（別紙２）

論文審査の結果の要旨

論文提出者氏名　ヤップ　リーフエン

本論文は、ユビキタスコンピューティング環境において提供される様々な情報通信サービスにおいて、多様な証明サービス（Attestation Service）を提供することを可能にする、利用者の行動（Activity）の証明サービスの枠組みを提案し、その有効性を実証的に検証し評価した。

本論文の研究の背景には、ユビキタスコンピューティングが社会に浸透し、社会のあらゆる活動をコンピュータの上で行なわれようとしていることがある。そうした中で、電子的に行なわれた活動をいかに信頼性の高いものとするか、つまり、「いつ、どこで、誰と、何がおこったのか」、ということが、後からきちんと証明できることは、現在の社会の仕組みの中で極めて重要である。本論文の研究は、利用者の実世界における行動を、電子的に高い精度で証明する手法を提案し、その際派生するいくつかの技術的な問題を解決した。

本論文で提案された行動証明のフレームワークは、次の３つの特長を備えている。まず第一に、ユビキタス・コンピューティング・アプリケーションを志向し、利用者の行動を実世界の時空間情報と紐付け、行動の起きた時刻と場所を証明する機能を提供していることである。第二に、利用者の行動情報を第三者機関に開示することなく証明を行ない、利用者の行動証明とプライバシー保護を同時に実現できていることである。第三に、eTRON を使った認証通信機能を活用することによって、一旦取得した証明情報を、認証されない利用者が不正に横取りすることを防いでいることである。

この枠組みを実証的に検証するために、２つのプロトタイプシステムを構築した。一つは SUCAS (Secure User-Centric Attestation Services) と呼ばれるもので、もう一つは SUCAS よりも、セキュリティー強度は弱いが軽量で簡素な COINS (Consumer-Oriented Integrated Service) である。実用化に向けた検討を行なうために、セキュリティーとコストのトレードオフに関して２種類の方式を考案して実装を行なった。これらの枠組みの上で、鉄道における遅延証明やヘルスケア分野における医療証明書、電子経済取引時のデジタル領収書などの実現手法を明らかにし、本論文で提案した枠組みの有用性が検証された。更に、本システムの実行性能及びセキュリティー強度に関する評価もなされ、本論文で報告された。

既に本研究の成果は、当該分野でも最も権威ある学会の一つである米国電気学会（IEEE）が主催する国際会議 "International Conference on International Conference on Information Privacy, Security, Risk and Trust (PASSAT) "をはじめとして、審査付きのフルペーパーの発表を既に４件行なっており、対外発表も十分に行なっている。

審査会においては、審査員から、いくつかの重要な指摘とそれに対するが行なわれた。まず第一に本枠組みは eTRON 仕様のスマートカード機構に依存している部分があり、本論文

の成果の普及が eTRON 仕様のスマートカードの普及に依存するのではないかという指摘がなされた。それに対して、既に現在ではいわゆるホワイトカードを呼ばれ、API を自由にプログラムできる環境が普及しており、代表的には Java カードで eTRON 仕様を実現することが確かめられており、問題ないと考えられる。第二に、証明を受ける時の実行性能が実用上不十分ではないかという指摘がなされたが、実際の証明をうけるときのユースケース上、必ずしも瞬時でおこなわれることが必須条件ではないため、本システムの性能でも十分であると考えられる。更に、今後のスマートカードの計算性能の向上により、応答性能を向上させることが可能であると主張された。こうした議論などを通して、論文の内容及びそれに関する質疑応答の内容に関して、学際情報学の博士の授与に十分であると本審査委員会は結論づけた。

よって本審査委員会は、本論文が博士（学際情報学）の学位に相当するものと判断する。