輪講資料 04/11/4 @ IDEON Fall Retreat

William Josephson, Emin Sirer and Fred Schneider, "Peer-to-Peer Authentication with a Distributed Single Sign-On Service"

資料作成: 門林 雄基（奈良先端科学技術大学院大学）

"Peer-to-Peer Authentication with a Distributed Single Sign-On Service" (Josephson, Sirer and Schneider) は分散認証サービスを提案している。従来のシングルサインオン認証サービスでは、アプリケーションが認証情報を受け付け、それを元に SSO サーバが認証・権限付与をおこなうというアプローチがとられているが、本論文では複数の管理ドメインに分散して存在する認証サーバがそれぞれクライアントを認証し、その結果として得られる「割り符」をクライアントが結合して認証トークンとし、アプリケーションサーバに提示することでサービスを受けるというモデルをとっている。

割り符の実現方式としては threshold cryptography と呼ばれるクラスの暗号アルゴリズムを署名用途に使う。これは秘密分散法に閾値を導入したものである。ここで (t, s) sharing of k とは鍵 k を $k_1, k_2, ..., k_s$ に分割し、それぞれの断片を用いた署名文から鍵 k を用いた署名文を復元できるというものである。その具体的なアルゴリズムについては本論文では触れられていない。

登場人物としてはクライアント、アプリケーションサーバ、および分散認証サーバが出てくる（ここでいうアプリケーションサーバは分散型ではない）。アプリケーションサーバは認証ポリシ P を指定し、その中で自らが信頼する分散認証サーバ群を複数、列挙する。クライアントはどの分散認証サーバ群をつかってもよいが、その中のサーバが指定した閾値を越える、複数の認証サーバで認証に成功する必要がある。

なお、個々の認証サーバにおいてどのようにクライアントを認証するかという点は本論文では述べられていない。また、複数の認証サーバに対してクライアントの認証情報を分散させることの危険性についても考察されていない。クライアントは一方的に公開鍵 K_C をえらぶことができ、またどの分散認証サーバ群を使うかもクライアントに委ねられているので、比較的少数の認証サーバを乗っ取ればなりすましが可能だと考えられる。