電子文書信頼性向上プロジェクト中間報告

―電子文書の信頼性を確保するための考え方や留意点－

Ver.1.0

2017 年 10 月

公益社団法人日本文書情報マネジメント協会

電子文書信頼性向上プロジェクト

はじめに

「人の意思を表す」表現手段としての文章は，長年紙の上に文字で記されて使用されてきた。しかし近年コンピュータやネットワークの進化で，パソコンを利用して電子的に文書を作り，その電磁データが送受信や保存に使われており，世界的にも一般化している。

しかし日本では電子文書に対する信頼性が薄く，正式の文書として取り扱われる場合は紙文書が依然として主体となっている。その最たるものが国税関係書類の保存であるが，昨年・一昨年と e－文書法のスキャナ保存の規制緩和がやっと行われ，電子化の１つの課題がクリアーとなり，企業での電子化の機運がでてきている。

この機に合わせ，JIIMA では「安心で社会生産性の高い電子文書情報社会の構築を目指して」をビジョン２０１６で掲げており，日本社会全体での電子文書の普及を促進したい。

本プロジェクトでは，普及遅れの様々な観点のうち，まず影響の大きい裁判手続きにおける電子文書の利用にあたっての問題点を取りあげ，続いて電子文書の信頼性のポイントを議論し，最後に信頼性確保の方策を検討した。

これらの法制度面，技術論を踏まえ，さらに議論を深堀りし，より具体的な形にまとめ関係方面に政策提言をおこないたい。

公益社団法人　日本文書情報マネジメント協会(JIIMA)
理事長　高橋通彦

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。

文書情報マネジメント

文書情報を正当に作成・取得，保存，廃棄及び長期保存する組織的な運用。

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。

＊本報告では，「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。本報告では刑法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」のこと。

説明責任の維持

文書情報を使用して経営及び業務を説明できるように組織及び文書を維持している状態。

可用性

文書情報を利用するために，その保存状態，検索方法，見読方法が，継続的に維持される性質。

完全性

電子文書が，虚偽入力，書換え（改ざん・すり替え），消去，混同，隠滅，破壊されていない性質。

検索性

電子文書が，速やかに検索できる性質。見読性確保のための要件の一つ。

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。

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

真実性

文書の内容が客観的事実と合致している性質

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

文書情報が，完全性，可用性，真正性，保存性など全てを満たす性質。

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が信用するに至る性質。

保存性

文書情報が，規程で定められた期間に渡って真正性と見読性を満たす性質。

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管状況。

長期保存

業務上の要求される保存期間を超えて保存する作業。

＊長期と呼ばれる期間は，管理システム又は媒体によって異なっている。

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. 電子文書の証拠性に関する法制度

ここでは，紙媒体と異なる電子文書の特徴を踏まえながら，裁判手続における電子文書の利用に当たっての問題点を検討する。まず，本書における議論対象たる電子文書の定義を確定し，その上で外国の状況を簡潔に見た後，我が国における電子文書の取扱いについて確認し，法制度面及び技術面での課題の抽出を行うことにする。

1.1. 電子文書の定義と特徴

1.1.1. 電子文書の定義

まず，本報告において議論の対象とすべき電子文書を定義する。本報告には，法制度面及び技術面の各々の当事者間の対話的な議論の発展を促す意図もある。そこで，電子文書の定義を，既存の法律の文言を用いながら，技術的な説明を補足する形で議論していきたい。

媒体の種類を問わず，情報のやり取りにおいて一定のミスコミュニケーションが発生することが紛争の原因になる。とすれば，そのような情報のやり取りの多くが電子データの形式でなされており，それが増加していくという予想の下においては，電子データに由来する情報は，裁判における証拠として不可欠になるという予想が成り立つ。情報のやり取りのために作成された電子データや，情報のやり取りのために直接に用いなくとも自身の思想内容をまとめるために保存しておいたデジタルデータの，証拠としての重要性が増すことには疑いがない。

このような背景を前提として，裁判手続における証拠としての電子文書をどのように考えるか，という問いに対しては，2 つの方向性が考えられる。第一に，電子文書というのは，コンピュータにおいて処理の対象となり得るデータを指す，とするものである。第二に，電子文書を，電磁的方法で記録され，コンピュータやスマートフォンで処理されるデータだと考える立場であり，法律にしばしば登場する電磁的記録とほぼ同じものとして捉えるアプローチである。

権限ある者による管理の対象として電子文書を捉え，その管理の在り方をも探求する本報告の趣旨からすれば，電子文書＝電磁的記録として捉えれば必要十分である。

文書には一定程度の認識可能状態の持続性が要求されるが，電子文書においても，電磁的記録において要求される記録性を要件とすることで，一定の機器を用いて認識可能にされ得る状態の持続性が要求される。それゆえ，メインメモリ上において処理中のデータや，有線又は無線で通信中のデータは電子文書の定義から外されることになる。アンリンク処理がなされて論理的に消去されたデータに関しては，物理的にデータが消去されたわけではなくなお電子文書に当たる，といいうる。このような解釈の結果は，電子文書が裁判手続において問題になり得るものである以上，妥当な方向であると考えられる。

以上の定義に基づき，持続的に存在するファイル等のデータを「電子文書」と呼び，USB メモリや HDD などを「電子文書に係る記録媒体」と呼ぶものとする。

1.1.2. 電子文書の特徴

前述のように理解された電子文書の特徴を列挙してみると，デジタルデータであることも含めて，例えば次のような特徴を指摘することができる。

① 永続的保存可能性 — ③の特徴と相俟って，媒体を乗り継げば理論的には永遠に保存が可能である。その際に，情報の劣化はない。

② 大容量のデータの保存可能性 — 省スペース

— 高度な検索

③ 全く同じデータのコピーの可能性 — オリジナルという概念がなくなり得る，又は，デジタルデータのオリジナルとは何かを定義する必要が生じ得る。

そして，何らの技術的措置を施さない前提で，次のような特徴が認められる。

④ 改ざんの検知の不可能性 — 痕跡を残さずに改ざんが可能であること

その場合の改ざんの内容や程度は問わないこと。

①は，裁判手続という観点からすれば，確実な保管年数をどの程度確保すればよいか，という問題と関連する。その場合，時効等の問題がある法律的な観点も考慮されよう。保管の過程での劣化がないことは，その内容の正確な再現について，紙等に対する電子文書の優位性を示している。紙等のアナログ媒体上の情報に関しては，適切な管理をしない限りその損耗劣化の程度が激しくなっていくであろうが，媒体の使用状況，存在する環境には依存するものの，データの劣化が存在しない電子文書には他の媒体と比較して保存面での優位性が認められる。だからこそ社会に浸透しつつあるのである。

②の特徴も現実的な書類の保存の観点からは極めて重要な要素である。大容量のデータを保存できるという特徴は，紙等の容量的に限界のある手段と比較して，同じ量の情報を省スペースで管理可能になる，ということを意味する。物理的空間を圧縮できることにより多大なコスト削減が見込まれることになる。

また，大容量の情報の中から情報検索技術を用いることにより，紙等の媒体上の情報と比較して，圧倒的に高速かつ正確に情報検索が可能になる。以上の点は，証拠の取扱いという観点からみても重要である，と思われ，高度な保存手段，検索手段を用いることにより，簡易迅速かつ正確に，重要な証拠を発見できることになる。

④は電子文書を証拠として取り扱う際に障害となる要素ではある。しかし，これについては，技術的な解決が図られている。（4.2 参照）

次に，以上のような特徴を有する電子文書について，その特徴を踏まえ，裁判手続の

ルールをどのように考えるべきかについて考えていきたい。

1.2. 海外の法制度

電子文書の裁判手続における利用に当たって課題になると思われるのが，電子文書の内容についての類型的信用性である。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，証拠として提出することについて実質的には支障がないはずである。

ここでは，網羅的ではないものの，電子文書の証拠としての取扱いについてのアメリカとカナダの状況の一部を簡潔に紹介し，我が国の法制について考えたい。

1.2.1. アメリカ

アメリカにおいては，多くの州において，機械・電子的複製物に，作成者の意図を重視せずオリジナルと同じ効果を与えている，とされている[1]。例えば，電子メールについては，一般に，受信されたメールがオリジナルとなり，送信済のメールは複製物だとされるようである。

このことは電子文書の持つ全く同じデータのコピーの可能性をよく表わしている（1.1.2. ③）と思われる。

1.2.2. カナダ

カナダでは，Evidence Act§31.1 以下で，電子文書についての取扱いが定められている。電子文書自体の定義は，§31.8 にあり，アウトプットやプリントアウトもこの概念に含まれるとされるが，基本的には，読み込み可能な形式でコンピュータ・システムや記録又は保存されたデータであることが念頭に置かれているから，ここでの議論に資すると思われる。

このような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)，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)。しかも，反証がなされない限り，電子文書システムの完全性は，§31.3(a)~(c)のいずれかの場合で推定される。このうち，本報告との関係で着目すべきは(a)であり，その内容は次の通りである。

> (a) 問題となるあらゆる時点において(at all material times)，電子文書システムが使用するコンピュータ・システム若しくは他の類似の装置が適切に作動していたこと，又は，そうではなかった場合に，当該適切に作動していなかったという事実が電子文書の完全性に影響しておらず，かつ，電子文書システムの完全性を疑うべき何の合理的な根拠もない，という認定を基礎付け得る証拠による方法。

[1] 田邉真敏，「アメリカ連邦証拠規則」，レクシスネクシス・ジャパン，2012，p.240.

すなわち，電子文書の出入力に使用されたシステムが，それを使う者が入力しようとした意思内容を歪曲せずに記録保存していること，及び，その上で，その者の意思とは別のところで改ざん等されていないことといった状況が担保されていることが重要であり，また，それが担保されているのであれば，反証がない限りシステムの完全性が推定され，ひいては，その真正が証明され得ることになるわけである。

以上からすると，我が国においても，電子文書を積極的に利用しようとする場合には，もちろん，一定の技術的な保障を得るべきことは前提ではあるが，それを得た後に，一定の要件の下で，電子文書を利用しやすい証拠法のルールを考えるべきではないか，と思われるところである。そこで，我が国の現状についての確認をしてみたい。

1.3. わが国の法制度

我が国の訴訟手続を取り扱う法律は主に民事訴訟法(以下「民訴法」という)及び刑事訴訟法(以下「刑訴法」という)である。そして，下記にみるように伝聞証拠に対する取扱いが異なる。

1.3.1. 刑事手続

我が国の刑訴法をみると，刑訴法 320 条において，伝聞証拠について原則として証拠能力を認めず，刑訴法 321 条以下で，各条の要件を充たす場合に，例外的に問題となる伝聞証拠の証拠能力を認めている。

そもそも，刑訴法 320 条が原則的に証拠能力を認めていないのは，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。電子証拠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と思われる。

もっとも，刑訴法 326 条に基づく同意により，伝聞証拠であっても証拠能力が付与される。そうすると，電子証拠に対する社会的信頼が十分に存在する状況の下では，その証拠が電子証拠であるから同意しない，というような仮定を置くことはあまり現実的ではないかもしれない。しかし，常にそのような同意が得られるとも限らないので，なお，電子証拠の特徴を踏まえた証拠能力の付与の方法を，立法論を含む法律論として考えるべきである。

1.3.2. 民事手続

一方で，我が国の民訴法においては，伝聞証拠であることを理由に証拠能力が否定されるわけではないので伝聞証拠に関連させた議論は乏しい。むしろ，実践的な観点から，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が議論されてきたといえる。証拠には証拠説明書を付して提出する等，詳細な議論はあり得るが，ここでは，電子証拠の特徴及び使用にあたっての利便性の観点から，①，②を分けて考える。

①については，そもそも，プリントアウトした物はそれ自体から思想内容を感得できる文書であって，もはや電子文書の特徴を具備しないものであるから，プリントアウト

を文書として証拠提出すればよい。多くの電子文書においては，普及しているフォーマットの文書ファイルを開くことはどのようなコンピュータ環境であっても容易であり，かつ，電子文書であれば省スペースで保存できるという利点がある。しかし，プリントアウトを提出するとすれば，その都度アウトプットする必要があることになってしまう。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有体物とは異なる利点を活かしているとはいえないし，同一の情報が電子文書のアウトプットの形式で存在することにより発生するアウトプット上の情報管理の必要性からセキュリティコストが増大することになり，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(民訴法 231 条)として提出することが考えられる。この場合においては，今度は，思想内容を感得するための再生の方法が非定型であり，裁判所や他の訴訟当事者にとって必ずしも簡明ではない可能性がある点に注意が必要である。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 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 ブラウザが起動するだけであって，そのソースを閲覧できるわけではないからである。したがって，再生方法の共有についての議論が不可欠になる。

1.3.3. 小括

現状では，紙等の有体物を使った手続への安心感があるせいか，それらに頼りがちな実務になっている，と思われる。コンピュータ及びインターネットが普及・浸透し，民間のビジネスにおいてもこれらに依存しており，さらに，ビジネスを守るためのセキュリティ技術も普及している。このような状況はコンピュータ黎明期ないしインターネット黎明期とは異なる技術的状況があるといえ，電子証拠の特徴を活かしながら，電子文書を直接的に活用することにより，裁判手続の関係者全てに発生し得るコストを削減すべきである。そして，将来的には，サーバにアップロードする形での証拠提出ということも考えられてよいと思われる。既に実用化されている国もあるようである。

したがって，電子的に情報をやり取りするという形態に依存している現代社会の状況を踏まえると，電子文書の証拠としての使用の観点からは，使用に耐えうるという意味での信頼性を確保することが重要となり，この点についての基礎的検討を行っておくことが重要な課題となる。そこで，さらに，**2.** において，電子文書の信頼性を確保する方法を考えていく。

2. 電子文書の証拠提出に向けたポイント

前章で述べたように，わが国の民事訴訟においては，伝聞証拠を含むあらゆる文書（電子文書を含む。民事訴訟法 231 条）を証拠として提出することができる。この意味では，いかなる電子文書であっても証拠能力はあるといえる。

ここでは，わが国の民事訴訟における電子文書の証拠力について論じる。

2.1. 形式的証拠力

文書を証拠として提出するときには，真正な成立を証明する必要がある（民事訴訟法 228 条 1 項)。ここで真正な成立とは，その文書の作成者とされる者（本人）が，その者の意思を表現したものとして文書を作成したものであること（本人が本人の意思で作成したこと）をいい，真正な成立にもとづき，本人の意思の表現であると認められることを形式的証拠力という。紙文書については，本人又は代理人の署名又は押印があれば，真正な成立が推定される（民事訴訟法 228 条 4 項)。また，一定の条件を満たす電子署名がある電子文書についても真正な成立が推定される（電子署名法 3 条)。

なお，訴訟の相手方が真正な成立を争わなければ，真正な成立が認められる。

2.1.1. 電子証明書による真正な成立の証明

電子署名による真正な成立の推定にあたっては，電子証明書が重要である。電子証明書は，いわば電子的な印鑑証明書のようなものであり，電子署名に係る本人を特定することができる。電子署名は一種の暗号文であり，それ自体では誰の署名であるかは判別できない。電子署名を検証するためには，そのための情報（公開鍵と呼ばれる）が必要であり，公開鍵の所有者を明示するために電子証明書が用いられる。

電子証明書の発行は，公的個人認証基盤の場合には地方公共団体情報システム機構が，電子署名法に基づく発行者の場合には認証業務が行う。公的個人認証基盤の電子証明書は，個人番号カードに搭載されており，実印並みの安全性が認められている。一方，電子署名法に基づく認証業務については，一定の技術要件を満たしたものを特定認証業務，特定認証業務であって，特に厳しい要件を満たして認定を受けた者を認定認証業務という。認定認証業務は実印並みの安全性がある。認定を受けていない特定認証業務の場合には，その運営方法（たとえば，本人確認方法や証明書の交付方法など）により，三文判程度の安全性のもの，銀行届出印程度の安全性のもの，実印に近い安全性のものなどがある。

2.1.2. 電子署名以外の方法による真正な成立の証明

真正な成立の証明は，電子署名以外の方法でも可能である。たとえば，文書情報マネジメントシステムにおいて，不正な変更や削除を防止する仕組及び規定があり，これら

による運営が行われていることが示せれば，真正な成立を証明できる可能性がある。特に，システムが，訴訟の当事者と利害関係のない第三者により運営されていれば，運営者をいわば目撃証人に相当するものとして，真正な成立を証明することに大きく寄与するものと考えられる。また，完全な第三者でなくても，通常の業務の一環として専門の担当者が管理している場合（社内システム部門や委託先事業者の場合など）にも，相当な証明力があると思われる。

2.2. 実質的証拠力

真正な成立にもとづいて形式的証拠力が認められた電子文書は，証拠となる。このときに，証拠としての実質的な効力が問題となる。これを実質的証拠力という。実質的証拠力は，証明しようとする事実（要証事実）に対する証明のための効力と考えられる。

たとえば，自動車事故の損害賠償訴訟において信号が赤なのに進行したという事実を証明するために，目撃者による陳述書が提出された場合を考える。この場合，目撃者が何を見たと陳述しているか（内容）と，その陳述内容は信用できるものか（信用性）が問題となる。信用性については，目撃者と当事者の利害関係，目撃の状況などの周辺事情が大きな意味を持つ。

企業が持つ電子文書は，その電子文書が作成された経緯，作成時期，作成者，配布先，などの情報や保管状況により，電子文書の信用性が大きく左右される。電子文書の周辺のこうした情報をコンテキスト情報と呼ぶ。

なお，わが国では伝聞証拠の提出に制限はないが，刑事訴訟や米国証拠規則等における伝聞例外条件を満たすことにより，証拠の信用性を大きく向上できるものと思われる。これらの伝聞例外は，類型的に信用性の高いものを法令化したものだからである。

2.2.1. コンテキスト情報の管理

文書（記録）は，コンテンツ（content）と，コンテキスト（context），構造（structure）および時間の経過に伴う管理に関する情報を記述したメタデータから構成される（ISO 15489-1:2016）。**図 2.2-1** 参照。

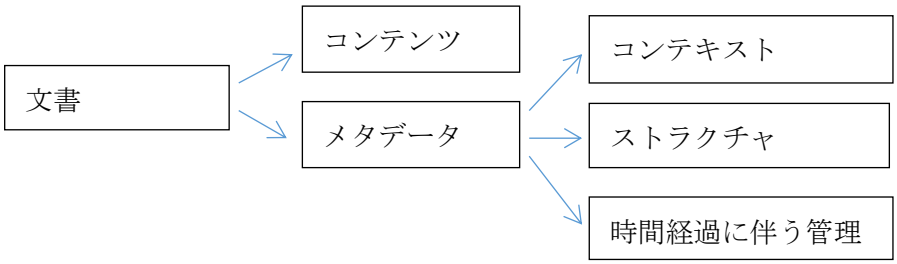


図 2.2-1　文書の構成

メタデータは，属性あるいはプロパティとも呼ばれ，文書のコンテンツと一緒にその内部に取り込まれたり，文書管理システムに取り込まれて管理される。

ここで，構造（ストラクチャ）は，コンテンツとコンテキストを結びつける働きをする。例えばビジネス書簡では，宛先の詳細，日付，段落に分かれた本文，そして最後の署名との間に形式的な構造上の関係がある。また，フォルダ内の個々の書簡の間にも，簿冊内の文書（記録）間にも構造上の関係がある。

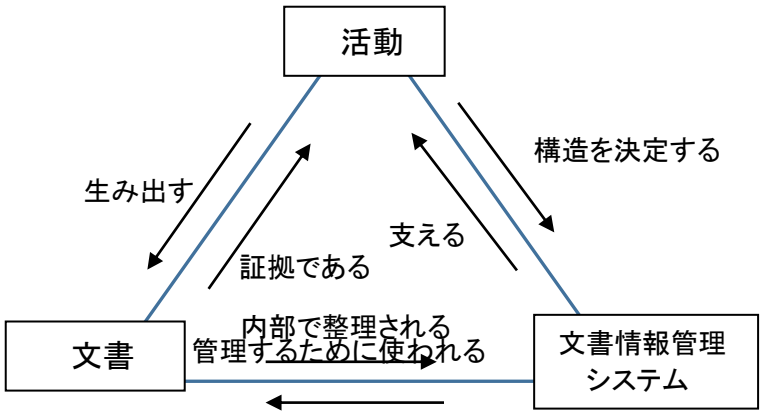
また，時間経過と共に蓄積される情報は，その文書の由来・来歴(provenance)などを，正しく記録する。

実際には，電子文書（記録）の管理は，紙媒体で行われている概念の延長で，仮想のファイル・キャビネットや電子フォルダの形をとる場合が多い。一般的には，メタデータがフォルダ代わりに文書（記録）のコンテキストの記録に使用されている。

たとえばレコード・マネジメント・ハンドブックでは，「機能や業務プロセスをフォルダやサブ・フォルダの階層構造にあてはめるというより，典拠ファイル（実態はメタデータデータベース）としてモデルが表現されることになる。文書（記録）作成にかかわる組織の規則やその他のルールや，活動を行った者の来歴や役割（例えば，メッセージの送信者や受信者など）もメタデータにしておくことができる。各従業員に関するメタデータは，名前，従業員が属する事業単位，事業単位内での地位や担当の変遷等の職務に関するデータベースから取得することもできる。文書（記録）に付与されたその種のメタデータは，将来的な利用者の役に立つ文書（記録）のコンテキストに，十分な定義を提供できるのである。」としている。

2.2.2. 文書管理システム

文書管理システムは，文書のコンテンツとメタデータを管理する。図 2.2-2 は，企業の活動，文書，文書情報管理システムの関係を表している。活動は文書を生み出し，文書は活動の証拠となる。文書情報管理システムは文書を管理するために使われ，文書は文書情報システムの中で整理される。そして，企業の活動は文書情報システムの構造を決定し，文書情報システムは企業の活動を支える。



出典　Managing Records, a handbook of principles and practice

図 2.2-2　活動，文書（記録），文書情報管理システム間の関係

2.3.　検索性

米国においては，e-ディスカバリの制度があり，訴訟に関連のある電子文書を適時に開示することが求められる。わが国にはこのような制度はないが，紛争が発生したときに，必要な証拠を迅速に検索できることは，訴訟において効果的な証拠を提出するためになくてはならないことである。

なお，電子帳簿保存法においては，電子取引のデータや，紙文書をスキャナ保存したデータについて，検索要件が定められている（電子帳簿保存法施行規則 3 条及び 8 条)。これは，税務調査の効率化のための要件と考えられるが，紛争時の証拠収集においても重要な要素が規定されているものと思われる。

このように，電子文書の検索が迅速かつ効果的に可能とすることが重要であるところ，コンテキスト情報や電子文書間の関係などについては，信用性のみならず検索に資する面も大きいため，一層の重要性を認めるべきである。

3. 証拠の対象となる電子文書の種類とその用途

保管管理の対象となる電子文書は多岐にわたるが，ここでは，いくつかのカテゴリーに分類して整理する。

3.1. 外部と取り交わす電子文書

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管義務があるため，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管する必要がある。

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ため，電子メールによるものも対象とする。

外部と取り交わす電子文書には，大きく分けて以下のようなものがある。

(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

・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

・見積書，請求書，納品書

(3) 公的文書

・公的申請，届出等

・法令により必要とされる記録など

(4) その他

・議事録（外部との会議などに関するもの）

・設計図，設計書

・プロジェクト報告書等の報告書

3.2. 内部の電子文書

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。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

・取締役会議事録，その他の社内会議議事録

・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）

3.3. 電子メール

組織内や組織間で最も一般的なコミュニケーション手段が「電子メール」である。電子メールは，公式文書とは違って，担当者間で気軽にコミュニケートができるし，書面の添付や交換も気軽にできる，電子文書社会では，極めて便利で不可欠なツールである。しかし電子メールは，意思疎通機能だけではなく，組織の業務記録として（作成・保存環境情報を含め）保存管理が必要な電子文書であることも認識する必要がある。

なお，内部統制の視点からは電子メールは，金融庁の監査基準で「経営者や組織の重要な構成員が電子メールを用いて，容易に不正を共謀することも可能としかねず，これを防止するべく適切な統制活動が必要」とされている[2]。

また電子取引と輸出入取引に関する電子メールは、電子帳簿保存法と関税法により添付書類を含めて保存が定められている。

[2] 金融庁『内部統制の評価及び監査に関する実施基準』 Ⅰ-2 (6) ②

4. 証拠としての電子文書管理の方向性

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る。組織的にオーソライズされた業務のなかで，権限のある者が文書を作成し，承認を行う。

証拠としての文書に要求される事項の第一のポイントは，どのような環境で作成または取得された文書であるか，すなわちその文書の作成・取得環境コンテキストが証明可能なことである。第二のポイントは，文書の真正性（作成者とされているものが真に作成したこと），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証明可能なことである。

4.1. 文書の作成･取得環境の文書化と保存

どのような環境で作成・取得された文書であるかを証明する（検証する）には，文書が作成・保存されたときの環境もまた文書として残っており，元の文書と関連付けられている必要がある。例えば，その文書が A 業務の一環で作成され，B 部長が承認したのであれば，A 業務はどのような業務であり，B 部長はその業務において承認す権限をもっていたのかを当時の作成・取得環境に関する文書を辿って検証できる必要がある。

作成・取得環境として，どのような内容が文書化され保存されている必要があるか，基本的な要件は ISO23081-1 の 9.3.1 に規定されている。

以下，要件と対応する規程類を例示する。

a) 文書（含，メタデータ）の作成・取得を統制する業務の規程
   業務規程，業務マニアル
b) 文書の管理・運用を統制する業務の規程
   文書管理規程
c) 文書へのアクセスを統制する規程
   秘密管理規程
d) 文書の作成，管理，維持処分を要求する法規制文書
   関連法規制
e) 業務における個々の取引に関する文書
   取引台帳
f) 担当者，承認者，取引先に関する文書
   職務分掌規程・分掌リスト，取引台帳
g) 業務，文書，担当者，承認者，取引先の関係についての文書
h) 文書と取引の関係についての文書
   文書管理規程，文書管理台帳
i) 文書相互間，文書と aggregation（簿冊など）との関係についての文書
   文書管理規定，文書管理台帳

別の観点から見ると，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る。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が必要となる。電子文書によって何かを証明しようとする場合にも同様で，当該電子文書が作成された背景情報をあわせて示すことが重要と考えられる。すなわち電子文書(What)をポツンと単独で提示しても信頼性がなく，その文書がどのような経緯で何のために誰がいつ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る。

このうち，「いつ」，「だれが」，「何を」の三つの要素は，例えば，電子署名とタイムスタンプにより証明可能となる。それ以外の，「なぜ」を明らかにするには，電子文書の作成目的や運用ルール，また，何の業務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るのでこれらの規程類の整備と保存が重要となる。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る。

4.2. 文書そのものの信頼性確保

電子文書そのものの信頼性確保のために特に重要な事項として，真正性（作成者とされているものが実際に作成したこと），成立時期，完全性があげられる。完全性は，すべての電子文書・情報に共通であるが，作成者の真正・成立時期の真正については，文書の種類により重要度が異なる。

外部から受領した電子文書の多くのものについては，真正性が重要である。特に意思表示に係るものについては，真正性が非常に重要である。しかし，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ケースが多い。

内部の文書について，まず，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。

内部の責任追及のための文書については，真正性が重要である。特に，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管にあたっては，システム管理部門等もその指揮命令かにあるため，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，作成時期の証明が，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，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，真正性の証明に大きく寄与することになる。

4.3. 信用性確保手段の選択

信用性に影響を与える真正性，成立時期の正しさ，完全性のそれぞれの要素については様々な実現方法が存在し，安全性の期待値もさまざまである。技術的な安全性は信用性を左右し，どの方法を選択するかは，期待値にかけるコストと証拠としての重要性の予測に依存する。

以下，それぞれについて代表的な方式に対する信用性の一考察を示す。

これ以外にも電子公証制度を利用する方法もあるが，本テーマとは前提が異なることからここでは触れない。

4.3.1. 真正性

(1) 作成者の意思表示の方法

電子文書の真正性の保証(ensure)に関しては，印鑑に近いイメージとしてまず電子署名が挙げられるが，意思表示方法として捉えると，PAD を使った電子サインや，電子決裁等で使われている“ワンクリック”意思表示もその範疇にある。それぞれ，信頼性のレベルは，前提となる事項や認証方法がどのように厳密に管理されているかにより異なる。

表 4.3-1 に意思表示の方法ごとの前提条件，意思表示確認方法，認証方法を記す。

表 4.3-1 意思表示の方法

	方法	前提条件	意思表示確認方法	認証方法
1	電子署名	危殆化していないアルゴリズムと本人による秘密鍵の厳密な管理	公開鍵による検証	認証局または対面で身分証明書提示＋公開鍵手渡し
2	電子サイン	署名値が他の文書に流用されないための署名値と文書の関係の厳密な管理	筆跡	身分証明書等による対面確認あるいは事後の筆跡鑑定
3	ワンクリック	クリック事象及びクリックに至る経緯も含めた情報と文書の関係の厳密な管理	事前の認証（ID，パスワード発行）及びログオン履歴	認証システム

(2) 意思表示の信用性

電子署名による意思表示の信用性は，署名に使用するアルゴリズム，秘密鍵の保管方法（耐タンパか否か，認証局の運用の信頼性（公的あるいは認定認証局か否か，認証局における本人確認の厳密さに依存する。(**表 4.3-2**)

一方，電子サインの信用性は，署名値の構成要素，署名値と文書の関係の管理方法，及び署名時の対面対応者による本人確認の厳密さに依存する。(**表 4.3-3**)

ワンクリック意思表示の信用性は，クリック事象と文書の関係の管理方法，及び認証システムにおける本人確認の厳密さに依存する。(**表 4.3-4**)

表 4.3-2　電子署名の信用性イメージ

信用性	アルゴリズム	秘密鍵保管	認証局	本人確認
H	RSA2048	耐タンパ装置	認定	住民票
M				
L			非認定	メールアドレス

表 4.3-3　電子サインの信用性イメージ

信用性	署名値の構成要素	署名値と文書の関係管理	本人確認
H	筆跡，筆圧，速度	厳密な管理	対面，免許証
M			
L	筆跡		会員カード

表 4.3-4 ワンクリック意思表示の信用性イメージ

信用性	クリック	クリックと文書の関係管理	本人確認
H	パスワード要求		
M			
L	クリックのみ	非改ざん	

4.3.2. 成立時期の正しさ

(1) タイムスタンプ方法

電子文書の成立時期の推定は，一般にタイムスタンプに依るところとなる。タイムスタンプは，第三者機関が提供するタイムスタンプサービスの利用と，システムの時刻を使ったタイムスタンプに大別される。(**表 4.3-5**)

表 4.3-5　タイムスタンプ方法

タイムスタンプ方法	備考
第三者機関が提供するタイムスタンプサービスの利用	
システム時刻	

(2) タイムスタンプの信用性

第三者機関が提供するタイムスタンプの信用性は，提供者，時刻源，非改ざん措置に依存する。(**表 4.3-6**)

システムタイムスタンプの信用性は，時刻源と非改ざん措置に依存する。(**表 4.3-7**)

表 4.3-6　第三者機関が提供するタイムスタンプの信用性イメージ

信用性	タイムスタンプ局	時刻源	非改ざん措置
H	認定	原子時計	↓
M			↓
L			タイムスタンプ局の署名

表 4.3-7　システムタイムスタンプの信用性イメージ

信用性	時刻同期	非改ざん措置
H	GPS 同期	厳密な運用を行う
M	NTP	
L	CPU クロック	なし

4.3.3. 完全性

(1) 完全性実現方法

文書（記録）の完全性を担保する方法には様々なものがあるが，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，ソフトウェア統制機能を持たせることである。ソフトウェア統制機能とは，エンドユーザーによる編集や削除を許可せず，文書（記録）へのアクセスのみ許可する機能である。一方で，文書（記録）管理スタッフは文書（記録）の廃棄は行なえるが，編集は許可されない。文書（記録）の完全性を確保するうえで，たいていの状況下においてソフトウェア統制は満足できるものである。

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管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。

非改ざんに着目すると，これには，改ざんを防御する方法と，改ざんを検知可能にする（あるいは，改ざんを検知可能にすることにより改ざんを抑止する方法とがある。

表 4.3-8 に代表的な改ざん防御／検知の実現方法を示す。

表 4.3-8　改ざん防御／検知の実現方法

方法	具体的方法	備考
改ざん防御	WORM 媒体に記録する	
	耐タンパ装置に保管する	
	ソフトウェア統制により変更･削除を制限する	
改ざん検知	電子署名	
	タイムスタンプ	
	ダイジェスト値の管理	

WORM　Write Once Read Many

(2) 完全性に対する信用性

信用性は，元となる完全性実現方法に依存する。

4.4. 文書情報管理システム

情報過多の時代，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，これまでの議論から，このシステムは次の要件を満たす必要があるといえる。もちろん，管理の規模によっ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) 文書化された文書の作成および取得時点における環境情報（**4.1** 参照)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なこと。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) 目的とする文書が直ちに取り出せること。
(6) 第三者による(1)～(4)の検証が可能なこと。

これらを実現するには，文書が体系的・組織的に作成され，維持管理される必要がある。「文書が，そうだと称する通りのものであり，作成者であると称する者が確かにそれを作成したこと」を証明できるようにするには，十分な対策を講じなければならない。どこかに弱点があれば，活動の証拠としての文書の重みを減じることになるからである。さらに，文書の利用性を保証するには，必要に応じ文書を検索し，閲覧し，解釈できる必要がある。

このように，文書のコンテンツ，構造，コンテキストを管理し，その完全性と利用性を長期にわたり保証するシステムが必要となる。

しかしながら，このような文書情報管理システムが，前述の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。

何らかの，第三者による評価の仕組みが必要となろう。

4.5. 証拠のパッケージ化

例えば，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場合を考えると，「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の提出が有効と考えられる。

- 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
- 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。

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。

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。

5. まとめ

本プロジェクトでは，電子文書の証拠提出を想定して，その条件や信頼性確保のための方法を検討してきた。今回，中間的な結論として一つの方向性をまとめることができた。

ポイントは 3 つに整理される。

① 電子文書の作成および取得時の業務や組織などの環境情報を，電子文書と合わせて保存しておくこと
② コストと期待する信頼性のバランスを考慮して真正性や信用性を担保する適切な方法を選択すること
③ 電子文書の証拠提出に耐える適切な文書管理システムを構築（あるいは選択）すること

これらのポイントについて，より具体化して広く示して行くことにより，訴訟対策として必要な方策が明らかになり，電子文書の普及に大きく貢献すると考えられる。

JIIMA 電子文書信頼性向上プロジェクト

座 長	宮内 宏	弁護士　宮内・水町 IT 法律事務所
	甲斐荘博司	JIIMA 法務委員長　株式会社ジェイ・アイ・エム
	木村 道弘	JIIMA 標準化委員長・特別研究員
	西貝 吉晃	日本大学法学部専任講師
	西山 晃	JIIMA 法務委員　セコムトラストシステムズ株式会社
担当理事	高橋 通彦	JIIMA 理事長
事務局	長濱 和彰	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