認定タイムスタンプ byGMO
サービスポリシー及び運用規程

Date: December 16, 2024
Version: v1.1

文書変更履歴

バージョン	公開日	変更概要
v 1.0	2024 年 4 月 17 日	初版
v 1.1	2024 年 12 月 16 日	1.5　問合せ先 ・電話番号の変更

目次

1. はじめに

本サービスポリシー及び運用規程（以下「本 TP/TPS」という）は、GMO グローバルサイン株式会社(以下「グローバルサイン」又は「当社」という)が、時刻認証サービス（以下「本サービス」という）を利用者に提供するための運用に関する基本事項について規定するものです。

1.1. 概要

本 TP/TPS は、令和 3 年総務省告示第 146 号に基づき総務大臣により認定される時刻認証業務として、グローバルサインが本サービスを実施するための、運用方針及び業務手続を規定しています。本 TP/TPS は、本 TP/TPS によって規定する利用者、依拠当事者、及び第三者に適用されるものとします。

1.2. 識別

1.2.1. 文書名、版

ドキュメント名称：認定タイムスタンプ byGMO サービスポリシー及び運用規程
バージョン：v1.1
適用開始日：2024 年 12 月 16 日
作成者：GMO グローバルサイン株式会社

1.2.2. OID

本サービス
GlobalSign nv/sa(グループ共通) 1.3.6.1.4.1.4146
時刻認証局タイムスタンプポリシー群 1.3.6.1.4.1.4146.2
認定タイムスタンプ byGMO 1.3.6.1.4.1.4146.2.6

本時刻認証局が使用する時刻ソース
光テレフォン JJY サービスにより UTC(NICT)と時刻同期

本時刻認証局が使用する認証局のポリシー
GlobalSign nv/sa(グループ共通) 1.3.6.1.4.1.4146
CP/CPS 群 1.3.6.1.4.1.4146.1
Timestamping Certificates Policy 1.3.6.1.4.1.4146.1.30
Timestamping Certificates Policy - AATL 1.3.6.1.4.1.4146.1.31

1.3. 定義

1.3.1. 用語

認証局 (CA (Certificate Authority、Certification Authority))：デジタル証明書を発行する、信頼される第三者機関。

Coordinated Universal Time (UTC) ：協定世界時。原子時計に基づく時刻系であり、世界各国の標準時の基準となる時刻。

NICT (National Institute of Information and Communications Technology)：総務省所管の情報通信に係る国立研究開発法人であり、事業の一つとして、UTC(NICT)時刻の維持管理、配信を行う。

NTA(National Time Authority)：国家標準時を生成、維持、配信する機関。日本では NICT が役割を担う。

NTP(Network Time Protocol)：RFC 5905 で標準化された、ネットワークで接続された機器の時刻同期に用いる通信プロトコル。

利用者：タイムスタンプトークン発行を受ける法人又は自然人。利用者の義務を負う。

タイムスタンプ：文書やデータなどのデジタル情報に対し、信頼性の高い時刻を用い、そのデジタル情報がある時刻に存在し、以降、変更や改ざんなどされていないことを証明する技術。

時刻認証局 **(TSA(Time-Stamping Authority))**：信頼される第三者機関として、タイムスタンプサービスを提供し、タイムスタンプトークンを発行する機関。

タイムスタンプトークン **(TST(Time Stamp Token))：**文書やデータなどのデジタル情報に対し、信頼性の高い時刻を用い、そのデジタル情報が、ある時刻に存在し、以降変更や改ざんなどされていないことを証明、検証できる情報。デジタル情報を一意に特定するためのハッシュ値に対して、タイムスタンプトークンが発行される。タイムスタンプトークンには二種類の方式があり、独立トークン方式(又は PKI 方式)は ISO/IEC 18014-2、RFC 3161 として、リンク方式は ISO/IEC 18014-3 として標準化されている。本サービスでは独立トークン方式を用いている。

TSU (Time-Stamping Unit)：時刻認証局が一台以上持つ、タイムスタンプトークンを発行する装置。信頼される時刻ソースから時刻を取得し、タイムスタンプトークン内に埋込む機能を有する。

TP (Time-stamp policy)：タイムスタンプが特定集団のアプリケーションに対し、一般的なセキュリティ要件を充足した状態で適用されることを示す、一連のルール。

TPS (Time-stamp practice statement)：タイムスタンプサービス提供元が規定し実施する、タイムスタンプサービス運用手順。

リポジトリ：タイムスタンプサービスの提供に必要となる、本 TP/TPS や、検証に必要な情報などの情報を公開するためのデータの置き場所をいう。一般にウェブサイトの、ある URI が示す場所を指す。

1.3.2. サービス概要

本サービスは、指定されたデータに対して、信頼できる時刻による存在時刻証明、改ざん検知のためのタイムスタンプトークンを発行するサービスです。本サービスは以下に示す機能、特徴があります。

- 独立トークン方式(PKI 方式)によるタイムスタンプトークンを発行します。
- HTTP(S)上の RFC 3161 及び RFC5816 に準拠した通信プロトコル、フォーマットでタイムスタンプトークンを発行します。
- 本サービスは令和 3 年総務省告示第 146 号に基づき総務大臣による認定を受けた時刻認証業務即ちタイムスタンプサービスです。
- タイムスタンプトークンの署名アルゴリズムは、SHA256withRSA / SHA384withRSA を使用します。
- 利用者が指定したタイムスタンプ対象のデータの内容は、時刻認証局へは送信されず、ハッシュ値のみを送るため、時刻認証局はデータの内容について関知しません。
- タイムスタンプトークンに記載される時刻は TSU の内部時計を使用します。
- TSU が発行要求を受理した時刻や対象データが作成された時刻ではなく、実際にタイムスタンプが生成された時刻を表します。

- TSU の内部時計は UTC(NICT)の時刻とトレーサビリティを持つように同期し、UTC(NICT)に対して誤差±1 秒以内の精度あることを保証します。
- TSU の内部時計が、定められた誤差範囲を超えて異常がある場合には、TSU はタイムスタンプの発行を停止します。
- タイムスタンプトークンの有効期間は、タイムスタンプトークンを付与した時刻からトークンの署名に使用した TSA 証明書の有効期限までです。TSA 証明書の有効期間は TSA 証明書を発行する認証局の CP/CPS に準じます。

1.4. サービス関係者及びタイムスタンプトークンの適用範囲

1.4.1. サービス関係者

グローバルサインは本サービスの運営主体です。グローバルサインは時刻認証局として、データが存在した時刻をタイムスタンプにより証明する業務を行います。この業務には、UTC(NICT)の時刻とトレーサビリティのある時刻との同期、トークンへの電子署名、及びこれを行うための秘密鍵の管理が含まれます。

利用者とは、時刻認証局と利用契約を結び、時刻認証局よりデータのハッシュ値に対するタイムスタンプトークンを受領する法人又は自然人を指します。

依拠当事者とは、利用者から直接的、間接的にタイムスタンプトークン、又はタイムスタンプトークンを付与されたデータを受領し、それに依拠する法人又は自然人を指します。

1.4.2. タイムスタンプトークンの適用範囲

タイムスタンプトークンは、利用者が所持する電子データのハッシュ値に対して、当該ハッシュ値に対応する電子データが、タイムスタンプトークンに含まれる時刻の状態であること、及びその時刻以前に存在していたことを確認することを目的としています。利用者は上記の用途でのみタイムスタンプトークンを利用できます。また、利用者及び依拠当事者がタイムスタンプトークンの複製、配布をすることは可能です。

1.5. 問合せ先

GMO グローバルサイン株式会社
〒150-0043 東京都渋谷区道玄坂 1-2-3 渋谷フクラス 13 階

GMO GlobalSign K.K.
13th Floor SHIBUYA FUKURAS 1-2-3, Dogenzaka, Shibuya-Ku, Tokyo 150-0043, JAPAN

e-mail アドレス： support-jp@globalsign.com
電話番号：+81 3 4545 1800

顧客サポート窓口営業時間：平日 月～金曜 10:00～18:00 (日本時間)
休業日：土日祝日、年末年始

2. 一般規定

2.1. 義務

2.1.1. 時刻認証局の義務

(1) 時刻認証局は、本 TP/TPS に基づきタイムスタンプトークンを生成し利用者に発行するサービスを提供します。

(2) 時刻認証局は、UTC(NICT)とトレーサビリティのある信頼できる時刻ソースから時刻を取得し、発行するタイムスタンプトークンの時刻が「4.6.1. 時刻の同期及び精度」に規定する誤差を超えないようシステムの時刻管理を行います。

(3) 時刻認証局は、「6.1 . 鍵の管理」の規定に基づき鍵を安全に管理し、各種ブラウザベンダー/アプリケーションサプライヤーより信頼を受けているパブリック認証局より証明書の発行を受けます。

(4) 時刻認証局は、本サービスを提供するためのシステムを安全に維持管理します。

(5) 時刻認証局は利用者に対し、タイムスタンプトークンの有効期間、公開情報への変更、セキュリティイベント等につき、必要な通知、告知を行います。

2.1.2. 利用者の義務

(1) 利用者は、本 TP/TPS、利用約款を承諾した上で、本サービスの提供を受けるものとします。

(2) 利用者は、本 TP/TPS を遵守すると共に、タイムスタンプトークンを複製・配布する場合は、その利用者に対して本 TP/TPS を遵守させなければなりません。

(3) 利用者は、サービス利用の申請などに際し、正確な情報を時刻認証局に提示するものとします。

(4) タイムスタンプの付与対象となる電子データの保存期間内にタイムスタンプの有効期間が満了する場合、利用者は当該有効期間内にタイムスタンプを再付与するために申請する必要があります。

(5) 利用者は、リポジトリ又は時刻認証局からの通知情報を定期的に収集しなければなりません。

(6) 利用者は、利用申込書に記載した利用者情報に変更が生じた際には、速やかにその変更内容を書面で当社に通知するものとします。

2.1.3. 依拠当事者の義務

(1) 依拠当事者は、タイムスタンプへの依拠にあたり、タイムスタンプが正しく署名され、その署名に用いられた証明書が現時点で有効であることを確認しなければなりません。

(2) 依拠当事者は、タイムスタンプの使用にあたり、本 TP/TPS が規定する利用制限を遵守しなければなりません。

(3) 依拠当事者は、タイムスタンプの使用にあたり、その他の規約に規定する義務を遵守しなければなりません。

2.1.4. 認証局の義務

認証局は、時刻認証局に対して、総務大臣による時刻認証業務の認定に関する規程に定める義務を負います。

2.1.5. リポジトリに関する義務

時刻認証局は、本サービスに関する情報のうち公開する情報を、「2.5. 公開とリポジトリ」に定める方法でリポジトリに公開するものとします。

2.2. 責任

2.2.1. 時刻認証局の損害賠償責任

本サービスにおいて当社が「2.1.1 時刻認証局の義務」に違反して発生した損害について損害賠償責任を負う場合、その範囲は利用約款の規定に従うものとし、いかなる場合においても当社は、この賠償額の上限を超える責任を負うものではありません。

2.2.2. 利用者の責任

利用者が「2.1.2. 利用者の義務」に違反したことにより当社が損害を被った場合、当社は利用者に対して当該損害の賠償を請求することができるものとします。

2.2.3. 免責事項

(1) 本認定サービスは、有効期間を満了したタイムスタンプの信頼性を裏付けるものではありません。

(2) 時刻認証局が発行したタイムスタンプトークンを利用者が使用する場合、タイムスタンプ対象となった電子データと付与されたタイムスタンプトークンを使用した結果について、当社は何ら責任を負わないものとします。

(3) 当社は、利用者が本サービスを使用するにあたり、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免責されます。

(4) 当社は、当社の責に帰することができない事由から生じた損害、及び、予見の有無を問わず、特別な事情から生じた損害については免責されます。

(5) 利用者はタイムスタンプトークンを、フェイルセーフ機能を必要とする用途や人命にかかわる機能、及び法により禁じられている用途には使用しないものとします。

(6) その他の免責事項及び賠償責任の限定については利用約款に従うものとします。

2.3. 解釈及び執行

2.3.1. 可分性

本 TP/TPS のある規定又は一部を含むその適用が、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には、当該規定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、適用されます。

2.3.2. 存続性

本 TP/TPS の「2.2. 責任」「2.3. 解釈及び執行」「2.6. 機密保持」「2.7. 知的財産権」「2.8. 個人情報の取り扱い」は、時刻認証局による本サービスが終了し、本 TP/TPS が廃止された後にも有効に存続します。

2.3.3. 通知

(1) 利用者から時刻認証局への通知

書面又は電子メールにて「1.5 問合せ先」に記載された連絡先で受け付けます。通知は受領日をもって有効とします。

(2) 時刻認証局から利用者および検証者への通知

時刻認証局は利用者より届け出がなされている連絡先にメール等により通知を行います。また、公式ホームページのお知らせを通じて利用者および検証者に通知します。

2.3.4. 準拠法及び裁判管轄

本 TP/TPS の解釈及び適用等は、日本法に準拠します。本 TP/TPS 又は本サービスに関して生じた一切の紛争については、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。

2.4. 料金

別途、本サービスの料金表にて定めるものとします。

2.5. 公開とリポジトリ

2.5.1. 時刻認証局に関する情報の公開

時刻認証局は、以下の情報を「2.5.4. リポジトリ」 に定めるリポジトリに公開します。

(1) 時刻認証局運用規程(本 TP/TPS)
(2) 公開鍵証明書情報
(3) 告知情報(公開鍵証明書失効情報を含む)
(4) 検証に必要な情報
(5) 利用約款およびサービス利用の注意事項

2.5.2. 公開の時期及び頻度

時刻認証局は公開情報につき、本 TP/TPS 変更時、又は時刻認証局の責任者が必要と判断した時に、随時更新するものとします。

2.5.3. リポジトリのアクセス管理

時刻認証局リポジトリで公開する情報は、インターネットを通じて提供します。権限のない者によるリポジトリの内容への追記、消去、又は改変を防ぐための、論理的及び物理的セキュリティ対策を実施します。

2.5.4. リポジトリ

「2.5.1. 時刻認証局に関する情報の公開」において定める情報を下記リポジトリに公開します。
URL　https://jp.globalsign.com/repository/

2.6. 機密保持

2.6.1. 機密情報

時刻認証局及び利用者は、本サービスに関連して相手方より提供を受けた技術上、営業上その他業務上の情報を機密情報とします。時刻認証局は機密情報を、管理責任者を定め取扱者を制限し、漏洩した場合の影響を考慮しながら安

全に保管管理します。機密情報は、本 TP/TPS 又は利用約款に定められている場合を除いて、いかなる第三にも原則として開示してはならず、また、サービスの目的の範囲を超えて使用してはならないものとします。また、発行したタイムスタンプが有効である期間、対象となる機密情報を最低限保管し、その後削除します。

以下の情報は機密情報に含まれるものとします。

(1) 申し込みに関する記録
(2) 時刻認証局が保管するセキュリティ検査ログ
(3) 不測の事態に対応する計画及び実行措置
(4) ハードウェア及びソフトウェアの運用、並びに時刻認証局の運営についてのセキュリティ対策
(5) 時刻認証局が利用者に提供した利用者を識別するための情報

利用者は、本サービスの利用にあたり時刻認証局から提供された利用者を識別するための情報を開示、漏えいしてはなりません。

2.6.2. 機密情報の例外

2.6.1. の規定にかかわらず、時刻認証局および利用者は、次に定める情報を機密情報とはしません。

(1) 本 TP/TPS、公開鍵証明書、失効情報等、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) 第三者から適法に入手し、かつ機密保持義務を負っていない情報。
(5) 開示者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。
(6) 被開示者が開示された情報によらずに独自に開発した情報。

2.6.3. 法執行機関への情報開示

時刻認証局で扱う全ての情報に対し、裁判所又は政府機関から法的根拠に基づく情報開示の請求があった場合は、時刻認証局は、法で定められた範囲内で当該情報を開示します。

2.6.4. 委託先に対する情報開示

時刻認証局は、業務の一部を第三者に委託するために業務委託先に機密情報を開示する場合は、業務委託先に対し委託契約の中で当該情報の守秘を義務付けるものとします。

2.7. 知的財産権

以下の各号に定めるものを含む、時刻認証局又はライセンサーが作成した文書、データ、プログラム等は、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、時刻認証局又は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) 時刻認証局から発行されたタイムスタンプトークン
(2) 時刻認証局が提供するタイムスタンプトークンを扱うソフトウェア
(3) 本 TP/TPS
(4) 商標、標章、標識及びその他のマーク

2.8. 個人情報の取り扱い

本サービスで取り扱う個人情報の取得、利用、管理、保存、破棄および開示は弊社のプライバシーポリシー (https://www.globalsign.co.jp/policy/privacy_translated.html) に従います。

保存については「4.5. アーカイブ」もご覧ください。

3. 識別及び認証

時刻認証局は、サービスの加入、利用、更新、解約に際し、本サービスの利用申請者又は利用者の情報を確認します。サービス利用条件については利用約款に準じます。

4. 運用規則

4.1. サービス提供時間

時刻認証局は以下の場合を除き、24 時間 365 日のサービス提供を行います。

(1) 予め通知したサービスメンテナンス期間
(2) 緊急メンテナンス時
(3) うるう秒処理時

4.2. サービスの利用

4.2.1. タイムスタンプトークンの発行

時刻認証局は、利用者の要求があった場合、タイムスタンプ要求が正しく受理されたか否かの状態を返答します。タイムスタンプ要求が正常に処理された場合には、時刻認証局は利用者の要求に応じて、時刻認証を行いたいデータに対して時刻情報及び改ざんを検知する為にデジタル署名を施したタイムスタンプトークンを利用者に発行します。ハッシュ関数には、SHA256 もしくは SHA384 を使用します。

4.2.2. タイムスタンプトークンの検証

タイムスタンプトークン、又はこれを含むデータを受領し、タイムスタンプトークンの有効性を確認する必要がある者は、タイムスタンプの対象となったデータのハッシュ値との照合及び、タイムスタンプトークンに施されたデジタル署名の検証が必要となります。一般にはタイムスタンプの検証ツールをもちいて検証します。

(1) タイムスタンプのデータ形式の崩れの判別

タイムスタンプのデータ形式は RFC 3161 タイムスタンププロトコルの TimeStampToken というバイナリ形式の ASN.1 データ構造として定義されています。TokeStampToken の ASN.1 文法に従っているかを解析することによりデータ形式の崩れが判別できます。

(2) タイムスタンプに TSA 証明書が含まれない場合の証明書一式の取得

タイムスタンプ要求で証明書チェーンを含めるフラグを設定した場合には、トークンには TSA 証明書からルート証明書までの証明書チェーンが含まれていますが、これをオフにした場合には含まれません。その場合には、リポジトリより証明書一式をダウンロードして取得します。

(3) TSA 証明書の有効性の検証

RFC 5280 6 章 認証パス検証で規定された方法により TSA 証明書、中間 CA 証明書、ルート証明書の証明書チェーンの有効性を確認します。検証対象データに利用可能な失効情報が含まれない場合には、証明書に記載された情報を用いて取得し失効検証します。また、TSA 証明書がタイムスタンプの発行に使用可能な証明書かを追加で検証します。

(4) TSA 証明書によるタイムスタンプのデータ形式の改ざんの判別

TSA 証明書を用いて RFC 5652 CMS SignedData であるタイムスタンプの署名フォーマットの署名を検証します。

(5) タイムスタンプ対象となる電子データの改ざんの判別

上記を以て、タイムスタンプ自体の有効性が確認できます。次にタイムスタンプに記載された対象データのハッシュ値と、対象データのハッシュ値が一致していた場合、タイムスタンプが対象データのためのタイムスタンプであることが確認でき、タイムスタンプの記載時刻に対象データが改ざんなく存在していたことが証明できます。

4.3. サービス監査

4.3.1. サービス監査の目的

本サービスが「時刻認証業務の認定に関する実施要項」および本 TP/TPS に沿って運用されていること、並びに運用、及びセキュリティ問題に対する措置が適切に講じられていることを中心に確認するために、サービス監査を実施します。

4.3.2. サービス監査人の適格性

時刻認証局のサービスに関する監査人は、当社の監査業務及び認証業務、並びに総務大臣による時刻認証業務の認定に関する規程に精通した者の中から選出されます。当該サービス監査人は、時刻認証局の責任者が任命し、必要に応じて外部の監査人より選出されることがあります。

4.3.3. サービス監査人と被監査部門との関係

サービス監査人は、時刻認証局の業務を行う部門より独立しています。

4.3.4. サービス監査の頻度

監査は年一回定期的に実施します。また、必要に応じて定期監査以外に監査を実施します。

4.3.5. サービス監査における指摘事項への対応

サービス監査における指摘事項に対して、時刻認証局の責任者は、判断に基づき計画を立て、対応し、指摘事項の改善確認をするものとします。時刻認証局は、重要又は緊急を要する深刻な問題の指摘がある場合、速やかに改善措置を講じます。

4.3.6. サービス監査結果の報告

サービス監査結果は、サービス監査人より時刻認証局の責任者及び認定機関に対し、監査報告書として提出されます。

4.4. 時刻モニター

時刻認証局の TSU の内部時計は、時刻モニター装置により、UTC(NICT)とトレーサビリティのある時刻との誤差を測定、監視します。

4.5. アーカイブ

4.5.1. アーカイブする情報の種類

アーカイブデータは次の各号に掲げるものとします。なお、括弧内は最低保管期間を表します。

(1) UTC(NICT)との時刻同期、時刻比較結果等、TST に付与される時刻の品質を保証する記録 (135 か月)
(2) 時刻認証局で使用する鍵ペアの生成、更新、廃棄、失効の記録 (135 か月)
(3) タイムスタンプ生成に関する全情報 (135 か月)
(4) サービス監査報告書 (135 か月)
(5) その他、時刻認証業務の運用に関する重要な記録 (135 か月)

4.5.2. 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じ完全性及び機密性を確保し保管します。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、適切な入退室管理室内に設置された、温度管理、湿度管理、磁気対策が行われている施錠可能な場所に保管します。

4.5.3. アーカイブデータの開示

時刻の品質を保証する記録は、利用者の求めに応じて「2.3.3 通知」に基づき開示します。

4.6. その他の運用規則

4.6.1. 時刻の同期及び精度

(1) TSU の時刻精度

時刻認証局は時刻認証局の使用する全ての TSU の時刻精度を UTC(NICT)に対して±1 秒以内に維持します。

(2) 時刻のトレーサビリティ

時刻認証局の使用する時刻サーバーは光テレフォン JJY サービスにより、十分小さな誤差で UTC(NICT)に追従するようなトレーサビリティを有します。時刻モニター装置は、時刻認証局が運用する全ての TSU に対して

UTC(NICT)との誤差が本 TP/TPS で定められた精度以内であるかどうかの時刻監視を行うことで、タイムスタンプの時刻のトレーサビリティを確保します。

(3) 時刻品質情報の公開

時刻認証局は、時刻品質の信頼性に関する情報として、UTC(NICT)とトレーサビリティのある時刻と TSU との時刻差をモニタリングし、Web 等を用いて定期的に公開します。

(4) うるう秒前後の計画停止

TSU 時計と UTC(NICT)との時刻同期を維持するために、うるう秒が発生した場合でもこれを考慮した時刻調整を行いません。うるう秒発生の前後で計画メンテナンスによりサービスを一時停止し、問題ないことを確認した上でサービスを再開します。

4.6.2. 暗号アルゴリズム危殆化への対応

(1) 暗号アルゴリズムの危殆化が予測される場合

タイムスタンプ生成に使用される暗号アルゴリズムが、タイムスタンプトークンの有効期間内に危殆化することが予測された場合、タイムスタンプの発行停止及び失効について計画を策定し関係者に事前周知します。TSA 証明書を失効申請し、既存のものより強化された暗号アルゴリズムを適用した TSA 証明書を再発行します。新しいタイムスタンプに更新することで有効性が維持されることを関係者に周知します。

(2)暗号アルゴリズムが危殆化した場合

予測無くタイムスタンプ生成に使用される暗号アルゴリズムが危殆化した場合、タイムスタンプの発行を停止し、TSA 公開鍵証明書の失効手続きを行います。既存のものより強化された暗号アルゴリズムが適用した TSA 証明書を再発行します。新しいタイムスタンプに更新することで有効性が維持されることを関係者に周知します。

4.6.3. サービス中断及び停止

時刻認証局がサービスを中断、終了、業務移管する際には、そのスケジュールと手続きを定め、内容を所定の手段で利用者、依拠当事者、CA、再販者、及びその他の関係者へ告知、周知、報告します。この過程において、秘密鍵は安全な方法にて保存、破棄、又は転送されます。

4.6.4. インシデント対応

(1) 時刻精度障害

TSU の時刻精度が「4.6.1 時刻の同期及び精度」の規定の範囲外となった場合、当該 TSU によるタイムスタンプトークンの発行は自動停止され、問題解決後に復旧させます。

(2) ハードウェア、ソフトウェア、ネットワーク、データ障害

ハードウェア、ソフトウェア、ネットワーク、データの障害が発生した場合、復旧作業を行います。必要に応じ、バックアップデータ、予備機を使用し復旧します。

(3) サービス障害

サービスを構成する多くの要素が冗長構成を採用しており、単一障害ではサービス提供に影響が無い構成となっていますが、サービスの提供に支障が生じた場合には、速やかに復旧にあたると共に、「2.3.4. 通知」に基づき関係者へ障害の報告を行います。

(4) 秘密鍵の危殆化

タイムスタンプユニットが使用する秘密鍵が危殆化した場合、当該ユニットの使用を停止し、認証局に対して紐づく TSA 証明書の失効を申請し、当該ユニットの秘密鍵を廃棄・再生成し、認証局に対して新しい鍵の TSA 証明書の再発行を申請する。利用者に対して秘密鍵の危殆化を通知する。

4.6.5. 災害対応

時刻認証局の設備が災害等により被害を受け、サービス提供に影響が出た場合、速やかに所定の手段で告知、周知するとともに、予備機を確保しバックアップデータを用いてサービスを復旧します。

5. 物理的セキュリティ

5.1. 物理的セキュリティの管理

5.1.1. 施設の所在地及び建築構造

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、水害など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対策が講じられた建造物の区画に設置します。

5.1.2. 施設への物理的アクセス

時刻認証局の区画及び設備へのアクセスは、あらかじめ許可された人員のみが可能となるように制限され、入退室や設備のアクセスを記録管理します。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。

5.1.3. 電源及び空調設備

時刻認証局施設の一次電源は電力会社より複数系統の供給を受けます。施設には無停電電源装置が配備されており、停電時には備蓄燃料により電源が供給されます。瞬断は UPS 設備により防止します。空調設備は冗長構成で運転され、機器の動作環境を適切に維持されます。

5.1.4. 水害対策

時刻認証局の施設は防水対策施され、常時監視されています。

5.1.5. 地震対策

時刻認証局の施設は免震及び耐震対策が施されています。ラックは転倒防止のため床にアンカーで固定され、機器はラックに固定されています。配線も地震の影響がないいよう配慮しています。

5.1.6. 火災対策

時刻認証局の設備を設置する建物は耐火構造、区画は防火区画となっています。また、消火設備を備えています。

5.1.7. 記憶媒体の管理

アーカイブデータ、バックアップデータを含む媒体は、適切な入退室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され、所定の手続き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

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、所定の手続きに基づいて適切に廃棄処理を行います。

5.2. 手続き上のセキュリティ管理

時刻認証局の業務の実施に当たっては、要員の及び関係組織との職務権限を分離して、相互牽制を行います。

(1) 認証局と時刻認証局

認証局は、時刻認証局の TSU を特定、認証するための公開鍵証明書を発行します。認証局は公開鍵証明書の発行業務について第三者監査されており、不正に公開鍵証明書が発行できない仕組みとします。当社内において、認証局業務と時刻認証局業務の、部署及び要員は分離されています。

(2) サービス監査人と時刻認証局の要員

当社においてサービス監査人は、監査の専門知識を持ち、時刻認証局の要員とは別の部署であり、第三者として内部監査を行います。

(3) 鍵管理者

「6.1. 鍵の管理」を行う鍵管理者は、鍵の操作、管理において、必ず複数人立ち会いにより実施され、相互牽制されています。

5.3. 要員のセキュリティ

5.3.1. 経歴及び適格性

時刻認証局の業務に従事する要員については、従事させる業務毎に、必要な専門知識、実務経験、公的資格、人事部門で保有する情報を元に、当該業務への従事に適格であるか確認を行った上で任用します。また、信頼性を確認するための経歴検査を行った上で任用します。

5.3.2. 教育訓練及びその頻度

時刻認証局の業務に従事する要員に対して、業務の種類に応じて別途定められた教育計画を基に、初期及び定期に教育訓練を実施します。

5.3.3. 職務分掌

時刻認証業務における各種権限は、各人員に対しその責務・役務に応じてのみ最低限付与されるものとします。これらの権限へは定期的に見直しがなされます。

5.3.4. 権限のない行為に対する懲罰

時刻認証局の業務に従事する要員が、規定された権限を逸脱して違反を行った場合には、就業規則、契約等に基づき処罰を行います。

5.3.5. 要員に提供される文書

時刻認証局は要員に対し、業務に必要となる運用規定、マニュアル、手順書等を提供します。

6. 技術管理

6.1. 鍵の管理

時刻認証局はタイムスタンプトークンのデジタル署名に用いる鍵について、以下のように管理します。

6.1.1. 鍵ペアの生成

(1) 鍵ペア生成

TSU の鍵ペアは、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。

(2) 鍵ペアは モジュラス 2048 bit 以上の RSA 公開鍵暗号方式 の鍵を使用します。

(3) TSU の公開鍵証明書の取得と保管

所定の手続きにより、認証局から当該鍵ペアに対し、タイムスタンプトークンの署名に用いる公開鍵証明書、ルート証明書、中間証明書を取得し、安全に保管します。

6.1.2. 秘密鍵の保護

(1) 暗号モジュールに関する基準

TSU の鍵を FIPS(米国連邦情報処理標準)PUB 140-2 レベル 3 以上又は ISO/IEC 15408 EAL4+以上の認定された暗号モジュール(HSM)により生成、保護します。

(2) 秘密鍵の複数人制御

TSU の秘密鍵の生成、活性化、廃棄等は複数の鍵管理者の下で行い、その操作を記録します。

(3) 秘密鍵の預託

秘密鍵の預託は行いません。

(4) 秘密鍵のバックアップ

秘密鍵のバックアップは行いません。

(5) 秘密鍵のアーカイブ

秘密鍵のアーカイブは行いません。

(6) 暗号モジュールへの秘密鍵の格納

TSU の秘密鍵は、暗号モジュール内で生成、保管されます。

(7) 秘密鍵の活性化方法

暗号モジュール内の秘密鍵の活性化は、複数の鍵管理者の下で所定の操作により行います。

(8) 秘密鍵の非活性化方法

暗号モジュール内の秘密鍵の非活性化は、適切な鍵管理者の下で所定の操作により行います。

(9) 活性化データの生成

時刻認証局は、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します。

(10) 活性化データの保護

時刻認証局は、秘密鍵を格納する暗号モジュールの活性化に必要な情報を安全に管理します。

6.1.3. 秘密鍵の利用及び管理

(1) 秘密鍵の利用

タイムスタンプトークンのデジタル署名に用いる秘密鍵はタイムスタンプ専用のもので、これ以外に使用することはありません。秘密鍵を用いたデジタル署名は、暗号モジュール内で実施します。

(2) 秘密鍵の使用期間と公開鍵証明書

秘密鍵の活性化期間(使用期間)は 15 か月以内とし、活性化期間(使用期間)満了前に新しい鍵ペアに鍵更新し、合わせて公開鍵証明書も更新します。認証業務の廃止、秘密鍵の危殆化、暗号アルゴリズムの危殆化が発生した場合には、公開鍵証明書の失効手続きを行います。

(3) 鍵の更新

時刻認証局は定められた期間(15 か月以内)ごとに定期的に鍵ペアの更新を行います。この際、公開鍵証明書は失効されません。利用している暗号アルゴリズムが危殆化した、又は不適切となった場合は、関係する秘密鍵が全て更新されます。

(4) 鍵の廃棄

時刻認証局は、必要な期間が終了した鍵、失効した鍵、危殆化した鍵、また利用終了となる機器に保存された鍵等を、所定の手順で安全に廃棄します。定期的に更新する秘密鍵については、更新後に廃棄するものとします。暗号モジュール内の秘密鍵の廃棄は、適切な鍵管理者の下で所定の操作により行います。

また、時刻認証局の電子証明書を発行する認証事業者が失効に係る認証業務を継続せずに認証業務を終了する場合には、認証事業者の認証業務終了までに、暗号モジュール内の秘密鍵の廃棄を、時刻認証局の秘密鍵を複数人の鍵管理者の下で所定の操作により行います。

6.2. 機器及びネットワークの管理

6.2.1. 使用する機器及びネットワークの要件

時刻認証局を構成する装置やソフトウェア、ネットワークは、所定のセキュリティ基準を満たす製品、設定、システム構成を使用します。

6.2.2. 機器及びネットワークへのセキュリティ調査

時刻認証局では、構成するシステム及びネットワーク全体のセキュリティに関する情報収集、脆弱性評価を行い、問題がある場合には所定のセキュリティ基準に基づき対応と再評価を実施します。システム及びネットワーク構成が変

更された場合にも、同様の手続きを実施します。タイムスタンプトークン生成を行うプログラムへ変更を行う場合には、認定機関に報告し確認をとります。脆弱性指摘やセキュリティインシデントが発生した場合には、速やかに対応します。

6.3. システムのライフサイクル管理

タイムスタンプトークン生成を行うシステムやプログラムへの変更・操作は複数人制御の下に行います。

6.3.1. システム開発の管理

時刻認証局は、使用されるシステム、ソフトウェアの開発、修正、変更にあたり、所定の品質管理基準を満足するよう、制御及び管理された環境において作業を実施します。

6.3.2. システム運用の管理

時刻認証局では、システム運用に関する規定、基準を設け、これに基づき、運用管理、維持管理、保守、監視を行います。

6.3.3. セキュリティ運用の管理

時刻認証局は、サービス導入前、システム構成もしくはサービス運用の変更時、及び定期的に所定の規定、基準に基づき、セキュリティの確認、評価を行います。

6.4. 暗号モジュールの管理

「6.1 鍵の管理」で定めます。

7. サービスポリシー及び運用規程の管理

7.1. サービスポリシー及び運用規程の変更管理

時刻認証局は所定の手続きに基づき、必要に応じて本 TP/TPS を変更します。

7.2. サービスポリシー及び運用規程に関する通知及び公開

本 TP/TPS を変更する際には、適用開始日より前に適用日を明記の上、リポジトリに事前に公開し、登録された利用者の連絡先に通知します。

8. タイムスタンプトークンのプロファイル

フィールド	内容	値
TimeStampToken		
ContentInfo		CMS SignedData構造
ContentType	CMSフォーマットの種別OID	id-signedData 1.2.840.113549.1.7.2
Content		SignedData構造
version	SignedData構造のバージョン	3 (使用するeContent, sid, certificates, revocationInfosの型により)
digestAlgorithms	署名で用いるハッシュアルゴリズム群	SHA256
encapContentInfo	署名対象データ	
eContentType	署名対象データの種類	id-TSTInfo 1.2.840.113549.1.9.16.1.4
eContent	署名対象データ	TSTInfo構造 (下記参照)
certificates	署名に使われる証明書群(オプション)	タイムスタンプ要求にcertReqがある場合に存在
certificate[0]		TSA証明書 GlobalSign Japan Accredited Timestamping AxxxPx-xxx
certificate[1]		中間CA証明書(オプション) GlobalSign R45 AATL TimeStamping Root CA 2021
certificate[2]		ルート証明書(オプション) GlobalSign Timestamping Root R45
signerInfos	署名情報リスト	
signerInfo[0]	TSA証明書による署名情報	
version	signerInfoのバージョン	1 (sidにIssuerAndSerialNumber形式を使用)
sid	署名者証明書識別情報	署名者証明書(=TSA証明書)の識別情報
issuer	発行者識別名	TSA証明書の発行者識別名
serialNumber	証明書シリアル番号	TSA証明書のシリアル番号
digestAlgorithm	eContentを識別するハッシュアルゴリズム	SHA256
signedAttrs	署名される属性(以下、属性と値)	
contentType	eContentTypeの属性	id-TSTInfo 1.2.840.113549.1.9.16.1.4
messageDigest	eContent(=TSTInfo)のハッシュ値	
signingTime	トークンの生成されたTSAが保証しない時刻	YYYYMMDDHHMMSSZ形式のUTC時刻の文字列
signingCertificateV2	署名者証明書(=TSA証明書)の識別情報	
hash	証明書ハッシュ値	TSA証明書のSHA256(デフォルト)ハッシュ値
issuer	発行者識別名	TSA証明書の発行者識別名 GlobalSign R45 AATL TimeStamping Root CA 2021
serial	証明書シリアル番号	TSA証明書のシリアル番号
signatureAlgorithm	署名アルゴリズムor暗号アルゴリズム	SHA256withRSA
signature	signerInfoの署名値	signerInfoの署名値
TSTInfo		
version	TSTInfoのバージョン	1
policy	TSAのポリシーOID	認定タイムスタンプ byGMOのTSAポリシーOID (JP Accredited Timestamping Tokens - AATL) 1.3.6.1.4.1.4146.2.6
messageImprint	要求に含まれたタイムスタンプ対象情報	タイムスタンプ要求に含まれる情報の写し
hashAlgorithm	タイムスタンプ対象情報の 識別に使うハッシュアルゴリズム	SHA256/SHA384/SHA512をタイムスタンプ要求で受理
hashedMessage	タイムスタンプ対象情報のハッシュ値	
serialNumber	タイムスタンプトークンのシリアル番号	16バイト (トークン毎に発行)
genTime	時刻認証を行ったUTC時刻	YYYYMMDDHHMMSSZ形式のUTC時刻の文字列
accuracy	時刻精度	1秒
ordering	順序性を表すフラグ	フィールドなし (即ち要求に対する順序性を保証しない)
nonce	ノンス	要求に含まれる場合、その値の写し
tsa	TSA識別名	TSA証明書の主体者識別名 GlobalSign Japan Accredited Timestamping AxxxPx-xxx
extensions	拡張領域	フィールドなし