デジタル時代におけるノウハウの保護～デジタル証拠を中心に～

弁護士　箱守英史

1. はじめに

DX（デジタル・トランスフォーメーション），デジタルシフトという言葉に代表されるように，近時はデジタル化への対応を怠ることはできません。そこで，ここではデジタル証拠にスポットを当てて，企業におけるノウハウ保護に有用な情報を整理したいと思います。なお，以下では，技術的な「ノウハウ」を想定して記載しておりますが，言うまでもなく，そのほかの分野でも利用することができます。

2. ノウハウの利用・保護についての一般論

まず，デジタル証拠に特徴的なお話をする前に技術的なノウハウの利用と保護について，もう一度整理します。

2.1. 「オープン＆クローズ戦略」と「先使用権」

技術的なノウハウの利用に関して「オープン＆クローズ戦略」が提唱されることがあります。これは，「企業が保有する技術について，差別化領域である自社のコア技術をクローズ化して技術的優位性を確実にするとともに，一部の技術をオープン化して製品関連技術を広く普及させて製品市場の拡大を図ることで事業収益を最大化する」事業戦略とされます (*1)。

技術をノウハウとしてクローズ化，つまり秘匿化しておけば，他社がその技術に思い至らない限りは，自社の競争優位を持続的に維持することができます。その一方で，秘匿化するということは，他社による特許の取得を妨げることはできません。したがって，他社が同一技術について特許権を取得してしまうというリスクもあるのです（なお，このことは積極的に技術を秘匿化している場合に限らないことは言うまでもありません）。

技術をノウハウとしてクローズ化するのであれば，そのノウハウが不正競争防止法上の営業秘密に該当するようにして，同法に基づくノウハウの保護が受けられるようにすることはもちろんのこととして，他社が特許権を取得してしまったときの備えもしておかなければなりません。他社の特許権の行使に対しては，自社の先使用権を主張することが考えられます。先使用権が認められれば，自社のノウハウを継続的に利用して事業を継続することができます。先使用権が認められる要件についてここでは詳細に触れませんが，大雑把にいうと，特許出願の際に，発明（つまりは，秘匿化したノウハウ）を完成させ，その製造や販売などをしていたこと，又はその準備をしていたことを立証しなければなりません。

2.2. 先使用権の立証のために（デジタル証拠との関係から）

そのためには，自社内においてノウハウに関する研究ノートその他の資料を適切に管理しておかなければなりません。そして，それらの資料をもとに，他社が「特許出願」をした時点において自社が発明を完成させていたこと，自社がその発明の実施である事業（の準備）をしていたことを裏付けていかなければなりません。

このことから明らかなように，先使用権の立証には時的な要素が非常に重要になります。そこで，例えば，公証役場で確定日付を取得するなどの方法で，資料の存在時点を確実に立証しうるようにすることが重要とされてきました。

ただ，このような方法は，基本的には紙が存在することが前提です。これからは，ペーパーレスを推進するために紙媒体でプリントアウトしなくなることも多くなるでしょうし，そもそも，データ量が多すぎてプリントアウトして保存するのに適さなくなることもあると思います。このほか，画像，動画，音声などの情報を証拠として保存しておきたいという要請もあろうかと思います。派生するデータが多数あるので，確定日付をもらうためにその都度公証役場に行くのが難しいということもあるかもしれません。

もちろん，今後も紙媒体での証拠の保存の重要性は変わることはないかもしれません。特に，重要な資料についてはそうかもしれません。その一方で，デジタル証拠についても，その保存・管理が重要になっていることは間違いないでしょう。

3. デジタル証拠の証明力を高めるための手法

そこで，デジタル証拠についても，その存在時点（作成日時）を後日に明らかにできるように管理する必要があります。また，デジタル証拠を長期的に保存しておかなければなりません。

以下では，存在時点を裏付けるための手法として，タイムスタンプ及び電子公証制度について説明するとともに，それに関連して電子署名についても簡単に述べることにします。そのうえで，電子データの保存に関して注意すべき事項に触れることにします。

3.1. タイムスタンプ

3.1.1. タイムスタンプとは

「タイムスタンプ」とは、「電子データに付与される時刻情報等の総体であって，①当該電子データがある時刻に存在していたことを示すためのものであること，及び②当該電子データについて改変が行われていないかどうか確認することができるものであることの要件を満たすもの」とされています（*2）。総務省の「タイムビジネスに係る指針」（平成16年11月5日）でも同様の定義がされています。この定義の要点は，①ある時点での存在証明及び②非改ざん証明ということになります。情報セキュリティの観点からは，否認防止に有効な技術と言われます。

3.1.2. タイムスタンプが必要な理由

このようなタイムスタンプが必要になるのは何故でしょうか。

まず，コンピュータについては，その内部の時刻を任意に設定できてしまうからです。言い換えれば，電子データの生成時刻を好きなように設定できてしまうのです。また，電子データには，物質的な劣化が存在しないという特性がありますので，新しいものと古いものを視覚的に区別することもできません（*3）。さらに，電子データの内容を変更したとしても，それがいつのことか分からないというおそれもあります。

したがって，先使用権との関係でいうと，ある時点での実験成果を示す電子データがあったとしても，それだけでは，その電子データの作成時期や内容を否定されてしまうおそれがあるのです。言い換えれば，事後的に時刻を変更したとか，その後にデータを書き換えたとかいう反論を許すことになるのです。

これに対して，タイムスタンプを利用することで，その電子データについて，①（ある時点における）存在証明及び②非改ざん証明をすることができるのです。このような理由からタイムスタンプは先使用権の根拠となる電子データを保存する際に非常によく利用されているのです。

3.1.3. タイムスタンプの仕組み

このようなタイムスタンプの仕組みを簡単にご紹介します。なお，分かりやすさを優先しておりますので，技術的に厳密な説明については専門の文献をご参照ください。

一言でいうと，タイムスタンプは，信頼できる第三者（Trusted Third Party: TTP）の時刻情報などを電子データに付与することでその信頼性を確保しようという考え方に基づくものです。なお，この考え方は後述する電子公証制度や電子署名も同様です。

3.1.3.1. タイムスタンプの付与

まず，タイムスタンプは次のようにして付与されます（図1参照）。

①タイムスタンプを取得したい者（要求者）が電子データからハッシュ値を生成します。

まず，元の電子データを規則性のない別のデータ（ハッシュ値）に変換します。ハッシュ値は元の電子データが少しでも異なっていると全く別の値になります。ですから，元の電子データが少しでも変更されていると，得られるハッシュ値は全く別の値になってしまいます。この特性をうまく活用して非改ざん性を基礎付けるのです。

②要求者はこのハッシュ値を時刻認証局（Time Stamping Authority: TSA）に送ります。

③時刻認証局（TSA）は，送られてきたハッシュ値に時刻の情報を連結します。この際に，時刻の情報がすり替えられたり，改ざんされたりしないような措置を施します（ここでの措置については3.1.3.2. で説明します）。

④なお，③の時刻の情報は，時刻認証局が時刻配信局（Time Authority: TA）から配信を受けた正確な時刻に基づくものです。

⑤時刻認証局（TSA)は，時刻の情報を連結したハッシュ値（タイムスタンプトークン）を要求者に返信します。

⑥要求者はタイムスタンプトークンを元の電子データとセットで保管します。なお，PDF形式のファイルではタイムスタンプを埋め込んで保存しておくこともできます。

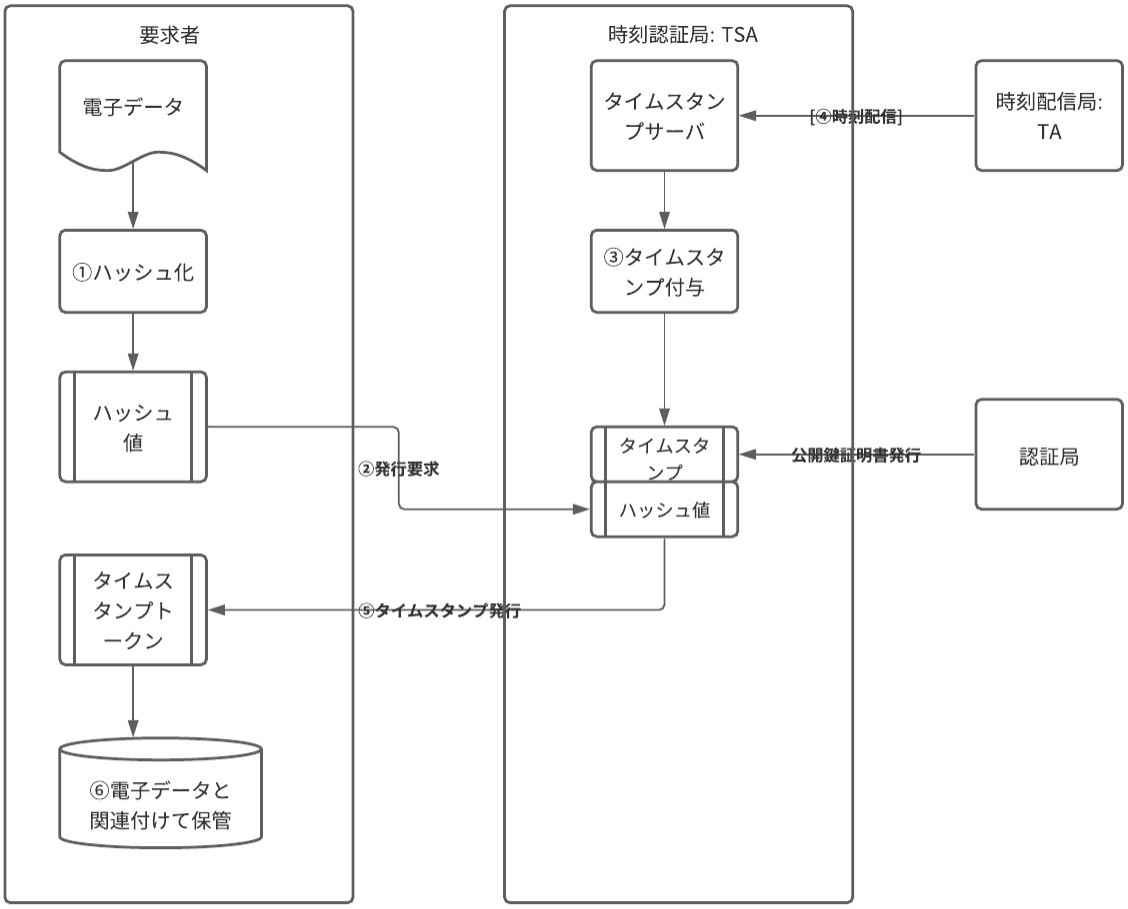

図1　タイムスタンプの発行
（電子文書保存のしくみと実務（*9） p.63を参考に筆者作成）

3.1.3.2. タイムスタンプの検証

それでは，電子データが改ざん等されていないことはどのようにして判別することができるのでしょうか。ここで，先ほど説明した③の「措置」（タイムスタンプの生成方式）には複数の方式があります。すなわち，(a) デジタル署名方式，(b) アーカイビング方式，(c) リンキング方式です。ただ，後述する日本データ通信協会により認定されている事業者は全てデジタル署名方式を採用しているようですので，ここでは(a) デジタル署名方式を前提に検証方法を説明します（図2参照）。

この方式は，時刻認証局（TSA)がタイムスタンプに電子署名を付与するものです（電子署名については3.3.に後述します）。そこで，タイムスタンプの検証の際には，まず電子署名がその時刻認証局（TSA)のものであるのかを確認します。問題がなければ，タイムスタンプトークンから電子データのハッシュ値を取り出します。この

ハッシュ値をもとの電子データのハッシュ値と比較するのです。既に述べたように，電子データが少しでも変更されているとハッシュ値は別物になります。これらのハッシュ値が一致すればその電子データは変更等されていないことになります。また，タイムスタンプトークンに含まれている時刻の情報からその存在していた時点を確定することもできます。

デジタル署名方式の特徴は，図2にあるように，時刻認証局（TSA)に依頼しなくても，タイムスタンプの検証が可能という点にあります（他の二方式は時刻認証局（TSA）が検証する必要がある）。その一方で，電子署名を利用していますので，それに関連する証明書の有効期間が設定されてしまうという問題もあります。

なお，証明書の有効期限については，（簡単に言うと）タイムスタンプの有効性を検証することができる情報をひとまとめにして，さらにタイムスタンプを付与するという手法で対応することができます（長期署名）。10年ごとに新しいタイムスタンプを付与していくようなイメージかと思います。詳細については，ここでは割愛します。

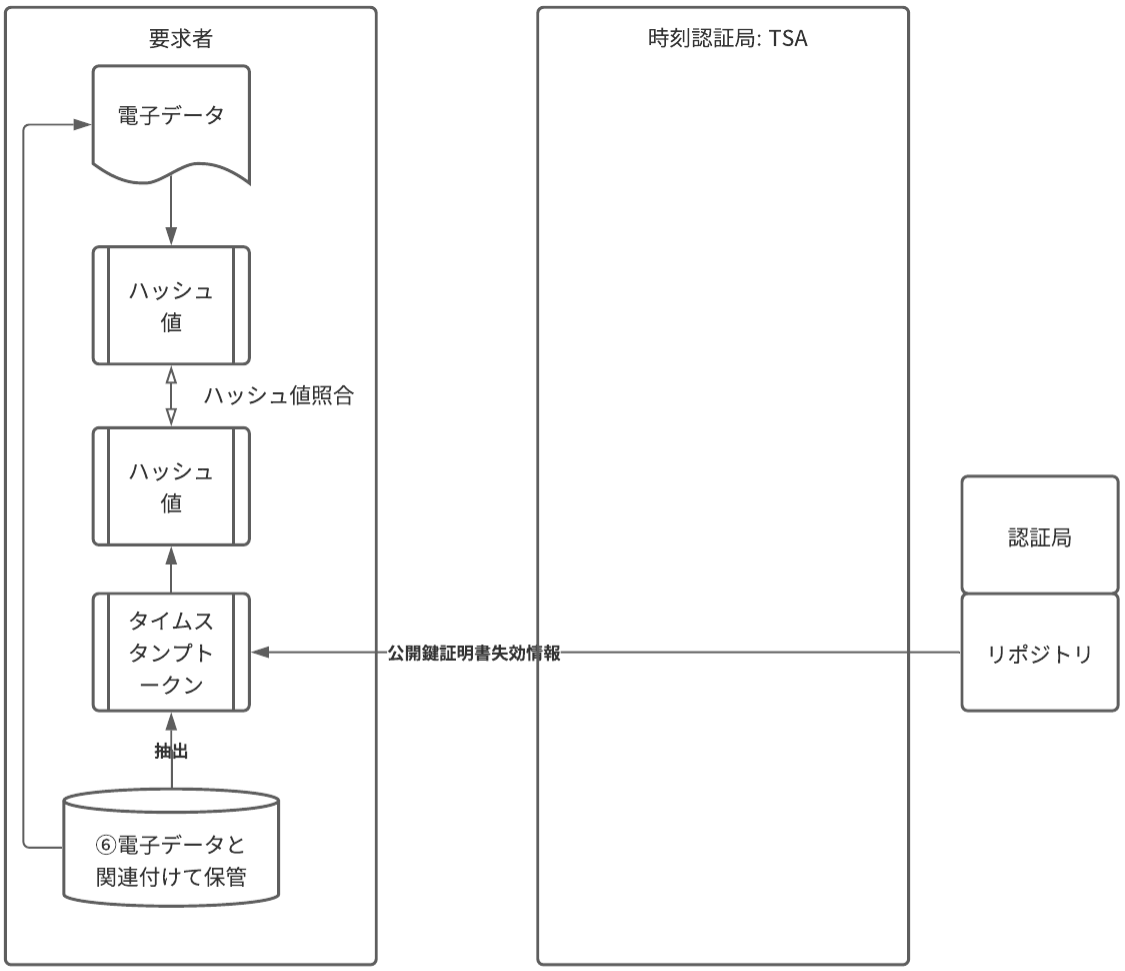

図2　タイムスタンプの検証
（電子文書保存のしくみと実務（*9） p.63を参考に筆者作成）

3.1.4. タイムスタンプ認証制度

このように，時刻認証局（TSA）を信頼できる第三者（TTP: Trusted Third Party）として，電子データの信頼性を確保するのです。後述の電子署名などとあわせて，このような信頼性を確保するための基盤となるサービスをトラストサービスといいます。電子データを利用して安全・安心な取引をすることができるようにするためには，このようなトラストサービス自体の信頼性が必要です。EUではeIDAS(Electronic Identification and Trust Service Regulation)という規則が制定されていて，それによる認定を受けたトラストサービスは適格トラストサービスとされ，適格トラストサービスには，一定の法的効力が認められています。

日本では，電子署名については，電子署名法による一定の規定はありますが，タイムスタンプについては，日

本データ通信協会による民間の認定制度（タイムビジネス信頼・安心認定制度）しかありませんでした。そこで，総務省において「タイムスタンプ認定制度に関する検討会」による検討が続けられ，2021年4月から総務省の告示として「時刻認証業務の認定に関する規程」が施行されています。

この告示は，国としてのタイムスタンプの認定制度を設けることで，その信頼性を担保しようとするものです。時刻認証局（TSA）の業務が杜撰なものだと，そこで付与されたタイムスタンプも信用することができません。そこで，告示では，時刻認証局（TSA）の時刻認証業務が所定の要件を満たす場合にのみ，総務大臣が認定時刻認証業務として認定することができるようになっています。また認定を受けた事業者はその旨の表示をしなければならないとされています。さらに，認定に関する情報をトラステッドリスト（仮称）として総務省ウェブサイトに掲載することなどが検討されています。これにより，ユーザーが安心してサービスを判別することができるようになるというわけです。認定制度の運用等も含めて引き続き注視が必要でしょう。

先使用権の立証などの重要な局面での使用が想定される電子データについては，総務大臣の認定を受けたサービスを利用するのが望ましいでしょう。

なお，認定の有無が重要であることはもちろんですが，サービスの選定にあたっては，そのほかの付加価値にも注目しなければなりません。例えば，電子データを指定のフォルダに保管することにより自動的にタイムスタンプが付与されるサービスや，前述した長期署名についても自動で対応できるサービスなどが存在しています。必要なサービスの内容と費用感から適切なタイムスタンプサービスを選択してください。

3.2. 電子公証制度

電子公証制度も信頼できる第三者（TTP）としての役割を果たすものです。

一般的に，公証役場で紙の文書に確定日付を付与してもらうことはよく行われていると思います。電子公証制度では，紙ではなくPDFファイルなどの電子データに確定日付を付与してもらうことができます（以下，「電子確定日付」とします。）。また，電子データの作成者を証明する「認証」をすることもできます。会社設立の際の定款の電子「認証」はよく利用されているので，ご存じの方も多いかもしれません（なお，この場合，印紙税（4万円）を節約することができます）。

3.2.1. 電子確定日付の付与

先述の通り，先使用権の立証においては，その文書の存在していた（作成された）日時が重要になります。したがって，重要な電子データについては，「電子確定日付」を付与してもらうのがよいでしょう。

電子確定日付に関しては，法務省が運営する「登記・供託オンライン申請システム」を用いて嘱託したい電子データを送信して，公証人がその電子データに日付情報を付与します。日付情報を付与された電子データはインターネット経由で取得することができます。紙ベースの文書については，確定日付の付与を受ける際に現実に

公証役場まで行く必要があるでしょうから，使い勝手はよいかもしれません（なお，電子認証については，自身の電子署名を付与して，公証役場で当該電子署名の確認などの手続きが必要になりますのでご注意ください）。

とはいえ，実際に，電子確定日付の付与を受けるには，日付情報を付与してもらう公証人を選んで事前に嘱託内容に不備がないかを確認してもらうなどの手間がありますので，前述したタイムスタンプの場合と比べてると一手間要するということになるでしょう。

その一方で，電子確定日付に関するデータは50年間にわたり保存されます（*5）（電子公証制度により認証されてた電子文書は20年間とされています）。タイムスタンプでも長期署名の仕組みはありますが，この保存年数は魅力があるのではないでしょうか。また，公証人は国の公務である公証事務を担う公務員であるという点でも信頼度は高いかと思います。

3.2.2. 電子確定日付の証明

このようにして確定日付を得た電子データは次のように検証することができます。電子データが改竄されていないことを証明するためには，公証人に対して，情報の同一性に関する証明の請求をします。公証人は，証明の請求者が保管していた電子データのハッシュ値と，公証人が保管していた電子データのハッシュ値とを比較して，これらが同一であれば同一であることの証明を発行します。

また，謄本の請求に相当するものとして，公証人から同一の情報の提供を受けることもできます（ただし，電子確定日付の付与の際に同一内容の情報を保管するように請求しておかなければなりません）。先程の電子データの保管期間からすると，かなりの長期間にわたり，謄本に相当する電子データの申請をすることができると思われます。

3.2.3. 電子確定日付の利活用

このような電子確定日付の利点を生かして電子データの証明力を確保していくことになります。なお，電子確定日付に関する手続の詳細については法務省ウェブサイト「公証制度に基礎を置く電子公証制度ご利用の手引」を確認ください（*6）。

また，日本公証人連合会によれば，電子確定日付センターと称する複数の公証役場を指定しており，こちらで大量の電子確定日付を迅速に付与することができるようにしています（*7）。多くの電子確定日付の付与が必要なときには，こちらの利用を検討いただいてもよいでしょう。

3.3. 電子署名

先使用権の立証という観点からは，以上のような，タイムスタンプや電子確定日付を利用することが多いかと

思われます。このほかには，電子データの証明に関する手法として電子署名があります。先述の通り，電子署名はタイムスタンプにも利用されています。

3.3.1. 電子署名とその特徴

電子署名はその電子データを誰が作成したのかを明らかにするものです。注意すべきは，証明の対象となるのが「電子データの作成者」であって，その電子データに表現された発明などの「発明者」ではないことです。つまり，電子署名をしていることで発明者を直接的に基礎付けることはできないのです。契約書等（処分証書）であれば，作成者が誰であるのかは決定的な意味をもちますので，電子署名は非常に有効な技術になります。しかし，発明の事実などを立証する方法としては少し事情が異なります。電子署名の活用にあたっては，このような特性をよく把握しておく必要があります。

3.3.2. 電子署名の効果

一定の要件を満たした電子署名ついては，「電子署名及び認証業務に関する法律」（以下，「電子署名法」とします。）第3条により「本人の意思に基づいて作成されたもの」（真正に成立したもの）であると推定されます。

それでは，どのような電子署名がその要件を満たすことになるのでしょうか。電子署名について，大まかに，①当事者が署名をするのか，②当事者以外の立会人とでもいうべき第三者が署名をするのかという区別があります。また，①の当事者が署名するものについても，①(a)ローカルの署名なのか，①(b)リモートの署名なのかという区分があります。

①(a)は，パソコンやICカードに保管された秘密鍵（印鑑のようなものと考えてください）を用いて署名するものです。例えば，マイナンバーカードを用いて電子確定申告の際に電子署名をするようなケースです。①(b)はその秘密鍵をサーバーに保管しておいて，必要なときにログインして電子署名を付与するイメージです。便利ではありますが，ログインIDやパスワードの管理が不十分であると，それらを知った者が電子署名をすることができてしまうという問題もあります。

②は立会人型などと言われており，①(b)と同様にリモートで署名がされるのですが，当事者ではなくサーバー（立会人）の電子署名を付すという点に特徴があります。②は当事者の電子証明書の準備などがいりませんので，手軽に利用することができます。ただ，その反面，本人が署名したものといえるのかという問題もあります。

このような方式の違いから，もっとも本人性が確実なものが①(a)であり，その次に①(b)，最後に②となることがおわかりいただけると思います。前述した電子署名法3条の推定効（本人の意思に基づいて作成されたものという推定）は，②の立会人型電子署名であっても，一定の要件（固有性の要件）を満たせば認められるとの見解が示されています（*8）。ただ，この問題については，最終的には裁判所の判断を待たなければはっきりしたことを述べることはできないと思います（以前は②については推定効が認められないとの見解が多かったように記憶しています）。また，ここでいう「固有性の要件」がどのようなものなのかもはっきりしていません。

電子署名サービスの導入にあたっては，このような事情も頭にいれておくべきでしょう。いずれにしても，電子

署名をどのような目的で利用するのかを決めて，どのようなレベルの電子署名（サービス）を採用する必要があるのかを検討すべきでしょう。

3.4. 電子文書・データの管理

最後に，電子文書・データの管理について述べておきます。どんなに強力な証拠書類であっても紛失したり，読めなくなったりしては意味がありません。電子データでも同じことです。また，先使用権を立証するためには，その証拠単体ではなく，前後の証拠との関係も重用です。

3.4.1. 電子データの見読性など

第一に，電子データ自体の保存に関する問題です。電子データの保存は紙の文書よりも複雑です。なぜなら，電子文書は，ハードウェア，OS，アプリケーションなどの各要素の上に成り立っているからです。アプリケーションのバージョンアップなどで電子ファイルの互換性が失われた経験のある方もいらっしゃるかもしれません。つまり，時間がたっても，電子データを表示することができるようにしておかなければならないのです。文書の見読性が損なわれないようにする必要があるなどと言います。

見読性の阻害要因としては，記録媒体の劣化，ハードウェアインターフェースの変化，ドライバの非互角，OS間のファイル非互換，アプリケーションのバックワード非互換及び文字コード改訂などが挙げられます。これらのリスクを洗い出したうえで，電子データ保存のための組織的な取り扱いプロセスを確立しておく必要があります。
また，長期保存に際してはファイル形式も重要です。一般的に，長期保存に適したファイル形式として，PDF形式，TIFF形式及びXML形式が挙げられます。JIS Z6016では前二者が推奨されているようです。また，ご存知のとおり，PDF形式はISO 32000-1として標準化されています。長期的な保存のためには，これらのファイル形式によるのが望ましいでしょう（*9）。

なお，電子データにタイムスタンプを付与した場合には，付与されたタイムスタンプトークンを電子データとセットにして保管しておかなければなりません。タイムスタンプトークンを埋め込む形式のものであれば，意識はしなくてよいのでしょうが，そうでない場合には，これらが1セットで存在することで意味をもつことを忘れないようにしなければなりません（*10）。

3.4.2. 一般的な意味での文書管理

第二に，一般的な意味での文書管理です。こちらは電子データに特徴的なものはそれほどないかもしれません。各種の電子データを関連付けていくこと，メタデータと言われるその文書に関するデータ（分類，作成者，作成時期，保存期間…）の管理をすることが重要でしょう。これらは紙媒体の場合でも変わりはありません。

ただ，電子データならではの工夫もできそうです。例えば，PDF形式で保存するのであれば，各種の映像データや設計図などをPDFファイルの添付ファイルとして一体化することなどができます。このようにしておけば，電子文書以外のデータも関連付けて保存しておくことができます（特許庁p.42，73）。そのほかにも，各社で創意工夫をする余地はありそうです。

4. さいごに

以上，先使用権の立証という観点から，電子データに特徴的な証明力の確保のための手法について説明させていただきました。そのほか，先使用権の活用に関する全般的な手法に関しては特許庁「先使用権制度の円滑な活用に向けて」（*1）に詳しく説明されているので，こちらもご参照ください。本稿がデジタル時代における電子データの管理とそれによるノウハウの保護に多少なりとも役立てば幸いです。

以上

<後注>

*1: 特許庁「先使用権制度の円滑な活用に向けて」平成28年5月，令和元年9月改訂
https://www.jpo.go.jp/system/patent/gaiyo/senshiyo/document/index/senshiyouken_2han.pdf

*2: 「時刻認証業務の認定に関する規程（案）」（総務省告示として令和3年4月施予定）参照。なお，本稿執筆時点では，未施行でしたので(案)としています。
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00090.html

*3: このほかに，デジタル署名や公開鍵証明書に有効期限があることもタイムスタンプを必要とする理由とされます（*9の文献に詳しく説明されています）。

*4: 総務省「タイムスタンプ認定制度に関する検討会　取りまとめ」令和3年3月

*5: 日本公証人連合会ウェブサイト「公証事務　7-5 電子公証」 http://www.koshonin.gr.jp/business/b07_5

*6: 法務省ウェブサイト「公証制度に基礎を置く電子公証制度ご利用の手引」
http://www.moj.go.jp/MINJI/DENSHIKOSHO/denshikosho1.html

*7: 日本公証人連合会ウェブサイト「電子確定日付センター」 https://www.koshonin.gr.jp/center

*8: 総務省・法務省・経済産業省「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ＆A（電子署名法第3条関係）」
https://www.meti.go.jp/covid-19/denshishomei3_qa.html

*9: 木村道弘・前田陽二・宮崎一哉著「電子文書保存のしくみと実務（第2版）」中央経済社，2008年，pp. 137-147参照

*10: タイムスタンプトークンの長期的な保管のために，独立行政法人工業所有権情報・研修館(INPIT)では，タイムスタンプトークンを保管し，預入証明書を発行するサービスを提供していました。ただ，利用の実績が少なかったようで，2021年3月31日をもってサービスを終了するとのことですので，ご注意ください。INPIT「タイムスタンプ保管サービスの終了について」https://www.inpit.go.jp/about/topic/20200930.html