# セキュリティレベルに応じた校内情報コンセントシステムの構成法と運用例

桝田 秀夫, 中西 通雄
大阪大学サイバーメディアセンター情報メディア教育研究部門
〒560-0043 大阪府豊中市待兼山町 1-30
TEL 06-6850-6076　Fax 06-6850-6084
h-masuda@cmc.osaka-u.ac.jp, naka@cmc.osaka-u.ac.jp

**概要**

大学などの教育現場において、利用者のパソコンをネットワークに接続させる為に情報コンセントシステムを提供することが広く行われるようになってきている。また、学会などを開催した際のネットワーク接続環境の提供や、研究室に来た来客へのネットワーク接続環境の提供など、さまざまなセキュリティレベルの情報コンセントシステムが運用されるようになってきている。しかし、情報コンセントの運用に関しては、そのシステムの運用場所や場面に応じて、管理方法や運用方法は異なる。本稿では、運用場所や場面に対しての、セキュリティレベルに応じた構内情報コンセントシステムの構成方法と、それぞれの要求に応じた実装とその管理・運用方法との関連、およびその運用例について述べる。

## 1　はじめに

大学などの教育現場において、教育用計算機システムとして、多くのパソコンを設置してサービスを提供する形態だけでなく、利用者が所有するパソコンをネットワークに接続させ、ネットワーク接続性とサーバ機能を提供するといった、情報コンセントシステムを提供することが広く行われるようになってきている。それだけではなく、学会などを開催する際のネットワーク接続環境の提供や、研究室に来た来客へのネットワーク接続環境の提供など、規模や接続許可のポリシーの異なる情報コンセントシステムが運用されるようになってきている。

そのような情報コンセントは、何の認証もなく利用できるような形で運用すると、不正アクセス[11]の温床になり易いと考えられ、認証付の情報コンセントシステムの実現に関する研究が盛んに行われている[1, 2, 4, 5, 6, 7]。

しかし、情報コンセントの運用に関しては、そのシステムの運用場所や場面に応じて、管理方法や運用方法は異なる。例えば、教育用計算機システムの一部として提供するような場合のように、既に利用者のアカウント情報は存在していて、利用者の識別必要とされるような場面が考えられる。また、研究室の来客にネットワーク接続環境を一時的に貸す場合のように、利用者の識別までは必要なく、その利用の時間帯程度が識別できれば十分であるような場面まで、セキュリティレベルはさまざまであり、要求される運用方法が異なると考えられる。

このように、運用方法に応じて要求される仕組みは異なってくるが、どのような方針で仕組みを選択するべきか、仕組みに要求される機能は何であるのか、どのような管理手法をとるべきか、といった方針付けに関する要求などは筆者の知る限り発表されていない。

本稿では、運用場所や場面に対しての、セキュリティレベルに応じた構内情報コンセントシステムの構成方法と、それぞれの要求に応じた実装とその管理・運用方法との関連、およびその運用例について述べる。

運用例としては、学会の研究会会場向けとして構築し、コンピュータに比較的長けた人達が集まった小人数の研究会で運用した場合と、教育用システム向けとして構築し、本センターの教育用計算機システムの一部として提供する無線 LAN アクセスサービスとして運用した場合の２つを取り上

Constructing on-campus LAN socket systems based on several kinds of security levels.
H.Masuda, M.Nakanishi
Cybermedia Center, Osaka University.

げる。

## 2 システムへの要求

情報コンセントシステムとは、接続しようとするパソコンに対してネットワークへの接続性を提供するシステム、と定義できる (図 1)。

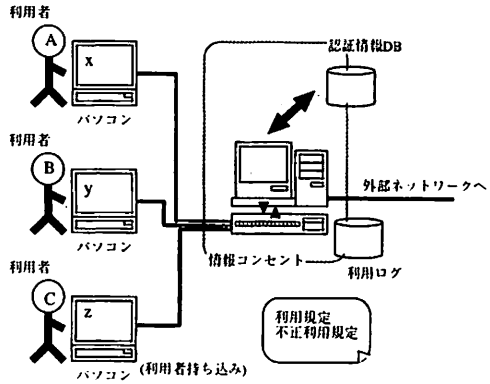


図 1: 情報コンセントシステムの概略

情報コンセントシステムに対する要求は大きく分けて以下の 4 つの観点が挙げられる。

**R1** : [**認証の確実性**] 情報コンセントシステムの利用状態を確認する為には、なんらかの方法によりアクセス主体を識別をする必要が発生する。このとき主体としては、

1. パソコンを識別できる
2. (パソコンの) 利用者を識別できる

といった識別が考えられる。一般に、あるパソコンの利用者は一人である、という前提のシステムが多く用いられている。

**R2** : [**利用できる認証情報**] アクセス主体を識別する際、なんらかの認証情報が必要となる。このとき利用可能な認証情報としては、

1. 既存のユーザアカウントシステム
2. ハードウェア情報 (MAC address など)

といったものが考えられる。

**R3** : [**利用者側のコスト**] 情報コンセントを利用する為に、利用者側で準備する必要があるものがどれだけあるのかも重要な要件である。

1. ドライバ(・アプリケーション)が OS に組み込まれている。
2. 利用者がドライバ(・アプリケーション)をインストールする必要があり、ドライバが無償で配布されている。
3. 利用者がドライバ(・アプリケーション)をインストールする必要があり、ドライバが有償で配布されている。

OS に標準で組み込まれたドライバやアプリケーションと標準ハードウェアで利用可能であるものが、もっともコストがかからないのは勿論である。しかし、利用者の環境は多種多様であり、高度なセキュリティレベルを提供する為に必要なドライバ・アプリケーションが OS に標準で含まれていることは期待できない場合もあり得る。

**R4** : [**設置側のコスト**] 設置側で準備する必要がある機器のコストは、実際に情報コンセントシステムを運用する際に、重要な要件となる。大きく分けて、

1. 専用装置
   Cisco 社製の PIX や EAP システムのような、認証が行える専用の装置を利用する場合。
2. 汎用装置+アプリケーション
   文献 [1, 2, 4, 5, 6, 7] にあるような、普通の PC と認証を行うためのアプリケーションを組み合わせて利用する場合。

で構成されるものが知られている。一般に、導入コストは後者の方が圧倒的に良いが、運用コストは前者の方がすぐれている場合が多い。

さらに、運用に関しては、以下の 2 つの項目が挙げられる。

**M1** : [**セキュリティ対策**] 情報コンセントシステムは、一般に利用者が多種多様であり、利用者のパソコン環境に対して仮定を置くことが困難である。また、もしなんらかの仮定が置けたとしても、利用者の善意・悪意に関わらず利用者の動きは、必要な場合に追跡できるようにしておく必要がある。従って、利用可能サービスを制限することや、すべてのアク

| | R1 | R2 | R3 | R4 |
|---|---|---|---|---|
| 研究室の一時接続向け | - | - | 1 | 2(1) |
| 学会の研究会会場向け | 1 | 2 | 1(2) | 2(1) |
| 教育用システム向け | 2 | 1 | 2(1) | 2(1) |
| 商用サービス向け | 2 | 1+2 | 3(1,2) | 1 |

表 1: セキュリティレベルからみた分類例

セスに関して利用ログを取得することが求められる。

1. 利用可能サービスの限定
2. ログの取得・監視

ログには最低限、時刻、アクセス元、アクセス先、アクセスプロトコルを記録しておく必要がある。

**M2**：[セキュリティポリシ] セキュリティを考える際、すべてを技術的に制約することはどうしても困難な場面がある。例えば、外部からのアクセス可能なポートを技術的に制約していても、内部から外部にトンネルを設定することで、技術的制約を回避するような利用方法が考えられる。このような利用方法に対して、技術的に完全に防ぐことは困難である。従って、明確な利用規定を設定しておくことが求められ、不正利用をポリシによって制限することが求められる。

# 3 構築における仕様

以上のような要求を考慮し、考えられる運用場面と、現在提案されているシステムの関連性を考察し、実際にさまざまな場面で運用できるシステムの仕様を考える。

前節のシステムの要求から、セキュリティレベルから見た分類として、表 1 のような構成の分類が挙げられる。

## 3.1 研究室の一時接続向け

この構築では、一時的にネットワークの接続環境を貸し与えることを想定する。利用にあたっては、接続環境を貸し与えたユーザがアクセスしていると見做すことで、借り主の識別は行わない。

- R1, R2 は特に配慮の必要がない。
- R3 は 1 であること。
- R4 は 2 であること。1 でも良い。

## 3.2 学会の研究会会場向け

パソコンが識別できるが、認証情報をあらかじめ登録はしないことを想定する。また、ほとんどの OS で標準的に存在しているドライバ・アプリケーションだけで利用可能であり、汎用装置とサーバアプリケーションで実装する。

- R1 は、1 であること。
- R2 は、2 であること。
- R3 は、1 であること。2 でも良い。
- R4 は、2 であること。1 でも良い。

## 3.3 教育用システム向け

利用者が識別でき、既存のユーザアカウントシステムが利用可能であることを想定する。また、無償で提供されているドライバ・アプリケーションを個別にインストールしてもよいと考え、汎用装置とサーバアプリケーションで実装する。

- R1 は、2 であること。
- R2 は、1 であること。
- R3 は、1 か 2 であること。
- R4 は、2 であること。1 でも良い。

## 3.4 商用サービス向け

利用者が識別でき、ユーザアカウントシステムとハードウェア情報を組み合わせて利用可能であることを想定する。また、有償 (サービスに附属も含む) で提供されるドライバ・アプリケーションを個別にインストールして、専用装置で実装する。

- R1 は、2 であること。
- R2 は、1 と 2 の組合せであること。
- R3 は、1 が望ましいが、2 でも 3 でも良い。
- R4 は、1 であること。

# 4 構築と運用における考察

本節では、前節で述べた仕様を満たす構築と、それを実際に運用した際に得られた知見を考察する。

## 4.1 研究室の一時接続向け

この構築では、特に凝った設定は必要ではなく、通常の DHCP サーバを配置するだけで実装可能である。

ただし、接続環境を貸し与えていることを用意に判定できるように、接続先のハブなどが置いてある場所が部屋の中の確認できる場所にあること、といった物理的な配慮は必要であろう。

## 4.2 学会の研究会会場向け

### 4.2.1 実装

この構築では、パソコンを識別する為に、MAC address を基本とする。サーバには、イーサネットインターフェイスを 2 つ持つごく普通のパソコン上で NetBSD を導入し、以下のサービスを設定した実装を行った。

1. DHCP サーバ + NAT(ipnat [2] )
2. arpwatch[3] による MAC address モニター
3. ipf [4] による IP パケットモニター
4. transparent proxy モード[5] で動作する squid

本構築では、パソコン側は、DHCP クライアントにさえなることが出来れば良く、特殊なドライバやアプリケーションを必要としない。また、アクセスの多くを占めると考えられる http でのアクセスに関しては、4 によるプロトコルレベルのログを取得することを想定した。squid のログには、M1 で述べた性質の記録が含まれている。他のプロトコルによるアクセスは、3 による IP レベルのログを取得することとした。これにより、どの時刻に、どのポートでどの計算機にアクセスしたか、を記録することにより、問題があった場合の追跡に利用できる。パソコンの識別の為に MAC address を基本としているが、設定ミスなどにより、IP address の衝突や他のネットワーク用の設定のまま接続されていることを検出する為に、2 によるモニタリングも行っている。

[2] NetBSD で採用されている、NAT(Network Address Translation) を行う実装。

[3] MAC address と IP address のペアを追跡するツール。`ftp://ftp.ee.lbl.gov/arpwatch.tar.gz`。

[4] NetBSD で採用されている、IP パケットの入出力に対するフィルタリングを行う仕組み。

[5] proxy サーバの存在を利用者側に陽には見せずに透過的に動作するモード。

### 4.2.2 運用

構築したシステムを、あるコンピュータ関連研究会で運用した。

ケース 1

| | |
|---|---|
| 利用時間 | 2002 年 2 月 14:30〜17:00 |
| 総利用者数 | 3 名 |
| ログサイズ | 116MBytes(IP パケットモニター) |
| | 4kBytes(squid, 約 30 アクセス) |

運用開始当初は、

ftp(21), ssh(22), telnet(23), smtp(25), http(80), pop(110), ident(113), imap(143), https(443)

のみを許可し、http と https は、transparent proxy によるプロトコルレベルのモニターを行うようにして運用した (M1)。

当日の広報不足で、パソコンの持ち込み者が少なかったことと、上位のネットワークの不調により、実際には最初の一時間ほどしか実質的に利用できなかったことによって、このようなデータになってしまった。許可ポートとしては、上記以外に、

ircd(6667), pops(995), imaps(993)

などを使いたいという要求があった。

また、IP パケットモニターは、かなりのサイズになってしまうことが分かったが、ほとんどは制限されたポートへの外部からアクセス記録であった。

M2 に関しては、「上流ネットワーク (この場合は大阪大学) と、情報コンセントシステムに迷惑をかける行為一般を禁止する」というポリシを規定して、広報するにとどめた。一般に、参加者がある程度限られている場合は、このような曖昧なポリシであっても十分に機能すると考えられる。

ケース2

| | |
|---|---|
| 利用時間 | 2002年5月中旬2日間 |
| 総利用者数 | 48名 |
| ログサイズ | 約11MBytes(IPパケットモニター) |
| | 約3.5MBytes(squid, 約2万接続) |

この運用時には、ポートによるアクセス制限を設けずに、IPパケットモニターのみを行うようにして運用した(M1)。その為、IPパケットモニターのログサイズが激減している。

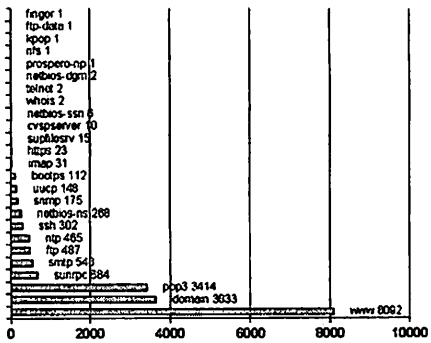


図2: 利用されたプロコトルポート

利用されたポートは、図2の通りで、ほとんどがhttp(80)であることが分かる[6]。このケースでは、UNIX系OSを用いたシステム設定に関する勉強会であった為、Windows系のOSでは見られないポート(sunrpcなど)が多く見られる。

M2に関しては、ケース1と同じものを提示した。

## 4.3 教育用システム向け

### 4.3.1 実装

この構築では、利用者を識別する為に、文献[4]にあるPPPoEを用いたシステムを利用した。PPPoEサーバには、3.2と同様にイーサネットインターフェイスを2つ持つパソコン上でDebian Linuxを導入し、以下のサービスを設定した。詳細は、文献[4]と同様である。

[6] squidのアクセス数よりも少ないのは、HTTP/1.1のkeepaliveにより、一回の接続で複数のコンテンツを取得している為と推測できる。

1. in-kernel pppoe server (+ RADIUSパッチ)
2. IDENT proxy

本構築では、パソコン側は、PPPoEサービスをを利用できるようになっている必要がある為、PPPoEドライバのインストールが必要となる。文献[7, 8]などでは、Javaを用いた認証モジュールを利用することで、ブラウザなどに入っているJavaの動作環境さえあれば利用できるようなものもあるが、セキュリティの為に多目的に使えるJavaの機能を停止しておきたい場合も考えられる。PPPoEは、このような利用者認証の為に特化している為、そのような場合でも安心して利用することが可能であると考えられ、またWindows XPなどではOS標準で利用できるようになってきている。

さらに、PPPoEサーバ以外に、利用者認証情報が格納されたサーバが必要であるが、本構築では、RADIUSによってアクセス可能なサーバが既に用意されているものとしている。

### 4.3.2 運用

構築したシステムを、本学の福利厚生棟の食堂において、無線LANによるネットワーク接続サービスとして運用した。

**利用時間**：2002年7月～

**総利用者数**：20名(2002年7月17日現在)

アクセス先は、本学の情報教育用システムのみとしており、インターネットとの直接通信は出来ないようになっている(M1)。その為、利用可能なサービスは、

- メールの送受信(smtp, imap[7])
- ニュースの送受信(nntp)
- ログインサービスとファイル転送(ssh[8])
- IRC(Internet Relay Chat)(irc)
- Web閲覧(http, https[9])

となっている。実際に使われた期間は非常に短いが、メールのチェック(smtp)とWeb閲覧(http)

[7] 情報教育用システムではpopのサービスは行っていない。
[8] ファイル転送には、sftpを利用するように指導している。
[9] 情報教育用システムで用意しているproxyサーバを利用する。

がほとんどで、メールの送信やニュースの送受信はほとんど見られなかった。

M2 に関しては、元々の情報教育システムの利用規定を踏襲するのみにとどめた。

このシステムは、情報教育システムが混雑している際に、センターまで赴かずに、利用者が通常集う場所でのアクセス手段を提供する、という目的で運用を始めたところでもあり、利用頻度はまだまだ高くない。利用者には、PPPoE ドライバのインストールと各種設定を行う必要があるが、現在の利用者は用意したドキュメントを読む程度で使える学生ばかりのようで、目だって大きな問題は発生していない。

しかし今後、もっと長期間の運用を行ってノウハウを蓄積する必要があると考えられる。

### 4.4 商用サービス向け

この構築に当てはまるサービスとしては、MIS 社の Genuine サービス [13] や Root 社の Secure IP Solution[12] などがある。

## 5 まとめ

本稿では、大学などの教育現場の、さまざまな運用場所や場面に対して、セキュリティレベルに応じた構内情報コンセントシステムの構成方法と、それぞれの要求に応じた実装とその管理・運用方法との関連、およびその構築・運用例について述べた。

構築したシステムは、比較的安価なパソコンで実現することが可能であり、必要なログ情報などの蓄積に関する知見は、セイキュリティレベルに応じたさまざまなシーンでの運用に役立つと思われる。

## 謝辞

有益な意見や実験の協力を戴いた大阪大学サイバーメディアセンター情報メディア教育研究部門の教職員および学生ボランティアスタッフの皆様に感謝します。

## 参考文献

[1] 石橋 勇人, 阪本 晃, 山井 成良, 安倍 広多, 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 (2001.1).

[2] 西村 浩二, 前田 香織, 相原 玲二 : "遠隔機器制御プロトコル RACP のフレームワークとその応用", 情報処理学会論文誌, Vol.42, No. 12, pp. 2869–2877 (2001.12).

[3] 広島大学情報メディア教育研究センター : "PortGuard.", http://www.portguard.org/ .

[4] 桝田 秀夫, 鈴木 未央, 中西通雄 : "PPPoE を用いた認証付き情報コンセントの実装と評価", マルチメディア、分散、協調とモバイルシンポジウム (DICOMO), Vol.2001, No.7, pp. 379–384 (2001.06.28).

[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), Vol.99, No.56, pp. 131–136 (1999.7.15-16). 京都大学総合情報メディアセンター

[6] 安東孝二, 吉岡顕, 田中哲朗 : "大規模計算機センターのセキュリティ対策事例", 情報処理学会研究報告 (99-DSM-16), Vol.99, pp. 43–47 (1999.11.26).

[7] 渡辺 健次, 只木 進一, 江藤 博文, 渡辺 義明 : "利用者認証と利用者記録機能を実現するゲートウェイシステム OpenGate の開発", 電子情報通信学会 技術研究報告 (INS99-95), pp. 43–48 (2000).

[8] 後藤英昭, 満保雅浩, 静谷啓樹 : "廉価なスイッチと Secure Shell を利用した安全な情報コンセントの構成方法", 信学論 (D-I), J84-D-I, No.10, pp.1502-1505, 2001.

[9] 後藤英昭, 安西従道, 二階堂秀夫, 千田栄幸, 満保雅浩, 静谷啓樹 : "ユーザ認証機構を有する安全な無線 LAN・情報コンセント統合システムの構築", 平成 13 年度情報処理教育研究集会講演論文集, pp.382-385, 2001.

[10] ほそかわたつみ :
"xfw - オープンスペース用 IP 認証システム -",
http://members.itc.keio.ac.jp/~hosokawa/xfw/
.

[11] "不正アクセス行為の禁止等に関する法律",
http://www.npa.go.jp/hightech/
fusei_ac2/kosshi.htm.

[12] "Secure IP Solution",
http://www.root-hq.com/.

[13] "Genuine サービス", http://www.miserv.net/.