平成21年度 情報工学コース卒業研究報告要旨

宮尾・八槇 研究室	氏　　名	森 文 宏
卒業研究題目	準同型暗号システムに基づく双方向ポリシマッチング	

インターネットでサービスを提供、あるいは利用する際には提供者と利用者の間で双方向のトラスト形成を行う必要がある。双方向のトラスト形成とは、サービス提供者が利用者を認証するだけではなく、利用者側からもサービス提供者を信頼出来るのか判断するようなトラスト形成のことである。サービス提供者と利用者がお互いに未知な場合における双方向のトラスト形成の仕組みとして Automated Trust Negotiation（ATN）が提案されている。ATN では、サービス提供者とサービス利用者それぞれが証明書及びそれらの証明書を開示するための情報開示ポリシを持つ。それに加えて、サービス提供者はサービスを利用するためにサービス利用者が満たすべきポリシ（Service Governance Policy-SGP）を持つ。以上のような状況において、双方向のトラスト形成を成立させるために互いの必要とする証明書を情報開示ポリシに反することなく開示する手順を求めることが ATN の目的である。しかし、ATN の基本的な戦略である Eager Strategy や Parsimonious Strategy では、交渉の過程で交渉には直接影響しない余分な証明書まで開示したり、交渉の最初の段階で相手に情報開示ポリシが漏れたりといった欠点が存在する。

そこで本研究では、最終的に求まる証明書開示手順以外の情報開示ポリシを相手に知られることなく、互いに必要な証明書集合を求める手法を考案した。この手法では単方向のトラスト形成しか実現できなかった準同型暗号システムに基づく単方向のポリシマッチングを拡張し、正方向ポリシマッチングと逆方向ポリシマッチングを繰り返すことにより、双方向のトラスト形成を実現している。正方向ポリシマッチングとは、クライアント側が開示してよいと考える証明書によってサーバ側に新たに開示可能になる証明書がないかを計算により求める手法であり、逆方向ポリシマッチングとは、サーバ側が開示してよいと考える証明書によってクライアント側に新たに開示可能になる証明書がないかを計算により求める手法である。準同型暗号システムに基づくポリシマッチングでは、互いの情報開示ポリシを暗号化したままの状態で計算を実行しているため、マッチングポリシ以外の情報が漏れることはない。

クライアントとサーバがお互いに情報開示ポリシを持った状態でこの手法を実行すると、正方向ポリシマッチングと逆方向ポリシマッチングを交互に行うことで交渉が進んでいく。各方向のポリシマッチングが終了した時点で、更なる交渉の余地があるかを判定し、ない場合は終了する。さらに、正方向ポリシマッチングが終了した時点では、SGP が満たされるかについての判定も行われ、満たされる場合には交渉成立となり、交換すべき証明書の最小集合を求めるためのやり取りが実行される。具体的には、それまでの各方向のポリシマッチングで得られた出力（マッチングポリシ）を交換し合うことによって交渉成立となる情報開示手順及び交換すべき証明書の最小集合が求められる。最後に求めた最小集合を出力して終了する。

本手法の考案により、単方向のポリシマッチングでは出来なかった双方向のトラスト形成が実現可能になった。さらに交渉過程における無駄な証明書の開示や情報開示ポリシの漏洩といった既存の ATN 戦略の欠点を解決した。