経済産業省委託調査

平成１４年度ＥＣ技術基盤の相互運用性に関する調査研究事業

（電子署名生成・検証システムのセキュリティ環境の国際標準化等の調査）

タイムスタンプサービスの運用ガイドライン

平成15年3月

電子商取引推進協議会
財団法人日本情報処理開発協会
電子商取引推進センター

この報告書は、平成１４年度受託事業として（財）日本情報処理開発協会電子商取引推進センターが経済産業省から委託を受けて、電子商取引推進協議会（ECOM）の協力を得て実施した「平成１４年度ＥＣ技術基盤の相互運用性に関する調査研究事業（電子署名生成・検証システムのセキュリティ環境の国際標準化等の調査）」の成果を取りまとめたものです。

はじめに

タイムスタンプ事業者は、利用者にサービスを安心して利用していただく為、電子認証事業者と同様、信頼性、安全性を十分に確保して業務を行う必要がある。そのため、タイムスタンプ事業者は、信頼性、安全性を確保する観点から業務に関する運用方針を定め、サービスの信頼性向上、トラブル時の迅速な対応、責任の明確化に努めなければならない。

ここでは、タイムスタンプ事業者が、タイムスタンプ業務を行う場合の運用規程（例）を ETSI TS 102 023 及び IETF PKIX RFC2527 を参考にしながら、できるだけ実運用に適用できる内容でまとめた。また、運用規程は、タイムスタンプ方式により内容が大きく異なるため、シンプルプロトコル方式、リンキングプロトコル方式の２通りについてまとめた。運用規程の内容は事業者により異なるので、できるだけ事業者に特化した内容は避け、各事業者が参考になるような配慮すべきポイントを例として取り上げた。利用者は、運用規程（例）から、運用規程作成の参考情報を得るだけでなく、各方式の特徴、タイムスタンプ業者選定の確認項目、リスク対応を運用面から理解することができる。

運用規程例は、以下の２部で構成されている。

平成 15 年３月

財団法人日本情報処理開発協会
電子商取引推進センター
電子商取引推進協議会

シンプルプロトコルを用いた
タイムスタンプサービス運用規程 例）

目　次

1. はじめに

本規程は、タイムスタンプ事業者がタイムスタンプ業務を行う場合に必要なタイムスタンプポリシー（Time-stamp policy）及びタイムスタンプ局の運用規程（TSA practice statement）を作成するうえで、参考となることを目的に作成された。

本規程では、タイムスタンプ局が行うタイムスタンプ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、本規程の構成および記載事項は、IETF PKIX RFC 2527 「Certificate Policy and Certification Practices Statement Framework 」及び、ETSI TS 102 023 V1.1.1(2002-04)「Policy requirements for time-stamping authorities」を参考としている。

1.1 概要

本規程は、○○○○○株式会社が運営する○○○用タイムスタンプ局（以下、単にタイムスタンプ局もしくは TSA と言う）が提供する○○○用タイムスタンプサービスの運用方針およ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。本規程では本タイムスタンプ局、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（TSA 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タイムスタンプ業務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	：タイムスタンプ局運用規程
バージョン	：1.0
作成日	：2003 年ｘ月ｘ日
作成者	：○○○○○株式会社

1.2.2 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。

・○○○用タイムスタンプポリシー：x.x.xxx.xxx.x.x

・本タイムスタンプ局が使用する時刻ソースのポリシー

○○○時刻配信局　△△△時刻配信サービスポリシー：y.y.yyy.yyy.y.y

1.3 コミュニティと適用範囲

1.3.1 タイムスタンプの関係者

（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、信頼される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。

（以降、単にタイムスタンプ局または TSA と記載した場合は、本タイムスタンプ局のことをいう。）

（2）時刻配信局(TA)

時刻配信局は、信頼され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サーバ(TSS)に UTC に同期した時刻の配信を行い、かつタイムスタンプサーバが運用する時刻の監査を行う。本タイムスタンプ局は○○○時刻配信局が実施する△△△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、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サーバ、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局とする。

本タイムスタンプ局の CA は XXXX 認証局とする。

（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サービスへの加入（サービスの利用）申込みを行い、タイムスタンプ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とする。

（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信頼して利用、または検証する者とする。

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。

a) 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作成し、それを加入者に対して発行する。

イ）適用されるハッシュアルゴリズムは SHA-1 とする。

備考：タイムスタンプサービスに使用されるハッシュアルゴリズムは、国家的セキュリティ評価機関によって認定されるか、タイムスタンプサービスの目的に適したアルゴリズムでなければならない。

ロ）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サーバを用いて生成され、タイムスタンプサーバ毎の秘密鍵を用いてデジタル署名が行われる。

ハ）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。

ニ）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。

ホ）タイムスタンプ局は加入者または依存者がタイムスタンプトークンを使用したことによる結果については一切責任を負わない。

へ）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。

b) 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。

イ）タイムスタンプトークンに記載される時刻は、UTC に対して±○○秒の誤差が許容されるものとする。

備考：許容される誤差は、適用する用途により異なる。

ロ）前記の許容される誤差範囲内においては、タイムスタンプトークに記載された時刻の順位に有意性はないものとする。

ハ）タイムスタンプトークンに記載される時刻は、タイムスタンプサーバ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。

ニ）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。

c) 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署名に使用する秘密鍵に対応する公開鍵証明書の有効期間とする。

イ）タイムスタンプ局が発行するタイムスタンプトークンの有効期間は少なくとも○年間以上とする。

ロ）タイムスタンプトークンへの署名に使用する秘密鍵に対応する公開鍵証明書の有効期間は「6.3 公開鍵と秘密鍵の有効期間」の項に示す期間とし、その有効期間を○年間以上残してその秘密鍵の使用を停止し、タイムスタンプサーバ鍵ペアの更新を行う。

d) 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は、タイムスタンプサーバの時刻を監査した時刻配信局が発行した時刻監査証明書が添付される。

イ）時刻監査証明書は、時刻配信局がタイムスタンプサーバの時刻を監査したときの日時・時刻誤差及び有効期間などの情報を含む。

ロ）タイムスタンプサーバの時計の誤差が、時刻配信局が監査した時点で規格の範囲内であった場合、タイムスタンプサーバは時刻配信局より受け取った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の生成を行う。

備考：時刻監査証明書をタイムスタンプトークに添付するか否かは、任意である。

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

備考：適正な用途は個々の TSA のサービスに依存するため、本書では規定しない。
なお、適正な用途に限りタイムスタンプトークンを複製・配布することは自由であることを表明すると良い。

（2）禁止される用途

備考：禁止される用途は個々の TSA のサービスに依存するため、本書では規定しない。

1.3.4 時刻監査証明書の適用範囲

（1）適正な用途

タイムスタンプ局は、タイムスタンプトークンを作成したタイムスタンプサーバの時刻ソースやタイムスタンプサーバが時刻監査を受けた日時及びそのときの時刻誤差を表す目的で、時刻監査証明書をタイムスタンプトークンに包含して加入者に発行する。加入者なら

びに依存者は時刻監査証明書を確認することで、対応するタイムスタンプトークンの時刻の正当性を確認することができる。

（2）禁止される用途

前記の目的以外で時刻監査証明書を使用してはならない。

1.4　本規程に関する問い合わせ先

本規程に関する問い合わせは下記の窓口にて受け付ける。

窓口	○○○○○株式会社
	○○○○部
	○○○○課
所在地	郵便番号○○○－○○○○
	○○県○○市○○丁○○番
電話	○○○－○○○－○○○○
ＦＡＸ	○○○－○○○－○○○○
電子メール	○○○○@○○○○.co.jp

2．一般規定

2.1 義務

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以下の業務を遂行する義務を負う。

（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の発行時刻が1.3.2項のｂ）に規定する誤差を越えないように、使用するタイムスタンプサーバの時刻管理を行う。

（3）セキュリティ管理

タイムスタンプ局は、本規程に基づき外部及び内部よりの脅威から、タイムスタンプサーバの時刻や秘密鍵、その他の機器およびシステムやデータの安全性を確保する。

（4）鍵の管理

タイムスタンプ局は、本規程に基づき本サービスに必要な秘密鍵を安全に管理する。

（5）失効申請と届出

タイムスタンプサーバの秘密鍵が危殆化した場合、タイムスタンプ局は速やかに鍵の失効をCAに申請する。

2.1.2 加入者及び加入申込者の義務

加入者及び加入申込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）時刻監査証明書等の利用制限の遵守

時刻監査証明書等はその目的、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時刻監査証明書等を利用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。

（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使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デジタル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、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。
（3）時刻監査証明書等の利用制限の遵守
時刻監査証明書等はその目的、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時刻監査証明書等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、時刻配信局がタイムスタンプ局に対して行う時刻配信サービスにおいて次の義務を負う。
（1）時刻配信局は、タイムスタンプ局のタイムスタンプサーバに対して時刻の配信およ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サーバに対する時刻監査の結果、時刻誤差の測定値が±○○○msec以内の場合は、当該タイムスタンプサーバに対して○○時間有効の時刻監査証明書を発行し、時刻鑑査証明書の有効期間内はタイムスタンプサーバがタイムスタンプを実施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±○○○msecを超えている場合は、タイムスタンプサーバのタイムスタンプ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を適正に維持するとともに、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、速やかにCA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する時刻監査と時刻監査証明書の発行等に関する監査ログ及びアーカイブデータを所定の期間安全に保管する。

2.1.5 CA の義務

（省略）

2.1.6 リポジトリに関する義務

タイムスタンプ局はタイムスタンプ業務に関する情報のうち公開する情報を、2.6 項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 タイムスタンプ局の責任

タイムスタンプ局は本サービスを提供するにあたり、加入者に対して 2.3 項に規定する財務上の責任を負う。

2.2.2 加入者の責任

加入者は、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デジタルデータとそのデジタル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すべての責任を負う。

2.3 財務上の責任

2.3.1 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、タイムスタンプ局が賠償する損害の範囲は予見可能な相当因果関係のある損害のみとし、逸失利益、データの消失、暖簾、偶発的損害、間接損害、特別損害、派生的損害、懲罰的賠償金等は賠償する損害の範囲には含まれない。

なお、タイムスタンプ局は、加入者以外にはいかなる場合であっても損害賠償責任を負わない。

2.3.2 免責事項

2.3.1 項の規定にかかわらず、下記の場合においては、タイムスタンプ局は加入者に対して賠償義務を負わない。

（省略）

備考：TSA の支配を超えた原因でサービスが停止する等の理由で損害賠償を要求される可能性がある場合は、本項で明示することを推奨する。

2.4 解釈及び執行

2.4.1 準拠法

当事者間の契約または他の準拠法を選択する旨の規定にかかわらず、本規程の解釈及び有効性等は、日本国内法及び規制に基づき解釈する。

2.4.2 可分性、効力の存続、承継、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 2.3、2.4、2.8、2.9 及び 2.10 の効力は有効に存続する。

（3）承継

明示的または黙示的に選任されたか、表見的なものかを問わず、本規程は、各当事者の承継人、遺言執行者、法定相続人、代表者、遺産管理人及び譲受人の利益のために効力を有し、かつ、これらの者を拘束する。

（4）通知

本規程に関するあらゆる通知、要求または要請は、書面または電子メールによって、1.4 項に記載される宛先に行う。書面による通知は受領日をもって有効とする。ただし、当該通知にその後の日付が記載されている場合は、記載日をもって有効とする。

タイムスタンプ局から加入者への通知先は、サービス加入申込書に記載された連絡先とする。

2.4.3 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、○○地方裁判所を第一審の専属的合意管轄裁判所とする。

2.5 料金

別途、本サービスの料金表に規定する。

2.6 公開とリポジトリ

2.6.1 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、タイムスタンプ局リポジトリに次の情報を公開する。

・タイムスタンプ局運用規程（本規程）

2.6.2 公開の頻度

公開する情報の更新頻度は次のとおりとする。

・タイムスタンプ局運用規程の変更の都度

・その他タイムスタンプ局の責任者が必要と判断した時

2.6.3 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。

2.6.4 リポジトリ

「2.6.1 タイムスタンプ局に関する情報の公開」において定める情報をリポジトリに公開する。

URL:http://www.○○○○.co.jp/

2.7 準拠性監査

2.7.1 監査頻度

タイムスタンプ局組織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。

2.7.2 監査人の身元・資格

タイムスタンプ局の監査人には、○○○○○株式会社及び関連会社の従業員の中から、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。

2.7.3 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は、タイムスタンプ局と直接利害関係を有しない者を選定する。

2.7.4 監査テーマ

本サービスがタイムスタンプ局運用規程及び運用マニュアル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。

2.7.5 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、タイムスタンプ局のタイムスタンプサーバ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。

2.7.6 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。

監査報告書は、○年間保管する。

2.8 機密保持

2.8.1 機密扱いとする情報

タイムスタンプ局および加入者は、漏えいすることによってタイムスタンプ局、加入者、時刻配信局、または CA の認証業務の信頼性が損なわれる恐れのある情報を機密扱いとする。機密扱いとする情報は、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。

2.8.2 機密扱いとしない情報

2.8.1 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) CA・時刻配信局または加入者からタイムスタンプ局に開示された時点で既に公知の情報
(3) CA・時刻配信局または加入者からタイムスタンプ局に開示された後、タイムスタンプ局の責によらずして公知となった情報
(4) CA・時刻配信局または加入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) CA・時刻配信局または加入者が第三者に対して、秘密保持義務を課すことなく開示した情報

2.8.3 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 CA において CRL として公開される。

個別のタイムスタンプトークン及び時刻監査証明書の信頼性低下に関する情報については、タイムスタンプ局のリポジトリ上に公開を行う。

2.8.4 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。

2.8.5 民事手続上の情報開示

タイムスタンプ局は、訴訟、仲裁、調停、その他の法的、裁判上または行政手続きの過程において、タイムスタンプ局で取扱う情報（機密情報を含む）を開示することができる。ただし、当該情報が機密情報である場合には、その旨を明示したうえで開示する。

2.8.6 情報の主体者の要求に基づく情報開示

CA・時刻配信局または加入者がタイムスタンプ局に開示した情報について、当該 CA・時刻配信局または加入者から開示要求があった場合、タイムスタンプ局は、当該開示要求者が当該情報を開示した本人であることを確認したうえで、当該開示要求者に対して当該情報を開示する。

2.8.7 その他の理由に基づく情報開示

規定しない。

2.9 知的財産権

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、商標権、意匠権（これらの登録を受ける権利を含む）および著作権はタイムスタンプ局に帰属し、また以下の各号に定めるものはタイムスタンプ局に帰属し、加入者その他の者には移転しないものとする。

(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) タイムスタンプトークン検証ソフト
(3) 本規程

なお、以下の各号に定めるもの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。

(4) タイムスタンプトークンに添付された時刻監査証明書
(5) 時刻監査証明書検証ソフト

備考：適正な用途を規定し、その場合に限りタイムスタンプトークンを複製・配布することは自由であることを表明すると良い。

2.10 個人情報の取扱い

タイムスタンプ局は、本サービスの申込時に加入者から提供される個人情報を、本サービスを提供するために必要な範囲をこえて使用しない。また、その保護について、以下に従うものとし、以下の内容について本サービスに係わる全ての就業者の役割に応じて理解されるようにする。

（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、勤務先その他の記述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のみ使用する。

（3）利用目的による制限
タイムスタンプ局は、上記 2.10(2)に規定される目的以外に個人情報を利用せず、かつ不正な手段によっては個人情報を取得しない。

(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、個人情報を正確かつ最新の状態で管理する。

(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または利用もしくは提供を拒まれた場合には、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、CA 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 名前の意味に関する要件

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サーバの固有名称は、CA 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

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サーバの固有名称は、CA により一意に割り当てられるものとする。

3.1.4 組織の認証

（省略）

3.1.5 個人の認証

（省略）

4．運用要件

4.1 サービスの利用申請

本サービスの利用を申請する者は、当社営業担当にサービス加入申込書を請求し、そのサービス加入申込書に必要事項を記入・捺印して当社営業担当宛に送付を行う。

タイムスタンプ局は、サービス加入申込書の審査を行い、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、加入申込者の本サービスへの加入を認め、本サービスの提供を行う。

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デジタルデータのハッシュ値を含むタイムスタンプ要求を、本タイムスタンプ局へ送付する。本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。

4.3 タイムスタンプトークンの発行

本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、本タイムスタンプ局の管理する任意のタイムスタンプサーバを用い、1.3.2 項「タイムスタンプサービスの内容」に規定されるタイムスタンプトークン（TST）の作成をおこない、それを加入者に対して発行する。本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については別途規定する。

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。

備考：検証方法として、検証用ソフトウェアを配布する方法や、TSA 局がオンラインで検証結果を返す等がある。検証方法は個々のサービスによって異なるので、本書では内容を省略する。

4.5 サービスの一時停止と解約

4.5.1 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。

（省略）

備考：TSA の支配を超えた原因等でサービスが停止する可能性がある場合は、本項で明示することを推奨する。

4.5.2 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 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を行う。

（省略）

4.6 セキュリティ監査の手順

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 監査ログに記録する情報

監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発効・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記録
（8）帳簿書類へのアクセス及び帳簿書類の廃棄についての記録

4.6.2 監査ログの検査頻度

監査ログの検査は、月次を最低頻度としてこれを行う。

4.6.3 監査ログの保存期間

前記の 4.5.1 項（記録する情報の種類）における（1）～（4）の監査ログは○年間保管する。
その他の記録については○年間保存する。

4.6.4 監査ログの保護

監査ログは、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。

4.6.5 監査ログのバックアップ手順

監査ログは、所定の方法・手順によりバックアップを行う。

4.6.6 監査ログの収集システム

タイムスタンプ局では、監査ログの収集機能はタイムスタンプ局システムの一機能とし、セキュリティに関する重要な事象をシステムの起動時から監査ログとして自動的に収集する。

4.6.7 監査ログ検査の通知

監査ログの検査は、事象を発生させた者に通知することなく行う。

4.6.8 脆弱性の評価

監査ログを検査することにより、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される。タイムスタンプ局の責任者は所定の手順に従って問題点を是正する。

4.7 アーカイブ

4.7.1 アーカイブデータの種類

アーカイブデータは、次のものとする。

（1）紙で保存するもの。
- 加入者からの加入申込書、変更・解約届け及び申込書・各種届けの添付書類

（2）デジタルデータで保存するもの
- 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）
- 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）

4.7.2 アーカイブデータの保管期間

アーカイブデータは、○年間保管する。

4.7.3 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。

4.7.4 アーカイブデータのバックアップ手順

所定の方法・手順によりアーカイブデータのバックアップを行う。

4.7.5 レコードのタイムスタンプに関する要件

レコードにタイムスタンプを付与するコンピュータのシステム時計は、定期的に UTC に対して時刻同期が行われる。

4.7.6 アーカイブデータの収集システム

アーカイブデータは、定められた手順で収集する。

4.7.7 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である事が保証された形式で保管する。

4.8 鍵更新

タイムスタンプサーバの公開鍵証明書の有効期間が満了する○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廃棄処理を実施するが、公開鍵証明書の失効処理は行わない。

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

タイムスタンプ局のタイムスタンプサーバの秘密鍵が危殆化した場合は、その鍵の公開鍵証明書が CA によって失効される（CA 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。

4.9.3 秘密鍵が危殆化した場合の対処

タイムスタンプサーバ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。

・タイムスタンプサーバの公開鍵の失効申請手続
・タイムスタンプサーバの秘密鍵の廃棄及び再生成手続
・タイムスタンプサーバの新しい鍵に対する公開鍵証明書の発行申請手続

4.9.4 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運用を行う。

4.10 タイムスタンプ業務の終了

（1）タイムスタンプ局は以下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情報の漏洩、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）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、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本サービス終了○○日前までに加入者及び依存者に公知または通知する。

（3）本サービス終了後、直ちに全てのタイムスタンプサーバの秘密鍵を確実に廃棄する。

4.11 タイムスタンプ業務の一時中断

タイムスタンプ局は、システムの点検等のために本サービスを一時中断することができる。この場合は、一週間前までに加入者に対して所定の方法で連絡するとともに、下記 URL に公開して通知を行う。

URL:http://www.○○○○.co.jp/

備考：うるう秒の挿入がある場合、TAS のサービスの内容によっては、うるう秒挿入の前後に一時的にサービスを中断した方が良い場合が考えられる。その場合は、本項に明記することを推奨する。

4.12 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「時刻配信サービス」を使用して全てのタイムスタンプサーバ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「時刻配信サービス」を使用して全てのタイムスタンプサーバのうるう秒設定を行う。

備考：時刻配信サービスを使用しない場合は、時刻同期の具体的管理方法・管理体制等について記載する。

4.13 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、タイムスタンプサーバ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保持する。

（2）時刻配信局は UTC を提供する１つ以上の国家時刻機関を直接もしくは間接的に経由して、UTC に対する時刻配信局の時刻のトレーサビリティを保持する。

備考：時刻配信サービスを使用しない場合は、時刻のトレーサビリティについての具体的立証方法・管理体制等について記載する。

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　物理的アクセス

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 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。

5.3 人事面の管理

5.3.1 経歴、資格、経験及び必要条件

本サービスに従事する者について、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 経歴調査手順

本サービス及び顧客情報管理業務に従事する予定の者全員について、それらの者の信頼性と適格性を見極めるために合理的な範囲で、当該業務に従事させる前に調査を行う。

5.3.3 トレーニング要件

本タイムスタンプ局の運用に関わる要員に対して､別途教育計画を定めトレーニングを実施する。

5.3.4 追加トレーニングの頻度及び要件

本タイムスタンプ局の運用に関わる要員に対しては、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。

5.3.5 ジョブローテーション及びその実施

本タイムスタンプ局では、必要に応じて勤務のローテーションを行う。

5.3.6 権限のない行為に対する制裁

本サービスに従事する者が、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契約等に基づき懲戒を行う。

5.3.7 担当者に提供される文書

本タイムスタンプ局の運用に関わる要員に対して、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。

・タイムスタンプ局の設備や機器のマニュアル類
・タイムスタンプ局の運用に関する規定・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

タイムスタンプサーバの鍵ペアは、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　タイムスタンプサーバの公開鍵の CA への登録

タイムスタンプサーバの公開鍵は所定の手続きにより CA に登録し、証明書の交付を受ける。

6.1.3　CA のルート証明書の受領

タイムスタンプ局は、CA のルート証明書を安全かつ確実に受領し保管する。

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、時刻配信局の公開鍵を証明する CA のルート証明書を安全かつ確実に受領し保管する。

6.1.5　鍵のサイズ

・タイムスタンプサーバの鍵には RSA 1024 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

「6.1.1 鍵ペア生成」において定める。

6.1.7　鍵の利用目的

タイムスタンプサーバの鍵は、以下の目的に使用する。

・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デジタル署名

6.2　秘密鍵の保護

6.2.1　暗号モジュールに関する基準

タイムスタンプサーバの鍵は、FIPS（米国連邦情報処理標準）140-1 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

タイムスタンプサーバの秘密鍵の生成、アクティベート、廃棄等は、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

タイムスタンプサーバの秘密鍵は、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

タイムスタンプサーバの秘密鍵は、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

タイムスタンプサーバの秘密鍵は、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サーバの秘密鍵の破棄は、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

タイムスタンプサーバ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○年とする。

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

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、またはその可能性がある場合は鍵更新を行う。

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

タイムスタンプサーバ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

タイムスタンプサーバ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管理

6.5.1 コンピュータセキュリティ機能要件

タイムスタンプ局では、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う。

6.5.2 コンピュータセキュリティ評価

タイムスタンプ局では、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する。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。

6.6 システムのライフサイクルにおけるセキュリティ管理

6.6.1 システム開発面における管理

タイムスタンプ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する。

6.6.2 システム運用面における管理

タイムスタンプ局では、セキュリティに関する基準を設け、コンピュータ装置やタイムスタンプサーバ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う。

6.6.3 ライフサイクルセキュリティ評価

タイムスタンプ局では、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する。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。

6.7 ネットワークセキュリティ管理

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。

6.8 暗号モジュールの技術管理

「6.1.1 鍵ペア生成」及び「6.2.1 暗号モジュールに関する基準」において定める。

7．タイムスタンプトークンのプロファイル

(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 :x.xxxx.xxx.xxx.x.x
messageImprint	
MessageImprint hashAlgorithm AlgorithmIdentifier algorithm parameters hashedMessage	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 ハッシュアルゴリズム ハッシュアルゴリズムのオブジェクトID 型 :OID 値 :1 3 14 3 2 26 (SHA1) ハッシュアルゴリズムの引数 型 :NULL 値 :なし 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[.sss]Z
accuracy	
Accuracy seconds	タイムスタンプ時刻の精度 時刻精度（秒） 型 :INTEGER 値：○○

millis	時刻精度（ミリ秒） 型：INTEGER 値：○○
micros	時刻精度（マイクロ秒） 型：INTEGER 値：○○
ordering	
ordering	時刻精度以上における順序性 型：BOOLEAN 値：FALSE
nonce	
nonce	ノンス 型：INTEGER 値：乱数
tsa	
GeneralName	TSAの識別情報
directoryName	
countryName	TSAの国名
type	国名のオブジェクトID 型：OID 値：2 5 4 6
value	国名の値 型：PrintableString 値：JP
organizationName	TSAの組織名
type	組織名のオブジェクトID 型：OID 値：2 5 4 10
value	組織名の値 型：PrintableString 値：○○○○○○
organizationalUnitName	TSAの部門名
type	部門名のオブジェクトID 型：OID 値：2 5 4 11

value	部門名の値 型 :PrintableString 値 :○○○○○○
commonName	TSA・TSSの固有名称
type	固有名称のオブジェクトID 型 :OID 値 :2 5 4 3
value	固有名称の値 型 :PrintableString 値 :○○○○○○
Extensions	
extensions	拡張領域 使用しない

備考：本書では TSTInfo のみ掲載し、タイムスタンプトークン全体の構成及びプロファイルは省略する。

8．タイムスタンプ局運用規程の管理

8.1　タイムスタンプ局運用規程の変更

タイムスタンプ局は所定の手続きに基づき、本運用規程を必要に応じて変更する。

8.2　タイムスタンプ局運用規程 の公開と通知

タイムスタンプ局は、本運用規程を変更した場合、速やかに変更した本運用規程を公開する。

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にて連絡を行う。依存者に対しては、本運用規程をリポジトリに公開することをもって通知とする。

8.3　タイムスタンプ局運用規程 の承認手続き

本運用規程の設定・変更は、タイムスタンプ局代表者によって承認される。

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
TSA	Time－stamping authority タイムスタンプ局
TSS	Time－stamp server タイムスタンプサーバ
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	時刻配信局（TA）が顧客の装置（タイムスタンプサーバ等）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。TSA に対して標準時刻の配信と、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。
タイムスタンプサーバ(TSS)	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、TSA によってデジタル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）	独立行政法人通信総合研究所（CRL）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	証明書に関する情報を保管したり配布したりするオンライン・データベース

参考文献

・ISO/IEC 18014-1:2002 Information technology-Security techniques-Time-stamping services-Part1:Framework
・RFC 3161(2001) Internet X.509:Public Key Infrastructure: Time-Stamp Protocol(TSP)
・ETSI TS 102 023 V1.1.1(2002-04) Policy requirements for time-stamping authorities
・FIPS PUB 140-1, Security Requirements for Cryptographic Modules, US Department of Commerce National Institute of Standards and Technology, January1994
・RFC 1305: Network Time Protocol (Version 3), March 1992
・Internet Attribute Certificate Profile for Authorization, draft-ietf-pkix-ac509prof-09.txt, 8th June 2001
・ISO/IEC 9594-8 | X.509: ITU-T Recommendation X.509 (1997), Information Technology -- Open Systems Interconnections -- The Directory: Authentication Framework. General Procedures 1997
・RFC 2527 Certificate Policy and Certification Practices Statement Framework
・経済産業省認証局運用管理規程（CP/CPS）（平成 13 年 5 月 29 日経済産業省）
・認証局運用ガイドライン（V1.0 版）-電子商取引実証推進協議会（ECOM）認証局検討ワーキンググループ 1998

リンキングプロトコルを用いた
タイムスタンプサービス運用規程 例）

目　次

1．総則

1.1　趣旨説明

1.1.1　本規程の概要

「○○サービス」は、特定の時間に特定の電子文書が存在し、それが改ざんされていないことを保証するサービス（以下、タイムスタンプサービス）を提供する。

本規程は、タイムスタンプサービスを提供するにあたり、タイムスタンプ局（以下、TSA）がタイムスタンプ業務遂行に必要な遵守事項、情報資産管理の方針を定めたものである。

1.1.2　本規程の範囲

本規程は、TSA 及び TSA により保証された電子文書に関わるすべての人、組織、情報、業務に適用される。

以下に具体的な適用範囲を例示する。

【人】

社員、協働者（派遣社員、SE・プログラマー、契約等に基づく TSA の支援者等）、販売代理店、加入者、依存者等

【組織】

TSA 運営／運用組織、担当、グループ等

【情報】

TSA に関わる印刷情報、電子情報（ハードディスク・FD 等、各種媒体に保存される情報、及び情報システム上の情報）、その他の情報（音声・知識情報等、媒体に保存されない情報等）等

【情報システム】

TSA にて提供されるシステム

【業務】

TSA に関わる設計、構築、試験、運用等の各フェーズにおけるすべての業務

業務遂行において、以下の条件・状況の下では、例外的に本規定が適用されない場合がある。こうした場合も、TSA の責任者に必ず報告し、逸脱の承認を得た上で運用しなければならない。ただし、人命に関わる緊急・災害時においてはこの限りではない。

1.2　本規程の位置づけ

著しく変化するセキュリティ技術・環境等に対応するため、本規程は TSA における情報セキュリティ確立のための方針とし、特定の人、組織、業務、技術及び情報システムに依存せず、頻繁な更新を必要としない基本的な考え方や方向を定めたものである。

本規程は TSA 運営委員会によって制定され、TSA に携わる社員、協働者はこれに従い、情報セキュリティを確保した上で、情報資産を創造的かつ効率的に活用しなければならない。

技術や状況の変化等に依存的で、頻繁な更新を必要とする詳細な手順や実施方法は、本規程の下部規則として、マニュアル等を別途定めることとする。

1.3　用語定義

本規程内で用いる用語の意味を明確にし、共通の解釈になるように用語の定義を行う。

【本規定に関する定義】

TSA

リンキングプロトコルを用いてタイムスタンプサービスを提供し、第三者機関としてタイムスタンプ記録を発行、検証するサービスプロバイダ

その運営機関も含む

タイムスタンプ記録

TSA が発行し、存在時刻と原本性を証明するデータ

登録

サービスの加入者がタイムスタンプ記録の発行を TSA へ依頼する行為

検証

サービスの加入者がタイムスタンプ記録を使用し存在時刻と原本性の検証を TSA へ依頼する行為

TSA 運営委員会

TSA に関わる社員、協働者から構成される。

TSA 責任者

TSA に関するすべての責任を有する者

TSA 管理者

TSA 責任者の指示のもと、本規定を運営及び推進していく者

監査者

TSA に関わる人、組織、情報、業務が本規定に準拠しているか監査を行う個人又は組織

データセンタ

TSA のシステムを収容した建物

完全性

電子文書の消失及び変化がなく、改ざんもされていない状態

機密性

アクセスを許されない者からの電子文書へのアクセスを防止され、電子文書の盗難、漏えい、

盗み見等がされていない状態

見読性

電子文書の内容が必要に応じ電子計算機その他の機器を用いて直ちに表示できること

原本性

電子文書の完全性、機密性、見読性が確保された状態

RHV

TSA がある時刻に受け付けたハッシュ値を二分木構造に組み上げ生成するハッシュ値

SHV

TSA が秒単位で生成するハッシュ値で、ある時刻(T)に生成された RHV とその時刻の一つ前(T-1)に生成された SHV から生成される

PHV

TSA が秒単位で生成する SHV を日単位、週単位…と定期的に集約し公開するハッシュ値

【人・組織に関する定義】

運営機関

TSA を保有、運営する組織

社員等

運営機関の社員、嘱託者

本規定では、以下は単に「社員」と表する

協働者

協働者とは、運営機関と雇用関係を持たない者のうち、契約等によって定められた範囲内で運営機関の業務を支援する者

すなわち、派遣社員、SE・プログラマー、警備員、清掃業者等

第三者

上記の運営機関、社員、協働者以外の個人、組織

運営機関との雇用関係を持つが運営機関の担当組織に所属しない者を含む

販売代理店

TSA との契約により、TSA のサービスを利用し、タイムスタンプサービスを二次的に提供する者その運営機関を含む

加入者

TSA または販売代理店と契約し、タイムスタンプサービスを利用する者

依存者

タイムスタンプ記録の検証を TSA または販売代理店へ依頼する者

利用者

加入者、依存者の総称

【情報に関する定義】

情報資産

TSA 業務に利用されるすべての情報及び情報システム等

個人情報

「個人に関する情報」であり、社員、協働者ならびに顧客の情報

個人の氏名が示されていなくとも他の情報と組み合わせて一意に個人を識別し得る情報も個人情報として取り扱う

情報所有者

情報の取得又は生成に係る当事者のうち、情報の内容に関して責任を有する個人又は組織

情報管理者

情報所有者により指名され、情報所有者と情報利用者に対して情報管理業務を実施する個人又は組織

情報利用者

情報を利用して業務を遂行する社員、協働者

情報のライフサイクル

情報の取得・生成、流通、保管、利用、廃棄等の一連のサイクル

可搬媒体

情報を格納している媒体のうち、持ち運びが可能なもの

【情報セキュリティに関する定義】

情報セキュリティ

業務遂行の基盤となる情報資産が、災害もしくは故障等により被害を受けたり、不正行為等に利用されることが防止されたりしている状態

セキュリティ対策

情報セキュリティを保つための技術もしくは運用による実現手段

情報セキュリティ侵害等

本規定では、情報セキュリティを侵害する行為ならびに機密情報の漏洩等を総称する

アクセス

情報又は情報システムを利用できる状態にすること

不正アクセス

不正な手段により、正当な利用者以外が行うアクセス、あるいは正当な利用者の過失等による権限外のアクセス

アクセス制御

個人が情報資産を利用できる範囲を、アクセス権限に基づき制限すること

暗号化

データを容易に解読されないように変換すること

可用性

情報又は情報システムが適時に利用可能な状態に保たれている特性

追跡性

情報または情報システムの利用者等を特定または、追跡することができる特性

識別・認証

ID（識別子）等により個人を認識し、パスワード等を利用することで本人であることを検証すること

なりすまし

他人であるように偽る不正行為

改ざん

情報所有者の許可なく情報の内容を変更する不正行為

不正プログラム

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラム

コンピュータウィルス

不正プログラムの中で、自己伝染機能、潜伏機能、発病機能のうち１つ以上を有し、コンピュータシステムやソフトウェア、フロッピーディスク等に侵入し、増殖し、データ等を破壊するプログラム

本規定において、以下は単に「ウィルス」と表する

ウイルスチェックソフトウェア

ウィルスの検出、予防又は修復のいずれかの機能を含むソフトウェア

【情報システムに関する定義】

情報システム

TSA で構築されるコンピュータシステム及びネットワークの総称

ネットワーク

「ネットワークサービス」と「ハード」の総称

ネットワークサービスとは、通信を成立させるために提供されるサービス群、ハードとは、ネットワークを物理的に構成する装置類

内部ネットワーク

外部ネットワークとの接続点を含み、運営機関が保有し運用管理するネットワーク

外部ネットワーク

運営機関以外により運用管理されているネットワーク

情報システム管理者

TSA 責任者から任命され、情報システムの構築、運用管理業務を遂行する個人又は組織

不正プログラム管理者

TSA 責任者から任命され、ウィルス等不正プログラムの予防、発見、駆除、復旧業務を支援・管理する者

バックアップ

情報が破壊あるいは改ざんされるなどし、使用不可能な状態になった際に、復元できるように

適切な媒体に保存すること

ログ

情報システムにおける利用状況（ログイン、ファイルアクセス等）を個人が識別できるよう記録したもの

外部接続

内部ネットワークを外部ネットワークと接続すること

1.4 公表

本運用規程は、以下の方法で公表されています。

(i)　Web サイト（http://www.○○.co.jp/）

(ii)　電子メール（△△@○○.co.jp）で電子データの請求

(iii)　印刷物の請求

宛先：　東京都～

○○株式会社△△担当

ＴＥＬ：**-****-****　ＦＡＸ：**-****-****

2．一般的概念

2.1　タイムスタンプサービス

本規程ではタイムスタンプサービスの提供を以下のコンポーネントに細分化する。

- タイムスタンプ記録発行：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データに対しタイムスタンプ記録を生成し、それを加入者に対して発行する。
- 文書検証：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データとタイムスタンプ記録に対し、原本性の検証を行い、それを加入者に対し通知する。
- PHV の公開：タイムスタンプ局は運営機関の正当性を示すために PHV を定期的に公開する。

タイムスタンプサービスに使用されるハッシュ値生成アルゴリズムは、国家的セキュリティ評価機関によって認定されるか、TSA 発行のタイムスタンプ記録の目的に適したアルゴリズムでなければならない。

2.2　タイムスタンプ局

タイムスタンプサービスの利用者によって信頼され、信頼できる時刻ソースを用い文書の登録・検証を行う機関を TSA と呼ぶ。TSA はタイムスタンプサービスの提供において全般的責任を負う。

TSA は加入者にタイムスタンプ記録を発行するサービスプロバイダである。

TSA は加入者または依存者からタイムスタンプ記録の検証を受付けるサービスプロバイダである。

TSA は販売代理店にタイムスタンプサービスの一部を提供可能とする。

2.3　販売代理店

運営機関によりサービスを販売する権利を与えられた組織。加入者を対象に販売、サービスの提供を可能とする。

2.4　加入者

運営機関または販売代理店よりサービスを受け社内の業務目的のみに使用するユーザを意味する。

2.5　依存者

加入者から取得したタイムスタンプ記録の検証を、運営機関または販売代理店へ依頼するユーザを意味する。

2.6　タイムスタンプ・ポリシー

2.6.1　目的

本規程では、タイムスタンプ・ポリシーが信頼あるタイムスタンプサービスの一般的要件を満

足するように定められている。TSA はこれらの要件がどのように満足されるかを実施規定により定める。

2.6.2 概要

タイムスタンプ・ポリシーは、「共通のセキュリティ要件のもとで、特定のコミュニティまたはアプリケーションに対するタイムスタンプ記録の適用可能性を示す規則の集まり」である。本規定は、タイムスタンプ記録を○秒またはそれ以上の精度で発行する TSA を対象として、ベースライン・タイムスタンプ・ポリシーの要件を定める。

TSA は、本規定に定めたポリシーを拡張する独自のポリシーを定めることができる。こうしたポリシーは、本規定に定めた要件を組み込むか、またはさらに制限される。

JST（日本標準時）または UTC（協定世界時）の時刻値に対して、±○秒以上の精度が TSA によって実現されている場合、その精度が TSA の開示規定に示す。

2.6.3 識別

TSA は、対応しているタイムスタンプ・ポリシーの識別子を TSA 開示規定に示し、利用者に明らかにすることにより、ポリシーを順守していることを示す。

本運用規程のタイムスタンプ・ポリシーのオブジェクト識別子は以下のとおり。

iso（○），加盟機関（○），jisc（○○○），組織登録番号（○○○○），****ポリシー（○）

2.6.4 利用者コミュニティと適用性

本ポリシーは、公的なタイムスタンプサービスまたは閉じたコミュニティ内で利用されるタイムスタンプサービスに適用する。

2.6.5 順守性

TSA は、タイムスタンプ記録内にタイムスタンプ･ポリシーの識別子を使用する。以下の場合には、TSA は本規定に定められたタイムスタンプ・ポリシーを組み込むか、あるいはさらに制限する独自のタイムスタンプ・ポリシーを定める。

a) TSA が定められたタイムスタンプ・ポリシーの順守を主張し、その順守の主張を証明する証拠を加入者や依存者に要求に応じて提供できる場合
b) 独立機関によって TSA が定められたタイムスタンプ・ポリシーを順守していると評価された場合

仕様を順守する TSA は以下を示す。

c) 3.1.1 に定める義務を果たしていること
d) 4 に定める規制を実施してきたこと

3．義務と責任

3.1 義務

3.1.1 TSA の義務

1. TSA は本規程に従いサービスの提供を行うものとする。
2. TSA は信頼性のあるシステムのみを用いて、サービスを提供する。
3. TSA は本規程に従いタイムスタンプ記録を生成し、加入者に対し発行する。
4. TSA は本規程に従い加入者がいつでも原本性の検証を行うことができるようにサービスを提供する。
5. TSA は本規程に従い、PHV を公表する。
6. 販売代理店からの販売契約書を受け付け、契約書の審査および適宜必要な追加調査を終えた後、当該申請者がサービスを提供できるか否か決定する。
7. 加入者からのサービス利用申し込み契約書を受け付け、契約書の審査および適宜必要な追加調査を終えた後、当該申請者がサービスを利用できるか否か決定する。
8. TSA はタイムスタンプ記録の目的に合致した最新のハッシュ値生成アルゴリズムを用いてタイムスタンプサービスを提供しなければならない。

3.1.2 販売代理店の義務

1. 販売代理店は本規程に従って、TSA を利用したサービスを提供する。
2. 販売代理店は信頼性のあるシステムのみを用いて、サービスを提供する。
3. 統一した信頼性の水準を達成するため、本規程が要求するさまざまな制約に服することに合意しなければならない。
4. 販売代理店となることを希望するサービス提供機関は、販売契約書に要求された追加情報も含めて漏れなく記入し、TSA 運営機関に提出しなければならない。

3.1.3 加入者の義務

1. 加入者は本規程に記載の事項、または本規程を含む販売代理店が制定する規定に了承した上でサービスの提供を受けるものとする。
2. 加入者はサービス申し込みにあたり、TSA 及び販売代理店の契約書に要求された追加情報も含めて漏れなく記入し、利用する TSA 運営機関または販売代理店運営機関に提出しなければならない。

3.2 責任

3.2.1 TSA の責任

1. 運営を維持し、かつその義務を履行するために十分な財政的基盤を有していなければならない。
2. 加入者より PHV の検証依頼があった場合は速やかに対応しなければならない。

3.2.2 販売代理店の責任

運営を維持し､かつその義務を履行するために十分な財政的基盤を有していなければならない。

3.2.3 加入者の責任

加入者は、その者が TSA に登録した電子データを、タイムスタンプ記録によって検証した第三者（依存者）に対し、虚偽の事実を表明したことから発生する全ての責任を負わなければならない。この規定は、本規程が規定する加入者の他の義務を制限するものではない。

3.2.4 依存者の責任

依存者は、その者が TSA に依頼したタイムスタンプ記録の検証結果について、虚偽の事実を表明したことから発生する全ての責任を負わなければならない。この規定は、本規程が規定する依存者の他の義務を制限するものではない。

3.2.5 賠償責任

（1）本規程「3.2.1 TSA の責任」に定める責任に違反して損害賠償責任を負う場合は、別途､「○○サービス」利用規約（以下「利用規約」とする）で定める金額を上限とする。いかなる場合においてもこの賠償額の上限を超える請求には応じない。ただし、TSA の責任に帰することができない事由から生じた損害、TSA の予見の有無を問わず特別の事情から生じた損害については賠償責任を負わない。

（2）利用者が､本規程に定める義務を履行しない又は本規程の｢3.2.3 加入者の責任､｢3.2.4 依存者の責任」に定める責任に違反したことにより、TSA が損害を被った場合、TSA は利用者に対し、当該損害の賠償を請求することができる。

（3）利用者が、タイムスタンプ記録を使用するにあたっての利用者自身のシステムに起因するあらゆる損失、損害又は費用について、TSA は免責される。

（4）利用者が提示されたタイムスタンプ記録の有効性の確認を行わずにタイムスタンプ記録を使用した結果被った損害については、TSA は何ら賠償責任を負わない。

（５）TSA は、以下の事由によるサービス停止によって利用者が損害を受けた場合、一切賠償責任を負わない。

- 地震、水害、噴火、津波などの天災
- 火災、停電など
- 戦争、動乱、騒乱、暴動、労働争議など
- その他、TSA が技術的あるいは運用上緊急にサービスを停止する必要があると判断した場合

4．運用要件

4.1 実施規定

TSA は、タイムスタンプサービスの提供に必要な信頼性を示すことを保証する。

1. TSA は資産への脅威を評価し、必要なセキュリティ管理と運営手順を決定するため、リスク調査を実施する。
2. TSA は本タイムスタンプ・ポリシーに定められた全ての要件を満足するために使用される実施規定および手順を用意する。
3. TSA の実施規定は、該当するポリシーや実施を含め、TSA サービスを支援するあらゆる外部組織の義務を定める。
4. TSA は加入者がその実施規定、タイムスタンプ・ポリシーの順守評価に必要なその他の関連文書を入手できるようにする。
5. TSA はすべての加入者に対して、そのタイムスタンプサービスの使用に関する条件を開示する。
6. TSA は、TSA 実施規定を承認する決定権限を備えた高レベルの管理組織を有する。
7. TSA の上層部経営者は、実施が適切に行われていることを保証する。
8. TSA は、TSA 実施規定の管理責任を含めた実施の審査プロセスを定める。
9. TSA は、意図する実施規定の変更について適正な通知を行う。また管理組織の承認後入手できるようにする。

4.2 開示規定

TSA は全ての加入者に対して、タイムスタンプサービスの使用に関する条件を開示する。

1. TSA の契約情報
2. 適用されているタイムスタンプ・ポリシー
3. タイムスタンプが付与されるデータを表現するために使用されるハッシュアルゴリズム
4. タイムスタンプ記録内の時刻の精度
5. タイムスタンプサービスの使用に関するあらゆる制限事項
6. 加入者の義務
7. 賠償責任の制限
8. TSA が定められたタイムスタンプ・ポリシーを順守していると評価されているかどうか、および評価されている場合には独立した評価機関

4.3　TSA による SHV の管理

4.3.1　SHV の生成

TSA は 4．6 に示すセキュアな管理環境のもとで SHV（Super Hash Value：スーパーハッシュ値）が生成されることを保証する。

SHV とは、ある特定時刻（ｔ：○秒単位）に受け付けたハッシュ値をツリー構造に組み上げ、新たなハッシュ値（RHV:ルートハッシュ値）を 1 つ作成し、その直前の SHV（ｔ-1）から、新しい SHV（ｔ）を作成したものである。また、時間との関連づけを持たせたハッシュ値であり、検証のためのデータとして後に利用されるものである。

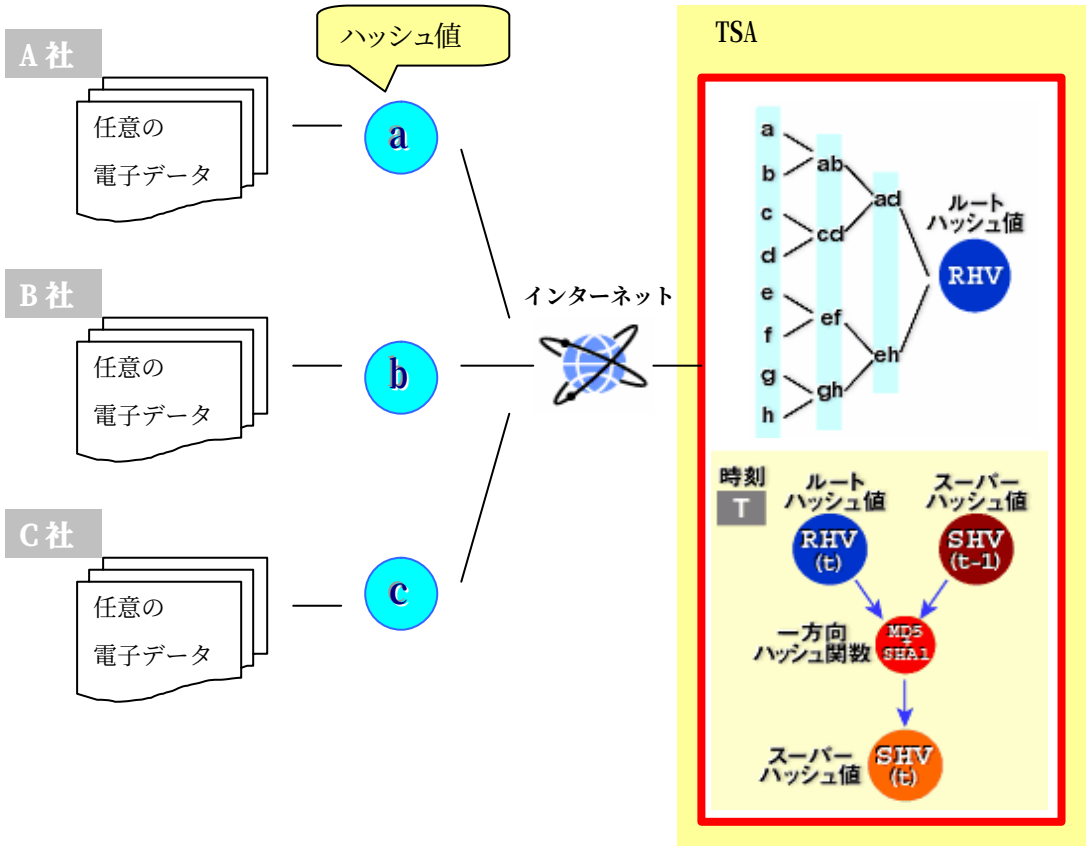

図 4-1　SHV 生成概念図

4.3.2　SHV 生成の開始

SHV の生成は、4.6 に示す物理的にセキュアな環境で TSA 管理者及び TSA 責任者により、二重管理のもとで開始する。また、セキュリティ基準が保証された信頼あるシステムで生成を行う。

4.3.3 SHV の保持

TSA は、サービス提供中は SHV を保持し、その完全性を維持することを保証する。
セキュリティ基準が保証された信頼あるシステムで保持する。
SHV へのアクセスは TSA 責任者、TSA 管理者の両者の合意のもとに行う。

4.3.4 PHV の公開

TSA は、運用機関の正当性を証明するために定期的に PHV（公開ハッシュ値）を公開しなければならない。本 TSA は、○○○○新聞社が発行する○○○○新聞の○○○日に掲載する。

取得要件

TSA 責任者、TSA 管理者の両者の合意の下に PHV の取得を行うこととする。

公開要件

公知の事実かつ改ざん不可能となるよう、新聞へ公開をする。
出版会社との原稿は、社外秘扱いとし、サービス提供中は保持する。

4.4 タイムスタンプ記録

TSA は、タイムスタンプ記録がセキュアに発行され、正しい時刻を含むことを保証する。

- 発行するタイムスタンプ記録には一意の識別子を付与する。
- TSA がタイムスタンプ記録において使用する時刻値は、JST（日本標準時）または UTC（協定世界時）の時刻値の少なくとも１つに基づく。
- タイムスタンプ記録に含まれる時刻は、このポリシーに定める精度内、または、タイムスタンプ記録そのものに精度が定められている場合にはその精度内で UTC と同期するものでなければならない。
- TSA の時計が定められた精度外にあると分かった場合、タイムスタンプ記録の発行を中止する。
- タイムスタンプ記録には、要求者の指示に従ってタイムスタンプを付与されたデータの表現（ハッシュ値など）を含む。
- タイムスタンプ記録には、検証に必要なデータ（SHV（t-1)、ルートハッシュ値を生成するのに必要な中間のハッシュ値）が含む。

4.5 時刻同期

TSA は、定められた範囲内で TSA 内の時計が JST（日本標準時）または UTC（協定世界時）と同期していることを保証する。

1. TSA の時計の補正を行い、時計が宣言された精度を維持するようにしなければならない。

2. TSA 時計は、その目盛りを超えるような気づかれない変化を時計にもたらす恐れがある脅威から保護されなければならない。
3. TSA は、タイムスタンプ記録に示される時刻がずれた場合、これが検出されることを保証しなければならない。
4. TSA はタイムスタン・ポリシーで定めた時刻精度と、うるう秒の補正を含む時刻の補正を保証できる時刻ソースを利用しなければならない。

4.6 TSA の管理および運営

4.6.1 セキュリティ管理

TSA 内における TSA 及び TSA に関わる人及び組織の情報は、機密性、完全性を明記し、適切に管理、運用する。情報の扱いについては、5.6 に示す。

4.6.2 物理的管理

4.6.2.1 ＜SHV を管理しているサーバについて＞

SHV を管理しているサーバを収容する居室へは、建物へ入館後、複数のセキュリティレベルで区画された場所を通った後に入室できる。

居室への入退室等については、以下の項目のように厳重に管理される。

（1）厳重に施錠管理し、防護措置としてその入室者の身体的特徴の識別手段を用いた施錠設備による本人確認を行う。

（2）予めその資格について審査され指定登録を済ませた 2 名をもって入室する。入室者と同数の者の退出をもって、退出を完了とする。１名のみで在室する状態にならないよう、対策を講じる。なお、入室権限を有しない者の入室は原則として認めない。ただし、やむを得ずこれを認める場合には、予め TSA 責任者の許可を得て、入室権限者同行の上この者を入室させる。

（3）入室のための装置操作に不正常な時間を要した場合、警報が発せられるよう設定を行う。

（4）居室への入退室者及び在室者の状況については、遠隔監視、モーションセンサ及び画像記録により、自動的かつ継続的に監視記録する。当該記録は、TSA 責任者が正確に点検し、定められた期間、安全に保管する。

（5）認証設備室の所在及び仕様は、関係者以外には厳重に秘匿する。建物の内外には、認証設備室の所在についての表示をしない。

4.6.2.2 ＜その他の端末および、サーバについて＞

居室は、これを独立した区画とし、無人の際には入退室口に施錠しなければならない。鍵の管理及び授受については予め認定された管理者がその任に就く。入室権限を有しない者の入室は原則として認めないこととする。やむを得ずこれを認める場合には、予め TSA 管理者の許可を得て、入室権限者同行の上この者を入室させることができる。

4.6.3 バックアップセンタ

TSA のバックアップセンタを物理的に離れた箇所に設置し、メインセンタとバックアップセンタ間で SHV の同期をとりお互いの SHV を保有しあうことにより、他方の災害時にサービスを継続することが可能である。

4.6.4 建物、機器等の災害対策

TSA に関連する情報の保管場所及び情報システム関連設備を収容する場所は、情報種別、情報システム種別に基づいて災害等から適切に保護する。

データセンタについては、以下を遵守する施設を利用する。

1. 建物は耐火構造、室は防火区画とし、消火設備を設置。
2. 漏水検知器を設置し、天井、床には防水対策を講じ、かつ２階以上フロアに設置。
3. 建物は耐震構造とし、システムの転倒･落下を防止する対策をしたラックに設置。
4. 非常時に備え、非常時用の連絡装置、照明設備、携帯用照明器具等を設置。
5. 電気の瞬断や停電に備えて、電源の 2 重化の措置を講ずる。また、システムは自家発電装置の設置された建物で運用。
6. システムを安定稼働させるため、適正な空調設備を設置。
7. システムの稼動状況を監視システムと監視員により 24 時間 365 日監視を行う。
8. システムが設置してある居室内への入退室管理は、カメラ監視及びモーションセンサを設置し、監視員により 24 時間 365 日監視を行う。
9. システムが設置してある居室内への立ち入りは、IC カードゲート及び身体的な特徴（指紋、虹彩など）を基にした本人認証ゲートを設置し、許可なく入室ができないような措置を講ずる。

4.6.5 手続き上のセキュリティ

運用者の役割

運用者はタイムスタンプサーバーへの重要な業務の遂行時には次のことに従う。

- TSA 運営委員会の決定に従い業務を遂行する。
- 運用者は、TSA 責任者の信任をうける。
- 運用者は、個人認証のため、TSA 管理者立会いのもと、IC カードゲート及び身体的な特徴（指紋、虹彩など）を基にした本人認証を行う。
- 運用者は常に ID カードを携帯する。

IDC への入室管理

・運用者が IDC へ入室する際には、入室申請書を作成し TSA 責任者の承認を受ける。

・運用者が入室する際には、正当な権限者であることの識別・認証を IC カードゲート及び身体的な特徴（指紋、虹彩など）を基にした本人認証によって権限者であることを認証される。

設備（サーバ）へのアクセス権限

・システムは施錠されたラックの中に設置され、権限の無い第三者からの物理的アクセスを不可能とする。

・システムが設置されたラックを開錠するための鍵を持ち出す際には、TSA 責任者の承認が必要である。

・サーバへのアクセスはパスワードによる認証を行う。

・パスワードは推測が困難な文字列であること

・パスワードは一定期間で変更すること

4.6.6 秘密情報

TSA は、次に掲げる情報を秘密として受領しまたは生成したとみなす。次に掲げる情報は、本項に別段の規定がある場合を除き公開できない。

- TSA 運営機関は、サービス利用に関する従業員の信頼性および適格性並びにその満足な職務執行を合理的に保証する人事管理に関する実務を確立し、これに従うものとする。実務は、本運用規定に適合していなければならない。
- トランザクションの記録（記録全体およびトランザクションの監査証跡の両方を含む。）
- TSA が作成し、または保管する TSA サービス監査証跡の記録
- TSA、または監査人（内部監査か外部監査を問わない。）が作成した TSA サービス監査報告書（監査報告書が保管されている限り）
- 不測の事態に対応する計画および災害時における回復措置
- TSA のハードウェアおよびソフトウェアの運用、並びにサービス運営についてのセキュリティ対策

TSA および販売代理店は、加入者名またはその他の同一性確認のための情報を開示または売却してはならず、かつ、本規定に規定される場合を除き、これらの情報を共有してはならない。

4.6.7 秘密情報の任意発表／開示

TSA は、（ｉ）当該情報についての秘密保持義務を負う相手方、および（ii）秘密情報を要求する人（（ｉ）と同一人物でない場合）からの、認証され合理的に特定された事前の要求、または裁判所の命令がなければ、秘密情報を発表してはならず、また発表する義務を負うものではない。TSA は、秘密情報の開示に当たって、開示を求める人に対して、合理的な金額の手数料を事前に支払うよう要求することができる。

4.6.8 保管対象の記録及び保管方法

TSA は、下記の情報を信頼に足る方法で保存する。

1. TSA および、販売代理店自身による本規定の遵守を証する書類
2. サービス利用に関する重要な情報に関する書類
3. TSA が発行するタイムスタンプ記録の発行、検証履歴
4. 加入者による TSA サービスへの登録、検証に関する重要な行為の記録

これらの記録は､コンピュータを利用したメッセージまたは書類のいずれかの形式で保存する。但し、その索引付け、記憶、保存および再生は、正確かつ完全になされなければならない。完全性を維持するために定期的にバックアップを取らなければならない。媒体及び書類に関しては、入退室管理のある居室内にある施錠された保管庫に保管し、搬入出の管理を適切に行うこととする。

本項を遵守するため、TSA および、販売代理店は、加入者またはその代理人に対して、必要な書類の提出を求めることができる。

4.6.9 記録保存年数

TSA は、前項にあげた保管対象の記録について○年間、信頼性のある方法で保存する。これらの記録は、検索可能なコンピュータ上のメッセージまたは書類の、いずれかの方式で保存されなければならない。

4.7 業務の終了または停止

以下に記載する義務は、遅滞のない通知、業務を承継する機関への責任の引き継ぎ、記録の保管、および一定の救済を規定することによって、TSA のサービスの終了が及ぼす影響を軽減することを目的とする。

4.7.1 停止に先立って充足すべき要件

業務活動の停止に先立ち、以下の措置を講じなければならない。

1. 販売代理店、加入者に対し、TSA としての活動を停止する旨の意思を通知すること。当該通知は、少なくとも活動を停止する○日前までになされる必要がある。
2. タイムスタンプサービスの打ち切りが、加入者および現存するタイムスタンプ記録を参照して原本性を検証する必要がある人にもたらす混乱を最小限にくい止めるための合理的な努力をなすこと。
3. 記録保存のために合理的な手配をなすこと。
4. サービスを停止することについて、加入者に対し合理的な金額の払戻をなすこと。〈サービス利用価額を超えないものとする。〉

4.7.2 業務を承継する運営機関によるサービスの継続

1. **サービス加入者に対し連続したサービスを提供するため、業務を停止する TSA は、他の運営機関の書面による事前の同意を得た上で、現存する加入者のタイムスタンプ記録を他の運営機関が行うサービスで使用できるように手配しなければならない。**
2. **サービスを継続するに当たり、業務を承継する運営機関は、業務を停止する TSA の権利および防禦上の抗弁を代位し、かつ両者間で書面によって合意した限度で、現存するサービスに関する義務および責任を引き受けることとする。**
3. **業務を停止する TSA と加入者の間の契約中に別段の定めがない限り、また、業務を承継する運営機関の書面による承認を条件として、本規定は、元の TSA に対して適用されるのと同様に、業務を承継する運営機関においても効力を有する。**

本項に定める要件は、契約によって変更することができる。但し、かかる変更は、契約当事者間においてのみ有効とする。

5．一般管理規定

5.1 運営組織体制

5.1.1 方針

本規程を遵守し、適正な TSA を管理・統括していくために、運営組織体制を整備し、TSA の運営を行う。

5.1.2 体制と役割

【TSA 責任者】

TSA 責任者は、以下の役割を負う。

1. **TSA の運営を統括し、法令及び本規定に基づき、情報セキュリティの運営、情報セキュリティに関する活動の推進、監査及び教育を統括する。**
2. **TSA 管理者、個人情報安全管理者ならびに監査者を統括する。**
3. **本規定の内容を審査し、承認を行う。また、必要に応じ TSA 管理者と協議し、改訂する。**
4. **TSA 管理者によって申請された、本規定の逸脱事項について承認または否決を行う。**
5. **TSA を適正に運営推進するため、TSA 管理者を任命する。**
6. **TSA で取り扱われる個人情報を適正に保護するため、個人情報保護管理者を任命する。**
7. **TSA の業務運営が本規定に則り適正に実施されているか監査するため、監査者を任命する。**

【TSA 管理者】

TSA 責任者より任命されるTSA 管理者は以下の役割を負う。

1. **TSA 責任者の指示のもと、本規定に基づき、TSA の運営推進を行う。**
2. **技術・環境の変化に合わせ、本規定を定期的に見直し、改訂の必要がある場合は、TSA 責任者と協議する。**
3. **情報セキュリティに関する技術、対策、脅威に関しての情報収集および関係者への情報提供を行う。**
4. **監査者等からの報告に基づき、改善策の実施を指示する。**
5. **逸脱申請の受付を行い、申請された事項を調査・分析し、逸脱事項として許諾可能かを審査の上、TSA 責任者に上申する。TSA 責任者の承認が得られた逸脱事項についてはその管理を行う。**
6. **情報システムの企画、設計・構築、運用に関して管理を行う。**
7. **TSA 責任者と協議し、本規定の下部規則として、情報システムの企画、設計・構築、運用の各フェーズにおける実施事項を規定した「運用マニュアル」を作成する。**
8. **情報セキュリティ侵害行為等の報告があった際は、TSA 責任者と協議し必要な措置をとる。**
9. **TSA 責任者と協議し、「コンティンジェンシープラン」を作成する。**
10. **情報セキュリティを運営するために、不正プログラム管理者を任命する。**

【TSA 運営委員会】

1. 本運用規程の策定及び決定、修正を行う。
2. TSA 責任者及び TSA 管理者を任免する。
3. TSA の運営方針を決定する。
4. TSA の業務の停止等を決定する。

【個人情報安全管理者】

TSA 責任者より任命される個人情報安全管理者は以下の役割を負う。

1. TSA 責任者の指示に従い、TSA にて取り扱われる個人情報が適正に保護・管理されているか管理を行う。
2. TSA において、個人情報保護に関する各種法令及び当社の規程・基準の普及・教育を行い、社員、協働者の個人情報保護意識の高揚に努める。

【監査者】

TSA 責任者より任命される監査者は以下の役割を負う。

1. TSA の業務運営が本規定に則った運用がされているか監査を行う。
2. 監査者は公正不偏の態度で監査を行い、監査の結果を TSA 責任者に報告する。

【不正プログラム管理者】

TSA 管理者より任命される不正プログラム管理者は以下の役割を負う。

1. TSA 管理者の指示に従い、TSA において全情報システムのウィルス等不正プログラムの管理を行う。
2. ウィルス等不正プログラム関連情報の収集に努め、最新のウイルスチェックソフトウェア及びそのパターンファイルを情報システムに導入する。
3. 広範囲に影響を与えるサーバ等の機器のウィルス対策実施を徹底・確認する。
4. 情報システムに対する最新ウイルスチェックソフトウェアのインストールの徹底・確認をする。
5. 不正プログラム対応手順書を作成する。
6. 不正プログラムが検知された際は、TSA 管理者と協議し、速やかに復旧を行う。

5.2 情報に関する管理

5.2.1 情報に関する基本的な考え方

ア 情報所有者および情報利用者は、管理監督者のもと、社会的良識を持ち情報を取り扱うよう心がける。

イ 情報はその価値や性質によって取り扱い方法が決まるべきものである。従って、情報の価値や性質に対する認識を統一するため、情報には「情報種別」を設定、明示し、情報利用者は情報種別に従った情報の取り扱いをおこなう。

ウ　情報は取得／生成、流通、複製／保管から廃棄に至るまでの一連の情報ライフサイクルをたどり、ライフサイクルの段階毎に適切な取り扱い方法が異なるものである。従って情報利用者は情報ライフサイクルの各段階に相応しい情報の取り扱いをおこなう。

エ　情報利用者による安全な情報活用の管理責任は管理監督者にある。従って管理監督者は十分な注意と責任をもって情報利用者の監督、指導にあたること。

5.2.2　管理体制と役割

TSA 運用に関わる情報資産を安全に活用するために､TSA 内部に以下のような管理体制を明確にする。

ア　管理監督者

(ｱ)　情報利用者が適切に情報を利活用するよう監督、指導する。その役割から管理監督者はTSA 管理者とする。

(ｲ)　情報所有者や情報利用者が情報種別の設定や情報の取り扱いについて判断に迷った時は、判断し指示を与える。

(ｳ)　情報の漏洩、改ざん、破壊ならびに無断転載など不正行為の発見をした場合、またはその報告を受けた場合は、TSA 責任者に報告するとともに、損害を最小限に抑え、原因究明、再発防止に努める。

イ　情報所有者

TSA 運用に関わる情報資産を取得/生成或いは編集した者であり、情報資産に対して情報種別を設定、明示する。

ウ　情報利用者

(ｱ)　情報所有者が設定、明示した情報種別や情報ライフサイクルに従い、情報を適切に利活用する。

(ｲ)　情報の漏洩、改ざん、破壊ならびに無断転載など不正行為を発見した際は、直ちに管理監督者に報告する。

5.2.3　情報種別の設定とその運用

5.2.3.1　機密性に基づく情報種別

情報は、機密性の観点から、「厳秘」「秘密」「社外秘」の情報種別を付与される。情報種別を付与するのは情報所有者である。

【厳秘】

ア　極めて機密性が高く、情報所有者によって開示された個人及びその所在が完全に把握されなければならない情報の種別である。情報所有者から開示された者は一切他の社員、協働者に開示してはならない。

イ　厳秘」指定の情報は、厳密に保護、管理するものとし、施錠可能な保管庫に保管しなければならない。

1　電子情報として保管される場合、必要最小限の情報利用者に閉じてアクセス制御を行うとともに、暗号化して保存する。また、ネットワーク流通する際は、暗号化を行う。
2　「厳秘」情報を配布する場合、必ず封書等内容を秘匿できる状態で行う。なお、緊急止むを得ない事由により FAX 等で送信する場合には、名宛人自らが受信を行う。
3　「厳秘」情報は、情報所有者及び情報所有者から許可を受けた者以外による書き込み、編集等を禁止する。
4　可搬媒体（紙、FD 等）として保管される場合は、原則として複製を禁止する。止むを得ず複製する場合は、情報管理者が所在と複製数を管理しなくてはならない。

【秘密】

ア　非常に機密性が高く、情報所有者が指定する範囲（個人、グループ等）に限って開示される情報の種別である。業務上特に必要のある場合に限り、他の社員、協働者に対して開示することができる。
イ　「秘密」指定の情報は、十分な注意をもって保護、管理するものとする。
1　電子情報として管理される場合は、業務上必要な情報利用者のみが利用できるようにアクセス制御を行うとともに、外部ネットワークを経由して暗号化されないまま流通させることを禁止する。
2　可搬媒体（紙、FD 等）として保管される場合は、情報所有者が示す開示範囲を守り、みだりに複製してはならない。

【社外秘】

ア　機密性が高く、社内に限って開示される情報の種別である。社員、協働者は社外に対して一切漏洩、開示してはならない。
イ　「社外秘」指定の情報は、社外に漏洩してはならない。
ウ　協働者を開示範囲に含まない情報に対して、特に「社外秘（社員）」又は「社外秘（社員限り）」等の表示を行う。

5.2.3.2　可用性、完全性に基づく情報種別

情報は可用性、完全性の観点から、「重要」の情報種別を付与される。情報種別の付与を行うのは情報所有者である。

【重要】

ア　業務の遂行に必要不可欠な情報であり、極めて高い完全性が要求され、又は常に利用し得る状態で管理されなければならない情報の種別である。この種別に指定された情報については、改ざん、欠落、破壊等から守るため、厳重に管理しなくてはならない。
イ　「重要」情報は、情報所有者及び情報所有者から許可を受けた者以外による書き込み、編集等を禁止する。
ウ　電子情報、紙等の媒体のいずれにより保管される場合でも、必ず複製をとり不測の事態に備えなければならない。

エ　「重要」種別の指定を受ける情報のイメージ

1　商法等において備置が法定されている書類等

2　緊急時にも利用できなくてはならない情報等

5.2.3.3　開示範囲

「厳秘」、「秘密」、「社外秘」情報は、情報所有者の開示する特定の関係者（「厳秘」の場合）、業務上情報の開示を必要とする関係者（「秘密」の場合）を必要に応じて的確に明示する。この表示が与えられた場合は、情報所有者の許可なく開示範囲を広く解釈してはならない。

（例：「厳秘（統括部長）」、「秘密（○○担当）」等）

5.2.3.4　保管期間

「厳秘」、「秘密」、「社外秘」情報は、法定又は情報所有者の判断により保管期間を定め、必要に応じて表示することができる。この表示が与えられた情報は、保管期間の経過後に定められた手続きに従い廃棄等所要の措置をとる。

5.3　本規程のライフサイクル管理

5.3.1　方針

本規定の実効性を高め、TSA を管理運営するために、普及・教育、逸脱管理、監査、改訂といった事項を組織的・計画的に実施する。

5.3.2　体制と役割

【TSA 責任者】

TSA 責任者は以下の役割を負う。

1. 監査者から得た監査結果を基に、現状の改善を図る。
2. 法令ならびに本規程を遵守しない社員、協働者には改善措置をとるように指示する。

【TSA 管理者】

TSA 管理者は以下の役割を負う。

1. 本規程の逸脱申請受付を行い、申請された事項を調査・分析し、逸脱事項として許諾可能かを審査の上、TSA 責任者に上申する。TSA 責任者の承認が得られた逸脱事項についてはその管理を行う。
2. 技術・環境の変化に合わせ、本規程を定期的に見直し、改訂の必要がある場合は TSA 責任者と協議を行い、改訂の原案を作成する。
3. 情報システムを適正に運用管理するために、本規程の下部規則として、運用・利用に関する規則を制定する。

【監査者】

監査者は以下の役割を負う。

1. 定期監査ならびに抜き打ち監査を実施し、TSA が法令ならびに本規定を遵守しているか運用実態を把握・評価する。
2. 監査の結果は、定期的に TSA 責任者に報告する。
3. 法令ならびに本規定を遵守しない社員、協働者には改善措置をとるように要請する。

5.3.3 普及・教育

本規程の普及・教育に関して、以下を遵守する。

1. TSA 管理者は、情報システムを適正に運用管理するために、本規定の下部規則として、運用・利用に関する規則を制定する。

5.3.4 逸脱管理

本規定の逸脱を管理するため、以下を遵守する。

1. TSA 管理者は、本規程の逸脱申請受付を行い、申請された事項を調査・分析し、逸脱事項として許諾可能かを審査の上、TSA 責任者に上申する。TSA 責任者の承認が得られた逸脱事項についてはその管理を行う。
2. TSA 責任者は、TSA 管理者に申請された、本規程の逸脱事項について承認または否決を行う。

【逸脱の基本的な考え方】

業務遂行において、例外的に本規定が適用されない場合を以下に例示する。

- 人命に関わる緊急時又は災害時等
- 社会的正義に関わる場合（司法からの要請等）
- 情報システムにおいて技術、運用、コスト面により本規定の適用が困難である場合等

こうした場合も、TSA 管理者に必ず申請し、TSA 責任者の承認を得た上で運用しなければならない。ただし、人命に関わる緊急・災害時においてはこの限りではない。

5.3.5 監査

TSA および、販売代理店は、サービス利用に関するあらゆる重要な出来事に関する監査証跡を保存するために信頼性のあるシステムを導入し、維持しなければならない。TSA および、販売代理店は、本規定、その他該当する契約、ガイドライン、手続および基準を遵守しているか否かを評価するために、その運営状況について、年 1 回監査を受ける。この費用は TSA および、販売代理店が負担する。

TSA における業務が、本規定に沿って執行されているかを把握するため、以下を遵守する。

1. 監査者は、定期監査ならびに抜き打ち監査を実施し、TSA が法令ならびに本規定を遵守しているか運用実態を把握・評価し、TSA 責任者に報告する。
2. TSA 責任者は、法令ならびに本規定を遵守しない社員、協働者には改善措置をとるように指示する。

5.3.6 本規程の改訂

本規程の改訂に関して、以下を遵守する。

1. TSA 管理者は、技術・環境の変化に合わせ、本規定を定期的に見直し、改訂の必要がある場合は TSA 責任者と協議を行い、改訂の原案を作成する。
2. TSA 責任者は、必要に応じて本規定を見直し、TSA 管理者と本規定の改訂を協議し、適宜改訂を行う。本規定を遵守し、適正な TSA を管理・統括していくために、TSA 運営組織体制を整備し、TSA の運営を行う。
3. 本規程の改訂の承諾は TSA 運営委員会が行う。

5.4 スタッフセキュリティ

5.4.1 方針

TSA 責任者は、人的リスクの面から情報セキュリティを確保するために、誓約書等の措置をとり、社員、協働者のすべてが情報セキュリティを守るよう適正に管理を行う。また、社員、協働者は、法令ならびに本規定を遵守し、TSA の情報セキュリティが適正に確保されるよう自ら責任をもって行動しなければならない。

5.4.2 体制と役割

【TSA 責任者】

1. 社員、協働者の模範となるよう法令ならびに本規定を遵守し、情報セキュリティ意識の向上に努める。
2. 管理監督の責任を有する社員、協働者の業務遂行及び法令ならびに本規定の遵守に関して管理監督責任を有する。
3. 協働者に対して法令ならびに本規定の教育・啓発を行い、情報セキュリティ意識の向上に努める。
4. 業務上の必要により協働者が機密度の高い情報に接すると想定される場合には、事前に機密保持契約義務を負わせる等セキュリティ関連事項を含んだ契約を本人と締結する等の措置をとる。
5. 前項の契約を締結した者が契約において定める範囲外の情報に接することがないよう、所要の措置をとる。

【TSA 管理者】

1. 法令ならびに本規定を遵守し、かつ情報セキュリティに関して自ら意欲的に学ぶ。
2. 協働者の業務遂行状況を把握し、適宜注意・指導を行いながらセキュリティ侵害等の問題発生を未然に防止する。

5.4.3 要員管理

要員管理に関して、以下を遵守する。

1. TSA の社員、協働者は、提供するサービスに必要な専門知識、経験、資格を有さなければならない。
2. 情報セキュリティ責任者は、情報セキュリティの適正確保、情報システムの円滑な運用のため、要員の配置、交替等人事管理を適切に行う。
3. 情報セキュリティ責任者は、各要員の配置にあたっては、職務権限を適切に分離し、相互牽制とチェックの利く分担とする。
4. 情報セキュリティ責任者は、作業環境の整備や要員の健康管理を適正に行う。

5.5 個人情報保護

5.5.1 方針

TSA にて取り扱われる個人に帰属する情報について、個人の権利利益を保護するため、適法かつ公正な手段によって収集し、適切な管理体制によって管理し、目的外の利用を禁止する。

5.5.2 体制と役割

個人情報安全管理者は以下の役割を負う。

1. TSA 責任者の指示に従い、TSA にて取り扱われる個人情報が適正に保護・管理されているか管理を行う。
2. TSA において、個人情報保護に関する各種法令及び当社の規程・基準の普及・教育を行い、社員、協働者の個人情報保護意識の高揚に努める。

5.5.3 個人情報の取扱

個人情報の取扱について、以下を遵守する。

1. 個人情報の取扱方法を明確にし、顧客に周知する。
2. 個人情報を収集する際は、適法かつ公正な手段によって収集し、業務上必要な範囲内で収集を行う。
3. 個人情報の収集に際して、個人情報の利用又は提供の目的を明確にし、同意を得るものとする。
4. 政治的見解、宗教、信教（宗教、思想及び信条）、組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する個人情報については、収集、利用又は提供を行わない。ただし、同意を得た場合、及び法令の規定による場合はこの限りではない。
5. 個人情報を第三者から収集するに当たっては、個人の利益を不当に侵害しないようにするものとする。
6. 個人情報を業務上必要な範囲内で正確かつ最新の状態に管理するものとする。
7. 個人情報への不当なアクセス又は個人情報の紛失、破壊、改ざん、漏洩その他の危険に対

して、必要な安全保護措置を講じるものとする。

8. 業務上必要な期間を経過した後は、個人情報の廃棄その他の処理を行うものとする。
9. 個人情報の取扱を委託する場合には、外部委託先との委託契約を締結するに当たって、TSA と同等に個人情報の保護に関する事項について定めるものとする。
10. 自己の個人情報について開示の請求があった場合、訂正の請求があった場合、及び利用又は提供の中止の請求があった場合には、これに応じるものとする。

5.6 情報システム管理

5.6.1 情報システム管理

TSA は、不正なアクセスを防止するためのファイアウォール及び不正なアクセスを検知するシステム並びに送信をした設備の誤認、通信内容の盗聴及び改変を防止するシステムを居室に備える。また、TSA は、OS 等の安全性に対する脅威についての情報を常に収集し、問題があればメーカ推奨の修正プログラムを適用する等の対策を実施する。

5.6.2 情報システムのサービス継続

情報システム及びネットワークのサービス中断等により TSA サービスの継続が脅かされることを回避し、影響を極力軽減するため、必要なセキュリティ対策の実施、コンティンジェンシープランの作成を行う。

5.6.3 電子情報保護

機密性、完全性の高い電子情報を保護するため、外部ネットワークのみならず内部の他のサーバからのアクセス制御、暗号化、日時の定期的なバックアップ等の措置を講じる。

5.6.4 不正使用防止

情報システムの不正使用を防止するため、IDS やファイアウォールにより不正アクセスの防御、検知、復旧等の対策を講じる。

5.6.5 コンピュータウィルス等不正プログラム

情報システムにコンピュータウィルス等不正プログラムの侵入や組込みによる被害が発生した場合、重大な損害が発生する可能性があるため、不正プログラム管理者を設置し、不正プログラムの侵入や組込みの防御、検知、復旧等の対策を講じる。

TSA の運用にあたり、外部からの媒体によるデータ及びプログラムのインストールは原則として行わず、もし、行う場合は、不正プログラム管理者により、媒体及びデータ、プログラムのウィルス等の検出を行い、問題の有無の確認を行う。

5.7 不測の事態に対する計画と災害時における回復措置

5.7.1 災害時の回復措置

災害などにより、一つのセンターが使用不能になったときは、もう一方のセンターでサービスの続行を行う。ただし、両センターともサービスの続行が不可能な場合は、速やかな復旧措置を行うとともに、サービスを提供する販売代理店、利用者への連絡を行う。

復旧手順については、コンティンジェンシープランに基づく。

5.7.2 TSA サービスの危殆化

TSA の情報セキュリティを侵害する行為ならびに機密情報の漏洩等を発見した場合は、直ちに情報セキュリティ責任者等へ連絡することとし、情報セキュリティ責任者等は速やかに必要な措置をとる。

- TSA の情報セキュリティ侵害行為ならびに情報漏洩・改ざん等の統括を行い、発見者より情報セキュリティ侵害行為等の報告があった際は、速やかに協議し必要な措置をとる。
- TSA 管理者は「コンティンジェンシープラン」を作成する。

5.7.3 コンティンジェンシープラン

TSA 責任者が主導となり、「コンティンジェンシープラン」を作成する

TSA 責任者は緊急時の対応が速やかに行えるよう作成した「コンティンジェンシープラン」の周知を TSA 管理者及び TSA 運用関係者に徹底する。

5.8 コンプライアンス

5.8.1 準運用要件拠法

当事者間の契約または他の準拠法を選択する旨の規定にかかわらず、本規定の解釈および有効性等は、日本国内法および規制に基づき解釈する。

5.8.2 遵守すべき法令・指針

管理職、社員、協働者は、以下の法令を遵守する。

（1）業務の遂行に当たり、遵守すべき法令

民事法、刑事法、商法、独占禁止法、不正競争防止法、著作権法、特許法、商標法、意匠法、不正アクセス行為の禁止等に関する法律等

5.8.3 紛争解決

本規定または本サービスに関する一切の紛争は、東京地方裁判所を第一審の専属合意管轄裁判所として処理するものとする。

メンバーリスト

事務局

川松　和成　電子商取引推進協議会　主席研究員
松山　博美　電子商取引推進協議会　主席研究員
前田　陽二　電子商取引推進協議会　主席研究員

顧問

松本　　勉　横浜国立大学大学院
平田　健治　大阪大学大学院

リーダー

木村　道弘　日本電気株式会社
宮崎　一哉　三菱電機株式会社
櫻井　徹　　株式会社 NTT データ

TF5 メンバー（編集メンバー）

氏名	会社名
鈴木　邦康	株式会社ＮＴＴデータ
磐城　洋介	ＮＴＴコムウェア株式会社
野村　　進	ＮＴＴコミュニケーションズ株式会社
鈴木　優一	エントラストジャパン株式会社
上畑　正和	セイコーインスツルメンツ株式会社
雨宮　隆征	セイコーインスツルメンツ株式会社
秋山　将	日本電信電話株式会社
島　成佳	日本電気株式会社
近藤　弓末	ソニー株式会社

SWG3 メンバー（参加メンバー）

氏名	会社名
河田　悦生	株式会社エヌ・ティ・ティ・ドコモ
関野　公彦 ＊	株式会社エヌ・ティ・ティ・ドコモ
風間　博之	株式会社ＮＴＴデータ
宍倉　勝仁	シャチハタ株式会社
岩崎　善徳 ＊	セイコーインスツルメンツ株式会社
藤川　真樹	綜合警備保障株式会社
星野　　理	株式会社帝国データバンク
藤岡　直美	日本アビオニクス株式会社
小暮　貢次郎	日本信販株式会社
野口　雄治	日本認証サービス株式会社
浅野　昌和	日本ボルチモアテクノロジー株式会社
松永　和男	株式会社日立製作所
永倉　　俊	富士通株式会社
小谷　誠剛	富士通株式会社
西谷　研次	株式会社 UFJ 銀行

（注）＊はオブザーバー

平成 14 年度
ＥＣ技術基盤の相互運用性に関する調査研究事業
（電子署名生成・検証システムのセキュリティ環境の
国際標準化等の調査）
タイムスタンプサービスの運用ガイドライン
平成 15 年３月発行

発行所　財団法人　日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園３丁目５番８号
機械振興会館３階
TEL：03(3436)7500
印刷所　新高速印刷株式会社
東京都港区新橋 5-8-4
TEL：03(3437)6365

この資料は再生紙を使用しています。