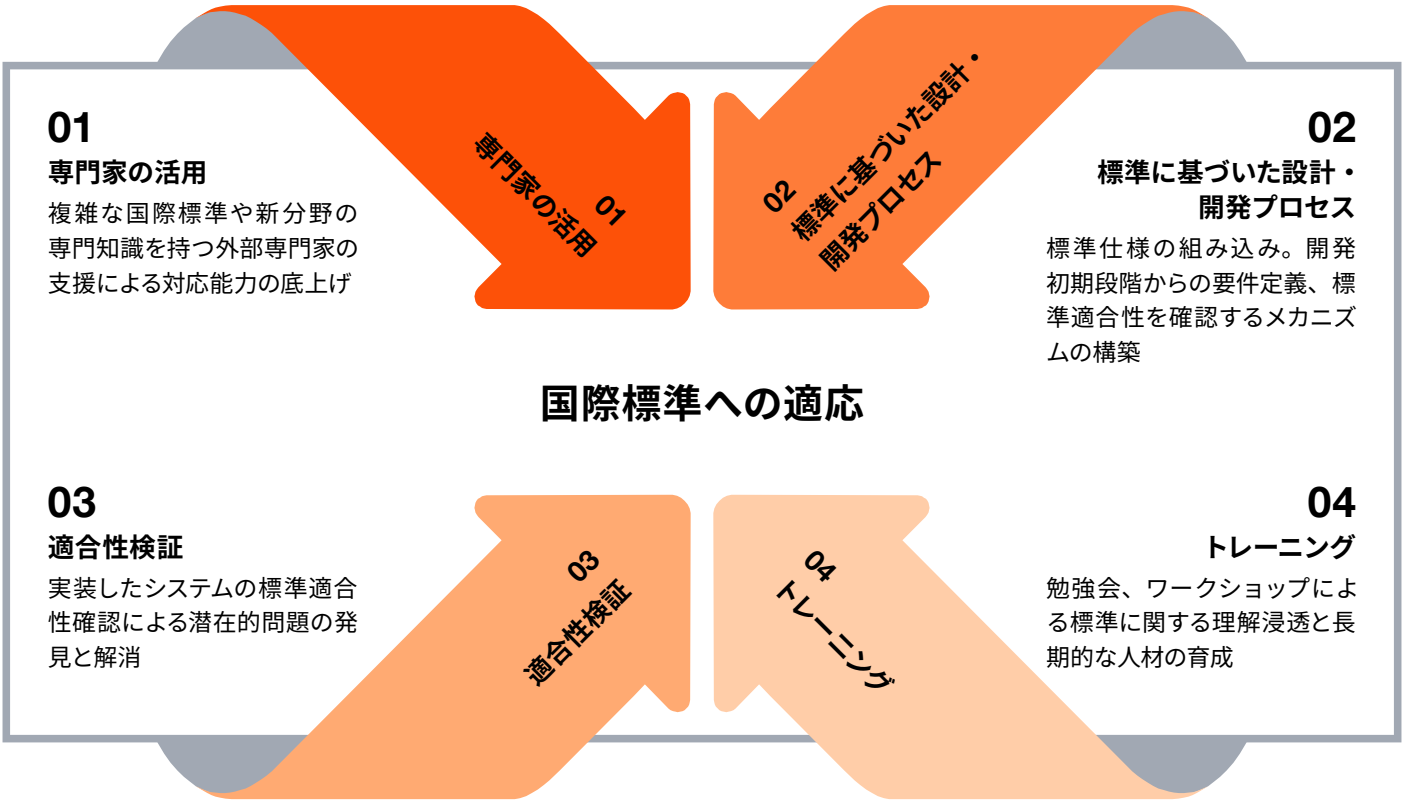
（3）適合性検証

実際に実装されたシステムが、標準仕様どおりに作られているかどうかの確認は非常に重要だ。実際、海外のある銀行では、公開鍵ではなく秘密鍵が公開されている事例が適合性検証によって見つかっている。このような検証によって、製品の市場投入時における失敗を防ぎ、企業の信用を守る。標準仕様に基づいた適切な適合性検証の実施により、企業は確実に国際標準を満たす製品を作ることができ、長期的な視野でのビジネス成功に貢献するだろう。

（4）トレーニング

国際標準は、長期的に知識と技術の保持し続けることが重要である。社内で社員が標準に詳しくなるためには、教育プログラムとトレーニングの提供が重要である。社員に対し、定期的な社内勉強会やワークショップを開催し、最新の標準について議論する場を設け、さらに、実務において標準を活用するための実践的なスキルを身につけられるようサポートする。これにより、社員全員が標準に対する理解を深め、組織全体でより一貫した基盤を築くことができる。

図表4：国際標準への適応のためのアプローチ



出所：PwC作成

おわりに

本稿では、デジタルアイデンティティの分野で標準化に準拠する重要性について記述しました。標準化は、企業にとって新たなビジネス機会を創出し、競争優位性を高める重要な要素です。国際的に整合性のあるフレームワークを構築することは、ビジネスの成長やセキュリティ対応の強化などにつながります。標準仕様の導入により、企業はイノベーションを促進し、長期的な成長が期待できます。グローバルでさまざまな国際標準が議論される中、今後も進化する標準仕様に柔軟に対応し、新たな市場チャンスを捉えることは、持続可能なビジネスの鍵となるでしょう。

pwc

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびブローダーアシュアランスサービス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約12,700人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、クライアントが複雑性を競争優位性へと転換できるよう、信頼の構築と変革を支援します。私たちは、テクノロジーを駆使し、人材を重視したネットワークとして、世界149カ国に370,000人以上のスタッフを擁しています。監査・保証、税務・法務、アドバイザリーサービスなど、多岐にわたる分野で、クライアントが変革の推進力を生み出し、加速し、維持できるよう支援します。

発刊年月：2025年9月　　管理番号：I202504-10