平成１６年度　継続評価書

研究開発課題	タイムスタンプ・プラットフォーム技術の研究開発	研究開発期間	Ｈ１５～Ｈ１７
研究機関	独立行政法人　情報通信研究機構	代表研究責任者	鳥山　裕史

①　平成１６年度研究開発の目標達成（見込み）状況

評価	コメント
C	平成１６年度について、表面的に見れば良い成果が出ていると読むことも可能である。また、平成１５年度の中間評価を踏まえて、改善を試み、十分な努力の跡が見られる点は高く評価したい。しかしながら、③でコメントするように、平成１６年度の結果が、最終目的に対して成果をあげているかどうか正確に判断し難い。この点については、計画を実施する側だけでなく計画を認めた側にも責任がある。 なお、安全性評価手法に関する研究において、タイムスタンプシステム・セキュリティシミュレータを構築する部分は、本研究開発の基本計画の目的からみて、全く不十分な結果しか見込めない状況であることがはっきりした。ただし、安全性評価手法そのものの研究自体は重要性が高く必要であることに変わりはない。

②　平成１６年度研究資金使用状況

評価	コメント
C	「効率的」の意味が、予算額と執行予定額の差が小さいということであるとすれば、効率的であったといえよう。しかし、基本計画の目的を達成するものとして行われた具体的な成果に見合う投入資金であると考えれば、必ずしも効率的であるとは言い難い。③でもコメントしているが、処理速度を競うシステムを組むだけでなく、セキュリティの観点も含めて構築すべきシステムの在り方を提案することに対しても資金を投入すべきであった。

③　研究開発実施計画

評価	コメント
c	本研究開発の進め方について見直すべき点がある。そもそも基本計画で定めた目的が達成できているかどうかという点においては、それを詳細化していく段階で定めた具体的な実施目標自体が適切であったかを併せて検討しなければならない。この点から本研究開発の実施計画を見ると、単に機能したことの確認や処理速度・件数の数値を達成すれば良いといった目標の立て方は不十分である。実は、処理速度や件数といったパラメータ１つを規定するだけではあまり意味がなく、必要な計算機・ネットワーク資源の制約や達成すべきセキュリティのレベル等も同時に満たすといった目標の定め方でなければ、よろしくない。 また、タイムスタンプシステム・セキュリティシミュレータは、①で記述したように中止すべきである。その代わり、統合化プロトタイプシステム全体の方式を定め、方式の明確な記述を行い、セキュリティ上の目標を明確に示すことと、統合化プロトタイプシステム全体のセキュリティ評価を理論的に示すことを計画に加え、個別開発においては、そのために必要部分のセキュリティ評価と改善を行うようにすべきである。 さらに、ハッシュ関数ＳＨＡ－１の危殆化の動向を見据え、独立トークン方式においてもＳＨＡ－１より安全なハッシュ関数を用いた方式を実装する計画とすべきである。

④　平成１７年度予算計画

評価	コメント
d	③であげたポイントを重視して研究計画の見直しを行い、これに併せた予算計画に変更すべきである。

⑤　実施体制

評価	コメント
d	情報通信研究機構内に、タイムスタンプについて熟知した情報セキュリティの研究者・技術者を迎え入れて研究開発に取り組む体制とすべきである。

⑥　総合評価

評価	コメント
C	本テーマの研究開発の意義は大きく、日本標準時に基づく信頼できるタイムスタンプをわが国において定着させるための国家的プロジェクトとして重要であり、本研究開発を情報通信研究機構に続けて委託する以外の選択肢は考えにくい。また、平成１６年度は、平成１５年度末の時点で行われた中間評価における指摘事項も検討し、力を入れた取組みがなされた結果、着実な進展が見られる。 しかし、この段階に至り、最終的に意義ある結果を得ることを目指すためには、達成目標を修正することが必要なのではないかと考えられる。①から⑤のコメントなどを参考にして、タイムスタンプシステム全体のセキュリティ要件の明確化、開発した方式に関するセキュリティ面からの妥当性の検証、性能面において実用に耐えるレベルの技術の確立を、同時に満たし、世界に誇れるレベルの内容と説明可能性を有する研究開発を仕上げていただきたい。