ネットワーク利用認証システム
Opengate の紹介

学術情報処理センター長
渡辺義明
Email:watanaby@is.saga-u.ac.jp

1　はじめに

ネットワークをキャンパス内のどこでも自由に利用できる環境の整備が望まれています。一方、インターネット上では、侵入破壊行為や誹謗中傷行為、詐欺行為等のトラブルが頻発しております。このような行為をキャンパス内から行われることは可能な限り回避するとともに、行ったときには当人に責任を取っていただく必要があります。

従来は、利用者が特定できる空間にネットワークを配備してきました。誰でも利用できる開放空間に、自由に接続可能なネットワークを配備するとなると、利用者を特定することが難しくなります。そこで、このような環境においても、利用資格を持つ者のみにネットワークの利用を許可し利用時刻の記録を取ることのできるシステム Opengate を開発しています。現在、文化教育学部演習室の PC および附属図書館内の公開端末や情報コンセントは、このシステムの下で稼動しています。ここでは、このシステムの利用方法と仕組みについて説明します。

2　利用手順

Opengate の動いているネットワークを利用する手順を以下に示します。以下では公開端末の利用を想定していますが、持参したノート PC を情報コンセントや無線 LAN 経由で接続する場合も同様な手順で利用できます。

1. **Web ブラウザを起動して、どこか任意の Web ページを呼び出します。**
2. **指定した Web ページの代わりに、ユーザ ID とパスワードを要求する Web ページ（図 1 上）が送られてきますので、それに返答します。**
3. **正しいパスワードであれば、許可を表わす Web ページ（図 1 下）が表示されます。その後は自由にネットワークを利用できる状態になります。**
4. **利用が終わったときは、必ず Web ブラウザを終了して下さい。**

なお、画面構成は変更の可能性があります。

3　留意事項

上述のように利用は簡単ですが、利用に際しては以下の点に留意して下さい。

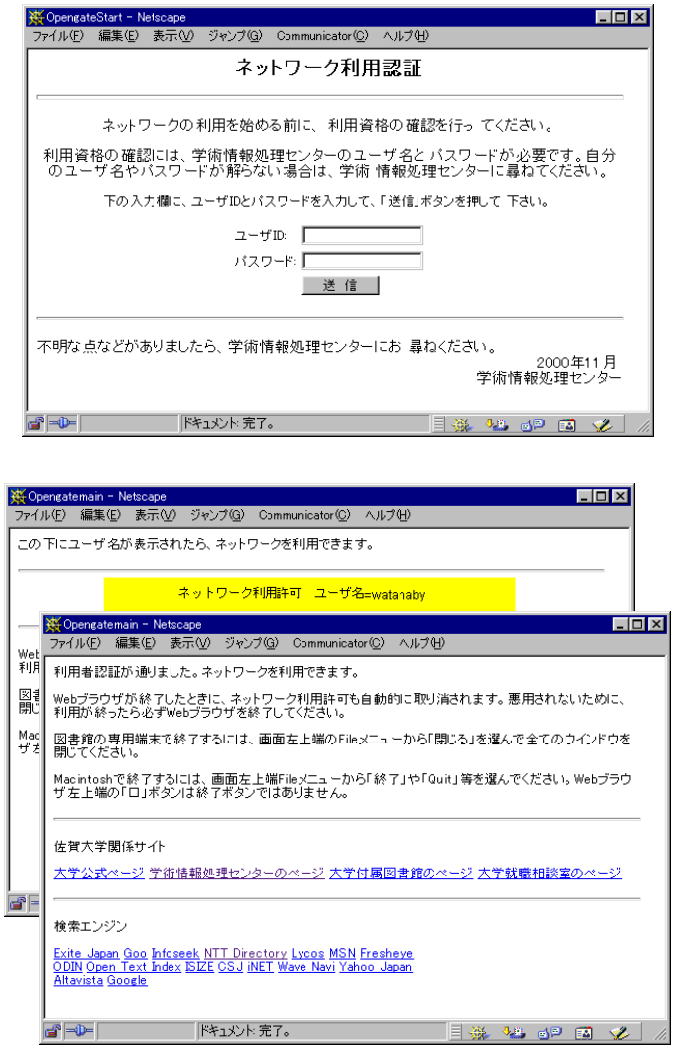

図 1: 利用者画面

1. センターのユーザ ID を所有していれば、事前の申し込みや設定は必要ありません。標準設定の PC を接続して Web ブラウザを起動するだけです。ユーザ ID を所有していない場合はセンターや附属図書館の窓口へご相談ください。身元確認の上、期限付きのユーザ ID を発行します。

2. 利用終了後には必ず Web ブラウザを終了してください。放置すると、その後の利用も放置した人が行ったものとみなされます。

3. telnet や FTP など、Web 以外のネットワークアプリケーションを利用する際にも、まず Web ブラウザを起動して認証を受け、利用が終わるまで、それを保持してください。最小化・アイコン化しても結構です。ただし設置場所によっては認証なしで使えるように設定されたネットワークアプリケーションもあります。例えば、文化教育学部演習室からはセンターのメールサーバに認証なしで接続できます。

4. Web ブラウザはできるだけ新しいものを使い、設定を Java・JavaScript 稼動可能にして下さ

い。一般的な Web ブラウザでは標準設定のままで良いでしょう。

4 システム構成

システムの構成を簡単に紹介します [1][2]。

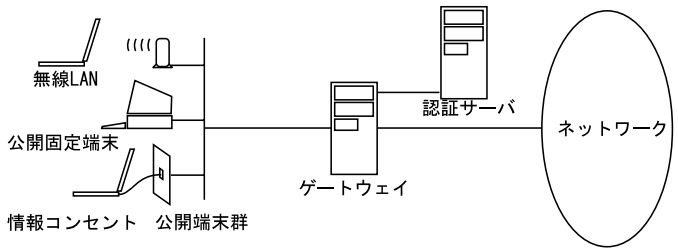

図 2: ハードウェアの構成

Opengate は、端末群と利用ネットワークとの間にゲートウェイを設置し、そこを通過する通信パケットをフィルタリングするシステムです（図 2）。利用者認証は認証サーバで行います。認証サーバは複数設置することが可能です。

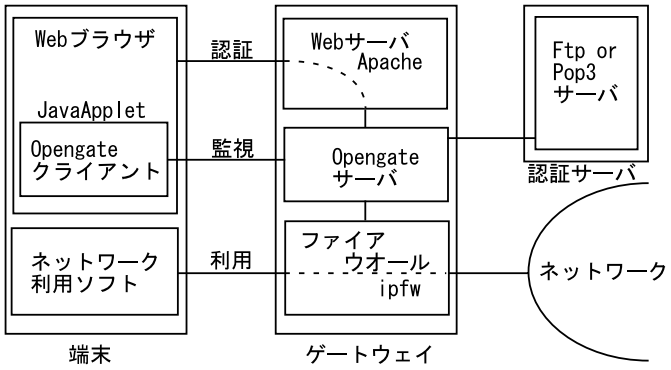

図 3: ソフトウェアの構成

ソフトウェアの構成を図 3 に示します。ファイアウオールは、閉鎖状態にある端末から任意のサーバに向けた Web アクセスを捕らえ、これをローカルの Web サーバへ振り向けます。Web サーバはこれに対して認証ページを送り返します。利用者が認証情報（ユーザ ID とパスワード）を返答すると、Web サーバは Opengate サーバ CGI を起動します。Opengate サーバ CGI は以下の処理を行います。認証情報を取得し認証サーバへ送ります。認証が通ると、ファイアウオールに規則を追加して、当該端末の通信パケットが通過できるようにします。また端末に Java アプレットを送り、それとコネクションを保持します。コネクションが切断された場合や Java アプレットが定期的チェックに返答しない場合、端末からの通信パケットが一定期間無い場合などには、ファイアウオールの規則を削除し、通過許可を取り消します。許可時および取り消し時には、その時刻とユーザ ID、アドレスなどを記録します。

5　特徴

このシステムは以下のような特徴を持っており、様々な環境で有効に利用することができます。

1. ゲートウェイのみを設定すれば良く、端末や HUB 等の分散した機器の事前設定が不要です。よって情報コンセントや無線 LAN に接続された持参 PC にも対応できます。Java が動く Web ブラウザがあれば良く、様々な OS の端末に対応できます。

2. ネットワークの電気的切断を検知するものではないため、常時ネットワークに接続されている公開固定端末にも対応できます。ただし、利用終了時には Web ブラウザを終了することが必要です。

3. Web ベースのユーザインターフェースであり、認証画面も自動的に表示されるため、ほとんど事前指導なしで簡単に利用できます。

4. ファイアウオールソフトを利用しており、通信制御の詳細な設定が可能です。例えば、特定アドレスに対する特定サービス要求を認証なしでも許可することなどが簡単にできます。

5. システムは、特殊なネットワーク機器を使用せず、汎用のソフトウェアとハードウェアで構成されているため、比較的安価に構築できます。

6. 既存システムのユーザ管理情報をそのまま利用でき、改めてユーザ登録をする作業が不要です。認証サーバも、ftp や pop3 を利用する方式ですので簡単に設置することができます。

7. 複数の認証サーバへユーザ認証を振り分けることができます。例えば、一時的な利用者に対して専用の認証サーバを用意し、他へ影響しない独自のユーザ管理体制を取ることなどもできます。

6　おわりに

本システムは、学術情報処理センターと知能情報システム学科の皆様の協力を得て開発を進めています。文化教育学部の皆様には試験運用に際してご迷惑をお掛けしました。ここに感謝いたします。

参考

[1] 利用者認証と利用記録機能を実現するゲートウェイシステム Opengate の開発、渡辺健次, 江藤博文, 只木進一, 渡辺義明, 信学技報 IN99-95, TM99-61, OFS99-48 (2000) 43-48.

[2] Opengate ホームページ、http://www.cc.saga-u.ac.jp/opengate/