学術情報処理研究
No.18 2014 pp.53–60

キャンパスネットワーク運用評価と MAC-IP 監視管理システムの構築

Assessment of the Campus Network System and Construction of MAC-IP Monitoring and Management System

清水さや子†，横田賢史†，吉田次郎†，萩原知明†，鈴木直樹†，戸田勝善†
Sayako Shimizu, Masashi Yokota, Jiro Yoshida, Tomoaki Hagiwara, Naoki Suzuki, Masayoshi Toda
{smz, yokota, jiroy, tomoaki, naoki, toda}@kaiyodai.ac.jp

†東京海洋大学情報処理センター
Information Processing Center, Tokyo University of Marine Science and Technology

概要

近年，多くの大学のネットワーク環境は，認証機能を追加するなどセキュリティや利便性を重視したシステムに更新されている．東京海洋大学品川キャンパスではキャンパスネットワークへの接続において，紙ベースによるネットワーク接続申請を行っている．また，IP アドレスと端末情報の管理のためのシステムである，DNS/端末管理システムを運用してきた．利用者は，発行 IP アドレスを端末に設定するだけでネットワークに接続でき，機器や人に対する認証などの制限はなかった．さらに，紙ベースの IP アドレス申請・承認で運用し厳密な管理が困難であったため，様々な運用上の問題点が発生していた．これらの問題の解消および利用者の利便性向上のため，端末の MAC アドレスと IP アドレスを関連付けして認証するシステム（MAC-IP 監視管理システム）を品川キャンパスにおいて試験的に導入した．このシステムでは，Web ベースでの申請・承認を導入し，ログイン時の認証には，複数の利用者が扱えるようにグループ管理機能を取り入れ，利便性を向上させた．本稿では，従来の IP アドレス発行システムの問題点を精査し，問題解決のための新システムの要件について述べるとともに，その要件に基づいた実装の詳細ならびに運用状況について報告する．

キーワード

IP アドレス，MAC アドレス認証，MAC-IP 監視管理，キャンパスネットワーク，グループ管理

１．はじめに

近年，多くの大学のネットワーク環境は，認証機能を追加するなどセキュリティを重視したシステムに更新されている．東京海洋大学品川キャンパスのキャンパスネットワークの接続に関しては，前身の東京水産大学当時から認証方式を用いることなく，ユーザからの紙ベースによるネットワーク接続申請を行っている．システム管理者は，IP アドレスと端末情報の管理のため，DNS/端末管理システムを継続してきている．なお，無線 LAN システムに関しては，2010 年度に学内の共有場所にのみ導入しているため，当初から Web 認証を採用している．

品川キャンパスのキャンパスネットワークでは，紙による申請であったため，申請した端末と発行された IP アドレスに対する厳密な管理が困難であり，ネットワーク接続時に，IP アドレスの使いまわしや，

IP アドレスの競合，使わなくなった IP アドレスが返却されないことなどの問題が頻繁に発生していた．そこで，セキュリティや利便性向上のため，他大学の状況を参考にキャンパスの利用状況に適合した独自の認証システム設計を行い，MAC-IP 監視管理システムを構築し，認証にはグループ管理機能を取り入れ，段階的に導入した．

本稿では，既存の DNS/端末管理システムの問題点を精査し，問題解決のための新システムの要件について述べるとともに，その要件に基づいた実装の詳細ならびに運用状況について報告する．

2 章では，既存システムに関して，3 章では，新システムの要件を述べる．4 章では，実装するシステムについて述べ，5 章では実装したシステムの評価，最後に 6 章では，まとめを述べる．

2．既存システムと運用上の問題点

2.1 既存の DNS 管理システム

これまでの IP アドレスと端末情報の管理は，端末情報管理機能により，システム管理者（情報処理センター職員）が IP アドレスと端末名，MAC アドレスを含む端末情報の登録をすれば，IP アドレスと端末情報が DNS サーバに登録される仕組みである（図 1）．端末情報管理機能により MAC アドレス情報や端末情報を登録するが，それらによる接続制限は設けていない．つまり，MAC アドレス情報が不正確でも接続可能である．ユーザの端末をキャンパスネットワークに接続する際には，各自固定 IP アドレスの設定を行っていた．

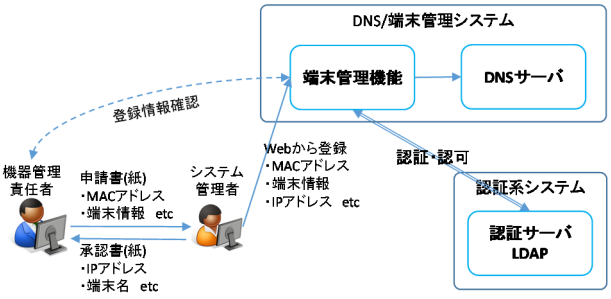

図 1　既存システム

また，端末情報管理機能により，研究室ごとにネットワークを使用する際の使用責任者（以下，機器管理責任者とする）が，指定の URL から自身の統合 ID とパスワードでログインすれば，管理する端末情報を閲覧することができる．機器管理責任者は，各研究室であれば教員がなり，事務局であれば事務局内のネットワークを管理する部局があるため，その部局の長職がなる．

2.2 IP アドレス発行と管理運用上の問題点

キャンパスネットワーク導入当初から IP アドレス発行プロセスは次の通りである．

① 紙ベースによる IP 発行申請
② 申請に応じて随時 IP アドレス発行，未使用・機器変更となった IP アドレスは返却
③ 発行 IP アドレスの管理は機器管理責任者に一任

①の IP 発行申請は研究室単位で機器管理責任者の教員が行う．数日後にネットワーク接続に必要な IP アドレスなどが記入された承認書が返送され，ユーザが許可された固定 IP アドレスを端末に設定して利用開始となる．②のとおり随時発行するため，端末情報管理機能により，管理する IP アドレスリストから，申請時に未使用アドレスを利用者に割り当てる．

上記の手順でこれまで運用していたが，様々なトラブルが日常的に発生しており，セキュリティ面での不備が問題であった．

①の紙ベースでの IP アドレス発行申請と②の紙ベースによる IP アドレス承認・発行の手続きでは，システム管理者（情報処理センター）と利用者のデータの同期に遅れが生じるため，利用者は申請後にすぐにネットワークが使えない．また，ネットワークトラブル時の緊急対応ができない．例えば，申請書の MAC アドレスは機器管理責任者自身が調べて記入することになっているが機器管理責任者の記入ミスや調査方法の間違いが頻発している．また，申請当初の端末から別の新しい端末に変更した場合も，端末変更届はほとんどないため，齟齬が生じてくる．これらが常態化しており，2013 年 11 月 19 日～27

日（9 日間）IP-MAC アドレスを調査した結果，申請書どおり正しく接続している端末は 28%（2327 件中 658 件）であった(図 2).

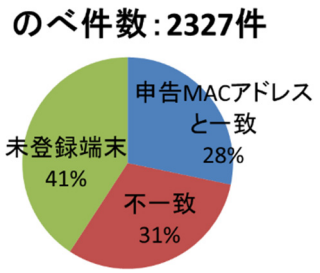

図 2　IP-MAC アドレス整合性調査結果(2013 年 11 月 19 日～27 日，対象エリア：品川キャンパスネットワーク)

IP アドレスの不正利用に伴う IP アドレス競合が発生した場合，正規申請されていても MAC アドレスが間違っているため，不正利用端末の調査が困難となる．結果的に，システム管理者が発生場所に出向いて接続端末を調査しなければならず，多大な労力と時間が必要となる．

②の IP アドレスは随時発行であるが，建屋ごとに，申請順に IP アドレスを割り当てるポリシーとなっていたため，機器管理責任者が管理する IP の範囲が決まっておらず，IP アドレスの入力ミスなどにつながる可能性が高かった．また，発行は申請に応じて行ったために，各研究室の IP アドレス発行数は不均衡となり，発行数の多い研究室ほどアドレス管理が杜撰になりがちである．そのため，IP アドレスの不正使用や，それによって IP 競合時に問題端末が特定できないなどのトラブル発生が多い傾向にあり，更に問題解決にも時間を要していた．ネットワークのトラブル発生時に該当ポートや MAC アドレスの特定はできるが，図 2 のとおり MAC アドレス情報が不正確なため，端末を割り出すための有効な手掛かりにならない場合が多い．正しい情報を得るためにも，ネットワーク接続の際の認証システムが必須であると考える[1].

③で述べた機器管理責任者は，ネットワーク事故などが発生した場合に，責任が取れる常勤職員である必要がある．研究室では教員が機器管理責任者となる．しかし，実際に端末を利用するのは学生を含む構成員であり，機器管理責任者が管理すべき IP アドレス情報や機器設定等は，非常勤職員あるいは大学院生が担当することが多い．ネットワークトラブルの際に機器管理責任者に問い合わせても状況把握が困難で，問題の洗出しに時間・労力がかかる．

これらの問題は，特に研究室や機器管理責任者がそれほどネットワークに精通していない部局ほど顕著であり，しばしば問題を引き起こしていた．ネットワークを利用するにあたって，セキュリティが重視される現在では，これまでの IP アドレス管理運用は危機的状態といえる．ネットワークセキュリティの重大な事態を回避するため，ネットワーク接続時に関する認証システムなどの導入が急がれる．一方で，利用者に受け入れやすいように既存の管理方式を踏襲し，システム管理者側の負担軽減にもつながる新システムの要件について検討した．

３．新システムの要件

新システムにおいて達成すべき目標･必須条件は，次の３つである．

● 手続き処理の自動化・簡素化

ネットワーク管理者側・利用者側双方の事務手続きを自動化し，管理業務量を削減あるいは簡素化できるシステムを目指す．元々，利用者側での IP アドレス管理が杜撰な一因は大学全体的な事務仕事量の増大がその要因の１つと考えられる．書類手続きを削減し，IT 技術の利点を上手く取り入れ，双方でデータを共有できるシステムの提案が必須である．

● 研究室内での接続端末の分散管理

研究室内でのネットワーク接続できる端末の管理は，従来どおり機器管理責任者の管理の元に行う．これは，分散管理を行うことで，システム管理者の負荷を分散させるだけでなく，これまでの大学内での研究室の独自性を重視しつつ，教職員のセキュリティ意識（ネットワーク利用に関する自由と責任の認識）向上にもつなげるためである．

- **ネットワーク関連トラブルの迅速な対応と回避策**

トラブル発生箇所の迅速な特定と，その対応ポリシーを明確化する．リアルタイムの IP 監視を実現して，利用者端末の設定変更を最小限に抑制しながら，トラブル発生率削減を目指す.

システム構築にあたり上記３つの目標を実現するため，次のような項目をシステム設定要件とした.

a. 未登録端末の監視
b. 建屋ごとの VLAN
c. 固定 IP アドレスの利用
d. 研究室ごとに一定数の IP アドレス管理
e. グループによる管理の実現
f. 利用者自身の Web 上での機器登録と利用者・管理者双方のリアルタイムの MAC-IP テーブルの共有

設定要件の a から d は，新システムの第 3 の目標であるトラブル回避・迅速解決を実現するためである.

要件 a を実現するためには，本学の品川キャンパスにおける有線 LAN では採用していなかった認証システムを導入する必要がある．他大学では一般の組織と異なり，一元的な組織で管理する端末以外の多くのネットワーク機器が利用されているため，様々な認証機能が採用されている[2,3]．当初は Web 認証方式が多かったが，プリンタ，複合機，IP 電話機など認証操作が困難なネットワーク接続端末も多数存在するため，端末の MAC アドレスを事前登録して接続に認証する方式（MAC アドレス認証）を併用する方法を多くの大学で採用している [4,5,6,7]．一方, 本学では認証システムを導入していないため，認証方式を併用する必然性は無く利便性に考慮した認証方法を採用することができる．そこで，本システムでは端末管理に重点を置いた MAC アドレス認証を採用することとした.

要件 b は従来からの本学品川キャンパスネットワークポリシーである．建屋別に概ね学科が分かれており，建屋ごとにネットワークを独立させてトラブルは建屋間に拡散させないというポリシーを 2010 年度に改めて決めた．この方針に従って，ある建屋のネットワーク停止によって，下の建屋内でのネットワーク停止を回避するため, 2010 年度にネットワークの物理配線もツリー型から情報処理センターからのスター型に変更している.

設定要件 c も品川キャンパスネットワークのポリシーである．各研究室では，ファイアウォール通過の設定を行い学外サーバとの接続をする端末がある他，共有プリンタ，複合機，監視カメラ等が存在するため，必ず固定 IP を必要とする．動的 IP アドレスと併用すると，問合せや個別対応が増え可能性が高くなり，システム管理者が不足する現在の状況にそぐわない. これらより, IP アドレス管理の一元化・簡素化のためにも固定 IP アドレスを継続することとした.

設定要件 d は，管理者側のトラブル箇所特定の迅速化のために盛り込んだ．従来の IP アドレス随時発行の際には，IP アドレスと各研究室の関係（ひもづけ）が任意であったため検出に手間と時間を要した．また，IP アドレス発行数の不均衡に起因するトラブル発生の増加と問題個所特定の煩雑さを解消するため，研究室ごとにあらかじめ連番で割当てることとした．これによって，トラブル時の対応の負荷軽減につながる.

設定要件の e と f は，新システムの第 1 の目標：利用者・管理者双方の作業量抑制と効率化を実現させるために新たに導入する．特に要件 e のグループによる管理は機器管理責任者の裁量でシステムを操作できる利用者（以下，機器管理者とする）を追加登録・削除できる．これは，第 2 の目標とも関連して，機器管理責任者の ID・パスワードの使い回しの防止だけでなく，非常勤職員や院生が管理する実情に合わせた形を実現することができる新たな試みである.

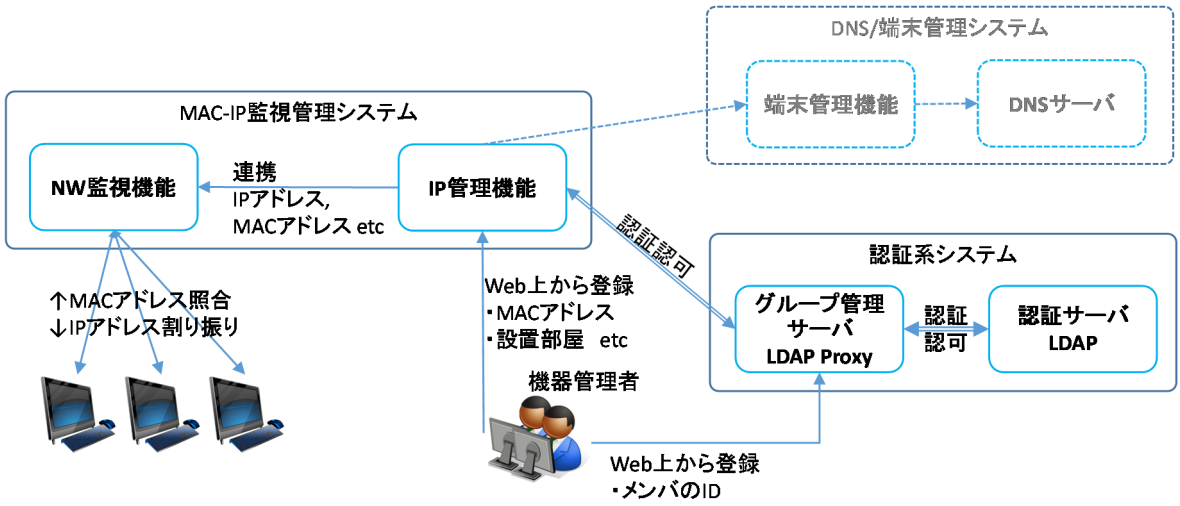

図 3　MAC-IP 監視管理システムと他システムの連携

4．MAC-IP 監視管理システムの実装

4.1 MAC-IP 監視管理システムと他システムの連携

本研究で実装した MAC-IP 監視管理システムは，ネットワーク監視機能と IP 管理機能を持つ．ネットワーク管理機能には，大きく以下の 3 つの機能を持つ．

- MAC アドレスの登録
- IP アドレスの払出し
- 未登録端末の検知

また，オープンソフトの DHCP サーバを使用し，IP-MAC 管理テーブルに登録された IP アドレスを払出す機能を提供する．

IP 管理機能では，機器管理者が Web インターフェースにより，IP アドレスの管理や端末情報の登録を行う．

なお，現時点では，既存のレンタルシステムである DNS 情報管理システムとの連携を必要とするため，端末情報管理機能と IP 管理機能は重複する箇所が多いが，次期システム更新時には，DNS サーバ上で IP 管理機能を動かす予定である（図 3）．

4.2 IP 管理機能への認証

IP 管理機能では，格納している IP アドレスや端末情報を csv で出力し，ネットワーク監視機能に送る．また，既存 DNS/端末管理システムと連携する為，端末情報管理機能にも送る．さらに，IP 範囲とグループ情報の紐づけをすることにより，該当グループのメンバを機器管理者とする．

グループ管理機能では，グループ管理者とメンバは統合 ID を用いる．グループの管理者は，機器管理責任者とし，グループのメンバは，グループの管理者である機器管理責任者が指名する学生や秘書などとする．グループのメンバに登録されると，機器管理者として，IP 管理機能の操作が行えるようになる．メンバの登録方法は，グループ管理者がグループ管理サーバに自身の統合 ID とパスワードでログインし，メンバとして登録したいユーザの ID を列挙する．また，グループ管理者である機器管理責任者が退職などにより，不在となる場合は，次に引き継ぐ機器管理責任者がグループ管理者として登録する．グループ管理者は，機器管理責任者だけでなく複数名を設定可能であるが，最低 1 名以上の責任権限のあるユーザ（正規教職員）を含むことが必要である [8]．

グループ管理者に統合 ID を用いることより，退職などにより統合 ID が削除されれば，グループ管理者からも削除される．グループ管理機能では，グループ管理者が不在になり管理されなくなったグループがいつまでも残らないよう，グループ管理者が不在になる場合は，グループは削除となる．グループ管理者を複数名設定している場合，責任権限のあるユーザが不在になれば，残りのグループ管理者にアラートを上げる．しかし，アラート後，一定期間

内に，残りのグループ管理者が責任権限のあるユーザをグループ管理者として設定しない場合は，グループは削除となる．グループが削除となった場合でも，IP 管理機能とグループ管理機能を切り離して管理していることより，IP 管理機能に登録されている情報は削除されず，これまで登録されている端末は，引き続き使用可能となる．ただし，端末の変更や追加時には，IP 管理機能にログインが必要となるため，再度グループの設定が必要となり，システム管理者が，個別対応を行うことになる．

IP 管理機能で端末情報を管理する場合，機器管理者が，自身のネットワーク名（所属グループ名）を選択し，自身の統合 ID とパスワードでログインする．システム側では，入力した ID が該当グループに含まれているか照合し，照合に成功すれば，ID とパスワードの認証問合せ処理を行う．認証に成功すれば，割当てられている IP アドレスの管理画面が表示され，端末情報の登録・管理を行う（図 4）．

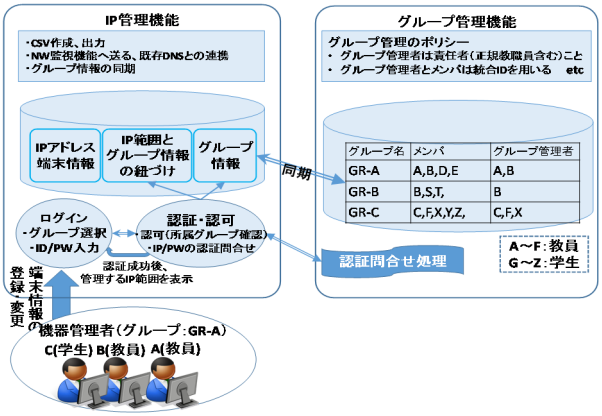

図 4　IP 管理機能への認証の仕組み

IP 情報追加時は，MAC アドレス，端末情報，端末利用者，利用場所などの必要情報を登録する．IP 情報変更時（端末変更時など）は，MAC アドレス，端末情報などの修正をする．IP 情報削除時は，削除が必要な行にチェックし，削除ボタンをクリックする（図 5）．

なお，端末名は IP アドレス割り当て時に，ネットワーク名を使って自動割り当てするため，機器管理者は設定しない．また，システム管理者は，研究室（グループ）ごとに IP アドレスの割り当てを，あらかじめ行う必要がある．

図 5　端末情報の管理画面のイメージ

4.3 ネットワークに接続時の動き

MAC アドレスが登録されている端末を，ネットワークに接続すると，DHCP サーバにより，IP-MAC テーブルに登録された IP アドレスを払出す（図 6）．

IP アドレスの払出すために，以下の機能を兼ね備えている．

- DHCP サーバ
- DHCP サーバ設定機能
- DHCP サーバログ設定・保存機能

MAC アドレスが未登録の場合，IP アドレスを払い出さないようにするために，以下の機能を備えている．

- パケット抽出機能
- 未登録端末検出機能
- パケット抽出・未登録機器検出のログ保存

この機能により，IP-MAC テーブルに登録されていない端末は，学内ネットワークに接続しても，ネットワークにはつながらない．なお，IP-MAC 登録機能としては，IP-MAC 管理テーブルに以下の情報を格納している．

- ✧ ネットワーク名
- ✧ ホスト名
- ✧ IP アドレス
- ✧ MAC アドレス

また，本システムでは，全てのキャプチャできるパケットを解析して DB 化している．これを基にして，その DB 化しているパケットのうち IP-MAC テーブルに関する情報を抽出している．この DB 化，別のパケットの抽出が必要な場合に，容易に対応が可能となる．

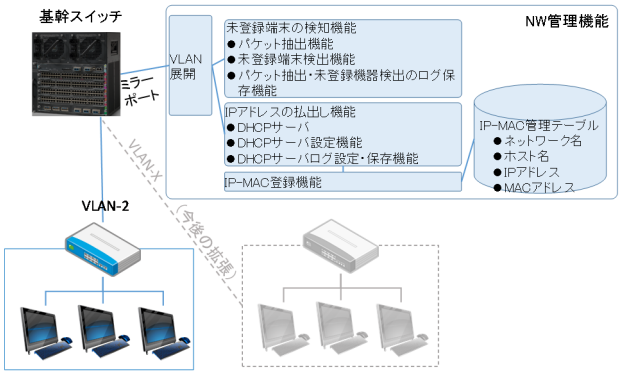

図 6　端末のネットワーク接続時の動き

５．新システムの運用評価

本学品川キャンパスで改修工事のため一時ネットワーク停止していた建屋（2 号館）を対象に，2014 年 3 月から試行的に MAC-IP 監視管理システムを導入した．2 号館には 13 研究室あり，2014 年 7 月時点で 252 件の MAC アドレスが登録されている．導入当初に 2 号館教職員全員に一斉メールで新システム移行を通知し，機器管理責任者向けの操作マニュアルと利用者向けの詳細な設定マニュアルを添付するとともに，学内 Web サイトで公開した．当初，MAC アドレスの調査ミス・入力ミスなどにより機器管理責任者から問い合わせが数件あったが，現在，問い合わせはほとんどなく順調に稼働している．MAC-IP 監視管理システムの運用および端末のネットワーク接続方法は 3 か月で概ね浸透したと考えられる．MAC アドレス認証未登録端末（未許可 PC・プリンタ）および規定外接続端末（固定 IP アドレス設定）の接続件数は，当初は 1 日あたり 20 件程度検出される日もあったが，システムの利用方法の周知により平日でも 10 件未満に減少してきた（図 7）．すなわち，2013 年 11 月の調査では未登録・不一致端末件数が 72%あったのに対し（図 2），システム導入後の未登録端末は登録件数の 4%未満に抑制できたことから，セキュリティレベルは格段に向上したと考えられる．

利用者にとっては，これまで 2-3 日要していた申請から IP アドレス発行の期間が，本システムに機器情報を登録すれば，即時にネットワーク接続ができるようになった．また，DHCP 機能を使うことにより，個々の利用者の端末に IP アドレス等の設定をする手間が削減され，利用者の利便性向上につながったと言える．端末に IP アドレス等の設定が不要になったことにより，これまで設定ミスにより，一か月に 1 度程度発生していた IP アドレスの競合件数が，本システムを導入してから約 5 か月の間 0 件である．

本システムの問題点としては，MAC アドレスが登録されている端末に，IP アドレスを設定した場合，その IP アドレスが，異なっていた場合でも，ネットワークに接続することができる．そのため，IP アドレスの競合が発生する可能性もある．現時点では，端末に IP アドレスを登録しないよう運用でカバーしているため，IP アドレスの競合は発生していない．発生した場合でも，これまでに比べると正しい MAC アドレス情報が管理されているため，該当端末の調査の時間が大幅に削減されることが期待される．

MAC アドレスは登録しているが，MAC-IP テーブルとは異なる端末が接続された場合に，その端末の場所を特定し，同室を管理する機器管理者に通知する機能を開発中である．

また，実装したシステムは，耐障害性を考慮していない構成のため，全学展開に向けて，コールドスタンバイなど，二重化の検討が必要であると考えている．

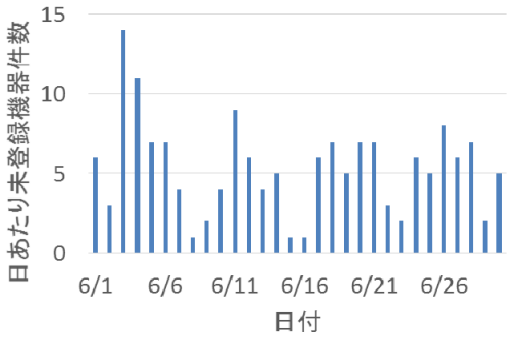

図 7 未登録機器検出のログ集計結果（2013 年 6 月）

６．まとめ

本研究では，学内ネットワークの運用に関する問題点を整理し，ネットワークシステム管理者と機器管理者双方の利便性とセキュリティレベル向上を実現するため，グループ管理を新たに取り入れたMAC-IP監視管理システムを設計し，１建屋に試行的に導入した．解決すべき点はいくつか残されているが，開始後3か月の運用状況からスムーズに移行されたと考えられる．

今後の予定は，2014 年 9 月より品川キャンパス全ての建屋に MAC-IP 監視管理システムを導入する予定である．また，現在開発中である未登録端末の検知と接続場所の特定を行う機能の開発を進め，不正利用の防止につとめ，情報セキュリティ向上を目指す．

謝辞

本稿で提案するシステムの設計および実装においてご協力頂いたコネクトドット社の星野氏, 中野氏, 京都大学学術情報メディアセンターの岡部寿男教授, 奈良先端科学技術大学院大学の大平健司助教に謹んで感謝の意を表する．

参考文献

[1] 大平健司，山口由紀子，八槇博史，高倉弘喜，星野寛，中野博樹：インシデント対応を考慮した IPv6 ノード情報収集システムの設計と試作，電子情報通信学会論文誌 D，J96-D(6)，1483-1492，2013

[2] 田島 浩一，近藤 徹，岸場 清悟，大東 俊博，岩田 則和，西村 浩二，相原 玲二：大規模キャンパスネットワークにおける MAC アドレス認証の管理手法，情報処理学会研究報告，2009

[3] 田島 浩一，近藤 徹，岸場 清悟，大東 俊博，岩田 則和，西村 浩二，相原 玲二：大規模キャンパスネットワークにおける MAC アドレス認証端末の移動管理，学術情報処理研究 No.15，2011

[4] 岡山 聖彦，山井 成良，大隅 淑弘，河野 圭太，藤原 崇起，稗田 隆：岡山大学における認証・ロケーションネットワークの構築，学術情報処理研究 No.15，2011

[5] 久長 穣，杉井 学，為末 隆弘，金山 知余，小河原 加久治：山口大学におけるネットワーク運用支援システム，学術情報処理研究 No.15，2011

[6] 板倉 紀子，島岡 章，小谷 明義，吉田 和幸：ユーザ機器とオンライン申請，登録，認証システムの開発とその運用について--センター管理業務の削減の観点から--，学術情報処理研究 No.16，2012

[7] 大谷 誠，江藤 博文，渡辺 健次，只木 進一，渡辺 義明:キャンパスで運用可能な MAC アドレス認証システム OpengateM，情報処理学会研究報告，2012

[8] 清水さや子，戸田勝善，岡部寿男：任意のグループと統合 ID を使ったメンバの管理を行うグループ管理システムの実装，情報処理学会インターネットと運用技術シンポジウム 2013,情報処理学会 p65-72，2013