設定が容易な可搬型の多用途情報コンセントサーバの設計と実装

桝田 秀夫†, 齊藤 明紀‡, 増澤 利光‡
h-masuda@ime.cmc.osaka-u.ac.jp, saitoh@ist.osaka-u.ac.jp, masuzawa@ist.osaka-u.ac.jp
† 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
‡ 大阪大学大学院情報科学研究科

概要 近年、学会や会議等でネットワーク接続サービス (情報コンセントあるいはホットスポット) を提供することが増えてきている。しかし常設の設備と異なり、短期間に構築・撤収しなければならない、要求されるセキュリティレベルは状況ごとに異なる– そのため設備の移設だけでなく設定や利用者登録および認証系の設定が複雑になる –、など多大な労力を必要とする。本稿では、運用場所や場面に応じたセキュリティレベルを柔軟に選択でき、有線と無線接続の双方に対応し、更に簡便に据え付け・設定・運用できるネットワーク接続サービスシステムとその実装について述べる。本システムはサービスの提供を行なう可搬型のサーバ計算機1台と、小型表示装置、利用者登録用の小型プリンタ等からなる。このサーバは、認証や利用状況の記録の他、通信状況の監視を行なうことができる。

キーワード 情報コンセント, ホットスポット, 利用者認証, 設定容易性, セキュリティレベル

Implementation of portable, easy-to-setup, and multi purpose LAN socket server

Hideo Masuda[1] , Akinori Saitoh[2] , Toshimitsu Masuzawa[2]
h-masuda@ime.cmc.osaka-u.ac.jp, saitoh@ist.osaka-u.ac.jp, masuzawa@ist.osaka-u.ac.jp
[1] Infomedia Education Division, Cybermedia Center, Osaka University
[2] Graduate School of Information Science and Technology, Osaka University

Abstract Recently, LAN sockets and Hot-Spot service are became indispensable at convention or conference. Different from permanent service, such temporary service needs great deal of labor because it must be installed and took away in short time, it must adopt to various security level and security policy for each convention – this means user registration and authentication mechanism set-up became complicated –.

In this paper, we propose a easy-to-setup, easy-to-manage, flexible security level server system which provides both wired LAN socket and wireless hot spot service. The system contains portable PC server which provides network service compact display and compact printer for user registration. The server PC also provides user authentication , logging and packet observation,

keywords LAN sockets, Hot-Spot, authentication, easy-to-setup, flexible security level

1 はじめに

大学や企業に於いて、ノートパソコンの普及などにより、持ち込みパソコンを接続したり、学会や会議などを開催する際の一時的なネットワーク接続性の提供や、来客へのネットワーク接続性の提供など、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。また、文献 [1, 2, 3, 4, 5] など、多くの認証付き情報コンセントシステムが開発・運用されてきている。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り、状況に応じた情報コンセントシステムの運用を行う場合には、そのつどネットワークやシステムに詳しい技術者が必要となるため、簡単には設置・運用ができないことが多いと考えられる。また、学会や会議を行う場合の情報コンセントシステムでは、仮運用を暫く行った後に本運用という時間的余裕はないことが多く、持ち込んでからすぐに運用を開始したいという要求がある。さらに、運用場面に応じて異なる運用ポリシに合わせた複数種類の情報コンセントシステムを保有することは大変であり、同一のシステムを異なる運用ポリシの元で運用できることが望まれる。一方、不正アクセス禁止法 [7] により、ネットワーク管理者はより厳密にアクセスに関する記録や制限を行う必要が出てきているが、まだまだ十分な対策をされないままに運用されている例が見受けられる。このような現状を踏まえ、本稿では、特に設置や運用の簡便性を主たる目的とし、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有線接続や無線接続の情報コンセントシステムを、簡便に設置・運用できるシステムの設計とその実装について述べる。

2 設計方針

本システムの適用範囲として、学会や会議などを開催する際や、来客用の一時的なネットワーク接続性の提供を主たる範囲として考慮する。このとき、本システムの設計方針は、以下の通りとなる。

(設定の容易性)
システム設置時に、その場で最小限の設定で確実に動くこと。また、多くのセキュリティレベルに対応できること。

(運用の容易性)
ユーザアカウントをその場で発行することが可能であること。さらに、事前に登録することも可能とする。

(設置の容易性)
出来る限りコンパクトで、一体型の持ち運び可能な形状であること。さらに、基本的に単体で設置可能とする。

アクセス制限を行えるような情報コンセントシステムを導入しないまま運用してしまっているケースの多くは、「知識を持つ技術者が居らず、導入時設定がたいへんであるから」という場合が多いと考えられる。そこで、情報コンセントシステムのネットワーク構成を数種類に限定することで、設定項目を最低限にすることを考える。

また、利用者認証の出来る情報コンセントシステムで、運用時にもっとも手間がかかるものが、利用者情報の管理であると考えられる。あらかじめ RADIUS などによりユーザアカウントシステムが利用可能である場合は良いが、学会や会議、来客の場合は、一時的なアカウントの発行を行う必要があり、どうしても手間がかかる。そこで、ユーザアカウントをその場で発行する仕組みや、パスワードの再発行の仕組みなどを実装することで、運用の補助を行う。

さらに、一時的なネットワーク接続性を提供する場合、システム自体が大きく、また多数の部品で構成されていると、どうしても設置に手間が掛かる。そこで、一体型のシステムでかつ、単体で設定可能な構成を考える。

3 システムの検討

3.1 設定の容易性

情報コンセントシステムに対する設定項目は、大きく分けて以下のものがある。

- (外部接続)
  外部ネットワークとの接続に関する設定
- (内部接続)
  各利用者パソコンとの接続に関する設定

外部接続に関しては、基本的に単一のIPアドレスをネットワーク管理者から得ることと、defaultの経路が設定できることを満たすことができれば、ほぼすべてのネットワーク接続のパターンを網羅できると考えられる。このとき、設定情報を静的に持つ場合、DHCPを利用して動的に持つ場合が考えられるので、これらを選択して設定可能とする。さらに、近年、B flet's などの低価格の定額インターネット接続が普及しており、郊外型の学会などを開催する場合に一時的に利用することも行われている。本システムではそれらを考慮し、PPPoEを利用して接続する場合も選択可能とする。

内部接続に関しては、文献[6]にあるような複数のセキュリティレベルに対応した接続方式を選択できるようにする。ここでは、少なくとも、

- ハードウェア情報(MAC address)を元にした通信記録取得型
- 利用者登録情報を元にした通信記録取得型

に対応する。

3.2 運用の容易性

利用者情報の管理方法については、大きく分けて以下のものが考えられる。

- (申告ベース)
  自己申告を行う
- (申請ベース)
  申請を行い運用者の手によりアカウントの発行を受ける

また、申告や申請を行う手段によって、

- (オンライン)
  利用者が(パソコンを)システムに接続して行う
- (オフライン)
  運用者の手により上記以外の経路で行う

が考えられる。

利用者情報に関しては、ユーザ名は該当人物の電子メールアドレスを基本とする。これにより、異なる人物のユーザ名が衝突することを回避できることと、何かあった場合の連絡先として機能すると考えられる。

申告ベースの場合は、事前に利用者情報を持っておく必要がないが、通信記録上の利用者情報として、利用者の電子メールアドレスを申告してもらうようにする。

申請ベースの場合は、あらかじめ参加者が分かっている場合は、参加者の電子メールアドレスの一覧を準備しておきシステムに投入しておくことで、受付などでパスワードと共に手渡せるようにする。そうではない場合には、電子メールアドレスをその場でシステムに入力することは時間が掛かると考えられるため、

「年月日+連番+チェックデジット」

をユーザ名として振りだし、ランダムなパスワードを付与したものを出力する。その後、システム利用時に電子メールアドレスをオンラインで申告してもらうことで、通信記録上の利用者情報とする。

本システムでは、あらかじめ用意された外部のアカウントシステムを利用できる仕組みは考慮しない。これは、外部のアカウントシステムの構成がどのようになっているかは、運用組織の都合により大きく異なるため、設定の容易性が大きく損なわれると考えられるからである。また、学会や会議などの一時的な利用を主眼に置いているため、恒常的に運用されている外部のアカウントシステムとの連係は通常必要とされないと考えて差し支えない。

3.3 設置の容易性

本システムは、実装の容易性から通常のパソコンを想定して構成する。このとき、入手可能なパソコンのタイプとしては以下のものがある。

1. 通常のATX型パソコン
2. 省スペース型パソコン
3. ノートパソコン
4. 組み込み用パソコン

通常のATX型パソコンは、どうしても大きく重くなってしまう。ノートパソコンは、ネットワークインターフェイスを複数持たせるための拡張性に乏しく、また拡張できたとしてもPCMCIAなどの高スループット性能を期待できないものしかない。

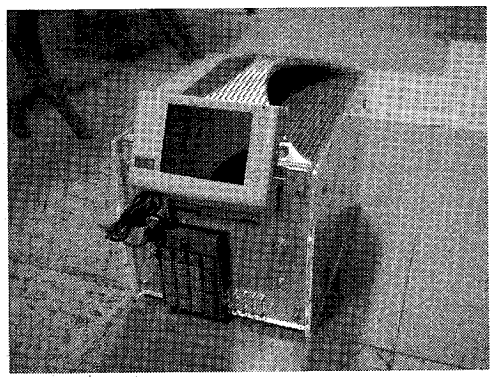

図 1: BOX 型パソコンの例

組み込み用パソコンは、入手性が若干悪い上にコストが高い。ここでは、省スペース型パソコンとして、BOX 型のパソコンを選択する (図 1)。

次に、本システムの入出力装置に関してであるが、設計方針で挙げたように、一体型の持ち運び可能な形状を満たすため、ディスプレイ装置やプリンタ装置、キーボードは、できるだけ小型であるか、そもそも存在しないことが求められる。

つまり、

1. Web ベースの入力・出力

2. 小型コンソール装置 (ディスプレイ, プリンタ 等)

という選択肢がある。Web ベースの入出力は広く使われているが、別途パソコンが必要な上、ネットワークのトラブルが発生した場合など、外部からでは手が出せない場合を考慮し、小型モニタ (図 1 中の 5 インチベイ装着部分) とラベルプリンタを選択する。特に、ラベルプリンタは安価で手に入る上、アカウント情報をシール上に印刷することにより、他の印刷物に貼り込むといった処理が容易となることが期待できる。

入力に関しては、通常のキーボードは場所を必要とすることや、そもそも設定を容易にするために多くの入力を行なわせないことを想定しているため、テンキーとマウスのみで運用可能であるように操作インターフェイスを設計する。

4 システムの構成

本システムの構成概略を図 2 に示す。

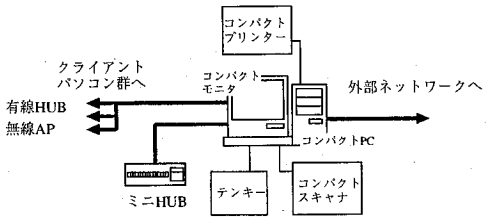

図 2: システム構成図

4.1 ハードウェア

サイズ	W215xD310xH230(mm)
CPU	AthlonXP 2GHz
Mem	512MB
HDD	80GB
I/F	SiS740
	FXP-4TX (PLANEX)
モニタ	LCM-T041A (Logitech)
プリンタ	ラベルプリンタ
その他	KeyPAD, マウス, スキャナ

表 1: システムスペック

システムの中心となるパソコンは、BOX 型の省スペースパソコンを利用し、ディスプレイには 5 インチベイに搭載可能なものを採用している。

コンパクトプリンタ (ラベルプリンタ) を装備し、その場でアカウント発行業務が行える。

キーボードを廃し、テンキーとマウスによる操作を基本とした。当然、必要に応じて通常のキーボードを接続することもできる。

また、即時発行を行う際、利用者情報を簡便に登録するために、コンパクトスキャナを装備すれば、名刺などを読み込んで保存しアカウント情報に対する身元確認情報が関連付けられると考えられる。

さらに、ミニ HUB を装備し、その場で利用者のパソコンを接続して MAC address を登録することも可能にしている。

4.2 ソフトウェア

OS NAT+パケットフィルタ	NetBSD-current(1.6H) IP Filter v3.4.29
Web サーバ Web プロキシ SMTP サーバ DNS サーバ NTP サーバ	apache 1.3.27 squid 2.5 STABLE1 sendmail 8.11.6(OS 附属) bind 8.3.4(OS 附属) ntp 4.0.99i(OS 附属)
DHCP サーバ PPPoE サーバ	ISC DHCP v3.0.1rc9 rp-pppoe-3.5(改造あり)
MAC address 監視	arpwatch 2.1a11

表 2: システムで利用しているアプリケーション

本システムでは、外部ネットワークとの間の通信には基本的に NAT を行い、内部ネットワークには、RFC1918 に定義されたプライベートアドレス空間のうち Class C 相当部分を利用する。また、すべての通過パケットに関して、パケットフィルタによるアクセス記録を取得する。さらに、Web アクセスと SMTP によるメール送信には透過型プロキシを利用したログ取得により、アクセスの監視および制限を行う。また、DNS サーバ, NTP サーバの機能も提供し、内部からの DNS, NTP 要求に応答する。

4.3 設定ツール

以下に設定時の流れを示す。

1. 外部ネットワークとの接続タイプを選択する。まずネットワークインターフェイスを選択し、static/DHCP/PPPoE のいずれかを選ぶ。static の場合は、IP アドレス、ネットマスク、デフォルトゲートウェイを設定する。PPPoE の場合は、アカウント情報を読み込むファイルを指定する。

2. 外部ネットワークとの接続性をチェックする。ping, traceroute, nslookup を用意している。

3. 内部ネットワークとの接続方式を選択する。まず、ネットワークインターフェイスを選択し、それに対して、申告ベースか申請ベースかの選択、MAC address 記録型かユーザ認証型かの選択、を行う。申請ベースの場合は、申請情報の収められたファイルを指定する。ユーザ認証型の場合、さらにユーザ認証方式を選択する[1]。

4. 運用記録レベルを選択する。内部と外部との間、内部同士、外部同士での通信の、いずれを記録するかを選択する。

運用を開始した後に利用できる機能は、以下の通りである。

- 外部ネットワークとの接続状態確認
- システム利用者情報の確認
- 記録ログの参照

5 運用事例

本システムのプロトタイプを、情報教育シンポジウム (SSS2002) で運用した [6]。

5.1 運用方針

本事例では、複数種類のセキュリティレベルの情報コンセントシステムをサービスすることのデモを兼ねていたので、以下の二種類の運用を行った。

1. 有線で接続する場合は、オンラインの申告ベースで利用者情報を登録し、その際に利用されている MAC address と IP アドレスの組が登録されている間のみ外部と通信できるもの。

2. 無線 (IEEE802.11b) で接続する場合は、別途オンラインの申請ベースで利用者情報を登録してもらった後、アカウントをオンラインで発行し、そのアカウント情報を元に PPPoE を用いた利用者認証を経て外部と通信できるもの。

この事例では、無線接続の場合は、一旦有線接続サービスを利用した上でオンライン申請を行うこととした。

[1] 現在のシステムでは PPPoE 型しか実装されていない。

5.2 運用時の設定

本システムを設置する際に必要となる情報は、

- 外部ネットワーク接続情報
- 内部向けの認証用情報

となる。

本運用では、外部ネットワークとの接続は開催時に一時的に付設された B'flets ビジネスタイプで、PPPoE を用いた接続であったため、PPPoE のアカウント設定が必要となるが、事前に設定情報を入れたフロッピーディスクから読み込ませた。

内部ネットワーク向けの認証用情報に関しては、申請情報の入ったファイル名を設定する必要があるが、フロッピーからではなく、オンラインで発行されたアカウント情報が入っているハードディスク上のファイルを指定して運用した。

6 まとめ

本稿では、特に設置や運用の簡便性を主たる目的とし、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有線接続や無線接続の情報コンセントシステムを、簡便に設置・運用できるシステムの設計とその実装について述べた。

これにより、学会や会議などの情報コンセントの運用に関して、単一の可搬型システムにより、様々な場面に適用したシステムが比較的簡単に設置・運用ができることが期待できる。

今後の課題としては、

1. パッケージとしてまとめ、本当に簡便に設置してもらえるかどうかの検証。
2. 他の認証方式も選択して利用できる為のシステム拡張の仕組み。
3. 取得したログ情報の管理方法のさらなる検討。
4. 以前の設定情報やログ情報をきちんとクリアする仕組み。

などが挙げられる。

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。

本研究の一部は、科学研究費補助金 基盤研究 (C)(2) 課題番号 14580449 による。

参考文献

[1] 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).

[2] 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 (1999.12).

[3] 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).

[4] 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の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 (2001.12).

[5] 西村 浩二, 秋成 秀紀, 野村 嘉洋, 相原 玲二 : “遠隔機器制御プロトコルを用いた有線/無線 LAN 用情報コンセントシステム”, 情報処理学会論文誌, Vol.43, No.2, pp. 662–670 (2002.02).

[6] 桝田 秀夫, 中西 通雄 : “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”, 情報処理学会 情報教育シンポジウム (SSS2002) pp. 31–36 (2002.8.21-23).

[7] “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.