

絵葉書を介したハルビンの景観変遷の 印象調査システムの構築 -サーバ構築とSSLを用いた通信の暗号化-

谷 研究室 石見 圭

概要

情報メディアとしてのコンピュータやインターネットの普及により人文科学においてもデジタル技術の応用が進んでいる。日本大学文理学部情報科学研究所の共同研究である「東アジアにおける都市形成プロセスの統合的把握とそのデジタル化をめぐる研究」の一環として、「絵葉書を介したハルビン景観変遷の印象調査」を実施した。本研究では、印象調査システム構築のうち、特に仮想マシンの構築とSSLを用いた通信の暗号化を担当した。

1 はじめに

情報メディアとしてのコンピュータやインターネットの普及により、人文科学においてもデジタル技術の応用が進んでいる。これに伴い、デジタルヒューマニティーズと呼ばれる学問領域が発展している。デジタルヒューマニティーズとは、人文科学の研究と教育をコンピュータを用いることにより新しい方法論を創出することを目的の一つとしている([1])。このようなデジタルヒューマニティーズ研究の一環として、デジタルライブラリ、デジタルアーカイブ、デジタルミュージアムの研究・開発が行われている。本研究室では過去に、デジタルヒューマニティーズの研究の一環として、ハルビン絵葉書検索システム(日本大学文理学部史学科と共同)やデジタルミュージアム(日本大学文理学部資料館と共同)を開発した。例えば、デジタルミュージアムでは、日本大学文理学部資料館の収蔵資料をデジタル化し公開しているが、ことは検索、テーマ検索の機能を有している。このことにより、今までは手作業で資料を探さなければならなかったが、パソコンでの検索が可能になることで作業効率が向上した。また、デジタル化した歴史資料の公開により、新たな歴史的事実の発見が期待される。

本研究は、平成22年度に文部科学省私立大学戦略的研究基盤形成支援事業に採択された日本大学文理学部情報科学研究所の共同研究である「東アジアにおける都市形成プロセスの統合的把握とそのデジタル化をめぐる研究」の一環である。このプロジェクトの研究目的は、東アジアの形成を様々な分野の研究の成果を統合的に把握し、東アジア都市の多面的かつ重層的な歴史の実態を総

体的に解明することである。特に、人文科学的アプローチからの都市形成の把握に、社会科学的アプローチからの都市形成の把握を加えることにより、より統合的な理解を深めることを目指している。そこで、社会科学的アプローチの一つとして、本プロジェクトの心理評価班と共同で心理実験を実施することとなった。実施した心理実験は「絵葉書を介したハルビン景観変遷の印象調査システム」であり、この調査のためのシステムを市川隆敏、石見圭、高田美聡が共同で開発した。報告者は仮想マシンの構築とSSLを用いた通信の暗号化について述べる。

2 仮想マシンの構築

絵葉書を介したハルビン景観変遷の印象調査システムでは、仮想サーバVMware ESXを導入している([3])。

2.1 仮想化技術

仮想化技術とは、コンピュータの物理的な資源、プロセッサやメモリ、ストレージを分割し、それぞれが独立したコンピュータのように稼働し、別々にOSやアプリケーションを動かせる。仮想化の利点は、物理的に複数の資源を管理する場合に比べ管理が容易であり、資源を必要に応じて配分できるという点である。

2.2 仮想マシンの構築

絵葉書を介したハルビン景観変遷の印象調査システムを構築する上で仮想マシンを構築した。平成23年度には北海道で実施したiPadを用いたアンケート調査と、平成23年度1月に実施した調査対象者各自の端末を使用したアンケート調査の2回の調査を実施した。それぞれのシステムは、異なる仮想マシンで稼働している。

2.3 仮想マシンの構成

- CPU:1 個
- メモリ:1GB
- ストレージ:20GB
- OS:ubuntu10.10
- Apache + MySQL + PHP

3 SSL を用いたセキュリティ対策

絵葉書を介したハルビン景観変遷の印象調査システムには、ログインページ、個人情報登録ページがある。ここでは WEB ブラウザ・Web サーバ間で重要な情報をやり取りしている。通常の HTTP による通信は送受信するデータが誰にでも見られる状態で通信を行なっている。そこで SSL を用いたセキュリティ対策を施すことにした。

3.1 セキュリティ対策

本システムにはパスワードや個人情報など重要な情報のやり取りをしている。そのためセキュリティ対策が必要である。そこでセキュリティ対策に SSL を使用した([2],[4])。

今年度の 1 月に行った調査では WEB ブラウザを用いたアンケート調査を実施した。その性質上対象者以外の者がアクセスする可能性があった。今回我々は事前に対象者に ID とパスワードを配布し、ログインしてもらう手法をとった。

3.2 SSL

SSL とは Secure Socket Layer の略で、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。

SSL には 2 つの大きな役割がある。1 つ目は Web ブラウザと Web サーバ間の通信を暗号化することで、第 3 者による盗聴を防止できる。2 つ目はサーバ証明書によりなりすましを防ぐ。

暗号化の処理は、クライアントとサーバ双方にとって負荷がかかり、暗号化と復号化を行う SSL では通信速度が低下する恐れがある。

3.3 サーバ証明書

サーバ証明書とは Web サイトの所有者の情報、Web サーバの公開鍵、発行者の署名データ等を持った電子証明書のことである。Web サーバに対して認証局が発行しているが、今回のシステムにおいては、自分自身が認証局となり証明書を発行している。

認証局とは、電子証明書の登録、発行などを行う信頼された第三者の認証機関である。

4 今後の課題

本システムは、システム全体に SSL で通信の暗号化が施されている状態である。しかし、SSL の処理はクライアント・サーバ双方に負荷がかかってしまう。負荷を軽くするために通信の暗号化は、ログインページや個人情報登録ページなどの重要な情報のやり取りを行う必要がある場所だけに留めたい。

参考文献

- [1] 出口直輝:—絵はがき歴史資料のデジタルアーカイブ化による付加価値の試み—日本大学大学院総合基礎科学研究 科地球情報数理科学専攻修士論文,2011.
- [2] 日本ベリサイン 【セキュリティ・電子証明書・SSL】: <https://www.verisign.co.jp/>
- [3] 島田裕輝: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サーバーの仮想化と冗長化について
- [4] 林裕之: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