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

SAG-1:2026
署名保証ガイドライン第1.00版
- 解説 -

JNSA **標準化部会 電子署名WG**

2026/06/17

保証レベルTFリーダー（有限会社ラング・エッジ）　宮地

電子署名WG 保証レベルTF について

歴史：

- 2017年 米国で NIST SP 800-63-3 Digital Identity Guidelines がリリースされる。
- 2018年 DS-500 行政手続き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 がリリースされる。本ガイドラインはJT2AとJNSA電子署名WGが関与して策定した。
  ※ DS-500 は改定版である DS-511 が策定されたことで廃止されています。
- 2021年度にJNSA電子署名WGの下に署名保証レベルを検討する保証レベルTFを**発足**。
- 2025年度までの4年間にわたりメンバーでブレストや議論を繰り返して内容を固める。
- 2026年4月8日：SAG-1:2026 署名保証ガイドライン第1.00版 を**公開**。
  https://www.jnsa.org/result/e-signature/2025/

保証レベルTFメンバー：

新井 聡　（NTTビジネスソリューションズ株式会社）
小川 博久　（株式会社三菱総合研究所）
酒巻 一紀　（三菱電機デジタルイノベーション株式会社）
櫻田 仁詩　（デロイト トーマツ サイバー合同会社）
柴田 孝一　（セイコーソリューションズ株式会社）
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）
西山 晃　（日本ネットワークセキュリティ協会 電子署名WG）
濱口 総志　（株式会社Maximax）
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）
森 大輔　（アビームコンサルティング株式会社）

SAG-1:2026 署名保証ガイドライン 目次

JNSA

署名保証ガイドライン

(Signature Assurance Guidelines)

第 1.00 版

(Ver 1.00)

2026 年 3 月 30 日

(2026/3/30)

NPO 法人 日本ネットワークセキュリティ協会

電子署名ワーキンググループ

(JNSA Electronic Signature Working Group)

１章：はじめに（電子署名の定義）
２章：電子署名方式の整理
３章：電子署名の保証レベル（SxAL）
４章：電子署名リスク管理（ESRM）
付属書：その他電子署名関連情報

電子署名（と電子認証）の定義

電子署名の要件（SAG-1:2026）：

署名要件	英語	概要
本人の身元	Identity	署名者が誰であるか識別できること
本人の意思	Approval	署名が署名者本人に帰属すること
非改ざん	Tamper-evidence	署名後に文書が変更されていないこと

電子認証の要件（NIST SP 800-63）：

認証要件	英語	概要
身元確認	Identity Proofing	申請者を一意に識別するとともに、その実在性を確認すること
当人認証	Authentication	申請者の当人性を確認すること
フェデレーション	Federation	身元確認や当人認証を、他者に依拠して実現すること

電子署名法との比較

電子署名法　第二条
この法律において「電子署名」とは、**電磁的記録**（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）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、次の要件のいずれにも該当するものをいう。
一　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。
二　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。

署名要件	SAG-1における署名要件	電子署名法の署名要件
本人の身元	署名者が誰であるか識別できること	**× 電子署名法では定められていない**
本人の意思	署名が署名者本人に帰属すること	**○ 電子署名法 第二条 一項 に該当**
非改ざん	署名後に文書が変更されていないこと	**○ 電子署名法 第二条 二項 に該当**

※ SAG-1において「本人の身元」を加えたのは、実社会における利用においては電子署名に求められる効力は署名者が誰であるかが特定されることが前提となっているからである。NIST SP 800-63 の IAL と同じ。

用語：電子署名とデジタル署名と電子認証

用語	SAG-1における定義
電子署名	電子署名法であるような**法律的または用途的な用語**とする。
デジタル署名	暗号技術を用いた**技術的用語**とする。

- SAG-1において「電子署名」と「デジタル署名」とは区別して利用する。
- PKIを利用したデジタル署名の仕組みは電子署名の実現方式の一種ではあるが、電子署名の要件さえ満たせばPKIやデジタル署名を用いない電子署名の実現方式もあり得る。
- 欧州定義も同様で、長期署名のAdES も元は Advanced Electronic Signature であったが、現在は AdES Digital Signature となっている。

電子認証：SAG-1:2026「付属書 D.1. トラストの設計段階からの組み込み」から抜粋。

電子認証（Electronic Authentication）と言う言葉はアイデンティティ業界では昨今あまり使われなくなったが、NIST SP 800-63においてもPart2まではタイトルが「Electronic Authentication Guideline」であり、Part3から「Digital Identity Guidelines」となった経緯がある。
NIST SP 800-63-3において「Electronic Authentication」の定義は「Digital Authentication」の古い呼び方であり「情報システムに対して電子的に表現されたユーザーの Identity の確からしさを確立するプロセス」とされている。

電子署名と電子認証の整理

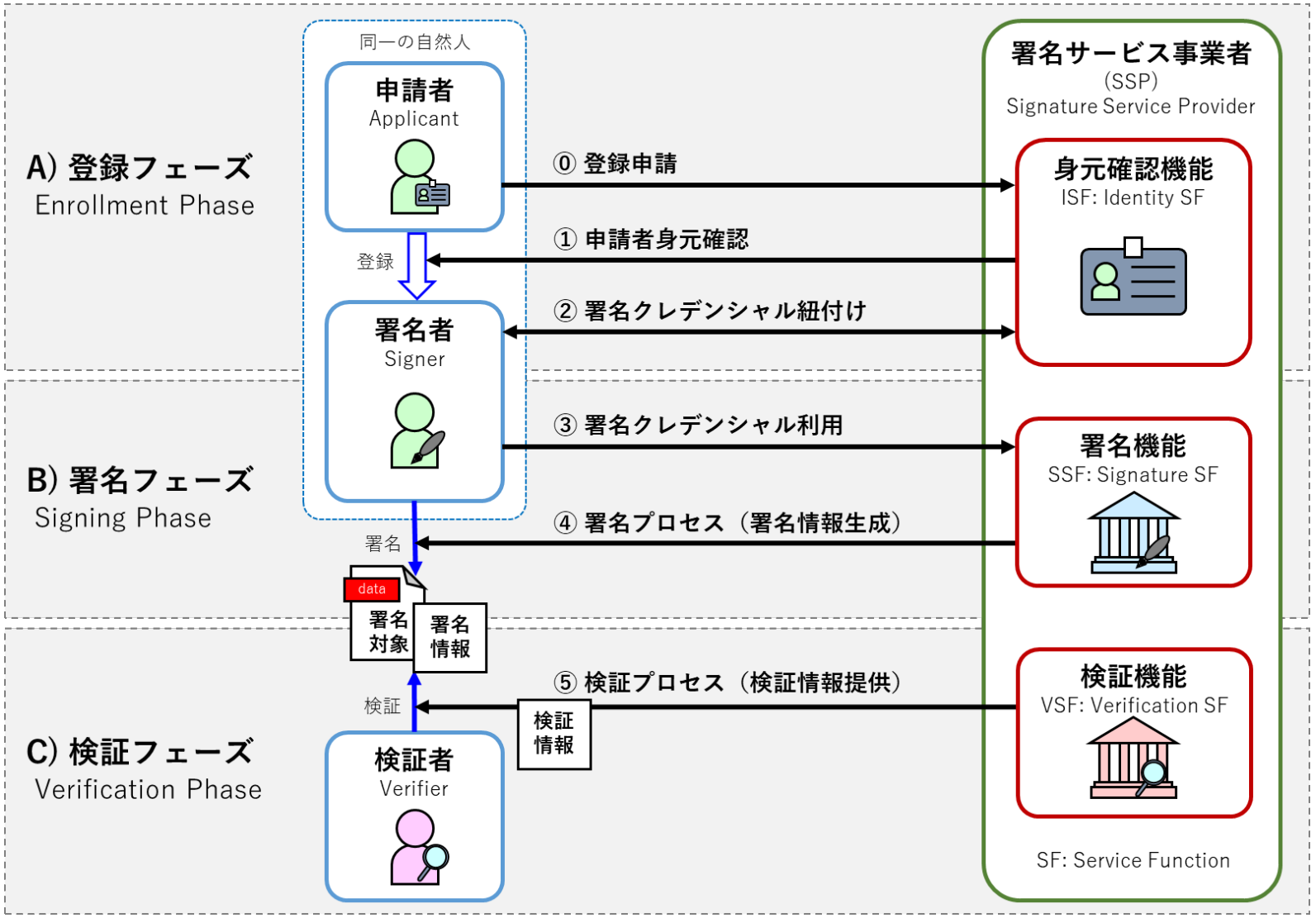
電子署名と電子認証（当人認証）の比較：

機能	時間	対象	目的
電子署名	**過去**から現在（署名時）	電子**データ**の保証	データからの**本人性の保証**
電子認証	現在（**リアルタイム**）	行為（**プロセス**）の保証	オンラインにおける**本人性の保証**

- 電子認証の重要な要件は「リアルタイムの当人認証」である。「今端末の前にいるのは誰だ？」と言うことである。ただこれだけではその時だけとなってしまう。
- このために「当人認証状態の維持（セッションの維持）」も重要だと考えられる。当人認証で確認済みの本人性（当人性）を認証時だけではなくその後も維持する要件である。
- セッション維持により電子認証はプロセスにおける本人性の保証を実現している。
- 電子署名は、電子データから過去におこなわれた署名認証操作の確認により本人性の保証をおこなうことである。
- 電子署名は、電子データの流通自体には影響されず、電子データ自体で確認が可能な仕組みが必要。

１章：はじめに（電子署名の定義）
２章：電子署名方式の整理
３章：電子署名の保証レベル（SxAL）
４章：電子署名リスク管理（ESRM）
付属書：その他電子署名関連情報

電子署名の基本モデル



フェーズ	利用者	サービス・機能
登録時	申請者	身元確認機能
署名時	署名者	署名機能
検証時	検証者	検証機能

SSPが必要とする3つの機能、ISF/SSF/VSFのうち、ISFとVSFは別の事業者となる可能性がある。

- 身元確認(ISF)事業者：ISP
- 検証(VSF)事業者：VSP

署名情報：
署名時に提供される情報。
例：XAdES等の署名ファイル

検証情報：
検証時に提供される情報。
例：CRL・OCSPや認証記録等

署名方式（当人型 と 第三者保証型）

PKI利用署名（当人型）：

- レガシーな **ローカル署名方式** が基本で、その発展型が **リモート署名方式** となる。
- 署名結果の保証を署名者当人の署名鍵/証明書でおこなうので当人型とも呼ばれる。

認証利用署名（第三者保証型）：

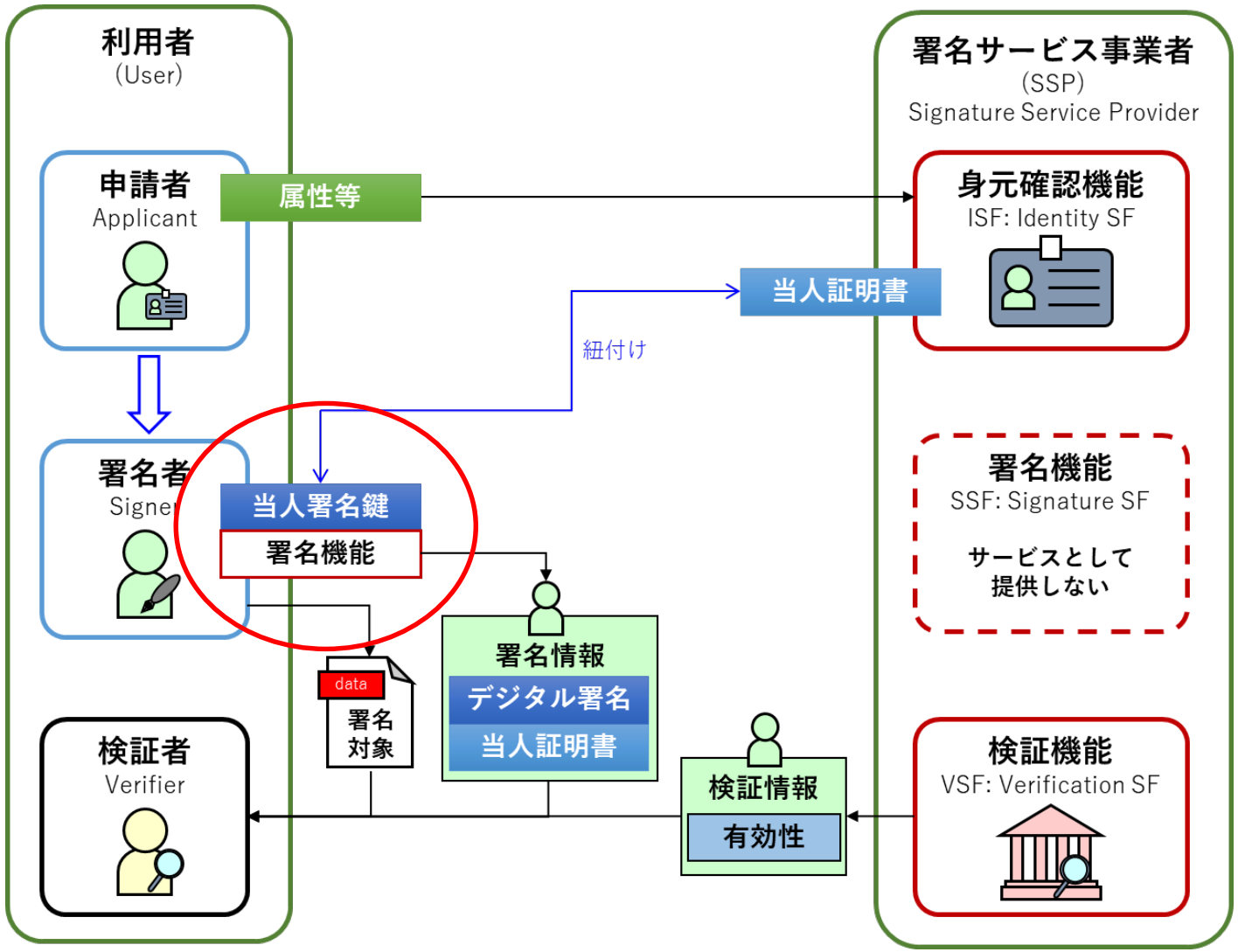
- 基本が **認証記録署名方式** で、その発展型が **事業者署名方式**（立会人型）となる。
- 署名結果の保証を第三者である事業者がおこなうので第三者保証型とも呼ばれる。

※ 上記の主な４署名方式以外の署名方式もあり得るが、SAG-1:2026ではスコープ外としている。

署名方式と署名の3要件：

方式	署名要件１：本人の身元	署名要件２：本人の意思	署名要件３：非改ざん
ローカル署名	**認証局**がおこない証明書発行	**所有する**署名鍵の行使	当人の**デジタル署名**
リモート署名	**認証局**がおこない証明書発行	**当人認証による**署名鍵の行使	当人の**デジタル署名**
認証記録署名	登録時に**事業者**がおこなう	当人認証による**署名操作**	**何らかの保証**（アクセス制御等）
事業者署名	登録時に**事業者**がおこなう	当人認証による**署名操作**	事業者の**デジタル署名**

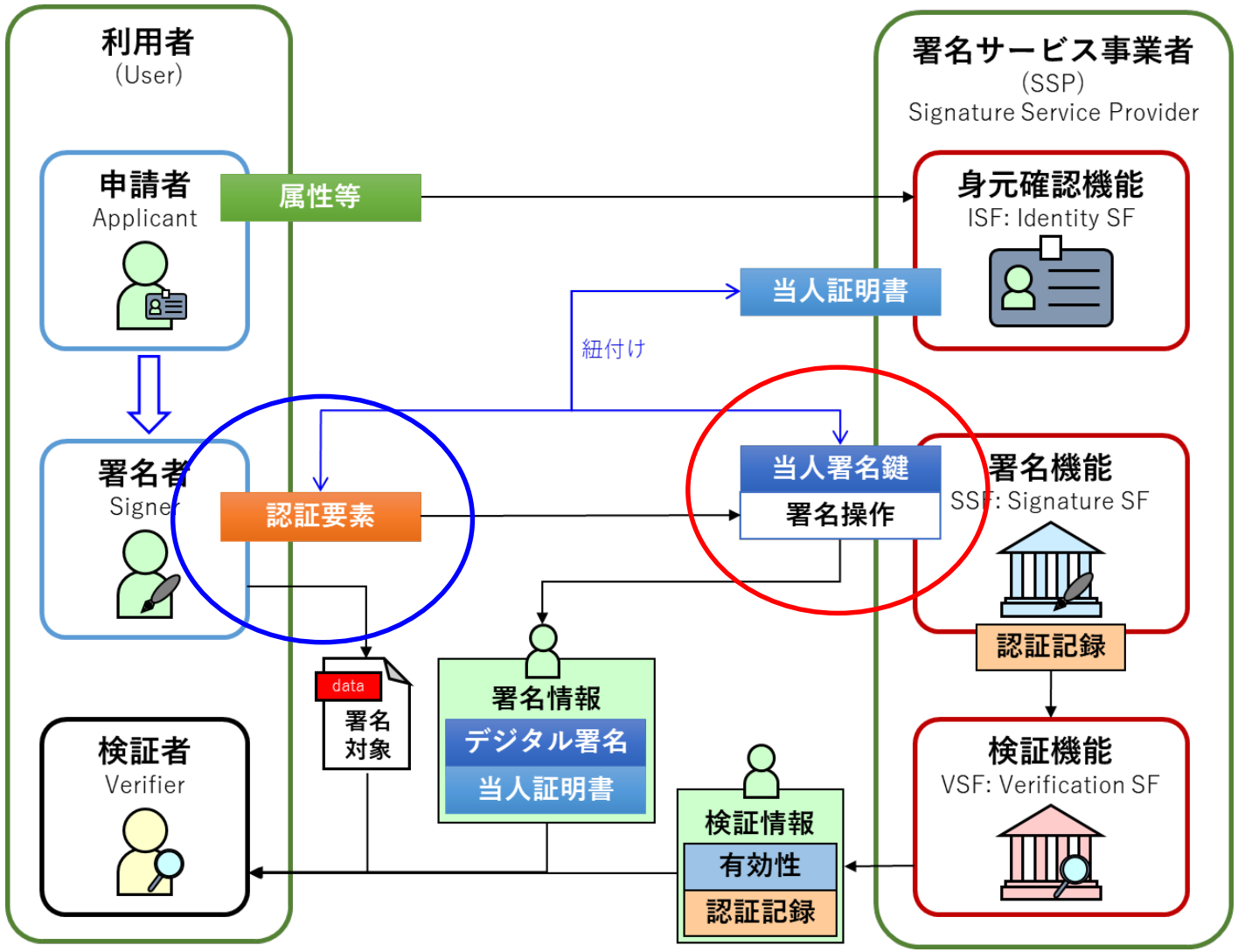
a. ローカル署名方式（当人型）



署名クレデンシャル	ローカル署名
署名鍵	○署名者管理
認証情報	△所有＋PIN等

- 基本となるレガシーな署名方式。
- PKIベースであり認証局が署名サービス事業者と言えるが、署名機能自体は提供していないことが多い。
- 署名機能は署名アプリとして別途取得して利用することが一般的。
  例：Adobe Reader 等
- 署名情報として、デジタル署名と当人証明書を含む標準化された署名フォーマットを利用する。
  例：PAdES/XAdES/JWS等
- 検証情報としては、署名者の有効性を確認するCRLやOCSPが提供される。

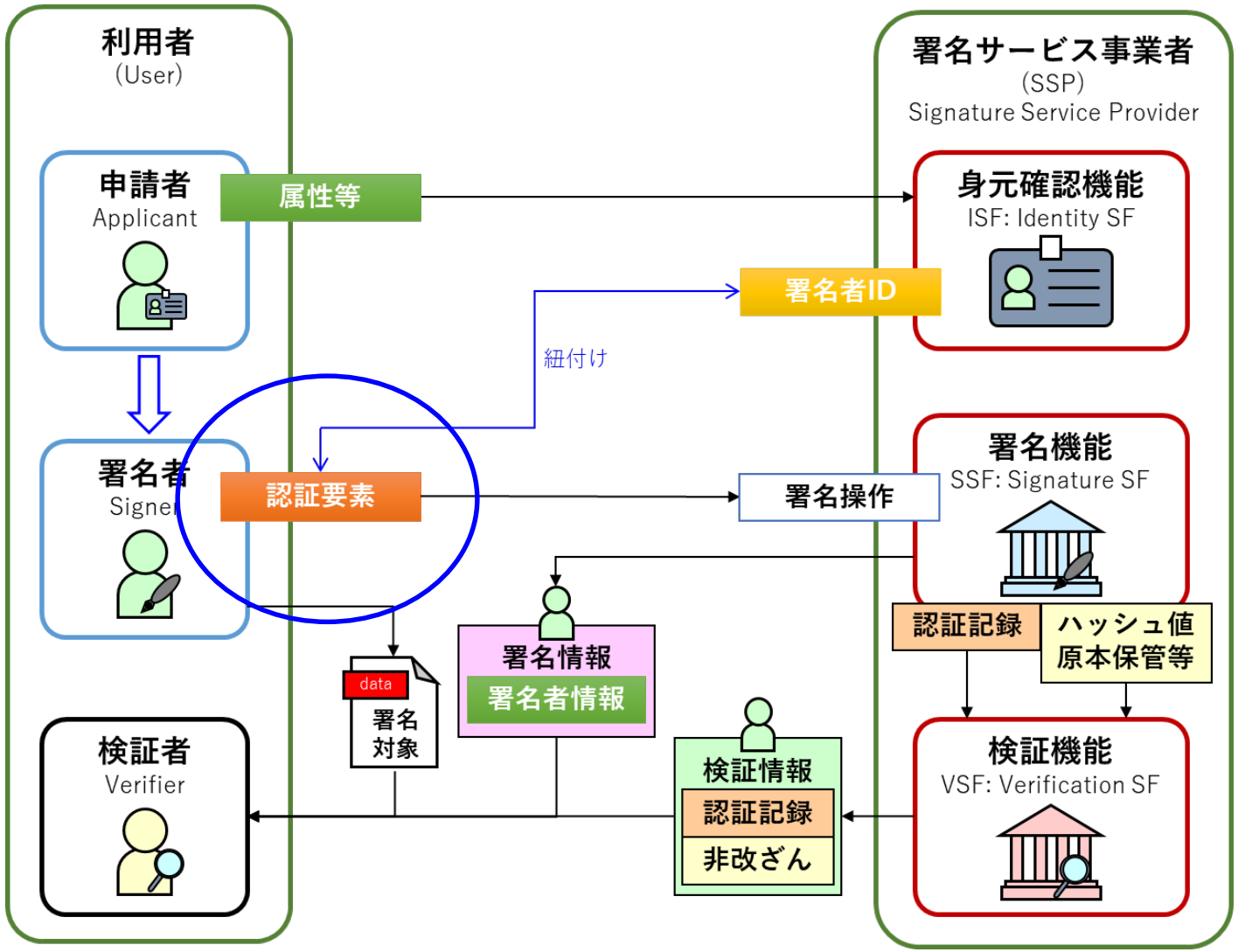
b. リモート署名方式（当人型）



署名クレデンシャル	ローカル署名
署名鍵	○事業者管理
認証情報	○必須（２要素等）

- ローカル署名の署名鍵を事業者に預け当人認証で利用する方式。
- PKIベースであり認証局と署名鍵管理事業者が署名サービス事業者と言える。
- 署名機能は署名鍵管理事業者が署名値のみ提供して、外部の署名アプリと連携する場合もある。
  例：商業登記リモート署名等
- 署名情報は、ローカル署名と同じ。
- 検証情報としては、署名者の有効性を確認するCRLやOCSPが提供されるが、当人認証をおこなっていることから、署名時の認証記録も提供する。

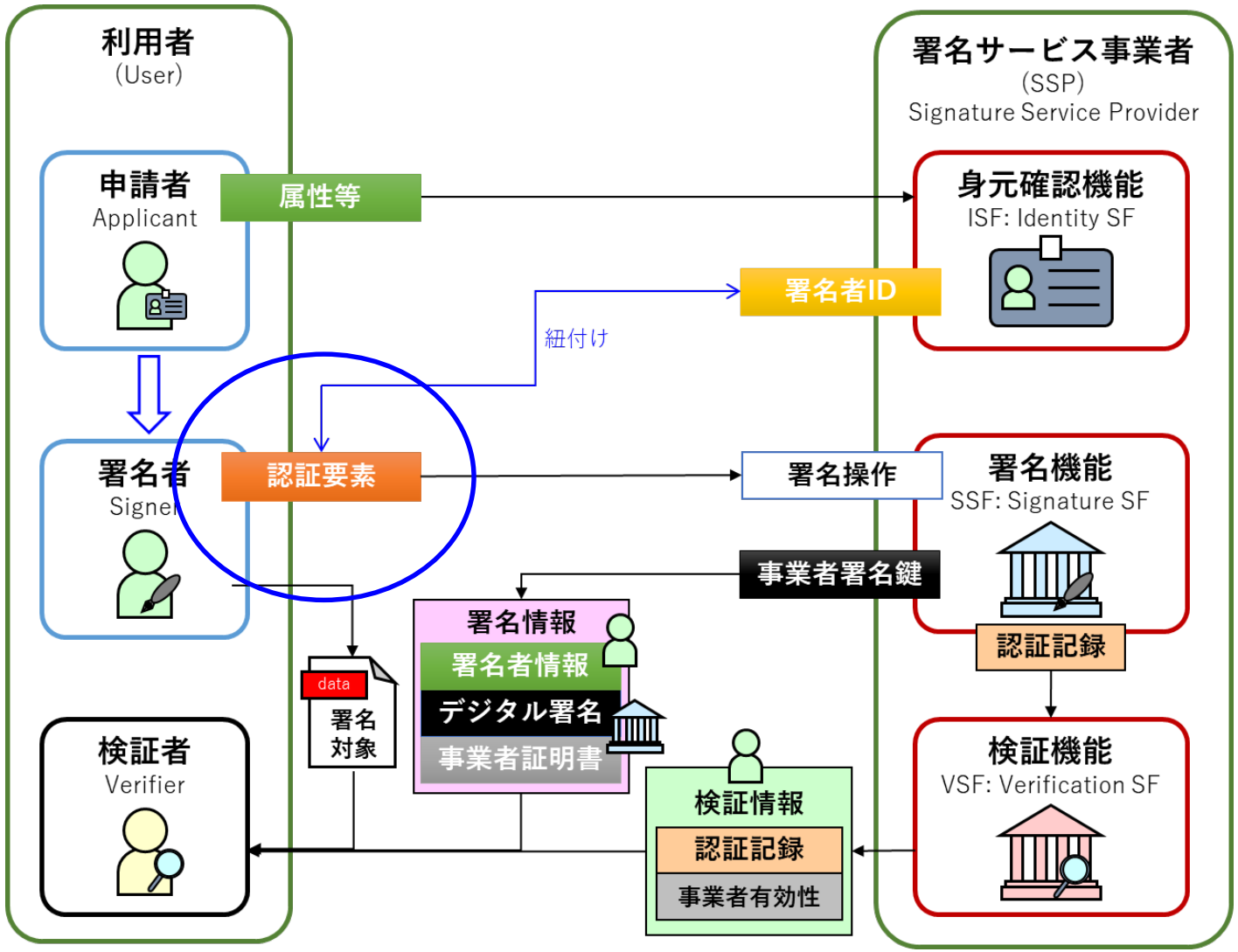
C. 認証記録署名方式（第三者保証型）



署名クレデンシャル	ローカル署名
署名鍵	×使わない
認証情報	○必須（２要素等）

- デジタル署名を利用しない、当人認証ベースの署名方式。
- 署名の保証は署名サービス事業者がおこなうことになる。
- 署名者は署名時に認証要素しか必要としないので利用が容易。
- 署名の意思は当人認証後の署名操作で保証する。
- 署名情報としては署名者情報を返す。
- 検証情報としては認証記録と非改ざんを保証する何らかの情報を提供する。
- ログインして電子申請するようなケースもこの認証記録署名方式の一種と言える。

d. 事業者署名方式（第三者保証型）



署名クレデンシャル	ローカル署名
署名鍵	×使わない（注）
認証情報	○必須（２要素等）

注：事業者署名鍵はあるがそれは署名クレデンシャルではない。

- 認証記録方式とほぼ同じ仕組みだが、署名時に事業者の署名鍵で署名することで、署名者と署名意思を保証する。
- 事業者のデジタル署名をすることで、非改ざんも保証する。
- 署名情報としてデジタル署名が含まれているので当人型の署名方式との区別が難しい。ちゃんと署名者の確認が必要。
- 検証情報としては認証記録型と同じく、認証記録の提供が必要。また事業者の証明書の有効性を保証する情報も必要となる。

１章：はじめに（電子署名の定義）
２章：電子署名方式の整理
３章：電子署名の保証レベル（SxAL）
４章：電子署名リスク管理（ESRM）
付属書：その他電子署名関連情報

4つの署名保証レベル SxAL

署名保証レベルの種類		フェーズ	保証の対象	SP 800-63
SIAL Signer Identity Assurance Level	**署名者身元**保証レベル	**登録**	**アイデンティティ**の保証 身元確認がどのようにおこなわれるかを保証 ➢ 利用する属性の種類や数に依存する。ほとんどIALと同じ。	**IAL** とほぼ同じ
SPAL Signing Process Assurance Level	**署名プロセス**保証レベル	**署名**	**プロセス**の保証 署名がどのようにおこなわれるかを保証 ➢ 署名認可がどのようにおこなわれているか、例えば認証要素数等のレベルに依存する。また対象の確認が必要。	**AAL** とほぼ同じ
SDAL Signature Data Assurance Level	**署名データ**保証レベル	**検証**	**データ**の保証 検証がどのようにおこなえるのかを保証 ➢ 検証結果自体の保証ではなく、データそのものをどのように検証できるかの、検証情報と検証手順のレベルの保証。	（該当無し） FALは少し近いかも…
SOAL Service Operation Assurance Level	**サービス運用**保証レベル	（全体）	**ガバナンス**の保証 運用が適切におこなわれているかを保証 ➢ 運用規定の公開や監査や認定の有無等に依存する。	（該当無し）

- SIAL/SPAL/SDALの３つは署名の各フェーズと対応している。SOALはサービス全体に関係する保証レベルである。
- NIST SP 800-63の３つの保証レベル全体を xAL と呼ぶように、４つの署名保証レベル全体を SxAL と呼ぶ。

保証レベルについて気を付けるべきこと

※ 必要以上の高レベルの保証を求めない。

理由：

- 一般に**高レベル**になるほど**利便性は低下**する。
  - 使われないサービスは存在していないのと同じ。
- レベルにおける**リスクが許容できるかどうか**の判断が重要。
  - リスク評価した上で**適切な保証レベル**を決定する。
- リスクを考慮した**追加策**や**代替策**を準備しても良い。
  - 追加策はより高レベルで代替策は同レベルの予備策。

※ 後述している電子署名リスク管理（ESRM）を参照。

1. 署名者身元保証レベル：SIAL

レベル	概要
SIAL1	**【厳格ではない身元属性の確認】** 公的・信頼できる情報源で属性をチェックし、大量の自動登録や雑ななりすましを主に防ぐ。 ※ **NIST SP 800-63AのIAL1相当**。 ※ 利用可能な身元属性例として銀行口座・クレジットカード等がある。
SIAL2	**【厳格な身元属性の確認】** 申請者が提出した顔写真付きの信頼された身元属性で確認し実在性を確かめること、SIAL1よりも厳格な身元確認を要求する。証拠の偽造・盗難や標的型のなりすまし攻撃にもある程度耐える。 ※ **NIST SP 800-63AのIAL2相当**。 ※ 信頼された身元属性とは主に公的な属性であり、戸籍・住民票(マイナンバーカード)・運転免許・パスポート等がある。
SIAL3	**【SIAL2に加えICチップと訓練済み担当者による確認／より厳格な身元属性の確認】** 申請者が提出したICチップ付きの信頼された身元属性を、訓練された担当者が対面または対面同等のリモート環境にて少なくとも一つの生体情報も取得して確認し実在性を確かめる最も厳格なレベル。高額取引や高リスク操作を想定し、高度な証拠偽造や巧妙な社会工学的攻撃にも耐えることを狙う。 ※ **NIST SP 800-63AのIAL3相当**。

- NIST SP 800-63-4においては、身元確認属性の確からしさのレベルとして、Fair（標準レベル）・Strong（高レベル）・Superior（最高レベル）の３段階がある。Fairは非公的な主に民間ベースの属性（例：銀行口座）であり、Strongは顔写真等がありデジタル暗号的な検証方法を持たない公的な属性であり、Superiorはデジタル暗号的に検証可能な公的な属性となっている。IAL1ではFair以上の属性１つが、IAL2とIAL3ではSuperior属性を1つまたは Fair属性を１つとStrong属性を1つの組み合わせが、必要なっている。更にIAL3では生体認証属性を収集するという要件がある。

2. 署名プロセス保証レベル：SPAL

レベル	概要
SPAL1	**【1要素の当人認証】** 署名時の当人認証を**1要素認証**でおこない、内容を確認して署名付与する。 ※ 署名認可をパスワードのみやメール送信した情報のみを利用する等。 ※ 当人認証の保証レベルは**NIST SP 800-63BのAAL1相当**。
SPAL2	**【2要素の当人認証とFIPSモードの暗号利用が必要】** 当人認証を**2要素認証**でおこないFIPSモードの暗号利用が必要とする。 ※ 当人認証または署名にFIPSモードのPKCS#12ファイルの利用等。 ※ 当人認証の保証レベルは**NIST SP 800-63BのAAL2相当**（注）。
SPAL3	**【SPAL2に加えてフィッシング耐性が必要】** 当人認証を**フィッシング攻撃**にも耐えられる2要素認証でおこなう。 ※ 認証器または署名鍵をICカードに格納して利用時にPIN要求する等。 ※ 当人認証の保証レベルは**NIST SP 800-63BのAAL3相当**。

- NIST SP 800-63-4においては、AAL2に対してフィッシング攻撃にも耐えられる2要素認証をオプション提供する必要がある等の追加要素があるが、SAG-1では大枠を定めるものとし、細かな追加のオプション指定は求めない。
- NIST SP 800-63BのAALと比較して、認証要素自体は同じであるが、署名対象の確認が増えている。
- 言い方を変えると、SPALは署名認可の保証レベルとも言える。

署名クレデンシャル

電子署名では、署名者の当人性を、署名鍵または認証情報を使って確認する。これら2つを合わせてSAG-1では署名クレデンシャルと呼ぶ。

- **署名鍵（Signing Key）**
  - 署名者当人のみ利用可能な（鍵管理された）暗号技術に基づいて署名に用いられるデジタル署名の私有鍵（秘密鍵）。
  - ローカル署名時には署名者が自身で署名鍵を管理して利用する。
  - リモート署名時には事業者に預け管理された署名鍵を当人認証によって利用する。ただし、リモート署名では認証情報も必要となる。
- **認証情報（Authentication Factors）**
  - 署名者当人を認証する為の署名者当人のみ利用可能な情報。
  - 当人の署名鍵を用いない認証記録署名や第三者署名時には認証情報の利用により、署名者の署名意思を確認する。例えば当人認証後の署名ボタンのクリックによる意思確認がある。
  - 認証情報の種類や要素は NIST SP 800-63 において解説され、1要素・2要素・フィッシング耐性等がある。リモート署名では2段階認証も使われることがある。

3. 署名データ保証レベル：SDAL

レベル	概要
SDAL1	**【事業者より提供される検証可能な証拠と時刻（ログ等）】** 事業者から何らかの署名者の本人の意思（承認）と非改ざんに関する、**第三者による検証が可能な**署名データ（属性情報）が提供できること、および**何らかの署名時刻**も提供できること。 ※ 署名者の承認意思（署名手順）に関しては、署名時の認証や操作のログ等でも良い。 ※ 非改ざんに関しては、原本保管とアクセスログやハッシュ値等でも良い。
SDAL2	**【手順に従った第三者による検証可能な証拠と時刻】** 標準化または事前に**定められた検証手順に従う**ことで署名者の本人の意思（承認）と非改ざんの第三者による確認が可能な署名データ（属性情報）が提供できること。および**信頼された署名時刻**が確認可能となること。 ※ 非標準の検証手順の場合には手順の事前公開が必要。 ※ 全電子証拠に事業者自身または信頼された組織によるデジタル署名が必要、例えば認証や操作のログ等。 ※ 非改ざんについてはデジタル署名等の暗号技術の利用が必要であり、アクセスログ等だけでは認められない。
SDAL3	**【SDAL2に加え信頼された第三者組織による保証】** SDAL2に加えて本人性と署名時刻に対して**信頼された第三者組織による保証**があること。 ※ 信頼された第三者組織の保証例として、国または国際的に認定されたPKIベースの認証局やIDプロバイダがある。

- SDALは検証時の署名データ自体の保証であり、署名時刻は検証時に重要な属性となるために保証を求めている。

検証可能な署名データ：Signature Data

- SDALでは第三者により検証可能（**Verifiable**）な証拠の提供を求めている。
- 検証可能とは、**定められた検証手順に従うことで第三者でも署名の有効性を確認できる**ことである。
- デジタル・フォレンジックは、予め定められたデータではなく、後から証拠となる情報を収集して分析することで、有効性を確認する手法である。これは電子署名ではない。
- 検証可能な証拠を提供できることを周知することで、**電子署名は抑止力**として働く。
- PKIベースの**標準化された署名フォーマット**では、デジタル署名と電子証明書を定められた手順で検証することで、署名の**有効性を保証**する仕組みとなっている。
- 電子署名に当人認証を利用する場合の、**当人認証記録の検証可能な証拠**は現時点では**標準化されていない**と言う課題がある。
- 当人認証記録の証拠例として、認証記録署名方式であるDocuSignでは**完了証明書**や**署名履歴**を署名後に提供している。完了証明書は事業者がデジタル署名した**独自フォーマット**のPDFファイルである。
- 最後にSDALは証拠としての保証レベルではない。署名データ自体の証拠力の保証である。

4. サービス運用保証レベル：SOAL

レベル	概要
SOAL1	**【何らかの運用基準の文書化と順守】** 署名サービスが提供している登録・署名・検証等について**運用基準を定めて（文書化して）順守**している。 ※ 最低でも何らかの運用基準を明確化して利用者に提示する必要がある。
SOAL2	**【運用基準の文書化と公開、廃業時の保証】** 署名サービスが提供している登録・署名・検証等について**運用基準を定め、文書として公開等（公開、開示または通知）**した上で順守し、また署名サービスの廃業時に保証が継続できる対応の必要がある。 ※ 認証局保証型のローカル署名方式であれば認証局の**CP/CPS**（RFC 3647準拠）の公開。 ※ 他の署名方式ではローカル署名と同等の運用規定の公開となるが、最低でもISO/IEC 20000や27001の認証取得に加え、署名プロセスに関する独自の運用規定の公開が必要。
SOAL3	**【SOAL2に加え標準化された運用基準と第三者による保証】** SOAL2に加えて、**標準化された運用基準の公開等**をおこない、**信頼された第三者組織の認定や監査**を受けている。 ※ 認証局保証型のローカル署名方式であれば電子署名法またはWebTrust等の認定と監査、他の署名方式ではローカル署名方式と同等の認定と監査。 ※ 信頼された第三者組織の例として国または国際的に認定された認証局やIDプロバイダがある。

- 事業者が何かを保証している場合には、事業者の廃業時の保証が重要となる。PKIにおいても過去に認証局が廃業をした例がある。第三者保証型では特にこの点は重要となる。

情報の公開・開示・通知

- ✓ SOAL2以上では、署名サービスが提供している登録・署名・検証等について運用基準を定め、文書として公開等（公開、開示または通知）を求めている。
- ✓ PKIベースのローカル署名においては、CP/CPS（証明書ポリシー／認証運用規程でありRFC 3647準拠）を公開することが求められている。これと同等のことを求めている。

種類	意味
公開	誰でもが取得できるようになっていること。 例：誰もがアクセス可能なWebサイト等において情報を公開する。
開示	関係者はもちろん関係者以外に対しても求められれば提供すること（受動的）。 例：開示情報の取得方法をWebサイト等で公開する。
通知	関係者に対して能動的に提供すること。 例：利用者に対して登録手続き中に情報を提供する。

１章：はじめに（電子署名の定義）
２章：電子署名方式の整理
３章：電子署名の保証レベル（SxAL）
４章：電子署名リスク管理（ESRM）
付属書：その他電子署名関連情報

DIRM と ESRM

DIRM : Digital Identity Risk Management

- ✓ NIST SP 800-63 に記載されているデジタルアイデンティティのリスク管理の手法。
- ✓ Normative（米国政府のシステムではDIRMを実施する必要がある）
- ✓ 結構難解でありまともに実施するのはコストがかかりそうに感じている。
- ✓ DS-511ではメインテーマとしてはスコープ外。

ESRM : Electronic Signature Risk Management

- ✓ SAG-1:2026 に記載されている電子署名のリスク管理の手法。
- ✓ Informative（参考のために記載されている）
- ✓ DIRMを参考にせず独自にできるだけ分かりやすく整理した。

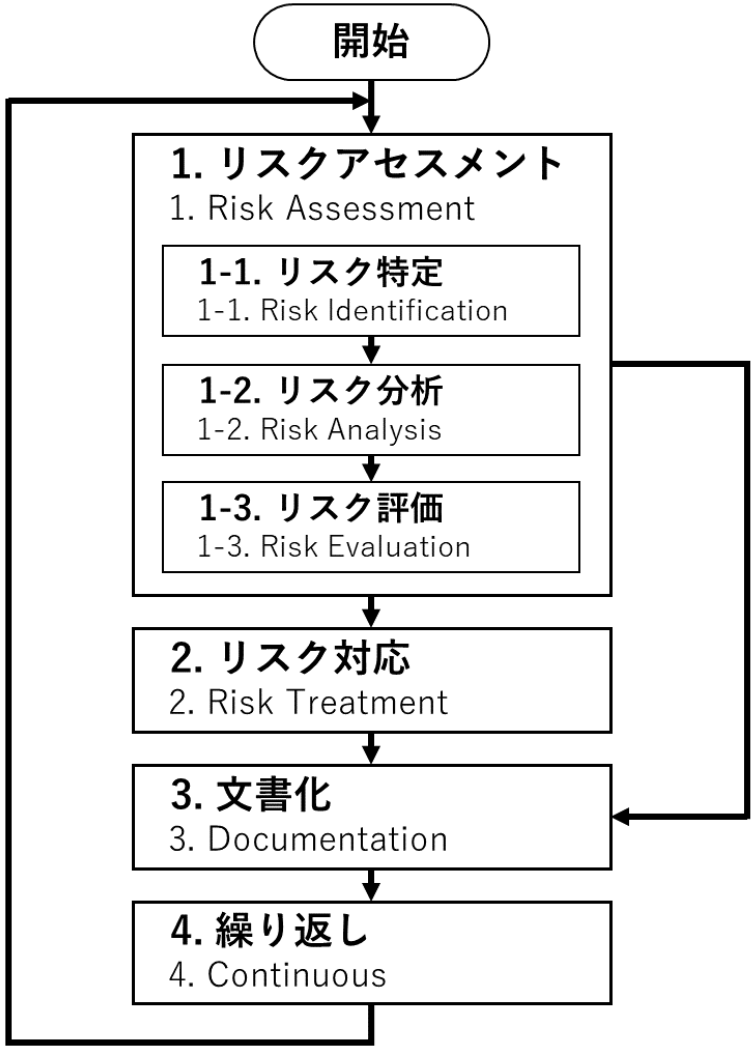
課題：リスク管理をおこなうことは、コスト面やスケジュール面で一般的には難しい。
提案：全体のリスク管理は難しくとも、個々のリスクに対してリスク管理的アプローチは有効。

リスク管理的アプローチ：
　顕在化したリスクに対して、分析と評価をおこない対応して最後に文書化して記録を残す。

ISO 31000 ベースの一般的なリスク管理手順

リスク管理
Risk Management
(ISO 31000 ベース)

Risk Assessment をリスク評価と呼ぶ場合もあるが本ドキュメントでは Risk Evaluation と区別するために、Risk Assessment をリスクアセスメントと呼び、Risk Evaluation をリスク評価と呼ぶ。



電子署名のリスク管理（ESRM）の手順

- 署名保証レベル SxAL を導入することで、ISO 31000 と比較して、Step0の**初期保証レベル**の仮置きと、Step2の**最終保証レベル決定**が追加されている。

初期保証レベルの仮置き：
対象となる署名サービスが目指す署名保証レベルを選択して仮置く。

最終保証レベル決定：
リスク管理の手順を経て調整された、最終の署名保証レベルを決定する。

リスクアセスメントとリスク対応

手順	目的と内容
リスク特定	目的：想定されるリスクの列挙 成果：電子署名のリスクと想定対策のリスト 出来るだけ多くのステークホルダーによるブレインストーミング等をおこない、現時点で想定される電子署名のリスクを列挙する。
リスク分析	目的：リスクのレベルの把握 成果：リスクリストの各リスクのレベル リスク特定で出てきた各リスクに対して想定している対策を整理した上で、影響度と発生頻度により各リスクのレベルを判定する。
リスク評価	目的：リスク毎の対応要否の判定 成果：対応が必要となるリスクリスト リスク分析の結果を評価して、リスク対応の要否を判定する。 ※ リスクアセスメントはリスク全体の評価でリスク評価とは異なる。
リスク対応	目的：リスク評価結果において対応が必要とされたリスクへの対応 成果：リスクへの対策結果 全てのリスク対応をした結果を用いて調整することで最終署名保証レベルが決定する。

リスク対応策

リスク対応策	説明
回避 Avoid	リスクの原因となる操作や機能の提供自体をやめることで、リスク自体を回避する。
軽減 Mitigate	影響度や発生頻度を下げる新たな対策を取り入れることで、リスクを軽減して受容可能なリスクにする。
移転 Transfer	リスク自体を第三者に契約や保険等で移転することで、リスクを回避する。
受容 Accept	リスクの影響度や発生頻度が許容できる場合には、残留リスクとして受け入れる。

基本策・代替策・追加策

種類	意味
基本策	必須：署名サービスの通常の運用においておこなうべき方策。
代替策	基本策が利用できない場合に事前に準備された代わりに利用する方策。 ※各種制限により基本策が利用できない場合に用いる策。
追加策	一時的にセキュリティ強化するために事前に準備された方策。 ※攻撃等により基本策のみではリスクが高まる時に用いる策。

- 基本策・代替策・追加策はDIRMにもある考え方。
- 代替策は、例えばスマホが使えない利用者のための当人認証の手法を容易するなどがある。
- 追加策は、PKIベースのデジタル署名を使った電子署名の場合には、例えば暗号危殆化時に長期署名の新暗号方式によるアーカイブタイムスタンプ追加もあるだろう。

文書化（SSAS/SSPS）の作成

署名サービス承認規定（SSAS）：必須・非公開

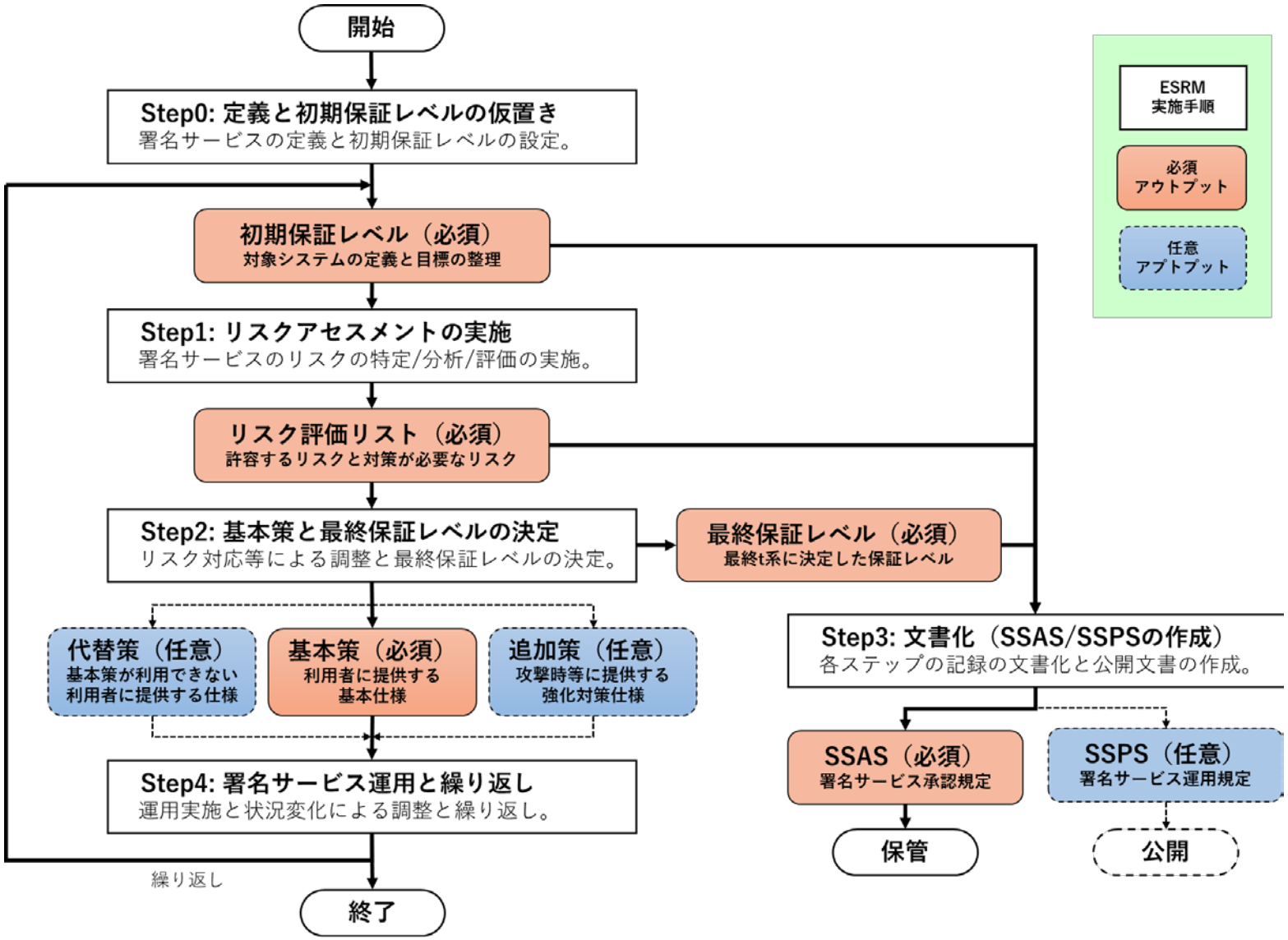
1. SSP自体を整理して記述した文書
2. 初期署名保証レベル（SxAL）選択の結果
3. 調整された署名保証レベル（SxAL）が初期と異なる場合にはその理由
4. 基本策と全ての代替策・追加策と残留リスク
5. その他すべての補足的な事項と利用した文書

署名サービス運用規定（SSPS）：オプション・公開が望ましい

※ ローカル署名の CP/CPS（RFC 3647）に相当する文書で、例えば以下のような項目を記載。

1. 概要（はじめに）
2. 情報公開の責任
3. 身元確認の方法
4. 署名クレデンシャルの運用要件（ライフサイクル）
5. 運用・手続き・人事のセキュリティ管理
6. 技術的なセキュリティ要件
7. 署名クレデンシャルの技術仕様
8. コンプライアンス監査およびその他の評価
9. その他のビジネスおよび法的事項

電子署名のリスク管理（ESRM）とアウトプット



１章：はじめに（電子署名の定義）
２章：電子署名方式の整理
３章：電子署名の保証レベル（SxAL）
４章：電子署名リスク管理（ESRM）
付属書：その他電子署名関連情報

署名保証レベル適合宣言書（規定）

※ 署名サービス事業者が公開する宣言書。

付属書 A. 署名保証レベル適合宣言書（規定）

A.1. 一般

この附属書は，JNSA 署名保証ガイドラインへの供給者適合宣言書の形式を指定する。

A.2. 供給者適合宣言書の様式

署名保証レベルへの供給者適合宣言書
番号:
サービスの名称:
事業者の名称:
事業者の住所:
宣言の対象:
上述の宣言の対象は，次の署名保証レベルの要求事項と適合している。
JNSA 署名保証ガイドライン
実装される要素は，下記の箇条 A.3 の中で明記されるとおりである。
追加情報
（ここに動作確認などの結果が挿入される場合がある。）
代表者又は代理者の署名:
（発行場所及び発行日）
（氏名、名称）

A.3. 供給者適合宣言書への別紙の様式

A.3.1. 一般

供給者適合宣言書の別紙には，A.3.2～A.3.5 に規定する項目を含めなければならない。

A.3.2. 参照する署名保証ガイドラインのバージョン番号

JNSA SAG-1: 2026

A.3.3. 署名保証レベル（SxAL）の適合性

表 A.1 - 署名保証レベル

保証レベル種類（SxAL）	実装保証レベル	特記事項（条件等）
SIAL: 署名者身元保証レベル		
SPAL: 署名手順保証レベル		
SDAL: 署名データ保証レベル		
SOAL: サービス運用保証レベル		

A.3.4. 条件付き項目の詳細

表 A.2 - 条件付き項目

番号	項目名	説明または参照する仕様の名称等
1		
2		

注記：表 A.1 に、"条件付き"とした項目名に関する説明または参照する仕様の名称を示す。

A.3.5. 留意事項

承認目的署名 と 発行元保証署名（参考情報）

電子署名 と **eシール**（電子シール）の違いは電子証明書の発行先（Subject属性）の違い。

名称	概要と用途
電子署名 **Electronic Signature**	電子証明書の**Subject属性が自然人**のデジタル署名。**電子署名法**の対象。 ※ 承認目的署名に利用されることが多い。
ｅシール（電子シール） **Electronic Seal**	電子証明書の**Subject属性が法人等(非自然人)**のデジタル署名。 ※ 発行元保証署名に利用されることが多い。

承認目的署名 と **発行元保証署名** の違いは目的（用途）の違い。

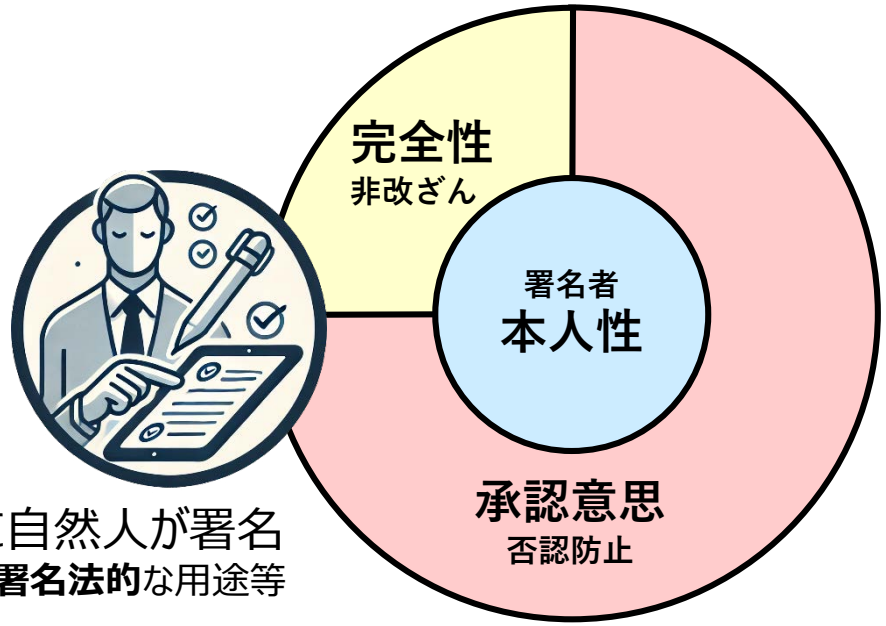
	承認目的署名 Approved Signature	**発行元保証署名 Issuer-Assured Signature**
署名付与主体	主に自然人：主に電子署名用証明書を利用	主に組織（法人や部署等）：主にeシール用証明書を利用
主な目的	署名者による承認意思の保証（否認防止）と非改ざん ※ 主に本人性と承認意思の保証	署名者（発行者）による内容の保証と非改ざん ※ 主に発行元の本人性と完全性の保証
署名付与	事前に定められた手順に従った署名操作の実行が必要	事前に定められたルールに従い自動的に署名しても良い
主な用途例	契約書、申請書、等	領収書、資格証明書、等

※ いわゆる**「eシール的使い方」**と呼ばれる場合が **発効元保証署名**。
※ **承認目的署名** では **署名対象の確認** が必要。また 承認目的署名 が **電子署名法の対象**。

承認目的署名 と 発行元保証署名 のイメージ

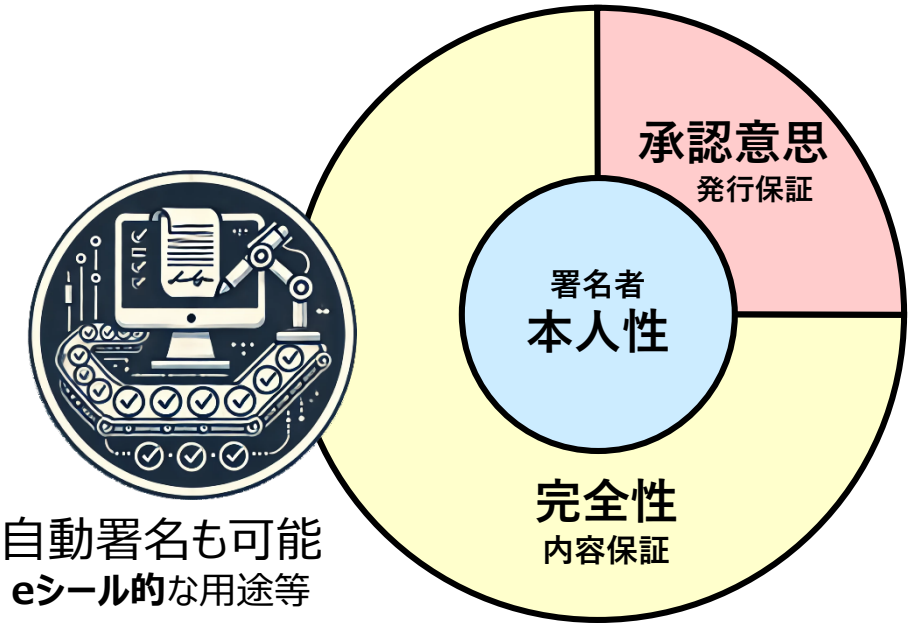
- 承認目的署名と発行元保証署名の関係はどちらか一方ではない。
- どちらの目的も持つケースが多く、**完全性**と**承認意思**のどちらの目的の**比率**が高いかで区別される。

承認目的署名のイメージ



主に自然人が署名
電子署名法的な用途等

発行元保証署名のイメージ



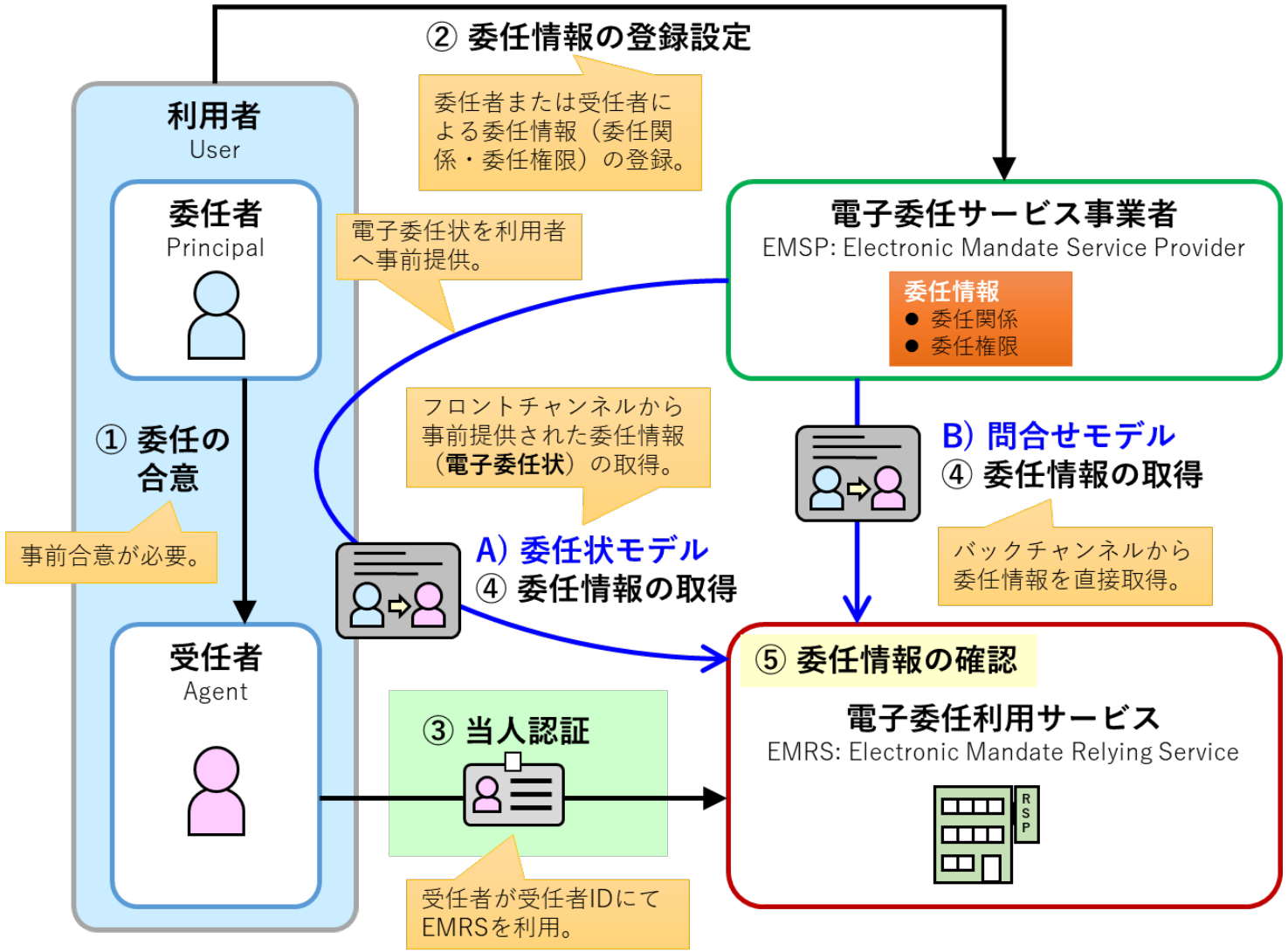
自動署名も可能
eシール的な用途等

電子委任（参考情報）：用語と委任情報

用語	概要
委任	委任者が受任者に対して権利や意思行使等の行為を委任すること。
代理	委任者より委任状や委任契約等により代理権（委任権限）が与えられた代理人（受任者）が、委任者に代わって交渉等においても代理人が自ら判断をおこない意思表示が可能とすること。法的にも定義されている。
代行	委任者より内規等も含めなんらかの委任権限が与えられた代行者（受任者）が、委任者に代わって委任権限の範囲で操作等の行為をおこなうこと。一般には代理と異なり代行者が独自の意思表示はおこなえない委任権限であることが多いが、明確な定義がないことが多い。電子委任では代理と代行の区別は明確ではない。

委任情報	概要
委任関係	**委任者IDと受任者ID**および関連する属性から構成される。電子委任利用サービスにおいて受任者が誰の代理または代行をおこなうかを確認するための情報。身元（委任者・受任者）や資格（受任者）の属性群を含む場合がある。委任状モデルの場合には委任者が受任者IDを含む委任状に電子署名することで委任意思を示すこともある。**受任者が委任者IDを用いる代行は判別不能なためにスコープ外**としている。
委任権限	受任者が行使可能な**権限の範囲を示す情報**。権限の種類により情報も異なるために明確な仕様はないが、電子委任利用サービスが判断可能である必要がある。権限のうち一般的には、代理権は受任者が自ら判断することを許し、代行の場合は受任者が判断をおこなわない範囲となる。

電子委任：委任状モデル と 問合せモデル



	概要
委任状モデル	EMRSは受任者より事前に受任者に提供された委任情報（電子委任状）を取得する。フロントチャンネルによる委任情報の取得モデルであるが、バックチャンネルによる有効性確認等はあり得る。一般には委任情報に委任者またはEMSPによる電子署名等で保護することから**電子署名を主としたモデル**である。
問合せモデル	EMRSは受任者が提示する委任者IDを用いてEMSPに問合せて委任情報を取得する。バックチャンネルによるリアルタイムの委任情報の取得モデルである。委任の認可を確認する**電子認証を主としたモデル**と言える。

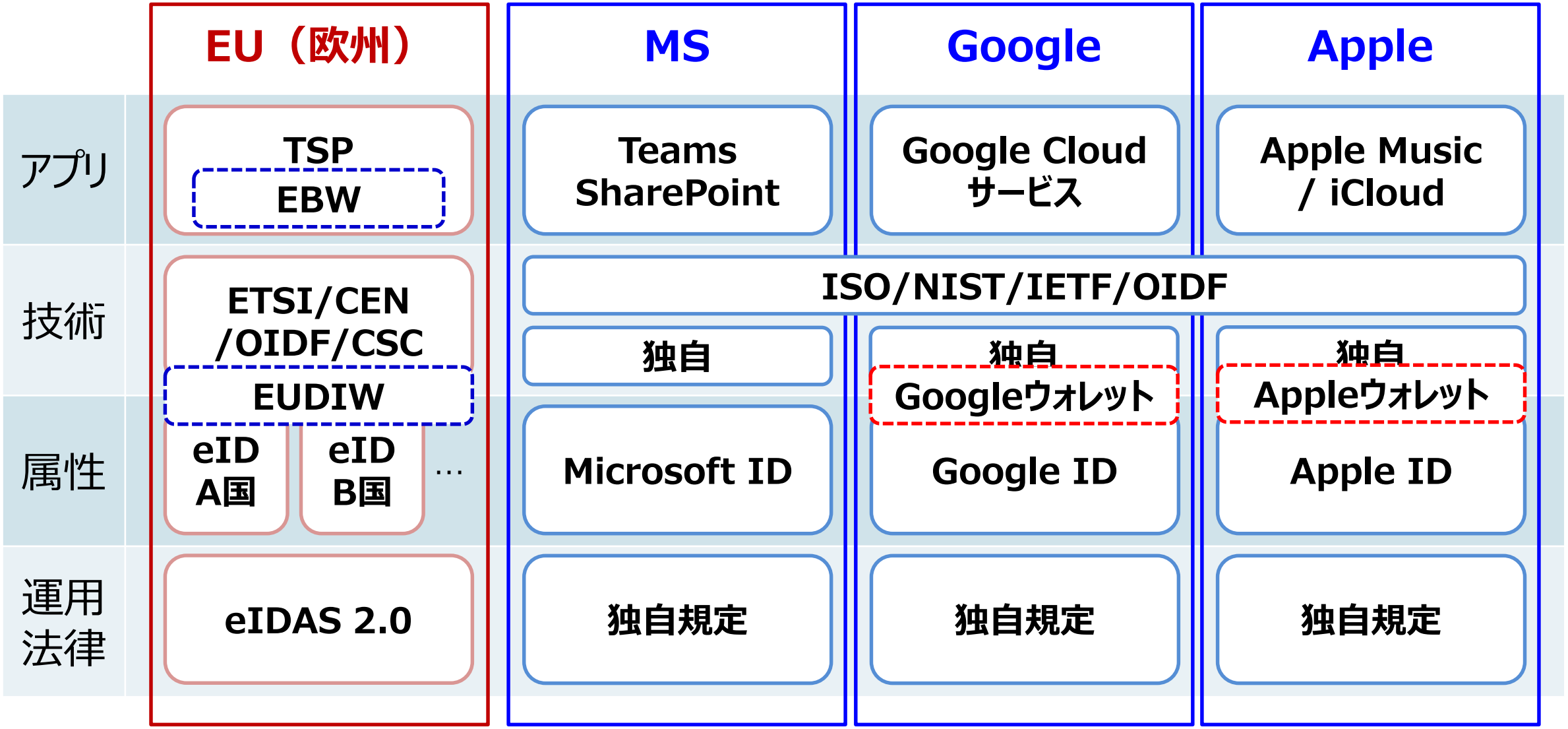
トラスト設計（参考情報）

- SAG-1:2026 の 付属書D. トラスト設計 はまだ**構想段階**で、今年度より詳細にしたい。
- トラスト（信頼）されるシステム設計では、**認証的アプローチ** と **署名的アプローチ** がある。
- **DS-511** と **SAG-1:2026** により、**認証保証レベル** と **署名保証レベル** が揃った。
- また、**プロセス・データ・アイデンティティ・ガバナンス** の、SxAL の構造も使えそう。

技術	**プロセス**（AAL / SPAL） **DS-511 / SAG-1**	**データ**（SDAL） **SAG-1**
属性	**アイデンティティ**（IAL / SIAL） **DS-511 / SAG-1**	
運用 **法律**	**ガバナンス**（SOAL） **SAG-1**	

トラスト設計の要素

トラスト設計の要素と実際の仕組み



認証的アプローチと署名的アプローチ

トラスト利用システムを設計する場合に大きく分けて2つのアプローチ方法があると考える。

認証的アプローチ：

- 利用者を当人認証してプロセスの本人性を保証して操作をおこなう。
- クラウドサービスとの相性が良いので利用が進んでいる。

例：電子委任の問合せモデル。
例：電子申請においてID入力してログインして申請ボタンをクリックする。

署名的アプローチ：

- 利用者の電子署名を確認してデータの本人性を保証して処理をおこなう。
- データのみの流通はリアルタイム性が低いが、アナログ手法に近い処理が可能となる。

例：電子委任の委任状モデル。
例：電子申請において電子署名済みのファイルをアップロードして申請する。

※ 当然ながら両方を利用するハイブリッドなアプローチもあり得る。

リスクに対するリスク管理的アプローチ

トラスト利用のシステム設計時に、顕在化したリスクに対して個別に分析と評価をおこない
対応して最後に文書化して記録を残すアプローチ。
ESRMをシステム全体ではなく、個別のリスクに対して適用する。

- 利用者が求めている保証レベルと、システムが守るべき保証レベルを明確にする。
- そのリスクの発生頻度と影響度からリスクレベルを割り出す。
- 安全性以外に、プライバシー・顧客体験・脅威 の3つの観点からも検討する。
- リスク対応として、回避・軽減・移転・受容 のいずれかが出来ないか検討する。
- 対応方法が決まったら決定までの経緯や理由を文書化して残す。

※ いたずらに最高の安全性を求めないことが重要。
※ 日本開発ベンダーは責任があるので最高の安全性に振りたがる傾向がある。
※ サービサー自身がしっかりと保証レベルを把握して指示する必要がある。

Thank you !

JNSA 電子署名WG　参加者募集中！
https://www.jnsa.org/active/std.html#std-es