

タイムスタンプに関する実証実験 報告書

平成18年5月

タイムビジネス推進協議会



目 次

1. 実証実験の目的と活動概要.....	1
1. 1 背景と目的.....	1
1. 2 検討メンバー（実証実験分科会メンバー）.....	2
1. 3 実証実験分科会検討体制.....	3
1. 4 分科会の開催.....	4
1. 5 分科会の活動概要.....	4
1. 5. 1 アプリケーションWG.....	4
1. 5. 2 長期保証WG.....	5
2. 実証実験の全体概要.....	6
3. アプリケーションWGの活動報告.....	8
3. 1 電子契約実証実験.....	8
3. 1. 1 背景.....	8
3. 1. 2 目的.....	8
3. 1. 3 概要.....	8
3. 1. 4 評価項目.....	9
3. 1. 5 成果.....	10
3. 1. 6 今後の課題.....	11
3. 2 ログサーバ実証実験.....	12
3. 2. 1 背景.....	12
3. 2. 2 目的.....	12
3. 2. 3 概要.....	13
3. 2. 4 評価項目.....	13
3. 2. 5 成果.....	14
3. 2. 6 今後の課題.....	15
4. 長期保証WGの活動報告.....	16
4. 1 文書管理システム実証実験.....	16
4. 1. 1 背景.....	16

4. 1. 2	目的.....	16
4. 1. 3	概要.....	16
4. 1. 4	評価項目.....	17
4. 1. 5	成果.....	18
4. 1. 6	今後の課題.....	19
4. 2	VAによる長期保証実証実験.....	20
4. 2. 1	背景.....	20
4. 2. 2	目的.....	20
4. 2. 3	概要.....	20
4. 2. 4	評価項目.....	21
4. 2. 5	成果.....	22
4. 2. 6	今後の課題.....	23
5.	うるう秒とコンピュータクロック.....	20

おわりに

【関連資料】

- ・タイムビジネス推進協議会 技術部会・実証実験分科会 アプリケーションWG・
長期保存WG実験報告
- ・うるう秒調整時における NTP とシステム時計の動作について

1. 実証実験の目的と活動概要

実証実験分科会では、平成 15 年度に具体的な実験課題選定を行い、平成 15 年度末から 16 年度にかけ、3つのワーキンググループ（時刻供給WG、知財WG、大阪WG）を中心に実証実験を進め、その結果のとりまとめ、ならびに報告を行った。

平成 17 年度は、新たにタイムスタンプ・プラットフォームを用いた実証実験を通じて各機能に関する検証を行うアプリケーション WG とタイムスタンプの効力を長期に保証する方策に関する検証を行う長期保証 WG を新設し実証実験のテーマとし取り組んだ。

本報告書では、これまでに行われてきた実証実験課題それぞれについて、目的、概要、ならびに、実験を通じて明らかになってきた問題点などについて述べる。

1. 1 背景と目的

パーソナルコンピュータ、高機能な携帯電話、情報家電製品などの普及に伴い、情報のやり取り、情報の保存の手段は、そのほとんどがデジタル化されつつある。その中で、契約書、申請書、医療カルテなど、まだ紙媒体が主役を担っている分野がある。この分野でデジタル化が進まないのは、古くから使われている紙媒体の証拠能力に対する安心感に比べ、容易にコピーできるデジタル情報への不安感が根強い、というのが一因と考えられる。実際、紙媒体であれば、書かれている内容以外に、筆跡、インクの種類、印影などから識別情報が得られ、さらには、インクの酸化の度合いから、書類の作成された、おおまかな時期までも推定することができるという。

一方、デジタル情報では、保存されている情報そのものしか頼れるものはない。こうしたことから、重要な情報を安心してデジタル化するためには、改ざん防止、原本性保障など、情報を強固に守る技術が必要となる。ここで、重要な役割を果たすと考えられているのが「時刻情報」である。電子署名技術によれば、第三者による情報の改ざんを防ぐことができるが、署名者本人が新たに作成したものとすり替えた場合、必ずしもこれを見破ることができない。このような本人、または当事者同士の結託による情報改ざんを防ぎ、また、ある時点でその情報が存在していたことを長期にわたって証明するには、十分な証拠能力を持つ「時刻情報」が不可欠なものとなる。

このような、「時刻情報」を活用し、安全・安心を補強する確固たる基盤を確保するためには、幅広い技術を連携させ、それらを高い信頼性で正しく機能させ、かつ、ビジネスとして成立させていく必要がある。

必要となる個別の技術は、各所で研究され、すでに実用化されているものも多いが、これらを集約し、時刻認証基盤として機能させていくには、実際にシステムを構築し、実際に近いアプリケーションに対して適用するなどの実証実験が必要になる部分も多い。

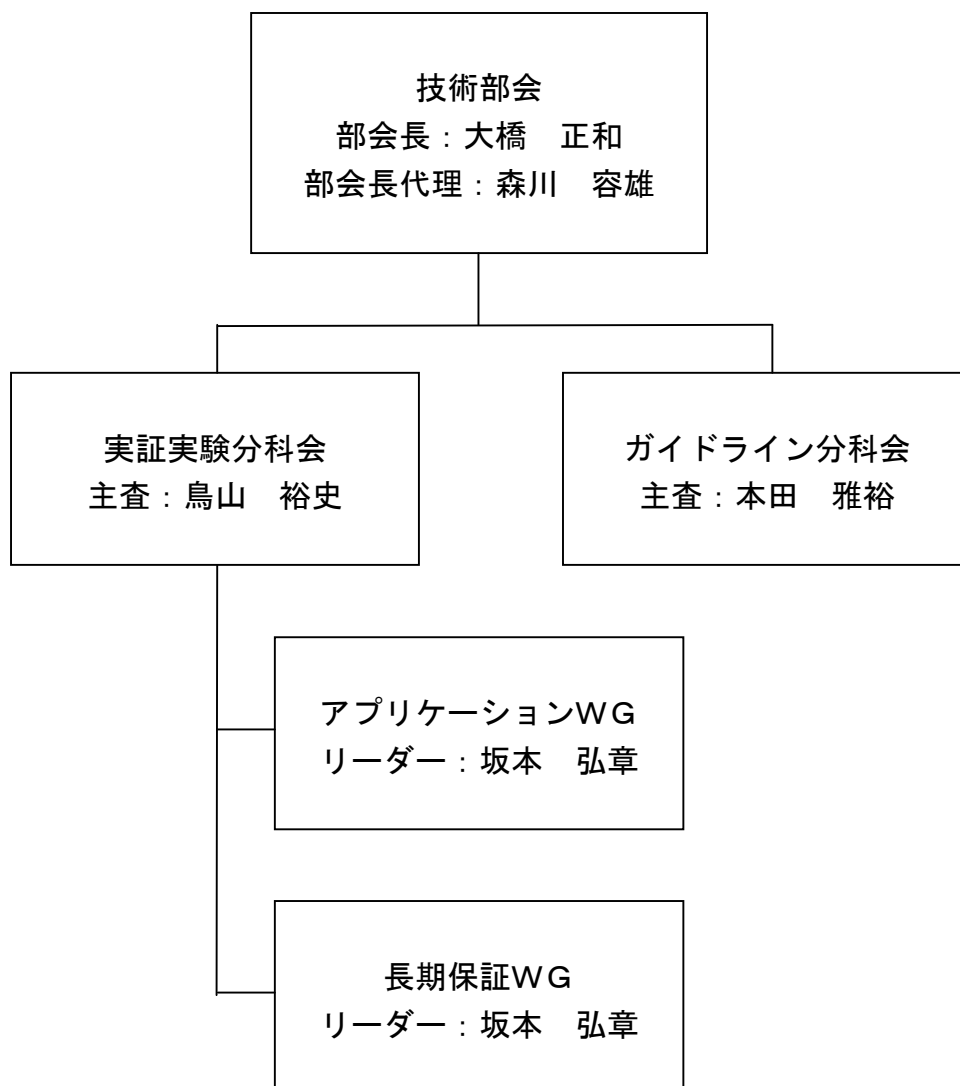
実証実験分科会では、このような実証実験を通じ、実サービスの開始前に技術的な問題、実運用上の問題などを洗い出し、新たな応用分野についても、可能性の検証を行う。すでに、実サービスが開始されているものも含め、安全性強化等のための新しい技術や、その安全評価方法についての実証を進める。また、これらの過程で指摘される問題点をガイドライン制定作業にフィードバックし、実際に動作するシステムを広報活動に利用し、広く一般の方々にタイムビジネスの理解を深めて頂くことも、実証実験の目的の一部である。

1. 2 検討メンバー（実証実験分科会メンバー）

（順不同・敬称略）

分科会主査		独立行政法人情報通信研究機構	鳥山 裕史
アプリケーション WG			
"	リーダー	株式会社 NTT データ	坂本 弘章
"	メンバー	独立行政法人情報通信研究機構	岩間 司
"	メンバー	株式会社 NTT データ	橋川 善之
"	メンバー	セイコーインスツル株式会社	上畑 正和
"	メンバー	日立製作所株式会社	田川 豊
"	メンバー	日立製作所株式会社	谷川 嘉伸
"	メンバー	日本電気株式会社	久保寺範和
"	メンバー	大成建設株式会社	鼠入 俊之
長期保証 WG			
"	リーダー	株式会社 NTT データ	坂本 弘章
"	メンバー	独立行政法人情報通信研究機構	岩間 司
"	メンバー	株式会社 NTT データ	橋川 善之
"	メンバー	セイコーインスツル株式会社	上畑 正和
"	メンバー	日立製作所株式会社	田川 豊
"	メンバー	日立製作所株式会社	谷川 嘉伸
"	メンバー	富士ゼロックス株式会社	小島 俊一
"	メンバー	富士ゼロックス株式会社	吉岡 直蔵

1. 3 実証実験分科会検討体制



1. 4 分科会の開催

1 回分科会 日時：平成 17 年 9 月 2 日（金）15:00～17:00

場所：(財) テレコム先端技術研究支援センター 7 階会議室

- 平成 17 年度分科会の活動について

新規実証実験の提案としてタイムスタンプ・プラットフォームを用いた実証実験を通じて各機能に関する検証を行うアプリケーション WG とタイムスタンプの効力を長期に保証する方策に関する検証を行う長期保証 WG により実証実験を推進することとなった。

第 2 回分科会 日時：平成 17 年 11 月 17 日（木）15:00～17:00

場所：(財) テレコム先端技術研究支援センター 別館 3 階会議室

- 実証実験成果報告について

アプリケーション WG、長期保証 WG より実証実験の中間報告が行われた。

第 3 回分科会 日時：平成 18 年 3 月 16 日（木）14:00～17:00

場所：N I C T 2 号館 1 F 会議室

- 実証実験成果報告について

アプリケーション WG、長期保証 WG より実証実験の最終報告が行われた。

その後、実証実験で使用した N T A、C A、V A 設備の見学、新日本標準時システムの見学をした。

1. 5 分科会の活動概要

今期の分科会では、2つのテーマを設定しアプリケーションWG、長期保証WGにより実証実験を行った。各WGの詳しい活動報告は後にまとめているが以下に各WGの実験概要を述べる。

1. 5. 1 アプリケーションWG

このWGでは、総務省委託研究『タイムスタンプ・プラットフォーム技術の研究開発』の一環として、これまでに情報通信研究機構が構築してきたプラットフォームシステムを用い、実サービスに近いアプリケーションを、実際の利用環境で動作させ、運用性の評価、機能の確認などを行う。実験対象とするアプリケーションとしては、電子契約システムおよびログサーバ用い、安定な運用できること、機能が正常動作していること、時刻トレー

サビリティが確保されていることの確認などを行った。

1. 5. 2 長期保証WG

このWGでは、タイムスタンプの効力を長期に保証する方策に関する検証を実施する。文書管理システム実証実験では、リンク情報を使用するアーカイビング方式のタイムスタンプ付与及び検証機能を組み込んだ文書管理システムを対象として、時刻の正確性の確認、デジタル署名及びタイムスタンプ効力の長期保証機能が正常に動作することを確認した。VAによる長期保証実証実験では、タイムスタンプによる長期保証方式とセキュア保管型タイムスタンプ長期保証方式の比較・評価を実施することにより、各方式のメリット・デメリットを検証する。

2. 実証実験の全体概要

総務省委託研究『タイムスタンプ・プラットフォーム技術の研究開発』の一環として、タイムスタンプ・プラットフォームを用い、各種実証実験を行う。

タイムスタンプ・プラットフォームとは、総務省からの委託研究により情報通信研究機構（NICT）が「日本標準時を利用して正確かつセキュリティの高いタイムスタンプ技術」を確立するために構築した研究・実験環境である。

タイムスタンプ・プラットフォームの概要を図2-1に示す。

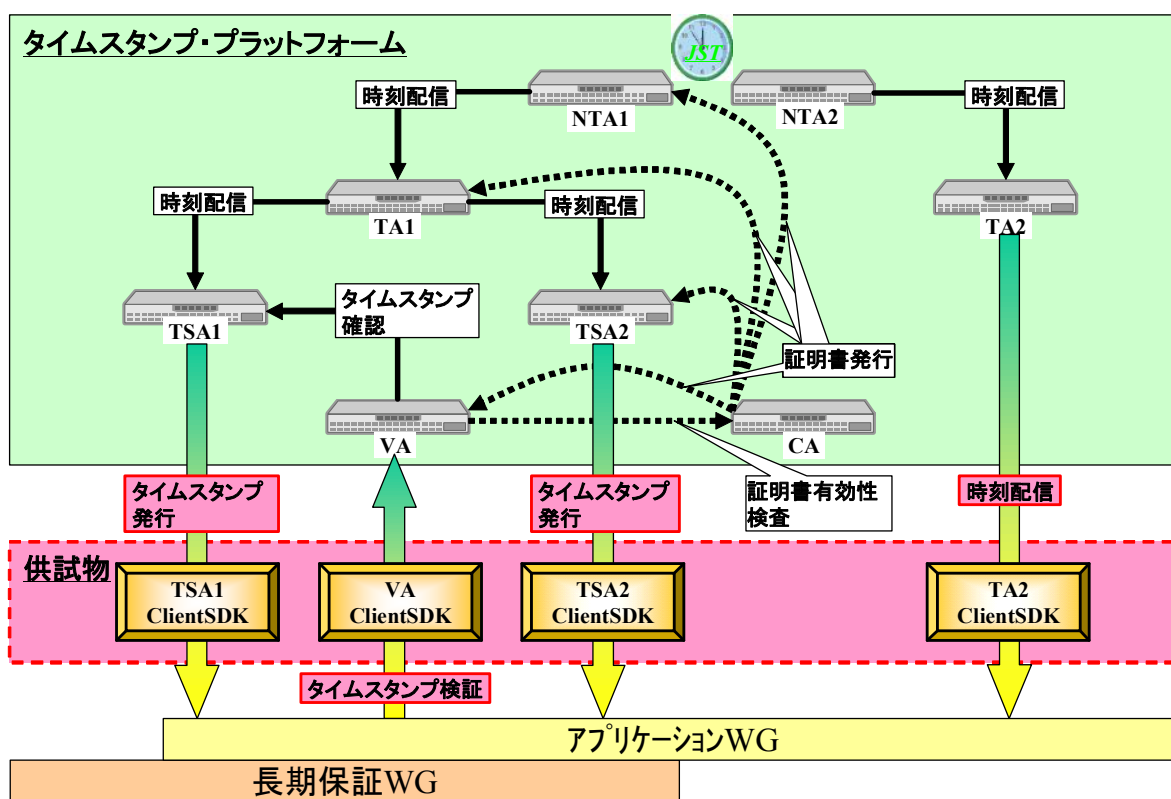


図2-1 タイムスタンプ・プラットフォーム概要図

NTA : National Time Authority

国家時刻標準機関。各時刻認証局に対して標準時の時刻情報を供給する国家的機関。

TA : Time Authority

標準時配信局。時刻関連事業者に標準時に基づく時刻の配信を行い、時刻関連事業者の時刻を認定する機関。

TSA : Time-Stamping Authority

タイムスタンプ局。タイムスタンプサービスを提供し、第三者機関としてタイムスタンプ記録を発行、検証するサービスプロバイダ。

CA : Certification Authority

認証局。PKIにおける公開鍵証明書を発行する機関。

VA : Validation Authority

検証機関。デジタル証明書の失効リストを集中管理して、証明書の有効性をチェックする機関。

図2-1において、TSA1はリンク情報を使用したアーカイビング方式のTSA、TSA2はRFC3161に準拠したデジタル署名を使用する方式のTSAである。TSA1及びTSA2は各々、TA1より、TA1はNTA1より認証連鎖方式^(※1)を用いて時刻配信を受ける。またTA2はNTA2より時刻リンク方式を用いて時刻配信^(※2)を受ける。

この環境を用いて以下の二つのWGに分かれて実証実験を実施した結果を本章では報告する。

- ・アプリケーションWG： タイムスタンプや時刻配信が想定される利用環境にタイムスタンプ・プラットフォームを適用し、サービスに対する機能の充足等を確認することを目的とする。
- ・長期保証WG： タイムスタンプの効力が長期に渡って保証されることをタイムスタンプ・プラットフォームを用いて検証すること等を目的とする。

※1：PKI(Public Key Infrastructure)認証技術を利用してTAが時刻配信先の時計を特定すると同時に時刻の計測と配信を行い、その計測結果を時刻監査記録として更に時刻配信先の時計に連鎖していく方式。

※2：TAが送受信する時刻情報について過去の記録と組合せたデータのハッシュ値を相互に関連付け、その関連性を検証・追跡することにより、時刻の配信元を特定する方式。

3. アプリケーションWGの活動報告

総務省委託研究『タイムスタンプ・プラットフォーム技術の研究開発』の一環として、タイムスタンプ・プラットフォームシステムを用いた実証実験を通じて各機能に関する検証を実施する。

3. 1 電子契約実証実験

3. 1. 1 背景

電子契約サービスにおいては、契約文書の存在日時と非改ざん性を証明するため、タイムスタンプの利用が進んでいる。現状の電子契約サービスにおいては、「サービス利用者以外による検証に対応できていない」、「時刻の正確性が不明である」といった課題があるが、平成 16 年度の実証実験において、タイムスタンプ検証サーバを利用することにより、方式を意識せずに第三者が容易にタイムスタンプを検証できる機能を確認するとともに、日本標準時に同期した時刻情報を含むタイムスタンプトークンの付与機能を確認しており、課題を解決するための基本的な機能の確認が完了している。

しかしながら、実環境に近いアプリケーションに適用した際の運用等まで含めた評価ができていないとともに、検証者側でタイムスタンプトークンの検証時に時刻情報の正確性までは確認できないという課題が残っている。また、万一使用しているタイムスタンプの有効性が損なわれた場合、どのように真正性を保証するかという課題もある。

3. 1. 2 目的

本実証実験においては、独立行政法人情報通信研究機構が研究開発したタイムスタンプ・プラットフォームに電子契約システムを接続し、プラットフォームにより提供される機能や接続した場合の運用性の評価を実施することにより、平成 16 年度の実証実験で残された課題も含めて、現状のサービスの課題を解決した仕組みの実現性を評価する。

3. 1. 3 概要

本実証実験は、デジタル署名を使用する方式及びリンク情報を使用するアーカイビング方式の 2 方式のタイムスタンプ付与及び検証機能を組み込んだ電子契約システムを対象として、実施する。平成 17 年度の実証実験においては、「電子契約システムによる第三者検証」及び「VA を介した第三者検証」の 2 種類のフローについて、実サービスに近い環境に

適用することにより第三者検証等の運用性を評価するとともに、検証サーバにおいて実現される時刻トレーサビリティ確認機能により、タイムスタンプトークンに含まれる時刻情報の経路と誤差を検証者が確認できる仕組みを評価する。また、タイムスタンプの信頼性を向上させる機能として、デジタル署名を使用する方式及びリンク情報を使用するアーカイビング方式の 2 方式によるマルチタイムスタンプ機能を試作し、機能性等の評価を実施する。

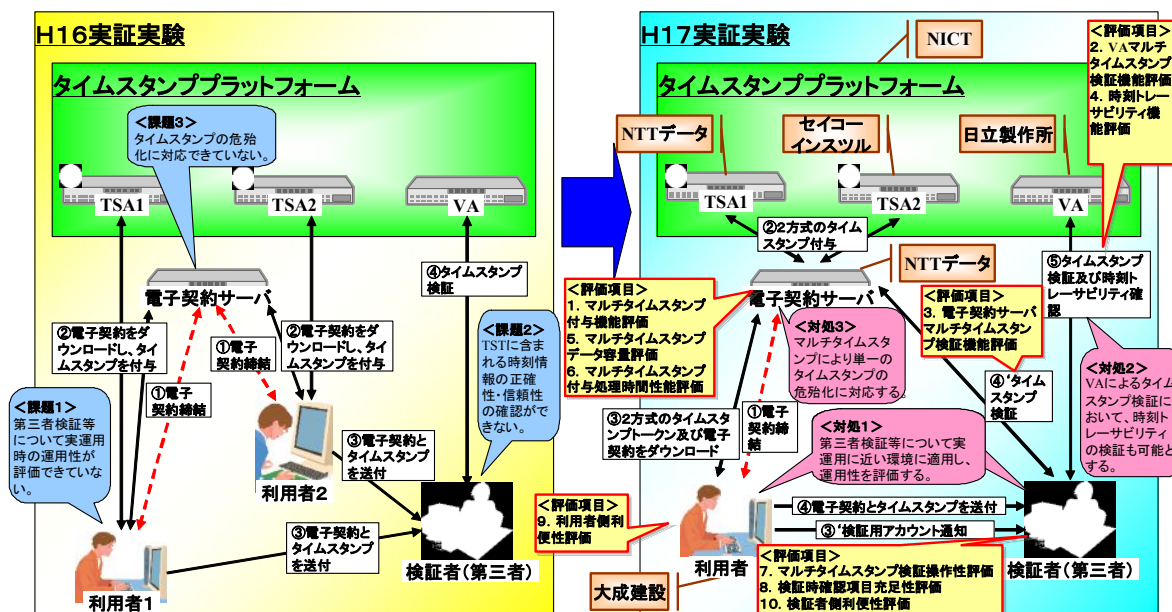


図 3-1 電子契約実証実験概要図

3. 1. 4 評価項目

本実証実験の評価項目を、以下の表 3-1 に記載する。

表 3-1 電子契約実証実験評価項目

項番	評価項目	評価方法
1	電子契約サーバにおいてマルチタイムスタンプが正常に付与されること	電子契約サービスの操作画面において、対象データの確定により 2 方式のタイムスタンプを取得し、その後対象データ及び 2 方式のタイムスタンプトークンをダウンロードする。また正常にダウンロードが行われたかを確認するため、対象データについては登録前後のデータの比較を行う。タイムスタンプについては、VA を介した検証を実施し、正常に検証できることを確認する
2	VA でマルチタイムスタンプの（両方式の）検証が正常に行えること	VA クライアントを使用して、ダウンロードした対象データと 2 方式のタイムスタンプ

項番	評価項目	評価方法
		の検証を実施する。対象データ及びタイムスタンプトークンの改ざんの検出の確認については、ダウンロード後に改変した対象データもしくはタイムスタンプトークンを用いての検証も実施する。また、片方の TSA が利用できない場合の動作確認も実施する
3	電子契約サーバに検証用アカウントでアクセスし、マルチタイムスタンプが付与された対象データの検証が正常に行えること	電子契約サーバに検証用アカウントでログインして登録されている対象データと 2 方式のタイムスタンプの検証を実施する。また対象データ及びタイムスタンプトークンの改ざんを検出できるか確認するため、登録されている対象データ及びタイムスタンプトークンのいずれかについて改変を行い、検証を実施する。また、片方の TSA が利用できない場合の動作確認も実施する
4	VA での検証において、時刻トレーサビリティが確認できること	VA クライアントを使用して、タイムスタンプの検証時に時刻監査レポートまたは時刻監査証明書により、時刻監査情報を確認する
5	マルチタイムスタンプとした場合のサーバで保管するデータの容量ならびにダウンロード及び検証者へ送付するデータの容量	100KBytes 、 1,000KBytes 及び 10,000KBytes の対象データに対して付与した 2 方式のタイムスタンプトークンをダウンロードし、それぞれのファイルサイズを測定する
6	マルチタイムスタンプとした場合のタイムスタンプ付与及び検証時の処理時間の変化	マルチタイムスタンプとした場合の、サーバにおけるタイムスタンプ付与及び検証の処理時間について、単一タイムスタンプの場合との差異を測定する
7	マルチタイムスタンプとした場合の検証の操作手順及び操作時間の変化	マルチタイムスタンプとした場合の、検証時の操作手順（必要な操作回数等）及び処理時間（操作も含めた全体の処理時間等）について、単一タイムスタンプの場合との差異を測定する
8	2 種類のフローにおける検証時に表示すべき情報及びチェックすべき項目の評価	業務上の要件を元に必要項目を抽出し、2 種類の第三者検証フローの検証結果画面等について、充足性を確認する
9	2 種類のフローにおける利用者側での利便性	業務で電子契約を使用している利用者に第三者検証の利用者向け機能を利用して頂き、その後ヒアリングを実施する
10	2 種類のフローにおける検証者へのデータ送付及び検証方法の利便性	業務で電子契約を使用している利用者に第三者検証の検証者向け機能を利用して頂き、その後ヒアリングを実施する

3. 1. 5 成果

本実証実験で得られた成果を、以下に記載する。

(1) 第三者検証の運用性評価

検証端末を商用環境と同じく、インターネット経由にて各サーバに接続する方式にて試験を行い、問題なく電子契約サーバによる第三者検証及びVAを介した第三者検証が行えることを確認した。

また、実業務で電子契約を行っている企業の担当者に検証を実施してもらい、実際の業務上の観点からの評価を得た。

(2) 時刻トレーサビリティ

VAにてタイムスタンプの検証を実施し、時刻トレーサビリティの検証が行えることを確認した。リンク情報を使用するアーカイビング方式のタイムスタンプの検証時は、VAクライアントの画面に表示されるURLで公開されている時刻監査レポートをブラウザにて確認した。デジタル署名を使用する方式のタイムスタンプの検証時には、VAクライアントの画面に表示される時刻トレーサビリティ情報を確認した。

(3) マルチタイムスタンプ

VAを介したタイムスタンプの検証及び電子契約サーバでのタイムスタンプの検証にて、リンク情報を使用するアーカイビング方式のタイムスタンプ、デジタル署名を使用する方式のタイムスタンプどちらかの方式のタイムスタンプが危殆化（改ざん）された場合や、片方のTSAが利用できず検証ができない場合でも、もう一方の方式のタイムスタンプで検証が行えることを確認した。

3. 1. 6 今後の課題

本実証実験で明らかとなった今後の課題を、以下に記載する。

(1) VAを介した第三者検証におけるデータの受け渡し

VAを介したタイムスタンプの検証については、電子契約の利用者より、文書送付のセキュリティや取得、文書送付及び検証操作等の操作性について改善が必要との意見があった。実業務に適用する場合には、それらまで含めたシステム化が求められると考えられる。

(2) 検証用アカウントのアクセス管理

電子契約サーバによるタイムスタンプの検証については、電子契約の利用者より、特定の対象だけを閲覧及び検証可能なようにする必要のあるとの意見があっ

た。実業務に適用する場合には、案件毎に細かくアクセス権を設定できるような機能が求められると考えられる。

(3) マルチタイムスタンプの検証

単一の場合と比べたマルチタイムスタンプの検証について、電子契約サーバによる検証ではサーバで2方式を一括して検証するため、操作性及び処理速度の低下はほとんど見られなかったが、VAを介した検証では方式毎に要求操作が必要のため、操作性及び処理速度の低下が顕著であった。実業務でマルチタイムスタンプの検証を行う場合は、サーバで一括検証する等の対処が求められると考えられる。

3. 2 ログサーバ実証実験

3. 2. 1 背景

一般に広がりつつある電子商取引や電子政府を安全に利用するには、正確で信頼できる時刻が必要である。タイムスタンプ局や企業内のタイムサーバ、システム、ネットワーク機器等の時刻の正確性を検証するには、正当な時刻配信機関からどのくらいの精度で時刻の配信を受けているか示す必要がある。しかし、現在一般に使用されている時刻配信方式では、時刻の正確性を検証するのは難しく、特に時刻のトレーサビリティに関しては検証できなかった。

そこで、平成16年度の実証実験では、時刻リンク方式時刻配信によって、日本標準時を基にした時刻情報がインターネットを介してiDC (internet Data Center : インターネットデータセンター) 内のログサーバに送信され、その時刻情報のトレーサビリティを検証可能であることを実証した。

しかし、日本標準時とiDC内のログサーバとの時刻誤差を検証できない、ログサーバ以外のiDC内の機器に時刻情報を配信することができない、時刻の正確性検証方法が実利用に適していないといった課題点があった。

3. 2. 2 目的

本実証実験においては、独立行政法人情報通信研究機構が研究開発したタイムスタンプ・プラットフォームからiDC内の機器へ時刻情報を配信することにより、平成16年度の実証実験での課題を含めて、時刻リンク方式時刻配信の実用性を評価する。

3. 2. 3 概要

本実証実験では、iDC 内に設置した、時刻リンク方式による時刻送受信機能を組み込んだ NTP サーバおよびログサーバを対象として、実施する。

平成 16 年度の実証実験でログサーバ以外の iDC 内の機器に時刻情報を配信できないという課題については、NTP バージョン 4 に時刻リンク方式の時刻情報を含めることにより、iDC 内の様々な機器へ時刻情報を配信可能とした。本実証実験では、NTP によって配信された時刻情報の日本標準時からのトレーサビリティ検証とその時刻誤差の検証を実施する。また、時刻情報の正確性検証は Web を介して実行可能とし、時刻情報の正確性検証の実用性について評価する。

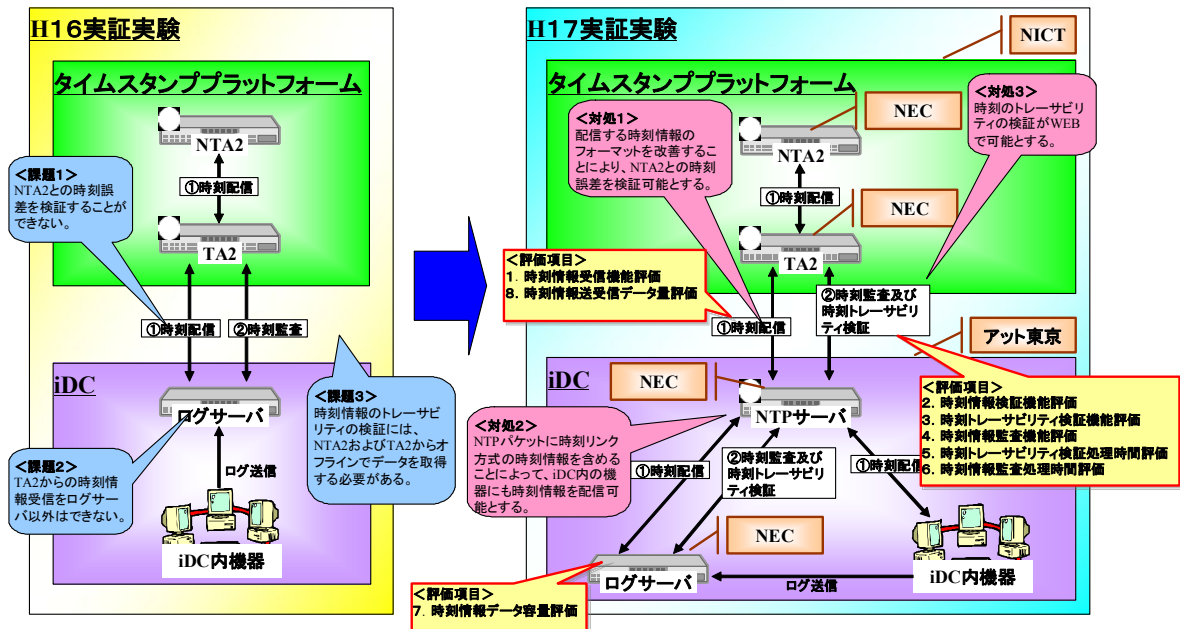


図 3-2 ログサーバ実証実験概要図

3. 2. 4 評価項目

本実証実験の評価項目を以下の表 3-2 に記載する。

表 3-2 ログサーバ実証実験評価項目

項番	評価項目	評価方法
1	iDC 内機器（ログサーバを含む）において、改良 NTP サーバから高信頼度な時刻情報を受信可能なこと	iDC 内機器が、高信頼度な時刻情報を生成・配信する改良 NTP サーバから時刻情報受信を可能なことの機能確認

項番	評価項目	評価方法
2	ログサーバに記録されたログの生成時刻を特定可能なこと	TA2 を使用して、ログに記録された時刻情報が正しいか否かの検証を行う。この検証が、Web を介して実行可能なことの機能確認
3	TA2 での検証において、ログサーバが受信した高信頼度な時刻情報のトレーサビリティが確認できること	TA2 を使用して、ログ内の時刻情報のトレーサビリティおよび日本標準時との時刻誤差の検証が、Web を介して実行可能なことの確認
4	TA2 での時刻監査において、改良 NTP サーバが正確な時刻情報を生成・管理していたことが確認できること	改良 NTP サーバに保存されている時刻情報を改ざん、削除といった不正行為検出のための監査ができることの機能確認
5	ログサーバにおいて、改良 NTP サーバから配信された時刻情報のトレーサビリティの検証を実施した際の処理時間	ログサーバから TA2 に対して、時刻情報のトレーサビリティの検証を要求してから検証結果が返却されるまでの時間を計測
6	改良 NTP サーバにおいて TA2 からの時刻監査を実施した際の処理時間	改良 NTP サーバにおいて、TA2 に対して、時刻監査の要求を行ってから監査結果が返却されるまでの時間を計測
7	長期運用した場合の改良 NTP サーバおよびログサーバで生成される時刻情報のデータ量	改良 NTP サーバおよびログサーバで、実証実験期間内に生成される時刻情報のデータ量を計測
8	高信頼度な時刻情報を送受信する際のネットワークのトラフィック量	TA2-改良 NTP サーバ間、および、改良 NTP サーバ-ログサーバ間のネットワークのトラフィック量を計測
9	本実証実験で使用した時刻配信方式の利便性	iDC 運用者、管理者等へのヒアリングもしくはアンケートを実施

3. 2. 5 成果

本実証実験で得られた成果を、以下に記載する。

(1) 時刻トレーサビリティ

インターネットを介してログサーバに高信頼度な時刻情報を配信し、ログサーバにおいて受信した高信頼度な時刻情報を付与したログの生成・保存機能が正常に動作することについて確認できた。また、ログに記載された高信頼度な時刻情報のトレーサビリティを検証する機能が正常に動作することについて確認できた。

(2) 高信頼度な時刻情報による時刻監査

高信頼度な時刻情報の生成・管理を行っている NTP サーバに対して、インターネットを介した時刻監査を行う機能が正常に動作することについて確認できた。

(3) 時刻精度

高信頼度な時刻情報の配信プロトコルには、改良した NTP を使用した。改良した NTP は、一般に使用されている NTP のパケットに高信頼度な時刻情報を埋め込んでいるが、iDC 内の NTP サーバと日本標準時との時刻誤差がほぼ数ミリ秒以内であったことを確認できた。

3. 2. 6 今後の課題

本実証実験で明らかとなった今後の課題を、以下に記載する。

(1) 時刻精度の向上

本実証実験では、一般に使用されている PC とソフトウェアにて時刻補正を行った。しかし、アンチウイルスソフトといった他のソフトウェア動作時に、時刻精度が低下してしまった。今後は、他ソフトウェアの動作で影響のない、時刻同期を行う方法を確立したい。

(2) 高信頼度な時刻情報の管理

本実証実験の時刻トレーサビリティ検証及び時刻監査の実施には、高信頼度な時刻情報を用いて行っている。しかし、高信頼度な時刻情報のバックアップ、リストアは行っておらず、障害が発生した場合の対処方法を確立していない。今後は、システムの 2 重化等を行い、障害発生時にも安定した時刻情報を提供するようになりたい。

4. 長期保証WGの活動報告

総務省委託研究『タイムスタンプ・プラットフォーム技術の研究開発』の一環として、タイムスタンプの効力を長期に保証する方策に関する検証を実施する。

4. 1 文書管理システム実証実験

4. 1. 1 背景

電子文書の保管等の業務においては、e-文書法の施行等に伴い、その存在日時と非改ざん性を証明するため、タイムスタンプの利用が促進されている。

その一例として、これらの電子文書の真正性を証明する機能を、既存の管理システムに組み入れて実現するため、文書管理システムにタイムスタンプの付与及び検証機能を組み込んだ製品が検討されているが、時刻の正確性の確認やデジタル署名及びタイムスタンプの効力の長期保証等、いくつかの課題が残っている。

4. 1. 2 目的

本実証実験においては、独立行政法人情報通信研究機構が研究開発したタイムスタンプ・プラットフォームに文書管理システムを接続し、プラットフォームにより提供される機能の評価ならびにデジタル署名及びタイムスタンプの効力延長機能の実装及び評価を実施することにより、現状の課題を解決した仕組みの実現性を評価する。

4. 1. 3 概要

本実証実験は、リンク情報を使用するアーカイビング方式のタイムスタンプ付与及び検証機能を組み込んだ文書管理システムを対象として、実施する。

まず、時刻の正確性の確認に係る課題については、TSA による時刻監査レポートの公開により、タイムスタンプに含まれる時刻情報のトレーサビリティの確認を可能とする。デジタル署名及びタイムスタンプ効力の長期保証に係る課題については、長期署名フォーマットをベースとして、タイムビジネス推進協議会より公開されている「タイムスタンプ長期保証ガイドライン」におけるリンク方式タイムスタンプ長期保証の実現例に沿った長期保証機能を実装し、タイムスタンプの再付与による効力延長を可能とする。

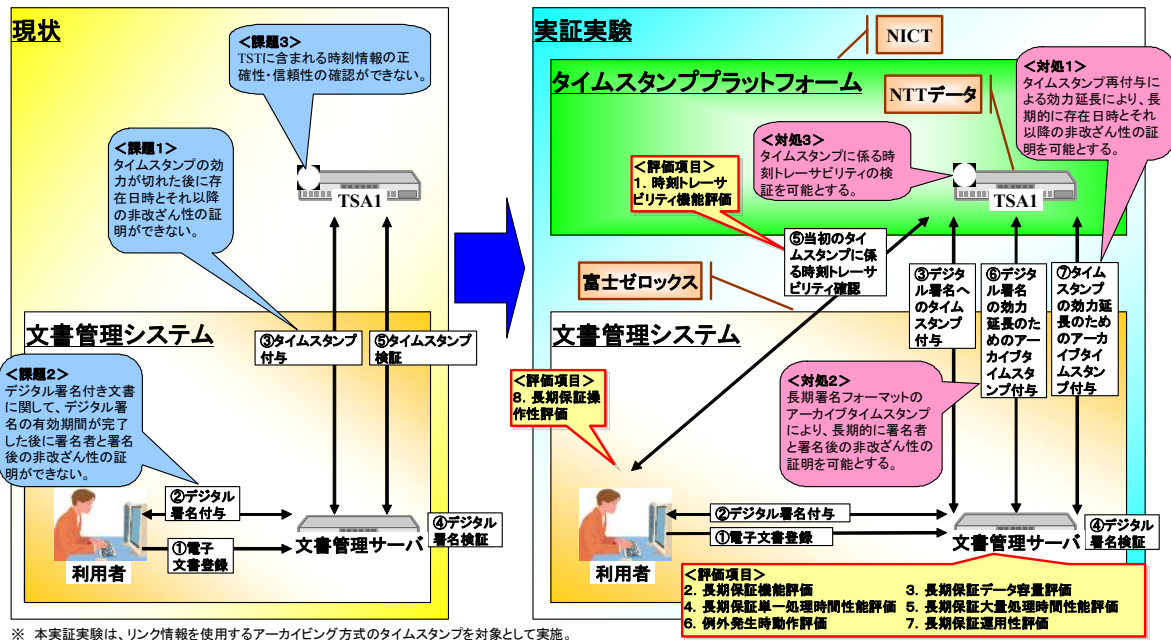


図 4-1 文書管理システム実証実験概要図

4. 1. 4 評価項目

本実証実験の評価項目を、以下の表 4-1 に記載する。

表 4-1 文書管理システム実証実験評価項目

項番	評価項目	評価方法
1	タイムスタンプの時刻情報に係る時刻トレーサビリティが確認できること	時刻監査レポートをダウンロードし、その真正性とタイムスタンプの時刻情報に係る配信経路及び誤差を確認できることを確認する
2	長期保証に対応したタイムスタンプの付与、再付与及び検証ができること	文書管理システムにおいて、XAdES をベースにしたフォーマットを用いて、以下を実行出来ることを確認する。 <ul style="list-style-type: none"> デジタル署名付与 デジタル署名検証 署名タイムスタンプ付与 署名タイムスタンプ検証 アーカイブタイムスタンプ付与 アーカイブタイムスタンプ再付与 アーカイブタイムスタンプ検証
3	長期保証する際に保管が必要となるデータの容量	XAdES をベースにしたフォーマットで、長期保証を継続するにあたり保管が必要となるデータ容量の増加具合の測定を行う
4	通常のタイムスタンプの付与及び検証	以下の処理を実行した際に、ログファイル

項番	評価項目	評価方法
	らびに長期保証に係るタイムスタンプの再付与及び検証の処理時間	に出力される処理時間を求める。 <ul style="list-style-type: none"> ・デジタル署名検証 ・署名タイムスタンプ付与 ・署名タイムスタンプ検証 ・アーカイブタイムスタンプ付与 ・アーカイブタイムスタンプ再付与 ・アーカイブタイムスタンプ検証
5	大量の文書に対して、一時に長期保証のためのタイムスタンプ再付与を実施した際の処理時間	1 万件の文書に対して以下の処理を実行した際に、ログファイルに出力される処理時間を求める。 <ul style="list-style-type: none"> ・デジタル署名及び署名タイムスタンプ付与 ・アーカイブタイムスタンプ付与 ・アーカイブタイムスタンプ再付与
6	タイムスタンプの付与処理及び検証処理における例外発生時の AP の振る舞い	例外発生時の AP の振る舞いについて、利用面からの妥当性の検証を行う
7	AP における長期保証に対応した運用性	タイムスタンプの有効性が損なわれる可能性が生じる代表的な場面を想定し、場面に合わせた条件を指定し、対象ファイルに対してタイムスタンプの効力延長を行なえる実効的な機能が備わっていることを確認する
8	通常タイムスタンプの付与及び検証ならびに長期保証に係るタイムスタンプの再付与及び検証の利便性	実際に利用者及び検証者がアプリケーションを利用する際に、一連の処理にどの程度の時間と操作回数を要するかを測定する

XAdES : XML 署名に対応した署名の長期保存フォーマット

4. 1. 5 成果

本実証実験で得られた成果を、以下に記載する。

(1) タイムスタンプ再付与によるタイムスタンプ長期保証

文書管理システムの環境において、XAdES をベースとし TBF タイムスタンプ長期保証ガイドラインに即した、リンク情報を使用するアーカイビング方式のタイムスタンプ再付与及びその検証の機能が正常に動作すること、保管に必要なデータ容量、単一文書の処理時間、実運用時の目安となる大量文書（1 万件）の再付与処理時間、例外発生時の動作、再付与を要する想定場面に応じた運用性及び利用者側の操作性について、確認できた。

(2) タイムスタンプ付与によるデジタル署名長期保証

文書管理システムの環境において、XAdES をベースとした、リンク情報を使用

するアーカイビング方式タイムスタンプの付与及び検証の機能が正常に動作すること、保管に必要なデータ容量、単一文書の処理時間、例外発生時の動作及び利用者側の操作性について、確認できた。

(3) 時刻トレーサビリティ

文書管理システム的环境において、時刻トレーサビリティ機能が正常に動作することについて、確認できた。

4. 1. 6 今後の課題

本実証実験で明らかとなった今後の課題を、以下に記載する。

(1) 時刻トレーサビリティ確認の利便性

本実証実験では、時刻監査レポートにより時刻トレーサビリティの確認を行ったが、目視での確認や手動による計算作業が必要となるため、長期間運用を行う際には、手順が煩雑であるとともに、確認ミスや計算ミスが生じる可能性がある。今後、検証者による時刻トレーサビリティ確認作業をよりスムーズかつ確実に行うために、時刻トレーサビリティの確認を自動で行なえるしくみがあることが望ましい。

(2) 多様な環境における処理性能測定

本実証実験では、長期保証大量処理における所要時間の指標を得ることが出来たが、ハードウェア構成、ネットワーク構成及び対象文書の容量により変化する可能性があるとともに、件数を変更した場合にその所要時間は比例関係とならない可能性も考えられる。様々な環境において参考とできる指標を得るためには、文書数や文書のデータ容量を変化させ、様々なシステム構成下で性能評価を行うことが望ましい。

4. 2 VAによる長期保証実証実験

4. 2. 1 背景

電子文書の保管等の業務においては、e-文書法の施行等に伴い、その存在日時と非改竄性を証明するため、タイムスタンプの利用が促進されている。タイムスタンプの方式には、大きく分類し、デジタル署名を使用する方式とリンク情報を使用する方式が存在する。デジタル署名を使用する方式に関しては、有効期間が明示的に設定されており、タイムスタンプの長期保証が重要な課題として挙げられている。また、タイムスタンプに使用された暗号アルゴリズムの脆弱化対策として、タイムスタンプの有効性を延長することも重要な課題である。

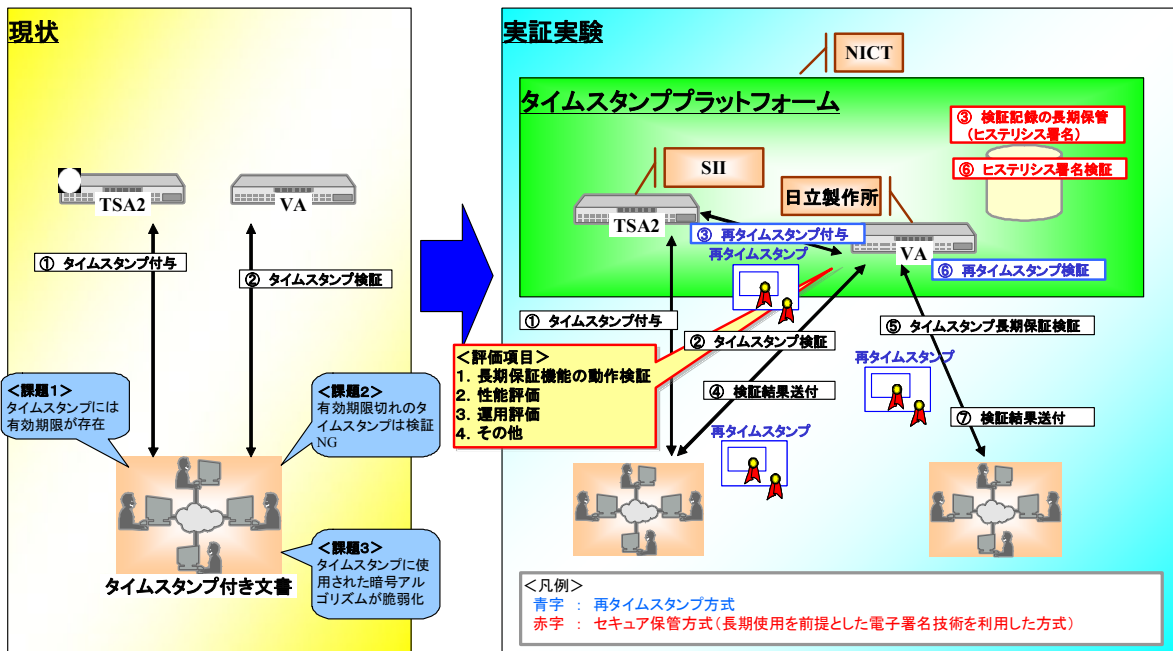
4. 2. 2 目的

本実証実験においては、独立行政法人情報通信研究機構が研究開発したタイムスタンプ・プラットフォームを用いて、①「タイムスタンプによる長期保証方式」（以下、再タイムスタンプ方式）、②「セキュア保管型タイムスタンプ長期保証方式（長期使用を前提とした電子署名技術を利用した方式）」（以下、セキュア保管方式）、の2方式において比較・評価を実施することにより、現状の課題を解決した仕組みの実現性を評価する。

4. 2. 3 概要

本実証実験は、デジタル署名を使用する方式のタイムスタンプを付与した電子文書を対象として、実施する。

タイムスタンプ・プラットフォームの検証サーバの起動モードを、①再タイムスタンプ方式、及び②セキュア保管方式、に切り替えて、それぞれの方式においてタイムスタンプ長期保証の評価を実施する。評価にあたっては、運用面、性能面などを中心に、各方式のメリット・デメリットを検証する。



※ 本実証実験は、デジタル署名を使用する方式のタイムスタンプを対象として実施。

図 4-2 VA による長期保証実証実験概要図

4. 2. 4 表価項目

本実証実験の評価項目を、以下の表 4-2 に記載する。

表 4-2 VA による長期保証実証実験評価項目

項番	評価項目	評価方法
1	長期保証機能動作検証	インターネット環境上における長期保証機能動作を検証する
2	性能評価	長期保証時及びタイムスタンプ検証時の処理性能を中心に、各方式を比較検討する
3	運用評価	VA 利用者側及び VA 管理者側の運用工数を評価し、各方式を比較検討する
4	その他	各方式の仕様上の課題、運用上の課題などを洗い出し、実利用に向けた対策を検討する

4. 2. 5 成果

本実証実験で得られた成果を、以下に記載する。

(1) 長期保証機能動作検証

プロキシ・サーバを含む企業内ネットワークから、インターネットを介してVAを利用した。再タイムスタンプ方式、及びセキュア保管方式（長期使用を前提とした電子署名技術を利用した方式）ともに、正常に動作することを確認した。

(2) 各方式の長所と短所

本実証実験における性能評価及び運用評価、また、机上検討を踏まえて、再タイムスタンプ方式及びセキュア保管方式の長所・短所の整理を表4-3に行った。

表4-3 再タイムスタンプ方式及びセキュア保管方式の長所・短所

No.	項目	再タイムスタンプ方式	セキュア保管方式
1	長所	<ul style="list-style-type: none"> ポータビリティ性あり VA利用者以外が受け取っても検証することが可能。 相互運用性あり 仕様を公開しそれを実現した他社製品でも、検証が可能。 	<ul style="list-style-type: none"> クライアント運用負荷小 一度登録すれば、その後永続的に検証することが可能であり、負荷が少ない。 データサイズは不変 永続的に同一のデータを利用できるので、データサイズは不変。 長期保証データ登録処理時間(*) 既存のデータ登録数などに影響を受けず、ほぼ一律の処理時間で登録が可能。
2	短所	<ul style="list-style-type: none"> クライアントの運用負荷大 タイムスタンプの有効期間管理、長期保証の要求、を定期的実施する必要があり、運用負荷が大きい。 データサイズの増大 再タイムスタンプの付与により、タイムスタンプのデータサイズが増大してゆく。 コストが発生 再タイムスタンプを付与することによる費用が発生する。 長期保証データ作成処理時間(*) 再タイムスタンプの数に応じて、検証処理時間が変動し長期保証データの作成処理時間も変動する。 長期保証データ検証処理時間(*) 	<ul style="list-style-type: none"> ポータビリティ性なし 長期保証の登録を行ったVAでのみ検証が可能。 相互運用性なし ヒステリシス署名技術は、日立製作所独自技術のため現状相互運用は難しい。 サーバの運用負荷大 登録データ量によって、ストレージ管理などの運用が発生する。 長期保証データ検証処理時間(*) 既存のデータ登録数に応じて、検証処理時間が変動する。

		再タイムスタンプの数に応じて、 検証処理時間が変動する。	
3	適用データ	他組織間で長期に亘ってやり取りする流通データなど。	組織内で閉じて利用するデータなど。

(*)処理時間に関しては、機器のスペック向上などによって改善が見込める為、今回の実験結果のみから、各方式を比較評価することは困難である。

4. 2. 6 今後の課題

本実証実験、及び机上検討により明らかとなった今後の課題を、以下に記載する。

(1) 利便性を考慮した考察

VA の利用者や VA の運用者の利便性の観点から見た考察結果は、表 4-4 の通りである。

表 4-4 再タイムスタンプ方式及びセキュア保管方式の利便性を考慮した考察

No.	方式	項目	課題と対策
1	再タイムスタンプ方式	クライアント運用負荷の軽減	長期保証の対象文書が大量に存在する実環境においては、クライアントの運用負荷が大きく、実用的ではない。 実運用で利用する場合には、文書管理サーバなどが一括してタイムスタンプ有効期間を管理し、自動的に VA に長期保証依頼を送信する、などの対策が必要であると考ええる。
		クライアント主導による長期保証	今回の実証実験では、VA の設定にて「受け付けたタイムスタンプに対して常に再タイムスタンプを付与する」としていた為、単純に検証だけを実施した場合でも再タイムスタンプを付与していた。 実運用で利用する場合は、クライアントにて「検証後、長期保証を実施する」「検証のみを実施する」などを選択できる作りにすることが望まれる。
2	セキュア保管方式	登録データの大容量化への対応	長期保証対象のデータが大量にある場合、サーバでの登録データ容量が膨大になる可能性がある。 定期的なディスク使用率の監視や登録データの圧縮による容量削減などの対策を講じる必要がある。

(2) 技術的な課題に係る考察

VAの実装に関わる技術的な課題に対する考察は、表4-5の通りである。

表4-5 再タイムスタンプ方式及びセキュア保管方式の技術的な課題に係る考察

No.	方式	項目	課題と考察
1	再タイムスタンプ方式	検証情報に含まれるトラストアンカ証明書の信頼性の検証	再タイムスタンプの検証情報に含まれるトラストアンカ証明書の信頼性を確認するための情報が、長期保証されたタイムスタンプの中には含まれておらず、信頼性を確認することができない。 トラストアンカ証明書の信頼性を確認することが必要であり、確認方法の一つとしては、VAが保管するトラストアンカ証明書と照合することにより信頼性を確認することが考えられる。具体的な検討は今後の課題である。
		Grace Period(猶予期間)を踏まえた検証	Grace Period(猶予期間)とは、公開鍵証明書の利用者が、証明書の失効申請を行ってから、CRLなどの失効情報が公開されるまでのタイムラグを示す。ある時点において、公開鍵証明書の有効性は有ると判断されたものが、後日に、当初の評価時点を再度確認すると、その公開鍵証明書の有効性は無いと判断される可能性がある。 長期保証されたタイムスタンプに含まれたTSAの公開鍵証明書を、当時の時点で再検証するときには、Grace Periodを踏まえたCRLを別途入手する必要があるかもしれない。Grace Periodを踏まえた検証方法に関しては、今後の課題である。
		暗号アルゴリズムの脆弱性評価を踏まえた検証	長期保証されたタイムスタンプの中には、現時点にて、脆弱性があると判断された暗号アルゴリズムが使用されている可能性がある。 長期保証されたタイムスタンプの検証では、当時の暗号アルゴリズムの脆弱性を判断することが重要である。方式については今後の課題である。
2	セキュア保管方式	署名履歴のトラストアンカの公開	署名履歴の正当性を第三者へ証明するための手段として、署名履歴のトラストアンカとなる最新のヒステリシス署名データを公開する運用は重要である。 具体的な公開運用としては、永続性が期待される公共的な機関へトラストアンカを預託することが好ましいと思われる。
		署名履歴の整合性検証の性能	サーバへの登録データ数が増えると、検証性能が劣化する可能性がある。 例えば、署名履歴に含まれるトラストアンカを定期的に作成し、署名履歴の整合性検査では、隣接するトラストアンカまでの整合性を確認することにより、検証性能を劣化させない方法が考えられる。

No.	方式	項目	課題と考察
		暗号アルゴリズム脆弱性への対策	長期に亘って VA を運用する場合、過去に作成されたヒステリシス署名に使用されたハッシュ関数（署名履歴の連鎖構造を保証する）に脆弱性が発見される可能性がある。 考えられる一つの方法としては、脆弱性が指摘される前に、再度、該当する検証記録とヒステリシス署名データに対して、最新のヒステリシス署名を適用することで有効性を延長させることが挙げられる。

5. うるう秒とコンピュータクロック

7年ぶりに実施される「うるう秒挿入」を前に、情報を整理、共有し、タイムビジネスへの影響を把握しておくことを目的に調査を行った。

5. 1 うるう秒調整

UTC（協定世界時）と UT1（地球回転の観測から決定されている時刻）の差が 0.9 秒以内となるよう、UTC での「月末の最後の分」の長さで調整する。実際には、6 月末と 12 月末が第 1 優先度の調整時期となっており、これまで、このいずれかにうるう秒挿入、つまり 1 分の長さを 61 秒とする調整が実施されている。

5. 2 7年ぶりのうるう秒挿入で起こり得る問題

地球自転速度の関係から、この7年間うるう秒調整は実施されていない。今回のうるう秒挿入では、次に示すような事項から問題が起こる可能性があるため、時刻が重要な役割を果たしているシステムでは、十分な準備をするのが望ましい。

- ・ 新しい機器、ソフトウェア、管理者は、うるう秒を経験していない
- ・ うるう秒挿入が休日、しかも多くの国では夜～早朝となる
- ・ NTP など秒単位以下の時刻供給手段の普及は、前回のうるう秒以降である
- ・ 7年前、コンピュータ時計の誤差 1 秒は問題にはならなかった
- ・ システムによっては、秒未満の部分で時計が逆戻りする可能性がある
- ・ トラステッドタイムスタンプなど、時刻情報に依存するサービスが始まっている

表 5-1 今回のうるう秒挿入前後の様子

UTC	JST	TAI-UTC	Leap Indicator	NTP Time	UNIX Time (*1)	UNIX Time (*2)

2005/12/30 23:59:59	2005/12/31 08::59:59	32	00	3344975999	1135987199	1135987221
2005/12/31 00:00:00	2005/12/31 09:00:00	32	01	3344976000	1135987200	1135987222

2005/12/31 23:59:59	2006/01/01 08::59:59	32	01	3345062399	1136073599	1136073621
2005/12/31 23:59:60	2006/01/01 08::59:60	32	01	3345062400	1136073599	1136073622
2006/01/01 00:00:00	2006/01/01 09:00:00	33	00	3345062400	1136073600	1136073623
2006/01/01 00:00:01	2006/01/01 09:00:01	33	00	3345062401	1136073601	1136073624

*1 うるう秒を考慮しない場合（POSIX 仕様：実際のシステムのほとんど）

*2 うるう秒を考慮した場合（設定変更を行うか、時刻関係のライブラリを入替える）

おわりに

実証実験の具体的な課題を検討していた平成 15 年頃と比べると、タイムビジネスを取り巻く環境が大きく変わってきており、現在も、その変化の速度は増加している。

当時、電子時刻認証技術について、ほとんどの人はその存在すら知らず、その有効性を説明するにも時間がかかる状態が続いた。このようなことから、実証実験の推進も、とにかく動作するものを用意し、できるだけ多くの人にその動作に触れてもらい、理解してもらおう、ということが重要な目的の 1 つであった。

このような状況は、平成 15 年度末頃から急激に変わりだした。それまでは、宣伝しても大きな反応がなかったのが、電子時刻認証関係の情報を求めて、外部から TBF に問い合わせが来るようになった。最も大きな変化は、この頃から法制面の整備が具体化する方向に動き出したことであろう。法制化促進は TBF からの要望でもあったが、e-文書法施行時期が平成 17 年 4 月と示された頃には、準備期間は 1 年を切っており、早期実現を唱えていた TBF 関係者も頭を抱えるほどの過密スケジュールとなった。

当初の実証実験スケジュールでは実験結果をまとめている予定だった時期に、認定を受ける商用サービスの立ち上が必須となり、実証実験の実施予定者が、商用サービス立ち上げに多忙をきわめるなど、周辺状況の変化に応じて実証実験スケジュールも柔軟に対応する必要があった。

初期に設定された実証実験課題については、商用サービス立ち上げの動きと照らし合わせ、遅れを取る前に成果をまとめる、実サービスへ成果を反映する、早期終結するなど、可能な限り有意義で無駄のない活動に絞るようにスケジュールを変更した。

平成 17 年度の課題は、電子時刻認証を用いた商用サービスをより安心して使うため、または長期にわたって安全性を確保するための技術実証を選択した。これらの実証実験は、電子時刻認証をめぐる速い動きに乗り遅れることのないよう、短期集中的に計画、実施、成果取りまとめを行い、すでに、成果の一部は商用サービス実施に役立っている。

これまで、実証実験分科会が具体的な課題の選定を始めてから、およそ 3 年間の活動を行ってきた。TBF 自体には、予算がなく実証実験を参加者負担で進める必要があり、タイムビジネスを取り巻く環境が急速に変化するなど、実証実験の実施は、困難な点多かったが、一定の活動成果をあげることができたと考えている。

平成 18 年度以降、どのような課題を推進するか、またそれ以前に、TBF で実証実験を取り上げるかどうか未定である。現時点で言えるのは、まだまだ、実証を行うべき課題は山積しており、かつ、状況の変化は加速を続けているということであろう。

かつて、電子メールも、その誕生からしばらくは、一部の技術者が使う特殊な道具とみなされていた。それが、パソコンの普及、メール機能の携帯電話への搭載などによって、現在では重要なインフラの 1 つとなっている。

電子時刻認証も、すでに実用化の段階には入っているが、インフラの 1 つとなるには、何らかのブレークスルーを経る必要があるだろう。これは、電子署名技術全般についても言えるかもしれない。ユーザが意識することなく、電子署名＋電子時刻認証で安全が確保される、守られる対象も、単なる電子文書に限らず、著作物の利用権、さらには、あらゆる利用権、所有権の証明に広く使われる状況もあり得る。

電子署名によらない電子時刻認証や、それ以外のタイムビジネスも、インフラの 1 つ、または重要なインフラを支える技術になり得る。今後も、TBF 参加者はもちろん、直接参加していない方々にも、タイムビジネスの意義と可能性をご理解頂き、今後の発展をサポートして頂けることを願っている。

タイムビジネス推進協議会
技術部会・実験実証分科会主査
独立行政法人情報通信研究機構
鳥山 裕史

【連絡先】

タイムビジネス推進協議会（T B F）

〒160-0022

東京都新宿区新宿 1-20-2 小池ビル

財団法人テレコム先端技術研究支援センター

タイムビジネス推進協議会事務局

Tel.03-3351-8166

Fax.03-3351-1624

URL : <http://www.scat.or.jp/time/>

※本報告書の無断転載を禁止します。