香川大学教育実践総合研究（*Bull. Educ. Res. Teach. Develop. Kagawa Univ.*），11:69－75，2005

# SSLを用いた学校教育現場におけるWWWサーバのアクセス制限システムの試作

宮崎　英一，竹森　元彦
（技術教育）　（発達臨床）

760-8522　高松市幸町１－１ 香川大学教育学部

# A Trial Production of the Access Limitation System Using SSL of the School Education Site

Eiichi Miyazaki, Motohiko Takemori

*Faculty of Education, Kagawa University, 1-1 Saiwai-cho, Takamatsu 760-8522*

**要　旨**　本研究では，インターネットショッピング等の個人データのアクセス時に使用されるSSLを応用して，WWWサーバにクライアントからのアクセスを制限するシステムを試作した。このシステムでは，閲覧者は特別なソフトウェアを準備する必要がなく，普段自分が使い慣れたブラウザがそのまま使用可能なため，学校教育現場においても比較的簡単に導入が可能である。ここでは，予めアクセスに必要なクライアント証明書をアクセス希望者にのみに配布しておき，クライアントは自分のブラウザにこの証明書をインストールするだけで，暗号化されたWWWページにアクセスが可能になる。この方式では，一般的なパスワード認証等の方法と比較してセキュアな環境を構築する事が可能になり，従来では個人保護の観点から不特定多数の公開が不可能であったWWWページでも公開が可能になり，より学校教育の現場に即した情報提供が可能になると考えられる。

キーワード　SSL，WWWページ，アクセス認証，パスワード，Webサーバ

## １．はじめに

現在，パーソナルコンピュータの低価格化と高機能化，および携帯電話やインターネットに代表される情報インフラの急速な一般家庭への普及[1]に伴い，学校教育現場においてはインターネット上の検索エンジン等を利用した調べ学習[2]はもとより，WWWページ（一般的にはホームページと称されることが多い）を利用した様々な情報発信は，もはや当たり前のように行われている。しかもこれらの情報発信は，学校やクラスといった不特定多数のグループからの発信は言うに及ばず，最近では生徒自身の自己紹介のような，個人そのものの情報までをも含んだ，より細分化された情報発信が普及しはじめている。

元来，これらで作成されるWWWページは，不特定多数の他人に公開することを目的として作成されている。しかし，教育現場に関しては，生徒のプライバシー保護や，その内容から学校関係者以外の不特定多数に閲覧されては問題が発生する恐れが有る，等の様々な教育上の

観点から，WWWページの閲覧にアクセス制限を設けることが必要な場合が多々ある。このアクセス制限に関して従来は，WWWサーバに実装された，パスワードやIPアドレス等を利用してアクセス制限を設ける「Basic認証」[3]が多く使用されていたが，個人情報保護の観点から，さらにセキュアなアクセス制限をサーバに実装する必要性がより求められている。

このため，本研究では学校現場のWWWサーバにおいて情報発信を行う場合，よりセキュアなアクセス制限を設けるために，SSL[4]（Secure Socket Layer）を用い，WWWサーバとブラウザの両者において，WWWページに関するアクセス制限の実装を行った。このSSLは，一般的には通信データの暗号化という点を用いて，ネットワーク上のショッピングにおける不正アクセス防止に使用される事が多く，個人情報閲覧のセキュリティ向上に使用されている手法である。

このSSLの中でもアクセス制御に，より高度なクライアント認証を用いる事で，ユーザからのアクセス認証がサーバとクライアントの相互認証型となり，学校教育現場における情報発信のように不特定多数の環境下のアクセスに関しても，きわめて強固な不正防止制限を設ける事が可能となる。その結果，セキュリティ上の観点から，従来では公開を見合わせていたような内容でも問題なく情報発信が可能となり，教育現場においても情報教育の，より一層の発展が見込まれる。

## 2．SSLの概要[5]

ここではシステムの基本となるSSLについて説明を行う。一般的なネットワークショッピングにおけるWWWサーバにおいて，クレジットカードの番号入力や，様々な個人情報のアクセスに関しては，SSLの暗号化を利用しており，これにより通信データの「盗聴」，「改竄」，「成りすまし」，「否認」等の不正アクセスを防止している。これらの通信に利用されるSSLは，サーバ側に証明書を持ち，クライアント側には持っていない片側認証型が採用されている。これは公開鍵と秘密鍵を使用するものであり，公開鍵を使用してクライアント側の情報を暗号化，サーバ側で秘密鍵を使用してデータの復号化を行うものである。この時のサーバとクライアント間の通信の流れを表１－１に示す。

表１－１　通常のSSL

| 順番 | クライアント（ブラウザ） | データの流れ | サーバ |
|---|---|---|---|
| 1 | 通信開始 | アクセス→ | |
| 2 | | ←公開鍵送付 | 電子証明書 |
| 3 | 公開鍵を用いてデータ暗号化 | | |
| 4 | | 暗号化されたデータ送付→ | |
| 5 | | | 秘密鍵を用いて複合化 |

しかしこの方式では，通信データそのものは暗号化されるので，「改竄」や「盗聴」などの不正アクセスから守られても，第三者からの不正アクセスを防止する事はできない。

そこで本研究では，さらに高度な認証方式として，クライアント側にも証明書を持たせ，サーバ側でもクライアントの認証をクライアント証明書で行うことが出来る，相互認証型のSSLをWWWシステムに使用した。このシステムにより通信データの暗号化だけでなく，クライアントとサーバはお互いを認証することが出来るようになり，クライアント証明書をもったクライアント側からのみサーバにアクセスが可能になるので，不特定多数のアクセスを防止する事が可能になる。これを表１－２に示す。

### 2．2　電子証明書と認証局（CA）[6]

電子証明書はユーザの公開鍵の正当性を保証するために使われるものである。その方法は，ユーザの公開鍵について信頼できる第三者である認証局（CA: Certificate Authority）が電子署名を作成し，それを公開鍵と共に公開することによって公開鍵が改竄されていないことを確認可能にするものであり，この公開された電子署名と公開鍵とを併せて電子証明書と呼んでいる。

表１－２　クライアント認証

| 順番 | クライアント（ブラウザ） | データの流れ | サーバ |
|---|---|---|---|
| 1 | 通信開始 | アクセス→ | |
| 2 | | ←電子証明書要求 | CA証明書 |
| 3 | クライアント側電子証明書 | | |
| 4 | CAに一致する証明書選択 | | |
| 5 | | 電子証明書提示→ | CAを用いて証明書検証 |
| 6 | | | クライアントの確認OK |
| 7 | | | 表１－１の１に続く |

SSLを使用する場合，サーバ認証およびクライアント認証の両者ともCAによる署名が必要となる。通常は，正式な機関[7]にCAを申請するのが普通であるが，本研究ではCA自身もプライベートとして作成している。しかしこれは，電子証明書の規格として正式な機関で使用されているのと同様なX.509に準拠して作成しているので，通常のインターネットショッピングに使用されるSSLと全く同じセキュリティ機能を有している。

## ３．WWWサーバの概要

これらのサーバは，ネットワーク関係のシステムから構成されるため，通常はLinux等のUNIX系のサーバに構築される事が普通である。しかし，本研究では実際の教育現場へのOSの普及度合いやコンピュータの配備状況から考察して，Windows2000上にこのシステムを実装した。以下に，この手順について説明を行う。

本研究で使用した代表的なソフトウェアを表２に示す。本研究では２種類のソフトウェアを用いたが，これらの基本的なインストール方法については通常のプログラムのインストールと同様であり，その情報も広く提供されているため，詳しくは割愛する。もし問題がある場合にはこれらの文献[8, 9, 10, 11]を参照されたい。

表２　使用したソフトウェア

| ソフト名 | 備考 |
|---|---|
| Openssl-0.9.7f-Win32.zip | Win32環境下でSSLの実装 |
| Apache_2.0.54-Openssl_0.9.7g-Win32.zip | SSL化されたWWWサーバ |

さらにここでは，主としてSSLの動作に必要なWWWサーバの設定や，SSLに使用される各種証明書や公開・秘密鍵の作成について説明するが，これらの作成についてはコマンドラインからの入力で行う上に，非常に煩雑な手間が要求される。よってここでは，プログラムの細部については言及せず，全体の流れだけの説明を行う。

### ３．１　Apache+SSL for Win32の設定[12]

ここではWWWサーバの動作に必要な制御ファイル（confファイル）の設定を行う。この設定ファイルにより，サーバ自身のSSLに関する制御を行う事が可能になる。

・　httpd.confの設定（SSLモジュールの組み込み）。
・　SSLを動かすための設定（ssl.confの設定。鍵，証明書のパスの変更）。

### ３．２　SSL用証明書の作成[13]

A）　プライベートCAの作成

認証の大元となる認証局（CA）を作成。この認証局は個人で作成。

A－１）CA用秘密鍵（cakey.pem）とCA用証明書（cacert.pem）の作成。

A－２）CA証明書をブラウザにインポートするためのca.derファイルの作成。

B）サーバ用証明書の作成

ここでは，WWWサーバとなるApache用のサーバ証明書を作成する。

B－１）サーバ用秘密鍵（server.key）の作成。鍵長1024ビットで指定。

B－２）サーバ用公開鍵（server.csr）の作成。CAに送るデジタル証明書のリクエスト

ファイルを作成。

B－3）サーバ用証明書（server.crt）の作成。認証局の証明書とキーを使って，X.509サーバ証明書の作成と署名を行う。

C）クライアント用証明書の作成

クライアント用証明書によるクライアント認証を導入すると，予め認証局で署名されたクライアント用証明書を持たない端末がアクセスしても，接続そのものが拒否される。

C－1）クライアント用証明書作成用リクエストファイル（newreq.pem）の作成。CAに送るデジタル証明書のリクエストファイルを作成。

C－2）クライアント用証明書（newcert.pem）の作成。認証局の証明書とキーを使って，X.509クライアント証明書の作成。

C－3）pkcs12形式のクライアント用証明書（ex. miya.p12ファイル）の作成。鍵と証明書を安全に外部に渡す（クライアントに渡す）ために，pkcs12という方法で鍵と証明書をひとつにまとめる。

### 3.3　ブラウザのSSL用設定

ここでは，上記で説明したクライント証明書（miya. p12）のクライアントへのインストール方法を示す。現時点で様々なブラウザがSSLに対応しているが，本研究では，この中でも教育現場において一般的に使用される事が多いと予想されるInternet Explorerを例として説明する。

もちろんNetscapeやFirefox等のブラウザもSSLに対応しているので，この証明書をそのまま利用して，WWWサーバにアクセスすることが可能である。クライアント側ユーザのSSLを用いたページへのアクセスであるが，下記の使用手順に従えばよい。

1）WWWサーバの管理者から，クライアント認証用のクライアント証明書が保存されたFD等を配布してもらう。

2）同じくWWWサーバの管理者から，クライアント証明書のインストールに必要なパスワードを配布してもらう。

3）クライアント側のブラウザにクライアント証明書をインストール。

4）［https://＊＊＊］で記述されたSSLページにアクセスが可能になる。

3）のインストールについては，ユーザが問題を発生しやすい場面であるので，下記に別途説明を加える。ここで注意するのが，1）と2）の配布方法であり，両者とも電子メールを使用して配布してはならない。通常の電子メールを用いた通信では，暗号化されていない平文で通信が行われるため，途中でデータに不正にアクセスされる可能性があるためである。また両者は同時に送ってはならない。これらが同時に流出した場合，セキュリティそのものが無効化されるためである。

### 3.4　クライアント証明書のインストール

ここでは，上記3）で示したブラウザに，クライアント証明書をインストールする方法について述べる。最初に，1）で配布されたクライアント証明書（miya. p12）をダブルクリックする。すると図1に示すように自動的にクライアント証明書のインポートウイザードが起動され，証明書のインストールが開始される。

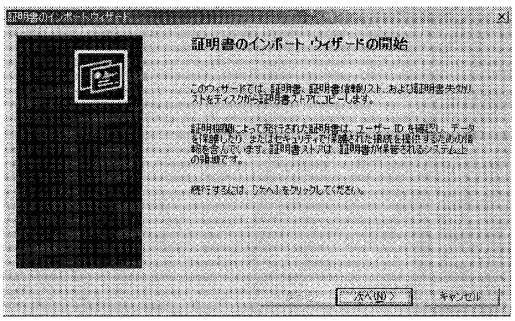


図1　インポートウィザード

次に図2に示すように秘密キーのパスワードを聞いてくるので，2）で配布されたパスワードを入力する。このパスワードが手に入らない限り，クライアント側では，証明書がインストールできないので，よりセキュアなシステムになっている。逆に言えば，パスワードを紛失するとインストールできないので，パスワード

の取り扱いに関しては注意する必要がある。

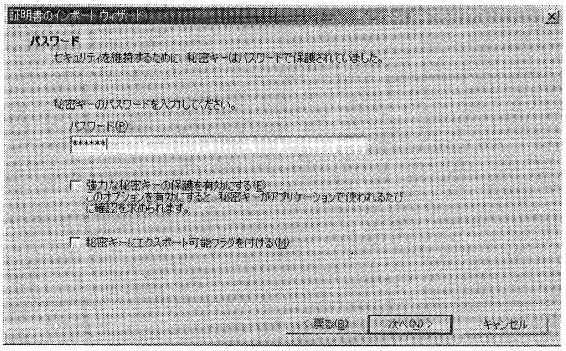


図2　パスワードを入力

ここで正しいパスワードが入力されれば，残りのストア処理が行われ，図3に示すように，インストールウイザードが完了する。

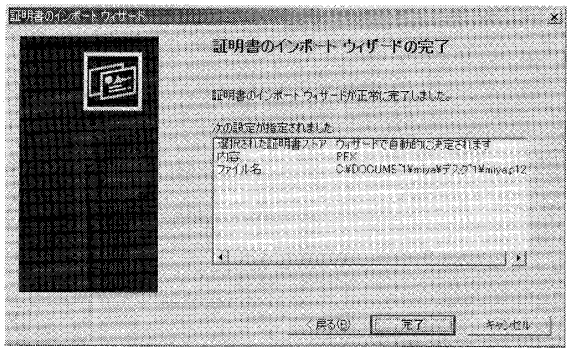


図3　インポート完了

ここで証明書がクライアント側のブラウザに正しくインストールされたかどうか確認するにはInternet Explorerの「インターネットオプション」→「コンテンツ」→「証明書」の順で確認できる。正しくインストールされていれば，図4に示すように証明書の「個人」のタグに上記でインストールした「miya」というクライアント証明書が表示されている。これがインストールされるとクライアント側のブラウザが，実際に「https」で記述が始まる暗号化されたページにアクセスが可能になる。

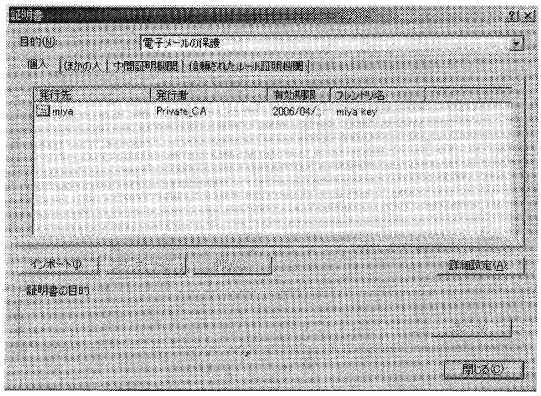


図4　インストールされた証明書

ここではアクセス制御の確認を行うため，上記で説明したSSLを実装した「https:// a 1200. ed.kagawa-u.ac.jp」というWWWサーバを立ち上げた。このテスト用サーバにクライアント認証を用いて，アクセス制限を設定したページにアクセスを行う。ちなみに，このサーバに対して，通常のアクセス方法として「http://a1200. ed.kagawa-u.ac.jp」のアドレスでアクセスすると，アクセス制限を設けていなく，かつ暗号化されていない通常のWWWページを表示することが可能である。

これにより，一つのWWWサーバのアドレスにおいて，通常のアクセス制限を設けていないWWWページから，アクセス制御されたページにシームレスに移動する事が可能であるため様々な応用が期待できる。またこれらのSSLによるアクセス制限を設けた状態においても，さらに通常のユーザアカウントとパスワードを用いたアカウント制御も可能なので，ユーザの目的に応じたシステムを構成する事が可能となっている。

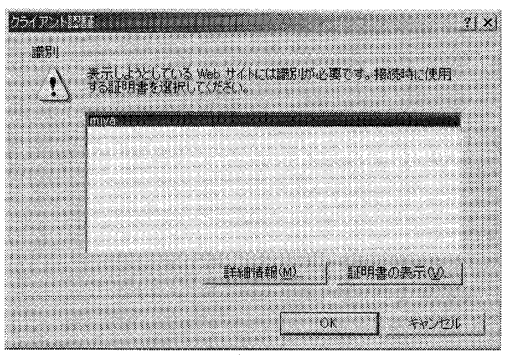


図5　証明書の確認

上記で説明したように，実際にSSLを応用したアクセス制限が設けられたテスト用のページにアクセスした場合，図５に示すように自動的にクライアント認証がサーバから要求されるので，先程インストールした「miya」という証明書を選択する。その結果，図６に示すように暗号化されたページへのアクセスが可能になる。ここではブラウザの下部の欄に鍵のマークが示され，このページに関しては，暗号化されたアクセスが行われている事が示されている。

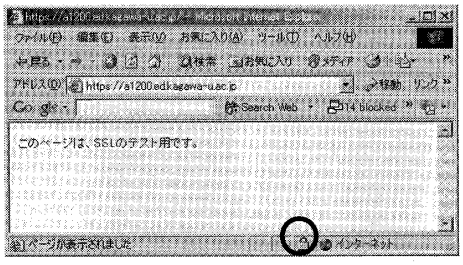


図６　アクセス成功

もし，クラインアント証明書がないユーザが，このページに無理やりにアクセスした場合，図７のようなエラーページが表示され，このクライアント証明書を持たない状態では，正常にアクセス出来ない事が示された。これにより，本システムにおいてクラインアント認証が，アクセス制限として正常に機能していることが判る。

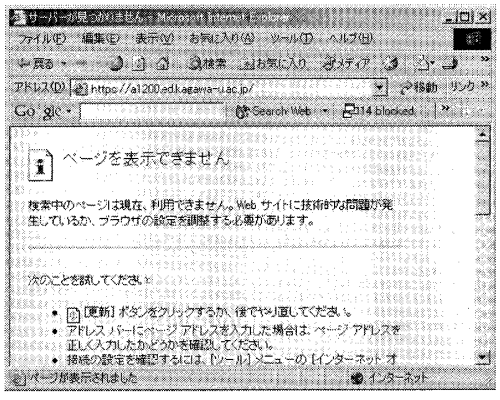


図７　アクセス失敗

## ４．まとめ

ユーザアカウントとパスワードを用いた従来のアクセス制限システムでは，教育現場のように多数のユーザが使用する場合，その取り扱いが問題になる場合がある。複雑なパスワードに設定するとセキュリティは向上するが，ユーザの入力の手間という問題が発生し，利便性が低下するので，これらの関係はトレードオフにあり，両者を同時に満足するのは困難である。またパスワードそのものが類推されたり，流出するといった問題が発生したりする場合も考えられる。

それと比較して，本研究で行ったクライアント認証を用いたアクセス制限システムでは最初にクライアント側のコンピュータにクライアント証明書をインストールする手間があるものの，一度インストールが完了してしまえば，その後のページに対するアクセスはマウス操作だけで完了するので，ユーザの利便性も保たれると考えられる。またこのシステムはパスワードを用いた方法と異なり，証明書が流出する可能性がきわめて低く（システムにセキュリティホールがあれば別であるが），よりセキュアなシステムが構築可能であると考えられる。

さらに，クライアント証明書には図８に示すようにアクセスに関する有効期限が設定されている。これを応用すれば，期間限定でページの閲覧を設定する事も可能であるため，学校教育現場において公開時期を設定したい場合の制限等様々な応用が考えられる。

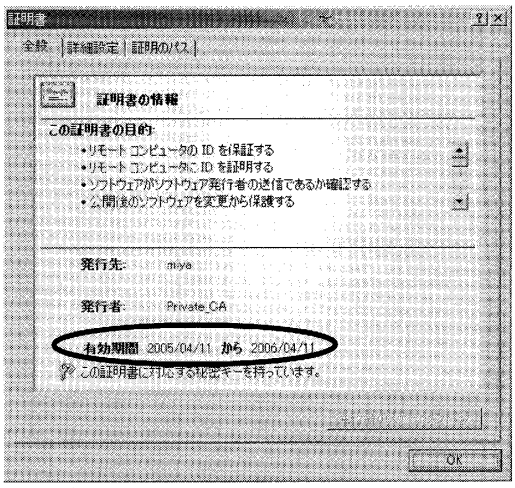


図８　有効期限の指定

## 5．さいごに

本研究で作成したシステムを使用する事で，比較的簡単にアクセス制限にSSLが適応可能な事が示された。このシステムでは非常にセキュアな通信環境を構築可能なため，従来では個人情報保護の観点から配信困難であった情報もインターネット上からでも配信可能になると考えられる。また特別なソフトウェアをインストールしなくても，普段使い慣れたブラウザがそのまま使用できるという利点もある。しかし一方，サーバ側ではクライアント証明書やパスワードの配布等の手間があり，これを自動化することはできない。よって閲覧者が数百名程度の規模になると個人的な対応では問題が発生する事も考えられる。

今後，学校が単なる教育の見地から情報発信を行うだけでなく，地域に還元する意味からもインターネットを介した情報の発信が必要不可欠になるのは間違いないであろう。その場合，本研究で作成したシステムが何らかの手助けになれば幸いである。

### 参考文献


1 自治体モバイル戦略—ケータイがつなぐ人と地域 ユビキタス社会へ向けて，河井 孝仁，細田 大造，信山社，2005

2 坂出市立坂出中学校，分かる授業づくりを目指したコンピュータ等の活用，平成16年度香川県中学校教育研究会情報教育研究部会教育研究大会，2004

3 実践インターネットセキュリティ，Bradley Dunsmore，Jeffrey W.Brown，秋田克彦訳，エクシード・プレス，2001

4 Linuxネットワーク WWWサーバ管理者ガイド，梅田 峰子，ソフトバンクパブリッシング，2000

5 暗号技術の基本と仕組み，若林 宏，秀和システム，2005

6 SSLと電子証明書を用いたWWWにおけるユーザ認証システムの検討，内藤 茂樹，平成16年度大阪大学総合技術研究会，分子科学研究所技術研究会報告書，2005

7 政府認証基盤（GPKI），総務省 行政管理局，http://www.gpki.go.jp

8 Apacheハンドブック，Ben Laurie，Peter Laurie，大川 佳織 訳，田辺 茂也著，オライリージャパン，1997

9 Turbolinux 7 Server サーバー構築入門，高原 利之，ソーテック，2002

10 TURBOLINUXで作るネットワークサーバ構築ガイド，秀和システム出版編集部著，秀和システム，2002

11 OpenSSL日本語サイト，http://www.infoscience.co.jp/technical/openssl/

12 Apache Web サーバー Black Book，Greg Holden，Matthew Keller，IDEAC訳，インプレス，1999

13 SSLによるSecureWWWサーバの構築（Windows編），http://www.aconus.com/~oyaji/www/apache_win_ssl.htm