時刻配信・監査サービス for TSU

運用規程（TP/TPS）

Ver 1.10

２０１７年３月

アマノ株式会社

目次

改版履歴

初版発行日：２００４年１１月２２日

版	変更日	内容
Ver 1.1 （公開前に修正された為、非公開）	2005/2/4	１．時刻監査証明書のプロファイル追記。 ２．時刻源の比較対象となる国家時刻標準機関のサービスポリシーID を追記。 ３．「1.3.3　サービスの概要」を追記。 ４．「4.8.3　時刻のトレーサビリティ」に GPS 時刻比較の記述を追記。 ５．「1.2.2　オブジェクト識別子」を表形式の表現に変更 ６．「6.1　鍵ペア生成とインストール」に、TSA との暗号化通信に用いる鍵についての記述を追記。 ７．「2.1.1　時刻配信局の義務－（５）」に鍵の危殆化発生時の失効処置を追記。 ８．「4.6　システムのトラブル、災害からの復旧」に利用者へ通知する旨を追記。 ９．「1.　はじめに」の記述から本サービスに関連するタイムスタンプサービスの記述を削除、最適化。
Ver1.2	2005/2/22	１．「2.1.1-(5)」の「鍵の失効手続き」という表現を「公開鍵証明書の失効手続き」に最適化。 ２．「6.3.2」のタイプミスを修正：「署ペア」→「秘密鍵」 ３．「6.3.2」の「鍵更新を行う」を「公開鍵証明書の失効手続きを行う」に修正。
Ver1.3	2005/12/06	１．アマノタイムビジネス（株）に運用が委託されてことに伴って「1.4 本規程に関する連絡先の詳細」の会社名を変更。
Ver1.4	2006/10/06	１．「1.2.2」の認証局の名称変更 ２．「1.4」の連絡先住所変更 ３．「2.6.4」リポジトリの URL 変更
Ver1.5	2007/11/22	１．「1.3.2 (3)」の認証局の名称修正 ２．「1.3.3 (3)」時刻オフセットの規定範囲表現を最適化。
Ver1.6	2010/9/27	１．「1.4　本規程に関する連絡先の詳細」の名称を、アマノタイムビジネス（株）からアマノビジネスソリューションズ（株）に変更し、それに伴って所在地も変更 ２．次の箇所の「時刻監査証明書」を「時刻監査証」に修正 「1.3.3 サービスの概要」、「2.1.1 時刻配信局の義務」、「8. 時刻監査証明書のプロファイル」 ３．「2.1.1 時刻配信局の義務」内の、連続でなかった段落番号を修正
Ver1.7	2012/2/19	１．TA 証明書の署名アルゴリズムを SHA1 から SHA-256 に変更したことによる「時刻監査証プロファイル」の変更 ２．改版履歴 Ver1.6 ２．誤記修正「時刻監査証」
Ver1.8	2012/9/19	「4.8.3」時刻比較の公開停止に伴い該当箇所を削除
Ver1.9	2012/12/07	「1.3.3」に「測定精度について」追加

Ver1.10	2017/3/27	１．表紙　AMANO ロゴの削除 ２．全ページ　著作権表示内容の変更 「1.2.2」の情報通信研究機構の法人名称の修正 正：国立研究開発法人 誤：独立行政法人 ３．「８．時刻監査証のプロファイル」の修正 holderとissuerの情報にstateOrProvinceNameと localityNameを追加、organizationalUnitNameに「固有値」 を追加、「leapEvent」項目を削除

1. はじめに

時刻配信・監査サービス for TSU とは、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時刻配信・監査サービス（以下「本サービス」と言う）であり、時刻配信・監査サービス for TSU 運用規程（以下「本規程」と言う）では、アマノ株式会社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

アマノ時刻配信局は、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。アマノ時刻配信局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時刻配信局の宣言書である。

なお、時刻配信局は、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、本規程を時刻配信局の本サービスに関する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、時刻配信局及びそれが提供する「時刻配信・監査サービス for TSU」の運用方針について定めたものである。 時刻配信局並びに時刻配信・監査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：時刻配信・監査サービス for TSU 運用規程

バージョン：１．１０

作成日：２０１７年3月２７日

作成者：アマノ株式会社

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

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
本サービスにおいて使用される時刻源の比較対象		
	国立研究開発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時刻配信局及び、そのサービスの運用、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時刻配信局並びにそのサービスの全ての利用者、及び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）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、かつ時刻認証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、アマノ時刻配信局のことを言う。

（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、時刻配信局が管理・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セコムトラストシステムズ株式会社とする。

（4）時刻認証局（TSA）

本規程において時刻認証局とは、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を、タイムスタンプユニットに対して発行する。

（1） 時刻の配信と監査の頻度は１日に１回以上とする。

（2） 時刻の配信と監査には、測定精度が 50 ミリ秒以内の通信環境と通信手順を用いる。

（3） 時刻の配信と監査を行う時刻はアマノが定める。

（4） 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 NTA に対して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：アマノビジネスソリューションズ株式会社

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 アドレス： etpost@e-timing.ne.jp

2.　一般規定

2.1　義務

2.1.1　時刻配信局の義務

（1）時刻配信局は、時刻配信局及び時刻配信・監査サービスの信頼性と安全性の確保を行う。

（2）時刻配信局は､本規程に従い､時刻配信･監査サービスとして時刻監査証を発行する。

（3） 時刻配信局は、本規程に従い時刻配信局で使用する署名鍵を安全に生成し管理する。

（4）時刻配信局は、署名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）時刻配信局は、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時刻配信・監査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時刻配信局に提示するものとする。

（3）利用者は、時刻配信・監査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 時刻配信局の責任

時刻配信局は、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、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時刻配信・監査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無い。

2.2.3 財務的な責任

アマノは、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はこの賠償額の上限を超える責任を負うものでは無い。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、利用者が時刻配信・監査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りなく、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、時刻配信局による時刻配信・監査サービスが終了し、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。時刻配信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、時刻配信局による時刻配信・監査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に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

時刻配信・監査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　時刻配信局に関する情報の公開

時刻配信局は、本規程を時刻配信局のリポジトリに公開する。

2.6.2　公開の時期

時刻配信局は、本規程変更時、その他時刻配信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

時刻配信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　時刻配信局のリポジトリ

本規程は下記の URL における時刻配信局のリポジトリで参照出来る。

URL　https://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

時刻配信局及び利用者は、その情報が漏えいする事によって時刻配信局、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。時刻配信局により機密扱いとみなされた情報は、時刻配信局により安全に保管、管理される。時刻配信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、時刻配信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）利用者又は時刻配信局に開示後、時刻配信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）利用者又は時刻配信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

時刻配信局は、時刻配信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

時刻配信局は、時刻配信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

時刻配信局は、利用者により時刻配信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時刻配信局に帰属し、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

時刻配信局は、時刻配信・監査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、時刻配信・監査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。

時刻配信局は、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

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

時刻配信局は、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。時刻監査証には時刻配信局の電子署名が施される。時刻配信局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、時刻配信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、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、時刻配信局の責任者が任命する。時刻配信局は、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

監査人は時刻配信局運用部門に属さない者とし、時刻配信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時刻配信局の責任者が判断し、場合により時刻配信・監査サービスの運用を停止する事もある。時刻配信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

時刻配信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。

4.3.8　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、時刻配信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

時刻配信局のアーカイブデータは次のものとする。

・時刻配信局の 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。
・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）時刻配信局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。 時刻配信局は、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）時刻配信局の災害等により時刻配信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、速やかに認証局及び利用者に通知する。

4.7　業務の終了

時刻配信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　時刻配信局内の時刻精度

時刻配信局は、時刻配信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　タイムサーバの時刻精度

時刻配信局は、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

時刻配信局は、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時刻配信局が運営・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、その記録を保管する事によって、時刻配信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

時刻配信・監査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時刻配信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２０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

時刻配信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､時刻配信局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

時刻配信局責任者は、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

時刻配信局は、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

時刻配信局は、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

時刻配信局は、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

時刻配信局は、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

時刻配信局は、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

時刻配信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　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

時刻監査証の署名鍵、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 2048 bit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

時刻配信局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

時刻配信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

時刻配信局は、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

時刻配信局は、タイム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 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 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

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年とする。

6.4　活性化データ

6.4.1　活性化データの生成

時刻配信局は、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

時刻配信局は、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

時刻配信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

時刻配信・監査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

時刻配信局は、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

時刻配信局は、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

時刻配信局は、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

時刻配信局は、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

時刻配信局は、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

時刻配信局は、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、時刻配信局の責任者により承認される。

8. 時刻監査証のプロファイル

項目	項目の意味	データ型	設定値
AttributeCertificate			
acinfo		–	
version	時刻監査証の、属性証明書としてのバージョン	INTEGER	1
holder	時刻監査証の所有者	–	
entityName	時刻監査証の所有者名	GeneralNames	
directoryName		–	
countryName	国名		
type	–	OBJECT IDENTIFIER	2.5.4.6
value	–	PrintableString	時刻監査証所有者の公開鍵証明書に従う
stateOrProvinceName	都道府県名		
type	–	OBJECT IDENTIFIER	2.5.4.8
value	–	PrintableString	時刻監査証所有者の公開鍵証明書に従う
localityName	市区町村名		
type	–	OBJECT IDENTIFIER	2.5.4.7
value	–	PrintableString	時刻監査証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	時刻監査証所有者の公開鍵証明書に従う
organizationalUnitName	固有値		
type	–	OBJECT IDENTIFIER	2.5.4.11
value	–	PrintableString	時刻監査証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	時刻監査証所有者の公開鍵証明書のハッシュ値

※前ページからの続き

項目	項目の意味	データ型	設定値
issuer		−	
issuerName		GeneralNames	
directoryName		−	
countryName	国名		
type	−	OBJECT IDENTIFIER	2.5.4.6
value	−	PrintableString	JP
stateOrProvinceName	都道府県名		
type	−	OBJECT IDENTIFIER	2.5.4.8
value	−	PrintableString	Kanagawa
localityName	市区町村名		
type	−	OBJECT IDENTIFIER	2.5.4.7
value	−	PrintableString	Yokohama
organizationName	組織名		
type	−	OBJECT IDENTIFIER	2.5.4.10
value	−	PrintableString	AMANO Corporation
organizationalUnitName	部門名		
type	−	OBJECT IDENTIFIER	2.5.4.11
value	−	PrintableString	e-timing TA
organizationalUnitName	固有値		
type	−	OBJECT IDENTIFIER	2.5.4.11
value	−	PrintableString	nCipher NTS ESN:xxxx-xxxx-xxxx ※xxxx-xxxx-xxxxはタイムサーバの機器固有番号
commonName	固有名称		
type	−	OBJECT IDENTIFIER	2.5.4.3
value	−	PrintableString	tsmc-xxx ※xxxはタイムサーバの管理番号
signature	時刻監査証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	1.2.840.113549.1.1.11 (SHA-256 withRSA)
parameters	アルゴリズムの引数	NULL	−
serialNumber	時刻監査証のシリアル番号	INTEGER	−

※前ページからの続き

項目	項目の意味	データ型	設定値
attrCertValidityPeriod	時刻監査証の有効期間	–	
notBeforeTime	開始日時	GeneralizedTime	–
notAfterTime	終了日時	GeneralizedTime	–
attributes		–	
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	時刻監査証の有効期間	–	
major	整数部	BigIntegerStr	–
fractionalSeconds	小数部	BigIntegerStr	–
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	–
signatureAlgorithm	署名アルゴリズム	AlgorithmIdentifier	
algorithm	署名アルゴリズムの識別子	OBJECT IDENTIFIER	1.2.840.113549.1.1.11 (SHA-256 withRSA)
parameters	アルゴリズムの引数	NULL	–
signatureValue	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。
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。

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（ＧＰＫＩ）「府省認証局ＣＰ／ＣＰＳ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」