ネットワークの一時利用を実現するコンポーネント独立で可搬性の高い利用者管理システムの設計と構築

益井賢次[†,☆] 岡田行央[†,☆] 新井イスマイル[†,☆]
市川本浩[†,☆] 中村豊[†,☆☆]

施設内のネットワーク資源を適切にかつ効率よく運用するために，利用者管理システムを導入することは有効な手段である．しかし，既存のシステムは用途が限定された構成であることが多く，機能拡張や他のシステムとの連携が難しい．そこで本論文では，このような問題を解決すべく，可搬性の高い利用者管理システムのモデルを提案する．本モデルは，属性情報の蓄積，認証・承認，属性情報の生成，サービス提供といった機能を分担する要素で構成される．各々が高い独立性を持つ設計のため，各要素の拡張と置換が柔軟かつ容易に行えることが特長である．また，我々は本モデルにもとづき，実際の利用者管理システムを構築した．本システムは現時点で3ヶ月間稼働しており，その運用状況を併せて報告する．

Design and Implementation of Network User Management System with Component-Independence and High-Portability for Temporary Use

KENJI MASUI,[†,☆] YUKIO OKADA,[†,☆] ISMAIL ARAI,[†,☆]
MOTOHIRO ICHIKAWA[†,☆] and YUTAKA NAKAMURA[†,☆☆]

The user management system provides proper and efficient management of network resources. However, existing ready-made systems are hard to be extended and to interconnect with other systems. To solve the above problems, we propose a model of the user management system that provides high portability. Our model consists of a number of components, which include storage of attributed data, authentication and authorization, generation of the data, and service provision. Since each component of our model is independent with each other, the benefit of our model is flexibility of future extensions and replacement of the components. According to the model, we implemented the user management system, which has been running in more than three months.

1. はじめに

21世紀を迎えた今日，インターネットの利用者数はなおも増加の一途をたどり，その用途も多様さを増すばかりである．それに伴い，宿泊施設や住居施設におけるインターネットへの接続性の要求が高まり，情報コンセントや無線LANアクセス環境の提供が一般的になりつつある．このようなインターネット接続環境は，社会的な情報流通基盤としても重要な役割を果たしている[1)~11)]．

施設が持つネットワーク資源をサービスとして利用者に提供する環境では，資源の適切かつ有効な運用が求められる．このような場合，利用状況に関する情報の収集とアクセス制御を行うネットワーク利用者管理システムを導入することは，有効な手段のひとつである．しかしながら，既存の管理システムは特定の用途を想定したもとで設計・構成されていることが多い．こうしたシステムは，必ずしもネットワーク管理者の多様な要求をすべて満足するわけではない．その結果，管理者はシステムによる制約のもとでの運用を強いられたり，あるいは管理者独自で機能拡張を施して対処することになる．さらに，ここでの機能拡張は特定の

† 奈良先端科学技術大学院大学
Nara Institute of Science and Technology
☆ 現在，情報科学研究科
Presently with Graduate School of Information Science
☆☆ 現在，情報科学センター
Presently with Information Technology Center

システムの性質に依存することもある．これは，管理者に対する負担が大きく，また将来におけるシステム構成の変更の際，再利用性が決して高くないことを意味する．

そこで我々は，前述のような問題を解決すべく，機能拡張が容易でかつその再利用性の高いネットワーク利用者管理システムのモデル化を行った．さらに，そのモデルにもとづき，大学内のゲストハウスにおけるネットワーク利用者管理システムを実際に設計・開発した．本システムは，利用者管理に関わる機能を分散させ，システムのコンポーネントの独立性を保つことで，高い可搬性を有する設計となっている．

本論文の構成は以下の通りである．第2節では，コンポーネント独立で可搬性の高いネットワーク利用者管理システムのモデルを提案する．そして，このモデルにもとづいて設計された大学内のゲストハウスにおけるネットワーク利用者管理システムについて，第3節ではその設計を，第4節では実装を取り扱う．第5節では，このシステムを実際に運用した結果を評価する．最後に第6節では本論文の総括を行い，今後の展望について述べる．

2. モデル

本節では，まず議論に必要な概念および用語について列挙し，ネットワーク利用者管理システムのモデルの提案とその議論へと進む．

2.1 概念と用語の定義

ネットワーク利用者管理システムには，いわゆるAAAと呼ばれるモデルにもとづく機能が求められる．AAAでは，サービス提供に伴うアクセス制御処理を，認証（Authentication），承認（Authorization），記録（Accounting）の3つの要素に分割して考える．認証とは正当な利用者であることの判別を行う機能を指し，判別の手段にはユーザIDとパスワードの組み合せが用いられることが一般的である．認証された利用者は，承認の段階で種々の情報にもとづきサービスの利用権限を付与され，あるいはその付与が拒否される．このようにしてサービスの利用を承認された者の利用状況（利用者のID，利用時刻，利用サービスの種類など）は，利用の事実として記録される．利用状況の記録は，異常時の対応手段のみならず，統計や課金を目的としても用いることができる．

ここで，システム内で発生する処理の表現を定義する．正当な利用者に対してサービスを提供するためには，まず認証・承認に関わる情報を生成および編集する処理が必要である．本論文では，このような情報を属性情報，それを生成・編集する処理を属性管理と名付け，属性管理を担うコンポーネントを属性管理点と呼ぶことにする．また，サービスの利用権限を付与するコンポーネントを承認点，実際のサービスの提供を制御するコンポーネントを制御点とする．以下では，これらの用語を用いて議論する．

2.2 モデルの構成

ここまでの内容をふまえた上で，我々が提案するネットワーク利用者管理システムのモデルを図1に示す．

本モデルは，DBM（database manager），manager，controller，targetをシステムのコンポーネントとして持ち，コンポーネント間で各種情報を授受することで各々が独立して動作する．図中の矢印はAAAに関する情報の流れを示している．DBMは情報の蓄積・管理を担うコンポーネントで，本モデルではすべての情報がDBMにおいて蓄積・管理される．managerは属性管理点であり，managerが生成した属性情報はDBMに渡され蓄積される．そして，利用者がサービスの利用を求めた段階で，承認点であるcontrollerはDBMから属性情報を取得して利用者を認証する．認証に成功した場合は，制御点であるtargetに属性情報を渡し，それにもとづいたサービスの提供がtargetによりなされる．サービスの利用状況は，controller自身が持つ情報やcontrollerがtargetから取得した情報をもとに，DBMに記録される．

以上のように，本モデルはシステム全体としてAAAのすべての機能を提供しており，ネットワーク利用者管理システムとして動作が可能であると考えられる．

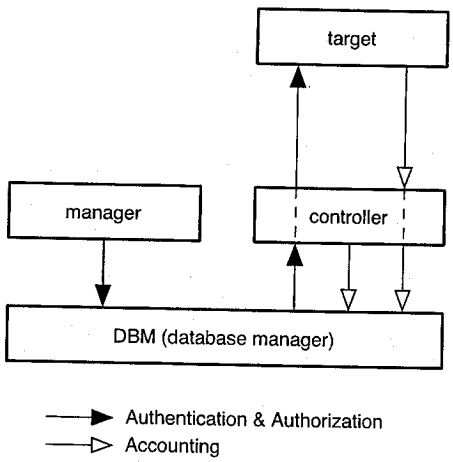

図1 ネットワーク利用者管理システムのモデルと情報の流れ

2.3 モデルの特長

本モデルでは，AAA の提供に関わるコンポーネントが機能ごとに独立・分散しており，コンポーネント間の情報の授受を通じて各々が動作している．さらに，授受される情報は DBM の一点で集中して蓄積・管理され，情報の所在や流れは明確である．これらの点は，システムの要件や問題の切分けを容易にし，設計や運用における一助となる．また，情報の授受に主眼を置いた本モデルでは，情報の形式の整合性を保ちさえすれば，コンポーネントの入替えにも柔軟に対応できる．加えて，情報の種類や形式を拡張し，各コンポーネントをそれに対応させることにより，独立性を保ちつつ容易に機能拡張が可能である．

このように，我々の提案したネットワーク利用者管理システムのモデルは，コンポーネントの独立性とシステム全体としての可搬性を兼ね備えており，多様なシステム要件に対応することが可能でかつ効率的な運用を実現するものとして期待できる．

3. 設　　計

前節で提案したモデルを実際に利用者管理システムとして機能させるための設計について，本節では議論する．

3.1 システムに求められる要素

一般に，システム設計にあたっては次の 3 つの要素を確保することが重要である．

- 利便性
- 可搬性
- メンテナンス性

利便性とは，そのシステムが便利で容易に使うことができるか，という性質を指す．これは管理者・利用者の双方に対して備えられることが好ましい．可搬性が高いということは，システム要件の変化に伴う一部のコンポーネントの入替えの際に，他のコンポーネントを修正する必要がない，あるいはそれが極力少ないことを指す．すなわち，システム構成の変化に対して小さな負担で柔軟に対応することができるかを考える．メンテナンス性は，システムの運用を持続していく上での負担の大小を指す．

これらの要素をすべて兼ね備えたシステムが最も望ましいが，それぞれが相反する要素を含むため，その実現は難しい．システム設計の上では，これらの要素をバランス良く分配し，要件に応じた最適な解を選択することが重要となる．

3.2 システム要件

今回我々は，奈良先端科学技術大学院大学に 2004 年 6 月に建設された「ゲストハウスせんたん」におけるインターネット接続サービスの利用者管理システムの設計を行った．本システムの前提条件として，以下の事項が挙げられる．

- ゲストハウスは大学外の来客・研究者が多く利用する．
- サービスとして提供するネットワーク資源は，大学が所有するものである．
- 本システムの運用・管理は，業者や専門家ではなく大学の関係者が行う．
- 本システムの管理の対象となるゲストハウスの宿泊部屋数は 29 で，規模として大きくはない．

これらを勘案し，我々は以下のようにシステムの概要を決定した．

(1) 管理者が Web フォームで利用者情報を入力することで，利用者のユーザ ID とパスワードが発行される．
(2) 利用者はユーザ ID とパスワードを用いて，Web ブラウザから認証を行う．
(3) 利用者は宿泊期間中，一回の認証でサービスの提供を続けて受けることができる．
(4) 適切な利用が行われているかを確認するため，ユーザ ID，割当 IP アドレス，MAC アドレスを対応付け，利用履歴を残す．
(5) 一部屋ごとに 1 つの IP アドレスを割当てる．
(6) 大学の学生や職員が中心の運用であることを考慮し，運用手順には複雑な処理を含まない．
(7) 本論文で提案したモデルにもとづき，システムを構成する．

ここで，前述の利便性に関しては (1)，(2)，(3)，(5)，(6)，可搬性に関しては (7)，メンテナンス性に関しては (4)，(5)，(6)，(7) を，それぞれの要素を満たすための項目として捉えることができる．

これらの項目に関する具体的な実装については，第 4 節において議論する．

3.3 提案モデルにもとづく設計

ネットワーク利用者管理システムに提案モデルを適用した場合の構成例を図 2 に示す．図中のそれぞれの要素について，Gateway[12] は図 1 における target に，Web AP（アプリケーション）サーバは manager に，RADIUS[13),14)] サーバは controller に，RDBMS (Relational Database Management System) サーバは DBM に対応する．

Web AP サーバは，システム管理者が Web ブラウザから入力した情報をもとに属性情報を生成し，RDBMS サーバに対して登録の問合せを行うことでそのデータ

ベースに登録する．RADIUS サーバは RDBMS サーバに問合せ属性情報を取得して認証を行い，Gateway にサービスの利用に関する承認情報を送信する．そして，Gateway はその情報にもとづき，サービスの提供を行う．サービスの利用状況は RADIUS サーバにより RDBMS サーバのデータベースに記録される．

以上のように，提案モデルの各コンポーネントを実際の機能を持つコンポーネントに置換した．我々はこの設計にもとづいて実装を行った．

4. 実　　装

本節では，ゲストハウスのネットワーク利用者管理システムの実装について言及する．

4.1 実装の概要

今回，図 2 の RDBMS サーバ，Web AP サーバ，RADUIS サーバは同一のホスト内で各サーバプログラムとして動作させた．このホストの OS には FreeBSD[15] を用いた．Web サーバプログラムには Apache[16] を用い，PHP 4[17] で記述された利用者登録スクリプトと組合わせて Web AP サーバを構成した．RDBMS サーバプログラムには MySQL[18] を，RADIUS サーバプログラムには FreeRADIUS[19] を選択した．

また，Gateway は FreeBSD 上で IP Filter[20] を動作させることで，ネットワーク利用の制御を行っている．同一ホスト上では，Apache と dhcpd（DHCP サーバ）も動作している．

4.2 RDBMS サーバの実装

本システムでは，属性情報と利用状況の記録のため，FreeRADIUS に付属のテーブル定義ファイルをもとにテーブル群をデータベース内に作成し，これらを用いている．加えて，本システムは学外の利用者が多いことを考慮し，その身元を明確にするため，以下の項目を対応付ける利用者情報テーブルをデータベース内に追加した．

- ユーザ ID
- 氏名
- 住所
- 連絡先
- 所属
- 部屋番号
- チェックイン・チェックアウトの日付

これらの情報は，Web AP サーバにより送信される．

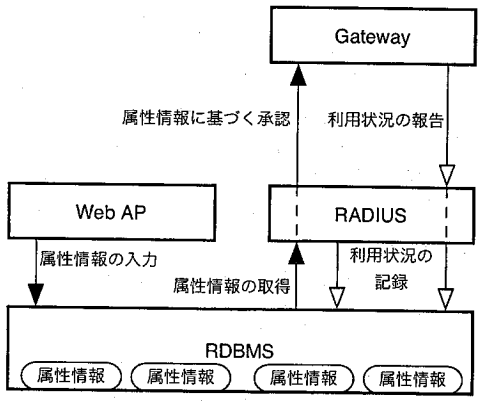

図 2　提案モデルにもとづいた利用者管理システムの構成

4.3 Web AP サーバの実装

管理者は，利用者を登録してユーザ ID とパスワードを発行するために，属性管理点である Web AP サーバに搭載された利用者登録スクリプトを用いる．Web ブラウザで利用者登録ページ（図 3）にアクセスすると，施設の利用情報を入力するためのフォームが表示される．このフォームに氏名・住所等を入力すると，送信された情報にもとづきスクリプトはユーザ ID，パスワードを含めた属性情報を生成する．ここで，ユーザ ID は部屋番号とチェックインの日付から一意に決定されるため，重複は起こらない．また，チェックイン・チェックアウトの日付からサービスの利用を承認する期間を算出し，これを属性情報の一部としている．最後に，スクリプトは RDBMS サーバに接続し，生成した属性情報をデータベースに登録する処理を実行する．

以上の手続きを経て，インターネット接続サービスの提供の準備が整ったことになる．

4.4 認証機構と Gateway の実装

利用者の認証手続きは，以下の手順により行われる．

(1) 未認証の利用者がゲストハウスの情報コンセントに端末を接続すると，Gateway 上の DHCP サーバは端末に対してプライベート IP アドレスを割当てる．Gateway は，プライベート IP アドレスが割当てられた端末から自身以外のリソースへのアクセスをすべて遮断する．

(2) プライベート IP アドレスが割当てられた端末が外部の Web サーバへ接続しようとすると，Gateway は認証のための Web ページ（図 3）に利用者を誘導する．

(3) Gateway は Web の BASIC 認証を利用して，ユーザ ID とパスワードの入力を利用者に求める．

(4) Gateway が RADIUS サーバに認証の問合せを

行い，認証および承認の応答があった場合は利用者端末にグローバルIPアドレスを割当てる．また，端末のMACアドレスを取得し，IPアドレスと対応付ける．Gatewayは，グローバルIPアドレスが割当てられ，かつそれに対応するMACアドレスが一致する端末に対してのみ，自身以外のリソースへのアクセスを許可する．

5. 運用評価

本システムは2004年6月より稼働を開始し，現在も継続して稼働中である．ここでは，2004年6月1日から2004年9月11日までの利用状況の記録をもとに，本システムの運用状況を報告する．

図4に，利用者のネットワーク接続時間の分布を示す．集計において，接続時間の幅は10分単位とした．1000分以上の接続は少数であったため，図中では省略している．この図から，ネットワーク接続時間の多くが100分以内に分布していることがわかる．なお，ネットワーク接続時間の平均は392.7分，標準偏差は1114.9分であった．これらの値がともに大きいのは，極めて長時間接続した端末が数点存在したためである．

また，図5は1日のネットワーク利用者数の推移を示したものである．期間中のネットワーク利用者数の1日平均は3.6人であった．数回見られる利用者の急激な増加は，大学で開催されたイベントによる宿泊客の増加が原因であると思われる．

現在，本システムは稼働開始時からシステム構成の大きな変更もなく順調に稼働を続けている．今後も各種要件に柔軟に対応しつつ，運用を継続する予定である．

6. おわりに

本論文では，ネットワーク管理者の多様な要求に応えうる，コンポーネント独立で可搬性の高いネットワーク利用者管理システムを提案した．さらに，提案モデルにもとづいたネットワーク利用者管理システムを設計し，大学内のゲストハウスに実際に導入して，

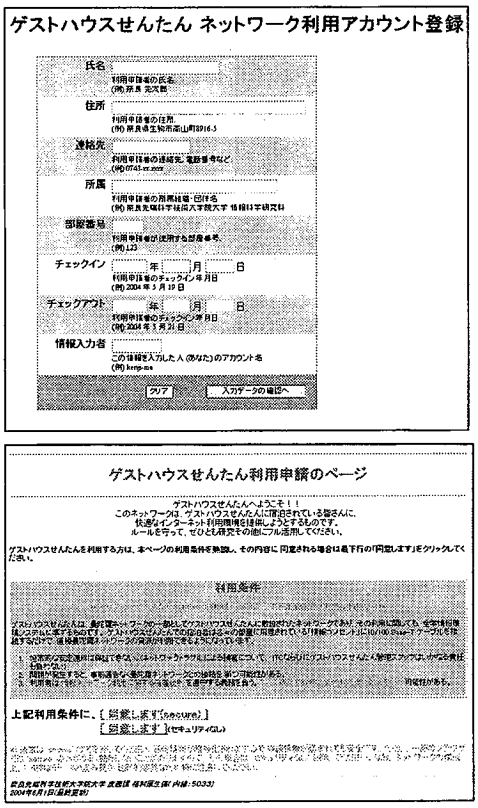

図3 利用者登録フォーム（上）と利用者認証ページ（下）

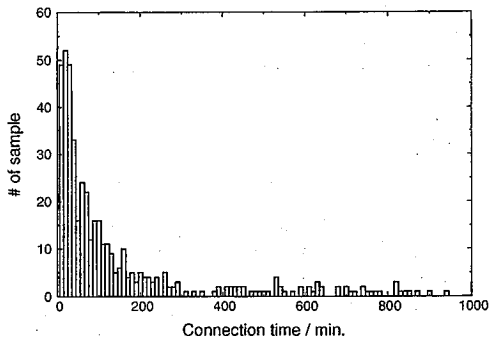

図4 ネットワーク接続時間の分布

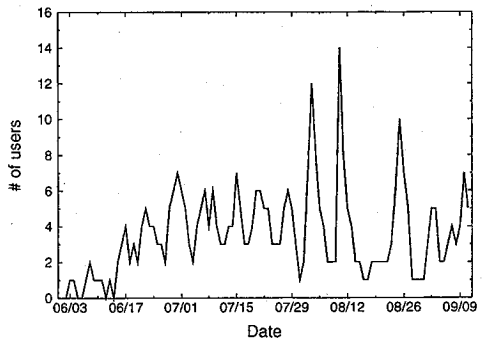

図5 ネットワーク利用者数の推移

これが問題なく稼働していることを確認することができた．現在までシステム構成に大きな変化はないため，実際の可搬性については十分な議論をなすことはできないが，モデルで示したようなシステムの柔軟性を実現しうるものと考える．

今後我々は，本システムの運用を続けてノウハウを蓄積しつつ，管理者・利用者の双方にとってメリットの大きいネットワーク利用者管理システムについての検討と改良を重ねていく予定である．

参考文献

1) JPCERT/CC: 技術メモ - コンピュータセキュリティインシデントへの対応，JPCERT/CC (2002)．
2) 渡辺 健次，江藤 博文，只木 進一，渡辺 義明: 利用者認証と利用記録機能を実現するゲートウェイシステム Opengate の開発，信学技法，Vol. 99, No. 591, pp. 43–48 (2000)．
3) 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)．
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，山井 成良，安倍 広多，阪本 晃，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. 01-008, pp. 79–88 (2001)．
6) 石橋 勇人，山井 成良，森下 英夫，森 俊明，安倍 広多，松浦 敏雄: 無線 LAN における利用者認証機構，情報処理学会 分散システム/インターネット運用技術，No. 021-003, pp. 13–18 (2001)．
7) 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 分散システム/インターネット運用技術，No. 014-024, pp. 131–136 (1999)．
8) 篠宮 俊輔，萩原 洋一: 大学キャンパス無線アクセスシステムの構築，情報処理学会 分散システム/インターネット運用技術，No. 021-002, pp. 7–12 (2001)．
9) 枡田 秀夫，鈴木 未央，中西 通雄: PPPoE を利用した認証付き情報コンセントの実装と評価，情報処理学会 分散システム/インターネット運用技術，No. 021-004, pp. 19–24 (2001)．
10) 高比良 廣人，藤村 直美，堀 良彰，平山 善一: 学内 LAN 管理・運用支援システムの構築と運用について，情報処理学会 分散システム/インターネット運用技術，No. 025-001, pp. 1–6 (2002)．
11) 奈古屋 広昭: 社会科学系大学における認証付きアクセスポイントの構築と運用，情報処理学会 分散システム/インターネット運用技術，No. 025-007, pp. 37–42 (2002)．
12) 市川 本浩，赤木 永治，新井 イスマイル，中村 豊，砂原 秀樹: ボランティアによる運用を考慮した簡便で可能性の高い認証管理ゲートウェイシステムの開発，マルチメディア，分散，協調とモバイル (DICOMO 2003) シンポジウム論文集，pp. 33–36 (2003)．
13) RFC 2138: Remote Authentication Dial In User Service (RADIUS).
14) RFC 2139: RADIUS Accounting.
15) http://www.freebsd.org/
16) http://www.apache.org/
17) http://www.php.net/
18) http://www.mysql.com/
19) http://www.freeradius.org/
20) http://coombs.anu.edu.au/~avalon/