NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

電子署名 保証レベル ガイド
JNSA eSignAL Guide
- 要約版 Ver 1.0 -

JNSA 電子署名WG 保証レベルTF

2022/09/08

はじめに:電子署名保証レベル

2001年4月電子署名法が施行された時は**「電子署名」**とは**「公開鍵暗号を利用したデジタル署名と公開鍵インフラ(PKI)」**を前提としていました。

一方で電子認証によるクラウド利用のサービスが一般化したこともあり、電子署名サービスも多様化し色々な電子署名の技術や方式が使われるようになりました。現在は単純に**「電子署名＝デジタル署名＋PKI」とは言えません。**

しかし技術や方式が異なる電子署名方式の比較は簡単ではありません。**「技術に関する電子署名の保証レベル」**を専門家が公平に策定し標準化を行い電子署名利用者が**目的に合った選択**ができるようになることが重要です。

JNSAの電子署名ワーキンググループでは新たに**保証レベルタスクフォース**を発足し**電子署名の保証レベル**の策定を行いました。最終的にはガイドブックの公開を目指していますが、本資料はその**要約版**として公開するものです。

１．電子署名の整理

最初に電子署名の法的要件や定義を整理して、電子署名の再定義を行います。

署名・押印と二段の推定（非電子）

非電子における署名・押印に関して 民訴法第228条第4項 に以下の規定があります。

「私文書は、本人[中略]の署名又は押印があるときは、真正に成立したものと推定する」（二段目の推定）

この「推定」の前提となる「押印」の「推定」が 最高裁判例 昭和39.5.12民集18-597 にあります。

「本人の印鑑による印影があれば本人の意思による押印と推定する」（一段目の推定）

「真正な成立」の「推定」を得る為には一段目の推定の前提の立証と、一段目及び二段目の推定の主張が必要となります。

これは署名・押印に関する**「二段の推定」**と呼ばれ、電子署名においても参照すべき考え方です。

参考：「暗号技術と法律について」 JNSAメールマガジン 第38号 2014.6.27
https://www.jnsa.org/aboutus/jnsaml/ml-38.html

用語解説＞
印章（ハンコ）：物理的なハンコのこと。これを「印鑑」と呼ぶ場合が多いが、本来は、印鑑は印影の一種であり、印鑑は物としてのハンコではない。
印影　：ハンコを使って押印した朱肉による跡のこと。
印鑑　：実印や銀行印などの登録された印影のこと。印鑑証明書は印影の証明であり真偽を確認する為に利用される。

電子署名と二段の推定の考察

電子署名法の第三条には、電子文書に関する、押印における二段目の推定と同様の規定があります。

「電磁的記録に記録された情報について本人（の意思）による電子署名が行われているときは、真正に成立したものと推定する」

この推定の前提については判例等がありません（押印の一段目の推定に相当するものがありません）ので、何らかの方法で「本人による電子署名が行われたこと」を証明する必要があります。このため、通常は、

「本人による電子署名（管理された署名鍵や認証要素による署名認可の行使）の証拠を提示することにより、本人の意思による電子署名を証明する」

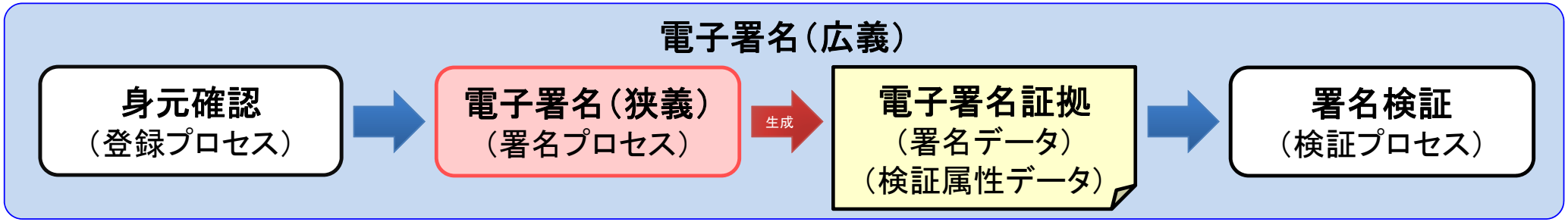
という証明方法が行うことになりますので、本人性の証明のために、こうした証拠を備えることが重要です。
また、電子署名法の第二条第一項第二号において非改ざんの要件も必要となります。

「当該情報について、改変が行われていないかどうかを確認することができるものであること」

電磁的記録に関しては改変が紙媒体に比較して容易であることから追加されたと考えられます。

用語解説＞
電子署名：法律上の用語であり（技術用語では無い）色々な署名方式が認められる（電子署名法2条1項）。
デジタル署名：公開鍵暗号方式を用いた署名技術であり署名鍵による署名者を証明し改ざん防止を実現する。

電子署名の定義



狭義：電子署名法 第２条第１項 の電子署名

「**デジタル情報**（電磁的記録に記録することができる情報）」について行われる「**措置**」であって以下のいずれにも該当するもの。

① 当該情報が、**当該措置を行った者の作成**に係るものであることを示すためのものであること（同項第１号）

② 当該情報について、**改変が行われていない**かどうかを確認することができるものであること（同項第２号）

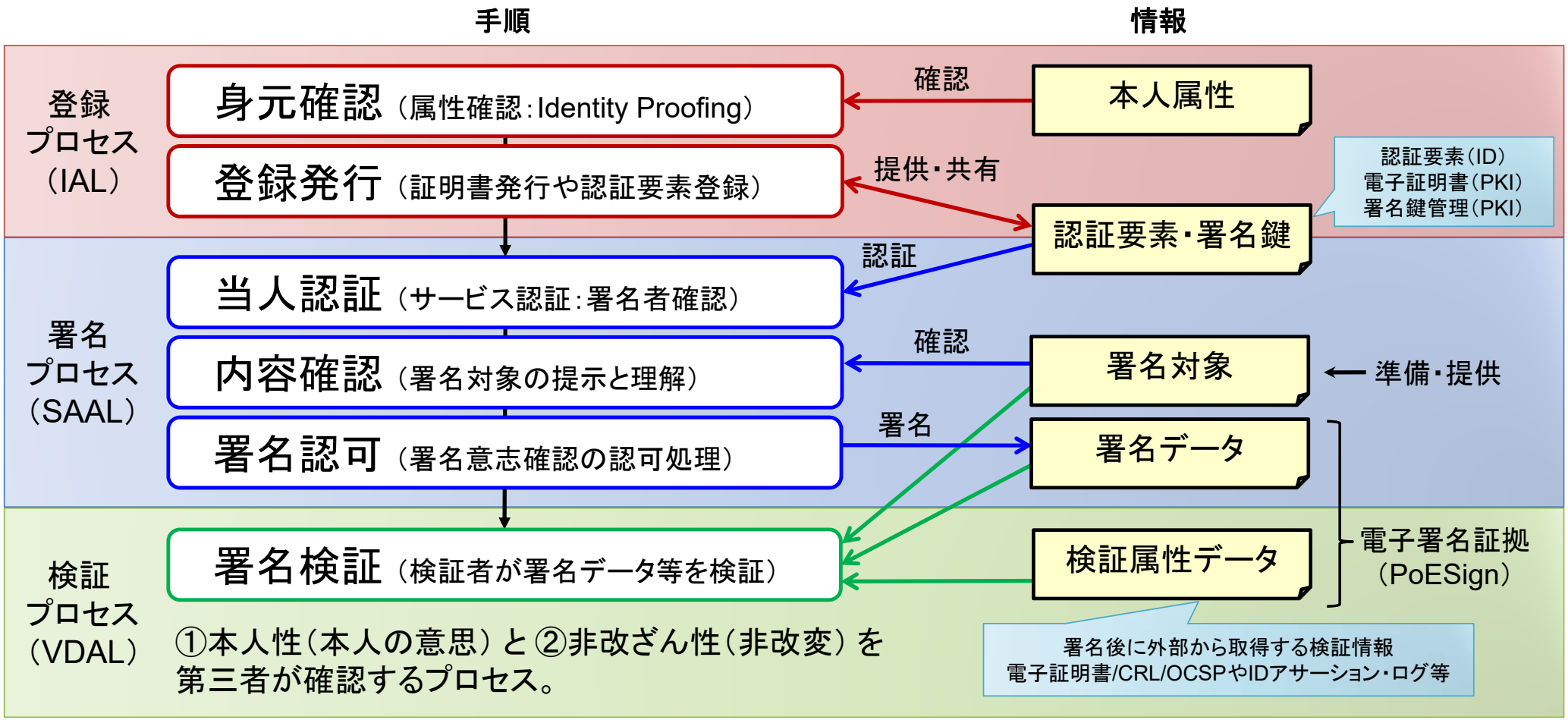
※ 本資料では「措置」とは「プロセス」と言えると考えている。

広義：本人確認から署名時生成した署名データを使い第三者が署名検証するまで

法的な定義は措置（署名プロセス）のみだが、登録プロセスの身元確認と署名プロセスで生成する電子署名証拠と検証プロセスまでの全体を指して広義の電子署名とする。本ガイド中では「電子署名」を広義の定義にて利用。

検証結果として **①本人性（本人の意思）** と **②非改ざん性（非改変）** が確認できることが必要となる。

電子署名の一般的手順


手順
情報
登録プロセス（IAL）
身元確認（属性確認：Identity Proofing）
登録発行（証明書発行や認証要素登録）
確認
本人属性
提供・共有
認証要素（ID）
電子証明書（PKI）
署名鍵管理（PKI）
認証要素・署名鍵
認証
署名プロセス（SAAL）
当人認証（サービス認証：署名者確認）
確認
内容確認（署名対象の提示と理解）
署名対象
準備・提供
署名
署名認可（署名意志確認の認可処理）
署名データ
検証プロセス（VDAL）
署名検証（検証者が署名データ等を検証）
検証属性データ
電子署名証拠（PoESign）
①本人性（本人の意思）と②非改ざん性（非改変）を第三者が確認するプロセス。
署名後に外部から取得する検証情報
電子証明書/CRL/OCSPやIDアサーション・ログ等

２．電子認証の整理

クラウドを利用した電子署名では必須となる電子認証の用語や定義も整理します。

電子認証：身元確認と当人認証

Onboarding（登録時）に **Identity Proofing（身元確認）**が必要

- **Identity Proofing：提供された属性情報の確かさを確認する。**
  例：メール到達・運転免許証・マイナンバーカード等を利用して本人属性を確認。
- ✓ **KYC（Know Your Customer）**も本人確認。
  サービス事業者のための、本人確認手続き（KYC）に関する調査レポート
  https://www.openid.or.jp/news/oidfj_kycwg_report_20200123.pdf
- ✓ 本人確認には継続した確認が必要でありコストもかかる（鮮度がある）。

Ongoing（利用時）に **Authentication（当人認証）**が必要

- **Authentication：利用者とID情報との紐付けを確認する。**
  例：パスワード（知識）・指紋（生体）・ICカード（所有）等を利用して当人を確認。
- ✓ 電子署名の場合は当人認証後に署名対象の内容確認を行ってから署名認可を行う。
  ローカル署名は、（正当な署名データの生成による）署名鍵の所持の証明が、当人認証相当と考える。

※ オンラインで**本人と認める為**には **身元確認済みのID情報を使った当人認証** が必要。

電子認証 / Digital Identity 用語

ID/Identifier：１つの実体（エンティティ）に付す識別子となる属性情報
Identity：実体（エンティティ）に関する属性情報の集合

- ID/IdentifierとはIdentityの持つ属性情報の１つで識別/特定に利用する。
- １つの実体は、複数のID/Identityを持つことができる。
- 人は実体をIdentity（属性の集合）を通じて認識する。

Authentication/AuthN（認証）：

端末の前にいる実体がサービス側が認識するどのIdentityと紐付いているかの確証を得るプロセス。
サービス認証：署名サービス等の利用開始時にどのIdentityと紐付いた実体かを確認する。
Authenticator（認証器/認証コード）：Credential（信用）情報を扱う

Authorization/AuthZ（認可）：

端末の前にいる実体がサービス側が提供するリソースに対するアクセス権限を持っているか確認するプロセス。
署名認可：電子署名付与の為に署名鍵（リソース）を利用する権限を持つか確認する。

Access Control（アクセス制御）＝**AuthN**＋**AutnZ**＋**Audit** [logging/監査ログ]

ID認証技術

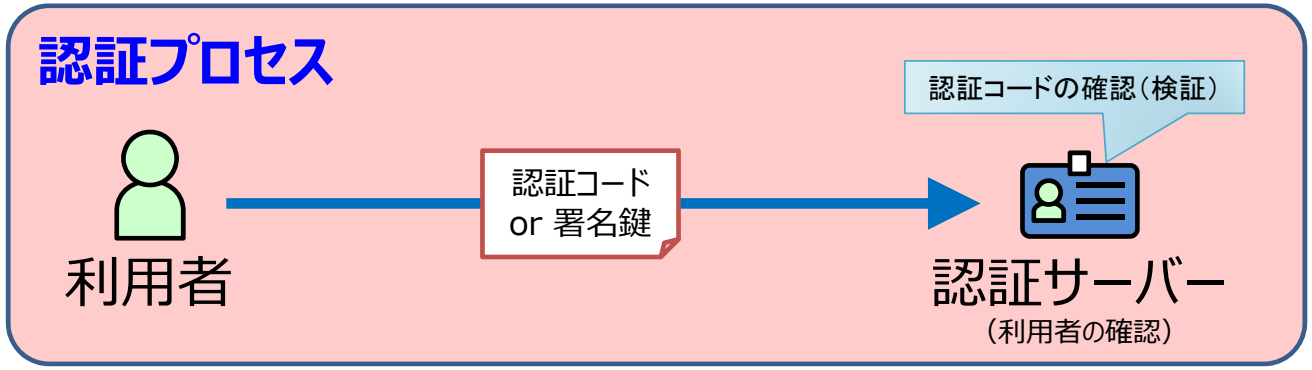
認証認可の広く使われている標準的な技術仕様には OAuth+OpenID Connect や SAML 等がある。
本資料では「電子認証」は「電子署名」に対応した用途全体を示す概念的な言葉として利用する。
本資料では「ID認証」と書いた場合には OAuth + OpenID Connect 等の具体的な技術を指す。

OAuth 2.0 + OpenID Connect (OAuth+OIDC) ※ OAuth 2.0 は認可の仕様 ※ OIDC はID認証の仕様	**OAuth 2.0 Authorization Framework**（RFC 6749） https://tools.ietf.org/html/rfc6749 https://openid-foundation-japan.github.io/rfc6749.ja.html [和訳] 策定：IETF（インターネットコミュニティ）2012年発行の認可標準仕様 メッセージ送受信：**HTTPS**（**RESTful**）、通信プロトコル：**JSON**ベース
	OpenID Connect 1.0 : OIDC （オープンIDファウンデーション） https://openid.net/connect/ http://openid-foundation-japan.github.io/openid-connect-core-1_0.ja.html [和訳] 策定：オープンIDファウンデーションが2014年に1.0を発行の認証標準仕様 OAuth 2.0 プロトコルにアイデンティティ層（認証）を追加した（OAuth 2.0を参照）
SAML ※ SAMLは認証認可の仕様	**SAML**（Security Assertion Markup Language） http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html 策定：OASIS　v2.0 を2005年発行の認証認可の標準仕様 メッセージ送受信：**SOAP/HTTP**、通信プロトコル：**XML**ベース 主な実装：Shibboleth（学術系で広く利用されている）

３．電子署名と電子認証の関係

電子署名を使った電子認証や、電子認証を使った電子署名もあります。
電子署名と電子認証の関係を整理します。

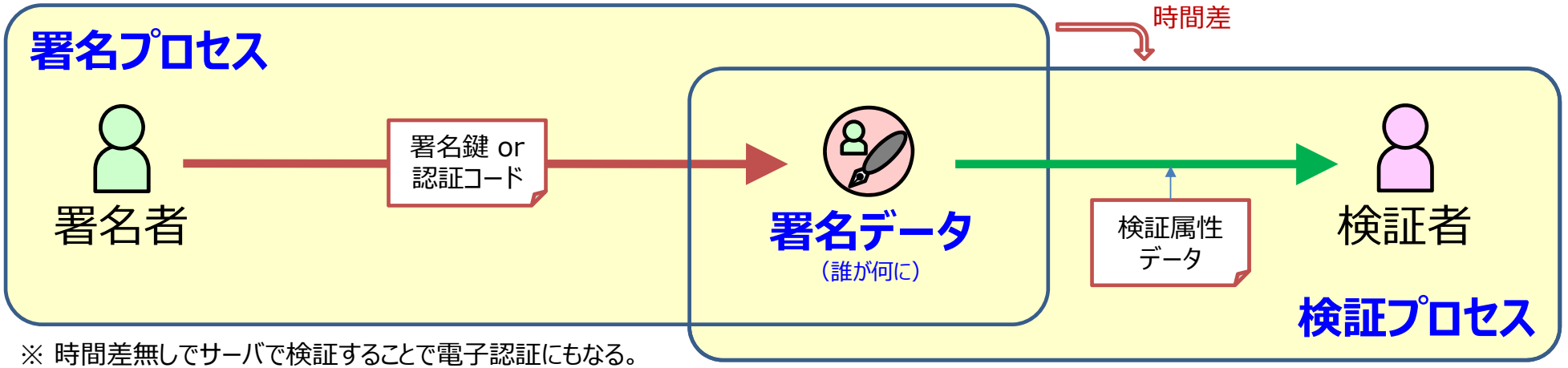
電子認証と電子署名の利用モデル比較



※ 認証コードの検証結果を第三者が検証可能な署名データとして残せば電子署名にもなる。

電子認証：
- ✓ 認証プロセスで利用者を確認。
- ※ 認可はリソースへの権限を確認。
- ※ リアルタイム処理。

電子署名：
- ✓ 署名プロセスで署名データを作成。
- ✓ 検証プロセスで署名データを確認。
- ※ 署名データを挟んで時間差あり。



※ 時間差無しでサーバで検証することで電子認証にもなる。

電子認証と電子署名の整理

- **電子認証＝認証プロセス**
  - ✓ 端末の前の実体（人）とIdentityを認証サーバー側で紐付ける**認証プロセス**。
  - ✓ 認可は認証後のリソースへのアクセス権限の確認プロセスであるが混同されがち。
    - 署名認可のように認可の為に２要素認証等の認証技術を使うことがあり区分が難しい。
  - ✓ 認証の結果は認証サーバーが確認できればよい（RP等サーバー連携はある）。
    - RP: Relying Party の略でサービス提供するサーバー
  - ✓ 認証時の情報は認証サーバー内にログ等として保存されるが通常開示されない。
- **電子署名＝署名プロセス＋署名データ＋検証プロセス**
  - ✓ 署名者による署名対象の**署名プロセス**と検証可能な**署名データ**の作成。
  - ✓ 署名プロセスでは署名者が当人であり（ここまで認証プロセスと同じ）、かつ当人が内容（署名対象）を理解し認めている必要がある。
  - ✓ 検証者による署名データ等から署名者と非改ざんを確認する**検証プロセス**。
  - ✓ 技術としてデジタル署名（PKI）とID認証のうち片方または両方を使っている。

※ 電子認証と電子署名のどちらも **事前の身元確認**（Onboarding）による実体の属性チェックが必要。

デジタル署名の用途

証拠：Authenticity/Non-Repudiation（意思表示・本来の電子署名）

- 署名対象の内容についての同意を後から否認できないように証拠を残すこと。電子署名法の対象。

証明：Certification（発信者保証）

- 署名対象の内容について発信者が保証する為に証拠を付けること。電子シール的な使い方。
- PKI（公開鍵基盤）では公開鍵証明書に付属するCA（認証局）の署名が発信者の証明をする。

※ 証拠と証明は用途では明確に分かれておらず多くの電子署名の使い方ではグラデーションのように両方の意味を持つ。
例：電子申請やS/MIME署名は同意と証明の両方の意味を持つが、同意単独よりは署名認可は厳密ではない。

認証：Authentication（当人確認）

- 署名対象に署名することで当人管理の署名鍵や認証要素の所持を確認（PoP/HoK）すること。
  - ・PoP：Proof-of-Possession（鍵所持の証明）　・HoK：Holded-of-Key（鍵の所持者）

分類		主目的	署名対象	署名データ	署名認可	利用例	
署名	証拠	否認防止 （電子署名的）	署名者の内容理解が必要	証拠として保管	署名毎に自然人が認可 （自動不可）	電子契約 重要文書の保管	電子申請
署名	証明	署名者保証 （電子シール的）	署名者が作成	確認時に利用	ルールによるシステム自動の認可も可能	発行文書の保証 公開鍵基盤（PKI）	電子申請
認証		当人確認	認証側が用意 例:チャレンジデータ	確認後は不要	認証毎に必要	TLSクライアント認証	

４．電子署名証拠：PoESign

新しい概念である電子署名証拠（PoESign）を定義することにより、
新しい電子署名方式の分類や整理が可能となります。

※ 電子署名証拠 PoESign は保証レベルTFから新たに提案する定義です。

電子署名証拠 PoESign（Proof of Electronic Signatures）

- 従来の電子署名（ローカル署名方式）では、本人管理の署名鍵によるデジタル署名とPKIベースの電子証明書を使って署名データを作成している。検証時に、認証局から発行される署名データと検証属性データ（CRL/OCSP）を使って本人性と非改ざんを確認している。
- デジタル署名は検証時に、**署名対象＋署名データ＋検証属性データ** が必要となる。

➢ **署名データ**：署名時に作成される情報
- ✓ 内包型署名データ：署名対象に署名データを埋め込む形式。例えばPDF署名は全て内包型となる。
- ✓ 分離型署名データ：署名対象とは別に署名データを管理する形式。XML署名のDetached形式等。

➢ **検証属性データ**：検証時に利用する外部情報（PKIなら電子証明書/OCSP/CRL等）
- ✓ 長期署名データ：署名データに必要な検証属性データを埋め込み全体をタイムスタンプで守る形式。
- ✓ アサーション：認証結果を示す認証サーバーがデジタル署名した情報。IDトークンと検証公開鍵等。

- 認証技術を利用した電子署名方式も署名データや検証属性データが証拠として必要。
- 署名データと検証属性データを組み合わせた情報群全体を、**電子署名証拠**（PoESign: Proof of Electronic Signatures）として定義することで電子署名の整理を容易にする。

※ 電子署名証拠（PoESign）：本人性（本人の意思）と非改ざん性（非改変）を確認できる情報群。

署名鍵証拠 PoKEY（Proof of signature KEY）

PKI（電子証明書）とデジタル署名を利用する場合の電子署名証拠は標準化されている。

PKI/CA（認証局）：X.509電子証明書/CRL/OCSP

- ✓ 認証局の運用による身元確認と、認証局がデジタル署名したX.509電子証明書が、署名鍵の所有者の本人性を保証する証拠となる。
- ✓ CRL（失効リスト）やOCSP（オンライン証明書ステータスプロトコル）を取得保存することにより電子証明書が発行後失効していないことの証拠となる。
- ✓ 国の認定や国際的なWebTrust認定等により認証局の運用が保証されている。

※ 事業者型の場合には事業者の保証であり本人性保証の証拠にはならない。

AdES：先進署名フォーマット（長期署名フォーマット）

- ✓ PAdES（PDF）、JAdES（Json）、XAdES（XML）、CAdES（CMS）等のISO 14533シリーズや欧州のETSI（eIDAS）で標準化された署名形式。
- ✓ 非改ざんに加えて、電子証明書の有効期間を超えた署名の保証が可能であり、署名アルゴリズムの危殆化にも対応した証拠となる。

署名認可ID証拠 PoAID（Proof of Authorization ID）

ID認証技術を電子署名に利用する場合の電子署名証拠には以下２つが想定できる。

署名時の認証認可の各種ログ情報（デジタル署名無し）

- ✓ 認証認可（アクセス）ログ・操作（イベント）ログ・アクセスログ等があるが、不足が無いように必要十分な情報を記録するようにする必要がある。
- ✓ 一般にはログ情報にデジタル署名をすることは無いが、削除や改ざんがされないような措置が必要。例えばRFC 3161形式のタイムスタンプを付与することで守る等。
- ✓ 署名時の監査ログに事業者がデジタル署名した上で検証属性データとして提供してもよい。フォーマットは標準化されていないが必要な情報を全て含む必要がある。
  - 署名時のイベント毎の日時・イベント種別・認証（実体の識別）・成否等とアクセス情報が必要。

署名時の認証認可のアサーション情報（デジタル署名済み）

- ✓ Open ID Connect の ID Token や SAML Assertion 等の、IdP等の認証サーバーでデジタル署名された認証時の情報。検証は後日行われる為に、デジタル署名を検証する公開鍵や電子証明書と共に保存されることが望ましい。

電子署名証拠 PoESign まとめ

PoESign : Proof of Electronic Signatures
電子署名証拠（現在はPoKEYとPoAIDのどちらか１つまたは両方で構成される）

PoKEY : Proof of signature KEY
署名鍵証拠（デジタル署名証拠）
format: PAdES/XAdES/CAdES/JAdES...

PoAID : Proof of Authorization ID
署名認可ID証拠（ID認証の証拠）
format: assertion（JWT） /audit logs..

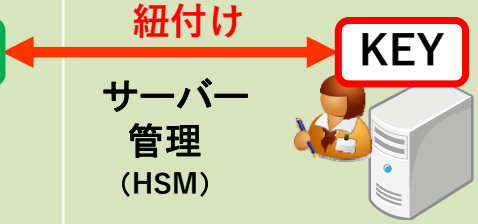
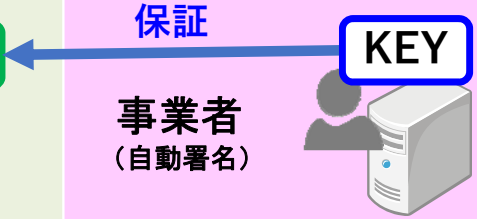
略称	名称	概要
PoESign	**電子署名証拠**	本人性と非改ざん性を保証する為のPoKEY・PoAID等で構成されるデータ群。 電子署名証拠は**第三者（検証者）により検証（確認）可能**である必要がある。
PoKEY	**署名鍵証拠** （デジタル署名証拠）	電子証明書と署名鍵利用のデジタル署名/PKIを保証する為のデータ群。 ISO/JIS等の先進署名（AdES）フォーマット等で標準化され非改ざんも保証される。 署名鍵は、本人所有の場合（本人保証）と、第三者（事業者保証）の場合がある。
PoAID	**署名認可ID証拠** （ID認証の証拠）	署名認可時のID認証認可を保証する為のデータ群。非改ざんの保証が別途必要。 アサーション（id_token等でIdP等の署名が必要）やアクセス/操作/監査のログ等。 アサーションの署名を後から検証可能とする為にIdP等の公開鍵も保管が必要。 IdPによる認証部以外はフォーマットが標準化されているとは言えず検討や策定が必要。

５．電子署名方式の分類

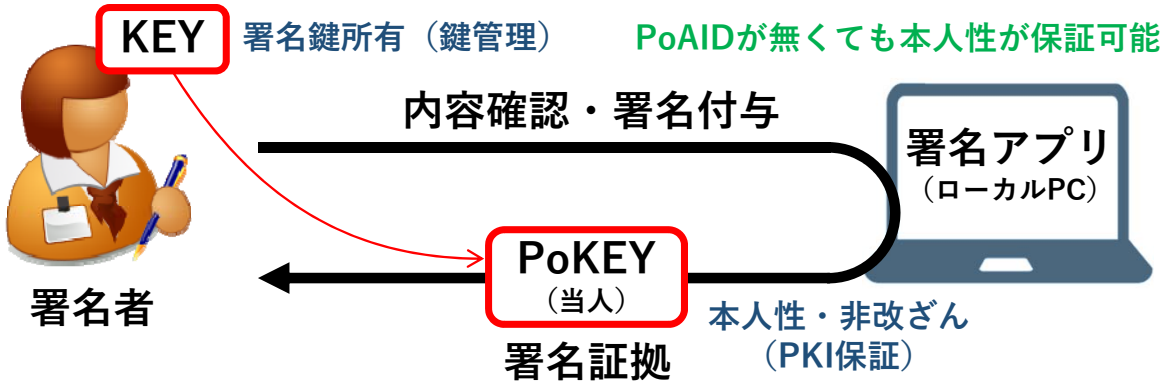
電子署名証拠（PoESign）により電子署名方式を分類します。
電子署名方式毎に求められる電子署名証拠の内容が異なります。

※ 各電子署名方式は保証レベルTFが独自に分類したものです。

電子署名証拠による電子署名方式の分類

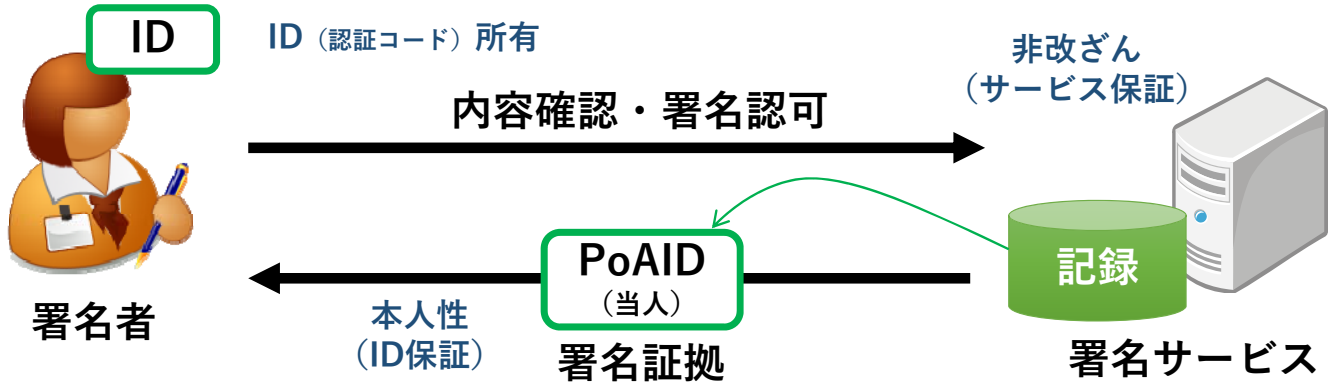
	認可ID（認証コード）	署名鍵	電子署名証拠（PoESign）
ローカル署名 （当人型署名）	不要 （本人鍵管理の為）	署名者 管理 （ICカード等） 	PoKEY：当人署名鍵証拠 （非改ざん・本人性保証） ※ 鍵は本人管理前提なのでPoAIDは不要
認証記録型署名 （新定義）	署名者 当人 	未使用	PoAID：署名認可ID証拠 （本人性保証） ※ 非改ざんはアクセスコントロール等で保証
リモート署名 （当人型署名）	署名者 当人 	紐付け  サーバー 管理 （HSM）	PoKEY：当人署名鍵証拠 （非改ざん・本人性保証） PoAID：署名認可ID証拠 （IDとKEYの紐付け保証・本人性保証）
事業者型署名	署名者 当人 	保証  事業者 （自動署名）	PoAID：署名認可ID証拠 （本人性保証） PoKEY：事業者署名鍵証拠 （非改ざんと署名の第三者保証）

方式1：ローカル署名（当人型署名）



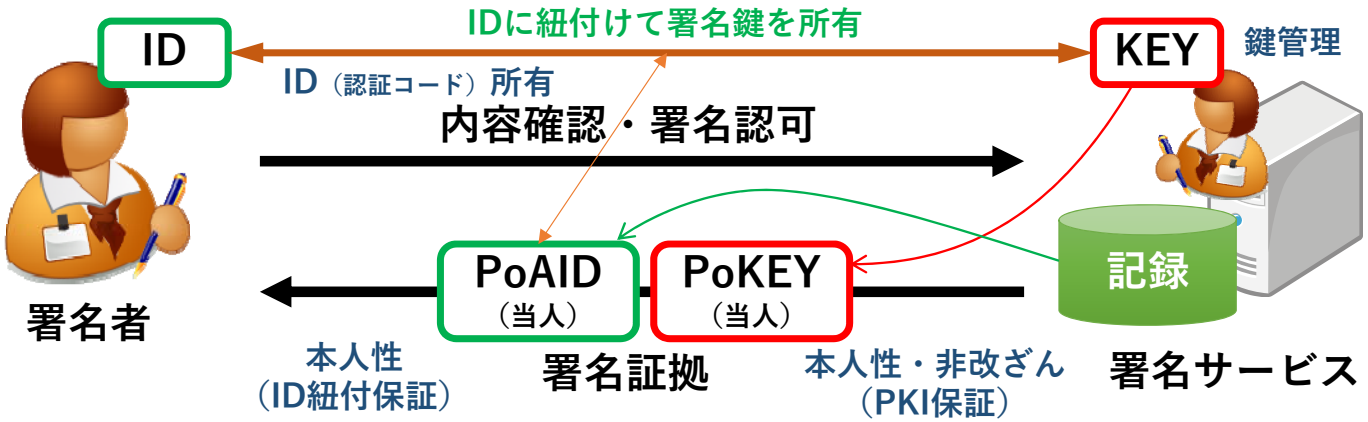
- ✓ **署名鍵の管理を署名者本人が行い**、ローカル環境で本人がデジタル署名を行う。
- ✓ 本人の署名鍵を使いデジタル署名の署名鍵証拠 **PoKEY**（PAdESやXAdES等）を生成する。署名データのフォーマットや検証手順は標準化されている。
- ✓ 本人の署名鍵と紐づいたPKIベースの電子証明書を、認証局が本人の身元確認を行った上で発行し保証することで本人保証を実現している。
- ✓ 電子署名法における認定認証業務は、ポリシーや運用が法令に規定された厳格な方法に従っていることが認定されており、本人による電子署名であることの証明は容易となる。
- ✓ 電子署名法が想定していた署名方式であり**ローカル署名の保証レベルが基本**となる。

方式2：認証記録型署名



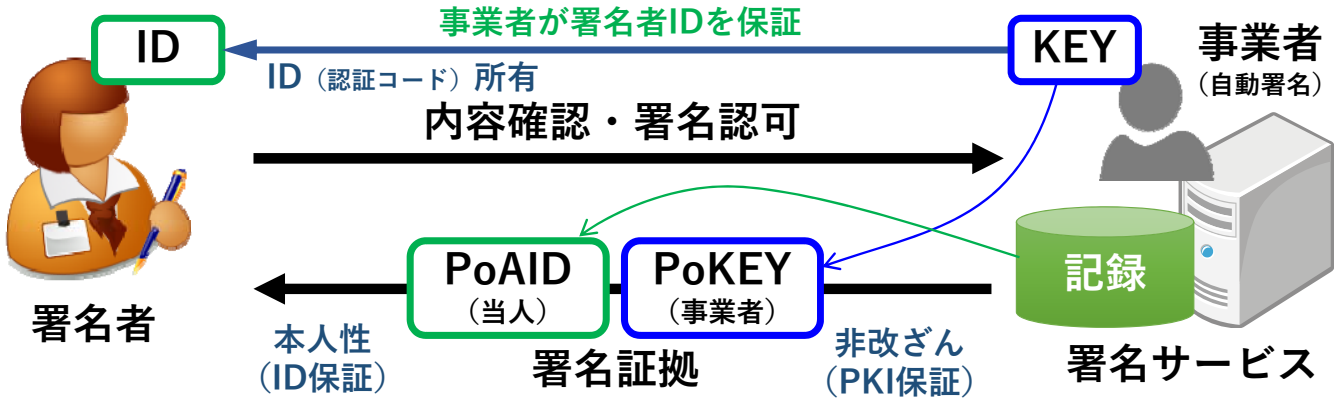
- ✓ **署名者が署名サービスに当人認証にてログイン**し、ログ情報や認証アサーションを保存する方式。**改ざん防止が別途必要**（アクセスコントロールや改ざん不可媒体保存等）。
- ✓ 電子署名とする為には認証要素の本人管理を行い、署名認可時の署名証拠 **PoAID**（認証アサーションやログ情報）を記録し検証者に提供する必要がある。
- ✓ 本人の電子署名であることをPoAIDや改ざん防止の証拠等で立証する必要がある。
- ✓ 認証局/PKIを利用した場合と比較して、署名者の身元確認の標準や認定が無い為、本人確認保証レベル（IAL）が低いことが多いので、確実な身元確認が望まれる。
- ✓ 業界（例：製薬）によっては認証記録型を「電子署名」として認めている場合もある。

方式3:リモート署名(当人型署名)



- ✓ **本人の署名鍵の鍵管理を署名サービス**に任せ**署名鍵に紐づいたIDを使った当人認証**の署名認可にてデジタル署名を行う。本人確認は基本的には認証局が行うが、署名認可用の認証要素の発行か登録が必要。署名認可用の認証要素は本人管理が必要。
- ✓ 署名データはローカル署名と同じ本人の署名鍵証拠 **PoKEY**(PAdESやXAdES等でローカル署名と同じ内容)となるが、署名鍵とIDとの**紐付けを保証**する為に署名認可時の署名証拠 **PoAID**(ログ情報や認証アサーション)も必要。
- ✓ 欧州では既に標準化されており、ローカル署名と同程度の保証レベルとされている。
- ✓ 同じ当人型のローカル署名と署名鍵証拠 PoKEY では区別が付かない課題がある。

方式4:事業者(立会人)型署名



- ✓ **署名者が署名サービスに当人認証にてログイン**し、ログ情報や認証アサーションを保存し、**改ざん防止と署名者の保証を事業者のデジタル署名**(自動署名)で行う方式。
- ✓ 署名データとして事業者の署名鍵証拠 **PoKEY**(PAdESやXAdES等)も提供されるが、電子署名とする為には認証要素の本人管理を行い、署名認可時の署名証拠 **PoAID**(認証アサーションやログ情報)を記録し**検証者に提供する**必要がある。
- ✓ 署名鍵の発行管理が不要であり、システムや利用者に対する利便性が高い利点がある。
- ✓ 認証局/PKIを利用した場合と比較して、署名者の身元確認の標準や認定が無い為、本人確認保証レベル(IAL)が低いことが多いので、確実な身元確認が望まれる。

6．電子認証保証レベル：NIST SP 800-63-3

電子署名の保証レベルを検討する前に、米国NISTの電子認証の
保証レベルを定義した NIST SP 800-63-3 を簡単に説明します。

※ NIST SP 800-63-3 を説明するドキュメントは多数ありますので詳しくはそちらを参照ください。
※ 2022年に新しい NIST PS 800-63-4 がリリースされる予定です。

「保証レベル」と言う考え方

NIST SP 800-63 シリーズと保証レベル：

- 2013年8月に公開された、NIST SP 800-63-2（Electronic Authentication Guideline）において **LoA**（Level of Assurance）と言う定義がなされた。
- これは電子認証において1つの保証レベルを定義していたが、複数の要件のうち1つでも低いレベルがあると全体の保証レベルも下がると言う問題があった。
- NIST SP 800-63-3 では後述する IAL/AAL/FAL の3つの保証レベルを定義することで、**それぞれ適切なレベルを選択**した組み合わせを可能とした。

NIST SP 800-63 シリーズから得られる保証レベルの知見：

- 保証レベルではレベル毎の具体的な要件を定義する必要がある。
- 高い保証レベルでは必要とする要件は増えるか厳しくなり難易度も高くなる。
- 最高の保証レベルが「正解」では無く、**利用目的に合致した保証レベルの選択が重要**となる。例：会議室予約システムの保証レベルは低くて良い。

電子認証保証レベル（NIST SP 800-63-3）

2017年6月に**NIST**（米国標準技術研究所）からFinal版が公開。
米国政府機関向けの**デジタルId実装ガイドライン**で2022年にSP 800-63-4が出る予定。
https://pages.nist.gov/800-63-3/

SP 800-63-3	**Digital Identity Guidelines** 「デジタルIdガイドライン」 全体の概要
SP 800-63A	**Enrollment and Identity Proofing** 「登録と身元情報の検証」 身元確認のガイドライン（登録時のレベル） **IAL**（Identity Assurance Level：身元確認保証レベル）の定義
SP 800-63B	**Authentication and Lifecycle Management** 「認証とライフサイクル管理」 当人確認のガイドライン（利用時のレベル） **AAL**（Authenticator Assurance Level：当人確認保証レベル）の定義
SP 800-63C	**Federation and Assertions** 「連携とアサーション」 連携時の認証/認可/属性情報のガイドライン **FAL**（Federation Assurance Level：連携情報保証レベル）の定義

※ 各保証レベルは各3レベルあり組み合わせて利用する。レベル1が最低限で、レベル3は機密情報アクセスのレベル。

IAL（身元確認保証レベル）：SP 800-63A

利用者が申請者として新規登録する際に、CSP（Credential Service Provider）が行う身元確認（Identity Proofing）の厳密さの保証レベルを示す。

レベル	要件概要
IAL.1	**身元確認不要、自己申告での登録でよい。** 例：メールアドレスの到達確認。
IAL.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。**
IAL.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の必要あり。** 例：マイナンバーカードの発行確認（対面必須）。

- ✓ 身元確認は電子署名でも必要な保証レベルであり、**そのまま電子署名の保証レベルとして利用が可能。**
- ✓ 電子署名においてデジタル署名＋PKI（公開鍵基盤）の場合には、認証局CAが行う身元確認のレベルと言える。正確には登録時の身元確認（本人性確認）は登録局RAの役割。
- ✓ パブリック認証局のIALのレベルは一般的に2以上となり、具体的な身元確認の方法はCP/CPSとして認証局が公開している。

※ CA：Certification Authority / RA：Registration Authority / CP：Certificate Policy / CPS: Certification Practice Statement

AAL（当人認証保証レベル）：SP 800-63B

登録済み利用者が、サービスにログインする際の認証プロセス（単要素認証、多要素認証、認証手段）の保証レベルを示す。

レベル	要件
AAL.1	**単要素認証でよい。**
AAL.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よい。**
AAL.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）が必要。**

※ AAL.2 以上では認証要素に Approved Cryptography（FIPS 140 Level 1 以上等）による技術やアルゴリズムが必要。

認証要素の種類：

知識	当人しか知り得ない情報（PIN番号・パスフレーズ 等）
所有	当人しか所有し得ない物に依存（ICカード・トークン 等）
生体	当人の生体としての情報（指紋・光彩・顔認識 等）

２要素認証：3つの認証要素の種類のうちの2つの要素の組み合わせ（知識＋所有等）による認証。
２段階認証：認証プロセスを２段階に分けて行う認証であり２要素とは限らない。

Authenticator（認証コード）の種類

No	名称	要素種別	鍵所持証明	ハードウェア
1	**Memorized Secret** 記憶シークレット （パスワード等）	**知識**	認められない	認められない
2	**Look-up Secret** ルックアップシークレット （乱数表等）	**所有**	認められない	認められない
3	**Out of Band Device** 経路外デバイス （SMS等、メール/VoIPは不可）	**所有**	認められない	認められない
4	**SF（Single Factor） OTP Device** 単一要素OTPデバイス/アプリ	**所有**	認められない	**△内容による**
5	**MF（Multi Factor） OTP Device** 多要素OTPデバイス/アプリ	**所有 +知識or生体**	認められない	**△内容による**
6	**SF Cryptographic Software** 単一要素暗号ソフトウェア （クライアント証明書等）	**所有**	**〇認められる**	認められない
7	**SF Cryptographic Device** 単一要素暗号デバイス （USBドングル等）	**所有**	**〇認められる**	**〇認められる**
8	**MF Cryptographic Software** 多要素暗号ソフトウェア	**所有 +知識or生体**	**〇認められる**	認められない
9	**MF Cryptographic Device** 多要素暗号デバイス （FIDO/ICカード等）	**所有 +知識or生体**	**〇認められる**	**〇認められる**

※ No.5/8/9は１つだけで多要素認証を実現可能だが、他の認証コードでは多要素にする為には組合せが必要。
※ ハードウェアと認められるのは通常はNo.7/9だが、No.4/5であってもデバイス利用であれば認められる。

FAL（連携情報保証レベル）：SP 800-63C

IDトークンやSAML Assertion等、Assertion（認証情報・属性・認可情報）のフォーマットやデータやり取りの仕方の保証レベルを示す。

レベル	要件
FAL.1	**Assertion（RPに送るIdPでの認証結果データ）へのデジタル署名が必要。**
FAL.2	**FAL. 1 に加えて、対象RPのみが復号可能な暗号化が必要。**つまりデジタル署名＋暗号化が必要。
FAL.3	**FAL. 2 に加えて、Holder-of-Key Assertionの利用（ユーザ毎の鍵と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）の確認）が必要。**

- ✓ FAL自体は電子認証の特有の保証レベルであり、そのまま電子署名の保証レベルとしては利用できない。
- ✓ 一方でFALをデータ仕様の保証レベルと考えると、電子署名において検証時に利用するデータ仕様の保証レベルとして見た場合に共通性がある。
- ✓ 特に電子署名証拠の1つであるPoAID（ID認証の証拠）と、Assertionと言う意味で共通した要件が多い。これはPoAIDとは（後から）検証可能なAssertionのことであるとも言えるからである。
- ✓ FAL.3 では HoK を要件として求めているが、これは PoP（Proof of Possession）と考えると署名鍵の所有と見ることが出来る。

7．電子署名保証レベル：JNSA eSignAL

電子認証の保証レベルである NIST SP 800-63-3 を利用して、
新しく定義をした電子署名の保証レベル eSignAL を説明します。

※ 電子署名保証レベル eSignAL は保証レベルTFから新たに提案する定義です。
※ NIST PS 800-63-4 がリリースされた場合には更新する可能性があります。

電子署名保証レベル eSignAL の定義

- ここまで電子署名と電子認証の整理と、電子署名証拠 PoESign の定義と署名方式の整理、及び電子認証の保証レベルの確認を行ってきた。
- これにより電子署名の保証レベル **eSignAL**（electronic Signatures Assurance Level）を定義する準備はできた。
- 基本的な考え方として NIST SP 800-63-3 の保証レベルを電子署名に拡張する為に、新たに3つの電子署名用の保証レベルを定義した。

1. **署名認可保証レベル　　：SAAL**（Signing Authorizartion Assurance Level）
2. **検証可能データ保証レベル　：VDAL**（Verifiable Data Assurasnce Level）
3. **運用ポリシー保証レベル　　：OPAL**（Operational Policy Assurance Level）

登録時の**「身元確認保証レベル：IAL」**に関しては電子署名保証レベルにおいてもそのまま利用する。

電子署名と電子認証の保証レベル

レイヤー	電子署名	電子認証
IDENTITY （身元）	**IAL: Identity AL（Assurance Level）** **本人確認保証レベル - NIST SP 800-63A** 登録時の本人の身元確認のプロセス保証レベル（電子署名と電子認証で共通）	
PROCESS （プロセス）	**SAAL: Signing Authorization AL** **署名認可保証レベル - JNSA eSignAL** 署名時（利用時）のプロセス保証レベル 署名手順と当人認証（AAL）のレベル	**AAL: Authenticator AL** **当人認証保証レベル - NIST SP 800-63B** 認証時（利用時）のプロセス保証レベル 認証要素（多要素等）に依存
DATA （データ）	**VDAL: Verifiable Data AL** **検証可能データ保証レベル - JNSA eSignAL** 検証に利用するデータ保証レベル 検証可能なPoESign（署名証拠データ）のレベル	**FAL: Federation AL** **連携情報保証レベル - NIST SP 800-63C** 連携時のデータ保証レベル アサーションの署名・暗号化・HoKアサーション
POLICY （ポリシー）	**OPAL: Operational Policy AL** **運用ポリシー保証レベル - JNSA eSignAL** 運用や認定・監査のポリシー保証レベル SP 800-63-3 には無い保証レベルだが電子認証でも必要ではないか	

利用

SAAL（署名認可保証レベル）：eSignAL

登録済み署名者が、署名対象の内容確認を行って、署名認可（署名付与）を行うまでのプロセスの保証レベルを示す。ローカル署名の場合は署名鍵の所持の保証レベルとなる。

レベル	要件
SAAL.1	署名前に署名対象の内容確認を行い、サービス認証（サービスへのログイン）または署名認可（署名毎の認可）に AAL.1（単要素認証）以上が必要。
SAAL.2	SAAL.1 に加えて、署名認可時（署名毎）に AAL.2（2要素認証）が必要。暗号利用の署名鍵を利用する場合は FIPS 140-2 Level 3 相当以上のハードウェア保護（HSM等）が必要。
SAAL.3	SAAL.2 に加えて、署名認可時（署名毎）に AAL.3（ハードウェア利用2要素認証）が必要。

※ AAL.2 以上では認証要素に Approved Cryptography（FIPS 140 Level 1 以上等）による技術やアルゴリズムが必要。

- ✓ 基本的にはAALと同じではあるが、署名時に**署名対象の内容確認ステップを要求**している点が異なる。
- ✓ SAAL.1では署名認可だけではなく、サービス認証によるログインセッション中に複数の署名付与を実行することを許している。SAAL.2以上では署名毎に認可を与える必要がある。
- ✓ 電子シール的な利用方法である自動署名（システムによる署名認可）に関してはスコープ外となる。
- ✓ SAAL.2以上においてデジタル署名を利用する場合（ローカル署名・リモート署名・事業者型署名）には認定されたHSMによる署名鍵の保護が要求される。

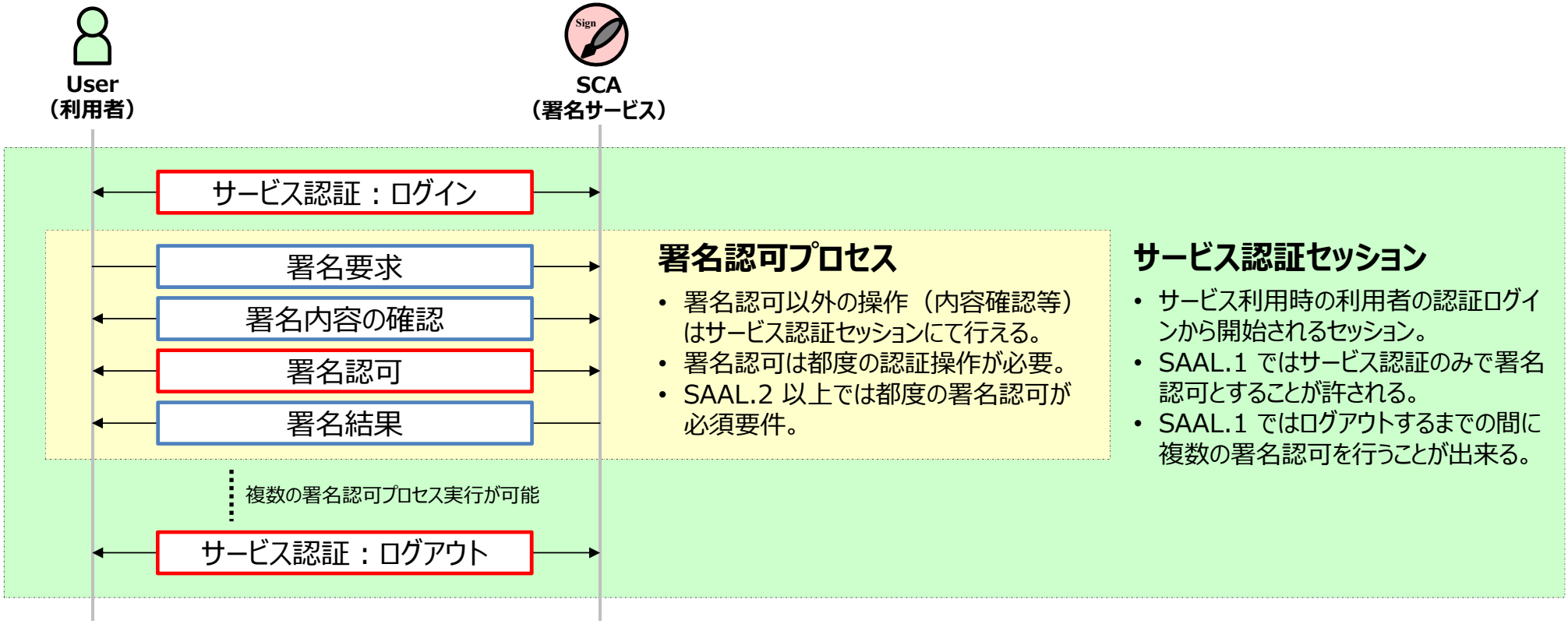
証明方式毎のSAAL考察

レベル	ローカル署名	認証記録型署名	リモート署名	事業者型署名
SAAL.1	自分で内容を確認した上で、ソフト的（PKCS#12等）に格納され管理された署名鍵（AAL.1相当）によるデジタル署名を付与する。	署名対象を確認した上で署名認可にIDとパスワード（AAL.1）を利用する。IDとパスワードによるサービス認証も可能。	署名対象を確認した上でサーバーに預けた署名鍵を、IDとパスワード（AAL.1）による署名認可によりデジタル署名を付与する。IDとパスワードによるサービス認証も可能。	署名対象を確認した上で署名認可にIDとパスワード（AAL.1）を利用する。署名時に事業者はデジタル署名を付与する。IDとパスワードによるサービス認証も可能。
SAAL.2	自分で内容を確認した上で、スマホ等に格納され管理された署名鍵（AAL.2相当）によるデジタル署名を付与する。	署名対象を確認した上で署名認可に2要素認証（AAL.2）を利用する。	署名対象を確認した上でサーバーのHSMに預けた署名鍵を、2要素認証（AAL.2）による署名認可によりデジタル署名を付与する。	署名対象を確認した上で署名認可に2要素認証（AAL.2）を利用する。署名時に事業者はHSMに預けた署名鍵でデジタル署名を付与する。
SAAL.3	自分で内容を確認した上で、ICカードやスマホSE等に格納され管理された署名鍵（AAL.3相当）によるデジタル署名を付与する。	署名対象を確認した上で署名認可にハード利用の2要素認証証（AAL.3）を利用する。	署名対象を確認した上でサーバーのHSMに預けた署名鍵を、ハード利用の2要素認証（AAL.3）による署名認可によりデジタル署名を付与する。	署名対象を確認した上で署名認可にハード利用の2要素認証証（AAL.3）を利用する。署名時に事業者はHSMに預けた署名鍵でデジタル署名を付与する。

- ✓ ローカル署名を除き、基本的には署名対象の確認が必要な以外はAALのレベルと同じになる。
- ✓ スマホSEとはスマホ（Android/iPhone）に搭載されているプロテクトされた Secure Element を指す。

サービス認証と署名認可

署名サービスを利用する場合にはまず利用者のサービス認証を行い、署名時に署名認可を行う。ただしローカル署名の場合にはサービス認証は不要となる。



VDAL（検証可能データ保証レベル）：eSignAL

本人性（本人の署名意思）と非改ざんを保証する、第三者によって検証可能なデータ（署名証拠：PoESign）の保証レベルを示す。

レベル	要件
VDAL.1	**サーバ保管された本人のID利用ログ等による意思確認と、アクセスコントロールや追記不可メディア保存等の運用による非改ざんに関する、第三者保証の検証可能データ（PoAID）が必要。** 第三者保証の検証可能データ：何らかの検証可能データが提供可能なレベル。 ✓ 非改ざんに関してはアクセスコントロールを証明するアクセスログ等により客観的に認められれば良い。 ✓ 署名時のデジタル署名は不要だが署名証拠として外部提供する場合には事業者（保証者）のデジタル署名付与が望ましい。
VDAL.2	**IAL.2 相当（プライベート認証局等）の身元確認と、本人管理の署名鍵によるデジタル署名データ（PoKEY）または検証可能な署名認可時の2要素認証（SAAL.2）のアサーション・ログ（PoAID）と、デジタル署名等の暗号利用による非改ざんの、証拠が必要。**
VDAL.3	**IAL.3 相当（パブリック認証局等）の身元確認と、本人管理のハードウェア利用署名鍵によるデジタル署名データ（PoKEY）または検証可能な署名認可時のハードウェア利用2要素認証（SAAL.3）のアサーション・ログ（PoAID）と、デジタル署名等の暗号利用による非改ざんの、証拠が必要。**

※ アサーション（assertion）は認証要求者の認証結果情報に認証器（IdP等）がデジタル署名した検証可能（JWS形式等）なデータであり一般には Open ID Connect ID Token や SAML Assertion を指している。NIST SP 800-63C より意訳。

※ VDALはあくまでデータの保証レベルを示すものなのでIALとSAALのプロセスの結果の証拠としてのデータが必要となる。

VDAL説明

- ✓ VDALでは、IAL（登録時）の証拠と、AAL（署名認可時）の証拠の、2つにより本人の意思を保証している。
- ✓ SAALとVDALはAALを利用しているが、SAALはAAL認証プロセスそのものを利用しているのに対して、VDALはAAL認証プロセスの結果を証拠（PoAID）としている点が異なる。
- ✓ ID認証（ID）の場合には認証サーバーがデジタル署名したIDトークン等（認証や認可の結果）でIAL/AAL相当の保証を提供する（PoAID）。
- ✓ デジタル署名（PKI）の場合には、電子証明書でIALの保証を行い、署名鍵の行使にてAAL相当の保証を提供する（PoKEY）。
- ✓ 非改ざんはデジタル署名等の暗号利用で保証する方法と、運用により保証する方法の2種類があるが、VDAL.2 以上では署名対象へのデジタル署名が必須となる。
- ✓ 標準化された署名証拠（PoESign）のフォーマットは、多数の専門家のチェックを受けており独自フォーマットよりも信頼できる。PoKEYであれば長期署名フォーマット（AdES）であり、PoAIDであればOIDCのIDトークンやSAMLアサーションが、標準化されたフォーマットと言える。
- ✓ VDAL.2 以上では標準化されたデータフォーマットの利用が推奨される。

証明方式毎のVDAL考察

レベル	ローカル署名	認証記録型署名	リモート署名	事業者型署名
VDAL.1	CP/CPS非公開独自証明書（IAL.1相当）と当人管理署名鍵のデジタル署名（PoKEY）	IAL.1相当の身元確認と、サービス認証時か署名認可時のログ（PoAID）と、非改ざんの証拠または運用	CP/CPS非公開独自証明書（IAL.1相当）とサーバー管理署名鍵のデジタル署名（PoKEY）と、サービス認証時か署名認可時のログ（PoAID）	IAL.1相当の身元確認と、サービス認証時か署名認可時のログ（PoAID）と、CP/CPS非公開独自証明書の事業者によるデジタル署名（PoKEY）
VDAL.2	公開プライベート認証局（IAL.2相当）証明書と当人管理署名鍵のデジタル署名（PoKEY）	IAL.2相当の身元確認と、署名認可時の2要素認証アサーション・ログ（AAL.2のPoAID）と、検証可能な非改ざんの証拠または運用	公開プライベート認証局（IAL.2相当）の証明書とサーバー管理署名鍵のデジタル署名（PoKEY）と、署名認可の2要素認証アサーション・ログ（AAL.2のPoAID）	IAL.2相当の身元確認と、署名認可時の2要素認証アサーション・ログ（AAL.2のPoAID）と、プライベート証明書の事業者によるデジタル署名（PoKEY）
VDAL.3	パブリック認証局（IAL.3相当）証明書とICカード等の当人管理署名鍵のデジタル署名（PoKEY）	IAL.3相当の身元確認と、署名認可時のハードウェア利用2要素認証アサーション・ログ（AAL.3のPoAID）と、検証可能な非改ざんの証拠または運用	パブリック認証局（IAL.3相当）の証明書とサーバーHSM管理署名鍵のデジタル署名（PoKEY）と、署名認可のハードウェア利用2要素認証アサーション・ログ（AAL.3のPoAID）	IAL.3相当の身元確認と、署名認可時のハードウェア利用2要素認証アサーション・ログ（AAL.3のPoAID）と、パブリック証明書の事業者によるデジタル署名（PoKEY）

✓ リモート署名と事業者型署名ではPoKEYとPoAIDの両方が必要となる。

OPAL（運用ポリシー保証レベル）：eSignAL

電子署名のサービスやプロセスに関する、運用ポリシー（公開・標準・認定や監査）による信頼性の保証レベルを示す。

レベル	要件
OPAL.1	非公開ポリシー準拠： **非公開でも独自の運用ポリシーがあり、その運用ポリシーの要件に従った運用が必要。**
OPAL.2	公開標準ポリシー準拠： **OPAL.1 に加え、運用ポリシーが標準化または公的に認められており、その運用ポリシーの公開が必要。**
OPAL.3	認定取得または定期的監査： **OPAL.2 に加え、運用について公的またはデファクト標準となる認定を取得しているか、有資格者による監査を定期的に受けた運用が必要。**

- ✓ 電子署名プロセス（登録から署名認可まで）を信頼する為の基準となる運用ポリシーについてのレベルを定義する保証レベル。
- ✓ 非公開よりも公開が、独自仕様よりも標準準拠が、非認定よりも認定済みが、非監査よりも定期監査が、保証レベルが高い。
- ✓ 電子認証においても運用ポリシー保証レベルは必要とは考えるが、ここではスコープ外とする。

証明方式毎のOPAL考察

レベル	ローカル署名	認証記録型署名	リモート署名	事業者型署名
OPAL.1	非公開CP/CPSの順守	非公開サービス運用ポリシーの順守	非公開CP/CPSと非公開サービス運用ポリシーの順守	非公開サービス運用ポリシーの順守
OPAL.2	標準準拠CP/CPSの公開と順守 ・RFC 3647等	標準準拠サービス運用ポリシーの公開と順守 ・標準化運用ポリシー無し	標準準拠CP/CPSと標準準拠サービス運用ポリシーの公開と順守 ・欧州eIDASの運用ポリシー等	標準準拠サービス運用ポリシーの公開と順守 ・標準化運用ポリシー無し
OPAL.3	認定済み公開CP/CPSの順守 ・認定認証局 ・WebTrust等	認定済み公開サービス運用ポリシーの順守 ・認定制度無し	認定済み公開CP/CPSと公開サービス運用ポリシーの順守 ・欧州eIDASのTSP認定等 ・日本には現在認定制度無し	認定済み公開サービス運用ポリシーの順守 ・認定制度無し

※ CP/CPS = 証明書ポリシー（Certificate Policy）/認証局運用規定（Certification Practice Statement）。
※ ローカル署名を除いてリモート・事業者型・認証記録の署名に関する認定制度（OPAL.3）が現在の日本に無いことは今後の課題。

- ✓ ローカル署名はPKIを直接利用する為に、運用ポリシーに関しても長い標準化や認定の歴史がありOPALのレベル1～3全てに対応が可能となっている。
- ✓ リモート署名は欧州では既に運用ポリシーの標準化や認定制度があるが、日本においての標準化はこれからであり、認定制度もこれからとなる。
- ✓ 認証記録型署名と事業者型署名に関しては、運用ポリシーの標準化も認定制度もまだない。

おわりに：電子署名保証レベル

本資料では電子署名保証レベルの説明をしましたが保証レベルは高いほど良いと言う訳ではありません。一般に保証レベルが高くなると利便性は低下します。**利用目的に合った適正な保証レベルの選択が必要**です。

電子署名保証レベルは **IAL/SAAL/VDAL/OPAL** で構成されますが、**各要素毎に異なる保証レベルの組合せが可能**です。個別に必要となる保証レベルを選択します。

また電子署名保証レベル検討では共通の保証レベルを策定する為に、署名方式を整理分類して**４つの署名方式**にまとめました。

電子署名保証レベルは、電子認証の保証レベル NIST SP-800-63-3 をベースとしています。しかし新しいバージョン **SP 800-63-4 が2022年にはリリースされる予定**です。この為に今後更新される可能性があります。今後も見直しつつ要約版ではない正式版をできるだけ早くリリースする予定です。

電子署名サービスの仕様検討時や、電子署名の利用者も自身が利用する電子署名の保証レベルを知る為の参考ガイドとして本資料をご利用ください。

付録:参考情報

付録1：代行・代理・委任の整理

	判断	署名操作	署名鍵	補足
本人	○ 本人	○ 本人	○ 本人	全て本人が一般的な電子署名。 署名鍵があれば本人が管理する。
代行	○ 本人	● 代行人	○ 本人	署名鍵は代行人が管理して本人の指示に従って署名操作を行う。代行人は判断をしない。
代理/委任	▲ 代理人	▲ 代理人	▲ 代理人 （○ 本人）	委任と代理は同じ。 例えば法人代表者は法人の代理人である。 ➢ 委任者＝本人（当人） / 受任者＝代理人 委任時に判断範囲（代理権）の制限も可能。 代理人が代行して本人署名鍵を利用する場合もありうるので署名鍵は本人の場合もある。

※ 代行や代理/委任を行う場合には運用ポリシーを決めて遵守する必要がある。
※ 代理/委任を行う場合には判断の範囲や内容を決めておく必要がある。

付録2：電子シール（eシール）の整理

eIDASの電子シール（eシール）定義：

- Similar in its function to the traditional business stamp. It can be applied to an electronic document to guarantee the origin and integrity of a document.
  ※ business stamp = company seal：社印と翻訳される場合が多い。
- 翻訳：従来のビジネススタンプの機能に似ている。電子文書に対して発行元と完全性を保証する。
  意訳：法人・組織（非自然人）電子証明書のデジタル署名にて発行元と非改ざんを保証する。
  ※ eIDASのQualified/Advancedの電子シールではデジタル署名とPKIを利用している。

目的：発行元（発行組織）を保証する**「証明」**を重視した利用が主と考えられる。
※ 電子署名の場合には「証明」より「証拠」としての目的が主となる点で異なる。Page14参照。

電子シールプロセス：

✓ 通常は自社が発行する電子文書に電子シールを付与する。
✓ 証明の場合は電子署名（本人の意思）と異なりシール毎に認可を行う必要はない。
✓ シール認可のルールを決めておきシステムにて自動シール（自動デジタル署名）が可能。
✓ 保証レベル的にはIALとOPALが重要。自動発行ではSAALはさほど重要ではない。

付録3：主な略語一覧

略語	フル名	日本語	説明
IAL	Identity Assurance Level	身元確認保証レベル	NIST SP 800-63-3A：身元確認の保証レベル
AAL	Authenticator Assurance Level	当人認証保証レベル	NIST SP 800-63-3B：利用者の認証プロセスの保証レベル
FAL	Federation Assurance Level	連携情報保証レベル	NIST SP 800-63-3C：Assertionの保証レベル
HoK	Holder of Key	鍵の所持者	鍵所持証明の認証要素を所有している状態
PoP	Proof of Possession	（鍵）所持の証明	鍵所持証明と言う意味でHoKとほぼ同じ意味
eSignAL	electronic Signatures Assurance Level	電子署名保証レベル	新定義：IAL/AALと新定義のSAAL/VDAL/OPALを使った電子署名の保証レベル
SAAL	Signing Authorization Assurance Level	署名認可保証レベル	eSignAL（新）：署名認可時のプロセスに関する保証レベルで、定義には当人確認保証レベルAALを利用
VDAL	Verifiable Data Assurance Level	検証可能データ保証レベル	eSignAL（新）：検証時のデータに関する保証レベルで、定義には電子署名証拠PoESignを利用
OPAL	Operational Policy Assurance Level	運用ポリシー保証レベル	eSignAL（新）：運用ポリシーに関する保証レベルで、定義には認定や監査も利用
PoESign	Proof of Electronic Signatures	電子署名証拠	新定義：本人性（本人の意思）と非改ざん性（非改変）を確認できる情報群 署名時生成の署名データと署名後に取得する検証属性データで構成される
PoKEY	Proof of signature KEY	署名鍵証拠	新定義：デジタル署名（PKI）を使った電子署名証拠
PoAID	Proof of Authorization ID	署名認可ID証拠	新定義：ID認証（ID）を使った電子署名証拠
eSign	electronic Signatures	電子署名	自然人によるデータに対する本人性（本人の意思）と非改ざん性（非改変）の保証
eSeal	electronic Seals	電子シール（eシール）	法人・組織によるデータに対する発行元証明と非改ざん性（非改変）の保証
IdP	Identity Provider	IDプロバイダ	認証サービス提供事業者。OIDCではOP（OpenID Provider）と呼ばれる。
RP	Relying Party	リライングパーティー	認証サービスを利用して独自のサービスを提供する事業者。SAMLではSP（Service Provider）と呼ばれる。

付録4：参考リンク

本資料を理解する為にはデジタル署名＋PKIやID認証に関する知識が必要となります。
以下は参考となる資料や情報へのリンクです。

ID認証入門：

OsSAL：今更聞けない電子認証入門 ～OAuth 2.0 / OIDC から FIDO まで～ <改定２版>
https://www.ossal.org/doc/LE-Auth-20200929.pdf

デジタル署名・PKI入門：

JNSA 電子署名WG：電子署名（PKI）ハンズオン ～電子署名・タイムスタンプ超入門！～
http://eswg.jnsa.org/sandbox/handson/ESig-PKI-handson-doc-v100.pdf

JNSA 電子署名WG：電子署名Q&A（オンラインQA集）
https://www.jnsa.org/result/e-signature/e-signature-qa/

JNSA 電子署名WG 署名検証TF：デジタル署名検証ガイドライン
https://www.jnsa.org/result/e-signature/2021/

JT2A リモート署名TF：リモート署名ガイドライン
https://www.jnsa.org/result/jt2a/2020/

JT2A 真正性保証TF：オンライン身元確認(eKYC)金融事例調査報告書
https://www.jnsa.org/result/jt2a/2021/

作成メンバー（五十音順）

JNSA
（NPO日本ネットワークセキュリティ協会）
標準化部会
電子署名ワーキンググループ
保証レベルタスクフォース

https://www.jnsa.org/
http://eswg.jnsa.org/

新井 聡	（NTTビジネスソリューションズ株式会社）
漆嶌 賢二	（GMOグローバルサイン株式会社）
小川 博久	（株式会社三菱総合研究所）
小久保 敏	（セコムトラストシステムズ株式会社）
酒巻 一紀	（三菱電機インフォメーションシステムズ株式会社）
佐藤 雅史	（セコム株式会社）
新宅 友也	（GMOグローバルサイン・ホールディングス株式会社）
杉崎 元	（三菱電機インフォメーションネットワーク株式会社）
高丸 祐典	（三菱電機インフォメーションシステムズ株式会社）
竹岡 義樹	（アドビ株式会社）
西窪 健太	（日本ネットワークセキュリティ協会 電子署名WG）
日戸 直紘	（株式会社エヌ・ティ・ティ・データ）
星 尚之	（株式会社エヌ・ティ・ティ・データ）
政本 廣志	（日本ネットワークセキュリティ協会 電子署名WG）
宮内 宏	（弁護士：宮内・水町IT法律事務所）
宮崎 一哉	（三菱電機株式会社：電子署名WGリーダー）
宮地 直人	（有限会社ラング・エッジ：保証レベルTFリーダー）