Opengate の IPv6 対応に関する研究

江口勝彦 †　渡辺健次 ‡

概要

佐賀大学において, 利用者認証と利用記録を行うためのゲートウェイシステム「Opengate」が開発された. Opengate は, Web アクセスによって認証画面が提供される平易なインタフェースを持つ. 認証には POP3 や FTP サーバを利用することができる. 認証によって, 利用者端末には Java Applet が送信され利用状況を監視し, 利用が終了すると即時に通信路を閉鎖する. このような方法により, 利用者端末には特殊な環境を必要とせず事前設定をすることなく端末を利用することができる. 本研究では, 以上の特徴を保持しつつ Opengate を IPv6 に対応させる研究を行った.

キーワード: Opengate, IPv6, ネットワーク認証, ファイアウォール, Java

Implementation of IPv6 Functions for Opengate

Katsuhiko Eguchi †　Kenzi Watabe ‡

Abstract:

"Opengate" is a gateway system for network users. This system has functions of user authentication, access control according to the authentication and logging of their usage. Opengate has a simple user interface via a Web browser. When the user enters his/her own user ID and password to the interface, the system tries to authenticate using authentication mechanism such as POP3, FTP and so on. After the authentication success, the system allows the user uses the network. Simultaneously, the system put JavaApplet into the user's Web browser. The applet establish a TCP connection to the Opengate CGI. When the connection closes, the system knows the user quit to use the network. In this research, we have implemented functions for IPv6 into Opengate without changing characteristic features of the system. During an evaluation experiment, the system worked well.

Keywords: Opengate, IPv6, Network Authentication, Firewall, Java

1　はじめに

2000 年に政府より「e-Japan 重点計画」が発表された. 同計画では, 「2005 年までにすべての国民が, 場所を問わず, 自分の望む情報の入手・処理・発信を安全・迅速・簡単に行える IPv6 が実装されたインターネット環境を実現する.」という方針が掲げられた.

2005 年 3 月現在, 多くの研究用ネットワークは IPv4・IPv6 デュアルスタックを実装しており, 商用ネットワークでも IPv6 サービスを提供する ISP が多数存在する. また, 一般的に利用されている OS (Windows XP, Mac OS X 等) も IPv6 をサポートしている. 現時点では, まだ意識的に IPv6 を利用しようと働かなければ IPv6 を利用することはできない. しかし, 近い将来にはエンドユーザまでもが, IPv6 を意識することなく利用するようになると考えられる.

一方, ネットワークの利用が日常的に行われるようになってきた昨今, その利便性を最大限活用するために, 公開端末の設置や情報コンセント・無線 LAN の整備をしている機関が増えている. 不特定多数の利用者に対してネットワークを公開する場合, 利用資格のない者にネットワークを利用されてしまう恐れがある. よって, ネットワークの利用者認証や利用記録の保存は大変重要である. しかし, 現在 IPv4・IPv6 デュアルスタックネットワークにおける利用者認証システムは実装されていない.

† 佐賀大学大学院工学系研究科
Graduate School of Engineering, Saga University
‡ 佐賀大学理工学部
Faculty of Science and Engineering, Saga University

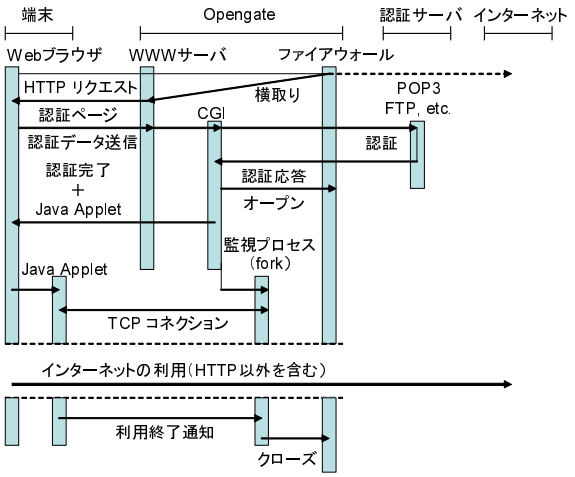

図 1: Opengate の動作の流れ

本稿では, 佐賀大学において開発された利用者認証ゲートウェイシステム “Opengate” について, IPv6 対応に関する研究と開発を行った.

2 Opengate

2.1 概要

Opengate とは, 不特定多数の利用者が多様な端末を接続するネットワーク環境に適応可能な, 利用者認証と利用記録を行うために佐賀大学において開発されたゲートウェイシステムである [1][2].

Opengate の認証は Web ベースの平易なインタフェースを用いているため, 利用者端末を制限しない. 利用者端末側で特殊な事前設定を必要としない. 利用者端末のネットワーク利用状況を監視し, 利用が終了すると即座に通信路を閉鎖する機能を有する. Opengate を導入するにあたっては, 特殊なネットワーク機器や環境を必要としないため, 導入と管理が容易である.

IPv4 ネットワークにおける Opengate の動作の流れを図 1 に示す.

2.2 機能

2.2.1 認証

Opengate を利用した利用者認証付ネットワークでは, 利用者はまず任意の Web サーバへ HTTP を用いてアクセスしなければならない. このとき, ゲートウェイは, ファイアウォールの転送機能を用いて HTTP リクエストを自身の Web サーバへ転送する. これによって, 利用者端末に認証ページが表示されることになる.

2.2.2 利用者端末情報の取得

Opengate は, 認証の過程で Web サーバを介して利用者端末の IP アドレスを取得する. Opengate は, 利用者端末の IP アドレスを用いて通信路を開放する. また, 取得した利用者端末の IP アドレスを元に ARP コマンドを用いて利用者端末の MAC アドレスを取得することが可能である.

2.2.3 通信状態と利用終了の監視

認証後, 利用者端末に認証完了ページが表示される. さらに, この認証完了ページとともに Java Applet がダウンロードされる. このとき, Opengate は利用者端末の利用状況を監視するために, 通信監視プロセスを立ち上げ, 利用者端末の Java Applet と TCP 接続を行う. この Java Applet との TCP 接続が切断されことを利用終了とみなして通信路を閉鎖する.

また, 利用者端末から送信されたゲートウェイを通過するパケット数を監視し, 一定時間パケットの通過が確認できない場合も, 通信路を閉鎖する機能を有する.

2.2.4 利用者情報の記録

“認証”, “ネットワーク利用開始” の手続きで取得した利用者 ID, 端末 IP アドレス, MAC アドレス, 利用開始時刻または利用終了時刻を SYSLOG 機能を用いて記録する.

3 Opengate の IPv6 対応

3.1 IPv4・IPv6 デュアルスタックネットワークでの利用者端末

IPv4・IPv6 デュアルスタックネットワークとは, 同一の物理ネットワーク内で IPv4 と IPv6 が同時に利用されているネットワークのことを指す.

IPv4・IPv6 デュアルスタックネットワークでは, 以下のような端末が利用される.

- IPv4 のみをサポートした端末
- IPv4 と IPv6 をサポートした端末
  - IPv4 を優先して利用する端末
  - IPv6 を優先して利用する端末
- IPv6 のみをサポートした端末

これらの端末を考慮して, Opengate の IPv6 対応を考察する.

3.2 IPv6 対応に関するポリシー

Opengate を IPv6 に対応させる上で, 次のようなポリシーで対応を計った.

- IPv4・IPv6 の両方プロトコルに同時に対応
  IPv4 アドレスと IPv6 アドレスを同時に管理し, IPv4 環境では従来と同様の動作が可能である.
- 従来の Opengate の利用方法の維持
  利用者側の操作は従来と同様の方法で利用可能である.

これらを実現するために我々は, 以下の方法を考案し Opengate_v6 として実装を行った.

- IPv4・IPv6 アドレスの取得
  認証時に利用者端末の IPv4・IPv6 アドレスの両方を取得し一元的に管理を行う（3.3.2 項）.
- IPv4・IPv6 通信路の開閉
  利用者端末の IPv4・IPv6 両方のアドレスに対して通信路の開閉を行う（3.3.1 項, 3.3.3 項）.
- 利用者端末の監視
  利用中の端末の IPv4・IPv6 の利用状況と IPv6 アドレスの利用状況を監視する（3.3.4 項）.

これらの方法について, 以降の節で詳細を述べる.

3.3 IPv6 対応に関する問題点と解決法

3.3.1 IPv6 通信路の開閉

IPv4･IPv6 デュアルスタックネットワークでは, IPv4 と IPv6 の両方の通信路を開閉する必要がある. そこで, Opengate_v6 では, 従来の Opengate 同様 IPv4 の開閉には ipfw（OS 標準装備）を用い, IPv6 の開閉には ip6fw（OS 標準装備）を用いる.

3.3.2 利用者端末の IPv4・IPv6 アドレスの取得

Opengate を IPv6 に対応させる上で最も重要な問題が, 利用者端末の IP アドレスの取得である.

IPv4・IPv6 デュアルスタック対応の利用者端末は IPv4 アドレスと IPv6 アドレスの 2 種類を所有することになる. 従来の Opengate 同様, Web サーバから IP アドレスを取得することは可能であるが, HTTP リクエストが送信された際に用いられたプロトコルのアドレスを取得することしかできない. また, 利用者端末には 3.1 節で述べたような種類があり, しかも IPv4 と IPv6 をサポートした端末では IPv6 のみを用いて通信することは無く, IPv4 と IPv6 が複合的に利用される.

よって, Opengate では利用者端末の IPv4 アドレスと IPv6 アドレスの両方を取得し, それぞれに対して通信路を開放しなければならない.

表 1: Opengate_v6 を構成する主要ソフトウェア

種類	ソフトウェア名
OS	FreeBSD 4.10
ファイアウォール	ipfw (OS 附属)
	ip6fw (OS 附属)
NAT	natd (OS 附属)
RA	rtadvd (OS 附属)
IPv6 router	route6d (OS 附属)
Web サーバ	Apache 2.0
DHCP	isc-dhcp3
Opengate	opengate090i

そこで, Web ブラウザの仕様と DNS の仕様を利用して IPv4・IPv6 アドレスの両方を取得する方法を考案し, 実装した.

まず, Opengate を導入するゲートウェイのために, 二つの FQDN を用意する. 一つには, IPv4 アドレスのみを登録する. もう一つには, IPv4 と IPv6 の両方を登録する.

IPv4･IPv6 デュアルスタックの端末が, 任意の Web サイトの FQDN に対してアクセスする際, その Web サイトの IPv4 アドレスのみ DNS に登録されていれば IPv4 を用いてアクセスする. もし, IPv4・IPv6 の両方が登録されている場合は, IPv6 を用いてアクセスする. この時, Web ブラウザは IPv6 によるアクセスに失敗した場合は, IPv4 で再度アクセスを試みる. (以上の仕様に沿わない端末も存在し, これについては 3.3.4 項と 3.4 節で述べる.)

以上の性質を利用して, 以下のそれぞれの条件において端末情報を取得する流れを説明する.

A : IPv4・IPv6 デュアルスタック端末が, IPv4・IPv6 アドレスを持つ Web サイトへアクセスする場合

B : IPv4･IPv6 デュアルスタック端末が, IPv4 アドレスのみを持つ Web サイトへアクセスする場合

C : IPv4 のみ対応した端末が, 任意の Web サイトへアクセスする場合

特に, 条件 A における利用者端末情報の取得の流れを図 2 に示す.

A : IPv4・IPv6 端末 ⇒ IPv4・IPv6 サイト

(1) Web ブラウザは, 任意の Web サーバに IPv6 HTTP リクエストを送信する. しかし, 通信路は閉鎖されているので HTTP リクエストはタイムアウトする.

(2) Web ブラウザは, その Web サーバに IPv4 HTTP リクエストを送信する. ここで, ファイアウォールによって, HTTP リクエストはゲートウェイ上の Web サーバへ転送される.

(3) HTML Refresh により, 認証ページを提供する CGI へ IPv4 HTTP を用いてアクセスする. このとき, 認証ページを提供する CGI では, 利用者端末の IPv4 アドレスを取得し, 認証ページに hidden タグを用いて埋め込む.

(4) 認証ページより, 利用者 ID とパスワードを入力し, これと一緒に IPv4 アドレスを IPv6 HTTP リクエストを用いて Opengate CGI へ送信する.

(5) 最後に Opengate CGI は, 認証データと一緒に送信された IPv4 アドレスを取得し, Web サーバを通して IPv6 アドレスを取得する.

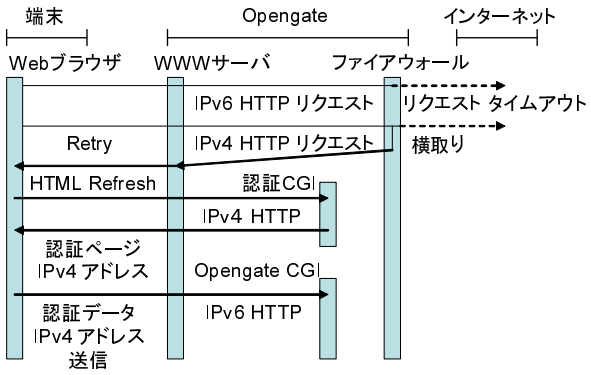

図 2: IPv4 と IPv6 アドレス取得の流れ

B : IPv4・IPv6 端末 ⇒ IPv4 サイト

(1) Web ブラウザは, 任意の Web サーバに IPv4 HTTP リクエストを送信する. ここで, ファイアウォールによって, HTTP リクエストはゲートウェイ上の Web サーバへ転送される.
以降, 条件 A の場合における (3)〜(5) と同様.

C : IPv4 端末 ⇒ 任意 Web サイト

(1) Web ブラウザは, 任意の Web サーバに IPv4 HTTP リクエストを送信する. ここで, ファイアウォールによって, HTTP リクエストはゲートウェイ上の Web サーバへ転送される.

(2) HTML Refresh により, 認証ページを提供する CGI へ IPv4 HTTP を用いてアクセスする. このとき, 認証ページを提供する CGI では, 利用者端末の IPv4 アドレスを取得し, 認証ページに hidden タグを用いて埋め込む.

(3) 認証ページより, 利用者 ID とパスワードを入力し, これと一緒に IPv4 アドレスを IPv4 HTTP リクエストを用いて Opengate CGI へ送信する.

(4) 最後に Opengate CGI は, 認証データと一緒に送信された IPv4 アドレスを取得し, Web サーバを通して再度 IPv4 アドレスを取得する.

認証ページの提供に, HTML Refresh を用いることにより, 従来のインタフェースを変更することなく, IPv4 と IPv6 の両方のアドレスを取得できる.

条件 A における端末情報取得の流れで留意すべき点は, 初回の任意の Web サーバに対しての IPv6 HTTP リクエストを転送できないことにある. これは, IPv6 ファイアウォール ip6fw が転送機能を実装していないためである.

このため, IPv6 による HTTP リクエストがタイムアウトする時間を待たなければならない. 各種ブラウザの仕様によってタイムアウトまでの時間は異なるものの, 約 5 〜 15 秒を要する. 現時点では, IPv6 アドレスを登録している Web サイトは多くないため大きな問題とはならない.

条件 B においては, 初回の HTTP リクエストが IPv4 を用いて行われるため, 条件 A における (1) の手順が省略されることとなる.

条件 C においては, 全ての HTTP リクエストは IPv4 用いて行われ, 条件 A,B における IPv6 アドレスを取得する手順で IPv4 アドレスが取得される. この場合は IPv4 通信路のみを開閉する.

3.3.3 通信状態と利用終了の監視

利用者端末の利用状況を監視するために, 従来どおりゲートウェイ側の利用監視プロセスと利用者端末にダウンロードされた Java Applet 間で TCP 接続を行い, 利用状況を監視する. このとき, IPv4・IPv6 デュアルスタックの 利用者端末の利用状況を監視する際は, IPv4 で TCP 接続を行うように実装している. これは, 利用者端末側に導入される Java VM の仕様のためである.

Java VM には, Microsoft 社のものと Sun Microsystems 社の二つがあり, Microsoft 社の VM を Windows XP を用いて利用した場合, IPv6 を利用することが不可能である. Sun Microsystems 社の VM を利用した場合は, IPv6 を利用することは可能であるが, IPv4 が利用可能な場合は IPv4 を優先するように実装されている. すなわち, IPv6・IPv4 デュアルスタック端末の場合でも, 必ずしも Java VM で IPv6 が利用可能であるとは限らないため, Opegate_v6 では IPv4 を用いて TCP 接続を行う.

また, Opengate_v6 は利用者端末から送信されゲートウェイを通過したパケット数を監視する. この際, 一定時間以上 IPv4 と IPv6 の両方のパケットの通過が確認できなかった場合に通信路を閉鎖する.

3.3.4 利用される IPv6 アドレスの監視

3.3.3 節で述べたように, Opengate_v6 が IPv4･IPv6 デュアルスタックネットワーク上で動作するためには, IPv4・IPv6 デュアルスタックに対応した利用者端末が IPv6 を優先して利用することが前提である. これは, 一般的に利用される Windows XP では問題なく動作する. しかし, 例えば Mac OS X ではデフォルトで IPv4 を優先するように実装されているため, Opengate の認証時に IPv6 アドレスを取得することができない.

このような端末で IPv6 を利用するために, 利用者端末を監視する際, Opengate_v6 側の NDP エントリも監視している. 利用者端末の MAC アドレスに対応する IPv6 アドレスが新たに登録されている場合は, その IPv6 アドレスに対しても通信路を開放する. 既

に通信路が開放されている IPv6 アドレスが NDP エントリから削除された場合は, その IPv6 アドレスに対する通信路を閉鎖する.

これによって, 利用者端末が複数の IPv6 アドレスをスタックしている場合や, 認証時に IPv6 優先して使用しない端末であっても, ネットワーク利用途中から IPv6 を利用することが可能となる.

3.3.5 利用者情報の記録

従来の Opengate 同様に, SYSLOG 機能を用いて利用者情報を記録する.

利用者端末が IPv4・IPv6 デュアルスタック対応であるならば, 利用者 ID, IPv4・IPv6 両方のアドレス, MAC アドレス, 利用開始時刻または利用終了時刻を記録する. 利用者端末が IPv4 のみ対応であるならば, IPv6 アドレスを省いたものを記録する. また, ネットワーク利用途中に利用開始された IPv6 アドレスについても同様に記録する.

3.4 制限

Opengate_v6 を導入するネットワークでは, Opengate_v6 と利用者端末間にルータが設置されない構成が望ましい. IPv6 を優先して利用する端末であれば, 認証時に用いた IPv6 アドレスについては問題ない. しかし, 認証後に利用開始された IPv6 アドレスや IPv6 を優先して使用しない端末については, MAC アドレスを取得し NDP エントリから IPv6 アドレスを検索しなければならないためである.

また, 利用者端末が認証時に任意の Web サイトにアクセスする際, 通信先の Web サーバの FQDN は, 少なくとも IPv4 アドレスが登録されていて, 場合によっては IPv6 アドレスが登録されていることを前提としている. 通信先 Web サーバが IPv6 アドレスしか持っていない場合は, 認証ページへ転送することが不可能である.

最後に, IPv4・IPv6 デュアルスタックネットワーク上では, IPv6 のみ実装した端末も利用可能である. (ただし, このような端末は求められていないのが現状と思われる.) しかし, Opengate_v6 の認証では IPv6 のアドレスを取得するために, IPv4 も複合的に利用しているため IPv6 のみに対応した端末は利用することができない. ただし, このような端末においても, 利用者が自ら認証ページにアクセスすることで利用可能である.

4 評価

今回開発した Opengate_v6 では, 従来の Opengate の認証インタフェースとその利用方法は全く変更していない. 認証インタフェースと認証後の動作状態を図 3, 図 4 に示す.

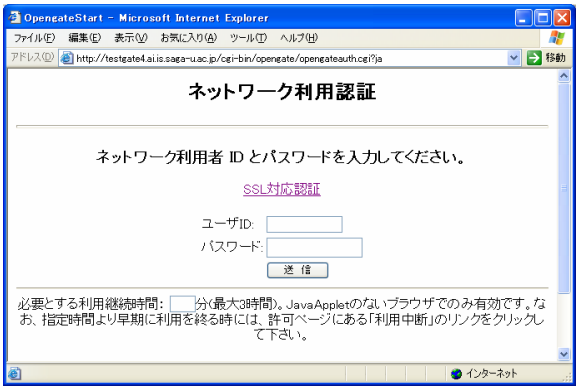

図 3: 認証インタフェース

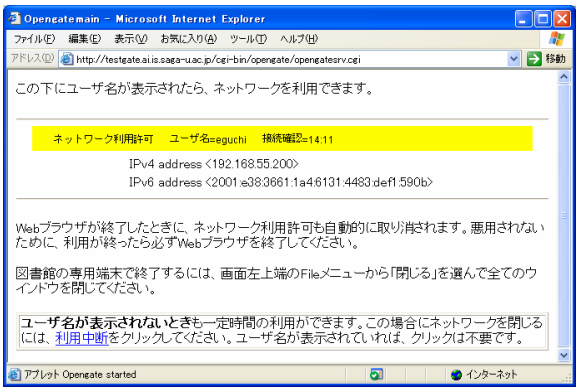

図 4: 認証後の動作状態

利用者数が 30 人ほどの小規模なネットワークにおいて, Opengate_v6 の運用実験を行った. 実験に用いたネットワークは IPv4・IPv6 デュアルスタックネットワークであり, IPv4・IPv6 デュアルスタック対応の端末と IPv4 のみ対応した端末の利用者が混在している. 実験ネットワークでは, IPv4 DHCP と IPv6 RA が Opengate_v6 から送信されており, 利用者端末は IPv4 アドレスと IPv6 アドレスを自動的に取得することが可能である. 運用実験を行ったネットワークを図 5 に示す.

実験ネットワークにおいて 11 月から 1 月までの利用記録を表 2 に示す. 全利用数の約半数が IPv6 を利用しているが, 問題なく利用者認証が行われ, ネットワークを利用することが可能である. 異常終了が約 5% 発生しているが, これは利用者が Java Applet が起動している Web ブラウザで他のページを読み込んでしまい, TCP 接続が切断したものである. この場合, 一定時間経過後に再度認証を行わなければならない. この問題については利用者が Opengate の利用に習熟することで解決されると考えられる.

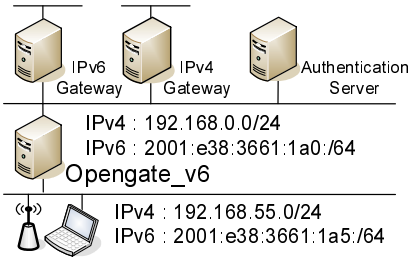

図 5: 運用実験ネットワーク

5 考察

5.1 スケーラビリティ

現在の Opengate_v6 では, 従来の Opengate と同様に一つの端末に対してサーバプロセスが一つ動作するマルチプロセスの構成になっている. 従来の Opengate では, 最大クラス C 程度のアドレス空間を管理し, 分散配置するように運用されている.

IPv4・IPv6 デュアルスタックネットワークにおいて運用する場合も, IPv4 ネットワーク同様に分散配置することが適当であると考えられるが, 実運用には IPv6 の膨大なアドレス空間に対して IPv4 のアドレス空間による制約が大きい. IPv4・IPv6 デュアルスタックネットワークにおけるアドレスの割り当ては今後の課題であり, より大規模な運用実験を通じて考察する必要がある.

5.2 研究の応用

現在, ネットワーク利用者認証を行うためのシステムは幅広く研究されている. これらの研究における通信のフィルタリングを大きく二つに分類すると, OSI 参照モデルにおける第 2 層で制御する方式 [3][4] と第 3 層で制御する方式 [5][6] に分類できる. 本研究において IPv6 対応を計った Opengate は第 3 層において通信をフィルタリングする方式をとっている.

第 2 層において通信をフィルタリングするネットワーク利用者認証システムについては, フィルタリングで IP アドレスを用いないため, 特に IPv6 を考慮する必要はない. しかし, 第 3 層において通信をフィルタリングするネットワーク利用者認証システムについては, IPv6 を考慮しなければならない. 第 3 層で通信をフィルタリングするシステムで IPv6 対応を計る場合は, 本研究において用いた方式が適用できると考えられる.

表 2: 利用記録

全利用数	1385
IPv6 利用数	660
認証失敗数	144
異常終了数	59

6 まとめ

利用者認証ゲートウェイシステム “Opengate” の IPv6 対応に関する研究と開発を行った. 今回, 開発した Opengate_v6 は, 動作実験において IPv4・IPv6 デュアルスタックネットワークで問題なく動作し, 利用者端末において IPv6 を利用することが可能である. IPv4 と IPv6 を同時に利用することが可能で, IPv6 アドレスを複数スタックした端末に応用可能である.

今後, IPv6 ネットワークの整備が進むにつれて, 既に導入されているネットワーク利用者認証システムの IPv6 対応は必須である. よって, 本研究における IPv6 に対応するための技術は有効である.

謝辞

システムの開発に際し, 有益な議論をしていただいた, 佐賀大学理工学部知能情報システム学科渡辺義明教授をはじめ, 佐賀大学学術情報処理センター只木進一教授, 大谷誠講師, 江藤博文助手, 他 Opengate 開発スタッフの皆様に感謝します. また, システムの運用実験に参加していただいた佐賀大学理工学部知能情報システム学科第 5 研究グループの皆様に感謝します.

参考文献

[1] 渡辺義明 他 : 「Opengate ホームページ」 http://www.cc.saga-u.ac.jp/opengate/

[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] 石橋勇人, 山井成良, 安部広多, 阪本晃, 松浦敏雄 : 利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方式, 情報処理学会論文誌 Vol.42, No.1, pp.79-88 (2001).

[4] 広島大学総合情報処理センター「PortGuard」 http://www.portguard.org/ (2001)

[5] 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).

[6] 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, 学術情報処理研究誌 No.2, pp.77-81 (1998)