Orchestrating a brighter world

NEC

Digital Finance Thought Leadership ホワイトペーパー

デジタルアイデンティティの基礎知識

2022 年 10 月　日本電気株式会社

最近、Web3.0（ウェブスリー）のキーワードを目にすることが多くなってきた。Web3.0 は英国のコンピュータ科学者であるギャビン・ウッド氏によって提唱された、「次世代の分散型インターネットの時代」という新たな概念である。
ここでは web3.0 時代に重要性を増すデジタルアイデンティティについて解説する。

目次

1. デジタルアイデンティティとは

デジタルアイデンティティは、**「アイデンティティ管理技術解説書」**(情報処理推進機構:IPA)によれば、“デジタル情報として統一的に管理された、人・デバイス・サービス等についての属性情報の集合”と定義されている。

また、**ISO/IEC 24760-1(※注1)**では、Identity を「実体に関する属性情報の集合」であると定義している。一般的にデジタルアイデンティティは自然人などの主体(Entity / Subject:エンティティ/サブジェクト) をコンピュータで処理するためのアイデンティティ情報で識別子(Identifier:アイデンティファイヤー)とその属性(Entity:エンティティ)から構成される。

主体(Entity:エンティティ)は、多くの場合は自然人であるが、組織・デバイス・サービスなども含まれる。アイデンティティ情報を管理する方法は任意であり、しばしば1つの実体に対するアイデンティティ情報が複数のアイデンティティ管理システムで別々に保持されているケースも多くある。属性の中にはクレデンシャル情報と言われるものがあり、そのエンティティが確かにアイデンティティ情報と結びついたエンティティであることを証明するための情報(パスワード情報など)を指す。また、ネットワーク上に存在する様々なエンティティやリソースを管理する範囲をドメイン(または、管理ドメイン)と言う。

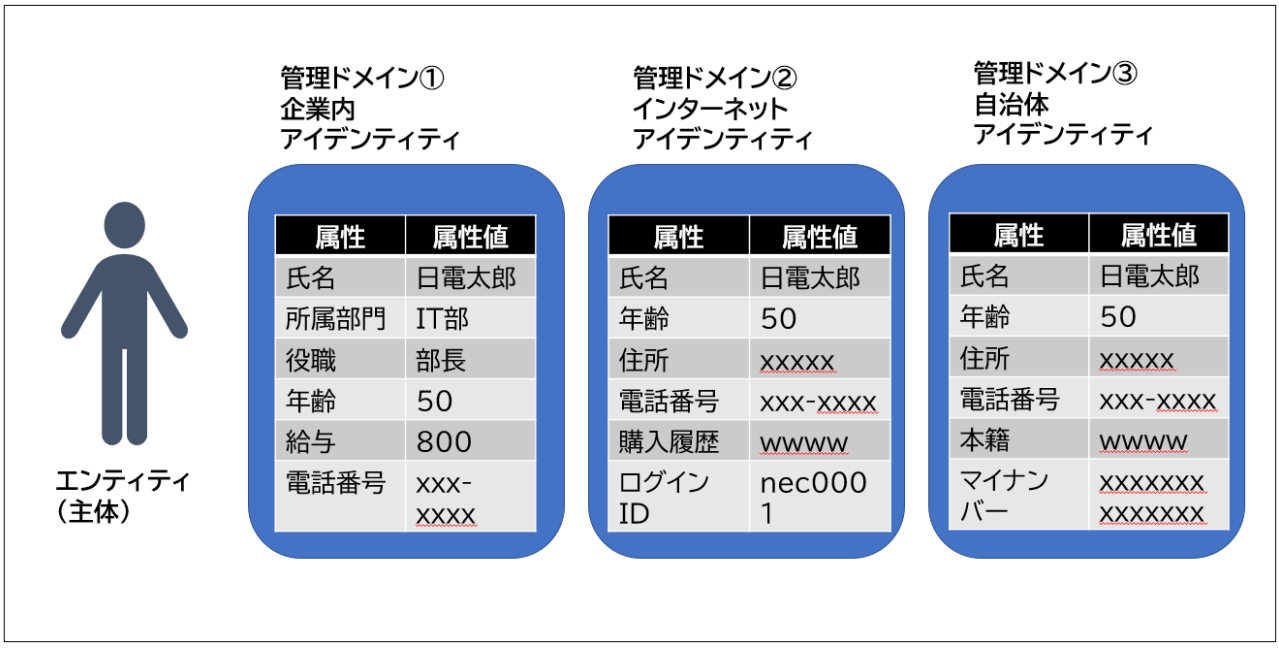


図1. エンティティと属性、管理ドメインの関係

※注1:ISO/IEC 24765-1 :ID ライフサイクル管理を定義した ISO 標準化ドキュメント
https://www.iso.org/standard/77582.html

2. 識別・認証・認可とアシュアランスレベル

米国国立標準技術研究所(NIST) が発表した、SP800-63 Digital Identity Guidelines(デジタルアイデンティティガイドライン)(現在、Ver.3)(※注2)では、デジタルアイデンティティの基本要素である、識別(Identification:アイデンティフィケーション)、認証(Authentication:オーセンティケーション)、認可(Authorization:オーソライゼーション)をモデル化し、アシュアランスレベル(保証レベル)の定義を行った。識別はユーザを他者と別すること。認証はユーザの正当性(当人性)を検証すること、認可はユーザに応じた権限を与えること、といった定義になる。
アシュアランスレベル(保証レベル)は、情報セキュリティの厳格さ(セキュリティレベル)を評価する際に用いられる指標のことである。

SP800-63 本体は、デジタルアイデンティティ全体のガイドラインを示し、Digital Identity Model の 3 つのフェーズ(Identity、Authenticator、Federation)をサブドキュメントで定義、それぞれで Assurance Level(保証レベル)を定義している。

※注2: NIST SP800-63-3 Digital Identity Guidelines
https://pages.nist.gov/800-63-3/

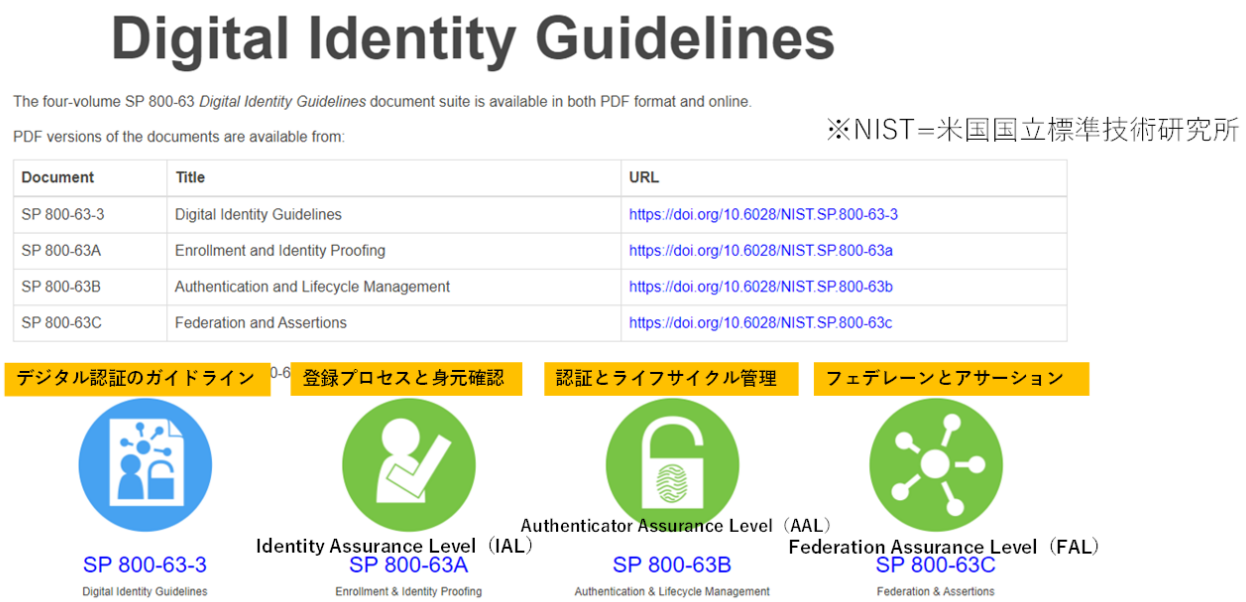


図2. NIST SP800-63-3 の文書校正
出典:NIST SP800-63-3 に筆者が説明を加筆したもの

63-A) IAL(Identity Assurance Level:アイデンティティアシュアランスレベル)は、ユーザの身元確認の強度で、ID(Identity:アイデンティティ)の認証プロセスを指す。Applicant(アプリカント)(後述)が、登録するときの本人確認(Identity Proofing:アイデンティティプルーフィング)

63-B) AAL(Authenticator Assurance Level:オーセンティケーターアシュアランスレベル)は、ユーザ認証の強度で、Claimant(クレイメント)(後述)が、ログインするときの認証プロセスを示す。

63-C) FAL(Federation Assurance Level:フェデレーションアシュアランスレベル)は、フェデレーションの確さで、フェデレーションする際のデータのやりとりの強さを示す。(フェデレーションについては後術する)なお、FAL は任意選択となる。

図3は、アカウントが登録されサービスが利用可能になるまでの状態を表している。
識別・認証・認可を意識したアカウント設計を行うことで、不正利用などの不正行為を排除しやすくなる。

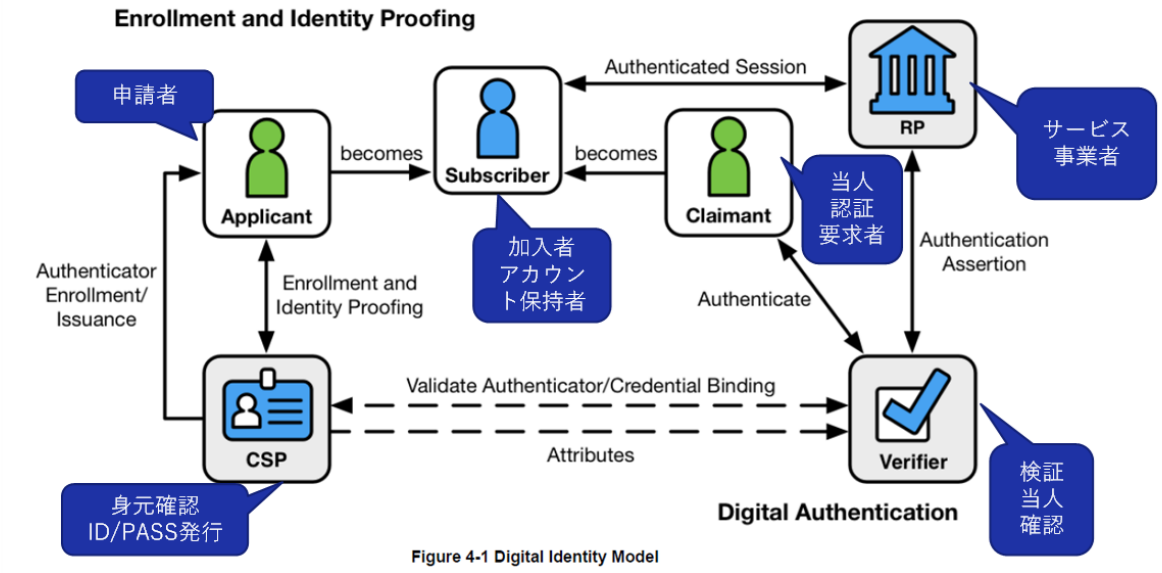


図3. NIST SP800-63-3 Digital Identity Model

出典:NIST SP800-63-3 Digital Identity Model に筆者が説明を加筆したもの

用語	読み方	説明
Applicant	アプリカント	サービスに登録されていない、アカウント未登録の人
Claimant	クレイメント	アカウントに登録された人。認可前の状態 「サービスを利用したい人」を要求する人
Subscriber	サブスクライバー	サービス利用が可能になった状態の人
Verifier	ベリファイヤー	Claimantからの要求が正しいかを検証する人
CSP (Credential Service Provider)	クレデンシャル サービス プロバイダー	クレデンシャル情報を提供する
RP (Relying Party)	リライング パーティー	アプリケーションまたはサービス提供者

表1. 図3の用語説明

評価保証レベル(Assurance Level)とは

各フェーズにおける、厳密さや強度をレベルと言った形で定義し、どのようなサービスではどの程度の保証レベルを適用すべきかをガイドしている。

SP800-63-3 では、リスクアセスメントを行った後に IAL、AAL、FAL のレベルを選定するためのチャートが提供されており、該当したレベルの要件をサブドキュメントで確認したうえで、要件を満たすサービス実装を行うことになる(下図　IAL レベル判定チャート)

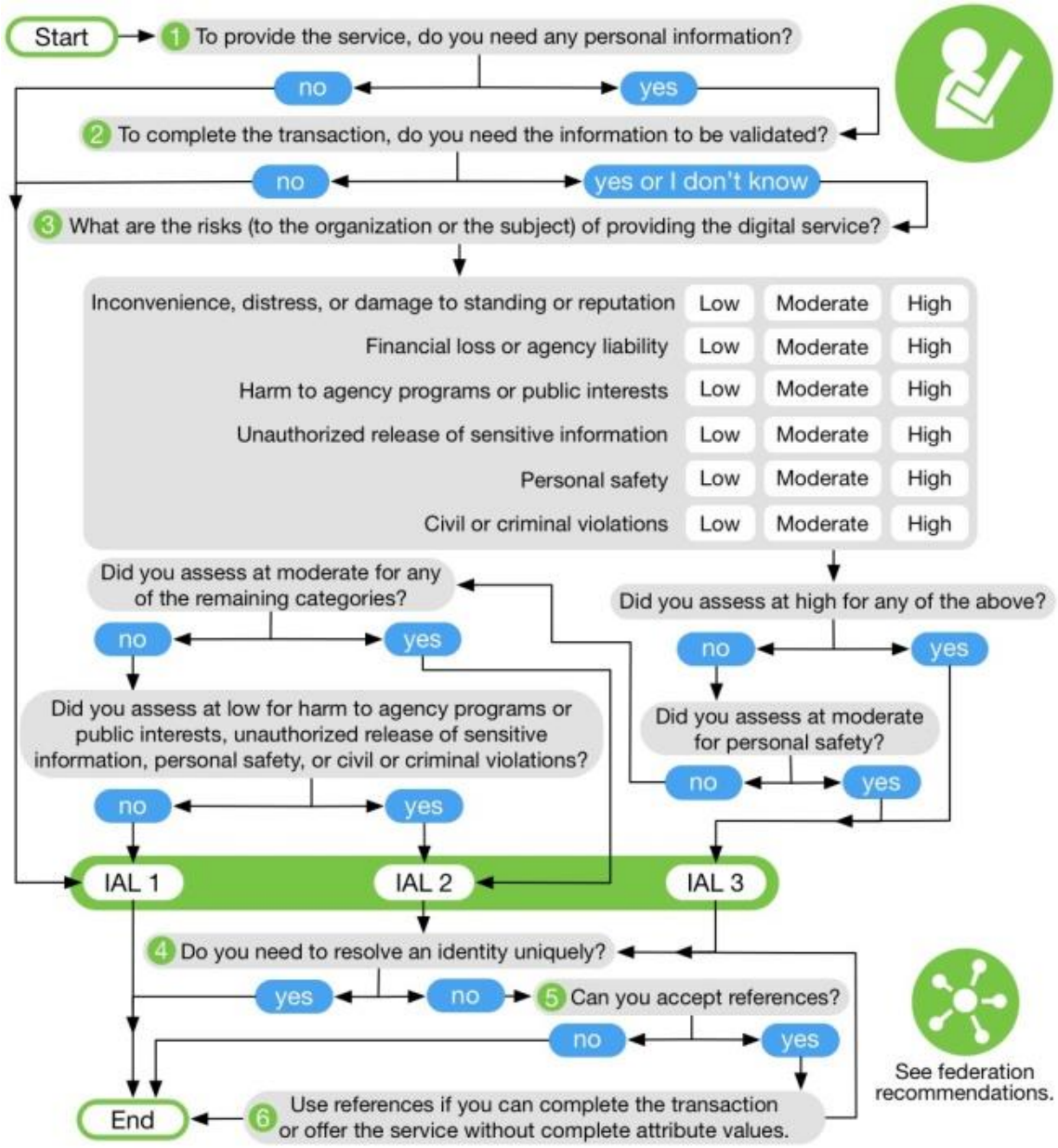


図4. NIST SP800-63-3 Selecting IAL チャート

出典：NIST SP800-63-3 Selecting IAL より抜粋

【図4. チャートの説明】

① サービスを提供するために個人情報が必要ですか
② 取引を完了するために、個人情報を検証する必要がありますか
③ デジタルサービスを提供する(組織/主体における)リスクは何ですか
  -地位または評判に対する不便、苦痛、または損害
  -金銭的損失または代行機関の責任
  -政府機関のプログラムまたは公益へあたえる害
  -機密情報の無断公開
  -個人の安全
  -民事または刑事上の罰
④ ID を一意に解決する必要がありますか
⑤ 「参照」を受け入れることができますか
⑥ 完全な属性値なしでトランザクションを完了したり、サービスを提供したりできる場合は、参照を使用してください

【IAL/AAL/FAL の説明】

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)

参考:認証方式の整理と NIST SP800-63 での認証方法決定: NEC セキュリティブログ | NEC
https://jpn.nec.com/cybersecurity/blog/210521/index.html

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)

3. アイデンティティライフサイクル管理とは

ISO/IEC24760-1 では、アイデンティティのライフサイクル管理（Identity Lifecycle Management）を状態遷移で表現し、それぞれの状態と遷移の関係を解説している。
Identity Lifecycle Management とは IT システムやサービスにおける Identity のライフサイクルを管理する仕組みである。

ISO/IEC 24760-1 では、アイデンティティ管理を「特定のドメイン内におけるアイデンティティのライフサイクルや属性値等のメタデータを管理するためのプロセスとポリシ」と定義している。各システム等で管理されるアイデンティティ情報を適切に管理するためには、このアイデンティティ情報を維持するためのアイデンティティ管理システムが必要となる。

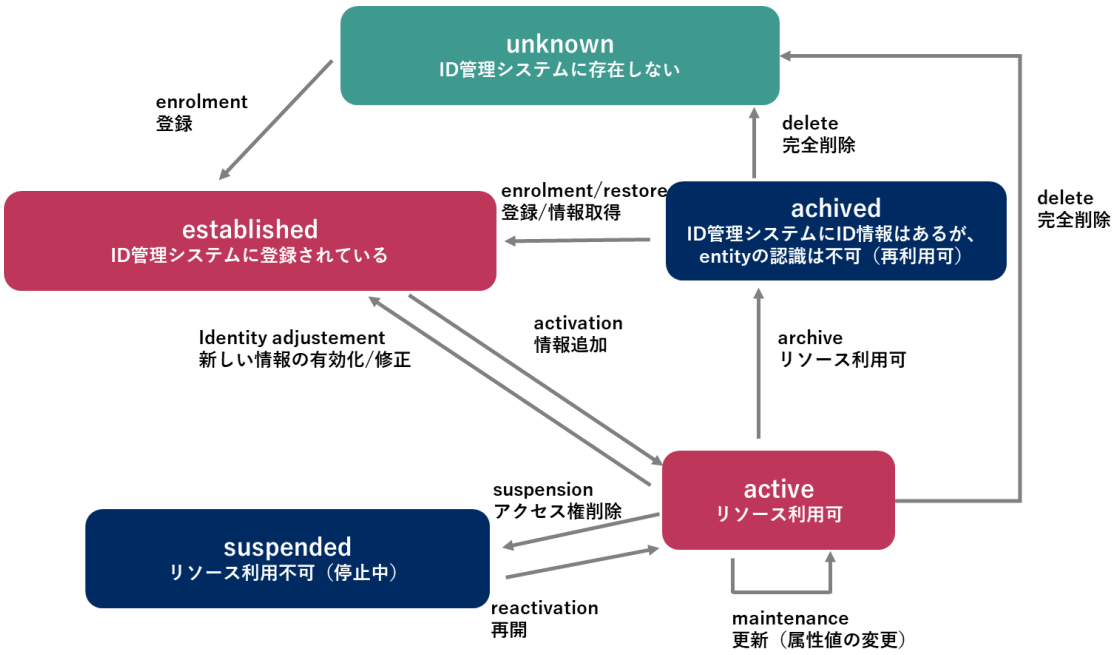


図 5. ISO/IEC24760-Part1 アイデンティティ ライフサイクル
出典：ISO/IEC24760-Part1 Identity Lifecycle を元に筆者が新たに作図

日本語訳	ISO文書の単語	解釈
登録	Enrolment エンロールメント	特定domainでentityを認識させるプロセス。 ID の証明/登録（検証/生成された ID 情報を使用）
登録/情報取得	Restore リストア	ID 証明として使用される ID 情報の一部が ID 管理システムから取得される。
情報追加	Activation アクティベーション	ID 情報の追加 entity のリソースへのアクセスが可能になる
新しい情報の有効化/修正	Identity Adjustment アイデンティティ アジャストメント	ID 情報の更新 新しい情報を有効化/情報を修正する場合が該当
アクセス権削除	Suspension サスペンション	ID 情報の一部を一時的に使用できないようフラグ立てすること アクセス権を削除することで実現
再開	Reactivation リアクティベーション	一時停止の取り消し
完全削除	Delete デリート	登録されたID 情報を完全に削除
部分削除	Archive アーカイブ	ID 情報の部分的な削除 情報が統計処理にのみ利用可能であり、entity によって提供された 追加情報を持つ entity に関連するものとしてのみアクセスできるようになる
更新（属性値の変更）	Maintenance メンテナンス	ID 情報の更新

表2. 図5中の各状態の説明

日本語訳	ISO文書の単語	解釈
ID管理システム に存在しない	Unknown アンノーン	entity の識別に使用できる情報が ID 管理システムに存在しない状態
ID管理システム に登録されている	Established エスタブリッシュ	必要な ID 情報に参照識別子などの追加 情報が生成され、ID 管理システムに登録された状態
リソース利用不可 （停止中）	Suspended サスペンディッド	entity がドメインのリソースを利用できない状態
ID管理システムにID情報はあるが、entityの認識は不可（再利用可）	Archived アーカイブ	原則 entity の認識には利用できない。 ただし、entity がドメインに存在 しなくなっても、その ID 情報は ID 管理システムに残っているため、再登録時に利用することができる （新しい entity の新しい ID を確立するために使用し、アーカイブされた情報の一部を含むことができる）
リソース利用可	Active アクティブ	entity によるリソースの利用が可能になった状態 IT システムでアクティブ・セッションを 開始する権利を持つ

表3. 図5中の各状態遷移の説明

4. アイデンティティ管理モデルとは

アイデンティティ管理の代表的なものとしては、「集中管理モデル」と「フェデレーションモデル」がある。
集中管理モデルは個別のアイデンティティ管理とサービス提供を行うため、ユーザはサービス毎に自身のアイデンティティ管理が必要となる。前述の Identity Lifecycle Management が参考になるだろう。

フェデレーションモデルは、 RP と IdP は別のエンティティであり、 ユーザは RP にアクセスする際、IdP のアイデンティティ情報を用いることでログインする 。また、ユーザは特定の IdP のアイデンティティ情報をもとに、複数の RP に SSO でアクセスできるようになる。フェデレーションモデルは利便性が高くなる一方で、IdPにどのSPを利用したかの情報が保管されることになり、情報が集中されやすくなる傾向があり、場合によってはプライバシーの問題になるかもしれない。

なお、フェデレーションモデルでは、ユーザ自身のアイデンティティ情報の連携に対する「同意」によってアイデンティティの連携を行うことになる。

【用語説明】
RP: Relying Party（リライティングパーティー）：IdP に認証を委託し、IdP による認証情報を信頼してユーザにサービスを提供する。SP（Service Provider：サービスプロバイダー）ともいう。
IdP: Identity Provider（アイデンティティプロバイダー）：クラウドサービス（RP）などにアクセスするユーザの認証情報を保存・管理するサービスのことを指します。
SSO: Single Sign On（シングルサインオン）：1 度ユーザ認証（ログイン）を行うと、以後そのユーザ認証に紐づけられているシステムやサービスを、追加認証なしで利用できる機能

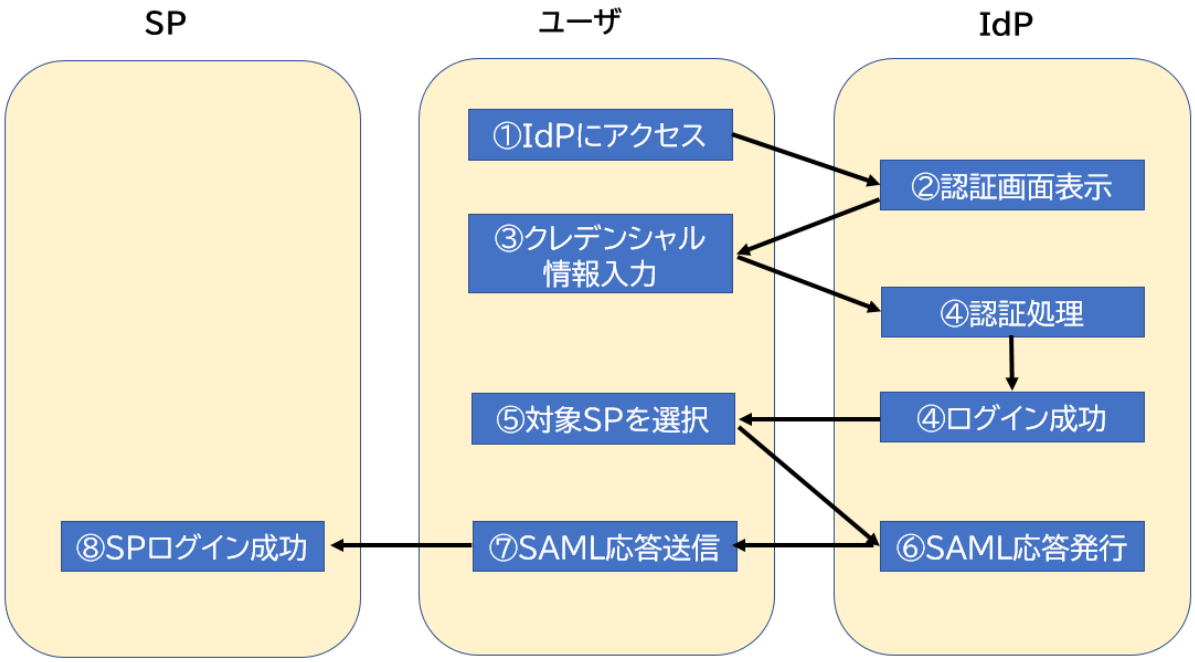


図6. SAML の場合の認証フロー例（IdP Initiate の例）

出典：筆者独自

【図6.SAML の場合の認証フロー例(IdP Initiate の例)の解説】

① ユーザが IdP にアクセスする
② IdP の認証画面が表示される
③ ユーザはログイン情報(クレデンシャル情報)を入力して IdP との間で認証処理を行なう
④ 認証が成功したら IdP にログイン成功
⑤ IdP の画面から対象の SP を選択する
⑥ IdP 側で SAML 認証応答が発行される
⑦ ユーザは IdP から受け取った SAML 認証応答を SP に送信する
⑧ SP に SAML 認証応答が受信されるとログインとなる

【図6の用語解説】

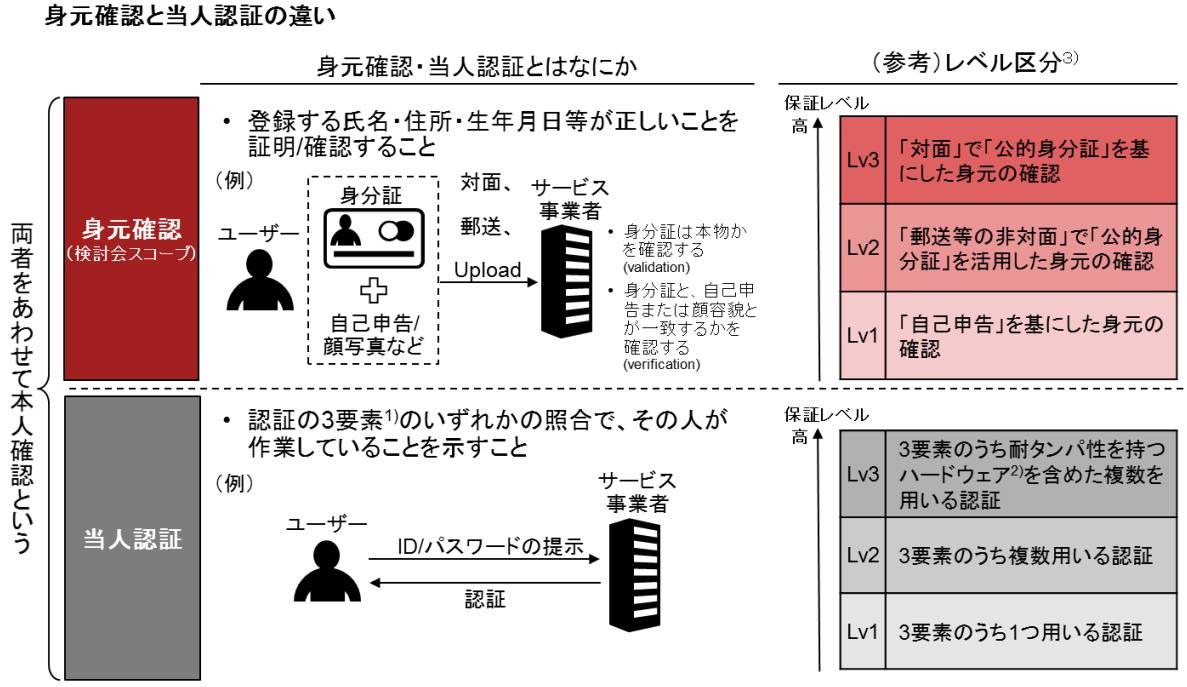
SAML(サムル)(Security Assertion Markup Language):OASIS によって策定された異なるインターネットドメイン間でユーザ認証を行うための XML をベースにした標準規格

SAMLを例に管理モデルについて解説したが、SAML以外にも OAuth や OpenID Connect 等も標準化されているものがあり、現状でも多く利用されている。なお、本書ではその詳細については割愛する。

5. 本人確認とは

「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」ではオンラインサービスにおける本人確認の考え方を整理している。

銀行の口座開設など、オンライン上で実在の個人を前提としたサービスが増加しているが、なりすましを防止するために**「本人確認」**の重要性が増している。
本人確認には、ID とパスワードによる認証、生体情報による認証などの**「当人認証」**だけでなく、ユーザの実在性を確認する**「身元確認」**も同時に行う必要があります。
「身元確認」はサービスの性質や業界のレギュレーションに沿った形の対応が求められます。



1)認証要素は「生体」（顔・指紋など）・「所持」（マイナンバーカードなど）・「知識」（パスワードなど）に分かれる
2)マイナンバーカードなど、内部の情報に対する不正な読み出しが困難である物理装置
3)「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」（2019年2月CIO連絡会議決定）のレベル区分

図7. 身元確認と当人認証の違い

出典：「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

この「本人確認」は、一般的に KYC（Know Your Customer：ノーンユアカスマター）とも言われ、金融業においては「犯罪収益移転防止法」にて定められている。また、通信業では「携帯電話移転防止法」、古物業では「古物営業法」で定められており、最近ではオンライン上での本人確認が可能になるように法制度の変更がなされており、一般的に eKYC と呼ばれている。

「身元確認」は前述の NIST SP800-63A に相当し、「当人確認」は NIST SP800-63B に相当する。それぞれ、サービスのリスクに応じた保証レベルを元に運用すべきとされている。

6. プライバシーと匿名化(anonymity(匿名化)/ pseudonymity(仮名化))

我々のデジタルアイデンティティ情報は、デジタル空間上で様々な活動を行うことで、GAFAM(Google、Apple、Facebook/Meta、Amazon、Microsoft)に代表されるプラットフォーマーに収集され、様々な形で利用されている。また、KYC 等により本人確認が行われることで、デジタルアイデンティティ情報が物理的なアイデンティティ情報と同一化されていく懸念がある。これにより、プライバシーの侵害リスクや、情報漏洩によって不正利用された場合のリスクが高まっていく状況がある。

本来であればプライバシー情報を自分でコントロールできることが望ましく、利用するコンテキスト毎に開示するプライバシー情報は最小限にしたい。また、場合によっては匿名や仮名で利用したいと思うかもしれない。デジタルアイデンティティ情報は本人属性の解像度を高めることに注力しがちであるが、プライバシーには最大限配慮したものでなければならない。Web3.0 時代のデジタルアイデンティティはこの辺りが肝になりそうだ。

さて、匿名化と仮名化にはどのような違いがあるか。匿名化は個人を識別することができないように「個人情報」を加工し、当該個人情報を復元できないようにした情報とされ、基本的には一方通行である。仮名化は「個人情報」を加工して個人を特定できる情報をトークン化し、単体では個人を特定できないようにした情報とされているため、元の「個人情報」に戻せるのが特徴である。トークン化とは、**機密データを非機密データに置き換えることで保護する仕組み**である。(図参照) トークン化によって、データは認識不可能なトークン形式になるが、元のデータのフォーマットは保持される特徴がある。元の情報に戻す場合は「秘密鍵」を用いて復号を行う。なお、トークン化は仮名化の一手段である。

匿名化と仮名化はそれぞれ特徴を理解して用途に応じて使い分ける必要がある。一般的に元の情報から仮名化することを“de-Link”いい、仮名情報から元の情報に戻すことを“Link”と言う。

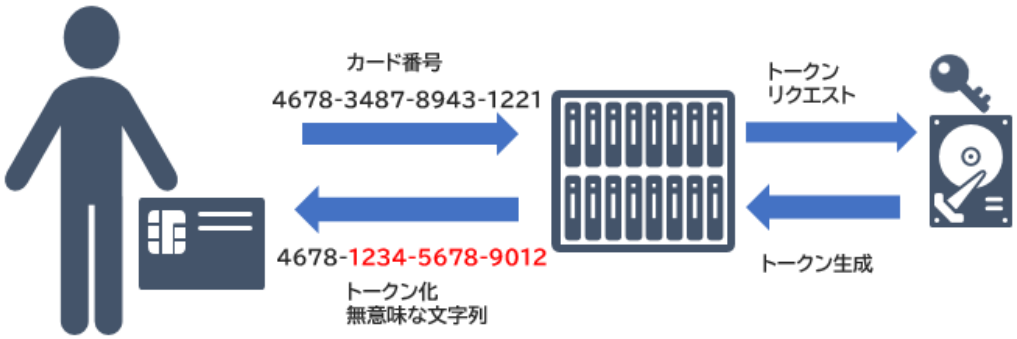


図8. トークン化の概要

出典:筆者独自

7. まとめ

Web3. 0時代のデジタルアイデンティティを考えるにあたって、現在のデジタルアイデンティティの基礎を解説してきた。Web1.0/2.0 の初期段階では、各サービス事業者が自社のルールに従ってアイデンディティの管理を行っていた。 その後、複数のサービスを横断しての利用が通常になり、ユーザのアイデンティティ情報を複数サービスが連携して管理する必要が出てきた。しかしながら各社の責任分界点の問題や、各アイデンティティ管理の保証レベルの整合等の課題等が出てきた。このような課題を解決するため、フェデレーションモデルへと変化していった経緯がある。 フェデレーションモデルでは、ユーザ自身のアイデンティティ情報の連携に対する「同意」によってアイデンティティの連携を行うことになる。Web3.0 では、デジタルアイデンティティの分散管理が必須にならざるを得ないと思われ、これまで述べた本人確認や属性検証、アイデンティティ管理の手法や各種保証レベルの整理が必要になる。すでに、Web3.0 とは別路線にて以前からいくつかの標準化団体によって検討が進み一部標準化が採択されているものもある。次回以降でこの点について解説できれば幸いである。

以上

＜お問い合わせ先＞
NEC デジタルファイナンス統括部
E-mail:digital_finance@mnn.jp.nec.com

NEC Digital Finance サイト
https://jpn.nec.com/nvci/finance/index.html

【筆者プロフィール】

NEC　金融システム統括部　金融デジタルイノベーション技術開発グループ
デジタルアイデンティティ・エバンジェリスト　　宮川　晃一

情報セキュリティおよびデジタルアイデンティティ分野のコンサルタントとして20年以上従事し、外部団体でのコミュニティー活動の立ち上げによる啓蒙活動と人材育成に従事してきた。現職では　Open API/eKYC　等の金融分野におけるデジタルアイデンティティ・エバンジェリストとして、所属団体での活動および講演活動や執筆活動に注力をしている。

（主な所属団体）
・日本ネットワークセキュリティ協会（JNSA）デジタルアイデンティティ WG リーダー
・クラウドセキュリティアライアンス（CSA）理事
・FISC　オープン API に関する有識者検討会　委員
（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」
・日経クロステックアクティブ　”まとめ”「特権アクセス管理とは：高権限のアカウント「特権 ID」で IT を統制」