WWWにおける利用者単位のアクセス制御機構

山井 成良[1]　山外 芳伸[1]　林　伸彦[1]　宮下 卓也[1]　松浦 敏雄[2]

[1]岡山大学 総合情報処理センター
[2]大阪市立大学 学術情報総合センター

概　要

WWWはインターネットにおいて最もよく利用されるサービスの１つである．しかし，十分に教育を受けていない利用者がWWWを利用した場合，個人情報の盗用やコンピュータウィルスの感染などのトラブルが発生する危険性がある．このようなトラブルを未然に防止するためには，利用者毎にアクセスできる範囲を限定し，ある程度以上の教育を受けた利用者だけがインターネットへアクセスできることが望ましい．

そこで本稿ではWWWでアクセスするときに利用者単位でアクセス制御を行う手法を提案する．本手法では与えられたURLに対して無条件にアクセスを許可あるいは拒否するだけでなく，特定の条件が満たされた場合のみ許可する機能を持つ．この機能により，注意事項の遵守に同意した利用者だけアクセスを許可するなど，教育効果を持たせることも可能になる．

Design and Implementation of User-Oriented Access Contol Mechanism for WWW

Nariyoshi Yamai[1], Yoshinobu Yamasoto[1], Nobuhiko Hayashi[1],
Takuya Miyashita[1], and Toshio Matsuura[2]

[1]Computer Center, Okayama University
[2]Media Center, Osaka City University

Abstract

WWW is one of the most popular services on the Internet. However, use of WWW often causes some troubles, such as abuse of personal information, infection with computer viruses, and so on, especially when novice users access to WWW servers in the Internet. To keep the users away from such troubles, it is desirable for the system administrator to restrict the access range for each user, so that only the advanced users are allowed to access the Internet.

In this paper, we propose a user-basis access control mechanism of WWW for this purpose. In addition to simple "allow" and "deny" functions, our mechanism also provides a conditional access control function. By virtue of this function, we can allow only the users agreeing with the "WWW access statement" to access the Internet, which is an educational application example of our mechanism.

1 はじめに

WWW はインターネットにおいて最も普及しているサービスの1つであり，大学等の教育機関においても講義情報，就職情報など様々な情報の取得手段として多くの学生が利用している．このような情報の取得，活用を支援するため，多くの大学ではコンピュータリテラシー教育の一環として WWW の利用方法を講義するだけでなく，情報処理センター等の施設において計算機を開放したり情報コンセントを設置したりするなど，学生が WWW によりインターネットに自由にアクセスできる環境を整備している．

一方，インターネットでは匿名性が高いため，WWW の自由な利用には危険が伴うこともある．例えば，氏名，住所，電話番号，電子メールアドレスあるいはクレジットカード番号などの個人情報を不用意に入力したためにこれらの情報が悪用されたり，ダウンロードしたプログラム等を介して利用者の計算機がコンピュータウィルスに感染したりする事例は頻繁に報告されている．また，逆に WWW を利用した掲示板に他人を誹謗中傷する文章を掲載するなど，利用者がインターネットの匿名性を悪用して問題を引き起こすこともあり得る．

上記のようなトラブルを未然に防止するため，大学等の教育機関では学生に対してインターネット利用に関する教育を十分に行うことはもちろん必要であるが，更に例えば十分な教育を受けていない利用者には学内ネットワークしかアクセスさせないなど，利用者毎にアクセスできる範囲を限定できる機能を導入することが望ましい．

そこで本稿では計算機の利用開始時に用いられる認証サーバと連係し，利用者単位で WWW のアクセス制御を行う手法を提案する．このとき，無条件にアクセスを許可あるいは禁止するだけでなく，特定の条件を満たした場合のみアクセスを許可する機能を組み込む．これにより，例えば学外サーバへの最初のアクセス時に自動的にネチケットに関する試験問題を出題して合格者だけにアクセスを許可するなど，教育効果を持たせることにより WWW 利用に関する様々なトラブルを軽減させる効果も期待できる．

以下，2 章では WWW における従来のアクセス制御方式を述べる．次に 3 章で利用者単位でのアクセス制御方式を提案し，4 章ではアクセス制御機構の実装方法について述べる．5 章では，試作したアクセス制御機構を応用した WWW 利用同意認証システムについて述べる．

2 WWW における従来のアクセス制御方式

2.1 WWW の利用環境

本手法では，図 1に示すようにクライアント計算機，フィルタリング機能付きルータ，WWW プロクシから構成されている利用環境を想定している．この環境において，クライアント計算機から WWW サーバへのアクセスは WWW プロクシを介して行われる．フィルタリング機能付きルータは WWW プロクシを経由しない直接アクセスを防止するために用いられる．

クライアント計算機については，次に示すような利用環境が考えられる．

（環境 1） 管理者だけが設定でき，利用開始に当たって利用者認証を要する計算機（例えば，適切に管理された UNIX を搭載する計算機）がネットワークに接続されている環境

（環境 2） 利用者が自由に設定できる計算機（例えば，Windows 95/98/Me を搭載した計算機）がネットワークに常時接続されている環境

（環境 3） 利用者が自由に設定できる計算機が公衆電話網などを介してネットワークに接続される環境

（環境 4） 利用者が自由に設定できる計算機が利用者に公開された情報コンセントを介してネットワークに接続される環境

このような環境はいずれも情報処理センター等の施設では一般的であり，またこのような環境を導入していない機関においても比較的容易に導入することが可能である．

2.2 従来のアクセス制御方式と問題点

図 1のような環境における WWW のアクセス制御機構として，black list 方式，white list 方式が知られている．これらは WWW プロクシにおいて，前者ではアクセスを拒否する URL のリスト，後者

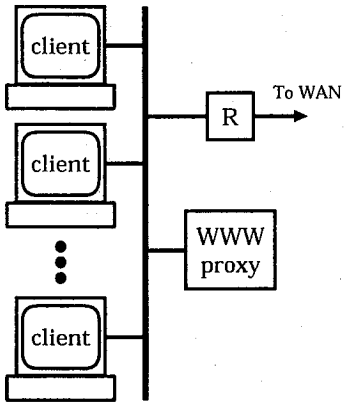

図 1: WWW の利用環境

ではアクセスを許可する URL リストを保持しておき，それ以外の全ての URL に対するアクセスはそれぞれ許可または拒否するものである．しかし，これらの方式では高々計算機毎にしかアクセス制御が行えないため，事実上全ての利用者に対して同一のアクセス制限が無条件で適用され，利用者単位でのアクセス制御を行うことはできない．

一方，利用者単位でアクセス制御を行う方式として PICS (Platform for Internet Content Selection)[1] がある．これは Web ページにその内容を示すタグ（レーティング）を埋め込んでおき，利用者用計算機側でレーティングに応じたフィルタリングを行うものである．従ってフィルタリングの内容を利用者毎に切り替えることにより，利用者単位でのアクセス制御が可能となる．しかし，この方式は性的・暴力的な表現を含む有害なコンテンツの排除を主要な目的としており，また全てのコンテンツにレーティングが埋め込まれているとは限らないため，1 章で述べたようなトラブルの回避には殆んど効果が期待できない．

3 利用者単位でのアクセス制御

3.1 設計方針

前節で述べたように，WWW における従来のアクセス制御にはいずれも問題がある．そこで本稿ではこれらの問題を解決するために利用者単位でのアクセス制御手法を提案する．図 1に示すような環境において利用者単位でアクセス制御を行う場合には，アクセス制御機構が以下の各条件を満たすことが望ましい．

（条件 1） 利用者が管理するクライアント計算機に特別なソフトウェアを必要とせずにアクセスした利用者を認証できること．

（条件 2） WWW アクセスに既存のブラウザをそのまま利用できること．

（条件 3） 利用者毎あるいは利用者グループ毎にアクセスを許可あるいは拒否する URL を指定できること．

（条件 4） 指定された内容に応じて利用者毎にアクセス制御を行えること．

本稿では，まず条件 1 を満たすために，認証サーバを導入してクライアント計算機からのネットワーク利用時にユーザ認証を行い，クライアント計算機から HTTP 要求メッセージを受けた時にアクセス制御機構が認証サーバにクライアント計算機の利用者名を問い合わせる手法を採用する．

この手法では環境 1〜4 のいずれにおいても条件 1 を満たすことができるかどうかが問題となるが，まず環境 3 においては例えば RADIUS サーバ [2] を導入して，ネットワーク接続時にユーザ認証を行うことができる．この場合，クライアント計算機には例えばダイアルアップ接続を行うために PPP 等のクライアントソフトウェアが必要になるが，このようなソフトウェアは環境 3 において本来必要なものであり，特別なソフトウェアを導入することにはならない．また，環境 1 においては，クライアント計算機に IDENT サーバ [3] を導入することによりユーザ認証を行うことができる．この場合，クライアント計算機は管理者が管理するため，IDENT サーバの導入はユーザの負担とならない．更に環境 2, 4 についても，例えば文献 [4], [5] の手法を用いることにより，認証サーバを導入してネットワーク利用時にユーザ認証を行うことができる．この場合，クライアント計算機には DHCP[6] 用のクライアントソフトウェアや認証用として WWW クライアントソフトウェアなどが必要となるが，いずれも標準的なソフトウェアであり，条件 1 の障害にはならない．これらのことから，いずれの環境においても本手法で条件 1 を満たすことができるといえる．

次に，条件 2〜4 を満たすために，本研究では WWW プロクシにアクセス制御機能を導入する．これにより従来のブラウザを設定変更することなくそのまま利用することができる．この機能の導入後では，WWW プロクシはクライアント計算機から HTTP 要求メッセージを受け取ると認証サーバにクライアント計算機の利用者名を問い合わせ，認証サーバから返された利用者名とアクセス先 URL の組に基づいてアクセス制御を行う．このアクセス制御の動作には，(1) 無条件に許可する，(2) 無条件に禁止する，の 2 種類の動作に加えて，(3) 特定の条件が満たされた場合のみ許可する動作を設ける．これにより例えば講義中のみアクセスを許可する，最初のアクセス時に注意事項を表示する，ネチケットに関する試験問題の合格者だけにアクセスを許可するなどの動作が可能となり，WWW 利用に関する様々なトラブルを軽減させる効果が期待できる．なお，アクセス禁止の場合には指定された URL を代わりにアクセスして表示する．

4 アクセス制御機構の実装

4.1 主要部の実装

我々は前節で述べたアクセス制御機能を FreeBSD 3.4 上で apache[7] のモジュールとして実装した．アクセス制御動作のうち (3) については，特定のファイルの有無によりアクセスの許可/禁止を判断し，禁止と判断した場合には条件中で指定された代替ページを表示する機能を実装した．

アクセス許可/禁止の設定は，URL とマッチするパターンリストを記述したファイル（URL パターンファイル）と各利用者に対するアクセス制御内容を記述するファイル（アクセス制御ファイル）2 種類のファイルを用いて行う．

このうち，URL パターンファイルは，図 2に示すように各行が（パターン番号，ホスト部，パス部）の 3 つ組から構成される．ホスト部，パス部はそれぞれ URL のホスト部とパス部（ホスト部より後の部分）に対応し，前者は後方一致で，後者は正規表現としてマッチするかどうかチェックする．例えば図 2では，1 行目はホスト部が ".okayama-u.ac.jp" で終わる任意の URL とマッチする．また，2 行目はホスト部が "www.okayama-u.ac.jp" で終わり，パス部が "student/" で始まる URL とマッチする．このファイルは起動時に一度だけ読み込まれ，正規表現部分のコンパイルが事前に行われる．

一方，アクセス制御ファイルは利用者毎に 1 つ存在し（存在しない場合には標準のアクセス制御ファイルを用いる），図 3に示すように各行は（アクション，パターン番号，0〜2 個の引数）から構成される．このうち，アクションには前節で述べたアクセス制御動作 (1)〜(3) に対応して allow，deny，check のいずれか 1 つを指定する．パターン番号は上記の URL パターンファイル中のパターンを示し，このパターンにマッチした URL に対して指定されたアクションを実行する．なお，パターン番号 0 は任意の URL にマッチする特別の意味を持つ．引数はアクションによって個数や意味が異なり，allow の場合には引数がなく，deny の場合には 1 つの引数があり代替 URL を示す．check の場合には 2 つの引数があり，最初の引数は存在の有無を確認するファイルを示し，2 つめの引数はファイルが存在しなかった場合の代替 URL を示す．

クライアント計算機からアクセスが行われると，アクセス制御ファイルが先頭の行から順にマッチするかどうかチェックされ，最初にマッチした行のアクションが実行される．アクション実行後は原則として次行以降のチェックは行わないが，アクションが check でかつ最初の引数で指定されたファイルが存在した場合には，次行以降のチェックも行われる．例えば，図 3では最初に無条件にファイル time-ok が存在するかどうかチェックされ，もし存在しなければ time-deny.html が表示され，2 行目以降のチェックは行わない．このファイルが存在する場合には，次に URL がパターン 2 とマッチするかどうかがチェックされ，マッチした場合にはその URL を表示して終了する．マッチしない場合には，3 行目以降の条件が順にチェックされる．なお，5 行目で%U は各利用者に対するチェック用ファイルのパス名を示し，%u，%l はそれぞれ利用者名，URL に置換される．また，最後の行は 5 行目までで表示するかどうかが決定されなかった全ての URL とマッチし，これを表示するためのものである．URL がどの行のパターンにもマッチしなかった場合には，標準の動作として deny が選択され，標準の代替 URL が表示される．

また，この実装では，apache 付属のアクセスログの他に新たにユーザ名を含めたアクセスログを syslog を用いて出力している．これによりこのアク

```
1 .okayama-u.ac.jp
2 www.adm.okayama-u.ac.jp ^student/
3 .adm.okayama-u.ac.jp
```

図 2: URL パターンファイルの例

```
check 0 time-ok time-deny.html
allow 2
deny 3 adm-deny.html
allow 1
check 0 %U accept_check.pl?url=%l&user=%u
allow 0
```

図 3: アクセス制御ファイルの例

セスログだけで誰がいつどこにアクセスしたかを容易に調査することができ，利用者が不正アクセスを行った疑いがある場合に素早く対処することが可能である．

4.2 動作の詳細

前節で述べた動作を含め，以下では 2.1で述べた環境 2 での利用を例にとってアクセス制御機構の全体の動作を述べる．

1. WWW プロクシ上でアクセス制御機能を組み込んだ apache を起動する．apache は URL パターンファイルを読み込み，各行に含まれるパス部の正規表現をコンパイルする．

2. 利用者はクライアント計算機を利用するためにログインする．このとき，認証サーバはクライアント計算機の利用者が正規の利用者であると認識すると，クライアント計算機の利用を許可するとともに，クライアント計算機の IP アドレスと利用者名を記録する．

3. 利用者はクライアント計算機上のブラウザを用いて WWW サーバにアクセスする．このとき，クライアント計算機と WWW プロクシとの間に TCP コネクションが確立され，このコネクションを用いて HTTP 要求メッセージが WWW プロクシに送られる．

4. WWW プロクシは HTTP 要求メッセージを受け取ると，送信元の IP アドレスを取得して認証サーバに利用者名を問い合わせる．

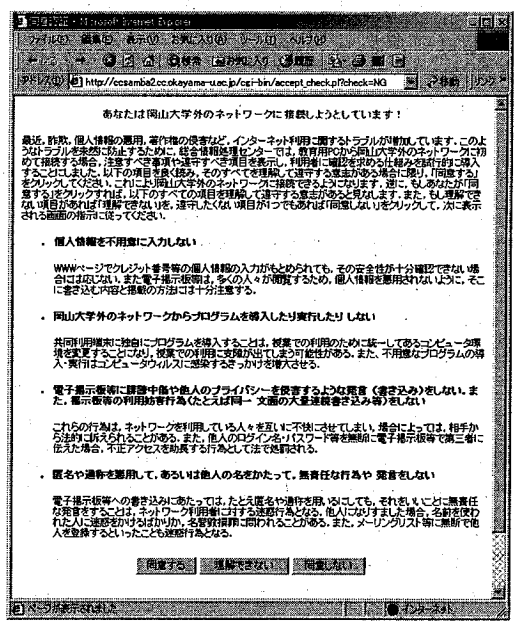

図 4: WWW 利用時の注意事項表示

5. WWW プロクシは認証サーバから利用者名を受け取ると，その利用者に対応するアクセス制御ファイルを読み込み，各行で指定されるパターンと HTTP 要求メッセージに含まれる URL とを順に照合する．マッチする行が見つかった場合には，その行で指定された動作を行う．

なお，環境 2 以外の環境における動作も同様である．

5 試作システムの運用

岡山大学総合情報処理センター（以下，センター）では，アクセス制御機構を応用した WWW 利用同意認証システムを平成 12 年 9 月より試験運用している．このシステムは，WWW 利用に関する様々なトラブルを軽減させるため，センターに設置されている教育用 PC の利用者が学外の WWW サーバに初めてアクセスする場合に図 4に示す注意事項を表示し，その遵守に同意した場合のみアクセスを許可するものである．

以下では本システムの設定と動作について述べる．

センターの環境は 2.1で述べた環境 2 と同様であり，クライアント計算機には Windows 95 を搭載し

たPCを用いている．また，WWWプロクシは認証サーバと兼用している．URLパターンファイル及びアクセス制御ファイルはそれぞれ図2，図3とほぼ同様の内容となっている．

この設定では，利用者がokayama-u.ac.jp以外のドメインのWWWサーバにアクセスした時にチェック用ファイルの有無がチェックされ，初回アクセス時にはこのファイルが存在しないため代替URLとして“accept_check.pl?url=%l&user=%u”がアクセスされる．accept_check.plはCGIプログラムであり，図4に示す注意事項を表示して利用者に同意を求める．ここで，もし利用者が「同意する」ボタンをクリックした場合には，チェック用ファイルを作成し，引数で与えられたURLを表示する．利用者がそれ以外のボタンをクリックした場合には，各ボタンに対応したページが表示される．これにより，一度「同意する」ボタンをクリックすると，2回目以降のアクセス時にはチェック用ファイルが存在するため注意事項は表示されず，初回アクセス時のみ表示されることになる．

次に本システムの運用結果について述べる．

センターでは，試験運用として平成12年10月から12月までの3カ月間に，約2000人の利用者が少なくとも1回は本システムを利用しているが，本システムは十分に機能しており，特に運用上の問題は発生していない．また，WWWプロクシの負荷は十分小さく，50台のPCからほぼ同時にアクセスした場合でも特に性能上の問題は発生していない．以上のことから，試作したWWWアクセス制御機構は十分実用的であるといえる．

6 まとめ

本稿では，WWWにおける利用者単位でのアクセス制御機構の設計及び実装方法を示した．また，この機構を応用したWWW利用同意認証システムについて述べた．試験運用の結果，試作したWWWアクセス制御機構は機能面，性能面のいずれにおいても十分実用的であるといえる．今後の課題としては，WWW利用同意認証システムの教育面での有効性の検証が挙げられる．また，単に注意事項を表示するだけでなく，ネチケットに関する試験問題を出題し，これに合格したものだけにWWWアクセスを許可することにより，更に教育効果を高める方法が考えられる．

参考文献

[1] Platform for Internet Content Selection (PICS), http://www.w3.org/PICS/.

[2] Rigney, C. et. al.: Remote Authentication Dial In User Service (RADIUS), RFC 2138, 1997.

[3] Johns, M. C. S.: Identification Protocol, RFC 1413, 1993.

[4] 石橋勇人，山井成良，安倍広多，大西克実，松浦敏雄: IPアドレス/MACアドレス偽造に対応した情報コンセント不正アクセス防止方式，情報処理学会論文誌，Vol. 40，No. 12，pp.4353–4361(1999).

[5] 石橋勇人，阪本晃，山井成良，安倍広多，大西克実，松浦敏雄: 情報コンセントにおける認証とアドレス偽造防止をVLAN機能により実現するシステムLANA2，情報処理学会研究報告，Vol. 99，No. 56，pp.137–142(1999).

[6] Droms, R.: Dynamic Host Configuration Protocol, RFC 2131, 1997.

[7] The Apache Software Foundation, http://www.apache.org/.