Opengate 認証の公開端末への適用

Application of the "Opengate" System to Public Terminals

安田伸一　羽石寛志　　江藤博文　只木進一　　渡辺健次　渡辺義明
佐賀大学経済学部　　佐賀大学学術情報処理センター　　佐賀大学理工学部
佐賀市本庄町大字本庄１　〒840-8502

Shinichi YASUDA　　Hiroshi HANEISHI
Faculty of Economics, Saga University
yasudas@cc.saga-u.ac.jp　　hhiro@cc.saga-u.ac.jp

Hirofumi ETO　　Shin-ichi TADAKI
Computer and Network Center, Saga University
etoh@cc.saga-u.ac.jp　　tadaki@cc.saga-u.ac.jp

Kenji WATANABE　　Yoshiaki WATANABE
Faculty of Science and Engineering, Saga University
watanabe@is.saga-u.ac.jp　　watanaby@is.saga-u.ac.jp

1 Honjo, Saga city, Saga 840-8502 JAPAN

概要

Opengate は、ネットワークの利用時に情報機器の利用者認証を行うネットワーク・システムである。公開端末の利用者認証として Opengate を利用したとき、電源を入れてからネットワークを利用するまでの時間帯は匿名で公開端末を利用でき、キーロガーの起動など不適正に利用される危険性が生じる。公開端末の匿名利用をなくすために、OpengateLogon を開発した。これは、Windows の稼動する公開端末に小さなプログラムを導入することにより、公開端末の利用開始時点で Opengate 認証を行なう。

キーワード

公開端末の利用者認証、Opengate、OpengateLogon

Abstract

The ″Opengate″ system is a network gateway system for the user authentication and usage logging. The ″Opengate″ system authenticates the user at accessing to the network. But one can use anonymously a public PC without a user authentication until accessing to the network. This causes a risk to be set a trap like a key-logger. This paper proposes the ″OpengateLogon″ system, an authentication system for a public PC with the ″Opengate″ system. This system allows us to introduce a startup authentication mechanism and to prevent an anonymous use.

Keywords

authentication at public computer, the Opengate system, the OpengateLogon system

1. はじめに

佐賀大学経済学部には、学生が自由に利用できる自習用コンピュータ(以下、公開端末)が設置されている。2003 年 10 月に、経済学部の公開端末から利用者 ID とパスワードが盗まれ、実際に使用される事件が発覚した。

事件に利用された公開端末では、ログオン時に設定が初期化され、利用者による設定の変更が破棄されるようになっていた。また、Opengate によるネットワーク利用の利用者記録が残されていた。ここで、Opengate とは、ネットワークの利用開始時にブラウザで利用者認証を行い、ネットワークの利用記録を行うネットワーク・システムである [1][2][3]。

しかし、ログオン後でネットワーク利用開始前に匿名で利用できる時間帯が存在する。この匿名の時間帯にキーボード入力記録ソフトウェアが起動され、そのまま無人となった公開端末をあとから利用した者の利用者 ID とパスワードが盗まれた。これは、公開端末において匿名で利用できる時間帯の危険性を認識していなかった結果であり、この問題に対応する必要性が明らかになった。

この事件を受けて、佐賀大学では二つの対策を行った。一つ目の対策として、電源が入ったままの公開端末を利用することの危険性を周知した。

二つ目の対策として、公開端末の匿名利用の時間帯をなくす OpengateLogon を開発し、経済学部において試験運用を始めた。

本論文では、ネットワーク管理の点から持込端末と公開端末の違いを考察し、Opengate において不備であり、OpengateLogon において付加した機能を明らかにする。また、現在、経済学部で試験運用中の OpengateLogon の設置例を報告する。

2. 適正なネットワーク利用の確保

2.1 Opengate

Opengate は、ネットワークの利用開始の時点にブラウザで利用者認証を行い、ネットワークの利用記録を行うネットワーク・システムである。

Opengate には、端末の認証を行うネットワーク(利用者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、認証サーバがあり、図 1 のように構成される。

利用者ネットワークに接続された機器(利用者端末と呼ぶ)は、ゲートウェイの 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、利用者端末は上流ネットワークと通信できない。利用者端末が上流ネットワークへ HTTP(80 番)で通信を行うと、ゲートウェイはこの通信を横取りして利用者端末に認証画面を返す。利用者が入力したユーザ名とパスワ

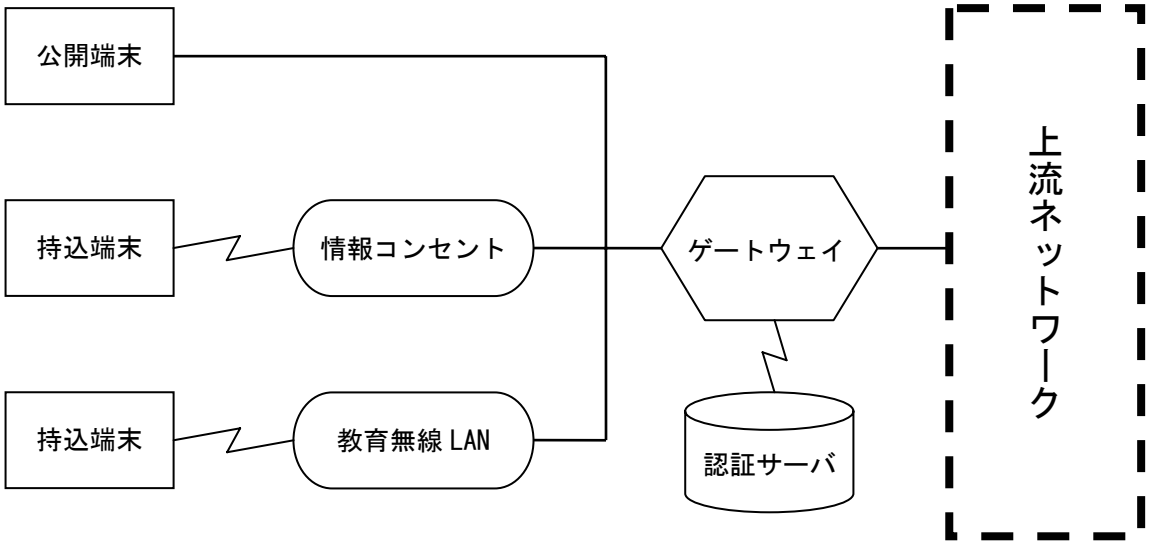
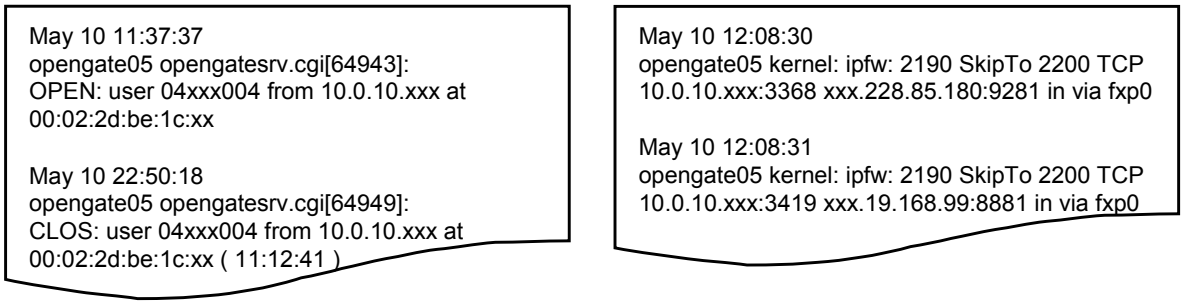


図 1　Opengate の構成



(A) 認証ログ　　(B) ファイアウォール・ログ

図 2　不適正なネットワーク利用の追跡

ードを認証サーバで照合し、認証に成功するとその利用者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。さらに、利用者端末に Java アプレットを送り、ゲートウェイとの間で TCP 接続を確立して、ブラウザの終了を監視する。Java アプレットの停止や利用者端末の終了などによって TCP 接続が切断されると、ゲートウェイはファイアウォール・ルールを削除する。Java アプレットが実行されない場合には、20 分後にファイアウォール・ルールが削除される。

Opengate は、接続される利用者端末に Web ブラウザがあれば利用者認証を行えるので、公開端末でのネットワーク利用の認証のほかに、個人所有のネットワーク機器（持込端末と呼ぶ）を大学の情報基盤に接続する場合にも利用できる。

Opengate と同様にネットワーク利用時にファイアウォールを制御する利用者認証には、丸山らや久長らの方法、広島大学の方法が知られている。

丸山らによる情報コンセントシステム［4］は、Opengate と同様にネットワークの利用開始時点でブラウザを使って利用者認証を行う。しかし、ネットワーク利用停止をポーリング動作によって検出しているため、Opengate で実現しているネットワーク利用停止後のファイアウォールの即時閉鎖ができない。また、認証手順が NIS に限られているので、既存の情報基盤に導入する場合に制限がある。

久長らによる情報コンセントのユーザ認証システム［5］や広島大学における PortGuard システム［6］では、ネットワークの利用のために指定された Web ページを開いてユーザ認証を行う。この方法は、学部や図書館などが公開端末を設置する場合や、持ち込まれる私物のパソコンで大学の情報基盤を利用する場合などに備えて、認証用の Web ページの参照を周知しなくてはならない。Opengate では、任意のネットワーク・アクセスが認証画面へ切り替わるので、認証画面の参照を義務づけなくてもよい分、運用の負担が小さい。

なお最近では、認証機能を持ったネットワーク・スイッチが各種商品化されている。しかし現状では、ユーザの利便性、多様な端末との互換性、価格等の面で未だ問題を持つものが多数である。また、端末からの集線部分に設置する方式では、広範囲に設置すると導入と維持のコストが大きくなる。

2.2　適正なネットワーク利用の実現方法

ネットワークの利用を適正に保つためには、次の二点を実現しなければならない。

- 部外者によるネットワーク利用を禁止すること
- 正規の利用者による不適正なネットワーク利用が追跡できること

ここで、正規の利用者のネットワーク利用の追跡とは、事件などが発覚した際に過去にさかのぼってネットワーク利用の記録を追跡でき、事後に利用者を特定できることを示す。

部外者によるネットワーク利用を禁止するためには、コンピュータ・ネットワークの利用時の利用者認証が有効である。佐賀大学では、教室や附属図書

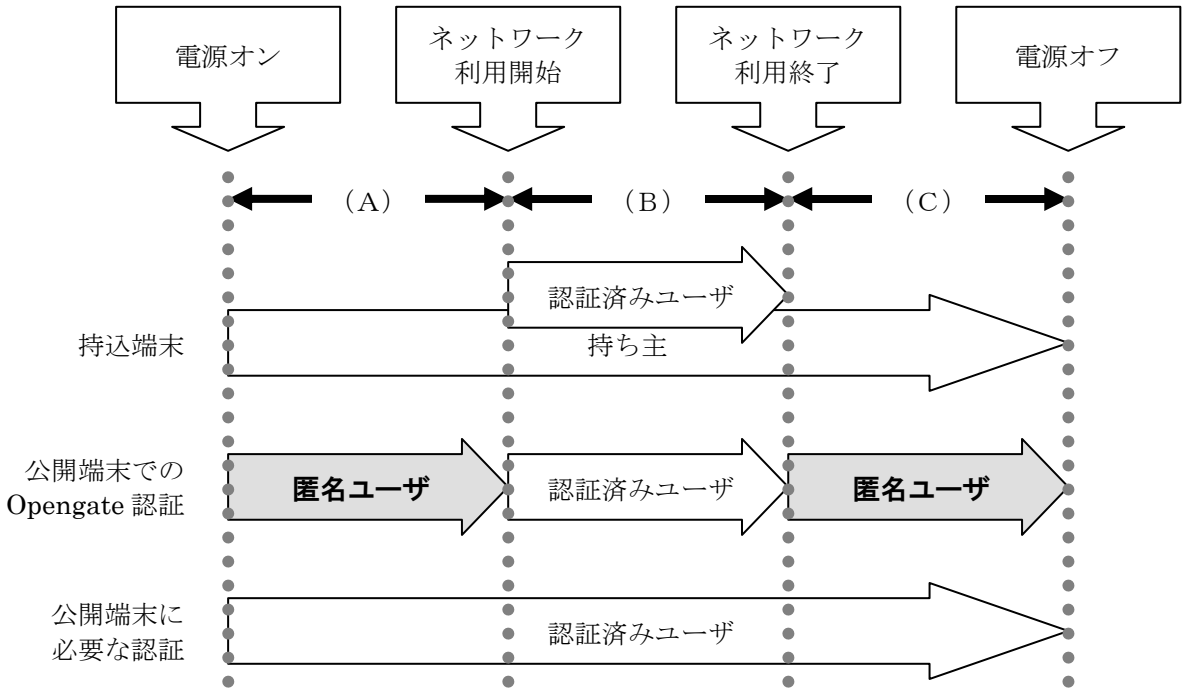


図 3　匿名時点の発生

館など不特定の人物がネットワーク機器を利用できる場所に利用者用ネットワークを配置し、ネットワーク利用時に利用者認証を行っている。

Opengate ゲートウェイは、利用者ネットワークに接続される端末への IP アドレス配布とネットワーク利用時の利用者認証、ファイアウォール機能を一体のシステムで提供するために、利用者記録とネットワークの利用記録を連携させ、容易に利用者と端末、時刻を抽出できる。例えば、利用者 ID が盗まれた場合には、認証ログによって盗まれた利用者 ID の使われた端末を特定し、ファイアウォール・ログによって通信の内容を調べることができる(図 2)。

このように、Opengate は、部外者によるネットワークの利用を禁止し、正規の利用者による不適正なネットワークの利用を追跡できる。

3. 公開端末での利用者認証の必要性

Opengate は、ネットワーク利用時の利用者認証に成功した時刻を利用開始として記録し、ブラウザを閉じた時刻を利用の終了として記録する。持込端末の場合、持ち込まれた機器は個人所有であるから、図 3 の A や C の時間帯も認証済みの B と同じユーザが利用しているとみなせる。

しかし、公開端末の場合には、大学に設置された機器を利用するので、電源を入れたまま席を離れるなどによって、A と B、C のユーザの一貫性が保障されない。例えば、A の時点の匿名ユーザが情報収集ソフトウェアを起動して席を離れると、Opengate に利用者記録を残さないで B や C の時点の利用者情報を収集できる。

このため、公開端末の場合、Opengate によるネットワーク利用開始時点での利用者認証では不十分であり、システム起動時から利用者の記録を取る必要があることがわかる。

4. OpengateLogon

学内全体には認証なしで利用できる多数の Windows 公開端末がある。OpengateLogon は Windows で構成される公開端末を対象として、システム起動時に Opengate による利用者認証を行う。この OpengateLogon は、ネットワーク上に構築された Opengate と、その利用者ネットワークに設置された

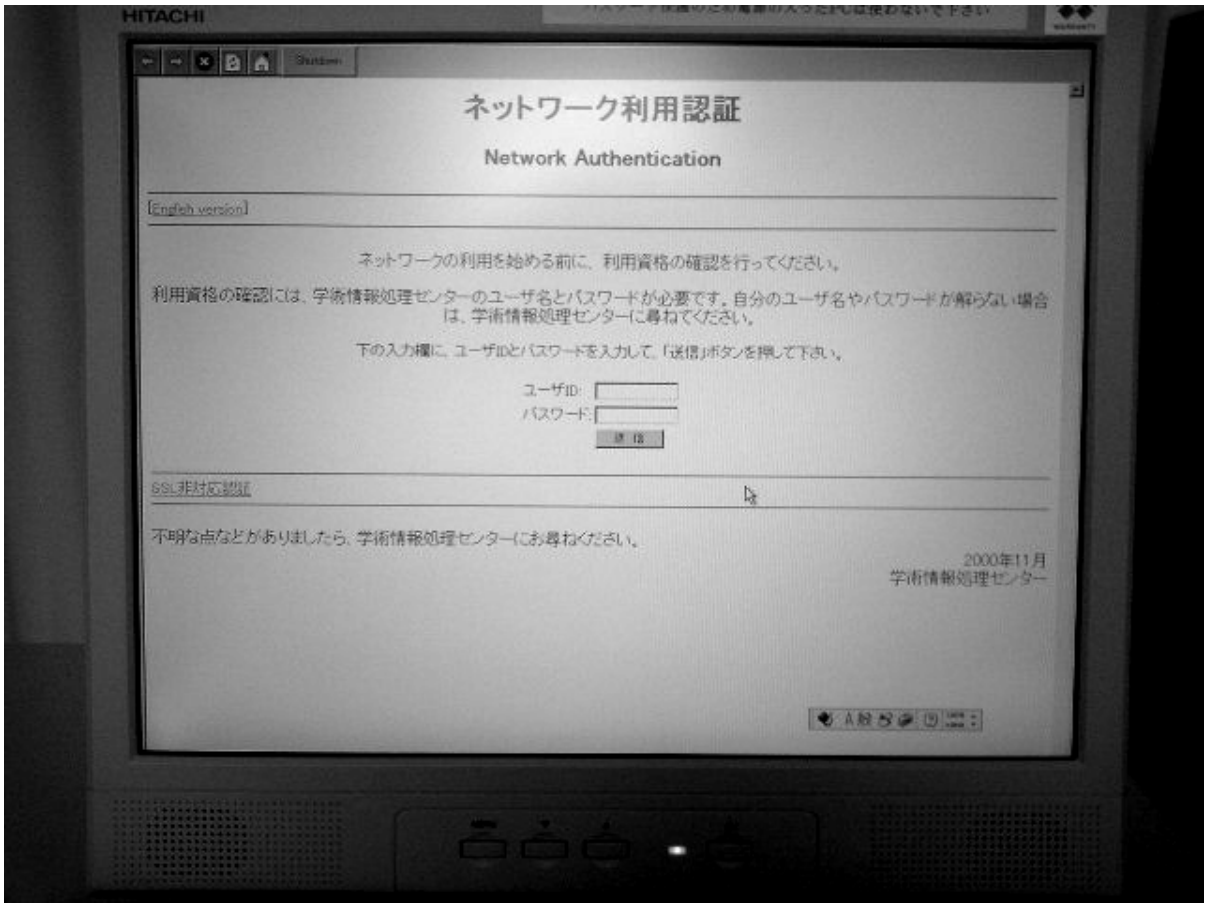


図 4　OpengateLogon の起動

Windows 公開端末上で稼動する OpengateLogon プログラムからなる。

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いて動作させる。ただし、Web ブラウザ動作に Internet Explorer のモジュールを利用するため、公開端末に Internet Explorer が必要である。

OpengateLogon プログラムは、Windows のユーザ認証機構を利用しないので、Windows XP/2000/NT と同様に Windows Me/9x でも動作する。

OpengateLogon プログラムは、起動するとタスク・バーとメニュー・バーの非表示、Windows キーの無効化、全画面の占有の後、Web ブラウザとして動作して画面上に Opengate の認証要求ページを表示する(図 4)。利用者の認証後、認証許可ページの受信を認識すると表示画面を最小化して常駐し、これ以降は通常の Windows 操作を許可する。最小化したプログラムは Opengate 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とファイアウォールが閉鎖される。なお、OpengateLogon プログラムは利用者の操作による終了ができない。

このプログラムを公開端末の利用開始時に動作させることで、公開端末の利用者認証を行う。なお、認証できない利用者が電源を入れる場合も考えられるので、画面上にシャットダウン・ボタンが用意される。

5. 設置例

OpengateLogon は、佐賀大学経済学部の公開端末に設定して、試験運用を行っている [7]。試験運用中の 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、画面を占有する

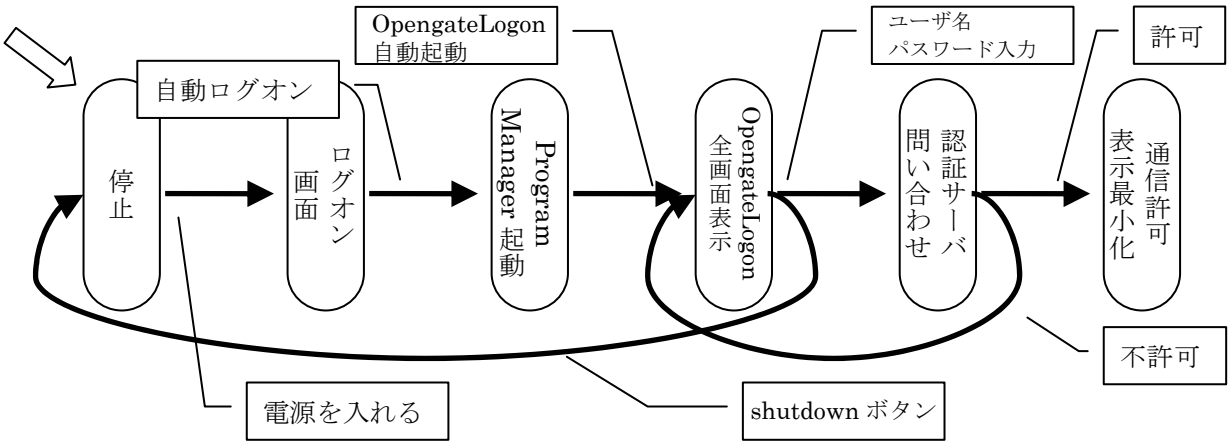


図 5　OpengateLogon の状態遷移

OpengateLogon が自動起動される(図 5)。

公開端末は Windows 2000 SP4 である。自動ログオンによって、標準ユーザに設定した公開端末用ユーザにログオンする。OpengateLogon の自動実行は、タスク・スケジューラの「ログオン時の実行」を利用する。さらに、OpengateLogon プログラムが強制終了されないために、セキュリティ・ウィンドウからのタスク・マネージャの起動を禁止した。

6. 考察

6.1　匿名利用の危険性の認識

佐賀大学の場合、冒頭の事件が発覚するまで学部や学科などが設置する公開端末では、機器の利用に関する利用者認証を行ってこなかった。これは、匿名での利用の危険性を理解していなかったためである。佐賀大学経済学部でも、機器の構成変更を防ぐ手段と Opengate によるネットワーク利用の利用者認証を併用していたが、電源投入時の匿名での利用には注意を払っていなかった。

しかし、匿名で利用される公開端末には、情報収集用ソフトウェアの実行など、不適正に機器を利用される危険性があることがわかった。

6.2　Opengate と OpengateLogon の併用

Opengate は、大学のネットワークに接続される情報機器に Web ブラウザがあるだけで、その設定をまったく改変することなく、大学の情報基盤の認証システムを使ったネットワークの利用者認証と利用の記録を行うことができる。したがって、Opengate を大学のネットワークに用意すれば、学生や教員の私物の情報機器などの学内での利用を容易に許可できる[8][9]。しかし、公開端末では、ネットワークを使わなければ匿名で利用でき、Opengate では不適正な機器の利用を防げない。

匿名で利用された公開端末を引き続き利用する危険性を避けるには、電源の入った公開端末を利用しないという、利用者指導が有効である。しかし、これだけでは不十分である。

OpengateLogon は、公開端末の匿名利用を許さない。また、不適正に公開端末が使われたとしても、その利用者を追跡できる。これは、悪意のある利用を牽制する効果もある。

このように、OpengateLogon は、Opengate では不足であった、公開端末の不適正な利用の危険性をなくすことができる。

6.3　容易な利用者認証の必要性

設置の容易な利用者認証の方法がなかったことも、匿名での公開端末利用が容認された原因のひとつである。これを解決するためには、さまざまな部局が設置した既存の公開端末と設置済みのネットワーク機器に適用でき、大学の情報基盤として整備済みの認証システムを利用できなければならない。

利用者を認証しない公開端末の危険性は、すべての部局の公開端末に共通の危険性である。したがって、公開端末の利用者認証は、情報センターの管理する公開端末だけでなく、全学的に展開されなければならない。そのためには、既存のパーソナル・コンピュータやネットワーク機器に適用できる認証方法でなくてはならない。

また、大学の認証システムは、情報センター固有の業務から、教務や図書館システム、知財管理、経理など学内の多数の機関で共通に利用される重要な基幹的基盤となった。したがって、公開端末の利用者認証も大学の認証システムを共通に利用する必要があり、認証システムの互換性が重要となる。

本論文で報告した OpengateLogon は、Opengate と通信する小さな Windows プログラムをパーソナル・コンピュータで実行し、Opengate の機能を使って利用者認証を行う。OpengateLogon プログラムは、Windows 固有の利用者認証を持つマルチ・ユーザ用の Windows（Windows XP/2000/NT）だけでなく、シングル・ユーザ用の Windows（Windows Me/98）でも動作する。このため、Windows で稼動する既存の多数の公開端末に適用することができる。

また、OpengateLogon や Opengate は、インターネット上の標準的なプロトコルで公開端末や認証システムと通信する。このため、既存のネットワーク機器と認証システムを、そのまま利用できる。

さらに Opengate を利用する利点として、次の二点が挙げられる。一つ目の利点は、図 1 のゲートウェイを情報センターなどに集中設置できることである。これに加えて、ディスクレスブートの導入によっても管理負担を軽減できる [3]。二つ目の利点は、利用者認証とネットワーク利用の記録がひとつのシステムに統合されるため、独立した認証システムに比べて、利用状況の追跡が容易なことである。

このように、OpengateLogon と Opengate の組み合わせは、公開端末の利用者認証を全学展開する上ですぐれた方法であることがわかる。

6.4 他の利用者認証方法との比較

Opengate と同様にネットワーク利用時に利用者認証してファイアウォールを制御する方法は、冒頭で紹介した。この他に、公開端末で利用者認証する方法には、次のようなものがある。

1. Windows 固有の利用者認証の利用
2. Windows の認証ライブラリの交換

Windows 固有の利用者認証を利用する方法には、三つの問題がある。一つ目の問題は、Windows 固有の利用者認証の互換性の問題である。上で述べたように、利用者認証の互換性は重要であり、既存の認証システムと Windows 認証を協働させるためには、認証情報の同期を行わなければならない。二つ目の問題は、シングル・ユーザ構成で十分に役に立っている公開端末を、認証のためだけにマルチ・ユーザ構成に変更し、さらに Windows ドメインに登録しなければならないことである。Windows ドメインへの登録にはドメイン管理者の権限が必要であり、すべての公開端末の設置にセンター管理者の派遣が必要となる。三つ目の問題は、シングル・ユーザ用 Windows で稼動する多数の公開端末が存在することである。Windows 認証ではシングル・ユーザ用 Windows での利用者認証ができない。また、公開端末認証の問題ではないが、事前に端末を Windows ドメインに参加させる方法では、持ち込み端末の認証に対応できない。

Windows の認証ライブラリを交換する方法 [10][11][12] は、既存の認証システムと通信できる点で OpengateLogon と同等である。しかし、OS の基盤的なライブラリを交換するために、他のアプリケーション・プログラムとの互換性を確認しなければならない。また、シングル・ユーザ用 Windows での利用者認証ができず、認証ライブラリの交換を拒否する持ち込み端末も認証できない。

7. むすび

佐賀大学経済学部の公開端末に設置した OpengateLogon は、2004 年 3 月以降、約 5 ヶ月間に

わたって試験稼動させ、ほぼ問題なく動作している。まれに、OpengateLogonプログラムがOpengateゲートウェイと接続できない場合がある。これは、直前にWindowsの異常終了などによりOpengateが利用終了を検出できず、ネットワークが即時閉鎖されないときに起きる。この場合も、しばらく待つとOpengateの遅延閉鎖が働くために、特に対策を立てていない。公開端末を使おうとした学生は、認証画面が表示されないと別の公開端末に移って利用している。

経済学部の公開端末は、春休み期間にOpengateLogonを使う運用方法に変え、使い方の変更点などの掲示を行った。しかし、Opengate 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、公開端末の使い方の変更による混乱はまったくなかった。これは、認証システムの全学的な統一の重要性を示している。

学術情報処理センターでは、公開端末を多く設置している附属図書館への OpengateLogon の導入を検討している。また、経済学部では、授業用のパソコンへの導入を予定している。

学内には OpengateLogon で利用者認証を行うWindows PC の他に、各種の UNIX や Mac OS で稼動する公開端末がある。今後、これらの OS で稼動する公開端末への適用も検討する。

文　献

[1] 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.

[2] 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, Vol.42, No.12, pp.2802-2809, 2001.

[3] 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.

[4] 丸山伸, 浅野善男, 辻斉, 藤井康雄, 中村順一,“既存の DHCP 端末で利用できる利用者にも管理者にも安全な情報コンセントシステムの構築,” 情報処理学会研究報告 99-DSM-14, pp.131-136, 1999.

[5] 久長穣, 岡田隆, 刈谷丈治,“情報コンセントのユーザ認証について,” 学術情報処理研究, No.2, pp.77-81, 1998.

[6] 広島大学総合情報処理センター, “PortGuard,” http://www.portguard.org/, 2001.

[7] 安田伸一, 羽石寛志, 渡辺健次, 渡辺義明, 江藤博文, 只木進一, “Opengate を利用した公開端末の認証および利用記録,” 信学技報, TM2004-12, pp.7-11, 2004.

[8] 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.

[9] 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.

[10] Nigel Williams, http://www.dcs.qmw.ac.uk/~williams/, 1997. （The Internet Archiveで参照できます。 http://web.archive.org/web/*/www.dcs.qmw.ac.uk/~williams/）

[11] 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.

[12] 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.