

(別紙2)

論文審査の結果の要旨

論文提出者氏名 カン エム ファヒム フェルドウス

本論文では、ユビキタスコンピューティング環境において、利用者のいる場所や行動、時刻といった実世界の状況情報 (Context) に応じて、デジタル情報への柔軟なアクセス制御を実現する新しい手法を提案し、試作することでその手法の有効性や安全性などを実証的に評価した。

近年の情報システムでは、情報アクセス権限が、実世界の Context に依存する 경우가多くみられる。例えば、ネットワーク上のビデオコンテンツは、特定の国以外からは試聴できないといったアクセス制限や、また美術館／博物館の展示に関する情報は、開館時間中に館内にいる来館者だけにアクセスさせたいケースなどがある。本論文の研究では、特に医療やヘルスケアに関する情報アクセス制御に着目し、情報閲覧者が物理的に存在する場所と時刻に応じて、柔軟なアクセス制御を実現できる機構を提供している。本機構では、こうしたアクセス制御が、例えば、大規模災害などが発生した緊急時には、通常時とは異なるアクセス制御ポリシーを適用することも可能である。また、各個人がアクセス制御権限をもつ個人情報も、その個人が大けがや大病の様な緊急時には、そのアクセス制御権限を他の人に委譲をすることで、その個人の生命を救うために必要な情報がきちんとした手順で獲得できることも実現可能である。

こうしたシナリオを実現するためには、実世界の Context をセキュリティー機構に高い整合性をもって組込む必要がある。本学位論文の研究においては、複数のアクセス制御方式を複合するハイブリッドなアプローチをとることによって、多様な Context 依存性に対応した。具体的には、Discretionary Access Control (DAC) と Role-Based Access Control (RBAC) を組合わせたアクセス制御フレームワークの中に、Context-aware アクセス制御を組込んだ。また、アクセス権限の委譲を実現するうえでは、アクセス制御や認証を物理的に担保するために、eTRON 仕様の対タンパ性を備えたハードウェアを用いた。本研究では、提案した手法を実装し、その機能検証及び性能評価を行なった。

既に本研究に関連する成果は、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 "IEEE International Conference on Information Theory and Information Security (ICITIS 2012)" をはじめとして、審査付きのフルペーパーが既に 5 件アクセプトされた実績をもっており、対外発表も十分に行なっている。

審査会では、本研究の主たる成果として、様々なセキュリティー上の要求をうまく実現できる機構を複数組み合わせるハイブリッドなアプローチをとることによって、実用性が高くかつ高機能なセキュリティーを実現している点が高く評価される。その一方で、性質の異なる複数のメカニズムを統合していることから、全体を包含しうる理論的な枠組みの構築が本

質的に難しく、本論文では扱っていない。こうした理論的な検証はハイブリッド方式に本質的な困難点であり、将来の課題である。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。