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)

目次

概要

本ガイドラインは、電子署名サービスに関する技術的及び運用ポリシーの要件を提供するものである。電子署名サービスを利用する利用者にとっては、電子署名サービスを選択する際の判断基準となるものであり、電子署名サービスを提供する事業者にとっては、電子署名サービスを構築する際の検討資料となるものである。電子署名サービスを提供する事業者は利用者の判断の為に、付属書 A の署名保証レベルに関する適合宣言書を提供することが望まれる。なお、本ガイドラインにおいて 2 章の保証レベルは規定（Normative）であり３章のリスク管理は参考情報（Informative）となっている。

キーワード：
電子署名、デジタル署名、 e シール、PKI（公開鍵基盤)、署名検証、身元確認、当人認証

1. はじめに

かつて電子署名と言えば PKI（公開鍵基盤）ベースのデジタル署名と同義であった。本ガイドラインにおいて「電子署名」を電子署名法であるような法律的または用途的な用語とし、暗号技術を用いた技術的用語である「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。実際に現在では認証技術等を使った多様な電子署名の実現方式も使われており、異なる実現方式間において保証レベルを比較して選択することが利用者に求められている。認証技術に関しては NIST（米国立標準技術研究所）の SP 800-63「Digital Identity Guidelines」において認証技術の要件と保証レベルが整理されており、本ガイドラインにおいても NIST SP 800-63 を参考にすると共に認証技術としての「デジタル ID（Digital Identity)」の要件を利用して説明をおこなう。

経済的な損失や重大な責任等を生じる可能性がある契約や申請等において、電子署名を利用することで、後日その時の内容や意思について確認することが可能となる。しかし電子署名を利用する場合には、署名者の否認や内容の改ざんのような、一定のリスクが存在する。利用者は電子署名のリスクについて判断するために要件の確認が必要となる。本ガイドラインでは、リスク評価をするために必要となる、電子署名サービスが満たすべき要件として「署名者身元」「署名手順」「署名データ」「サービス運用」の保証レベルを設定している。なお一般的に保証レベルが高くなると利便性は低下する傾向があり、必要以上に高い保証レベルを求めるべきではない。本ガイドラインでは、電子署名におけるリスク管理をおこない適切な保証レベルを選択する為の指針を示すものである。

1.1. スコープ

本ガイドラインでは電子署名サービスに求められる項目として、登録時の申請者の身元確認による身元保証、署名時の署名プロセス保証、検証時の署名データ自体の信頼性の保証および運用全体のサービス運用保証の 4 つを主なスコープとする。また参考情報として電子署名のリスク管理についても解説する。

表 1-1　本ガイドラインの対象となる電子署名サービスに求められる 4 つの保証

項目	説明
署名者身元保証 Signer Identity	署名者（自然人または法人・組織）が誰であるかの身元の保証 ※　申請者が提示する属性により身元を確認して署名者とする。
署名プロセス保証 Signing Process	署名者当人により署名手順が正しくおこなわれることの保証 ※　当人認証と署名意思の確認が必要。
署名データ保証 Signature Data	検証者が検証時に利用する署名情報と検証情報の信頼性の保証 ※　署名情報と検証情報を合わせて署名データと呼ぶ。
サービス運用保証 Service Operation	運用者が運用ポリシー等に従い正しく運用している保証 ※　登録・署名・有効性管理等が正しくおこなわれる必要がある。

1.2. 電子署名の定義

本ガイドラインでは、「電子署名」の定義を、署名対象である電子データに証拠としての効力を持たせる事とし、「本人の身元（Identity）」「本人の意思（Approval）」と「非改ざん（Tamper-evidence）」の 3 つの要件を備えるものとする。「非改ざん」については「完全性（Integrity）」と呼ぶ場合もある。電子署名において署名者は自然人を前提としており、組織等の非自然人は電子シール（e シール）となり要件も異なるためにスコープ外とする。電子署名で利用される承認目的署名と、電子シールで利用される発行元保証署名の差異については「付属書 B. 承認目的署名と発行元保証署名（参考情報）」において整理する。

表 1-2　本ガイドラインが定義する電子署名の要件

項目	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（完全性）

日本の電子署名法や欧州の eIDAS 規則（EU 域内における電子署名を含むトラストサービス全般の共通規則）等において、法的には本人の意思（Approval）と非改ざん（Tamper-

evidence）の２つのみが要件となっているが、本ガイドラインでは更に「本人の身元（Identity)」の保証を要求している。要件が多いと言うことは電子署名法や eIDAS 規則等よりも本ガイドラインの方が厳しい仕様となっている。本人の身元（Identity）の要件を追加している理由は、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。また NIST SP 800-63「Digital Identity Guidelines」においても IAL（身元確認保証レベル）が要件として求められている。

1.3. ガイドラインの構成

本ガイドラインでは、第２章においてまず 2.1.章にて用語の定義を示し、2.2.章にて表 1-3 にある代表的な４つの署名方式であり「ローカル署名方式」「リモート署名方式」「認証記録署名方式」「事業者署名方式（立会人型)」について解説する。

表 1-3　本ガイドラインで解説する代表的な４つの署名方式

解説章	概要
2.2.1.章 ローカル署名方式	PKI ベースの署名鍵を署名者自身で管理する署名
2.2.2.章 リモート署名方式	PKI ベースの署名鍵を預け当人認証により署名
2.2.3.章 認証記録署名方式	当人認証と署名操作の記録を保存して署名とする
2.2.4.章 事業者署名方式	当人認証と署名操作を事業者が保証する署名

次に 2.3.章にて表 1-3 にある４つの電子署名の保証レベルである「署名者身元保証レベル：SIAL」「署名プロセス保証レベル：SPAL」「署名データ保証レベル：SDAL」「サービス運用保証レベル：SOAL」を要件と共に解説する。

表 1-4　本ガイドラインで解説する４つの電子署名保証レベル

解説章	概要
2.3.1.章 署名者身元保証レベル：SIAL	署名者の身元確認による本人性の保証
2.3.2.章 署名プロセス保証レベル：SPAL	署名時の当人性と署名意思確認の保証
2.3.3.章 署名データ保証レベル：SDAL	署名データ自体の信頼性に関する保証
2.3.4.章 サービス運用保証レベル：SOAL	運用ポリシー遵守に関する信頼性の保証

※　本ガイドラインでは SIAL/SPAL/SDAL/SOAL を総称して SxAL と呼ぶ。

第３章では、参考情報として電子署名のリスク管理（ESRM）について表 1-5 で示した５つのステップである「定義と初期保証レベルの仮置き」「リスクアセスメント実施」「基本策と最終保証レベルの決定」「文書化（SSAS/SSPS 作成)」「署名サービス運用と再評価」に分けて解説する。

表 1-5　電子署名のリスク管理の 5 ステップ

解説章	概要
3.2.章 ステップ 0：定義と初期保証レベルの仮置き	サービス定義と初期レベル仮置き
3.3.章 ステップ 1：リスクアセスメントの実施	リスクの特定/分析/評価の実施
3.4.章 ステップ 2：基本策と最終保証レベルの決定	基本策と最終保証レベルの決定
3.5.章 ステップ 3：文書化（SSAS/SSPS の作成）	検討記録の保管と運用規定の公開
3.6.章 ステップ 4：署名サービス運用と再評価	運用実施と定期的な再評価

最後に、付属書として「署名保証レベル適合宣言書（規定）」「承認目的署名と発行元保証署名（参考情報）」「電子委任（参考情報）」「トラスト設計（参考情報）」を付けている。

2. 電子署名の方式と保証レベル

現在は様々な署名方式が使われており、異なる署名方式間の保証レベルの比較が困難になっている。本章では、最初に代表的な署名方式の整理をおこない、次に電子署名の保証レベルについて解説する。

2.1. 概要

本ガイドラインでは現在利用されている技術を反映した署名方式を扱う。署名方式の扱う主体（ロール）と要素は以下となる。

利用者（User）

署名サービスを利用するエンティティ（人・組織・システム）であり、申請者が署名サービス事業者に申請して身元確認され署名者になり署名する（署名情報を生成する）ことができる。検証者は署名者とは別の第三者であり提供された署名データを検証して署名者の意思と非改ざんを確認する。署名クレデンシャルは署名サービス事業者から提供して署名者（申請者）と紐づけるケースと、申請者が事前に所有しているクレデンシャルを署名クレデンシャルとして署名者（申請者）と紐付けるケースが考えられる。

- 申請者（Applicant）
  - 申請者は身元確認する為の属性等を提示する必要がある。
  - 署名サービス事業者に申請し身元確認後に署名クレデンシャルを紐付けて署名者となる。
- 署名者（Signer）
  - 身元確認され、当人に紐付く署名クレデンシャルを所有する者を署名者とする。
  - 署名対象を確認し署名クレデンシャルにより当人であることを確認して署名することで署名情報を生成することができる。
- 検証者（Verifier）：
  - 署名データ（署名情報と検証情報）を検証して署名対象と署名者（検証者に開示される署名者のアイデンティティ）への紐付け（意思）と非改ざんを確認する。
  - 通常は署名者ではない第三者の検証者による検証プロセスを想定する。

署名サービス（Signature Service）

利用者に署名サービスを提供する事業者（SSP：Signature Service Provider）であり、機能毎に身元確認サービス機能（ISF）・署名サービス機能（SSF）・検証サービス機能（VSF）の 3 種類がある。1 つの SSP では、最低限 SSF を含み、全てを提供する場合もあるが、

別々に提供される場合もある。例えば PKI を利用したデジタル署名方式であれば、認証局（CA）が ISF（身元確認と発行）と VSF（検証情報の提供）の機能を提供し、SSP は SSF（署名付与）のみをおこなう場合がある。

- 身元確認サービス機能（ISF：Identity Service Function）：署名者身元保証
  - 申請者の身元確認をおこない署名クレデンシャルを紐付けることで署名者とする。
  - ISF は外部の CSP（Credential Service Provider）を利用する場合もある。
- 署名サービス機能（SSF：Signature Service Function）：署名プロセス保証
  - 署名クレデンシャルを持つ署名者へ署名手順を提供し署名情報を生成する。
  - SSP は最低限 SSF を提供する必要がある（ISF/VSF は外部利用が可能）。
- 検証サービス機能（VSF：Verification Service Function）：署名データ保証
  - 検証者に対して署名対象の検証に必要となる検証情報または検証結果を提供する。
  - VSF は外部の VSP（Verification Service Provider）を利用する場合もあるが通常は SSP が提供することが多い。

署名データ（Signature Data）

署名データは、署名対象（署名者が内容を保証する対象となるデータまたはデータ群）と署名者の紐付け（意思）と非改ざんを保証する情報（群）で構成される。署名データには、署名時に生成/提供される署名情報（群）と、検証時に提供される検証情報（群）の 2 種類がある。

- 署名情報（Signature Information）
  - 署名時に SSF が生成/提供する署名対象と署名者の紐付け（意思）と非改ざんを保証する情報群であり、署名対象と共に提供される。
- 検証情報（Verification Information）
  - 検証時に VSF から提供される署名者の有効性情報等の情報群。

署名クレデンシャル（Signature Credential）

署名者は、署名時に署名クレデンシャルの所有証明（PoP：Proof of Possession）により当人であることを保証する。署名クレデンシャルは、当人がデジタル署名をおこなう場合には署名鍵であり、デジタル ID を使った当人認証をおこなう場合には認証情報となる。署名鍵と認証情報は少なくともどちらか一方が必要であるが、当人型リモート署名方式のように両方を紐付けて利用する場合もある。

- 署名鍵（Signing Key）
  - 署名者当人のみ利用可能な（鍵管理された）暗号技術に基づいた署名に用いる鍵

- 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

基本モデルの利用には、図 2-1 で示すように大きく分けて登録フェーズ・署名フェーズ・検証フェーズの 3 つに分けることができる。

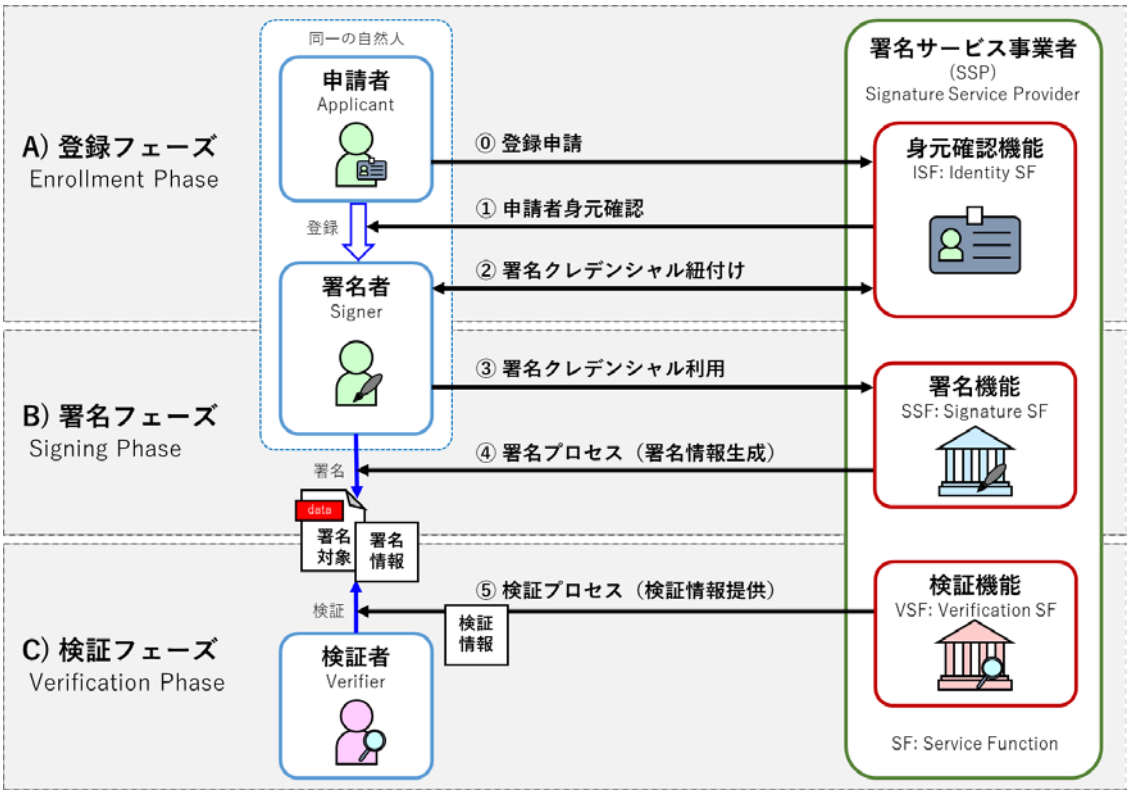

図 2-1　署名サービスの基本モデル

基本モデルにおける登録フェーズ・署名フェーズ・検証フェーズの各フェーズにおける手順を表 2-1 で示す。

表 2-1　署名サービスの基本モデルにおけるフェーズと手順の説明

A）登録フェーズ（Enrollment Phase）：署名者（申請者）が行う	
	手順⓪ 登録申請 申請者が署名サービス利用時に ISF（身元確認サービス機能）へ登録申請をおこなうことで手順が開始される。
	手順① 申請者身元確認 申請者は署名サービス利用時に ISF に自身の属性情報を提示することで身元確認がおこなわれる。

	手順② 署名クレデンシャル紐付け ISF は申請者の身元確認後に署名クレデンシャル（署名鍵 or 認証情報）の提供または申請者が所有するクレデンシャルとの紐付けをおこなう。これにより申請者は署名者となる。
B） 署名フェーズ（Signing Phase）：署名者（申請者）が行う	
	手順③ 署名クレデンシャル利用 署名者は署名時に署名クレデンシャルを SSF（署名サービス機能）に提示して当人認証をおこなう。SSF は署名クレデンシャルを確認して署名者当人であることを確認する。
	手順④ 署名プロセス（署名情報生成） SSF は署名者に署名対象の確認を求め、署名クレデンシャル利用等により署名情報を生成する。検証に必要な署名情報の全てまたは一部を署名プロセスでは提供せず後日 VSF（検証サービス機能）から検証情報として提供する場合もある。
C） 検証フェーズ（Verification Phase）：署名者と異なる検証者（第三者）が行う	
	手順⑤ 検証プロセス（検証情報提供） 検証者は署名者より受け取った署名対象と署名情報に対して検証をおこなう。VSF は必要があれば有効性等の検証情報を提供することで、署名対象に対しての署名者の意思と署名時点からの非改ざんが確認できるようにする。

本ガイドラインでは、電子署名を目的や用途によって「承認目的署名（Approval Signature）」と「発行元保証署名（Origin Assurance Signature）」に分けている。承認目的署名は署名者の意思を示す目的で利用されるものであり電子署名法が想定している用途と言える。本ガイドラインでは単に署名とした場合には承認目的署名を意味している。発行元保証署名は発行元（署名者）が内容を保証する目的で利用される。承認目的署名と発行元保証署名に関してより詳しくは「付属書 B. 承認目的署名と発行元保証署名」を参照されたい。

署名サービスは署名者と検証者に署名と検証に必要となるサービスや情報を提供する。署名サービスを機能に分割すると、「登録フェーズ」は ISF（身元確認サービス機能）が、「署名フェーズ」は SSF（署名サービス機能）が、「検証フェーズ」は VSF（検証サービス機能）がサービスを提供する。これら機能は 1 つの事業者にて提供することもあるが、別々の事業者が提供する場合もある。

署名者と署名サービスは検証者に対して、署名対象である電子データと、署名対象に紐づく電子署名の 3 要件（本人の身元・本人の意思・非改ざん）について、電子的な証拠である署名情報を提供する。署名対象である電子データと署名情報を合わせて 1 つのファイルとして提供する場合もあるが、別々に提供しても構わない。電子的な証拠は署名時ではなく検

証時に検証情報として提供しても良い。なお署名情報と検証情報に対しても発行者（通常は署名サービス）の保証と非改ざんの保証が必要となる。

ISF では、登録時の身元確認（Identity Proofing）は署名に限らない概念であり、NIST SP 800-63A「Enrollment and Identity Proofing」において技術要件が整理されている。署名サービスでは通常利用の登録時に申請者の身元確認をおこなうが、署名依頼される場合には署名時に身元確認をおこなう場合もある。身元確認のリスクとしては署名者本人以外を署名者として登録してしまうことで別人が署名者に成りすますことがあげられる。

SSF では、署名時の承認意思の為に「当人性（身元確認済みの当人であるかどうか)」と「内容の同意（署名対象の内容を承認)」の 2 点を保証する為の署名データを生成する。当人性（Authentication）の部分は NIST SP 800-63B「Authentication and Lifecycle Management」において技術要件が整理されている。当人性のリスクに対応する為に、署名独自の要件として、署名時に署名者が内容を確認して同意するプロセスの保証が別途必要になる。

VSF では、検証時に検証者が、署名者や署名サービスから提示された署名対象と署名情報を検証する。検証方法は署名方式により異なるが「本人の意思」と「非改ざん」が確認できる必要がある。検証に利用する署名情報群を信頼する為には、検証者が信頼する信頼基点（トラストアンカー）による保証が必要となる。検証時のリスクとしては署名対象の改ざんや署名者の入れ替え等がある。検証により検証者は、身元確認された当人が承認した署名対象であり、かつこれが改ざんされていないことを確認できる必要がある。

2.2. 署名方式の整理

最も基本となる署名方式は、PKI（公開鍵基盤）ベースのデジタル署名を署名者当人が管理する署名鍵で署名をおこなう認証局保証（Certification Authority Assurance）の鍵自己管理（Key Self Management）である「ローカル署名方式（Local Signature Method)」である。ローカル署名方式では署名鍵を署名者自身が保有管理（自己管理）することで当人保証をおこなっているが、デジタル ID の認証情報を用いた当人認証により当人保証をおこなう署名方式も使われるようになった。なお認証局保証とは、署名者の身元保証を PKI ベースの認証局（CA：Certificate Authority）が担う。なお PKI ベースであっても認証局を使わない自己署名証明書を電子署名に使った場合（いわゆるオレオレ証明書の利用）には、身元確認がされておらず、第三者による保証がされていないことになる。自己署名証明書を使った場合に、同じ当人であることを保証するような当人認証には使えるが、電子署名としては要件が不足することになる。

ローカル署名方式と同じく、認証局保証の鍵預託管理のモデルである「リモート署名方式（Remote Signature Method）」では、署名鍵自体はリモート署名サービス事業者（RSSP：Remote Signing Service Provider）が保管管理しており、署名者に紐付いた認証情報により署名認可（Signature Authorize）することでオンライン上にて署名付与をおこなう方式となる。

PKI ベースで署名者の身元保証をおこなわない署名方式としては、署名者の身元保証を署名事業者（SSP）自身が担うもの（事業者保証）として「認証記録署名方式（Authentication Record Method）」と「事業者署名方式（Provider Signature Method）」がある。これらの方式については署名者の承認意思の保証に関する標準化がおこなわれていないことから、署名者の身元確認の保証と、署名認可の記録をどのような署名情報として残すかを明確にすることが重要となる。これらが欠けると、電子署名としては要件が不足することになる。

本ガイドラインでは、表 2-2 に示すこれら 4 つの署名方式について整理するが、今後更に新しい署名方式が出てくる可能性もある。例えばブロックチェーンを利用するモデル等が考えられるが、一般にはまだ普及していないことから本ガイドラインにおいて現時点では整理対象外とする。

表 2-2　4 種類の署名方式

署名方式	概要
ローカル署名方式 ・認証局保証 ・鍵自己管理	身元確認と本人性の保証を PKI ベースの認証局がおこなう。 電子証明書と紐付いた署名鍵を手元（ローカル）にて署名者自身が所有管理して、手元（ローカル）にある署名アプリ等を利用してデジタル署名する。
リモート署名方式 ・認証局保証 ・鍵預託管理	身元確認と本人性の保証を PKI ベースの認証局がおこなう。 電子証明書に紐付いた署名鍵をリモート署名事業者が管理保管する。署名者自身は認証情報を所有管理し、署名時に当人認証して署名認可することで署名鍵を利用しデジタル署名する。
認証記録署名方式 ・事業者保証 ・認証記録	身元確認と本人性の保証を署名サービス事業者がおこなう。 署名者自身が認証情報を所有管理し、署名時の当人認証と署名操作の記録を事業者が保存することで電子署名とする。
事業者署名方式 ・事業者保証 ・事業者署名	身元確認と本人性の保証を署名サービス事業者がおこなう。 署名者自身が認証情報を所有管理し、署名時の当人認証と署名操作の記録を事業者が保存し、事業者の電子証明書と紐付いた署名鍵でデジタル署名する。立会人型署名と呼ばれることもある。

身元確認に関しては署名方式には依存せず共通とする為にここでは説明を省略する。身元確認は署名する前には終わっている前提とする。署名時の当人認証に利用する署名クレデンシャルが署名方式でどのように異なるか、また検証時の本人性保証と非改ざん保証の方式はどのように異なるかを以下の表 2-3 に示す。

表 2-3　署名方式の整理

署名方式	クレデンシャル	検証時本人性保証	非改ざん保証
ローカル署名	署名鍵	PKI ベース認証局	当人デジタル署名
リモート署名	署名鍵と 認証情報	PKI ベース認証局と リモート署名事業者	当人デジタル署名
認証記録署名	認証情報	署名サービス事業者	何らかの改ざん防止措置 (アクセス制御等)
事業者署名	認証情報	署名サービス事業者	事業者デジタル署名

電子署名に認証情報を用いた当人認証を利用することが増えている。当人認証を利用することで、端末を当人が操作していることを保証することができる。更に当人認証によりアクセストークン等を発行することで、当人によるセッションを維持したリアルタイムでのプロセス保証をおこなえる。電子署名は署名対象となるデータの保証に関して時間差をおいておこなえる必要があるので、当人認証だけでは電子署名の要件を満たせない。

2.2.1. ローカル署名方式

認証局保証の鍵自己管理のモデルであるローカル署名方式は、古くから使われており電子署名の基本と言える署名方式である。PKI ベースの認証局（CA：Certificate Authority）が ISF（身元確認サービス機能）と VSF（検証サービス機能）を提供するが、署名者当人がローカルな署名機能を使って直接署名付与する為に、外部に SSF（署名サービス機能）を提供するサービスの必要がない。図 2-2 にローカル署名方式の概念図を示す。

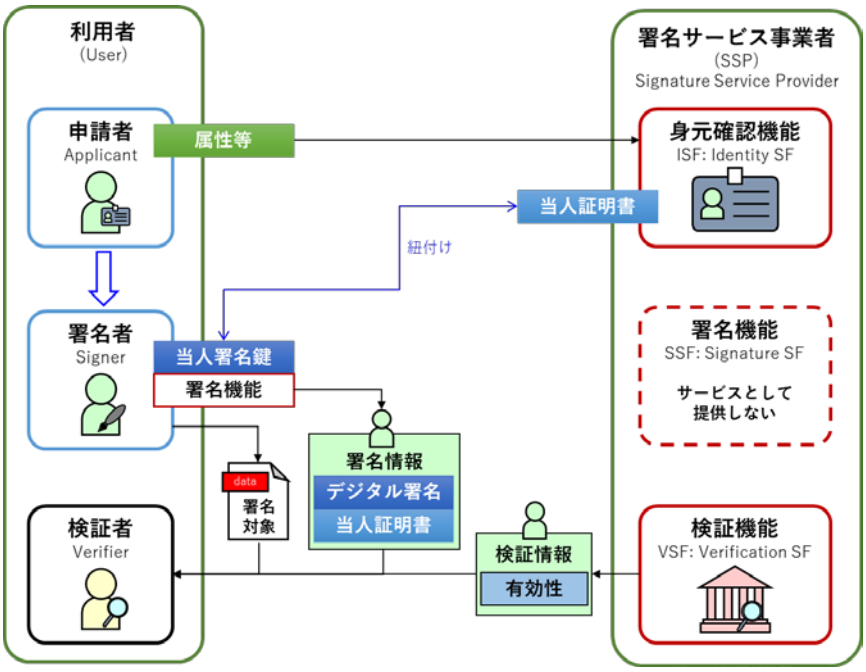

図 2-2　ローカル署名方式（認証局保証 鍵自己管理）

ISF は登録局（RA：Registration Authority）で身元確認を行った後に、発行局（IA：Issuing Authority）から署名鍵に紐付いた電子証明書を発行する。署名者は署名クレデンシャルとして署名鍵を所有管理する。RA と IA の機能は別の事業者が提供する場合もある。

SSF は署名者自身が署名対象を確認した後にローカルなデジタル署名機能により、当人の署名鍵を使ったデジタル署名をおこなう。外部にある SSF（署名サービス機能）が提供する当人認証はおこなわれないが、署名鍵の所持と IC カードや USB トークン等であれば利用時に PIN を利用することで当人を確認していることになる。IC カード・USB トークンであれば耐タンパな認証器の所有と同等であり PIN（知識）も必要となることから 2 要素認証と同等と考えられる。また PKCS#12 形式の場合にはソフト的な所有となり当人認証レベルとしては低くなると考えられる。

VSF は署名時における署名電子証明書の有効性を示す検証情報（CRL/OCSP）を検証局（VA：Validation Authority）から取得して検証することで実現している。またデジタル署名により署名対象に改ざんが無かったことも確認できる。検証情報を署名データに追加することで長期署名化して全ての情報をコンパクトにまとめることも可能である。また検証サービスとして VSF の機能を別サービスから提供する場合もあるが、この場合に検証サービスは VA から検証情報を取得して確認した結果を返すことになる。

認証局保証のローカル署名方式では、検証の手順や方法が標準化されており、また認証局

運用の要件も標準化された認定基準がある。一般的にはこれらの情報は CP/CPS（証明書ポリシー/認証運用規程）として認証局から公開されているので検証者も確認できる。ローカル署名方式は、署名鍵の管理が運用規定に従いきちんとおこなわれていると言う前提条件はあるが、シンプルで信頼性が高い署名方式と言える。ただし PKCS#12 形式の場合には署名鍵が容易にコピーできる点で安全性が低く、IC カードを使った場合には読み取りに IC カードリーダーかスマートフォンが必要となる点および IC カードの事前配布が必要な点が課題となる。またローカルに署名鍵がある為にクラウド上のサービスとの連携が難しいと言う課題もある。

2.2.2. リモート署名方式

認証局保証の鍵預託管理のモデルであるリモート署名方式は、ローカル署名方式と同じく PKI ベースの認証局（CA）が ISF（身元確認サービス機能）と VSF（検証サービス機能）を提供するが、それに加えてリモート上の署名サービスが SSF（署名サービス機能）を提供する。ローカル署名方式とはリモート上の SSF の有無が異なる。署名鍵の管理を SSP 自身がおこなうこともあるが、外部の RSSP（リモート署名サービス事業者）であることも多い。図 2-3 にリモート署名方式の概念図を示す。

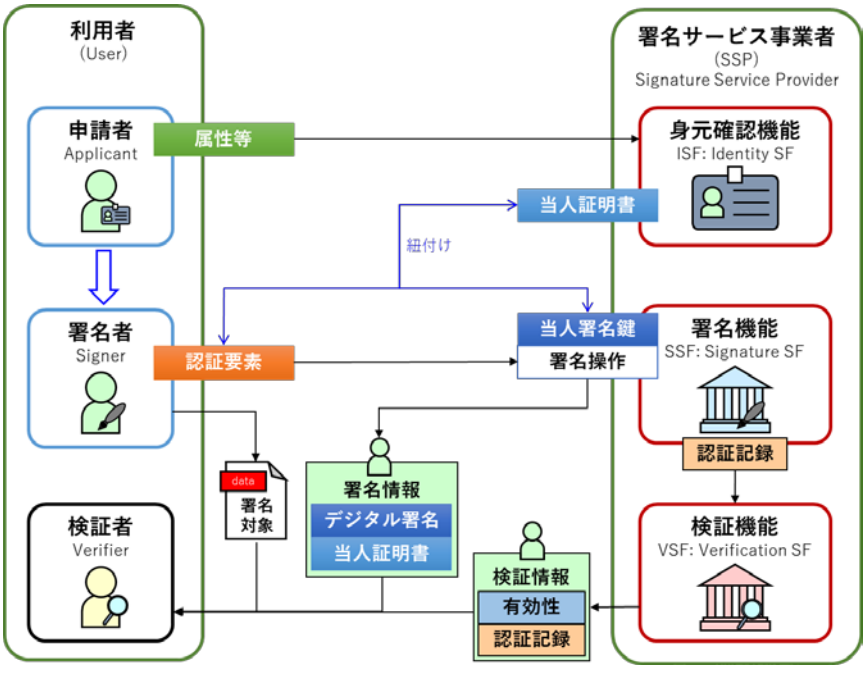

図 2-3　リモート署名方式（認証局保証型 鍵預託管理モデル）

ISF は身元確認後に、署名鍵と署名者が管理する認証情報を紐付ける。ISF の身元確認は、認証局の登録局（RA）がおこなう。その際に登録局が外部の CSP（Credential Service Provider）

を利用することがある。身元確認に CSP を利用するかどうかはリスク評価の上で運用ポリシーとして決める必要がある。身元確認後に発行局（IA：Issuing Authority）から SSF が管理する署名鍵に紐付いた PKI ベースの電子証明書を発行する。同時に署名鍵への認証情報の紐付け登録をおこなう。認証情報は署名者が所有している情報を ISF へ提示して紐付けても良いし、ISF が署名者へ発行しても良い。

SSF は署名鍵に紐付いた認証情報にて当人認証をおこなう（署名認可する）ことで署名付与を許可する。なお承認目的の電子契約等の用途では署名者による内容確認が必要となる。SSF は不正に署名鍵が利用されないことを運用ポリシーとして保証する必要がある。また当人認証の保証レベルが低い場合（例えばパスワードのみの 1 要素認証等）は署名者以外の不正な第三者が署名鍵を使うリスクがある。

リモート署名方式において生成される署名データは、同じ認証局保証型のローカル署名方式と同一となる為に、VSF はローカル署名と変わらない。ただし当人認証時のログ等が存在するので必要に応じて認証ログや操作ログを検証情報として提供できるようにすべきであるし、署名情報の何らかの属性（例えば電子証明書の属性）にてリモート署名されたものであることを判別できることが望ましい。

認証局保証型のリモート署名方式ではローカル署名方式と同じく、検証の手順や方法が標準化されており、また認証局の要件も標準化された認定基準があり、信頼性が高い署名方式と言える。ただし追加で必要となる、認証ログや操作ログを検証情報に関する標準はまだないと言う課題がある。一方でローカル署名方式と異なり、署名操作に関するログが SSF に残ることから不正利用の検知が可能となる利点がある。リモートに署名鍵がある為にクラウド上のサービスとの連携が容易である点も利点となる。

また事前に身元確認をおこなわず、当人認証時に身元確認をおこない、1 回のみ（One Time）または 1〜2 日程度の短期間有効（Short Lived）な電子証明書をその場で発行するようなリモート署名方式も考えられる。

2.2.3. 認証記録署名方式

事業者保証の認証記録のモデルである認証記録署名方式では、署名者は認証情報を所有し署名時に当人認証をおこない、署名ボタンのクリック等の署名操作（署名認可）をおこなう。なお否認防止目的の電子契約等の用途では署名手順として内容確認が必要となる。この時の認証ログと操作ログを記録保存しておき承認意思の電子証拠として提示できるようにすることで電子署名を実現する。デジタル署名を用いないことから、もう 1 つの要件である

非改ざんに関しては署名サービス側で原本保管（コピー等と区別できるようオリジナルデータを原本として保管する仕組み）やハッシュ値を保存することで保証する必要がある。図2-4 に認証記録署名方式の概念図を示す。

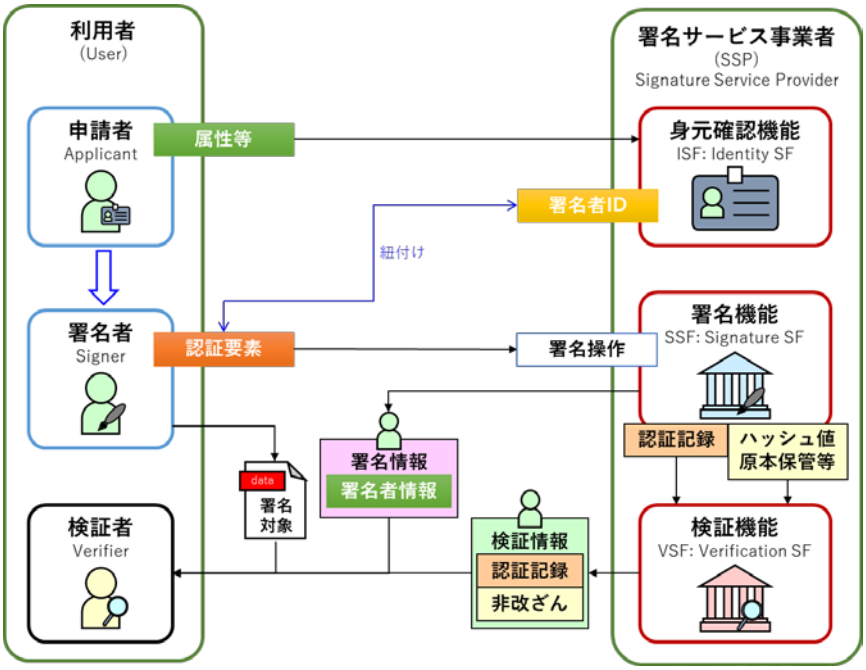

図 2-4　認証記録署名方式（事業者保証 認証記録）

ISF は CSP（Credential Service Provider）の機能となる。CSP は申請者の身元確認（Identity Proofing）および署名者への認証情報の登録を含む機能を持つ。詳しくは NIST SP 800-63 で説明されている。認証情報は署名者から CSP へ提供するか、CSP から署名者に発行する。

SSF は、署名者に紐付いた認証情報による当人認証および、これを前提とする署名認可操作（例えば署名ボタンのクリック等）等を署名処理のセッションとして行い、署名情報として署名者情報を提供する。SSF は、当人認証・署名認可操作のログを保存する必要がある。SSF は不正に認証情報が利用されないことを運用で保証する必要がある。また当人認証の保証レベルが低い場合（例えばパスワードのみ等）は署名者以外の不正な第三者が電子署名を行うリスクを生じる。最後に SSF は改ざんを防止する為に原本保管やハッシュ値等による措置をおこなう。

事業者保証型の VSF における検証手順はまだ標準化されていない。承認意思に関して当人認証と署名認可操作を保証する検証情報の電子データを証拠として提供する必要がある。非改ざんについてはアクセスログやハッシュ値等で電子証拠として提供する必要がある。

認証記録署名方式では、認証情報の管理は必要だが署名鍵を管理する必要がないためにシンプルな仕組みに出来る利点がある。またクラウド上のサービスとの連携も容易となる。しかしながら電子証拠として見た場合には書式や検証方法が標準化されていない。また事業者保証型では署名サービス事業者自身の信頼性として、認証局保証と比較した場合に認証局と同等の基準等の信頼性が望まれる。

2.2.4. 事業者署名方式

事業者保証の事業者署名のモデルである事業者署名方式は、認証記録署名方式に事業者による保証としてデジタル署名を加えた方式となる。認証記録署名方式と同じく、署名者は認証情報を所有し、署名時に当人認証を経て、署名ボタンのクリック等の署名操作（署名認可）をおこなう。なお承認目的の電子契約等の用途では署名手順として内容確認が必要となる。この時の認証ログと操作ログを記録保存しておき承認意思の電子証拠として提示できるようにすることで電子署名を実現する。もう 1 つの要件である非改ざんに関しては、事業者証明書によるデジタル署名により保証される。事業者のデジタル署名がある点では、認証記録署名方式よりも事業者による保証が明確となる利点がある。図 2-5 に事業者署名方式の概念図を示す。

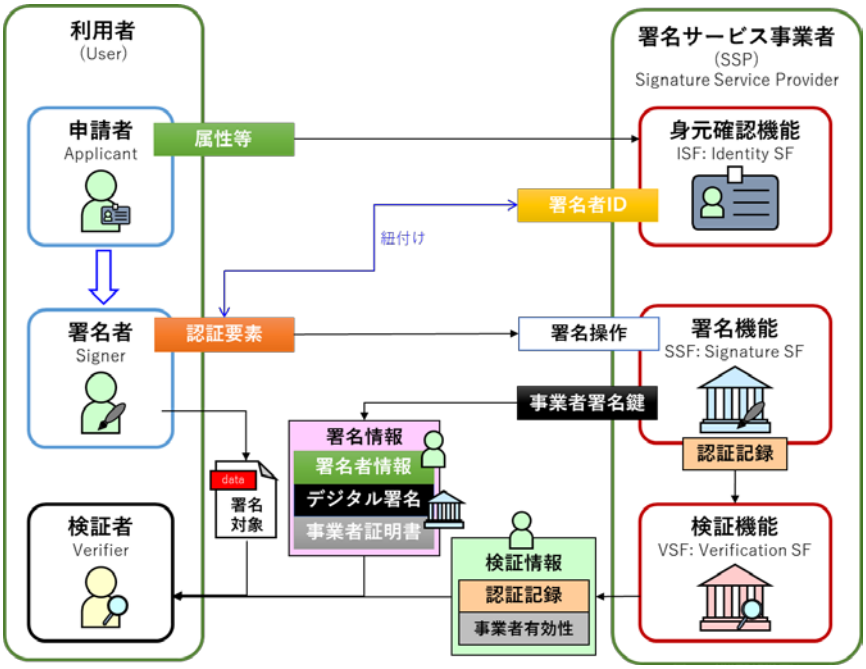

図 2-5　事業者署名方式（事業者保証 事業者署名）

ISF は CSP（Credential Service Provider）の機能となる。CSP は申請者の身元確認（Identity Proofing）および署名者への認証情報の登録を含む機能を持つ。詳しくは NIST SP 800-63

で説明されている。認証情報は署名者から CSP へ提供するか、CSP が署名者へ発行する。

SSF は、署名者に紐付いた認証情報による当人認証および、これを前提とする署名認可操作（例えば署名ボタンのクリック等）等を署名処理のセッションとして行う。SSF は、当人認証・署名認可操作のログを保存する必要がある。SSF は不正に認証情報が利用されないことを運用で保証する必要がある。また当人認証の保証レベル（SIAL/IAL）が低い場合（例えばパスワードのみ、メール URL クリックのみ等）は署名者以外の不正な第三者が電子署名を行うリスクを生じる。最後に SSF は事業者の電子証明書に紐付いた署名鍵によりデジタル署名を付与して署名操作と署名対象の内容を保証する。この結果、署名情報として事業者によるデジタル署名と事業者証明書と署名者が誰であるかの署名者情報を提供する。

事業者保証型の VSF における検証手順はまだ標準化されていない。承認意思に関して当人認証と署名認可操作を保証する検証情報の電子データを証拠として提供する必要がある。非改ざんについては事業者の電子証明書によるデジタル署名を検証する。一見すると認証局保証型と署名データ自体は同じに見えるが、事業者保証型のデジタル署名に利用する電子証明書は事業者のものであり、事業者のデジタル署名を PKI 的に検証するだけでは承認意思の保証とはならない。承認意思を別途保証する手段やデータを提供する必要がある。表 2-4 にリモート署名方式と事業者署名方式の比較をまとめる。

表 2-4　リモート署名方式と事業者署名方式の比較

	リモート署名方式	**事業者署名方式**
デジタル署名	署名者の電子証明書	事業者の電子証明書
身元保証	認証局（CA）	署名サービス事業者（SSP）
当人認証	リモート署名事業者（RSSP）	署名サービス事業者（SSP）
検証手順	ほぼ標準化されている	署名サービス事業者に依存

事業者署名方式では、認証情報の管理は必要だが署名鍵を管理する必要がないためにシンプルな仕組みに出来ると言う認証記録署名方式と同じ利点がある。更に事業者によるデジタル署名がある為に認証記録方式よりも事業者としての責任は重いと言える。またクラウド上のサービスとの連携も容易となる。しかしながら電子証拠として見た場合に承認意思の確認についての書式や検証方法が標準化されていない。認証記録署名方式と同様に、事業者保証型では署名サービス事業者自身の信頼性として、認証局保証型と比較した場合に認証局と同等の基準等の信頼性が望まれる。

一方で例えば電子申請を考えた場合に、受付印のように事業者署名が使えることから、身元確認と当人認証の保証レベルが必要十分なレベルである場合には有用な署名方式と言え

る。この例では申請者側にとって受け付けられた保証（証拠）として事業者署名が使える。逆に受付側において申請者の身元確認と当人認証が必要な場合には、認証局保証型のローカル署名方式やリモート署名方式の方が電子証明書のみで確認できる利点があると言える。

2.3. 電子署名の保証レベル

ここでは表 2-5 に示す 4 つの署名要件の解説と、それぞれに対応した、署名者身元保証レベル SIAL・署名手順保証レベル SPAL・署名データ保証レベル SDAL・サービス運用保証レベル SOAL、について解説する。

表 2-5　電子署名の保証レベル

署名要件	フェーズ	保証レベル
証明者身元保証	登録	署名者身元保証レベル SIAL: Signer Identity Assurance Level
署名プロセス保証	署名	署名プロセス保証レベル SPAL: Signing Process Assurance Level
署名データ保証	検証	署名データ保証レベル SDAL: Signature Data Assurance Level
サービス運用保証	全体	サービス運用保証レベル SOAL: Service Operation Assurance Level

2.3.1. 署名者身元（Signer Identity）保証レベル：SIAL

ここでは登録フェーズにおける署名者の身元確認について、申請者と ISF（身元確認サービス機能）の関係と責任について説明する。申請者は身元確認後に登録されることで署名者となる。署名者の身元確認を保証するレベルとして、SIAL（署名者身元保証レベル）を定義する。SIAL は NIST SP 800-63A に定義されている IAL（Identity Assurance Level）とほぼ同じ内容となっている。

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。詳細については NIST SP 800-63 を参照。

SIAL1 は申請者の氏名や住所などが現実に存在し矛盾しないことを確認する基本レベル。SIAL2 は顔写真付きの証拠により、その真正性や有効期限、申請者が本当の持ち主かをより厳格に確認するレベル。SIAL3 は IC チップ付の証拠を用いて、訓練された担当者が対面で手続きを行い、少なくとも一つの生体情報も取得する最も厳格なレベル。表 2-6 にて SIAL 各レベルの定義を示す。

表 2-6　署名者身元保証レベル SIAL の定義

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】** 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。

署名フェーズで利用する署名者（申請者）と紐付けされる署名クレデンシャルには、署名鍵と認証情報の 2 種類がある。ISF は以下のいずれかの対応をおこなうことができる。

署名鍵（デジタル署名用）：

- 申請者が生成または用意した署名鍵に紐付いた電子証明書を発行する。
- ISF が生成または用意した署名鍵に紐付いた電子証明書を発行する。

認証情報（当人認証用）：

- 登録時に ISF が発行した認証情報を申請者に発行する。

- 申請者が所有する認証情報を紐付ける。
- 必要に応じて後日認証情報を紐付ける。

署名クレデンシャルは事前に定められたライフサイクルポリシーに従って更新される。ISF は署名者（申請者）の属性の正確性と最新性をある程度保証する為に認証クレデンシャルの有効期間を定める。有効期間内であっても署名者の属性に変更があるか再確認できない場合または署名者から失効の申請があった場合には、ISF は認証クレデンシャルを無効化（失効）する必要がある。有効期限が近くなった場合に事前に定められた更新ポリシーにより認められた場合、ISF は認証クレデンシャルの再発行または再紐付けをおこなうことが出来る。

2.3.2. 署名プロセス（Signing Process）保証レベル：SPAL

ここでは署名フェーズの署名プロセス（署名手順）について、署名者と SSF（署名サービス機能）の関係と責任について説明する。署名プロセスを保証するレベルとして、SPAL（署名プロセス保証レベル）を定義する。署名プロセスには「署名者の当人認証」と「内容確認と署名付与」の 2 つの手順が必要となる。

署名プロセスで必要となる手順：

- 署名者の当人認証（登録され身元確認済みの当人であることの認証）を実行する。
- 署名者が署名対象の内容を確認して承認した証として署名付与を実行する。

このうち当人認証の保証レベルについては、NIST SP 800-63B に AAL（Authentication Assurance Level）として定義されており、この中で認証情報としては以下の 3 種類が定義されている。

認証における要素の種類：

- 知識（Something you know）　：例としてパスワード等
- 所有（Something you have）　：例として ID カードや暗号鍵
- 生体（Something you are）　：例として指紋やその他生体特有データ

2 要素認証にはこれら 3 種類のうち 2 種類が必要となる。どのような認証情報があるかは NIST SP 800-63B にて説明されている。当人型ローカル署名方式では署名クレデンシャルとして署名鍵を用いて認証情報を利用していない為に、AAL をそのまま利用が出来ない。しかしながら署名鍵を所有要素として見ると、利用時に PIN 入力が必要な IC カードに署名鍵を入れている場合には、所有＋知識の 2 要素でありかつフィッシング耐性もあると考

える。

署名プロセスでは、署名者に対して署名対象の確認と承認意思の証として署名付与を求めるが、これは NIST SP 800-63B にはない署名プロセス独自の要件となる。なお e シール等の発行者保証署名では、別途署名する条件を定めることで署名対象の確認を省き自動署名をすることが可能となる。e シールや発行者保証署名に関しては「付属書 B. 承認目的署名と発行元保証署名」にて解説する。

SPAL1 では 1 要素認証の当人認証をおこなう。SPAL2 では 2 要素認証の当人認証をおこなう。SPAL3 では SPAL2 に加えてフィッシング耐性が必要となる。なおどのレベルであっても署名対象となる内容を確認した上で署名付与することが求められる。表 2-7 にて SPAL 各レベルの定義を示す。

表 2-7　署名プロセス保証レベル SPAL の定義

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】** SPAL1 の当人認証を 2 要素認証でおこない FIPS モードの暗号利用が必要。 ※ 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。
SPAL3	**【SPAL2 に加えてフィッシング耐性が必要】** SPAL2 の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。

なお 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、本ガイドライン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 800-63 への準拠が必要となる場合には、準拠するドキュメントを確認する必要がある。

2.3.3. 署名データ（Signature Data）保証レベル：SDAL

ここでは検証フェーズにおいて検証者が検証に利用する署名データについて説明する。検証者は署名対象と署名データを利用して検証をおこなう。署名データは表 2-8 で示すように、署名時に作成される「署名情報」と、検証時の為に VSF（検証サービス機能）が提供する「検証情報」、が含まれる。本ガイドラインでは署名データを検証時に利用されるデータ群と定義する。この署名データの保証レベルとして、SDAL（署名データ保証レベル）を定義する。SDAL は署名データ自体の信頼性を保証する保証レベルであり、検証した結果についての保証レベルではない。

表 2-8　署名データを構成する要素

要素	概要
署名情報	署名時に SSF 等にて作成または提供される属性群。デジタル署名であれば署名値や署名に利用した署名鍵に紐付いた X.509 電子証明書や署名対象のハッシュ値や形式等がある。PKI ベースのデジタル署名の場合には PDF 署名、CMS 署名、XML 署名、JWS 等の署名フォーマットおよび PAdES、CAdES、XAdES、JAdES 等の長期署名フォーマット（ISO 14533 シリーズ）として署名情報の仕様が標準化されている。事業者保証型の場合には標準化された仕様は現時点ではない。
検証情報	検証時に VSF 等の外部より提供される属性群。PKI ベースであれば CRL や OCSP 等の有効性確認情報があるが、他にも信頼基点（トラストアンカー）や有効な暗号リスト等も含まれる。また事業者保証型の場合には、署名時の操作ログ等から署名を保証するために提供される情報も検証情報となる。必要に応じて公開されている署名サービス運用規定（SSPS）も外部から提供されると言う意味では検証情報と言える。

電子署名の検証において署名対象と署名データにより確認が必要な項目は電子署名の 2 要件となる。詳細は「2.2.章 電子署名の定義」を参照。

- 本人の意思：署名者の「本人性」と署名時の「承認意思（署名手順)」の確認
- 非改ざん：署名対象が署名時点から改ざんされていないことの確認

SDAL1 では SSP から本人の意思と非改ざんについて何らかの署名データが検証者に提供される必要がある。SDAL2 では署名データに対して標準化または事前に定められた検証手順をおこなうことで本人の意思と非改ざんが保証される必要がある。SDAL3 では SDAL2 に加えて信頼された第三者組織による認定や監査等の保証が必要となる。表 2-9 にて SDAL

各レベルの定義を示す。

表 2-9　署名データ保証レベル SDAL の定義

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。 ※ 署名時刻に関しては、SSP の署名システム上の時刻でも良い。
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に対してもデジタル署名が必要。 ※ 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。 ※ 信頼された署名時刻とは、PKI ベースのタイムスタンプまたは信頼された運用がおこなわれているシステム時刻による保証等がある。
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。 ※ 本人性についての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。 ※ 署名時刻について信頼された第三者組織の保証例として、PKI ベースのタイムスタンプがある。

署名時刻は正確には検証時に利用される時刻であって、署名がおこなわれた時刻、または少なくともその時刻の前に署名がおこなわれたことを証明できる時刻である。過去に作成された署名データを検証する必要がある意味から、署名時刻は SDAL の要件となる。署名時刻には幾つかの考え方がある。１つにはシステム時刻であり PKI ベースのタイムスタンプ（RFC 3161）では厳密にタイムスタンプを要求した時刻が残される。タイムスタンプは

署名後に追加される場合が多く、厳密には署名を実際におこなった時刻ではないし、例えば電子申請において受付側でタイムスタンプを追加する場合には受付時刻である。一方で電子契約等においては申告時刻（Claiming Time）として契約が発効する時刻（日付）を指定する場合もある。このように検証時に利用する時刻には複数の可能性があるが、どれを署名時刻として利用するかは運用ポリシーに依存する。署名時刻がないまたは信用できない場合には検証時の時刻が利用される。SDAL においては、SDAL1 では何らかの署名時刻の提供が必要であり、SDAL2 では信頼される署名時刻の提供が必要であり、SDAL3 では第三者保証がされた署名時刻の提供が必要となる。

PKI ベースの認証局保証型では、署名鍵を使ったデジタル署名の場合に鍵管理のレベル（PKCS#12・サーバーHSM・IC カード等）が電子証明書の属性等で確認できるべきであり、署名時の承認（署名認可）に認証情報を使った場合（リモート署名方式や事業者保証型の場合）には利用した認証情報の数やその種類が確認できるべきである。

登録時の SIAL・署名時の SPAL・運用時の SOAL のレベルも、署名サービス運用規定（SSPS）等から確認できることが望ましい。PKI ベースの認証局保証型では、ポリシーOID 等の情報を電子証明書に埋め込み、文書自体は CP/CPS として公開することが一般的となっている。認証局保証型であってもリモート署名方式の場合には、リモート署名事業者より認証情報の配布手順や電子署名付与の方法についてのポリシー情報も別途提供されることが望ましい。事業者保証型である、認証記録署名方式・事業者署名方式の場合には、CP/CPS 同等のポリシー情報と署名サービス事業者より身元確認の手順・認証情報の配布手順・署名認可の方法等についてのポリシー情報を提供することが望まれる。各ポリシーは文書化されるべきであるが、詳しくは「3.5.2 章 署名サービス運用規定（SSPS）の作成と公開」にて解説する。

事業者保証の電子署名方式では、現時点では標準化されたガイドライン等は存在しておらず、事業者が独自の署名データを設定する必要がある。なおデジタル署名された認証アサーション（例：JWT 形式の ID トークンや SAML アサーション等）を認証アサーションへの署名に利用した X.509 電子証明書や検証鍵と共に保存して証拠とするような方法は有効と考えられる。また保証レベルとしては低くなるが、認証情報を使った当人認証時の認証ログや操作ログを保存して VSF がデジタル署名を行って証拠として提供する方法も考えられる。また署名者の認証ユーザーID や認証時刻および氏名や所属および各種ポリシー情報へのリンクを署名対象の一部として埋め込むことで別途提供される認証ログ等と紐付ける方法も考えられる。いずれにしても電子署名において検証手順は事前に定めておく必要がある。後から証拠を探す手法はデジタル・フォレンジック（デジタルデータを調べて証拠となる情報を取得する技術）として知られており、電子署名とは別の手法と言える。

2.3.4. サービス運用（Service Operation）保証レベル：SOAL

ここでは署名サービス事業者（SSP）が提供するサービスにおける運用の信頼性について説明する。サービス運用の信頼性を保証する保証レベルとして、SOAL（サービス運用保証レベル）を定義する。SOAL では ISF の登録時・SSF の署名時・VSF の検証時の全てのフェーズを対象とした、署名サービス運用規定（SSPS: Signature Service Practice Statement）とその公開・監査・認定についての保証レベルである。SSPS の策定時にはリスク管理が必要となるが、詳しくは「3章 署名サービスのリスク管理」にて解説する。署名サービスの中でも検証は署名後時間を置いて長く保証される必要がある。この点から VSF（検証サービス機能）を提供する事業者（SSP や CA や CSP 等）が廃業された場合の検証リスクについてどのように保証されるのかは重要なポイントとなる。

SOAL1 では運用基準を定めて遵守ことは求めるが公開等は求めない。SOAL2 では定めた運用基準(SSPS)を公開等(公開･開示･通知)して遵守する。SOAL3 では運用基準(SSPS)の公開に加えて信頼された第三者組織の認定や監査が必要となる。表 2-10 にて SOAL 各レベルの定義を示す。

表 2-10　サービス運用保証レベル SOAL の定義

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。

公開・開示・通知に関しては、公開が最も広く情報を提供することであり、開示と通知は必要となる検証者に提供することとなる。表 2-11 にて各意味を示す。

表 2-11　公開・開示・通知の意味

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。

サービス運用の保証レベルは NIST SP 800 63 にも関連するような内容は記載されておらず、本ガイドラインにおける独自の定義となっている。PKI ベースの認証局においては CP/CPS の公開と遵守は常識となっており、電子署名においては重要な保証レベルであるが、信頼性を求められるサービスであれば運用について確認するために必要な保証レベルと言える。

3. 電子署名のリスク管理（ESRM）

本ガイドラインではリスク管理（Risk Management）を、「プロジェクトや組織の目標を妨げるリスクを特定し、リスクが発現した際のダメージを最小限に抑えるための評価と対応をおこなうプロセス」と定義する。この定義は ISO 31000（JIS Q 31000）の定義と同等である。ISO 31000 ベースのリスク管理では、まずリスクアセスメント（Risk Assessment）をおこない、その結果からリスク対応（Risk Treatment）として対策や軽減策を実施すると共に、ここまでの結果や対策を文書（Document）として残す。リスク管理のプロセスは定期的に繰り返し（Continuous）おこなわれる。なおリスクアセスメントは、リスク特定（Risk Identification）・リスク分析（Risk Analysis）・リスク評価（Risk Evaluation）の 3 ステップに分けられる。以上の手順を可視化した図を図 3-1 に示す。

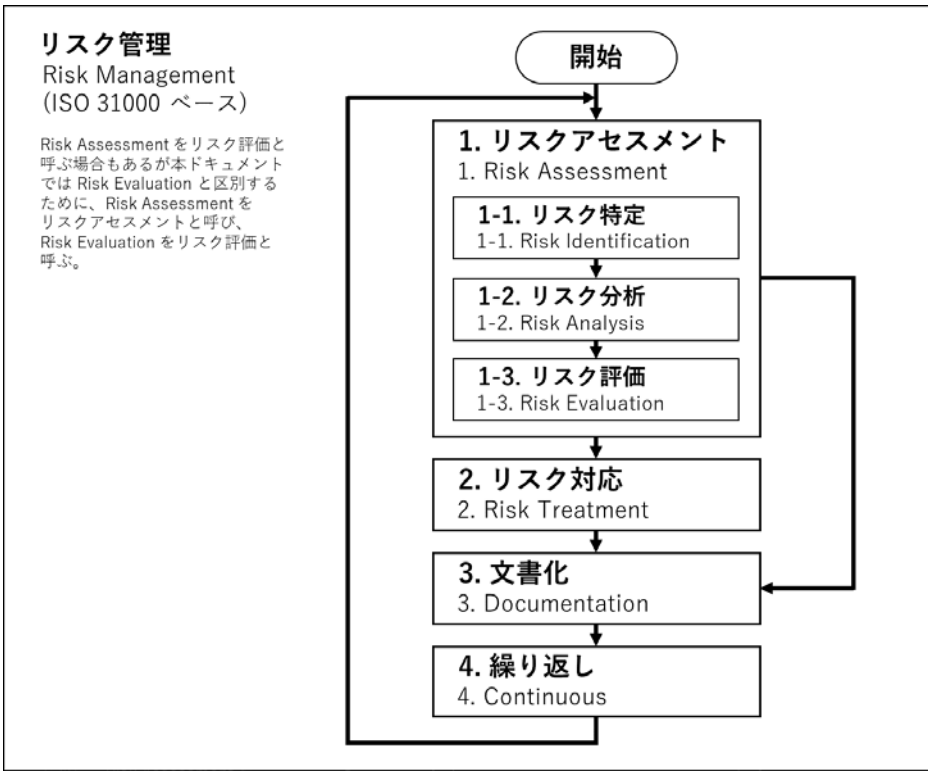

図 3-1　ISO 31000 ベースの一般的なリスク管理の手順

本章では電子署名のリスク管理（ESRM：Electronic Signature Risk Management）について参考情報（Informative）として解説をする。電子認証（デジタル ID）のリスク管理については NIST SP 800-63 の Digital Identity Risk Management（DIRM）にて解説がされている。日本の行政手続きのための、「DS-511 行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン」も参考となる。全般的な一般的なリスク管理については ISO 31000（JIS Q 31000）や IEC/ISO 31010（JIS Q 31010）等で整理がされて

いるので参照することを推奨する。また直接リスク管理の標準ではないが、ISO/IEC 27000 シリーズも情報セキュリティマネジメントシステム（ISMS）を扱っており参考となる。これらのドキュメントを利用して署名システムのリスク管理をおこなう。参考情報として表 3-1 にてリスクの種類毎に利用されるドキュメントの例を示す。

表 3-1　リスク種類毎のドキュメント例

リスクの種類	リスク管理に関するドキュメントの例
一般的リスク	➢ ISO 31000（JIS Q 31000）Risk management – Guidelines ➢ ISO/IEC 31010（JIS Q 31010）Risk assessment techniques ➢ ISO/IEC 27000 シリーズ（JIS Q 27000 シリーズ）ISMS
電子署名	➢ [SAG-1] 署名保証ガイドライン（本ガイドライン） ・3 章の電子署名のリスク管理（ESRM）
電子認証	➢ NIST SP 800-63 Digital Identity Guidelines ・Digital Identity Risk Management（DIRM）の章 ➢ DS-511 行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン

3.1. 概要

本章では、署名サービスの署名保証レベル（SxAL）の利用による電子署名リスク管理（ESRM：Electronic Signature Risk Management）の手順を整理する。一般的なリスク管理と比較して、署名保証レベル（SxAL）を評価基準として利用できることが利点となる。

署名サービスのリスク管理においては、最初に「ステップ 0：定義と初期保証レベルの仮置き」をおこなう。これからリスク管理をおこなう署名システムがどの保証レベル（SxAL）を必要とするかを初期保証レベルとして仮置きすることで、その後のリスクアセスメントやリスク対応をスムーズに進めることができる。なおリスク管理は繰り返しおこなわれるが、2 回目以降では前回の署名保証レベルから初期保証レベルを設定するために「ステップ 0：定義と定義と初期保証レベルの仮置き」を実施する必要はない。

「ステップ 0：定義と初期保証レベルの仮置き」を実施以降の手順は、基本的には一般的な ISO 31000 ベースのリスク管理の手順と同じく「ステップ 1：リスクアセスメントの実施」「ステップ 2：基本策と最終保証レベルの決定」「ステップ 3：文書化（SSAS/SSPS の作成）」「ステップ 4：署名サービス運用と繰り返し」の 4 ステップを繰り返すこととなる。「ステップ 3：文書化」は他のステップのアウトプットと検討の過程の記録をおこない、他のステップ全てと関係することから位置付けが異なるが「ステップ 4：署名サービス運用と繰り

返し」の前には終わらせる必要がある。この手順を可視化した図を図 3-2 に示す。ISO 31000 ベースの一般的なリスク管理の手順と比較すると、署名保証レベル（SxAL）を当初から利用するために「ステップ 0：定義と初期保証レベルの仮置き」が追加されている点が異なる。

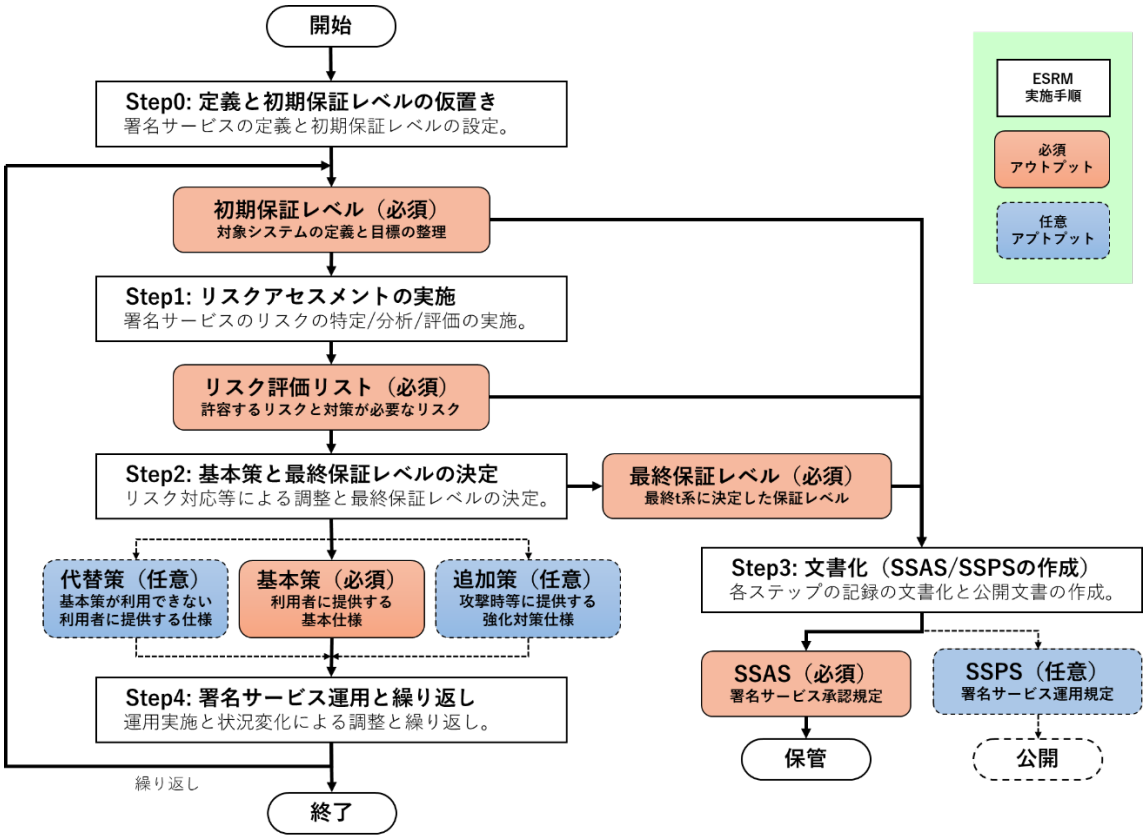

図 3-2　電子署名のリスク管理（ESRM）の手順

リスク管理の方法や手順は、ESRM で採用している方法や手順以外にも各種存在している。図 3-2 の手順をおこなうことが望ましいが、それ以外の方法であってもよいので、署名サービス（SSP）に対して何らかのリスク管理を実施することが求められる。本ドキュメントの ESRM を参考として各手順等を取捨選択また追加をして、まず署名サービスのリスク管理をおこなうことを推奨される。

なお NIST SP 800-63-4 の Digital Identity Risk Management（DIRM）おいては初期保証レベルを仮置きするまでに「Step1: Define the Online Service（オンラインサービスの定義）」と「Step2: Conduct Initial Impact Assessment for each User Group（各ユーザーグループによる初期影響評価の実施）」と「Step3: Select initial assurance levels（初期保証レベルの選択）」の 3 ステップがある。ESRM においてはこの 3 ステップは「ステップ 0：定義と初期保証レベルの仮置き」の 1 ステップにまとめられている。他にも DIRM と ESRM が異なる

点があるが、ESRM は ISO 31000 ベースとしているためであり、どちらが正しいと言うものではなく、自身のサービスに合ったリスク管理を実施する。NIST SP 800-63-4 において DIRM は normative（要件）となっているが、本ドキュメントでは ESRM は informative（参考情報）となる。

リスク管理と言えばセキュリティ・プライバシーに関するリスクのイメージがあるが、別カテゴリーとして、利便性・UI/UX やコスト・財務的等のリスクカテゴリーも合わせて評価する必要がある。一般にはセキュリティリスクに対して高い要求をすると、利便性やコストが悪化する面があり、セキュリティリスク以外のカテゴリーもリスク管理する必要がある。リスクのカテゴリーに関しては「3.3. ステップ 1 ：リスクアセスメント実施」において解説する。

3.2. ステップ 0 ：定義と初期保証レベルの仮置き

署名サービスのリスク管理を初めておこなう場合は、最初に署名サービス（SSP）自体の範囲・目的・利用者・手順・データ・業務上の役割・影響を受ける関係者を整理して文書化する。簡単に言えば「どのような署名サービスを誰にどこまで保証するか」を明確化する。その上で、評価する SSP が求める初期保証レベル（SxAL）を設定する。

繰り返し ESRM を実施する時には前回の最終署名保証レベルを利用することで、このステップ 0 はスキップできる。このステップで仮置きした初期保証レベルは、SSP が利用者に提供する予定の保証レベルを想定するものであり、リスクアセスメントによる評価を経て調整されることで、最終保証レベルとなる。

3.2.1. 初期 SIAL（署名者身元保証レベル）の選択

SIAL は申請者の実在性を保証するためのレベルを示す。提供する署名サービスが求められる身元確認のレベルを処刑 SIAL として設定する。身元確認サービス機能（ISF）を外部に依存することも可能であるために、SSP 自身が身元確認をおこなう必要があることを意味しない。影響度によって 3 つのレベルから身元確認の初期保証レベルを選択する。詳しくは「2.3.1. 署名者身元（Signer Identity）保証レベル：SIAL」を参照。

- **影響度 低（Low）：SIAL1 - 厳格ではない身元属性の確認**
- **影響度 中（Moderate）：SIAL2 - 厳格な身元属性の確認**
- **影響度 高（High）：SIAL3 - SIAL2 に加え IC チップと訓練済み担当者による確認**

SIAL の各保証レベルの概要を以下に示す。

SIAL1：署名者身元保証レベル 1 では、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りすましを主に防ぐ。（厳格な身元属性情報を要求しない。）

SIAL2：署名者身元保証レベル 2 では、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。

SIAL3：署名者身元保証レベル 3 では、S 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。

※ 身元確認には、申請者の実在性を必要としない場合（匿名等）もあるが、電子署名の要件の 1 つに「本人の意思」があることを考えると匿名等のケースは本ガイドラインではスコープ外とする。

3.2.2. 初期 SPAL（署名プロセス保証レベル）の選択

SPAL は署名者当人が署名をおこなうプロセスを保証するためのレベルを示す。身元確認された当人であることを保証するレベルとなる。SPAL の選択をおこなうことは、SSP 自身が署名クレデンシャルの発行をおこなう必要があることを意味しない。影響度によって 3 つのレベルから署名プロセスの初期保証レベルを選択する。詳しくは「3.2.2. 署名プロセス（Signing Process）保証レベル：SPAL」を参照。

- **影響度 低（Low）：SPAL1 - 1 要素の当人認証**
- **影響度 中（Moderate）：SPAL2 - 2 要素の当人認証と FIPS モードの暗号利用が必要**
- **影響度 高（High）：SPAL3 - SPAL2 に加えてフィッシング耐性が必要**

SPAL の各保証レベルの概要を以下に示す。

SPAL1：署名プロセス保証レベル 1 では、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。

SPAL2：署名プロセス保証レベル 2 では、SPAL1 の当人認証を 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。

SPAL3：署名プロセス保証レベル 3 では、SPAL2 の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。

3.2.3. 初期 SDAL（署名データ保証レベル）の選択

SDAL は署名データ自体の信頼性を保証するレベルである。第三者（検証者）が、予め定められた検証手順に従って署名データを利用することで、「署名の意思」と「非改ざん」がどのように確認できるのか、を示す保証レベルとなる。初期 SDAL では検証者にどのような署名データ（署名情報と検証情報）を提供するかにより選択する。詳しくは「3.2.3. 署名データ（Signature Data）保証レベル：SDAL」を参照。

- **影響度 低（Low）：SDAL1 - 事業者より提供される検証可能な証拠と時刻（ログ等）**
- **影響度 中（Moderate）：SDAL2 - 手順に従った第三者による検証可能な証拠と時刻**
- **影響度 高（High）：SDAL3 - SDAL2 に加え信頼された第三者組織による保証**

SDAL の各保証レベルの概要を以下に示す。

SDAL1：署名データ保証レベル 1 では、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。

SDAL2：署名データ保証レベル 2 では、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。

SDAL3：署名データ保証レベル 3 では、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。

3.2.4. 初期 SOAL（サービス運用保証レベル）の選択

SOAL は署名サービスの運用を保証するためのレベルを示す。初期 SOAL は、署名サービスの運用を利用者に保証するレベルと言える。影響度によって 3 つのレベルから署名サービス運用の初期保証レベルを選択する。詳しくは「3.2.4. サービス運用（Service Operation）保証レベル：SOAL」を参照。

- **影響度 低（Low）：SOAL1 - 何らかの運用基準の文書化と順守**
- **影響度 中（Moderate）：SOAL2 - 運用基準の文書化と公開、廃業時の保証**
- **影響度 高（High）：SOAL3 - SOAL2 に加え標準化された運用基準と第三者による保証**

SOAL の各保証レベルの概要を以下に示す。

SOAL1：サービス運用保証レベル 1 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て（文書化して）順守している。

SOAL2：サービス運用保証レベル 2 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）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。

SOAL3：SOAL2 に加えて、標準化された運用基準の公開をおこない、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以外の署名方式において、SOAL3 で求められる要件を満たす認定基準は現時点では存在しないが、今後制定されることを期待する。

3.3. ステップ１：リスクアセスメント実施

リスクアセスメントは表 3-2 に示すとおり、リスク特定・リスク分析・リスク評価の 3 ステップが必要となる。リスクアセスメントの目的は、署名サービスに固有の、登録と身元確認（Signer Identity）・署名プロセスと当人認証（Signing Process）・署名データと検証（Signature Data）・署名サービス運用（Service Operation）における、潜在的な全てのリスクをアセスメント（評価）することである。

表 3-2　リスクアセスメントの手順

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。

1. 影響を受ける主体

リスクアセスメントをおこなう時に、SSP（署名サービス事業者）は、まず検討中の署名サービスによって影響を受ける主体を決定する必要がある。署名システムの障害によって生じる異なる各主体への影響を考慮することが不可欠であるが、特に重要なのは利用者（個人）に対する潜在的な影響を、事業者（組織）に対する影響と並んで考慮することである。

2. リスクのカテゴリー

リスクアセスメントは、表 3-3 に示す各カテゴリーの潜在的な被害を評価することにより決定されるべきである。最初の「セキュリティ・プライバシー」「利便性・UI/UX」「コスト・財務」の 3 つのカテゴリーに関しては、相互に影響することが多いことに留意する必要がある。

表 3-3　リスクの主なカテゴリー

No	カテゴリー	主なリスク例	説明
1	セキュリティ・プライバシー	✓ なりすまし ✓ 改ざん ✓ クレデンシャル漏洩 ✓ アルゴリズム危殆化 ✓ 機密情報の消去 ✓ 個人情報保護違反	セキュリティとプライバシーのリスクは最も重要なカテゴリーではあるが、セキュリティリスクを重視し過ぎると利便性やコストのリスクが高まる場合があるので注意が必要である。
2	利便性・UI/UX	✓ 使い勝手の悪さ ✓ 操作の複雑さ ✓ 利用者離脱	利便性のリスクを軽視するとサービスが利用されないことに繋がるので重視する必要がある。
3	コスト・財務	✓ 初期導入費用 ✓ 運用維持費用 ✓ 追加対策費用 ✓ 賠償金の可能性	セキュリティや利便性のリスクに対応した場合の対策費や運用費の増加リスクはサービスの継続性リスクに繋がる。
4	法的・信頼性	✓ 法的有効性	電子署名は生成した署名データ

		✓ コンプライアンス違反 ✓ 信頼性不足 ✓ インシデント対応 ✓ SNS 等評判	についての法的有効性や準拠性が求められる傾向がある。また信頼して使って貰えるサービスとしての運用も重要となる。
5	運用・業務継続	✓ サービスの継続性 ✓ 障害時対応手順と復旧 ✓ 検証環境の維持 ✓ 連携サービス障害や停止 ✓ 連携サービス側の不正	安定したサービスの提供を支える運用体制が重要でありサービス停止等を生じた場合には信頼性のリスクが増大する。外部に連携するサービスがあれば連携サービスのリスク評価も必要。
6	人的・組織的	✓ 誤操作 ✓ 不適切な利用 ✓ 不正な利用 ✓ フィッシングや詐欺 ✓ ガバナンス不備 ✓ 組織内の情報共有	人的や組織的なリスクに対しては完璧な対策はあり得ないが、教育やガイドライン整備や運用手順等を運用開始後であっても見直しつつ改善して行くことが望ましい。

3.3.1. 電子署名のリスク特定

一般的な署名サービスのリスクを、登録時・署名時・検証時の 3 つのフェーズと運用に分けると以下のリストとなる。ただしこれらは一般的なケースを想定しており、各サービス独自の事情や法的な準拠性等も考慮し、必要に応じて項目を増やしてリストを特定する。リスクの特定には多方面からの視点が必要であり、可能な限りステークホルダーと共に検討するかリスクを指摘して貰うことが望ましい。登録時のリスク例を表 3-4 にて、署名時のリスク例を表 3-5 にて、検証時のリスク例を表 3-5 にて、最後に運用時のリスク例を表 3-6 に示す。

1. 登録時のリスク例

表 3-4　登録時のリスク例

分類	リスクの内容
身元確認の不備	本人確認が不十分（属性情報の不足や信頼性の低さ）で、別人がなりすまして登録されるリスク。
なりすまし登録	ソーシャルエンジニアリング等により担当者がだまされることで、他人の属性で不正登録されるなりすましのリスク。
署名クレデンシャル誤紐付け	署名クレデンシャルが誤って別人に紐付けられることで、なりすましが発生するリスク。

外部委託の信頼性	身元確認や署名クレデンシャルの発行を外部業者に委託した際の不正や不備によるなりすましのリスク。
外部発行の署名クレデンシャルの不備	外部にて発行された署名クレデンシャルを利用する場合に、何らかの不備によりなりすまし等が発生するリスク。
更新時の情報消失	外部からの攻撃や事故により、署名クレデンシャル更新時に認証情報の紐付けが外れ、署名が使えなくなるリスク。
プライバシー侵害	過度な本人確認により、必要以上の個人情報を収集・開示してしまうリスク。
低い利便性/UX	登録手順において、UX（User Experience）の設計が悪く、利便性が低下して申請者離脱やサポート負荷が増加するリスク。

2. 署名時のリスク例

表 3-5　署名時のリスク例

分類	リスクの内容
署名クレデンシャル管理不備	署名クレデンシャルの盗難や複製により、別人が署名を行うリスク。１要素認証等の低保証レベルの場合にリスクが高くなる。
通信経路不備によるなりすまし	フィッシング攻撃やセッション乗っ取り等により通信が乗っ取られ、別人が署名をおこなうリスク。
通信経路不備による改ざん	中間者攻撃等により、確認と異なる文書に署名させられるリスク。
署名時刻の偽装	意図していない時刻が署名に記録され、証明上の誤解が生じるリスク。
ローカル署名時の不正	通信を伴わない署名操作では、ログや証跡が残らず不正が発生しやすくなるリスク。
低い利便性/UX	署名手順において、UX（User Experience）の設計が悪く、利便性が低下して署名の失敗やサポート負荷が増加するリスク。

3. 検証時のリスク例

表 3-6　検証時のリスク例

分類	リスクの内容
署名意思の否認	本人が「署名していない」と主張するリスク（操作記録や証跡の不足）。
署名対象の否認	文書が入れ替え・改ざんされた可能性があり、真正性が確認できない、または本人が「内容が異なる」と主張するリスク（真正性の証跡の不足）。
署名時刻の否認	署名の日時が証明できず、意思表明時刻や対象情報の存在時刻の

	信頼性がないリスク。
証明書の有効性不足	電子証明書の期限切れ等により、署名の有効性を検証できないリスク。
技術の危殆化	暗号技術の脆弱化等により、署名の改ざんや否認が可能になるリスク。
プライバシー侵害	不必要な属性情報（住所・年齢・性別等）の開示により、個人情報保護の問題が発生するリスク。
属性フレッシュネス	署名時点での属性情報（所属・役職等）が古く、正確性に欠けるリスク。
事業者の信頼性不足	電子証明書の発行が信頼性の低いプライベートな認証局であったり、検証用の署名データを発行する SSP の信頼性が低い、等による証拠能力不足のリスク。
検証手順の信頼性不足	検証手順が標準に則っていない、公開されていない場合に、どこまで検証結果を信頼して良いか不明となるリスク。
検証器の信頼性不足	公開され実績のある検証器ではない場合に、検証者が検証結果を信頼して良いか不明となるリスク。

4. 運用のリスク例

表 3-7　運用のリスク例

分類	リスクの内容
運用正当性の説明	運用手順や署名プロセスや準拠している標準仕様を公開しておらず、運用の正当性を証明できないリスク。
内部不正操作	運用担当者自身による不正な署名処理や情報操作のリスク。
担当者なりすまし	不正ログイン等により、運用担当者になりすまして行われる不正な操作のリスク。
操作記録の欠如	運用の正当な操作を示すログや証跡が取得されていないリスク。
不正侵入・改ざん	外部からの侵入により、記録の改ざん・削除、不正操作が行われるリスク。
バックアップ復元不備	障害時の復元に失敗し、署名や証明に必要な情報が欠落するリスク（システム切り替えやデータの復元等）。
事業者廃業やサービス停止	検証に必要なサービスが停止し、署名の有効性確認が困難になるリスク。

3.3.2. 電子署名のリスク分析

リスク特定で得られたリスクの数は多い。まずリストの各項目に対して、現時点で想定し

ている実装や対策を記入する。選択肢がある場合には全ての選択肢も記入する。表 3-8 は各項目の主なリスクに関する実装や対策の例である。

表 3-8　主なリスクに対する実装や対策の例

項目	初期 SxAL	リスク例	想定している実装や対策の例
登録時	SIAL2	身元確認の不備	IC チップを利用した公的な身分証明書による厳格な身元確認。
署名時	SPAL2	署名クレデンシャル管理不備	知識（パスワード）と所有（スマホの認証アプリ）による 2 要素認証。所有や生体の要素を加えることで漏洩等のリスクに備える。
検証時	SDAL2	署名意思の否認	本人が管理した署名鍵による公的な PKI ベースのデジタル署名による否認防止。
運用	SOAL2	運用正当性の説明	遵守する運用規定の公開と、ISMS 認証の取得。

次に表 3-9 に示す各リスクの影響度と発生頻度によるリスクマトリクスを使い、リスクのレベルを最高・高・中・低・最低の 5 段階で判定する。各リスクレベルを表 3-10 に示す。

表 3-9　リスクマトリクスの例

発生頻度＼影響度	影響大	影響中	影響小
高（時々）	最高リスク	高リスク	中リスク
中（まれ）	高リスク	中リスク	低リスク
低（ほぼない）	中リスク	低リスク	最低リスク

表 3-10　リスクレベル

リスクレベル	次の対応
最高リスク	最高優先度でより詳細にリスク分析をおこない見直す必要がある
高リスク	早急に詳細なリスク分析をおこない見直す必要がある
中リスク	より詳細なリスク分析をおこない見直す必要がある
低リスク	時間が許せばより詳細なリスク分析をおこない見直す、想定している保証レベルが低ければ残留リスクとできる場合もある
最低リスク	想定している保証レベルが低ければ残留リスクとすることも可能ではあるが、リスクがゼロではなく時間があるならばより詳細なリスク分析をおこない見直す

リスクマトリクスで得られたリスクレベルが高い方から時間が許す限り詳細にリスクの分析をおこなう。

3.3.3. 電子署名のリスク評価

リスク分析結果としてリスクレベルが出てくるので、次のステップとしてリスク毎のリスクレベルが署名保証レベル（SxAL）として許容可能かどうかを評価する。リスク評価の結果として対応が必要な（許容不可な）リスクをリストアップされる。表 3-11 にリスクアセスメントのまとめ方の例を示す。なお、中リスク以上の場合には影響度を被害額により評価することが望ましい。

表 3-11　リスクアセスメントのまとめ方の例

段階	リスク項目	頻度	影響度	評価結果	補足事項
登録	身元確認の不備				
	なりすまし登録				
	署名クレデンシャル誤紐付け				
	外部委託の信頼性				
	外部発行の署名クレデンシャルの不備				
	更新時の情報消失				
	プライバシー侵害				
	低い利便性/UX				
署名	署名クレデンシャル管理不備				
	通信経路不備によるなりすまし				
	通信経路不備による改ざん				
	署名時刻の偽装				
	誤操作による				
	ローカル署名時の不正				
	低い利便性/UX				
検証	署名意思の否認				
	署名対象の否認				
	署名時刻の否認				
	証明書の有効性不足				
	技術の危殆化				

	プライバシー侵害				
	属性フレッシュネス				
	事業者の信頼性不足				
	検証手順の信頼性不足				
	検証器の信頼性不足				
運用	運用正当性の説明				
	内部不正操作				
	担当者なりすまし				
	操作記録の欠如				
	不正侵入・改ざん				
	バックアップ復元不備				
	事業者廃業やサービス停止				
※ 分析結果としてリスクレベル（最高・高・中・低・最低）を、評価結果として対応の必要性の有無を記載する。					

3.4. ステップ２：基本策と最終保証レベルの決定

ステップ１の成果物であるリスクアセスメントの評価結果をベースとして、リスク対応が必要なリスクへの対策の検討と、各種要因としてプライバシー・公平性・利便性・脅威を配慮した調整をおこない、基本策と最終保証レベルを決定する。

3.4.1. 電子署名のリスク対応

ステップ１のリスク評価結果として「対応が必要とされたリスク」をリストアップして各リスクへの対応を検討する。リスク対応には表 3-12 に示すように大きく分けて、回避（Avoid）・軽減（Mitigate）・移転（Transfer）・受容（Accept）の４種類がある。許容できないリスクが残った場合には、保証レベル自体を下げる等の根本的な対応が必要となる。すべてのリスクが許容できるレベルになることで、リスク対応を終了することができる。

表 3-12　リスク対応の種類

リスク対応	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）	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。

リスクの回避は、リスクの原因となっている操作や機能を利用しないことで、リスク自体を回避する。リスクの原因となっている操作や機能が本当に必要なのか検討して判断する。例えば、安全性が低下している暗号方式の場合に、非サポートとすることでリスクを回避するような対応となる。

リスクの軽減は、影響度や発生頻度を低下させる新たな対策を追加することで対応する。例えば、知識認証要素の安全性を強化するために、2 段階認証や知識の複雑さを増やすような対応となる。

リスクの移転は、リスク自体を第三者に移転することでの対応となる。例えば、金額的な損害に対して保険を利用することや、当人認証のような機能の一部を外部の ID プロバイダに任せるような対応となる。

リスクの受容は、リスクが発生する可能性や影響を認識したうえで、特に対策を講じずにそのリスクを受け入れる選択となる。リスクの受容には「受動的受容（そのまま放置）」と「能動的受容（予算化・計画化して損失発生時に備える）」がある。能動的受容とは、例えば損失を予想してリスク予備費を設定するような対応となる。

リスクの回避・軽減・移転・受容ができない場合には、根本的に求める保証レベルの見直しを含めて検討する必要がある。

3.4.2. プライバシー・公平性・利便性・脅威による調整

SSP は、プライバシー（Privacy）・顧客体験（Customer Experience）・脅威（Threat）の 3 つの観点から初期署名保証レベルを見直す。

- プライバシー（Privacy）：SSP の管理の対象となる個人と、SSP が関連する組織または第三者の影響を受ける個人の、プライバシーに対して意図しない結果を生じるかどうかを判断して見直すこと。
- 顧客体験（Customer Experience）：保証レベルの実装がサービス利用者に過度な障壁や負担を与えないかを評価する。すべての利用者（能力・リソース・技術アクセス・経済状況を問わず）がサービスを受けられる経路を確保することが求められる。一般には保

証レベルが上がると顧客体験は低下する傾向がある。

- 脅威（Threat）：選択した SxAL が、環境・脅威要因・既知の戦術・技術・手順に対応できているか判断して見直すこと。

SSP は更に本ガイドラインに記載されていない目的や独自の考慮事項を完全に把握する為に必要に応じてそれらのリスク評価をするべきである。この評価には基準策に対する代替策や追加策も含まれなければならない。

3.4.3. 基本策の策定と代替策と追加策の検討

調整を経て、複数の選択肢がある場合にはどれを採用するか決定し、最終的に基本策として具体的な手順と対策を整理する。またリスクアセスメントの結果として採用はされなかったが有用な方策があれば、代替策や追加策として整理しておくことで、将来のリスクを減らすことが可能となる場合がある。

代替策とは、何らかの理由により基本策が利用できない場合に利用する方策である。例えば、利用している認証要素の危殆化や、利用者に障害があり基本策が使えない場合等、が考えられる。特別に認められる理由がない場合、代替策を用いた場合においても署名保証レベルは維持する。

追加策とは、署名サービスに攻撃等があった場合に、一時的に追加の対策を用いてセキュリティレベルを上げる場合に利用する方策である。例えば、身元確認に利用する属性の信頼性が低下した場合に要求する追加の属性や、署名クレデンシャルの脆弱性発覚時に要求する追加の認証要素等、が考えられる。その結果として署名保証レベルが上がることもあるので基本策との差異を明確にしておく。表 3-13 に各策の説明を示す。

表 3-13　基本策・代替策・追加策の説明

種類	意味
基本策	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。

3.4.4. 最終的な保証レベルの決定と残留リスク

初期保証レベルに対して見直しをおこなった結果を、最終的な署名保証レベルとして決定する。決定する際に表 3-14 に示すような表を利用して記録を残すことを推奨する。

表 3-14　初期署名保証レベルと最終署名保証レベルの比較表

保証種別	初期署名保証レベル	最終署名保証レベル
SIAL:署名者身元保証レベル	低:AL1 / 中:AL2 / 高:AL3	低:AL1 / 中:AL2 / 高:AL3
SPAL:署名プロセス保証レベル	低:AL1 / 中:AL2 / 高:AL3	低:AL1 / 中:AL2 / 高:AL3
SDAL:署名データ保証レベル	低:AL1 / 中:AL2 / 高:AL3	低:AL1 / 中:AL2 / 高:AL3
SOAL:サービス運用保証レベル	低:AL1 / 中:AL2 / 高:AL3	低:AL1 / 中:AL2 / 高:AL3

残留リスク（Residual Risk）とは、最終的に残ったリスクであり、SSP として受容（Accept）したリスクのことである。残留リスクは受容した根拠も含めて文書化して残しておく。

3.5. ステップ３：文書化（SSAS/SSPS 作成）

署名サービスのリスク管理のプロセスの記録としての SSAS と、利用者に運用方法を提示する SSPS は、作成すべきである。署名サービス選択時の判断基準とするため SSPS は公開することが望まれる。

3.5.1. 署名サービス承認規定（SSAS）の作成と保管

署名サービス承認規定（SSAS: Signature Service Acceptance Statement）は、署名サービスのリスク管理におけるプロセスの過程と結果を記載した文書である。これには、全ての ESRM ステップの出力と記録が含まれる。SSAS には以下を含めること。

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

SSAS を公開することは求められないが保管をしておき、定期的な再評価と改善の実施時に利用する。

3.5.2. 署名サービス運用規定（SSPS）の作成と公開

署名サービス運用規定（SSPS: Signature Service Practice Statement）は、選択した署名保証レベル（SxAL）により決定された運用内容を記載した文書である。当人型ローカル署名方式では CP/CPS（RFC 3647）に相当する文書であり、以下に相当する内容を網羅することが望ましい。

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

SSPS は常に最新版を用意し、SOAL2/SOAL3 の場合には公開し利用者に提示する。公開することで利用者は自身のリスクを理解して署名サービスを選択することができるようになる。

また付属書 A にある「署名保証レベル適合宣言書」も SSPS の 1 つである。「署名保証レベル適合宣言書」も公開されることが望ましい。

3.6. ステップ４：署名サービス運用と再評価

3.6.1. 署名サービスの運用

最終保証レベルが決定したら署名サービスを開発実装し、運用規定に従って署名サービスの運用を開始する。SOAL2/SOAL3 の場合には SSPS も署名サービスの開始時には公開等、利用者・依拠者への提示をおこなう必要がある。

3.6.1. 署名サービスの再評価

署名サービスに対する脅威・利用者のニーズ・法的な要件等は常に変化している。定期的に署名サービスのリスク管理のプロセスをおこなうことで、その時代に合った署名サービ

スの保証を選択するべきである。

外部の、身元確認プロバイダ（ISP）や検証サービスプロバイダ（VSP）を利用する場合には影響評価が複雑になる可能性があるが、定期的な再評価は契約または法的な仕組みの中で考慮されるべきである。

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

付属書 B. 承認目的署名と発行元保証署名（参考情報）

B.1. 電子署名の３要素

電子署名が必要とする要素としては表 B-1 に示すように「本人性（Identity)」と「完全性（Integrity)」「承認意思（Approval)」との３つがある。なお承認意思は否認防止（Non-repudiation）と呼ばれることもある。本ガイドラインの「2.2 章 電子署名の定義」では「本人性（Identity)」と「承認意思（Approval)」の２つを合わせて「本人の意思」としている。

表 B-1　電子署名の３つの目的

要素	利用目的と一般的な保証方法
本人性：Identity	署名者が身元確認済みの誰であるかの保証 ※ 通常は、署名に紐づいた第三者により発行された証明書等で保証される。
完全性：Integrity (非改ざん：Anti-Tamper)	署名時より改ざんされていないことの保証 ※ 通常は、ハッシュ値や署名値等の暗号技術やアクセス制御された運用等で保証される。
承認意思：Approval (否認防止：Non-repudiation)	署名者が内容に同意し承認したことの保証 ※ 通常は、運用規定に定められ署名者が管理するクレデンシャル（署名鍵等）の行使や、第三者に保証された承認手続きの記録（ログ）等で保証される。

B.2. 電子署名と e シール

一般に「e シール」の技術としては、デジタル署名と PKI（公開鍵基盤）が使われている。その意味では「e シール」は技術的には PKI ベースの「電子署名」と同じである。両者の違いは、電子署名では電子証明書の発行先の識別名（Subject）が自然人であるが、e シールでは電子証明書の発行先が法人等（非自然人）である点である。表 B-2 にて電子署名と e シールを比較する。

表 B-2　電子署名と e シール

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。 承認目的署名に利用されることが多い。
e 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。

電子署名では一般に署名者は自然人であり、後述する承認目的署名に用いられることが多い。eシールでは署名者はシステムやプログラムまたは組織より権限を与えられた自然人であり、後述する発行元保証署名に用いられることが多い。ただし、電子署名であってもシステムにより自動署名される発行元保証署名に用いられることもあり、「eシール的な使い方」と呼ばれる場合がある。またeシールであっても権限がある自然人が承認目的署名として用いることもある。つまり、電子署名・eシールと承認目的署名・発行元保証署名は別の定義であり、電子署名が承認目的署名と同じであり、eシールが発行元保証署名と同じである、と言うわけではない。電子署名とeシールの違いは基本的には電子証明書のSubject（発行先）が自然人か非自然人かの属性的な差異であり、承認目的署名と発行元保証署名の違いは目的や用途の差異である。

B.3. 承認目的署名と発行元保証署名

電子署名においては、本人性・完全性・承認意思の3要素は必須となるが、用途やユースケースによりこのうちのどの要素を特に重視する（目的とする）かが分かれる。例えば電子契約のような用途においては、完全性も必要となるが本人性と承認意思による「本人の承認意思」が特に重要となる。またeシールによる発行文書の保証のような用途においては、承認意思も必要となるが本人性と完全性（非改ざん）による「発行元の保証」が特に重要となる。本ガイドラインでは、「本人の承認意思」を主目的する場合を「承認目的署名（Approved Signature）」と呼び、「発行元の保証」を主目的とする場合を「発行元保証署名（Origin Assurance Signature）」と定義する。用途によっては承認目的署名と証明目的署名の両方を、同じ程度重視する場合もあるが、主目的の違いにより求められる要件が異なる場合があるので、ここでは分けて説明をする。

承認目的署名は電子署名法が意図している署名と言える。一般に承認目的署名の場合、署名実行の主体は自然人であり、定められた署名手順に従い内容を確認した上で署名実行の認可を与えることになる。本ガイドライン中で電子署名とある場合は承認目的署名を意図している。

発行元保証署名はeシールが意図している署名と言える。自らが発行する文書の内容を発行元として保証する目的では、自動的に署名実行がされることが多い。この場合であっても全く署名実行の認可をしていない訳ではなく、事前に定められたルールに従って署名実行を認可していることになる。もちろん発行元保証署名であっても、都度内容を確認して署名実行の認可を与えても良い。なお、発行元保証署名の目的にかんがみると契約書等の意思表示にあたっては発行元保証署名はもちいられないことになる。

表 B-3 に承認目的署名と発行元保証署名の比較をまとめる。

表 B-3　承認目的署名と発行元保証署名の比較

	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	主に組織（法人や部署等）
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	署名者（発行者）による内容の保証と非改ざん ※　主に本人性と完全性
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

付属書 C. 電子委任（参考情報）

現実世界において「委任」とは、委任者が受任者に対して権利行使や意思表示等の行為を委任し、申請や取引等を受任者が委任者に代わって「代理」や「代行」をおこなうことである。委任者と受任者の関係は、委任契約・委任状・内規等で保証される。代理をおこなう代理人へは、委任者より委任状や委任契約等により代理権が与えられる。代理人は与えられた代理権により、委任者に代わって交渉等において自ら判断をおこない意思表示を行うことができる。代理人は代理人名義で意思表示し、その効果は委任者本人に生じることになる。代理人・代理権については法的にも定義されている。一方で代行は代理と異なり明確な定義はない。一般には代行では代理と異なり受任者自身が判断をおこなう権限は与えられていない。表 C-1 に現実世界の委任・代理・代行の整理を示す。

表 C-1　現実世界の委任・代理・代行の整理

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。

電子世界の委任を電子委任（Electronic Mandate）とする。電子世界では利用者を ID 等の識別子（Identity）にて識別する。つまり電子委任は、委任者 ID と受任者 ID の委任関係を示す紐付けと、その間の委任権限と整理することができる。電子世界において代理と代行の区別は委任権限の内容に依存する。受任者が委任者に代わって自ら判断をおこない意思表示が可能となる委任権限では代理と言えるが、電子委任を利用するシステムにおいて代理と代行を区別する必要性は低い。本ガイドラインでは電子委任を代理と代行の区別ではなく委任権限の違いとして整理する。また委任情報を、委任関係と委任権限の 2 つに整理する。

電子世界において、受任者が委任者 ID をそのまま利用するようなケースも考えられる。この場合は、利用サービスから見ると実体が別人であっても委任者として見えてしまい区別ができないためにここではスコープとしない。ここでは受任者が自身の受任者 ID

により利用サービスを利用した上で、委任者より委任された電子委任の行為をおこなうケースを前提とする。

C.1. 電子委任のモデル

電子委任を実現する方法は、委任情報を電子委任状（ePoA：Electronic Power of Attorney）として添付して得る方法（委任状モデル）と、委任情報を電子委任サービス事業者（EMSP：Electronic Mandate Service Provider）に問合せて得る方法（問合せモデル）がある。ここでは委任情報を取得して利用する電子申請や電子取引等のサービスを電子委任利用サービス（EMRS：Electronic Mandate Relying Service）と呼ぶ。図 C-1 に電子委任サービス事業者を使った利用モデル例を示し、表 C-2 にて手順を示す。

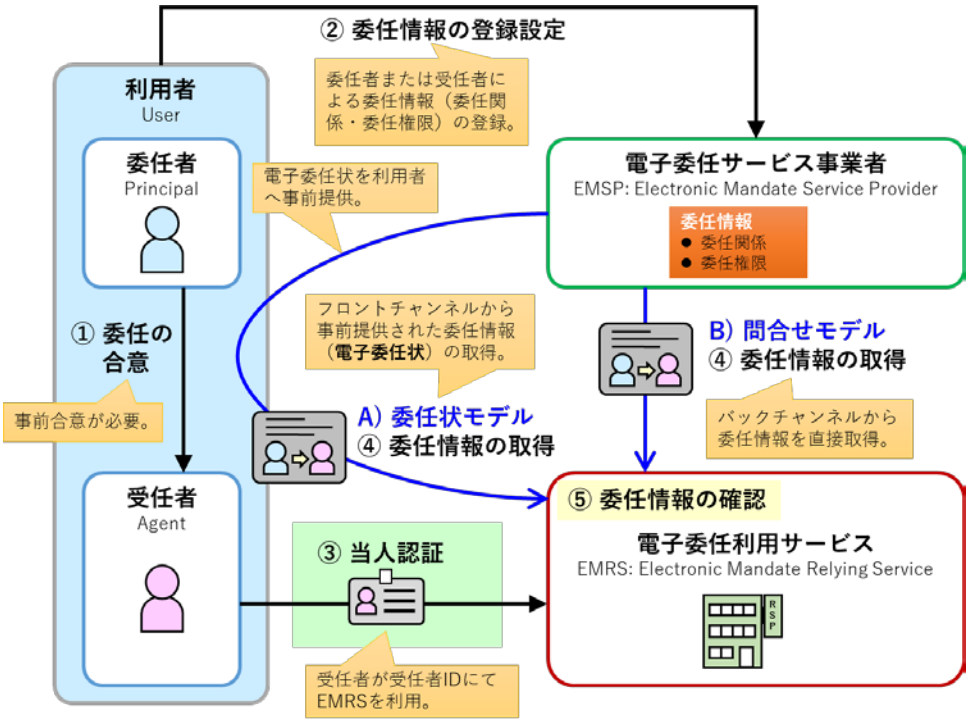

図 C-1　電子委任サービス事業者を使った利用モデル例

表 C-2　電子委任サービス事業者を使った利用モデル例の手順

手順	説明
①　委任の合意	事前に委任者と受任者が委任について合意する必要がある。
②委任情報の登録	EMSP を使う場合には EMSP に委任情報を登録する。 ※　委任状モデルの場合には EMSP は電子委任状を発行する。
②　当人認証	受任者が受任者 ID を使い EMRS にて当人認証をおこなう。
④委任情報の取得	A）委任状モデルの場合には電子委任状（委任情報）を添付する。

	B）問合せモデルの場合には提示された受任者 ID と委任者 ID を使い EMSP へ問合せして委任情報を取得する。
⑤委任情報の確認	委任情報から委任関係と委任権限を確認する。

委任状モデルで利用する電子委任状には PKI ベースの電子証明書を使ったデジタル署名を利用するケースが多い。一方で問合せモデルは当人認証で得られた ID を利用するケースが多い。その意味では、委任状モデルは電子署名をベースとしたモデルあり、問合せモデルは電子認証をベースとしたモデルと言える。表 C-3 にて委任状モデルと問合せモデルの整理を示す。

表 C-3　電子委任の利用モデルによる分類

種類	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。

委任状モデルにおいて、EMSP を使わずに委任者自身の電子証明書を使って電子委任状に電子署名する場合がある。これは委任者の電子証明書を発行した認証局を信頼する電子署名のローカル署名方式に近いモデルと言える。この EMSP を利用しないモデルにおいては電子委任状のフォーマットを電子委任状を受け取った EMRS が読み取ることができることが必要となる。

C.2. 委任情報（委任関係と委任権限）

どのような電子委任のモデルであっても委任を判断する EMRS が必要とする情報は、委員者と受任者の関係を示す委任関係の情報と、受任者がおこなえる操作を定めた委任権限の情報の、2 つとなる。委任関係の情報が含むべき属性として、最低でも委任者 ID と受任者 ID が必要となる。受任者に資格が必要である場合には受任者の資格を示す属性を含む場合もある。委任権限の情報が含むべき属性は決められたものはないが、無制限の委任ではない限り何らかの委任権限の属性は必要となる。委任権限を何も設定しない場合であっても、例えば暗黙の了解として利用する EMRS 内の利用に限る等の整理は必要であろう。

表 C-4 にて委任情報である委任関係と委任権限の概要を示す。

表 C-4　委任情報の概要

項目	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。EMRS 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。
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、EMRS 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。

EMRS が受け取った委任情報をどのように信頼するかと言う問題がある。委任状モデルの場合には PKI ベースのデジタル署名を使った電子署名を利用する場合が多い。この場合に電子署名を付与する主体は委任者または電子委任状を発行した EMSP となる。EMSP による電子署名は事業者署名方式と言える。問合せモデルの場合には、問合せ先である EMSP を信頼していれば受領した委任情報をそのまま信頼することもできるが、EMSP によりデジタル署名をした委任情報を渡すことで発行元保証署名をすることでより安全となる。

サービス間で交換する ID 情報（アサーション）の保証については、NIST SP 800-63C「Federation and Assertions」において技術要件が整理されており、連携情報保証レベル FAL（Federation Assurance Level）が定義されている。サービス間の情報保証と言う意味では委任情報の連携時においても参考となる。NIST SP 800-63-4 から情報連携のエッセンスを抜き出すと、まず連携する情報にはデジタル署名による発行元保証が要求されている。また信頼合意（Trust Agreement）と呼ばれる、IdP（EMSP）と RP（EMRS）の間で事前または動的（連携時）におこなわれる合意形成についても要求されている。委任状モデルではフロントチャンネルにて委任状（委任情報）が渡されるが、この場合でも EMSP と EMRS の間における信頼合意は必要となる。

付属書 D. トラスト設計（参考情報）

トラストと言う言葉は多様なケースで利用されるが、ここではトラストを利用者から見た信頼性とする。ここではトラスト（信頼性）設計を、サービスやシステムの利用者に信頼してもらうための仕組みやルールの検討と仕様策定をおこなう。トラスト設計時の基本的な考え方を示す。まず、トラストの仕組みは後付けではなくシステム設計段階から考慮され組み込む。次に、第三者により検証可能であり仕組みやルールの透明性を確保する。最後に、サービスやシステムが提供する予定のトラストに対して適切な信頼基点（トラストアンカー）を選択する。これを表 D-1 で示すようにトラスト設計の 3 原則とする。

表 D-1 トラスト設計の 3 原則

設計段階で組み込む Trust by Design (TbD)	サービスやシステムの設計をおこなう時にプライバシーやセキュリティと同時にトラストの設計もおこなう。
第三者により検証可能 Verifiable and Auditable	第三者からの信頼を得るためには検証可能であることと仕組みやルールの透明性が確保されている必要がある。
適切な信頼基点選択 Selection of a Trust Anchor	信頼基点をどこに置くか、また求められているトラストのレベルに対して必要十分な内容か検討する。 ※ 必要以上に高いトラストレベルでないかも検討。

D.1. トラストの設計段階からの組み込み

例えば十分なトラスト設計がおこなわれなかった電子署名サービスにおいて、署名者が署名意思を否認したような場合に、後から電子データやシステムから証拠を抽出・解析する技術と手法であるデジタル・フォレンジック等の実施が必要となる。事前にトラスト設計をおこなうことで、否認のようなインシデント時の対応として適切な情報や保証を提供することが可能となる。近年では設計時にプライバシー保護やセキュリティ対策のリスク管理や組み込みすることが求められているが、トラスト保証の組み込みも同様に実施されるべきである。

トラスト（信頼）の対象はシステム全体ではあるが、トラストを必要とする要素として、アイデンティティ（ID）・プロセス・データの 3 つが特に重要となる。に分けてトラスト設計をおこなうことができる。アイデンティティ（ID）を保証する技術が身元確認であり、プロセスを保証する技術が当人認証（電子認証）であり、データを保証する技術が電子署名と言える。これら 3 要素は相互に関連しており総合的に見てトラスト設計をおこなう。また本ガイドラインや NIST SP 800-63 で解説されているような保証レベルの観点でも、適切な保証レベルを選択すべきである。表 D-2 にてトラスト要素の種類を整理する。

表 D-2　トラスト要素の種類

トラスト要素	保証技術	概要
アイデンティティ （身元）	身元確認	身元確認によりアイデンティティ（ID）を保証。 ※ 保証レベルとして SIAL や IAL がある。
プロセス （処理）	当人認証 （電子認証）	当人認証とセッションによりプロセスを保証。 ※ 保証レベルとして SPAL や AAP がある。
データ （情報）	電子署名	対象データに署名データを加えてデータを保証。 ※ 保証レベルとして SDAL がある。

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。一方で「Digital Identity（デジタル ID）」は NIST SP 800-63-4 において「特定のコンテキスト内でサブジェクトを一意に説明する属性または属性のセット」とされており、意味としては認証よりもアイデンティティに主眼が置かれた言葉となっている。以上の経緯を理解した上で、用途や法的な意味である電子署名と技術的な意味であるデジタル署名と区別していることに対比することを考えて、本ガイドラインでは「電子認証」を用途や法的な意味として用いるものとする。

D.2. 第三者による検証可能な仕組みと透明性

サービスやシステムの利用者および外部の第三者に対して、検証可能な仕組みやルールを提供する（透明性を確保する）ことでトラスト（信頼）を担保することができる。このためには幾つか方法があるが、標準化された検証可能なトラストの仕組みやルールの採用や、内容が公開されている監査や認定を得る、暗号技術の利用による証拠性の確保等がある。

標準化された仕組みやルールは専門家が評価して確認した上で認められた仕様となっており信頼性が高いと言える。逆に独自の仕組みやルールは専門家の評価を経ていない場合も多く注意が必要となる。また採用した仕組みやルールは外部公開されることで透明性を得ることができる。

公的または業界として認められている監査や認定の制度があれば利用することで仕組みやルールを第三者に公開することで高い信頼性を提供することが可能となる。コスト面等

も含めて許されるのであれば、利用可能な制度の有無を含めて検討すべきである。

D.3. 適切な信頼基点の選択

無条件にトラスト（信頼）を得ることは難しいために、通常は信頼基点（トラストアンカー）を信頼することでトラストを担保する。なおサービスやシステムによっては複数の信頼基点を必要とする場合がある。例えば PKI ベースの電子署名であれば署名者証明書とタイムスタンプ証明書の信頼基点が異なる場合もある。また身元確認の場合も国民 eID カードであったりその他属性であったりと信頼基点が異なる場合がある。どこに信頼基点が必要であるかを検討して選択する。

信頼基点のレベルも考える必要がある。一般には信頼された第三者を信頼基点することでトラストを担保する。例えば本人が内容の保証を主張しても、その内容がその当人の利益になるような場合には、他者からの信頼を得ることは難しい。自己署名の電子証明書が良い例である。利用者自身による自己署名の電子証明書はオレオレ証明書と呼ばれ、利用者自身が信頼を自己主張するものでありトラストとしてのレベルは低い。電子証明書であれば運用や仕様が決められかつ遵守している PKI ベースの認証局（CA）が発行した場合には、信頼された第三者の保証となり、信頼性が高くなる。更にその認証局が認定を受けているような場合に最も高いトラストを担保することができる。サービス事業者自身が信頼基点となることもある。この場合にはサービス事業者が信頼基点として信頼できるかどうかが検証可能である必要がある。サービス事業者がどのような範囲や内容を保証するのか等は公開して第三者によって検証可能とすべきである。

近年ではサービス全体を保証する仕組みとして、トラストフレームワークや信頼基点をリストとして管理するトラストリスト（トラステッドリスト）の提供がおこなわれるようになっている。しかしこれらも最終的には何らかの信頼基点に依存している。例えばトラストリストであればリスト自体に PKI ベースのデジタル署名されていることが多く、そのデジタル署名の信頼基点を信頼する必要がある。しかしながら必要となる信頼基点を減らすことは可能となる。

高いレベルの信頼基点の採用することは利便性やコストの面で不利になる場合もある。サービスやシステムが提供するトラストのレベルに応じた信頼基点の選択をする。いたずらに高いレベルは求めるべきではない。

略語

本ガイドラインで利用している略語のフルスペルと日本語訳を以下に示す。

略語	フルスペル	日本語訳
AAL	Authentication Assurance Level	当人認証保証レベル
API	Application Programming Interface	アプリケーション・プログラミング・インターフェイス
AuthN	Authentication	当人認証
AuthZ	Authorization	認可
CA	Certificate Authority	認証局
CAdES	CMS Advanced Electronic Signature	CMS 長期署名（※1）
CMS	Cryptographic Message Syntax	暗号化メッセージ構文
CP	Certificate Policy	証明書ポリシー
CPS	Certification Practice Statement	認証運用規程
CRL	Certificate Revocation List	証明書失効リスト
CSP	Credential Service Provider	クレデンシャルサービス事業者
DIRM	Digital Identity Risk Management	デジタル ID リスク管理
DS	Digital Society	デジタル社会推進標準ガイドラインの略称
eID	electronic identification	電子 ID / EU No 910/2014
EMRS	Electronic Mandate Relying Service	電子委任利用サービス
EMSP	Electronic Mandate Service Provider	電子委任サービス事業者
ePoA	Electronic Power of Attorney	電子委任状
ESRM	Electronic Signature Risk Management	電子署名リスク管理
EU	European Union	ヨーロッパ連合
FAL	Federation Assurance Level	連携情報保証レベル
FIPS	Federal Information Processing Standards	連邦情報処理標準
HSM	Hardware Security Module	ハードウェア・セキュリティ・モジュール（装置）
IA	Issuing Authority	発行局
IAL	Identity Assurance Level	身元確認保証レベル
IC	Integrated Circuit	集積回路
ID	Identity	アイデンティティ（Identification 等

		の略としても利用される）
IdP	Identity Provider	アイデンティティプロバイダ（本ガイドラインでは ISP と同じ）
IEC	International Electrotechnical Commission	国際電気標準会議
ISF	Identity Service Function	身元保証サービス機能
ISO	International Organization for Standardization	国際標準化機構
ISP	Identity Service Provider	身元保証サービス事業者
JAdES	JSON Advanced Electronic Signature	JSON 長期署名（※1）
JIS	Japanese Industrial Standards	日本産業規格
JNSA	Japan Network Security Association	日本ネットワークセキュリティ協会
JSON	JavaScript Object Notation	JavaScript オブジェクト記法
JWS	JSON Web Signature	JSON ウェブ署名
JWT	JSON Web Token	JSON ウェブトークン
KYC	Know Your Customer	顧客の身元確認
NIST	National Institute of Standards and Technology	米国立標準技術研究所
OCSP	Online Certificate Status Protocol	オンライン証明書状態確認プロトコル
PAdES	PDF Advanced Electronic Signature	PDF 長期署名（※1）
PDF	Portable Document Format	ポータブル・ドキュメント・フォーマット
PIN	Personal Identification Number	個人識別番号
PKCS	Public Key Cryptography Standards	公開鍵暗号規格群
PKI	Public Key Infrastructure	公開鍵基盤
PoP	Proof of Possession	所有証明
RA	Registration Authority	登録局
RP	Relying Party	サービス提供者（IdP とペアで使われる）
RSSP	Remote Signing Service Provider	リモート署名サービス事業者
SAG	Signature Assurance Guidelines	署名保証ガイドライン
SAML	Security Assertion Markup Language	セキュリティアサーション記述言語
SDAL	Signature Data Assurance Level	署名データ保証レベル
SIAL	Signer Identity Assurance Level	署名者身元保証レベル

SNS	Social Networking Service	ソーシャル・ネットワーキング・サービス
SOAL	Service Operation Assurance Level	サービス運用保証レベル
SP	Special Publication	特別出版物（NIST 発行の技術ガイドライン等）
SPAL	Signing Process Assurance Level	署名プロセス保証レベル
SSAS	Signature Service Acceptance Statement	署名サービス承認規定
SSF	Signature Service Function	署名サービス機能
SSP	Signature Service Provider	署名サービス事業者
SSPS	Signature Service Practice Statement	署名サービス運用規定
SxAL	Signature Assurance Level	署名保証レベル
TbD	Trust by Design	トラスト設計
TFP	Trust Framework Provider	トラストフレームワーク事業者
TSA	Time Stamping Authority	時刻認証事業者
UI	User Interface	ユーザーインターフェース
USB	Universal Serial Bus	汎用シリアルバス
UX	User Experience	利用者体験
VA	Validation Authority	検証局
VSF	Verification Service Function	検証サービス機能
VSP	Verification Service Provider	検証サービス事業者
XAdES	XML Advanced Electronic Signature	XML 長期署名（※1）
xAL	Digital Identity Assurance Level	デジタル ID 保証レベル
XML	eXtensible Markup Language	拡張可能マークアップ言語

※1　CAdES/JAdES/PAdES/XAdES は、現在は略語ではなく固有名詞とされており、例えば PAdES であれば PAdES Digital Signature というような使い方がされる。これは Digital Signature と Electronic Signature を明確に使い分けるためである。

用語定義

多くの用語には複数の定義がありうるため、本ガイドラインで利用している用語の定義を以下に示す。

用語	定義
電子署名 **(Electronic Signature)**	広い意味で電子署名とは、電磁的記録（電子データ）に関連付けられ、検証により確認可能な、電子的措置。この措置に主に求められるのは、電磁的記録に証拠としての効力を持たせる事で、「本人の意思」と「非改ざん」の 2 つを備える必要がある。実装には、デジタル署名と PKI を使う方式や、認証技術を使った方式等、様々な方式がある。[JNSA SAG-1（本書）2.2 章 参照]
デジタル署名 **(Digital Signature)**	電子署名の一種で、署名者による署名後にデータが改ざんされていない事を、公開鍵暗号等の暗号技術を使って検証できる技術。本ガイドラインではデジタル署名を技術用語としており電子署名とは使い分けている。[JNSA SAG-1（本書）1 章 参照]
長期署名 **(Long-Term Signature)**	署名に用いられた電子証明書の有効期間満了後または失効後であっても、当該署名の真正性および有効性を延長し長期間にわたり検証可能とするための情報を付加した署名仕様。[ISO 14533 シリーズ参照]
運用ポリシー **(Operation Policy)**	署名等のサービスを安全かつ信頼性高く運用するためのルールや手順を定めた文書。[JNSA SAG-1（本書）2.3.4 章 参照]
証明書ポリシー **(CP)**	認証局が発行する電子証明書の身元確認手順や利用可能な用途等のルールや手順を定めた文書であり、通常認証局より公開される。[RFC 3647 参照]
認証運用規程 **(CPS)**	証明書ポリシーで規定された内容を、認証局がどのように運用するのかを定めた文書であり、通常認証局より公開される。[RFC 3647 参照]
署名サービス承認規定 **(SSAS)**	署名サービスのリスク管理におけるプロセスの過程と結果を記載した文書。[JNSA SAG-1（本書）3.5.1 章 参照]
署名サービス運用規定 **(SSPS)**	署名サービスが選択した署名保証レベルで示される内容を、署名サービスがどのように運用するのかを定めた文書。[JNSA SAG-1（本書）3.5.2 章 参照]

e シール (Electronic Seal)	電子署名では所有者(Subject)は自然人であるが、 e シールでは所有者は自然人では無く法人等の組織となる。e シールはデジタル署名と PKI を使い、PKI ベースの電子署名と技術的には同一である。[JNSA SAG-1（本書）付属書 B.2 章 参照]
公開鍵基盤（PKI）	デジタル署名を利用して、公開鍵暗号を安全かつ信頼して利用するための仕組み全体（制度・技術・運用）を指す。認証局が発行した X.509 電子証明書を利用して、署名者の身元を保証することができる。[RFC 5280 参照]
認証局（CA）	申請者の身元を確認して、X.509 電子証明書を発行と失効をおこなう機関。 [RFC 5280 参照]
登録局（RA）	認証局業務のうち、証明書発行申請を受け付け、申請内容の審査および主体情報の確認を行い、その結果を IA（または CA）に通知する機関。[RFC 5280 参照]
発行局（IA）	認証局業務のうち、登録局からの承認情報に基づき、X.509 電子証明書を生成し、署名して発行する機関。
検証局（VA）	認証局業務のうち、X.509 電子証明書の有効性（失効状態、期限等）を確認するための検証サービスを提供する機関。
身元確認 (Identity Proofing)	申請者が主張する身元属性を検証して信頼できることを確認して利用者と認めるプロセス。[NIST SP 800-63 参照]
当人認証 (Authentication)	利用者が提示する認証属性を検証して身元確認済みの当人であることを認めるプロセス。[NIST SP 800-63 参照]
認可 (Authorization)	利用者が資源や操作をおこなう資格があるかを確認して認めるプロセス。[NIST SP 800-63 参照]
署名認可 (Signature Authorization)	署名者(利用者)が、署名対象の内容を確認して署名をおこなうことを認めるプロセス。[JNSA SAG-1（本書）2.3.2 章 参照]
署名者身元保証レベル (SIAL)	署名サービスの申請者が主張する本人であるかどうかを確認した確からしさを保証するレベルを示す。IAL とほぼ同じ内容となる。[JNSA SAG-1（本書）2.4.1 章 参照]
署名手順保証レベル (SPAL)	端末の前にいる署名者（利用者）が身元確認済みの当人であり署名対象の内容を確認して承認する署名プロセスの確からしさを保証するレベルを示す。[JNSA SAG-1（本書）2.3.2 章 参照]
署名データ保証レベル (SDAL)	検証者が検証に利用する署名データ自体の確からしさを保証するレベルを示す。署名データを用いた検証手順は事前に

	決められている必要がある。[JNSA SAG-1（本書）2.3.3 章参照]
サービス運用保証レベル（SOAL）	署名サービス運用規定（SSPS）等とその公開・監査・認定により、署名サービスの運用についての信頼性についての保証レベルである。[JNSA SAG-1（本書）2.3.4 章 参照]
身元確認保証レベル（IAL）	認証サービスの申請者が主張する本人であるかどうかを確認した確からしさを保証するレベルを示す。[NIST SP 800-63A 参照]
当人認証保証レベル（AAL）	端末の前にいる利用者が身元確認済みの当人であるかどうかを確認した確からしさを保証するレベルを示す。[NIST SP 800-63B 参照]
連携情報保証レベル（FAL）	サーバー間の連携（フェデレーション）において ID 情報の信頼性を保証するレベルを示す。[NIST SP 800-63C 参照]
時刻認証事業者（TSA）	電子データのハッシュ値に対し、信頼できる時刻情報を付与し、自らの電子署名を付してタイムスタンプトークンを発行することにより、当該データが特定時刻以前に存在していたことを第三者として証明する事業者。[RFC 3161 参照]
クレデンシャルサービス事業者（CSP）	利用者の本人確認に基づき、電子署名・認証・暗号等に用いる電子証明書や秘密鍵等のクレデンシャルを発行・管理・保護し、当該クレデンシャルを用いた信頼サービスを提供する事業者。[NIST SP 800-63 参照]
信頼基点／トラストアンカー（Trust Anchor）	サービスの利用者・検証者がサービスや仕組みの信頼性を判断する際の基点となる情報・証明書・サービス等のこと。信頼基点は、トラストフレームワークにおいて定義される信頼の起点であり、検証時の信頼の判断基準として利用される。
トラストフレームワーク（Trust Framework）	サービスの信頼性を確保するために、関係主体の役割、運用ポリシー、技術要件、保証レベル、ならびに監査・評価の仕組み等を体系的に定めた枠組み。トラストフレームワークに基づき、利用者および検証者はサービスの信頼性を判断することができる。PKI はトラストフレームワークの一例である。

参考文献

- 日本トラストテクノロジー協議会(JT2A) - リモート署名ガイドライン第 1 版
  https://www.jnsa.org/result/jt2a/2020/

- 日本ネットワークセキュリティ協会(JNSA) - デジタル署名検証ガイドライン V1.1
  https://www.jnsa.org/result/e-signature/2021/

- 日本ネットワークセキュリティ協会(JNSA) 電子署名 WG - 電子署名 Q&A
  https://www.jnsa.org/result/e-signature/e-signature-qa/

- 日本ネットワークセキュリティ協会(JNSA) - 長期署名プロファイル JIS 規格の発行について
  https://www.jnsa.org/result/e-signature/2025/standard/index.html

- NIST SP 800-63-4 - Digital Identity Guidelines
  https://pages.nist.gov/800-63-4/

- DS-511 行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン
  https://www.digital.go.jp/resources/standard_guidelines#ds511

- CSC API Technical Specifications
  https://cloudsignatureconsortium.org/resources/download-api-specifications/

- RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
  https://datatracker.ietf.org/doc/html/rfc5280

- RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
  https://www.ietf.org/rfc/rfc3161.txt

- RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
  https://www.ietf.org/rfc/rfc3647.txt

- ISO 31000（JIS Q 31000）- Risk management – Guidelines
  https://www.iso.org/standard/65694.html
  https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=JIS+Q+31000:2019

- ISO 31000（JIS Q 31000）- Risk management – Guidelines
  https://www.iso.org/standard/65694.html
  https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=JIS+Q+31000:2019

- IEC/ISO 31010（JIS Q 31010）- Risk assessment techniques
  https://www.iso.org/standard/72140.html
  https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=JIS+Q+31010:2022

- ISO/IEC 27000（JIS Q 27000）- Information security management systems
  https://www.iso.org/standard/73906.html
  https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=JIS+Q+27000:2019

- ISO/IEC 20000（JIS Q 20000）- Information technology - Service management
  https://www.iso.org/standard/70636.html
  https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=JIS+Q+20000:2020

変更履歴

JNSA SAG-1 :2026

- JNSA 署名保証ガイドライン（SAG）初版。2026 年発行。

作成メンバー（五十音順）

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）