



**AMANO Time Distribution and Audit Service**

**Type-Free-A**

**運用規程 (TP/TPS)**

**Version 1.01**

**2010年5月12日**

アマノタイムビジネス株式会社

Copyright (C) AMANO Time Business Corporation, All Rights Reserved.

## 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 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 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 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 TA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 TA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.....	9
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 .....	10
2.5 料金.....	10
2.6 公表とリポジトリ .....	11
2.6.1 TA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	時刻配信局のリポジトリ .....	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 .....	11
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 .....	12
3.	本人確認と認証 .....	12
4.	運用要件 .....	13
4.1	時刻監査証の発行 .....	13
4.2	時刻監査証の検証 .....	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 .....	13
4.3.3	監査人と被監査部門との関係 .....	13
4.3.4	監査周期 .....	13
4.3.5	監査情報の保管期間 .....	13
4.3.6	監査指摘事項への対応 .....	13
4.3.7	監査情報の保護 .....	13
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 .....	14
4.4.1	アーカイブデータの種類 .....	14
4.4.2	アーカイブデータの保管期間 .....	14
4.4.3	アーカイブデータの保護 .....	14
4.4.4	アーカイブデータのバックアップ .....	14
4.4.5	記録へのタイムスタンプ要件 .....	14
4.4.6	アーカイブデータの収集システム .....	14
4.5	鍵の定期更新 .....	15
4.6	システムのトラブル、災害からの復旧 .....	15
4.7	業務の終了 .....	15

4.8	タイムソースの管理・トレーサビリティ .....	15
4.8.1	TA内の時刻精度 .....	15
4.8.2	タイムサーバの時刻精度 .....	15
4.8.3	時刻のトレーサビリティ .....	15
5.	物理的、手続き的及び要員的なセキュリティ管理 .....	15
5.1	物理的なセキュリティ管理 .....	15
5.1.1	施設の場所と建物構造 .....	15
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 .....	16
5.1.5	火災対策 .....	16
5.1.6	地震対策 .....	16
5.1.7	媒体管理 .....	16
5.1.8	廃棄物処理 .....	16
5.1.9	外部バックアップ .....	16
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 .....	17
5.3	要員的なセキュリティ管理 .....	17
5.3.1	従事者の要件 .....	17
5.3.2	経歴検査 .....	17
5.3.3	トレーニング要件 .....	17
5.3.4	トレーニング周期 .....	17
5.3.5	ジョブローテーションの実施 .....	17
5.3.6	不正行為の罰則 .....	17
5.3.7	要員へ提示する文書 .....	17
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	時刻監査証の公開鍵証明書の配布 .....	18
6.1.3	鍵長 .....	18
6.1.4	鍵生成 .....	18
6.1.5	鍵使用の目的 .....	18
6.2	秘密鍵の防護 .....	18

6.2.1	暗号モジュールの基準 .....	18
6.2.2	秘密鍵の複数人管理 .....	18
6.2.3	秘密鍵の預託 .....	18
6.2.4	秘密鍵のバックアップ .....	18
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 .....	19
6.2.8	秘密鍵非活性化方法 .....	19
6.2.9	秘密鍵破棄方法 .....	19
6.3	その他の鍵管理について .....	19
6.3.1	公開鍵記録保存 .....	19
6.3.2	秘密鍵の使用期間 .....	19
6.3.3	鍵ペアの有効期間 .....	19
6.4	活性化データ .....	19
6.4.1	活性化データの生成 .....	19
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 .....	20
6.5.1	使用するコンピュータセキュリティの技術要件 .....	20
6.5.2	コンピュータセキュリティ評価 .....	20
6.6	システムのライフサイクル管理 .....	20
6.6.1	システム開発管理 .....	20
6.6.2	システム維持管理 .....	20
6.6.3	セキュリティ運用管理 .....	20
6.6.4	セキュリティ評価のライフサイクル .....	20
6.7	ネットワークセキュリティ管理 .....	20
6.8	暗号化モジュールの管理 .....	20
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 .....	21
8.	時刻監査証明書のプロファイル .....	22
	用語集A .....	24
	用語集B .....	24

改版履歴

初版発行日：2006年8月23日

版	変更日	内容
Ver 1.01	2010/05/12	1. 「1.1.1」、「1.2.1」、「1.2.2」 サービス名称 誤記修正 2. 「1.4 所在地」 住所変更

## 1. はじめに

AMANO Time Distribution and Audit Service Type-Free-A は、国家時刻標準機関に追跡可能な信頼のおける時刻の維持・配信および監査を行う民間の時刻配信局（以下「TA」と言う）として提供する時刻配信・監査サービス（以下「本サービス」と言う）であり、AMANO Time Distribution and Audit Service Type-Free-A 運用規程（以下「本規程」と言う）では、アマノタイムビジネス株式会社（以下「アマノタイムビジネス」と言う）が本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

本サービスを運用する TA（以下「本 TA」と言う）は、UTC（協定世界時）にトレーサブルな原子時計を運用管理しており、その原子時計の時刻を用いて本サービスを提供する。本 TA は契約利用者の管理、運用するタイムスタンプユニットに対して、定期的に時刻を配信すると同時に時刻監査を行い、その結果を反映した電子的な証明書を発行する。

本規程は、本サービスの信頼性を維持する為に、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本 TA の宣言書である。

なお、本 TA は、標準時配信ポリシー及び時刻配信局運用規程をそれぞれ独立したものとせず、本規程を本 TA の運用方針として位置づける。

#### 1.1.1 本規程の位置づけ（定義）

本規程は、本 TA 及びそれが提供する本サービス「AMANO Time Distribution and Audit Service Type-Free-A」の運用方針について定めたものである。本 TA 並びに本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 識別

### 1.2.1 ドキュメント名称、バージョン

名称：AMANO Time Distribution and Audit Service Type-Free-A 運用規程

バージョン：1.01

作成日：2010年5月12日

作成者：アマノタイムビジネス株式会社

### 1.2.2 オブジェクト識別子

内容	OID
本サービス	
アマノタイムビジネス株式会社	0.2.440.200217

	AMANO Time Distribution and Audit Service Type-Free-A	0.2.440.200217.100.100
	サービスポリシー	0.2.440.200217.100.100.100
本サービスにおいて使用される認証局		
	AMANO RootCA for TA/TSA	0.2.440.200217.100.10
本サービスにおいて使用される時刻源の比較対象		
	独立行政法人情報通信研究機構（NICT）が NTA（国家時刻標準機関）として公開している時刻比較データ公開ポリシー	0.2.440.200168.1.1.1

### 1.3 コミュニティーと適用性

#### 1.3.1 適用範囲と対象

本規程の適用範囲は、本 TA 及び、本サービスの運用、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、本 TA 並びに本サービスの全ての利用者、及び本サービスに関する法人、個人、組織を含む。

#### 1.3.2 関係者

##### (1) 時刻配信局（TA）

本規程において時刻配信局とは、UTC に対してトレーサビリティのある時刻の配信を行い、かつタイムスタンプ局が管理する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。本規程において時刻配信局とは、本 TA のことを言う。

##### (2) 国家時刻標準機関（NTA）

本規程において国家時刻標準機関とは、TA が管理・運用する時計の比較校正元となる時計を管理・運用する機関を言い、本サービスにおける国家時刻標準機関は独立行政法人情報通信研究機構とする。

##### (3) 認証局（CA）

本規程において認証局とは、時刻配信局が発行する時刻監査証に使われる公開鍵証明書の認証を行う事業者をいう。本サービスにおける認証局は AMANO RootCA for TA/TSA とする。

##### (4) タイムスタンプ局（TSA）

本規程においてタイムスタンプ局（以下「TSA」と言う）とは、時刻配信局から時刻の配信と監査を受け、タイムスタンプトークンを発行する事業者を言う。

##### (5) 社員

本規程において社員とは、アマノタイムビジネスの社員及び嘱託者の事を言う。

##### (6) 利用者

本規程において利用者とは、本サービスに加入した上で利用する者の事を言う。

##### (7) 協働者

本規程において協働者とは、アマノタイムビジネス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時刻配信局の業務を支援する者の事を言う。

#### (8) 第三者

本規程において第三者とは、時刻配信局、社員、協働者以外の個人、法人の事を言う。

### 1.3.3 サービスの概要

本サービスでは、利用者が申請したタイムスタンプユニットに対して時刻の配信と監査を行うと同時に、その時刻監査結果を示す時刻監査証明書を、タイムスタンプユニットに対して発行する。

<タイムスタンプユニット>

- (1) 時刻の配信と監査の頻度は1日に1回以上とする。
- (2) 時刻の配信と監査を行う時刻はアマノタイムビジネスが定める。
- (3) 時刻監査を行った時点のタイムスタンプユニットの時刻オフセットが1秒以内であった場合、その時点から25時間有効な時刻監査証明書を発行する。

### 1.4 本規程に関する連絡先の詳細

名称：アマノタイムビジネス株式会社

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 フォーム：<https://www.e-timing.ne.jp/inquiry/general/formmail.html>

## 2. 一般規定

### 2.1 義務

#### 2.1.1 TAの義務

- (1) 本TAは、本TA及び本サービスの信頼性と安全性の確保を行う。
- (2) 本TAは、本規程に従い、本サービスとして時刻監査証を発行する。
- (3) 本TAは、本規程に従い、本TAで使用する秘密鍵、公開鍵を安全に生成し管理する。
- (4) 本TAは、秘密鍵、公開鍵を定期的に更新する。万一危殆化が判明した場合は、その鍵を使った時刻監査証明書の発行を中止し、認証局への連絡及び公開鍵証明書の失効手続きを行うとともにサービス利用者へ通知を行う。
- (5) 本TA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、本規程及び利用規約に了承した上で本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本TAに提示するものとする。
- (3) 利用者は、本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 TA の責任

本 TA 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、時刻監査証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本サービスを利用した事から発生する全ての責任を負う。但し、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

アマノタイムビジネスは、本規程の「2.2.1 時刻配信局の責任」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タイムビジネス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タイムビジネスが損害を被った場合、アマノタイムビジネス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

アマノタイムビジネスは、利用者が本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。アマノタイムビジネスは、アマノタイムビジネス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、本TAによる本サービスが終了し、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。本TA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、本TA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、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

アマノタイムビジネスは、天災、戦争、伝染病、停電、火災、地震、テロ、その他の災害など、アマノタイムビジネス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タイムビジネス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

規定しない。

## 2.6 公表とリポジトリ

### 2.6.1 TAに関する情報の公開

本TAは、本規程をリポジトリに公開する。

### 2.6.2 公開の時期

本TAは、本規程変更時、その他本TA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

本TA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 時刻配信局のリポジトリ

本規程は、下記のURLにおける本TAのリポジトリで参照出来る。

URL : [https://www.e-timing.ne.jp/repository/ta/tfa\\_repository.html](https://www.e-timing.ne.jp/repository/ta/tfa_repository.html)

## 2.7 守秘性のポリシー

### 2.7.1 機密扱いとみなす情報

本TA及び利用者は、その情報が漏えいする事によって本TA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。本TAにより機密扱いとみなされた情報は、本TAにより安全に保管、管理され、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、本TA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) 利用者又は本TAに開示後、本TA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) 利用者又は本TA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

本TAは、本TA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

本TAは、本TA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

本TAは、利用者により本TA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、アマノタイムビジネス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、アマノタイムビジネス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本TAに帰属し、利用者を含むその他の者には移転しない。

- (1) 商標、標章、標識及びその他のマーク

### 2.9 個人情報の扱い

本TAは、本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、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。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。本TA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

時刻配信局は、「2.7.5 利用者の要求による情報開示」の規程に基づき時刻配信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 時刻監査証の発行

本 TA は、予め規定した頻度で利用者のタイムスタンプユニットに対して時刻の配信を行うと同時に時刻監査を行い、その結果を反映した時刻監査証をタイムスタンプユニットに対して発行する。時刻監査証には、本 TA の電子署名が施される。本 TA が運営するタイムサーバは、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 時刻監査証の検証

時刻監査証を検証する為には、時刻監査証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、本 TA 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、本規程、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、アマノタイムビジネスもしくはアマノ株式会社の従業員であり、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、本 TA の責任者が任命する。本 TA 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、本 TA の運用部門に属さない者とする。

#### 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、本 TA 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。本 TA 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

本 TA 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。

#### 4.3.9 監査結果の開示と対処

監査実施後、本 TA 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

本 TA のアーカイブデータは次、のものとする。

- ・本 TA 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。
- ・利用者の管理するタイムスタンプユニットに対する時刻監査記録。

#### 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

時刻監査証を生成に関わる鍵ペアは、2年に1度定期的に更新する。

#### 4.6 システムのトラブル、災害からの復旧

- (1) 本 TA の使用する時刻配信・監査システムの時刻精度が、本規程の「4.8.2 タイムサーバの時刻精度」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、タイムサーバを緊急停止し速やかに復旧作業を行う。本 TA 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、速やかに復旧作業を行う。
- (2) 本 TA は、災害等により本 TA の設備が被害を受けた場合は、速やかに復旧作業を行う。
- (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、速やかに認証局及び利用者に通知する。

#### 4.7 業務の終了

本 TA 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 TA 内の時刻精度

本 TA は、本 TA 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 タイムサーバの時刻精度

本 TA は、時刻配信局の使用するタイムサーバの時刻精度を、NTA に対して30ミリ秒以内に維持する。

##### 4.8.3 時刻のトレーサビリティ

本 TA は、国家時刻標準機関が公表している GPS 時刻比較データを使用して本 TA が運営・管理する原子時計と国家時刻標準機関の原子時計との時刻比較を行い、その記録を公開・保管する事によって、本 TA 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

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本 TA 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電源の瞬断には、UPS 設備が機能する。空調設備は常時運転され、設備機器に最適な温度に保たれる。

#### 5.1.4 水害対策

規定しない。

#### 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、火災報知器により火災対策が施されている。

#### 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。

#### 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

規定しない。

## 5.2 手続きの管理

### 5.2.1 信頼される役割

本 TA 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る。本 TA 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

本 TA 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

本 TA 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

本 TA 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

本 TA 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

本 TA 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

本 TA 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

本 TA 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 時刻監査証の公開鍵証明書の配布

時刻監査証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

時刻監査証の秘密鍵、及び TSA との間の暗号化通信に用いる公開鍵暗号の鍵は、RSA 2048bit 以上の鍵を使用する。

#### 6.1.4 鍵生成

時刻監査証に関わる鍵ペアの生成は、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

本 TA は、時刻監査証に対する署名と、TSA との間の暗号化通信の為に、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

タイムサーバの秘密鍵は、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

本 TA 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

本 TA は、タイムサーバ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

本 TA は、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

本 TA 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

本 TA 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 PIN 入力して活性化する。

### 6.2.8 秘密鍵非活性化方法

本 TA 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 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により暗号モジュールの鍵更新操作によって行われる。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

時刻監査証検証用の公開鍵は、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 秘密鍵の使用期間

本 TA の秘密鍵の使用期間は 2 年とし、鍵ペアを生成し活性化した日から起算して 2 年毎に鍵更新を行う。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

時刻監査証に使用する鍵ペアの有効期間は 10 年 1 ヶ月間とする。

## 6.4 活性化データ

### 6.4.1 活性化データの生成

本 TA 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

本 TA 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

本 TA 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

本 TA 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

本 TA 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

本 TA 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

本 TA 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

本 TA 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

本 TA 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、本 TA の責任者により承認される。

## 8. 時刻監査証明書のプロファイル

項目	項目の意味	データ型	設定値
<b>AttributeCertificate</b>			
<b>acinfo</b>		-	
<b>version</b>	時刻監査証明書の、属性証明書としてのバージョン	INTEGER	1
<b>holder</b>	時刻監査証明書の所有者	-	
entityName	時刻監査証明書の所有者名	GeneralNames	
directoryName		-	
countryName	国名		
type	-	OBJECT IDENTIFIER	2.5.4.6
value	-	PrintableString	時刻監査証明書所有者の公開鍵証明書に従う
organizationName	組織名		
type	-	OBJECT IDENTIFIER	2.5.4.10
value	-	PrintableString	時刻監査証明書所有者の公開鍵証明書に従う
organizationalUnitName	部門名		
type	-	OBJECT IDENTIFIER	2.5.4.11
value	-	PrintableString	時刻監査証明書所有者の公開鍵証明書に従う
commonName	固有名称		
type	-	OBJECT IDENTIFIER	2.5.4.3
value	-	PrintableString	時刻監査証明書所有者の公開鍵証明書に従う
objectDigestInfo	オブジェクトのダイジェスト値の情報		
digestedObjectType	データのタイプ	ENUMERATED	1:publicKeyCert
digestAlgorithm	ハッシュアルゴリズムの識別子	-	
algorithm	-	OBJECT IDENTIFIER	1.3.14.3.2.26 (SHA1)
parameters	アルゴリズムの引数	NULL	-
objectDigest	ハッシュ値	BIT STRING	時刻監査証明書所有者の公開鍵証明書のハッシュ値
<b>issuer</b>		-	
issuerName		GeneralNames	
directoryName		-	
countryName	国名		
type	-	OBJECT IDENTIFIER	2.5.4.6
value	-	PrintableString	JP
organizationName	組織名		
type	-	OBJECT IDENTIFIER	2.5.4.10
value	-	PrintableString	AMANO Time Business Corporation
organizationalUnitName	部門名		
type	-	OBJECT IDENTIFIER	2.5.4.11
value	-	PrintableString	AMANO RootCA for
commonName	固有名称		
type	-	OBJECT IDENTIFIER	2.5.4.3
value	-	PrintableString	tsmc-Fxxx
<b>signature</b>	時刻監査証明書への署名に使用されたアルゴリズム	AlgorithmIdentifier	
algorithm	署名アルゴリズムの識別子	OBJECT IDENTIFIER	1.2.840.113549.1.1.5 (SHA1 withRSA)
parameters	アルゴリズムの引数	NULL	-
<b>serialNumber</b>	時刻監査証明書のシリアル番号	INTEGER	-

※次ページに続く

※前ページからの続き

	<b>attrCertValidityPeriod</b>	時刻監査証明書の有効期間	-	
	notBeforeTime	開始日時	GeneralizedTime	-
	notAfterTime	終了日時	GeneralizedTime	-
	<b>attributes</b>		-	
	type	データタイプ	OBJECT IDENTIFIER	1.3.6.1.4.1.601.10.4.1
	values		TimingMetrics	
	ntpTime	時刻監査が行われた時刻	-	
	major	整数部	BigIntegerStr	-
	fractionalSeconds	小数部	BigIntegerStr	-
	offset	上位タイムサーバとの間の時刻オフセット	-	
	major	整数部	BigIntegerStr	-
	fractionalSeconds	小数部	BigIntegerStr	-
	sign	符号	INTEGER OPTIONAL	マイナスの時(-1)がセットされ、それ以外は本項目自体が存在しない
	delay	時刻監査時のネットワーク遅延	-	
	major	整数部	BigIntegerStr	-
	fractionalSeconds	小数部	BigIntegerStr	-
	expiration	時刻監査証明書の有効期間	-	
	major	整数部	BigIntegerStr	-
	fractionalSeconds	小数部	BigIntegerStr	-
	leapEvent	うるう秒設定情報	-	
	leapTime	うるう秒設定日時	-	
	major	整数部	BigIntegerStr	-
	fractionalSeconds	小数部	BigIntegerStr	-
	action	うるう秒の設定方法	INTEGER	挿入の場合(1)、削除の場合(-1)
	type	データタイプ	OBJECT IDENTIFIER	1.3.6.1.4.1.601.10.4.2
	values		TimingPolicy	
	policyID	時刻監査ポリシー識別子	OBJECT IDENTIFIER	0.2.440.200192.100.100.100
	maxOffset	上位タイムサーバとの間の最大時刻オフセット 規定値	-	
	major	整数部	BigIntegerStr	-
	fractionalSeconds	小数部	BigIntegerStr	-
	maxDelay	最大ネットワーク遅延時間の規定値	-	
	major	整数部	BigIntegerStr	-
	fractionalSeconds	小数部	BigIntegerStr	-
	<b>signatureAlgorithm</b>	署名アルゴリズム	AlgorithmIdentifier	
	algorithm	署名アルゴリズムの識別子	OBJECT IDENTIFIER	1.2.840.113549.1.1.5 (SHA1 withRSA)
	parameters	アルゴリズムの引数	NULL	-
	<b>signatureValue</b>	署名値	BIT STRING	

## 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。
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。
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。

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。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。