e－文書法におけるタイムスタンプ適用ガイドライン

平成１７年１０月

タイムビジネス推進協議会

目　　次

１．はじめに ..... - 1 -
１．１　背景 ..... - 1 -
１．２　本ガイドラインの対象範囲 ..... - 1 -
２．e-文書の業務プロセスモデル ..... - 4 -
２．１　e-文書のカテゴリ ..... - 4 -
２．２　電子化文書のライフサイクル ..... - 4 -
２．３　紙文書の電子化文書生成の業務プロセス ..... - 5 -
２．３．１　紙文書をスキャニングして電子化するプロセス ..... - 5 -
２．４　電子化文書のレコードマネージメントの運用システム ..... - 7 -
３．電子署名及びタイムスタンプの必要性 ..... - 8 -
３．１　文書の電子化における問題点 ..... - 8 -
３．２　電子署名とタイムスタンプの効果 ..... - 8 -
３．２．１　電子署名の効果 ..... - 8 -
３．２．２　タイムスタンプの効果 ..... - 9 -
３．２．３　タイムスタンプと電子署名の組み合わせの効果 ..... - 9 -
３．３　電子文書の長期保存 ..... - 9 -
４．電子化文書の真実性確保のために用いるタイムスタンプ適用ガイドライン ..... - 11 -
４．１　電子署名の付与対象とタイミング ..... - 11 -
４．１．１　基本的な考え方 ..... - 11 -
４．１．２　実務的な運用 ..... - 11 -
４．２　タイムスタンプの付与対象とタイミング ..... - 12 -
４．２．１　文書存在証明 ..... - 12 -
（１）基本的な考え方 ..... - 12 -

（２）実務的な運用 ..... - 13 -
４．２．２　長期保存証明 ..... - 14 -
（１）基本的な考え方 ..... - 14 -
（２）実務的な運用 ..... - 14 -
４．３　電子署名とタイムスタンプ付与例 ..... - 16 -
４．４　電子署名及びタイムスタンプの格納方式とフォーマット ..... - 17 -
４．５　タイムスタンプ検証 ..... - 19 -
４．５．１　タイムスタンプ検証タイミング ..... - 19 -
４．５．２　タイムスタンプ検証例 ..... - 20 -
５．電子化文書の真実性確保のためのタイムスタンプサービス利用上の留意点 ..... - 22 -
５．１　タイムスタンプの有効性について ..... - 22 -
５．１．１　タイムスタンプの有効期間 ..... - 22 -
５．１．２　タイムスタンプ事業者の事業継続性 ..... - 22 -
５．１．３　暗号技術の脆弱性の判明 ..... - 22 -
５．２　　タイムスタンプの時刻の精度等について ..... - 22 -
５．２．１　時刻の信頼性 ..... - 22 -
５．２．２　タイムスタンプの要求時刻と付与される時刻の差 ..... - 22 -
５．３　免責事項について ..... - 23 -

１．はじめに

１．１　背景

2001 年 1 月、内閣に設置された高度情報通信ネットワーク社会推進戦略本部（IT 戦略本部）は『5 年以内（2005 年まで）に世界最先端の IT 国家を実現する』ことを目標とし、「e-Japan 戦略」を打ち出した。これに伴うさまざまな施策により急速に IT インフラの整備が進んだ。そしてその利活用を着実なものとするために、2003 年 7 月には「e-Japan 戦略Ⅱ」が、2004 年 2 月には e-Japan 戦略Ⅱを加速させるために政府として取り組むべき重点施策を明らかにした「e-Japan 戦略Ⅱ加速化パッケージ」が策定された。

e-Japan 戦略Ⅱ加速化パッケージにおいて重点施策として位置づけられた 5 分野の一つ、「IT 規制改革の推進」において取り上げられた具体的施策に、「e-文書イニシアチブ」がある。現状では保存が義務付けられている文書のなかで電子的な保存が認められている文書は少数の一部の文書のみに限られているが、e-文書イニシアチブでは、『法令により民間に保存が義務付けられている財務関係書類、税務関係書類等の文書・帳票のうち、電子的な保存が認められていないものについて』、『原則としてこれら（すべて）の文書・帳票の電子保存が可能となるようにすること』を目的としている。更にこれを可能とするための『統一的な法律（通称「e-文書法」）の制定等を行う』ともしている[1]。

上記方針に沿い、2004 年 11 月 19 日に「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（通則法）及び「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」（整備法）が成立、2005 年 4 月 1 日に施行されることとなった。これら通則法、整備法の総称として、e-文書法と呼ぶことにする。

電子保存を容認するにあたり、『近年の情報技術の進展等を踏まえ、文書・帳票の内容、性格に応じた真実性・可視性等を確保』することが要件として挙げられており、それら『電子保存の容認の要件』を明確化することが要請されている。本ガイドラインでは、タイムビジネス推進協議会（以下「TBF」という。）としての立場から、電子保存の容認の要件に応えるために、タイムスタンプの適用の在り方についてまとめる。

なお、タイムスタンプサービス提供者側の要件については、「信頼されるタイムスタンプ技術・運用基準」を参照されたい。

１．２　本ガイドラインの対象範囲

（１）e-文書法が対象とする文書の定義
e-文書法では、当初から電子的に作成された書類を電子的に保存することと、書面で作成

[1] ＩＴ戦略本部の e-Japan 戦略 II 加速化パッケージのお知らせページ
（http://www.kantei.go.jp/jp/singi/it2/kettei/040206honbun.html）より。

された書類をスキャナでイメージ化して電子的に保存することの双方を視野に入れている。本ガイドラインでは、JIS Z6016:2003「紙文書及びマイクロフイルム文書の電子化プロセス」による定義に従い、それぞれの電子的な文書を「電子文書」と「電子化文書」の語を用いて区別することとする。JIS Z6016:2003 による両語の定義を次に示す（原文どおり）。

電子文書：ワードプロセッサ、PC（パーソナルコンピュータ）上のソフトなどで作成されたコードデータで構成されたもの。

電子化文書：紙文書又はマイクロフィルム文書を電子画像（ビットマップ）化した文書。

なお、電子文書と電子化文書との両文書を総称する用語として、「電磁的記録に記録することができる情報[2]」を用いる。

（2）本ガイドラインの対象範囲の定義
本ガイドラインで対象とする範囲を次のとおり定める。

・真実性の確保を目的とする
- TBF が普及を目指す時刻認証サービス（タイムスタンプサービス）、あるいはそれを実現する技術は、電子保存容認の要件として挙げられている真実性の確保[3]に深く関係する。一方で、可視性の確保と TBF が対象とするサービスや技術はほとんど接点がない。従って本ガイドラインでは、真実性の確保を目的とした事項を策定することとする。

・電子化文書を対象文書とする
- 電子文書は、作成から保存・廃棄にいたるライフサイクルや業務プロセス全体をとおして電子的な状態にある。タイムスタンプを付与するタイミングは保存への移行段階に限定されることはなく、また付与の目的も文書の内容と性格に大きく依存するものと考えられる。TBF では既に、電子入札と電子申請に関わる電子文書に対してタイムスタンプを適用するためのガイドラインを示しており[4]、その中では保存のみでなく、送受信及び存在の証明を目的としたタイムスタンプの付与を対象としている。電子文書に対してはこのような広範な検討が必要であるため、前述の既存のガイドラインに対し、更に文書の種別を広げていくという方向で整備することが適当であると考える。
- 電子化文書においては、必ず「スキャナによるイメージ化」という、紙あるいはマイクロフィルムといったアナログメディアからデジタルメディアへの変換点が存在する。アナログ－デジタル変換点をまたがる真実性確保のための要件は、対象文書の内容や性格に強く依存することのない、中心的かつ共通的、しかも電子化文書特有の課

[2] 電子署名及び認証業務に関する法律第二条にある『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をいう。）に記録することができる情報』に準じ、この用語を用いることとする。
[3]帳簿書類の保存等の在り方に関する研究会：「帳簿書類の保存等の在り方について」（平成 9 年 3 月 26 日）によると、『真実性を確保するためには、（1）電子データの改ざん可能性を減殺すること、（2）入力及び出力の正確性を確保するなどにより電子データの信頼性を高める措置を取ることが必要であり、具体的な方法として、データの訂正・加除の履歴の確保、コンピュータ処理過程の適正性の確保、データの入出力記録の保存等システム上の方策のほか、書換えのできない保存媒体にするといった保存媒体の制限等が考えられる。』としている。タイムスタンプ及び電子署名は、（1）を実現する具体的方法のひとつである。
[4] タイムビジネス推進協議会：「時刻認証基盤ガイドライン」（平成 16 年 5 月）

題として捉えることができる。従って、本ガイドラインでは電子化文書を対象文書として取り上げることとする。なおこのとき、電子化以前の紙あるいはマイクロフィルム文書の真実性は確保されていることを前提として整理する。

・タイムスタンプ適用のためのガイドラインとする

- 電子化後のデータ（一般の電子データ）の真実性確保にはタイムスタンプと電子署名が有効である。タイムスタンプと電子署名を組み合わせることにより、真実性確保の安全性をより高めることができる。本ガイドラインでは真実性確保のためのタイムスタンプの適用を中心にまとめるが、電子署名についてもタイムスタンプとの関係において必要な事項につき、言及することとする。

本ガイドラインの対象範囲（斜線部）を図１－１に示す。

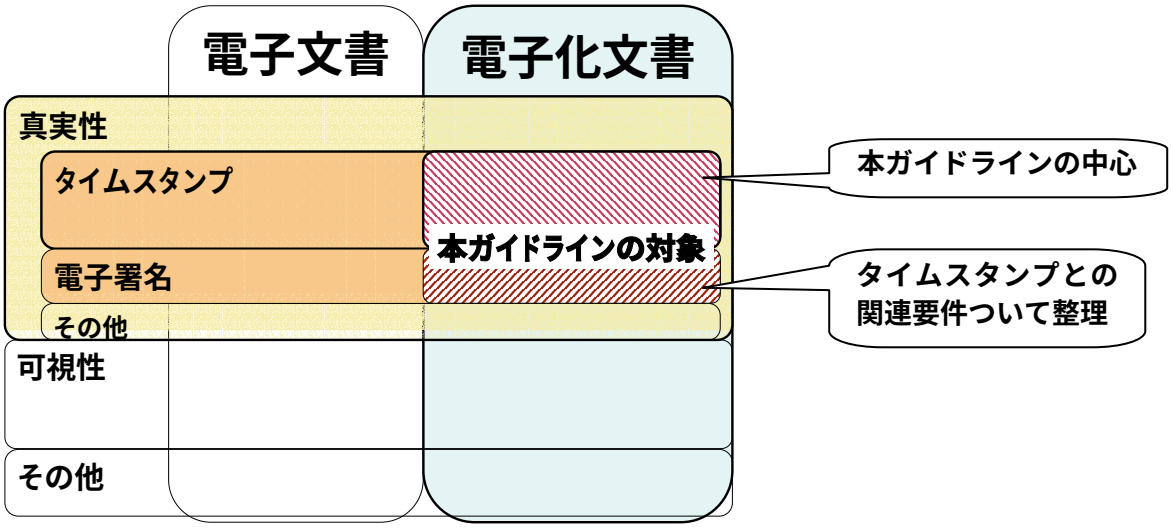

図１－１　本ガイドラインの対象範囲

２．e-文書の業務プロセスモデル

文書は、様々な目的のために作成・利用された後に保存され、最後には破棄されるものと破棄されない場合が存在する。e-文書法においては、従来の法律及び省令では紙のみでしか原本として保存の認められなかった文書を、「紙からスキャンして電子化文書とし、紙を破棄し電子化文書を保存する事」が容認される。既に電子文書が各法律及び省令で容認されている文書もあり「電磁的記録による保存をする場合は署名押印に代わる措置を執ること」と合わせた運用が想定される。また、e-文書法施行後においても文書によっては紙でのみ保存が義務づけられているものもある。

レコードマネージメントの分野においては、ISO15489（記録管理国際標準）で、企業の訴訟対策の説明責任（Accountability）が重要視されており、証拠性確保のために電子署名及びタイムスタンプが活用できる。

２．１　e-文書のカテゴリ

e-文書法における電磁的記録による保存等が認められる文書は３つのカテゴリに分類される

① 紙文書または電子文書で保存を容認する規定が既にある文書
② 紙文書でのみ保存が義務付けられていて、通則法の適用すべき規定がある文書
③ 整備法により何らかの規定が摘要される文書

①は紙または電子文書のどちらかを選択して原本とすることができる。電子文書は電磁的記録による保存となる。②及び③は紙を電子化文書にする場合が２通りあり、通則法だけが適用されるか、整備法によって適用されるかの違いがある。現行法においては、保存すべきものは、財産目録、貸借対照表及び損益計算書又は収支計算書並びに営業報告書又は事業報告書を含む「財務諸表等」などがあり、作成してから７年間事業所に備えて置くことを義務付けている。その他には書面、帳簿、記録（検査など）、図面は紙による保存のみ義務としている。e-文書法においては法令・省令で保存容認のための要件が示される予定なので参照し内容を確認する必要がある。文書の種類としては、各種帳簿類、議事録、注文書、見積書、契約申込書、報告書、名簿、個人情報、各種記録文書、領収書などがある。なお、e-文書法においては電子化にそぐわない「免許証」、「～士証」、「許可証」、「手帳」、「登録証」などは対象からは除外される。

２．２　電子化文書のライフサイクル

紙文書の電子化におけるライフサイクルは、作成（署名・押印）－利用－電子化（電子署名・タイムスタンプ）－利用（閲覧・検証）－保存（保存義務年限）－破棄（保存義務年限を越えた時）となる。

保存義務期間は、１年以上から数十年のものと永久保存のものがある。

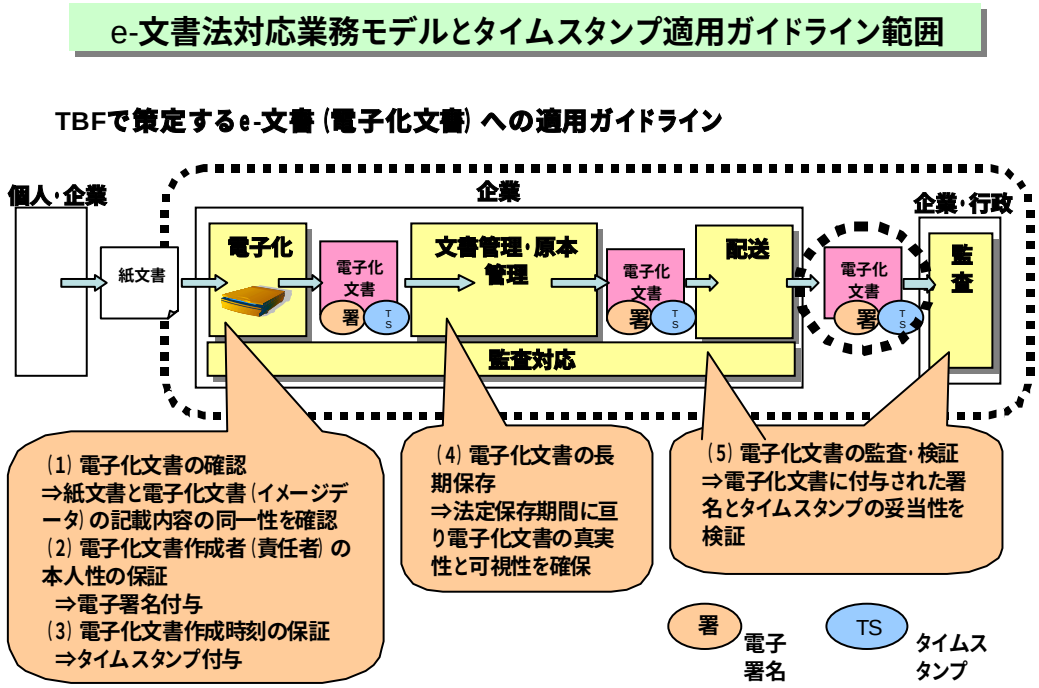

図２－１　e-文書法対応業務モデルとタイムスタンプ適用ガイドライン範囲

以下には現行法における文書の保存義務期間を参考例として記載する。各電子化文書の保存義務期間は主務省令等において確認する必要がある。

表 2-1　各法令による最低保存期間の例

文書の種類例	保存期間
公的許認可	３０年
商業帳簿	１０年
ＰＬ法関連	１０年
契約書の控え	７年

２．３　紙文書の電子化文書生成の業務プロセス

紙文書を電子化するプロセスとしては、運用の指針となる JIS Z 6016:2003 「紙文書及びマイクロフィルム文書の電子化プロセス」があり、以下に一例を記述する。

２．３．１　紙文書をスキャニングして電子化するプロセス

現行法において、一部の紙文書は紙のまま保存する義務がある。一方、e-文書法では、それらの文書もいくつかの例外を除いて、一旦作成された紙文書に関して電子化して保存することが容認される。電子化文書への電子署名及びタイムスタンプの要件は各法律及び省

令で定められる模様である。[*1] 以下に紙文書から電子化文書に変換する業務プロセスにおける電子署名及びタイムスタンプの技術を活用したモデルを紹介する。

① 準備
ページ数及び順番、紙折れ、しわ・汚れその他の付着物がない事などの確認、クリップ／ステープルの除去などを準備作業として実施する。

② スキャナでスキャニング
スキャナでスキャニングし、紙文書を電子化文書に変換する。

③ 電子化文書の品質と紙原本との同一性の確認
スキャニングする紙文書上の文字が確実に読めることを確認する必要がある。ページの欠損などが無いこと、修正などの痕跡が判別できるように変換されたことを確認する。

④ 電子化作業者の電子署名
紙と電子化文書の内容を比較して確認したことを担保するために電子署名を付与する。電子化責任者が電子署名する場合も有り得る。電子化作業者の電子署名は内容の真実性を保証するものでなく、紙文書と電子化文書をつき合せて間違いなく変換された事やページなどが揃っていること等の品質を保証するために電子署名を付与するものである。

⑤ 電子化責任者による確認
電子化責任者は電子化文書の品質、ページ枚数・順番などが適正であることを確認する。

⑥ 電子化責任者の承認
承認の手段として電子署名を用いることができる。電子化文書の内容に間違いが無い事を担保するために電子署名の付与などにより承認する。また作業担当者の電子署名が無く、電子化責任者のみが電子署名する場合もあり得る。

⑦ タイムスタンプの付与
第 5 章及び「信頼されるタイムスタンプ技術・運用基準」で定めるタイムスタンプを付与すると良い。タイムスタンプ付与直後にタイムスタンプトークンに含まれる時刻と利用者の時刻に大幅な差がないことを必要に応じて検証すると良い。

⑧ 保存及び管理
タイムスタンプを付与した電子署名付き電子化文書は、安全なメディアまたは安全なストレージなどに保存する。タイムスタンプに期限があるなどの場合、必要とされる保存期間は有効性延長用タイムスタンプを取得し、管理する。

[*1] 保存を義務付ける個別の法令ごとに、スキャン文書とする場合の改ざん防止や原本の正確な再現性の要請の程度が異なりうるので、電子的な保存の対象、方法等については主務省令で具体的に定める。（出典：平成 16 年 9 月内閣官房ＩＴ担当室発表の「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律案（骨子）について」）

⑨ 紙文書の廃棄
電子化された元の紙文書を廃棄する場合は、法令／省令などを確認の上で基準に沿って廃棄する。

２．４　電子化文書のレコードマネージメントの運用システム

具体的な記録管理を行う上で考慮すべきことは、主務省令において規定されるカラーでのスキャニング品質と内容の確認後に付与する電子署名及びタイムスタンプ、上書きしないバージョン管理の手法、紙と同等な可視性の確保、第三者検証、保存義務年限を網羅することある。電子化における運用システムについては、JIS Z 6016:2003 の「手作業での変換方式」、「自動変換方式」が参考になる。保存に関しては記録管理国際標準の ISO15489 レコードマネージメントが参考になる。この２つの規格は運用を主体とした証明力を高める方法であるが、真実性を確保するための手段としては電子署名及び信頼されるタイムスタンプを利用することができる。

３．電子署名及びタイムスタンプの必要性

３．１　文書の電子化における問題点

文書の電子化により、業務の効率化、サービス内容の向上、管理コストの削減などの実現が期待される。一方、問題点としては、改変が行われた際の痕跡検出困難や情報漏洩、保存時の読み出し不能等がある。したがって、紙文書の電子化にあたっては、その電子化情報が、紙文書と同一であることが必須条件とされている。このためには「完全性」、「機密性」および「見読性」の３要件が充足されなければならない。

「完全性」とは、改ざん等を未然に防ぐとともに、かつ改ざん等の事実の有無が検証できる状態で保存されることであり、「機密性」とは、許可されたもの以外からのアクセスを制限することにより盗難、漏洩等を防止するように保存管理されることであり、「見読性」とは、文書の内容が必要に応じて直ちに表示できることである。ここで、「見読性」については、ハードウェア、ソフトウェアや保存媒体などさまざまな要因が関係した要件であり、本書では、言及しない。

「完全性」「機密性」を含む要件として、「真実性の確保」が提示されることがある[5]。真実性の確保とは、（１）電子データの改ざん可能性を減殺すること、（２）入力及び出力の正確性を確保するなどにより電子データの信頼性を高める措置を取ることであると報告されている。具体的な方法として、データの訂正・加除の履歴の確保、コンピュータ処理過程の適正性の確保、データの入出力記録の保存等システム上の方策のほか、書換えのできない保存媒体にするといった保存媒体の制限等が考えられる。

電子署名とタイムスタンプは、これらの要件のうち、真実性の確保（または「完全性」と「機密性」）を確保する手段として利用される。なお、電子署名とタイムスタンプは、電子文書においても電子化文書と同様の効果があることから、本章では区別した記述をしていない。

３．２　電子署名とタイムスタンプの効果

３．２．１　電子署名の効果

電子署名とは、電子文書の本人性と内容の真正性を保証するものである。2001 年 4 月施行の「電子認証及び認証業務に関する法律」（いわゆる電子署名法）で電子署名が付与された電子文書について、真正な成立の推定が働くことが制定された。これにより、一定の要件を満たす電子署名を付与した電子文書（法律上は電磁的記録）は、後日の係争において、本人が作成し、内容が妥当性を持ち、改ざんされていないということを主張できる。電子化文書は、紙文書から電子化された時点で、電磁的記録となり、一定の要件を満たす電子署名が付与されると推定効が働くこととなる。電子署名を付与する技術として多く用いられているのは公開鍵暗号基盤（以降 PKI[6]：Public Key Infrastructure という）を用いる方式である。PKI では、認証局が利用者の公開鍵に対して、保持者である保証を与えるための署名をした公開鍵証明書を発行する。

---

[5] 平成 9 年 3 月 26 日 「帳簿書類の保存等の在り方について」帳簿書類の保存等の在り方に関する研究会

[6] PKI については、平成 15 年 3 月、当協議会発行の「時刻認証基盤ガイドライン」に技術説明をしているから参照されたい。

電子署名は、電子文書に対して、利用者が自身の秘密鍵を使用して付与するが、この電子署名の正当性を検証するには、認証局が発行した公開鍵証明書を利用する。すなわち、信頼ある認証局より発行された公開鍵証明書に含まれる公開鍵で検証が可能な電子署名は、公開鍵証明書に記載された利用者が作成したものであり、電子文書は改ざんされていないことを表す。しかし、これは電子署名を付与した時刻を保証してはいないため正当な時刻を保証するには、なんらかの別の手段が必要となる。

また、公開鍵証明書には、その有効期限が規定されている。一般に、有効期限後は鍵の安全を保証する役割が定義されていないため、公開鍵証明書の有効期限後に電子署名の有効性の検証を保証することはできない。このため、電子化文書時に署名の有効性が確認できた時点における有効な時刻と、署名検証のための証拠情報が必要となる。

３．２．２　タイムスタンプの効果

タイムスタンプとは、「特定の電子情報と時刻情報を結合することにより、その時刻より前にそのデータが存在したことの証明（存在証明）とその時刻から検証した時刻までの間にその電子情報が変更・改ざんされていないことを証明（非改ざん証明）することができる手段およびその証拠に結びつく情報」である[7]。このタイムスタンプを電子文書に付与することで、以下の効果が期待できる。

（１）文書存在証明
　　電子文書がある時点で存在したことを証明できること。
（２）電子署名文書の長期保存証明
　　電子署名文書の長期間経過後も真正性を保証すること。（3.3 で後述）

３．２．３　タイムスタンプと電子署名の組み合わせの効果

電子署名とタイムスタンプを組み合わせることにより、電子文書の本人性と内容の真正性を保持し、かつ電子文書の存在証明とさらには、長期保存を可能とすることができる。

３．３　電子文書の長期保存

電子文書を長期保存するためには、その電子文書が原本であることを示すため「真実性」（または、「完全性」「機密性」）を証明することが必要となる。PKI を使用する電子署名技術では、公開鍵証明書に含まれる有効期限を越えた電子署名の有効性を保証する必要があり、このためには、以下の要件が求められる[8]。

要件 1　電子署名時の時刻が正しい
要件 2　電子署名時の署名検証情報が正しい
要件 3　信頼されるタイムスタンプサービスが存在する
要件 4　安全な媒体に保存する。

このうち、要件４については、本書の対象外であるが、要件１～３について、電子署名とタイムスタンプを使用することによって実現することが可能である。すなわち、タイムスタンプにより、電子署名時の時刻を保証し（要件１）、電子署名時の署名検証情報を取得し、これにタイムスタンプを付与することで、これら署名検証情報を後日検証可能とする証拠情報（要件２）とする。当然、利用するタイムスタンプは、信頼あるタイムスタンプ局か

[7] タイムビジネス推進協議会 2004「時刻認証基盤ガイドライン」
[8] 2001.3　ECOM　「電子署名文書の長期保存に関する中間報告」

ら発行されるものでなければならない（要件３）。
図３－１に電子文書を長期保存するための要件を示した。

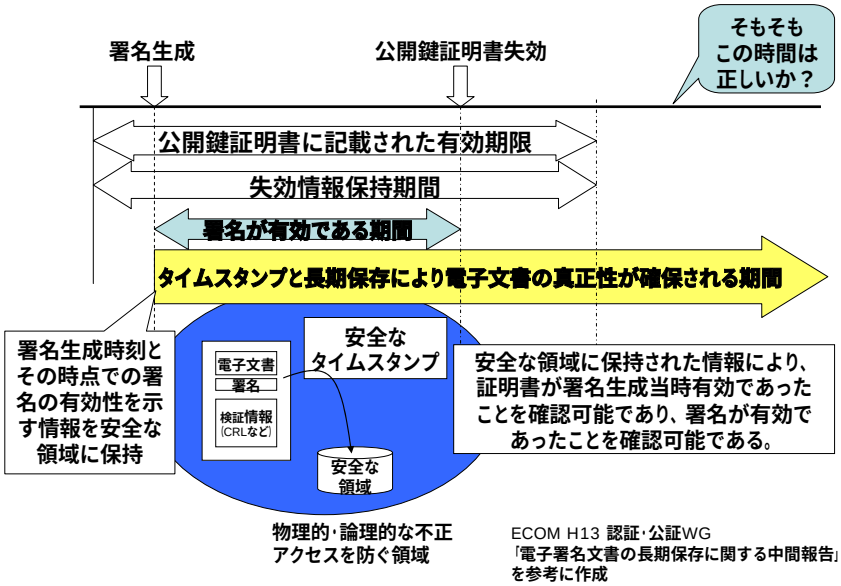

図３-１　電磁的記録の長期保存に対する要件

４．電子化文書の真実性確保のために用いるタイムスタンプ適用ガイドライン

紙文書を電子化文書として保存する場合、電子化文書は、紙文書と同等の真実性と可視性を備えている必要がある。前章で述べられたように、電子化文書の真実性確保の手段として、電子署名及びタイムスタンプが有効である。本章では、電子化文書の真実性確保のためにタイムスタンプサービスを利用するユーザ向けタイムスタンプ適用ガイドラインを記述する。

４．１　電子署名の付与対象とタイミング

紙文書と電子化文書の記載内容の同一性、及び電子化文書の妥当性を保証し、後日に、その保証者を特定できるようにするために、電子署名が使用できる。なお、ここで言う、同一性の確認と妥当性の確認とは、2.3.1「紙文書をスキャニングして電子化するプロセス」で定義される。

（１）同一性の確認

スキャニングする紙文書上の文字が確実に読めることを確認する。ページの欠損などが無いこと、修正などの痕跡が判別できるように変換されたことを確認する。

（２）妥当性の確認

電子化文書の品質、ページ枚数・順番などが適正であることを確認する。

４．１．１　基本的な考え方

電子化作業者及び電子化責任者の二種類の電子署名を使用することができる。

表４－１：電子署名者の役割と署名タイミング

電子署名者の役割	電子化作業者	電子化責任者
電子署名対象	紙文書の電子化文書	電子化作業者の電子署名など
電子署名タイミング	電子化作業者が、紙文書と電子化文書の同一性を確認した後、速やかに電子署名を付与する	電子化責任者が、電子化作業者が作成した電子化文書の妥当性を確認した後、速やかに電子署名を付与する

４．１．２　実務的な運用

（１）電子署名対象の電子データ種類

電子化作業者は、紙文書の電子化文書に加えて電子化文書作成時に生成される電子化文書の管理情報も電子署名対象としてもよい。管理情報とは、電子化文書を説明する情報である。検索のためのインデックス情報やビジネス処理用の OCR 結果情報などが例である。

なお、スキャン作業後の同一性の確認や再スキャン等の作業プロセスは、標準的な規格に基づいて行うことができる。例えば、JIS Z6016:2003 がある。

電子化責任者は、電子化作業者の電子署名が付与された電子化文書を電子署名対象としてもよいし、電子化文書のみにしてもよい。また、電子化文書の管理情報も

電子署名対象としてもよい。

表４－２：電子署名の対象と適用ガイド

署名者	電子署名対象	適用ガイド
電子化作業者	電子化文書	電子化文書だけの真正性を保証する時に選択
	電子化文書と管理情報	管理情報も含めて真正性を保証したい時に選択
電子化責任者	電子化文書	電子化文書だけの真正性を保証する時に選択
	電子化文書と管理情報	管理情報も含めて真正性を保証したい時に選択
	電子化作業者の電子署名	署名の順番を後日証明することが必要な場合に選択。署名による真正性保証範囲の考え方に応じて署名対象を選択する
	電子化作業者の電子署名が付与された電子化文書	
	電子化作業者の電子署名が付与された電子化文書と管理情報	

（２）電子署名対象の単位

電子化文書が複数のページを含むとき、ページ毎に署名を行ってもよいし、文書全体に対して署名を行ってもよい。ただし、文書全体に署名した場合、電子署名検証時に改ざんが検出されると、この電子署名に係わる全てのページの信頼性が失われることに注意を要する。

業務上一つの単位として意味を持たせた複数の電子化文書、あるいは、電子化作業者の電子署名に対して、一つの電子署名を付与することも可能である。ただし、電子署名検証時に改ざんが検出された場合、この電子署名に係わる全ての電子化文書の信頼性が失われることに注意を要する。

４．２　タイムスタンプの付与対象とタイミング

４．２．１　文書存在証明

（１）基本的な考え方

電子署名よりも先に、スキャニング直後の電子化文書に対してタイムスタンプを付与し、電子化文書の存在時刻や完全性を保証する考え方がある。しかしながら、この考え方では、紙文書との同一性の保証のない電子化文書に対するタイムスタンプとなる恐れがある。

現状は、紙文書と同等な真実性を確保した電子化文書を生成するスキャナ装置仕様やその設定・操作仕様が定義されていない。そのため、e-文書法では、電子化文書の真実性確保のために、電子化作業者による電子化文書と紙文書の同一性の確認作業及び電子署名付与が求められることになる見込みである。よって、タイムスタンプ付与対象は、スキャニング直後の電子化文書ではなく、電子化作業者の電子署名、あるいは、電子化作業者の電子署名が付与された電子化文書とすべきである。そのため、電子署名の後にタイムスタンプが付与される（図４－１参照）。

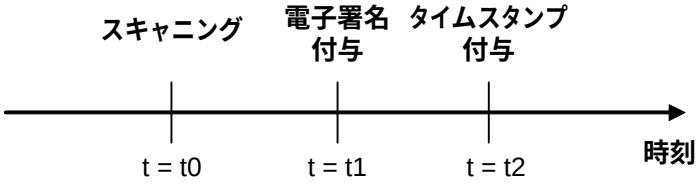

図４－１：電子署名とタイムスタンプの付与タイミング

表４－３：タイムスタンプ付与対象と付与タイミング

タイムスタンプの付与対象	電子署名、あるいは、電子署名が付与された電子化文書
タイムスタンプの付与タイミング	電子化作業者と電子化責任者の署名が付与された後、速やかにタイムスタンプを付与する

（２）実務的な運用

（ａ）タイムスタンプ付与対象の電子データ種類

タイムスタンプ付与対象となる電子データには制限はない。そのため、e-文書法において、タイムスタンプ付与対象として、電子署名に加えて電子署名付与対象となる電子化文書もタイムスタンプ付与対象としてもよい。

表４－４：タイムスタンプの付与対象と適用ガイド

タイムスタンプの付与対象	適用ガイド
電子署名	電子署名の存在時刻と非改ざん性を保証したい時に選択。タイムスタンプの検証により、電子署名の存在時刻と電子署名の非改ざん性が確認されると、次に、この署名を検証することにより、間接的に電子化文書の真正性と存在時刻を証明することが可能。 タイムスタンプ付与時に電子化文書の取得・ハッシュ化処理が不要なため、比較的処理が軽い。
電子署名が付与された電子化文書	電子署名と電子化文書から構成されたデータの存在時刻と非改ざん性を保証したい場合に選択。電子署名が付与された電子化文書の存在時刻と非改ざん性をタイムスタンプにより直接的に判断することが可能[9]。

（ｂ）タイムスタンプ付与対象の単位

[9] 正確には、タイムスタンプ検証により、「電子化文書」と「電子署名」から構成された電子データの改ざん有無が分かる。改ざんのパターンとして、次の 3 パターンがあるが、タイムスタンプ検証の結果からこれらを区別できないことに注意を要する。 (1)電子化文書のみ改ざん、(2)電子署名のみ改ざん、(3) 電子化文書と電子署名の両者が改ざん。

タイムスタンプ付与対象として、業務上一つの単位として意味を持たせた複数の電子化文書、あるいは、電子署名に対して、一つのタイムスタンプを付与することも可能である。ただし、タイムスタンプ検証時に改ざんが検出された場合、このタイムスタンプに係わる全ての電子化文書、あるいは、電子署名の信頼性が失われることに注意を要する。

４．２．２　長期保存証明

電子化文書の保存期間を満たす前に、電子化文書に付与されたタイムスタンプの有効期間が終了してしまうことがあり得る。この場合、タイムスタンプ利用者は、当該電子化文書の存在証明を延長するために、一つの方法として、現在のタイムスタンプの有効期間が満了する前に、新規のタイムスタンプを付与してもらう必要がある。

（1）基本的な考え方

電子化文書､電子化文書に付与された電子署名やタイムスタンプが有効であったことを後日に証明できるようにするためには､新規にタイムスタンプを付与する直前に､電子化文書に付与された電子署名とタイムスタンプに関し､新規にタイムスタンプの付与を求める者がそれぞれの有効性をこの時点で検証し､それに係る情報全てを新規のタイムスタンプの付与の対象とすることが必要である。

表４－５：タイムスタンプ付与対象と付与タイミング

タイムスタンプの付与対象	電子化文書、電子署名、タイムスタンプ、電子署名とタイムスタンプに係る公開鍵証明書パス情報[10]と公開鍵証明書失効情報（個々のデータにタイムスタンプを付与してもよいし、これらを一纏めにしたデータに対して付与してもよい）
タイムスタンプの付与タイミング	電子化文書に付与された電子署名とタイムスタンプの有効性が失われる可能性があると判断された後、電子署名の検証情報（電子署名に係る公開鍵証明書パス情報と公開鍵証明書失効情報）とタイムスタンプが有効なうちに速やかに新規のタイムスタンプを付与する 二回目以降の延長に関しては、直前に付与したタイムスタンプが有効なうちに速やかに新規のタイムスタンプを付与する。

（2）実務的な運用

ECOM ガイドライン[11]では、電子署名付き文書を長期間保存するためのモデルを次図のように定義している。

① 即ち、署名生成後、証明書の有効期限内かつ失効前に署名の存在時刻を確定する
② 検証に必要な情報（公開鍵証明書パス情報や公開鍵証明書失効情報）を収集する
③ 検証に必要な情報を改竄検出可能な状態にする

[10]タイムスタンプ局の公開鍵証明書からトラストアンカとなる認証局までの一連の公開鍵証明書群
[11] 電子商取引推進協議会 認証・公証 WG：電子署名文書長期保存に関するガイドライン（平成 14 年 3 月）

④　電子署名付き文書と上記の検証に必要な情報を保存する
⑤　長期間経過後の再検証において、元の署名の存在時刻を確認する
⑥　その時刻における検証のための証拠情報に基づき署名の有効性を確認する
⑦　更に証拠情報の完全性が確認できることにより、元の署名が確かに有効であったことが確認できる

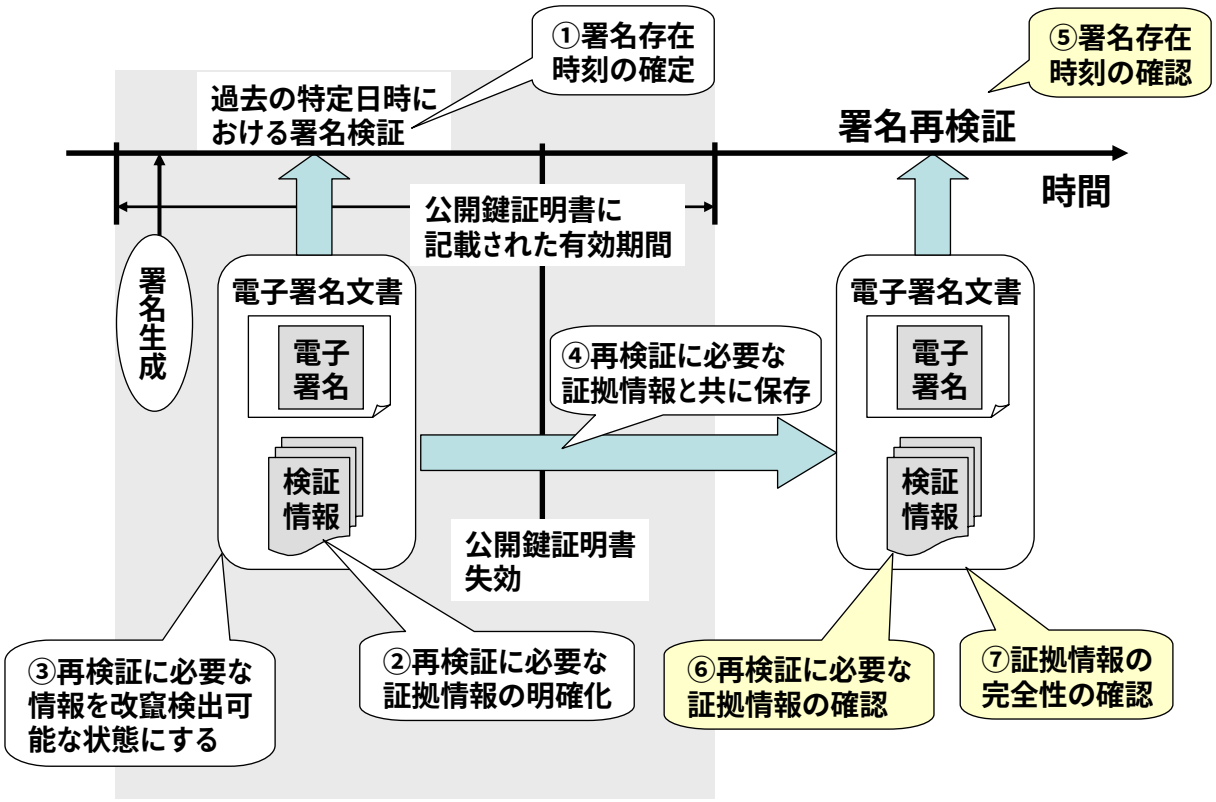

図４－２　電子署名文書長期保存モデル

このモデルに適合する現状考えられる対策案を以下に示す。利用者は、各自の判断に基づいて、これらの対策案から適当な方法を採用するものとする。

（1）対策案1

ETSI[12] TS 101 733、W3C[13] XAdES、ETSI TS 101 733（RFC 3126）、ECOM ガイドライン、などに記載されている長期署名フォーマットに基づく対策である。適切なタイミングで、電子化文書の電子署名の検証情報とタイムスタンプの有効性を確認し、その直後に、新たなタイムスタンプを付与することにより、電子化文書の署名や

12　欧州電気通信標準化機構を示す。ヨーロッパにおける電気通信の共通仕様を策定している。ETSI とは、European Telecommunications Standards Institute の略である。

13　WWW で利用される技術の標準化をすすめる団体である。W3C とは、World Wide Web Consortium の略である。

タイムスタンプの有効期間を延長させる。

（2）対策案2

電子化文書の署名やタイムスタンプが有効なうちに、検証を実行し、検証結果と共に安全な保存方法をとる。また、有効なうちに保存したことを示すために、ストレージ登録日時を後日証明できるようにすることも必要である。

安全な保存方法の実現方式としては、厳密なアクセス制御を実行し、アクセスログは改ざん検出コードを付与して保管され、保存データ個々に保存時に与えられた所定保存年限内での削除を禁止する処置が講じられる、などの機能を実装する。

４．３　電子署名とタイムスタンプ付与例

前節を踏まえ、電子署名及びタイムスタンプ付与対象の具体例を示す。

例１）
電子化文書：申込書と添付書類から構成される
電子化作業者の署名対象：電子化文書全体
電子化責任者の署名対象：電子化作業者の電子署名
タイムスタンプ付与対象：電子化責任者の電子署名

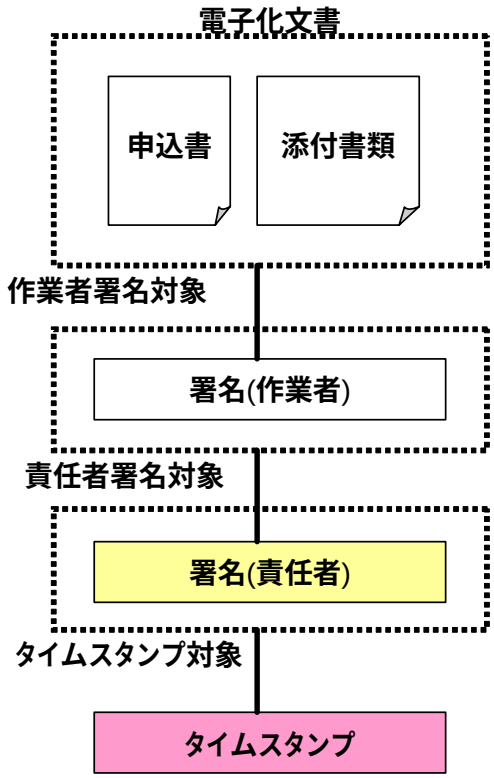

図４－３：電子化責任者の電子署名に対してタイムスタンプ付与

例２）
電子化文書：申込書と添付書類から構成される
電子化作業者の署名対象：電子化文書全体
電子化責任者の署名対象：電子化作業者の電子署名
タイムスタンプ付与対象：電子化作業者及び電子化責任者の電子署名が付与された電子化文書

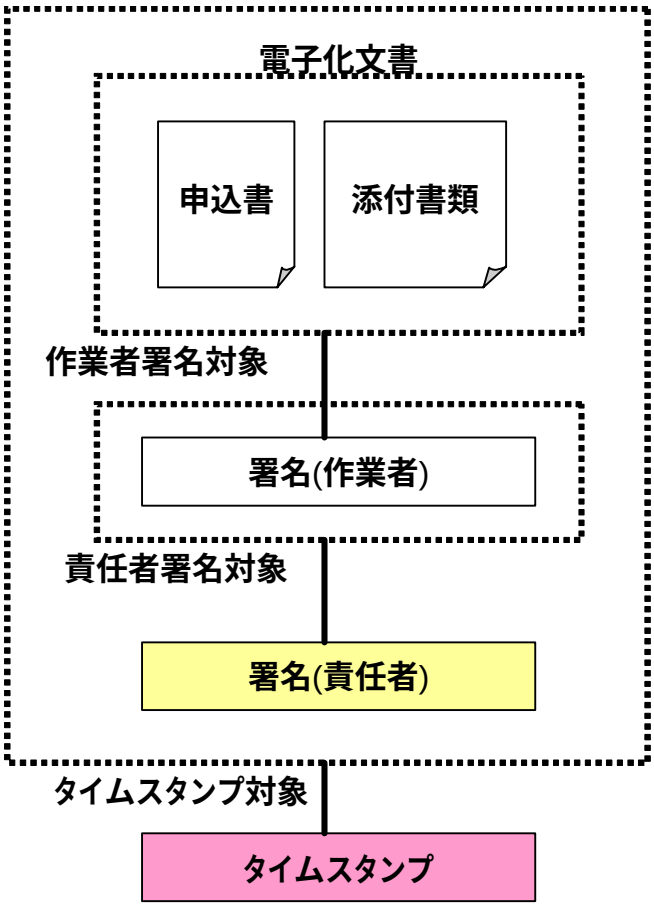

図４－４：電子署名が付与された電子化文書に対してタイムスタンプ付与

４．４　電子署名及びタイムスタンプの格納方式とフォーマット

（１）標準規格

現状の主な標準規格（デファクト標準、デジュール標準、コンソーシアム標準など）を以下にまとめる。なお、技術進歩により格納方式やフォーマットは変更・追加がありうることに注意を要する。

表４－６：電子署名とタイムスタンプの標準規格

項目	標準規格	説明
電子署名	RFC 2315	PKCS#7 フォーマット
	RFC 3852	CMS SignedData フォーマット
	ETSI TS 101 733 V1.5.1	ASN.1 ベースの長期署名フォーマット
	RFC 3126	ETSI TS101 733 V.1.2.2 に基づく長期署名フォーマット
	W3C XML Signature	XML 署名フォーマット
	RFC – 3275	XML 署名フォーマット（W3C と同等）
	ETSI TS 101 903 V1.2.2	XML ベースの長期署名フォーマット
	W3C XAdES	ETSI TS 101 903 に基づく長期署名フォーマット
タイムスタンプ	RFC 3161	PKI 技術を使用した独立トークン型タイムスタンプ規格
	ISO/IEC 18014-1:2002	タイムスタンプサービスのフレームワーク
	ISO/IEC 18014-2:2002	独立トークン型タイムスタンプ規格
	ISO/IEC 18014-3:2004	リンクトークン型タイムスタンプ規格
	JIS X 5062:2003	ISO/IEC 18014-1:2002 に基づく国内規格

署名属性に、署名ポリシー(RFC 3125)、コミットメントタイプ(RFC 3126)、などが含まれると署名の目的や意味がより正確になる。

（2）データ格納形式例

例１）

電子署名として、RFC 3369（CMS SignedData）、タイムスタンプとして RFC 3161 を採用した場合のデータ格納形式を以下に示す。

表４－７：データ格納形式

データ格納形式（仮名称）	説明
個別管理方式	電子化文書データ、電子署名データ、タイムスタンプデータをそれぞれ個別に管理する。例えば、電子化文書ファイル、電子署名データファイル、タイムスタンプデータファイルとして管理する。 個別のファイルの関連性に関しては別途対策を講じる必要がある。例えば、これらのファイルを一つのアーカイブファイル(e.g. LZH アーカイブファイル)にする方法として管理するなど。
署名・タイムスタンプ一体型管理方式	電子署名とタイムスタンプを一体として管理する。 電子化責任者の署名データは、電子化作業者の署名データの Countersignature として格納される。電子化責任者の電子署名に対するタイムスタンプは、電子化責任者の電子署名の非署名属性へ格納する。 電子化文書データと署名・タイムスタンプとの関連性に関しては別途対策を講じる必要がある。例えば、これらのファイルを一つのアーカイブファイル(e.g. LZH アーカイブファイル)にする方法として管理するなど。
電子化文書・署名・タイム	電子化文書データ、電子署名データ、タイムスタンプデータを一体のデータとして管理する。上記の署名・タイムスタンプ一体型管理方式に加え

スタンプ一体型管理方式	て、電子署名のコンテンツフィールドへ電子化文書データを含める。

例２）
電子署名として ETSI TS 101 733 や RFC 3126 を採用すると、電子化文書、電子署名、タイムスタンプを一体のデータとして管理することができる。

例３）
電子署名として ETSI TS 101 903 や XAdES を採用すると、電子化文書、電子署名、タイムスタンプを一体のデータとして管理することができる。

例４）
電子化文書、電子署名、電子署名やタイムスタンプに係る公開鍵証明書を一組にしたデータに対してタイムスタンプを付与する。また、電子署名やタイムスタンプに係る公開鍵証明書パス情報と公開鍵証明書パス上の公開鍵証明書失効情報にも失効情報の発行のタイミングでタイムスタンプを付与し、これらの情報を安全に保管する。

４．５　タイムスタンプ検証

４．５．１　タイムスタンプ検証タイミング

タイムスタンプは検証によってタイムスタンプの有する機能を確認することができる。タイムスタンプの検証により、タイムスタンプ付与対象の電子データの存在時刻とそれ以降の改ざん有無を確認することができる。表４－８にタイムスタンプ検証対象とタイミングの例を示す。

また、タイムスタンプ検証の応用として、電子化のタイミングを確認することもできる。例えば、タイムスタンプ検証後、タイムスタンプに含まれる時刻情報と電子化文書上の日付を比較することにより、紙文書の作成時から電子化までの時間を見積もることができる。

表４－８：タイムスタンプ検証対象とタイミング

検証対象	タイムスタンプとタイムスタンプ付与対象電子データ
検証のタイミング	（１）　タイムスタンプ付与直後 （２）　タイムスタンプが付与された電子化文書を他システム、他組織、外部機関へ送信前 （３）　タイムスタンプが付与された電子化文書を他システム、他組織、外部機関から受信後 （４）　監査時 ・　電子署名文書の存在証明や非改ざん証明が必要になった時 ・　長期保存証明が必要になった時 （５）　長期保存を行う時 ・タイムスタンプの有効期間を延長する時

４．５．２　タイムスタンプ検証例

タイムスタンプ検証の具体例を以下に示す。

例１）
タイムスタンプ付与対象：電子署名

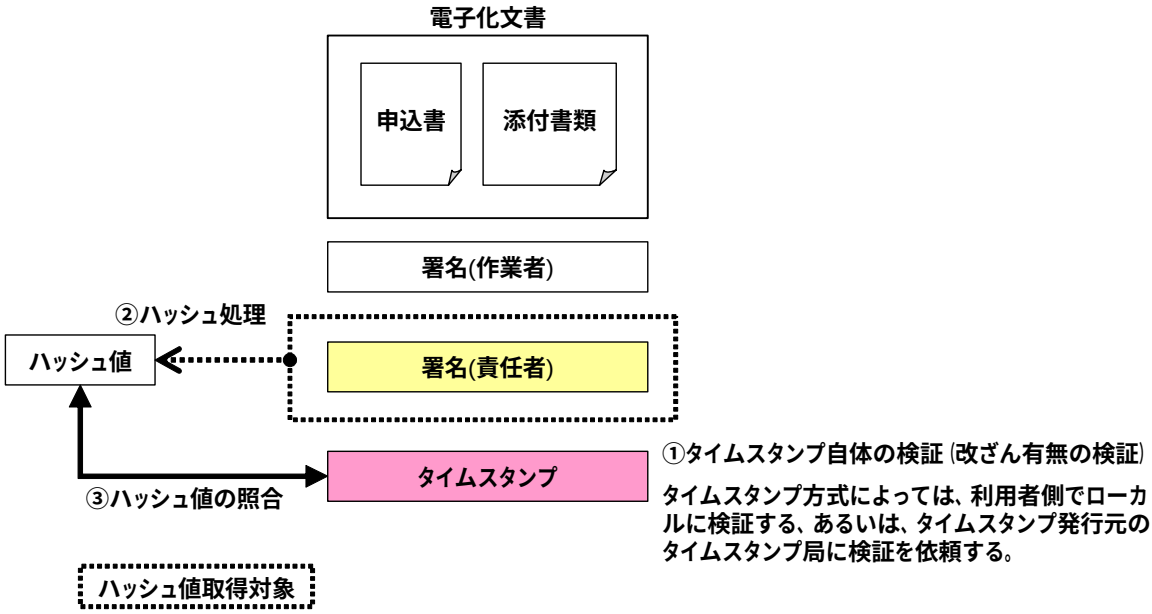

図４－５：電子署名に付与されたタイムスタンプ検証

①タイムスタンプ自体の検証
　タイムスタンプ自体の改ざん有無を検証する。タイムスタンプ方式によってタイムスタンプ自体の検証方法は異なる。例えば、デジタル署名技術を使用する方式のタイムスタンプの場合、利用者側でローカルに検証（署名の検証と公開鍵証明書の検証）することができる。また、デジタル署名技術を使用しない方式のタイムスタンプの場合、タイムスタンプ発行元のタイムスタンプ局に検証を依頼する。

②ハッシュ処理
　タイムスタンプで使用されたハッシュ関数を用いて、タイムスタンプ付与対象の電子署名データのハッシュ値を求める。

③ハッシュ値の照合
　②で求めたハッシュ値とタイムスタンプに含まれる該当ハッシュ値を比較する。

　これらの①から③の検証を行うことで、タイムスタンプ付与対象の電子署名データが、タイムスタンプに含まれる時刻において存在し、それ以降、改ざんされていないことを確認することができる。

例１）
タイムスタンプ付与対象：電子署名が付与された電子化文書

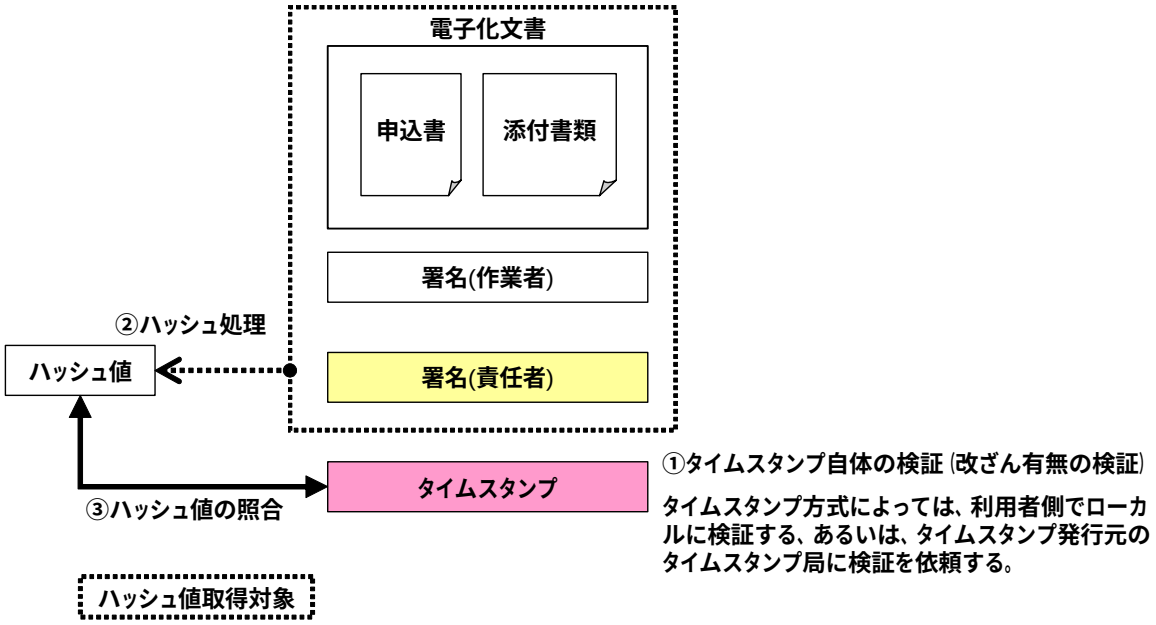

図４－６：電子署名を伴う電子化文書に付与されたタイムスタンプ検証

①タイムスタンプ自体の検証
　タイムスタンプ自体の改ざん有無を検証する。タイムスタンプ方式によってタイムスタンプ自体の検証方法は異なる。例えば、デジタル署名技術を使用する方式のタイムスタンプの場合、利用者側でローカルに検証（署名の検証と公開鍵証明書の検証）することができる。また、デジタル署名技術を使用しない方式のタイムスタンプの場合、タイムスタンプ発行元のタイムスタンプ局に検証を依頼する。

②ハッシュ処理
　タイムスタンプで使用されたハッシュ関数を用いて、タイムスタンプ付与対象の電子化文書と電子署名データのハッシュ値を求める。

③ハッシュ値の照合
　②で求めたハッシュ値とタイムスタンプに含まれる該当ハッシュ値を比較する。

　これらの①から③の検証を行うことで、タイムスタンプ付与対象の電子署名が付与された電子化文書が、タイムスタンプに含まれる時刻において存在し、それ以降、改ざんされていないことを確認することができる。

５．電子化文書の真実性確保のためのタイムスタンプサービス利用上の留意点

本章では、電子化文書の真実性を確保するためにタイムスタンプサービスを利用する場合に、その利用者が留意すべき事項について記述する。

タイムスタンプサービスが電子文書の存在時刻の証明や非改竄の証明に用いられることから、利用者は、タイムスタンプサービスの運用規定等を確認した上で、特に下記について、留意すべきと考えられる。

５．１　タイムスタンプの有効性について

５．１．１　タイムスタンプの有効期間

電子化文書の保存義務期間以上の有効期間を持つタイムスタンプであることを確認した上で使用すること。

もし利用しようとするタイムスタンプの有効期間が、保存義務期間以下の場合では、４．２．２に示したようにその有効期間が終了する前に再度、タイムスタンプを付与する等のタイムスタンプの有効期間延長処理が実現できること。

５．１．２　タイムスタンプ事業者の事業継続性

タイムスタンプ事業者が、タイムスタンプの有効期間内に事業から撤退する場合でも、既に付与したタイムスタンプの検証が可能となるように、検証に係る業務の継続性が保証されることを確認すること。例えば、事業を他の事業主体に引継ぎ可能であることを確認すること。

更にタイムスタンプサービスの事業者がその事業から撤退する場合に、その連絡が必ず利用者に通知されるとともに、通知されてからサービスが終了するまでの期間が利用者にとって業務上十分であることを認識すること。

５．１．３　暗号技術の脆弱性の判明

利用者は、タイムスタンプサービスに使用している暗号技術の脆弱性の判明や暗号アルゴリズムの危殆化に備えて、タイムスタンプサービス事業者や利用者が行うべき対応について理解した上で、タイムスタンプサービスを利用すること。

５．２　　タイムスタンプの時刻の精度等について

５．２．１　時刻の信頼性

タイムスタンプに用いられる時刻情報源と精度を確認すること。

５．２．２　タイムスタンプの要求時刻と付与される時刻の差

タイムスタンプサービスにおいては、回線やサーバの輻輳等の事由により、利用者がタイムスタンプの付与を要求した時刻と付与されたタイムスタンプで証明される時刻に差が生ずることを認識した上で、そのサービスを利用すること。

５．３　免責事項について

利用者はタイムスタンプサービスに関する免責事項、補償範囲を確認すること。

参加メンバー　ガイドライン分科会

（ｅ－文書適用ＷＧメンバー）

（順不同・敬称略）

主　査	株式会社エイベック	本田　雅裕
リーダー	三菱電機株式会社	宮崎　一哉
メンバー	アマノ株式会社	清井　洋平
〃	株式会社ＮＴＴデータ	神山　忠弘
〃	株式会社ＮＴＴデータ	坂本　弘章
〃	株式会社ＮＴＴデータアイテック	伊地知　理
〃	菅沼俊広税理士事務所	菅沼　俊広
〃	東京税理士会情報システム委員会	板倉　勝
〃	日本電気株式会社	小松　文子
〃	株式会社日立製作所	谷川　嘉伸
〃	株式会社 PFU	野口　隆弘
〃	富士通株式会社	小谷　誠剛
〃	三菱化学メディア株式会社	入沢　芳久
〃	横浜著作権研究会	臼杵　稔

【連絡先】

タイムビジネス推進協議会（ＴＢＦ）

〒160-0022
東京都新宿区新宿 1-20-2　小池ビル
財団法人テレコム先端技術研究支援センター
タイムビジネス推進協議会事務局
Tel.03-3351-8423
Fax.03-3351-6690
URL：http://www.scat.or.jp/time/