「標準化部会各WGにおけるサイバーセキュリティ標準化との関わり」

～デジタルアイデンティティの標準化動向～

デジタルアイデンティティWGリーダー
日本電気株式会社（NEC）
シニアエキスパート
宮川　晃一

自己紹介

宮川　晃一（みやかわ　こういち）

NEC 金融システム本部　シニアエキスパート
（兼務）デジタルビジネス基盤本部
（兼務）サイバーセキュリティ戦略本部
（兼務）レギュレーション調査室

【主な所属団体】
- **日本ネットワークセキュリティ協会（JNSA）**
  標準化部会　デジタルアイデンティティWGリーダ
- **クラウドセキュリティアライアンス（CSA-J）　理事**
- **FISC　オープンAPIに関する有識者検討会　委員**
- **OpenID Foundation Japan eKYC WG**
- **MyDATA Japan**
- **Guard Tech コミュニティー（保険API)**

【主な著書】
「クラウド環境におけるアイデンティティ管理ガイドライン」
「セキュリティエンジニアの教科書」
「Software Design 2020年11月号　第一特集」

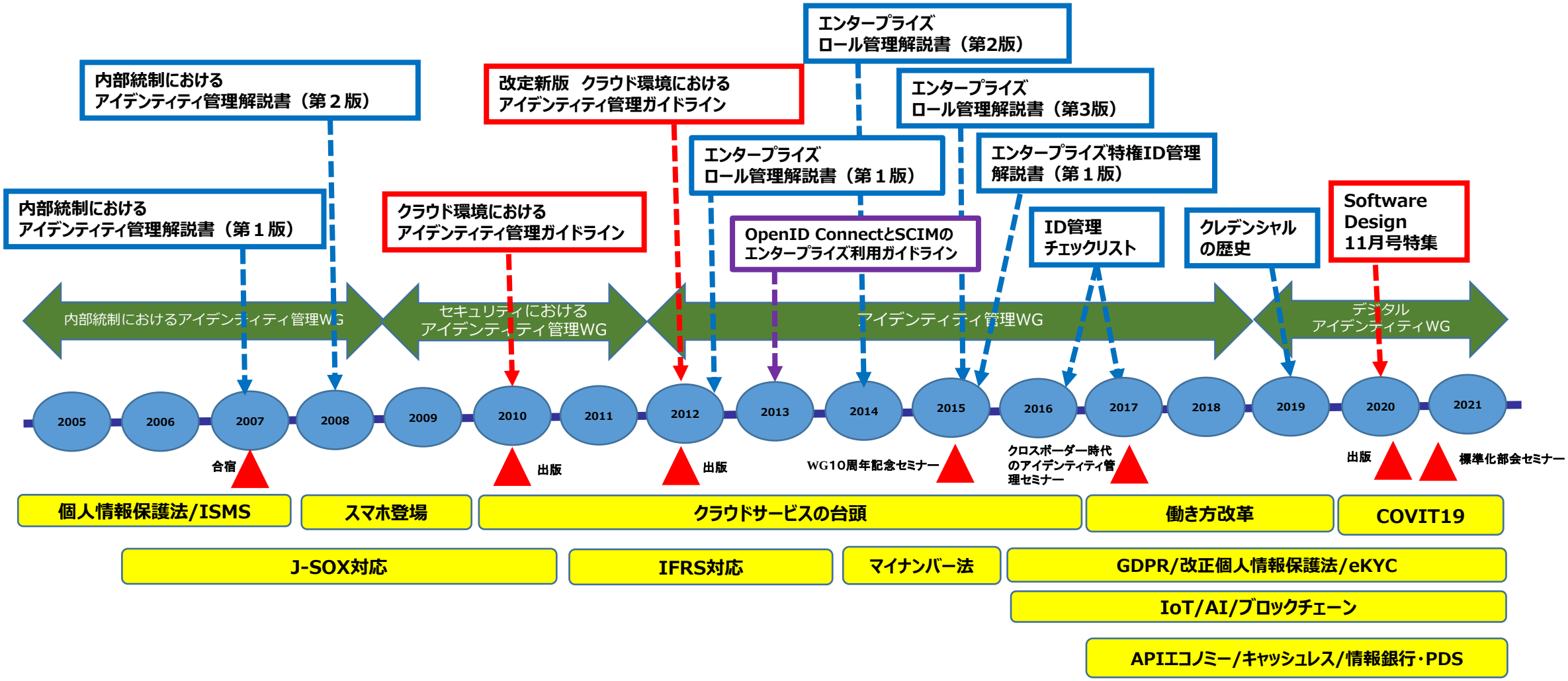
ＷＧの活動目的

「デジタルアイデンティティＷＧの活動目的」

本WGでは、デジタルアイデンティティの課題等について幅広く議論し、導入指針（ガイドライン）や各種レポートの提示などにより、啓蒙活動、普及促進、人材育成、関連他団体との連携等による市場活性化等を目的とした活動を行っています。

２００５年からWGを発足し、今年で１５年目のWGです。

ＷＧの変遷とこれまでの成果物



（ご参考）成果物リンク集

１．エンタープライズロール管理解説書（第３版）
http://www.jnsa.org/result/2016/idm_guideline/index.html

２．エンタープライズにおける特権ID管理解説書（第１版）
http://www.jnsa.org/result/2016/idm_pum/index.html

３．OpenID ConnectとSCIMのエンタープライズ利用ガイドライン
（JNSAと OpenID Foundation Japan との共同執筆）
http://www.jnsa.org/press/2013/131220.pdf
https://www.openid.or.jp/news/2013/12/openid-openid-connectscim.html

４．出版書籍
＜改訂新版＞クラウド環境におけるアイデンティティ管理ガイドライン
http://www.amazon.co.jp/dp/4844395866

5．クレデンシャルの歴史
https://www.jnsa.org/result/digitalidentity/

６．Software Design 11月号　第１特集「今さら聞けない認証・認可」
https://gihyo.jp/magazine/SD/archive/2021/202111

今年度の活動内容

- **技術評論社 Software Design 11月号執筆**
  作業完了

- **エンタープライズにおける特権IDガイドライン（第２版）執筆中**
  第１版のアップデート　2021月４月ごろ発行予定

- **認証要素、認可要素、その関係の整理**
  認証や認可に使われる要素とその関係性についての議論　2021月４月ごろ発行予定

- **デジタルアイデンティティ LT大会**
  実施済み　優勝テーマ：「行動的生体認証はフィクションなのか」

- **標準化ドキュメントを読んでみる（初心者向け勉強会）**
  NIST SP-800-63 シリーズ

デジタルアイデンティティと主な標準化

1. **NIST SP800-63シリーズ (63-3/63-A/63-B/63-C)**
2. **ISO/IEC 24760-1:2019 (A framework for identity management)**
3. **OpenID Foundation (OpenID Connect/CIBA/FAPI)**
4. **FIDO (First IDentity Online)**
5. **犯罪収益移転防止法とeKYC**

NIST SP800-63シリーズ(63-3/63-A/63-B/63-C)

Digital Identity Guidelines

The four-volume SP 800-63 *Digital Identity Guidelines* document suite is available in both PDF format and online.

PDF versions of the documents are available from:

※NIST=米国国立標準技術研究所

Document	Title	URL
SP 800-63-3	Digital Identity Guidelines	https://doi.org/10.6028/NIST.SP.800-63-3
SP 800-63A	Enrollment and Identity Proofing	https://doi.org/10.6028/NIST.SP.800-63a
SP 800-63B	Authentication and Lifecycle Management	https://doi.org/10.6028/NIST.SP.800-63b
SP 800-63C	Federation and Assertions	https://doi.org/10.6028/NIST.SP.800-63c

デジタル認証のガイドライン **登録プロセスと身元確認** **認証とライフサイクル管理** **フェデレーンとアサーション**

SP 800-63-3

Digital Identity Guidelines

Identity Assurance Level（IAL）

SP 800-63A

Enrollment & Identity Proofing

Authenticator Assurance Level（AAL）

SP 800-63B

Authentication & Lifecycle Management

Federation Assurance Level（FAL）

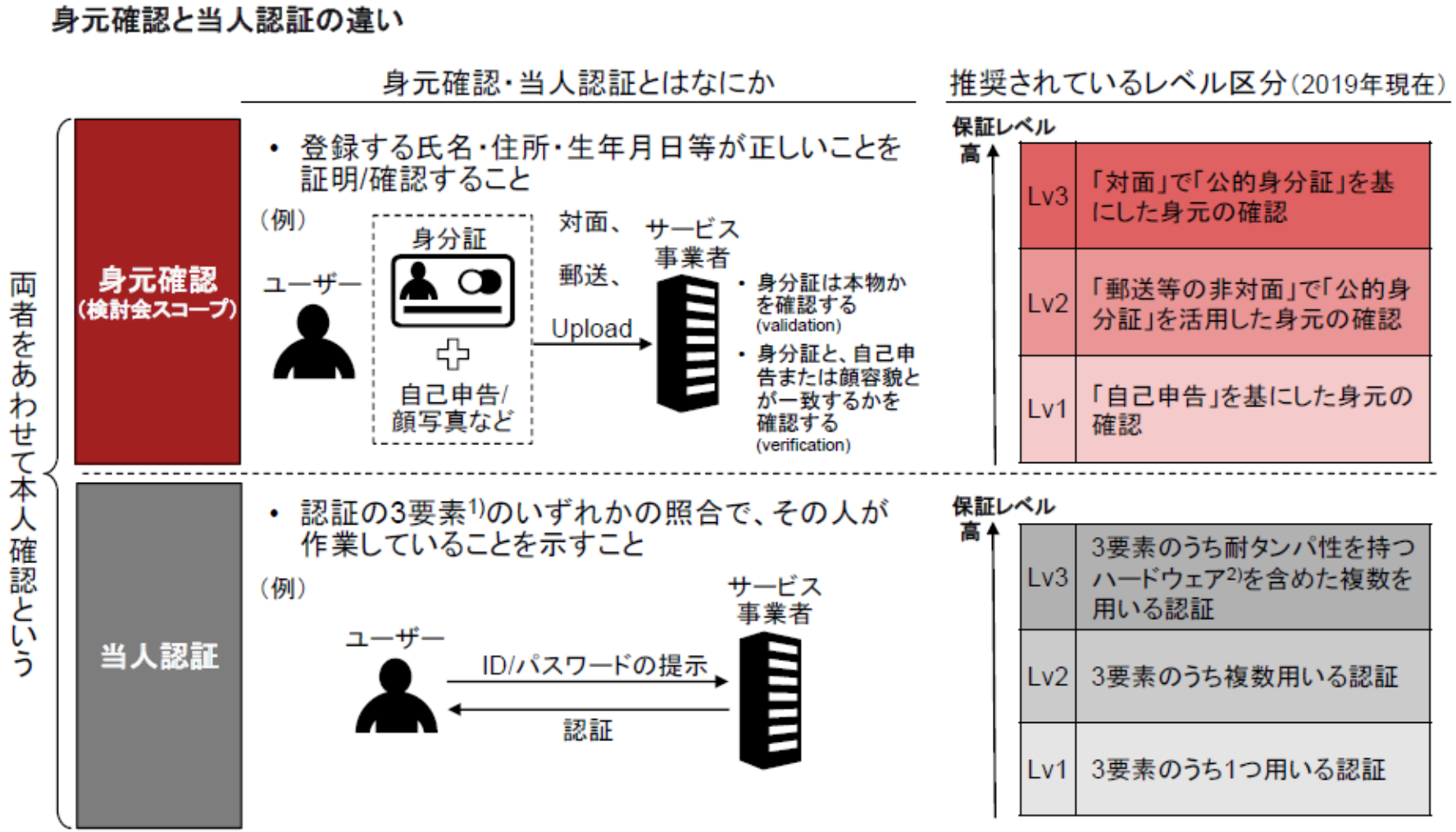
SP 800-63C

Federation & Assertions

Additional informative resources:

引用：NIST SP 800-63 Digital Identity Guidelines

本人確認＝身元確認＋当人認証



引用：オンラインサービスにおける身元確認手法の整理に関する検討報告書
https://www.meti.go.jp/press/2020/04/20200417002/20200417002.html

NIST SP800-63シリーズ(63-3/63-A/63-B/63-C)

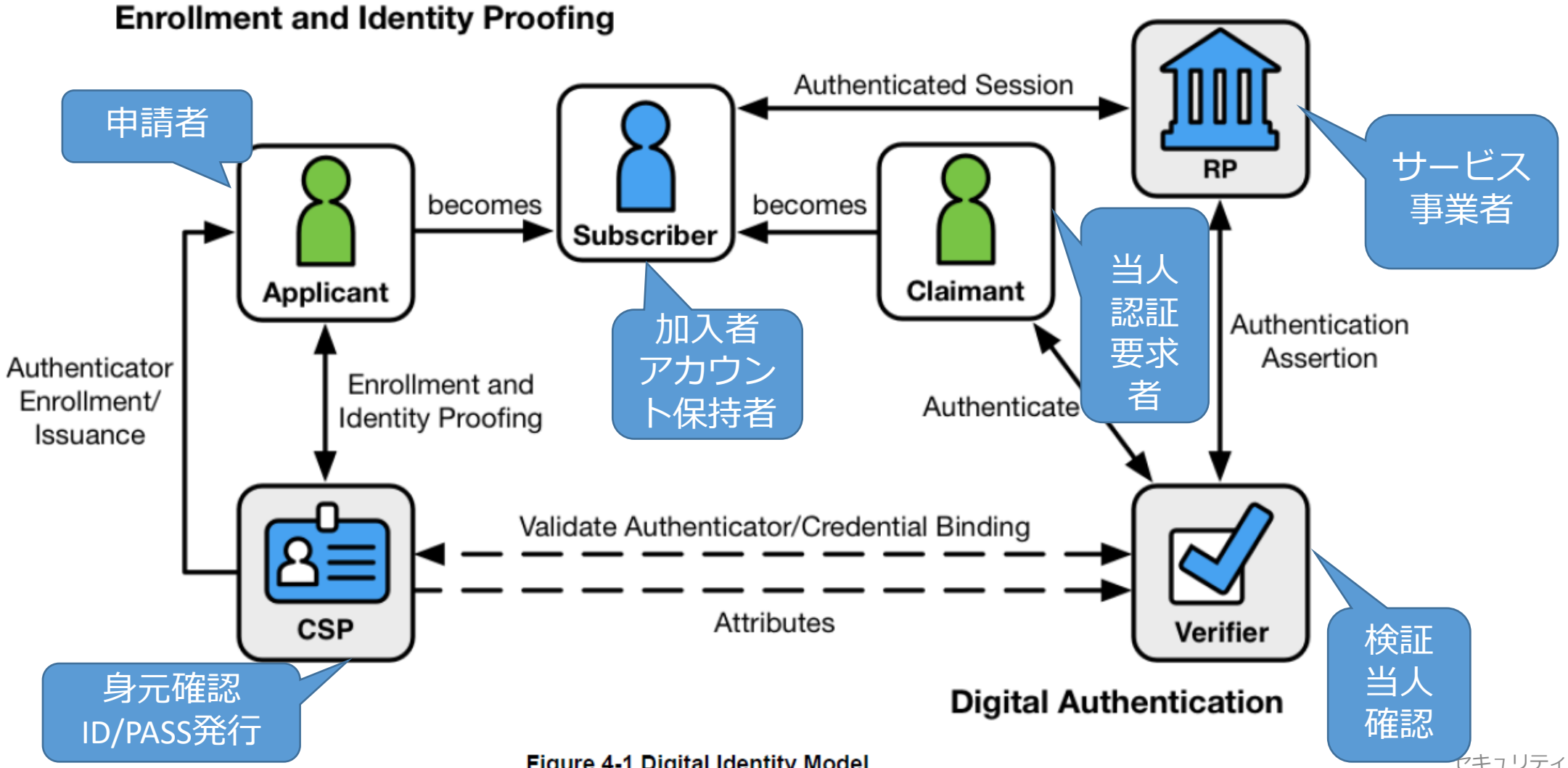


Figure 4-1 Digital Identity Model

引用：NIST SP 800-63 Digital Identity Guidelines

NIST SP800-63シリーズ(63-3/63-A/63-B/63-C)

- **Identity Assurance Level（IAL）（SP 800-63A）**
  ユーザが申請者（Applicant）として新規登録（SignUp）する際に、CSP（Credential Service Provider）が行う本人確認（身元確認）（Identity Proofing）の厳密さや強度を示す
  Lv.1 本人確認不要、自己申告での登録でよい
  Lv.2 サービス内容により識別に用いられる属性をリモートまたは対面で確認する必要あり
  Lv.3 識別に用いられる属性を対面で確認する必要があり、確認書類の検証担当者は有資格者

- **Authenticator Assurance Level（AAL）（SP 800-63B）**
  登録済みユーザー（Claimant）がログインする際の認証（当人認証）プロセス（単要素認証or多要素認証、認証手段）の強度を示す
  Lv.1 単要素認証でOK
  Lv.2 2要素認証が必要、2要素目の認証手段はソフトウェアベースのものでOK
  Lv.3 2要素認証が必要、かつ2要素目の認証手段はハードウェアを用いたもの（ハードウェアトークン等）

- **Federation Assurance Level（FAL）（SP 800-63C）**
  IDトークンやSAML Assertion等、Assertionのフォーマットやデータやり取りの仕方の強度を示す
  Lv.1 Assertion（RPに送るIdPでの認証結果データ）への署名
  Lv.2 署名に加え、対象RPのみが復号可能な暗号化
  Lv.3 Lv.2に加え、Holder-of-Key Assertionの利用（ユーザごとの鍵とIdPが発行したAssertionを紐づけてRPに送り、RPはユーザがそのAssertionに紐づいた鍵を持っているか（ユーザの正当性）を確認）

ISO/IEC 24760-1:2019
(A framework for identity management)

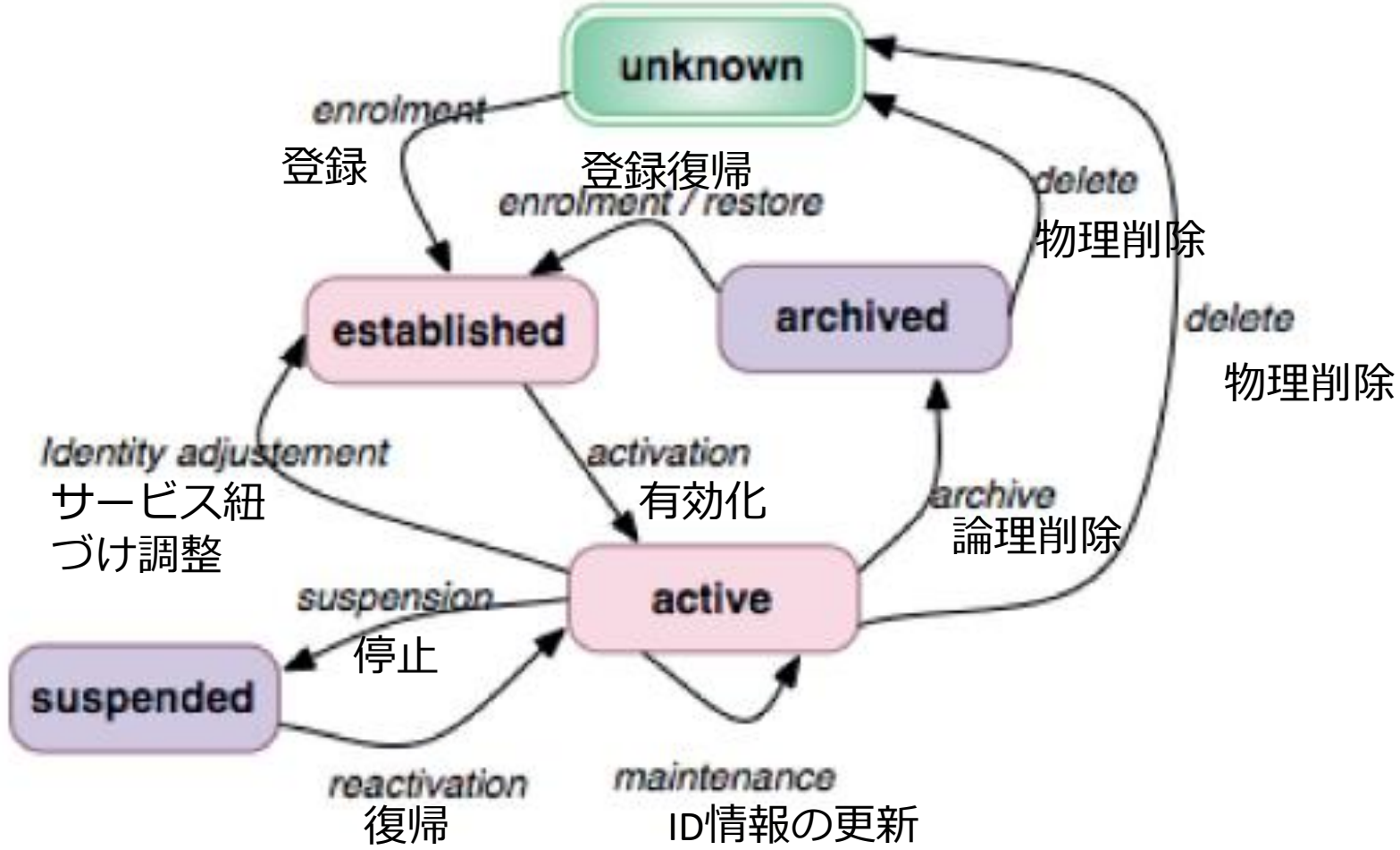


Figure 1 — Identity lifecycle

引用：https://www.iso.org/standard/77582.html

OpenID Foundation (OpenID Connect/CIBA/FAPI)

【OAuth2.0】(RFC6749)

OAuth2.0は、複数のWebサービスを連携して動作させるために使われる仕組み。通常、Webサービスを利用するためは、個別にユーザーIDとパスワードを入力してユーザーを認証する必要があるが、OAuthを利用することで、IDやパスワードを入力することなく、アプリケーション間の連携ができる認可のフレームワーク。

【OpenID Connect1.0】

OpenID Connectとは、OAuthのフローをベースにして、本来クライアント側で行っていた認証処理を、他のサーバー(OpenID Provider)にまかせて、その認証結果や属性情報を安全な方式(JSON Web Token)でクライアントが受け取って認証する方式。

【ＦＡＰＩ】

FAPI とは OpenID Foundation 傘下のワーキンググループが策定を進めている Financial-grade API (FAPI) で、非常にセキュアな OAuth プロファイルにより保護された REST/JSON データモデルの仕様群と、その仕様群をオンライン金融サービスに適用する上での実装ガイドラインの提供を目標としている。

【ＣＩＢＡ】

CIBA とは. Client Initiated Backchannel Authentication (CIBA:シーバ) は OpenID Foundation によって新たに策定された、新しいタイプの認証 (authentication) および認可 (authorization) に関する仕様の一つ。

FIDO (First IDentity Online)

- モバイル生体認証ではFIDO仕様への準拠がデファクトスタンダード
  - FIDO Alliance（米）で進めているパスワードレス認証の標準
  - 加盟企業は200社以上で、ボードメンバーにはMicrosoft, Google, NTTドコモや LINE, Bank of america, VISA等の世界的に著名な企業が多く、影響力が大きい

FIDOによる認証の仕組み

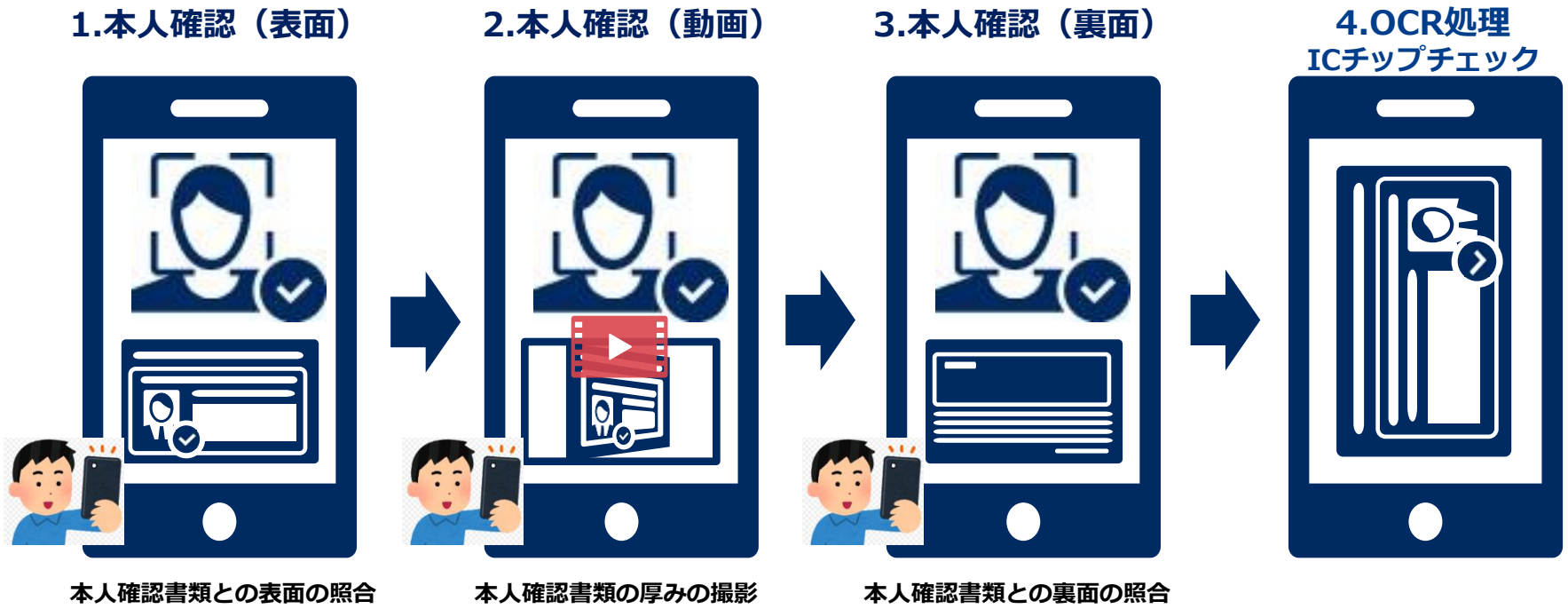
端末とサーバーをセットで標準化

主な加盟企業

改正犯罪収益移転防止法（平成30年11月30日）

（画像出典：金融庁,https://www.fsa.go.jp/news/30/sonota/20181130/01.pdf）

eKYC の実現例（NEC）



- 照合１：ライブネス
  指示通りに動作されたかを確認（ライブネス判定）　表面　裏面
- 照合2：本人の容貌
  申請者が本人である（変わっていない）ことを確認　表面　動画　裏面
- 照合3：確証の顔写真
  申請者の確証であることを確認　表面　動画

- 確証の表裏判定（AI-OCRの導入が必要、デモでは未実装）
  画像から、対象帳票の表裏の特徴量を判定

- 照合：確証の顔写真
  申請者の確証であることを確認

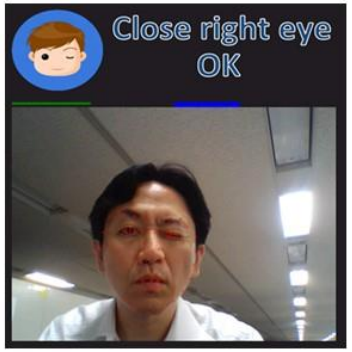
- 簡易画質＆真贋判定
  読取り帳票に対して簡易的な画質判定と真贋判定を実施
- 処理：OCR処理
  氏名、住所等券面記載事項をOCR

eKYC ライブネスによるなりすまし対策（NEC）

動作指示（ライブネス）は、犯収法改正での「ランダム動作」のチェックで活用、
パラメータで動作をあらかじめ絞ったり、スキップ機能でスマホユーザが該当アクションを飛ばすことも可能

笑顔指示

片目を閉じる指示



左右の首振り指示

口を開ける指示

両目を閉じる指示

うなずき指示