「マルチメディア，分散，協調とモバイル
(DICOMO 2003)シンポジウム」平成15年6月

ボランティアによる運用を考慮した簡便で可用性の高い認証管理ゲートウェイシステムの開発

市川本浩　赤木永治　新井イスマイル　中村豊　砂原秀樹

奈良先端科学技術大学院大学　情報科学研究科

An User Authorization Management Gateway System with Convenience and High-Availability in consideration of volunteer activities

Motohiro ICHIKAWA, Eiji AKAGI, Ismail ARAI, Yutaka NAKAMURA and Hideki SUNAHARA

Graduate School of Information Science, Nara Institute of Science and Technology

概要

大学における教育・研究を支援するための環境として、情報コンセント、無線LAN等の設置／配備が一般的になりつつある。これらの運営管理は、教官・学生等を主体としたボランティアによって行われていることが多い。我々は、ボランティアによる運用・保守を考慮し、学内に登録されている特定多数の利用者が、さまざまな機器を接続し利用するネットワーク環境に適用可能な、利用認証登録と利用記録を行う為の認証管理ゲートウェイシステムを開発した。本システムは、接続機器よりのWebアクセスによる利用認証登録を行い、接続機器の登録と利用者との関連付けを行う。認証登録後は、接続機器の固有識別子によるゲートウェイの制御を行い、接続中のみアクセス可能とする。利用権限失効、または、Webアクセスによる接続機器の終了申請までは、接続毎の利用認証登録の必要はなく、かつ、運用スタッフ等による事前の利用登録といった作業は発生しない。ボランティアによる運用・保守性を考慮し、標準的なUNIX環境での運用を想定し、標準的なアプリケーションとシェル・スクリプトによる構築を前提として、設計・構成を行った。プロトタイプ・システムのホストOSは、Linux上で行った。本運用システムは、運用に関わる学生ボランティアに合せ、FreeBSD上とした。本システムは、学内の学生宿舎ネットワークに適用し、2002年11月より、運用を行っている。

1　はじめに

近年、インターネットアクセス可能な機器の低価格化、ブロードバンドメディアの急速な展開、そして、パソコン等で稼動する無料で高性能なOSの普及を背景としたインターネット利用環境の拡大に伴い、いわゆる、情報コンセント、無線LAN等のアクセス環境の存在や接続性に対する要求が増しつつある。その一方で、社会における情報の流通基盤としての役割も、期待されつつある[1][2][3]。しかしながら、外部委託や専任スタッフの導入といった手段も、予算や要員のスキル、そして、時代の変化に合わせた運用ポリシーや手法等確立といった問題もあり、一筋縄ではいかない。運用等を、教育・学習や訓練の一環としている場合は、例外として、運用管理を、教官・学生等を主体としたボランティアによって行う場合、スキル・レベルが一定ではなかったり、管理に幾つかの問題が発生する事が多い[4]。そこで、我々は、ボランティアによる運用・保守における各問題点の軽減を図りながら、利用側にも、利用に際して負荷をかけにくい、学内に登録されている特定多数の利用者が、さまざまな機器を接続し利用するネットワーク環境に適用可能な、利用認証登録と利用記録を行う為の認証管理ゲートウェイシステムを開発した。設計にあたり、要件として、

(1) 利用機器が、Windows、MACOS、PDA、そして、PC-UNIX等、多岐に渡り対応可能とする為、新たなソフトを必要としない可能性の高い、DHCPを利用する。

(2) 登録にはWebブラウザを利用するものとし、利便性を考え、テキスト・ブラウザでも登録可能とする。

(3) サービス利用者の機器とその割当IPと利用者とを関連付けを行うなんらかの仕組みにより管理を行う。

(4) サービス利用開始と終了の記録とこれに伴うIPフィルタ等によるアクセス制御を行う。

といった項目があり、これに基づき、

(1) 学生ボランティアが中心となる運用を考慮。

(2) Virus対策やセキュリティ対策等に伴うシステム更新がし易い様に、メンテナンス性を考えて、できる限り特殊な仕組やプログラムは利用しない。

(3) 管理は、利用者割当IPとユーザーIDを対応付け、これに、利用機器の識別子（MAC Address）を関連させる事により行う。

(4) ゲートウェイシステムとして利用するPC UNIXのOS固有機能に頼らなくてもすむ実装とする。

(5) 省労力化を考慮する（e.g. MAC Addressの登録等の利用者登録）。

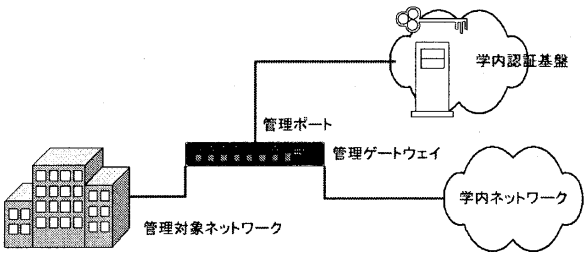

図1　システム概要

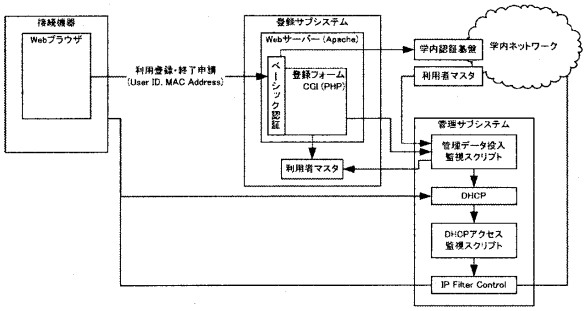

図2　システム構成

といった方向性で、開発を行った。本論文での構成は、下記のようになっている。2章では、本システムの概要を述べる。3章では、適用をした学内の学生宿舎ネットワークにおける構成について述べる。4章では、学生宿舎ネットワークでの運用評価について述べる。最後に5章で本論文をまとめる。

2　システムの概要

本章では、システムのおおまかな構成と概観について述べる。具体的なシステムの振る舞いについては、3章で述べる。

2.1　構　　成

構成は、いたって単純である。制御対象となる2つのインターフェースに、学内の認証基盤への接続や管理を行うインターフェースの計3個から構成されている。図1に概要を示す。管理対象となるネットワークは、DHCPにより管理を行う。DHCPが配布するアドレスは、2種類ある。新規登録時の配布されるプライベート・アドレスと、登録後に割当配布されるアドレスである。図2に構成を示す。システムは、おおまかに、登録サブシステムと管理サブシステムから構成されている。これらのサブシステムは、1章で述べた方針に基づき、メンテナンス性、可搬性を考慮して、

(1) シェル・スクリプトで構成。

(2) ファイルシステムをデータベースとして利用、割当IPアドレスをファイル名として、インデックスの代わりに使用。

として、設計を行った。

2.2　登録サブシステム

(1) 利用者情報および利用機器情報（MAC address）の登録と削除。

(2) 処理の記録。

2.3　管理サブシステム

(1) 利用者と割当IPの関係表である利用者マスタ更新時の管理情報の整合。

(2) 登録情報に基づくDHCPの設定ファイルの更新とその際のDHCP daemonの再起動（1分毎に、RequestQueueを監視）。

(3) DHCPの管理ログからのDHCPアドレスの配布状況の監視とIPフィルタの制御（アクセス制御）。

(4) 接続の管理単位である有効期限（10分）の監視とIPフィルタの制御（アクセス制御）。

(5) 上記処理の記録。

3　学生宿舎ネットワークの構成

本章では、システムを実際に適用した「学生宿舎ネットワーク」を例にとり、まず、「学生宿舎ネットワーク」を簡単に説明し、次に、登録サブシステムと管理サブシステムの処理について述べる。図3と図4にそれぞれの処理の流れを、図5と図6に各状態の画面を示す。

3.1　学生宿舎ネットワーク

学生宿舎ネットワークは、学内の統合情報ネットワーク（曼陀羅ネットワーク）の一部として学生宿舎に敷設されたネットワークである[1]。8棟から構成され、490名前後が利用登録を行っている。10Mと100Mが混在している。本システムは、それらのネットワークを100MのL2 switchに集約の後、管理対象インターフェースに接続し、管理を行っている。

[1] http://itcw3.aist-nara.ac.jp/dormitory/index-j.html

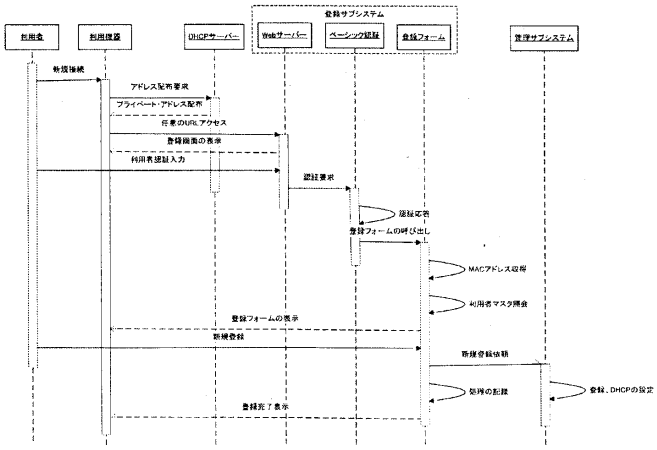

図3　登録サブシステムの処理

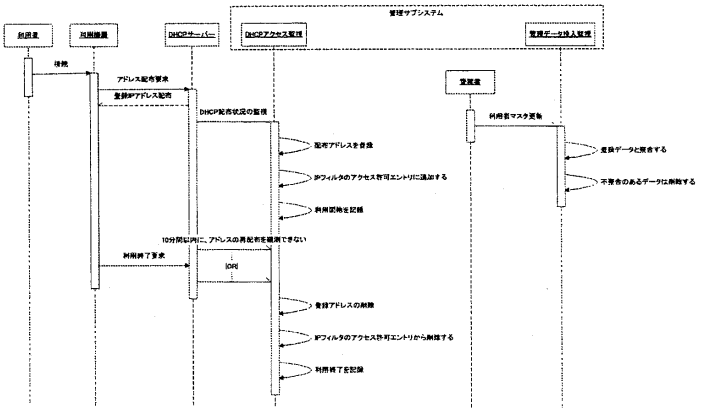

図4　管理サブシステムの処理

図5　利用者認証・登録完了画面

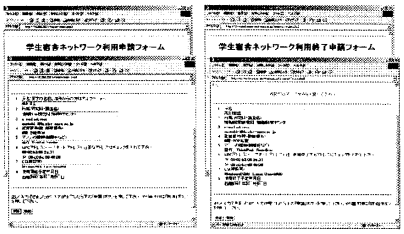

図6　利用登録・終了申請画面

3.2　登録サブシステムの処理

3.2.1　利用機器登録

閉鎖状態 (新規機器登録 Web フォームの動作)

(1) 未登録機器を接続すると DHCP により、プライベート・アドレス (10.254.252.0/21) の割り付け。

(2) 任意の Web ブラウザにより、任意のアドレスをアクセスすると、10.254.252.1 の利用機器登録の Web フォームへ、誘導される。

(3) Web のベーシック認証を利用し、利用者の認証を行う。認証モジュールは、mod_auth_external を利用し、任意の認証方式が利用可能とした。認証データベースは、学内システムの提供する環境を利用し、nis を利用した。

(4) 利用者認証情報を元に、利用者マスタ (宿舎名簿) より、宿舎での利用可能の有無と割当 IP を確認する。なお、Web フォームのスクリプト言語は、PHP3 を使用。

(5) Web へのリクエスト IP 情報と ARP を利用して、接続機器の MAC Address を得る。登録ログを検索し、新規登録で無い場合は、登録データベースより登録済 MAC Address を抽出し、追加登録の際に利用終了 MAC Address の削除を行える様にする。

(6) 簡単な整合性チェックの後、登録リクエストのファイルを作成し、所定のフォルダに書き込む。登録ログに、CSV 形式で、登録情報を記録する。また、処理のログを作成する。

(7) 1 分毎に実行される、登録管理ジョブにより、DHCP 配布データベースの再構築が行われ、利用機器を再接続後、所定のグローバル・アドレスが割り振られ、かつ、ゲートウェイを通して、学内および学外へアクセス可能となる。

3.2.2　利用終了（削除）申請

機器利用終了申請は、

(1) 新規（追加）登録 Web フォーム。

(2) 機器利用終了申請 Web フォーム（学内からアクセス可能）。

(3) 利用者マスタ (宿舎名簿) の更新時のバッチジョブ。

のいずれかで、行われる。(1) は、前項と同様である。(2) は、前項のフォームより、新規登録機能を省いたものであり、認証手順等は、同等の方法で行われる。(3) は、利用者マスタ (宿舎名簿) 更新時、利用者識別子と割当 IP の整合性と有無の確認を行い、整合しない場合は、データベースより削除を行い、処理をログに記録する。

3.3　管理サブシステム

3.3.1　登録管理ジョブ

(1) Web フォームよりのリクエストをリクエスト・フォルダを監視する事によって行う。リクエストは、処理中を示すロックファイルの有無、ファイルのタイムスタンプの、利用開始（変更）希望日比較を経て実行される。

(2) 簡単な妥当性確認の後、既存レコードがある登録情報は、利用済を格納するフォルダへ移動され、リクエストファイルは、その後、登録される。その際、DHCP 設定ファイルの再生成や、ログへの記録が行われる。

(3) 利用者マスタ (宿舎名簿) 更新ファイルの投入監視により行う。処理は、前項の (2) と同じである。

3.3.2　利用管理

(1) 利用機器識別子（Mac Address）と利用機器からの DHCP 再収得によって、アクセス制御を行う。具体的には、

(2) リース期間を最大 10 分とし、割当アドレスの配布を行う。

(3) 配布時、割当アドレスがゲートウェイを通過可能な様に IP パケットフィルタテーブルに登録。また、ログに利用開始を記録。

(4) リース期限内に再リース要求が来ない場合、もしくは、リリース要求が来た場合、利用終了と判断し、IP パケットフィルタテーブルから、削除。また、ログに利用終了を記録。

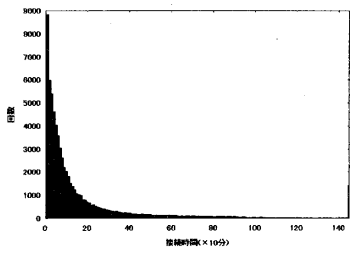

図7　接続時間ヒストグラム

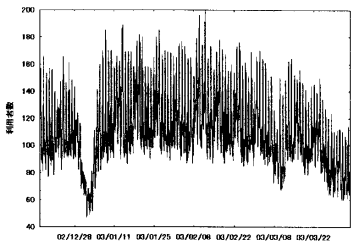

図8　利用者数の推移

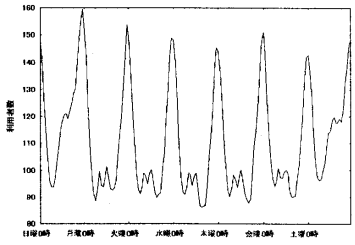

図9　週平均による利用者数の推移

4　運用評価

2002年11月より、割当IPへの複数のMAC Addressの割付等の機能拡張を行いながら、運用を行って来た。当初、試作・実験システムのホストOSは、RedHat Linuxで行い。初稼動時は、運用予定の学生ボランティアの希望に合わせ、Debian GNU Linuxを使用した。2003年4月より、運用する学生ボランティアに合わせ、FreeBSDで稼動させている。図7に、2003年4月までの利用接続時間のヒストグラムを、図8に、毎時集計した利用者数の推移を、図9に、曜日ごとに集計して平均を求めた週間の推移を示す。常時接続数は、平均100名前後、持続接続時間は、平均140分前後であった。この状態で、アクセス制御付のゲートウェイとしては、安定して動作しており、当初の設計目標は、達成されていると考える事ができる。しかしながら、当初から予想されていた事であるが、幾つかの問題点もある。

(1) 独自DHCPサーバー（Apple社のAirStation問題等）。

(2) MAC Address詐称。

(3) 盗聴等にたいする、プライバシに関する配慮。

(1)に関しては、運用当初、度々、問題となった。しかしながら、学生ボランティア諸氏の啓蒙活動により、鎮静化した。しかしながら、可能であれば、マルチプルVLAN[2]等の機器と組み合わせ利用すべきと考える次第である。(2)は、現行システムでは、防ぎようがない。しかしながら、利用されていないIPアドレスが野放しにならないよう利用者管理がされ、同時に利用される機会が多くIP衝突によって、発見される機会が多ければ、詐称による被害は、致命的にはなりにくいかと考える。(3)に関しては、10Mのセグメントは、10base2を一部に利用している為、深刻であり、認証等を行う際は、SSLを利用するといった予防処置の啓蒙を行っている。また、本システムは、職員宿舎ネットワークに、適用予定である。

5　まとめ

本論文では、ボランティアによる運用・保守を考慮した、特定多数の利用者が、さまざまな機器を接続し利用するネットワーク環境に適用可能な、利用認証登録と利用記録を行う為の認証管理ゲートウェイシステムの開発について、述べた。本システムは、簡便な仕組みを利用した、メンテナンス性の高く、カスタマイズ等の行いやすいシステムであり、管理負担も少ないシステムである。しかしながら、記録時間の粒度、MAC Address詐称や独自のDHCPサーバー問題等の問題がある。これらの特性を考慮した上で、ほどほどの利用管理が可能なシステムとしては、有用ではないかと考えている。また、利用記録といった面では、不特定多数の利用者に関しても、時間を基準として、また、メール等と組み合わせ、適用可能ではないかと考えている。

謝辞　学生宿舎ネットワークでの適用・構築にあたって、御協力頂きました、Student Volunteer Program(SVP)[3]ならびに寮ネットワーク運営委員の皆さん、そして、情報科学センターの皆さん[4]、末筆ながら、感謝いたします。

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.「特集：次世代のインターネット／分散システムの構築・運用技術」情報処理学会論文誌 Vol.l42 Number12, 2001.

[3] 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 8, 2000.

[4] 飯島昭博, 菊池豊, 越塚登, 今泉貴史, 大野浩之, 松田林, 新美誠, 本城弘幸, 藤井光昭. ボランティアに依存せずキャンパスLANを運用する7つの鉄則　東京工業大学Titanet運用センターの試み. 情報処理学会 分散システム運用技術 No.004, 1996.

[2] http://www.allied-telesis.co.jp/products/product/switch/multivlan/

[3] http://svp.aist-nara.ac.jp/index.html

[4] http://itcw3.aist-nara.ac.jp/index-j.html