民間電子サービスにおける真正性保証の解説書

2019 年 11 月

日本トラストテクノロジー協議会（JT2A）

真正性保証タスクフォース

目次

1 はじめに

日本工業規格 JIS Q 27000:2019「情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―用語」において、機密性（Confidentiality），完全性（Integrity），可用性（Availability），否認防止（Non-Repudiation），責任追跡性（Accountability），真正性（Authenticity）並びに信頼性（Reliability）を情報セキュリティの特性として定義している。真正性は、JIS Q 27000:2019 の中で『エンティティは，それが主張するとおりのものであるという特性。』と定義されている。一方、厚生労働省が発行している「医療情報システムの安全管理に関するガイドライン 第 5 版（平成 29 年 5 月）」では、『正当な権限において作成された記録に対し、虚偽入力、書換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であることである。』と定義しており、定義している規格や発行業界により、真正性の対象の広狭、浅深があることがわかる。

本解説書は、民間における電子サービスを対象とし、真正性の保証が求められるユースケースや電子サービスの利用、開発、運用時に真正性に関係するセキュリティ技術や実装方法をまとめ、真正性の一意な定義は定めず、5 章の中で、真正性に関連する特性を持つセキュリティ技術、実装方法を紹介することとする。

対象読者は真正性の保証が求められる民間電子サービスの利用者、開発者、運用者等を想定した。利用者は 3 章の真正性の保証が求められるケースの例にて各ユースケースで関係する法規則やガイドライン、利用される真正性保証に関する技術を確認、開発者、運用者は 4 章の真正性保証のレベルの定義にて、開発・運用するシステムの真正性保証レベルの確認や、5 章の真正性を保証するための実装方法にて、開発・運用するシステムに適用する真正性保証に関連する技術の選定等で利用いただきたい。

2 真正性とは

真正性は表 2-1 の通り、様々な規格や業界で定義されている。これらの定義を見ると、「主体や資源が、主張通りであること」が全てにおいて定義されており、規格や業界の背景や文化に依存し、追加の要件として定義されているように思われる。

表 2-1 各規格／ガイドラインの真正性の定義（2019 年 10 月現在）

規格／ガイドライン	定義
JIS Q 27000	エンティティは、それが主張する通りのものであるという特性。
医療情報システムの安全管理に関するガイドライン	正当な権限において作成された記録に対し、虚偽入力、書換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であることである。
JIIMA 電子化文書取扱いガイドライン簡易版（2013 年 10 月）	文書の記載内容が、真実で正しいことを主張できる要件。電子化文書等の故意・過失による虚偽入力、書換え（改ざん・すり替え）、消去、混同、隠滅、破壊などがないこと。かつ改変・改ざん等の事実の有無が確認・検証できることが条件となる。

表 2-1 の定義から、真正性に関連する特性として、本人性、完全性、否認防止、実在性、存在時刻等があげられる。

3 真正性の保証が求められるケースの例

3.1 電子申請

3.1.1 電子申請とは

電子申請は、インターネットなどを介して、官公庁などに対して、許可・認可等を求める申請行為を自宅や会社の PC やスマートフォン等を利用して行うことである。申請手続きを電子化することで時間的な制約（役所の窓口や受付が閉まる時間帯でも申請が可能）、地理的な制約（行政期間の窓口に行かなくても申請が可能）をうけること無く申請が可能になる。その一方で、成りすましによる申請行為や申請情報の改ざんへの対策が必要となる。なお、e-Gov を利用した申請数は、年々増加している。

電子申請では、申請の真正性が必要な手続きにおいては、申請者が電子署名を行うことによりその真正性を保証する。

図 3-1 図タイトル電子政府の総合窓口「e-Gov」[1]

[1] http://www.e-gov.go.jp/

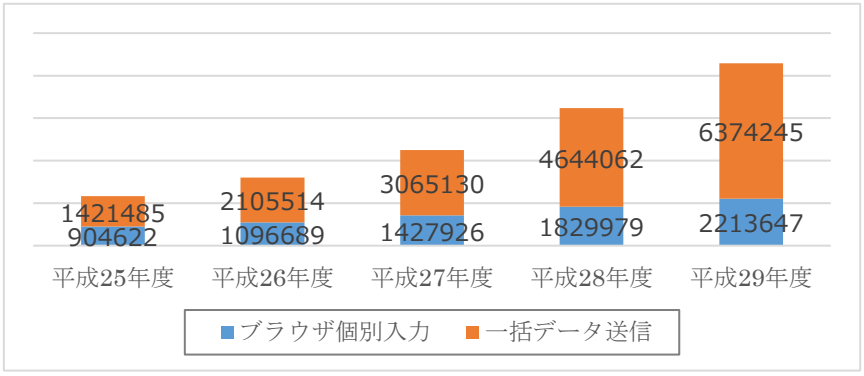

図 3-2 e-Gov の利用状況（電子申請受付件数）[2]

3.1.2 電子申請の流れ

代表的な電子申請の処理を説明する。電子申請は、申請者と電子申請システムで構成される。申請者は、予め電子申請システムに対して、①身元情報が確認できる情報を送り、電子申請システムは、申請者を登録する。申請を行う前に、②利用者認証を行う。認証後に、③申請手続き検索を行い、④申請書入力を行い、申請する手続きで電子署名が必要な場合は、⑤署名送信を行い、電子申請システムが署名の検証を行う。申請した内容が申請システムで受け付けられたかを確認するため、⑥到達確認を行い、申請する手続きで手数料が必要な場合は、⑦手数料等の納付を行う。また、⑧申請・届出の状況確認も行うことができる。

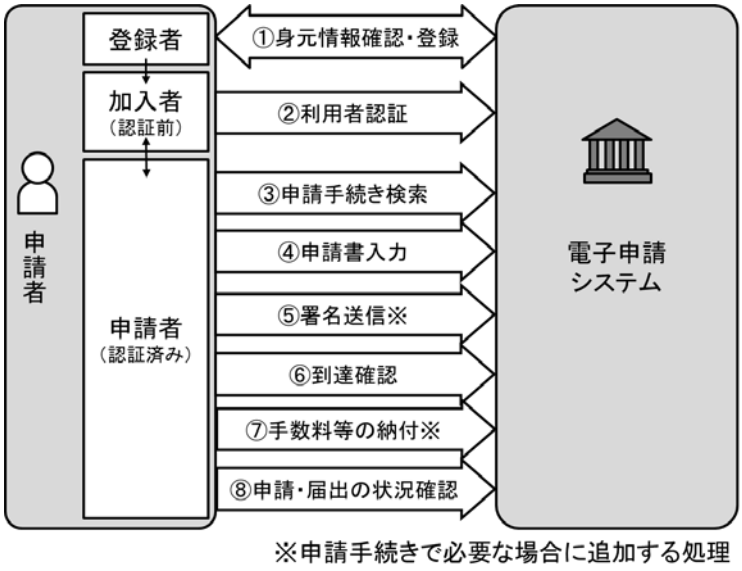

図 3-3 電子申請の処理

[2] http://www.e-gov.go.jp/about/use.html

3.2 電子入札

3.2.1 電子入札とは

電子入札は、調達の一つの方法で、インターネットを介して、従来の紙による入札行為や開札行為を自宅や会社の PC から行うことである。電子申請と同様に、場所や時間の制約を受けずに入札行為や入札参加者への落札決定の通知が行え、電子契約まで行うシステムも運用されている。その一方で、成りすましによる申請行為や申請情報の改ざんへの対策が必要となる。

政府電子調達（GEPS）の電子入札システムでは、電子証明書を利用して認証を行い、電子調達システム上に保管される情報は、電子署名とタイムスタンプ（時刻証明）を組み合わせて、電子文書の完全性、存在時刻の真正性が長期において保証される。

図 3-4 政府電子調達「GEPS」[3]

3.2.2 電子入札の流れ

代表的な電子入札の処理を説明する。電子入札は、入札者と電子入札システムで構成される。入札者は、予め電子入札システムに対して、①身元情報が確認できる情報を送り、電子入札システムは、入札者を登録する。入札を行う前に、②利用者認証を行う。認証後に、③調達・入札検索を行い、④入札登録を行い、入札した内容が入札システムで受け付けられたかを確認するため、⑤入札内容確認

[3] https://www.geps.go.jp/introduction

を行う。また、⑥入札内容・状況確認も行うこともできる。

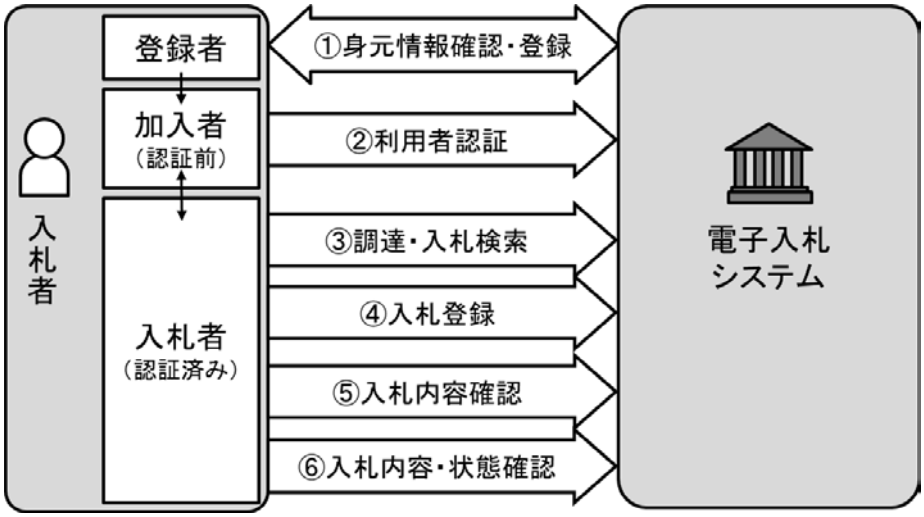

図 3-5 電子入札システムの処理

3.3 電子処方箋

3.3.1 電子処方箋とは

電子処方箋は、従来、書面（紙）で取り扱われていた処方箋の電子版である。厚生労働省は平成28 年 3 月 31 日付通知にて「厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令」を一部改正し、「電子処方箋の運用ガイドライン」ならびに「電子処方箋引換証」の様式を制定した旨を公表した。これにより、処方箋の電磁的記録による作成、交付および保存が可能となった。それに伴い、処方に基づき薬局で作成する調剤情報の電子的な取り扱いも可能となっている。これにより、医療機関と薬局との情報連携を促進し、地域医療連携を推進し、国民がそのメリットを享受できることが期待されている。

電子処方箋には、その正当性を保証するために電子処方箋を作成した医師の電子署名及びその存在証明のためのタイムスタンプを、また、調剤情報にはその正当性を保証するために調剤情報を作成した薬剤師の電子署名及びその存在証明のためのタイムスタンプを付さなければならない。付すことにより、電子処方箋及び調剤情報の完全性、それら情報の存在時刻、署名者の本人性を保証することができる。

3.3.2 電子処方箋の流れ

「JAHIS 電子処方箋実装ガイド Ver.1.1」に基づき、電子処方箋に関わる代表的な処理を説明する。関連する構成要素は、医療機関及び医師、電子処方箋 ASP（Application Service Provider）、薬局及び薬剤師、患者である。電子処方箋 ASP は電子処方箋や調剤情報の交換を

仲介する機能を持ち、それらを長期保存する役割は持たない。

予め電子処方箋 ASP に対して、①身元及び医師や薬剤師の資格が確認できる情報を送り、電子処方箋 ASP は、登録者となる医師と参照者となる薬剤師を登録する。電子処方箋の登録を行う前に、②医師は利用者認証を行う。認証後に、③電子処方箋に付与する ID（処方箋 ID）を要求、④取得し、⑤医師の電子署名及びタイムスタンプを付与した電子処方箋を送信する。患者には⑥処方箋 ID を記された電子処方箋引換証（書面）を手渡す。

⑦薬局で薬剤師が患者から電子処方箋引換証の提示を受けると、⑧薬剤師が利用者認証を行った後、⑨電子処方箋引換証に記された処方箋 ID をキーとして電子処方箋を受け取る。薬剤師が受け取った電子処方箋に基づき調剤情報を作成し、電子署名及びタイムスタンプを付与した後、⑪その調剤情報を送付する。その後、⑫元の処方を行った医師に調剤情報は送付される。

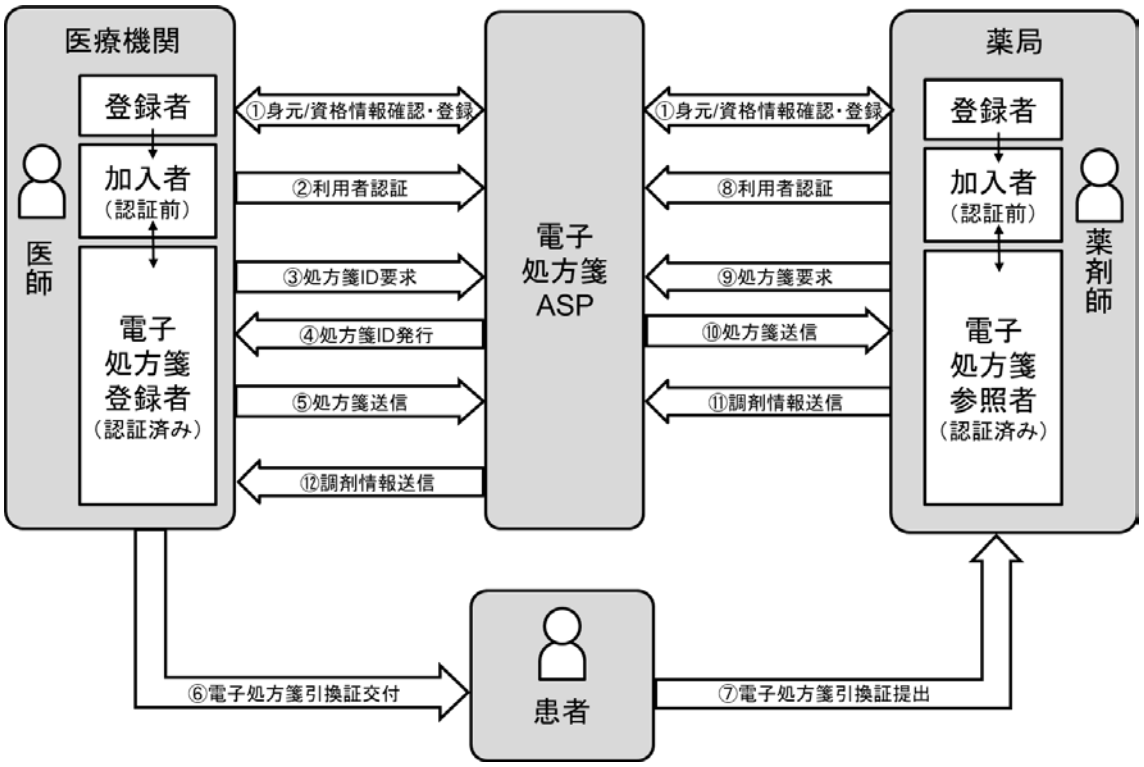

図 3-6 電子処方箋の処理

3.4 本人確認

3.4.1 本人確認とは

「本人確認」とは、『その人が本人かどうか』を確認する作業で、オンラインでの活動や取引が増加する中で、あるデジタル上のアカウントを利用している人が本当に本人かどうかを確認する必要性が高まっている。ここでは、住民としての実在性に基づく本人確認を基本として記述する。

本人確認を詳細に分類すると、その人が該当する所在地に本当に実在するかどうかの確認（身元確認）と、この瞬間にこの場所にいる人が、本当に本人なのかを確認（当人確認）するという、2 つの意味合いを含んでいる。

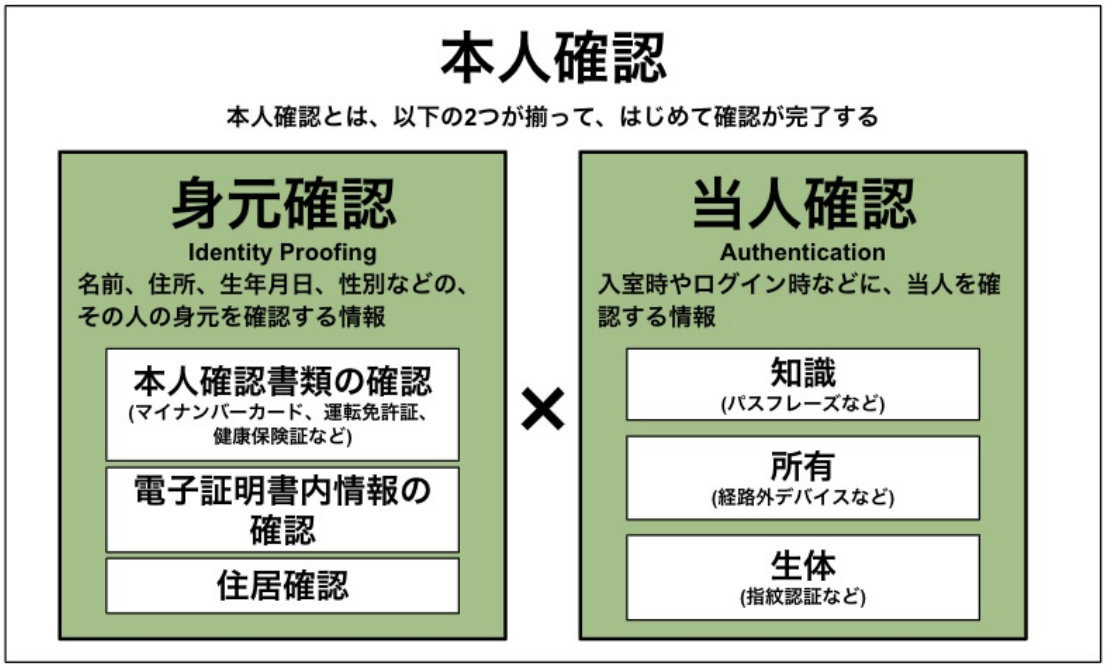

図 3-7 本人確認の分類

身元確認には、その人の身分証を確認するプロセスや、住居を確認するプロセスが含まれる。本人確認においては、当人確認は欠くことのできない要素ではあるが、身元確認と複合的に行われることも多く、概して身元確認の比重が高いことから、ここでは、身元確認のことを「本人確認」と説明する。当人確認については、5.3 節を参照。
身元確認・当人確認のレベルの定義および、サービスのリスク評価に応じたレベルの選択については、4 真正性保証のレベルの定義を参照。

本人確認が必要なサービスは多岐にわたる。マネーロンダリング及びテロ資金供与を防止するための法律である犯罪収益移転防止法は、金融業を中心に適用される法律で、金融機関と直接取引する利用者、及び金融機関が取引の間を取り持つ双方の利用者に対する本人確認を厳格に規制している。犯罪収益移転防止法に関連するものとして、古物営業法、割賦販売法などの法律が規定され、本人確認プロセスが法令で決められている業界のほか、業界団体で本人確認プロセスが決められている業界もある。

表 3-1 本人確認が必要な事業と関連する法律の例

事業	本人確認に関連する法律
銀行業・証券業・貸金業・送金業・保険業仮想通貨交換業などの金融業	犯罪収益移転防止法
クレジットカード	割賦販売法
古物商	古物営業法
携帯電話販売	携帯電話不正利用防止法
マッチングアプリ	出会い系サイト規制法

3.4.2 本人確認の流れ

本人確認の流れは、業法で指定されている本人確認プロセスごとに異なる。ここでは一般的なオンラインでの証券口座の開設を例にとって説明する。

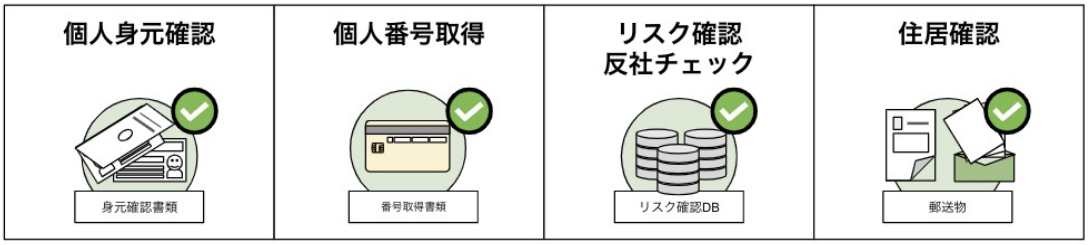

図 3-8 オンライン証券の口座開設プロセスの例

表 3-2 オンライン証券の口座開設プロセスの説明

プロセス	説明
身分証確認	顧客の身分証画像に不備がないことなどを確認し、本人が申請した情報との一致確認を行う。
個人番号取得	顧客のマイナンバーを取得します。いわゆる番号法に則ったプロセス[4]で実施する必要がある。
リスク確認・反社チェック	顧客が反社会的勢力や金融犯罪者、公的要人などではないかを、リスクデータベースを照会して確認する。

[4] 参考資料として、JNSA マイナンバー業務プロセス・リスク分析シートがある。
https://www.jnsa.org/mynumber/data/mynumber_risk_sheet_ver3_0.pdf

プロセス	説明
住居確認	書留などの転送不要郵便を送り到達を確認することにより、顧客が申請した住所に住んでいることを確認する。

【1】 従来の本人確認プロセスについて

従来、本人確認プロセスは、対面で身分証を確認する方法、郵送で本人確認書類の原本やコピーを受け取り確認する方法、ウェブサイトで本人確認書類を撮影した画像のアップロードを受け付ける方法などで行われている。昨今は、オンラインサービスの広がりと、顧客体験の向上のために迅速に本人確認プロセスを完了したいニーズが高まっていることから、アップロードによる手法も多く利用されている。

【2】 オンライン完結の本人確認プロセスについて

オンライン完結の本人確認プロセスの代表として、公的個人認証がある。公的個人認証では、市区町村が窓口で身元確認を行い、その市区町村が署名した電子証明書と当該個人の電子署名用の署名鍵等を書き込んだマイナンバーカードを発行する。マイナンバーカードを所有する個人は、自分で設定したパスワードを入力してカード内の署名鍵、電子証明書を利用するので、本人以外がその電子証明書を利用できない仕組みを導入している。電子証明書を受け取ったものは、その電子証明書に付与された市区町村の電子署名等の有効性を検証し、その内容を確認することで、本人確認ができる。さらに、カード内の署名鍵で電子署名した文書も同様に本人が作成したものであることが確認できる。公的個人認証は、本人確認書類の真正性や当人の確認もデジタルで担保し、瞬時に本人確認の結果がわかる最も有効な手段とされている。

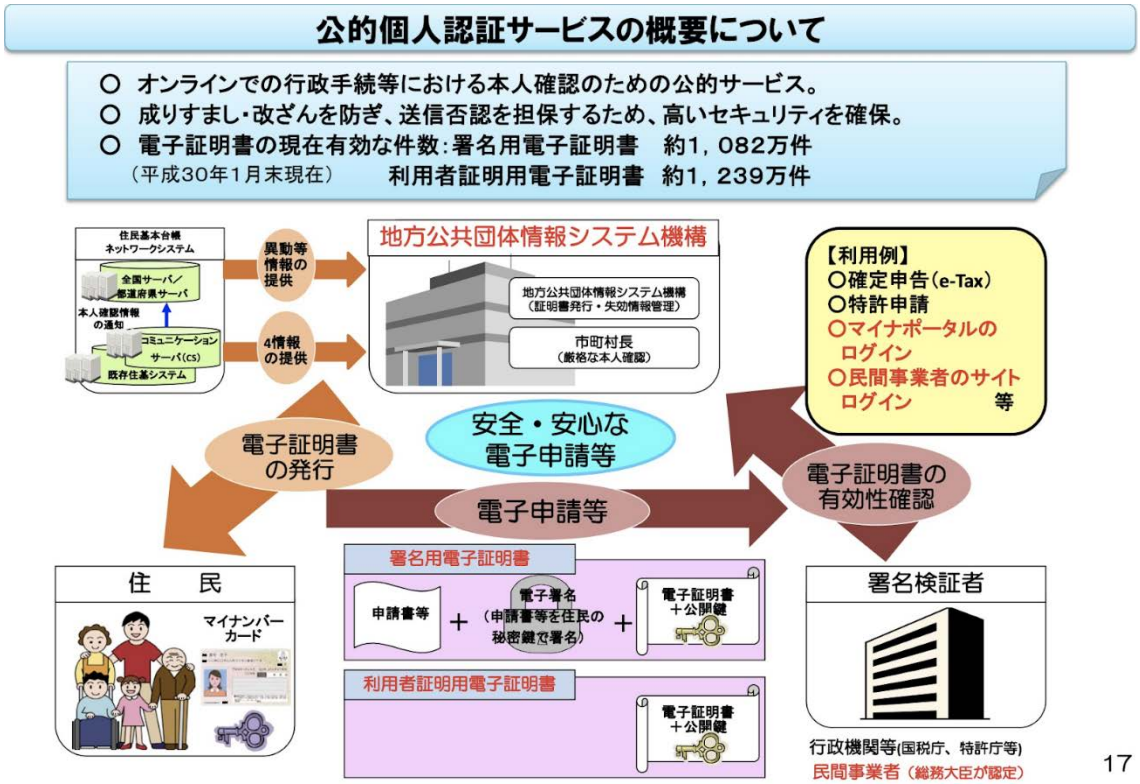

図 3-9 公的個人認証サービスの概要 [5]

さらに、2018 年 11 月 30 日、犯罪収益移転防止法施行規則の改正に伴い、オンライン完結の本人確認手法が整備された(通称「eKYC」)。本人確認書類の原本がその場で撮影され、本人の容貌と一致することを保証するための専用ソフトウェアで撮影すること、もしくは預貯金口座・クレジットカード契約の確認を補助確認とすることを条件に、郵便による住居確認が不要となる。

[5] マイナンバーカードを活用したオンライン取引等の可能性について
http://www.soumu.go.jp/main_content/000534321.pdf

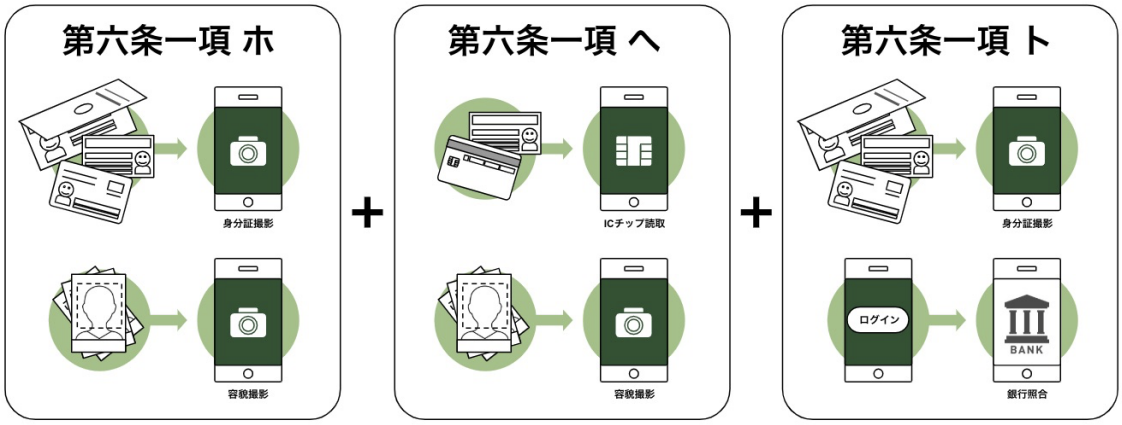

図 3-10 犯罪収益移転防止法施行規則の改正 オンライン完結の新手法

改正犯罪収益移転防止法施行規則第六条一項一号ホおよびトの手法において、本人確認書類画像の真正性確認については、現在の技術を前提とすれば目視による確認が必要と考えられている。第六条一項一号への手法は、カード内の IC チップ情報を読み取るため、真正性の確認をデジタル完結することができるとされている。第六条一項一号ホおよびへの手法において、顧客の容貌の画像と本人確認書類に貼り付けられた画像もしくは IC チップ内に格納された写真画像の一致については、もっぱら機械を利用して行うことも許容される。

仮に、スマートフォンアプリを専用ソフトウェアとした場合の連携例は以下の通りとなる。

PC にて口座開設を行っている場合は、口座開設トランザクションの ID を発行し、QR コード読み取りなどによってアプリと連携する。口座開設アプリを利用の場合は、改正犯罪収益移転防止法施行規則に対応する本人確認の機能を、口座開設アプリに盛り込むなどの方法がある。新手法は撮影要件が厳しく、プロセスが複雑なため、要件を守りつつも、顧客が撮影途中に離脱しないような設計をすることが望ましい。

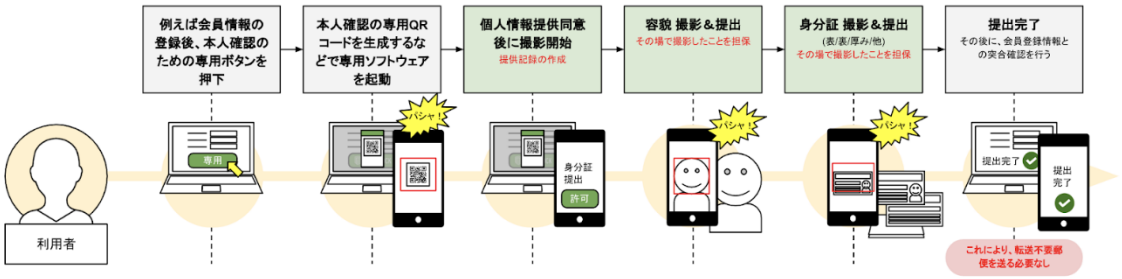

図 3-11 PC での口座開設途中にスマートフォンアプリと連携する例

4 真正性保証のレベルの定義

本章では、米国 NIST（米国国立標準技術研究所：National Institute of Standards and Technology） SP800-63-3 を参照し、真正性保証のレベルを定義した。図表の和訳は、NIST SP800-63-3（一般財団法人日本情報経済社会推進協会による和訳）及び NIST SP800-63-3 の元となる OMB（米国行政管理予算局：Office of Management and Budget） M-04-04（独立行政法人情報処理推進機構による和訳）を基に作成した。

本章は NIST SP800-63-3 の和訳をそのまま記載している箇所があるため、政府機関や合衆国政府の単語が現れるが、これら単語は顧客、自社等、読者の環境に合わせ、読み替えていただきたい。

4.1 IAL・AAL の説明と保証レベル

NIST SP800-63-3 では、身元情報の検証プロセス（3.4 節の身元確認）の保証レベルである IAL（Identity Assurance Level）と認証プロセス（3.4 節の当人確認）の保証レベルである AAL（Authenticator Assurance Level）を定義し、リスク評価に応じたレベルを選択する。レベルは数字が大きくなるほど要求が厳しくなる。参考のために以下に IAL 及び AAL の選択の概要を示す。

4.1.1 IAL の選択

IAL は、個人の身元情報を確信を持って判断するための検証プロセスの堅牢性のレベルをいい、潜在的な身元確認の誤りを軽減する目的で、リスクに応じて選択する。以下に NIST SP800-63-3 の IAL の選択概要を示す。

表 4-1 IAL の概要

レベル	内容
IAL1	申請者を特定の現実の身元情報と関連付ける必要はない。提供されるいかなる属性も自己表明か自己表明相当。
IAL2	主張された身元情報が現実に存在することを確認し、申請者がその実在する身元情報に適切に関連付けられていることを検証できる証拠が必要。IAL2 ではリモート（遠隔）か対面での身元情報の検証が必要。
IAL3	対面での身元情報の検証が要求される。身元を識別する属性は、訓練を受けた上で認可された組織の担当者によって検証が必要。

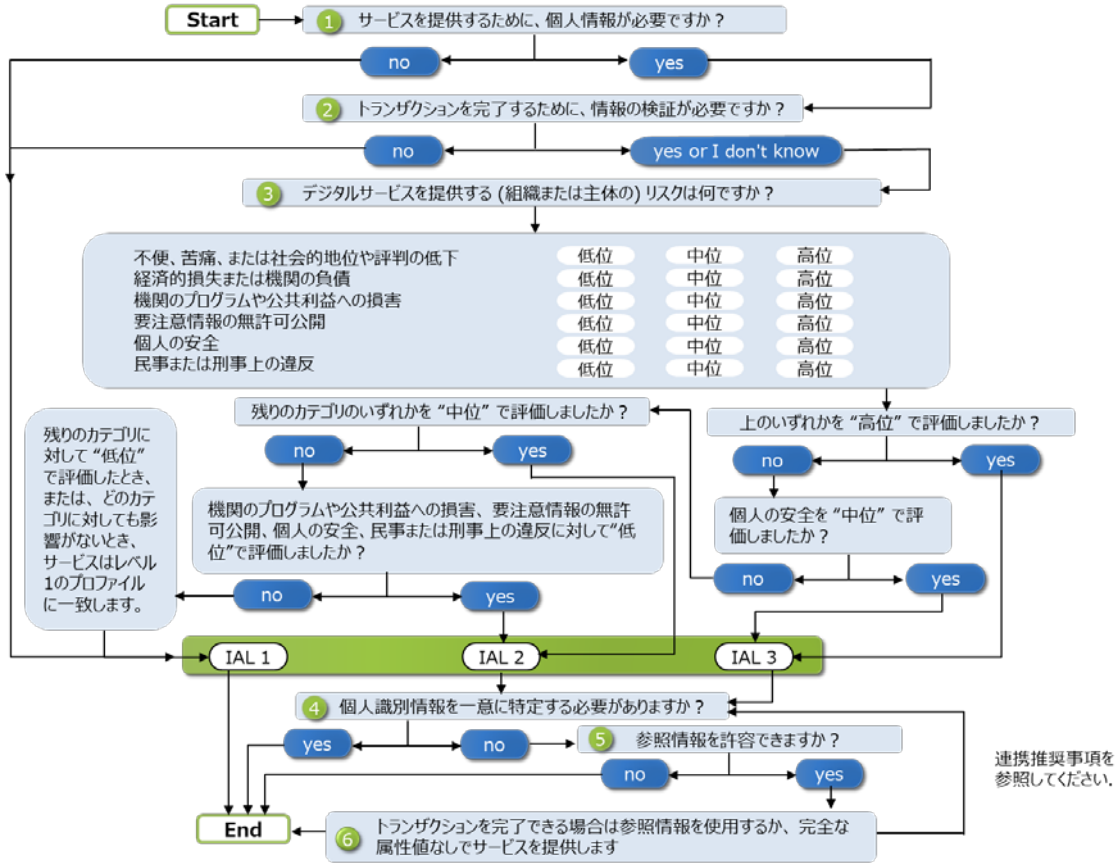

図 4-1 NIST SP800-63-3 の IAL の選択概要図

4.1.2 AAL の選択

AAL は、認証プロセス自体の堅牢性、およびオーセンティケータと特定個人の識別要素との結びつきの強さのレベルをいい、潜在的な認証誤り（すなわち、自身のものではない証明書等を使用する虚偽の請求者など）を軽減する目的で、リスクに応じて選択する。以下に NIST SP800-63-3 の AAL の選択概要を示す。

表 4-2 AAL の概要

レベル	内容
AAL1	認証要求者が加入者のアカウントに結び付けられた認証コードを管理していることが、ある程度の確信度で保証されるレベル。 AAL1 は、単要素か多要素の認証コードを保持し管理していることをセキュアな認証プロトコルによって証明することが必要。
AAL2	認証要求者が加入者のアカウントに結び付けられた認証コードを管理していることが、高い確信度で保証されるレベル。 AAL2 は、多要素の認証コードを保持し管理していることをセキュアな認証プロトコルによって証明することが必要。また、承認済みの暗号化技術が要求される。
AAL3	認証要求者が加入者のアカウントに結び付けられた認証コードを管理していることが、非常に高い確信度で保証されるレベル。 AAL3 は、AAL2 に加え、ハードウェアベースの認証コードと検証者に偽装耐性を提供する認証コードを使用し、暗号プロトコルによる鍵の所有の証明することが必要。また、承認済みの暗号化技術が要求される。

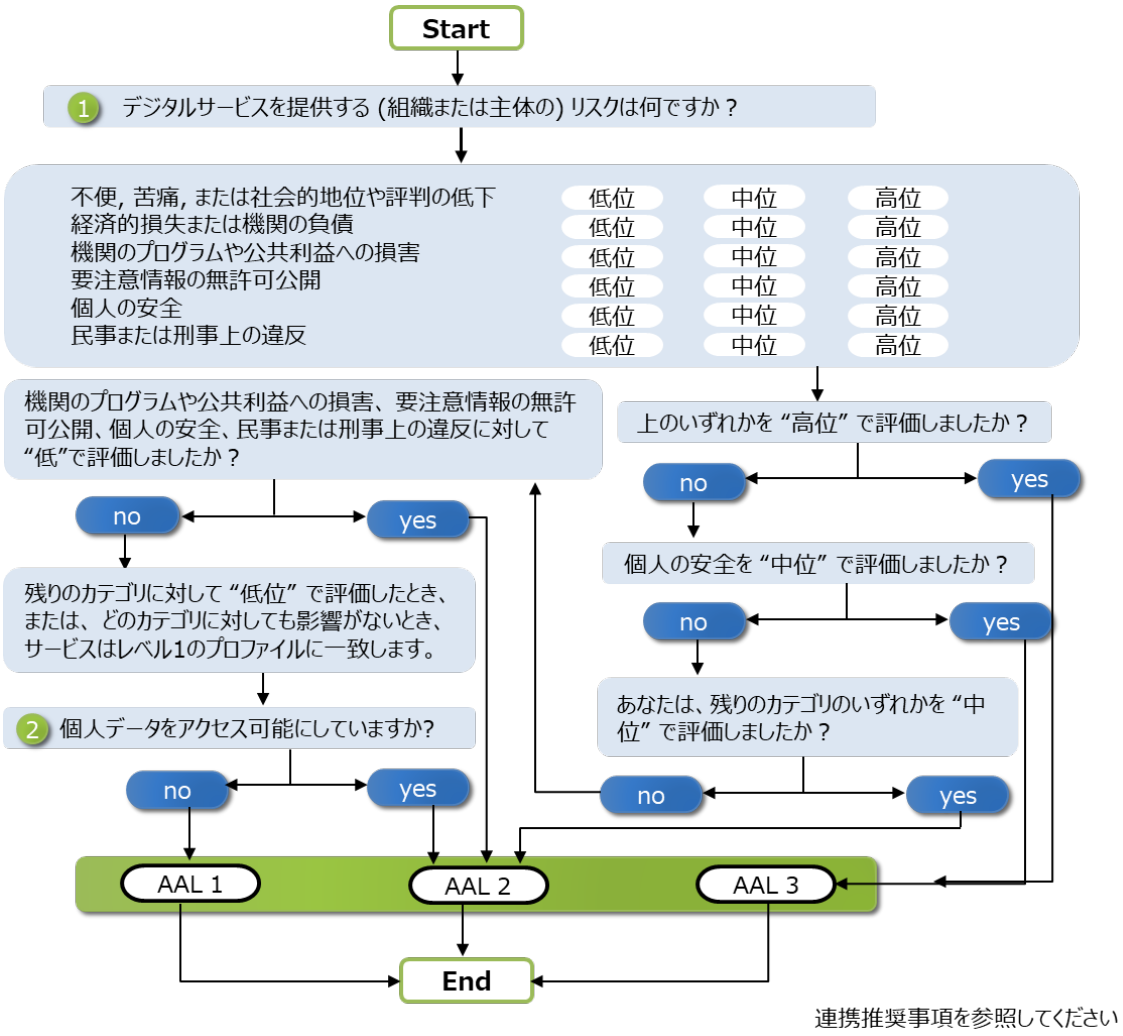

図 4-2 NIST SP800-63-3 の AAL の選択概要図

4.2 潜在的影響の分類と保証レベル

IAL や AAL のリスク評価に応じたレベルを選択するために保証レベルを決定する必要がある。潜在的影響の分類は、「不便、苦痛もしくは地位または評判に対する打撃」、「財務上の損失または政府機関の賠償責任」、「政府機関の活動計画または公共の利益に対する害」、「機密情報の無許可の公開」、「身の安全」、「民事上または刑事上の法律違反」の 6 種類の潜在的影響に分類される。潜在的な影響の分類と保証レベル及び各々の概要を示す。

表 4-3 各保証レベルにおける最大の潜在的影響

潜在的影響の分類	保証レベル		
	1	2	3
不便、苦痛もしくは地位または評判に対する打撃	低位	中位	高位
財務上の損失または政府機関の賠償責任	低位	中位	高位
政府機関の活動計画または公共の利益に対する害	該当なし	低位／中位	高位
機密情報の無許可の公開	該当なし	低位／中位	高位
身の安全	該当なし	低位	中位／高位
民事上または刑事上の法律違反	該当なし	低位／中位	高位

4.2.1 不便、苦痛もしくは地位または評判に対する打撃

不便、苦痛もしくは地位または評判に対する打撃の保証レベルは、深刻度と期間によって低位、中位、高位が決定される。

表 4-4 「不便、苦痛もしくは地位または評判に対する打撃」の潜在的影響

レベル	内容
低位	最悪の場合、限定的かつ短期間の不便、苦痛または任意の当事者の当惑。
中位	最悪の場合、深刻かつ短期間または限定的かつ長期間の不便、苦痛または任意の当事者の地位または評判に対する打撃。
高位	深刻または長期間の不便、苦痛または任意の当事者の地位または評判に対する打撃（通常は、特に深刻な影響のある状況や多くの個人に影響する状況のために用意されている）。

4.2.2 財務上の損失または政府機関の賠償責任

財務上の損失または政府機関の賠償責任の保証レベルは、回復可能性や財務上の損失、政府機関の賠償責任等によって低位、中位、高位が決定される。

表 4-5 「財務上の損失または政府機関の賠償責任」の潜在的影響

レベル	内容
低位	最悪の場合、任意の当事者の回復不能で軽微または若干の財務上の損失、もしくは最悪の場合、政府機関の軽微または若干の賠償責任。
中位	最悪の場合、任意の当事者の深刻で回復不能な財務上の損失、もしくは政府機関の深刻な賠償責任。
高位	任意の当事者の壊滅的で回復不能な財務上の損失、もしくは政府機関の深刻または壊滅的な賠償責任。

4.2.3 政府機関の活動計画または公共の利益に対する害

政府機関の活動計画または公共の利益に対する害の保証レベルは、組織の運営または資産もしくは公共の利益に対する悪影響の範囲や度合い等によって低位、中位、高位が決定される。

表 4-6 「政府機関の活動計画または公共の利益に対する害」の潜在的影響

レベル	内容
低位	最悪の場合、組織の運営または資産もしくは公共の利益に対する限定的な悪影響。限定的な悪影響の例としては以下が考えられる。（i）組織が「著しく」低下した効率で主要な機能を実施せざるを得ず、その状態が継続する、業務能力の劣化。（ii）組織の資産または公共の利益の軽微な損害。
中位	最悪の場合、組織の運営または資産もしくは公共の利益に対する深刻な悪影響。深刻な悪影響の例としては以下が考えられる。（i）組織が「大幅に」低下した効率で主要な機能を実施せざるを得ず、その状態が継続する、業務能力の大幅な劣化。（ii）組織の資産または公共の利益の重大な損害。
高位	組織の運営または資産もしくは公共の利益に対する重大または壊滅的な悪影響。重大または壊滅的な悪影響の例としては以下が考えられる。（i）組織が主要な機能の 1 つ以上を実施できず、その状態が継続する、業務能力の激しい劣化または喪失。（ii）組織の資産または公共の利益の際立った損害。

4.2.4 機密情報の無許可の公開

機密情報の無許可の公開の保証レベルは、機密性喪失によって予測される悪影響の範囲や度合い等によって低位、中位、高位が決定される。

表 4-7 「機密情報の無許可の公開」の潜在的影響

レベル	内容
低位	最悪の場合、許可のない当事者に対する個人情報、合衆国政府の機密情報または企業秘密の限定的な公開に起因する、組織活動、組織資産、または個人に限定的な悪影響をもたらすことが予測されうる機密性喪失。
中位	最悪の場合、許可のない当事者に対する個人情報、合衆国政府の機密情報または企業秘密の公開に起因する、組織活動、組織資産、または個人に重大な悪影響をもたらすことが予測されうる機密性喪失。
高位	許可のない当事者に対する個人情報、合衆国政府の機密情報または企業秘密の公開に起因する、組織活動、組織資産、または個人に致命的または壊滅的な悪影響をもたらすことが予測されうる機密性喪失。

4.2.5 身の安全

身の安全の保証レベルは、医療措置の必要性や負傷または死亡のリスクによって低位、中位、高位が決定される。

表 4-8 「身の安全」の潜在的影響

レベル	内容
低位	最悪の場合、医療措置を必要としない軽症。
中位	最悪の場合、軽症が生じる中程度のリスクまたは医療措置を必要とする負傷が生じる限定的なリスク。
高位	深刻な負傷または死亡のリスク。

4.2.6　民事上または刑事上の法律違反

民事上または刑事上の法律違反の保証レベルは、法執行の対象の可能性や法律違反のリスクによって低位、中位、高位が決定される。

表 4-9「民事上または刑事上の法律違反」の潜在的影響

レベル	内容
低位	最悪の場合、通常は法執行の対象とならないような性質の民事上または刑事上の法律違反のリスク。
中位	最悪の場合、法執行の対象となる可能性のある民事上または刑事上の法律違反のリスク。
高位	法執行の計画にとって特に重要とされている民事上または刑事上の法律違反のリスク。

5 真正性を保証するための実装方法

5.1 電子署名

5.1.1 電子署名の特長

電子署名は、紙の文書への押印やサインに相当する役割を、電子文書に対して電子的に行ったことを証明する証拠となるものである。本節では電子署名技術の一つである公開鍵暗号方式を使ったデジタル署名（5.1 節では、「電子署名」＝「デジタル署名」とする。）について説明する。

電子署名は、署名者本人であること（本人性）、署名時点から改ざんがなされていないこと（完全性）、署名した本人であることの否認を防止すること（否認防止）の特長を持つ技術である。

5.1.2 電子署名の処理フロー

電子入札や電子処方箋等での電子署名の利用には、その用途に応じた認証局から発行された電子証明書と電子証明書の公開鍵と対となる秘密鍵（署名鍵）の準備を行い、申請書や処方箋等の文書に対して署名を付与、申請、送付を行う。処理フローを図 5-1 に示す。

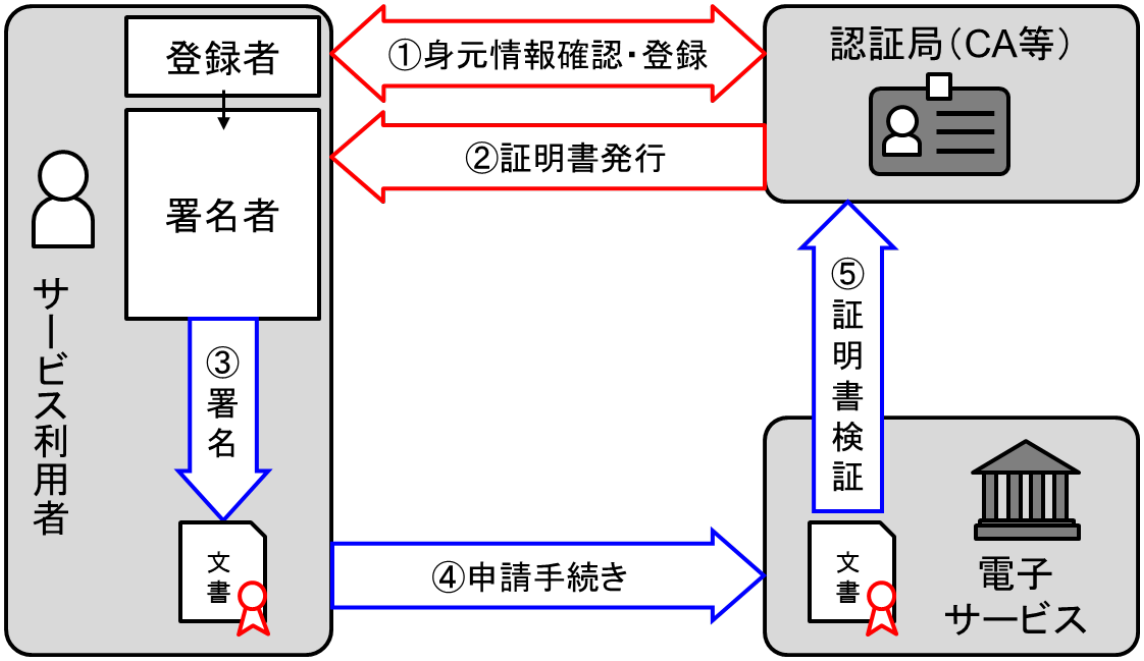

図 5-1 電子署名の処理フロー

電子証明書等の準備である登録プロセスでは、認証局が公開している運用規定等に示されている身

元情報の確認（3.4.1 項「身元確認」参照）、登録が行われた後に、認証局から電子証明書が発行される。これらは初回のみ必要なプロセスである。登録プロセスの処理フローを表 5-1 に示し、署名利用時の署名及び検証プロセスは以降に説明する。

表 5-1 電子署名の処理フロー（登録プロセス）

フェーズ	処理	実装例
登録プロセス	① 身元情報確認・登録	・ 民間で利用可能な電子証明書の発行に必要な身元確認方法と電子証明書の発行形式の例は表 5-2 を参照
	② 証明書発行	
	③ 署名	以降の図 5-2、表 5-3等で説明
	④ 申請手続き	
	⑤ 証明書検証	

表 5-2 民間で利用可能な主な電子証明書の発行に必要な身元確認方法の例

種類	身元確認方法と発行形式
公的個人認証サービス（マイナンバーカード）	・ 発行元は地方公共団体で、発行先は民間個人である。 ・ 署名用証明書は属性に基本四情報（氏名、住所、生年月日、性別）が含まれる。 ・ 市区町村窓口にて対面で本人確認を行い発行される。 ・ 政府認証基盤（GPKI）と相互認証されている。 発行形式：IC カード
商業登記に基づく電子認証制度（商業登記証明書）	・ 発行元は法務省で、発行先は法務省に登記済みの法人代表者である。 ・ 属性に基本三情報（商号又は名称、所在地、法人番号）と代表者氏名が含まれる。 ・ 本人確認は法務省への商業登記時に完了している。 ・ 政府認証基盤（GPKI）と相互認証されている。 発行形式：ソフトウェア（PKCS#12）

種類	身元確認方法と発行形式
電子署名法の特定認証業務	・ 発行元は民間認証局で、発行先は民間個人だが士業等の資格を必要とする場合もある。 ・ 属性に氏名と組織属性や資格属性等が含まれる。 ・ 電子署名法に適合した認証局が本人確認を行う。 ・ 認定を受けた認定認証業務（認定認証局）と、認定を受けない特定認証業務（特定認証局）がある。 ・ 認定認証業務は政府認証基盤（GPKI）と相互認証されているが、特定認証業務は相互認証されていない。 http://www.moj.go.jp/MINJI/minji32.html 発行形式：IC カード・ソフトウェア等

署名プロセスでは、本人性、完全性等を確保するため、サービス利用者が電子署名の生成を行い、受信者が受理した電子署名及び文書とシステムログ、サービスログ等を保管する。一方、検証プロセスでは、電子署名と文書の検証、ログの確認を行う。これらの処理フローを図 5-2、表 5-3 に示す。

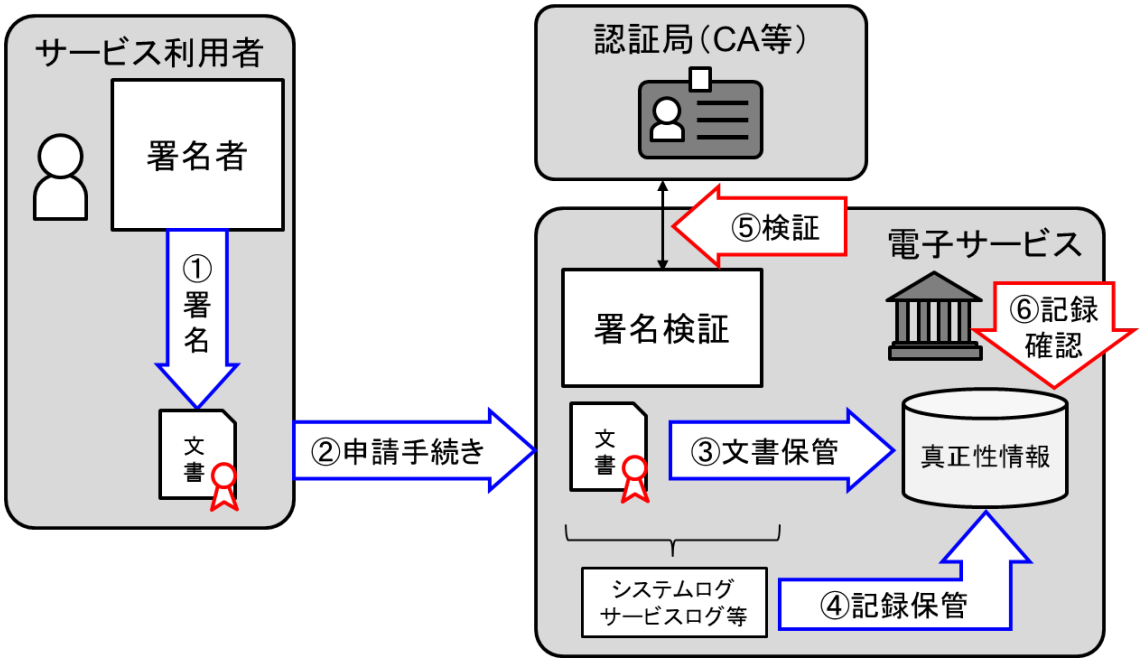

図 5-2 電子署名を使った電子サービスの利用

表 5-3 電子署名の処理フロー（署名／検証プロセス）

フェーズ	処理	実装例
署名プロセス	① 署名	・ 申請書等の文書に対して電子署名を生成 ・ 署名フォーマットとして文書（もしくは文書の参照情報）が含まれる方式（CAdES／XAdES／PAdES 等）を利用
	② 申請手続き	・ 電子署名と申請書等の文書を送付
	③ 文書保管	・ 受理した電子署名及び文書を保管
	④ 記録保管	・ システムログ、サービスログ等のデジタル記録を保管
検証プロセス	⑤ 検証	・ 電子署名の検証 ・ 証明書の検証（認証パスの構築、信頼性確認、有効性の確認） ・ タイムスタンプを付与した CAdES／XAdES／PAdES 等の場合はタイムスタンプの時刻による有効性を確認
	⑥ 記録確認	・ システムログ、サービスログ等のデジタル記録を確認

5.1.3 電子署名の開発時、利用時の留意点

5.1.2 項の通り、電子署名では登録、署名、検証のプロセスに分けられる。本節では各プロセスにおける留意点と、考えうる脅威の例に対する対策例を説明する。

登録フェーズにおける開発時、利用時の留意点を表 5-4 に示す。

表 5-4 電子署名（登録フェーズ）の開発時、利用時の留意点

手順	内容	留意点
鍵ペアの生成	署名に利用する鍵ペア（秘密鍵・公開鍵）を生成する。	・ 利用者側と認証局等のどちらで生成してもよいが、秘密鍵が漏えいしないセキュアな手順の検討が必要 ・ 業界標準やガイドラインに記載された公開鍵暗号による署名方式及び鍵長にて生成することが必要
身元情報の確認	利用者から提出された情報から認証局が身元情報を確認する。	・ 業界標準やガイドライン(NIST SP800-63-3 等)を参考に身元情報の保証レベル（IAL）の検討が必要
証明書の発行と登録	利用者が証明書と秘密鍵を利用できるようにする。	・ IC カード等のハードウェアに証明書と秘密鍵を格納するのか、ソフトウェアのファイルとして提供するのか、検討が必要

署名フェーズにおける開発時、利用時の留意点を表 5-5 に示す。

表 5-5 電子署名（署名フェーズ）の開発時、利用時の留意点

手順	内容	留意点
文書への署名	申請文書に署名を付与する。	・ 署名対象と内容が署名者の意図した通りかを署名者が確認させることが必要 ・ 署名フォーマットには署名者の証明書が署名対象として含まれる方式（CAdES／XAdES／PAdES 等）を利用
申請手続き	署名済み文書を送付、アップロードする。	・ 明示的なアクション（申請ボタンのクリック等）を経て、送付することで、利用者の意思確認を行うことが必要

検証フェーズにおける開発時、利用時の留意点を表 5-6 に示す。

表 5-6 電子署名（検証フェーズ）の開発時、利用時の留意点

手順	内容	留意点
申請受付時の処理	文書の署名者証明書を表 5-7 の電子証明書の検証項目と手順に従って検証することで証明書の正当性を確認する。	・ 失効の確認には認証局や証明書検証サーバ等へ外部接続することが必要

表 5-7 電子証明書の検証項目

証明書の検証項目	検証内容
認証パス（証明書チェーン）構築の確認	・ 申請者の証明書から認証局のルート証明書まで正しく証明書のチェーンが構築できることを確認 ・ X.509 と RFC 5280 の仕様に準拠
ルート証明書の信頼性の確認	・ 信頼リスト等を利用してルート証明書（トラストアンカー）が、信頼され認められている認証機関により発行されている証明書であることを確認
有効性（失効していない）の確認	・ 利用時点で認証パスの全ての証明書が有効期間内であることを確認 ・ CRL（失効リスト・RFC 5280）または認証局の OCSP レスポンダ（RFC 6960）への問い合わせによって証明書が失効していないことを確認

電子署名の考えうる脅威の例に対する対策例を表 5-8 に示す。

表 5-8 電子署名の考えうる脅威の例に対する対策例

脅威	説明	脅威例	対策例
中間者攻撃	署名等プロセスに介入し、意図せぬ署名を生成させる。	機器やソフトウェアの脆弱性等を利用して、署名対象の改ざん、差し替え等を行い、利用者が意図しない対象に署名させる。	・ 機器やソフトウェアの正当性を検証可能とする機能を搭載する。
アルゴリズムの危殆化	危殆化した暗号アルゴリズムを用いるように誘導し、安全性の低い電子署名を行わせる。	複数の暗号アルゴリズムを併用可能なシステムにて、危殆化した暗号アルゴリズムを用いるように利用者を誘導し、安全性の低い電子署名を行わせた後、改ざんを行なう。	・ 危殆化した暗号アルゴリズムに関する機能をシステムから削除し、安全な暗号アルゴリズムのみが動作するようにする。
フィッシング	利用者を欺いて、不正なサイトに誘い出し、利用者が意図せぬ対象に電子署名を行わせる。	不正なサイトに誘い出し、認証と見せかける、あるいは不正なデータを送付する等して、利用者が意図せぬ対象に電子署名をさせる。	・ 証明書等のトークンや認証情報を認証用と署名用に分離し、使い分ける。 ・ 認証用と署名用のトークンを活性化させるPINを分け、利用者が使い分けを意識しやすくする。

脅威	説明	脅威例	対策例
利用者が意図しない秘密鍵の利用	署名に利用する秘密鍵を不正利用することで、意図せぬ署名を生成させる。	ICカードを不正利用して、利用者が意図せぬ対象に電子署名をさせる、あるいはログインしたまま不在になっている機器を利用して、利用者が意図せぬ対象に電子署名をさせる。	・ IC カード等トークン利用の場合には物理的な盗難に合わないように管理して、PIN も漏えいしないように管理して、席を外す場合に IC カードを挿したままにしないようにする。 ・ ソフトウェアを機器にインストールして利用する場合には、機器をログインするパスワード等が漏えいしないように管理して、席を外す場合に必ずログアウトするようにする。 ・ PKCS#12 形式のようなソフトウェアファイルの場合にはコピーされないように管理して、PIN も漏えいしないように管理する。
書き換え	署名者が前に署名した文書を変更し、変更を気づかせずに受信者が変更した文書を受領する。	前の文書と変更後の文書の署名者が同じであるため、署名者が前に署名したにもかかわらず、受信者に変更後の文書を受領させる。	・ タイムスタンプや電子証拠の保全等の対策を行う。
消去	受信者が文書を受領したことを隠蔽するため、文書を消去する。	文書を受領したことを隠蔽するため、システムに保管している文書の消去を行う。	・ 電子証拠の保全等の対策を行う。

5.2 タイムスタンプ

5.2.1 タイムスタンプの特長

タイムスタンプは、電子文書がある時刻に存在したこと（存在時刻）と、その時刻から現在に至るまで変更・改ざんされていないこと（完全性）を第三者的に証明する技術である。

電子文書には紙文書のように経年劣化や筆跡・修正痕等が残らないことに加え、文書作成・署名環境のローカルマシン時計は変更可能であるため、タイムスタンプは第三者的なサービスとして提供される。

5.2.2 タイムスタンプの処理フロー

タイムスタンプの処理フローは、タイムスタンプの要求（図 5-3 の青矢印）、タイムスタンプの発行（図 5-3 の赤矢印）、タイムスタンプの検証（図 5-3 の緑矢印）の処理過程から構成される。尚、本節ではデジタル署名を用いるタイムスタンプについて説明する。

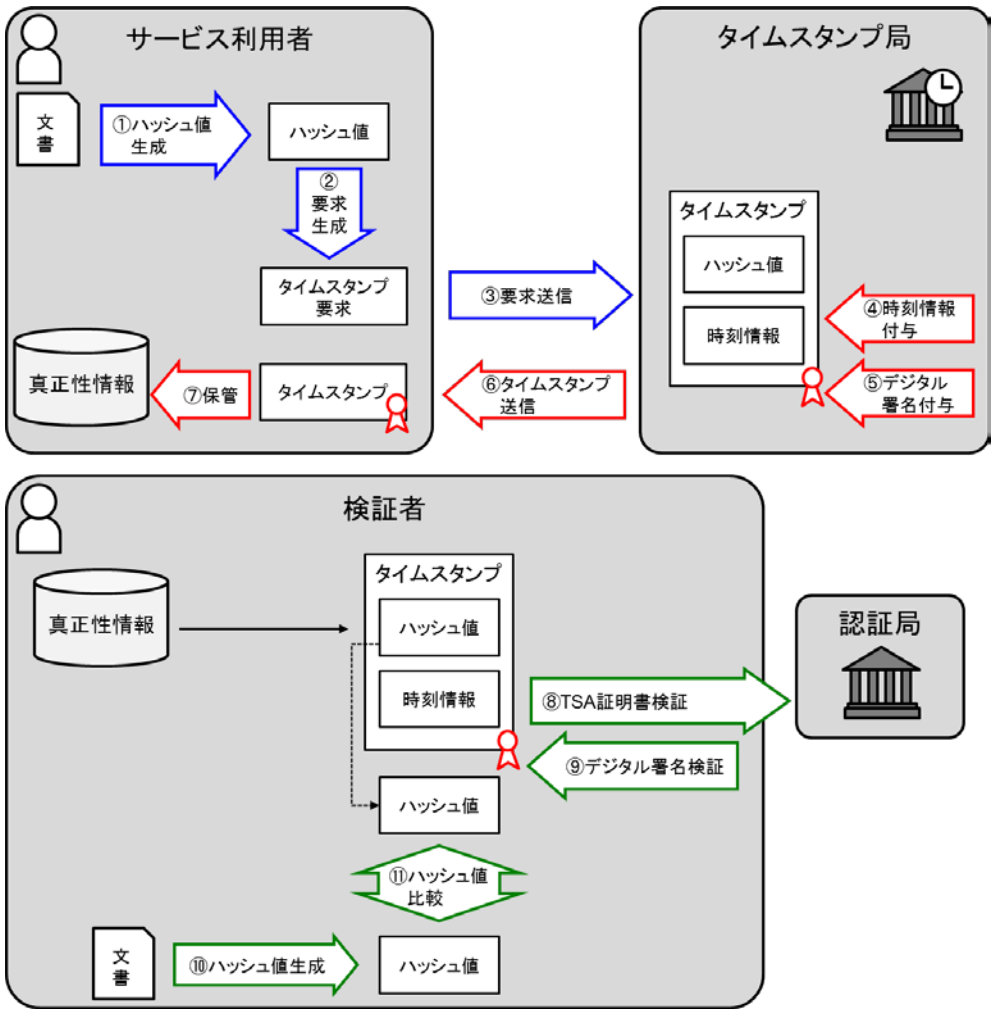

図 5-3 タイムスタンプの処理フロー

表 5-9 タイムスタンプの処理フロー

フェーズ	処理	実施者	内容
タイムスタンプ要求	① 電子文書のハッシュ値の生成	利用者	タイムスタンプ付与対象の電子文書のハッシュ値を生成する。
	② タイムスタンプ要求の生成		規定されたフォーマットに則り、前述のハッシュ値等を含めたタイムスタンプ要求を生成する。
	③ タイムスタンプ要求の送信		タイムスタンプ局に対して前述のタイムスタンプ要求を送信する。
タイムスタンプ発行	④ ハッシュ値に対する時刻情報の付与	タイムスタンプ局	利用者から受領した電子文書のハッシュ値に対して、国際標準時に追跡性がある時刻源による時刻情報を付与する。
	⑤ タイムスタンプ局のデジタル署名の付与		前述のハッシュ値および時刻情報等に対してタイムスタンプ局の秘密鍵でデジタル署名を付与する。
	⑥ タイムスタンプの送信		前述のデジタル署名が付与されたデータをタイムスタンプとして要求者に送信する。
	⑦ タイムスタンプの受信・保管	利用者	タイムスタンプを受信し、タイムスタンプ付与対象の電子文書と関連付けて保管する。
タイムスタンプ検証	⑧ TSA証明書の検証	検証者	タイムスタンプを検証するためのTSA証明書を検証する。
	⑨ タイムスタンプ局のデジタル署名の検証		タイムスタンプ局証明書（TSA証明書）を使用して、タイムスタンプに付与されたタイムスタンプ局のデジタル署名を検証する。
	⑩ 電子文書のハッシュ値再生成		タイムスタンプ付与対象の電子文書のハッシュ値を生成する。
	⑪ ハッシュ値の比較		電子文書のハッシュ値とタイムスタンプに含まれたハッシュ値を比較する。

5.2.3 タイムスタンプの開発時、利用時の留意点

タイムスタンプの開発時・利用時における留意点を前述のフェーズ毎に表 5-10 に示す。

表 5-10 タイムスタンプの開発時、利用時の留意点

フェーズ	留意点	内容
タイムスタンプ要求	ハッシュ値生成時のハッシュアルゴリズム	電子文書のハッシュ値生成に使用するハッシュアルゴリズムには安全なアルゴリズムを利用する必要がある

フェーズ	留意点	内容
	利用者認証	タイムスタンプ要求送信時には利用するタイムスタンプ局に応じた利用者認証が必要である。
	通信リトライ	タイムスタンプはインターネット通信での接続が一般的であるため、通信エラーや通信タイムアウト時のタイムスタンプ要求のリトライ機能を実装することが望ましい。
タイムスタンプ発行	タイムスタンプ受信時の検証	タイムスタンプ局から送信されたタイムスタンプに対して通信系路上で変更・改ざんが行われる可能性等を想定し、タイムスタンプを受信した際に検証することが望ましい。
	タイムスタンプの保管	・ タイムスタンプデータをタイムスタンプ付与対象文書と一体化して保管する場合は、標準化されたフォーマット（CAdES、XAdES、PAdES 等）に則って保管することが望ましい。 ・ タイムスタンプデータをタイムスタンプ付与対象文書と独立して保管する場合は、対象文書と関連付けて保管する必要がある。
タイムスタンプ検証	証明書の検証	・ TSA 証明書からルート CA 証明書まで正しく証明書チェーンが構築できることを確認する必要がある。 ・ TSA 証明書からルート CA 証明書までの各証明書の有効期限が切れていないことを確認する必要がある。 ・ TSA 証明書からルート CA 証明書までの各証明書が失効していないことを確認する必要がある。
その他	利用するタイムスタンプ局の信頼性	・ タイムスタンプ局の運用要件を定義した国際的な標準規格として ETSI EN 319 421 がある。 ・ 日本国内では、一般財団法人日本データ通信協会において同協会が定める審査基準に適合した技術・システム・運用体制によってタイムスタンプ局が運用されていることを認定する「タイムビジネス信頼・安心認定制度」が設けられており、同認定を取得したタイムスタンプの利用が義務付けられた法律や、利用が推奨されたガイドラインがあることに留意する必要がある。

5.3 電子認証

5.3.1 電子認証の特長

電子認証は本人性や実在性を保証する技術である。匿名にて利用可能な電子サービスにおいても実在性を保証する為には電子認証を利用する。電子認証を利用しない電子サービスはオープンで制限が無い利用となる。また IoT 機器であっても実在性を保証する為に電子認証が使われることがある。

クラウドにおいて電子サービスを提供する場合に電子認証の技術は必須とも言える。この為に電子認証の技術は標準化が進んでいる一方で、日進月歩で新しい技術も提供されているので注意が必要である。電子認証の分野では、米国立標準技術研究所（NIST）の電子認証ガイドライン「Electronic Authentication Guideline」の第 3 版（NIST SP 800-63-3）が参照されることが多い。NIST SP 800-63-3 に関して詳しくは「4.1 IAL・AAL の説明と保証レベル」を参照。

NIST SP 800-63-3 は IAL（Identity Assurance Level：本人確認のレベル）・AAL（Authenticator Assurance Level：認証プロセスのレベル）・FAL（Federation Assurance Level：認証連携のレベル）の 3 種類のレベルが定義されている。ここで認証プロセスや技術に関する AAL に関してまとめる。

電子認証には、毎回認証を求める単発的な利用と、最初に認証を受けた後にそのまま継続してサービスの利用が可能な SSO（シングルサインオン）がある。ここでは主に SSO の技術をまとめる。SSO 可能な技術（認証 API や認証プロトコルの仕様）は多数あるが、現在は OAuth 系と SAML 系が主流になっている。

電子認証においてもう 1 つ明確化が必要な分類として認証（Authentication）と認可（Authorization）がある。「認証」は本人性・実在性の確認を意味し、「認可」は認証完了後に属性等の利用権限を与えることを意味する。電子認証の手順としては、最初に「認証」が行われ、次に「認可」が与えられる。しかし「認証」と「認可」が同時に行われることもあり混同される一因になっている。「認証」と「認可」は明確に意識して区別して利用することが必要である。

表 5-11 認証と認可の比較

種類	略称	説明
認証: Authentication	AuthN	本人性・実在性の確認をすること。
認可: Authorization	AuthZ	認証完了後に属性等の利用権限を与えられる（または制限される）こと。

例えば OAuth は認可仕様であるがしばしば認証にも利用されることがある。OpenID Connect は

OAuth 2.0 の認証の拡張仕様と言える。OpenID Connect はサービスを利用する為に本人性・実在性を確認してアクセストークン（ID トークン）を得るまでの仕様であり、OAuth 2.0 はアクセストークン取得後（認証完了後）に認可を与える仕様として使う。

一方で SAML には認証と認可の両方の仕様が含まれるが、1 つの認証サービス（Authentication Assertion）と 2 つの認可サービス（Authorization Assertion と Authorization Decision Assertion）があり明確に区別されている。

近年の電子認証では、本人確認と認証を行う Id プロバイダ、認証を要求するサービスプロバイダ、属性を提供する属性プロバイダ等のシステムに分かれており連携（フェデレーション）して動作することが多い。

5.3.2 電子認証の処理フロー

5.3.1 項で説明した通り電子認証には本人確認のフェーズと認証プロセスのフェーズがある。本人確認時に発行された認証コードを電子サービス利用時に提示して認証プロセスを行う。電子サービスは認証機関でもある場合には認証コードを確認し、外部の認証機関を利用している場合には問い合わせることで認証コードを確認する。確認した結果が正しければ認証済みとなり電子サービスの利用が可能となる。

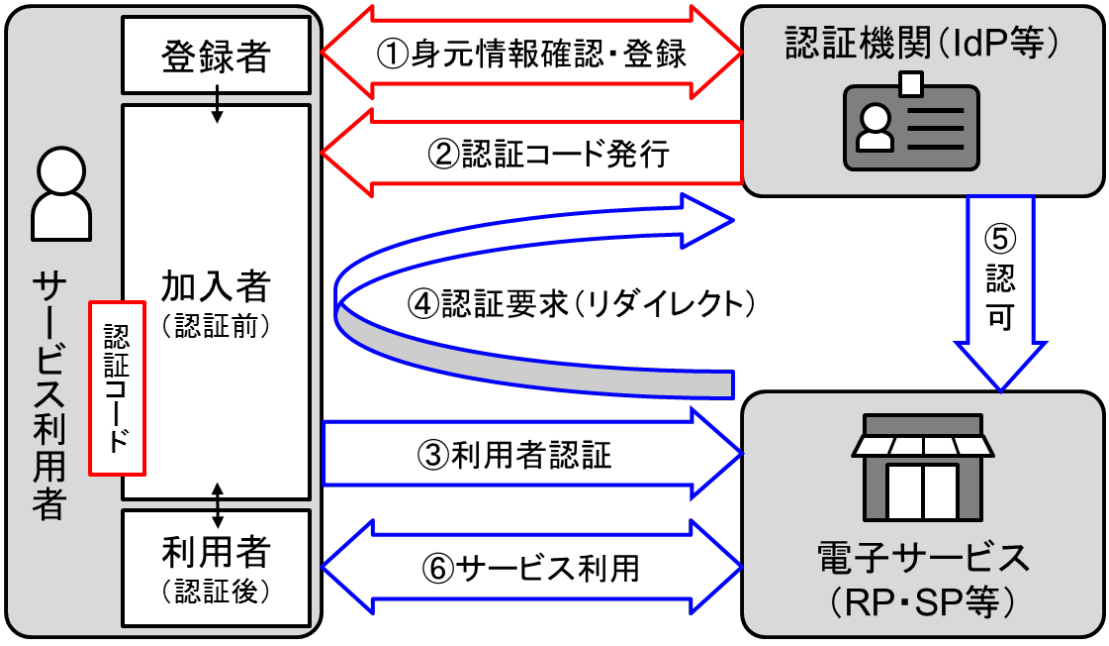

図 5-4 電子認証を使った電子サービスの利用

表 5-12 電子認証の処理フロー

フェーズ	処理	説明
本人確認 （1 回のみ）	①身元情報確認・登録	登録者より提示された属性情報により本人であることを確認。
	②認証コード発行	認証レベルに応じた認証コードを発行し返す。
認証プロセス （利用都度）	③利用者認証	サービス利用時に認証コードにより認証要求。
	④認証要求（RP⇒IdP）	IdP は認証コードを検証して本人性を確認。
	⑤認可（IdP⇒RP）	認証結果と認可情報（オプション）を返す。
	⑥サービス利用（認証完了）	認証結果と認可情報を使ってサービスを利用。

5.3.3 電子認証の開発時、利用時の留意点

電子認証の認証プロセスに利用する認証コードには各種あるが要素としては、知識・所有・生体の 3 種類がある。高い AAL（認証レベル）では 2 要素や多要素の認証コードが要求されるが、同じ要素を 2 つ重ねても多要素認証にはならないので注意すること。同じ要素を重ねる場合は多段認証と呼ばれる。例えば ID とパスワードに加えて秘密の質問を使うような場合はパスワードと秘密の質問のどちらもが知識要素である為に 2 段階認証ではあるが 2 要素認証にはならない。

表 5-13 認証要素の種類と例

要素	説明	例
知識	本人のみが有する知識に基づく	記憶シークレット（パスフレーズ等）
所有	本人のみが所有する物に基づく	IC カード、乱数表、経路外デバイス等
生体	本人の生体情報に基づく	指紋、静脈、虹彩、顔認証等

生体要素は後から変更ができない認証要素であるので利用時には漏洩しないような仕組みと注意が必要である。他の認証要素（知識・所有）と組みわせて多要素認証にするか、生体情報をサービス側に渡さないで認証を行う FIDO（Fast IDentity Online）のような仕組みを利用すべきである。

認証の仕組みを自分で実装する場合には認証プロセス中に脆弱性が無いか可能であれば専門家の確認を得た方が良い。認証はプロセスであるので利用手順や運用手順に注意をする。また運用時に適切な記録やログを取得して保存しておくことも必要となる。記録やログは後から正しい認証プロセスが実行されたことを検証する為に利用する。

多要素認証を利用すれば高い安全性が期待できるが、同時に利便性が低下するケースもある。利用するサービスの要求する認証レベルを検討して適切な認証レベルを選択するべきである。

認証と認可の違いに関してもしっかりと理解した上で認証プロセスと認証後の利用プロセスを設計する。特に電子サービスと異なる認可サーバを利用する時には認可手順とその内容についても確認をする。

5.3.4 電子認証とトークン

電子認証を使う中ではトークンと呼ばれる情報が使われる。例えば ID トークン、アクセストークン、リフレッシュトークン、認証トークン、認可トークン等である。電子認証で使われるトークンには認証結果や属性情報と場合によっては認可情報が含まれる。

単純に認証済みであることを示す識別子として利用する場合には乱数値を利用したトークンを利用することもあるが、この場合には漏洩による成りすましのリスクがある。

近年ではトークンにデジタル署名を付与することで改ざんを防ぎ正しい発行元を保証する方法が主流になっている。例えば JSON であれば JWT（JSON Web Token：RFC 7519）でもデジタル署名の仕様が組み込まれている。この場合は認証認可を行うサービスが保持する秘密鍵で署名することで正しいサービスのトークンであることが保証できる。自分でデジタル署名したトークンを自分で受け取り利用するのであれば PKI の仕組みは不要であり自己署名証明書と秘密鍵で良い。発行元と異なった場所で利用されるのであれば PKI の仕組みを利用した方が良い。

JWT の仕様のうち JWS（JSON Web Signature：RFC 7515）の Compact Serialization 形式をトークンの例として見てみると、Base64 化されたヘッダ部・ペイロード部・署名部の 3 つに分けることができる。ヘッダ部は署名方式等を記述してある部分であり、デジタル署名によりペイロード部を守っている。ペイロード部にトークンの有効期限等の認証情報や認可情報が格納される。トークンを取得した側ではまず署名を確認することで正しい発行元から発行された改ざんされていない情報であることが確認できるようになっている。

5.4 電子証拠

5.4.1 電子証拠の特長

一般に証拠とは「（裁判において裁判官が）事実の認定を行う為に判断を下す根拠となる資料」とされている。電子サービスにおいて資料は電子情報となり「電子証拠（Electronic Evidence）」または「デジタル証拠（Digital Evidence）」と呼ばれる。適正な電子証拠を保全することにより完全性や否認防止を実現することが可能となる。

電子証拠と言うと一般にはコンピュータフォレンジックが想定されるが、コンピュータフォレンジックではコンピュータを使ったインシデントが発生した後に電子的な調査を行って電子証拠を集めることを示すことが多い。ここではインシデントが発生する前から必要となる電子証拠を得る為の設計・運用・保管・活用に関して説明する。つまりより積極的に電子証拠を保全して活用する為に必要な方法をまとめる。

電子証拠の活用例としては、電子サービスにおいて本人確認された電子認証を使った電子署名がある。例えば米国の電子署名法ではデジタル署名は要求されておらず電子証拠だけでも良い。電子認証による本人性確認時の記録と同意の意思（同意ボタンのクリック等の行動）の記録を整合性のある形式（アプリケーションログ・行動追跡ログ等）により保管することで電子署名とする例である。またこの場合には電子署名のシステムが健全に運用されていること（不正アクセスが無い等）を示す記録（システムログ等）も保管する必要がある。暗号を使ったデジタル署名とは異なり暗号技術は使わなくても良いが、適切な運用が求められる。もっとも適切な運用はデジタル署名のシステムにおいても求められるものである。

本人性が担保された電子認証を使ったシステムにおいても、適切な電子証拠の設計と保管がされていない場合には電子署名的な利用は出来ない点に留意が必要である。

電子署名的な利用に限らずどのような電子サービスにおいても健全なシステム運用と利用者の行動記録は必要となっている。インシデントや問題が発生した時に必要な電子証拠を活用できる仕組みは全ての電子サービスにおいて必要であろう。

5.4.2 電子証拠の利用フロー

電子証拠を利用するには設計・運用・保管・活用の４つのフェーズが必要となる。最も難しいのは最初の設計フェーズである。設計フェーズでは構築する電子サービスの内容に合わせてどのような電子記録が必要となるか、またリスクに見合った運用規定を行う必要がある。

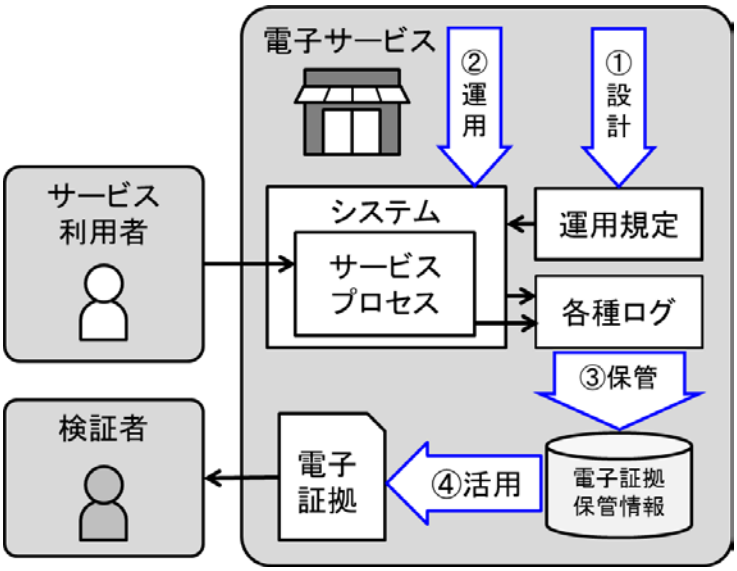

図 5-5 電子証拠の利用フロー

表 5-14 電子証拠の処理フロー

フェーズ	内容
設計	電子証拠に必要な電子記録を規定すると共に、運用の規程を策定する。法的な面での検討が必要になる場合もあり必要に応じて弁護士等に相談する。
運用	策定済みの運用規程の元で策定済みの電子証拠を取得し保管を行う。
保管	改ざんや紛失を防止する措置と共に、長期保管時には見読性を維持する必要がある。各種ログに対してタイムスタンプやデジタル署名による改ざん防止も有効な方法である。
活用	電子証拠として提出及び検証が可能な形式を整えておく。生のログ情報を提示するのではなく論理的な整合性のあるレポート形式で提示できることが望ましい。

5.4.3 電子証拠の開発時、利用時の留意点

電子証拠では設計フェーズにおける、どの電子記録をどのように保管すべきかの判断が一番難しい。基本的には利用者が電子サービスを利用している間の行動や操作のログが必要であろう。電子証拠の有用性に関しての最終的な判断は裁判官となる為に必要充分と考えられる電子証拠を残す必要がある。

また適正な運用も求められる。電子証拠の完全性を保証するのは適正な運用とそのログとなる。不正な改ざんや削除等が無かったことを運用として保証する必要がある。

5.5 電子サイン

電子サインは、合意の証として作成された文書の本人性（署名者本人であること）と完全性（文書が改ざんされていないこと）を保証する技術である。契約書や受発注書、同意書などにおいて、一人または複数の関係者の同意や承認の意思を本人確認に資するデジタル記録とともに保管することで、文書の真正性を確保するサービスとして提供される。利用者認証を行った後、文書および監査証跡（本人とその意思の確認に関係する手続きのプロセスの情報）が記録保管される。文書や監査証跡レポートは、いつでも真正性が保証された形態で入手することができる。

5.5.1 電子サインの特長

電子サインには、ペンタブレットを使用した手書きの筆跡を生体情報として記録するものがあるが、ここでは、手書きサインや印影イメージを署名の意思を示す入力情報として使用するものの、サービス利用者を識別する ID 情報により本人性を確認し、署名対象の文書と紐づけて保管するサービスを電子サインとして説明する。

電子サインは、サインや押印が必要となる契約や同意、承認などのプロセスをデジタル化して、契約や承認のスピードアップ、コスト削減、コンプライアンス強化といった効果をあげることを目指すサービスである。

そのため、一般的に、クラウドサービスとして提供され、電子メールや Web ブラウザを通知やアクセスの手段として利用する。

このサービスの実装においては、「誰が」、「いつ」、「何を」合意したかを電子文書やデジタル記録として電子サインサービス事業者が記録・保管する。その文書や記録が利用者に送付される際には、サービス事業者の電子署名により保護される。契約や同意、承認のプロセスの中で、署名者がデバイス上で手書きのサインを行ったり、印影のイメージを選択して押印したりするが、その手書きサインや印影イメージが真正性を保証するものではなく、真正性の保証レベルは、事業者が行う利用者認証や文書管理、利用記録管理に依存する。

電子サインの特長を図 5-6、モデルを図 5-7 に示す。

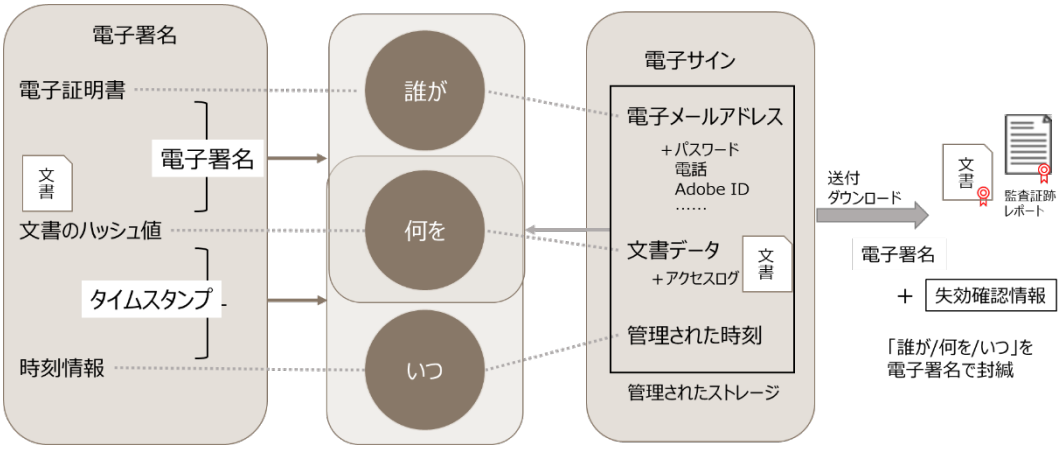

図 5-6 電子サイン（例 AdobeSign）の特長（電子署名との対比）

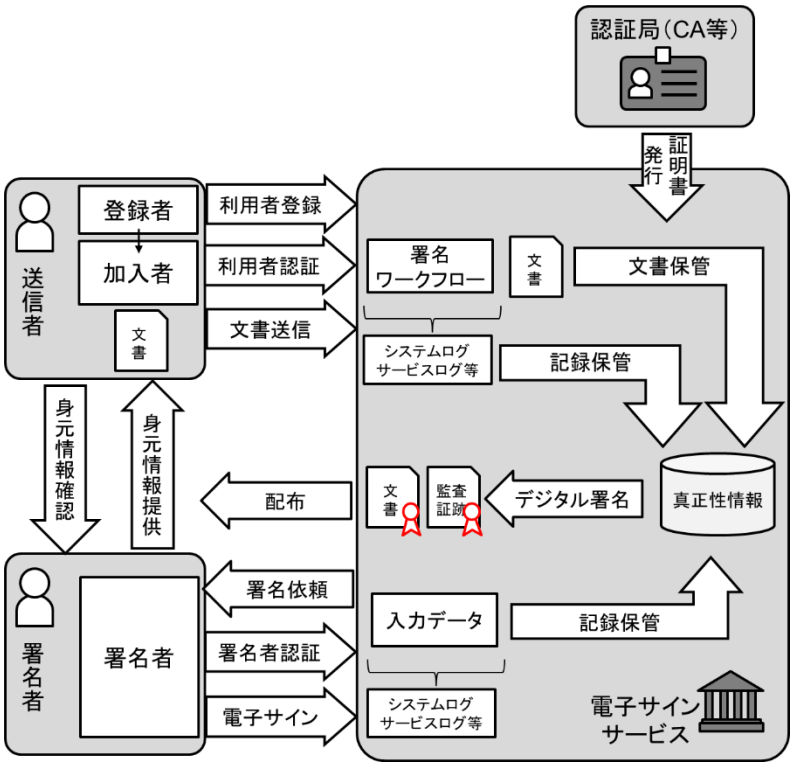

図 5-7 電子サインのモデル

【1】電子サインのモデル

電子サインの利用者には送信者と署名者があり、送信者は文書を用意して合意や同意を求めるプロセスを開始、署名者は送信者の依頼に応じて合意や同意の意思を示す。送信者が署名者を兼ねる場合もある。電子サインサービスがそのプロセスを進行させ、プロセスの進行過程や署名の依頼などは電子メールで利用者に通知される。

電子サインのプロセスを図 5-8 に示す。

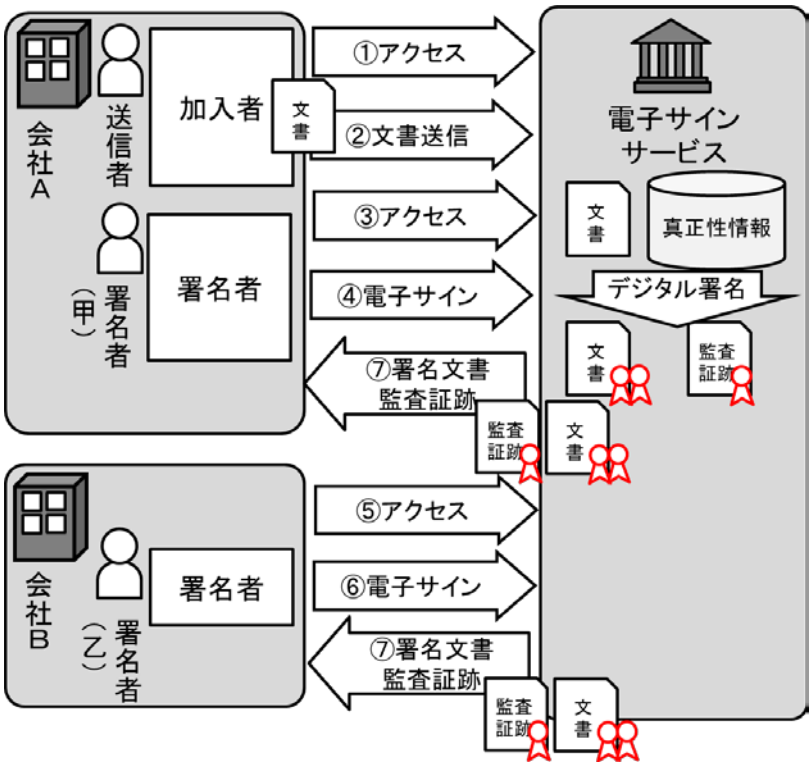

図 5-8 電子サインのプロセス

① 電子サインサービスの加入者が送信者としてサービスにアクセスする。
② 送信者はアクセス画面で文書ファイルと署名者、その他必要情報を入力して送信する。電子サインサービスは署名者に署名依頼の電子メールを送る。
③ 署名者は署名依頼の電子メールに記されたリンクをたどってアクセス画面を開く。
④ 署名者はアクセス画面で電子サインを描画／入力して送信する。電子サインサービスは電子サインを文書に書き込むとともに、いつ、誰が署名した等の記録をシステムに保存し、次の署名者に署名依頼の電子メールを送る。
⑤ 次の署名者が署名依頼の電子メールに記されたリンクをたどってアクセス画面を開く。
⑥ 署名者はアクセス画面で電子サインを描画／入力して送信する。
指定された署名者が署名を完了するまで⑤、⑥が繰り返される。
⑦ プロセスが完了したら、署名済みの文書が関係者に送付される。

この間、対象の文書は、署名に関連する基本情報や署名のワークフローで発生するイベントのデジタル記録などとともに保管され、必要に応じて利用者に提供される。

【2】利用者の本人性

一般的に電子サインサービスでは、2 種類の利用者認証が行われる。一つは送信者の認証で、もう一

つは署名者の認証となる。

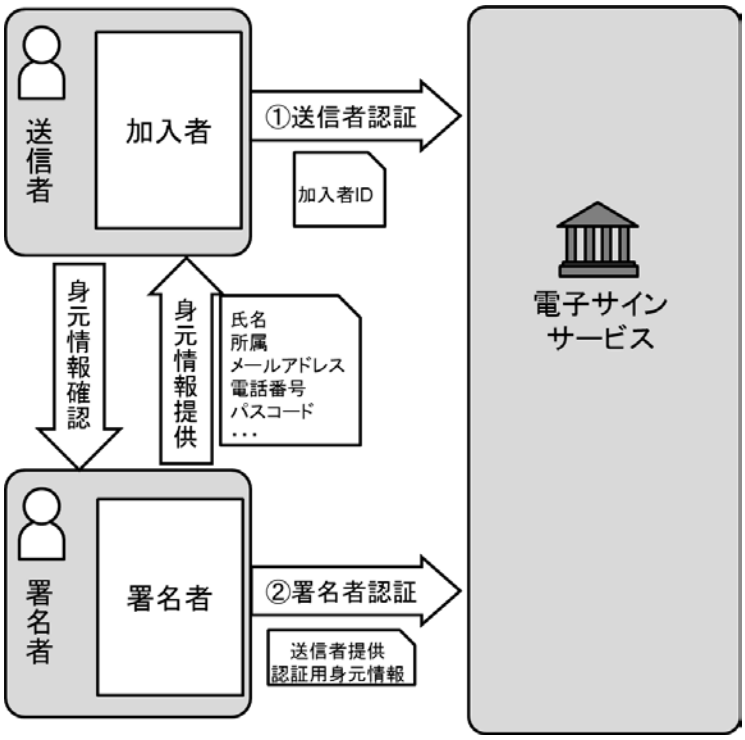

図 5-9 電子サインの利用者認証

① 送信者認証
一般的に、電子サインサービスの加入者であることで送信者になることができる。加入者登録時にサービス事業者がその身元情報を確認する。送信者は電子サインサービスにサインインして利用者認証を行い、認証に成功することで署名依頼が許可される。

② 署名者認証
署名者はサービスの加入者である必要はない。署名者の本人性は、送信者から提供された身元情報に基づいて電子サインサービスが認証し、通常は送信者が提示した電子メールアドレスを使用する。本人性の保証レベルを上げたい場合には、他の認証コードを併用する多要素認証を行うことができる。

利用者（送信者・署名者）の認証に関しては、取引先間や同一組織内などある程度の信頼性が存在する利用者間での利用を想定しているため、利用者の身元情報の保証レベルを上げるよりも、主張された身元情報の利用記録を証拠として残すことを重視している。

【3】文書と署名記録の保管

文書は不正な改ざんが行われないように電子サインサービスのストレージに保管される。署名のプロセス

が進むに従い、署名者の入力や同意・承認の意思を示す痕跡としてのサインや押印などの更新が行われる。署名プロセスが完了すれば、以後は更新されない。

文書の証拠性を確保するため、文書とともに、署名者の本人確認情報、追加入力の記録や署名に関連する情報（署名者、署名日付など）、システムログなどが証跡として保管される。こうした記録のうち、文書名、署名者、署名日付など署名関連の基本的情報の他、IP アドレスや本人確認方法、文書の提示方法（例：電子メールで送信）などを記録したものを監査証跡として表示・出力することができる。

【4】文書と署名記録の利用

署名のプロセスが完了すると関係者に署名済み文書や監査証跡レポートが送付される。また、サービス加入者は自身のアクセスが認められた文書や監査証跡をいつでも入手することができ、契約や同意の証拠として提示することができる。このときには、文書および監査証跡が改ざんされていないことを証明するため、サービス事業者のデジタル署名が付与される。

5.5.2 電子サインの処理フロー

電子サインサービスは、クラウドサービスとして提供され、電子メールとインターネットを利用して以下のような処理を行う。

表 5-15 電子サインサービスが行う処理

処理	処理概要
利用者認証	利用者の認証を行う
文書送信	送信者が指定した文書と記入した文書情報、署名者情報システムに格納し、署名プロセスを開始する
署名	署名者に署名用の画面を用意し、署名者が示した意思に基づいて画面入力や署名情報等を記録する
署名プロセスの進行管理	文書送信や署名などのイベントに応じて、次の処理を開始する
文書や監査証跡の管理と提供	文書や監査証跡等の記録を管理し、利用者に提供する

【1】利用者認証

送信者は、電子サインサービスの加入者であり、登録時にサービス事業者が発行した認証コードによって認証される。

署名者は、送信者が提示した署名者の電子メールアドレスによって認証される。

署名者には、送信者が指定した電子メールアドレスに署名依頼通知が送られる。この通知には文書を閲覧、確認するためのアクセス情報が記載されている。例えば、第三者が推定しえない一時的 URL など。この情報を使用したということが、本人が署名したという証拠になる。また、送信者が指示した認証要素によって追加の認証が行える。署名者の認証の流れを図 5-10 に示す。

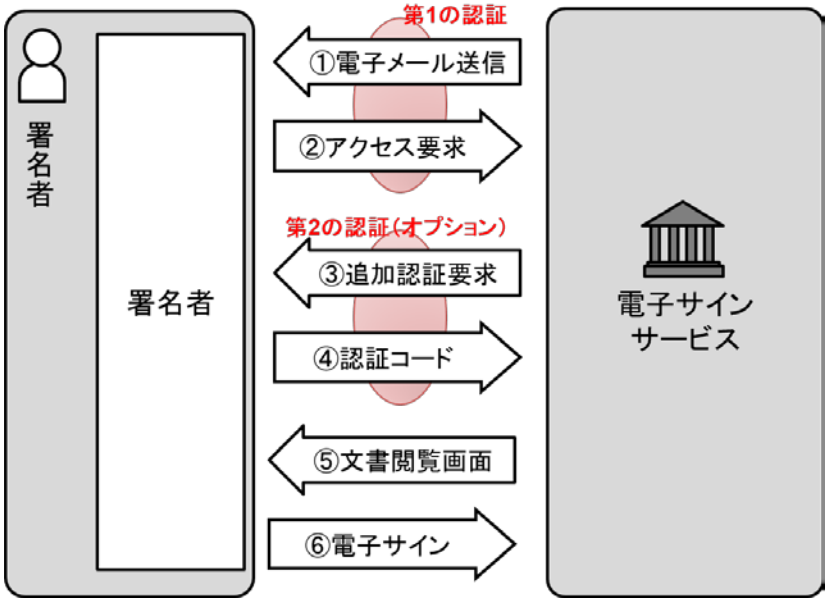

図 5-10 署名者の認証

① 電子メール送信

送信者が指定した電子メールアドレスに署名依頼の電子メールが届く。

② アクセス要求

署名者が署名依頼メールに記されたリンクをクリックしてアクセス画面（文書閲覧画面）を呼び出す。

③ 追加認証要求（オプション）

送信者が追加認証を要求していた場合に、第二の認証を行う画面が表示される。

④ 認証コード（オプション）

署名者は認証の画面に認証コード入力して送信する。

⑤ 文書閲覧画面

署名者の認証に成功すると文書が閲覧できる。

⑥ 署名、送信

署名者は文書内容を確認後、電子サインを行って送信する。

【2】文書送信

文書の作成者が送信者として署名依頼のワークフローを開始する。文書送信時のフローを図 5-11 に示す。

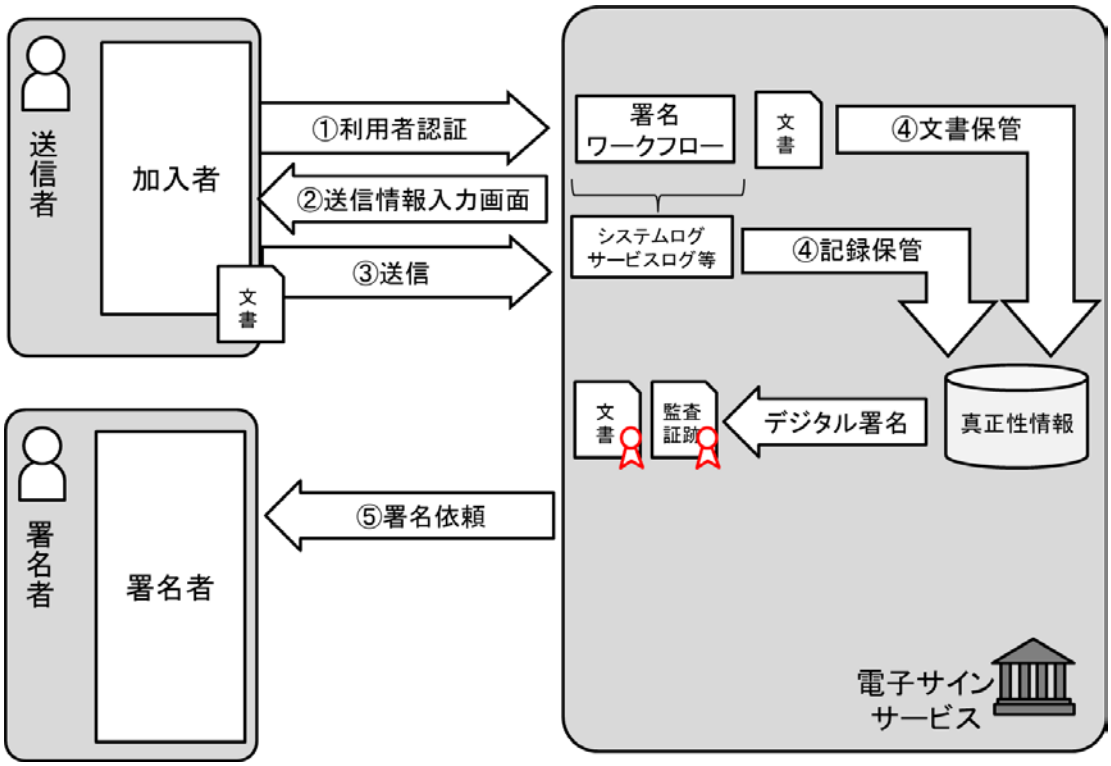

図 5-11 文書送信処理のフロー

① 利用者認証

送信者の認証を行う。

② 送信情報入力

Web ブラウザやアプリ等の画面で、送信する文書ファイルを選択し、署名者情報および文書名などの関連情報の入力を行った上で署名のプロセスを開始する。署名者情報には、電子メールアドレスなどの署名者の身元情報が含まれる。電子サインサービスは、署名者の認証に、ここで指定された身元情報を使用する。

③ 送信（文書その他の情報送信）

送信者が指定した文書ファイルはシステムにアップロードされ、署名者情報などの入力情報もサービスログとともに記録される。署名者用の入力欄やサイン・押印欄が必要な場合はここで作成する。

④ 保管（文書保管・記録保管）

保管段階では画面入力の情報やアップロードされた文書ファイルやシステムログ、サービスログ等を保管する。

⑤ 署名依頼（署名プロセスの開始）

最初の署名者に署名依頼通知を電子メールで送信する。

送信者が自身で署名を行う場合は、引き続いて署名処理も実行される。

【3】署名

送信処理の最後で、電子サインサービスが署名者に署名依頼の電子メールを送信し、署名のワークフローを開始する。署名時には以下の処理を行う。

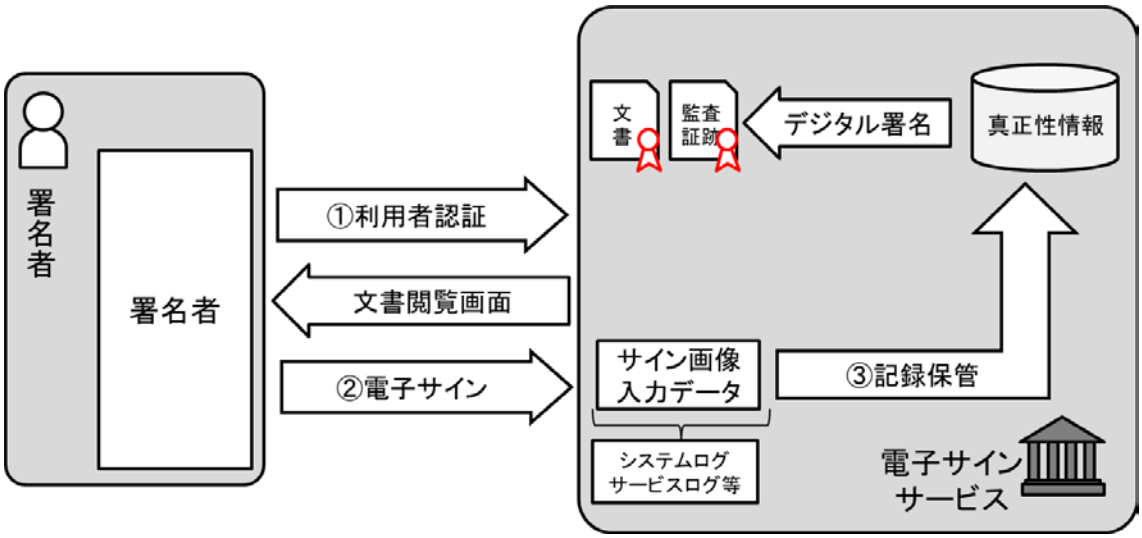

図 5-12 署名処理のフロー

① 利用者認証

署名者は、署名依頼通知に従い、文書閲覧画面にアクセスする。このとき署名者の利用者認証が行われる。

② 入力と署名

署名者は、文書閲覧画面に Web ブラウザやアプリでアクセスし、画面上で入力や署名（同意・承認を示す操作）を行う。

③ 保管

署名者の入力や署名イメージは電子サインサービスに送られ、システムが保管されている文書上でそれを再現して文書を更新する。画面入力の情報やシステムログ、サービスログ等を保管する。

④ 署名プロセスの進行制御

次の署名者があれば、署名依頼通知を送る。最後の署名が完了したのであれば、完了の記録を行う。

【4】文書や監査証跡の管理と提供（記録の管理）

電子サインサービスは、受理した文書と監査証跡、システムログ等を保管する。真正性の検証のために、利用者は文書や監査証跡を画面上で確認したり、ファイルとしてダウンロードしたりする機能を提供する。ダウンロードされるファイルには、サービス事業者のデジタル署名を付与し、このとき、ダウンロード時の事業者の電子証明書が失効していなかったことを保証するため、失効確認情報を文書や監査証跡レポートに埋め込む。

5.5.3 電子サインの開発時、利用時の留意点

【1】サービス加入者の登録と認証

送信者は、サービス利用に先立ってサービス事業者に登録の申請を行う。サービス事業者はそのサービス規程に基づいて加入者の身元情報を確認し、認証コードを発行する。

加入者の身元情報の保証レベルは、個人の自己表明、組織の代表者による身元情報の提供などサービス事業者が用意した枠組みに依存する。

加入者の身元情報の保証レベルは、サービス事業者が検証する身元情報の範囲と確認方法に依存する。電子サイン方式では、個人の自己申告による身元情報が使用されるが、企業にサービスを提供する場合には、組織の管理者が作成するアカウントを ID として使用する利用者のタイプも用意する。

表 5-16 サービス事業者の身元情報検証例

加入者タイプ	身元情報の存在証明	証拠	事業者による検証
個人	自己表明	電子メールアドレス	なし
組織の一員	組織のシステム管理者の表明	ドメイン	ドメインの所有権の確認

認証コードの保証レベルは、偽造に対する強度の違い、認証コードのライフサイクル管理など、サービス事業者が用意した認証コードの特性や運用に依存する。

【2】署名者の身元情報と認証

電子サイン方式では、送信者から指定された電子メールアドレスが署名者の身元情報として使用される。署名者の認証がより厳格に行えるよう、他の身元情報と組み合わせて認証を行う、多要素認証を実装する。

表 5-17 署名者の認証要素例

認証要素		事業者による認証
必須認証要素	電子メールアドレス	送信者が指定した電子メールアドレスに署名依頼を送信
追加認証要素	サービス加入者	サービス加入者としてサインインを要求する
	共有パスコード	送信者が指定したパスコードの入力を署名者に要求する
	電話番号	送信者が指定した電話番号にパスコードを通知する

どの認証要素を使用したかは、サービスのログとして記録し、監査証跡として提供します。

【3】電子サインを利用することによる完全性と真正性の確保

「誰が」、「いつ」、「何を」合意したかは、電子サインサービスが保管している文書と監査証跡によって証明する。しかし、第三者への文書や監査証跡の提示や、組織内の文書管理システムに保管しなければならないことがある。そのため、文書や監査証跡がダウンロードできるようにする必要があるが、このときに文

書および監査証跡の記録の完全性と真正性を確保するために電子サインサービスが電子サインを行う。

表 5-16 に検討すべき主な脅威と対策の例を示す。

表 5-18 検討すべき主な脅威と対策の例

脅威	対策	留意事項
通信における盗聴や傍受	暗号化通信	危殆化していないアルゴリズムを使用して常に暗号化すること
フィッシングメール、なりすましメール	電子メール認証	Sender Policy Framework（SPF）、DomainKeys Identified Mall（DKIM）などにより、送信元の確認ができるようにすること
合意済み文書の偽造、改ざん	秘密鍵の不正利用防止	最終合意済み文書の完全性を保証する電子署名の生成に使う秘密鍵を HSM（Hardware Security Module）で管理すること

【4】保管すべきデジタル記録

監査証跡として利用者に提供するものも含め、サービスに関連する記録は、登録された文書等が登録された当初から改ざんされていないことを証明する上で、重要な役割を果たす。

表 5-17 に保管すべきデジタル記録を示す。

表 5-19 保管すべきデジタル記録と留意事項

種類	内容	記録項目例	留意事項
本人性確認に関係する情報	送信者を特定するための情報	接続日時、接続元の情報、ユーザ ID、パスワード照合結果	いつ、誰が署名プロセスを開始したかをトレースできること。
	署名者を特定するための情報	接続日時、接続元の情報、電子メールアドレス、追加の認証に利用した身元情報	いつ、誰が署名したかをトレースできること
合意の意思に関係する情報	合意の意思を特定するための情報	接続日時、操作場所、操作内容（署名ボタンのクリック等）	いつ、誰が、どのような意思を示したかをトレースできること。
合意内容に関係する情報	システムへの入出力の情報	接続日時、対象文書、入力データ、リクエスト情報、レスポンス情報	署名時の内容と保管している内容が同じであることをトレースできること。

5.6 組織（属性）確認

5.6.1 組織（属性）確認の特長

組織（属性）とは、個人が所属する組織や役職などを指し、従業員が組織としての意思表示（契約など）を行う場合に利用される。電子証明書の属性情報や電子委任状内の情報、属性管理サーバから発行される情報（アサーション等）により、確認することができる。いずれの技術もデジタル署名やサーバ認証などが施され、組織（属性）情報の完全性の保証を担保している。本節では電子証明書に組織（属性）情報を格納する例を挙げて説明する。

5.6.2 組織（属性）確認の処理フロー

組織属性に関して責任を持つ組織により認められたものである必要がある。そのため、組織（属性）の確認としては、組織や当該団体が認めていることを十分に確認した上で電子証明書を発行することになる。具体的には組織に所属する利用者から認証局に対して、所属する組織の組織情報を格納する電子証明書を申請する場合は、当該利用者の所属する組織の実在性及び電子証明書に組織情報を記録することの代表者からの許諾を確認する。

デジタル署名の電子文書を受け取った者は、デジタル署名の検証を行う際に電子証明書の格納内容を確認し、属性（組織）情報を確認する。確認方法については、デジタル署名の確認方法と同等である。

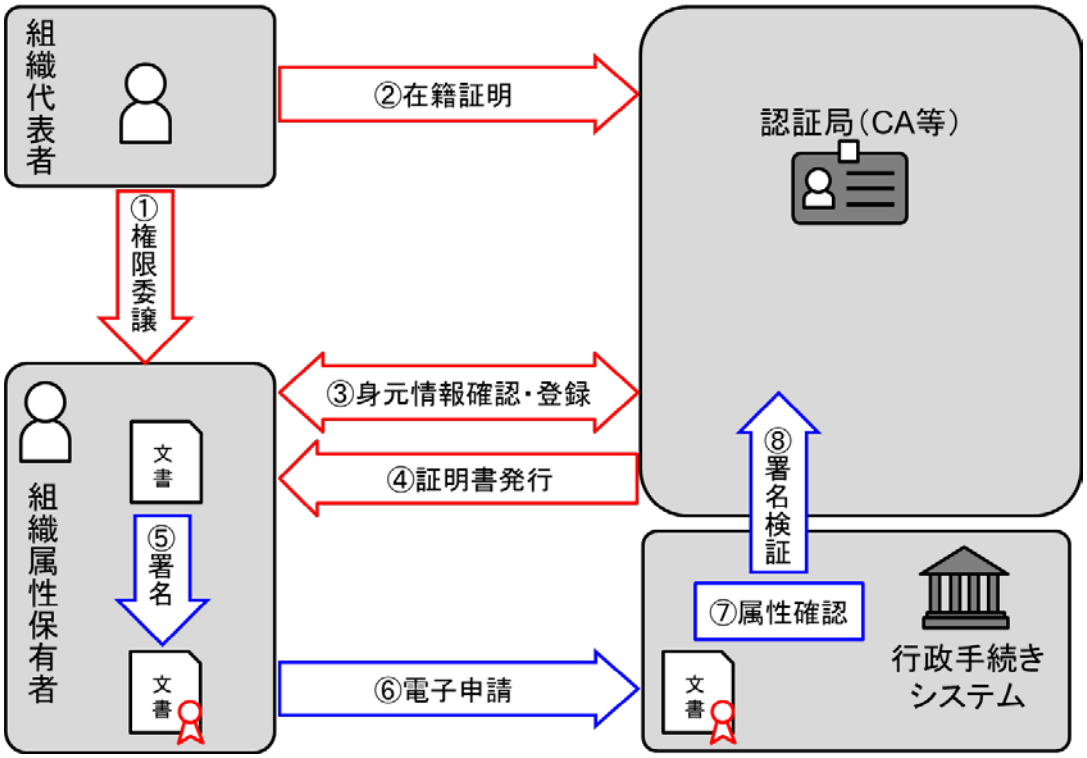

図 5-13 属性（組織）の確認モデル（電子証明書方式）

① 権限委譲

組織代表者が組織属性保有者に権限を委譲する。

② 在籍証明

組織代表者が組織属性保有者の在籍証明を認証局に送る。

③ 身元情報確認・登録

組織属性保有者が登録申請を行い、認証局が身元確認を行う。

④ 証明書発行

認証局が組織属性保有者に対し、属性証明書を発行する。

⑤ 署名

文書（申請書）に対し、署名を実施する。

⑥ 電子申請

行政手続きシステムへ署名文書を送り、申請する。

⑦ 属性確認

行政手続きシステムは、署名文書に付与している証明書から属性を確認する。

⑧ 署名検証

文書の完全性等を確認するために、署名の検証を行う。

組織の属性として主なものは、表 5-20 に示す。

表 5-20 主な組織属性

名称	説明
組織名	「商業登記簿」の「商号」や個人事業主の「屋号」。
組織住所	「商業登記簿」の「本店」の住所。
組織番号	企業を一意に識別可能な番号 例：法人番号（国税庁が付番） 会社法人等番号（法務局が付番） LEI（Legal Entity Identifier：取引主体識別コード） 株式会社帝国データバンクの TDB 企業コード 一般財団法人日本情報経済 社会推進協会の標準企業コード
部門名	部局や部課など。
部門住所	上記「組織住所」以外の部門住所。
メールアドレス	申請を受けたメールアドレス
代表者名	組織の代表者氏名。
代表者肩書	組織代表者の肩書。
役職肩書	役職（組織代表者以外の場合）。

出典：電子証明書に格納された属性情報の信頼性と利用に関するガイドライン（電子認証局会議属性ガイドライン検討会）

5.6.3 組織（属性）確認の開発時、利用時の留意点

電子証明書方式、電子委任状方式にかかわらず記録される情報が、当該発行事業者（電子証明書であれば、電子認証局）が信頼されその事業者が発行していること、かつ改ざん検知の仕組み、有効性の確認の仕組みを有することが重要である。多くはデジタル署名が付与されている、またはサーバ認証が用いられ、発行事業者の信頼性については、第三者機関の認定が一つの目安となる。

5.7 閾値暗号

5.7.1 閾値暗号とは

しきい値暗号（Threshold Cryptography）は、秘密分散法(Secret Sharing Scheme)などを利用した暗号方式であり、鍵を複数に分散する方式や暗号化したデータを複数に分散する方式などが提案、開発されている。現在、NIST（National Institute of Standards and Technology）CSRC（Computer Security Resource Center）では、しきい値暗号化の標準化と検証における課題をまとめ NIST IR 8214 Threshold Schemes for Cryptographic Primitives:

Challenges and Opportunities in Standardization and Validation of Threshold Cryptography を発行している。

用語集

用語	説明
AAL	本人確認プロセスの強度を示したもの。NIST SP800-63-3 で定義されている。
ASP	インターネット等を通じて、アプリケーションを利用させる役割を持つ：Application Service Provider
e-GOV	電子政府の総合窓口。
FAL	認証連携の強度を示したもの。NIST SP800-63-3 で定義されている。
FIDO	Fast IDentity Online の略語で、従来のパスワードに代わるとみられている認証技術のひとつ。FIDO Alliance で規格策定がなされている。
HSM	ハードウェアセキュリティモジュール：Hardware Security Module
IAL	認証プロセスの強度を示したもの。NIST SP800-63-3 で定義されている。
IdP	各種サービスがそれぞれ行う認証を代わって実施し、認証情報（認証結果等）を各種サービスに提供する役割を持つ：Identity Provider
NIST	アメリカ国立標準技術研究所：National Institute of Standards and Technology
OMB	アメリカ合衆国行政管理予算局：Office of Management and Budget
RP	認証を行う各種サービスのこと。IdP と対抗となる役割を持つ：Relying Party
TSA	タイムスタンプ局：Time Stamp Authority
オーセンティケータ	認証を行う時に利用するソフトウェアやハードウェア（認証器）
クレデンシャル	ID やパスワード等の認証で用いられる認証情報

引用規格、引用文献

- 日本規格協会, JIS Q 27000:2019 情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―用語
- 厚生労働省, 医療情報システムの安全管理に関するガイドライン 第 5 版（平成 29 年 5 月）, https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf
- 公益社団法人日本文書情報マネジメント協会(JIIMA) 法務委員会, JIIMA 電子化文書取扱ガイドライン簡易版 （2013 年 10 月）, https://www.jiima.or.jp/wp-content/uploads/policy/denshika_guideline_dijest.pdf
- e-Gov, http://www.e-gov.go.jp/
- 政府電子調達（GEPS）, https://www.geps.go.jp/introduction
- 厚生労働省, 電子処方せんの運用ガイドライン, https://www.mhlw.go.jp/content/10800000/000342367.pdf
- 厚生労働省,電子処方せん引換証, https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000119551_2.pdf
- 一般社団法人 保健医療福祉情報システム工業会, JAHIS 電子処方箋実装ガイド Ver.1.1 https://www.jahis.jp/files/user/04_JAHIS%20standard/18-101_JAHIS%E9%9B%BB%E5%AD%90%E5%87%A6%E6%96%B9%E7%AE%8B%E5%AE%9F%E8%A3%85%E3%82%AC%E3%82%A4%E3%83%89Ver.1.1.pdf
- 特定非営利活動法人 日本ネットワークセキュリティ協会 マイナンバー対応情報セキュリティ検討 WG 構築検討チーム, JNSA マイナンバー業務プロセス・リスク分析シート, https://www.jnsa.org/mynumber/data/mynumber_risk_sheet_ver3_0.pdf
- 総務省, マイナンバーカードを活用したオンライン取引等の可能性について http://www.soumu.go.jp/main_content/000534321.pdf
- NIST SP 800-63-3, Digital Identity Guidelines, https://pages.nist.gov/800-63-3/sp800-63-3.html
- OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf
- 法務省, 電子署名法の概要と認定制度について, http://www.moj.go.jp/MINJI/minji32.html
- ISO 14533-1:2014, Processes, data elements and documents in commerce, industry and administration — Long term signature profiles — Part 1: Long term

signature profiles for CMS Advanced Electronic Signatures (CAdES)
- ISO 14533-2:2012, Processes, data elements and documents in commerce, industry and administration — Long term signature profiles — Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)
- ISO 14533-3:2017, Processes, data elements and documents in commerce, industry and administration — Long term signature profiles — Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)
- ITU-T, X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks
- RFC5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://tools.ietf.org/html/rfc5280
- RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, https://tools.ietf.org/html/rfc6960
- PKCS #12: Personal Information Exchange Syntax Standard, version 1.1, https://web.archive.org/web/20140401120450/http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs12-personal-information-exchange-syntax-standard.htm
- 一般財団法人日本データ通信協会，タイムビジネス信頼・安心認定制度, https://www.dekyo.or.jp/tb/contents/summary/index.html
- RFC6749, The OAuth 2.0 Authorization Framework, https://tools.ietf.org/html/rfc6749
- OASIS, Assertions and Protocols for the OASIS Security Assertion Markup Language, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
- RFC7519, JSON Web Token (JWT), https://tools.ietf.org/html/rfc7519
- RFC7515, JSON Web Signature (JWS), https://tools.ietf.org/html/rfc7515
- NIST IR 8214, Threshold Schemes for Cryptographic Primitives: Challenges and Opportunities in Standardization and Validation of Threshold Cryptography, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8214.pdf

執筆者（五十音順）

新井　聡　　株式会社エヌ・ティ・ティ ネオメイト
今西　祐之　　アドビシステムズ株式会社
上田　祐輔　　アマノセキュアジャパン株式会社
小川　博久　　株式会社三菱総合研究所
菊地　梓　　株式会社 TRUSTDOCK
宮崎　一哉　　三菱電機株式会社
宮地　直人　　有限会社ラング・エッジ
山中　忠和　　三菱電機株式会社

レビュアー（五十音順）

雨宮　明　　日本電気株式会社
佐藤　雅史　　セコム株式会社
杉崎　元　　三菱電機インフォメーションシステムズ株式会社
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