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

【実証実験評価報告書の構成】

統合化プラットフォームシステム

・電子契約実証実験

・ログサーバ実証実験

・文書管理システム実証実験

・VA による長期保証実証実験

電子契約実証実験評価報告書

平成 18 年 3 月 16 日

独立行政法人情報通信研究機構
株式会社エヌ・ティ・ティ・データ
大成建設株式会社
セイコーインスツル株式会社
株式会社日立製作所

目次

第 1 章 はじめに 1
1. 背景と目的 1
1-1 課題 1
1-2 目的 1
1-3 概要 1
2. 実証実験の基礎となっている技術 2
2-1 タイムスタンプについて 2
2-1-1 概要 2
2-1-2 タイムスタンプの方式 3
2-1-3 マルチタイムスタンプについて 5
2-2 時刻トレーサビリティについて 6
2-3 VA（検証サーバ）について 7
2-4 電子契約サービスについて 9
第 2 章 実証実験の内容 10
1. 実証実験の概要 10
1-1 実証実験の対象とする課題と目的 10
1-2 実証実験での確認概要 11
2. 実証実験の体制 11
2-1 試験環境準備での分担及び実施内容 11
2-2 機能確認試験での担務分担 11
2-3 実証実験での役割分担 11
2-4 実験結果整理時の分担 11
3. 実験項目 11
4. 実証実験構成 11
5. 実証実験処理の手順 11
5-1 作業日程 11
5-2 マルチタイムスタンプの付与手順 11
5-3 VA を介した検証手順 11
5-4 電子契約サーバによる検証手順 11
6. 実証実験の結果 11
6-1 マルチタイムスタンプ付与機能評価 11
6-2 VA マルチタイムスタンプ検証機能評価 11
6-2-1 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 11
6-2-2 デジタル署名を使用する方式のタイムスタンプの検証 11
6-2-3 VA での対象データ改ざんの検出（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） 11
6-2-4 VA での対象データ改ざんの検出（デジタル署名を使用する方式のタイムスタンプ） 11
6-2-5 VA での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トークン改ざんの検出 11
6-2-6 VA でのデジタル署名を使用する方式のタイムスタンプ改ざんの検出 11
6-2-7 TSA1 切断時の VA での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 11
6-2-8 VA マルチタイムスタンプ検証機能評価結果 11
6-3 電子契約サーバマルチタイムスタンプ検証機能評価 11
6-3-1 電子契約サーバでのマルチタイムスタンプの検証 11
6-3-2 電子契約サーバでの対象データ改ざんの検出 11
6-3-3 電子契約サーバでの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トークン改ざんの検出 11
6-3-4 電子契約サーバでのデジタル署名を使用する方式のタイムスタンプトークン改ざんの検出 11
6-3-5 電子契約サーバでの TSA1 切断時のタイムスタンプ検証 11
6-3-6 電子契約サーバマルチタイムスタンプ検証機能評価結果 11
6-4 時刻トレーサビリティ機能評価 11
6-4-1 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時刻トレーサビリティ確認 11
6-4-2 デジタル署名を使用する方式のタイムスタンプでの時刻トレーサビリティの確認 11
6-4-3 時刻トレーサビリティの確認方法の比較 11
6-5 マルチタイムスタンプデータ容量評価 11
6-6 マルチタイムスタンプ付与及び検証処理時間性能評価 11
6-6-1 処理能力測定に係る装置スペック 11
6-6-2 処理速度測定における処理フロー 11
6-6-3 マルチタイムスタンプ付与及び検証時間測定結果 11
6-6-4 付与時間 11
6-6-5 電子契約サーバでの検証時間 11
6-6-6 VA での検証時間 11
6-7 マルチタイムスタンプ検証操作性評価 11
6-7-1 マルチタイムスタンプ付与 11
6-7-2 マルチタイムスタンプ検証 11
6-7-3 マルチタイムスタンプ付与及び検証の操作性について 11
6-8 検証時確認項目充足性評価 11
6-9 利用者側利便性評価 11
6-10 検証者側利便性評価 11
第 3 章 終わりに 11

1. 成果..... 11
1-1 第三者検証などについて実運用に近い環境に適用し、運用性を評価する..... 11
1-2 VA を介した第三者検証において時刻トレーサビリティの検証も可能とする..... 11
1-3 マルチタイムスタンプにより単一のタイムスタンプの危殆化に対応する..... 11
2. 今後の課題..... 11
2-1 VA を介した第三者検証におけるデータの受け渡し..... 11
2-2 検証用アカウントのアクセス管理..... 11
2-3 マルチタイムスタンプの検証..... 11
付録 実証実験アプケーション操作方法..... 11

図目次

図 1-1　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付与及び検証 3
図 1-2　デジタル署名を使用する方式のタイムスタンプの付与及び検証 4
図 1-3　マルチタイムスタンプの付与及び検証 5
図 1-4　時刻トレーサビリティ 6
図 1-5　VA（検証サーバ）での TSA1 の発行したタイムスタンプの検証 7
図 1-6　VA（検証サーバ）での TSA2 の発行したタイムスタンプの検証 8
図 1-7　電子契約サービス 9
図 2-1　電子契約実証実験処理概要図 11
図 2-2　システム構成概要図 11
図 2-3　マルチタイムスタンプの付与 11
図 2-4　対象データ登録フロー 11
図 2-5　VA を介した検証(電子契約サーバからの対象データと 2 方式のタイムスタンプトークンのダウンロード） 11
図 2-6　VA を介した検証（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） 11
図 2-7　VA を介した検証（デジタル署名を使用する方式のタイムスタンプの検証） 11
図 2-8　VA を介した検証フロー 11
図 2-9　電子契約サーバによる検証 11
図 2-10　電子契約サーバでの検証フロー 11
図 2-11　ダウンロードファイルを格納したフォルダ 11
図 2-12　ダウンロードした対象データの確認 11
図 2-13　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トークン及び対象データの指定 11
図 2-14　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 VA での検証結果 11
図 2-15　デジタル署名を使用する方式のタイムスタンプトークン及び対象データの指定 ... 11
図 2-16　デジタル署名を使用する方式のタイムスタンプの VA での検証結果 11
図 2-17　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トークン及び改ざん対象データの指定 11
図 2-18　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での改ざんデータの検証結果 11
図 2-19　デジタル署名を使用する方式のタイムスタンプトークン及び改ざん対象データの指定 11
図 2-20　デジタル署名を使用する方式のタイムスタンプでの改ざんデータの検証結果 11
図 2-21　改ざん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トークン及び対象データの指定 11
図 2-22　改ざん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での検証結

果 11
図 2-23　改ざんしたデジタル署名を使用する方式のタイムスタンプトークン及び対象データの指定 11
図 2-24　改ざんしたデジタル署名を使用する方式のタイムスタンプでの検証結果 11
図 2-25　切断試験での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トークンの指定 11
図 2-26　TSA1 切断時の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検証のエラー 11
図 2-27　切断試験でのデジタル署名を使用する方式のタイムスタンプトークンの指定 11
図 2-28　TSA1 切断時のデジタル署名を使用する方式のタイムスタンプ検証画面 11
図 2-29　電子契約サーバでの検証結果 11
図 2-30　電子契約サーバでの改ざん文書検証結果 11
図 2-31　改ざん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結果 11
図 2-32　改ざん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結果 11
図 2-33　TSA1 切断時の電子契約サーバでの検証 11
図 2-34　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付与時刻の確認 11
図 2-35　時刻監査レポート（表紙） 11
図 2-36　時刻監査レポートのデジタル署名情報 11
図 2-37　TA-TSA1 の監査情報 11
図 2-38　時刻配信及び監査経路の情報 11
図 2-39　TSA1 に対する監査記録 11
図 2-40　NTA-TA の監査情報 11
図 2-41　TA に対する監査記録 11
図 2-42　配信経路の確認（時刻トレーサビリティ情報スクロール前） 11
図 2-43　誤差情報の確認（時刻トレーサビリティ情報スクロール後） 11
図 2-44　処理能力測定対象装置接続図 11
図 2-45　タイムスタンプ付与シーケンス 11
図 2-46　タイムスタンプ検証シーケンス 11
図 2-47　タイムスタンプ付与時間（全体） 11
図 2-48　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生成時間 11
図 2-49　デジタル署名を使用する方式のタイムスタンプ生成時間 11
図 2-50　タイムスタンプ検証（全体時間） 11
図 2-51　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検証時間 11
図 2-52　デジタル署名を使用する方式のタイムスタンプ検証時間 11
図 2-53　VA 内の検証時間 11
図 2-54　電子契約サーバでのタイムスタンプ取得時間比較 11
図 2-55　VA でのタイムスタンプ検証時間比較 11
図 2-56　電子契約サーバでのタイムスタンプ検証操作時間比較 11

表目次

表 2-1　平成 16 年度課題 10
表 2-2　第三者検証が必要とされる場面 11
表 2-3　事前準備時の分担試験環境準備での役割分担及び実施内容 11
表 2-4　機能確認試験での役割分担 11
表 2-5　実証実験での役割分担 11
表 2-6　実証実験結果整理での役割分担 11
表 2-7　平成 17 年度実証実験評価項目 11
表 2-8　本実証実験の作業日程 11
表 2-9　マルチタイムスタンプ付与機能評価 11
表 2-10　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結果 11
表 2-11　デジタル署名を使用する方式のタイムスタンプの検証結果 11
表 2-12　VA での対象データ改ざんの検出（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）の検証結果 11
表 2-13　VA での対象データ改ざんの検出（デジタル署名を使用する方式のタイムスタンプ）の検証結果 11
表 2-14　VA での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トークン改ざんの検出の検証結果 11
表 2-15　VA でのデジタル署名を使用する方式のタイムスタンプ改ざんの検出の検証結果 11
表 2-16　TSA1 切断時の VA を介してのマルチタイムスタンプ検証結果 11
表 2-17　電子契約サーバでのマルチタイムスタンプの検証結果 11
表 2-18　電子契約サーバでの対象データ改ざん検出の検証結果 11
表 2-19　電子契約サーバでの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改ざん検出の検証結果 11
表 2-20　電子契約サーバでのデジタル署名を使用する方式のタイムスタンプ改ざんの検出の検証結果 11
表 2-21　電子契約サーバでの TSA1 切断時のタイムスタンプ検証 11
表 2-22　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時刻トレーサビリティ確認 11
表 2-23　TSA1 の時刻トレーサビリティ確認結果 11
表 2-24　デジタル署名を使用する方式のタイムスタンプの時刻トレーサビリティ確認 11
表 2-25　TSA2 の時刻トレーサビリティ確認結果 11
表 2-26　時刻トレーサビリティ確認方式の違いによる利用者への影響 11
表 2-27　時刻トレーサビリティ確認方式の違いによる TSA 構築時の影響 11
表 2-28　タイムスタンプトークンファイルサイズ 11
表 2-29　TSA1 スペック 11
表 2-30　TSA2 スペック 11

表 2-31　VA スペック 11
表 2-32　WEB サーバ スペック 11
表 2-33　電子契約サーバ スペック 11
表 2-34　DB サーバ スペック 11
表 2-35　中継サーバ スペック 11
表 2-36　試験端末 スペック 11
表 2-37　タイムスタンプ付与及び検証時間 11
表 2-38　タイムスタンプの付与に必要な操作数及び操作時間 11
表 2-39　VA を介したタイムスタンプ検証 11
表 2-40　電子契約サービスによるタイムスタンプ検証 11
表 2-41　検証時に確認する項目 11
表 2-42　第三者検証の実施による業務効率の改善 11
表 2-43　電子契約サーバによる第三者検証 11
表 2-44　VA を介した第三者検証 11
表 2-45　マルチタイムスタンプの必要性 11
表 2-46　時刻トレーサビリティの必要性 11
表 2-47　第三者検証の実施による業務効率の改善について 11

第1章 はじめに

1. 背景と目的

1-1 課題

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。

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。

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、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。

2. 実証実験の基礎となっている技術

2-1 タイムスタンプについて

2-1-1 概要

タイムスタンプとは、電子化された情報がそれによって示された時間以前に存在していたことを証明し、その時間以降に変更及び改ざんがされていないことを証明する技術である。それを実現する方法として、タイムスタンプは電子化された情報のハッシュ値に対して信頼できる時刻情報を付与している。この時刻情報は、信頼できる第三者機関であるタイムスタンプ局(TSA)の管理する時計を参照して生成される。

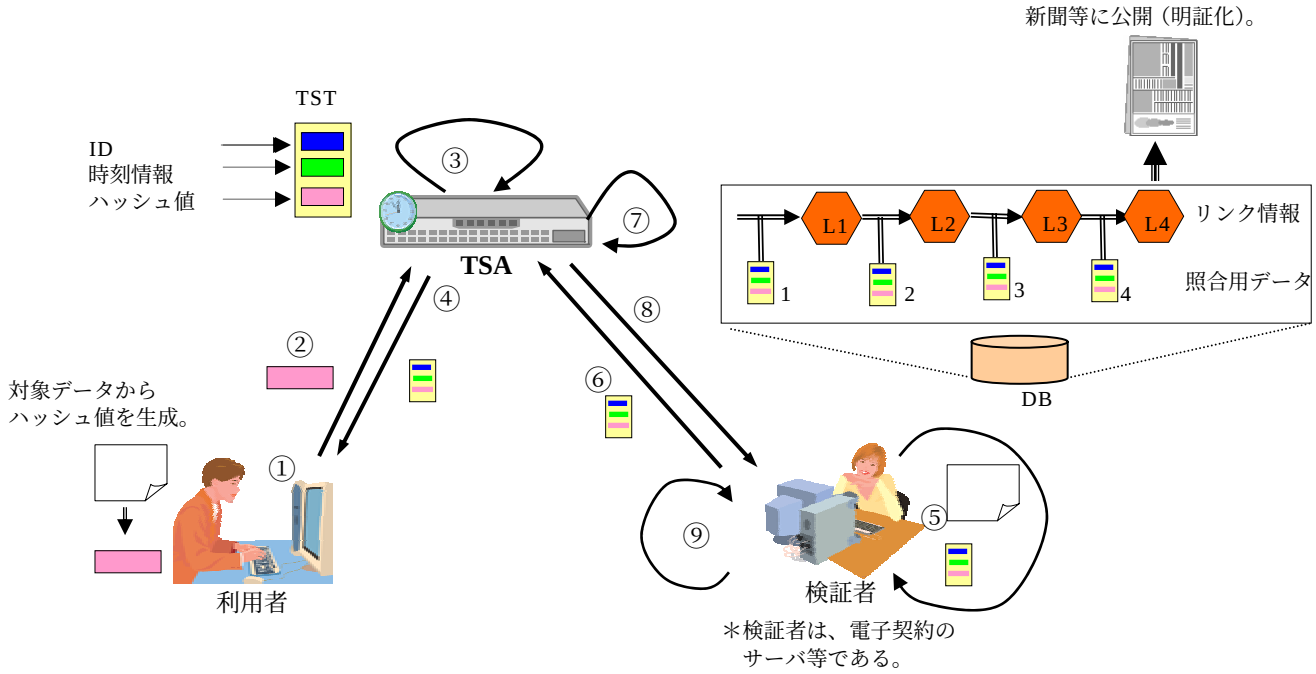
タイムスタンプの時刻情報は、対象としている電子化された情報がその時刻以前に存在していたことを示す証拠と成ることから、正確である必要があり、それを証明できる必要がある。その実現方法として、タイムスタンプ局が信頼できる時刻配信局より時刻の配信を受け、その精度についても時刻配信局より時刻監査を受ける方法があり、これにより時刻の正確性を確保することが可能である。時刻の正確性の確認については、この時刻監査情報を確認することにより、行えるようになっている。

紙文書に比べ改ざんの容易な電子情報を扱う場合において、タイムスタンプは電子文書に係る内容の改ざんや作成時刻の詐称を防止するための重要な技術である。

2-1-2 タイムスタンプの方式

(1) リンク情報を使用するアーカイビング方式

本実証実験では、ISO/IEC18014-2 アーカイビング方式に準拠したタイムスタンプを用いている。タイムスタンプ付与及び検証処理の概要を以下に示す。



－付与－

①利用者は対象データからハッシュ値を生成する。

②利用者は対象データに対するタイムスタンプの付与を TSA に要求する。(対象データのハッシュ値を含む要求を送付)

③TSA はタイムスタンプトークン(TST)の生成、照合用データの登録ならびにリンク情報の作成及び登録を行う。

④TSA は利用者に対し、タイムスタンプトークン(TST)を送付する。

－検証－

⑤検証者はタイムスタンプトークン(TST)に含まれるハッシュ値と対象データから計算したハッシュ値の一致を確認する。

⑥検証者は TSA へタイムスタンプトークン(TST)の情報を送り、タイムスタンプの確認を要求する。

⑦TSA は受信したタイムスタンプトークン(TST)の情報を照合用データと比較する。

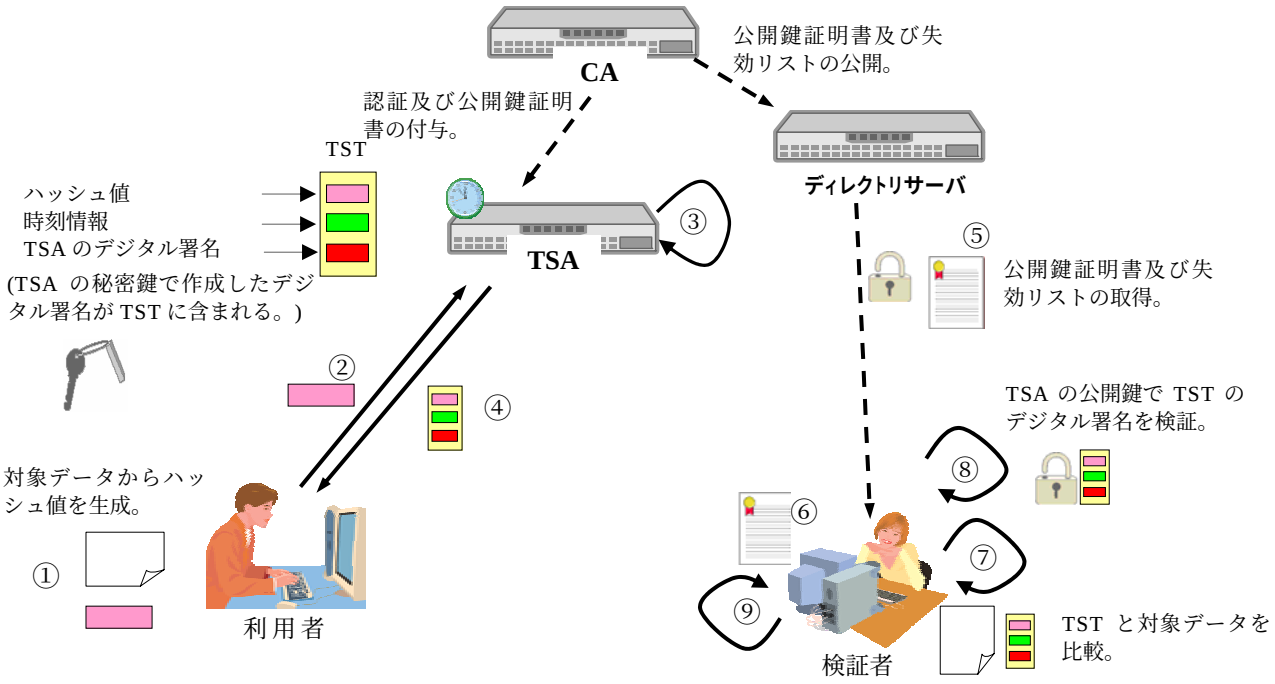
⑧TSA はタイムスタンプトークン(TST)の照合用データとの比較結果を利用者へ送付する。

⑨検証者は非改ざん性及び存在日時の正しさを⑤⑧の結果から判断する。

図 1-1　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付与及び検証

(2) デジタル署名を使用する方式

本実証実験では、RFC3161 に準拠したタイムスタンプを用いている。タイムスタンプ付与及び検証処理の概要を以下に示す。



－付与－

①利用者は対象データのハッシュ値を生成する。

②利用者は対象データに対するタイムスタンプの付与を TSA に要求する(対象データのハッシュ値を含む要求を送付)。

③TSA はハッシュ値及び時刻情報等に対してデジタル署名を付与し、タイムスタンプトークン(TST)の生成を行う。

④TSA は利用者に対し、タイムスタンプトークン(TST)を送付する。

－検証－

⑤検証者は TSA のデジタル署名の検証に必要な公開鍵証明書及び失効リスト(CRL)を取得する。

⑥検証者は TSA の公開鍵証明書を確認する。

⑦検証者はタイムスタンプトークン(TST)に含まれるハッシュ値と対象データから計算したハッシュ値の一致を確認する。

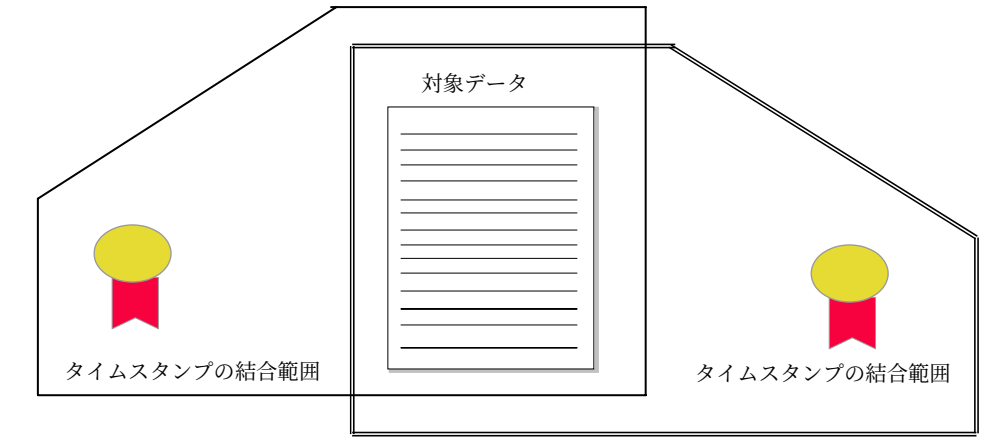
⑧検証者は TSA の公開鍵を用いてタイムスタンプ中のデジタル署名を検証する。

⑨検証者は非改ざん性及び存在日時の正しさを⑦⑧の結果から判断する。

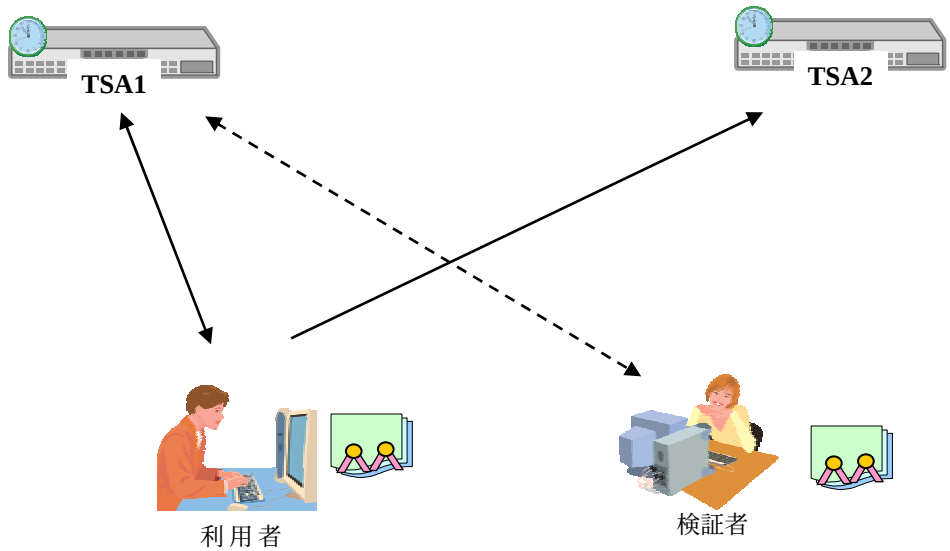
図 1-2　デジタル署名を使用する方式のタイムスタンプの付与及び検証

2-1-3 マルチタイムスタンプについて

本実証実験では、1 つの対象データに対し 2 方式のタイムスタンプの取得を行い、その検証を行う。取得した一方のタイムスタンプは他方の方式とは独立して存在する。そのため一方のタイムスタンプはもう一方の検証結果に影響を受けない。タイムスタンプの取得は、それぞれの TSA に順次アクセスして行う。本実証実験においては、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及びデジタル署名を使用する方式のタイムスタンプを用いる。



TSA1：リンク情報を使用するアーカイビング方式の TSA
TSA2：デジタル署名を使用する方式の TSA



タイムスタンプの取得時には TSA1 及び TSA2 に順次アクセスし、タイムスタンプの取得を行う。

検証時にはどちらか検証可能な方式を選択し、検証する。両方検証可能な場合は、2 方式を順次検証することも可能。

図 1-3　マルチタイムスタンプの付与及び検証

2-2 時刻トレーサビリティについて

タイムスタンプに含まれる時刻情報はその信頼性を確保するために一定の精度を保つ必要がある。時刻同期精度については、信頼できる時刻配信局より時刻配信を受けることにより、高い精度を確保することが可能である。時刻トレーサビリティは、タイムスタンプに係る時刻情報の正確性及びその配信経路の確認を行うための機能である。

本実証実験においては、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の時刻トレーサビリティの確認では、TA の発行する時刻監査レポートを確認し、デジタル署名を使用する方式のタイムスタンプの時刻トレーサビリティの確認では、タイムスタンプトークンに含まれる時刻監査証明書を確認する。時刻監査レポート及び時刻監査証明書には時刻配信元である国家時刻配信局(NTA）から TSA までの配信経路毎の時刻監査情報が含まれており、タイムスタンプに係る時刻情報の日本標準時との誤差を確認することができる。

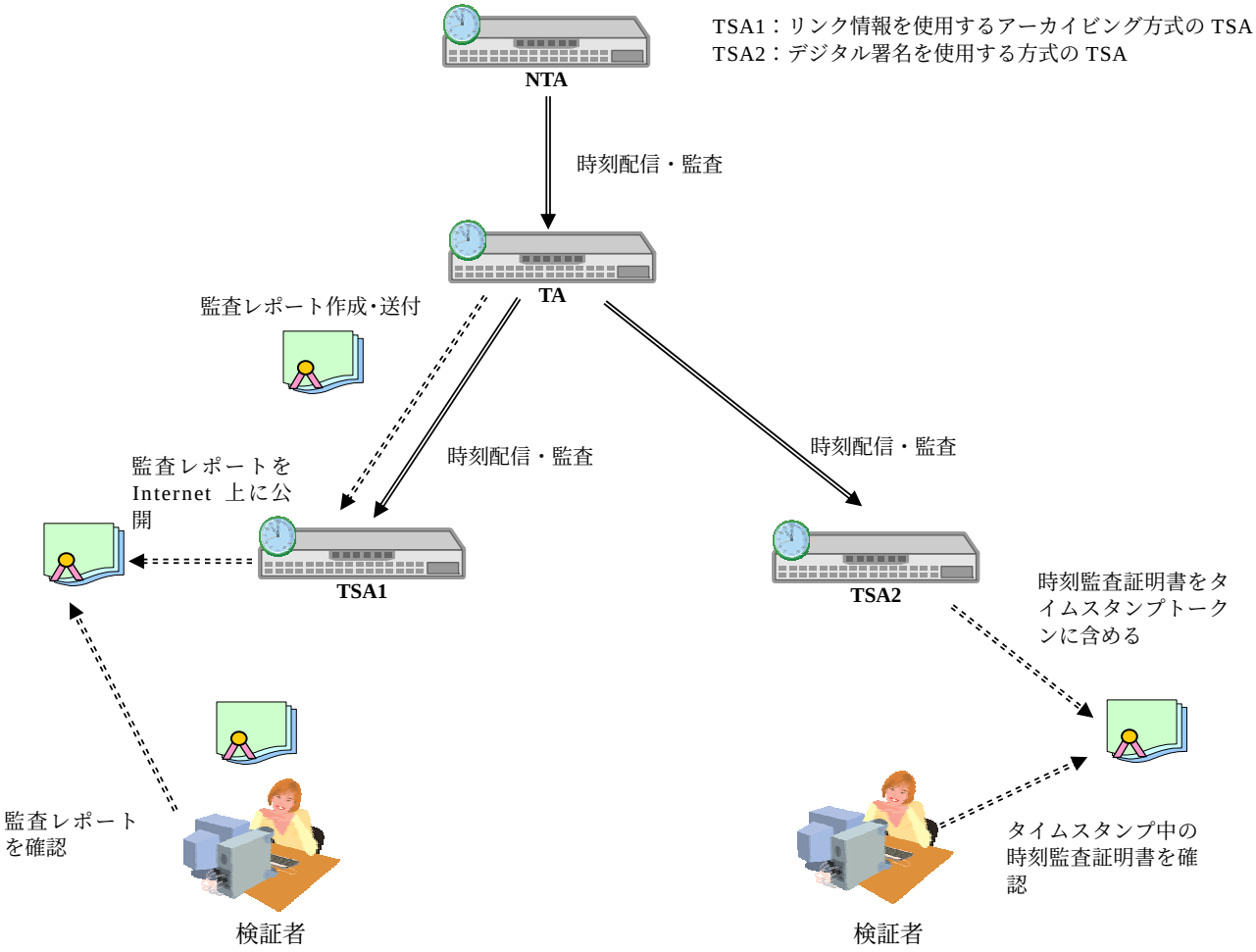


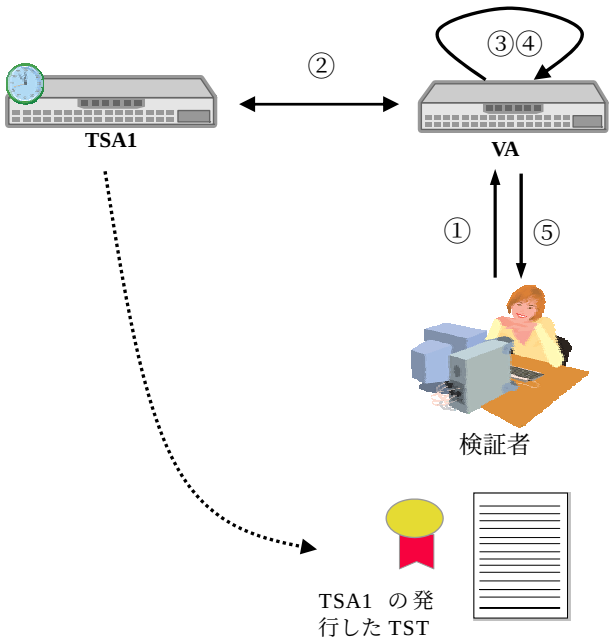
図 1-4　時刻トレーサビリティ

2-3 VA（検証サーバ）について

VA は検証者からの検証要求に応じ、検証者の代わりにタイムスタンプの検証を行う。そのため、必要に応じて TSA へのアクセスや CA の発行する公開鍵証明書及び失効リスト(CRL)の取り込みを行い、タイムスタンプの正当性の確認を行う。

VA がタイムスタンプの検証を検証者に代わって実施するため、VA を利用することにより検証者は容易に検証結果を得ることができる。本実証実験で用いる VA 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及びデジタル署名を使用する方式のタイムスタンプに対応しており、両方式の検証が可能である。またこの VA は、タイムスタンプの検証に続いて、タイムスタンプに係る時刻情報の時刻トレーサビリティの確認を行う機能を持つ。

以下に、検証者が TSA1 の発行したリンク情報を使用したアーカイビング方式のタイムスタンプの検証を行う際のフローを示す。

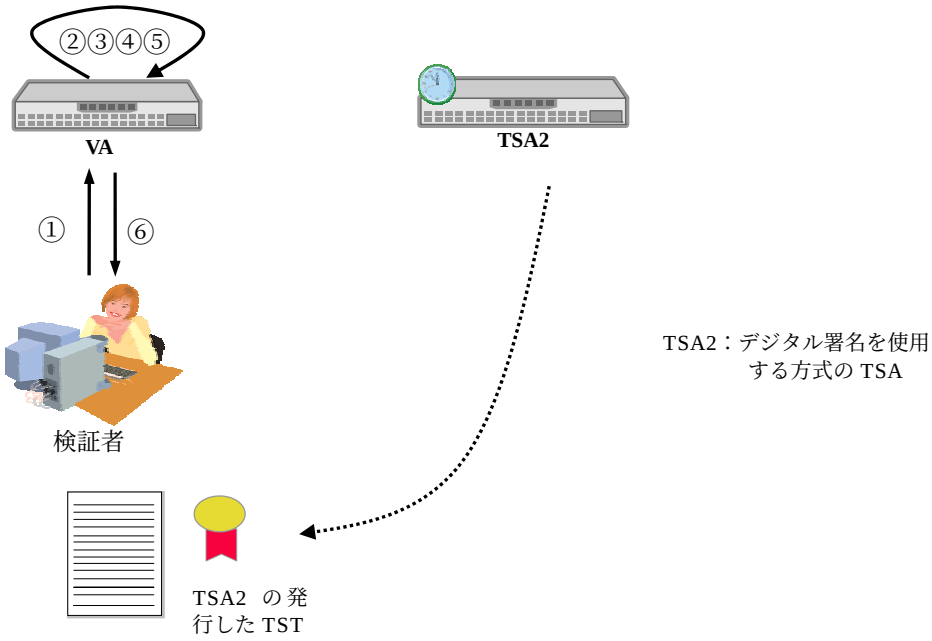


TSA1：リンク情報を使用するアーカイビング方式の TSA

① 利用者は対象データと TSA1 の発行したタイムスタンプトークンの組合せを VA に送付する。
② VA はリンク情報を使用するアーカインビング方式のタイムスタンプを受け取った場合には、タイムスタンプの正当性を TSA1 に確認する。
③ VA は対象データから計算したハッシュ値とタイムスタンプトークンに含まれるハッシュ値の一致を確認する。
④ VA は非改ざん性及び存在日時の正しさを②及び③の結果から判断する。
⑤ VA は検証結果及び時刻トレーサビリティの確認のための時刻監査レポートの URL を検証者に通知する。

図 1-5　VA（検証サーバ）での TSA1 の発行したタイムスタンプの検証

以下に、検証者が TSA2 の発行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を行う際のフローを示す。



① 利用者は対象データとタイムスタンプトークンの組合せを VA に送付する。
② VA は TSA2 の発行したデジタル署名を使用する方式のタイムスタンプを受け取った場合には、タイムスタンプトークン中のデジタル署名を検証し正当性の確認を行う。
③ VA は対象データから計算したハッシュ値とタイムスタンプトークンに含まれるハッシュ値の一致を確認する。
④ VA は非改ざん性及び存在日時の正しさを②及び③の結果から判断する。
⑤ VA は時刻トレーサビリティの確認のため、タイムスタンプ中の時刻監査証明書の正当性を検証し、時刻監査情報を取り出す。
⑥ VA は検証結果及び時刻トレーサビリティの確認のための時刻誤差情報及び時刻配信経路情報を検証者に通知する。

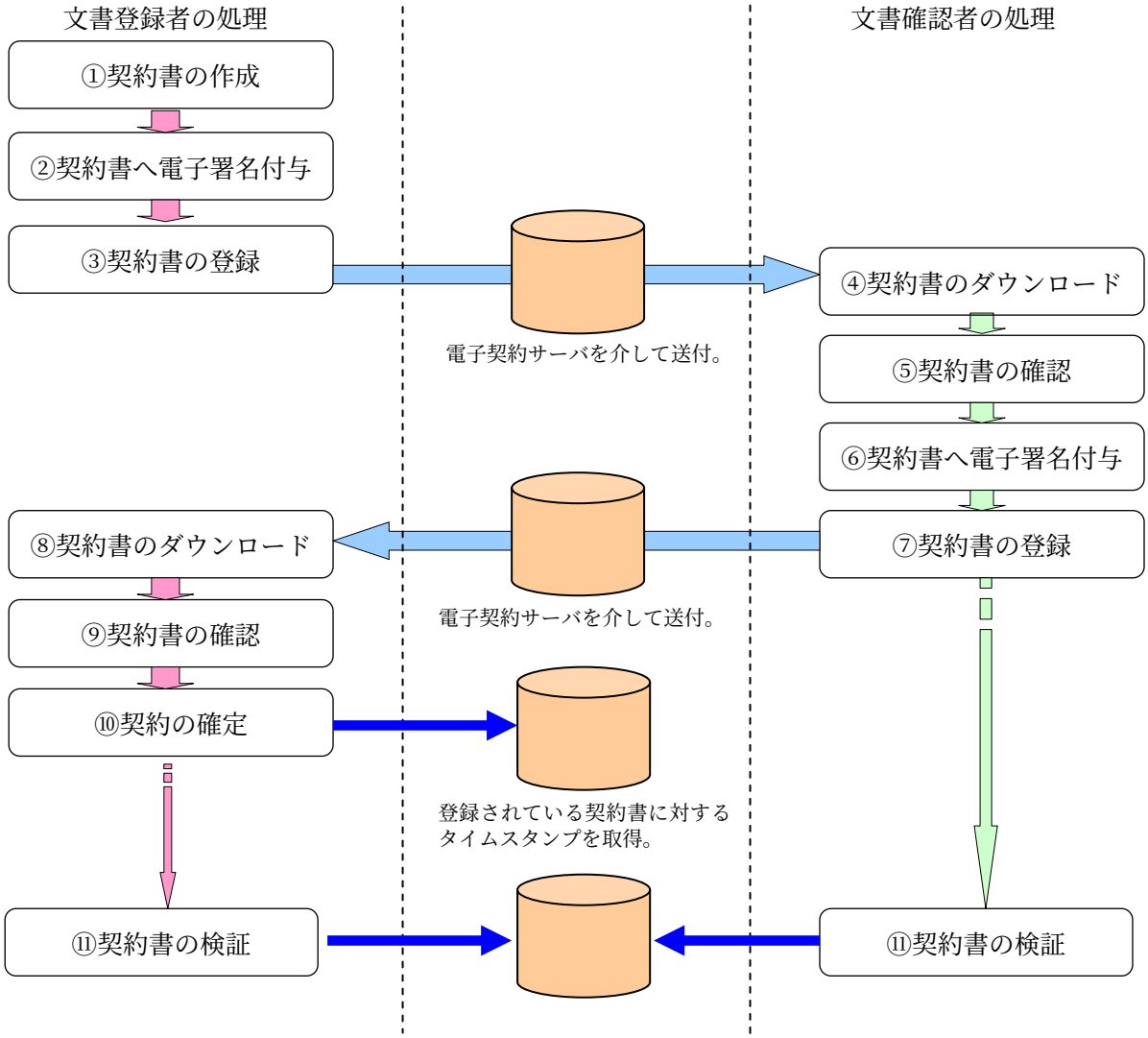
図 1-6　VA（検証サーバ）での TSA2 の発行したタイムスタンプの検証

2-4 電子契約サービスについて

電子契約サービスとは、企業間の契約書を電子的にやり取りするためのサービスである。2001年４月の IT 書面一括法によって契約文書の電子化が認められるようになったことを機に、従来署名捺印を行った書面の交換によって契約を行っていたものを電子データにて行うことができるようになった。

電子契約サービスは企業間での電子化された契約書の交換、保存及び検証をサポートするものである。今回実証実験で使用した電子契約サービスは、電子化された書面に対し、両社の契約担当者によるデジタル署名を付与し、契約が確定した際に自動的にタイムスタンプの取得を行っている。その後、取得したタイムスタンプは電子契約サーバで保存される。電子契約サービスの利用者は、保存されている契約書とタイムスタンプの検証を行うことができる。

契約書の登録、確認及び確定（タイムスタンプの取得）の操作フローを以下に示す。



※本図では、契約書の作成及び確定を行う者を文書登録者、契約書の確認を行うものを文書確認者と言う。

図 1-7　電子契約サービス

第2章 実証実験の内容

1. 実証実験の概要

1-1 実証実験の対象とする課題と目的

平成 16 年度の電子契約実証実験において、リンク情報を使用するアーカイビング方式の TSA 及びデジタル署名を使用する方式の TSA の時計が日本標準時と同期していること、VA にて複数方式のタイムスタンプの検証が行えることを確認した。しかし平成 16 年度の実証実験では、内部での機能確認を行ったのみであり実環境に即した検証が行えていない。また、検証者側でタイムスタンプトークンに含まれる時刻情報の配信経路と誤差の確認も実現できていなかった。

さらに、タイムスタンプを業務で用いる場合には、付与対象の電子文書の保存期間の間タイムスタンプの効力を確保しなければならない場合があるが、万一タイムスタンプが危殆化した場合にも効力を確保するための対策が十分考慮されていないという課題も見つかっている。

そこで本年度の実証実験では、平成 16 年度の実証実験等において課題となった事項の解決を目指す。

課題と対処事項について以下の表 2-1　にまとめる。

表 2-1　平成 16 年度課題

課題事項	対処事項
第三者検証等について実運用時の運用性が評価できていない。	第三者検証等について実運用に近い環境に適用し、運用性を評価する。
検証者による TST に含まれる時刻情報の正確性及び信頼性の確認ができていない。	タイムスタンプ検証において、時刻トレーサビリティの検証も可能とする。
タイムスタンプの危殆化に対応できていない。	マルチタイムスタンプにより単一のタイムスタンプの危殆化に対応する。

今年度の実証実験は、タイムスタンププラットフォームを電子契約サービスへ適用し、表 2-1 に記載されている各々の対処事項について、以下の評価を実施することを目的とする。

① 第三者検証の実運用に近い環境での評価

試験端末をインターネット経由で電子契約サーバ及び VA に接続して検証を実施し、実運用上、第三者検証が必要とされる場面を想定しての運用性を評価する。また実際の業務において電子契約サービスを使用している企業に協力を求め、その担当者が検証を実施した際の運用性の評価を得る。第三者検証のフローに関しては、「VA を介した複数方式タイムスタンプの検証」及び「検証用アカウントを用いた電子契約サーバでの検証」の 2 方式について検証を行い、その運用性の評価を得る。

本評価項目の実用上のニーズについて、建設業界を例として、実際の業務担当者へのヒアリング等を参考に、第三者検証が必要とされる場面を、以下の表 2-2 に示す。

表 2-2　第三者検証が必要とされる場面

№	想定場面	利用者	検証者	第三者検証による確認方法の１例
1	公共入札における施工体制台帳の提出	建設会社の公共入札の担当者	府省・地方公共団体等における公共入札担当者	公共入札への応札を想定し、建設会社の公共入札の担当者が請負契約に関する電子契約文書をタイムスタンプごと提出し、府省及び地方公共団体等における公共入札担当者がタイムスタンプの検証等により電子契約文書の真正性を確認する。
2	公共工事に係る経営事項審査	建設会社の経営事項審査の対応者	府省・地方公共団体等における経営事項審査担当者	公共工事に係る経営事項審査を想定し、建設会社の経営事項審査の対応者が審査の対象となる電子契約文書をタイムスタンプごと提出し、府省及び地方公共団体等における経営事項審査担当者がタイムスタンプの検証等により電子契約文書の真正性を確認する。
3	施工契約を元にした融資	建設会社の発注先の資金調達担当者	銀行等の金融機関の融資担当者	工事の受注時における資金調達を想定し、建設会社の発注先の資金調達担当者が施工契約に係る電子契約文書をタイムスタンプごと提出し、銀行等の金融機関の融資担当者がタイムスタンプの検証等により電子契約文書の真正性を確認する。
4	国税庁による監査	建設会社の経理担当者等の国税監査対応者	国税庁の監査担当者	国税庁による監査を想定し、建設会社の経理担当者等の国税監査対応者が監査の対象となる電子契約文書をタイムスタンプごと提出し、国税庁の監査担当者がタイムスタンプの検証等により電子契約文書の真正性を確認する。

② 時刻トレーサビリティの検証

VA を使用しての第三者検証において、対象データに付与されたタイムスタンプの時刻トレーサビリティの確認が行えることを検証する。

本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及びデジタル署名を使用する方式の 2 方式のタイムスタンプを使用するが、それぞれ時刻トレーサビリティの確認が行えることを検証する。

③ マルチタイムスタンプの対応

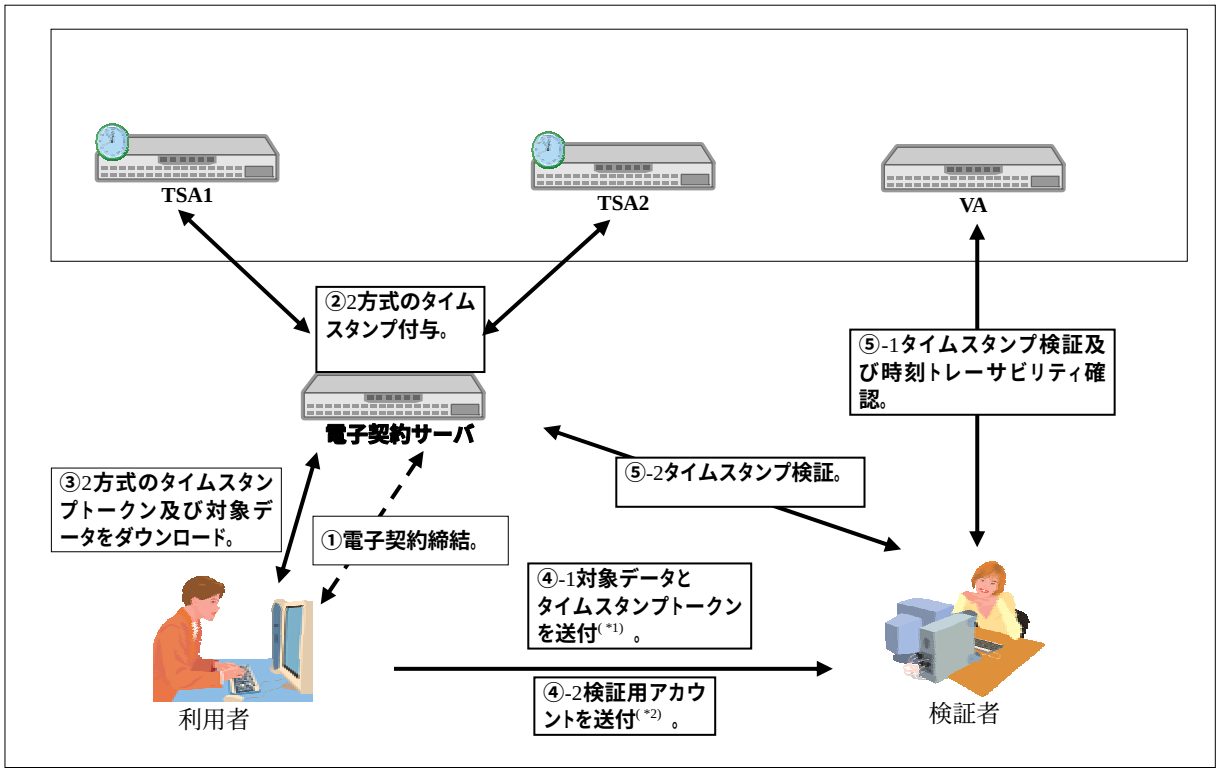
対象データに 1 方式のタイムスタンプのみを付与している場合、そのタイムスタンプが危殆化した際に対象データの非改ざん性及び存在時刻を証明できなくなる。このような場合でも、別の方式の有効なタイムスタンプを用いて対象データの非改ざん性及び存在時刻を証明可能とするため、1 つの対象データに対し複数方式のタイムスタンプを付与するマルチタイムスタンプ機能を検証する。

1-2 実証実験での確認概要

本実証実験では電子契約サービスでのタイムスタンプの利用を想定し、その利用者が電子契約サーバに登録されている対象データを確定した際にタイムスタンプが取得され、対象データとタイムスタンプの検証を第三者が行えることの確認を行う。

利用者は電子契約サーバに登録された対象データに対し、「第 1 章 2 実証実験の基礎となっている技術」で説明したリンク情報を使用するアーカイビング方式及びデジタル署名を使用する方式の 2 方式のタイムスタンプを取得する。2 方式のタイムスタンプが付与された対象データについて、第三者が VA または電子契約サーバを利用して検証する。VA での検証時には合わせて時刻トレーサビリティの確認を行う。

本実証実験の概要図を以下に示す。



*1 VA での第三者検証を実施するため
*2 電子契約サーバでの第三者検証を実施するため

図 2-1　電子契約実証実験処理概要図

2. 実証実験の体制

2-1 試験環境準備での分担及び実施内容

試験準備においては、本実証実験でタイムスタンププラットフォーム(TSPF）に接続する電子契約サーバ、利用者端末及び検証者端末の設定等を行った。

作業時の分担を以下の表に示す。

表 2-3　事前準備時の分担試験環境準備での役割分担及び実施内容

№	役割	担当
1	CA の準備	日立製作所
2	NTA の準備	セイコーインスツル
3	TA の準備	セイコーインスツル
4	VA の準備	日立製作所
5	TSA1（リンク情報を使用するアーカイビング方式）の準備	NTT データ
6	TSA2（デジタル署名を使用する方式）の準備	セイコーインスツル
7	電子契約サービス及びアプリケーションの準備	NTT データ
8	電子契約サービス接続環境（NTT データ内）の準備	NTT データ
9	電子契約サービス接続環境（大成建設内）の準備	大成建設

2-2 機能確認試験での担務分担

12 月に実施した機能確認試験では、本実証実験において機能追加したマルチタイムスタンプの付与、VA を使用しての検証及び電子契約サーバを使用しての検証の機能確認ならびに各操作段階での性能測定を実施した。

作業時の分担を以下の表に示す。

表 2-4　機能確認試験での役割分担

№	役割	担当
1	試験計画及び項目／手順書の作成	NTT データ
2	CA の運用	日立製作所
3	NTA の運用	セイコーインスツル
4	TA の運用、時刻監査レポートの発行	セイコーインスツル
5	VA の運用	日立製作所
6	TSA1（リンク情報を使用するアーカイビング方式）の運用	NTT データ
7	TSA2（デジタル署名を使用する方式）の運用	セイコーインスツル
8	電子契約サービスの運用、ログの取得	NTT データ
9	機能確認試験の実施	NTT データ

2-3 実証実験での役割分担

1 月に実施した実証実験では、実運用を踏まえたフローについて試験を実施し、運用性についての評価を行った。そのため、第三者検証を実際の利用者と同等の作業場所に設置し、その操作性及び利便性についての評価を行った。

作業時の分担を以下の表に示す。

表 2-5　実証実験での役割分担

№	役割	担当
1	CA の運用	日立製作所
2	NTA の運用	セイコーインスツル
3	TA の運用、時刻監査レポートの発行	セイコーインスツル
4	VA の運用	日立製作所
5	TSA1（リンク情報を使用するアーカイビング方式）の運用	NTT データ
6	TSA2（デジタル署名を使用する方式）の運用	セイコーインスツル
7	電子契約サービスの運用、ログの取得	NTT データ
8	試験データの登録	NTT データ
9	ユーザビリティの確認としての試験実施（実運用者としての評価）	大成建設及び NTT データ

2-4 実験結果整理時の分担

機能確認試験では、処理速度及びデータ容量についての測定を実施し、実証実験ではユーザビリティの確認を行った。これらの作業が終了した後の実証実験の結果整理では、試験時に出力されたログを収集するとともに、電子契約サービス利用者によるユーザビリティの評価を行った。また、試験終了後に出力されたログ及び評価の解析も行った。

作業時の分担を以下の表に示す。

表 2-6　実証実験結果整理での役割分担

№	役割	担当
1	VA サーバのログ収集	日立製作所
2	電子契約サーバのログ収集	NTT データ
3	ユーザビリティの評価（ヒアリングシート記入）	大成建設
4	実証実験結果の収集及び整理	NTT データ

3. 実験項目

本章では実証実験の評価項目とその評価方法に関して記述する。

表 2-7　平成 17 年度実証実験評価項目

№	項目名	評価項目	評価目的	評価方法
1	マルチタイムスタンプ付与機能評価	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。	タイムスタンプの危殆化に対応するため、2 方式のタイムスタンプが対象文書に付与されることを確認。また VA を介しての第三者検証を実施するため、対象データ及び 2 方式のタイムスタンプトークンを利用者が取得できることを確認。	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 マルチタイムスタンプ検証機能評価	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 2 方式のタイムスタンプの検証が可能であることを確認。	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	電子契約サーバマルチタイムスタンプ検証機能評価	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。	電子契約サーバを使用して 2 方式のタイムスタンプの検証をそれぞれ行えることを確認。	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	時刻トレー	VA での検証にお	VA での検証でタイムスタ	VA クライアントを使用し

№	項目名	評価項目	評価目的	評価方法
	サビリティ機能評価	いて、時刻トレーサビリティが確認できること。	ンプ時刻の誤差及び配信経路の検証が行えることを確認。	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データ容量評価	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。	マルチタイムスタンプとした場合に、電子契約サーバ、利用者及び検証者が取り扱うデータの総容量について、単一タイムスタンプの場合との差異を比較。	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付与及び検証処理時間性能評価	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処理時間について、単一のタイムスタンプの場合と比較。	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検証操作性評価	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数及び操作時間について、単一タイムスタンプの場合と比較。	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	検証時確認項目充足性評価	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。	検証時に表示すべき情報及びチェックすべき項目のそれぞれの第三者検証フローにおける充足性の確認。	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	利用者側利便性評価	2 種類のフローにおける利用者側での利便性。	実際の業務における電子契約サービス利用者による、本実証実験で実現した利用者向け機能の利便性評価。	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	検証者側利便性評価	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（もしくは、データの保持、参照方法）の利便性。	実際の業務における電子契約サービス利用者による、本実証実験で実現した検証者向け機能の利便性評価。	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。

4. 実証実験構成

本実証実験において使用する主要装置間の接続を、以下に示す。

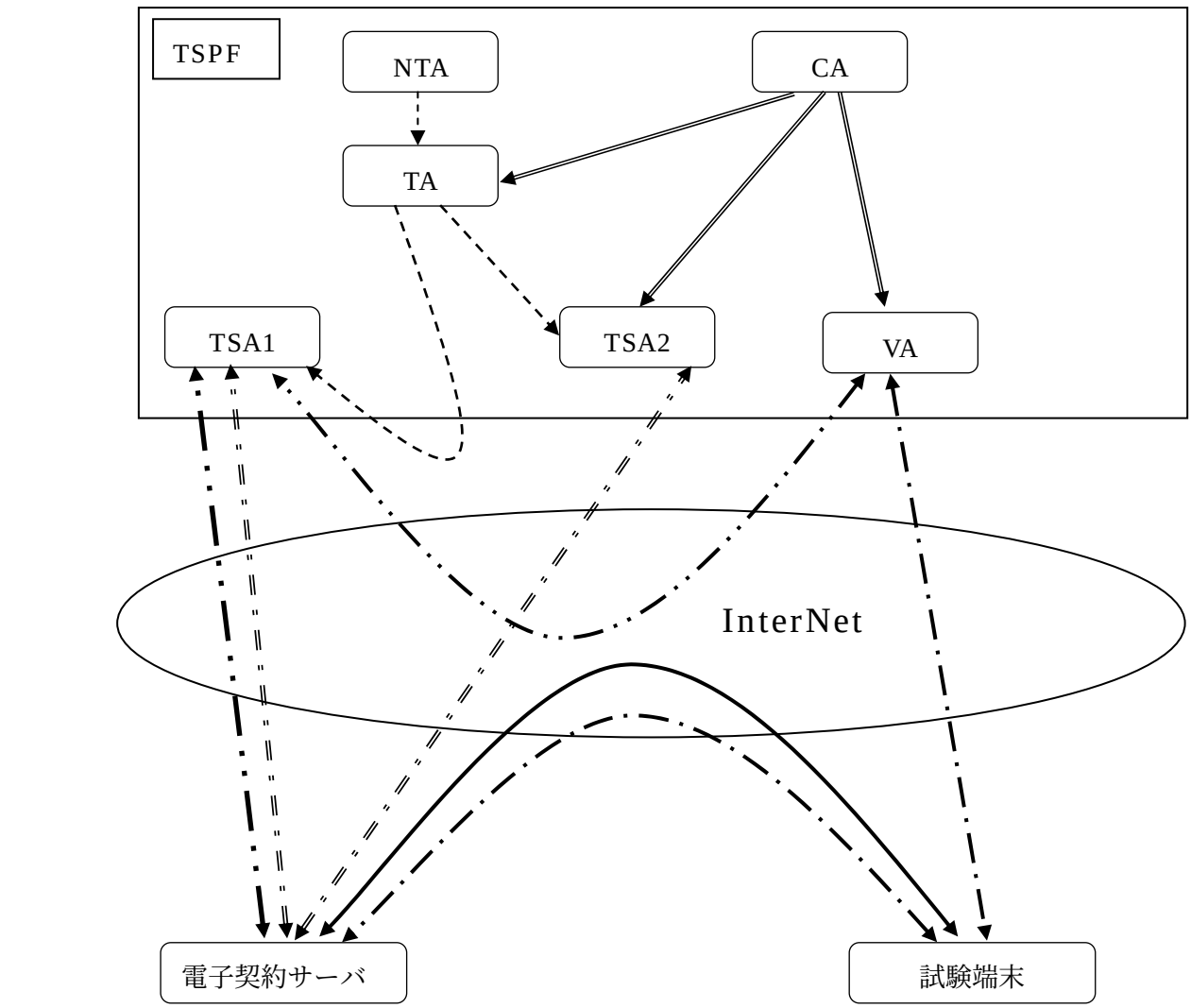


図 2-2　システム構成概要図

5. 実証実験処理の手順

本実証実験の作業日程、作業手順及び試験者が使用するアプリケーションの使用方法を以下に示す。

5-1 作業日程

以下の日程にて実証実験を実施し、評価を行った。

表 2-8　本実証実験の作業日程

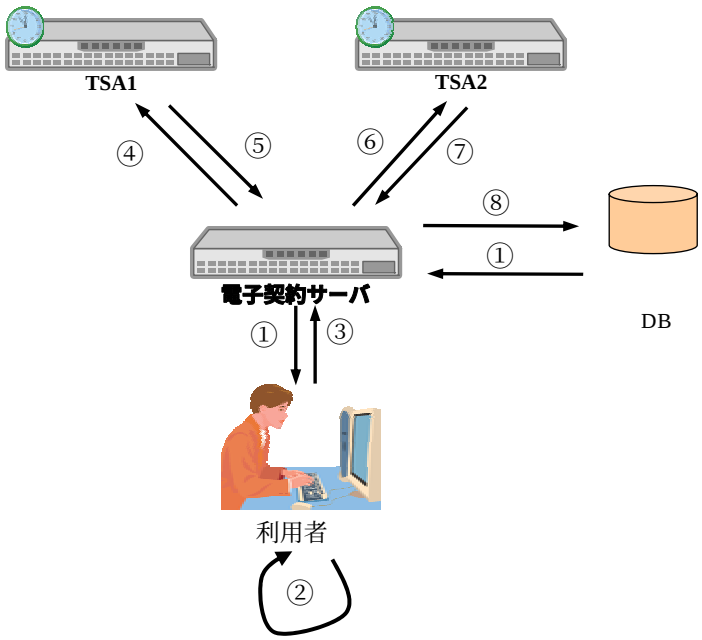
	日付	工程	作業内容
1	11 月 25 日（金）	事前準備	電子契約サービスと TSPF の接続の確認。
2	12 月 1 日（木）	機能確認実施	マルチタイムスタンプ付与。
3	12 月 1 日（木）		VA でのマルチタイムスタンプが付与された対象データの検証。
4	12 月 1 日（木）		電子契約サーバでのマルチタイムスタンプが付与された対象データの検証。
5	12 月 21 日（水）		VA でのタイムスタンプ検証時の時刻トレーサビリティの確認。
6	12 月 7 日（水）		VA での改ざんしたタイムスタンプトークンもしくは対象データを使用した検証。
7	12 月 7 日（水）		電子契約サーバでの改ざんしたタイムスタンプトークンもしくは対象データを使用した検証。
8	12 月 13 日（火）		性能測定（操作時間、処理時間及びファイルサイズ）。
9	1 月 18 日（水）	運用性確認試験	実運用者によるユーザビリティ確認。
9	12 月 19 日（月）	実験結果整理	電子契約サーバ及び VA のログの収集。
10	1 月 19 日（木）～2 月 28 日（火）		実証実験結果の整理及び結果の解析。

5-2 マルチタイムスタンプの付与手順

マルチタイムスタンプの取得は、電子契約サーバより行う。利用者は事前に電子契約サーバに対象データを登録する。そして契約の確定時に電子契約サーバはリンク情報を使用するアーカイビング方式の TSA1 及びデジタル署名を使用する方式の TSA2 にアクセスし、それぞれの方式のタイムスタンプの付与を受け、その後 2 方式のタイムスタンプを対象データと共に保存する。

このように本実証実験では、電子契約サーバが 2 方式のタイムスタンプを取得するため、各 TSA に対してタイムスタンプの付与要求を行っている。

TSA1：リンク情報を使用するアーカイビング方式の TSA
TSA2：デジタル署名を使用する方式の TSA



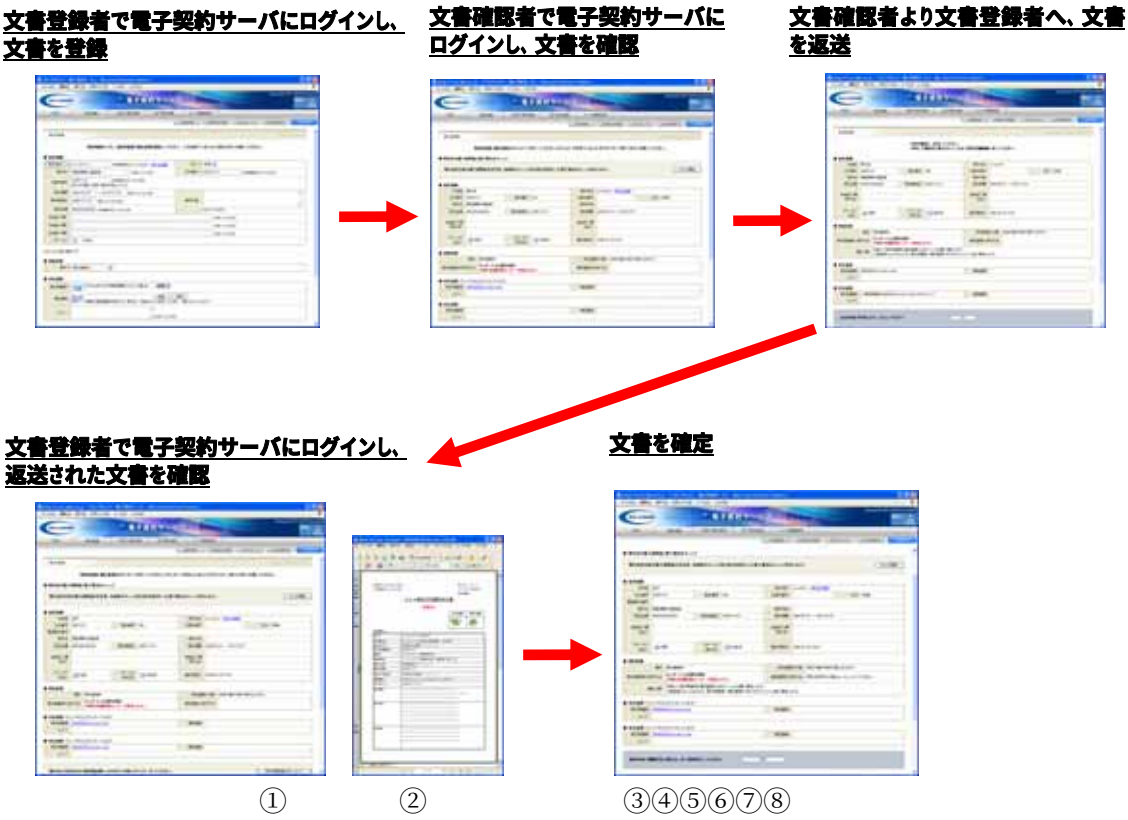
①利用者は電子契約サーバに登録されている対象データをダウンロードする。
②利用者は対象データ（契約書）を確認する。
③利用者は電子契約サーバに登録されている対象データの確定を行う。
④電子契約サーバは TSA1 に対象データに対するタイムスタンプの付与を要求する。
⑤TSA1 はタイムスタンプトークンを生成し、電子契約サーバに送付する。
⑥電子契約サーバは TSA2 に対象データに対するタイムスタンプの付与を要求する。
⑦TSA2 はタイムスタンプトークンを生成し、電子契約サーバに送付する。
⑧電子契約サーバは両方式のタイムスタンプトークンを対象データと共に保存する。

※ 図にて①が DB から電子契約サーバへ向かう線及び電子契約サーバから利用者へ向かう線に付与されているのは、対象データのダウンロードを行う際、DB からの対象データの取り出し及び利用者への送付が一連の処理で行われるため。

図 2-3　マルチタイムスタンプの付与

以下に、実証実験で使用する電子契約サービスの対象データ登録時の画面遷移を示す。

操作の詳細については、付録「実証実験操作説明書（マルチタイムスタンプ付与－ダウンロード）」を参照すること。



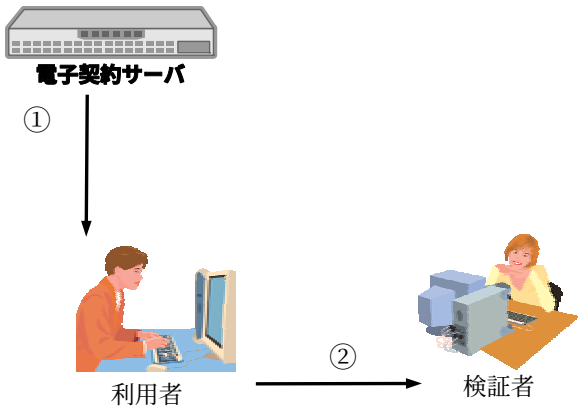
※図中の①～⑧の番号は「図 2-3　マルチタイムスタンプの付与」の処理番号に対応している。

図 2-4　対象データ登録フロー

5-3 VA を介した検証手順

検証者が対象データとタイムスタンプトークンを VA に送り、タイムスタンプの検証と時刻トレーサビリティの確認を実施するフローである。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及びデジタル署名を使用する方式のタイムスタンプの検証を個別に実施する。

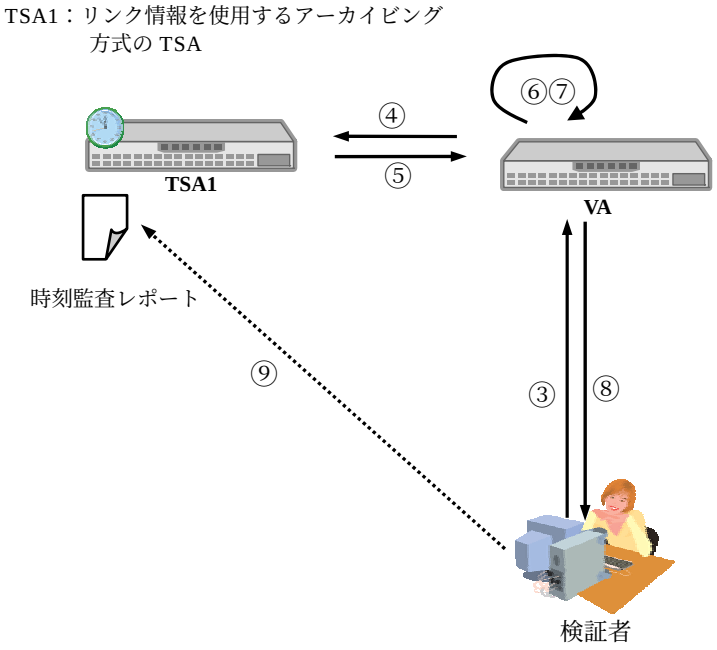
以下に、利用者が対象データとタイムスタンプトークンを電子契約サーバよりダウンロードし、検証者に送付するフローを示す。



①利用者は 2 方式のタイムスタンプトークン及び対象データを電子契約サーバよりダウンロードする。
②利用者は 2 方式のタイムスタンプトークン及び対象データを検証者へ送付する。

図 2-5　VA を介した検証(電子契約サーバからの対象データと 2 方式のタイムスタンプトークンのダウンロード)

以下に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 VA を介した検証のフローを示す。



－検証者によるタイムスタンプの検証－

③検証者は、VA に対象データと TSA1 が発行したタイムスタンプトークンを送付する。

④VA は TSA1 にタイムスタンプトークンの情報を送り、タイムスタンプの正当性の確認を依頼する。

⑤TSA1 は、タイムスタンプの正当性を確認し、その結果を VA に通知する。

⑥VA はタイムスタンプトークン内のハッシュ値と対象データから計算したハッシュ値の比較を行う。

⑦VA は⑤⑥の結果から、対象データの非改ざん性及び存在時刻の正しさを判断する。

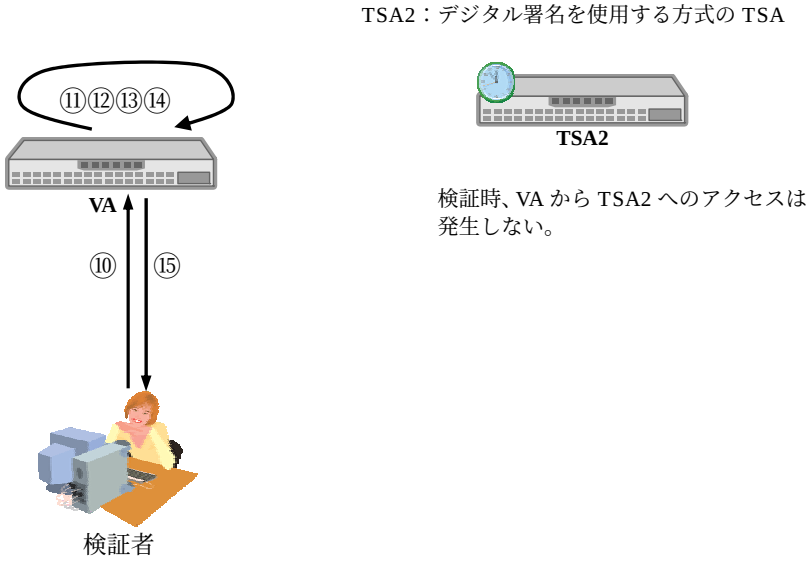
⑧VA はタイムスタンプの検証結果及び時刻トレーサビリティの確認のための時刻監査レポートの URL を検証者へ通知する。

⑨検証者は時刻トレーサビリティの確認のため、ブラウザにて時刻監査レポートを参照する。

※時刻監査レポート参照先の URL は VA に設定されている。

図 2-6　VA を介した検証（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）

以下にデジタル署名を使用する方式のタイムスタンプの VA を介した検証のフローを示す。



－検証者によるタイムスタンプの検証－

⑩検証者は、VA に対象データと TSA2 が発行したタイムスタンプトークンを送付する。

⑪VA はタイムスタンプトークン内の TSA2 のデジタル署名を検証し、正当性を確認する。

⑫VA はタイムスタンプトークン内のハッシュ値と対象データから計算したハッシュ値を比較する。

⑬VA は⑪⑫の結果から、対象データの非改ざん性及び存在時刻を判断する。

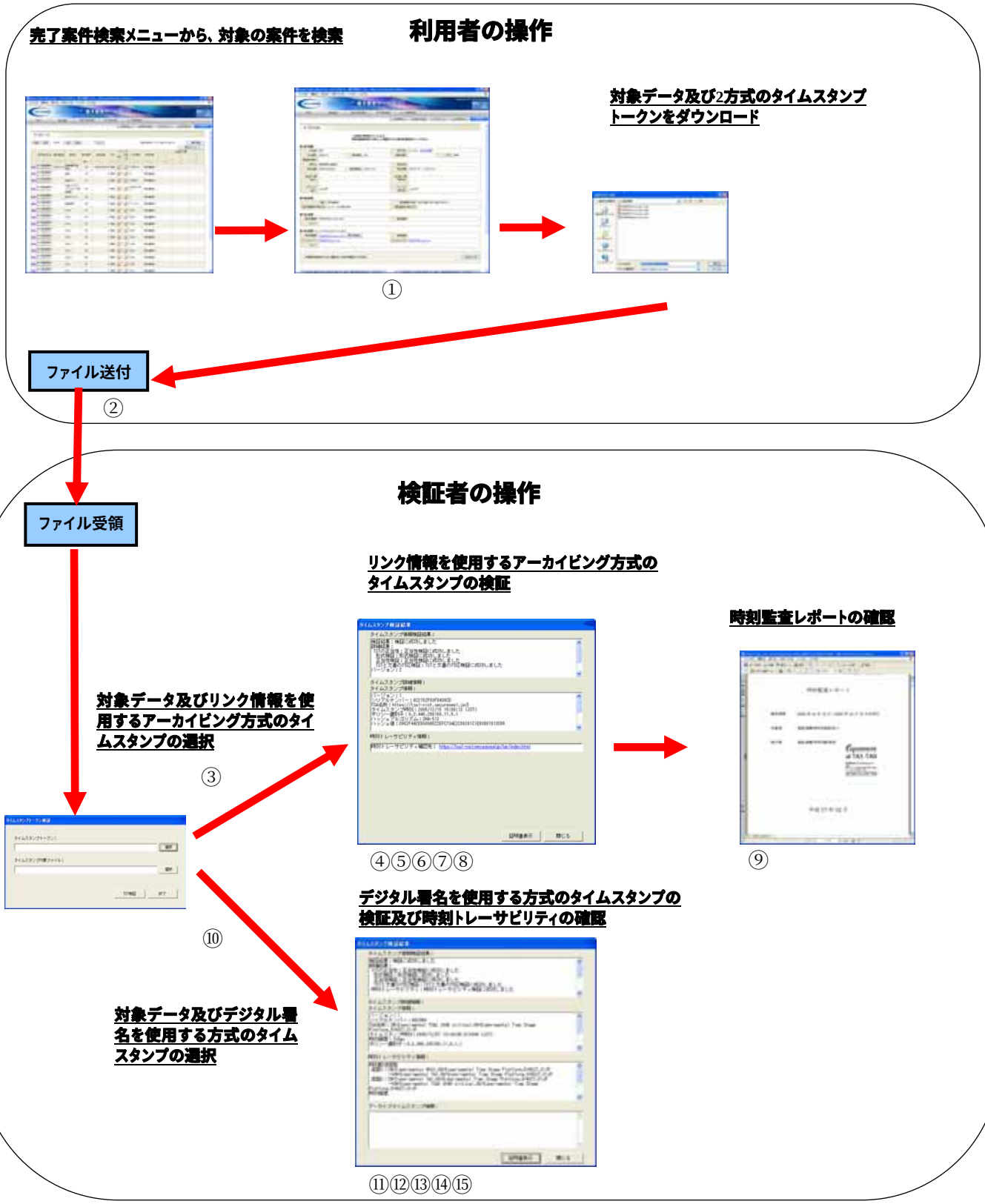
⑭VA は時刻トレーサビリティの確認のため、タイムスタンプ中の時刻監査証明書の正当性を検証し、時刻監査情報を取り出す。

⑮VA はタイムスタンプの検証結果及び時刻トレーサビリティの確認結果を検証者へ通知する。

図 2-7　VA を介した検証（デジタル署名を使用する方式のタイムスタンプの検証）

以下に、実証実験で使用する VA を介した検証フローの画面遷移を示す。

操作の詳細については、付録「実証実験操作説明書（VA クライアント操作説明書)」を参照すること。

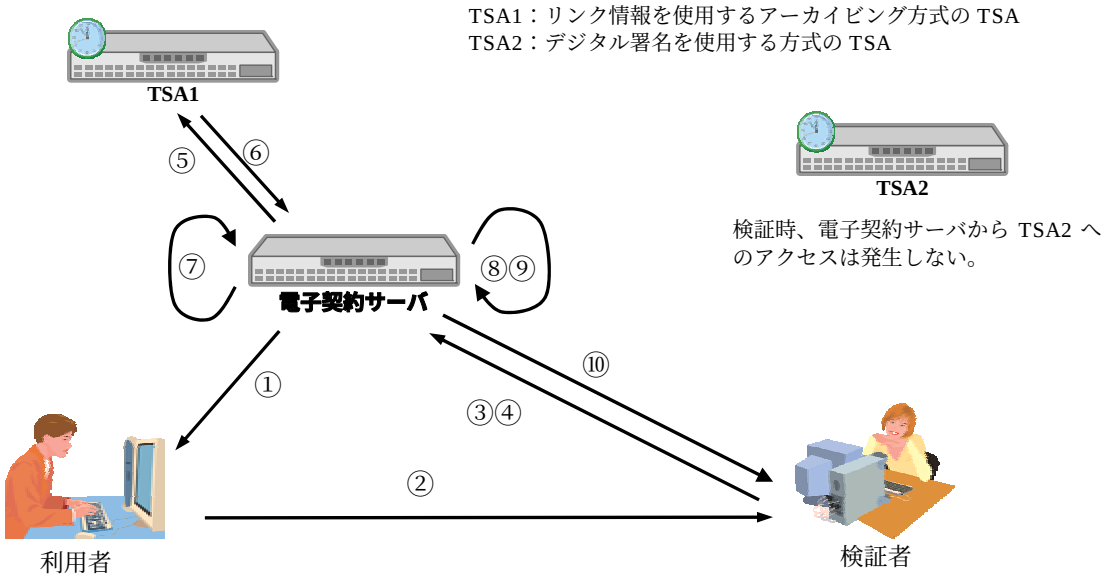


※図中の①～⑮の番号は図 2-5、図 2-6 及び図 2-7 の処理番号に対応している。

図 2-8　VA を介した検証フロー

5-4 電子契約サーバによる検証手順

検証者が利用者から通知された検証用アカウントにより電子契約サーバにログインし、保管されている対象データ及びタイムスタンプトークンの検証を行うフローである。そのため、VA を使用した第三者検証と異なり、利用者から検証者へ対象データ及びタイムスタンプトークンを送る必要がない。



－利用者側の処理－

①利用者は電子契約サーバより検証用アカウントを取得する。

②利用者は検証用アカウントを検証者に通知する。

－検証者側の処理－

③検証者は検証用アカウントにて電子契約サーバにアクセスし、検証を行う対象データを検索する。

④検証者は電子契約サーバに対象データの検証を要求する。

⑤電子契約サーバ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トークンの情報を TSA1 に送り、タイムスタンプの確認を依頼する。

⑥TSA1 はタイムスタンプの正当性を確認し、結果を電子契約サーバに通知する。

⑦電子契約サーバ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トークン内のハッシュ値と対象データから計算したハッシュ値の比較を行う。

⑧電子契約サーバは TSA2 の公開鍵でデジタル署名を使用する方式のタイムスタンプトークンのデジタル署名を検証し、正当性を検証する。

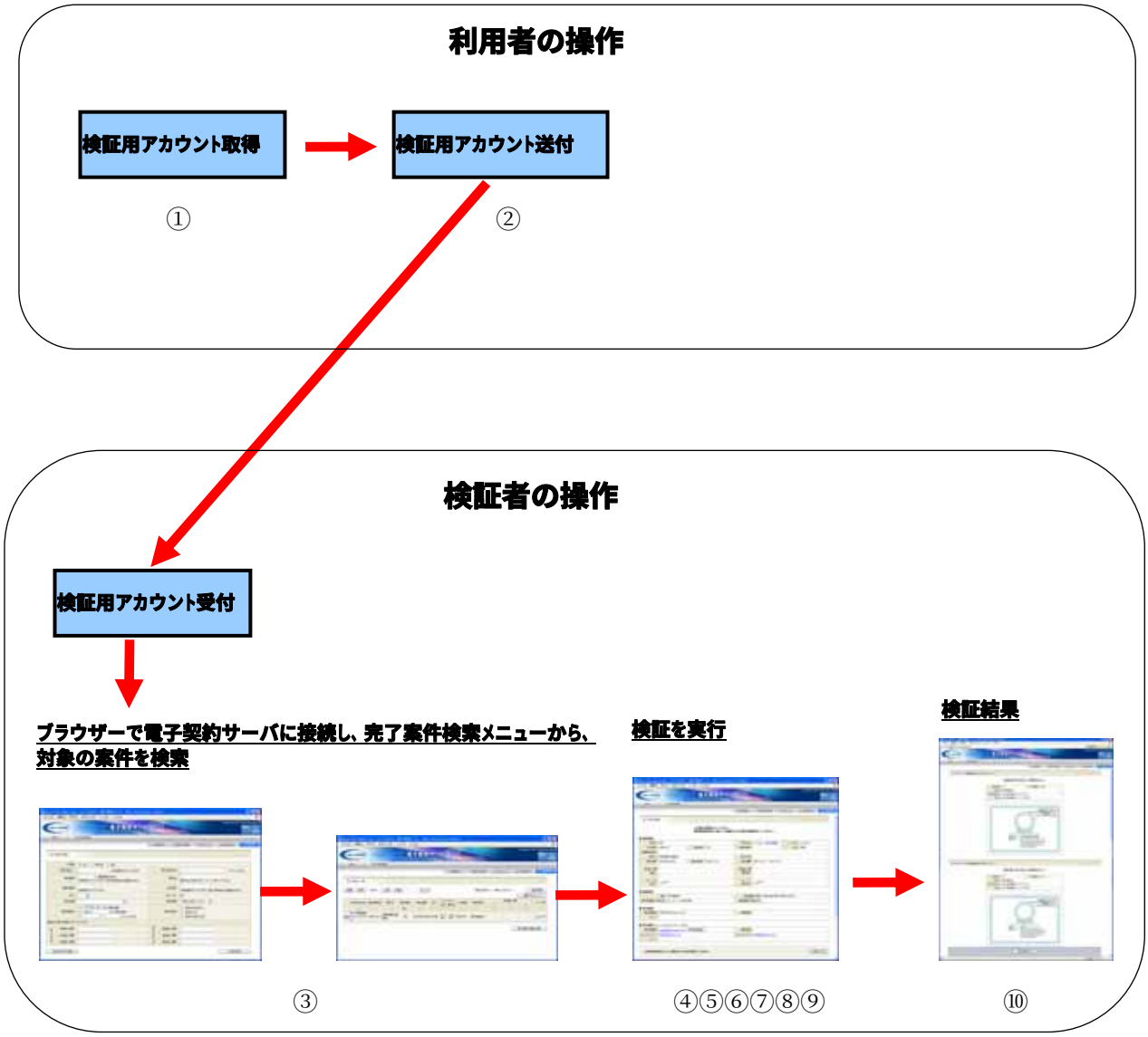
⑨電子契約サーバはデジタル署名を使用する方式のタイムスタンプトークン内のハッシュ値と対象データから計算したハッシュ値の比較を行う。

⑩電子契約サーバは検証者に対象データに対する両方式のタイムスタンプの検証結果を通知する。

図 2-9　電子契約サーバによる検証

以下に、実証実験で使用する電子契約サービスの対象データ検証時の画面遷移を示す。

操作の詳細については、付録「実証実験操作説明書（電子契約サーバでの検証）」を参照すること。



※図中の①～⑩の番号は「図 2-9　電子契約サーバによる検証」の処理番号に対応している。

図 2-10　電子契約サーバでの検証フロー

6. 実証実験の結果

6-1 マルチタイムスタンプ付与機能評価

本試験では、電子契約サービスに利用者のアカウントでログインし、対象データに対するマルチタイムスタンプの取得を行った。タイムスタンプの取得後、対象データ及び 2 方式のタイムスタンプトークンのダウンロードを行った。

表 2-9　マルチタイムスタンプ付与機能評価

対象データ	0000000043_keiyaku_1.pdf
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トークン	0000000043_tsa1_1.tst
デジタル署名を使用する方式のタイムスタンプトークン	0000000043_tsa2_1.tst
「試験結果」 対象データに対して、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及びデジタル署名を使用する方式のタイムスタンプを取得でき、対象データ、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トークン及びデジタル署名を使用する方式のタイムスタンプトークンのダウンロードが行えることを確認した。	

以下の図は、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したフォルダの状態である。対象データ及びタイムスタンプトークンがダウンロードされたことが確認できる。

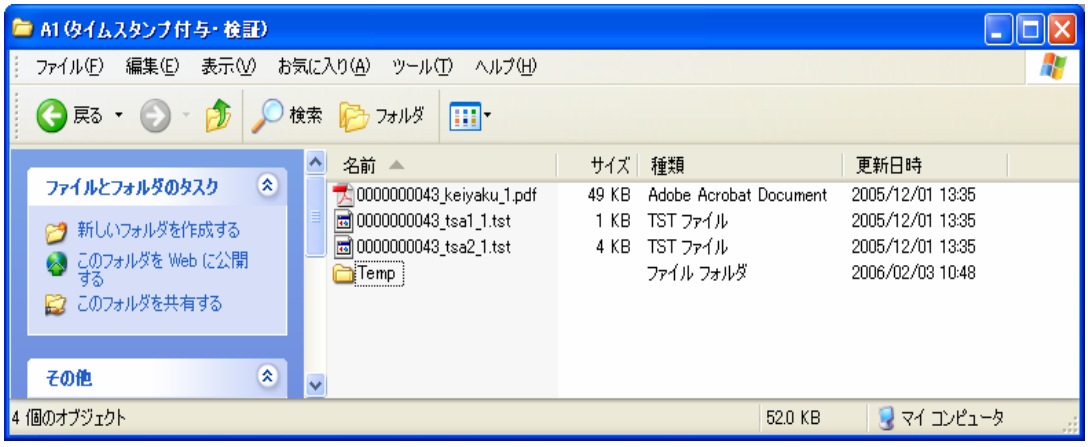
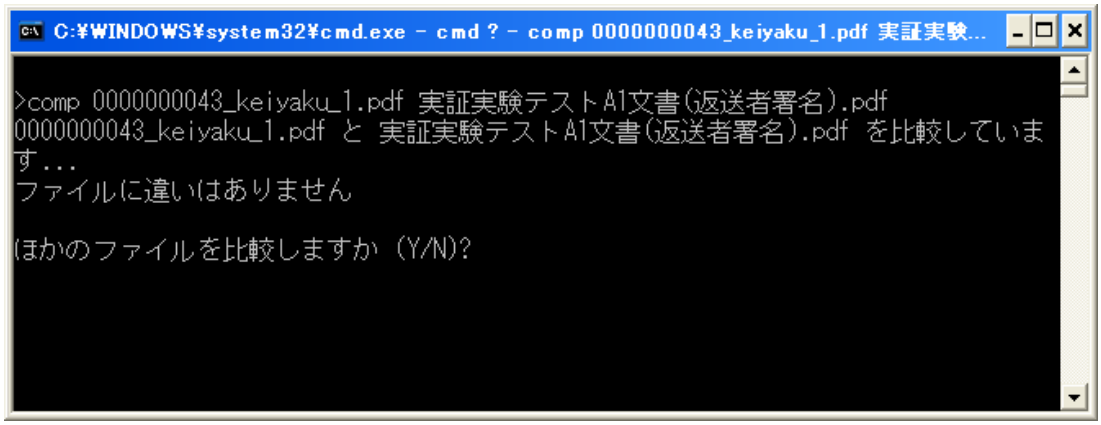


図 2-11　ダウンロードファイルを格納したフォルダ

以下の図は、ダウンロードした対象データを登録前のデータと比較したものである。登録前後のデータに違いは無く、正常にダウンロードできていることが確認できる。



実証実験テスト A1 文書（返送者署名）.pdf：電子契約サーバに登録した対象データ
0000000043_keiyaku_1.pdf：電子契約サーバよりダウンロードした対象データ

図 2-12　ダウンロードした対象データの確認

タイムスタンプトークンが正常にダウンロードできていることの確認は、対象データとの検証が成功することで判断できる。

「第 2 章 6-2VA マルチタイムスタンプ検証機能評価」にて、今回ダウンロードを行った対象データと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トークンの組合せ及び対象データとデジタル署名を使用する方式のタイムスタンプトークンの組合せについて検証が成功したため、正常にダウンロードできていることが確認された。

6-2 VA マルチタイムスタンプ検証機能評価

ダウンロードしたタイムスタンプトークン及び対象データの組合せを VA に送付し、検証を行った。なお、改ざん検出の確認では、ダウンロードした試験対象のタイムスタンプトークン及び対象データのいずれかに変更を加え、検証を行った。また VA での検証時に TSA1 をネットワークから切断し、その際の検証処理の動作確認も行った。

6-2-1 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

本試験では、「第 2 章 6-1 マルチタイムスタンプ付与機能評価」でダウンロード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トークン及び対象データの組合せを使用して検証を行った。

表 2-10　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結果

対象データファイル	0000000043_keiyaku_1.pdf			
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トークン	0000000043_tsa1_1.tst			
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結果	期待値	成功	結果	成功
「試験結果」 VA を使用して、正常な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トークンと対象データの組合せについて検証を行い、検証に成功することを確認した。				

以下の図は、VA クライアントでのファイル指定画面である。

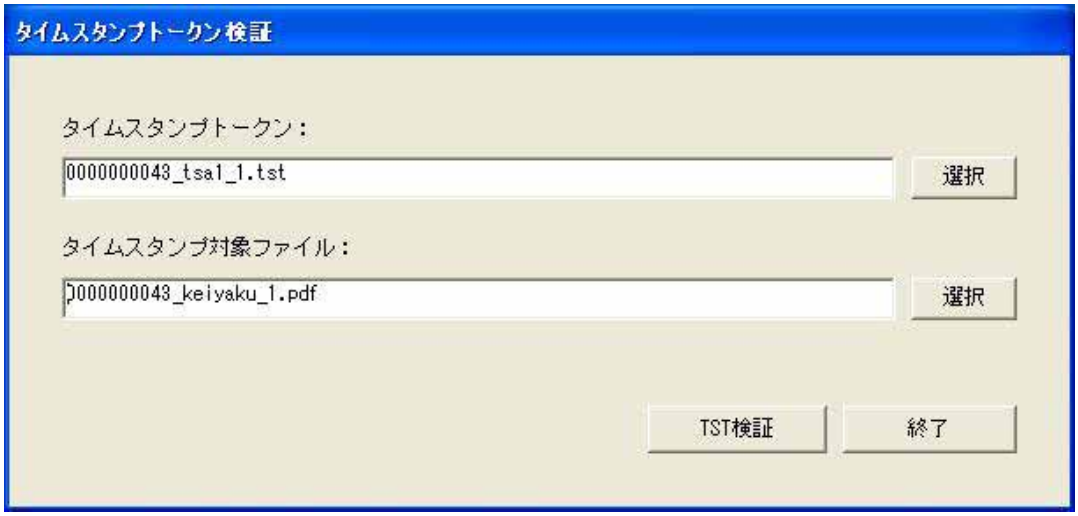


図 2-13　リンク情報を使用するアーカイビング方式のタイムスタンプトークン及び対象データの指定

以下の図は、VA クライアントでの検証結果画面である。

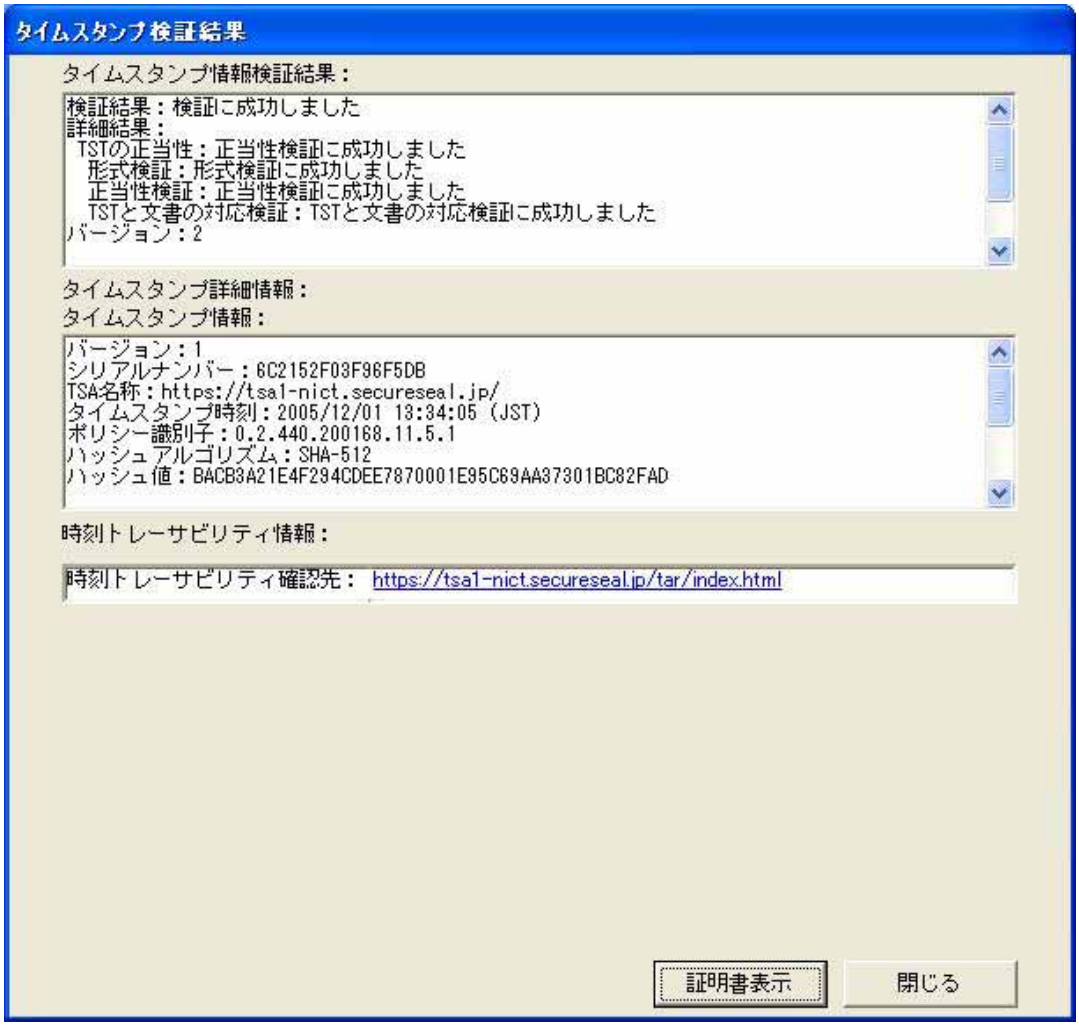


図 2-14　リンク情報を使用するアーカイビング方式のタイムスタンプの VA での検証結果

6-2-2 デジタル署名を使用する方式のタイムスタンプの検証

本試験では、「第 2 章 6-1 マルチタイムスタンプ付与機能評価」でダウンロードしたデジタル署名を使用する方式のタイムスタンプトークン及び対象データの組合せを使用して検証を行った。

表 2-11　デジタル署名を使用する方式のタイムスタンプの検証結果

対象データファイル	0000000043_keiyaku_1.pdf			
デジタル署名を使用する方式のタイムスタンプトークン	0000000043_tsa2_1.tst			
デジタル署名を使用する方式のタイムスタンプの検証結果	期待値	成功	結果	成功
「試験結果」 VA を使用して、正常なデジタル署名を使用する方式のタイムスタンプトークンと対象データの組合せについて検証を行い、検証が成功することを確認した。				

以下の図は、VA クライアントでのファイル指定画面である。

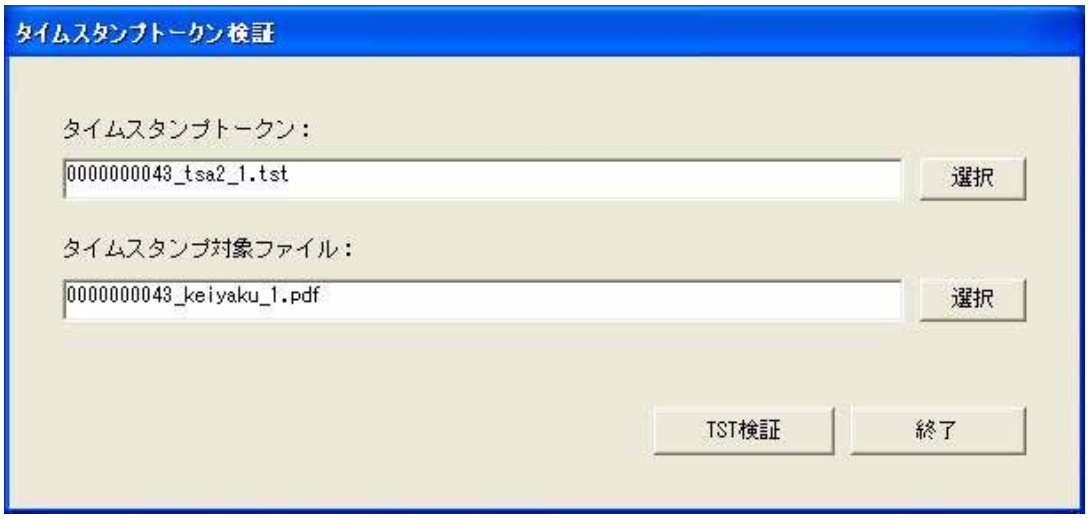


図 2-15　デジタル署名を使用する方式のタイムスタンプトークン及び対象データの指定

以下の図は、VA クライアントでのファイル検証結果画面である。

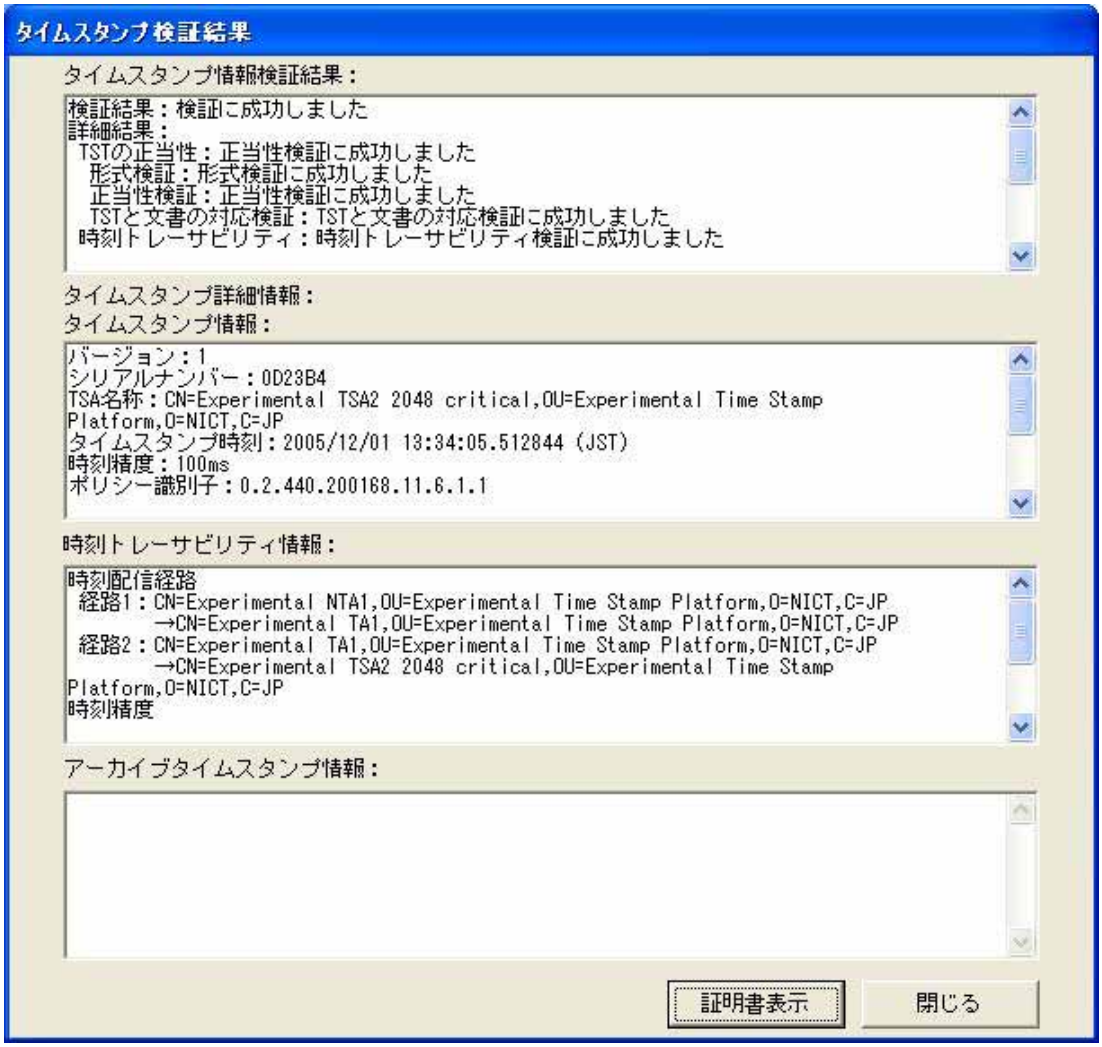


図 2-16　デジタル署名を使用する方式のタイムスタンプの VA での検証結果

6-2-3 VA での対象データ改ざんの検出（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）

本試験では、試験端末にダウンロードした対象データに対し変更を加え、そのファイルと、変更前の対象データに対して付与され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について、検証を実施した。

表 2-12　VA での対象データ改ざんの検出（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）の検証結果

対象データファイル	(改竄データ)0000000055_keiyaku_1.pdf			
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トークン	0000000055_tsa1_1.tst			
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結果	期待値	失敗	結果	失敗
「試験結果」 VA 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トークンと改ざんした対象データの組合せを検証し、対象データの改ざんが検出できることを確認した。				

以下の図は、VA クライアントでのファイル指定画面である。

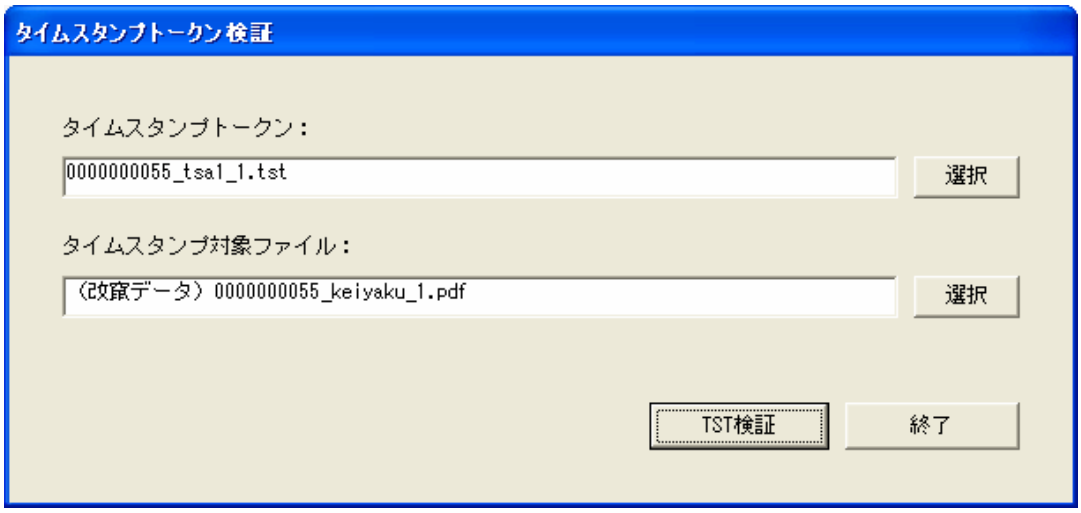


図 2-17　リンク情報を使用するアーカイビング方式のタイムスタンプトークン及び改ざん対象データの指定

以下の図は、VA クライアントでのファイル検証結果画面である。

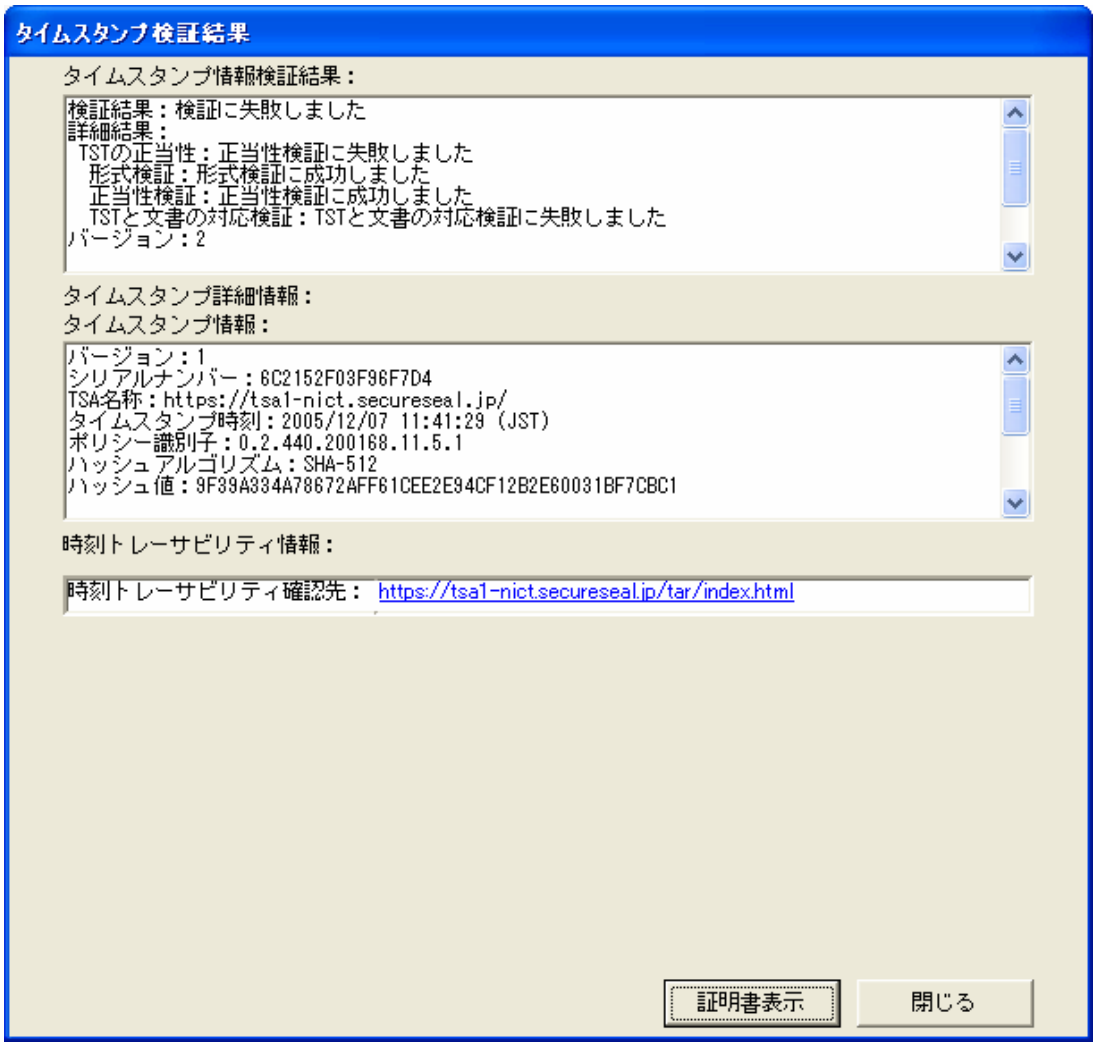


図 2-18　リンク情報を使用するアーカイビング方式のタイムスタンプでの改ざんデータの検証結果

6-2-4 VA での対象データ改ざんの検出（デジタル署名を使用する方式のタイムスタンプ）

本試験では、試験端末にダウンロードした対象データに対し変更を加え、そのファイルと、変更前の対象データに対して付与されたデジタル署名を使用する方式のタイムスタンプについて、検証を実施した。

表 2-13　VA での対象データ改ざんの検出（デジタル署名を使用する方式のタイムスタンプ）の検証結果

対象データファイル	(改竄データ)0000000055_keiyaku_1.pdf			
デジタル署名を使用する方式のタイムスタンプトークン	0000000055_tsa2_1.tst			
デジタル署名を使用する方式のタイムスタンプの検証結果	期待値	失敗	結果	失敗
「試験結果」 VA にてデジタル署名を使用する方式のタイムスタンプトークンと改ざんした対象データの組合せを検証し、対象データの改ざんが検出できることを確認した。				

以下の図は、VA クライアントでのファイル指定画面である。

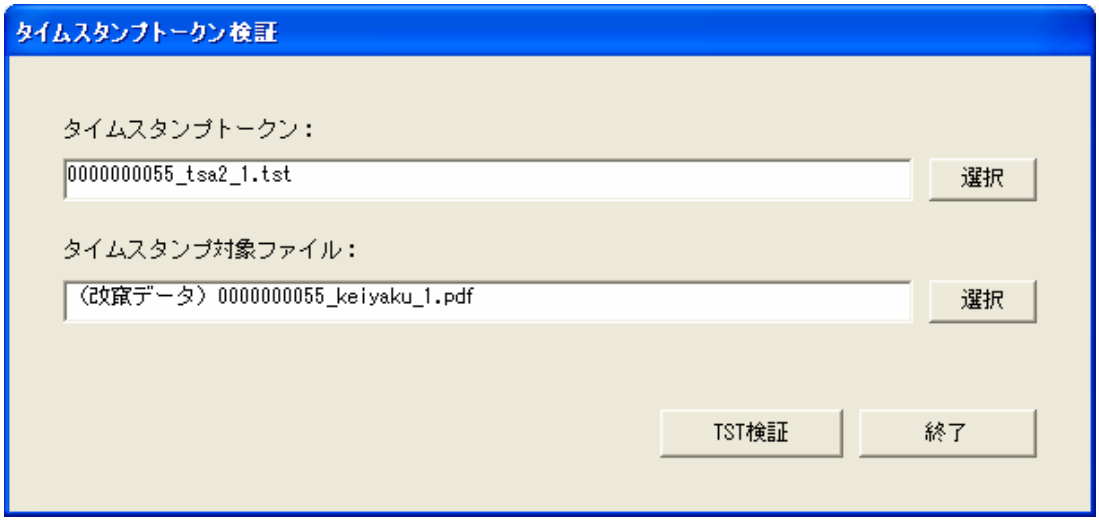


図 2-19　デジタル署名を使用する方式のタイムスタンプトークン及び改ざん対象データの指定

以下の図は、VA クライアントでのファイル検証結果画面である。

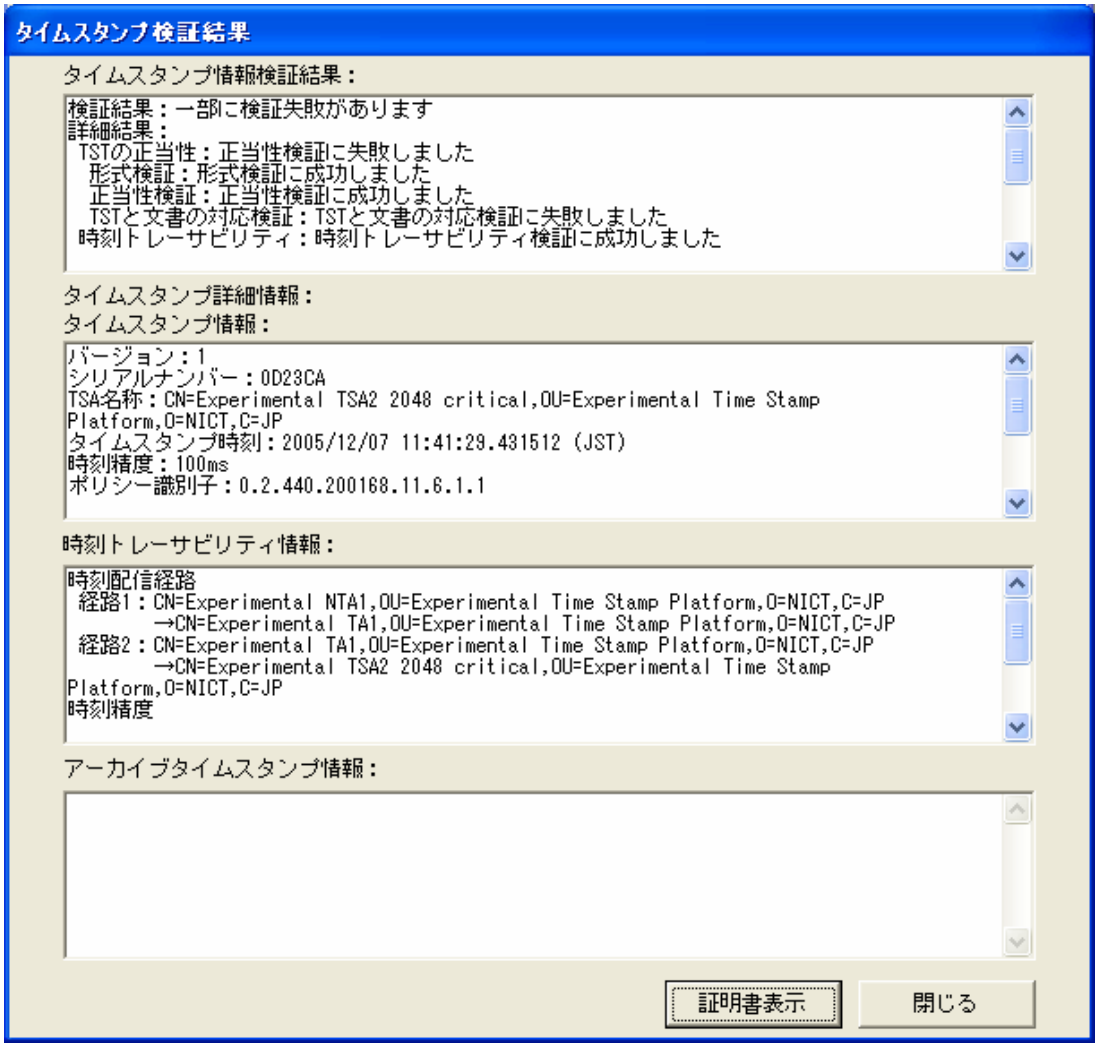


図 2-20　デジタル署名を使用する方式のタイムスタンプでの改ざんデータの検証結果

6-2-5 VA での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トークン改ざんの検出

本試験では、試験端末にダウンロード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トークンに対し変更を加え、そのファイルと対象データの組合せにて検証を実施した。

表 2-14　VA での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トークン改ざんの検出の検証結果

対象データファイル	0000000056_keiyaku_1.pdf			
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トークン	(改竄)0000000056_tsa1_1.tst			
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結果	期待値	失敗	結果	失敗
「試験結果」 VA にて、改ざん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トークンと対象データの組合せについて検証し、タイムスタンプトークンの改ざんが検出できることを確認した。				

以下の図は、VA クライアントでのファイル指定画面である。

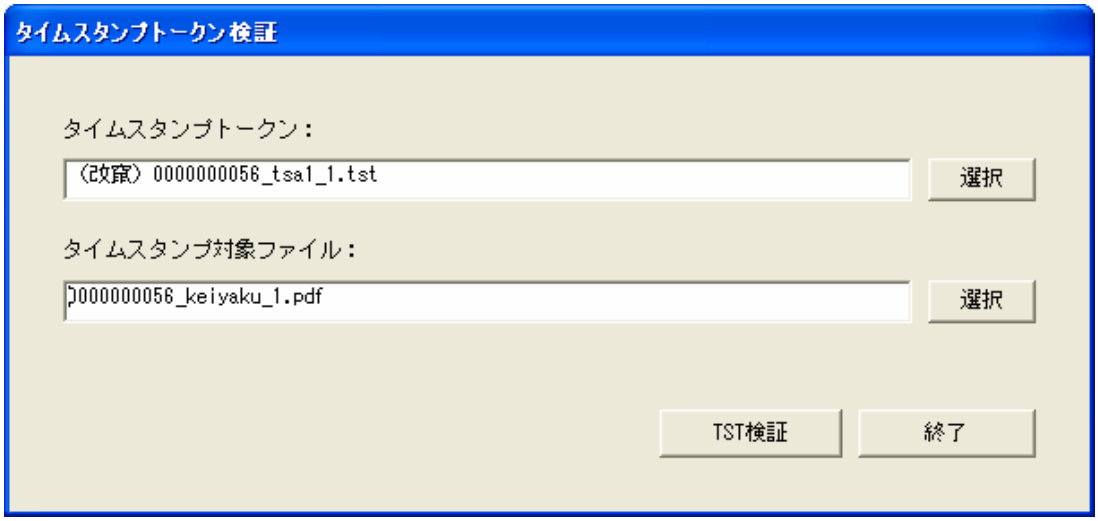


図 2-21　改ざんしたリンク情報を使用するアーカイビング方式のタイムスタンプトークン及び対象データの指定

以下の図は、VA クライアントでのファイル検証結果画面である。

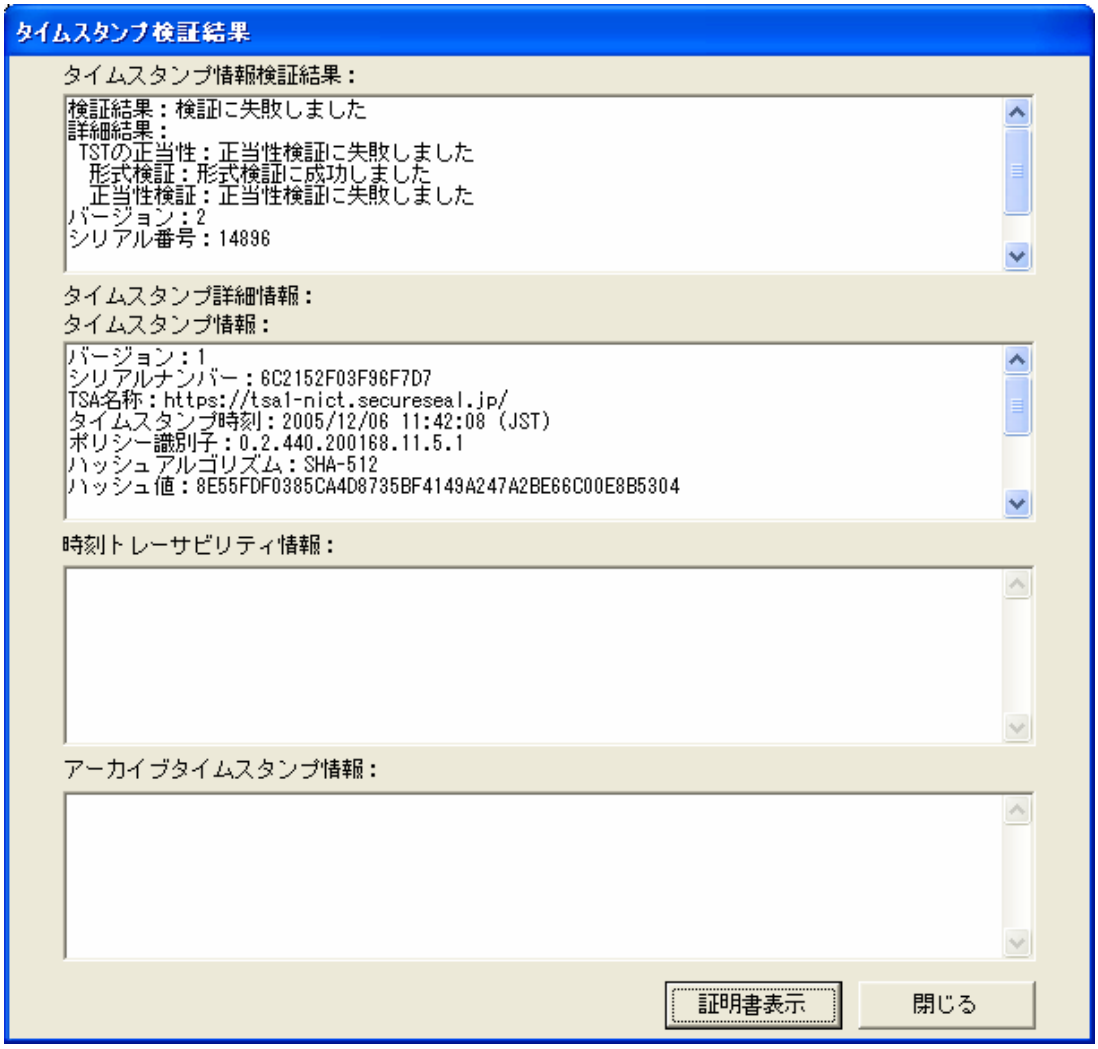


図 2-22　改ざんしたリンク情報を使用するアーカイビング方式のタイムスタンプでの検証結果

6-2-6 VA でのデジタル署名を使用する方式のタイムスタンプ改ざんの検出

本試験では、試験端末にダウンロードしたデジタル署名を使用する方式のタイムスタンプトークンに対し変更を加え、そのファイルと対象データの組合せにて検証を実施した。

表 2-15　VA でのデジタル署名を使用する方式のタイムスタンプ改ざんの検出の検証結果

対象データファイル	0000000057_keiyaku_1.pdf			
デジタル署名を使用する方式のタイムスタンプトークン	(改竄)0000000057_tsa2_1.tst			
デジタル署名を使用する方式のタイムスタンプの検証結果	期待値	失敗	結果	失敗
「試験結果」 VA にて、改ざんしたデジタル署名を使用する方式のタイムスタンプトークンと対象データの組合せについて検証し、タイムスタンプトークンの改ざんが検出できることを確認した。				

以下の図は、VA クライアントでのファイル指定画面である。

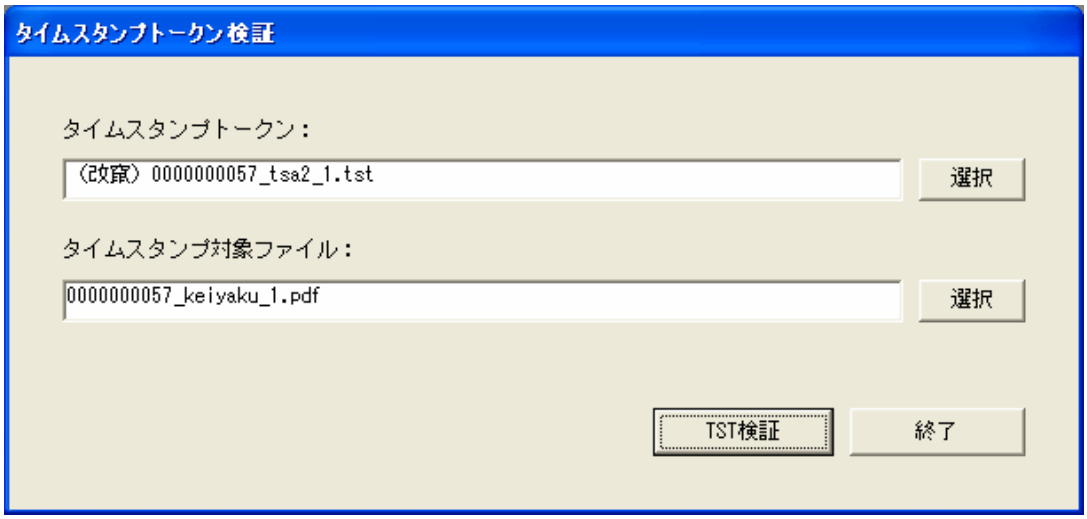


図 2-23　改ざんしたデジタル署名を使用する方式のタイムスタンプトークン及び対象データの指定

以下の図は、VA クライアントでの検証結果画面である。

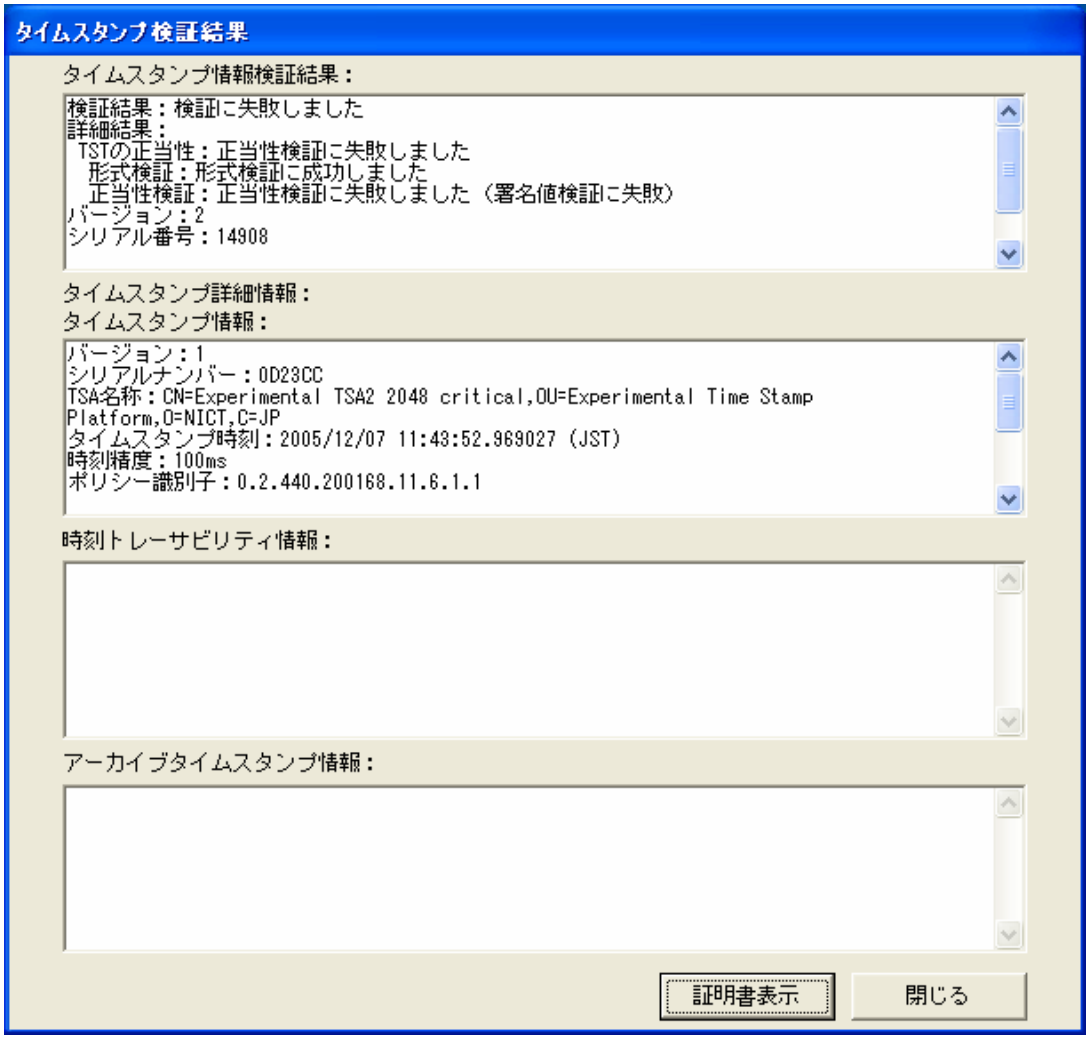


図 2-24　改ざんしたデジタル署名を使用する方式のタイムスタンプでの検証結果

6-2-7 TSA1 切断時の VA での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

本試験では、2 方式のタイムスタンプが付与された対象データの検証を VA にて行う場合、片方の TSA が何らかの異常により接続できない場合に、他方のタイムスタンプにより検証が行えることを確認するため、片方の TSA が利用できない環境での検証を実施した。試験の実施にあたり、TSA1 を LAN から切り離し、検証を実施した。

なお、TSA2 の付与するデジタル署名を使用する方式のタイムスタンプの検証では、VA より TSA2 に対するアクセスが発生しないため、TSA2 の切断試験は実施しない。

表 2-16　TSA1 切断時の VA を介してのマルチタイムスタンプ検証結果

対象データファイル	0000000210_keiyaku_1.pdf			
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トークン	0000000210_tsa1_1.tst			
デジタル署名を使用する方式のタイムスタンプトークン	0000000210_tsa2_1.tst			
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結果	期待値	失敗	結果	失敗
デジタル署名を使用する方式のタイムスタンプの検証結果	期待値	成功	結果	成功
「試験結果」 TSA1 が切断されている状態で、マルチタイムスタンプが付与された対象データの検証を行い、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が失敗する場合でも、デジタル署名を使用する方式のタイムスタンプの検証が成功し、対象データの真正性の確認が行えることを確認した。				

以下の図は、VA クライアントでのファイル指定画面である。（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トークンを指定）

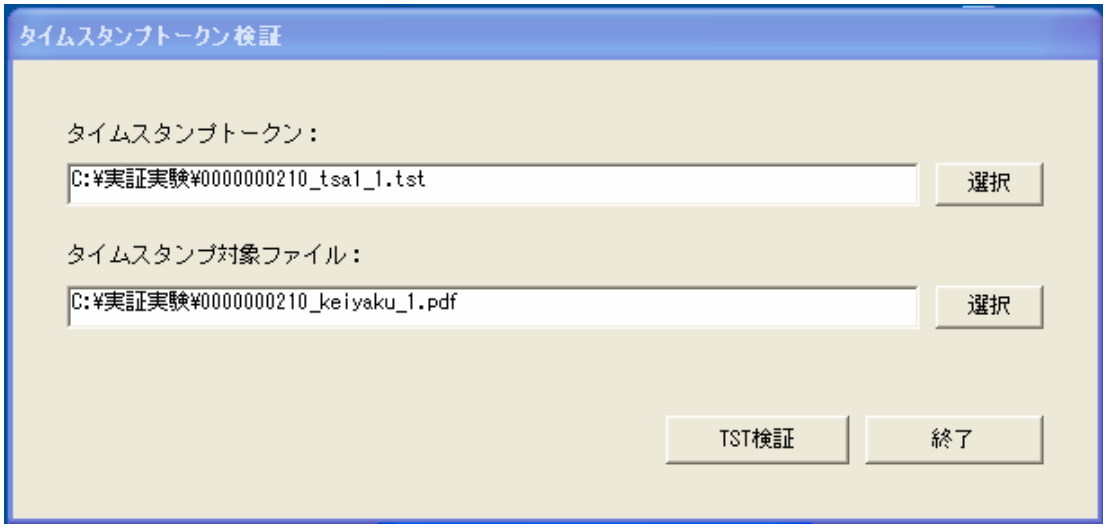


図 2-25　切断試験でのリンク情報を使用するアーカイビング方式のタイムスタンプトークンの指定

以下の図は、VA クライアントが表示したエラーメッセージを示している。
VA より TSA1 に接続できないため、ネットワークエラー(status:0225)が発生している。

図 2-26　TSA1 切断時の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検証のエラー

以下の図は、VA クライアントでのファイル指定画面である。（デジタル署名を使用する方式のタイムスタンプを指定）

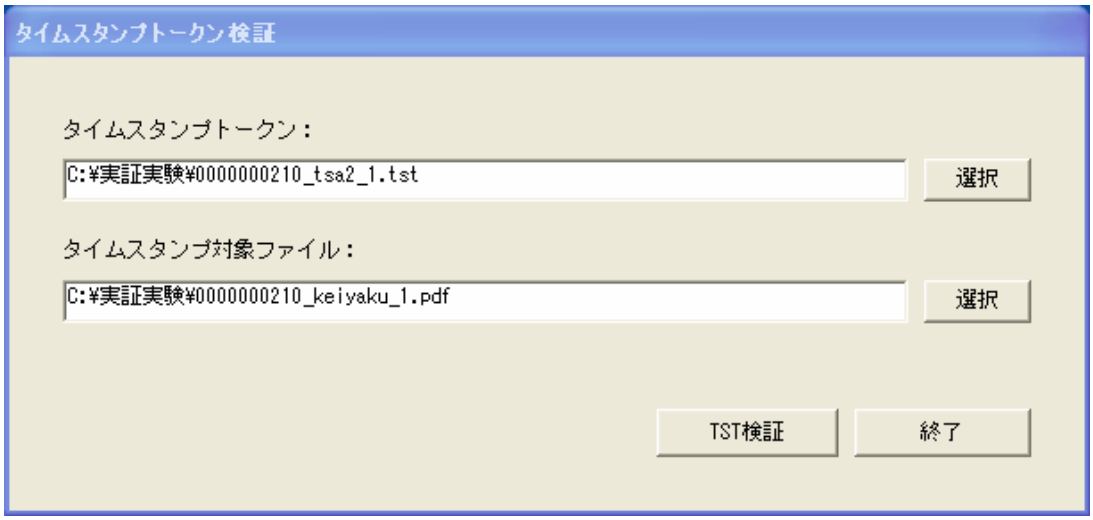


図 2-27　切断試験でのデジタル署名を使用する方式のタイムスタンプトークンの指定

以下の図は、VA クライアントでの検証結果画面である。

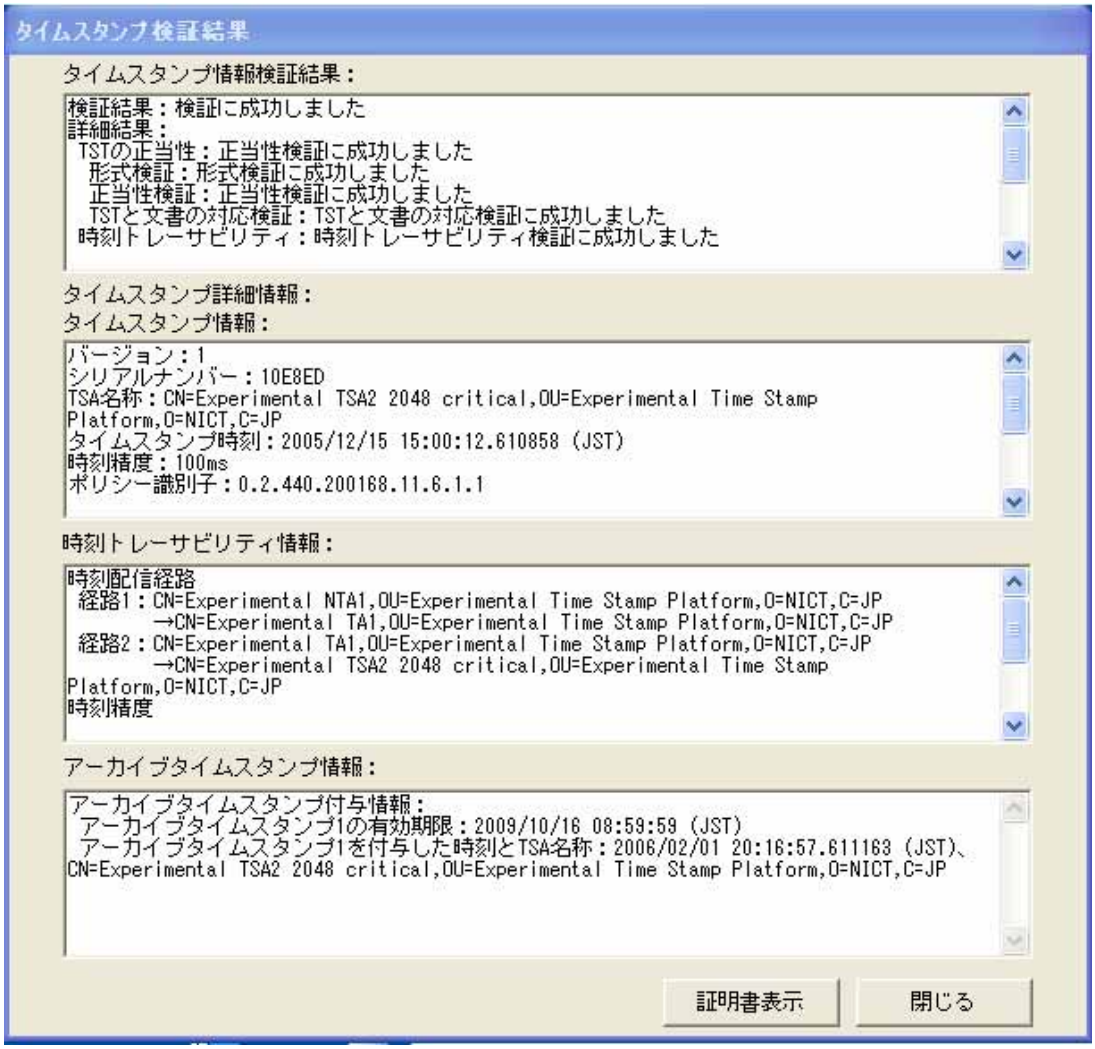


図 2-28　TSA1 切断時のデジタル署名を使用する方式のタイムスタンプ検証画面

6-2-8 VA マルチタイムスタンプ検証機能評価結果

VA を介したタイムスタンプの検証にて、対象データと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及びデジタル署名を使用する方式のタイムスタンプ両方式の検証が行えることを確認した。

対象データ及び 2 方式のタイムスタンプトークンのいずれかが改ざんされた場合については、VA を介した検証により各々改ざんが検出できることを確認した。

また、VA での検証時に VA から TSA1 に接続できない状態でも、TSA2 の付与したタイムスタンプトークンを用いて対象データの検証が行えることを確認した。

6-3 電子契約サーバマルチタイムスタンプ検証機能評価

本試験では、検証用アカウントにて電子契約サーバにログインし、対象データの検証を行った。なお、改ざん検出の確認では、電子契約サーバ内に保管されているタイムスタンプトークンの情報及び対象データのいずれかを直接改ざんし、検証を実施した。また、電子契約サーバでの検証時に TSA1 をネットワークから切断し、その際の検証処理の動作確認を行った。

6-3-1 電子契約サーバでのマルチタイムスタンプの検証

本試験では、「第 2 章 6-1 マルチタイムスタンプ付与機能評価」で登録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トークン及びデジタル署名を使用する方式のタイムスタンプトークンと対象データの組合せを使用して、検証を行っている。

表 2-17　電子契約サーバでのマルチタイムスタンプの検証結果

対象データ	0000000043_keiyaku_1.pdf			
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トークン	0000000043_tsa1_1.tst			
デジタル署名を使用する方式のタイムスタンプトークン	0000000043_tsa2_1.tst			
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結果	期待値	成功	結果	成功
デジタル署名を使用する方式のタイムスタンプの検証結果	期待値	成功	結果	成功
「試験結果」 検証用アカウントを用いて電子契約サーバにログインし、対象データと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トークン及びデジタル署名を使用する方式のタイムスタンプとの組合せについて検証を行い、両方式の検証が成功することを確認した。				

以下の図は、電子契約サービスでの検証結果画面である。なお、検証結果画面は 1 画面に収まらないため、上下にスクロールし 2 画面に分けて表示している。

図 2-29　電子契約サーバでの検証結果

6-3-2 電子契約サーバでの対象データ改ざんの検出

本試験では、電子契約サーバ内に保管されている対象データを直接改ざんし、検証を実施した。

表 2-18　電子契約サーバでの対象データ改ざん検出の検証結果

対象データ	0000000052_keiyaku_1.pdf			
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トークン	0000000052_tsa1_1.tst			
デジタル署名を使用する方式のタイムスタンプトークン	0000000052_tsa2_1.tst			
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結果	期待値	失敗	結果	失敗
デジタル署名を使用する方式のタイムスタンプの検証結果	期待値	失敗	結果	失敗
「試験結果」 電子契約サーバにて改ざんされた対象データの検証を実施すると、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及びデジタル署名を使用する方式のタイムスタンプについての検証が両方とも失敗となり、対象データの改ざんが検出できることを確認した。				

以下の図は、電子契約サーバでの検証結果画面である。

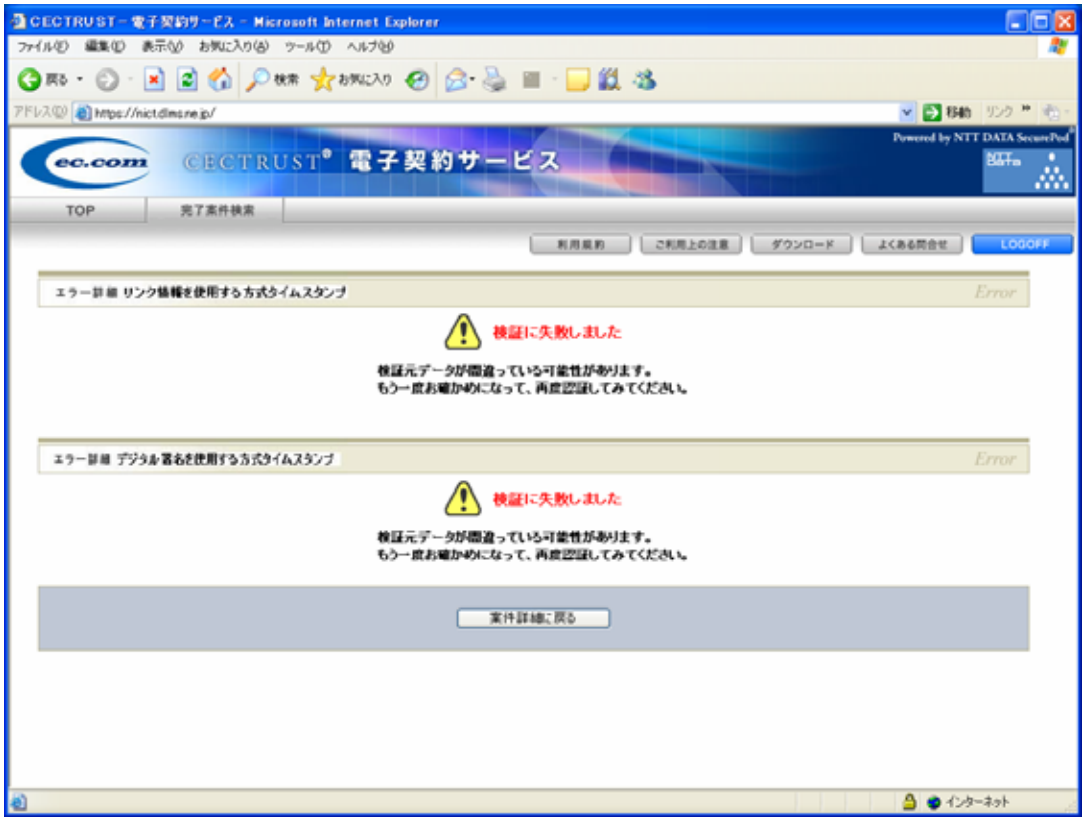


図 2-30　電子契約サーバでの改ざん文書検証結果

6-3-3 電子契約サーバでの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トークン改ざんの検出

本試験では、電子契約サーバ内に保管されている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トークンの情報を直接改ざんし、検証を実施した。

表 2-19　電子契約サーバでの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改ざん検出の検証結果

対象データ	0000000053_keiyaku_1.pdf			
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トークン	0000000053_tsa1_1.tst			
デジタル署名を使用する方式のタイムスタンプトークン	0000000053_tsa2_1.tst			
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結果	期待値	失敗	結果	失敗
デジタル署名を使用する方式のタイムスタンプの検証結果	期待値	成功	結果	成功
「試験結果」 登録されている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トークンを改ざんし、検証を実施すると、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は検証に失敗し、デジタル署名を使用する方式のタイムスタンプは検証に成功することを確認した。				

以下の図は、電子契約サーバでの検証結果画面である。

図 2-31　改ざん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結果

6-3-4 電子契約サーバでのデジタル署名を使用する方式のタイムスタンプトークン改ざんの検出

本試験では、電子契約サーバ内に保管されているデジタル署名を使用する方式のタイムスタンプトークンの情報を直接改ざんし、検証を実施した。

表 2-20　電子契約サーバでのデジタル署名を使用する方式のタイムスタンプ改ざんの検出の検証結果

対象データ	0000000054_keiyaku_1.pdf			
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トークン	0000000054_tsa1_1.tst			
デジタル署名を使用する方式のタイムスタンプトークン	0000000054_tsa2_1.tst			
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結果	期待値	成功	結果	成功
デジタル署名を使用する方式のタイムスタンプの検証結果	期待値	失敗	結果	失敗
「試験結果」 登録されているデジタル署名を使用する方式のタイムスタンプトークンを改ざんし、検証を実施すると、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は検証に成功し、デジタル署名を使用する方式のタイムスタンプは検証に失敗することを確認した。				

以下の図は、電子契約サーバでの検証結果画面である。

図 2-32　改ざん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結果

6-3-5 電子契約サーバでの TSA1 切断時のタイムスタンプ検証

本試験では、2 方式のタイムスタンプが付与された対象データの検証を電子契約サーバにて行う場合、片方の TSA が何らかの異常により接続できない場合に、他方のタイムスタンプにより検証が行えることを確認するため、片方の TSA が利用できない環境での検証を実施した。試験の実施にあたり、TSA1 を LAN から切り離し検証を行った。なお、TSA2 の付与するデジタル署名を使用する方式のタイムスタンプの検証では、電子契約サーバより TSA2 に対するアクセスが発生しないため TSA2 の切断試験は実施しない。

表 2-21　電子契約サーバでの TSA1 切断時のタイムスタンプ検証

対象データ	0000000283_keiyaku_1.pdf			
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トークン	0000000283_tsa1_1.tst			
デジタル署名を使用する方式のタイムスタンプトークン	0000000283_tsa2_1.tst			
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結果	期待値	失敗	結果	失敗
デジタル署名を使用する方式のタイムスタンプの検証結果	期待値	成功	結果	成功
「試験結果」 TSA1 が切断されている状態で、マルチタイムスタンプが付与された対象データの検証を行い、片方のタイムスタンプ（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）の検証が失敗する場合でも、もう一方のタイムスタンプ（デジタル署名を使用する方式のタイムスタンプ）の検証が成功し、対象データの真正性を確認できることを確認した。				

以下の図は、電子契約サーバでの検証結果画面である。

※エラーメッセージは原因別の表示を行っていないため、本図の表示となる。

図 2-33　TSA1 切断時の電子契約サーバでの検証

6-3-6 電子契約サーバマルチタイムスタンプ検証機能評価結果

電子契約サーバを使用した検証にて、対象データと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及びデジタル署名を使用する方式のタイムスタンプ両方式の検証が行えることを確認した。

対象データ及び 2 方式のタイムスタンプトークンのいずれかが改ざんされた場合については、電子契約サーバを介した検証により各々改ざんが検出できることを確認した。

また、電子契約サーバでの検証時に電子契約サーバから TSA1 を接続できない状態でも、TSA2 の付与したタイムスタンプトークンを用いて対象データの検証が行えることを確認した。

6-4 時刻トレーサビリティ機能評価

VA を使用してタイムスタンプの検証を実施する際、合わせて時刻トレーサビリティの確認を行った。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監査証明書の情報を確認した。

6-4-1 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時刻トレーサビリティ確認

本試験では、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の時刻トレーサビリティの確認を行った。

表 2-22　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時刻トレーサビリティ確認

対象データ	0000000159_keiyaku_1.pdf
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トークン	0000000159_tsa1_1.tst
TSA1 の時刻精度及び配信経路の確認	時刻監査レポートを参照
TA の時刻精度及び配信経路の確認	時刻監査レポートを参照
「試験結果」 公開されている TSA1 に対する時刻監査レポートを、操作端末よりブラウザを用いて閲覧し、時刻精度及び時刻配信経路を確認した。	

表 2-23　TSA1 の時刻トレーサビリティ確認結果

TST1 時刻情報 (JST) (*1)	TSA1 の監査時刻(UTC)	TA-TSA1 間の offset[us]	TA の監査時刻(UTC)	NTA-TA 間の offset[us]	時刻誤差の合計[us](*2)
2005/12/13 14:13:10	2005/12/13 04:44:08.386	583	2005/12/13 04:37:13.625	-146	729

*1 TST1 は TSA1 の発行したタイムスタンプトークンを表す。

*2 時刻誤差の合計は、TA-TSA1 間の offset、NTA-TA 間の offset の絶対値の和である。

以下の図は、VA クライアントでの検証結果画面である。検証対象のタイムスタンプの付与時刻が確認できる。

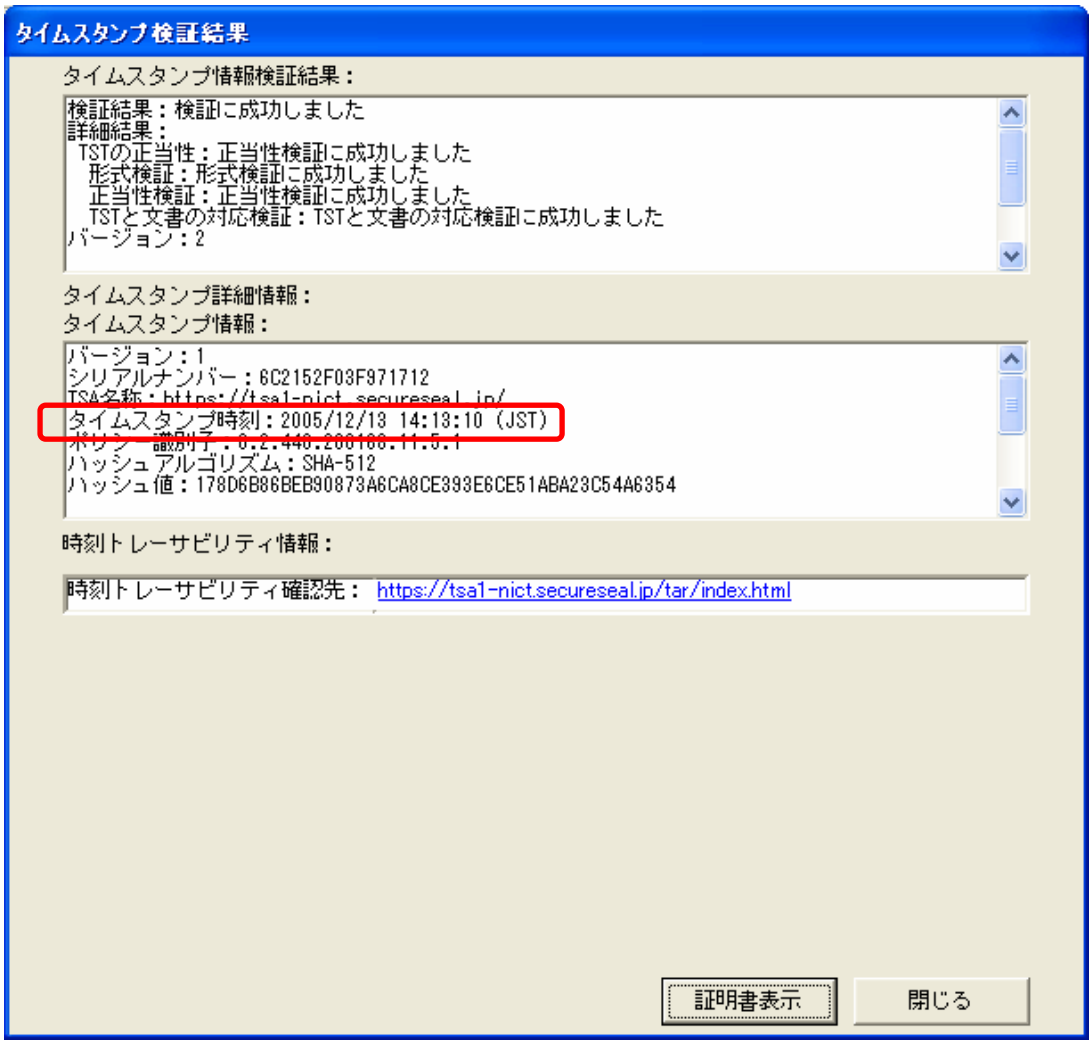


図 2-34　リンク情報を使用するアーカイビング方式のタイムスタンプの付与時刻の確認

以下に時刻監査レポートの表紙を示す。署名マークによって、TA のデジタル署名が付与されていることが分かる。

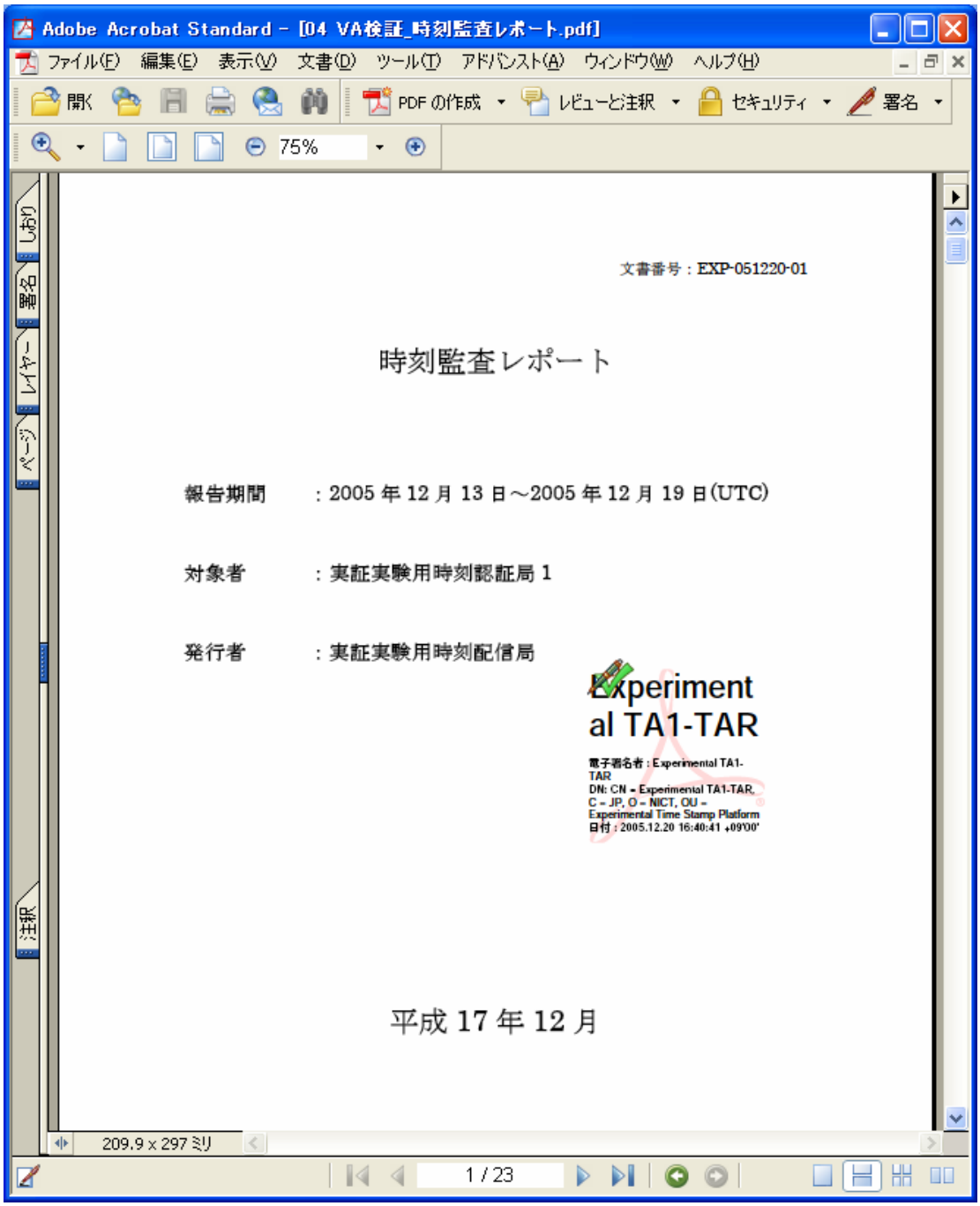


図 2-35　時刻監査レポート（表紙）

以下にデジタル署名のプロパティを示す。時刻監査レポートがデジタル署名を付与された日時以降に変更されていないことが分かる。

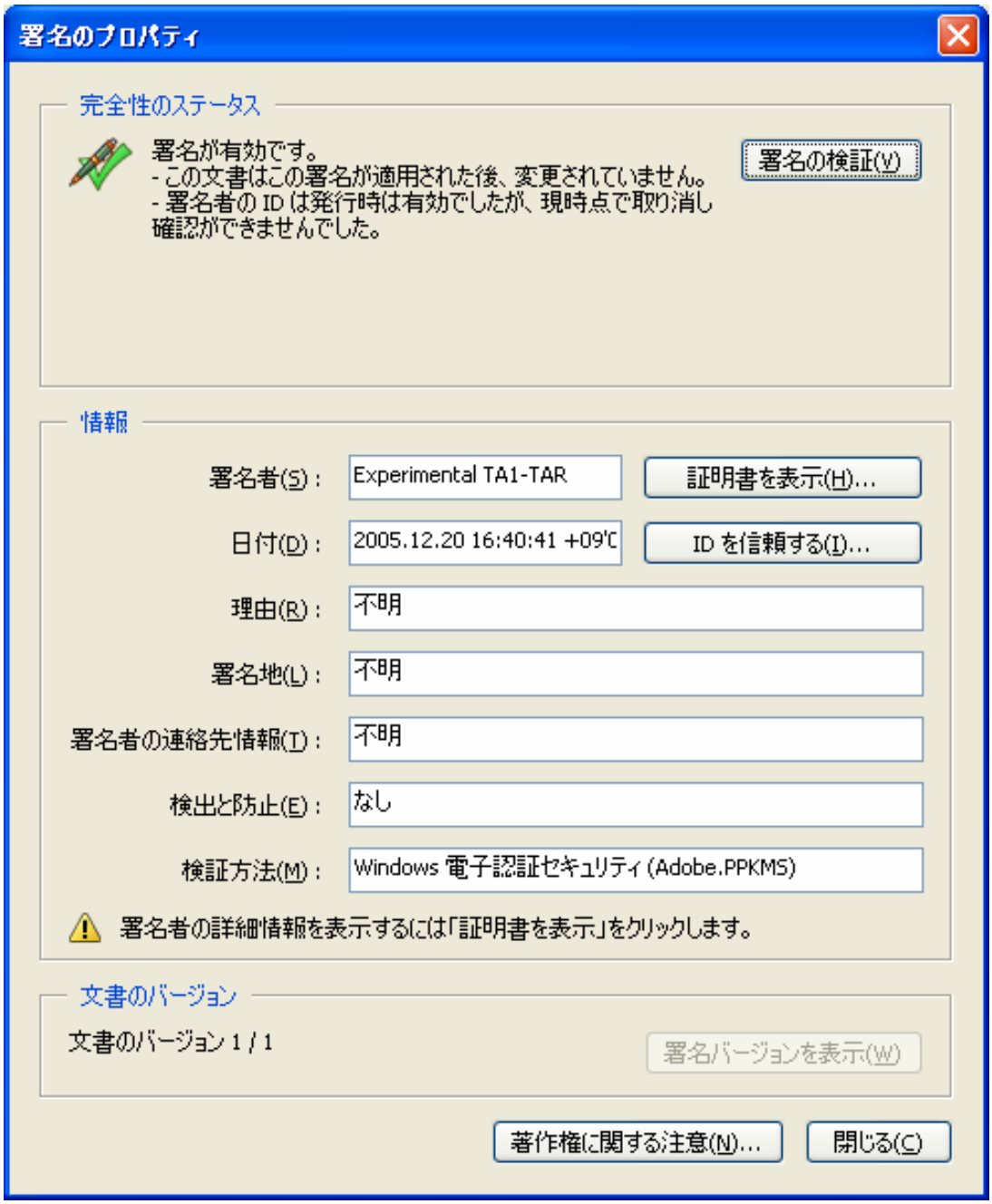


図 2-36　時刻監査レポートのデジタル署名情報

以下に TSA1 に対する TA の監査規格を示す。

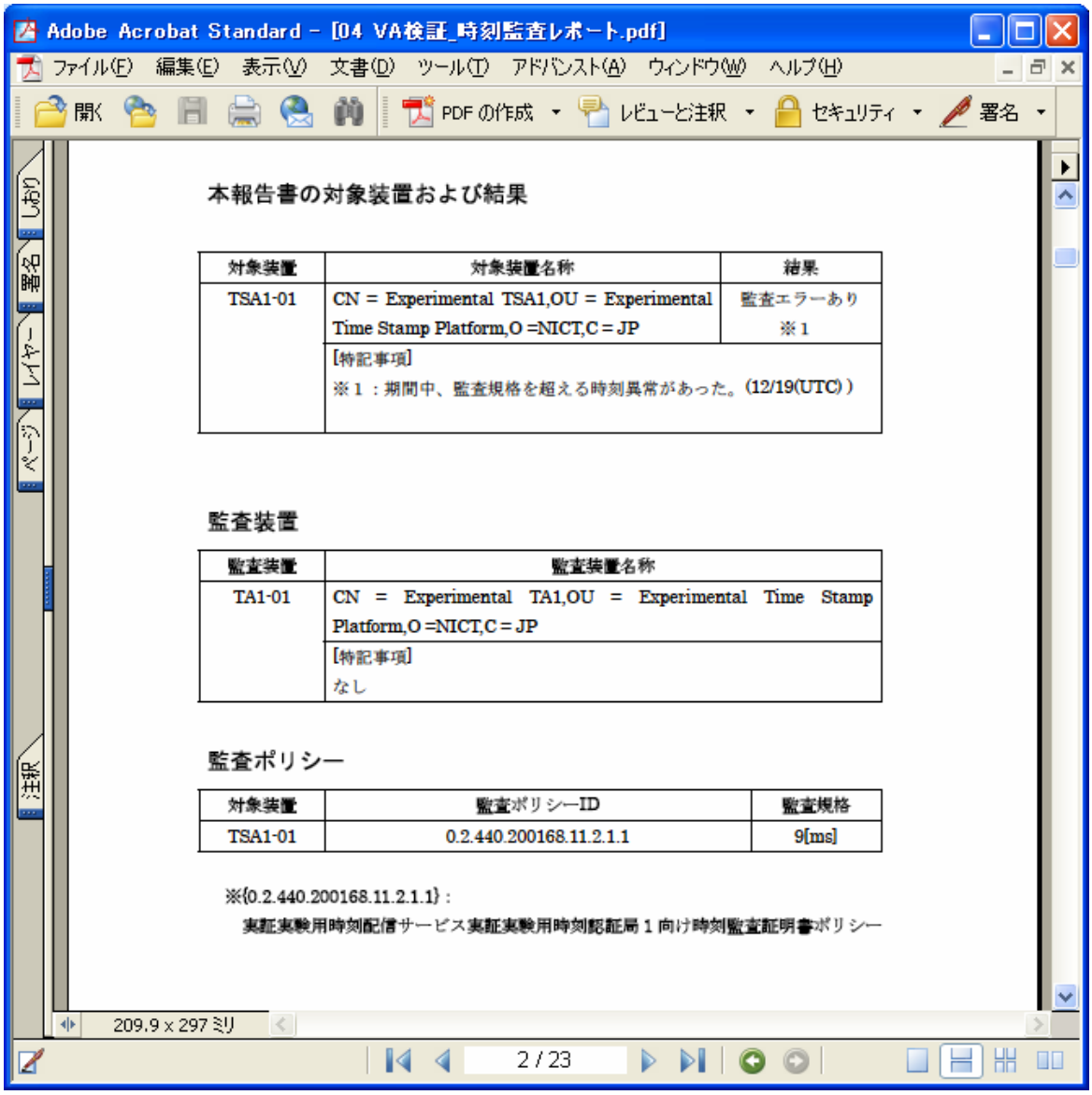


図 2-37　TA-TSA1 の監査情報

以下に時刻配信及び監査ルートを示す。

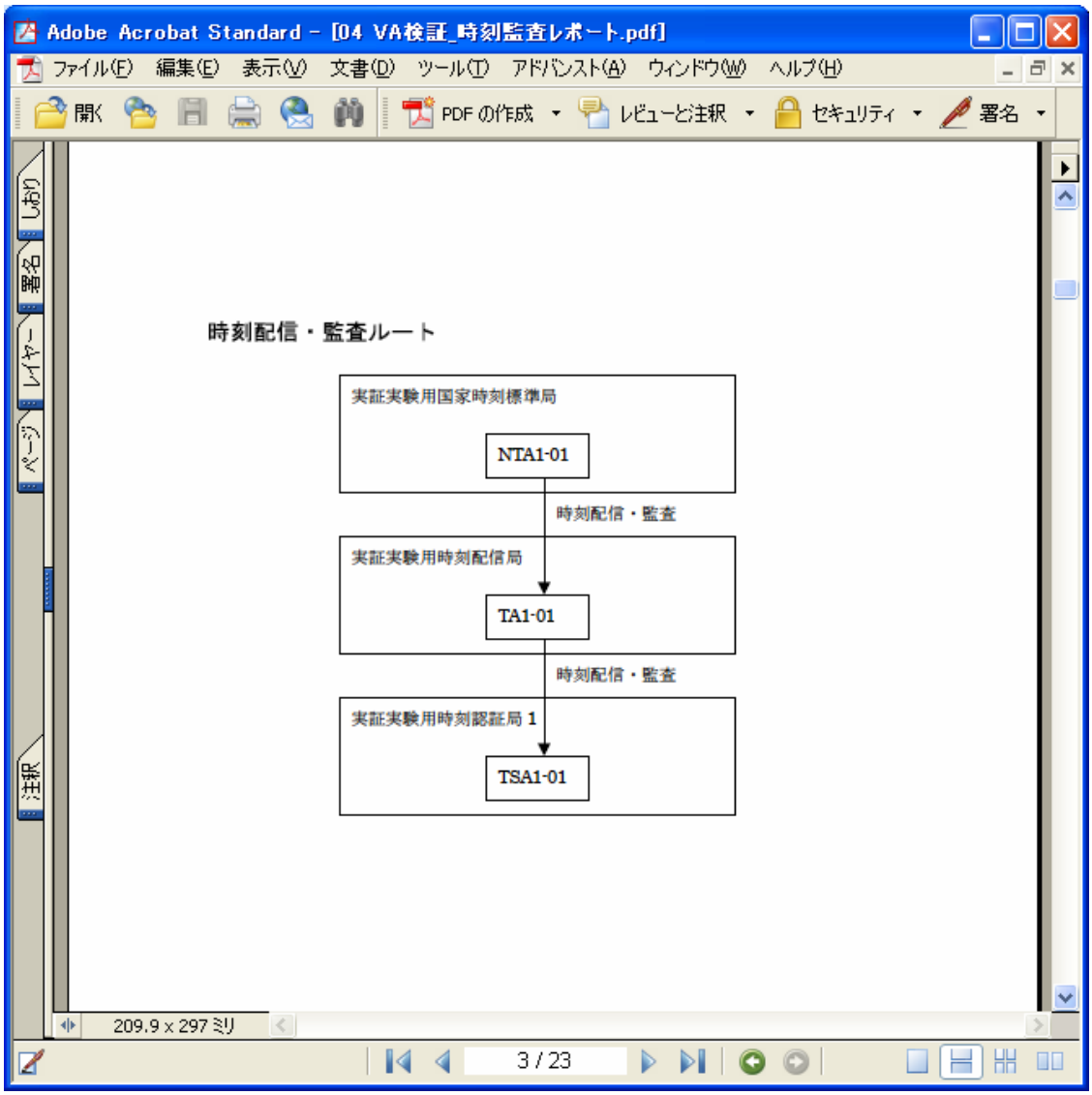
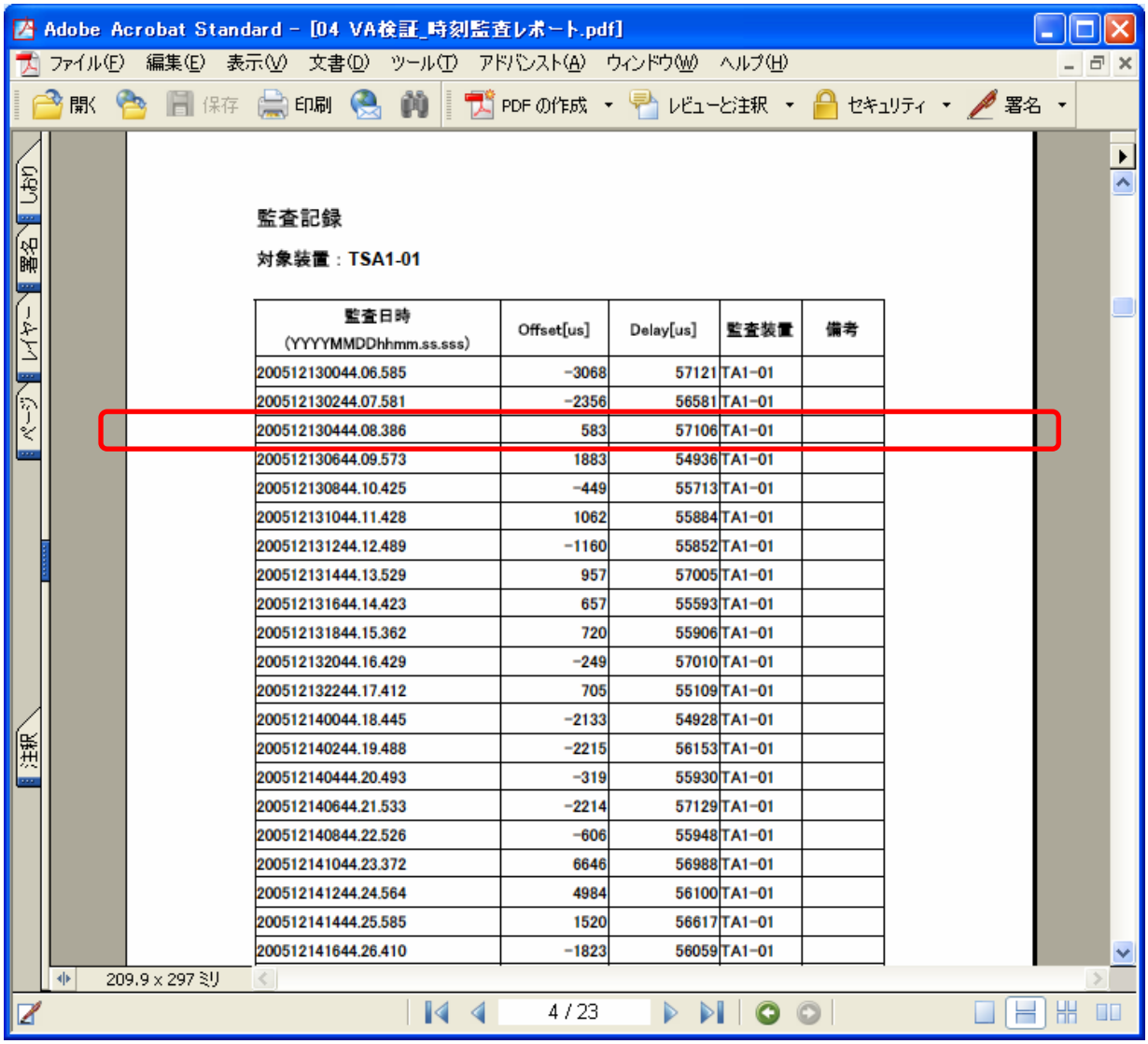


図 2-38　時刻配信及び監査経路の情報

以下に TSA1 に対する監査記録を示す。検証対象のタイムスタンプトークンが付与された時刻の直前の TSA1 の時計の誤差情報が分かる。なお、VA クライアントではタイムスタンプ発行日時を JST で表記していたが、時刻監査レポートの監査日時では UTC 表記である。そのため、時刻監査レポートを確認する際には VA クライアントに表示された時刻から 9 時間引いた時刻を参照した。



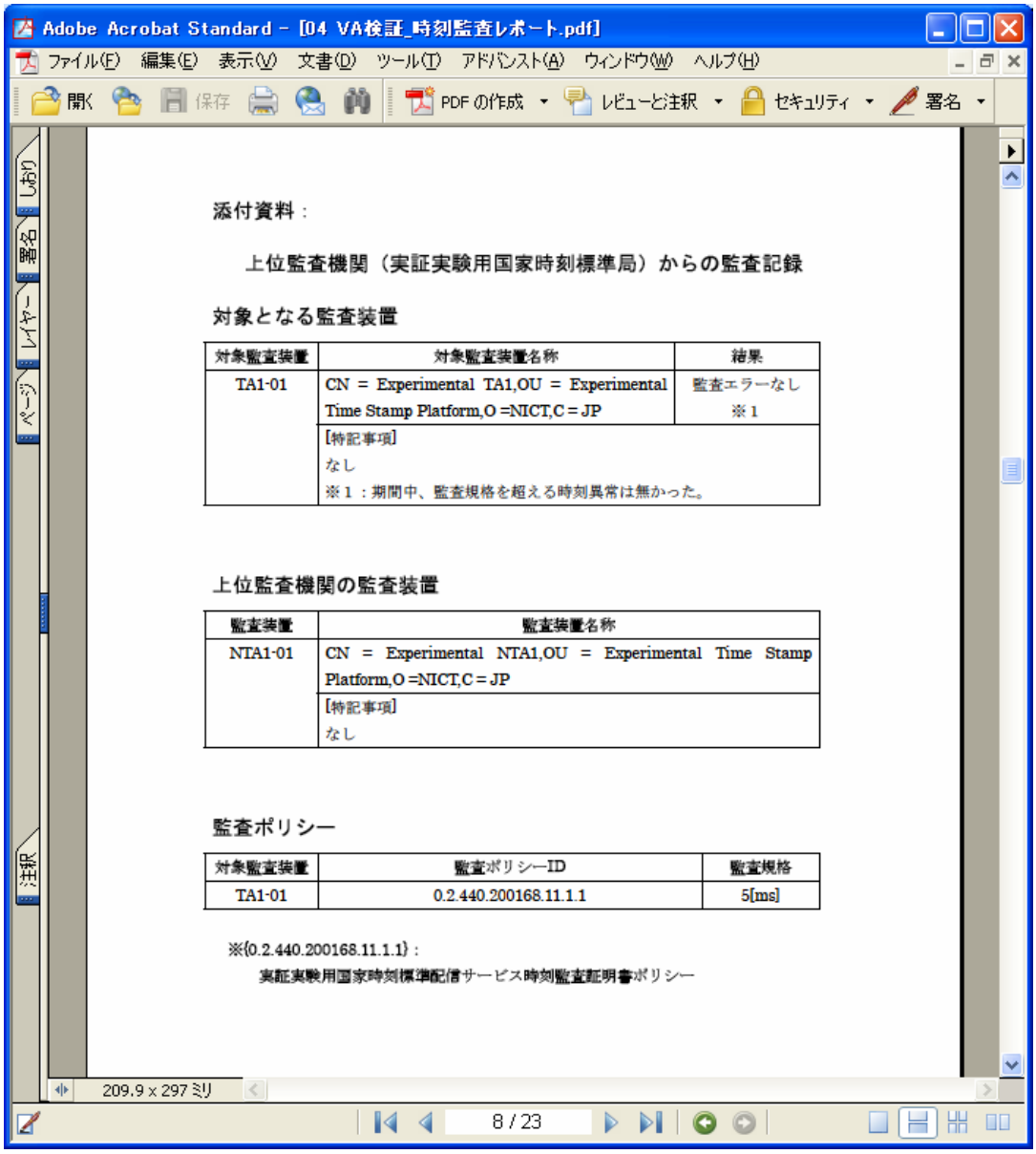
監査記録

対象装置：TSA1-01

監査日時 (YYYYMMDDhhmm.ss.sss)	Offset[us]	Delay[us]	監査装置	備考
200512130044.06.585	-3068	57121	TA1-01	
200512130244.07.581	-2356	56581	TA1-01	
200512130444.08.386	583	57106	TA1-01	
200512130644.09.573	1883	54936	TA1-01	
200512130844.10.425	-449	55713	TA1-01	
200512131044.11.428	1062	55884	TA1-01	
200512131244.12.489	-1160	55852	TA1-01	
200512131444.13.529	957	57005	TA1-01	
200512131644.14.423	657	55593	TA1-01	
200512131844.15.362	720	55906	TA1-01	
200512132044.16.429	-249	57010	TA1-01	
200512132244.17.412	705	55109	TA1-01	
200512140044.18.445	-2133	54928	TA1-01	
200512140244.19.488	-2215	56153	TA1-01	
200512140444.20.493	-319	55930	TA1-01	
200512140644.21.533	-2214	57129	TA1-01	
200512140844.22.526	-606	55948	TA1-01	
200512141044.23.372	6646	56988	TA1-01	
200512141244.24.564	4984	56100	TA1-01	
200512141444.25.585	1520	56617	TA1-01	
200512141644.26.410	-1823	56059	TA1-01	

図 2-39　TSA1 に対する監査記録

以下に、TA に対する NTA の監査規格を示す。



添付資料：

上位監査機関（実証実験用国家時刻標準局）からの監査記録

対象となる監査装置

対象監査装置	対象監査装置名称	結果
TA1-01	CN = Experimental TA1,OU = Experimental Time Stamp Platform,O =NICT,C = JP	監査エラーなし ※1
	[特記事項] なし ※1：期間中、監査規格を超える時刻異常は無かった。	

上位監査機関の監査装置

監査装置	監査装置名称
NTA1-01	CN = Experimental NTA1,OU = Experimental Time Stamp Platform,O =NICT,C = JP
	[特記事項] なし

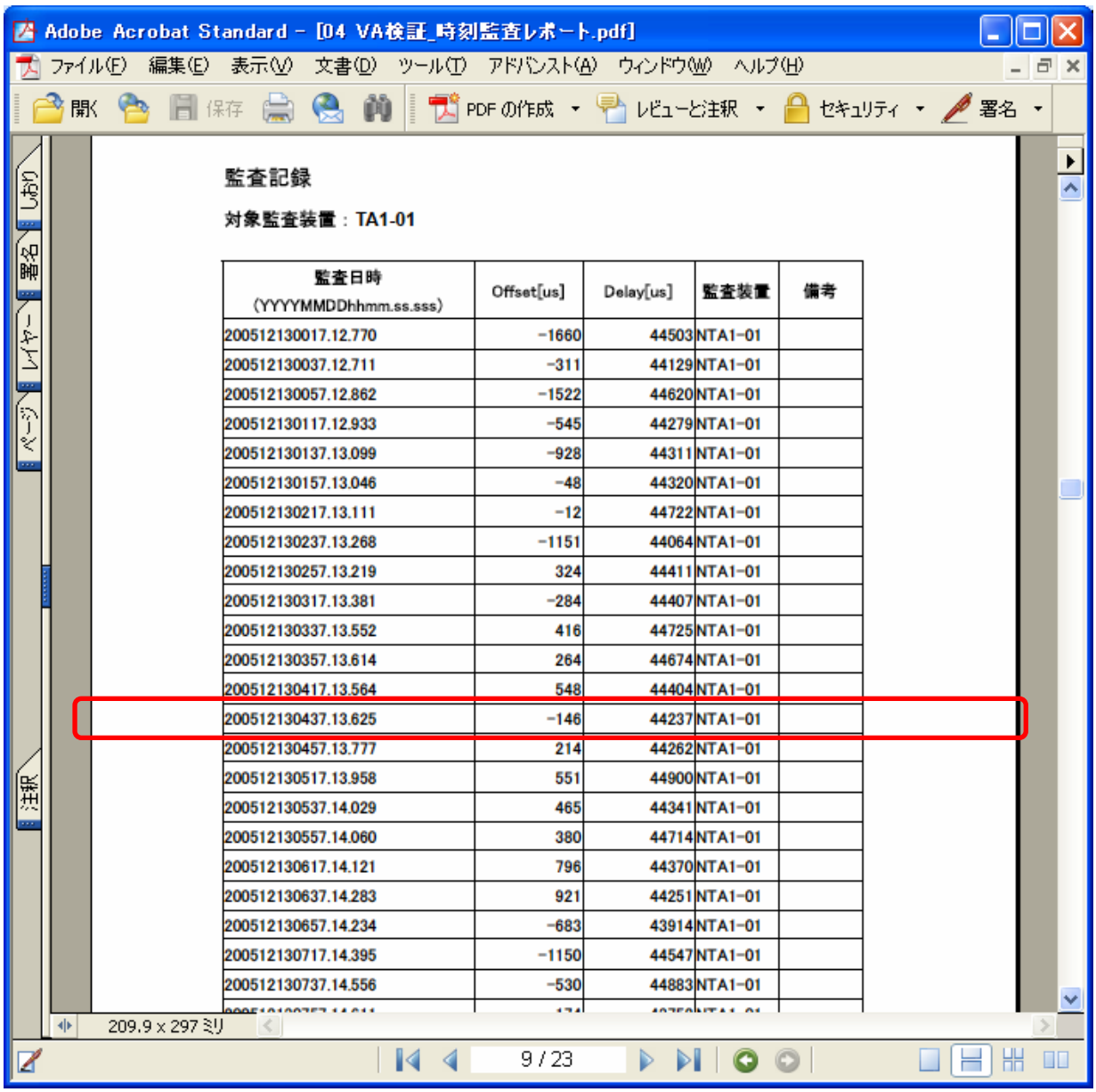
監査ポリシー

対象監査装置	監査ポリシーID	監査規格
TA1-01	0.2.440.200168.11.1.1	5[ms]

※{0.2.440.200168.11.1.1}：
実証実験用国家時刻標準配信サービス時刻監査証明書ポリシー

図 2-40　NTA-TA の監査情報

以下に、TA に対する監査記録を示す。



監査記録

対象監査装置：TA1-01

監査日時 (YYYYMMDDhhmm.ss.sss)	Offset[us]	Delay[us]	監査装置	備考
200512130017.12.770	-1660	44503	NTA1-01	
200512130037.12.711	-311	44129	NTA1-01	
200512130057.12.862	-1522	44620	NTA1-01	
200512130117.12.933	-545	44279	NTA1-01	
200512130137.13.099	-928	44311	NTA1-01	
200512130157.13.046	-48	44320	NTA1-01	
200512130217.13.111	-12	44722	NTA1-01	
200512130237.13.268	-1151	44064	NTA1-01	
200512130257.13.219	324	44411	NTA1-01	
200512130317.13.381	-284	44407	NTA1-01	
200512130337.13.552	416	44725	NTA1-01	
200512130357.13.614	264	44674	NTA1-01	
200512130417.13.564	548	44404	NTA1-01	
200512130437.13.625	-146	44237	NTA1-01	
200512130457.13.777	214	44262	NTA1-01	
200512130517.13.958	551	44900	NTA1-01	
200512130537.14.029	465	44341	NTA1-01	
200512130557.14.060	380	44714	NTA1-01	
200512130617.14.121	796	44370	NTA1-01	
200512130637.14.283	921	44251	NTA1-01	
200512130657.14.234	-683	43914	NTA1-01	
200512130717.14.395	-1150	44547	NTA1-01	
200512130737.14.556	-530	44883	NTA1-01	

図 2-41　TA に対する監査記録

6-4-2 デジタル署名を使用する方式のタイムスタンプでの時刻トレーサビリティの確認

本試験では、デジタル署名を使用する方式のタイムスタンプの時刻トレーサビリティの確認を行った。

表 2-24　デジタル署名を使用する方式のタイムスタンプの時刻トレーサビリティ確認

対象データ	0000000159_keiyaku_1.pdf
デジタル署名を使用する方式のタイムスタンプトークン	0000000159_tsa2_1.tst
TSA2 の時刻精度及び配信経路の確認	VA クライアントに表示される時刻トレーサビリティ情報を参照
TA の時刻精度及び配信経路の確認	VA クライアントに表示される時刻トレーサビリティ情報を参照
「試験結果」 VA クライアントに表示される時刻トレーサビリティ情報を参照し、時刻精度及び時刻配信経路を検証できることを確認した。	

表 2-25　TSA2 の時刻トレーサビリティ確認結果

TST2 時刻情報 (JST) (*1)	TA-TSA2 間の時刻監査結果[sec]	NTA-TA 間の時刻監査結果[sec]	時刻誤差の合計 [sec](*2)
2005/12/13 14:13:10.637755	-0.002009	0.000214	0.002223

***1** TST2 は TSA2 の発行したタイムスタンプトークンを表す。

***2** 時刻誤差の合計は、TA-TSA2 間の時刻監査結果、NTA-TA 間の時刻監査結果の絶対値の和である。

以下の図に、デジタル署名を使用する方式のタイムスタンプの時刻トレーサビリティの確認において、時刻トレーサビリティの情報が表示されている箇所を示す。

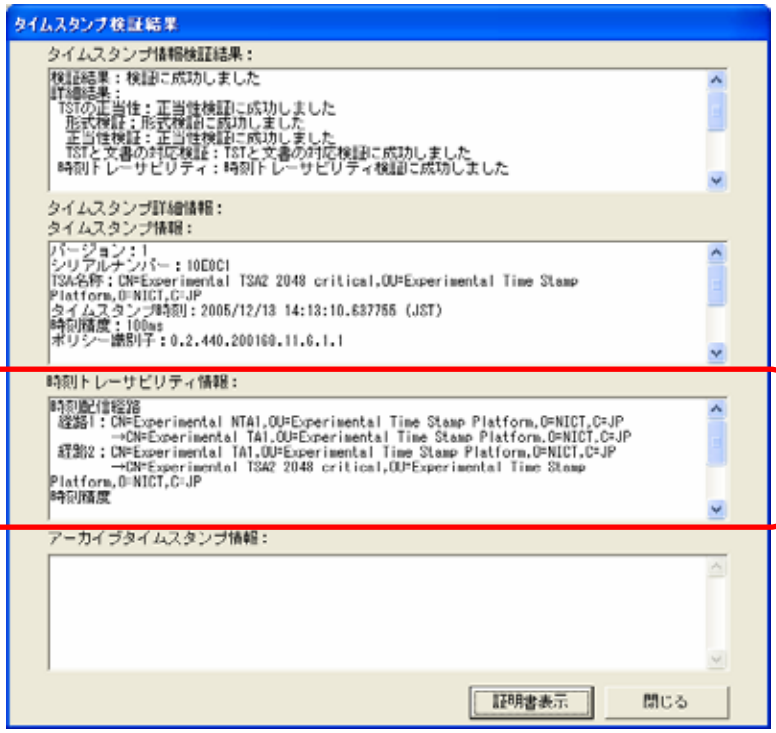


図 2-42　配信経路の確認（時刻トレーサビリティ情報スクロール前）

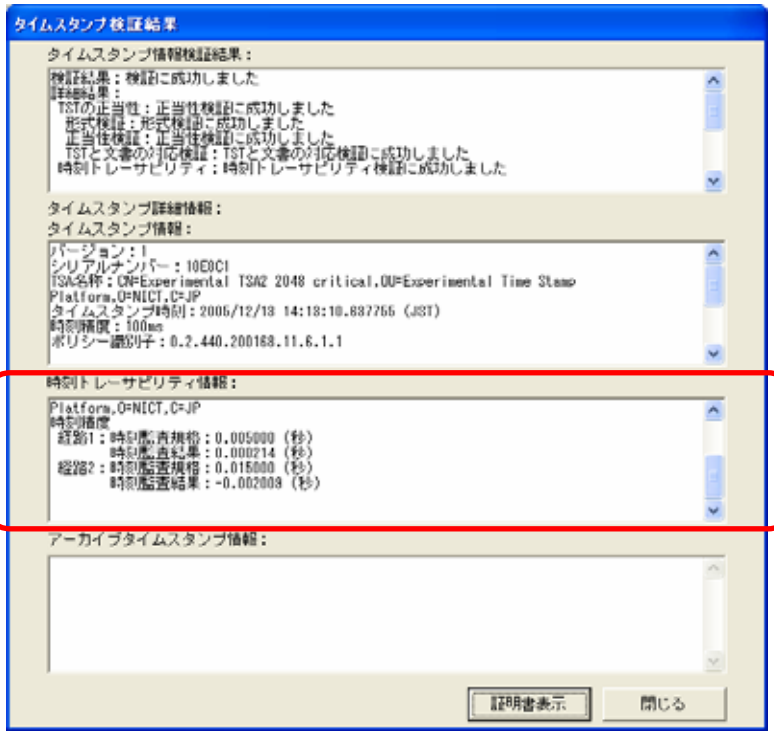


図 2-43　誤差情報の確認（時刻トレーサビリティ情報スクロール後）

6-4-3 時刻トレーサビリティの確認方法の比較

時刻トレーサビリティの検証において、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では時刻監査レポートを確認する時刻監査レポート確認方式、デジタル署名を使用する方式のタイムスタンプでは時刻監査証明書を確認する時刻監査証明書確認方式が採用されている。

両方式について、表 2-26 では利用者の観点からの評価結果、表 2-27 では TSA 構築時の影響に関する評価結果を示す。

表 2-26　時刻トレーサビリティ確認方式の違いによる利用者への影響

<table>
<tr><td></td><td colspan="2">時刻監査レポート確認方式</td><td>時刻監査証明書確認方式</td></tr>
<tr><td rowspan="3">確認が可能になるまでの期間</td><td colspan="2">タイムスタンプ発行直後、時刻監査レポートの発行間隔程度の間は、時刻トレーサビリティを確認できない。</td><td>タイムスタンプ発行直後に時刻トレーサビリティの確認が行える。</td></tr>
<tr><td colspan="2">△</td><td>○</td></tr>
<tr><td colspan="3">タイムスタンプの時刻情報の信頼性を確認する場合、タイムスタンプ発行直後にも確認が可能である、時刻監査証明書確認方式が即時性に優れる。</td></tr>
<tr><td rowspan="3">確認時の利便性</td><td>PDF ファイルで表示する必要がある。またタイムスタンプ付与時刻から時刻監査レポート上の監査記録を検索し、目的の監査記録を得る必要がある。</td><td>検証用ソフトウェアにより、時刻トレーサビリティ確認の自動化が実現されている。</td></tr>
<tr><td>△</td><td>○</td></tr>
<tr><td colspan="2">VA クライアントの検証結果画面において時刻トレーサビリティ情報が確認できる時刻監査証明書確認方式が、利便性に優れる。時刻監査レポート確認方式では、時刻トレーサビリティ情報を確認するために、PDF ファイル表示ソフトを立ち上げる等の更なる操作が必要となる。また、時刻監査レポートが検証対象のタイムスタンプを発行した TSA に対する監査記録であることを、検証者が確認する必要がある。</td></tr>
<tr><td rowspan="2">時刻監査情報の取得容易性</td><td>時刻監査レポートは TSA より公開されているため、TST の流通時にもインターネット経由で取得し、確認できる。</td><td>時刻監査証明書はタイムスタンプトークンと一体となっているため、タイムスタンプトークンの流通時にも失われることなく確認できる。</td></tr>
<tr><td>○</td><td>○</td></tr>
</table>

	時刻監査レポート確認方式	時刻監査証明書確認方式
	いずれの方式においても、必要時に時刻監査情報を容易に入手することが可能である。	
オフラインでの検証	タイムスタンプトークンを入手しても、インターネットに接続できる環境でない場合は、時刻トレーサビリティを確認できない。	タイムスタンプトークンや検証用の情報があれば、インターネットと接続できない環境でも、ローカルで時刻トレーサビリティを確認できる。
	△	○
	時刻監査証明書確認方式では、タイムスタンプトークンと検証用の情報があれば、オフラインでも時刻トレーサビリティが確認可能である。ただし時刻監査レポート確認方式でも、タイムスタンプと共に時刻監査レポートを流通させれば、確認可能である。	
時刻精度の経過確認	タイムスタンプ発行前後の一定期間の時刻同期精度の経過を確認できる。	タイムスタンプ発行直前の時刻同期精度しか確認できず、一定期間の時刻同期精度の経過を確認できない。
	○	△
	タイムスタンプ発行前後の一定期間の時刻同期精度は、時刻監査証明書確認方式では確認することができず、時刻監査レポート確認方式が優れる。	
汎用性	汎用的な PDF ファイル表示ソフトにより、時刻トレーサビリティを確認できる。	時刻監査証明書の正当性検証や内容の読込み及び表示のため、専用のソフトウェアが必要となる。
	○	△
	汎用的な PDF ファイル表示ソフトで確認可能である時刻監査レポート方式が、汎用性に優れる。	

【凡例】　○：要件を満たす。　△：一部制限がある。　×：要件を満たさない。

時刻監査レポート確認方式及び時刻監査証明書確認方式の運用性の評価としては、表 2-26 にまとめた結果となった。それぞれの方式で機能や利便性等に長所短所があり、利用場面に応じて選択するのが適切であると思われる。

表 2-27　時刻トレーサビリティ確認方式の違いによる TSA 構築時の影響

	時刻監査レポート確認方式	時刻監査証明書確認方式
TSA のシステムとの親和性	一般のタイムスタンプについて本方式を適用する場合、タイムスタンプトークンと時刻監査レポートは独立性が高いため、タイムスタンプのシステム側に大きな改造が必要ない。	一般のタイムスタンプについて本方式を適用する場合、タイムスタンプトークンに時刻監査証明書を包含するため、タイムスタンプのシステム側に改造が必要となる可能性が高い。
	○	△
	タイムスタンプ生成に係る処理と、時刻トレーサビリティを確認するための情報を生成するための処理を分離できる時刻監査レポート確認方式が、TSA 構築時のシステム改造の負荷が少ないと思われる。ただし、時刻監査レポート確認方式では、TA の運用上、TA 側において時刻監査レポート作成し、TSA に送付する処理が必要になる。	
時刻トレーサビリティの確認の自動化	PDF ファイルであり、また確認する箇所がタイムスタンプトークンの時刻情報により変化するため、自動化を行うことは難しい。	タイムスタンプトークン中の値を直接読み込めるため、自動化は容易。
	△	○
	タイムスタンプトークンに時刻監査証明書を包含し、必要な情報を抽出し易い時刻監査証明書確認方式が、時刻トレーサビリティの確認の自動化が容易と考えられる。	

【凡例】　○：TSA 構築時に影響が少ない。　△：TSA 構築時に影響が多い。

タイムスタンプ生成に係る処理と、時刻トレーサビリティを確認するための情報を生成するための処理を分離できる時刻監査レポート確認方式が TSA 構築時のシステム改造の負荷は少ない。ただし、この場合は TSA の時刻精度の監査を行う上位の TA に、時刻監査レポートを生成し TSA に送付する機能が必要になる。

時刻トレーサビリティの確認の自動化については、時刻監査証明書確認方式の方が容易であると考えられる。

6-5 マルチタイムスタンプデータ容量評価

マルチタイムスタンプとした場合に取り扱うデータ容量の変化を測定するため、約 100KBytes、約 1,000KBytes 及び約 10,000KBytes の対象データに対してマルチタイムスタンプを付与し、そのタイムスタンプトークンのファイルサイズを測定した。

表 2-28　タイムスタンプトークンファイルサイズ

試験パターン	対象データサイズ (Byte) (*1)	タイムスタンプトークンファイルサイズ	
		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トークン(Byte)	デジタル署名を使用する方式のタイムスタンプトークン(Byte)(*2)
100K(1 回目)	123,367	255	3,716
100K(2 回目)	123,367	255	3,716
100K(3 回目)	120,197	255	3,716
100K(4 回目)	120,021	255	3,712
100K(5 回目)	120,073	255	3,716
100K 平均(*3)	**121,405**	**255**	**3,715**
1,000K(1 回目)	1,042,054	255	3,714
1,000K(2 回目)	1,023,684	255	3,714
1,000K(3 回目)	1,042,076	255	3,714
1,000K(4 回目)	1,023,672	255	3,714
1,000K(5 回目)	1,042,072	255	3,713
1,000K 平均(*3)	**1,034,712**	**255**	**3,714**
10,000K(1 回目)	10,048,464	255	3,716
10,000K(2 回目)	10,048,462	255	3,716
10,000K(3 回目)	10,048,470	255	3,716
10,000K(4 回目)	10,048,449	255	3,713
10,000K(5 回目)	10,048,465	255	3,716
10,000K 平均(*3)	**10,048,462**	**255**	**3,715**

*1 Acrobat 上でデジタル署名を付与したためサイズは同一にならない。（描画する署名マークの大きさに影響を受ける）
*2 デジタル署名を使用する方式のタイムスタンプのサイズは、GeneralizedTime の桁数（小数部の最後の桁が 0 の場合は省略）、誤差が負になる場合の指定等により一定と成らない。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 GeneralizedTime は整数部までであり、また誤差の情報を保持しないためサイズは一定となる。
*3 平均値は小数点以下を四捨五入している。

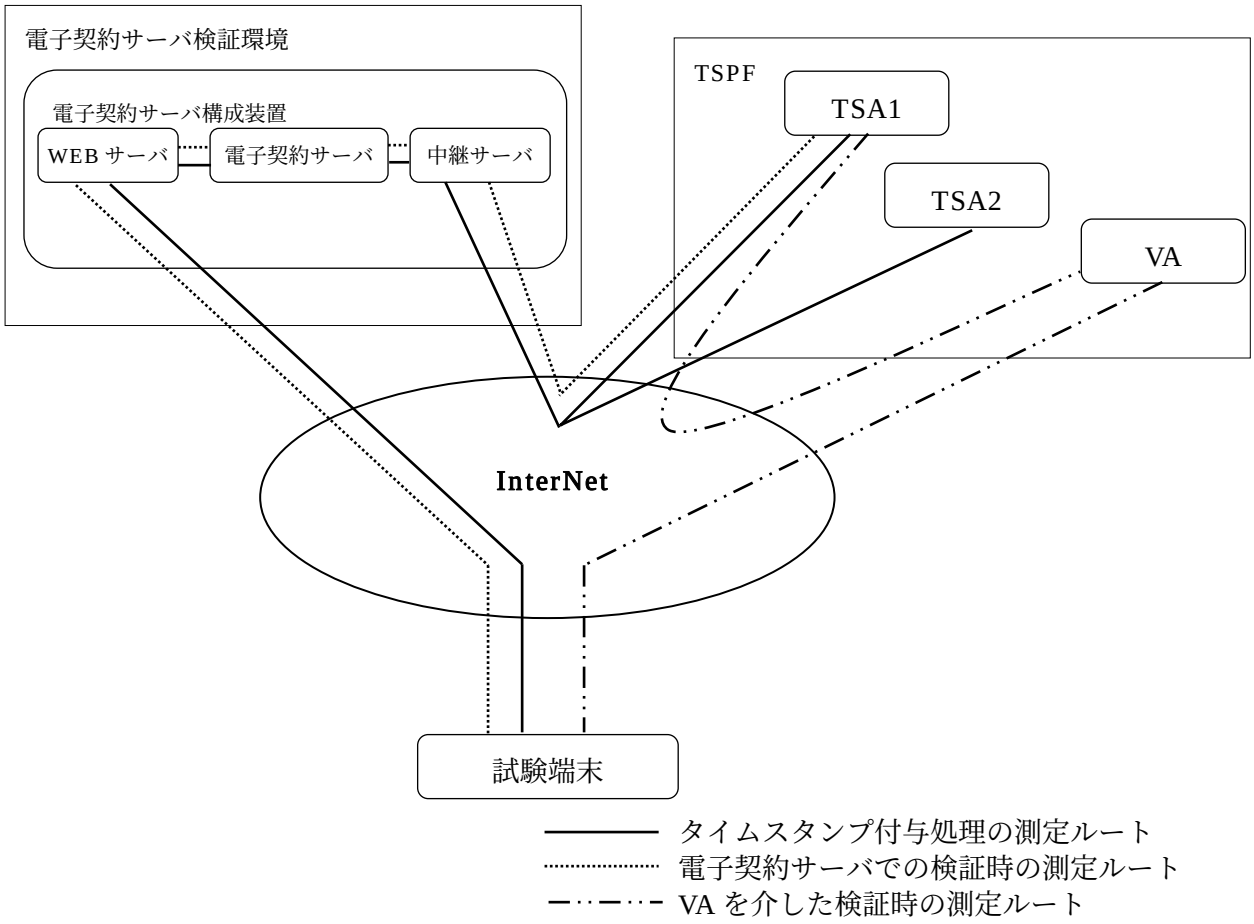
表 2-28 の結果より、タイムスタンプトークンのサイズはリンク情報を使用するアーカイビング方式のタイムスタンプで、255Bytes、デジタル署名を使用する方式のタイムスタンプで約 3,715Bytes となる。対象データにマルチタイムスタンプを付与した場合に増えるデータ量としては、このタイムスタンプトークンのサイズを足した値となる。現在、商用の電子契約サービスに登録されているデータの内容は A4 サイズの PDF ファイルが多く、そのサイズは数十 KBytes 程度である。仮に対象データのサイズを 50KBytes とした場合、対象データに対するタイムスタ

ンプトークンのデータサイズの比率は、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トークンで約 0.5%、デジタル署名を使用する方式のタイムスタンプトークンで約 7.2%となる。これは、利用者がダウンロードし、メールに添付して検証者に送付するような場面を想定すると、さほど影響が出る値ではないと考えられる。しかし電子契約サーバ等、多数のタイムスタンプトークンを内部で保存する場合には、このデータ容量を考慮した設計を行う必要がある。

6-6 マルチタイムスタンプ付与及び検証処理時間性能評価

タイムスタンプ付与及び検証の処理能力を測定するため、約 100KBytes、約 1,000KBytes 及び約 10,000KBytes の対象データに対してマルチタイムスタンプの付与及び検証を行い、その処理時間を測定した。マルチタイムスタンプ付与及び電子契約サーバでの検証に要する時間は電子契約サーバのログから測定し、VA を介した検証に要する時間は VA のログより測定した。本測定値は電子契約サーバ及び VA 内の処理時間であり、操作端末内の処理時間及び操作端末とサーバ間の通信処理に要する時間は含まれていない。

以下に実証実験の処理時間測定に係る装置構成を示す。



WEB サーバ　　：ユーザとのインターフェース部分の処理を行う。
電子契約サーバ　：対象データの格納、検索及びタイムスタンプ付与要求等を行う。
中継サーバ　　：タイムスタンプ付与及び検証時のハッシュ計算、タイムスタンプトークン内のハッシュ値と対象データから計算したハッシュ値の比較ならびに TSA に対するタイムスタンプ付与要求及び確認要求を行う。

※DB サーバは電子契約サーバと一体のため、本図では記載していない。

図 2-44　処理能力測定対象装置接続図

6-6-1　処理能力測定に係る装置スペック

以下に処理能力測定に係る装置のスペックを記す。

表 2-29　TSA1 スペック

使用機材	IBM xSeries 225
CPU	Xeon　2.80GHz×2
メモリ	2GB
OS	Linux AdvancedServer2.1

表 2-30　TSA2 スペック

使用機材	DELL PowerEdge 650
CPU	Pentium4　2.4GHz
メモリ	1GB
OS	Red Hat Professional Workstation

表 2-31　VA スペック

使用機材	Sun Blade 150
CPU	UltraSPARC IIi 550MHz
メモリ	640MB
OS	Solaris 8

表 2-32　WEB サーバ スペック

使用機材	Sun Fire V100
CPU	UltraSPARC IIi 550MHz
メモリ	1GB
OS	Solaris 8

表 2-33　電子契約サーバ スペック

使用機材	Sun Fire V100
CPU	UltraSPARC IIi 550MHz
メモリ	1GB
OS	Solaris 8

表 2-34　DB サーバ スペック

使用機材	Sun Fire V100
CPU	UltraSPARC IIi 550MHz
メモリ	1GB
OS	Solaris 8

表 2-35　中継サーバ スペック

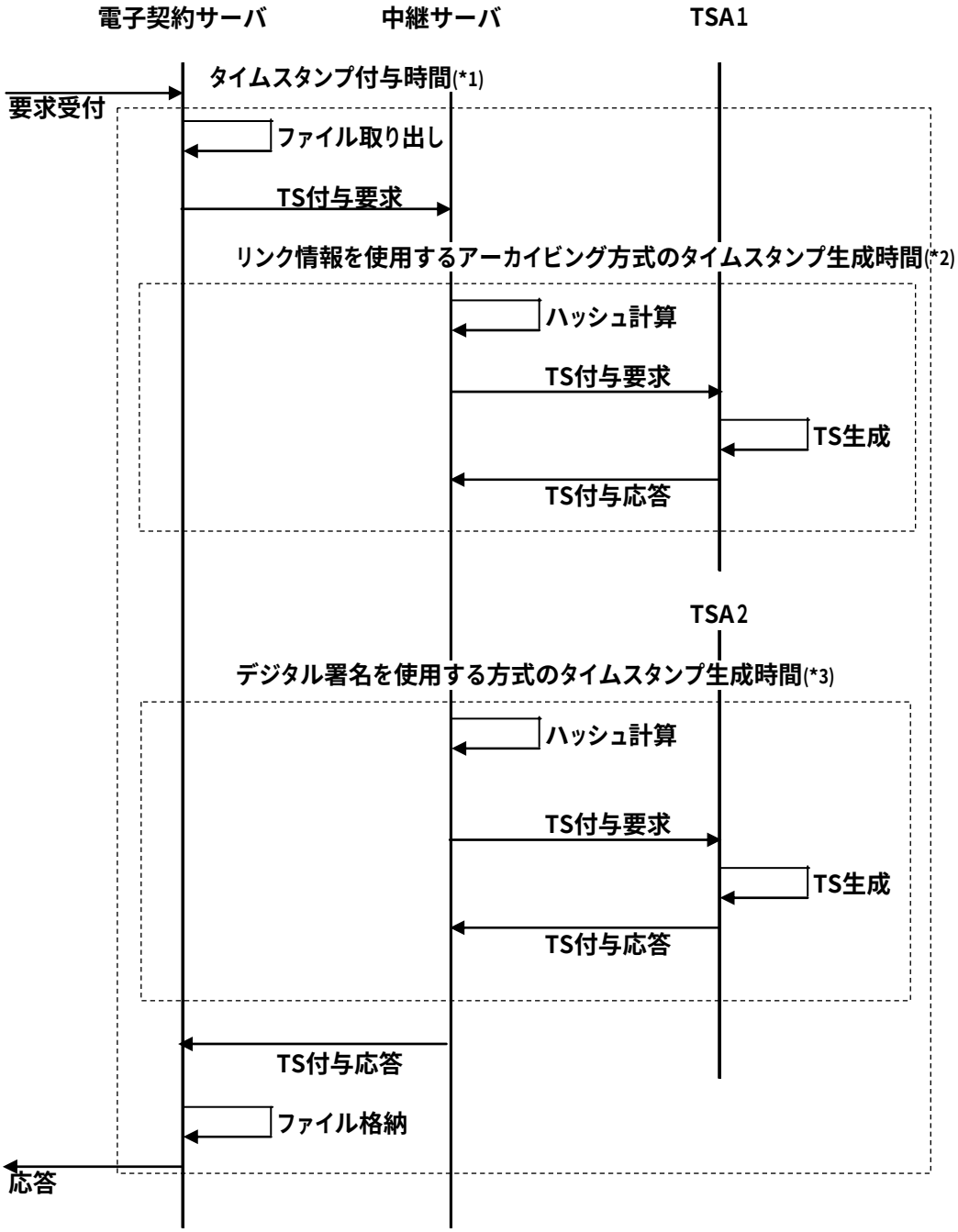
使用機材	PowerEdge 850 SATA 構成スタンダードパッケージ
CPU	Celeron 2.53GHz
メモリ	512MB
OS	Windows Server2003 SP1

表 2-36　試験端末 スペック

使用機材	HP　Compaq dc5100 SFF
CPU	Pentium(R)4 2.80GHz
メモリ	512MB
OS	Windows XP Professional SP2

6-6-2 処理速度測定における処理フロー

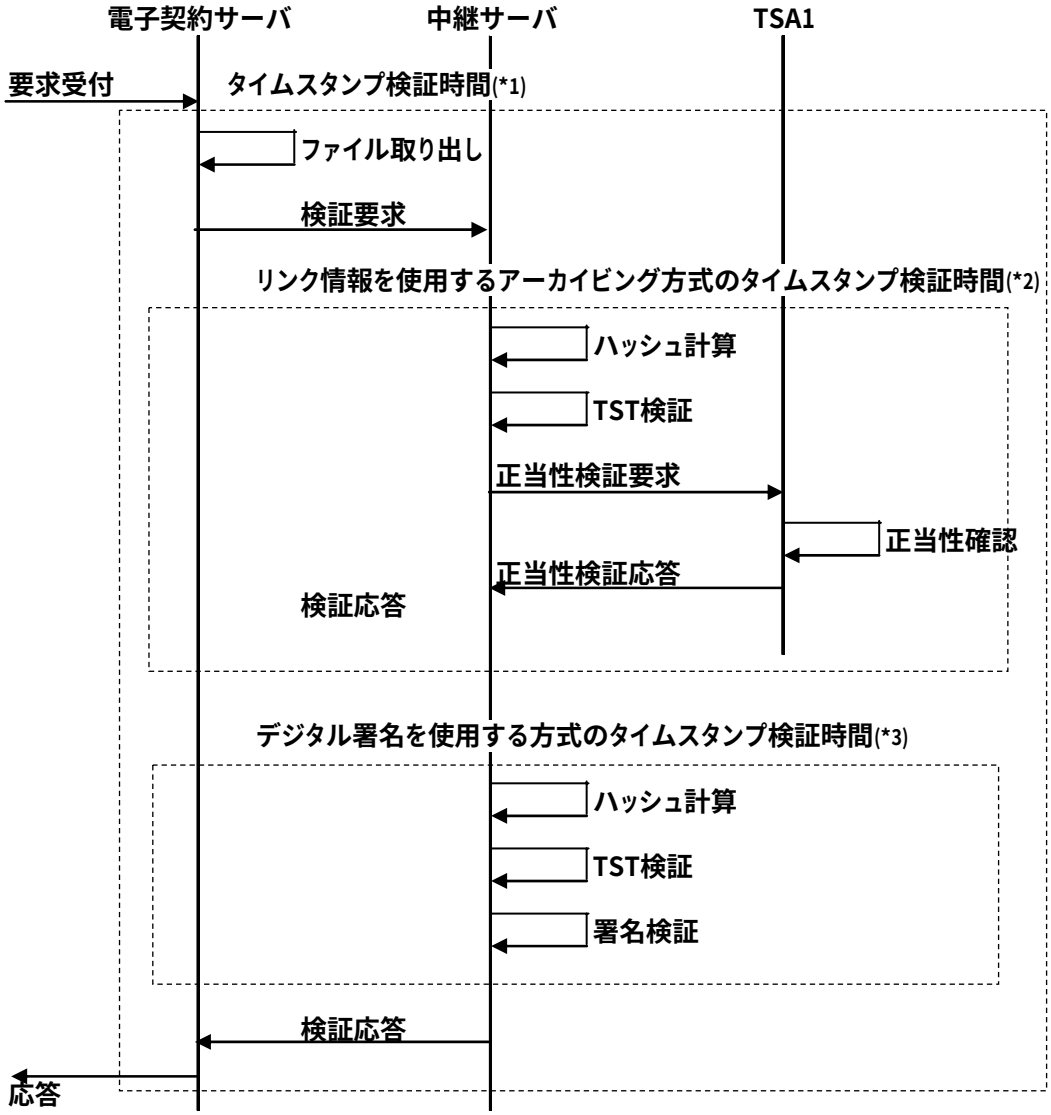
以下にタイムスタンプ付与時の電子契約サーバ及び中継サーバ内でのシーケンスを示す。



*1 **表** 2-37 で計測したタイムスタンプ付与時間の処理。
*2 **表** 2-37 で計測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生成処理。
*3 **表** 2-37 で計測したデジタル署名を使用した方式のタイムスタンプの生成処理。

図 2-45　タイムスタンプ付与シーケンス

以下にタイムスタンプ検証時の電子契約サーバ及び中継サーバ内でのシーケンスを示す。



*1 **表** 2-37 で計測した電子契約サーバでの検証処理。
*2 **表** 2-37 で計測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処理。
*3 **表** 2-37 で計測したデジタル署名を使用した方式のタイムスタンプの検証処理。

図 2-46　タイムスタンプ検証シーケンス

6-6-3 マルチタイムスタンプ付与及び検証時間測定結果

測定結果を表 2-37 に示す。

表 2-37　タイムスタンプ付与及び検証時間

試験パターン	対象データサイズ (Byte) (*1)	方式 (*2)	タイムスタンプ付与時間		電子契約サーバでの検証時間		VA での検証時間 ( )は TAC 検証時間 (sec)(*5)
			全体 (sec) (*3)	タイムスタンプ生成時間 (msec) (*4)	全体 (sec) (*3)	タイムスタンプ検証時間 (msec)(*4)	
100K_1	123,367	リンク	6	125	1	593	9
		署名		734		32	9(4)
100K_2	123,367	リンク	4	94	1	563	9
		署名		735		31	8(3)
100K_3	120,197	リンク	5	94	1	579	8
		署名		718		31	8(3)
100K_4	120,021	リンク	4	94	1	547	6
		署名		719		31	7(3)
100K_5	120,073	リンク	5	110	1	579	7
		署名		719		15	8(3)
100K 平均		**リンク**	**4.8**	**103.4**	**1.0**	**572.2**	**7.8**
		署名		**725.0**		**28.0**	**8.0(3.2)**
1,000K_1	1,042,054	リンク	5	250	2	703	9
		署名		813		109	7(4)
1,000K_2	1,023,684	リンク	5	250	2	687	8
		署名		813		109	7(4)
1,000K_3	1,042,076	リンク	6	266	1	703	7
		署名		812		109	7(3)
1,000K_4	1,023,672	リンク	5	282	1	672	8
		署名		797		110	8(4)
1,000K_5	1,042,072	リンク	5	250	1	859	9
		署名		812		125	8(4)
1,000K 平均		**リンク**	**5.2**	**259.6**	**1.4**	**724.8**	**8.2**
		署名		**809.4**		**112.4**	**7.4(3.8)**
10,000K_1	10,048,464	リンク	9	1,485	15	2,266	23
		署名		1,672		938	23(4)
10,000K_2	10,048,462	リンク	13	1,468	15	2,281	23
		署名		1,657		953	23(4)
10,000K_3	10,048,470	リンク	14	1,468	7	2,250	30
		署名		1,657		953	29(3)
10,000K_4	10,048,449	リンク	18	1,453	7	2,234	30
		署名		1,656		953	32(3)
10,000K_5	10,048,465	リンク	12	1,468	6	2,297	42
		署名		1,641		953	37(3)
10,000K 平均		**リンク**	**13.2**	**1,468.4**	**10.0**	**2265.6**	**29.6**
		署名		**1,656.6**		**950.0**	**28.8(3.4)**

*1 Acrobat 上でデジタル署名を付与したためサイズは同一にならない。（描画する署名マークの大きさに影響を受ける）
*2 リンク：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／署名：デジタル署名を使用する方式のタイムスタンプ。
*3 電子契約サーバが要求を受け付けてから、結果を返送するまでの時間。
*4 タイムスタンプ生成に要する時間／検証に要する時間。
*5 デジタル署名を使用する方式のタイムスタンプを検証する際、同時に TAC（時刻監査証明書）検証が行われる。

6-6-4 付与時間

表 2-37 の結果より、電子契約サーバ内でタイムスタンプの付与要求を受けてから応答を返すまでに要する時間は、対象データが 100KBytes の場合約 4.8 秒、1,000KBytes の場合約 5.2 秒、10,000KBytes の場合約 13.2 秒である。この内、タイムスタンプの生成に要する時間は、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で、対象データが 100KBytes の場合は約 0.10 秒、1,000KBytes の場合約 0.26 秒、10,000KBytes の場合約 1.47 秒である。デジタル署名を使用する方式のタイムスタンプでは、対象データが 100KByte の場合は約 0.73 秒、1,000KBytes の場合約 0.81 秒、10,000KBytes の場合約 1.66 秒である。

タイムスタンプ付与に要する時間のうち、生成自体の時間の割合はそれぞれリンク情報を使用するアーカイビング方式で 100KBytes の場合は 2%、1,000KBytes の場合 5%、10,000KBytes の場合 11%、デジタル署名を使用する方式のタイムスタンプで 100KBytes の場合で 15%、1,000KBytes の場合 16%、10,000KBytes の場合 13% となる。

これは付与に要する時間の内、多くが対象データの DB からの取り出しに要する I/O の処理等に使われ、タイムスタンプ生成に要する時間は比較的に少ないためと思われる。

このことから、マルチタイムスタンプにした場合でも処理時間の増加は僅かであり、大きな負荷とはならないと考えられる。

以下に、対象データのサイズ毎のタイムスタンプ付与時間（全体）をグラフにしたものを示す。

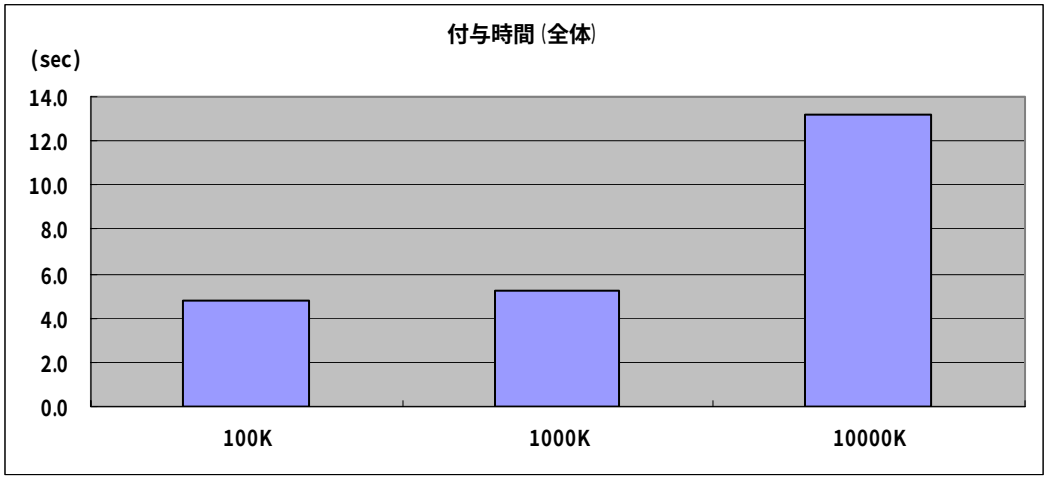


図 2-47　タイムスタンプ付与時間（全体）

以下に、対象データのサイズ毎の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生成の時間をグラフにしたものを示す。

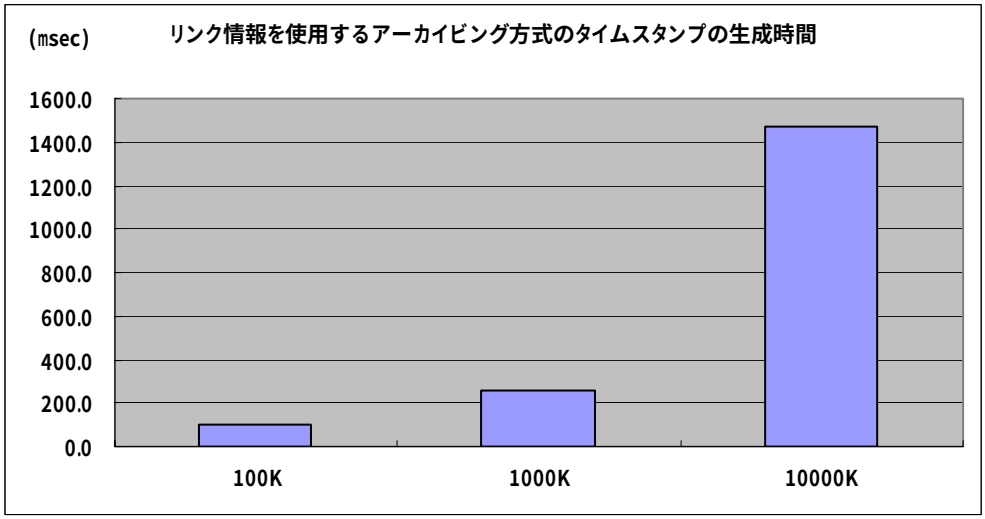


図 2-48　リンク情報を使用するアーカイビング方式のタイムスタンプ生成時間

以下に、対象データのサイズ毎のデジタル署名を使用する方式のタイムスタンプ生成の時間をグラフにしたものを示す。

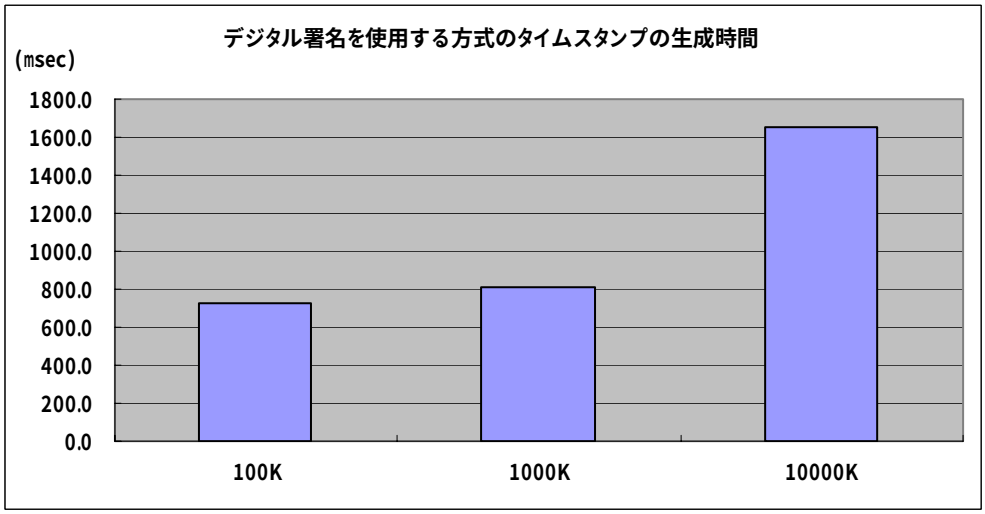


図 2-49　デジタル署名を使用する方式のタイムスタンプ生成時間

6-6-5 電子契約サーバでの検証時間

表 2-37 の結果より、電子契約サーバ内でタイムスタンプ検証要求を受けてから応答を返すまでに要する時間は、対象データが 100KBytes の場合約 1.0 秒、1,000KBytes の場合約 1.4 秒、10,000KBytes の場合約 10.0 秒である。タイムスタンプの検証に要する時間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で、対象データが 100KBytes の場合は約 0.57 秒、1,000KBytes の場合約 0.72 秒、10,000KBytes の場合約 2.27 秒である。デジタル署名を使用する方式のタイムスタンプでは対象データが 100KBytes の場合は約 0.03 秒、1,000KBytes の場合約 0.11 秒、10,000KBytes の場合約 0.95 秒である。

タイムスタンプ検証要求を受けてから応答を返すのに要する時間のうち、検証自体の時間の割合はそれぞれリンク情報を使用するアーカイビング方式で 100KBytes の場合で 57%、1,000KBytes の場合 51%、10,000KBytes の場合 23%、デジタル署名を使用する方式のタイムスタンプで 100KBytes の場合 3%、1000KBytes の場合 8%、10000KBytes の場合 10% となる。

検証に関する処理では、タイムスタンプの検証自体に掛かる割合が多く、対象データに付与するタイムスタンプの数が増えた場合、処理時間の増加は比較的大きい。

実業務に提供する場合には、この処理時間の増加を見込んだシステムの要件を決める必要があると考えられる。

以下に、対象データのサイズ毎のタイムスタンプ検証時間（全体）の違いをグラフにしたものを示す。

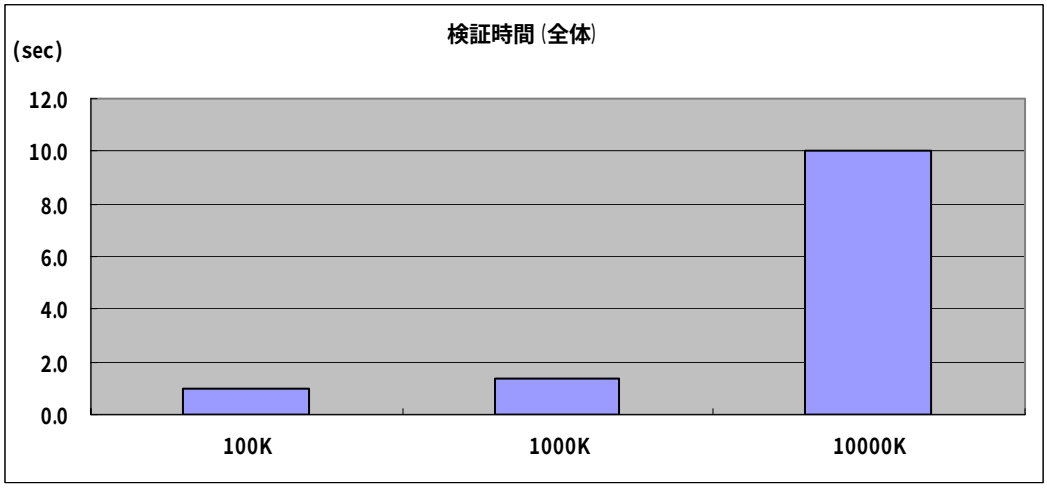


図 2-50　タイムスタンプ検証（全体時間）

以下に、対象データのサイズ毎の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検証時間の違いをグラフにしたものを示す。

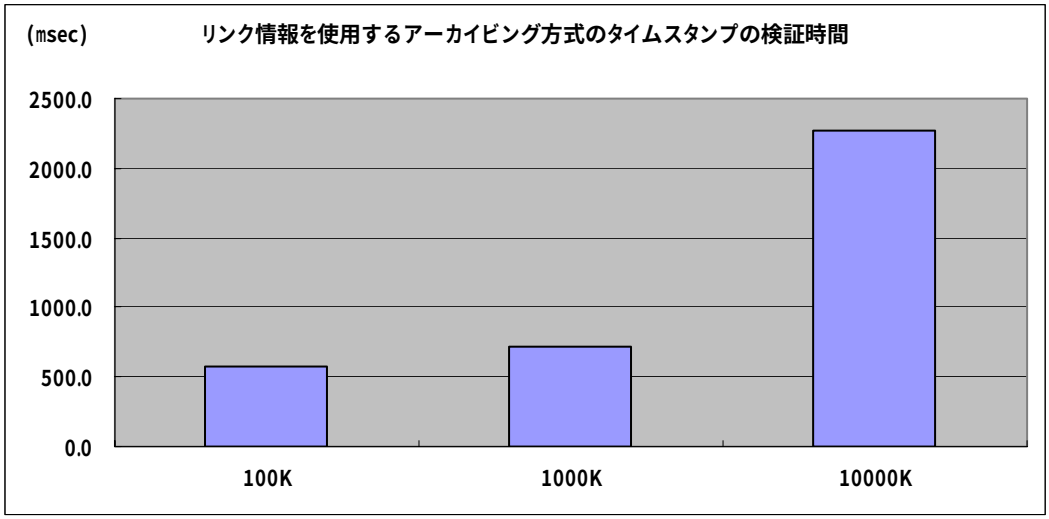


図 2-51　リンク情報を使用するアーカイビング方式のタイムスタンプ検証時間

以下に対象データのサイズ毎のデジタル署名を使用する方式のタイムスタンプ検証時間の違いをグラフにしたものを示す。

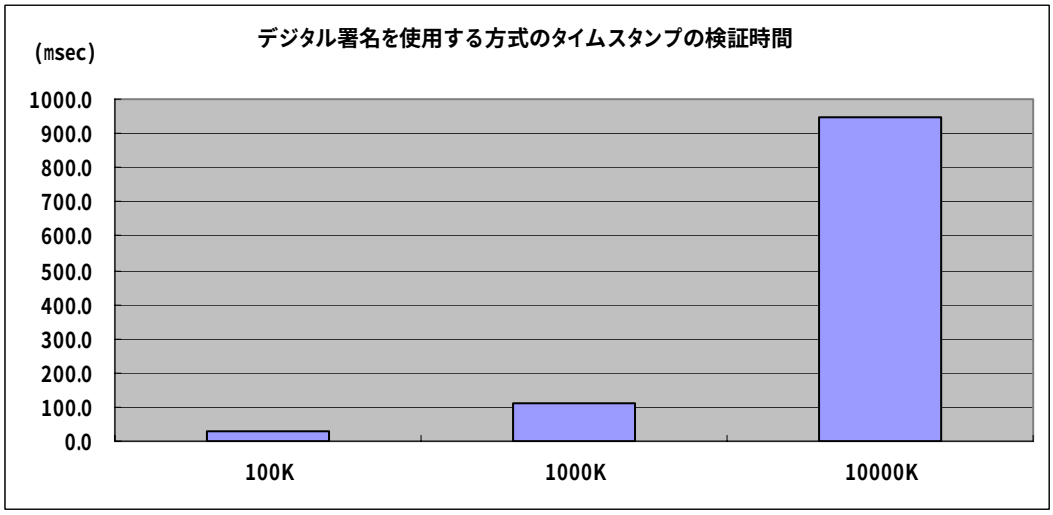


図 2-52　デジタル署名を使用する方式のタイムスタンプ検証時間

6-6-6 VA での検証時間

表 2-37 の結果より、VA での検証に要する時間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ではデータが 100KBytes の場合約 7.8 秒、1,000 KBytes の場合約 8.2 秒、10,000KBytes の場合約 29.6 秒である。デジタル署名を使用する方式のタイムスタンプを検証する場合、100KBytes の場合は約 8.0 秒、1,000KBytes で約 7.4 秒、10,000KBytes で約 28.8 秒である。

VA での検証は、タイムスタンプトークン及び対象データの検証を、その組合せ毎に行う方式である。そのためマルチタイムスタンプとした場合に両方式の検証を実施した場合、それぞれの処理時間を単純に足し合わせた時間が掛かることになる。

マルチタイムスタンプを実業務において使用し、2 方式のタイムスタンプの検証を実施する場合には、この処理時間を見込んだシステムの要件を決める必要があると考えられる。

以下に、対象データのサイズ毎の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及び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間の違いをグラフにしたものを示す。

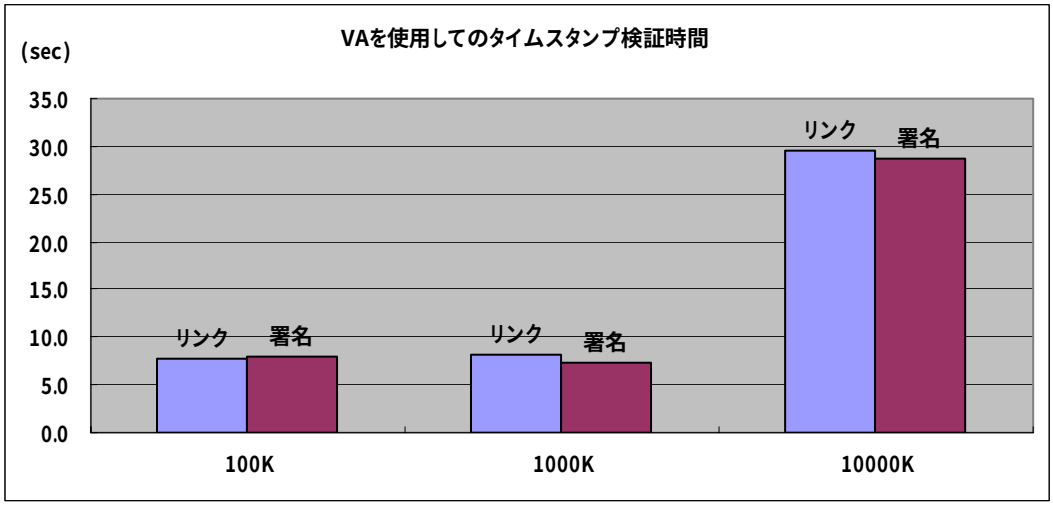


図 2-53　VA 内の検証時間

6-7 マルチタイムスタンプ検証操作性評価

対象データにマルチタイムスタンプを付与する場合の付与処理及び検証処理の操作性を確認するため、マルチタイムスタンプの取得に必要な操作数及び操作時間ならびに検証に必要な操作数及び操作時間について、単一のタイムスタンプを扱う場合と比較した。

なお、今回の実証実験における電子契約サーバを用いてのマルチタイムスタンプの付与及び検証では、単一タイムスタンプを扱う試験アプリケーションは用意しないため、マルチタイムスタンプでの操作数及び処理時間から、表 2-37 で求めた方式毎のタイムスタンプ生成及び検証に係る値を引くことによって差を求めた。また、対象データのサイズによる操作時間の差を求めるため、100KBytes、1,000KBytes 及び 10,000KBytes の対象データに対する署名及びマルチタイムスタンプの付与を行った。

6-7-1 マルチタイムスタンプ付与

電子契約サーバにおいて、登録されている対象データを確定し、電子契約サーバにおいてタイムスタンプの取得を行う操作の操作数及び操作時間を測定した。

なお、操作時間については 5 回測定を実施し、平均を記している。

表 2-38　タイムスタンプの付与に必要な操作数及び操作時間

方式	操作数		操作時間（秒）		
			100KBytes	1,000KBytes	10,000KBytes
マルチタイムスタンプ	ボタン	8 回	48	66	82
リンク情報を使用するアーカイビング方式	ボタン	8 回	47.3(*1)	65.2(*3)	80.3(*5)
デジタル署名を使用する方式	ボタン	8 回	47.9(*2)	65.7(*4)	80.5(*6)

*1 マルチタイムスタンプの操作時間から、デジタル署名を使用する方式のタイムスタンプ生成時間 0.7 秒を引いた値。
*2 マルチタイムスタンプの操作時間から、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生成時間 0.1 秒を引いた値。
*3 同 0.8 秒を引いた値。
*4 同 0.3 秒を引いた値。
*5 同 1.7 秒を引いた値。
*6 同 1.5 秒を引いた値。

以下に、対象データのサイズ毎の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及びデジタル署名を使用する方式のタイムスタンプの付与に必要な操作時間の違いをグラフにしたものを示す。

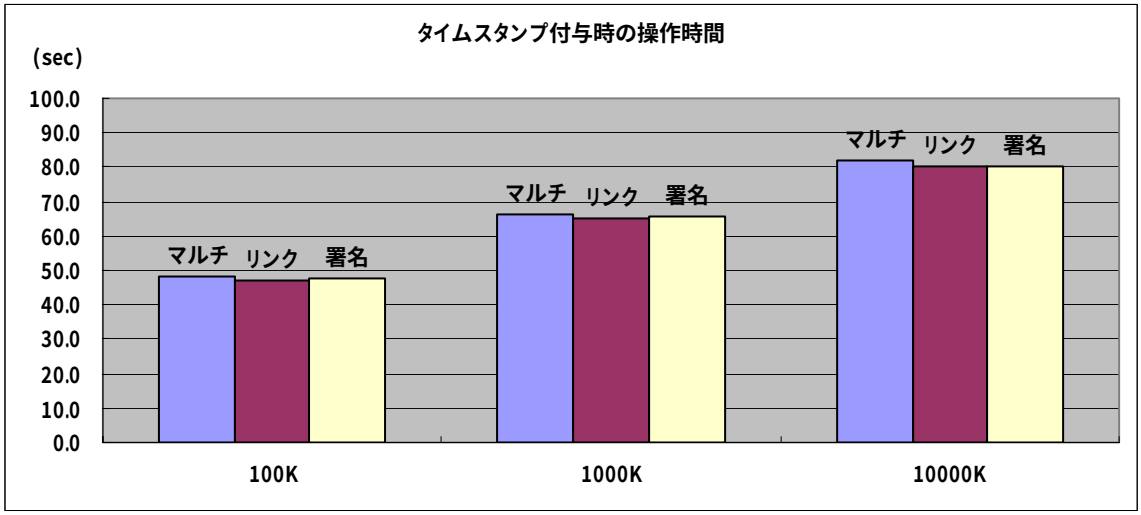


図 2-54　電子契約サーバでのタイムスタンプ取得時間比較

6-7-2 マルチタイムスタンプ検証

(1) VA を使用してのマルチタイムスタンプの検証

VA を用いて、対象データとタイムスタンプトークンの組合せの検証を行う操作の操作数及び操作時間を測定した。

なお、操作時間については 5 回測定を実施し、平均を記している。

表 2-39　VA を介したタイムスタンプ検証

方式	操作数		操作時間（秒）		
			100KBytes	1,000KBytes	10,000KBytes
マルチタイムスタンプ	ボタン	7(*1)	20	30	122
	選択	3(*1)			
リンク情報を使用するアーカイビング方式	ボタン	4	10	16	70
	選択	2			
デジタル署名を使用する方式	ボタン	4	10	14	52
	選択	2			

*1 VA クライアントの検証では、2 方式のタイムスタンプの検証を個々に行うため、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、デジタル署名を使用する方式のタイムスタンプの検証を続けて行った結果の操作数及び時間である。対象データの選択は 1 回のため操作数は個々の検証を行った操作数の和とはならない。

以下に、対象データのサイズ毎のマルチタイムスタンプ、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及びデジタル署名を使用する方式のタイムスタンプの検証に必要な操作時間の違いをグラフにしたものを示す。

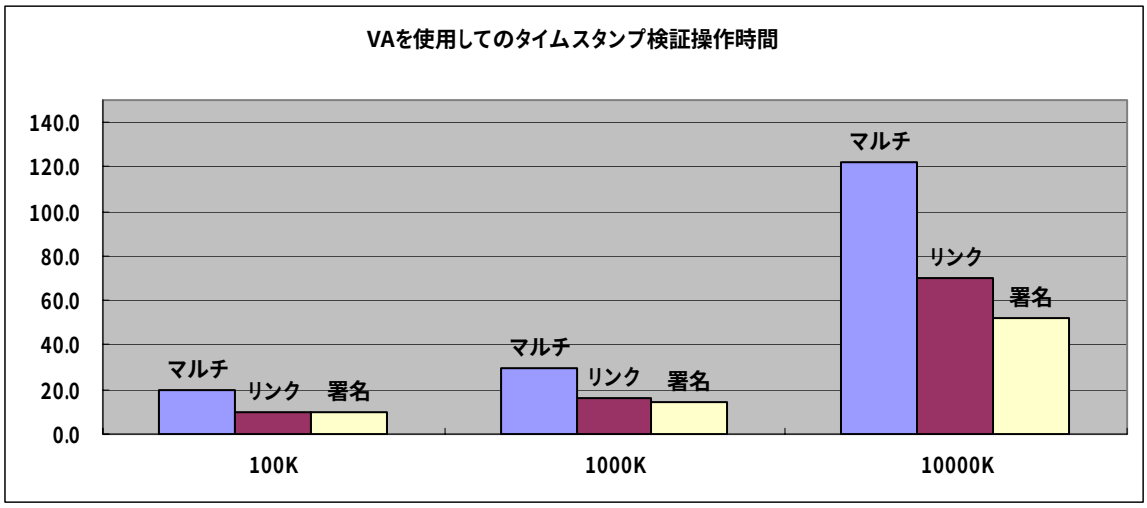


図 2-55　VA でのタイムスタンプ検証時間比較

(2) 電子契約サーバを使用してのマルチタイムスタンプの検証

電子契約サーバを用いて、対象データとタイムスタンプトークンの組合せの検証を行う操作の操作数及び操作時間を測定した。

なお、操作時間については 5 回測定を実施し、平均を記している。

表 2-40　電子契約サービスによるタイムスタンプ検証

方式	操作数		操作時間（秒）		
			100KBytes	1,000KBytes	10,000KBytes
マルチタイムスタンプ	ボタン	2 回	14	15	23
リンク情報を使用するアーカイビング方式	ボタン	2 回	14(*1)	14.9(*3)	22.0(*5)
デジタル署名を使用する方式	ボタン	2 回	13.4(*2)	14.3(*4)	20.8(*6)

*1 マルチタイムスタンプの操作時間から、デジタル署名を使用する方式のタイムスタンプ検証時間 0.03 秒を引いた値
本表では 0 秒として扱う。
*2 マルチタイムスタンプの操作時間から、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検証時間 0.6 秒を引いた値。
*3 同 0.1 秒を引いた値。
*4 同 0.7 秒を引いた値。
*5 同 1.0 秒を引いた値。
*6 同 2.2 秒を引いた値。

以下に、対象データのサイズ毎のマルチタイムスタンプ、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及びデジタル署名を使用する方式のタイムスタンプの検証に必要な操作時間の違いを、グラフにしたものを示す。

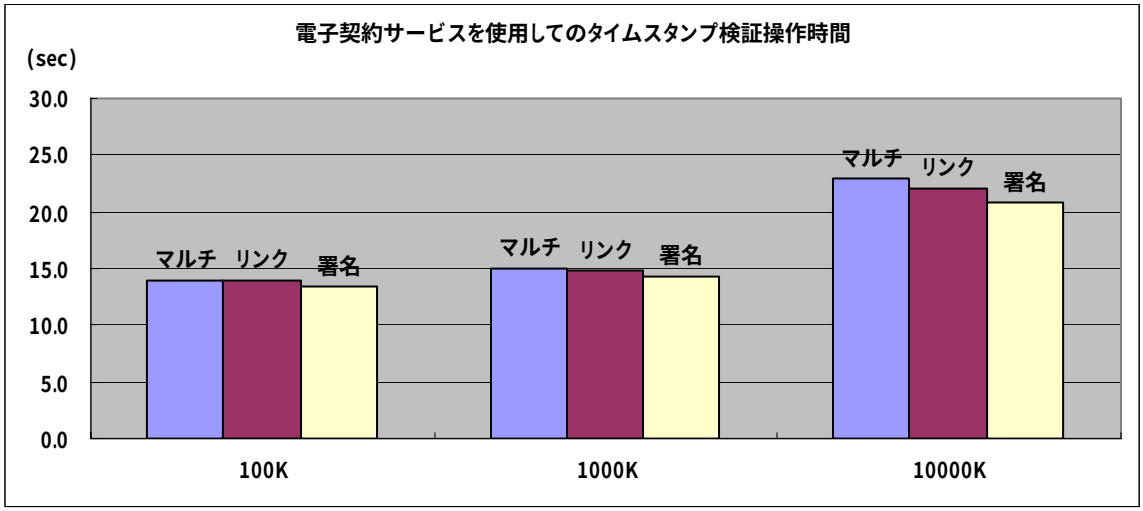


図 2-56　電子契約サーバでのタイムスタンプ検証操作時間比較

6-7-3 マルチタイムスタンプ付与及び検証の操作性について

対象データにマルチタイムスタンプを付与することによる操作時間の増加について、電子契約サーバでのタイムスタンプの付与及び検証では実質的な増加はほとんど見られず、操作性の悪化はないと判断できる。理由として、全体の操作に要する時間がマルチタイムスタンプの付与では 48 秒から 82 秒、マルチタイムスタンプの検証では 14 秒から 23 秒程度であるが、電子契約サーバ内でデジタル署名を使用する方式のタイムスタンプの付与及び検証に要する時間は、測定結果の中で最も長い 10,000KBytes のデータ扱う場合でも 2.3 秒未満であり、全体の操作性を悪化させる程の処理時間の増加が見られないからである。また操作数については、2 方式のタイムスタンプの検証を電子契約サーバ内部で実施しているため、マルチタイムスタンプ化による操作数の違いは発生せず、操作性の悪化はない。

VA での検証において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の検証及びデジタル署名を使用する方式のタイムスタンプの検証を個々に実施するため、両方を合わせた場合には操作時間及び操作数はほぼ足し合わせた値程度必要となる。常に両方式のタイムスタンプの検証を実施するか、片方の検証が成功した場合にそこで終了するかは検証者の判断やサービスのポリシー等により異なるが、片方のタイムスタンプが異常となった場合にのみもう片方の方式のタイムスタンプの検証を行うような運用の場合には、処理時間に関する支障はないと考えられる。

6-8 検証時確認項目充足性評価

電子契約サーバの利用者として建設業界を想定し、検証時に最低限確認する必要がある項目を抽出した。抽出にあたっては、建設業界向けの電子契約サービスを構築した担当者に対するヒアリング結果を参考とした。

表 2-41　検証時に確認する項目

項目名	電子契約サーバ検証で確認可能な項目	VA 検証で確認可能な項目	備考(*1)
発注会社名	○	○	
受注会社名	○	○	
契約責任者（発注会社）	○	○	電子契約書のデジタル署名。電子契約サービスでは、電子契約書にデジタル署名がされていないと登録が行えない。
契約責任者（受注会社）	○	○	電子契約書のデジタル署名。電子契約サービスでは、電子契約書にデジタル署名がされていないと登録が行えない。
案件名(*2)	○	○	
案件番号	○		電子契約サービスでは、電子契約書を登録する際に、システムにて自動付与する。
元案件番号	○		電子契約サービスに登録済みの案件に関連する電子契約書を登録する場合、その案件番号を入力する。
注文番号	○		
契約期間	○	○	
契約締結日	○	○	
契約金額	○	○	
案件内容	○	○	
自由記入欄	○		

*1 備考欄の記述は、電子契約サービスに電子契約書を登録する際の説明である。
*2 契約書の契約名と同義とし、VA 検証で確認可能な項目とした。

ヒアリング結果より、検証時に最低限確認する必要がある項目は、表 2-41 に示す結果となった。電子契約サーバでの検証時には、これら全ての情報が確認できる。一方、VA を介した検証

時には、表 2-41 において○のついていない項目を確認する場合には、利用者が別途通知する必要がある。

実際の業務において VA を介したタイムスタンプ検証を利用する場合は、別途通知が必要な情報も含めて、データの受け渡しまでシステム化するのが望ましいと考えられる。

6-9 利用者側利便性評価

実証実験の一環として、実業務で電子契約を行っている企業の担当者に参加して頂き、マルチタイムスタンプの付与、第三者検証及び時刻トレーサビリティについて評価した。その結果を以下に記す。

1. 第三者検証の実施による利用者側の業務効率の改善について

表 2-42　第三者検証の実施による業務効率の改善

設問	第三者検証が実業務で可能となった場合、業務効率が改善されるか？
回答	・現在、電子契約書を第三者（銀行等）に確認してもらう必要がある場合、印刷を行い本物であることを保証するため、契約を行った両者の印を押す等の対応が必要である。これが不要にできることで業務効率があがる。
考察	現在の電子契約サービスでは、電子契約サービスに加入していない第三者に電子契約の原本性を証明することが難しい。そのため、電子契約を行った場合でも結局印刷を行い、原本であることを担保する捺印を行う等の紙の運用を行わなければならず業務に負荷が生じている。こういった作業を不要にできることで、利用者の業務効率が大幅にあがると考えられる。

2. 電子契約サーバでの第三者検証の評価

表 2-43　電子契約サーバによる第三者検証

設問	電子契約サーバでの第三者検証は、業務上許容できるか？
回答	・検証者が任意の対象データを見読可能な状態になるなら許容できない。 ・特定の対象（物件毎、文書毎）だけを閲覧及び検証可能なようにする必要がある。
考察	今回の実証実験で構築した電子契約サーバでの第三者検証機能は、電子契約サービス利用者の単位で検証用アカウントを発行し、検証を実施するものであった。そのため検証用アカウントに対応する利用者に係る全ての電子契約を検証者が閲覧及び検証できてしまうため、検証者の閲覧可能となる対象データを任意に設定できなければ実運用には耐えないとの評価であった。これらの結果より、実運用に供する場合、検証用アカウントによる閲覧可能範囲を対象データ単位や案件単位等フレキシブルに設定できる機能のニーズが高いと考えられる。

3. VA を介した第三者検証の評価

表 2-44　VA を介した第三者検証

設問	VA を介した第三者検証は、業務上許容できるか？
回答	・送付する際の対象データのセキュリティが確立されなければ許容できない。 ・対象データ及びタイムスタンプトークンの送付を利用者が手動で行うことは煩雑となりすぎ、実業務の中で実施することはできない。 ・検証者が多数の対象データの検証を行う場合、煩雑に成り過ぎる。 ・対象データ及びタイムスタンプトークンのダウンロード及び送付、検証者が検証を行う際のサポートをスマートに実現できるアプリケーションがあるなら業務に適用可能。 ・VA を介した検証では、検証者が実際に検証を行った日時がわからないがこの情報も業務上必要である。
考察	VA を介した第三者検証では、対象データを検証者へ送付する必要がある。この際のセキュリティに不安があるなら業務には適用できないとの回答が多く得られた。また対象データ及びタイムスタンプトークンのダウンロード、検証者への送付及び検証者の検証作業を利用者もしくは検証者が行うには煩雑であるとの意見もあり、これらの業務をサポートするアプリケーションの構築が求められた。また検証者が電子契約文書の検証を行った日時がわからないが、その記録が業務上必要との意見もあった。実運用に供する場合、対象データ及びタイムスタンプトークンの指定及び安全な方法による検証者への送付ならびに検証のサポートについて、支援アプリケーションのニーズが高いと考えられる。また、検証者の特定や検証時間の記録といった機能についても、ニーズがあると思われる。

4. マルチタイムスタンプの必要性

表 2-45　マルチタイムスタンプの必要性

設問	実際の業務を行う際に、一つの対象データに複数のタイムスタンプを付与する必要があるか？
回答	・タイムスタンプの利用者としては、1 つのタイムスタンプによって非改ざん性及び存在日時の証明が行えれば業務上問題なく、現状では不要である。 ・マルチタイムスタンプの目的が、完全性及び安全性の確保ならばタイムスタンプサービス提供側の利用者に対する非改ざん性及び存在日時の証明を長期に渡り保証するための機能提供の保証である。

	・第三者検証を行う場合、検証者が特定のタイムスタンプ方式の検証しか行えない場合、複数方式のタイムスタンプを付与することによって検証が実施できない可能性を減少させることができるため、将来第三者検証を行う場合には必要となるかもしれない。
考察	電子契約文書にマルチタイムスタンプを付与することは利用者の立場からは求められなかった。タイムスタンプの危殆化に対する保障であるならばタイムスタンプサービス提供側が行うべきこととの意見であった。しかしタイムスタンプの危殆化の発生の可能性は僅かながら必ず残存し、タイムスタンプの有効性を完全に保証できるサービスの実現は今のところ考えにくいため、非常に重要な電子契約文書については複数方式のタイムスタンプを付与することは有効であると考えられる。 また第三者検証を行う際の利便性として、電子契約文書に複数方式のタイムスタンプが付与されているならば、検証側でタイムスタンプの検証を実施できない可能性を減らせるとの意見があった。各々の検証者がある特定のタイムスタンプの検証環境しか持っていない場合に、マルチタイムスタンプは有効な対策となる。

5. 時刻トレーサビリティが確認できることの必要性

表 2-46　時刻トレーサビリティの必要性

設問	実際の業務を行う際に、タイムスタンプの時刻精度を確認する必要はあるか？
回答	・現状の電子契約業務では、本実証実験の TSA 及び TA が実現しているほどの時刻精度の確認は必要ない。 ・契約行為では、実際の契約日が重要であり、タイムスタンプ精度は議論されない。 ・現在は契約日とタイムスタンプがリンクしていないが、将来契約時点での時刻証明が必要となれば、必要になるかもしれない。
考察	タイムスタンプについて、電子契約では契約日の概念がタイムスタンプとリンクしていないため、その時刻精度の確認は必要とは思われないという意見であった。将来的に契約日とタイムスタンプの関係を定義するよう諸規則が改正されたなら必要になるという意見もあったが、その場合でも証明が必要な単位は日単位であり、本実証実験における TSA 及び TA が実現しているほどの精度は業務上必要ないという意見であった。 今回は日単位での精度しか求められない業務を対象としたため、余り必要性は高くないという結果となったが、時刻にセンシティブな業務を対象とした場合には、また違った結果が得られると考えられる。

6-10 検証者側利便性評価

１．業務効率の改善について

表 2-47　第三者検証の実施による業務効率の改善について

設問	第三者検証が実業務で可能となった場合、業務効率が改善されるか？
回答	・検証者が対象データの検証を行う場合、検証が行える場所（電子契約サービスの利用者の社屋）に出向いている。これが不要となるため、業務効率は大いに上がる。
考察	現在の電子契約サービスでは第三者検証を実施する機能がなく、検証者が電子契約サービス利用者のところに出向いて検証を行っている。これを不要とできることが大きな改善につながるため、第三者検証に対するニーズはとても高いと考えられる。

第3章 終わりに

1. 成果

1-1 第三者検証などについて実運用に近い環境に適用し、運用性を評価する

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。

1-2 VA を介した第三者検証において時刻トレーサビリティの検証も可能とする

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。

1-3 マルチタイムスタンプにより単一のタイムスタンプの危殆化に対応する

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. 今後の課題

本実証実験によって明らかとなった今後の課題を、以下に示す。

2-1 VA を介した第三者検証におけるデータの受け渡し

今回の実証実験においては、VA を介した第三者検証について機能の確認を行うことができた。

しかし、ユーザビリティの検証における実業務担当者からの意見にも有ったように、実際の業務に適用する際には対象データのセキュリティに配慮したアプリケーションを構築が強く求められている。また VA を介した第三者検証のためには、対象データ及びタイムスタンプの送付及び検証を、総合的にサポートする支援アプリケーションの構築が必要になると考えられる。検証時の確認項目の充足性の面からも、現状は契約文書に記載されていない情報は利用者が別途通知しないと検証者は確認できないということもあり、VA による第三者検証を実業務の中で利用できるようにするためには、データ受け渡しまで含めたシステム化が強く求められると考えられる。

2-2 検証用アカウントのアクセス管理

今回の実証実験においては、検証用アカウントを使用することにより、電子契約サーバでの第三者検証について機能の確認を行うことができた。

しかし、ユーザビリティの検証における実業務担当者からの意見にも有ったように、今回は対象利用者に係る全ての電子契約が検証者に閲覧されてしまう設定となっていたため、開示が不要であり、かつ見られたくない文書まで閲覧されてしまい、開示する必要がある文書のみ閲覧を許可することが求められている。電子契約サーバでの第三者検証を実業務の中で利用できるようにするためには、検証用アカウントについて、案件毎に細かくアクセス権を設定できるような機能が強く求められると考えられる。

2-3 マルチタイムスタンプの検証

電子契約サーバでの検証においては、マルチタイムスタンプとした場合でも単一の場合と同じユーザインタフェースとなっているため、1 回の要求で 2 方式のタイムスタンプを検証することができ、マルチタイムスタンプとしたことによる操作性や処理速度の低下はほとんど見られなかった。一方、VA を介した検証においては、タイムスタンプ毎に検証要求を必要とするユーザインタフェースとなっているため、マルチタイムスタンプとした際の 2 方式の検証においては、操作回数や処理時間がそれぞれの方式の検証に必要な値をほぼ足し合わせた値となり、操作性や処理速度の低下が顕著に見られる。

これらの結果より、実業務の中で VA を介したマルチタイムスタンプの検証を行う場合は、サーバ側でタイムスタンプ毎の検証を順次繰り返す等、方式の改良が求められると考えられる。

参考文献

[1]”タイムスタンプ･プロトコルに関する技術調査”,独立行政法人 情報処理推進機構(IPA),2004 年 2 月
[2]”信頼されるタイムスタンプ基準・運用ガイドライン”,タイムビジネス推進協議会(TBF),平成 17 年 11 月

付録 実証実験アプケーション操作方法

実証実験操作説明書（マルチタイムスタンプ付与－ダウンロード）

はじめに

本資料は実証実験を行う際に電子契約サーバを使用してタイムスタンプを付与するまでの操作をまとめたものです。

本資料を参考にして、実証実験を行ってください。

また操作説明中に下線が引かれている項目は、操作画面のラベルやボタンに対応しています。

なお、実証実験では試験用電子契約サーバにログインする際に、試験用の URL を指定し、試験用 ID 及びパスワードを入力する必要があります。

接続先 URL

実証実験を実施する場合は、以下の URL に接続してください。

https://nict.dlms.ne.jp/

試験用アカウント パスワード

以下、2 種類のアカウントが必要です。試験管理者に確認してください。

・文書登録者

・文書確認者

端末の設定

試験端末はブラウザより試験用電子契約サーバに接続できるよう設定してください。

また試験端末には Acrobat（Version6 または 7)、及び E-TOKEN ドライバがインストールされている必要があります。

PDF ファイルは、Acrobat Reader ではなく、Acrobat に関連付けを行っておいてください。

マルチタイムスタンプ付与

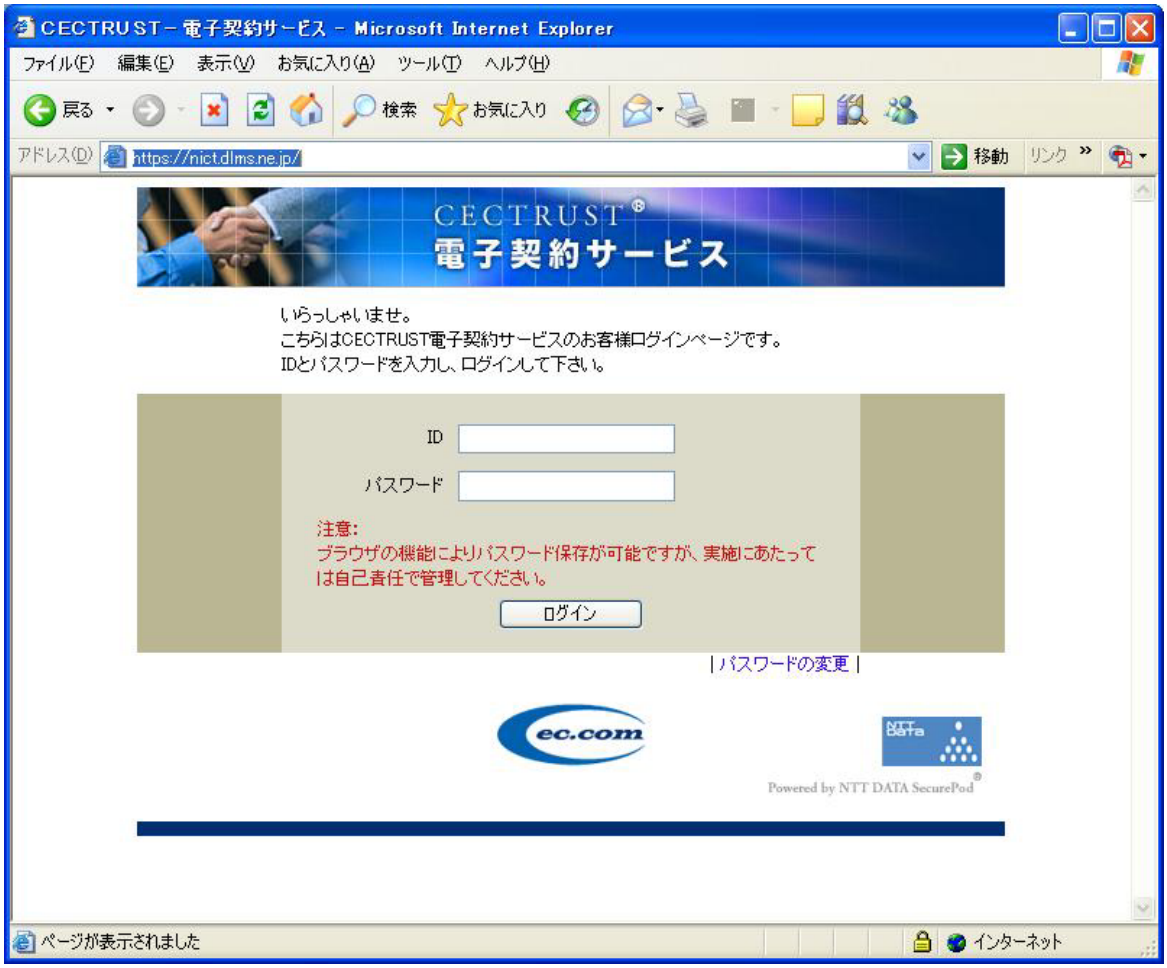
1．文書の登録作業

1.1 登録文書の用意

事前に PDF 形式の対象データを作成し、文書登録者のデジタル署名を付与してください。

1.2 ログイン

InternetExplorer より電子契約サーバにアクセスします。正しく URL が指定されていれば、次の Login 画面が表示されます。



試験用に用意された文書登録者用 ID 及びパスワードを入力しログインボタンをクリックしてください。

1.3　登録文書の指定

ログインすると TOP 画面が表示されます。

案件登録タブをクリックしてください。

案件登録画面が表示されます。

取引先 ID、案件名、注文番号、様式、契約用書類を指定してください。その他の項目の入力は任意となっています。

取引先 ID には、文書確認者の ID を指定します。

案件名は任意の文字を入力してください。

注文番号は任意の数字を入力してください。

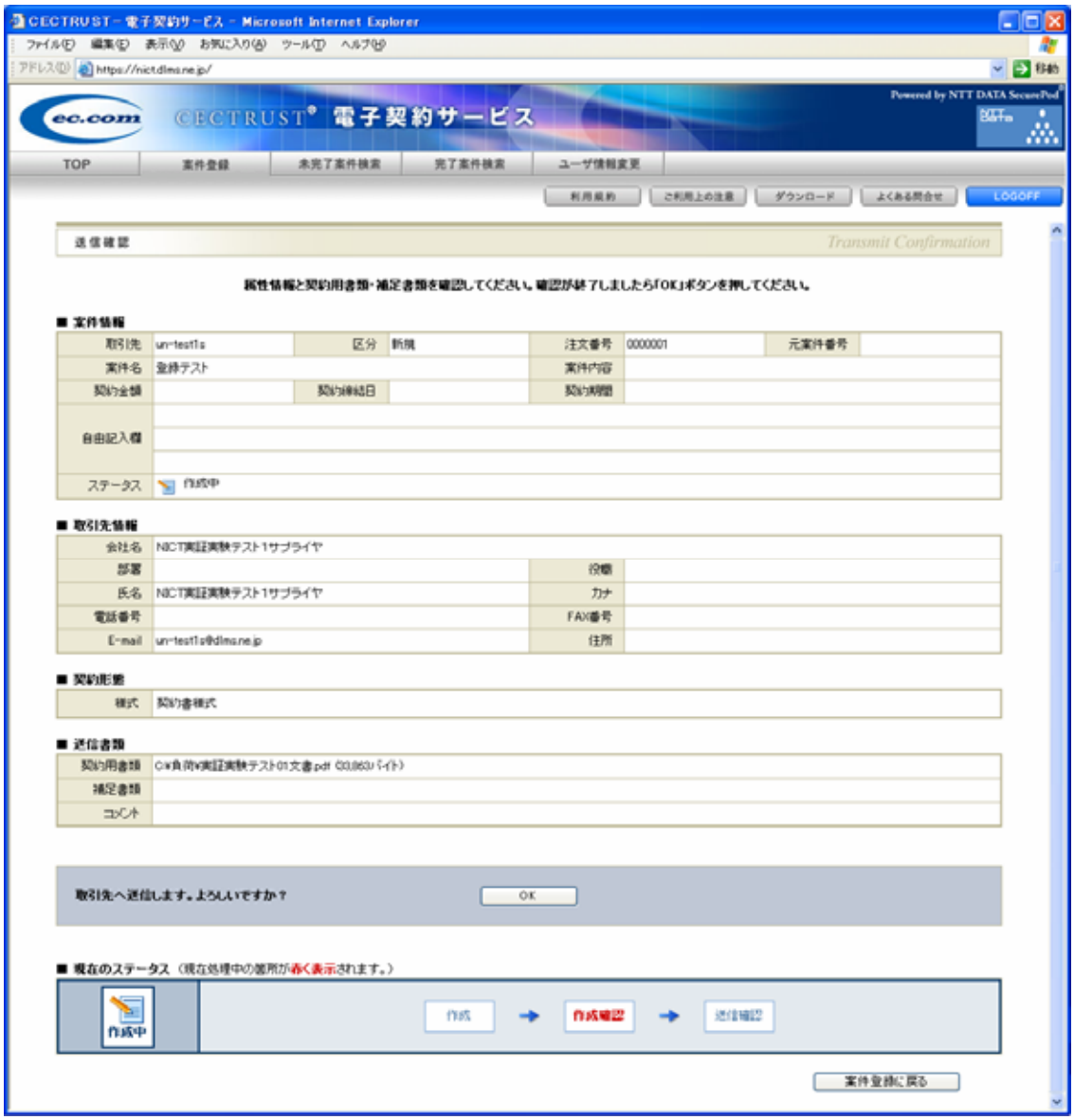
様式はプルダウンメニューから任意の様式を選択してください。

契約用書類には、文書登録者のデジタル署名が付与されたファイルを指定してください。

各項目を指定後、送信ボタンをクリックしてください。

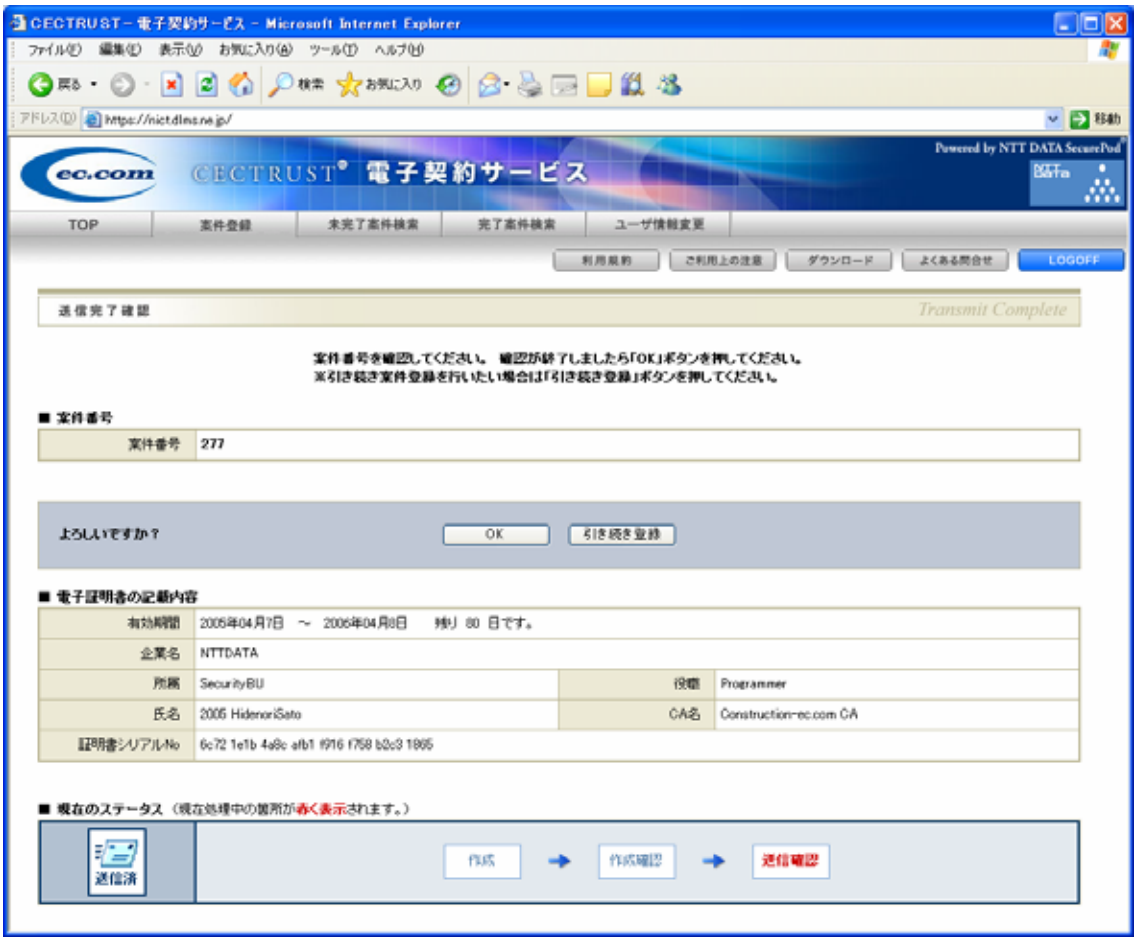
1.4 文書の登録

送信確認画面が表示されます。



OK ボタンをクリックしてください。

送信完了確認画面が表示されます。



登録された文書の案件番号が表示されます。確認後、OK ボタンをクリックしてください。

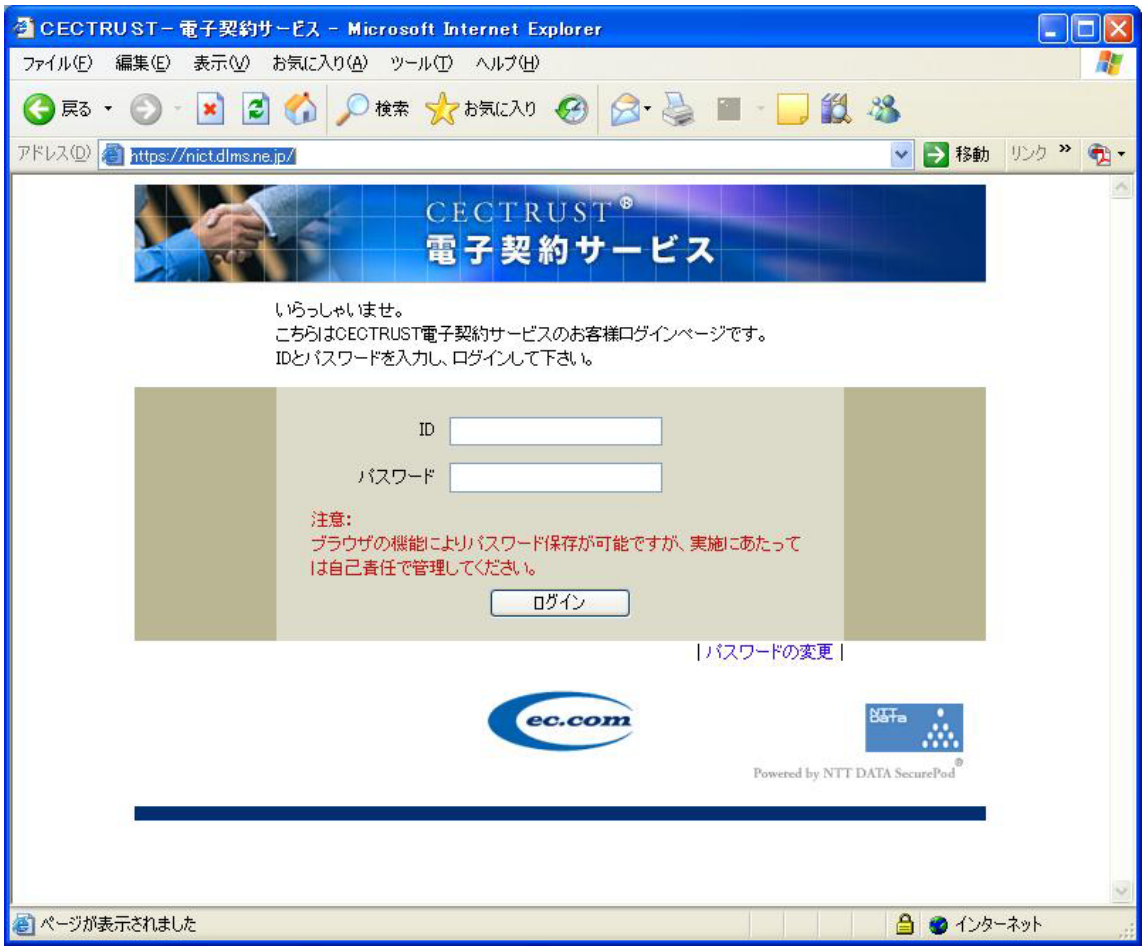
以上で文書登録者による、文書の登録作業は終了です。画面上部の LOGOFF ボタンを押すか、ブラウザを終了させてください。

続けて文書確認者の操作を行います。

2．文書の確認作業

2.1　ログイン

InternetExplorer より試験用 CECTRUST にアクセスします。正しく URL が指定されていれば、次の Login 画面が表示されます。



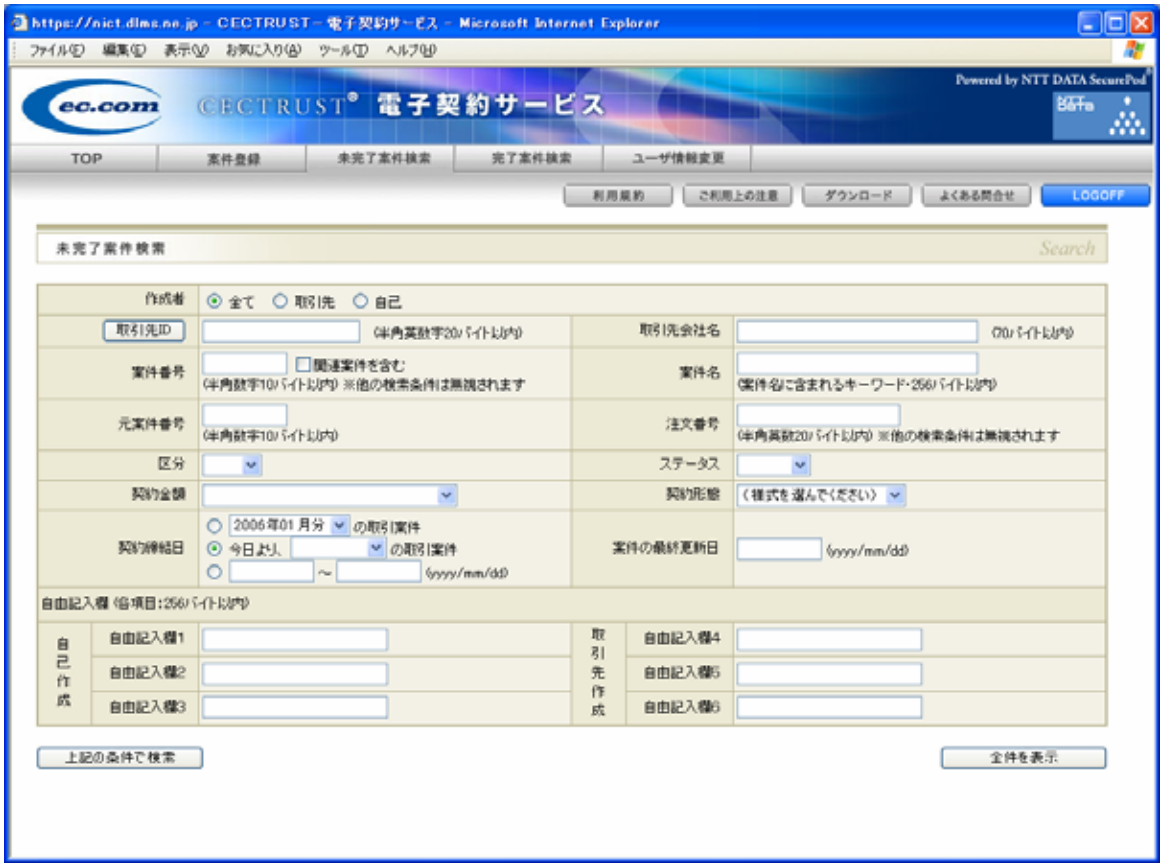
試験用に用意された文書確認者用 ID 及びパスワードを入力しログインボタンをクリックしてください。

2.2 確認文書の検索

TOP 画面が表示されます。

未完了案件検索タブをクリックしてください。

未完了案件検索画面が表示されます。



未完了案件検索画面が表示されます。

登録した文書の案件番号を入力し、上記の条件で検索ボタンをクリックするか、全件を表示ボタンをクリックしてください。

未完了案件一覧画面が表示されます。

検索を行った対象の文書が表示されます。全件を表示を行った場合は、文書が複数表示されます。

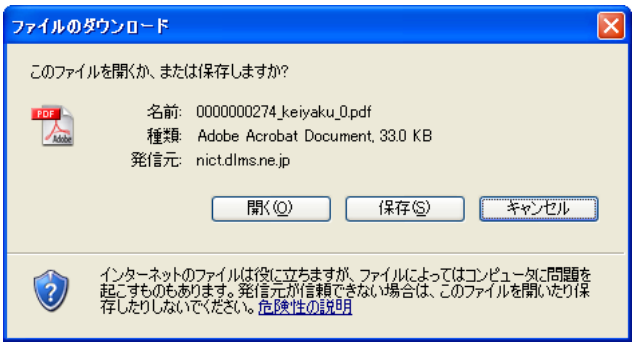
目的の文書を確認し、詳細ボタンをクリックしてください。

2.3　確認文書の表示

案件詳細画面が表示されます。

受信書類の契約用書類欄のファイル名をクリックするか、契約用書類をダウンロードボタンをクリックしてください。

ファイル保存のダイアログボックスが表示されます。
開くボタンをクリックし、文書を Acrobat で表示してください。



Acrobat にて、文書に文書確認者のデジタル署名を行い、任意のフォルダに保存してください。

このとき、ブラウサを終了しないでください。続けて電子契約サーバの処理を行います。
終了した場合は、2-1 から 2-3 の画面表示までを行ってください。

2.4　文書の文書作成者への返信

再度、案件詳細画面を表示してください。

文書確認者の署名を行った後、ダウンロード終了（次画面へ）ボタンをクリックしてください。

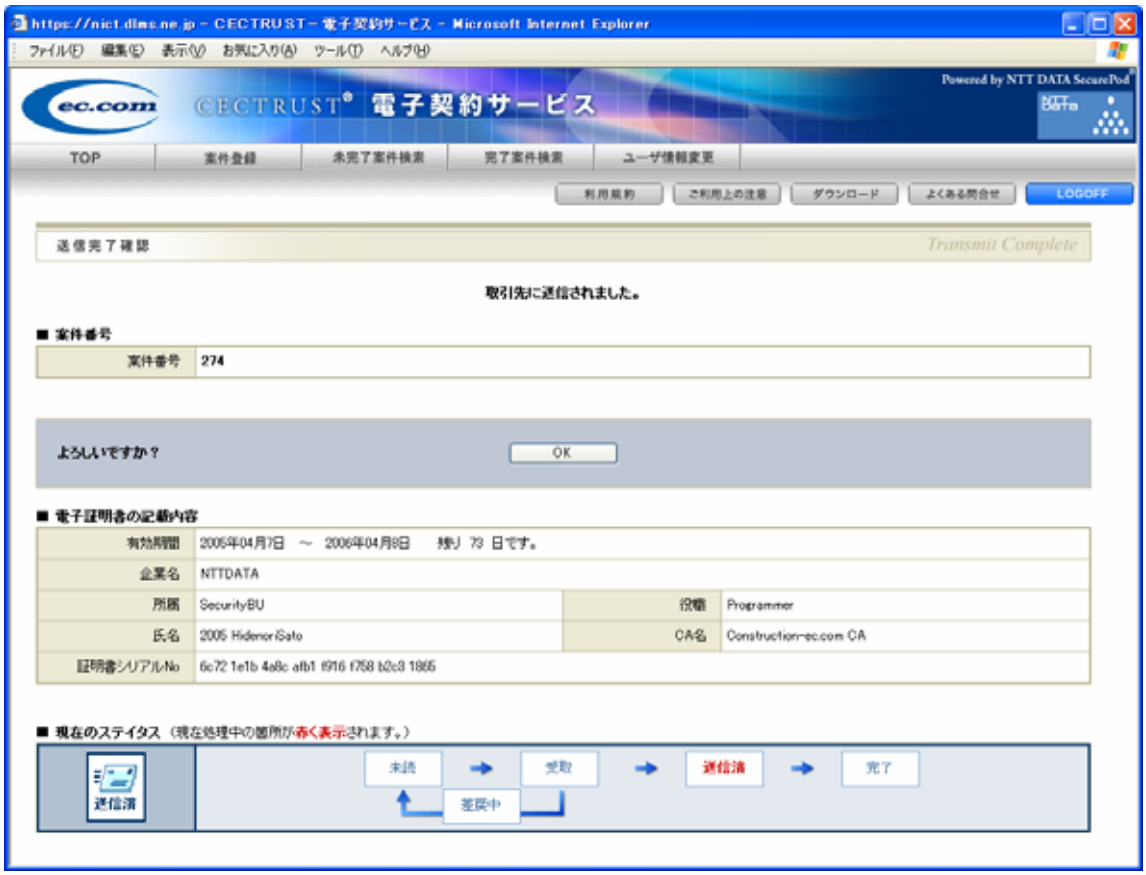
確認した契約用書類を指定する画面が表示されます。

契約用書類にデジタル署名を付与したファイルを指定し、取引先へ送信ボタンをクリックしてください。

送信確認画面が表示されます。

OK ボタンをクリックしてください。

送信完了確認画面が表示されます。



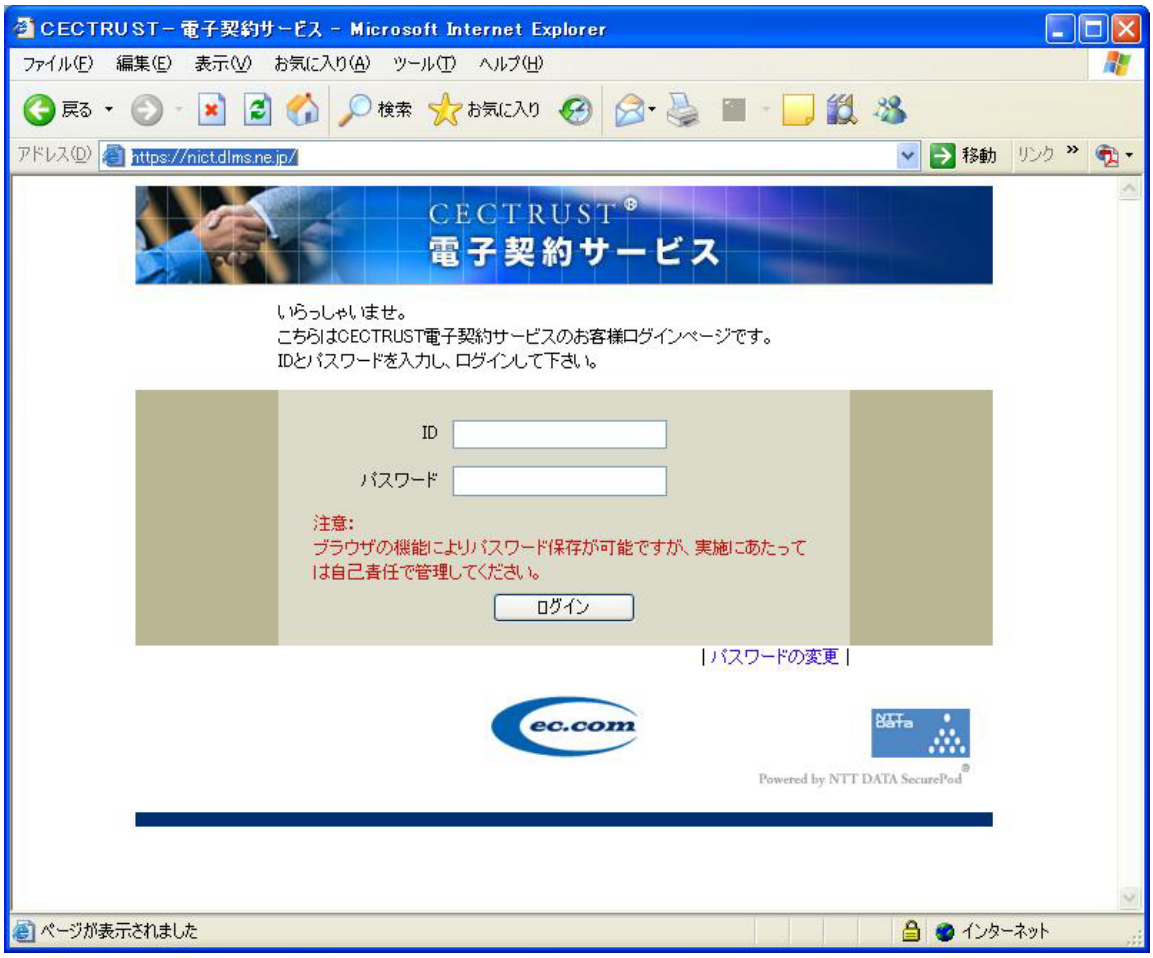
OK ボタンをクリックしてください。

以上で文書確認者による、文書の確認作業は終了です。画面上部の LOGOFF ボタンを押すか、ブラウザを終了させてください。

3．マルチタイムスタンプの付与、文書及びタイムスタンプのダウンロード

3.1　ログイン

InternetExplorer より試験用 CECTRUST にアクセスします。正しく URL が指定されていれば、次の Login 画面が表示されます。



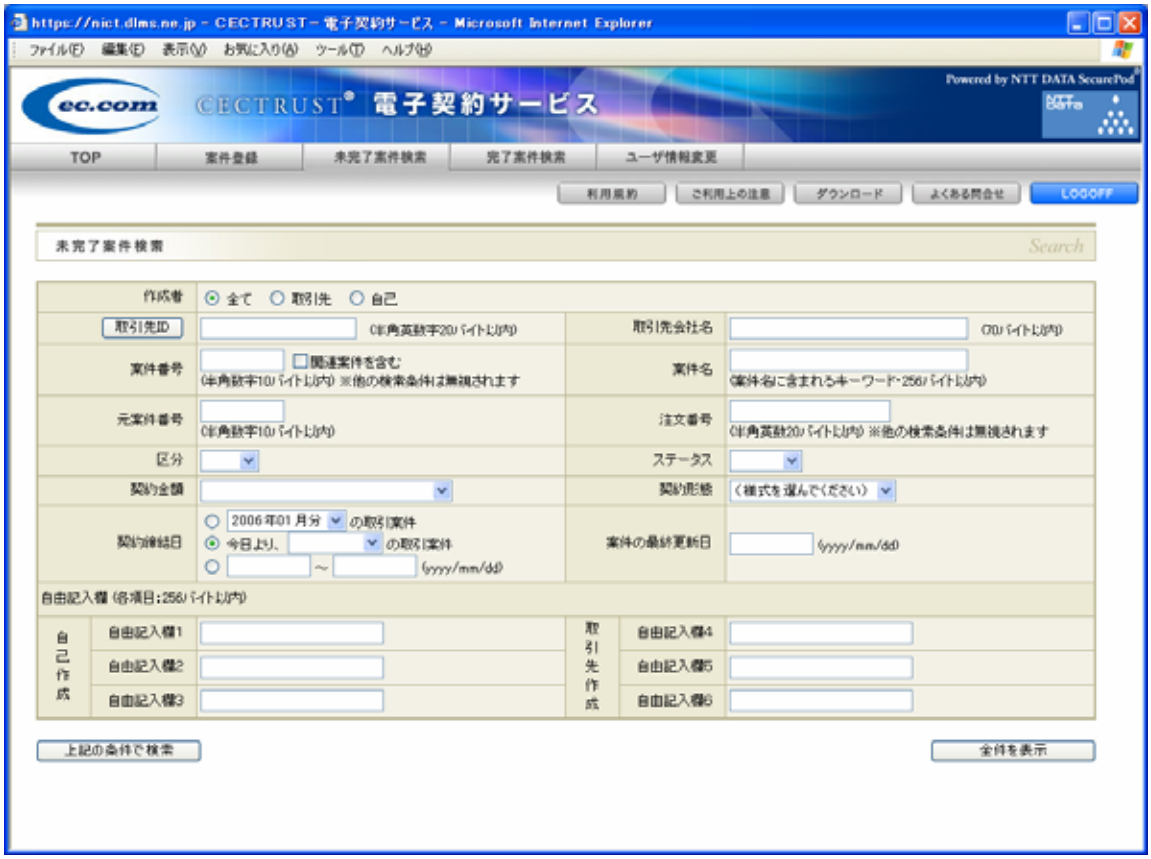
試験用に用意された文書登録者用 ID 及びパスワードを入力しログインボタンをクリックしてください。

3.2　マルチタイムスタンプ付与文書の検索

TOP 画面が表示されます。

未完了案件検索タブをクリックしてください。

未完了案件検索画面が表示されます。



確認した文書の案件番号を入力し、上記の条件で検索ボタンをクリックするか、全件を表示ボタンをクリックしてください。

未完了案件一覧が表示されます。全件を表示を行った場合は、文書が複数表示されます。

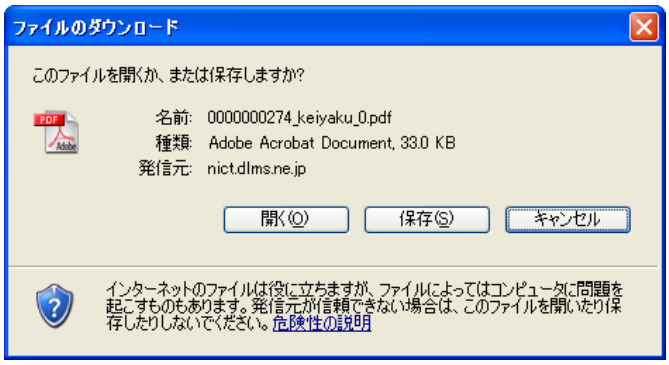
目的の文書を確認し、詳細ボタンをクリックしてください。

3.3　文書の確認

案件詳細画面が表示されます。

表示されている受信書類欄の契約用書類のファイル名をクリックするか、契約用書類をダウンロードボタンをクリックしてください。

ファイル保存のダイアログボックスが表示されます。
開くボタンをクリックし、文書を Acrobat で開いてください。



文書内容を確認後、Acrobat を終了させてください。
このとき、ブラウサを終了しないでください。続けて電子契約サーバの処理を行います。
終了した場合は、3-1 から 3-3 の画面表示までを行ってください。

3.4　契約の確定

再度、案件詳細画面を表示します。

文書確認後、ダウンロード終了（次画面へ）ボタンをクリックしてください。

文書の確認を行う画面が表示されます。

完了ボタンをクリックしてください。

完了確認画面が表示されます。

OK ボタンをクリックしてください。

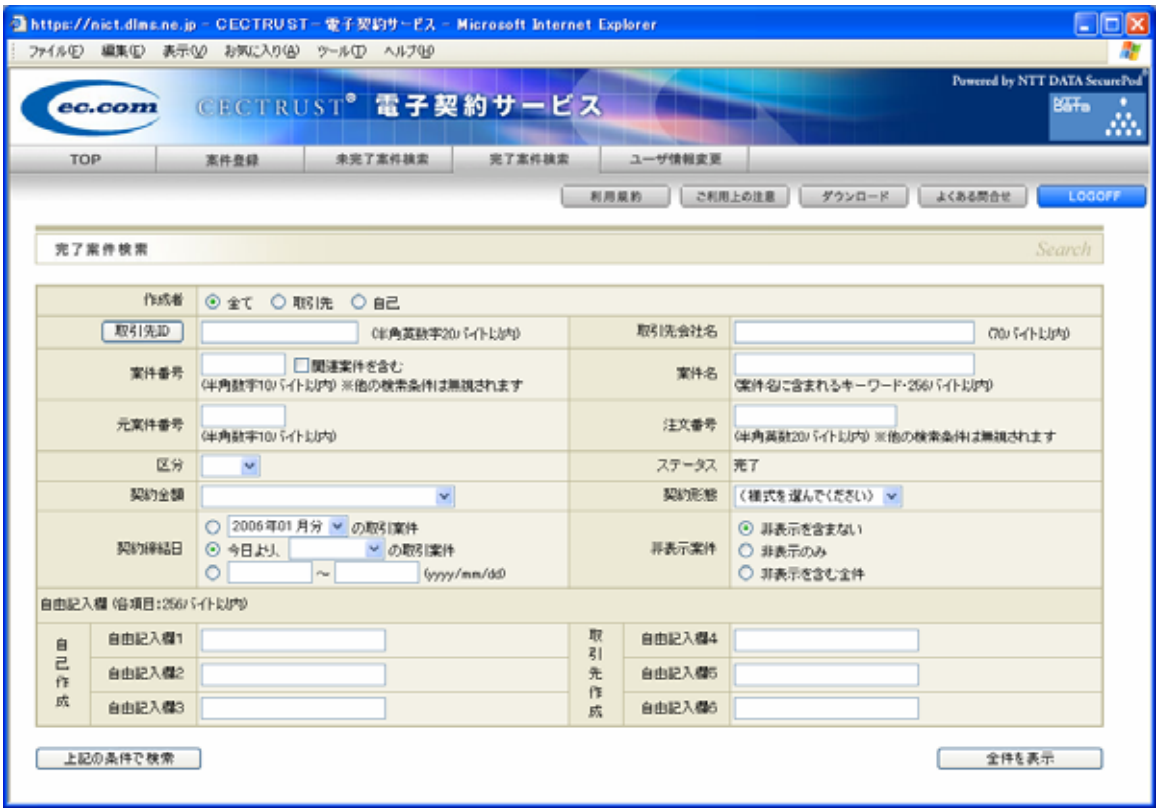
契約の確定が行われ、文書にマルチタイムスタンプが付与されました。

3.5　マルチタイムスタンプが付与された文書の検索

次にマルチタイムスタンプが付与された文書のダウンロードを行います。

完了案件検索タブをクリックしてください。

完了案件検索画面が表示されます。



マルチタイムスタンプを付与した文書の案件番号を指定して、上記の条件で検索ボタンをクリックするか、全件を表示ボタンをクリックしてください。

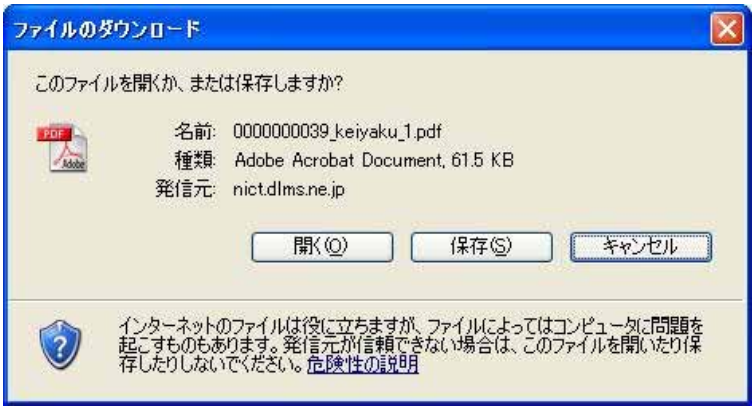
完了案件一覧が表示されます。全件を表示を行った場合は、文書が複数表示されます。

目的の文書を確認し、詳細ボタンをクリックしてください。

完了案件詳細画面が表示されます。

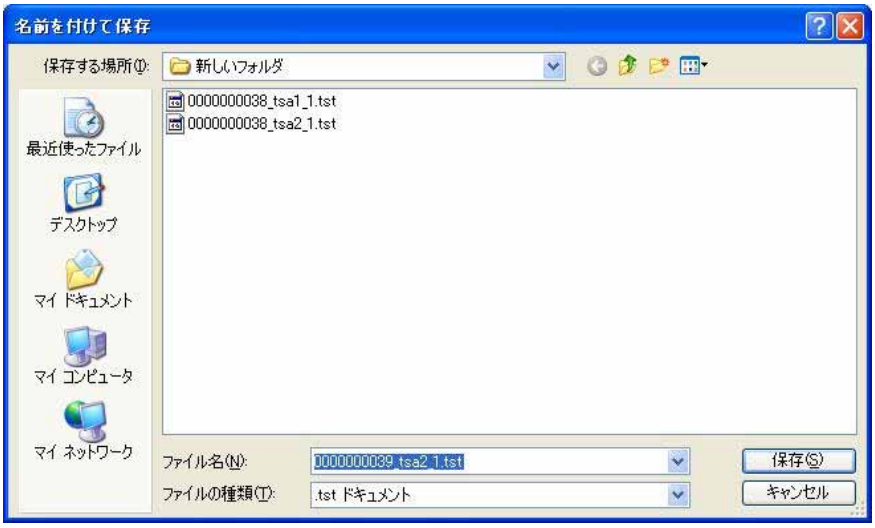
受信書類欄の契約用書類のファイル名、タイムスタンプ１及びタイムスタンプ２欄のファイル名をクリックしてください。

ファイル保存のダイアログボックスが表示されます。



保存をクリックし、ファイルを保存してください。契約文書、タイムスタンプ 1 及びタイムスタンプ 2 の 3 個のファイルをダウンロードしてください。

保存ボタンをクリックすると以下の画面が表示されます。



ここで任意のフォルダを指定し、ファイルの保存を行ってください。
ファイル名の変更は通常は不要です。

3.6　ダウンロードしたファイルの検証者への送付

ダウンロードしたファイルを、メールや媒体にて VA を介した第三者検証の実施者へ送付してください。

―以上―

実証実験操作説明書（VA クライアント操作説明書）

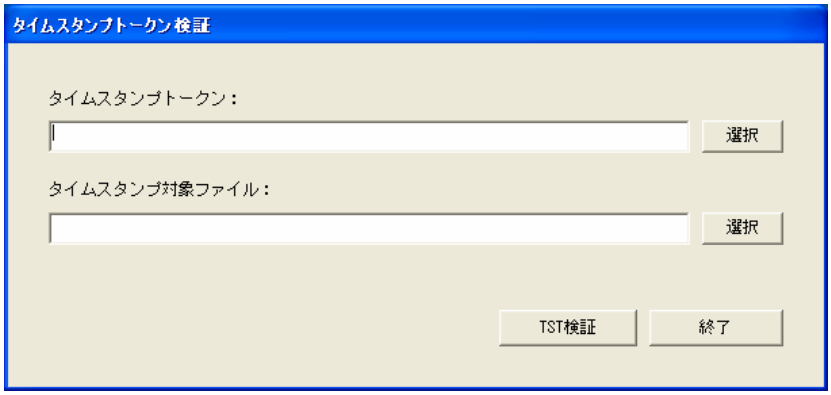
はじめに

本資料は VA を介した第三者検証を行うために必要な VA クライアントの操作を説明するものです。本資料を参考にして、VA での第三者検証を行ってください。

１．VA クライアント起動

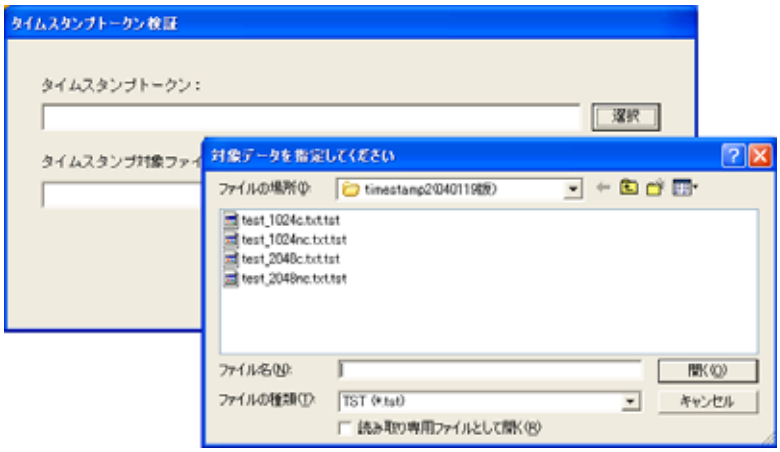
デスクトップ上にある、以下のアイコンをクリックしてください。VA クライアントが起動します。

起動すると、次の画面が表示されます。



２．検証対象タイムスタンプトークンの指定

起動画面上で、タイムスタンプトークンの選択ボタンをクリックすると、ファイル選択画面が表示されます。



検証対象のタイムスタンプトークンを指定してください。

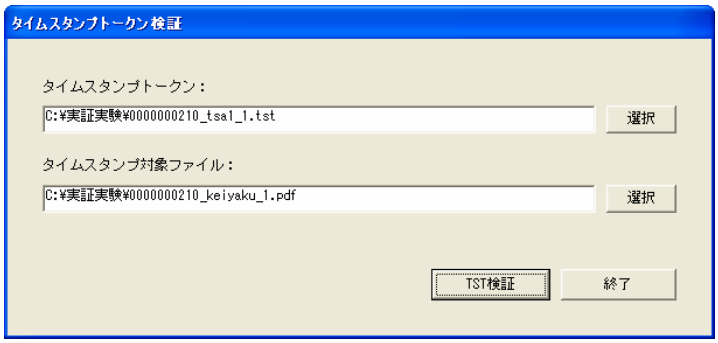
3．タイムスタンプ対象ファイルの指定

起動画面上で、タイムスタンプ対象ファイルの選択ボタンをクリックすると、ファイル選択画面が表示されます。

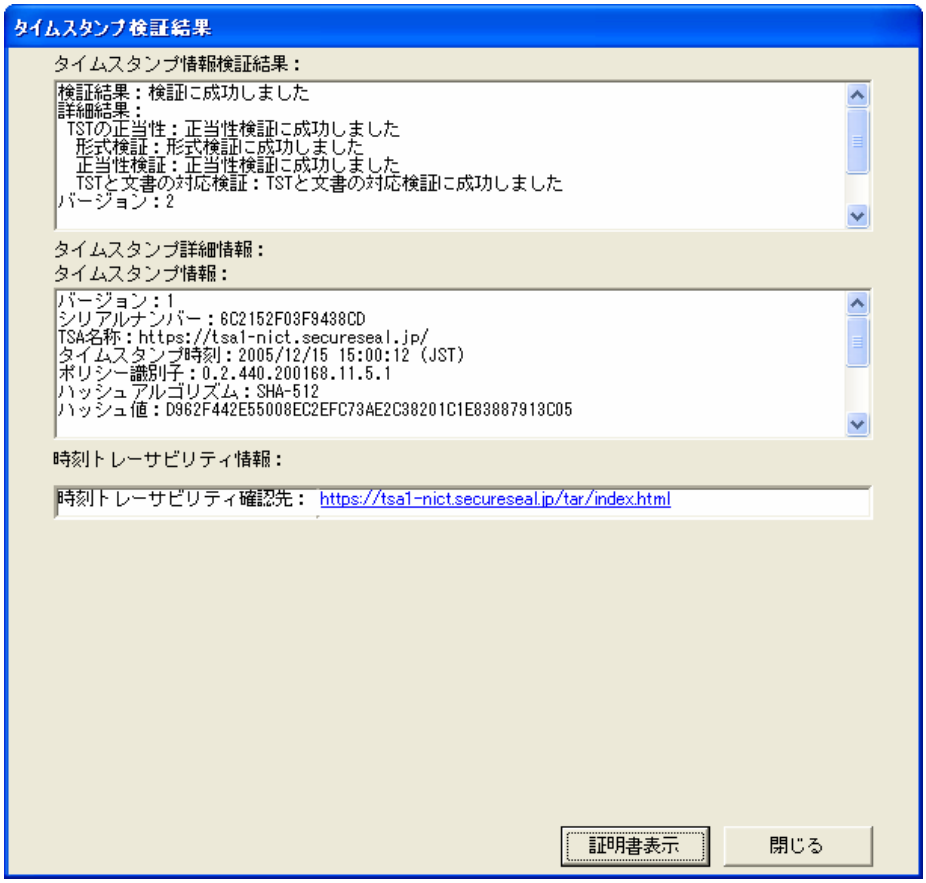
検証対象の文書ファイルを指定してください。

4. タイムスタンプの検証

タイムスタンプトークン、タイムスタンプ対象ファイルの指定が完了したら、TST 検証ボタンをクリックしてください。



検証結果が表示されます。



－以上－

実証実験操作説明書（電子契約サーバでの検証）

はじめに

本資料は実証実験を行う際に電子契約サーバを使用して第三者検証を行う際の操作についてまとめたものです。

本資料を参考にして、実証実験を行ってください。

また操作説明中に下線が引かれている項目は、操作画面のラベルやボタンに対応しています。

なお、実証実験では電子契約サーバにログインする際に、試験用の URL を指定し、試験用 ID パスワードを入力する必要があります。

接続先 URL

実証実験では一般の CECTRUST とは別に試験用のサーバを用意しています。

実証実験を実施する場合は、以下の URL に接続してください。

https://nict.dlms.ne.jp/

試験用アカウント パスワード

以下のアカウントが必要です。試験管理者に確認してください。

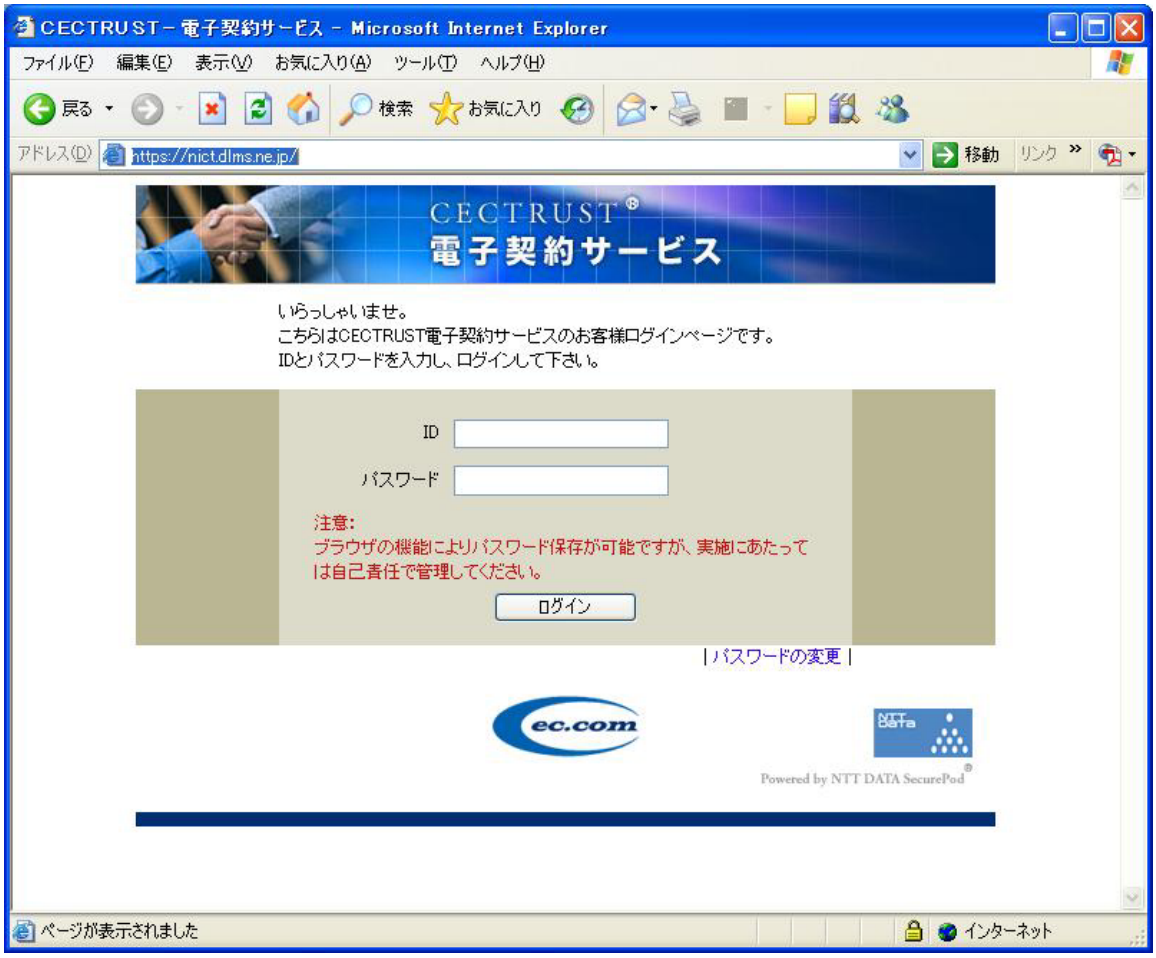
・検証用アカウント

試験用 CECTRUST の操作

1. ログイン

ブラウザを起動し、電子契約サーバにアクセスします。

正しく URL が指定されていれば、次の Login 画面が表示されます。



試験用 ID 及びパスワードを入力しログインボタンをクリックしてください。

2. 検証文書の指定

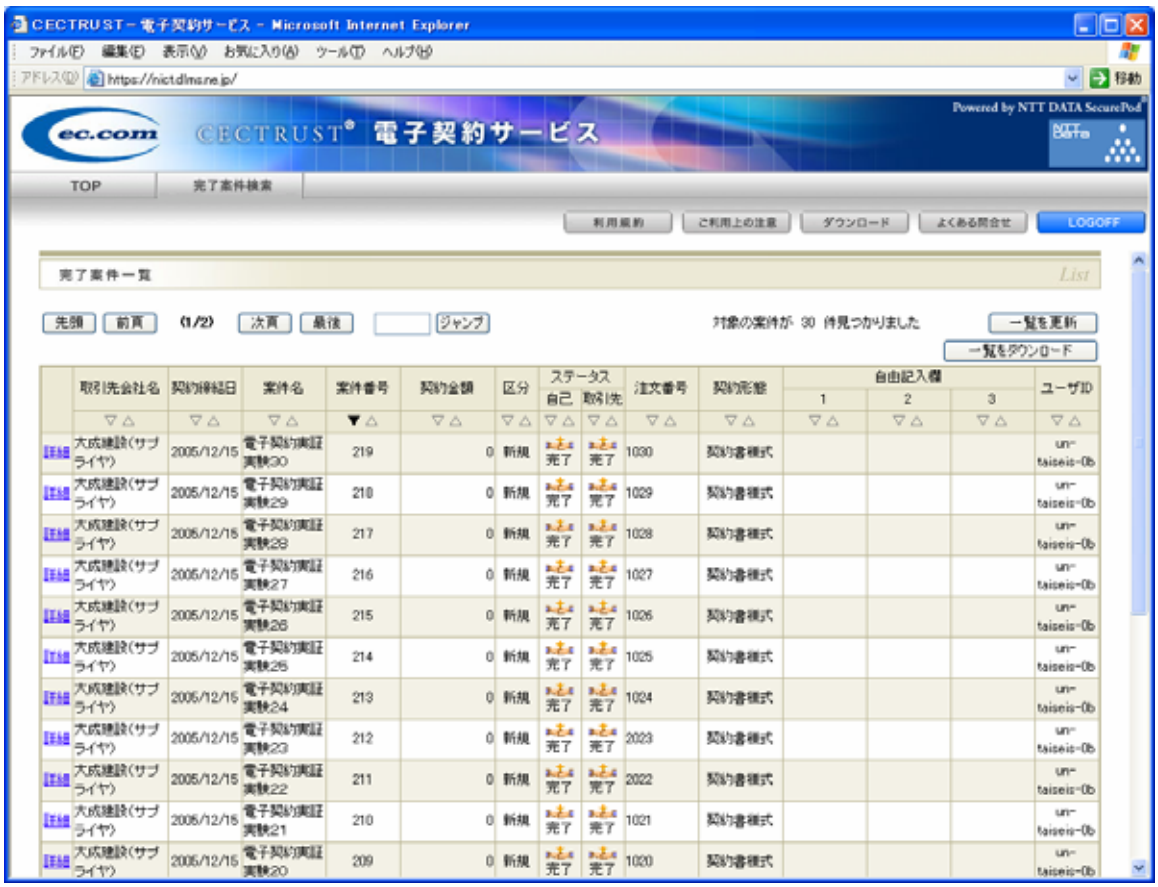
TOP 画面が表示されます。

完了案件検索タブをクリックしてください。

完了案件検索画面が表示されます。

全件を表示ボタンを押すか、検証する案件番号を入力して上記の条件で検索ボタンを押してください。

完了案件一覧画面が表示されます。



検証を行う文書の詳細ボタンをクリックしてください。

3. 文書の検証

完了案件詳細画面が表示されます。

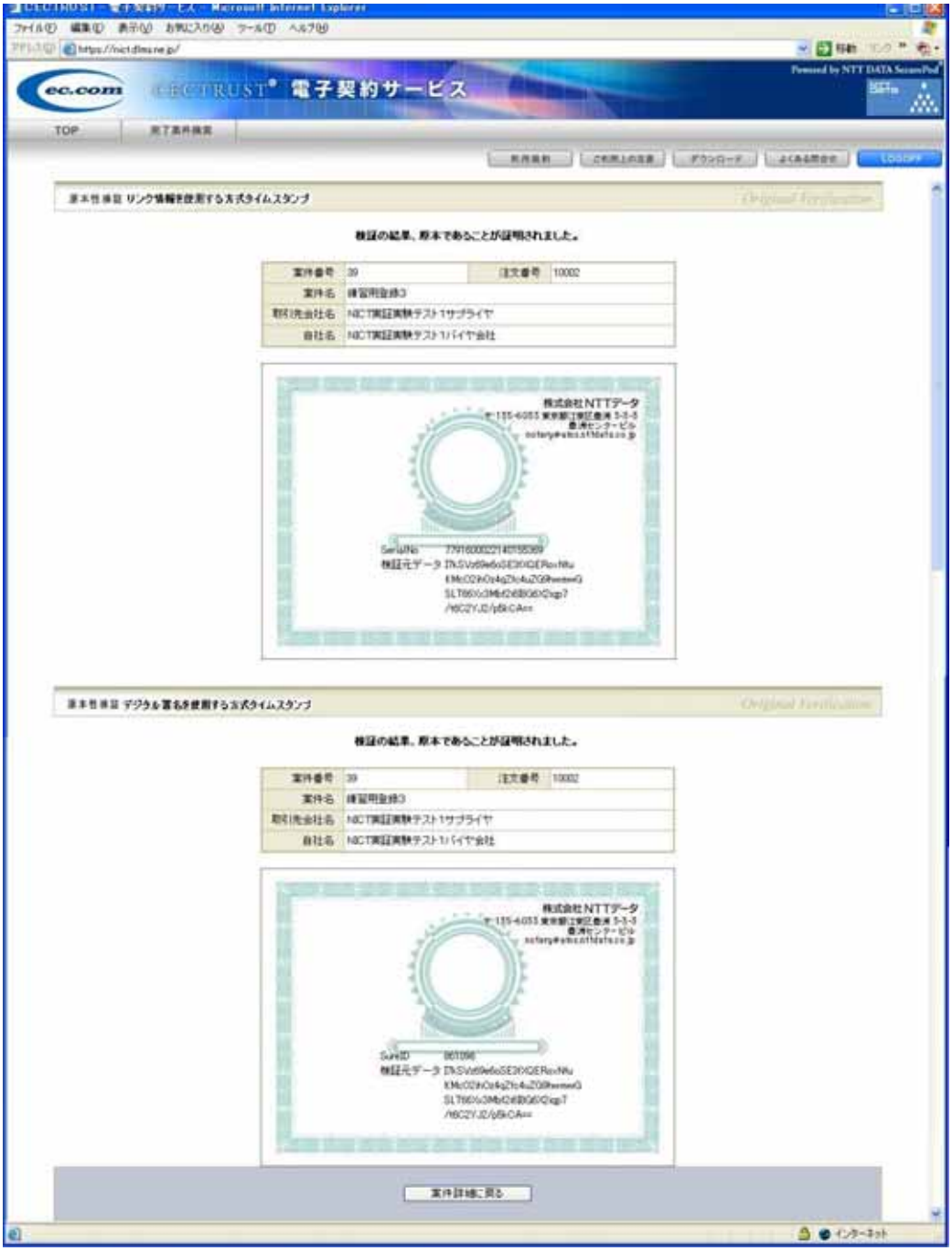
文書の検証を行います。

原本性検証ボタンをクリックしてください。

ここで下の課金メッセージが表示されますが、実証実験では課金は発生しませんので

そのまま OK ボタンをクリックしてください。

原本性検証のマークが表示されます。



試験用 CECTRUST では、1 文書に 2 方式のタイムスタンプが付与されています。そのため、検証マークが 2 つ表示されます。

本表示にて、対象の文書の検証が確認されました。

―以上―

ログサーバ実証実験評価報告書

平成 18 年 3 月 16 日

独立行政法人情報通信研究機構

日本電気株式会社

株式会社アット東京

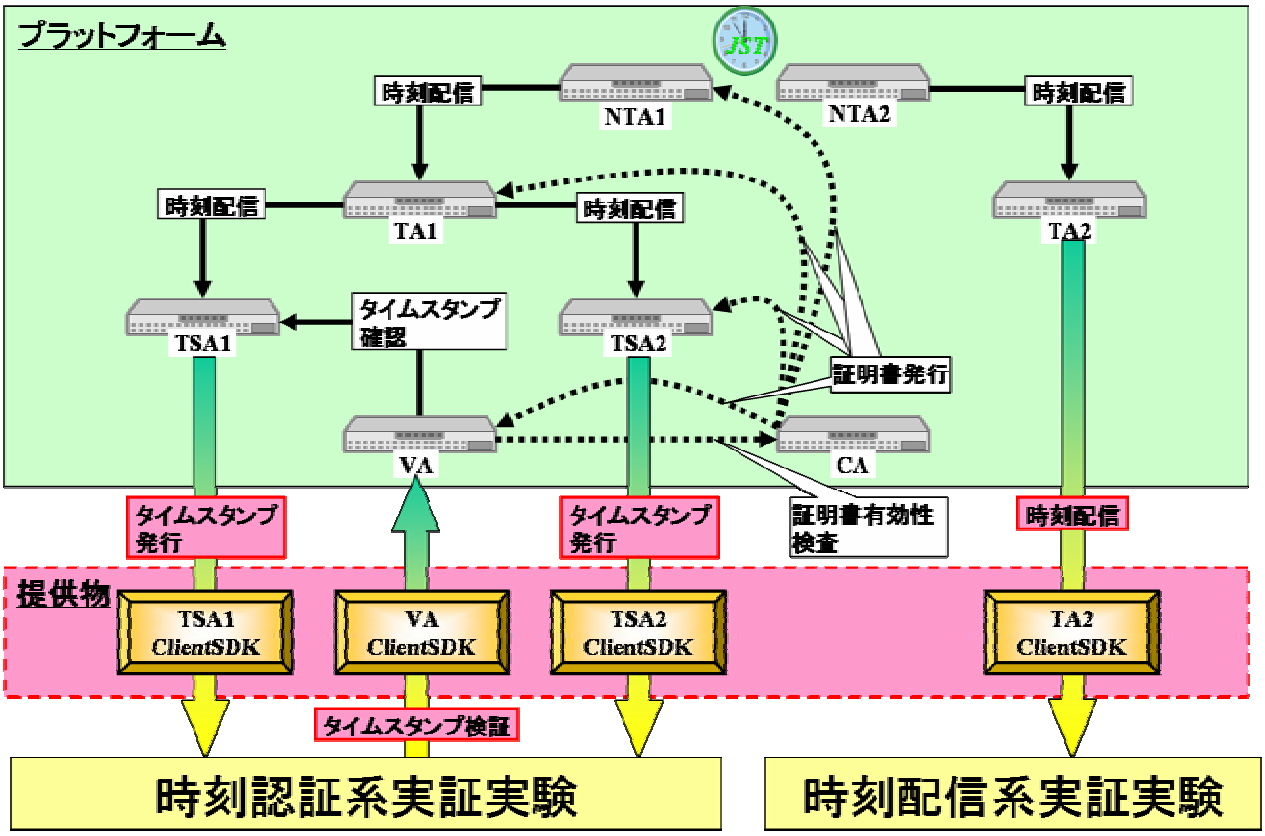
目次

第 1 章 はじめに 1
第 2 章 ログサーバ実証実験目的 2
第 3 章 ログサーバ実証実験概要 3
1. 実証実験概要 3
2. 実証実験評価項目 4
第 4 章 ログサーバ実証実験期間 5
第 5 章 システム構成 6
1. ネットワーク 6
2. ハードウェア 6
2-1 NTA2 6
2-2 TA2 6
2-3 NTP サーバ 7
2-4 ログサーバ 7
3. ソフトウェア 8
3-1 NTA2 8
3-2 TA2 8
3-3 NTP サーバ 8
3-4 ログサーバ 9
第 6 章 ログサーバ実験手順 10
1. 実験内容 10
1-1 時刻配信機能 10
1-2 時刻誤差計測 10
1-3 時刻情報トレーサビリティ検証機能 10
1-4 時刻監査機能 10
2. 実験手順 10
2-1 時刻配信機能 10
2-2 時刻誤差計測 11
2-3 時刻情報トレーサビリティ検証機能 11
2-4 時刻監査機能 13
第 7 章 実験結果と考察 16
1. 実験結果 16
1-1 時刻配信機能 16
1-2 時刻誤差計測 16
1-3 時刻情報トレーサビリティ検証機能 19
1-4 時刻監査機能 19

2. 実証実験アンケートの実施 19
3. 考察 20

第1章 はじめに

本報告書は、「タイムスタンプ・プラットフォーム技術の研究開発」で、平成 17 年に構築した統合化プラットフォームを使用して実施した、実証実験について記載している。下記に統合化プラットフォームの全体概要図を記した。本報告書では、時刻配信系実証実験として TA2 から配信された時刻を利用したログの生成および保存を行う実証実験について記載している。



第2章 ログサーバ実証実験目的

近年、高度な情報通信ネットワークが発達し、情報通信を利用した知的活動や産業活動等が活発に行われるようになった。特に電子商取引や電子政府等の利用が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。例えば、企業や行政機関で情報漏えいが発生した場合、機密情報に誰が「いつ」アクセスしたか確認、立証する必要がある。しかし、現在の時刻配信方式では、日本標準時から時刻を受信し、高精度な時刻を保持していることを証明するのは難しい。そこで、国家時刻標準機関（NTA：National Time Authority）から日本標準時を改ざんされることのない時刻配信方式の策定とその実装を、平成 17 年度に「配信時刻高精度高信頼化サブシステムー３（トレーサビリティの保証）」（以下､(1)-(iii)と記す）として、行った。

(1)-(iii)では、NTA、標準時配信局（TA：Time Authority）、各種サーバにて高信頼度な時刻情報である時刻認証子を生成し、各装置間で時刻認証子を送受信することにより、時刻正当性とトレーサビリティの確認を可能としている。また、時刻の正当性とトレーサビリティの検証は第三者によって実施可能なプロトコルであるため、システム内の時刻の正当性を立証可能であり、裁判時には有効な証拠として時刻認証子の提出を想定している。

(1)-(iii)は同一 LAN 内で動作テストを実施しており、実使用されているインターネット網を使用した時刻配信とその時刻利用の動作確認は行っていなかった。そのため、実際に時刻受信とその時刻利用をする環境下で動作確認を行う必要がある。(1)-(iii)には、高信頼度な時刻情報を配信する機能「時刻配信機能」と、時刻同期を行いその時刻誤差を計測する機能「時刻誤差計測機能」と、日本標準時から時刻が配信されたことを検証する「時刻情報トレーサビリティ検証機能」と、時刻を正しく生成・管理していたか証明する「時刻監査機能」がある。本実証実験では、実使用されているインターネットを介した場合、これらの機能が実現されているか検証を行った。

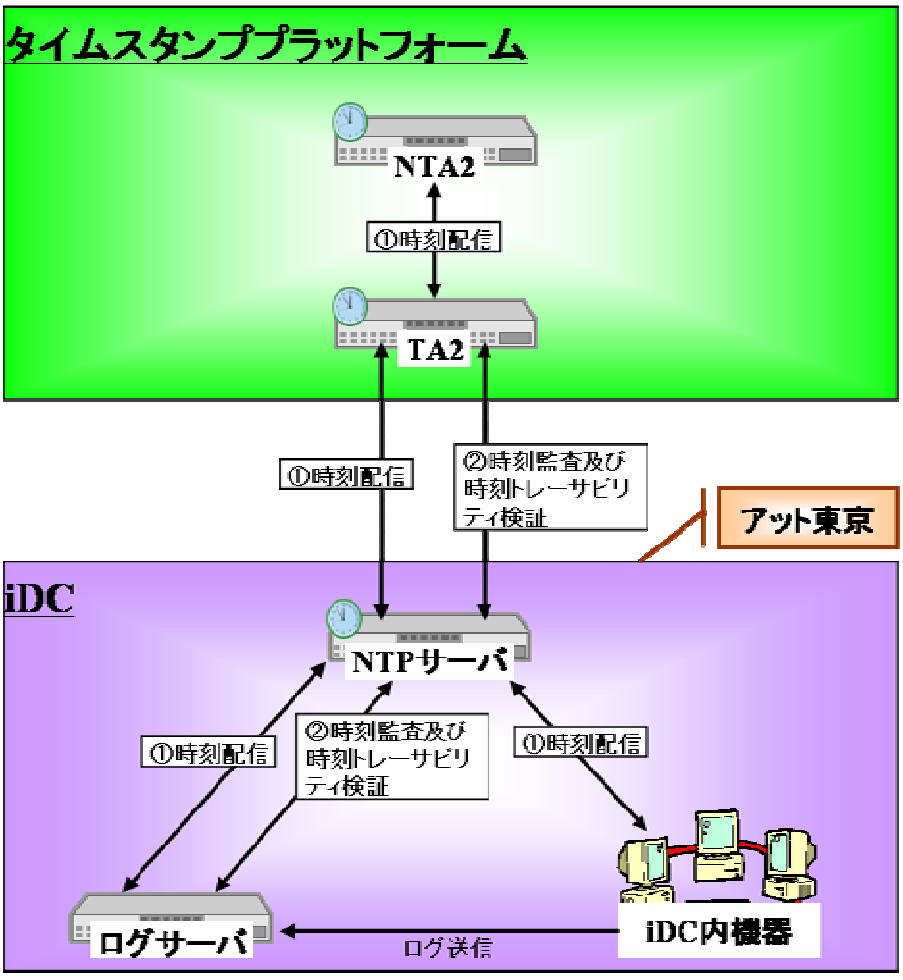
第3章 ログサーバ実証実験概要

1. 実証実験概要

上記統合化プラットフォームの TA2 から iDC 内の NTP サーバに、インターネットを介して時刻を配信し、iDC 内のログサーバに高信頼高精度の時刻情報である時刻認証子を提供する。時刻の配信方式は、時刻リンク方式※である。時刻リンク方式の時刻トレーサビリティ技術により、iDC 内のサーバ機器の時刻情報の信頼性を確認でき、ログの生成時刻の信頼性向上を実現する。

また、iDC と通信回線の使用は、株式会社アット東京様にご協力頂いた。概要図を以下に示す。

※　ここでいう時刻リンク方式とは、TA2 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。



1. NTA2 から TA2 に時刻情報を配信する。

2. TA2 から iDC 内の NTP サーバにインターネットを介して時刻情報を配信する。
3. TA2 は、iDC 内の NTP サーバが生成・保存している時刻情報に対して時刻監査を実施する。
4. NTP サーバは、ログサーバを含む iDC 内の機器へ時刻情報を配信する。
5. NTP サーバは、ログサーバが生成・保存している時刻情報に対して時刻監査を実施する。
6. iDC 内の機器からログサーバにログを送信する。
7. ログサーバは、iDC 内機器のログに高信頼度な時刻情報である時刻認証子を付与して保存する。
8. 後にログサーバ内で保存されたログに付与された時刻認証子の正当性および時刻トレーサビリティの検証を実施する。

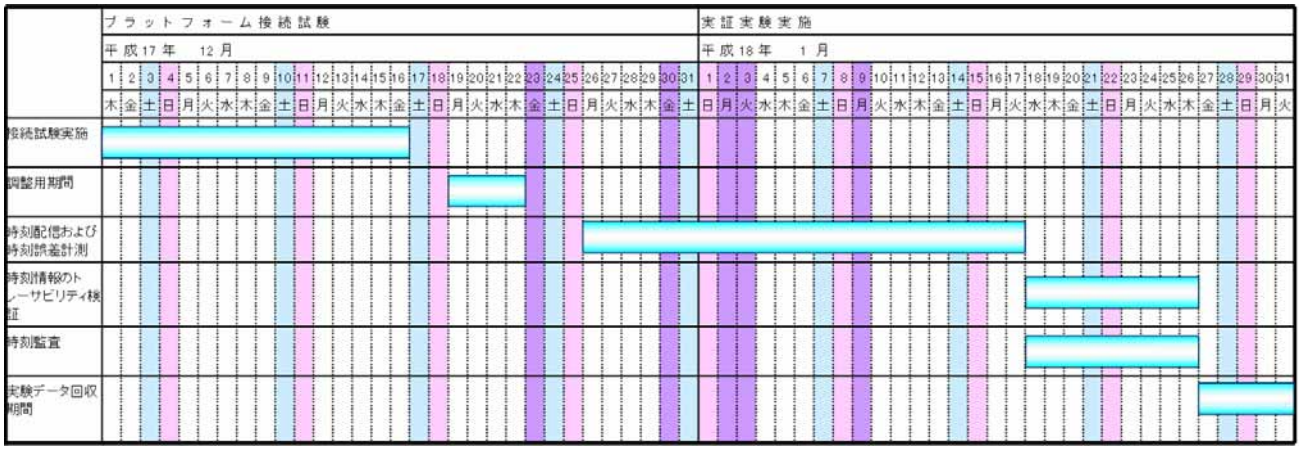
2. 実証実験評価項目

ログサーバ実証実験は、以下の項目について評価を行う。

- iDC 内機器（ログサーバを含む）において、NTP サーバから高信頼度な時刻情報を受信可能なこと。特に NTP サーバと日本標準時との時刻誤差がミリ秒以内であること
- 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 で実施する検証において、ログサーバの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
- 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
- TA2 でのインターネットを介した時刻監査において、NTP サーバが正確な時刻情報を生成・管理していたことを確認できること
- 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
- 長期運用した場合の 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
- 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
- ログサーバ実証実験で使用した時刻配信方式である時刻リンク方式の利便性について

第4章 ログサーバ実証実験期間

ログサーバ実証実験は、平成 17 年 12 月 26 日から平成 18 年 1 月 26 日まで実施した。以下に接続試験から実証実験終了までを記した。



第5章 システム構成

1. ネットワーク

ログサーバ実証実験のネットワーク構成を以下に示す。

NTA2-TA2 間	ローカルネットワーク接続
TA2-NTP サーバ間	インターネット接続(10Mb/s、上り下り対称)

2. ハードウェア

2-1 NTA2

NTA2 のハードウェア仕様を以下に示す。

項目		内容
本体		
	製品名・型番	NEC Mate MA32Y/G-D
	CPU	Pentium4　3.20GHz ×1
	メモリ	1.0GB
	HDD	120GB
	インタフェース	
	ボード・外部装置等	
	寸法	235(W)×350(D)×371(H)[mm]
	重量	約 9.8kg
	電源容量	最大約 240W
キーボード		
	有無	有
	寸法	456(W)×169(D)×40(H)[mm]
ディスプレイ		
	有無	有
	寸法	415(W)×251(D)×428(H)[mm]
	重量	約 7.8kg
	電源容量	最大約 40W

2-2 TA2

TA2 のハードウェア仕様を以下に示す。

項目		内容
本体		
	製品名・型番	NEC Mate MA32Y/G-D
	CPU	Pentium4　3.20GHz ×1
	メモリ	1.0GB
	HDD	120GB
	インタフェース	
	ボード・外部装置等	

	寸法	235(W)×350(D)×371(H)[mm]
	重量	約 9.8kg
	電源容量	最大約 240W
キーボード		
	有無	有
	寸法	456(W)×169(D)×40(H)[mm]
ディスプレイ		
	有無	有
	寸法	415(W)×251(D)×428(H)[mm]
	重量	約 7.8kg
	電源容量	最大約 40W

2-3 NTP サーバ

NTP サーバのハードウェア仕様を以下に示す。

項目		内容
本体		
	製品名・型番	NEC Mate MA32Y/G-D
	CPU	Pentium4　3.20GHz ×1
	メモリ	1.0GB
	HDD	120GB
	インタフェース	
	ボード・外部装置等	
	寸法	235(W)×350(D)×371(H)[mm]
	重量	約 9.8kg
	電源容量	最大約 240W
キーボード		
	有無	有
	寸法	456(W)×169(D)×40(H)[mm]
ディスプレイ		
	有無	有
	寸法	415(W)×251(D)×428(H)[mm]
	重量	約 7.8kg
	電源容量	最大約 40W

2-4 ログサーバ

ログサーバのハードウェア仕様を以下に示す。

項目		内容
本体		
	製品名・型番	NEC Mate MA32Y/G-D
	CPU	Pentium4　3.20GHz ×1
	メモリ	1.0GB
	HDD	120GB
	インタフェース	
	ボード・外部装置等	

	寸法	235(W)×350(D)×371(H)[mm]
	重量	約 9.8kg
	電源容量	最大約 240W
キーボード		
	有無	有
	寸法	456(W)×169(D)×40(H)[mm]
ディスプレイ		
	有無	有
	寸法	415(W)×251(D)×428(H)[mm]
	重量	約 7.8kg
	電源容量	最大約 40W

3. ソフトウェア

3-1 NTA2

NTA2 のソフトウェア仕様を以下に示す。

項目	名称・バージョン等
OS	Linux (RedHat 9)
時刻情報配信装置	時刻情報生成ソフトウェア、時刻情報管理ソフトウェア、時刻情報整合性ソフトウェア、時刻情報拡張配信ソフトウェア、時刻情報内部監査ログソフトウェア、時刻情報監査ソフトウェア
時刻情報受信装置	時刻情報生成ソフトウェア、時刻情報管理ソフトウェア、時刻情報整合性ソフトウェア、時刻情報拡張配信ソフトウェア、時刻情報内部監査ログソフトウェア、時刻情報監査ソフトウェア

3-2 TA2

TA2 のソフトウェア仕様を以下に示す。

項目	名称・バージョン等
OS	Linux (RedHat 9)
時刻情報配信装置	時刻情報生成ソフトウェア、時刻情報管理ソフトウェア、時刻情報整合性ソフトウェア、時刻情報拡張配信ソフトウェア、時刻情報内部監査ログソフトウェア、時刻情報監査ソフトウェア
時刻情報受信装置	時刻情報生成ソフトウェア、時刻情報管理ソフトウェア、時刻情報整合性ソフトウェア、時刻情報拡張配信ソフトウェア、時刻情報内部監査ログソフトウェア、時刻情報監査ソフトウェア

3-3 NTP サーバ

NTP サーバのソフトウェア仕様を以下に示す。

項目	名称・バージョン等
OS	Linux (RedHat 9)

時刻情報配信装置	時刻情報生成ソフトウェア、時刻情報管理ソフトウェア、時刻情報整合性ソフトウェア、時刻情報拡張配信ソフトウェア、時刻情報内部監査ログソフトウェア、時刻情報監査ソフトウェア
時刻情報受信装置	時刻情報生成ソフトウェア、時刻情報管理ソフトウェア、時刻情報整合性ソフトウェア、時刻情報拡張配信ソフトウェア、時刻情報内部監査ログソフトウェア、時刻情報監査ソフトウェア

3-4 ログサーバ

ログサーバのソフトウェア仕様を以下に示す。

項目	名称・バージョン等
OS	Linux (RedHat 9)
時刻情報配信装置	時刻情報生成ソフトウェア、時刻情報管理ソフトウェア、時刻情報整合性ソフトウェア、時刻情報拡張配信ソフトウェア、時刻情報内部監査ログソフトウェア、時刻情報監査ソフトウェア
時刻情報受信装置	時刻情報生成ソフトウェア、時刻情報管理ソフトウェア、時刻情報整合性ソフトウェア、時刻情報拡張配信ソフトウェア、時刻情報内部監査ログソフトウェア、時刻情報監査ソフトウェア
ログ生成装置	改良 syslog-ng、libol

第6章 ログサーバ実験手順

本実証実験の作業手順および利用者が使用するログサーバの使用方法を以下に記す。

1. 実験内容

1-1 時刻配信機能

TA2 にて生成された高信頼度な時刻情報である「時刻認証子」は、時刻同期の標準的なプロトコルである NTPv4 を用いることにより NTP サーバに配信される。NTPv4 により時刻の配信を受けた NTP サーバは、TA2 から受信した時刻認証子を元にして時刻認証子を生成する。実験では、NTP サーバがインターネットを介して TA2 から時刻認証子を受信可能なことを確認する。

NTP サーバの時刻補正機能は、NTPv4 の機能を用いて実現している。実験では、NTP サーバがインターネットを介して TA2 と時刻同期が可能なことを確認する。

1-2 時刻誤差計測

NTP サーバは、上記の 1-1 時刻配信機能で TA2 と時刻補正を行っているが、実証実験では、TA2 との時刻誤差および NTA2 との時刻誤差を計測する。その結果、NTP サーバが、日本標準時と高い精度で時刻同期していたことを確認する。

1-3 時刻情報トレーサビリティ検証機能

NTA2、TA2、NTP サーバ、ログサーバが発行する時刻認証子には、時刻認証子を発行した機器を識別する IP アドレスを含んでいる。NTA2 から時刻認証子を受信した TA2 は、自身が生成する時刻認証子に NTA2 の機器の IP アドレスを含める。TA2 から配信される時刻認証子には TA2 の機器識別子しか含まれないが、時刻認証子が連続性を保つことで、NTA2-TA2-NTP サーバ-ログサーバ間の配信経路の特定が可能になる。

ログサーバで生成・保存されるログには時刻認証子が付与されている。この時刻認証子を検証することにより、日本標準時からログサーバまでの時刻のトレーサビリティが明らかとなる。

実験では、ログサーバからインターネットを介して TA2 に時刻のトレーサビリティ検証が可能であることを確認し、検証に要する時間を計測する。

1-4 時刻監査機能

時刻認証子は時刻認証子を生成した時刻や配信経路情報などを含む管理情報でもある。そのため、時刻認証子の正当性を検査することで、時刻認証子を生成・保存している機器が正しく時刻を生成し、管理、配信を行っていたことを確認することが可能となる。上記の時刻認証子の正当性検査を時刻監査と呼ぶ。

実験では、TA2 が、インターネットを介して NTP サーバへの時刻監査を可能であることを確認し、時刻監査に要する時間を計測する。

2. 実験手順

2-1 時刻配信機能

2-1-1 時刻同期

NTP サーバが TA2 と時刻同期を行っていることを確認する手順を以下に記す。

① NTP サーバにて、ntpq コマンドを実行する。
② ntpq コマンドによって表示された内容から、NTP サーバが TA2 と時刻同期を行っていることを確認する。

2-1-2 時刻認証子配信

NTP サーバが TA2 から時刻認証子を受信していることを確認する手順を以下に記す。

① NTP サーバにて、less コマンドで時刻認証子を保存しているファイル”time.dat”を開く。
② NTP サーバ内に、TA2 から配信されたことを示す時刻認証子が存在することを確認する。

2-2 時刻誤差計測

NTP サーバと日本標準時との間の時刻誤差を計測する手順を以下に記す。

① NTP サーバで保存されている NTP ログから、TA2-NTP サーバ間の時刻誤差を調べる。
② TA2 で保存されている NTP ログから、NTA2-TA2 間の時刻誤差を調べる。
③ ①②で得られた各装置間の時刻誤差の絶対値の和を求めることにより、NTA2-TA2-NTP サーバ間の時刻誤差を計測する。
④ NTA2 サーバは日本標準時と同期しているので、③で得られた値が NTP サーバと日本標準時との時刻誤差である。

2-3 時刻情報トレーサビリティ検証機能

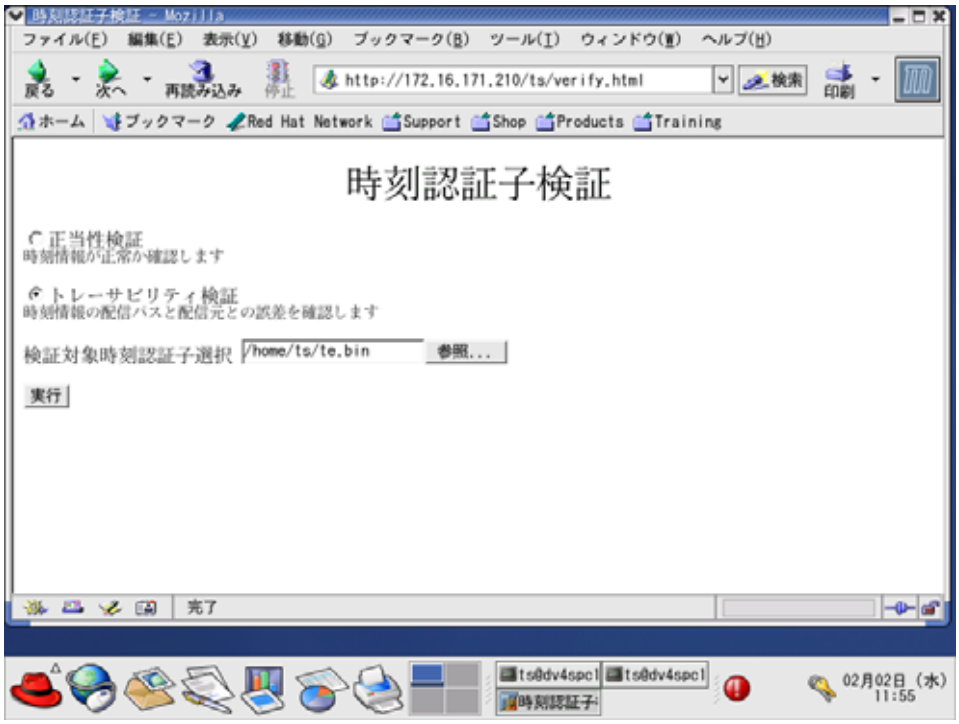
ログサーバで生成・保存されているログに記録されている時刻のトレーサビリティを確認する手順を以下に記す。

① ログサーバで生成・保存されているログに記録されている時刻認証子（下記の赤いアンダーライン部分）をコピーする。

```
2月 21 08:56:09 src@logserver su(pam_unix)[3244]: session opened for user root b
y ts(uid=500) te=027F000104D38403AB00000000000000000DD920A00000000000010104D38403A
A00080957FA43985305000008000000284B74863F00081857FA43414B050020078F725E8A4F8A7D9
3C1A75ECB58F7BE6E63D8EBF43409EF031680C86DA4F80DB9D754A3FC26731E1768ED04304B55BE9
9A1DF92BBAB22AFD64A2325878E4229 hash=73BF59E4DDBADFBB4D184241545DA76B9974049F051
9F9D2456D29E4CD3ED2E2
Feb 21 08:57:10 src@logserver syslog-ng[22763]: STATS: dropped 0 te=027F000104D3
8403AB00000000000000001F930A000000000010104D38403AA00084957FA438797050000080000
0000847F31BF00085657FA43E38A0500208678B67186FBE5035E9C06138718D02C69CC05321A5184
A3A6CABF2F0A2320CC7412BCE3F2D22332B5C80D4881A500707CC63F004475153BA2C804CA98520A
F0 hash=B78BD40638D23141230A82306666E017C38DDE4292C3AC4A36B6475901E9815A
Feb 21 08:57:10 src@logserver syslog-ng[22763]: STATS: dropped 0 te=027F000104D3
8403AB00000000000000001F930A000000000010104D38403AA00084957FA438797050000080000
0000847F31BF00085657FA43E38A0500208678B67186FBE5035E9C06138718D02C69CC05321A5184
A3A6CABF2F0A2320CC7412BCE3F2D22332B5C80D4881A500707CC63F004475153BA2C804CA98520A
F0 hash=9FFC95888DB2164FD3FB33EB1A7E3C60626E8EA2E39243832D3DA2E1B21C864A
```

② ログサーバで時刻認証子取得ツール”getTEfromLog”を実行し、時刻認証子を取得する。(取得した時刻認証子名の例：2006.02.15_13:12:48:225)

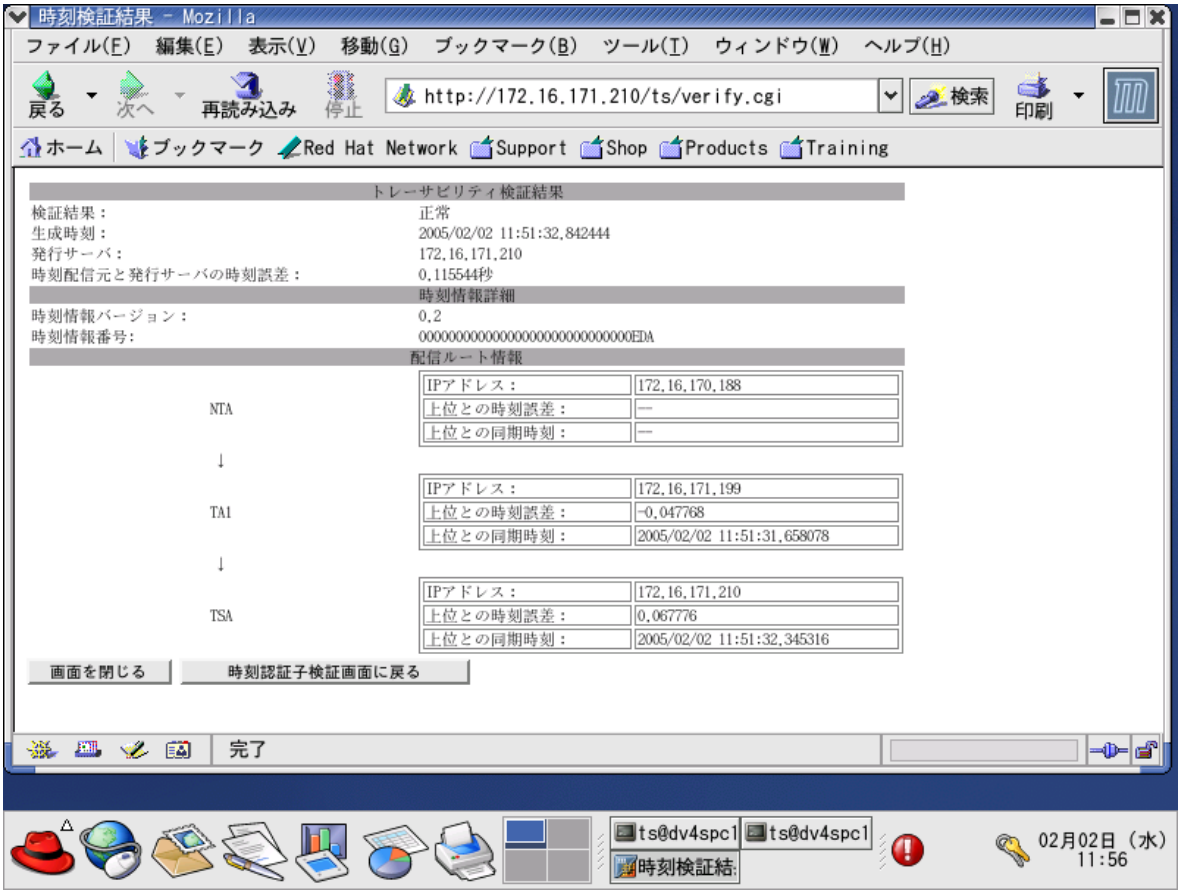
③ ログサーバから TA2 の時刻認証子検証の Web ページにアクセスする。



④ ③の Web ページで「トレーサビリティ検証」を選択し、検証対象時刻認証子を②で取得した時刻認証子を指定する。

⑤ ③の Web ページで実行ボタンを押下する。

⑥ トレーサビリティ検証結果が以下のように表示されるので、NTA2 とログサーバとの時刻誤差、NTA2-TA2-NTP サーバ-ログサーバ間の時刻トレーサビリティを確認する。



⑦　⑤の実行ボタン押下から⑥のトレーサビリティ検証結果が表示されるまでの時間を計測する。

2-4 時刻監査機能

NTP サーバが TA2 から時刻監査を受けていることを確認する手順を以下に記す。

①　NTP サーバから TA2 の時刻認証子監査結果の Web ページにアクセスする。

② ①の Web ページの監査対象期間を入力し、確認ボタンを押下する。

③ 時刻認証子監査結果が以下のように表示されるので、監査結果がすべて正常に完了していることを確認する。

④　また、TA2 に保存されている NTP サーバへの監査記録”audit.log”から監査にかかった時間を確認する。

第7章 実験結果と考察

1. 実験結果

実験手順に従って得られた結果を以下に記す。

1-1 時刻配信機能

NTP サーバが TA2 とインターネットを介した時刻同期が可能であることを確認した。

また、NTP サーバが、インターネットを介して時刻認証子を受信可能であることを確認した。

1-2 時刻誤差計測

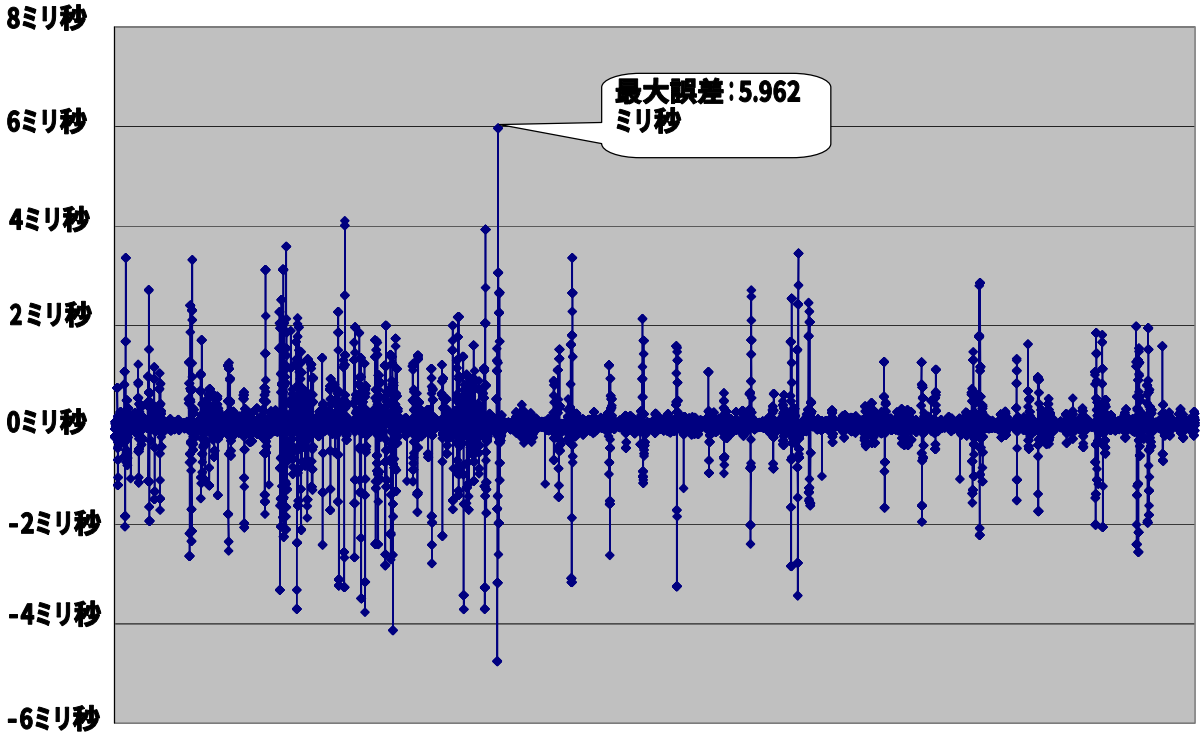
時刻誤差の計測には、1/10～1/17 の一週間の期間で行った。

1-2-1 NTA2-TA2 間の時刻誤差

時刻認証子配信機能を持った NTPv4 による NTA2-TA2 間の時刻誤差を以下に記す。

・平均誤差：0.002322 ミリ秒

・最大誤差：5.962 ミリ秒

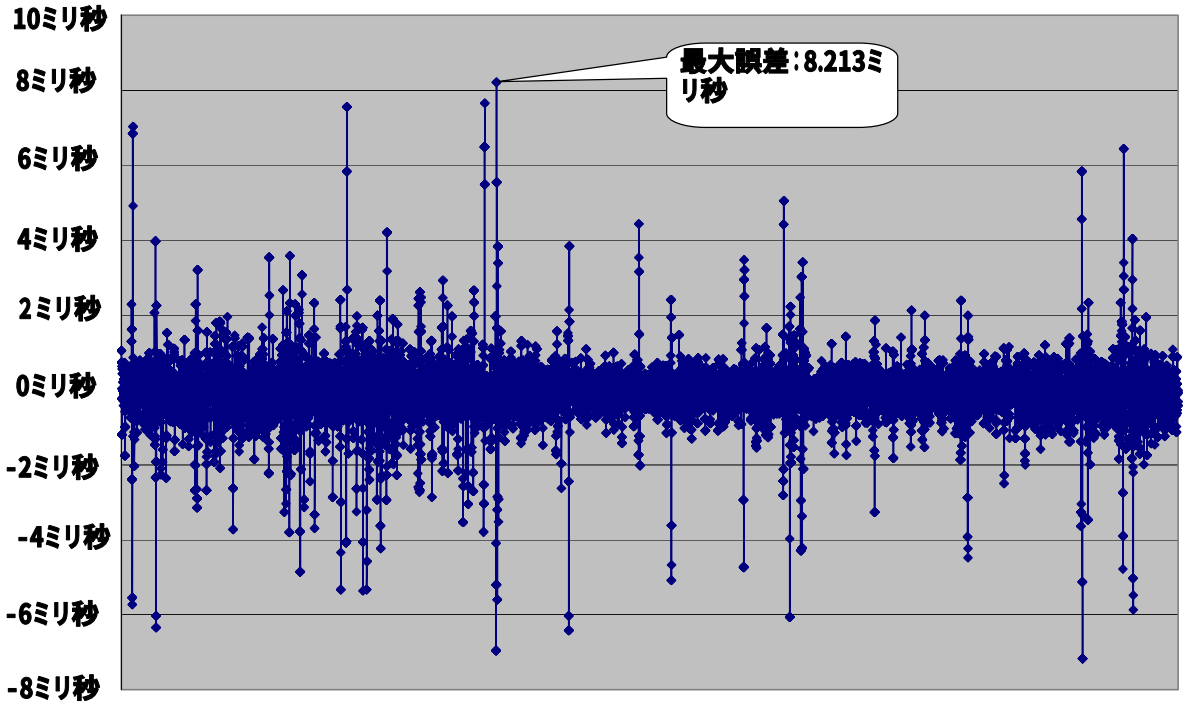


1-2-2 TA2-NTP サーバ間の時刻誤差

時刻認証子配信機能を持った NTPv4 による TA2-NTP サーバ間の時刻誤差を以下に記す。

・平均誤差：0.0438 ミリ秒

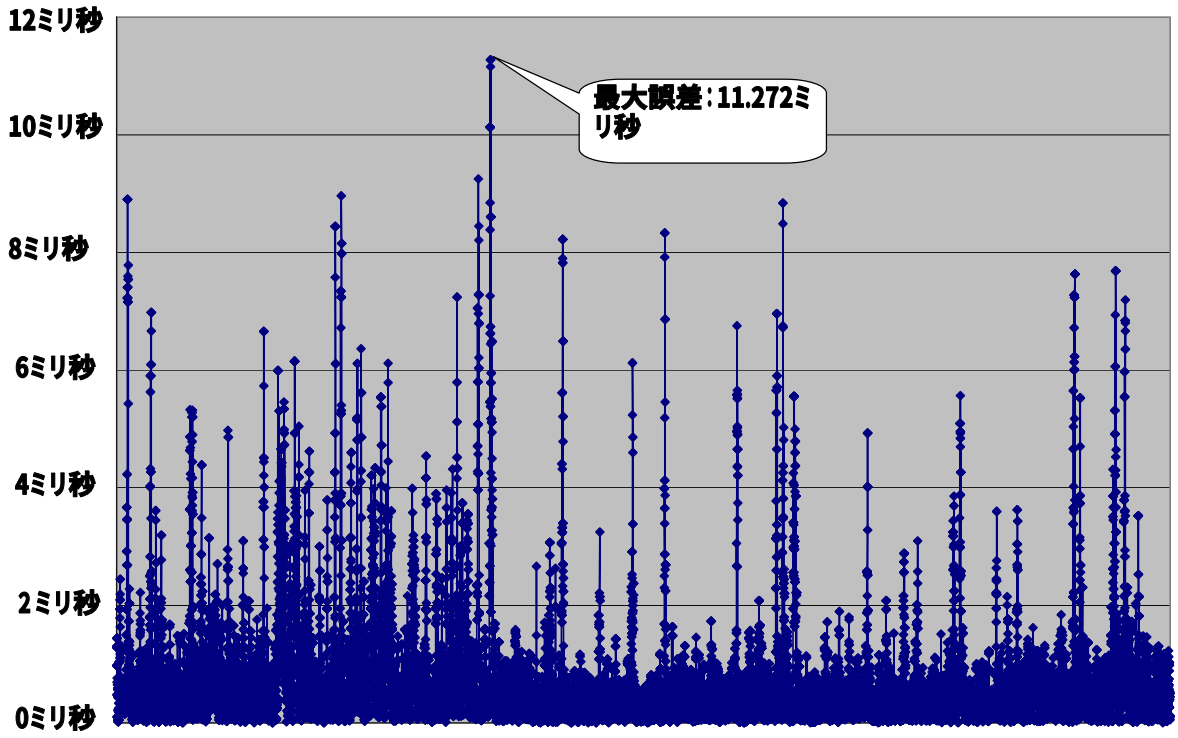
・最大誤差：8.213 ミリ秒



1-2-3 NTP サーバと日本標準時との時刻誤差

時刻認証子配信機能を持った NTPv4 による NTA2-TA2 間の時刻誤差と TA2-NTP サーバ間の時刻誤差のそれぞれの絶対値の和を NTP サーバと日本標準時との時刻誤差とした。以下に NTP サーバと日本標準時との時刻誤差を記す。

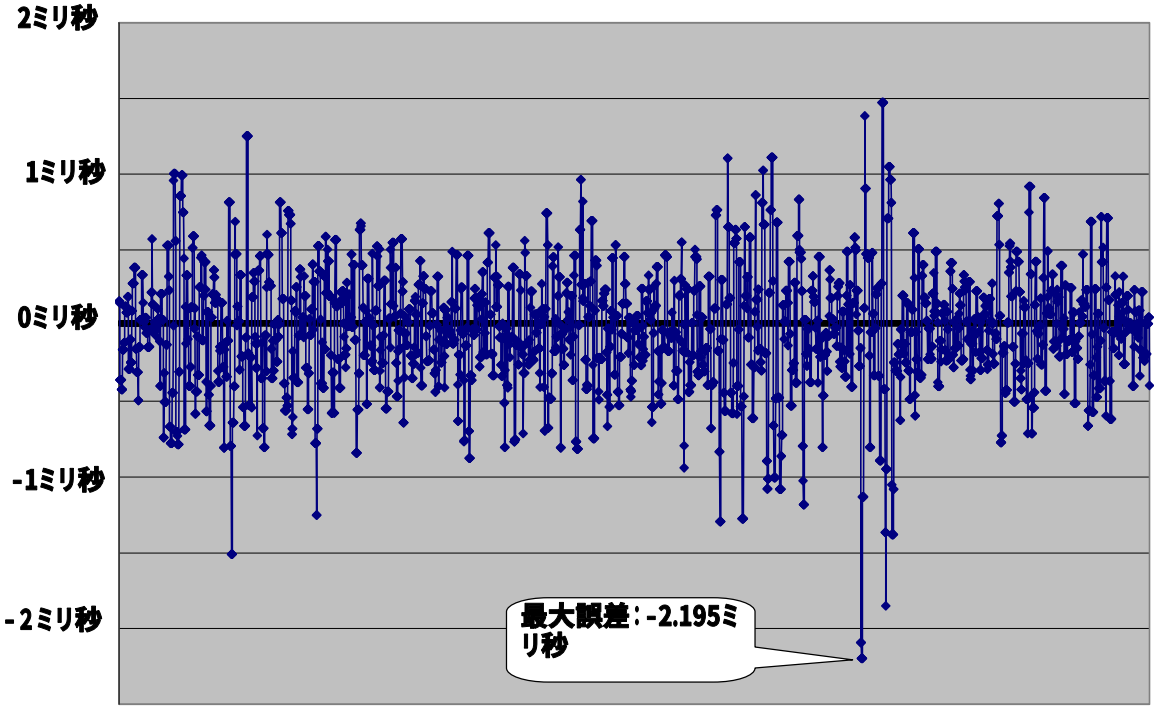
・平均誤差：0.677545 ミリ秒
・最大誤差：11.272 ミリ秒



1-2-4 通常の NTPv4 による時刻同期精度（参考）

一般に使用されている NTPv4 を用いて、TA2-NTP サーバ間の時刻誤差を計測した。なお、計測した期間は 1 日である。

・平均誤差：0.0246 ミリ秒
・最大誤差：-2.195 ミリ秒



1-3 時刻情報トレーサビリティ検証機能

NTA2-TA2-NTP サーバ-ログサーバまでの時刻情報のトレーサビリティの検証がインターネットを介して可能であることを確認した。

また、時刻のトレーサビリティ検証にかかる時間を測定し、その結果を以下に記す。

・時刻のトレーサビリティ検証を行った回数：100 回
・時刻のトレーサビリティ検証にかかった平均時間：8.899 秒

1-4 時刻監査機能

NTP サーバが、インターネットを介して TA2 から時刻監査を受けられることを確認した。

NTP サーバは、TA2 から 1 日 1 回時刻監査を受ける。1 日分の時刻監査を受ける NTP サーバの平均データ量および監査に要する平均時間を以下に記す。

・1 日分の時刻認証子データ量の平均：約 22.22MB
・1 日分の時刻監査に要する時間の平均：約 9 分 37.3 秒

上記から、1 年分の時刻情報の監査に要する時間は、2.5 日程度かかると思われる。

2. 実証実験アンケートの実施

本ログサーバ実証実験結果についてアット東京へアンケートを行ったが、概ね良好の回答を得られた。

3. 考察

上記の実証結果から第 3 章 2.実証実験評価項目についての評価結果および考察を以下に記す。

- **iDC 内機器（ログサーバを含む）において、NTP サーバから高信頼度な時刻情報を受信可能なこと。特に NTP サーバと日本標準時との時刻誤差がミリ秒以内であること**

（評価結果）NTP サーバから iDC 内機器へ高信頼度が受信可能であった。また、NTP サーバと日本標準時との誤差がほぼ 10 ミリ秒以内であった。一部 10 ミリ秒を超えた箇所があるが、アンチウィルスソフトウェア等による影響と思われる。

- **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**

（評価結果）ログ内の時刻認証子のトレーサビリティを検証可能とし、ログの生成時刻の信頼性が向上した。

- **TA2 で実施する検証において、ログサーバの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**

（評価結果）インターネットを介した時刻のトレーサビリティの検証ができた。インターネット上で時刻のトレーサビリティ検証が可能なことにより、インターネット上での信頼できる時刻情報の取得とその時刻情報の検証が可能となった。

- **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**

（評価結果）トレーサビリティ検証にかかる時間は平均 8.899 秒であった。これはトレーサビリティ検証にかかる時間としては十分実用可能な時間と思われる。

- **TA2 でのインターネットを介した時刻監査において、NTP サーバが正確な時刻情報を生成・管理していたことを確認できること**

（評価結果）インターネット上で時刻監査を可能としたことで、時刻認証子による時刻監査はネットワークに依存せず実行可能と思われる。

- **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**

（評価結果）1 年分の時刻認証子の時刻監査に要する時間が約 2.5 日と思われる。1 年分の時刻監査処理が実用可能な時間で完了すると考えている。

- **長期運用した場合の 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**

（評価結果）本実証実験から、30 年間で生成される時刻認証子のデータ量は、約 260GB と予測される。現在一般に使用されている PC でも十分保存可能なデータ量と思われ、実

用可能と考えられる。

- **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**

（評価結果）通常の NTP で 1 日にネットワークを流れるデータ量は、約 13KB と思われる。また、本実証実験で使用した改良 NTP で 1 日にネットワークを流れるデータ量は、約 2742KB と思われる。

通常の NTP と改良 NTP では、通常の NTP のほうが時刻精度が高い。改良 NTP は、時刻のトレーサビリティを保証するための処理やインターネットを介した時刻監査を行っているために通常 NTP より時刻誤差が大きくなっていると思われる。

- **ログサーバ実証実験で使用した時刻配信方式である時刻リンク方式の利便性について**

（評価結果）アット東京へのアンケートによって、時刻リンク方式による時刻配信は、十分実用可能な時刻配信方式と思われる。

以上

文書管理システム実証実験報告書

平成 18 年 3 月 16 日

独立行政法人情報通信研究機構

株式会社エヌ･ティ･ティ･データ

富士ゼロックス株式会社

目次

第 1 章 はじめに 1
1. 背景と目的 1
1-1 背景 1
1-2 目的 1
1-3 概要 1
2. XAdES 2
2-1 概要 2
2-2 本実証実験で用いるタイムスタンププロトコル 4
3. タイムスタンプ付与処理及び検証処理 6
第 2 章 実証実験の内容 11
1. 実証実験の概要 11
2. 実験項目 13
3. 実証実験の体制 15
4. 実証実験の手順 16
4-1 実験環境 16
4-2 作業手順 17
4-3 操作方法 25
4-3-1 文書管理システムへのログイン方法 26
4-3-2 文書登録操作方法 29
4-3-3 デジタル署名及び署名タイムスタンプ付与の操作方法 30
4-3-4 デジタル署名及びタイムスタンプ検証操作方法 35
4-3-5 アーカイブタイムスタンプ（初回）取得操作方法 36
4-3-6 アーカイブタイムスタンプ（効力延長）取得操作方法 36
4-3-7 大量文書一括登録操作方法 37
4-3-8 登録文書の改ざん方法 38
5. 実証実験の結果 39
5-1 時刻トレーサビリティ機能評価 39
5-2 長期保証機能評価 48
5-3 長期保証データ容量評価 54
5-4 例外発生時動作評価 56
5-5 長期保証単一処理時間性能評価 60
5-5-1 署名タイムスタンプ及びアーカイブタイムスタンプ付与の処理時間 60
5-5-2 デジタル署名及び署名タイムスタンプ、アーカイブタイムスタンプ検証の処理時間 62
5-6 長期保証大量処理時間性能評価 65
5-6-1 デジタル署名及び署名タイムスタンプ付与処理 65

5-6-2 アーカイブタイムスタンプ（初回）付与処理結果 68
5-6-3 アーカイブタイムスタンプ（効力延長）付与処理結果 70
5-7 長期保証運用性評価 73
5-8 長期保証操作性評価 75
第 3 章 おわりに 76
1. 成果 76
1-1 各評価項目の評価結果 76
1-1-1 時刻トレーサビリティ機能評価結果 76
1-1-2 長期保証機能評価結果 76
1-1-3 長期保証データ容量評価結果 76
1-1-4 例外発生時動作評価結果 76
1-1-5 長期保証単一処理時間性能評価結果 77
1-1-6 長期保証大量処理時間性能評価結果 77
1-1-7 長期保証運用性評価結果 77
1-1-8 長期保証操作性評価結果 77
2. 今後の課題 79
2-1 時刻のトレーサビリティ調査の自動化 79
2-2 環境や測定条件を変えた際の、大量文書長期保証の処理性能の推移と特性の計測 79

図目次

図 1-1　XAdES フォーマット [3] 3
図 1-2　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処理概要 4
図 1-3　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検証処理概要 5
図 1-4　XAdES における保存形式の変遷 6
図 1-5　署名タイムスタンプ付与処理概要（原本→XAdES-T） 7
図 1-6　アーカイブタイムスタンプ付与処理概要（XAdES-T→XAdES-A） 8
図 1-7　アーカイブタイムスタンプ再付与処理概要（XAdES-A→XAdES-A） 9
図 1-8　署名タイムスタンプ及びアーカイブタイムスタンプの検証処理概要 10
図 2-1　文書長期保存実証実験概要図 11
図 2-2　実験環境 16
図 2-3　ログイン画面の表示 26
図 2-4　ドキュメントスペース一覧画面 27
図 2-5　ドキュメントサービス一覧画面 28
図 2-6　ドキュメントサービス画面 29
図 2-7　「すべて選択」ボタン 30
図 2-8　「証明付与」の選択 31
図 2-9　証明付与画面 32
図 2-10　ファイルの一時ダウンロード確認ダイアログ 33
図 2-11　証明付与画面（証明付与完了後） 34
図 2-12　「原本性検証」の選択 35
図 2-13　検証結果画面 36
図 2-14　大量文書一括登録の様子 37
図 2-15　ApeosWare Flow Service メイン画面 38
図 2-16　ApeosWare Flow Service 履歴画面 38
図 2-17　時刻監査レポート 39
図 2-18　時刻監査レポートの署名情報 40
図 2-19　タイムスタンプの時刻情報に係る配信経路 41
図 2-20　本実証実験で使用した TSA（リンク情報を使用するアーカイビング方式）に対する監査記録 42
図 2-21　本実証実験で使用した TA に対する監査記録 43
図 2-22　タイムスタンプ取得時刻（署名タイムスタンプの検証） 44
図 2-23　TSA の時刻監査規格 46
図 2-24　TA の時刻監査規格 47
図 2-25　原本性保証情報ファイル(XAdES-A)の内容 50
図 2-26　原本性保証情報のデータ容量の変化 55
図 2-27　デジタル署名付与に失敗した際の画面 58
図 2-28　署名タイムスタンプに失敗した際の画面 59

図 2-29　付与処理時間の推移 61
図 2-30　検証処理時間の推移 63
図 2-31　処理時間、総所要時間及び平均所要時間の関係 65
図 2-32　デジタル署名及び署名タイムスタンプ付与の処理時間 66
図 2-33　アーカイブタイムスタンプ（初回）の処理時間 68
図 2-34　アーカイブタイムスタンプ（効力延長）の処理時間 70
図 2-35　推測される処理対象の文書数と所要時間の関係 72
図 2-36　検索条件ファイル 73

表目次

表 1-1　XAdES 形式の種類 2
表 2-1　評価項目及び評価方法 13
表 2-2　事前準備時の分担 15
表 2-3　実証実験期間中の分担 15
表 2-4　実験結果整理時の分担 15
表 2-5　文書管理サーバの構成 17
表 2-6　本実証実験の作業手順 17
表 2-7　各操作と関連手順 25
表 2-8　TST の取得時刻とその時刻誤差 45
表 2-9　本実証実験で用いた XAdES-A をベースにしたフォーマット（概要） 51
表 2-10 デジタル署名、署名タイムスタンプ及びアーカイブタイムスタンプの付与処理結果 52
表 2-11 デジタル署名、署名タイムスタンプ及びアーカイブタイムスタンプの検証処理結果 52
表 2-12　改ざんを実施した際の検証処理結果 53
表 2-13　原本性保証情報ファイルのデータ容量の変化（Bytes） 54
表 2-14　例外発生時のメッセージ一覧（ユーザインタフェース上に現れるものを抜粋） 56
表 2-15　付与処理の処理時間(msec) 60
表 2-16　検証処理の処理時間(msec) 62
表 2-17　改ざんを実施した際の検証処理の処理時間 63
表 2-18　本項で用いる処理時間と所要時間の定義 65
表 2-19　デジタル署名及び署名タイムスタンプ付与の処理結果(msec) 66
表 2-20　デジタル署名及び署名タイムスタンプ付与の所要時間 67
表 2-21　アーカイブタイムスタンプ（初回）の処理結果(msec) 68
表 2-22　アーカイブタイムスタンプ（初回）付与の所要時間 69
表 2-23　アーカイブタイムスタンプ（効力延長）の処理結果(msec) 70
表 2-24　アーカイブタイムスタンプ（効力延長）付与の所要時間 71
表 2-25　タイムスタンプの有効性が損なわれる可能性が生じる場合毎の検索条件キー 74
表 2-26　ユーザビリティ評価結果 75

第1章 はじめに

1. 背景と目的

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効力の長期保証等、いくつかの課題が残っている。

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。

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や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」[1]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。

2. XAdES

2-1 概要

XAdES は CMS 長期署名フォーマットである ETSI[1] TS101 703 V1.5.1(2003-12)"Electronic Signature Formats"を XML 署名に適用するものであり、ETSI TS 101 903(2005-05)"XML Advanced Electronic Signatures(XAdES)"[2]で定義されている。

本実証実験では XAdES 形式をベースにした方式を用いて原本の長期保証を行う。

XAdES には表 1-1 に示す種類がある。

表 1-1 XAdES 形式の種類

#	XAdES 形式の種類	概要
1	XAdES	XAdES 形式の基本となる形式。文書に対するデジタル署名のみ
2	XAdES-T	XAdES 形式にデジタル署名へのタイムスタンプを加えたもの
3	XAdES-C	XAdES-T 形式に署名者及び CA の証明書検証用データを加えた形式(以下の形式を使用する際はオプション要素)
4	XAdES-X	XAdES-C 形式に署名者及び CA の証明書検証用データに対するタイムスタンプを加えた形式(以下の形式を使用する際は非推奨オプション要素)
5	XAdES-X-L	XAdES-X 形式に証明書チェーンへの参照とデジタル署名検証のための証明書の証拠情報を加えた形式
6	XAdES-A	XAdES-X-L 形式の様々な情報に対して再タイムスタンプ(アーカイブタイムスタンプ)を行った形式

デジタル署名が付与された時刻を証明するタイムスタンプを加えた形式を XAdES-T 形式、文書長期保証のための形式を XAdES-A 形式と呼び、本実証実験では XAdES-T 形式及び XAdES-A 形式をベースにした方式のみを用いるものとする。

XAdES 形式は入れ子構造となっており、基本となる XAdES のデジタル署名のみの形式に対し、新たな要素を追加することで XAdES-T 等の情報が追加された形式を表す。

[1]欧州通信規格協会(European Telecommunications Standards Institute) http://www.etsi.org/

XAdES 形式を以下の図 1-1 に示す。

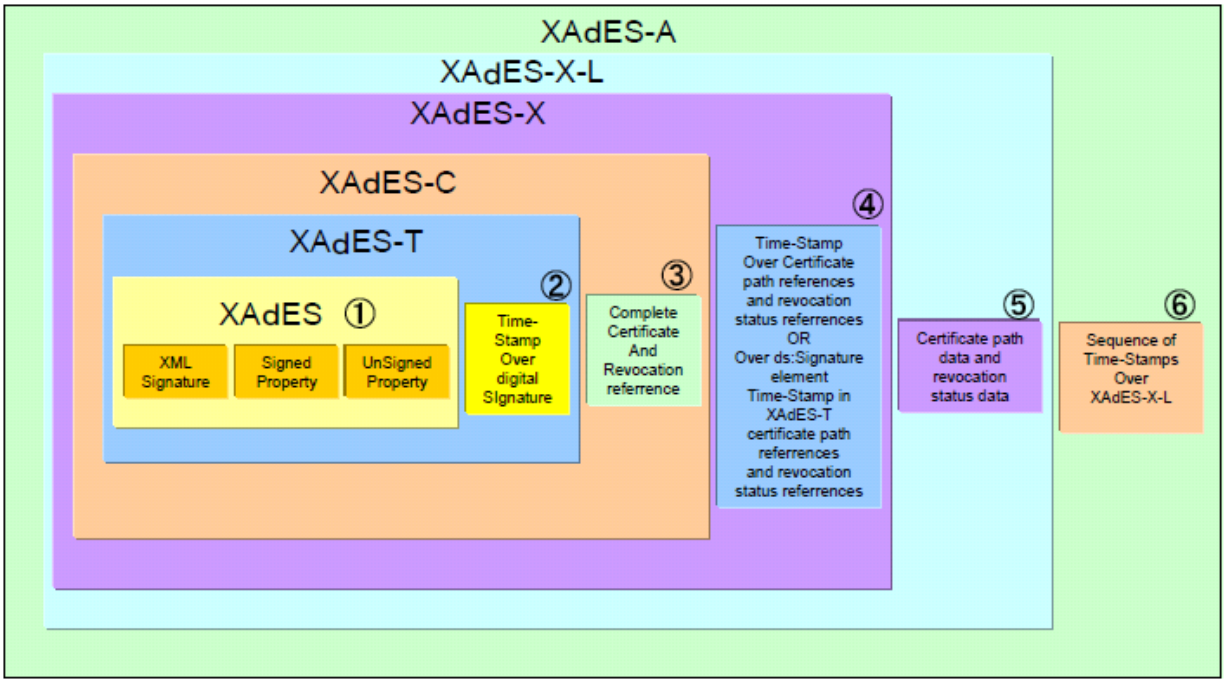


図 1-1 XAdES フォーマット [3]

2-2 本実証実験で用いるタイムスタンププロトコル

XAdES では、格納するタイムスタンプトークンの形式に ISO18014-2 で定義されている ASN.1 形式のバイナリデータが用いられる。

本実証実験では ISO18014-2 で定義されている中のアーカイビング方式に準拠した形式の、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トークンを用いる。

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処理を図 1-2 に示す。

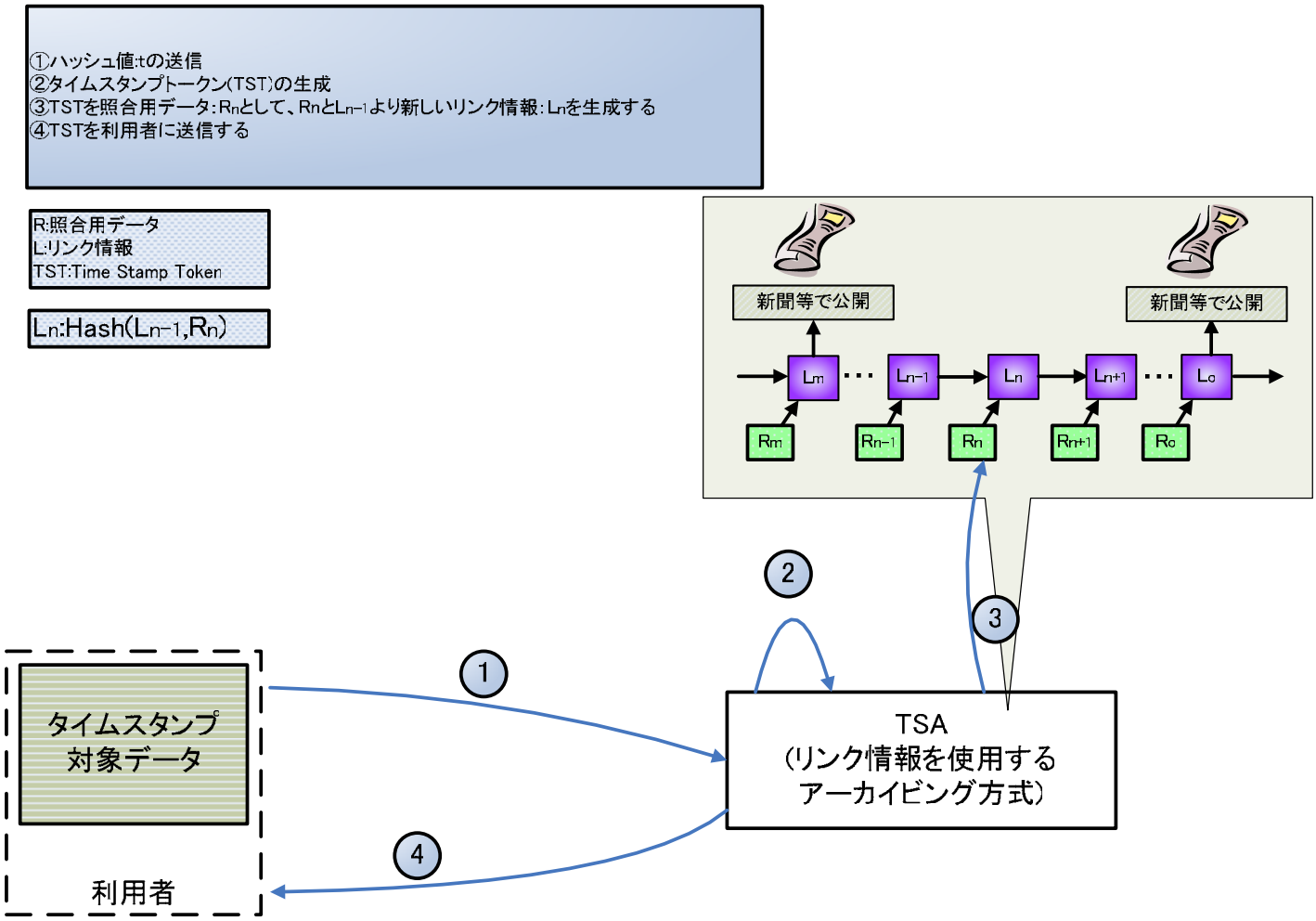


図 1-2 リンク情報を使用するアーカイビング方式のタイムスタンプ付与処理概要

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検証処理を図 1-3 に示す。

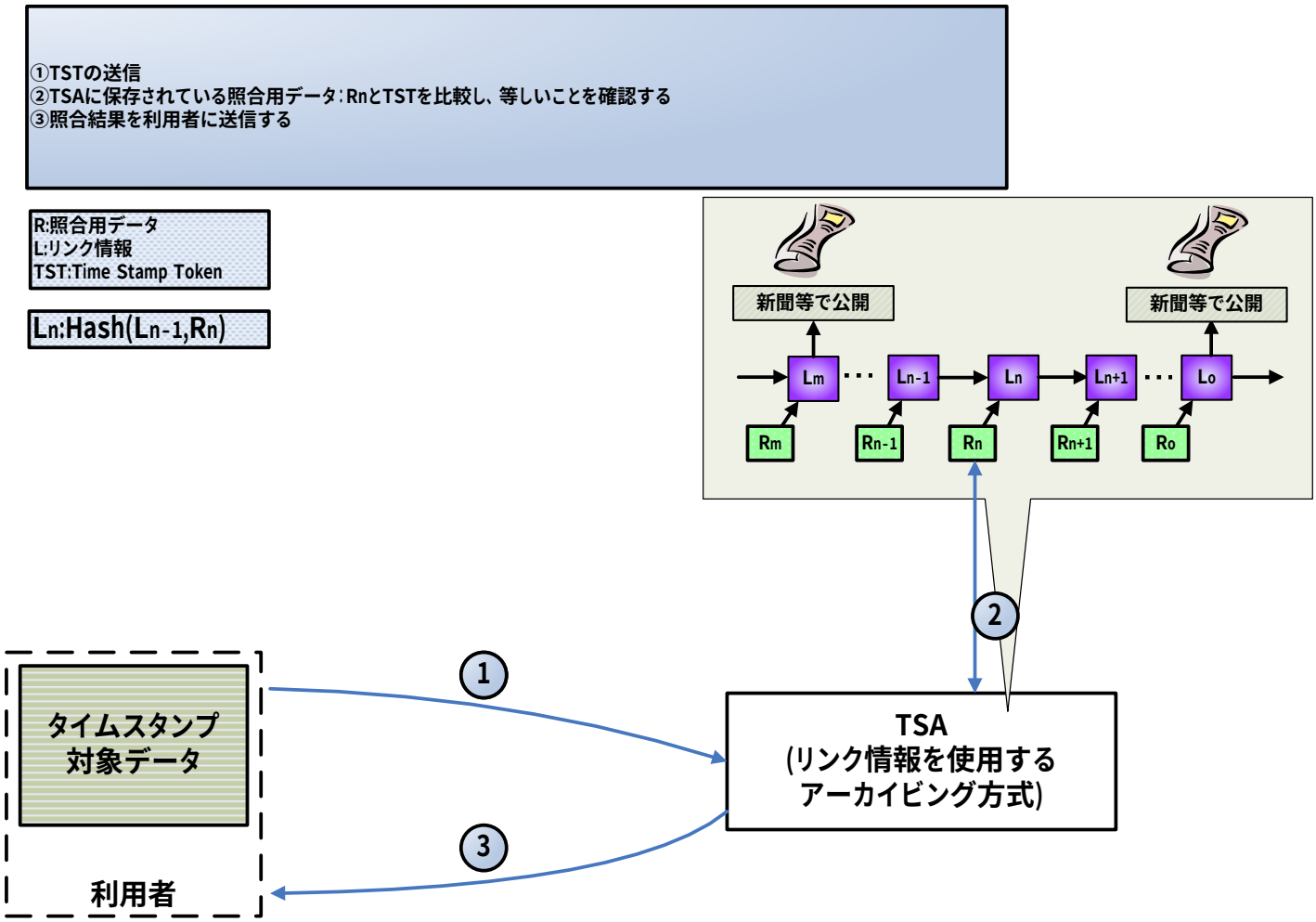


図 1-3 リンク情報を使用するアーカイビング方式のタイムスタンプ検証処理概要

3. タイムスタンプ付与処理及び検証処理

本実証実験では、次世代電子商取引推進協議会（ECOM）において公開されている「XML 長期署名プロファイル（XAdES）（案）」で示されているフォーマットをベースに、タイムビジネス推進協議会（TBF）で公開されている「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（照合業務が継続される場合）に従った長期保証機能を実装し、評価する。

本節では本実証実験で用いられる XAdES 形式をベースにした方式でのタイムスタンプ付与、再付与及び検証の処理概要に関して述べるものとする。

前述したように XAdES-A 形式は文書長期保証のための形式であり、証明書の期限切れやハッシュ関数の脆弱化が発生する前に、原本、デジタル署名、署名情報及びタイムスタンプトークン等の情報に対し、さらにタイムスタンプ（このタイムスタンプをアーカイブタイムスタンプと呼ぶ）を付与することで、原本の再保証を行う。

また、アーカイブタイムスタンプが既に付与されている場合も、既存のアーカイブタイムスタンプを含めて新たなタイムスタンプを付与することが出来る。

XAdES 形式では、このアーカイブタイムスタンプの再付与を繰り返すことによって原本の長期間にわたる保証を可能としている。

図 1-4 に XAdES における保存形式の変遷を示す。

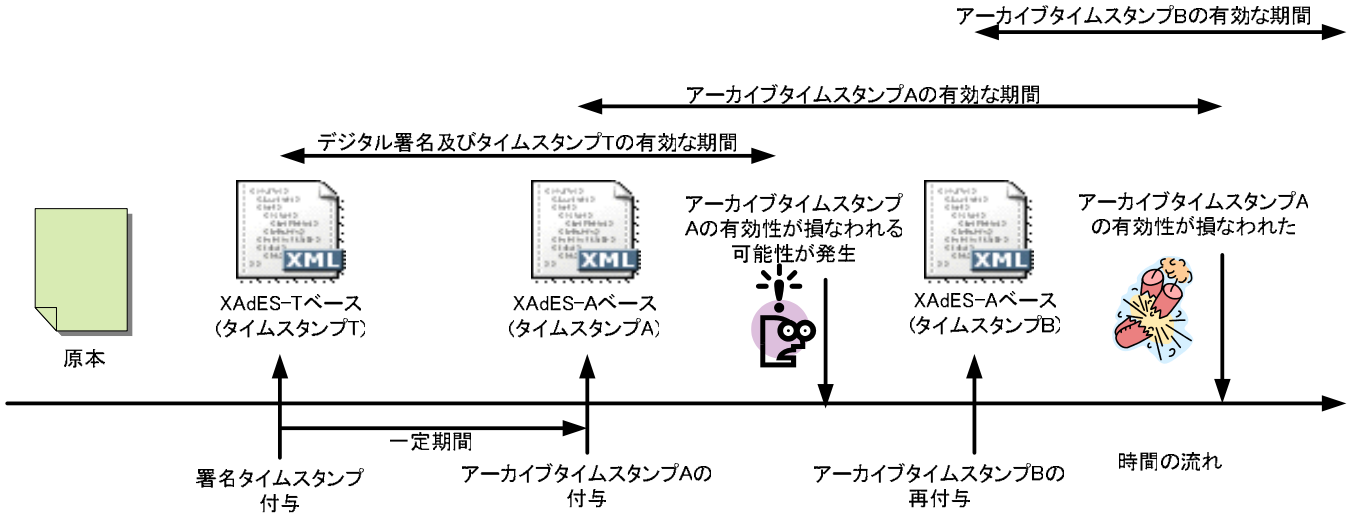


図 1-4　XAdES における保存形式の変遷

図 1-4 中の署名タイムスタンプ T は原本のデジタル署名に対するタイムスタンプであり、タイムスタンプ A はデジタル署名及び署名タイムスタンプ T の効力を担保する。

タイムスタンプ A の有効性が損なわれる可能性が発生した場合、タイムスタンプ A の有効性が損なわれる前に新たにタイムスタンプ B を付与し、タイムスタンプ A の効力を担保する。

各処理の概要に関しては、以降で記述するものとする。

原本のデジタル署名に対する署名タイムスタンプ付与処理の流れを図 1-5 に示す。

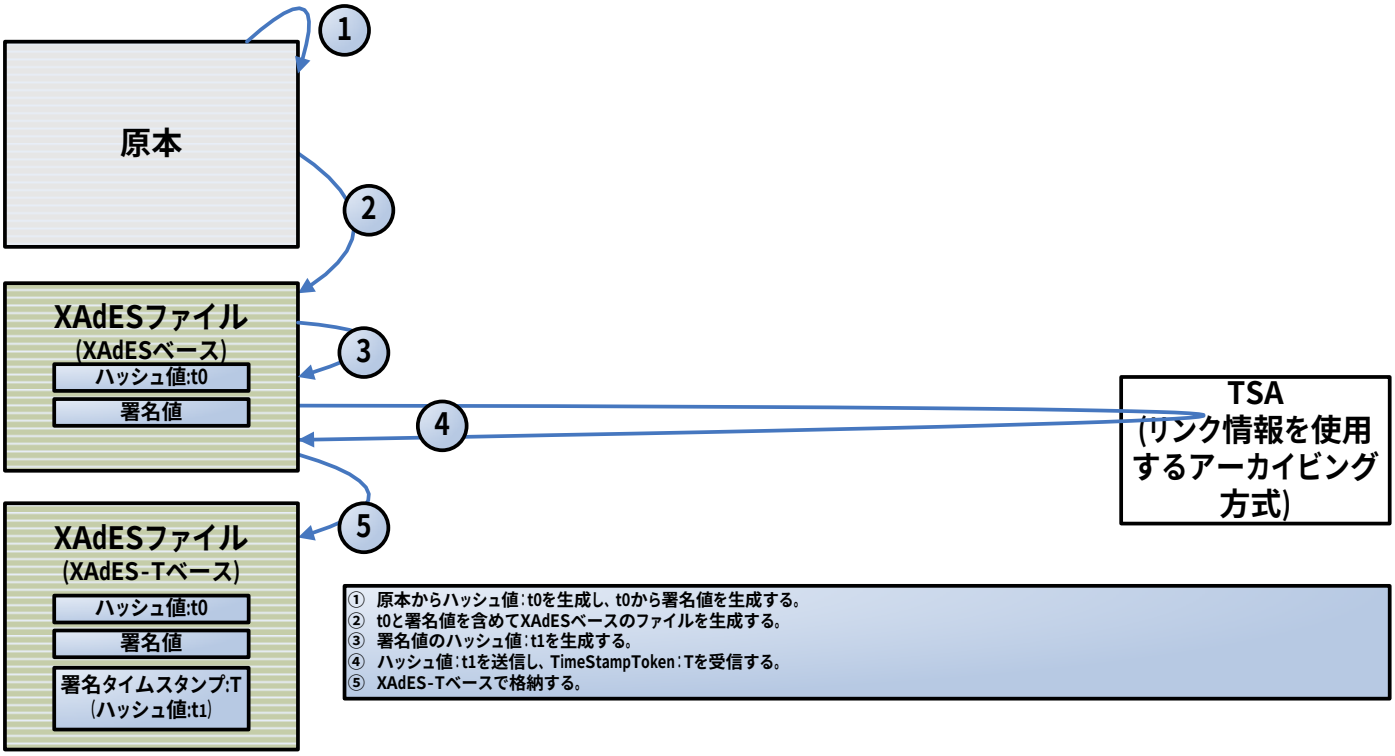


図 1-5　署名タイムスタンプ付与処理概要（原本→XAdES-T）

図中の④が示す処理は、図 1-2 に示すタイムスタンプ付与処理を表している。

XAdES-T 形式に対するアーカイブタイムスタンプ付与処理の流れを図 1-6 に示す。

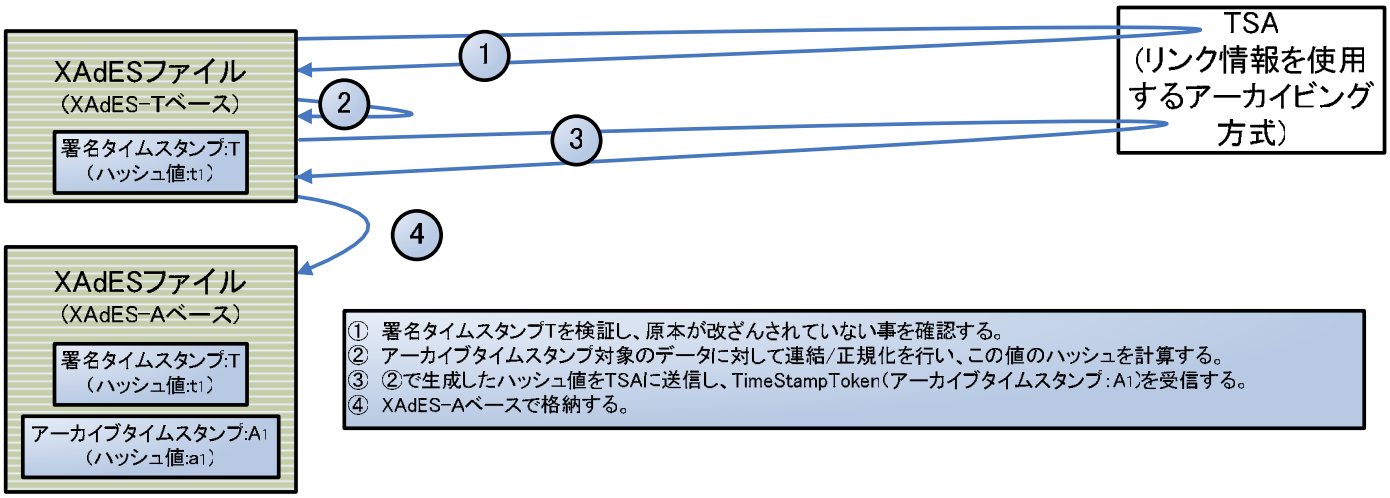


図 1-6　アーカイブタイムスタンプ付与処理概要（XAdES-T→XAdES-A）

図中の①が示す処理は図 1-3 に示すタイムスタンプ検証処理を、図中の③が示す処理は図 1-2 に示すタイムスタンプ付与処理を表している。

XAdES-A 形式に対するアーカイブタイムスタンプ再付与処理の流れを図 1-7 に示す。

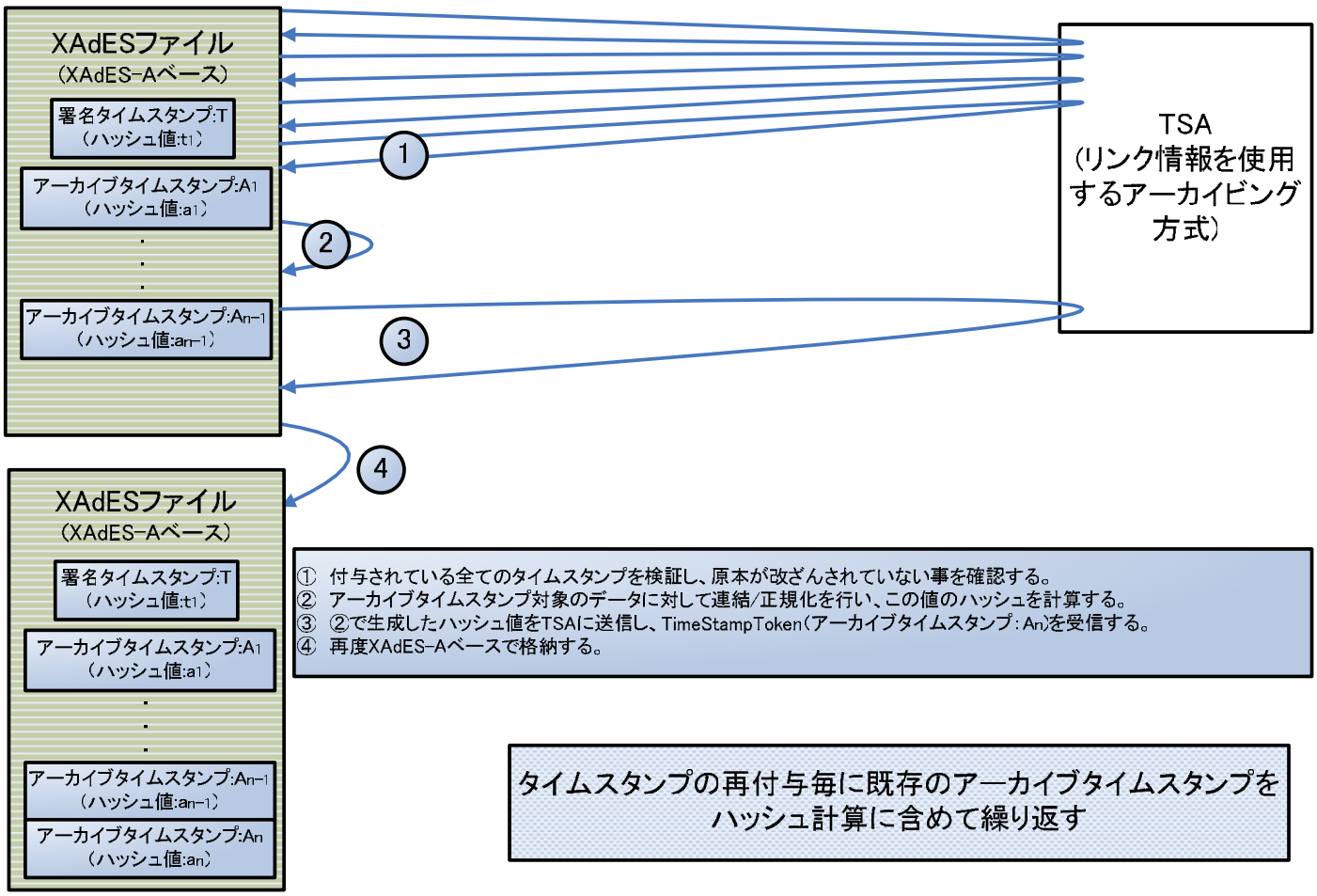


図 1-7　アーカイブタイムスタンプ再付与処理概要（XAdES-A→XAdES-A）

図中の①が示す処理は図 1-3 に示すタイムスタンプ検証処理を、図中の③が示す処理は、図 1-2 に示すタイムスタンプ付与処理を表している。

署名タイムスタンプ及びアーカイブタイムスタンプの検証処理概要を図 1-8 に示す。

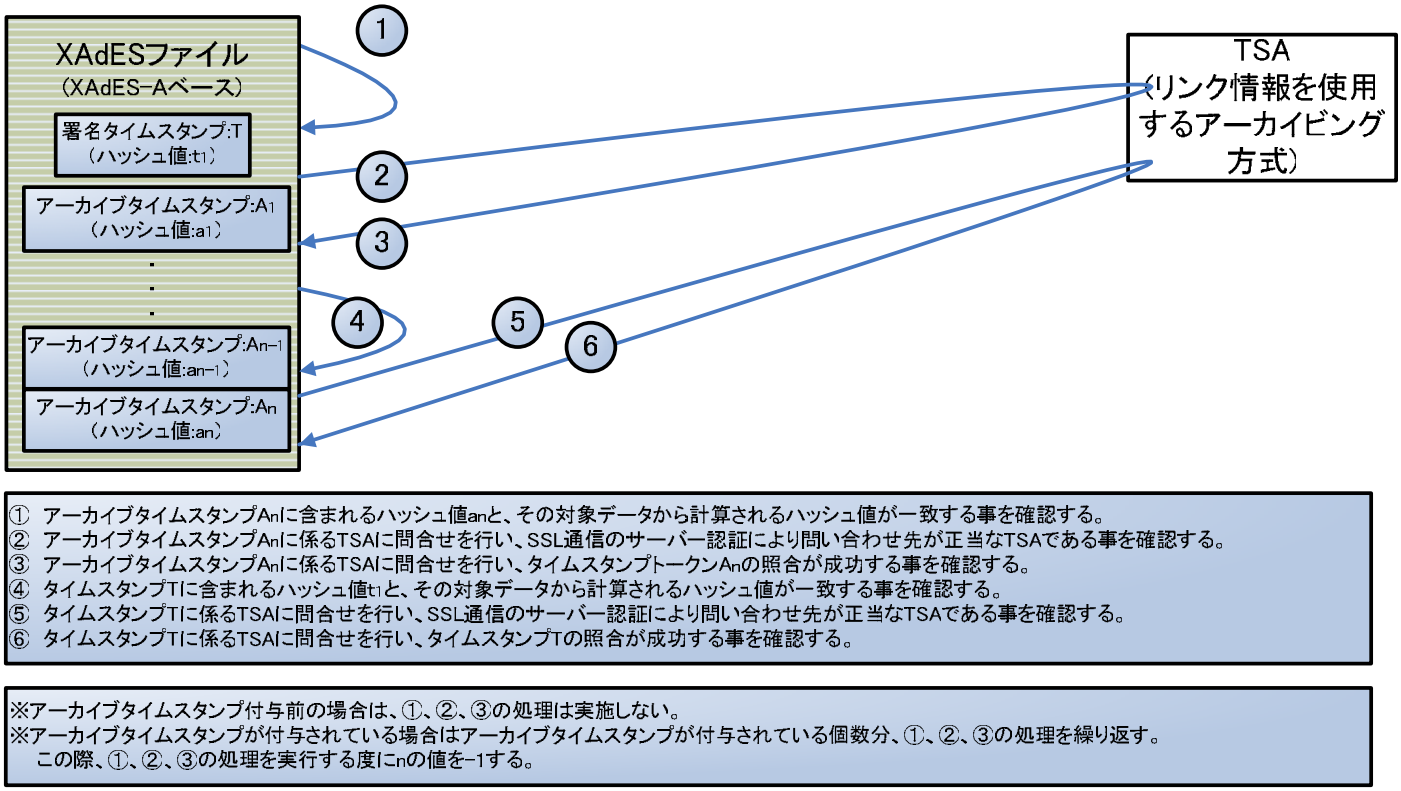


図 1-8　署名タイムスタンプ及びアーカイブタイムスタンプの検証処理概要

図中の③及び⑥が示す処理は図 1-3 に示すタイムスタンプ検証処理を表している。

第2章 実証実験の内容

1. 実証実験の概要

本実証実験では電子文書における原本の存在日時及び真正性を、再タイムスタンプ（アーカイブタイムスタンプ）を繰り返すことによって長期間証明するしくみを文書管理システムに実装し、その性能及び機能を検証する。

利用者及び検証者等の役割を富士ゼロックス及び NTT データで分担して実施する。

利用者は、文書管理システムを操作してタイムスタンプの取得操作を行う。

検証者は、文書管理システムに登録されているファイルに対するタイムスタンプの検証や時刻トレーサビリティの検証を行う。

本実証実験の概要図を図 2-1 に示す。

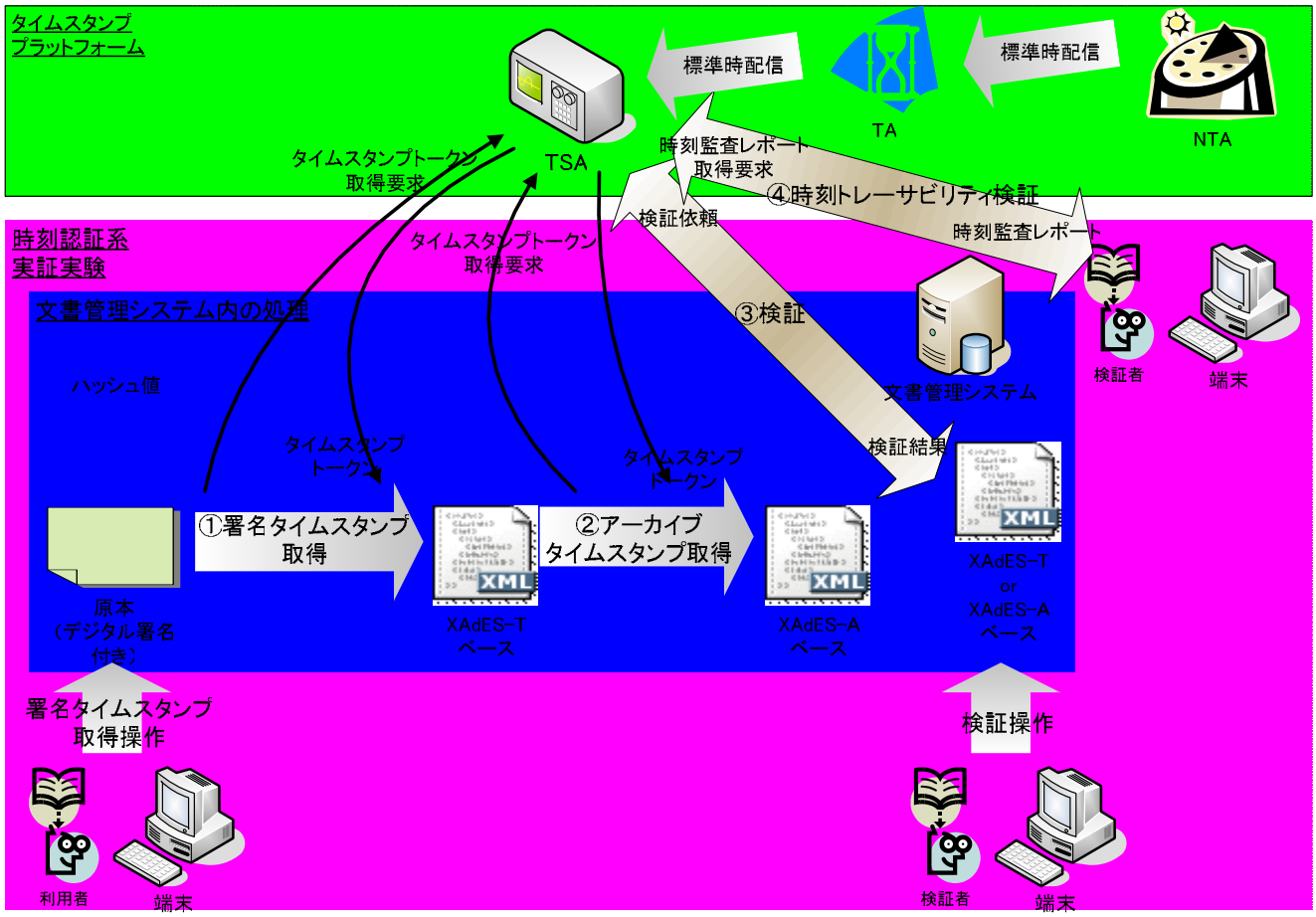


図 2-1　文書長期保存実証実験概要図

文書管理システムに対し、利用者によって署名タイムスタンプ取得操作が行われると、文書管理システムは TSA に接続してタイムスタンプトークンの取得を行い、対象文書のデジタル署名に対して「①署名タイムスタンプ取得」を実行する。

署名タイムスタンプを付与された文書に対しては、一定期間が経過した後に、自動的に「②アーカイブタイムスタンプ取得」が行われる。

署名タイムスタンプ及びアーカイブタイムスタンプに対する「③検証」は検証者が文書管理システムに対して検証操作を行うことによって行われる。

「④時刻トレーサビリティ検証」は National Time Authority(NTA)から TSA までの時刻配信経路情報と、NTA が管理する時刻とタイムスタンプトークンに含まれる時刻情報との時刻誤差情報の検証であり、検証者によって手動で行われる。

2. 実験項目

本章では実証実験の評価項目とその評価方法に関して記述する。

表 2-1 に評価項目及び評価方法を記述する。

表 2-1　評価項目及び評価方法

#	分類	項目名	評価項目	評価目的	評価方法
1	接続試験	時刻トレーサビリティ機能評価	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	タイムスタンプに含まれている時刻情報の配信経路と誤差を確認する機能を利用者環境より利用できることを確認すること	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		長期保証機能評価	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	XAdES をベースにしたフォーマットで、タイムスタンプ長期保証ガイドラインに従った方式により、アーカイブタイムスタンプの付与によるデジタル署名及びタイムスタンプの長期保証の機能が正常に動作することを確認すること	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		長期保証データ容量評価	長期保証する際に保管が必要となるデータの容量	実際にデジタル署名及びタイムスタンプの効力延長を行った際に、どの程度データ容量が増加するかの指標を求めること	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		例外発生時動作評価	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	エラーが発生した場合、適切な対応を判断できるユーザインタフェースとなっていることを確認すること	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。

#	分類	項目名	評価項目	評価目的	評価方法
5	実証実験（性能評価）	長期保証単一処理時間性能評価	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処理時間	署名タイムスタンプ及びアーカイブタイムスタンプに関する単一の処理を実施した際の処理時間の指標を求めること	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
6		長期保証大量処理時間性能評価	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	タイムスタンプの有効性が損なわれる可能性が生じた場合に、それまでに保管された大量の文書に対して効力延長のためのアーカイブタイムスタンプの再付与を行うが、この際にどの程度の時間を要するかの指標を求めること	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
7	実証実験（運用評価）	長期保証運用性評価	AP における長期保証に対応した運用性	アーカイブタイムスタンプによる長期保証が必要となると想定される場面に応じた運用に適した機能となっていることの確認をすること	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		長期保証操作性評価	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	アーカイブタイムスタンプの付与によるデジタル署名及びタイムスタンプの長期保証及びその検証に係る操作性等の利用面からの評価をすること	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。

3. 実証実験の体制

本実証実験における各社の分担を表 2-2、表 2-3 及び表 2-4 に示す。

表 2-2　事前準備時の分担

#	役割	担当
1	TSA の準備	NTT データ
2	文書管理システムの準備	富士ゼロックス

表 2-3　実証実験期間中の分担

#	役割	担当
1	利用者	富士ゼロックス及び NTT データ
2	検証者	富士ゼロックス及び NTT データ
3	TSA の運用	NTT データ

表 2-4　実験結果整理時の分担

#	役割	担当
1	TSA のログ収集	NTT データ
2	文書管理システムからのログ収集	富士ゼロックス
3	TST 検証結果の収集	富士ゼロックス
4	実証実験結果の整理	NTT データ

4. 実証実験の手順

本実証実験の実験環境、作業手順ならびに利用者のタイムスタンプ取得操作及び検証者の検証操作の使用方法を本節に示す。

4-1 実験環境

図 2-2 に本実証実験の環境を示す。

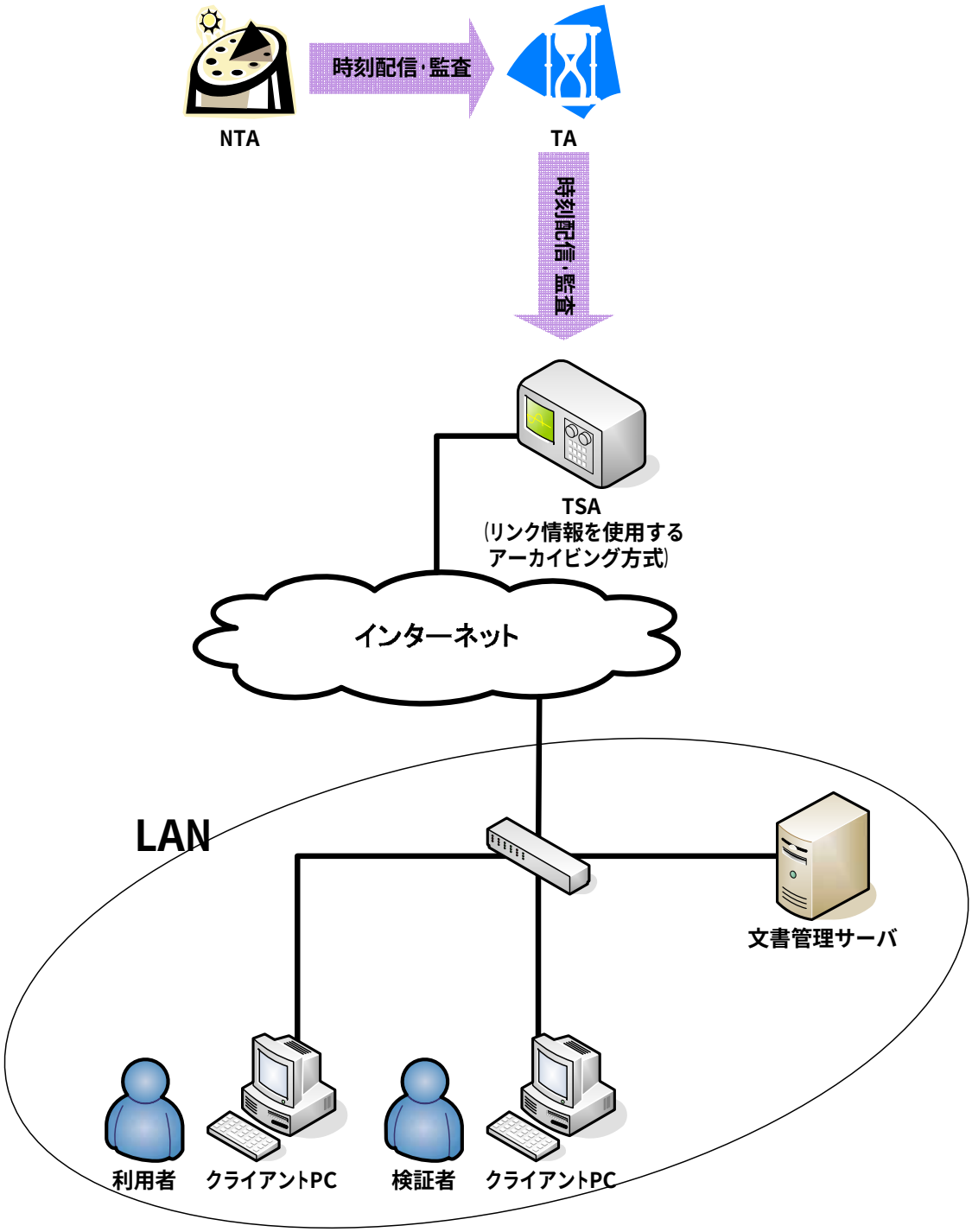


図 2-2　実験環境

また、図 2-2 中の文書管理サーバの機器構成に関して表 2-5 に示す。

表 2-5　文書管理サーバの構成

#	項目名	
1	メーカー	Dell
2	型番	Precision 370
3	OS	Microsoft Windows Server 2003 Standard Edition
4	CPU	Intel Pentium4 3.40 GHz
5	メモリ	3.0 GB

4-2 作業手順

本実証実験の作業手順を表 2-6 に示す。

表 2-6　本実証実験の作業手順

項番	作業項目	作業項目	作業内容	実施日
1-1	事前環境構築	サーバ設定/ネットワーク環境設定/アプリケーション設定		～12/1
2-1	アプリケーション動作確認	動作確認用ファイル生成/登録	①動作確認用のファイルを生成する。 ②動作確認用ファイルを文書管理システムに登録する。	12/5
2-2		デジタル署名付与	①動作確認用のファイルに対してデジタル署名の付与を行う。	12/5
2-3		デジタル署名検証	①2-2 でデジタル署名を付与した全てのファイルに対しアプリケーションの「デジタル署名検証機能」を用いて検証を行う。	12/5
2-4		署名タイムスタンプ付与	①動作確認用のファイル全てに対して署名タイムスタンプの付与を行う。	12/5
2-5		署名タイムスタンプ検証	①2-4 で署名タイムスタンプを付与された全てのファイルの検証を行う。	12/5
2-6	バッチ処理	アーカイブタイムスタンプ付与（バッチ）	①バッチ処理によりアーカイブタイムスタンプ（初回）が付与される。	12/9

項番	作業項目	作業項目	作業内容	実施日
2-7		アーカイブタイムスタンプ検証	①2-6 のバッチ処理の結果、動作確認用ファイル全てにアーカイブタイムスタンプが付与されたことを確認する。 ②全ての動作確認用ファイルに対して検証を行う。	12/9
2-8		アーカイブタイムスタンプ再付与	①動作確認用ファイルに対してアーカイブタイムスタンプの再付与を行う。	12/9
2-9		アーカイブタイムスタンプ検証	①2-8 でアーカイブタイムスタンプを再付与した全てのファイルに対してアーカイブタイムスタンプの検証を行う。	12/9
2-10		アーカイブタイムスタンプ再々付与	①動作確認用ファイルに対してアーカイブタイムスタンプの再々付与を行う。	12/9
2-11		アーカイブタイムスタンプ検証	①2-10 でアーカイブタイムスタンプを再々付与した全てのファイルに対してアーカイブタイムスタンプの検証を行う。	12/9
3-1	ユーザビリティ評価	ユーザビリティ評価 （確認項目 8）	①評価項目に沿って評価を行う。	12/9
4-1	実証実験(機能)	試験用原本ファイルの準備	①10 個の試験用原本ファイルを準備する。 ②①で生成されたファイルのデータ容量を Dir コマンドの結果をテキストファイルに貼り付けることにより記録する。 ③10 個の試験用原本ファイルのコピーを保存する。 ④10 個の試験用原本ファイルを文書管理システムへ登録する。	12/13

項番	作業項目	作業項目	作業内容	実施日
4-2		長期保証時の付与、再付与、検証ができること （確認項目 2） （確認項目 3） （確認項目 5）	①10 個の試験用原本ファイルに対してデジタル署名を行う。 ②生成された XAdES 形式をベースにした方式のファイルを全てアプリケーションの「ファイルのダウンロード機能」を用いてダウンロード後、保存する。 ③②でダウンロードしたファイルに対し、Dir コマンドを実行し、結果をテキストファイルに貼り付けて記録する。	12/13
4-3			①10 個の試験用原本ファイルに対し、署名タイムスタンプを付与する ②署名タイムスタンプ付与前後の XAdES 形式をベースにしたフォーマットのファイルをアプリケーションの「ファイルのダウンロード機能」を用いてダウンロード後、保存する。 ③Dir コマンドの結果をテキストファイルに貼り付けて記録する。	12/13
4-4			①原本を 2 つ改ざんする。 ②アプリケーションに登録されている署名タイムスタンプが付与された文書に対して署名タイムスタンプの検証を行う。 ③「処理時間チェックスクリプト」を用いてログファイルより処理時間を求め、その値を記録する。	12/13
4-5	バッチ処理	アーカイブタイムスタンプ付与（バッチ）	①10 個の XAdES-T 形式をベースにした方式のファイルに対しアーカイブタイムスタンプの付与を行う	12/17

項番	作業項目	作業項目	作業内容	実施日
4-6			①ログファイルを参照して 4-5 の処理が全て成功したことを確認する。 ②4-5 で生成された XAdES-A 形式をベースにした方式のファイルを全てアプリケーションの「ファイルのダウンロード機能」を用いてダウンロード後、保存する。 ③4-5 でアーカイブタイムスタンプされたファイルのデータ容量をアプリケーションの「ファイルのダウンロード機能」を用いてダウンロード後、Dir コマンドの結果をテキストファイルに貼り付けることにより記録する。 ④「処理時間チェックスクリプト」を用いてログファイルより 4-5 での処理時間を求め、その値を記録する。	12/19
4-7			①原本を 2 つ改ざんする。 ②10 個(+改ざん済み 2 個)の XAdES-A 形式をベースにした方式のファイルに付与されている全てのアーカイブタイムスタンプに対する検証を行う ③「処理時間チェックスクリプト」を用いてログファイルより処理時間を求め、その値を記録する。	12/19

項番	作業項目	作業項目	作業内容	実施日
4-8			2 回目のアーカイブタイムスタンプ付与 ①10 個の XAdES-A 形式をベースにした方式のファイルに対し、アーカイブタイムスタンプの再付与を行う ②アーカイブタイムスタンプ付与後のファイルのデータ容量をアプリケーションの「ファイルのダウンロード機能」を用いてダウンロード後、保存する。 ③Dir コマンドの結果をテキストファイルに貼り付けて記録する。 ④「処理時間チェックスクリプト」を用いてログファイルより処理時間を求め、その値を記録する。	12/19
4-9			2 回目のアーカイブタイムスタンプ検証 ①XAdES-A 形式をベースとした方式の原本ファイルを 2 つ改ざんする。 ②4-8 で処理した 10 個の XAdES-A 形式をベースにした方式のファイル及び改ざんした 2 個のファイルに付与されている全てのタイムスタンプに対する検証を行う。 ③「処理時間チェックスクリプト」を用いてログファイルより処理時間を求め、その値を記録する。	12/19

項番	作業項目	作業項目	作業内容	実施日
4-10			3 回目のアーカイブタイムスタンプ付与 ①10個のXAdES-A形式をベースにした方式のファイルに対し、アーカイブタイムスタンプの再付与を行う ②アーカイブタイムスタンプ付与後のファイルのデータ容量を測定するため、アプリケーションの「ファイルのダウンロード機能」を用いてダウンロード後、保存する。 ③Dir コマンドの結果をテキストファイルに貼り付けて記録する。 ④「処理時間チェックスクリプト」を用いてログファイルより処理時間を求め、その値を記録する。	12/19
4-11			3 回目のアーカイブタイムスタンプ検証 ①XAdES-A 形式をベースとした方式の原本ファイルを 2 つ改ざんする。 ②4-10 で処理した 10 個の XAdES-A 形式をベースにした方式のファイル及び改ざんした 2 個のファイルに対し、付与されている全てのタイムスタンプに対する検証を行う。 ③「処理時間チェックスクリプト」を用いてログファイルより処理時間を求め、その値を記録する。	12/19

項番	作業項目	作業項目	作業内容	実施日
4-12			4 回目のアーカイブタイムスタンプ付与 ①10 個の XAdES-A 形式をベースにした方式のファイルに対し、アーカイブタイムスタンプの再付与を行う ②アーカイブタイムスタンプ付与後のファイルのデータ容量を測定するため、アプリケーションの「ファイルのダウンロード機能」を用いてダウンロード後、保存する。 ③Dir コマンドの結果をテキストファイルに貼り付けて記録する。 ④「処理時間チェックスクリプト」を用いてログファイルより処理時間を求め、その値を記録する。	12/19
4-13			4 回目のアーカイブタイムスタンプ検証 ①4-12 で処理した 10 個の XAdES-A 形式をベースにした方式のファイルに付与されている全てのタイムスタンプに対する検証を行う。 ②「処理時間チェックスクリプト」を用いてログファイルより処理時間を求め、その値を記録する。	12/19
5-1		時刻トレーサビリティが確認できること （確認項目 1）	①TSA の Web サーバへブラウザよりアクセスを行い、時刻監査レポート（PDF）を取得する。 ②取得したレポートの内容の確認を行う。 ③取得したレポートを保存する。	12/21
6-1	準備	試験用原本ファイルの準備	①1 万個の試験用原本ファイルを生成する。	01/17

項番	作業項目	作業項目	作業内容	実施日
6-2	実証実験 (性能評価)	一時に大量の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 （確認項目 6） （確認項目 7）	①AP に XAdES-T 形式をベースにした方式で 1 万件の文書ファイルを登録する	01/17-18
6-3			①1 万件の文書に対してデジタル署名及び署名タイムスタンプを付与する。	
6-4			①1 万件登録されていることを AP の「ファイル検索機能」を用いて確認する。	01/18
6-5	バッチ処理	アーカイブタイムスタンプ付与（バッチ）（確認項目 7）	①1 万文書の再付与処理を行う。	01/21-22
6-6		バッチ処理の結果確認 （確認項目 7）	①6-5 のバッチ処理が 1 万件の各文書に対するアーカイブタイムスタンプの付与に全て成功していることをログファイルを参照して確認する。 ②「処理時間チェックスクリプト」を用いてログファイルより全体の処理時間を求め、その値を「ファイル形式遷移管理表」に記録する。	01/23
7-1	実証実験 (運用評価)	AP で長期保証に対応した運用の確認 （確認項目 7）	①タイムスタンプの有効性が（仮想的に）損なわれる可能性が発生した全てのファイルに対し再タイムスタンプ付与を行う。 ②「処理時間チェックスクリプト」を用いてログファイルより全体の処理時間を求め、その値を「ファイル形式遷移管理表」に記録する。	01/23-25
7-2		例外発生一覧の入手 （確認項目 4）	①検証済みの例外一覧を取得し、報告書に記載する。	01/23

※　以下のような網掛け部に関しては、自動で処理される項目であることをあらわしている。

6-5	バッチ処理	アーカイブタイムスタンプ付与（バッチ）（確認項目 7）	①1 万文書の再付与処理を行う。	01/21-22

4-3 操作方法

本項では、4-2 作業手順に記述した手順を実行する際の、文書管理システムの操作方法に関して説明を行う。

本項で説明を行う各操作と、4-2 作業手順の各手順との関連を表 2-7 に示す。

表 2-7　各操作と関連手順

#	操作項目	関連手順
1	4-3-1 文書管理システムへのログイン方法	文書管理システムに関する全ての手順に関係
2	4-3-2 文書登録操作方法	2-1,3-1,4-1
3	4-3-3 デジタル署名及び署名タイムスタンプ付与の操作方法	2-2,2-4,3-1,4-2,4-3,6-3
4	4-3-4 デジタル署名及びタイムスタンプ検証操作方法	2-3,2-5,2-7,2-9,2-11,3-1,4-4,4-7,4-9,4-11,4-13
5	4-3-5 アーカイブタイムスタンプ（初回）取得操作方法	2-6,4-6,6-5
6	4-3-6 アーカイブタイムスタンプ（効力延長）取得操作方法	2-8,2-10,4-8,4-10,4-12,7-1
7	4-3-7 大量文書一括登録操作方法	6-2
8	4-3-8 登録文書の改ざん方法	4-4,4-7,4-9,4-11,4-13

4-3-1 文書管理システムへのログイン方法

Internet Explorer を起動し、文書管理システムのページを開くと、以下の図 2-3 のようにログイン画面が表示される。

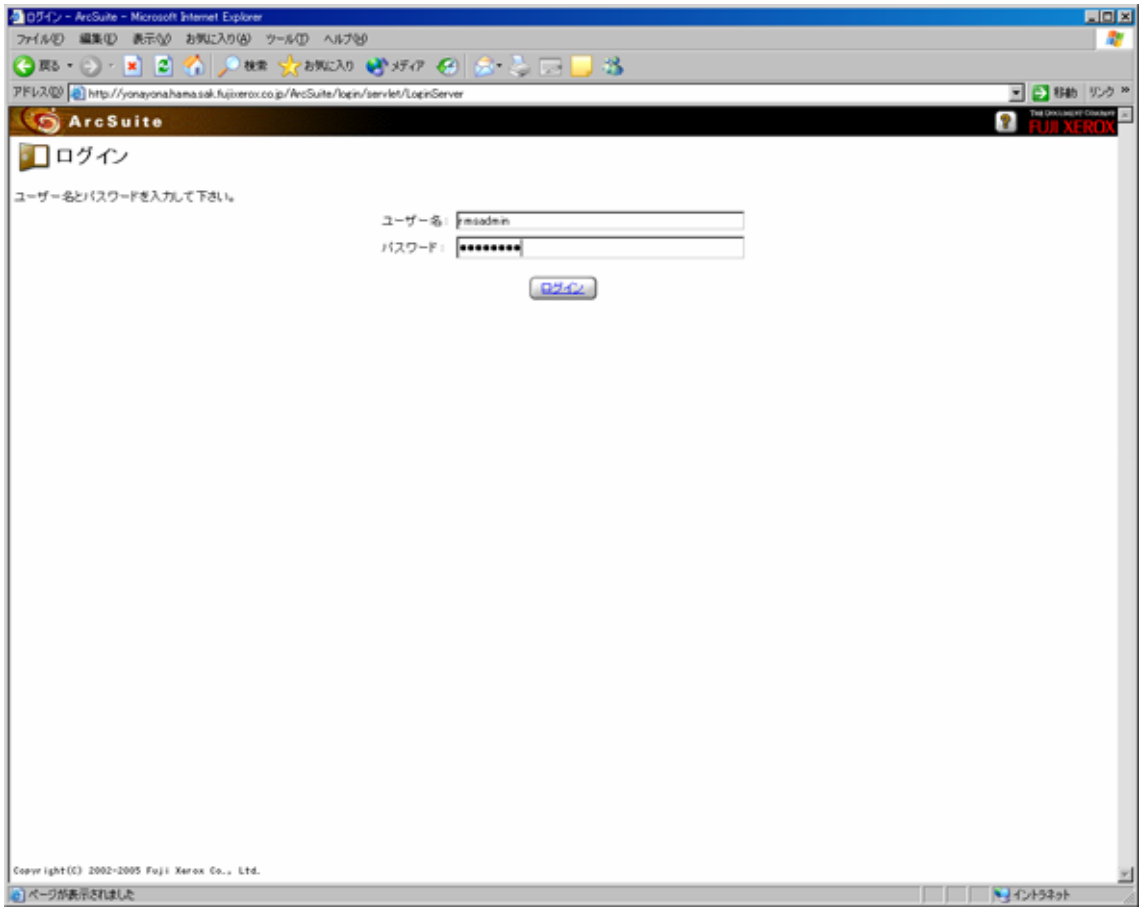


図 2-3　ログイン画面の表示

ログイン画面が表示されたら、ユーザー名とパスワードを入力し、「ログイン」ボタンを押下する。

ログインに成功すると、以下の図 2-4 のように、ドキュメントスペース一覧が表示される。

図 2-4　ドキュメントスペース一覧画面

ドキュメントスペース一覧画面より、使用するドキュメントスペースを選択する。

選択したドキュメントスペース内のドキュメントサービス一覧が図 2-5 のように表示される。

図 2-5　ドキュメントサービス一覧画面

ドキュメントサービス一覧画面より、使用するドキュメントサービスを選択する。

選択したドキュメントサービス画面が図 2-6 のように表示される。

図 2-6　ドキュメントサービス画面

以降の操作は特に説明が無い限りはこの画面より操作を行うものとする。
なお、この操作は利用者及び検証者の両者によって実行される。

4-3-2 文書登録操作方法

文書ファイルの登録は、「図 2-6　ドキュメントサービス画面」に対象ファイルをドラッグ＆ドロップすることで行う。この操作は利用者によって実行される。

4-3-3 デジタル署名及び署名タイムスタンプ付与の操作方法

ここで説明する操作は利用者によって実行される。

文書ファイルへのデジタル署名及び署名タイムスタンプの付与では、「図 2-6　ドキュメントサービス画面」から、まず対象文書のフォルダを表示し、「すべて選択」ボタンをクリックしてフォルダ内の全ての文書を選択する。（フォルダ内の一部の文書を選択する場合はチェックボックスにチェックを入れる。単一のファイルを処理したい場合は、ファイル名の右横のボタン群より、「証明付与」ボタンをクリックする。）

「すべて選択」ボタンについて、以下の図 2-7 に示す。

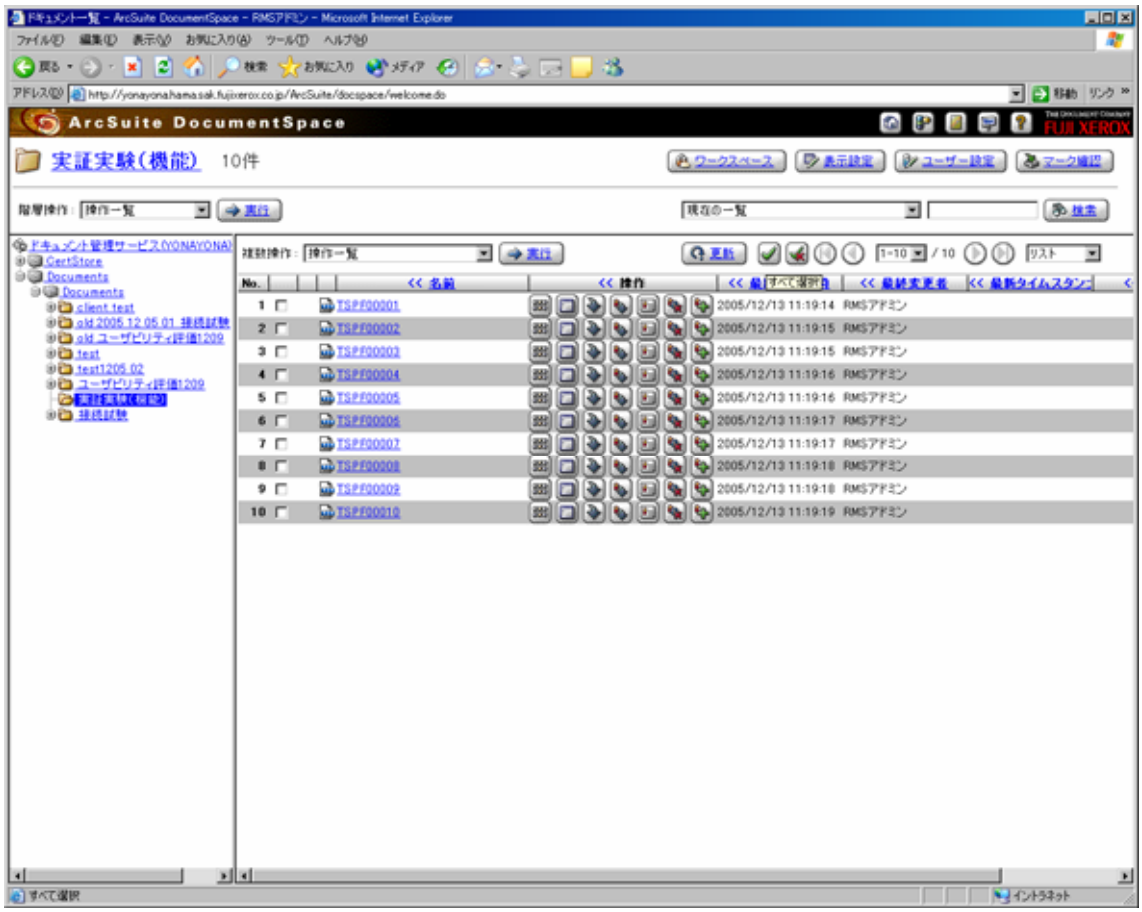


図 2-7　「すべて選択」ボタン

ファイルの選択が終了したら、次にページ上部の「複数操作」リストより「証明付与」を選択する。

「証明付与」ボタンについて、以下の図 2-8 に示す。

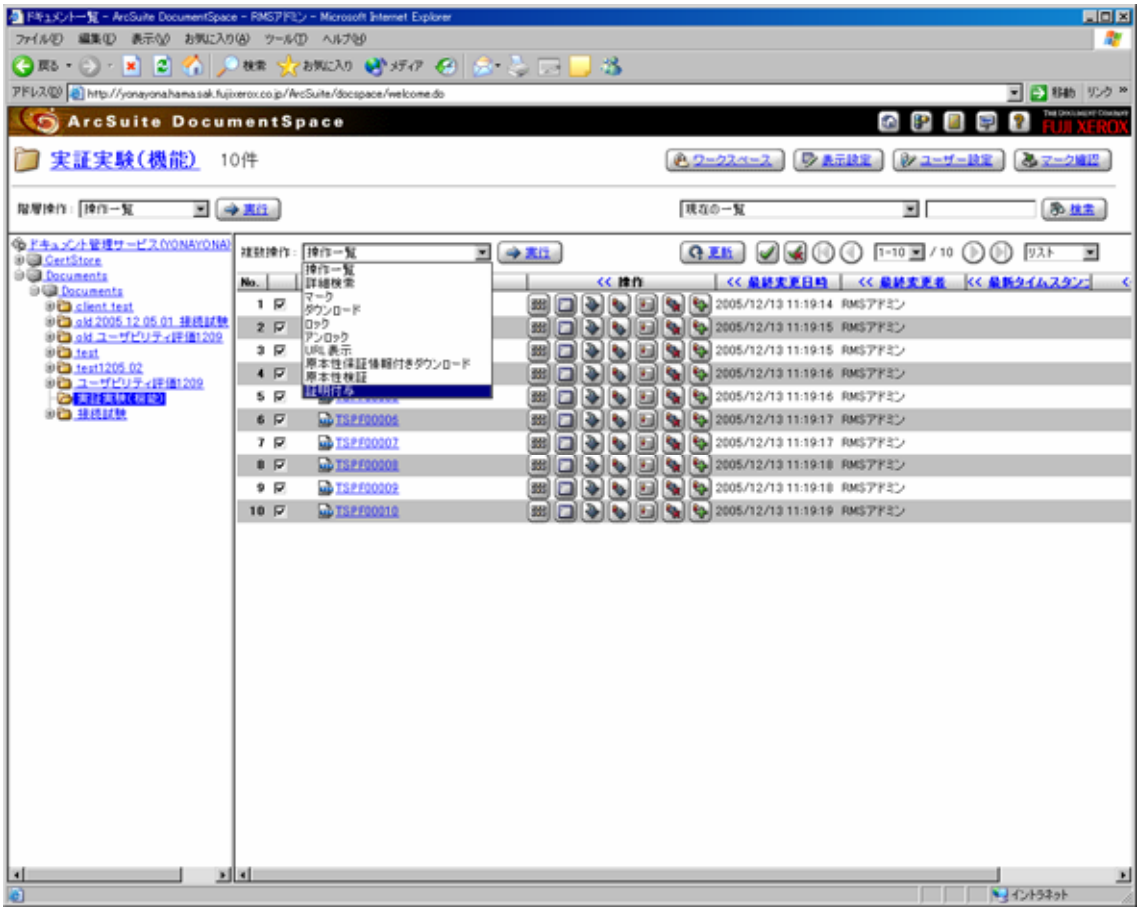


図 2-8　「証明付与」の選択

選択後、図 2-9 のように証明付与画面が表示される。

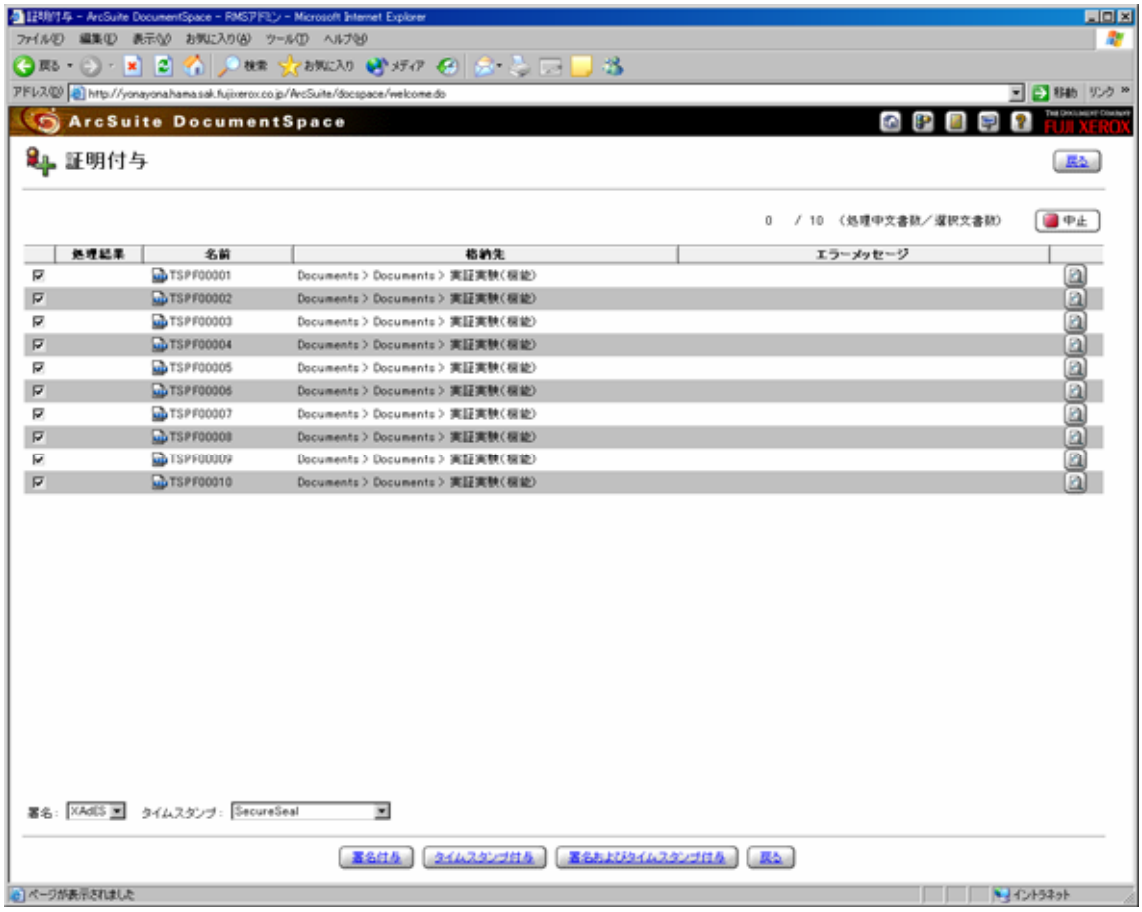


図 2-9　証明付与画面

デジタル署名のみを付与したい場合は「署名付与」ボタンを、既にデジタル署名が付与されているファイルに署名タイムスタンプを付与したい場合は「タイムスタンプ付与」ボタンを、デジタル署名と署名タイムスタンプの両方を一度に付与したい場合は「署名及びタイムスタンプ付与」ボタンを押下する。

ボタン押下後、図 2-10 のようにファイルを一時的にダウンロードするか確認を求めるダイアログが表示される。

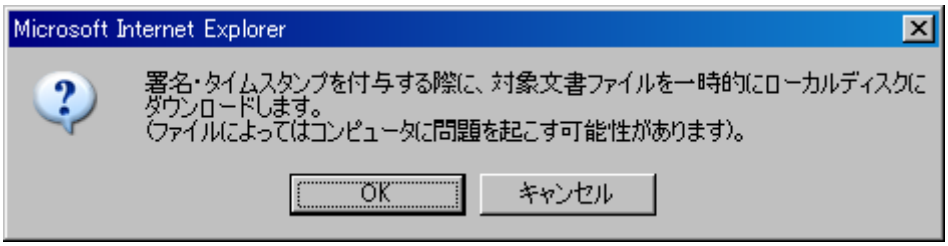


図 2-10　ファイルの一時ダウンロード確認ダイアログ

ダイアログで「OK」ボタンをクリックすると、全ての対象ファイルにデジタル署名及び署名タイムスタンプの付与が実行される。

処理が完了した後、図 2-11 のように付与結果が表示される。

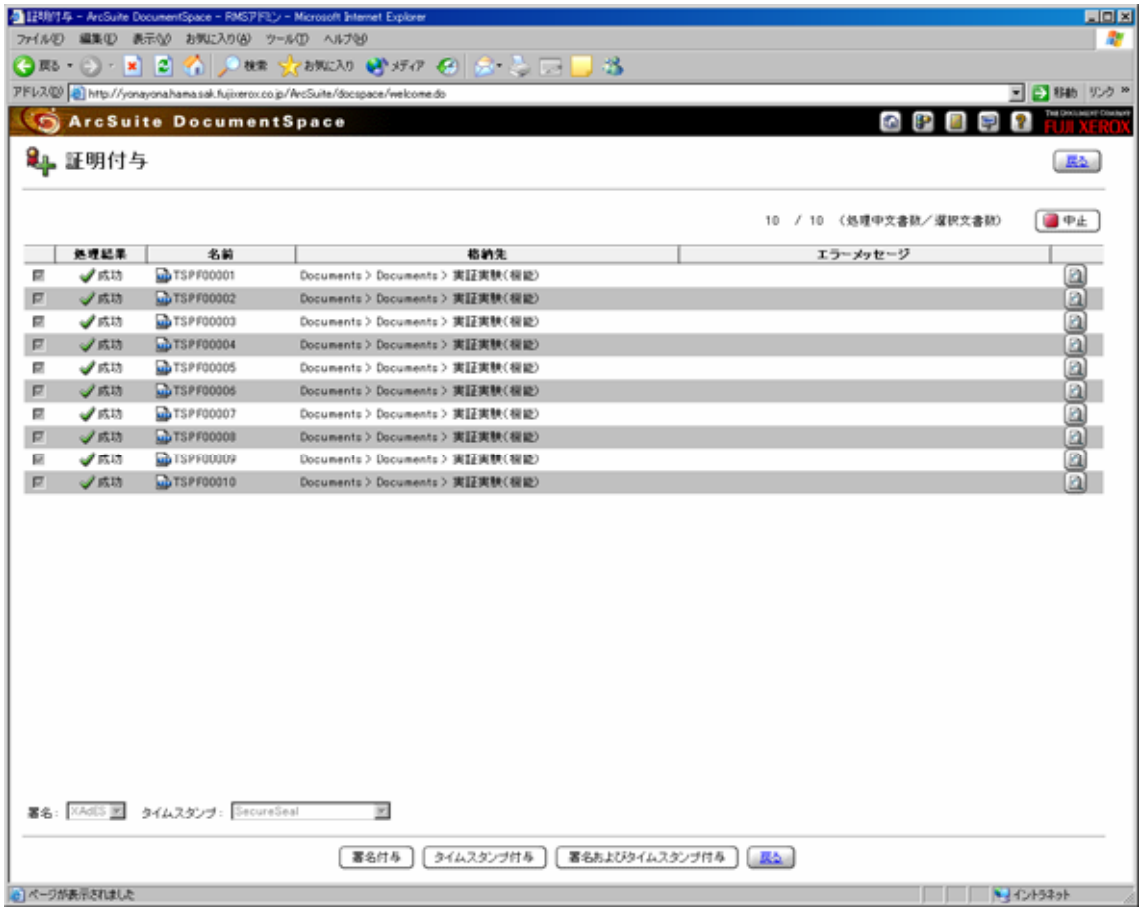


図 2-11　証明付与画面（証明付与完了後）

「戻る」ボタンをクリックするとドキュメントサービス画面に戻る。

4-3-4 デジタル署名及びタイムスタンプ検証操作方法

デジタル署名のみが付与された文書、署名タイムスタンプ付与済みのファイル、アーカイブタイムスタンプ付与済みのファイルのいずれも同じ操作で検証を行うことが出来る。

この操作は検証者によって実行される。

デジタル署名や署名タイムスタンプ、アーカイブタイムスタンプが付与された文書ファイルの検証は、「図 2-6　ドキュメントサービス画面」から、対象文書のフォルダを表示し、「すべて選択」ボタンをクリックしてフォルダ内の全ての文書を選択する。（フォルダ内の一部の文書を選択する場合はチェックボックスにチェックを入れる。単一のファイルを検証したい場合は、ファイル名の右横のボタン群より、「原本性検証」ボタンをクリックする。）

検証対象ファイルを選択したら、「複数操作」リストから「原本性検証」を選択すると、検証処理が実行される。

「原本性検証」の選択について、以下の図 2-12 に示す。

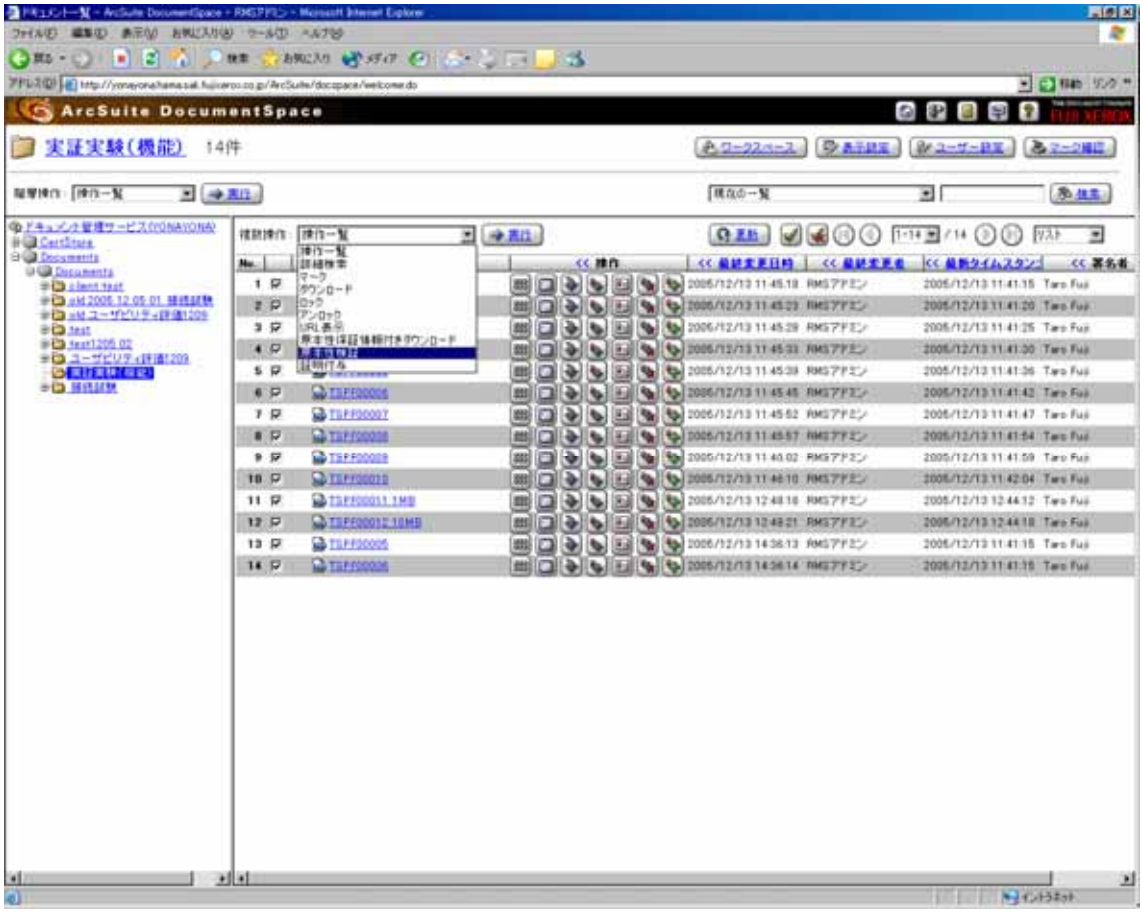


図 2-12　「原本性検証」の選択

選択後、図 2-13 のように検証結果画面が表示される。

図 2-13　検証結果画面

なお、文書の内容が原本性保証情報内の情報と異なる場合は検証に失敗する。

4-3-5 アーカイブタイムスタンプ（初回）取得操作方法

アーカイブタイムスタンプ(初回)は署名タイムスタンプ付与後、一定期間が経過した後に、文書管理システムによって自動的に付与されるため、操作を行う必要は無い。

4-3-6 アーカイブタイムスタンプ（効力延長）取得操作方法

アーカイブタイムスタンプ（効力延長）はハッシュアルゴリズムに脆弱化が生じるなど、タイムスタンプの有効性が損なわれる可能性が生じた場合等に、文書管理システムの管理者によってサーバ上の既存のアーカイブタイムスタンプ（効力延長）用の検索条件ファイルを設定することで行われる。

この操作は文書管理システムの管理者によって実行されるため、利用者及び検証者共にこの操作を実行する必要は無い。

4-3-7 大量文書一括登録操作方法

ここで説明する操作は本実証実験のための操作であり、通常は利用者がこの操作を行うことは無い。

一括登録用 CSV ファイルを作成し、このファイルを引数として「drregist」というツールをコマンドラインより実行することで一括登録を行う。

一括登録の実行画面を、以下の図 2-14 に示す。

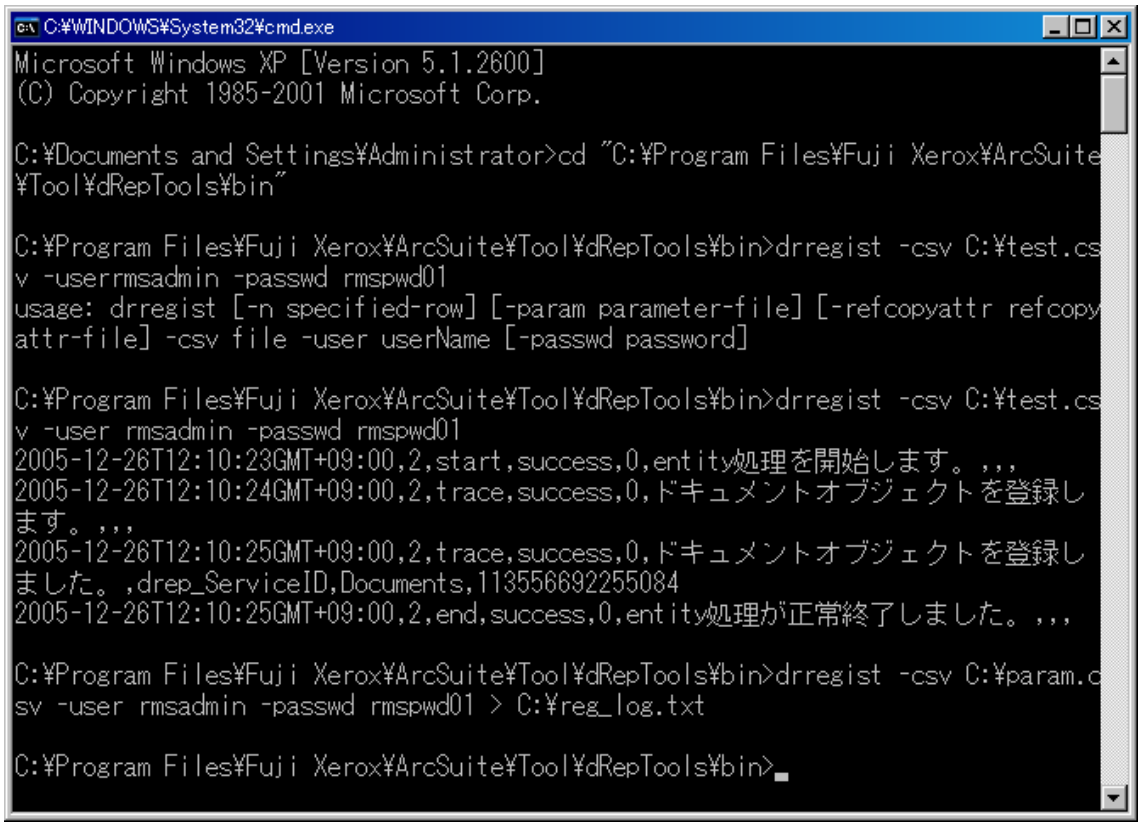


図 2-14　大量文書一括登録の様子

4-3-8 登録文書の改ざん方法

ここで説明する操作は本実証実験のための操作であり、通常は利用者がこの操作を行うことは無い。

本実証実験では、改ざんされたファイルに対して検証処理が失敗することを確認するため、以下の方法を用いてファイルを擬似的に改ざんされた状態にして実験を行った。

ファイルの改ざんには「Fuji Xerox ApeosWare Flow Service」というソフトウェアを使用する。

このソフトウェアは、文書ファイルを原本保証情報の XML ファイル（XAdES をベースにしたフォーマット）と関連付けて、文書管理システムへ直接登録することが出来る。

本実証実験では、このソフトウェアを利用し、実際には対にならない原本ファイルと原本性保証情報の XML ファイルを紐付け、サーバ上に登録することで、擬似的に原本が改ざんされたのと同じ状態を作成した。

ApeosWare Flow Service のメイン画面を図 2-15 に、履歴画面を図 2-16 に示す。

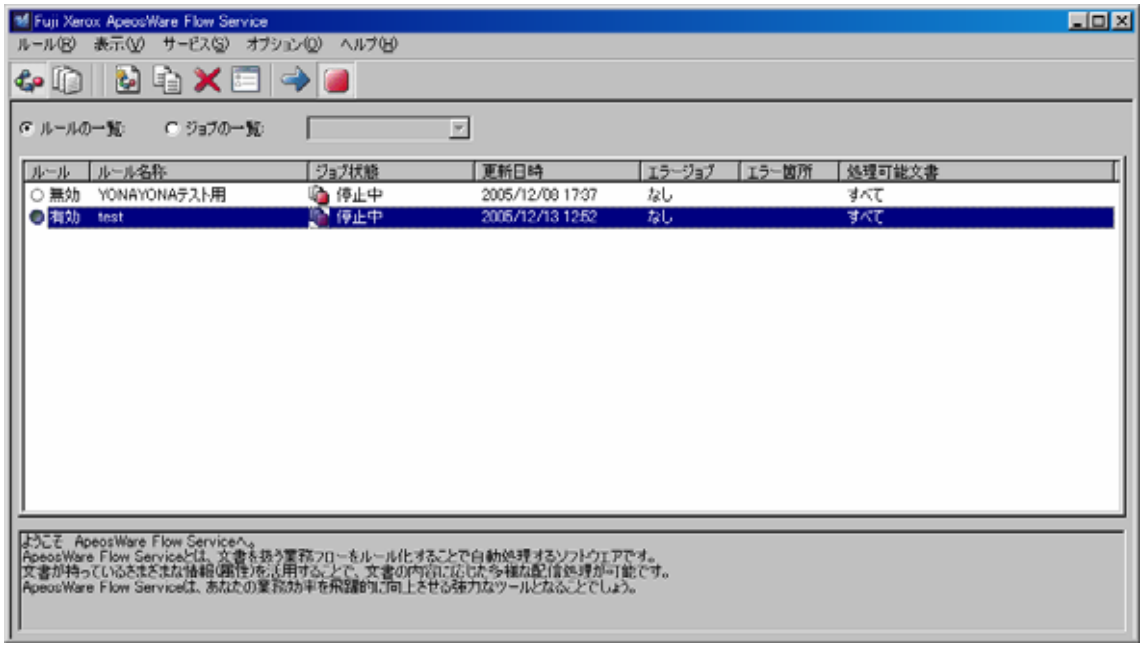


図 2-15　ApeosWare Flow Service メイン画面

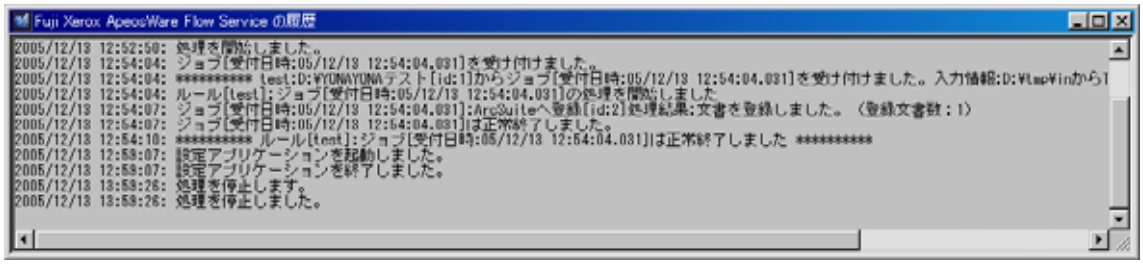


図 2-16　ApeosWare Flow Service 履歴画面

5. 実証実験の結果

本節では、本実証実験の結果を示す。

5-1 時刻トレーサビリティ機能評価

実証実験の手順において取得した時刻監査レポートより、時刻監査情報の確認結果を以下に示す。（一部抜粋）

本実証実験では、時刻監査結果の確認を、時刻監査レポートを TSA の Web サーバより取得することで行った。

図 2-17 は、時刻監査レポートの表紙である。画面右下にデジタル署名が付与されていることがわかる。

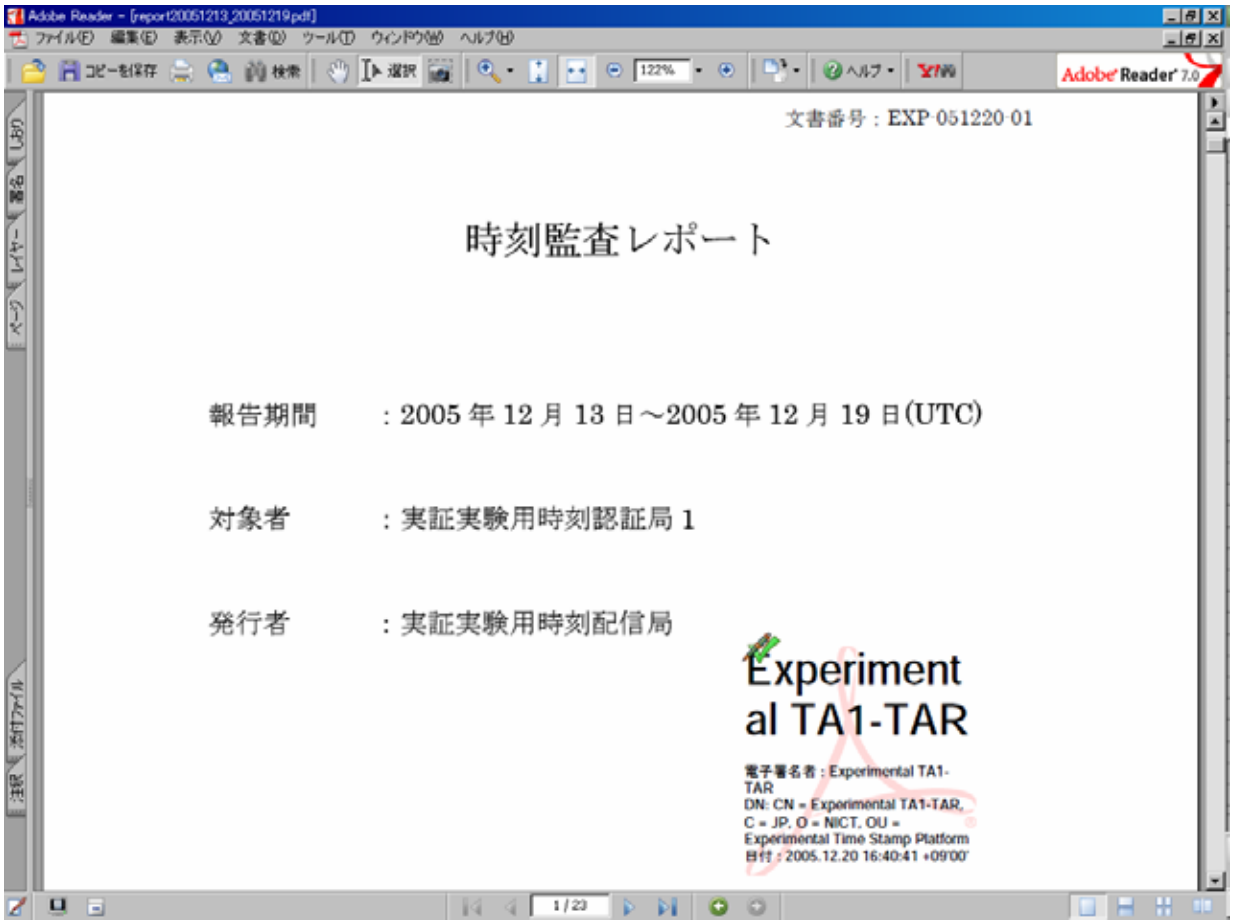


図 2-17　時刻監査レポート

図 2-18 は、時刻監査レポートのデジタル署名のプロパティである。

図 2-18 より、時刻監査レポートに付与されているデジタル署名の検証によって、文書が変更されていないことが証明されていることがわかる。

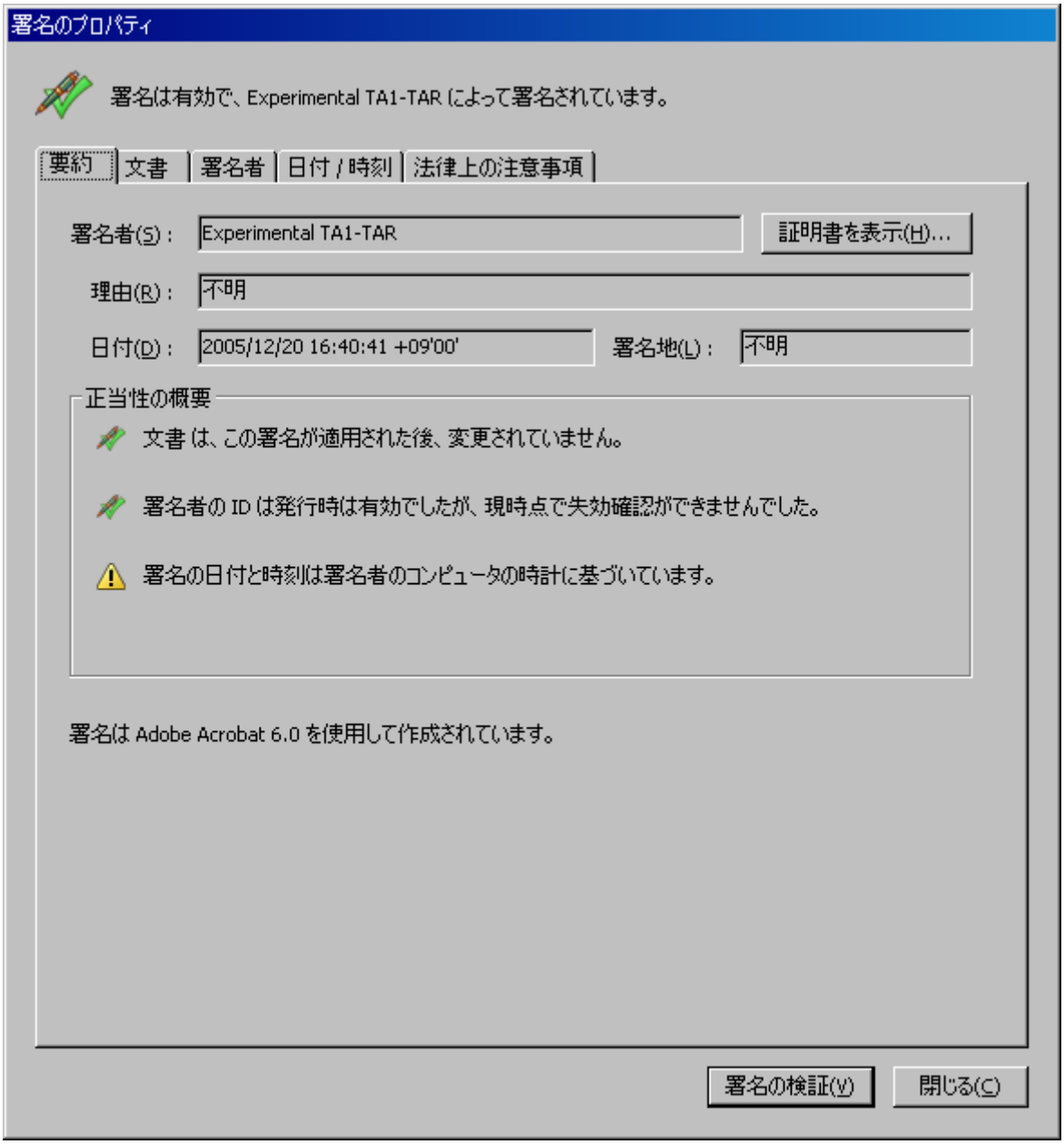


図 2-18　時刻監査レポートの署名情報

図 2-19 に、時刻監査レポート中のタイムスタンプの時刻情報に係る配信経路を示す。

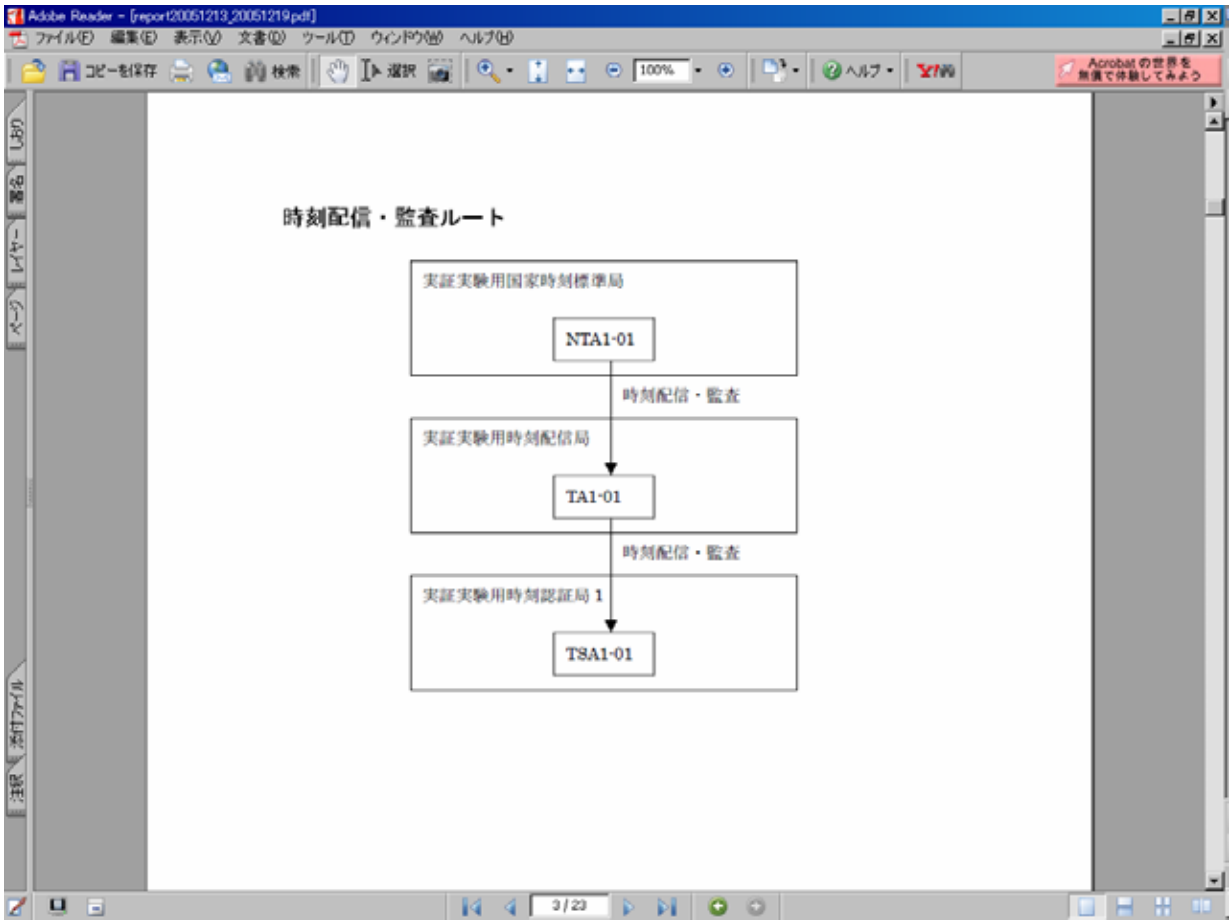


図 2-19　タイムスタンプの時刻情報に係る配信経路

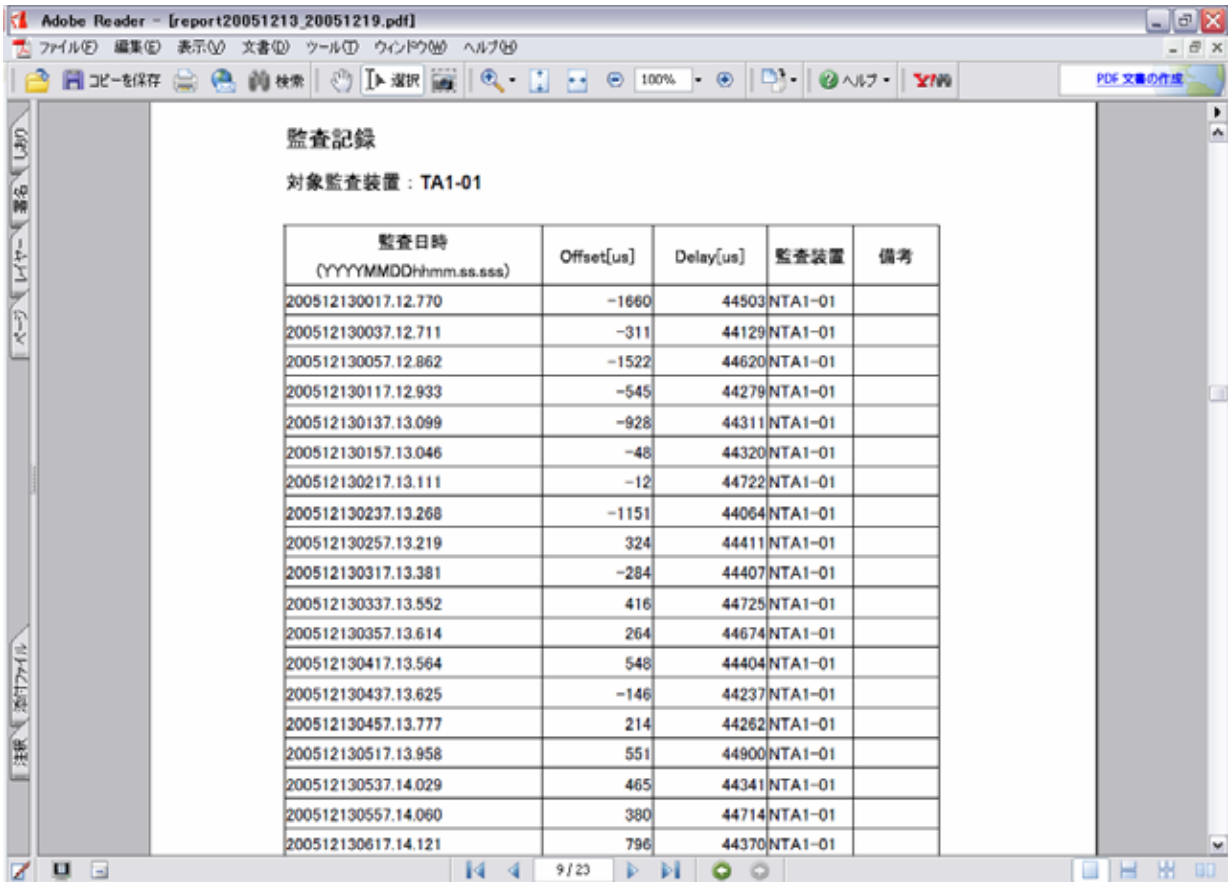
図 2-20 及び図 2-21 は時刻監査レポート中の本実証実験で使用した TSA（リンク情報を使用するアーカイビング方式）及び TA に対する監査記録である。

監査記録

対象装置：TSA1-01

監査日時 (YYYYMMDDhhmm.ss.sss)	Offset[us]	Delay[us]	監査装置	備考
200512130044.06.585	-3068	57121	TA1-01	
200512130244.07.581	-2356	56581	TA1-01	
200512130444.08.386	583	57106	TA1-01	
200512130644.09.573	1883	54936	TA1-01	
200512130844.10.425	-449	55713	TA1-01	
200512131044.11.428	1062	55884	TA1-01	
200512131244.12.489	-1160	55852	TA1-01	
200512131444.13.529	957	57005	TA1-01	
200512131644.14.423	657	55593	TA1-01	
200512131844.15.362	720	55906	TA1-01	
200512132044.16.429	-249	57010	TA1-01	
200512132244.17.412	705	55109	TA1-01	
200512140044.18.445	-2133	54928	TA1-01	
200512140244.19.488	-2215	56153	TA1-01	
200512140444.20.493	-319	55930	TA1-01	
200512140644.21.533	-2214	57129	TA1-01	
200512140844.22.526	-606	55948	TA1-01	
200512141044.23.372	6646	56988	TA1-01	
200512141244.24.564	4984	56100	TA1-01	
200512141444.25.585	1520	56617	TA1-01	

図 2-20　本実証実験で使用した TSA（リンク情報を使用するアーカイビング方式）に対する監査記録



監査日時 (YYYYMMDDhhmm.ss.sss)	Offset[us]	Delay[us]	監査装置	備考
200512130017.12.770	-1660	44503	NTA1-01	
200512130037.12.711	-311	44129	NTA1-01	
200512130057.12.862	-1522	44620	NTA1-01	
200512130117.12.933	-545	44279	NTA1-01	
200512130137.13.099	-928	44311	NTA1-01	
200512130157.13.046	-48	44320	NTA1-01	
200512130217.13.111	-12	44722	NTA1-01	
200512130237.13.268	-1151	44064	NTA1-01	
200512130257.13.219	324	44411	NTA1-01	
200512130317.13.381	-284	44407	NTA1-01	
200512130337.13.552	416	44725	NTA1-01	
200512130357.13.614	264	44674	NTA1-01	
200512130417.13.564	548	44404	NTA1-01	
200512130437.13.625	-146	44237	NTA1-01	
200512130457.13.777	214	44262	NTA1-01	
200512130517.13.958	551	44900	NTA1-01	
200512130537.14.029	465	44341	NTA1-01	
200512130557.14.060	380	44714	NTA1-01	
200512130617.14.121	796	44370	NTA1-01	

図 2-21　本実証実験で使用した TA に対する監査記録

図 2-20 及び図 2-21 より、タイムスタンプの時刻情報に係る誤差情報が確認できることがわかる。

タイムスタンプの取得時刻はドキュメントサービス画面より確認することができる。（図 2-22）

図 2-22 は署名タイムスタンプ付与時の検証結果の画面である。検証に失敗している箇所は、改ざん試験を実施した際のファイルである。

図 2-22　タイムスタンプ取得時刻（署名タイムスタンプの検証）

タイムスタンプ日時が画面に表示されることが分かる。

図 2-22 中の有効なタイムスタンプの付与時刻より、各タイムスタンプに係る時刻情報の時刻誤差を表 2-8 にまとめる。

表 2-8 の offset はタイムスタンプトークンが発行される直前の時刻配信における、配信元と配信先の時刻の差であり、時刻誤差合計は TA-TSA 間の offset と NTA-TA 間の offset の絶対値を合計した値である。

なお、表 2-8 には改ざん試験を実施した際の結果は含めていない。

表 2-8　TST の取得時刻とその時刻誤差

#	文書名	TST 時刻情報 (JST)	TSA の監査時刻(UTC)	TA-TSA 間の offset[us]	TA の監査時刻(UTC)	NTA-TA 間の offset[us]	時刻誤差合計[us]
1	TSPF00001	2005/12/13 11:41:15	2005/12/13 00:44:06.585	-3068	2005/12/13 00:37:12.711	-311	3379
2	TSPF00002	2005/12/13 11:41:20	2005/12/13 00:44:06.585	-3068	2005/12/13 00:37:12.711	-311	3379
3	TSPF00003	2005/12/13 11:41:25	2005/12/13 00:44:06.585	-3068	2005/12/13 00:37:12.711	-311	3379
4	TSPF00004	2005/12/13 11:41:30	2005/12/13 00:44:06.585	-3068	2005/12/13 00:37:12.711	-311	3379
5	TSPF00005	2005/12/13 11:41:36	2005/12/13 00:44:06.585	-3068	2005/12/13 00:37:12.711	-311	3379
6	TSPF00006	2005/12/13 11:41:42	2005/12/13 00:44:06.585	-3068	2005/12/13 00:37:12.711	-311	3379
7	TSPF00007	2005/12/13 11:41:47	2005/12/13 00:44:06.585	-3068	2005/12/13 00:37:12.711	-311	3379
8	TSPF00008	2005/12/13 11:41:54	2005/12/13 00:44:06.585	-3068	2005/12/13 00:37:12.711	-311	3379
9	TSPF00009	2005/12/13 11:41:59	2005/12/13 00:44:06.585	-3068	2005/12/13 00:37:12.711	-311	3379
10	TSPF00010	2005/12/13 11:42:04	2005/12/13 00:44:06.585	-3068	2005/12/13 00:37:12.711	-311	3379
11	TSPF00011_1MB	2005/12/13 12:44:12	2005/12/13 02:44:07.581	-2356	2005/12/13 02:37:13.268	-1151	3507
12	TSPF00012_10MB	2005/12/13 12:44:18	2005/12/13 02:44:07.581	-2356	2005/12/13 02:37:13.268	-1151	3507

表 2-8 より、本実証実験において、上記タイムスタンプトークンが発行された際の時刻誤差合計は 3379us 及び 3507us であったことが分かる。

図 2-23 及び図 2-24 に、本実証実験における監査規格を示す。

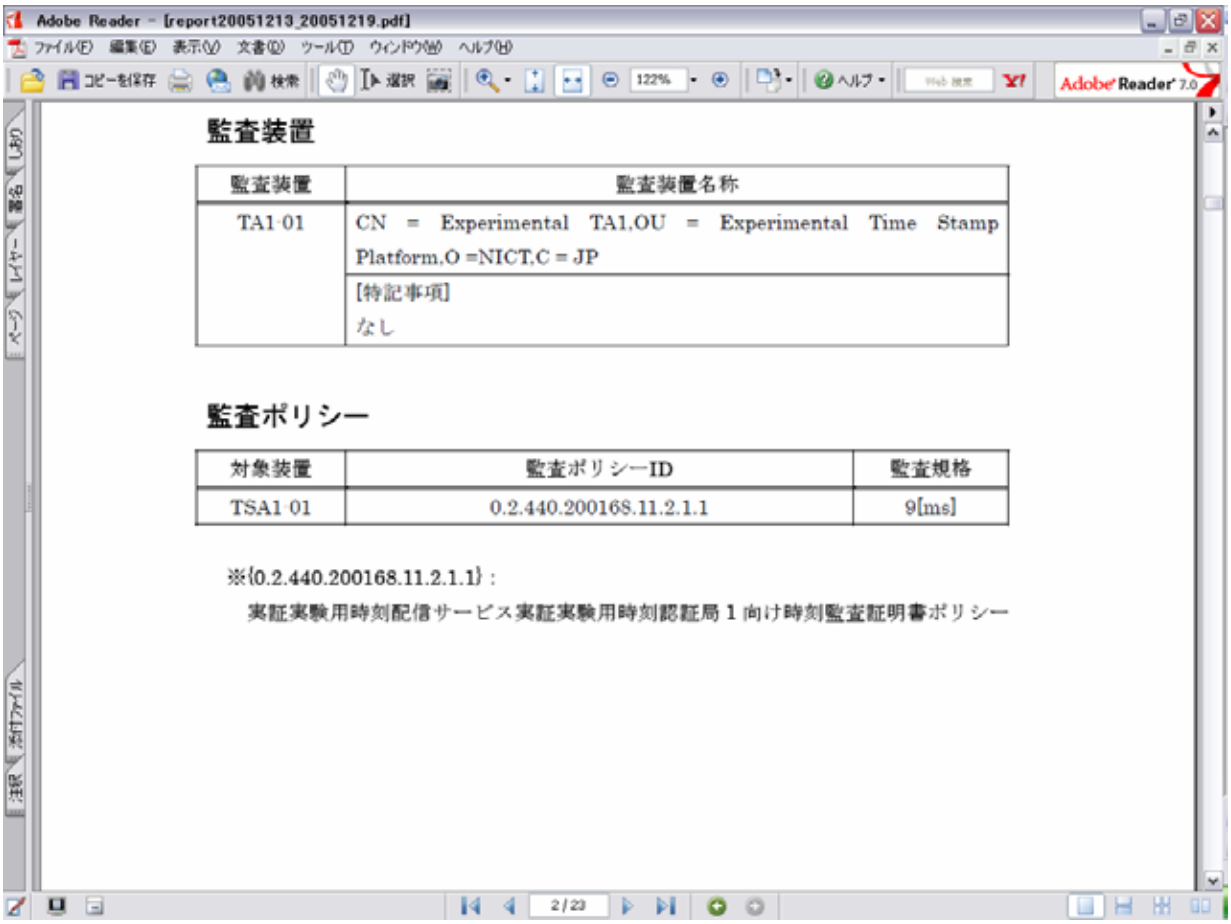


図 2-23　TSA の時刻監査規格

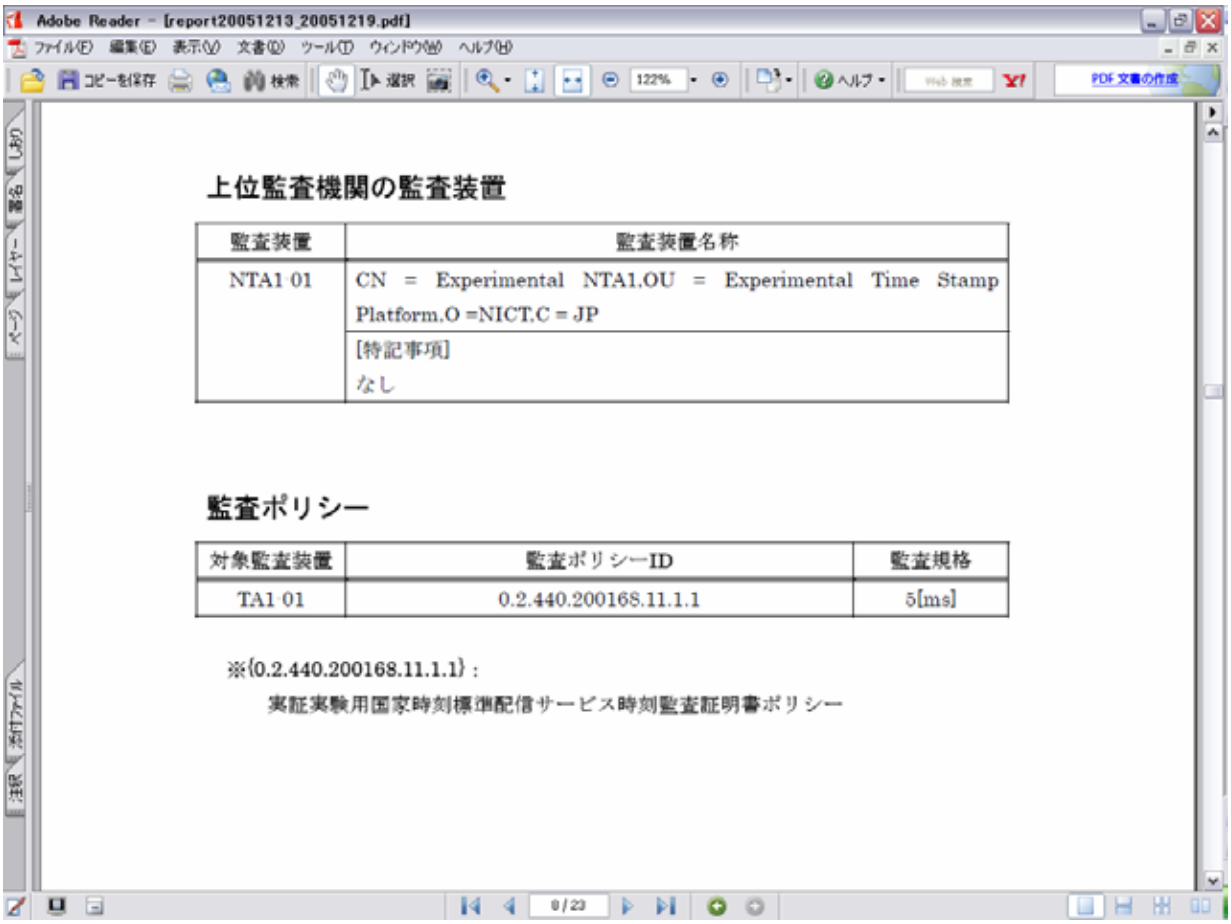


図 2-24　TA の時刻監査規格

表 2-8 ならびに図 2-23 及び図 2-24 より、表 2-8 の各タイムスタンプに係る時刻情報は、監査規格内の時刻精度であったことがわかる。

本項の結果より、本実証実験における文書管理システムの利用環境において、時刻トレーサビリティを確認する機能が利用できることが確認できた。

5-2 長期保証機能評価

以下の図 2-25 に、署名タイムスタンプ、アーカイブタイムスタンプ（初回）及びアーカイブタイムスタンプ（効力延長）の付与までを行った場合の原本性保証情報ファイル（XAdES-A をベースにしたフォーマット）の例を示す。

なお、図 2-25 中に「～中略～」の文字があるが、これは、タグの内容の一部を省略していることを表している。


```
<?xml version="1.0" encoding="UTF-8"?><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature0">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference Id="Reference0">
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>RpLQT7vlMmxOtQ7BS5p1HLEekUM=</ds:DigestValue>
</ds:Reference>
<ds:Reference Id="Reference1" URI="#Keyinfo0">
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>s946RVa2OdkSmbC9HBpzEI5jIr8=</ds:DigestValue>
</ds:Reference>
<ds:Reference Id="Reference2" Type="http://uri.etsi.org/01903/v1.3.1#SignedProperties" URI="#SignedProperties0">
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>ReqKWQCZu1/xUZJWiadI3W53DqE=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>M+PGwsvJClJWfYgBQu6xYOOpURuquy0vBPma+rLvivbAo59Qwuqlmgfho2VPv4ApKsBnYBblzSIv8H8jwJP/7ln5n5VklTtNOAWmkI9NvuDPFWudAay0faxLqRx0v9ZYxHnTk+nZLJHlx9KmcVJsUC9+du9WklKhNl9oljCAnbY=</ds:SignatureValue>
<ds:KeyInfo Id="Keyinfo0">
<ds:X509Data>
<ds:X509Certificate>MIIDdDCCAlygAwIBAgICNnEwDQYJKoZIhvcNAQEFBQAwSDELMAkGA1UEBhMCSlAxHTAbBgNVBAoTFEZ1amkgWGVyb3ggQ28uL
～中略～
7oFkiX+SOgNkDyGwS3NubFOl3fn9mwOMl+y11fn09dBs</ds:X509Certificate>
<ds:X509IssuerSerial>
<ds:X509IssuerName>CN=Fuji Xerox AAA CA, O=Fuji Xerox Co.¥, Ltd., C=JP</ds:X509IssuerName>
```

<ds:X509SerialNumber>13937</ds:X509SerialNumber>
</ds:X509IssuerSerial>
<ds:X509SubjectName>CN=Taro Fuji, OU=MC0000000661-fujitaro, O=Fuji Xerox Co.¥, Ltd., C=JP</ds:X509SubjectName>
</ds:X509Data>
</ds:KeyInfo>
<ds:Object>
<QualifyingProperties xmlns="http://uri.etsi.org/01903/v1.3.1#" Target="#Signature0">
<SignedProperties Id="SignedProperties0">
<SignedSignatureProperties>
<SigningTime>2005-12-13T02:18:59Z</SigningTime>
</SignedSignatureProperties>
</SignedProperties>
<UnsignedProperties>
<UnsignedSignatureProperties>
<SignatureTimeStamp>
<EncapsulatedTimeStamp>MIH8BgkqhkiG9w0BBwGgge4wgesCAQEGCQKDOIybaAsFATBPMAsGCWCGSAFlAwQCAwRAUpxnGucjnEdDAFXowNnXIpdvZ0KjG3CQq3nVhgVshzI7+lETDRUP278Nph9pQ6rvMxsUHijGmpyzMM8m397QXgIIbCFS8D+XFy4YDzIwMDUxMjEzMDI0MTE1WqAihiBodHRwczovL3RzYTEtbmljdC5zZWN1cmVzZWFsLmpwL6FLMBcGBiiBjF4BAgEB/wQKMAgGBiiBjF4CAzAwBgYogYxeAQEBAf8EIzAhMB8wBwYFKyQDAgEEFLPxJrz/6SSBUTQCri0Yyk3N6W+t</EncapsulatedTimeStamp>
</SignatureTimeStamp>
<CertificateValues>
<EncapsulatedX509Certificate>MIIDhTCCAm2gAwIBAgIBATANBgkqhkiG9w0BAQQFADBIMQswCQYDV
～中略～
LUgGub5+Og=</EncapsulatedX509Certificate>
</CertificateValues>
<RevocationValues>
<CRLValues>
<EncapsulatedCRLValue>MIIpCzCCJ/MCAQEwDQYJKoZIhvcNAQEFBQA
～中略～
LycLi7qHuFl6arwQUsLOfJloSVPIAaro1A=</EncapsulatedCRLValue>
</CRLValues>
</RevocationValues>
<ArchiveTimeStamp>
<Include URI="#Reference0" referencedData="true"/>
<Include URI="#Reference1" referencedData="true"/>

<Include URI="#Reference2" referencedData="true"/>
<EncapsulatedTimeStamp>MIH8BgkqhkiG9w0BBwGgge4wgesCAQEGCQKDOIybaAsFATB
PMAsGCWCGSAFlAwQCAwRAH5Dm5FoL64HztffU1QajRHnTlps/HrcozeeD5Si+hNqf40J0K
GK98RIhZ618eEZNNXqUBhPmKUGVu1y8rW1hCwIIbCFS8D+U0bYYDzIwMDUxMjE3MDI
0MTEwWqAihiBodHRwczovL3RzYTEtbmljdC5zZWN1cmVzZWFsLmpwL6FLMBcGBiiBjF4B
AgEB/wQKMAgGBiiBjF4CAzAwBgYogYxeAQEBAf8EIzAhMB8wBwYFKyQDAgEEFEhuJdJo
wcwqdubHJogZinyWbTuH</EncapsulatedTimeStamp>
</ArchiveTimeStamp>
<ArchiveTimeStamp>
<Include URI="#Reference0" referencedData="true"/>
<Include URI="#Reference1" referencedData="true"/>
<Include URI="#Reference2" referencedData="true"/>
<EncapsulatedTimeStamp>MIH8BgkqhkiG9w0BBwGgge4wgesCAQEGCQKDOIybaAsFATB
PMAsGCWCGSAFlAwQCAwRAgkeTDqc5jy4sVcLvVteF3/BaXxANcIzr5g20Kdgz0zP1UPCB0
B+QQffDT/Jr+cxBT7SkPzep5AIJwT7yeLpt7wIIbCFS8D+U0aIYDzIwMDUxMjE5MDQ1NjE3
WqAihiBodHRwczovL3RzYTEtbmljdC5zZWN1cmVzZWFsLmpwL6FLMBcGBiiBjF4BAgEB/w
QKMAgGBiiBjF4CAzAwBgYogYxeAQEBAf8EIzAhMB8wBwYFKyQDAgEEFHfLGyrimKfuXc
6nB5P3vJK/1bQB</EncapsulatedTimeStamp>
</ArchiveTimeStamp>
</UnsignedSignatureProperties>
</UnsignedProperties>
</QualifyingProperties>
</ds:Object>
</ds:Signature>

図 2-25　原本性保証情報ファイル(XAdES-A)の内容

図 2-25 より、XAdES-A をベースにしたフォーマットでのアーカイブタイムスタンプ付与が実施出来ていることがわかる。

本実証実験で用いた XAdES-A をベースにしたフォーマットを表 2-9 に示す。

表 2-9　本実証実験で用いた XAdES-A をベースにしたフォーマット（概要）

#	要素名	説明
1	QualifyingProperties	<ds:Object>要素内に含められ長期保存に必要な要素を格納するコンテナの役割を果たす。
2	SignedProperties	XMLDSIGの署名値の計算対象。
3	SignedSignatureProperties	XML署名を限定する特性を子要素に持つ。
4	SigningTime	XML署名時の時刻。xsd:DateTime形式で指定する。
5	UnsignedProperties	署名値の計算対象にならない。
6	UnsignedSignatureProperties	XML署名を限定する特性を子要素に持つ。
7	SignatureTimeStamp	署名タイムスタンプを格納する。
8	CertificateValues	CAの証明書を格納する。 内部に一つ以上の <EncapsulatedX509Certificate>を設定する。
9	EncapsulatedX509Certific	証明書の実体をBase64形式でエンコードした値を設定する。
10	RevocationValues	署名検証に必要な証明書の失効情報が格納される。
11	ArchiveTimeStamp	アーカイブタイムスタンプを格納する。この要素は期間をおいて複数付与される。

なお、図 2-25 において、SignatureTimeStamp、RevocationValues、ArchiveTimeStamp 中の実際にタイムスタンプトークンを格納しているタグに関しては、参考文献[4]の「XML 長期署名プロファイル（XAdES）（案）」を参照。

表 2-10 及び表 2-11 に、デジタル署名、署名タイムスタンプ及びアーカイブタイムスタンプの付与及び検証についての機能確認の結果を示す。

表 2-10 デジタル署名、署名タイムスタンプ及びアーカイブタイムスタンプの付与処理結果

#	ファイル名	デジタル署名	署名タイムスタンプ	アーカイブタイムスタンプ			
				初回	2 回目	3 回目	4 回目
1	TSPF00001.txt	成功	成功	成功	成功	成功	成功
2	TSPF00002.txt	成功	成功	成功	成功	成功	成功
3	TSPF00003.txt	成功	成功	成功	成功	成功	成功
4	TSPF00004.txt	成功	成功	成功	成功	成功	成功
5	TSPF00005.txt	成功	成功	成功	成功	成功	成功
6	TSPF00006.txt	成功	成功	成功	成功	成功	成功
7	TSPF00007.txt	成功	成功	成功	成功	成功	成功
8	TSPF00008.txt	成功	成功	成功	成功	成功	成功
9	TSPF00009.txt	成功	成功	成功	成功	成功	成功
10	TSPF00010.txt	成功	成功	成功	成功	成功	成功

表 2-10 より全ての付与処理が成功していることが分かる。

表 2-11 デジタル署名、署名タイムスタンプ及びアーカイブタイムスタンプの検証処理結果

#	ファイル名	デジタル署名	署名タイムスタンプ	アーカイブタイムスタンプ			
				初回	2 回目	3 回目	4 回目
1	TSPF00001.txt	成功	成功	成功	成功	成功	成功
2	TSPF00002.txt	成功	成功	成功	成功	成功	成功
3	TSPF00003.txt	成功	成功	成功	成功	成功	成功
4	TSPF00004.txt	成功	成功	成功	成功	成功	成功
5	TSPF00005.txt	成功	成功	成功	成功	成功	成功
6	TSPF00006.txt	成功	成功	成功	成功	成功	成功
7	TSPF00007.txt	成功	成功	成功	成功	成功	成功
8	TSPF00008.txt	成功	成功	成功	成功	成功	成功
9	TSPF00009.txt	成功	成功	成功	成功	成功	成功
10	TSPF00010.txt	成功	成功	成功	成功	成功	成功

表 2-11 より全ての検証処理に成功していることがわかる。

本実証実験では、「第 2 章 4-3-8 登録文書の改ざん方法」で述べた手法を用いて文書ファイルが改ざんされている状況を擬似的に作り出し、文書が改ざんされた場合の検証処理の動作を確認した。

「第 2 章 4-3-8 登録文書の改ざん方法」で述べたように、本実証実験で使用した文書管理システムでは、通常は文書の改ざんを行うことは出来ないため、実際には文書管理システムに登録されたファイルを一度クライアント PC にダウンロードし、別の原本性保証情報と紐付けてアップロードしている。

このアップロードされたファイルは、文書管理システム上にある既存の登録済みファイルと同様のファイル名を持つが、文書管理システム上では別のファイルとして管理される。

表 2-12 に改ざんしたファイルの検証結果を示す。

表 2-12　改ざんを実施した際の検証処理結果

#	改ざんしたファイル名	改ざんを実施したタイミング	検証結果
1	TSPF00005.txt	署名タイムスタンプ検証前	検証失敗
2	TSPF00006.txt	署名タイムスタンプ検証前	検証失敗
3	TSPF00007.txt	アーカイブタイムスタンプ（初回）検証前	検証失敗
4	TSPF00008.txt	アーカイブタイムスタンプ（初回）検証前	検証失敗
5	TSPF00009.txt	アーカイブタイムスタンプ（2回目）検証前	検証失敗
6	TSPF00010.txt	アーカイブタイムスタンプ（2回目）検証前	検証失敗

注 1：表 2-11 中のファイルと同じファイル名であるが、文書管理システム上では別の文書として扱われる。

表 2-12 より、改ざんしたファイルについて検証に失敗することを確認した。

改ざんしたファイルに対するタイムスタンプの付与処理に関しては、署名タイムスタンプ及びアーカイブタイムスタンプ付与の際には付与処理の中で付与済みのタイムスタンプの検証処理を行うため、検証処理と同様に全て失敗した。

本項に示した結果より、本実証実験において、XAdES 形式をベースにした方式での長期保証に対応したアーカイブタイムスタンプ付与及び検証を正常に行えていることがわかる。

5-3 長期保証データ容量評価

表 2-13 にデジタル署名、署名タイムスタンプ及びアーカイブタイムスタンプ付与を実施した際の原本性保証情報ファイルのデータ容量の変化を示す。

表 2-13　原本性保証情報ファイルのデータ容量の変化（Bytes）

#	実ファイル名	デジタル署名	署名タイムスタンプ	アーカイブタイムスタンプ			
				初回	2回目	3回目	4回目
1	TSPF00001.txt	3104	3691	20126	20720	21314	21908
2	TSPF00002.txt	3104	3691	20126	20720	21314	21908
3	TSPF00003.txt	3104	3691	20126	20720	21314	21908
4	TSPF00004.txt	3104	3691	20126	20720	21314	21908
5	TSPF00005.txt	3104	3691	20126	20720	21314	21908
6	TSPF00006.txt	3104	3691	20126	20720	21314	21908
7	TSPF00007.txt	3104	3691	20126	20720	21314	21908
8	TSPF00008.txt	3104	3691	20126	20720	21314	21908
9	TSPF00009.txt	3104	3691	20126	20720	21314	21908
10	TSPF00010.txt	3104	3691	20126	20720	21314	21908
11	TSPF00011_1MB.txt	3104	3691	20126	20720	21314	21908
12	TSPF00012_10MB.txt	3104	3691	20126	20720	21314	21908

表 2-13 より、デジタル署名付与によって約 3KBytes の原本性保証情報ファイルが生成され、署名タイムスタンプ付与時には約 600Bytes データ容量が増加している。この署名タイムスタンプ付与時の増加分は、署名タイムスタンプのデータに相当する。

また、アーカイブタイムスタンプ（初回）を付与した際には原本性保証情報ファイルのデータ容量は約 20KBytes となり、約 17KBytes データ容量が増加している。このアーカイブタイムスタンプ（初回）付与時の増加分は、デジタル署名検証用の証明書及び CRL ならびにアーカイブタイムスタンプのデータに相当する。

アーカイブタイムスタンプ（初回）の付与以後、アーカイブタイムスタンプを多重で付与する度に約 600Bytes ずつデータ容量が増加している。このアーカイブタイムスタンプ（２回目以降）付与時の増加分は、再付与されたアーカイブタイムスタンプのデータに相当する。

図 2-26 に原本性保証情報ファイルのデータ容量の変化を示す。

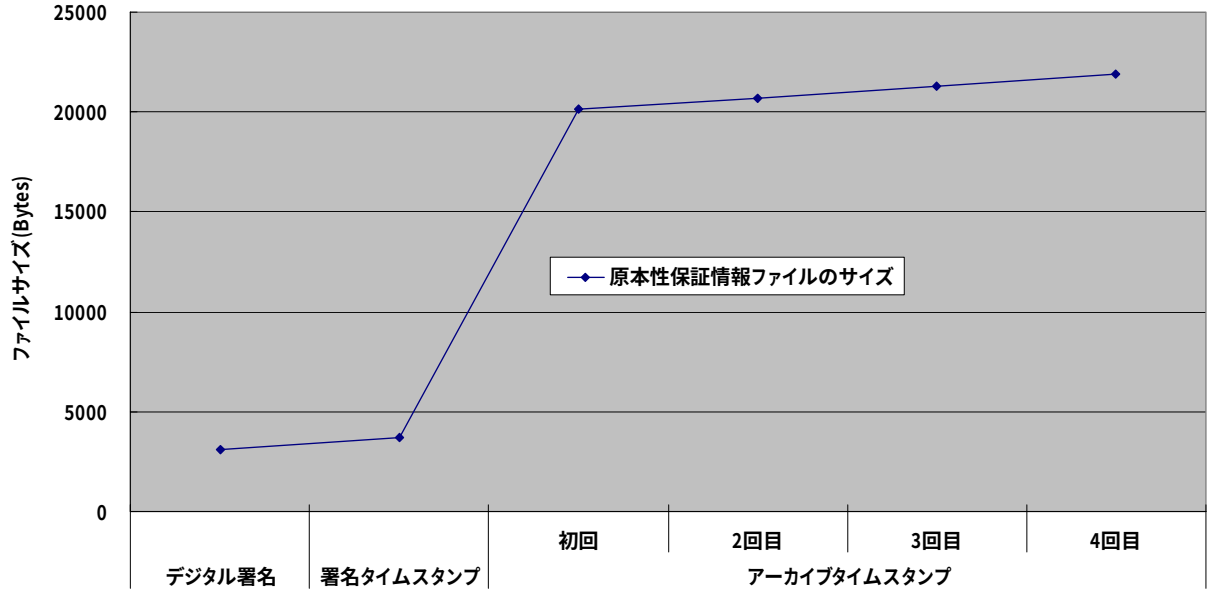


図 2-26　原本性保証情報のデータ容量の変化

5-4 例外発生時動作評価

本項では、操作ミスや意図しないエラーが発生した場合、利用者や検証者がその後の操作を続行できる、もしくはその後にどのような対応をすれば良いか判断できるユーザインタフェースとなっていることを確認するために、具体例を挙げ、本実証実験で使用したアプリケーションが動作することを検証する。

まず最初に、長期保証に関連した例外が発生した際のメッセージ一覧（ユーザインタフェースに現れるものを抜粋）を表 2-14 に示す。

表 2-14 より、本実証実験で用いたアプリケーションにおいて様々な例外の発生に合わせた例外処理が適切に実装されていることがわかる。

表 2-14　例外発生時のメッセージ一覧（ユーザインタフェース上に現れるものを抜粋）

#	メッセージ	原因	対処法
1	署名が付与できませんでした。	署名 ActiveX コントールが署名を付与することができませんでした。	署名を付与する際の証明書を Windows にインストールしているか確認してください。 インストールしてある場合は、システム障害である可能性がありますので、システム管理者へ連絡してください。
2	文書がアップロードできませんでした。	署名した文書の署名情報 XML（XAdES をベースにしたフォーマット）ファイルのアップロードができませんでした。 （アップロードするドキュメント数が規定最大数をオーバーした場合が該当するが、１ファイルしかアップロードはしないので有り得ない。）	なし。
3	文書へのタイムスタンプ付与時にエラーが発生しました。	タイムスタンプを付与するために必要な情報の取得時に何らかのエラーが発生しました。	システム管理者へ連絡してください。
4	原本性検証時にエラーが発生しました。	原本性検証に必要な情報の取得時に何らかのエラーが発生しました。	システム管理者へ連絡してください。
5	原本性保証情報の取得時にエラーが発生しました。	原本性保証情報の取得時、あるいは原本性保証情報中の属性抽出時に何らかのエラーが発生しました。	システム管理者へ連絡してください。

#	メッセージ	原因	対処法
6	タイムスタンプのみ付与することはできません。	タイムスタンプ付与の対象ドキュメントに署名が付与されていません。	事前に署名付与を実行する。あるいは、「署名およびタイムスタンプ付与」を実行してください。
7	既に署名が付与されているので、スキップしました。	署名付与の対象ドキュメントにはすでに署名が付与されています。	仕様です。
8	既にタイムスタンプが付与されているので、スキップしました。	タイムスタンプ付与の対象ドキュメントにはすでにタイムスタンプが付与されています。	仕様です。
9	文書へのタイムスタンプ付与時にエラーが発生しました。	タイムスタンプ付与時に、タイムスタンプの有効性の検証でエラーとなりました。	TSA のルート CA 証明書が規定のドロワーに登録されているか、あるいはこのルート証明書が有効なものかどうか確認してください。
10	署名の検証時にエラーが発生しました。	署名付与後に、署名の有効性の検証でエラーとなりました。または、それまでの過程で何らかのエラーが発生しました。	署名を付けた証明書のルート CA 証明書が規定のドロワーに登録されているか、あるいはこのルート証明書が有効なものかどうか確認してください。 問題が見当たらない場合は、システム障害である可能性がありますので、システム管理者へ連絡してください。
11	信頼できる証明書が取得できませんでした。	信頼できる証明書(トラストアンカー)が規定のドロワーから取得できませんでした。	信頼できる証明書(トラストアンカー)が登録されているキャビネットがメンテナンスモードになっていないか、または証明書が格納されているキャビネットの ID やドロワーが規定の名前となっているか確認してください。

また、上記メッセージに加え、証明付与画面上にユーザインタフェース（UI）メッセージの補足として表示される、ActiveX のメッセージが存在する。

例外発生時の振る舞いの具体例の１つ目として、デジタル署名付与が失敗した際の画面を図 2-27 に示す。

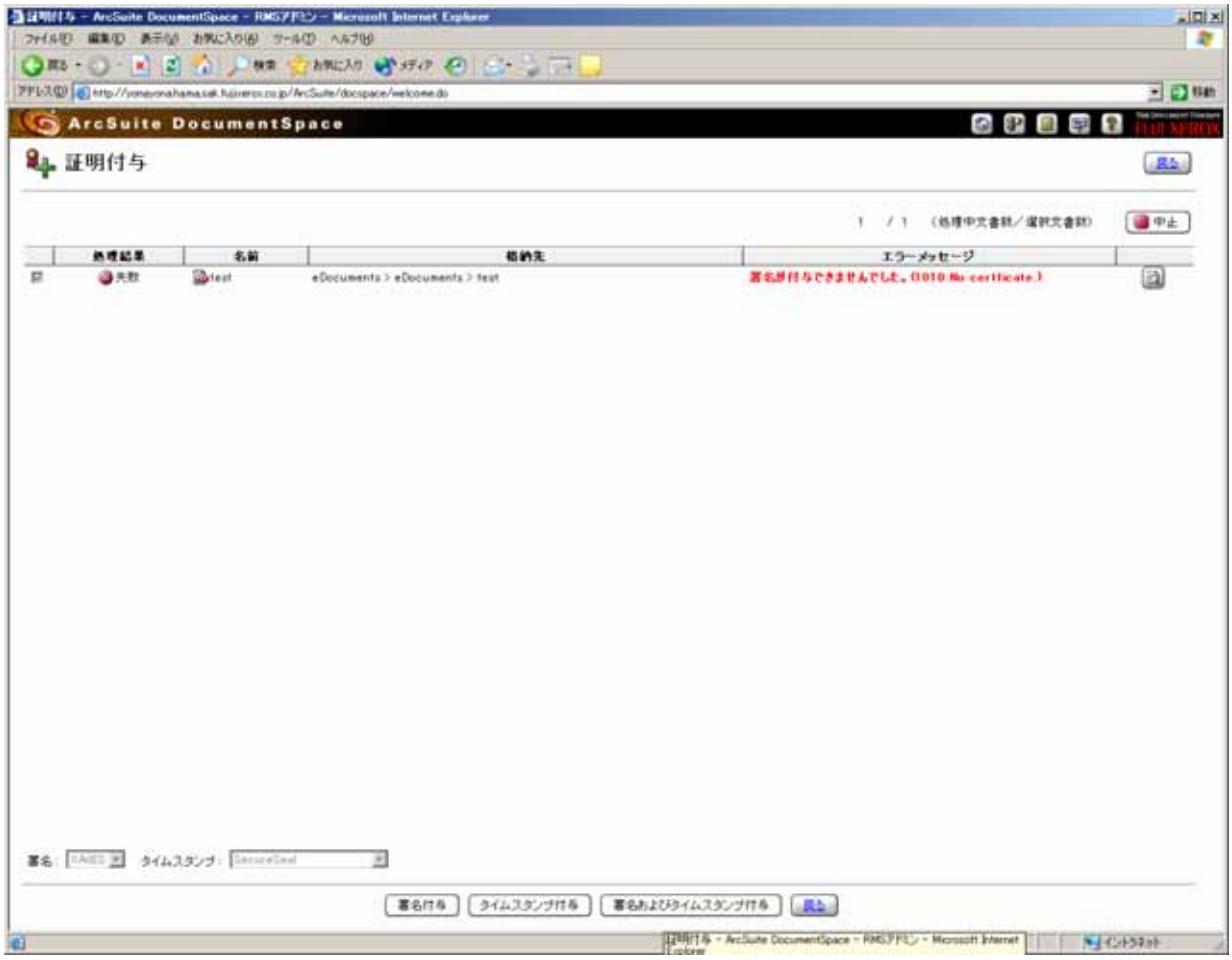


図 2-27　デジタル署名付与に失敗した際の画面

表 2-14 と照らし合わせることで原因と対応法を調べることが出来る。

上記例は何らかの原因により、デジタル署名の付与に失敗した場合の画面である。

表 2-14 及び図 2-27 より、デジタル署名付与に必要な証明書がクライアント PC 上に存在しない可能性があることが分かる。

具体例の 2 つ目として、署名タイムスタンプ付与処理に失敗した際の画面を図 2-28 に示す。

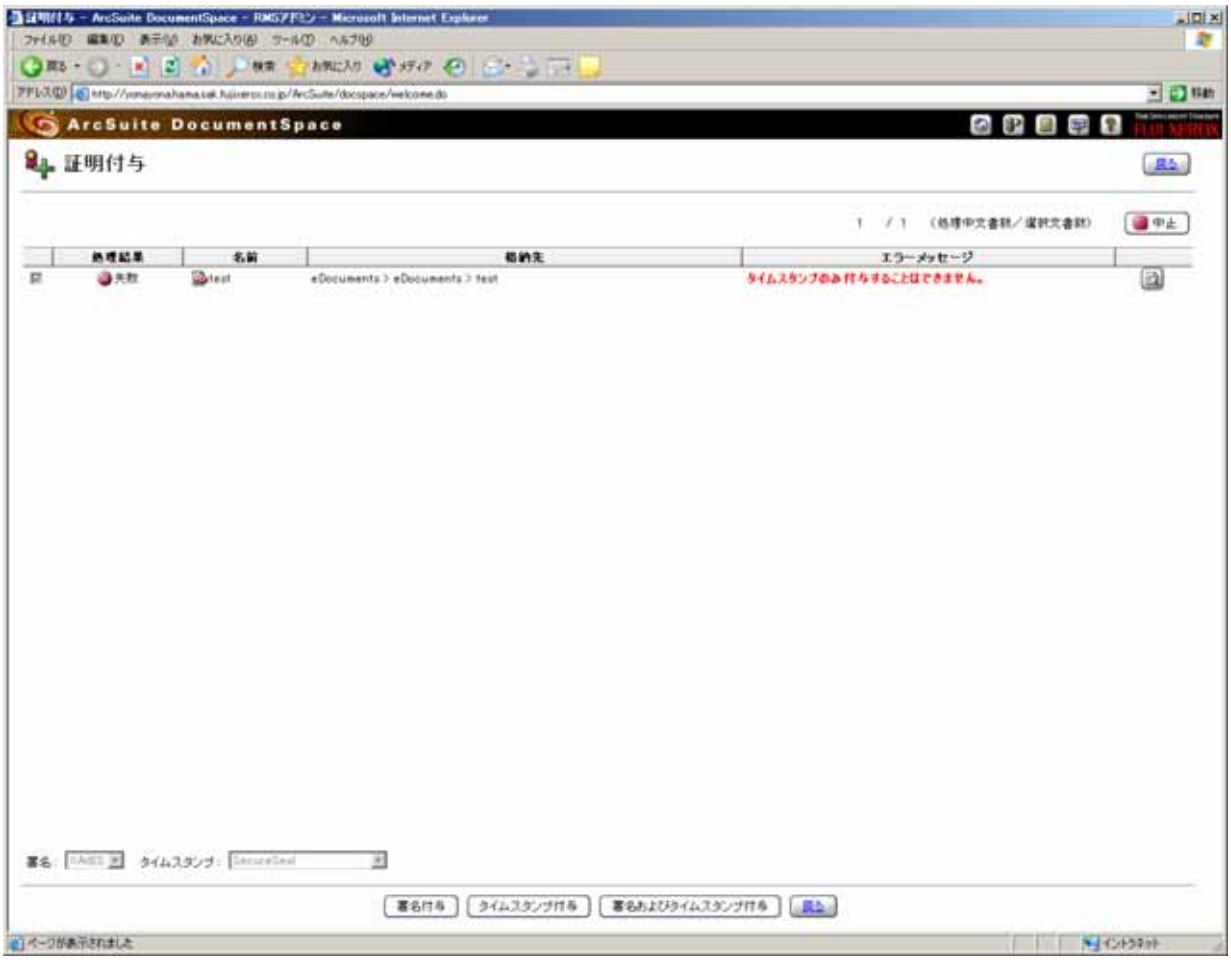


図 2-28　署名タイムスタンプに失敗した際の画面

メッセージを表 2-14 と照らし合わせることで原因と対応法を調べることが出来る。

表 2-14 及び図 2-28 より、上記例は既に署名タイムスタンプが付与されている文書に対して署名タイムスタンプ付与を実行した際に本エラーが発生することがわかる。

5-5 長期保証単一処理時間性能評価

本項では、本実証実験で使用したアプリケーション上でのアーカイブタイムスタンプの処理時間の測定に主眼を置き、署名タイムスタンプ及びアーカイブタイムスタンプの付与処理ならびにデジタル署名、署名タイムスタンプ及びアーカイブタイムスタンプの検証処理を行い、処理時間の測定結果をまとめている。

なお、本項で使用されている評価用文書ファイルのうち、TSPF00001.txt～TSPF00010.txt は 100KBytes の、TSPF00011_1MB.txt は 1MBytes の、TSPF00012_10MB.txt は 10MBytes のランダムな文字列によって構成されたテキストファイルである。

また、本項の表中の値はログファイルに記録された当該処理を実行するモジュール内での処理時間である。

なお、デジタル署名付与処理はクライアント側で実行され、上記モジュールが使用されないため、デジタル署名の処理時間はログファイルに出力されない。よって、本実証実験ではデジタル署名付与の計測は行っていない。（デジタル署名検証については、このモジュールによって処理が行われるため、ログファイルに処理時間が出力される。）

5-5-1 署名タイムスタンプ及びアーカイブタイムスタンプ付与の処理時間

署名タイムスタンプ及びアーカイブタイムスタンプの付与処理の処理時間を表 2-15 に示す。

表 2-15　付与処理の処理時間(msec)

#	ファイル名	署名タイムスタンプ	アーカイブタイムスタンプ			
			初回	2回目	3回目	4回目
1	TSPF00001.txt	718	2828	2359	2500	3250
2	TSPF00002.txt	500	2735	2141	2531	3032
3	TSPF00003.txt	500	4031	2125	2719	2891
4	TSPF00004.txt	645	2610	2156	2469	3047
5	TSPF00005.txt	1719	2657	2343	2500	4391
6	TSPF00006.txt	500	2750	2125	2516	4750
7	TSPF00007.txt	3031	2640	2515	2469	2937
8	TSPF00008.txt	469	2656	2125	2719	2875
9	TSPF00009.txt	468	2719	2187	2468	2875
10	TSPF00010.txt	3078	3156	2781	2485	2859
11	TSPF00011_1MB.txt	2156	3110	2718	4500	3703
12	TSPF00012_10MB.txt	797	6156	8469	10734	12188
	100KBytes処理平均	1163	2878	2286	2538	3291

署名タイムスタンプ及びアーカイブタイムスタンプの付与処理の処理時間の推移を図 2-29 に示す。

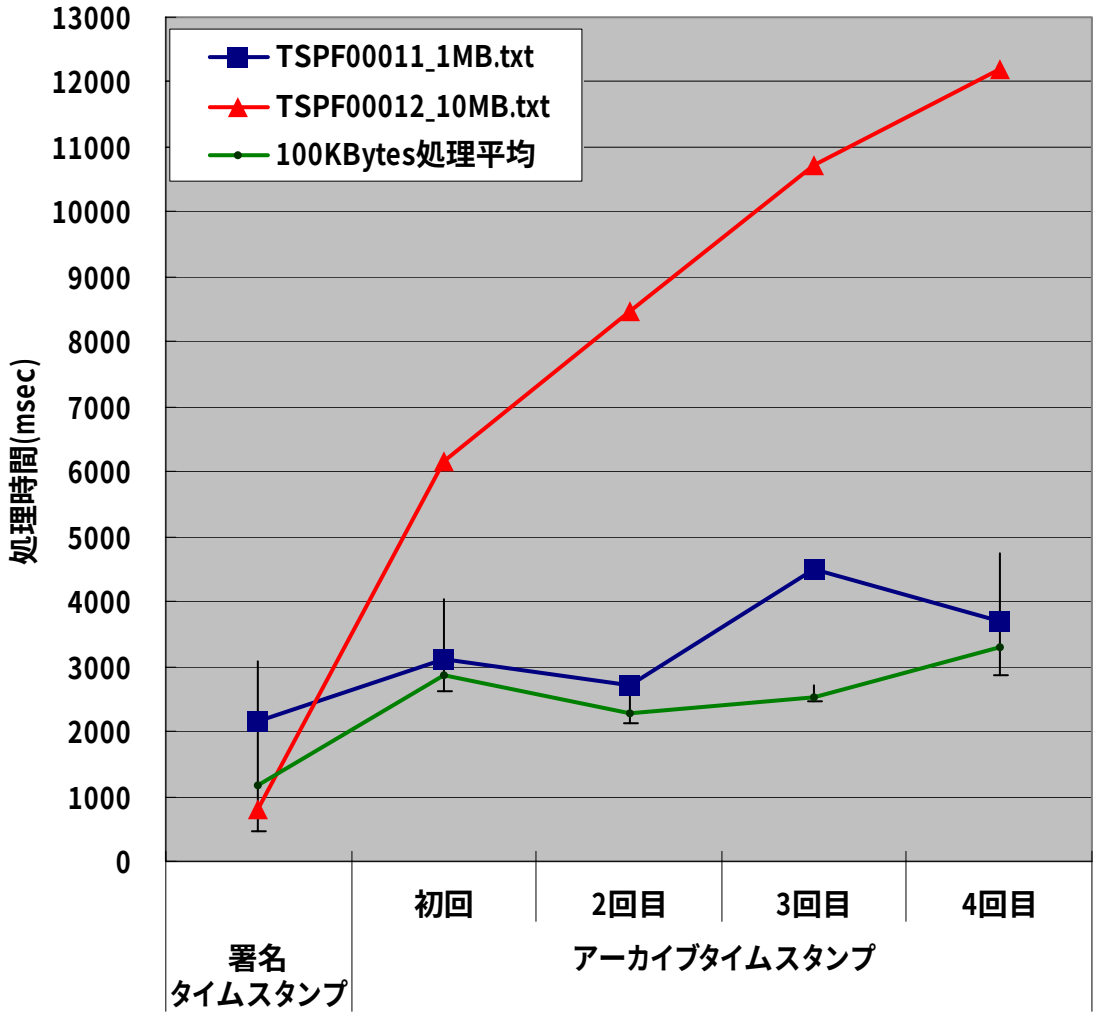


図 2-29　付与処理時間の推移

5-5-2 デジタル署名及び署名タイムスタンプ、アーカイブタイムスタンプ検証の処理時間

デジタル署名、署名タイムスタンプ及びアーカイブタイムスタンプの検証処理の処理時間を表 2-16 に示す。表中の全ての検証処理は成功した。

表 2-16　検証処理の処理時間(msec)

#	ファイル名	デジタル署名	署名タイムスタンプ	アーカイブタイムスタンプ			
				初回	2回目	3回目	4回目
1	TSPF00001.txt	234	578	953	1203	1609	1953
2	TSPF00002.txt	219	437	735	1062	1422	2281
3	TSPF00003.txt	219	500	688	1031	1375	2969
4	TSPF00004.txt	594	453	734	2484	1375	1828
5	TSPF00005.txt	219	437	735	2203	2609	2359
6	TSPF00006.txt	204	484	735	1062	1735	1891
7	TSPF00007.txt	219	454	672	1062	1359	2891
8	TSPF00008.txt	234	469	766	1172	1375	1765
9	TSPF00009.txt	219	437	704	1125	1407	1734
10	TSPF00010.txt	219	421	735	1140	1438	1766
11	TSPF00011_1MB.txt	484	453	1110	1422	1907	2344
12	TSPF00012_10MB.txt	375	593	2328	4219	6000	7922
	100KBytes処理平均	258	467	746	1354	1570	2144

デジタル署名、署名タイムスタンプ及びアーカイブタイムスタンプの検証処理の処理時間の推移を図 2-30 に示す。

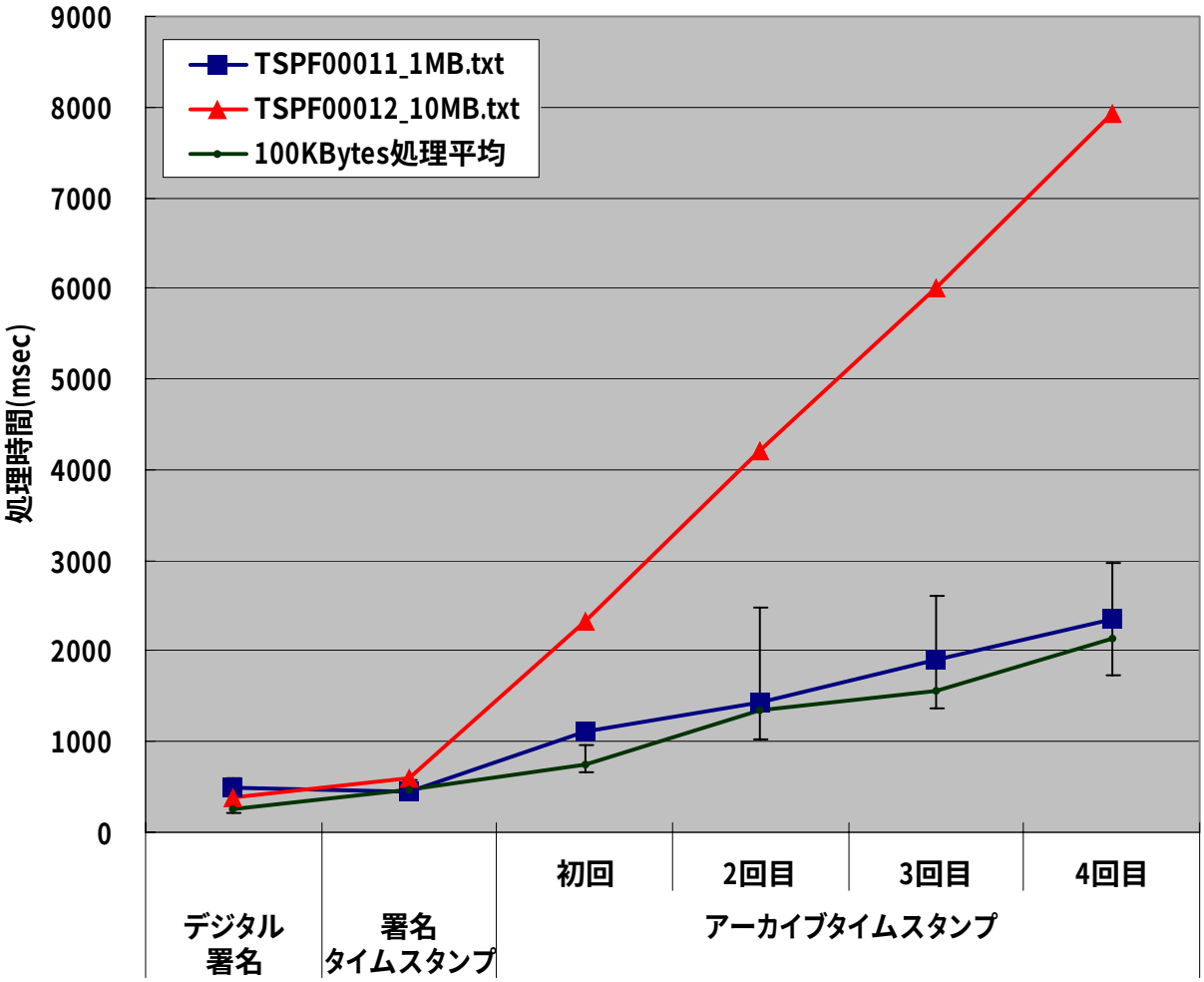


図 2-30　検証処理時間の推移

また、本実証実験では、検証の際に前述の方法でファイルを改ざんして検証を実施した。表 2-17 に改ざんが行われた場合の処理時間を示す。

表 2-17　改ざんを実施した際の検証処理の処理時間

#	ファイル名	改ざんの実施したタイミング	処理時間(msec)
1	TSPF00005.txt	署名タイムスタンプ検証前	16
2	TSPF00006.txt	署名タイムスタンプ検証前	0
3	TSPF00007.txt	アーカイブタイムスタンプ（初回）検証前	0
4	TSPF00008.txt	アーカイブタイムスタンプ（初回）検証前	16
5	TSPF00009.txt	アーカイブタイムスタンプ（2回目）検証前	0
6	TSPF00010.txt	アーカイブタイムスタンプ（2回目）検証前	15

表 2-17 において処理時間が 0ms となっている箇所が存在するが、これは本実証実験環境における時間の分解能によってこのような結果が記録されたものと推測される。

5-6 長期保証大量処理時間性能評価

本項で用いるファイルは TSPF00001.txt～TSPF10000.txt までの連番のファイル名を持つ、100KBytes のランダムな文字列によって構成されたテキストファイルである。

また、本項の表中の値はログファイルに記録された当該処理を実行するモジュール内での処理時間である。

本項では処理時間、総所要時間及び平均所要時間を表 2-18 の定義に従って使用している。

表 2-18　本項で用いる処理時間と所要時間の定義

#	項目	説明
1	処理時間	各処理における、ログファイルに記録された、当該処理を実行するモジュール内での処理に掛かった時間
2	総所要時間	最初の処理の開始時刻から最後の処理の終了時刻までの経過時間
3	平均所要時間	各処理に実際に掛かった時間の平均値。総所要時間を処理文書数で割った値

本項における「処理時間」は当該処理を実行するモジュール内での処理に掛かった時間であり、Web インタフェースや他のモジュールの処理にかかった時間を含まない。

それに対し、「総所要時間」は Web インタフェースや他のモジュールの処理（処理が行われていない時間も）を含む実際に掛かった時間である。

図 2-31 に本実証実験における処理時間、総所要時間及び平均所要時間の関係を示す。

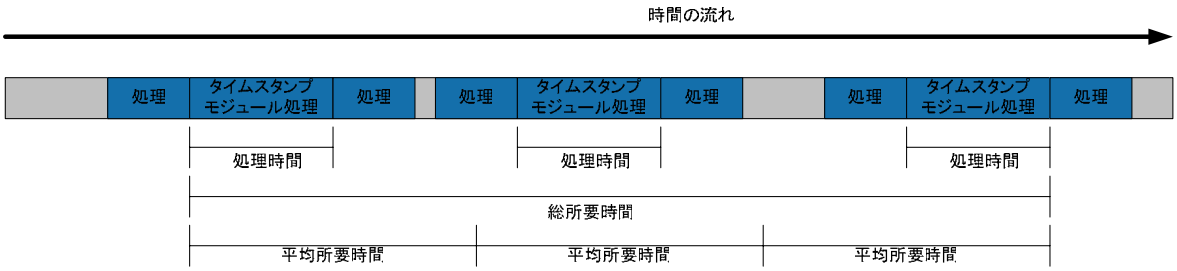


図 2-31　処理時間、総所要時間及び平均所要時間の関係

5-6-1 デジタル署名及び署名タイムスタンプ付与処理

本項では、デジタル署名及び署名タイムスタンプ付与処理に要した時間の測定結果を示す。

1 万件のデジタル署名及び署名タイムスタンプ付与は 2006/01/17 13:02～2006/01/18 06:31 の期間に 4 台のクライアント PC を用いて並行して行った。

図 2-32 にデジタル署名及び署名タイムスタンプ付与の処理時間を示す。

なお、図 2-32 はログファイル上に記録された処理の開始時間と終了時間の間を処理時間とし、処理の開始時間に対して処理時間の値をプロットしたものである。

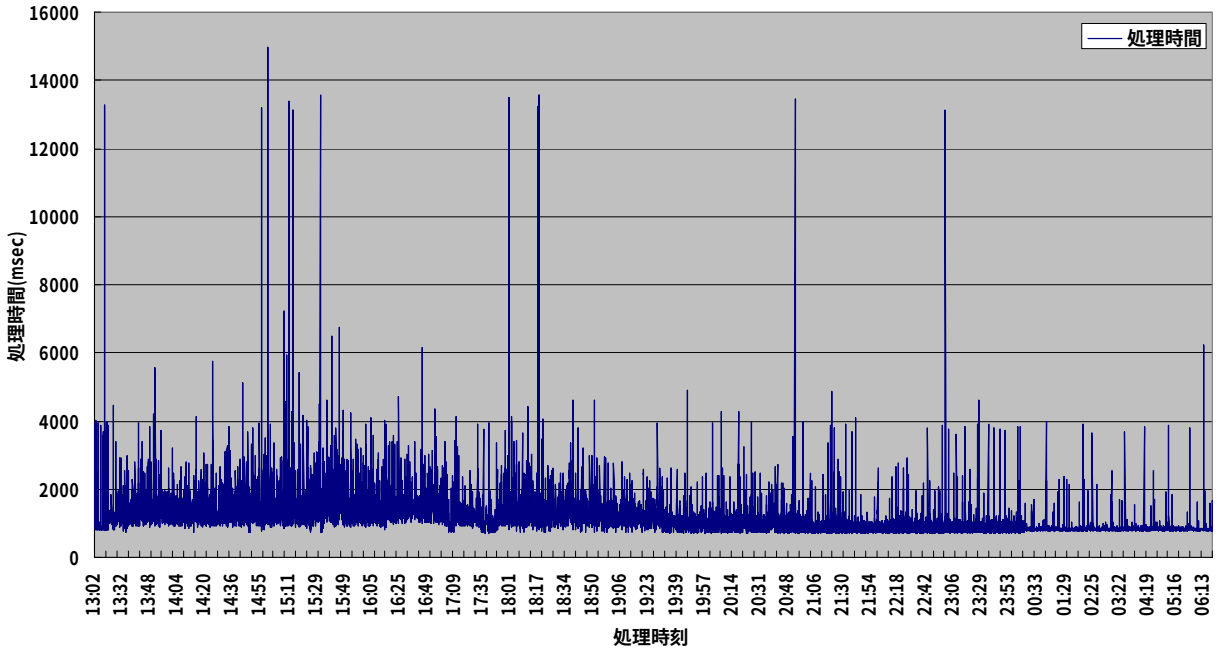


図 2-32　デジタル署名及び署名タイムスタンプ付与の処理時間

表 2-19 にデジタル署名及び署名タイムスタンプ付与の処理結果を示す。

なお、表 2-19 はログファイル上に記録された各処理時間の平均時間、最大値及び最小値である。

表 2-19　デジタル署名及び署名タイムスタンプ付与の処理結果(msec)

#	項目名	処理時間（msec）
1	平均値	1204
2	最大値	14953
3	最小値	687

表 2-20 にデジタル署名及び署名タイムスタンプ付与の所要時間を示す。

なお、表 2-20 の総所要時間とは一連の処理において、最初の処理の開始時刻から最後の処理の終了時刻までの実際に掛かった時間であり、平均所要時間は総所要時間を処理回数（＝文書数＝10000）で割った値である。

表 2-20　デジタル署名及び署名タイムスタンプ付与の所要時間

#	項目名	所要時間
1	総所要時間	17時間29分20秒703
2	平均所要時間	6296 ms

5-6-2 アーカイブタイムスタンプ（初回）付与処理結果

1 万件のアーカイブタイムスタンプ（初回）の付与は 2006/01/21 13:01～2006/01/22 06:30 の期間に実行された。

なお、アーカイブタイムスタンプの付与は署名タイムスタンプが付与されてから 4 日経過後に順次実施されるため、各々の署名タイムスタンプの付与されたタイミングによって総所要時間が決定する。

図 2-33 にアーカイブタイムスタンプ（初回）付与の処理時間を示す。

なお、図 2-33 はログファイル上に記録された処理の開始時間と終了時間の間を処理時間とし、処理の開始時間に対して処理時間の値をプロットしたものである。

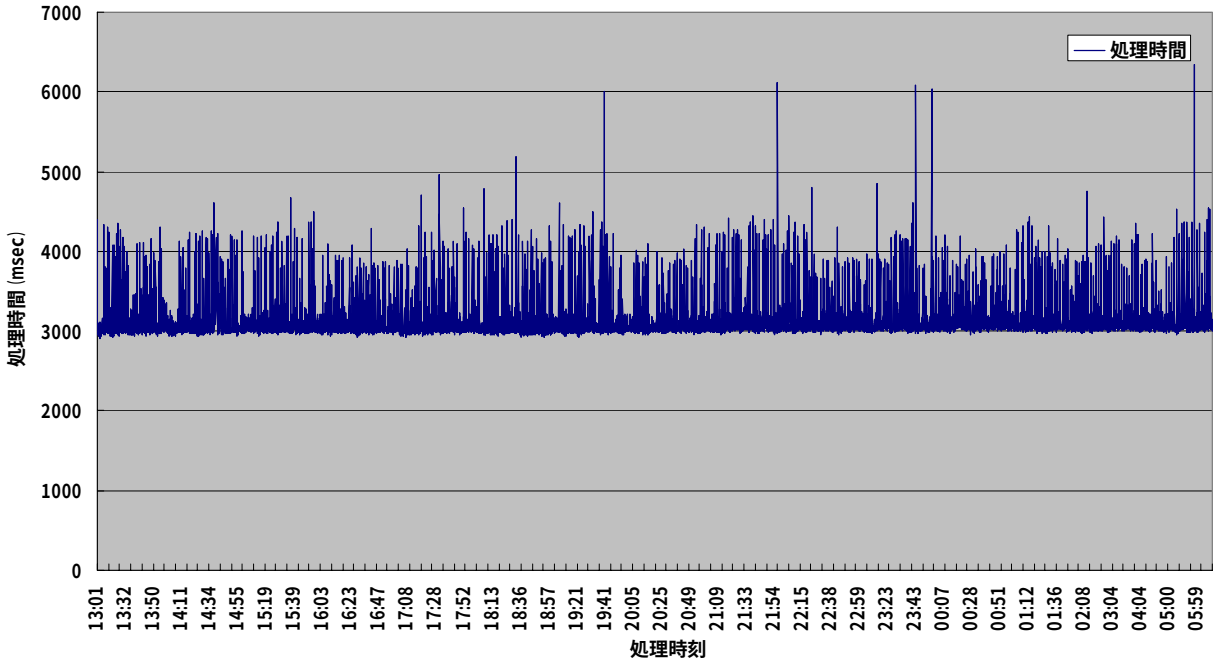


図 2-33　アーカイブタイムスタンプ（初回）の処理時間

表 2-21 にアーカイブタイムスタンプ（初回）の付与処理結果を示す。

なお、表 2-21 はログファイル上に記録された各処理時間の平均時間、最大値及び最小値である。

表 2-21　アーカイブタイムスタンプ（初回）の処理結果(msec)

#	項目名	処理時間（msec）
1	平均値	3111
2	最大値	6344
3	最小値	2907

表 2-22 にアーカイブタイムスタンプ（初回）付与の所要時間を示す。

なお、表 2-22 の総所要時間とは一連の処理において、最初の処理の開始時刻から最後の処理の終了時刻までの実際に掛かった時間であり、平均所要時間は総所要時間を処理回数（＝文書数＝10000）で割った値である。

表 2-22　アーカイブタイムスタンプ（初回）付与の所要時間

#	項目名	所要時間
1	総所要時間	17時間28分13秒047
2	平均所要時間	6289 ms

5-6-3 アーカイブタイムスタンプ（効力延長）付与処理結果

1 万件のアーカイブタイムスタンプ（効力延長）の付与は 2006/01/23 16:21～2006/01/24 06:29 の期間に実行された。

図 2-34 にアーカイブタイムスタンプ（効力延長）付与の処理時間を示す。

なお、図 2-34 はログファイル上に記録された処理の開始時間と終了時間の間を処理時間とし、処理の開始時間に対して処理時間の値をプロットしたものである。

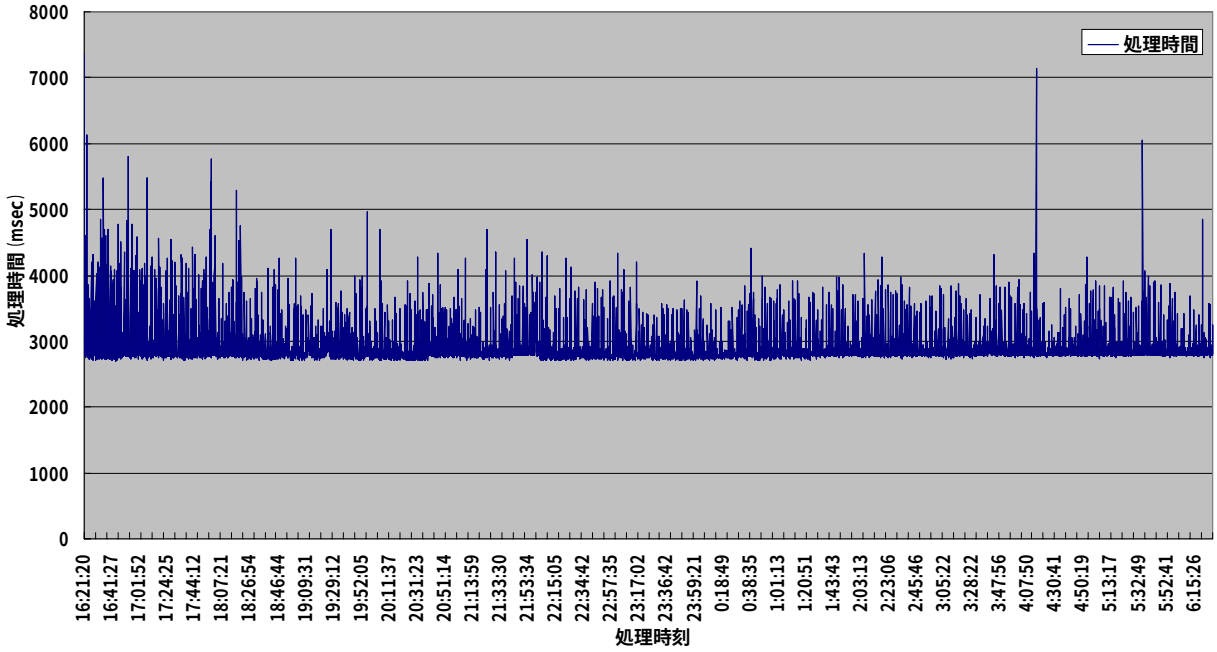


図 2-34　アーカイブタイムスタンプ（効力延長）の処理時間

表 2-23 にアーカイブタイムスタンプ（効力延長）の付与処理結果を示す。

なお、表 2-23 はログファイル上に記録された各処理時間の平均時間、最大値及び最小値である。

表 2-23　アーカイブタイムスタンプ（効力延長）の処理結果(msec)

#	項目名	処理時間（msec）
1	平均値	2885
2	最大値	7344
3	最小値	2687

表 2-24 にアーカイブタイムスタンプ（効力延長）付与の所要時間を示す。

なお、表 2-24 の総所要時間とは一連の処理において、最初の処理の開始時刻から最後の処理の終了時刻までの実際に掛かった時間であり、平均所要時間は総所要時間を処理回数（＝文書数＝10000）で割った値である。

表 2-24　アーカイブタイムスタンプ（効力延長）付与の所要時間

#	項目名	所要時間
1	総所要時間	14時間08分00秒750
2	平均所要時間	5088 ms

本項の結果より、本実証実験と同様の環境において、処理対象の文書数と各文書へのアーカイブタイムスタンプ（効力延長）付与の所要時間に比例関係があると仮定すると、例としてアーカイブタイムスタンプを 100 万件の文書に対して再付与を行う際に必要な日数は、

14時間08分00秒(一万件の効力延長の所要時間)×100　59日　　…(式1)

となり、タイムスタンプの有効性が損なわれる前にタイムスタンプの再付与処理に必要と見込まれる期間は、約２ヶ月程度となる。

式 1 と同様の仮定に基づいて、処理対象の文書数とその再付与処理の所要時間について推測される関係を図 2-35 に示す。

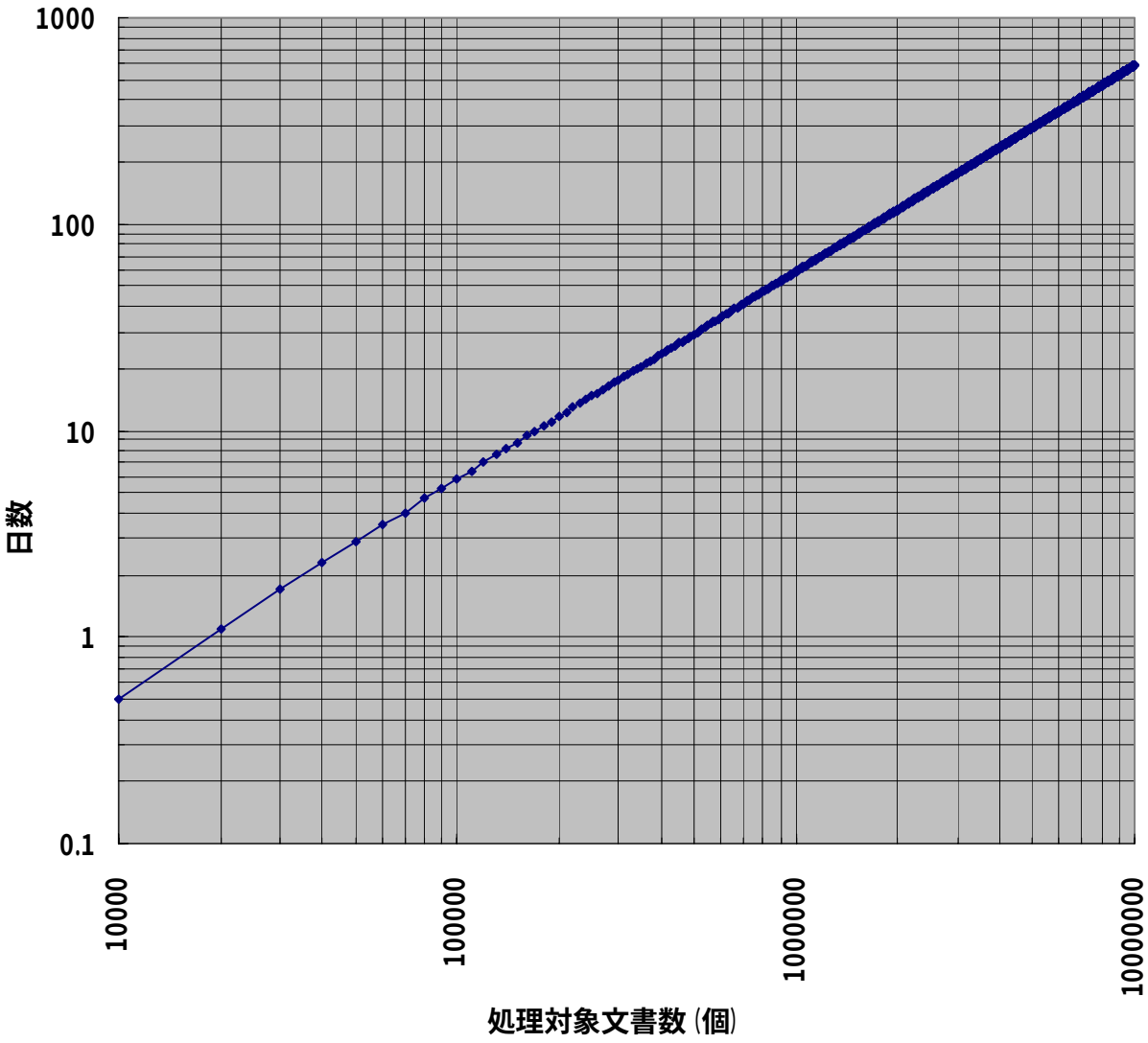


図 2-35　推測される処理対象の文書数と所要時間の関係

5-7 長期保証運用性評価

4-3-6 で述べたように、アーカイブタイムスタンプ（効力延長）の付与は、文書管理システムの管理者によってサーバ上の既存のアーカイブタイムスタンプ（効力延長）用の検索条件ファイルを設定することで行われる。

本実証実験では、アーカイブタイムスタンプの再付与を実施する際に、最終更新日時を指定して行った。

図 2-36 にアーカイブタイムスタンプの再付与を行う際に設定する検索条件ファイルを示す。

```
<?xml version="1.0" encoding="Shift_JIS"?>
<eappli:between xmlns:eappli="http://www.fujixerox.co.jp/2002/09/eappli">
  <eappli:idExpr>
    <system:modifiedon xmlns:system="system"/>
  </eappli:idExpr>
  <eappli:valueExpr>
    <eappli:dateValue>2006-01-21 12:00:00 JST</eappli:dateValue>
  </eappli:valueExpr>
  <eappli:valueExpr>
    <eappli:dateValue>2006-01-22 08:00:00 JST</eappli:dateValue>
  </eappli:valueExpr>
</eappli:between>
```

図 2-36　検索条件ファイル

図 2-36 は本実証実験で用いた検索条件ファイルである。

上記のようなファイルを文書管理サーバへ設定することにより、タイムスタンプの有効性が損なわれる可能性が発生した場合でも、アーカイブタイムスタンプ再付与を実施することで、その効力を保つことができる。

図 2-36 は最終更新日を検索条件のキーとしている。

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合としては、以下が挙げられる。

- 近い将来にハッシュアルゴリズムの脆弱化が発生することが予想される。
- 近い将来にタイムスタンプの有効期間が完了する。

表 2-25 に代表的なタイムスタンプの有効性が損なわれる可能性が生じる場合と、各場面に応じた検索条件のキーを示す。

表 2-25　タイムスタンプの有効性が損なわれる可能性が生じる場合毎の検索条件キー

#	タイムスタンプの有効性が損なわれる可能性が生じる場合	検索条件キー
1	近い将来にハッシュアルゴリズムの脆弱化が発生することが予想される。	暗号アルゴリズム
2	近い将来にタイムスタンプの有効期間が完了する。	最終変更日時

5-8 長期保証操作性評価

ユーザビリティ評価は全てログイン後、ドキュメントサービス画面において、試験用のフォルダを表示している状態より実施した。

表 2-26 にユーザビリティ評価の結果を示す。

なお、表 2-26 の所要時間は操作の開始後、画面が遷移してゆき、処理終了後、操作開始時の画面に戻るまでの時間を表している。また、ファイル検索に関しては画面上部の検索フィールドより「usability」をファイル名に含むファイルを検索した際の結果を表している。

表 2-26　ユーザビリティ評価結果

#	操作名	操作概要	所要時間	操作内容			
1	ファイル登録	ファイルを登録する。	41.4秒	クリック		入力	
				ボタン	4回	テキスト	0回
				チェックボックス	0回		文字程度
				選択	0回	Dクリック	1回
						D&D	1回
2	デジタル署名付与	登録したファイルにデジタル署名を付与する	32.1秒	クリック		入力	
				ボタン	4回	テキスト	0回
				チェックボックス	0回		文字程度
				選択	1回		
3	デジタル署名検証	2でデジタル署名付与されたファイルの検証	19.4秒	クリック		入力	
				ボタン	2回	テキスト	0回
				チェックボックス	0回		文字程度
				選択	1回		
4	署名タイムスタンプ付与	2で署名されたファイルに対するタイムスタンプの付与	38.2秒	クリック		入力	
				ボタン	4回	テキスト	0回
				チェックボックス	0回		文字程度
				選択	1回		
5	アーカイブタイムスタンプ検証	アーカイブタイムスタンプ（初回）が付与されたファイルに対してタイムスタンプ検証処理を実行する。	19.6秒	クリック		入力	
				ボタン	2回	テキスト	0回
				チェックボックス	0回		文字程度
				選択	1回		
6	ファイルダウンロード	アプリケーションの「ファイルダウンロード機能」を使用してファイルを取得する。	11.6秒	クリック		入力	
				ボタン	3回	テキスト	0回
				チェックボックス	0回		文字程度
				選択	1回		
7	ファイル検索	アプリケーションの「ファイル検索機能」を使用してファイルを検索する。	10.3秒	クリック		入力	
				ボタン	1回	テキスト	1回
				チェックボックス	0回		9文字程度
				選択	0回		

第3章 おわりに

1. 成果

本実証実験では、評価項目に沿って、デジタル署名、署名タイムスタンプ及びアーカイブタイムスタンプに係る各種評価結果を得られた。

本実証実験で得られた成果を以下に示す。

1-1 各評価項目の評価結果

1-1-1 時刻トレーサビリティ機能評価結果

第 2 章 5-1 の結果より、以下が確認できた。

1. 時刻監査レポートの真正性を確認可能であること
2. 時刻監査レポートより、時刻配信経路を確認できること
3. 時刻監査レポートより、タイムスタンプトークンの発行時の誤差を確認できること

本実証実験では、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を実現できた。

1-1-2 長期保証機能評価結果

第 2 章 5-2 の結果より、以下が確認できた。

1. XAdES をベースにしたフォーマットを実装し、原本性保証情報の格納ができること
2. タイムスタンプ長期保証ガイドラインに従った方式により、アーカイブタイムスタンプの付与によるデジタル署名及びタイムスタンプの長期保証ならびにその検証が行えること

本実証実験では、長期保証に対応したタイムスタンプの付与、再付与及び検証を XAdES をベースにしたフォーマットで実装できた。

1-1-3 長期保証データ容量評価結果

第 2 章 5-3 の結果より、以下が確認できた。

1. 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

本実証実験では、XAdES をベースにしたフォーマットで長期保証を行う場合に必要となるデータの容量の指標を得られた。

1-1-4 例外発生時動作評価結果

第 2 章 5-4 の結果より、以下が確認できた。

1. アプリケーションの操作時に例外が発生した場合に、発生した例外に応じてエラーメッセージが出力されること

本実証実験では、実証実験で使用した文書管理システムに例外発生時のユーザインタフェースが適切に実装されていることを確認した。

1-1-5 長期保証単一処理時間性能評価結果

第 2 章 5-5 の結果より、以下が確認できた。

1. 署名タイムスタンプ付与及びアーカイブタイムスタンプ付与の処理時間
2. デジタル署名、署名タイムスタンプ付与及びアーカイブタイムスタンプ検証の処理時間

本実証実験では、アーカイブタイムスタンプの付与における、デジタル署名及びタイムスタンプの長期保証ならびにその検証を行った際の処理時間の指標を得られた。

1-1-6 長期保証大量処理時間性能評価結果

第 2 章 5-6 の結果より、以下が確認できた。

1. 大量の文書に対するデジタル署名、署名タイムスタンプ付与及びアーカイブタイムスタンプ付与の処理時間

本実証実験では、大量の文書に対して、アーカイブタイムスタンプの付与によるタイムスタンプの長期保証を行った際の処理時間の指標を得られた。

1-1-7 長期保証運用性評価結果

第 2 章 5-7 の結果より、以下が確認できた。

1. 文書管理サーバの管理者の操作により、効力延長対象の文書に対し、条件を指定してアーカイブタイムスタンプ（効力延長）を付与できること

本実証実験では、実際にタイムスタンプの有効性が損なわれる可能性が発生した場合に、管理者の適切な操作によって対象となる文書の抽出を簡易に実行でき、タイムスタンプの効力延長を柔軟に行えることを確認した。

1-1-8 長期保証操作性評価結果

第 2 章 5-8 の結果より、以下が確認できた。

1. 利用者のタイムスタンプ付与の操作に係る操作回数と所要時間
2. 検証者のタイムスタンプ検証の操作に係る操作回数と所要時間

本実証実験では、実際に利用者及び検証者がアプリケーションを操作した際に、どの程度の操作回数及び時間を要するかの指標を得られた。

2. 今後の課題

本実証実験においては、実環境に近い形でのアプリケーションと連携し、タイムスタンプの長期保証に係る実験を実施した。

今後、さらなる利便性の向上や実運用上の指標の明確化に向けて、以下の課題が存在する。

2-1 時刻のトレーサビリティ調査の自動化

本実証実験で使用した文書管理システム及び方式では、時刻トレーサビリティの確認の際に、時刻監査レポートと文書管理システムの画面を目視にて確認を行ない、誤差情報を手動にて求めた。

今回の手法では、時刻トレーサビリティの確認の際に目視での確認や手動による計算作業が入るため、長期間運用を行う際には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。

2-2 環境や測定条件を変えた際の、大量文書長期保証の処理性能の推移と特性の計測

本実証実験では、第 2 章 5-6 で示したように、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。

しかしながら、この指標は環境に依存する点が多く、以下の環境が変化することで所要時間が大きく変わる可能性がある。

- ハードウェア構成（CPU、メモリ、HDD 等、負荷分散環境の有無）
- 文書管理サーバと TSA 間の回線速度

また、本実証実験では大量文書の処理を 100KBytes のファイルに対してのみ実施していたが、ファイルのデータ容量がある程度以上になると処理時間が大幅に変化することは「図 2-29　付与処理時間の推移」及び「図 2-30　検証処理時間の推移」より明らかであり、大量の文書を処理する際に各ファイルのデータ容量が変化することで所要時間が大きく変化することが予測できる。

さらに、本実証実験では 1 万件の文書の処理に掛かる所要時間からより大量の文書に対する処理の所要時間を、単純な比例関係と仮定して指標を求めているが、より大量の文書を処理する際に、処理の所要時間と処理件数の間に単純な比例関係ではない値となる可能性も考えられる。

以上の点を踏まえ、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。

参考文献

[1] ”タイムスタンプ長期保証ガイドライン Ver1.1”,タイムビジネス推進協議会(TBF),2005/02
[2] ” XML Advanced Electronic Signatures (XAdES)”, Ver1.3.1, 欧州通信規格協会(ETSI),2005/05
[3] ”タイムスタンプ･プロトコルに関する技術調査”,独立行政法人 情報処理推進機構(IPA),2004/02
[4] ”XAdES 長期署名プロファイル(案)”,次世代電子商取引推進協議会(ECOM),2005/08

VA による長期保証実証実験評価報告書

平成 18 年 3 月 16 日

独立行政法人情報通信研究機構

株式会社 日立製作所

セイコーインスツル株式会社

目次

第 1 章 はじめに 1
1. 背景 1
2. タイムスタンプの課題 1
3. 課題への対策状況 1
4. 実験の目的 1
第 2 章 実験内容 3
1. 実験概要 3
2. 前提条件 3
3. システム構成 4
4. 各機器の役割とスペック 4
5. シナリオ 6
6. 実験スケジュールと作業内容 6
7. 測定項目 8
8. 評価項目 9
第 3 章 実験結果と評価結果 10
1. 項目別評価結果 10
1-1 長期保証機能の動作検証 10
1-2 性能評価 10
1-2-1 再タイムスタンプ方式 10
1-2-2 セキュア保管方式 12
1-2-3 方式ごとの比較 14
1-3 運用評価 15
1-4 その他の評価 16
1-4-1 データサイズ 16
2. 全体評価結果 18
第 4 章 考察 19
1. 実運用に向けた考察 19
1-1 利便性を考慮した考察 19
1-1-1 再タイムスタンプ方式 19
1-1-2 セキュア保管方式 19
1-2 技術的な課題に係わる考察 19
1-2-1 再タイムスタンプ方式 19
1-2-2 セキュア保管方式 20
第 5 章 終わりに 22

第1章 はじめに

1. 背景

2005 年 4 月の e-文書法の施行などに見られるように、タイムスタンプの利用用途が拡大してきている。今後タイムスタンプが益々普及することが予想され、課題である「タイムスタンプの長期保証」に関して議論され始めている。将来に渡って安全にタイムスタンプを利用する為に、現時点から長期保証に関して検討し、指針等を整理しておく必要がある。

2. タイムスタンプの課題

独立トークン方式を利用するタイムスタンプにおいて、タイムスタンプを長期にわたって使用する場合に、以下の課題が残されている。

- タイムスタンプには有効期限が存在する。
  （有効期限の切れたタイムスタンプは信頼性が保たれない。）
- タイムスタンプ用の公開鍵証明書が失効された場合、信頼性を保つことができない。
- タイムスタンプに使用された暗号アルゴリズムが脆弱化した場合に、信頼性を保つことができない。

3. 課題への対策状況

上述の課題に対して、タイムビジネス推進協議会の「タイムスタンプ長期保証ガイドライン」では以下の対策方法が提示されている。

表 1-1「タイムスタンプ長期保証ガイドライン」概要

No.	分類	方式	説明
1	本文	再タイムスタンプ方式	タイムスタンプに対して、再タイムスタンプを繰り返し付与することにより、効力を延長する。
2	参考 1	セキュア保管方式	保管対象データを、厳密な運用の下に管理して保管する。 その中の方式の一つとして、「長期使用を前提とした電子署名方式」があり、今回は「長期使用を前提とした電子署名方式（ヒステリシス署名方式）」にて実験を実施する。
3	参考 2	DS-IMT 方式	イベント登録時期の前後関係を、ハッシュ関数の安全性に基づいて証明することにより、タイムスタンプの長期保証を実現する。 なお、本方式は現段階で研究レベルの為、本実証実験ではスコープ外とする。

各方式の詳細説明は、「タイムスタンプ長期保証ガイドライン」を参照のこと。

4. 実験の目的

上述の通り、タイムスタンプの長期保証に関しては、ガイドラインが提示されているが、以下の

点を中心に検証が十分であるとは言い難い。

- 実機を用いた検証結果がない。
- 各方式の比較検証がない。

そこで、本実証実験においては、ガイドラインにて提示された各方式のうち、実用化を前提に検討されている「再タイムスタンプ方式」及び「セキュア保管方式」に関して、実フィールドにて実験を行う。そして、実際に利用する場合のメリット／デメリットなどを比較評価し、考察を行う。

また、各方式の課題の整理、解決策の検討・提案を行い、実用化に向けた一つの指標を提示する。

第2章 実験内容

1. 実験概要

「再タイムスタンプ方式」及び「セキュア保管方式」の各タイムスタンプ長期保証方式において、実機を用いて、性能・運用負荷などを評価する。

2. 前提条件

以下前提条件のもと、実証実験を実施した。

- 実験のプラットフォームとして、独立行政法人情報通信研究機構が構築した「時刻認証基盤実験装置」を使用する。
- 50 年間の想定シナリオを、5 日間に短縮して実験を行う。
  50 年間とは、著作物における有効期間の目安の一つであり、それをもとに設定した。
  例えば、実際には 5 年間有効なタイムスタンプは実験では約 12 時間有効である、と仮定する。
- 「再タイムスタンプ方式」及び「セキュア保管方式」に関して、それぞれ 5 日間実験を行う。
- 50 年の想定シナリオのイベントとして、「検証を 5 年に 1 度」、「アルゴリズム等の危殆化を 50 年に 2 度」、と設定する。
- 検証サーバ(VA)の利用者は 15 人、利用頻度は 1 回／月、とする。
  VA のビジネスモデルが明確になっていない現状においては、基準を設定することは困難であるが、仮に上記の値に設定した。
- 長期保証対象データは 3 種類準備し、10KB／100KB／1MB のファイルサイズとする。
  長期保証対象データは著作物などを想定しているが、実験では意味をなさないデータで行う。
- 50 年の想定シナリオにおいて、機器の性能向上は考慮しない。
  例えば、50 年後でも現在と同一スペックの機器を利用しているものと仮定する。

表 2-1 想定シナリオの時間と実証実験での時間の対応

No.	項目	想定	実験	備考
1	シナリオ	50 年	5 日	
2	検証間隔	5 年に一度	半日に一度	実験では、午前に 1 回、午後に 1 回の頻度で検証する。
3	タイムスタンプ有効期間	(例)5 年	(例)12 時間	実験で取得する TST の有効期間は(例)5 年であるが、机上にて 12 時間に変換して考える。(再タイムスタンプ方式の場合、「12 時間以内に再タイムスタンプを取得する必要がある」と考える。)
4	CA 証明書有効期間	10 年	*1 日*	正確に実験する場合は、証明書や失効リストを短いスパンで更新する必要があるが、今回の実験では、更新は行わないものとする。（今回は、性能や運用負荷を中心に評価を行う為、実験自体には影響を及ぼさない。）
5	NTA/TA/TSA 証明書有効期間	5 年	*12 時間*	
6	失効リスト(ARL/CRL)	10 日	*約 4 分*	

3. システム構成

本実証実験におけるシステム構成を図 2-1に示す。

ネットワーク環境に関して、検証クライアント－VA 間は社内ネットワーク経由のインターネット、VA－ディレクトリ間は LAN、VA－TSA 間はインターネットを介して接続されている。

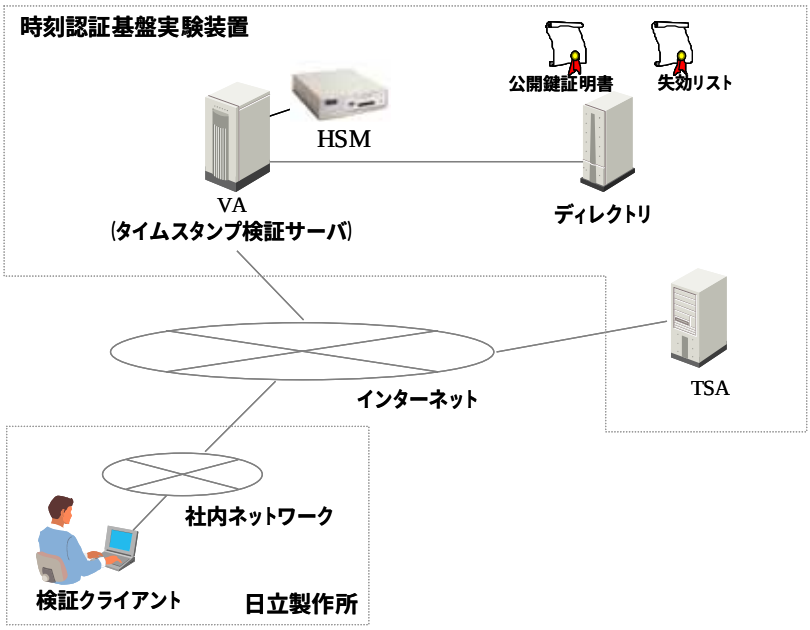


図 2-1　実証実験システム構成図

4. 各機器の役割とスペック

本実証実験における各機器の役割とスペックを、表 2-2に示す。

表 2-2 各機器の役割とスペック

No.	機器名称	役割	機器スペック
1	VA (タイムスタンプ検証サーバ)	検証クライアントからタイムスタンプ検証要求を受け付け、検証(*1)を実施後、検証結果を返却する。 また、長期保証機能に関しては、「再タイムスタンプ方式」ではタイムスタンプに対して再タイムスタンプを付与し、「セキュア保管方式」では検証した結果をヒステリシス署名にて長期保管する、それぞれの機能を併せ持つ。 「再タイムスタンプ方式」では、検証結果と共に、”再タイムスタンプされたタイムスタンプ”が返却される。	機器：Sun Blade 150 OS：Solaris 8 CPU：UltraSPARC Ⅱi 550MHz メモリ：768MB HDD：80GB
2	ディレクトリ	VA がタイムスタンプ検証を実施する際に必要となる、「各種公開鍵証明書」及び「失効リスト」を公開する。	機器：HA8000/30 OS：Windows 2000 Server CPU：Celeron 2GHz メモリ：512MB HDD：80GB

3	TSA	「再タイムスタンプ方式」の場合に、VA からアクセスし再タイムスタンプを付与する。	機器：DELL PowerEdge 650 OS ： Red Hat Professional Workstation CPU：Pentium4 2.4GHz メモリ：1GB HDD：40GB
4	検証クライアント	VA に対してタイムスタンプ検証要求を送付し、検証結果を受け取る。	機器：FRORA 310 OS：Windows 2000 Professional CPU：Pentium3 866MHz メモリ：128MB HDD：20GB

(*1)VA で実施するタイムスタンプ検証とは以下表 2-3の項目を示す。

表 2-3 VA におけるタイムスタンプ検証項目

No.	検証項目	詳細	備考
1	正当性検証	(1) タイムスタンプトークン(以下、TST)の形式が正しいことを確認する。 (2) TST が改ざんされておらず、信頼できる発行元で作成されていることを確認する。 (3) TST と文書の対応が正しいことを確認する。	長期保証データの作成を実施する場合、「正当性検証」「時刻トレーサビリティ検証」にて正常であることを確認後、それぞれの方式に応じた処理を行う。
2	時刻トレーサビリティ検証	(1) TST 及び TST に添付される監査証明書、より時刻配信経路を検証する。 (2) TST 及び TST に添付される監査証明書、より時刻誤差を検証する。	
3	長期保証検証	＜再タイムスタンプ方式＞ 再タイムスタンプの検証、過去の時点でのタイムスタンプの検証、により過去時点でタイムスタンプの有効性を確認する。	
		＜セキュア保管方式＞ ヒステリシス署名を検証することにより、過去時点でのタイムスタンプの有効性を確認する。	

5. シナリオ

以下図 2-2に示す想定シナリオに基づき、長期保証の実証実験を実施する。50 年間の想定シナリオを 5 日間に短縮して実験を行う。

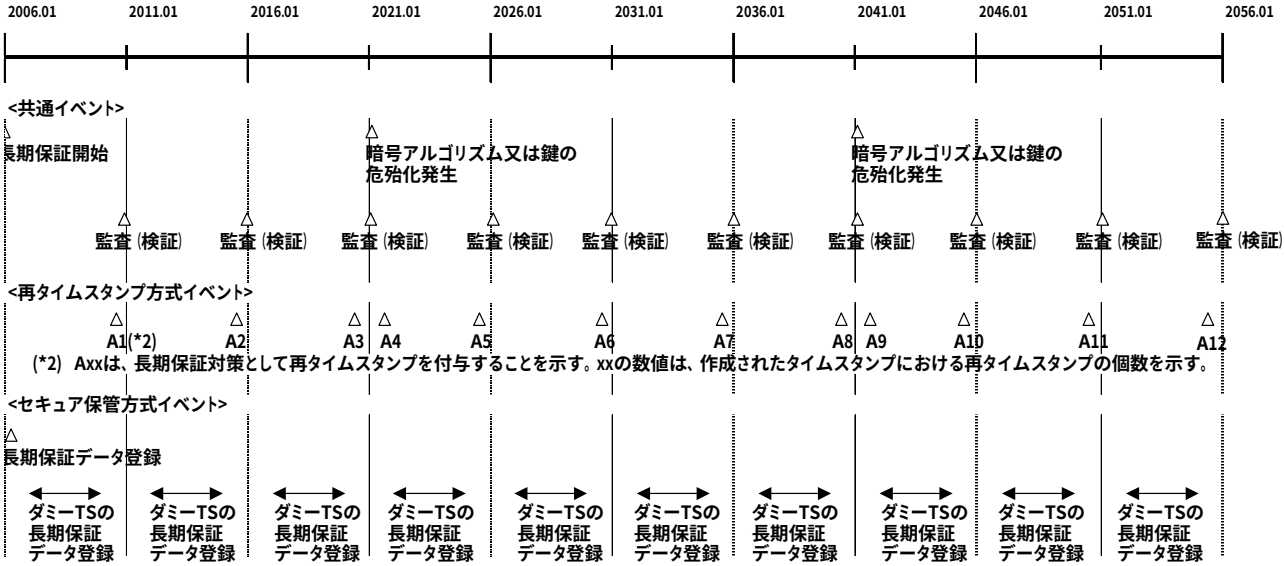


図 2-2 想定シナリオ

6. 実験スケジュールと作業内容

実証実験のスケジュールを以下表 2-4に示す。また、作業内容を以下表 2-5に示す。

表 2-4 実証実験スケジュール

No.	方式	実験日程	実験期間
1	再タイムスタンプ方式	2006 年 1 月 11 日(水)～2006 年 1 月 17 日(火)	うち 5 日間
2	セキュア保管方式	2006 年 1 月 19 日(木)～2006 年 1 月 25 日(水)	うち 5 日間

表 2-5 実証実験作業内容

No.	方式	日付	作業内容	備考
1	全体	事前	① 長期保証対象文書の作成(3 種類) ② 長期保証対象 TS の作成(3 種類)	
2	再タイムスタンプ方式	1/11(水)	① 長期保証データの作成(A1 を作成) ② A1 の検証 ③ ダミーTS 検証(5 年分:900 件) ④ 長期保証データの作成(A1 から A2 を作成) ⑤ A2 の検証	作成時間を測定 検証時間を測定 作成時間を測定 検証時間を測定

3		1/12(木)	① ダミーTS 検証(5 年分:900 件) ② 長期保証データの作成(A2 から A3 を作成) ③ A3 の検証 ④ 長期保証データの作成(A3 から A4 を作成) ⑤ ダミーTS 検証(5 年分:900 件) ⑥ 長期保証データの作成(A4 から A5 を作成) ⑦ A5 の検証	作成時間を測定 検証時間を測定 脆弱化対策 作成時間を測定 検証時間を測定
4		1/13(金)	① ダミーTS 検証(5 年分:900 件) ② 長期保証データの作成(A5 から A6 を作成) ③ A6 の検証 ④ ダミーTS 検証(5 年分:900 件) ⑤ 長期保証データの作成(A6 から A7 を作成) ⑥ A7 の検証	作成時間を測定 検証時間を測定 作成時間を測定 検証時間を測定
5		1/16(月)	① ダミーTS 検証(5 年分:900 件) ② 長期保証データの作成(A7 から A8 を作成) ③ A8 の検証 ④ 長期保証データの作成(A8 から A9 を作成) ⑤ ダミーTS 検証(5 年分:900 件) ⑥ 長期保証データの作成(A9 から A10 を作成) ⑦ A10 の検証	作成時間を測定 検証時間を測定 脆弱化対策 作成時間を測定 検証時間を測定
6		1/17(火)	① ダミーTS 検証(5 年分:900 件) ② 長期保証データの作成(A10 から A11 を作成) ③ A11 の検証 ④ ダミーTS 検証(5 年分:900 件) ⑤ 長期保証データの作成(A11 から A12 を作成)	作成時間を測定 検証時間を測定 作成時間を測定
7	セキュア保管方式	1/19(木)	① 長期保証データの作成 ② ダミーTS の検証、長期保証作成(5 年分:900 件) ③ 長期保証データの検証 ④ ダミーTS の検証、長期保証作成(5 年分:900 件) ⑤ 長期保証データの検証	作成時間を測定 検証時間を測定 検証時間を測定
8		1/20(金)	① ダミーTS の検証、長期保証作成(5 年分:900 件) ② 長期保証データの検証 ③ ダミーTS の検証、長期保証作成(5 年分:900 件) ④ 長期保証データの検証	検証時間を測定 検証時間を測定

9		1/23(月)	① ダミーTS の検証、長期保証作成(5 年分:900 件) ② 長期保証データの検証 ③ ダミーTS の検証、長期保証作成(5 年分:900 件) ④ 長期保証データの検証	検証時間を測定 検証時間を測定
10		1/24(火)	① ダミーTS の検証、長期保証作成(5 年分:900 件) ② 長期保証データの検証 ③ ダミーTS の検証、長期保証作成(5 年分:900 件) ④ 長期保証データの検証	検証時間を測定 検証時間を測定
11		1/25(水)	① ダミーTS の検証、長期保証作成(5 年分:900 件) ② 長期保証データの検証 ③ ダミーTS の検証、長期保証作成(5 年分:900 件) ④ 長期保証データの検証	検証時間を測定 検証時間を測定

7. 測定項目

長期保証方式を比較するにあたって重要となる、性能に関して測定を行う。測定する項目を以下表 2-6に示す。各項目とも、検証クライアント、サーバ(VA)にてそれぞれ測定する。

表 2-6 実証実験測定項目

No.	項目	測定内容
1	長期保証データの作成(登録)	＜再タイムスタンプ方式＞ 検証クライアント：要求送付~応答受領、までの時間を測定する。(レスポンスタイム) サーバ：要求受付~TS 検証~長期保証データの作成~結果応答、までの時間を測定する。 ＜セキュア保管方式＞ 検証クライアント：要求送付~応答受領、までの時間を測定する。(レスポンスタイム) サーバ：要求受付~TS 検証~長期保証データの登録~結果応答、までの時間を測定する。
2	長期保証データの検証	＜再タイムスタンプ方式＞ 検証クライアント：要求送付~応答受領、までの時間を測定する。(レスポンスタイム) サーバ：要求受付~長期保証データの検証~結果応答、までの時間を測定する。 ＜セキュア保管方式＞ 検証クライアント：要求送付~応答受領、までの時間を測定する。(レスポンスタイム) サーバ：要求受付~長期保証データの検証~結果応答、までの時間を測定する。

8. 評価項目

それぞれの長期保証方式を比較検討することによって、各方式のメリット／デメリット及び課題を洗い出し、利用シーンに応じた適正などを評価する。本実証実験において評価を行う項目を以下表 2-7に示す。

表 2-7 実証実験評価項目

No.	評価項目	評価内容
1	長期保証機能の動作検証	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	各方式における長期保証データ作成(登録)時 及び 長期保証データ検証時の処理性能を測定結果より評価する。
3	運用評価	各方式における検証クライアント 及び VA 管理者の運用工数を評価する。
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。

第3章 実験結果と評価結果

1. 項目別評価結果

1-1 長期保証機能の動作検証

インターネットを介した環境（図 2-1　実証実験システム構成図）において、「再タイムスタンプ方式」「セキュア保管方式」のそれぞれの方式について、長期保証機能を実現可能であることを実機を用いて確認することができた。

表 3-1 各方式における長期保証の動作検証

No.	項目	再タイムスタンプ方式	セキュア保管方式
1	長期保証の動作検証	○	○
		インターネット上の環境でも、問題なく長期保証を実現することが可能。	インターネット上の環境でも、問題なく長期保証を実現することが可能。

1-2 性能評価

1-2-1 再タイムスタンプ方式

(1) 長期保証データの作成

サイズが異なる 3 種類の文書に対して、再タイムスタンプ方式にて長期保証データを作成した時の処理時間を以下表 3-2に纏める。

サーバとクライアントの 2 箇所においてログを取得することによって、測定を行った。サーバは、クライアントからの要求の受け付け～結果送付までの処理時間を測定した。クライアントは、要求送信～応答受領までの処理時間を測定した。

なお、データは 3 回実測した結果の平均値を表示している。

表 3-2 再タイムスタンプ方式　長期保証データの作成処理時間の纏め

No.	文書サイズ	測定箇所	再タイムスタンプの個数(*3)											
			1	2	3	4	5	6	7	8	9	10	11	12
1	10KB	サーバ	8s	7s	8s	9s	9s	10s	13s	14s	12s	13s	13s	14s
2		クライアント	9s	8s	10s	10s	11s	12s	15s	18s	15s	15s	17s	17s
3	100KB	サーバ	7s	7s	8s	8s	9s	12s	13s	15s	12s	13s	14s	14s
4		クライアント	9s	9s	10s	10s	11s	14s	15s	18s	15s	15s	16s	17s
5	1 MB	サーバ	8s	10s	10s	11s	12s	16s	20s	15s	18s	17s	19s	20s
6		クライアント	11s	12s	13s	14s	15s	20s	24s	19s	21s	20s	22s	23s

(*3) 長期保証により作成したタイムスタンプに含まれる再タイムスタンプの総数

サーバにおける、再タイムスタンプ個数ごとの長期保証データの作成処理時間をグラフにて図 3-1に示す。

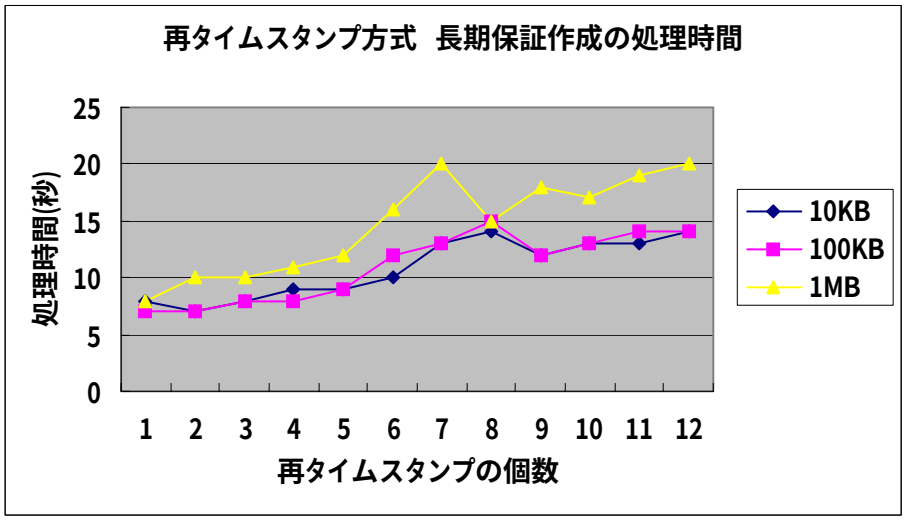


図 3-1 再タイムスタンプ方式　長期保証作成の処理時間

再タイムスタンプの個数が増加する毎に、長期保証データの作成処理時間が増加することが、分かる。これは、再タイムスタンプを付与する前に実施するタイムスタンプ検証処理の時間が、再タイムスタンプの個数に応じて変動することに起因する。

なお、再タイムスタンプ個数「7」の場合に突出して時間を要している理由は不明であるが、可能性としては VA に対する他のアクセスによって、サーバ或いはネットワークに負荷がかかっていたことが考えられる。

以下は、サーバでの処理時間に関して、機能ごとの詳細処理時間を纏めた表である。本表から、再タイムスタンプの個数に応じて、長期保証検証処理時間が変動することが分かる。

表 3-3 再タイムスタンプ方式　長期保証データの作成処理時間の詳細

No.	文書サイズ	機能(*4)	再タイムスタンプの個数											
			1	2	3	4	5	6	7	8	9	10	11	12
1	10KB	正当性検証	2s	—	—	—	—	—	—	—	—	—	—	—
2		時刻トレーサビリティ検証	4s	—	—	—	—	—	—	—	—	—	—	—
3		*長期保証検証*	—	*6s*	*6s*	*7s*	*7s*	*7s*	*9s*	*10s*	*9s*	*9s*	*10s*	*10s*
4		再 TS 付与	1s	1s	1s	1s	1s	1s	2s	3s	1s	1s	1s	1s
5		その他(*5)	1s	0s	1s	2s	1s	2s	2s	2s	2s	2s	3s	2s
6		合計	8s	7s	8s	9s	9s	10s	13s	14s	12s	13s	13s	14s
7	100KB	正当性検証	2s	—	—	—	—	—	—	—	—	—	—	—
8		時刻トレーサビリティ検証	3s	—	—	—	—	—	—	—	—	—	—	—
9		*長期保証検証*	—	*6s*	*6s*	*6s*	*7s*	*9s*	*9s*	*10s*	*9s*	*10s*	*10s*	*11s*
10		再 TS 付与	1s	1s	1s	1s	1s	1s	2s	1s	1s	1s	1s	1s
11		その他(*5)	1s	1s	1s	1s	1s	2s	2s	3s	2s	2s	3s	2s
12		合計	7s	7s	8s	8s	9s	12s	13s	15s	12s	13s	14s	14s

13	1MB	正当性検証	2s	―	―	―	―	―	―	―	―	―	―	―
14		時刻トレーサビリティ検証	4s	―	―	―	―	―	―	―	―	―	―	―
15		*長期保証検証*	―	*6s*	*7s*	*7s*	*8s*	*12s*	*11s*	*11s*	*11s*	*11s*	*13s*	*14s*
16		再 TS 付与	1s	1s	1s	1s	1s	2s	2s	1s	3s	1s	1s	1s
17		その他(*5)	2s	2s	2s	3s	3s	3s	8s	3s	2s	5s	4s	5s
18		合計	8s	10s	10s	11s	12s	16s	20s	15s	17s	17s	19s	20s

(*4) 検証するタイムスタンプの中に再タイムスタンプが存在するか否かによって、検証内容が異なる。再タイムスタンプの個数「1」と「2 以上」で実施項目が異なるのは、その為である。VA の詳細仕様は、「取扱説明書　複数方式タイムスタンプ検証サブシステム(3)」を参照のこと。

(*5) その他の機能は、要求データの解析処理など「機能」項目に登場しない処理を指し示す。

(2) 長期保証データの検証

再タイムスタンプ方式の検証処理は、「長期保証データの作成」処理に包含されている。従って、「長期保証データの作成」の全体処理時間から、「再タイムスタンプ付与」の処理時間を省いたものが、再タイムスタンプ方式の検証処理時間に該当する。

今回の実験では、VA の設定において「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」と設定していた為、純粋に検証のみの時間を測定することは出来なかった。従って、実測値を元にした計算によって、検証処理時間を導き出した。

表 3-4 再タイムスタンプ方式　長期保証検証処理時間

No.	文書サイズ	測定箇所	再タイムスタンプの個数										
			1	2	3	4	5	6	7	8	9	10	11
1	10KB	サーバ	7s	6s	7s	8s	8s	9s	11s	11s	11s	12s	12s
2	100KB	サーバ	6s	6s	7s	7s	8s	11s	11s	14s	11s	12s	13s
3	1MB	サーバ	7s	9s	9s	10s	11s	14s	18s	14s	14s	16s	18s

前述の通り、再タイムスタンプの個数の増加によって、検証処理時間も増加していることが分かる。

1-2-2 セキュア保管方式

(1) 長期保証データの作成

セキュア保管方式の場合、長期保証データの作成(登録)は 1 度実施すればよい。要求受付 ~ TS 検証~長期保証データの登録~結果応答を、以下表 3-5に示す。

表 3-5 セキュア保管方式　長期保証作成の処理時間

No.	文書サイズ	測定箇所	長期保証データの作成処理時間
1	10KB	サーバ	8s
2	100KB	サーバ	8s

3	1MB	サーバ	9s

なお、ダミーで大量に長期保証データを登録しているが、登録件数に係らず長期保証データの新規作成時間は一律 7～9s であった。

(2) 長期保証データの検証

セキュア保管方式の場合の検証処理時間を、以下表 3-6に示す。なお、検証の各回の間に、ダミーTS の長期保証作成(登録)が 900 件なされている。よって、ヒステリシス署名技術の仕様上、検証の際は前回の検証時より、900 回署名検証を実施することになる。

なお、データは 3 回実測した結果の平均値を表示している。

表 3-6 セキュア保管方式　長期保証検証処理時間

No.	文書サイズ	測定箇所	検証回数									
			1	2	3	4	5	6	7	8	9	10
1	10KB	サーバ	4s	5s	6s	8s	9s	11s	14s	16s	19s	19s
2		クライアント	5s	7s	9s	9s	11s	13s	16s	17s	21s	21s
3	100KB	サーバ	4s	5s	6s	7s	8s	10s	13s	15s	17s	19s
4		クライアント	5s	6s	9s	9s	10s	11s	17s	16s	19s	20s
5	1 MB	サーバ	5s	7s	9s	9s	11s	12s	16s	17s	20s	21s
6		クライアント	8s	9s	11s	11s	13s	14s	18s	19s	22s	23s

また、サーバにおける、長期保証データの検証処理時間をグラフにて図 3-2に示す。

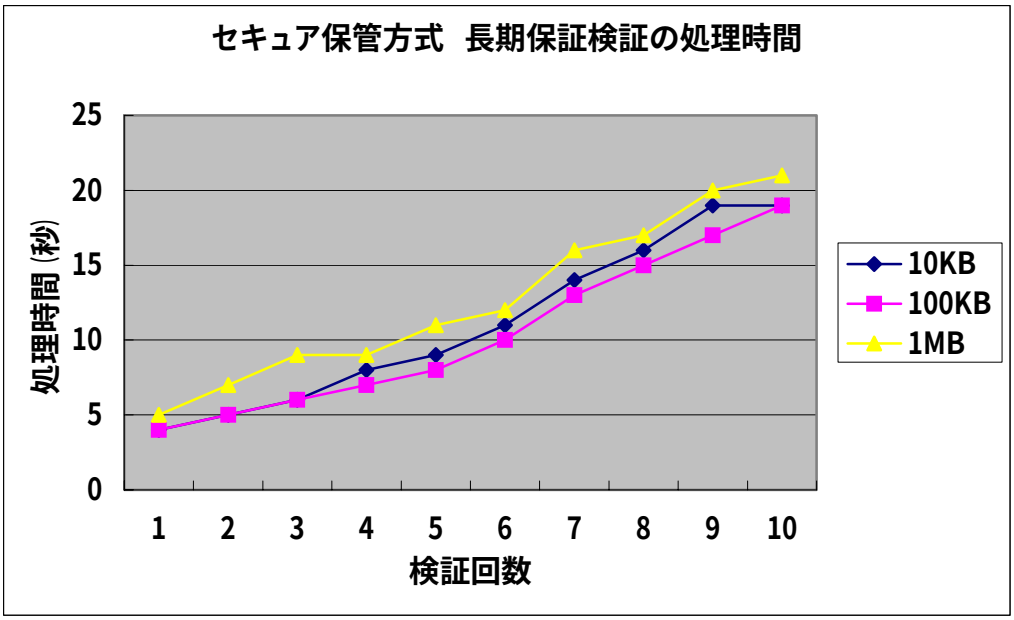


図 3-2 セキュア保管方式　長期保証検証の処理時間

グラフより、検証回数が増すにつれて、検証処理時間が増加することが確認できる。

以下表 3-7は、サーバでの処理時間に関して、機能ごとの詳細処理時間を纏めた表である。本表から、検証回数が増すにつれて、「長期保証データの検証」処理時間が増加することを確

認できる。

表 3-7 セキュア保管方式　長期保証データの検証処理時間の詳細

No.	文書サイズ	機能	検証回数									
			1	2	3	4	5	6	7	8	9	10
1	10KB	正当性検証(*6)	1	2	2	3	2	2	2	2	1	2
2		時刻トレーサビリティ検証	—	—	—	—	—	—	—	—	—	—
3		*長期保証検証*	*2*	*4*	*4*	*7*	*9*	*11*	*14*	*14*	*21*	*18*
4		その他	1	0	1	0	0	0	1	1	1	1
5		合計	4	6	7	9	11	13	17	17	23	21
6	100KB	正当性検証(*6)	1	1	2	1	2	1	2	1	2	2
7		時刻トレーサビリティ検証	—	—	—	—	—	—	—	—	—	—
8		*長期保証検証*	*2*	*3*	*4*	*6*	*7*	*8*	*11*	*13*	*15*	*16*
9		その他	1	1	0	1	0	1	1	1	1	1
10		合計	4	5	6	8	9	10	14	15	18	19
11	1MB	正当性検証(*6)	2	2	2	2	2	2	2	2	2	2
12		時刻トレーサビリティ検証	—	—	—	—	—	—	—	—	—	—
13		*長期保証検証*	*2*	*4*	*4*	*5*	*7*	*8*	*13*	*13*	*15*	*17*
14		その他	2	1	3	2	2	2	2	2	2	2
15		合計	6	7	9	9	11	12	17	17	19	21

(*6) 正当性検証にて公開鍵証明書が無効であることが判明し、長期保証検証へと移る。その為、時刻トレーサビリティ検証は実施しない。VA の詳細仕様は、「取扱説明書　複数方式タイムスタンプ検証サブシステム(3)」を参照のこと。

1-2-3 方式ごとの比較

再タイムスタンプ方式とセキュア保管方式を性能面から見た場合の比較を以下表 3-8に示す。

表 3-8 性能面から見た各方式の比較

No.	項目	再タイムスタンプ方式	セキュア保管方式
1	長期保証作成(登録)	△	○
		前回の再タイムスタンプの有効期限までに、再度長期保証データの作成を行う必要がある。さらに、再タイムスタンプの数に応じて、長期保証データの作成処理時間も増加する。 (7～20 秒)	長期保証の登録は文書ごとに 1 度で済み、登録時間も一律でごく僅かである。 (7～9 秒)
2	長期保証検証	○	○

		再タイムスタンプの個数に応じて、検証処理時間が変動する。 (6～19 秒) なお、再タイムスタンプの個数の上限は概ね想定できる為、検証時間も想定が可能である。	長期保証データの登録件数に応じて、検証処理時間が変動する。 (4～21 秒) なお、長期保証データの登録件数の上限は想定できない為、環境によっては膨大な検証時間を要する可能性もある。

なお、性能に関しては、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一概に判断することはできない。

1-3 運用評価

実際の運用を想定した場合、再タイムスタンプ方式とセキュア保管方式では、運用方法が大きく異なる。

想定する実際の運用のなかで最も負荷の大きいと考えられる、「再タイムスタンプ方式」のクライアントでの運用に関して、考えうる項目を以下表 3-9に詳細を記載する。

表 3-9 再タイムスタンプ方式におけるクライアントでの運用

No.	分類	項目	備考
1	タイムスタンプ有効性管理	タイムスタンプ有効期限の確認	
2		暗号アルゴリズムの脆弱化確認	
3	再タイムスタンプ取得処理	タイムスタンプ対象データの取り出し	
4		タイムスタンプの取り出し	
5		VA への再タイムスタンプ要求	
6	再タイムスタンプ管理	新規に再タイムスタンプを付与したタイムスタンプの管理	管理対象データの入れ替え

各方式を運用負荷の観点から見た場合の比較を、以下表 3-10に示す。

表 3-10 運用面から見た各方式の比較

No.	項目	再タイムスタンプ方式	セキュア保管方式
1	クライアントでの運用	△	○
		タイムスタンプの有効期間を管理し、有効期限間近のタイムスタンプに対して長期保証の要求を出す必要がある。	長期保証の登録を一度済ませればよく、有効期間の管理などの運用は特に発生しない。
2	サーバでの運用	○	△
		一般的なサーバ管理の運用でよく、長期保証に向けた運用としては、TSA 局の選択程度である。	一般的なサーバ管理の運用に加え、長期保証登録データ用のストレージ管理やヒステリシス署名用の鍵更新などの運用が発生する。

1-4 その他の評価

1-4-1 データサイズ

再タイムスタンプ方式においては、再タイムスタンプを付与することによってタイムスタンプのファイルサイズが増加する。逆に、セキュア保管方式においては、タイムスタンプ自体のファイルサイズは変化しないが、サーバ側で保管する長期保証の登録データのファイルサイズが増加する。

タイムスタンプのファイルサイズの推移を表 3-11に、サーバ側での登録データのファイルサイズを表 3-12に示す。

表 3-11 各方式のタイムスタンプのファイルサイズ推移

No.	再タイムスタンプ方式	再TSの個数	セキュア保管方式	備考 (シナリオ上の経過時間)
1	3.6 Kbyte	0 個	3.6 Kbyte (ファイルサイズに変化はなし)	
2	17.5 Kbyte	1 個		
3	31.2 Kbyte	2 個		長期保証から 10 年後
4	45.0 Kbyte	3 個		
5	58.7 Kbyte	4 個		
6	72.5 Kbyte	5 個		長期保証から 20 年後
7	86.2 Kbyte	6 個		
8	100.0 Kbyte	7 個		長期保証から 30 年後
9	113.7 Kbyte	8 個		
10	127.5 Kbyte	9 個		
11	141.2 Kbyte	10 個		長期保証から 40 年後
12	155.0 Kbyte	11 個		
13	168.8 Kbyte	12 個		長期保証から 50 年後

表 3-12 各方式でのサーバでの登録データサイズ

No.	再タイムスタンプ方式	セキュア保管方式	長期保証登録数	備考 (シナリオ上の経過時間)
1	登録データはなし	195 Mbyte	900 件	
2		390 Mbyte	1800 件	長期保証から 10 年後
3		585 Mbyte	2700 件	
4		779 Mbyte	3600 件	長期保証から 20 年後
5		974 Mbyte	4500 件	
6		1,169 Mbyte	5400 件	長期保証から 30 年後
7		1,364 Mbyte	6300 件	
8		1,559 Mbyte	7200 件	長期保証から 40 年後
9		1,754 Mbyte	8100 件	
10		1,949 Mbyte	9000 件	長期保証から 50 年後

セキュア保管方式の登録データは、ダミーTS の検証により登録されたデータであり、対象文書は一律 200KB である。

表 3-12よりセキュア保管方式で登録数が多い環境で利用する場合は、大容量のストレージが必要となる、ことが分かる。

再タイムスタンプ方式とセキュア保管方式をデータサイズの観点から見た場合の比較を以下表 3-13に示す。

表 3-13 データサイズから見た各方式の比較

No.	項目	再タイムスタンプ方式	セキュア保管方式
1	タイムスタンプのファイルサイズ	△	○
		再タイムスタンプの個数によりファイルサイズが変化する。 (3.6 Kbyte～168.8 Kbyte)	タイムスタンプ自体のファイルサイズの変化はない。 (3.6 Kbyte)
2	サーバへの登録データのファイルサイズ	○	△
		サーバへ登録するファイルはない。 (0Byte)	登録数に応じたストレージ(*7)の容量が必要になる。 (目安：9000 件で 1,949 Mbyte)

(*7) オンラインでアクセス可能な大容量ストレージ

なお、タイムスタンプのファイルサイズはクライアントが留意する項目であり、サーバへの登録データのファイルサイズはサーバが留意する項目である。

2. 全体評価結果

各方式にはそれぞれ長所・短所が存在する。各方式の特徴と、その特徴を活かせる適用データの纏めを以下表 3-14に示す。

表 3-14 全体評価結果

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。
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。	・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。
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。

なお、性能に関しては、機器のスペック向上などによって、改善が見込める為、今回は比較対象から外した。

第4章 考察

1. 実運用に向けた考察

1-1 利便性を考慮した考察

ここでは、実証実験を通じて浮上した課題に対する実運用を想定した対策に関して、考察する。

1-1-1 再タイムスタンプ方式

(1) クライアント運用負荷の軽減

今回の実験では、タイムスタンプ有効期間 或いは 再タイムスタンプの有効期間を、クライアント端末で手動確認し、必要であれば長期保証データの作成依頼を VA に送信した。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、実験の手順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。

(2) 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。

1-1-2 セキュア保管方式

(1) 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。その場合の運用として、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。

1-2 技術的な課題に係わる考察

ここでは、再タイムスタンプ方式、及びセキュア保管方式による長期保証に関する技術的な課題について考察する。

1-2-1 再タイムスタンプ方式

(1) 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

再タイムスタンプ方式により長期保証されたタイムスタンプの非署名属性の中には、検証時に使用されたトラストアンカ証明書が含まれている。また、繰り返し適用される再タイムスタンプの非署名属性の中にも、この再タイムスタンプ検証時に使用されたトラストアンカ証明書が格納されている。再タイムスタンプ検証により、これらのトラストアンカ証明書の存在時刻と非改ざん性を確認することが出来るが、そのデータ自体の信頼性を確認することは出来ない。何故ならば、その当時に、信頼の出来る CA が発行したトラストアンカ証明書だったのかどうか？　また、そのトラストアンカ証明書は有効だったのかどうか？など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いないからである。

今回の実験では、信頼された VA だけが長期保証されたタイムスタンプを作成するという前提が成り立つため、検証情報の中に含まれるトラストアンカ証明書の信頼性は別途確認されたものとしている。ところが、再タイムスタンプ方式による長期保証されたタイムスタンプを誰でも作れるような状況が現れた場合は、長期保証されたタイムスタンプを検証するときに、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ことが必要となる。

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。そのためには、VA は、検証に使用したトラストアンカ証明書や CA が発行した歴代のトラストアンカ証明書、及び、その失効有無に関する情報を全てセキュアに保管することが必要になると思われる。具体的な検討は今後の課題である。

(2) 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。この Grace Period のため、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。よって、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 は、CA の運用規程に依存したものであり、汎用的に定義できるものではない。そのため、今回の実験では、この Grace Period を踏まえた検証は実施していない。Grace Period を踏まえた検証方法に関しては、今後の課題である。

(3) 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。例えば、タイムスタンプトークンに含まれるタイムスタンプ対象データのハッシュ値に関わるハッシュ関数が脆弱化（例：第 2 原像困難性の脆弱化）した場合、悪意者は、本来のタイムスタンプ対象データとは異なる別のデータに対して同じタイムスタンプトークンが適用されたと見せかけることが可能である。よって、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。

現時点では、過去に使用されたものも含めて、暗号アルゴリズムの脆弱性を客観的に評価し、いつの時点で脆弱化したのか？　また、どのようなアプリケーションでは影響があるのか？などの情報を公にしている機関は存在しない。そのため、今回の実験では、暗号アルゴリズムの脆弱性評価を踏まえた検証は行っていない。今後の課題と認識している。

1-2-2 セキュア保管方式

(1) 署名履歴のトラストアンカの公開

VA は、信頼される第三者機関（TTP）である。そのため、今回の実験では、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（widely-witnessed）ことは行っていない。

しかし、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、この公開運用は重要である。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。例えば、新聞や国立国会図書館で保管される刊行物にトラストアンカに関わる情報（トラストアンカデータの BASE64 値、など）を掲載するこ

とが考えられる。

(2) 署名履歴の整合性検証の性能

VA は、長期保証されたタイムスタンプを検証するとき、署名履歴に含まれるトラストアンカとなる最新のヒステリシス署名データから検証対象のタイムスタンプに関わるヒステリシス署名データまでの整合性をハッシュ関数により検査する。長期に亘って VA を運用する場合、辿るべき署名データの数が膨大なものになる可能性がある。そのため、VA の機器のスペックが低い場合、この署名履歴の整合性検査に膨大な時間がかかり、リアルタイム性を確保した検証サービスを実行することは困難になることが予想される。

この問題を解決するためには、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。

(3) 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。例えば、過去に使用されたハッシュ関数に第 2 原像困難性の脆弱化が指摘された場合は、署名履歴の該当箇所の連鎖構造に対する信頼性が乏しくなる。

今回の実験では、このような状況は想定せずに実験を行ったが、実運用では、何らかの対策が必要になると思われる。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。

第5章 終わりに

今回の実証実験では、「再タイムスタンプ方式」と「セキュア保管方式」の比較という観点から、実測・検討・評価を実施した。本観点からも、「第 4 章 考察」で挙げた課題を中心として、更なる検討を進めていく必要がある。

今回の実証実験を契機として、長期保証の実用化に向けて更なる議論を実施していく予定である。

以上