タイムスタンプサービス iScign

運用規程

Rev1.0

改版履歴
CHANGE

Rev.	変更日付	変更箇所	変更内容	発行責任者
1.0	2025 年 8 月 1 日	―	初版作成	iScign 責任者

目次
CONTENTS

1. はじめに

タイムスタンプサービス iScign とは、サイエンスパーク株式会社（以下「当社」という）の運営する時刻認証局が行う電子データに対して信頼のおける時刻のタイムスタンプトークンを付与するサービス（以下「本サービス」という）のことである。

タイムスタンプサービス iScign 運用規程（以下「本規程」という）では、本サービスを利用者に提供するにあたり基本的な事項について定める。

本規程で取り扱うタイムスタンプトークンは、IETF による RFC3161 及び RFC5816 に準拠する。

1.1. 概要

本規程は、当社が令和 3 年総務省告示第 146 号に基づき総務大臣により認定を受けた時刻認証業務を提供するための運用方針及び業務手続きを規定するものである。

本規程の適用対象は、時刻認証局並びに本サービスの全ての利用者、及び本サービスに関係する法人、個人、組織を含み、本規程によって、適用対象の権利と義務を表明する。

時刻認証局は、サービスポリシーと時刻認証局の運用規程をそれぞれ独立したものとせず、本規程を時刻認証局のサービスに関する運用方針として位置付ける。

1.2. 識別

1.2.1. ドキュメント名称、バージョン

ドキュメント名称：タイムスタンプサービス iScign 運用規程

バージョン：1.0 版

適用開始日：2025 年 8 月 8 日

作成者：サイエンスパーク株式会社

1.2.2. オブジェクト識別子

本規程において適用するオブジェクト識別子（OID、URL）は以下とする。

本サービス	
サイエンスパーク株式会社	0.2.440.200356
タイムスタンプサービス iScign	0.2.440.200356.1
時刻認証局サービスポリシー	0.2.440.200356.1.1
認定タイムスタンプ by iScign	0.2.440.200356.1.1.1

本時刻認証局が利用する認証局のポリシー	
GlobalSign 認証業務運用規程	https://jp.globalsign.com/repository/

本時刻認証局が利用する認証局のポリシー	
GlobalSign nv/sa(グループ共通)	1.3.6.1.4.1.4146
CP/CSP 群	1.3.6.1.4.1.4146.1
Timestamping Certificates Policy – AATL	1.3.6.1.4.1.4146.1.31
Hosted Timestamping Certificates Policy – AATL	1.3.6.1.4.1.4146.1.35

1.3. 定義

1.3.1. 用語の定義

(1) 時刻認証局（TSA）

本規程において時刻認証局とは、時刻ソースから時刻の提供を受けて、RFC3161 及び RFC5816 に基づくタイムスタンプトークンプロトコルに準拠したタイムスタンプトークン発行業務を行う事業者をいう。

(2) 認証局（CA）

本規程において認証局とは、公開鍵基盤（PKI)の認証局（CA）であり、時刻認証局が使用する公開鍵証明書の認証を行う事業者をいう。

本時刻認証局の認証局は以下のサービスを利用する。

a) GMO グローバルサイン株式会社が運営する「GlobalSign 認証業務」

「GlobalSign 認証業務」の認証局は、GMO グローバルサイン株式会社のグループ会社である、GlobalSign NV となる。

（注）電子証明書（TSA 証明書）では GlobalSign nv-sa と表記。

(3) 利用者

本規程において利用者とは、時刻認証局の提供するサービスへの加入申請を行い、時刻認証局からサービスへの加入を認められ、そのサービスを受ける者をいう。

(4) 検証者

本規程において検証者とは、時刻認証局の提供するタイムスタンプトークンの有効性について公開鍵証明書や失効情報などをもとに検証する者をいう。

(5) タイムスタンプトークン

本規程においてタイムスタンプトークンとは、利用者から送付されたハッシュ値に対し、信頼性の高い時刻を用い、そのデータが、ある時刻に存在し、以降変更や改ざんなどされていないことを証明できる情報をいう。デジタル情報を一意に特定するためのハッシュ値に対して、署名を付与することでタイムスタンプトークンが生成される。

(6) リポジトリ

本規程においてリポジトリとはタイムスタンプサービスの提供に必要な関連情報を格納するオンライン上のデータの置き場所のことをいう。

(7) 国立研究開発法人 情報通信研究機構(NICT)
日本標準時および標準周波数を定め、維持する公的機関で、国際的に定義された「秒の定義」にしたがって原子時計から、協定世界時との差が±10 ナノ秒になるように日本標準時を生成・比較・供給する。本サービスは、NICT から供給される時刻源を参照して、時刻の正当性を維持する。

(8) Adobe Approved Trust List（AATL）
米アドビシステムズが管理している信頼ルート証明書のリスト。このリストに公開されている認証事業者が発行する証明書を使用することで Adobe 製品での文書の有効性確認が容易となる。

1.3.2. 時刻認証サービスの内容

本サービスの内容は以下とする。

(1) 時刻認証局は、利用者の依頼に基づき、利用者から送付されたハッシュ値に対して RFC3161 及び RFC5816 に基づいたタイムスタンプトークンを生成し、発行する。
   a) 利用者から送付されるハッシュ値に対して適用されるハッシュアルゴリズムは最新の「電子政府推奨暗号リスト」に準拠した SHA-256・SHA-384・SHA-512 とする。
   b) タイムスタンプトークンの署名アルゴリズムは、6.1.1.(4)で規定された方式を用いる。
   c) 時刻認証局は、利用者から送付されたハッシュ値の元データの内容については一切関知しない。
   d) タイムスタンプトークンには利用者を特定する情報は含まれない。
   e) 時刻認証局と利用者間の通信は、セキュリティを考慮した方法で行い、予め規定された通信要件に従ってデータの受け渡しを行う。手順の詳細については別途規定する。

(2) タイムスタンプトークンに含まれる時刻は本規程に基づいて以下の条件で付与する。
   a) タイムスタンプトークンに含まれる時刻は、当該時刻を生成するタイムスタンプサーバの内部時計（以下、「TSA 時計」という。）により生成される。
   b) TSA 時計は、NICT により提供される光テレホン JJY サービスを使用して UTC（NICT）に同期する。また、時刻精度に影響を及ぼす脅威からの保護等により、UTC（NICT）に対し±1 秒以内の誤差で同期することを保証する。
   c) TSA 時計が定められた誤差範囲を超えて異常がある場合には、該当のタイムスタンプサーバにおけるタイムスタンプトークンの生成を停止する。
   d) ±1 秒の誤差範囲内においては、タイムスタンプトークンに記載された時刻の順位に有意性はないものとする。また、シリアル番号についても複数のタイムスタンプサーバによって発行されることから有意性はないものとする。
   e) タイムスタンプトークンに含まれる時刻は、タイムスタンプサーバがタイムスタンプトークン発行要求を受け付けた時刻ではなく、タイムスタンプトークン生成処理において TSA 時計から取得した時刻を表すものとする。
   f) タイムスタンプ要求の受付順位とタイムスタンプトークンの作成順位(時刻の順位)が等しいことは保証されない。

(3) 本時刻認証局の発行するタイムスタンプトークンには有効期間がある。

a) タイムスタンプトークンの有効期限は、タイムスタンプトークンを付与した時刻からタイムスタンプトークンの署名に使用した TSA 証明書の有効期限までとする。

b) 上記の有効期間は 10 年間以上とする。ただし、秘密鍵の危殆化や暗号アルゴリズムの脆弱化が発生した場合には、TSA 証明書の失効などによってタイムスタンプトークンに示される有効期限より以前にその有効性を失効させることがある。

c) 有効期限を超過したタイムスタンプトークンは、その信頼性を裏付けるものではない。

(4) うるう秒が発生した場合、TSA 時計が UTC(NICT)に対し±1 秒以内の誤差で同期していることを保証できない。そのため、サービス提供中にうるう秒を考慮した調整は行わず、うるう秒発生前にサービスを一時停止し、うるう秒発生後に時刻同期・精度について問題がない事を確認した上で、サービスを再開する。うるう秒発生有無の把握については、定期的に規定の手続きで確認する。

1.3.3. タイムスタンプトークンの適用範囲

(1) 適正な用途

タイムスタンプトークンは、時刻認証局の利用者が所持する電子データのハッシュ値に対して、当該ハッシュ値に対応する電子データがタイムスタンプトークンに含まれた時刻の状態であること及びその時刻以前に存在していたことの確認を目的とし、利用者はその用途でのみタイムスタンプトークンを利用できる。また、利用者がタイムスタンプトークンの複製・配布をすることは可能とする。

(2) 禁止される用途

利用者は、前号の目的以外でタイムスタンプトークンを使用することはできない。

1.4. 本規程に関する問い合わせ先

名称：サイエンスパーク株式会社

英語名称：SciencePark Corporation

所在地：〒252-0029 神奈川県座間市入谷西 3-24-9

問い合わせフォーム：https://sciencepark.co.jp/contact

電話番号：046-255-2544

2. 一般規定

2.1. 義務

2.1.1. 時刻認証局の義務

時刻認証局は、本サービスの提供にあたって本規程に従い、利用者に対して以下の業務を遂行する義務を負い、また 2.2.に規定する責任を負う。

(1) タイムスタンプトークンの生成・発行

時刻認証局は、本規程に基づいてタイムスタンプトークンを生成し、利用者に対して発行する。

(2) 時刻の管理

時刻認証局は、発行するタイムスタンプトークンに含まれる時刻が規定する誤差を超えないようにタイムスタンプサーバの時刻管理を行うとともに、時刻認証局で用いる全ての時計の時刻を十分な精度に維持するためにタイムスタンプサーバ以外の機器における時計についても同様に時刻管理を行う。

(3) セキュリティ管理

時刻認証局は、本サービスを提供するためにシステムを安全に維持管理する。

(4) 秘密鍵の公開鍵証明書の失効申請と届出

秘密鍵または暗号アルゴリズムが危殆化し、またはそのおそれが生じた場合、時刻認証局はただちに本サービスを停止し、当該秘密鍵の公開鍵証明書の失効を認証局に申請後、速やかに利用者へ連絡する。また、秘密鍵が危殆化した場合以外での理由で秘密鍵の失効を行う場合、時刻認証局は、利用者に対して事前に連絡を行うこととする。なお利用者への連絡方法等は、2.3.4.に定めるとおりとする。

(5) 認証事業者への通知

認定業務を終了する時や用いる電子証明書の記載事項に変更がある場合、認証事業者が定める方法で認証事業者へ通知する。

(6) 検証者への連絡

検証者への連絡はリポジトリ公開によって行う。

2.1.2. 利用者の義務

利用者は本サービスの加入にあたって本規程を了承した上で次の義務を負い、また、本規程に基づいて時刻認証局より発行されたタイムスタンプトークンを使用する場合、タイムスタンプトークンの対象となった電子データとその電子データに対して付与されたタイムスタンプトークンを使用した結果に対する責任を負うものとする。

(1) タイムスタンプトークンの利用制限の遵守

タイムスタンプトークンはその目的、適用範囲等などを記載した本規程に基づいて発行されており、利用者はこれを十分に理解した上でタイムスタンプトークンを利用しなければならない。

(2) 本規程の遵守

利用者は本規程を遵守するとともに、タイムスタンプトークンを複製・配布する場合はその利用者に対して本規程を遵守させなければならない。

(3) リポジトリ又は通知の確認
利用者は、リポジトリ又は時刻認証局からの通知の情報を定期的に収集しなければならない。
(4) 利用者情報の変更通知
利用者は、利用申込書に記載した利用者情報の内容に変更が生じたときは、ただちにその変更内容を書面で当社に通知するものとする。

2.1.3. 認証局の義務

時刻認証局の認証局は時刻認証局への証明書発行サービスにおいて、時刻認証局に対して次の義務を負う。
(1) 長期保存を目的としたタイムスタンプトークンの発行用に時刻認証局の公開鍵証明書を発行する。なお当該証明書の有効期間は本規程に従って設定されるものとする。
(2) 認証局の秘密鍵を安全に保持し、万一秘密鍵が危殆化した場合は、ただちにその旨を時刻認証局に通知する。
(3) 公開鍵証明書の失効リストおよび公開鍵証明書発行に関連するその他の情報をただちに時刻認証局へ通知する。また、時刻認証局から公開鍵証明書の失効申請があった場合はただちに公開鍵証明書の失効を行う。

2.1.4. リポジトリに関する義務

時刻認証局は本サービスに関する情報のうち公開する情報を 2.5.で規定される方法でリポジトリに公開する。

2.2. 責任

2.2.1. 時刻認証局の損害賠償責任

本サービスに関する当社の責任は、「2.1.1 時刻認証局の義務」に記述する範囲に限られるものとし、適用される法令により許容される最大限の範囲において、当社は賠償責任その他の保証および責任を負わないものとする。また、法令により強制される場合であっても、賠償総額は利用申込書に記載するサービス料金相当額を超えないものとし、当社の責に帰することのできない事由から生じた損害、逸失利益、当社の予見の有無を問わず特別の事情から生じた損害、間接損害、派生的損害、付随的損害、データ・プログラムの喪失については、当社は賠償責任を免れるものとする。

2.2.2. 免責事項

2.2.1.の規定にかかわらず、以下のいずれかに該当する場合においては、時刻認証局は賠償義務を負わないものとする。
(1) 時刻認証局が本規程ならびに個別のサービス契約に従い、本サービスを適正に遂行していた場合
(2) 利用者の故意、過失もしくは違法行為に起因して損害が発生した場合

(3) 利用者による本規程もしくは個別のサービス契約への違反に起因して損害が発生した場合
(4) 利用者のシステムに起因して損害が発生した場合
(5) 次にあげる時刻認証局の支配を超えた事由に起因して損害が発生した場合
(6) 火災、地震、噴火、津波、台風等の天災地変
(7) 戦争、暴動、変乱、争乱、労働争議
(8) 放射性物質、爆発性物質、環境汚染物質
(9) 通信回線の不通
(10) その他の時刻認証局の支配を超えた事由
(11) 4.3.1、4.3.2.および 4.4.に定める事由により本サービスの一時停止または終了が発生した場合
(12) 時刻認証局が一般的な認証事業者の知見および技術水準に照らし解読困難とされている暗号その他のセキュリティ手段を用いていたにもかかわらず、当該暗号が解読され、またはセキュリティ手段が破られた場合
(13) 4.7.3.に記載のタイムスタンプトークンの失効に起因して損害が発生した場合

2.3. 解釈および執行

2.3.1. 準拠法

本規程の解釈および有効性等は、日本法に準拠する。

2.3.2. 可分性

本規程のある規定もしくはその一部、あるいはその適用が、何らかの理由により無効又は執行不可能であると判明した場合、当該規程又は当該範囲のみが無効又は執行不可能となり、本規程の他の部分は有効でありかつ適用される。

2.3.3. 存続性

時刻認証局による本サービスが終了し、本規程が廃止された場合であっても、本規程の 2.2.、2.3.、2.6.、2.7.の効力は有効に存続する。

2.3.4. 通知

(1) 利用者から時刻認証局への通知

書面又は電子メールによって、「1.4 本規程に関する問い合わせ先」に基づき特定される宛先に行い、通知は受領日をもって有効とする。

(2) 時刻認証局から利用者及び検証者への通知

時刻認証局から利用者への通知は、利用申込書に基づき利用者が登録した連絡先へ発信した時点で通知したものとする。利用者は連絡先を変更する場合、速やかに時刻認証局に届け出るものとし、当該届け出がなされない場合においては、時刻認証局は届け出がなされている通知先へ通知することにより、通知

義務を履行したとみなす。また、公式ホームページのお知らせを通じて利用者および検証者に通知する。

2.3.5. 紛争解決

本規程の解釈及び適用等は、日本国法に準拠する。本規程又は時刻認証局による本サービスに関して生じた紛争を法廷にて解決を図る場合は、東京地方裁判所を第一審の専属的合意管轄裁判所とする。本規程又は本規程に定められていない事項に関して協議の必要がある場合、各当事者は誠意を持って協議するものとする。

2.4. 料金

別途、本サービスの料金表に規定する。

2.5. 公開とリポジトリ

2.5.1. 時刻認証局に関する情報の公開

時刻認証局は、2.5.4.に定めるリポジトリに次の情報を公開する。

(1) 本運用規程
(2) 公開鍵証明書情報（ルート認証局や中間認証局を含む）
(3) 告知情報（公開鍵証明書失効情報を含む）
(4) 検証に必要な情報
(5) 利用約款およびサービス利用の注意事項

2.5.2. 更新の頻度

公開する情報の更新頻度は以下とする。

(1) 時刻認証局運用規程の変更の都度
(2) その他時刻認証局の責任者が必要と判断したとき

2.5.3. アクセス制御

時刻認証局のリポジトリ上で公開する情報は、インターネットを通じて提供するものとし、情報公開にあたって特段のアクセス制御は行わない。

2.5.4. リポジトリ

2.5.1.に定める情報を下記リポジトリに公開する。

URL：https://sciencepark.co.jp/iscign-repository/

2.6. 機密保持

2.6.1. 機密扱いとする情報

時刻認証局は、漏えいによって時刻認証局、利用者又は認証局の認証業務の信頼性が損なわれるおそれ

のある情報を機密扱いとし、次の情報は機密扱いとする情報に含まれるものとする。
(1) 申し込みに関する記録(承認の可否は問わない)
(2) 時刻認証局が保管するセキュリティ検査ログ
(3) 不測の事態に対応する計画および実施措置
(4) ハードウェアおよびソフトウェアの運用、ならびに時刻認証局の運営についてのセキュリティ対策
(5) 時刻認証局が利用者に提供した利用者を識別するための情報
利用者は、本サービスを受けるにあたって時刻認証局から提供された利用者を識別するための情報を開示・漏洩してはならない。

2.6.2. 機密扱いとしない情報

2.6.1.の規定にかかわらず、次の各号に定める情報については機密扱いとはしない。
(1) 公開鍵証明書、失効情報、本規程等、公開する情報として明示的に示すもの
(2) 開示の時点で、被開示者の責によらずして公知となった情報
(3) 開示後、被開示者の責によらずして公知となった情報
(4) 第三者から秘密保持義務を負うことなく適法に入手した情報
(5) 被開示者が、開示された情報によらずして独自に開発した情報
(6) 開示者が第三者に対し、秘密保持義務を課すことなく開示した情報

2.6.3. 機密情報の保管・管理

時刻認証局は、機密扱いとする情報について、当該情報を含む書類及び記憶媒体の管理責任者を定め、適正な保護のため措置を講じた上で安全に保管する。機密扱いとする情報は、本規程又はサービス契約に開示することを定めている場合を除いて、原則として開示、漏えいしないとともにサービスの範囲を超えて使用しないものとする。

2.6.4. 機密情報の保存期間

時刻認証局は、発行したタイムスタンプトークンが有効である期間、対象となる機密情報を保存する。

2.6.5. 機密情報の廃棄

時刻認証局は、廃棄対象となる機密情報を含む書類・記憶媒体については、所定の手順に基づいて適切かつ安全に廃棄処理を行う。

2.6.6. 機密情報の開示

時刻認証局は、法執行機関から法的根拠に基づいて機密情報を開示するように請求があった場合は、法の定めに従い当該法執行機関へ当該情報を開示する。
また、時刻認証局が業務の一部を第三者に委託する場合、機密情報を委託先に開示することがあるがその場合は委託契約の中で守秘を義務付けるものとする。

2.7. 知的財産権

以下の各号に定めるものを含み、時刻認証局が作成した文書、データ、プログラム等に関する特許権、実用新案権(これらの登録を受ける権利を含む)、商標権および著作権(以下、知的財産権と呼ぶ)は時刻認証局またはそのライセンサーに帰属し、利用者その他の者には移転しないものとする。

(1) 時刻認証局から発行されたタイムスタンプトークン

(2) 本運用規程

2.8. 個人情報の取り扱い

時刻認証局は、本サービスの利用契約締結時に利用者から提供される個人情報を、以下に沿って取り扱うものとする。ただし、法令に定められた場合はこれに限らない。

2.8.1. 個人情報の定義

時刻認証局は、利用者から提供された情報のうち、個人の識別が可能な情報を個人情報として扱う。

2.8.2. 個人情報の取得

時刻認証局は、利用者から必要な範囲を超えて個人情報の取得は行わない。

2.8.3. 個人情報の利用

時刻認証局は、利用者から提供された個人情報を本サービスの提供のために利用する。なお利用者から別途承諾を得た場合、本サービスに関連したサービス等の案内のために利用することがある。
ただし、上記に規定される目的以外に個人情報を利用しない。

2.8.4. 個人情報の保管・管理

時刻認証局は、個人情報について、当該情報を含む書類及び記憶媒体の管理責任者を定め、適正な保護のため措置を講じた上で安全に保管する。個人情報は、本規程又はサービス契約に開示することを定めている場合を除いて、原則として開示、漏えいしないとともにサービスの範囲を超えて使用しない。

2.8.5. 個人情報の保存期間

時刻認証局は、サービスが継続している期間、対象となる個人情報を保存し、サービス解約時まで保存する。

2.8.6. 個人情報の廃棄

時刻認証局は、利用者のサービス契約終了に伴い、利用者から提供された個人情報をサービス提供のために利用する必要がなくなった場合は、速やかに廃棄する。

2.8.7. 個人情報の開示

時刻認証局は、法執行機関から法的根拠に基づいて個人情報を開示するように請求があった場合は、法の定めに従い当該法執行機関へ当該情報を開示する。また、個人情報について本人から開示、訂正もしくは廃棄を求められた場合、合理的な範囲内で対応する。

3. 識別と認証

3.1. 初期登録

3.1.1. 名前の型

タイムスタンプサーバ用の公開鍵証明書の主体者名は、認証局により X.500 識別名（DN: Distinguished Name）の形式に従って設定されるものとする。

3.1.2. 名前の意味

時刻認証局が発行するタイムスタンプトークンに記載されるタイムスタンプサーバの固有名称は、認証局が発行したタイムスタンプサーバ用の公開鍵証明書に記載された名称とする。

3.1.3. 名前の一意性

時刻認証局が発行するタイムスタンプトークンに記載されるタイムスタンプサーバの固有名称は、タイムスタンプサーバ毎に認証局により一意に割り当てられるものとする。

3.2. 利用申請者の認証と利用可否

時刻認証局は、合理的な範囲内で本サービスの利用申請者の真偽を確認し、利用可否を判断する。

3.3. サービスの加入更新

本サービスの契約更新時における識別と認証は 4.2.において定める手続きに基づいて行う。

3.4. サービスの解約申請

本サービスの解約時における識別と認証は 4.3.4.において定める手続きに基づいて行う。

4. 運用規則

4.1. サービスの提供時間

時刻認証局は以下の場合を除き、24 時間 365 日のサービス提供を行う。

(1) あらかじめ通知したサービスメンテナンス期間

(2) 緊急メンテナンス時

(3) うるう秒処理時

4.2. サービスの利用

4.2.1. サービスの利用申請

本サービスの利用を申請する者は、時刻認証局が用意する本サービス利用に関する契約を締結しなけれ

ばならない。
時刻認証局は、当該契約の締結に先立って、当該利用申請者に対する審査を行い、サービスを提供することが適当であると判断した場合は、当該利用申請者との本サービスの利用に関する契約の申し込みを承諾し、当該契約を締結するとともに、本サービスを利用するにあたり利用者を識別するための情報を提供する。

4.2.2. タイムスタンプ要求

本サービスの利用者は、電子データのハッシュ値を含むタイムスタンプ要求を本時刻認証局へ送付するものとする。本時刻認証局と利用者間の通信手段にはなりすまし対策を講じ、認定業務を特定するための手段を用いる。通信要件については別途規定する。
また、タイムスタンプ要求はタイムスタンプトークン発行以外の目的で行ってはならない。

4.2.3. タイムスタンプトークンの発行

本時刻認証局は、利用者からのタイムスタンプ要求があった場合、その要求が正しく受け付けられたか否かの状態（status）を返す。タイムスタンプ要求が正常に受け付けられた場合は、その要求に応じてタイムスタンプトークンの発行処理を行う。ハッシュ関数には SHA512 を使用する。

4.2.4. タイムスタンプトークンの検証

タイムスタンプトークン又はこれを含むデータを受領した者は、以下に示す方法でタイムスタンプトークンの有効性検証を行うものとする。なお、タイムスタンプトークンの検証は、一般にはタイムスタンプの検証ツールを用いて行う。

(1) タイムスタンプのデータ形式の崩れの判別
タイムスタンプのデータ形式は RFC3161 の中で TimeStampToken というバイナリ形式の ASN.1 データ構造として定義されている。この TokeStampToken を解析し、ASN.1 文法に従っていることを確認することでデータ形式の崩れを判別する。

(2) タイムスタンプに TSA 証明書が含まれない場合の証明書一式の取得
タイムスタンプ要求で証明書チェーンを含めるフラグを設定した場合（certReq=true）は、トークンには TSA 証明書からルート証明書までの証明書チェーンが含まれる。
しかし、これをオフに設定した場合（certReq=false 又は未指定）には含まれないため、別途リポジトリより証明書一式をダウンロードして取得する。

(3) TSA 証明書の有効性の検証
RFC 5280 6 章 認証パス検証で規定された方法により TSA 証明書、中間 CA 証明書、ルート証明書の証明書チェーンの有効性を検証する。検証対象データに利用可能な失効情報が含まれない場合には、証明書に記載された情報をもとに失効情報を取得し、失効検証を行う。また、TSA 証明書がタイムスタンプの発行に使用可能な証明書であることも検証する。

(4) TSA 証明書によるタイムスタンプのデータ形式の改ざんの判別
TSA 証明書を用いて RFC5652 CMS SignedData であるタイムスタンプの署名フォーマットの署名を検証する。

(5) タイムスタンプ対象となる電子データの改ざんの判別
上記(1)~(4)によって、タイムスタンプ自体の有効性が確認できていることを前提とする。
タイムスタンプに含まれる対象データのハッシュ値と対象データ自体から算出したハッシュ値が一致していることを確認する。一致していた場合、当該タイムスタンプが対象データのものであることが判明し、タイムスタンプの記載時刻に対象データがなく存在していたことが証明できる。

4.3. サービスの一時停止と解約と変更

4.3.1. サービスの一時停止

時刻認証局は、サービスの一時停止の必要が発生した場合は、事前にそのスケジュールと手続きを決め、停止日の 30 日前までに公知、もしくは利用者へ通知する。
ただし、下記の事由が発生した場合は、予告なしに本サービスを一時停止することができるものとする。
(1) 火災、停電、不正アクセス等の事故により本サービスの中断がやむを得ない場合
(2) 保守、運用上の点検整備又はセキュリティ管理上中断がやむを得ない場合
(3) 認証局が一時停止又は終了し、時刻認証局が一時停止を判断した場合
(4) システム構成の重大な故障やその他システムに関する重大な障害が発生し、業務を継続することにより被害が拡大するおそれがある場合
(5) 時刻認証局の秘密鍵の漏洩、偽造又は変造など本サービスのシステム全体等に重大な障害を与える可能性がある事由が発生した場合

4.3.2. 利用者におけるサービスの一時停止

サービス利用料金の支払期日を経過しても、利用者から支払いがない場合、時刻認証局は、事前に利用者に告知した上で翌月以降の本サービスの利用を停止することができるものとする。
また、下記の事由が発生した場合は、予告なしに本サービスを一時停止することができるものとする。
(1) 利用者の債務不履行により、該当利用者に対する本サービスの提供を中断する場合
(2) 利用者が本サービスの利用の一時停止を申請した場合
(3) 利用者が違法に、又は明らかに公序良俗に反する態様において本サービスを利用した場合
(4) 利用者が他の本サービス利用者に支障を与える態様において本サービスを利用した場合

4.3.3. サービスの一時停止の解除

本サービスの提供を一時停止した理由が解決した場合、所定の手続きによる確認後に本サービスの一時停止の解除を行い、公知、もしくは利用者へ通知する。

4.3.4. サービスの解約

時刻認証局は、下記の事由が発生した場合に本サービスの解約ができるものとする。

(1) 利用者が加入の解約を申請した場合

(2) 利用者が本規程に違反し、相当の期間を定め催告をしたにもかかわらず、改善が見られない場合

(3) 時刻認証局が本サービスを終了する場合

(4) 利用者に以下の事由が発生した場合

a) 手形交換所の不渡り処分を受け、又は金融機関からから取引停止処分を受けたとき

b) 監督官庁から営業の取り消し、停止等の処分を受けたとき

c) 第三者から仮差押、仮処分、強制執行等を受け、本規程の履行が困難と認められるとき

d) 破産の申し立て、商法上の整理開始の申し立て、特別清算開始の申し立て、再生手続き開始の申し立て又は会社更生手続き開始の申し立ての事実が生じたとき

e) 解散、合併又は営業の全部若しくは重要な一部の譲渡の決議をしたとき

f) 財産状態が悪化し又はそのおそれがあると認められる相当の事由があるとき

g) 第三者の支配下に実質的に入り、時刻認証局の利益を損なうと認められるとき

上記の事由により本サービスが停止した場合、時刻認証局は利用者に対して利用者の責によって被った損害賠償の請求ができるものとする。

4.3.5. 変更の認定

時刻認証局は認定業務の変更（軽微な変更を除く）を行うときに、あらかじめ総務大臣への申請を行い、変更に対する認定を受けることとする。また、認定を受けた場合は、その内容を利用者及び検証者へ通知または連絡する。

4.3.6. 名称及び住所並びに代表者の氏名の変更

(1) 時刻認証局は、名称及び住所並びに代表者の氏名に変更がある場合、以下の事項を記載した文書を総務大臣に提出する。

a) 届出に係る認定業務の名称

b) 変更前の名称（英語表記含む）及び住所並びに代表者の氏名（英語表記含む）

c) 変更後の名称（英語表記含む）及び住所並びに代表者の氏名（英語表記含む）

d) 変更の理由

e) 変更しようとする年月日

(2) 前項により総務大臣への届け出を行った場合、その内容を利用者及び検証者へ通知または連絡する。

4.4. サービスの終了

(1) 時刻認証局は以下の何れかの事由が生じたときに、本サービスを終了することができるものとする。サービスの終了とは、時刻認証局の終了を意味する。

a) システム構成機器の重大な故障やその他システムに関する重大な障害が発生し、業務を継続することにより被害が拡大するおそれがある場合
b) 時刻認証局の秘密鍵の漏洩、偽造又は変造など本サービスのシステム全体等に重大な障害をあたえる可能性がある事由が発生した場合
c) 認証局が一時停止又は終了し、時刻認証局が本サービスを継続することが困難となった場合
d) その他時刻認証局が本サービスを終了すべきと判断する事由が発生した場合

(2) 本サービスの終了が決定した場合は、タイムスタンプトークンの検証に必要な情報の継続的な提供と利用者及び検証者を保護するために十分な内容を含む終了計画と併せて、原則として本サービス終了 90 日前までに、総務大臣に届け出るとともに、利用者に公開又は通知する。
通知又は連絡する内容には、以下の情報を含めることとする。
a) 廃止しようとする認定業務の内容
b) 廃止しようとする年月日
c) 廃止理由
d) 廃止しようとする認定業務に関する利用者及び検証者からの苦情又は相談に応ずる連絡先
e) 廃止する認定業務に係る役務の代替となる役務に関する情報（当該認定業務に係る役務と当該代替となる役務との比較検討が可能となる情報を含む）
f) 廃止しようとする認定業務に係る役務に関する利用者及び検証者の被害の発生又は拡大の防止に資する情報
廃止しようとする認定業務に係る役務に関する利用者及び検証者の被害の発生又は拡大の防止に資する情報は、リポジトリに公開する。廃止しようとする認定業務に係る役務の代替となる役務に関する情報、廃止しようとする認定業務に関する利用者及び検証者からの苦情又は相談に応ずる連絡先は、リポジトリに公開する。

(3) 本サービス終了決定後、速やかに全てのタイムスタンプサーバの秘密鍵を安全に廃棄する。

(4) 本サービス終了後、速やかに全ての個人情報を削除する。

4.5. 適合性監査

4.5.1. 監査頻度

時刻認証局は監査人による監査を年 1 回定期的に実施するものとする。また、時刻認証局は必要に応じて定期監査以外に監査を実施する。

4.5.2. 監査人の身元・資格

時刻認証局の監査人には、当社の監査業務及び認証業務に精通した者を任命する。必要に応じて外部の監査人に監査を依頼する場合がある。監査人の任命は時刻認証局の責任者が行う。

4.5.3. 監査人と被監査部門との関係

時刻認証局の監査を実施する監査人には、時刻認証局の業務を直接担当しない者を選定する。

4.5.4. 監査テーマ

本サービスが総務省の時刻認証業務の認定に関する実施要項に準拠して実施されていること、並びに適切な運用や不正アクセスに対する措置が適切に講じられていることを中心に監査を実施する。

4.5.5. 監査指摘事項への対応

時刻認証局は、重要又は緊急を要する監査指摘事項について、時刻認証局の責任者の決定に基づき速やかに対応する。運用している時刻に異常が確認された時やタイムスタンプサーバの秘密鍵の危殆化に関する指摘があった場合は緊急事態と位置付け、緊急時対応の手続をとる。重要又は緊急を要する監査指摘事項が改善されるまでの間、時刻認証局のタイムスタンプサーバの運用を停止するか否かは時刻認証局の責任者が決定するものとする。運用の停止が必要な場合はリポジトリを介して公知、もしくは 2.3.4（通知）に基づき利用者へ通知する。また時刻認証局の責任者は、時刻認証局が監査指摘事項に対して対策を実施したことを確認する。

4.5.6. 監査結果の報告

時刻認証局の監査結果は、監査人から時刻認証局の責任者に対して監査報告書として提出される。
時刻認証局の責任者は速やかに監査結果を総務大臣に報告する。

4.6. アーカイブ

4.6.1. アーカイブの種類

アーカイブデータは、次のものとする。なお（）内の年数は保管期間を表す。
保管は、発行したタイムスタンプトークンが有効である間は最低限保証する。

(1) TSA 時計の UTC（NICT）との同期および参照時刻との比較記録等、タイムスタンプトークンに付与される時刻の品質を証明する記録（11 年 3 か月）
(2) タイムスタンプトークン生成に使用する鍵ペアの生成・失効記録並びに秘密鍵廃棄の記録（11 年 3 か月）
(3) 時刻認証局システムの動作異常の記録（11 年 3 か月）
(4) 適合性監査報告書（11 年 3 か月）
(5) その他、時刻認証業務の運用に関する重要な記録（11 年 3 か月）

4.6.2. アーカイブデータの保護

アーカイブデータは、所定の方法・手順により改竄、削除、外部への流出等から保護する。また、温度、湿度、磁気などの環境を考慮して保管する。

4.6.3. アーカイブデータの保管

アーカイブデータは保管期間を通じて可読な状態で保管する。

4.6.4. アーカイブデータの開示

時刻認証局は、時刻の品質を証明する記録を利用者および検証者の求めに応じて、「2.3.4 通知」に基づき開示する。

4.7. システムトラブルと危殆化、災害からの復旧

認定業務の確実性又は安定性を損なうおそれがある事態が発生又は発覚した場合の利用者及び検証者への通知又は連絡は、電話や電子メール、ホームページ等の日常的に利用でき、かつ広く周知を図ることができる方法により行い、通知又は連絡の内容については事態への対処状況又はその方針についても含むこととする。

4.7.1. 時刻精度障害

TSA 時計の時刻精度が「1.3.2 時刻認証サービスの内容 (2)-b)」で規定した範囲から外れた場合、当該 TSA 時計を保持するタイムスタンプサーバでのタイムスタンプトークン発行は自動停止され、管理者に通知される。障害が解消されたのちに、当該タイムスタンプサーバでのタイムスタンプトークンの発行を再開する。

4.7.2. 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

ハードウェア、ソフトウェア又はデータが何らかの形で破壊された場合、バックアップ用のハードウェア、ソフトウェア又はデータにより、速やかに復旧作業を行う。
サービスに支障を生じた場合には、利用者・検証者・総務大臣へ連絡し、対処後に総務大臣へ報告する。

4.7.3. タイムスタンプトークンを失効する場合の要件

認証局または時刻認証局のタイムスタンプ生成に使用する秘密鍵が危殆化した場合は、その鍵の公開鍵証明書が認証局の失効リストに掲載されることにより、その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。また、認証局が発行した時刻認証局の公開鍵証明書が誤って発行され、当該誤った公開鍵証明書が添付され発行されたタイムスタンプトークンについても、当該誤りの事実が明らかになった時点で、タイムスタンプトークンは一括して失効される。

4.7.4. 秘密鍵の危殆化が発覚した場合の対処

認定業務で用いる秘密鍵の危殆化が発覚した場合、当該秘密鍵の使用を停止し、速やかに総務大臣に通知するとともに次の手続きを行う。

(1) 認証局に対して紐づく TSA 証明書の失効を申請
(2) 利用者へ秘密鍵の危殆化を通知
(3) 当該秘密鍵の廃棄・再生成
(4) 認証局に対して TSA 証明書の発行を申請

(5) 総務大臣への報告

4.7.5. 災害等発生時の設備の確保

災害等により時刻認証局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復旧作業を行う。

4.7.6. 暗号アルゴリズムの危殆化が発覚した場合の対処

認定業務で用いる暗号アルゴリズムの危殆化が発覚した場合は、当該暗号アルゴリズムを使用した鍵の利用を停止し、速やかに総務大臣に通知するとともに次の手続きを行う。

(1) 認証局に対して紐づく TSA 証明書の失効を申請
(2) 当該秘密鍵の廃棄・再生成（より高いレベルの安全なアルゴリズムに変更）
(3) 認証局に対して TSA 証明書の発行を申請
(4) 利用者へ秘密鍵の危殆化を通知
(5) 総務大臣への報告

4.7.7. 暗号アルゴリズムの危殆化が有効期間内に予想される場合の対処

認定業務で用いる暗号アルゴリズムの危殆化がタイムスタンプトークンの有効期間内に予想される場合は、速やかに総務大臣に通知するとともに次の手続きを行う。

(1) タイムスタンプの発行停止及び TSA 証明書の失効について計画・策定
(2) 関係者への周知
(3) タイムスタンプの発行停止
(4) TSA 証明書の失効手続き
(5) 強化された暗号アルゴリズムを適用した TSA 証明書の再発行手続き（秘密鍵の廃棄・生成を含む）
(6) 関係者への周知
(7) 総務大臣への報告

4.7.8. 設備・システムの重大な故障、自然災害又はセキュリティ事故により当該認定業務の運営に大きな影響を与える可能性がある場合の対処

設備・システムの重大な故障、自然災害又はセキュリティ事故の発生により、認定業務の運営に大きな影響を与える可能性がある事態が発生した場合は、速やかに総務大臣に通知するとともに次の手続きを行う。

(1) 利用者及び検証者へ本サービスの一時停止のスケジュールと対処状況又は対処方針を通知又は連絡
(2) 被害状況の把握及び原因究明と措置の実施
(3) 復旧に向けた点検又は確認作業
(4) 利用者及び検証者へ本サービスの再開スケジュールの通知又は連絡
(5) 総務大臣への報告

4.7.9. 本サービスの全部又は一部の提供停止、又はサービスの品質低下を生じさせる事態が発生した場合の対処

本サービスの全部又は一部の提供の停止又は品質を低下させる事態が発生した場合は、速やかに総務大臣に通知するとともに次の手続きを行う。

(1) 利用者及び検証者へ本サービスの一時停止のスケジュールと対処状況又は対処方針を通知又は連絡
(2) 被害状況の把握及び原因究明と措置の実施
(3) 復旧に向けた点検又は確認作業
(4) 利用者及び検証者へ本サービスの再開スケジュールの通知又は連絡
(5) 総務大臣への報告

4.8. UTC との時刻同期

時刻認証局は、光テレホン JJY を介して NICT が提供する UTC（NICT）と同期される全ての TSA 時計が所定の精度で同期するように管理する。また、この時刻源とは別系統の比較時刻源を参照することにより TSA 時計が所定の精度で UTC（NICT）と同期していることを確認する。

4.9. 時刻のトレーサビリティ

時刻認証局は、TSA 時計が光テレホン JJY を介して NICT が提供する UTC（NICT）時刻と同期されるまでに経由する各機器における時計間の時刻差を取得・保管することにより、タイムスタンプトークンに使用した時刻のトレーサビリティを確保する。

5. 物理的、手続き的及び要員的なセキュリティ管理

5.1. 物理的管理

5.1.1. 施設の場所と建物構造

本サービスを提供するにあたって必要な設備は、地震、火災、水害その他の災害の被害を容易に受けない施設の施錠された区画内に設置し、建物構造上、耐震、耐火及び不正侵入防止のための対策を講じる。
時刻認証局の建物、フロア、部屋の出入り口等に、当施設であることを示す表示は一切行わない。

5.1.2. 物理アクセス

本規程の「5.1.1 施設の場所と建物構造」で規定された施設へのアクセスはあらかじめ登録された人員のみが許可される。その人員以外がアクセスする場合は、所定の手続きを取り、定められた人員が立ち会う。

5.1.3. 電源設備

本規程の「5.1.1 施設の場所と建物構造」で規定された施設の一次電源は電力会社より複数系統の供給を

受ける。無停電電源装置および非常用発電機を配備し、停電時も継続して電源が供給される。

5.1.4. 空調設備

本規程の「5.1.1 施設の場所と建物構造」で規定された施設の空調設備は、設備機器に適切な温度となるように保たれる。

5.1.5. 風水害対策

本規程の「5.1.1 施設の場所と建物構造」で規定された施設は鉄骨または鉄筋コンクリート構造で、津波・高潮・洪水時のリスクが考慮された場所に位置する。また、設備機器は窓のない部屋に設置する。

5.1.6. 落雷対策

本規程の「5.1.1 施設の場所と建物構造」で規定された施設は避雷設備を設置し、落雷の被害を容易に受けないように対策を講じる。

5.1.7. 地震対策

本規程の「5.1.1 施設の場所と建物構造」で規定された施設は耐震構造とし、各機器類の転倒及び落下を防止する対策を講じる。

5.1.8. 火災対策

本規程の「5.1.1 施設の場所と建物構造」で規定された施設は耐火構造、室は防火区画とし、消火設備を備える。

5.1.9. 媒体管理

アーカイブデータ、バックアップデータを含む媒体は、適切な入退出管理が行われている室内に設置された施錠可能な保管庫に保管するとともに、所定の手続に基づき適切に搬入出管理を行う。

5.1.10. 廃棄物処理

機密扱いとする情報を含む書類・記憶媒体の廃棄については、所定の手続に基づいて適切に廃棄処理を行う。

5.1.11. 遠隔地バックアップ

重要なデータ等の媒体を遠隔地で保管するに当たっては、所定の手続きに従いセキュリティを確保できる方法で行う。

5.2. 手続きの管理

タイムスタンプサーバの起動・停止、タイムスタンプサーバの鍵の生成等の重要な業務の遂行にあたっては、それぞれの役割に対して信任された要員を設定するものとする。

操作員がシステム操作を行う際、システムは操作員が正当な権限者であることの識別・認証を行い、タイムスタンプサーバの鍵の生成・更新等の重要操作は複数の要員が立ち会って行う。
本時刻認証局は、本サービスの業務を委託する場合、当該委託先に本章の規定の遵守を求め、詳細手順書の作成とこれに沿った運用を実施させることで、本章に従った物理的、手続的及び人的なセキュリティの維持を図る。

5.3. 要員の管理

5.3.1. 経歴、資格、経験および必要条件

時刻認証局は、本サービスの実施にあたる要員について、履歴書及び人事票等の人事部門で保有する情報により、入社前・入社後の賞罰の記録、資格の取得等の経歴や実務経験、従事させる業務毎に必要な専門的な知識・経験の有無等、当該業務に従事するのに適格であるかどうかの確認を行ったうえで、任命・配置を行うものとする。

5.3.2. トレーニング要件

本サービスの実施にあたる要員に対して、別途教育計画を定めトレーニングを実施する。

5.3.3. 追加トレーニングの頻度および要件

本サービスの実施にあたる要員に対しては、初期的なトレーニングだけではなく、教育計画に基づき定期的に教育を行う。

5.3.4. 権限のない行為に対する制裁

本サービスの実施にあたる要員が、過失、故意に関わらず、その者に与えられた権限を越える行為をした場合、又は本規程又は本サービスに関する運用ルール、マニュアル若しくは手続に違反した場合は、時刻認証局における就業規則又はその他の規則若しくは雇用契約等に基づき懲戒を行う。

5.3.5. 担当者に提供される文書

本サービスの実施にあたる要員に対して、その要員の職務に必要な場合に以下の文書が提供される。
(1) 時刻認証局の設備や機器のマニュアル類
(2) 時刻認証局の運用に関する規程・手順書等

6. 技術的管理

6.1. 鍵の管理

6.1.1. 鍵ペアの生成

(1) 鍵ペア生成

鍵ペアは、複数人立ち会いのもとで暗号モジュール（HSM）を用いて生成する。

(2) 公開鍵の認証局への登録

所定の手続きにより認証局に登録し、公開鍵証明書の交付を受ける。

(3) 認証局のルート証明書等の受領

所定の手続きにより、認証局から取得したルート証明書、中間証明書及びタイムスタンプトークンの署名に用いる公開鍵証明書を安全かつ確実に保管する。

(4) 鍵長と署名アルゴリズム

鍵ペアは 2048bit 以上の RSA 公開鍵暗号方式を用い、署名アルゴリズムには SHA512withRSA を使用する。

6.1.2. 秘密鍵の保護

(1) 暗号モジュールに関する基準

秘密鍵は、FIPS 140-2 のレベル 3 以上若しくは FIPS 140-3 のレベル 3 以上又は ISO/IEC 15408 EAL4＋以上（EN 419 221-5 に対応するもの）の認定を受けた暗号モジュール（HSM）を使用して生成・保護する。

(2) 秘密鍵の複数人管理

秘密鍵の生成、活性化、廃棄等は、複数人管理の下で行い、その操作を記録する。

(3) 秘密鍵の預託

秘密鍵の預託は行わない。

(4) 秘密鍵のバックアップ

秘密鍵のバックアップは行わない。

(5) 秘密鍵のアーカイブ

秘密鍵のアーカイブは行わない。

(6) 暗号モジュールへの秘密鍵の格納

暗号モジュール（HSM）の中で生成・保管する。

(7) 秘密鍵の活性化方法

複数人管理の下で所定の操作により行う。

(8) 秘密鍵の非活性化方法

複数人管理の下で所定の操作により行う。

6.1.3. 秘密鍵の利用及び管理

(1) 秘密鍵の利用

タイムスタンプトークンのデジタル署名に用いる秘密鍵はタイムスタンプ専用のものであり、これ以外には使用しない。秘密鍵を用いてデジタル署名を付与する際は、暗号モジュール(HSM)の内部で安全に実施する。

(2) 秘密鍵の使用期間と公開鍵証明書

秘密鍵の活性化期間（使用期間）は 15 か月以内とし、活性化期間（使用期間）満了前に新しい鍵ペアへの鍵更新と公開鍵証明書の更新を行う。公開鍵証明書の有効期間内に認証業務の終了、秘密鍵の危殆化、暗号アルゴリズムの危殆化が発生した場合には、速やかに公開鍵証明書の失効手続きを行う。

(3) 鍵の更新

時刻認証局は定められた期間（15 か月以内）ごとに定期的に鍵ペアの更新を行う。この際、公開鍵証明書は失効されない。利用している暗号アルゴリズムが危殆化又は不適切となった場合、関係する秘密鍵を全て更新する。

(4) 鍵の廃棄

時刻認証局は、必要な期間が終了した鍵、失効した鍵、危殆化した鍵（秘密鍵を用いていた認定業務が認定の効力を失った場合を含む）、また利用終了となる機器に保存された鍵等を、所定の手順で安全に廃棄する。定期的に更新する秘密鍵については、更新後に廃棄する。

また、時刻認証局の電子証明書を発行する認証事業者が失効に係る認証業務を終了する場合には、認証事業者の認証業務終了までに、複数人管理の下で暗号モジュール内の秘密鍵を廃棄する。

6.1.4. 暗号鍵の管理

時刻認証局で用いる暗号鍵（タイムスタンプトークンの生成に用いる秘密鍵以外の暗号鍵）は、安全な設備を用いて生成・保管し、更新時期を適切に定め、所定の手続きに従い、更新する。

また、危殆化時には所定の手続きに従い、速やかに廃棄する。

6.2. 機器及びネットワークの管理

6.2.1. 使用する機器及びネットワーク要件

時刻認証局を構成する装置やソフトウェア、ネットワークに対してセキュリティに関する基準を設け、それを満たす製品、設定、システムとなるように構成する。

6.2.2. 機器及びネットワークへのセキュリティ調査

時刻認証局では、構成するシステム及びネットワーク全体のセキュリティに関する情報収集、脆弱性評価を定期的に行い、問題がある場合には所定のセキュリティ基準に基づき、処置と再評価を実施する。

また、システム及びネットワーク構成が変更された場合にも、同様の手続きを実施する。特にタイムスタンプトークンの生成に係るプログラムに対して変更を行う場合は、認定機関に報告・確認を行う。

脆弱性指摘やセキュリティインシデントが発生した場合には、所定の手続きに従い、速やかに対応する。

6.3. システムのライフサイクル管理

タイムスタンプトークン生成に係るシステムやプログラムへの変更・操作は複数人制御の下で行う。

6.3.1. システム開発における管理

時刻認証局は、使用されるシステムやソフトウェアの開発、修正、変更にあたって所定の品質管理基準を設け、これを満たすように制御及び管理された環境において実施する。

6.3.2. システム運用における管理

時刻認証局では、システム運用に関する規定、基準を設け、これに基づき、運用管理、維持管理、保守、監視を行う。

6.3.3. セキュリティ運用における管理

時刻認証局では、サービス導入前、システム構成又はサービス運用の変更時、及び定期的に所定の規定・基準に基づき、セキュリティの確認、評価を行う。

6.4. 暗号モジュールの管理

「6.1 鍵の管理」に記載の通り。

7. 運用規程の管理

7.1. 運用規程の変更

時刻認証局は所定の手続きに基づき、本規程を必要に応じて変更する。

7.2. 運用規程の公開と通知

時刻認証局は、本規程を変更する場合、その適用開始日を明記の上、変更後の本規程をリポジトリに公開する。

本サービスの利用者に対しては、登録された連絡先に速やかに通知を行う。

8. 本サービスの休止及び再開

本サービスを休止する場合は、タイムスタンプトークンの検証に必要な情報の継続的な提供と利用者及び検証者を保護するために十分な内容を含む再開計画と併せて、総務大臣に届け出るとともに、休止する旨を速やかに利用者及び検証者へ通知又は連絡する。

通知又は連絡する内容には、以下の情報を含めることとする。

(1) 休止する認定業務の内容

(2) 休止する年月日

(3) 休止期間

(4) 休止理由

(5) 利用者及び検証者からの苦情又は相談に応ずる連絡先

(6) 休止する認定業務に係る役務の代替となる役務に関する情報（当該認定業務に係る役務と当該代替と

なる役務との比較検討が可能となる情報を含む）

(7) 休止する認定業務に係る役務に関する利用者及び検証者の被害の発生又は拡大の防止に資する情報

本サービスを再開する場合は、総務大臣に対し認定業務の再開を届け出るとともに、再開する旨を速やかに利用者及び検証者へ通知又は連絡する。通知又は連絡する内容には、再開計画を含めるものとする。

9. タイムスタンプトークンのプロファイル

フィールド	内容	値
TimeStampToken		
Contentinfo		CMS SignedData構造
ContentType	CMSフォーマットの種別OID	id-signedData (OID=1.2.840.113549.1.7.2)
Content		SignedData構造
Version	SignedData構造のバージョン	3（eContent,sid,certificates,revocationInfosの型により決定される）
digestAlgorithms	署名で用いるハッシュアルゴリズム群	SHA-512 (OID=2.16.840.1.101.3.4.2.3)
encapContentInfo	署名対象データ	-
eContentType	署名対象データの種類	id-ct-TSTInfo (OID＝1.2.840.113549.1.9.16.1.4)
eContent	署名対象データ	TSTInfo構造（下記「TSTInfo」参照）
certificates	署名に使われる証明書群(オプション)	タイムスタンプ要求にcertReqがある場合に存在
certificate[0]		TSA証明書（オプション） iScign Accredited Timestamping SPxxUx-xxx
certificate[1]		中間CA証明書（オプション） GloabalSign R45 AATL TimeStamping Root CA 2021
certificate[2]		ルート証明書（オプション） GloabalSign TimeStamping Root R45
signerInfos	署名情報リスト	-
signerInfo[0]	TSA証明書による署名情報	-
version	signerInfoのバージョン	1（sidにissuerAndSerialNumber形式を使用）
sid	署名者証明書識別情報	署名者証明書（＝TSA証明書）の識別情報
issuer	発行者識別名	TSA証明書の発行者識別名
serialNumber	証明書シリアル番号	TSA証明書のシリアル番号
digestAlgorithm	eContentを識別するハッシュアルゴリズム	SHA-512 (OID=2.16.840.1.101.3.4.2.3)
signedAttrs	署名される属性(以下属性と値)	-
Attribute		
attrType	属性	contentType (OID=1.2.840.113549.1.9.3)
attrValues	値のセット	-
AttributeValue	eContentTypeの属性値と一致	id-ct-TSTInfo (OID＝1.2.840.113549.1.9.16.1.4)
Attribute		
attrType	属性	signingTime (OID=1.2.840.113549.1.9.5)
attrValues	値のセット	-
AttributeValue	トークンの生成されたTSAが保証しない時刻	YYMMDDHHMMSSZ形式のUTC時刻の文字列
Attribute		
attrType	属性	messageDigest (OID=1.2.840.113549.1.9.4)
attrValues	値のセット	-
AttributeValue	eContent(=TSTInfo)のハッシュ値	
Attribute		
attrType	属性	signingCertificateV2 (OID=1.2.840.113549.1.9.16.2.47)
attrValues	署名者証明書(TSA証明書)の識別情報(ESSCertIDv2)	-
AttributeValue	TSA証明書のハッシュアルゴリズム(hashAlgorithm)	SHA-512 (OID=2.16.840.1.101.3.4.2.3)
AttributeValue	TSA証明書のハッシュ値(certHash)	
signatureAlgorithm	署名アルゴリズム	sha512WithRSAEncryption (OID=1.2.840.113549.1.1.13)
signature	signerInfoの署名値	
TST Info		
version	TSTInfoのバージョン	1
policy	TSAのポリシーOID	0.2.440.200356.1.1.1
messageImprint	要求に含まれたタイムスタンプ対象情報	—
hashAlgorithm	タイムスタンプ対象情報の識別に使うハッシュアルゴリズム	タイムスタンプ要求に従う（SHA256/SHA382/SHA512）
hashedMessage	タイムスタンプ対象情報のハッシュ値	
serialNumber	タイムスタンプトークンのシリアル番号	
genTime	時刻認証を行ったUTC時刻	YYYYMMDDhhmmss[.s...]Z ※小数点以下は最大6桁となる
accuracy	時刻精度	1秒
ordering	順序性を表すフラグ	FALSE
nonce	ノンス	タイムスタンプ要求に従う
tsa	TSA識別名	TSA証明書の主体者識別名 iScign Accredited Timestamping SPxxUx-xxx
extensions	拡張領域	(未使用)