Proxy サーバに対する ユーザ単位のアクセス制御手法について

服部 裕之　土井 強　松崎 英樹
明治大学情報科学センター

1997.7.18

1 はじめに

本学情報科学センターは、Web ブラウザ等を用いて学外のコンピュータへのアクセスを希望する利用者に対し、事前にある一定のスキルを満たしていることを利用の条件としている。その為に、学外への telnet, ftp は、ファイアウォール上の UNIX を経由する仕組みを用意している。これによって、ユーザ単位のアクセス制御を実現している。

しかし、パソコンから Web ブラウザを利用する場合、学外へのアクセスをユーザ単位で制御することは、既存のソフトウェアの組み合わせでは困難である。何故ならば、http プロトコルを中継する Proxy サーバプログラムのほとんどがホスト単位でのアクセス制御であり、ユーザ単位でのアクセス制御を行なえる仕組みがない。

そこで、筆者らは、既存のフリーソフトウェアをベースにし、ユーザ単位でのアクセス制御を実現するシステムを新たに構築した。

2 システム概要

2.1 全景

Proxy サーバへのアクセス制御をユーザ単位で行なうシステムの概要を、図 1 に示す。

2.2 構成要素

本システムは以下のプログラムから構成される。

1. (WS 用) Identd プログラム

   RFC1413 に記載されている "Identification Protocol" サーバをワークステーション上で実現する。既存のフリーソフトウェア[1]を利用した。

2. (PC 用) Identd プログラム

   RFC1413 に記載されている "Identification Protocol" サーバを PC (Windows3.1, Windows NT) で実現する[2]。このプログラムは、新規に開発した。

---

[1] pidentd-2.2

[2] 但し、ポート番号やシステム名のチェックを省略するなど、RFC1413 の完全なインプリメンテーションではない。

3. 認証サーバプログラム

   PC 用 Identd から入力された「ログイン名」「パスワード」が正当なものであるかどうかを判断する。PC 用 Identd と認証サーバ間は、FOP(Facemark Oriented Protocol) という独自プロトコルを用いている。このプログラムは、新規に開発した。

4. Proxy サーバプログラム

   Web ブラウザからの http を中継する。電総研で開発された delegate に独自の拡張を行なっている。

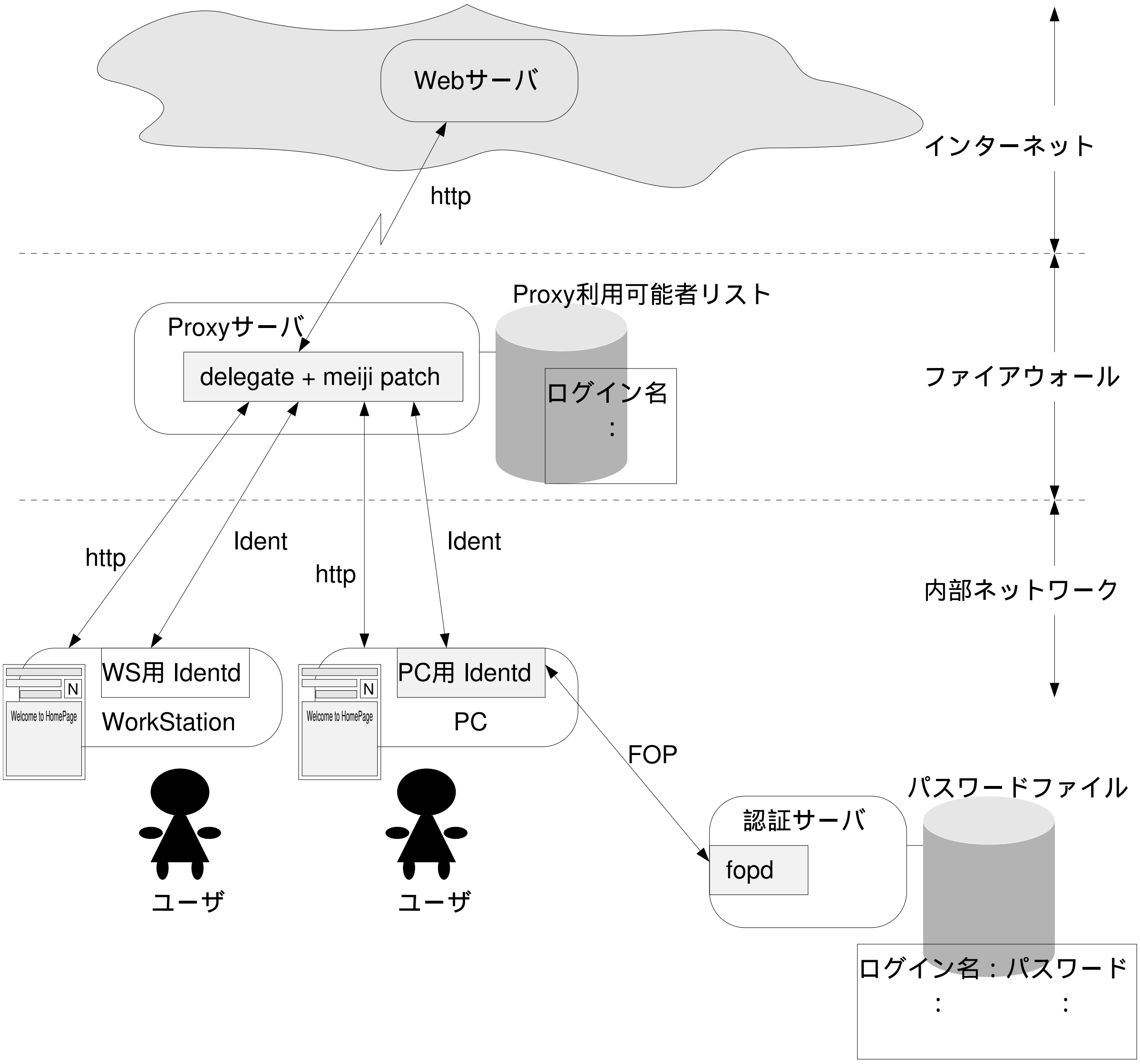

図１ ：システム概要

2.3 利用手順

PC 利用者が Web ブラウザを用いて、学外の Web サーバをアクセスする際の操作、およびサーバ間のやりとりについて紹介する。

事前準備

- Proxy サーバに、学外の Web サーバへのアクセスを許可しているるユーザのリスト（「Proxy 利用可能者リスト」）を登録する。（UNIX 4.2BSD の passwd ファイル形式）
- 認証サーバに、センター利用者のパスワードファイルを登録する。（UNIX 4.2BSD の passwd ファイル形式）

1. Identd の起動
   (a) ユーザは、PC で「(PC 用)Identd プログラム」を起動。自分のログイン名とパスワードを入力する。
   (b) 「(PC 用)Identd プログラム」は入力されたログイン名とパスワードを、認証サーバ上の「FOPD プログラム」に問い合わせる。
   (c) 「FOPD プログラム」は、与えられたログイン名とパスワードが正しいかどうかを判定。結果を「(PC 用)Identd プログラム」に返す。
   (d) 「(PC 用)Identd プログラム」は、(c) のチェックの結果、ログイン名とパスワードが正しいと判断された場合は、RFC1413 の Ident protocol を用いた参照に対し、(a) で入力されたログイン名を返すように動作を開始する。
2. Web ブラウザの起動
   (a) Identd が起動されたら、次にユーザは Web ブラウザを起動する。Web ブラウザは、Netscape Navigator, Internet Explorer, Infomosaic 等いずれでも構わない。但し、学外の Web サーバにアクセスする為には、Proxy サーバの指定が必要である。
   (b) ユーザが、学外 Web サーバの URL を指定すると、Web ブラウザは Proxy サーバに http リクエストを送信する。
   (c) Proxy サーバは、Ident protocol を用い、リクエストを送ってきたクライアントからユーザの「ログイン名」を取得する。
   (d) Proxy サーバは、(c) で取得したログイン名が、「Proxy 利用可能者リスト」に掲載されているかどうかをチェックする。
   (e) (d) のチェックの結果、リストに掲載されていれば、リクエストを学外の Web サーバに転送する。掲載されていなければ、リクエストを拒否する。

3 システム詳細

3.1 Proxy サーバ

Proxy サーバは、電総研で開発された “delegate3.0.57” をベースにし、HotList 記述書式において、次に示す 2 点の拡張を行なった。

1. HostList に、ユーザ名として、任意のファイル（但し、/etc/passwd 書式）を参照できるようにした。
2. HostList に、ユーザ名として、FOPD サーバ名を記載できるようにした。

[例 1]

```
PERMIT='*:*:{&\etc\passwd_sagami2}@133.26.[0-255].[0-255]}
```

& [PASSWD ファイル名（ディレクトリ区切りは “/” ではなく、“¥”)] と記載することにより、

- [PASSWD ファイル名] にアカウントが記載されており
  かつ
- そのユーザのシェルは/etc/shells に記載されている

ような全てのユーザにマッチせよ、という意味になる。

[例 2]

```
PERMIT='*:*:{&sagami2}@133.26.[0-255].[0-255],{naomi,ob00015}@133.26.160.5'
```

& [FOPD サーバ名] と記載することにより、

- FOPD が稼働しているコンピュータにアカウントがあり
  かつ
- そのユーザのシェルは/etc/shells に記載されている

ような全てのユーザにマッチせよ、という意味になる。

3.2 WS 用 Identd

ワークステーション用 Identd プログラムは、フリーソフトウェアをそのまま利用している。

3.3 PC 用 Identd

RFC1413 で定義されている “Identification Protocol”（以下単に Ident）は、各種ネットワークサービスに際してサーバ側からクライアント側の利用者情報を得るために広く用いられている。しかし、パソコンには基本的にユーザ認証の概念が欠如している為、Ident によるパソコン利用者本人の認証は困難であった。

そこで、WWW Proxy サーバからクライアント PC（MS-Windows 3.1）の利用者を特定可能とするため、パソコン上で動作可能な、Ident ソフトウェアを開発した。

特記事項として、ユーザの概念を持たない Windows 3.1 の PC でユーザ認証を行うため、UNIX WS に認証サーバを実装し、PC 側から認証サーバに認証文字列（ユーザ名とパスワード）を送付して認証を行うことが挙げられる。この時認証に用いられるのは、UNIX 側で有効なユーザ名 / パスワードの組である。

なお、実装に際しては Winsock API を用いたため、当初のターゲットであった Windows 3.1 のみならず、Windows 95 , Windows NT 3.5.1/4.0 上でも動作している。

PC 用 Identd を起動すると、まずユーザ名とパスワードの入力を求める（図 2）。次に、入力された文字列を認証サーバに送り、このユーザ名とパスワードの組が有効かどうかを確認する。認証サーバから有効との回答が得られれば、以後はこのユーザ名を用いて Ident 要求に応答する。

Identd: ユーザ認証

ユーザ名: ee12345

パスワード: ********

レベル2認証サーバ

● 生田
○ 和泉
○ 駿河台

図 2 ：**PC 用 Identd 起動時の画面**

3.4 認証サーバ

認証サーバは、PC 用 Identd から問い合わせのあった、「ログイン名」と「パスワード」の組が正当なものであるかどうかをチェックし、結果を PC 用 Identd に返す。認証サーバと PC 用 Identd 間は、前述の通り、独自プロトコルの FOP を使用している。

4 運用実績

本システムは、1996 年 4 月より、駿河台、和泉、生田の各地区情報科学センターで運用している。稼働実績は次の通りである (1997 年 3 月末時点)。

4.1 ユーザ用コンピュータ (Identd)

1. 駿河台

コンピュータ	LAN カード	OS	TCP/IP ドライバ
NEC PC-9821Ce2,Cs2,Ap2,Bf	CONTEC C-NET series	Windows3.1	CONTEC SuperTCP
Fujitsu FMV-466D2	Fujitsu 純正 LAN カード	Windows3.1	Fujitsu InetBIOS

等、合計約 60 台

2. 生田

コンピュータ	LAN カード	OS	TCP/IP ドライバ
Fujitsu FMV-590DE	Fujitsu 純正 LAN カード	Windows3.1	Fujitsu InetBIOS
Fujistu FMV-5150T4	Fujitsu 純正 LAN カード	Windows NT 3.51	OS 附属
Fujitsu S4/2,5,20	内蔵	SunOS4.1.3+JLE	OS 附属

等、合計約 350 台

3. 和泉

コンピュータ	LAN カード	OS	TCP/IP ドライバ
DEC Celebris590	Accton NE2000 互換	Windows3.1	Chamereon 附属ドライバ

等、合計約 80 台

4.2 認証サーバ

1. 駿河台

コンピュータ	LAN カード	OS	TCP/IP ドライバ
Fujitsu S4/20	内蔵	SunOS4.1.3+JLE	OS 附属

2. 生田

コンピュータ	LAN カード	OS	TCP/IP ドライバ
Fujitsu S4/5	内蔵	SunOS4.1.3+JLE	OS 附属

3. 和泉

コンピュータ	LAN カード	OS	TCP/IP ドライバ
Sun Sparc 20/61	内蔵	SunOS4.1.4+JLE	OS 附属

4.3 Proxy サーバ

1. 駿河台・生田・和泉 いずれも同様。

コンピュータ	LAN カード	OS	TCP/IP ドライバ
Fujitsu S4/20H125	内蔵	SunOS4.1.4+JLE	OS 附属

5 問題点

本システムは、本格的な運用を開始してから、既に 1 年半が経過している。これまでに遭遇したトラブルは次の通りである。

1. Identd 起動時、あるいは使用中に”access():10035” などのメッセージが表示されて Identd がハングすることがある。

   → おそらく TCP/IP ドライバ (SuperTCP,InetBIOS) が原因。

2. (1)Identd を起動、(2) ユーザ名・パスワードを入力、(3)OK ボタンをクリックの後、稀に 認証中」の表示がされたままになってしまうことがある。

   → 原因不明・調査中

6　今後の課題

今後の検討課題としては、以下の点が挙げられる。

- 認証プロトコル FOP の Internet 標準への対応。

  より安全な認証プロトコルである、Radius (RFC2138) などの採用。

- スケーラビリティへの配慮と対策。

  ユーザ用コンピュータがさらに増えた場合、あるいは、より高速なネットワークへ移行した場合の配慮の必要性。