MIND タイムスタンプサービス
運用規程(総務大臣認定版)

1.7 版

発行：2022 年 5 月 13 日

改訂：2025 年 1 月 28 日

三菱電機インフォメーションネットワーク株式会社

改版履歴

版	変更日付	変更箇所	変更内容	発行責任者
1.0	2022 年 5 月 13 日		初版作成（総務大臣認定用）	時刻認証局責任者
1.1	2022 年 8 月 3 日	1.3.3 4.2.1	うるう秒に関する記載を修正	時刻認証局責任者
1.2	2022 年 11 月 8 日	1.3.3 9	うるう秒に関する記載を修正 テスト用 OID を削除	時刻認証局責任者
1.3	2022 年 12 月 12 日	1.3.1	認証局の記載を修正	時刻認証局責任者
1.4	2024 年 2 月 9 日	2.5.4	リポジトリの URL 変更に伴う修正	時刻認証局責任者
1.5	2024 年 7 月 6 日	4.6.4 付録	DR 環境についての記載を追加 専用線ユーザについての記載を追加	時刻認証局責任者
1.6	2025 年 1 月 24 日	4.6.4 4.6.7	DR 環境についての記載を削除	時刻認証局責任者
1.7	2025 年 1 月 28 日	1.3.3 4.5.1 6.1.1 9	TST の有効期間に関する記載を修正 アーカイブの最低保管期間の記載を修正 暗号方式の記載を修正	時刻認証局責任者

目次

1. はじめに

MIND タイムスタンプサービス運用規程(以下「本規程」といいます)では、三菱電機インフォメーションネットワーク株式会社(以下「当社」といいます)の運営する時刻認証局が行う MIND タイムスタンプサービス-DiaStamp-(以下「本サービス」といいます)の基本的事項について述べます。本規程で取り扱うタイムスタンプは RFC5816 による更新を採用した IETF RFC 3161「Public Key Infrastructure: Time-Stamp Protocol(TSP)」に準拠して発行されるものとします。

1.1. 概要

本規程は、当社が運営する時刻認証局が提供する本サービスの運用方針及び業務手続きについて記述するものです。
本規程の適用対象は本サービスのすべての利用者及び本サービスに関連する個人・法人・組織を含みます。本規程では本時刻認証局、すべての利用者、及び本サービスに関連する個人・法人・組織の権利と義務を表明します。
時刻認証局は、タイムスタンプポリシー(Time-stamp policy)及び時刻認証局運用規程(Time-stamping practice statement)をそれぞれ独立したものとせず、本規程を時刻認証局の本サービスに関する運用方針として位置付けます。

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　:MIND タイムスタンプサービス運用規程(総務大臣認定版)
バージョン　:1.7 版
適用開始日　:2025 年 1 月 28 日
作成者　:三菱電機インフォメーションネットワーク株式会社

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)を以下に示します。

本サービス	
三菱電機インフォメーションネットワーク株式会社	1.3.6.1.4.1.1291
MIND タイムスタンプサービス-DiaStamp-	1.3.6.1.4.1.1291.1.1
時刻認証局タイムスタンプポリシー	
Type A2	1.3.6.1.4.1.1291.1.1.1.1

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/

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、RFC5816 による更新を採用した RFC3161 に基づくタイムスタンププロトコルに準拠したタイムスタンプトークンを発行する事業者をいいます。本規程において時刻認証局とは、本時刻認証局のことをいいます。

(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、時刻認証局の TSU が使用する公開鍵証明書の認証を行う事業者をいいます。
本時刻認証局の認証局は以下のサービスを利用します。
・ 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 です。
（注）電子証明書（TSA 証明書）では GlobalSign nv-sa と表記されます。

(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(サービスの利用)申込みを行い、時刻認証局からサービスへの加入(サービスの利用)を認められ、そのサービスを受ける者をいいます。

(4) タイムスタンプトークン(TST)
本規程においてタイムスタンプトークン(以下「TST」といいます)とは、1.3.3(1)に記載されていることを目的として、利用者から送付されたハッシュ値に対して発行される電子証明書をいいます。
TST には、発行した TSU による発行時刻及び同ユニットの識別情報が記載されます。
また、TST のプロファイルは 9 に記載されます。

(5) タイムスタンプ生成装置（TSU）
本規定において、タイムスタンプ生成装置（以下「TSU」といいます。）とは、TSA が管理する秘密鍵でタイムスタンプトークンを発行する HSM を搭載した装置をいいます。

(6) リポジトリ
本規程において、リポジトリとは TST の検証に必要な関連情報等を格納するシステムのことを示すものとします。

(7) 情報通信研究機構(NICT)
周波数や時間の元となる国家標準値を定める公的機関で、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、日本標準時を生成・供給しています。
TSU は、NICT から供給される複数の時刻源を参照して、時刻の正当性を維持するものとします。

(8) Adobe Approved Trust List(AATL)
米アドビシステムズが認定した、信頼できるルート証明書の一覧。

1.3.2. 時刻認証サービスの様態

総務省告示第 146 号「時刻認証業務の認定に関する規程」による認定を受けた認定事業者として当社が提供するタイムスタンプサービスであり、以下のタイプとなります。

Type A2
GMO グローバルサイン株式会社による「GlobalSign 認証業務」の内、AATL に登録された CA から認証された TSA 証明書を用いた認定タイムスタンプサービス

1.3.3. 時刻認証サービスの内容

本サービスの内容は以下のとおりとします。

(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 RFC5816 による更新を採用した RFC3161 に準拠した TST を生成し、それを利用者に対して発行します。
   ① 適用されるハッシュアルゴリズムは、SHA-256、SHA-384、SHA-512 とします。
   ② TST は時刻認証局が管理する任意の TSU を用いて生成され、TSU 毎の秘密鍵を用いてデジタル署名が行われます。
   ③ TST のデジタル署名に使用される公開鍵暗号方式は、6.1.1 で規定された方式を用います。
   ④ 時刻認証局は、タイムスタンプを行う対象の内容(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ものとします。
   ⑤ TST には利用者を特定する情報は含まれません。
   ⑥ 時刻認証局と利用者間のデータの受け渡しは、セキュリティを考慮した方法で行います。通信手順の詳細については別途規定します。

(2) TST が示す時刻は本規程に基づいて下記の条件で付与されます。
   ① TST に記載される時刻は TSU 内の時計の時刻とします。
   ② TSU 内の時計の時刻は、NICT により供給される時刻源 UTC（NICT）に同期することで TST に付与される時刻を保証します。本時刻認証局は時刻源と TSU 内時計の同期が外れ±1 秒を超える誤差が発生した場合、TSU の TST 発行機能を速やかに停止します。
   ③ TST を発行する TSU は、NICT より供給される時刻源 UTC（NICT）とは別の系による比較時刻源を随時参照することにより、TSU が管理する時刻が±1 秒を超える誤差が発生していないことを確認します。NICT から供給される時刻と±1 秒を超える誤差が検知された場合は、TST の発行機能を停止し、本規程で定められた時刻範囲内で TST が発行されることを保証します。
   ④ ±1 秒の誤差範囲内においては、TST に記載された時刻の順位に有意性はないものとします。TST のシリアル番号も複数の TSU により発行されるため有意性はないものとします。
   ⑤ TST に記載される時刻は、TSU がタイムスタンプ発行要求を受け付けた時刻ではなく、実際にタイムスタンプ処理を実施した時刻を表すものとします。
   ⑥ タイムスタンプ要求の受け付け順位と TST の作成順位(時刻の順位)が等しいことは保証されません。
   ⑦ 本時刻認証局が保証する時刻精度は UTC (NICT)に対して±1 秒です。

(3) 認証局が発行する TST には有効期間があります。
   ① TST の有効期間は、タイムスタンプを付与した時刻から、TST のデジタル署名に使用する 6.1.4. に記載する秘密鍵に対応する公開鍵証明書の有効期限迄としており、最低限 10 年保証します。ただし 4.6.2.（タイムスタンプトークンを失効する場合の要件）及び 4.6.5.（暗号アルゴリズムの危殆化又は、そのおそれが生じた場合の対処）に記載の場合については、これに限りません。
   ② タイムスタンプの付与対象となる電子データの保存期間内にタイムスタンプの有効期間が満了する場合は、当該有効期間内にタイムスタンプの再付与等の措置が必要です。
   ③ 有効期限を超過したタイムスタンプは、その信頼性を裏付けるものではありません。

(4) TST を発行するサービスの提供時間帯は、24 時間 365 日とします。ただし、4.2.（サービスの一時停止と解約）に記載の場合、サービスの一時停止が発生します。

(5) TSU 内の時計は UTC (NICT)との時刻同期を維持するため、うるう秒が発生した際でも、うるう秒を考慮した調整は行いません。ただし、うるう秒発生前後にサービスを一時停止し、問題がない事を確認した上で、サービスを再開します。

1.3.4. タイムスタンプトークンの適用範囲

(1) 適正な用途

TST 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 TST に含まれる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を確認することを目的とします。利用者は上記の用途でのみ TST を利用することが出来ます。また利用者が TST の複製・配布をすることは可能です。

(2) 禁止される用途

利用者は、前号の目的以外、及び、極めて高度な安全性が要求され、仮に当該安全性が確保されない場合、直接生命・身体に対する重大な危険性を伴う用途で TST を使用してはなりません。

1.4. 本規程に関する問い合せ先

名称　　:三菱電機インフォメーションネットワーク株式会社
英語名称:MITSUBISHI ELECTRIC INFORMATION NETWORK CORPORATION
所在地　:〒108-0023 東京都港区芝浦 4-6-8 田町ファーストビル
HP　　:https://www.mind.co.jp/contact/

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 に規定する財務上の責任を負います。時刻認証局は、業務の一部を第三者に委託する場合であっても業務の責任を負います。ただし、時刻認証局は、利用者が本規程に基づいて時刻認証局より発行された TST を使用する場合、タイムスタンプ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 TST を使用した結果に対して何らの責任も負わないものとします。

(1) TST の生成・発行
時刻認証局は、本規程に基づき TST を生成し、利用者から送付されたハッシュ値に対して RFC5816 による更新を採用した RFC3161 に準拠した TST を生成し、利用者に対して発行します。

(2) 時刻の管理
時刻認証局は、発行する TST の発行時刻が 1.3.3(2)の⑦に規定する誤差を超えないように、時刻認証局のシステムの時刻管理を行います。

(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 TSU の時刻や秘密鍵、その他の機器及びシステムやデータを管理します。

(4) 秘密鍵の公開鍵証明書の失効申請と届出
TSU の秘密鍵が危殆化し、又はそのおそれが生じた場合、時刻認証局は直ちに当該秘密鍵の公開鍵証明書の失効を認証局に申請します。その後利用者に連絡を行います。
タイムスタンプ生成に使用する暗号アルゴリズムが危殆化した場合、時刻認証局は直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します。その後利用者に対して連絡を行います。
また、TSU の秘密鍵が危殆化した場合以外の理由で TST 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います。
なお利用者への連絡方法等は、2.3.4 に定めるとおりとします。

(5) 認証事業者への通知
認定業務を廃止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します。

(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います。

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は本規程に記載の事項を了承したうえで次の義務を負い、また、本規程に基づいて時刻認証局より発行された TST を使用する場合、タイムスタンプ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 TST を使用した結果に対する責任を負うものとします。

(1) TST の利用制限の遵守
TST はその目的、適用範囲等などを記載した本規程にもとづいて発行されており、利用者はこれを十分理解した上で TST を利用しなければなりません。

(2) 本規程の遵守
利用者は本規程を遵守すると共に、TST を複製・配布する場合、利用者に対して本規程を遵守させなければなりません。

(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りません。

(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、直ちにその変更内容を書面で当社に通知するものとします。

また、利用者は TST を使用するにあたっては本規程に記載の事項を了承したうえで次の義務を負うものとします。また、本規程に基づいて時刻認証局より発行された TST を利用する場合、タイムスタンプ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 TST を利用した結果に対する責任を負うものとします。

(5) TST の検証義務
利用者は TST を利用するに当たっては、TST を検証しなければなりません。TST の検証には、TST 内のハッシュ値が対象となる電子データのハッシュ値と等しいことの確認、TST 自体の署名確認、TST に署名している秘密鍵に対応する公開鍵証明書の失効確認及び TST の失効確認を含みます。

(6) TST の利用制限の遵守
TST はその目的、適用範囲等などを記載した本規程にもとづいて発行されており、利用者はこれを十分理解した上で TST を利用しなければなりません。

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います。

① 長期保存を目的とした TST の発行用に時刻認証局の公開鍵証明書を発行します。なお当該証明書の有効期間はそれぞれの運用規程に従って設定されます。
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、直ちにその旨を時刻認証局に通知します。
③ 公開鍵証明書の失効リスト、及び公開鍵証明書発行に関連するその他の情報を直ちに時刻認証局に通知します。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直ちに公開鍵証明書の失効を行います。

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します。

2.2. 財務上の責任

2.2.1. 時刻認証局の損害賠償責任

(1) 当社は、本サービスを提供すべき場合において、当社の責に帰すべき事由によって本サービスの提供が出来なかったことにより契約者に損害を与えたときは、本サービスが全く利用出来ない状態にあることを当社が知った時刻から起算して、24 時間以上その状態が連続したときに限り、当該契約者の損害を賠償します。
その場合において、当社は、本サービスが全く利用出来ない状態にあることを当社が知った時刻以後のその状態が連続した時間(24 の倍数である部分に限ります)に対応する当該サービスに係る料金額(サービスの一部が全く利用出来ない状態の場合は、その部分に係る料金額)を契約者に発生した損害とみなし、その額に限って賠償します。また、賠償額は本サービスに定める利用料金の 1ヶ月分に相当する金額の範囲内とします。

(2) 当社は、天災、事変その他非常事態の発生等当社の責に帰することが出来ない事由から生じた損害、当社の予見の有無を問わず特別の事情から生じた損害、逸失利益及び第三者からの損害賠償請求に基づく契約者の損害については、責任を負わないものとします。

2.2.2. 免責事項

(1) 2.2.1 の規定にかかわらず、下記の何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します。
① 天災地変、事変、戦争、暴動、内乱、法令の制定改廃、公権力による命令処分、 輸送機関の事故、争議行為、伝染病、疫病その他不可抗力の場合
② 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
③ 利用者の故意、過失若しくは違法行為に起因して損害が発生した場合

④ 利用者による本規程若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
⑤ 利用者のシステムに起因して損害が発生した場合
⑥ 契約者が個々に契約するインターネットサービスプロバイダ接続が原因で、損害が発生した場合
⑦ 当社及び契約者が個々に契約するインターネットサービスプロバイダ以外の電気通信事業者が提供する通信サービスに起因する事象により、全ての通信に著しい支障が生じ、全く利用出来ない状態となることにより契約者に損害が発生した場合
⑧ 4.2.1、及び 4.3 に定める事由により本サービスの一時停止又は終了が発生した場合
⑨ 時刻認証局が一般的な認証事業者の知見及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、又はセキュリティ手段が破られた場合
⑩ TST の失効に起因して損害が発生した場合

(2) 当社は、2.2.1 に定める場合を除き、前項に定めるものの他、契約者が本サービスの利用により被った損害については、債務不履行責任、不法行為責任、その他の法律上の責任を問わず賠償の責任を負いません。ただし当社に故意または重大な過失がある場合はこの限りではないものとします。

(3) 前項但し書きにより、当社が責任を負担する場合は、本サービスに定める利用料金の 1 ヶ月分に相当する金額の範囲内で責任を負担するものとします。

2.3. 解釈及び執行

2.3.1. 準拠法

本規程の解釈及び有効性等は、日本法に基づき解釈します。

2.3.2. 可分性

本規程のある規定又はその適用が、何らかの理由により無効又は執行不可能であるとされた場合、当該規定のみが無効又は執行不可能となり、本規程の他の規定は有効に存続し適用されます。

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します。

2.3.4. 通知

利用者から時刻認証局への通知は書面又は電子メールによって、1.4 に基づき特定される宛先に行います。書面による通知は受領日をもって有効とします。
時刻認証局から利用者への通知は、サービス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します。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ます。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します。

2.3.5. 紛争解決

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します。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します。

2.4. 料金

別途、本サービスの料金表に規定します。

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します。

① 時刻認証局運用規程(本規程)
② 公開鍵証明書情報
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 利用規約
利用者との利用規約（契約約款）を別途定め、公開します。
⑥ その他の注意事項
その他、利用に関わる注意事項を別途定め、公開します。

2.5.2. 更新の頻度

公開する情報の更新頻度は次のとおりとします。
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時

2.5.3. アクセス制御

時刻認証局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します。公開情報を提供するに当たっては、特段のアクセス制御は行わないものとします。

2.5.4. リポジトリ

2.5.1 において定める情報を下記リポジトリに公開します。
URL: https://www.mind.co.jp/contact/tsa/

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ます。
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、安全に保管管理します。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、漏えいしないと共にサービスの範囲を超えて使用しないものとします。
時刻認証局は、発行したタイムスタンプが有効である間は、対象となる機密情報を最低限保管し、その後削除します。
次の情報は機密扱いとする情報に含まれるものとします。
① 申し込みに関する記録(承認されたか否かを問わない)
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及び実施措置
④ ハードウェア及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り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・漏洩してはなりません。

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、機密扱いとはしません。
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. 公開鍵証明書失効情報の公開

時刻認証局の公開鍵証明書の失効情報は、該当する公開鍵証明書の認証局において公開鍵証明書失効リストとして公開されます。
TST の信頼性低下に関する情報については、時刻認証局が認識した時点で速やかに対象となる失効情報をリポジトリ上に公開を行います。

2.6.4. 法執行機関への情報開示

時刻認証局で取扱う情報(機密情報を含む)について、法執行機関から法的根拠に基づいて当該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します。

2.6.5. その他の理由に基づく情報開示

時刻認証局が業務の一部を第三者に委託する場合、秘密情報を委託先に開示する事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します。

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)、商標権及び著作権(以下知的財産権と呼ぶ)は時刻認証局又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します。

① 時刻認証局から発行された TST
② 時刻認証局が用意する TST 検証用ソフトウェア
③ 本規程

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、以下に特定する範囲を超えて使用しません。また、その保護について、以下に従うものとします。ただし、法令に定められた場合はこれに限りません。

(1) 個人情報の取得
時刻認証局は、利用者から提供された情報のうち、個人の氏名、電話番号、勤務先その他個人の識別が可能な情報を個人情報として扱うものとします。また、必要な範囲を超えて取得はしません。

(2) 利用目的の特定
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使用します。なお利用者から別途承諾を得た場合、時刻認証局は、本サービスに関連した自ら又は自らの子会社の商品、サービス等の案内のために利用することがあります。

(3) 利用目的による制限
時刻認証局は、上記に規定される目的以外に個人情報を利用しません。

(4) 保有個人情報に関する事項の公開
時刻認証局は、個人情報の利用目的を本規程に記載し公開します。

(5) 正確性の確保
時刻認証局は、個人情報を利用者からの申し出に基づき正確な状態で管理します。

(6) 安全管理措置
時刻認証局は、合理的な安全対策を講じて、個人情報への不正アクセス、個人情報の紛失、破壊、改竄、漏えい等の防止に努めます。また、個人情報の取扱いを第三者に委託する場合は、当該第三者が当該個人情報を安全に管理するよう、必要かつ適切な監督を行います。

(7) 開示・訂正
時刻認証局は、個人情報について、本人から開示、訂正若しくは削除を求められた場合、合理的な範囲内で対応します。

(8) 保存期間・廃棄
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、サービス解約時に削除します。

3. 識別と認証

3.1. 初期登録

3.1.1. 名前の型

TSU 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します。

3.1.2. 名前の意味

時刻認証局が発行する TST に記載される TSU の固有名称は、認証局が発行した TSU 用の公開鍵証明書に記載された名称とします。

3.1.3. 名前の一意性

時刻認証局の発行する TST に記載される TSU の固有名称は、TSU 毎に認証局により一意に割り当てられるものとします。

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、利用可否を判断します。

3.3. サービスの加入の更新

本サービスの契約更新時における識別と認証は 3.2.において定める手続きに基づいて行います。

3.4. サービスの解約の申請

本サービスの解約時における識別と認証は 3.2.において定める手続きに基づいて行います。

4. 運用要件

4.1. サービスの利用

4.1.1. 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りません。
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します。

4.1.2. タイムスタンプ要求

本サービスの利用者は、タイムスタンプを行う対象となる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します。本時刻認証局と利用者間の通信手段及びタイムスタンプ要求の詳細手順については別途規定します。
また、タイムスタンプ要求はタイムスタンプ発行以外の目的で行ってはなりません。

4.1.3. 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、タイムスタンプ要求を正しく受け付けたか、拒否したか、又はその他の応答の状態(status)を返します。タイムスタンプ要求が正常に受け付けられた場合は、本時刻認証局の管理する任意の TSU を用い、1.3.3 に規定される TST の作成をおこない、それを利用者に対して発行します。本時刻認証局と利用者間の通信手段及び TST の発行の詳細手順については利用者に対して加入時に別途通知します。

4.1.4. タイムスタンプトークンの検証

TST を受領した者は、以降に記す方法で TST の検証を行うものとします。なお、タイムスタンプトークンの検証は、利用者側でツールを使用して実行します。

① タイムスタンプ対象電子データのハッシュ値と TST に含まれるハッシュ値を比較することにより、タイムスタンプ対象電子データと TST が対であるあるいは、対象電子データが改竄されていない事を確認します。
② TST に署名した秘密鍵に対する公開鍵証明書を利用して、時刻認証局のデジタル署名の確認を行うことにより、TST が改竄されていない事を確認します。
③ 認証局の証明書を含む公開鍵チェーンの検証を行うことにより、公開鍵証明書が有効である事を確認します。
④ 時刻認証局のリポジトリから TST の失効情報を確認することにより、TST が有効である事を確認します。
⑤ TST に含まれているタイムスタンプ付与時刻を利用することで、その時刻に対象電子データが存在し、以降改ざんされていないことを確認します。

4.2. サービスの一時停止と解約と変更

4.2.1. サービスの一時停止

時刻認証局は、定期的な点検整備(認証局の点検整備による場合を含む)及びうるう秒の設定による中断等により、サービスの一時停止の必要が発生した時は、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します
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します。

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

4.2.2. 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します。
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します。
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

4.2.3. 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します。

4.2.4. サービスの解約

(1) 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します。
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
(ア) 手形交換所の不渡り処分を受け、又は金融機関から取引停止処分を受けたとき
(イ) 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
(ウ) 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
(エ) 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
(オ) 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
(カ) 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
(キ) 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
(ク) その他本規定の義務の履行が期待出来ないと認められる相当の事由があるとき。

(2) 前項により本サービスを停止した場合、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出来るものとします。

4.2.5. 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、あらかじめ総務大臣への申請を行い認定を受けます。認定を受けたらその内容を利用者に通知するとともにリポジトリに公開します。

4.2.6. 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します。
1 届出に係る認定業務の名称
2 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）
3 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）
4 変更の理由
5 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、その内容をリポジトリに公開します。

4.3. 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します。サービスの終了とは、時刻認証局の終了を意味します。
   ① 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
   ② 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
   ③ 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
   ④ 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、本サービス終了の事実、廃止しようとする認定業務の内容、年月日、廃止の理由及び本サービス終了後の時刻認証局のバックアップデータ、アーカイブデータ等の保管組織及び開示方法を原則として本サービス終了 90 日前までに利用者に公開又は通知します。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します。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ついての情報、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先はリポジトリに公開します。

(3) 本サービスの終了決定後、速やかに全ての TSU の秘密鍵を安全に廃棄します。

(4) 本サービス終了後、速やかに全ての個人情報を削除します。

4.4. 準拠性監査

4.4.1. 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します。また、時刻認証局組織は、必要に応じて定期監査以外に監査を実施します。

4.4.2. 監査人の身元・資格

時刻認証局の監査人には、当社の中から監査業務及び認証業務に精通した者を任命するものとします。必要に応じて外部の監査会社に監査を依頼します。監査人の任命は時刻認証局の責任者が行います。

4.4.3. 監査人と被監査部門の関係

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

4.4.4. 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します。

4.4.5. 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ものとします。運用している時刻に異常が確認された時や TSU 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ります。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 TSU 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します。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します。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します。

4.4.6. 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ます。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します。

4.5. アーカイブ

4.5.1. アーカイブの種類

アーカイブデータは、次のものとします。なお( )内の年数は最低保管期間を表します。
保管は、発行したタイムスタンプが有効である間は最低限保証します。

① TSU 時計の UTC（NICT）との同期および比較時刻との比較記録等、TST に付与される時刻の品質を保証する記録（10 年）
② 利用者との本サービスの利用契約の成立・本サービスの利用開始から契約解除・本サービス停止までのプロセスにおける全記録(10 年)
③ タイムスタンプ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(10 年)
④ 時刻認証局設備への入退室記録(10 年)
⑤ 時刻認証局システムに対する操作記録(10 年)
⑥ 時刻認証局システムの動作異常の記録(10 年)
⑦ 時刻認証局システムに対する不正アクセスに関する記録(10 年)
⑧ 準拠性監査報告書(10 年)

4.5.2. 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します。また、温度、湿度、磁気などの環境を考慮して保管するものとします。

4.5.3. 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します。

4.5.4. アーカイブデータの開示

時刻認証局は、時刻の品質を保証する記録を利用者の求めに応じて、2.3.4（通知）に基づき開示します。

4.6. 危殆化と災害からの復旧

4.6.1. ハードウェア、ソフトウェア又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います。また、サービスに支障を生じた場合は、速やかにリポジトリに公開及び利用者及び総務大臣へ連絡します。利用者及び検証者への通知又は連絡は、2.3.4 に基づき電話や電子メール、ホームページ等の日常的に利用され、かつ広く周知できる方法によって行い、事態への対処状況もしくはその方針を連絡します。対処完了後、総務大臣に報告します。

4.6.2. タイムスタンプトークンを失効する場合の要件

認証局又は時刻認証局の TSU のいずれかの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によって失効される(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 TST は一括して失効されます。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 TST についても、当該誤りの事実が明らかになった時点で、TST は一括して失効されます。

4.6.3. 秘密鍵が危殆化した場合の対処

TSU の秘密鍵が危殆化した場合は、本サービスを停止し、速やかに総務大臣に通知するとともに次の手続を行います。

① 認証局に対して TSU の公開鍵証明書の失効に関する申請手続き
② 利用者及び検証者に秘密鍵の危殆化と対処状況又は対処方針を通知又は連絡
③ TSU の秘密鍵の廃棄及び再生成手続き
④ TSU の新しい鍵に対する公開鍵証明書の発行申請手続き
⑤ 利用者及び検証者へ本サービスの再開スケジュールを通知又は連絡

⑥ 総務大臣への報告

4.6.4. 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います。

4.6.5. 暗号アルゴリズムが危殆化した場合の対処

タイムスタンプ生成に使用する暗号アルゴリズムが危殆化した場合は、本サービスを停止し、速やかに総務大臣に通知するとともに次の手続を行います。

① 利用者及び検証者に危殆化と対処状況又は対処方針を通知又は連絡
② サービス設備の新たな暗号アルゴリズムへの対応
③ 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およびタイムスタンプ再取得の依頼
④ 総務大臣への報告

4.6.6. 暗号アルゴリズムの危殆化が予測される場合の対処

タイムスタンプ生成に使用す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測される場合は、速やかに総務大臣に通知するとともに次の手続を行います。

① 利用者及び検証者へ暗号アルゴリズムの危殆化と対処状況又は対処方針、本サービスの一時停止のスケジュールを通知又は連絡
② サービス設備の新たな暗号アルゴリズムへの対応
③ 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およびタイムスタンプ再取得の依頼
④ 総務大臣への報告

4.6.7. 自然災害又はセキュリティ事故が発生した場合の対処

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います。

① 利用者及び検証者へ本サービスの一部中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
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

4.6.8. 本サービスの全部又は一部の提供停止、又はサービス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います。

① 利用者及び検証者へ本サービスの一時中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
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. 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）時刻と同期される時刻サーバを TSU の時刻ソースとして、全ての TSU の時刻が所定の精度で UTC に同期するように管理します。また、この時刻源とは別の系による比較時刻源を参照することにより、TSU が管理する時刻が所定の精度で UTC と同期していることを確認します。

4.8. 時刻のトレーサビリティ

時刻認証局は光テレホン JJY を介して NICT が提供する UTC（NICT）時刻と同期される時刻サーバおよび TSU 内の時計の同期の記録および比較時刻源との比較結果記録を保持することにより、タイムスタンプに使用した時刻のトレーサビリティを確保します。

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. 施設の位置と建物構造

時刻認証局の施設は、水害、地震、火災その他の災害の被害を容易に受けない場所に設置し、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ます。また、使用する機器等を災害及び不正侵入から防護された安全な場所に設置します。
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いません。

5.1.2. 物理アクセス

時刻認証局施設内の各室へのアクセスはあらかじめ許可された人員のみが可能となるようにします。施設内の各部屋及び設備についてアクセス可能な人員が定義され、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ものとします。また入室する際は所定の入退室記録に記録します。

5.1.3. 電源設備と空調設備

時刻認証局の設備を設置する建物の一次電源は電力会社から複数系統の供給を受けます。時刻認証局の設備へは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ます。また、空調設備を設置することにより機器類の動作環境及び要員の作業環境を適切に維持します。

5.1.4. 浸水対策

時刻認証局の設備は建物の 2 階以上に設置し、全ての部屋には漏水検知器を設置してあります。また、天井、床には防水対策を講じます。

5.1.5. 地震対策

時刻認証局の設備を設置する建物は耐震構造とし、機器什器の転倒及び落下を防止する対策を講じます。

5.1.6. 火災対策

時刻認証局の設備を設置する建物は耐火構造、室は防火区画とし、ガス消火設備を備えます。

5.1.7. 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います。

5.1.8. 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います。

5.1.9. 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います。

5.2. 手続きの管理

TSU の起動・停止、TSU 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します。
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・認証を行います。また、TSU 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います。

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ります。

5.3. 要員の管理

5.3.1. 経歴、資格、経験及び必要条件

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・配置を行うものとします。

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します。

5.3.3. 追加トレーニングの頻度及び要件

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います。

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います。

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ます。

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

時刻認証局は、TST のデジタル署名に用いる秘密鍵について、以下のように管理します。

6.1.1. 鍵の生成

(1) 鍵ペア生成
TSU の鍵ペアは、複数人立ち会いのもとで暗号モジュール(HSM)を用いて生成します。

(2) TSU の公開鍵の認証局への登録
TSU の公開鍵は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ます。

(3) 認証局のルート証明書等の受領
時刻認証局は、認証局から受領したルート証明書及び TSU の公開鍵証明書から当該ルート証明書に至る証明書検証に必要となる中間の証明書を、安全かつ確実に保管します。

(4) 鍵のサイズとアルゴリズム
TSU の鍵には RSA2048 ビットの鍵を使用します。暗号方式は RSASSA-PKCS1-v1_5 を使用します。

(5) 鍵を生成するハードウェア/ソフトウェア
鍵を生成するハードウェア/ソフトウェアは、6.1.2(1)に定める基準を満たす暗号モジュール(HSM)を備えた TSU とします。

6.1.2. 秘密鍵の保護

(1) 暗号モジュールに関する基準
TSU の鍵は、FIPS(米国連邦情報処理標準)140-2 レベル 3 以上の認定を受けた暗号モジュール(HSM)を使用して生成・保管します。

(2) 秘密鍵の複数人制御
TSU の秘密鍵の生成、活性化、廃棄等は、複数人の管理の下で行います。

(3) 秘密鍵の預託
秘密鍵の預託は行いません。

(4) 秘密鍵のバックアップ
秘密鍵のバックアップは行いません。

(5) 秘密鍵のアーカイブ
秘密鍵のアーカイブは行いません。

(6) 暗号モジュールへの秘密鍵の格納
TSU の秘密鍵は、暗号モジュール(HSM)の中で生成・保管します。

(7) 秘密鍵の活性化方法
TSU の秘密鍵は、複数人の管理のもとで暗号モジュール(HSM)に活性化データを入力することにより活性化します。

(8) 秘密鍵の非活性化方法
TSU の秘密鍵は、複数人の管理のもとで暗号モジュール(HSM)に対して所定の操作を行うことにより非活性化します。

(9) 秘密鍵の廃棄方法
暗号モジュール(HSM)内の TSU 秘密鍵の廃棄は複数人の管理のもと所定の手続きに従い廃棄します。

6.1.3. 秘密鍵の利用

認定業務で TST へのデジタル署名に用いる秘密鍵は専用のものであり、これ以外には使用しません。
秘密鍵を用いたデジタル署名は、HSM の内部で実施します。

6.1.4. 鍵と証明書の有効期間

TSU の公開鍵証明書の有効期間は、公開鍵証明書を発行する認証局の運用に依存し、証明書は HSM 内部に保存します。
また、秘密鍵の活性化期間(使用期限)は 2 年以内とし、活性化期間(使用期限)満了前に新しい鍵ペアに交換します。ただし、暗号のセキュリティが脆弱になったと判断した場合、又はその可能性がある場合は鍵更新を行います。

6.1.5. 鍵の更新

時刻認証局は、定められた期間毎(2 年以内)に定期的に鍵ペアの更新を行います。この際、公開鍵証明書は失効されません。

6.1.6. 鍵の廃棄

時刻認証局は、必要な期間が終了した鍵や、失効した鍵、危殆化した鍵などを、所定の手順で安全に廃棄します。定期的に更新する秘密鍵については、更新後 1 ヶ月以内に廃棄するものとします。また、電子証明書を発行する認証事業者が認証業務を終了する場合、当該認証事業者の認証業務終了までに、当該認証事業者の発行に係る電子証明書に対応する秘密鍵を所定の手順で安全に廃棄します。

6.1.7. 活性化データ

(1) 活性化データの生成とインストール
TSU の秘密鍵に対する活性化データは、所定の規則に従って生成し、インストールを行います。

(2) 活性化データの保護
TSU の秘密鍵に対するものを含めて、時刻認証局で使用するすべての活性化データは、所定の規則に従って保護・管理します。

6.2. コンピュータセキュリティ管理

6.2.1. コンピュータセキュリティ機能要件

時刻認証局では、セキュリティに関する基準を設け、コンピュータ装置や時刻関連機器のハードウェアやソフトウェアの導入時にはこれを遵守するための確認を行います。

6.2.2. コンピュータセキュリティ評価

時刻認証局では、セキュリティの脆弱性に関する情報等を定期的に収集し、問題があればセキュリティ基準に基づき再評価を実施します。再評価において問題が認められた場合は是正処置を行います。

6.3. システムのライフサイクル管理

6.3.1. システム開発面における管理

時刻認証局内で使用されるソフトウェアの開発、修正、変更にあたっては、所定の品質管理基準を設け、これを遵守するよう制御された環境において作業を実施します。

6.3.2. システム運用面における管理

時刻認証局では、セキュリティに関する基準を設け、コンピュータ装置や TSU 等のハードウェアやソフトウェアの導入時にはこれを遵守するための確認を行います。

6.3.3. ライフサイクルセキュリティ評価

時刻認証局では、セキュリティの脆弱性に関する情報等を定期的に収集し、問題があればセキュリティ基準に基づき再評価を実施します。再評価において問題が認められた場合は是正処置を行います。

6.3.4. セキュリティマネジメントにおける管理

時刻認証局では定期的なワクチンソフトの適用により、ウィルス感染の検出、回復を行います。

6.4. ネットワークセキュリティ

時刻認証局では、ネットワークセキュリティに関して基準を設け、システム導入時や変更時、運用時にこれを遵守するための確認を行います。

6.5. 暗号モジュールの技術管理

6.1.1(1)及び 6.1.2(1)において定めます。

6.6. 暗号鍵の管理

時刻認証局で用いる暗号鍵（TST の署名に用いる秘密鍵以外の暗号鍵）に関しては、その生成・保管は安全な設備を用いて行い、定められた時期に適正に更新し、危殆化時には速やかに廃棄する措置をとります。

7. 時刻認証サービス運用規程の管理

7.1. 時刻認証サービス運用規程の変更

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します。

7.2. 時刻認証サービス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、変更後の本規程を公開します。本サービスの利用者に対しては、リポジトリに公開するとともに、登録された連絡先に速やかに通知を行います。

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、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、あらかじめその旨を総務大臣に届け出るとともに、速やかに休止する旨を利用者及び検証者へ通知又は連絡します。

通知又は連絡する内容には、休止する認定業務の内容、休止する年月日、休止期間、休止の理由、利用者及び検証者からの苦情又は相談に応ずる連絡先、 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。）、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を含めるものとします。

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、速やかに再開する旨を利用者及び検証者へ通知又は連絡します。通知又は連絡する内容には、再開計画を含めるものとします。

9. タイムスタンプトークンのプロファイル

フィールド	意味	値
TimeStampToken		
ContentInfo		
ContentType	content(データ)の型	1.2.840.113549.1.7.2(pkcs7-signedData
Content		
Version	CMS のバージョン	3
digestAlgorithms	署名に使用するダイジェストアルゴリズムの識別子	2.16.840.1.101.3.4.2.3(SHA-512)
encapContentInfo		
eContentType	署名の対象となるデータの型	1.2.840.113549.1.9.16.1.4 (id-smime-ct-TSTInfo)
eContent	署名の対象となるデータ	(下記「TSTInfo」参照)
certificates	署名の検証に必要な証明書のリスト	
certificate	TSA の公開鍵証明書、中間 CA 証明書、ルート CA 証明書	
signerInfos	署名者に関する情報	
Version	CMS のバージョン	1
Sid	署名者(TSA)を識別するための情報	
digestAlgorithm	署名に使用するダイジェストアルゴリズムの識別子	2.16.840.1.101.3.4.2.3(SHA-512)
signedAttrs	署名の属性	
Attribute		
attrType	属性のタイプ	1.2.840.113549.1.9.3 (ContentType)
AttributeValue	属性の値	1.2.840.113549.1.9.16.1.4 (id-smime-ct-TSTInfo)
Attribute		
attrType	属性のタイプ	1.2.840.113549.1.9.4 (messageDigest)
AttributeValue	属性の値	署名の対象となるデータのハッシュ値
Attribute		
attrType	属性のタイプ	1.2.840.113549.1.9.16.2.47 ※id-smime-aa-signingCertificateV2
AttributeValue	属性の値	
signatureAlgorithm	署名に使用するアルゴリズム	1.2.840.113549.1.1.13 SHA512 with RSA Encryption (RSASSA-PKCS1-v1_5)
Signature	署名値	
TSTInfo		
Version	TST のフォーマットバージョン	1
TSAPolicyId	サービスポリシーの識別子	1.3.6.1.4.1.1291.1.1.1.1
messageImprint		
hashAlgorithm	ハッシュアルゴリズム	2.16.840.1.101.3.4.2.1(SHA-256) 2.16.840.1.101.3.4.2.2(SHA-384) 2.16.840.1.101.3.4.2.3(SHA-512)
hashedMessage	タイムスタンプ対象のハッシュ値	
serialNumber	タイムスタンプトークンのシリアル番号	
genTime	タイムスタンプトークン生成時の時刻情報	YYYYMMDDhhmmss[,s]Z [s]※小数点以下 3 桁まで表示
Accuracy	時刻精度	1000msec
Ordering	タイムスタンプトークン発行の順序性の有無	false
Nonce	特定の要求を識別するための値	ランダム値
Tsa	タイムスタンプユニットの識別情報	TSA 公開鍵証明書の DN に従う
Extensions	拡張領域	使用しない

【付録】略語と用語解説

項目	説明
認証局(CA)	(Certification authority) PKI における公開鍵証明書を発行する機関。
日本標準時(JST)	独立行政法人情報通信研究機構(NICT)が管理・発信する日本国の標準時刻。UTC を 9 時間進めたものに等しい。
NIST	(National Institute of Standards and Technology) 米国商務省標準化技術研究所。
公開鍵証明書(PKC)	(Public-key certificate) ITU/ISO X.509 に規定された公開鍵証明書を示す。公開鍵が本人の持つ秘密鍵に対応していることを証明する。
RSA	大きな桁数の素因数分解が困難であることを利用した公開鍵暗号の方式の一つ。
SHA-(n)	ハッシュ関数のひとつ。NIST によって米国政府の標準ハッシュ関数 Secure Hash Standard(SHS)として採用されている。
国際原子時(TAI)	1958 年 1 月 1 日 0 時 0 分 0 秒を世界時の原点とした原子時間。
時刻認証局(TSA)	(Time－stamping authority) 公開鍵インフラストラクチャー(PKI)の技術に基づく TST を発行する信頼ある第三者機関。
タイムスタンプユニット(TSU)	RFC3161 タイムスタンププロトコルに準拠した TST を発行するサーバ。
タイムスタンプトークン(TST)	RFC3161 に準拠した様式に基づき、時刻認証局(TSA)によってデジタル署名された電子情報。
協定世界時(UTC)	(Coordinated universal time) 国際原子時(TAI)と地球の自転を基準とした世界時とのズレが 0.9 秒以上にならないように「うるう秒」で調整した時刻。
X.509	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。
リポジトリ	TST の検証に必要な関連情報等を格納するシステム。
DR 環境	Disaster Recovery（災害対策）環境

以上