平成24年度 情報工学コース卒業研究報告要旨

高倉 研究室	氏　　名	薮　田　信
卒業研究題目	近距離無線通信での自動トラスト交渉による柔軟な会員認証システムの開発	

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．また，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し，SGP が満たされなかった場合には，サービスの提供は拒否される．

本研究では近距離無線通信での ATN による柔軟な会員認証システムの開発を行った．会員認証ではサービス利用者は信頼できる第三者機関（TTP:Trusted Third Party）から会員証明書を受け取る．TTP は複数存在し，サービス利用者は複数の TTP から別の会員証明書を受け取ることができ，それぞれに優先順位をつける．まず，サービス利用者がサービス利用要求を行う．サービス利用者と提供者はポリシに従って ATN を行い，証明書の交換を行う．最終的に，サービス提供者の SGP が満たされれば交渉は成立し，サービスの提供が行われる．図１では，会員認証を行う ATN の一例を示す．この例では，両者は交換する証明書の要求を送信しあい，要求が満たされるならば証明書の交換を行う．会員証明書の有効性が TTP によって確認されれば，サービスの提供を行う．

実装は android 端末で行い，通信には近距離無線通信規格の一つである NFC IP-2 と Bluetooth を使用した．ハンドシェイクに NFC IP-2 の P2P 通信を使うことによって明示的な通信の確立を行い，Bluetooth を使用することによって高速な証明書の交換を行うことが目的である．

実験を行った結果，通信方式の切り替えの実行時間が大きく，不安定であるため全体の実行時間が大きく変動することが分かった．実行時間を安定させるためには，この切り替えの安定性を考える必要がある．

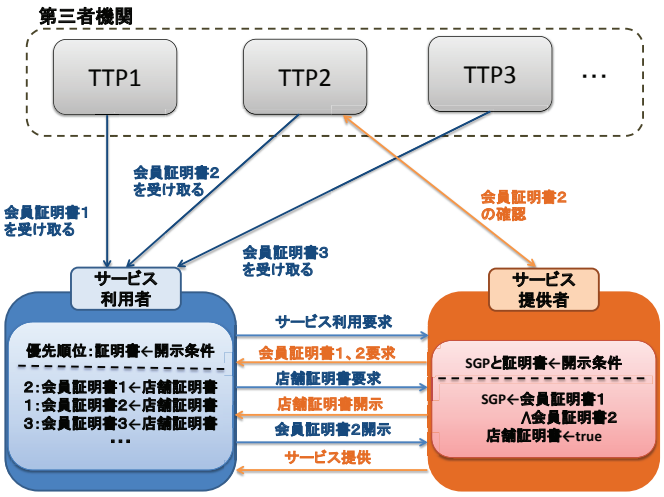

図１：会員認証例