平成 14 年度卒業研究		
入学年度　平成 11 年度	学籍番号　11117933	氏名　　辻 正嗣
論文題目　複数 Web サーバに対するシングルサインオンに関する研究		中野研究室

1　はじめに

近年のコンピュータやコンピュータネットワーク技術は急激に発展し，個人の情報や企業秘密などもインターネット上で行き交うようになった．そのため，盗聴やなりすましなどの被害を防ぐためにも，インターネットにおいても安全性 (セキュリティ) が求められる．そのセキュリティの一端である「認証」のうち，複数 Web サーバの認証が一度で済ませられるシングルサインオンを可能とする認証システムの構築をする．

2　セキュリティ技術

インターネットの世界でもセキュリティは重要課題である．そのための技術には以下のようなものなどがある．

2.1　公開鍵暗号方式

公開鍵暗号方式は，自分で秘密裏にもつ秘密鍵と，世界一般に公開されている公開鍵という，2 つの異なる鍵ペアを使用する暗号方式である．秘密鍵は，公開鍵から類推できないような鍵を生成する必要がある．公開鍵暗号方式を用いることで，通信の秘匿性や実在確認までの認証を可能とする．

2.2　公開鍵基盤 (PKI)

公開鍵基盤とは，公開鍵暗号方式に基づいて，電子署名や相手の認証などを実現するための環境のことである．なりすまし，盗聴，改竄，事後否認を防ぐため，安全と信頼を高めることができる．

2.3　電子証明書

電子証明書とは，認証機関がある ID に関連づけられた属性が正しいと認定したときに発行されるものである．電子証明書には，被証明者の国籍，名前などの情報と被証明者の公開鍵が入っている．さらに，認証機関の秘密鍵による電子署名がされており，証明書の内容をが正しいことをその認証機関のよって認定されているものとなる．

2.4　セキュア通信

相手と通信を行なう際に，データの盗聴，改竄を防ぐために通信路をセキュアな状態にする技術がある．その技術として，トンネリングを行なう VPN，SSH や通信を共通鍵で暗号化する SSL/TLS などが挙げられる．

3　Cookie

HTTP ではリクエストとレスポンスを基本として成り立っているため，状態の保持ができない．そのために開発されたものが Cookie である．Cookie は，Web サーバがある状態の情報を Web ブラウザに保存させ，次回アクセス時にその状態の情報を Web サーバに送ることでその状態を取り戻すことができる．オンラインショピングでのショッピングカートやアクセス回数のカウントなどにも利用されている．

4　目標とする認証システム

目標としている認証システムは，複数の Web サーバに対して，クライアントが認証を受けるのは 1 回だけでよい，というシングルサインオンを可能とする認証システムである．また，なるべくクライアントの手間を省き，自動で行えるものが好ましい．そのためには，Cookie によるセッション管理機能や電子証明書によるクライアント認証を用いることを考えた．Cookie は発行したサーバの Domain でしか有効でないため，他の Domain に属するサーバは受けとれない仕組みになっている．よって，Web サーバの Domain が認証サーバの Domain に後方一致する場合としない場合について分けて考える必要がある．なお，いずれの場合においても，秘匿すべき情報が流れる場合にはセキュアな通信を確立しているものとする．

4.1　後方一致する場合

後方一致する場合は認証サーバの発行した Cookie を Web サーバが受けとれる．この場合の認証の流れを図 (1) に示す．

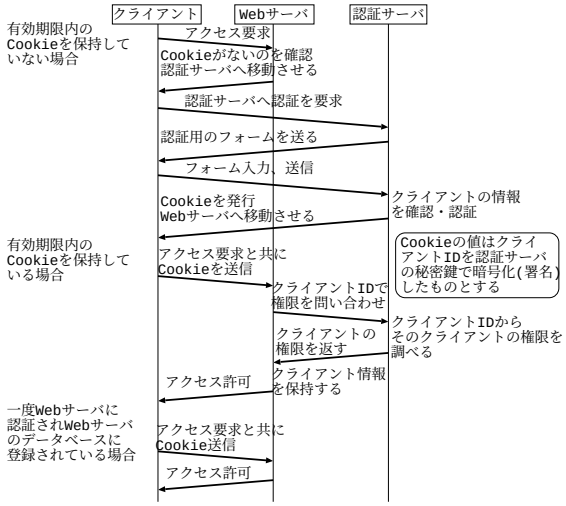

図 1: Web サーバの Domain が認証サーバの Domain に後方一致する場合

4.2　後方一致しない場合

後方一致しない場合は認証サーバの発行した Cookie を Web サーバが受けとれない．しかし，クライアントが認証サーバに暗黙的にアクセスすることにより，認証サーバに Cookie を送ることが可能である．その Cookie で認証ができ，認証サーバから Web サーバにクライアントが認証済みであることを伝えれば，Web サーバからクライアントにアクセス許可できる．

4.3　証明書を用いる場合

証明書は Web サーバも受けとれて，認証サーバがクライアントを認証したかを確認でき，さらにクライアントの情報も入れることができる．よって，クライアント証明書が Web サーバの信頼する認証サーバから発行されていることが確認できれば，そのクライアントにはアクセス許可できる．

4.4　考察

Cookie は発行や取り扱いが簡単な反面，Domain，ブラウザの制限や発行する際にはセキュリティ問題を考える必要がある．一方，証明書は信頼度が高く Domain，ブラウザの制限を受けないが，認証機関に対する信頼性も考慮に入れる必要があり，提示できる証明書を複数所持しているとクライアントに証明書を選択させる手間が生じる．

5　まとめ

複数の Web サーバの認証を一度で済ませられるか，そしてクライアントの手間をいかに減らすか，という点を中心に認証システムを構築した．今後の課題として，この認証システムの実装をして，動作や安全性の検証を行うことが挙げられる．