日本大学文理学部資料館 デジタルミュージアムシステムの構築 ―SSL を用いたセキュリティ対策―

谷　研究室　　林 裕之

概要

日本大学文理学部の資料館と情報科学研究所は共同して，資料館の収蔵資料のデジタルミュージアムシステムを開発した．本システムは，目録のみならずデジタル化した資料を一般に公開する機能も併せ持っている．このような意味で，デジタルミュージアムシステムとも言えるものである．本システムを用いて本学部資料館の収蔵資料を内外に広く公開することで，より広い分野の研究素材と成り得ることが期待される．本研究では，資料館デジタルミュージアムシステムのセキュリティ対策を担当した．

1　はじめに

博物館や資料館に収蔵されている現物資料を閲覧する際，収蔵元が地理的に離れているために閲覧するのが困難な場合がある．また，資料によっては，公開することにより損傷する恐れがあるため，公開そのものが困難な場合もある．資料をデジタル化し Web で公開することにより，このような問題の一部は解決し，多くのユーザがコンテンツにアクセスすることができるようになる．また，デジタル化した歴史資料の公開によって，新たな歴史的事実の発見に寄与することも期待される．実際，多くのデジタルアーカイブやデジタルミュージアムと呼ばれるシステムが，様々な機関により開発・公開されている ([1]).

日本大学文理学部は，100 年以上の歴史を持ち，研究・教育のために，人文科学，社会科学，自然科学に関する多種多様な資料の収集をし，それらの調査・研究ならびに保管・展示を行ってきた．このような多年にわたって集められた資料を教職員，学生および一般の利用に供することを目的として，日本大学文理学部資料館は 2006 年に設立された ([2]). 本学部資料館では従来収蔵資料の管理を紙媒体を用いて行ってきた．昨年度より日本大学文理学部の情報科学研究所と資料館との共同研究として，資料館が収蔵する多種多様な資料の目録のデジタル化の検討を始めた．検討当初は，目録のデジタル化のみを目的にシステムを設計していたが，検討を進めるうち，目録のデジタル化のみならずデジタル化した資料を一般に公開する機能を含めることとなった．このシステムは，そのような意味でデジタルミュージアムシステムとも言えるものである．このシステムを用いて本学部資料館の収蔵資料を内外に広く公開することで，より広い分野の研究素材と成り得ることが期待される．

この本学部資料館デジタルミュージアムシステムは一般公開されるため，多くのユーザが本システムへアクセスすることが考えられる．本システムの利用者の中で悪意のあるユーザがいないとは限らない．そのため，本システムに登録されている多くの資料を保護するためセキュリティ対策を施す必要がある．本研究では，本システム構築の中でセキュリティ対策を担当した．本稿では担当したセキュリティ対策について述べる．

2　SSL を用いたセキュリティ対策

本学部資料館デジタルミュージアムシステムは，管理ページと公開ページにわけられる．管理ページは，本学部資料館にて資料データを登録・変更・削除を行うページである．公開ページとは，一般に公開されるページである．セキュリティ対策は本システムの管理ページに行った．

2.1　セキュリティ対策

本システムの管理ページへログインできるアカウントは，登録資料データを削除する権限がある. 仮に管理ユーザのアカウントとパスワードが流出した場合，悪意のある第三者によって本システムへログインし不正な操作をするおそれがある．このため，管理ページへログインできるアカウントとパスワードを悪意のあるユーザから保護しなければならない．本システムの管理ページでは，SSL による暗号化通信の実現でパスワードの盗聴を阻止することを実現している．

通常の HTTP による通信は送受信するデータを誰で

も見られる状態で通信を行なっている．しかし SSL はサーバとブラウザの間の通信を暗号化することで第三者による盗聴を阻止できる ([3])．本管理システムではパスワードを送信する login ページや項目・資料の削除などの操作時，アカウントの管理ページにて SSL を使用している．

この SSL による暗号通信を利用すると通常の通信よりサーバ側・利用者側のコンピュータに大きな負荷がかかる．これを防止するため SSL を利用するページはパスワードを送受信するページに限り利用し，管理ページのトップや新規追加等のページでは通常の通信を使用している．

これによって管理ページのセキュリティ確保と負荷軽減を実現している．

2.1.1 SSL

SSL とはインターネット上で情報のセキュリティを高める暗号化通信プロトコルである ([4])．SSL には二つの利点がある．一つ目は，データを暗号化し送受信するため第三者による盗聴を防止できる．二つ目は，サーバ証明書により, なりすましを防ぐことができることである．なりすましとは，インターネットのアクセス機能を悪用して第三者が他人を装い，さもその人のようにふるまい情報を盗むことである．

これに対し，SSL を使う欠点として以下が挙げられる．暗号化の処理は、クライアント側・サーバ側双方にとって負荷のかかる処理であり結果として通信速度の低下を招くことである．暗号化・復号をその都度行うこの SSL ではそのような問題が発生する。

2.1.2 サーバ証明書

サーバ証明書とは，Web サーバに対して認証局が発行する電子証明書のことである．サーバ証明書には、サーバのホスト名・組織名・認証局の組織名・証明書の有効期限・Web サーバの公開鍵等が書きこまれている．これを認証局の秘密鍵で暗号化することによって Web サーバの身元が保証される．

2.1.3 認証局

認証局とは，電子証明書の登録、発行などを行う第三者の認証機関である．今回のシステムにおいては、自分自身のサーバがルート認証局となり証明書を発行し、暗号化通信を利用している．この場合は Web ブラウザに認証局の公開鍵がインストールされていないので Web ブラウザが警告文を表示する．

2.2 アカウント管理

管理ページにアクセスできるアカウントを管理するページを**アカウントの管理**ページと呼ぶ．管理ページへアクセスできるアカウントの種類には，管理ユーザと root 権限を持ったユーザ (以下 root ユーザ) がある．root ユーザは，本ページにて管理ユーザのアカウント管理と root ユーザのパスワード変更を行える．root ユーザは本学部資料館にて管理され，通常の資料登録作業には使用されない．管理ユーザは，資料の管理作業を行う際に使用されるアカウントである．管理アカウントで本ページを表示する際は自身のパスワードのみ変更できるようになっている．

管理ユーザのアカウント管理を行う場合は，root ユーザでログインした後，アカウントの管理ページから**他のアカウントの管理**ページに進む．他のアカウントの管理ページでは，現在登録されているユーザのうち root 以外の全てユーザ名が一覧表示され，各アカウントのパスワード変更と，アカウントの追加と削除ができる．これらの操作のうち，アカウントのパスワード変更や削除をする場合は，再度 root のパスワードを入力する必要がある．

root 以外の管理ユーザで，アカウント管理ページを閲覧すると，**自分のパスワード変更**へのリンクのみが表示される．自分のパスワード変更ページでは，ログインしているユーザ自身のパスワードを変更できる．この操作を行うには，現在のパスワードを入力することが要求される．パスワードを失念した場合は，root ユーザにパスワードの変更を依頼する必要がある．また，管理ユーザが URL を入力する等不正な方法で「他のアカウント管理」に移動しようとしても，root 以外のユーザは移動できない．

本システムでは，セキュリティ対策としてデータベースにパスワードを保存する際，ハッシュ化して保存するようにした．これによってデータベースのデータが外部に漏れたとしても，パスワードを復元することは不可能である．

3 おわりに

本システムはこのようなセキュリティ対策を施した．SSL を使用したことで秘匿性が高まり第三者ユーザに管理ページのアカウントやパスワードの流出する危険性を低減している．これによって安全な運用が可能であり，広く一般公開できることで利用者が増え，広い分野の研究への寄与が期待される．

参考文献

[1] 国立公文書館「デジタルアーカイブ・システム標準仕様書」
http://www.archives.go.jp/law/pdf/da_100118.pdf

[2] 日本大学文理学部資料館：
http://www.chs.nihon-u.ac.jp/museum/

[3] Ben Laurie Peter Laurie
Apache ハンドブック

[4] SSL 3.0 Specification ：
http://www.freesoft.org/CIE/Topics/ssl-draft/3-SPEC.HTM