情報コンセントのユーザ認証について

久長　穣[*1]、岡田　隆[*2]、刈谷　丈治[*3]

[*1, 3]山口大学総合情報処理センター
TEL：0836-35-9496
FAX：0836-35-9497
[*1]hisa@yamaguchi-u.ac.jp
[*3]joji@yamaguchi-u.ac.jp

[*2]山口大学附属図書館
TEL：0836-9410
FAX：0836-35-9499
haido@po.cc.yamaguchi-u.ac.jp

概要

平成9年度、山口大学総合情報処理センターと附属図書館は情報コンセントを設置した。情報コンセントは端末を接続し電源投入すれば、端末のネットワーク設定が自動的に行なわれる。誰でも容易にネットワークが利用できる反面、利用者を大学構成員などに限定することは困難である。情報コンセントを大学構成員であれば誰でも自由に利用できるようにするため認証機能を導入したので報告する。

キーワード

情報コンセント、ユーザ認証、DHCP

1．はじめに

ネットワーク利用者の多くは、個人所有の携帯端末（例えばノートパソコン）を持ち歩いて利用していることが多くなってきた。携帯端末がネットワークを利用するためには何らかの方法で、学内 LAN に接続する必要がある。いくつかの手法が実用されているが、利用方法の簡便さ、通信速度の高速化の点で、携帯端末にイーサネットのネットワークカードを挿入し、教室あるいは

ホールに用意されたモジュラコンセントに接続し、学内 LAN を利用する情報コンセントが有効である。

情報コンセントにおいても利用者を限定するため、また、誰が利用しているかを明らかにするため、利用者が利用を始める前にあらかじめ、情報コンセントの利用のための認証機能が必要となる。本学においては、情報コンセントの認証機能を導入し運用している。ここでは、この認証機能について報告する。

２．情報コンセント

２．１　ネットワーク構成

運用している情報コンセントの論理ネットワーク構成図を図１に示す。図中のＤＨＣＰサーバは情報コンセントに接続された端末へ設定を指示するほか、学内ＬＡＮへのルータ、ネームサーバ、認証のための画面と処理を提供する Web サーバとして機能する。物理的なネットワークはＡＴＭイーサスイッチを介し ATM ネットワークに接続して、情報コンセントの ELAN を構成している。情報コンセント ELAN に属している ATM イーサスイッチの設置場所は総合情報処理センター及び附属図書館である。各部局に ATM イーサスイッチを ATM ネットワークで接続し、情報コンセント ELAN に参加すれば、各部局において各種サーバを設置することなく、情報コンセントを設置することができる。

２．２　DHCP サーバ

DHCP サーバは次のハードウェア及びソフトウェアで構成される。

ハードウェア	DOS/V パソコン	CPU 486DX2 66MHZ
ソフトウェア	OS	FreeBSD 2.2.5-RELEASE
	DHCP サーバ	WIDE DHCP server 1.4.0
	WWW サーバ	Apache 1.2.5
	ルータ機能	（OS 標準）
	フィルター機能	IPFW （OS 標準）

２．３　端末設定

DHCP サーバは情報コンセントに接続された端末の電源投入時にその端末からの問い合わせに対して IP アドレスなどの諸条件を送信し、該当端末のネットワーク設定を行わせる。その際、自動設定される主な項目は以下のものがある。

(1) IP アドレス

(2) サブネットマスク
(3) ルータ（ゲートウェイ）アドレス
(4) ネームサーバアドレス

ここで(1)は接続毎に異なることがあるが、（2）～ (4) は同じである。

3．情報コンセントでの認証

3．1　認証の条件

情報コンセントをある特定の利用者のみに利用を許可する場合、次の３点に注意が必要である。

(1) 利用を許可された人のみが、情報コンセントに接続でる必要がある。言い換えると、許可されていない人は情報コンセントを利用できてはならない。
(2) 利用している間は、誰が利用しているかを明らかにする必要がある。
(3) 利用を終了したことを感知できなければならない。

これらに加えて、導入に当たっては次の点を考慮した。

(4) 全学どこからでも、同じように利用できる。

本学はキャンパスが分散しているため、キャンパス間の移動が困難であり、キャンパス内の状況が異なっている。移動の問題はマルチメディアネットワークを使って移動しないようにできるかもしれないが、人の移動をともなう交流が望ましい。できるだけキャンパスの独自の状況を無くし、どのキャンパスに移動しても同じように利用できるよう配慮した。

(5) IP アドレスはできるだけ、利用者固有のものとする。

これは (2) の条件をより進めたものである。すなわち、IP アドレスを利用者固有にすることにより、情報コンセント利用時には IP アドレスは不変となる。

不正利用等があった場合、サーバ側のログ情報にはクライアントの IP アドレスが残されているため、IP アドレスをもちいて追跡しやすくすることにより、不正利用などのいたずらを防止する効果を期待している。（ただし、完全に防止できるわけではない。）

一人に一つづつ IP アドレスを割り当てようとした場合、本学の構成員の総数は 1 万数千人であるので、IP アドレスは 1 万数千個必要になる。そこで、プライベート IP のクラス B(172.16.0.0-172.31.0.0 の内)を利用することにした。プライベート IP を使用しているので、インターネットを利用するには、学内に設置されたサーバや、プロキシを経由して利用しなければならない。

割り当て方法については、入学時に割り当てるという案もあろうが、周知の手続き等を考えると現実的でない。今回は DHCP でアドレスを割り当てる際に、一度割り当てたアドレスはそれ以降、その MAC アドレス以外には割り当てない機能があるので、これを利用して割り当てることにした。

3．2 認証方法

認証の手順は次のとおりである。

(1) 利用者が端末を情報コンセントに接続し、電源投入後、DHCP サーバより該当端末のネットワーク設定が自動的に行われる。

(2) 利用者は WWW ブラウザを用いて、http://ic.lib-e.yamaguchi-u.ac.jp/（図 1 での DHCP サーバ）に接続する。図 2 のパスワード受付画面が表示されるので、総合情報処理センターのメールサーバのユーザ名とパスワードを入力する。

(3) WWW サーバは cgi を用いて、入力されたユーザ名とパスワードをセンターのメールサーバに問い合わせる。処理を単純化するため POP サーバの認証機能を利用している。

(4) (3) の問い合わせが正しければ、WWW サーバは「情報コンセントが利用できる」というページを送出し、該当端末の IP アドレスに対し通過可能のフィルタをルータに設定する。これにより、該当端末は学内 LAN と通信できるようになる。（注意：ルータのデフォルト設定は学内 LAN へのすべての通信は禁止である。） (3) の問い合わせが間違っていれば、WWW サーバは「パスワードが間違っている」というページを送出するほかは、特に何もしない。

(5) ルータの ARP テーブルに該当端末のエントリがなくなった場合

(6) 、該当端末が情報コンセントの利用を停止したと判断し、 (4) で設定したルータのフィルターを解除する。これにより該当端末は学内 LAN と通信できなくなる。

4．おわりに

本学に設置されている情報コンセントは定常的に多くの利用者で利用されており、必要性が増している。情報コンセントの認証機能の導入について述べた。しかし、完全な認証を提供できるものではない。今回の認証機能には次の問題点がある。

(1) DHCP サーバは端末に認証なしで情報を送出してしまう。そのため、情報コンセント内の通信は認証なしに利用できてしまう。このために、DHCP サーバに認証機能を持たせるか、情報コンセントの個々のコンセントでフィルタリングの機能を設置する方法などを導入する必要がある。

(2) 端末が情報コンセントを利用停止した時点で、そのことを直接知ることができない。そのため、停止後もしばらく該当 IP アドレスの通過フィルタが設定されてしまう。このためには、利用を停止したことを知らせる方法、あるいは、利用中を知らせる方法が必要となる。

今後、情報コンセントの利用者は増えていくこと、総合情報処理センターや附属図書館だけでなく各学部においても情報コンセントを設置されることが予測される。端末側の OS を含めて、情報コンセントの認証機能を整理し、充実させていく必要がある。

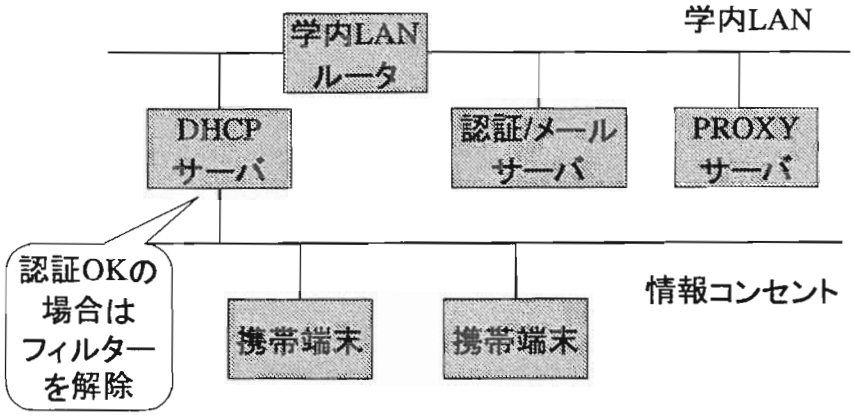

図１　情報コンセントの論理ネットワーク構成図

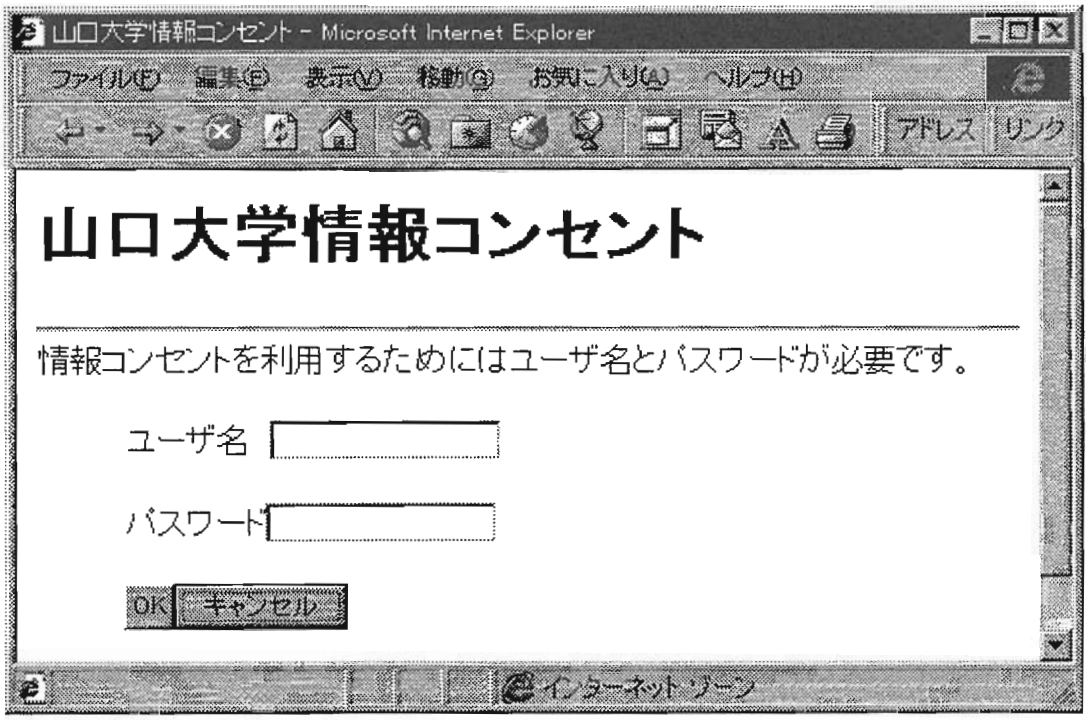

図２　情報コンセントのパスワード入力画面