ＴＫＣタイムスタンプ運用規定（TP/TPS）

Ver 1.02

2019年9月13日

株式会社TKC

目次

1. はじめに 6

1.1 概要 6
1.2 識別 6
1.2.1 ドキュメント名称、バージョン 6
1.2.2 オブジェクト識別子 6
1.3 目的と定義 6
1.3.1 目的 6
1.3.2 用語の定義 7
1.3.3 本サービスの概要 7
1.3.4 本サービスの内容 8
1.3.5 本サービスの利用時間 8
1.4 本規定に関する連絡先 8

2. 一般規定 9

2.1 義務 9
2.1.1 当時刻認証局の義務 9
2.1.2 利用者の義務 9
2.2 財務上の責任 10
2.2.1. 当時刻認証局の損害賠償責任 10
2.3 解釈と執行 11
2.3.1 準拠法 11
2.3.2 可分性 11
2.3.3 存続性 11
2.3.4 通知 11
2.3.5 紛争解決の手続き 12
2.3.6 不可抗力 12
2.4 公表とリポジトリ 12
2.4.1 当時刻認証局に関する情報の公開 12
2.4.2 公開の時期 12
2.4.3 アクセス制御 12
2.4.4 リポジトリ 12
2.4.5 その他の開示情報 12
2.5 ビジネス情報の秘匿性 12
2.5.1 機密扱いとする情報 12

2.5.2 機密扱いとしない情報 13
2.5.3 法執行機関への情報開示 13
2.5.4 民事手続き上の情報開示 13
2.5.5 利用者の要求による情報開示 13
2.6 知的財産権 13
2.7 個人情報の扱い 14
3. 本人確認と認証 14
4. 運用要件 14
4.1 タイムスタンプトークンの発行 14
4.2 タイムスタンプの検証 14
4.3 監査 14
4.3.1 監査情報の定義 14
4.3.2 監査人の身元、資格 15
4.3.3 監査人と被監査部門との関係 15
4.3.4 監査内容 15
4.3.5 監査周期 15
4.3.6 監査情報の保管期間 16
4.3.7 監査指摘事項への対応 16
4.3.8 監査情報の保護 16
4.3.9 監査情報の保管 16
4.3.10 監査結果の開示と対処 16
4.4 記録のアーカイブ化 16
4.4.1 アーカイブデータの種類 16
4.4.2 アーカイブデータの保管期間 16
4.4.3 アーカイブデータの保護 16
4.4.4 アーカイブデータのバックアップ 17
4.4.5 記録へのタイムスタンプ要件 17
4.4.6 アーカイブデータの収集システム 17
4.5 鍵の定期更新 17
4.6 システムのトラブル、災害からの復旧 17
4.7 業務の終了 17
4.8 タイムソースの管理・トレーサビリティ 17
4.8.1 当時刻認証局内の時刻精度 17
4.8.2 タイムスタンプユニットの時刻精度 18
4.8.3 時刻のトレーサビリティ 18

4.9 暗号アルゴリズムの危殆化対応 18

5. 物理的、手続き的及び要員的なセキュリティ管理 18

5.1 物理的なセキュリティ管理 18
5.1.1 施設の場所と建物構造 18
5.1.2 入退室管理と機器へのアクセス 18
5.1.3 電源、空調設備 19
5.1.4 水害対策 19
5.1.5 火災対策 19
5.1.6 地震対策 19
5.1.7 媒体管理 19
5.1.8 廃棄物処理 19
5.1.9 外部バックアップ 19
5.2 手続きの管理 19
5.2.1 信頼される役割 19
5.2.2 人員配置 20
5.2.3 各役割の認証と認可 20
5.3 要員的なセキュリティ管理 20
5.3.1 従事者の要件 20
5.3.2 経歴検査 20
5.3.3 トレーニング要件 20
5.3.4 トレーニング周期 20
5.3.5 ジョブローテーションの実施 20
5.3.6 不正行為の罰則 20
5.3.7 要員へ提示する文書 20

6 技術的管理 21

6.1 鍵ペア生成とインストール 21
6.1.1 鍵ペア生成 21
6.1.2 タイムスタンプトークンの公開鍵証明書の配布 21
6.1.3 鍵長 21
6.1.4 鍵生成 21
6.1.5 鍵使用の目的 21
6.2 秘密鍵の防護 21
6.2.1 暗号モジュールの基準 21
6.2.2 秘密鍵の複数人管理 21
6.2.3 秘密鍵の預託 21

6.2.4 秘密鍵のバックアップ 21
6.2.5 秘密鍵のアーカイブ 21
6.2.6 暗号モジュールへの秘密鍵格納 22
6.2.7 秘密鍵活性化方法 22
6.2.8 秘密鍵破棄方法 22
6.3 その他の鍵管理について 22
6.3.1 公開鍵記録保存 22
6.3.2 秘密鍵の使用期間 22
6.3.3 鍵ペアの有効期間 22
6.4 活性化データ 22
6.4.1 活性化データの生成 22
6.4.2 活性化データの保護 22
6.5 コンピュータセキュリティ管理 23
6.5.1 使用するコンピュータセキュリティの技術要件 23
6.5.2 コンピュータセキュリティ評価 23
6.6 システムのライフサイクル管理 23
6.6.1 システム開発管理 23
6.6.2 システム維持管理 23
6.6.3 セキュリティ運用管理 23
6.6.4 セキュリティ評価のライフサイクル 23
6.7 ネットワークセキュリティ管理 23
6.8 暗号化モジュールの管理 23
7. 仕様の管理 23
7.1 仕様の変更手順 23
7.2 公開と通知の規則 24
7.3 本規定の承認手順 24
8. タイムスタンプトークンのプロファイル 25
用語集 A 26
用語集 B 26

改版履歴

初版発行日：２０１６年5月２０日

版	変更日	内容
Ver 1.00	2016/5/20	初版
Ver 1.01	2018/5/25	1.「1.2.2 オブジェクト識別子」の認証局の OID を、認証局ポリシーの閲覧先 URL に変更 2.「4.5 鍵の定期更新」の期間を 1 年から 1 年 1 カ月以内に変更 3.「6.3.2 秘密鍵の使用期間」の期間を 1 年から 1 年 1 カ月以内に変更 4.「6.3.3 鍵ペアの有効期間」の有効期間の記述内容を変更
Ver 1.02	2019/9/13	1.「6.2.1 暗号モジュールの基準」の FIPS 140-2 Level 3 以上の表記を、FIPS 140-2 Level 3 相当 に変更 2.「6.8 暗号モジュールの管理」の FIPS 140-2 Level 3 認定品の表記を、140-2 Level 3 相当の製品 に変更

1. はじめに

「ＴＫＣタイムスタンプ運用規定」（以下、「本規定」という。）は、株式会社ＴＫＣ（以下、「当社」という。）が運営する時刻認証局（以下、「当時刻認証局」という。）が実施するタイムスタンプサービス（以下、「本サービス」という。）について定める。

1.1 概要

本規定は、当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について規定する。本規定は、タイムスタンプポリシー（Time-stamp policy）と時刻認証局運用規程（Time-stamping practice statement）を一つにしたものである。

1.2 識別

1.2.1 ドキュメント名称、バージョン

名称：ＴＫＣタイムスタンプ運用規定
バージョン：１．０１
作成日：２０１８年5月２５日
作成者：株式会社ＴＫＣ

1.2.2 オブジェクト識別子

内容	OID、URL
本サービス	
株式会社ＴＫＣ	0.2.440.200312
ＴＫＣタイムスタンプ	0.2.440.200312.100.100
サービスポリシー	0.2.440.200312.100.100.100
本サービスにおいて使用される認証局	
セコムトラストシステムズ株式会社	1.2.392.200091
Security Communication RootCA タイムスタンプサービス用証明書ポリシー	https://repository.secomtrust.net/
本サービスにおいて使用される時刻源	
アマノ株式会社	0.2.440.200192
時刻配信・監査サービス for TSU	0.2.440.200192.100.100
サービスポリシー	0.2.440.200192.100.100.100

1.3 目的と定義

1.3.1 目的

当社は、当社または当社が認定した法人が提供するシステムまたはサービス（以下、総称して「ＴＫＣシステム等」という。）を用いて作成された電子文書にタイムスタンプを発行することにより、タイムスタンプに刻印されている時刻以前に文書が存在し（存在証明）、その時刻以降文書が改ざんされていないことを証明する（非改ざん証明）ことで、もって当

該電子文書の原本性を確保し証拠性を高めることを目的として、当時刻認証局を運営する。

1.3.2　用語の定義

本規定で使用する用語は、以下のとおりとする。

（１）時刻認証局（TSA）

当社が運営する、RFC3161 に基づくタイムスタンプトークン（TST）を発行する局をいう。

（２）役社員

当社の役員及び社員をいう。

（３）利用者

ＴＫＣシステム等を通じて、別途当社が定めるＴＫＣタイムスタンプ利用規約に同意して本サービスを利用する者をいう。

（４）時刻配信局（TAA）

協定世界時（UTC）に対して追跡可能性（トレーサビリティー）のある時刻の配信を行い、かつ当時刻認証局が管理するタイムスタンプユニット（TSU）内の時計の時刻監査を行う事業者をいう。当時刻認証局が利用する時刻配信局は、アマノ株式会社が運営する時刻配信・監査サービス for TSU とする。

（５）認証局（CA）

当時刻認証局の TSU に使われる公開鍵証明書の認証を行う事業者をいう。当時刻認証局が利用する認証局は、セコムトラストシステムズ株式会社とする。

（６）国家時刻標準機関（NTA）

本規定において国家時刻標準機関とは、TAA が管理・運用する時計の比較校正元となる時計を管理・運用する機関をいう。

1.3.3　本サービスの概要

本サービスは、当時刻認証局が利用者からの TST 発行要求に対して RFC3161 に準拠した TST を生成し発行するサービスをいう。

（１）当時刻認証局は、タイムスタンプの対象となるデータの内容については一切関知しない。

（２）TST に含まれる時刻情報は、当時刻認証局が TST を生成した時点の時刻とする。

（３）TST の有効期間は 10 年間とする。ただし、秘密鍵の危殆化やハッシュ及び暗号アルゴリズムの脆弱化が発生した場合には、TST 示される有効期限より以前に、その有効性を失効させることがある。

（４）TST 内で使用するハッシュアルゴリズムは、「８．タイムスタンプトークンのプロファイル」に記載のとおりとする。

（５）TST には利用者の情報は含めない。

1.3.4　本サービスの内容

本サービスの内容は以下のとおりとする。

（１）当時刻認証局は、利用者の依頼に基づき、利用者から送付されたハッシュ値に対して RFC3161 に準拠した TST を生成し、それを利用者に対して発行する。

a) TST は当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電子署名が行われる。

b) TST の電子署名に使用される公開鍵暗号方式は、6.1.3で規定された方式を用いる。

c) 当時刻認証局は、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する。

d) 当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う。

（２）TST に含まれる時刻情報は本規定に基づいて以下の条件で付与される。

a) TST に記載される時刻は TSU の ハードウェアセキュリティモジュール（HSM）内の時計の時刻とする。

b) 時刻配信局が行う時刻監査により TSU 内の時計の時刻が UTC に対して±1 秒以内であることを確認する。当時刻認証局は時刻配信局から時刻監査結果の異常を通知された場合、TSU の TST 発行機能を速やかに停止するものとする。

c) TST を発行する TSU は、時刻配信局から供給される時刻とは別の手段にて UTC 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する。UTC の時刻と±1 秒を超える誤差が検知された場合は、TSU を停止し、本規定で定められた時刻範囲内で TST が発行されることを保証する。

d) 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生成を実施した時刻を表すものとする。

e) 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ない。

f) 当時刻認証局が維持する時刻精度は±1 秒とする。

（３）TST の有効期間は、タイムスタンプを押印した時刻から、TST の電子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限迄とする。

1.3.5　本サービスの利用時間

本サービスの利用時間は、原則２４時間３６５日とする。

1.4　本規定に関する連絡先

名称：株式会社ＴＫＣ
所在地：〒320-8644 栃木県宇都宮市鶴田町１７５８番地
e-mail アドレス： tkctimestamp@tkc.co.jp

2. 一般規定

2.1 義務

2.1.1 当時刻認証局の義務

当時刻認証局は、本サービスの提供にあたり、本規定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う。ただし、当時刻認証局は、利用者が本規定に基づいて当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する。

（1）TST の生成・発行

当時刻認証局は、本規定に基づき TST を生成し、利用者に対して発行する。

（2）時刻の管理

当時刻認証局は、発行する TST の発行時刻が 1.3.4.(2) の f） に規定する誤差を超えないように、当時刻認証局のシステムの時刻管理を行う。

（3）セキュリティ管理

当時刻認証局は、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する。

（4）秘密鍵に対応する公開鍵証明書の失効申請と届出

TSU の秘密鍵が危殆化した場合、当時刻認証局はただちに当該秘密鍵を使用した TST の発行を中止し、認証局への連絡及び秘密鍵に対応する公開鍵証明書の失効手続を行うとともに、速やかに利用者に連絡する。また、TSU の秘密鍵が危殆化した場合以外の理由で秘密鍵に対応する公開鍵証明書の失効を行う場合、当時刻認証局は、利用者に対して事前に連絡を行う。なお利用者への連絡方法等は、2.3.4.に定めるとおりとする。

2.1.2 利用者の義務

利用者は本サービスの利用にあたっては本規定に記載の事項を了承したうえで以下の義務を負い、また、本規定に基づいて当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する。

（1）TST の利用制限の遵守

TST はその目的等を記載した本規定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 を利用するものとする。

（2）本規定の遵守

利用者は本規定を遵守すると共に、TST を複製・配布する場合、利用者に対して本規定を遵守させるものとする。

（３）リポジトリ又は通知の確認

利用者はリポジトリ又は当時刻認証局からの通知の情報を定期的に収集するものとする。

（４）利用者情報の変更通知

利用者は、当時刻認証局に届け出た利用者情報の内容に変更が生じたときは、ただちにその変更内容を定められた手順で当社に通知するものとする。

（５）TST の検証義務

利用者は TST を利用するにあたっては、TST を検証するものとする。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を含む。

（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定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 を利用するものとする。

2.2 財務上の責任

2.2.1. 当時刻認証局の損害賠償責任

本サービスに関する当社の責任は、2.1.1.に記述する範囲に限られるものとし、適用される法令により許容される最大限の範囲において、当社は、賠償責任その他の保証及び責任を負わないものとする。また、法令により強制される場合であっても、賠償総額は、本サービスを利用する根拠となるＴＫＣシステム等の利用契約書に記載する賠償額を超えないものとし、当社の責に帰すことのできない事由から生じた損害、逸失利益、当社の予見の有無を問わず特別の事情から生じた損害、間接損害、派生的損害、付随的損害、データ・プログラムの喪失については、当社は賠償責任を免れるものとする。

2.2.2. 免責事項

2.2.1.の規定にかかわらず、下記の何れかに該当する場合においては、当社は賠償義務を負わないものとする。

（１）当時刻認証局が本規定ならびに個別のサービス契約に従い、本サービスを適正に遂行していた場合

（２）利用者の故意、過失若しくは違法行為に起因して損害が発生した場合

（３）利用者による本規定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

（４）利用者のシステムに起因して損害が発生した場合

（５）次にあげる当時刻認証局の支配を超えた事由に起因して損害が発生した場合

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) その他の当時刻認証局の支配を超えた事由

（6）4.6 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

（7）当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

（8）TST の失効に起因して損害が発生した場合

2.3 解釈と執行

2.3.1 準拠法

本規定の解釈及び有効性等は、日本法に基づき解釈するものとする。

2.3.2 可分性

本規定中の一部の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、本規定の他の規定は有効に存続し適用される。

2.3.3 存続性

本規定の「2.2 財務上の責任」、「2.3 解釈と執行」、「2.5 ビジネス情報の秘匿性」、「2.6 知的財産権」及び「2.7 個人情報の扱い」は、本サービスの終了または本規定の廃止後も有効に存続する。

2.3.4 通知

本規定に関する通知は、以下のとおりとする。

（1） 利用者から当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 本規定に関する連絡先」に基づき特定される宛先に送付するものとする。書面による通知は受領日をもって有効とする。

（2） 当時刻認証局から利用者への通知は、利用者が登録した連絡先へ発信した時点で通知したものとする。利用者は連絡先を変更する場合、速やかに当時刻認証局に届け出るものとする。当該届け出がなされない場合においては、当時刻認証局は届け出がなされている通知先へ通知することにより、通知義務を履行したとみなすものとする。

2.3.5　紛争解決の手続き

本規定又はそれに付随して生じた紛争、当時刻認証局による本サービスに関する紛争について法廷での解決を図る際、訴額に応じ、東京地方裁判所又は東京簡易裁判所をもって第一審の専属的合意管轄裁判所とする。

2.3.6　不可抗力

当社は、天災地変、戦争、伝染病、停電、火災、地震、テロ、その他の災害など、当社の支配を超える事件から生じた本規定に関する違反、遅滞、不履行に、一切責任を負わない。

2.4 公表とリポジトリ

2.4.1　当時刻認証局に関する情報の公開

当時刻認証局は、以下の情報を当時刻認証局のリポジトリに公開する。

（１）ＴＫＣタイムスタンプ運用規定（本規定）

（２）公開鍵証明書情報

2.4.2　公開の時期

当時刻認証局は、本規定変更時、その他当時刻認証局の責任者が必要と判断した時に随時更新を行う。

2.4.3　アクセス制御

当時刻認証局のリポジトリには、インターネットでアクセスできる。特にアクセスの制御は行わない。

2.4.4　リポジトリ

当社は、2.4.1 において定める情報を下記リポジトリに公開するものとする。

URL　https://www.tkc.jp/tsa/repository

2.4.5　その他の開示情報

TST に時刻監査証明書が含まれない場合には、利用者の求めに応じ時刻配信局発行の時刻監査記録を開示する。

2.5　ビジネス情報の秘匿性

2.5.1　機密扱いとする情報

当時刻認証局は、その情報が漏えいすることによって当時刻認証局、利用者、時刻配信局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する。

当時刻認証局は、機密扱いとした情報を含む書類及び記憶媒体を、安全に保管、管理する。

当時刻認証局は、機密扱いとした情報を、本規定又はＴＫＣシステム等の利用規約又は使用許諾契約に定められている場合を除いて、いかなる者にも原則開示しない。

2.5.2　機密扱いとしない情報

「2.5.1　機密扱いとする情報」の規定に関わらず、当時刻認証局は次に定める情報については機密扱いとしない。

（１）本規定等、公開する情報として明示するもの。

（２）開示した時点又は開示後に、当該情報の開示を受けた利用者又は当時刻認証局の責によらずして公知となった情報。

（３）第三者から機密保持義務を負うことなく適法に知得した情報。

（４）当該情報を開示した利用者又は当時刻認証局が第三者に対し機密保持の義務を課すことなく開示した情報。

（５）個人的に識別可能な全ての情報を除き、その情報の元の所有者を識別できなくした統計目的で編集したデータ。

2.5.3　法執行機関への情報開示

当時刻認証局は、当時刻認証局で扱う全ての情報に対し法的根拠に基づく情報開示の要求が法執行機関よりなされた場合、法で定められた範囲内で当該情報の開示を行う。

2.5.4　民事手続き上の情報開示

当時刻認証局は、当時刻認証局で扱う全ての情報に対し、訴訟、調停、その他民事手続き上での開示が可能である。

2.5.5　利用者の要求による情報開示

当時刻認証局は、利用者により当時刻認証局にすでに開示された情報への開示を当該利用者から求められた場合、その要求者がその情報を開示した本人かどうかを確認する手続きを経た上で、要求者への当該情報の開示を行う。

2.6 知的財産権

本規定は当社の知的財産の一部を構成するものであり、商標法、著作権法、その他知的財産に関する法律で保護されており、一切のライセンス、譲渡、その他の使用許可を認めない。所有者の書面による明示の許可が無ければ、当社の知的財産の使用は明示的に禁止する。また以下の各号に定めるものに関する権利は当社に帰属し、利用者を含むその他の者には移転しない。

（１）TST の取得、検証を行うためのソフトウェア

（２）商標、標章、標識及びその他のマーク

2.7 個人情報の扱い

当時刻認証局は、利用者から提供される個人情報を、本サービスを提供する為に必要な範囲内でのみこれを使用するとともに、不正な手段による個人情報の取得は行わないものとする。また、当時刻認証局は、業務上必要な期間を経過した後は、個人情報の廃棄、又はその他の処理を行う。

当時刻認証局は、個人情報への不正アクセス、個人情報の紛失、改ざん、漏洩、その他の危険に対し合理的な安全保護措置を講じる。個人情報の取扱いを第三者に委託する場合は、当該委託先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。

なお、利用者が自己の情報の開示を求める場合もしくはその開示結果に誤った情報があり訂正、削除を求める場合には、利用者は当時刻認証局にその旨書面もしくは口頭により申し出ることができる。当時刻認証局は本人確認を実施した上で、原則２週間を目処に情報の開示もしくは訂正、削除を行う。

個人情報に関する開示・訂正・削除、及び個人情報の利用、提供の拒否に関する事項についての問い合わせは、以下のとおり当社のホームページで受け付ける。

URL　http://www.tkc.jp/inquiry/privacy_policy

3.　本人確認と認証

当時刻認証局は、「2.5.5 利用者の要求による情報開示」の規定に基づき当時刻認証局が本人確認手続きを行う必要のある場合を除き、本人確認又は認証は行わない。

4.　運用要件

4.1　タイムスタンプトークンの発行

当時刻認証局は、利用者の要求に応じて当時刻認証局にて時刻情報を付与し、改ざんを検知する為の電子署名データを発行する。また、当時刻認証局は、「4.8.2 タイムスタンプユニットの時刻精度」を満たさないタイムスタンプトークンの発行を防止する処置を講ずる。

4.2　タイムスタンプの検証

タイムスタンプを検証する為には、タイムスタンプの対象となったデータのハッシュ値との照合及び、タイムスタンプトークンに施された電子署名の検証が必要となるが、それらは利用者の環境にて行われるものであり、当時刻認証局にて実施するものではない。

4.3　監査

4.3.1　監査情報の定義

監査情報とは、以下の各号に掲げる、本規定、利用規約、技術情報、安全対策実施状況、システム操作、作業記録、システムイベント、時刻配信局から発行された時刻監査の記録等

の監査を行う為に必要な情報をいう。
（１）TAA からの時刻監査月次レポート
（２）本サービス利用契約の発効、本サービスの利用開始から本サービスの利用停止までのプロセスにおける全記録
（３）本サービス設備設置場所への入退室記録および承認記録
（４）システムに対する操作記録
（５）システムの動作記録

4.3.2　監査人の身元、資格

監査人は、当社の内部監査を担当する部門に属する役社員で本規定の「4.3.1　監査情報の定義」に定めた監査情報を取り扱う業務に精通した者から選任する。当時刻認証局の責任者は、必要に応じて外部の監査人を任命する。

4.3.3　監査人と被監査部門との関係

監査人は当時刻認証局の運用部門に属さない者とし、当時刻認証局内で独立した地位を有するものとする。

4.3.4　監査内容

監査人は、以下の各号に掲げる内容について監査を実施する。
（１）TAA からの時刻監査月次レポート
　　時刻監査月次レポートの保管状況：　手順書に基づき安全に保管されていること
（２）本サービス利用契約の発効、本サービスの利用開始から本サービスの利用停止までのプロセスにおける全記録
　　記録の保管状況：　プロセスにおける全ての記録が保存されていること
（３）本サービスの設備への入退室記録および承認記録
　　入退室の記録：　サーバルームへの入退室記録が保管されていること
（４）システムに対する操作記録
　　操作記録：　システムに対する変更操作、顧客データへのアクセス記録が保管されていること
（５）システムの動作記録
　　動作記録：　システムの動作状況の記録が保管されていること
（６）認定機関が定めた認定審査基準を満たしていること。

4.3.5　監査周期

監査の頻度は原則年１度行う。

4.3.6　監査情報の保管期間

監査情報は永久保管する。

4.3.7　監査指摘事項への対応

監査指摘事項に対しては当時刻認証局の責任者が判断し、場合により本サービスの運用を停止する事もある。当時刻認証局の責任者は指摘事項の改善作業の確認を行う。

4.3.8　監査情報の保護

当時刻認証局による監査情報及び監査結果の保存の為には、不正なアクセスによる情報の変更、改ざん、削除、漏洩等が無いよう適切かつ合理的な安全対策を講ずる。

4.3.9　監査情報の保管

監査情報は、そのアクセス権限を明確にし、不正アクセスによる情報の変更、改ざん、削除、漏洩等から保護され、必要に応じ適正な期間内に提供可能な状態で保管される。また、監査情報は適正な間隔でバックアップを取る。

4.3.10　監査結果の開示と対処

監査実施後、当時刻認証局は関係機関の要求に応じて監査結果を速やかに開示するものとし、監査の結果として欠陥が指摘された場合には以下の対処を行う。

（１）欠陥が修正されるまでの対処（例えば運用の停止、利用者に対する十分なアナウンス等）

（２）欠陥への対処

（３）再発防止対策

4.4　記録のアーカイブ化

4.4.1　アーカイブデータの種類

当時刻認証局のアーカイブデータは次のものとする。

（１）時刻配信局から発行された時刻監査記録

（２）当時刻認証局で使用する鍵ペアの生成・更新破棄・失効記録

（３）監査情報及び監査報告書

4.4.2　アーカイブデータの保管期間

アーカイブデータは永久保管する。

4.4.3　アーカイブデータの保護

アーカイブデータにはアクセス制御を施すとともに、改ざん検出を可能とする措置を

講ずる。アーカイブデータのバックアップは、定期的に外部記憶媒体に取得し、適切な入退室管理が行われている室内に設置された施錠可能な場所に保管する。

4.4.4　アーカイブデータのバックアップ

アーカイブデータは、所定の方法、手順によりバックアップを行う。

4.4.5　記録へのタイムスタンプ要件

記録に時刻情報を付与するコンピュータのシステム時計は、UTC と同期させる。

4.4.6　アーカイブデータの収集システム

規定しない。

4.5　鍵の定期更新

TST の生成に関わる鍵ペアは１年１ヶ月以内に１度定期的に更新を行い、定期更新時期以前に更新する場合は、利用者に対して事前に通知する。

4.6　システムのトラブル、災害からの復旧

（１）当時刻認証局の使用するタイムスタンプシステムの時刻精度が、本規定の「4.8.2　タイムスタンプユニットの時刻精度」に規定する範囲外になった場合はシステムトラブルとみなし、TSU を緊急停止し速やかに復旧作業を行う。当時刻認証局は、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。

（２）当時刻認証局の災害等により当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運用を行う。

（３）システムのトラブルや災害などにより、サービスに支障を来たす事態が生じた場合には、速やかに利用者及び認証局に通知する。

（４）当時刻認証局は、障害発生時等、予期できない場合の緊急停止措置を除き、サービスを停止する際は、そのスケジュールと手続きを決め、事前に利用者へ通知する。

4.7　業務の終了

当時刻認証局がサービスを終了する際は、そのスケジュールと手続きを決め、終了日の４ヶ月前までに利用者に通知する。また、その内容をホームページ上に公知する。

4.8　タイムソースの管理・トレーサビリティ

4.8.1　当時刻認証局内の時刻精度

当時刻認証局は、当時刻認証局内で稼動する全システムの時刻の精度を、NTA に対して１

秒以内に維持する。

4.8.2　タイムスタンプユニットの時刻精度

当時刻認証局は、当時刻認証局の使用する TSU の時刻精度を、NTA に対して１秒以内に維持する。

4.8.3　時刻のトレーサビリティ

当時刻認証局は、当時刻認証局が運営・管理する TSU に対する時刻監査記録を TAA から取得・保管する事により、TST の時刻の UTC に対するトレーサビリティを保持する。

4.9 暗号アルゴリズムの危殆化対応

（１）危殆化が予測される場合

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 TST の有効期間内に予測される事態になった場合、必要に応じて当該タイムスタンプの発行停止予定日、TSA 公開鍵証明書の失効予定日および、タイムスタンプ更新によりその有効性が維持できることを関係者へ周知･報告し､新たな暗号アルゴリズムのサービスに移行する。

（２）危殆化した場合

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、必要に応じてタイムスタンプの発行を停止し、TSA 公開鍵証明書の失効手続きを行うとともに、新たな暗号アルゴリズムのサービスへの移行を関係者へ周知・報告する。

5.　物理的、手続き的及び要員的なセキュリティ管理

5.1　物理的なセキュリティ管理

5.1.1　施設の場所と建物構造

本サービスを運用するにあたって必要な設備は、地震、火災、水害などの災害対策設計された施設内の施錠された区画内に設置する。

5.1.2　入退室管理と機器へのアクセス

本規定の「5.1.1 施設の場所と建物構造」で規定された施設には、事前に申請・登録が必要であり、施設の監視員と対面確認が必要である。施設内の施錠された区画には、機械による身体的特徴検査を受け、本人であることが確認できた者のみ入室出来る。退室時も同様の確認を行う。事前に登録の無い者は予め当時刻認証局の責任者によって任命された担当責任者より承認を受け、所定の手続きを行った後事前に登録され入室を許可された者と同伴で入室する。

5.1.3　電源、空調設備

本規定の「5.1.1　施設の場所と建物構造」で規定された施設の一次電源は電力会社より複数系統から供給を受け、瞬断にはＵＰＳ設備が機能する。停電時は自家発電装置により電力供給を受ける。発電機用燃料備蓄があり、外部からの供給を受けなくても約 72 時間連続で電力供給出来る。空調設備は冗長構成で運転され、設備機器に最適な温度に保たれる。

5.1.4　水害対策

本規定の「5.1.1　施設の場所と建物構造」で規定された施設は防水対策が施され常時監視される。

5.1.5　火災対策

本規定の「5.1.1　施設の場所と建物構造」で規定された施設は耐火構造になっており、各階も防火区画化される。また窒素ガスなどによる消火設備がある。

5.1.6　地震対策

本規定の「5.1.1　施設の場所と建物構造」で規定された施設は免震又は耐震対策が施されている。機器はラックに固定し、ラックは倒れないようにアンカーで床に固定する。

5.1.7　媒体管理

システムやデータをバックアップした記憶媒体は、空調とセキュリティが管理された場所に厳重に保管され、所定の手続きに基づき搬入出管理される。

5.1.8　廃棄物処理

機密扱いとみなす情報を含むＣＤ、ＤＶＤ等の記憶媒体の廃棄については、厳密な分類の後適切に処理される。特に情報の格納に使用した全ての媒体は、破壊してから破棄処分する。また、機器類は、所定の手続きにより破棄処分する。

5.1.9　外部バックアップ

バックアップ媒体を遠隔地で管理する時は、厳重な管理の元移動し空調とセキュリティが管理された場所に厳重に保管する。

5.2　手続きの管理

5.2.1　信頼される役割

当時刻認証局の責任者より承認された各オペレータのシステムアクセスは、その業務遂行上実行しなければならない行為に限定され、当時刻認証局の責任者はオペレータを兼務する事はできない。

5.2.2　人員配置

当時刻認証局の責任者は、業務に支障が出ない範囲内で人員配置を必要最小限にする。

5.2.3　各役割の認証と認可

全てのオペレータは、所定の手続きにより同一性を証明しシステムへのアクセスを許可される。

5.3　要員的なセキュリティ管理

5.3.1　従事者の要件

業務に従事する者については、人事情報により適格性の確認を行った後任命される。

5.3.2　経歴検査

当時刻認証局は、業務に従事する者について任命する前に信頼性、適格性を確認する為の調査を行う。

5.3.3　トレーニング要件

当時刻認証局は、運用に必要な知識取得の為要員に対しトレーニングを行う。

5.3.4　トレーニング周期

当時刻認証局は、要員に対するトレーニングを計画に基づき実施する。

5.3.5　ジョブローテーションの実施

当時刻認証局は、要員のジョブローテーションを必要に応じて行う。

5.3.6　不正行為の罰則

要員が、規定された権限より逸脱して違反を行った場合は、就業規則、契約等に基づき処分を行う。

5.3.7　要員へ提示する文書

当時刻認証局は、それぞれの職務に必要な文書を提示する。

運用規定、機器類のマニュアル、各種手順書等。

6　技術的管理

6.1　鍵ペア生成とインストール

6.1.1　鍵ペア生成

当時刻認証局による鍵ペアの生成は、鍵管理モジュールにおいて複数人管理の下で行う。

6.1.2　タイムスタンプトークンの公開鍵証明書の配布

TST に使用される公開鍵証明書はリポジトリにて公開される。

6.1.3　鍵長

TST の署名生成鍵には、RSA 2048 bit 以上の鍵を使用する。

6.1.4　鍵生成

TST に関わる鍵ペアの生成は、本規定の「6.2.1　暗号モジュールの基準」で定められたハードウェアで行う。

6.1.5　鍵使用の目的

当時刻認証局は、TST の発行に必要な署名の為に鍵を用いる。

6.2　秘密鍵の防護

6.2.1　暗号モジュールの基準

TSU の秘密鍵は、FIPS 140-2 Level 3 相当の HSM により保護する。

6.2.2　秘密鍵の複数人管理

TSU の秘密鍵の生成、破棄を行う際は、複数の鍵管理者の下で行う。生成、破棄の方法と手順については所定の手続きに従う。

6.2.3　秘密鍵の預託

当時刻認証局は秘密鍵の預託を行わない。

6.2.4　秘密鍵のバックアップ

当時刻認証局は、TSU の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

当時刻認証局は、TSU の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格納

TSU の秘密鍵は、暗号モジュール内で生成され格納される。

6.2.7　秘密鍵活性化方法

暗号モジュール内の秘密鍵の活性化は、複数の鍵管理者の下により所定の操作で行う。

6.2.8　秘密鍵破棄方法

暗号モジュール内の秘密鍵の破棄は、複数の鍵管理者の下により所定の操作で行う。尚、暗号モジュールを破棄目的等で室外に持ち出す場合には、複数の鍵管理者の下で所定の手続きに従い破棄を実施する。

6.3　その他の鍵管理について

6.3.1　公開鍵記録保存

TST 検証用の公開鍵は、本規定の「4.4.2　アーカイブデータの保管期間」において定める期間、保管する。

6.3.2　秘密鍵の使用期間

秘密鍵の使用期間は１年１ヶ月以内とし、鍵ペアを生成し活性化した日から起算して１年１ヶ月以内に鍵更新を行う。また、鍵の危殆化が判明した場合には、その時点で公開鍵証明書の失効手続きを行う。

6.3.3　鍵ペアの有効期間

TST に使用する鍵ペアの有効期間は公開鍵証明書の有効期間と同一で、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する。ただし、秘密鍵の危殆化や、ハッシュ及び暗号アルゴリズムの脆弱化が発生した場合には、TST に示される有効期限より以前に、その有効性を失効させる事がある。

6.4　活性化データ

6.4.1　活性化データの生成

当時刻認証局は、秘密鍵を格納する暗号モジュールの操作に必要な活性化データを、所定の手続きにより生成する。

6.4.2　活性化データの保護

当時刻認証局は、秘密鍵を格納する暗号モジュールの活性化に必要な情報を安全に管理する。

6.5　コンピュータセキュリティ管理

6.5.1　使用するコンピュータセキュリティの技術要件

当時刻認証局の装置やソフトウェアはセキュリティ条件を満たすものを導入する。

6.5.2　コンピュータセキュリティ評価

本サービスを運用する為に必要な全ての機器類に対して、定期的にセキュリティの脆弱性評価を行い、問題がある場合は対処する。また、機器類に変更があった場合においても同様の手続きを行う。

6.6　システムのライフサイクル管理

6.6.1　システム開発管理

当時刻認証局は、使用されるソフトウェアの開発、修正、変更を品質管理された環境で行う。

6.6.2　システム維持管理

当時刻認証局は、使用される機器及びソフトウェアの維持管理を行い、保守体制を備える。

6.6.3　セキュリティ運用管理

当時刻認証局は、ハードウェアやソフトウェアの導入時に、セキュリティの確認調査を行う。

6.6.4　セキュリティ評価のライフサイクル

当時刻認証局は、定期的にセキュリティの脆弱性評価を行い、問題がある場合は対処する。

6.7　ネットワークセキュリティ管理

当時刻認証局は、システム導入時、運用時、変更時においてネットワークセキュリティが確保されているかどうかの確認を行う。

6.8　暗号化モジュールの管理

当時刻認証局は、暗号モジュールに FIPS 140-2 Level 3 相当の製品を使用する。

7.　仕様の管理

7.1　仕様の変更手順

本規定の仕様は必要に応じて変更する。

7.2　公開と通知の規則

本規定の変更時は、速やかに新しい規定をリポジトリに公開する。

7.3　本規定の承認手順

本規定の変更は、代表取締役社長により承認される。

8. タイムスタンプトークンのプロファイル

フィールド	内容	値
TimeStampToken		
ContentInfo		
ContentType	content (データ) の型	id-signedData (OID:1.2.840.113549.1.7.2)
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	sha256 (OID:2.16.840.1.101.3.4.2.1) ※1 sha384 (OID:2.16.840.1.101.3.4.2.2) ※1 sha512 (OID:2.16.840.1.101.3.4.2.3) ※1
encapContentInfo		
eContentType	署名の対象となるデータの型	id-smime-ct -TSTInfo (OID:1.2.840.113549.1.9.16.1.4)
eContent	署名の対象となるデータ	TSTInfo (後述参照)
certificates	署名の検証に必要な証明書のリスト	※OPTIOANAL
certificate	TSAの公開鍵証明書	
attrCert	TAの時刻監査証明書	
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	sha256 sha384 sha512 ※1
signedAttrs	署名の属性	
Attribute		
attrType	属性のタイプ	ContentType (OID:1.2.840.113549.1.9.3)
AttributeValue	属性の値	id-smime-ct-TSTInfo (OID:1.2.840.113549.1.9.16.1.4)
Attribute		
attrType	属性のタイプ	messageDigest (OID:1.2.840.113549.1.9.4)
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	id-aa-signingCertificate (OID:1.2.840.113549.1.9.16.2.12)
AttributeValue	属性の値	
SigningCertificate	証明書署名	ESSCertID certHash:sha1
signatureAlgorithm	署名に使用するアルゴリズム	sha256WithRSAEncryption (OID:1.2.840.113549.1.1.11) ※1 sha384WithRSAEncryption (OID:1.2.840.113549.1.1.12) ※1 sha512WithRSAEncryption (OID:1.2.840.113549.1.1.13) ※1
signature	署名値	
TSTInfo		
version	タイムスタンプトークン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	OID:0.2.440.200312.100.100.100
messageImprint		
hashAlgorithm	ハッシュアルゴリズム	sha256,sha384,sha512
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[.sss]Z
accuracy	時刻精度	msec
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

※1 各ダイジェストアルゴリズムは、TSTInfo中のハッシュアルゴリズムと同一のものが適用されます。

用語集 A

用語	スペル	解説
FIPS 140-2	Federal Information Processing Standard 140-2	米国 NIST が策定した暗号モジュールに関するセキュリティ認定基準。最低レベル１から最高レベル 4 まである。
HSM	Hardware Security Module	ハードウエアセキュリティモジュール。物理的に暗号モジュール等の機密性を保護する装置。分解したり、衝撃を加えたりすると装置内のデータが消失する仕掛けになっているものや、温度変化や気圧の変化を検出するものもある。
UPS	Uninterruptible power supply	様々な電源トラブルを取り除き、サーバ・ネットワーク機器等のシステム全体にクリーンかつ 高品質の電源供給を行い、貴重なデータの消失を防止する為の装置。
UTC	Coordinated Universal Time	協定世界時。現在全世界で公式に採用されている原子時系。UTC は実時間では生成出来ず、各国の国家時刻標準機関が生成する協定世界時を基に国際相互比較し、後日それらのデータを集計し計算により決定される。
公開鍵暗号基盤	Public Key Infrastructure	公開鍵暗号技術と電子署名を使って、インターネットで安全な通信が出来るようにする為の環境の事。
時刻監査		対象となる装置の時刻を監視し、標準時とのズレを検査する事。
時刻同期		基準となる時刻に対象装置の時刻を合わせる事。
身体的特徴		本人認証では、虹彩、手のひらの血流、指紋、声紋などが用いられる。

用語集 B

用語	スペル	解説
タイムスタンプ	Time Stamp	信頼の置ける時刻と文書などのデジタル情報に対し、変更、改ざんがあったかどうかを検知出来る情報もしくはそれを指し示す情報を付与し、それ以降、内容や時刻に変更・改ざんがあったかどうかを証明する技術。
当時刻認証局	Time-Stamping Authority	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。
タイムスタンプトークン	Time-Stamp Token	信頼の置ける時刻と文書などのデジタル情報に対し、変更、改ざんがあったかどうかを検知出来る情報。もしくはそれを指し示す情報。デジタル情報のハッシュデ

		ータに時刻情報等を付与し、電子署名として発行する。TST には独立トークンとリンクトークンの二種類が存在し、それぞれ ISO/IEC18014-2,3 に規定されている。
タイムソース	Time Source	時刻源の事を言う。
トレーサビリティ	Traceability	トレーサビリティとは、「不確かさが全て表記された、切れ目の無い比較の連鎖を通じて、通常は国家標準又は国際標準である決められた標準に関連づけられ得る測定結果又は 標準の性質」を言う。 VIM（国際計量基本用語集）より抜粋
リポジトリ	Repository	ここでは本規定などの情報を保存・配布出来るようにしたオンライン上のデータベースの事。