タイムスタンプサービス運用規程

2.3 版

2011 年 7 月 7 日

改版履歴

版	変更日付	変更箇所	変更内容
初版	2004年9月21日		初版作成
1.1版	2005年3月4日	全般 許容誤差(時刻精度) タイムスタンプトークンの失効条件	用語の変更 許容誤差を±1秒以内に変更 時刻精度に問題がある場合は予め発行しないことで、時刻精度を理由とするタイムスタンプトークンの失効を廃止
2.0版	2005年11月30日	全般 1.2.2 1.3.2 a) 1.3.2 (3) 2.1.5 (1) 4.7.1 4.8 6 6.1.5 6.2.1 6.3 8	10年有効サービスへの変更のため2.0版に版数アップ サービスのOIDを変更。伴いポリシーのOIDも変更 SHA-1をSHA-512に変更。 タイムスタンプの有効期間変更(5年→10年) 公開鍵証明書の有効期間変更(6年→11年) アーカイブ保管期間変更(10年→15年) 鍵更新タイミング変更(5年前→10年前) 章タイトル変更 公開鍵長修正(1024→2048) FIPS認定変更(FIPS 140-1 レベル3→FIPS 140-2 レベル3) 公開鍵証明書の有効期間変更(6年→11年) 秘密鍵の活性期間説明変更(5年前→10年前) 文書ハッシュアルゴリズム変更(SHA-1→SHA-512) 署名アルゴリズム変更(SHA-1 with RSA Encription → SHA512 with RSA Encription) TSAのポリシーOID変更(0 2 440 200185 1 1 1→ 0 2 440 200185 1 2 1)
2.1版	2006年9月21日	1.2.1 1.2.2 2.3.2(3) 3.2 4.1 4.5.1 4.6.4 4.6.5 5.2	バージョン番号、および作成日を変更 公開鍵証明書ポリシー修正(1.2.392.20075.2.7→ 1.2.392.200075.2.7) 通知先届出がなされない場合について追記 加入申請者の真偽を確認する条件を追記 個人情報が提供されない加入申請の取り扱いについて追記 通知先届出がなされない場合について追記 タイトルおよび本文変更(バックアップ手順→保管手順) セキュリティ検査ログ収集方法(自動的に収集→収集) 不適当な記述(冗長な表現)を修正
2.2版	2010年6月15日	1.2.1 1.2.2 1.3.1(2) 1.3.1(3) 2.1.4(3) 2.5.2 4.5.1(2) 4.11(1) 4.11(2) 4.6.5 6.5、6.6、6.7 8	バージョン番号、および作成日を変更 サービスおよびポリシーOIDの変更 時刻配信局の変更 認証局の変更 誤差の値の変更 失効情報の追加 サービスを一時停止する事由の修正 時刻配信局の変更 時刻配信局の変更 セキュリティ検査ログの収集方法について修正 重複している記述を修正 誤記の修正 eContentTope → eContentType parameters の追加 GenTime の変更 TSApolicyIdの変更 Orderingの変更
2.3版	2011年7月7日	1.2.1 1.2.2 1.3.1(3) 8	バージョン番号、作成日および適用開始日を変更 タイムスタンプポリシーおよびタイムスタンプ局が利用する認証局のポリシーの変更 認証局およびサービスの変更 TSApolicyIdの変更

目次

1. はじめに

本規程では、株式会社 PFU(PFU)が運営するタイムスタンプ局が行うタイムスタンプサービス(本サービス)についての基本的事項について述べる。本規程で取り扱うタイムスタンプは IETF RFC 3161「Public Key Infrastructure: Time-Stamp Protocol(TSP)」に準拠して発行されるものとする。また、本規程の構成及び記載事項は、電子商取引推進協議会の「タイムスタンプサービスの運用ガイドライン」を参考としている。

1.1 概要

本規程は、PFU が運営するタイムスタンプ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ある。

本規程の適用対象は本サービスのすべての申請者、加入者、依存者、及び本サービスに関連する個人・法人・組織を含む。本規程ではタイムスタンプ局、すべての申請者、加入者、依存者、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する。

タイムスタンプ局は、タイムスタンプポリシー（Time-stamp policy）及びタイムスタンプ局運用規程（Time-stamping practice statement）をそれぞれ独立したものとせず、本規程をタイムスタンプ局の本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運用規程

バージョン　:2.3 版

作成日　:2011 年 07 月 07 日

作成者　:株式会社PFU

本バージョンの運用規程の適用開始日:2011 年 08 月 01 日

1.2.2 本サービスとOID

本規程において適用するオブジェクト識別子（OID）を以下に示す。

- 株式会社PFU　:0.2.440.200185
- タイムスタンプサービス　:0.2.440.200185.1.2
- タイムスタンプポリシー　:0.2.440.200185.1.2.3
- タイムスタンプ局が使用する時刻ソース

  SecureNTP 時刻配信サービス　:0.2.440.200125.1.6

  時刻監査証明書ポリシー　:0.2.440.200125.1.6.1
- タイムスタンプ局が利用する認証局のポリシー

  Security Communication RootCA タイムスタンプサービス用証明書ポリシー ： 1.2.392.200091.100.901.2

1.3 定義と適用範囲

1.3.1 定義

（1） タイムスタンプ局（TSA）

本規程においてタイムスタンプ局とは、時刻ソースから時刻の提供を受けて、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う。本規程においてタイムスタンプ局とは、本タイムスタンプ局のことをいう。

（2） 時刻配信局(TA)

本規程において時刻配信局とは、4.12 に従い協定世界時(UTC)に対するトレーサビリティを有する時刻ソースとして、タイムスタンプ局の管理するタイムスタンプユニット(TSU)にUTC に同期した時刻の配信を行い、かつタイムスタンプユニット内の時計の時刻監査を行う事業者をいう。タイムスタンプ局はセイコーインスツル株式会社が運営する SecureNTP 時刻配信局を時刻配信局とし、同局が実施する SecureNTP 時刻配信サービスを用いる。

（3） 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、タイムスタンプ局のタイムスタンプユニット、または、時刻配信局の時刻配信サーバが使用する PKI の公開鍵証明書の認証を行う事業者をいう。タイムスタンプ局の認証局はセコムトラストシステムズ株式会社とし、同社が実施するパブリック CA 署名サービスを用いる。時刻配信局の認証局については、時刻配信局の運用規程を参照。

（4） 加入者

本規程において加入者とは、タイムスタンプ局の提供する本サービスへの加入（本サービスの利用）申込みを行い、タイムスタンプ局から本サービスへの加入（本サービスの利用）を認められ、そのサービスを受ける者をいう。

（5） 依存者

本規程において依存者とは、タイムスタンプ局が発行したタイムスタンプトークンを利用、または検証する者をいう。前項に定める加入者はタイムスタンプトークンを利用または検証する場合において依存者となる。

（6） 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とは、1.3. 3(1)に記載されていることを目的として、加入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う。タイムスタンプトークンには、発行したタイムスタンプユニットによる発行時刻および同ユニットの識別情報が記載される。

また、タイムスタンプトークンのプロファイルは 8.に記載される。

（7） 時刻監査証明書

本規程において時刻監査証明書とは、タイムスタンプトークンを発行したタイムスタンプユニットの時刻ソースやタイムスタンプユニットが時刻監査を受けた日時及びそのときの時刻誤差が記載された電子証明書をいう。時刻監査証明書は、時刻配信局からタイムスタンプ局へ発行される。時刻配信局が監査した時点において、タイムスタンプユニットの時計の誤差が UTC に対して±500 ミリ秒の範囲内であった場合、タイムスタンプユニットは時刻監査証明書の有効期間内に限りタイムスタンプトークンを発行することができる。

また、タイムスタンプ局が時刻監査証明書をタイムスタンプトークンに含めることは自由とする。

（8） 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トークン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する。

1.3.2 タイムスタンプサービスの内容

本サービスの内容は以下のとおりとする。

（1） タイムスタンプ局は、加入者の依頼に基づき、加入者から送付されたハッシュ値に対して RFC3161 に準拠したタイムスタンプトークンを生成し、それを加入者に対して発行する。

a） 適用されるハッシュアルゴリズムは SHA-512 とする。

b） タイムスタンプトークンはタイムスタンプ局が管理する任意のタイムスタンプユニットを用いて生成され、タイムスタンプユニット毎の秘密鍵を用いて電子署名が行われる。

c） タイムスタンプ局は、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。

d） タイムスタンプトークンには加入者を特定する情報は含まれない。

e） タイムスタンプ局と加入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う。通信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が示す時刻は本規程に基づいて下記の条件で付与される。

a） タイムスタンプトークンに記載される時刻はタイムスタンプユニット内の時計の時刻とする。

b） 2.1.4 (1) に基づき時刻配信局が行う時刻監査によりタイムスタンプユニット内の時計の時刻が UTC に対して ±500 ミリ秒を超える誤差が確認された時点で 2.1.4 (2) に従いタイムスタンプユニットのタイムスタンプトークンの発行機能が停止する。

c） 個々のタイムスタンプトークンの発行時点において、時刻配信局以外の UTC に同期した時刻ソースとの比較により、タイムスタンプユニットが生成したタイムスタンプトークンの記載時刻に UTC に対して±1秒を超える誤差があることをタイムスタンプ局が確認したタイムスタンプトークンは、タイムスタンプ局内で破棄され利用者に対して発行されない。

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。タイムスタンプトークンのシリアル番号も複数のタイムスタンプユニットにより発行されるため有意性はないものとする。

e） タイムスタンプトークンに記載される時刻は、タイムスタンプユニット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する。

f） タイムスタンプ要求の受け付け順位と、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） タイムスタンプトークンの有効期間は、タイムスタンプトークンの電子署名に使用する 6. 3 に記載する秘密鍵に対応する公開鍵証明書の有効期間とする。6.3 に従い、タイムスタンプ局は加入者に発行されるタイムスタンプトークンについて 10 年間の有効期間を確保するものとする。ただし 4.9.2 に記載の場合については、これに限らない。

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、タイムスタンプ局の加入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する。加入者、依存者は上記の用途でのみタイムスタンプトークンを利用することが出来る。また加入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である。

（2） 禁止される用途

加入者、依存者は、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タイムスタンプトークンを使用してはならない。

1.4 本規程に関する問い合せ先

本規程に関する問い合わせ窓口は、以下の URL に掲載する。

URL：http://www.pfutsa.net/faq

2. 一般規定

2.1 義務と責任

2.1.1 タイムスタンプ局の義務

タイムスタンプ局は、本サービスの提供にあたって本規程に従い加入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う。ただし、タイムスタンプ局は、加入者または依存者が本規程に基づいてタイムスタンプ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して何らの責任も負わないものとする。

（1） タイムスタンプトークンの生成・発行

タイムスタンプ局は、本規程に基づきタイムスタンプトークンを生成し、加入者に対して発行する。

（2） 時刻の管理

タイムスタンプ局は、発行するタイムスタンプトークンの発行時刻が1.3.2.(2) のc） に規定する誤差を超えないように、タイムスタンプ局のシステムの時刻管理を行う。

（3） セキュリティ管理

タイムスタンプ局は、本サービスを提供するためにタイムスタンプユニットの時刻や秘密鍵、その他の機器及びシステムやデータを管理する。

（4） 秘密鍵の失効申請と届出

タイムスタンプユニットの秘密鍵が危殆化した場合、タイムスタンプ局は当該秘密鍵の失効を認証局に申請する。その後加入者に連絡を行う。また、タイムスタンプユニットの秘密鍵が危殆化した場合以外の理由で秘密鍵の失効を行う場合、タイムスタンプ局は、加入者に対して事前に連絡を行う。

なお加入者への連絡方法等は、2.3.2.(3)に定めるとおりとする。

2.1.2 加入者の義務

加入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、本規程に基づいてタイムスタンプ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もとづいて発行されており、加入者はこれを十分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

加入者は本規程を遵守すると共に、タイムスタンプトークンを複製・配布する場合、依存者に対して本規程を遵守させなければならない。

（3） リポジトリまたは通知の確認

加入者はリポジトリまたはタイムスタンプ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。

2.1.3 依存者の義務

依存者はタイムスタンプトークン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する。また、本規程に基づいてタイムスタンプ局より発行されたタイムスタンプトークンを利用する場合、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タイムスタンプトークンを利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検証義務

依存者はタイムスタンプトークンを利用するにあたっては、タイムスタンプトークンを検証しなければならない。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、タイムスタンプトークン自体の署名確認、タイムスタンプトークン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およびタイムスタンプトークンの失効確認を含む。

（2） 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もとづいて発行されており、依存者はこれを十分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。

2.1.4 時刻配信局の義務

時刻配信局 は、タイムスタンプ局に対して次の義務を負う。

（1） 時刻配信局は、タイムスタンプ局のタイムスタンプユニットに対して時刻の配信及び監査を少なくとも 1 日 1 回実施する。

（2） タイムスタンプ局のタイムスタンプユニットに対する時刻監査の結果、UTC に対する時刻誤差の測定値が±500 ミリ秒以内の場合は、当該タイムスタンプユニットに対して 25 時間有効の時刻監査証明書を発行し、当該時刻監査証明書の有効期間内においてタイムスタンプユニットがタイムスタンプトークンを発行することを許可する。また、時刻監査実施時の時刻誤差の測定値が±500 ミリ秒を超えている場合は、タイムスタンプユニットのタイムスタンプトークンの発行機能を停止する処置を行う。

（3） 時刻配信局で使用する時計の UTC に対する時刻同期精度については、その誤差が±30 ミリ秒を超えないように維持し、うるう秒を国家時刻標準機関の告示に基づき設定するとともに、UTC に対する時刻のトレーサビリティを維持する。

（4） 時刻配信サーバ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、直ちに認証局に鍵の失効申請を行うとともにタイムスタンプ局に通知する。

（5） タイムスタンプ局に対して発行した時刻監査証明書及び当該時刻監査と時刻監査証明書の発行等に関する時刻監査ログ、ならびに時刻配信局内の装置に対して発行した時刻監査証明書、時刻配信局が作成する UTC との時刻比較データ等 UTC に対する時刻のトレーサビリティを証明するためのデータを 10 年間安全に保管する。なお時刻配信局は、タイムスタンプ局からの依頼があった場合、当該データの提供を行う。

2.1.5 認証局の義務

タイムスタンプ局の認証局はタイムスタンプ局への証明書発行サービスにおいて、タイムスタンプ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タイムスタンプ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 11 年間とする。

（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、直ちにその旨をタイムスタンプ局に通知する。

（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タイムスタンプ局に通知する。また、タイムスタンプ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う。

2.1.6 リポジトリに関する義務

タイムスタンプ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 財務上の責任

2.2.1 損害賠償責任

タイムスタンプ局の故意または過失に起因して、加入者に損害が生じた場合その賠償に代えて、タイムスタンプ局は、その対象となるタイムスタンプ局の発行したタイムスタンプトークンの数量に相当する数量を限度として、加入者からのタイムスタンプトークンの発行依頼に無償で応じるものとする。4.9.3 で定めるタイムスタンプトークンの無償発行が、タイムスタンプ局の賠償責任の全てとし、タイムスタンプ局は、依存者に対する損害賠償は行わない。但し、法令により強制される場合には、タイムスタンプ局は、同一原因から生じた加入者および依存者の損害総額に対して10万円を上限として、加入者または依存者に対してタイムスタンプ局の過失により生じた損害を賠償するものとする。なお、タイムスタンプ局の責に帰することができない事由から生じた損害、逸失利益、予見の有無を問わず特別の事情から生じた損害は賠償する損害の範囲には含まれない。

2.2.2 免責事項

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、タイムスタンプ局は賠償義務を負わない。

（1） タイムスタンプ局が本規程ならびに個別のサービス契約にしたがい、本サービスを適正に遂行していた場合。

（2） 加入者または依存者の故意、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） 加入者または依存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） 加入者または依存者のシステムに起因して損害が発生した場合。

（5） 次にあげるタイムスタンプ局の支配を超えた事由に起因して損害が発生した場合。

a） 火災、地震、噴火、津波、台風等の天災地変。

b） 戦争、暴動、変乱、争乱、労働争議。

c） 放射性物質、爆発性物質、環境汚染物質。

d） 通信回線の不通。

e） その他のタイムスタンプ局の支配を超えた事由。

（6） 4.5.1、4.5.3、4.5.5 及び 4.10 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。

（7） タイムスタンプ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、またはセキュリティ手段が破られた場合。

（8） 4.9.2 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する。

2.3.2 可分性、効力の存続、通知

（1） 可分性

本規程のある規定またはその適用が、何らかの理由により無効または執行不可能であるとされた場合、当該規定のみが無効また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る。

（2） 効力の存続

タイムスタンプ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、2.7、2.8 の効力は有効に存続する。

（3） 通知

加入者からタイムスタンプ局への通知は書面また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う。書面による通知は受領日をもって有効とする。ただし本サービスの利用の加入申請の時に加入者からタイムスタンプ局に対して加入者の連絡先等の個人情報の届出がなされない場合についてはこの限りでなく、タイムスタンプ局から加入者への通知は行わない。

タイムスタンプ局から加入者への通知は、個別のサービス契約に基づき加入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。加入者は連絡先を変更する場合、速やかにタイムスタンプ局に届け出る。当該届け出がなされない場合においては、タイムスタンプ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。

2.3.3 紛争解決

本規程またはタイムスタンプ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。本規程また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 タイムスタンプ局に関する情報の公開

タイムスタンプ局は、2.5.4 に定めるリポジトリに次の情報を公開する。

（1） タイムスタンプ局運用規程（本規程）

（2） 公開鍵証明書情報

（3） 告知書（公開鍵証明書失効情報を含む）

2.5.2 公開情報の更新

公開する情報の更新は次のとおりとする。

（1） タイムスタンプ局運用規程の変更の都度

（2） 公開鍵証明書失効情報を認証局より取得した時

（3） その他タイムスタンプ局の責任者が必要と判断した時

2.5.3 アクセス制御

タイムスタンプ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する。

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。

2.5.4 リポジトリ

2.5.1 において定める情報をリポジトリに公開する。

URL: https://www.pfutsa.net/repository/

2.6 準拠性監査

2.6.1 監査頻度

タイムスタンプ局は監査人による監査を年1回定期的に実施する。また、タイムスタンプ局組織は、必要に応じて定期監査以外に監査を実施する。

2.6.2 監査人の身元・資格

タイムスタンプ局の監査人には、PFU 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。必要に応じて外部の監査会社に監査を依頼する。監査人の任命はタイムスタンプ局の責任者が行う。

2.6.3 監査人と被監査部門の関係

タイムスタンプ局の監査を実施する監査人として、タイムスタンプ局の業務を直接担当しない者を選定する。

2.6.4 監査テーマ

本サービスが本規程に準拠して実施されていること、並びに外部からの不正及び内部の不正行為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。

2.6.5 監査指摘事項への対応

タイムスタンプ局は、重要又は緊急を要する監査指摘事項について、タイムスタンプ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ユニット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、タイムスタンプ局のタイムスタンプユニットの運用を停止するか否かはタイムスタンプ局の責任者が決定する。またタイムスタンプ局の責任者は、タイムスタンプ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。

2.6.6 監査結果の報告

タイムスタンプ局の監査結果は、監査人からタイムスタンプ局の責任者に対して監査報告書として提出される。

2.7 機密保持

2.7.1 機密扱いとする情報

漏えいによってタイムスタンプ局、加入者、時刻配信局、または認証局の認証業務の信頼性が損なわれる虞のある情報を、タイムスタンプ局は機密扱いとする。タイムスタンプ局は、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、安全に保管管理する。

機密扱いとする情報は、本規程または本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本サービスの範囲を超えて使用しないものとする。

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（承認されたか否かを問わない）

（2） タイムスタンプ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、ならびにタイムスタンプ局の運営についてのセキュリティ対策

（5） タイムスタンプ局が加入者に提供した加入者を識別するための情報

加入者は、タイムスタンプサービスを受けるにあたりタイムスタンプ局から提供された加入者を識別するための情報を開示・漏洩してはならない。

2.7.2 機密扱いとしない情報

2.7.1 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

2.7.3 公開鍵証明書失効情報の公開

タイムスタンプ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る。

2.7.4 法執行機関への情報開示

タイムスタンプ局で取扱う情報(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する。

2.7.5 その他の理由に基づく情報開示

タイムスタンプ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。

2.8 知的財産権

以下の各号に定めるものを含み、タイムスタンプ局が作成した文書、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)はタイムスタンプ局またはそのライセンサーに帰属し、加入者その他の者には移転しないものとする。

(1) タイムスタンプ局から発行されたタイムスタンプトークン

(2) タイムスタンプ局が用意するタイムスタンプトークン検証用ソフトウェア

(3) 本規程

なお、タイムスタンプトークンに添付された時刻監査証明書の知的財産権は時刻配信局に帰属し、加入者その他の者には移転しないものとする。

2.9 個人情報の取り扱い

タイムスタンプ局は、本サービスの利用契約締結時に加入者から提供される個人情報を、以下に特定する範囲をこえて使用しない。また、その保護について、以下に従うものとする。ただし、法令に定められた場合はこれに限らない。

(1) 入手する個人情報の位置付け

タイムスタンプ局は、加入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。

(2) 利用目的の特定

タイムスタンプ局は、加入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する。なお加入者から別途承諾を得た場合、タイムスタンプ局は、本サービスに関連した自らまたは自らの子会社の商品等の案内のために利用することがある。

(3) 利用目的による制限

タイムスタンプ局は、上記 2.9(2)に規定される目的以外に個人情報を利用しない。

(4) 保有個人情報に関する事項の公開

タイムスタンプ局は、個人情報の利用目的を本規程に記載し公開する。

(5) 正確性の確保

タイムスタンプ局は、個人情報を加入者からの申し出に基づき正確な状態で管理する。

（6） 安全管理措置

タイムスタンプ局は、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、改ざん、漏えい等の防止に努める。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う。

（7） 開示・訂正

タイムスタンプ局は、個人情報について、本人から開示、訂正もしくは削除を求められた場合、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

タイムスタンプユニット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

タイムスタンプ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ユニットの固有名称は、認証局が発行したタイムスタンプユニット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

タイムスタンプ局の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ユニットの固有名称は、タイムスタンプユニット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 加入申請者の認証と利用可否

タイムスタンプ局は、加入申請の時点でタイムスタンプ局に加入者の個人情報が提供された場合に限り、合理的な範囲内で本サービスの加入申請者の真偽を確認し、利用可否を判断する。

ただし、加入申請の時点でタイムスタンプ局に加入者の個人情報が提供されなかった場合には、タイムスタンプ局はこの確認・判断を行わない。

3.3 本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う。

3.4 本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う。

4. 運用要件

4.1 本サービスの加入申請

本サービスの加入を申請する者は、タイムスタンプ局が用意する本サービスの利用に関する契約を締結しなければならない。

タイムスタンプ局は、当該契約の締結に先立って、加入申請の時点で加入者の個人情報がタイムスタンプ局に提供された場合に限り、当該加入申請者に対する審査を行い、本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、当該加入申請者からの本サービスの利用に関する契約の申し込みを承諾し、当該加入申請者と本サービスの利用に関する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加入者を識別するための情報を加入者に提供する。

なお、第三者が加入申請を仲介する場合には、タイムスタンプ局は当該第三者に対する審査を行い、本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、当該第三者からの本サービスの利用に関する契約の申し込みを承諾し、当該第三者と本サービスの利用に関する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加入者を識別するための情報を当該第三者に提供する。この場合、加入者は当該第三者との間で本サービスの利用に関する契約を締結することにより、本サービスを利用することができる。

4.2 タイムスタンプ要求

本サービスの加入者は、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、タイムスタンプ局へ送付する。タイムスタンプ局と加入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する。

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らない。

4.3 タイムスタンプトークンの発行

タイムスタンプ局は、加入者からのタイムスタンプ要求が有った場合、タイムスタンプ要求を正しく受け付けたか、拒否したか、またはその他の応答の状態(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、タイムスタンプ局の管理する任意のタイムスタンプユニットを用い、1.3.2 に規定されるタイムスタンプトークンの作成をおこない、それを加入者に対して発行する。タイムスタンプ局と加入者間の通信手段及びタイムスタンプトークンの発行の詳細手順の情報が必要な場合には、PFU と秘密保持契約を締結の上、無償で入手することができる。

4.4 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を受領した者は、以降に記す方法でタイムスタンプトークンの検証を行う。

（1） タイムスタンプ対象電子データのハッシュ値とタイムスタンプトークン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タイムスタンプトークンが対である、あるいは、対象電子データが改ざんされていない事を確認する。

（2） タイムスタンプトークンに含まれる公開鍵証明書を利用して、タイムスタンプ局の電子署名の確認を行うことによ

り、タイムスタンプトークンが改ざんされていない事を確認する。

(3) タイムスタンプトークンに含まれる、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する。

4.5 本サービスの一時停止と解約

4.5.1 本サービスの一時停止

タイムスタンプ局は、下記の事由が発生した場合に予告なしに本サービスを一時停止することができる。

(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) 運用上またはセキュリティ管理上中断がやむを得ない場合。ただし、定期的な点検整備(時刻配信局および認証局の点検整備による場合を含む)及び4. 11に記載しているうるう秒の設定による中断については1週間前までに加入者に通知するとともに、下記URLにて公開する。

URL: http://www.pfutsa.net/

ただし加入申請にあたり加入者の個人情報の届出がタイムスタンプ局に対してなされない場合についてはこの限りではなく、タイムスタンプ局は加入者への通知を行わない。

(3) 時刻配信局または認証局が一時停止または終了し、タイムスタンプ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) タイムスタンプ局の秘密鍵の漏洩、偽造また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

4.5.2 本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う。

4.5.3 加入者における本サービスの一時停止

タイムスタンプ局は下記の事由が発生した場合、予告なしに加入者の本サービスの利用を一時停止することができる。

(1) 加入者の債務不履行により、該当加入者に対する本サービスの提供を中断する場合

(2) 加入者が本サービスの利用の一時停止を申請した場合

4.5.4 加入者における本サービス利用の一時停止の解除

該当する加入者において本サービスの利用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利用の一時停止の解除を行う。

4.5.5 本サービスの解約

タイムスタンプ局は、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。

（1） 加入者が加入の解約を申請した場合

（2） 加入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、なお改善が見られない場合

（3） タイムスタンプ局が本サービスを終了する場合

（4） 加入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、または金融機関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、また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、合併または営業の全部もしくは重要な一部の譲渡の決議をしたとき

f） 財産状態が悪化したとき、また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、タイムスタンプ局の利益を損なうと認められるとき

4.6 セキュリティ検査の手順

タイムスタンプ局は、そのシステムの安全性及び信頼性を維持するため、タイムスタンプ局の本サービスに関わる情報を記録し、これを定期的に検査する。

4.6.1 セキュリティ検査ログに記録する情報

セキュリティ検査ログに記録する情報はタイムスタンプ局のシステムにおけるセキュリティに関する重要な事象を対象とし、少なくとも下記のものを記録する。

（1） タイムスタンプトークンの発行記録（または、発行したタイムスタンプトークンのコピー）

（2） 時刻配信局より受けた時刻監査記録（または、時刻監査証明書のコピー）

（3） 加入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

（4） タイムスタンプ局で使用する鍵ペアの生成・失効記録

（5） タイムスタンプ局設備への入退室記録及びそれに対する承認記録

（6） タイムスタンプ局システムに対する操作記録

（7） タイムスタンプ局システムの動作異常の記録

（8） タイムスタンプ局システムに対する不正アクセスに関する記録

4.6.2 セキュリティ検査ログの検査頻度

セキュリティ検査ログの検査は、月次を最低頻度としてこれを行う。

4.6.3 セキュリティ検査ログの保護

セキュリティ検査ログは、所定の方法・手順により改ざん、削除、外部への流出等から保護する。

4.6.4 セキュリティ検査ログの保管手順

セキュリティ検査ログは、所定の方法・手順により保管を行う。

4.6.5 セキュリティ検査ログの収集

タイムスタンプ局では、セキュリティに関する重要な事象を定期的にセキュリティ検査ログとして収集する。

4.6.6 脆弱性の評価

タイムスタンプ局は運用面及びシステム面におけるセキュリティ上の脆弱性を評価する。セキュリティ上の問題が有れば、タイムスタンプ局の責任者に報告し、再評価において問題が認められた場合は是正処置を行う。

4.7 アーカイブ

4.7.1 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。

（1） 監査報告書（15 年）

（2） タイムスタンプトークンの発行記録（または、発行したタイムスタンプトークンのコピー）（15 年）

（3） 時刻配信局より受けた時刻監査記録（または、時刻監査証明書のコピー）（15 年）

（4） 加入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（15 年）

（5） タイムスタンプ局で使用する鍵ペアの生成・失効記録（15 年）

（6） タイムスタンプ局設備への入退室記録及びそれに対する承認記録(3 年)

（7） タイムスタンプ局システムに対する操作記録(3 年)

（8） タイムスタンプ局システムの動作異常の記録(3 年)

（9） タイムスタンプ局システムに対する不正アクセスに関する記録(3 年)

4.7.2 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・手順により改ざん、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。

4.7.3 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。

4.8 鍵更新

タイムスタンプ局はタイムスタンプユニットの公開鍵証明書の有効期間が満了する 10 年前に鍵ペアの更新を行い、従来使用していた秘密鍵は所定の手順で安全に破棄するが、公開鍵証明書の失効申請は行わない。

4.9 危殆化と災害からの復旧

4.9.1 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う。

4.9.2 タイムスタンプトークンを失効する場合の要件

認証局、時刻配信局の時刻配信サーバまたはタイムスタンプ局のタイムスタンプユニット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、認証局が発行したタイムスタンプ局の公開鍵証明書が誤って発行され、当該の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。

4.9.3 タイムスタンプトークンを無償発行する場合の要件

前項によりタイムスタンプトークンが失効した場合は、タイムスタンプ局は、以下の場合に限り、当該タイムスタンプトークンの数量に相当する数量を限度として、加入者からのタイムスタンプトークンの無償発行に応じる。ただし、認証局、時刻配信局またはタイムスタンプ局の秘密鍵のアルゴリズムが危殆化した場合には、対応するタイムスタンプトークンの無償発行は行わないものとする。

(1) タイムスタンプ局の秘密鍵が危殆化した場合(2.2.2(7)の場合は除く)

(2) タイムスタンプ局が誤った時刻配信局の時刻監査証明書を受け取った場合

(3) タイムスタンプ局が誤った公開鍵証明書を用いたタイムスタンプトークンを発行した場合

4.9.4 秘密鍵が危殆化した場合の対処

タイムスタンプユニットの秘密鍵が危殆化した場合は、本サービスを停止し、次の手続を行う。

(1) 認証局に対してタイムスタンプユニットの公開鍵証明書の失効に関する申請手続

(2) タイムスタンプユニットの秘密鍵の破棄及び再生成手続

(3) タイムスタンプユニットの新しい鍵に対する公開鍵証明書の発行申請手続

(4) 加入者に秘密鍵の危殆化の通知

4.9.5 災害等発生時の設備の確保

災害等によりタイムスタンプ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。

4.10 本サービスの終了

(1) タイムスタンプ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。

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) タイムスタンプ局の秘密鍵の漏洩、偽造また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) 時刻配信局または認証局が一時停止または終了し、タイムスタンプ局が本サービスを継続することが困難となった場合

d) その他タイムスタンプ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、タイムスタンプユニットの公開鍵証明書の失効申請日並びに本サービス終了後のタイムスタンプ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60日前までに加入者及び依存者に公開または通知する。

(3) 本サービス終了後、速やかに全てのタイムスタンプユニットの秘密鍵を安全に破棄する。

(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。

4.11 UTCとの時刻同期

(1) 時刻同期管理

タイムスタンプ局は、時刻配信局の提供する「SecureNTP 時刻配信サービス」を使用して、全てのタイムスタンプユニットの時刻が所定の精度で UTC に同期するように管理する。

(2) うるう秒の設定

タイムスタンプ局は、時刻配信局の提供する「SecureNTP 時刻配信サービス」を使用して全てのタイムスタンプユニットのうるう秒設定を行う。

4.12 時刻のトレーサビリティ

(1) タイムスタンプ局は、時刻配信局より配信される時刻をタイムスタンプ局の時刻ソースとして使用し、タイムスタンプユニットが時刻配信局より受けた時刻監査の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する。

(2) 時刻配信局は、国家時刻標準機関が定めるサービス運用規程に基づく時刻配信情報との時刻比較および保管作業を行うことにより、UTC との時刻のトレーサビリティを確保する。

5. 物理面、手続面及び人事面のセキュリティ管理

5.1 物理的管理

5.1.1 施設の位置と建物構造

タイムスタンプ局の施設は、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ずる。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する。

タイムスタンプ局の建物、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

タイムスタンプ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する。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。

タイムスタンプ局の施設には、監視員を配置して監視システムにより 24 時間 365 日監視を行う。

5.1.3 電源設備と空調設備

タイムスタンプ局の重要な装置は、瞬断や停電に備えて無停電電源装置(UPS)に接続する。長時間停電した場合は、一定時間内に自家発電装置から電源供給を行う。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する。

5.1.4 浸水対策

タイムスタンプ局の設備を設置する建物、室には漏水検知器を設置し、天井、床には防水対策を講ずる。

5.1.5 地震対策

タイムスタンプ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ずる。

5.1.6 火災対策

タイムスタンプ局の設備を設置する建物は耐火構造、室は防火区画とし、消火設備を備える。

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う。

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う。

5.1.9 オフサイトバックアップ

重要なデータ等の媒体を別地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 手続面の管理

タイムスタンプユニットの起動・停止、タイムスタンプユニット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。

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・認証を行う。また、タイムスタンプユニットの鍵の生成・更新等の重要操作は複数の要員が立ち会って行う。

タイムスタンプ局は、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、手続的および人的なセキュリティの維持を図る。

5.3 人事面の管理

5.3.1 経歴、資格、経験及び必要条件

タイムスタンプ局は、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。

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、または本規程または本サービスに関する運用ルール、マニュアルもしくは手続に違反した場合は、タイムスタンプ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） タイムスタンプ局の設備や機器のマニュアル類

（2） タイムスタンプ局の運用に関する規程・手順書等

6. 技術的セキュリティ管理

6.1 鍵ペア生成とインストール

6.1.1 鍵ペア生成

タイムスタンプユニットの鍵ペアは、複数人立ち会いのもとで暗号モジュール（HSM）を用いて生成する。

6.1.2 タイムスタンプユニットの公開鍵の認証局への登録

タイムスタンプユニット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る。

6.1.3 認証局のルート証明書等の受領

タイムスタンプ局は、認証局から受領したルート証明書およびタイムスタンプユニット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する。

6.1.4 時刻配信局の公開鍵証明書のルート証明書の受領

タイムスタンプ局は、時刻配信局から受領した時刻配信サーバの公開鍵を証明する認証局のルート証明書を安全かつ確実に保管する。

6.1.5 鍵のサイズ

タイムスタンプユニットの鍵には RSA2048 ビットの鍵を使用する。

6.1.6 鍵を生成するハードウェア/ソフトウェア

6.2.1 に定める基準を満たす暗号モジュール(HSM)を備えたタイムスタンプユニットとする。

6.1.7 鍵の利用目的

タイムスタンプユニットの鍵は、タイムスタンプ局が発行するタイムスタンプトークンへの電子署名に使用する。

6.2 秘密鍵の保護

6.2.1 暗号モジュールに関する基準

タイムスタンプユニットの鍵は、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・保管する。

6.2.2 秘密鍵の複数人制御

タイムスタンプユニットの秘密鍵の生成、活性化、破棄等は、複数人の管理の下で行う。

6.2.3 秘密鍵の預託

秘密鍵の預託は行わない。

6.2.4 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。

6.2.5 秘密鍵のアーカイブ

秘密鍵のアーカイブは行わない。

6.2.6 暗号モジュールへの秘密鍵の格納

タイムスタンプユニットの秘密鍵は、暗号モジュール（HSM）の中で生成・保管する。

6.2.7 秘密鍵の活性化方法

タイムスタンプユニットの秘密鍵は、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する。

6.2.8 秘密鍵の非活性化方法

タイムスタンプユニットの秘密鍵は、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する。

6.2.9 秘密鍵の破棄方法

暗号モジュール（HSM）内のタイムスタンプユニットの秘密鍵の破棄は、複数人の管理のもとで所定の手続きに従い破棄する。

6.3 公開鍵と秘密鍵の有効期間

タイムスタンプユニットの公開鍵証明書の有効期間は、有効とする日から起算して 11 年とする。

また、秘密鍵の活性期間（使用期限）は公開鍵証明書の有効期間が満了する日の 10 年前までとし、活性期間（使用期限）満了前に新しい鍵ペアに交換する。

ただし、秘密鍵が危殆化した場合、またはその可能性がある場合は有効期間が満了する前に鍵の失効を行い、鍵更新を行う。

6.4 活性化データ

6.4.1 活性化データの生成とインストール

タイムスタンプユニット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、インストールを行う。

6.4.2 活性化データの保護

タイムスタンプユニットの秘密鍵に対するものを含めて、タイムスタンプ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・管理する。

6.5 コンピュータセキュリティ

タイムスタンプ局では、コンピュータ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う。

6.6 ネットワークセキュリティ

タイムスタンプ局では、ネットワークセキュリティに関して基準を設け、システム導入時や運用時にこれを遵守するための確認を行う。

6.7 暗号モジュールの技術管理

6.1.1 及び 6.2.1 において定める。

7. タイムスタンプサービス運用規程の管理

7.1 タイムスタンプサービス運用規程の変更

タイムスタンプ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 タイムスタンプサービス運用規程の公開と通知

タイムスタンプ局は、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する。

本サービスの加入者に対しては登録された連絡先に電子メールまたは郵便の発信により通知とする。依存者に対しては、本規程をリポジトリに公開することをもって通知とする。

8. タイムスタンプトークンのプロファイル

(TimeStampToken)

ContentType	
ContentType	コンテントのタイプ 型:OID 値:1 2 840 113549 1 7 2 (pkcs7-signedData)
Content	
SignedData	
version	CMSのバージョン 型:INTEGER 値:3
digestAlgorithms	署名者が使うハッシュアルゴリズムの情報
DigestAlgorithmIdentifier	
algorithm	ハッシュアルゴリズムのオブジェクトID 型:OID 値: 2 16 840 1 101 3 4 2 3 (SHA-512)
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
encapContentInfo	署名されるコンテントの情報
eContentType	コンテントタイプのオブジェクトID 型:OID

	値:1 2 840 113549 1 9 16 1 4 (id-smime-ct-TSTInfo)
eContent	コンテント(署名対象のデータ=TSTInfo)
	型:OCTET STRING
	値:derエンコードされたTSTInfo
certificates	証明書チェーン
certificate	TSAの公開鍵証明書(※CAのCPS参照)
attrCert	TAの時刻監査証明書(※TAのTPS参照)
signerInfos	署名者情報
signerInfo	
version	CMSのバージョン
	型:INTEGER
	値:1
sid	署名者ID
issuer	証明書の発行者名(※公開鍵証明書に従う)
serialNumber	証明書のシリアル番号
	型:INTEGER
	値:ユニークな整数
digestAlgorithm	署名者の使うハッシュ関数のアルゴリズム
algorithm	ハッシュアルゴリズムのオブジェクトID
	型:OID
	値:2 16 840 1 101 3 4 2 3 (SHA-512)
parameters	暗号アルゴリズムの引数
	型:NULL
	値:なし
signedAttrs	署名属性
Attribute	属性
attrType	属性のタイプ
	型:オブジェクトID

	値:1 2 840 113549 1 9 3 (ContentType)
attrValues	
AttributeValue	属性の値
	型:オブジェクトID
	値:1 2 840 113549 1 9 16 1 4 (id-smime-ct-TSTInfo)
Attribute	属性
attrType	属性のタイプ
	型:オブジェクトID
	値:1 2 840 113549 1 9 4 (messageDigest)
attrValues	
AttributeValue	属性の値
	型:OCTET STRING
	値:コンテントのハッシュ値
Attribute	属性
attrType	属性のタイプ
	型:オブジェクトID
	値:1 2 840 113549 1 9 16 2 12 (id-aa-signingCertificate)
attrValues	
SigningCertificate	証明書署名
certs	証明書
ESSCertID	証明書識別子
certHash	公開鍵証明書のハッシュ値
	型:OCTET STRING
	値:公開鍵証明書のハッシュ値
issureSerial	発行者名とシリアル番号
issure	公開鍵証明書の発行者名(※公開鍵証明書に従う)
serialNumber	公開鍵証明書のシリアル番号
	型:INTEGER
	値:ユニークな整数

ESSCertID	証明書識別子
certHash	時刻監査証明書のハッシュ値 型:OCTET STRING 値:時刻監査証明書のハッシュ値
signatureAlgorithm	署名に利用するアルゴリズム
algorithm	署名アルゴリズムのオブジェクトID 型:OID 値:1 2 840 113549 1 1 13 (SHA512 with RSA Encryption)
parameters	署名アルゴリズムの引数 型:NULL 値:なし
signature	署名値 型:OCTET STRING 値:署名値

(TSTInfo)

version	
version	タイムスタンププロトコルのバージョン 型:INTEGER 値:1
policy	
TSApolicyId	TSAのポリシーのオブジェクトID 型:OID 値:0 2 440 200185 1 2 3
MessageImprint	
MessageImprint	タイムスタンプされるデータのハッシュアルゴリズムとハッシュ値
hashAlgorithm	
AlgorithmIdentifier	ハッシュアルゴリズム
algorithm	ハッシュアルゴリズムのオブジェクトID 型:OID 値:2 16 840 1 101 3 4 2 3 (SHA-512)
parameters	暗号アルゴリズムの引数

	型:NULL 値:なし
hashedMessage	ハッシュ値 型:OCTET STRING 値:ハッシュ値
SerialNumber	
serialNumber	タイムスタンプトークンのシリアル番号 型:INTEGER 値:ユニークな整数
GenTime	
GenTime	タイムスタンプトークンの発行時刻 型:GeneralizedTime 値:YYYYMMDDhhmmss[.ssssss]Z
Accuracy	
Accuracy millis	タイムスタンプ時刻の精度 時刻精度(ミリ秒) 型:INTEGER 値: ミリ秒
Ordering	
Ordering	時刻精度上における順序性 型:BOOLEAN 値:FALSE
Nonce	
nonce	ノンス(乱数) 型:INTEGER 値:乱数
tsa	
GeneralName directoryName	TSAの識別情報 公開鍵証明書の本人名のDN(※公開鍵証明書に従う)
Extensions	
extensions	拡張領域 使用しない

付録　略語と用語解説

項目	説明
CA	Certification authority 認証局
PKC	Public-key certificate 公開鍵証明書
PKI	Public key infrastructure 公開鍵インフラストラクチャー
NIST	National Institute of Standards and Technology米国商務省標準化技術研究所
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-1,SHA-512	ハッシュアルゴリズムのひとつ。NISTによって米国政府の標準ハッシュアルゴリズムSecure Hash Standard(SHS)として採用されている
TSA	Time－stamping authority タイムスタンプ局
TSU	Time－stamp unit タイムスタンプユニット
TST	Time－stamp token タイムスタンプトークン
TA	Time authority 時刻配信局
UTC	Coordinated universal time 協定世界時
X.509	公開鍵インフラストラクチャー（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
協定世界時（UTC）	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
公開鍵証明書（PKC）	ITU/ISO X.509に規定された公開鍵証明書のこと。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証明書
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
時刻監査証明書(TAC)	時刻配信局（TA）が顧客の装置（タイムスタンプユニット等）に対して時刻の監査を行った際に発行する時刻に関する証明書のこと
時刻配信局(TA)	時刻に関する認証業務を実施する機関。タイムスタンプ（TSA）に対して標準時刻の配信と、タイムスタンプ局（TSA）が運用する時刻の監査を行う
タイムスタンプ局(TSA)	PKIの技術に基づくタイムスタンプトークン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タイムスタンプトークンを発行するサーバ
タイムスタンプトークン(TST)	RFC3161に準拠した様式に基づき、タイムスタンプ局（TSA）によって電子署名された電子情報
認証局（CA）	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
リポジトリ	タイムスタンプトークンの検証に必要な関連情報等を格納するシステム