平成１５年度　情報工学専攻修士論文要旨

坂部・酒井 研究室	氏　　名	岡田　泰典
論 文 題 目	関数の暗号化に基づく耐タンパーモバイルエージェントに関する研究	

モバイルエージェントはコンピュータ間を移動可能な能動的なプログラムであり、分散処理における通信遅延及び回数の削減、並列実行及び負荷分散、耐故障性の向上などの数多くの利点があり、次世代の分散処理システムとして注目を集めている．しかし、ネットワーク中を移動しながら実行されるモバイル・プログラムは、実行環境を提供するホストコンピューターからの攻撃を受ける（自身が保持する機密情報を盗聴される）可能性がある。このことは、例えばユーザーの代わり情報収集・電子決済・価格交渉などの電子商取引を行うエージェントの場合、クレジットカードの情報や個人情報が意図しないホストに見られ、悪用されることにつながる。よってモバイルエージェントを、インターネットを活動の場とした本格的な応用と呼べるものは、現状では存在しない。これに対し、Sander と Tschudin は、モバイル・エージェントの保護への応用を目的として、暗号化されたまま実行可能なプログラムの概念を定式化た。これを Mobile Cryptography という。

本研究では、この理論的なアプローチを採用した耐タンパー（機密情報を不正に読んだり、改竄することが困難）なモバイルエージェントシステムを実装し、評価をおこなう。これにより、Mobile Cryptography の実用性について検討する。まず河口等 [2001] が開発したモバイルエージェントシステム cogma に、関数の暗号化をすることでモバイルエージェントを保護する機能を追加する。暗号化する関数は n 変数 d 次の斉次多項式の n 次ベクトルとする。さらに、その例として消費者・販売会社・クレジット会社間での 3 者間契約を行う実用的なモバイルエージェントの実装をすることで、販売会社が作成した契約の確認をする関数が耐タンパーであることを示す。

セキュリティの効果と実用性については、暗号化される関数の条件を変えることで考察する。また、本研究で実装した 3 者間契約とクレジットカード決済用プロトコルの世界標準となっている SET との比較を行い、本手法が通信回数の低減と消費者の機密情報の保護において優れていることを示す。