信頼されるタイムスタンプ技術・運用基準
ガイドライン

平成１７年１１月

タイムビジネス推進協議会

はじめに

電子データは容易に複製・転送できることから、ネットワーク環境の整備に伴いその高い利便性から流通量は増加している。

しかしながら、電子データは自己証明の信頼性が低いため、その証拠能力や証明力は第三者に依存する必要があり、電子データに時刻情報を付与するシステムにより原本性担保や改ざん防止を実現するタイムスタンプを提供するための技術・運用基準が望まれている。

本資料は、タイムスタンプの発行に関わる時刻配信・認証業務の責務を明確にし、各々の事業者が遵守すべき技術およびシステム運用基準の枠組みを明示的に示すために、平成16年5月にタイムビジネス推進協議会にて発行された「時刻認証基盤ガイドライン」のうち第Ⅲ編「提供ガイドライン」にて記述されていた「技術基準・運用基準・基盤項目」について、「信頼されるタイムスタンプを発行する」という視点で検討会を実施し策定した。

これによってタイムスタンプサービスの水準を、安全・安心な社会基盤として妥当な、デジタルな時の痕跡に法的な証拠能力を提供できる高さに保つことを目的とする。

なお、本資料で使用される用語については、「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発行）を参照いただきたい。

目　　次

１．タイムスタンプの全体像 ..... - 1 -

１．１　タイムスタンプの定義 ..... - 1 -

１．２　タイムスタンプサービスのモデル ..... - 2 -

１．３　信頼されるタイムスタンプとは ..... - 4 -

２．技術･運用基準 ..... - 5 -

２．１　国家時刻標準機関 ..... - 5 -

２．２　時刻配信事業者 ..... - 6 -

２．３　時刻認証事業者 ..... - 12 -

２．３．１　デジタル署名技術を使用する方式 ..... - 13 -

２．３．２　デジタル署名技術を使用しない方式 ..... - 22 -

２．４　時刻認証事業者むけ認証局 ..... - 28 -

２．５　タイムスタンプ検証 ..... - 29 -

１．タイムスタンプの全体像

１．１　タイムスタンプの定義

本資料でいう「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事により、その時刻以前にそのデータが存在した事の証明（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）する事ができる手段、およびその証拠に結びつく情報」とする。

タイムスタンプは、その利用目的から、長期にわたり安全かつ安定したシステムが求められているので、仕様が明確に定義されており、公開されている必要がある。それには国際的な標準規格に準拠していることが望ましい。

(1)　タイムスタンプとタイムスタンプトークン

ISO18014-1 では、用語定義において、タイムスタンプ（ＴＳ）とタイムスタンプトークン（ＴＳＴ）を分けて定義している。本資料では、タイムスタンプとは、単なる時刻を文字表現として表したもの（YYMMDDHHMMSS など）を対象とせず、「時刻と電子情報を結合する手段および情報」であり、要件として「特定の時刻以前に存在したことの証拠を提供するために、改ざん・分離できない状態で特定の電子情報と時刻情報を結合すること」とし、電子情報と時刻情報の結合の検証が可能なデータ構造体を広義のタイムスタンプと区別してタイムスタンプトークンと記載する。

(2)　タイムスタンプへの要件

容易に変更可能な電子情報の使用には、それらの情報がいつ作成されたか、または最後にいつ変更されたかをいかに証明するかという課題が存在する。タイムスタンプは、このような時間の証拠保全に役立てなければならない。したがって、タイムスタンプは、以下の要件を満たさなければならない。

・存在証明

時刻情報は、特定の電子情報が特定の時刻より以前に存在したことを証明するための重要な証拠となることから、時刻情報が信頼できる標準時配信局から配信されたものであり、特定の電子情報との結合が立証できるシステムでなければならない。

・非改ざん証明

特定の電子情報が不正に改ざんされた場合の検知可能なシステムの提供

タイムスタンプは、電子情報の正当性と機密性の制御のために、電子情報自体ではなく、電子情報のハッシュ値に対して信頼できる時刻情報を付与することによってタイムスタン

プトークンを生成することで、これらの要件を解決している。従ってタイムスタンプトークンには、電子情報自体が含まれておらず、電子情報の機密性は保たれている。

電子情報のハッシュ値は、信頼できる第三者機関であるタイムスタンプ局（ＴＳＡ：Time Stamping Authority）で管理運用されている時計の時刻と暗号手段で結合されている。この結合が、その時間での電子情報の正当性を客観的に証明する。

１．２　タイムスタンプサービスのモデル

電子情報のハッシュ値に信頼できる時刻情報を付与しタイムスタンプトークンを発行するタイムスタンプサービスは、図１－１に示すモデルにおいて信頼できる第三者機関であるＴＳＡから提供される。

タイムスタンプサービスモデルは、タイムスタンププロトコルによりモデルが異なる。

例えば、ＩＥＴＦで２００１年に標準化が完了したＲＦＣ３１６１に準拠した独立トークン方式は、デジタル署名を用いた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方式で、公開鍵証明書を発行する認証局は必須である。一方、リンクトークン方式は、タイムスタンプトークンの偽造を行うことができないように過去に発行したタイムスタンプトークンすべてとのリンクを作成し、このリンク情報の偽造を困難にするため定期的に新聞等でリンク情報を衆目にさらす運用を行っている。リンク情報公開先は必須である。なお、独立トークン方式およびリンクトークン方式の技術解説詳細については、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発行）第Ｉ編、第５章タイムスタンプの仕組みを参照されたい。

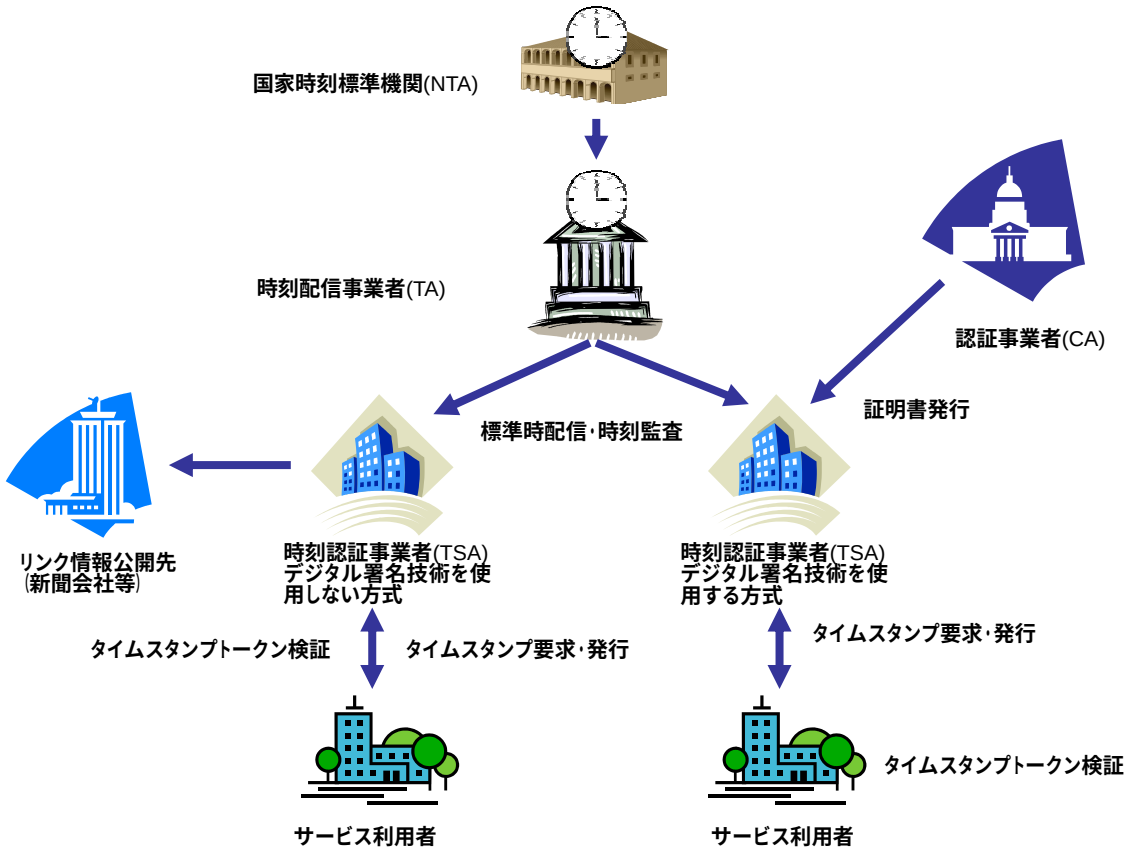

図１－１　タイムスタンプサービスのモデル

図１－１において使用されている用語の説明を以下に記す。

・国家時刻標準機関－ＮＴＡ（National Time Authority）

国家時刻標準機関（ＮＴＡ）は、国の標準時を生成・維持・配信する機関である。日本では独立行政法人　情報通信研究機構（ＮＩＣＴ）が実施している。

・時刻配信事業者－ＴＡ（Time Authority)

時刻認証事業者へ国家時刻標準時に基づく時刻の配信を行い、時刻認証事業者の時刻を監査する信頼できる第三者機関である。

・時刻認証事業者－ＴＳＡ（Time Stamping Authority)

ＴＡから時刻配信を受け、利用者からの要求に応じて時刻証拠となる時刻証明書を作成し発行する信頼できる第三者機関である。

・認証局－ＣＡ（Certification Authority）

ＴＳＡに対して認証、あるいはデジタル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。公開鍵暗号基盤（ＰＫＩ：Public Key Infrastructure）を利用したタイムスタンプ方式には必須である。

・リンク情報公開先

主に新聞会社である。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。リンクトークン方式を用いたタイムスタンプには必須である。

・サービス利用者

電子情報の存在と非改ざん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の発行を要求する利用者と自分ないし他者の取得したタイムスタンプトークンの検証を要求する利用者。

１．３　信頼されるタイムスタンプとは

ＮＴＡで生成された時刻と時刻のトレーサビリティが確保された時計の時刻を使用して付与されるタイムスタンプを「信頼されるタイムスタンプ」と定義する。次章に記載される各事業者における技術・運用基準を満足することで提供される。

ここで時刻のトレーサビリティとは、「電子的環境で使われる時計がＮＴＡで生成された時刻に対する精確性を辿れること」と定義する。

実際に、時刻のトレーサビリティを確保するには、

１．ＮＴＡで生成された時刻を起点とした時刻情報の配信経路が安全に確保されること

２．配信経路上の時計品質が確保されていること

３．上記２項目の安全性が証明可能な手段を有すること

が必要である。

信頼されるタイムスタンプは、その証明力が価値であり、裁判において「紙」に比してどれだけ疑わしい要素を排除することができるかが重要な課題である。各事業者がそれぞれの責務を遂行し相互証明力を高めるため、独立した事業体で運用されることが望ましい。

２．技術･運用基準

２．１　国家時刻標準機関

国家時刻標準機関（ＮＴＡ）は、標準時を生成・維持・配信する機関である。

現在、日本では独立行政法人情報通信研究機構（ＮＩＣＴ）が独立行政法人情報通信研究機構法に基づいて標準時の通報を実施している。ＮＴＡとしての業務は、この法律に基づいて厳格に運用される。

ここで参考として標準時を通報しているＮＩＣＴの技術基準を示す。

（１）　技術基準

	項目	概要	
1	国家時刻標準機関の時計 UTC（NICT）	協定世界時（UTC）の時刻と同期し、時刻差が±５０ナノ秒以内となるよう維持	
		1	UTCの時刻との同期精度 ・同期精度　時刻差が±５０ナノ秒以内
		2	複数原子時計のアンサンブル平均による標準時システム
2	UTCとの連携	国際時刻比較ネットワークに参加、原子時計データをUTCの算出に寄与	
		1	国際時刻比較ネットワーク ・毎日　定時比較を実施、国際度量衡局（BIPM）へデータ提供
		2	比較データの公表とUTC算出へ提供 ・BIPMが発行するCircular T 及びannual Reportに比較結果が公表 ･規定された重み付けによりUTC算出に利用
3	時刻の完全性	UTCに対して時刻差が±５０ナノ秒以内にある事の保証 ・BIPMが発行するCircular T、及び annual Reportに比較結果が公表 BIPMホームページで閲覧可能	
4	時刻配信	UTCの時刻と同期した時刻の提供	
		1	提供形式 ・時刻ラベル、GGTTSデータ等
5	時刻異常への対応	配信時刻の異常検知、配信先に通知する手段の確保	
		1	異常時刻の検知と停止機能
		2	時刻異常の通知機能

２．２　時刻配信事業者

時刻配信業務は、国家時刻標準機関（ＮＴＡ）が運用管理する標準時と比較し、その差が一定の範囲にあることを維持しつつ、生成された時刻情報を安全に安定配信し、配信対象機器の時刻校正記録を保管、提供するサービスである。時刻の配信利用対象者は時刻認証事業者だけでなく、金融・証券業界などの時刻がクリティカルとなる業務を持つユーザ全般となる。ここではそれを踏まえた上で、時刻配信業務の技術基準と運用基準を提供している。

（１）　技術基準

	項目	概要	
1	時刻配信業務の時計	NTAの時刻と同期し、必要十分な時刻精度の維持	
		1	NTAの時刻との同期精度 ・同期精度　±３０ミリ秒以内 ※うるう秒の処理時は例外とする
		2	複数原子時計のシステム構成による高精度システム ・時計の安定度　　±１ｘ１０$^{-9}$　以上（１日）の安定度を有する時計を使用する
		3	うるう秒の処理をUTC（NICT）に同期して適正に行う手段を備える
2	NTAとの時刻比較（NTA-TA）	NTAとの時刻比較	
		1	NTAからの時刻受信精度 ・受信精度　±３０ミリ秒以内
		2	時刻比較用GPSデータ公開ポリシーリンク 表記例＞OID方式　0.2.440.XXXXXX.X.X URL方式　http://www.nict.go.jp/XXXXX/XXXXX ※配信ポリシーリンク：NTAが定める技術上の基準に適合していることをTAが自ら検査し、所定の表示を付すことができる制度
3	時刻の完全性	UTC（NICT）に対して規定する精度内にある事の保証	
		1	UTC（NICT）との時刻比較のためのデータ記録と保管 ・測定したGGTTSデータの記録および保管
		2	受信機器に関する操作記録の保管
4	時刻配信先の機器の特定（認証）	配信対象機器を特定する手段、なりすまし対策	
		1	配信先機器の特定および認証可能な手段をもちいること
		2	配信先機器の特定やなりすまし対策が講じられている手段について確認すること

5	時刻配信 （TA-TSA）	配信経路での改ざん防止、規定する精度内での安定配信	
		1	配信時刻の改ざん防止機能あるいは改ざん検知可能な手段を用いること
		2	対象装置に対する時刻配信・監査の実施 ・時刻配信精度　±５０ミリ秒以内　（平均値）
		3	時刻配信事業者からの配信ポリシーリンク 表記例＞OID方式　0.2.440.XXXXXX.X.X URL方式　http://www.nict.go.jp/XXXXX/XXXXX ※配信ポリシーリンク：TSAに配信される時刻は、NTAが定める技術上の基準に適合していることをTAが自ら検査し、所定の表示を付すことができる制度
6	時刻配信先の機器に対する時刻監査 （TA-TSA）	配信先の機器が正しく運用されている事の時刻監査および計測記録の提供	
		1	対象機器に対する時刻監査の実施 ・時刻計測精度　±５０ミリ秒以内 注：計測能力のみ対象とする ※別途時刻監査規格を事業者毎に定める
		2	時刻監査記録の保管
		3	時刻監査記録情報の改ざん防止
7	時刻異常への対応 （TA-TSA）	時刻配信先の時刻の異常検知、配信先に通知する手段	
		1	時刻異常の通知もしくは配信先機器の稼働停止機能、あるいはそれらを実現する手段を有すること。

（2） 運用基準

	項目	概要	
1	義務	時刻配信事業者自身の信頼性と安全性の確保、配信先に対する適切な情報提供義務	
		1	対象機器に対して時刻の配信および計測を行うこと。
		2	対象機器に対して時刻の配信・時刻監査等を行った事実を証明するための監査証などを発行すること。
		3	配信業務で公開鍵暗号方式を用いる場合は、使用するすべての秘密鍵を安全に生成し、管理すること。
		4	配信業務で公開鍵暗号方式を用いる場合の使用する秘密鍵が危殆化した場合は、速やかにCAに鍵の失効請求を行うとともに加入者に連絡することなどによりTSAの信頼性を確保するための処理を講じること。
		5	配信業務に関する月次レポートを作成し、配信先に提出すること。 ・保管年数　　１０年以上
2	責務	時刻配信事業者自身の責任と保証に関するポリシーの開示	
		1	賠償責任の開示
		2	免責事項の開示
3	組織・人事管理	適切な組織構成及び開発・運用維持、信頼性確保、可用性確保に対処できる能力・体制	
		1	独立性が確保された組織構成
		2	時刻やセキュリティに関する専門性の優れた要員を配置すること。
		3	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。
		4	部署外からの監査等のチェック機能が働くこと
		5	事故発生時に、その発生源が特定できること
4	情報開示	経営情報、技術情報、安全対策実施状況、運用規定、サービス利用規約など	
		1	・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な技術情報の開示。
		2	・運用規定 事業者が規定する運用規定の開示。

		3	・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の開示。
5	機密保持	セキュリティ維持にかかわる機密情報の保持とサービス加入者個人情報の保護	
		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、それに従った運用を行うこと。
		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、それに従った運用を行うこと。
		3	加入者情報や監査情報、設備・システムセキュリティ等々の機密情報を保護する保管設備については、物理的に隔離されていること。
6	業務の中断・終了	業務中断・終了時のサービス加入者への事前通知義務	
		1	サービスを中断・終了時は、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こと。 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。
7	加入者個人情報の取扱い	サービス加入者情報の「利用目的の公開」「保護」「開示ポリシー」	
		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こと。

		3	・個人情報の開示 サービス提供事業者は、加入者個人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。 １．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。 ２．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 加入者個人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手段を備えること。
		5	・保管 加入者個人情報は、不正な改ざん・消去・漏洩等が困難な保管システムの導入、および必要に応じて安全に取り出せる仕組みを備えること。
		6	加入者個人情報は、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体制を備えること。
8	監査	監査情報の定義、保管、頻度、保管期間、監査結果の開示と対処	
		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。加えて時刻配信事業者においては時刻精度の証明を行う必要がある。例えば、監査情報には以下のような情報が含まれる。 １．国家時刻標準機関（NTA）との時刻比較、調整記録 ２．時刻認証事業者（TSA）との時刻比較、調整記録 ３．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 ４．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 ５．サービス提供事業者システムに対する操作記録 ６．サービス提供事業者システムの動作記録 ７．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	・監査の頻度 監査の頻度は、最低年１回実施すること。
		3	・監査情報の保管期間 監査情報は１０年以上保管すること。
		4	・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、以下要件をすみやかに対処すること。 １．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) ２．欠陥への対処
		5	・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改ざん・削除等が困難かつ適切な安全対策を施すこと。
9	システムのトラブル、危殆化、災害からの復旧	代替設備の確保、緊急停止手段、バックアップデータからのリカバリ	
		1	・システムトラブル対処 サービス提供事業者が使用する時計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、システムの緊急停止および復旧作業を速やかに行うこと。
		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こと。
		3	・代替設備の確保 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継続すること。

２．３　時刻認証事業者

時刻認証業務は、ＮＴＡで生成された時刻と時刻のトレーサビリティが確保された時計の時刻を使用して、タイムスタンプトークンを発行し保証するサービスである。その利用者は特定の時刻以前に、当該電子情報が存在した事の証拠を必要とする利用者全般となる。ここでは、それを踏まえた上で信頼されるタイムスタンプトークンを発行する時刻認証事業者の認定基準の項目を提案している。　以下、時刻認証事業者についてデジタル署名技術を使用する方式とデジタル署名技術を使用しない方式の二つに分けて、認定基準を説明する。　なお、各々の方式に該当する方式は下記のとおりである。

・デジタル署名技術を使用する方式

ISO18014-2：独立トークン方式（デジタル署名を用いる方式）

・デジタル署名技術を使用しない方式

ISO18014-2：独立トークン方式（アーカイビング方式）

ISO18014-3：Linked Token 方式

２．３．１　デジタル署名技術を使用する方式

（１）　技術基準

	項目	概要	
1	時刻ソース	タイムスタンプトークン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）や時刻配信者について、利用者が必要に応じて確認できる手段を有すること。	
2	精度	タイムスタンプサーバの時刻ソースはNTAで生成された時刻に対して十分な精度（±１秒以内）を持つ。	
3	精度の証明	タイムスタンプサーバで使用された時計の品質を証明する手段を持つ。	
		1	第三者機関もしくは時刻認証業務とは権限分離された組織・機能がTAとして時刻同期／時刻監査／時刻配信などを行った事実を証明する。 【証明方法例】 １.TAが証明する監査証をタイムスタンプトークンに含める ２.リポジトリに監査証や監査記録を常に公開する
4	タイムスタンプサーバの特定	タイムスタンプサーバを特定する手段および、なりすまし対策を講ずること	
		1	配信元機器の特定および認証可能な手段を用いること
		2	時刻認証サービスを受け付けるサーバの特定が可能な手段を用いること
5	TSAポリシー	タイムスタンプトークンの発行ポリシー（TSAポリシー）について、利用者が必要に応じて確認できる手段を有すること。	
		1	タイムスタンプトークンには、TSAポリシーの識別情報、リファレンス情報、ハッシュ値など、TSAポリシーを一意に特定できる情報を含める。
		2	TSAポリシーの内容は、随時参照可能にしておく。
6	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、運用規定等に明確に定義し、公開していること。	
7	発行者情報	タイムスタンプトークン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トークンに含める。	
8	要求者情報	タイムスタンプトークンにはタイムスタンプの要求者の情報は含まない。	

9	順序性	タイムスタンプトークン内あるいはTSAポリシー内に、タイムスタンプトークンに付加されたシリアル番号や時刻情報の順序に関する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）を示す。		
10	タイムスタンプ対象データ	タイムスタンプトークンには、ハッシュ値などタイムスタンプ対象データを表現する為の情報を含み、タイムスタンプトークンと対象データの照合を可能とする。		
11	非改ざん（完全性）を保証する情報	タイムスタンプトークン自体が改ざんされていないことを確認できるように、MAC、デジタル署名などの情報を添付するか、その他の改ざん検知手段を施す。		
12	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に関する情報をタイムスタンプトークンに含めるか、あるいはTSAポリシーに含める。（デジタル署名の方式を利用する場合）		
			1	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をサポートする。
			2	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をサポートする。
			3	鍵長として、RSAの1024ビット相当以上のものを使用する。
13	秘密鍵	デジタル署名に使う秘密鍵は、HSM（FIPS140-1または140-2のレベル3認定相当以上の製品）を用いて保護する。		
14	証明書	証明書の管理／配布		
			1	利用者の要求によりタイムスタンプトークンの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トークンに含める。
			2	タイムスタンプトークンの生成に公開鍵暗号基盤を利用する場合、第三者機関もしくは時刻認証業務とは権限分離された組織・機能が公開鍵証明書を発行する。
15	安全な通信路	利用者とタイムスタンプサーバ間の通信は、なりすまし、改ざんなどへのセキュリティ対策がなされていること。		

（2） 運用基準

	項目	概要	
1	義務	時刻認証事業者自身の信頼性と安全性の確保、利用者および検証者に対する適切な情報提供義務	
		1	タイムスタンプトークンの生成・発行
		2	時刻認証業務で使用するすべての時計の時刻管理
		3	時刻認証業務で使用するすべての秘密鍵を安全に生成し、管理すること。
		4	時刻認証業務で使用する秘密鍵が危殆化した場合は、速やかに当該秘密鍵の使用を中止するとともに利用者に連絡すること。また、当該秘密鍵とペアになる公開鍵について認証局から証明書の発行を受けている場合には、速やかに失効請求を行うこと。
		5	時刻認証業務を終了する時やTSA証明書の記載事項の変更が有る場合、CAの定める方法によりCAに通知すること。
		6	検証者に対してタイムスタンプトークンの検証に必要な情報を提供すること。
2	責務	時刻認証事業者自身の責任と保証に関するポリシーの開示	
		1	賠償責任の開示
		2	免責事項の開示
3	組織・人事管理	適切な組織構成及び開発・運用維持、信頼性確保、可用性確保に対処できる能力・体制	
		1	業務間の権限分離がされた、独立性が確保された組織構成
		2	時刻やセキュリティに関する専門性の優れた要員を配置すること。
		3	クリティカルデータに接触可能な設備は物理的に隔離されていること
		4	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。
		5	部署外からの監査等のチェック機能が働くこと。
		6	事故発生時に、その発生源が特定できること。
4	情報開示	経営情報、技術情報、安全対策実施状況、運用規定、サービス利用規約など	

		1	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な技術情報の開示。
		2	運用規定 事業者が規定する運用規定の開示。
		3	サービス利用規定 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の開示。
		4	認証局の情報 デジタル署名に公開鍵暗号基盤を用いる場合は、タイムスタンプトークンの検証に必要なTSA証明書と、TSA証明書の検証に必要な一連の情報またはその取得方法などについて、利用者に対して示すこと。利用者へ示す情報の内容に変更があった場合にはすみやかに連絡すること。
5	機密保持	セキュリティ維持にかかわる機密情報の保持と利用者個人情報の保護	
		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、それに従った運用を行うこと。
6	業務の中断・終了	業務中断・終了時の利用者への事前通知義務	
		1	サービスを中断・終了時は、事前に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こと。
		2	サービスを終了する際は、利用者が新たなタイムスタンプトークンを取得するために十分な移行期間（例：半年）を確保できるよう考慮してサービス終了の予告をすること。
		3	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。
7	利用者個人情報の取扱い	利用者情報の「利用目的の公開」「保護」「開示ポリシー」	
		1	利用範囲 サービス提供事業者は、利用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こと。

		3	個人情報の開示 サービス提供事業者は、利用者個人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。 １．利用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。 ２．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 利用者個人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こと。
		5	保管 利用者個人情報は、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備えること。また、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。
		6	利用者関連情報保護 利用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、それに従った運用を行うこと。

8	業務監査	監査情報の定義、保管、頻度、保管期間、監査結果の開示と対処	
		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業務監査を行うために必要な情報をいう。加えて時刻認証事業者においては時刻精度の証明を行う必要がある。例えば、監査情報には以下のような情報が含まれる。 １．時刻配信事業者（TA）との時刻比較・校正記録 ２．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 ３．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 ４．サービス提供事業者システムに対する操作記録 ５．サービス提供事業者システムの動作記録 ６．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 保管すべき監査情報は前述「監査情報の定義」全てを対象とし、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こと。
		3	監査情報の保管期間 監査情報は１０年以上保管すること。
		4	監査の頻度 監査の頻度は、最低年１度行うこと。
		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、以下要件をすみやかに対処する事。 １．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) ２．欠陥への対処

9	システムのトラブル、危殆化、災害からの復旧	代替設備の確保、緊急停止手段、バックアップデータからのリカバリ	
		1	システムトラブル対処 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こと。
		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こと。
		3	代替設備の確保 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継続すること。
		4	タイムスタンプトークン生成用の秘密鍵が危殆化した際の対処 例えば事業者の意図しない形で発行されてしまったタイムスタンプトークンなど、発行済の一部のタイムスタンプトークンをやむを得ず無効化する必要がある場合には、時刻認証事業者は当該タイムスタンプトークンが無効であることを公表するなど利用者へ周知すること。
10	鍵管理	タイムスタンプトークンのデジタル署名生成鍵／検証鍵ペアや通信に使用する暗号化鍵／復号鍵などの安全管理	
		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、複数人管理のもとで行うこと。 なおタイムスタンプトークンへの署名に用いる秘密鍵は、HSM（FIPS140-1または140-2のレベル3認定相当以上の製品）内で生成すること。

		2	秘密鍵の保管 １．鍵生成システムによって生成された鍵は、HSM（FIPS140-1または140-2のレベル3認定相当以上の製品）内に保管すること。 ２．複数人の権限を有する者が揃わなければ、HSM（FIPS140-1または140-2のレベル3認定相当以上の製品）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こと。 ３．秘密鍵がバックアップ可能な場合、運用規定に記載し、バックアップの盗難および漏洩対策として金庫などに保管したり分散管理すること。バックアップの保管および取り出しは複数人立ち会いのもとで実施すること。
		3	鍵の利用 １．保管されている秘密鍵や共通鍵を用いてデジタル署名や復号する際には、HSM（FIPS140-1または140-2のレベル3認定相当以上の製品）内部で安全に処理すること。 ２．HSM（FIPS140-1または140-2のレベル3認定相当以上の製品）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、HSM（FIPS140-1または140-2のレベル3認定相当以上の製品）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こと。
		4	公開鍵の保存 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こと。
		5	鍵の廃棄 １．必要な期間が終了した鍵や、失効した鍵、危殆化した鍵などは、その後の不正利用が行われないように廃棄すること。 ２．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こと。

		6	鍵の定期更新 時刻認証事業者の鍵は、あらかじめ有効期間と活性化期間を設け定期的に更新する。なお、それらの期間設定は時刻認証事業者のポリシーによる。 【期間設定例】 １. 1024 ビット RSA 相当の TSA 秘密鍵を使用し、鍵の有効期間を６年、活性化期間を１年とする事で、最低５年間有効なタイムスタンプトークンを発行する。 ２. 2048 ビット RSA 相当の TSA 秘密鍵を使用し、鍵の有効期間を１１年、活性化期間を１年とする事で、最低１０年間有効なタイムスタンプトークンを発行する。 注意：上記設定例はあくまでも事例であり、その安全性を保証するもではない。期間設定をする際は必ず、署名アルゴリズム、ハッシュアルゴリズムの最新の安全性評価情報を元にして決定する。
		7	鍵の危殆化時／災害時の復旧 １．時刻認証事業者は、時刻認証事業者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時刻認証事業者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こと。 ２．時刻認証事業者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、時刻認証事業者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こと。 ３．タイムスタンプトークンの署名に用いる秘密鍵が危殆化した場合、時刻認証事業者は当該秘密鍵で生成した全てのタイムスタンプトークンが無効となるため、異なる秘密鍵によるタイムスタンプトークンを再取得する必要があることを、利用者に通知する。 ４．時刻認証事業者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こと。

２．３．２　デジタル署名技術を使用しない方式

（１）　技術基準

	項目	概要	
1	時刻ソース	タイムスタンプトークン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）や時刻配信者について、利用者が必要に応じて確認できる手段を有すること。	
2	精度	タイムスタンプサーバの時刻ソースはNTAで生成された時刻に対して十分な精度（±１秒以内）を持つこと。	
3	精度の証明	タイムスタンプサーバの時計の品質を証明する手段を持つこと。	
		1	第三者機関もしくは時刻認証業務とは権限分離された組織・機能がTAとして時刻同期／時刻監査／時刻配信などを行った事実を証明する。 【証明方法例】 １.TA が証明する監査証や監査記録をタイムスタンプトークンに含める ２.リポジトリに監査証や監査記録を常に公開する ３.TSA が監査証や監査記録を電子もしくは紙でもっており、必要に応じて、監査の結果を証明できる。
4	タイムスタンプサーバの特定	タイムスタンプサーバを特定する手段および、なりすまし対策を講じること	
		1	TAから時刻配信を受ける際には、配信元の機器の特定および認証可能な手段を用いること
		2	利用者からタイムスタンプの要求を受け付ける際には、時刻認証サーバを受け付けるサーバの特定が可能な手段を用いること
5	TSAポリシー	TSAポリシーについて、利用者が必要に応じて確認できる手段を有すること。	
		1	タイムスタンプトークンには、TSAポリシーの識別情報、リファレンス情報、ハッシュ値など、TSAポリシーを一意に特定できる情報を含める。
		2	TSAポリシーの内容は、随時参照可能にしておく。
		3	ISOもしくはITUが管理する体系のもとでTSAポリシーに対してオブジェクトIDを適切に発行および付与しなくてはならない。
6	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については、ISO18014に準拠するかもしくはそれと同等の事項を含む形式を明確に定義し、TSAポリシー等に記載し公開していること。	

7	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トークンに含める。	
8	要求者情報	タイムスタンプトークンにはタイムスタンプの要求者の情報は含めない。	
9	順序性	タイムスタンプトークン内あるいはTSAポリシー内に、タイムスタンプトークンに付加されたシリアル番号や時刻情報の順序に関する整合性保証の有無や範囲（例：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）を示す。	
10	タイムスタンプ対象データ	タイムスタンプトークンには、ハッシュ値などタイムスタンプ対象データを表現する為の情報を含み、タイムスタンプトークンと対象データの照合を可能とする。	
		タイムスタンプ対象データの表現として、タイムスタンプ発行者にはその内容が判らないようにハッシュ化処理を施した情報を受け付ける。	
11	ハッシュアルゴリズム	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と鍵長に関する情報をタイムスタンプトークンに含めるか、あるいはTSAポリシーに含める。	
		1	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をサポートする。
12	有効期間	タイムスタンプの有効期間は、ハッシュアルゴリズムが危殆化すると予測される時期以前に終了するよう、ハッシュアルゴリズムの最新の安全性評価情報を元に、全ての発行済みのタイムスタンプについて、任意の時点で適切に設定・変更し、公開すること	
13	安全な通信路	利用者とタイムスタンプサーバ間の通信ではセキュリティ対策（なりすまし、改ざん、盗聴の対策、など）がなされていること	
14	検証で使用される情報の完全性	サーバ内でタイムスタンプ検証に使用される情報については、リンク情報の代表値を明証化する等の手段により改ざんを検知するための技術的な対策を講ずること	

（2） 運用基準

	項目	概要	
1	義務	時刻認証事業者自身の信頼性と安全性の確保、利用者および検証者に対する適切な情報提供義務	
		1	タイムスタンプトークンの生成・発行
		2	時刻認証業務で使用するすべての時計の時刻管理
2	責務	時刻認証事業者自身の責任と保証に関するポリシーの開示を行うこと	
		1	賠償責任の開示
		2	免責事項の開示
3	組織・人事管理	適切な組織構成及び開発・運用維持、信頼性確保、可用性確保に対処できる能力・体制を備えること	
		1	独立性が確保された組織構成とすること
		2	時刻やセキュリティに関する専門性の優れた要員を配置すること。
		3	クリティカルデータに接触可能な設備は物理的に隔離されていること
		4	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。
		5	部署外からの監査等のチェック機能が働くこと。
		6	事故発生時に、その発生源が特定できるような要員を配置すること。
4	情報開示	経営情報、技術情報、安全対策実施状況、運用規定、サービス利用規約など	
		1	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な技術情報の開示。
		2	運用規定 事業者が規定する運用規定の開示。
		3	サービス利用規定 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の開示。
5	機密保持	セキュリティ維持にかかわる機密情報の保持と利用者個人情報の保護	

		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、それに従った運用を行うこと。
6	業務の中断・終了	業務中断・終了時の利用者への事前通知義務	
		1	サービスを中断・終了時は、事前に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こと。
		2	サービスを終了する際は、利用者が新たなタイムスタンプトークンを取得するために十分な移行期間（例：半年）を確保できるよう考慮してサービス終了の予告をすること。
		3	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。
7	利用者個人情報の取扱い	利用者情報の「利用目的の公開」「保護」「開示ポリシー」	
		1	利用範囲 サービス提供事業者は、利用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こと。
		3	個人情報の開示 サービス提供事業者は、利用者個人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。 １．利用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。 ２．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 利用者個人情報へのアクセスは、利用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、権限を有する者だけが行える様にすること。

		5	保管 利用者個人情報は、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備えること。また、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。
8	監査	監査情報の定義、保管、頻度、保管期間、監査結果の開示と対処	
		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。加えて時刻認証事業者においては時刻精度の証明を行う必要がある。例えば、監査情報には以下のような情報が含まれる。 １．時刻配信事業者（TA）との時刻比較・校正記録 ２．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 ３．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 ４．サービス提供事業者システムに対する操作記録 ５．サービス提供事業者システムの動作記録 ６．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こと。
		3	監査情報の保管期間 監査情報は１０年以上保管すること。
		4	監査の頻度 監査の頻度は、最低年１度行うこと。
		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、以下要件をすみやかに対処する事。 １．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) ２．欠陥への対処

9	システムのトラブル、危殆化、災害からの復旧	代替設備の確保、緊急停止手段、バックアップデータからのリカバリ	
		1	システムトラブル対処 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こと。
		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こと。
		3	代替設備の確保 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継続すること。
10	リンク情報の生成	リンク情報を用いる場合は、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	
11	リンク情報の保持	リンク情報を用いる場合は、TSAは、サービス提供中はセキュリティ基準が保証された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	
12	リンク情報の代表値の明証化	リンク情報を用いる場合は、TSAはその正当性を証明するために定期的にリンク情報の代表値を明証化し、明証化時期を合理的に説明できること。	
13	リンク情報の監査	リンク情報を用いる場合は、TSAは、運用時の監査を実施する際に、明証化済みリンク情報の代表値とTSAが実際に管理しているリンク情報の整合性を監査項目に含めなければならない。	
14	検証に必要な情報の保持	TSAは、検証に必要な情報を保持し、その完全性を維持すること	

２．４　時刻認証事業者むけ認証局

時刻認証事業者が TSA 証明書の発行を受ける認証局に対する要件を記載する。

（1）運用基準

	項目	概要	
1	CAの責任	CAは、TSAの管理する秘密鍵が、発行するTSA証明書の公開鍵に対応したものであることを確認すること。 CAは、時刻認証事業者の存在を確認し、発行するTSA証明書の主体者名との関係を証明すること。	
2	CA証明書が失効した場合の対処	TSA証明書の有効期間内にCA証明書が秘密鍵の危殆化などの理由で失効した場合は、CAは直ちに失効処理を行い、TSAに通知を行なうこと。 この際に発生したトラブルに関してはCAが責務を負うこと。	
3	TSA鍵の更新	1	時刻認証事業者に対して、TSA証明書の有効期間よりも短い範囲でTSA秘密鍵の活性化期間を定め、活性化期間終了後は当該秘密鍵を廃棄するよう確認すること。
		2	CAは、鍵の更新に際して、TSAの存在と、証明書の使用目的を確認できること。
		3	CAは、証明書の更新を行うに際して、既存のTSA秘密鍵の破棄を確認できること。
4	TSA証明書の失効	TSA証明書のCRLを定期的に発行し、危殆化時の影響を最小化しているCAであること。 TSA証明書が失効した時などの緊急時には、速やかに新しいCRLを発行できること。	
		1	TSAとして定められた基準を満たさなくなったとき、およびTSAが閉局する場合は、証明書を失効させられること。
		2	CAはTSA証明書の失効に理由コードを記載していること。
5	リポジトリの公開	1	検証情報の公開 常に安全に参照できるリポジトリに、発行した全てのTSA証明書について、信頼の起点となるルート認証局から当該TSA証明書までの証明書チェーンの検証に必要となる一連の証明書情報や失効情報、あるいはその取得方法について利用者に公開すること。また、これらの情報や取得方法に変更があった場合には速やかにリポジトリへ反映させること。

		2	過去の検証情報 1に記した情報または取得方法については、発行した全てのTSA証明書の有効期間終了後も相当期間以上長期にわたって検証できるよう、利用者に対して公開すること。以下に長期にわたって検証可能な失効情報の公開方法の例を示す。 例1) 過去に発行したCRLの履歴を公開する。 例2) 過去の全ての失効情報を常に最新のURLに含めて公開する。
		3	CP、CPS、TSAの審査記録、TSA証明書の発行記録をTSA証明書の失効情報をTSA証明書の有効期限後または相当期間以上長期にわたって、安全に保管し、開示できるようにしていること。
6	CA業務の終了	CAがTSAに対する認証業務を終了する場合、利用者がタイムスタンプを検証するために必要な、5項に定めた情報またはその取得方法を、TSA証明書の有効期限後または相当期間以上長期にわたって参照できるよう、他の信頼できる機関に引き継げるように定めていること。	

２．５　タイムスタンプ検証

（１）　技術基準

	項目	概要	
1	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を実行する。	
2	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。	
3	検証処理	1	検証処理は、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。
		2	エラーメッセージにはエラーの理由を含める。
		3	検証処理は、利用者から送信される検証要求データの形式及びタイムスタンプトークンの妥当性を検査した上で、検証結果データを利用者へ返信する。
4	デジタル署名技術を用いる場合のタイムスタンプトー	1	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。

	クンの妥当性	2	タイムスタンプトークンに公開鍵証明書が含まれない場合、安全なリポジトリからタイムスタンプトークンのデジタル署名に用いられた証明書を取得し、検査する。
		3	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デジタル署名の妥当性を検査する。
5	検証結果データ	1	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か、トークンの識別子を含むこと
		2	検証結果データの中に検証結果を含むこと
6	デジタル署名技術を使用しない方式の場合のリンク情報の検証	1	TSA事業者は、必要に応じてリンク情報の代表値が少なくともいつの時点に明証化されていたか客観的に説明できること
		2	TSA事業者は、必要に応じてタイムスタンプトークンと対応するリンク情報の関係を客観的に説明できること

参加メンバー　ガイドライン分科会

（技術・運用基準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	セイコーインスツル株式会社	柴田　孝一
メンバー	アマノ株式会社	市川　桂介
〃	株式会社ＮＴＴデータ	坂本　弘章
〃	セイコーインスツル株式会社	上畑　正和
〃	セイコープレシジョン株式会社	松丸　宗彦
〃	セイコープレシジョン株式会社	中嶋　勝治
〃	独立行政法人情報通信研究機構	岩間　司
〃	株式会社 PFU	石川　昭一
事務局	財団法人テレコム先端技術研究支援センター	刑部　正敏

【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/