平成22年度 情報工学コース卒業研究報告要旨

高倉 研究室	氏　　名	青 山　桃 子
卒業研究題目	BPPM/AHES に基づく 自動トラスト交渉基盤の開発	

サービスの利用者と提供者が互いに未知である場合に，互いの信頼を確立することをトラスト形成という．インターネットを介してサービスを利用または提供する場合には，サービスの利用者と提供者の間でトラスト形成を行う必要がある．インターネット上でトラスト形成を行う仕組みとして，自動トラスト交渉（ATN:Automated Trust Negotiation）が提案されている．ATN では，サービスの利用者と提供者は各自の証明書と，証明書を開示するためのポリシを持つ．さらにサービスの提供者は，サービスを利用するために満たすべき条件（SGP:Service Governance Policy）を持つ．ATN の過程では，サービスの利用者と提供者は互いのポリシに反することなく証明書を交換する．その結果，SGP を満たすことができれば，サービス提供者は利用者に対してサービスを提供する．SGP が満たされなかった場合，交渉は失敗となり，サービスの提供は拒否される．

ATN によってトラスト形成を自動化するためには，ポリシに反することなく証明書を交換するための証明書交換手順の算出方法が必要となる．算出方法は様々なものが提案されているが，実装されている例は少ない．本研究では算出方法として BPPM/AHES（Bidirectional Private Policy Matching based on Additively Homomorphic Encryption Systems）を使用し，通信に REST（REpresentational State Transfer）を使用した ATN 基盤，RATN（Restful Automated Trust Negotiation）システムの開発を行った．

BPPM/AHES は加法的準同型性を持つ暗号を使用した交渉プロトコルである．証明書の交換手順をポリシを暗号化したまま算出するため，開示の必要ない証明書やポリシが相手に知れるのを防ぐという優れた特徴を持つ．本研究では BPPM/AHES のプロトコルを実際の REST 環境で動作させるための通信手順などを考案し，Java によるシステムとして実装した．サーバとクライアント間の通信に使用した REST は，実装が容易で汎用性の高い HTTP のインターフェースを用いる．それゆえ様々なサービスに適用されることが想定される本システムに適している．

本システムは RATN クライアントと RATN サーバの二つから構成されている．これらはあるサービスを利用するためのアプリケーションがクライアントとサーバを持っていた場合，それらの間で ATN によるトラスト形成を行うための基盤として動作する．サービス用アプリケーションのクライアントがサーバに対してサービスの利用を要求した時，サーバとクライアント間のトラスト形成がされていない場合は交渉が行われることになる．この時，クライアントは RATN クライアントを呼び出し，RATN サーバと交渉をさせる．交渉が成立すればクライアントはサービスを利用することができるようになる．

BPPM/AHES では暗号を用いるために，ポリシマッチングという独自の方法で互いのポリシを満たすかを判定する．ポリシマッチングには，所持している証明書数に応じて，大量の計算と通信を行う必要がある．実装を行った結果，一回の交渉における通信回数と交渉時間が非常に大きくなってしまうことが分かった．またポリシマッチングの際に使用する生成部分集合の大きさに伴って交渉時間が増大することが分かった．実際の環境に適用するためには，システムをクラウドに置き，エージェントに自動で交渉を行わせるなどの方法で，その欠点を補う必要がある．