時刻認証基盤ガイドライン

平成１６年５月

タイムビジネス推進協議会

はじめに

本ガイドラインの第１版を公開して早や一年が経過した。物理的な時間は万人に等しく均等に流れている筈であるが、本協議会の関わる IT 業界では特別に早い時計(時刻)に基づいているが如く急速に変化している。この種のガイドラインは不易であることが必要であるが、環境の激変に対応して在り様を変えることもその一方で望まれている。

それに応えるべく、時刻認証基盤として時刻の大本に遡るのに必須の、標準時配信と時刻監査、および信頼の根拠をより強固にするための CA 局の運用に関するガイドラインを追加することとした。あわせて本ガイドラインの利用を考慮して構成を大幅に改定した。

現代社会ではいたるところに時計が組み込まれ、「時」がなくては社会が成り立たないと言っても過言ではない。情報化社会を支えるコンピュータも高精度の時計を内蔵し、全ての回路がそれと同期して動作している。コンピュータを用いて構築されている電子的環境・デジタルな世界の記録は全て、コンピュータの内蔵時計の時刻と関連しているわけである。第 1 版の公開以降、社会の情報化・デジタル化の一層の進展に伴い、電子的に付与した時刻の証拠能力を担保することや、協調して動作する複数のコンピュータの時計を同期させることの重要性が認識されるようになった。

この状況を元に情報社会の基盤として、デジタルな世界における「時」を適切に定めるだけでなく、具体的にどのように利用すべきか、安心して使えるための要件は何かを示すべく、タイムビジネス推進協議会の技術部会にあって、当ガイドライン分科会は利用者および提供者への指針作成を分担している。

第 1 版では拙速を旨として対象範囲を絞り、指針そのものを公にすることに重点をおいた。すなわち、主として政府・地方公共団体におけるタイムスタンプの利用に焦点を合わせて、利用側と提供側双方に対する一般的な指針を作成した。今回、タイムビジネスにとってタイムスタンプと同様に重要で標準時配信に関するガイドラインを作成することにした。いずれも実証的に評価して今後段階的に充実させていく予定であるが、それには実証の時間を要する。

次の段階では、利用対象の範囲を広げる方向と、システム評価プログラムあるいは認定プログラムの領域で、指針の意味するところを具体化し、評価シートにまで深めることが考えられる。

標準時配信および時刻監査、タイムスタンプの利用・適用および提供のガイドラインの整備を通じて、時刻関連の技術の適用および制度の改革を促進し、標準時配信や時刻認証などタイムビジネスを確立し、信頼できる電子社会基盤の整備に寄与することに資すれば幸いである。

2004 年 5 月

タイムビジネス推進協議会

目　　次

第Ⅰ編　解　　説

第１章　概　要

１．１　背景と目的

（１）「デジタルな時の痕跡」の必要性

日常の生活においては、商取引や各種申請から個人間の約束に至るまで、意識してあるいは無意識のうちに「時」の概念が付随している。そのため、物理化学的さらには社会的に様々な手段で「時の痕跡」を文書に残している。情報が記録されている媒体や記録手段、形態など、いわばアナログ的に「時の痕跡」が刻み込まれているわけである。

現在、情報通信技術の進展によって文書をデジタル化する動きが急である。e-Japan 構想に基づく行政の電子化はその典型的な例で、それは社会の諸活動がデジタル化された文書に基づいて運営されるようになることを意味する。しかし、紙を主体とした文書とは異なり、デジタル化されたデータ・文書は原本と複製の区別が本質的に不可能である。そのため、原本性確保や改ざん防止など、その扱いには検討すべき課題が多い。「時の痕跡」の真正性もその中の大きな課題の一つである。

社会の諸活動においてデジタルデータを電子的環境で完結させるということは、記録媒体に依存しない「デジタルな時の痕跡」を実現させなければならないことを意味する。すなわち、デジタルデータそのものに電子的に「時の痕跡」を残す必要がある。技術的には既に幾つかの方式が提案され、それに基づいたツールも実装されているし、一部ではサービスも始まっている。しかし、今までの長い歴史で培われてきた慣習・規則は、広くかつ深く社会生活に浸透しているので、電子的な「時の痕跡」が従来の方法と同様の立場を確保するには至っていない。

（２）時計が正確に運用されていることに対する第三者証明の必要性

インターネットの世界的な普及により、24 時間を通した世界各国間の商取引が増加しているのは言うまでもない。従来は、一般的には一日の境目は業務が稼動していない夜中の 12 時だったこともあり、時間の正確性というのはさほど重要視されていなかったと思われるが、日本国内で 10 時であっても取引先の地域では夜中の 12 時である事も珍しくない世の中となった。また、国内だけを考えた場合であっても、24 時間ノンストップのインターネットショップも増えてきた。そうなると、日単位、月単位に取引を締めようとした場合、互いの運用する時計の時刻がずれている事によるトラブルが発生する事は当然の結果と言える。

そこで、まずは運営しているシステムの時計を正確に保つ事が必要になるが、インターネット上に無料で公開されている NTP サーバや GPS、電波時計などを使ったタイムサーバ機器を利用すれば、それは決して難しい事ではない。ところが、本当に正しい時刻に保たれていたという事を、自分自身だけで第三者に証明する事は非常に困難であり、その証明を第三者に依存したいというニーズが発生するようになってきた。

また、近年になって出現したタイムスタンプ局や電子公証局、電子認証局などの使用する時刻の正確性と信頼性の確保に関しては前述と同等、もしくはそれ以上の重要性とニーズがある事は言うまでもない。

（3）ガイドライン策定の目的

電子的環境における「時」の概念が広く社会に受け入れられるには、技術の確立に加えて、社会的に認知され、人々から信頼され、実生活において日用されるようになる必要がある。「デジタルな時の痕跡」に信頼を与える仕組み全体は、「時」が現代社会の基礎を成しているということから、電子化・デジタル化された社会の基盤といえる。それを時刻認証基盤と総称すると、本ガイドラインを策定する目的は、その時刻認証基盤を社会に定着させることにある。

具体的には、将来に備えて保存される電子文書や電子データに対して付与する「デジタルな時の痕跡」としてのタイムスタンプとは何か、タイムスタンプの重要性、タイムスタンプ導入による効果などを解説し、利用者に対してはタイムスタンプ導入の指針を、提供者に対してはタイムスタンプ提供の指針を提示する。すなわち、タイムスタンプの利用者には、どの文書・データに、どの時点で、どのような痕跡を残したら良いか、業務へ適用の判断基準を示す一方、タイムスタンプサービス提供者には、どのようなタイムスタンプをどの程度の信頼性でどのように提供したら良いか、サービス品質の目安を示すことである。

一方、タイムスタンプに使用される時刻はもちろんの事、電子データに付与される時刻情報の元となった時計の信頼性に関して、第三者によるサポートと証明をする技術の紹介をする。また、タイムスタンプのガイドラインと並行して、サービスを利用する側と提供する側とに分けて指針にまとめている。

当面の目標としては、タイムスタンプ、標準時配信・監査の提供と導入のガイドライン制定を通じて、電子自治体や電子政府関連事業で時刻の重要性が認識され、時刻認証基盤がそれらシステムの基本仕様に取り入れられることを目指している。

１．２　検討の方針

本ガイドラインの検討に際しては、次の各点に留意した。

(a) 利用・適用を重視

時刻認証基盤の基礎となる協定世界時およびタイムスタンプの技術的な検討は、国内外の関連諸団体組織で精力的に進められている。しかし、他の多くの技術と同様、それをどのように利用するか、適用するかを示さなければ、活用されない恐れがある。ここでは技術そのものでなく、利用・適用の視点で、利用者および提供者双方に対して指針を提供する。特に、利用側が安心して採用できるよう、時刻の専門集団として、技術的に安全性が裏づけされた指針を提供する。

(b) 実用を重視

標準化の動きは、IETF および ISO/IEC で活発に進められている。電子文書に対するタイムスタンプ付与についても、電子文書交換の規約として重要な XML にタイムスタンプ付与の規定がある。しかしながら現状は、標準規定があっても実装が不十分であったり、特定の事業者に特化した仕様であったりして、実用にはまだ改善の余地が大きい。したがって、ここでは第一義的には国内外の技術標準に準拠するが、実装およびサービス提供の実情を勘案して、現実的な指針と

なるよう留意した。

(c) 中立の姿勢

本文で詳述するように、時刻を配信について手段に複数の方式があり、タイムスタンプには幾つかの方式が並存している。しかしながら、それぞれに特徴があり、現時点では方式を特定することが困難である。そのため、標準時配信は複数の方式を前提として時刻監査について述べ、タイムスタンプサービス利用者への指針では、タイムスタンプ利用の要件の明確化に注力し、特定の方式には依存せず、特定の方式を偏重しないようにした。サービスの提供側に対する指針も、適切なサービス提供の実現を目的とし、事業者が特定されるような内容としないよう配慮した。方式に言及する場合は該当する方式を複数併記し、それぞれ準拠すべき基準を明確にする。

(d) 汎用性・一般性を指向

技術は一般に汎用的なので、その適用対象・範囲を定め、内容を限定することによって、実用に供される。時刻認証基盤の各技術も同様で、本ガイドラインも適用対象・範囲の業務を限定している。しかしながら、個別具体的になるほど、その対象には直接的に役立つ指針となるが、少しでも異なる業務には役立たなくなる。一方、あまりに汎用的に一般化すると、技術の解説と変わらなくなる。本ガイドラインではそのどちらにも偏らないように心掛けて、適用範囲を設定した。

(e) 電子政府関連から着手

時刻認証基盤が有効と思われる分野は数多いが、今回はまず、e-Japan 構想に基づいて構築される電子申請と電子入札を対象にした。どちらもこれから本格的に構築されるので、タイムスタンプ適用を働きかけることが急務である。なお、両者は業務フローが異なるので、それぞれについて利用側の指針をまとめ、それに対応して提供側の指針をまとめた。

１．３　ガイドラインの構成

（１）解説編

適正な「時」とそれに基づくデジタルな時の痕跡の重要性、必要性を明らかにし、時刻認証基盤の導入による効果を示すことも本ガイドラインの目的の一つである。そのため、デジタル文書に特有の課題、課題への対処としての時刻認証基盤の仕組み、およびその主要な構成要素である標準時配信および時刻監査とタイムスタンプの仕組みを解説する。

電子化情報の課題では、時刻認証が何故必要なのかを解説する。すなわち、原本と複製が識別不可能というデジタル文書の本質から、改ざんやなりすまし等の情報の信憑性にかかわる問題があり、否認による契約不成立等のトラブルが生じること、電子署名の仕組みでは存在証明、完全性、順序性等に限界があることを示している。

時刻認証基盤の仕組みでは、時刻認証のための仕掛けと信憑性について記載することで、時刻認証の必要性を訴求する。ここでは、時刻認証にかかわる事業者とその役割、協定世界時からタイムスタンプ発行および検証までの流れ、時刻のトレーサビリティについて記載する。

（2）利用ガイドライン編

何らかのサービスを顧客に提供する事業者、あるいは住民に行政サービスを提供する地方公共団体を対象にした､標準時配信･時刻監査サービス導入およびタイムスタンプ付与の指針である。前者はおおむね様々な業務に共通する指針であるが、後者は電子政府の入札業務と申請業務に対する指針を個別具体的に示すことにする。

標準時配信・時刻監査サービスの指針では最初にサービスを受ける際の要件提示方法と、それに沿って各サービスの導入に必要な選定基準をサービスモデルとともに示す。時刻に関しては他のサービス以上に導入時もさりながら、運用が重要であるので、利用者側の注意すべき点を運用指針として示すこととする。

指針の内容としては先ず業務フローを明確にして、それを基にタイムスタンプを付与すべき対象文書とタイミングを抽出する。さらに、タイムスタンプを利用する理由ないし目的を明らかにすることにより、システム仕様に反映する際の判断材料を提供する。付与するタイムスタンプの要件は対象業務によって異なるので、業務別に有効期間、時刻精度、検証機能などについての要件を示す。また、タイムスタンプを取得しただけでは当該文書の信憑性を保証することはできないので、取得したタイムスタンプの取扱いと検証に関する指針も示すことにする。

今回は電子申請と電子入札についての指針を示しているが、考え方や着眼点は他の業務に応用できることが多い。タイムスタンプの要件項目は、業務を通じて共通する点が多いので、多くのシステムで基本仕様への取り込みに流用することが可能である。

（3）提供ガイドライン編

時刻認証基盤の諸サービス提供にかかわる事業者を対象に、サービスをどう継続的に実現するかの必要最小限の要件を示した指針で、サービス別に事業者が準拠すべき技術および運用の基準を示す。これを基礎にして事業者独自の付加機能を加えるのが適切である。

今回対象としたサービスは、標準時配信と時刻監査、タイムスタンプ発行およびタイムスタンプ検証の三種類である。それに共通事項としてファシリティ、ネットワーク、サーバの基準を含めた。なお、タイムスタンプ発行の方式には、大別してシンプルプロトコルとリンキングプロトコルの二種類があり、それぞれに特徴があるので、両方式を併記している。

サービス提供にはまずは事業方針あるいはビジネスモデルを確立することが必要である。それを具体化する際に本ガイドラインを参照して、適切な水準の技術基準と運用基準を定めることになる。なお、本ガイドラインの範疇外であるが、タイムスタンプサービスの性格上、経営に関する基準も設定することが望ましい。

第２章　電子化情報の課題

高度なネットワーク社会では、電子化情報はますます重要となっている。電子商取引も行われつつあるが、安全な取引を保証する情報ネットワーク基盤が不可欠である。安全な取引においては、通信路の秘匿、相手確認である認証と、取り交わす文書の真正性が必須の要件となる。特に真正性は、電子化情報が、その流通の容易さおよび波及する速度が高速であるまた容易に複製を作成しやすいということからその確保が大きな課題である。

２．１　想定される脅威

電子化情報の流通において、なりすまし、改ざん、漏洩、事後否認という脅威が想定される。

①　なりすまし

悪意のある第三者が本人を偽って本人の行為を行うことである。ネットワーク上での商取引等では厳密な本人の確認がないままであれば、本人の知らぬ間に取引がなされ、被害を被るケースがある。これに対しては電子署名によって本人性を保証し、本脅威を防ぐことが可能である。

②　改ざん

悪意のある第三者が、電子文書を改ざんして重要な情報を書き換えることがある。電子文書の変更が容易でこれを検出できない場合、誤った情報による電子申請などで被害を被るケースが想定される。電子署名を付与すれば文書の真正性を保証するから、電子文書の改ざんを検出することが可能である。

③　事後否認

ある事実を後になって否認することである。例えば電子申請では、申請を受信した事実、申請を送信した事実、契約文書などでは文書に対して署名した事実などである。これらは、多くのネットワークにおけるやりとりにおいて容易に起きることが想定される。特定の事実に対して証拠を記録しなければこの脅威を防ぐことはできない。電子署名は、本人性を保証することで、後日の否認を防ぐことが可能である。

２．２　電子署名技術

（１）電子文書の真正性とは

従来の紙の社会では、文書を本人が作成したものである場合に、その文書を「真正に作成された文書」または「真正な文書」と言う[1]。さらに、本人である作成者が押印するということは、その内容の真正性についても推定されるということになる。2001 年より施行された電子署名法（正式名称：電子署名および認証業務に関する法律）では、民事訴訟法 228 条第 4 項における私文書の真正性の推定効を電子文書（正確は電磁的記録）に対しても認めることを制定した。これにより、公開鍵暗号技術（PKI：Public　Key　Infrastructure）を利用した信頼性の高い認証局から発行された公開鍵証明書によって保証された鍵によって署名されていれば、電子文書の真正性は

[1] 「電子署名法」　夏井高人　リックテレコム

法的な裏づけを持つこととなった。電子署名法では信頼ある認証局の認証業務に対する要件も定めている。

（2）電子署名技術

電子署名技術は、電子文書の本人性と内容の正当性を保証する技術である。PKI を利用すると、信頼ある認証局から発行された公開鍵証明書の情報を用いることで、誰が署名し、作成し、内容が改ざんされていないかを確認できる。

図 2-1 に PKI における電子署名の概要を示す。従来の紙の世界では、実印に対して役所が印鑑証明を発行し、取引の当事者は印鑑証明によって証明された印影と本人しか押印できない実印の印影を確かめ、その押印された文書の真正性を確認している。これに対して PKI では、信頼ある認証局が厳密な本人確認を行ったうえで、本人が持つ公開鍵ペア（公開鍵と秘密鍵）に対して公開鍵証明書を発行する。取引の当事者は、本人しか持つことのできない「秘密鍵」を用いて電子署名を作成し、秘密鍵とペアになっている公開鍵でのみ内容を確認できる。

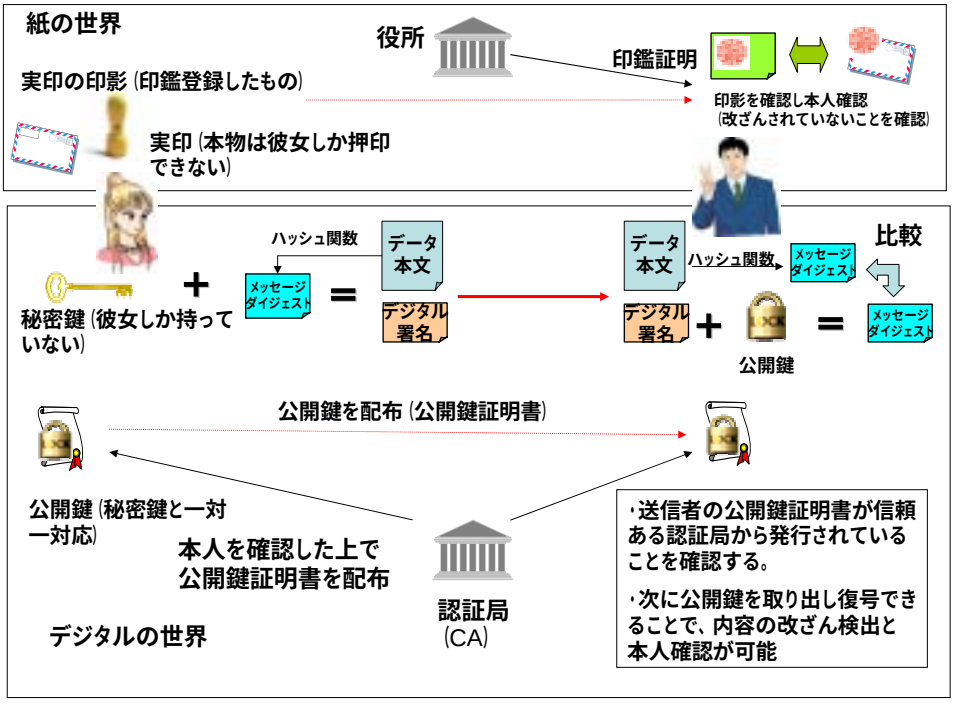

図 2-1　PKI の仕組み

PKI の技術基盤である公開鍵暗号方式では、データを暗号化・復号化する場合に使用する一対の「かぎ」が一方向性を持つ。すなわち、鍵（公開鍵）の一方から他方（秘密鍵）を推論するのは困難であるという理論に基づく。そこで秘密鍵を本人のみが持つこととし、公開鍵は認証局によって本人を保証された上で公開鍵証明書に含み、利用される範囲に開示する。公開鍵証明書には、公開鍵のほか、本人を識別するための名前、有効期限、利用用途、その他運用情報などが含まれ、認証局により電子署名が付与されている。これにより確かにその認証局が発行した公開鍵証明書であることを保証し、他者による改ざん等を検出できる。

電子文書の真正性を保証する電子署名では、ハッシュ関数により電子文書を縮退したメッセー

ジダイジェストに対して、本人のみが保持する秘密鍵による暗号演算を行う。電子署名付き文書の受け取り人は、作成者の公開鍵証明書と認証局の公開鍵証明書を入手し、作成者の公開鍵証明書が有効で信頼ある認証局から発行されたことを検証する。その後作成者の公開鍵により電子署名付き文書の署名を検証することで、本人が作成したものであることを確認する。メッセージダイジェストもまた一方向性を持つため、送信途中などで壊れたり、改ざんされると、受信者が電子署名を検証するとき、これを検出することが可能である。

２．３　電子署名の限界

電子署名技術は、インターネットにおける電子申請などで必須の要件である文書の真正性を確認できる技術として電子政府や電子自治体基盤に導入されてきた。しかしながら、公開鍵暗号基盤（PKI：Public Key Infrastructure）を利用した電子署名文書には、以下の課題が存在する。

- 電子署名自体には時間情報が含まれないため、その文書がその時点で存在したかということは保証しない。（図 2-2 で、時間軸自身の正しさを証明できない）
- 署名付文書が PKI における認証局によって保証される期限は、その署名に利用した秘密鍵の有効期限を示す公開鍵証明書の有効期限内に留まる。または、有効期限内に失効した場合はその失効申請を認証局が受理し失効処理を行った時点までとなる。（図 2-2）。
- PKI による電子署名による文書の真正性は、悪意の第三者の改ざんを防ぐことは可能であるが本人の改ざんを防ぐことはできない。

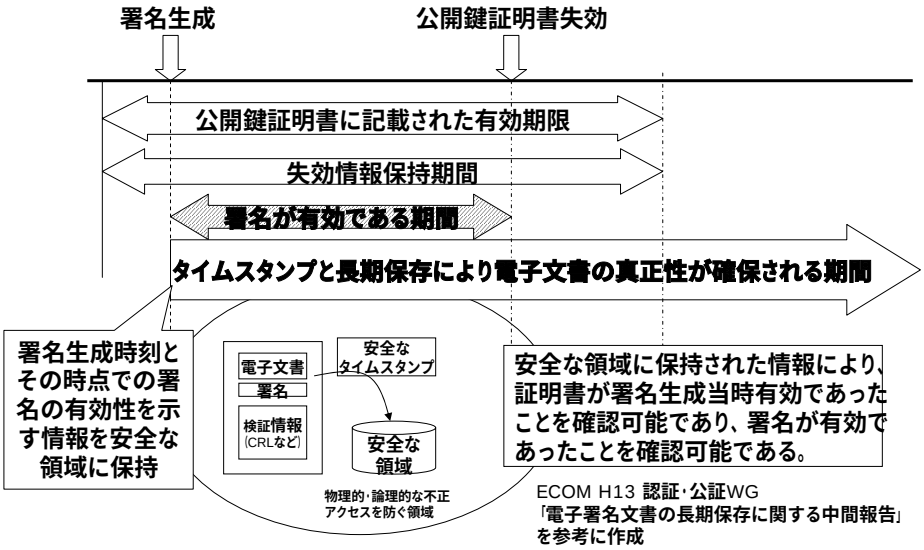

図 2-2　電子文書の真正性を保証する期間

以上の課題を解決するために、タイムスタンプ技術を導入し、電子文書にタイムスタンプを付与して特定の時間における電子化情報の存在証明を実現する必要がある。

第３章　時刻認証基盤の仕組み

時刻認証基盤とは技術面からすると、標準時配信サービスとタイムスタンプサービスおよび関連する諸サービスを提供するシステム基盤である。標準時配信サービスは国家時刻標準機関(NTA)に代わって標準時を配信するサービス、そして、タイムスタンプサービスは NTA または標準時配信サービス等から配信される時刻を時刻源として、文書などのデジタル情報に対して存在証明や非改ざん証明を行うサービスである。

タイムスタンプサービスの基盤では、①タイムスタンプトークン発行機能、②タイムスタンプトークン検証機能、③時刻のトレーサビリティ機能を提供し、標準時配信サービスの基盤では、タイムスタンプ局をはじめとしたサービス利用者に対する、①標準時の配信機能と、②時刻監査機能を提供する。

本章では、時刻認証基盤の仕組みについて全体的な概要を記述し、標準時配信及びタイムスタンプの仕組みの詳細に関しては、第 4 章および第 5 章に記述する。

３．１　時刻認証サービスモデル

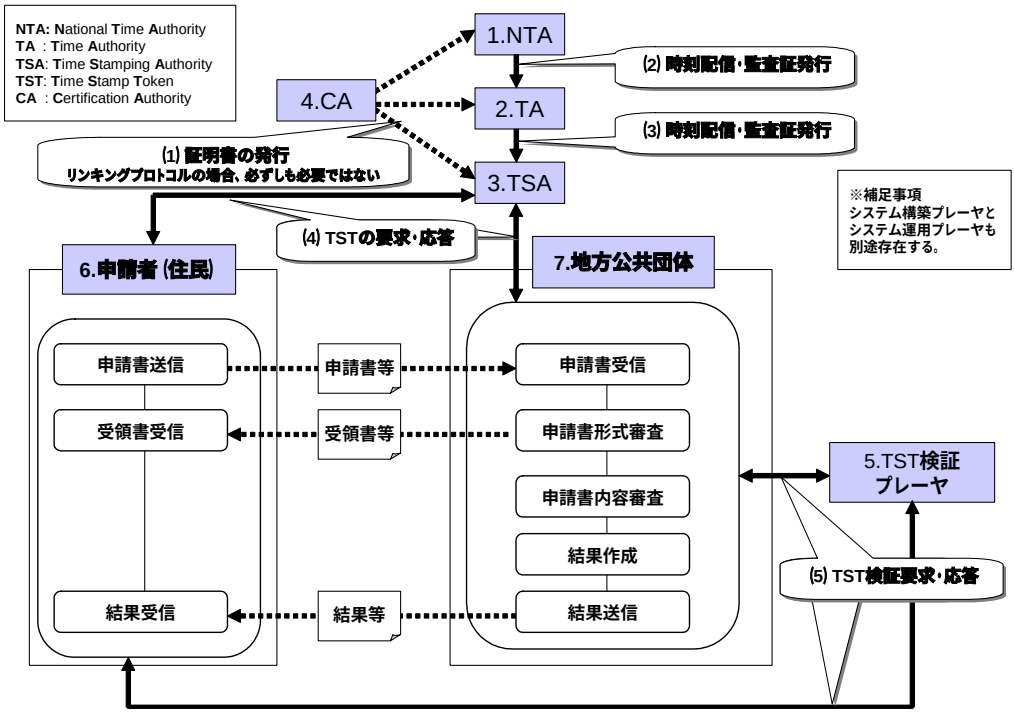

図 3-1　電子申請における時刻認証サービスモデル図

電子自治体の電子申請システムへ時刻認証サービスを適用した時刻認証サービスモデルを説明する。このモデルの構成要素となるプレーヤは次の通りである。

・NTA（National Time Authority）

国家時刻標準機関である。国家標準時を生成、維持、配信する。TA、あるいは、TSA に対して標準時を配信する。また、定期的に TA の時刻の監査を行う場合もある。

・TA（Time Authority）

標準時配信局である。TSA に対して標準時を配信する。また、定期的に TSA の時刻の監査を行う。標準時配信局は、信頼できる第三者機関である。

・TSA（Time Stamping Authority）

タイムスタンプ局である。利用者から送られてきた電子データに対するタイムスタンプトークンを作成し、発行する。タイムスタンプ方式によっては、後述する TST 検証プレーヤを兼任する。タイムスタンプ局は、信頼できる第三者機関である。

・CA（Certification Authority）

認証局である。NTA、TA、TSA に対して認証、あるいは署名用の公開鍵証明書を発行する。信頼できる第三者機関である。タイムスタンプ方式によっては、このプレーヤは存在しない。

・TST 検証プレーヤ

タイムスタンプトークンの妥当性を検証するプレーヤである。タイムスタンプ方式により、プレーヤの実体は異なる。例えば、シンプルプロトコルのタイムスタンプトークンの場合は、PKI 基盤上で利用者自身が妥当性を検証することが可能である。一方、リンキングプロトコルのタイムスタンプトークンの場合は、トークン発行元となる TSA、あるいは、その他の第三者機関が TST 検証プレーヤとなる。

・申請者（住民）

申請を行う住民、および住民が操作するソフトウェア、あるいは、装置を表す。地方公共団体の申請受付システムと通信を行い、申請手続きを実行する。自身が作成した申請書の存在証明を行うために、TSA に対してタイムスタンプ発行を依頼することもありうる。トラブル発生時などに、TST 検証プレーヤを利用して、地方公共団体から受け取ったタイムスタンプトークンの妥当性検証を行う。

・地方公共団体

住民に対して申請サービスを提供する地方公共団体、および申請システムを表す。TSA が提供するタイムスタンプサービスを利用し、申請者から受け取った申請書、申請業務時に作成する受領証、結果、などにタイムスタンプを付与する。トラブル発生時などに TST 検証プレーヤを利用して、タイムスタンプトークンの妥当性検証を行う。

・システム構築プレーヤ

時刻認証基盤システム、および時刻認証サービスを適用したアプリケーションシステムを構築する事業者である。

・システム運用プレーヤ

時刻認証基盤システム、および時刻認証サービスを適用したアプリケーションシステムを運用する事業者である。

３．２　標準時配信と監査

標準時を配信する手段としては、NTA からブロードキャストされる電波や、GPS からの電波、インターネット上で公開されている NTP サーバなどがあり、電波時計や GPS レシーバ、NTP クライントソフトなどの利用環境さえ整備すれば、標準時を受信して運用する事ができる。

一方では、配信される時刻情報の信頼性を確保する為に、TA により通信回線を確保した上で標準時を配信するサービスが存在するが、その場合も NTP などの汎用的なプロトコルが利用されていることが多い。

また、タイムスタンプ局を初めとするサービス利用者の運用する時刻と、標準時との時刻差を測定し監査するサービスが存在し、それは標準時配信サービスと併せて提供される事もあれば、独立してサービス提供される事もある。

TA がサービス利用者の時刻を監査する仕組みについては、現在のところ世界的にも標準化の動きは見られないが、NTP のプロトコルを応用してサービス利用者と TA との時刻差を測定する手法が取られていることが多い。

３．３　時刻認証のトレーサビリティ

時刻認証のトレーサビリティとは、タイムスタンプトークンに含まれる時刻情報の追跡可能性を表す。本ガイドラインでは、時刻認証のトレーサビリティがあるとは、以下の二つの要件を満足していることを示す。時刻認証基盤では、タイムスタンプトークンが主張する時刻情報の信頼性を高めるために、この時刻認証のトレーサビリティを提供する。

（１）信頼のできる時刻源

TSA は、TA の時刻源、可能であれば、NTA が管理する時刻源を参照し、その時刻源に基づく時刻情報をタイムスタンプトークンに含めていることを証明できる。

（２）国家標準時との同期

TSA がタイムスタンプトークン発行時に使用する時刻と国家標準時との誤差が、許された範囲内に入っていることを証明できる。

時刻認証のトレーサビリティ確保の仕組みとしては、いくつか考えられる。例えば、以下の（１）、あるいは、（２）の方法がある。

（１）タイムスタンプトークン内に時刻認証のトレーサビリティを示す情報を含める

（２）TSA が、信頼のできる時刻源を参照し、さらに、標準時配信局、あるいは、国家時刻標準機関から定期的に監査を受けていることを証明する

第４章　標準時配信の仕組み

４．１　標準時配信の概要

（１）市場での課題

タイムスタンプが電子データ単体の存在証明と非改ざん証明を可能にするものであるのに対し、「標準時にトレーサブルな時刻をセキュアに安定配信してほしい」というニーズや、更に「配信されて時刻校正されながら運用しているという事実を第三者に証明（証言）してもらいたい」というニーズがある。即ち、そのシステムに関わる連続的な時間の運用状況そのものの信頼性に関して、自己宣言だけでなく信頼のおける第三者機関に依拠したいという要求である。

（２）ガイドラインの対象となる標準時配信・監査サービスの定義

標準時配信・監査サービスには様々なサービス範囲とレベルが存在し得るが、ここではガイドラインとしての便宜上、次のように定義する。

『標準時配信・監査サービスとは、NTA にトレーサブルなタイムソースを元にした時刻をセキュアに安定配信し、配信元に対する配信対象機器の時刻差情報と校正記録を、第三者証明に耐えうるような形で提供するサービス』であり、『時刻監査サービスとは、NTA にトレーサブルなタイムソースを元にした時刻に対する監査対象機器の時刻差情報を、第三者証明に耐えうるような形で提供するサービス』である。

（３）ガイドラインの対象者

標準時配信・監査に関わるプレーヤとしては、国家時刻標準機関、標準時配信局、タイムスタンプ局を含む標準時配信・監査を受けるエンドユーザがあるが、ここではサービス提供側の指針として標準時配信局及び時刻監査局を対象にし、サービスを受ける側の指針としてはタイムスタンプ局を含む標準時配信・監査を受けるエンドユーザを位置付けた。

４．２　標準時配信、時刻監査サービスモデル

（１）概要

標準時の配信手段や、時刻校正手段、異常時の警告報知手段、更には、サービス対象機器の時計が期待通りに動作していたかどうかを監査する手段などは様々な形態が考えられ、標準時配信、時刻監査サービスモデルはそれらの要素の組み合わせで構成される。

標準時配信、時刻監査サービスを提供する TA は、①信頼のおける第三者機関である事、②NTA との時刻のトレーサビリティを確保している事、③サービス利用者の運営する時刻と TA との時刻の差分情報をレポートとして提供できる事が必要条件としてあげられる。

この章ではサービスモデルを紹介する。また、標準時配信サービス及び時刻監査サービスの両サービス共に、配信、監査に使用する時刻は NTA にトレーサブルである必要があるが、NTA-TA 間の時刻差を遠隔地にて計測する技術を紹介する。

（2）標準時配信・監査サービスモデル

標準時の配信をすると同時に、配信先の時刻の運用状態をセンターに保管、監査を行うサービスモデルである。

このサービスを提供するセンターでは、原子時計とタイムサーバをセキュアで安定した環境にて運用し、時刻監査対象となる利用者側サーバに対して専用に確保した回線を使って時刻を配信する。

利用者側サーバでは、専用のクライアントソフトにより、クライアント識別情報や時刻の運用に関わる計測、管理情報をセンターにアップロードする。

センターにアップロードされた情報は、データベースに保管され、利用者は Web ブラウザなどでそのログ情報と解析結果を確認する事ができる。また、必要に応じて監査証書の発行も行う。

タイムソースである原子時計の NTA とのトレーサビリティを確保する為に、GPS との時刻比較データを記録・保管し、その内、未加工の測定データを GGTTS フォーマットで Web などに公開、及び NTA である独立行政法人情報通信研究機構が公開している GPS 時刻比較データをもとに比較計算した結果（時刻差測定、時刻比較結果平均値、時刻比較結果標準偏差）も Web などにて公開する。

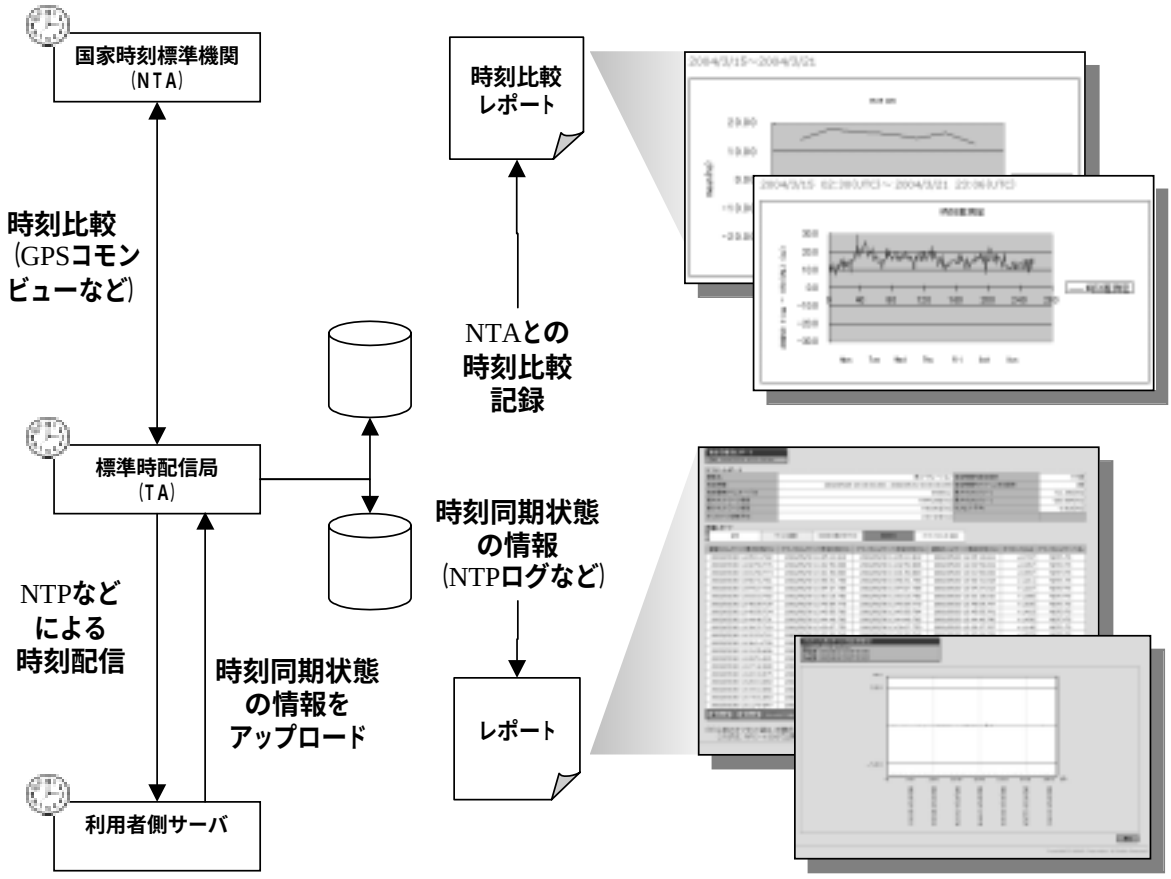

図 4-1　標準時配信、時刻監査サービスモデル

（3）時刻監査サービスモデル

独自に NTA からの時刻配信を利用して時刻同期している利用者側サーバに対して、時刻監査局が時刻運用状況の監査を行うサービスモデルである。

時刻監査局は、時刻精度の高い時計により運用され、NTA とのトレーサビリティを確保するため NTA と時刻同期を行う。

また、NTA または NTA に代わる監査機関から時刻監査を受け、NTA との時刻差を比較検証できる仕組みを有する。

時刻監査局は、時刻監査対象となる利用者側サーバに対して、ISDN 回線などを経由して、1 日に 1 回以上時刻監査局側の時刻と比較検証を行い、時刻の差異が規定値を越えた場合、警告を管理者に通知する。

時刻監査局は、時刻監査対象となる利用者側サーバの監査結果を監査レポートとして、定期的に管理者に通知する。また、時刻監査記録は、時刻監査局で不正な改変や削除から保護する仕組みを持って必要な期間保管する。

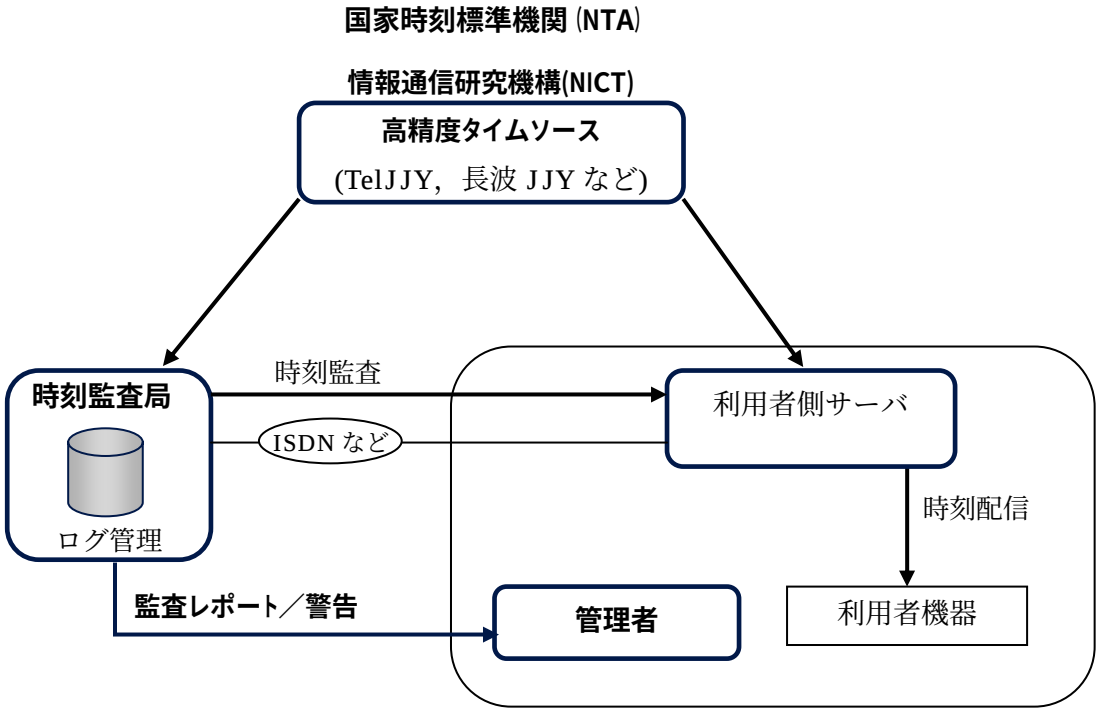

図 4-2　時刻監査サービスモデル

4．3　NTA-TA 間の時刻校正技術

標準時配信局及び時刻監査局に時刻を提供する TA は、運用しているタイムソースが協定世界時と TA 自身で規定する一定範囲内に同期している事を証明する必要があるが、現時点ではこれに関する法的な枠組みや明確な定義が無い為、実際にタイムビジネスを展開している標準時配信局及び時刻監査局やタイムスタンプ局はそれぞれ独自の方法を用いている。

独立行政法人情報通信研究機構では、周波数標準器校正サービスの拡充を目的として、GPS を仲介とした、いわゆるコモンビュー法を用いた周波数の遠隔校正システム研究開発が進められている。

このシステムは計量標準に連鎖性を持たせた測定器・標準器等の遠隔校正を主目的としてはいるものの、周波数の校正だけでなく、遠隔地の時刻校正にも応用が可能である事から、電子時刻認証基盤への導入も重要な研究課題と位置付けられていり。第 105 回研究発表会予稿（独立行政法人通信総合研究所、現：情報通信研究機構 2003 年 11 月発行）の中の「電子時刻認証システム開発」によると、東京都小金井市にある独立行政法人情報通信研究機構と神奈川県横浜市にある民間企業との間でこのシステムの実証実験を行った結果、遠隔地の標準時校正がナノ秒オーダーで達成されている。

また今後の課題として、独立行政法人情報通信研究機構と TA 間のトレーサビリティを確保する為に時刻校正証明の開示方法等の検討が上げられている。

第５章　タイムスタンプの仕組み

５．１　タイムスタンプの役割

多くの業務がコンピュータによる処理が行われ、文書、図表、映像、音声などの情報は電子情報（デジタルデータ）として存在する。デジタルデータは、情報社会において利用されることから容易に複製を作成可能であること、情報の伝播が高速などの特性を持つ。

このために、従来の社会とは異なる「証拠」の確保が必要となる場合がある。ある情報が「いつ」存在したかを証明するための証拠もそのひとつである。たとえば、文書が紙で作成されていた場合、その文書が存在したことは、そこに記された「日時」情報などとペンや紙の経年変化によって証明できる。しかし電子文書で存在する文書は、日時が付与されていても、容易に改ざんされ、複製も可能である。また、企業等における多くの文書は保存することが法律で義務付けられており（表 5-1）、これは文書の存在が必要とされていることでもある。

表　5-1　民間において保存が必要とされる文書の例

10年	株主総会議事録	商法、製造物責任法
	商業帳簿	
	製品の製造、加工、出荷、販売の記録	
7年	仕訳帳	所得税法、法人税法
	総勘定元帳等の帳簿	
	棚卸表	
	賃借対照表	
	損益計算書	
	注文書･見積書･契約書の控え	
5年	財産形成非課税貯蓄申込書	所得税法
	移動申請書	

文書のほかにも証拠として明らかにしておく必要があるものに、送受信の証明がある。ネットワーク上を契約当事者間でやりとりされた、契約書などの文書は確実に相手に届く必要がある。紙の場合であれば、郵政公社の配達記録や書留郵便で相手への送出、相手からの受け取りを証明することができる。しかしネットワーク上では、送信にかかわる多くのシステムやサーバ機器、通信機器、通信路などが存在し、どれかの障害によっては相手に届かないケースも考えられる。したがって、確実に相手に届く・相手が受け取る・自身が送信したことなどを証拠として保存することが必要とされる。この送達を確認するために使用する証拠情報は、送受信したことを表す「事実」の存在を証明することである。

これまで述べた文書を保存するための存在証明や、送達確認のための証拠情報としてタイムスタンプを利用することが有効である。タイムスタンプは、あるデジタルデータがその時刻より以降に存在したことを証明できる情報である。タイムスタンプはデジタルデータの特性を暗号技術によって保持した上で時間を証明するため、デジタルデータが変更された場合は、その存在を証明することは不可能となる。

一方、電子署名は、タイムスタンプとともにデジタルデータの証拠を確保する手段である。公開鍵暗号方式を使用した電子署名では、本人が作成したこと（本人性の確認）、タイムスタンプと同様に内容の改ざんがされていないことを証明することが可能である。タイムスタンプと電子署名を併用することで、デジタルデータの証拠性は、「本人性」「完全性」「存在性」を証明することが可能である。

また、電子署名文書を長期に保存する場合、公開鍵証明書の期限を超えた電子文書の場合や、鍵アルゴリズムが危殆化した場合を想定し、正当な時点での検証情報等に対してタイムスタンプを付与し存在証明をした上で、長期間経過後も電子文書の「本人性」「完全性」「存在性」を保証することが可能となる。

表 5-2 にタイムスタンプ付与により実現可能な効果を示す。

表 5-2　タイムスタンプ付与による効果

効果	内容
送受信証明 （事後否認を防止）	文書の送受信結果の事後証明を目的とし、送受信された事実を示す事象等に対して、非改ざんを証明および事後否認を防止するためのタイムスタンプを付与する。
文書存在証明	文書の存在時刻や、施行時刻に関する順序性あるいは一定時刻との前後関係が重要な場面で、非改ざんを証明および事後否認を防止するために、文書にタイムスタンプを付与する
長期保存証明	電子署名の有効期間を補うことを目的とし、長期的に内容の非改ざんおよび電子署名付与時の電子署名・証明書が有効であったことを過去に遡って証明するために、タイムスタンプを付与する。

５．２　タイムスタンプサービスモデル

5.2.1　タイムスタンプサービスに求められる機能

タイムスタンプサービスは特定の時点で電子化情報が存在したことを保証するサービスを提供する。タイムスタンプサービスは、少なくとも以下の２つの要件を満たさなければならない。

- ある時点で電子化情報が存在したことの証拠として、時刻情報と電子化情報の関連を技術的に対応付けられること。
- 電子化情報の内容に関知しない。

前者の対応付けについては、暗号技術を利用することが多いため、さらに暗号技術を利用する際のセキュリティに対する要件も必須となる。

タイムスタンプサービスは、図 5-1 に示すモデルにおいて TSA（Time Stamping Authority）により提供される。

- NTA（National Time Authority）

国家時刻標準機関である。国家標準時を生成・維持・配信する国家機関をさす。

- TA（Time Authority）
  標準時配信業者。NTA から時刻配信を受け、TSA へ標準時を配信する。
- TSA（Time Stamping Authority）
  TA より時刻配信を受け、利用者からの要求に応じて時刻証拠となるタイムスタンプトークンを発行する。
- 時刻利用者
  電子データの存在を証明してもらうため、TSA に対してタイムスタンプトークンを要求する。また、取得したタイムスタンプトークンを検証するために検証主体に対して検証を要求する。
- タイムスタンププロトコル（TSP；Time-Stamping Protocol）
  TSA/TA 間の通信手順を指す。ISO WD18014、RFC3161 などで規定されている。
- タイムスタンプトークン（TST）
  時刻証拠となる電子データ。

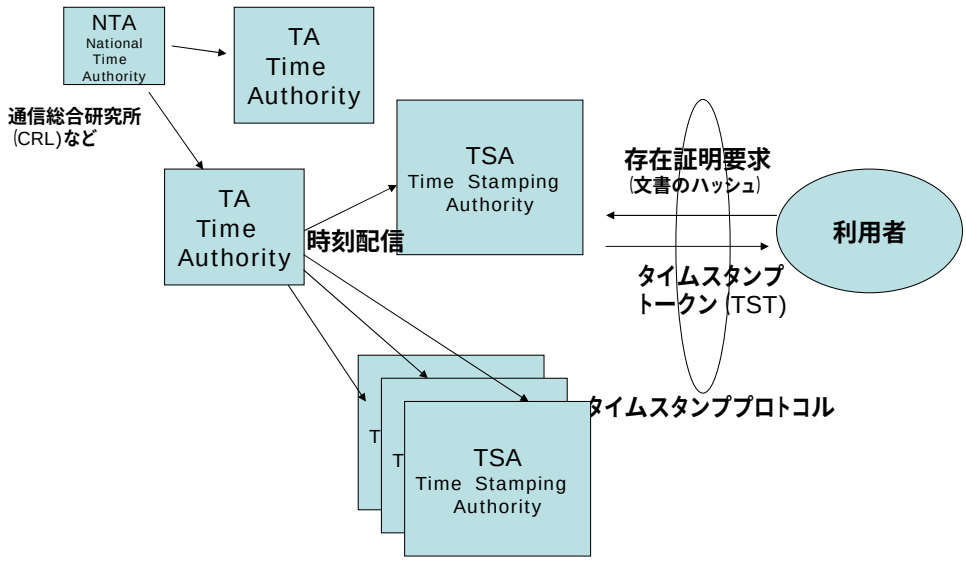

図 5-1　タイムスタンプサービスのモデル

5．2．2 タイムスタンプトークン発行の流れ

ISO18014 では、タイムスタンプトークンの形式によって、独立トークン方式、リンクトークン方式の２つのタイムスタンプ方式があると定義している。これらの方式に共通して、利用者が電子文書に対してタイムスタンプを付与する基本的な手順は以下のようになる。

- 利用者が TSA へタイムスタンプ要求メッセージを送信する

要求メッセージの中には、利用者が計算した電子文書のハッシュ値が含まれている。

- TSA がタイムスタンプを作成する
  TSA は、受信したハッシュ値と信頼のできる時刻情報を結びつけたタイムスタンプトークンを作成し、それを利用者へ送信する。
- 利用者がタイムスタンプ局からタイムスタンプ応答メッセージを受信する
  受け取った応答メッセージ内に含まれるタイムスタンプトークンを電子文書と一緒に保存する。

なお、トランスポートメカニズムは、オンラインプロトコル（例えば、HTTP)、ストアアンドフォワードプロトコル（例えば、電子メール）などが考えられる。また、通信時のセキュリティ対策(なりすまし、改ざん、盗聴の対策)は、トランスポートメカニズム上、あるいは、アプリケーションレイヤ上で実現されているものとする。以上のことは、発行手順に限らず後述する検証手順にも適用される。

以下に各方式の代表的な例を説明する。

（1）独立トークン方式

独立トークンは国内ではシンプルプロトコルとも呼ばれている。この方式を代表するものに、PKI を用いたタイムスタンプがありこれは IETF で RFC3161 として標準化されている。時刻情報に TSA の電子署名を付与し、TSA による第三者保証をしたものである。ユーザは、タイムスタンプの対象文書のハッシュ値（メッセージダイジェストと呼ぶ）を含む、決められたフォーマットのタイムスタンプ要求を TSA に送付する。TSA は、受信したメッセージダイジェストと受付時刻を含む規定のフォーマット（タイムスタンプトークンの形式）の文書に電子署名を付け、タイムスタンプトークン（TST：Time Stamp Token）を作成して、ユーザに返送する。ユーザは、受け取ったタイムスタンプトークンを保管しておき、将来、元の文書のタイムスタンプトークンが必要になった時点で、タイムスタンプトークンを TSA の公開鍵証明書を用いて検証することにより、時刻証明書が発行された時点において、元の文書が存在していたことを証明することができる。

この方式の特徴は、発行されたタイムスタンプトークンおよびその証明書作成に用いられた公開鍵暗号の公開鍵証明書を用いるだけでタイムスタンプトークンの検証が可能であるということである(図 5-3)。この方式が有効であるためには、TSA は信頼のおける第三者機関(Trusted Third Party: TTP)でなければならない。

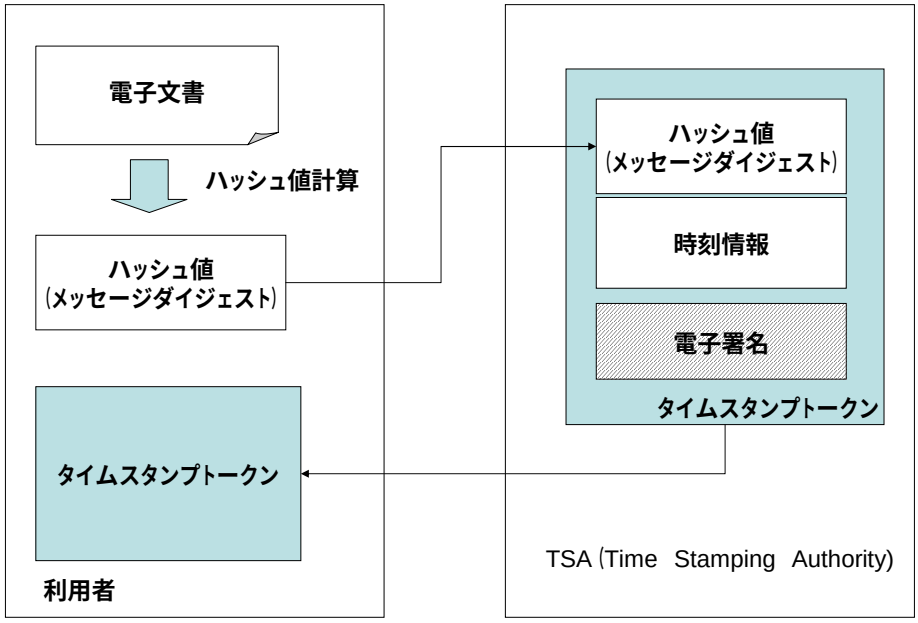

図 5-2　独立トークン方式のタイムスタンプ（PKI 方式）

独立トークン方式によるタイムスタンプには、他にメッセージ認証コード（Message Authentication Code; MAC）を用いる方式とアーカイブ方式がある。

MAC 方式は、ISO/IEC 18014 において標準化されているが、図 5-2 で説明した方式とは、電子署名のかわりにメッセージ認証コードを用いるところが異なる。この方式では、TSA が所有する秘密鍵を用いて、MAC を作成する。すなわち、検証には TSA が秘密にして保持する秘密鍵が必須である。このため、時刻証明書を受け取ったユーザが時刻証明書だけを用いて、証明書の正しさを検証することができない。この方式では、TSA は第三者信頼機関でなければならない。この性質を第三者機関による TSA の監査によって保証する枠組みが必要となる。すなわち、時刻証明書を受け取ったユーザが時刻証明書の検証に一切かかわることがないため、TSA が正しい時刻証明書を発行し続けていることの監査が必要となる。

アーカイブ方式は、TSA にアーカイブされているメッセージダイジェストと時刻情報の対応関係への参照情報を時刻証明書に含める時刻証明方式である。TSA の信頼性だけで成り立つ方式である。

（2）リンクトークン方式

リンキングプロトコルはハッシュアルゴリズムの安全性に依存する方式である。利用者から電子文書のハッシュ値を受け取り、証拠となるリンクトークンを返す。また定期的に全体のハッシュ値を歴史的な証拠となるように新聞等に公開している。

図 5-3 は、TSA が直前あるいは時間的に近傍で受け付けたタイムスタンプ要求に含まれるメッセージダイジェストとハッシュ関数により関連付けた時刻証明書を発行する方式である。この方式では、結果的に過去に発行した時刻証明書すべてとのリンクが作成されることになる。このた

め、過去に発行したすべての証明書との整合性を取らない限り、時刻証明書の偽造を行うことができない。また、定期的に時刻証明書のリンク情報を新聞等で衆目にさらすことにより、リンク情報の偽造をさらに困難にするとともに、リンク情報の検証を定期的な公開期間内だけで済ませることが可能となる。

この方式では発行された時刻証明書の検証に TSA が常に必要となる。

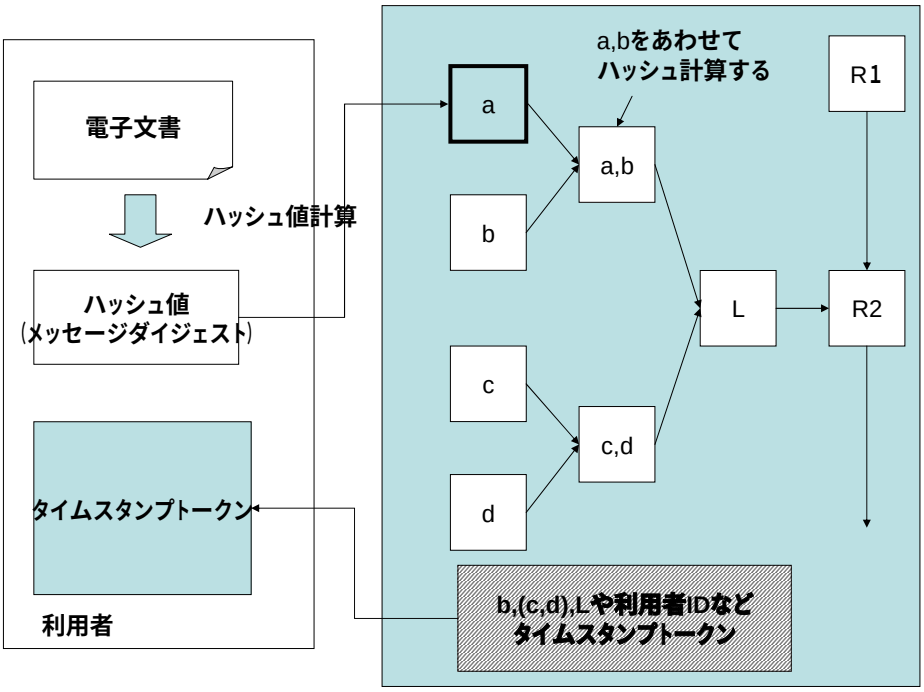

図 5-3　リンクトークン方式

5.2.3 タイムスタンプトークン検証の流れ

タイムスタンプ方式によりタイムスタンプトークン検証の手順は異なる。

シンプルプロトコルを用いたタイムスタンプトークンの場合、PKI 上で利用者自身が検証することができる。基本的な検証手順は次の通りである（図 5-4 の①）。

- タイムスタンプトークンの形式検査を行う
- 検証対象の電子データのハッシュ値とタイムスタンプトークン内の該当するハッシュ値が同一かどうかを検査する
- タイムスタンプトークン内に含まれる TSA の電子署名を検証する
  TSA の公開鍵証明書の有効性を検査し、その公開鍵証明書に含まれる公開鍵を使用してタイムスタンプトークン内の電子署名を検証する。

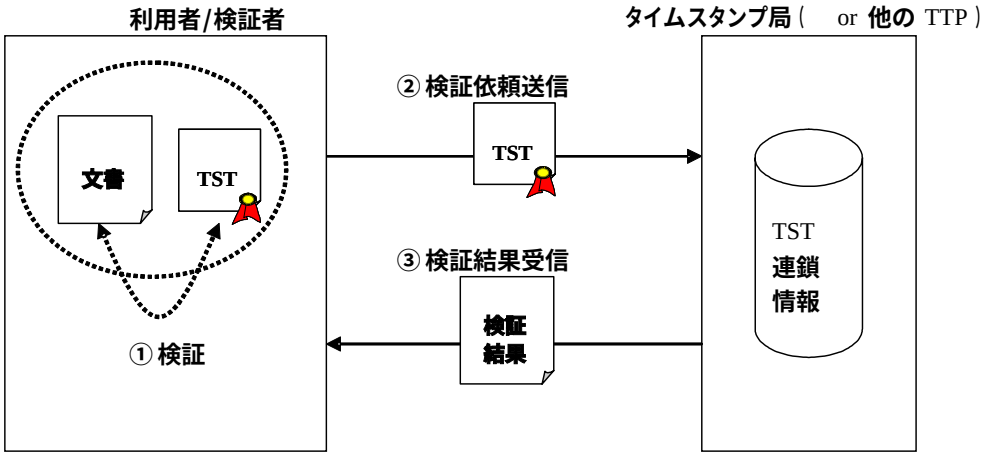

図 5-4 タイムスタンプトークン検証の流れ

もちろん、利用者自身が検証するだけでなく、信頼のできる第三者機関に検証を依頼することもできる。

リンキングプロトコルを使用したタイムスタンプトークンを検証する場合、検証に必要な連鎖情報を所有するプレーヤを利用する必要がある。具体的には、タイムスタンプトークン発行元となる TSA、あるいは、その他の信頼できる第三者機関を利用する必要がある。基本的な検証手順は次の通りである（図 5-4 の①、②、③）。

- タイムスタンプトークンの形式検査を行う
- 検証対象の電子データのハッシュ値とタイムスタンプトークン内の該当するハッシュ値が同一かどうかを検査する
- タイムスタンプトークンの正当性を検証するために、発行元となる TSA、あるいは、その他の信頼できる第三者機関に検証を依頼する
- 発行元となる TSA、あるいは、その他の信頼できる第三者機関から検証結果を受信する

５．３　技術動向

5.3.1 タイムスタンプの標準化動向

タイムスタンプ技術は、以下の国際規格（ITU-T/ISO）、インターネット標準などにおいて規定されている。

（1）国際規格

ISO/IEC　18014-1 Information technology – Security techniques – Time stamping services

- Part 1: Framework
  タイムスタンプサービスの要件、スコープ、提供サービス・機能などの枠組みについて規定している。タイムスタンプの証拠となるトークンについて、独立トークンおよびリンクトークンの 2 つの実現方式の概要を記述している。
- Part 2: Mechanisms producing independent tokens
  独立トークン方式のメカニズムについて定義する。電子署名を使用したトークン（RFC3161 互換)、MAC を使用したトークン、アーカイブを使用したトークンという３種類のトークンを規定している。
- Part 3: Mechanisms producing linked tokens
  リンクトークン方式のメカニズムを定義する。電子署名を使用したトークンと電子署名を使用しないトークンの２種類のトークンを規定する。

（2）インターネット標準（IETF：Internet Engineering Task Force）

- RFC3161　　Internet X.509 Public Key Infrastructure　Time-Stamp Protocol (TSP)
  インターネットで PKI を利用する上での標準群のひとつ。タイムスタンプモデルにおける手順とフォーマットであるプロトコル、タイムスタンプトークンについて規定する。
- IETF Policy Requirements for Time-Stamping Authorities (draft – ietf – pkix – pr – tsa-00.txt) (2002-03)
  TSAの運用ポリシーに関する要件について規定する。

（3）欧州標準

- ETSI TS 101 861v1.2.2 Time Stamping Profile
  RFC3161に基づく仕様書。タイムスタンプクライアントとタイムスタンプサーバが従う要件を定義する。

5．3．2 タイムスタンププロトコルに関する標準化

タイムスタンププロトコル（Time-Stamping Protocol）に関して、IETF では RFC3161 として 2001 年に標準化が完了している。ISO/IEC では、現在標準化の途中にあり、IETF の RFC3161 を含む形で標準化が進められている。

これらに関する標準化動向を表 5-1 に示す。

表 5-1　タイムスタンププロトコルに関する標準化動向

タイムスタンプトークンに用いる暗号方式		概要	検証	特徴	標準
電子署名		証明内容（メッセージダイジェストと時刻）に TSA の電子署名添付	証明書だけで検証が可能	・TSA は TTP	・IETF RFC3161 ・ISO/IEC 18014
メッセージ認証コード(MAC)		証明内容に TSA の対称鍵による MAC を添付	TSA の所有する秘密鍵が必要	・TSA は TTP ・TSA の監査が必須	・ISO/IEC 18014
アーカイブ		メッセージダイジェストに時刻を対応させる参照情報	TSA に保管される参照情報で検証	・TSA は TTP ・TSA の監査が必須	・ISO/IEC 18014
リンク方式	リンク情報のみ	時間的に近傍の証明書とハッシュ関数でリンク（結果的に過去のすべての証明書とリンク）	TSA のアーカイブが必要	・同一時刻の証明書間での順序が特定可能 ・暗号攻撃では偽造不可能	・ISO/IEC 18014
	リンク情報と電子署名	時間的に近傍の証明書とハッシュ関数でリンクをとるとともに、電子署名も作成	証明書だけでも、TSA のアーカイブを使っても検証が可能	・順序特定可能。 ・暗号攻撃では偽造不可能 ・証明書での検証可能	・ISO/IEC 18014

第Ⅱ編　利用ガイドライン

第１章　利用の枠組み

１．１　標準時配信の利用

標準時配信サービスを利用者側に立ってみると、①信頼のおける時刻の配信を受けること、②自身の時刻が正しいか監査を実施してもらうこと、③上述の①と②を組み合わせて受けることの３種類が考えられる。しかしながら、最終的には、自身の時刻が正しいことを信頼のおける第三者が証明しなければ価値がないため、①だけの利用ニーズは乏しく、②または③の利用が現実的である。

具体的な利用ニーズとしては、後述するタイムスタンプにより対外的に時刻の証明を行う場合（知的財産権の主張、電子契約の有効性確認等）や、自身が運営するシステム・アプリケーション群内での時刻規制に使用する場合（システム間連携、時刻不整合の場合のエラー処理等）が考えられる。現在のところ、上述のような時刻の正確さについての訴訟・係争はほとんど発生してはいないが、今後ビジネスや個人間取引のデジタル化が進展することは間違いなく、時刻の重要性は更に高まっていくであろう。

なお、標準時配信サービスの実例モデルは、第Ⅰ編 第４章で説明しているが、本編では、実際の利用に際し考慮すべき、具体的ガイドラインを第２章に示し、実例として「入札業務」と「申請業務」をそれぞれ第３章、第４章に掲げている。

１．２　タイムスタンプの利用

タイムスタンプは、企業や政府・地方公共団体の業務に一般的に見られる、文書が作成され、取り交わされ、利害関係が発生するといった文書の内容や活動の実行を証明しなければならないすべての場面において必要となると考えられる。しかしながら、それを必要とするすべての業務についてタイミングやその内容を明らかにし、まとめて記述することは困難である。また、必要とされるタイミングやその内容には類似性があるため、２、３の例を示すことで他の業務についても類推が可能であると考えられる

本ガイドラインでは典型的な利用例について、業務アプリケーション内でタイムスタンプの導入が推奨される場面と、その利用方法について述べる。それに先立って、この節では、タイムスタンプ付与に関する要件提示に関して、本編で述べる各種業務に共通な事項について述べる。

本書で示すタイムスタンプの利用ガイドラインは、タイムスタンプ付与のタイミングと対象を業務フロー上に示し、各付与対象の推奨レベルと内容を一覧表形式で示す(図 1-1)。したがって、業務毎にその業務の専門家がフローの形に表現することが必要である。

ここで、タイムスタンプ付与のタイミングと対象は業務によって異なるが、概ね、文書ないしデータの発生(作成)時、受け渡し時、判断・決定時、保存時がその候補である。すなわち、独立した文書・データがどのように存在していたかというためだけではなく、業務遂行の過程で改ざん、なりすまし、事後否認などが起こらないよう、文書・データの存在を証明するためにタイム

スタンプを付与する。

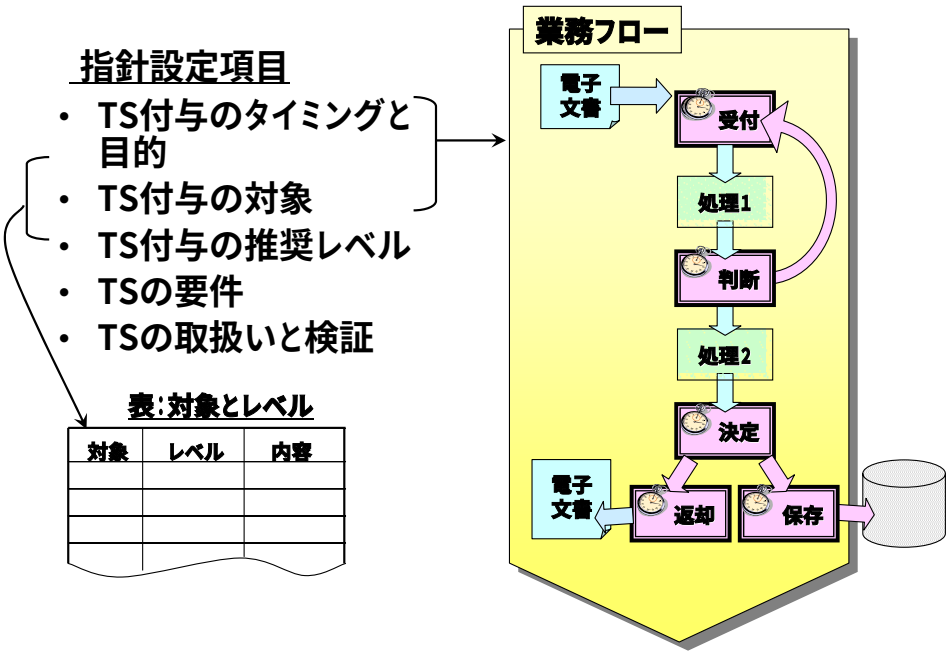

図 1-1　タイムスタンプ利用ガイドラインの枠組み

改ざん、なりすまし、事後否認によるトラブルを防止するためには、それらの文書・データが、(1) 当初どのようであったか、(2) 業務の手順上どのように変更されていったか、(3) 最終的にどのような情報として、手続きが行われたか、(4) その結果どのような通知が発行されたかなど、業務の手続きごとに案件の処理状況を確認する必要がある。それと同時に、その手順ごとに相手方との間でどのような文書･データが交わされ、しかも相互に認識したかを確認する必要がある。

ただし、全てのタイミングにおいてタイムスタンプを付与することは不経済である。そのため、対象文書・データ毎に、推奨レベルを設定することにしてある。前編に解説したようにタイムスタンプの目的は、送受信証明、文書存在証明、長期保存証明の三点である。それに即して、本ガイドラインでは、対象文書・データがそのいずれにおいてタイムスタンプを必要とするかを、強く推奨、推奨、必要に応じて、の三段階に分けて示すことにする。送受信証明のためのタイムスタンプは、システムのログと機能的に一部重複するが、各送受信の行為に対してタイムスタンプを付与するか、ログの計時精度を一定以上に高めると共に、ログファイルに対して、その非改ざん、非否認のためにタイムスタンプを付与する必要がある。

タイムスタンプの要件は文書・データ単位でなく、全体として、タイムスタンプの性能、有効期間、検証機能および利用するサービスそれぞれに関して示すことにする。

タイムスタンプの検証では、前述の目的を確実の実現するため、タイムスタンプ取得時、タイムスタンプ付き文書の受領時および保存時に検証することを規定している。

以下の各章で具体的な業務のタイムスタンプ利用指針について述べる。今回は利用例として、地方公共団体における e-Japan 構想への取り組みの代表的な業務である電子入札と電子申請を取り上げた。なお、ここでは、地方公共団体を利用者として捉えているため、実際の申請や入札を行うことになる申請者や受注者に関するタイムスタンプ利用については触れないこととする。

第２章　標準時配信・時刻監査の利用ガイドライン

２．１　サービスを導入する際の要件

本節では、標準時配信・時刻監査サービスを導入する際の要件について述べる。

（１）時刻精度

利用者は、システム間の連携やアプリケーション群の時間規制などの時刻を考慮し、システム全体の時刻精度を決定する必要がある。

（２）システム構築の選定要件

利用者は、標準時配信サービスまたは時刻監査サービスを利用したシステム構築を選定しなければならない。

以下に標準時配信サービスまたは時刻監査サービスを利用したシステム構築例を示す。

①標準時配信サービスを利用したシステム構築

時刻配信局から、時刻配信および時刻監査サービスを受ける利用者側サーバを設置する。

②時刻監査サービスを利用したシステム構築

独自に NTA からの時刻配信を利用して時刻同期する利用者側サーバを設置し、時刻監査局からの時刻監査サービスを受ける。

いずれも利用者機器に対しては、利用者側サーバから時刻配信を行う。

ここで、時刻配信のみのサービスを利用したシステムや、標準時配信サービスおよび時刻監査サービスを利用せず、独自に NTA からの時刻配信を利用して時刻同期するシステムを構築合することができるが、時刻の運用状況が第三者機関から証明されないため、本ガイドラインでは対象外とする。

（３）標準時配信サービスの選定要件

標準時配信サービスを選定する際の要件を以下に示す。

・利用者が必要かつ十分な時刻精度を有するサービスであること。
・NTA にトレーサブルなタイムソースを元に、標準時配信を行うサービスであること。
・NTA または NTA に代わる監査機関から時刻監査を受けているサービスであることが望ましい。
・時刻較正記録を提供できるサービスであること。
・うるう秒の処理をＵＴＣに同期して適性に行う手段を備えているサービスであること。
・時刻配信された利用者側サーバに対して、時刻監査を行うこと。
・時刻監査の事実や結果を示す証明書を発行するサービスであること。

・発行した時刻構成記録や証明書に関しては、時刻配信局側で必要な保管期間にわたり不正な改変や削除から保護する仕組みを持つことが望ましい。
・時刻配信局と利用者側サーバ間は、十分なセキュリティを有する回線であること。

（4）時刻監査サービスの選定要件

時刻監査サービスを選定する際の基準を以下に示す。

・利用者が必要かつ十分な時刻精度を有するサービスであること。
・NTA にトレーサブルなタイムソースを元に、時刻監査を行うサービスであること。
・NTA または NTA に代わる監査機関から時刻監査を受けているサービスであることが望ましい。
・時刻監査の事実や結果を示す証明書を発行するサービスであること。
・発行した証明書に関しては、時刻監査局側で必要な保管期間にわたり不正な改変や削除から保護する仕組みを持つことが望ましい。
・時刻監査局と利用者側サーバ間は、十分なセキュリティを有する回線であること。

（5）利用者側サーバの選定要件

利用者側サーバを選定する際の基準を以下に示す。

・利用者が必要かつ十分な時刻精度を有するサーバ機器であること。
・利用者側サーバに関しては、専用機器であることが望ましい。
・標準時配信サービスを利用する場合は、標準時配信サービスに耐えうるサーバ機器であること。
・時刻監査サービスを利用する場合は、時刻監査サービスに耐えうるサーバ機器であること。
・利用者側サーバから利用者機器に対する時刻配信機能を有すること。

2．2　サービス導入後の運用

本節では、標準時配信・時刻監査サービスを導入した後の運用について述べる。

（1）利用者側サーバの運用

利用者側サーバは、標準時配信サービスまたは時刻監査サービスによる時刻監査を 1 日 1 回以上受けなければならない。

時刻監査の事実や結果を示す証明書に関しては、必要な保管期間にわたり不正な改変や削除から保護する仕組みを持つことが望ましい。

標準時配信サービスを利用しない利用者側サーバの場合は、NTA からの時刻のトレーサビリティを確保するため、NTA からの経路および同期方法を明確にし、時刻較正ログを残す仕組みを持つことが望ましい。

（2）利用者機器の運用

利用者機器は、必要かつ十分な時刻精度を保てるように利用者側サーバと時刻同期を取らなければならない。

NTA からの時刻のトレーサビリティを確保するため、利用者側サーバからの経路および同期方式を明確にしなければならない。

第３章　入札業務における利用ガイドライン

本章では、地方公共団体の入札業務におけるタイムスタンプのタイミングおよびその目的や各々の目的に応じた要件を整理し、タイムスタンプ利用の指針を示す。

３．１　タイミングと目的

前節で示したタイムスタンプの目的に応じて、入札業務における目的、利用タイミング、対象文書等を整理した。

以下に入札業務における目的を示す。

- ✓ 送受信証明…入札書、通知書等の送受信結果の事後証明を目的に、送受信された事実を示す受領書、通知書等にタイムスタンプを付与し、非改ざん証明および事後否認防止を実現する。
  例）受領書、通知書等

- ✓ 文書存在証明…予定価格情報登録、開札執行等の入札業務上において存在時刻や実施時刻に順序性が問われる文書、また、提出等の締切が存在しその存在時刻が重要と考えられる文書にタイムスタンプを付与し、非改ざん証明および事後否認防止を実現する。
  例）予定価格情報登録、開札執行等

- ✓ 長期保存証明…電子署名の有効期間を補うことを目的に、電子署名文書にタイムスタンプを付与し、長期的に内容の非改ざん証明および電子署名付与時の検証結果を保存することにより電子署名・証明書が有効であったことを過去に遡って証明する。
  例）入札書、通知書等

これらを目的に応じた業務上のタイミングおよび目的を、平成 13 年 11 月に国土交通省より無償公開された「電子調達システム」の基本設計書等を参考に、公共工事部門の調達である「工事関係」と非公共工事部門の調達である「物品関係」に分けて、代表的な業務フローである一般競争入札方式を用いて説明する。

3．1．1　工事関係（一般競争入札方式の場合）

（1）業務フロー

工事関係の調達における業務フローを以下の図 3-1 および図 3-2 に示す。

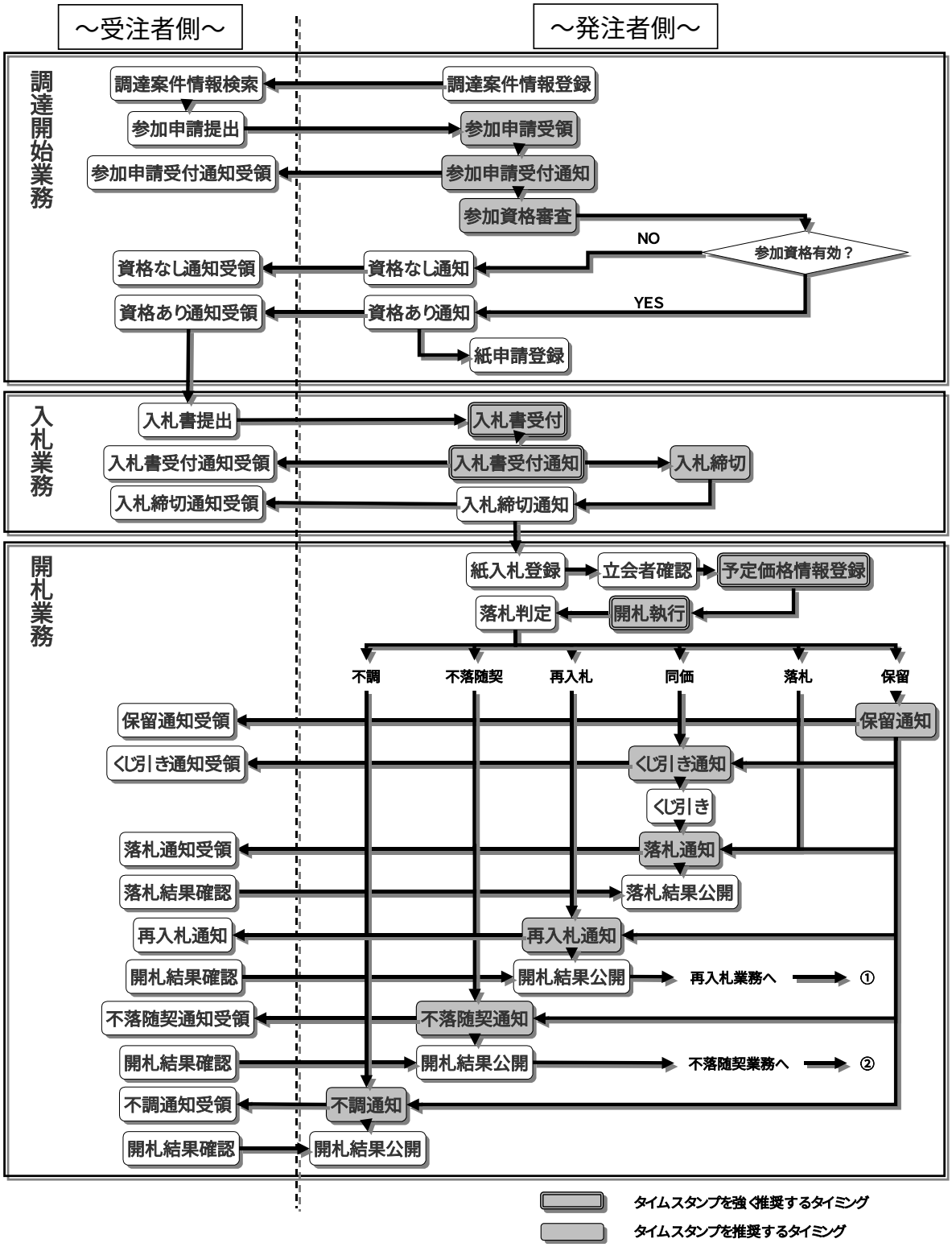

図 3-1　工事関係入札業務フローおよびタイムスタンプのタイミング（1／2）

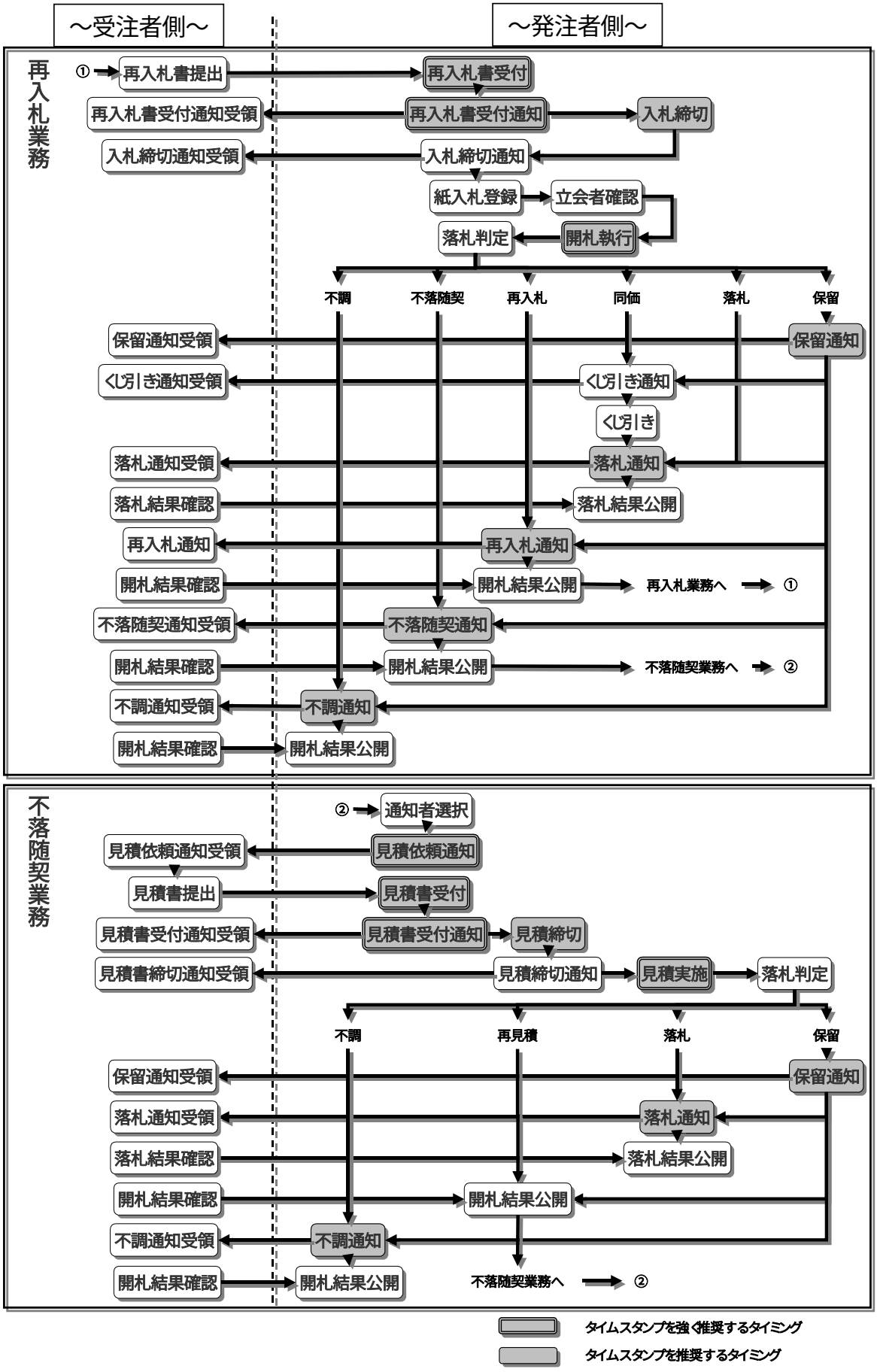

図 3-2　**工事関係入札業務フローおよびタイムスタンプのタイミング（２／２）**

（2）タイムスタンプの目的および推奨レベル

上記の業務フローにおけるタイムスタンプのタイミングに応じた目的の詳細および各々の目的に対するタイムスタンプの推奨レベルを表 5-2 に示す。

表 3-1　タイミングに応じたタイムスタンプの目的

業務種別	業務名称	対象文書名	種別/推奨レベル 送受	存在	長期	内容
調達開始業務	参加申請受領	競争参加資格確認申請書		○	○	・ 発注者が競争参加資格確認申請書を受領したタイミングにおいて、申請書等に対してタイムスタンプを付与することにより、受領した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。 ・ なお、ログへのタイムスタンプについては「5.4 内部ログのタイムスタンプ取得」を参照。
	参加申請受付通知	競争参加確認申請受付票	○			・ 発注者が競争参加資格確認申請書受付票を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
	参加資格審査			○	○	・ 発注者が申請書等から参加資格の審査を行った結果に対してタイムスタンプを付与することにより、審査した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	資格なし通知	競争参加資格確認通知書	△			・ 発注者が競争参加資格確認通知書（資格なし）を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
	資格あり通知	競争参加資格確認通知書	△			・ 発注者が競争参加資格確認通知書（資格あり）を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
入札業務	入札書受付	入札書		◎	◎	・ 発注者が入札書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が入札書を受領したタイミングにおいて、申請書等に対してタイムスタンプを付与することにより、受領した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。 ・ なお、ログへのタイムスタンプについては「5.4 内部ログのタイムスタンプ取得」を参照。
	入札書受付通知	入札書受付票	◎			・ 発注者が入札書受付票を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。

業務種別	業務名称	対象文書名	種別/推奨レベル 送受	存在	長期	内容
	入札締切			○	○	・ 発注者が入札締切日時に入札書の受付を締め切った結果に対してタイムスタンプを付与することにより、締め切った内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	入札締切通知	入札締切通知書	△			・ 発注者が入札締切通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
開札業務	予定価格情報登録			◎	◎	・ 発注者が予定価格および調査基準価格を登録した結果に対してタイムスタンプを付与することにより、予定価格として入力した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	開札執行			◎	◎	・ 発注者が入札書を開札した結果に対してタイムスタンプを付与することにより、開札結果の内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	保留通知	保留通知書	○	○	○	・ 発注者が保留通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が保留通知書を作成したタイミングにおいて、保留通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	くじ引き通知	くじ引き通知	○	○	○	・ 発注者がくじ引き通知を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者がくじ引き通知を作成したタイミングにおいて、くじ引き通知に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	落札通知	落札者決定通知書	○	○	○	・ 発注者が落札者決定通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が落札者決定通知書を作成したタイミングにおいて、落札者決定通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。

業務種別	業務名称	対象文書名	種別/推奨レベル 送受	存在	長期	内容
	再入札通知	再入札通知書	○	○	○	・ 発注者が再入札通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が再入札書を作成したタイミングにおいて、再入札通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	不落随契通知	不落随契通知	○	○	○	・ 発注者が不落随契通知を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が不落随契通知を作成したタイミングにおいて、不落随契通知に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	不調通知	取止め通知書	○	○	○	・ 発注者が取止め通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が取止め通知書を作成したタイミングにおいて、取止め通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
再入札業務	再入札書受付	再入札書		◎	◎	・ 発注者が再入札書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が再入札書を受領したタイミングにおいて、申請書等に対してタイムスタンプを付与することにより、受領した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。 ・ なお、ログへのタイムスタンプについては「5.4 内部ログのタイムスタンプ取得」を参照。
	再入札書受付通知	入札書受付票	◎			・ 発注者が再入札書受付票を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
	入札締切			○	○	・ 発注者が入札締切日時に入札書の受付を締め切った結果に対してタイムスタンプを付与することにより、締め切った内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。

業務種別	業務名称	対象文書名	種別/推奨レベル 送受	存在	長期	内容
	入札締切通知		△			・ 発注者が入札締切通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
	開札執行			◎	◎	・ 発注者が入札書を開札した結果に対してタイムスタンプを付与することにより、開札結果の内容と時刻および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	保留通知	保留通知書	○	○	○	・ 発注者が保留通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が保留通知書を作成したタイミングにおいて、保留通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	くじ引き通知	くじ引き通知	○	○	○	・ 発注者がくじ引き通知を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者がくじ引き通知を作成したタイミングにおいて、くじ引き通知に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	落札通知	落札者決定通知書	○	○	○	・ 発注者が落札者決定通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が落札者決定通知書を作成したタイミングにおいて、落札者決定通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	再入札通知	再入札通知書	○	○	○	・ 発注者が再入札書通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が再入札書を作成したタイミングにおいて、再入札通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。

業務種別	業務名称	対象文書名	種別/推奨レベル 送受	存在	長期	内容
	不落随契通知		○	○	○	・ 発注者が不落随契通知を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が不落随契通知を作成したタイミングにおいて、不落随契通知に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	不調通知	取止め通知書	○	○	○	・ 発注者が取止め通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が取止め通知書を作成したタイミングにおいて、取止め通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
不落随契業務	見積依頼通知	見積依頼通知書	◎	◎	◎	・ 発注者が見積依頼通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が見積依頼通知書を作成したタイミングにおいて、見積依頼通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。 ・ なお、ログへのタイムスタンプについては「5.4 内部ログのタイムスタンプ取得」を参照。
	見積書受付	見積書		◎	◎	・ 発注者が見積書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が見積書を受領したタイミングにおいて、見積書に対してタイムスタンプを付与することにより、受領した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	見積書受付通知	見積書受付票	◎			・ 発注者が見積書受付票を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
	見積締切			○	○	・ 発注者が見積締切日時に見積書の受付を締め切った結果に対してタイムスタンプを付与することにより、締め切った内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。

業務種別	業務名称	対象文書名	種別/推奨レベル 送受	存在	長期	内容
	見積締切通知	見積締切通知書	△			・ 発注者が見積締切通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
	見積実施			◎	◎	・ 発注者が見積書を開封した結果に対してタイムスタンプを付与することにより、見積結果の内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	保留通知	保留通知書	○	○	○	・ 発注者が保留通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が保留通知書を作成したタイミングにおいて、保留通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	落札通知	落札者決定通知書	○	○	○	・ 発注者が落札者決定通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が落札者決定通知書を作成したタイミングにおいて、落札者決定通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	不調通知	取止め通知書	○	○	○	・ 発注者が取止め通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が取止め通知書を作成したタイミングにおいて、取止め通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等のおよび付与された電子署名・証明書が有効であったことを将来的に保証することが可能。

◎…強く推奨　　送受…送受信証明
○…推奨　　存在…文書存在証明
△…必要に応じて　　長期…長期保存証明

（3）タイムスタンプ推奨レベルの判断ポイント

上記の表内に示した各推奨レベルにおける判断ポイントを各々の目的毎に以下に記述する。

- 送受信証明

◎　入札業務における時刻の保証が最も重要であると考えられる入札書受付、再入札書受付、見積書受付のタイミングにおいて、送受信証明を目的にタイムスタンプの付与を強く推奨する。

○　受注者側の事後否認防止が必要となる重要な通知書の送信タイミングにおいて、送受信証明目的にタイムスタンプの付与を推奨する。

△　上記以外の文書等における送受信についても、必要に応じてタイムスタンプを付与する。

- 文書存在証明

○　入札業務における存在時刻や実施時刻に順序性が問われる文書等の作成、または業務実施のタイミングにおいて、文書存在証明を目的にタイムスタンプの付与を強く推奨する。

○　受注者側に送信する各種通知書の作成タイミングにおいて、作成された電子文書の存在証明を目的にタイムスタンプの付与を推奨する。

- 長期保存証明

◎　入札業務における文書内容の保証が最も重要であると考えられる入札書、再入札書、見積書の受付または開封のタイミングにおいて、内容・時刻・電子署名の長期保存証明目的にタイムスタンプの付与を強く推奨する。

◎　紙入札登録､予定価格情報登録､開札執行等の手入力や目視判断された結果に対して、内容・時刻・電子署名の長期保存証明目的にタイムスタンプの付与を強く推奨する。

○　受注者側に送信する各種通知書の作成タイミングにおいて、内容・時刻・電子署名の長期保存証明目的にタイムスタンプの付与を推奨する。

3．1．2 物品関係（一般競争入札方式（総合評価）の場合）

（1）業務フロー

物品関係の調達における業務フローを以下の図 3-3、図 3-4、図 3-5 に示す。

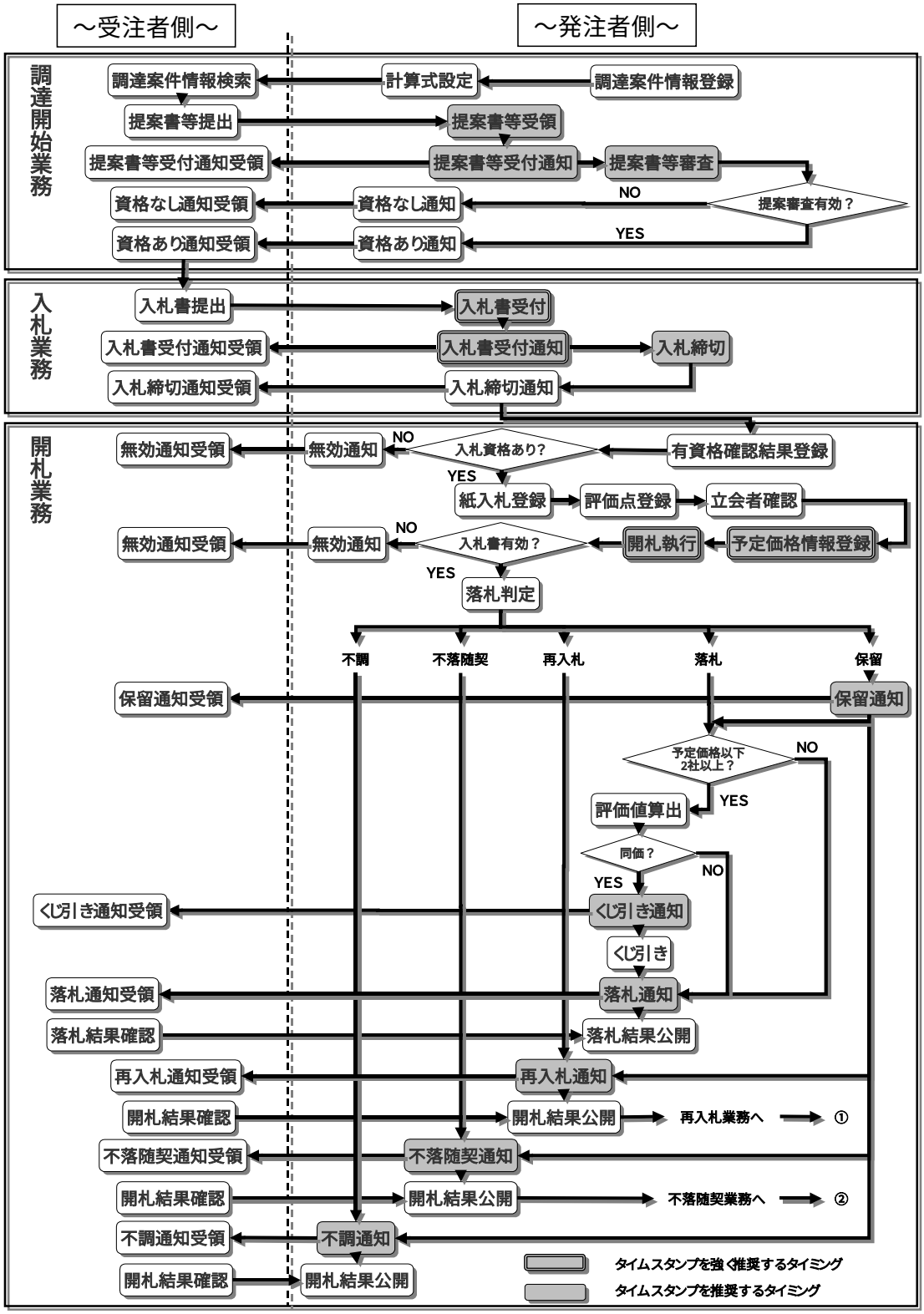

図 3-3　物品関係入札業務フローおよびタイムスタンプのタイミング（1／3）

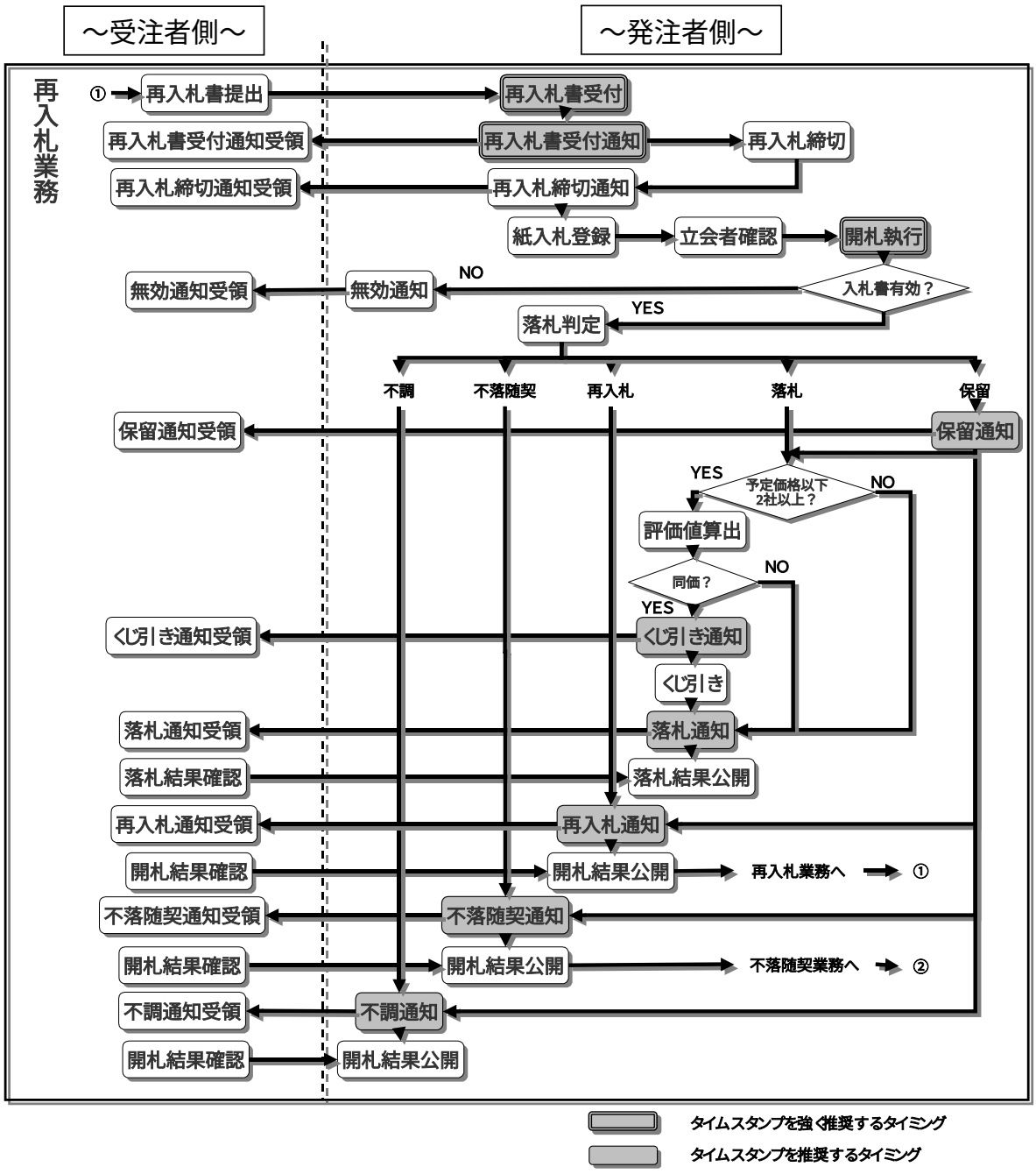

図 3-4　物品関係入札業務フローおよびタイムスタンプのタイミング（２／３）

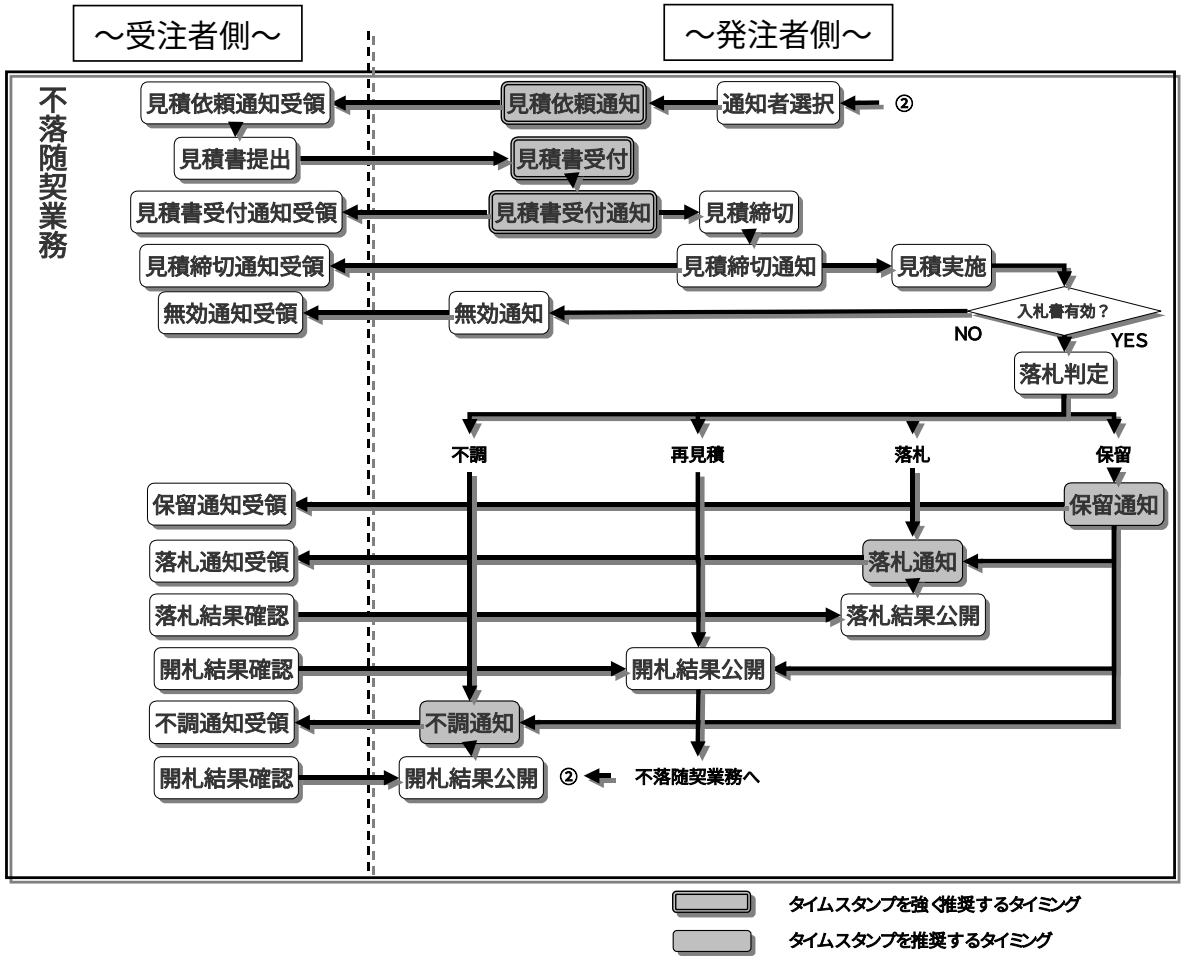

図 3-5　**物品関係入札業務フローおよびタイムスタンプのタイミング（３／３）**

（2）タイムスタンプの目的および推奨レベル

上記の業務フローにおけるタイムスタンプのタイミングに応じた目的の詳細および各々の目的に対するタイムスタンプの推奨レベルを表 3-2 に示す。

表 3-2　タイミングに応じたタイムスタンプの目的

業務種別	業務名称	対象文書名	種別/推奨レベル			内容
			送受	存在	長期	
調達開始業務	提案書等受領	提案書等		○	○	・ 発注者が提案書等を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が提案書等を受領したタイミングにおいて、申請書等に対してタイムスタンプを付与することにより、受領した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。 ・ なお、ログへのタイムスタンプについては「5.4　内部ログのタイムスタンプ取得」を参照。
	提案書等受付通知	提案書等受付票	○			・ 発注者が提案書等受付票を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
	提案書等審査			○	○	・ 発注者が申請書等から提案書等の審査を行った結果に対してタイムスタンプを付与することにより、審査した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	資格なし通知	競争参加資格確認通知書	△			・ 発注者が競争参加資格確認通知書（資格なし）を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
	資格あり通知	競争参加資格確認通知書	△			・ 発注者が競争参加資格確認通知書（資格あり）を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
入札業務	入札書受付	入札書		◎	◎	・ 発注者が入札書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が入札書を受領したタイミングにおいて、申請書等に対してタイムスタンプを付与することにより、受領した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。 ・ なお、ログへのタイムスタンプについては「5.4　内部ログのタイムスタンプ取得」を参照。
	入札書受付通知	入札書受付票	◎			・ 発注者が入札書受付票を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。

業務種別	業務名称	対象文書名	種別/推奨レベル 送受	存在	長期	内容
	入札締切			○	○	・ 発注者が入札締切日時に入札書の受付を締め切った結果に対してタイムスタンプを付与することにより、締め切った内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	入札締切通知	入札締切通知書	△			・ 発注者が入札締切通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
開札業務	予定価格情報登録			◎	◎	・ 発注者が予定価格および調査基準価格を登録した結果に対してタイムスタンプを付与することにより、予定価格として入力した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	開札執行			◎	◎	・ 発注者が入札書を開札した結果に対してタイムスタンプを付与することにより、開札結果の内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	保留通知	保留通知書	○	○	○	・ 発注者が保留通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が保留通知書を作成したタイミングにおいて、保留通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	くじ引き通知	くじ引き通知	○	○	○	・ 発注者がくじ引き通知を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者がくじ引き通知を作成したタイミングにおいて、くじ引き通知に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	落札通知	落札者決定通知書	○	○	○	・ 発注者が落札者決定通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が落札者決定通知書を作成したタイミングにおいて、落札者決定通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。

業務種別	業務名称	対象文書名	種別/推奨レベル			内容
			送受	存在	長期	
	再入札通知	再入札通知書	○	○	○	・ 発注者が再入札書通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が再入札書を作成したタイミングにおいて、再入札通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	不落随契通知	不落随契通知	○	○	○	・ 発注者が不落随契通知を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が不落随契通知を作成したタイミングにおいて、不落随契通知に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	不調通知	取止め通知書	○	○	○	・ 発注者が取止め通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が取止め通知書を作成したタイミングにおいて、取止め通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
再入札業務	再入札書受付	再入札書		◎	◎	・ 発注者が再入札書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が再入札書を受領したタイミングにおいて、申請書等に対してタイムスタンプを付与することにより、受領した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。 ・ なお、ログへのタイムスタンプについては「5.4　内部ログのタイムスタンプ取得」を参照。
	再入札書受付通知	再入札書受付票	◎			・ 発注者が再入札書受付票を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
	再入札締切			○	○	・ 発注者が再入札締切日時に再入札書の受付を締め切った結果に対してタイムスタンプを付与することにより、締め切った内容と時刻および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。

業務種別	業務名称	対象文書名	種別/推奨レベル 送受	存在	長期	内容
	再入札締切通知	再入札締切通知書	△			・ 発注者が再入札締切通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、受領した事実と時刻を保証することが可能。
	開札執行			◎	◎	・ 発注者が入札書を開札した結果に対してタイムスタンプを付与することにより、開札結果の内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	保留通知	保留通知書	○	○	○	・ 発注者が保留通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が保留通知書を作成したタイミングにおいて、保留通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	くじ引き通知	くじ引き通知	○	○	○	・ 発注者がくじ引き通知を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者がくじ引き通知を作成したタイミングにおいて、くじ引き通知に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	落札通知	落札者決定通知書	○	○	○	・ 発注者が落札者決定通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が落札者決定通知書を作成したタイミングにおいて、落札者決定通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の通知および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	再入札通知	再入札書通知書	○	○	○	・ 発注者が再入札書通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が再入札書を作成したタイミングにおいて、再入札通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。

業務種別	業務名称	対象文書名	種別/推奨レベル 送受	存在	長期	内容
	不落随契通知	不落随契通知	○	○	○	・ 発注者が不落随契通知を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が不落随契通知を作成したタイミングにおいて、不落随契通知に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	不調通知	取止め通知書	○	○	○	・ 発注者が取止め通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が取止め通知書を作成したタイミングにおいて、取止め通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
不落随契業務	見積依頼通知	見積依頼通知書	◎	◎	◎	・ 発注者が見積依頼通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が見積依頼通知書を作成したタイミングにおいて、見積依頼通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	見積書受付	見積書		◎	◎	・ 発注者が見積書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が見積書を受領したタイミングにおいて、見積書に対してタイムスタンプを付与することにより、受領した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。 ・ なお、ログへのタイムスタンプについては「5.4　内部ログのタイムスタンプ取得」を参照。
	見積書受付通知	見積書受付票	◎			・ 発注者が見積書受付票を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
	見積締切			○	○	・ 発注者が見積締切日時に見積書の受付を締め切った結果に対してタイムスタンプを付与することにより、締め切った内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。

業務種別	業務名称	対象文書名	種別/推奨レベル 送受	存在	長期	内容
	見積締切通知	見積締切通知書	△			・ 発注者が見積締切通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。
	見積実施			◎	◎	・ 発注者が見積書を開封した結果に対してタイムスタンプを付与することにより、見積結果の内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	保留通知	保留通知書	○	○	○	・ 発注者が保留通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が保留通知書を作成したタイミングにおいて、保留通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	落札通知	落札者決定通知書	○	○	○	・ 発注者が落札者決定通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が落札者決定通知書を作成したタイミングにおいて、落札者決定通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。
	不調通知	取止め通知書	○	○	○	・ 発注者が取止め通知書を送信したタイミングにおいて、当該文書に対してタイムスタンプを付与することにより、送信した事実と時刻を保証することが可能。 ・ 発注者が取止め通知書を作成したタイミングにおいて、取止め通知書に対してタイムスタンプを付与することにより、作成した内容と時刻等の事実および付与された電子署名・証明書が有効であったことを将来的に保証することが可能。

◎…強く推奨　　送受…送受信証明
○…推奨　　存在…文書存在証明
△…必要に応じて　　長期…長期保存証明

（3）タイムスタンプ推奨レベルの判断ポイント

上記の表内に示した各推奨レベルにおける判断ポイントを各々の目的毎に以下に記述する。

- 送受信証明

◎　入札業務における時刻の保証が最も重要であると考えられる入札書受付、再入札書受付、見積書受付のタイミングにおいて、送受信証明を目的にタイムスタンプの付与を強く推奨する。

○　受注者側の事後否認防止が必要となる重要な通知書の送信タイミングにおいて、送受信証明目的にタイムスタンプの付与を推奨する。

△　上記以外の文書等における送受信についても、必要に応じてタイムスタンプを付与する。

- 文書存在証明

◎　入札業務における存在時刻や実施時刻に順序性が問われる文書等の作成、または業務実施のタイミングにおいて、文書存在証明を目的にタイムスタンプの付与を強く推奨する。

○　受注者側に送信する各種通知書の作成タイミングにおいて、作成された電子文書の存在証明を目的にタイムスタンプの付与を推奨する。

- 長期保存証明

◎　入札業務における文書内容の保証が最も重要であると考えられる入札書、再入札書、見積書の受付または開封のタイミングにおいて、内容・時刻・電子署名の長期保存証明目的にタイムスタンプの付与を強く推奨する。

◎　紙入札登録､予定価格情報登録､開札執行等の手入力や目視判断された結果に対して、内容・時刻・電子署名の長期保存証明目的にタイムスタンプの付与を強く推奨する。

○　受注者側に送信する各種通知書の作成タイミングにおいて、内容・時刻・電子署名の長期保存証明目的にタイムスタンプの付与を推奨する。

３．２　タイムスタンプの要件

（１）性能に関する要件

タイムスタンプの性能に関し、表 3-3 の要件を満たすこと。なお、入札業務の求める範囲については、各発注者の入札業務におけるピーク件数（ex.件数/日）に仕様として定めるタイムスタンプ数や想定オンライン化率等を考慮し算出することとする。

表 3-3　タイムスタンプの性能に関する要件

要件	送受信証明	文書存在証明	長期保存証明
タイムスタンプに含まれる時刻精度	±3 秒以内	±3 秒以内	±3 秒以内
入札業務の求める範囲でタイムスタンプの付与が可能なこと	○	○	○

※表内に示した時刻精度とは、TSA 側でのタイムスタンプ付与時の精度であり、業務システムと TSA 間ネットワークによる誤差は考慮していない

（２）タイムスタンプの有効期間に関する要件

タイムスタンプの付与にあたり、表 3-4 に定める有効期間に関する要件を満たすタイムスタンプを採用すること。目的毎に必要となる有効期間の要件が違うため、必要に応じて採用するタイムスタンプを使い分けることも可能とする。

表 3-4　タイムスタンプの有効期間に関する要件

要件	送受信証明	文書存在証明	長期保存証明
タイムスタンプの有効期間	3 年以上	5 年以上	10 年以上

上記に定める期間は一般的な入札業務において必要となる最低限を想定しており、これ以上に各発注者側における文書管理規定等の規程類で対象文書の保存期間が長期に定めているものについては、それらの規程に従うこと。また、調達金額に応じて保存期間が定められている場合は、調達金額毎にサービスを使い分けるのではなく、規程類により定められている有効期間の最大値を用いることが望ましい。

以下、表 3-5 に文書管理規定による保存期間の例を示す。

表 3-5　文書管理規程による保存期間の例（東京都の場合）

区分	保存年限
請負又は委託による事業に関するもの	
予定価格が 9 億円以上の工事又は製造の請負に関するもの	10 年
予定価格が 1 億円以上の請負又は委託により行う工事、船舶の製造、修繕、通信および運搬にかかわる役務の提供に関するもの	5 年
予定価格が 1 億円未満の請負又は委託により行う工事、船舶の製造、修繕、通信および運搬にかかわる役務の提供に関するもの	3 年
物件の買入れ等に関するもの	
予定価格が 2 億円以上の不動産若しくは動産の買入れ若しくは売払い又は不動産の信託の受益権の買入れ若しくは売払いに関するもの	10 年
予定価格が 6 千万円以上の物件の買入れ、売払い、借入れおよび貸付けに関するもの	5 年
予定価格が 6 千万円未満の物件の買入れ、売払い、借入れおよび貸付けに関するもの	3 年

なお、上記の有効期間を満たさないタイムスタンプを利用する場合は、新たに発行されたタイムスタンプを付与する等の方法により、有効期間を延長することも可能であるが、その場合は発注者側で確実に実施できる仕組み、体制を整備する必要がある。

このような更新という煩雑な業務からの解放し、更新ミスによるリスク回避の観点から、タイムスタンプは技術的に１０年以上の有効期限を保証できるものを採用することが望ましい。なお、技術動向等により採用が困難な場合は、有効期間を延長する仕組み、体制を十分に整備し、確実に実施することとする。

（３）検証機能に関する要件

入札業務を実施するにあたり、必要となるタイミングおよび方法で検証可能なサービスを採用すること。また、検証対象者は発注者のみならず、受注者も対象とすることとし、両者が容易かつ経済的に検証可能な環境を提供するサービスを用いることが望ましい。

（４）利用するサービスに関する要件

利用するタイムスタンプのサービスに関し、表 3-6 の要件を満たすこと。なお、下表を満たした場合においても、信頼のおける第三者機関の提供するサービスを利用することが望ましい。

表 3-6　利用するサービスに関する要件

要件	送受信証明	文書存在証明	長期保存証明
ガイドラインで定めるタイムスタンプ発行サービスの技術基準および運用基準を満たしていること	○	○	○
ガイドラインで定めるタイムスタンプ検証サービスの技術基準および運用基準を満たしていること	○	○	○

また、ガイドラインで定める各サービスの基準については、「第Ⅲ編 第１章１．２　タイムスタンプ発行サービス」および「第Ⅲ編 第１章１．３　タイムスタンプ検証サービス」の「シンプルプロトコル」と「リンキングプロトコル」それぞれの技術基準と運用基準を参照すること。

３．３　取得タイムスタンプの取扱いと検証

入札業務における入札書等文書に対するタイムスタンプを取得しただけでは当該文書の各目的に応じた証明を実現するには不十分である。タイムスタンプを付与した文書のライフサイクルに応じ、タイムスタンプの検証作業を適正に行うことにより、タイムスタンプを付与した文書の送受信、文書存在、長期保存等の証明を確実に実現することが可能となる。

入札業務におけるタイムスタンプの検証タイミングを以下に示す。なお、これらのタイミングはあくまでも実施すべきタイミングであり、業務上の必要性、システムへの負荷、コスト等を踏まえ、実施する頻度等を十分に検討することが望ましい。

（１）タイムスタンプ取得時の検証

タイムスタンプの取得後直ちにタイムスタンプトークンの内容確認、タイムスタンプの署名検証およびタイムスタンプの公開鍵証明書の検証（PKI の技術を利用したものの場合）を行うことが望ましい。

なお、タイムスタンプトークンの内容確認には、タイムスタンプトークンが作成された時刻の妥当性確認やタイムスタンプポリシー等のタイムスタンプ情報(TSTInfo)が申請した内容に対応しているか等の確認が含まれることとする。

（２）タイムスタンプ付き文書受領時の検証

タイムスタンプが付与された文書を受領し、そのタイムスタンプの時刻を利用して業務処理を実施する必要がある場合において、当該業務処理の実施前にそのタイムスタンプを検証することが望ましい。

なお、タイムスタンプの対象が電子署名付き文書である場合は、その電子署名の検証と公開鍵証明書の検証も同時に実施することが望ましい。

（３）タイムスタンプ付き文書保存時の検証

タイムスタンプが付与された文書を保存するにあたり、保存前にタイムスタンプの検証を実施することが望ましい。

なお、タイムスタンプの付与対象となる文書とタイムスタンプの対応が明確になる形式での保管を実現し、更に当該文書の改ざんが困難なセキュアな環境で保管することが望ましい。

第４章　申請業務における利用ガイドライン

本項では、地方公共団体の申請業務におけるタイムスタンプのタイミングおよびその目的や各々の目的に応じた要件を整理し、指針を示す。

４．１　タイミングと目的

（１）タイムスタンプの目的および推奨レベル

紙の申請書には申請者の押印（または直筆署名）・申請日付、受付日付（および受付担当印）が記入または捺印され、申請書の審査過程においても担当者や責任者の署名（又は印）および処理日付が記入または捺印される。また、申請の受理通知や結果の通知、発行される許認可等の公文書にもしかるべき署名や日付の記入および公印の捺印が行われる。

これらの署名や捺印は誰がその行為を行ったかをあらわし、署名および捺印された文書の真正性を証明するものである。記入された日付はその行為および存在の確定日を表わす。

電子申請においては直筆署名や捺印に代わるものとして電子署名を用い、その電子署名が表明する行為の確定日付として電子的に検証可能なタイムスタンプが使用される。電子申請業務の多くの場面においてタイムスタンプを利用することで、電子申請業務の信頼性・安全性を高めることが可能である。

電子申請業務におけるタイムスタンプの目的は以下の三つに大別される。

- ✓ 送受信証明･･･申請書､届出書等の送受信結果の事後証明を目的に送受信された事実を示す通知書および受領書等にタイムスタンプを付与し、改ざん検知および事後否認防止を実現する。
- ✓ 文書存在証明･･･申請書様式、手数料等の納付情報、申請書および添付資料、通知書/公文書等の申請・届出業務において、作成・修正や実施した時刻に順序性が問われる文書、また、申請・届出に締切が存在することから、そのときの時刻が重要と考えられる文書にタイムスタンプを付与し、改ざん検知および事後否認防止を実現する。
- ✓ 長期保存証明･･･電子署名の有効期間を補うことを目的に､電子署名文書にタイムスタンプを付与し、長期的に内容の改ざん検知を実現するとともに電子署名付与時の電子署名・証明書が有効であったことを過去に遡って証明する。

実際にタイムスタンプを電子申請業務に適用するにあたって､「地方公共団体における申請・届出等手続きに関する汎用受付システムの基本仕様（平成 14 年 3 月 27 日　自治事務等オンライン化推進関係省庁連絡会議編）」の申請・届出システムの地方公共団体側利用者向け機能要件を参考に説明する。申請業務のフローとタイムスタンプのタイミングを図 4-1 に示し、タイムスタンプの目的を表 4-1 において説明する。

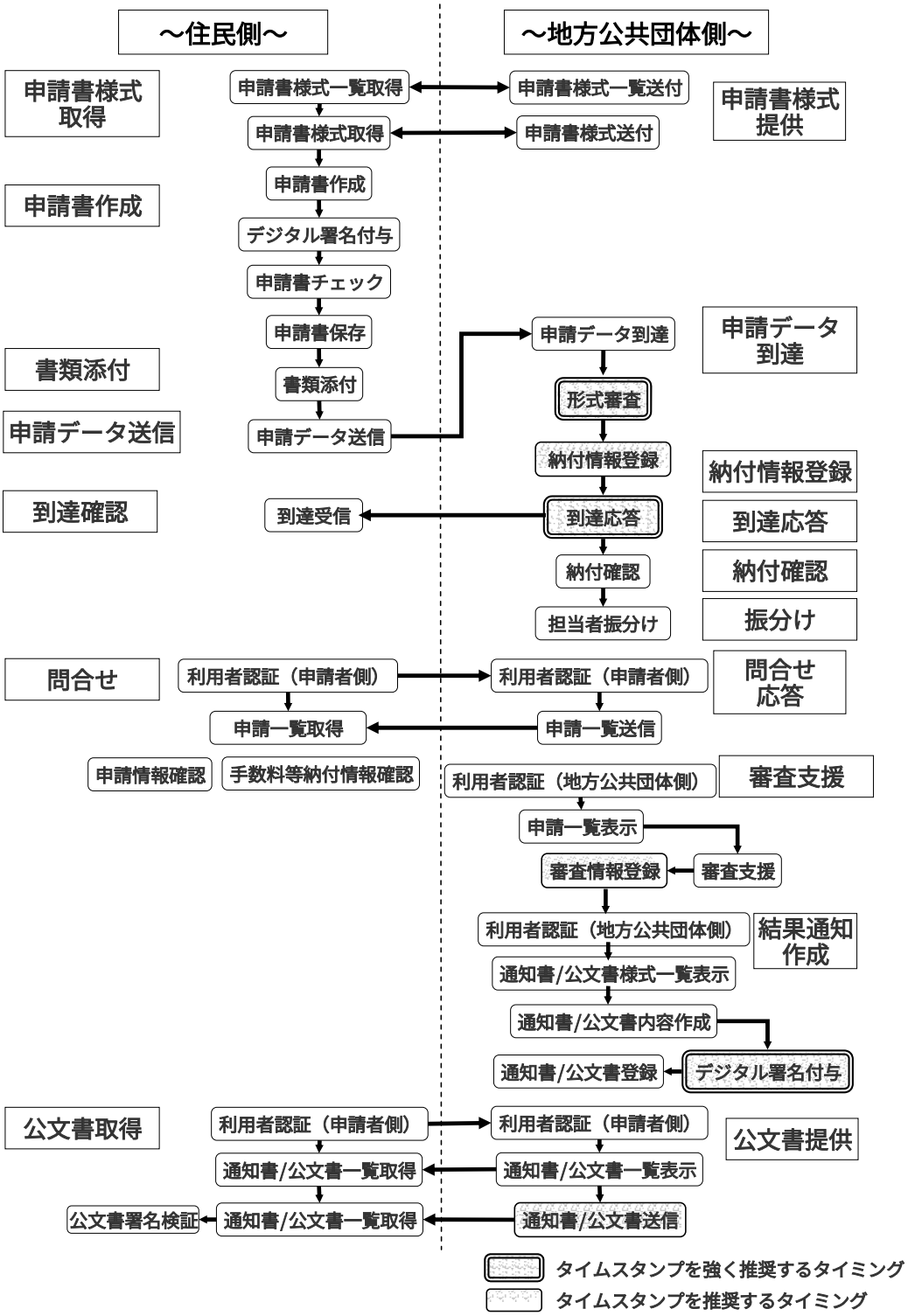

図 4-1　申請業務フローおよびタイムスタンプのタイミング

表 4-1　申請業務におけるタイムスタンプの目的

項番	機能項目	機能名称	対象文書名	種別/推奨レベル			内　　容
				送受	存在	長期	
1	申請書様式提供	申請書様式一覧送付	申請様式一覧		△	△	･申請書一覧に対して定期的なタイムスタンプと更新時のタイムスタンプの付与で申請書一覧が存在していた事実を保証することが可能。
		申請書様式送付	申請書様式		△	△	･申請書様式に対して定期的なタイムスタンプと更新時のタイムスタンプの付与で申請書様式が存在していた事実を保証することが可能。
2	申請データ到達	申請データ到達	受付ログ等		△	△	・第５章ログの管理参照。
		形式審査	申請書および添付資料等	◎	◎	◎	･地方公共団体側が申請書および添付資料等を受領したタイミングで申請書および添付資料等に対してタイムスタンプを付与することで受領した内容と時刻等の事実および付与された電子署名･証明書が有効であったことを将来的に保証することが可能。
3	納付情報登録	納付情報登録	納付情報		○	○	・受領時に手数料等が確定する場合、手数料等確定時に手数料等の納付情報にタイムスタンプを付与することで確定事実と内容を保証することが可能。
4	到達応答	到達応答	申請データ到達情報	◎			･申請データ到達の結果として申請書の到達、受付番号、不備の有無等を申請者へ送信するタイミングで当該情報にタイムスタンプを付与することで応答事実と内容を保証することが可能。

表 4-1　申請業務におけるタイムスタンプの目的（続き）

項番	機能項目	機能名称	対象文書名	種別/推奨レベル			内　　容
				送受	存在	長期	
5	納付確認	納付確認					
6	振分け	担当者振分け					
7	問合せ応答	利用者認証（申請者側）	受付ログ		△	△	・第５章ログの管理参照。
		申請一覧送信（処理状況一覧送付）					
8	審査支援	利用者認証（地方公共団体側）					
		申請一覧表示					
		審査支援					
		審査情報登録	審査情報		○	○	・不備等の指示の情報を入力したタイミングで担当者識別情報と当該指示等情報にタイムスタンプを付与することで情報の履歴を保証することが可能。
9	結果通知作成	利用者認証（地方公共団体側）					
		通知書/公文書様式一覧表示					
		通知書/公文書内容作成					
		電子署名付与	通知書		○	○	・通知書／公文書に電子署名されたタイミングでタイムスタンプを付与することで通知書／公文書がその時刻に生成されていたことを保証することが可能。
			公文書		◎	◎	
		通知書/公文書登録					

表 4-1　申請業務におけるタイムスタンプの目的（続き）

項番	機能項目	機能名称	対象文書名	種別/推奨レベル			内容
				送受	存在	長期	
10	公文書提供	利用者認証（地方公共団体側）	受付ログ		△	△	・第５章ログの管理参照。
		通知書/公文書一覧表示					
		通知書/公文書送信	通知書	△			・申請者が選択した通知書/公文書を送信したタイミングで通知書/公文書にタイムスタンプを付与することで当該情報を発信した事実を保証することが可能。
			公文書	○			

◎･･･強く推奨　　送受･･･送受信証明
○･･･推奨　　存在･･･文書存在証明
△･･･必要に応じて　　長期･･･長期保存証明
空白･･不要

（2）タイムスタンプ推奨レベルの判断ポイント

前記の表内に示した各推奨レベルにおける判断ポイントを各々の目的毎に以下に記述する。

・送受信証明

◎　申請・届出業務において、申請書および添付資料を受領したタイミング（形式審査時）において、送受信証明を目的にタイムスタンプの付与を強く推奨する。

◎　申請・届出業務において、申請書および添付資料を受理したタイミング（到達確認通知送信時）において、到達確認証明目的にタイムスタンプの付与を強く推奨する。

○　公文書の提供において、到達確認証明目的にタイムスタンプの付与を推奨する。

△　通知書等の提供においても、必要に応じてタイムスタンプを付与する。

・文書存在証明

◎　申請・届出業務において、存在した時刻や実施した時刻が問われる文書等の作成、または業務実施のタイミングにおいて、文書存在証明を目的にタイムスタンプの付与を強く推奨する。

◎　申請者側に送信する公文書の作成タイミングにおいて、作成された公文書の存在証明を目的にタイムスタンプの付与を強く推奨する。

○　申請者側に送信する通知書の作成タイミングにおいて、作成された通知書の存在証明を目的にタイムスタンプの付与を推奨する。

△　申請様式提供において、作成された電子文書の存在証明を目的に必要に応じてタイムスタンプを付与する。

・長期保存証明

◎　申請・届出業務において、申請書および添付資料を受領したタイミングにおいて、内容・時刻・電子署名の長期保存証明目的にタイムスタンプの付与を強く推奨する。

◎　申請者に送信する公文書の作成時に、内容・時刻・電子署名の長期保存証明目的にタイムスタンプの付与を強く推奨する。

○　申請者に送信する通知書の作成時に、内容・時刻・電子署名の長期保存証明目的にタイムスタンプの付与を推奨する。

○　審査情報を登録するタイミングにおいて、内容・時刻・電子署名の長期保存証明目的にタイムスタンプの付与を推奨する。

△　なお、送受信結果が判別可能なアプリケーションログ、問い合わせ応答、および送信ログ等に一定周期で包括的にタイムスタンプを付与することが望ましい。

４．２　タイムスタンプの要件

（１）性能に関する要件

タイムスタンプの性能に関し、表 4-2 の要件を満たすこと。なお、申請・届出業務の求める範囲については、申請・届出業務におけるピーク件数（ex.件数／時）に仕様として定めるタイムスタンプ数や想定オンライン稼働率等を考慮して算出することとする。

表 4-2　タイムスタンプの性能に関する要件

要件	送受信証明	文書存在証明	長期保存証明
タイムスタンプに含まれる時刻精度	±3 秒以内	±3 秒以内	±3 秒以内
申請・届出業務の求める範囲でタイムスタンプの付与が可能なこと	○	○	○

（2）有効期間に関する要件

タイムスタンプの有効期間に関し、表 4-3 に示す文書保存期間を満たすこと。なお、表 4-3 に示す期間はタイムビジネス推進協議会が独自に定めた最低限の期間であり、業務上これ以上必要であれば、各地方公共団体が独自に判断して必要な期間を採用することができる。

表 4-3　文書保存期間の例

文書	送受信証明	文書存在証明	長期保存証明
許認可等をするための決裁文書であって、当該許認可等の効果が 10 年間存続するもの（有効期間が 10 年以上の許認可等をするための決裁文書）	1 年以上	10 年以上	許認可等の有効期間以上
許認可等をするための決裁文書であって、当該許認可の効果が 5 年間存続するもの（有効期間が 5 年以上 10 年未満の許認可等をするための決裁文書）	1 年以上	5 年以上	10 年以上
許認可等をするための決裁文書であって、当該許認可の効果が 3 年間存続するもの（有効期間が 3 年以上 5 年未満の許認可等をするための決裁文書）	1 年以上	3 年以上	5 年以上
許認可等をするための決裁文書（有効期間が 1 年以上 3 年未満の許認可等をするための決裁文書）	1 年以上	1 年以上	3 年以上

※　上記は「行政文書の管理方策に関するガイドラインについて（平成 12 年 2 月 25 日各省庁事務連絡会議申合せ）」を参考に、各目的に応じた期間をタイムビジネス推進協議会が独自に定めた。

（3）検証機能に関する要件

対象となる業務に適した検証方法を使用できること。

タイムスタンプは業務上、必要に応じて検証が行われる。タイムスタンプの検証方法には、タイムスタンプ取得者や検証者が自身で行える方法と、タイムスタンプ事業者や専門の検証事業者に依頼して行う方法がある。検証の容易性や検証にかかる時間（ターンアラウンドタイム）・費用、および検証システムの維持の容易性や維持費用等について検討を行い、適用する用途に適した検証方法を使用することとする。特に申請者や第三者がタイムスタンプの検証を行う場合について十分に検討することが望ましい。

４．３　取得タイムスタンプの取扱いと検証

タイムスタンプを取得しただけではタイムスタンプを付与した文書の信頼性を保証することはできない。タイムスタンプを付与した文書のライフサイクルにおいて、タイムスタンプの検証作業を適正に行うことで、タイムスタンプを付与した文書の信頼性は保たれる。タイムスタンプの検証を行うことが望ましい主なタイミングを以下に示す。

（１）タイムスタンプ取得時の検証

タイムスタンプを取得したら直ちに、タイムスタンプトークンの検証を行うことが望ましい。タイムスタンプトークンの検証には、タイムスタンプトークンが作成された時刻の妥当性の確認や、タイムスタンプポリシー等のタイムスタンプ情報(TSTInfo)が申請した内容に対応しているか等の確認が含まれる。なお、PKI の技術を利用したタイムスタンプの場合は、タイムスタンプの署名検証およびタイムスタンプの公開鍵証明書の有効性検証も行うことが望ましい。

（２）タイムスタンプ付き文書受領時の検証

タイムスタンプ付き文書を受け取り、そのタイムスタンプの時刻を利用して処理を行う場合は、処理を行う前にそのタイムスタンプを検証すべきである。

タイムスタンプの対象が電子署名である場合は、その電子署名の検証と公開鍵証明書の検証も行うべきである。

（３）タイムスタンプ付き文書保存時の検証

タイムスタンプが付与された文書を保存する場合には、タイムスタンプの検証後に保存することが望ましい。また、タイムスタンプの付与対象の文書とタイムスタンプの対応が管理できる様式で保存することが望ましい。

第５章　ログの管理

ログとは、情報システムにおける事象を収集、保管し、後日事象を確認するために利用する情報である。一般にはイベントログと監査ログとに分類する。イベントログは、ソフトウェアなどの動作を確認するために収集する。監査ログは、監査のためのログであり、監査すべき点においてあるべき動作を行っているかを確認するために収集する。

５．１　ログのセキュリティ

システムログに関しては、一般的なログの正当性を確保するために、時刻に関して以下の対策を講じることが望ましい。

・　マシンの時刻を TA と同期を取る。

一方、監査ログは、セキュリティ機能を提供するシステムにおいては、後日の不正な動作を確認するための唯一の情報であるから、その信憑性を保つ必要がある。具体的には、監査ログに対する不正アクセスを防ぐ､監査ログをバイパスしない､破壊しない等のシステム構造上の対策と、内容の正当性を確保することである。

監査ログの内容の正当性を確保するためには、以下の手段を用いる。

・　ログファイルを構成する各ログレコードの内容が改ざんされない

・　ログレコードの順序性が保障されている。（順序とともに、抜けもない）

この正当性を確保するために、ログレコードへのタイムスタンプの付与と、ログファイルへのタイムスタンプの付与が効果的である。

（１）ログの保護

ログには、リアルタイムの改ざん検知と改ざん防止対策を施す。また、ログファイルの削除に対しても対抗可能とする。

（２）ログのタイムスタンプ取得

ログレコードおよびファイルには、第三者機関によるシンプルプロトコルまたは、リンキングプロトコルを用いたタイムスタンプを取得し、存在証明を可能とする。

タイムスタンプ取得は、管理業務プロセス上で遺失や、変更、改ざんなどが行われていないことを証明するために、次のタイミングで行うことが望ましい。

(a) ログレコード採取のタイミング

(b) ファイルのローテーションタイミング

(c) ログホストまたは、他の計算機に転送するタイミング

(d) 外部記録媒体や保管用ストレージにアーカイブするタイミング

(e) 分析、監査など、タイムスタンプの検証を行うタイミング

（３）ログの収集

ログの収集は、システムの一機能とし、システムの起動時から終了時までのすべての稼働履歴をログに記録して収集する。

（４）ログの保存期間

ログのタイムスタンプは、業務に伴う文書の保存規定と同等または、それ以上の必要期間有効にし、保存するものとする。また、システム管理規定により、ログの保存期間が定められている場合も同等にタイムスタンプを有効にし、保存する。

（５）ログの分析調査

サービスシステムが正常に稼働しているかどうかの現状を把握するために、ログの出力や取得状況、ログ情報に記録されている内容に関する分析調査を、日次または週次で行うことが望ましい。

（６）ログの監査

ログの取得方法、管理状況と共に、監査ログの内容に関して定期的なログ監査を行う。このうち、外部監査は、業務運用と無関係のものが行うものとする。

５．２　ログに記録する情報

セキュリティに関する重要な事象を対象に、システムログ、アクセスログは監査に使用するための要件を確保し、監査ログとして記録する。

監査ログには、次の情報を含むものとする。

(a)　事象の種類
(b)　事象が発生した日付および時刻
(c)　各種処理の結果
(d)　事象の発生元の識別情報（操作員名、システム名等）
(e)　タイムスタンプによる存在証明

第III編　提供ガイドライン

第１章　技術基準

１．１　標準時配信・時刻監査サービス

標準時配信サービスとは、NTA に代わって標準時を配信するサービスを言い、標準時配信サービスを行う機関を標準時配信局（TA）と呼ぶ。また、標準時監査サービスとは、NTA に代わって利用者側サーバの時刻を監査するサービスを言い、時刻監査サービスを行う機関を時刻監査局（TAA）と呼ぶ。

本ガイドラインでは、利用者側サーバ（タイムスタンプ局（TSA）を含む）に標準時を配信するサービスと、利用者側サーバ（タイムスタンプ局（TSA）を含む）の時刻を監査するサービスを対象とし、標準時配信局および時刻監査局が、標準時配信サービスおよび時刻監査サービスを行う上で必要とされる基準について述べる。

（１）標準時配信局および時刻監査局の時計

標準時配信局および時刻監査局は、十分な精度を持った時刻で標準時配信サービスおよび時刻監査サービスを運用しなければならない。

- 必要とされる配信および監査の時刻精度の目安　：　±300 ミリ秒　程度
- 上記配信時刻精度を実現するために、標準時配信局および時刻監査局は、時刻配信サービスおよび時刻監査サービスを使用するのに必要かつ十分な精度を有した時計を使用しなければならない。
- 標準時配信局および時刻監査局は、標準時配信サービスおよび時刻監査サービスに使用する時計の時刻を NTA の提供する UTC に対して必要かつ十分な精度で同期できる手段を備えなければならない。
- うるう秒の処理を UTC に同期して適性に行う手段を備えなければならない。

（２）NTA からの時刻監査

標準時配信局および時刻監査局は、標準時時刻配信サービスおよび時刻監査サービスに使用する時計の時刻監査をＮＴＡから受けることが望ましい。

- 必要とされる時刻監査制度の目安　：　±30 ミリ秒　程度（NTA-TA 間）
- NTA による時刻監査は、標準時時刻配信サービスおよび時刻監査サービスに必要かつ十分な監査制度が確保される方法で実施されることが望ましい。
- 時刻監査の事実や結果を示す証明書を NTA より受け取る仕組みを持つことが望ましい。
- NTA から受け取った時刻監査の証明書を、必要な保管期間にわたり不正な改変や削除から保護する仕組みを持つことが望ましい。

（３）時刻の完全性

標準時配信局および時刻監査局が運用する時刻は、UTC に対して所定の精度内にあること

を保証しなければならない。

・標準時配信局および時刻監査局が運用する時刻の精度が所定の規格から外れた場合に、検出できる手段を持たなければならない。

・時刻の完全性を維持するための操作記録を残す仕組みを持たなければならない。

（４）利用者側サーバの時刻監査

標準時配信局および時刻監査局が、利用者側サーバの時刻を監査する場合、利用者側サーバの時刻が正確に運用されているかを監査すること。

・利用者側サーバの時計の時刻を必要かつ十分な精度で監査できる手段を持つこと。

・時刻監査の頻度は、１日１回以上実施すること。

・監査した結果は、時刻運用の重要な証拠となるため、後日においても検証可能な様式で保管できる機能を有すること。

・保管した監査結果が改ざんされない、もしくは改ざんが検出可能な機能を備えること。

以下の各項目では、特に標準時配信局が、タイムスタンプ局（TSA）に標準時配信サービスを行う上で必要とされる基準について述べる。

（５）TSA の特定（認証）

標準時配信局は、タイムスタンプサーバに時刻を配信またはタイムスタンプサーバの時刻を監視する場合には、タイムスタンプサーバを特定すること。

・標準時配信局は、標準時配信サービスを提供するＴＳＡの使用するタイムスタンプサーバを特定する手段を有し、タイムスタンプサーバとの通信においてタイムスタンプサーバのなりすましができないような手段を持たなければならない。

・タイムスタンプサーバを特定する手段としてＰＫＩを利用した相互認証の技術を導入することが望ましい。

（６）TSA への標準時配信

標準時配信局は、ＴＳＡの使用するタイムスタンプサーバに対して、正確な時刻を安全に配信すること。

・タイムスタンプサーバとの通信時は、配信する時刻が途中で改ざんされなか、または改ざんを検出できる通信方法を使用すること。

・タイムスタンプサーバの時計の時刻を TSA が必要とする精度で UTC に同期できる方法を使用すること。

（７）TSA の時刻監査

標準時配信局は、タイムスタンプサーバの時刻を監査する場合、タイムスタンプサーバに配信した時刻が正確に運用されているかを監査すること。

・タイムスタンプサーバの時計の時刻を必要かつ十分な精度で監査できる手段を持つこと。

・時刻監査の頻度は、１日１回以上実施すること。

・監査した結果を、タイムスタンプサーバの時刻運用の重要な証拠となるため、後日においても検証可能な様式で保管および TSA に提供できる機能を有すること。
・保管した監査結果が改ざんされない、もしくは改ざんが検出可能な機能を備えること。
・タイムスタンプサーバの時刻を監査するにあたり、TSA が配信された時刻を改ざんできないかまたは改ざんしたことを検出できる機能を有すること。

（8）TSA の時刻異常への対応

時刻配信サービスを提供したタイムスタンプサーバの時計の時刻が規定の範囲外にあることを検出したときは、TSA にタイムスタンプサーバの時刻の異常を通知する機能を有すること。

・タイムスタンプサーバの時計の時刻が、規定の範囲外にあることを検出したときに、タイムスタンプサーバがタイムスタンプを行わないように制御する機能を裕することが望ましい。

１．２　タイムスタンプ発行サービス

タイムスタンプ発行サービスとは、加入者からの要求に応じて安全なタイムスタンプを発行するサービスを言い、タイムスタンプ発行サービスを行う機関をタイムスタンプ局（TSA）と呼ぶ。安全なタイムスタンプを生成する代表的な方式にはシンプルプロトコルとリンキングプロトコルが存在する。本節では、両方式それぞれにつき、タイムスタンプ局がタイムスタンプ発行サービスを行う上で必要とされる技術基準について述べる。

1.2.1　シンプルプロトコル

シンプルプロトコル方式を利用するタイムスタンプ局に必要とされる技術基準を以下に示す。

(a) 時刻ソース

タイムスタンプを生成する際のタイムスタンプサーバの時刻ソース（クロック）や時刻配信者を明確にしなければならない。

- TA 事業者や、GPS、標準電波、NTP など配信方式や同期方式を明確に提示しなければならない。
- 同期処理には、安全かつ確実に同期を取れる仕組みを利用しなければならない。

(b) 精度

タイムスタンプサーバの時刻ソースは日本標準時に対して十分な精度を持っていなければならない。

- 必要とされる時刻精度の目安：　±3 秒　程度

(c) 精度の証明

タイムスタンプサーバの時刻ソースの精度を証明する手段を持つことが望ましい。

- TA との間で時刻同期／時刻監査／時刻認証などを行った事実を TA が証明する監査証や監査記録をタイムスタンプに含めるなどして、随時参照可能とすることが望ましい。
- 監査証や監査記録は、時期／結果／実施者などを特定できる情報を含み、改ざんの有無を検証可能であることが望ましい。

(d) タイムスタンプポリシー

タイムスタンプの発行ポリシー（タイムスタンプポリシー）を明確にしなければならない。

- タイムスタンプには、タイムスタンプポリシーの識別情報、リファレンス情報、ハッシュ値など、タイムスタンプポリシーを一意に特定できる情報を含めなければならない。
- タイムスタンプポリシーの内容は、随時参照可能としなければならない。
- タイムスタンプポリシーの内容が改ざんされていないことを検証できるようにすることが望ましい。

(e) タイムスタンプのデータ形式

タイムスタンプのデータ形式が明確に定義されており、時刻等の誤解のない表示が可能でなければならない。

(f) 発行者情報

タイムスタンプの発行者やタイムスタンプサーバの識別情報をタイムスタンプに含めなければならない。

(g) 要求者情報

タイムスタンプにはタイムスタンプの要求者の情報を含んではならない。

(h) シリアル番号

タイムスタンプにはタイムスタンプごとにユニークな識別子を含めることが望ましい。

- 識別子として、タイムスタンプ発行順序を示すシリアル番号を含めることが望ましい。
- シリアル番号を使用しているか否かをタイムスタンプポリシーに示さなければならない。

(i) 順序性

タイムスタンプ内あるいはタイムスタンプポリシー内に、タイムスタンプに付加されたシリアル番号と時刻情報の順序の整合性保証の有無や範囲（順序の整合性は保証されている、秒単位での順序の整合性は保証されている、など）を示さなければならない。

(j) 元データの表現

タイムスタンプには、ハッシュ値など元データの表現を含み、タイムスタンプと元データの照合を可能としなければならない。なお元データの表現はタイムスタンプ発行者にわからない方法（ダイジェスト化、暗号化）としなければならない。

(k) 非改ざん（完全性）を保証する情報

タイムスタンプ自体が改ざんされていないことを確認できるよう、MAC、署名などの情報を添付するか、その他の手段を施さなければならない。

(l) ハッシュアルゴリズム、署名アルゴリズム、鍵長

タイムスタンプの対象文書に対するハッシュ値を計算するアルゴリズム、タイムスタンプの署名アルゴリズムと鍵長（署名を利用する場合）をタイムスタンプに含めるか、あるいはタイムスタンプポリシーに含めなければならない。

- ハッシュアルゴリズムとして、電子政府推奨暗号リスト記載のアルゴリズム（SHA-1、SHA256、SHA384、SHA512、RIPEMD-160）をサポートしなければならない。
- 署名アルゴリズムとして、電子政府推奨暗号リスト記載のアルゴリズム（RSASSA-PKCS1-v1_5、RSA-PSS、DSA、ECDSA）をサポートしなければならない。
- 鍵長として、RSA の 1024 ビット相当をサポートしなければならない。RSA の 2048 ビット相当の鍵長のサポートが望ましい。

(m) 署名鍵

署名を用いる場合、署名鍵は HSM を用いて保護しなければならない。

- HSM は FIPS140-2 レベル３以上の認定を受けていることが望ましい。
- 署名鍵のバックアップが不可能であるような仕組みを持つことが望ましい。

(n) 証明書、失効情報

署名を用いる場合、証明書、失効情報を適切に管理／配布しなければならない。

- 利用者の要求によりタイムスタンプ検証用の公開鍵証明書あるいはその識別情報をタイムスタンプに含めなければならない。
- 証明書は、タイムスタンプ専用のものを用いなければならない。
- 証明書パスや失効情報などをタイムスタンプ検証者が取得できるようにしなければならない。
- 特に長期保存に用いるタイムスタンプの場合、証明書情報や失効情報を十分長い期間にわたって利用可能な状態に保持しなければならない。

(o) 有効期間

公開鍵証明書の有効期間やハッシュの脆弱度などで決まるタイムスタンプの有効期間は、タイムスタンプポリシーなどに明記しなければならない。また、十分長い有効期間（例えば有効期間５年の証明書を毎年更新して利用するなど）を設定することが望ましい。

(p) 危殆化への対応

ハッシュや署名には安全性の確認されているアルゴリズムを用いてタイムスタンプを発行しなければならない。脆弱化が指摘された場合には、その時点で安全性の確認されているアルゴリズ

ムに更新可能であることが望ましい。

(q) 転送プロトコル
タイムスタンプリクエストおよびレスポンスは、少なくとも HTTP あるいは HTTPS で転送できなければならない。

(r) 再送攻撃への対処
nonce をサポートするなどして再送攻撃への対抗策を実施していなければならない。

1.2.2 リンキングプロトコル

タイムスタンプ発行サービスについて、リンキングプロトコルに依存する技術の基準について以下に記す。

(a) タイムスタンプトークンのデータ形式
タイムスタンプトークンのデータ形式は以下の情報を含み、時刻などの誤解のない表示が可能でなければならない。

- バージョン番号
- メッセージインプリント・・・TSA の時刻にバインドされた情報（ハッシュ値など）
- シリアル番号・・・タイムスタンプ記録に割り当てられた一意の番号
- タイムスタンプ・・・ISO8601 準拠の UTC 表記が可能な情報を含むこと

(b) 証明期間
タイムスタンプによる存在時刻証明及び非改ざん証明は、発行対象である電子文書の保存期間と同等の期間、継続して可能でなければならない。電子文書の保存期間は文書種別や利用者毎に異なるが、十分な証明期間を利用者に対して提供するためには、一般に以下の要件を満たす必要がある。

ハッシュ値長・・・160 ビット以上
ハッシュアルゴリズム・・・RIPEMD-160, SHA-1, SHA-256, SHA-384, SHA-512

タイムスタンプによる証明期間の長さは、ハッシュ値長に依存する。それぞれの証明期間に必要なハッシュ値長は、以下の通りである。[2]

１６０ビット・・・2013 年まで有効
１６８ビット・・・2018 年まで有効
１７６ビット・・・2023 年まで有効
１８４ビット・・・2028 年まで有効

[2] A.K. Lenstra, E.R. Verheul, Selecting Cryptographic Key Sizes, 1999 のデータを参考に算出

１９２ビット・・・2033 年まで有効

(c) アルゴリズム危殆化に対する対策

リンキングプロトコルを用いたタイムスタンプ発行サービスは、ハッシュアルゴリズムの危殆化に備えて ISO/IEC 18014-3（Mechanisms producing linked tokens）に定められた ExRenewal 拡張をサポートすることが望ましい。利用者は、タイムスタンプトークンが既に付与されている電子文書について、TSA が使用しているハッシュアルゴリズムの危殆化が予測されるタイミングを越えて保存する場合、ExRenewal 拡張の機能を利用してタイムスタンプトークンの有効期限を延長することができる。利用者は、ハッシュアルゴリズムを強化した TSA に対して、拡張機能を使って現在のタイムスタンプ発行要求が、過去に発行されたタイムスタンプトークンの更新であることを示し、それにより古いタイムスタンプの有効期間を延長することを希望することができる。

(d) オペレーション

リンキングプロトコルを用いたタイムスタンプ発行サービスは、ISO/IEC 18014-3 に定められた以下のオペレーションを実現するための技術をサポートしなければならない。

・リンキング

TSA において時刻とバインドされて管理される情報（ハッシュ値など）は、過去に生成されたものと計算上のリンクを持つこと。

・集約

ある特定のタイミングに複数のタイムスタンプ発行要求を並行して処理するために、発行要求を集約する機能を持つこと。この場合、集約に関係する全てのタイムスタンプトークンは、同じ時刻を割り当てられるものとする。

・公開

TSA で管理しているリンク情報を、定期的なタイミングで広く公開すること。

１．３　タイムスタンプ検証サービス

1.3.1　シンプルプロトコル

(a) 安全な通信路

セキュリティ対策（なりすまし、改ざん、盗聴の対策、など）が行われた通信路上で利用者とタイムスタンプ検証サービス間の検証プロトコルが実行されることが望ましい。

(b) 検証要求データ

・検証要求データの中には、検証対象となるタイムスタンプトークンが含まれること。

・検証要求データの中にタイムスタンプ対象の電子データが含まれていてもよい。

(c) 検証処理

・利用者から送信される検証要求データの形式を検査すること。
・利用者から送信されるタイムスタンプトークンの妥当性を検査すること。
・検証要求データ形式に不備がある場合や検証に失敗した場合はエラーメッセージを返すこと。メッセージにはエラーの理由を含めていること。
・検証が成功した場合は、検証結果データを利用者へ返却すること。

(d) タイムスタンプトークンの妥当性

・タイムスタンプトークンに公開鍵証明書が含まれる場合、検証時におけるその証明書の有効性を検査すること。
・タイムスタンプトークンに公開鍵証明書が含まれる場合、タイムスタンプトークン発行時におけるその証明書の有効性を検査することが望ましい。
・有効性を確認した公開鍵を用いてタイムスタンプトークンに含まれる電子署名の妥当性を検査すること。
・PKI 技術を利用した検証だけでなく、他の技術を用いた検証方法を採用してもよい。例えば、検証対象となるタイムスタンプトークンと TST 検証プレーヤ内で安全に保管されたタイムスタンプトークン情報を比較し検証を行ってもよい。

(e) 検証結果データ

・検証結果データの中には、利用者の検証要求データの中にあるタイムスタンプトークンが含まれること。
・検証結果データの中に TST 検証プレーヤの電子署名を含めてもよい。

1.3.2 リンキングプロトコル

本章 1.2.2 項で述べた内容と同じ基準が、タイムスタンプ事業者に対して求められる。

リンキングプロトコルを用いた TSA から発行されたタイムスタンプトークンは、その際に生成されたリンク情報等を保持している TSA によってのみ検証が可能である。従って、検証時、タイムスタンプに求められる技術基準は、発行時に求められるものと同一のものとなる。

第２章　運用基準

本章では標準時配信サービスやタイムスタンプサービス、認証局等に適用される運用基準について示す。タイムスタンプサービスについてはシンプルプロトコルとリンキングプロトコルについて示す。

２．１　共通事項

標準時配信サービスおよびタイムスタンプサービス（本節では両者をまとめて単にサービスと呼ぶ）に共通する事項を以下に示す。

(a) 義務

① サービスの信頼性と安全性の確保

それに適したサービスを実行するために必要な具体的手順・手続きを定めて、適切な運用を継続する義務がある。

② 加入者および依存者に対する適切な情報提供

サービス提供事業者は、加入者および依存者の義務について周知させる義務がある。また、その履行に必要な各種情報を適切なタイミングで提供する義務もある。

(b) 責務

① サービス提供事業者は、サービス提供事業者自身の義務を定めておく必要があるとともに、その前提とするサービス提供事業者の責任と保証に関するポリシーを定め、開示する必要がある。

② サービス提供事業者はポリシーを開示する際に、利用者がサービスの信頼度を評価でき、さらに利用者の履行すべき義務およびサービス提供事業者の履行すべき義務について利用者が容易に理解できるように、運用規定書、サービス利用規約書を開示するだけでなく、重要な事項については概要をまとめて開示する工夫が必要である。

③ 運用規定に反する行為により利用者に損害を与えた場合、責任と補償の内容を定める必要がある。

(c) 組織・人事管理

① 独立性／第三者性

サービスの安全性と信頼性を長期的に確保するためには、特定の企業・機関・組織の短期的/自己戦略的な影響からできるだけ独立しており、また第三者的に公平な立場を保持できることが望まれる。

② 専門性

安全性と信頼性の高い運用を持続的に行い、また技術進歩に適切かつ充分に対応していくため、さらにはトラブル等に迅速に対応するためには、情報セキュリティ技術やシステム

監査等の専門家を配置しておくことが望ましい。

③ 組織体制

サービスの運用にかかわる組織の体制としては、以下が必要である。

- クリティカルデータに接触可能な部署は他から隔離されていること。
- 事故を未然に防ぐために、部署内での内部牽制が行われること。
- 部署外からの監査等のチェック機能が働くこと。
- 事故発生時に、その発生源が特定できること。

(d) 財務基盤

万一、倒産等で存続が立ち行かなくなった場合、利用者に提供したサービスの信頼性が危機にさらされることになる。よって、物理的に安全な設備や、暗号・コンピュータ・法律の専門家や技術者の採用、高度で安全なサービスの開発・運用や信頼性の確保等を賄うに充分な資金を有していることが必要であり、損害賠償にも対処できるだけの十分な財務基盤を保持して事業を運営していく必要がある。

(e) 情報開示

利用者からの信頼を得るため、その判断基準となる経営情報、技術情報、運用などについて、サービスのセキュリティ維持に影響を及ぼさない範囲で、十分な情報の開示あるいは公開を行う必要がある。また、異常時に際しても必要情報が利用者に適切に知らされるよう、開示方式、開示タイミングなどの条件を定めておくことも必要である。

開示すべき情報として以下のようなものがある。

① 経営情報

利用者がサービス提供事業者の経営に対する健全性を確認できるように、財務状況を含めた経営情報の開示あるいは公開が必要である。

② 技術情報

利用者がサービスの安全性や信頼性を判断できるように、開示あるいは公開できる範囲での技術情報の開示あるいは公開が必要である。

③ 安全対策実施状況

サービス提供事業者の業務運営が安全に実施されているか利用者が確認できるように、業務運営（内部不正防止対策、権限の分散、教育など）に対する定期的な監査実施結果などを開示あるいは公開する必要がある。

④ 運用規定

本ガイドラインに準じた運用規定を公開する必要がある。

⑤ サービス利用規約

サービス内容、賠償責任などのポリシーが含まれるサービス利用規約書を公開する必要がある。

(f) 機密保持

サービスの安全性や信頼性に影響を及ぼすような情報に対しては、情報システムの持つ瞬

時性と広域性を念頭に置いた適切な情報管理が必要である。

① セキュリティ維持にかかわる機密情報の保持

運用者の特定、運用体制、マシン室のレイアウト、監査情報、設備・システムセキュリティ等の機密にすべき情報については、その影響度を十分考慮した取扱い方法を定め、それに従った運用が適正に行われているか適時確認することが必要である。

② 加入者関連情報保護

加入者にかかわる情報が目的外に利用されたり、不正に漏洩されたりすることがないように、機密範囲とその取扱い方法を定め、それに従った運用が適正に行われているか適時確認することが必要である。

(g) 業務の中断・終了

サービスを中断・終了する際は、そのスケジュールと手続きを決め、その内容を公知、もしくは利用者へ通知する必要がある。

また、障害発生時などの予期できない場合の緊急停止措置以外は、事前の通知なしに業務を中断してはならない。

(h) 加入者個人情報の取扱い

① 利用範囲

サービス提供事業者は、加入者から提供される個人情報については、サービスを提供するために必要な範囲を越えて使用してはならない。

② 利用目的の公開

個人情報の利用目的を運用規定に記載し公開する必要がある。

③ 個人情報の開示

サービス提供事業者は、加入者秘密情報を開示してはならない。ただし、以下の場合はその限りではない。

- 加入者本人または本人の代理人から自己の登録情報に関して開示要求があった場合。ただし、サービス提供事業者はあらかじめ本人であることを確認する要領を定める必要があり、その要領に従って本人確認を実施した後、開示するものとする。
- 法令の定めにより、回答が義務づけられているもの。また、法令の範囲内で本人の同意を得た場合。

④ アクセス制限

加入者秘密情報へのアクセスは、機密保持のために、権限を有する者だけが行える様にする必要がある。

⑤ 保管

- 加入者秘密情報は、不正に改ざん・消去・漏洩等がなされないように安全に保管する仕組み、および必要に応じて取り出せる仕組みを持つことが必要である。
- 加入者秘密情報は、災害等により消失することのないように必要に応じてバックアップをとることが望ましい。

(i) 監査

サービス提供事業者は、そのシステムの安全性および信頼性を維持するため、提供するサービスにかかわる情報を記録し、これを定期的に監査する必要がある。

① 監査情報の定義

監査情報とは、サービス運用規定・サービス利用規約・技術情報・安全対策実施状況・システムイベントの記録等の監査を行うために必要な情報をいう。例えば、監査情報には以下のような情報が含まれる。

- 国家時刻標準機関(NTA)や標準時配信機関(TA)との時刻比較・校正記録
- 加入者とサービス利用契約の発効・サービスの利用開始から契約解除・サービス停止までのプロセスにおける全記録
- サービス提供事業者設備への入退室記録およびそれに対する承認記録
- サービス提供事業者システムに対する操作記録
- サービス提供事業者システムの動作記録
- 帳簿書類へのアクセスおよび帳簿書類の廃棄についての記録

② 監査情報の保管

監査情報は、そのアクセス権限を明確にし、不正アクセスによる情報の改ざん、消去、漏洩等に対して保護し、必要に応じ適正な期間内に提供可能な状態で保管しておく必要がある。また、監査情報は適正な間隔でバックアップを取り、隔地保管することが望ましい。

③ 監査の頻度

監査の頻度は、最低年１度行う必要がある。

④ 監査情報の保管期間

監査情報は１０年以上保管する。

⑤ 監査結果の開示と対処

監査実施後は、監査結果を速やかに開示するものとし、監査の結果として欠陥が指摘された場合には、以下の対処を行う必要がある。

- 欠陥が修正されるまでの対処(例えば、運用の停止、利用者に対する十分なアナウンス等)
- 欠陥への対処

⑥ 監査情報および監査結果の保存

監査情報および監査結果の保存は、監査後の保存期間を予め定め、不正なアクセスによる情報の変更・改ざん・削除等が無いよう適切かつ合理的な安全対策を講ずる必要がある。

(j) システムのトラブル、危殆化、災害からの復旧

サービスの提供においては、予定外のサービス停止による利用者の被害は大きい。よってその場合は速やかに対処できるように、復旧手順や対処手順を明確にしておく必要がある。

① サービス提供事業者の使用するシステムの時刻精度が運用規定の規定範囲 外になった場合はシステムトラブルとみなし、システムを緊急停止し速やかに復旧作業を行う。

②　ハードウェア、ソフトウェアまたはデータが破壊された場合の対処

バックアップ用のハードウェア、ソフトウェアまたはデータより速やかに復旧作業を行う。

③　災害等発生時の設備の確保

災害等によりサービス提供事業者の設備が被害を受けた場合は、予備機を確保しバックアップデータを用いて運用を行う体制が必要となる。

(k) タイムソースの管理・トレーサビリティ

① 標準時との時刻同期管理

提供するサービスの時刻は、UTC と時刻同期している必要がある。

② 時刻精度

提供するサービスの時刻精度は、UTC に対して適正に維持される必要がある。

必要とされる精度は提供するサービスにより異なり、標準時配信サービスにおいては 300 ミリ秒以内、タイムスタンプサービスにおいては３秒以内を目安とする。（本章の技術基準の項参照）

③ 時刻のトレーサビリティ

サービス提供事業者は、提供したサービスの時刻の UTC に対するトレーサビリティを保持する必要がある。

２．２　シンプルプロトコル

タイムスタンプ発行サービスについて、シンプルプロトコルに依存する運用の基準について以下に記す（シンプルプロトコルに依存しない運用基準については前節を参照）。

(a) タイムスタンプ局の鍵管理[3]

タイムスタンプ局は、タイムスタンプトークンの署名生成鍵／検証鍵ペアや通信に使用する暗号化鍵／復号鍵などについて、それらの全ライフサイクルにわたって安全で信頼性の高い管理が要求される。

① 鍵の生成

- 鍵ペアや共通鍵の生成は、信頼できる鍵生成システムを利用して行う必要がある。なお、鍵生成システムの機能は鍵管理モジュールの内部に実装されていることが望ましい。
- 鍵ペアや共通鍵の生成は、複数人管理のもとで行う必要がある。

② 鍵の保管

- 鍵生成システムによって生成された鍵は、複数の鍵構成要素に知識分散することによって単独では鍵に関する秘密情報を一切知り得ないように保管するか、あるいは鍵管理モジュール内に保管する必要がある。
- 鍵を知識分散して保管する場合には、知識分散された鍵の情報は各鍵構成要素について、権限を有する者が個別に保管する必要がある。
- 一方、鍵を鍵管理モジュール内で保管する場合には、複数人の権限を有する者が揃わ

3　参考文献：認証局運用ガイドライン（V1.0），電子商取引実証推進協議会 認証局検討ワーキンググループ，1998.3 “http://www2.ecom.jp/report/pdf/H09/h9_cert2.pdf”

なければ鍵管理モジュールの持ち出し等ができないよう、複数人管理のもとで保管する必要がある。

③　鍵の利用

・ 保管されている秘密鍵や共通鍵を電子署名や復号に利用する際には、鍵管理モジュールに入れて使用することが必要である。鍵が知識分散されて保管されている場合には、利用の前に秘密情報を鍵管理モジュールにロードする必要があるが、そのロード処理は複数人管理のもとで行うことが必要である。

・ 鍵管理モジュールをタイムスタンプトークン生成システム等に接続したり、鍵管理モジュール内の鍵を利用可能状態にする操作は、複数人管理のもとで行う必要がある。

④　鍵の保存

・ タイムスタンプ局の公開鍵は有効期間後も可用性を確保することが必要であり、改ざんされないように保存する必要がある。

⑤　鍵の廃棄

・ 有効期間が終了したタイムスタンプ局のタイムスタンプトークンの署名生成鍵や、保存期間が終了した鍵などは、その後の不正利用が行われないように廃棄する必要がある。

・ 廃棄は、複数人管理のもとで、秘密情報の一部でも露顕したり残存させたりすることなく行われる必要がある。

⑥　鍵の定期更新

・ タイムスタンプ局の鍵は、あらかじめ有効期間を設け、定期的に更新する必要がある。なお、鍵の有効期間の設定はタイムスタンプ局のポリシーによる。

⑦　鍵の危殆化時／災害時の復旧

・ タイムスタンプ局は、タイムスタンプ局の秘密鍵が内部不正によって漏洩したり、第三者によって秘密鍵が解読された場合、さらには災害によってタイムスタンプ局がダメージを受けた場合などの事態に対して、事前に対応策を策定しておく必要がある。

・ タイムスタンプ局の秘密鍵が危殆化した場合、あるいはその可能性がある場合、タイムスタンプ局は速やかに対応する鍵の失効処理と新たな鍵への更新処理を行う必要がある。

・ タイムスタンプ局の秘密鍵が危殆化した場合、その秘密鍵で生成したタイムスタンプトークンは一括して失効されることが必要となる

・ タイムスタンプ局の秘密鍵が危殆化した場合、対応する鍵を失効させたことをサービス利用者に通知、もしくは情報公開する必要がある。

(b) システムのトラブル、危殆化、災害からの復旧

タイムスタンプサービスにおいては、予定外のサービス停止による利用者の被害は大きい。よってその場合は速やかに対処できるように、復旧手順や対処手順を明確にしておく必要がある。

①　タイムスタンプ局のタイムスタンプシステムの秘密鍵が危殆化した際の対処

タイムスタンプトークンを失効する場合、秘密鍵を使用して発行されたタイムスタン

プトークンは一括して失効されることが必要となる。

２．３　リンキングプロトコル

タイムスタンプ発行サービスについて、リンキングプロトコルに依存する運用の基準について以下に記す（リンキングプロトコルに依存しない運用基準については本章 2.1 節を参照）。

(a) TSA によるリンク情報の管理

・　リンク情報の生成

TSA は本章 2.1 節に示すセキュアな管理環境のもとでリンク情報が生成されることを保証しなければならない。

リンク情報とは、ある特定時刻(t)に受け付けたハッシュ値を集約して複数の要求を代表する１つのハッシュ値を作成し、その直前のリンク情報（t-1）から新しいリンク情報（t）を作成したものである。また、時間との関連づけを持たせたハッシュ値であり、検証のためのデータとして後に利用されるものである。

・　リンク情報生成の開始

リンク情報の生成は、本編第 3 章に示す物理的にセキュアな環境で TSA 管理者および TSA 責任者により、二重管理のもとで開始されなければならない。また、セキュリティ基準が保証された信頼あるシステムで生成が行われなければならない。

・　リンク情報の保持

TSA は、サービス提供中はセキュリティ基準が保証された信頼あるシステムでリンク情報を保持し、その完全性を維持することを保証しなければならない。リンク情報へのアクセスは TSA 責任者、TSA 管理者の両者の合意のもとに行われなければならない。

・　リンク情報の公開

TSA は、運用機関の正当性を証明するために定期的にリンク情報を公開しなければならない。公開方法および公開先については任意であるが、下記の公開要件を満たすべきである。

✓ 取得要件

TSA 責任者、TSA 管理者の両者の合意の下で、リンク情報の取得が行われなければならない。

✓ 公開要件

公知の事実かつ改ざん不可能となるよう、定期的に新聞等へ公開しなければならない。公開情報は、サービス提供中保持し、いつでも参照できるようにしておかなければならない。

・　リンク情報の監査

TSA は、本章 2.1 節に定める監査を実施する場合に、公開済みリンク情報と TSA が実際に

管理しているリンク情報の整合性を監査情報に含めなければならない。

(b) タイムスタンプ記録

TSA は、タイムスタンプトークンがセキュアに発行され、正しい時刻を含むことを保証しなければならない。

- 発行するタイムスタンプトークンには一意の識別子を付与する。
- TSA がタイムスタンプトークンにおいて使用する時刻値は、JST（日本標準時）または UTC（協定世界時）の時刻値の少なくとも 1 つに基づく。
- タイムスタンプトークンに含まれる時刻は、タイムスタンプ事業者のポリシーに定める精度内、または、タイムスタンプトークンそのものに精度が定められている場合にはその精度内で UTC と同期するものでなければならない。
- タイムスタンプトークンには、要求者の指示に従ってタイムスタンプを付与されたデータの表現（ハッシュ値など）を含む。
- タイムスタンプトークンには、検証に必要なデータ（リンク情報、ルートハッシュ値を生成するのに必要な中間のハッシュ値）を含む。

２．４　認証局に対するガイドライン

2.4.1　概要

シンプルプロトコルとして知られる RFC 3161 準拠のタイムスタンプ方式では、PKI 技術（公開鍵基盤技術）が利用されている。認証局は、タイムスタンプ局に対して、タイムスタンプ局の主体と公開鍵の結びつきを証明する公開鍵証明書を発行する。タイムスタンプ局は、この公開鍵に対応する私有鍵を用いてタイムスタンプのデジタル署名を作成する。

PKI では、認証局の信頼性を前提としている。タイムスタンプ局は、信頼の出来る認証局からタイムスタンプ向けの公開鍵証明書を発行してもらう。また、タイムスタンプを受け取った検証者は、タイムスタンプのデジタル署名を検証する時は、認証局の公開鍵証明書を信用する必要がある。厳格な検証を行う場合は、タイムスタンプ局の公開鍵証明書の発行ポリシーを受用可能かどうかも確認する必要がある。

認証局は、自身の信頼性を示すために、CP/CPS を作成・発行している。CP とは、証明書の利用目的や範囲を示す証明書ポリシー（CP: Certificate Policy)であり、CPS とは、認証局の運用実践を表明した認証実施規程(CPS: Certification Practice Statement)である。認証局の利用者から見れば、この CP/CPS は、認証局の信頼性を判断するための材料の一つとなる重要な文書である。

本節では、タイムスタンプ局向けの公開鍵証明書を発行する認証局に対する CP/CPS に対するガイドラインを記述する。CP/CPS の雛型としては、RFC 2527(Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework)に基づき、タイムスタンプ局に特化した要件について説明する。

2.4.2 タイムスタンプ局向け認証局の特徴

タイムスタンプ局向けの認証局は、一般的な認証局(例：官職証明書を発行する認証局や Web サーバ向け証明書を発行する認証局)とは異なる以下の特徴を持つ。これらの特徴を踏まえた CP/CPS が必要である。

（1）標準的なタイムスタンプ技術規格への対応

RFC 3161 では、タイムスタンプ局が使用する公開鍵証明書の鍵使用目的を制限する規定がある。タイムスタンプ局向け認証局は、このような標準技術規格に準拠する必要がある。

（2）電子文書の長期保存への対応

タイムスタンプ局が発行するタイムスタンプは、電子文書の存在時刻と原本性を長期に亘って証明するために使用される場合がある。訴訟時などに行われるタイムスタンプの真正性の検証では、認証局における公開鍵証明書発行・失効記録が遡及される可能性があるため、認証局は、これらの記録を長期間、安全に保管する必要がある。

2.4.3 TSA 向け CA に特化した CP/CPS 要件

TSA 向け CA に特化した CP/CPS 要件を以下の表に示す。CP/CPS で記載される項目とその項目に対する TSA 向け CA の要件を記す。なお、一般的な CA に対する共通的な要件の場合は、「－」で表す。

表 2-1　TSA 向け CA に特化した要件

項目	項目の説明	TSA 向け CA の要件
General Provisions（一般的な規定）		
Obligations （義務）	CA、RA、登録者、証明書利用者、リポジトリの義務を記述する	証明書利用者（TSA）の義務 ・定められた基準（TSA ガイドライン*1 など）に沿って運用する
		証明書検証者の義務 ・証明書の有効期間中に、タイムスタンプ／TSA 証明書を検証する
Liability（責任）	CA、RA、登録者、証明書利用者の責任を記述する	CA の責任 ・CA は、TSA の存在のみを証明し、TSA のタイムスタンプ行為に関する責任は負わない
		TSA の責任 ・TSA は、タイムスタンプの時刻／タイムスタンプの有効期間等を保証しなければならない

Financial Responsibility（財務的な責任）	賠償などの財務上の責任を記述する	・CA が失効処理をしていたにも拘らず、証明書利用者が証明書の有効性検証を怠ったことに起因するトラブルについては、CA は一切責任を負わない
Interpretation and Enforcement（解釈と執行）	解釈と執行を記述する（準拠する法律の記述。条項の可分性、継続性、合併、通知の記述。紛争の解決手続きの記述）	―
Fees（料金）	料金を記述する	―
Publication and Repository（公表とリポジトリ）	公表とリポジトリを記述する（CP、CPS、アグリーメントなどの発行頻度、発行場所、アクセスコントロールなどの記述）	・常に安全に参照できるリポジトリに、CP、CPS、発行した全ての TSA の証明書、ルート CA／サブ CA の証明書、CRL、審査記録・発行記録など（有効期間の切れた証明書／CRL も含む）を（リポジトリや Web 上で）公表する
Compliance Audit（準拠性監査）	準拠性監査に関する諸条件を記述する	―
Confidentiality Policy（守秘性のポリシー）	機密保持のポリシーを記述する	―
Intellectual Property Rights（知的財産権）	知的財産権に関する情報を記述する	―
Identification and Authentication（識別と本人認証）		
Initial Registration（初期登録）	主体登録、あるいは証明書発行における識別と本人認証の手続きについて記述する	・登録時に、定められた基準（TSA ガイドライン*1 など）を満たす TSA であることを証明書発行ポリシの一環として確認する ・有効期間６年間、私有鍵の使用期間１年（例）の証明書を発行する （GPKI で用いられる EE 証明書の有効期限が 3 乃至 5 年であることから、その期間をカバーするためにはこの数値が妥当、また、TSA 事業者の活動単位を 1 年と考え、私有鍵の使用期間を設定した･･･※）

Routine Rekey（ルーチン鍵更新）	通常の証明書の更新のための識別と本人認証の手続きを記述する	・１年（例）ごとに TSA の適合性を確認する ・有効期間６年間、私有鍵の使用期間１年（例）の証明書を発行する （前記※と同様の理由による）
Rekey After Revocation（失効後の鍵更新）	証明書失効後の証明書の再発行における識別と本人認証の手続きを記述する	・登録時に、定められた基準を満たす TSA であることを確認したうえで更新する
Revocation Request（失効要求）	証明書の失効時における識別と本人認証の手続きを記述する	・TSA として定められた基準を満たさなくなったとき、閉局のときには失効要求を提出する
Operational Requirements（運用要件）		
Certificate Application（証明書アプリケーション）	証明書の申請手続きを記述する	・定められた基準を満たす TSA であることを確認する
Certificate Issuance（証明書発行）	証明書の発行手続きを記述する	―
Certificate Acceptance（証明書受領）	証明書の受領手続きを記述する	―
Certificate Suspension and Revocation（証明書留保と失効）	証明書失効と一時的な使用停止の手続きを記述する	・CRL 発行の周期は数日程度とする。なお、CRL の有効期間を発行周期＋数日程度とする（対象がオーソリティであり FIPS140-2 Level3 の HSM で私有鍵を保護されているエンティティであることから、失効の可能性は極めて低い。従って CRL 発行頻度は一般のエンドエンティティ向け証明書の場合（48 時間の有効期間を持つ CRL を 24 時間周期で発行）に比較して発行間隔は長くて良い）。ただし、失効が発生した場合、速やかに CRL に反映させる
Security Audit Procedures（セキュリティ監査手順）	セキュリティ監査の手順を記述する	―

Records Archival（レコードのアーカイブ化）	記録の保管について記述する	・発行した全ての TSA の証明書、ルート CA・サブ CA の証明書、CRL、審査記録・発行記録などを、安全な状態で永続的に（有効期限後／失効後 30 年間以上（法定保存期間を有するものの中で最も長い例の一つ））保管する
Key Changeover（鍵再発行）	鍵の切り替え手続きを記述する	―
Disaster Recovery and Key Compromise（改ざんや災害からの復旧）	改ざんや災害が起きた場合における通知と復旧手順を記述する	―
CA Termination（CA 期限）	CA や RA の期限や業務の終了手続きを記述する	・発行した全ての TSA の証明書、ルート CA／サブ CA の証明書、CRL、審査記録／発行記録など（有効期間の切れた証明書／CRL も含む）を永続的に保管しておき、CA の事業が閉鎖される場合、CA はこれらの情報を他の CA 相当の機関に引き継がなくてはならない
Physical, Procedural, and Personnel Security Controls（物理的、手続的及び要員的なセキュリティ統制）		
Physical Controls（物理的セキュリティ統制）	物理的セキュリティ管理を記述する	―
Procedural Controls（手続き的統制）	手続き的セキュリティ管理を記述する	―
Personnel Controls（要員的セキュリティ統制）	要員のセキュリティ管理を記述する	―
Technical Security Controls（技術的セキュリティ統制）		
Key Pair Generation and Installation（鍵ペア生成とインストール）	鍵ペア生成とインストール手順を記述する	・必ず TSA の鍵管理装置内で鍵ペアを生成する ・TSA の鍵のサイズは、RSA1024 ビット以上（2048 ビット以上が望ましい）を使用する ・TSA の私有鍵はタイムスタンプの署名以外には使用しない

Private Key Protection（私有鍵の防護）	私有鍵の保護を記述する	・TSA の私有鍵は FIPS140-2 Level3 相当の HSM により保護する ・TSA の私有鍵は鍵管理装置の内部で生成し、格納する
Other Aspects of Key Pair Management（鍵ペア管理の他の側面）	鍵ペア管理の他の側面を記述する	・TSA の公開鍵の有効期間は６年間とし、私有鍵の有効期間は１年間とし、１年ごとに鍵の更新を行う（前記※と同様の理由による）
Activation Data（アクティヴェーションデータ）	活性化データ（Secret Shares）を記述する	－
Computer Security Controls（コンピュータセキュリティ統制）	コンピュータのセキュリティ管理を記述する	－
Life Cycle Security Controls（ライフサイクルセキュリティ統制）	システム開発管理及びセキュリティ運用管理について記述する	－
Network Security Controls（ネットワークセキュリティ統制）	ネットワークセキュリティ管理を記述する	
Cryptographic Module Engineering Controls（暗号モジュールエンジニアリング統制）	暗号化モジュール技術の管理を記述する	
Certificate and CRL Profile（証明書と CRL プロファイル）		
Certificate Profile（証明書プロファイル）	証明書のプロファイルを記述する	・拡張鍵使用法として、"id-kp-timeStamping"（オブジェクト識別子として、iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) kp (3)

		timestamping (8)）を設定しなければならない。（RFC 3161 の要件） ・鍵長は 1024bit 以上とする。2048bit 以上が望ましい ・有効期間は６年、私有鍵使用期間は１年（例）とする（前記※と同様の理由による）
CRL Profile（CRL プロファイル）	CRL のプロファイルを記述する	・CRL エントリ拡張の理由コード(reasonCode)を使用し、unspecified (0)、affiliationChanged (3)、superseded (4)、cessationOfOperation (5)のいずれかを設定する ・鍵更新の場合の理由コードとしては、superseded (4)を用いる ・TSA 閉局の場合の理由コードとしては、cessationOfOperation (5)を用いる
Specification Administration（仕様管理）		
Specification Change Procedures（仕様変更手続き）	仕様変更手続きを記述する	－
Publication and Notification Policies（公表と通知の手続き）	公表と通知の手続きを記述する	－
CPS Approval Procedures（CPS 承認手続き）	CPS 承認手続きを記述する	－

2．4．4　記録(*2)の長期保存

署名文書を長期的に、しかも安全に保管するためにタイムスタンプが使用された場合、このタイムスタンプを長期に亘って検証できることが重要である。

ETSI や IETF では、署名文書の長期保存のために、長期署名フォーマットを提案している（*3)。ここでは、署名文書で使用された暗号アルゴリズムや鍵が危殆化する前にアーカイブタイムスタンプと呼ばれる RFC 3161 準拠のタイムスタンプを署名文書と検証情報（公開鍵証明書情報と失効リスト情報）に対して適用する。さらに、このアーカイブタイムスタンプの暗号アルゴリズムや鍵が脆弱化する前に、更なるアーカイブタイムスタンプを署名文書、検証情報、以前のアーカ

イブタイムスタンプに対して適用する。

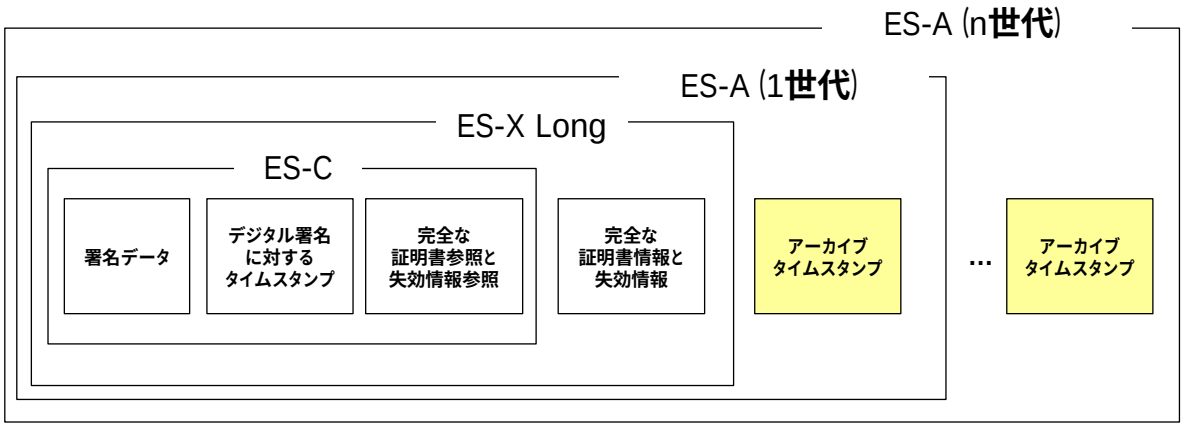

図 2-1　ETSI と IETF で策定された長期署名フォーマット

複数のアーカイブタイムスタンプが適用された長期署名フォーマットを検証するときは、一番外側（最新）のアーカイブタイムスタンプを検証し、このタイムスタンプ適用対象である署名文書、検証情報、及びアーカイブタイムスタンプの真正性を確認する。その後、内側のアーカイブタイムスタンプを検証することになる。ここで、内側のアーカイブタイムスタンプは、過去に有効であった TSA 証明書の鍵を用いて検証されることになるが、まず、この TSA 証明書及び TSA 証明書を発行した CA 証明書の正当性が検査されなければならない。なぜならば、悪意を持ったユーザであれば、都合よく、TSA 証明書と CA 証明書を偽造できる可能性があるからである。

このような偽造を検知するためには､内側のアーカイブタイムスタンプの TSA 証明書と CA 証明書が外側のアーカイブタイムスタンプ発行時点に確かに失効せずに存在していたのかどうかを確認する必要がある。一つの方法としては、CA でアーカイブされた記録と照合することが考えられる。そのため、認証局は、発行した全ての TSA の証明書、ルート CA・サブ CA の証明書、CRL、審査記録・発行記録などを、安全な状態で永続的に（有効期限後／失効後 30 年間以上（法定保存期間を有するものの中で最も長い例の一つ））保管する必要がある。

現状では、電子的な記録の長期保存としては、以下のような方法が考えられる。

（1）紙文書による長期保存

長期保存が必要な電子的な記録を紙文書として印刷し、紙文書して保管する。例えば、公証役場の確定日付を取得することで、紙文書の存在時刻を保証することができる。

（2）完全性と存在時刻が証明できる措置を講じた長期保存

長期保存が必要な電子的な記録に対し、保管期間中、公知に安全と認められたタイムスタンプ事業者が提供するタイムスタンプサービスを利用する。あるいは、それに相当する措置を講じて電子的な記録を長期保存する。

*1 TSA ガイドライン

・"時刻認証基盤ガイドライン", タイムビジネス推進協議会（平成 15 年 3 月）

・”タイムスタンプサービスの運用ガイドライン”, 電子商取引推進協議会, (財)日本情報処理開発

協会電子商取引推進センター（平成 15 年 3 月）

・ ETSI TS 102 023 V1.1.1 (2002-04) Policy requirements for time-stamping authorities

・ RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs) （2003 年 11 月）

*2 記録

ここで言う記録とは、CP/CPS の Records Archival（レコードのアーカイブ化）で規定される記録を表す。具体的には、CA が発行した全ての TSA の証明書、ルート CA・サブ CA の証明書、CRL、審査記録・発行記録など。

*3 長期署名フォーマット

・ ETSI TS 101 733 V1.5.1 (2003-12) Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats

・ RFC 3126 Electronic Signature Formats for long term electronic signatures （2001 年 9 月）

第３章　基盤項目

３．１　ファシリティ

タイムビジネスを提供するシステムを設置するファシリティの基準について以下に示す。タイムビジネスにおいては、そのビジネス上システムには信頼性、安定性、完全性について厳しく管理している必要があり、本ガイドラインでは、そのような要求を満たすファシリティとしてiDC の利用を前提とした基準を示している。

表 3-1　ファシリティの基準

分　類	項　目	達成基準	
(1)　建築	耐震基準	ビルの耐震基準を満たしていること	必須
	免震構造	建物免震装置採用時は耐震固定でも可	推奨
	内装材	不燃材であること 静電対策が施されていること	必須
	ノイズ、ＥＭＣ対策	電磁シールド対策など	推奨
(2)　電気設備	電気設備の二重化	受電設備から分電盤・動力盤まで二重化。ビルの電源検査時に無停電で行えること	必須
	非常用バックアップ発電機	ガスタービン発電機などサーバエリア受電容量以上で N+1 の冗長性を確保。	推奨
	ジェネレータ用オイルタンク	目安は補給可能間隔以上の容量。燃料小出槽を設置すること。	推奨
	無停電電源装置	各群に１台の予備機を含む	推奨
	火災報知システム	高感度火災感知システム	推奨
	中央監視システム	設備・機器全体の動作状態を把握できること。24 時間常時監視可能であること	推奨
	接地システム	統合接地システムとすること	推奨
	入退室管理	IC カード式ゲートシステムとバイオメトリックスシステムを組合わせる	推奨
	サーバ室内管理	ＩＴＶカメラ監視システムなどを導入し、死角を作らない。	推奨
(3)　空調設備	空調タイプ	下吹き出し、上吸い込み型	推奨
	空調容量	各サーバエリア毎に N+1 以上	推奨
	空調稼動時間	24 時間連続運転	推奨
	水漏れ検知システム	空調機排水廻りに漏水検知システムを設置すること	推奨
	温度・湿度調整	温度：22～24℃±2℃湿度：50%±20%	推奨
(4)　設置場所	ラック	前背面錠付き EIA 規格 19 インチラック。	推奨
	架台	耐震固定もしくは、二次元、三次元免震架台が望ましい。	推奨
	設置場所	他システムとの共通スペースに設置しない。別室または別にケージにて囲うことが望ましい。	必須
	二重化電源	2 系統配電盤からの引き込みによる電源の二重化に対応していること。	推奨
	床材	静電気対策床材の利用	推奨

（参考資料　「iDC 活用ガイドライン」iDC イニシアティブ発行）

３．２　ネットワーク

タイムビジネスを提供する上でネットワークに要求される基準について以下に示す。本基準は、タイムビジネスを提供するシステムの構成要素のうち、ネットワークが備えるべき要件について示しており、実現するための実装方法、ハードウェアおよびソフトウェア等について個別に定めるものではない。

なお、本基準は、TSA、TST 検証プレーヤの双方に適用されるものとする。

表 3-2　ネットワークの基準

分　類	項　目	達成基準	
(1)外部ネットワークとの接続	不正アクセス防止	外部ネットワークからの不正アクセス、攻撃等に対し、それを検知および防御するためのシステム（ファイアウォール等）を備えること。また、サービス停止、秘密情報取得、認証情報取得、情報改ざん、ウィルス等の攻撃に対する対策が取られていること。	必須
	サーバ認証	タイムスタンプサービス提供者は、サービス利用者に対し、サーバ認証により正当性を証明するとともに、盗聴、改ざん等を防止する機能を提供すること。	必須
	時刻情報取得	時刻情報の取得にかかわる通信においては、遅延等の回線品質が安定しかつ他のトラフィックの影響を受けない回線サービスを利用すること。	必須
	他のネットワークとの接続	複数の外部ネットワークとの接続を有する場合、一のネットワークから他のネットワークに対して、IP リーチャビリティがないこと。	必須
	信頼性	TA と接続する回線、ハブ／スイッチ、ファイアウォールおよびルータ等の装置は、冗長構成をとること。 但し、バックアップセンターを別に設けるなど、システム全体として事業の継続性を担保している場合は、この限りではない。	必須
	高負荷対策	サービスが集中し、高いトラフィック（大量のサービス要求）が発生した場合でも適正な遅延の範囲内でサービスを提供できる構成であること（ロードバランサー等)。	推奨
(2)内部ネットワーク（LAN）	アーキテクチャ	サービス若しくは機能ごとに、サーバ等機器を適切なセグメントに配置し、セグメント間においては、不要な通信を遮断することができること。特に、電子署名に関連するサーバや時刻認証を施した情報を保管するサーバは、安全なセグメントに設置し、外部からの直接のアクセスを禁ずること。	必須
	信頼性	構成する装置（ハブ／スイッチ、ファイアウォール、ルータ等）および LAN 経路は冗長構成をとること。	必須
	高負荷対策	高トラフィックの場合も適正な遅延の範囲内でサービスを提供できる構成であること（サーバロードバランサ等)。	推奨

３．３　サーバ・ストレージ

タイムビジネスを提供する上でシステムに要求される基準について以下に示す。

本基準は、タイムビジネスを提供するシステムが備えているべき性能について示しており、実現するための手法、ハードウェア、ソフトウェアについて個別に定めるものではない。

表 3-3　サーバ・ストレージの基準

分　類	項　目	達成基準	
(1)システム設計	拡張性	将来的な拡張を見据え、フロントサーバの並列拡張、および時刻認証サーバ、データベースサーバなどの処理性能に拡張性を持たせること。	推奨
	機能分割	NTP、タイムスタンプ発行、検証サービスは、システムを分割すること。また、それぞれのシステムにおいてアプリケーション単位でのサーバの分割を実施すること。	推奨
	信頼性	システムの冗長化、電源の二重化、ホットスワップ機能、UPS の導入など信頼性向上のための対策を実施すること。	推奨
	可用性	負荷分散構成、ホットスタンバイ、クラスタリングなどの技術を用いた、サービスを継続するための対策を実施していること。	必須
	バックアップ／リストア	システムデータ、ログデータのバックアップ／リストアを確実に実施するためのミラーリング、クラスタリング、可搬メディアへのバックアップなどの対策を実施していること。	必須
(2)セキュリティ関連	アクセス制限	サーバ自体の堅牢性の向上のための不要アクセスの拒否、不要アプリケーション削除、不要ポートの利用停止などの対策を実施していること。	必須
	セキュリティ管理	サーバ自体のセキュリティ対策として、十分なテストをした上でのセキュリティパッチ対応、ファイルの整合性の確認、システムログの記録など、サーバ自体のセキュリティ対策を実施していること。	必須
(3)品質管理	サービス品質	タイムビジネスを提供するサーバは、NTP 等を利用して UTC 時刻同期を行っていること。	必須
	システム監視	CPU 負荷、メモリ消費量、HDD リソース、I/O 使用率などを監視する監視システムを用意すること。また監視システムについては、ハードウェア障害、ハードウェア内温度監視機能があることが望ましい。	推奨
	障害管理	テスト環境の用意、予備パーツを準備など不測の事態に対応するための対策を実施していること。	推奨

付録

付録１　用語集

用語	スペル	解説
AutoKey	AutoKey	NTP における認証方法。PKI を利用した相手認証・鍵交換、メッセージの改ざん検出等が可能。
CA	Certification Authority	認証局。PKI における公開鍵証明書を発行する機関。
FIPS 140-2	Federal Information Processing Standard 140-2	米国 NIST が策定した暗号モジュールに関するセキュリティ認定基準。最低レベル１から最高レベル 4 まである。
GGTTS	The Group on GPS Time Transfer Standards	コモンビュー方式における時刻比較用データフォーマット。
GMT	Greenwich mean time	グリニッジ標準時。英国グリニッジを通る子午線上にて太陽が南中する時刻を正午とする時系。1967 年までは世界の標準時系として使われていた。
GPS	Global Positioning System	グローバルポジショニングシステム。人工衛星と各機器の正確な時間を利用して、地球上どこにいても現在位置を正確に割り出す測位システム。
HSM	Hardwere Security Module	ハードウエアセキュリティモジュール。物理的に暗号モジュール等の機密性を保護する装置。分解したり、衝撃を加えたりすると装置内のデータが消失する仕掛けになっているものや、温度変化や気圧の変化を検出するものもある。
IETF	Internet Engineering Task Force	インターネットで使用されるプロトコルを決定するための民間主導の標準化団体。IETF から RFC 番号がつけられて公表された規格は、実質的に世界標準規格である。
ISO/IEC 13888	International Organization for Standardization/International Electrotechnical Commission 13888	電子文書の送受信証明を行うためのプロトコルを規定。特定のデータが特定時刻に存在したことを証明するタイムスタンププロトコルも、その中の 1 つに含まれている。
ISO/IEC 14516	International Organization for Standardization/International Electrotechnical Commission 14516	電子認証、電子公証、タイムスタンプ、暗号機能の鍵管理など、TTP(信頼できる第三者)によるサービスに対しての利用と管理の規定。

用語	スペル	解説
ISO/IEC 18014	International Organization for Standardization/International Electrotechnical Commission 18014	タイムスタンプサービスに関する国際標準。Part 1: Framework、Part 2: Mechanisms producing independent tokens（独立トークン方式）、Part 3: Mechanisms producing linked tokens（リンクトークン方式）の 3 部構成をとっている。
JST	Japan Standard Time	日本標準時。独立行政法人情報通信研究機構（NICT）が生成・維持・供給している。UTC に対して９時間進んでいる。
Local-TSS	Local Time Stamp Server	当事者間の信頼関係において有効なタイムスタンプトークン（Local-Stamp)を発行するタイムスタンプサーバ。
NICT	National Institute of Information and Communications Technology	独立行政法人情報通信研究機構（旧通信総合研究所)。日本標準時を生成・維持・供給している機関。
NIST	National Institute of Standards and Technology	米国商務省標準技術研究所。米国の標準時を生成・維持・供給している機関。
NTA	National Time Authority	国家時刻標準機関。各時刻認証局に対して標準時の時刻情報を供給する国家的機関。
NTP	Network Time Protocol	ネットワークタイムプロトコル。インターネットにつながれたコンピュータの時刻を同期させるための手順。
OATS	Order Audit Trail System	注文監視追跡システム。米国証券取引市場における、時刻についてのルール。あらゆるコンピュータシステムやタイムスタンプ装置は NIST の原子時計に対して 3 秒以内で同期していなければならない、としている。
PKC	Public-Key Certificate	公開鍵証明書。
PKI	Public Key Infrastructure	公開鍵暗号基盤。公開鍵暗号技術と電子署名を使って、インターネットで安全な通信ができるようにするための環境のこと。
Public-TSS	Public Time Stamp Server	第三者に対する証拠能力を有するタイムスタンプトークン(Public-Stamp)を生成するタイムスタンプサーバ。信頼できる時刻ソースを用い、セキュリティの確保された環境で運用される必要がある。

用語	スペル	解説
RFC2630	Request For Comment 2630	IETF が策定した Cryptographic Message Syntax(CMS)を規定した文書。RFC3161 において、CMS はタイムスタンプトークンのフォーマットである。
RFC3161	Request For Comment 3161	IETF が策定した PKI を利用したタイムスタンプ（シンプルプロトコル）のプロトコルフォーマットを規定した文書。
SNTP	Simple Network Time Protocol	NTP の階層構造を簡素化したもの。NTP と互換性がある。
TA	Time Authority	標準時配信局。時刻関連事業者に標準時に基づく時刻の配信を行い、時刻関連事業者の時刻を認定する機関。
TAI	International Atomic Time	国際原子時。1958 年 1 月 1 日 0 時 0 分 0 秒を原点とた、世界各地の原子時計のデータをもとに BIPM が合成する時刻。
Tel-JJY	Telephone-JJY	テレフォン JJY。独立行政法人情報通信研究機構（旧通信総合研究所）が行っている電話回線経由の時刻配信サービス。
TSA	Time-Stamping Authority	タイムスタンプ局。タイムスタンプサービスを提供し、第三者機関としてタイムスタンプ記録を発行、検証するサービスプロバイダ。
TST	Time-Stamp Token	タイムスタンプトークン。信頼の置ける時刻と文書などのデジタル情報に対し、変更、改ざんがあったかどうかを検知できる情報。もしくはそれを指し示す情報。デジタル情報のハッシュデータに時刻情報等を付与し、電子署名として発行する。タイムスタンプトークンには独立トークンとリンクトークンの二種類が存在し、それぞれ ISO/IEC18014-2,3 に規定されている。
TSU	Time-Stamp Unit	タイムスタンプユニット。タイムスタンプトークンを生成・発行する装置。
TTP	Trusted Third Party	特定のサービスを提供する、信頼できる第三者。
UTC	Coordinated Universal Time	協定世界時。現在全世界で公式に採用されている原子時系。UTC は実時間では生成できず、各国の国家時刻標準機関が生成する協定世界時を基に国際相互比較し、後日それらのデータを集計し計算により決定される。

用語	スペル	解説
VA	Validation Authority	検証機関。デジタル証明書の失効リストを集中管理して、証明書の有効性をチェックする機関。
X.509		公開鍵インフラストラクチャ（PKI）のために必要な電子証明書の標準フォーマットを規定した ITU-T の勧告。ISO/IEC9594-8 として国際標準化された。
コモンビュー		遠隔地の原子時計の時刻比較方式。国際間の原子時計の時刻比較手段として用いられている。
時刻監査		対象となる装置の時刻を監視し、標準時とのズレを検査すること。
時刻監査局		時刻監査サービスを行う機関。
時刻監査サービス		サーバ時刻の監査･証明も行うサービス。
時刻同期		基準となる時刻に対象装置の時刻を合わせること。
時刻認証		対象となる装置の時刻が標準時に対して一定の誤差の範囲内にあることを証明すること。
シンプルプロトコル	Simple Protocol	独立トークン方式の一種で、データのハッシュ値に時刻情報等を添付して電子署名（タイムスタンプ）を生成する方式。RFC3161 で標準化されている。⇔リンクトークン方式
タイムスタンプ	Time Stamp	信頼の置ける時刻と文書などのデジタル情報に対し、変更、改ざんがあったかどうかを検知できる情報もしくはそれを指し示す情報を付与し、それ以降、内容や時刻に変更・改ざんがあったかどうかを証明する技術。
タイムスタンプ局	Time-Stamping Authority	→TSA
タイムスタンプサービス	Time-Stamp Service	情報が時間軸上におけるある特定の点より以前に存在していたことを第三者に証明するサービス。
タイムスタンプトークン	Time-Stamp Token	→TST

用語	スペル	解説
長波 JJY		独立行政法人情報通信研究機構（旧通信総合研究所）が行っている標準電波による時刻配信サービス。
テレフォン JJY	Telephone-JJY	→Tel-JJY
独立トークン方式	Independent Token	他のタイムスタンプトークンに含まれる情報を用いずにタイムスタンプトークンを生成する方式。独立トークン方式には、電子署名を用いたシンプルプロトコルの他、メッセージ認証コード（MAC）を用いた方式、アーカイブを用いた方式がある。ISO/IEC18014 で標準化されている。⇔リンクトークン方式
トレーサビリティ	Traceability	本ガイドラインでは時刻のトレーサビリティを指す。国家標準時刻への校正情報の取得が可能なこと。時刻認証で使われる時計の誤差に関して、その親時計、さらにその親時計とたどっていき最後にオーソライズされた NTA にたどれること。
日本標準時		→JST
ハードウエアセキュリティモジュール	Hardwere Security Module	→HSM
ハッシュ関数	Hash Function	元の平文からメッセージダイジェストを作成する関数。元の平文の 1 ビットが変化しただけで、メッセージダイジェストの大半のビットが変化する。MD5、SHA-1 などがある。
標準時配信サービス		高精度で高信頼の時刻を必要としている企業に信頼できる標準時を配信するサービス。標準電波等により提供される時刻情報の配信のみ行う「受信型」サービスと、国家時刻標準機関等から標準時の配信を受け、その標準時のトレーサビリティを維持しつつ標準時配信を行うとともにサーバ時刻の監査・証明も行う「証明型」サービスがある。
標準時配信局	Time Authority	→TA
リポジトリ	Repository	証明書に関する情報を保管したり配布したりするオンラインデータベース。
リンキングプロトコル	Linking Protocol	→リンクトークン方式

用語	スペル	解説
リンクトークン方式	Linked Token	リンキングプロトコルまたは連鎖型プロトコル。他のタイムスタンプトークンに含まれる情報を用いてタイムスタンプトークンを生成する方式。タイムスタンプを時系列的に結びつける連鎖情報を利用する。ISO/IEC18014 で標準化されている。⇔独立トークン方式
連鎖型プロトコル		→リンクトークン方式
ログ	Log	情報システムの機器の稼動状況と利用状況を記録した履歴情報。システムログとアクセスログがある。また、セキュリティ監査に用いるログを監査ログという。

付録２　参考・参照資料一覧

- 申請・届出等手続きのオンライン化にかかわる汎用受付等システムの基本的な仕様（2001 年 8 月 6 日　総務省）
- 地方公共団体における申請・届出等手続きのオンライン化にかかわる汎用受付システムの基本仕様（2002 年 3 月 27 日　総務省）
- 汎用受付システム調達の参考資料(共同方式の場合)（改定第 2 版）（2002 年 11 月総務省自治行政局地域情報政策室）
- 国交省 WEB 記事「自動車保有関係手続きのワンストップサービスグランドデザイン」（資料参 1-4）
- 「電子署名法」　夏井高人　リックテレコム

参加メンバー（ガイドライン分科会メンバー）

分科会主査：本田雅裕

氏名	所属
市川　桂介	アマノ株式会社
本田　雅裕	株式会社エイベック
櫻井　徹	株式会社ＮＴＴデータ
三谷　宣之	株式会社ＮＴＴデータ
大和　喜一	株式会社ガッツデイト
向井　徹	シーア・インサイト・セキュリティ株式会社
岩間　司	独立行政法人情報通信研究機構
上畑　正和	セイコーインスツルメンツ株式会社
柴田　孝一	セイコーインスツルメンツ株式会社
松丸　宗彦	セイコープレシジョン株式会社
小松　文子	日本電気株式会社
谷川　嘉伸	株式会社日立製作所
廣瀬　智康	丸文株式会社
米川　知希	丸文株式会社
宮崎　一哉	三菱電機株式会社
奥瀧　芳雄	株式会社 UFJ 銀行
臼杵　稔	横浜著作権研究会

（組織名 50 音順）

【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/

第 2 版　2004 年 5 月