2004－ＤＳＭ－33 (12)
2004／5／14

Opengateを利用した公開端末の認証および利用記録

安田 伸一† 羽石 寛志† 渡辺 健次‡ 渡辺 義明‡ 江藤 博文* 只木 進一*

†佐賀大学経済学部、‡佐賀大学理工学部、＊佐賀大学学術情報処理センター
〒840-8502 佐賀市本庄町大字本庄1

E-mail: †yasudas@cc.saga-u.ac.jp, hhiro@cc.saga-u.ac.jp
‡watanabe@is.saga-u.ac.jp, watanaby@is.saga-u.ac.jp
＊etoh@cc.saga-u.ac.jp, tadaki@cc.saga-u.ac.jp

あらまし ネットワーク利用者の認証と利用記録を行うOpengateを用いて、Windows公開固定端末のシステム利用開始時に認証を行う方法OpengateLogonを開発した。この方式では、Windows側に簡単なプログラムを導入するだけで、Windowsドメインなどを構築せずに、容易に認証および利用記録を行うことができる。本稿では、OpengateLogonについて紹介し、運用実験について報告する。

キーワード 公開端末の利用者認証、Opengate、OpengateLogon

Authentication and Logging at Public Terminals with the "Opengate" system

Shinichi YASUDA† Hiroshi HANEISHI† Kenzi Watanabe‡ Yoshiaki Watanabe‡
Hirofumi ETO* and Shin-ichi TADAKI*

† Faculty of Economics, Saga University, ‡ Faculty of Science and Engineering, Saga University
＊Computer and Network Center, Saga University 1 Honjo, Saga-shi, Saga, 840-8502 Japan

E-mail: †yasudas@cc.saga-u.ac.jp, hhiro@cc.saga-u.ac.jp
‡watanabe@is.saga-u.ac.jp, watanaby@is.saga-u.ac.jp
＊etoh@cc.saga-u.ac.jp, tadaki@cc.saga-u.ac.jp

Abstract This paper proposes "OpengateLogon", a user authentication system for public PCs with the "Opengate" system. The Opengate system is originally developed for authenticating users and recording connections for the Internet. The OpengateLogon system allows us to introduce a user authentication mechanism into PCs by installing simple programs without constructing Windows domains.

Keyword Authentication at Public Computer, Opengate System, OpengateLogon System

1. はじめに

学生用情報機器の設置要求に大学のさまざまな部局が個別に対応し、多くの大学では学生が自由に利用できるパーソナル・コンピュータ（以下、公開端末と呼ぶ）が大学全体に分散して設置されている。佐賀大学でも、多数の公開端末が附属図書館や学部などに設置されている。

学部などに設置される公開端末は利用者管理などを行わず、単に電源を入れるだけで自由に使える場合が多い。公開端末の利用に関する匿名性は、気軽に利用できる利点がある反面、悪意を持った利用も招く。

公開端末を利用した不正なアクセスや利用不能攻撃を防ぐには、コンピュータ・ネットワーク機能を利用した時点での利用者認証と通信制御を利用する方法がある。佐賀大学では、インターネットへの接続時にブラウザで利用者認証を行うゲートウェイ Opengate システムを開発し、2000 年に稼動させた[2][3]。これは既存の公開端末の設定を変更することなく、インターネット利用者を認証でき、その利用を記録できる。現在は、佐賀大学のすべての公開端末や教育用情報コンセント、教育用無線 LAN が Opengate システムに接続され、インターネット接続時の利用者認証を実現している[6]。

しかし、Opengate システムはネットワークを利用する際に認証および記録を行うシステムであるので、公開端末単体で実行される不正行為に対応できない。例えば、キーロガーによるパスワードの収集を予防できない。これに対応するには、公開端末のシステム利用開始時点で利用者を認証し、特定する必要がある。我々は、既存の Opengate 環境を利用して、公開端末に利用者認証機能を加える *OpengateLogon* を開発した。

今回、佐賀大学経済学部で運用実験を行った

OpengateLogon システムは、Opengate システムと通信する小さなアプリケーション・プログラムをパーソナル・コンピュータで実行し、佐賀大学学術情報処理センターの認証サーバで利用者認証を行うものである。従来、公開端末で利用されている Windows PC などで利用者認証を行う場合には、Windows ドメインやアクティブ・ディレクトリと大学の教育用情報基盤の利用者情報との同期を取る必要があり、パーソナル・コンピュータをマルチ・ユーザ用に構成する必要があった。この方法と比較して、OpengateLogon は、スタンドアロンでシングル・ユーザ用に設置されたパーソナル・コンピュータの構成をそのまま使って利用者を認証するため、設置が非常に簡便である。

本論文では、OpengateLogon システムを紹介し、運用実験の内容を報告する。第 2 章で利用者認証方法の考察を行う。第 3 章で Opengate システムの概要を紹介し、第 4 章と第 5 章で OpengateLogon システムの構成と設置を説明する。第 6 章で OpengateLogon システムを評価する。

2. 公開端末のセキュリティ確保

学生が自由に利用できる公開端末の多くは、全学の情報基盤を管理運営する組織とは別に、各学部などが独自に設置する。公開端末の中には利用者認証をまったく行わないなどセキュリティ上の問題点の残されているものがあり、設置者が別だとしても全学的な情報基盤の適切な運用のためにはセキュリティ上の制限を設ける必要がある。

全学的な情報基盤の運用のために必要な対策は、二つある（表 1)。一つ目は、公開端末の利用者を認証することによる利用者の把握である。利用者の認証により、部外者による利用を防止し、利用者の記録により不正利用の追跡が可能となる。

二つ目は、ファイアウォールによる不正なネットワーク利用の遮断である。ネットワークを不正に利用する端末を特定しファイアウォールで通信を遮断することにより、公開端末などを使ったネットワーク利用の不正利用を防止することができる。

2.1. 公開端末の利用者認証

多くの公開端末に利用されている Windows PC では、大学における公開端末の利用者認証の方法として、Windows の認証システムをそのまま利用する方法と Windows の認証ライブラリを拡張して教育用情報基盤の認証システムと連動させる方法とがある。

Windows の認証システムは、Windows XP/2000/NT をマルチ・ユーザ構成に設定し、Windows ドメインに参加させて実現する。この方法は、多くの公開端末がすでにシングル・ユーザ構成で設置されている場合には、多数の公開端末の構成変更作業が必要となり現実的ではない。また、多数稼動している Windows Me/98/95 に適用することができない。さらに、原則として認証サーバに Windows サーバを利用しなくてはならないために、大学の既存の情報基盤との共通化が困難である。このため、既存の公開端末のセキュリティ確保に利用するには困難が多い。

Windows の認証ライブラリを拡張して利用者認証する方法は、Nigel Williams の NISGINA[1]を情報処理教育環境に適用した古瀬らの報告[5]や、丸山の CO-GINA[7] などが知られている。認証ライブラリを拡張することで Windows サーバ以外の認証サーバを利用することができ、大学の情報基盤との共通化が可能になる。しかし、動作中のライブラリの入れ替えは不可能であるなど、導入には専門的な知識が必要であり、全学的な利用にはサポートが欠かせない。

2.2. 不正な通信の遮断と追跡

ネットワークの不正な利用による通信を遮断するには、通常のファイアウォールがあればよい。しかし、通常のファイアウォールで通信を遮断する場合の問題点は、不正な利用の行われた公開端末を特定するために、複数のログを突き合せなくてはならないことである。例えば、DHCP で不特定の IP アドレスが割り当てられている場合に端末を特定したり、特定の時間の利用者を確定するには、ファイアウォールのログだけでは情報が不足する。

我々の開発した Opengate システム[2][3]は、利用者認証を受けてファイアウォールの開閉を行うシステムである。このシステムでは通信と利用者の対応がファイアウォールのログとして記録されるので、不正な利用を発見し通信を遮断した後で迅速に対応することができる。

3. Opengate システム

表 1　公開端末の利用者認証

防止する事柄	方針	対策
部外者による利用の防止 他の利用者の情報収集	利用者の把握	公開端末の利用者認証
不正アクセス 利用不能攻撃　など	不正な通信の遮断	ファイアウォールによる通信の遮断

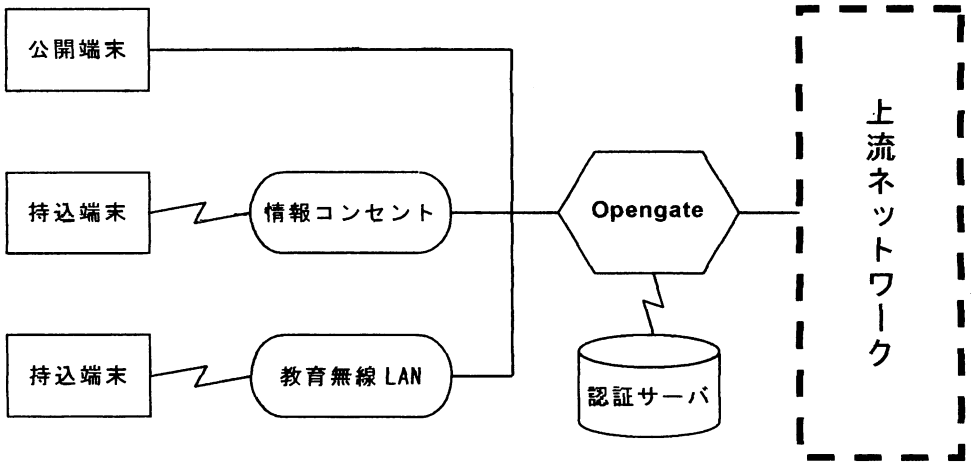

図 1　Opengate システムの構成

Opengate システムは、ネットワーク利用時にブラウザで利用者認証を行うネットワーク・システムである。

Opengate システムには、端末の認証を行うネットワーク（認証ネットワークと呼ぶ）と上流のネットワーク、両者をつなぐゲートウェイ（Opengate と呼ぶ）、認証サーバがあり、図 1 のように構成される。

認証ネットワークに接続された機器（認証端末と呼ぶ）は、Opengate の DHCP 機能により IP アドレスが割り当てられる。この状態では、認証端末は上流ネットワークと通信できない。

認証端末が上流ネットワークへ HTTP（80 番）で通信を行うと、Opengate はこの通信を横取りして公開端末に認証画面を表示する。入力されたユーザ名とパスワードを認証サーバで照合し、認証されるとその認証端末と上流ネットワークとの通信を許可するルールをファイアウォールに追加する。

公開端末のブラウザが Java アプレットを実行できる場合には、Java アプレットの停止によってファイアウォール・ルールが削除される。Java アプレットが実行されない場合には、通信の有無にかかわらず、20 分後にファイアウォール・ルールが削除される。

なお、認証端末として、公開端末のほかに、情報コンセントや無線 LAN に接続される持ち込み端末も接続できる[4][8]。

4. OpengateLogon システム

OpengateLogon システムは、*Windows* で構成される公開端末の利用開始時に Opengate による利用者認証を行うシステムである。OpengateLogon システムは、ネットワーク上に構築された Opengate システムと、そのネットワーク下に設置された公開端末上で稼動する OpengateLogon プログラムからなる。

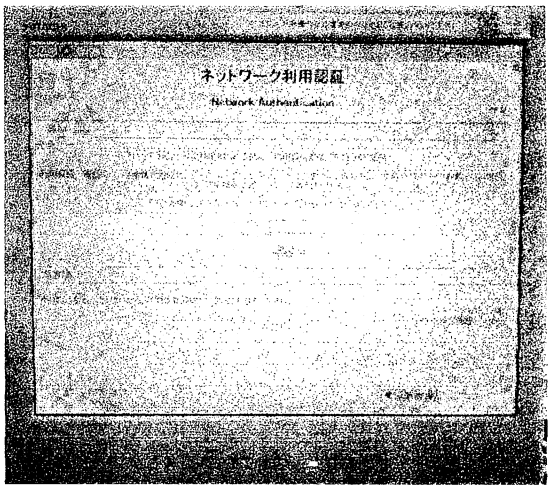

図 2　OpengateLogon 認証画面

OpengateLogon プログラムは、Visual Basic で作成された実行ファイルと Visual C++ で作成された DLL ファイルからなる。この 2 つを任意のフォルダに置くだけで動作する。Web ブラウザ動作に Internet Explorer のモジュールを利用するため、公開端末上には Internet Explorer が導入されていることが必要である。

OpengateLogon プログラムは、起動するとタスク・バー、メニュー・バーを消し、Windows キーを無効にして、全画面を占有した後に Web ブラウザとして動作する。よって Opengate システムの下では画面上に Opengate の認証要求ページが表示される（図 2）。その後も、Opengate の認証許可ページが受信されるまで、Web ブラウザとして動作する。認証許可ページが受信されたことをページ記述から認識すると、表示画面を

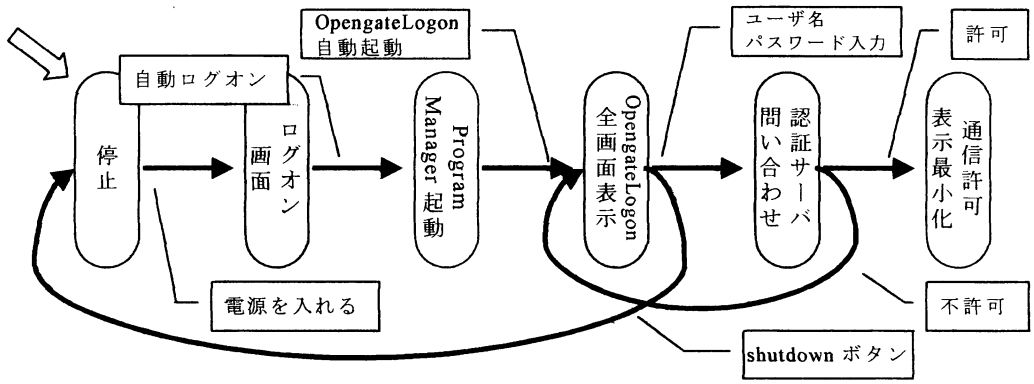

図 3　OpengateLogon システムの状態遷移

最小化して常駐し、通常の Windows 操作を可能とする。最小化したプログラムは Opengate システムと TCP 接続を保っており、システム終了時にこの接続が切れることによりファイアウォールの閉鎖が起きる。

以上の動作を既存の Opengate システムに変更を加えずに実現した。このプログラムを公開端末のシステム起動時に動くように設定することで、システムの利用認証を行う。なお、利用者が認証できない場合も考えられるのでシャットダウンボタンを用意した。

5. 設置例

OpengateLogon システムは、現在、経済学部の公開端末に設定して、試験運用を行っている。ここでは、経済学部公開端末での具体的な設定を示す。

5.1. 起動までの流れ

OpengateLogon システムが設定された Windows 公開端末では、電源を投入すると Windows の自動ログオン機能を利用して公開端末用ユーザ名でログオンし、OpengateLogon が自動起動される（図 3）。

起動した OpengateLogon プログラムはタスク・バーなどを消した Windows の全画面表示で表示され、Opengate ゲートウェイと通信して認証画面を表示する。入力されたユーザ名とパスワードが認証されると最小化表示に変わり、通常の利用ができるようになる。

5.2. Windows の種類

Windows 2000 SP4 を利用している。

Windows 2000 を利用するのは、学術情報処理センター演習室に設置された Windows にあわせるためと、読み出し専用の移動プロファイルを利用するためである。移動プロファイルとは、Windows ログオン時に C:¥Documents and Settings 以下のユーザ個人用ディレクトリを指定された場所からコピーする機能である。これを読み出し専用にすると、利用中の設定変更は可能だが、ログオフ時にすべての変更は破棄される。

経済学部の公開端末では、標準ユーザに設定した公開端末用共通仮想ユーザの移動プロファイルを読み出し専用に設定していて、ログオン時に必ず初期設定で開始される。なお、マイ・ドキュメントが初期化されると不便なので、ここだけは初期化されない。

5.3. 自動ログオン

Windows 2000 での自動ログオンは、標準の機能である。コントロール・パネルの「ユーザとパスワード」を開き、「このコンピュータを使うには、ユーザー名とパスワードを入力する必要があります」を解除すれば、自動ログオンが設定できる。

5.4. OpengateLogon の自動実行

ログオン時の自動実行には、いくつもの方法がある。例えば、スタート・メニューのスタートアップ・フォルダの登録、タスク・スケジューラの登録、レジストリの登録などがある。

今回は試験運用であり、構成変更の容易さを考慮して、共有ユーザのスタートアップ・フォルダに登録した。スタートアップ・フォルダはユーザにより編集可能だが、上に示したように編集結果は破棄されるので、もし編集されたとしても初期設定どおりに OpengateLogon は必ず実行される。

5.5. タスク切り替えの無効化

OpengateLogon プログラムはキーボード操作を監視し、Ctrl-Esc や Windows キーなどのタスク切り替えを伴うキー操作を禁止する。しかし、Ctrl-Alt-Del で表示されるセキュリティ・ウィンドウの表示をプログラムで禁止することはできないので、別にセキュリティ・ウィンドウ対策が必要になる。

セキュリティ・ウィンドウで表示される機能は、ロック、ログオフ、シャットダウン、パスワードの変更、タスク・マネージャの五つである。このうち、レジストリを変更することによりタスク・マネージャの起動を禁止する。ただし、このレジストリを変更するには Administrators 権限が必要なので、一時的に権限を変更

してレジストリを変更する。

```
HKEY_CURRECT_USER¥Software¥Microsof
t¥Windows¥CurrentVersion¥Policies¥S
ystem¥DisableTaskMgr=dword:00000001
```

5.6. Java 環境のインストール

現在、経済学部の Windows 2000 で利用できる Java 環境には Microsoft VM と Sun Plug-in がある。今回は Microsoft VM を利用した。

5.7. 自動シャットダウンの設定

偽の OpengateLogon 認証画面などによるパスワードの盗難を避けるために、必ず自分で電源を入れるように利用者指導を行っている。このため、電源を入れたまま放置される公開端末が増えると、学生にシャットダウンの時間を余分に待たせることになり、自分で電源を入れるルールが守られなくなると予想した。

そこで、タスク・スケジューラとシャットダウン・ユーティリティを利用して、10 分間の無操作で 5 分間の遅れを設定したシャットダウン・ユーティリティを起動する。これにより 15 分の無操作で自動的に電源が切れ、通常の利用では、電源が切れた状態で公開端末が提供されるようにした。

6. 考察

OpengateLogon システムで公開端末の利用者を認証するには、スタンドアロンで運用されている公開端末の一台一台に OpengateLogon プログラムをインストールし、その他に第5章の作業を行わなくてはならない。

しかし、この作業は、公開端末をマルチ・ユーザ構成に変更し、既存の利用者情報と Windows 認証サーバの利用者情報との同期を取り続けなくてはならない Windows 認証をそのまま利用する方法に比べて、作業量が少ないといえる。

また、さまざまな構成の公開端末で事前に動作確認を行わなくてはならない Windows 認証ライブラリを交換する方法に比べて、他のアプリケーション・プログラムとの関わり合いを考慮する必要がない点が有利である。したがって、導入に必要な準備や個々の作業量は他の利用者認証の方法と比べて少ないといえる。

加えて、OpengateLogon による利用者認証は Opengate システムに組み込まれるために、二つの利点が生まれる。一つ目は、Opengate システムのファイアウォール機能が使える点である。コンピュータ・ネットワークの不正防止では、自システムを守ることと同様に他システムを攻撃させないことも重要である。不正な利用者の追跡が容易な Opengate システムを利用することで、社会的な責任を果たしているといえる。

二つ目の利点は、Opengate システムのオープンな認証システムにより、大学の情報基盤の認証システムを利用できることである。

シングル・ユーザ構成で機能的に充分な公開端末に利用者認証を必要とする最大の理由は、公開端末に仕掛けられる情報収集ソフトウェアの排除である。例えば、キー入力の監視によるパスワードの盗難を防がなくてはならない。OpengateLogon を設置したとしても、例えば古典的な偽のログオン画面によるパスワード盗難を防ぐことはできない。したがって、「利用者は必ず自分で電源を入れる」という利用者指導を欠かすことはできない。

7. むすび

OpengateLogon のインタフェースは佐賀大学では見慣れた認証画面なので、経済学部に設置された公開端末の利用に混乱は見られなかった。これは、認証システムを全学的に統一することの重要性を示している。

今後、二ヶ月程度の期間をおいて利用状況を調査し、問題点を整理する予定である。

文　献

[1] Nigel Williams, http://www.dcs.qmw.ac.uk/~williams/

[2] 渡辺健次,江藤博文,只木進一,渡辺義明,"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," 信学技報 IN99-95, TM99-61, OFS99-48 pp.43-48, 2000.

[3] 渡辺義明, 渡辺健次, 江藤博文, 只木進一, "利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発," 情報処理学会論文誌, Vol42, No.12, pp.2802-2809, 2001.

[4] 只木進一, 江藤博文, 渡辺健次, 渡辺義明, "公開端末及び利用者移動端末の認証システムとそのディスクレスマシンによる運用," 学術情報処理研究, No.5, pp.15-20, 2001.

[5] 古瀬一隆, 坂口瑛, "UNIX と Windows を統合した情報処理教育環境の構築," 学術情報処理研究, No.5, pp.21-30, 2001.

[6] 江藤博文, 只木進一, 渡辺健次, 渡辺義明, "新しい教育用情報基盤の実現へ向けて－認証システムをベースとしたキャンパス規模のオープンネットワーク," 学術情報処理研究, No.6, pp.13-20, 2002.

[7] 丸山伸, "CO-GINA による Windows 認証のカスタマイズ," http://www.co-conv.jp/product/co-gina/, 2003.

[8] 只木進一, 江藤博文, 渡辺健次, 渡辺義明, "利用者移動端末に対応したネットワークの運用 -佐賀大学での *Opengate* の運用-," 情報処理学会シンポジウムシリーズ, Vol.2004, No.3, pp.85-90, 2004.