＜基本計画＞

タイムスタンプ・プラットフォーム技術の研究開発

１．目的

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。

このため、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」を確立し、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。

２．政策的位置付け

「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おり、「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、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．目標

日本標準時を利用して、有効かつセキュリティの高いタイムスタンプを高速に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。

４．研究開発内容

(1) 高精度時刻情報配信技術の研究開発

① 概要

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、ネットワーク環境が不安定であっても、配信時刻の十分な精度と信頼性を保証するための技術を開発する。なお、研究開発の過程および最終段階においては、性能評価のための実証実験を行う。

② 技術課題及び到達目標

（技術課題）

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の誤差を日本標準時と高精度に同期する技術を開発する。通信回線の遅延に影響されない技術的手段と、ネットワークの遅延計測で得られた誤差を、補正情報として正確にフィードバックする技術的手段および運用的手段の確立を行う。

（到達目標）

日本標準時に対して、遠隔地の時刻同期精度がミリ秒以内の精度を実現する。

(2) 高信頼時刻認証技術の研究開発

① 概要

時刻情報に上位の配信元の認証情報を埋込むことにより、「改ざん・なりすましが行われていないこと」を検証可能な時刻配信基盤技術を確立する。また、タイムスタンプを付与された利用者から直接、または時刻認証事業者を通して、そのタイムスタンプが有効であることを後日確認することが可能な、タイムスタンプ検証技術もあわせて確立する。なお、研究開発の過程および最終段階においては、性能評価のための実証実験を行う。

② 技術課題及び到達目標

（技術課題）

改ざんされることなく NTA からユーザーまで、認証連鎖を維持して時刻を配信し、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。

（到達目標）

NTA/TA/TSA 間で、日本標準時を改ざんされることなく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。NTAからユーザーまで数ミリ秒以内の精度で実現する。

(3) 高速時刻認証技術の研究開発

① 概要

長期間有効なタイムスタンプを実現し、かつ、タイムスタンプ付与要求の増加に対応するため、より安全な鍵長で高負荷時にも十分な処理能力を持つスタンプ技術を開発する。なお、研究開発の過程および最終段階においては、性能評価のための実証実験を行う。

② 技術課題及び到達目標

（技術課題）

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。

（到達目標）

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。

５．実施期間

平成１５年度から平成１７年度までの３年間

６．その他

特になし。