電子契約活用ガイドライン

2021 年 10 月　Ver.2.0

公益社団法人　日本文書情報マネジメント協会（ＪＩＩMA）

電子取引委員会

はじめに

急速に立ち上がってきた電子契約市場においてさまざまな電子契約サービスが出現する中で、日本文書情報マネジメント協会（以下、JIIMA）の電子契約委員会（現、電子取引委員会）では2019年５月に「電子契約活用ガイドラインVer.1.0」を作成公開しました。2020年４月（JIIMA第60期）に入り、日本でも新型コロナウイルスの感染拡大による第１回目の緊急事態宣言が発出され、コロナ禍において押印のための出社が社会的な問題となりました。結果、内閣府の規制改革推進会議においてリモートワーク推進の必要から書面規制、押印、対面規制についての見直しが進みました。そのようなデジタル社会の推進に向けた社会環境の急速な変化の中、電子契約に係るトラストサービスの国内外の動向にも急速な変化があり、本ガイドラインの内容を更新することといたしました。

本ガイドラインでは、これから電子契約を導入しようと検討する企業や、すでに活用し始めている企業が安心して活用でき、一層の利用促進につながることを目的としています。本書では電子契約とはどのようなものか、必要となる電子署名などの基礎的な技術や電子署名法などの関連法令、導入に際して留意すべき点、訴訟対応など導入検討や安定した運用を行う上で参考となると思われる内容をまとめました。また電子契約に係るトラストサービスにおける国内外の動向についても合わせて解説いたしました。電子契約の導入や利用拡張をご検討されている皆様の参考の一助になれば幸いです。

目次

1.電子契約とは

1-1. 本書で定義する電子契約とは

インターネットが普及し電子的な手段を用いた商取引は、もはや商業活動において切り離せない要素となっています。商品・サービスの宣伝やマーケティング、契約、売買、製品の受発注や出荷、請求や決済などを電子的なネットワークを利用して行う商業活動は様々な分野で広がっています。広義で、このような取引の手段を電子取引といいます。

国税庁では、電子取引の範囲を、取引情報が電磁的記録の授受によって行われるすべての取引と定義しています[1]。

> 【参考】　電子帳簿保存法取扱通達２－２
> 法第２条第５号（(電子取引の意義)）に規定する「電子取引」には、取引情報が電磁的記録の授受によって行われる取引は通信手段を問わず全て該当するのであるから、例えば、次のような取引も、これに含まれることに留意する。
> (1) いわゆるＥＤＩ取引
> (2) インターネット等による取引
> (3) 電子メールにより取引情報を授受する取引（添付ファイルによる場合を含む。）
> (4) インターネット上にサイトを設け、当該サイトを通じて取引情報を授受する取引

取引情報とは見積書、注文書、契約書、納品書、請求書、領収書、送り状などの書類に通常記載されるような事項を指し、商業活動の中では、用途に合わせて様々な様式で作成され当事者を介して授受されています。

電子取引の広がりとあわせて、電子文書のやり取りだけで契約を締結する方法、いわゆる電子契約といった手段が広がっています。いままで一般的な企業間の契約では、裁判における証拠性や、各種法令を遵守するため、書面に署名捺印を行った紙の契約書を用いて合意し、それを契約当事者双方で保管してきました。

一方、本書で定義する電子契約とは、以下です

> 電子的に作成した契約書を、インターネットなどの通信回線を用いて契約の相手方へ開示し、契約内容への合意の意思表示として、電子署名法２条１項の電子署名を付与することにより契約の締結を行うもの。

契約条件という取引情報を電子的に授受する手段となるため、電子契約は電子取引に含まれる手段の一つといえます。

---

[1] https://www.nta.go.jp/law/tsutatsu/kobetsu/sonota/030628/pdf/01.pdf

電子契約では、書面への手書き署名や押印に代え、電子文書へ「電子署名」や「電子サイン」が付されます。詳しくは後述いたしますが、それらには認証方法や技術に違いがあります。

一般的には、「電子サイン」はサインを行う際に第三者認証までは行わないため導入しやすく、電磁的記録（電子文書等）の確認や承認などのプロセスで幅広く利用される傾向があり、「電子署名」は、第三者による本人認証や高度な暗号技術要素が加わるため、重要性の高い厳格な契約の締結で利用される傾向があります。

わが国では、「電子署名及び認証業務に関する法律」（いわゆる電子署名法）があり、電磁的記録（電子文書等）に本人の電子署名を付与することにより、書面に手書き署名や押印を付した場合と同等の法的効力が得られるよう法整備がされています。

厳格な契約締結時に「電子署名」を使うのは、電子署名に押印と同等の法的効力を期待するからです。その法的根拠は、電子署名法第３条「・・・本人による電子署名（・・・）が行われているときは、真正 に成立したものと推定する。」という条文にあります。この条文を簡単に説明すると、「一定の要件を満たした本人の電子署名がある文書（電子ファイル）は、真正に成立した（＝本人の意思により作成され、改ざんがない）ことが法律により推定される」ということです。

訴訟において契約の成立が争われた場合、その契約書の「成立の真正」を挙証者（通常は提出側）が立証する必要があります。しかし電子文書の場合、実際にその「成立の真正」の証明は簡単ではありません。そこで、適切な電子署名があるだけで、電子契約書が偽造ではなく、署名した本人の意思により作成され、改ざんがないという推定が受けられる署名法第３条は、契約を取り交わすものにとって大変便利なものなのです。

業界や業務によって様々な法令や規則がありますが、契約書の締結を電子契約で行う場合は前述の電子署名法に定める要件を求めるものもあることから、国内においては法的な有効性をもって立証するためには「電子署名」による電子契約が有効であるといえます。

取引に利用される書類の性質	取引に利用される書類	電子署名	電子サイン
契約当事者双方の意思や合意を確認するもの	契約書	◎	△
⇕	注文書、注文請書	○	○
契約を行う相手側へ証跡の意味合いで通知するもの	見積書、請求書、納品書、領収書	△	◎

表 1　取引書類の性質と締結方法

1-2. 電子化に向けた動向

実際の国内における電子契約の活用状況にも目を向けてみましょう。

建設産業は、国民総生産の約１３％に相当し、全産業就業人口１０％を擁する基幹産業です。この建設産業は、工事目的物毎に、様々な業種の建設業者がその都度協働する産業であり、そのために多数の建設業者間で交わされる契約等取引も膨大であることから、ＩＴ化の進展は重要なテーマとなっていました。

そういった背景の中、1990 年代の後半には工事業者間での調達業務を電子化する仕組みが運用され始めましたが、当時は建設業法の兼ね合いで、工事請負契約書は書面での保存が義務づけられており、完全な電子化までは進んでおりませんでした。

2001 年 4 月に書面一括法が成立したことで、さまざまな法律で書面の電子化に向けた規制緩和が行われました。

これにより、2002 年には、建設産業は他産業に先駆けて、電子署名による契約システムが稼動を開始し、工事請負契約書をはじめ注文書、注文請書の電子化により関係法人間ではコスト削減や業務効率の向上をはじめとするメリットを享受しています。

近年では、ＢtoＢ（企業間）だけでなくＢtoＣ（企業対個人）に及ぶ範囲でも電子契約の活用が広がっています。例えば、個人向け住宅ローンを提供する金融機関でも活用されています。住宅ローンの借入人は、金融機関が提供する電子契約サービスを利用することで、場所や時間の制約を受けることなく、ＰＣやスマートフォンを使って、簡単にローン契約手続を行うことができるようになりました。

また、2020 年から日本でも急激に拡大した新型コロナウイルスの感染予防対策として、リモートワークの導入が進む中、その阻害要因として浮かび上がったのが「紙と印鑑」による従来の業務フローでした。これを受け、政府も「押印についてのＱ＆Ａ」（令和２年６月 19 日、内閣府・法務省・経済産業省）[2]、「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）」（令和２年７月 17 日、総務省・法務省・経済産業省）[3]、「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）」（令和２年９月４日、総務省・法務省・経済産業省）[4]を立て続けに発表されました。

[2] https://www.meti.go.jp/covid-19/ouin_qa.html
[3] https://www.meti.go.jp/covid-19/denshishomei_qa.html
[4] https://www.meti.go.jp/covid-19/denshishomei3_qa.html

一般財団法人日本情報経済社会推進協会（JIPDEC）が実施した最近の調査においても、企業が重視する経営課題の上位に「業務プロセスの効率化」や「従業員の働き方改革」が挙がっており、企業の間においても非常に関心が高まっているテーマとなっています。

このような背景と関連して、様々な分野において紙ベースで行っている業務をデジタル化しようとする動きも進展してきており、契約業務の電子化もその一つとなっています。2020 年の前述の JIPDEC の調査でも、調査対象企業の４３．３％と半数近い企業が電子契約を活用しているとの結果が出ています。

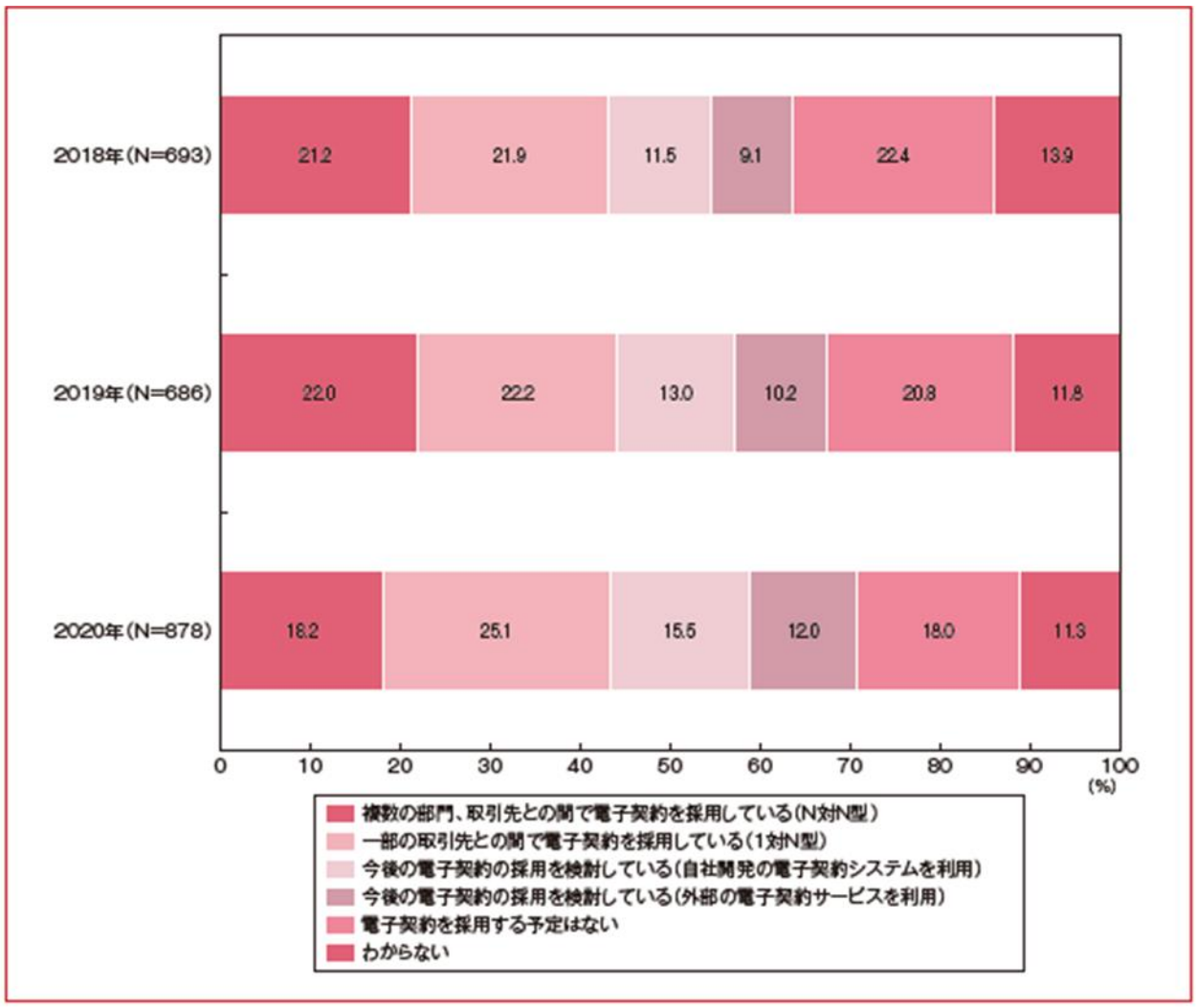

図 1　電子契約の利用状況の経年比較　（2018 年～2020 年調査）

出典：一般財団法人日本情報経済社会推進協会「企業 IT　利活用動向調査 2017」にみる IT 化の現状より（JIPDEC／ITR「IT-REPORT 2020 Spring」）

1-3. 電子契約の社会的意義

公益社団法人日本文書情報マネジメント協会（JIIMA）では、「日本のあらゆる組織の価値を高めるために、文書情報マネジメントの実践を通じてＤＸを加速するようにリードする協会」という「JIIMA ビジョン 2020」[5]を掲げて活動しています。その中で、組織間に跨る文書情報マネジメントとして、文書情報の信頼性を担保することが課題であり、真のデジタル社会を実現するには実務的にそこまでを対象とする必要があるとしています。
本ガイドラインでは次章より、「電子署名」による電子契約で作成される電子文書が、いかに安心で信頼性の高いものであるかを細かく解説していきます。

電子契約の活用は、書面による契約に比べ、労力、経費の削減や手続きに要する時間の短縮が図られるだけでなく、契約の適正化の促進、取引の活性化につながります。さらには旧態依然とした古い業界構造からの脱却、透明性・競争性の向上、それらによる新しい技術とアイデア豊富な優れた企業が成長する健全な市場環境を作り出すチャンスが期待できます。

●電子契約のメリット

① 業務の効率化
電子契約に変わることで契約締結プロセスにある煩雑な業務が効率化できます。例えば、契約書の印刷、製本、封入、投函、郵送、捺印、保管、進捗管理、督促などの作業が大幅に減少し、契約スピードの向上と人的工数の削減が期待できます。

② 管理性の向上
膨大な数の契約を簡単に検索・閲覧・共有できることから、契約進捗管理、契約文書管理におけるコンプライアンスを強化することが可能となります。また、複数の堅牢なサーバーでデータを管理、バックアップが実現できるため BCP 対策にも有効な手段といえます。

③ コスト削減
コスト削減のうちメリットが大きいものとして印紙税の削減があげられます。多額の印紙が必要となる契約を行っている企業にとっては、電子契約を採用することで、すぐに大幅な節税効果が実現できます。さらに、契約書の印刷、製本、郵送にかかわる費用が削減でき、ペーパーレス化と合わせてコスト削減効果は非常に大きなものとなります。

【参考】　印紙税について
印紙を貼る必要があるのは、印紙税法第２条に規定されている契約書などの課税対象となる文書（課税文書といいます）を書面（紙の文書）で作成した場合で、書面

[5] https://www.jiima.or.jp/wp-content/uploads/about/vision2020.pdf

の種類と記載されている金額に応じて、定められた金額の印紙を貼ることで納税する仕組みです。電子ファイルで作成される電子契約はこの「課税文書」にあたらないので、印紙税対象外と考えられています。
国会における総理大臣の答弁でも課税はされないと回答されています。
（参照：内閣参質１６２第９号　五について）

インターネットを巡る環境変化は急速であり、今後も一層の拡大が予想される市場環境のなかで、電子契約は誰もが安心して活用できるものでなくてはなりません。将来にわたって信頼できるための要件を満たした電子契約サービスとはどのようなものか、信頼・安心につながる要件を明らかにし、それらをしっかり認識して活用することが社会生産性の高い電子文書情報社会の構築に必要となると考えられます。

1-4. 電子契約を取り巻く法律について

導入の前提となる法令面について、検討すべき主なポイントを紹介します。

(1) 民事訴訟における証拠力（電子署名による契約の法的有効性）

電子契約でとりかわされた契約も、紙の契約書と同様に、万一の係争時には裁判上の証拠となることが、最低限必要です。

民事裁判に文書を証拠として提出する場合、提出者はその文書が真正に成立したこと（署名者本人が自分の意思で作成したこと、偽造ではないこと）を証明する必要があります（**民事訴訟法**第２２８条第１項）。これはその文書が電子データであっても同様です（同法第２３１条）。

紙の契約書に本人の署名や押印があれば、その文書が真正に成立したことが推定されます（同法第２２８条第４項）。紙の契約書に署名や押印をおこなうのは、この推定を得て、係争時の証明の負担を軽減させるためといえます。

同様に電子データの文書の場合、適切な電子署名（「本人による一定の条件を満たす電子署名」）があれば、本人の手書き署名・押印がある文書と同じように真正に成立したことが推定されます（**電子署名法**第３条）。ですから電子署名は強い証拠力をもつわけです。本人の電子署名がない場合、操作ログ、タイムスタンプなど様々な証拠から成立の真正性を証明する必要が生じます。

なお、1-2. で触れたように、2020 年に電子署名法の主務三省から電子署名法第２条と第３条に関するＱ＆Ａとして新たな解釈・見解が示されました。

- 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（電子署名法２条１項に関するＱ＆Ａ）
- 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）

これらの解釈・見解により、従来の電子署名（本書では「当事者型電子署名」と定義します）に加えてリモート署名や「事業者型電子署名」[6]といった電子署名の様々な形態が電子署名法の枠組みの中で認められるようになりました。なお主務三省Ｑ＆Ａ２点に関しては、トラストサービス推進フォーラムと電子認証局会議による「主務三省Ｑ＆Ａ（電子署名法

[6] 主務三省Ｑ＆Ａ２点におけるサービス提供事業者による電子署名を「事業者型電子署名」と定義します。なお、事業者型電子署名は立会人型電子署名と呼ばれることがありますが本書では事業者型電子署名に統一しています。

第３条関係）に関する解説」が参考となります[7] 。リモート署名や事業者型電子署名に関しては本書の中で説明しています。

(2) 税法への対応

紙の見積書、注文書、注文請書、納品書、請求書、契約書等は、国税関係書類として、法人税法等により、保存義務があり、税務調査時に調査官に要求されたら提示する必要があります。

同様に、電子契約の場合は、**電子帳簿保存法**[8]で定める要件に従い、取引情報を保存する必要があります。電子帳簿保存法（以下、電帳法という）は、同法第１条（趣旨）に規定されている通り、納税者の国税関係帳簿書類保存方法についての特例を定めた法律です。電帳法は、法人税法や所得税法などの税法の定めにより、紙保存が原則となる国税関係帳簿書類を、一定の要件満たす事により電磁的記録やマイクロフィルム（ＣＯＭ） による保存を容認し、第４条で国税関係帳簿書類の電磁的記録の保存等について規定しています。一方、電帳法第７条（旧第１０条）は帳簿書類の保存方法の特例の規定ではなく、電帳法施行前に保存義務がなかった電子取引に係る電磁的記録を保存しなければならないとし、2005 年の改訂時に新たに加えられた規定です。

電帳法第７条で所得税及び法人税に係る取引情報記録の保存が規定されている電子取引は、次のように定義されています。

「取引情報（取引に関して受領し、又は交付する注文書、契約書、送り状、領収書、見積書その他これらに準ずる類に通常記載される事項をいう。）の授受を電磁的方法により行う取引をいう」

すなわち、インターネットなどを利用し取引先との間で情報をやりとりした場合は、電子取引の取引情報に係る電磁的記録の保存として規定されている、電帳法施行規則[9]第４条第１項（旧第８条第１項）の要件に従って保存する義務が生じるということとなります。表２にその要件内容を整理します。

なお、この電子取引に係る規定は、令和３年（2021年）の法改正で、法旧第１０条において容認されていた書面またはマイクロフィルム（ＣＯＭ）での保存が廃止され、取引情報の隠蔽、又は仮装された事実があった場合には、その事実に関し生じた申告漏れ等に課される重加算税が１０％加重される措置が整備されました。

---

7 https://www.dekyo.or.jp/tsf/wp-content/uploads/2021/02/電子署名法Q&Aに関する解説.pdf

8 本書では令和４年１月１日施行の条文に基づきます。

9 本書では令和４年１月１日施行の条文に基づきます。

法令等の項目	分類	項目・概要
施行規則第４条第１項	保存場所	事業所在地、又は納税地
	保存期間	７年間
	保存要件	① 関係書類の備え付け 施行規則第２条第２項第１号イ
		② 見読性の確保 施行規則第２条第２項第２号
		③ 検索機能の確保 施行規則第２条第６項第６号
	保存上の措置	下記措置のいずれか ① 送信側のタイムスタンプ ② 受信側でのタイムスタンプ付与および保存する者の情報 ③ 訂正・削除できない、もしくは訂正・削除の事実・内容を確認できるシステムを使用して授受・保存 ④ 訂正・削除防止規程での運用
取扱通達７－１	保存方法詳細	保存すべき取引情報
取扱通達７－８	その他	ファクシミリの取り扱い

表 2　電帳法の電子取引情報保存要件

※詳細は JIIMA HP にて公開中の「電子取引 取引情報保存ガイドライン Ver2.00」を参照することにより、関連性の理解が深まります。

(3) 契約シーンに応じて注意が必要な法令

- 電子契約法

電子契約法は正式名称を「電子消費者契約及び電子承諾通知に関する民法の特例に関する法律」といい、電子商取引における消費者の操作ミスの救済と、電子商取引における契約の成立時期の転換で構成されています。

ＢtoＣ（企業対個人）で契約を取り交わす場合、個人がうっかりミスにより契約を取り交わしてしまった場合、契約を無効にできることを定めた法律となるため、電子契約の利用範囲がＢtoＣの場合は、操作ミスではなく本人の契約の意思表示が明確にできる仕組みとなっていることが重要です。

- 電子委任状の普及の促進に関する法律（電子委任状法）

契約行為の中でかなりの割合を占める企業間で取り交わす書面の契約書においては、そ

れぞれの企業の代表者等が署名し、代表者印や会社印を押印するのが通常です。しかし、代表者自身が直接署名・押印するケースは少なく、組織の担当者が稟議承認等を得た後に、法務・管理部門が代表者に代わって署名・押印し、契約書を作成するのが実状といえましょう。このような日本の商習慣を踏まえて、実態に合わせて電子契約を行うための法令も整備されています。

この法律は、電子的な手続において、法人の使用人等が手続を行う権限を当該法人の代表者から委任されていることを証明するための電磁的記録である「電子委任状」の基本指針と、それら法人等の委託を受けて電子委任状を保管し、関係者に提示等する「電子委任状取扱業務」の認定制度について定めた法律です。

例えば、電子委任状を利用して社員等に代理権を付与したことを電子的に証明することができれば、社員等の代表者以外でも電子契約を締結することができるようになる、ということです。実務に即していることから、電子契約が更に身近なものとなると想像されます。主に行政における電子申請や企業間における電子商取引で利用され、ネットワークを利用した経済活動のデジタル化促進が期待されています。

- 地方自治法施行規則 第１２条の４の２

地方自治体との契約シーンで電子署名をおこなう場合、これまでは地方自治法施行規則第１２条の４の２において、電子署名法に基づく特定認証業務の認定事業者による厳格な本人確認により発行された電子証明書などが必要でしたが、2021 年 1 月 29 日付の同規則の改正により、電子署名法第２条第１項に規定する電子署名とされました。

(4) その他関連する法令

法令上の文言に「書面で交付する」「書面で保存する」とある場合、この「書面」は紙を意味しています。しかし、多くの場合法律の同条の次項などに、「電磁的措置」「電子情報処理組織を使用する方法その他の情報通信の技術を利用する方法」などの表現で**一定の要件のもと電子的な交付や保存を認める条文があります。この場合この要件を満たすことにより、電子契約が可能になります。**例えば以下がその例です。

【法律に書面で交付等が記載されているが電子契約が認められる例】

- 下請法（下請代金支払遅延等防止法）第３条（書面の交付等）

第１項　「親事業者は（中略）その他の事項を記載した書面を下請事業者に交付しなければならない。」

第２項　「(前略) 前項の規定による書面の交付に代えて、(中略) 電子情報処理組織を使用する方法その他の情報通信の技術を利用する方法であつて公正取引

委員会規則で定めるものにより提供することができる。この場合において、当該親事業者は、当該書面を交付したものとみなす。」

- 建設業法第１９条（建設工事の請負契約の内容）
  - 第１項　「建設工事の請負契約の当事者は、・（中略）・次に掲げる事項を書面に記載し、署名又は記名押印をして相互に交付しなければならない。」
  - 第３項　「（前略）前二項の規定による措置に代えて、（中略）電子情報処理組織を使用する方法その他の情報通信の技術を利用する方法であつて、当該各項の規定による措置に準ずるものとして国土交通省令で定めるものを講ずることができる。この場合において、当該国土交通省令で定める措置を講じた者は、当該各項の規定による措置を講じたものとみなす。」

- 民法第４４６条（保証人の責任等）
  - 第２項　「保証契約は、書面でしなければ、その効力を生じない。」
  - 第３項　「保証契約がその内容を記録した電磁的記録（中略）によってされたときは、その保証契約は、書面によってされたものとみなして、前項の規定を適用する。」

- 借地借家法第２２条（定期借地権）
  - 第１項　「その特約は、公正証書による等書面によってしなければならない。」
  - 第２項　「前項前段の特約がその内容を記録した電磁的記録（中略）によってされたときは、その特約は、書面によってされたものとみなして、前項後段の規定を適用する。」

- 借地借家法第３８条（定期建物賃貸借）
  - 第１項　「公正証書による等書面によって契約をするときに限り、第三十条の規定にかかわらず、契約の更新がないこととする旨を定めることができる。」
  - 第２項　「前項の規定による建物の賃貸借の契約がその内容を記録した電磁的記録によってされたときは、その契約は、書面によってされたものとみなして、同項の規定を適用する。」

- 借地借家法第３９条（取壊し予定の建物の賃貸借）
  - 第２項　「前項の特約は、同項の建物を取り壊すべき事由を記載した書面によってしなければならない。」

第３項　「第一項の特約がその内容及び前項に規定する事由を記録した電磁的記録によってされたときは、その特約は、同項の書面によってされたものとみなして、同項の規定を適用する。」

このように、法令に「書面交付」「書面保存」の規定があり、「情報通信の技術を利用する方法」などへの言及がない場合、紙が要件となるため、電子契約は法令上認められません。

基本的に、契約は当事者同士が合意をすれば成立します。しかし、契約方式自由の原則の例外として、下記に示す契約は、書面の作成が契約の成立要件となっているものや、義務付けられている契約となります。
（「書面」の電子化は経済界や産業界の動向に合わせて運用の見直しが進められており、実務にあたっては関係省庁の確認が必要です。）

【書面作成が契約の成立要件となる契約の一例】

①　任意後見契約（任意後見契約に関する法律第３条）
任意後見契約は、法務省令で定める様式の公正証書によらなければなりません。

②　事業用定期借地権設定契約（借地借家法第２３条第３項）
専ら事業のために使用する建物を所有する目的で、契約の更新や建物の買い取りが認められず、契約期間が満了すると確実に土地を明け渡さなければならない借地権の設定契約は、公正証書によらなければなりません。

【書面作成が法律で義務付けられている契約の一例】

①　農地の賃貸借契約（農地法第２１条）
農地又は採草放牧地の賃貸借契約については、契約存続期間、借賃等の額及び支払条件、その他の契約内容を書面により明らかにしなければなりません。

②　割賦販売法に定める指定商品ついての月賦販売契約（割賦販売法第４条）
割賦販売法に定める指定商品について割賦販売契約結ぶときは、売主から買主に対して、割賦販売価格、商品の引渡時期等を記載した書面を交付しなければなりません。

③　宅地建物取引業法（第３４条、第３５条、第３７条）
宅建業者は、売買又は交換の媒介契約を締結したら遅滞なく必要事項を記載した書

面（通称、第３４条の２書面）を作成し、記名押印して依頼者に交付しなければなりません。また、宅建業者の関わる宅地建物取引では法定の事項を記入した契約書（業界用語で３７条書面という）を作成しなければなりません。ただし、令和３年にデジタル改革関連法が成立し、その中に含まれる宅地建物取引業法が改正されることが決まりました（公布から１年以内に施行される)。本改正によりＩＴ重要事項説明や不動産の各種契約においての電子化が可能となります。

2. 電子契約に求められる電子署名について

本書では、電子署名の主務三省 Q&A に合わせ、電子証明書に紐づく秘密鍵を電子署名で使用する場合に署名鍵と呼ぶこととし、必要に応じて秘密鍵と署名鍵を使い分けています。

2-1. 電子文書（電磁的記録）の種類や電子署名の方式

電磁的記録は、電子帳簿保存法第２条では「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」と定義され、電子計算機(コンピュータ)で処理可能なデジタルデータを指します。（注：法律によっては電子的方式、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」と定義され、ビデオテープやカセットテープなどのアナログデータが含まれる場合もあります。）

デジタルデータの書面を作成するには、Word、Excel、PowerPoint 等お馴染みの方法がありますが、デジタルデータの書面を電子契約書として用いるには、誰と誰がいつ取交したのか、契約締結時だけでなく後々からも確認できるように対処しておくことが必要です。具体的には、誰と誰が契約を取交したのかを明らかにすると共に改ざんされた場合には検知できる様に電子証明書を用いて電子署名を行うこと、いつ取交したのかを明らかにする為にタイムスタンプを付与することが上げられます。（電子証明書、電子署名、タイムスタンプについては後の項で記述します。）

また、電子契約書が取交されて以降長期にわたり必要に応じて「誰と誰が」及び「いつ」について確認できる様、電子契約書への電子署名やタイムスタンプのフォーマットを規定した標準規格（長期署名フォーマット）もあります。代表的な標準規格として、CAdES、XAdES、PAdES、ASiC が上げられます。

CAdES（CMS Advanced Electronic Signatures）はバイナリーデータ形式の電子署名フォーマット規格、XAdES（XML Advanced Electronic Signatures）は XML 形式の電子署名フォーマット規格で、アプリケーションを開発する際に参照されます。この２つの規格のもとでは、署名対象データと電子署名を分けて扱うこともあり、様々なアプリケーションでの実装の差異により電子署名された文書の見え方や電子署名、タイムスタンプの確認（検証）が必ずしも一様とならない場合もあります。

PAdES（PDF Advanced Electronic Signatures）は、PDF 文書自体に電子署名やタイムスタンプを組込むものとして、フォーマットについて規定されており、PDF 文書に対する一般的

な認知が進んできていることやAdobe Reader等の普及が進んでいるアプリケーションで電子署名やタイムスタンプの検証や可視化が可能になっていることから、PAdESに準拠して電子契約書が作成されるケースが増えてきているのが現状です。
また、最近の動きとしては、ASiC（Associated Signature Containers）という署名対象データ、電子署名、タイムスタンプ、その他関連する複数の電子データを一つにパッケージングするフォーマットの規格化をETSI等が進めています。

2-2. 電子証明書の役割

1960 年代から発達した「公開鍵暗号基盤」（PKI=Public Key Infrastructure）は、インターネット社会に潜む、盗聴、なりすまし、改ざんなどのリスクを防ぐために有効な技術として現在世界的に普及しています。電子契約を取り交わす当事者は、この PKI 技術を使った仕組みのもとで、自身の電子署名が正しいものであることを相手や第三者に対して証明できるようになります。電子契約の世界では、紙の契約書における印章や印鑑証明書に相当するのは、PKI 技術における秘密鍵と電子証明書です。本人がこれらを所持し、使用することで、安全で確実な電子契約を取り交わすことができるようになります。また、万が一、係争に発展するような事態になったとしても電子署名法によって、本人の電子証明書による電子署名が付与されている場合には真正な成立が推定され、押印された紙の書面と同様の証拠力を持つことになります。ここで電子証明書とは、本人の秘密鍵とペアをなす公開鍵を第三者機関（認証局と呼びます）が審査し、発行する電子データで、より正確には公開鍵電子証明書と言われます。個人の電子証明書には主に以下の内容が記載されます。

- 本人の氏名
- 本人の所属情報（会社名や部署名など）
- 本人の公開鍵データ
- 電子証明書の有効期間開始日と終了日（有効期間は通常１年～３年）
- 電子証明書の発行番号（シリアル番号とも言う）
- 電子証明書に使用する暗号の種類
- 認証局の名前
- 認証局の署名（認証局の秘密鍵による電子証明書全体の電子署名）

電子契約を取り交わす上で、どの認証局から発行された電子証明書を用いて電子署名をおこなうかが重要となってきます。すなわち、電子契約の当事者は、厳正な本人確認をした上で電子証明書を発行する認証局を発行先として選ぶ必要があります。そうでなければ、係争時に電子署名の有効性を疑われることになりかねません。表３は国内における主な認証局の種類です。一般的な電子契約では、認定認証業務対応認証局または特定認証業務対応認証局の証明書を選択すればよいでしょう。なお、現状は PDF ファイルフォーマット化した電子文書が多くを占めるため、さらに AATL 対応認証局であれば、電子署名をチェック（署名検証）する際のユーザー利便性が向上します。

認証局種別	概要
公的個人認証（JPKI）	公的個人認証法に従って、地方公共団体情報システム機構（J-LIS）が運営する認証局。国民または日本に住所を持つ外国人の希望者に対して電子証明書を無償で発行。マイナンバーカードの IC チップ内に格納する。電子署名に利用する署名用電子証明書と、システムログインの認証などに利用する利用者証明用電子証明書の 2 種類がある。
商業登記に基づく電子認証制度	登記所に商業登録された企業や法人の登記情報に基づいて、登記所が運営する認証局。企業・法人の代表者に電子証明書を発行する。
認定認証業務対応認証局	電子署名法で規定している設備や業務方法の基準に適合し、主務大臣（総務大臣、法務大臣、経済産業大臣）の認定を受けた認証局。2021 年 9 月現在、民間企業による 9 の認証局が認定を受けている。
特定認証業務対応認証局	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民間認証局。認証局の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。
AATL 対応認証局	AATL とは、Adobe Approved Trust List の略称で Adobe 社が認可した認証局。WebTrust 認定、ETSI 認定、または、ISO 21188 を取得している必要がある。 ※　本認証局は、Adobe 社の Adobe Acrobat または Reader ソフトウェアで信頼された認証局と認識されるので、発行した電子証明書を利用した電子署名の検証を簡単に実施できる

表 3　認証局の種類

ルート認証局と中間認証局の二階層構造をとる認証局構成例を図で示します。ここでは、登録局が発行審査をおこない、発行が承認されたら中間認証局から個人の電子証明書を発行しています。

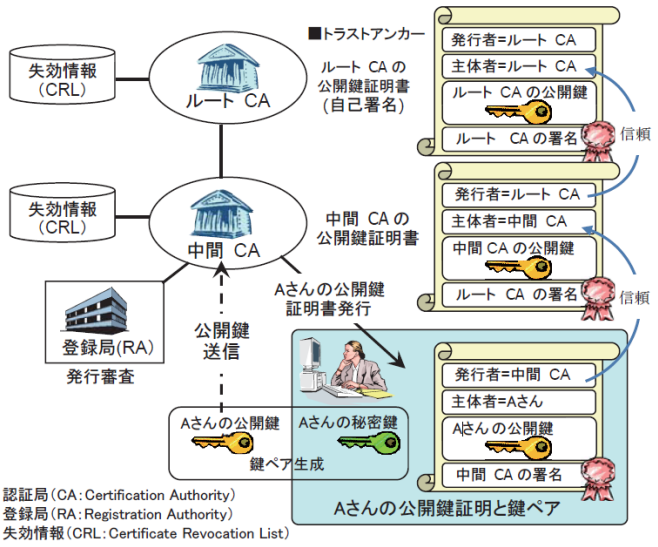

図 2　認証局の構成例

2-3. 電子署名の役割

電子署名とは、紙の契約書に対してハンコを押す行為、すなわち押印と同等の行為を電子的に行う処理となります。押印という行為では紙の契約書にハンコを押し印影という結果が残りますが、電子署名では電子証明書の秘密鍵を利用して署名データという形で電子的な結果が残ります。また、その結果が正しいかを確認する場面では、紙の契約書では実際の印影を重ねたり、透かしたり等、目視で確認しますが、電子署名の確認では署名検証という電子的な手段によって簡単・確実に確認出来ます。この署名検証によって、その電子文書に対して誰が？どのような内容？（本人性や非改ざん性）について、電子署名を行ったかを確認可能となります。

電子署名に用いる署名鍵は、契約者が唯一の所有者となる仕組みが必要です。電子データで秘密鍵がコピーできる状態や、誰でもアクセスできる状態では電子署名の信頼性はなくなります。

２者間での電子契約を行う際には、契約者それぞれが同一の電子文書に対して電子署名を行う事で契約内容の合意を行う事が可能になります。ただし、電子署名された電子文書には、紙の契約書とは異なり、いつまで有効か？という時間の概念があります。この有効期間は、電子署名に利用した電子証明書の有効期間と同一なります。（電子署名に利用した電子証明書の有効期間を過ぎると電子署名の有効性が確認できなくなります。通常電子証明書の有効期間は５年以内です。）電子署名の有効性を確認できる期間を延長するために、後述するタイムスタンプが必要になります。

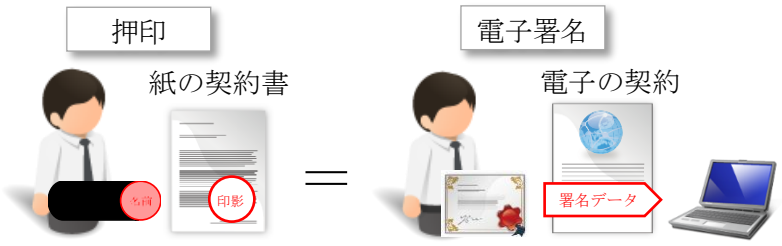

図 3　電子署名の役割

	書面契約	電子契約
誰が	契約者本人	契約者本人
何で	印章（印影が登録されているハンコ）	秘密鍵（署名鍵）
何を	紙に記された契約内容	電子の契約情報
どのように	押す行為	電子的演算（電子署名）
結果	印影	署名データ（署名値）
確認	印影を目視で確認	署名検証

表 4　書面契約と電子契約の違い

では、なぜ電子署名を行うと電子文書に対して電子証明書の本人がどのようなデータに対して電子署名を行ったか確認出来るのかについて、技術的な観点で説明します。

電子署名では、はじめに電子文書のハッシュ値を特定のアルゴリズムを利用して計算します。ハッシュ値とは、電子文書の内容（データ配列）によって必ずユニークになる一定サイズの値となります。電子文書内の１バイトでも異なればハッシュ値は全く異なる値となります。次に、このハッシュ値を署名鍵で暗号化（署名データ）します。この時、電子署名に利用する署名鍵の電子証明書が認証局によって失効されていないか、または、電子証明書の有効期間が切れていないかを確認し、有効な電子証明書の場合のみ電子署名は実行可能となります。

ハッシュ値を利用する事で電子文書の内容を特定し、電子証明書記載の本人が管理している秘密鍵で暗号化されていることで電子証明書記載の本人が電子署名を行った電子文書であることを特定可能となります。

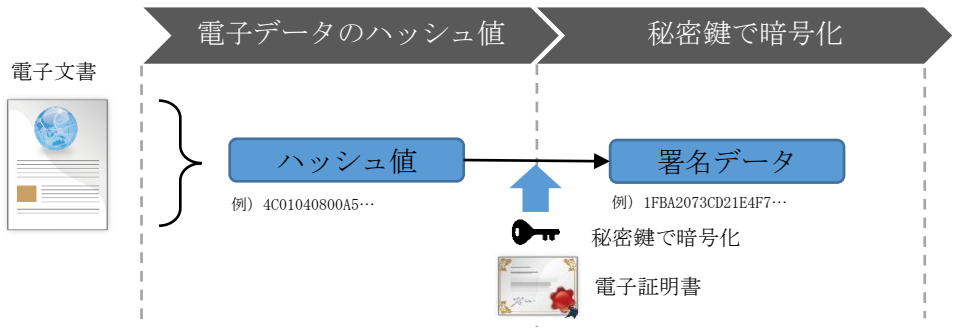

図 4　電子署名の処理概要

電子署名の署名検証では、暗号化された署名データ（署名値）を電子証明書に内包の公開鍵で復号し、復号されたハッシュ値と検証したい電子文書のハッシュ値を比較し、同一か否かで署名検証を行います。ハッシュ値が異なっていた場合には署名対象の電子文書とは異なることが確認できます。さらに、署名検証では電子署名に利用した電子証明書が正しいものであるかを確認するために、電子証明書の「パス検証」を行い、自分が信頼している認証局から発行された正しい電子証明書であることを確認します。（図 2　認証局の構成例では、署名者の電子証明書に付された認証局の署名を辿って、信頼されるルート認証局を確認するパス検証のイメージを示しています）

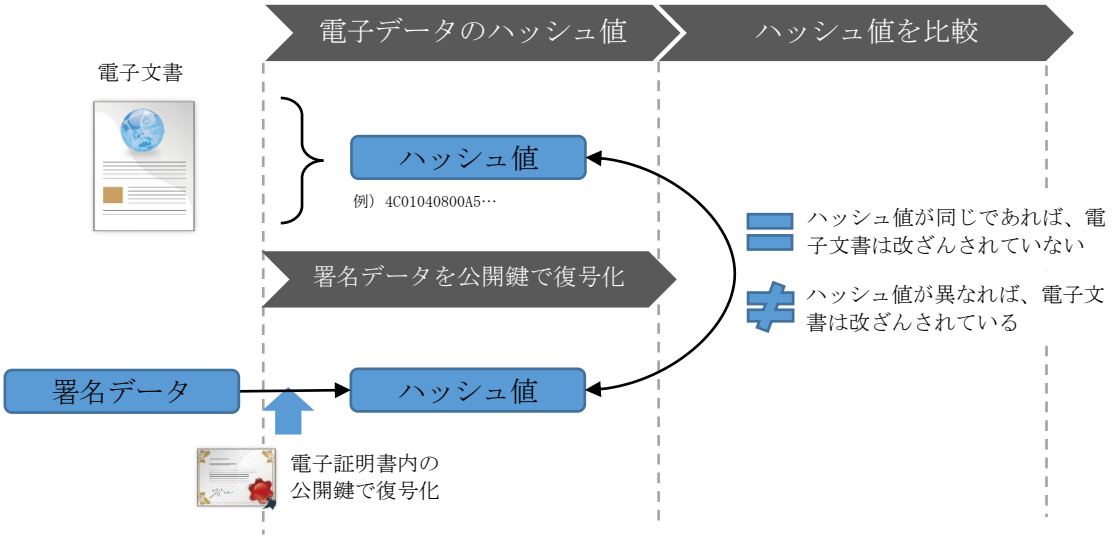

図 5　電子署名の検証処理概要

2-4. タイムスタンプ、長期署名の役割

電子契約においてタイムスタンプは契約時点の明確化と電子署名の有効性検証に必要な、後述の“長期署名“を行うために必要となり、以下の目的で使用されます。

① 署名タイムスタンプ（Signature timestamp） 電子契約書に「いつ」電子署名されたかをタイムスタンプ時刻により担保する ② アーカイブタイムスタンプ（Archive timestamp） 署名対象文書や電子署名の値、それに電子署名の有効性を検証する際に必要な情報をまとめたものにタイムスタンプを付与し、タイムスタンプ時刻以降、それらが改ざんされていないことを証明する ③ ①、②により、電子署名の有効性が検証できる期間を延長する ④ 電子帳簿保存法の電子取引情報の電子保存要件に対応する

(1) タイムスタンプとは

タイムスタンプは、タイムスタンプに記録されている時刻以前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（非改ざん証明）ものです（図 6　タイムスタンプの機能）。

タイムスタンプサービスの信頼の基盤は、タイムスタンプを発行する時刻認証局（TSA: Time-Stamping Authority）が信頼できる第三者（TTP: Trusted Third Party）であることに基づいています。時刻認証局の信頼性について、これまでは一般財団法人日本データ通信協会の民間制度である「タイムビジネス信頼・安心認定制度」の認定をうけた業務かどうかがポイントとなり、この認定をうけた業務により発行されたタイムスタンプを利用することが e-文書法や電子帳簿保存法のタイムスタンプの要件とされてきましたが、2021 年４月にタイムスタンプサービスに関する総務大臣認定制度が開始されたことに伴い、法制度に基づく認定を受けた業務として提供されるタイムスタンプサービスの利用へと順次移行していくこととなりました。

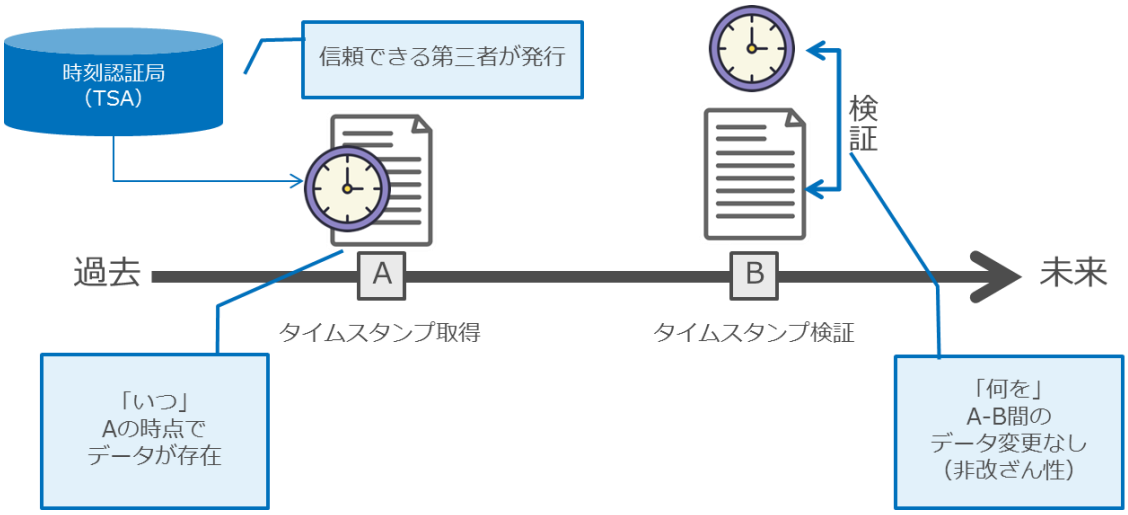

図 6　タイムスタンプの機能

(2)　タイムスタンプの仕組み

タイムスタンプサービスは、①タイムスタンプの要求、②発行と③検証の過程から構成されています（図 7　タイムスタンプの仕組み）。

要求・発行は、利用者が対象電子文書のハッシュ値を時刻認証局（TSA）に送付し、TSA がこのハッシュ値に時刻情報を付与したタイムスタンプを利用者に送付する過程です。検証は、対象電子文書のハッシュ値とタイムスタンプ内のハッシュ値を比較する過程で、タイムスタンプに含まれるハッシュ値と、後日、対象電子文書から再度取得したハッシュ値が一致していれば、タイムスタンプ付与時点以降、改ざんされていないことを証明できます。

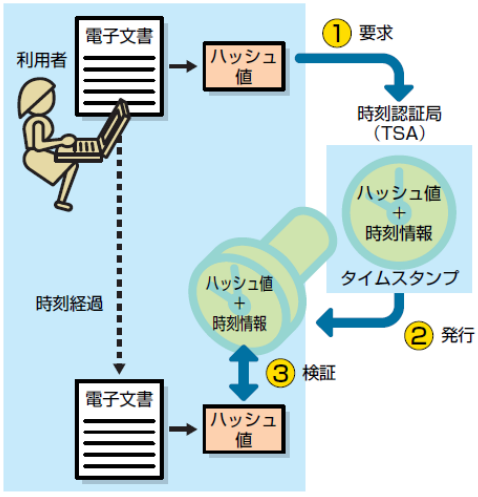

図 7　タイムスタンプの仕組み

出典：電子署名・認証・タイムスタンプ その役割と活用 - 総務省

タイムスタンプそのものの信頼性を確保するため、例えばデジタル署名を使用する方式では、タイムスタンプに TSA が管理している秘密鍵でデジタル署名をし、タイムスタンプ自体が改ざんされていないことを保証しています。

(3) 長期署名の必要性

電子署名やタイムスタンプが付与された電子文書には有効期限（署名を検証できる期間）があります。どちらも暗号技術を利用しているため、技術進歩等により暗号が破られるリスクを考え、有効期間が設定されています。

- 電子署名の有効期間

電子署名の有効期限は電子署名に用いた電子証明書の有効期間内に限られ、主務三省の大臣認定を受けた認定認証局から発行された電子証明書の場合は署名法施行規則により、電子証明書の発行日から５年を超えない期間となります。これは、自然人に対して発行する電子証明書の暗号アルゴリズムの脆弱性を考慮し期限を定めていること、また、電子証明書は一定の期間経過後は改めて本人を確認して再発行する必要があると考えられているためです。認定外の電子証明書でも多くの場合はこれに準じた運用がされています。ここで注意が必要なのは、「仮に５年間の有効期間を持つ電子証明書を有する秘密鍵を用いて電子署名した場合でも、電子署名の有効期間は電子証明書が発行されてから５年以内なので、発行後４年後に電子署名を行った場合は、その電子署名の有効期間は１年以内となる」ということです。

- タイムスタンプの有効期間

デジタル署名方式のタイムスタンプの有効期間はやはりタイムスタンプを発行する際に用いたタイムスタンプ局の電子証明書（TSA 証明書）の有効期間内に限られます。ただし TSA 証明書は TSA を運営する法人が正しく管理するタイムスタンプサーバーが生成する秘密鍵に対して発行され、暗号アルゴリズムは強固なものが用いられます。また、自然人には必要と考えられたような一定期間後の本人確認も不要と考えられるので、TSA 証明書の有効期間は長く設定することが可能です。現在、日本のタイムスタンプ局の TSA 証明書を発行している認証局は、IE や CHROME などの主要なインターネットブラウザに、そのルート証明書が登録されている「パブリック認証局」から発行されており、その有効期間は１１年３ヶ月未満であることが定められています。[10]ここでタイムスタンプ局は、タイムスタンプの有効期間を最短でも１０年間を保証するために毎年新しい TSA 証明書に更新し、古い TSA 証明書に紐づく TSA 秘密鍵は安全に廃棄し、同じ TSA 秘密鍵を１年以上使い続けることができない

10 サーバー証明書を発行する認証局やブラウザーベンダー等から構成される任意団体、CA/Browser Forum（CA ブラウザーフォーラム）にて規定

よう運用しています。したがってタイムスタンプの有効期間は、TSA 証明書の更新直後は１１年近い有効期間となり TSA 証明書の更新直前に発行されたたタイムスタンプでも１０年以上の有効期間になることを保証しています。

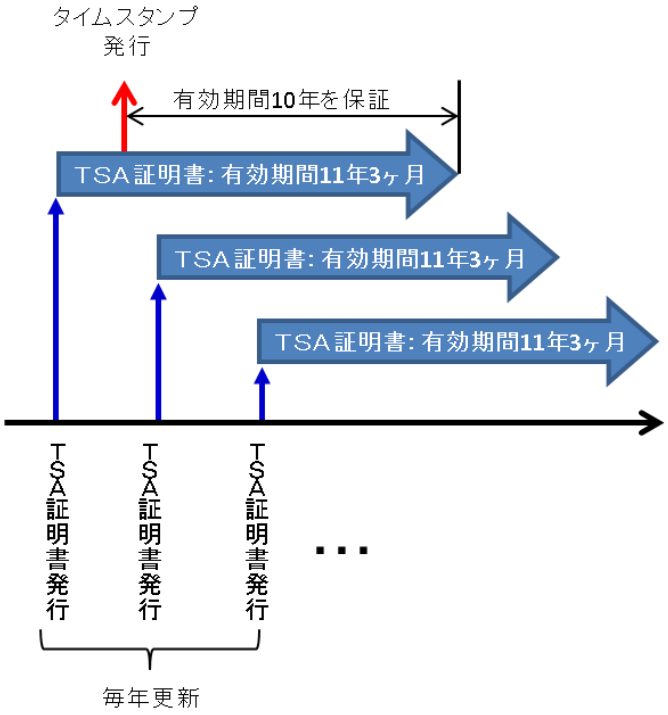

図 8　タイムスタンプの有効期間（例）

実際の契約では、２０年から３０年継続する基本契約も存在するため、電子署名の有効性が確認できる期間が電子証明書の有効期間に限られてしまう電子署名だけでは対応することができません。この問題に対応するために作られた国際規格がタイムスタンプを併用した「長期署名」です。

長期署名では電子署名を付与した直後に、署名値に対してタイムスタンプを付与し署名時刻を担保します（署名タイムスタンプ： Signature timestamp)。したがって署名検証する際に証明書の有効期間が切れていても、署名タイムスタンプが付いているので、この時刻に電子証明書が有効であったことを確認できれば良いことになります。その後に電子署名の有効性を検証する際に必要な情報として証明書チェーン上の認証局の証明書や署名者の証明書、失効情報などを集めて署名およびタイムスタンプを付与した署名文書とひとまとめにし、タイムスタンプを付与します（アーカイブタイムスタンプ： Archive timestamp)、アーカイブタイムスタンプ時刻以降、その対象電子文書が改ざんされていないことが証明

できるため、アーカイブタイムスタンプが有効な間は電子署名の検証が可能となります。タイムスタンプは常に強固な暗号アルゴリズムを利用できるため、新しいアーカイブタイムスタンプを追加していくことで、署名検証の有効期限を長期にわたって延長していくことが可能となります。

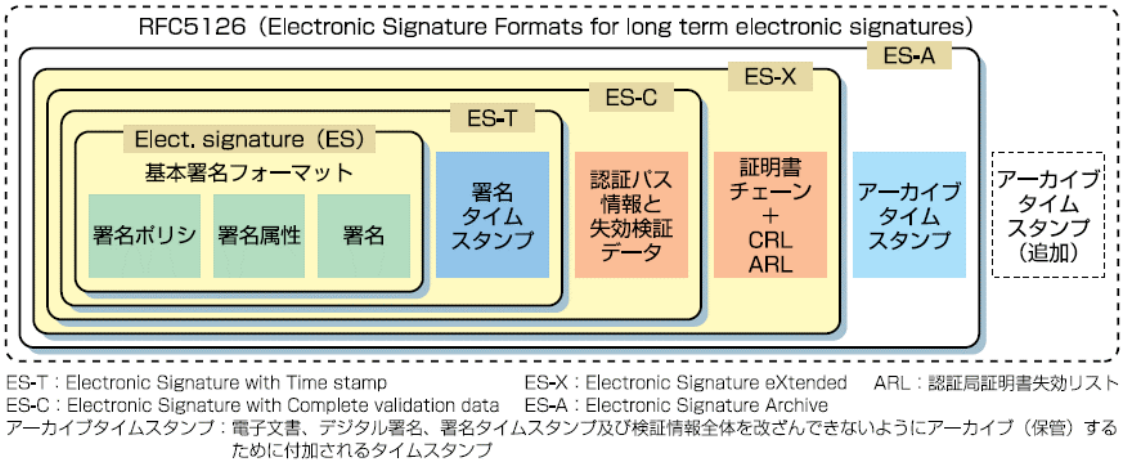

図 9　長期署名フォーマット

出典：電子署名・認証・タイムスタンプ その役割と活用 - 総務省

　このように電子契約書が取り交されて以降、長期にわたり「いつ、誰と誰が」合意したかを第三者が検証判断できるためには、長期署名を行うことが必要となります。

なお、長期署名のフォーマットを規定した標準規格（長期署名フォーマット）には、「2-1. 電子文書（電磁的記録）の種類や電子署名の方式」に記載した CAdES、XAdES、PAdES、ASiC があります。

- 電子帳簿保存法とタイムスタンプ

電子契約のように、インターネット等で紙を介さずに取引を行うことを「電子取引」といいます。所得税および法人税を納税する企業が電子取引を行った場合に、取引情報をデータで保存しておくことが、電子帳簿保存法の第７条（旧第１０条）で義務付けられています。この電子帳簿保存法第７条に求められる、保存要件の一つとしてタイムスタンプの付与が求められています。

詳細については JIIMA 発行の「電子取引　取引情報保存ガイドライン」第 2.00 版[11]をご参照ください

11 https://www.jiima.or.jp/wp-content/uploads/policy/denshitorihiki_guideline_v2.pdf

2-5. 電子契約の形態について

契約とは、当事者間における合意です。「申込み」と「承諾」によって契約は成立します（民法５２１条～）。原則として口頭の約束でも契約は成立すると言えます。
世の中に様々な電子契約サービスがありますが、極端な言い方ですが、契約当事者間の合意が認められる電子契約サービスであればどんなサービスを使っても契約が行えると言えます。

これら電子契約には、電子文書への署名方法としてここまで記載致しました「電子署名」の仕組み以外にもタブレット等の端末の画面上で手書きのサインを行い契約の合意の意思表示を行う「電子サイン」と呼ばれる仕組みもあります。
この２つは署名を構成する認証方法（本人の意思確認）や技術に違いがあり、署名に関する法律や規制の要件に関わっています。

さらに、最近は、電子署名の方法が多様化してきています。電子署名に使う署名鍵の保管場所によって「ローカル署名」と「リモート署名」という２種類の方法があります。また、契約当事者自身が所有する署名鍵で電子署名をおこなう従来の署名方法（当事者型電子署名）に加えて、電子契約サービス提供事業者の署名鍵で電子署名をおこなう署名方法（事業者型電子署名）が普及し始めています。

以下に、電子契約における電子署名などの利用形態について整理します。

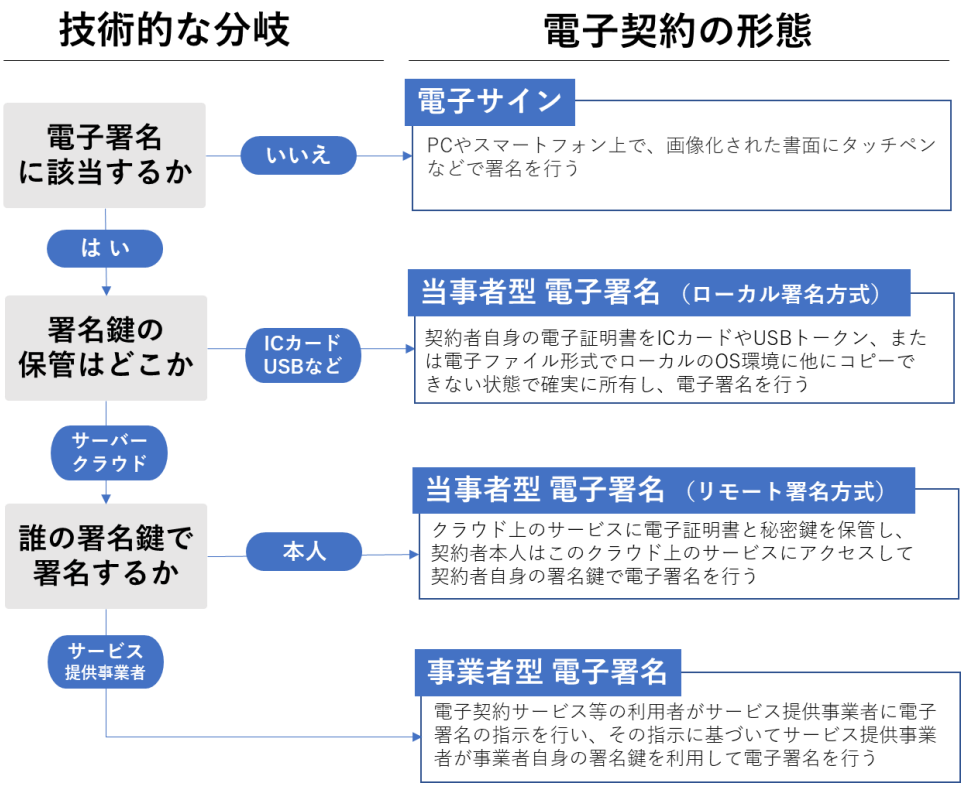

図 10　電子契約の形態

（１）当事者型電子署名（ローカル署名方式）

署名鍵をＩＣカードやＵＳＢトークン、または電子ファイル形式でローカルの OS 環境に他にコピーできない状態で確実に契約者本人が所有し、電子署名をローカルの OS 環境で行う方式となります。ローカル署名では、契約者本人の署名鍵によって生成された電子署名は、署名鍵を利用出来る環境が契約者本人に限定されるために、確実に本人の意志によって生成された電子署名であるという事が確認出来ます。物理的な媒体を所有しているという事と、ＩＣカードやＵＳＢトークンの利用時には利用者本人しか知らないＰＩＮがローカル環境で必要となるため、本人以外が電子署名を付与出来る可能性が少なくなります。

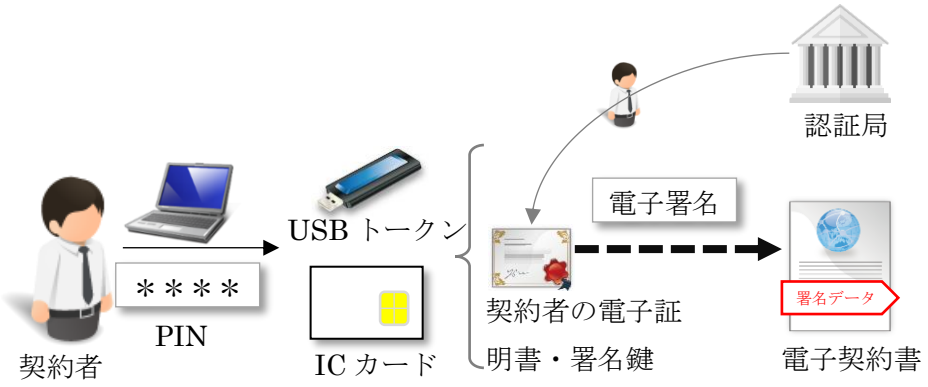

図 11　当事者型電子署名（ローカル署名方式）

（２）当事者型電子署名（リモート署名方式）

クラウド上のサービスに契約者本人の電子証明書と署名鍵を保管し、契約者本人はこのクラウド上のサービスにアクセスし、電子署名を行う方式となります。この方式では、クラウド側のサーバーにて署名鍵を HSM[12]（Hardware Security Module）などの安全な機器に保管し不正に外部にコピーされない対策を行ったうえで、その署名鍵を契約者本人以外が利用出来ないような厳格な認証（２要素認証など）を行った後に、クラウド上で電子署名を行います。リモート署名では、不正に契約者本人以外が電子署名を行うことが出来ないようにシステムの仕組みや運用について安全性及び信頼性を確保することが重要となりますが、その指標として日本トラストテクノロジー協議会（JT2A）が、主務３省及び JIPDEC によるオブザーバー参画のもとに策定した「リモート署名ガイドライン第一版」が 2020 年４月に公開されました。また、欧州では、既に eIDAS[13]規則によってリモート署名の法整備が進ん

12 証明書の署名鍵を安全かつ適切に保管し運用するための専用装置

13 EU は、eIDAS（electronic Identification and Authentication Services）規則を 2016 年７月に発効した。eIDAS 規則及び参照技術標準により、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・プロバイダーとして認定する法的枠組みが整備されている。電子署名においては手書き署名と同等の法的効果がある適格電子署名が規定され、リモート署名においても適格署名生成装置や多要素認証などの要件を満たすことにより適格電子署名の認定を受けることができる。

でおり、２要素認証など厳格に本人を認証する事でリモート署名であっても手書き署名と同等な法的効果が認められております。

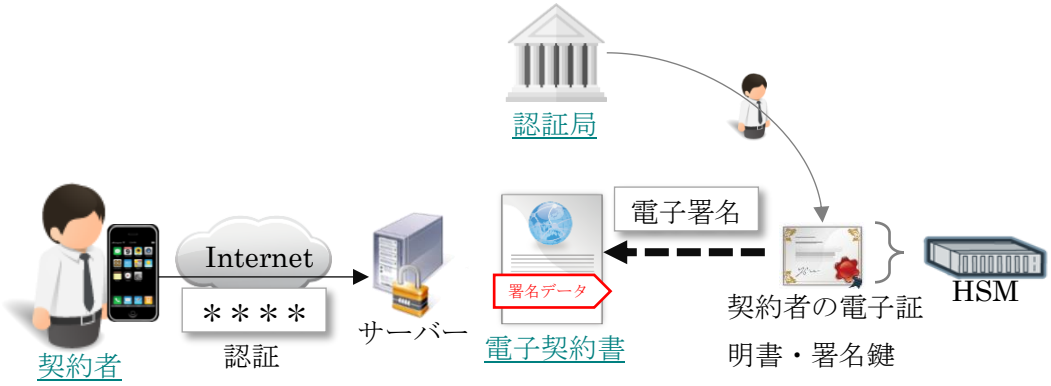

図 12　当事者型電子署名（リモート署名方式）

（３）事業者型電子署名

契約者本人はクラウド上のサービスにアクセスし、サービス画面より契約に合意する操作を行うことでサービス上に合意のログを記録します。サービス提供事業者はクラウド上のサービスにサービス提供事業者自身の電子証明書と署名鍵をあらかじめ保管しておきます。契約者本人による合意操作が行われた後、サービス提供事業者が自身の電子証明書と署名鍵にて電子署名を行う方式となります。この方式では、電子契約書に対してそれぞれの契約者が内容を確認した際にサービス提供事業者の電子証明書と署名鍵で電子署名を行います。

電子署名に利用する電子証明書の違い以外は、基本的には当事者型電子署名（リモート署名方式）とシステム構成としては同様となります。

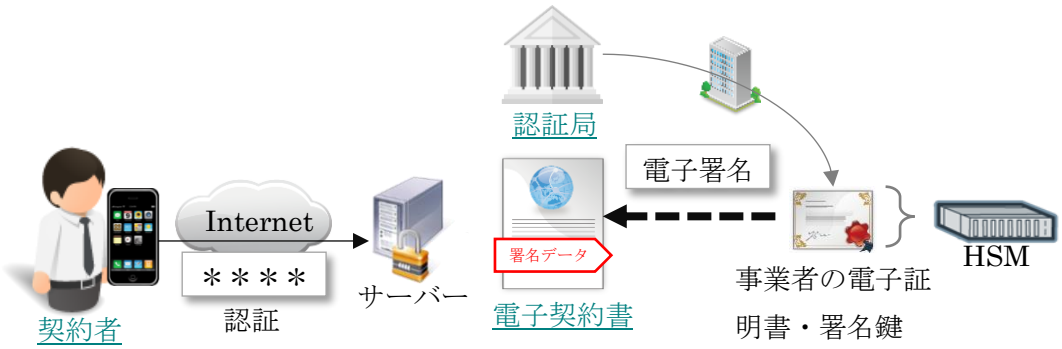

図 13　事業者型電子署名

電子の世界はなりすましや改ざんが比較的容易に行われることから、これらが防止され、法令とリスクのバランスを見ながら、一定の安心・安全が担保された仕組みを選んでいただくことが重要であると考えています。

特にビジネスにおいて厳格性が求められる重要な契約は、契約書が真正に成立していることの推定が容易な電子署名法準拠の電子証明書を用いた電子署名を行う電子契約サービスなど適切なサービスを選ぶ事が重要です。

（電磁的記録の真正な成立の立証については第 3 章にて解説します。）

3. 電子契約の運用と証拠性について

3-1. 電子契約の運用ポイント

電子契約を導入する際、もっとも重要となるのは、導入する電子契約システムを運用して作成された電子契約書が電子署名法第３条の推定効を得られるかです。すなわち従来の書面による契約書と同等の法的効果が得られることが必要となるわけです。

また、電子契約を行う前に、契約の相手側への説明と同意も必要となります。主な運用のポイントは以下が考えられます。

（１）契約内容の重要性に応じた契約当事者の本人性確認を行うこと

- ＢtoＢでの契約の場合、電子契約サービスのログインＩＤ（及び当事者型電子署名の場合は、当事者に対する電子証明書）を発行する際の本人確認時に法人代表者本人であるか、または法人代表者から契約締結の権限委任を受けている本人であるかを確認
- ＢtoＣでの契約の場合、電子契約サービスのログインＩＤ（及び当事者型電子署名の場合は、当事者に対する電子証明書）を発行する際の本人確認の審査レベルは契約内容の重要度に応じて適切かを確認
  - 重要な契約の場合はマイナンバーカード、住民票+印鑑登録証明書等の確認を推奨
  - 重要な契約の場合は、「犯罪による収益の移転防止に関する法律（犯収法）」への対応も考慮に入れた対面による（オンライン面談を含む）本人確認も検討
  - 重要な契約以外は、運転免許証コピーなどを確認
- メールアドレスのみの審査は推奨されない

（２）既存業務との連携をどこまで実施するか

- ユーザーＩＤ、契約書作成審査システム、その他の業務システムとどこま（で連携するか、またその連携開始時期を何時にするかなどを検討（必ずしも電子契約の導入当初からシステム連携が必須とは限りません）

（３）運用規程等の備え付けと契約の相手側への説明と同意

- 電子契約を採用する業務や、どのような仕組みを利用し、どのような本人審査を行なうことで電子的に契約締結がなされるのかを運用規程に定め、それを備え付けることが必要
- 電子契約の利用者向けにＩＤ・パスワードや電子署名の際のＰＩＮ（暗証コード）の管理方法などを定めた電子契約の利用規程を作成することが必要

・ 上記で定めた運用規定や利用規程に対して契約相手の同意を得ることが必要

なお、これらの規程書の作成に当たっては、電子契約サービス事業者の規程文書の参照や同事業者が提供する雛形文書を利用することができる場合もあります。

（４）関連法制度、ガイドラインの要求や推奨基準を満たすこと

・本ガイドライン「1-4. 電子契約を取り巻く法律について」で取り上げた、関連する法令やガイドライン、技術基準等にて求められる要求事項や推奨基準を満たすこと

（５）電子契約では、本人による契約合意の意思表明が行なわれていることが重要となるため、電子契約システムは本人以外が電子契約サービスにログインを行い、契約合意が行えないよう十分な安全性が確保された運用が行われていること

■事業者型電子署名のサービスの場合

① （１）でも解説をした厳格な本人確認に基づいて発行されたログインＩＤに加えてワンタイムパスワードを組み合わせるなどの多要素認証によって、契約当事者のみが電子契約サービスにアクセスの上で契約合意が行える仕組みとなっていて、かつその記録がきちんと管理されていること

② ①で行った契約合意が、改ざんされないよう電子契約サービス提供事業者などにより、電子署名・タイムスタンプなどを付すことによって改ざん防止が図られる仕組みとなっていること、

また利用者（署名者）を特定するために必要となる契約への同意入力を行った際の操作ログなど、当該サービス内で保有するアクセスログの真正性が担保されていること

■当事者型電子署名のサービスの場合

① 証明書の秘密鍵が厳格に管理されている認証局を選択することが大切となるため、利用する認証局の CPS（Certification Practice Statement）[14]等に以下の様な内容が記述されているかを確認

・利用者の電子証明書を発行するために用いられる認証局の秘密鍵は FIPS140-２レベル３ [15]の認定を取得した HSM（Hardware Security Module）で適切に管理され、複数人コントロールがなされていること

・適切な準拠性監査が行われていること

---

14 認証局が証明書を発行する際の運用方針とその実施手順などを定めた規定書

15 FIPS140（Federal Information Processing Standardization 140）は、暗号モジュールに関するセキュリティ要件の仕様を規定する米国連邦標準規格。現在の規格の最新版が FIPS140-2 となる。FIPS140-2 ではレベル 1 からレベル 4 までの 4 段階のレベルが定義されレベル 3 は 3 番目に高いセキュリティレベル

② リモート署名サービスを利用する場合、本人以外が電子署名できないよう十分な対策がなされていること

・リモート署名サービスへの利用者の秘密鍵の登録は認証局からの直接発行を推奨

・重要な電子契約を取り扱う場合、リモート署名サービスへの認証方式は２要素認証を推奨

3-2. 訴訟対応

海外より遅れていた司法の電子化に政府がようやく動き出しました。内閣官房が事務局を務める日本経済再生本部で、2017 年 10 月 30 日より、「裁判手続き等のＩＴ化検討会」[16]がスタートしています。

これにより、インターネットでの裁判所への書面提出、訴訟記録の電子化、テレビ会議システムを使用した審理の拡充などについて議論が行われ、2018 年３月に「裁判手続等のＩＴ化に向けた取りまとめ」が公開されました。近い将来に電子情報が有効活用されるとはいえ、現状では、既存の法律やルールを踏まえた対応が必要となります。

電子署名が付された電子契約書が、「署名または押印」された紙の契約書と同様に有効であることを証明するには、「電磁的記録の真正な成立」を立証することが必要です。そこで電子文書の証拠性と立証について、係争時の対応も想定して整理してみます。

（１）電子文書の証拠性を支える５Ｗ１Ｈ

一般に、何らかの事実を証明するには、５Ｗ１Ｈを明らかにすることが重要とされています。すなわち、いつ(When)、どこで(Where)、だれが(Who)、何を(What)、なぜ(Why)、どのように(How)したかを明らかにすることです。「電磁的記録の真正な成立」を証明する場合にも同様と考えられます。すなわち電子文書をそれ自身だけ単独で提示しても信憑性がなく、その文書がどのような経緯で何のために誰が何時どのようにして作成したのかなどを明らかにすることにより信頼性が得られると考えられます。図４に「電子文書の証拠性を支える５Ｗ１Ｈ」を図示します。

５Ｗ１Ｈを明らかにする際、長期署名が付された電子文書であれば、「いつ」、「だれが」、「何を」の３つの要素は電子署名とタイムスタンプにより証明可能となります。それ以外、「なぜ」を明らかにするには、当該電子文書がどのような業務のために作成されたものなのかを明らかにする作成目的やルール、何のために電子署名するのかなどを定めた運用規程や利用規約などの提示が有効と考えられます。従ってこれらの規程類の整備と保存が重要となります。また「どのように」して当該電子文書が作成されたのかを明らかにするには、電子文書を作成し電子署名を付与する「署名システム」の仕様や操作説明書、さらに操作ログなどの提示が有効と考えられます。

16 https://www.kantei.go.jp/jp/singi/keizaisaisei/saiban/index.html

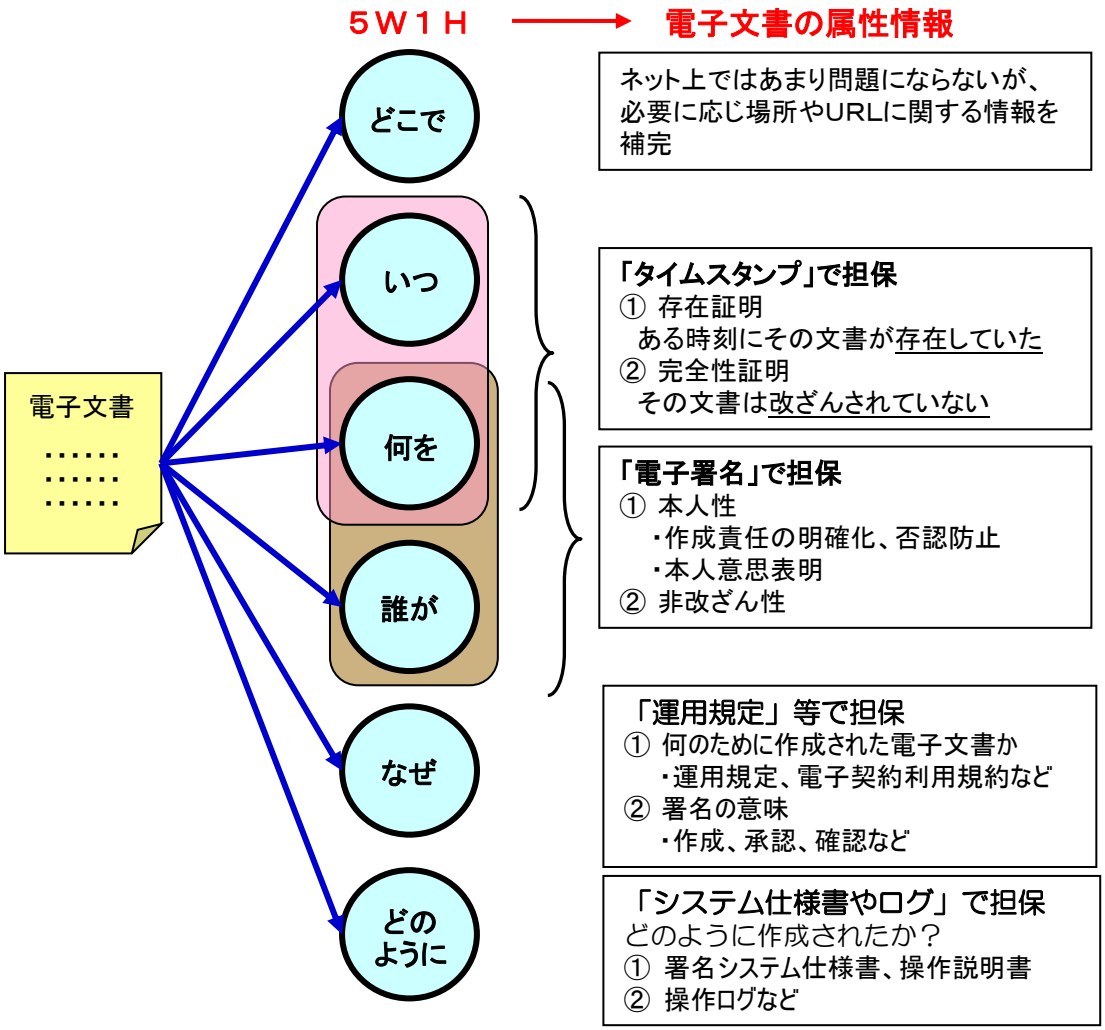

図 14　電子文書の証拠性を支える５W1H

（２）二段の推定による立証

電子署名済み文書の真正な成立を立証するには、私文書の真正な成立についての最高裁判例に従って以下の「二段の推定」に従って論点を組み立てることが有効と考えられています。

- 二段の推定による、私文書の真正な成立について(形式的証拠力の立証)

私文書の成立の真正について、最高裁判例（最判昭和３９・５・１２民集１８巻４号５９７頁）では「文書中の印影が本人または代理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、該印影は本人または代理人の意思に基づくものと推定するのが相当とすることから、該文書が真正に成立したものと推定すべきである」とされています。

これがいわゆる「二段の推定」で、そこに押印されている印影が本人又は代理人の印章（ハンコ）のものと一致していれば、本人の意思に基づいて押印されたと推定され（一段目の推定）、この押印が本人の意思に基づくものなら文書の成立の真正が推定される（二段目の推定：民訴法第 228 条第 4 項）ことになります。

- 電子文書の真正な成立について(形式的証拠力の立証)

電子文書の成立の真正については、電子署名法第３条にて「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」とされています。「二段の推定」に従って考えると、当事者型電子署名については、電子文書に付与されている電子署名が「本人に発行された電子証明書の秘密鍵」によりなされたものであることが認定されると、そのことから、**その電子署名は本人の意思に基づいて成立したものと推定され（一段目の推定）、**この電子署名の真正からさらに**電子文書の成立の真正が推定される（二段目の推定）**と言えます。印鑑証明書による推定との比較を図 15　二段の推定（印鑑証明書による推定との比較）に示します。

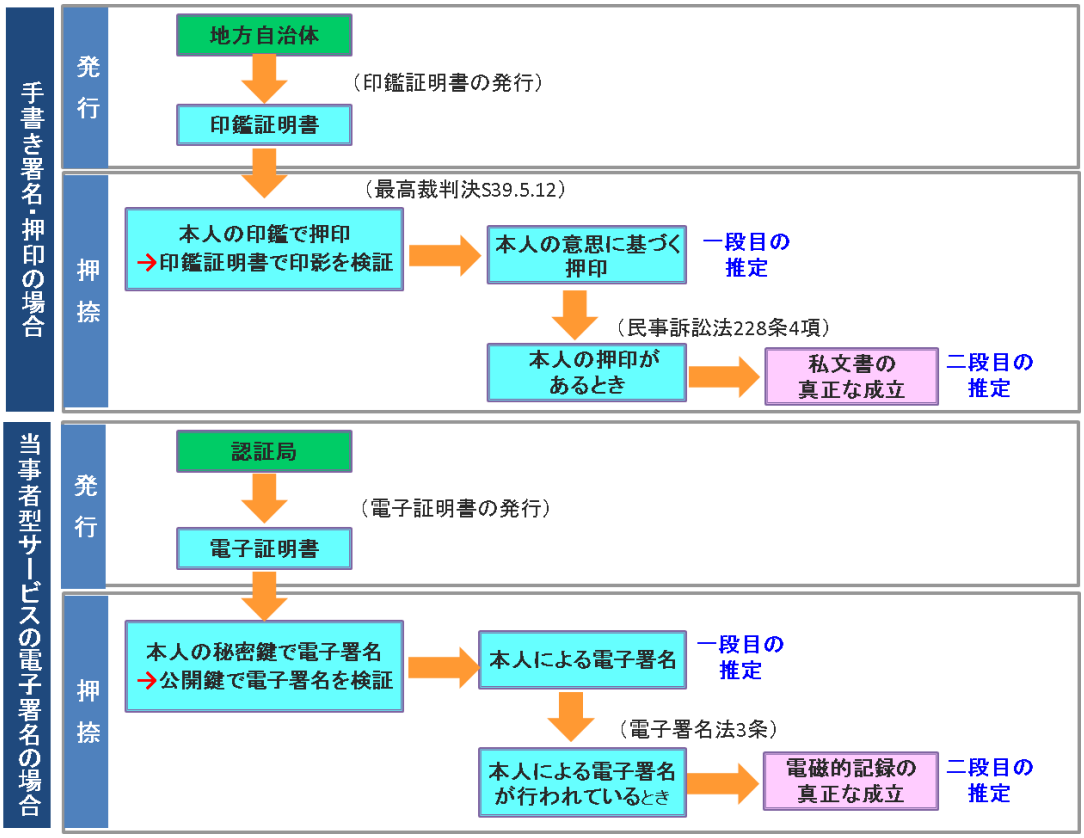

図 15　二段の推定（印鑑証明書による推定との比較）

（３）本人による電子署名であることの立証

署名の本人性を裁判で証明するためには以下の資料などの提出が有効と考えられます。

① 電子証明書（秘密鍵）が確かに本人に対して発行されていたことを示すもの

・認証局の証明書発行に関する規程（CP: Certificate Policy 証明書ポリシなど）

・証明書発行の際に認証局が受領した発行申請書や本人確認書類、証明書受領書

② 秘密鍵は本人だけが使用できる状態であり、その署名操作が確認できるもの

・システム概要書、仕様書、必要に応じ署名時の操作ログなど

③ 長期署名の検証結果

・タイムスタンプの有効性検証を含む署名検証レポートやその解説書など

③の検証レポートでは、電子署名した時刻が何時なのかタイムスタンプを検証することにより明らかとなり、正当な認証局が発行した証明書（秘密鍵）が用いられており、署名時刻の時点で証明書の有効期間が切れておらず、かつ失効していない証明書の秘密鍵が用いられていたこと、署名対象データに改ざんがないこと、などが証明できます。電子契約を導入する際は、このような立証に必要な情報があらかじめ用意されているか、また、ログ収集などの機能があるか確認しておくと安心です。

（４）事業者型電子署名における立証

事業者型電子署名を用いた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のか、2020 年９月４日に署名法主務三省（総務省・法務省・経済産業省）より電子署名法第３条の推定効が働く要件がＱ＆Ａの形で示されています（以下、「三省Ｑ＆Ａ」）。また、この三省Ｑ＆Ａに対して「電子認証局会議（CAC）」と「トラストサービス推進フォーラム（TSF）」から共同で解説書が公開されておりますので、以下にその概要を示します。

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三省Ｑ＆Ａにおいて「十分な水準の固有性」を有することが要件とされました。この要件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二要素による認証等、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) 利用者ごと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ひも付いて適切に行われる）

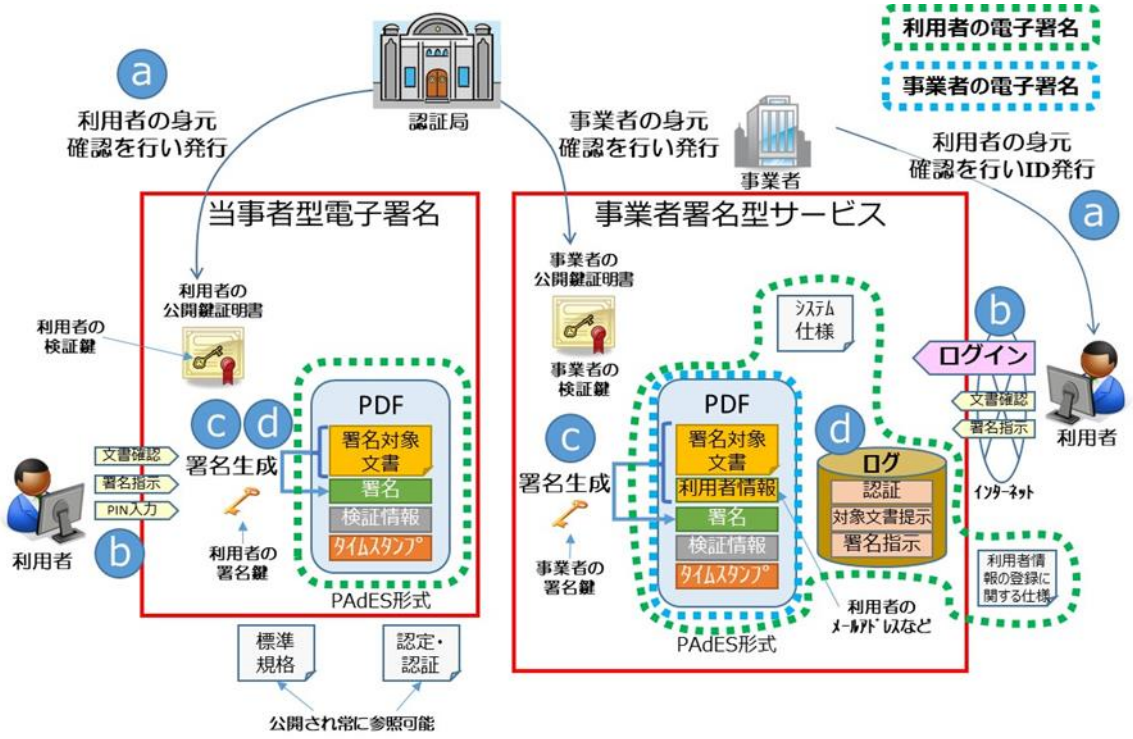

図 16　当事者型電子署名と事業者型電子署名の比較図

出典：「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/電子認証局会議）

当事者型電子署名の電子契約サービスが、前述のとおり対象文書に付された電子署名の検証を行うことで電子署名法第３条の推定効が得られるのに対して、事業者型電子署名の電子契約サービスの場合は、当事者型電子署名で求められる情報に加えて、利用者が契約に合意した際のシステムログ情報など、より広範囲な情報を固有性確保のために管理する必要があります。特に上記の d)を証明するためには、システムが当該利用者によって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。

①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。

②運用担当者が不正を行えないようなシステム設計、運用設計がなされていること。

③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。

④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。

したがって利用者は、これらの要件がどの程度満たされているサービスであるのか、事前に確認しておくことが重要となります。

	事業者型電子署名	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

表 5　事業者型電子署名と当事者型電子署名の立証方法の比較

出典：「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/電子認証局会議）

電子文書情報社会では、署名・押印がある紙書面に代わり、同等の証拠力のある電子文書の利用が不可欠となります。それには信頼に足りる公開鍵証明書とタイムスタンプを利用した長期署名方式による電子署名が有効となります。その証拠性の立証には署名の本人性

を証明する必要があり、電子文書の作成に係わる５Ｗ１Ｈの属性情報の提示や長期署名の検証レポートの提示が重要となります。署名の本人性が認められると電子文書の真正な成立が推定され署名・押印がある書面と同等の証拠性が認められたことになります。

実は「署名・押印がある紙書面」には印鑑登録の失効メカニズムはなく、タイムスタンプのように作成日時を証明できるものもありません。また、署名当時から書面に追記、改変がないことを確実に証明する手段もありません。そう考えると、長期署名を付与した電子文書の方がよほど高い証拠能力を有していると考えられるのではないでしょうか。

4. 電子契約を始める際に注意すべきポイント

「契約」は企業にとって、取引先や顧客と、様々な目的で取り交わし、法的拘束力をもつ、最も基本的かつ重要な活動の一つです。そのため、「契約」を従来の紙から電子に置き換える「電子契約」の導入にあたっては、注意が必要です。本章では、電子契約を始めるにあたってどのような仕組み（サービス）を利用して、電子契約を行なうのか、契約と取り交わす取引先や顧客とは、どのような調整を行わなければならないのか、自社内でどのような調整が必要となるのかなど、運用を始めるにあたってのポイントを説明します。

4-1. 電子契約サービスを選定する際に考慮すべき要件

電子契約が始まった当初は、契約文書を社外に保管することに抵抗があり、社内にシステムを構築するオンプレミスで導入を希望される企業が多くありましたが、初期導入コストや、運用コストが高額となること、運用が煩雑になることから、なかなか普及しませんでした。しかしながら、ここ数年でＳａａＳ型の電子契約サービスが数多く提供されるようになり、今後主流となってくるように思われます。

企業活用の中でＩＴを活用したサービスを導入する際、一般的には、それぞれのサービスの特長や導入コスト、セキュリティ、導入実績などの観点から、自社に適したサービスを選定していると思いますが、電子契約サービスの導入に際しては、以下の様な要件を考慮されることを推奨します。

(1) 法的証拠力について

第３章で既にご説明しましたとおり、電子的に作成した文書ファイルに電子署名、タイムスタンプを付与した場合、「署名者本人が文書を作成したこと」、「タイムスタンプの時刻に存在したこと」、「検証時まで改ざんされていないこと」が証明できるので、その文書は係争時には裁判上強い証拠力を持つと考えられます。

しかし、必ずしもすべての文書が強い証拠能力をもつ必要があるわけではなく、より簡単に作成し、締結できる利便性が優先される文書も企業には多くあります。そこで、電子署名を操作ログや電子手書きサインに置き換える方法や、提供ベンダーの電子署名のみ付与する方法などで電子契約サービスを提供しているベンダーもあります。ただし、このような方法については、係争時の証拠力は弱くなる可能性があります。

また、これまでの章で説明したとおり、電子証明書を利用した電子契約サービスであっても、認証局や、本人確認審査などの認証方法の違いにより、紙の契約での実印に相当するも

のから、認印レベルのものまで様々な電子証明書が存在します。電子契約サービスを導入する際には、文書の重要性、訴訟の可能性、即時締結が必要か否かなどを勘案し、どのような方式で法的証拠力を担保するか検討する必要があります。

また、電子署名を用いた電子契約を行なう場合、ローカル署名とリモート署名の方式があり、今後リモート署名の方式が普及しつつあることについては、第２章で述べました。このリモート署名方式を採用したサービスを検討する際には、不正に契約者本人以外が電子署名を出来ないよう、電子署名に用いる電子証明書が、安全な機器に保管される仕組みとなっていること、署名者本人しか電子署名が行なえないよう認証の仕組みがしっかりしているものなど、システムの信頼性が考慮された仕組みを選定する必要があります。

(2) データ保存の有無

日本における電子契約サービスの多くは電子署名、タイムスタンプ機能を提供するとともに、クラウド上に契約書を保存し、検索する機能を提供しています。他方、電子署名、タイムスタンプ機能だけを提供し、保存はユーザー側で行うサービスもあります。

前者の場合は電子帳簿保存法など各種法令で求められる保存期間の担保や、検索機能など電子保管に際して求められる各種要件の対応をベンダー側で対応しているケースが多くありますが、そのサービスを終了となった場合や、解約する場合には、クラウド上で保管されている契約文書がどのように取り扱われるのかを事前に確認しておく必要があります。

後者のケースでは、サービスが終了となった場合や、解約する場合でも、自社に契約文書を保管するため契約書の取り扱いについては、事前の考慮が不要とはなるものの、電子帳簿保存法などの法令で求められる保管期間の担保や、検索要件を満たせる仕組みを準備するなどの法令対応を別途自社で行なう必要があります。

図 17 データ保存機能の有無

検討の対象となる契約書が電子帳簿保存法などで保存が義務付けられている文書なのか等を鑑みながらデータ保存が含まれるサービスを選択すべきか適切なサービスを選択すると良いでしょう。

(3) 導入実績

導入実績については、同業他社での実績があるか、またその導入規模が自分たちの実態に近しい実績があるか、などを確認されることをお奨めします。これは、同業他社での実績が多ければ、これから電子契約を結ぼうとする相手先に対して、電子契約を行なうことの合意を得やすいためです。

サービス事業者が謳う、サービス利用者数や、業界シェアなどだけで判断せずに、自社利用をふまえた、確認を行うようにしてください。

(4) ＢtoＢ電子契約かＢtoＣ電子契約か

企業間（ＢtoＢ）契約は、同じ相手先に対して、同じような契約が繰り返されることが多く、特定の担当者に対して操作教育もできるため、汎用機能をもつ電子契約サービスを利用した方が多くの業務で利用でき、効果を上げること可能です。他方、住宅ローン契約や賃貸契約など企業と個人間の（ＢtoＣ）契約は、１回だけしか利用しないことがほとんどなので、個人が初めてでも利用できるように、専用のＵＩ（画面）を用意した方が、利用者の利便性を高めるためにもよいでしょう。

導入する契約がＢtoＢ用途なのかＢtoＣ用途なのかにより、利用する電子契約サービスの選択も変わることがあります。

(5)セキュリティ、可用性

自社セキュリティポリシーに沿ったセキュリティ機能やデータ保全体制が備わっているか、システムの可用性が自社の求める水準を満たしているかも選定の初期段階から考慮するとよいでしょう。

サービス事業者ごとに標準機能として備わっているセキュリティレベルは異なるため、自社のセキュリティポリシーに沿ったサービスを選定するうえで考慮すべき要件となります。

4-2. 電子契約を開始するに当たっての調整のポイント

電子契約を開始するに当たっては、お取引先との調整および、自社内での調整が必要となります。ここでは、電子契約を開始するに当たっての調整事項のポイントを説明します。

(1) 取引先との調整事項

電子契約を開始するに当たっては、契約当事者間で契約を電子契約で取り交わすことについて事前に同意を取っておく必要があります。企業間取引を電子契約で行なう際の同意取得に当たっては、以下の様なポイントに留意いただくと良いかと思います。

・契約締結を電子契約で行なうことに対する同意

ここには、どのような仕組みで電子契約を締結するのか、そのシステム概要や電子証明書の発行にかかわる本人審査基準、署名に用いるＰＩＮ（暗証コード）の発行管理などの説明と同意が含まれます。

・電子契約システムを利用する担当者情報の申請

–申請された担当者が、当該法人に在籍していることの確認

–申請された担当者が、当該法人の代表者または、代表者から契約締結の権限を委任された者であることの確認

電子署名に使用する電子証明書は自然人に対して発行することが原則となります。そのため、書面契約の際に用いられる代表者印のような役職印に相当する電子証明書は通常発行できませんので、電子契約に使用する電子証明書は電子契約サービスを利用する担当者に対して発行されます。従って、電子証明書の発行を受ける担当者が、本当に当該法人に在籍しているのか、契約を締結する権限を有した担当者なのかを事前に確認されることが大切となります。

(2) 社内規定の見直し

従来の書面契約を行う場合は、押印規定等の社内規定に従って、印鑑の捺印を行なっているかと思いますが、電子契約を行なう場合、押印規定に電子署名を行なう運用についてのルールを定義する必要があります。

・規定策定に当たってのポイント

- 電子証明書の管理責任者
- 電子署名を行なう者に対する権限の委任
- 電子署名を行なう際の承認ルール
- 証明書発行申請の手続きについて
- 電子署名を行なう者が遵守すべき事項について

ルールの策定に当たっては、既存の押印規定に、電子署名のルールを追記の上で改訂いただく形でも、新たに電子署名規定のような規定を策定いただく形でも問題ありません。

また、電子契約にて締結された契約書は、クラウドサービス上や、社内のファイルサーバー、文書管理システムなどで管理されることになるかと思いますので、それにともない、文書管理規定の修正が必要となることがあります。文書管理規定を修正する場合は、以下の様な点に留意します。

- 電子契約で締結した場合の契約書保管先の追加
- 文書にアクセスできる権限及び閲覧申請についてのルール追加
- 契約文書の保管期限、廃棄ルールの追加

(3) 契約文書の見直し

契約書内の文言に書面による締結を意図した文言が含まれている場合、電子契約に合わせて契約内容の見直しを行なっていただく必要があります。見直しのポイントは以下となります。

- クラウドサービス内に契約文書を保管し、当事者間で共有するような仕組みを利用する場合、契約書内の「合意の証として、本書２部作成の上で、甲乙が各１部を保管するものとします。」などの内容は、実態と合わなくなってしまうため、例えば「本契約は電磁的に作成、保管するものとし、甲乙双方の電子署名をもって締結することとします。」のような適切な内容に修正が必要となります。
- 契約書内に「書面による取交し」など「書面」という文言が含まれている場合は、「紙」による対応を意図した内容となりますので、電子契約運用後の適切な内容に修正が必要となります。

5. トラストサービスに関する国内外の動向

近代私法の基本原則のひとつである「契約自由の原則」は、一般的に以下の自由を指します。
①契約締結の自由：契約を締結し、又は締結しない自由
②相手方選択の自由：契約の相手方を選択する自由
③内容決定の自由：契約の内容を自由に決定することができること
④方式の自由：契約締結の方式を自由に決定することができること
そして、後日締結内容について疑義が生じたときに、関係者間で納得するために、なんらかの記録として残されることになります。

跡形もなく修正・コピーができ瞬時に世界中に発信できてしまうデジタル記録においては、誰が（主体・意思）、何を（事実・情報）、いつ（時刻）という要素について、方式が自由とはいえ、誰もが納得できる標準に則っていることを確認することで信頼できる制度が必要です。
記録が主張されたとおりのものであること（真正性）、改ざんされていないこと（完全性）を確保するための社会的通用性が求められるのです。
デジタル社会の発展に伴い、これらを担保するサービスとしてトラストサービスが、国内外で整備が進んでいます。

5-1. EU におけるトラストサービス

ＥＵ委員会は、2010 年５月に、欧州デジタル・アジェンダの行動計画を発表しました。全体目標として、「超高速インターネット及び相互接続可能なアプリケーションを基盤とする『デジタル単一市場』の創設から、持続可能な経済的・社会的便益が得られるようにすること」を掲げ、７つの優先課題を明確にしました。
【１】活力あるデジタル単一市場、【２】相互運用性と標準化、【３】信頼性向上と情報セキュリティ、【４】高速及び超高速インターネットアクセス、【５】研究とイノベーション、【６】デジタル・リテラシー、スキル及びインクルージョンの向上、【７】ＩＣＴが可能とするＥＵ社会への恩恵
そして、ＥＵの加盟国内でデジタル単一市場として電子取引の適切な機能を確保するために、
「電子署名の分かりにくさ」と「ビジネス視点不足」が、域内加盟国間での相互運用性を阻害していると結論づけ、それまでの e-Signature Directive（各国内法への置き換え指示である指令）を破棄して、加盟国で同一の規制内容である直接法として、電子本人確認（eID）

と電子トラストサービス（eTS）に係る Regulation として eIDAS[17]を 2014 年７月 23 日に成立し 2016 年から施行しています。

さらに、eIDAS 第４９条に規定されているレビュープロセスによって実施されたレビューの結果、現状の eIDAS では、eID スキームの適用範囲がＥＵ人口の５９％に限定されていることが判明し、より利活用されるべく、大きく見直しが検討され、Proposal[18]が 2021 年６月３日に発出されました。
この Proposal では、属性情報まで含むことができるＥＵデジタルＩＤウォレットが規定され、リモートのための適格電子署名と適格 e シールの生成装置の管理についての規定が加わり、新たなトラストサービスとして、属性認証、適格アーカイビングサービス、電子台帳サービスが追加されています。

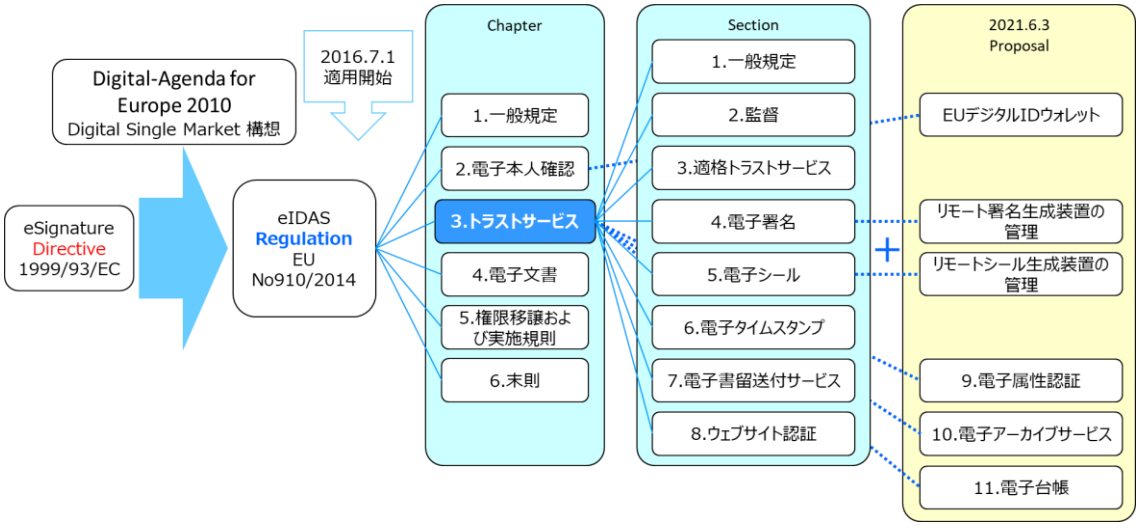

図 18　eIDAS

17 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
18 https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation?fbclid=IwAR2lBn9zUQyY10ThoJ20q3rVK1APfs8-R18h90sIGAsbpnqUm-xQ3DYt7dk

5-2. 世界的な動き

国際商取引法の調和を図るため、条約・モデル法・立法ガイドラインなどを策定する機関として 1966 年に創設された、国際連合国際商取引法委員会（UNCITRAL）の電子商取引に関して検討している第４部会（WG-Ⅳ）[19]において、2011 年ごろから、Identity Management (IdM) and Trust Services について作業候補として挙げられ議論されています。

2019 年の第 58 回会議にて、国際商取引の障害として以下の４点があると整理されました。

① IdM とトラストサービスに法的効果を与える法制度が無いこと

② システム間の相互運用性の問題

③ 紙ベースのものを求める法制度の存在

④ 国ごとに異なる法制度の存在とクロスボーダー相互の法的承認メカニズムの欠如

そして、これらの障害を取り除くには、IdM and Trust Services 利用への信頼を高めるための法的裏付けが必要であり、そのためには、サービス提供者など当事者の義務や責任などを明確化することが重要であるとされ、法的承認及び相互承認を作業目標として特定されました。

2021 年７月現在、条文の形で、作業文書

″Provision on the Use and Cross-border Recognition of Identity Management and Trust Services″[20]が策定され、2021 年秋の第 61 回での最終化を目標に議論されています。

第１章 総則、第２章 IdM、第３章 トラストサービス、第４章 国際的側面の４章構成で、トラストサービスについては、トラストサービスの法的効果と、トラストサービスとして、電子署名、e シール、タイムスタンプ、電子アーカイビング、e デリバリ、web サイト認証が規定されており、それらサービスの信頼性判断要件、指定、責務が規定されています。

成果物の形式は未定ですが、国家間でのやりとりとなることから、統一的な規範となるモデル法として提案されることになると推定されます。

[19] https://uncitral.un.org/en/working_groups/4/electronic_commerce

[20] https://undocs.org/en/A/CN.9/WG.IV/WP.167

5-3. 我が国の動向

我が国においても Society5.0 を実現するためには DFFT を確保する仕組みが必要であるとの認識から、総務省において「トラストサービス検討ワーキンググループ」で検討され、2020 年２月に最終とりまとめが整理されました。この内容は、統合イノベーション戦略 2020 に組み入れられ、総務省内での具体的な施策として国際的な相互運用性を確保すべく、制度化の推進が検討されたところです。
2021 年４月には、総務省告示第 146 号[21]が発出され、これまで民間の認定制度であったタイムスタンプについては、新たに総務大臣認定制度が開始されました。
また、これまで未定義だった、電子文書の発出元を証明できる仕組みについて、e シールに係る指針[22]として公開されました。この指針において、e シールを「電子文書等の発行元の組織等を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組み」と定義し、今後、国が一定程度関与した基準に基づく認定制度を具体化することが示されています。

さらに、COVID-19 の影響による急激なデジタル社会化のなかで、浮彫りとなった脆弱な安心・安全のための基盤の早急な整備が必要とのことから、デジタルガバメント閣僚会議の「データ戦略タスクフォース」で喫緊の取組としてトラストの枠組みの整備が挙げられました。[23]
トラストの枠組みの整備については、「トラストに関するワーキングチーム」において議論検討された結果
-電子署名法や公的個人認証法など個別の制度構築がなされているが、データ社会全体を支える包括的なトラスト基盤が必要
-意思表示の証明、発行元証明、存在証明等のトラストサービスに共通する水平横断的な一般原則と共通要件を整理し、認定スキームを創設することが必要
-その際、国際的な同等性などを配慮した国際相互承認を念頭に置いて検討する。
と整理され、認定のスキームの想定イメージとして、図 19　認定スキームの想定イメージが示されています。

[21] https://www.soumu.go.jp/main_content/000742664.pdf
[22] https://www.soumu.go.jp/main_content/000748208.pdf
[23] https://www.kantei.go.jp/jp/singi/it2/dgov/dai10/siryou_a.pdf

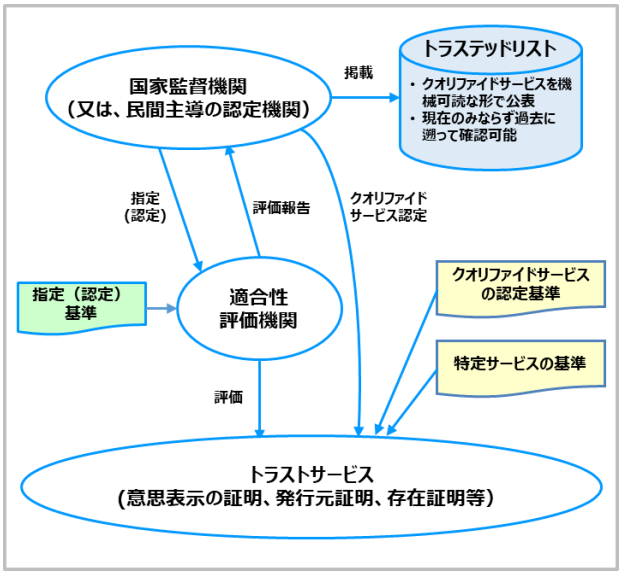

図 19　認定スキームの想定イメージ

このトラスト基盤の構築（認定スキームの創設）は、「包括的データ戦略」[24]の第５層に位置付けられ、ルール分野の重点項目として、「デジタル庁を中心として関係省庁が協力して、2020 年代早期の実装を目指す」こととなりました。

[24] 2021 年 6 月 18 日閣議決定
https://cio.go.jp/sites/default/files/uploads/documents/210618_01_doc03.pdf

5-4. 海外におけるクラウド型電子契約サービスの判決例

クラウドでの電子署名サービスがその利用しやすさから、国内外で展開されています。デジタル署名を利用する電子署名は、本人の意思で本人の管理下にある唯一の署名鍵を利用することで、対象情報内容において、本人意思が含まれていることを示すことになります。ここで、この署名鍵が署名した本人の管理下にあるものであることが重要になるため、一般的には、当該署名鍵のペアである公開鍵に対して第三者である認証局が、本人確認をしたうえで、認証局の電子署名をすることで発行される電子証明書によって担保することになります。

クラウドサービスによる電子署名のうち、現在「事業者型」とか「立会人型」といった名称のタイプのサービスは、上記のように署名鍵への電子証明書を発行する方法とは、別の手段で、本人確認と本人意思確認を実施し、事業者の署名鍵による電子署名をすることで、一定程度の対象情報の真正性を担保する方式のサービスです。

この場合、実際に署名した本人から、否認される可能性を残すこととなり、実際に海外では、本人否認による裁判が行われ、本人意思が認められず、契約が成立しない判決例も出ているので、契約内容のリスクを鑑みて利用を検討ください。以下にその事例を紹介します。

5-4-1. オランダの事例[25]

判決日：2020 年 10 月 7 日

ケース番号：8077607 CV EXPL 19-4084

内容：個人役員を保証人としたビジネスローンの電子契約。

判決文によると

本裁判で対象となった SMS を利用して署名者本人を特定するクラウド型の電子署名については、署名者が提供した電話番号に SMS で受信したコードは、署名者が「単独の管理下で、高い信頼性をもって」使用できるものではないとし、この電子署名が使用された目的である、相当額の貸付契約に基づく義務の履行のために、取締役が法人の保証人となる契約の締結を考えると、この電子署名は、十分に信頼できるものとはいえず、手書きの署名に添付されている同じ法的な結果ではないと判断され、

「この電子署名は十分に信頼できるものとはいえず、自然人である署名者とデジタルデータとの間には、この場合と保証契約との間の関係は成立しない。したがって、電子文書は保釈契約締結のやむを得ない証拠とはならない。」

と結論されています。

[25] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBZWB:2020:4817

5-4-2. カリフォルニアの事例[26]

判決日：2019 年 11 月 19 日

ケース番号：No. D075519

内容：一般家庭において太陽光発電システムが不適切に設置。業者と契約者間での電子契約において契約者が署名したことを立証できなかった事件。

訴訟対象の業者は、クラウド型電子契約のクラウドサービス事業者による電子署名によって、原告が 2017 年２月 28 日に太陽エネルギーシステムの設置資金を調達するために契約を「締結」したと主張したが、原告は、契約書に物理的にも電子的にも署名しておらず、原告の電子署名と称されるものは、本人の同意、承認、知識なしに契約書に「置かれた」ものであると主張した事件であり、控訴裁判において、被告側が十分な証拠を提示できなかったことから、原告の主張が認められ当該契約は締結されていないと判断されました。

この控訴裁判において、説明が求められ、被告側が証明できなかった内容は以下の通りです。
- 誰が原告に契約書を送付したか、
- 契約書をどのように彼女に送付したか、
- 原告の電子署名をどのように契約書に記入したか、
- 署名された契約書を誰が受け取ったか、
- 署名された契約書をどのように事業者に返却したか、
- 契約書に実際に署名した人物として 原告の身元をどのように確認したか
- 契約書が署名された具体的な場所
- 契約書が署名された時間
- 契約書が署名されたときに原告がいたことをどのように確認したか。

26 https://scholar.google.co.jp/scholar_case?case=9895567310196832704&q=Fabian+v.+Renovate+America&hl=en&as_sdt=2006&as_vis=1

さいごに

本ガイドラインでは電子契約とそれを取り巻く要素について、各章で述べてきました。ビジネスでは、多くの取引先と様々な文書（見積書、注文書、請書、請求書、基本契約書・・）が日々取り交わされています。非対面手続きが求められる昨今の社会情勢を鑑みても、電子契約は業務効率化、コスト削減に対して有効な手段となっています。そこで、取引の相手先や契約内容の重要性、本書に記載した法令・制度、技術、運用のポイント、国際的な動向などを加味して、様々な電子契約サービスの利用形態の中から適切なサービスを選択し、利用することが重要になると思われます。

本書が電子契約活用の一助となりますと幸いです。

電子取引委員会　作成・監修メンバー

委員長	西山　晃	フューチャー・トラスト・ラボ
副委員長	岡本　敦	サイバートラスト株式会社

（委員　社名 50 音順）

委員	渡辺 弘幸	サイバートラスト株式会社
委員	牛島 直紀	ＧＭＯグローバルサイン・ホールディングス株式会社
委員	稲葉 厚志	ＧＭＯグローバルサイン株式会社
委員	柴田 孝一	セイコーソリューションズ株式会社
委員	相良 直彦	セコムトラストシステムズ株式会社
委員	飯嶋 高志	寺田倉庫株式会社
委員	山下 誠路	株式会社ＴＲＥＡＳＵＲＹ
委員	齋木 康二	日鉄ソリューションズ株式会社
委員	植木 伸補	株式会社日立ソリューションズ
委員	大川 洋史	株式会社ワンビシアーカイブズ

担当理事	小澤 行男	株式会社ジェイ・アイ・エム
事務局	甲斐荘 博司	日本文書情報マネジメント協会

電子契約活用ガイドライン　Ver.2.0

発行者：公益社団法人　日本文書情報マネジメント協会(JIIMA)　電子取引委員会

発　行：2021 年 10 月

問合せ：公益社団法人　日本文書情報マネジメント協会　電話　03-5821-7351

https://www.jiima.or.jp/about/contact/