



アマノタイムスタンプ局運用規程

Version 1.01

2004年1月



アマノ株式会社

目次

1. はじめに.....	6
1.1 概要.....	6
1.1.1 本規程の位置づけ（定義）.....	6
1.2 本規程の識別.....	7
1.3 コミュニティーと適用性.....	7
1.3.1 適用範囲と対象.....	7
1.3.2 関係者.....	7
1.3.3 タイムスタンプサービスの概要.....	8
1.4 本規程に関する連絡先の詳細.....	8
2. 一般規定.....	8
2.1 義務.....	8
2.1.1 タイムスタンプ局の義務.....	8
2.1.2 サービス利用者の義務.....	8
2.2 責任.....	9
2.2.1 タイムスタンプ局の責任.....	9
2.2.2 利用者の責任.....	9
2.2.3 財務的な責任.....	9
2.3 免責事項.....	9
2.4 解釈と執行.....	9
2.4.1 準拠法.....	9
2.4.2 可分性.....	10
2.4.3 存続性.....	10
2.4.4 承継.....	10
2.4.5 通知.....	10
2.4.6 紛争解決の手続き.....	10
2.4.7 不可抗力.....	10
2.4.8 解釈.....	10
2.4.9 権利放棄の禁止.....	11
2.5 料金.....	11
2.6 公表とリポジトリ.....	11
2.6.1 タイムスタンプ局に関する情報の公開.....	11
2.6.2 公開の時期.....	11
2.6.3 アクセス制御.....	11

2.6.4	タイムスタンプ局のリポジトリ	11
2.7	守秘性のポリシー	11
2.7.1	機密扱いとみなす情報	11
2.7.2	機密扱いとみなさない情報	11
2.7.3	法執行機関への情報開示	12
2.7.4	民事手続き上の情報開示	12
2.7.5	利用者の要求による情報開示	12
2.7.6	その他の理由に基づく情報開示	12
2.8	知的財産権	12
2.9	個人情報の扱い	13
3.	本人確認と認証	13
4.	運用要件	13
4.1	タイムスタンプの発行	13
4.2	タイムスタンプの検証	13
4.3	監査	13
4.3.1	監査情報の定義	13
4.3.2	監査人の身元、資格	14
4.3.3	監査人と被監査部門との関係	14
4.3.4	監査周期	14
4.3.5	監査情報の保管期間	14
4.3.6	監査指摘事項への対応	14
4.3.7	監査情報の保護	14
4.3.8	監査情報の保管	14
4.3.9	監査結果の開示と対処	14
4.4	記録のアーカイブ化	15
4.4.1	アーカイブデータの種類	15
4.4.2	アーカイブデータの保管期間	15
4.4.3	アーカイブデータの保護	15
4.4.4	アーカイブデータのバックアップ	15
4.4.5	記録へのタイムスタンプ要件	15
4.4.6	アーカイブデータの収集システム	15
4.5	鍵の定期更新	15
4.6	システムのトラブル、危殆化、災害からの復旧	15
4.7	業務の終了	16
4.8	タイムソースの管理・トレーサビリティ	16

4.8.1	タイムスタンプ局内の時刻精度.....	16
4.8.2	タイムスタンプサーバの時刻精度.....	16
4.8.3	時刻のトレーサビリティ.....	16
5.	物理的、手続き的及び要員のセキュリティ管理.....	16
5.1	物理的なセキュリティ管理.....	16
5.1.1	施設の場所と建物構造.....	16
5.1.2	入退室管理と機器へのアクセス.....	16
5.1.3	電源、空調設備.....	16
5.1.4	水害対策.....	17
5.1.5	火災対策.....	17
5.1.6	地震対策.....	17
5.1.7	媒体管理.....	17
5.1.8	廃棄物処理.....	17
5.1.9	外部バックアップ.....	17
5.2	手続きの管理.....	17
5.2.1	信頼される役割.....	17
5.2.2	人員配置.....	17
5.2.3	各役割の認証と認可.....	18
5.3	要員のセキュリティ管理.....	18
5.3.1	従事者の要件.....	18
5.3.2	経歴検査.....	18
5.3.3	トレーニング要件.....	18
5.3.4	トレーニング周期.....	18
5.3.5	ジョブローテーションの実施.....	18
5.3.6	不正行為の罰則.....	18
5.3.7	要員へ提示する文書.....	18
6	技術的管理.....	18
6.1	鍵ペア生成とインストール.....	18
6.1.1	鍵ペア生成.....	18
6.1.2	タイムスタンプトークンの署名検証用公開鍵の配布.....	19
6.1.3	鍵長.....	19
6.1.4	鍵生成.....	19
6.1.5	鍵使用の目的.....	19
6.2	秘密鍵の防護.....	19
6.2.1	暗号モジュールの基準.....	19

6.2.2	秘密鍵の複数人管理.....	19
6.2.3	秘密鍵の預託.....	19
6.2.4	秘密鍵のバックアップ.....	19
6.2.5	秘密鍵のアーカイブ.....	19
6.2.6	暗号モジュールへの秘密鍵格納.....	19
6.2.7	秘密鍵活性化方法.....	20
6.2.8	秘密鍵非活性化方法.....	20
6.2.9	秘密鍵破棄方法.....	20
6.3	その他の鍵管理について.....	20
6.3.1	署名検証公開鍵記録保存.....	20
6.3.2	署名生成秘密鍵の使用期間.....	20
6.3.3	署名検証公開鍵の有効期間.....	20
6.4	活性化データ.....	20
6.4.1	活性化データの生成.....	20
6.4.2	活性化データの保護.....	20
6.5	コンピュータセキュリティ管理.....	21
6.5.1	使用するコンピュータセキュリティの技術要件.....	21
6.5.2	コンピュータセキュリティ評価.....	21
6.6	システムのライフサイクル管理.....	21
6.6.1	システム開発管理.....	21
6.6.2	セキュリティ運用管理.....	21
6.6.3	セキュリティ評価のライフサイクル.....	21
6.7	ネットワークセキュリティ管理.....	21
6.8	暗号化モジュールの管理.....	21
7.	仕様の管理.....	21
7.1	仕様の変更手順.....	21
7.2	公開と通知の規則.....	21
7.3	本規定の承認手順.....	22
	用語集 A.....	23
	用語集 B.....	24
	参考文献.....	24

改版履歴

初版発行日：2003年6月18日

版	変更日	内容
Ver1.01	2004.1.1	タイムソースに関する記述を変更

1. はじめに

アマノ株式会社は、電子データの信頼性の補強を目的としてアマノ時刻認証サービスを広く利用者に提供していく。アマノ時刻認証サービスには、国家時刻標準機関に追跡可能な信頼のおける時刻を維持、配信する民間の時刻標準機関として提供する標準時配信・認証サービスと、タイムスタンプ局として電子データに信頼のおける時刻のタイムスタンプを付与する「アマノデジタルタイムスタンプサービス」がある。アマノタイムスタンプ局運用規程（以下「本規程」と言う）では、アマノ株式会社が信頼のおける第三者機関として運営する「アマノタイムスタンプ局」が「アマノデジタルタイムスタンプサービス」を利用者に提供する為の運営方針を述べる。

尚、本規程の構成は、IETF PKIX による RFC2527「Certificate Policy and Certification Practices Statement Framework」を参考としている。

1.1 概要

デジタルタイムスタンプは、ある電子データの「存在証明」や「非改ざん証明」を行う場合に非常に有効な手法である。アマノデジタルタイムスタンプサービス（以下「タイムスタンプサービス」と言う）は、信頼のおけるタイムソースと公開鍵暗号技術を用いた高度な仕組みを採用し、利用者にとって簡単、安価、迅速に利用出来るものとして提供する。

しかしながらこの有効性を確保するには以下の条件が必要である。

(1) 利用するタイムソースが信頼のおけるものである事。

ここで信頼がおけるとは国家時刻標準機関との追跡性が確保されている事を言う。

(2) タイムソース及びデジタルタイムスタンプの生成、検証に関わる設備の信頼性や安全対策の確保。

(3) 署名生成鍵、検証鍵の管理に代表される運用管理体制の信頼性の確保。

(4) タイムスタンプ方式自体が持つ信頼性と強度の確保。

(5) 運営主体及び利用者の義務と責任の遂行。

本規程は、上記の一連の信頼の鎖を途切れる事無く確保する為に、重要な要件に関して可能な限り明確化し、実行する事を文書化するとともに公開するアマノタイムスタンプ局（以下「タイムスタンプ局」と言う）の宣言書である。

1.1.1 本規程の位置づけ（定義）

本規程は、タイムスタンプ局及びそれが提供するタイムスタンプサービスの運用方針について定めたものである。タイムスタンプ局並びにタイムスタンプサービスの業務に携わる社員及び協働者はこれに従い業務を遂行しなければならない。

1.2 本規程の識別

名称：アマノタイムスタンプ局運用規程

バージョン：1.01

作成日：2004年1月1日

作成者：アマノ株式会社

1.3 コミュニティと適用性

1.3.1 適用範囲と対象

本規程の適用範囲はタイムスタンプ局及びタイムスタンプサービスの運用、その情報を扱う業務全般である。また本規程の適用対象はタイムスタンプ局並びにタイムスタンプサービスの全ての利用者、及びタイムスタンプサービスに関係する法人、個人、組織を含む。

1.3.2 関係者

(1) タイムスタンプ局

本規程においてタイムスタンプ局とは、公開鍵暗号技術によるタイムスタンプトークン発行業務を行い、アマノ株式会社（以下「アマノ」と言う）によって運営されているものを言う。

(2) 社員

本規程において社員とは、アマノの社員及び囑託者の事を言う。

(3) 申請者

本規程において申請者とは、タイムスタンプ局の提供するサービスへの加入申請を行った者の事を言う。

(4) 利用者

本規程において利用者とは、タイムスタンプ局の提供するサービスへの加入申請を行いタイムスタンプ局からサービスへの加入を認められ、そのサービスを受ける対象装置を所有、管理、又は使用する者の事を言う。あるいは加入申請が必要で無いサービスの場合は、アマノデジタルタイムスタンプサービス利用規約（以下「利用規約」と言う）及びソフトウェア使用許諾契約書（以下「使用許諾」と言う）に同意して利用する者の事を言う。

(5) 協働者

本規程において協働者とは、アマノと雇用関係を持たず、契約等によって定められた範囲においてタイムスタンプ局の業務を支援する者の事を言う。

(6) 第三者

本規程において第三者とは、タイムスタンプ局、社員、協働者以外の個人、法人の事を言う。

1.3.3 タイムスタンプサービスの概要

タイムスタンプサービスとは、アマノがタイムスタンプクライアントソフトウェアの登録ユーザに対し、タイムスタンプ局への要求に応じてタイムスタンプトークンを発行し PDF ファイルに埋め込むサービス、及び埋め込まれたタイムスタンプの有効性の検証を行うサービスの事を言い、タイムスタンプを埋め込んだ文書の内容には一切関与しない。

1.4 本規程に関する連絡先の詳細

名称：アマノ株式会社 e-timing オペレーションセンター

所在地：〒222-0011 神奈川県横浜市港北区菊名7丁目3番24号

e-mail アドレス：etpost@e-timing.ne.jp

2. 一般規定

2.1 義務

2.1.1 タイムスタンプ局の義務

- (1) タイムスタンプ局は、タイムスタンプ局及びタイムスタンプサービスの信頼性と安全性の確保を行う。
- (2) タイムスタンプ局は、本規程に従い、タイムスタンプサービスとして、タイムスタンプの発行、検証サービスを提供する。
- (3) タイムスタンプ局は、タイムスタンプサービス利用申請に対し、当該申請者がタイムスタンプサービスを利用出来るか審査し決定する。
- (4) タイムスタンプ局は、本規程に従いタイムスタンプ局で使用する署名生成鍵、署名検証鍵を安全に生成し管理する。
- (5) タイムスタンプ局は、署名生成鍵、署名検証鍵を定期的に更新する。万一危殆化が判明した場合は鍵の更新を行うとともにサービス利用者へ通知を行う。
- (6) タイムスタンプ局は、サービス利用者の義務について周知させるとともにその履行に必要な各種情報を必要に応じて提供する。

2.1.2 サービス利用者の義務

- (1) 利用者は、本規程、利用規約及び使用許諾に了承した上でタイムスタンプサービスの提供を受けるものとする。
- (2) 利用者は、サービス利用の申請などに際し正確な情報をタイムスタンプ局に提示するものとする。

(3) 利用者は、タイムスタンプサービスの利用に際し利用者側で使用するソフトウェア、機器類に対しては自己の責任と判断の下に利用し安全対策などの一切の必要な管理を行う。

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、運営を維持しかつその義務を履行する為に必要な財政的基盤を有するものとする。

2.2.2 利用者の責任

利用者は、タイムスタンプを検証した第三者に対し、本規程の「2.1.2 サービス利用者の義務」で定められた内容に反してタイムスタンプサービスを利用した事から発生する全ての責任を負う。ただし、これは、本規程で定める利用者の他の責任及び義務を制限するものではない。

2.2.3 財務的な責任

アマノは、本規程の「2.2.1 タイムスタンプ局の責任」に違反して損害賠償責任を負う場合、利用規約に従うものとし、いかなる場合においてもアマノはこの賠償額の上限を超える責任を負うものではない。利用者が本規程に定める義務を履行せず、又は本規程の「2.2.2 利用者の責任」で定める責任に違反した事によりアマノが損害を被った場合、アマノは利用者に対し当該損害の賠償を請求する事が出来る。

2.3 免責事項

アマノは、利用者がタイムスタンプサービス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は免責される。アマノは、アマノの責任に帰する事が出来ない事由から生じた損害、及び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免責される。その他の免責事項及び賠償責任の限定については利用規約及び使用許諾に従うものとする。

2.4 解釈と執行

2.4.1 準拠法

当事者間の契約又は他の法規選択にかかわらず、本規程の適用、構成、解釈、妥当性等は、日本法に準拠する。

2.4.2 可分性

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

2.4.3 存続性

本規程の「2.2.3 財務的な責任」、「2.3 免責事項」、「2.4 解釈と執行」、「2.7 守秘性のポリシー」、「2.8 知的財産権」及び「2.9 個人情報の扱い」は、タイムスタンプ局によるタイムスタンプサービスが終了し、本規程の廃止後も有効に存続する。

2.4.4 承継

本規程は、明示、黙示、表見上に関わらず、双方当事者の承継者、遺言執行者、相続人、代表者、管理者及び譲受人の利益となり、また拘束する。

2.4.5 通知

本規程に関する通知は書面、又は電子メールにて本規程の「1.4 本規程に関する連絡先の詳細」にある連絡先で受け付ける。通常は受領日をもってその通知は有効となるが、当該通知に受領日以降の日付がある場合にはこの限りでは無い。タイムスタンプ局から利用者に対し通知が必要と判断される場合には、登録されている通知先へ行う。

2.4.6 紛争解決の手続き

本規程又はそれに付随して生じた紛争、タイムスタンプ局によるタイムスタンプサービスに関する紛争について法廷での解決を図る際、東京地方裁判所が第一審の専属的合意管轄裁判所となる。

2.4.7 不可抗力

アマノは、天災、戦争、伝染病、停電、火災、地震、テロ、その他の災害など、アマノの支配を超える事件から生じた本規程に関する違反、遅滞、不履行に、一切責任を負わない。

2.4.8 解釈

特に他の規定が無ければ、本規程はあらゆる状況の下で商業的な妥当性と合理性を失う事の無いように解釈すべきものとする。本規程を解釈するにあたっては、国際的な視野や目的、その目的で一貫性を押し進める利益、誠実な履行を考慮する。

2.4.9 権利放棄の禁止

本規程の違反に関してのアマノ又は利用者の権利放棄は書面によって行うが、いかなる場合もその後生じる規程違反に関しての権利放棄やその規定そのものの権利放棄と解釈してはならない。

2.5 料金

タイムスタンプサービスの料金表に定める。

2.6 公表とリポジトリ

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、本規程をタイムスタンプ局のリポジトリに公開する。

2.6.2 公開の時期

タイムスタンプ局は、本規程変更時、その他タイムスタンプ局の責任者が必要と判断した時に随時更新を行う。

2.6.3 アクセス制御

タイムスタンプ局のリポジトリには、インターネットでアクセス出来る。特にアクセスの制御は行わない。

2.6.4 タイムスタンプ局のリポジトリ

本規程は下記の URL におけるタイムスタンプ局のリポジトリで参照出来る。

URL <http://www.e-timing.ne.jp/repository>

2.7 守秘性のポリシー

2.7.1 機密扱いとみなす情報

タイムスタンプ局及び利用者は、その情報が漏えいする事によってタイムスタンプ局、及び利用者の信頼性、適格性が損なわれる恐れのある情報を機密扱いとする。タイムスタンプ局により機密扱いとみなされた情報は、タイムスタンプ局により安全に保管、管理される。タイムスタンプ局により機密扱いとみなされた情報は、本規程又は利用規約に定められている場合を除いては、いかなる者にも原則開示しない。

2.7.2 機密扱いとみなさない情報

「2.7.1 機密扱いとみなす情報」の規定に関わらず、タイムスタンプ局は次に定める情報については機密扱いとはみなさない。

(1) 本規程等公開情報として明示するもの。

- (2) 利用者又はタイムスタンプ局に開示後、タイムスタンプ局の責任の範囲外で公知となった情報。
- (3) 合法的に入手し、かつ利用者又は第三者から機密保持の義務を負っていない情報。
- (4) 利用者又はタイムスタンプ局が第三者に対し機密保持の義務を課す事無く開示した情報。
- (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出来なくした統計目的で編集したデータ。

2.7.3 法執行機関への情報開示

タイムスタンプ局は、タイムスタンプ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。

2.7.4 民事手続き上の情報開示

タイムスタンプ局は、タイムスタンプ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。

2.7.5 利用者の要求による情報開示

タイムスタンプ局は、利用者によりタイムスタンプ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。

2.7.6 その他の理由に基づく情報開示

規定しない。

2.8 知的財産権

本規程はアマノ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、アマノ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タイムスタンプ局に帰属し、利用者を含むその他の者には移転しない。

- (1) タイムスタンプ局が発行するタイムスタンプトークン
- (2) 検証ソフトウェア
- (3) 商標、標章、標識及びその他のマーク

2.9 個人情報の扱い

タイムスタンプ局は、タイムスタンプサービスの加入申請時に利用者が提供した個人情報に対し、タイムスタンプ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。また不正な手段による個人情報の取得は行わない。また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。

タイムスタンプ局は、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。

3. 本人確認と認証

タイムスタンプ局は、「2.7.5 利用者の要求による情報開示」の規程に基づきタイムスタンプ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 タイムスタンプの発行

タイムスタンプ局は、利用者の要求に応じてタイムスタンプ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、PDF ファイルに埋め込む。タイムスタンプ局が運営するタイムサーバ及びタイムスタンプサーバは、不慮の事故による停止及び本規程の「4.8.2 タイムスタンプサーバの時刻精度」に定めた時刻精度以下にならないように最大限の努力をする。

4.2 タイムスタンプの検証

(1) タイムスタンプの検証は、タイムスタンプ局にて行われる検証とクライアントが保持している署名検証鍵での検証の二種類がある。タイムスタンプ局での検証を行う場合はインターネット通信環境が必要となる。

(2) タイムスタンプ検証用の署名検証鍵は定期的に更新される。

4.3 監査

4.3.1 監査情報の定義

監査情報とは、本規程、利用規約、使用許諾、技術情報、安全対策実施状況、システムイベントの記録等の監査を行う為に必要な情報を言う。

4.3.2 監査人の身元、資格

監査人は、アマノの従業員で本規程の「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出し、タイムスタンプ局の責任者が任命する。タイムスタンプ局は、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

監査人はタイムスタンプ局運用部門に属さない者とし、タイムスタンプ局内で独立した地位を有するものとする。

4.3.4 監査周期

監査の頻度は最低年1度行う。

4.3.5 監査情報の保管期間

監査情報は10年以上保管する。

4.3.6 監査指摘事項への対応

監査指摘事項に対してはタイムスタンプ局の責任者が判断し、場合によりタイムスタンプサービスの運用を停止する事もある。タイムスタンプ局の責任者は指摘事項の改善作業の確認を行う。

4.3.7 監査情報の保護

タイムスタンプ局による監査情報及び監査結果の保存の為に、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。

4.3.8 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。

4.3.9 監査結果の開示と対処

監査実施後、タイムスタンプ局は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。

- ・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)
- ・欠陥への対処
- ・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

タイムスタンプ局のアーカイブデータは次のものとする。

- ・タイムスタンプ局の UTC との同期水準に関する国家時刻標準機関との時刻比較記録。
- ・タイムスタンプサービス利用料金請求の為のタイムスタンプトークン発行記録。

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10年以上保管する。

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、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

タイムスタンプ局で保有する暗号化鍵は1年に1度定期的に更新する。

4.6 システムのトラブル、危殆化、災害からの復旧

- (1) タイムスタンプ局の使用するタイムスタンプシステムの時刻精度が、本規程の「4.8.2 タイムスタンプサーバの時刻精度」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、タイムスタンプサーバを緊急停止し速やかに復旧作業を行う。タイムスタンプ局は、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) タイムスタンプ局の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。

4.7 業務の終了

タイムスタンプ局がサービスを中断、終了する際は、そのスケジュールと手続きを決め、その内容をホームページ上に公知する。また、障害発生時などの予期出来ない場合の緊急停止措置以外は、事前の通知なしには業務を中断しない。

4.8 タイムソースの管理・トレーサビリティ

4.8.1 タイムスタンプ局内の時刻精度

タイムスタンプ局は、タイムスタンプ局内で稼動する全システムの時刻の精度を、UTC に対して 1 秒以内に維持する。

4.8.2 タイムスタンプサーバの時刻精度

タイムスタンプ局は、タイムスタンプ局の使用するタイムスタンプサーバの時刻精度を、UTC に対して 1 0 0 ミリ秒以内に維持する。

4.8.3 時刻のトレーサビリティ

タイムスタンプ局は、国家時刻標準機関との時刻比較記録を公開・保管する事により、タイムスタンプ局が取り扱う時刻の UTC に対するトレーサビリティを保持する。

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

タイムスタンプ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

本規程の「5.1.1 施設の場所と建物構造」で規定された施設に入館する者は事前に登録が必要である。さらに施設の監視員と対面確認が必要であり機械による身体的特徴検査を受け、本人である事が確認出来た者のみ許可され入館出来る。退室時も同様の確認を行う。事前に登録の無い者は予めタイムスタンプ局の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館を許可された者と同伴で入館する。

5.1.3 電源、空調設備

本規程の「5.1.1 施設の場所と建物構造」で規定された施設の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 2 0 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

本規程の「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

本規程の「5.1.1 施設の場所と建物構造」で規定された施設は耐火構造になっており、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

本規程の「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。機器はキャビネットに固定し、キャビネット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書類、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。

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

タイムスタンプ局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る。

5.2.2 人員配置

タイムスタンプ局責任者は、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

タイムスタンプ局は、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

タイムスタンプ局は、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

タイムスタンプ局は、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

タイムスタンプ局は、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

タイムスタンプ局は、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、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

タイムスタンプ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署名検証用公開鍵の配布

タイムスタンプトークンの署名検証用公開鍵は、アマノがタイムスタンプ検証機能を有したソフトウェアに実装して配布するか、もしくは専用ホームページから契約ユーザへ安全な方法により配布される。

6.1.3 鍵長

タイムスタンプトークンの署名生成鍵には、RSA 1024 bit 以上の鍵を使用する。

6.1.4 鍵生成

タイムスタンプトークンの署名生成鍵の生成は、本規程の「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

タイムスタンプ局は、タイムスタンプトークンの署名、及びタイムスタンプトークン発行時と検証時の暗号化通信に鍵を用いる。

6.2 秘密鍵の防護

6.2.1 暗号モジュールの基準

タイムスタンプサーバの秘密鍵は、FIPS 140-2 Level 3 以上の HSM により保護する。

6.2.2 秘密鍵の複数人管理

タイムスタンプサーバの秘密鍵の生成、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

タイムスタンプ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

タイムスタンプ局は、タイムスタンプサーバの秘密鍵のバックアップを複数の鍵管理者の下で行う。その方法と手順については所定の手続きに従う。

6.2.5 秘密鍵のアーカイブ

タイムスタンプ局は、タイムスタンプサーバ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

タイムスタンプサーバの秘密鍵は、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

タイムスタンプサーバの秘密鍵は、定められた鍵管理者により暗号モジュールにICカードを挿入及びPIN 入力して活性化する。

6.2.8 秘密鍵非活性化方法

タイムスタンプサーバの秘密鍵は、定められた鍵管理者により暗号モジュールにICカードを挿入及びPIN 入力して非活性化する。

6.2.9 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で暗号モジュールを初期化する事によって行われる。尚、初期化した暗号モジュールを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する。

6.3 その他の鍵管理について

6.3.1 署名検証公開鍵記録保存

署名検証公開鍵は、タイムスタンプ検証ソフトウェアのアーカイブに含まれ、本規程の「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 署名生成秘密鍵の使用期間

署名生成秘密鍵の使用期間は1年とし、鍵ペアを生成し活性化した日から起算して1年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、その時点で鍵更新を行う。

6.3.3 署名検証公開鍵の有効期間

署名検証公開鍵の有効期間は7年とする。ただしここで規定する有効期間はタイムスタンプの検証操作を制限するものではない。

6.4 活性化データ

6.4.1 活性化データの生成

タイムスタンプ局は、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

タイムスタンプ局は、秘密鍵を格納する暗号モジュールの活性化に必要なPINなどの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

タイムスタンプ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

タイムスタンプ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

タイムスタンプ局は、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 セキュリティ運用管理

タイムスタンプ局は、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。

6.6.3 セキュリティ評価のライフサイクル

タイムスタンプ局は、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

タイムスタンプ局は、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

タイムスタンプ局は、暗号モジュールに FIPS 140-2 Level 3 認定品を使用する。

7. 仕様の管理

7.1 仕様の変更手順

本規程の仕様は必要に応じて変更する。

7.2 公開と通知の規則

本規程の変更時は、速やかに新しい規程をリポジトリに公開する。

7.3 本規定の承認手順

本規程の変更は、タイムスタンプ局の責任者により承認される。

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までである。
HSM	Hardware Security Module	ハードウェ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。
IETF	Internet Engineering Task Force	インターネットで使用されるプロトコルを決定する為の民間主導の標準化団体。IETF から RFC 番号がつけられて公表された規格は、実質的に世界標準規格である。
NIST	National Institute of Standards and Technology	米国立標準技術研究所
PDF ファイル	Portable Document Format	Adobe 社により作られ公表されている、電子的文書を扱うフォーマットに基づいて作成されたファイルの事。
PIN	Personal Identification Number	個人認識番号。
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。
時刻認証		対象となる装置の時刻が標準時に対して一定の誤差の範囲内にある事を証明する事。
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。
タイムスタンプ局	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。タイムスタンプトークン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。
トレサビリティ	Traceability	トレサビリティとは、「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	ここでは本規程などの情報を保存・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。

参考文献

- ・ IETF PKIX RFC2527 「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」
- ・ 政府認証基盤 (G P K I) 「府省認証局 C P / C P S ガイドライン」
- ・ タイムビジネス推進協議会 「時刻認証基盤ガイドライン」
- ・ ECom 「認証局運用ガイドライン」