タイムスタンプ・プラットフォーム技術の研究開発
Research and Development of Time-Stamping Platform Techniques

研究代表者　鳥山　裕史　独立行政法人　情報通信研究機構

研究期間　　平成 15 年度～平成 17 年度

【Abstract】

This research aims to establish time-stamping platform technology to provide accurate and secure time stamps using Japan Standard Time.

With this technology, electronic commerce and administrative procedures on the computer networks can be done more safely.

We have researched and developed (1) technology for highly accurate network time-transfer, (2) technology for highly trustworthy time-stamping, and (3) technology of high-speed time-stamping.

After confirming the efficiency evaluating these individual subfunctions, we developed the "Time-Stamping Platform system" to operate them jointly. The total performance of the platform was evaluated using some practical applications.

We experimented on the long-term security of the time stamp token using two different methods, and compared the methods' features.

We confirmed that the time-stamping platform system meets our security guidelines.

1　研究体制

○　**研究代表者**　　鳥山　裕史（独立行政法人情報通信研究機構
電磁波計測部門ﾀｲﾑｱﾌﾟﾘｹｰｼｮﾝｸﾞﾙｰﾌﾟ　ｸﾞﾙｰﾌﾟﾘｰﾀﾞ）

○　**研究分担者**　　システム開発担当　岩間　司　（独立行政法人情報通信研究機構
電磁波計測部門ﾀｲﾑｱﾌﾟﾘｹｰｼｮﾝｸﾞﾙｰﾌﾟ　主任研究員）
セキュリティ担当　谷川　嘉伸（独立行政法人情報通信研究機構
電磁波計測部門ﾀｲﾑｱﾌﾟﾘｹｰｼｮﾝｸﾞﾙｰﾌﾟ　招聘専門員）

○　**研究期間**　　平成 15 年度～平成 17 年度

○　**研究予算**　　総額　494 百万円

（内訳）

平成 15 年度	平成 16 年度	平成 17 年度
249 百万円	153 百万円	92 百万円

2　研究課題の目的および意義

高度情報通信社会の進展に伴い、ネットワーク上で行われた電子商取引や各種行政手続等の時刻を安全かつ正確に把握することや、その原本性を第三者に証明することが必要になってきており、今後、様々な場面で取り扱われる電子情報の信頼性、正確性を確保することがますます重要となる。「e-Japan 重点計画」においては、行政の情報の電子的提供、手続きの電子化等を通じ、電子情報を紙情報と同等に扱う行

政を実現することが目標とされている。

このため、安心して利用できる高度情報通信ネットワーク社会の実現に資することを目標に、日本標準時を利用して正確かつセキュリティの高いタイムスタンプを付与することができる「タイムスタンプ・プラットフォーム技術」を確立することを本研究開発の目的とする。

「e-Japan2002 プログラム」では、高度情報通信ネットワークの安全性及び信頼性の確保の重要性が指摘されており、本研究開発はこれらの目標、指摘に対応するものである。また、総合科学技術会議の「平成 15 年度の科学技術に関する予算、人材等の資源配分の方針」において、重点 4 分野の一つである情報通信分野において、情報通信システムの安全性・信頼性確保の必要性が特に言及されているが、この安全性・信頼性確保に貢献する研究開発である。

3　研究成果

本研究開発では、「タイムスタンプ・プラットフォーム技術」を確立するために以下に示す 3 つの技術課題を掲げシステム開発を実施した。

- 高精度時刻配信技術の研究開発
- 高信頼時刻認証技術の研究開発
- 高速時刻認証技術の研究開発

本システム開発では単独の要素技術ではなく、各機能相互の連携が重要であるため、図 3.1.1 に示すタイムスタンプ・プラットフォームシステムを開発して機能確認を行った。これらについて３．１から３．４に成果を示す。

また昨今の情報セキュリティに関する様々な問題に対して開発したシステムの安全性を評価するため、

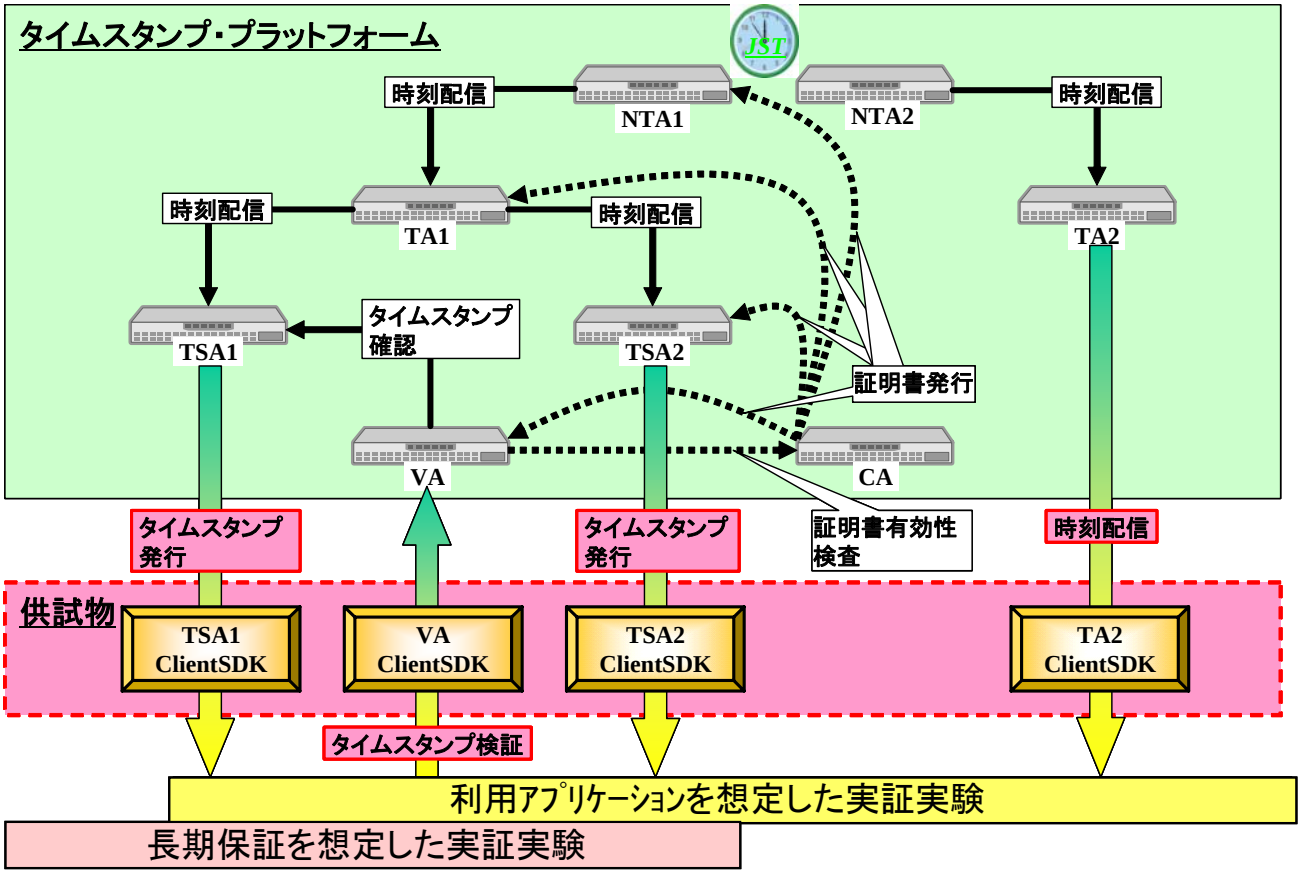

図 3.1.1　タイムスタンプ・プラットフォームシステム構成図

タイムスタンプ用のセキュリティ・ガイドラインを制定し、タイムスタンプ・プラットフォームシステム全体のセキュリティ評価を実施した。この結果について３．４．１に示す。

さらに実際の利用場面を想定した動作確認、及び今後必要となる長期保証に関する実証実験を実施して動作検証を行った。この結果について３．４．２に示す。

３．１　高精度時刻情報配信技術の研究開発

インターネット上での時刻配信技術の課題として、通信トラフィック量の輻輳による「遅延」やトラフィック量の変動による「遅延の揺らぎ」が時刻精度を劣化させ、精度の高い時刻情報の配信・同期が困難であることがあげられる。このため、基盤としての時刻配信の信頼性を高めるため、遠隔地における時刻同期精度が日本標準時に対してミリ秒以内となるような技術を開発する。また、３．２の高信頼時刻認証技術の研究開発で策定された時刻認証プロトコルを用いてNTA*1/TA*2/TSA*3間で数ミリ秒以内の精度を実現する。

*1　National Time Authority ····· 国家時刻標準機関
*2　Time Authority ····· 標準時配信事業者
*3　Time Stamp Authority ····· 時刻認証事業者

タイムスタンプ・プラットフォームシステムでは、３．２の高信頼時刻認証技術の研究開発で策定された時刻認証プロトコルの違いにより、NTA1、TA1、TSA1 及び TSA2 からなる「認証連鎖方式」と NTA2、TA2 及び NTP サーバからなる「時刻リンク方式」の 2 種類の時刻配信・認証方式がある。相手方認証や監査の方式は異なるが、どちらの方式においても時刻配信プロトコルには NTP（Network Time Protocol）を使用している。

認証連鎖方式のシステムでは、NTA1 を東京都小金井市、TA1 及び TSA2 を千葉県千葉市（幕張）、TSA1 を中央区築地に配置してそれぞれの局間を ISDN64kbps で接続した。NTA1/TA1 間の時刻配信において 1 週間の測定期間内で時刻誤差が±1 ミリ秒を超えた割合は約 4%あったが、散発的な発生で使用機器内の割り込み処理によるものと考えられる。また NTA1 から TSA1、TSA2 までの時刻配信において±10 ミリ秒を超えることはなかった。

時刻リンク方式のシステムでは、NTA2 及び TA2 を東京都小金井市、NTP サーバを港区新橋に設置して局間を 10Mbps で上り下り対称なインターネット回線で接続した。こちらはインターネット回線を用いているため、トラヒックの影響を受けるが、ほぼ 1 ミリ秒以内を達成している。また、ローカルに直接 10Mbps で接続した場合でも 1 ミリ秒を超える場合があり、主として割り込み処理によるものであった。また NTA2 から NTP サーバ間の時刻誤差はやはり±10 ミリ秒を超えることはなかった。

以上の結果から、当初の目標は達成しているものと考えられる。更に、時刻精度劣化の要因は、測定結果からネットワーク上の不要なトラヒックによるものと装置内での他のプログラムによる割り込み処理が主たる要因であると考えられる。これらの影響を排除することで時刻精度を向上させることが可能である。

これら精度の劣化に対し、ネットワークの割り込みを抑える方法としては ISDN やダークファイバなどの専用線を利用することが有効である。また装置内の割り込み処理を軽減する方法として究極的には NTP をハードウエアで実現することであるが、今回のタイムスタンプ・プラットフォームシステムの場合においては、不用なプログラムを停止させることで割り込み処理による精度劣化を軽減できた。不用なプログラムを停止させることはセキュリティの面からも有効な手段である。

しかし、タイムスタンプ・プラットフォームシステム上では３．４で報告するセキュリティ評価の観点から定期的にウイルスチェックのためのディスクスキャンを実施しており、これが最大の精度劣化の要因となっていることがわかった。これに対しては、それぞれの装置でディスクスキャンを実施している間は NTP を停止させる等の処置を行う必要がある。

３．２　高信頼時刻認証技術の研究開発

改ざんされることなく NTA/TA/TSA 間で、認証連鎖を維持して時刻を配信する技術を確立し、理論的な安全性の評価が可能である時刻認証プロトコルを策定する。かつ、それを埋め込んで生成されるタイムスタンプトークンの妥当性とその時刻情報の信頼性を、エンドユーザが確認可能とするためのタイムスタンプトークン検証技術を開発する。また、NTA で生成された時刻であることを証明可能とするための証跡を提供する技術をあわせて確立する。

ここでは高信頼時刻認証技術のうちタイムスタンプ自身の正確性、非改竄性についての成果を扱い、タイムスタンプ・プラットフォームシステムのシステムの安全性については３．４．１で言及する。

タイムスタンプ・プラットフォームシステムでは、時刻認証プロトコルの違いにより「認証連鎖方式」と「時刻リンク方式」の 2 種類の時刻配信・認証方式を採用した。

「認証連鎖方式」では TSA1 でリンク情報を用いるアーカイビング方式タイムスタンプを、TSA2 で PKI 方式タイムスタンプをそれぞれ発行している。PKI 方式タイムスタンプでは、各局における時刻情報を含んだ時刻監査証明書をタイムスタンプトークンに順次付与することにより、配信経路と時刻誤差を検証時に確認できる。また、アーカイビング方式タイムスタンプでは検証時に TSA 局の公開する時刻監査レポートを閲覧することにより、配信経路と時刻誤差を確認できる。

またこれらタイムスタンプの方式を意識せずにユーザがタイムスタンプ検証を行うことができる手段として、タイムスタンプ検証局（VA）を新設した。VAを用いることにより、上記のタイムスタンプの方式の差異に関わらずタイムスタンプ検証時に合わせて配信経路と時刻誤差を確認できる。合わせて、検証時にタイムスタンプの有効期限が迫っている場合は、有効期限を延長するために「再タイムスタンプによる長期保証方式」及び「セキュア保管型タイムスタンプ長期保証方式（長期使用を前提とした電子署名技術を利用した方式）」の 2 方式を実装してタイムスタンプの長期保証に対応できる仕様とした。長期保証に関する成果は３．４．２（４）にて報告する。

「時刻リンク方式」では、時刻認証に用いられる時刻認証子に時刻情報のほかに受信時の時刻誤差、生成機関情報、過去の時刻認証子ハッシュ等を含めて生成し、NTP パケット内に時刻認証子を含めて配信する。各局内では自身の局の生成する時刻認証子のハッシュと各局から送られてくる時刻認証子のハッシュを用いてハッシュリンクを生成する。このハッシュリンクは接続している各局からの時刻認証子も内包しているため、時刻認証子の改竄が行われた場合、改竄を検知することができる。

「時刻リンク方式」では NTP サーバ等のログに時刻認証子を埋め込むことができ、後日、時刻認証子に含まれている情報により、改竄検知のほか時刻誤差、生成機関情報、配信経路の情報を確認できる。

「認証連鎖方式」、「時刻リンク方式」とも、配信経路、時刻誤差などの NTA で生成された時刻であることを証明可能とするための技術が盛り込まれている。また、VA の新設により、タイムスタンプの方式の差異に関わらずタイムスタンプ検証が可能となり合わせて、検証時にタイムスタンプの有効期限が迫っている場合は、有効期限を延長する機能も有しておりユーザの利便性を高めたシステムを構築した。以上により、当初の到達目標を達成し、更に VA を新設することでユーザの利便性を高めたシステムを構築できた。

３．３　高速時刻認証技術の研究開発

大量なトランザクション要求に耐えられる高速タイムスタンプサーバーを開発する。長期保存にも利用可能とするため、短い時間での電子署名生成技術を確立し、より安全な鍵長で、高負荷時にも耐えられる処理能力を持つタイムスタンプ技術を開発する。具体的には 1024 ビット署名鍵を用いる場合には毎秒 500 スタンプ以上、タイムスタンプの安全性を高めるために 2048 ビットの署名鍵を用いる場合には毎秒 100 スタンプ以上の処理を可能とする。

タイムスタンプ・プラットフォームシステムでは、タイムスタンプ技術としてリンク情報を用いるアーカイビング方式タイムスタンプを発行する TSA1 と PKI 方式タイムスタンプを発行する TSA2 を開発した。

TSA1 では、大量のトランザクション処理のボトルネックとなっている部分の洗い出しを行った結果、サーバ内でプロセス間通信のオーバヘッドが大きな阻害要因となっていることがわかり、この部分の改善を実施したところ最大毎秒 70,000 件のタイムスタンプ処理が可能となった。しかし、３．４に基づいてハッシュ関数の２重化、HTTPS 通信の採用などのセキュリティ改善、システム信頼化のためにタイムスタンプ発行ごとの DB 書き込み処理などの信頼性重視の処理を行うと毎秒 80 件程度のタイムスタンプ処理件数となった。今回のセキュリティ改善及び信頼性重視の処理は安全性を重視したかなりオーバスペックな仕様となっており、かつ、安全性の処理については DB 装置の速度向上など速度改善の余地がある。

TSA2 では、大量のトランザクション処理のボトルネックとなっている部分の洗い出しを行った結果、HSM (Hardware Security Module) 内部での処理速度が速度向上の阻害要因となっていることがわかった。このため、HSM 内で行っていた処理のうち３．４のセキュリティ評価で問題のない部分を高速処理系で処理するようにアルゴリズムを改良したところ、最終的に 1024 ビット署名鍵を用いる場合には毎秒 130 スタンプ、タイムスタンプの安全性を高めるために 2048 ビットの署名鍵を用いる場合には毎秒 26 スタンプの処理が可能となった。さらに現在では HSM の処理性能が 4 倍以上まで向上しているため、現在市販されている HSM の性能で TSA2 の処理能力を換算すると、1024 ビット署名鍵を用いる場合には毎秒 500 スタンプ以上、タイムスタンプの安全性を高めるために 2048 ビットの署名鍵を用いる場合には毎秒 100 スタンプ以上の処理が可能となり目標性能を達成できる。さらに TSA2 では、最近報告されている SHA-1 の脆弱化（衝突困難性の特性に関わる脆弱化）の対策として、タイムスタンプクライアントから送信される電子データのメッセージダイジェストに SHA-512 を採用し、SHA-1 であるものを受け付けない仕様として安全性に配慮した設計となっている。

ここで取り扱うタイムスタンプの高速化と、３．２及び３．４に関連するシステムの安全性は裏腹な関係となる。必要とされるタイムスタンプの特性に応じて速度設計を行う必要がある。

３．４　その他の研究実績

３．４．１　タイムスタンプ・プラットフォームのセキュリティ評価

本研究開発は、高度情報通信ネットワークの安全性・信頼性確保に貢献するために時刻配信基盤・時刻認証基盤となるタイムスタンプ・プラットフォーム技術の確立を目指しており、構築する統合化プラットフォームシステム全体のセキュリティ要件を明らかにするとともに、本システムによって実現するタイムスタンプ付与・検証等に関するセキュリティ面の分析を行う。このため、タイムスタンプ・プラットフォームシステムに関する総合的なセキュリティ要件や必要となるセキュリティ対策等を実用性の観点から明らかにし、タイムスタンプ・プラットフォームシステムが提供するタイムスタンプに関し、セキュリティの観点からその妥当性について分析する。

セキュリティ評価に関する国際標準 ISO/IEC 15408 の考え方に基づいて、タイムスタンプ・プラットフォームシステムのセキュリティ評価を実施した。NICT が策定した『統合化プラットフォーム・セキュリティ評価ガイドライン』に従い、タイムスタンプ・プラットフォームシステムのサブシステム毎の評価対象（Target of Evaluation: TOE）を明確化し、その TOE に対してセキュリティ評価を実施した。セキュリティ評価における特記事項を以下に示す。

（１）暗号コンポーネント

タイムスタンプ・プラットフォームシステムでは、暗号技術を実装した暗号コンポーネントが含まれている。例えば、PKI 方式のタイムスタンプトークンを発行する TSA システムでは、タイムスタンプトークンの作成に際して、ハッシュ関数やデジタル署名技術が利用されている。本セキュリティ評価では、TOE に関する暗号コンポーネントを明確化した。そして、暗号技術そのものの安全性を評価するのではなく、「セキュリティ環境」の「組織のセキュリティポリシー」にて定められた「暗号技術の使用に関するセキュリティポリシーへの準拠性」への観点から評価した。

また、暗号技術の脆弱化に関する脅威も検討した。例えば、PKI 方式のタイムスタンプの有効期間（公開鍵証明書の有効期間）が満了する前に、タイムスタンプに使用された暗号技術の脆弱化を想定した脅威を想定し、セキュリティ評価を実施した。

その結果、すべての TOE において、暗号技術コンポーネント動作に関わる安全性に関しては、(1)TOE そのものが物理的・電磁波的に守られた領域に設置されること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、問題がないと思われる。また、最近報告されている SHA-1 の脆弱化（衝突困難性の特性に関わる脆弱化）の対策として、TOE は、タイムスタンプクライアントから送信される電子データのメッセージダイジェストが SHA-1 であるものを受け付けないという安全対策がとられていることを確認した。

一方、通信のプロトコルとして SSL、TLS、SNTP 等を使用しており、これらのプロトコル内では「電子政府推奨暗号リスト（平成 15 年 2 月 20 日、総務省、経済産業省）に記載されていない暗号が使用されている。

SSL/TLS に関しては、脆弱性が報告されている MD5 や SHA-1 が使用されているが、ハッシュ関数単独の使用ではなく、HMAC として使用されている。NIST の報告によれば、切迫した脅威として見なされているわけではない。しかしながら、SSL/TLS の仕様の維持管理を行っている IETF では、将来的な脅威を想定におき、MD5/SHA-1 依存の仕様を変更する活動が行われている。SSL/TLS を利用するシステムは、このような TLS/SSL 仕様改定の動向を踏まえ、最新の TLS/SSL の実装コンポーネントに交換可能なメカニズムを組み込むことが重要である。

SNTP に関しては、HMAC として脆弱性が報告されている MD5 を使用しているものがあった。これも SSL/TLS と同様、切迫した脅威として見なす必要性はないが、今後の暗号解読技術の進展などを踏まえ、対策を講じておくことが重要である。例えば、SNTP の前提となるネットワーク層や物理層におけるセキュリティ対策として専用線を用いる、または、SNTP の仕様を拡張し、MD5 よりも安全なハッシュ関数に交換できる仕組みを設けることが考えられる。特に、後者の方法を選択した場合は、SNTP の仕様の維持管理をおこなっている IETF との協調作業を視野に置く必要がある。

（２）時刻情報

タイムスタンプ・プラットフォームシステムでは、時刻情報が重要である。例えば、PKI 方式のタイムスタンプトークンを発行する TSA システムが発行するタイムスタンプトークンには、タイムスタンプ作成時刻を示す時刻情報が含まれている。この時刻情報は、TSA システムの資産である「時刻情報」に基づいて作成されている。本セキュリティ評価では、TOE に関する時刻情報を明確化し、その情報に対する脅威及び対策を検討した。

その結果、すべての TOE において、TOE が参照する時刻情報の安全性を確認した。TOE が参照する時刻情報は、(1)信頼のできる時刻ソース（NTP サーバ）と安全な通信路上で定期的に同期していること、(2)不必要/不正なソフトウェアは導入しない、(3)内部不正は存在しない、などの前提により、安全性が確保されていると思われる。

（３）内部不正

タイムスタンプ・プラットフォームシステムは、信頼される管理者・運用者によって運用されることを想定している。そのため、内部不正の可能性は限りなくゼロに近い。このような考えに基づき、基本的に内部不正は存在しないという前提を置き、セキュリティ評価を実施した。

なお、可能性としては限りなく小さいが、内部不正を考慮したセキュリティ評価も重要であるとの考えから、オプション的なセキュリティ評価作業として、内部不正を踏まえた脅威の検討も行った。この場合、複数の悪意者の結託は考慮せず、単独犯による内部不正を想定した。

その結果、内部不正に対する TOE の対策機能は、未実装のものが多かった。内部不正に対する対策としては、(1)複数人の操作による相互牽制、(2)教育/罰則の強化、などが考えられる。

（４）将来的にタイムスタンプが検証できなくなる脅威

タイムスタンプは、署名文書や電子文書の長期保証に有効な技術であると言われている。ところが、将来的にタイムスタンプが検証できない状況が生じた場合、長期保証の役割を果たせなくなる可能性がある。本セキュリティ評価では、このような状況を別途、考察し、脅威及びその対策を検討した。具体的には、タイムスタンプサービス利用者側のセキュリティ環境を想定し、セキュリティ評価を行った。

その結果、TOE は、暗号技術が使用された「時刻監査証明書」、「時刻認証子」、「タイムスタンプ（タイムスタンプトークン）」、「公開鍵証明書」、「公開鍵証明書失効リスト」等を作成・配付・蓄積する。時間の経過とともに、使用された暗号技術が脆弱化することが想定され、過去に作成した「時刻監査証明書」、「時刻認証子」、「タイムスタンプ（タイムスタンプトークン）」、「公開鍵証明書」、「公開鍵証明書失効リスト」等の信頼性が失われる可能性がある。このような脅威に関しては、「時刻監査証明書」、「時刻認証子」、「公開鍵証明書」、「公開鍵証明書失効リスト」の所有者による長期保証の必要性があることが明らかになった。また、本 TOE を使用したタイムスタンプ事業者及び関連するエンティティ・装置な

どの存在が仮定できなくなる可能性もある。このような状況を踏まえ、脅威を洗い出し、対策を明確化した。

３．４．２　タイムスタンプ・プラットフォーム実証実験

タイムスタンプ・プラットフォームシステムを用いた実証実験において、様々な分野で利用されるアプリケーションを適用し、利用面から観た実用性に関する評価と技術・運用等の課題を明らかとする。さらに、タイムスタンプ・プラットフォームシステムを用いた実証実験において、既に付与されたタイムスタンプの有効期間が切れる前あるいは脆弱化する前に当該タイムスタンプの効力を延長保証する技術・運用面の方策について検証を行い、課題を明らかにする。

（１）電子契約実証実験

タイムスタンプ・プラットフォームに電子契約システムを接続し、プラットフォームにより提供される機能や接続した場合の運用性の評価を実施することにより、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した。

その結果、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。また、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。PKI 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。更に、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、PKI 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）ログサーバ実証実験

タイムスタンプ・プラットフォームから iDC 内の機器へ時刻情報を配信することにより、iDC 内に設置した、時刻リンク方式による時刻送受信機能を組み込んだ NTP サーバおよびログサーバに正確な時刻供給を行い精度の高いシステム構築の可能性について検討した。

その結果、インターネットを介してログサーバに高信頼度な時刻情報を配信し、ログサーバにおいて受信した高信頼度な時刻情報を付与したログの生成・保存機能が正常に動作することについて確認できた。また、ログに記載された高信頼度な時刻情報のトレーサビリティを検証する機能が正常に動作することについて確認できた。上記の動作確認によって、第三者に対しログサーバ内に保存されたログの生成時刻の証明を可能とした。また、高信頼度な時刻情報の生成・管理を行っている NTP サーバに対して、インターネットを介した時刻監査を行う機能が正常に動作することについて確認できた。更に、高信頼度な時刻情報の配信プロトコルには、改良した NTP を使用した。改良した NTP は、一般に使用されている NTP のパケットに高信頼度な時刻情報を埋め込んでいるが、iDC 内の NTP サーバと日本標準時との時刻誤差がほぼ数ミリ秒以内であったことを確認できた。

（３）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を用いた長期保証実証実験

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、実施した。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した。デジタル署名及びタイムスタンプ効力の長期保証に係る課題については、長期署名フォーマットをベースとして、タイムビジネス推進協議会より公開されている「タイムスタンプ長期保証ガイドライン」におけるリンク方式タイムスタンプ長期保証の実現例に沿った長期保証機能を実装し、タイムスタンプの再付与による効力延長を可能とした。

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

（４）VA による長期保証実証実験

タイムスタンプ・プラットフォームを用いて、VA によるタイムスタンプ検証時に①「タイムスタンプによる長期保証方式」（以下、再タイムスタンプ方式）、②「セキュア保管型タイムスタンプ長期保証方式（長期使用を前提とした電子署名技術を利用した方式）」（以下、セキュア保管方式）、の 2 方式の長期保証を行った場合において結果の比較・評価を実施することにより、現状の課題を解決した仕組みの実現性を評価した。

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

本実証実験における性能評価及び運用評価、また、机上検討を踏まえて、再タイムスタンプ方式及びセキュア保管方式の長所・短所の整理を表３．４．２．１に行った。

表3．4．2．1　再タイムスタンプ方式及びセキュア保管方式の長所･短所

№	項目	再タイムスタンプ方式	セキュア保管方式
1	長所	・ポータビリティ性あり 　VA 利用者以外が受け取っても検証することが可能。 ・相互運用性あり 　仕様を公開しそれを実現した他社製品でも、検証が可能。	・クライアント運用負荷小 　一度登録すれば、その後永続的に検証することが可能であり、負荷が少ない。 ・データサイズは不変 　永続的に同一のデータを利用できるので、データサイズは不変。 ・長期保証データ登録処理時間(*) 既存のデータ登録数などに影響を受けず、ほぼ一律の処理時間で登録が可能。

2	短所	・クライアントの運用負荷大 タイムスタンプの有効期間管理、長期保証の要求、を定期的に実施する必要があり、運用負荷が大きい。 ・データサイズの増大 再タイムスタンプの付与により、タイムスタンプのデータサイズが増大してゆく。 ・コストが発生 再タイムスタンプを付与することによる費用が発生する。 ・長期保証データ作成処理時間(*) 再タイムスタンプの数に応じて、検証処理時間が変動し長期保証データの作成処理時間も変動する。 ・長期保証データ検証処理時間(*) 再タイムスタンプの数に応じて、検証処理時間が変動する。	・ポータビリティ性なし 長期保証の登録を行った VA でのみ検証が可能。 ・相互運用性なし ヒステリシス署名技術は、日立製作所独自技術のため現状相互運用は難しい。 ・サーバの運用負荷大 登録データ量によって、ストレージ管理などの運用が発生する。 ・長期保証データ検証処理時間(*) 既存のデータ登録数に応じて、検証処理時間が変動する。
3	適用データ	他組織間で長期に亘ってやり取りする流通データなど。	組織内で閉じて利用するデータなど。

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

4　研究成果の更なる展開に向けて

・今後の研究成果の展開

本研究開発で開発した NTA から TSA まですべてネットワークを用いた 2 種類の時刻配信・認証方式では、配信経路、時刻誤差などの NTA で生成された時刻であることを証明可能とするための技術が盛り込まれており、インターネット上での時刻配信と各システムの時刻証明に有効な手法である。特に、近年情報漏えいが問題となっており、情報漏えいが発生した場合には、機密情報に「いつ」誰がアクセスしたかを確認し、立証する必要がある。例えば時刻リンク方式をログサーバに適応することより、ログの生成時刻の証明が可能となり、記録されたアクセスログから「いつ」アクセスしたか確認可能となり、情報漏えいの原因特定の手助けとなる。今後は、これらの機能を利用した様々な製品開発が考えられる。

また、本研究開発で使用したタイムスタンプ方式は、財団法人日本データ通信協会の認定制度である「タイムビジネス信頼・安心認定制度」に準拠しており、特に本研究開発で開発した「リンク情報を用いるアーカイビング方式タイムスタンプ」をもとにして「アーカイビング方式」の認定基準が制定されるなど、実用化に向けたフィードバックがすでに行われている。このため、今後、国内のタイムビジネス製品および TA・TSA サービスにおいて、本研究の成果の組み込みや、本研究によって明らかになった課題を解消するなど、様々な形で利用されていくと考えられる。

さらに今回実施したセキュリティ評価であるが、国内のタイムスタンプ関連システムとしてははじめての試みである。今回の評価結果を踏まえて、今後のセキュリティ評価の指針となるよう「セキュリティ評価ガイドライン」の実用化に向けた改定を「タイムビジネス推進協議会」等の関係団体とともに整備していきたい。

しかしタイムスタンプサービスはすでに商用サービス（タイムビジネス）の段階に入っているが、現在のところ、重要な情報を扱う特定用途での利用がほとんどである。タイムスタンプによる安全な電子化の恩恵を最大限とするには、今後、一般の利用者が気軽に、低コストで利用できる環境を整備するこ

とが必要であると考えている。このような環境実現に向けて、パソコンの基本ソフト、ファイルサーバ、メールサーバ等にタイムスタンプ機能を組み込む技術、大量のタイムスタンプ需要をさばくための高性能サーバの開発、クライアント側機器でタイムスタンプを付与する技術等についての研究開発実施を検討している。

・予測される波及効果

本研究成果を利用したタイムビジネス製品および TA・TSA サービスの利用することで、これまでより高度に電子データの真実性を確保することが可能となる。本研究成果は、安心・安全に電子データの流通が行われる社会の実現に寄与するとともに、日本が情報化大国として海外の模範となるための基盤になると考える。

５　査読付き誌上発表リスト

[1] 町澤朗彦、鳥山裕史、岩間司、金子明弘、“通過型高精度 UDP タイムスタンパの開発“、電子情報通信学会論文誌Ｂ、(2005 年 10 月)

６　その他の誌上発表リスト

[4] 鳥山裕史、町澤朗彦、岩間司、金子明弘、“高速インターネット環境におけるパケット遅延時間の精密測定”、電子情報通信学会インターネットアーキテクチャ研究会（大阪大学中ノ島センター）(2005 年 1 月 19 日)

[5] 町澤朗彦、鳥山裕史、岩間司、金子明弘、“通過型高精度 UDP タイムスタンパの開発”、電子情報通信学会インターネットアーキテクチャ研究会（大阪大学中ノ島センター）(2005 年 1 月 19 日)

[6] 谷川嘉伸、本多義則、小黒博昭、高村昌興、“DVCS を拡張した複数方式タイムスタンプ検証サーバの開発”、第 28 回コンピュータセキュリティ研究会(CSEC)（大阪大学吹田キャンパス）(2005 年 3 月 22 日～23 日)

[7]鳥山裕史・町澤朗彦・岩間司・金子明弘、”ハードウェア SNTP サーバの開発”、電子情報通信学会コミュニケーションクオリティ研究会(ＡＴＲ)（2005 年 4 月）)

[14] 岩間司、金子明弘、町澤朗彦、鳥山裕史、“インターネット環境下における高精度時刻比較技術”、電子情報通信学会インターネットアーキテクチャ研究会（東京大学）(2005 年 10 月 28 日)

７　口頭発表リスト

[2] 岩間司、金子明弘、鳥山裕史、“時刻認証基盤技術実験装置の開発”、2004 年電子情報通信学会総合大会（東京工業大学大岡山キャンパス）(2004 年 3 月 22 日～25 日)

[8] 岩間司、鳥山裕史、橋川善之、雨宮隆征、久保寺範和、谷川嘉伸、“時刻認証基盤技術実験装置－（１）統合化プロトタイプシステムー”、電子情報通信学会２００５年ソサエティ大会（北海道大学）(2005 年 9 月 20 日～23 日)

[9] 久保寺範和、島成佳、石崎健太郎、岩間司、鳥山裕史、“時刻認証基盤技術実験装置－（２）配信時刻高精度高信頼化サブシステム：時刻リンク方式時刻配信ー”、電子情報通信学会２００５年ソサエティ大会（北海道大学）(2005 年 9 月 20 日～23 日)

[10] 小黒博昭、橋川善之、谷川嘉伸、田川豊、岩間司、鳥山裕史、“時刻認証基盤技術実験装置－（３）複数方式タイムスタンプ検証サブシステム：時刻トレーサビリティー”、電子情報通信学会２００５年ソサエティ大会（北海道大学）(2005 年 9 月 20 日～23 日)

[11] 谷川嘉伸、田川豊、岩間司、鳥山裕史、“時刻認証基盤技術実験装置－（４）複数方式タイムスタンプ検証サブシステム：タイムスタンプ長期保証ー”、電子情報通信学会２００５年ソサエティ大会（北海道大学）(2005 年 9 月 20 日～23 日)

[12] 坂本弘章、西尾秀一、橋川善之、堅田昌弘、岩間司、鳥山裕史、“時刻認証基盤技術実験装置－（５）高速・高セキュリティタイムスタンプ付与・検証サブシステム１：タイムスタンプ付与の高速化ー”、電子情報通信学会２００５年ソサエティ大会（北海道大学）(2005 年 9 月 20 日～23 日)

[13] 雨宮隆征、上畑正和、岩間司、鳥山裕史、“時刻認証基盤技術実験装置－（６）高速・高セキュリティタイムスタンプ付与・検証サブシステム２：タイムスタンプ付与の高速化ー”、電子情報通信学会２００５年ソサエティ大会（北海道大学）(2005 年 9 月 20 日～23 日)

[15] 岩間司、谷川嘉伸、町澤朗彦、鳥山裕史、“安全安心なタイムスタンプに関する研究開発”、情報通信研究機構第 4 回研究発表会（マイドームおおさか）（2005 年 11 月 30 日）

８　取得特許リスト

９　国際標準提案リスト

１０　参加国際標準会議リスト

１１　受賞リスト

１２　報道発表リスト

[1]“日本標準時」タイムスタンプ・プラットフォーム実証実験の開始－電子商取引や電子申請の安全確保に向けて－ ”、日経産業新聞等、2005 年 12 月 14 日

[2]“世界最高性能のインターネット用時刻同期サーバによる日本標準時配信の開始 ”、日経産業新聞等、2006 年 6 月 12 日

研究開発による成果数

	平成 15 年度	平成 16 年度	平成 17 年度	平成 18 年度	合計
査読付き誌上発表数	件（　件）	件（　件）	1 件（　件）	件（　件）	1 件（　件）
その他の誌上発表数	件（　件）	3 件（　件）	2 件（　件）	件（　件）	5 件（　件）
口　頭　発　表　数	1 件（　件）	件（　件）	7 件（　件）	件（　件）	8 件（　件）
関 連 特 許 出 願 数	2 件（　件）	2 件（1 件）	6 件（　件）	件（　件）	10 件（1 件）
関 連 特 許 取 得 数	件（　件）	件（　件）	件（　件）	件（　件）	件（　件）
国 際 標 準 提 案 数	件（　件）	件（　件）	件（　件）	件（　件）	件（　件）
国 際 標 準 獲 得 数	件（　件）	件（　件）	件（　件）	件（　件）	件（　件）
受　　賞　　数	件（　件）	件（　件）	件（　件）	件（　件）	件（　件）
報　道　発　表　数	件（　件）	件（　件）	1 件（　件）	1 件（　件）	2 件（　件）

注１：　（括弧）内は、海外分を再掲。

注２：　「査読付き誌上発表数」には、論文誌や学会誌等、査読のある出版物に掲載された論文等を計上する。学会の大会や研究会、国際会議等の講演資料集、アブストラクト集、ダイジェスト集等、口頭発表のための資料集に掲載された論文等は、下記「口頭発表数」に分類する。

注３：　「その他の誌上発表数」には、専門誌、業界誌、機関誌等、査読のない出版物に掲載された記事等を計上する。

注４：　関連特許数は、本研究開発を実施する上で活用した特許及び本研究成果を応用し出願した特許を計上する。

（参考）

関連特許リスト

[1]（株）日立製作所、“タイムスタンプ情報検証方法”、日本、2003 年 6 月.30 日（公開番号：2005-020651）
[2] セイコーインスツル(株)、“認証用鍵の更新システム、認証用鍵の更新方法および認証用鍵の更新プログラム”、日本、2004 年 3 月 26 日
[3]（株）日立製作所、“タイムスタンプサービスシステム”、日本、2004 年 10 月 7 日
[4] セイコーインスツル(株)、“時刻証明サーバ、基準時刻配信サーバ、時刻証明方法、基準時刻配信方法、時刻証明プログラム、及び通信プロトコルプログラム”、日本、2005 年 4 月 11 日
[5] セイコーインスツル(株)、“情報処理装置、時刻情報処理装置、情報処理方法、及び時刻情報処理方法”、日本、2005 年 9 月 5 日
[6]（株）日立製作所、“タイムスタンプサービスシステム”、中国・韓国、2005 年 1 月 14 日
[7]（株）日立製作所、“タイムスタンプサービスシステム”、日本、2005 年 9 月 16 日
[8]（株）NTT データ、“タイムスタンプ情報検証支援サーバ”、日本、2005 年 10 月 31 日
[9]（株）NTT データ、“情報処理装置、タイムスタンプトークンの発行方法、及び、コンピュータプログラム”、日本、2006 年 3 月２４日
[10]（株）NTT データ、“時刻証明装置及びプログラム“、日本、2006 年 3 月 31 日