平成１５年度　情報工学コース卒業研究報告要旨

宮尾 研究室	氏　　名	Hamzaoui　Karim
卒業研究題目	ユビキタス情報環境における機器間認証に関する研究	

近年、計算機の小型化、携帯電話やPDAなどの無線端末の普及にともない、コンピュータがあらゆる場所に存在するユビキタスコンピューティングが注目を集めている。ユビキタス情報環境の利便性は多様な機器やサービスの登場によって次第に高まりつつある。その一方で、セキュリティに関する課題も同時に増大しつつある。インターネットにおいては、セキュリティのインフラとしてPKI（Public Key Infrastructure）が広く用いられており、公開鍵暗号化方式や電子署名に基づいたユーザ認証が情報セキュリティシステムの基盤となっている。これに対して、インターネットに接続されていない環境において携帯端末間で一時的に構築されるアドホックネットワークでは、PKIも、信用できる第三者も存在しないため一般的な認証システムの実現は困難である。しかしながらアドホック環境においても、機器間に何らかの信頼関係が存在すれば、信頼関係に応じたデータの通信が可能になる。

本研究では、まずユビキタス環境における機器間の信頼関係を新しく定義する。その上で、機器上のソフトウェアが持つ機能に基づく認証方式を提案する。本方式では、アドホック環境で通信可能な機器間において同一の機能を持つことを唯一の根拠とした認証を行う。ここで、機器が同一の機能を持つとは、同一のソフトウェアが動作していることを意味する。同一のソフトウェアを持つことを証明するために、各機器上では“ 機能認証コード ”と呼ばれる自己参照が可能なバイナリコードが用いられる。必要な機能の同一性確認により、対象の機器はサービス提供者の意図に沿った動作のみを行うため、IDなどの通信相手の認証情報を用いなくても、機器が安全にデータを利用することを保証できる。例えば、画像を3回しか表示できない機能を持った機器に対してのみ画像配布を行うサービスが実現できる。本手法を用いることによって、アドホックネットワークの動的な特徴を保持したまま、機能の改ざんや第三者による攻撃などのセキュリティ問題を回避することが可能になる。本手法の実現可能性を検証するために、画像データを転送するプログラムの機能をJAVAのJDIに基づき実現した。