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

- 電子署名再定義と今後の動き –

電子署名保証レベルについて

【 JNSA2023年度活動報告会 】

JNSA 標準化部会 電子署名WG

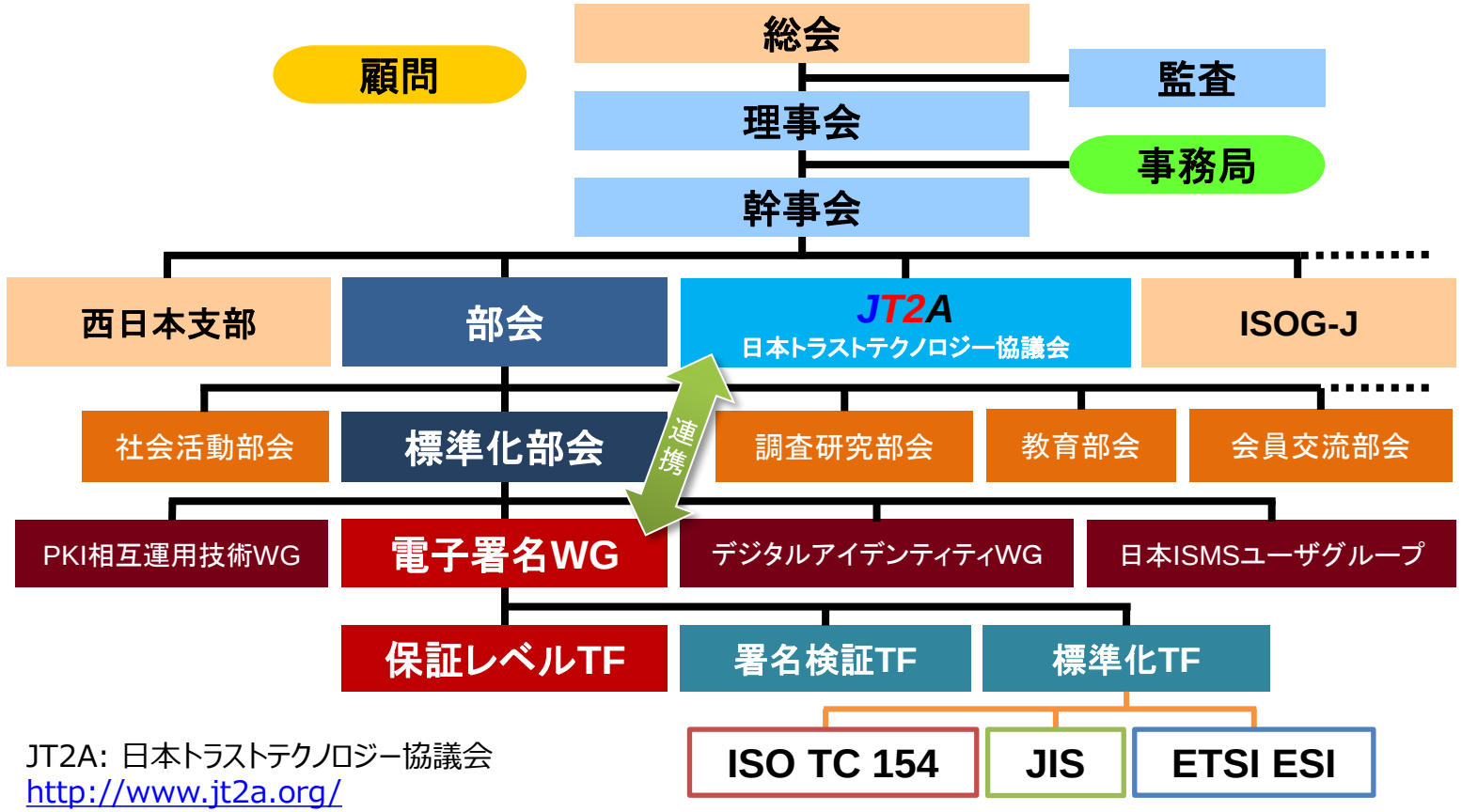
2023/06/07

電子署名WGサブリーダー（有限会社ラング・エッジ） 宮地

電子署名WGについて

JNSAの標準化部会下に電子署名WGがあります。

JNSA組織図



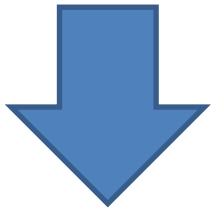
JT2A: 日本トラストテクノロジー協議会
http://www.jt2a.org/

名称：
Japan Network Security Association（略称JNSA）
特定非営利活動法人日本ネットワークセキュリティ協会
会員数：
2023年5月17日現在 263社
メンバー：
セキュリティ関連ベンダー

電子署名WGは、JNSAの標準化部会の1つとして、ISO TC 154にて長期署名プロファイルISO 14533シリーズの標準化やJIS化や、欧州ETSIメンバーとしての活動に加え、各種ガイドライン・調査資料の作成を行っています。
JT2Aは独立していますが電子署名WGメンバーと、セキュリティベンダー以外のメンバーも加えてリモート署名ガイドラインの作成等を行っています。

電子署名とは？

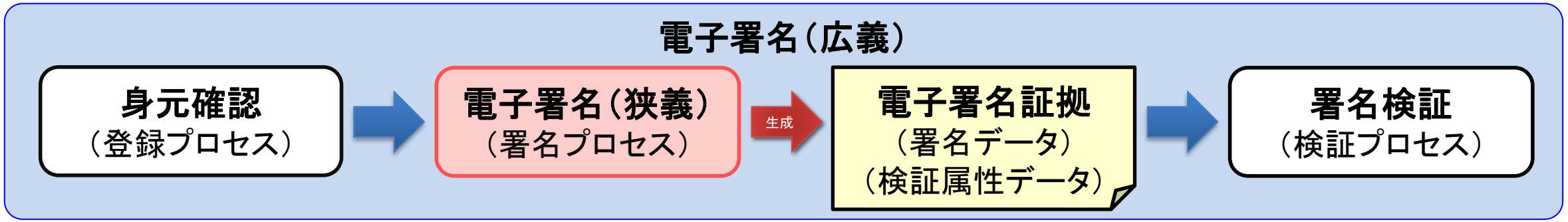
Q: 電子署名とは何でしょう？



レガシーな回答：

PKIベースのX.509電子証明書と紐づけられた公開鍵暗号方式の署名鍵によるデジタル署名をおこなうことが電子署名。これが電子署名法が施行された2001年以降の定義だった。

電子署名の要件確認と再定義



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。

クラウド（オンライン）化と認証技術の進歩

2017年 NIST SP 800-63-3 Final公開：「保証レベル」と言う考え方 ← 重要！
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 Draft 公開。
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（連携時のレベル） **FAL**（Federation Assurance Level：連携情報保証レベル）の定義

※ **認証**（デジタルId）も**署名**（PKI）も**本人性を保証するトラスト技術**。違いは何？

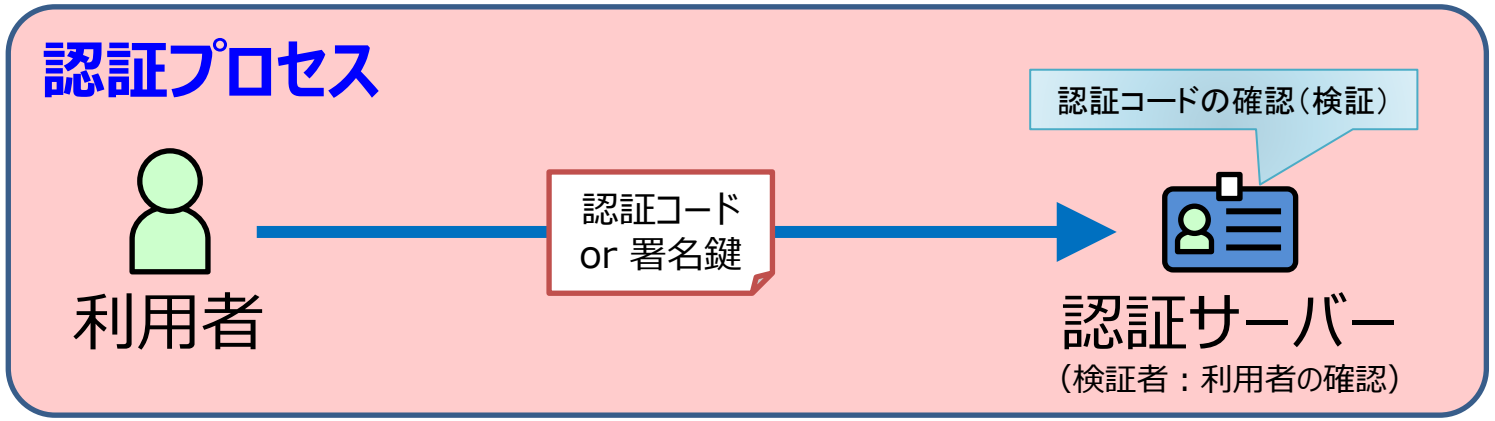
技術的整理：認証/承認署名/証明署名

	認証	承認署名（電子署名法）	証明署名
保証対象	**プロセス保証**	**データ保証**	**データ保証**
保証タイミング	**リアルタイム**	リアルタイム～**時差あり**（後で検証可）	**リアルタイム**～時差あり
利用目的	端末前の当人認証	内容への同意（承認・意思）	データ発行元と非改ざんの保証
保証内容	**本人性**・属性 ※ リアルタイムの本人性確認	**本人性**・非改ざん性 ※ 後日第三者により本人性確認が可能	発行元・非改ざん性 ※ 発行元は本人性だが非自然人も可
代表的技術	Id認証/認可 ※ OIDC/SAML/FIDO等	電子署名/X.509**個人**証明書 ※ ローカル署名/リモート署名等	電子シール/X.509**組織**証明書 ※ サーバー署名/タイムスタンプ等
署名認可		内容を確認して署名の**都度必要** ※ 自動署名してはいけない	自発行データに**自動署名可能** ※ 都度認可しても良い
マイナンバーカード	利用者証明用電子証明書	署名用電子証明書	

- 認証と承認署名は本人性と言う意味では同じだが保証対象と保証タイミングが異なる。
- 承認署名と証明署名はデータ保証と言う意味では同じだが利用目的が異なる。自動署名が可能かどうかで区別することができる。「電子署名保証レベル要約版」は「承認署名」の保証レベル解説書となっている。

※ 本整理は今年度おこなったものであり現在公開中の「電子署名保証レベル要約版」の記載とは異なっている。「承認」を「証拠」としていた。今年度作成予定の「電子署名保証レベルガイドブック（仮）」には反映予定。

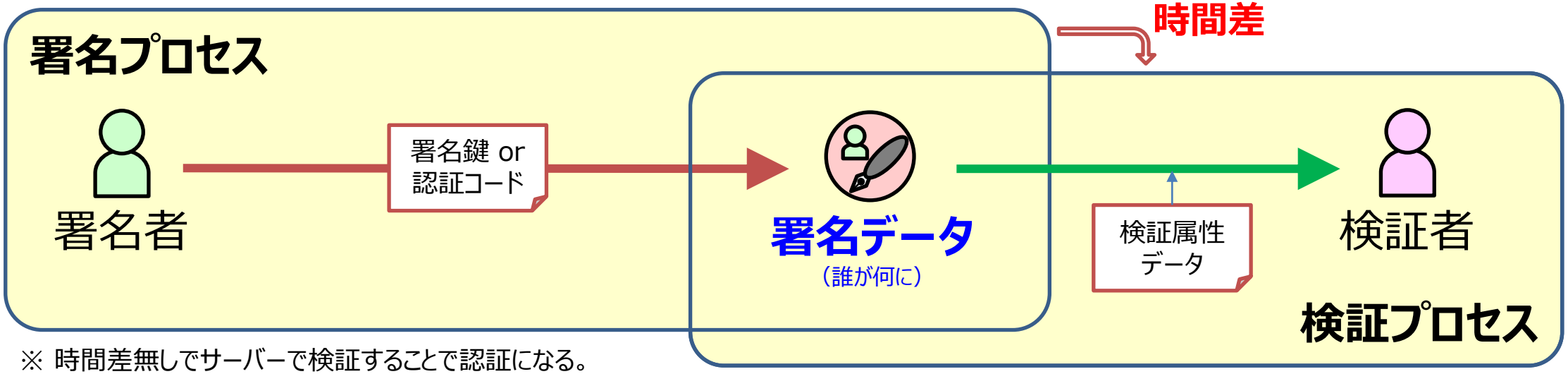
認証と署名の利用モデル比較



※ 認証コードの検証時のログを第三者が検証可能な署名データとして残せば署名になる。

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。

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ーで検証することで認証になる。

署名と認証の保証レベル比較

レイヤー	署名	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	≒ 利用 **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	≠ 異なる **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	

電子署名証拠 PoESign

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...

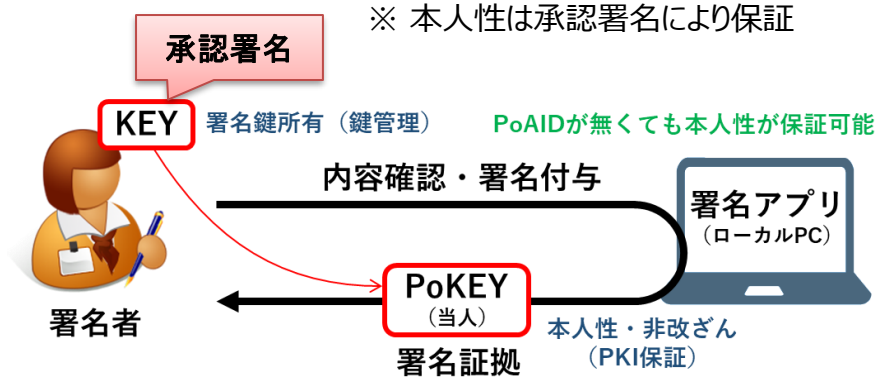
PoAID：Proof of Authorization ID
署名認可ID証拠（ID認証の証拠）
format: assertion（JWT） /audit logs..

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。

電子署名方式の分類

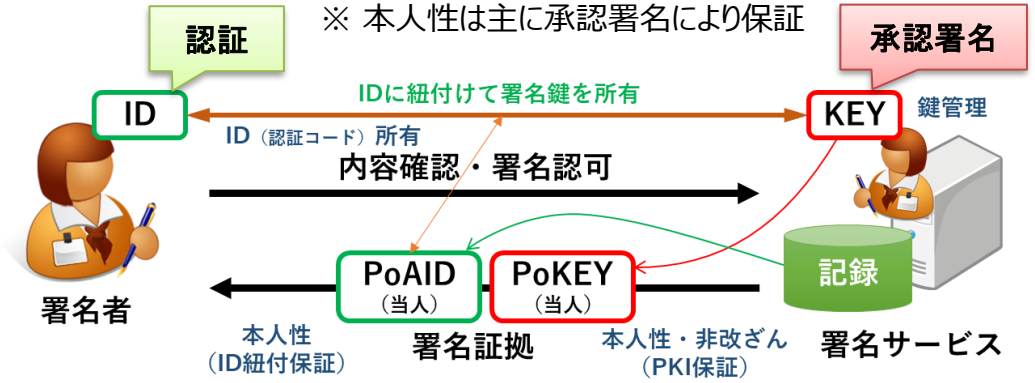
方式1：ローカル署名（当人型署名）

※ 本人性は承認署名により保証



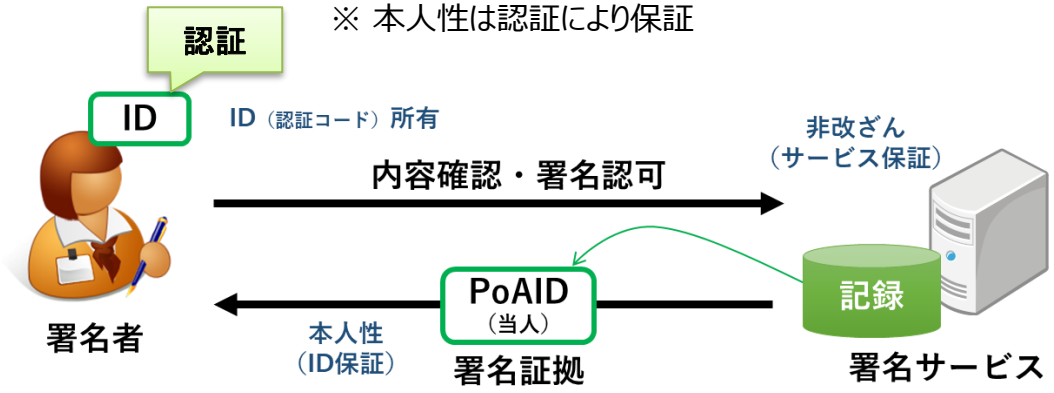
方式3：リモート署名（当人型署名）

※ 本人性は主に承認署名により保証



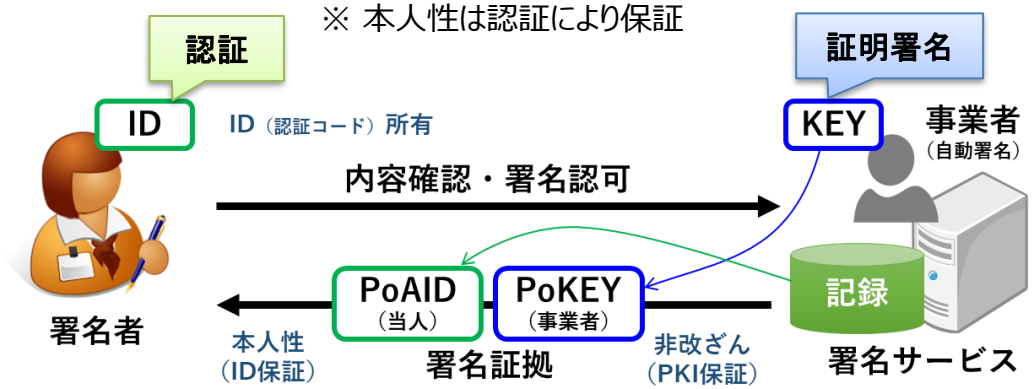
方式2：認証記録型署名（新定義）

※ 本人性は認証により保証



方式4：事業者（立会人）型署名

※ 本人性は認証により保証



電子署名WG 保証レベルTF 活動

活動履歴：
2021/07/29 保証レベルTF 説明会（募集開始）
2021/08/30 保証レベルTF ブレスト1
2021/08/31 電子署名WG2021#05 保証レベルTF
2021/09/27 電子署名WG2021#06 保証レベルTF
2021/10/11 保証レベルTF ブレスト2
2021/10/27 電子署名WG2021#07 保証レベルTF
2021/11/08 保証レベルTF ブレスト3
2021/11/29 電子署名WG2021#08 保証レベルTF
2021/12/15 保証レベルTF ブレスト4
2021/12/22 電子署名WG2021#09 保証レベルTF
2022/01/22 電子署名WG2021#10 保証レベルTF
2022/02/18 電子署名WG2021#11 保証レベルTF
2022/03/23 保証レベルTF ブレスト5
2022/04/22 電子署名WG2022#01 保証レベルTF
2022/05/23 電子署名WG2022#02 保証レベルTF
2022/06/24 保証レベルレビュー（ブレスト6）
2022/06/27 電子署名WG2022#03 保証レベルTF
※ 2022/07/05 要約版リリース

計6回開催したブレスト会議は毎回2時間以上かけ電子署名の保証レベルについて具体的に内容の検討を行った。

メンバーはそれぞれの立場と知識からコメントをして修正して行く作業を行った。

毎月開催の電子署名WG時15～40分程度の簡単な報告と場合によっては検討を行った。

※ 2023年度はWord形式の「電子署名保証レベルガイドブック(仮)」の発行を計画中。

保証レベルTFメンバー（五十音順）

電子署名保証レベル要約版 https://www.jnsa.org/result/e-signature/2022/index.html

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）

今後の動き（業界動向）

電子署名保証レベルで現在の各種
電子署名は分類比較できるように
なりましたが、まだまだ色々な動きが…

時代は変わる…過去・現在・未来

第２期なう。時代は変わっても第１期に
作られた仕様標準は使われている。
しかしこれからの新時代（第３期）では
少し様相が変わって来ている…？
今日はその辺りのお話をします。

JNSA 電子署名保証レベル要約版で整理
https://www.jnsa.org/result/e-signature/2022/

電子署名基本
の標準仕様

電子署名 第１期（基礎）

電子署名＝**ローカル署名＋PKI**
長期保管可能なAdESフォーマット
ローカルに署名鍵を所有し利用する
等の仕様標準化が進む

EU電子署名指令
eSignature Directive

電子署名応用と
ID連携の標準仕様

電子署名 第２期（ID連携）

クラウドを利用した署名サービス
PKI：ローカル署名からリモート署名へ
ID認証技術標準の取り込みが進む
クラウドで署名鍵を管理して利用する

欧州 eIDAS 1.0
Regulation

新しいIDと電子署名の標準仕様
※仕様策定が現在進行中

電子署名 第３期（ID融合）

DIW：デジタルIDウォレットの登場
スマホで署名鍵を管理して利用する
属性も自分で管理して利用する（VC）
新しいトラスト構造（DID等）もある

欧州 eIDAS 2.0
Regulation

署名鍵の所有管理
の方法が変わるよ。

DIWとVCをめぐる世の中の動向

欧州：EUDIW（EU Digital Identity Wallet）

- 欧州委員会が推進、eIDAS 2.0の目玉であり ISO 23220 シリーズ他の標準準拠も推進。
- 2023年初頭に実装の実証となるToolkitを公開予定（2022年秋公開から遅延中）。
- Toolkitの実証実験後にEU各国は自国向けにEUDIWの実装をおこなう必要がある。
- 国民ID・電子旅券・mDL・国家資格・学位証明書等、幅広いVCを取り込む予定。

OAuth/OIDCやFIDOとは連携しているがスマホのプラットフォーマー（Apple/Google）の影が薄い気がする…

米国：mDL（モバイル運転免許証/mobile Driver's License）

- **Apple** Wallet に実装。**Google** Wallet でもベータ実装している模様。
- アリゾナ州、コロラド州、アイオワ州、オクラホマ州、ユタ州、ワイオミング州等で開始または予定。
- ISO 18013-5 定義の mdoc データモデルを利用、ISO 23220 シリーズにも準拠。

Microsoft：Microsoft Entra リリース（2022年5月31日）

- Azure AD・CIEM・Verfied ID（VC）等を統合したあらゆるIDを管理するID統合製品。
- Microsoft Entra Verified ID のドキュメント：
  https://learn.microsoft.com/ja-jp/azure/active-directory/verifiable-credentials/
- 現在はDIDとしてブロックチェーンを使わない "did:ion:ロングフォーム" を利用。
  ※ "ion" は本来BitCoinを使ったメソッドでBitCoinはショートフォームにて使われる。

OpenID：OpenID 4(for) Verifiable Credentials

- OpenID4CI・OIDC4VP・SIOPの3つで構成されたOAuth/OpenIDのVC拡張仕様。

W3C: Verifiable Credentials Data Model

Verifiable Credentials はW3Cが標準化したデータモデルにすぎないが、
現在生じている新しい動きは全てVCが関連している。以下の関係図がベースとなる。

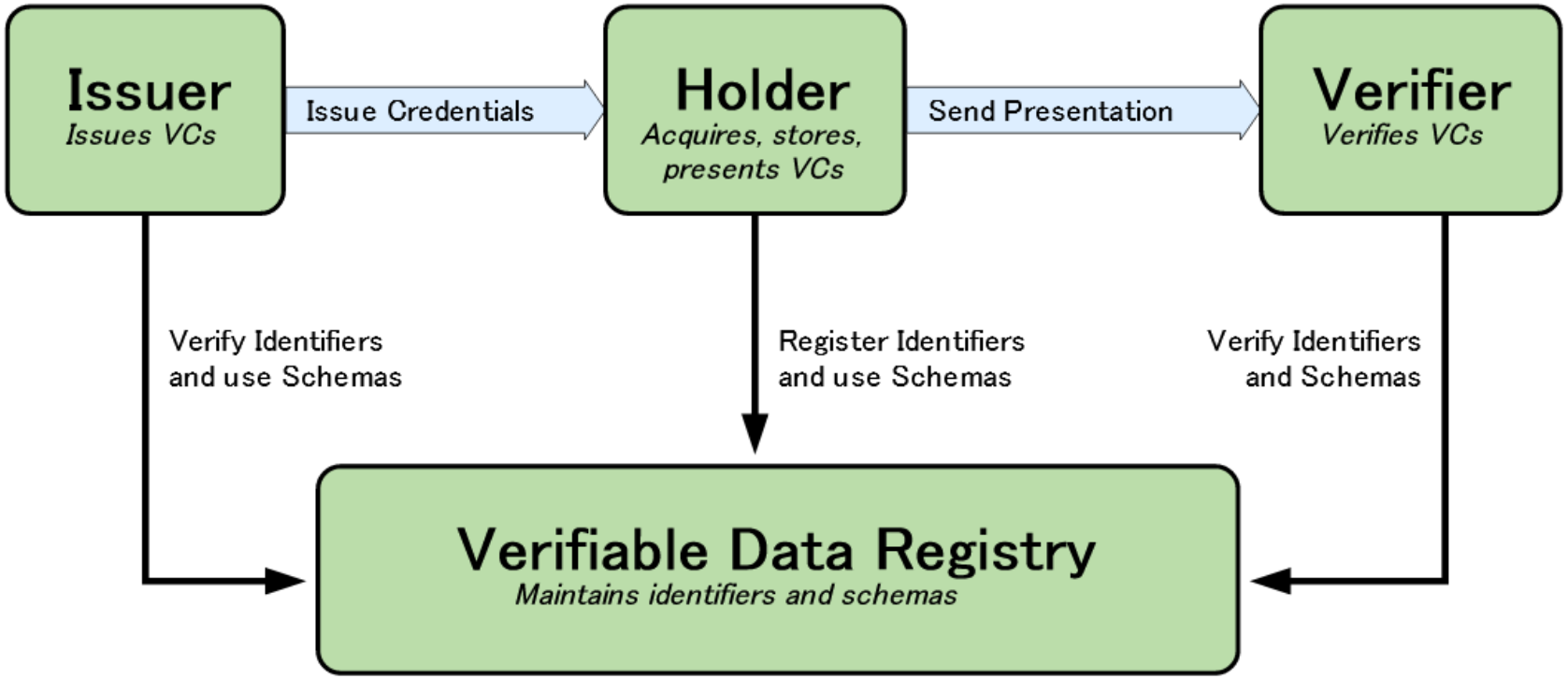


Figure 1 The roles and information flows forming the basis for this specification.

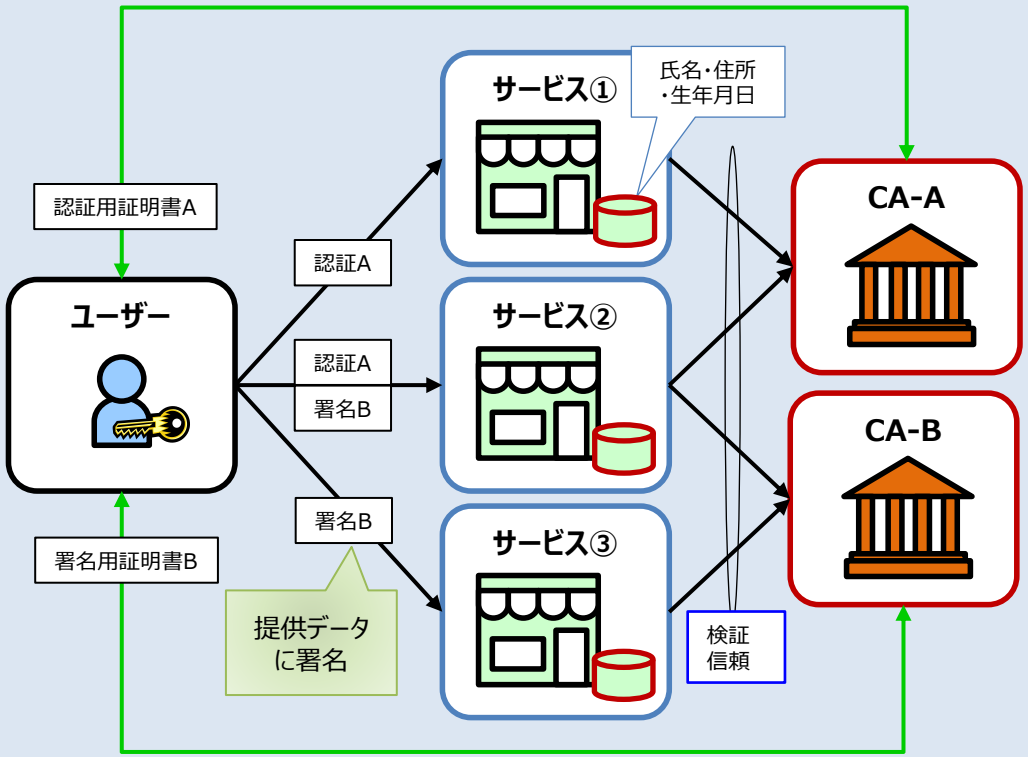
https://www.w3.org/TR/vc-data-model/

DIWにより中央集権から自己主権モデルへ

中央集権的な現在のモデル例

（ローカル署名＋PKIの例）

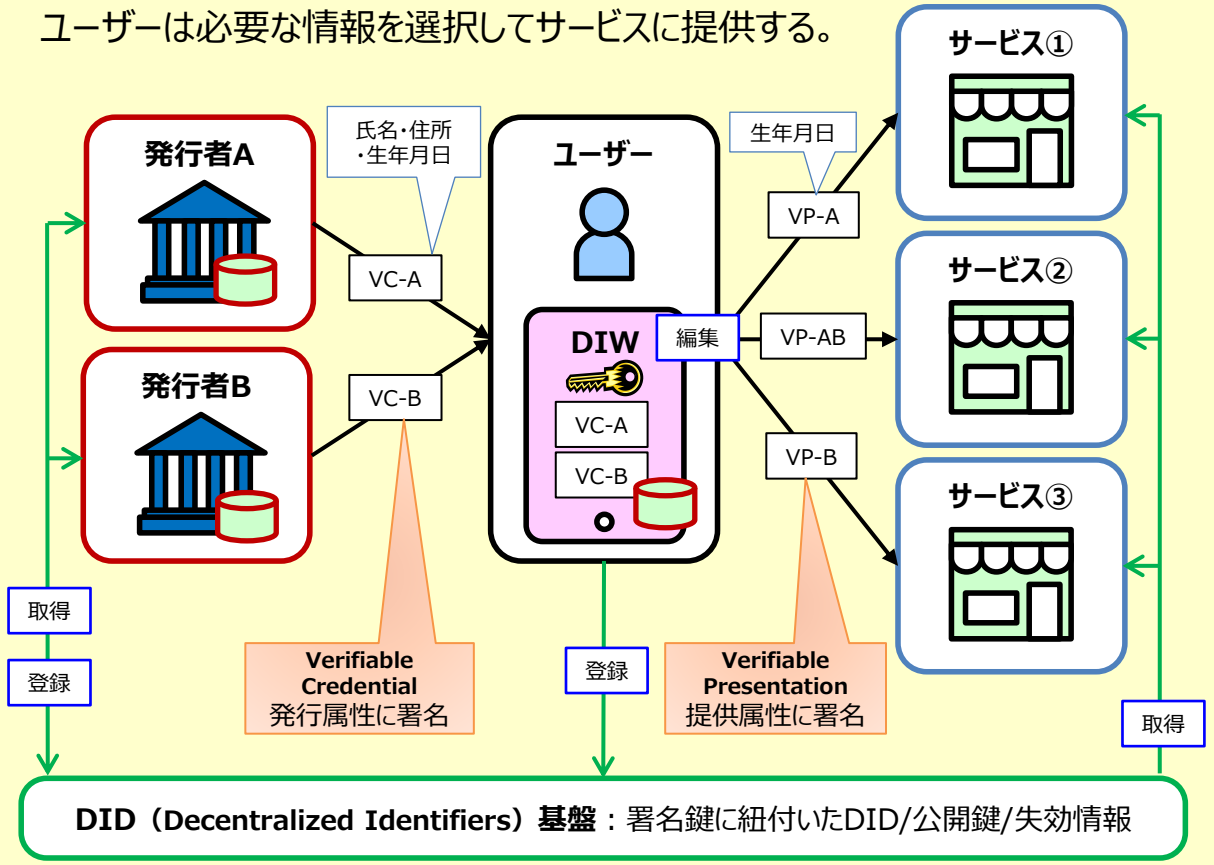
サービスはTSP（認証局等）を直接信頼して接続する。
サービスとTSPの数だけ相互接続されているので複雑。
ユーザーは認証や署名した情報をサービスに提供する。



自己主権型アイデンティティのモデル例

SSI（Self-Sovereign Identity）

ユーザーのDIWを中心としたモデルとなる。
発行者はユーザーの身元確認した上でVCを発行する。
ユーザーは必要な情報を選択してサービスに提供する。



DIWとVCに関連した技術選択肢

コンポーネント	技術標準
ウォレット	EUDIW Toolkit, OpenWallet (Linux Foundation), Apple Wallet, Google Wallet
鍵保護 （署名鍵）	GP-SE (Secure Element), GP-TEE (Trusted Execution Environment), HSM, SIM ※ GP=Global Platform
公開鍵	W3C DID method, X.509 Certificate (PKI), Raw Keys
暗号	RSA, ECDSA, EdDSA, 耐量子暗号
EAAフォーマット （EAA:属性証明書）	オンライン：X.509 Certificate, W3C Verifiable Credentials, ISO/IEC 23220 オフライン：ICAO Doc 9303 (Visa/Passport), ISO 18013-5 (mDL), ISO/IEC 23220
署名フォーマット	AdES (ETSI/ISO 14533), RFC 7515 JWS, SD-JWT (SD=Selective Disclosure)
失効	W3C Status List 2021, X.509 CRL, RFC 6960 OCSP
信頼	EU Trusted List, X.509 PKI Domain, Verifiable Data Registry, OIDC Federation

見たことがある技術も
見たことがない技術も
新旧色々ある。

まだまだカオスな状況が続きそうです。
多くのベンダーも様子見しつつ主流に
なる技術を見極めようとしています。

DIWと電子署名

もう全部DIW/VCの世界に移っちゃえ！

利点：

- 自分の情報は自分で管理できるしサーバー/クラウド側の管理が不要になり実装も楽になる？
- DIW/VCの本来の使い方だしこれからの主流になる？

課題：

- VC発行の仕組み/インフラの構築が必要。サービスも全部再構築。
- まだまだ発展途上の技術で標準化しているところ。

２つの道がある…

予想：おそらく両方が
同時進行するのでは…

DIWを認証器として使いリモート署名すれば良いじゃない！

利点：

- 既存の署名系サービスがそのまま使えるよ！
- リモート署名ならサーバー側で管理できる。中央集権/中央管理が良いよね？

課題：

- VC使わないとDIWの真価が発揮できなくない？世の中は既に動きつつある。
- 新規サービスはVCを使った方が良いんじゃない？

電子署名WG/JT2A 参加者募集中です

電子署名のノウハウを学びながら一緒に活動しませんか？

JT2A 日本トラストテクノロジー協議会
Japan Trust Technology Association

JNSA電子署名WG：2023年度の活動予定

- 保証レベルTF
  - より検討を進めWord形式（仕様書形式）のガイドブック（仮称）を作成予定。
- 署名検証TF
  - 2021年に公開した「デジタル署名検証ガイドライン」をベースにより一般向けの資料を作成して公開予定。
- 標準化TF
  - CAdES/XAdESのJIS仕様更新対応と新たにPAdESのJIS化の検討。

JT2A：2023年度の活動予定

- リモート署名TF
  - 「リモートeシールガイドライン」を作成中。
- API標準化TF（仮称）
  - リモート署名のAPIであるCSC APIの拡張を検討予定。