平成 14 年度卒業研究		
入学年度　平成 11 年度	学籍番号　11117905	氏名　　伊藤卓也
論文題目　既存データベースに基づくシングルサインオンシステム構築に関する研究		中野研究室

1　はじめに

現在のインターネットを介して提供されるサービスは多岐に渡る．通常，Web クライアントは制限されたサービスを利用するために Web サーバに対してログインの手続きを行ない，認証を受ける．利用するサービスが複雑になり Web サーバの数が多くなると認証手続きの回数が増え，Web クライアントの利便性が低下する．そのために，Web クライアントの認証を一回で済ますシングルサインオンというシステムが存在する．

本研究では，クライアントの認証に必要な情報を蓄積したデータベースが存在する環境において，シングルサインオンシステムを構築する．

2　公開鍵基盤

インターネット上のセキュリティは，公開鍵基盤によるものが多く存在する．

2.1　公開鍵暗号方式

公開鍵暗号方式とは，公開鍵と公開鍵に対応する秘密鍵と呼ばれる鍵のペアを使用する暗号化方式である．公開鍵は一般に公開するが，秘密鍵は他人に漏洩しないように管理する．“公開鍵によって暗号化されたデータは秘密鍵によってのみ復号可能である” ことを利用した暗号化方式である．

2.2　電子署名

電子署名は “秘密鍵によって暗号化されたデータは公開鍵によってのみ復号可能である” ことを利用したものである．公開鍵基盤は，秘密鍵が他人に漏洩していないことを前提としているため，公開鍵で正常にデータが復号されれば秘密鍵を持っている本人によって作成され，改竄されていないことが確認できる．

2.3　公開鍵証明書

公開鍵証明書は，公開鍵暗号方式と電子署名の基盤となる公開鍵の正当性を証明するためのものである．公開鍵は一般に公開されるため第三者により改竄が可能である．そこで公開鍵に電子署名の技術を用いて改竄を防ぐ．署名を行う存在は認証局と呼ばれ，公開鍵基盤で構成されるシステムでは絶対に信頼される．

2.4　公開鍵認証

公開鍵認証は，認証を受ける対象が，公開鍵証明書の公開鍵に対応する秘密鍵を持っているかどうかを検証する方式である．被認証者に，あるデータを被認証者の公開鍵で暗号化したものを送り，秘密鍵で復号化したものを認証者が受けとり，一致すれば認証は成立する．被認証者の秘密情報である秘密鍵そのものが認証者に渡らない認証方式である．

2.5　SSL

SSL はインターネットにおける身近な公開鍵基盤の実装である．SSL は Web サーバと Web クライアントに対して公開鍵認証を実現し，暗号化通信路の確立も行う．

3　提案するシステム

提案するシステムは，複数の Web サーバが特定の Web クライアントに対してサービスを提供することを前提としている．システムはシングルサインオン (SSO) の実現を目的としているため，Web クライアントは各 Web サーバに対して 1 種類の認証情報を提示するだけで，Web サーバからサービスを受けることが出来ることとする．また，ユーザの利便性だけでなく，提案するシステムの構築によって安全性も確保されていなければならない．

3.1　既存のデータベース

複数の Web サーバは既存のデータベースに基づいてサービスを提供するが，オープンな環境であるインターネット上では信頼できない Web サーバに，Web クライアントの秘密情報が登録されているデータベースを直接参照させることは避けなければならない．そのため Web サーバがデータベースを参照することなく Web クライアントの認証を行う仕組みが必要になる．

3.2　チケット方式と SSO サーバの導入

チケット方式とは，Web クライアントがチケットと呼ばれる認証情報を Web サーバに提示することで認証を受ける方式であり，SSO サーバはそのチケットを発行する存在である．Web クライアントは最初に SSO サーバにログインし，SSO サーバから既存のデータベースに基づいて発行されたチケットを入手し，Web サーバに提示することによってサービスを受ける．

3.3　公開鍵証明書の利用

Web クライアントが Web サーバに提示するチケットに公開鍵証明書を用いる．Web サーバは，提示された公開鍵証明書が SSO サーバによって発行されたことを確認する．その後 Web サーバは Web クライアントに対して公開鍵認証を行ない，認証が成立した後サービスを提供する．図 3.1 に提案システムの概要を示す．

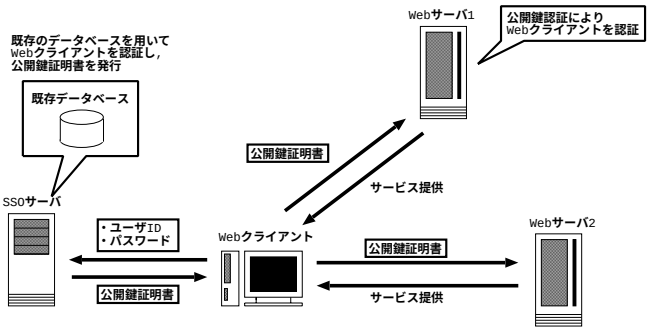

図 3.1: 提案システムの概要

3.4　考察

Web クライアントの秘密情報は Web サーバへ渡らず，公開鍵証明書は自動で Web ブラウザによって Web サーバへ提出される．Web クライアントは SSO サーバへ入力した秘密情報のみで複数の Web サーバに接続しているように感じられ，シングルサインオンが実現できる．

公開鍵証明書による認証は既存の技術である SSL を用いて実装が可能であるため，Web サーバや Web クライアントに特別なソフトウェアを必要とせず，安全性も高い認証方式であると考えられる．Web サーバの提供するサービスやシステム全体に求める安全性によっては公開鍵証明書の有効期限についても考える必要がある．

4　まとめ

認証に利用できるデータベースシステムが既に存在する環境において，高い安全性を持つシングルサインオンシステムを構築した．今後の課題としては，提案システムの実装により安全性や利便性の検証を行うことがあげられる．