経済産業省委託調査

平成１４年度ＥＣ技術基盤の相互運用性に関する調査研究事業

（電子署名生成・検証システムのセキュリティ環境の国際標準化等の調査）

タイムスタンプサービス調査

報　告　書

平成15年３月

電子商取引推進協議会
財団法人日本情報処理開発協会
電子商取引推進センター

この報告書は、平成１４年度受託事業として（財）日本情報処理開発協会電子商取引推進センターが経済産業省から委託を受けて、電子商取引推進協議会（ECOM）の協力を得て実施した「平成１４年度ＥＣ技術基盤の相互運用性に関する調査研究事業（電子署名生成・検証システムのセキュリティ環境の国際標準化等の調査）」の成果を取りまとめたものです。

はじめに

タイムスタンプは、その電子文書がタイムスタンプ生成時刻以前に確かに存在した事を証明(存在証明）すると共に、その当時の状態を保持していることを証明（完全性証明）することができる。電子署名文書の長期保存にタイムスタンプは不可欠であり、タイムスタンプサービスが高い信頼を得て長期にわたりそのサービスを継続し、社会インフラとして広く認められることは、非常に重要である。

現在、ワールドワイドに複数の時刻源が存在しており、既に、幾つかのタイムスタンプサービスが提供され始めた。

本報告書では、国内における時刻源やタイムスタンプサービスの具体的事例を調査すると共に、タイムスタンプ局の運用規定に関する海外の検討状況や、タイムスタンププロトコルの標準化動向を調査した。

本報告書が、日本企業・各機関の方々にとって、タイムスタンプの理解の一助になれば幸いである。

平成 15 年 3 月

財団法人日本情報処理開発協会
電子商取引推進センター
電子商取引推進協議会

目　次

はじめに

1　タイムスタンプサービスの現状……1
1.1　通信総合研究所における日本標準時の供給　（独立行政法人　通信総合研究所）……1
1.1.1　通信総合研究所の役割……1
1.1.2　サービス概要……1
1.1.3　電子時刻認証システム開発……3
1.1.4　今後の展開……4
1.2　クロノトラスト（セイコーインスツルメンツ株式会社）……5
1.2.1　サービス概要……5
1.2.2　シンプル・プロトコル（RFC3161）……10
1.2.3　サービスの利用イメージ……10
1.2.4　今後の展開……13
1.3　SecureSeal（NTTデータ）……15
1.3.1　サービスの概要……15
1.3.2　リンキングプロトコル……16
1.3.3　サービスの利用イメージ……17
1.3.4　今後の予定……21
1.4　e-timing　（アマノ株式会社）……22
1.4.1　アマノ標準時配信・認証サービス……22
1.4.2　アマノデジタルタイムスタンプサービス……25
1.5　参考文献……29

2　ETSI TS 102 023の概要……31
2.1　タイムスタンプ局、加入者、依存者……31
2.2　タイムスタンプ・ポリシー……31
2.3　義務と責任……32
2.4　TSAの実施規定……32
2.5　TSA公開説明書……32
2.6　鍵管理ライフサイクル……33
2.7　タイムスタンピング……33
2.8　TSAの管理および運営……33
2.9　組織について……34

3　タイムスタンプ・プロトコルの動向……35
3.1　RFC3161bis……35

3.2　TSP相互運用性テスト……36
3.3　XMLタイムスタンププロトコル（TMIL）……36
3.4　ISO/IEC18014-3：2002（リンクトークンの生成メカニズム）……37

4　NTP v4……39
4.1　ネットワーク遅延と時計誤差の測定方法……39
4.2　NTPプロトコルヘッダ……40
4.2.1　NTPプロトコルヘッダとタイムスタンプフォーマット……40
4.2.2　NTPv4 拡張フィールド……41
4.3　NTPv4 における認証の仕組み……41
4.3.1　NTPv3 からの変更点（認証関連）……41
4.3.2　NTP Autokeyの概要……42

付録　ETSI TS 102 023 全訳……45

メンバーリスト……85

1．タイムスタンプサービスの現状

1.1　通信総合研究所における日本標準時の供給
（独立行政法人　通信総合研究所）

1.1.1　通信総合研究所の役割

通信総合研究所（CRL）は、総務省設置法（第４条：所掌事務）および独立行政法人 通信総合研究所法（第 10 条：業務の範囲）等に基づき、周波数国家標準値を定め、日本標準時を発生し、長波標準電波やネットワーク回線等の各種伝送手段を用い、標準周波数および日本標準時を日本全国に高精度、且つ、高安定に供給するための研究開発およびサービス等を行っている。また、産業・貿易・通商等を支えるための基盤技術として、周波数と時刻に関する校正サービス体系を構築している。さらに、電子商取引・電子政府等で不可欠となる電子時刻認証システムの基盤技術開発にも着手している。

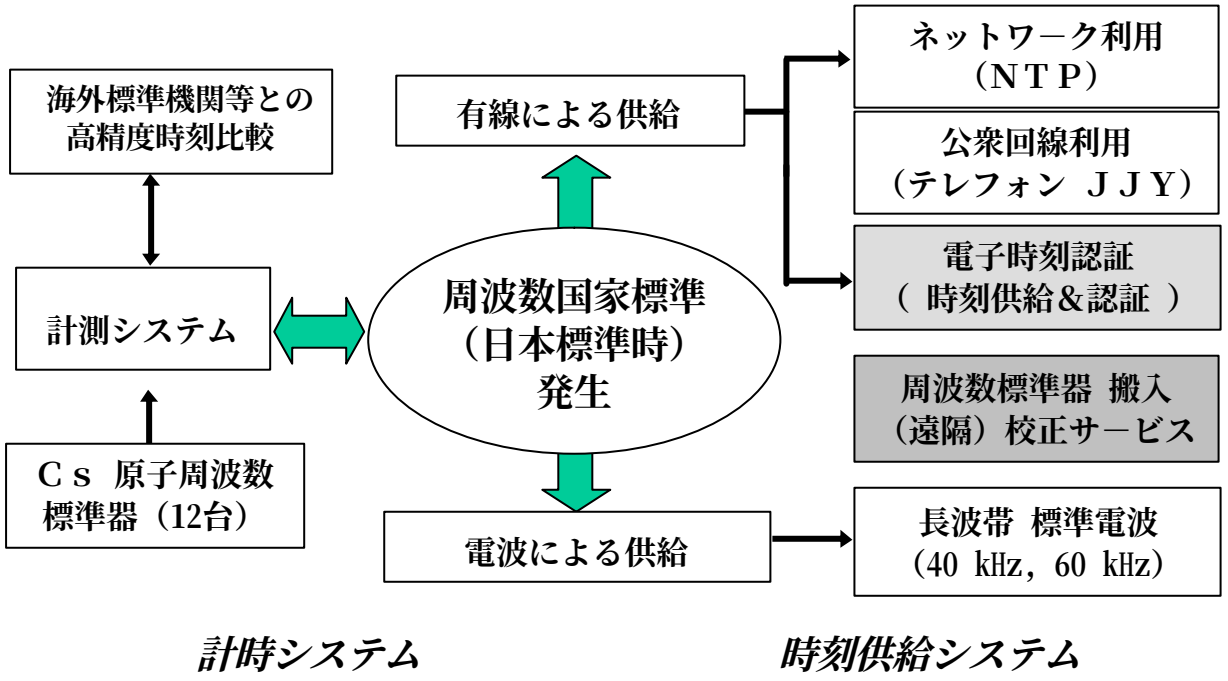

図 1−1　周波数国家標準（日本標準時）の設定および供給の概念図

1.1.2　サービス概要

CRLは、周波数国家標準（日本標準時）の「生成」・「比較」・「供給」をカバーする国内唯一の標準機関として、研究および周波数標準（日本標準時）供給サービスを定常的に実施している。こうしたサービスは、CRLが維持運用する実用セシウム周波数標準器 12 台を基に「生成」したもので、国内の計測機器および通信機器メーカーの社内標準器の校正や、テレビ・ラジオ放送局

の時報や、NTT 117 時報サービス等の基準源として利用されている。

また、国際化が進んだ現代社会においては、各国独自に決定した標準時の高精度比較や、それらの整合性をとることが不可欠となってきている。このため、国際度量衡局（BIPM）をはじめとする各国の標準機関が互いに協力し、GPS／GLONASS／静止通信衛星等を利用して各国の標準時を「比較」し、国際原子時（TA）構築や、協定世界時（UTC）を決定している。この中で、CRLは周波数・時間に関する技術力と安定した運用実績等が評価され、BIPMからGPS国際精密時刻比較網のアジア太平洋地域のノード局に指定されている。

最も身近な標準時の「供給」手段としては、平成 11 年 6 月に「おおたかどや山標準電波送信所（福島県）」からの長波帯による標準電波送信が本格運用を開始した。標準電波による時刻供給は、電波時計や、交通機関・観測機器の時刻管理等に利用され始めている。また、標準電波送信の安定運用のため「はがね山標準電波送信所（佐賀県）」が整備され、平成 13 年 10 月に標準電波送信所二局運用体制が確立している。

さらに、日本標準時の供給手段としては、公衆回線を利用した「テレフォン JJY」サービスや、インターネットで接続される計算機間の時刻合わせに日本標準時をリンクさせるNTPサーバ立上げ等の研究開発も実施している。

ここで、CRLが供給する日本標準時は、CRLが生成する協定世界時：UTC（CRL）を9時間（東経 135 度分の時差）進めた時刻である。

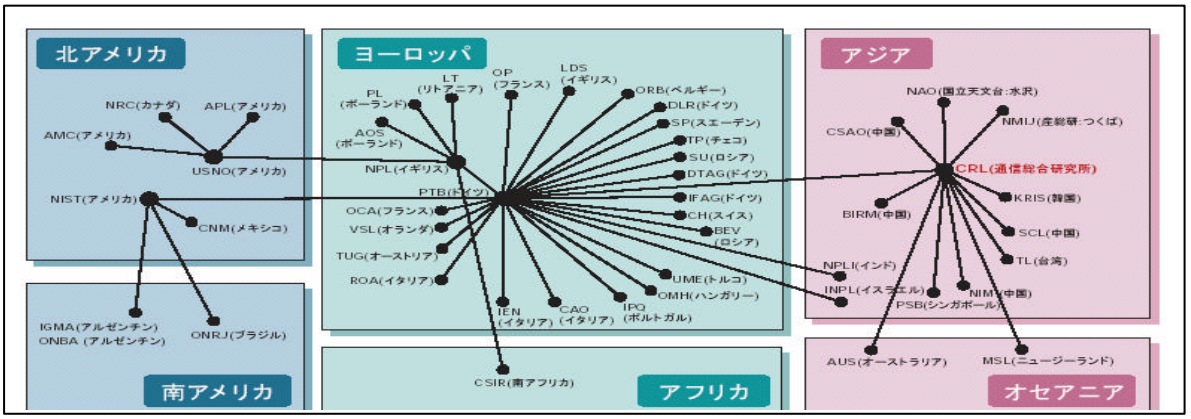

図 1－2　国際原子時構築のための GPS利用国際時刻比較ネットワーク

図1－3　長波標準電波送信所（福島局・九州局）の配置と、想定される電界強度計算値

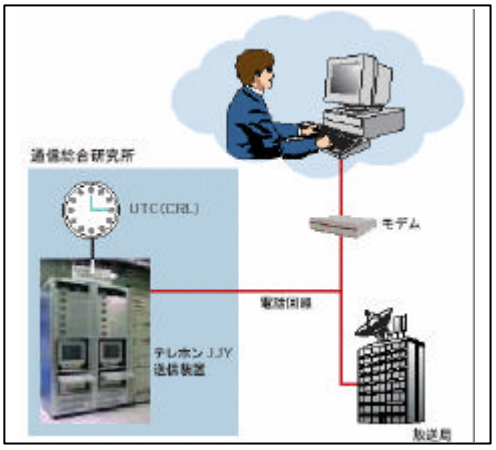

図1－4　テレフォン JJYの概念図

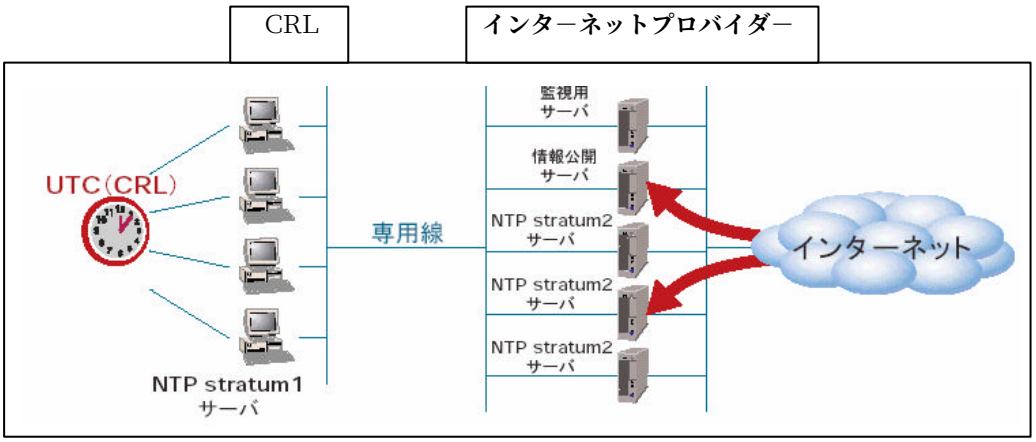

図1－5　ネットワークによる 日本標準時 時刻同期 概念図（NTPサーバ）

1.1.3　電子時刻認証システム開発

近年の電子商取引、電子決済の飛躍的な進展、そして 2003 年度からの電子政府の発足に伴い、こうした電子的な手続きにおいて、正確で、且つ、社会的にオーソライズされた時刻情報が求められている。CRLでは、国際的なトレーサビリティが確保された日本標準時をタイムスタンプ機関（TSA：Time Stamp Authority）に確実に供給するための電子時刻認証システム技術開発を開始した。具体的には、図1－6に示したようにCRLが国家時刻認証機関（NTA：NationalTime Authority）として、各TSAに時刻情報を供給し、各 TSAの時刻を確認の上、それを認証するシステムを想定している。これらにより、日本標準時にトレーサブルな時刻情報が利用者に供給されることになる。

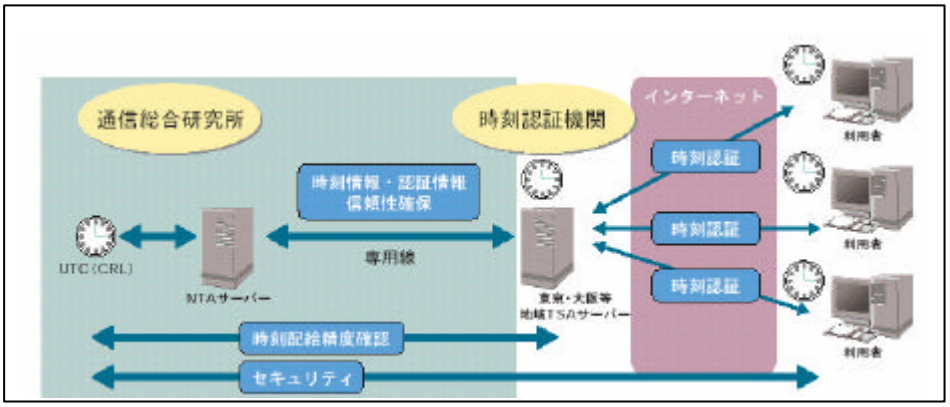

図1－6　電子時刻認証システム開発概念図

1.1.4　今後の展開

電子時刻認証システムでは、CRLから日本標準時を供給するにあたり、各タイムスタンプ機関に安全で正確な時刻をどのようにして供給するかが課題であり、現在供給源の複数化や供給時刻のモニタリングなどハード・ソフトの両面から様々な対策を行い、実運用に耐えうるシステムの開発を行っている。併せて、総務省・タイムビジネス推進協議会等との連携も図り、実サービスの早期実現を目指している。また、今後タイムビジネスに関係するタイムスタンプ機関（組織）や行政等との連携をさらに深め、利用者のニーズにあった日本標準時サービスを提供する予定である。

1.2 クロノトラスト（セイコーインスツルメンツ株式会社）

1.2.1 サービス概要

セイコーインスツルメンツ株式会社（以下、SII）の提供する時刻認証サービス「クロノトラスト」は、企業の重要な時刻システムに対して、厳正かつ公正な時刻配信を行うことを目的としたサービスである。具体的には、配信した時刻の完全性と時計精度を確保し、時刻配信の信頼性を高めるというサービスモデルを展開している。クロノトラストの基本的なサービス内容は、時刻配信と監査手法に違いがあることから、それぞれ「時刻認証サービス」、「時刻配信サービス」、「時刻監査サービス」の３種類が用意されている。

(1) 時刻認証サービス(図 1−7)

時刻認証サービスは、シンプル・プロトコルによるタイムスタンプを発行可能なタイムスタンプサーバ Ni−5110A（図1−8）およびアプリケーション開発用 API／SDK の販売と、タイムスタンプサーバに対して、クロノトラスト情報センタより厳正かつ公正な時刻配信を提供するサービスモデルである。基本的なサービスシステムの構成としては、タイムスタンプサーバを使用してタイムスタンプを発行するタイムスタンプ発行局（以下、TSA）と、TSA に対して時刻の配信と監査を行うクロノトラスト情報センタで構成される。クロノトラスト情報センタと TSA との間の通信は、PKI ベースの相互認証技術を採用したセキュアな NTP プロトコルを利用しており、双方の認証に成功した場合のみ時刻配信と監査が行われ、時刻ソースのなりすましや通信過程での改ざんなどの不正な攻撃からサーバシステムを保護している。

また、タイムスタンプサーバは、耐タンパ構造のハードウェアセキュリティモジュール（FIPS 140−1 Level3 取得）が採用されており、外部からの物理的な衝撃や攻撃が加わると自動的に内部データが抹消される構造となっている。これにより、タイムスタンプサーバの時刻の改ざん、およびタイムスタンプに使用する秘密鍵の危殆化を防止し、PKI による認証以外、いかなる外部からのアクセスを許さない堅牢性の高いセキュリティ強度を保持している。このため、クロノトラスト情報センタ側からの時刻の配信と監査が適切に行われ、確実にタイムスタンプサーバを経由した時刻でタイムスタンプが行われていることを証明可能である。

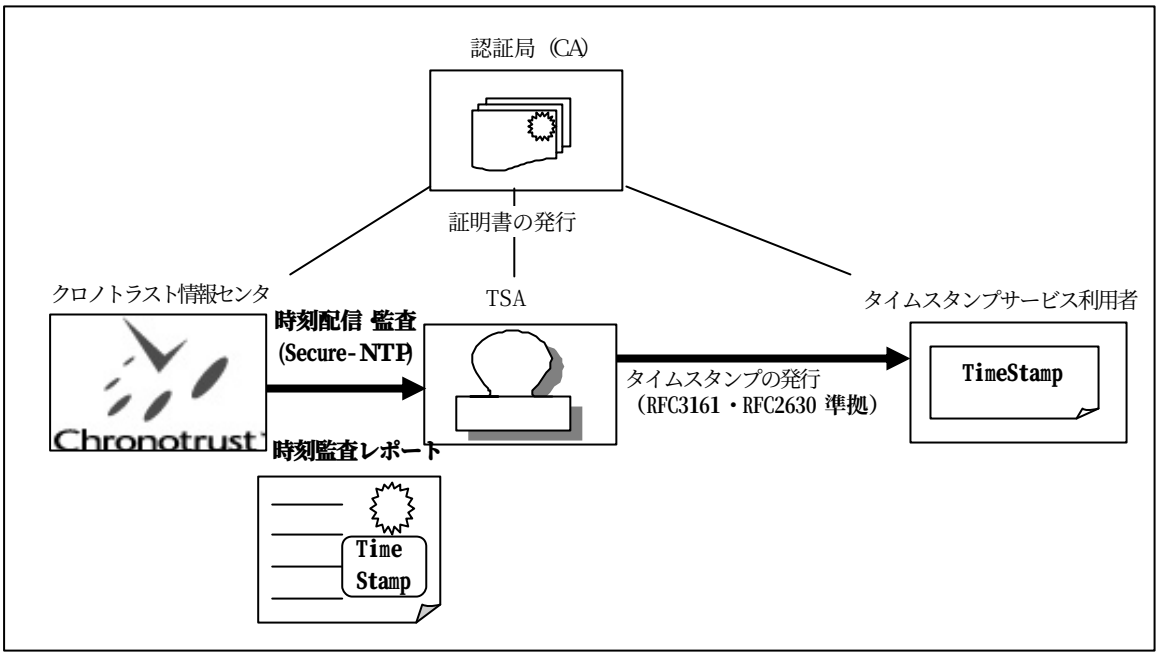

図１－７　時刻認証サービス

図１－８　タイムスタンプサーバＮｉ-5110Ａ

さらに、クロノトラスト情報センタからＴＳＡに対する時刻配信のトレーサビリティを確保するために、属性証明書を利用したアクセス制御を行っている。属性証明書によるアクセス制御とは、時刻監査時に比較的有効期間の短い属性証明書を発行することで、ＴＳＡが不正な時刻を利用できないようタイムスタンプサーバの制御を行うものである。具体的には、クロノトラスト情報センタからの定期的な時刻監査の結果が「適正値」の範囲内であれば、タイムスタンプサーバは正常に機能し、ＴＳＡが監査を受けなかった場合、あるいは監査を拒否した場合は、短い有効期限内でしか機能しないように設計されている。つまり、属性証明書の有効期限が切れた段階でタイムスタンプサーバは自動的に停止するように制御されている。

タイムスタンプサーバを制御している属性証明書は、クロノトラスト情報センタからの時刻監査に適合した場合のみ発行される（例：±500ms の精度）。時刻の精度が規定値を越えた場合、あるいは配信に失敗した場合等、何らかのトラブルが発生した場合、有効期間０秒（瞬時停止）の属性証明書が発行される。このように、定期的な時刻配信と監査結果に基づくアクセス制御を行うことで、ＴＳＡの所有するタイムスタンプサーバは常時適正であることが保証されている。

このような手続きで発行された属性証明書は、証明書の使用目的および機能的な性格から「時

刻監査証明書」と呼ばれている。この時刻監査証明書は、タイムスタンプサーバが正常に機能していた証として、TSAが発行したすべてのタイムスタンプに含まれており、ＳＩＩが監査しているタイムスタンプ時刻であることを確認することが可能である。(図 1－9)

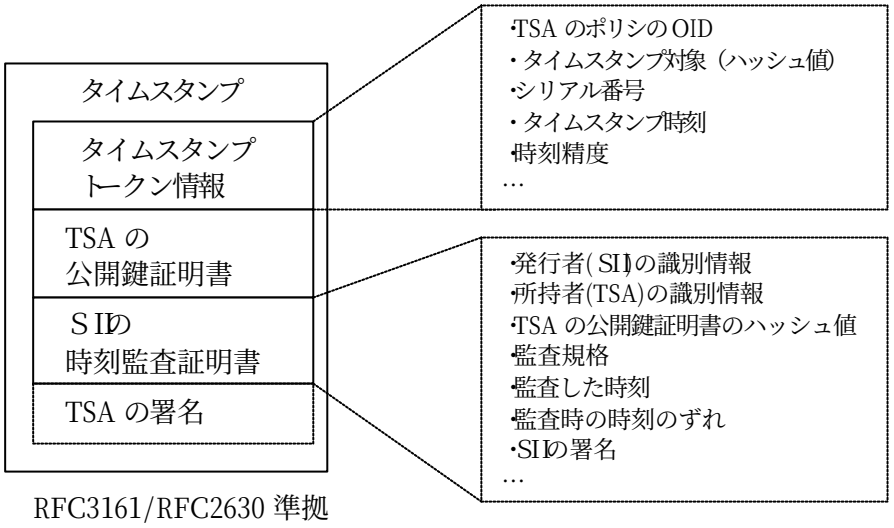

図 1－9　タイムスタンプの構造

また、タイムスタンプサーバは、 IETFが RFC3161／2630 として標準化し、公開されている仕様を実装しており、提供されるタイムスタンプは国際標準に準拠している。このため、提供されるタイムスタンプは将来に渡り安心して使用することができる。なお、このタイムスタンプにはTSAの公開鍵証明書・時刻監査証明書・タイムスタンプトークン情報等が含まれており、ローカルな環境でタイムスタンプの検証が可能である。

この時刻認証サービスは、タイムスタンプサービスを行う TSA事業者に対して前述のように高セキュリティのタイムスタンプサーバと高精度で改ざんできない時刻を提供する仕組みである。タイムスタンプの実施形態としては、タイムスタンプサービスの利用者は、アプリケーションサーバを介してタイムスタンプサーバからタイムスタンプを受け取る、もしくはタイムスタンプ用のアプリケーションを実装し、直接タイムスタンプサーバからタイムスタンプを受け取るなど、アプリケーションに合わせて TSA側で柔軟な対応をとることができる。また、これらのアプリケーションの開発には、ＳＩＩの販売するアプリケーション開発用 API／SDKを利用することが可能である。

(2)　時刻配信サービス(図 1－10)

時刻配信サービスは、高精度なタイムサーバの販売と、タイムサーバに対して、ＳＩＩの運営するクロノトラスト情報センタより、厳正かつ公正な時刻を配信し、また時刻の監査を行うサービスモデルである。このサービスでは、 PKIを利用した NTP Version 4 による時刻配信を行い、さらに利用事業者に配信された時刻をクロノトラスト情報センタが監査することで、時刻の信頼

性を高めることを目的としている。

サービスの構成としては、クロノトラスト情報センタから利用事業者内に設置されたタイムサーバへ時刻を配信する。この利用事業者内に設置されたタイムサーバより、各サーバシステムへの高精度で信頼できる時刻同期を実現することが可能になる。なお、サービスの利用者に対しては、そのタイムサーバが時刻同期を行っているサイトの機器に対して、SIIがサービスを行っていることを示す「Trusted Time Site Seal」を表示することが認められる。

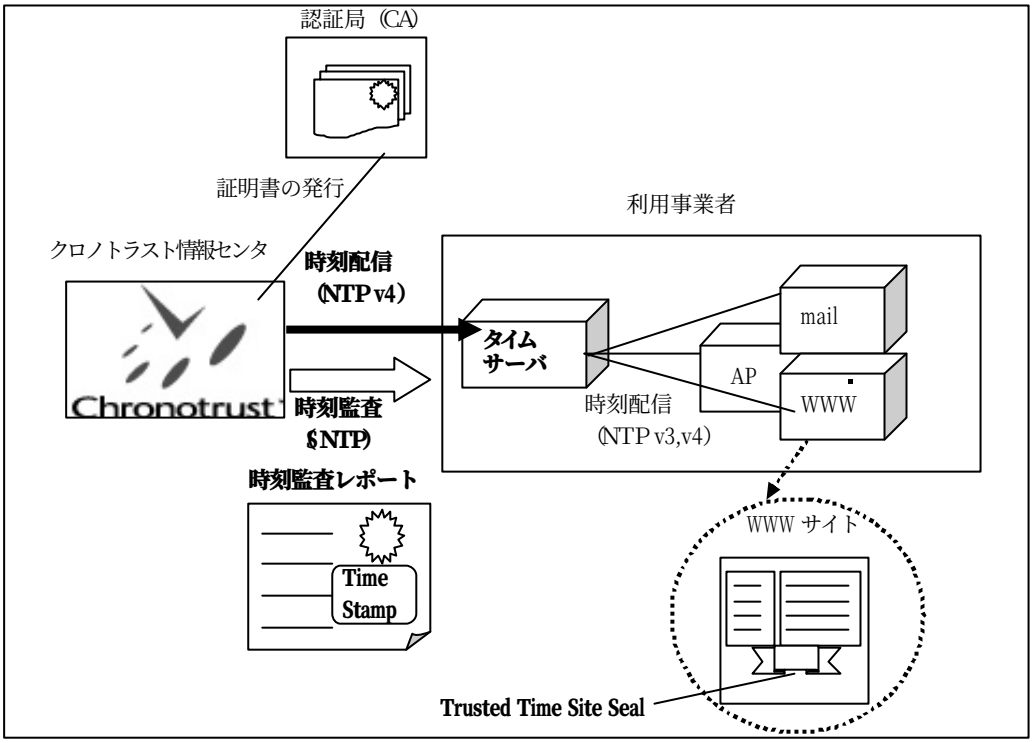

図 1－10　時刻配信サービス

(3)　時刻監査サービス(図 1－11)

時刻監査サービスは、利用事業者内の機器の時刻監査と監視を行うことを目的としたサービスモデルである。時刻監査サービスでは、SIIが第三者機関としてユーザ企業の時刻を監査することで、時刻の運用が適切だったことを証明する。また、時刻監査サービスでは、前述の時刻配信サービスと異なり直接的な時刻配信は行わないが、利用事業者のシステム環境に合わせた時刻同期が選択できるメリットがある。例えばコンピュータルームの設置条件として、GPSのアンテナが設置可能であればGPS時計を設置し、不可能であれば有線のテレホンJJY方式の時計システムを採用するといった選択が可能である。

時刻監査サービスにおける時刻の監査手法としては、対象となる利用事業者側のNTPサーバとクロノトラスト情報センタ側の時刻をSNTPにより比較検証する。また、時刻監査と同時に時刻精度のチェックおよび稼働状況の常時監視（１時間に１回）を行い、時刻の誤差発生時におけるシステム全体への悪影響についても最小限に抑える配慮が施されている。さらに、障害発生時の通報システムをサポートしており、監査対象のサーバシステムで何らかの障害が発生した場合は、管理者に対して電子メールで通報する。

この時刻監査サービスにより、利用事業者内の基準となるNTPサーバの時刻が第三者機関からの監査を受けた時刻となることから、様々なシステム上のファイル日時やログファイル、システムログなどの完全性を高めることが可能である。また、サービスの利用者に対しては、その時刻監査対象のサイトに対して、SIIがサービスを行っていることを示す「Trusted Time Site Seal」を表示することが認められる。

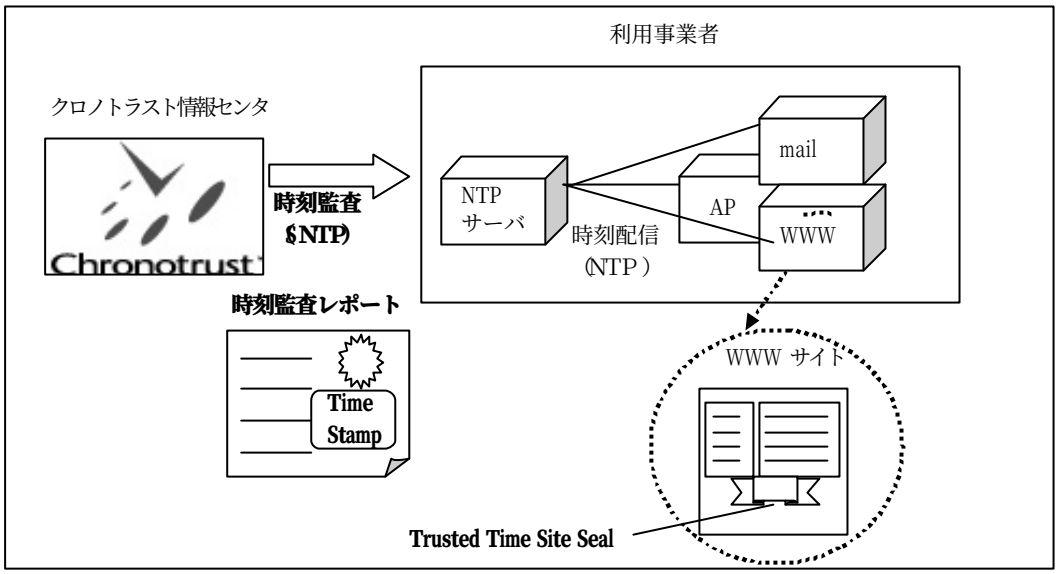

図1－11　時刻監査サービス

これらのサービスを提供するクロノトラスト情報センタは、時刻の基となる時刻ソースとして、自社で高精度の標準時刻生成サーバを運用している。この標準時刻生成サーバは、UTC（NIST）とのトレーサビリティを維持している。

さらに、クロノトラスト情報センタはCA・TSAとの保証範囲を明確化できるよう、運用規程を公開する予定である（図1－12）。この運用規程にはオブジェクト識別子が割り当てられており、TSAのポリシ・運用規程とリンクを取る際に使用することができる。

また、各サービスのユーザに対しては、クロノトラスト情報センタより監査の証拠として時刻監査レポートが発行される。この時刻監査レポートについても、クロノトラスト情報センタのタイムスタンプを付けて発行されており、信頼性を高めている。

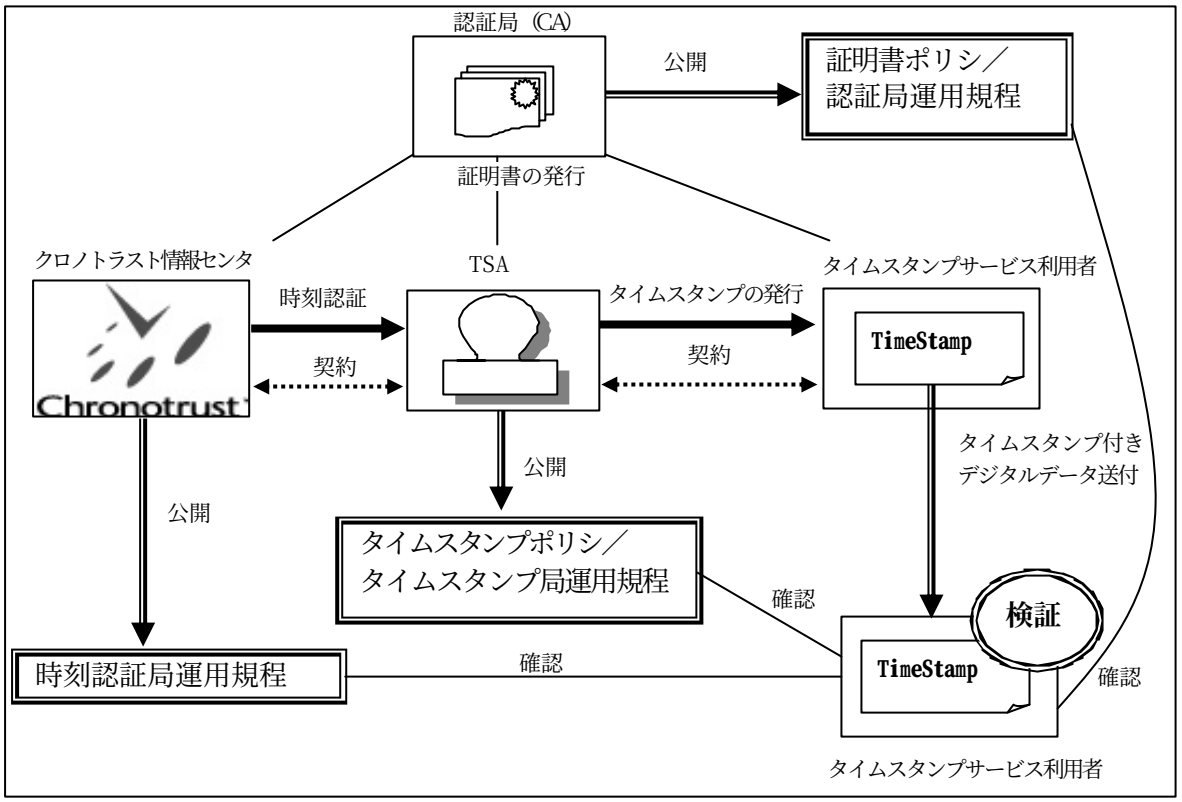

図 1－12 CA・TSA・タイムスタンプサービス利用者と時刻認証局運用規程の関係

1.2.2 シンプル・プロトコル（RFC3161）

IETFが RFC3161／2630 として標準化しているタイムスタンプ・プロトコルは、シンプル・プロトコルと呼ばれるものである。シンプル・プロトコルは、デジタル署名を用いたタイムスタンプ・プロトコルで、タイムスタンプを希望するデータのハッシュ値に時刻情報等を添付してデジタル署名（タイムスタンプ）を生成するものである。長所としては、システムの作りが単純で済む、ローカルな環境での検証が可能であるなどの点が挙げられる。一方、課題としては、TSAが署名者と結託するとタイムスタンプの改ざんが可能であると言われている。これに対しクロノトラストでは、クロノトラスト情報センタから TSAへの、PKIベースの相互認証技術を採用したセキュアな NTPプロトコルによる時刻配信・監査や、耐タンパ構造のタイムスタンプサーバにより、シンプル・プロトコルの課題を解決している。

1.2.3 サービスの利用イメージ

1.2.3.1 タイムスタンプの実施形態

クロノトラストのサービスモデルでは、タイムスタンプサーバを設置し、時刻認証サービスを受ける利用事業者が TSAとなって、タイムスタンプを行う。TSAに対する、クロノトラスト情報センタからの時刻認証サービスの提供方法としては、 ISDN・インターネット・専用線等が用意されている。

タイムスタンプの実施形態としては、TSAとタイムスタンプサービス利用者の関係について、

以下のように区分できる。

(1)　タイムスタンプサービス利用者が、TSAの行うタイムスタンプサービスを直接利用する場合（図 1－13）

(2)　タイムスタンプサービス利用者が、サービスプロバイダ等のサービスを通して、TSAのタイムスタンプサービスを間接的に利用する場合（図 1－14）

また、タイムスタンプサーバとのデータ連携について、図 1－13 中に記載されるように、以下の区分がある。

①　直接タイムスタンプサーバとデータ連携を行う

②　アプリケーションサーバを介してタイムスタンプサーバとデータ連携を行う

(1)においては、タイムスタンプサービス利用者は、TSAのサービスに応じた形でタイムスタンプを利用する。例えば、①の形態では、タイムスタンプサービス利用者に、RFC3161 に準拠したタイムスタンプを扱えるアプリケーションが必要となるが、②の形態ではアプリケーションサーバで利用方法を自由に設定できる。

一方、(2)では、タイムスタンプサービス利用者は、サービスプロバイダのサービスに応じた形でタイムスタンプを利用する。この場合も、サービスプロバイダ側で利用方法を自由に設定できる。

なお、タイムスタンプの実施形態としては、さらに TSAの区分として内部（社内等）でタイムスタンプを行う場合と外部のタイムスタンプサービスを利用する場合があるが、

タイムスタンプサーバの所有者等が異なるのみで、どちらの場合においても TSAとタイムスタンプサービス利用者の関係は(1)、(2)で説明可能である。このため、ここでは内部・外部のタイムスタンプサービスといった区別は行わず、TSAとして一つにまとめている。同様に、タイムスタンプサービス利用者は、個人・企業、サービスプロバイダ・社内用タイムスタンプサービス利用者といった区分を行わず、タイムスタンプサービス利用者として一つにまとめている。

また、タイムスタンプ検証については、TSA、もしくは TSAを利用するサービスプロバイダの提供する方法により異なる。WWW サービスを利用した検証を行う場合はネットワーク接続が必要となるが、検証用プログラムが提供されている場合、ローカルな環境での検証も可能である。

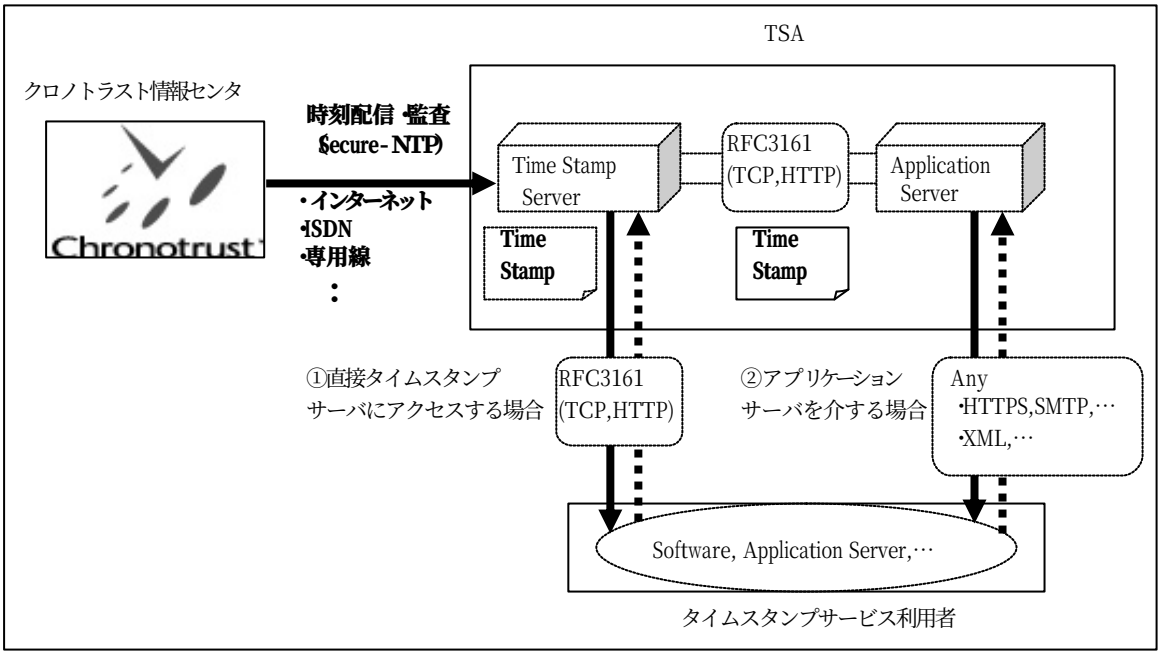

図１－13　TSAとタイムスタンプサービス利用者の関係(1)

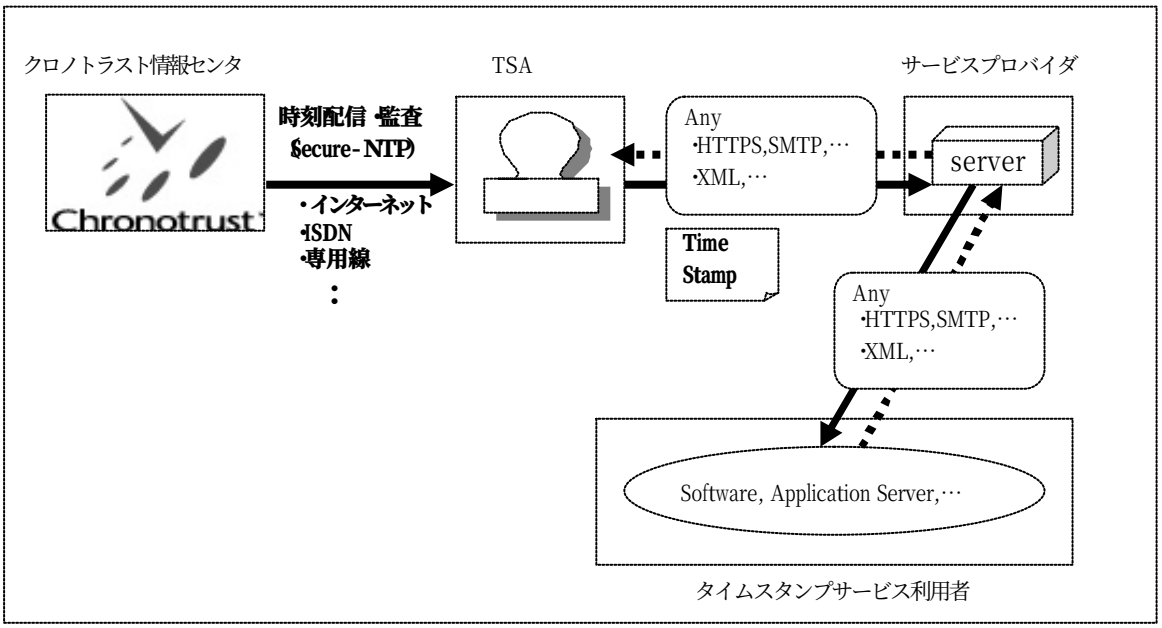

図１－14　TSAとタイムスタンプサービス利用者の関係(2)

1.2.3.2　アプリケーション開発

ＳＩＩのタイムスタンプサーバは、ＩＥＴＦがＲＦＣ3161／2630 として標準化し、公開している仕様を実装しているため、タイムスタンプ用アプリケーションの開発に特別な環境を必要としない。ＳＩＩで提供しているアプリケーション開発用ＡＰＩ／ＳＤＫを利用することも可能であり、ライブラリとしては以下のものが用意されている。

・ＪＡＶＡクラスライブラリ

・Ｃ言語ライブラリ（Ｗｉｎ32ＤＬＬ、Ｓｕｎ Ｓｏｌａｒｉｓ、Ｌｉｎｕｘ）

1.2.3.3 利用事例

(1) ｅマーケットプレイス

ｅマーケットプレイスで電子商取引を行う場合、契約における改ざん、成りすまし、盗聴を防止することは重要である。さらに、契約の際にタイムスタンプを発行することにより、その契約が行われた時刻を証明することが可能である。クロノトラストは、ｅマーケットプレイスにおける契約の日付・時刻の証明を可能とする時刻認証の機能として採用されている。

(2) セキュリティ基盤システム

ＳＩＩは、申請や決裁など業務の電子化の実現を目的としたセキュリティ基盤システムの開発において、数社と技術協力を行うことを発表している。この基盤システムは、電子文書の真正性を証明するDVCS（Data Validation and Certification Server）を実装した国内初の製品化を含む電子公証局システムや署名文書保管システムなどを統合したもので、電子文書/データの証拠力を高めるための環境を提供する「EDM（Evidenced Data Management：エビデンスド・データ・マネジメント）」を実現するものである。この中で、ＳＩＩは時刻認証サービス、タイムスタンプ技術を提供している。

(3) タイムスタンプ付与型音声記録公証システム

コールセンターや金融サービス業界など電話による商取引を行っている多くの企業では、電話で行われる取引内容を、ボイス・ロギング・システムにより、音声、相手先電話番号や取引内容等に関する情報を記録している。従来のシステムでは、通話音声をデジタル暗号化して保存する際に、ローカルな時刻が記録されていた。このため、取引をする両者の間で取引成立時刻に差異が出ることがある。

ログイット株式会社、株式会社日本電子公証機構、ＳＩＩの 3 社は、このような課題を解決するため、ボイス・ロギングに対して第三者によるタイムスタンプと公証を行う、タイムスタンプ付与型音声記録公証システムを共同開発した。これにより、音声データの原本性と取引時刻の保証を可能にし、取引時の当事者間の立場と公正さの証拠性をより強固なものにすることができる。適用分野としては、証券などの金融取引、コールセンターでの商品売買やクレーム処理、弁護士事務所などが挙げられる。

1.2.4 今後の展開

ＳＩＩでは、タイムスタンプサーバを活用した各種アプリケーションの開発を既に各業界の数社とアライアンスにより、電子メールや公証サービスといったアプリケーション開発を共同で進めることで、利用者の拡大を狙った様々な開発を進めている。また、より汎用的なアプリケーション開発の必要性から、NET対応やXML署名、Ｗｅｂサービスへといった最新のテクノロジーに対応するため、より多くの企業や政府機関、団体との連携をしている。さらに、タイムスタンプサーバに関しても、2048bit 署名対応、パフォーマンス向上など、幅広いアプリケーションに対応するための検討を行っている。

また、タイムビジネスに対する取り組みの強化として、セイコー株式会社、セイコープレシジョン株式会社とともに、ネットワーク上における時刻認証・配信に関する事業を、「ＳＥＩＫＯサイバータイムビジネス」として共同事業展開し、規模の拡大と充実を図ることを発表している。

一方、サービスの提供だけでなく、タイムビジネスの普及活動にも力を入れている。タイムビジネス推進協議会への幹事としての参画や、ホワイトペーパーの配布、各種セミナーの開催などを行っており、今後もこのような活動の強化を予定している。

（注）

SIIで使用している「時刻認証サービス」という言葉は、クロノトラスト情報センタから、TSAのタイムスタンプサーバ（タイムスタンプ用内部時計）に対し、ＰＫＩによる相互認証（Mutual Authentication）を行い、時刻同期をとるサービスのことである。

1.3 SecureSeal（NTT データ）

1.3.1 サービスの概要

NTTデータは、2000 年 4 月から電子的な記録の原本性と作成時刻を証明する「電子文書証明サービス SecureSeal」の提供を行っている。SecureSealは、「電子化された情報がある特定の日時に確かに存在していたこと」かつ「それ以降電子化された情報の内容が改ざんされていないこと」を証明するものであり、いわゆるタイムスタンプサービスに相当するものである。SecureSealは、NTTデータが運用・管理する電子文書証明センタに利用者がアクセスするという形態をとっており、この電子文書証明センタが TSAとして機能している。

このサービスは米国 Surety. com社が開発した「DigitalNotary Service」をベースにしたものであり、リンキングプロトコルと呼ばれる方式を採用していることが大きな特徴である。日本国内をはじめ、北米でも多くの企業で利用実績を持ち、法律文書、電子カルテ、研究開発文書の管理などに幅広く利用されている。

具体的なサービスのイメージを以下に記す。

1．非改ざん証明を行いたい文書を選択し、文書からハッシュ値を作成する。
2．インターネット経由でハッシュ値を電子文書証明センタに送信する。
3．センタでは、不特定多数のユーザからのハッシュ値を集めて更にハッシュ値を時刻単位で生成・管理すると同時に、個別データ毎に公証記録を発行する。
4．ユーザは、必要に応じて「元のデジタルデータ」「公証記録」を利用して、非改ざん・時刻証明の検証を行うことができる。

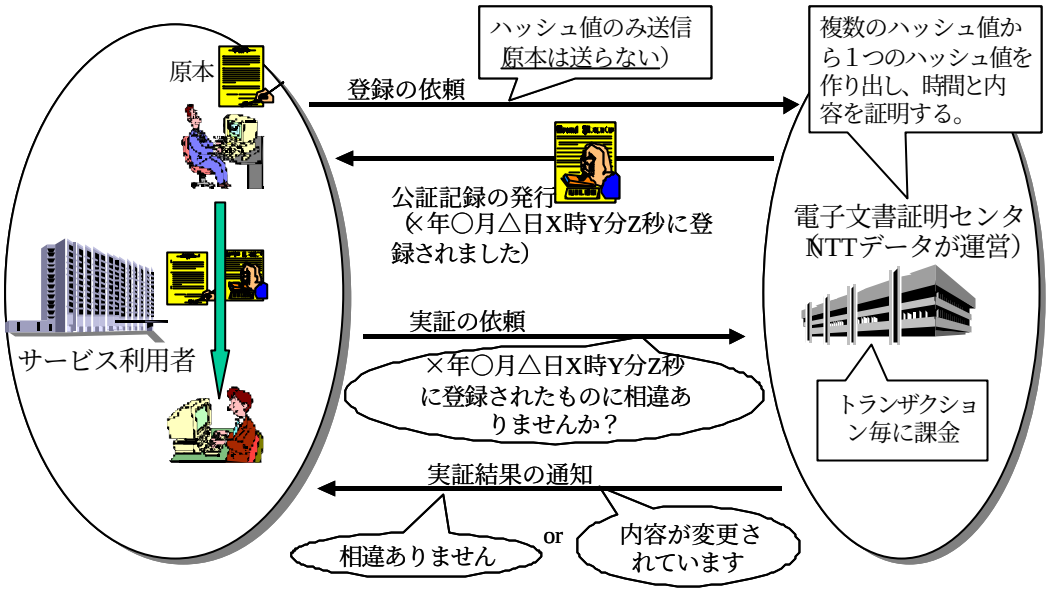

図１－15　SecureSeal の概要

SecureSealの特徴を以下に記す。

- 証明の有効期限がない（長期の文書証明が可能）。
- リンキングプロトコルの採用により、TSAと利用者が結託して不正を行うことが仕組上不可能となっている。
- ハッシュアルゴリズムにＭD5と SHA1を併用しており、ハッシュ値の衝突に対する耐性が高い。
- 電子情報そのものを送る必要がないため、利用者のプライバシを確保しながら証明のサービスを利用できる。
- センタ運用の透明性を保つため、週間ハッシュ値（１週間に蓄積されたハッシュ値全体から生成したハッシュ値）を毎週日経産業新聞で公開している。

1.3.2　リンキングプロトコル

リンキングプロトコルの“リンキング”とは、複数のハッシュ値から１つのハッシュ値を生成するという操作を繰り返し行うことにより、ハッシュ値同士をリンクさせていくことを指している。この方式のタイムスタンプ（公証記録）には、対象となっている文書のハッシュ値、時刻情報、タイムスタンプの正当性を証明するための必要情報（リンク情報など）が含まれる。全てのタイムスタンプは、これまで生成されたタイムスタンプに依存するように生成され、その過程で発生したリンク情報（ハッシュ値）を定期的に新聞等に公表することで、システムの安全性を確保している。

主なリンキングプロトコルとして、リニアリンキングプロトコルとツリー構造のリンキングプロトコルがあるが、SecureSealではツリー構造のリンキングプロトコルを採用している。ツリー構造のリンキングプロトコルでは、一定時間（ラウンド）でリンク情報（SRH）を生成する。このリンク情報は、同一ラウンド内において複数の利用者データのハッシュ値をツリー状に結合・ハッシュ化して生成される（図2－5）。生成されたリンク情報と、時刻、リンク情報を生成する過程のハッシュ値全てを含むタイムスタンプ（公証記録）を生成し利用者に渡される。

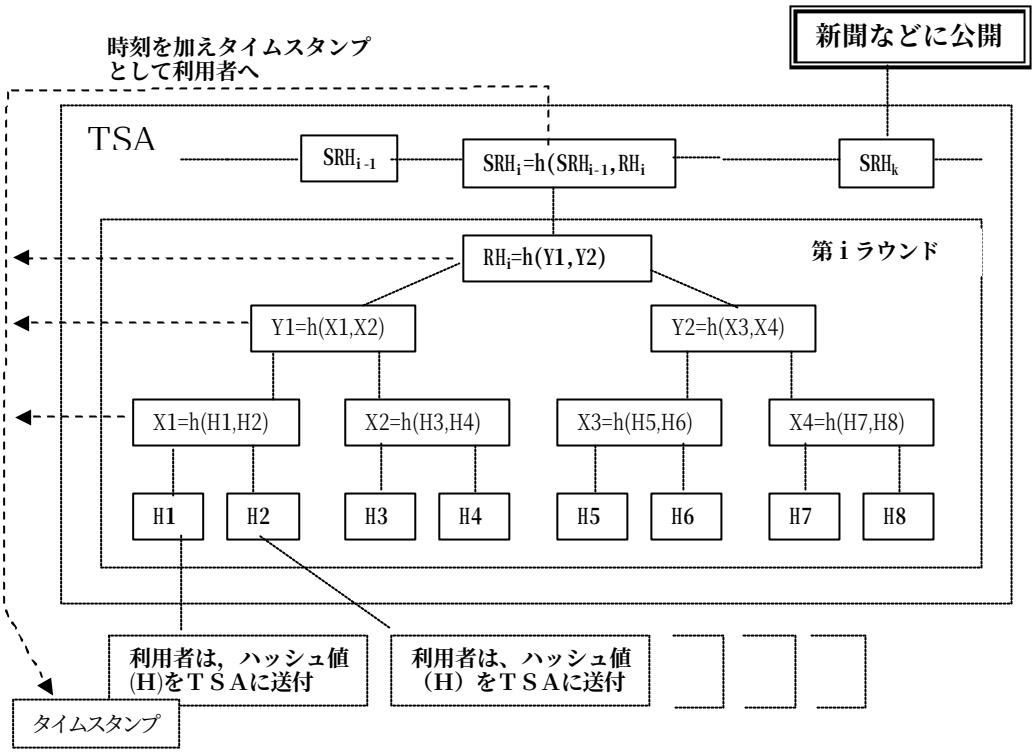

図 1－16 ツリー構造のリンキングプロトコル

1.3.3 サービスの利用イメージ

1.3.3.1 タイムスタンプの実施形態

1.3.1 で述べたように、SecureSeal は TTP として運用されている TSA のセンタに利用者がアクセスするというサービス形態をとっている。基本的にセンタへのアクセスはインターネット経由で行う形になるが、セキュリティ上の理由から専用線によるアクセスを利用者が希望する場合は、そのような構成も可能である。

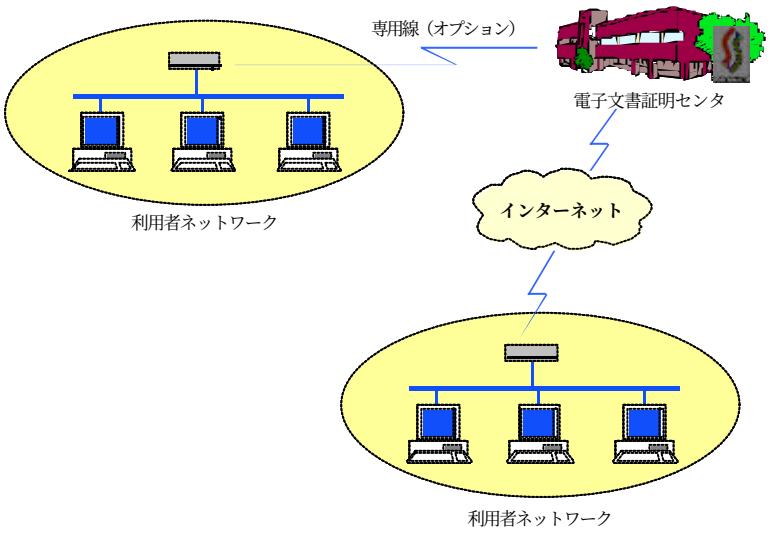

図 1－17 センタへの接続形態

利用者側に特別なハードウェアを用意する必要はなく、インターネットへの接続のみが必要となる。

センタと接続して電子文書を登録・検証するために、NTTデータでは以下のものを無償で提供している。

(1)　SecureSealクライアントプログラム

MS-Windowsから SecureSealを利用するためのクライアントプログラムを提供している。このプログラムは、ツリー表示されたファイルから対象を選択し、簡単な操作でファイルの登録・検証ができるものになっている。

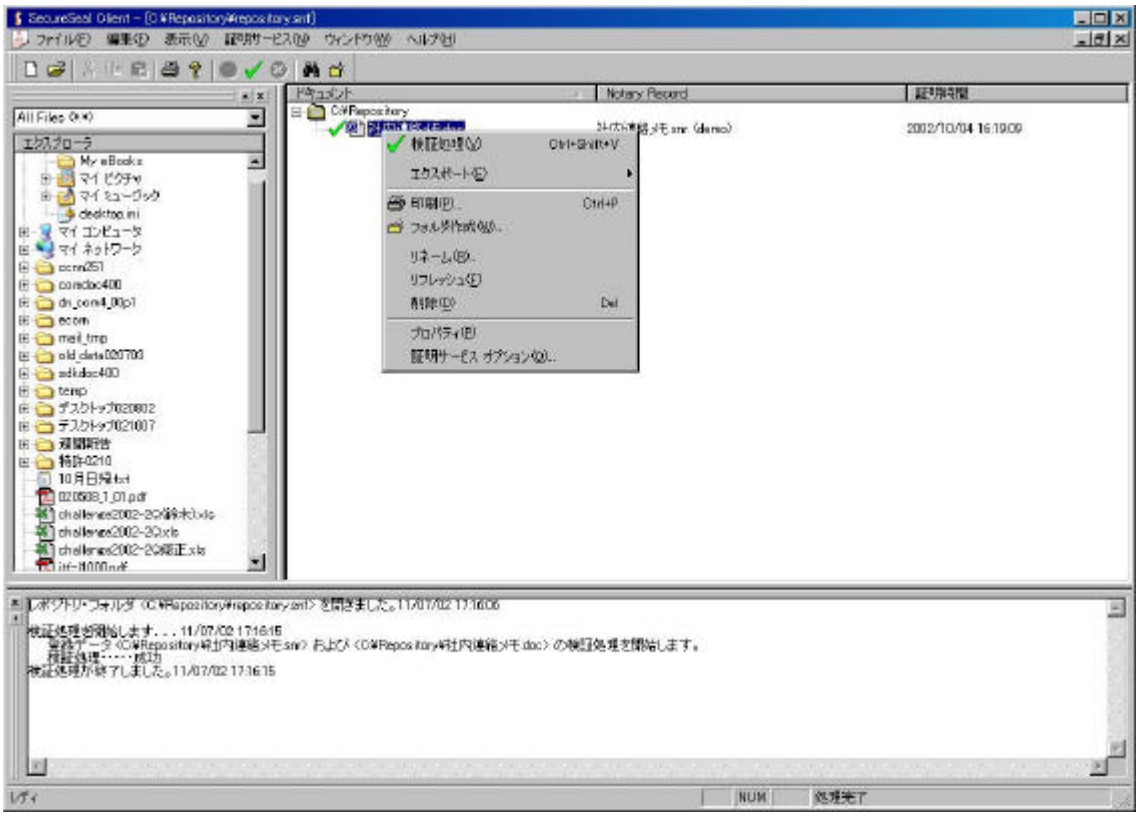

図1－18　SecrueSeal クライアントプログラム

(2)　開発環境

SecureSealを利用するために必要な機能一式を、ライブラリとして提供している。現在提供している開発環境を以下に記す。

C++クラスライブラリ（Windows95/98/NT/2000/XP,Solaris7 以降, Red Hat Linux6.0 以降に対応）

MS-Windows用 automation object（COM コンポーネント）

JumpStart Kit for Lotus（LotusNotes用開発環境）

なお、これらの開発環境は http://www.ssc.nttdata.co.jp/dl_index.html で提供している。

実際に利用者が SecureSealを使用する場合、典型的な利用形態がいくつか挙げられる。

パターン１：利用者が自身の端末から直接登録と検証を行う。

パターン２：利用者のネットワーク内に設置されたサーバから、センタに対して登録・検証を

行う。

パターン３：利用者から見て外部のネットワークに設置されたサーバから、センタに対して登録・検証を行う。

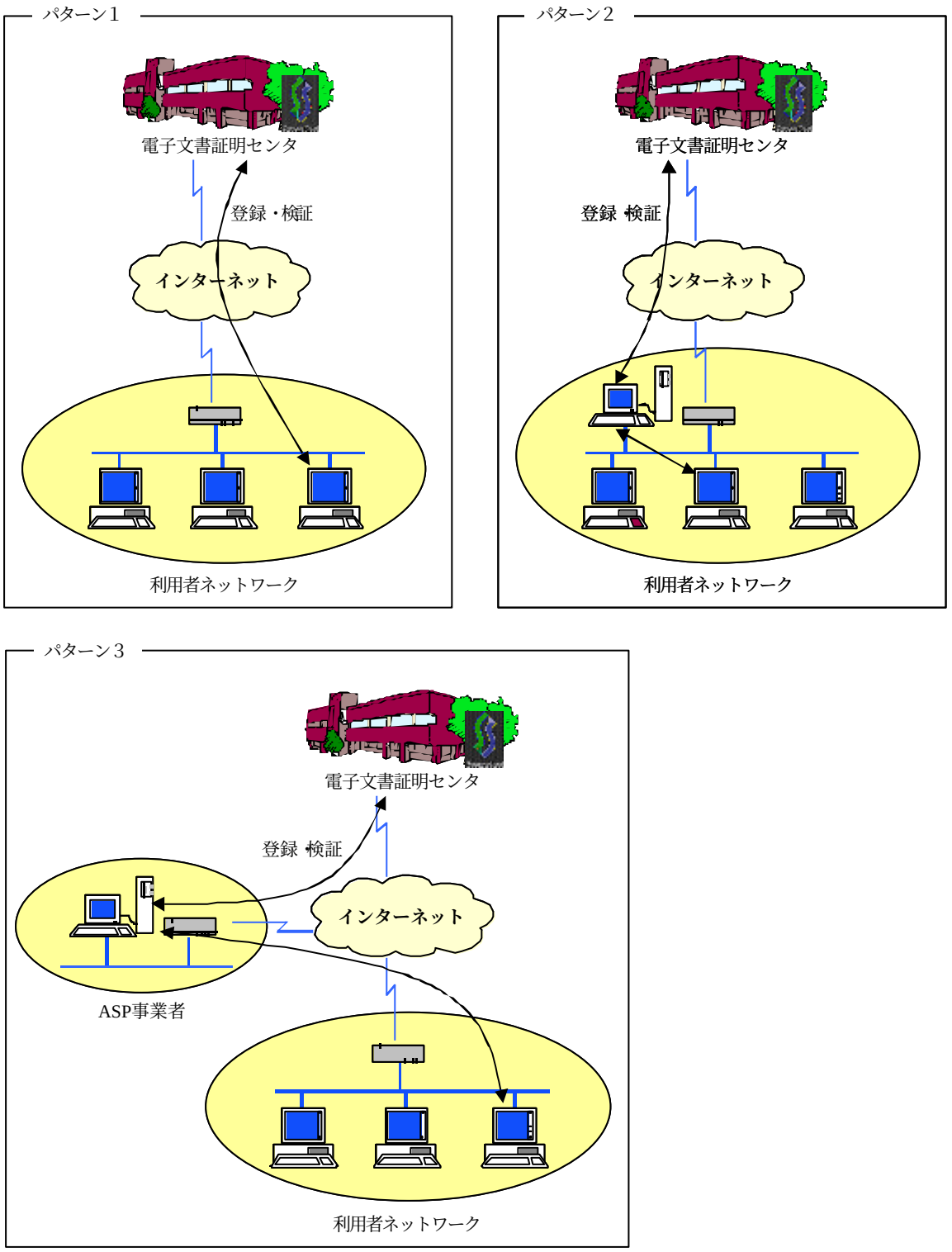

図 1－19　SecureSeal の利用形態

パターン１の場合、利用者の端末に SecureSealクライアントプログラム（図 2−4 を参照）または SecureSealライブラリが組み込まれたプログラムをインストールし、端末から直接ファイルの登録と検証を行う。センタから発行される公証記録（タイムスタンプ）は、独立したファイルとして生成され端末に保管される。登録したファイルとそれに対応する公証記録のファイルをセットで受け渡しすることで、利用者間での検証が可能になる。

パターン２の場合、利用者の端末に専用プログラムをインストールする必要は基本的にない。利用者はネットワーク内に設置されたサーバを使用し、センタとの通信はこのサーバが行う形になる。そのため、サーバ上には SecureSealライブラリが組み込まれたプログラムをインストールする必要がある。この場合のサーバは、具体的にはファイルサーバや文書管理用サーバといったものであるケースが多い。

パターン３の場合についても、利用者の端末に専用プログラムをインストールする必要はない。この場合、 SecureSealは何らかの ASPサービスの一部として利用者に提供されることが多い。利用者はファイルの登録・検証を直接意識する必要がなく、Ｗebブラウザを通じて ASPのサイトに POSTしたファイルがセンタに登録される、といった処理が通常行われる。

1.3.3.2　ユーザ事例

(1)　電子カルテシステム

電子カルテの非改ざんと作成時刻を証明するために、株式会社ビー・エム・エルが開発・販売している電子カルテシステム ＭedicalStationに、SecureSeaが採用されている。診療録の電子保存は 1999 年 4 月の厚生省通知により認められているが、そのためには電子保存の方式が一定の基準を満たすことが要求されている。具体的には「保存義務のある情報の真正性が確保されていること」「故意または過失による虚偽入力、書換え、消去及び混同を防止すること」などが要求されており、ＭedicalStationでは SecureSealを使用してこれらの条件を満たしている。

(2)　電子契約文書の長期保存

電子的な契約書の原本性を確保するために、株式会社コンストラクション・イーシー・ドットコム(以下 CEC. Com)が提供する建設業界向け電子契約サービス CECTRUSTで、SecureSeaが採用されている。2001 年 4 月に施行された IT書面一括法を受けて建設業法が改正になり、これまで書面を取り交わすことが義務づけられていた工事請負契約について、電子文書による契約が容認された。これを受けて、CEC. Com は建設業界向けの電子契約サービス CECTRUSTを 2002 年 4 月から開始した。このサービスは、PDFなどで作成された電子文書を受発注会社間で流通させ、両社の電子署名を添付して契約を成立させるものである。また、締結済みの契約書の長期保管（10 年）も行っており、電子署名文書の作成時刻と原本性を保証するために、 SecureSeaが利用されている。

(3)　わかしお医療ネットワーク

平成 12 年度経済産業省公募事業であり、現在千葉県の重点事業として展開されているわかしお医療ネットワークにおいて、医療データの原本性を保証するために SecureSeaが利用されている。わかしお医療ネットワークは、病院、診療所、調剤薬局をネットワークで接続し、それらが連携して遺伝子解析・遺伝子治療などの高度な医療を実現することを目的としており、千葉県立東金病院と山武医療圏の診療所・調剤薬局が参加している。このシステムで発生するデータにつ

いては、高度なセキュリティと真正性の確保が必要とされているため、SecureSealを用いて解析依頼書、患者情報、解析結果情報等の原本性を確保している。

(4) 知的財産管理

製造業などにおける特許関連の技術文書管理に、SecureSealが現在利用されている。これは、米国の特許制度である先発明主義（出願ではなく発明の順番を重視する制度）に対応するためである。日本国内の企業は多くの米国特許を出願・取得しており、そのため国内の企業であっても「いつどのような発明を行ったのか」を外部に対して証明できるようにしておく必要がある。これは、技術文書の管理を紙で行う場合には比較的容易なことだが、それらの文書が電子的に作成された場合には極めて難しい。この問題を解決するために、現在複数の企業で SecureSealが利用されている。

1.3.4 今後の予定

SecureSealは現在、電子文書を安全に流通・保管するための基盤サービスである NTTデータの電子文書流通プラットフォーム SecurePodに組み込まれている。SecurePodは電子署名文書の交換と長期保管を想定したものであり、かつ電子文書の送達確認機能等も備えている。この枠組みにより、SecureSealの電子契約システムや電子政府・電子自治体に対する展開を現在行っている。

また、NTTデータは総務省タイムビジネス推進協議会に参画しており、協議会で今後行われる検討に沿った形で SecureSealの更なる機能強化を予定している。

1.4 e-timing（アマノ株式会社）

e-timingは、米国の国家時刻標準機関とトレーサブルな「信頼のおける時刻」を基にネットワーク社会の信頼性向上を目的として以下の二つのサービスを行っている。

・標準時配信・認証サービス

・デジタルタイムスタンプサービス

1.4.1 アマノ標準時配信・認証サービス

本サービスは、アマノ株式会社が信頼のおける第三者である時刻配信・認証機関（Trusted Timing Authority）として契約ユーザーのタイムサーバの時刻を協定世界時(注2)に同期させ、その健全性（1.4.1.3 を参照）を監視・証明するものである。ネットワークを構成しているサーバ等の機器類の時刻が同期していないと、処理・記録等の時系列確保が困難であり、たとえ閉ざされたネットワーク内で同期していても協定世界時に同期がとれていないとネットワーク間の通信や情報処理において時刻の信頼性確保ができなくなる。サービスは以下の３つの要素からなっており、ネットワーク上の時刻の信頼性向上をサポートする。

1.4.1.1 標準時の配信と同期

契約ユーザーのタイムサーバにインストールされたアマノ時刻同期・管理ソフト（e-timing Node Agent）がアマノタイミングセンター(注1)のタイムサーバから協定世界時(注2)の配信を受け、サーバの時計を同期状態に保つ。

アマノタイミングセンターと契約ユーザーは、MPLS 技術を利用した IP−VPN 網（私設ネットワーク網）で接続され、通信の信頼性を確保する。

1.4.1.2 配信・同期の記録、保管、証明

配信・同期の状態は、記録としてアマノタイミングセンター内で厳重に保管される。保管期間は３年以上で、契約ユーザーの許可された管理者のみが、この記録をWeb上で閲覧可能である。指定した期間内の記録の閲覧や、同期状態をグラフ表示することも可能である。また契約ユーザーの要求により、配信・同期状態の証明書を発行することも可能である。

1.4.1.3 配信・同期状態の監視と異常検知時の警告

配信・同期状態は常にセンターの監視下にあり、異常を検知すると契約ユーザーの管理者へメール等で知らせる。この場合の異常とは、時刻の改ざんが発生した場合、時刻差がしきい値を越えた場合、サービスの開始･停止、通信障害が発生した場合等、契約ユーザーのタイムサーバが健全でないと認められる状態を指す。

注１：高度なセキュリティと 24 時間 365 日連続的な運用を可能にするインターネットデータセンター内にアマノ株式会社が設立した日本で初めての商用時刻配信・認証のためのセンターであ

る。重要な設備はすべて二重化等の障害対応もされている。

注２：国家間の時刻比較にも利用されるGPSコモンビュー方式によりＮＩＳＴ（米国商務省国立標準技術研究所）より直接時刻の監査・校正を受けたセシウム原子時計が保持している協定世界時UTC（ＮＩＳＴ）でBIPM（国際度量衡局）とのトレーサビリティを確保している。

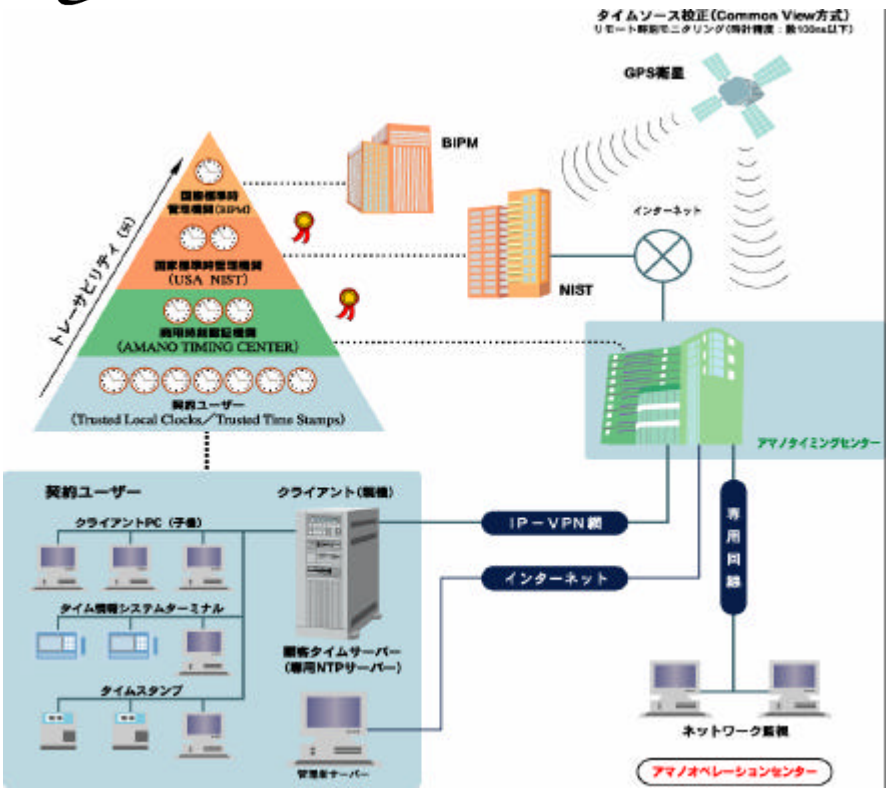

図 1－20　システム概要図

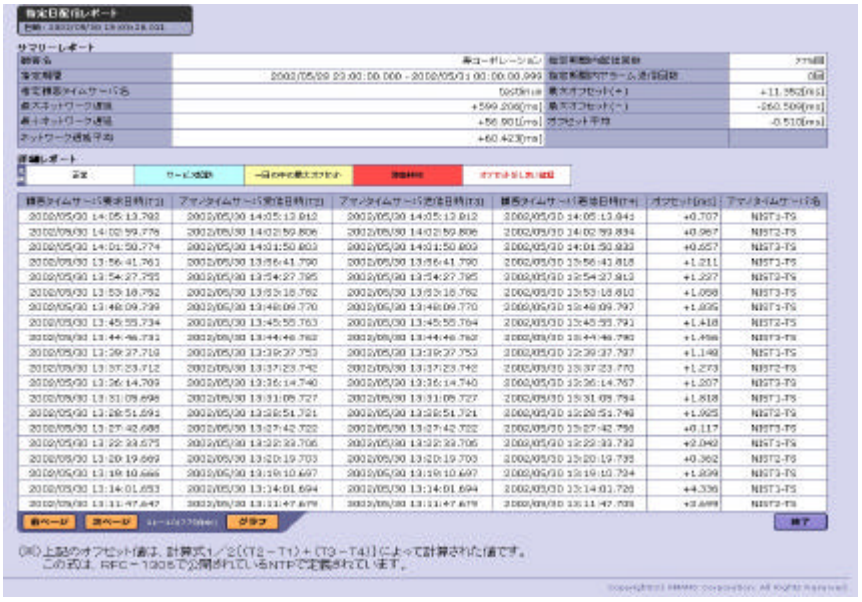

図 1－21　レポート例

1.4.2　アマノデジタルタイムスタンプサービス

昨今の企業活動において、重要な電子文書をＷebサイトで公開したり、社内外の人と共有・流通させる機会が増えている。万が一その重要な電子文書が改ざんされたり、また、文書を作成した後で都合が悪くなったとき、自ら改ざんして事実をもみ消すことが無いような公平性が求められている。「e-timing EVIDENCE for Adobe Acrobat」は、信頼のおける時刻に基づくデジタルタイムスタンプを電子文書に埋め込むことで、電子文書の「非改ざん」を手軽に証明することができるソフトウェアで、デジタルタイムスタンプの生成は１文書につき 20 円である。印鑑を押す感覚で利用することができる。

図１－22　e-timing EVIDENCE for Adobe Acrobat

1.4.2.1　デジタルタイムスタンプの特徴

１．存在証明（アリバイ証明）

ある時刻にすでに、その文書（データ）が存在していたことの証明ができる。

２．完全性証明（非改ざん証明）

デジタルタイムスタンプが電子文書に押されてからスタンプを検証するまでの間、文書が改ざんされていないことを証明できる。文書に少しでも変更があれば、すぐに検出される。

図１－23　存在証明と完全性証明

1.4.2.2　電子署名とデジタルタイムスタンプが違う点

電子署名は「誰が」「何を」そして「非改ざん」の証明をすることができるが、電子署名を行う際に参照される時計が個人の PCである以上、何時から何時までその文書が改ざんされていないのかを証明することはできない。

デジタルタイムスタンプでは、電子署名では証明できなかった「何時から何時まで文書が存在したのか」ということを証明することができる。信頼のおける時刻に基づくデジタルタイムスタンプは、「電子文書確定時刻」と「文書が改ざんされていない期間」を証明することができる。

[電子署名] 個人の PCに基づく時刻。誰でも簡単に変えることのできる不確かな時刻。

[デジタルタイムスタンプ] ＮＩSTに基づく時刻。誰も変えることのできない信頼できる時刻。

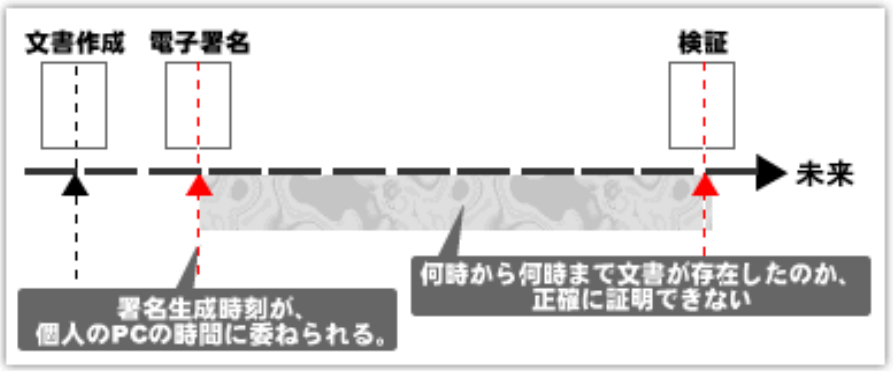

図 1－24　個人の PC での電子署名生成

1.4.2.3　PC の時刻が信用できない点

文書の作成時刻は個人の PCに基づいた時刻である。PCの時刻は誰でも簡単に変えることができるため、改ざんされた文書が実際の文書が作成された時刻と同じ時刻に作成されたように装うことも簡単である。また、実際の文書より先に存在したように装うこともできてしまう。つまり、文書の履歴管理が信用できなくなってしまう場合がある。

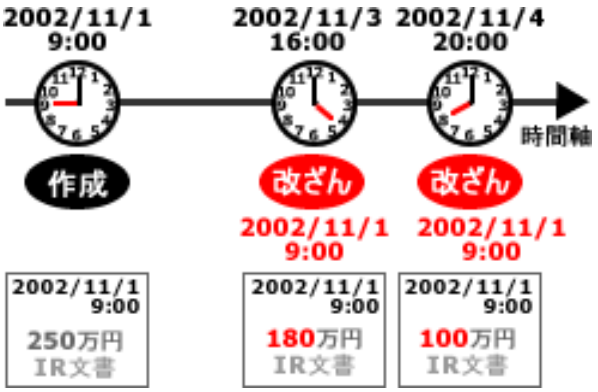

図 1－25　PC の時刻の改ざん

1.4.2.4　デジタルタイムスタンプの仕組み

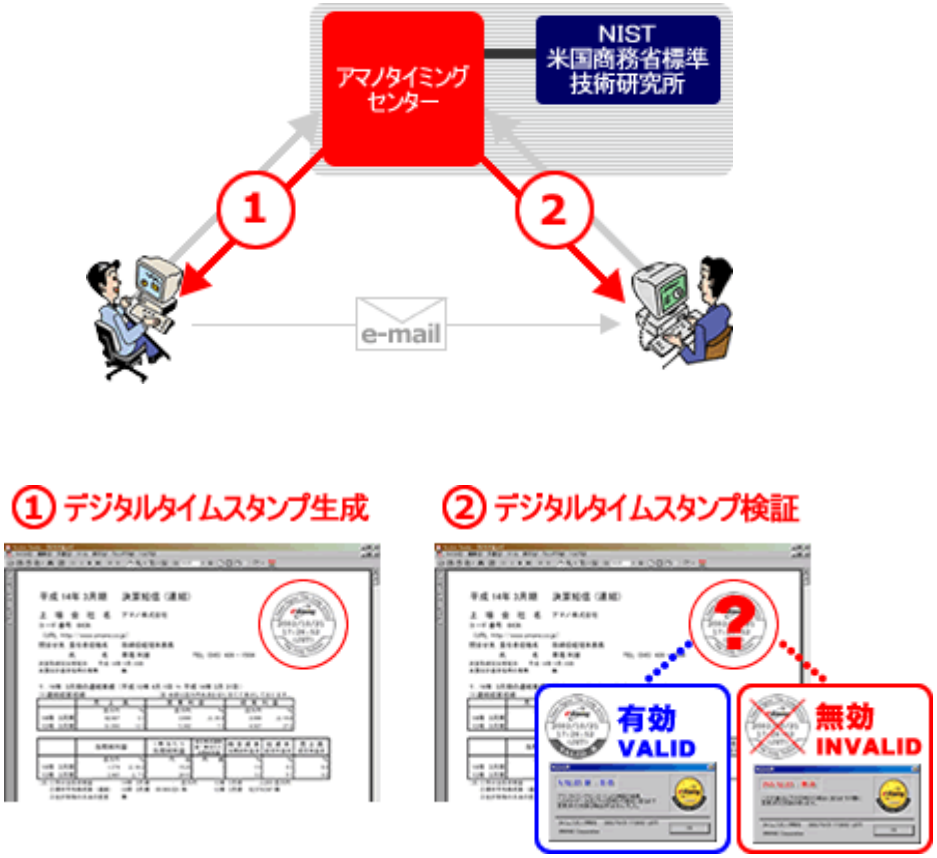

図 1－26　デジタルタイムスタンプの生成と検証

(1)　デジタルタイムスタンプ生成

①　PDF文書のデジタルタイムスタンプを埋め込みたい場所をマウスでクリックする。

②　アマノタイミングセンターがデジタルタイムスタンプを PDF文書に埋め込む。

・PDF文書本体のハッシュ値とアマノタイミングセンターの時刻情報を紐付け、RSA セキュリティ社の PKI・暗号化技術を使い、電子文書に改ざん検知可能なデジタルタイムスタンプ情報を埋め込む。

・コピー／メール送信しても、デジタルタイムスタンプは消えない。

・デジタルタイムスタンプのイメージは「丸型・角型・不可視パターン」から選ぶことができる。

(2)　デジタルタイムスタンプ検証

①　PDF文書に埋め込まれたデジタルタイムスタンプへマウスを近づけると、ポインタが変化する。

②　そのままクリックすると検証が行われ、結果が表示される。

(3)　タイムスタンプ検証ソフトの無料配布

①　Adobe Acrobat Readerのプラグイン検証ソフトを無償でダウンロード可能。

② 検証ソフトを利用することで、PDFに貼り付けられたデジタルタイムスタンプの印影が誰でも手軽に検証できる。

1.4.2.5 e-timing EVIDENCE for Adobe Acrobat の利用例

- IR情報の保護（Web上での添付書類の保護）
  決算短信/事業報告書/目論見書/財務諸表/会計・財務文書など
- 監査対象文書
  作業報告書/検査報告書/ ISO関連文書/連結文書/会計情報など
- 特許・著作権の保護
  技術資料/アイデアシート/企画書など
- 技術資料作成時
  マニュアル/仕様書/出図図面/測定機器校正記録/検査報告書/アイデアシートなど
- Webコンテンツ（画面）の証拠文書としてキャプチャー
  オンラインショッピングの決済手続完了確認画面/特許・著作権侵害・不正ロゴ使用/カタログ情報・価格情報・約款など
- 取引業務
  通知書/契約書/請求書/見積書/価格表/打合せ確認書など
- 日々の報告業務
  役員会の議事録/日報・週報・月報/連結文書/稟議書など
- IT書面一括法で電子化される文書作成
  保険業法/割賦販売法/旅行業法/証券業法の適用文書
- 行政機関・公共事業機関・士業などが関わる届出・申請・公文書作成時
  公文書/届出書/入札書類/申請書など
- 学術的な電子文書
  論文/成績証明書/在学証明書/表彰状/時間割/学術レポートなど
- 総務・人事業務
  辞令/通達/訓告/組織表など

注：本章に記載されている会社名、製品名はすべて各社の登録商標または商標です。

1.5　参考文献

タイムスタンプの現状の検討を進める過程で参考とした文献を以下に示す。特にＷＥＢ上の文書はバージョンが更新されることがあるので、注意を要する。

１．独立行政法人　通信総合研究所　日本標準時グループ
http://jjy.crl.go.jp/

２．電子署名と時刻に関する小論集 Vol.1
http://www.sii.co.jp/ni/tss/wp_index.html

３．セイコーインスツルメンツ株式会社　時刻認証サービス　クロノトラスト
http://www.sii.co.jp/ni/tss/index.html

４．クロノトラスト時刻認証局運用規定
http://www.sii.co.jp/ni/repository/index.html

５．セイコーサイバータイム
http://www.seiko-cybertime.jp/

６．アマノ株式会社　e-timing
http://www.e-timing.ne.jp/

７．標準時配信・時刻認証サービスの研究開発に関する研究会
http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/time/index.html

８．タイムビジネスの普及に向けて「標準時配信・時刻認証サービスの研究開発に関する研究会」
　　－タイムビジネス研究会－報告書
http://www.soumu.go.jp/s-news/2002/020618_2.html

９．タイムビジネス推進協議会
http://www.scat.or.jp/time/

10. The Network Time Protocol Project
http://www.eecis.udel.edu/~ntp/

11. RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002

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

13. RFC 1305: Network Time Protocol (Version 3), March 1992

14. FIPS PUB 140-1, Security Requirements for Cryptographic Modules, US Department of Commerce National Institute of Standards and Technology, January1994

15. RFC 3281: An Internet Attribute Certificate Profile for Authorization, April 2002

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

17. RFC 2630: Cryptographic Message Syntax, June 1999

18. Public Key Cryptography for the Network Time Protocol Version. 2, draft-ietf-stime-ntpauth-04.txt, November 2002

19. RFC 2527 Certificate Policy and Certification Practices Statement Framework

20. ETSI TS 102 023 V1.1.1(2002-04) Policy requirements for time-stamping authorities

2．ETSI TS 102 023 の概要

ETSI TS 102 023 は、公開鍵暗号、公開鍵証明書、信頼できるタイムソースの使用を前提とした、タイムスタンプ局（TSA）の運営に関連するポリシー要件を定めている。このポリシー要件は、電子署名の証明に使用されるタイムスタンプ・サービスを主な目的としているが、あるデータが特定の時刻以前に存在していたことの証明が必要なあらゆる目的に使うことができる。

タイムスタンプ・ポリシーは「何を遵守するか」について定めている。これに対して、タイムスタンプの作成やその時計の精度の維持に使用するプロセスなど、「どのように遵守するか」について定めているのが TSA 実施規定である。TSA 実施規定は、TSA の業務および運営実施についても詳細に定めている。

2.1 タイムスタンプ局、加入者、依存者

タイムスタンプ・サービスに関わる主なプレイヤーは、タイムスタンプ局、加入者、依存者である。ここではそれぞれ次のように位置付けている。

(a) タイムスタンプ局

タイムスタンプ・トークンの発行を行う機関。TSAは、外部委託等、ほかの関係者を活用してタイムスタンプ・サービスの一部を提供できるが、常に全般的責任を負い、ポリシー要件が満たされていることを保証する。

TSAは、識別可能な複数のタイムスタンプ・ユニット（TSU）を運用することができ、各ユニットは異なる鍵を有する。

(b) 加入者

TSAに、タイムスタンプを付与するよう要求するエンティティ。複数または単一のエンドユーザーで構成される組織を加入者とすることができる。加入者が組織の場合、その組織に適用される義務の一部は、エンドユーザーにも適用されるものとする。いかなる場合においても、組織は、エンドユーザーの義務が正しく果たされない場合に責任を負い、したがって、組織は、そのエンドユーザーに対して情報を適切に提供することが期待されている。加入者がエンドユーザーの場合、そのエンドユーザーは、その義務が正しく果たされていない場合に直接責任を負う。

(c) 依存者

タイムスタンプ・トークンの受信者。

2.2 タイムスタンプ・ポリシー

タイムスタンプ・ポリシーは、「共通のセキュリティ要件のもとで、特定のコミュニティまたはアプリケーションに対するタイムスタンプ・トークンの適用可能性を示す規則の集まり」であるとし、ここでは、1 秒以内の精度をもつ TSAのためのベースライン・タイムスタンプ・ポリシーの要件を定義している。

ベースライン・タイムスタンプ・ポリシーは次のオブジェクト識別子を持つ。

{itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(02023) policy-identifiers(1)

baseline-ts-policy (1)}

2.3 義務と責任

TSAについては、必要な要件が、信頼あるタイムスタンプ・ポリシーによって適切に実現されていることを保証しなければならないとしている。TSAの機能を外部委託する場合においても、ポリシーに定められた手順の順守を保証する必要がある。また、タイムスタンプに直接あるいは参照先に示された、付随する義務の遵守についても保証しなければならない。

加入者については、特に規定していないが、依存者については、利用条件として以下の義務を含めることとしている。

(a) タイムスタンプ・トークンが正しく署名され、署名に使用された秘密鍵がその時点まで危殆化されなかったことの検証

(b) タイムスタンプ・ポリシーに定められたタイムスタンプの使用に関する制限事項の考慮

(c) 契約その他で定められたそのほかのあらゆる制限事項の考慮

2.4 TSAの実施規定

ここでは、タイムスタンプ・サービス提供に必要な信頼性を明示するために、実施規定として以下を定めている。TSAはこの要件を満たす管理を実施しなければならない。

a) TSAはビジネス資産およびそれらの資産への脅威を評価し、必要なセキュリティ管理と運営手順を決定するため、リスク調査を実施するものとする。

b) TSAは本タイムスタンプ・ポリシーに定められたすべての要件を満足するために使用される実施規定および手順を用意するものとする。

c) TSAの実施規定は、該当するポリシーや実施を含め、TSAサービスを支援するあらゆる外部組織の義務を定めるものとする。

d) TSAは加入者と依存者がその実施規定や、タイムスタンプ・ポリシーの順守評価に必要なその他の関連文書を入手できるようにするものとする。

e) TSAは、第 7.1.2 項に定める通り、すべての加入者と潜在的依存者に対して、そのタイムスタンプ・サービスの使用に関する条件を開示するものとする。

f) TSAは、TSA実施規定を承認する決定権限を備えた高レベルの管理組織を有するものとする。

g) TSAの上層部経営者は、実施が適切に行われることを保証するものとする。

h) TSAは、TSA 実施規定の管理責任を含めた実施の審査プロセスを定めるものとする。

i) TSAは、意図する実施規定の変更について適正な通知を行うものとし、また、上記（f）の承認の後、改訂した TSA実施規定を上記（d）に定める通り直ちに入手可能とする。

2.5 TSA公開説明書

TSAはすべての加入者と依存者に対して、タイムスタンプ・サービスの使用に関する条件を開示することとしている。ここでは、TSAが対応している各タイムスタンプ・ポリシーについて以下を定めている。

a) TSAの契約情報
b) 適用されているタイムスタンプ・ポリシー
c) タイムスタンプが付与されるデータを表現するために使用されている少なくとも 1 つのハッシュ・アルゴリズム
d) タイムスタンプ・トークンに署名するために使用される署名の予想寿命
e) タイムスタンプ・トークン内の時刻の UTC に対する精度
f) タイムスタンプ・サービスの使用に関するあらゆる制限事項
g) 加入者の義務
h) 依存者の義務
i) 依存者がタイムスタンプ・トークンに「合理的に依存」しているとみなされるよう、タイムスタンプ・トークンの検証方法に関する情報および有効期間に関するあらゆる制限事項
j) TSAのイベント・ログが保持される期間
k) 国内法のもとでタイムスタンプ サービスに対する要件を満足しているとの主張を含めた適切な法体系
l) 賠償責任の制限
m) 苦情や紛争解決の手順
n) TSAが定められたタイムスタンプ・ポリシーを順守していると評価されているかどうか、および評価されている場合には独立した評価機関

2.6 鍵管理ライフサイクル

TSAは、あらゆる暗号鍵が、自己の制御可能な環境のもとで生成されたことを保証しなければならないこと、TSAの秘密鍵を安全に保持すること、TSAの秘密署名鍵は、期限終了後は利用しないことを保証すること、TSAの秘密鍵のバックアップは、鍵危殆化リスクを最小化するためにすべきでないとなっている。

なお、TSAの秘密鍵の生成、格納は次の暗号モジュールで実施されることとなっている。

- FIPS 140-1 レベル 3 以上に定める要件を満足するモジュール
- CEN Workshop Agreement 14167-2 に定める要件を満足するモジュール
- ISO 15408 EAL4 以上または同等のセキュリティ基準が保証された信頼あるシステム

2.7 タイムスタンピング

TSAは、タイムスタンプ・トークンがセキュアに発行され、正しい時刻を含むことを保証し、その時計が定められた範囲内で UTC と同期していることを保証する。タイムスタンプ・トークンのプロトコルは RFC3161 に従う。

2.8 TSAの管理および運営

保護資産、要員のセキュリティ、物理的セキュリティ、運用管理、アクセス管理、導入とメンテナンス、TSAサービスの危殆化、TSAの閉鎖について定めている。

TSAサービスの危殆化については、TSA秘密鍵の危殆化や未較正の検出を含めた、TSAサー

ビスのセキュリティに影響する事象に関して、加入者と依存者が関連情報を入手できることを保証するものとしており、すべての加入者および依存者が発生した危殆化の説明を参照できるようにすること、危殆化から回復する手順が遂行されるまで、タイムスタンプ・トークンを発行すべきではないこと、可能であれば、すべての加入者および依存者に対して、TSAユーザーのプライバシー、またはTSAサービスのセキュリティを侵害しない限りにおいて、影響のあったタイムスタンプ・トークンを特定するために使用された恐れのある情報を入手可能にすることなどを定めている。

また、TSAの閉鎖については、TSAがそのタイムスタンプ・サービスを終了する前に、すべての加入者および依存者に対してその終了に関する情報を提供すること、監査ログを第三者機関に委譲すること、公開鍵や証明書を依存者に適切な期間にわたって提供するためにその義務を維持するか、または信頼できる機関に委譲すること、TSA秘密鍵は破壊されるべきであることなどを定めている。

2.9 組織について

その組織が信頼できることを保証するために、非差別、賠償責任に対応する十分な措置、財務的安定性、教育、研修、必要十分な人員の採用、苦情や訴えを解決するための方針や手順の用意、外部委託時の契約文書締結などについて定めている。

3．タイムスタンプ・プロトコルの動向

シンプルプロトコルとして知られるPKIをベースとしたタイムスタンプ標準はIETFのもとで2001年9月にRFC3161として発行された。このRFC3161のプロトコル概要は2001年度のECOM認証・公証WGの長期署名保存TF（TF5）の報告書に解説がある。デジタル署名がある時点以前に正しく存在していたことを示すためにはタイムスタンプが必須である。また長期署名保存技術にとってもタイムスタンプが重要な役割を果たす。RFC 3161はASN.1を用いてプロトコル仕様を定めたものである。ここで定められたタイムスタンプトークンはCMS SignedData(RFC2630)形式をとっている。

一方XML構文を用いたデジタル署名がW3CとIETFのジョイントで標準化されXML文書へのより木目の細かなデジタル署名が可能になってきた。最近政府への電子申請についてXML署名がが推奨されるようにもなってきている。当然XML署名文書にタイムスタンプを付ける要求も持ち上がってくる。XML署名文書にASN.1ベースのRFC 3161のタイムスタンプを丸ごとBase64でエンコードして添付することもできるが相性が良くない。XML署名ベースのタイムスタンププロトコルが望まれる。

また、リンキングプロトコルについては現在ISO／IEC 18014-3で標準化の検討が行われており、まもなく正式な国際標準として文書が公開される予定となっている。18014-3では、タイムスタンプトークンの生成に使用されるメソッドやプロセスが記述されている他、リンキングプロトコルを用いたTSAに固有のオペレーションについても言及している。

ここではタイムスタンプ標準について3つの動向について述べることにする。RFC3161標準のステータスをより安定したステータスに上げる努力と、XMLタイムスタンププロトコルの標準化活動、ISO／IECにおけるリンキングプロトコルの標準化についてである。

3.1 RFC3161bis

RFC 3161は現在Proposed Standardのステータスであるが、IETFのもとでこれをDraft Standardにすべく RFC 3161の改定作業が行われている（ドラフトRFC3161bis）。以下に示すようにこの改定は以下に示すように6箇所の変更が成されようとしているが大幅なものではなく字句の適正な使用法や曖昧さの無い記述の変更である。プロトコル仕様はv1のまま変更は無い。

参考：RFC3161bisで述べられている変更点（APPENDIX E: Summary of changes with RFC 3161.）

CHANGE N*1:

TSA、TSU（Time-stamp unit）、Time-stamp tokenの違いの明確化を行った。TSUは1つのTSAのユニットとして管理されるハードウェア、ソフトウェアの集合である。そしてTSUは1つの時間には活性化された1つの署名鍵を有している。

CHANGE N*2:

2.4.1 節の言葉の訂正　SHOULD→ SHALL

CHANGE N*3:

拡張の解釈を変更

クリティカルでない拡張を解釈できないサーバは拡張を無視し（SHALL)、これをエラーとして返しては行けない（SHALL NOT)。拡張を解釈できるサーバは、クリティカルフラグのいかんに関わらず、この拡張を処理しなければならない（SALL）。解釈できないクリティカルな拡張に出会ったならサーバはこの要求をリジェクトし、この場合失敗（Failure）を返さなければならない（SHALL)。

CHANGE N*4:

セキュリティ考察（セクション４）の第１項の変更

理由コード拡張が key Compromiseのとき、対応する私有鍵で署名したトークンはすべて有効でないと考えなければならない（SHALL)。

理由コード拡張が affiliationChanged(3)や cessationOfOperation (5)のように他の理由の場合は、この理由コードは確定的である。しかし、後に key compromiseが起こったならばこのことは CAに報告されないであろう。TSAにとって望ましい対策は加入者に前もってこれから失効されることを警告することである。そうすれば加入者は以前のタイムスタンプトークンに別のタイムスタンプトークンを付けることができ、以前の TSUに対して証明書を発行した CAから CRLを得ることができる。

CHANGE N*5:

2.2 節の SHOULD→ should

CHANGE N*6:

2.4.1 節の SHOULD→ should

3.2　TSP 相互運用性テスト

IETFでは Proposed Standardから Draft Standardにステータスを上げるためには RFC 2026に沿って２つ以上の独立に実装したシステム間で相互運用性が確認される必要があること、RFCが引用する標準 RFCに Proposed Standardが含まれないこととしている。このために現在 10 の独立実装されたタイムスタンプサーバ間で相互運用性のテストが行われている。しかし現在の段階（2002.10）で相互運用性についてまだ完全な確認が成されていない。

TSPのテスト仕様は以下の URLで示されている。

http://www.imc.org/ietf-pkix/mail-archive/doc00004.doc

3.3　XMLタイムスタンププロトコル（TML)

最近（2002.10.24） OASISにおいて DigitalSignature Services Technical Committee（DSS TC）が創設されてWebサービスにおける XMLデジタル署名に関する標準化を図るとした。ここではWebサービスにおいての署名生成、署名検証および XML Time StampProtocolの

標準化を企画している。このXMLタイムスタンプは署名生成、署名検証の一部として位置付けられている。すなわち、タイムスタンプを付けた署名はタイムスタンプ時刻以前に存在していたことを示すものとして、署名検証時にその署名の有効性を確認する手段を提供する。現在まだDraftドキュメントは公開されていないがタイムスタンプの Draft XMLスキーマが近く公開される予定に成っている。この TCは 2002.12.2 に最初の TC Meetingが予定されている。

http://www.oasis-open.org/committees/dss/

XMLタイムスタンププロトコルはTML（Temporal Integrity Markup Language）と言い、ASN.1 ベースのRFC3161 をベースにほぼ 1 対 1 対応で XMLに置き換えたもので、RFC3161 のオプションなどで冗長性のある部分を省いた案が出されている。

関連するWebサービスのセキュリティ技術は

OASIS Access Control TC （XACML）

OASIS Rights Language TC （XrML）

OASIS Security Services TC （SAML）

OASIS Web Services Security TC （WSSTC）

W3C XML Signature

W3C XML Key Management

があるが、これらの TCとの連携をとって活動をして行こうとしている。

この TCは以下のメンバーが提唱者である。

Robert Zuccherato, Entrust Inc.；

Brian Phelps, Datum;

Bill Burr, NIST;

Jeremy Epstein, webMethods;

Don Adams, TIBCO.

3.4 ISO/IEC18014-3：2002（リンクトークンの生成メカニズム）

ISO/IECにおいて、タイムスタンプサービスに関する標準が JTC1/SC27 18014で検討されている。18014は３つのパートで構成されており、既に18014-1と18014-2が International Standard Publishedというステータス（ISOとしての正式文書）になっている。

18014-1……タイムスタンプサービス－ Part1：フレームワーク

18014-2……タイムスタンプサービス－ Part2：独立トークンの生成メカニズム

18014-3……タイムスタンプサービス－ Part3：リンクトークンの生成メカニズム

18014-3 はリンキングプロトコルを用いたタイムスタンプサービスに関する標準であり、現在 International Standard Publishedに向けた最終投票を実施している。2003 年前半には、International Standard Publishedとして正式に公開される予定である。

18014-3 では、リンキングプロトコルを採用した TSA間の相互運用を実現するために、主にTSAのオペレーション内容とタイムスタンプトークンのデータ構造について、検討を行っている。

オペレーションでは、リンキング、集約（aggregation）、パブリッシングの３つが規定されている。集約とは、リンク操作を複数のトークンに対して一括して行うオペレーションであり、これによりTSAは短時間で大量のタイムスタンプ要求に応えることができる。また、パブリッシングはリンク情報を広く公開することを意味している。このオペレーションにより、TSAにおけるリンク操作の完全性をアルゴリズムにより検証することが可能となり、その結果TSAの信頼性を確保することができる。

タイムスタンプトークンのデータ構造に関しては、以下のものが規定されている。

- オブジェクト識別子
- ノード
- リンク
- チェーン
- BindingInfo
- 拡張

ノードはリンク計算の対象となるデータを表すものであり、リンクはリンク計算で用いるアルゴリズムの種別とノードを含む。チェーンはチェーン計算時に用いるアルゴリズム種別とリンクを含んでいる。BindingInfoは、タイムスタンプトークンと過去のタイムスタンプトークンをリンクし、その結果をカプセル化して格納するためのものである。

4．NTP v4

2002 年 11 月時点において NTPv4 そのものは RFC/ Internet-Drafts ドキュメントになっていないため、以下の資料を参考に概要をまとめた。

NTP Architecture, Protocol and Algorithms

http://www.eecis.udel.edu/~mills/database/brief/arch/arch.pdf

NTP Version 4 Release Notes

http://www.eecis.udel.edu/~mills/ntp/html/release.htm

Public key Cryptography for the Network Time Protocol Version 2

http://www.ietf.org/internet-drafts/draft-ietf-stime-ntpauth-04.txt

Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI

http://www.ietf.org/rfc/rfc2030.txt

また、NTPv4 を理解する上では v3 に関する知識も必要となるため、本章の記述には v3 に関する内容も含む。

4.1 ネットワーク遅延と時計誤差の測定方法

NTP プロトコルヘッダに含まれているタイムスタンプを用いて、ネットワーク遅延と時計誤差を測定する（v3, v4 共通）。

タイムスタンプ名	ID	生成のタイミング
開始タイムスタンプ	T1	クライアントにより要求が送信された時刻
受信タイムスタンプ	T2	サーバにより要求が受信された時刻
送信タイムスタンプ	T3	サーバにより応答が送信された時刻
終了タイムスタンプ	T4	クライアントにより応答が受信された時刻

往復遅延 d、ローカル時計の誤差 t は次のように定義される。

d = (T4 - T1) - (T3 – T2)

t = ((T2 - T1) + (T3 - T4)) / 2

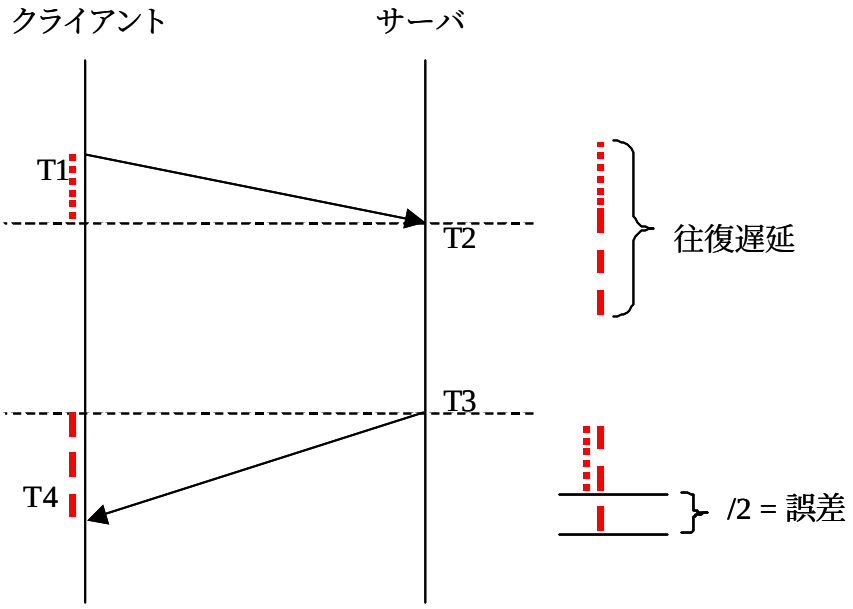

図 4－1　遅延と誤差の計算方法

その他、クロックフィルタリングや学習アルゴリズムにより、時計の校正を行う

4.2　NTPプロトコルヘッダ

4.2.1　NTP プロトコルヘッダとタイムスタンプフォーマット

NTPプロトコルヘッダを図 5－2 に示す。

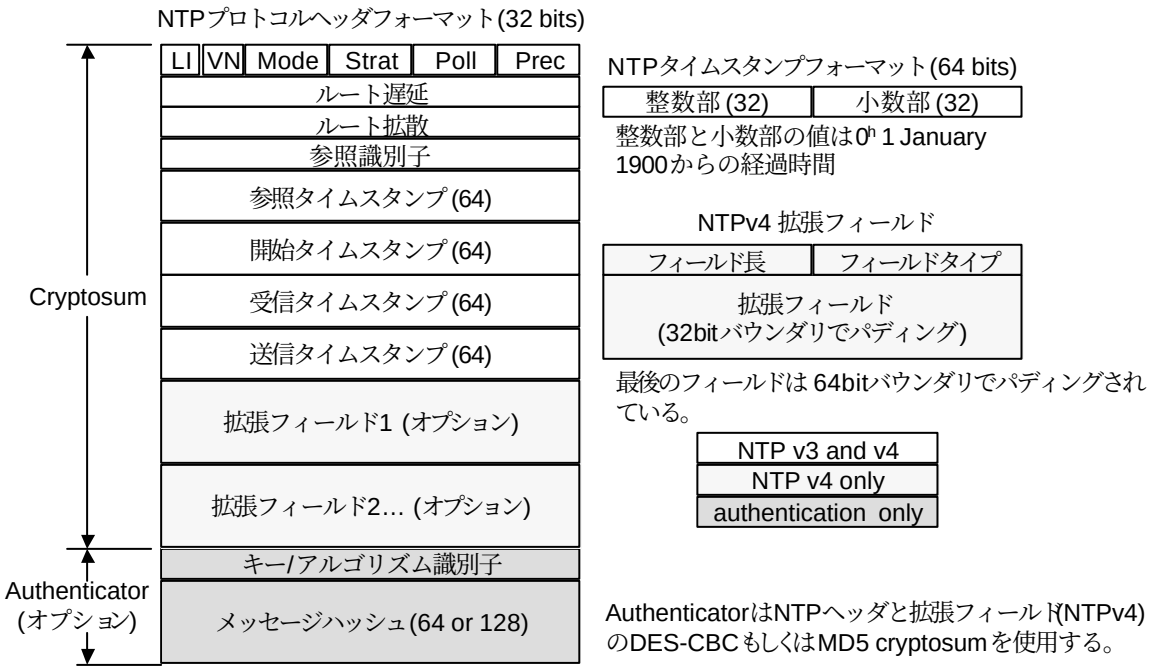

図 4－2　NTP プロトコルヘッダ

各フィールドの内容について、以下に簡単に説明する。

LI(閏秒指示子)……閏秒の挿入、削除を指示するために使用

VN(version number)……ntp/sntpのバージョン番号

Mode……ntpの動作モード

Strat(stratum)……時刻の参照レベルを表す整数

Poll……ポーリング間隔

Prec……ローカル時計の精度

ルート遅延……1次参照源までの往復遅延合計

ルート拡散……1次参照源との相対誤差

参照識別子……時刻の参照源(GPS、ラジオなど)を表す識別子

4.2.2 NTPv4拡張フィールド

NTPv4拡張フィールドのフォーマットを図5−3に記す。

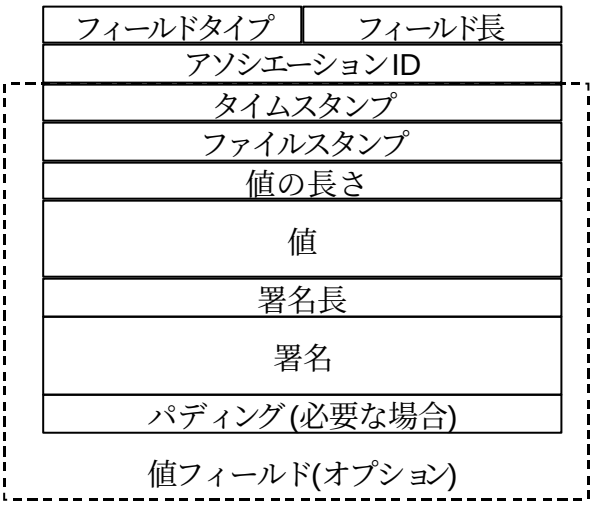

図4−3 NTPv4拡張フィールド

NTPv4ではAutokeyと呼ばれる認証方法を採用しており、これはクライアント・サーバ認証に使用されている。この認証に使用する署名データを、NTPv4拡張フィールドに格納する。署名の生成には、X.509 version 3の証明書を使用することができる。

4.3 NTPv4における認証の仕組み

4.3.1 NTPv3からの変更点(認証関連)

NTPv3では、ntpサーバが鍵ペアを生成、認証鍵(32bitの公開鍵)ファイルを作成し、クライアントは予めサーバから鍵ファイルを入手するという方式を採用している。

これに対し、NTPv4では新たに以下の機能が追加されている。

- Autokeyと呼ばれる認証方式の採用
- OpenSSLソフトウェアライブラリによる、メッセージダイジェストとデジタル署名の追加サポート
- 改善、簡易化された鍵管理
- X.509 version 3 証明書のサポート

これらの機能が実装されたことにより、証明書をベースにしたntpサーバの認証が可能となった。

4.3.2 NTP Autokey の概要

NTPメッセージは、セッションキーとメッセージダイジェストを用いて認証される仕組みとなっている。

セッションキーは、送信元アドレス、送信先アドレス、キー IDとクッキーから成る、16 オクテットのデータである。クッキーの値は、ntpの動作モードにより異なる。クライアント・サーバモードで動作する場合、クッキーはクライアントアドレス、サーバアドレス、キー ID、プライベート値のハッシュ値となる。クッキーに対して署名を生成し、タイムスタンプと共にこれを拡張フィールドに格納する。クッキーはサーバからクライアントに転送されるとき、クライアントの公開鍵で暗号化される。クライアントは、サーバからのリプライを検証し、リクエストキー IDとリプライキー IDが同一であることを確認するために、クッキーを使用する。

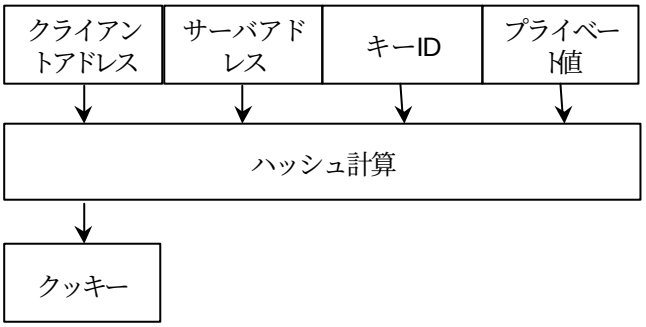

図 4−4　クッキーの計算

また、セッションキーのハッシュ値を生成し、この先頭4オクテットを次のキー IDとして用いる。この操作を繰り返し、サーバはセッションキー IDのリストを生成する。生成されたセッションキー IDリストの最終データ（インデックス番号とキー ID）から署名を生成し、タイムスタンプと共にこれを拡張フィールドに格納し、クライアントに対して提供する。

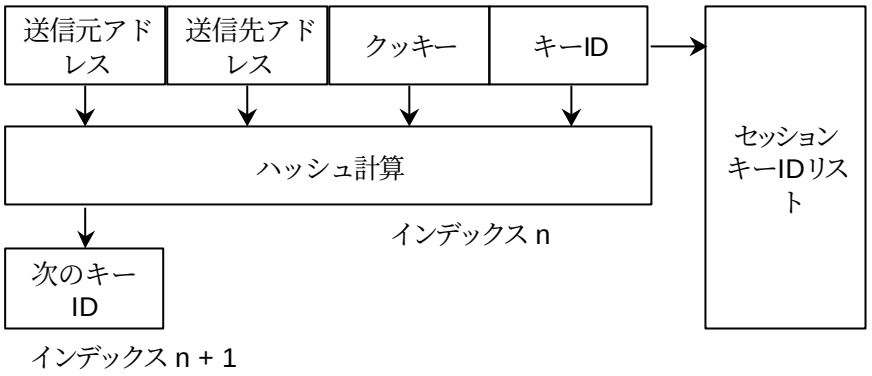

図 4−5　セッションキーリストの作成

メッセージを送受信する際には、メッセージハッシュとキー IDを用いて認証を行う。サーバでは、予め生成したセッションキー IDリストから1つのキー IDを取り出し、メッセージハッシュ（NTPヘッダと拡張フィールドから生成したハッシュ値）と組み合わせてMAC（図 5−2 のAuthenticatorに相当）に格納し、クライアントに送信する。クライアントは、受信したNTPヘッダと拡張フィールドからハッシュ値を計算し、MACに格納されているメッセージハッシュと比較する。また、アドレス、キー IDとクッキーからキー値を計算し、MACに格納されているキーIDと比較する。

ntpがクライアント・サーバモードで動作している場合、クッキーの生成にプライベート値を用いているため、クライアント・サーバのメンバ以外はメッセージの検証を行うことができず、正しいメッセージを生成することもできない。

付録

ETSI TS 102 023 V1.1.1 (2002-04)

技術仕様書

タイムスタンプ局のポリシー要件

参照番号

DTS/SEC-004005

キーワード

電子商取引、電子署名、セキュリティ、
タイムスタンプ、信頼サービス

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex – FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association a but non lucratif enregistree a la Sous-Prefecture de Grasse (06) N° 7803/88

重 要

この文書のダウンロード先：

http://www.etsi.org

この文書は、複数の電子バージョンまたは印刷物の形で入手可能である。各バージョンの内容に差異がある場合、ポータブル・ドキュメント・フォーマット (PDF) **のバージョンを基準とする。議論が生じた場合、ETSI 事務局内の特定のネットワークドライブに保存された** PDF **バージョンを** ETSI **のプリンタで印刷したものを基準とする。**

この文書の利用者は、改訂やステータス変更が行われることに注意する必要がある。

この文書およびほかの ETSI **文書の現在のステータスに関する情報の入手先**:

http://portal.etsi.org/tb/status/status.as

この文書内の誤りに対するコメントの送信先：

editor@etsi.fr

著作権について

Sophia Antipolis, 19 December 2002

Mr. Kazushige Kawamatsu

Kikai Shinko Kaikan Bldg. 3F
3-5-8 Shibakouen, Minato-ku
TOKIO 105-0011
JAPAN

Our ref.: L/2002-217/STR/mtc

Subject: Copyright Autorisation from ETSI to Kazushige Kawamatsu

Dear Mr. Kazushige Kawamatsu,

In response to your request of 25 November 2002, please be informed that the ETSI Standard TS 102 023 v 1.1.1 is protected by copyright and is the property of the European Telecommunications Standards Institute (ETSI).

By the present letter, ETSI is pleased to grant you the right to translate in your report "The present state of Time Business" the above-mentioned standard in Japanese provided that:

- you endorse full responsibility for the translation. ETSI shall not be held liable with regards to quality and content of the translation in Japanese, and
- due acknowledgment of the source " *Individual copies in English of the ESTI TS 102 023 v 1.1.1 can be downloaded from: http://www.etsi.org*" is inserted whenever and wherever appropriate.

Should the above information fall under patent protection, the present copyright authorisation is not to be construed as an authorisation to use and/or implement patent information without fulfilling any attached obligations.

Yours sincerely,

K. H. Rosenbrock

Karl Heinz Rosenbrock
Director-General

European Telecommunications Standards Institute - Institut européen des normes de télécommunication - Europäisches Institut für Telekommunikationsnormen
ETSI - 650, route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE
e-mail : secretariat@etsi.fr - http://www.etsi.fr
Tél. : +33 (0)4 92 94 42 00
Fax : +33 (0)4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C - Association à but non lucratif enregistrée à la Sous-Préfecture de Grasse (06) N° 7803/88 - N° TVA : FR 14 348 623 562
InfoCentre : Tel. : +33 (0)4 92 94 42 22 - Fax : +33 (0)4 92 94 43 33 - e-mail : infocentre@etsi.fr

目次

知的所有権について……51
前書き……51
はじめに……51
1　適用範囲……53
2　参考文献……53
3　定義と略語……54
3.1　定義……54
3.2　略語……55
4　一般的概念……55
4.1　タイムスタンプ・サービス……55
4.2　タイムスタンプ局……55
4.3　加入者……56
4.4　タイムスタンプ・ポリシーと TSA 実施規定……56
4.4.1　目的……56
4.4.2　詳細レベル……56
4.4.3　アプローチ……56
5　タイムスタンプ・ポリシー……56
5.1　概要……56
5.2　識別……57
5.3　利用者コミュニティと適用性……57
5.4　順守性……57
6　義務と賠償責任……58
6.1　TSA の義務……58
6.1.1　全般……58
6.1.2　TSA の加入者に対する義務……58
6.2　加入者の義務……58
6.3　依存者の義務……58
6.4　賠償責任……58
7　TSA の実施に関する要件……59
7.1　実施および開示規定……59
7.1.1　TSA 実施規定……59
7.1.2　TSA 開示規定……60
7.2　鍵管理ライフサイクル……61
7.2.1　TSA 鍵の生成……61
7.2.2　TSA 秘密鍵の保護……61
7.2.3　TSA 公開鍵の配布……62

7.2.4 TSA 鍵の再発行……62
7.2.5 TSA 鍵のライフサイクルの終了……62
7.2.6 タイムスタンプへの署名に使用される暗号モジュールのライフサイクル管理……63
7.3 タイムスタンピング……63
7.3.1 タイムスタンプ・トークン……63
7.3.2 UTC との時計の同期……64
7.4 TSA の管理および運営……64
7.4.1 セキュリティ管理……64
7.4.2 資産分類と管理……65
7.4.3 人員のセキュリティ……65
7.4.4 物理的および環境的セキュリティ……67
7.4.5 運用管理……67
7.4.6 システム・アクセス管理……69
7.4.7 信頼あるシステムの開発とメンテナンス……69
7.4.8 SA サービスの危殆化……70
7.4.9 TSA の閉鎖……70
7.4.10 法的要件の順守……71
7.4.11 タイムスタンプ・サービスの運営に関する情報の記録……71
7.5 組織について……72

附属書 A (参考): タイムスタンプ・サービスの提供における潜在的賠償責任……74
附属書 B (参考): モデル TSA 開示規定……75
B.1 概要……75
B.2 TSA 開示規定の構成……76
附属書 C (参考): 協定世界時……77
附属書 D (参考): タイムスタンプ・トークンの長期的検証……79
附属書 E (参考): 実装アーキテクチャ - タイムスタンプ・サービス……80
E.1 管理されるタイムスタンプ・サービス……80
E.2 選択的代替クオリティ……81
附属書 F (参考): 参考文献……82
履歴……83

知的所有権について

この文書に含まれる知的所有権またはその可能性のある知的所有権は既に ETSI に申告されている場合がある。これらの知的所有権に関連する情報があれば、その情報は、ETSI の会員および会員以外に公開され、ETSI から入手可能な ETSI SR 000 314: "Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards (知的所有権 (IPR); ETSI 規格に関して ETSI に通知される重要な IPR または潜在的に重要な IPR)" で参照できる。最新の更新は ETSI の Web サーバー (http://webapp.etsi.org/IPR/home.asp) に掲載されている。

ETSI の知的所有権に関する方針に従い、これまで ETSI によって知的所有権を含む調査は行われていない。この文書に含まれるか、または現在あるいは将来においてその可能性があるが、ETSI SR 000 314 (もしくは ETSI Web サーバー上の更新) では言及されていないほかの知的所有権の存在については、いかなる保証も与えることができない。

前書き

この技術仕様書 (TS) は ETSI セキュリティ技術委員会 (SEC) によって作成された。

はじめに

信頼性の高い管理可能なデジタル証明書の作成においては、時間データをトランザクションに関連付け、後で互いに比較できるようにする統一的な手法が必要になる。こうした証明書のクオリティに基づいて行われるのが、イベントとそれらを実際の世界に結びつけるパラメータ・データ・ポイントのクオリティを表すデータ構造の作成および管理処理である。ここでは、時間データとその使用方法について述べる。
また、電子署名を検証するためには、署名者のデジタル署名の適用が署名者の証明書の有効期間中に行われたことを証明しなければならない場合がある。これは以下の 2 つの状況において必要となる。

1) 署名者の証明書の有効期間中に署名者の秘密鍵が危殆化し、それにより失効した場合。
2) 署名者の証明書の有効期間終了後、認証局 (CA) は、自局の発行した証明書の失効ステータス情報を処理する義務がないため。

この問題を解決するには、2 種類の一般的方法がある。一つは、タイムマークを使用する方法である。タイムマークは、信頼ある第三者機関のセキュアな監査証跡に保管された監査記録であり、署名値に日付を付加する。これにより、署名がタイムマークの日付以前に生成されたことが証明される。この方法は、本仕様書では取り上げない。

もう一つは、あるデータが特定時刻以前に存在していたことを証明できるタイムスタンプを使用する方法である。この方法により、タイムスタンプ・トークンに格納された日付以前に署名が生成されたことの証明が可能になる。このようなケースに対応するポリシー要件が、本仕様書を提供する一義的理由である。

ただし、これらのポリシー要件はほかのニーズにも対応可能であることに注意する必要がある。電子タイムスタンプは、ビジネス界でますます大きな関心を集め、電子署名の重要な要素となっており、IETF (RFC 3161) のタイムスタンプ・プロトコルに準拠した ETSI 電子署名フォーマット規格 TS101 733 でも扱っている。長期的な電子署名の信頼ある検証を可能にするには、統一的な最小限のセキュリティおよびクオリティ要件が必要である。

電子署名の共同体枠組みに関する欧州議会および 1999 年 12 月 13 日欧州理事会指令 1999/93/EC は、認証サービス・プロバイダを「証明書を発行したり、電子署名関連のほかのサービスを提供したりするエンティティまたは法・自然人」と定義している。認証サービス・プロバイダの一例がタイムスタンプ局である。

1 適用範囲

本仕様書は、タイムスタンプ局 (TSA) の運営に関連するポリシー要件を定める。本仕様書が TSA の運営・管理実施についてポリシー要件を定めるのは、加入者と依存者がタイムスタンプ・サービスの運営に対して信頼感を持てるようにするためである。

これらの要件は（電子署名の共同体枠組みに関する欧州指令第 5.1 条などに従って）電子署名の証明に使用されるタイムスタンプ・サービスを主な目的としているが、あるデータが特定の時刻以前に存在していたことの証明が必要なあらゆる目的に使用できる。

これらのポリシー要件は公開鍵暗号、公開鍵証明書、信頼できるタイムソースの使用を前提としている。

本仕様書は、TSA がタイムスタンプ・サービスの提供にあたって信頼できることを確認するための基準として、独立機関によって使用される。

本仕様書は、タイムスタンプ・トークンを発行する TSA の要件を対象としている。それらのタイムスタンプ・トークンは、協定世界時 (UTC) と同期し、TSA によってデジタルで署名される。

加入者と依存者は、本タイムスタンプ・ポリシーの特定の TSA による正確な運用方法（サービス提供に使用されるプロトコル）について詳細を入手するには、TSA の実施規定を参照する必要がある。

本仕様書は、以下を定めていない。

- TSA へのアクセスに使用されるプロトコル
  注記 1： タイムスタンプ・プロトコルは RFC 3161 で定義され、TS 101 861 で概要が説明されている。
- 本仕様書に定めた要件が独立機関によって評価される方法
- 独立機関が情報を利用可能できるようになるための要件
- 独立機関に関する要件
  注記 2：CEN Workshop Agreement 14172 "EESSI Conformity Assessment Guidance (EESSI 適合性認定の手引き)" を参照。

2 参考文献

以下の文書は、本仕様書内の規定で参照される規定を含んでいる。

- 参照には、(刊行日および/またはエディション番号あるいはバージョン番号によって) 指定されたものと指定されないものがある。
- 指定された参照では、その後の改訂は適用されない。
- 指定されない参照では、最新バージョンが適用される。

[1] ITU-R Recommendation TF.460-5 (1997): "Standard-frequency and time-signal emissions (標準周波数と時刻信号の発生)"

[2] ITU-R Recommendation TF.536-1 (1998): "Time-scale notations (時間スケールの表記法)"

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free

movement of such data (個人データの処理に関する個人の保護およびデータの自由な移動に関する欧州議会および 1995 年 10 月 24 日欧州理事会指令 95/46/EC)
[4] FIPS PUB 140-1 (1994): "Security Requirements for Cryptographic Modules (暗号モジュールのセキュリティ要件)"
[5] ISO/IEC 15408 (1999) ISO/IEC 15408 (1999) (parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security (情報技術 - 機密保持手法 - IT セキュリティの評価基準)"
[6] CEN Workshop Agreement 14167-2 : "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP) (電子署名の証明書管理を行う信頼できるシステムのセキュリティ要件 - 第 2 部 CSP 署名処理のための暗号モジュール - 保護プロファイル (MCSO-PP))"

3 定義と略語

3.1 定義

本使用書の目的に応じて、以下の用語と定義が使用される。

注記 : 定義を参考文献から引用した場合、その定義の末尾に参照番号を付すことにより、その旨を示す。

依存者 (relying party) : タイムスタンプ・トークンの受信者。そのタイムスタンプ・トークンに依存している。

加入者 (subscriber) : TSA によりデータにタイムスタンプを付与するよう要求するエンティティ

タイムスタンプ・トークン : データの表現を特定の時刻に結びつけ、これによってその時刻以前にデータが存在したことを証明するデータオブジェクト

タイムスタンプ局 : タイムスタンプ・トークンを発行する機関

TSA 開示規定 : 法的要件を満足するために加入者や依存者への強調または開示などを特に要求する、TSA のポリシーおよび実施に関する一連の規定

TSA 実施規定 : TSA がタイムスタンプ・トークンを発行する際に採用する実施規定

TSA システム : タイムスタンプ・サービスの提供を支援する IT 製品および部品の構成物

タイムスタンプ・ポリシー : 共通のセキュリティ要件のもとで、特定のコミュニティまたはアプリケーションに対するタイムスタンプ・トークンの適用可能性を示す規則の集まり。

タイムスタンプ・ユニット : 1 つの単位として管理され、一度にただ 1 つのタイムスタンプ・トークンの署名鍵を有効にするハードウェアおよびソフトウェアの集まり

協定世界時 (UTC) : ITU-R Recommendation TF.460-5 [1]に定められた秒数を単位にした時間スケール

注記 : ほとんどの実用的な目的で UTC はグリニッジ子午線 (0°) における平均太陽時に等しい。正確には、UTC は、安定した国際原子時 (Temps Atomique International - TAI) を基にして、地球の不規則な回転 (グリニッジ平均恒星時 (GMST) に関連) による太陽時との誤差を修正したもの(詳細については附属書 C を参照)。

UTC(k) : 誤差±100 ナノ秒 (ns) を目標にして研究所 "k" によって実現され、UTC との一致が保持されている時間スケール(ITU-R Recommendation TF.536-1 [2] 参照)
注記：UTC (k) の研究所のリストは、国際度量衡局 (BIPM) の配布する「Circular T」第 1 節に記載されており、BIPM の Web サイト (http://www.bipm.org/) から入手できる。

3.2 略語
本仕様書の目的に応じて、以下の略語が使用される。

TSA タイムスタンプ局
TSA タイムスタンプ・トークン
UTC 協定世界時

---

4 一般的概念

4.1 タイムスタンプ・サービス
本仕様書では、要件を分類する目的で、タイムスタンプ・サービスの提供が以下のコンポーネントに細分化される。

- タイムスタンプ付与 : このサービス・コンポーネントはタイムスタンプ・トークンを生成する。
- タイムスタンプ管理 : 提供されるサービスの TSA の規定への準拠を確保するため、タイムスタンプ・サービスの運用を監視し、制御するサービス・コンポーネント。
  このサービス・コンポーネントは、タイムスタンプ付与サービスの実装および削除を受け持つ。例えば、タイムスタンンピングに使用される時計を UTC に正確に同期する。

このサービスの下位区分は、本仕様書で定める要件を明確にする目的でのみ使用され、タイムスタンプ・サービスの実施のあらゆる下位区分に対してなんら制限事項を設けない。

4.2 タイムスタンプ局
タイムスタンプ・サービスの利用者 (加入者および依存者) によって信頼され、タイムスタンプ・トークンの発行を行う機関はタイムスタンプ局 (TSA) と呼ばれる。TSA は、第 4.1 項に定めるタイムスタンプ・サービスの提供について全般的責任を負う。TSA の鍵はタイムスタンプ・トークンに署名するために使用され、TSA はタイムスタンプ・トークンにおいて発行者として識別される。

TSA は、ほかの関係者を活用してタイムスタンプ・サービスの一部を提供できる。ただし、TSA は、常に全般的責任を負い、本仕様書に定めたポリシー要件が満たされていることを保証する。例えば、TSA は、TSA の鍵を使用してタイムスタンプを生成するサービスを含むあらゆるコンポーネント・サービスを外部委託することができる。ただし、秘密鍵およびタイムスタンプ・トークの生成に使用される鍵は、本仕様書に定める要件の満足に対して全般的責任を負う TSA に属するものとされる。

TSA は、識別可能な複数のタイムスタンプ・ユニットを運用することができる。各ユニットは異なる鍵を有する。

TSA は、電子署名に関する EU 指令 (第 2 (11) 条参照) に定める通り、タイムスタンプ・トークンを発行する認証サービス・プロバイダである。

4.3 加入者

複数または単一のエンドユーザーで構成される組織を加入者とすることができる。

加入者が組織の場合、その組織に適用される義務の一部は、エンドユーザーにも適用されるものとする。いかなる場合においても、組織は、エンドユーザーの義務が正しく果たされない場合に責任を負い、したがって、組織は、そのエンドユーザーに対して情報を適切に提供することが期待されている。
加入者がエンドユーザーの場合、そのエンドユーザーは、その義務が正しく果たされていない場合に直接責任を負う。

4.4 タイムスタンプ・ポリシーと TSA 実施規定

本項では、タイムスタンプ・ポリシーと TSA 実施規定の対応する役割について説明する。この説明は、タイムスタンプ・ポリシーまたは実施規定の仕様の形式に制限事項をなんら設けない。

4.4.1 目的

一般的に見て、タイムスタンプ・ポリシーは「何を順守するか」について定めるのに対して、TSA 実施規定は、タイムスタンプの作成やその時計の精度の維持に使用するプロセスなど、「どのように順守するか」について定める。タイムスタンプ・ポリシーと TSA 実施規定の関係は、業務の要件を定めたほかの業務ポリシー同士の関係に性質が似ているが、これらのポリシーの運用方法について実施や手順を定義するのは、各運用組織である。

本仕様書では、タイムスタンプ・ポリシーが信頼あるタイムスタンプ・サービスの一般的要件を満足するように定めている。TSA はこれらの要件がどのように満足されるかを定める。

4.4.2 詳細レベル

タイムスタンプ・ポリシーは、TSA 実施規定よりも大まかな文書である。TSA 実施規定は、条件だけでなく、発行やほかのタイムスタンプ・サービス管理における TSA の業務および運営実施についても詳細に説明している。TSA の TSA 実施規定は、タイムスタンプ・ポリシーによって定められた規則を運用する。TSA 実施規定は、タイムスタンプ・ポリシーに定められた技術・組織・手順に関する要件を特定の TSA がどのように満足するかについて定めている。

注記 : より下位レベルの内部文書であっても、その TSA 実施規定に定めた実施を行うのに必要な特定の手順について詳細に定める TSA には適切な場合がある。

4.4.3 アプローチ

タイムスタンプ・ポリシーのアプローチは、TSA 実施規定とは大きく異なっている。タイムスタンプ・ポリシーは、TSA の特定運営環境の具体的詳細とは無関係に定められるが、TSA 実施規定は、TSA の組織構造、運営手順、施設、コンピューティング環境に応じて定められる。タイムスタンプ・ポリシーは、タイムスタンプ・サービスの利用者が定めることができるが、TSA 実施規定は必ずプロバイダによって定められる。

---

5 タイムスタンプ・ポリシー

5.1 概要

タイムスタンプ・ポリシーは、「共通のセキュリティ要件のもとで、特定のコミュニティまたはアプリケーションに対するタイムスタンプ・トークンの適用可能性を示す規則の集まり」である (第 3.1 項および第 4.4 項参照)。本仕様書は、タイムスタンプ・トークンと公開鍵証明書を 1 秒またはそれ以上の精度で発行する TSA を対象として、ベースライン・タイムスタンプ・ポリシーの要件を定める。

注記 1： 依存者は、追加措置がなければ、証明書の有効期間終了後タイムスタンプ・トークンの有効性を確保することはできない。TSA の証明書の有効期間終了後のタイムスタンプ・トークンの有効性の検証については附属書 D を参照。

TSA は、本仕様書に定めたポリシーを拡張する独自のポリシーを定めることができる。こうしたポリシーは、本仕様書に定めた要件を組み込むか、またはさらに制限いなければならない。

1 秒以上の精度が TSA によって実現されている場合、その精度が TSA の開示規定 (第 7.1.2 項参照) および 1 秒以上の精度で発行された各タイムスタンプ・トークンに示されなければならない。

注記 2： タイムスタンプ・トークンは、適用可能なポリシーの識別子を含まなければならない(第 7.3.1 項参照)。

5.2 識別

ベースライン・タイムスタンプ・ポリシーのオブジェクト識別子は以下の通り。

```
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(02023)
policy-identifiers(1)
baseline-ts-policy (1)
```

TSA はまた、対応しているタイムスタンプ・ポリシーの識別子を TSA 開示規定に示し、加入者や依存者に明らかにすることにより、ポリシーを順守していることを示さなければならない。

5.3 利用者コミュニティと適用性

本ポリシーは、有効期間 (TS 101 733 などに定義) の長いタイムスタンプ付き電子署名 (電子署名に関する欧州指令参照) を満足することを目的としているが、同等のクオリティのあらゆる用途に広く適用可能である。

本ポリシーは、公的なタイムスタンプ・サービスまたは閉じたコミュニティ内で利用されるタイムスタンプ・サービスに適用することができる。

5.4 順守性

TSA は、第 5.2 項に定めるタイムスタンプ・トークン内のタイムスタンプ・ポリシーの識別子を使用するか、または、以下の場合には、本仕様書に定めた要件を組み込む、あるいはさらに制限する独自のタイムスタンプ・ポリシーを定めなければならない。

a) TSA が定められたタイムスタンプ・ポリシーの順守を主張し、その順守の主張を証明する証拠を加入者や依存者に要求に応じて提供できる場合
b) 独立機関によって TSA が定められたタイムスタンプ・ポリシーを順守していると評価された場合

仕様を順守する TSA は以下を示さなければならない。

a) 第 6.1 項に定める義務を果たしていること
b) 第 7 項に定める規制を満足する規制を実施してきたこと

6 義務と賠償責任

6.1 TSA の義務

6.1.1 全般

TSA は、第 7 項に詳述する TSA に関するすべての要件が満足され、選択された信頼あるタイムスタンプ・ポリシーに適用できることを保証しなければならない。

TSA は、TSA の機能を下請業者が引き受ける場合においても、本ポリシーに定められた手順の順守を保証しなければならない。

TSA はまた、タイムスタンプに直接示されるか、または参照によって組み込まれたあらゆる付加的な義務も果たさなければならない。

TSA はそのタイムスタンプ・サービスをすべて、その実施規定に従って提供しなければならない。

6.1.2 加入者に対する TSA の義務

TSA は、そのサービスの利用可能性と正確性を含めて条件に指定した通り、その主張を満足させなければならない。

6.2 加入者の義務

本仕様書は、TSA の条件に定めた TSA 固有の要件以外には、加入者に具体的義務を課すことはしない。

注記 : 加入者はタイムスタンプ・トークンを取得するとき、タイムスタンプ・トークンに正しく署名が行われていること、また、タイムスタンプ・トークンへの署名に使用される秘密鍵が危殆化されていないことを検証することが推奨される。

6.3 依存者の義務

依存者が入手できる条件 (第 7.1.2 項参照) は、依存者がタイムスタンプ・トークンに依存する場合の以下のような義務を含まなければならない。

a) タイムスタンプ・トークンに正しく署名が行われたことの検証、および、タイムスタンプに署名するのに使用された秘密鍵がその時点まで危殆化されなかったことの検証

注記 : TSA 証明書の有効期間中に署名鍵の有効期間は、TSA の証明書の現在の失効ステータスを使用してチェックすることができる。検証時刻が有効期間の終了時刻を超過している場合には附属書 D を参照。

b) タイムスタンプ・ポリシーに定められたタイムスタンプの使用に関する制限事項の考慮

c) 契約その他で定められたそのほかのあらゆる制限事項の考慮

6.4 賠償責任

本仕様書は、賠償責任に関する要件について定めていない。とりわけ、特に法律で定めない限り、TSA はあらゆる賠償責任を負わないか、制限できることに注意する必要がある。

詳細については附属書 A を参照。

7 TSA の実施に関する要件

TSA は以下の要件を満足する管理を実施しなければならない。

これらのポリシー要件は、TSA サービスの料金請求に対するなんらかの制限を示すことを意図されていない。

要件はセキュリティ目標ごとに示され、セキュリティ目標達成の信頼性獲得に必要と考えられる場合には、目標を達成するためのより具体的な管理要件も補足される。

注記 :ある目標の達成に要求される管理の詳細は、必要な信頼性の獲得と、TSA がタイムスタンプ・トークンの発行時に採用可能な手法に対する制限の最小化の間のバランスである。第 7.4 節 (TSA の管理と運営) の場合、より詳細な管理要件のソースとして使用可能なほかのより一般的規格が参照されている。これらの原因により、特定の表題のもとで定められた要件の詳細さが変わる場合がある。

要求に対する応答にタイムスタンプ・トークンを含めるかどうかは、加入者とのサービス・レベルの契約に応じて TSA によって判断される。

7.1 実施および開示規定

7.1.1 TSA 実施規定

TSA は、タイムスタンプ・サービスの提供に必要な信頼性を示すことを保証するものとする。
特に以下を定めなければならない。

a) TSA はビジネス資産およびそれらの資産への脅威を評価し、必要なセキュリティ管理と運営手順を決定するため、リスク調査を実施しなければならない。
b) TSA は本タイムスタンプ・ポリシーに定められたすべての要件を満足するために使用される実施規定および手順を用意しなければならない。

注記 1： このポリシーは、TSA 実施規定に関して要件を定めていない。

c) TSA の実施規定は、該当するポリシーや実施を含め、TSA サービスを支援するあらゆる外部組織の義務を定めなければならない。

d) TSA は加入者と依存者がその実施規定や、タイムスタンプ・ポリシーの順守評価に必要なその他の関連文書を入手できるようにしておかなければならない。

注記 2：TSA は、必ずしも一様にその実施の詳細をすべて公にするよう要求されるわけではない。

e) TSA は、第 7.1.2 項に定める通り、すべての加入者と潜在的依存者に対して、
そのタイムスタンプ・サービスの使用に関する条件を開示しなければならない。

f) TSA は、TSA 実施規定を承認する決定権限を備えた高レベルの管理組織を有さなければならない。

g) TSA の上層部経営者は、実施が適切に行われることを保証しなければならない。

h) TSA は、TSA 実施規定の管理責任を含めた実施の審査プロセスを定めなければならない。

i) TSA は、意図する実施規定の変更について適正な通知を行わなければならない、また、上記 (f) の承認の後、改訂した TSA 実施規定を上記 (d) に定める通り直ちに入手できるよ

うにしなければならない。

7.1.2 TSA 開示規定

TSA はすべての加入者と依存者に対して、タイムスタンプ・サービスの使用に関する条件を開示しなければならない。

この規定は、TSA が対応している各タイムスタンプ・ポリシーについて少なくとも以下を定めるなければならない。

a) TSA の契約情報

b) 適用されているタイムスタンプ・ポリシー

c) タイムスタンプが付与されるデータを表現するために使用されている少なくとも 1 つのハッシュ・アルゴリズム

d) タイムスタンプ・トークンに署名するために使用される署名の予想寿命 (使用されるハッシュ・アルゴリズム、使用される署名アルゴリズム、および秘密鍵の長さに依存)

e) タイムスタンプ・トークン内の時刻の UTC に対する精度

f) タイムスタンプ・サービスの使用に関するあらゆる制限事項

g) 場合に応じて第 6.2 項に定められた加入者の義務

h) 第 6.3 項に定められた依存者の義務

i) 依存者がタイムスタンプ・トークンに「合理的に依存」しているとみなされるよう、タイムスタンプ・トークンの検証方法に関する情報(第 6.3 項)および有効期間に関するあらゆる制限事項

j) TSA のイベント・ログ (第 7.4.10 参照) が保持される期間

k) 国内法のもとでタイムスタンプ サービスに対する要件を満足しているとの主張を含めた適切な法体系

l) 賠償責任の制限

m) 苦情や紛争解決の手順

n) TSA が定められたタイムスタンプ・ポリシーを順守していると評価されているかどうか、および、評価されている場合には独立した評価機関

注記 1： また、TSA がそのタイムスタプ開示規定の中に、タイムスタンプ・サービスの予想平均故障時間、平均回復時間、およびバックアップ・サービスなどの障害回復のための規定を含めることが推奨される。

この情報は、耐久性のある通信手段によって利用可能でなければならない。この情報は、即座に理解可能な言語を通じて提供されなければならない。この情報は電子的に送信できる。

注記 2： そのような通信の土台として使用できる TSA 開示規定のモデルが附属書 B に示されている。あるいは、これを加入者/依存者契約の一部として提供することもできる。これらの TSA 開示規定が読み手の目にふれやすい場合には、TSA 実施規定に含めることもできる。

7.2 鍵管理ライフサイクル

7.2.1 TSA 鍵の生成

TSA は、管理環境のもとであらゆる暗号鍵が生成されることを保証しなければならない。

特に以下を定める。

a) TSA の署名鍵の生成は、物理的にセキュアな環境 (第 7.4.4 項参照) において信頼ある役割につく人員 (第 7.4.4 項) により、少なくとも二重管理のもとで行われなければならない。
この機能の遂行を許可されるのは、TSA の実施のもとで、そのような行為が必要とされる者に制限されるものとする。

b) TSA の署名鍵の生成は、以下のいずれかの暗号モジュール内で実行されなければならない。
- FIPS 140-1 [4] レベル 3 以上に定める要件を満足するモジュール。
- CEN Workshop Agreement 14167-2 [6] に定める要件を満足するモジュール。
- ISO 15408 [3] の EAL 4以上または同等のセキュリティ基準が保証された信頼あるシステム。

リスク分析に基づき、また、物理的およびその他の非技術的セキュリティ対策を考慮して、これを本仕様書の要件を満足するセキュリティ目標または保護プロファイルとしなければならない。

c) TSA 鍵生成アルゴリズム、生成する署名鍵の長さ、およびタイムスタンプ・トークンの鍵に使用される署名アルゴリズムは、国家的監督組織によって認定されるか、または、TSA 発行のタイムスタンプ・トークンの目的に合致した最新のアルゴリズムに準ずるものでなければならない。

注記 : 署名アルゴリズムと鍵の長さに関する概要は、"Algorithms and parameters for Secure Electronic Signatures (セキュアな電子署名のアルゴリズムとパラメータ)"(EESSI-SG (欧州電子署名標準化構想運営グループ) の下で活動するアルゴリズムグループ (ALGO) が刊行) を参照。

7.2.2 TSA 秘密鍵の保護

TSA は、TSA 秘密鍵が機密性を保持し、その完全性を維持することを保証しなければならない。

特に以下を定める。

a) TSA 秘密鍵は、以下のいずれかの暗号モジュール内に保持され、使用されなければならない。
- FIPS 140-1 [4] レベル 3 以上に定める要件を満足する。
- CEN Workshop Agreement 14167-2 [6] に定める要件を満足する。
- ISO 15408 [3] の EAL 4以上または同等のセキュリティ基準が保証された信頼あるシステム。

リスク分析に基づき、また、物理的およびその他の非技術的セキュリティ対策を考慮して、これを本仕様書の要件を満足するセキュリティ目標または保護プロファイルとしなければならない。

注記 : 鍵の危殆化のリスクを最小限に抑えるため、TSA 秘密鍵のバックアップはすべきでない。

b) TSA 秘密鍵のバックアップを行う場合、物理的にセキュアな環境において信頼ある役割につく人

員のみが少なくとも二重管理を使用してコピー、保存、回復を行わなければならない。(第 7.4.4 項参照)
この機能の遂行を許可されるのは、TSA の実施のもとで、そのような行為が必要とされる者に制限されなければならない。

C) TSA 秘密署名鍵のあらゆるバックアップ・コピーは、そのユニット以外に保存される前に暗号モジュールによって保護され、機密性が保持されなければならない。

7.2.3 TSA 公開鍵の配布

TSA は、TSA 署名検証 (公開) 鍵とあらゆる関連パラメータの完全性および真正性が依存者への配布中に維持されることを保証しなければならない。

特に以下を定める。

a) TSA 署名検証 (公開) 鍵は、公開鍵証明書の中で依存者が利用できなければならない。

注記 ： 例えば、TSA の証明書は、TSA と同じ組織によって運営される認証局、またはほかの機関が発行できるものとする。

b) TSA の署名検証 (公開) 鍵証明書は、このタイムスタンプ・ポリシーと同等またはそれ以上のセキュリティのレベルを定める証明書ポリシーにもとで運営される認証局によって発行されなければならない。

7.2.4 TSA 鍵の再発行

TSA の証明書の寿命は、選択されたアルゴリズムと鍵の長さが目的に合致したものとして認定されている期間より長くしてはならないものとする (第 7.2.1c) 参照)。

注記 1 : 寿命を制限する際、以下の追加事項が検討される。
- 第 7.4.10 項に従って、タイムスタンプ・サービスに関するレコードが TSA 署名鍵の有効期間終了後少なくとも 1 年間保持されなければならない。TSA 証明書の有効期間が長くなると、保持されるレコードのサイズは長くなる。
- TSA 秘密鍵が危殆化された場合、寿命が長くなればなるほど、そのタイムスタンプ・トークンはより多くの影響を受ける。

注記 2 : TSA 鍵の危殆化は、使用されている暗号モジュールの特性だけでなく、システムの初期化と鍵のエクスポート (この機能がサポートされている場合) で使用される手順によっても決まる。

7.2.5 TSA 鍵のライフサイクルの終了

TSA は、TSA 秘密署名鍵は、そのライフサイクル終了後は使用されないことを保証しなければならない。
特に以下を定める。

a) TSA の鍵が期限切れになった場合に新しい鍵を提供するための運営上または技術上の手順が定められなければならない。

b) TSA 秘密署名鍵、または、あらゆるコピーを含むあらゆる鍵の部分は破壊され、秘密鍵が取得できないようにしなければならない。

c) 署名秘密鍵が期限切れになった場合、TST 生成システムは、TST を発行するあらゆる試みを拒否するものとする。

7.2.6 タイムスタンプへの署名に使用される暗号モジュールのライフサイクル管理

TSA は、そのライフサイクルを通じて暗号ハードウェアのセキュリティを確保されなければならない。
特に TSA は以下を保証しなければならない。

a) タイムスタンプ・トークン署名暗号ハードウェアは、出荷時に改変されないものとする。

b) タイムスタンプ・トークン署名暗号ハードウェアは、保管時に改変されないものとする。

c) 暗号ハードウェアへの TSA 署名鍵の導入、有効化、複製は、物理的にセキュアな環境において信頼ある役割につく人員のみが行わなければならない (第 7.4.4 項参照)

d) タイムスタンプ・トークン署名暗号ハードウェアが正常に動作すること

e) TSA 暗号モジュールに保存された TSA 秘密署名鍵は、装置の使用を終了する際に消去する。

7.3 タイムスタンピング

7.3.1 タイムスタンプ・トークン

TSA は、タイムスタンプ・トークンがセキュアに発行され、正しい時刻を含むことを保証しなければならない。

特に以下を定める。

a) タイムスタンプ・トークンは、タイムスタンプ・ポリシーの識別子を含まなければならない。

b) 各タイムスタンプ・トークには、一意の識別子が与えられなければならない。

c) TSA がタイムスタンプ・トークンにおいて使用する時刻値は、UTC(k) の研究所によって配信される実際の時刻値の少なくとも 1 つに基づくものでなければならない。

注記 1：国際度量衡局 (BIPM) は、世界中の国家的気象台および国家的天文観測所の原子時計から現地の UTC(k)に基づき UTC を計算する。BIPM は、月刊の Circular T [List 1] を通じて UTC の普及を行う。この刊行物は、BIPM の Web サイト (www.bipm.org) で入手可能であり、認定 UTC(k)時間スケールを有するすべての研究所を公式に指定している。

d) タイムスタンプ・トークンに含まれる時刻は、このポリシーに定める精度内、または、タイムスタンプ・トークンそのものに精度が定められている場合にはその精度内で UTC と同期するものでなければならない。

e) タイムスタンプ・プロバイダーの時計が定められた精度 (第 7.1.2e)項参照) 外にあると分かった場合 (第 7.3.2c)項参照)、タイムスタンプ・トークンは発行されない。

f) タイムスタンプ・トークンは、要求者に指示に従ってタイムスタンプを付与されたデータの表現(ハッシュ値など) を含まなければならない。

g) タイムスタンプ・トークンには、生成された専用の鍵を使用して署名が行われなければならない。

注記 2：タイムスタンプ・トークンのプロトコルは、RFC3161 に定められ、TS 101 861 に概要が説明されている。

注記 3：ほぼ同時に複数の要求が行われる場合、TSA 時計の精度内の時間の順序付けは必須ではない。

h) 発行を行う TSA の名前は、タイムスタンプ・トークンに指定されなければならない。これには以下が含まれる。

- 該当する場合には、TSA が設置されている国の識別子
- TSA の識別子
- タイムスタンプを発行するユニットの識別子

7.3.2 UTC との時計の同期

TSA は、その時計が定められた範囲ないで UTC と同期していることを保証しなければならない。

特に以下を定める。

a) TSA の時計の較正を行い、時計が宣言された精度を維持するようにしなければならない。

b) TSA 時計は、その目盛りを超えるような気づかれない変化を時計にもたらす恐れのある脅威から保護されなければならない。

注記 1： 脅威には、不正な人物、無線、電気的ショックによる改変が含まれる。

c) TSA は、タイムスタンプ・トークンに示される時刻が UTC からずれた場合、これが検出されることを保証しなければならない (第 7.3.1 項参照)。

注記 2： 依存者は、そうしたイベントについて情報の提供を受ける必要がある (第 7.4.8 項参照)。

d) TSA は、該当する機関によって通知された通り、うるう秒が発生するとき、時計の同期が維持されることを保証しなければならない。うるう秒を考慮した変更は、うるう秒の発生が予定されている日の最後の 1 分間に行われなければならない。この変更が行われた場合、レコードは (定められた精度内で) その正確な時間を維持されなければならない。詳細については附属書 C を参照。

注記 3： うるう秒とは、UTC 月の最後の秒を省略したり、新しい秒を追加したりすることにより、UTC を調整することである。最初の初期設定は 12 月と 6 月の末、2 回目の初期設定は 3 月と 9 月に行われる。

7.4 TSA の管理および運営

7.4.1 セキュリティ管理

TSA は、適切で、認定された最善の実施方法に対応する管理手順が適用されることを保証しなければならない。

特に以下を定める

TSA 一般

a) TSA は、本タイムスタンプ・ポリシーの適用範囲内のタイムスタンプ・サービスの提供のすべての側面について、その役割が下請業者に外部委託されているかどうかにかかわらず、責任を保持しなければならない。第三者機関の責任は、TSA および、第三者機関が TSA によって要求されたあらゆる管理を実施するようにするための適切な措置によって、明確

に定められなければならない。TSA はすべての関係者の関連実施の開示について責任を保持しなければならない。

b) TSA の経営者は、TSA の情報セキュリティ・ポリシーを定める適切な高レベルの運営フォーラムを通じて情報のセキュリティに関する指示を与えなければならない。TSA は、影響を受けるすべての従業員にこのポリシーを公開し、連絡することを保証しなければならない。

c) TSA内でセキュリティを管理する必要のある情報セキュリティ・インフラストラクチャは、常にメンテナンスが行われなければならない。セキュリティのレベルに影響するあらゆる変更点が TSA 管理フォーラムの承認を受けるものとされなければならない。

注記 1：情報セキュリティ・インフラストラクチャ、管理情報セキュリティ・フォーラム、情報セキュリティ・ポリシーなどの情報セキュリティ・ポリシーに関する手引きについては ISO/IEC 17799 を参照。ほかの補助的な手引きには附属書 F に収録されている。

d) タイムスタンプ・サービスを提供する TSA 設備、システム、情報資産のセキュリティ管理と運営手順が文書化され、実施され、維持管理されなければならない。

注記 2：本仕様書 (通常はシステム・セキュリティ・ポリシーまたはマニュアルと呼ばれる) は、第 7.1.1a)項で定められたリスク調査に基づき、あらゆるターゲット、提供されるサービスに関連したオブジェクトと脅威、および、それらの脅威の効果を避ける/制限するために必要なセーフガードを定めなければならない。事件や災害に関するポリシーを定めるとともに、指定されたサービス、および関連のセキュリティ確保がどのように提供されているかについて、規則、指令、手順を説明しなければならない。

e) TSA は、TSA の機能の職務がほかの組織またはエンティティに外部委託するときに情報のセキュリティが維持されることを保証しなければならない。

7.4.2 資産分類と管理

TSA は、その情報やほかの資産が適切なレベルの保護を受けることを保証しなければならない。

特に以下を定める。

a) TSA はすべての資産の目録を維持し、リスク分析に従って保護要件の分類をそれらの資産に割り当てなければならない。

7.4.3 職員のセキュリティ

TSA は、人事および雇用が TSA の運営の信頼性を高め、支えることを保護しなければならない。

特に以下を定める (TSA 一般):

a) TSA は、提供するサービスに必要な専門知識、経験、資格を融し、職務にふさわしい職員を採用しなければならない。

注記 1: TSA の職員は、正式な研修と証明書、実地経験、あるいはその 2 つの組み合わせを通じて「専門知識、経験、資格」の要件を満足する必要がある。

注記 2：TSA により採用される職員には、TSA のタイムスタンプ・サービスを支援する職務の遂行に個人契約を結び従事する者を含む。TSA サービスの監視に従事できる職員

は、TSA の職員である必要がある。

b) TSA のセキュリティ・ポリシーに指定されたセキュリティの役割および職責は、職務記述書に記されなければならない。TSA の運営のセキュリティが依存する信頼ある役割については、明確に定められなければならない。

c) TSA の職員 (臨時雇用および常勤) は、職務記述書を職務と最低の権利の分離の観点から定義し、職務とアクセス レベル、経歴調査、従業員の研修と意識に基づき、職位に対する意識を決定するものでなければならない。該当する場合、これらは一般的役割と TSA 固有の役割の間を区別するものでなければならない。これらは、技量と経験に関する要件を含むものとする。

d) 職員は、TSA の情報セキュリティ管理手順 (第 7.4.1 項を参照) に基づく管理手順/プロセスを実行しなければならない。

注記 3：詳細は ISO/IEC 17799 を参照。

タイムスタンプ管理には以下の追加管理が適用されなければならない：

e) 以下を有する管理職員が採用されなければならない。

- タイムスタンプ技術の知識
- デジタル署名技術の知識
- TSA の時計の較正または UTC との同期のメカニズムに関する知識
- セキュリティ任務にある職員のセキュリティ手順への精通性
- 情報セキュリティおよびリスク調査の経験

f) 信頼されるべき役割のすべての TSA 職員は TSA 運営の公正性を損なう恐れのある利害の対立を免れなければならない。

g) 信頼されるべき役割には、以下の職務に関する役割が含まれる。

- セキュリティ担当者 ： セキュリティ実施を管理する総合的責任
- システム管理者 ： タイムスタンプ管理のための TSA の信頼あるシステムの導入、設定、管理を許可されている。
- システム運用者：TSA の信頼あるシステムを日常的に運用する責任を負う。システムのバックアップの回復の実行を許可されている。
- システム監査者：TSA の信頼あるシステムのアーカイブや監査ログの照会が許可されている。

h) TSA の職員は、セキュリティを担当する上級管理者によって信頼ある役割に正式に任命されなければならない。

i) TSA は、その地位への適正に影響する重大な犯罪またはその他の不法行為を行ったとして有罪判決を受けたとされる人物を信頼ある役割や管理職に任命してはならない。職員は、必要なチェックが終了するまで信頼ある職務につくことはできない。

注記 4: 一部の国では、TSA が、従業員候補者の協力なく過去の有罪判決に関する情報を入手できない。

7.4.4 物理的および環境的セキュリティ

TSA は重要なサービスの物理的アクセスが管理され、その資産への物理的リストが最小化されることを保証しなければならない。

特に以下を定める (全般) :

a) タイムスタンプの提供およびタイムスタンプの管理の両方について:

- タイムスタンプ・サービスに関連する施設への物理的アクセスは認可を受けた個人に制限しなければならない。

- 資産の損失、破損、危殆化およびビジネス活動の中断を避けるために管理が行われなければならない。

- 情報および情報処理施設の危殆化または盗難を避けるために管理が行われなければならない。

b) 第 7.2.1 項および第 7.2.2 項に定める暗号モジュールのセキュリティの要件を満足するために暗号モジュールにアクセス管理を適用されなければならない。

c) タイムスタンプ管理には以下の追加制御が適用されなければならない。

- タイムスタンプ管理施設は、システムまたはデータへの不正アクセスを通じた危殆化からサービスを物理的に保護する環境において運営されなければならない。

- 物理的保護は、タイムスタンプ管理のまわりの明確に定義されたセキュリティの境界 (物理的障壁) の作成を通じて実現されなければならない。ほかの組織と共有した建造物のあらゆる部分はこの境界の外側にあるものとする。

- 物理的および環境的セキュリティ管理は、システムリソースを収容する施設、システムリソースそのもの、およびそれらの運営を支援するために使用される施設、を保護するために実施されなければならない。タイムスタンプ管理にかかわるシステムの TSA の物理的および環境的セキュリティ・ポリシーは、最低限、物理的なアクセス管理、自然災害からの保護、火災防止、公益企業 (電力、電気通信など) のサポート、構造破綻、配管漏洩、盗難に対する保護、不法侵入、災害からの復旧に対応しなければならない。

- 許可なく敷地外に持ち出されたタイムスタンプ・サービスに関連する設備、情報、メディア、ソフトウェアを保護するために管理が実施されなければならない。

注記 1 :物理的および環境的セキュリティに関する手引きについては ISO/IEC 17799 を参照。

注記 2 : アクセスが認可された人員に制限されている場合と同じセキュアな領域内では、ほかの職務もサポートされる場合がある。

7.4.5 運用管理

TSA は、障害のリスクを最小に押さえ、TSA システムコンポーネントがセキュアであり、正式に運用されていることを保証しなければならない。

特に以下を定める (全般) :

a) TSA システムコンポーネントと情報の完全性はウイルス、悪意ある不正なソフトウェアに対して保護されなければならない。

b) 事件のレポートおよび対応手順は、セキュリティ上の事件や故障からの損害を最小にするような方法で採用されなければならない。

c) TSA の信頼あるシステム内で使用されるメディアは、損害、盗難、不正アクセス、無効化からメディアを保護するために安全な方法に処理されなければならない。

注記 1：管理責任のある各メンバーは､TSA 実施規定に定められたタイムスタンプ・ポリシーおよび関連実施の計画および有効な実施について責任を負う。

d) タイムスタンプ・サービスの提供に影響を及ぼすすべての信頼ある管理役割について、手順が確立され、実施されなければならない。

メディア処理とセキュリティ

e) すべてのメディアが情報分類方式 (第 7.4.2 項参照) の要件に従ってセキュアに処理されなければならない。機密データを含むメディアは、必要がなくなったら、セキュアに処理されなければならない。

システム計画

f) 容量要求が管理されなければならない。十分な処理パワーと保存容量が使用できることを保証するために将来の要領の要件の予想が作成された。

事故の報告と応答

g) TSA が事件に素早く対応し、セキュリティの侵犯の影響を制限するために、適宜協力しながら行動しなければならない。すべての事故は、事故後できるだけ迅速に報告されなければならない。

タイムスタンプ管理には以下の追加管理が適用されなければならない

適用手順と管理

h) TSA セキュリティ運用は、ほかの運用から区別されなければならない。

注記 2：TSA セキュリティ運用の責任には以下が含まれる。

- 運用手順と責任
- セキュアなシステム経営と承認
- 悪意あるソフトウェアからの保護
- 会社財産管理
- ネットワーク管理
- 監査帳、イベント分析、およびフォローアップの積極的監視
- メディア処理とセキュリティ
- データとソフトウェアの交換

これらの運用は、TSA の信頼ある人員によって管理されなければならないが、適切なセキュリティ・ポリシー、役割、責任に関する文書に定義される通り、専門家、運用要員 (監督のもとで)

によって実際に実行可能である。

7.4.6 システム・アクセス管理

TSA は、TSA システムのアクセスが正しく認可された個人に限定されることを保守しなければならない。

特に以下を定める (全般) :

a) 加入者と第三者機関からのアクセスを含め、不正アクセスから TSA の内部ネットワークドメインを保護するために管理 (ファイアウォールなど) が実施されなければならない。

注記 1 : ファイアウォールは、また、TSA の運営に必要とされないすべてのプロトコルとアクセスを妨げるためにも設定する必要がある。

b) TSA は、ユーザーのアカウント管理、監査と適時変更、またはアクセス除去を含む、システムセキュリティをいじするためのユーザー (この場合、運用者、管理者、監査者) の効果的管理を確保しなければならない。

c) TSA は、情報およびアプリケーションシステム機能へのアクセスがアクセスコントロールポリシーに基づいて制限されていることや、TSA システムがシステム管理者と運営機能の分離など TSA の実施に定められた信頼ある役割の分離に対して十分なコンピュータセキュリティ管理を行うことを保証しなければならない。特にシステム・ユーティリティ・プログラムの使用が制限され、厳しく管理される。

d) TSA の人員は、タイムスタンプに関連した重要なアプリケーションを賞する前に正しく指定され、認証さえも指定されなければならない。

e) TSA の人員は、イベント・ログの保持 (第 7.4.10 項参照) など、その活動について報告義務がある。

タイムスタンプ管理には以下の追加管理が適用されなければならない。

f) TSA はローカル ネットワーク コンポーネント (ルーターなど) が物理的にセキュアな環境に保管されること、また、それらの設定は、TSA の定める用件に従って定期的に監査されることを保証しなければならない。

g) TSA が、システムのリソースへアクセスしようとする不正および/または変則的な試行を適宜、検出、登録、対応できるようにするため、連続的な監視とアラーム設備が用意されなければならない。

注記 2 : これは、例えば、進入検出システム、アクセス管理監視、およびアラーム設備を使用できる。

7.4.7 信頼あるシステムの導入とメンテナンス

TSA は、変更から保護されている信頼あるシステムおよび製品を使用しなければならない。

注記 : TSA サービスで実行されるリスク解析は、(第 7.1.1 項参照) は、信頼あるシステムを必要とするその重要なサービスと必要な保証レベルを特定する必要がある。

特に以下を定める :

a) セキュリティ要件の分析は、セキュリティが IT システムに組み込まれていることを保証するために TSA によって、または TSA に代わって実行されるシステム開発プロジェクトの設計および要件決定段階において行われなければならない。

b) 変更管理手順は、あらゆる運用ソフトウェアのリリース、変更、緊急のソフトウェア修正に適用されなければならない。

7.4.8 TSA サービスの危殆化

TSA は、TSA 秘密鍵の危殆化や未較正の検出を含めた、TSA サービスのセキュリティに影響するイベントにおいて、加入者と依存者が関連情報を入手できることを保証しなければならない。

特に以下を定める。

a) TSA の災害復旧計画は、それまで発行されたタイムスタンプ・トークンに影響を及ぼしてきた可能性のある、TSA の秘密鍵の危殆化またはその恐れ、あるいは TSA 時計の未較正に対応しVなければならない。

b) 危殆化またはその恐れ、あるいは未較正の場合、TSA はすべての加入者および依存者が発生した　危殆化の説明を参照できるようにしなければならない

c) TSA の運営に対する危殆化 (TSA 鍵の危殆化など)、危殆化の恐れ、あるいは未較正の場合、危殆化から回復する手順が遂行されるまで、タイムスタンプ・トークンを発行してはならない。

d) TSA の運営の大きな危殆化、または未較正において、可能であれば、TSA は、すべての加入者および依存者に対して、TSA ユーザーのプライバシー、または TSA サービスのセキュリティを侵害しない限りにおいて、影響のあったタイムスタンプ・トークンを特定するために使用された恐れのある情報を入手可能にしなければならない。

注記 : 秘密鍵が危殆化されていない場合、TSA によって生成されらすべてのトークンの監査証跡は、過去の本物と偽者のトークンを区別する手段となる場合がある。2 つの異なる TSA からの 2 つのタイムスタンプ・トークンは、この問題に対するもうひとつの方法となる可能性がある。

7.4.9 TSA の閉鎖

TSA は、加入者および依存者の混乱が TSA のタイムスタンプ・サービスの中止の結果最小化されること、特にタイムスタンプ・トークンの正しさの検証に必要な情報の連続的なメンテナンスを保証しなければならない。

特に以下を定める。

a) TSA がそのタイムスタンプ・サービスを終了する前に以下の手順を最低限実行しなければならない。

- TSA がすべての加入者および依存者に対してその終了に関する情報を提供しなければならない。

- TSA は、タイムスタンプ・トークンの発行処理に関連するあらゆる業務の遂行を TSA に代わって行うすべての下請け業者に認可を終了しなければならない。
- TSA は、適切な期間に TSA の正しい運用を示すためにひつ追うなイベント ログおよび監査アーカイブ (第 7.4.10) のメンテナンスについて義務を信頼できる第三者機関に委譲しなければならない。
- TSA は、その公開鍵や証明書を依存者に適切な期間にわたって提供するためにその義務を維持するか、または信頼できる機関に委譲しなければならない。
- バックアップ コピーを含む TSA 秘密鍵は、秘密鍵を取得できないような方法で破壊されなければならない。

b) TSA が破産したり、その他の理由でその費用を自身で払えなくなった場合、最低限の要件を満足するための費用をまかなう措置を持たなければならない。

c) TSA は、サービス終了の条項をその実施規定において定めなければならない。これには以下が含まれる。
- 該当するエンティティの通知
- TSA の義務のほかの関係者への委譲

d) TSA はその証明書を失効するステップを実行しなければならない。

7.4.10 法的要件の順守

TSA は必ず法的要件を順守しなければならない。

特に以下を定める。

a) TSA は、欧州データ保護指令 [3] の要件が、国内法による場合と同様に満足されることを保証しなければならない。

b) 個人データの無許可または違法な処理、および個人データの偶発損失や破壊、あるいは損傷に対して、適切な専門的および組織的措置が講じられなければならない。

c) 利用者から TSA に提供された情報は、利用者の同意または裁判所の命令あるいはその他の法的必要性がない限り、開示は全く行われないものとされなければならない。

7.4.11 タイムスタンプ・サービスの運営に関する情報の記録

TSA は、タイムスタンプ・サービスの運営に関するすべての関連情報が、特に法的手順で証拠を提出する目的で指定期間に記録されることを保証しなければならない。

特に以下を定める。

全般

a) ログを記録すべき特定のイベントおよびデータが TSA によって文書化されなければならない。

b) タイムスタンプ・サービスの運営に関する現在の記録およびアーカイブされたレコードについて、機密性と完全性が維持されなければならない。

c) タイムスタンプ・サービスの運営に関するレコードは、開示された業務実施に基づき、完全な機密保持された形でアーカイブされなければならない。

d) タイムスタンプ・サービスの運営に関するレコードは、法的手順でタイムスタンプ・サービスを適正に運営している証拠を提供する目的で必要な場合には利用できるようにしなければならない。

e) TSA の環境、鍵の管理、時計の同期の各重要イベントの正確な時刻は記録されなければならない。

f) タイムスタンプ・サービスに関する記録は、必要な法的証拠の提供に当たる場合、TSA 開示規定において通知される通り (第 7.1.2 項参照) TSA の署名鍵の有効期間終了後もある期間だけ保持されなければならない。

g) イベントは、保持が必要な期間内に (長期保存可能なメディアに確実に転送される場合を除き) 簡単に削除されたり、破壊されたりできない方法でログを記録されなければならな

い。

注記 : これは、例えば、書込み専用のメディアの使用、使用される各リムーバブル・メディアのレコード、およびオフサイト・バックアップの使用を通じて、可能になる。

h) 加入者に関して記録されたあらゆる情報は、その公開に関して加入者から同意が得られる場合を除き、機密が保持されなければならない。

TSA の鍵の管理

i) TSA の鍵のライフサイクルに関連したすべてのイベントに関するレコードのログが記録されなければならない。

j) TSA の証明書 (該当する場合) のライフ・サイクルに関連したすべてのイベントに関するレコードのログが記録されなければならない。

時計の同期

k) TSA の時計の UTC への同期に関連したすべてのイベントに関するレコードのログが記録されなければならない。この中には、タイムスタンプで使用される時計の通常の再較正または同期に関する情報を含まれなければならない。

l) 非同期の検出に関連したすべてのイベントに関するレコードのログが記録されなければならない。

7.5 組織について

TSA はその組織が信頼できることを保証しなければならない。

特に以下を定める。

a) TSA の運営について定めるポリシーおよび手順では差別を行ってはならない。

b) TSA は、その活動が運営の明示された範囲内に収まり、TSA 開示規定に定められた義務を順守することに同意する申請者すべてがそのサービスを利用できるようにしなければならない。

c) TSA は、国内法の定める法的エンティティである。

d) TSA は、提供しているタイムスタンプ・サービスに適したクオリティおよび情報セキュリティ管理のための 1 つまたは複数のシステムを有する。

e) TSA はその運営および/または活動から発生す賠償責任に対応する十分な措置を用意する。

f) TSA は、本ポリシーを巡視して運営するのに必要な財務的安定性とリソースを有する。

注記 1 : この中には第 7.4.9 に定められる TSA 解約の要件が含まれる。

g) TSA は、タイムスタンプ・サービスの提供に必要な仕事のタイプ、範囲、量に関連して必要な教育、研修、技術知識、経験のある十分な数の人員を採用する。

注記 2 : TSA によって採用される人員には、TSA のタイムスタンプ・サービスを支援する機能に個人契約を結んで携わる者が含まれる。TSA サービスの監視にのみ従事する人員は、TSA の職員 (社員) である必要はない。

h) TSA は、顧客やほかの関係者から寄せられた、タイムスタンプ・サービスの提供やほかの問題に関する苦情や訴えを解決するための方針や手順を用意している。

i) TSA は、サービス提供が下請け、外部委託、その他第三者機関を必要とする場合には、適切な契約文書を取り交わす。

附属書 A (参考):

タイムスタンプ・サービスの提供における潜在的賠償責任

賠償責任は、契約または法律 (国内法) のいずれか 1 つに基づき発生する。

消費者が関係する場合、法的な保護、特に保護のレベルを引き上げる可能性のある不正契約条項指令 (93/13/EEC) および該当する国家的実施が適用される。

これらの規則は、TSA による賠償責任の制限に制約を加える場合がある。なぜなら、不正契約条項指令は、個別交渉を行うことなく、当事者間の権利や消費者の損害への義務に重大な不均衡をもたらす恐れのある取り決めを禁止しているためである。

国内法はまた、賠償責任の制限に対して制約を追加する行うこともでできる。

これらの例外に該当しない場合、TSA は、あらゆる保証責任を放棄し、その賠償責任を制限することができる。

附属書 B (参考) :

モデル TSA 開示規定

B.1 概要

提案された TSA 開示規定は、開示および通知の補助的手段としてタイムスタンプ・トークンを発行する TSA によって使用されるよう意図されている。TSA 開示規定は、TSA が法的な要件および懸念、特に消費者向け提供に関連したものに対応するのを支援できる。さらに、モデル TSA 開示規定の目的は、業界の "自主規定" を守り、セキュリティ・ポリシーの要素についてのコンセンサス、および/または強調および開示を必要とする実施規定を策定することである。

セキュリティ・ポリシーと実施規定の各文書は、タイムスタンプ・ポリシーとその実施の説明と管理にとって不可欠だが、多くの TSA 利用者、特に消費者にとってこれらの文書の理解が難しい場合がある。TSA 利用者の情報に基づき信頼性の高い決定を支援できる補助的で単純化された手段が必要とされる。また TSA 開示文書は、セキュリティ・ポリシーや実施規定の代わりになることを目的としていない。

この附属書は、TSA 開示規定の構成例を示し、展開されたタイムスタンプ・サービスに含まれる調和の取れた規定タイプ (カテゴリ) について説明する。

B.2 TSA 開示規定の構成

TSA 開示規定は、各海事規定タイプの項目を含む。TSA 開示説明書の各セクションには、説明文書が含まれ、その中に関連する証明書ポリシー/認証実施規定の項目へのハイパーリンクが含まれる場合がある。

規定のタイプ	規定の説明	具体的要件
契約全体	開示規定が契約のすべてではなく、一部にすぎないことを示す規定	
TSA 連絡先情報	TSA の名称、所在地、関連連絡先情報	
タイムスタンプ・トークンのタイプと使用法	TSA によって（タイムスタンプ・ポリシーに従って）発行されたタイムスタンプ・トークンの各クラス/タイプの説明	適用されるポリシーの表示。タイムスタンプ・トークンが使用されるコンテキスト、ハッシュ・アルゴリズム、タイムスタンプ・トークンの予想寿命、タイムスタンプ・トークンの使用に関するあらゆる制限事項、タイムスタンプ・トークンの検証方法に関する情報を含む。
信頼限界	信頼限界(ある場合)	タイムスタンプ・トークンの時刻の精度、および、TSA イベント・ログ（第 7.4.10 節参照）が保持される（証拠提供に利用できる）期間を示す。
加入者の義務	重要な加入者の義務の説明または参照	本仕様書には特定の要件は定められていない。場合によって TSA が追加の義務を指定することが可能。
依存者の TSA 公開鍵ステータスのチェック義務	依存者が TSA 公開鍵のステータスと、詳細説明の参照のチェックを義務付けられている程度。	依存者がタイムスタンプ・トークンに "正当に依存" していると見なされるために TSA 公開鍵ステータスを検証する方法についての情報（第 6.3 項参照)。TSA 公開鍵の失効ステータスのチェック要件を含む。
制限された保証責任、賠償責任の否認/制限	保証責任、免責、賠償責任の制限、およびあらゆる保証または保険プログラムの概要	損害賠償の制限（第 6.4 項参照)
適用可能な契約および実施規定	適用可能な契約、実施規定、タイムスタンプ・ポリシー、その他の関連文書の特定と参照	
プライバシー・ポリシー	適用可能なプライバシー・ポリシーの説明と参照	注記 ： このポリシーのもとで TSA は、「データ保護法」に従う必要がある。
返金ポリシー	適用可能な返金ポリシーの説明と参照	
適用可能な法律、苦情・紛争解決方法	法律選択、苦情処理手順、紛争解決メカニズムに関する規定	苦情および紛争解決の手順、適用可能な法体系
TSA およびレポジトリ・ライセンス、信頼マーク、監査	あらゆる政府ライセンス、シール・プログラム、監査プロセス、および該当する場合は監査会社	TSA が指定のタイムスタンプ ポリシーに準拠していると評価されているかどうか、また、評価した独立団体。

附属書 C （参考）

協定世界標準時

協定世界標準時 (UTC) は 1972 年 1 月 1 日から実施されている国際的時間標準である。UTC はグリニッジ標準時に代わって使われるようになったが、実際には両者の誤差は 1 秒以内である。したがって、多くの人々は UTC を採用後も実際には GMT を採用していた。

UTC ゼロ (0) 時間は、基準子午線にあるイギリス・グリニッジの深夜 0 時である。世界時は 24 時間時計に基づき、従って、UTC の午後 4 時など午後の時間は 16:00 UTC (16 時 0 分) と表される。

国際原子時 (TAI) は国際度量衡局 (BIPM) により、世界 30 カ国以上の気象台や観測所にある 200 以上の原子時計を読み込んで計算される。TAI に関する情報は毎月 BIPM 発行の「BIPM Circular T」で入手できる (ftp://62.161.69.5/pub/tai/publication)。TAI は、仮想的な完全な時計に対して年間ミリ秒 (0.0000001 秒) の 10 分の 1 しか誤差しかない。

協定世界時 (UTC) は、国際電気通信連合無線通信部門 (ITU-R) によって制定・推奨される、秒を基準にした時間スケールである。国際度量衡局 (BIPM) により管理される。BIPM による管理には世界中のさまざまな国家的研究所の協力が必要である。UTC の全体の定義は、ITU-R Recommendation TF. 460-4 に記されている。

原子時が単位としている国際単位 (SI) の 1 秒は、セシウム 133 の基底状態の 2 つの超微細準位の間の遷移に対応する放射の 9,192,631,770 周期の継続時間として定義される。TAI は、多数の原子時計に基づく統計的時間スケールである国際原子時のスケールである。

世界時 (UT) は、深夜 0 時からカウントされ、平均太陽日を単位とし、地球の回転が変動しても、可能な限り一様に定義されるものとする。

- UTO は、観察される特定の場所の回転時間である。それは、星の日周運動や地球外無線源として観測される。
- UT1 は観測サイトの緯度における極運動の効果によって UT0 を修正することによって計算される。これにより、地球の自転の不規則性により一様性が変化する。

UT1 は地球のわずかに不規則な回転をベースにしている。回転の不規則性は通常、地球の平均的回転速度の減少をもたらし、UTC に対して UT1 が遅れる。
世界標準時 (UTC) は、国際的計時の基礎であり、2001 年の統合秒数 32 を除き、TAI に正確に従うものとする。このうるう秒は国際地球回転サービス (IERS) (http://hpiers.obspm.fr/) の勧告に従い、不規則性を考慮して、太陽がグリニッジの子午線において 12:00:00 UTC からのずれが 0.9 秒以内であることを保証する。UTC は、時間単位が平均太陽日だった時代に使用されたグリニッジ標準時 (GMT) を引き継ぐ最も新しい標準時である。

原子による時間スケールすなわち UTC の調整では、うるう秒と呼ばれるちょうど 1 秒間の追加または削除が行われる。年 2 回、つまり、6 月 30 日および 12 月 31 日の最終分の調整により、UTC と UT1 の間の累積した差違が、次に予定された調整まで 0.9 秒を超えないようにする。歴史的に見ると、調整は通常、必要に応じて、UTC 時間スケールに秒数を加えて、地球の回転が "追いつく" ようにする。したがって、調整が行われる日の UTC 時間スケールの最終分は、61 秒になる。

したがって協定世界時 (UTC) は、整数秒だけ TAI と異なる。

UTC は、UTC に 1 秒きざみの "うるう秒" を導入することにより、UT1 の 0.9 秒以内に保たれる。これまでうるう秒は正であった。

附属書 D (参考)：

タイムスタンプ・トークンの長期的検証

通常、タイムスタンプ・トークンは TSA の証明書の有効期限終了後は検証できなくなる。なぜなら、証明書を発行した CA が、鍵の危殆化による失効に関するデータなど、失効データの公開を保証しないためである。しかしながら、タイムスタンプ・トークンの検証は、検証時に以下を知ることが可能であれば、TSA の証明書の有効期間終了後も実行される場合がある。

- TSA 秘密鍵がタイムスタンプ・トークンの検証を行うときまでに危殆化されていない。
- タイムスタンプ・トークンに使用されるハッシュ・アルゴリズムが検証時に衝突を示していない。
- タイムスタンプ・トークンの署名に使用された署名アルゴリズムと署名鍵のサイズが依然として、検定時の暗号攻撃の範囲を超えている。

これらの条件を満足できない場合、追加のタイムスタンプを適用して以前のタイムスタンプを保護することによって維持できる。条件が満足された場合には、タイムスタンプデータがセキュアな保管場所に保管される。

本仕様書は、そうした保護を確保する方法については指定しない。当分の間、いくつかの拡張が定義され、これらの機能をサポートするまで、閉じた環境の中で情報が取得されるものとする。例えば、CA が有効期間終了後も TSA の失効ステータスを維持することを保証するならば、これは最初の要件を満足する。

注記 1：イムスタンプに代わる手法は、信頼あるサービス・プロバイダが監査証跡の特定字のデータの表現を記録し、これにより、データがその時刻以前に存在していたという証拠を示すことである。タイムマーキングとよばれるこの手法は、署名の長期的有効性をチェックする有効な方法となる。

注記 2：SA またはほかの信頼ある第三者サービス・プロバイダは、タイムスタンプ・トークンの検証をサポートすることができる。

附属書 E (参考) :

実装アーキテクチャ - タイムスタンプ・サービス

E.1 管理されたタイムスタンプ・サービス

一部の機関は、1 つまたは複数のタイムスタンプ局のホスティングを行い、これらのタイムスタンプ局の設置、運営、管理の責任を負うことなく、タイムスタンプ・サービスの近傍性とクオリティを利用することができる。

これは、ホスティング機関から構内に設置されたユニットを使用して実現でき、ホスティング機関に提供されるサービスの全般的責任を負うタイムスタンプ・サービスによってリモートで管理される。

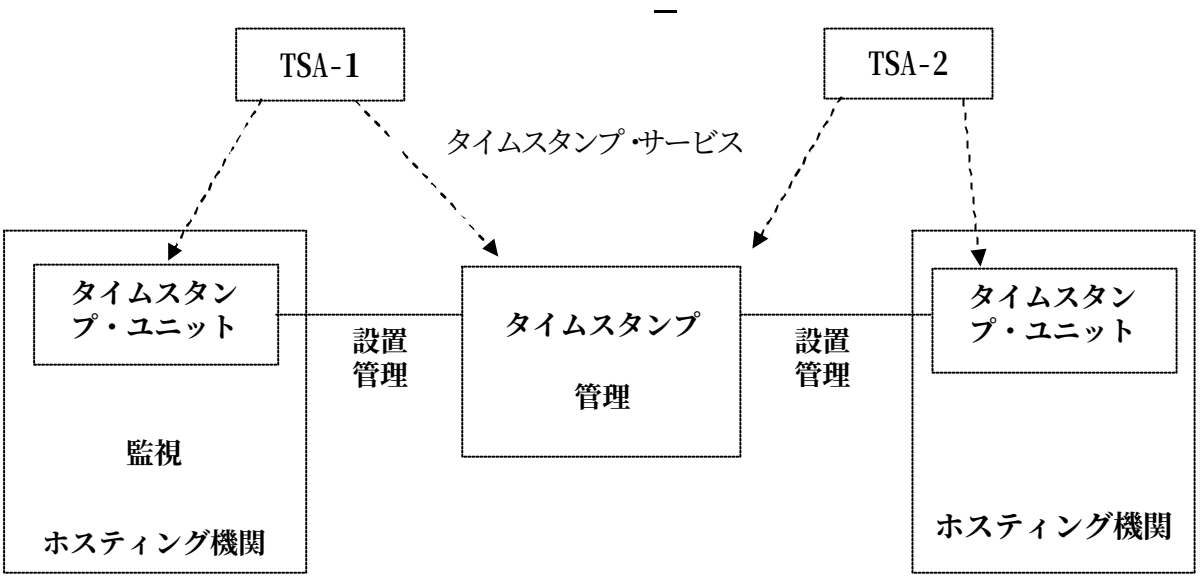

図 E.1 : 管理されたタイムスタンプ・サービス

本仕様書に説明されたタイムスタンプ・サービスの要件には、タイムスタンプの管理とタイムスタンプ・サービスを発行するユニットの運用に関する両方の要件が含まれる。タイムスタンプ・トークンに指定される通り、TSA はこれらの要件が (契約上の義務等を通じて) 満足されることを保証する責任を負う。

ホスティング機関は通常、サービスの使用を監視し、少なくとも、サービスが稼動中か否かを知ることができ、また、ある期間中に生成されるタイムスタンプの数などのサービスのパフォーマンスを計測できることを希望する。そうした監視は、TSA のタイムスタンプ・サービスの範囲外であると見なすことも可能である。

したがって、本仕様書本体における管理運用の記述は限定的ではない。運用の監視は、直接ユニットについて遂行される場合には、タイムスタンプ・サービス・プロバイダによって許可される。

E.2 選択的代替クオリティ

一部の依存者は、特定の署名アルゴリズムおよび/または鍵の長さ、あるいはタイムスタンプ・トークンに保持される時間の正確さなど、タイムスタンプ・トークンの特定の特性を利用することができる。これらのパラメータは、タイムスタンプ・トークンの "クオリティ" を指定するとみなされる。

さまざまなクオリティのタイムスタンプ・トークンは、同じまたは異なる TSA によって運用されるさまざまなタイムスタンプ・ユニットによって発行することができる。

特定のタイムススタンプ・ユニットは、アルゴリズムと鍵の長さのみを提供する (タイムスタンプ・ユニットは、ユニットとして管理されるハードウェアおよびソフトウェアの装置であり、単一のタイムスタンプ・トークン署名鍵を持つため)。アルゴリズムと鍵の長さのさまざまな組み合わせを取得するには、様々なタイムスタンプ・ユニットが使用されるものとする。特定のタイムスタンプ・ユニットはタイムスタンプ・トークンに保管された時間だけ、一定の正確さを実現し、もし、特定のアクセスモード (電子メール、http など) や要求の特定のパラメータを使用することによって指示された場合には異なる精度を実現するものとする。

附属書 F (参考):

参考文献

消費者契約中の不正条項に関する 1993 **年** 4 **月** 5 **日欧州理事会指令** 93/13/EEC

遠隔契約における消費者保護に関する欧州議会および 1997 **年** 5 **月** 20 **日欧州議会指令** 1997/7/ec - **欧州理事会および欧州議会による規定** re **第** 6 **条**(1) - **欧州委員会による規定** re **第** 3 (1)**、第** 1 **インデント**
電子署名の共同体枠組みに関する欧州議会および 1999 **年** 12 **月** 13 **日欧州理事会指令** 1999/93/EC

RFC3161 (2001) Internet X. 509 : "Public Key Infrastructure: Time-Stamp Protocol (TSP)**公開鍵インフラストラクチャ : タイムスタンプ・プロトコル** (TSP)"

Algorithms and parameters for Secure Electronic Signatures" (to be published by the Algorithms group (ALGO) working under the umbrella of EESSI-SG (European Electronic Signature Standardization Initiative Steering Group)

"**セキュアな電子署名のアルゴリズムとパラメータ**" (EESSI-SG (**欧州電子署名標準化構想運営グループの下で活動するアルゴリズムグループ** (ALGO) **が刊行**)

ISO/IEC 14516: "**情報技術 - セキュリティ手法 - 信頼ある第三者サービスの利用と管理の手引き**)"

ISO/IEC TR 13335-2 (1997): "Information technology - Guidelines for the management of IT Security - Part 2: Managing and planning IT Security (**情報技術** - IT **セキュリティ管理の手引き - 第** 1 **部** : IT **セキュリティの概念とモデル**"

ISO/IEC TR 13335-2 (1997): "Information technology - Guidelines for the management of IT Security - Part 2: Managing and planning IT Security (**情報技術** - IT **セキュリティ管理の手引き - 第** 2 **部** : IT **セキュリティの管理と計画**)"

ISO/IEC TR 13335-3 (1998): "Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security (**情報技術** - IT **セキュリティ管理の手引き - 第** 3 **部** : IT **セキュリティ管理の手法**)".

ISO/IEC TR 13335-4 (2000): "Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards (**情報技術** - IT **セキュリティ管理の手引き - 第** 4 **部**): **セーフガードの選択**"

ITU-R Recommendation TF.460-4: "Standard-frequency and time-signal emissions (**標準周波数と時刻信号の発信**)"

ETSI TS 101 733: "Electronic signature formats (**電子署名フォーマット**)"

ETSI TS 101 861 : "Time stamping profile (**タイムスタンプ・プロファイル**)"

ISO/IEC 17799: "Information technology - Code of practice for information security management(**情報技術 - 情報セキュリティ管理の作業標準**)"

履歴

文書の履歴		
V1.1.1	2002 年 4 月	発行

メンバーリスト

事務局

川松　和成　電子商取引推進協議会　主席研究員
松山　博美　電子商取引推進協議会　主席研究員
前田　陽二　電子商取引推進協議会　主席研究員

顧問

松本　　勉　横浜国立大学大学院
平田　健治　大阪大学大学院

リーダー

木村　道弘　日本電気株式会社
宮崎　一哉　三菱電機株式会社
櫻井　徹　　株式会社 NTT データ

TF5 **メンバー（編集メンバー）**

氏名	会社名
鈴木　邦康	株式会社ＮＴＴデータ
磐城　洋介	ＮＴＴコムウェア株式会社
野村　　進	ＮＴＴコミュニケーションズ株式会社
鈴木　優一	エントラストジャパン株式会社
上畑　正和	セイコーインスツルメンツ株式会社
雨宮　隆征	セイコーインスツルメンツ株式会社
秋山　将	日本電信電話株式会社
島　成佳	日本電気株式会社
近藤　弓末	ソニー株式会社

SWG3 メンバー（参加メンバー）

氏名	会社名
河田　悦生	株式会社エヌ・ティ・ティ・ドコモ
関野　公彦 ＊	株式会社エヌ・ティ・ティ・ドコモ
風間　博之	株式会社ＮＴＴデータ
宍倉　勝仁	シャチハタ株式会社
岩崎　善徳 ＊	セイコーインスツルメンツ株式会社
藤川　真樹	綜合警備保障株式会社
星野　　理	株式会社帝国データバンク
藤岡　直美	日本アビオニクス株式会社
小暮　貢次郎	日本信販株式会社
野口　雄治	日本認証サービス株式会社
浅野　昌和	日本ボルチモアテクノロジー株式会社
松永　和男	株式会社日立製作所
永倉　　俊	富士通株式会社
小谷　誠剛	富士通株式会社
西谷　研次	株式会社 UFJ 銀行

（注）＊はオブザーバー

平成 14 年度
ＥＣ技術基盤の相互運用性に関する調査研究事業
（電子署名生成・検証システムのセキュリティ環境の
国際標準化等の調査）
タイムスタンプサービス調査報告書
平成 15 年３月発行

発行所　財団法人　日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園３丁目５番８号
機械振興会館３階
TEL：03(3436)7500
印刷所　新高速印刷株式会社
東京都港区新橋 5-8-4
TEL：03(3437)6365

この資料は再生紙を使用しています。