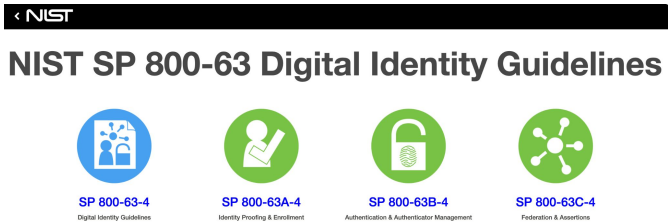
学術認証基盤における次世代認証と認証強度の考え方

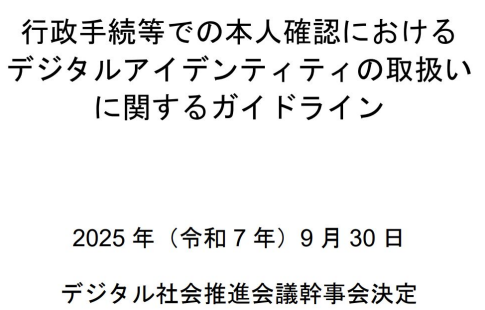
近年、Passkeysなどのパスワードレス認証をはじめとする次世代認証方式の導入が進んでいます。一方、学術認証フェデレーションのように複数のサービスが共通の認証基盤を利用する環境では、サービスごとに求められる認証強度が異なるなど、認証方式と認証強度の関係をどのように扱うかが課題となっています。

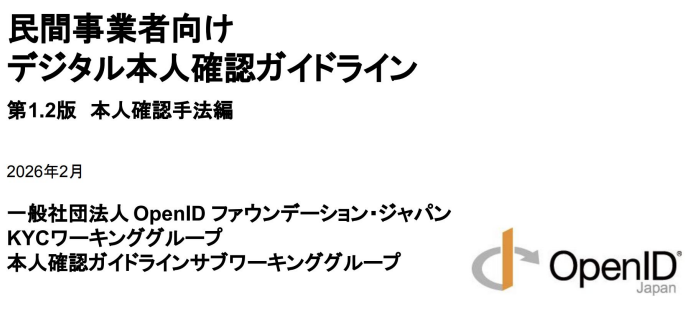
- デジタル認証における保証レベル（IAL/AAL）の基本的な考え方を整理
- フェデレーション環境における認証方式と認証強度の課題について紹介
- Shibboleth環境において認証強度を考慮した認証機能を実装した事例
- 大学における実証的な取り組みを紹介
- 学術認証基盤における次世代認証のあり方について議論

2025年はデジタルアイデンティティの基準が改訂された年でした

- NIST SP 800-63 Rev.4 Digital Identity Guidelines pages.nist.gov/800-63-4/
- DS-511 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 www.digital.go.jp/resources/standard_guidelines#ds511
  - DS-512 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に関するガイドライン解説書
- 民間事業者向け デジタル本人確認ガイドライン 第1.2版 本人確認手法編 www.openid.or.jp/news/2026/02/-12.html







なぜ改訂されたの？

（中村の勝手なまとめです

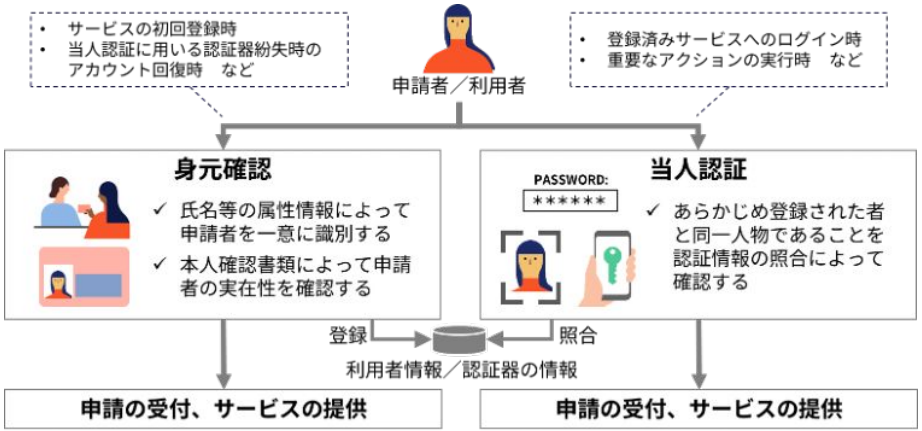
- オンラインでの手続きやサービスが当たり前に
- フィッシング，本人確認書類の偽造，ディープフェイクなど脅威が日常に
- パスキー，Verifiable Credentialsなど次世代技術がこれから普及期に

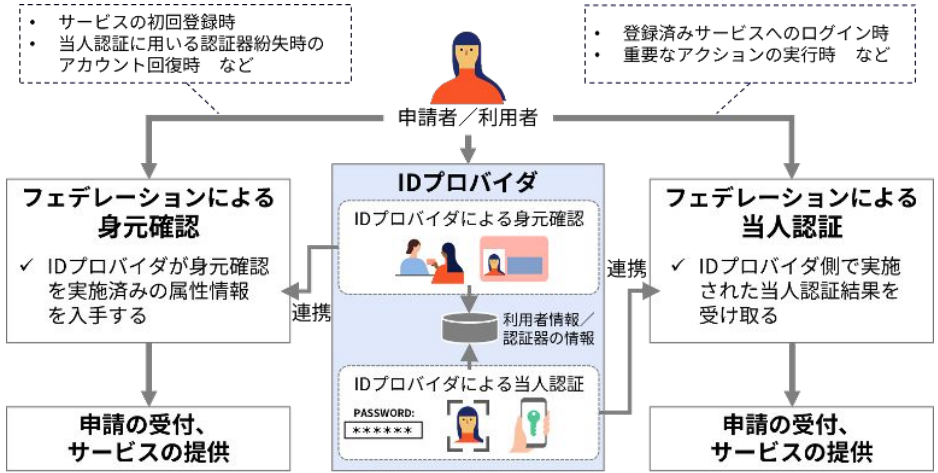
- フィッシング耐性，公開鍵認証，Verifiable Credentialsに関する記述を充実
  - リスク管理，ユーザに対する配慮に関する記述も充実
  - 毎度のことですがパスワード要件も進化
  - （とってもボリューミーです...

本人確認とは

身元確認と当人認証から構成され，フェデレーションによりプロセスの一部を第三者に頼ることもできる

- 利用者，提供者，関係者がなぜ，どういったプロセスが採用されているか認識を共有することが大事





「DS-511 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」より

本人確認の確らしさを保証レベルとして3段階で定義

- 当人認証 Authentication → **Authentication Assurance Level (AAL)**
  - **AAL3** 多要素認証, フィッシング耐性を必須, **AAL2** 多要素認証を必須，フィッシング耐性は選択可, **AAL1** 単要素認証 (DS-511)
  - **AAL1** Provide minimal protections against attacks. Deter password-focused attacks, **AAL2** Require multifactor authentication. Offer phishing-resistant options, **AAL3** Require phishing resistance and verifier compromise protections (NIST)
- 身元確認 Identity Proofing → **Identity Assurance Level (IAL)**
  - **IAL3** デジタル署名の検証 , **IAL2** 信頼できる情報源への照会 or 対面での物理的検査を許容 , **IAL1** 非対面での物理的検査を許容 (DS-511 位置づけ)
  - **IAL1** Limit highly scalable attacks. Protect against synthetic identity, **IAL2** Limit scaled and targeted attacks. Protect against basic evidence falsification and theft, **IAL3** Limit sophisticated attacks. Protect against advanced evidence falsification, theft, and repudiation. Protect against advanced social engineering attacks (NIST Control objectives)
- フェデレーション → **Federation Assurance Level (FAL)**
  - **FAL1** Protect against forged assertions, **FAL2** Protect against forged assertions and injection attacks, **FAL3** Protect against IdP compromise (NIST)

AALの改訂 (NIST)

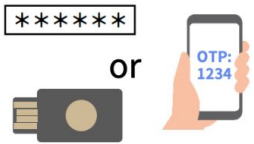
例えばAAL3だと（hardware → non-exportable

- **3版**: Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a **“hard”** cryptographic authenticator that provides *verifier impersonation resistance*.
- **4版**: Authentication at AAL3 is based on the proof of possession of a key through the use of a cryptographic protocol and either an *activation factor* or a password. AAL3 authentication requires the use of a public-key cryptographic authenticator with a **non-exportable** private key that provides *phishing resistance*.

AALの改訂 (DS-511)

当人認証保証レベルの見直し

- 当人認証保証レベルについては大幅な変更は行わないが、フィッシング攻撃など最新の脅威動向、技術動向、国民向けの行政手続等において想定されるリスク等を考慮し、脅威耐性の観点から各レベルの対策基準を一部見直す。

保証レベル	対策基準	
	認証要素	脅威への耐性要件
当人認証 保証レベル3	**「公開鍵暗号に基づく認証器」を含む多要素認証** 例） ・ 暗証番号付きのICカード ・ パスキー 	・ **フィッシング耐性（必須）** 「必須」：全ての利用者に対してフィッシング耐性をもつ認証方式を適用する ＋ ・ 保証レベル2の耐性
当人認証 保証レベル2	**多要素認証** 例） ・ 暗証番号付きのICカード ・ パスキー ・ パスワード ＋ワンタイムパスワード 	・ **フィッシング耐性（推奨）** 「推奨」：フィッシング耐性をもつ認証方式を利用者に対して提供し、その利用を推奨するが、他の認証方式についても選択可能とする ・ **認証器等の盗用に対する耐性** ※ICカードやパスワード等の認証要素のうち一つが盗用された場合の耐性 ＋ ・ 保証レベル1の耐性
当人認証 保証レベル1	**単要素認証**（又は多要素認証） 例） ・ パスワード ・ ワンタイムパスワード ・ USB接続型セキュリティキー ・ 又は保証レベル2以上の手法 	・ 盗聴 ・ リプレイ攻撃 ・ オンライン上での認証情報の推測

「本人確認ガイドライン改定方針　令和6年度とりまとめ」より

IALの改訂 (NIST)

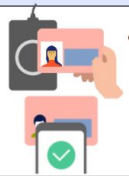
例えばIAL1だと（3版のIAL1はなくなり，3版のIAL2（の一部）が4版のIAL1に）

- **3版**: **There is no requirement** to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the subject's activities are self-asserted or should be treated as self-asserted (including attributes a CSP asserts to an RP). **Self-asserted attributes are neither validated nor verified**.
- **4版**: IAL1 supports the real-world existence of the claimed identity and provides some assurance that the applicant is associated with that identity. Core attributes are obtained from identity evidence or self-asserted by the applicant. **All core attributes are validated against authoritative or credible sources**, and **steps are taken to link the attributes to the person undergoing the identity proofing process**.

IALの改訂 (DS-511)

身元確認保証レベルの見直し　―　全体概要

- 昨今の脅威動向を踏まえ、身元確認保証レベルは「ICチップ等によるデジタル的な検証の有無」を、保証レベルの差として表現できるように改定する。また低リスクの手続・サービス向けの保証レベルとして「レベル1」を定義※する。（※現行ガイドラインの「レベル1」は「身元確認なし」の位置づけであったが、今回の改定で簡易的な身元確認を行うレベルとして再定義する。）

保証レベル	保証レベルの位置づけ	
	本人確認書類の検証手法	申請者の検証手法
身元確認 保証レベル3	 • ICチップ等による**デジタル的な検証を必須**とし、**偽造や改ざんに対する厳格な耐性**を確保するレベルとする。（「デジタル的な検証」：発行者によって付与されたデジタル署名等による暗号学的な検証を行うこと。）	 • 本人確認書類の盗用に対し、**容貌の確認**又は**暗証番号による検証**を必須とする。 暗証番号: ＊＊＊＊ • 本人確認書類の貸し借りに対しては、対象手続のリスクに応じた個別検討※を行うこととする。 ※ 暗証番号のみでは本人確認書類の貸し借りを検知できないため、貸し借りのリスクを許容できない場合は「容貌の確認」の追加実施等を検討する。
身元確認 保証レベル2	 • 本人確認書類の**物理的な券面の検査等も許容**する。ただし検証強度を考慮しカメラ越しや複写物による検査（非対面での券面検査）は不可とし、一定の耐性を確保する。	
身元確認 保証レベル1	 • 保証レベル2までの手法に加えて、**非対面での券面検査（カメラでの撮影、複写物の郵送等）も許容**する。偽造・改ざんへの簡易的な耐性をもつレベルとして位置付ける。	 • 保証レベル2までの手法に加えて、**本人確認書類に記載された住所等に確認コードを送付することでの間接的な検証**も許容する。（例：当該住所に居住していることをもって、本人確認書類との紐づきを確認する 等）

「本人確認ガイドライン改定方針　令和6年度とりまとめ」より

FALの改訂 (NIST)

その前にOpenID Connectがメインに, Subscriber-Controlled Walletsが追加された

- **3版**: 暗号化の有無
- **4版**: 脅威対策と
  信頼の確立

FAL2ではIdP-initiated SSOと
front-channel presentationはNG

FAL	Requirement
1	Bearer assertion, signed by IdP.
2	Bearer assertion, signed by IdP and encrypted to RP.
3	Holder of key assertion, signed by IdP and encrypted to RP.

3版

Requirement	FAL1	FAL2	FAL3
Audience Restriction	Multiple RPs allowed per assertion; single RP per assertion recommended	Single RP per assertion	Single RP per assertion
Replay Protection	Required per RP	Required	Required
Assertion Injection Protection	Recommended for all transactions	Required; transaction begins at the RP	Required; transaction begins at the RP
Trust Agreement Establishment	Subscriber-driven or pre-established	Pre-established	Pre-established
Identifier and Key Establishment	Dynamic or Manual	Dynamic or Manual	Manual
Presentation	Bearer Assertion	Bearer Assertion	Holder-of-key Assertion or bound authenticator

4版