SecureNTP 時刻配信サービス運用規程

1.3 版

2008 年 5 月

セイコーインスツル株式会社

改版履歴

版	変更日付	変更箇所	変更内容	承認
1.0	2006 年 3 月 16 日		初版作成	クロノトラスト時刻配信局代表者
1.1	2006 年 3 月 27 日	2.2.1. 時刻配信局の損害賠償責任	賠償総額に関する記載を修正	クロノトラスト時刻配信局代表者
1.2	2006 年 11 月 7 日	1.3.3. 時刻監査証明書の適用範囲	適正な用途に関する記載を修正	クロノトラスト時刻配信局代表者
		4.1.1.システムへの接続	参照先を修正	
		4.1.4. 時刻監査証明書の発行	語句を一部修正	
		4.2.4.サービスの解約	法律改正により無くなった制度に関する記載を削除	
		全般	句読点の抜けを修正	
1.3	2008 年 5 月 14 日	1.2.2.オブジェクト識別子	語句を一部修正	クロノトラスト時刻配信局代表者
		8.時刻監査証明書のプロファイル	8.1. 追記 8.2. 記載内容の一部修正 8.2. 拡張領域の追記	

目次

1. はじめに

SecureNTP 時刻配信サービス運用規程（以下「本規程」といいます。）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（TA）が、時刻認証局（TSA）が行う時刻認証サービス（以下「TSA サービス」といいます。）に対して UTC(NICT) に同期した時刻の配信と監査を行うサービスについての基本的事項について述べます。

1.1. 概要

本規程は、第三者が運営する TSA サービスに対する SecureNTP 時刻配信サービス(以下「本サービス」といいます。)の運用方針及び業務手続きについて記述するものです。
本規程の適用対象は、本規程によって規定される本サービスの申請者、利用者、及び本サービスに関連する個人・法人・組織とします。本規程では本サービスに関連する権利と義務を表明します。

クロノトラスト時刻配信局は、本規程を本サービスに関する運営方針として位置付けます。

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　　：SecureNTP 時刻配信サービス運用規程
バージョン　　：1.3 版
作成日　　：2008 年 5 月 14 日
作成者　　：セイコーインスツル株式会社
本バージョンの運用規程の適用開始日：2008 年 6 月 1 日

1.2.2. オブジェクト識別子

本規程において適用するオブジェクト識別子（OID）を以下に示します。
・セイコーインスツル株式会社　　：　0.2.440.200125
・SecureNTP 時刻配信サービス　　：　0.2.440.200125.1.6
・時刻監査証明書ポリシー　　：　0.2.440.200125.1.6.1
・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. 定義

1.3.1. 用語の定義

（1） 時刻認証局（TSA）
本規程において時刻認証局とは、時刻ソースから時刻の配信を受けて、タイムスタンプトークン（以下「TST」といいます。）を発行する事業者をいいます。

（2） 時刻配信局(TA)
本規程において時刻配信局とは、本規程に従い UTC(NICT)に対するトレーサビリティを有する時刻ソースとして、時刻認証局の管理するタイムスタンプユニット(以下「TSU」といいます。)に UTC(NICT)に同期した時刻の配信を行い、かつ TSU 内の時計の時刻監査を行う事業者をいいます。

（3） 認証局(CA)
本規程において認証局とは、公開鍵基盤(PKI)の認証局（CA）であり、利用者の TSU、又は、時刻配信局の時刻配信サーバが使用する PKI の公開鍵証明書の認証を行う事業者をいいます。

（4） 利用者
本規程において利用者とは、時刻配信局から時刻の配信を受ける時刻認証局として本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者をいいます。

（5） 時刻監査証明書(TAC)
本規程において時刻監査証明書とは、TSU が時刻監査を受けた日時及びそのときの時刻誤差が記載された電子時刻監査証明書をいいます。時刻監査証明書は、時刻配信局から時刻認証局へ発行されます。時刻配信局が監査した時点において、TSU の時計の誤差が UTC(NICT)に対して±500 ミリ秒の範囲内であった場合、TSU は時刻監査証明書の有効期間内に限り TST を発行することができます。
時刻監査証明書は、時刻配信局による秘密鍵で署名され改ざんから保護されています。

（6） リポジトリ
本規程においてリポジトリとは、本規程等を格納するシステムのことを示すものとします。

（7） 情報通信研究機構（NICT）
本規程において情報通信研究機構とは、周波数や時間の元となる国家標準値を定める公的機関をいいます。国際的に定義された「秒の定義」にしたがってセシウム原子時計から、日本標準時を生成・供給しています。時刻配信局は、情報通信研究機構から供給される時刻源を参照・比較して、時刻の正当性（トレーサビリティ）を維持しています。

1.3.2. SecureNTP 時刻配信サービスの内容

本サービスの内容は以下のとおりとします。

（1）時刻配信局は、高精度の時刻維持が可能な時計を用い、本サービスに使用する時刻の UTC(NICT)との同期を高精度に維持します。

a） 時刻配信局は複数の原子時計を用いた時計システムを用います。
b） 時計システムは±1 x 10-9 以上（1 日）の安定度を維持します。
c） GPS 受信機、原子時計、時刻配信サーバに関する操作記録の保管を行います。
d） 原子時計と接続された時刻配信サーバの時刻を GPS を用いたコモンビュー方式により UTC(NICT)と±30 ミリ秒以内に同期していることを確認します。
e） 時刻配信サーバの時刻を GPS またはその他の方法を用いて、UTC(NICT)と±30 ミリ秒以内に同期していることを監視します。

（2）時刻配信局は、利用者に対して、利用者の TSU の時刻と時刻配信局が管理する時刻の誤差を測定し、測定結果に対する TAC を生成し、それを安全な通信手段を用いて TSU に対して発行します。

a） 時刻監査結果を記述した TAC は、時刻配信局が管理する時刻配信サーバを用いて生成され、時刻配信サーバ毎の秘密鍵を用いて電子署名を行い、配信時刻、監査結果の改ざん防止を行います。
b） TAC の署名に用いる秘密鍵は FIP140-2 Level3 相当以上の鍵保護機構で管理します。
c） 時刻配信サーバは、TAC を発行する TSU を PKI を用いた技術で特定し認証します。
d） 時刻配信サーバは、TSU の時刻監査・配信を行う際には、改ざんおよび成りすまし対策を行います。
e） 時刻配信には、測定精度が±50 ミリ秒以内の通信環境と通信手順を用います。
f） TAC には時刻監査証明書ポリシーを示す OID を含めます。

（3）TAC が示す時刻は本規程に基づいて下記の条件で付与されます。

a） TAC を発行する時刻配信局は、原子時計システムから取得される時刻とは別に、GPS またはその他の方法で UTC(NICT)を随時参照することにより、時刻配信局が管理する時刻が UTC(NICT)と±30 ミリ秒を超える誤差が発生しないことを監視します。規定値以上の誤差が検出された場合は時刻配信機能を即座に停止し、本規程で定められた時刻範囲内で TAC が発行されることを保証します。
b） TSU の時計が UTC(NICT)と±500 ミリ秒以内であることを確認し、その測定結果を TAC に記載します。TAC の有効期間は 25 時間とし有効期間の範囲内において TSU が時刻認証機能を活性化させる権限を TSU に付与します。
c） TSU の時計が UTC(NICT)と±500 ミリ秒を超える誤差があるものと判断された場合、またはその他の合理的な理由がある場合、時刻配信局は TSU に対して、TAC に TSU の時刻認証機能停止命令を記載し、発行することで利用者に時刻異常を通知するとともに、TSU の時刻認証機能停止を促します。

1.3.3. 時刻監査証明書の適用範囲

（1）適正な用途

TAC は、時刻配信局より利用者に対して配信された時刻を用いたタイムスタンプトークンの発行を所定の期間行うことを許可する目的で発行されます。

時刻認証局は、タイムスタンプトークンの利用者がタイムスタンプトークンの生成時刻の有効性を確認可能なように、TSU の時刻ソースおよび TSU が時刻監査を受けたときの時刻誤差を明示する目的で、TAC 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ます。時刻認証局は、上記以外の目的で配信された時刻および TAC を使用してはなりません。

（2）禁止される用途

時刻配信局より配信された時刻および TAC を、前号の目的以外、および、人間の生命や身体に危害が及ぶ可能性がある用途へ適用することを禁止します。 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します。

1.4. 本規程に関する問い合せ先

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ます。

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

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、利用者に対して次の義務を負います。

（1）時刻配信局は、利用者の TSU に対して時刻の配信及び監査を少なくとも 1 日 1 回実施します。

（2）利用者の TSU に対する時刻監査の結果、UTC(NICT)に対する時刻誤差の測定値が±500ミリ秒以内の場合は、当該 TSU に対して 25 時間有効の時刻監査証明書を発行し、当該時刻監査証明書の有効期間内において TSU が TST を発行することを許可します。また、時刻監査実施時の時刻誤差の測定値が±500ミリ秒を超えている場合は、TSU の TST の発行機能を停止する処置を行います。

（3）時刻配信局で使用する時計の UTC(NICT)に対する時刻同期精度については、その誤差が±30 ミリ秒を超えないように維持します。

（4）うるう秒を国家時刻標準機関の告示に基づき時刻配信サーバに設定し、運用します。

（5）時刻配信サーバの秘密鍵を安全に保持し、万一秘密鍵が危殆化した場合は、直ちに認証局に鍵の失効申請を行うとともに利用者に通知します。

（6）本規程4.5で規定するアーカイブデータを保管します。

（7）本サービスの月次報告書を利用者に提出します。

2.1.2. 利用者の義務

利用者は、利用者の使用するシステムに対して次の義務を負います。

（1） 利用者は、TAC を受信した場合、即時に TAC の有効性確認を行い、TAC に示される時刻情報を元に、TSU の時刻を維持するものとします。

（2） 利用者は、時刻配信局に接続する TSU の接続情報、接続に使用する認証情報を正しく申告するものとします。

（3） 利用者は、時刻配信局より、TAC による時刻認証機能停止命令を受信した場合、即時に該当する TSU の時刻認証機能を停止するものとします。

（4） 利用者は、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安全に管理するものとします。

（5） TSU の秘密鍵が危殆化し、又はそのおそれが生じた場合等、利用者の信頼性に重大な問題が発生した場合、利用者はただちに時刻配信局への通知を行うものとします。

（6） 配信された時刻と TAC 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、利用者はこれを十分理解した上で時刻と TAC 等を利用しなければなりません。

（7） 利用者は時刻配信局より配信された時刻や TAC を変更・改ざんをしてはなりません。TSU を不当に分解・改造・解析等してはなりません。TSU の機能・性能が維持できるように TSU を適正に管理しなければなりません。適正な管理には、TSU の周囲温度を管理すること、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ます。

2.1.3. 認証局の義務

認証局は時刻配信局への証明書発行サービスにおいて、時刻配信局に対して次の義務を負います。

（1）TAC の発行用に時刻配信局の公開鍵証明書を発行します。
（2）認証局の秘密鍵を安全に保持し、万一秘密鍵が危殆化した場合は、直ちにその旨を時刻配信局に通知します。
（3）公開鍵証明書の失効リスト、及び公開鍵証明書発行に関連するその他の情報を時刻配信局および利用者に公開します。また、時刻配信局から公開鍵証明書の失効申請があった場合は直ちに公開鍵証明書の失効を行います。

2.1.4. リポジトリに関する義務

時刻配信局は本サービスに関する情報のうち公開する情報を、2.4 で規定される方法でリポジトリに公開します。

2.2. 財務上の責任

2.2.1. 時刻配信局の損害賠償責任

本サービスに関する時刻配信局の責任は、2.1.1 に記述する範囲に限られるものとします。また、法令により強制される場合であっても、賠償総額は、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利用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します。なお、時刻配信局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、時刻配信局は賠償責任を免れるものとします。

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、時刻配信局は賠償義務を負わないものとします。
（1）時刻配信局が本規程ならびに個別の契約に従い、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）利用者による本規程若しくは個別の契約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） 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） その他の時刻配信局の支配を超えた事由
（6）4.2.1、4.2.3、及び 4.3 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）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、又はセキュリティ手段が破られた場合
（8）その他時刻配信局の責に帰すべき事由によらない場合

2.2.3. 信認関係の不存在

時刻配信局は、利用者または利用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ものとします。利用者または利用者の発

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ものとします。

2.3. 解釈及び執行

2.3.1. 準拠法

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します。

2.3.2. 可分性

本規程のある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、本規程の他の規定は有効に存続し適用されます。

2.3.3. 存続性

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 2.2、2.3、2.6 及び 2.7 の効力は有効に存続します。

2.3.4. 通知

利用者から時刻配信局への通知は、書面又は電子メールによって、1.4 に定める宛先に行うものとします。書面による通知は受領日をもって有効とします。

時刻配信局から利用者への通知は、書面又は電子メールによって、本サービスの加入時に利用者が登録した連絡先へ行うものとし、発信した時点で通知したものとします。利用者は連絡先を変更する場合、速やかに時刻配信局に届け出るものとします。当該届け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します。

2.3.5. 紛争解決

本規程又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します。本規程又は本規程に定められていない事項に関して協議の必要がある場合、各当事者は誠意を持って協議するものとします。

2.4. 公開とリポジトリ

2.4.1. SecureNTP 時刻配信サービスに関する情報の公開

時刻配信局は、2.4.4 に定めるリポジトリに次の情報を公開します。

・本規程

2.4.2. 公開の頻度

公開する情報の更新頻度は次のとおりとします。

（1）本規程の変更の都度

（2）その他時刻配信局の責任者が必要と判断した時

2.4.3. アクセス制御

2.4.4 に定める時刻配信局の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します。

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ものとします。

2.4.4. リポジトリ

2.4.1 において定める情報をリポジトリに登録し、以下の URL にて公開します。

URL:　http://www.sii.co.jp/ni/tss/

2.5. 機密保持

2.5.1. 機密扱いとする情報

漏えいによって利用者、時刻配信局、又は認証局の業務の信頼性が損なわれる虞のある情報を、時刻配信局および利用者は機密扱いとします。時刻配信局および利用者は、機密扱いとする情報について、当該情報を含む書類及び記憶媒体の管理責任者を定め、安全に保管管理します。機密扱いとする情報は、本規程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、漏えいしないと共に本サービスの範囲を超えて使用しないものとします。

次の情報は機密扱いとする情報に含まれるものとします。

（1）時刻配信局が保管するセキュリティ検査ログ

（2）不測の事態に対応する計画及び実施措置

（3）ハードウェア及びソフトウェアの運用、ならびに時刻配信局の運営についてのセキュリティ対策

（4）利用者の本サービスの申し込みに関する記録（承認されたか否かを問わない）

（5）本サービス利用のために時刻配信局が利用者に付与する識別情報

2.5.2. 機密扱いとしない情報

2.5.1 の規定にかかわらず、次の各号に定める情報については、機密扱いとはしません。

（1）公開鍵証明書、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）開示の時点で、被開示者の責によらずして公知となった情報

（3）開示後、被開示者の責によらずして公知となった情報

（4）第三者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） 被開示者が、前項に基づき機密扱いとする情報によらずして独自に開発した情報
（6） 開示者が第三者に対し、秘密保持義務を課すことなく開示した情報

2.5.3. 公開鍵証明書失効情報の公開

時刻配信局の公開鍵証明書の失効情報は、該当する公開鍵証明書の認証局において公開鍵証明書失効リストとして公開されます。

2.5.4. 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します。

2.5.5. その他の理由に基づく情報開示

時刻配信局が業務の一部を第三者に委託する場合、2.5.1 に定める機密扱いとする情報を委託先に開示する事があるがその場合は委託契約の中で守秘を義務付けるものとします。

2.6. 知的財産権

以下の各号に定めるものを含み、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（これらの登録を受ける権利を含む）、商標権及び著作権（以下知的財産権と呼ぶ）は時刻配信局又はそのライセンサーに帰属し、利用者その他の者には移転しないものとします。

（1） 時刻配信局から発行された TAC
（2） 時刻配信局から発行された TAC の発行記録
（3） 本規程

2.7. 個人情報の取り扱い

時刻配信局は、利用者への本サービスの提供にあたり、利用者から提供される個人情報を、以下に特定する範囲を超えて使用しません。また、その保護について、以下に従うものとします。ただし、法令に定められた場合はこれに限りません。

（1） 入手する個人情報の位置付け
時刻配信局は、利用者から提供された情報のうち、個人の氏名、電話番号、勤務先その他個人の識別が可能な情報を個人情報として扱うものとします。

（2） 利用目的の特定
時刻配信局は、利用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使用します。なお利用者から別途承諾を得た場合、時刻配信局は、本サービスに関連した自ら又は自らの子会社の商品、サービス等の案内のために利用することがあります。

（3） 利用目的による制限
時刻配信局は、上記 2.7(2)に規定される目的以外に個人情報を利用しません。

（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します。

（5） 正確性の確保

時刻配信局は、個人情報を利用者からの申し出に基づき正確な状態で管理します。

（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、改竄、漏えい等の防止に努めます。また、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います。

（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、訂正若しくは削除を求められた場合、合理的な範囲内で対応します。

（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します。

3. 確認と認証

3.1. 利用申請者の認証と利用可否

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し、利用可否を判断します。

3.2. サービスの加入の更新

本サービスの契約更新時における識別と認証は 3.1 において定める手続きに基づいて行います。

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 において定める手続きに基づいて行います。

3.4. システムへの接続の認証と利用可否

時刻配信局は、本システムに接続される TSU に対して接続審査を行い、適切に接続が行われることを確認し記録します。

3.5. 接続の更新

時刻配信局は、本サービスに使用される TSU に対して定期的な接続状況審査を行い、適切に接続が行われることを確認し記録します。

3.6. 接続の終了

時刻配信局は、本サービスに使用される TSU に対して接続解除の審査を行い、適切に接続が終了されたことを確認し記録します。

4. 運用要件

4.1. サービスの提供

4.1.1. システムへの接続

時刻配信局は、本サービスに使用される TSU を、3.4、3.5 及び 3.6 に定められた手順によって、管理します。

4.1.2. 時刻配信・監査の実施

時刻配信局は、本サービスに使用される TSU に対して、1.3.2 で定められた手順で定期的に時刻配信・監査を実施します。

4.1.3. 時刻配信・監査の要求に対する応答

本サービスに使用される TSU は、本サービスで使用する時刻配信サーバに設定された時刻配信・監査実行機会とは別に、TSU に対する TAC を更新維持する目的で、時刻配信局に対して時刻配信・監査の要求を行うことができます。時刻配信局は、要求が妥当性を持つ場合に時刻配信・監査を実施します。

4.1.4. 時刻監査証明書の発行

時刻配信局は、本サービスを実行し、TSU が時刻配信・監査を許可されたサーバであることが認証された場合、TAC の発行を行います。

4.2. サービスの一時停止と解約

4.2.1. サービスの一時停止

時刻配信局は、本サービスの一時停止の必要が発生した時は、事前にそのスケジュールと手続きを決め、その内容を停止日の 1 週間前までに公知、もしくは利用者へ通知します。
ただし、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ものとします。

（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） 保守、運用上の点検整備又はセキュリティ管理上中断がやむを得ない場合。ただし、定期的な点検整備（認証局の点検整備による場合を含む）及び 4.8(2)に定めるうるう秒の設定による中断については1週間前までに利用者に通知する。
（3） 時刻配信局又は認証局が一時停止又は終了し、時刻配信局が一時停止を判断した場合
（4） システム構成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、本サービス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
（5） 時刻配信局の秘密鍵の漏洩、偽造又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与える可能性がある事由が発生した場合

4.2.2. 利用者におけるサービスの一時停止

本サービスの利用料金の支払期日を経過しても、利用者から支払いがない場合、時刻配信局は、事前に利用者に告知した上で本サービスの利用を停止することができるものとします。
また、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ものとします。

（1） 利用者の債務不履行により、該当利用者に対する本サービスの提供を中断する場合
（2） 利用者が本サービスの利用の一時停止を申請した場合
（3） 利用者が違法に、又は明らかに公序良俗に反する態様において本サービスを利用した場合
（4） 利用者が他の本サービス利用者に支障を与える態様において本サービスを利用した場合

4.2.3. サービスの一時停止の解除

時刻配信局は、本サービスの提供を一時停止した理由が解決した場合、所定の手続きによる確認後に本サービスの一時停止の解除を行います。

4.2.4. 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本サービスの解約ができるものとします。

（1） 利用者が加入の解約を申請した場合
（2） 利用者が本規程に違反し、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） 利用者に以下の事由が発生した場合
    a） 自ら振り出し、もしくは引き受けた手形・小切手が不渡になったとき、又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り消し、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、本規程の履行が困難と認められるとき
    d） 破産の申し立て、特別清算開始の申し立て、再生手続き開始の申し立て又は会社更生手続き開始の申し立ての事実が生じたとき
    e） 解散、合併又は営業の全部若しくは重要な一部の譲渡の決議をしたとき

f) 財産状態が悪化し又はそのおそれがあると認められる相当の事由があるとき
g) 第三者の支配下に実質的に入り、時刻配信局の利益を損なうと認められるとき

4.3. サービスの終了

（1）時刻配信局は以下の何れか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ものとします。
a) 本サービスの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の漏洩、偽造又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) 認証局が一時停止又は終了し、時刻配信局が本サービスを継続することが困難となった場合
d) 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 日前までに利用者に通知すると共に、リポジトリ上に公開します。ただし、緊急の場合は 180 日を待たずに本サービスを終了することができるものとします。

（3）本サービス終了後、速やかに全ての時刻配信サーバの秘密鍵を安全に廃棄するとともに、公開鍵証明書の失効申請を実施します。

（4）本サービス終了後、速やかに全ての個人情報を破棄します。

4.4. 準拠性監査

4.4.1. 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ものとします。また、時刻配信局は、必要に応じて定期監査以外に監査を実施します。

4.4.2. 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の中から監査業務に精通した者を任命するものとします。なお、時刻配信局は、必要に応じて外部の監査会社に監査を依頼します。監査人の任命は時刻配信局の責任者が行います。

4.4.3. 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として、時刻配信局および利用者の業務を直接担当しない者を選定するものとします。

4.4.4. 監査テーマ

本サービスが本規程に準拠して実施されていること、並びに適切な運用や不正アクセスに対する措置が適切に講じられていることを中心に監査を実施します。

4.4.5. 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ものとします。運用している時刻に異常が確認された時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ります。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ものとします。また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します。

4.4.6. 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ます。監査報告書の保存期間は、10 年間とします。

4.5. アーカイブ

4.5.1. アーカイブの種類

アーカイブデータは、次のものとします。なお( )内の年数は保管期間を表します。

（1） 月次報告書（10 年）
（2） 時刻配信局が発行した時刻監査記録（時刻監査証明書）（10 年）
（3） GPS-CV 方式によるUTC（NICT）との時刻比較データ（GGTTS データ）（10 年）
（4） 時刻配信局で使用する鍵ペアの生成・失効記録（10 年）
（5） 時刻配信局設備への入退室記録(3 年)
（6） GPS 受信機器、時刻配信サーバを含む時刻配信局システムに対する操作記録(3 年)
（7） 時刻配信局システムの動作異常の記録(3 年)
（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(3 年)
（9） 利用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（10 年）
（10）利用者の TSU の公開鍵情報、変更記録（10 年）

4.5.2. アーカイブデータの保護

時刻配信局は、アーカイブデータを、所定の方法・手順により改竄、削除、外部への流出等から保護します。また、温度、湿度、磁気などの環境を考慮して保管するものとします。

4.5.3. アーカイブデータの保管

時刻配信局は、アーカイブデータを 4.5.1 に定める保管期間を通じて可読な状態で保管します。

4.6. 鍵更新

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います。

4.7. 危殆化と災害からの復旧

4.7.1. 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の対処

時刻配信局は、本サービスに使用するハードウェア、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います。

4.7.2. 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処理を行いません。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利用者に通知します。

4.7.3. 秘密鍵が危殆化した場合の対処

時刻配信局は、時刻配信局の秘密鍵が危殆化した場合は、本サービスを停止し、次の手続を行います。

（1） 認証局に対して時刻配信サーバの公開鍵証明書の失効に関する申請手続き

（2） 時刻配信サーバの秘密鍵の破棄及び生成手続き
（3） 時刻配信サーバの新しい鍵に対する公開鍵証明書の発行申請手続き
（4） 利用者に秘密鍵の危殆化の通知

4.7.4. 災害等発生時の設備の確保

時刻配信局は、災害等により時刻配信局の設備が被害を受けた場合に備えて、予備機を確保し、災害等により時刻配信局の設備が被害を受けた場合にはバックアップデータを用いて復旧作業を行います。

4.8. UTC(NICT)との時刻同期

（1） 時刻同期管理
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±30 ミリ秒を越えないように管理します。

（2） うるう秒の設定
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、および利用者の TSU に対して、うるう秒の設定を実施します。

4.9. 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します。

（2） 利用者への時刻のトレーサビリティ
時刻配信局は、TSU に対して行った時刻監査の記録を保持することにより、TSU の時刻のUTC（NICT）に対するトレーサビリティを確保します。

5. 物理的、手続き的及び要員的なセキュリティ管理

5.1. 物理的管理

5.1.1. 施設の位置と建物構造

時刻配信局は、時刻配信局の施設を、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じます。また、時刻配信局は、本サービスに使用する機器等を災害及び不正侵入から防護された安全な場所に設置します。

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いません。

5.1.2. 物理アクセス

時刻配信局は、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します。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ものとします。また、時刻配信局は、時刻配信局の施設の入退室の記録を行います。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 日監視を行います。

5.1.3. 電源設備と空調設備

時刻配信局は、本サービスの施設電源について、定期的な検査を受け、システムに安定した電力を供給できるようにするものとします。また、空調設備を設置することにより機器類の動作環境及び要員の作業環境を適切に維持します。

5.1.4. 浸水対策

時刻配信局は、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、床には防水対策を行います。

5.1.5. 地震対策

時刻配信局は、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じます。

5.1.6. 火災対策

時刻配信局は、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、消火設備を備えます。

5.1.7. 媒体管理

時刻配信局は、本サービスのアーカイブデータ、バックアップデータを含む媒体を、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います。

5.1.8. 廃棄物処理

時刻配信局は、2.5.1 に定める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います。

5.1.9. 遠隔地バックアップ

時刻配信局は、本サービスに関する重要なデータ等の媒体を遠隔地で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います。

5.2. 手続きの管理

時刻配信局は、時刻配信サーバの起動・停止または時刻配信サーバの鍵の生成等の重要な業務の遂行にあたっては、それぞれの役割に対して信任された要員を設定するものとします。
操作員が本サービスのシステム操作を行う際、当該システムによって操作員が正当な権限者であることの識別・認証を行われます。また、時刻配信サーバの鍵の生成・更新等の重要操作は複数の要員が立ち会って行います。
時刻配信局は、本サービスの業務を委託する場合、当該委託先に本章の規定の遵守を求め、詳細手順書の作成とこれに沿った運用を実施させることで、本章に従った物理的、手続的及び人的なセキュリティの維持を図ります。

5.3. 要員の管理

5.3.1. 経歴、資格、経験及び必要条件

時刻配信局は、本サービスの実施にあたる要員について、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・配置を行うものとします。
時刻配信局は、本サービスの業務を委託する場合、当該委託先に本章の規定の遵守を求め、詳細手順書の作成とこれに沿った運用を実施させることで、本章に従った要員の管理を図ります。

5.3.2. トレーニング要件

時刻配信局は、本サービスの実施にあたる要員に対して、別途教育計画を定めトレーニングを実施します。

5.3.3. 追加トレーニングの頻度及び要件

時刻配信局は、本サービスの実施にあたる要員に対しては、初期的なトレーニングだけではなく、教育計画に基づき定期的に教育を行います。

5.3.4. 権限のない行為に対する制裁

本サービスの実施にあたる要員が、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、又は本規程又は本サービスに関する運用ルール、マニュアル若しくは手続に違反した場合、時刻配信局は時刻配信局における就業規則又はその他の規則若しくは雇用契約等に基づき懲戒を行います。

5.3.5. 担当者に提供される文書

本サービスの実施にあたる要員に対して、その要員の職務に必要な場合に以下の文書が時刻配信局より提供されます。

（1）時刻配信局の設備や機器のマニュアル類

（2）時刻配信局の運用に関する規程・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

時刻配信局は、時刻配信サーバの鍵ペアを、複数人立ち会いのもとで暗号モジュール（HSM）を用いて生成します。

6.1.2. 時刻配信サーバの公開鍵の認証局への登録

時刻配信局は、時刻配信サーバの公開鍵を所定の手続きにより認証局に登録し、公開鍵証明書の交付を受けます。

6.1.3. 認証局のルート証明書の受領

時刻配信局は、認証局から受領したルート証明書を、安全かつ確実に保管します。

6.1.4. 鍵のサイズとアルゴリズム

時刻配信局は、時刻配信サーバの鍵には RSA1024 ビットの鍵を使用します。暗号方式は公開鍵暗号方式の SHA-1 with RSA Encryption を使用します。

6.1.5. 鍵を生成するハードウェア/ソフトウェア

時刻配信局は、6.2.1 に定める基準を満たす暗号モジュール(HSM)を備えるものとします。

6.1.6. 鍵の利用目的

時刻配信サーバの鍵は、時刻配信局が発行する TAC への電子署名に使用します。

6.2. 秘密鍵の保護

6.2.1. 暗号モジュールに関する基準

時刻配信局は、時刻配信サーバの鍵を、FIPS（米国連邦情報処理標準）140-2 レベル 3 以上の認定を受けた暗号モジュール（HSM）を使用して生成・保管します。

6.2.2. 秘密鍵の複数人制御

時刻配信局は、時刻配信サーバの秘密鍵の生成、活性化、破棄を、複数人の管理の下で行います。

6.2.3. 秘密鍵の預託

時刻配信局は、時刻配信サーバの秘密鍵の預託は行いません。

6.2.4. 秘密鍵のバックアップ

時刻配信局は、時刻配信サーバの秘密鍵のバックアップは行いません。

6.2.5. 秘密鍵のアーカイブ

時刻配信局は、時刻配信サーバの秘密鍵のアーカイブは行いません。

6.2.6. 暗号モジュールへの秘密鍵の格納

時刻配信局は、時刻配信サーバの秘密鍵を、暗号モジュール（HSM）の中で生成・保管します。

6.2.7. 秘密鍵の活性化方法

時刻配信局は、時刻配信サーバの秘密鍵を、複数人の管理のもとで暗号モジュール(HSM)に活性化データを入力することにより活性化します。

6.2.8. 秘密鍵の非活性化方法

時刻配信局は、時刻配信サーバの秘密鍵を、暗号モジュール(HSM)に対して所定の操作を行うことにより非活性化します。

6.2.9. 秘密鍵の破棄方法

時刻配信局は、暗号モジュール（HSM）内の時刻配信サーバの秘密鍵を、複数人の管理のもとで所定の手続きに従い破棄します。

6.3. 公開鍵と秘密鍵の有効期間

時刻配信サーバの公開鍵証明書の有効期間は、有効とする日から起算して 73 箇月とします。ただし、時刻配信局は、暗号のセキュリティが脆弱になったと判断した場合、又はその可能性がある場合は鍵更新を行います。

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

時刻配信局は、時刻配信サーバの秘密鍵に対する活性化データを、所定の手続きに従って生成します。

6.4.2. 活性化データの保護

時刻配信局は、時刻配信サーバの秘密鍵に対する活性化データを、所定の規則に従って保護・管理します。

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、セキュリティに関する基準を設け、コンピュータ装置や時刻関連機器のハードウェアやソフトウェアの導入時にはこれを遵守するための確認を行います。

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情報等を定期的に収集し、問題があればセキュリティ基準に基づき再評価を実施します。再評価において問題が認められた場合は是正処置を行います。

6.6. システムのライフサイクル管理

6.6.1. システム開発面における管理

時刻配信局内で使用されるソフトウェアの開発、修正、変更にあたっては、時刻配信局は所定の品質管理基準を設け、これを遵守するよう制御された環境において作業を実施します。

6.6.2. システム運用面における管理

時刻配信局では、セキュリティに関する基準を設け、コンピュータ装置や時刻配信サーバ等のハードウェアやソフトウェアの導入時にはこれを遵守するための確認を行います。

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情報等を定期的に収集し、問題があればセキュリティ基準に基づき再評価を実施します。再評価において問題が認められた場合は是正処置を行います。

6.7. ネットワークセキュリティ

時刻配信局では、ネットワークセキュリティに関して基準を設け、システム導入時や変更時、運用時にこれを遵守するための確認を行います。

6.8. 暗号モジュールの技術管理

6.1.1 及び 6.2.1 において定めます。

7. SecureNTP 時刻配信サービス運用規程の管理

7.1. SecureNTP 時刻配信サービス運用規程の変更

時刻配信局は所定の手続きに基づき、本規程を必要に応じて変更します。

7.2. SecureNTP 時刻配信サービス運用規程の公開と通知

時刻配信局は、本規程を変更する場合、その適用開始日を明記の上、変更後の本規程をリポジトリに公開します。

本サービスの利用者に対しては、リポジトリに公開することをもって通知とします。

8. 時刻監査証明書のプロファイル

8.1. 時刻監査証明書の ASN.1 記述

時刻監査証明書の ASN.1 記述による定義情報を下記に記載します。

```
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

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE {
   extnID OBJECT IDENTIFIER,
   critical BOOLEAN DEFAULT FALSE,
   extnValue OCTET STRING
}
```

<属性情報 1>
name : TimingMetrics
OID : 1.3.6.1.4.1.601.10.4.1
syntax:

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

   BigTime ::= SEQUENCE {
      major INTEGER,
      fractionalSeconds INTEGER,
      sign INTEGER OPTIONAL
   }

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

<属性情報 2>
name : TimingPolicy
OID : 1.3.6.1.4.1.601.10.4.2
syntax:

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

<拡張情報 1>
name id-ce-authorityKeyIdentifier
OID { id-ce 35 }
syntax AuthorityKeyIdentifier
criticality MUST be FALSE

```
AuthorityKeyIdentifier ::= SEQUENCE {
   keyIdentifier [0] KeyIdentifier OPTIONAL,
   authorityCertIssuer [1] GeneralNames OPTIONAL,
   authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL
}
```

<拡張情報 2>
name id-ce-noRevAvail
OID { id-ce 56 }
syntax NULL (i.e. '0500'H is the DER encoding)
criticality MUST be FALSE

8.2. 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 directoryName	時刻監査証明書の所有者名
countryName type	時刻監査証明書所有者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6
value	国名の値 型：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 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 type	時刻監査証明書所有者の組織名 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：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 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
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：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 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：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 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	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

algorithm	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	時刻監査証明書の発行者
v2Form	バージョン２の記述形式
issuerName	時刻監査証明書の発行者名
directoryName	時刻監査証明書発行者の国名
countryName	国名のオブジェクト ID
type	型：OID 値：2 5 4 6
value	国名の値 型：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 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
organizationName	時刻監査証明書発行者の組織名
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：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 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
organizationalUnitName	時刻監査証明書発行者の部門名
type	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：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 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	時刻監査証明書発行者の固有名称
type	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：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 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	属性証明書の有効期間
notBeforeTime	開始日時 型：GeneralizedTime 値：YYYYMMDDHHMMSSZ
notAfterTime	終了日時 型：GeneralizedTime 値：YYYYMMDDHHMMSSZ
attributes	
[attribute: TimingMetrics] type value	属性情報 型：OID 値： 1 3 6 1 4 1 601 10 4 1
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：INTEGER 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：INTEGER 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：INTEGER 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：INTEGER 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：INTEGER 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：INTEGER 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：INTEGER 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：INTEGER 値：時刻監査証明書の有効期間の小数部
leapEvent leapTime	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
major	うるう秒設定日時の整数部 型：INTEGER 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：INTEGER 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
attributes	
[attribute: TimingPolicy]	属性情報
type	型：OID
value	値： 1 3 6 1 4 1 601 10 4 2
policyID	時刻監査証明書ポリシー 型：OID 値：時刻監査証明書ポリシーのＯＩＤの値
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：INTEGER 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：INTEGER 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：INTEGER 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：INTEGER 値：時刻監査規格（ネットワーク遅延）の小数部

（拡張領域）

extensions	
[Extension: authorityKeyIdentifier] extnID	時刻監査証明書発行者鍵識別子 型：OID 値：2 5 29 35
critical	型：BOOLEAN 値：FALSE
extnValue keyIdentifier	型：OCTET STRING 値：時刻監査証明書発行者の公開鍵証明書の公開鍵値に従う
authorityCertIssuer directoryName countryName type	時刻監査証明書発行者の公開鍵証明書の発行者名 公開鍵証明書の発行者の国名 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：時刻監査証明書発行者の公開鍵証明書の発行者名に従う
organizationName type	公開鍵証明書の発行者の組織名 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：時刻監査証明書発行者の公開鍵証明書の発行者名に従う 値：時刻監査証明書発行者の公開鍵証明書の発行者名に従う
organizationalUnitName type	公開鍵証明書の発行者の部門名 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：時刻監査証明書発行者の公開鍵証明書の発行者名に従う 値：時刻監査証明書発行者の公開鍵証明書の発行者名に従う
commonName type	公開鍵証明書の発行者の固有名称 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：時刻監査証明書発行者の公開鍵証明書の発行者名に従う 値：時刻監査証明書発行者の公開鍵証明書の発行者名に従う
authorityCertSerialNumber	型：INTEGER 値：時刻監査証明書発行者の公開鍵証明書のシリアル番号に従う

extensions	
[Extension: No Revocation Available] extnID critical extnValue	属性証明書の失効のサポート 型：OID 値：2 5 29 56 型：BOOLEAN 値：FALSE 型：NULL 値：NULL

（付録）　略語と用語解説

項目	説明
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。
公開鍵証明書（PKC）	Public-key certificate。 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。
RSA	大きな桁数の素因数分解が困難であることを利用した公開鍵暗号の方式の一つ。
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。
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 TST を発行するサーバ
タイムスタンプトークン(TST)	RFC3161 に準拠した様式に基づき、時刻認証局（TSA）によって電子署名された電子情報。
協定世界時（UTC）	Coordinated universal time。国際原子時（TAI）と地球の自転を基準とした世界時とのズレが 0.9 秒以上にならないように「うるう秒」で調整した時刻。
X.509	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。
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 ）。