社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＱＡＩ－22 (12)
2007／1／19

レガシー Web アプリケーションに対応する PKI を用いた簡易 Single Sign-On の実現

西村 健† 佐藤 周行‡

†‡東京大学情報基盤センター 〒113-8658 東京都文京区弥生 2-11-16
E-mail: †takeshi@itc.u-tokyo.ac.jp, ‡schuko@cc.u-tokyo.ac.jp

あらまし 近年、Web アプリケーションの安全性とプライバシー保護の重要性からアクセス制御の厳格な管理が求められてきた。この問題に対して PKI はより良い解決策となりうるが、特に大学では認証方式として PKI を採用できない Web アプリケーションが存在する（「サイボウズ問題」として詳述する）。我々はクライアント認証として PKI 認証を行ない、これを中継点として Web アプリケーションにアクセスするゲートウェイを構築した。さらにこのゲートウェイは Web アプリケーションに対してユーザ名・パスワードを提供するパスワードサーバとしても機能する。このシステムによって安価なコストで簡易的な Single Sign-On (SSO) を実現することができる。

キーワード PKI, 認証, SSL-VPN, パスワードサーバ

Implementing Simple Single Sign-On with PKI for Legacy Web Applications

Takeshi NISHIMURA† and Hiroyuki SATO‡

†‡Information Technology Center, The University of Tokyo 2-11-16 Yayoi, Bunkyo-ku, Tokyo, 113-8658 Japan
E-mail: †takeshi@itc.u-tokyo.ac.jp, ‡schuko@cc.u-tokyo.ac.jp

Abstract Today, because some contents are closely related to security and privacy, there is a requirement for a strict management of access control. PKI is considered as a solution of the management. However, there are some systems that PKI is hard to adopt (Cybozu problem). We consider a gateway that provides PKI authentication, and making access to servers via the gateway. Furthermore, the gateway works as a password server for content servers. This gives an SSO-like solution for users with reasonable cost.

Keyword PKI, authentication, SSL-VPN, password-server

1. はじめに

今日我々は Web を通して数々の情報サービスを受けられるようになっている。Web は情報提供の場として重要度を増していくとともに、別の側面で特定のコミュニティにおける情報共有の場としても利用されてきている。多くの大学の Web ページが各学部からの広報の場として利用されている。その利便性から多くの情報が Web 上に掲載されるようになってきた。学部、学科など特定の単位のコミュニティの人々がこの Web によってつながりを持っている。この場面での問題は情報に対するアクセス制御である。アクセス制御は情報の中身による分類と捉えられる。例えば試験の採点結果は特定の教授にのみアクセスを許され、任意の学生に許されるものではない。財務部門のシステムに対するアクセス制御は厳格におこなわれなければならない。またオンラインジャーナルやソフトウェアパッケージなど、ライセンスからの要請でアクセス制御が必須のものもある。セキュリティやプライバシーの観点からアクセス制御の厳格な管理が必要とされている。

PKI (Public Key Infrastructure) はこのようなアクセス制御に対する一つの解であると考えられる。つまり適切に運用されるという前提の元で、PKI は最も厳格な認証方式であり、ゆえにこの認証の元でのアクセス制御は厳格に行なうことができる。

PKI は厳格なセキュリティを必要とする小規模の組織から採用され始めてきた。特に法律により厳格なセキュリティが必要とされる官吏の仕事の電子化においては PKI の採用が現実的な唯一の選択肢となる。アメリカやカナダのいくつかの政府機関は既に PKI 運用の経験を積んでいる。カナダでは 1993 年から政府の PKI を運用している。アメリカでは 1990 年代初頭から省向けの PKI を運用しており、それらは Fedetal PKI としてブリッジで接続されている。日本では 2001 年から GPKI (Government PKI) の運用が開始されている。その主な目的は官吏へのデジタル署名の提供である。また PKI は住基ネットでも利用されている。

東京大学情報基盤センター PKI プロジェクトの取組 [1,2]

東京大学は 2004 年に大学の教職員および学生の身分証として IC カードを採用し、認証基盤として PKI を整備する計画があるというプレスリリースを出した。情報基盤センターは PKI を整備し、PKI アプリケーションの利用を促進し、PKI 運用コストの最適化を検討し、東京大学および大学一般における最適な認証のフレームワークを開発するために「PKI プロジェクト」を発足させた。

PKI プロジェクトはすでに大学での運用に合わせたプライベート CA のプロトタイプを構築し、大学内の数部局と共同で実証実験を行なっている。一方で PKI アプリケーションの普及のため、既存のサーバ群と安全な認証を行なう上での問題に取り組んでいる。

大学のサーバへの安全な認証の組み込み

PKI アプリケーションの普及において重要なのはサーバが PKI 認証を利用することである。東京大学ではすでに全学レベルから研究室レベルまで多くのサーバが稼動しており、多くの情報が Web を通じて提供されている。しかし多くのサーバで認証は旧来の ID およびパスワードによるものである。財務部門やオンラインジャーナルなど機密情報を扱う必要があるサーバはアクセスを大学内からのみに制限し安全性を保っている。つまり利用者は大学内にある端末からそのようなサーバにアクセスしなければならない。PKI 認証を採用すればこの制限を緩和できる可能性がある。

しかしながら大学のサーバには既製品のソフトウェアパッケージにより構築されたものも多い。つまりそのパッケージが提供する（多くの場合 ID およびパスワード方式の）特定の認証方式に制限されるということである。そのようなシステムで PKI 認証を組み入れることは難しく、そのようなサーバ群をカバーするのは大きな問題になっている。我々はこの問題を、大学内でよく使われていて認証方式に ID/パスワードを採用しているグループウェアの名称をとって「サイボウズ問題」と呼んでいる。

この問題の解決策として、我々は PKI 認証を用いるゲートウェイシステムを提案する。このゲートウェイが上述したサーバ群のアクセスポイントとなる。PKI 認証の後にゲートウェイがサーバに対する ID およびパスワードを送出する。このシステムを用いればサーバに手を加えることなくさらなる安全性を得ることができる。

技術的にはこのシステムはサーバ側でサインオンを行なわないため SSO (Single Sign-On) システムではない。しかし利用者の視点ではゲートウェイでのみ認証を行なっているように見えるため、利用者の立場では SSO システムとして動作していると言える。このシステムの利点はサーバを改変することなく行なえることで、SAML ベースの SSO を実現するのに必要な莫大なコストを抑えることができる。小規模の組織に対するセキュリティの改善案としては安価なコストでの現実的な解になりうると考える。

本論文の構成

本論文は以下のように構成される。次節で構築したシステムのベースとなっている SSL-VPN について触れ、第 3 節でシステムの核となるレガシー Web アプリケーションに対応するためのパスワードサーバの概念について説明する。第 4 節および第 5 節で構築したシステムのセキュリティ面およびコスト面の考察を行う。第 6 節で関連研究について触れ、第 7 節で本論文のまとめを行なう。

2. PKI 認証による SSL-VPN

一般的な情報サービスにおいて、利用に制限があるのはよくあることである。制限には IP アドレスによるものやファイアウォールによるものなど様々である。とりわけセキュリティ上もしくはプライバシー上重要な情報を扱う場合は、悪意のある攻撃から情報を守るために必要な措置だと考えられる。上記に挙げた制限は（完全ではないにしろ）ある程度有効ではあるが、ある面で利便性を犠牲にしている。つまり利用者はネットワーク上特定のセグメントに居ることが必要であり、例えば出張で別の場所に居るとそのサービスを受けられないということになってしまう。サービス提供者はその安全性と利便性のトレードオフを考慮しなければならない。

一方 VPN (Virtual Private Network) はこの問題の一つの解決策となりうる。VPN 技術とはつまり、インターネット上の特定の利用者もしくは端末が特定のプライベートネットワーク上にあたかも存在するかのように見せる技術である。プライベートネットワーク内に居るとみなされれば、そこでのサービスを自由に受けられることになる。

VPN の実装には IPSec、PPTP、SSL-VPN、SoftEther 等がある。SSL-VPN は機器間の通信に SSL 技術 [3] を用いるもので、IPSec 等と比較してクライアント側に追加の設定が必要なく、経路上のファイアウォールの影響を受けないなどの利点を持つ。このような点から SSL-VPN はリモートアクセス型、つまり不特定多数の

クライアント端末が特定のサーバにアクセスするような状況において有効な選択肢とみなされている。

しかしながら、どのようなVPN技術を利用しても利用者もしくはクライアント端末に対する認証が確実なものでなければ安全であるとはいえない。多くのVPN製品がPKIを含んだ複数の認証方式をサポートしている。認証方式としてPKIを採用すれば、VPN機器はPKIの厳格な認証により大部分の不正アクセスからの保護が実現でき、サーバはVPN機器による保護の恩恵を受けることができる。つまり間接的にサーバ自体がPKIが提供する安全性を享受できることになる。

我々はSSL-VPNサーバをゲートウェイとしてプライベートネットワークへ接続するVPN環境を構築している。認証にPKIを用いプライベートネットワーク内にサーバを配置することによって、安全なサーバ環境を実現している。

3. レガシー Web アプリケーションに対応するパスワードサーバ

SSL-VPNの形態として機能がシンプルで設定も容易なリバースプロキシ型を想定すると、PKI認証によるSSL-VPNの一つの問題は、VPNサーバとコンテンツサーバで認証情報を共有できないことである。コンテンツサーバ側での認証はVPNサーバでのPKI認証とは独立に用意しなければならない。旧来のID/パスワード式の認証の場合はVPN接続後にそのログイン画面が表示され、利用者はIDおよびパスワードをそれぞれのサーバに対して入力する必要がある。

サイボウズ株式会社のサイボウズグループウェアは直接的にはPKI認証をサポートしない。問題はこれが費用効果が高くユーザフレンドリであるため大学において多く導入されていることである。しばしば機密情報を共有するために使われるので、システムの安全性の向上は重要である。これが「サイボウズ問題」である。

3.1.システム構成

この問題を解決するため、我々はSSL-VPNサーバと連携するpassword pushout serverというサーバを提案する。Password pushout serverは(証明書のDN, server ID, userID, 暗号化されたパスワード)の組をそれぞれの利用者証明書、コンテンツサーバに対して保管しておく。SSL-VPNに対する認証が成功し、利用者が特定のコンテンツサーバへ接続を指示すると、SSL-VPNはその要求をフックしpassword pushout serverへ接続するように要求する。クライアントがpassword pushout serverへ接続すると、そのクライアント証明書情報から対応するuserIDおよびパスワードをクライアントへ返す。クライアントは取得したuserIDおよびパスワードをSSL-VPN経由でコンテンツサーバへ送信し正しく認証を行なうことができ、以降コンテンツサーバからサービスを受けられる。

ここでのポイントはpassword pushout serverに保管されるパスワードは利用者の公開鍵で暗号化されているということである。Password pushout serverは暗号化されたパスワードのみを扱い、コンテンツサーバへの送信の直前にクライアント側で復号を行なう。これによって平文のパスワードの漏洩先が最小限に抑えられる。図3.1にサーバ群の構成を示す。

4. 利用者へ想定される脅威とその解決策

前節で説明したpassword pushout serverシステムについて、利用者に対して想定される脅威には以下のものが挙げられる。

- 経路上での盗聴
- キーロガーによるパスワードの窃盗
- 管理者による不正

以下、それぞれの脅威に対して考察を行ない、本システムが満たすセキュリティ上の位置付けを明確にする。

4.1. 経路上での盗聴

まず、ネットワーク経路上での盗聴への対処法であるが、SSL-VPN本来の機能であるSSLによる暗号化によって対処する。またクライアント端末－password pushout server間についても同様にSSLによる暗号化を行なう。

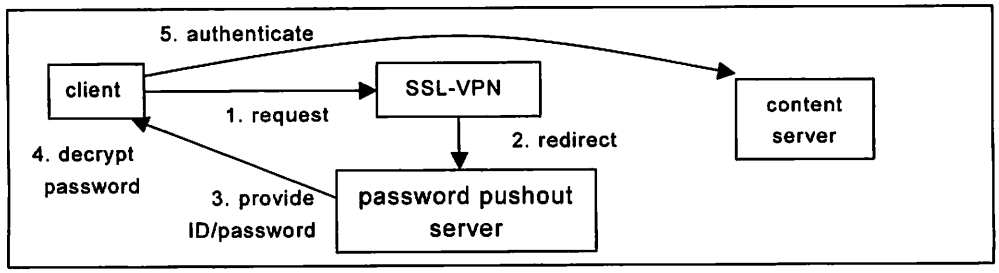

図 3.1: password pushout serverおよびその他のサーバの構成

4.2. キーロガーによるパスワードの窃盗

私有鍵の PIN 以外にパスワードを入力することはなく、その意味では安全であるといえる。ただしクライアント端末上で任意の悪意あるプログラムが実行できる場合には、password pushout server から送信された暗号化されたパスワードを復号するか、コンテンツサーバへ送信する平文のパスワードを盗聴することによりコンテンツサーバに対するパスワードの窃盗は可能である。

4.3. password pushout server 管理者による不正

password pushout server には各種のサーバに対する ID/パスワードの組が保管されるため、この部分におけるセキュリティは特に重要になる。前述のとおり password pushout server に保管されるパスワードは利用者の公開鍵により暗号化されており、その点では安全であるといえる。

ただしクライアント端末は password pushout server から送信されたスクリプトに従いパスワードの復号等を行なうため、そのスクリプトに悪意のあるコードが含まれていた場合平文のパスワードの奪取が可能になる。

つまり安全性は利用者がクライアント端末で実行するスクリプトが信頼できるものであるかどうかの一点に集約されることになる。

4.4. 本システムの位置付け

以上の考察から、本システムは、(1)クライアント端末に悪意あるプログラムが実行される可能性がなく、(2) password pushout server から送信されるスクリプトが第三者による精査で問題ないと判断されそれがデジタル署名等で確認できる場合に有効なシステムと位置付けることができる。

5. コストの考察

以上で述べた password pushout server システムについてそのプロトタイプの実装を行ない、その実利用面でのコストの検討を行なった。

使用機器：

SSL-VPN: FirePass 1010

password pushout server:

Mac mini 1.83GHz 512MB メモリ 80GB HDD

client: Windows マシン Firefox 2

5.1. クライアント側での暗号化および復号の問題点

今回の検証で用いた Web ブラウザは Firefox のみであるが、Windows 環境で広く利用されている Internet Explorer においても ActiveX (CAPICOM) の利用で同等のシステムが実現できると考えている。

なお、クライアント端末上の証明書へのアクセスなど本 password pushout server システムの実装の一部は大抵の Web ブラウザでは任意の Web アプリケーションに対して認められているものではない。すなわち本来スクリプトへのデジタル署名等により回避すべき事象であるが、本プロトタイプではその実装は行なわず、ブラウザのセキュリティ設定変更[1]で上記操作を可能にしている。回避手段には以下の方法が考えられる。

- 使用スクリプトへのデジタル署名

  これは Firefox、Internet Explorer 共に提供している手段であり、また組織内での利用という想定では署名証明書を発行した認証局を各利用者に信頼してもらうのも現実的である。
- 拡張機能もしくは ActiveX を利用したブラウザへの組み込み

  あらかじめクライアント端末にインストールしておく必要がある。ただし前述の通り自分でもしくは他人が精査したスクリプトのみを信用し不用意に新たなスクリプトを実行しないという立場に立てば、意味のある手段である。

5.2. 実利用面での追加コスト

本 password pushout server システムは各 Web アプリケーションの処理と連携しないため、各 Web アプリケーション上のユーザ名とクライアント証明書の DN との一対一の対応付け、およびパスワードの初期登録は利用者に任されている。主な Web アプリケーションにおけるユーザ名(ID)の管理はおおむね以下の 2 つに分類される。それぞれについて利用者の負担を軽減させる方法を検討する。

- 内部的な ID で管理している場合

  大抵の場合ログイン画面にユーザ一覧のドロップダウンリストが表示され、それを選択することでログインする形式になっている。対処方法としては、ログイン画面の HTML ファイルを取得・解析し、表示名と内部 ID の対応付けを自動的に得ることが考えられる。ただしこの場合も表示名と証明書 DN との対応付けは別途入力しておく必要がある。
- Web アプリケーション毎に管理者が登録する場合

  Web アプリケーションへの登録時に password pushout server へも同時に登録することが考えられる。この場合管理者の負担増は避けられない。

[1] about:config にて signed.applets.codebase_principal_support を有効にすることによる

6. 関連研究

PKI を利用した認証にはいくつかの方式がある。とりわけ RSA 認証（チャレンジレスポンス形式）と公開鍵認証がよく利用される。SSH1 は RSA 認証を利用し、SSH2 は公開鍵認証を利用する [4,5]。

PKI を利用した認証モジュールは多数公開されている。Apache [6] 上での実装は最も有名なものの一つである。SSL のサーバ認証においては PKI 認証が利用されている。一方クライアント側の認証はまだ始まったばかりで普及しているとはいえない。例えばアメリカにおける Grid ミドルウェアのデファクトスタンダードである Globus [7] はサーバ間の認証に SSL クライアント認証を利用している。

認証基盤は ID 管理と組み合わせて利用される。そのような環境では利用者は一度サインオンするだけで十分で、認証を行なったという事実を複数サーバ間で共有することにより各サーバでの認証の代わりとする。この概念は SSO と呼ばれ、標準プロトコルが規定されている。SAML [8] は認証情報をサーバ間で受け渡すために設計された。

7. まとめ

我々 PKI プロジェクトは、ID およびパスワードによる認証のみをサポートするレガシー Web アプリケーションに PKI 認証を組み込む方法を提案した。現在遍在するレガシー Web アプリケーションに PKI による厳格な認証を付加することは安全性の向上につながり、PKI アプリケーションの普及および啓蒙に役立つと考える。まず、システムのベースとなる SSL-VPN サーバをゲートウェイとして利用することを説明し、その SSL-VPN サーバと連携する安全なパスワードサーバを提案した。利用者は自身のパスワードをパスワードサーバ管理者に知られることはない。PKI 認証の SSL-VPN と我々のパスワードサーバの組み合わせは、安価なコストで安全性向上の一つの解となることを示した。

文　献

[1] T. Nishimura, H. Sato, "Authentication with PKI – a Case Study in Information Technology Center in The University of Tokyo," International Symposium on Advanced ICT, pp. 251-255, Tokyo, Japan, Aug. 2006.

[2] 東京大学情報基盤センターPKI プロジェクト, http://www.pki.itc.u-tokyo.ac.jp/

[3] Netscape Communications, SSL 3.0 Specification, http://wp.netscape.com/eng/ssl3/, Nov. 1996.

[4] RFC 4252, The Secure Shell (SSH) Authentication Protocol.

[5] OpenSSH, http://www.openssh.org/

[6] The Apache HTTP Server Project, http://httpd.apache.org/

[7] The Globus Alliance, http://www.globus.org/

[8] OASIS, http://www.oasis-open.org/