Vol.2016-CSEC-73 No.2
Vol.2016-IOT-33 No.2
2016/5/26

# ネットワークアクセス認証連動型IP管理データベースの運用と機能拡張について

宮北 和之[1,a)]　山本 一幸[1]　青山 茂義[1]　三河 賢治[1]

**概要**：新潟大学では，平成 21 年 3 月より，MAC アドレスによるネットワークアクセス認証を全学に対して導入している．また，部局管理者の負担軽減および情報セキュリティ対策強化（セキュリティインシデント機器の管理者の即時検索）のため，各グローバル IP アドレスに対して，利用者情報，設置情報，MAC アドレス等を登録・管理する IP 管理データベース（IPDB）も独自開発した．IPDB の大きな特徴の一つは，ネットワークの MAC アドレス認証システムと連動しており，IPDB 上に登録・削除した MAC アドレスを用いて，アクセスリストがスイッチ上に自動生成され，MAC アドレス認証が実現されていることである．平成 22 年 5 月開催の本学会 IOT 研究会において，IPDB の基本的な設計やその運用について報告を行ったが，その後の運用結果や機能拡張について研究報告を行う．特に，管理性向上（IP アドレス利用状況の可視化）に関する機能追加の提案と試験結果についての考察・報告を行う．

# Operation and Extension of IP Address Management Database with Network Access Authentication

Kazuyuki Miyakita[1,a)]　Kazuyuki Yamamoto[1]　Shigeyoshi Aoyama[1]　Kenji Mikawa[1]

## 1. はじめに

新潟大学は，9 学部，7 研究科，附属病院，附置研究所等からなる総合大学であり，学生及び教職員およそ 20,000 人が教育，研究に取り組んでいる．筆者らの所属する情報基盤センターは，本学の教育，研究用情報システムの構築やネットワーク環境の整備等，主に全学向けの企画，運営を行っている．本学では，組織毎に利用可能なサブネットを決定し，組織の代表者（以下，部局管理者）の責任においてグローバル IP アドレスを払い出し，固定グローバル IP アドレスを基本とした運用を行っている．

平成 20 年度末に，ネットワークの不正利用対策の一環として，キャンパスネットワーク更新に合わせて全学規模のネットワークアクセス認証システムを導入した [1]．認証方式は，利用者の利便性の観点から，MAC アドレスによる認証を基本とし，ユーザ ID とパスワードによる認証を併用する運用とした．この方式により，利用者は，機器の MAC アドレスさえ部局管理者に申請していれば，認証を意識することなくネットワークを利用可能となった．

また，平成 21 年 9 月には，部局管理者の負担軽減および情報セキュリティ対策強化（セキュリティインシデント機器の管理者の即時検索）のため，各グローバル IP アドレスに対して，利用者情報，設置情報，MAC アドレス等を登録・管理する IP 管理データベース（IPDB）も独自開発した [2]．IPDB の大きな特徴の一つは，ネットワークの MAC アドレス認証システムと連動しており，IPDB 上に登録・削除した MAC アドレスを用いて，アクセスリストがスイッチ上に自動生成され，MAC アドレス認証が実現されていることである．

平成 22 年 5 月開催の本学会 IOT 研究会において，IPDB の基本的な設計やその運用について報告を行ったが [2]，本報告では，まず，その後の IPDB の運用結果について報告を行う．また，この運用結果を踏まえて，現状の IP アドレス管理の問題点を指摘し，この問題点を解決するための

[1] 新潟大学 学術情報基盤機構 情報基盤センター
Center for Academic Information Service, Niigata University
[a)] miyakita@cais.niigata-u.ac.jp

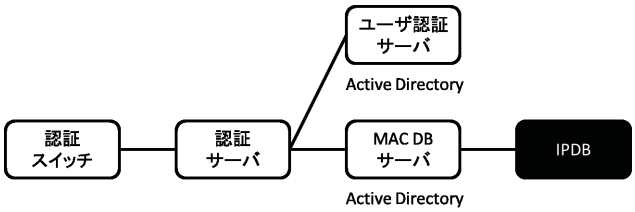


**図 1** ネットワーク認証関連のサーバ [1]
**Fig. 1** Servers for the network access authentication [1].

IPDB の機能拡張の提案を行う．特に，管理性向上（IP アドレス利用状況の可視化）に関する機能追加の提案と試験結果についての考察・報告を行う．

## 2. ネットワークアクセス認証連動型 IP 管理データベース（IPDB）

本節では，平成 20 年度末に導入したネットワークアクセス認証システム [1]，及び，平成 21 年 9 月に独自開発したネットワークアクセス認証連動型 IP 管理データベース（IPDB）[2] の概略を紹介する．

### 2.1 ネットワークアクセス認証システム [1]

新潟大学でのネットワークアクセス認証は L2 スイッチのネットワーク認証機能を用いて行っている．認証は，MAC アドレス認証とユーザ認証を併用しており，ユーザはどちらかの方式で認証を行えばネットワークが利用できる．機器の MAC アドレスが予め登録されていれば MAC アドレス認証により通信が許可され，登録されていなければユーザ認証ページが表示される．常時利用する機器については，MAC アドレス認証を行うことを推奨している．認証の許可／拒否を決めるために，L2 スイッチは認証サーバに問い合わせを行い，認証が許可された場合のみ L2 スイッチにアクセスリストが自動生成され，利用者は L2 スイッチを通して通信を行うことができる．

**図 1** に外部サーバを含む認証サーバの概要を示す．認証サーバは，MAC アドレス，ユーザアカウント情報（ユーザ ID，パスワード）などの認証情報は持っておらず，外部サーバ（MAC DB サーバ及びユーザ認証サーバ）に問い合わせて認証情報を得る．MAC アドレス認証を行うための MAC アドレス情報は MAC DB サーバ，ユーザ認証を行うためのユーザアカウント情報はユーザ認証サーバにそれぞれ登録されている．

### 2.2 ネットワークアクセス認証連動型 IP 管理データベース（IPDB）[2]

本学では，クラス B のネットワークを 24 ビットマスクのサブネットに分割して，情報基盤センターで部局に割り当てたサブネットを部局管理者が管理している．IPDB では，ユニークなログイン ID を部局管理者に発行し，部局管理者が所属する部局をグループとして，グループ毎に割り当てられたサブネットを管理する．部局管理者は，利用者の申請に基づき IP アドレスを払い出し，IPDB に登録している．情報基盤センターでは，IPDB の情報から全学の IP アドレスの払い出しや機器の状況を部局管理者と共有している．なお，ネットワーク管理に関わる部局数は約 30 部局あり，関係する部局管理者は約 60 人である．

**表 1** IPDB の管理情報
**Table 1** Information registered on IPDB.

| 属性 | 必須項目 | 自動入力 |
|---|---|---|
| IP アドレス | ○（キー） | |
| MAC アドレス | ○（キー） | |
| MAC 登録の有無 | ○ | |
| ホスト名 | | |
| ドメイン名 | | |
| 学外公開の有無 | ○ | |
| DNS 登録（学内）の有無 | ○ | |
| DNS 登録（学外）の有無 | ○ | |
| 管理者名 | ○ | |
| 部局 | ○ | |
| 学科 | | |
| 設置場所 | ○ | |
| 機種 | ○ | |
| 備考 | | |
| 更新日時 | ○ | ○ |
| 更新者 | ○ | ○ |

このように，本学では，複数の部局管理者による分散管理を行っているので，クライアントの環境に依存しないユーザインタフェースを提供することが必須である．このため，ユーザインタフェースとしてウェブブラウザを利用しており，IPDB は，PHP を介して，ウェブアプリケーションと親和性が高い PostgreSQL を採用している．

IPDB の属性を**表 1** に示す．IP アドレスと MAC アドレスは複合キーとして定義している．なお，表 1 に示した属性のうち，「学外公開の有無」は，IPDB 構築当初 [2] には存在しなかったが，部局管理者からの要望により，平成 26 年 8 月に追加した．

IPDB が搭載している代表的な機能を以下に示す．

- 部局管理者が，担当する部局に割り当てられたサブネットについてのみ，データを閲覧，登録，変更，削除することができる機能．
- 検索機能．
- CSV ファイルによる入出力機能（一括登録，同期，全管理データの出力，検索結果の出力）．
- 部局管理者パスワード変更機能．

2.1 節で述べたとおり，本学のネットワークアクセス認証の構成では，IPDB に登録された MAC アドレスは，MAC DB サーバに登録されて初めて，ネットワークアクセス認証に利用できるようになる．このため，IPDB 上の MAC ア

ドレスと MAC DB サーバ上の MAC アドレスの連携を確実に行うことが重要である．特に，IPDB では PostgreSQL が稼動しているが，MAC DB サーバでは Active Directory が稼動している．異なる DBMS 間で確実に MAC アドレスを連携するため，以下の手順により定期的に同期を行っている．

- IPDB は定期的に，MAC DB サーバに登録されているレコードの一覧を MAC DB サーバから取得する．
- IPDB において，IPDB の登録レコードと MAC DB サーバの登録レコードの差分を計算し，追加（add）と削除（del）に分類した上で，MAC DB サーバに返送する．
- MAC DB サーバにおいて，返送された差分データを反映することによって，IPDB の登録レコードと完全に同じになるように，レコードの追加・削除を行う．

## 3. IPDB の運用結果と問題点

[2] において，IPDB の運用開始（平成 21 年 9 月）から約 6 ヶ月間の運用状況について報告されているが，本節では，まず，その後の長期的な（約 6 年半）IPDB の運用結果について報告する．**図 2** に，平成 21 年 9 月から平成 28 年 2 月までの IPDB への登録数の推移を示す．どの月も 100 程度以上の登録があるが，年度切り替わり前後の 3 月，4 月に特に多くの登録があり，多い月には 500 を超えていることが分かる．これは，年度の切り替わりに伴い，新たに赴任してきたり，他部局から異動してくる教職員が管理する機器をまとめて登録しているためであると考えられる．**図 3** に，平成 21 年 9 月から平成 28 年 2 月までの IPDB からの削除数の推移を示す．基本的には登録数と似たような推移の傾向を示しているが，削除数の方が登録数に比べてばらつきが大きいことが分かる．具体的には，少ない月には削除数は 30 程度であり，多い月には削除数は 1,000 を超えている．これは，部局管理者の登録作業は利用者からの申請に応じてある程度コンスタントに行っているのに対し，削除作業は年度末等にある程度まとめて行っているためであると考えられる．

また，全体的に，削除数よりも登録数の方が多い傾向がある．実際に，図 2 と図 3 に示している約 6 年半の間で，登録数の方が削除数よりも 1,000 程度多くなっている．これは，教職員の退職等で使わなくなった IP アドレスを部局管理者が把握しきれていない，もしくは，消し忘れていることが主な要因であると考えられる．

確認のために，IPDB に登録されている IP アドレスのうち，実際に使用された IP アドレスの割合を，**図 4** に示す．平成 28 年 4 月 9 日を基準日として，基準日において IPDB に登録されている IP アドレスすべての集合（ただし，基幹ネットワーク用スイッチなどの認証対象外機器は除く）を $S_{\mathrm{regist}}$，$S_{\mathrm{regist}}$ の中で基準日から遡って $d$ 日間の間に実際

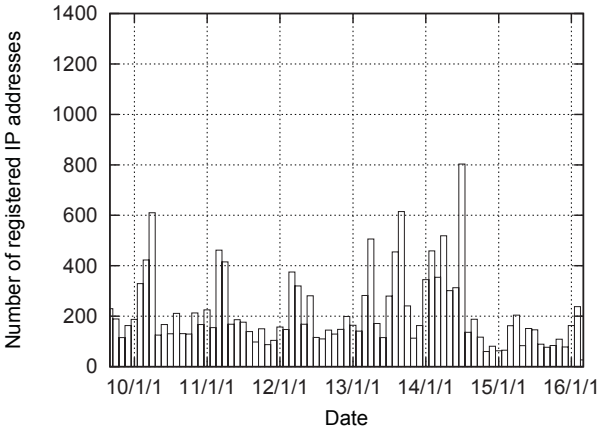


**図 2** IPDB への登録数
**Fig. 2** Number of registered IP addresses.

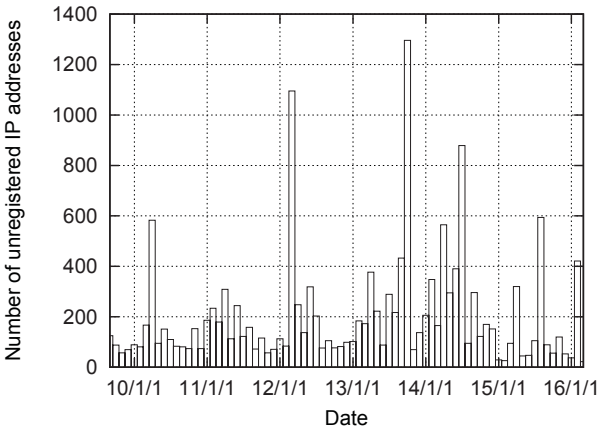


**図 3** IPDB からの削除数
**Fig. 3** Number of unregistered IP addresses.

に使用された IP アドレスすべての集合を $S_{\mathrm{used}}(d)$ とおく．図 4 は，横軸を $d$，縦軸を $\frac{|S_{\mathrm{used}}(d)|}{|S_{\mathrm{regist}}|}$ として表している．ただし，$|\cdot|$ は，$\cdot$ の要素数である．ここで，実際に使用された IP アドレスは，ネットワークアクセス認証システムの認証ログから，認証に成功した IP アドレスの数として取得している．

図 4 を見ると，まず，基準日の 1 日間だけで実際に使用されている IP アドレス数は登録数の 36%程度であることが分かる．観測する日数が長くなるほど実際に使用されている IP アドレスの割合は大きくなっていくが，観測日数 80 日を超えたあたりから実際に使用されている IP アドレスの割合は伸びなくなっており，43%程度で飽和していることが分かる．この傾向から，次の 2 点のことが読み取れる．

- IPDB に登録されている IP アドレスのうち，3 ヶ月間実際に使用されていない IP アドレスは，実質的には既に使われておらず，その後使われることはほとんどない．
- IPDB に登録されている IP アドレスのうち，約 57%は実質的には使われていない．

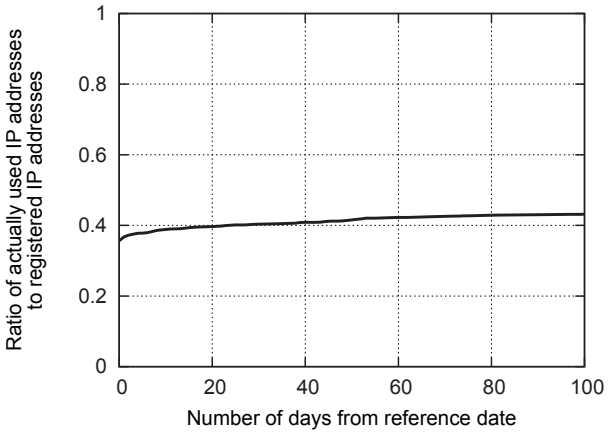


**図 4** IPDB に登録されている IP アドレスの使用率
**Fig. 4** Ratio of actually used IP addresses to registered IP addresses in IPDB.

上記のように，使われなくなった IP アドレスに対して，削除処理が適切に行われていないという問題点がある．このような問題が起こる原因として，使われなくなった IP アドレスを部局管理者が把握しきれないということが考えられる．実際に，部局管理者から情報基盤センターに対して，使われなくなった IP アドレスを把握するために，長期間実際には使われていない IP アドレスを教えて欲しいとの要望が出たこともある．

## 4. IPDB の機能拡張

前節で述べた問題点を解決するために，IPDB に対して下記の機能拡張を行った．まず，部局管理者が IPDB の管理データを閲覧するホーム画面において，どの IP アドレスが実質的に使われていないかを容易に把握できるように，長期間使われていない IP アドレスを赤字で表示するようにした．ここで，前節の調査結果を踏まえて，具体的には，3 ヶ月間使われていない IP アドレスを赤字で表示するようにした．

具体的な，機能拡張部分の構成と動作を以下に示す．

- 毎日早朝の決められた時刻に，ネットワークアクセス認証システムの認証ログサーバにおいて，その前日に認証が成功した IP アドレスの一覧を IPDB サーバに転送する．この操作は，認証ログサーバ上に置いたスクリプトファイルを毎朝自動的に実行することにより，実現する．
- IPDB サーバ側では，受け取った IP アドレスの一覧を加工して，「各 IP アドレスについて最後に認証が成功した日時」のテーブル（テーブル名：access_date）を PostgreSQL のデータベース上に作成する．具体的には，受け取った IP アドレスの一覧を順に参照していき，
  - access_date の中にその IP アドレスを含むレコードがあれば，そのレコードの日付の値を，前日の日付に書き換える，
  - access_date の中にその IP アドレスを含むレコードが無ければ，その IP アドレスと前日の日付の組を新規レコードとして access_date に追加する．

  この操作は，IPDB サーバ上に置いたスクリプトファイルを毎朝自動的に実行することにより，実現する．
- IPDB における，部局管理者管理データの一覧を表示させる PHP ファイルの中で，各レコードを表示させる際に，テーブル access_date にアクセスして照合を行う．該当のレコードに対応する IP アドレスが access_date 内に存在しており，かつ，その IP アドレスが最後に認証に成功した日時が現在の日時の 3 ヶ月前以降であったら黒字で表示し，さもなくば赤字で表示する．

**図 5** に，機能拡張後のホーム画面を示す．この図は，部局管理者のアカウントでログインしており，この部局管理者の管理サブネットは 172.35.1.0/24〜172.35.30.0/24 であるような場合を想定している．なお，具体的な IP アドレス帯や図 5 における具体的な登録データは，現在実際に運用しているものとは異なる，架空のものであるので，注意されたい．図 5 は，画面上部の管理サブネット一覧において「16」をクリックし，サブネット 172.35.16.0/24 を表示させた状態を示している．このように色で区別して表示させることにより，長期間使用されていない IP アドレスが一目で確認できる．この画面を部局管理者が確認することにより，赤字で表示されている IP アドレスの使用者に連絡を取り，本当に使用されていなければ（使用者が既に退職・異動している，該当機器が既に無くなっている，等）IPDB から削除する，というような運用方法を想定している．

また，付随する機能として，赤字で表示されている（3 ヶ月の間実際には使用されていない）IP アドレスだけを表示する機能も搭載した．**図 6** に，この機能を実行した際の画面を示す．図 5 のホーム画面において「赤字だけ表示」と書かれたボタンを押すことにより，この機能が動作する．この機能により，登録 IP アドレス数が多いようなサブネットにおいても，長期間使用されていない IP アドレスがどの程度あるのかを容易に確認できる．

また，特定のサブネットの IP アドレスの使用状況をグラフ化して表示する機能も搭載した．図 5 のホーム画面において「集計グラフの表示」と書かれたボタンを押すことにより，この機能が動作し，ウェブブラウザの新規ウインドウで PHP ページを開き，その PHP ページ内でグラフの自動作成および表示を行う．表示されるグラフの例を**図 7** に示す．横軸は該当サブネットにおける第 4 オクテットの値であり，縦軸は「現在（閲覧を行っている日時）を基準日として，該当 IP アドレスが最後に使われた日までの日数」を表している．例えば，図 7 において横軸の値が 57 のときに縦軸の値は 15 となっているが，これは，172.35.16.57 の IP アドレスが現在から 15 日前に最後に使われたという


| NW情報 | | | | | | DNS申請 | | 管理者情報 | | | 機器情報 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IP | MAC | MAC登録 | ホスト名 | ドメイン名 | 学外公開 | 学内 | 学外 | 管理者名 | 部局 | 学科 | 設置場所 | 機種 | 備考 | 更新日 |
| 172.35.16.8 | 00:00:00:00:00:06 | 済 | host06 | | 不要 | 不要 | 不要 | 新潟 太郎 | 情報基盤センター | | AAA研究室 | | | 2016-04-15 |
| 172.35.16.10 | 00:00:00:00:00:07 | 不要 | host07 | | 不要 | 不要 | 不要 | 新潟 太郎 | 情報基盤センター | | AAA研究室 | | | 2016-04-15 |
| 172.35.16.20 | 00:00:00:00:00:08 | 不要 | host08 | cais | 済 | 済 | 済 | 新潟 太郎 | 情報基盤センター | | AAA研究室 | | | 2016-04-15 |
| 172.35.16.21 | 00:00:00:00:00:09 | 済 | host09 | | 不要 | 不要 | 不要 | 五十嵐 花子 | 情報基盤センター | | BBB研究室 | | | 2016-04-15 |
| 172.35.16.24 | 00:00:00:00:00:10 | 不要 | host10 | | 不要 | 不要 | 不要 | 五十嵐 花子 | 情報基盤センター | | BBB研究室 | | | 2016-04-15 |
| 172.35.16.25 | 00:00:00:00:00:11 | 済 | host11 | | 不要 | 不要 | 不要 | 五十嵐 花子 | 情報基盤センター | | BBB研究室 | | | 2016-04-15 |
| 172.35.16.26 | 00:00:00:00:00:12 | 済 | host12 | | 不要 | 不要 | 不要 | 旭 次郎 | 情報基盤センター | | CCC研究室 | | | 2016-04-15 |
| 172.35.16.27 | 00:00:00:00:00:13 | 済 | host13 | | 不要 | 不要 | 不要 | 旭 次郎 | 情報基盤センター | | CCC研究室 | | | 2016-04-15 |
| 172.35.16.28 | 00:00:00:00:00:14 | 要 | host14 | | 不要 | 不要 | 不要 | 旭 次郎 | 情報基盤センター | | CCC研究室 | | | 2016-04-15 |
| 172.35.16.29 | 00:00:00:00:00:15 | 済 | host15 | | 不要 | 不要 | 不要 | 村松 三郎 | 情報基盤センター | | DDD研究室 | | | 2016-04-15 |
| 172.35.16.30 | 00:00:00:00:00:18 | 済 | host18 | | 不要 | 不要 | 不要 | 村松 三郎 | 情報基盤センター | | DDD研究室 | | | 2016-04-15 |

**図 5** 通常画面（特定サブネット表示）
**Fig. 5** Main screen of extended IPDB.


| NW情報 | | | | | | DNS申請 | | 管理者情報 | | | 機器情報 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IP | MAC | MAC登録 | ホスト名 | ドメイン名 | 学外公開 | 学内 | 学外 | 管理者名 | 部局 | 学科 | 設置場所 | 機種 | 備考 | 更新日 |
| 172.35.16.10 | 00:00:00:00:00:07 | 不要 | host07 | | 不要 | 不要 | 不要 | 新潟 太郎 | 情報基盤センター | | AAA研究室 | | | 2016-04-15 |
| 172.35.16.20 | 00:00:00:00:00:08 | 不要 | host08 | cais | 済 | 済 | 済 | 新潟 太郎 | 情報基盤センター | | AAA研究室 | | | 2016-04-15 |
| 172.35.16.24 | 00:00:00:00:00:10 | 不要 | host10 | | 不要 | 不要 | 不要 | 五十嵐 花子 | 情報基盤センター | | BBB研究室 | | | 2016-04-15 |
| 172.35.16.31 | 00:00:00:00:00:19 | 済 | host19 | | 不要 | 不要 | 不要 | 村松 三郎 | 情報基盤センター | | DDD研究室 | | | 2016-04-15 |
| 172.35.16.33 | 00:00:00:00:00:21 | 済 | host21 | | 不要 | 不要 | 不要 | 新潟 太郎 | 情報基盤センター | | AAA研究室 | | | 2016-04-15 |
| 172.35.16.34 | 00:00:00:00:00:22 | 済 | host22 | | 不要 | 不要 | 不要 | 新潟 太郎 | 情報基盤センター | | AAA研究室 | | | 2016-04-15 |
| 172.35.16.35 | 00:00:00:00:00:23 | 済 | host23 | cais | 不要 | 済 | 不要 | 五十嵐 花子 | 情報基盤センター | | BBB研究室 | | | 2016-04-15 |
| 172.35.16.38 | 00:00:00:00:00:31 | 済 | host31 | | 不要 | 不要 | 不要 | 五十嵐 花子 | 情報基盤センター | | BBB研究室 | | | 2016-04-15 |
| 172.35.16.39 | 00:00:00:00:00:33 | 済 | host33 | | 不要 | 不要 | 不要 | 旭 次郎 | 情報基盤センター | | CCC研究室 | | | 2016-04-15 |
| 172.35.16.41 | 00:00:00:00:00:37 | 済 | host37 | | 不要 | 不要 | 不要 | 旭 次郎 | 情報基盤センター | | CCC研究室 | | | 2016-04-15 |
| 172.35.16.43 | 00:00:00:00:00:39 | 済 | host39 | | 不要 | 不要 | 不要 | 村松 三郎 | 情報基盤センター | | DDD研究室 | | | 2016-04-15 |

**図 6** 赤字（3 ヶ月以上使用されていない IP アドレス）だけ表示
**Fig. 6** Display of only IP addresses that have not been used for three months.

ことを意味している．グラフ上に表示されていない IP アドレスについては，最後に使われたのが 90 日以上前であるか，これまで一度も使われていないということを意味している．このグラフは，より最近に使われているほど棒が長く表示されるので，グラフを一目見るだけで，サブネット全体としてどの程度活発に使われているかということや，サブネットの中のどのあたりの IP アドレス帯が全く使用されていないかということを把握することが容易になると

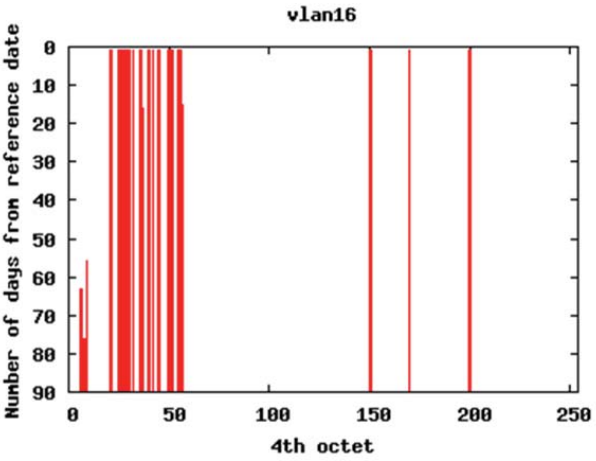


**図 7** 特定サブネットの IP アドレス使用状況のグラフ

**Fig. 7** Graph that shows usage status of IP addresses in a specific subnet.

考えられる．

## 5. おわりに

本報告では，平成 21 年 9 月に独自開発した，ネットワークアクセス認証連動型 IP 管理データベース（IPDB）の長期的な運用結果について報告した．ネットワークの MAC アドレス認証システムとの連動部分も含めて，導入開始時から現在に至るまで大きな問題が起こることなく運用できているが，部局管理者の不要データの削除し忘れ等の原因により，登録されている IP アドレスのうち約 57%は実際には使用されていないという問題点を明らかにした．この問題点を解消するため，過去 3 ヶ月間の間に実際に使われていない項目を赤字で表示させる，特定のサブネットの IP アドレスの使用状況をグラフ化して表示するという機能拡張を行った．これらの機能拡張により，部局管理者が既に使われていない IP アドレスを把握する手助けになることが期待される．

今後の課題としては，より長期間（例えば 1 年間）使用されていない IP アドレスを IPDB から自動削除する機能の追加等が挙げられる．

### 参考文献

[1] 浜元信州，青山茂義，三河賢治：全学ネットワークアクセス認証システムの導入，インターネットと運用技術シンポジウム 2009，IPSJ Symposium Series Vol. 2009, No. 15, pp. 1–8 (2009).
[2] 浜元信州, 五十嵐瑛介, 青山茂義, 三河賢治：ホスト登録システムを利用したネットワークアクセス認証システムの運用，情報処理学会研究報告，Vol. 2010-IOT-9, No. 4, pp. 1–6 (2010).