主務三省 Q&A（電子署名法第 3 条関係）に関する解説

トラストサービス推進フォーラム 会長
慶應義塾大学 教授　　手塚　悟
電子認証局会議 会長
日本電子認証株式会社　宮脇 勝哉

電子認証局会議およびトラストサービス推進フォーラムは、それぞれ電子署名法の認定認証事業者、タイムスタンプ事業者を中心に組織された団体で、これまで国内におけるトラストサービスの普及に尽力して参りました。トラストサービスとは「インターネット上における人・組織・データ等の正当性を確認し、改ざんや送信元のなりすまし等を防止する仕組み」[1]であり、デジタルデータの信頼性を確保するために重要な役割を担っています。2019 年 1 月より、総務省ではトラストサービス検討ワーキンググループが立ち上がり、制度整備に向けた検討が継続されています。また、内閣府ではテレワークの推進に向け書面規制、押印、対面規制についての見直しが開始され[2]、電子署名法に新たな解釈・見解を加える文書が発表されるなど、トラストサービス関連の制度が時代に合わせ再度整備されつつあります。

一方でクラウドサービスの発展によりトラストサービスの技術を利用した多種多様な電子契約サービスが登場しておりますが、信頼性の確保という観点から見ると異なる信頼レベルの電子契約サービスが入り混じって提供され、利用者にとってどのサービスを選択することが適当であるかわかりにくい状態になっています。2001 年の電子署名法の施行以降、安定的にトラストサービスを提供してきた立場として、電子契約サービスを利用する方々が引き続き安心してサービスを利用できるよう、今回 2 団体が共同で解説を発表することとしました。

1. はじめに

新型コロナウイルスの感染拡大に伴い、社員の出社が制限され在宅勤務などのテレワークが拡大しています。企業においては紙文書から電子文書への転換が課題とされ、「脱ハンコ」の動きが活発化しました。昨今では企業のデジタルトランスフォーメーションも本格化し、電子契約サービスが注目を浴びています。

政府からも契約業務における押印廃止・電子化を後押しする文書が次々発表されました。2020 年 6 月 19 日に「押印に関する Q&A[3]」、7 月 17 日に「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）[4]」、そして 9 月 4 日に「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

---

[1] 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最終取りまとめ」https://www.soumu.go.jp/main_content/000668595.pdf 2020 年 2 月 7 日

[2] 内閣府「第 6 回経済財政諮問会議：緊急提言～感染症の長期化・再発と経済変動に備えるために～（有識者議員提出資料）」https://www5.cao.go.jp/keizai-shimon/kaigi/minutes/2020/0427/agenda.html 2020 年 4 月 27 日

[3] 内閣府 法務省 経済産業省「押印に関する Q&A」https://www.meti.go.jp/covid-19/ouin_qa.html 2020 年 6 月 19 日

[4] 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 2 条 1 項に関する Q&A）」https://www.meti.go.jp/covid-19/denshishomei_qa.html 2020 年 7 月 17 日

電子契約サービスに関するＱ＆Ａ（電子署名法第３条関係）[5]」（以下、「３条 Q&A」という。）が公表されました。これらの文書では昨今民間で利用が拡大しつつある、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（以下、「事業者署名型電子契約サービス」という。）についての電子署名法における定義・解釈が示されました。

本解説は、既に電子契約サービスを利用している方、および利用を検討している方へ向け、先に示された政府の見解に関して、具体的にどのような点に注意するべきかについて解説を述べるものです。現在普及している利用者自身の署名鍵により行う電子署名（以下、「当事者型電子署名」という。）を用いたサービスとは異なり、事業者署名型電子契約サービスは政府の Q&A だけではその内容にわかりにくい部分もあります。本解説では、2 章で「3 条 Q&A」のポイントを示し、3 章以降では、次のような観点から述べています。

３章：電子署名法第３条の推定効が得られるための一般要件
４章：なりすまされるリスクへの対応―利用者の本人確認（身元確認、当人認証）
５章：裁判での立証
６章：当事者型電子署名の利便性向上
７章：事業者型電子契約サービスと当事者型電子署名の比較整理

2.　事業者署名型電子契約サービスの特徴と主務三省の「３条Ｑ＆Ａ」

近年、電子契約サービスの一形態として第三者が提供するインターネット上のサービスを介して当該サービスの利用企業間で取り交わされた契約の事実を証明するサービスが現れました。特徴を以下に述べます。

A)　電子契約サービスへのアクセスや操作を証跡として記録することで利用者（署名者）を特定し、利用者自身による契約であることを操作ログ等に記録
B)　上記 A)にサービス提供事業者の電子署名を付与することで、当該記録が契約以後に、改ざんされていないことを担保

このような事業者署名型電子契約サービスにより作成された電子文書が真正に成立するかについて、2020 年 9 月 4 日に電子署名法主務三省より電子署名法第 3 条の電磁的記録の真正な成立の推定効が働くのか Q&A の形で示されており、以下にその回答の要約を記載します。

「問 1．電子署名法第 3 条における「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。）」とは、どのようなものか。」

【回答要約】

電子署名法第３条が電子文書の成立の真正を推定するという効果を生じさせるものであるため、電子署名が「本人による」ものであることを要件としているのは、**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ものであること**を要求する趣旨である。

[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（電子署名法３条に関する Q&A）」 https://www.meti.go.jp/covid-19/denshishomei3_qa.html 2020 年 9 月 4 日

「問 2．サービス提供事業者が利用者の指示を受けてサービス提供事業者自身の署名鍵による暗号化等を行う電子契約サービスは、電子署名法第 3 条との関係では、どのように位置付けられるのか。」

【回答要約】

上記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には当該サービスが本人でなければ行うことができないものでなければならないこととされている。そのためには当該サービスが以下の①、②について**十分な水準の固有性（固有性の要件＝他人が容易に同一のものを作成することができないこと）**を満たしていることが必要であると考えられる。

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

例えば、利用者が 2 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考えられる。

② 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

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ついて、

・暗号の強度

・利用者毎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、電子文書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満たされていると評価できるものである場合には、固有性の要件を満たすものと考えられる。

個別の事案における具体的な事情を踏まえた裁判所の判断に委ねられるべき事柄ではあるものの、一般論として上記サービスは、①及び②のプロセスのいずれにつ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、電子署名法第 3 条の電子署名に該当するものと認められることとなるものと考えられる。

「問 3」本解説では省略

「問 4．電子契約サービスを選択する際の留意点は何か。」

【回答要約】

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、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各サービスの利用に当たっては、当該各サービスを利用して締結する契約等の重要性の程度や金額といった性質や、**利用者間で必要とする身元確認レベルに応じて、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。

3. 電子署名法第 3 条の推定効が得られるための一般要件

契約は、法令に特別の定めがある場合を除き、口頭でも成り立ちますが（民法 522 条 1 項）、通常は締結の有無やその内容を後から確認できるように契約書を作成します。また民事訴訟時の証拠力（民事訴訟法 228 条 1 項）を確保するために、当事者それぞれが契約書へ押印（同条 4 項）する実務が定着しています。したがって契約を電子化する際にも自署または押印と同等の証拠力を確保することが

実務上重要であり、電子署名法第 3 条の推定効が適用され、裁判実務においても当該電子契約の有効性、すなわち電磁的記録の真正な成立が認められる仕組みが備わっているか否かが、電子契約サービス事業者を選ぶ上で重要な点となります。

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は、電子署名法第 3 条の規定により、その電子文書は真正に成立したものと推定されますが、事業者署名型電子契約サービスがその効果を得るために 3 条 Q&A において要件とされた『十分な水準の固有性』を整理すると以下のようになります。

a. 利用者の身元確認レベルが十分であること。
b. サービス利用時の当人認証レベルが 2 要素による認証等、強固なものであること。
c. サービス提供事業者が自らの署名鍵を用いて行う電子署名の暗号強度が十分なものであり、署名鍵が安全に管理されていること。
d. 利用者毎に行われた処理の個別性を担保する仕組みを備えていること。（例：システム処理が当該利用者に紐付いて適切に行われる）

なお、主務三省のＱ＆Ａでは説明が省略されていますが、サービス提供事業者の公開鍵証明書を発行する際の事業者自身の身元確認も重要で、これは証明書を発行する認証局により実施されます。

次に、事業者署名型電子契約サービスにおける、上記ａ～ｄは、当事者型電子署名ではどのように対応付けられるか比較[6]して以下に記載します。

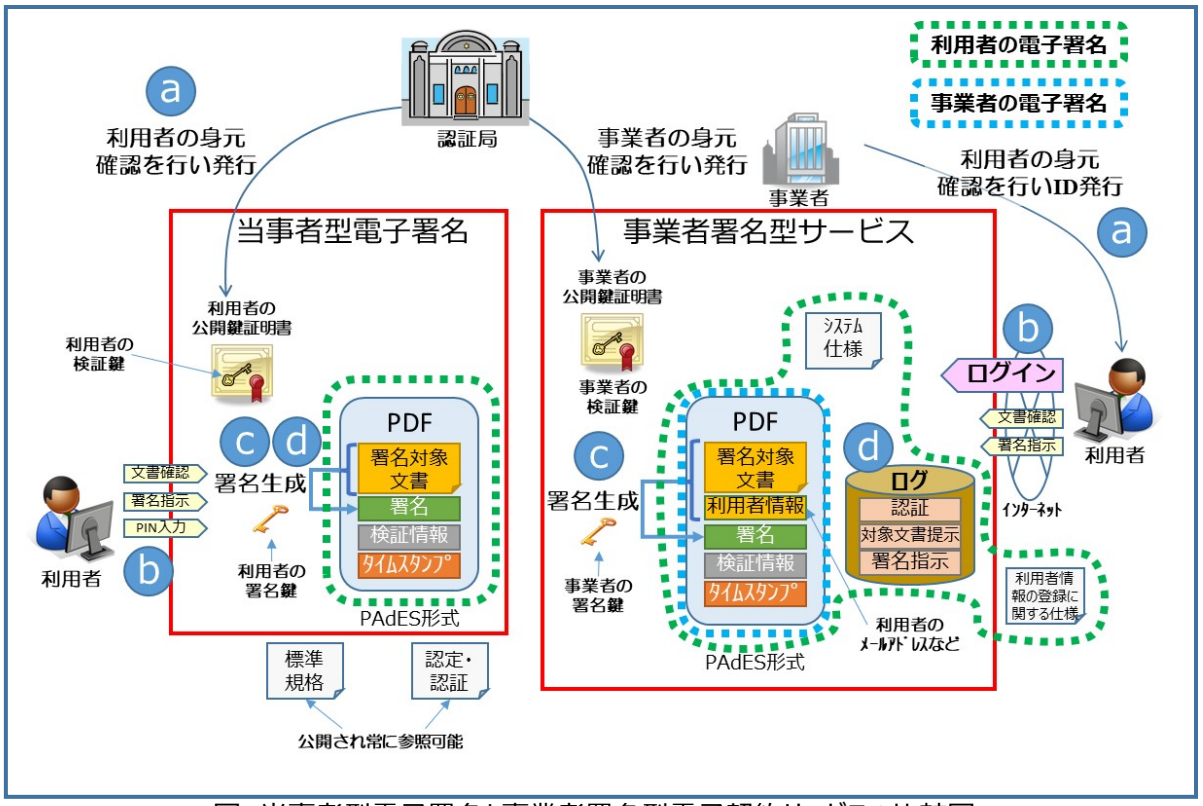

図　当事者型電子署名と事業者署名型電子契約サービスの比較図

[6] JNSA 2019-2020 年度活動報告会（2020 年 11 月 26 日）標準化部会電子署名 WG リーダー　宮崎一哉氏　発表資料より抜粋、一部加筆

当事者型電子署名の場合のａ～ｄは以下のように整理できます。

ａ．利用者の身元確認は認証局の証明書発行ポリシに則り実施される。第三者の準拠性監査や電子署名法の認定により証明。

ｂ．当人認証レベルはローカル署名の場合は「署名鍵の所有」と「本人のみが知りえる PIN の入力」の 2 要素による認証。後述するリモート署名サービスを利用する場合は、本人の署名鍵にアクセスする際に 2 要素認証を実施。

ｃ．署名生成に用いる暗号アルゴリズムの強度や署名鍵の安全な管理に関しては電子署名法の関連法令等で規定。なおリモート署名では署名鍵の安全な管理について ETSI[7]の標準規格[8]で耐タンパーなハードウェアセキュリティモジュールを用いることが定められ、我が国でもリモート署名ガイドライン[9]で同様に規定。

ｄ．利用者毎に行われた処理の個別性を担保する仕組みは、本人の署名鍵を用いて行われる電子署名によって担保され、署名を検証することで確認可能となる。

上記の図では利用者の電子署名を担保するために必要な範囲が緑の点線で示されており、事業者署名型電子契約サービスでは、利用者の電子署名を担保するための範囲が当事者型電子署名より広い範囲に及ぶ事を図示しています。

従って事業者署名型電子契約サービスで電子文書の真正な成立の推定効を得ようとする場合は、広い範囲において**十分な水準の固有性が確保されているかの**検証が必要となると考えられます。特に事業者署名型電子契約サービスのｄ.を証明するためには、当該利用者によってシステムが操作されたことを担保することが必要となり、それを証明するためには以下の対応が必要となると考えられます。

- アクセスや操作ログ等は正しく適切に記録され、それが改ざんや削除ができない仕様となっていること
- 運用担当者の不正ができないようシステム設計、運用設計がなされていること
- 正しく適切に運用されていることが監査等でチェックされていること
- 個別性の証明が必要になった際に、ログや監査等の記録やシステム仕様書等が提出できるよう十分な期間保存しておくこと

利用者は、これらの要件を確認し、締結する契約等の重要性や金額に照らし合わせて、電子契約サービスを選択する必要があります。

4. なりすまされるリスクへの対応―利用者の本人確認（身元確認、当人認証）

3 条 Q&A 問 4 で「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、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」と示されているとおり、その文書に電子署名した人物が文書の作成名義人と同一か否

---

[7] ETSI(European Telecommunications Standards Institute)、欧州電気通信標準化協会。欧州内外の 59 か国が参加する標準化団体

[8] ETSI EN 419 241-1 サーバー署名の一般セキュリティ要求、EN 419 241-2 サーバー署名の QSCD の Protection profile 、EN 419 221-5 TSP の暗号モジュールの Protection Profiles、ETSI TS 119 431-1 リモート QSCD / SCDev のポリシ、など

[9] 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」https://www.jnsa.org/result/jt2a/2020/index.html 2020 年 4 月 30 日

か身元確認が必要となります。例えば電子契約サービスにアカウントを登録する際、身分証等での身元確認を行っていない場合は悪意を持った人物が別の人物になりすまして登録できてしまいます。

経済産業省では「オンラインサービスにおける身元確認に関する研究会[10]」にて身元確認の保証レベルを区分別に整理し、公表しています。電子署名した人物が文書の作成名義人と同一か否かの身元確認においては、保証レベル 2～3 相当の身元確認を行うことが適切と考えられます。身元確認の保証レベルは電子契約サービスごとに異なっており、なりすまされるリスクや、訴訟時の証明の難易度に違いがあるため、利用者は締結する契約等の重要性や金額に照らし合わせて、電子契約サービスを選択する必要があります。

5. 裁判での立証

日本では、電子契約の形式的証拠力が裁判で争われた判例は今のところありません。しかしながら、電子契約の普及に伴って、今後電子契約の真正性について裁判で争われる場面を想定してあらかじめ対応を検討しておくべきです。これまで述べてきた電磁的記録の真正な成立の推定効が電子契約に適用されると裁判での立証が容易となるため、利用する電子契約サービスの選択は大きなポイントとなります。

紙文書の場合、最高裁判例により、印影と本人すなわち作成名義人の印鑑が一致すれば、本人の意思に基づき押印されたことが推定され（1 段目の推定）、民事訴訟法 228 条 4 項により、その押印された文書は真正に成立されたものと推定されます（2 段目の推定）。電子署名の場合、電子署名法第 3 条の要件を満足させれば 2 段目の推定はなされますが、1 段目の推定については紙文書の場合のような判例がまだ存在しません。したがって、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たことを何らかの方法で立証しなくてはなりません。この時、電子契約サービスにおいて身元確認を厳格におこなっていれば、立証の負担も軽減されます。

逆に、自己申告レベルの簡易な身元確認では、なりすまし等が懸念されるため、確かに本人が電子署名を行ったのかどうかという立証のために、他の立証手段を用意しておかねばなりません。この場合、電子契約サービス事業者から各種ログの提供やサポートを受けられるかまで考慮する必要があります。また、その事業者が廃業・倒産した後に立証する必要に迫られる可能性も考えられ、重要な契約については万が一の場合に備えた対策が必要です。

3 条 Q&A で示された電子署名法 3 条の推定に関する要件としては、事業者による身元確認までは必須ではないものの、訴訟における利用者の特定に備えるため身元確認レベルが高い電子署名を用いることは重要です。

6. 当事者型電子署名の利便性向上

当事者型電子署名は、訴訟時の立証などで事業者署名型電子契約サービスよりも優位性があると考えられますが、電子証明書の発行手続きや電子署名の方法が煩雑であるなどの声も聞かれます。これを解消するために、本人確認については公的書類を必要とせずに、マイナンバーカードを使ってオンライン上で申込を完結させることも可能です。また、電子署名の付与方法についても、利用者の署名鍵をサーバー上に置き、遠隔で電子署名を行えるリモート署名についてその要件が整理されつつあります。このような方法で当事者型電子署名を用いれば、信頼性を損なわずに利便性を高めることができます。

---

[10] 経済産業省「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」https://www.meti.go.jp/press/2020/04/20200417002/20200417002.html 2020 年 4 月 17 日

7. 事業者型電子契約サービスと当事者型電子署名との比較整理

事業者署名型電子契約サービスと当事者型電子署名で、前述の電子署名法第 3 条の推定効が得られるための一般要件 a～ｄを証明する仕組みを比較すると、以下のように整理できると考えられます。

	事業者署名型電子契約サービス	当事者型電子署名
a. 利用者の身元確認レベル	・身元確認の標準規程や第三者監査に関する規定は無いが、事業者自身が規定文書を作成し、適切な運用を行っていることを証明。またそれ等の規定、監査記録、本人確認書類の提出が考えられる	・認証局が証明書ポリシ（CP)の規定に従い身元確認、第三者の準拠性監査や電子署名法の認定により証明。またそれ等の規定、監査記録、本人確認書類の提出が考えられる
b. 当人認証レベル	・2 要素以上の認証を行っていることを証明	・署名鍵や PIN を利用者本人が適切に管理していたことを証明 ・リモート署名を利用している場合は当該サービスが 2 要素以上の認証を行っていることを証明
c. 電子署名の暗号強度	・電子署名法の関連法令等や電子政府推奨暗号リスト（CRYPTREC）で指定	・電子署名法の関連法令等や電子政府推奨暗号リスト（CRYPTREC）で指定
d. 利用者毎の個別性	・アクセスや操作ログ等は正しく適切に記録され、それが改ざんや削除ができない仕様となっていること ・運用担当者の不正ができないようシステム設計、運用設計がなされていること ・正しく適切に運用されていることが監査等でチェックされていること ・ログや監査等の記録、システム仕様書等は証明が必要な際に提出ができるよう必要な期間保存しておくこと	・PKI 技術標準に従って署名検証により電子署名の有効性を証明

当事者型電子署名の場合は、多数の PKI 技術標準や前述の ETSI の標準規格が用意されており、当該規格等への準拠性監査、署名検証などを通じて、電磁的記録の真正な成立の立証方法が明らかになっています。一方、事業者署名型電子契約サービスの場合は、標準規格や監査制度が揃っているわけではなく上記相当の事項につき独自の規定や監査等で適切に運用を行っていたことを証明することが必要となります。

8.　まとめ

契約書は、当事者間の合意内容を明示しその証拠力を高めるために作成するものです。オンラインでの電子契約締結には「事業者署名型電子契約サービス」、「当事者型電子署名」を問わず、内容の重要性に応じた本人確認が求められます。また、クラウドサービスを利用する場合、「事業者署名型電子契約サービス」、「当事者型リモート署名サービス」を問わず 2 要素以上の認証による本人確認が必要となります。

契約書は簡単かつスピーディーに証拠として提出できることが肝要だと考えます。当事者型の電子署名には、当事者名の電子署名が付されているため、契約書のファイルを提出するだけで証拠の提示が可能です。さらに認定認証局による電子証明書であれば、証明書発行時に厳格な身元確認が行われているため、契約者本人が署名したかどうかの争いを容易に回避可能になると考えられます。

今回政府から、押印に関する Q&A、事業者署名型の電子契約サービスに対する電子署名法 2 条、3 条に関する Q&A が示されましたが、最終的には利用者間にて契約の性質や金額、重要性に応じた電子署名サービスの選択が求められます。本解説が電子契約サービスを選定する上での皆様の理解の一助となり、ひいては健全なトラストサービスの発展に貢献できましたら幸いです。

以上

問合先：事務局

- トラストサービス推進フォーラム
  Mail：tsf@dekyo.or.jp
- 電子認証局会議
  Mail：info@c-a-c.jp