



2025年の振り返り

成長、信頼、確かなインパクトを生んだ一年

2026年4月1日

はじめに

このレポートでは、OpenID Foundation（OIDF）が行った2025年の活動を振り返る。2025年は、これまでにない規模の影響と標準の採用があった年であった。年間を通じて、各産業分野が連携し、安全性を支え、[継続的アイデンティティ（Continuous identity）](#)を可能にする標準の強化に取り組んだ。複数の大陸にわたり、実装者は、OIDFの標準仕様群が現実世界における相互運用性を実現することを実証した。2025年は、萌芽的なアイデアと技術仕様とを、実運用のインフラストラクチャへと真に転換した年であった。

さらに注目すべきは、この先に控える展開である。すでに数十の政府が、デジタルウォレットおよび検証可能な資格情報（Verifiable credentials）を実現するために、OIDFの標準を採用している。そしてこのことで、2026年、2027年、そしてその先に数千万人が日常的なサービスのためにこれらの仕様を利用するための基盤が整いつつある。

本レポートは、意思決定者、実装者、政策立案者が一貫して提示する次の4つの問いを軸に構成されている。

- これらの標準は信頼できるのか。
- 実際の運用において、それらは相互に連携して機能するのか。
- 意味のある規模で展開されているのか。
- 次に到来する課題に対応できる備えができていくのか。

各セクションでは、この問いに順次答えていく。すなわち、国際認知において如何に信頼を確立したか、相互運用性試験でどう現実での実行可能性を証明したか、国家レベルの導入でどのようなスケールを示したか、そしてOIDFが次なる展開に向けてどのような準備しているかを示す。

内容

はじめに.....	1
第1部：グローバルな信頼を獲得するコミュニティ標準.....	4
国際的な認知.....	4
独立したセキュリティ検証.....	5
第2部：相互運用性の実証.....	5
ベンダ、プラットフォーム、国境を越えた相互運用性の証明.....	5
第3部 パイロットから国家インフラ、エコシステムへの展開.....	10
デジタルクレデンシャルプロトコル.....	10
FAPI 2.0.....	13
Shared Signals.....	15
第4部: 標準を支える原動力.....	15
OpenID Foundation がいかにしてグローバルな採用を可能にするか.....	15
仕様.....	15
適合性と認定.....	16
オープンソースプラットフォームのサポート.....	17
パートナーシップ.....	18
リエゾンおよび標準化団体とのパートナーシップ.....	18
第5部: 次に来るものへの備え.....	19
新たな課題に関する公的な議論の牽引.....	19
死とデジタル遺産.....	19
AI とアイデンティティ管理.....	20
オンラインにおける年齢確認と未成年保護.....	21
KYC 規制を遵守するための金融業界における mDL および検証可能なクレデンシャルの採用 拡大.....	21
オープンデータエコシステムの支援.....	22
EU デジタルアイデンティティウォレット (EUDIW) コミュニティ向けの専用リソース.....	22
SIDI ハブ.....	23
主要なフォーラム.....	24
政策および政府との連携.....	26
まとめ：2025 年が証明したもの.....	27
感謝を込めて。.....	27
OpenID Foundation 指導部の振り返り.....	28
OpenID Foundation について.....	29

第1部：グローバルな信頼を獲得するコミュニティ標準



国際的な認知

国際標準化機構（ISO）が[2024年に9つのOpenID Connect仕様を公開仕様書（Publicly Available Specifications : PAS）](#)として公表したことに続き、2025年にはさらなる画期的なマイルストーンを達成した。

5月、[国際電気通信連合（ITU）](#)は[OpenID Connect Core 1.0を勧告X.1285](#)として正式に採択した。これは、OIDFの仕様が国際的なITU-T標準となった初めての事例である。[10月のITUによる標準の公式発行](#)はこの認知をさらに強化し、世界中の政府に対して独立の、信頼できる権威あるリファレンス基準として提供された。

なぜこのことが重要なのか。ITUに標準として採択されると、その技術が実証済みで成熟しており信頼性が高いことを世界中の政府や規制当局に示すことになり、採用の可能性が大幅に高まる。政府や規制当局にとって、デジタルアイデンティティ標準への信頼は独立した検証と国際的な認知に依存しており、このマイルストーンはその両方を実現した。

この勢いを拡大する形で、OIDFの3つの追加仕様ファミリーが2025年後半にISO投票を通過し、ISO公開仕様書（PAS）として認められた。現在、これらはISOのコメントに対応するための編集プロセスにあり、その後以下のISO/IEC番号の下で公開される予定である。

- FAPI 1.0 Advanced（[ISO/IEC DIS 25791-1](#)、[ISO/IEC DIS 25791-2](#)）

- OpenID for Identity Assurance (OID4IDA、[ISO/IEC DIS 25831-1](#)および[ISO/IEC DIS 25831-2](#))
- FAPI 2.0 ([ISO/IEC DIS 26083-1](#)および[ISO/IEC DIS 26083-2](#))

これらの標準は、すでに世界中の金融サービスおよびアイデンティティエコシステムで実際に使用されている。これらの正式な認知によって、採用前に国際標準の承認を必要とする政府、あるいは仕様を選択する前に独立した検証を求める政府への道が開かれる。

独立したセキュリティ検証

正式な認知と並行して、2025年にはOIDFの検証可能なクレデンシャル関連の取り組みに対する独立したセキュリティ検証も実施された。8月、[シュトゥットガルト大学](#)の独立した学術研究者たちが、[Digital Credentials APIを用いたOpenID for Verifiable Presentations \(OpenID4VP\) の包括的な数学的解析](#)を完了した。その結果、脆弱性は発見されず、セキュリティ解析によってOIDFは仕様のセキュリティ特性を明確に理解することができた。重要なのは、このフィードバックが本仕様の最終ステータスに達する前に組み込まれたことであり、これは広範な採用に先立ってセキュア・バイ・デザイン標準へのOIDFのコミットメントを強化するものである。

また、上記は過去数年間における他の標準の正式なセキュリティ解析に続くものであり、全体では以下が含まれる。

- [OpenID for Verifiable Credentials](#)
- [FAPI 2.0 Message Signing、Dynamic Client Registration \(DCR\)、Dynamic Client Management \(DCM\)、およびFAPI-CIBA](#)
- [FAPI 2.0 Security Profile](#)
- [OpenID Financial-grade API](#)

2025年末、OIDF理事会はOpenID for Verifiable Credentials 1.1 + IAEのセキュリティ解析を進めることに合意し、この重要な取り組みのセキュリティ特性をより深く理解することとした。さらに、2026年にはOIDFはOpenID Federation 1.0のセキュリティ解析の更新も追求する予定である。

これらのマイルストーンを総合すると、一貫したストーリーが浮かび上がる。OIDFのコミュニティによって作成された仕様は、今や国際的に認知された標準となっている。これらは独立して検証された構成要素であり、世界中の政府や規制当局が安全に依拠できるものであり、OIDFはこの高い基準を維持することにコミットしている。

第2部：相互運用性の実証

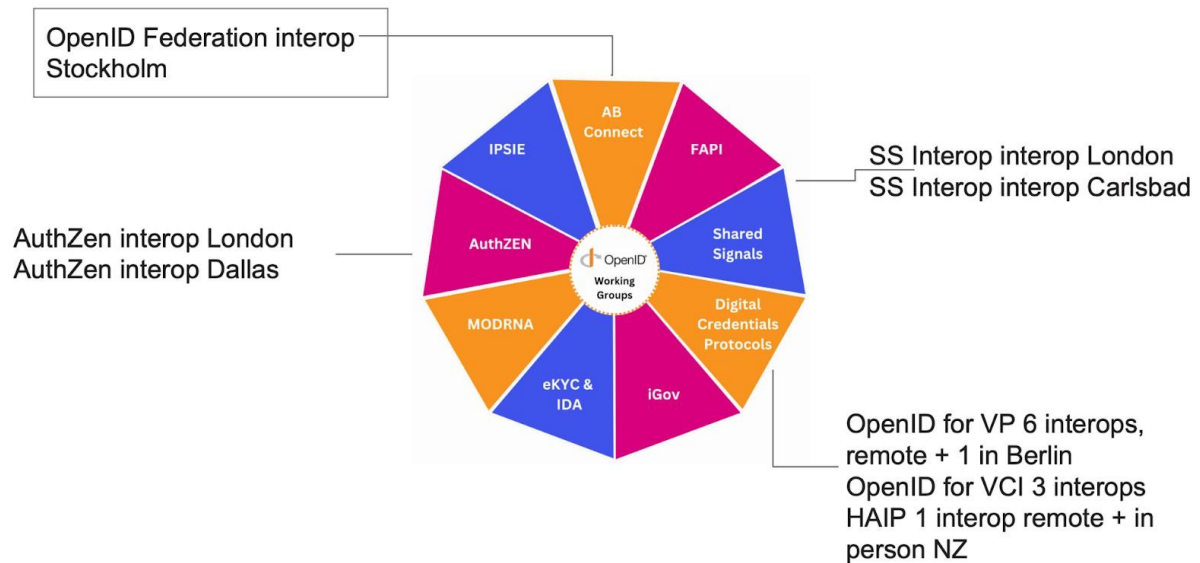
ベンダ、プラットフォーム、国境を越えた相互運用性の証明

認識されるだけでは十分ではない。デジタルアイデンティティおよびセキュリティの標準化が成功するためには、異なるベンダ、実装、デバイス、法域にまたがって機能しなければならない。

2025年を通じて、OIDFとそのメンバーは、実運用における相互運用性の実証に注力し、自らの標準がそれを提供することを示した。複数の仕様ファミリーにわたり、仕様が最

終ステータスに到達する前に、実装者が一堂に会して実システム同士の相互試験を実施した。そこでは、国境や技術スタックをまたいだ試験もしばしば行われた。

WG Spec / Test Support - 15 Interop Events!



Digital Credentials Protocols (DCP) Working Group

- [ブレイクスルーの瞬間](#)は、5月に発生した。OIDFが世界で最初に到達したのである。DCPワーキンググループが作成したデジタルアイデンティティ・クレデンシャルの標準仕様が、シームレスに多様なプラットフォーム、デバイス、国々をまたいで連携した。三か国からステークホルダーが集まった場で、OIDFは独立して構築したシステムが実際に連携することを証明したのである。開発中だった OpenID for Verifiable Credential 1.0は[6月について最終仕様となった](#)。



- 2か月後、世界中から集まった[7つのIssuerと5つのウォレットプロバイダ](#)が[OpenID for Verifiable Credential Issuance \(OpenID4VCI\)](#) のテストを行った。
OpenID for Verifiable Credential Issuance 1.0 は、[9月に最終仕様となった](#)
- 11月、OpenID4VPとOpenID4VCIの連携で[High Assurance Interoperability Profile \(HAIP\) 1.0](#) のテストが行われ98%が疎通した。その後、[HAIPは12月に最終仕様となった](#)



OpenID Federation

- 4月、30の国際的な代表者が、[SUNET](#)がホストとなり15か国14の実装組織を代表してストックホルムに集まり、[3日間のOpenID Federationの集中テスト](#)を行った。参加者らはシステム間の相互運用性を成功のうちに実証し、最終仕様に必要な具体的改善点が特定されるとともに、OpenID Federationを組織が採用するのは「可能か」ではなく「いつなのか」という方向へと国際的な議論を転換させた。OpenID Federation 1.0は[最終仕様が承認](#)されている。
- 12の調査・教育に関するフェデレーションが、OpenID Federation for [eduGAIN](#)のパイロット開発を開始している。内部的な連携は世界約80の国際的な調査教育機関で行われており、[10,000以上のエンティティ](#)があります。パイロットは、これらの運営者がSAMLからOpenIDフェデレーションへの移行を理解するのに役立つであろう



Shared Signals

- 10月、8つの主要なテクノロジー企業が集まり、[Shared Signals Framework \(SSF\)](#)と[Continuous Access Evaluation Protocol \(CAEP\)](#)そしてOpenID RISC最終仕様が複数のベンダ、プラットフォーム間でリアルタイムにセキュリティ対応を連動するデモを行った。そのデモは、9月に3つの仕様が最終化した後、[The global Authenticate conference](#)に参加して行われた。この場では、企業や組織が今や、簡単にセキュリティシグナルや脅威を共有することができ、ユーザに再認証を何度も要求するようなことをしなくてもよいことを証明して見せた。これは[Shared Signals ワーキンググループ](#)がホストした4度目の相互接続イベントあり、共有シグナルのオープンソーステストを成熟させ、実装者がデフォルトで相互運用性を達成するのに役立つ相互運用性プロファイルを進展させるために機能した。



AuthZEN

- 12月の[Gartner IAM Summit](#)でAuthZENは、エンタープライズへの適用準備が出来ていることを証明した。実装者からの質問も「本当に動作するのか」から「どうやってインプリするのか」になった。これは17のベンダによるテストと、Gartnerが標準への対応を正式に薦める対象としたことのサポートがあった



このデモは、相互運用性はもはや願望ではないことを示した。エビデンスベースで再現性もある。彼らはまた、OIDFの標準は、最終化する前に厳密に検証されて

いることを示した。これら仕様ファミリーのすべてがOIDFの標準化プロセスに沿う中で、ベンダやプラットフォームをまたがり、世界中のエキスパートが関与するのに一役買っている。

第3部 パイロットから国家インフラ、エコシステムへの展開



重要インフラで活用される標準

トラストが作られ、相互運用性が証明されたことで、2025年はOpenID ファウンデーションの標準が国家およびエコシステム規模での本格的な導入へと決定的に移行した一年となった。

デジタルクレデンシャル、オープンデータ、医療、金融サービス、セキュリティシステムをまたがり、OIDFの仕様は単なるパイロットではなく長く活用するインフラのためとして選ばれた。各国政府はデジタルウォレットとVerifiable Credentialsの実装を公共サービス向けに始めた。FAPIを導入したある国の医療システムは、高セキュリティなAPIを配備し、機微なデータフローを保護することに成功した。テクノロジーベンダは、Shared Signalsをリアルタイムのリスク対応に向け実装した。

これらのデプロイにより、OIDFの仕様は、確実かつ安全に、全住民規模に対応しなければならないシステムに適用されていることを実証している。

デジタルクレデンシャルプロトコル

ヨーロッパの、[最初のEUDIWリリース](#)イベントでは、OpenID for Verifiable Presentation

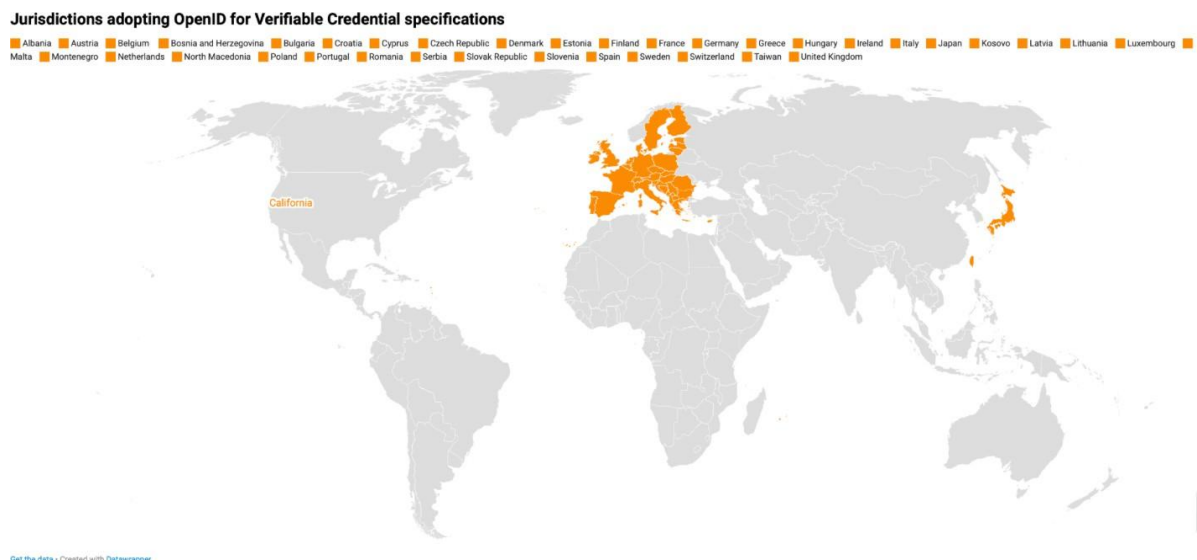
1.0と OpenID for Verifiable Credential Issuance 1.0、そしてHAIP 1.0の仕様とテストをハイライトする[OIDF のプレゼンテーション](#)が行われた。



日本では、[デジタル庁](#)が[学生向けのVerifiable Credentialsを利用したサービスのパイロット事業](#)を[西日本旅客鉄道株式会社](#)と[国立情報学研究所](#)と立ち上げた。学生は、自分の個人情報を過度に提示することなく、自分のステータスをサービスにアクセスする際に証明できるようになる。プライバシー保護に配慮されているデジタルクレデンシャル技術の設計および実装の利点を示す好例である。



OpenID for Verifiable Credential仕様ファミリーの現在の対応状況は下の地図に表しているが、38の法域でみられており、さらに継続して増加することが期待される。



これらの仕様を選択した多くの組織はまた、OIDFのアクティブなパートナーである。複数の法域の政府機関が [Digital Credentials Protocols](#) ワーキンググループ (DCP WG) に参加し、域内や越境による相互運用性要件への対応を強化している。

Examples include:

- [カリフォルニア州 Department of Motor Vehicles \(DMV\)](#) : [メンバー組織であり、OIDFと2回のハッカソンイベントにて共同でホストした](#)
- [SPRIN-D](#) : ドイツの破壊的イノベーションを進める政府組織で[OIDFの DCP Working Group](#)のメンバーである。また、ドイツ政府として紙幣、IDカード、パスポート、有価証券を開発する[Bundesdruckerei](#)という企業は、[DCP WGの相互運用性イベント](#)に参加し、仕様の開発に貢献している
- [NIST NCCoE Digital Identities - Mobile Driving License \(mDL\)](#) プロジェクト : OIDFはCRADAの参加者として活動しており、11回にわたる相互運用性イベントの共同ホストを行った。そして、OIDFは[NIST SP 800-42A Digital Identities - Mobile Driving License "Accelerating Development and Adoption for Financial Institutions"](#) ガイドラインをドラフトする際のマテリアルコントリビューターとなった
- [eIDAS 2.0](#) と [EUDIW Architecture Reference Framework \(ARF\)](#) : OIDFはEuropean Commissionとのパートナーシップの中で、ARFで選定された仕様群に関するレポートや、将来、参加する地域やエコシステムに対して求められるであろう適合性確認の仕組み作りで貢献した。前に書いたようにOIDFは、EUDIW リリースイベントでリソースハブを提供しており、ヨーロッパのコミュニティに貢献している

FAPI 2.0

ノルウェーでは、FAPI 2.0（OIDFの規制産業向けの高セキュリティAPI標準）が、HelseIDサービスを通じて[ノルウェー保健ネットワーク（NHN）全体に導入されつつある](#)。すべての新規APIに同標準の採用が義務付けられ、既存サービスも段階的に移行することから、全国の数千に及ぶ医療提供者間における機微な医療データの流れが保護されることになる。このことは、OIDFのオープン標準が、国全体の医療システムを保護する上で信頼に足るものであることを実証している。



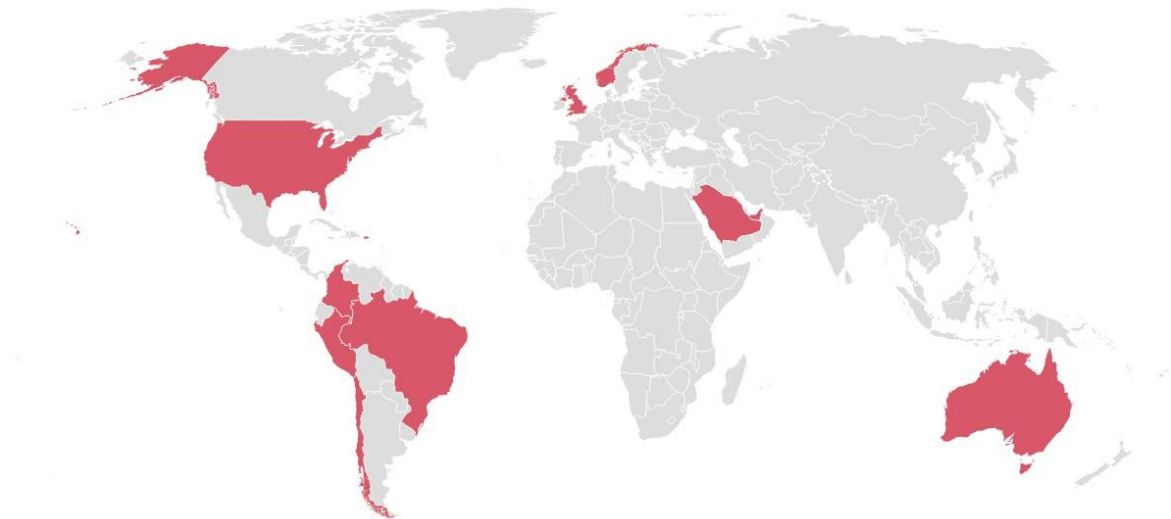
そしてこれは、オープンバンキングのエコシステムにおけるFAPIの成功に基づいている。[英国の先駆的なオープンバンキング実装](#)や、[金融部門全体に義務付けられたブラジルの展開](#)から、[ConnectIDによるデジタルアイデンティティネットワークでのFAPIの利用](#)に至

るまで、その実績は明らかである。これらの国家レベルでの展開は、**FAPI 2.0**の堅牢なセキュリティフレームワークが金融サービスをはるかに超えて広がり、あらゆる規制産業における機微なデータを保護することを示す展開のほんの一部にすぎない。

また、ノルウェー保健ネットワークは、その運用経験をコミュニティに還元するために、メンバーとしてOIDFに加入した。

FAPIを採用した、あるいは採用の軌道に乗っている現在のエコシステムは、以下のグローバルマップに示されている。

Jurisdictions Adopting FAPI



Created with Datawrapper

OIDFとデューデリジェンスや適合性支援において積極的に連携しているその他のエコシステムには、以下が含まれる。

- [オープンバンキング実装機関（英国）](#)
- [オーストラリアデータ標準化団体](#)
- [ConnectID（オーストラリア）](#)
- [チリ金融監督庁](#)
- [サウジアラビア金融庁](#)
- [アラブ首長国連邦中央銀行](#)
- [Financial Data Exchange（米国）](#)
- [オープンファイナンス・ブラジル](#)
- [オープンインシュアランス・ブラジル](#)
- [ペルー政府](#)
- [ノルウェー保健ネットワーク](#)
- [コロンビア](#)

この広範な採用は、安全でスケーラブル、かつ信頼性の高いオープンデータエコシステムを提供するOIDFのFAPI標準に対する、主要な実装者の信頼を示している。

Shared Signals

2025年には米国政府から、OIDFのShared Signals仕様が果たし得る重要な役割を強調する、新たな提言もなされた。直近では、米国立標準技術研究所（NIST）が[NIST highlighted in its interagency report \(IR 8587\)](#)のセクション6.6において、Shared Signalsが米国政府機関やより広範なクラウドサービスプロバイダーのセキュリティ確保において果たし得る役割を強調した。これは、以下の2つの先行レポートにおける助言と一致するものである。

- NIST (SP 800-63C-4) [デジタルアイデンティティガイドライン：フェデレーションのアサーション - セクション4.8「共有シグナリング \(Shared Signaling\)」](#)
- [国土安全保障省サイバーセキュリティ・インフラセキュリティ庁 \(CISA\) サイバー安全審査理事会の提言](#)

米国政府による認知にとどまらず、Apple、Google、Ciscoを含む主要なテクノロジー企業から、SGNL、SailPoint、Oktaなどのアイデンティティ専門企業に至るまで、幅広い業界での採用が進んでいる。

第4部: 標準を支える原動力

OpenID Foundationがいかにしてグローバルな採用を可能にするか

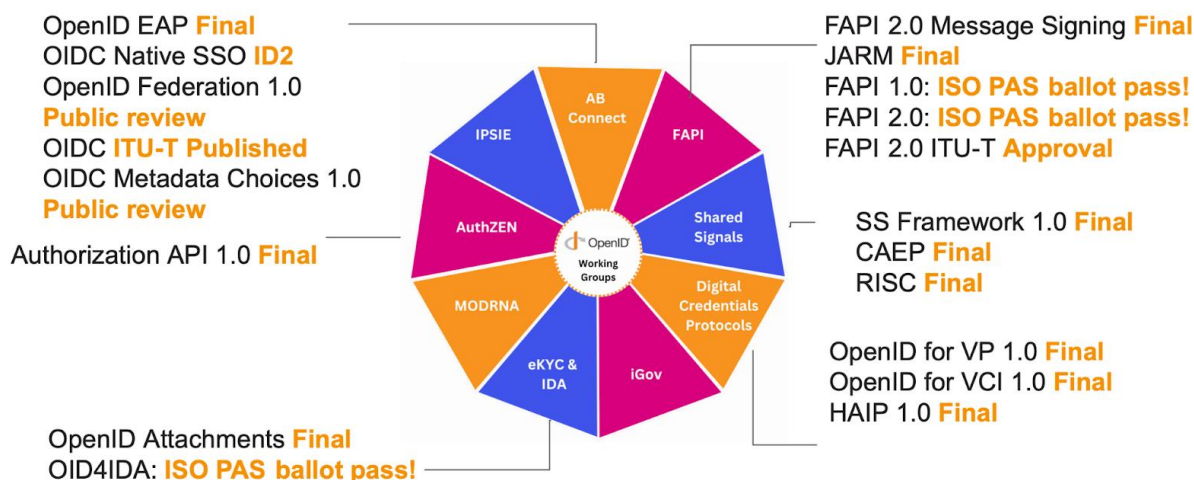
国家規模の展開、エコシステムの立ち上げ、そして国境を越えた実装のすべての背後には、相互運用可能で安全な採用を大規模に可能にする、パートナーシップ、テスト、およびコミュニティ支援からなる意図的なインフラストラクチャが存在する。

2025年、OIDFは世界中の実装者が確信を持って標準を採用できるようにする運用メカニズムを強化した。OIDFの影響範囲は、実装が正しく機能することを証明する適合性テストから協調ネットワークへと拡大し、グローバルな断片化を防止する戦略的パートナーシップにまで及んでいる。

仕様

2025年、OIDFのメンバーは高セキュリティAPI（FAPI 2.0 Message Signing）、Verifiable Credentials（OpenID4VP、OpenID4VCI、HAIP）、共有セキュリティシグナル（SSF、CAEP、RISC）、およびAuthorization API標準にわたる、計11の最終仕様を承認した。

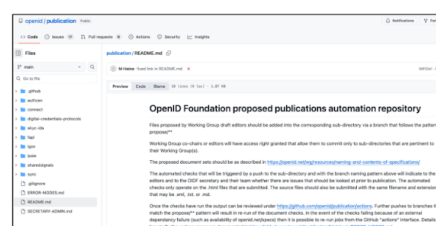
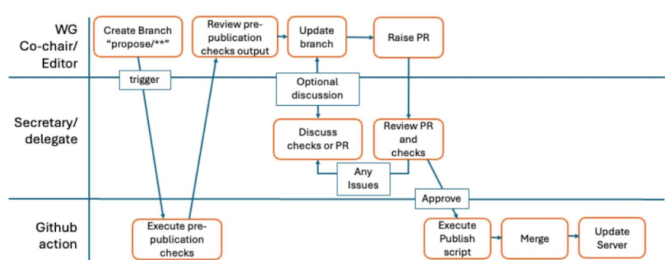
11 specs to Final & strong ISO/ITU Recognition



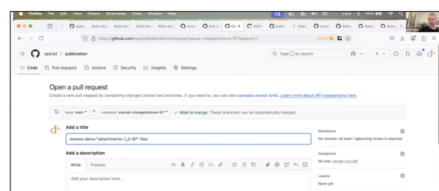
OIDFの仕様自動化ツールの提供開始は、仕様のエディターやワーキンググループの共同議長に大きな利益をもたらし、ワーキンググループの仕様最終段階の呼びかけ（Final Call）から仕様ライフサイクルの次の段階である公開への移行を効率化した。

Spec Process and Automation Tool Launched

Tool live & proven out



Video on YouTube



適合性と認定

2025年、適合性テストは7月のFAPI 2.0認定の開始により大きく進展した。これはOIDFの既存の認定プログラムに加わり、年間を通じて力強い成長を示した。新規認定数は15%増の663件となり、累計認定数は4,545件に達した。これらの認定の多くは、オープンバンキング向けのFAPIプロファイルを実装しているブラジル、オーストラリア、英国、サウジアラビア、UAE、およびその他の法域のエコシステム参加者によるものであった。

OIDFはまた、2026年第2四半期に開始予定の適合性検証サービスへの投資を承認し

た。既存の自己認定プログラムを補完するこのサービスは、大規模な適合性プログラムを展開する、または複雑な国内規制体制を敷く規制当局やエコシステム運営者を支援する。デジタルアイデンティティとオープンデータの両ドメインから、複数のエコシステムパートナーがすでにこのプログラムの開発に参加している。MOU（覚書）パートナーに関する最新情報や開始の詳細は、確定次第、2026年中に[ニュースセクション](#)に掲載される予定である。

最後に、OIDFは[国連のDPI（デジタル公共インフラ）セーフガード・ワーキンググループ](#)が、調達プロセス、契約、およびエコシステム規則に適合性および認定要件を当初から組み込むべきであると推奨したことを非常に喜ばしく思っている。国連DPIセーフガード・フレームワークは、個人と社会を保護するための不可欠なツールとして、セキュリティコントロールを明確に特定している。OIDFの無料の適合性テストスイートは、適切な実装を通じて標準が確実に価値を提供することに貢献している。



オープンソースプラットフォームのサポート

OIDFには、オープンソースプロジェクトをサポートしてきた強力な実績がある。OIDF独自の適合性認定プラットフォームはオープンソースであり、コミュニティメンバーはOIDFのテストやオープンソースプロジェクトを利用して、OpenID仕様に対する自己認定をすべて無償で行うことができる。このアプローチにより、組織は障壁なくOpenID標準を採用し、実装することが容易になる。

2025年、OIDFはOpen Wallet Foundationの理事会に[アソシエイト代表](#)として参画した。この期間中、両組織はOpen Wallet FoundationのプロジェクトがOIDFの適合性機能をどのように活用できるかを模索した。また、OIDFは2025年6月にジュネーブで開催された「[Global Digital Collaboration](#)」イベントを共同開催し、デジタルアイデンティティエコシステム全体の関与を促進した。

OIDFは、2025年を通じてModular Open Source Identity Platform（MOSIP）とのパートナーシップを継続した。

MOSIPは、Bluetooth経由のOpenID for Verifiable Presentation（OpenID4VP）に貢献した。

- MOSIPのプラットフォームは、ウォレットおよび検証可能なクレデンシャル機能において、引き続きOpenID4VPおよびOpenID4VCIをサポートした。

- OIDFの専門家は[MOSIP Connectイベント](#)にも参加し、MOSIPオープンソースコードの各国実装者と直接連携した。

OIDFはまた、世界銀行、MOSIP、およびその他の政府間・非営利パートナーに加わり、[Digital Convergence Initiative \(DCI\)](#) とその標準委員会を支援した。OIDFの[Ecosystem Support Community Group \(ES CG\)](#) のリーダーたちは、DCIによる仕様のデューデリジェンスに情報を提供するため、積極的なフィードバックを提供した。

その後、DCIワーキンググループは、**National ID Security Profile (NISP)** のコアコンポーネントとして、OIDFの3つの仕様を選定した。

- OpenID4VP
- OpenID4VCI
- FAPI 2.0

社会給付プログラムにNISPを選択する法域は、国内および国境を越えた相互運用性、セキュリティ、および規模の目標をサポートする、実証済みの仕様から恩恵を受けることになる。

パートナーシップ

戦略的パートナーシップが強化され、[Bloombergがメンバーとしてコミュニティに加わり、AuthZENへの使途指定資金の提供](#)を約束した。一方で、[Cloud Signature Consortium](#)、[FIDO Alliance](#)、および[Open Wallet Foundation](#)との協調により、金融、サイバーセキュリティ、およびオープンソースコミュニティにおける分野横断的な結びつきが深まった。

リエゾンおよび標準化団体とのパートナーシップ

OIDFは、OpenID仕様が補完的な標準とスムーズに統合され、エコシステムの断片化を防ぐために、世界中の標準化団体や業界組織と正式なパートナーシップを維持している。

- ISO/IEC リエゾン：
 - カテゴリAステータス：[SC68 and SC17](#)
 - カテゴリAステータス申請中：[SC27](#).
- Standards body liaisons or memoranda of understanding (short list):
 - [ITU-T](#),
 - [FIDO Alliance](#),
 - [ETSI](#),
 - [EMVCo](#),
 - [Decentralized Identity Foundation \(DIF\)](#),
 - [GSMA](#),
 - [Linux Foundation](#),
 - [IETF](#),
 - [W3C](#),
 - [Cloud Signature Consortium](#),

- [SIA/OSIA](#).
- Industry memberships:
 - [Financial Data Exchange \(FDX\)](#)
 - [Open Wallet Foundation](#)
- Observer roles:
 - [国際決済銀行（Bank of International Settlements）のProject Aperta](#).

これらのパートナーシップにより、OIDFの仕様は、競合するアプローチを生み出すのではなく、同等の組織による標準と連携して機能することが保証される。

パートナー組織へのリエゾンとしての活動に関心がある者は、<mailto:director@oidf.org> まで連絡されたい。すべてのパートナーシップは、OIDFのリエゾン委員会によって承認される。

第5部: 次に来るものへの備え

新たな課題に関する公的な議論の牽引

多くの組織が今日の展開のみに焦点を当てる中、OIDFは次に来るものに向けてエコシステムを準備させるという極めて重要な役割も果たしている。OIDFは、より広範な議論を形成し、政府、企業、そして社会がデジタルアイデンティティをどのように捉えるかに影響を与えてきた。

2025年、OIDFは、死とAIという、まったく異なる2つの文脈において、安全で倫理的、かつ責任ある権限委譲に関する新たなソートリーダーシップの方向性を展開した。OIDFは、リファレンスアーキテクチャのガイダンスを提供することでエコシステムを支援し、また、分析やステークホルダーとの連携を通じて、グローバルに相互運用可能なデジタルクレデンシャルを構築する取り組みを支援した。

死とデジタル遺産

9月、OIDFは、不都合な真実に向き合う包括的な新しい研究論文『[Unfinished Digital Estate](#)（未完のデジタル遺産）』を公開レビューに付した。デジタルライフが通常の寿命を超えて存続するようになった現在、ほとんどの社会は、人々が死亡または意思能力を喪失した際に何が起こるかについて、依然として準備ができていない。



Dean H. Saxe氏、Mike Kiser氏、およびHeather Flanagan氏が「[Death and Digital Estate Community Group](#)」と共同で作成したこの論文は、電子メールアカウントや創作活動から、作成した個人よりも長く存続する可能性のあるAI生成コンテンツに至るまで、デジタルレガシーの全領域を扱っている。本研究は、立法機関や標準化団体にフレームワークを提供すると同時に、デジタル時代における尊厳、レガシー、そして備えに関する本質的な議論を喚起するものである

AIとアイデンティティ管理

6月、OIDFはまだほとんど誰も直面していなかった課題、すなわち「自律型AIエージェントをいかに安全に認証・認可するか」に対処するため、「[AI and Identity Management Community Group](#)」を結成した。10月、OIDFは、Tobin Southが主導する[ホワイトペーパーを公開](#)し、既存のフレームワークにおけるギャップを評価するとともに、AIシステムが人や組織を代理して動作する際に、明確なガバナンス、説明責任、および制御の下で機能するパラダイムに向けた極めて重要なステップを提案した。

同コミュニティグループは現在145名以上の参加者を擁し、毎週会合を開いて、標準化の現状、ギャップ分析、およびより幅広い議論（分類学、ユースケース、脅威モデリングなど）に資する成果物の推進に取り組んでいる。また、AIIM CG（AI and Identity Management Community Group）は、政府からの情報提供依頼（RFI）や意見募集（RFC）に対する回答を一本化する役割も果たしており、国家規模および世界規模での能力開発の推進を支援している。



オンラインにおける年齢確認と未成年保護

2025年には、OIDF理事会の監督下にある、オンラインにおける児童の安全という文脈での権限委譲のテーマに触れた3つ目の公開文書も作成された。これは2026年上半期にパブリックコメント向けのドラフトとして公開される予定である。この取り組みは、[eKYC and Identity Assurance Working Group \(eKYC and IDA WG\)](#)との提携により育成されてきたものであり、権限委譲に関連する要件は同ワーキンググループにおいて策定が進められている。この分野の分析や仕様策定に関心のある者は、eKYC and IDA WGに参加し、ドラフトペーパーへのフィードバックを提供することが推奨される。

KYC規制を遵守するための金融業界におけるmDLおよび検証可能なクレデンシャルの採用拡大

11月、OIDFは、[複数の州やウォレットから提供されるモバイル運転免許証 \(mDL\) を銀行がいかにして信頼すべきか、という極めて重要な課題の解決を支援するため、Juliana Cafikが主導した研究成果](#)を公開した。NISTのNCCoE技術ブループリントに準拠したこの取り組みは、OIDFおよび[ISO/IEC SC17 WG10](#)の現行の仕様が、現在いかにして規制遵守（レギュラトリーコンプライアンス）を実現しているか、また、米国市場における金融機関によるmDLおよびVerifiable credentialsの採用を促進するために、他に何が必要であるかを示している。

2025年12月と2026年1月には、このフレームワークが欧州連合（EU）、オーストラリア、およびニュージーランドの金融機関向け規制文脈にどのように適用されるかについても対応するため、報告書が更新された。この取り組みは現在、**eKYC and IDA WG**の[新しい作業項目（new work item）](#)の下で進められており、複数の法域におけるKYCポリシーへのプロトコルレベルでの準拠を容易にするために、仕様におけるギャップを埋めることを目標としている。



オープンデータエコシステムの支援

95カ国以上がオープンバンキングおよびオープンデータの取り組みを推進する中、OIDFは13のFAPIベースのオープンデータ展開を支援している。この経験を踏まえ、[2025年に発足](#)したOIDFのEcosystem Support Community Group（ES CG）は、[Open Banking Reference Technical Architecture](#)のドラフトを公開した。このガイドは、各国が自国のオープンバンキングシステムに適した技術標準を選択するのを支援すると同時に、国内における機能性と将来的な国境を越えた接続性の確保を両立させるものである。

ES CGは、エコシステムの意思決定者がアーキテクチャの選択肢について議論し、他法域の意思決定者やOIDFの専門家からピアサポートを受けられる無償のフォーラムを提供している。このコミュニティは、技術的およびガバナンス上の課題について率直に議論できる安全な場を提供している。

コミュニティ全体における長年のFAPI 1.0およびFAPI 2.0の展開経験を活かし、ES CGは、アーキテクチャのデューデリジェンス、地域の要件を満たすための仕様プロファイリング、ならびに立ち上げおよびそれ以降に向けたロードマップ策定においてエコシステムを支援する。新興のエコシステムは、同様の課題をすでに克服した同業者の経験から恩恵を受けると同時に、国境を越えた相互運用性などの将来的な発展を支える関係を構築することができる。

EUデジタルアイデンティティウォレット（EUDIW）コミュニティ向けの専用リソース

12月、OIDFは、[欧州のデジタルウォレットおよび検証可能なクレデンシャル（verifiable credentials）の実装者に向けた専用のリソースハブ](#)を開設した。このハブは、eIDAS 2.0の実装に必要な仕様、テストツール、および実践的なガイドラインを組織に提供するも

のである。OIDFは、本報告書で前述した欧州委員会主催の「EUDIW Launchpad」イベントを利用して、このリソースハブを立ち上げた。



SIDI ハブ

OIDFは、電話、電子メール、パスポートと同様に、国境を越えたデジタルアイデンティティの相互運用性の実現を目指す「SIDIハブ（Sustainable and Interoperable Digital Identity Hub）」の[共同主催者および共同資金提供者](#)として、継続的に積極的な役割を果たしてきた。45カ国以上および25の組織を結集し、OIDFは技術および政策のワークストリームを主催したほか、[アディスアベバ](#)と[パリ](#)でサミットを開催した。



この取り組みにより、サイバーセキュリティを扱う[ITU-T第17研究グループ（ITU-T Study Group 17 on Cybersecurity）](#)において、新たなITU-T作業項目（SG17 #145）が採択されるに至った。これは、個人アイデンティティ、法人アイデンティティ、および非人間（ノンヒューマン）アイデンティティにおけるギャップを特定し、技術、政策、および相互運用性のギャップを埋めるために必要な作業を定義することを目的としている。

OIDFの支援のもと、SIDIはトラスト管理報告書を作成し、10の国内トラストフレームワークのマッピングを拡張した。これは、金融サービス、難民アイデンティティ、教育資格証明など、SIDIが過去に実施した先進的なユースケースの分析成果を基盤としている。



Cross-Border “Champion” Use Cases

Approach

- Use Case demand from past efforts & Summit attendees
- Score 30+ Use Cases and prioritize based on opportunity & benefits
- Interview global experts & organizations
- Document use case insights, benefits, and collaborative opportunities
- This analysis grounds SIDI hub’s policy & technical workstreams

Education Experts	Displaced People	Open a Bank Account
• GEANT / EduGAIN • UNESCO • Groeninger Declaration Network • MIT Digital Credentials Consortium • Jobs for the Future	• UNHCR • US Department of Homeland Security • Japanese Gov’t • California DMV	• NIST NCCoE mDL Project (US) • DNP/Meeco/ConnectID (Australia & Japan) • EUDI Wallet use case (Europe) • Utah DMV (US) • SelectID (UK)

主要なフォーラム

OIDFは、主要な国際フォーラムにおいて重要な議論を形成し、デジタルアイデンティティの実装と相互運用性における新たな課題に対処してきた。

主な活動は以下の通りである。

- リレストロムで開催された「[インターネットガバナンスフォーラム（IGF）2025](#)」において、デジタルアイデンティティの主権と国境を越えた相互運用性のバランスに関するワークショップを共同開催し、アフリカ、アジア、欧州の政策立案者、技術専門家、市民社会の主体を交え、途上国および後発開発途上国向けの包摂的なデジタルアイデンティティソリューションの推進について議論した

**IGF²⁰
NORWAY**

20TH INTERNET GOVERNANCE FORUM
Main Theme: *Building Digital Governance Together*

Workshop Title:
**SOVEREIGNTY AND INTEROPERABLE
DIGITAL IDENTITY IN DLDCs**

June 25, 2025
7:00 - 8:30 am (UTC)
Lillestrøm, (Room 6) Norway & Online
(8:00am Abuja | 9:00am Joburg | 10:00am Nairobi)

Moderator:
Ms. Gail Hodges
Executive Director,
OpenID Foundation & Special Advisor California
DMV, North America

Speakers:

Mr. Ter Alvik
Registrar, Agency for public
Mgmt. & e-Government, Europe

Eng. Dr. Alissio Coker-Adasun
Chair/CEO National Identity Mgmt
Commissioner (NIMC), Africa

Dr. Jimson Olufeye
CEO, Interoperable Identifying
Roundtable Chair, Chair of the
Advisory Council, ANCTA, Africa

Mr. Naohiro Fujie
Chair, OpenID Foundation
Japan, Asia

Dr. Kessi AMESSINOU
Chief, Private Sector Monitoring
& Support Service, Ministry of
Economy & Finance, Chair,
ONG Women Be Free, Africa

Ms. Debara Comparin
Technical Director of the Secure
Identity Alliance, Europe

ARCTA
Africa 2025 Alliance

SIDIHub

- 米国連邦政府主催の「mDL Day」において「Voices of the Future」パネルのモデレーターを務め、全米5つの州のリーダーを招いてモバイル運転免許証（mDL）の導入における課題を議論した。
- 「西バルカン・デジタルサミット（Western Balkans Digital Summit）」においてウォレットの相互運用性について登壇し、新興デジタル経済圏における国境を越えたアイデンティティの課題に対処した



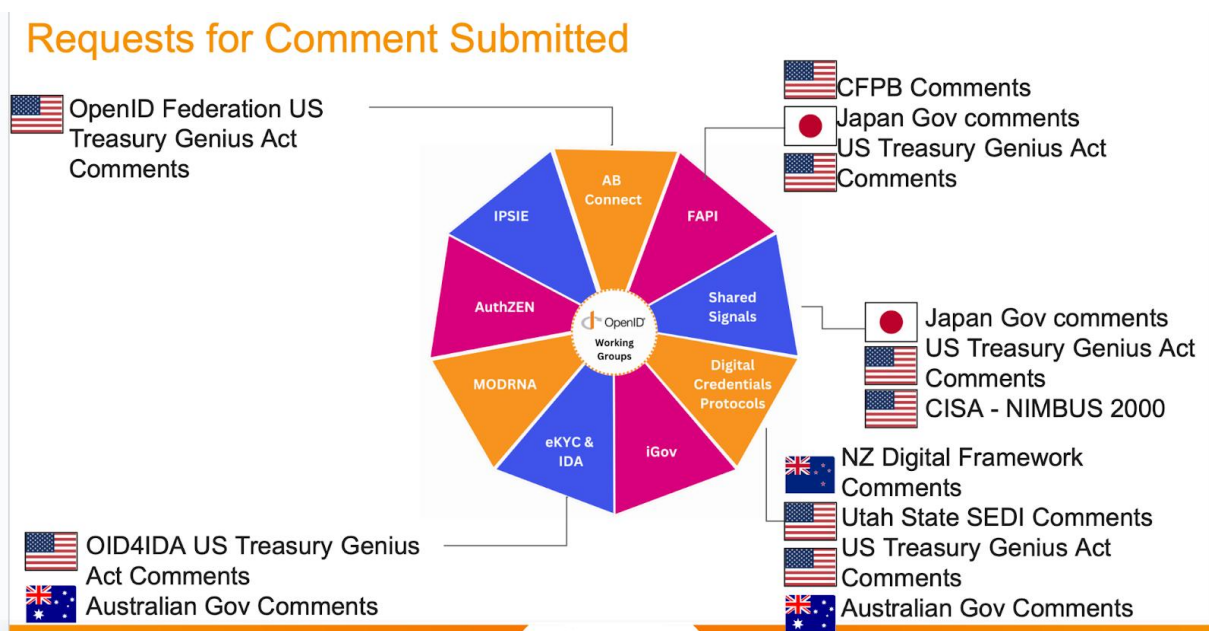
- デジタルアイデンティティに関する「[G20 TechSprint](#)」の審査員を務め、現実世界のアイデンティティ問題に対する革新的なソリューションを評価した

- 「[Identiverse](#)」や「[European Cloud and Identity Conference](#)」などのカンファレンスから、「[Internet Identity Workshop \(IIW\)](#)」などのフォーラムに至るまで、その他多くのイベントで議論を主導した。

これらのエコシステムパートナーシップや公開フォーラムを通じて、OIDFは、新たな標準化の課題や実務上の導入障壁に関する最先端の知見を提供してきた。OIDFのアプローチは「すべての船を引き上げる（全体の底上げを図る）」ことを中心に据えており、AIエージェントから国境を越えた相互運用性に至るまで、デジタルアイデンティティにおける新たな課題に協調して取り組むことで、いかなる実装者、国家、エコシステムも取り残されないようにすることを目指している。

政策および政府との連携

デジタルアイデンティティが世界中の政策アジェンダで重要性を増す中、OIDFは規制に関する議論において不可欠な発言者となった。2025年、OIDFは、[米国国立標準技術研究所 \(NIST\)](#)、[米国消費者金融保護局 \(CFPB\)](#)、[ユタ州のデジタルアイデンティティプログラム](#)、オーストラリア生産性委員会、そして主権と相互運用性のバランスをテーマとした[インターネットガバナンスフォーラム](#)での議論を含め、世界中の規制当局に対して専門的な知見を提供した。



これらの連携を通じて、新たに策定されつつある法律や規制が、実証済みでオープン、かつグローバルに相互運用可能な標準に常に裏づけられたものとなるよう担保してきた。

まとめ：2025年が証明したもの

OIDFの標準は、世界のデジタルインフラストラクチャの一部としてますます不可欠なものとなっている。国際的な認知は信頼を確立した。相互運用性テストは現実世界における実用性を証明した。国家およびエコシステム規模での展開は、そのスケーラビリティを実証した。そして、未来を見据えたリーダーシップにより、新たなリスクや機会への早期の対処が確実に行われている。

デジタルウォレットが世界中に普及し、より多くの法域が国境を越えたクレデンシャルを展開し、AIシステムが人や組織を代理して動作することが増え、さらにリスクシグナルがかつてないほど複雑化する中、我々のコミュニティは引き続きこの課題に立ち向かっている。OIDFのミッションを支える素晴らしいメンバーやコントリビュータ諸氏と、今後も協力を継続できることを大変嬉しく思う。2025年に完了した取り組みは、2026年、2027年、そしてそれ以降におけるデジタルアイデンティティのあり方を決定づけるものとなるであろう。

感謝を込めて。



2025年4月、サニーベールにて開催されたプレIWワークショップに集結したコミュニティ



2025年10月、OpenID Foundation理事会

OpenID Foundation指導部の振り返り

本報告書を締めくくりにあたり、OIDFの指導部は、本書に記載された2025年の進展と成果に伴う責任について、いくつかの振り返りを共有したい。

OIDF標準の採用が世界規模で加速する中、我々は急速な成長が機会だけでなくリスクをももたらすことを認識している。我々のプロセスに対する信頼を維持し、仕様および適合性プログラムの品質が堅牢であり続けることを保証しながら、運用の規模を拡大することは、我々が真摯に受け止めている課題である。

そのために、2026年において我々は、何を提供するかということと同様に、我々がどのように取り組むかという点にも同等の注力することを約束する。我々は、既知の標準開発要件を満たすだけでなく、AIが従来の標準開発を破壊する際に生じるであろう需要を予測することを目指し、標準化のベストプラクティスに関連した我々の活動方法の自己監査を開始した。我々は、プロセスにおけるギャップを埋め、グローバルなオープン標準化団体にふさわしい制度的段階（インスティテューショナル・グレード）の基盤を確保することを目指している。厳格なプロセスそれ自体が、その根底にある仕様への信頼に対する主要な貢献要素であり、その信頼は一度確立された後も能動的に維持されなければならないことを、我々は理解している。

我々がこの取り組みを進めるにあたり、コミュニティからの率直なフィードバックを歓迎する。我々の目の前にある機会は極めて大きい。しかし、我々の使命を尊重し、メンバーをサポートし、市場の現在の局面に適う方法でその機会を十分に捉えるためには、我々が管理する仕様に求めるものと同等の厳格さと透明性の基準を、我々自身にも課すことが求められる。

OpenID Foundationについて

OIDFは、人々が自ら選択するあらゆる場所でアイデンティティを表明できるよう支援することに尽力する、グローバルなオープン標準化団体である。2007年に設立されたOIDFは、安全で相互運用可能、かつプライバシーを保護するオープンなアイデンティティ標準の創出を主導する技術専門家のコミュニティである。OIDFのOpenID Connect標準は、現在、数百万のアプリケーションにわたり数十億の人々に利用されている。過去5年間において、相互運用可能で高度なセキュリティを実現するOAuth2ベースのFAPI標準は、オープンバンキングおよびオープンデータ実装のための事実上の標準となり、人々が組織をまたいでデータにアクセスし、共有することを可能にした。今日、OIDFの標準は、人々がインターネット規模でアイデンティティを表明し、自身のデータにアクセスすることを可能にする結合組織（コネクティブ・ティッシュ）であり、世界規模で「ネットワークのネットワーク」が相互運用することを可能にしている。個人、企業、政府、および非営利団体の参加を推奨している。詳細については、openid.netを参照されたい。

適合性テストおよび自己認定の詳細については、OIDFの[FAQ](#)セクションを参照されたい。