クロノトラスト時刻配信サービス運用規程

Ver.　2．0

2005 年　3月　1日

セイコーインスツル株式会社

改定履歴

版	変更日付	変更内容	承認者
1．0	2002年7月1日	初版設定	クロノトラスト 時刻認証局代表者
1．1	2002年11月19日	公開版設定	クロノトラスト 時刻認証局代表者
1．2	2003年9月1日	リポジトリのURL、時刻監査証明書のプロファイル、その他実質的な影響のない変更	クロノトラスト 時刻認証局代表者
1．3	2004年9月1日	社名変更および時刻監査証明書のプロファイルに関する説明・用語解説の修正	クロノトラスト 時刻認証局代表者
2．0	2005年3月1日	GPS-CV方式による時刻比較方式の採用、サービス名称の変更、説明・用語解説の修正	クロノトラスト 時刻配信局代表者

All rights reserved. Copyright©2005,Seiko Instruments Inc.

目 次

All rights reserved. Copyright©2005,Seiko Instruments Inc.

All rights reserved. Copyright©2005,Seiko Instruments Inc.

All rights reserved. Copyright©2005,Seiko Instruments Inc.

All rights reserved. Copyright©2005,Seiko Instruments Inc.

１． はじめに

本規程では、セイコーインスツル株式会社が運営するクロノトラスト時刻配信局がクロノトラスト時刻配信サービスを提供するにあたっての基本的事項について述べる。

本規程の構成は、IETF PKIX による RFC 2527「Certificate Policy and Certification Practices Statement Framework 」を参考としている。

１．１ 概要

あるデジタル情報の存在日時を証明したい場合に、信頼できる第三者機関に PKI の技術に基づくタイムスタンプを実施してもらうことは、そのデジタル情報の存在日時を証明する有効な方法である。このようなタイムスタンプに使用する時刻の時刻ソースは厳正で信頼できるものである必要がある。クロノトラスト時刻配信局はタイムスタンプを行う事業者などに対して、厳正で信頼できる時刻ソースとしてクロノトラスト時刻配信サービスを提供する。

クロノトラスト時刻配信局はUTC（NICT）との時刻比較により精度を確保した原子時計を有しており、その原子時計から生成される時刻を元にクロノトラスト時刻配信サービスを提供する。クロノトラスト時刻配信局が時刻配信を行った際に、時刻配信サービスの加入者に時刻に関する属性証明書を発行する。この属性証明書は、時刻配信サービスの加入者が運用する時刻がクロノトラスト時刻配信局の定めた基準に適合していたことを証明するものである。なお、本規程では、時刻に関する属性証明書のことを時刻監査証明書と呼ぶ。

タイムスタンプ事業者がクロノトラスト時刻配信局からサービスを受けるためには、本規程の内容を理解したうえで、本規程に準拠してタイムスタンプトークンの発行業務を行う必要がある。

クロノトラスト時刻配信局は、本規定（クロノトラスト時刻配信サービス運用規定）をクロノトラスト時刻配信業務に関する運営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	:クロノトラスト時刻配信サービス運用規程
バージョン	:２．０
作成日	:2005 年3月１日
作成者	:セイコーインスツル株式会社

All rights reserved. Copyright©2005,Seiko Instruments Inc.

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。

・セイコーインスツル株式会社　　：　0.2.440.200125
・クロノトラスト時刻配信サービス　　：　0.2.440.200125.1.2
・時刻監査証明書ポリシー　　：　0.2.440.200125.1.2.1
・クロノトラスト時刻配信局が参照する UTC(NICT)との時刻比較データ
　時刻比較データ（GPS-CV データ）　　：　0.2.440.200168.1.1.1

１．３ コミュニティと適用範囲

１．３．１ 時刻配信の関係者

（1）時刻配信局

時刻配信局は、サービスの加入者が申請したタイムスタンプユニット等の装置（以下、「対象装置」という）にUTC（NICT）に同期した時刻の配信を行い、その対象装置が運用している時刻を監査するサービスを行う。

本規程において時刻配信局とは、クロノトラスト時刻配信局のことをいう。

（以下、単に時刻配信局と記載した場合は、クロノトラスト時刻配信局のことをいう。）

（2）タイムスタンプ局

本規程においてタイムスタンプ局（TSA）とは、時刻配信局から時刻の配信と監査を受け、PKI の技術に基づくタイムスタンプトークンを発行する事業者をいう。

（3）証明書認証局

PKI の認証局（CA）であり、本規程においては時刻配信局の時刻配信サーバ、または、サービス加入者の対象装置が使用する PKI の公開鍵証明書の認証局とする。

（4）国家時刻標準機関（NTA）

本規定における国家時刻標準機関（NTA）とは、標準時を生成・維持・配信する機関であり、現在日本では NICT（独立行政法人情報通信研究機構）が独立行政法人情報通信研究機構法に基づいて、時刻比較データ（GPS-CV データ）を公開した国家時刻標準局国家時刻標準配信サービスを実施している。

※時刻比較データ（GPS-CV データ）

国家時刻標準機関である NICT が Web 上で公開する GPS コモンビュー方式（以下 GPS-CV という）による計測データ。NICT が規定した GPS-CV スケジュールに基づく時刻比較データを Web 上で公開することにより、UTC(NICT)と時刻配信局との正確な時刻比較データの計測が可能となる。

（5）加入者

本規程において加入者とは、下記の者のことをいう。

時刻配信局の提供するサービスへの加入申込みを行い、時刻配信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又は管理、あるいは使用する者とする。

１．３．２ 時刻配信サービスの内容

クロノトラスト時刻配信サービス（以下、「本サービス」という）の内容は以下のとおりとする。

（1） 時刻配信局の管理する時刻配信サーバは、本サービスの対象となる加入者が申請した

All rights reserved. Copyright©2005,Seiko Instruments Inc.

対象装置に対して時刻の配信を行い、かつ対象装置がタイムスタンプに使用する時刻の監査を実施する。

イ） 時刻の監査および配信の頻度は1日に1回以上とする。

ロ） 時刻の監査および配信を実施する時刻は時刻配信局が定める。

ハ） 時刻の監査および配信は1台以上の時刻配信サーバによって実施される。

(2) 時刻配信サーバは、対象装置に対して実施した時刻の監査結果を表す時刻監査証明書を、時刻に関する属性証明書の形式で対象装置に対して発行する。

イ） 監査した時点の対象装置の時刻誤差が加入者の申請した監査規格の範囲内であった場合、時刻配信局の時刻配信サーバは対象装置に対して有効期間が 25 時間の時刻監査証明書を発行する。

ロ） 対象装置は時刻監査証明書を受け取った時点から次の時刻監査証明書を受け取るか、もしくは受け取った時刻監査証明書の有効期間が終了するまでの間、受け取った時刻監査証明書に基づくタイムスタンプトークンを対象装置内で生成し、発行する事が許可される。

ハ） 対象装置は、自身の生成するタイムスタンプトークンに時刻監査証明書を包含して発行することが許可される。

１．３．３ 配信された時刻と時刻監査証明書の利用制限

(1)適正な用途

時刻監査証明書は、時刻配信局より加入者に対して配信された時刻を用いた業務を所定の期間行うことを許可する目的で発行される。対象装置がタイムスタンプユニットの場合は、タイムスタンプユニットの時刻ソースや、タイムスタンプユニットが時刻監査を受けたときの時刻誤差を明示する目的で、時刻監査証明書を該当するタイムスタンプトークンに包含することができる。それ以外の目的で配信された時刻および時刻監査証明書を使用してはならない。

(2)禁止される用途

人間の生命や身体に危害が及ぶ可能性がある用途への適用を禁止する。 たとえば、核施設関連での設備制御や航空機・列車等の運行制御、直接生命にかかわる医療装置などへの適用は禁止する。

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、書面もしくは電子メールで受け付ける。

窓口　セイコーインスツル株式会社
クロノトラスト情報センタ
所在地　郵便番号 261-8507
千葉県千葉市美浜区中瀬1－8
電子メール　chronotrust_info@sii.co.jp

All rights reserved. Copyright©2005,Seiko Instruments Inc.

２．一般規定

２．１ 義務

２．１．１ 時刻配信局の義務

時刻配信局は、本サービスの提供にあたって善良なる管理者の注意義務をもって以下の業務を遂行する義務を負う。

(1) 本規程に基づいて対象装置に対して時刻の配信および監査を行う。

(2) 本規程に基づいて対象装置に対して時刻監査証明書の発行を行う。

(3) 時刻配信業務に使用する時刻を４．１０に規定する精度で管理する。

(4) 時刻配信業務に使用するすべての秘密鍵を安全に生成し、管理する。

(5) 時刻配信業務に使用する時刻配信サーバの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加入者に通知する。

(6) 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本規程２．７．６および４．６．２で規定する期間保管する。

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) 情報届出義務

加入申込者は本サービスへの加入申込みにあたり、時刻配信局が必要とする情報を正しく届け出なければならない。

加入者は本サービスを受けるにあたり必要な情報を、時刻配信局の要求に従い、届け出なければならない。本情報には、本サービスを利用するために必要な公開鍵証明書やルートCAの証明書が含まれるものとする。届出事項に変更が生じるときや鍵を更新したときは、速やかに時刻配信局へ届け出なければならない。

(2) 配信された時刻と時刻監査証明書等の利用制限の遵守

配信された時刻と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と時刻監査証明書等を利用しなければならない。

(3) 時刻及び機器の管理義務

加入者は時刻配信局より配信された時刻や時刻監査証明書を変更・改ざんをしてはならない。対象装置を不当に分解・改造・解析等してはならない。対象装置の機能・性能が維持できるように対象装置を適正に管理しなければならない。適正な管理には、対象装置の周囲温度を18℃から28℃に維持し、かつ24時間あたりの温度変動を±3℃以内に維持すること、および時刻配信局の指定するバージョンのソフトウエアをインストールすることが含まれる。

(4) セキュリティ確保の義務

加入者は、時刻配信局の時刻配信サーバと対象装置間の通信のセキュリティが保たれるように、加入者側の通信経路のセキュリティを確保しなければならない。外部及び内部からの脅威（時刻の改ざん等）から、使用する対象装置やその他の機器およびシステムを守らねばならない。

All rights reserved. Copyright©2005,Seiko Instruments Inc.

(5) 鍵の管理義務

加入者は、本サービスを利用するために必要となる秘密鍵を安全に管理しなければならない。

(6) すみやかな失効申請と届出

対象装置の秘密鍵が危殆化した場合、加入者は速やかに公開鍵証明書の失効をCAに申請するとともに、時刻配信局に届出を行わなければならない。

(7) 鍵危殆化に対する処理

加入者は、時刻配信局より時刻配信サーバの公開鍵証明書の失効についての連絡を受領した場合には、時刻配信局サーバの公開鍵証明書の失効リストを対象装置に設定することを遅滞なく行うものとする。

２．１．３ リポジトリに関する義務

時刻配信局は時刻配信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 時刻配信局の責任

時刻配信局は、本規程に従い本サービスを提供する。対象装置の運用結果については加入者がその責任を負い、加入者が対象装置を使用した結果として発生した損害については、時刻配信局は一切の責任を負わない。

２．２．２ 加入者の責任

加入者は、本規程に従い本サービスを利用する。

２．３ 財務上の責任

時刻配信局は、本サービスを提供するにあたり、加入者に対して 2．3．1に規定する賠償責任を負う。

２．３．１ 賠償責任

時刻配信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、時刻配信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。賠償額は、一会計年度(時刻配信局の一会計年度のことをいう)に生じた全ての損害に対して、全体として 600 万円もしくは当該一会計年度に加入者が時刻配信局に対して支払った本サービスの対価のいずれか低い金額を限度とする。

時刻配信局は、加入者以外に対しては、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 の規定にかかわらず、下記の場合においては、時刻配信局は加入者に対して賠償義務を負わない。

(1)時刻配信局が本規程ならびに個別のサービス規約にしたがい、本サービスを適正に遂行していた場合

All rights reserved. Copyright©2005,Seiko Instruments Inc.

(2)加入者の故意、過失または違法行為に起因して損害が発生した場合
(3)加入者による本規程ならびに個別のサービス規約への違反に起因して損害が発生した場合
(4)加入者のシステムに起因して損害が発生した場合
(5)次に掲げる時刻配信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)地震、噴火、津波、台風などの自然災害に起因して損害が発生した場合
(b)戦争、暴動、変乱、争乱、労働争議に起因して損害が発生した場合
(c)放射性物質、爆発性物質、環境汚染物質に起因して損害が発生した場合
(d)通信回線の不通に起因して損害が発生した場合
(e)その他の時刻配信局の支配を超えた事由に起因して損害が発生した場合
(6)4．4．1および4．4．3に定める事由による本サービスの中断または終了に起因して損害が発生した場合。
(7)加入者が時刻監査証明書の有効期間以外に時刻を利用したことに起因して損害が発生した場合。
(8)時刻配信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、またはセキュリティ手段が破られた場合。
(9)監査した時点の対象装置の時刻誤差が監査規格の範囲を超えていたことに起因して損害が発生した場合。

２．３．３ 信認関係の不存在

時刻配信局は、加入者または加入者の発行したタイムスタンプトークンを信頼して利用する者の代理人、受任者、受託者またはその他の代表者とは見なされない。加入者または加入者の発行したタイムスタンプトークンを信頼して利用する者のいずれも、契約によるかその他の方法によるかを問わず、時刻配信局に何らかの権利または義務を帰属させる権限を持たない。

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

時刻配信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

All rights reserved. Copyright©2005,Seiko Instruments Inc.

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。

時刻配信局から加入者への本規程に関する事項の通知先は、サービス加入申込書に記載した連絡先とする。

加入者は通知先を変更する場合、速やかに時刻配信局に届け出る。当該届出がなされない場合においては、時刻配信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。

２．４．３ 紛争解決

本規程または時刻配信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、東京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 時刻配信局に関する情報の公開

時刻配信局は、時刻配信局リポジトリに次の情報を公開する。

・ 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。

・ 本規程の変更の都度
・ その他時刻配信局の責任者が必要と判断した時

２．６．３ アクセス制御

時刻配信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 時刻配信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登録し、下記URL にて公開する。

URL:　http://www.sii.co.jp/ni/tss/

All rights reserved. Copyright©2005,Seiko Instruments Inc.

２．７ 準拠性監査

２．７．１ 監査頻度

時刻配信局は監査人による監査を年1 回定期的に実施する。時刻配信局は、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

時刻配信局の監査人には、セイコーインスツル株式会社またはその関連会社の従業員の中から、監査業務に精通した者を任命する。監査人の任命は時刻配信局の責任者が行う。
時刻配信局は、必要に応じて外部の監査法人に監査を依頼する。

２．７．３ 監査人と被監査部門の関係

時刻配信局の監査を実施する監査人は、時刻配信局運用部門に所属しない者を選定する。

２．７．４ 監査テーマ

本サービスが本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、時刻配信システムの管理が適切に行われていること、並びに外部からの不正アクセスに対する処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

時刻配信局は、重要又は緊急を要する監査指摘事項について、時刻配信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場合や時刻配信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、時刻配信局の時刻配信サーバの運用を停止するか否かは時刻配信局の責任者が決定する。時刻配信局の責任者は、時刻配信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

時刻配信局の監査結果は、監査人から時刻配信局の責任者に対して監査報告書として提出される。
監査報告書の保存期間は、10 年間とする。

２．８ 機密保持

２．８．１ 機密扱いとする情報

時刻配信局および加入者は、漏えいすることによって時刻配信局、加入者または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。
機密扱いとする情報は、本規程またはサービス規約に開示することを定めている場合を除いて、原則として開示しない。
次の情報は機密扱いとする情報に含まれるものとする。

(1) 申込に関する記録（承認されたか否かを問わない）
(2) 時刻配信局が保管する監査ログ

All rights reserved. Copyright©2005,Seiko Instruments Inc.

(3) 監査人が作成した監査報告書
(4) 不測の事態に対応する計画及び災害時における回復措置
(5) ハードウエア及びソフトウエアの運用、並びに時刻配信局の運営についてのセキュリティ対策

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) 時刻監査証明書、公開鍵証明書、公開鍵証明書の失効情報、本規程等公開する情報として明示的に示すもの
(2) 加入者またはCAから時刻配信局に開示された時点で既に公知の情報
(3) 加入者またはCAから時刻配信局開示された後、時刻配信局の責によらずして公知となった情報
(4) 加入者またはCA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) 加入者またはCA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

時刻監査証明書の失効情報の公開はおこなわない。

２．８．４ 法執行機関への情報開示

時刻配信局で取扱う情報（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

時刻配信局は、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、時刻配信局で取扱う情報（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または加入者が時刻配信局に開示した情報について、当該CAまたは加入者から開示要求があった場合、時刻配信局は、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。

２．９ 知的財産権

以下の各号に定めるものを含め、時刻配信局が作成した文書、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。ただし、時刻監査証明書等の確認時に表示される「SEIKO」の商標権はセイコー株式会社に帰属する。
(1) 時刻配信局から発行された時刻監査証明書
(2) 時刻配信局から発行された時刻監査証明書の発行記録

All rights reserved. Copyright©2005,Seiko Instruments Inc.

(3) 本規程

２．10 個人情報の取扱い

時刻配信局は、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。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

時刻配信局は、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

時刻配信局は、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

時刻配信局は、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

時刻配信局は、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

時刻配信局は、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

時刻配信局は、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。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

時刻配信局は、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。

(8) 破棄・消去

時刻配信局は、個人情報について、保有する必要がなくなった場合、裁断、焼却、記録媒体の破棄、データの完全な消去等、原状に復し得ない方法で速やかに破棄する。

All rights reserved. Copyright©2005,Seiko Instruments Inc.

３．識別と認証

３．１ 初期登録

３．１．１ 名前の型

時刻配信局が発行する時刻監査証明書の発行者名および所有者名は、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

時刻配信局が発行する時刻監査証明書の発行者名および所有者名は、CAが発行した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

時刻配信局の発行する時刻監査証明書の発行者名および所有者名は、CAにより一意に割り当てられるものとする。

３．１．４ 秘密鍵の所有を検証するための方法

時刻配信局は、所定の手続きにより加入者の秘密鍵所有を検証する。

３．１．５ 組織の認証

時刻配信局は、合理的な範囲内で本サービスの利用申請者組織の真偽を確認する。

３．１．６ 個人の認証

時刻配信局は、合理的な範囲内で本サービスの利用申請者の真偽を確認する。

３．２ サービス加入の更新

本サービスの契約更新時における識別と認証は、「３．１ 初期登録」において定める手続に基づいて行う。

３．３ サービスの解約の申請

本サービスの解約時における識別と認証は、「３．１ 初期登録」において定める手続に基づいて行う。

All rights reserved. Copyright©2005,Seiko Instruments Inc.

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、本規程およびサービス規約に記載された事項に同意のうえ時刻配信局に対して所定のサービス加入申込書を提出して加入申込みを行う。時刻配信局は、サービス加入申込書に基づいて加入申込者の審査を行う。

４．２ 時刻監査証明書の発行

時刻配信局は、1．3．2 で規定する内容のサービスを加入者に対して提供し、本規程に基づく時刻監査証明書を対象装置に対して発行する。対象装置は、受領した時刻監査証明書の有効期間内にかぎり、1．3．2で規定する時刻監査証明書の権限に依存する処理を実行することが許可される。

４．３ 時刻監査証明書の失効

時刻配信局は、発行した時刻監査証明書の失効を行わない。ただし、発行した時刻監査証明書の信頼性が疑われる場合は、その事実を対象となる加入者に通知する。

４．４ サービスの一時停止と解約

４．４．１ サービスの一時停止

時刻配信局は、時刻配信サービスの品質保持および安定稼働を目的とした当該サービスの保守点検および一時停止を行うことができる。ただし、当該サービスの一時停止を行う際には、加入者に対してサービスの一時停止に関する通知を行うが、下記の事由が発生した場合は、予告なしに本サービスを一時停止することができる。

(1)火災、停電、不正アクセス等の事故により本サービスの中断がやむを得ない場合

(2)セキュリティ管理上中断がやむを得ない場合

(3)加入者の債務不履行により、当該加入者に対する本サービスの提供を中断または終了する場合

(4)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に、中断または終了するとき

(5)時刻配信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に、中断または終了するとき

(6)加入者が本サービスの一時停止を申請した場合

４．４．２ サービスの一時停止の解除

時刻配信局は、サービスの一時停止の解除を行うにあたり、一時停止した理由が解決したことの確認を行う。

４．４．３ サービスの解約

時刻配信局は、下記の事由が発生した場合に、加入者の本サービスへの加入の解約を行う。

(1)加入者が加入の解約を申請した場合

All rights reserved. Copyright©2005,Seiko Instruments Inc.

(2)加入者が本規程に違反している事が明白で、改善が見られない場合
(3)時刻配信局が本サービスを終了する場合
(4)加入者に以下の事由が発生した場合
a)手形交換所の不渡り処分を受け、または金融機関から取引停止処分を受けたとき
b)監督官庁から営業の取消、停止等の処分を受けたとき
c)第三者から仮差押、仮処分、強制執行等を受け、本規約の履行が困難と認められるとき
d)破産の申立て、商法上の整理開始の申立て、特別清算開始の申立て、再生手続開始の申立てまたは会社更生手続開始の申立ての事実が生じたとき
e)解散、合併または営業の全部もしくは重要な一部の譲渡の決議をしたとき
f)財産状態が悪化しまたはそのおそれがあると認められる相当の事由(振り出した手形の銀行への提示の延期を要請したときを含むが、これに限定されない)があるとき
g)第三者の支配下に実質的に入り、本規約に関する時刻配信局の利益を損なうと認められるとき

４．５ セキュリティ監査の手順

時刻配信局は、そのシステムの安全性及び信頼性を維持するため、時刻配信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。

４．５．１ 監査ログに記録する情報

監査ログに記録する情報は時刻配信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)対象装置に対する時刻監査異常の記録
(2)時刻配信局内の装置に対する時刻監査異常の記録
(3)加入者の本サービスへの加入申込み・本サービスの提供開始から解約・本サービス停止までの申請および運用にかかわる記録
(4)時刻配信局で使用する鍵ペアの生成・失効記録
(5)加入者の装置の公開鍵情報、変更記録
(6)時刻配信局設備への入退室記録及びそれに対する承認記録
(7)時刻配信局システムに対する操作記録
(8)時刻配信局システムに対する不正アクセスに関する記録
(9)時刻配信局システムの動作異常の記録

４．５．２ 監査ログの検査頻度

時刻配信局は、監査ログの検査を少なくとも月1回の頻度で行う。

４．５．３ 監査ログの保存期間

前記の「４．５．１ 記録する情報の種類」における(1)～(5)の監査ログは10年間保存される。
その他の記録については3年間保存される。

４．５．４ 監査ログの保護

All rights reserved. Copyright©2005,Seiko Instruments Inc.

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される。

４．５．５ 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される。

４．５．６ 監査ログの収集システム

時刻配信局は、セキュリティや配信する時刻に関する重要な事象を監査ログとして自動システムとオペレータによる作業を組み合わせて収集する。

４．５．７ 脆弱性の評価

時刻配信局は、定期的に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、時刻配信局の責任者に報告される。

４．６ アーカイブ

４．６．１ 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。

・対象装置に対して発行した時刻監査証明書
・時刻配信局内の装置に対して発行した時刻監査証明書
・GPS-CV方式によるUTC（NICT）との時刻比較データ（GGTTSデータ）

４．６．２ アーカイブデータの保管期間

アーカイブデータは、すくなくとも10年間保管される。

４．６．３ 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され、温度、湿度、磁気などの環境を考慮して保管される。

４．６．４ アーカイブデータのバックアップ手順

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。

４．６．５ 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（NICT）に対して時刻補正が行われる。

４．６．６ アーカイブデータの収集システム

アーカイブデータは、自動システムとオペレータによる作業を組み合わせて収集される。

４．６．７ 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な状態で保管される。

４．７ 鍵更新

All rights reserved. Copyright©2005,Seiko Instruments Inc.

時刻配信局は、時刻配信サーバの公開鍵証明書の有効期間が満了する1ヶ月前までに鍵ペアの更新を行う。

４．８ 危殆化と災害からの復旧

４．８．１ ハードウエア、ソフトウエア又はデータが破壊された場合の対処

ハードウエア、ソフトウエ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エア、ソフトウエア又はデータにより、速やかに復旧作業を行う。

４．８．２ 時刻監査証明書を失効する場合の要件

発行した時刻監査証明書の失効処理は行わない。

４．８．３ 秘密鍵が危殆化した場合の対処

時刻配信サーバの秘密鍵が危殆化した場合は、「４．４ サービスの一時停止と解約」に従って本サービスの一時停止を行い、次の手続を含む所定の復旧作業を実施する。

・秘密鍵の危殆化に関する事実の加入者への通知

・時刻配信サーバの公開鍵証明書の失効申請

４．８．４ 災害等発生時の設備の確保

災害等により時刻配信局の設備が被害を受けた場合は、すみやかに予備機を確保しバックアップデータを用いて復旧作業を行う。

４．９ 時刻配信業務の終了

(1)時刻配信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)時刻配信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)その他時刻配信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時刻配信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180日前までに加入者に通知すると共に、リポジトリ上に公開する。ただし、緊急の場合は180日を待たずに業務を終了することができる。

本サービス終了後直ちに、使用中の時刻配信局秘密鍵の廃棄と公開鍵証明書の失効申請を実施する。

４．10 UTC(NICT)との時刻同期

(1)時刻精度

時刻配信局は、時刻配信サーバの時刻をUTC(NICT)に対する誤差が±10msecを越えないように管理する。

(2)うるう秒の設定

All rights reserved. Copyright©2005,Seiko Instruments Inc.

時刻配信局は、国家時刻標準機関の告示に基づき時刻配信サーバ、および加入者の対象装置に対して、うるう秒の設定を実施する。

４．11 時刻のトレーサビリティ

(1)時刻配信局の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(NTA)が定めるサービス運用規定に基づく時刻配信情報との時刻比較および保管作業を行うことにより、UTC(NICT)との時刻のトレーサビリティを確保する。

(2)タイムスタンプ局への時刻のトレーサビリティ

時刻配信局は、タイムスタンプ局の対象装置に対して行った時刻監査の記録を保持することにより、対象装置の時刻のUTC(NICT)に対するトレーサビリティを確保する。

All rights reserved. Copyright©2005,Seiko Instruments Inc.

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

時刻配信局の施設は、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。使用する機器等は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。

時刻配信局の建物、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

時刻配信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。

時刻配信局の施設には、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

時刻配信局の重要な装置は、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。

空調設備を設置して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

時刻配信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

時刻配信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

時刻配信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。

All rights reserved. Copyright©2005,Seiko Instruments Inc.

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

時刻の管理、時刻監査証明書の発行、停止、時刻配信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。
システムの操作は正当な権限を持つ操作者に限られ、時刻配信局の運用する時刻の設定・変更および時刻配信サーバの鍵の生成等の重要操作は複数人でおこなう。

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

時刻配信局は、教育計画を定め時刻配信局の運用に関わる要員に対して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

時刻配信局は、時刻配信局の運用に関わる要員に対しては、教育計画に基づき定期的にトレーニングを実施する。運用にかかわる変更が発生した場合は、すみやかに追加のトレーニングを実施する。

５．３．５ ジョブローテーション及びその実施

時刻配信局は、時刻配信局の運用にかかわる要員に対して必要に応じて交代制などの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、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

時刻配信局の運営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

All rights reserved. Copyright©2005,Seiko Instruments Inc.

提供される。

- 時刻配信局の設備や機器のマニュアル類
- 時刻配信局の運営に関する規定・手順書等

All rights reserved. Copyright©2005,Seiko Instruments Inc.

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

時刻配信サーバの鍵ペアは、複数人立ち会いのもとで暗号モジュールを用いて生成する。

６．１．２ 時刻配信サーバの公開鍵のCAへの登録

時刻配信サーバの公開鍵は、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 加入者の公開鍵証明書のルート証明書の受領

時刻配信局は、加入者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。

６．１．４ 時刻配信サーバの公開鍵証明書のルート証明書の配付

時刻配信局は、時刻配信サーバの公開鍵を証明するCAのルート証明書を加入者に対して安全かつ確実な手段で配付する。

６．１．５ 鍵のサイズ

(1)時刻配信サーバの鍵にはRSA 1024 bitの鍵を使用する。
(2)時刻配信サーバの公開鍵証明書のCAはRSA 2048bitの鍵を使用する。

６．１．６ 鍵を生成するハードウエア／ソフトウエア

「６．１．１ 鍵ペア生成」において定める。

６．１．７ 鍵の利用目的

時刻配信サーバの鍵は、以下の目的に使用する。
(1)時刻配信サーバが対象装置に発行する時刻監査証明書へのデジタル署名
(2)時刻配信サーバと対象装置とが通信を行う際の認証

６．２ 秘密鍵の保護

６．２．１ 暗号モジュールに関する基準

時刻配信サーバの鍵は、FIPS(米国連邦情報処理標準)140-1 レベル2以上 の認定を受けた暗号モジュールを使用して生成・保管される。

６．２．２ 秘密鍵の複数人制御

時刻配信サーバの秘密鍵の生成は、複数人の管理の下で行われる。

６．２．３ 秘密鍵の預託

時刻配信サーバの秘密鍵の預託は行わない。

６．２．４ 秘密鍵のバックアップ

All rights reserved. Copyright©2005,Seiko Instruments Inc.

時刻配信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の格納

時刻配信サーバの秘密鍵は、暗号モジュールの中で生成・保管される。

６．２．７ 秘密鍵の活性化方法

時刻配信サーバの秘密鍵は、権限を有した操作員が暗号モジュールに活性化データを入力することにより活性化される。

６．２．８ 秘密鍵の非活性化方法

時刻配信サーバの秘密鍵は、権限を有した操作員が暗号モジュールに対して所定の操作を行うことにより非活性化される。

６．２．９ 秘密鍵の破棄方法

暗号モジュール内の時刻配信サーバの秘密鍵は、権限を有した操作員が所定の操作を行うことで破棄される。

６．３ 公開鍵と秘密鍵の有効期間

時刻配信サーバの鍵の有効期間は、有効とする日から起算して5年とする。
ただし、秘密鍵が危殆化する可能性があると判断した場合は、その時点で鍵更新を行う。

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

時刻配信サーバの秘密鍵の活性化データは、所定の手順に従って生成され、インストールが行われる。

６．４．２ 活性化データの保護

時刻配信サーバの秘密鍵の活性化データは、所定の手順に従って保護・管理される。

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

時刻配信局では、コンピュータ装置や時刻関連機器のハードウエアやソフトウエアの導入時にはセキュリティに関する確認を行う。

６．５．２ コンピュータセキュリティ評価

時刻配信局では、セキュリティの脆弱性に関する評価を定期的に実施し、問題が認められた場合は是正処置を行う。

All rights reserved. Copyright©2005,Seiko Instruments Inc.

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

時刻配信局内で使用されるソフトウエアの開発、修正、変更にあたっては、適正な品質管理の下で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

時刻配信局では、コンピュータ装置等のハードウエアやソフトウエアの導入時にはセキュリティに関する確認を行う。

６．６．３ ライフサイクルセキュリティ評価

時刻配信局では、セキュリティの脆弱性に関する評価を定期的に実施し、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

時刻配信局では、システム導入時や運用変更時にネットワークセキュリティに関して確認を行う。

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。

All rights reserved. Copyright©2005,Seiko Instruments Inc.

７．時刻監査証明書(時刻属性証明書)のプロファイル

７．１ 時刻監査証明書のASN.1記述

本サービスの時刻監査証明書は、下記のASN.1記述に基づく属性証明書である。

(基本情報)

```
  Attribute Certificate ::= SEQUENCE {
     acinfo AttributeCertificateInfo,
     signatureAlgorithm AlgorithmIdentifier,
     SignatureValue BIT STRING
  }
  AttributeCertificateInfo ::== SEQUENCE {
     version AttCertVersion
     holder Holder,
     issuer AttCertIssuer,
     signature AlgorithmIdentifier,
     serialNumber CertificateSerialNumber,
     attrCertValidityPeriod AttCertValidityPeriod,
     attributes SEQUENCE OF Attribute,
     issuerUniqueID UniqueIdentifier OPTIONAL,
     extensions Extensions OPTIONAL
  }
  Attribute ::== SEQUENCE {
     type AttributeType,
     values SET OF AttributeValue
}
AttributeType ::= OBJECT IDENTIFIER
AttributeVlaue ::= ANY DEFINED BY AttributeType


  TimingMetrics ::= SEQUENCE {
     ntpTime BigTime,
     offset BigTime,
     delay BigTime,
     expiration BigTime,
     leapEvent SET OF LeapData OPTIONAL
  }


  BigTime ::= SEQUENCE {
     major                    BigIntegerStr,
```


All rights reserved. Copyright©2005,Seiko Instruments Inc.

```
    fractionalSeconds       BigIntegerStr,
    sign                    INTEGER OPTIONAL
  }

  LeapData ::= {
    leapTime BigTime,
    action INTEGER
}
```

(追加情報)

```
  TimingPolicy ::= SEQUENCE {
    policyID       SEQUENCE SIZE (1..MAX) OF OBJECT IDENTIFIER,
    maxOffset      [0] BigTime OPTIONAL,
    maxDelay       [1] BigTime OPTIONAL
  }
```

7．2 時刻監査証明書のプロファイル

(基本情報)

Version	
AttCertVersion	時刻監査証明書の、属性証明書としてのバージョン 型:INTEGER 値:1
Holder	
Holder	時刻監査証明書の所有者
entityName	時刻監査証明書の所有者名
directoryName	
countryName	時刻監査証明書所有者の国名
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:時刻監査証明書所有者の公開鍵証明書のサブジェクト名に従う
organizationName	時刻監査証明書所有者の組織名
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:時刻監査証明書所有者の公開鍵証明書のサブジェクト名に従う

All rights reserved. Copyright©2005,Seiko Instruments Inc.

organizationalUnitName type	時刻監査証明書所有者の部門名 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:時刻監査証明書所有者の公開鍵証明書のサブジェクト名に従う
commonName type	時刻監査証明書所有者の固有名称 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:時刻監査証明書所有者の公開鍵証明書のサブジェクト名に従う
objectDigestInfo digestedObjectType	オブジェクトのダイジェスト値の情報 オブジェクトのダイジェスト値の型 型:ENUMERATED 値:1
digestAlgorithm algorithm	オブジェクトのダイジェストに使用されたハッシュアルゴリズムの識別子 暗号アルゴリズムのオブジェクトID 型:OID 値:1 3 14 3 2 26 (SHA1)
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
objectDigest	オブジェクトのダイジェスト値 型:BIT STRING 値:公開鍵証明書のハッシュ値
Issuer	
AttCertIssuer v2Form issuerName directoryName countryName type	時刻監査証明書の発行者 バージョン2の記述形式 時刻監査証明書の発行者名 時刻監査証明書発行者の国名 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 type	時刻監査証明書発行者の組織名 組織名のオブジェクトID

All rights reserved. Copyright©2005,Seiko Instruments Inc.

	型:OID 値:2 5 4 10
value	組織名の値 型:PrintableString 値:SeikoInstrumentsInc
organizationalUnitName type	時刻監査証明書発行者の部門名 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:時刻監査証明書発行者の公開鍵証明書のサブジェクト名に従う
commonName type	時刻監査証明書発行者の固有名称 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:時刻監査証明書発行者の公開鍵証明書のサブジェクト名に従う
Signature	
AlgorithmIdentifier	時刻監査証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクトID 型:OID 値:1 2 840 113549 1 1 5 (SHA1withRSA)
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
serialNumber	
CertificateSerialNumber	時刻監査証明書のシリアル番号 型:INTEGER 値:ユニークな正の整数
attrCertValidityPeriod	
AttCertValidityPeriod	時刻監査証明書の有効期間
notBeforeTime	開始日時 型:GeneralizedTime 値:YYYYMMDDHHMMSSZ
notAfterTime	終了日時 型:GeneralizedTime 値:YYYYMMDDHHMMSSZ
Attributes	
[attribute: TimingMetrics]	属性情報

All rights reserved. Copyright©2005,Seiko Instruments Inc.

type	型:OID 値: 基本情報のみの場合:1 3 6 1 4 1 601 10 1 追加情報がある場合:1 3 6 1 4 1 601 10 4 1
value	
ntpTime	時刻監査が行われた時刻
major	時刻監査が行われた時刻の整数部 型:BigIntegerStr ([UNIVERSAL 2] IMPLICIT OCTET STRING) 値:時刻監査が行われた時刻の整数部
fractionalSeconds	時刻監査が行われた時刻の小数部 型:BigIntegerStr ([UNIVERSAL 2] IMPLICIT OCTET STRING) 値:時刻監査が行われた時刻の小数部
offset	上位時刻配信サーバとの時刻のずれ(オフセット)
major	上位時刻配信サーバとの時刻のずれの整数部 型:BigIntegerStr ([UNIVERSAL 2] IMPLICIT OCTET STRING) 値:上位時刻配信サーバとの時刻のずれの整数部
fractionalSeconds	上位時刻配信サーバとの時刻のずれの小数部 型:BigIntegerStr ([UNIVERSAL 2] IMPLICIT OCTET STRING) 値:上位時刻配信サーバとの時刻のずれの小数部
sign	上位時刻配信サーバとの時刻のずれの符号 型:INTEGER OPTIONAL 値: 上位時刻配信サーバとの時刻のずれが負の値の場合:-1 それ以外の場合:本項目は時刻監査証明書に含まれない
delay	時刻監査時のネットワーク遅延
major	ネットワーク遅延の整数部 型:BigIntegerStr ([UNIVERSAL 2] IMPLICIT OCTET STRING) 値:ネットワーク遅延の整数部
fractionalSeconds	ネットワーク遅延の小数部 型:BigIntegerStr ([UNIVERSAL 2] IMPLICIT OCTET STRING) 値:ネットワーク遅延の小数部
expiration	時刻監査証明書の有効期間
major	時刻監査証明書の有効期間の整数部 型:BigIntegerStr ([UNIVERSAL 2] IMPLICIT OCTET STRING) 値:時刻監査証明書の有効期間の整数部
fractionalSeconds	時刻監査証明書の有効期間の小数部 型:BigIntegerStr ([UNIVERSAL 2] IMPLICIT OCTET STRING) 値:時刻監査証明書の有効期間の小数部
leapEvent leapTime major	うるう秒設定情報 (※うるう秒設定時のみ含まれる) うるう秒設定日時 うるう秒設定日時の整数部 型:BigIntegerStr ([UNIVERSAL 2] IMPLICIT OCTET STRING)

All rights reserved. Copyright©2005,Seiko Instruments Inc.

	値:うるう秒設定日時の整数部
fractionalSeconds	うるう秒設定日時の小数部 型:BigIntegerStr　([UNIVERSAL 2] IMPLICIT OCTET STRING) 値:うるう秒設定日時の小数部
action	うるう秒の設定方法 型:INTEGER 値:　挿入の場合:1 削除の場合:-1

(追加情報)

attributes	
	属性情報
[attribute: TimingPolicy]	型:OID
type	値: 1 3 6 1 4 1 601 10 4 2
value	時刻監査証明書ポリシー 型:OID
policyID	値:0.2.440.200125.1.2.1
maxOffset major	時刻監査規格(オフセット) 時刻監査規格(オフセット)の整数部 型:BigIntegerStr　([UNIVERSAL 2] IMPLICIT OCTET STRING) 値:時刻監査規格(オフセット)の整数部
fractionalSeconds	時刻監査規格(オフセット)の小数部 型:BigIntegerStr　([UNIVERSAL 2] IMPLICIT OCTET STRING) 値:時刻監査規格(オフセット)の小数部
maxDelay major	時刻監査規格(ネットワーク遅延) 時刻監査規格(ネットワーク遅延)の整数部 型:BigIntegerStr　([UNIVERSAL 2] IMPLICIT OCTET STRING) 値:時刻監査規格(ネットワーク遅延)の整数部
fractionalSeconds	時刻監査規格(ネットワーク遅延)の小数部 型:BigIntegerStr　([UNIVERSAL 2] IMPLICIT OCTET STRING) 値:時刻監査規格(オフセット)の小数部

All rights reserved. Copyright©2005,Seiko Instruments Inc.

８．本規程の管理

８．１ 本規程の変更

時刻配信局は、本規程を必要に応じて変更する。

８．２ 本規程の公開と通知

時刻配信局は、本規程を変更した場合、速やかに変更した本規程を2．6項に定めた手順に従い公開する。

時刻配信局の本サービス提供について個別契約した加入者に対しては、個別契約の内容に影響がある場合については、別途個々の契約に応じて対応する。

上記以外の加入者及び、タイムスタンプ利用者及びタイムスタンプトークンの検証者等の時刻配信局の本サービスの関係者に対しては、本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 本規程の承認手続き

本規程の設定・変更は、時刻配信局代表者によって承認される。

All rights reserved. Copyright©2005,Seiko Instruments Inc.

付録 A. 略語と用語解説

項目	説明
AA	Attribute Authority 属性認証局
AC	Attribute Certificate 属性証明書
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
TAC	Time Attribute Certificate 時刻監査証明書 本来は時刻属性証明書のことであるが、本規程においては時刻監査証明書と記載する
TSA	Time-Stamping Authority タイムスタンプ局
TSU	Time Stamp Unit タイムスタンプユニット
TST	Time Stamp token タイムスタンプトークン
TA	Time Authority 時刻配信局
UTC（NICT）	独立行政法人情報通信研究機構（NICT） が決定する協定世界時（Coordinated universal time ）
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）	国際度量衡局が決定する協定世界時（Coordinated Universal Time）。国際原子時と世界時（UT1）の誤差が 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(TAC)	時刻配信局（TA）が顧客の装置（タイムスタンプユニット等）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属性証明書のこと
時刻配信局(TA)	時刻に関する配信業務を実施する機関、本時刻配信局では時刻の認証手段として時刻属性証明書を発行するため、時刻に関する属性認証明局でもある。
属性認証局（AA）	証明書所有者の権限等の属性を認証し、属性証明書を発行する機関
属性証明書（AC）	属性証明書の所有者の権限等の属性を指定するために、属性証明局（AA）によりデジタル署名された証明書（2000 年版 X.509 で追加された）。 公開鍵証明書が証明書所有者の身元を証明するのに対して、属性証明書は証明書所有者の権限等の属性を証明する
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。
タイムスタンプユニット(TSU)	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装置
タイムスタンプトークン(TST)	特定の電子情報の存在日時を明示する RFC3161に準拠した様式をもつ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）	独立行政法人情報通信研究機構（NICT）が管理・発信する日本国の標準時刻。UTC（NICT）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

All rights reserved. Copyright©2005,Seiko Instruments Inc.

付録 B. 参考文献

・RFC 3161(2001)　Internet X.509 Public Key Infrastructure: Time-Stamp Protocol(TSP)

・RFC 2527 Certificate Policy and Certification Practices Statement Framework

・ETSI TS 102 023 V1.1.1(2002-01) 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

・RFC 3281(2002)　An Internet Attribute Certificate Profile for Authorization

・ISO/IEC 9594-8 | X.509: ITU-T Recommendation X.509 (1997), Information Technology -- Open Systems Interconnections -- The Directory: Authentication Framework. General Procedures 1997

All rights reserved. Copyright©2005,Seiko Instruments Inc.