国立国会図書館

調査と情報―ISSUE BRIEF―

No. 1135（2021. 2. 4）

電子契約・電子署名の概要と課題

キーワード：電子契約、電子署名、電子署名法、電子証明書、公開鍵暗号方式、
タイムスタンプ、リモート署名、立会人署名型、トラストサービス

● 新型コロナウイルス感染症の流行を契機に、電子契約や電子署名に注目が集まっている。電子契約とは、契約書等を電子文書で作成する契約方法であり、電子文書の作成者のなりすましや改ざんを防止するための方策の一つとして、公開鍵暗号方式を用いた電子署名が用いられることが多い。

● 企業が電子署名を利用するに当たって、近年登場したリモート署名や立会人署名型の電子署名が、電子署名法に基づく電子署名に該当するかが不明確であるという課題があったが、近時関係省庁が法解釈に関する見解を発表し、電子署名法の適用が認められる可能性が示された。

● 今後の課題としては、電子署名法の適用要件の更なる明確化、特定認証業務の認定制度の在り方の検討、トラストサービスの制度整備が挙げられる。

国立国会図書館 調査及び立法考査局
経済産業課　鈴木（すずき） 絢子（あやこ）

第１１３５号

はじめに

新型コロナウイルス感染症の流行を契機に、政府や企業では、これまでの書面・対面・押印の手続を見直し、オンラインのみで完結する電子契約や電子申請を積極的に取り入れようとする機運が高まっている。令和2年7月、政府は、経済団体とともに、「「書面、押印、対面」を原則とした制度・慣行・意識の抜本的見直しに向けた共同宣言」[1]を採択した。宣言では、社会課題として顕在化した「書面、押印、対面」を見直し、行政手続と民間取引の双方におけるデジタル化を推進することが掲げられ、民間取引に関しては押印の廃止や書面の電子化、電子署名の活用等が挙げられた。電子署名については、近年、クラウドを利用した新しいタイプの電子署名サービスが出現し、迅速性や利便性を背景に普及しつつある。

令和2年7月の「企業IT利活用動向追跡調査」によると、取引先との間で電子契約を採用していると回答した企業は約4割であった[2]。さらに、電子契約を今後採用することを検討していると回答した企業は4割弱存在し、企業の電子契約への関心の高さがうかがえる。

一方、企業が電子契約を採用する上で、「電子署名及び認証業務に関する法律」（平成12年法律第102号。以下「電子署名法」）を始めとする関係法律の解釈が明瞭でない点が問題となっていた。これに対処するため、近時、関係省庁が法解釈に関する見解を相次いで発表した[3]。

本稿では、電子契約及び電子署名の概要をまとめるとともに、関係省庁が発表した電子署名法の解釈に関する見解について概説し、今後の課題を論じる。

Ⅰ　電子契約

1　電子契約とは

電子契約とは、契約書や注文書・請書を電磁的記録（電子文書のこと）で作成する契約方法をいう[4]。民法（明治29年法律第89号）第522条第2項は、「契約の成立には、法令に特別の定めがある場合を除き、書面の作成その他の方式を具備することを要しない」として、契約方式の自由を定めている。したがって、書面を作成しない電子契約であっても有効に成立する。

また、技術的な実現方式も自由であり、後述する電子署名が使われていなくてもよい。法令

---

* 本稿におけるインターネット情報の最終アクセス日は、令和3年1月28日である。

1 「「書面、押印、対面」を原則とした制度・慣行・意識の抜本的見直しに向けた共同宣言―デジタル技術の積極活用による行政手続・ビジネス様式の再構築―」2020.7.8. 内閣府ウェブサイト <https://www8.cao.go.jp/kisei-kaikaku/kisei/publication/document/200708document01.pdf>

2 日本情報経済社会推進協会「「企業IT利活用動向追跡調査2020」集計結果（詳細版）」2020.9, p.48. <https://www.jipdec.or.jp/archives/publications/J0005164.pdf> なお、この場合の電子契約は、電子署名の有無は問わない。

3 本稿では主に、総務省ほか「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ&A（電子署名法2条1項に関するQ&A）」2020.7.17. 経済産業省ウェブサイト <https://www.meti.go.jp/covid-19/denshishomei_qa.html>; 同「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ&A（電子署名法3条に関するQ&A）」2020.9.4. 同 <https://www.meti.go.jp/covid-19/denshishomei3_qa.html> を取り上げる。このほかに出されたものとして、法務省ほか「論点に対する回答」（規制改革推進会議第10回成長戦略ワーキング・グループ 資料1-2）2020.5.12. 内閣府ウェブサイト <https://www8.cao.go.jp/kisei-kaikaku/kisei/meeting/wg/seicho/20200512/200512seicho04.pdf>; 内閣府ほか「押印についてのQ&A」2020.6.19. <https://www8.cao.go.jp/kisei-kaikaku/kisei/publication/document/200619document01.pdf> 等がある。

4 宮内宏「電子契約をめぐる法規制と導入の検討軸」『ビジネス法務』20巻4号, 2020.4, p.13.

によっては、契約において一定の内容を記載した書面の交付を義務付けているものがあるが、電子文書で代えることができる旨の規定が置かれているものもある[5]。

2　電子契約の利点

電子契約の利点は、第1に迅速性と経済性である[6]。紙の契約書の場合、契約書の印刷、押印、相手方への郵送、返送などに相応の手間と日数を要する。電子契約は、電磁的記録を電子的に送信するため、簡便・迅速に手続を行うことができる。また、税法上、契約書等の取引情報に関する書面は、一定期間保存する義務があり[7]、紙として保存するためのスペースが必要だが、電子契約の場合は、電子帳簿保存法[8]において、電子契約に関する電磁的記録をそのまま保存する方法が認められている（同法第10条）。さらに、文書による契約書には原則として印紙税がかかるが、電子契約書は課税文書に当たらないとの運用がなされている[9]。

第2に、締結した契約の管理等に係る利便性である。電磁的記録であれば検索ができるので、決済や税務申告に必要な情報収集も容易になり、監査の効率も著しく向上する[10]。

第3に、改ざんの防止や検証ができることである。一般に、電子文書は、本人以外の者が作成する「なりすまし」や改ざんが容易であるというデメリットが指摘されるが、紙の文書であっても改ざんや印鑑・署名の偽造は可能である。しかし、後述するデジタル署名やタイムスタンプ等の信頼性の高い方法を用いた電子契約では、改ざんの防止や検証が紙の文書よりも厳格にできる。この点を、電子契約の第3の利点として挙げることができよう[11]。

3　電子契約の民事訴訟上の取扱い（電子署名法第3条）

前述のように、契約書は契約の成立要件ではないが、後に契約の成立や内容をめぐって裁判になった際に、署名・押印がある契約書は有力な証拠となり得る。

民事訴訟で書面による証拠を提出する場合には、その書面の作成者とされる人が、本人の意思に基づいて作成したものであること（これを「真正な成立」という。）を証明しなければならない（民事訴訟法（平成8年法律第109号。以下「民訴法」）第228条第1項）。その際、証拠として提出した書面に、本人又はその代理人の署名又は押印があるときは、その文書は真正に成立したものと推定される（同法第228条第4項）。ただし、書面に本人名義の署名や押印があるだけでは文書の真正な成立の推定は認められず、本人の意思に基づく署名又は押印であることを証明する必要がある。

---

5 例えば、保証契約は民法第446条第2項で書面を要するとされているが、同条第3項により電子文書で代替することが認められている。

6 宮内　前掲注(4), pp.14-15; 牧野二郎・牧野剛「信頼性や導入メリットは？電子契約の基本」『ビジネス法務』17巻10号, 2017.10, pp.49-50.

7 法人税法施行規則（昭和40年大蔵省令第12号）第59条等。

8 正式名称は、「電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律」（平成10年法律第25号）。電子文書の保存に関する法律の1つで、主に国税関係の帳簿を電子データとして保存する手段について定めた法律。

9 「参議院議員櫻井充君提出印紙税に関する質問に対する答弁書」（平成17年3月15日内閣参質162第9号）<https://www.sangiin.go.jp/japanese/joho1/kousei/syuisyo/162/touh/t162009.htm>

10 宮内　前掲注(4), pp.14-15; 牧野二郎・牧野剛　前掲注(6), p.49.

11 高橋郁夫ほか編『即実践!!電子契約―電子契約・DX・文書管理〈文書の電子化〉の導入から運用まですべてを体験できる―』日本加除出版, 2020, p.40.

印鑑の場合、通常は一定の水準以上の注意をもってこれを管理すると考えられる。そのため、文書に押印されている印影が、印鑑証明書等により、本人の印鑑により顕出されたものであると認定されれば、反証のない限り、当該印影は本人の意思に基づいて行われたものと推定される（一段目の推定）[12]。これにより、民訴法第 228 条第 4 項に基づき、当該文書について真正な成立が推定される（二段目の推定）。この論理を「二段の推定」という（表 1 左列）[13]。

表１　二段の推定の考え方

	紙の文書の場合	電子文書の場合
一段目の推定	本人の印鑑による印影であることが認定されれば、本人の意思による押印を推定する （最判昭和 39.5.12 民集 18 巻 4 号 597 頁）	本人の電子署名であることが認定されれば、本人の意思による電子署名の生成を推定する (注)
二段目の推定	本人の（意思による）押印があれば、私文書の真正な成立を推定する （民事訴訟法第 228 条第 4 項）	本人（の意思）による電子署名があれば、電子文書の真正な成立を推定する （電子署名法第 3 条）

（注）電子契約についての判例は現時点では存在しないが、当事者の電子署名を付す電子契約に関しては同様の推定が及ぶ可能性が高いと考えられている（圓道至剛「二段の推定との関係，証拠提出の方法等 電子契約の民事訴訟上の取扱い」『ビジネス法務』20 巻 4 号，2020.4，p.23）。
（出典）宮内宏編著『電子契約の教科書―基礎から導入事例まで―　改訂版』日本法令，2019，p.56 を基に筆者作成。

電子契約の場合は、電子署名法第 3 条において、一定の要件を満たす電子署名が行われていれば、当該電子文書は真正に成立したものと推定するとの規定が設けられている。なお、同法第 3 条は、民訴法第 228 条第 4 項と同様に、二段の推定における二段目の推定と同じ効果を定めたものである。したがって、一段目の推定は、ここでも証明する必要がある（表 1 右列）[14]。

４　電子委任状

法人が結ぶ電子契約であっても、契約書となる電子文書に付される電子署名は、法人の組織名でなく個人の電子署名になる。これは、電子署名法が、電子署名の実施者が個人（自然人）であることを前提としていることに基づく[15]。

一方、実務においては、法人契約の全てに代表者自身が署名をすることは現実的ではなく、法人の代表者から委任を受けた使用人等が契約手続を行うこともある。そこで、電子契約においても、当該使用人等が代表者から委任されていることを示すため、「電子委任状」を国の認定機関[16]が発行し、使用人等がそれにより代理権を表示して契約手続を行えるようにした。この法律が、電子委任状法（「電子委任状の普及の促進に関する法律」（平成 29 年法律第 64 号））である。これにより、法人の代表者以外の者による電子署名であっても、契約の相手方が安心

12 最高裁判例昭和 39 年 5 月 12 日民集 18 巻 4 号 597 頁。
13 高林淳・商事法務編『電子契約導入ガイドブック　国内契約編』商事法務，2020，pp.126-131. なお、今般の関係省庁による見解では、文書上に本人による押印がなくても、他の方法によって文書の真正な成立を立証することは可能であることが強調されている（内閣府ほか　前掲注(3)，p.2）。
14 関係省庁による見解でも、第 3 条は「電子署名を行ったのが本人であること自体を推定するものでなく、電子署名を行ったのが本人であると裁判所により認定されることを要件として、電磁的記録の成立の真正を推定するものである」とされる（法務省ほか　前掲注(3)）。
15 電子署名法第 2 条第 1 項第 1 号、同法施行規則（平成 13 年総務省・法務省・経済産業省令第 2 号）第 5 条第 1 項等。
16 認定は業務に対し行われる。令和 2 年 7 月現在、7 つの業務が認定を受けている（「電子委任状取扱業務の認定について」総務省ウェブサイト <https://www.soumu.go.jp/menu_seisaku/ictseisaku/ictriyou/densi_ininjou/nintei.html>）。

して法人と電子契約できるようになった。

Ⅱ　電子署名

電子契約の方式に決まりはないが、電子文書の作成者のなりすましや改ざんを防止するための方策の 1 つとして、電子署名が用いられることが多い。単に「電子署名」（electronic signature）と言う場合の概念は多義的であるが[17]、日本で法的に定義された電子署名は、電子署名法に基づくものである。以下でその要件と仕組みについて解説する。

1　電子署名法に基づく電子署名

(1) 電子署名法第 2 条第 1 項の電子署名

電子署名法とは、安全かつ信頼性のある電子商取引を促進するため、一定の要件を満たす電子署名が、手書きの署名や押印と同等に通用することを規定した法律であり、平成 13 年 4 月に施行された。同法に基づく「電子署名」とは、第 2 条第 1 項において、電磁的記録に記録することができる情報について行われる措置であって、①当該情報が当該措置（電子署名）を行った者により作成されたことを示すものであること（本人性）、②当該情報について改変が行われていないことを確認できること（非改ざん性）の 2 つの要件を満たしているものと定められている[18]。

①の「本人性」においては、署名者が電磁的記録を作成したことを「示すもの」であれば足り、署名者が誰であるかという身元確認がされている必要はない。また、②の「非改ざん性」についても、将来的な技術変化に対応するため、具体的な方法の指定はされていない。

このように同条の電子署名の定義は、身元確認や一定の技術水準の充足が求められていない緩い定義であり、印鑑に例えると、三文判から実印まで全ての印鑑を含んだ概念と言える[19]。

(2) 電子署名法第 3 条の電子署名

電子署名法第 3 条は、一定の要件を満たす電子署名が行われている場合には、当該電子文書は真正に成立したと推定するとしている。第 3 条が適用されるためには、（ア）第 2 条第 1 項で定義される「電子署名」であること（①本人性、②非改ざん性）に加え、（イ）「これ（当該電子署名）を行うために必要な符号及び物件（秘密鍵や IC カード等）を適正に管理することにより、本人だけが行うことができることとなるもの」であること、（ウ）本人による（本人の意思に基づく）電子署名であることが要件とされている[20]。第 3 条が適用される電子署名には、（イ）のとおり一定の技術水準が求められており、印鑑でいうところの実印に近い概念と言える[21]。

---

17 例えば、タブレットに表示された電子文書にタッチペンで署名したものも電子的な署名であることには変わりない。
18 宮内宏編著『電子契約の教科書―基礎から導入事例まで―　改訂版』日本法令, 2019, p.29.
19 高林・商事法務編　前掲注(13), pp.95-96.
20 宮内編著　前掲注(18), p.30; 同上, pp.129-131; 福岡真之介「電子署名法 3 条の推定効についての一考察」『NBL』1179 号, 2020.10.1, pp.35-36.
21 「第 11 回成長戦略ワーキング・グループ議事概要」2020.5.22, p.28. 内閣府ウェブサイト <https://www8.cao.go.jp/kisei-kaikaku/kisei/meeting/wg/seicho/20200522/gijiroku0522.pdf>

電子署名法第３条

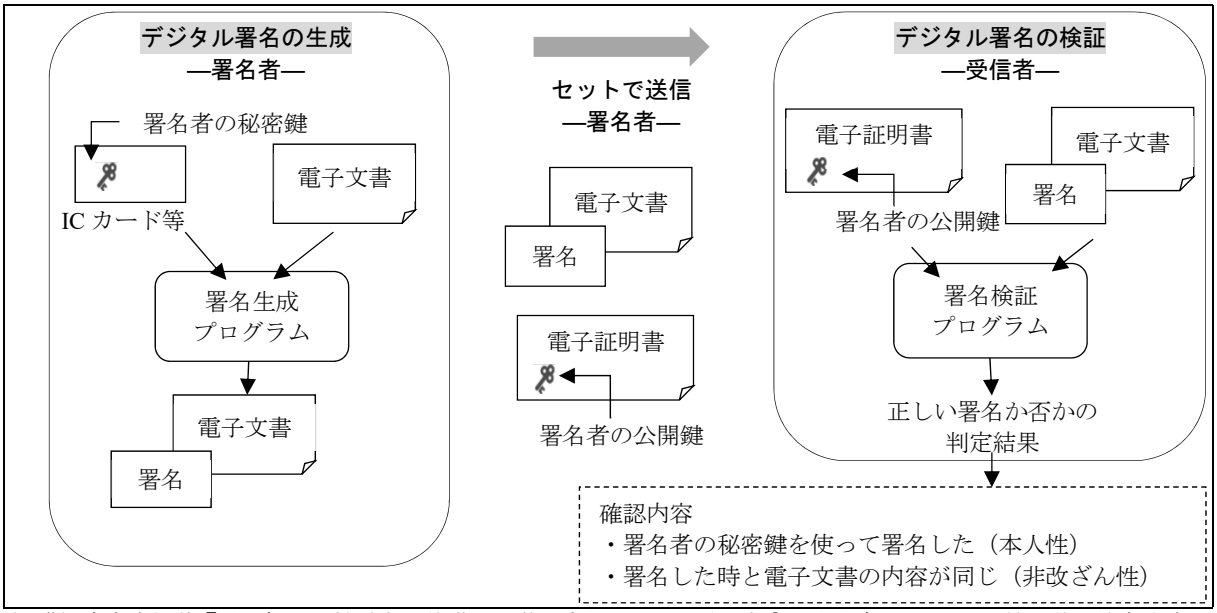
電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

２　電子署名の仕組み

電子署名法第 2 条第 1 項の①本人性と②非改ざん性を、暗号技術を使って検証できるものを「デジタル署名」（digital signature）という[22]。現在、デジタル署名に一般に用いられる暗号技術は、公開鍵暗号方式である。公開鍵暗号方式とは、秘密鍵と公開鍵という 2 つの鍵を 1 組の暗号鍵として用い、2 つの鍵を合わせたときに初めて暗号が解けるようにしたものである。

デジタル署名を生成することを「署名」、デジタル署名が有効であることを確認することを署名の「検証」という[23]。図 1 は、デジタル署名の生成と検証の仕組みを図示したものである。

図１　デジタル署名の生成と検証



（出典）宮内宏編著『電子契約の教科書―基礎から導入事例まで―　改訂版』日本法令, 2019, p.25 等を基に筆者作成。

署名したい電子文書と、署名者の秘密鍵（署名に使うため署名鍵ともいう。）の両方を、署名生成プログラムに投入すると、一種の暗号化が実施され、署名が生成される[24]。署名の検証には、署名生成時に用いた秘密鍵と 1 対 1 に対応する公開鍵を使う。この公開鍵が、署名者本人のものであることを示すことにより、署名が本人により生成されたことが示される。

---

[22] 「Q4.電子署名とデジタル署名の違いはなんですか？」2020.9.16. 日本ネットワークセキュリティ協会ウェブサイト <https://www.jnsa.org/result/e-signature/e-signature-qa/index.html#TId_433689edd43ef17eaa23f7c41256d320>

[23] 「2.4 デジタル署名（PKI 関連技術情報）」2012.7.20. 情報処理推進機構ウェブサイト <https://www.ipa.go.jp/security/pki/024.html>

[24] 厳密には、電子文書をそのまま暗号化すると処理時間がかかるため、電子文書をハッシュ関数に入力して得られたハッシュ値を対象に、暗号化及び復号を行う。ハッシュ関数とは、任意の大きさの文書を入力して、固定長のデータを作成するもの。

公開鍵の持ち主を特定するためには、電子証明書が用いられる。電子証明書とは、紙の世界の印鑑証明書に相当するもので、公開鍵とその持ち主が記載されている（電子証明書については後述）[25]。

署名者は、署名対象の電子文書、デジタル署名、電子証明書をセットで相手方に送信する[26]。受信者は、電子文書、デジタル署名、電子証明書記載の公開鍵を検証プログラムに投入し、その3つが整合的かどうかを判定する[27]。

3　認証業務と電子証明書

前述のとおり、公開鍵暗号方式を用いた電子署名（デジタル署名）では、電子署名が本人のものかを証明するために、電子証明書を用いる。電子署名法では、電子署名が本人のものかどうかを証明する業務を「認証業務」という（第2条第2項）。

表2は、国内における主な認証業務の種類である[28]。電子署名法に基づくものとしては、公開鍵暗号方式を用いた電子署名の認証業務（特定認証業務）、特定認証業務のうち一定の基準を満たしたもので主務大臣に認定された認証業務（認定認証業務）がある（表2）。

表2　主な認証業務の種類

認証業務	概要	発行対象	関連法令
特定認証業務	認証業務のうち、電子署名法で規定している技術的な基準に適合している認証業務（現在の基準では、公開鍵暗号方式を用いた電子署名の認証業務）。信頼性向上のために、第三者機関の認定を受けている場合がある。	個人	電子署名法第2条第3項、同法施行規則第2条
認定認証業務	特定認証業務のうち、電子署名法で規定している設備・本人確認の方法・業務体制等の基準に適合し、主務大臣の認定を受けた認証業務。※認定認証業務の数は、令和2年10月時点で9業務。	個人	電子署名法第4条
商業登記に基づく電子認証制度	登記所に商業登記された法人の登記情報に基づき、登記所が行う認証業務。商業登記に基づくものであるという制度上、代表取締役や支配人の電子証明書のみが発行される。	法人代表者等	商業登記法第12条の2

（出典）宮内宏編著『電子契約の教科書―基礎から導入事例まで―　改訂版』日本法令, 2019, pp.34, 38; 日本文書情報マネジメント協会電子契約委員会「電子契約活用ガイドライン」2019.5, p.17. <https://www.jiima.or.jp/wp-content/uploads/policy/denshikeiyaku_guideline_20190619.pdf> 等を基に筆者作成。

認証業務を行う者は「認証局」と呼ばれる。認証局は、利用者の申請に基づき本人確認を行い、公開鍵とその持ち主を示した電子証明書を発行する。

電子証明書を発行する際の本人確認のレベルは、認証局により異なる。認定認証業務を行う認証局（認定認証局）は、主務大臣の認定を受ける基準として、住民票の写しや印鑑証明書等を用いた「利用者の真偽の確認」が要件となっているため[29]、本人確認の信頼性は高い。一方、

25 宮内編著　前掲注(18), pp.21-25.
26 デジタル署名は、本文図1のように元の電子文書と併せて1つのファイルに格納することも、別のファイルで保存することもできる（同上, p.22）。
27 同上, pp.23-25.
28 このほか、主なものとして、マイナンバーカードを用いた公的個人認証基盤があるが、電子証明書に個人の住所等が記載されるため、企業での利用は想定しにくい。
29 電子署名法第6条第1項第2号、同法施行規則第5条。

主務大臣の認定を要せず、特定認証業務を行う認証局（特定認証局）は、より簡便な方法での本人確認が可能である。本人確認の手段によっては、認定認証局の電子証明書に比べ信頼性が劣る可能性もあるが、その分、迅速かつ低価格で電子証明書が取得できるというメリットがあり、用途や目的に応じた使い分けが必要である[30]。

４　タイムスタンプと長期署名

電子証明書の有効期間は、電子署名法施行規則（平成 13 年総務省・法務省・経済産業省令第 2 号）第 6 条第 4 号により、5 年を超えないものとすることが定められている。デジタル署名だけでは、いつ署名が行われたか明らかでないため、電子証明書の有効期間内に行われたデジタル署名であることを証明するために、タイムスタンプが用いられる[31]。

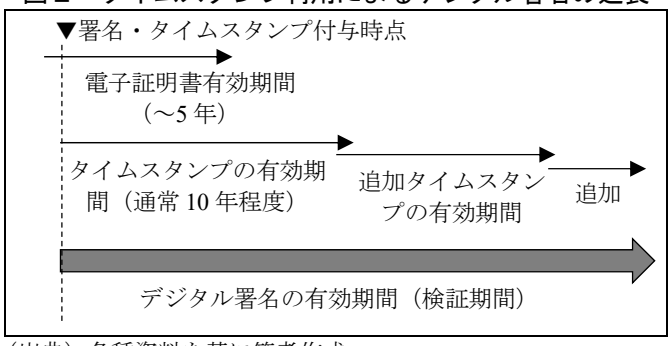
タイムスタンプとは、記録されている時刻にその文書が存在し（存在証明）、その時刻以降文書が改ざんされていないことを証明する（非改ざん性証明）ものである。タイムスタンプの信頼の基盤は、タイムスタンプを発行する時刻認証局（Time-Stamping Authority: TSA）が信頼できる第 3 者（Trusted Third Party: TTP）であることに基づいている。これは、紙文書において、郵便局が TTP となり、その消印を用いるのと同じ考え方である[32]。

日本では、日本データ通信協会の認定[33]を受けた TSA（現在 5 事業者）が発行する認定タイムスタンプが、信頼性の高いタイムスタンプとして扱われる。利用者は、タイムスタンプを付与したい電子データ（デジタル署名付き電子文書等）[34]を TSA に送付する。TSA は、それに時刻情報を付与し、偽造できないようにして結合した[35]タイムスタンプを利用者に送付する。

なお、タイムスタンプにも有効期間があるが、期限切れ前に再びタイムスタンプを付加し続けることで、デジタル署名の有効性を延長し、検証できる状態を維持することができる（図 2）。この方法を長期署名といい、国際標準化されたフォーマットが存在する[36]。

認定タイムスタンプは、法令等でその利用が定められる[37]など、証明力への信頼性は高い。ただし、法的効果を定めた法律

図２　タイムスタンプ利用によるデジタル署名の延長



（出典）各種資料を基に筆者作成。

30 高林・商事法務編　前掲注(13), p.103.
31 天野文雄「契約者署名型,サービス提供者署名型,サイン型電子契約の種類と技術」『ビジネス法務』20 巻 4 号, 2020.4, pp.20-21.
32 「タイムスタンプのしくみ」日本データ通信協会タイムビジネス認定センターウェブサイト <https://www.dekyo.or.jp/tb/contents/summary/system_2.html>
33 総務省の「タイムビジネスに係る指針」（平成 16 年 11 月 5 日策定）を基に、平成 17 年に日本データ通信協会が始めた任意の認定制度「タイムビジネス信頼・安心認定制度」に基づく認定（「制度概要」日本データ通信協会ウェブサイト <https://www.dekyo.or.jp/tb/contents/summary/index.html>）。
34 厳密には、電子データをハッシュ関数に入力して得られたハッシュ値を、TSA に送付する。
35 偽造防止の仕組みは、タイムスタンプの方式により異なるが、タイムスタンプに TSA が自身のデジタル署名を付す方式が一般的である（「タイムスタンプのしくみ」前掲注(32)）。
36 天野　前掲注(31), p.21.
37 例えば、電子帳簿保存法施行規則（平成 10 年大蔵省令第 43 号）では、国税関係書類をスキャナ保存する際の要件として、認定タイムスタンプの付与が義務付けられている。

は日本にはないため、制度の永続性や国際的な通用性が保証されるかが課題となっており、総務省の検討会で、国の認定制度の創設について検討がなされている[38]。

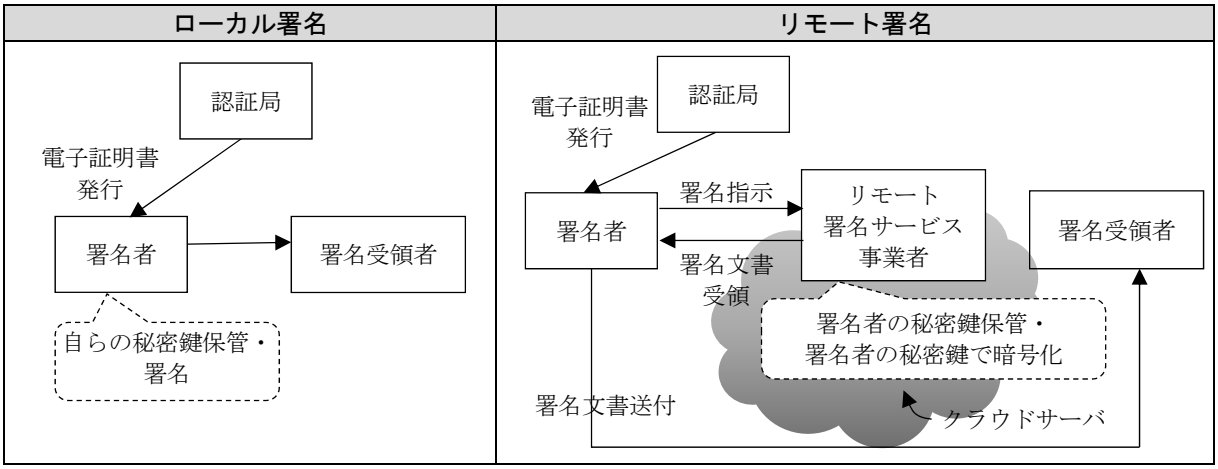
Ⅲ　新しい電子署名サービス

１　リモート署名

電子署名法の制定（平成 12 年）当時は、図 1 のように、署名者が、秘密鍵が格納された IC カード等を手元に保管し、自身の環境下で署名を行うことが想定されていた（これを「ローカル署名」という。）。しかし、近年のクラウドサービスの普及やマルチデバイス化を背景に、署名者の秘密鍵をクラウドサーバに保管し、署名者の指示に基づき、クラウド上で第三者が署名者の秘密鍵を用いて暗号化を行う「リモート署名」が普及しつつある（図 3）[39]。

リモート署名のメリットとしては、一定のネットワーク環境があれば、端末を選ばずにデジタル署名を利用できること、IC カードの紛失等のリスクがなくなること等がある[40]。リモート署名では、本人以外が不正に署名できないよう、高度なユーザー認証とセキュリティが求められる。日本では、日本トラストテクノロジー協議会が、秘密鍵の管理や運用等に関して、リモート署名サービス事業者が参照すべきセキュリティ基準等を示した「リモート署名ガイドライン」を公表している[41]。

図３　ローカル署名とリモート署名の例



（出典）日本トラストテクノロジー協議会「リモート署名ガイドライン」2020.4.30, p.9. 日本ネットワークセキュリティ協会 <https://www.jnsa.org/result/jt2a/data/RemoteSignatureGguide_All-r1.pdf> を基に筆者作成。

38 サイバーセキュリティ統括官室「タイムスタンプ認定制度の現状と主な論点について」（第 1 回タイムスタンプ認定制度に関する検討会 資料 1-2）2020.3.30, pp.2, 10. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000679656.pdf>

39 日本トラストテクノロジー協議会「リモート署名ガイドライン」2020.4.30, p.8. 日本ネットワークセキュリティ協会 <https://www.jnsa.org/result/jt2a/data/RemoteSignatureGguide_All-r1.pdf>

40 「トラストサービスに関する主な検討事項」（プラットフォームサービスに関する研究会トラストサービス検討ワーキンググループ（第 1 回） 資料 1-2）2019.1.31, p.9. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000597573.pdf>

41 日本トラストテクノロジー協議会　前掲注(39)

２　立会人署名型

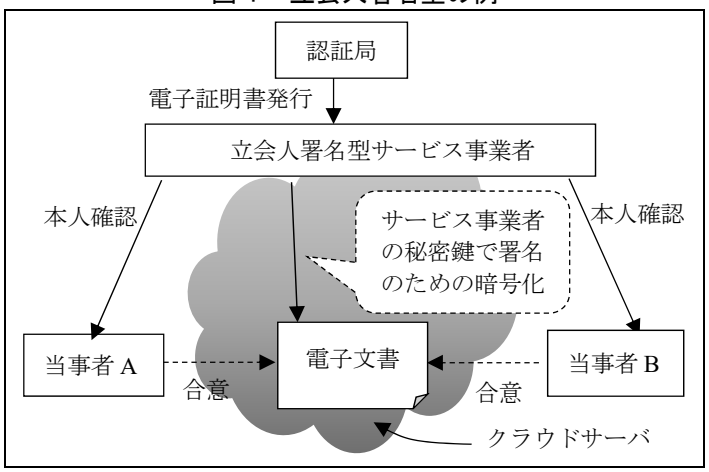
電子契約において、取引の相手方にも契約書となる電子文書へのデジタル署名を求める場合、相手方にも電子証明書の取得等を行ってもらわなければならず、電子契約導入の大きな障壁となってきた。そこで近年、電子契約の際に、契約当事者のデジタル署名でなく、第三者であるサービス事業者が、立会人的な立場で自身のデジタル署名を用いる、「立会人署名型」[42]の電子署名サービスが普及している（図４）。立会人署名型は、その簡便さから、日本の電子署名市場の過半を占めているとされる[43]。

立会人署名型の仕組みとして一例を挙げる。まず、契約の当事者Ａが、サービス事業者の提供するクラウドサーバに、契約書となる電子文書をアップロードする。すると、相手方として指定した当事者Ｂのメールアドレス宛てに、当該電子文書へのアクセスURLが記載されたメールが届く。当事者Ｂはメールに記載された URL にアクセスして、合意の意思を示す操作をする。これにより契約が締結される。

契約締結と同時に、サービス事業者から当事者Ａ及びＢ宛てに、サービス事業者のデジタル署名が付与された契約書のファイルがメールで届く[44]。

この例では、当事者Ａ及びＢのデジタル署名を用いない代わりに、二要素認証[45]や利用者のアクセスログ等を使い、本人確認や意思の確認が行われる。

図４　立会人署名型の例



（出典）高橋郁夫ほか編『即実践!!電子契約―電子契約・DX・文書管理〈文書の電子化〉の導入から運用まですべてを体験できる―』日本加除出版, 2020, pp.323-325 等を基に筆者作成。

Ⅳ　法的効果に関する見解と課題

近年利用されるようになってきたリモート署名や立会人署名型の電子署名は、電子署名法に基づく電子署名に当たるかが不明確であり、企業からは明確化が求められていた。

この点につき、総務省・法務省・経済産業省は、令和２年５月の成長戦略に関する会議において、「論点に対する回答」と題する報告を行い、リモート署名には電子署名法第２条第１項、第３条が適用され得るが、立会人署名型は「本人による電子署名」には当たらず、第３条の推

---

42 同様の類型を指す呼び名として、クラウド型、事業者署名型等がある。ただし、クラウド型については、クラウドを利用したリモート署名（当事者の秘密鍵による署名）を指す場合と、クラウドを利用した立会人署名型（事業者の秘密鍵による署名）を指す場合がある。

43 「電子署名 脱ハンコで急拡大　3年後200億円市場に」『日本経済新聞』2020.10.13.

44 高橋ほか編　前掲注(11), pp.323-325; 弁護士ドットコム株式会社クラウドサイン事業本部「クラウドサインによる電子契約の締結等に関する説明書 第５版」2020.10.22, pp.3-7. <https://www.cloudsign.jp/pdf/litigation_support_documents.pdf>

45 本人確認に異なる要素を２つ組み合わせる方法。利用者が、あらかじめ登録されたメールアドレス及びログインパスワードの入力に加え、当該メールアドレスの利用以外の手段（スマートフォンへのSMS送信や手元にあるワンタイム・パスワード生成機器の利用等）により取得したワンタイム・パスワードの入力を行うことにより、認証を行うものなどが挙げられる。

定効は働き得ないとの考えを示した[46]。これに対して、立会人署名型の取扱いについては、使い勝手の観点から再考を促す意見が出されていた[47]。

総務省・法務省・経済産業省は、立会人署名型に関する解釈を見直すとともに、リモート署名も含め、法適用の要件を詳細化する形で、令和2年7月に「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ&A（電子署名法2条1項に関するQ&A）」（以下「2条1項Q&A」）[48]を、続く9月に「同（電子署名法3条に関するQ&A）」（以下「3条Q&A」）[49]を発表した。

1　2条1項Q&A

リモート署名や立会人署名型は、直接的にはサービス事業者が、利用者の指示に基づき署名のための暗号化を行っている。このことから、電子署名法第2条第1項の要件である、「①当該情報が当該措置（電子署名）を行った者により作成されたことを示すものであること（本人性）」について、「当該措置を行った者」（署名者）が利用者なのか、サービス事業者なのかが問題となる。

この点について、2条1項Q&Aでは、物理的にはA（サービス事業者）が署名のための暗号化を行った場合であっても、B（契約当事者）の意思のみに基づき、Aの意思が介在することなく暗号化が行われたと認められる場合であれば、署名者はBであると評価することができるとの考えが示された。

また、立会人署名型についても、サービス事業者の意思が介在する余地がなく、利用者の意思のみに基づいて機械的に暗号化されたものであることが担保されていると認められる場合であって、さらに付随情報[50]を用いて、暗号化が利用者の意思に基づいた措置であることが明らかになる場合には、署名者は利用者と評価でき、①の要件を満たすと考えられるとした。

2　3条Q&A

リモート署名や立会人署名型の電子署名サービスが、電子署名法第3条に規定する電子署名に該当するかという点については、3条Q&Aにより、該当し得るとの見解が示された。

第3条は、一定の要件を満たす電子署名が行われた電子文書は、真正に成立したものと推定するという規定であり、電子署名の要件として、第2条第1項の①本人性、②非改ざん性（Ⅱ章1節（2）の（ア））のほか、本人だけが行うことができるもの（同（イ））という要件が加重されている。

この趣旨に照らし、3条Q&Aは、第3条の適用には相応の技術水準が要求されるとして、第2条第1項に関する前節の要件に加え、「暗号化等の措置を行うための符号について、他人が容易に同一のものを作成することができないと認められる」場合（Q&Aでは、これを「固有性の要件」と呼ぶ。）には、3条の規定する電子署名に該当するとの見解を示した。そして、これ

---

46 法務省ほか　前掲注(3)

47 「第10回成長戦略ワーキング・グループ議事概要」2020.5.12, pp.29-35. 内閣府ウェブサイト <https://www8.cao.go.jp/kisei-kaikaku/kisei/meeting/wg/seicho/20200512/gijiroku0512.pdf>

48 総務省ほか「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ&A（電子署名法2条1項に関するQ&A）」前掲注(3)

49 総務省ほか「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ&A（電子署名法3条に関するQ&A）」前掲注(3)

50 例えば、二要素認証や利用者のアクセスログ等。

らの要件に適合する電子署名は、立会人署名型であっても第3条の電子署名に該当し得るとされた。

どのようなサービスであれば「固有性の要件」を満たすのかについては、a) 利用者とサービス事業者の間で行われる認証プロセス、b) サービス事業者内部のプロセスに分けた上で、両プロセスが十分な固有性を満たしていることが必要であるとした。a) の例として、二要素認証が導入されていること、b) の例として、リモート署名では、暗号の強度や利用者ごとの個別性を担保する仕組み（例えばシステム処理が当該利用者に紐付いて適切に行われること）等が挙げられている。そのほかにも、各プロセスにおける固有性の水準評価の参考となるガイドライン等[51]が示された。

実際の裁判において第3条の適用が認められるかは、個別の事案に応じて裁判所が判断するが、3条Q&Aにより、リモート署名に加え、立会人署名型であっても第3条の電子署名に該当し得ることが明らかになった。また、裁判所の認定を得るために必要と考えられる技術水準の目安が、各種ガイドライン等を参照する形で示されたことの意義は大きいと言えよう。

3　今後の課題

(1) 身元確認の要否

実際の裁判において、電子署名法第3条の推定効が認められるためには、本人による電子署名であると認められること（Ⅱ章1節 (2) の（ウ））が必要であり、3条Q&AのQ4では、「電子契約サービスの利用者と電子文書の作成名義人の同一性が確認される（いわゆる利用者の身元確認がなされる）ことが重要な要素になると考えられる」としている。したがって、（ウ）の認定に当たり、サービス事業者による利用者の身元確認は必要であるか否かが問題となる[52]。特に、当事者の電子署名を用いない立会人署名型のサービス事業者や利用者にとっては、重要な論点となろう。

オンラインサービスを利用するユーザーの本人確認には、ID・パスワードや生体認証などを用いて、ユーザーが実際にサービスを利用していることを確認する「当人認証」と、公的身分証等を用いて、実際にその行為を行うユーザーが実在する特定の存在であることを確認する「身元確認」がある。オンラインサービスの性質によっては、なりすましや複数のアカウント保有による犯罪等を防止するため、当人認証に加え身元確認も同時に行うことが重要となる[53]。

第3条の推定効を得るために「身元確認」まで必要かについては、識者の間でも見解が分かれている。立法経緯や同法施行規則に照らすと身元確認までは求められていないとの意見[54]や、郵送等の非対面での公的身分証を活用した身元確認が必要との意見[55]、また、政策判断として

---

51 例えば、a) については、Paul A. Grassi et al., “NIST Special Publication 800-63-3: Digital Identity Guidelines,” 2017.6. <https://doi.org/10.6028/NIST.SP.800-63-3>;「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（平成31年2月25日各府省情報化統括責任者（CIO）連絡会議決定）首相官邸ウェブサイト <https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20190225kettei1-1.pdf> 等が、b) については、日本トラストテクノロジー協議会　前掲注(39); Cryptography Research and Evaluation Committees「暗号鍵管理システム設計指針（基本編）第1版」2020.7. <https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3002-1.0.pdf> 等が挙げられている。

52 福岡　前掲注(20), pp.38-39.

53 経済産業省ほか「オンラインサービスにおける身元確認手法の整理に関する検討報告書」2020.3.31, pp.3, 5. <https://www.meti.go.jp/press/2020/04/20200417002/20200417002-3.pdf>

54 福岡　前掲注(20), pp.38-39.

55 「【宮内弁護士監修】立会人型（事業者署名型）の電子契約サービスにおける電子署名法第3条に関する政府見解

身元確認を求めるならば、法的安定性の観点から、行政解釈によるのではなく法改正をすべきとの意見[56]がある。いずれにしても、確立した見解はなく、電子署名を安定的に利用しようとする立場からは、今後の明確化が期待される。

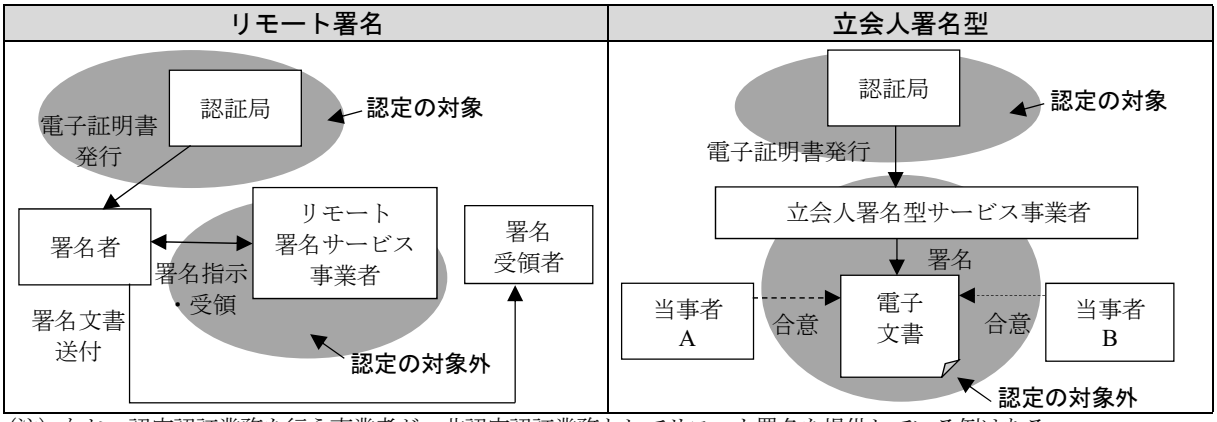
(2) 特定認証業務の認定制度

Ⅱ章3節で述べたとおり、特定認証業務のうち、一定の認定基準を満たしている者は主務大臣の認定を受けることができるが、認定認証業務の数は令和2年10月時点で9業務にとどまっている。

認定認証業務は、認定の基準として、証明書を発行する本人の身元確認と、証明書と鍵を本人に結び付ける作業に関して非常に高いハードルを課している。厳しい認定基準は、電子署名の利用における不正等を防止する効果があるが、利用する者にとっては利便性や迅速性が損なわれるため、結果として利用が増えない事態が生じている[57]。認定認証局から発行された電子証明書は、ここ10年は年間30～35万枚程度で頭打ちとなっており、用途も地方自治体の電子入札等が主で、電子契約用途は少ないとされる[58]。

現行の電子署名法が認定の対象としているのは認証業務であり、リモート署名や立会人署名型の電子署名サービスは認定の対象とはなっていない（図5）[59]。

図５　電子署名法における特定認証業務の認定対象



（注）なお、認定認証業務を行う事業者が、非認定認証業務としてリモート署名を提供している例はある。
（出典）日本トラストテクノロジー協議会「リモート署名ガイドライン」2020.4.30, pp.18-19. 日本ネットワークセキュリティ協会ウェブサイト <https://www.jnsa.org/result/jt2a/data/RemoteSignatureGguide_All-r1.pdf> を基に筆者作成。

について」2020.9.16. GMO 電子印鑑 Agree ウェブサイト <https://www.gmo-agree.com/media/trend/post-116/> なお、電子署名法は、認定認証業務の要件として、公的身分証等を用いた「利用者の真偽の確認」（いわゆる身元確認）を求めており、非対面での確認手段も郵便（又はそれに準じた手段）に限られる。

56 渡部友一郎「電子署名法の再興―20 年前の立法者意思とクラウド技術を活用した電子認証サービスの接合―」『Business Law Journal』13 巻 10 号, 2020.10, pp.45-46.

57 松本泰「社会基盤としての電子認証と電子署名」『日本印刷学会誌』43 巻 5 号, 2006, pp.3-4.

58 「認定認証業務から発行された電子証明書（有効枚数）の推移」電子署名・認証センターウェブサイト <https://esac.jipdec.or.jp/designated-investigative-organization/index.html#hakkou>; 経済産業省「平成 27 年度サイバーセキュリティ経済基盤構築事業（電子署名・認証業務利用促進事業（電子署名及び認証業務に関する調査研究等））調査報告書」（平成 27 年度第 4 回電子署名法研究会 資料 1）2016.3.25, p.11. <https://www.meti.go.jp/committee/kenkyukai/shoujo/denshishomeihou/pdf/h27_004_01_00.pdf>

59 日本トラストテクノロジー協議会　前掲注(39), pp.17-19;「トラストサービス検討ワーキンググループ（第 13 回）議事要旨」（プラットフォームサービスに関する研究会トラストサービス検討ワーキンググループ（第 14 回） 参考資料 14-1）2019.11.8, p.6. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000654837.pdf>

そもそも認定制度は、「認定を受けている認証機関を利用すれば基本的には推定効は受けられる」という利用者の予見可能性のために設けられたとされるが[60]、リモート署名や立会人署名型の電子署名サービスが認定制度の枠外に置かれていることにより、これらのサービスを利用する者に予見可能性の恩恵は届いていない。

2条1項Q&A及び3条Q&Aにより、リモート署名及び立会人署名型電子署名の電子署名法上の位置付けは示されたが、これらのサービスを提供する事業者が、認定制度上どのように位置付けられるのかという論点については、今後検討する必要があろう[61]。

(3) トラストサービスの制度整備

電子署名法の範囲を超えた課題となるが、最後に、トラストサービスについて言及する。トラストサービスとは、オンラインでの人やデータ等の正当性を確認し、なりすましや改ざんを防止するための仕組みであり、電子署名やタイムスタンプもこれに含まれる[62]。日本では、電子署名以外のトラストサービスが法制化されておらず、信頼性を担保する仕組みがないことが課題となっており、令和元年、総務省のワーキンググループによりトラストサービスの制度整備に向けた論点整理が行われた[63]。

論点として取り上げられたのは、日本での法的位置付けが不明確なリモート署名とタイムスタンプ（前述）、eシール等である。eシールとは、電子文書の発信元の組織を示す目的で行われる暗号化等の措置で、社印の電子版のようなものであり、組織名や社名で電子証明をしたい場合に用いられる[64]。

EUでは、先行してこれらのトラストサービスを法制化しており、リモート署名やタイムスタンプも法的位置付けが明確化されている[65]。日本においても、電子取引の安全性や信頼性を確保するため、トラストサービス全般についての制度整備が必要と言えよう[66]。

---

60 渡部　前掲注(56), p.47.

61 同上;「トラストサービス検討ワーキンググループ（第13回）議事要旨」前掲注(59), p.6. 特に、当事者の電子署名であるリモート署名に関し、日本トラストテクノロジー協議会　前掲注(39), p.12では、リモート署名サービスに求められるセキュリティレベルを3つに分け、レベル2を認定認証業務と同等の信頼性を達成できるレベルと定めている。このレベルを満たすリモート署名サービスを、認定認証業務の対象とすることは考えられよう。

62 電子署名とタイムスタンプ以外のトラストサービスには、eシール、eデリバリー、モノの正当性の確認、ウェブサイト認証等があり、これらのサービスに関連する証明書の生成、検証、照合等を行うことが含まれる。

63 プラットフォームサービスに関する研究会トラストサービス検討ワーキンググループ「プラットフォームサービスに関する研究会トラストサービス検討ワーキンググループ中間とりまとめ」2019.8.9, pp.8-9. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000638266.pdf>

64 電子署名法は個人での電子署名を前提としており、電子証明書に所属組織や肩書など（組織属性）を載せている認証局もあるが、現行法ではこれらは認定認証業務の認定対象外となっている（同法施行規則第6条第8号）。したがって、組織属性の記述については法律上の保証がないとされる（宮内編著　前掲注(18), pp.37-38）。

65 eIDAS規則（Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 2014.8.28, pp.73-114. <http://data.europa.eu/eli/reg/2014/910/oj>）。電子署名を含む各トラストサービスの共通規則を定めたものであり、2016年7月に施行された。トラストサービスに法的効果を認めるとともに、一定の要件を満たすトラストサービスの提供者を適格トラストサービスプロバイダーとして規定し、EU各国はそれらをトラストリストとして公開することにより、信頼性を担保する仕組みとなっている。

66 トラストサービスの制度整備については、総務省の「組織が発行するデータの信頼性を確保する制度に関する検討会」（令和2年4月～）やIT総合戦略本部の下に置かれた「データ戦略タスクフォース」（令和2年10月～）等で検討が進められている。

おわりに

デジタル化の進展とともに様々な電子署名サービスが生まれ、電子署名の概念が多義的になる中、20 年前に制定された電子署名法の規定や運用が実態に合致しなくなってきていることは否定し難い。今回関係省庁が、電子署名市場で主流となっているリモート署名や立会人型電子署名に、一定の法的効果が認められる可能性を示したことは、制度と実態の隔たりを埋め、企業の予見可能性を高めることに資するであろう。しかし、これらはあくまで行政解釈であり、具体的な事案について裁判所がどのように解釈するか、今後の動向を注視する必要がある。

電子署名を含むトラストサービスは、電子取引の信頼の基盤となるサービスである。民間取引のデジタル化を進める上で、国内の法制度の更なる整備が期待される。また、米国や欧州では、企業間取引における電子契約や電子署名の利用は一般的になりつつある。国際的な電子取引への対応も視野に入れ、諸外国の制度との連携や相互運用も将来的な課題と言えよう。