

# 電子署名法の解釈問題

——クラウド型署名（本人型リモート署名および  
立会人型署名）に着目して——

高橋宏司

- I. 本稿の目的
- II. 電子署名の種類
- III. 電子署名の普及の阻害要因
- IV. 「電子署名」の定義（2条1項）
  1. 概説
  2. クラウド型署名
- V. 電磁的記録の真正な成立の推定（3条）
  1. 概説
  2. クラウド型署名
- VI. 若干の比較法的検討
  1. UNCITRAL 電子署名モデル法
  2. EU の eIDAS 規則
  3. 小括
- VII. 結語

## I. 本稿の目的

2020年、世界的にコロナウイルス（Covid 19）が蔓延し、感染抑止のため、日本でもテレワークが推奨された。それにもかかわらず、押印のために出社せざるをえない事例が多いという不都合が指摘され、書面や押印の必要性が見直されるとともに、押印の代替策として電子署名が脚光を浴びることになった<sup>1)</sup>。

---

1) 本稿は、同志社大学「新型コロナウイルス感染症に関する緊急研究課題」のテーマの一つである「電子署名の法的問題」の研究成果である。

電子署名は、紙媒体である文書に対しては付与できず、電磁的記録のみがその対象となる。そもそも法が書面の作成を要求していなければ、押印の必要もないが、法が書面の作成を要求しており、それを電磁的記録で代替することを認めていない場合には、電子署名は利用できない。したがって、電子署名の利用を促進するためには、まずは、法が書面を電磁的記録で代替することを認めていなければならない<sup>2)</sup>。しかし、いかなる場合に電磁的記録によることができるかは、本稿のテーマではない。本稿の目的は、法令上、電磁的記録の使用が認められており、電子署名が要求されている場合について、電子署名の要件と効果を「電子署名及び認証業務に関する法律」(以下、「電子署名法」と呼ぶ)に即して検討することにある。

電子署名法は、2条1項に、「電子署名」の定義を置いている。電子署名法以外にも「電子署名」の用語が使われている法令は多いが、その意味するところとして、同項の定義が引用されたり、それと内容を同じくする定義が置かれたりしている。また、電子署名法は、3条に、電磁的記録に記録された情報(以下、「デジタル情報」と呼ぶ)に一定の技術的特性を備えた「電子署名」が行われている場合に、それが本人によるものであることを要件として、民事訴訟において、当該電磁的記録が真正に成立したことを推定する規定を置いている。

電子署名法の解釈問題を検討するに当たり、本稿が特に着目するのは、近年利用が広がっているクラウド型署名と呼ばれる類の電子署名であり、その関係で発出された「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」という文書である。これは、同法を共管する総務省、法務省、経済産業省の三省により、令和2年7月17日および令和2年9月4日の二回に分けて発出された文書で、前者<sup>3)</sup>は電子署名法2条に関係し(以下、「第2条関係Q & A」と呼ぶ)、後者<sup>4)</sup>

2) 例えば、会社法369条4項は、取締役会の議事録を電磁的記録によって作成することを認めている。

3) [https://www.meti.go.jp/covid-19/pdf/denshishomei\\_qa.pdf](https://www.meti.go.jp/covid-19/pdf/denshishomei_qa.pdf)

4) [https://www.meti.go.jp/covid-19/pdf/denshishomei3\\_qa.pdf](https://www.meti.go.jp/covid-19/pdf/denshishomei3_qa.pdf)

は同法3条に係る（以下、「第3条関係Q & A」と呼ぶ）。

## II. 電子署名の種類

電子署名は、デジタル情報に対する作成名義人の何らかの了承を示すための措置であり、広義では、電磁的記録への名前の付記や署名画像の添付のほか、チェックボックスへの✓印の入力も含む概念である。他方、電子署名には、デジタル情報を暗号化し、その改竄の検出が可能なものもあり、その代表格である公開鍵暗号方式と呼ばれる方式では、暗号化されたデジタル情報は、暗号化に使われた整数（署名鍵）と対を成す整数（検証鍵）によるのみ復号できる。署名鍵は、署名者が他人に知られないように管理すべきものであるため「秘密鍵」と呼ばれ、検証鍵は、一般に公開して差し支えないものなので「公開鍵」と呼ばれることが多い。検証鍵を使って復号することで、当該デジタル情報の暗号化は当該検証鍵と対になっている署名鍵によってなされたことを確認できるが、その署名鍵の管理者の身元は、信頼できる第三者の発行する電子証明書に基づいて判断するほかない。

公開鍵暗号方式の電子署名には、いわゆるローカル（オンプレミス）型署名とクラウド型署名がある。ローカル型署名は、署名者が自身で管理する端末で行う電子署名である。これに対して、クラウド型署名は、電子署名サービス提供事業者が署名鍵を保管し、遠隔からログインした利用者の指示に従い、事業者のサーバ上で行う電子署名である。コンピューティング全般の歴史の中でクラウドの歴史は比較的浅く、クラウド型電子署名サービスは、2000年代に入ってから登場した<sup>5)</sup>。

クラウド型署名は、本人型リモート署名（remote signature）と立会人型署名（事業者型署名とも呼ばれる）に分類できる。本人型リモート署名は、サービス提供事業者のサーバに利用者の署名鍵を設置し、利用者の指示に基

---

5) 後掲注36) に対応する本文参照。

づき、事業者が利用者の署名鍵で行う電子署名である。これに対して、立会人型署名は、サービス提供事業者が自身のサーバに自身の署名鍵を設置し、利用者の指示に基づき、事業者自身の署名鍵で行う電子署名である。立会人型署名は、サービス提供事業者の視点に立てば、自らの署名を自らの端末で行う署名であるから、ローカル型署名であるとも言いうるが、利用者の指示に基づき行われるものであるから、本稿では、利用者視点に立ち、クラウド型署名の一類型として扱う。

立会人型署名は、利用者の名称を象った印影等の画像データを署名に係る電磁的記録に付して、あたかも利用者の署名がなされているかのような外観を作出するものが多いように見受けられるが、署名データには、当該電磁的記録の暗号化がサービス提供事業者の署名鍵によってなされたことが示される。前記「第2条関係 Q & A」および「第3条関係 Q & A」は、「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」と題されているように、立会人型署名を対象としている。

立会人型署名の対象は、法的に見れば、利用者の作成に係るデジタル情報ではなく、当該デジタル情報に利用者が何らかの了承を与えたことをサービス提供事業者が証人として確認した旨の報告証書である。したがって、電子契約サービスの場合、契約書という処分証書ではなく、契約当事者双方の意思確認を行った旨の報告証書に対して、サービス提供事業者が証人として、自らの名義で電子署名していることになる。報告証書は、利用者の作成に係るデジタル情報に署名データとして埋め込まれると目立たないが、立会人型署名により、当該デジタル情報が署名時点において存在していたことが証明され、改竄の検出が可能となる。

クラウド型署名サービスに利用者がログインする際に求められる身元確認の方法とその確実度は、サービスによって様々である。特に立会人型署名のサービスは、メールアドレスの確認のみで済みますなど、利用の手軽さを謳うものが多い。

### Ⅲ. 電子署名の普及の阻害要因

電子署名の普及は、遅々として進んで来なかった。電子署名法が成立した平成12年（西暦2000年）頃に想定されていた電子署名は、ローカル型署名であった。ところが、これを安全に行うためには、署名鍵が格納されたICカード等を安全に保管しておき、署名作業の都度、それを取り出してきて、カードリーダーライター等で読み取るなどの面倒な作業が必要となる。さらに、身元確認を経た電子署名を行うならば、認証サービス提供事業者等に依頼し、認証プロセスを経て、電子証明書の発行を受ける必要があり、しかも電子証明書の有効期間は限られている。署名の対象が契約である場合には、相手方当事者にも同様の手間と費用の負担を求めなければならず、契約締結機会そのものを失うことにつながりかねない<sup>6)</sup>。

このような阻害要因を回避するものとして、近年クラウド型署名が広まり始めた。この署名は、署名サービス提供事業者のサーバ上でなされるので、利用者は、ICカード等の保管や、カードリーダーライター等の使用といった手間から解放される。また、場所の制約を受けずにマルチデバイスで利用できることから、テレワークにも使いやすい。クラウド型署名の中でも立会人型署名ならば、利用者は、自らの署名鍵を事業者に預ける必要すらない。ところが、クラウド型署名は、電子署名法上の要件を満たすかなどの法的位置付けが不明確であったため、それが普及の阻害要因となってきた。

### Ⅳ. 「電子署名」の定義（2条1項）

電子署名法2条1項は、次のように「電子署名」を定義する。

---

6) 櫻庭信之『リーガルテック活用の最前線』152頁（ぎょうせい、2020）。

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

- 一 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。
- 二 当該情報について変更が行われていないかどうかを確認することができるものであること。

本章（第四章）では、まず本項を概説し、次にクラウド型署名が本項の定義を備え得るかを検討する。

## 1. 概説

電子署名法2条1項の重要性は、その定義する「電子署名」が、電磁的記録の真正な成立の推定効を規定する同法3条の要件を構成している点にあるだけでなく、「電子署名」の用語が使われているその他の多くの法令<sup>7)</sup>において、その意味するところとして本項の定義が引用されたり<sup>8)</sup>、それと同一内容の定義が置かれたりしている<sup>9)</sup>点にもある。例えば、会社法369条4項は、取締役会の議事録を電磁的記録によって作成することを認め、その場合には、法務省令で定める署名又は記名押印に代わる措置をとらなければならないと規定する。これを受けて、会社法施行規則225条は、当該代替措置は、「電子署名」とすると規定し（1項）、その定義を置いている（2項）が、その定

---

7) 総務省のe-Gov法令検索で「電子署名」の用語が含まれている法令を検索すると、190件の法令が表示される（2021年3月現在）。

8) 「法務省の所管する法令の規定に基づく情報通信技術を活用した行政の推進等に関する規則」2条1項1号などの例がある。

9) 会社法施行規則225条2項などの例がある。また、商業登記法12条の2第1項1号の規定する「措置」は、「電子署名」という用語は当てられていないが、その内容は同じである。

義内容は、電子署名法2条1項の定義と同じである。

2条1項の「電子署名」の定義は、次に見るとおり、極めて緩やかである。電子署名法の立法担当者も、「いわゆる『署名』目的で、何らかの形で暗号化等されているものについては、全て含まれることになると考えられる」と述べていた<sup>10)</sup>。

まず、本項1号は、署名対象のデジタル情報が当該措置（電子署名）を行った者の作成に係るものであることを示すためのものであることを「電子署名」の要件としている。この要件から外れるのは、情報内容を秘匿する目的で暗号技術を利用している場合など、非常に限定的な場合である<sup>11)</sup>。また、本号は、「示すためのもの」と規定しているように、単に署名の目的を要件化しているにすぎず、実際に「当該情報が当該措置を行った者の作成に係るものであること」は、本号の要件ではない。「電子署名」を要求する各個の法令において、署名者の身元確認が必要とされる場合には、電子証明書が別途要求されており、その種類も、求められる認証の確実度に応じて特定されている<sup>12)</sup>。

次に、本項2号は、署名対象のデジタル情報について、変更が行われていないかどうかを確認することができるものであること（改竄検出可能性）を「電子署名」の要件としている。改竄検出可能性は、文書の場合には、変更の痕跡を残す紙媒体としての性質に依存しており、契印を除いて、押印には不完全にしか認められない。したがって、本項は、「電子署名」に、押印との機能的等価性を要求しているのではなく、むしろ押印よりも強固な機能を要求していると言えよう。デジタル情報への名前の付記や署名画像の添付は、

---

10) 酒井秀夫「電子署名及び認証業務に関する法律について」ジュリ1183号（2000）38頁。

11) 酒井・前掲注10）37頁。

12) 商業登記規則102条3項ないし5項などの例がある。例えば、代表取締役の選任を証する取締役会議事録を電磁的記録により作成し、商業登記申請の際にそれを添付する場合には、変更前の代表取締役が商業登記電子証明書、公的個人認証サービス電子証明書、または特定認証業務電子証明書を送信すれば、他の取締役は、同条4項2号所定の「法務大臣の定める」電子証明書（具体的には、法務省の商業・法人登記のオンライン申請についてのホームページ <http://www.moj.go.jp/MINJI/minji60.html> に記載されているもの）を送信すれば足りる。

改竄検出可能性がないため、本項で定義されている「電子署名」に当たらない。本項は技術中立的な表現をとっているが、本号の要件に照らし、本項の「電子署名」に該当する電子署名としては、一般に、公開鍵暗号方式のものが想定されている。ただし、本号は、改竄の検出可能性を要求するのみであり、改竄に対する耐性を要求するものではない<sup>13)</sup>。

## 2. クラウド型署名

では、クラウド型署名は、本項の定義する「電子署名」に該当し得るであろうか。本項の定義は、本文の要件、1号要件、および2号要件からなるが、デジタル情報について行われる措置であるという本文の要件をクラウド型署名が満たすことには疑問の余地がない。また、公開鍵暗号方式の電子署名を用いているクラウド型署名は、2号要件も充足する。そこで、以下では、1号要件の充足可能性について、まず私見を述べ、次に前記「第2条関係Q & A」に示された見解を検討する。

### (1) 私見

本項1号によると、「電子署名」は、署名対象のデジタル情報が当該措置（電子署名）を行った者の作成に係るものであることを示すためのものでなければならない。クラウド型署名の目的は、それが本人型リモート署名であろうと、立会人型署名であろうと、署名対象のデジタル情報が同署名サービスの利用者の作成に係るものであることを示すことにある。当該措置を行った者は、直接的、物理的には署名サービス提供事業者である。しかし、それが利用者の意思に基づいて行われているときには、利用者が当該措置を行った者であると評価することが可能である。そして、電子署名法の技術中立的な表現や、「電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進」を図る（1条）という同法の目的に照らせば、クラウド

---

13) 酒井・前掲注10) 38頁。第V章で見ると、電子署名の暗号が十分な強度を備えていることは、電子署名法3条括弧書の要件となっている。



型署名の場合には、そのように評価することが妥当であろう。したがって、クラウド型署名は、それが本人型リモート署名であろうと、立会人型署名であろうと、1号要件も充足し得ると考えるべきである。

## (2) 「第2条関係 Q & A」

法務省は、従来、立会人型署名は、1号要件を具備しないとの見解を取っていたと見受けられる。これは、会社法施行規則225条1項6号の「電子署名」について同省が示した解釈から垣間見ることができる。第I章に述べたとおり、取締役会の議事録を電磁的記録によって作成する場合には、出席した取締役又は監査役が「電子署名」しなければならない（会社法369条4項、会社法施行規則225条1項6号）、この「電子署名」の定義は、電子署名法2条1項のそれと同じ内容となっている（会社法施行規則225条2項）。法務省は、内閣府規制改革推進会議成長戦略ワーキング・グループの第11回会合（令和2年5月22日開催）に提出した「論点に対する回答」（資料1-3）において、「出席した取締役又は監査役が『電子契約事業者が利用者の指示を受けて電子署名を行うサービス』を利用して電磁的記録をもって作成された取締役会の議事録に電子署名をしても、当該電子署名は取締役等の電子署名ではない」という理由を付して、立会人型署名は、「電子署名」としては認められないとの見解を示した。しかし、この解釈は同会合において批判を受け<sup>14)</sup>、その約一週間後の同月29日に、法務省は、各経済団体に対して、上記見解を変更する次の見解を伝えた（角括弧内は本稿の筆者による<sup>15)</sup>）。

いわゆるリモート署名やサービス提供事業者が利用者の指示を受けて電子署名を行うサービスであっても、取締役会に出席した取締役又は監査

14) 同会合議事概要（<https://www8.cao.go.jp/kisei-kaikaku/kisei/meeting/wg/seicho/20200522/gijiroku0522.pdf>）参照。

15) 事務局からのお知らせ「取締役会議事録に施す電子署名についての法務省見解」（2020年6月2日）新経済連盟 HP（<https://jane.or.jp/proposal/notice/10829.html>）。

役が「取締役会の議事録の内容が正確であり、異議がないと判断」したことを示すものとして、当該取締役会の議事録について、その意思に基づいて当該措置がとられていれば、署名又は記名押印に代わる措置としての電子署名として有効なものであると考えられます。

それから約2か月後の7月17日に、電子署名法2条1項の「電子署名」の定義について、総務省、法務省、経済産業省の三省は共同で、「第2条関係Q & A」を發出し、1号要件の意味につき次のような解釈を示した。これは、上記の新見解に整合的である。

「当該措置を行った者」に該当するためには、必ずしも物理的に当該措置を自ら行うことが必要となるわけではなく、例えば、物理的にはAが当該措置を行った場合であっても、Bの意思のみに基づき、Aの意思が介在することなく当該措置が行われたものと認められる場合であれば、「当該措置を行った者」はBであると評価することができるものと考えられる。

「第2条関係Q & A」は、この解釈を立会人型署名に対して次のように適用し、1号要件の充足可能性を認めた<sup>16)</sup>（下線は、本稿の筆者による）。

例えば、サービス提供事業者に対して電子文書の送信を行った利用者やその日時等の情報を付随情報として確認することができるものになっているなど、当該電子文書に付された当該情報を含めての全体を1つの措置と捉え直すことによって、電子文書について行われた当該措置が利用者の意思に基づいていることが明らかになる場合には、これらを全体とし

---

16) この見解は、一般に好意的に受け止められている。福岡真之介「電子署名法3条の推定効についての一考察」NBL1179号37頁（2020）、渡部友一郎「電子署名法の再興」Business Law Journal 13巻10号42頁（2020）など参照。

て1つの措置と捉え直すことにより、「当該措置を行った者（＝当該利用者）の作成に係るものであることを示すためのものであること」という要件（電子署名法第2条第1項第1号）を満たすことになるものと考えられる。

下線部は、誤って挿入されたものと思われる。助詞が一つ欠落している上、「付随情報」が「措置」という言葉に含まれるというのは、文法的に意味をなさない<sup>17)</sup>。下線部を省いて読むと、付随情報の確認を可能とする仕組みが「全体として」の「一つの措置」を構成する要素として位置付けられ、意味が通る。

「第2条関係Q & A」は、クラウド型署名の中でも、「サービス提供事業者自身の署名鍵により暗号化を行う」サービス、すなわち立会人型署名に関するものである。しかし、そこに示された上記解釈は本人型リモート署名にも妥当するものであり、「第2条関係Q & A」は、1号要件の充足可能性の点で本人型リモート署名を立会人型署名と区別する趣旨ではないであろう。以上により、「第2条関係Q & A」は、私見に沿うものであると見ることができる。

## V. 電磁的記録の真正な成立の推定（3条）

電子署名法は、3条に、電磁的記録の真正な成立を推定する規定を置いている。同条は、以下のように規定する。

電磁的記録であつ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

---

17) にもかかわらず、その後に発出された「第3条関係Q & A」には、「第2条関係Q & A」を紹介する部分で、「付随情報を含めて全体を1つの措置と捉え直す」という表現が再度用いられている（4頁）。

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。

本章（第V章）では、まず本条を概説し、次にクラウド型署名が本条の要件を備え得るかを検討する。

## 1. 概 説

### (1) 民事訴訟法228条4項の特則としての位置付け

民事訴訟法228条1項は、証拠として提出される「文書は、その成立が真正であることを証明しなければならない」と規定し、同条4項は、「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立したものと推定する」と規定する。これらの規定を含む「第五節 書証」の規定は、同法231条によって、「情報を表すために作成された物件で文書でないものについて準用」されている。したがって、電磁的記録が証拠として提出された場合にも、その成立が真正であることを証明しなければならないが、真正な成立の推定規定（228条4項）は、「署名又は押印」が電磁的記録に対しては物理的に行えないため、単純に準用できない。そこで、同項の特則として適用されるのが電子署名法3条である。

本条は、デジタル情報に「電子署名」が行われている場合に、当該電磁的記録の真正な成立を推定する要件として、当該「電子署名」が一定の技術的特性を備えていること（括弧書）および「本人による」ものであること（本文）を定めている。本条の「電子署名」の意義は、2条1項が本法における「電子署名」とは何かを定義しているので、それに従う。そこで、以下では、括弧書の要件と本文の要件を順に検討する。

### (2) 電子署名の技術的特性（括弧書）

3条括弧書は、「電子署名」に限定を付し、それが一定の条件下で一定の

技術的特性を有することを要件としている。すなわち、当該電子署名を「行うために必要な符号及び物件を適正に管理する」という条件下においては、「本人だけが行うことができることとなるもの」であるという技術的特性である。

「電子署名」として通常想定されている公開鍵暗号方式の電子署名は、十分な暗号強度があるものならば、これを行うために必要な署名鍵（符号）およびそれが格納されたICカード等（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であるから、この要件を充足する。反対に、暗号の強度が不十分であって、容易に検証鍵を解読して署名鍵を割り出すことができる電子署名は、この要件を備えないことになる。

文書の真正な成立の推定を本人の押印によって認める民事訴訟法228条4項には、電子署名法3条括弧書の要件に対応する要件は規定されていない。この要件をあえて押印に引き直して表現すると、「印章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」押印に限るとなる。同一の印影を顕出する印章が複数あり得るし、3Dプリンターの登場によって印章の模倣が容易になったことに鑑みれば、押印は、認印であれ、実印であれ、このような技術的特性を備えているとは言い難いのではないだろうか。

3条括弧書では、電子署名が「本人だけが行うことができることとなる」という部分が要件であり、署名を「行うために必要な符号及び物件を適正に管理すること」は、要件部分の命題の条件として記述されているにすぎない。したがって、問題となっている事案において、本人が署名鍵を厳重に保管していたこと、他人と共用していなかったこと、他人に盗まれていないこと等は、括弧書の要件ではない。問題となっている事案において、電子署名を「行うために必要な符号及び物件を適正に管理すること」が実際になされていたかは、本文の要件である電子署名が「本人による」ものであることを推認させる事実であり<sup>18)</sup>、次に検討するように、この点について経験則が認められ

---

18) 平成28年度第4回電子署名法研究会（平成29年3月14日開催）議事要旨（[https://www.meti.go.jp/committee/kenkyukai/shoujo/denshishomeihou/pdf/h28\\_04\\_giji.pdf](https://www.meti.go.jp/committee/kenkyukai/shoujo/denshishomeihou/pdf/h28_04_giji.pdf)）1頁も同旨。

るかが問題となる。

### (3) 電子署名が「本人による」ものであること（本文）

3条の本文は、電子署名が「本人による」ものであることを要件としており、これは、電子署名が本人の意思に基づいて成立していることを意味する。この点の証明は、困難が大きい。本人が電子署名している場面が動画撮影等されていることは通常ないし、その場面に立ち会った者がいてその者から証言が得られることも多くはないからである。

前記民事訴訟法228条4項の要件である本人等の押印は、押印が本人等の意思に基づいて成立していることを意味する<sup>19)</sup>が、この点の証明にも同様の困難がある。そこで、この困難を軽減する判例法理が形成されており、その基礎となっている最高裁の判旨は、「文書中の印影が本人・・・の印章によって顕出された事実が確定された場合には、反証がない限り、該印影は本人・・・の意思に基づいて成立したものと推定するのが相当」であると判示した<sup>20)</sup>。この判例法理による推定に加えて、民事訴訟法228条4項による推定が認められるため、合わせて「二段の推定の法理」と呼ばれている。第一段目の推定は、「文書中の印影が本人・・・の印章によって顕出された事実」を要証事実とし、印章は、通常、むやみに他人に使わず、適正に管理されているものであるという経験則が基礎となって認められていると考えられる。この経験則は、特に認印については、その妥当性に疑問を挟む余地があるが、第一段目の推定が事実上の推定に過ぎず<sup>21)</sup>、反証を許すものであるから、強固なものでなくともよい。「文書中の印影が本人・・・の印章によって顕出された事実」の証明に当たっては、印章の管理者と本人、すなわち作成名義人（それを作成したと挙証者によって主張されている者）が一致することの証明も必要となる。この点については、印章が実印である場合には、

19) 伊藤眞『民事訴訟法』（有斐閣、第7版、2020）433頁。

20) 最判昭和39年5月12日民集18巻4号597頁。

21) 伊藤・前掲注19) 434頁。

印鑑証明書を得ることにより、証明の負担が緩和される。

電子署名については、第一段目の推定を認める判例法理は存在しない。もし、公開鍵暗号方式の電子署名に押印と同様の推定を認めるとすれば、それは、当該電子署名が本人の署名鍵によって作成されたことを要証事実とし、電子署名を行うのに必要な署名鍵は、通常、むやみに他人に開示せず、適正に管理されているものであるという経験則を基礎として認められるべきものである。では、そのような経験則は認められるであろうか。経験則は、立法時に存在していなくとも、技術的、社会的基盤が進めば醸成される可能性がある。確かに、署名鍵と検証鍵のペアの作成は、そのための演算プログラムを利用すれば、誰でも容易にできてしまうわけであり、署名鍵が常に適正に管理されているとは言えない。しかし、この経験則は、印章の場合と同様、反証を許すものであるから、強固なものである必要はない。公開鍵暗号方式の電子署名を行うのに必要な署名鍵は、ICカード等の耐性ある物件に格納されて安全に保管されていることが多く、通常、適正に管理されているものであるという経験則を認めることができるのではないだろうか<sup>22)</sup>。

公開鍵暗号方式の電子署名について上記の経験則が認められるならば、「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」という3条括弧書の条件部分が成就するので、暗号強度が十分であれば、当該電子署名は、「本人だけが行うことができることとなる」(括弧書)。したがって、第一段目の推定を認める判例法理が存在しなくとも、上記の経験則が認められるならば、括弧書を通じて、「本人による」という本文の要件充足性の証明が容易になる。そもそも、民事訴訟法228条4項と対比すれば、電磁的記録の真正な成立を推定する要件としては、本来は、「電子署名」が「本人による」ものであるという電子署名法3条本文の要件で十分なはずであり、「電子署名」を所定の条件下で「本人だけが行うことができることとなるもの」に限

---

22) 事実上の推定を認めるのに前向きな見解として、辛島陸・飯田耕一郎・小林善和『Q & A 電子署名法解説』77頁(三省堂、2001)、高野真人・藤原宏高『電子署名と認証制度』54頁(第一法規出版、2001)など参照。

定する括弧書の要件は、一見すると蛇足であるかに思われる。しかし、括弧書は、「本人による」という本文の要件充足性の証明の道筋を示しており、上記の経験則が認められるならば、証明の負担が軽減されることになる。

なお、括弧書の要件は、技術的特性により「電子署名」を限定するものであるから、それを満たせば、技術的に、符号及び物件の管理者しか署名できないことは担保されるが、その管理者が本人、すなわち電磁的記録の作成名義人であることまでは担保され得ない。言い換えれば、「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」は、「本人だけが行うことができることとなる」ための必要条件ではあるが、十分条件ではない。当該電子署名を行うために必要な符号及び物件を管理していた者が作成名義人と一致することの証明は、別途、「本人による」という本文の要件の中で行われなければならない。この証明の負担は、当該電子署名に紐付いた電子証明書が存在する場合には、その作成の際に行われた身元確認の確実度に応じて軽減されるであろう<sup>23)</sup>。

## 2. クラウド型署名

では、クラウド型署名は、本条の要件を備え得るであろうか。クラウド型署名が2条1項の定義する「電子署名」に該当し得ることは、前章において検討した。3条の「電子署名」の意義は、同項の定義に従っている。そこで、以下では、3条の残りの要件を検討する。すなわち、当該電子署名が所定の条件下において「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（括弧書）、そして、それが本人によってなされること（本文）である。まず立会人型署名、次に本人型リモート署名の順に検討する。

### (1) 立会人型署名

前記「第3条関係 Q & A」は、立会人型署名が利用された場合につき、

---

23) 酒井・前掲注10) 38頁および高野・藤原・前掲注(22) 55頁も同旨。



3条の要件が充足されるかを検討している。そこで、まず同Q & Aに示された見解を紹介し、次に私見を述べる。

### 1) 「第3条関係Q & A」

「第3条関係Q & A」は、括弧書の条件部分である「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」につき、その具体的内容は個別のサービス内容により異なり得るとしつつ、例えば、サービス提供事業者の署名鍵及び利用者のパスワード（符号）並びにサーバ及び利用者の手元にある2要素認証用のスマートフォン又はトークン（物件）等を適正に管理することがこれに該当するとの解釈を示した。

かかる条件下において「本人だけが行うことができることとなるもの」であるという括弧書の要件については、「第3条関係Q & A」は、立会人型署名サービスであっても、①利用者とサービス提供事業者の間で行われるプロセスおよび②サービス提供事業者内部で行われるプロセスのいずれにおいても十分な水準の固有性が満たされていると認められる場合には備わっているという解釈を示した。「固有性」という表現は、電子署名法上の用語ではないが、「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こと」（「第3条関係Q & A」3頁）という意味で使われている。そして、①のプロセスについては、例えば、利用者が二要素による認証を受けなければ措置を行うことができない仕組みが備わっているような場合には、十分な水準の固有性が満たされていると認められ得るとした。また、②のプロセスにおける固有性の水準については、サービス提供事業者が自身の署名鍵により暗号化等を行う措置について、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）等に照らして評価できるとした。

このように、「第3条関係Q & A」は、立会人署名であっても、その仕組み次第では、3条に規定する電子署名に該当し得るという見解を示した。そのため、立会人型署名によっても電磁的記録の真正な成立の推定効が認めら

れ得ることにつき、行政のお墨付きが得られたとの受け止め方が強いように見受けられる<sup>24)</sup>。しかし、同条は、電子署名が「本人による」ものである（本文）も要件としていることを忘れてはならない。「第3条関係Q & A」も、「同条に規定する電子署名が本人すなわち電子文書の作成名義人の意思に基づき行われたと認められる場合に」電磁的記録の真正な成立が推定されると述べて、この点を確認する。そして、そのためには、「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」と指摘し、「電子契約サービスにおける利用者の身元確認の有無、水準及び方法やなりすまし等の防御レベルは様々であることから、各サービスの利用に当たっては、・・・適切なサービスを慎重に選択することが適当と考えられる」と締め括っている。ここで注意すべきは、前記①のプロセスにおける十分な水準の固有性が認められる電子署名であっても、それが「本人による」ものであるという本文の要件が充足されることには、必ずしもならないということである。というのは、①のプロセスにおける十分な水準の固有性の要件は、署名要求者について、二要素認証等によって、サービス提供事業者の把握している利用者の属性情報と一致していることを確認するものにすぎず、利用者が作成名義人と一致していることを意味するものではないからである。立会人型署名サービスは、利用者の身元確認をメールアドレスだけで行うなどの手軽さにより普及してきたが<sup>25)</sup>、利用者と作成名義人の同一性の証明がなされないかぎり、「第3条関係Q & A」の見解に立っても、本条の推定効は認められないことに注意が必要であろう。

---

24) 「電子署名、法的な懸念解消」日本経済新聞朝刊2020年9月21日11頁は、「第3条Q & A」の公表を受けて、利用者に二要素認証を提供するなどの動きがサービス提供事業者にあることを伝えている。

25) 「電子契約 トラブル防ぐには」日経産業新聞2020年6月29日6頁。

## 2) 私見

「第3条関係 Q & A」は、前記したとおり、立会人署名であっても、その仕組み次第では、3条に規定する電子署名に該当し得るという見解を示した。私見は、これに反対であり、「第3条関係 Q & A」に示されたこの点に関する行政解釈は、司法解釈では採用されるべきでないと考える。と言うのは、そもそも本条は、本人すなわち作成名義人の署名を基礎として、電磁的記録の真正な成立を推定していると見るべきであり、したがって、立会人型署名は、括弧書の「本人だけが行うことができることとなるもの」に当たらないと解すべきだからである。

法務省も、従来は、私見と同じ立場であったと見受けられる。内閣府規制改革推進会議成長戦略ワーキング・グループ第10回（令和2年5月12日開催）では、同省の民事局商事課長より、「電子契約サービス提供事業者が利用者の指示を受けて自ら電子署名を行うサービスにつきましてですけれども、立法の経緯からいたしまして、本人というところが非常に重要な要素でございます。本人が電子署名をしたということが判明しない仕組みにつきましては、既存の電子署名法3条の規定の効力を及ぼすというのはなかなか難しいのではなかろうかと認識しております」との発言がなされていた<sup>26)</sup>。しかし、その約2か月後の7月17日に閣議決定された「規制改革実施計画」では、「総務省、法務省及び経済産業省は、電子署名に対し、民事訴訟において署名・押印同様の推定効を定める電子署名法第3条の在り方に関して、サービス提供事業者が利用者の指示を受けて電子署名を行うサービスなどについても一定の要件を満たせば対象となり得ることにに関して、その考え方を明らかにする」ことが要請された<sup>27)</sup>。この要請は、「書面規制、押印、対面規制の見直し」の一環としてなされたものであり、立会人型署名サービスが電子署名法3条

26) 同会議事概要18頁（<https://www8.cao.go.jp/kisei-kaikaku/kisei/meeting/wg/seicho/20200512/gijiroku0512.pdf>）。

27) 「規制改革実施計画」10頁（<https://www8.cao.go.jp/kisei-kaikaku/kisei/publication/keikaku/200717/keikaku.pdf>）。

の対象になり得るという結論は謂わば既定路線となっており、その理論構成の検討が求められたものと見受けられる。そして、その約2か月後の9月4日に発出されたものが「第3条関係Q & A」である。

ところで、「第3条関係Q & A」は、「電子契約において電子署名を行う際にサービス提供事業者が自動的・機械的に利用者名義の一時的な電子証明書を発行し、それに紐付く署名鍵により暗号化等を行う電子契約サービス」も「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」に含めて議論している（同Q & Aの脚注1）。確かに、そのようなサービスを立会人型署名サービスに分類するならば、その限りで、立会人型署名サービスが電子署名法3条の対象になり得るという結論は妥当であろう。しかし、電子証明書の発行が自動的・機械的かは身元確認の確実性に関する問題にすぎないので、そのようなサービスは、本来、本人型リモート署名サービスに分類して議論すべきではないかと思われる。

立会人型署名は3条に規定する電子署名に該当しないという私見の解釈をとると、同条を通じて立会人型署名の普及を後押しすることはできず、「規制改革実施計画」の意図した「書面規制、押印、対面規制の見直し」が進まないとの批判があるかもしれない。しかし、立会人署名も、その仕組み次第では、3条に規定する電子署名に該当し得るという「第3条関係Q & A」の見解を取っても、署名が「本人による」ものであるという本文の要件がハードルとして残っていることは、前述したとおりである。また、電磁的記録の真正な成立は、電子署名法3条の推定を通じてしか認められないわけではなく、当該記録の成立経緯を裏付ける資料など個々の事情の立証がなされれば、証拠全般に照らし、裁判所の自由心証により判断される。クラウド型署名サービスは、メールアドレス、IDおよびパスワード、IPアドレス、タイムスタンプ等を幾重にも用いて、いつ、誰が、どこで、どの電子機器からアクセスしたか等の証跡を取ることができる仕組みである。したがって、本条による推定効が立会人署名によっては働かないと解しても、電磁的記録の真正な成立を証明する道が閉ざされるわけではない。また、そもそも真正な成

立を証明する必要が生ずるのは、紛争が裁判になり、提出された電磁的記録について、相手方当事者が真正な成立を否認したか、不知であるとの主張をした場合に限られるのであるから、電子契約の保存等の様々な付随サービスを提供することで、立会人型署名サービスの需要を喚起することは可能であろう。

## (2) 本人型リモート署名

前記「第3条関係 Q & A」は、立会人型署名につき検討しているが、本人型リモート署名に妥当しうる解釈も含まれている。

まず、括弧書の条件部分である「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」については、「第3条関係 Q & A」の示した解釈と同様に、「符号」や「物件」には、サービス提供事業者の管理するものも含まれると解することができる。ただし、本人型リモート署名の場合、立会人型署名と異なり、サービス提供事業者が保管しているのは利用者の署名鍵である。したがって、事業者の管理する利用者の署名鍵および利用者が自身で管理するパスワードが「符号」に当たり、事業者のサーバおよび利用者の手元にある二要素認証用のスマートフォンやトークンが「物件」に当たると解することになる。

次に、かかる条件下において「本人だけが行うことができることとなるもの」であるという括弧書の要件について、「第3条関係 Q & A」は、①利用者とサービス提供事業者の間で行われるプロセスおよび②サービス提供事業者内部で行われるプロセスのいずれにおいても十分な水準の固有性が満たされていると認められる場合には備わっているという解釈を示した。私見では、前述したとおり、立会人型署名は「本人だけが行うことができることとなるもの」に当たらないと解するが、本人型リモート署名は、本人、すなわち署名サービス利用者の署名鍵を使って行われるので、①および②のプロセスのいずれにおいても十分な水準の固有性が満たされていると認められる場合には、括弧書の要件を備えると考ええる。

最後に、電子署名が「本人による」ものであるという要件（本文）については、本章第1節で見たように、仮に、当該電子署名を行うために必要な符号および物件は、通常、適正に管理されているという経験則が認められるならば、括弧書を通じて、証明の負担が軽減されることになる。しかし、リモート署名の場合、「符号」や「物件」には、サービス提供事業者の管理するものも含まれ、そのサービスの仕組みや利用のされ方は様々であるから、そのような経験則は認められないであろう。したがって、「本人による」という本文の要件については、事案に即して、本人、すなわちリモート署名サービス利用者の意思に基づいていることの証明が必要である。

## VI. 若干の比較法的検討

「第3条関係 Q & A」は、その作成に当たって、「国際標準との整合性等の観点も踏まえ、検討を行った」と述べているが、具体的にどのような検討がなされたのかは明らかでない。そこで、本稿では、以下に、国連と EU の場での立法について若干の検討を行う。

### 1. UNCITRAL 電子署名モデル法

電子署名モデル法 (Model Law on Electronic Signatures) は、2001年に国連国際商取引法委員会 (UNCITRAL) によって作成された。執筆時 (2021年3月) 現在、これまでに35か国が同法に基づくか、同法に影響を受けた国内立法を行ったとされる<sup>28)</sup>。

同法6条1項は、「法が人の署名を要件とする場合、データメッセージとの関係では、関係する合意を含むすべての事情を勘案し、当該メッセージが作成または通信された目的に照らして適当な信頼可能性を有する電子署名が使用されているときは、当該要件は満たされるものとする」と規定する。そ

---

28) [https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic\\_signatures/status](https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures/status) 参照。

して、同条3項は、電子署名が信頼可能性を有すると認められるための要件を列挙し、その一つとして、「署名作成データが署名時に署名者の管理下にあり、他の者の管理下になかった」ことを挙げる（同項b号）<sup>29)</sup>。UNCITRAL事務局の作成した「モデル法立法ガイド」によると、署名作成データとは、公開鍵暗号方式の電子署名では署名鍵を指すとされている<sup>30)</sup>。

では、本人型リモート署名サービスを利用する場合でも、サービス利用者を署名者として見て、「署名作成データが署名者の管理下にあり、他の者の管理下になかった」と言えるのであろうか。この点についての論稿は、管見の及ぶ限りは見つからないが、「モデル法立法ガイド」は、この要件に関し、署名作成データが複数人の利用が可能なネットワーク上に設置され、複数人により利用され得る状態になっている事例を挙げ、ネットワークが特定の団体に属しており、その団体が署名作成データを管理しているような場合は格別、署名作成データが広く利用可能となっている場合には、この要件は満たされないと述べている（122パラグラフ）。同ガイドは、本人型リモート署名は取り上げていないが、これは、そのような署名の方法が当時存在していなかったためであろう。しかし、同ガイドは、一般論の文脈では、モデル法の解釈に際しては、技術中立性の原則に従い、将来行われることになるような電子署名の方法の使用を抑制する解釈は避けるべきであると述べている（34

---

29) 原文の該当部分は、以下のとおり。

Article 6. Compliance with a requirement for a signature

1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

...

3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:

...;

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

...

30) UNCITRAL Secretariat, "Guide to Enactment" (2001) 97パラグラフ。

パラグラフ)。したがって、本人型リモート署名サービスが利用される場合でも、その仕組み次第では、サービス利用者を署名者として見て、「署名作成データが・・・署名者の管理下にあり、他の者の管理下になかった」という要件が満たされると解すべきであろう。

他方、立会人型署名サービスにおいては、署名者はサービス提供事業者であって、利用者ではないので、「署名作成データが署名時に署名者の管理下にあり、他の者の管理下になかった」という要件の充足可能性に特に困難はないと思われる。ただし、立会人型署名サービスを用いてなされた電子署名によって行われたとみなされることになる「人の署名」(6条1項)は、あくまでサービス提供事業者自身の署名であることに注意を要する。サービス利用者の署名がサービス提供事業者の電子署名によって代替されうるとの解釈は、困難なように思われるからである。

## 2. EU の eIDAS 規則

EU では、電子署名に関して、「域内市場における電子取引のための電子識別および信頼役務に関する規則」(eIDAS 規則)<sup>31)</sup> が施行されている。

同規則は、前文において「リモート電子署名 (remote electronic signature)」に触れ、その経済的便益に鑑み、利用が増加するであろうと予測している (52パラグラフ)。ここで「リモート電子署名」と呼ばれているのは、「署名者に代わって (on behalf of the signatory)」信頼役務提供者によって電子署名作成環境が管理されているものとされている (同パラグラフ) ことから、本人型リモート署名のものがこれに該当する。そして、「利用者に代わって」とされているわけではないので、立会人型署名は対象となっていないのではないかとと思われる。

同規則は、同じく前文において、電子署名作成データが署名者の単独支配

---

31) 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 (OJ L 257, 28.8.2014, p. 73).



に服するような仕組みと手続が適切に実施され、適格電子署名作成装置の利用によって「適格電子署名 (qualified electronic signature)」の要件を満たすならば、署名者は第三者に同装置を託すことができると述べる (51パラグラフ)。これは、「リモート電子署名」の要件を要約したものと見受けられる。「適格電子署名」は、「電子署名 (electronic signature)」、「先進電子署名 (advanced electronic signature)」と並んで、同規則が定義する電子署名の一類型である。「適格電子署名」の定義は、「先進電子署名」のうち、「適格電子署名作成装置」によって作成され、「適格電子署名証明書」に依拠しているものであるとなっている (3条12号)。そこで、次に、この定義の三要素である「適格電子署名作成装置」、「適格電子署名証明書」、「先進電子署名」を略説する。

「適格電子署名作成装置」は、附則Ⅱの要件を満たす電子署名作成装置であるとされている (3条23号)。附則Ⅱは、「適格電子署名作成装置の要件」と題されており、その第3項は、署名者に代わって電子署名作成データを生成し、管理することができるのは、適格信頼役務提供者のみであると規定している。したがって、「リモート電子署名」のサービスは、適格信頼役務提供者のみが提供できることになる。適格信頼役務提供者とは、本規則に基づいて監督機関に資格を認められた適格信頼役務の提供者を言う (3条20号)。

「適格電子署名証明書」は、適格信頼役務提供者により発行され、附則Ⅰの要件を満たした電子署名証明書である (3条15号)。

「先進電子署名」の定義は、26条<sup>32)</sup>に置かれており、それが「高度の信頼を持って署名者が単独支配下に置くことのできる電子署名作成データによって作成されている (created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control)」こ

---

32) 原文の関連部分は、次のとおり。

Article 26 Requirements for advanced electronic signatures

An advanced electronic signature shall meet the following requirements: …

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and …

とがその要件の一つとなっている（同条c号）。前記した前文の51・52パラグラフは、「リモート電子署名」でも「適格電子署名」の要件を満たしうることを前提としているから、署名者に代わって信頼役務提供者により管理されている電子署名作成環境で作成された電子署名も、その仕組みと手続が適切に実施されれば、「高度の信頼を持って署名者が単独支配下に置くことのできる電子署名作成データによって作成されている」との要件を満たし得るとの解釈<sup>33)</sup>が導かれる。この解釈が可能であるのは、署名者に代わって信頼役務提供者によって電子署名作成環境が管理されていても、その仕組みと手続が適切に実施されていれば、電子署名作成データは署名者が「高度の信頼を持って」単独支配下に置いていると評価し得るからである。

なお、「高度の信頼を持って」の語は、本規則の前身である「電子署名のための共同体枠組みに関する1999年指令」（電子署名指令<sup>34)</sup>の「先進電子署名」の定義（2条2項）には含まれておらず、端的に、「署名者が単独支配下に置くことのできる方法によって作成されている（created using means that the signatory can maintain under his sole control）」（同項c号）ことが対応する要件となっていた。クラウド型署名は、同指令制定時には存在していなかったが、2005年、構成国の監督機関の団体であるヨーロッパ電子署名監督機関フォーラム<sup>35)</sup>が「サーバ上の署名（server-based signature）に関する声明」<sup>36)</sup>を公表した。同声明は、近年になってサーバ上の署名サービスが新

---

33) Alessio Zaccaria, Martin Schmidt-Kessel, Reiner Schulze, Alberto Maria Gambino (eds), *EU eIDAS Regulation* (2020) p. 248 [Katharina Erler 執筆担当]; 米丸恒治「eIDAS規則」専修ロージャーナル14号40頁（2018）参照。

34) Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 013, 19.12.2000, p.12). この指令は、eIDAS規則によって廃止された。

35) Forum of European Supervisory Authorities for Electronic Signatures (FESA). 現在は、名称が変わり、「ヨーロッパ信頼役務提供者監督機関（Forum of European Supervisory Authorities for trust service providers; FESA）」となっている。

36) Forum of European Supervisory Authorities for Electronic Signatures, “Public Statement on Server Based Signature Services” (17 October 2005) (<http://www.fesa.eu/public-documents/PublicStatement-ServerBasedSignatureServices-20051027.pdf>).

たに出現したことを指摘し、そのようなサービスでは、サービス提供者が「署名者 (signatory)」に代わって署名を行うと述べている。クラウド型署名のうち、本人型リモート署名がこれに該当するのは明らかであるが、「利用者」に代わって行うものと言っているわけではないので、立会人型署名は該当しないのではないかと思われる。同声明は、サーバ上の署名サービスによっても、電子署名指令2条2項c号の単独支配要件は満たされ得るのであり、「先進電子署名」が作成され得るとの見解を示しつつも、脚注において、ドイツ法の下では、単独支配は物理的支配を示唆するので、サーバ上の署名サービスによっては「先進電子署名」は作成され得ないと注記していた。

現行のeIDAS規則の下では、以上に見たとおり、「リモート電子署名」は、適格信頼役務提供者の提供するサービスによって、電子署名作成データが署名者の単独支配に服するような仕組みと手続が適切に実施され、所定の要件を備えていれば、「適格電子署名」となる<sup>37)</sup>。EU法においては、一般に、規則という法形式は、指令という法形式と異なり、各構成国で直接に効力を生じ、すべての構成国で法が統一されるので、ドイツも例外とはならない。eIDAS規則は、「適格電子署名は、手書き署名と同じ法的効力を有するものとする」と定める(25条2項)が、手書き署名がどのような法的効力を有するかは各構成国法に委ねている。また、各構成国は、適格電子署名の効力を独自に規定することができる。例えば、ドイツ民事訴訟法(Zivilprozessordnung)には、電子的方式の供述は、eIDAS規則に従って検証された適格電子署名に基づいて、真正に成立したとの推定が働き、それは

---

37) この点に関しては、批判的な論考 (Gisela Qirking-Kock, "Entwurf EU-Verordnung über elektronische Identifizierung und Vertrauensdienste" Datenschutz und Datensicherheit (2013) 1, 22) もあるが、中立的または肯定的な評価が多いようである (Alexander Roßnagel, "Neue Regeln für sichere elektronische Transaktionen" NJW 2014, 3686, 3689; Christian Seegebarth, "Perspektiven aus der eIDAS-Verordnung" 675, 677; Klaus Schmech, "Neue Signatur-Gesetzgebung: Sind aller guten Dinge drei?" 29, 30; Dennis Kügler, "Remote Signatures und mögliche Angriffe" [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/SmartCard\\_Workshop/Workshop\\_2015\\_Kuegler.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/SmartCard_Workshop/Workshop_2015_Kuegler.pdf) (2015) 22, 24; Erlер 前掲注 (33) 248)。

作成名義人の供述であることに重大な疑義を生ぜしめる事実によってのみ反駁することができるとの規定（371a条1項）が置かれている<sup>38)</sup>。これは、日本の電子署名法3条と類似性を有する規定であり、「リモート電子署名」も「適格電子署名」の要件を満たすものには、同項の効力が及ぶことになる。

### 3. 小 括

以上に検討したところでは、クラウド型署名のうち、本人型リモート署名については、EUのeIDAS規則の下で「適格電子署名」に該当し得るし、構成国法次第では、それによって文書の真正な成立が推定される。また、UNCITRALモデル法の下でも、手書き署名に代わる「信頼可能性を有する」電子署名に該当し得るとの解釈が可能である。これに対して、クラウド型署名のうち立会人型署名については、それに焦点を当てた議論は管見の及ぶ限り見当たらないが、署名サービス提供事業者自身の署名としての法的効果は認められるにしても、サービス利用者の署名に代替する署名としての法的効果は認められないのではないかと推察される。

## Ⅶ. 結 語

本稿では、第Ⅳ章で、クラウド型署名も電子署名法2条1項に定義されている「電子署名」に該当し得るが、第Ⅴ章で、3条との関係では、クラウド

---

38) 原文は次のとおりである。

Auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung der qualifizierten elektronischen Signatur nach Artikel 32 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73) ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung von der verantwortenden Person abgegeben worden ist.

型署名のうち、立会人型署名は、同条の対象としている「本人だけが行うことができることとなる」電子署名には該当しないとの解釈を示した。この解釈をとると、3条を介して立会人型署名の普及を後押しすることはできないが、第V章では、それでも不都合ではない理由も挙げた。本章では、立会人型署名に対比される場所の本人型署名について、その将来性を展望して本稿を締め括りたい。

クラウド型署名に注目が集まったのは、第III章で見たとおり、ローカル型署名の使い勝手の悪さのせいで、電子署名の普及が遅々として進んでこなかったからである。使い勝手の悪さの一つの原因は、電子証明書の発行を受ける手間と費用である。身元確認を経た電子署名を行うならば、認証サービス提供事業者等に依頼し、認証プロセスを経て、電子証明書の発行を受ける必要があるが、特に、日常的に大きな取引を行うわけではない個人が手間をかけて発行申請を行うことは、あまり期待できない。しかし、今後、署名鍵と電子証明書を格納したマイナンバーカードの普及が進むと、あらためて電子証明書の発行を求める費用や手間をかけることなく、確実性の高い公的個人認証に基づいて電子署名を行うことができる環境が整う<sup>39)</sup>。

ローカル型署名の利便性が悪いのは、これを安全に行うためには、署名鍵が格納されたICカードを安全に保管しておき、署名作業の都度、それを取り出してきて、カードリーダーライターで読み取るなどの面倒な作業が必要となるからでもある。しかし、普段から携帯するスマートフォンに、ICカードを読み取る近距離無線通信（NFC: Near Field Communication）機能を備えるものが増えてきており、カードリーダーライターが不要となりつつある。さらに、スマートフォン内のセキュリティー機能を備えた領域に署名鍵と電子証明書を格納できるようになる可能性もある。

本人型署名には、ローカル型署名の他に、クラウド型署名の一類型である本人型リモート署名があり、その潜在的可能性も大きいように思われる。例

---

39) 宮内宏『電子契約の教科書』95頁（日本法令、第三版、2021）も同旨。

えば、電子契約サービス提供事業者は、自らが公的個人認証サービス利用の認定<sup>40)</sup>を総務大臣から受ければ、契約当事者の電子署名の検証を公的個人認証基盤によって行うことができるので、各当事者が相手方当事者の署名検証を自ら行う必要のないスキームのサービスを提供することができる<sup>41)</sup>。また、電子契約サービス提供事業者は、自らが総務大臣の認定を受けなくとも、プラットフォーム事業者制度<sup>42)</sup>の下で、既存の総務大臣認定事業者に電子証明書取扱業務を委託することで、公的個人認証サービスの効果を享受することもできる。したがって、本人型リモート署名サービスの創意工夫が積み重ねられて行けば、公的個人認証に基づく電子署名の民間での利用が進む可能性もあるように思われる。

こうして見ると、本人型署名の将来性は大きく、ローカル型署名や本人型リモート署名の利用を支援すれば電子署名の普及は進む可能性があるようにも見受けられ、立会人型署名を後押しするために無理のある法解釈をする必要はないのではないかと思われる。

---

40) 電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律17条1項6号。

41) 詳しくは、宮内・前掲注(39)96頁参照。

42) 総務省「民間事業者における公的個人認証サービスの活用」([https://www.soumu.go.jp/main\\_content/000649058.pdf](https://www.soumu.go.jp/main_content/000649058.pdf))