電子文書信頼性向上ガイドライン

第 1 版

2019 年 3 月 28 日

公益社団法人日本文書情報マネジメント協会

政策提言プロジェクト／電子文書信頼性向上タスクフォース

はじめに

JIIMA は 60 数年の長きにわたり文書情報マネジメントの普及に取り組んでおり，その対象はマイクロフィルム，電子化文書（スキャナー文書)，そして現在は電子文書と変遷している。直近の JIIMA ビジョンでは“安心で社会生産性の高い電子文書社会の構築”を標榜している。

その一方で，現在の日本社会ではまだまだ紙文書信仰が強く電子文書の普及が遅れている。確かに電子文書は，扱いによっては不安定な面もあり利用を避ける人も多いが，適切な扱いをすれば紙よりはるかに便利で，処理能力も高い。

日本国自身は長年紙文書を優先して来たが，最近，公文書の電子化に舵を切り，デジタルガバメントを宣言し，デジタルファーストを法制化するなど電子文書中心の施策を進めている。

このような状況の下，電子文書の信頼性を高め，情報セキュリティ上の懸念や証拠能力の不安を払拭し，電子文書が組織間，企業間で流通し出来るよう本ガイドラインをまとめた。

これにより，電子文書が電子たる利便性に加え紙文書と同等またはそれ以上のものとして扱われ，電子文書社会の構築に寄与することを願っている。

目次

用語

文書

文字，その他の記号，画像などの手段で記録媒体に記録したもの。コンテンツ，コンテキスト及びストラクチヤから構成される。

文書情報

組織が職務上作成又は取得した文書。

書面

紙媒体に記録された文書情報。

電子文書

電子的な手段によって作成された文書情報。

電子化文書

スキャナなど文書読取り装置を利用して書面を画像情報として電子化した文書情報。

本ガイドラインでは，「電子文書は電子化文書を含む」と広義に解して記述している。

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。

電磁的記録の定義は法律により異なる。本ガイドラインでは刑法 7 条の 2 の定義を用いる。

証拠

特定の紛争における，真偽や違法行為の存否を判断する根拠となるもの。

証拠力

文書が訴訟における証拠としての効力。民事訴訟では，証拠としての効力を持つための前提条件として形式的証拠力（真正な成立の証明＝文書の作成名義人の意思で作成された文書であることが証明され，本人の意思の表現であると認められること）が必要。

証拠能力

裁判手続において証拠として用いることができるか否かの基準。刑事訴訟では，伝聞情報の原則禁止などの条件がある。民事訴訟では，あらゆる文書が証拠能力を持つ。

証明力

裁判官の心証への影響力という意味での証拠の実質的「価値」。

完全性

電子文書及び他の文書情報との関係が書換え（改ざん・すり替え）られていない性質。

検索性

電子文書が，速やかに検索できる性質。見読性（文書情報が作成されてから，人が継続的に理解できるように維持される性質）確保のための要件の一つ。

真正性

文書の作成者とされている者によって実際に作成されたという性質。

正当性

文書が権限，業務によって正しく作成されている性質。

信頼性

正当性の全体的，総合的な確信の度合い。

信用性

証拠として提出された文書が，真実であると裁判官などの第三者が信用するに至る度合い。

メタデータ

文書情報に関する管理付属情報。プロパティ又はアトリビュートともいう。

コンテキスト

メタデータの一種。環境周辺情報。電子文書が作成された経緯，作成時期，作成者，配布先などの情報及び保存状況。

長期保存

あらかじめ決められた保存条件で，長期間にわたり，文書の保存・管理を行うこと。

電子署名

文書情報に作成者及び／又は承認者の意思を表示する電子的な情報であって改ざん検知が可能なもの。

タイムスタンプ

文書情報がその時刻に存在したことを確認できる時刻情報。

記録媒体

文書を記録する媒体。記録メディアともいう。

1. 目的

本ガイドラインの目的は，電子文書の信頼性を向上させることにより，組織等における文書の電子化，及びその効果的な利用を推進していくことにある。電子文書については，情報セキュリティ上の懸念が残っているほか，訴訟等の手続における証拠能力についても不安がある。そのため，電子文書利用による効果が十分に享受されない状況が続いている。

そのような状況を改善するため，本ガイドラインでは，電子文書の信頼性向上のための施策を提示する。

2. 適用範囲

本ガイドラインは，組織で職務上，作成又は取得した情報を対象とする。また，伝送途中の情報など一時的な情報は対象とせず，記録媒体に格納された情報だけを対象として，その信頼性を確保・向上させる施策について述べる。

3. 電子文書の信頼性

信頼性向上の目標について，明確な基準は存在しないが，本ガイドラインは，通常行うべき施策を示す他，特に重要な情報が対象になる場合にとるべき施策や，やや簡易な施策ではあるが過渡的な状況等において用いるものについても示す。

3.1 背景・必要性

3.1.1 背景

組織活動において，従来の紙文書に代わって電子文書を用いることが多くなってきている。特に，組織内においては，文書作成や決裁を電子的に行うワークフローの普及が進んでいる。組織内は電子化されていても，外部に対する文書については，紙を利用していることがまだまだ多い。これは，文書の相手方が紙を要求しているケースがあるだけでなく，電子文書の信頼性に不安を感じることが多いように思われる。

電子文書の信頼性が問題になる理由として，改ざん，消去等のおそれがあること，作成者の特定が可能かどうかに不安があること，それらにより，訴訟などの法的手続きにおいて証拠としての効力を持つかどうかにも不安があることなどが挙げられる。

3.1.2 必要性

このように，電子文書に対する信頼性は一般的には高いとはいえない状況にある。組織活動において，紙に代えて電子文書を活用していくためには，信頼性を持たせるための施策の設定と，その確実な実施が必要である。

最近は，紙文書による不動産取引において印鑑証明書の偽造が報じられるなど，紙文書の一般的な信頼性が低下している状況にある。情報セキュリティの適切な施策を講じれば，電

子文書は紙よりもはるかに安全な利用・運用が可能になる。この点も踏まえて，電子文書の信頼性向上の施策を述べていくこととする。

3.2 信頼性と信用性のとらえ方

方策の提示に先立って，本ガイドラインにおける用語について，簡単に述べるとともに，信頼性が求められる場面を分析する。これらに基づいて，場面や文書の種類等を前提条件とした方策を示すこととする。

3.2.1 定義

信頼性の高い電子文書について論じるにあたって，「信頼性」及び「信用性」についての本ガイドラインにおける考え方を示しておく

① 信頼性

文書の成立や保存が正当であると考えられる度合い。周辺の事情などを含めて総合的に評価される。信頼性の判断には，信用性も大きく影響する。つまり，信頼性は，正当性の全体的・総合的な確信度ともいうべきものであり，信用性に比べると抽象的な性質だと考える。

② 信用性

内容が真実であると信じられる度合い。主として，裁判所の心証を想定するが，紛争における相手方や第三者が信じる度合いをも含む。

信用性について，民事訴訟法では裁判官の自由心証に任されているが，刑事訴訟においては，伝聞証拠の採用に関する要件となっている。また，海外の法制でも，信用性が高いものに証拠能力を与えていると思われるものがある。これらの法制度は，民事訴訟における信用性を論じるために参考となるものであり，第４章にて詳しく述べることとする。

3.2.2 信頼性が求められる場面

電子文書の信頼性は，その文書がどのような場面で必要とされるかによって，求められる内容に違いがある。ここでは，以下の３項目に分けて考える。

① 外部から受領する文書

外部から受領する文書は，その作成者の責任の範囲を示すために使われることが多い。このような場合には，第三者から見て，作成者の真正性（その文書の名義人が，実際にその文書を作成したこと）が重要となる。また，内容については，その文書の成立の経緯などが，信用性に影響することが多い。したがって，作成者および（文書受領に至る）成立の経緯などが明らかになる施策が求められる。

② 外部へ提出する文書

外部に提出する文書は，受領側が使用するものであるから，基本的には，受領側のポリシーに従って作成すべきである。しかし，そのようなポリシーが明確でない場合には，①に準

じた施策を行うことが望ましい。

③ 内部での責任追及・正当な手続の提示／説明のための文書

内部で利用するために作成される文書であっても，訴訟等で有効なものとなるものも多い。例えば，以下のような場合に，その信頼性が問題となりうる。

- 組織内の者に対する，責任追及・処分等のための資料として電子文書を用いる
- 組織内で正当な手続を踏んでいたことを，官公庁や，利害関係のある第三者に示す

このような場合を想定して，施策を考える必要がある。

文書の種類等，具体的な対象については，第 6 章で述べる。

4. 法制度

ここでは，法制度からみた証拠としての電子文書（電磁的記録）の取扱いを確認しつつ，法制度にも対応できるような電子文書の信頼性確保の方法論について述べる。

電子文書の裁判手続での利用に当たって課題になるのが電子文書の内容についての信用性である。電子文書が類型的に信用できないのであれば，証拠調べの対象になる(証拠として法廷で使用される)べきではないし，逆に，類型的に信用性が低くなるという傾向がみられないのであれば，形式的なルールの面での障害があったとしても，証拠として使用することについて支障はないことになる。

我が国の裁判手続は，主に民事訴訟法によって規律される民事手続と，主に刑事訴訟法によって規律される刑事手続とに分けることができる。

4.1 電子証拠と訴訟

我が国の訴訟は，民事訴訟法が適用されるものと刑事訴訟法が適用されるものとに大別される。このうち，民事訴訟法における証拠の取扱いでは伝聞法則が適用されないが，刑事訴訟法においては伝聞法則が大きなルールとして存在する。（**表 4.1**）

表 4.1　我が国の訴訟法と伝聞法則

	民事訴訟法	刑事訴訟法
伝聞法則の適用	なし	あり

伝聞法則においては伝聞証拠と呼ばれる一定の証拠[1]について，類型的にその信用性を評価するので，まずは，電子証拠と伝聞法則との関係を確認したい。

[1] 事実についての言明が記載された文書や電子文書であって，その事実の有無を証明するための証拠として用いるもの

4.1.1 伝聞法則と電子証拠

(1) 我が国の状況

刑事訴訟法は，原則として伝聞証拠の証拠能力を認めない(刑事訴訟法 320 条)。ただし，伝聞例外（刑事訴訟法 321 条以下）の要件を充たす場合に，例外的に伝聞証拠の証拠能力を認める。伝聞証拠の証拠能力が原則認められないのは，人の知覚・記憶・表現・叙述の過程のそれぞれに誤りが混入しているリスクがあるからだとされる。したがって，電子文書を証拠として用いる場合には，この点の誤り混入のリスクを低減させることができるか否かが重要になる。

商業帳簿やある程度の継続性を持つ業務の過程で作成された文書は，機械的継続的に作成されたものであって虚偽の内容が記載されるおそれが少なく，作成者に供述をさせるよりもその文書の方が類型的に信用できるため，証拠能力が認められる(刑事訴訟法 323 条 2 号)。これは，業務で電子文書を使う場合についても適用できる。電子文書(電磁的記録)が簿冊（複数の文書をまとめて綴じたもの）の役割を果たしている場合は，記憶装置自体ないし記憶装置から機械的に印字された書面について同号を適用でき[2]，伝聞例外(証拠能力が認められる伝聞証拠)として証拠能力が認められる。もっとも，この場合，刑事訴訟法 323 条 2 号の適用対象になること（航海日誌，商業帳簿その他業務の通常の過程において作成されたこと）は示さなければならず，その際には，作成過程たるコンテキスト情報を立証する必要があることになる。したがって，どのようなコンテキスト情報が重要であるかが問題となる。

(2) 外国からの示唆

この点に関連する外国の議論をみてみる[3]。まず，訴訟における証拠として使うためには，電子証拠が変更(改ざん)されていないことを担保することが重要である。この点，アメリカにおいては，改ざんの有無の検知は困難だと評価されつつも，そのことゆえに電子証拠が許容されなくなるわけではない，とされる[4]。しばしば被告人側からデータの変更が容易であることに基づいた改変の主張がなされるが，裁判所は，改変にかかる特定の証拠がない限りこの主張を認めない傾向があるともされている[5]。電子証拠の使いやすさを物語っている。

そして，カナダでは，電子文書の証拠採用を求めるものは，その真正を立証する責任を負うが(§31.1，原則として記録の外にある証拠を提供して立証することとされる[6])，それを記録等する電子文書システムの完全性の証明を行うことで，その真正の証明が可能だと規定されている(§31.2)。その証明の際の考慮要素として挙げられているのが，データの源泉，事実を記録している場合の事実発生と記録作成との間の時間の短さ，業務過程で作成され

---

[2] 松本時夫＝土本武司＝池田修＝酒巻匡『条解 刑事訴訟法〔第 4 版増補版〕』882 頁(弘文堂，2016)，河上和雄＝中山善房＝古田佑紀＝原田國男＝川村博＝渡辺咲子『大コンメンタール刑事訴訟法 第 7 巻第 2 版』683 頁〔岡部信也＝中川博之〕(青林書院，2012)。

[3] 我が国とは異なり，ここで紹介している議論は民事と刑事の双方の事件で適用される。

[4] 田邉真敏『アメリカ連邦証拠規則』223 頁(レクシスネクシスジャパン，2012)。

[5] Nat'l Inst. of Justice, U.S. Dep't Of Justice, Digital Evidence in the Courtroom: A Guide For Law Enforcement And Prosecutors, p. 31 (2007)

[6] Canadian General Standards Board, “Electronic records as documentary evidence”, p 9 (2017).

たか否か，組織が適用され得る電磁的記録の管理基準を遵守しているか否か，組織が記録システム内の電磁的記録に依拠して意思決定をしているか否か，組織で使っているソフトウェアの信頼性，システムの変更履歴の記録の有無，プライバシーに関する法令遵守の有無，セキュリティの確保の有無である[7]。これらの事情は電子証拠の管理に関する基準を提供している。

4.1.2 電子証拠の訴訟における取扱い

民事訴訟法の下では伝聞法則は適用されず，その代わりに，電子証拠の提出方法に係るより実践的な議論が展開されてきている。ここでは①電子証拠のプリントアウトや②電子証拠に係る記録媒体の取扱いをみる。

①については，プリントアウトした文書はそれ自体が内容を見読できる文書なので，電子文書ではなくプリントアウトだけを文書として証拠提出する。この場合，本来の原本である電子文書とアウトプットの内容の同一性を示すために，結局，電子文書自体を電子媒体で提出する必要が生じかねない。これでは，アウトプットという行為自体やそれを提出する行為に追加のコストがかかる点で電子文書の有する利点を活かしているとはいえない。また，同一の情報が電子文書及びそのアウトプットの形式で存在することにより情報管理のコストが増大することにもなり，情報セキュリティの考え方からしても妥当でない。

そこで，②のように，電子証拠に係る記録媒体を準文書(情報を表すために作成された物件で文書でないもの。民事訴訟法 231 条)として提出することが考えられる。この場合には，その内容を見読するための方法が多様であり，裁判所や他の訴訟当事者にとってどのような方法をとるべきかが必ずしも明らかではない可能性がある。例えば，HTML ファイルのソースが訴訟における重点的な課題になっている場合に，HTML ファイルを焼き付けた記録媒体(USB メモリや CD-R)を提出するだけでは足りない。多くのコンピュータ環境ではそれをダブルクリックすると WWW ブラウザが起動してそのブラウザの設定に従った表示が行われるが，他のブラウザで同じ表示になるとは限らないし，そのソースを閲覧できるわけでもないからである。したがって，表示方法や閲覧方法の共有が必要になる。

我が国の民事訴訟においては，現状においても電子証拠を証拠として使うことができるといえるが，実務上の運用方法次第では，コストの増大を招くことになる点に注意が必要である。

4.2 文書管理のための標準

アメリカやカナダでは，電子証拠が相当程度信頼できる証拠であることに基づいて，その信頼性を担保するための，電子証拠の管理の方法について，一定の議論がある。とりわけ，一定の文書管理のための標準が考慮要素になる，とカナダ政府の資料が明言していることも着目に値する。

---

[7] Canadian General Standards Board, “Electronic records as documentary evidence”, p 10-11 (2017).

その一方で，我が国の手続法は，電子証拠を許容しようとしているものの電子証拠の特徴を活かそうとする明示的な規定を持ってはいない。しかし，民事裁判の IT 化が進められようとしている我が国の現況[8]にも鑑みると，我が国においても電子証拠の信頼性の確保のための施策が必要である。法制化による実施が最も望ましいが，それを待つことなく，民間においても，電子証拠の信頼性を担保するような電子証拠の取扱い方式の標準の議論を進めていく必要がある。

5. 推奨方式とその考え方

ここでは，前章までの背景を踏まえて，一般的な電子文書の信頼性を確保するために重要と思われる施策を列挙する。電子文書の内容などによって，必要な施策のレベルは異なってくると考えられるため，すべての文書に対応する施策を定めることは困難である。そこで，本ガイドラインでは，多くの電子文書に共通に必要となる施策のセットを，推奨方式として提示することとした。

従来の諸ガイドライン等では，セキュリティのレベルとして，高・中・低などの複数のレベルを設定し，それらを満たすための施策を記載していた。しかし，具体的な場面において，高・中・低のうちのどれを採用すればよいかという問題があり，ガイドラインの利用促進の障害になってきた。

本ガイドラインでは，一般的な利用を対象とする「推奨」と，より高い信頼性を確保するための「厳密」，そして事情によって「推奨」が実現できない場合に備えた「簡易」の３つのレベルを提示する。

5.1 重要なポイント

電子文書が信頼性を持つためには，大きく分けて２種類の施策が考えられる。一つは，電子署名やタイムスタンプのようなメカニズムによる，情報そのものが持つ証明力であり，もう一つは，作成・取得経緯，文書に対するアクセス等の記録による，いわばプロセスによる証明力である。電子文書が類型的に信用性を持つと考えられるケース（前章参照）に鑑みると，後者については，独立な運用主体による正当な記録・保存が行われていることが重要な意味を持つ。特に，組織内での処理の正当性を示すために，この点は重要といえる。

5.2 個別法への対応

本ガイドラインでは，会社法等の一般的な法令で定められた措置については，その施策について言及する（例えば，取締役会議事録への電子署名）。

一方，業法等の特定の事業領域に関する法令により，一定の措置が法定されている電子文書がある。例えば，建設設計分野，医療情報分野，金融・銀行分野などである。業法を網羅する記載は本ガイドラインのスコープを逸脱するものと考えられるので，このような措置

[8] 「裁判手続等の IT 化検討会」 https://www.kantei.go.jp/jp/singi/keizaisaisei/saiban/index.html

については，本ガイドラインでは記載しない。これらについては，各領域のガイドラインを参照されたい（付録 E 記載の JIIMA 発行のガイドラインにも事業領域に係るものがあるので参考にしていただきたい）。

5.3 推奨方式

通常の利用において，十分な信頼性が得られると考えられる施策を，推奨方式を用いれば相当の信頼性が得られると考えている。一般的な電子文書の利用にあたっては，このレベルの施策を推奨するという趣旨である。

推奨方式を策定するにあたっては，記録管理の国際標準である ISO 15489-1[9]及び ISO 30301[10]，メタデータの標準である ISO 23081-1[11] などを参考に，プロセス定義や対象となる情報の枠組を策定した。ここから信頼性についての施策を抽出し，組織で活用するために具体化した。これに基づいて，JIIMA において専門家の討議を経て推奨方式として策定したものである。

5.4 厳格方式

より重要性の高い電子文書等に対応するため，厳密な施策を示す。本ガイドラインでは，厳格方式をとるべき電子文書の明確な判断基準は示さない。厳格方式をとるかどうかは，組織の経営判断の一環として考えるべき課題である。なお，一般的には，問題が発生した場合のインパクト（金銭的損害，事業上の不利益，その他）と，その問題が発生する可能性の大小をもとにリスクを評価し，リスクの大きいものについて厳格方式をとることが多い。

5.5 簡易方式

簡易方式として示す施策は，推奨方式よりも低いレベルのものとなる。これは，過渡的な状況等，なんらかのやむを得ない事情においてだけ採用すべきものである。簡易方式は，このようなやむを得ない場合であっても，最低限，満たすべきものとして記載したものと理解されたい。

なお，簡易方式を採った場合には，可及的速やかに，推奨方式に移行すべきである。

6. 対象文書

保存管理の対象となる電子文書は多岐にわたる。本ガイドラインでは，対象文書を**表 6.1** のように類型化した。

---

[9] Information and documentation -- Records management -- Part 1: Concepts and principles 記録管理の概念及び原則

[10] Information and documentation -- Management systems for records -- Requirements 記録のためのマネジメントシステムー要求事項

[11] Information and documentation -- Records management processes -- Metadata for records -- Part 1: Principles 記録のためのメタデータの原則

表 6.1　電子文書の類型

類型	特質		例
A	外部と取り交わす電子文書	意思表示	契約書，注文書
B		通知	見積書，請求書
C	内部の電子文書		稟議書
D	公的文書，その他		法令により必要とされる記録

6.1 外部と取り交わす電子文書(類型 A, 類型 B)

企業等が，他の企業等の外部に交付し又は外部から受領する電子文書は契約書等多数のものがある。これらのうち，外部から受領したものは，訴訟等の証拠になりうるものが多い。また，取引に関する電子文書は税法上の保存義務があるため，外部から受領したものだけでなく，外部に交付した文書の控えも，7 年から 10 年の期間にわたって保存する必要がある。

以下に示す電子文書の形態は，一つのファイル，複数のファイルの組み合わせなどが考えられるが，電子メールによる意思表示や通知もありえる。詳しくは，JIIMA 発行の「電子取引 取引情報保存ガイドライン」を参照願いたい。

外部と取り交わす電子文書は，大きく次のように類型化される。

(1) 意思表示を表す文書（処分証書）など，法的行為・事実を表すもの（類型 A）

- 契約に関するもの： 契約書，注文書・請書，借用書
- 契約後の行為に関するもの： 領収書，検収書
- その他： 誓約書，預金通帳，預り証

(2) 通知に関するもの（類型 B）

- 見積書，請求書，納品書

6.2 内部の電子文書(類型 C)

内部で利用するために作成される文書であっても，訴訟等で有効なものとなるものも多い。以下に示すものは，その例である。

(1) 先使用権確保など知的財産権に関するもの

- 企画書，計画書，研究ノート等

(2) 企業内部での責任追及に関するもの

- 社内会議議事録[12]
- 稟議書
- 決裁記録（ワークフローの記録など）

(3) その他コンテキスト情報になりうるものなど

- システムログ
- 電話通話内容記録，訪問報告書
- ノート，メモなど（個人管理のものが多い。メールでのやり取りも含まれる）

[12] 社内会議議事録のうち，取締役会議事録については，別途，6.4(1)に記載する。

6.3 法令により必要とされる記録（類型 D）

法令により作成，提出，（官公庁以外への）交付，保管等が必要な文書は，このカテゴリに入る。典型的な文書例としては以下のものが挙げられる。

- 公的申請書，届出書等
- 法令により必要とされる記録など
- 議事録（外部との会議などに関するもの）
- 設計図書
- プロジェクト報告書等の報告書

これらの文書については，類型 A～C としての扱いに加えて，法令上の要件を満たす必要があるものが多い。具体的な要件については，本ガイドラインでは述べないので，該当する法令を参照されたい。ただし，多くの組織に共通に適用される一般法については，次節にて述べる。

6.4 一般法や個別法への対応

一般法や個別法で電子文書の作成，保存に関する信頼性確保のための措置が示されているものを例示する。

(1) 会社法（第 369 条第 4 項）

取締役会議事録について，電子データで作成されている場合は，同法施行規則第第 225 条により電子署名法 2 条 1 項に規定するものと同様の電子署名を付与しなければならないとされている。また，電子的に作成した議事録を「商業・法人登記」の申請書の添付書面として提出する場合は，法人代表者等，登記所に印鑑を提出した者は電子認証登記所登記官が発行した電子証明書を用い，取締役会に出席したその他の者は公的個人認証サービスの電子証明書または，政府認証基盤のブリッジ認証局と接続する民間の認定認証局のうち法務大臣の指定する電子証明書を用いる必要がある。（詳細は，法務省のホームページ> 登記-商業・法人登記-> 商業・法人登記の申請書の添付書面を電磁的記録で作成している場合について > ご利用の手引き，参照）

尚，電子証明書の種別については「付録 D 電子証明書の信頼性」を参照されたい。

(2) 電子帳簿保存法[13]（第 10 条）

電子取引の取引データは，電子帳簿保存法第 10 条に保存義務が規定されている。

電子帳簿保存法では，電子取引は次のように定義されている。「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書類に通常記載される事項をいう。）の授受を電磁的方式により行う取引をいう。」（電子帳簿保存法第 2 条第 6 項）

つまり，インターネット取引や電子メール，EDI，その他の手段で取引先との間で取引情報の授受を電子的に行った場合は，授受後遅滞なくタイムスタンプを付すか，または正当な

[13] 電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律

理由がない訂正及び削除の防止に関する事務処理規程を定めて運用する等，法令の要件に従って保存する義務が生じるということである。電子取引の取引情報は，紙に出力して保存する場合を除き，電子保存することが義務となるため注意が必要である。

(3) 電子委任状の普及の促進に関する法律

法人が行政手続を電子申請で行う場合や契約締結を電子的に行う場合，法人代表者名義で行うことが多くあるが，実際は法人代表者自ら行う場合は少なく，当該業務を委任された役員または従業員が実施する場合がほとんどである。そのように受任者が手続きを行う場合の電子化を促進するために「電子委任状の普及の促進に関する法律」が 2018 年 1 月に施行された。同法では受任者が法人代表者から委任を受けた者であることを示す「電子委任状」の信頼性を確保するための基本的な指針が示されている。（詳細は，「付録 C　電子委任状」参照）

7. 信頼性向上策

7.1 信頼性向上策の概要

文書の真正性，すなわち「作成者であるとされる者が実際にそれを作成したこと」を証明し，かつ，その文書の内容が真実であると信用されるようにするには，十分な対策を講じなければならない。特に，企業活動における文書は，企業活動の実体が反映されたものであり，組織的にオーソライズされた業務のなかで，権限のある者が作成し，承認が行われることが重要である。

証拠としての文書に要求される第一の事項は，どのような環境で作成または取得された文書であるかが保存期間を通して確認できることである。作成・取得環境についての確かな情報があることにより，証拠としての信用性が高まるためである。作成・取得環境の情報については次節で詳述する。

証拠としての文書に要求される第二の事項は，文書の真正性，成立時期，および完全性（改ざんされていないこと）が保存期間を通して確認できることである。

外部から取得した電子文書，特に意思表示に係るものは，真正性が非常に重要である。相手方の電子署名がある場合には，それにより真正性を証明できることが多いが，電子署名がない場合には，周辺情報の積み上げで証明することになり，周辺情報の取扱いが特に重要となる。押印された紙で受け取った文書をスキャナで読み取り，（紙の原本を破棄して）電子データのみを保存する場合，電子データは原本ではなく写しの扱いなので，押印による真正性の推定（民事訴訟法 228 条 4 項）は得られない。この場合も，電子署名のない電子文書の受領と同様に，周辺情報が重要な役割を持つ。

見積書等の通知文書については，その電子文書の発行元（発信元）たる企業が明確であれば，作成した個人を特定することには大きな重要性はない。設計書・報告書や，外部との会議等の議事録などについては，関係者に通知したことや成立時期などのコンテキスト情報が，真正性よりも重要な場合が多い。

内部の文書については立証趣旨(利用目的)に応じて場合分けが必要である。

まず，内部の責任追及のための文書については，外部の文書と同様，真正性が重要である。取締役会議事録のように，経営陣が関与している情報の保存にあたっては，システム管理部門等もその指揮命令下にあるため，管理の独立性などを十分に留意する必要がある。内部文書一般について，成立時期の証明が，信用性や真正性の証明の間接証拠（状況証拠）となるケースが多い。たとえば，会議開催直後に作成された議事録の内容は真実である可能性が高いため，成立時刻の証明により信用性を高めることができる。また，システムログ等が紛争のはるか以前に改ざんされることは，ほとんどありえないことであるから，システムログの成立時期の証明は，システムログの内容の信用性を高め，ひいてはそのシステムログにより示される電子文書の真正性の証明に大きく寄与することになる。

一方で，社内文書においては，真正性よりも成立時期が相対的に重要になる場合もある。例えば，先使用権等の知的財産権に係る電子文書は，成立時期が最も重要である。このような内部文書については，企業内部の者が作成したことが示せれば十分なケースが多いため，作成者の真正性はそれほど高い重要性を持たない。なお，相手方に交付した電子文書等の控え（紙で交付する文書をスキャンしたデータを含む）については，その成立時期は，相手方に交付したことの周辺情報として有効である。この場合にも，社内における作成は明らかであり，真正性よりも成立時期の証明が重要である。

真正性や成立時期を示す際に重要な点は，完全性，すなわち，文書作成のときから内容が変更されていないことである。仮に文書の内容が変更されているとすると，現在の文書内容は真正性や成立時期が証明できる内容とは異なるものになってしまう。この点から，文書の完全性は，真正性及び成立時期の証明の基盤であり，完全性なくしては，真正性や成立時期の証明もできなくなるといえる。

7.2 保存すべきコンテキスト情報

7.2.1 文書とコンテキスト

文書は，コンテンツ，コンテキスト，ストラクチャからなる[14]。**図 7.1** に文書の構成要素のイメージを示す。　ここで，コンテンツは文書の内容そのもの，コンテキストは法的・社会的環境，ビジネス環境，作成・取得環境などであり，ストラクチャはコンテンツを収容するためのフォームやフォーマットである。

作成者の署名や作成時刻もコンテキストの一部である。文書の内容，即ちコンテンツの信頼性は，作成時にコンテンツが置かれていた環境，即ち，コンテキストの裏付けなしには成り立たない。受け取り側ではコンテキスを含めて信頼性を判断することから，様々なコンテキストのなかで，とりわけ作成・取得環境が重要である。

[14] ISO 15489-1 記録管理の概念と原則で定義されている。原文の用語は“記録”であるが，ここでは“文書”に読み替えている。

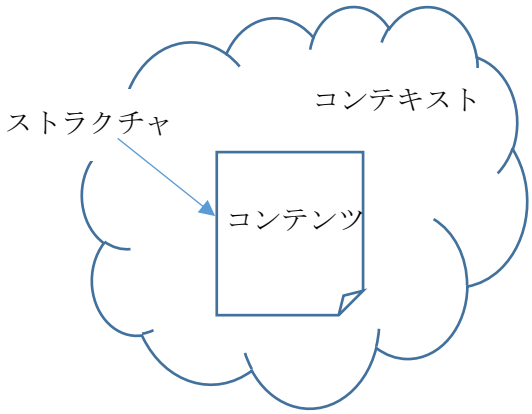
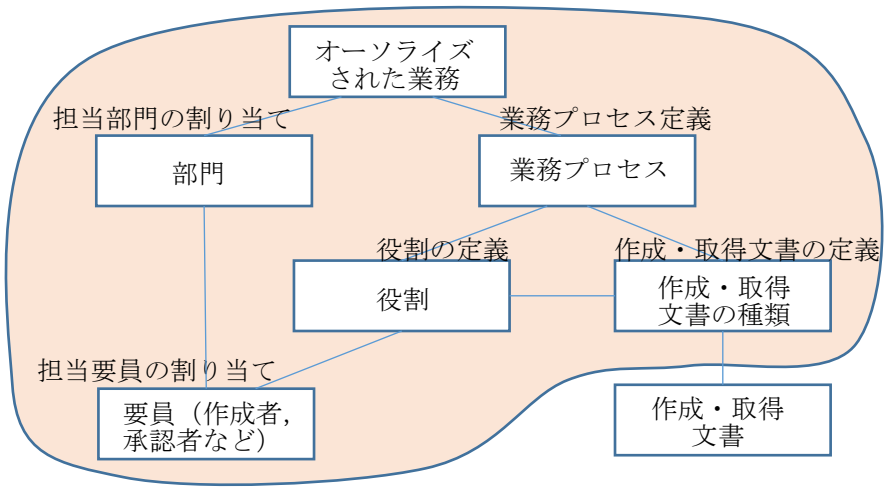


図 7.1　文書の構成要素のイメージ

7.2.2 文書の作成･取得環境

図 7.2 に文書の作成・取得環境（コンテキスト）の構成要素とそれらの関係を示す。組織的にオーソライズされた業務（例えば，資材購入業務）について具体的な業務プロセス（例えば，100 万円以下の資材購入手続フロー）が定義され，その業務プロセスにおける要員の役割分担（例えば，作成者と部長級の承認者）と，作成・取得すべき文書又はそのタイプ（例えば，注文書）が定義される。更に具体化した様式（例えば，注文書のフォーム）を定義する場合もある。また，この業務に対して担当組織（例えば，資材部）が割り当てられ，役割に応じた担当要員が割り当てられる（例えば，承認者＝佐藤花子部長，作成者＝田中一郎）。文書は，この要員によって作成・取得され，図 7.2 に示す構図が保存期間を通して確認できるようになっていなければならない。



□　構成要素

－　要素間の関係

図 7.2　コンテキストとしての文書の作成・取得環境

7.2.3 文書の作成･取得環境の文書化

どのような環境で作成･取得された文書であるかを確認できるようにするには，文書が作成･取得されたときの環境が規程や文書として残っており，文書がこれらと関連付けられている必要がある。例えば，その文書が業務の一環で作成され，部長が承認したのであれば，その業務がオーソライズされた業務であり，その部長はその業務において承認権限をもっていたことを当時の規程や文書を辿って確認できなければならない。

文書の信頼性確保に係る，作成・取得環境を特定する要素を**表 7.1** に示す[15]。

表 7.1　文書の信頼性確保に係る，作成・取得環境を特定する要素

カテゴリ	作成・取得環境を特定する要素
文書	作成日時
	作成者，関係者
	様式
	文書と取引/活動の関係
	関係する文書，ファイルとの関係
業務規程等	文書の作成と管理に関する業務規程/システム統制規程
	メタデータの作成と管理に関する業務規程/システム統制規程
	文書管理運用に関する業務規程/システム統制規程
	アクセスと権限に関する業務規程/システム統制規程
規制等	生成に関する法令・規制要件
	保存，セキュリティ，廃棄に関する法令・規制要件
	文書，文書管理プロセスと法令・規制情報の関係
部門，要員	作成担当者
	承認者
	アクセス権限を与えられた関係者
業務プロセス	文書，要員，取引先，業務/取引/活動の関係
	取引相手
	アクセス規則
	業務分類
	文書の分類
	取引日時

表 7.1 における用語について，以下に説明する。

「文書」の「作成者」「関係者」は，その文書の作成等に実際に関与した者の氏名等を記載する（「部門,要員」は，作成等を行うことが可能な者が書かれる）。何らかの理由により，本来の担当者以外の者が作成した場合にも，実際に作成した者の氏名等を記載する。ここで，「関係者」は，文書作成に関与する者（例えば，予算管理部門などの，当該文書の作成・利用の影響を受ける者であって，文書作成時に関与する者）をいう。「文書」の「様式」は，

[15] これらは，ISO 23081-1 の 9.3～9.5 に規定された要素から，信頼性に関するものを抽出したものである。なお，用語については適宜意訳している。

電子文書のフォーム（記入すべき項目が列挙されており，ここに内容を書き込むことにより，電子文書が作成されるもの）の名称等が記載される。「文書と取引/活動との関係」は，ある取引や活動（例えば，「2019 年度生産設備新規購入活動」）と文書との関係，すなわち，その文書が，どの取引又は活動のために作成されたかを明示するものである。「関係する文書，ファイルとの関係」は，密接な関係のある複数の文書（例えば，見積書と，それに基づく注文書）の関係を示すものである。

「業務規程等」においては，それぞれの区分について，社内規程の名称を記載する。文書に対する規程というよりもシステム統制による管理による記載がふさわしい場合には，システム統制に係る規程の名称を明示する。第 4 章で述べたように，継続性を持つ業務の過程で作成された文書は類型的に信用がおける。したがって，業務規程やシステム統制に係る規程に基づき，組織内で正当な業務として作成等が行われたことを示すことが信用性確保のために重要である。

「規制等」には，当該文書の作成が，法令等による規制（公的機関や業界団体によるガイドライン等がこれにあたる。例えば JIIMA のガイドラインがここに該当する）に基づいて作成が義務付け又は推奨されている場合に，その法令や規制の名称（例えば，法律名と条番号）を明記する。

「部門，要員」には，役割と，その役割につきうる者の組合せを記載する。例えば，作成担当者として「資材部職員」，承認者として「資材部の部長又は課長」のように，役割と，その役割を持つ者の集合を記載する。「文書」カテゴリの「作成者」等が，実際に文書に関与した者であるのに対し，ここでの記載は，要員として割当てられるべき者の集合である。

「業務プロセス」は，当該文書に関連する業務の手順やフローに関する記載である。「業務分類」には，業務名（「資材調達」等，業務の機能をあらわす名称）が記載され，この業務において当該文書の作成が行われる。「文書，要員，取引先，業務/取引/活動の関係」には，具体的な業務（例えば，上期××資材調達業務）と文書や要員の関係（例えば，文書一覧）が記載される。業務プロセスや事務フローは，「業務分類」に記載された業務名から特定することができきる。「取引相手」「取引日時」は，当該文書が社外との取引に関するものの場合に，取引の相手方及び取引の実施日時等を記載するものである。「アクセス規則」には，当該文書にアクセスできる者を特定する情報が書かれる。「文書の分類」には，文書を格納するフォルダ名等を記載する。

7.2.4 本人の意思表示，作成時刻，完全性の確保

本人の意思表示，作成時刻の特定，及び完全性を客観的に検証可能とするための手段として，本ガイドラインでは以下の項目について選択肢を定義し，選択肢の組み合わせ（プロファイルと呼ぶ）を可能とする。

(1) 発行対象

電子証明書又は ID/パスワード（以下，PW）の発行対象。選択肢として，次がある。

① 自然人に対する電子証明書又は ID/PW の発行

② 組織に対する電子証明書 ID/PW 発行[16]

(2) 発行時の本人確認

電子証明書，又は ID/PW を発行するにあたっては，発行対象者が，その電子証明書等を発行されるべき本人であることを確認する必要がある。

本人確認の方法の選択肢として，次がある。

① 信頼性が確認できる機関（WebTrust[17]や ETSI[18]認定などを受けている機関)による本人確認

② 第三者による本人確認

③ 社内での人事 DB 等を用いた一元的確認（社内で公式に認められている情報による確認）

④ 社内での③以外の方法による確認

(3) 作成者の確認

選択肢として，次がある。

① 電子署名

② 第三者システムにおける ID/PW を用いた認証

③ 社内システムにおける ID/PW を用いた認証

(4) 作成時刻

選択肢として，次がある。

① 第三者が提供する時刻証明（第三者によるタイムスタンプ，文書管理等）

② システム内で管理する時刻の記録（データベースへの時刻の記録等）

(5) 取得時の相手確認

(2)と同様。

(6) 改ざん検知・防止

選択肢として，次がある。

① 電子署名又はタイムスタンプ検証

② ソフトウェア統制（付録 A 参照）による不正な変更・削除の防止

(7) 立証

文書の真正性，作成時刻，完全性の証明をの選択肢として次がある。

---

[16] 組織に発行される証明書としては，欧州などで使われている eSeal 用の電子証明書，コード署名用の電子証明書等がある。また，組織としての依頼（例えば送金依頼）のための ID/PW もある。

[17] 米国公認会計士協会およびカナダ勅許会計士協会が共同で開発・管理運営している、認定制度

[18] 欧州の電気通信の全般にかかわる標準化組織の欧州電気通信標準化機構（ETSI：European Telecommunications Standards Institute の略）

① 証明に必要な情報の，文書作成時期における収集。例えば，立証パッケージ（付録B参照）
② ログ監査と関係者の協力など，事後的な情報による証明

7.2.5 文書情報管理システム

ビッグデータをはじめとして大量の情報が流通する時代においては，電子文書を手動で管理することは非効率かつ困難になりつつある。このため，電子文書の管理を文書情報管理システムに委ねることになるが，文書の信頼性を確保するには，システムは次の要件を満たす必要がある[19]。これらの要件を満たすことにより，必要な機能を備えたシステムが，組織が指名した正当な担当者により管理されていることを示すことが可能となる。もちろん，管理規模に応じてその一部または大半を手動で代替することもあり得る。

① 文書化された文書が作成・取得され，作成・取得時点における環境情報が取り込まれ，保存されていること
② 規程に沿った文書管理運用が可能であり，その実施が記録されていること
③ 文書の真正性，完全性が確保されていること
④ 文書の成立時期が記録として確保されていること
⑤ 第三者による①～④の検証が可能なこと
⑥ 目的とする文書が直ちに取りだせること（見読性）

7.3 信頼性を確保する方式

本ガイドラインでは，第5章に述べたとおり，信頼性を確保する方式として，推奨方式，厳格方式及び簡易方式を定める。以下に，これらの具体的な内容を示す。

7.3.1 推奨方式

(1) 推奨方式における作成・取得環境を特定する要素及びプロファイル

推奨方式における，作成・取得環境を特定する要素を**表 7.2** に，また，意思表示の確認，作成時刻の特定及び完全性を確保する方法のプロファイルを**表 7.3** に示す。

表 7.2 は，**7.2.3** において述べたもののうち，標準的に必要と考えられる要素に絞ったものである。ここで，「文書」の「様式」については，すべての文書に様式を定めることを要求するものではなく，様式が定められたものについては，その名称を記載する。また，「規制等」については，該当する法令等の明記は努力義務に留めている。これは，実際には法令等に基づいて作成された文書であっても，個々に法令名等を明記せず，別途，規程等に記載する方法でも可能であることを意味している。

[19] 要件を満たしているか否かを一般の利用者が確認，判断することは容易ではない。システム化されていない場合は尚更である。今後，第三者評価の仕組みが望まれる。

表 7.2　推奨方式における，作成・取得環境を特定する要素

カテゴリ	作成・取得環境を特定する要素	備考
文書	作成日時	
	作成者，関係者	
	様式（定義されている場合）	
業務規程等	文書の作成と管理に関する業務規程/システム統制規程	
	文書管理運用に関する業務規程/システム統制規程	
	メタデータの作成と管理に関する業務規程/システム統制規程	
	アクセスと権利に関する業務規程/システム統制規程	
規制等	生成に関する法令・規制要件	努力義務
	保存，セキュリティ，廃棄に関する法令・規制要件	
	文書，文書管理プロセスと法令・規制情報の関係	
部門，要員	作成担当者	
	承認者	
	アクセス権限を与えられた関係者	
業務プロセス	文書，要員，取引先，業務/取引/活動の関係	
	取引相手	
	アクセス規則	
	業務分類	
	文書の分類	
	取引日時	

表 7.3　推奨方式のプロファイル

項目	類型 A	類型 B	類型 C
発行時の本人確認	・対象は自然人に限る ・第三者による確認に基づく，電子証明書又は ID/PW 発行	・組織及び自然人の双方が対象となりうる ・第三者による確認に基づく電子証明書又は ID/PW 発行	・対象は自然人に限る ・社内での一元的な確認に基づく ID/PW 発行
作成者の確認	電子署名 又は 第三者システムにおいて，ID/PW による認証を経て文書を登録・保管	左記に加えて，e シール，コード署名等も許容される。	対象外
作成時刻	第三者による時刻証明	←	内部の時刻管理
取得時の相手確認	電子署名	←	対象外
改ざん検知・防止	電子署名 又は ID/PW によるアクセス制御	←	ソフトウェア統制
立証	関係者の協力	←	ログ監査（委託先等を含む）

注記　類型 D は，各法令に従った取扱いを行うため，表には記載していない。

(2) 推奨方式における各要素の記載例

表 **7.4** に，推奨方式における各要素の記載の例を示す。

表 7.4 推奨方式における各要素の記載例

カテゴリ	作成・取得環境を特定する要素	記載例
文書	作成日時	2019 年 4 月 1 日 13 時 15 分 20 秒
	作成者，関係者	作成者＝資材部 田中一郎 承認者＝資材部 佐藤花子部長 関係者＝経理部 山田次郎
	様式	資材注文書①
業務規程等	文書の作成と管理に関する業務規程/システム統制の規程	文書管理規程
	文書管理運用に関する業務規程/システム統制規程	文書管理規程
	メタデータの作成と管理に関する業務規程/システム統制規程	データベースシステム管理規程
	アクセスと権利に関する業務規程/システム統制規程	データベースシステム管理規程
規制等	生成に関する法令・規制要件	○○法施行規則○条○号
	保存，セキュリティ，廃棄に関する法令・規制要件	○○法施行規則△条△号
	文書，文書管理プロセスと法令・規制情報の関係	資材調達＝○○法施行規則○条○号，△条△号
部門，要員	作成担当者	資材部職員
	承認者	資材部 部長及び課長
	アクセス権限を与えられた関係者	資材部職員，経理部職員
業務プロセス	文書，要員，取引先，業務/取引/活動の関係	上期××資材調達プロジェクトにおける文書一覧，メンバー一覧
	取引相手	○○興業株式会社
	アクセス規則	資材部職員＝作成・閲覧 経理部職員＝閲覧
	業務分類	資材調達
	文書の分類	上期××資材調達文書
	取引日時	2019 年 4 月 25 日 14 時 00 分

7.3.2 厳格方式

厳格方式は，推奨方式における作成・取得環境を特定する要素，並びに，意思表示の確認，作成時刻の特定及び完全性を確保する方法が強化される。

厳格方式は，必要に応じて特定の業務に対して適用することを想定している。

表 7.5 に作成・取得環境の特定に関する強化要素を，**表 7.6** に意思表示の確認，作成時刻の特定及び完全性を確保する方法の強化措置を示す。

ここで，推奨方式の要素（**表 7.2**）と厳格方式の強化要素（**表 7.5**）を合わせたものが，

全体の要素（**表 7.1**）になる。すなわち，厳格方式は，表 7.1 の全ての要素が対象となる。

表 7.5 において，「文書と取引/活動の関係」及び「関係する文書，ファイルとの関係」は，推奨方式では求めていないが，厳格方式においては，これらも記載を求めている。また，業務規程等について，推奨方式では，各文書についての要素としては努力義務としていたが，厳格方式では，記載を求めるものとなっている。

表 7.5　厳格方式における作成・取得環境の特定に関する強化要素

カテゴリ	強化される要素
文書	文書と取引/活動の関係
	関係する文書，ファイルとの関係
業務規程等	生成に関する命令・規制要件
	保存，セキュリティ，廃棄に関する命令・規制要件
	文書，文書管理プロセスと命令・規制情報の関係

厳格方式は，推奨方式に比べて，真正性をより厳格にするため，**表 7.6** の類型 A については，発行時の本人確認を信頼性が確認できる機関によることとする。立証パッケージについては，その要否の判断を求めている。ここで，発行機関における本人確認に係る情報については立証パッケージの作成を基本とするべきである。また，作成文書については，その重要性に鑑みて立証パッケージの作成の要否を判断する基準を策定する必要がある。

類型 C については，第三者による本人確認に基づく電子証明書と電子署名を求めるものとし，作成時刻も第三者による時刻証明を求めている。

なお，類型 A における作成時の本人の意思表示に関わる電子署名については，電子委任状による委任（付録 C 参照）の適用が可能である。すなわち，本来は，組織の代表者の意思表示が必要なものについて，代表者からの電子委任状と，これにより権限を付与された受任者の電子署名により行うことが可能である。

表 7.6　厳格方式における強化措置

項目	類型 A	類型 B	類型 C
発行時の本人確認	信頼性が確認できる機関による確認	―	第三者による確認に基づく電子証明書発行
作成者の確認	―	―	電子署名のみ
作成時刻	―	―	第三者による時刻証明
取得時の相手確認	―	―	―
改ざん検知・防止		―	―
立証	立証パッケージの要否の判断を行う	―	―

注記　‘―’は推奨方式に対して変りがないことを示す。
　　類型 D は，各法令に従った取扱いを行うため，表には記載していない。

7.3.3 簡易方式

簡易方式は，推奨方式における作成・取得環境を特定する要素，並びに，意思表示の確認，作成時刻の特定及び完全性を確保する方法が緩和される。

表 7.7 に，簡易方式における作成・取得環境の特定に関する要素を，また，**表 7.8** に，簡易方式のプロファイルを示す。プロファイルでは，発行時の本人確認を社内での確認（一元的な情報によるものに限らない）を許容している。

表 7.7　簡易方式における作成・取得環境の特定に関する要素

カテゴリ	作成・取得環境を特定する要素	備考
文書	作成日時	
	作成者，関係者	
業務規程等	文書の作成と管理に関する業務規程/システム統制規程	文書化までは求めない
	文書管理運用に関する業務規程/システム統制規程	
	メタデータの作成と管理に関する業務規程/システム統制規程	
	アクセスと権利に関する業務規程/システム統制の規程	
部門，要員	作成担当者	
	承認者	
	アクセス権限を与えられた関係者	
業務プロセス	文書，要員，取引先，業務/取引/活動の関係	
	取引相手	
	アクセス規則	
	業務分類	
	文書の分類	
	取引日時	

表 7.8　簡易方式のプロファイル

項目	類型 A	類型 B	類型 C
発行時の本人確認	推奨方式と同じ	推奨方式と同じ	自然人が対象 ・社内での確認 ・ID/PW 発行
作成者の確認			推奨方式と同じ
作成時刻			
取得時の相手確認			
改ざん検知・防止			
立証			

注記　類型 D は，各法令に従った取扱いを行うため，表には記載していない。

7.4 長期保存

前節まで，電子文書の信頼性向上策について述べてきた。電子文書を長期に保存する場合は，次のような阻害要因への対応が必要となる。

a. 保存媒体やドライブ装置の劣化
媒体の劣化，装置の故障やサポート終了などで電子文書が媒体から読み出せない場合がある。

b. 電子署名やタイムスタンプに用いた電子証明書の期限切れ
電子証明書の有効期間を超えると，デジタル署名やタイムスタンプの検証ができない場合がある。

c. 電子文書を読み出し表示するためのビューアの互換性消失
電子文書が正しく表示されない，またはビューアが起動できない場合がある。

これらの阻害要因を取り除くには，次の対策が有効である。

(1) 媒体移行またはシステム移行

媒体の記録品質を定期的に検査し，閾値を超えた場合は新たな媒体にコピーする。装置についてはサポート終了前に後継システムに移行する。現在，次のような JIS 規格がある。

JIS Z 6017　電子化文書の長期保存方法

JIS Z 6018　電子データのアーカイビング−コンピュータアウトプットマイクロフォーム（COM）／コンピュータアウトプットレーザディスク（COLD）

JIS Z 6019 磁気テープによるデジタル情報の長期保存方法

(2) 長期署名

電子証明書の有効期限が切れる前に，有効期限後も検証を可能とする対策が施された電子署名やタイムスタンプを長期署名という。いくつかの方法があるが，電子的なタイムカプセルに，対象文書や電子証明書などの検証情報を封入する，アーカイブタイムスタンプ方式が主流である。現在，次のような JIS 及び ISO 規格がある。

JIS X 5092　CMS 利用電子署名（CAdES）の長期署名プロファイル

JIS X 5093　XML 利用電子署名（CAdES）の長期署名プロファイル

ISO 14533-3　PDF 電子署名（PAdES）の長期署名署名プロファイル

ここで，JIS X 5092 は電子メールに，JIS X 5093 は Office 文書等の電子署名に使われている。

(3) PDF/A

長期保存を目的としたアーカイブ用 PDF フォーマット。実装を自己完結型とすることにより，OS 等の影響を受けず互換性が維持される。ISO 規格となっている。

ISO 19005　Electronic Document File Format For Long-Term Preservation

付録 A　ソフトウェア統制

文書の完全性を担保する方法として，多くの文書情報管理システムに用いられている単純な方法は，ソフトウェア統制である。ソフトウェア統制は，利用者による編集や削除を許可せず，文書へのアクセスのみ許可する。一方で，文書管理スタッフは文書の廃棄は行なえるが，編集は許可されない。大抵の状況下においてソフトウェア統制は要求を満たす。

この方法は監査証跡と併用ができる。監査証跡は，文書（記録）は取り込まれるとき，または文書（記録）にメタデータが付与されるときに，自動的にデータと操作者の身分のログをとり，文書（記録）にアクセスがあった場合いつでも同様の情報のログをとる。文書（記録）が変更された際は（例えば。メタデータを編集するときや文書（記録）を削除するとき），これらの変更のログもとる。そうすれば許可された変更のみが行われていることを確認できる。

監査証跡はそれ自体が記録であり，監査ログファイルは編集不可の状態で保存しなければならない。特に業務フロー・システムではそのようなファイルは急速に増加する。そのため監査ログデータの保存要件を評価し，保存期間を設定しなければならない。

付録Ｂ　立証パッケージ

押印がある書面に代えて，電子署名とタイムスタンプが付与された電子文書を法廷に証拠書類として提出する場合を考え，「電磁的記録の真正な成立」の推定効を得るため署名の本人性を証明する以下の資料など必要な情報を保持しておき，必要な時に取り出せるようにする[20]。

- 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 証明書ポリシーなど）
- 証明書発行の際に認証局が取得した発行申請書や本人確認書類，証明書取得書
- 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
- 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

これらの資料により，署名時刻に証明書が有効で，かつ，署名対象データに改ざんがないこと，などが証明できるため，民事訴訟において，電子署名法３条による真正な成立の推定を受けることができる。

また，当該電子文書が作成された背景情報として，なぜ当該文書が作成されたのか文書作成に至った理由を示すことも有効である。業務文書であれば，業務規程，契約書であれば，その取り扱いを契約当事者間で定めた規約などの提出が考えられる。

[20] 文書情報システムが，これらの情報を当該文書に係わる関連情報一式を含むパッケージとして提供することが望まれる。

付録 C　電子委任状

BtoG，BtoB では，組織の代表者が職員等に権限を委任して，意思表示や通知などを行わせることが多い。委任の事実を証明するための電子文書として，電子委任状が用いられる。電子委任状法では，一つの案件の委任だけでなく，一定期間にわたる権限（たとえば，２年以内に行われる公共入札を行う権限）を示す電子委任状をも対象としている。電子委任状法[21]は，電子委任状を発行・管理する電子委任状取扱業務を規定している。電子委任状取扱業務には認定制度があり，認定事業者によって発行された電子委任状であれば，その委任内容について法的効力が認められる。

電子委任状の普及を促進するための基本的な指針（平成 29 年総務省・経済産業省告示第 3 号）[22]では，電子委任状の記録方式として以下の 3 方式を定めている（同指針 第 3 の 1，2，第 4 の 2）

① 委任者記録ファイル方式

委任者が電子委任状に記録すべき事項を電子ファイル（XML，PDF）に記録し，委任者の電子署名を付与する方式。なお，委任者の電子署名に用いる電子証明書は，認定認証局，商業登記認証局，公的個人認証サービスのいずれかのものを用いる必要がある。

② 電子証明書方式

電子委任状取扱事業者が，委任者の委託を受けて，電子委任状に記録すべき事項を受任者の電子証明書に記録する方式。この方式では電子委任状取扱事業者は電子認証局となるが，その適格性について，認定認証局であること，または，米国公認会計士協会及びカナダ勅許会計士協会によって共同開発された電子商取引認証局監査プログラム（WebTrust for CA 監査）又は欧州電気通信標準化機構の規格に基づく認証局の ETSI 監査を年一回以上の頻度で受けることが求められている。

なお，この認証局の電子署名は，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・経済産業省令第 2 号。以下「電子署名法施行規則」という。）第 2 条に定める署名暗号アルゴリズムの基準に該当するものでなければならない。

③ 取扱事業者記録ファイル方式

電子委任状取扱事業者が，委任者の委託を受けて，電子委任状に記録すべき事項を電子ファイル（XML，PDF）に記録し電子委任状取扱事業者の電子署名を付与する方式。電子委任状取扱事業者の電子署名は，電子署名法施行規則第 2 条に定める署名暗号アルゴリズムの基準に該当するものでなければならない。

---

[21] 電子委任状の普及の促進に関する法律（平成 29 年法律第 64 号）、平成 30 年 1 月施行

[22] http://www.soumu.go.jp/main_content/000538995.pdf

①, ③のファイル方式の電子委任状は, 受任者の電子証明書とともに用いる必要があり, 受任者の利用する電子証明書の発行番号等により, 電子委任状と受任者の利用する識別子とを紐付けなければならない。(第 4 の 3 の二)

また, ファイル方式の電子委任状に付された電子署名や電子証明書方式の電子委任状で電子契約書等に付された電子署名は, 長期的に有効性が確認できる必要があることから, 「電子契約の当事者, 電子委任状取扱事業者その他の関係者が, 電子委任状を取り扱うときは, 当該電子委任状の受領者等が, 当該電子委任状等に長期署名(XAdES, PAdES 等の長期署名に関する標準的規格に適合しているものに限る。)を行うことが可能となるよう努めるものとする。」(第 5 の 1)としておりタイムスタンプを用いた長期署名を行えることを努力義務としている。

付録 D　電子証明書の信頼性

電子証明書に基づく電子署名の信頼性は，その電子証明書の発行機関すなわち認証局の信頼性に依存する。わが国の官民の認証局の種別について，「図 C.1　政府認証基盤と民間認証局」に示す。

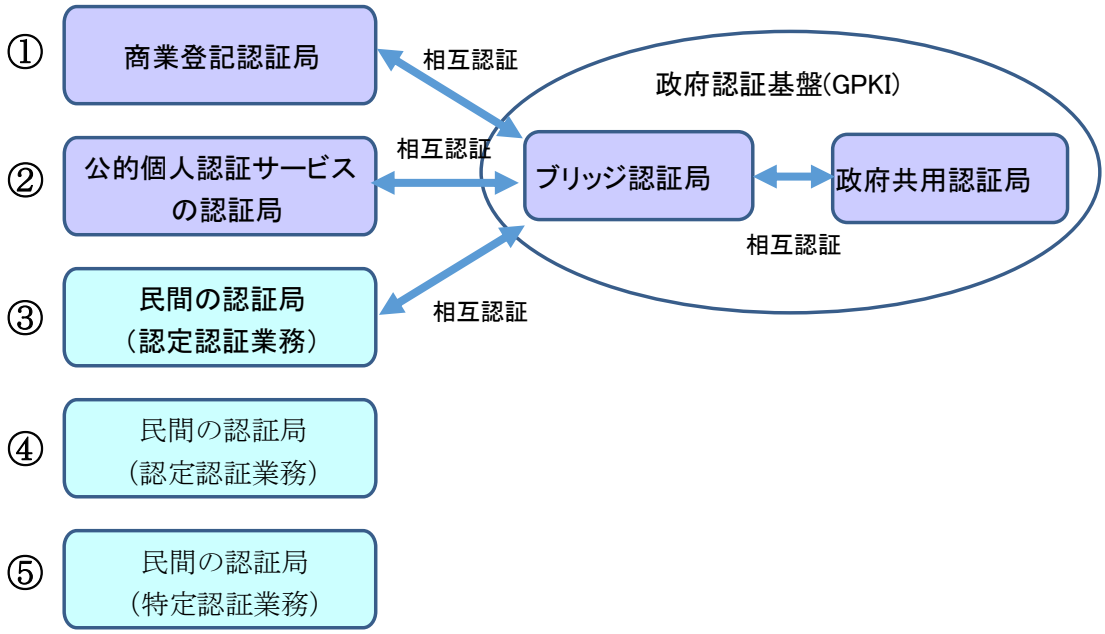


図 C.1　政府認証基盤と民間認証局

また，上記の各認証局から発行される電子証明書の特色，行政手続きにおける電子申請での使用の可否（GEPS による場合）を，「**表 C.1**　電子証明書の種別と特色」に示す

表 C.1 の①～④は，公的機関または公的機関による認定を受けた認証局であるから，適切な運用が確認されており，これらにより発行された電子証明書は高い信頼性を持つ。

また⑤においても，信頼性の高い認証局が存在する。このような認証局の例としては，WebTrust や ETSI 認定を受けたパブリックルート認証局から認証されている認証局（パブリック認証局と呼ばれる）などが挙げられる。パブリックルート認証局は IE や Chrome など主要なインターネットブラウザーに，「信頼されたルート認証機関」として登録されているためそこから認証を受けているパブリック認証局から発行された電子証明書は電子署名の有効性検証を行う時にその信頼性が容易に確認できる。

表 C.1　電子証明書の種別と特色

	電子証明書の種別	特色	電子申請
①	商業登記法第十二条の二第一項及び第三項の規定に基づき登記官が作成した電子証明書	会社・法人の代表者等に対して発行される電子証明書であり，申請者が法人代表者である場合などに用いることができる。このため法人代表者以外の者は使用できない。	利用可
②	電子署名に係る地方公共団体の認証業務に関する法律第三条第一項に規定する電子証明書	個人番号カード（マイナンバーカード）に格納された，公的個人認証証明書(署名用)。利用者の基本 4 情報（氏名，住所，性別，生年月日）が証明書に記載されているため，電子署名済みの電子文書に基本 4 情報が付加されることになり，個人情報保護の観点から利用者がそれを望まないことが考えられる。また，その署名検証には地方公共団体情報システム機構（J-LIS）の失効情報にアクセスすることが必要となり，検証システムは総務大臣認定を受けるか，その認定を取得しているプラットフォーム事業者のサービスを利用する必要がある。	利用可
③	政府認証基盤ブリッジ認証局と相互認証を行っている認証局が作成する電子証明書	民間の認定認証局が発行する電子証明書で一般的な電子申請等で用いられる。政府認証基盤と接続しているため，公的機関での署名検証が容易で，電子申請などの行政手続きにも利用できる。	利用可
④	民間の認定認証事業を運営している事業者が発行する電子証明書（政府認証基盤ブリッジ認証局と相互認証を行っていないもの）	政府認証基盤ブリッジ認証局と相互認証をしていないため，行政手続きでの利用はできないが，本人性が確保された電子署名が可能。	利用不可
⑤	民間認証局が発行する特定認証業務の電子証明書	電子署名法では特定認証業務の基準として電子署名に用いる暗号アルゴリズムが定められているだけであり，，認証局の運用基準や本人性の確認レベルの基準が定められていない。したがって，電子署名の本人性を担保するためには，それらを一定の基準の下に運用し，信頼性が確認できる認証事業者（特定認証業務）が発行する電子証明書を用いることが望ましい。	利用不可

電子署名法 2 条 1 項の電子署名に用いる特定認証業務の電子証明書は，署名者の「なりすまし」を防ぎ，本人確認を確実に行なった上で発行する必要がある。

したがって，認証局においては本人以外に電子証明書が発行されないよう適切な運用が必要となる。また，電子署名が付与された電子契約書などは広く当事者や関係者などで利用されるため電子証明書が信頼された認証局から発行されたものであることを広く確認できることが必要となる。認証局の信頼性を確認するためには，国や標準化団体などにより作成された技術・運用基準に基づいて適切に運用され，監査が適切に行われていることなどを，公開されている運用規程や電子証明書の発行基準（CP/CPS）により確認することが必要となる。

付録 E　JIIMA ガイドライン等

1. JIIMA　建築設計業務における設計図書の電磁的記録による作成と長期保存のガイドライン Ver. 1.1 （2018 年 3 月）＜PDF＞
2. JIIMA　電子帳簿保存法第 10 条 電子取引の取引情報に係る電磁的記録の保存 電子取引 取引情報保護ガイドライン 第 1.00 版（2018 年 10 月） ＜PDF＞
3. JIIMA　平成 27 年度改正・平成 28 年度改正準拠　税務関係書類の電子化保存運用ガイドライン Ver.4（2016 年 10 月改訂）
4. 厚生労働省　医療情報システムの安全管理に関するガイドライン第 4.2 版（第 9 章）の手引きと解説（2015 年 9 月）＜PDF＞
5. JIIMA　効率とコンプライアンスを高める e－文書法電子化早わかり（第 2 版）　平成 29 年 10 月刊

政策提言プロジェクト／電子文書信頼性向上タスクフォース

座 長	宮内 宏	弁護士　宮内・水町 IT 法律事務所
	西貝 吉晃	日本大学法学部専任講師
	西山 晃	セコムトラストシステムズ株式会社
	木村 道弘	JIIMA 特別研究員
	高橋 通彦	JIIMA 顧問
事務局	甲斐荘博司	JIIMA 専務理事

公益社団法人 日本文書情報マネジメント協会

〒100-0032　東京都千代田区岩本町 2-1-3　和光ビル 7 階
TEL 03-5821-7351　　FAX 03-5821 7354
http://www.jiima.or.jp
法人番号　6010005003693