# JNSA 電子署名WG 保証レベルTF

# 電子署名保証レベル作業提案

LangEdge,Inc.
有限会社 ラング・エッジ

プログラマ/取締役
宮地直人（miyachi@langedge.jp）

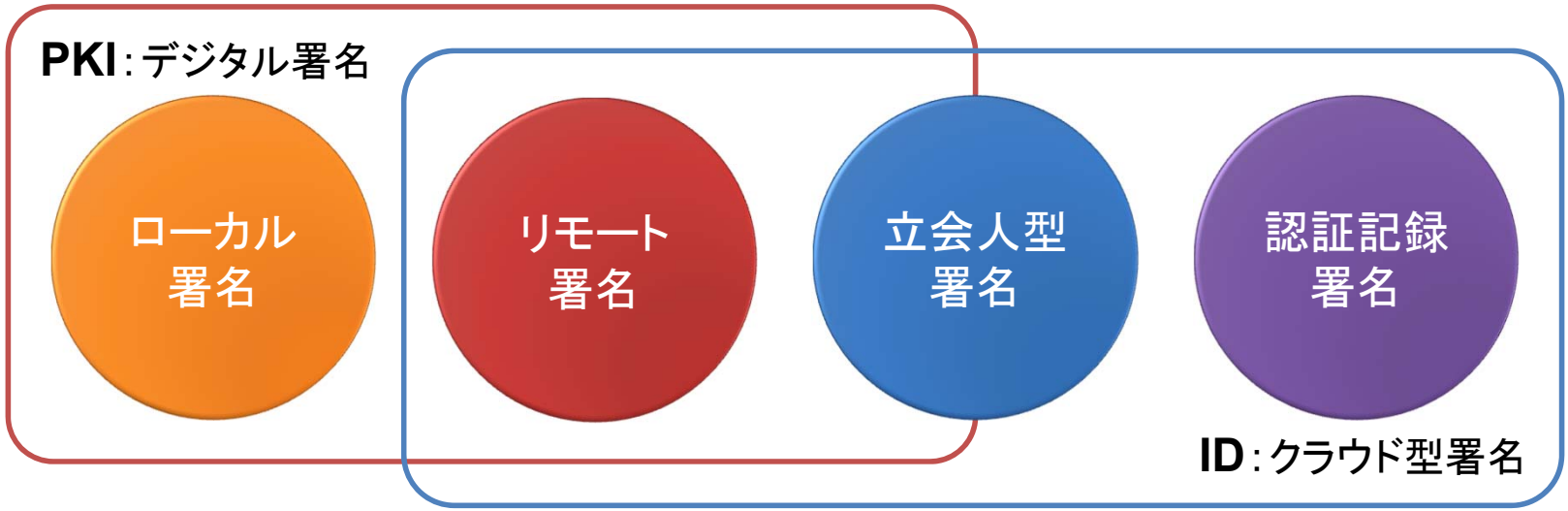
2021年9月29日

# 電子署名市場と保証レベルの必要性

# 日本 多様な電子署名方式（民間）

**従来「 電子署名 ＝ PKI/デジタル（ローカル）署名 」だった。**
**電子署名をクラウド上に置く場合に、ID/認証技術を利用する必要があり、現在は様々な電子署名方式が使われている。**

| 電子署名の種類 | 本人性（否認防止） | 非改ざん性 |
|---|---|---|
| ローカル署名 | PKI/デジタル署名 | PKI/デジタル署名 |
| リモート署名 | PKI/デジタル署名 ＋ ID/認証 | PKI/デジタル署名 |
| 立会人型署名 | ID/認証（立会人が保証） | PKI/デジタル署名 |
| 認証記録型署名 | ID/認証 | サーバ保管等 |



# 日本 電子署名法

**「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ＆A」**を主務三省が公開している。

- **電子署名法第2条関係Q＆A（令和2年7月17日）から抜粋**
  https://www.moj.go.jp/content/001323974.pdf
  - ✓ 電子契約サービスにおける利用者の本人確認の方法やなりすまし等の防御レベルなどは様々であることから、各サービスの利用に当たっては、当該サービスを利用して締結する契約等の性質や、利用者間で必要とする本人確認レベルに応じて、適切なサービスを選択することが適当と考えられる。

- **電子署名法第3条関係Q＆A（令和2年9月4日）から抜粋**
  https://www.moj.go.jp/content/001327658.pdf
  - ✓ 実際の裁判において電子署名法第3条の推定効が認められるためには、電子文書の作成名義人の意思に基づき電子署名が行われていることが必要であるため、電子契約サービスの利用者と電子文書の作成名義人の同一性が確認される（いわゆる利用者の身元確認がなされる）ことが重要な要素になると考えられる。
  - ✓ この点に関し、電子契約サービスにおける利用者の身元確認の有無、水準及び方法やなりすまし等の防御レベルは様々であることから、各サービスの利用に当たっては、当該各サービスを利用して締結する契約等の重要性の程度や金額といった性質や、利用者間で必要とする身元確認レベルに応じて、適切なサービスを慎重に選択することが適当と考えられる。

**解釈**:

基本的考え方として様々なサービスを認めており**立会人型署名**も認めているようだ。
同じ流れから判断して**リモート署名**も認められると考えられる。

# 日本 電子署名の保証レベルの必要性

電子署名法のQ＆Aでは「締結する契約等の重要性の程度や金額といった性質や、利用者間で必要とする身元確認レベルに応じて、適切なサービスを慎重に選択することが適当」と言っているが、選択する為のレベル感は提示されていない。

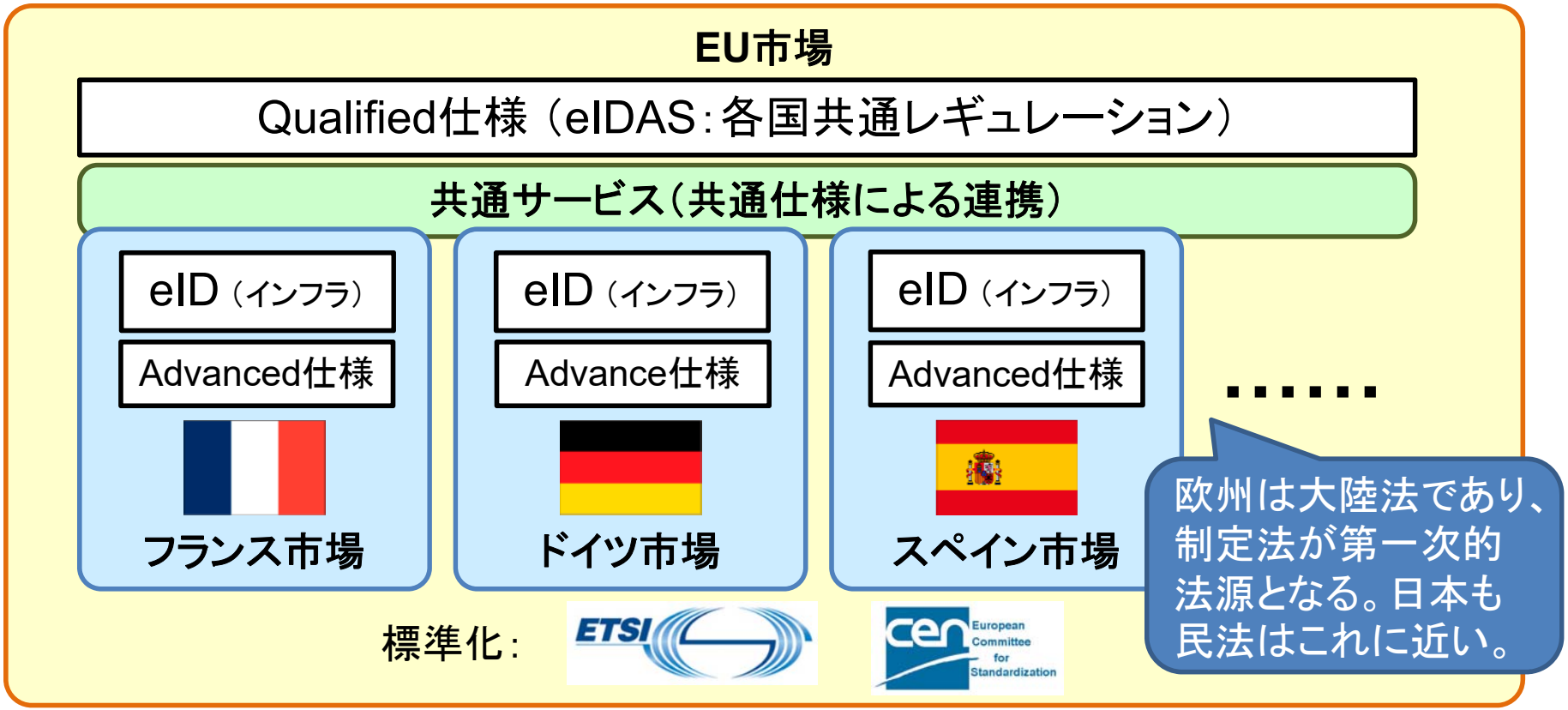
利用者が様々な電子署名サービスから選択するにあたり指標として参考になるような「構成要素毎の保証レベル」が必要となるだろう。

**電子署名保証レベルの目的**:

電子署名サービスを選択する一般の利用者及び法務関係者にとって選択する際の判断材料となる保証レベルを提供する。
その為に以下の2点を整理し策定する。

1. **電子署名の定義**:様々な署名方式に対応した再定義
2. **保証レベル**:電子署名の構成要素を分解しレベルを策定

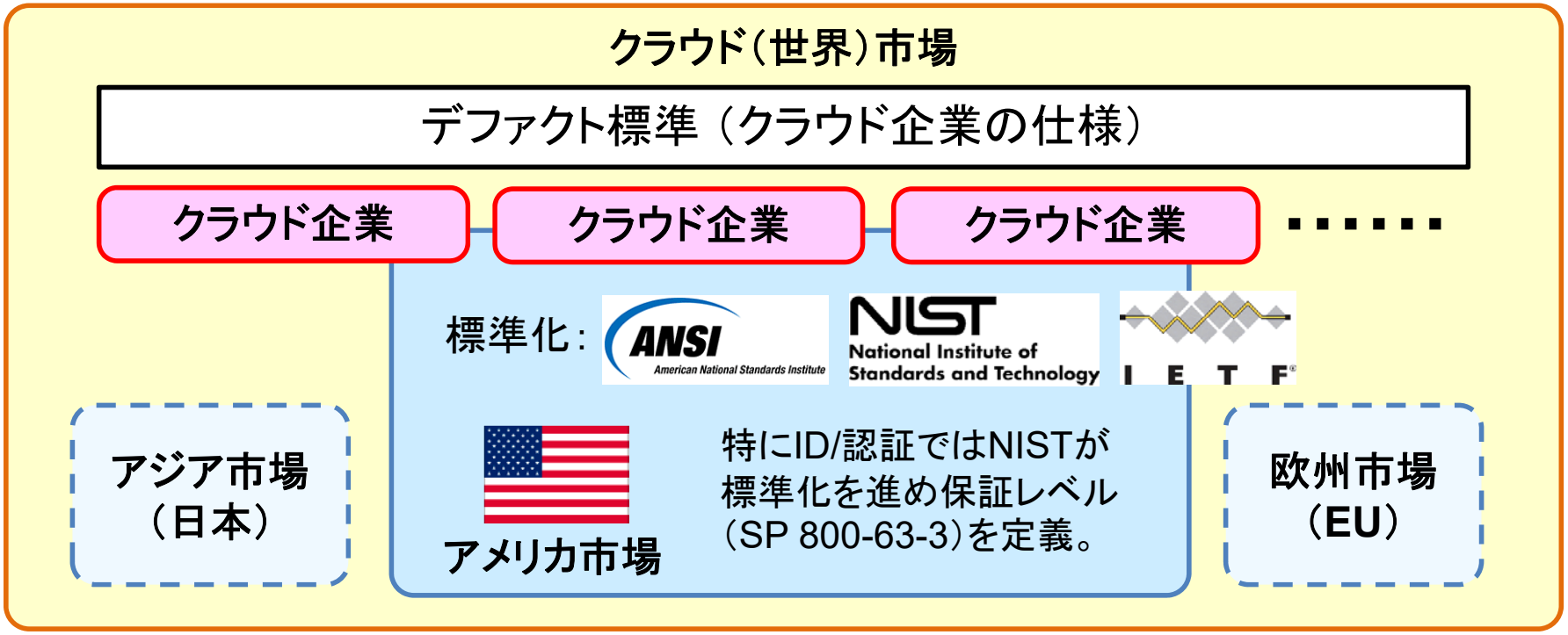
# 参考：欧州 eIDAS規則 レベル




**a. Qualified（適格）**：厳密に守るべき仕様やポリシーが定められている。
**b. Advanced（高度）**：仕様に幅があり各国の電子署名法に合わせられる。
**c. Simple（単純）**：eIDAS仕様外の簡易な電子署名。

- 適格電子署名は手書き署名と同等の法的効力を持つ。
- eID保証レベル：High / Substantial（実質）/ Low

# 参考：米国（世界）クラウド署名




米国の電子署名法ではデジタル署名は必ずしも求められない。

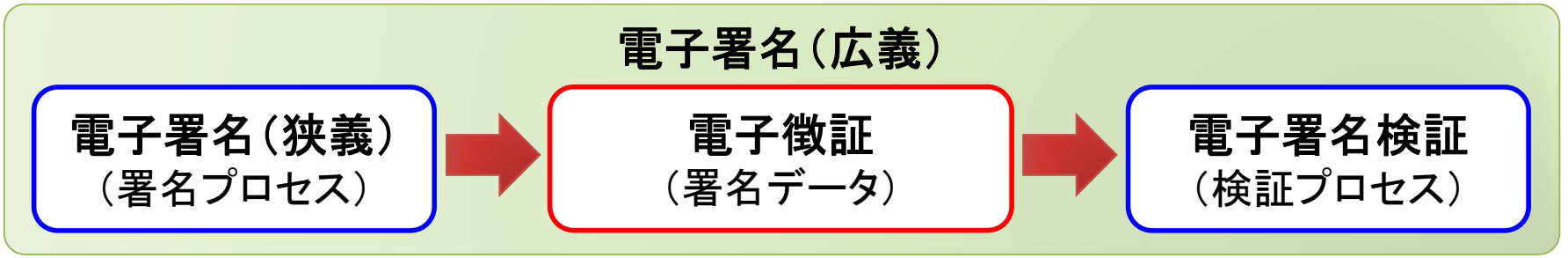
- ✓ 署名する意図が明白でなければならない。
- ✓ 署名は記録と関係していなければならない。
- ✓ はっきりした同意が電子取引するためになければならない。
- ✓ 記録へのアクセスが可能でなければならない。
- ✓ 文書の改ざんがされていないこと。

英米法では、判例が第一次的法源となる。
日本も判例は無視できない。

米国型クラウド署名は「認証記録型電子署名」でも良い。

# 電子署名の定義

# 電子署名の定義：狭義と広義がある




**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。 ※「措置」とは「プロセス」と言える。

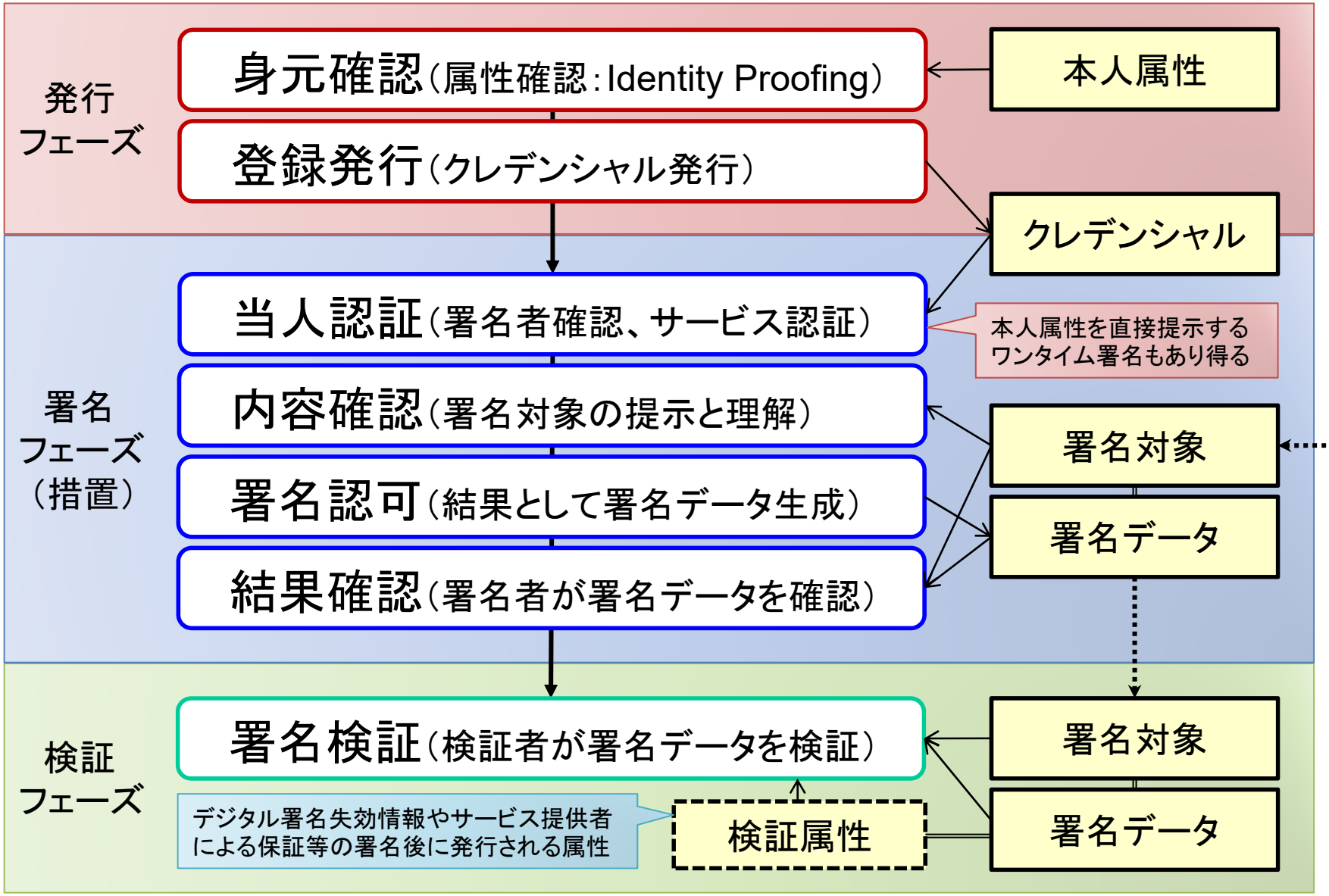
① 当該情報が、**当該措置を行った者の作成**に係るものであることを示すためのものであること（同項第１号）

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）

**広義：署名プロセスで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）のみであるが、署名プロセスで生成された署名データと、署名データを使った検証プロセスの全体を指して電子署名とする。
なお検証結果として**本人性**と**非改ざん**が確認できるか保証される必要がある。

# 電子署名の手順と情報の流れ



# 電子署名の保証レベル（案）

注：保証レベルに関してはまだ提案となります。

# 電子署名保証レベル（eSignAL）案

**eSignAL : eSignature Assurance Level（電子署名保証レベル）**
eSignAL は3つの保証レベル（IAL/SAL(AAL)/PAL）で構成される。

| 略称 | 概要 |
|---|---|
| **IAL** | **Identity Assurance Level（身元確認保証レベル）**<br>**発行フェーズにおける保証レベル**<br>署名者の身元確認を保証するレベルで、NIST SP 800-63-3A そのまま。<br>PKI認証局であればRA（Registration Authority）の行う内容。 |
| **SAL（AAL）** | **Signing Assurance Level（署名プロセス保証レベル）**<br>**署名フェーズにおける保証レベル**<br>署名プロセスにおける署名手順を保証するレベル。<br>**内容に AAL: Authenticator Assurance Level を含む**<br>署名認可時にAALのどのレベルを利用しているかにも依存する。 |
| **PAL** | **Proofability Assurance Level（署名証拠力保証レベル）**<br>**検証フェーズにおける保証レベル**<br>第三者による検証時の署名データの証拠力を保証するレベル。<br>署名対象・署名データ・検証属性（外部）を入力した場合の証拠力の保証。 |

# 電子署名の本人性保証レベル（IAL / AAL）

## ➢ IAL: Identity Proofing（身元確認/本人確認）

身元確認に関しては NIST SP 800-63-3A を使う。

| | |
|---|---|
| **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（対面必須）。 |

## ➢ AAL: Authentication（当人認証/当人確認）

クラウド型のサービスでは NIST SP 800-63-3B を使う。

例：ICカードとPINは、多要素暗号デバイス（所有＋知識）となる。

注：メール到達は特定デバイス所有証明にならないので認証要素にはならない。

※ **ローカル署名**でも、署名鍵と証明書が発行されるクレデンシャルと考えると NIST SP 800-63-3B と同じと言えるのではないか。

| | |
|---|---|
| **AAL.1** | 署名者に紐づいた単要素または2要素による認証。例：パスワード（知識）。 |
| **AAL.2** | 署名者に紐づいた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も可。 |
| **AAL.3** | 署名者に紐づいた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。例：ICカード（所有）とPIN（知識）。 |

「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」もIAL/AALを参照している。
https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_honninkakunin_20190225.pdf

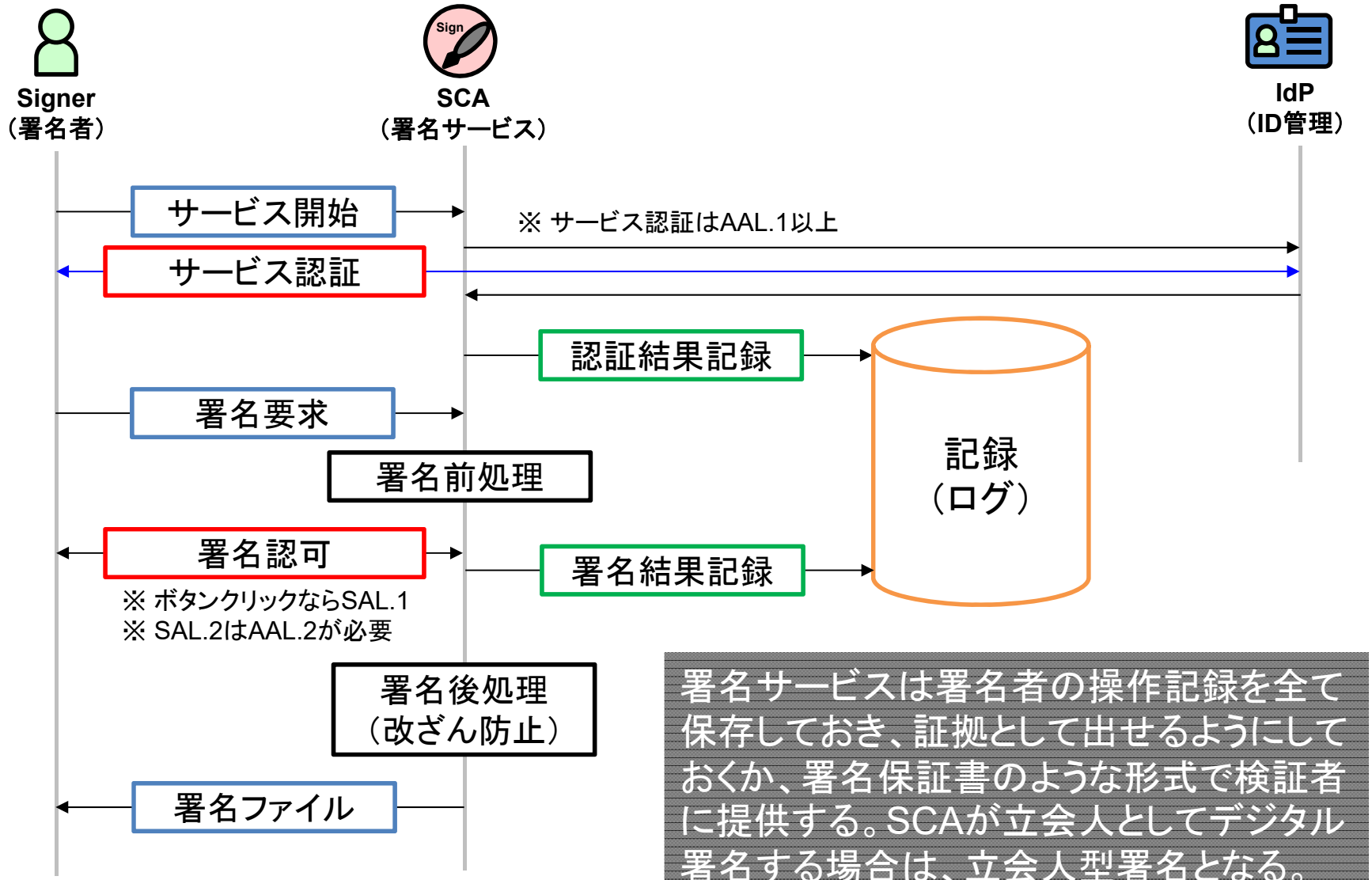
# 署名プロセス保証レベル（SAL: Signing Assurance Level）

## 署名プロセスにおいて認証認可フローを保証するレベル。

| | |
|---|---|
| **SAL.1** | メール記載のランダムなURLクリックにより当人確認を行うか、サービス認証に単要素の認証（AAL.1）を行い、署名認可時にクリック操作等で意志確認を行う。 |
| **SAL.2** | サービス認証（任意AAL）とは別に、署名認可毎にAAL.2の当人認証を行う。 |
| **SAL.3** | サービス認証（任意AAL）とは別に、署名認可毎にAAL.3の当人認証を行う。 |

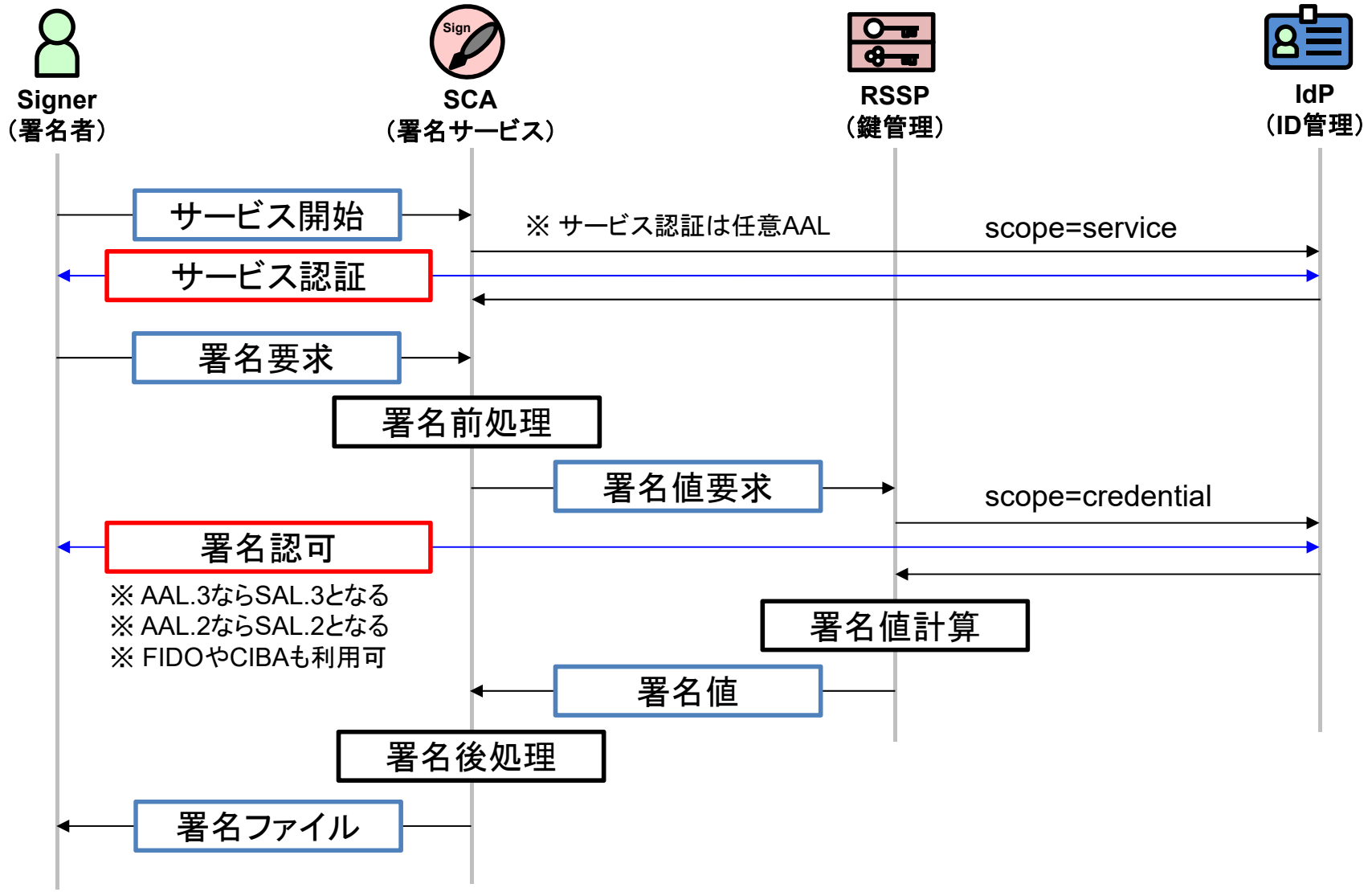
- ✓ 署名プロセスには、**サービス認証**と**署名認可**の2段階があり、主にこれらの**AAL**の組み合わせによりSALが決まる。
- ✓ JT2Aのリモート署名ガイドラインのレベル2以上では、署名毎に2要素認証を必要とするのでSAL.2以上となる。
- ✓ 電子契約の場合は署名者が2人となるが、保証レベルとしては低い方の署名プロセスのレベルとなる。
- ✓ SALが低い場合には、利用が簡易で利便性は増すが、当人確認のレベルは低くなる。

# 署名プロセス：認証記録型署名（SAL.1）




署名サービスは署名者の操作記録を全て保存しておき、証拠として出せるようにしておくか、署名保証書のような形式で検証者に提供する。SCAが立会人としてデジタル署名する場合は、立会人型署名となる。

# 署名プロセス:リモート署名（SAL.3）



# 署名証拠力保証レベル（PAL: Proofability Assurance Level）

## 第三者検証時の署名データの証拠力を保証するレベル。

| | |
|---|---|
| PAL.1 | 本人性と非改ざんについて独自形式だが何らかの情報がある。<br>情報の保証については事業者が間接的に保証する。 |
| PAL.2 | 事前に公開された内容で本人性と非改ざんの情報を提供できる。<br>情報の保証については認定等を受けた事業者が間接的に保証する。 |
| PAL.3 | 事前に公開され標準化された形式（内容）で本人性と非改ざんの情報を提供できる。<br>第三者が公開された検証手順により情報の真正性を確認することができる。<br>署名データの作成についても監査を行い認定された事業者が行っている。 |

- ✓ 署名後に残される署名データによる、本人性と非改ざんの保証の内容と、検証の相互運用性による第三者検証の可能性により証拠力を示す。
- ✓ 署名データ情報の形式が、独自か、公開されているか、標準化され相互運用性を持つか、によりレベルが決まる。
- ✓ 事業者の保証についても、運用について監査を行い認定されていることも高いレベルで要求される。

# 署名証拠力：検証と保証の違い

**検証：**

署名データと補助属性情報により**第三者が確認できる**方式。

例＞ デジタル署名は署名値・証明書・失効情報を認証局を信頼点として標準化された手順で本人性と非改ざんの確認が可能。証明書で本人性を署名値で非改ざんを保証出来る。現在既に相互運用性の実績がある。

**保証：**

信頼された事業者が**第三者に間違いないことを示す**方式。

例＞ 認証型は身元確認結果・認証ログ・操作ログを事業者を信頼点として保証する。否認された時に事業者には署名内容を信頼する為の根拠となる証拠提出が求められる。事業者の信頼性向上には証拠の仕様公開・監査・認定・相互運用性（標準化）が求められる。

# eSignALによるユースケース毎の保証レベル例

ユースケース1：会議室の予約申請（認証記録型署名）

| IAL（本人性） | SAL（署名プロセス） | PAL（証拠力） |
|---|---|---|
| 1 | 1 | 1 |
| 自己申請 | サービス認証のみ | サーバーログのみ |

ユースケース2：NDA等の電子契約（立会人型署名）

※ 保証レベルは全体に低くアンバランスさもあるが、簡易に利用可能であり利便性は高い。
※ 証拠力（PAL）を2に上げる為には立会人型署名の規格化と標準化が必要。

| IAL（本人性） | SAL（署名プロセス） | PAL（証拠力） |
|---|---|---|
| 1（～2） | 1（相手）/ 2～3（依頼者） | 1 |
| メール到達<br>（事前確認なら2に近いかもしれない） | 依頼者は2要素認証だが<br>相手側はクリックによる認可のみ | 事業者保証<br>（事業者のみ検証可能で独自形式） |

ユースケース3：高金額が関係する電子申請や電子契約（リモート署名）

※ 電子契約であっても相互にリモート署名する場合は同じレベルを維持できる。

| IAL（本人性） | SAL（署名プロセス） | PAL（証拠力） |
|---|---|---|
| 3 | 2～3 | 3 |
| 対面確認<br>（マイナンバーカード） | 署名毎に2要素認証<br>（ハードとしてICカード等を利用） | デジタル署名＋PKI<br>（標準化され第三者ツールで検証可能） |

# 電子署名サービスにおけるオプション選択

- ✓ 電子署名サービスにはオプションにより提供機能が異なる場合がある。**オプション選択**により eSignAL の **IAL/SAL/PAL の各レベルが異なる場合がある。**
- ✓ 例えば「当人認証」の手段としてAALのレベルを選択できるケースがある。当然レベルを低くすると利便性は増すが、全体の信頼性のレベルは低下することになる。
- ✓ 電子署名法のQ＆Aで「締結する契約等の重要性の程度や金額といった性質や、利用者間で必要とする身元確認レベルに応じて、適切なサービスを慎重に選択することが適当」と言っているが**サービスの選択と共にオプションを確認して必要とするレベルを選択する必要がある。**

# おまけ：電子シール（eシール）の場合

# 電子シールと電子署名の違い

## 1. IAL：証明書が法人･組織向けに発行される。

- ✓ 電子署名法は自然人に対しての証明書のみを前提としている。
- ✓ 本人確認（IAL）では無く電子シールでは法人確認となる。

## 2. SAL：デジタル署名時毎に署名認可を必要としない。

- ✓ 電子シールはサーバーで連続複数の一括デジタル署名が可能。
- ✓ 署名プロセス（SAL）は異なるか必要が無い可能性がある。

## 3. PAL：署名データ形式は同じだが大量の対応が必要。

- ✓ PKI利用の場合には基本的に署名データ形式は同一。他の方式でも基本的に署名データ形式に違いは無いと考えられる。
- ✓ 大量の電子シール発行があるので自動検証が求められる。

➢ eSignAL とは相違点があるので**電子シール保証レベル eSealAL** として別にまとめるべきだろう。今後の宿題。

# Thank you !

ご注意： 電子署名保証レベルの作業提案資料です。
今後保証レベルTF内で検討されて行き、
その結果を反映して更新される予定です。
正式には令和3年度末に公開予定です。