電子署名法に基づく推定効の及ぶ電子署名の射程

海　野　敦　史

The Legal Range of Electronic Signatures That Have "Presumption Effect" under Electronic Signature Act of Japan

Atsushi UMINO

Abstract

While the legal range of electronic signature that has "presumption effects" under Article 3 of the electronic signature act of Japan (hereinafter "act") has been ambiguous, this paper attempts to make it clear by identifying the following conditions. First, it has to be the electronic signature defined by Article 2 of the act. Thus, it needs to have the function to identify the person who made the signature by the fact relevant to the measures taken. It should also have the function to find falsification, if any, of the electronic records that have electronic signatures. Second, it has to be the electronic signature that can be made only by the empowered signer. Therefore, it needs to have processes of the identification to confirm the existence of the signer as a writer of an electronic document as well as the authentication to check the right signer via different factors. It is also required to ensure the safety of the system of the signature in view of the necessity of the proper management of "requisite code and property." In particular, in the electronic signature with the assistance of a third party, system safety in the context of the internal processes of service providers (third parties) should be fully ensured so that unauthorized persons cannot make an access to the signature. It implies that the proper authentication process by using multiple factors should be ensured to confirm that only the right signer can direct service providers with regards to the signature.

Key Words

electronic signature act of Japan, presumption effects, identification, authentication, electronic signature with the assistance of a third party

目　　次

1 序　論

近年，新型コロナウイルス感染症の流行等を背景として，トラストサービス[1)]と称される各種のオンライン上のやり取りの有効性等を担保する仕組みに対する関心が高まっている．このトラストサービスの根幹をなすのが，電子契約等において当事者の正当性を確認するために用いられる電子署名である[2)]．

電子署名及び認証業務に関する法律（平成12年法律102号．以下，「電子署名法」という）3条は，「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」と規定し，電磁的記録に対して本人による一定の電子署名が行われている場合に，当該記録の成立の真正性を推定することを定めている．この推定の効力は，一般に「推定効」と称され，私文書に関して本人の署名・押印がある場合にその成立の真正性を推定することを定めた民事訴訟法（平成8年法律109号）228条4項の趣旨に相当するものと解されている[3)]．

すなわち，民事訴訟法228条1項において，（民事裁判上の証拠として用いられる）文書については，その成立の真正性を証明しなければならないこととされているところ，「情報を表すために作成された物件で文書でないもの」（以下，「準文書」という）に関して定めた同法231条により同法228条4項が準用される結果，準文書を証拠として用いる場合にも，その成立の真正性が証明されなければならないこととなる．これは，民事裁判において，証拠としての文書又は準文書は，その意味内容を証拠資料とするものであり，挙証者（ある事実を証明しようとして文書又は準文書を証拠として提出する者）の主張どおりの作成者の意思に基づいて作成されたものでない限り，当該意味内容を議論する前提を欠くことになるという点によるものであると解されている[4)]．それゆえ，電子署名が行われた電磁的記録を準文書として提出する場合にも，証拠調べを請求する者は，その成立の真正性を証明することが求められる．

このとき，その真正性とは，問題となる準文書たる電磁的記録の内容が，挙証者の主張する特定人（作成者）の意思に基づいて作成されたものであること意味する．それゆえ，電子署名法3条の推定効は，当該電磁的記録に関して，それに一定の要件を充足する電子署名が行われている場合について，その作成者の意思に基づいて作成されたものとして，成立の真正性を推定するというわけである．この推定は，民事裁判の相手方が当該真正性を争うときに実質的に意義を有することとなる．

それでは，具体的にどのような電子署名が電子署名法3条の推定効を得るのであろうか．この点については，一次的には「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」という法律上の要件を手がかりとして判断されることとなるが，電子署名の態様の多様化と相まって，当該要件の内実はやや曖昧であった．もっとも，近年，電子署名法の関係規定をめぐる行政解釈の整理が進展したことにより[5)]，かなりの明確化が図られつつある．しかし，当該整理の進展にもかかわらず，なお不明瞭となっているところもあり，いまだ確立した見解はないと指摘されている[6)]．それゆえ，更なる検討と実務上の知見の蓄積が求められる状況にあると言える．

そこで本稿は，電子署名法3条の推定効を受けるために電子署名が充足すべき要件の具体的な内実について法的考察を加え，当該推定効の及ぶ電子署名の射程を明らかにすることを目的とする．この目的を達成するため，まずは電子署名法上の電子署名の意義及び主な類型について整理したうえで（第2節），同法3条に基づく推定効の意義について確認するとともに，その推定効を得ることとなる電子署名の射程に関して，主な論点を摘示しつつ考察し（第3節），一定の結論を導く（第

4節）こととする．なお，文中の意見にわたる部分はもっぱら筆者の私見であり，その所属組織の見解とは一切無関係である．

2　電子署名の意義と主な類型

2.1　電子署名の定義

まず，考察の前提として，電子署名法上の電子署名の意義について，確認しておきたい．電子署名法3条の適用については，同法2条1項において定義される電子署名を対象とすることをその前提としているからである．

一般に，電子署名においてはいわゆる公開鍵暗号方式[7]が採られることが多く，暗号化のプロセスを経て実施される．すなわち，署名の対象となる電磁的記録（電子文書）と署名者の署名鍵（秘密鍵）との双方を署名生成プログラムに投入し，一種の暗号化が実施されることにより，電子署名が生成される．もっとも，電磁的記録をそのまま暗号化するには相当の処理時間を要するため，当該記録をハッシュ関数[8]に入力して得られるハッシュ値に基づき，暗号化及び復号が行われることが通常である．このように，電子署名の実体は暗号化された電子データであることから，電子署名を確認する（当該署名を検証する）ためには，署名生成時に用いられた署名鍵に個別に対応する公開鍵を用いることとなる．この公開鍵が署名者（電磁的記録の作成者）本人のものである事実が確認される（そのために当該本人の公開鍵が格納された電子証明書が添付され電子署名を検証する相手方に交付される）ことを通じて，署名が本人により生成されたことが明らかとなる．かかる公開鍵暗号方式を利用した電子署名は，しばしば「デジタル署名」と称される．

このような実態を踏まえ，電子署名法2条1項は，電子署名の概念を緩やかに定義づけている．すなわち，「電磁的記録（電子的方式，磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって，電子計算機による情報処理の用に供されるものをいう．以下同じ.）に記録することができる情報について行われる措置」であって，「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」（本人性）及び「当該情報について改変が行われていないかどうかを確認することができるものであること」（非改ざん性）の双方の要件を充足するものを指すという旨を規定している．これは，電子署名が付与された電磁的記録（電子文書）については改ざんがなく，誰が署名を行ったかを証明することが可能であるということを意味する．

それゆえ，本人性の要件に照らし，例えばある情報をもっぱら通信の内容を秘匿する目的で暗号化する行為が行われたとしても，それは電子署名を行ったことにはならない．一方，デジタル署名の場合，署名鍵で暗号化された暗号文を公開鍵によって復号することで得られた情報と電子署名の対象となる情報（のハッシュ値）との照合により電磁的記録の改変の有無を確認できるため，その限りにおいて非改ざん性の要件を充足することとなる．

ここで，本人性に関する「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当然に求められるわけではなく，他人が行った措置についても，署名者本人の意思のみに基づき当該他人の意思が介在することなく行われたものと認められる場合には，その本人が「当該措置を行った者」に該当するものと解されている[9]．そして，本人性が認定されるためには，署名者が電磁的記録を作成した旨を「示すもの」であれば足り，署名者が誰であるかということに関する身元確認までは要求されていないとされる[10]．すなわち，署名者の意思・認識を表すための措置（電子署名）が行われていることが，本人性の確認の決め手となる．

他方，非改ざん性に関しては，「確認」のための具体的な方法は特定されていないが，電子署名を行った後に，電磁的記録が改変されていないかどうかを確認可能な機能及び改変がされていた場合にそれを検知する機能を有していれば足りるも

のと考えられている[11]．それゆえ，電子署名における暗号の強度や改ざんの容易性の程度等については，電子署名法２条１項との関係上，直接問題となるものではない（改ざんが技術的に不可能な仕組みとなっていることまでは求められていない）と解される．

2.2　電子署名の主な態様

次に，電子署名の主な態様についても整理する．現在一般に行われている電子署名については，以下の各類型に大別することができる．

第一に，「ローカル署名」と称される伝統的な態様で，秘匿する署名鍵を IC カード等に格納して利用者の手元で自ら管理する方式の電子署名である．通常，署名鍵や利用者識別符号については，第三者的立場に立つ認証局等[12]から「安全かつ確実に利用者に渡すことができる方法」により交付される．

第二に，「リモート署名」と称される態様で，署名鍵や利用者識別符号を利用者が委託するサービス提供事業者のサーバに記録することにより行われる方式の電子署名である[13]．署名鍵はリモート（サーバ）上で管理されるものの，利用時にどこからでも利用者の認証によって署名することが可能となるものであり，電子契約サービス等の普及に伴いリモート署名の利用の拡大が期待されている[14]．

第三に，「立会人型署名」と称される態様で，利用者がサービス提供事業者のサイトに電磁的記録を送信し，当該サイト上で利用者の意思表示等の操作記録を残すことにより電子契約を成立させるサービスにおける電子署名である．政府は当該サービスについて，「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」と称している[15]．当該電磁的記録や操作記録については，利用者の指示に基づきサービス提供事業者の署名鍵により暗号化されるため，当該事業者が利用者の指示を受けてサービスとして電子署名を外形的に行うこととなる[16]．このとき，利用者が直接暗号化等に関する作業を行う必要がなくなるため，簡便に利用可能であるというメリットがある．

前述のとおり，「署名者本人の意思のみに基づき当該他人の意思が介在することなく行われたものと認められる場合」には本人性が肯定されることから，立会人型署名についても，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事実にかかわらず，利用者による電子署名と評価され得ることとなる．この点につき，政府は，「利用者が作成した電子文書について，サービス提供事業者自身の署名鍵により暗号化を行うこと等によって当該文書の成立の真正性及びその後の非改変性を担保しようとするサービスであっても，技術的・機能的に見て，サービス提供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」における電子署名の署名者は，（サービス提供事業者ではなく）利用者自身であるという旨を明示している[17]．ゆえに，立会人型署名においては，形式的に署名鍵による暗号化を行う者と電子署名の署名者とは異なり得ることとなる．

2.3　電子署名の技術の応用

電子署名は，電子契約の締結等に際して用いられることが多かったが，近年では，サイバーセキュリティを確保するための方途としても応用されている．具体的には，インターネット経由の通信を成立させる際に不可欠となるドメイン名システム（DNS）のセキュリティを確保するための DNSSEC（DNS Security Extensions）と称される仕組みにおいて，電子署名の技術が用いられている．

一般に，DNS の利用者がドメイン名に関する情報を得る場合，当該利用者から所定のネームサーバ[18]に対し，問合せを依頼する．その依頼を受けたネームサーバは，問合せ内容に基づき，起点となるルートサーバ[19]から委任をたどりつつ順に問合せを行い，目的のドメイン名情報を保有する権威ネームサーバから結果を取得する．そし

て，その問合せの結果を利用者に返答することとなる．問合せを処理するネームサーバは，その処理の途中で得たドメイン名に関する情報を一時的に保存（キャッシング）する仕組みを実装していることが多いため，「DNS キャッシュサーバ」とも称される．DNS キャッシュサーバは，権威ネームサーバへの問合せを行う際に，「ID」という 16 ビットの識別子を DNS メッセージの中で指定しつつ送信する．そして，当該問合せにより得た応答のメッセージ中の ID を確認し，両 ID が一致している場合には，当該問合せに対する応答であると判断することとなる．

ところが，ID は 16 ビット（65,536 通り）しか取り得る値がないため，総当たりでパケットを生成するなどの手段で偽装されるリスクを内包している．このような偽装が発生すると，ホスト名と IP アドレスとの対応が本来の情報とは異なるものとして利用者に伝わり，特定のウェブサイトへ到達できなくなったり，攻撃者がコントロールする別のウェブサイトへ誘導されたりする危険性が発生する．かかる危険性に対して，DNS における応答の正当性を保証するための拡張仕様である DNSSEC においては，公開鍵暗号方式による電子署名の仕組みに基づき，DNS キャッシュサーバが問合せにより得た応答が，問い合わせた本来の権威ネームサーバからの応答か否か，パケット内容が改ざんされていないか否か，問い合わせた記録が存在するか否か，などの点を検証することが可能となっている [20]．それゆえ，電子署名の技術は，サイバー空間における基幹的な DNS のセキュリティを支えることにも資していると言える．

3　電子署名法 3 条に基づく推定効の及ぶ射程

3.1　推定効の意義

前節で概観した電子署名の意義を踏まえ，電子署名法 3 条が規定する推定効の及ぶ射程について検討するのに先立ち，当該推定効の意義について簡潔に確認する．民事裁判において，証拠となる文書又は準文書がその作成者の意思に基づいて作成されたものと認められ，当該文書又は準文書が真正に成立すれば，それは当該作成者の思想等を表すものとして，形式的証拠力が肯定される．これは，その文書又は準文書の内容の真実性等に関する実質的証拠力を判断するための土台となるものとされている [21]．

この形式的証拠力については，挙証者が自ら証明することも可能であるが，民事訴訟法 228 条 4 項又はその特則としての電子署名法 3 条に基づく推定効により，その証明の必要性がなくなることとなる．もっとも，民事訴訟法学説上の通説は，当該推定効について，相手方が反証により覆すことが可能であるとしており [22]，証明責任を転換する推定であるとは位置づけられていない．また，この推定効は，あくまで民事裁判における文書又は準文書の証拠としての利用可能性を支えるものであり，契約や電子署名等の有効性の判断に直結するものではない．それゆえ，電子契約に電子署名法 3 条の示す電子署名が行われていなくとも，自由心証主義（民事訴訟法 247 条参照）[23] の下での証拠提示方法に特段の制限はないため，契約当事者間の合意の内容を明らかにし得る限り，当該契約の成立の真正性や有効性は肯定され得る．

民事訴訟法 228 条 4 項にいう「押印」に関しては，私文書の作成名義人の印影が当該名義人の印章と一致していれば，別段の反証のない限りその印影は当該名義人の意思に基づいて押印されたものと推定（一段目の推定）され [24]，その結果として，その私文書全体が作成名義人の意思に基づいて作成されたことが推定（二段目の推定）されるものと捉えられている [25]．ただし，判例は，印章の保管や使用の状況によっては，印影が作成名義人の印章に符合する場合でも，一段目の推定が認められないことがあるという旨を示している [26]．このような「二段の推定」が電子署名法 3 条においても適用されるか否かについては必ずしも明らかになっていないが [27]，同条が求める要件を充足する電子署名であれば，二段の推定が成立する可能性は十分にあると指摘されている [28]．そこで，電子署名法 3 条が推定効の付与に当たっ

て要求する具体的な要件が問題となる．

3.2　推定効を受けるための要件

電子署名法３条は，電子署名法２条１項にいう電子署名に該当するものを対象とすることを前提としつつ，「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」という要件を加重している．この要件に関しては，以下の各点において，曖昧さを抱えており，それらについて解釈論的に究明される必要があると考えられる．

第一に，「本人だけが行うことができることとなるもの」という要素について，どのように署名者本人の確認を行うことが求められるのかということである．一般に，オンライン上の利用者に対する本人確認の手段については，公的身分証等により実際にその行為を行う利用者が実在する特定の存在であることを確認する「身元確認」と，ID・パスワードや生体認証等を通じて利用者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」とに大別される[29]．これを電子署名における本人確認の過程に当てはめれば，電磁的記録への署名者が確かに存在してそれが当該記録の作成名義人と同一であることを本人確認書類や電子証明書内の情報等から確認する「身元確認」のプロセスと，実際に電磁的記録に電子署名が行われる時点で身元が確認された当人であることをログイン情報等から確認する「当人認証」のプロセスとがあるということになる．それゆえ，この問題は，① そもそも電子署名法３条において身元確認を行うことが求められているのか，② 同条において求められる当人認証の水準はどのようなものか，という二つの論点を内包する．これらのうち，前記①に関しては，後述するとおり一定の議論の蓄積があるが，一義的な解釈が導かれているわけではない．

第二に，「必要な符号及び物件を適正に管理する」という要素に照らし，電子署名の実施を支えるシステム上の安全性が求められると考えられるところ，どのような安全性が要求されているのかということである．この点に関しては，学説上の議論自体が乏しいところである．以上の各点について，既に提示されている議論を踏まえつつ，以下において順次考察を加える．

3.3　身元確認の必要性

政府によれば，電子署名法３条にいう「本人」とは電子文書の作成名義人[30]を指し，「本人だけが行うことができることとなるもの」に該当するためには，「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」が必要であるとされている．これは，「固有性の要件」と称され，「電子署名について相応の技術的水準が要求されることになるもの」であるとされる．その例として，「十分な暗号強度を有し他人が容易に同一の鍵を作成できないものである場合」が挙げられている[31]．このような一定の技術的水準が求められていることは，押印の場合の実印の使用に近いとも言える[32]．

ところが，固有性の要件との関係における身元確認のあり方については必ずしも明らかにされておらず，その必要性それ自体やそれが認められる場合の方法が問題となる[33]．すなわち，「本人だけが行うことができることとなるもの」を肯定する前提として，問題となる電子署名における署名者本人の確認が必要となり得る中で，当該確認については，署名者自身が電子署名の時点で行った行為であるかを確認するだけでなく，電磁的記録の作成名義人としての当該署名者の実在性を確認することまで求められるのか否かが論点となっている．

この身元確認の必要性について，論者の見解は分かれている．ある見解は，電子署名法３条を適用するうえで，「サービス上で署名する際のセキュリティを高める『当人認証』だけでなく，署名者の実在性（署名者が『どこの誰なのか』）を担保する『身元確認』と併せた『本人確認』が必要不可欠である」と説く．これによれば，身元確認

を経ない単純な二要素認証（3.4 参照）等ではこの要件を満たさないという[34]．

一方，電子署名法 3 条に基づく推定効との関係において，身元確認は不要であるとする見解も提示されている．その理由として，① 電子署名法 3 条はもとより，「電子署名のうち，その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務」（同法 2 条 3 項）に関する基準を定めた電子署名及び認証業務に関する法律施行規則（平成 13 年総務省・法務省・経済産業省令 2 号．以下，「電子署名法施行規則」という）2 条においても，（暗号の困難性に関する水準が規定されているものの）身元確認の必要性を明示する定めはないこと，② 固有性の要件の本質は暗号の強度に関するものであって，利用者の真偽の確認はあえて定められなかったのが立法経緯であること，が指摘されている[35]．

これらに対し，立法による趣旨の明確化を求める見解も提示されている．これによれば，政策判断上，身元確認を求める場合には，法的安定性を確保する観点から，法律改正が必要であるという[36]．

思うに，電子署名法 3 条にいう「本人だけが行うことができることとなるものに限る」という電子署名の加重要件は，「本人だけ」という形で代理人等の意思に基づく行為を排している以上，署名者本人が電磁的記録の作成名義人として真に実在することを当然の前提とするものであろう．換言すれば，（法律改正を行わずとも）現行の電子署名法 3 条の下で，固有性の要件に裏づけられた「本人だけが行うことができることとなるもの」であることの認定には，署名者本人の身元確認が不可欠となると解される．これは，電磁的記録への署名者が確かに存在し，それが当該記録の作成名義人と同一であることを確認するプロセスとなる．特に，他人へのなりすましや複数のアカウント保有に伴う犯罪等を防止する観点からは，（当人認証に加えて）身元確認も同時に行うことが強く求められ得る[37]．

それゆえ，電子署名法 3 条及びその関連法令の規定が身元確認を明示的に求めていないことは，身元確認のプロセスを経ることを当然視した結果であると捉えることが可能であり，当該プロセスを不要とする趣旨とは解しがたい．また，判例が押印に関して「印章は通常第三者が勝手に押印できないよう大切に扱われる」という経験則に基づき「一段目の推定」を肯定してきたことにかんがみれば，推定効の及ぶ対象となる電子署名の射程に関しても，我々の経験則も踏まえて判断する必要が生じるところ，署名者の実在性が確認可能であることが当該経験則になじむように思われる[38]．よって，固有性の要件に関しては，電子署名が署名者自身による行為であるかを確認する当人認証だけでなく，当該署名者の実在性を確認する身元確認をも要求するものと解される．

実際，政府も「電子署名法第 3 条の推定効が認められるためには，電子文書の作成名義人の意思に基づき電子署名が行われていることが必要であるため，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」と説いている[39]．逆に，十分な身元確認が行われないまま，当人認証が厳格に行われたとしても，なりすましを十分に防止することは困難であり，電子署名法 3 条を適用するための適切な措置が採られているとは言えないと考えられる．特に，外形的には署名者本人以外の者が署名を行うこととなる立会人型署名においては，一般に認証局による身元確認を欠くこととなるため，サービス提供事業者に指示を行う利用者が実在し，それが電磁的記録の作成名義人と同一であるか否かの確認が別途行われることが，電子署名法 3 条の推定効が及ぶうえで重要となろう[40]．

なお，身元確認の具体的な方法については，（当人認証とともに）「本人だけが行うことができることとなるもの」であることが確認できる限り，一義的なものではないと考えられる．近年では，伝統的な対面や郵送等による本人確認書類の確認のほか，オンライン上で完結する身元確認の方

法[41]も実用化されており，注目に値する．

3.4　当人認証のあり方

一方，求められる本人確認のあり方に関して，当人認証をどのように行うことが求められるのであろうか．当人認証については，一般に，生体（顔，指紋等），所持（個人番号カード等），知識（パスワード等）のいずれかの要素の照合により，本人が（ログイン時等に）作業していることが確認される必要があるとされている[42]．そして，電子署名法3条との関係においては，しばしば二要素（以上）の認証の重要性が指摘されている[43]．同条の「本人だけ」という要件に照らせば，少なくとも多要素認証（生体要素と知識要素との組合せ等）[44]を通じて確実に（署名時点における）署名者自身による行為である事実が確認されることが，推定効が付与されるうえで求められるものと考えられる．

もっとも，多要素認証さえ行われれば常に求められる当人認証の水準を充足するのかといえば，そうとは言い切れない．この点については，技術的になお検討の余地があるが，米国の国立標準技術研究院（NIST：National Institute of Standards and Technology）が当人認証に関して3段階の技術的水準を設定していることが参考となろう．これによれば，認証の対象者が正規の利用者のアカウントに結びつけられた認証の要素を保有・管理していることについて，ある程度の確信度で保証される水準（AAL1）[45]，高い確信度で保証される水準（AAL2），非常に高い確信度で保証される水準（AAL3）があるとされる．そして，AAL1水準の認証が行われるうえでは，認証の対象者が単一の認証の要素を保有・管理していることが安全な認証プロトコルにより証明される必要がある．AAL2水準の認証が行われるうえでは，認証の対象者が異なる複数の認証の要素を保有・管理していることが安全な認証プロトコルにより証明され，かつ承認済の暗号化技術が利用される必要がある．AAL3水準の認証が行われるうえでは，認証の対象者による暗号プロトコルを通じた鍵の保有が証明される必要があり，AAL2で示される認証の要素に加え，検証者に偽装耐性を提供する暗号化された認証の要素が求められるという[46]．これらのうち，多要素認証を必須の前提としているのはAAL2以上であることを踏まえ，推定効が及ぶ電子署名となるためには，AAL2以上に相当する技術的水準の内容を充足する手法での当人認証が行われた電子署名であることが求められるように思われる．

このような当人認証のあり方が実務上特に問題となり得るのが，利用者の指図に基づき外形的には事業者により署名が行われることとなる立会人型署名である．かつて政府は，立会人型署名の場合は形式的には署名者が事業者であって「本人」自身の電子署名ではないので，電子署名法3条に基づく推定効が認められない可能性が高いという旨を示していた[47]．しかし，その後，立会人型署名であっても，「本人」の意思に基づく措置が講じられていると認められる一定の場合に関して，署名又は記名押印に代わる措置としての電子署名の推定効に肯定的な見解が示されるようになった[48]．これによれば，サービス提供事業者のサービスが十分な水準の固有性を充足していると認められることが必要となるところ，そのためには，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，② 前記①における利用者の行為を受けてサービス提供事業者内部で行われるプロセス，の双方が問題となるとされている．そして，前記①に関しては，利用者が二要素による認証を受けなければ措置を講じることができない仕組みが備わっているような場合について，前記②に関しては，サービス提供事業者が当該事業者自身の署名鍵により暗号化等を行う措置にお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に照らして電磁的記録が利用者の作成に係るものであることを示すための措置として十分な水準の固有性が充足されていると評価できるような場合について，それぞれ固有性の要件の充足が肯定されている[49]．前者については前述の当人認証の問題であり，後者についてはサービス提供事業者の支配下にあ

るシステムの安全性を問題とするものであると言える．そして，政府が例示するこれらの場合には，立会人型署名についても，電子署名法３条に基づく推定効が認められ得るということが示唆されている．

このような政府の見解に照らせば，立会人型署名においては，(ア) 署名者（サービスの利用者）の身元確認が行われること，(イ) 署名者の当人認証プロセスについて十分な固有性が充足されていること，(ウ) サービス提供事業者内部のプロセスにおいてシステム上の安全性が確保されつつ十分な固有性が充足されていること，の各要件が肯定されて初めて，電子署名法３条に基づく推定効が認められ得るという帰結が導かれ得る．これらのうち，立会人型署名の実務上，前記(イ)の当人認証が電子メールにより行われる場合が少なくないことに照らすと，かかる場合が固有性の要件を充足するか否かがさらに問題となる．

この点に関しては，一般的な電子メールについて，(a) メールアドレスの持ち主に素早く確実に届く到達容易性，(b) 印章よりも確実にアクセス管理できる安全性，(c) 送受信内容が日時とともにログとして残る記録性等を有することのほか，多くのフリーメールでは二要素認証が実施されている実態があることにかんがみ，推定効を支える有効な本人確認手段となり得るという旨が指摘されている．これによれば，一意性を有する有効期限付きの専用署名 URL をメールアドレスに配信し，多要素認証を通じて署名者本人のみが電子署名の指図を可能な仕組みが用いられている限り，専用署名 URL を通じて電子署名の実施を指図できるのは当該メールアドレスの利用者本人である蓋然性が高いとされる[50]．これらの要素に照らして考えれば，立会人型署名においても，署名者の実在性が確認されたうえで，電子メールを通じた多要素認証（当人認証）を通じて署名者本人のみが電子署名の指図を可能な状態となっていると認められる限り，電子署名法３条の推定効が及ぶこととなるものと解される[51]．

3.5　システム上の安全性の確保のあり方

他方，電子署名法３条の推定効が及ぶうえでは，同条にいう「必要な符号及び物件を適正に管理する」という要素から，電子署名の実施におけるシステム上の安全性（セキュリティ）の確保が求められるということは前述のとおりである．しかも，前述の「印章の保管や使用の状況によっては，印影が作成名義人の印章に符合する場合でも，一段目の推定が認められないことがある」という旨の判例法理に照らせば，電子署名の署名鍵の保管・使用状況次第では，たとえ十分な本人確認が行われ得たとしても，（一段目の推定の対象とならず）推定効を有する電子署名の射程から外れることとなる可能性がある．それゆえ，電子署名法３条に基づく推定効を受けるためには，本人確認のプロセスのほか，電子署名のための署名鍵の保管・使用状況を含むシステム上の安全性についても考慮に加えられる必要があると考えられる．

このシステム上の安全性が求められる具体的な水準ないし程度については，電子署名法３条が特段明示していないため，一義的に明らかなものではない．しかし，同条にいう「本人だけが行うことができる」と同一の文言を用いた電子署名法２条３項が電子署名法施行規則２条の規定にその内容を委任しており，当該規定が「ほぼ同じ大きさの二つの素数の積である 2048 ビット以上の整数の素因数分解」等の「困難性」に基づき「電子署名の安全性」を求めていることにかんがみると，かかる困難性に基づくものと同等の高いレベルの安全性が必要になるものと考えられる[52]．しかも，実印は物理的に唯一性を有し，その管理は一般に利用者のガバナンスに服しているのに対し，電子署名の場合は署名鍵がひとたび漏えい又は窃用されてしまうと容易に第三者にコピーされ流布することとなってしまうというリスクを抱えているため，相当のシステム上の安全性が求められるとも言える．

もっとも，ローカル署名の場合，本人のみが署名鍵を取り扱うこととなるため，一定のシステム上の安全性（一般的な実印の保管のあり方に近似

する水準の安全性）が一応推定され得るところであり，その意味において押印の実務と著しい格差があるわけではない．それゆえ，署名鍵等の取扱いにおいて，前述の電子署名法施行規則２条における困難性に基づくものと同等の水準での安全性が確保されていると認められる限り，推定効の及ぶ可能性が高いと思われる[53)]．これに対し，立会人型署名の場合においては，かかる水準での安全性がより厳格に要求されることとなろうが，サービス提供事業者内部のプロセスやシステムの管理の実態に照らして当該安全性が肯定される限り，同様に推定効が認められ得ると考えられる．

このように，電子署名法施行規則２条における困難性に基づくものと同等の水準でのセキュリティの確保を通じて，一般的な実印の保管状況に近似した程度の安全性が保証される限り，電子署名法３条の推定効が及ぶ電子署名の付された電磁的記録と民事訴訟法 228 条４項に基づいて真正性が推定される押印のある私文書とは，作成名義人の意思に基づいて作成されたことを推定し得る程度に関してほぼ同等であると捉えることができる．したがって，かかる電磁的記録に対しては，（押印のある私文書と同様に）二段の推定が成立することとなるものと考えられる．

4　結　　論

電子署名法３条が規定する推定効を受ける電子署名の射程については，これまで曖昧な部分が残されてきたが，以下のように整理することができる．第一に，電子署名法２条１項にいう電子署名に該当することが前提となる．それゆえ，電子署名として行われる「措置に関する事実」から，署名を行った者が誰であるかを識別し，それ以外の者にはリンクしないこと又は署名を行った者以外の者の意思が介在していないことを確実にする機能（本人性）に加え，電子署名が付された電磁的記録が改ざんされていないかどうかを確認することができる機能及び改ざんがなされた場合にそれを技術的に検知することができる機能（非改ざん性）が確保された電子署名である必要がある．

第二に，電子署名法３条にいう「本人だけが行うことができることとなるもの」に該当する電子署名でなければならない．そのためには，適切な本人確認のプロセスを経ることに加え，「必要な符号及び物件」の適正な管理の必要性を踏まえたシステム上の安全性（セキュリティ）の確保が必要となる．すなわち，① 電磁的記録の作成名義人としての署名者の実在性を確認する身元確認（確認の方法は一義的なものではなく，オンライン上で完結するものもあり得る），② 多要素認証等を通じた適切な当人認証（対象者が異なる複数の認証の要素を保有・管理していることが的確に証明される形での当人認証が行われること），③ 電子署名における署名鍵の保管・使用状況等を含むシステム上の安全性，が実施又は確保されていることが求められる．特に，立会人型署名においては，前記③に関してサービス提供事業者内部のプロセスにおける十分な固有性が充足されていることが重要であり，多要素による当人認証等を通じて署名者（利用者）本人のみが電子署名の指図を可能な状態となっていると認められることが不可欠である．

これらの条件が確保された電子署名が施された電磁的記録に対しては，押印された私文書と同様に二段の推定が成立し，電子署名法３条に基づく推定効が及ぶものと解される．この推定効は，民事裁判における自由心証主義を覆すものではないが，民事裁判の相手方が電磁的記録の成立の真正性を争う場合において，その真正性を反証がない限り推定することにより，実質的に大きな意義を有するものとなる．

注

1）政府によれば，トラストサービスについては，「サイバー空間と実空間の一体化が進展し，社会全体のデジタル化が進む中，その有効性を担保する基盤として，送信元のなりすましやデータの改ざん等を防止する仕組み」として位置づけられる．（総務省 2020：3）参照．

2）（総務省 2020：3）参照．

3）（岡村 2011：201）参照．

4）（兼子ほか 2011：1263）参照.
5）総務省・法務省・経済産業省「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」（令和 2 年 7 月 17 日．以下，「2 条 1 項 Q&A」という），総務省・法務省・経済産業省「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（電子署名法第 3 条関係）」（令和 2 年 9 月 4 日．以下，「3 条 Q&A」という）参照.
6）（福岡 2020：39）参照.
7）署名鍵（秘密鍵）及び公開鍵を 1 組の暗号鍵として使用しつつ，双方の鍵を合わせた場合に初めて暗号が解読できるようにする方式を指す．署名鍵で暗号化された情報については，公開鍵でなければ原初の状態には戻らない.
8）入力されたデータに対して一定の手順で計算を行ったうえで，入力値の長さにかかわらず，あらかじめ決められた固定長の出力データを発出する関数のことを指す.
9）2 条 1 項 Q&A 参照.
10）（鈴木 2021：4）参照.
11）（宮川＝望月 2020）参照.
12）ここでいう認証局とは，電子証明書の申請・発行や署名鍵・公開鍵の発行を担当する機関のことであり，電子契約を締結する際にその契約主体となる法人・個人の実在性や正当性を保証する役割を一般に担うものである.
13）なお，署名鍵をサーバやクラウド等のリモート上で管理するが，本人又はサービス提供事業者がそれを署名時に利用可能となる電子署名の態様を「クラウド署名」と総称することがある．リモート署名はクラウド署名の一形態であると言える.
14）リモート署名に関する民間団体によるセキュリティ対策用ガイドラインとして，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 年 4 月 13 日）参照.
15）3 条 Q&A 参照.
16）それゆえ，「事業者型署名」ないし「第三者型署名」と称されることもある.
17）2 条 1 項 Q&A 参照.
18）インターネット経由の通信において，ドメイン名を IP アドレスに変換する名前解決を行うサーバのことを指す.
19）階層構造を有するドメイン名空間の頂点である DNS 最上位に存在する「ルートゾーン」を提供するネームサーバのことを指す.
20）一般社団法人日本ネットワークインフォメーションセンター「DNSSEC」，https://www.nic.ad.jp/ja/newsletter/No43/0800.html（2023 年 1 月 3 日最終閲覧）参照.
21）（伊藤 2020：432–433），（三木ほか 2018：314–315）参照.
22）（秋山ほか 2019：551），（三木ほか 2018：315–317）参照.
23）裁判に必要となる事実の認定や証拠の評価について裁判官の自由な判断に委ねる主義のことを指す.
24）最判昭和 39 年 5 月 12 日民集 18 巻 4 号 597 頁参照．印鑑登録されている実印のみならず，認印でもこの推定は適用され得るとされる．最判昭和 50 年 6 月 12 日集民 115 号 95 頁参照.
25）（伊藤 2020：433–434），（三木ほか 2018：316–317）参照.
26）最判昭和 45 年 9 月 8 日集民 100 号 415 頁参照.
27）なお，政府は，二段の推定により証明の負担が軽減される程度について，限定的であるという旨を説いている．その理由として，① 推定である以上，印章の盗用や冒用等により他人がその印章を利用した可能性があるなどの反証が相手方から示された場合には，その推定は破られ得ること，② 印影と作成名義人の印章が一致することの立証は，実印である場合は印鑑証明書等を通じてある程度容易であるが，認印の場合は事実上の困難が生じ得ること，が指摘されている．内閣府・法務省・経済産業省「押印についての Q&A」（令和 2 年 6 月 19 日）参照.
28）（福岡 2020：42）参照.
29）（経済産業省ほか 2020：5）参照．併せて，（日本トラストテクノロジー協議会真正性保証タスクフォース 2019：7–12）参照.
30）これは，基本的には電子署名の署名者（署名の意思を有する者）に符合すると考えられる.
31）3 条 Q&A 参照.
32）（鈴木 2021：4）参照.
33）（福岡 2020：39）参照.
34）GMO グローバルサイン・HD・プレスリリース（2023 年 1 月 3 日），https://www.gmogshd.com/news/press/gmo-hs/200918_3086.html（2023 年 1 月 3 日最終閲覧）参照.
35）（福岡 2020：38–39）参照.
36）（渡部 2020：45–46）参照.
37）（鈴木 2021：11）参照．もっとも，身元確認は当

人認証のプロセスと一体的・複合的に行われることも少なくなく，その場合には両者の厳格な峻別が困難となり得るが，少なくとも身元確認が適切に行われないまま（他人によるなりすましの可能性を内包したまま）当人認証が行われたとしても，十分な本人確認が行われたことにはならない．

38）もっとも，その前提として，「電子署名を行う方法が，押印を施す印章と同様に，本人によって大切に扱われている」という経験則が認められることが必要となる．電子署名法3条が，民事訴訟法228条4項の「特則」となり得る推定効を一定の電子署名に認めていることにかんがみれば，かかる経験則は肯定され得ると考えられる．

39）3条Q&A参照．もっとも，政府は身元確認を電子署名法3条の適用のための必要条件であるとは指摘しておらず，利用者間でどの程度の身元確認を行うかということについては，電子契約の重要性の程度等を考慮して決められるべきであるとしている．第3回デジタルガバメントワーキング・グループ（令和2年11月17日）「論点に対する回答」（総務省・法務省・経済産業省提出資料）参照．

40）なお，そもそも確実な身元確認が必要な場合には，認証局が身元確認を行うローカル署名を利用すればよいことから，実務上立会人型署名が利用されるのは，店舗等で身元確認が既に行われている契約や，犯罪による収益の移転防止に関する法律（平成19年法律22号．以下，「犯罪収益移転防止法」という）4条等により本人確認が義務化されている契約のほか，契約の性質・金額等からリスクが少ないものと利用者が判断のうえ電子署名法3条の推定効を求めない場合が少なくない．一般社団法人日本ネットワークインフォメーションセンター・前掲（注20）参照．

41）行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律27号）2条7項で定義される「個人番号カード」を利用した公的個人認証のほか，犯罪収益移転防止法施行規則（平成20年内閣府・総務省・法務省・財務省・厚生労働省・農林水産省・経済産業省・国土交通省令1号）6条1項1号ホ及びトに規定する方法等がある．

42）（経済産業省ほか2020：3・5）参照．

43）政府は，二要素認証について，「十分な水準の固有性の要件を満たすための措置の例」としている．第3回デジタルガバメントワーキング・グループ・前掲（注39）参照．

44）多要素認証の例として，「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，スマートフォンへのSMS送信や手元にあるトークンの利用等当該メールアドレスの利用以外の手段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するもの」が指摘されている．3条Q&A参照．

45）AALとは”Authenticator Assurance Level”の略である．

46）*See* NIST（2017a: 19）．*See also* NIST（2017b），NIST（2017c），NIST（2017d）．

47）規制改革推進会議第11回成長戦略WG（2020年5月12日）資料参照．

48）3条Q&A参照．

49）3条Q&A参照．

50）Cloudsign「電子署名と二段の推定―メールアドレス認証によって電子署名法3条の推定効は及ぶか」（2020年8月27日），https://www.cloudsign.jp/media/20200827-nidannosuitei/（2023年1月3日最終閲覧）参照．

51）もっとも，電子契約は，押印による契約と異なり，電子署名により改変が困難なファイルを作成できるうえに，電子メールアドレス以外にもアクセスログが無数に残り得るため，二段の推定に依拠しなくとも電子文書の真正な成立を争う訴訟はそもそも発生しにくく，仮に発生したとしても相手方を追求しやすいという特徴を有する旨が指摘されている．（高橋2020：238）参照．

52）ただし，電子署名法3条の規定は電子署名法施行規則2条と直接紐づけられていないことから，電子署名法施行規則2条を充足することはシステム上の安全性が認められるための十分条件であって，必要条件ではないと解される．すなわち，必ずしも電子署名法施行規則2条を充足していなくとも，他の方法により「必要な符号及び物件を適正に管理する」ものと認められ，電子署名法3条括弧書きの条件を充足する場合には，同条の推定効が肯定される余地があると考えられる．日本ネットワークセキュリティ協会「電子署名Q&A」，https://www.jnsa.org/result/e-signature/e-signature-qa/（2023年1月3日最終閲覧）参照．

53）（圓道2020：22）参照．併せて，Cloudsign・前掲（注50）参照．

【参考文献】

［邦文文献］

秋山幹男ほか（2019）『コンメンタール民事訴訟法Ⅳ［第2版］』日本評論社.

伊藤眞（2020）『民事訴訟法［第7版］』有斐閣.

圓道至剛（2020）「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（4）：22–27.

岡村久道（2011）『情報セキュリティの法律［改訂版］』商事法務.

兼子一ほか（2011）『条解 民事訴訟法［第2版］』弘文堂.

経済産業省ほか（2020）「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年3月31日）.

鈴木絢子（2021）「電子契約・電子署名の現状と課題」『調査と情報–ISSUE BRIEF–』1135.

総務省（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）（2020）「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最終取りまとめ」（2020年2月）.

高橋郁夫ほか編（2020）『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.

日本トラストテクノロジー協議会真正性保証タスクフォース（2019）「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）.

福岡真之介（2020）「電子署名法3条の推定効についての一考察」『NBL』1179: 34–42.

三木浩一ほか（2018）『民事訴訟法 第3版』有斐閣.

宮川賢司＝望月亮佑（2020）「電子契約・電子署名の活用に関する諸問題–テレワーク・在宅勤務における利用拡大に備えて」『AMT Newsletter』2020/6.

渡部友一郎（2020）「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（10）：38–47.

［英文文献］

National Institute of Standards and Technology（NIST）（2017a), NIST Special Publication 800–63–3, Digital Identity Guidelines（June, 2017), https://pages.nist.gov/800–63–3/（2023年1月3日最終閲覧).

NIST（2017b), NIST Special Publication 800–63A, Digital Identity Guidelines: Enrollments and Identity Proofing Requirements（June, 2017), https://pages.nist.gov/800–63–3/sp800–63a.html（2023年1月3日最終閲覧).

NIST（2017c), NIST Special Publication 800–63B, Digital Identity Guidelines: Authentication and Lifecycle Management（June, 2017), https://pages.nist.gov/800–63–3/sp800–63b.html（2023年1月3日最終閲覧).

NIST（2017d), NIST Special Publication 800–63C, Digital Identity Guidelines: Federation and Assertions（June, 2017), https://pages.nist.gov/800–63–3/sp800–63c.html（2023年1月3日最終閲覧).