時刻認証基盤技術実験装置
―統合化プラットフォームシステム―

実証実験評価報告書

平成 18 年 3 月 16 日

目　　次

１．実証実験全体概要

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、各種実証実験を行った。

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１－１に示す。

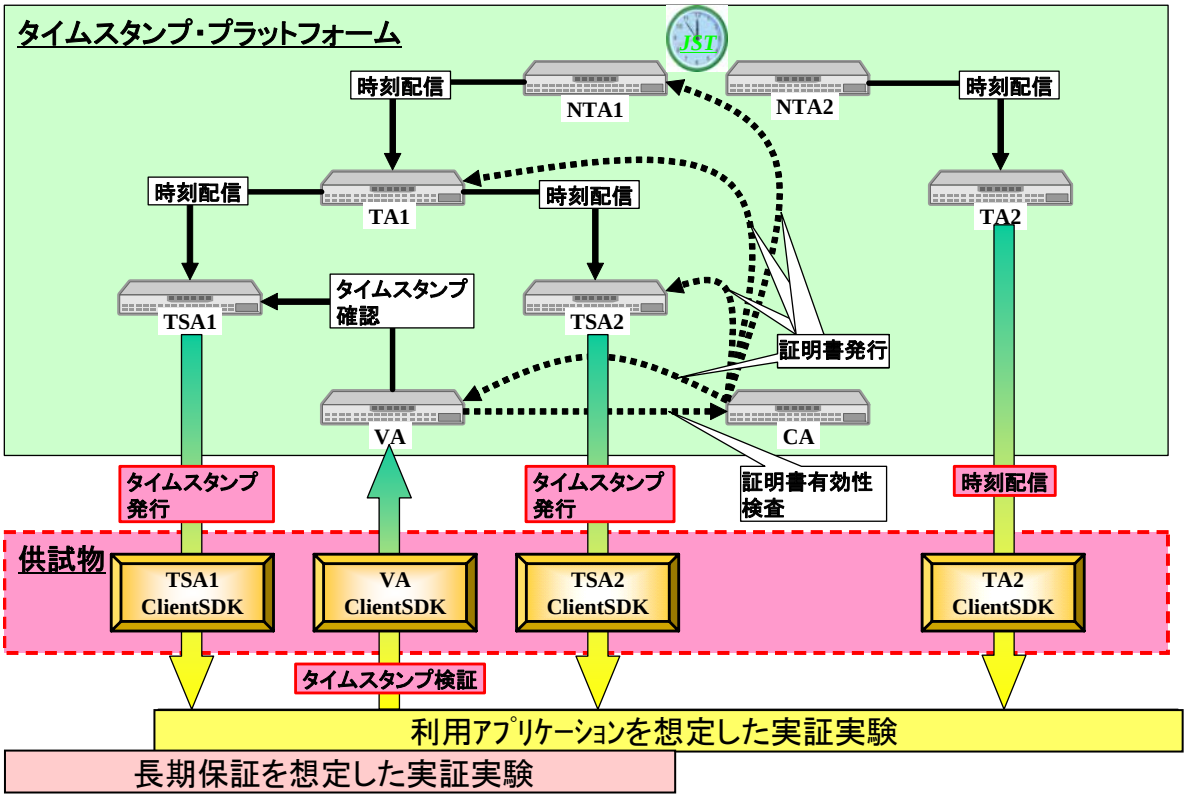


図１－１　タイムスタンプ・プラットフォーム概要図

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１－１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。

※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。

２．　利用アプリケーションを想定した実証実験

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。

２．１　電子契約実証実験

２．１．１　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。

２．１．２　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。

２．１．３　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。

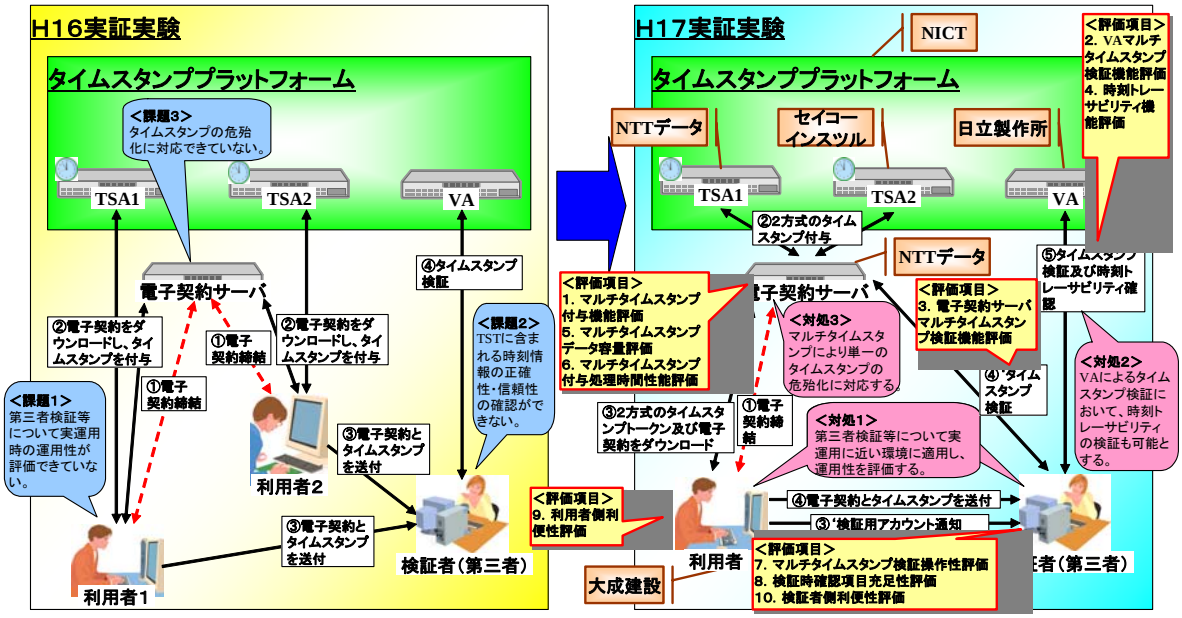


図２－１　電子契約実証実験概要図

２．１．４　評価項目

本実証実験の評価項目を、以下の表２－１に記載する。

表２－１　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

項番	評価項目	評価方法
		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

２．１．５　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。

２．１．６　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が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なため、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。

２．２　ログサーバ実証実験

２．２．１　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。

２．２．２　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。

２．２．３　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。

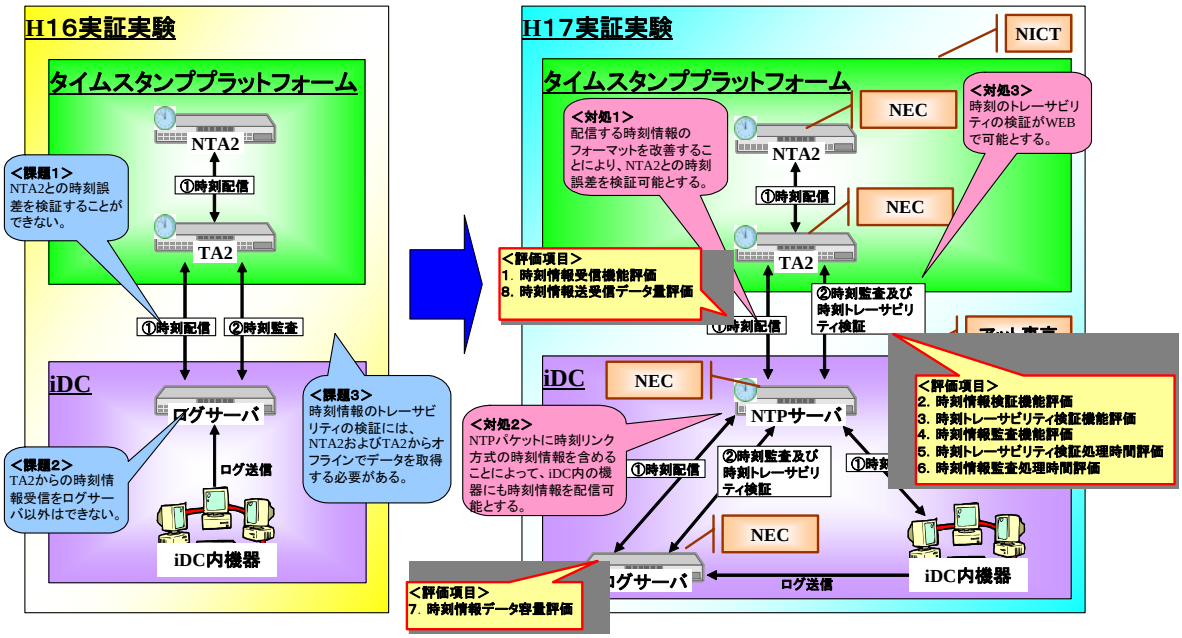


図２－２　ログサーバ実証実験概要図

２．２．４　評価項目

本実証実験の評価項目を以下の表２－２に記載する。

表２－２　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
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

項番	評価項目	評価方法
		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 サーバー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

２．２．５　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。

２．２．６　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したい。

３．長期保証を想定した実証実験

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。

３．１　文書管理システム実証実験

３．１．１　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。

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。

３．１．３　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。

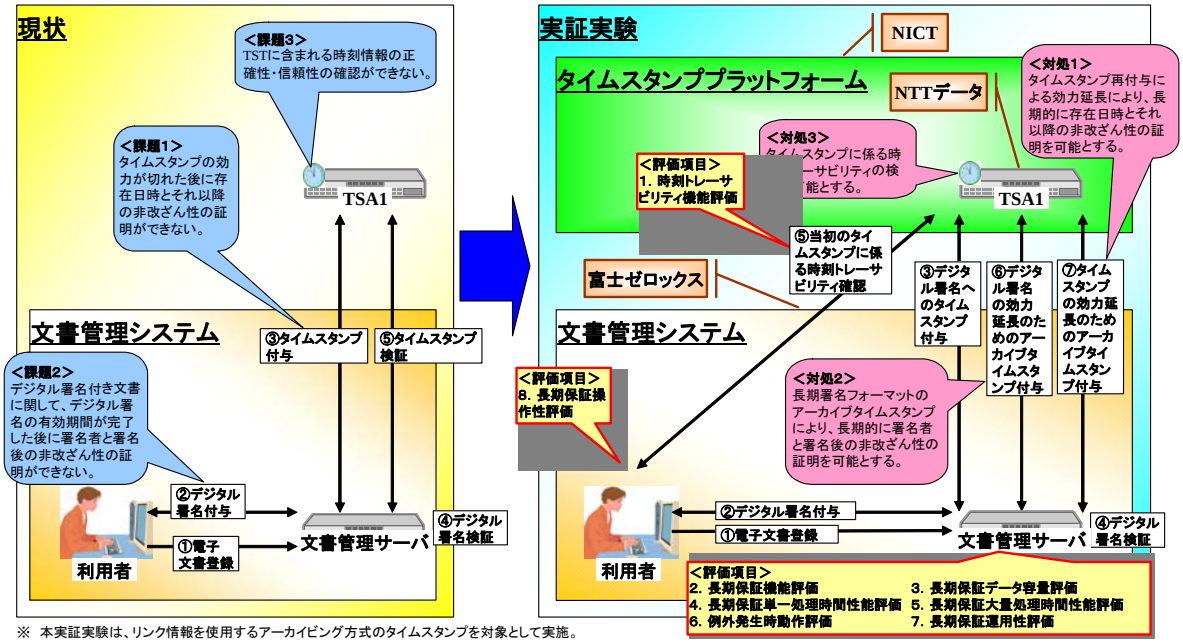


図３－１ 文書管理システム実証実験概要図

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 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。 ・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な	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。 ・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。 ・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	通常の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

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）　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

文書管理システムの環境において、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。

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） 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。

３．２　VA による長期保証実証実験

３．２．１　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。

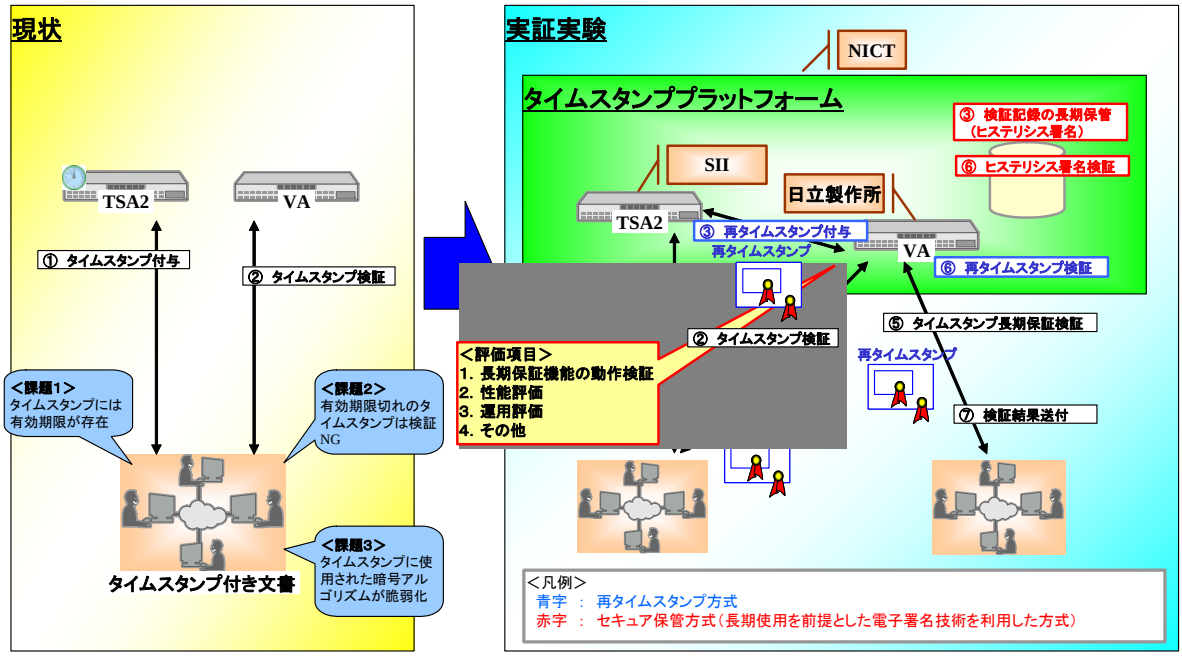
３．２．２　目的

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。

３．２．３　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３－２ VA による長期保証実証実験概要図

３．２．４　表価項目

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 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

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）　長期保証機能動作検証

プロキシー・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３－３に行った。

表３－３　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	・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。	・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	・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、を定期的に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(*) 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。	・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。
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。

３．２．６　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３－４の通りである。

表３－４　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

№	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い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。 定期的なディクス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３－５の通りである。

表３－５　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

№	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

№	方式	項目	課題と考察
			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性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、現在時点にて、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一手段として、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多くなると、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。
		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。