Vol.2010-IOT-9 No.4
2010/5/13

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

浜元信州[†1]　五十嵐瑛介[†2]
青山茂義[†1]　三河賢治[†1]

新潟大学では，全学規模で導入したネットワークアクセス認証システムを導入した．これにより，MAC アドレスなどのネットワーク情報の管理が必要となったが，ホスト登録用の「ネットワーク管理用データベース」を新たに開発することと，このデータベースと認証サーバの自動連携を行うことで管理負担を大きく軽減できた．本稿では，新たに開発したネットワーク管理用データベース，及び，認証サーバの連携，現在の運用状況について述べる．

Operation of Network Access Authentication System Using Host Registration System

Nobukuni Hamamoto ,[†1] Eisuke Ikarashi ,[†2]
Shigeyoshi Aoyama [†1] and Kenji Mikawa[†1]

To manage network information used for the network access authentication, such as MAC addresses, we develped network management database for Niigata university. Operations of the database are based on host registration by the administrators of the departments.

In this report, we describe details and operations of the network management database. The method to syncronize the database and the authentication server is also discussed.

†1 新潟大学 情報基盤センター
Center for Academic Information Service, Niigata University
†2 新潟大学 工学部 情報工学科
Department of Information Engineering, Faculty of Engineering, Niigata University

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，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．著者らの所属する情報基盤センターは，本学の教育，研究用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に決定し，組織の代表者（以下，部局管理者）の責任において IP アドレスを払い出し，固定 IP アドレスを基本とした運用を行っている．部局管理者は，IP アドレスや機器の情報をネットワーク管理用データベースサーバ（以下，管理用 DB サーバ）に登録し，情報基盤センターでは，このサーバの情報から全学の IP アドレスの払い出しや機器の状況を把握している．

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．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．一方で，MAC アドレスを認証サーバに登録する作業は迅速かつ正確な作業が要求されるが，従来の管理用 DB サーバを用いた情報共有や認証サーバへの登録は手作業によるため，部局管理者と情報基盤センター職員の負担が著しく増大してしまった．

著者らは，管理用 DB サーバを新たに構築し，認証システム導入に伴う負担を軽減することに成功した．本稿では，本システムの構築過程及び運用状況について報告する．横浜国立大学[2),3)]，広島大学[1)] の事例報告は，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先例として，本システムの開発を検討する上で非常に参考になった．

2. 新潟大学ネットワークアクセス認証システム

新潟大学では，2009 年度より，ネットワークアクセス認証システムを導入し，ネットワークセキュリティが大きく向上した．このシステムについての詳細は，筆者らの報告[4)] に譲り，概略のみを下記に述べる．

新潟大学でのネットワークアクセス認証は L2 スイッチ（catalyst2960）のネットワーク認証機能を用いて行っている．認証は，ユーザ認証と，MAC アドレス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．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

表 1 各認証サーバの構成
Table 1 Configuration of the authentification servers.

	認証サーバ	MAC DB サーバ	ユーザ認証サーバ	管理用 DB サーバ
機器名	NEC Express5800/110Ri-1	NEC Express5800/110Ri-1	Dell PowerEdge 2850	NEC Express5800 110GR-1c
CPU	Intel Xeon X3350 2.66GHz	Intel Xeon X3350 2.66GHz	Intel Xeon 3.2GHz	Intel Pentium4 3.2GHz
メモリ	2GB	2GB	3GB	2GB
HDD	73.2GB×2 (RAID1)	73.2GB×2 (RAID1)	73.2GB×3 (RAID5)	80.0GB×2 (RAID1)
OS	Win2003 Server Standard R2 SP2	Win2003 Server Standard R2 SP2	Win2003 Server Standard R2 SP2	CentOS 5.4
主なソフトウエア	Cisco Secure ACS	Active Directory	Active Directory	Apache 2.2, PHP 5.1, PostgreSQL 8.1

に，L2 スイッチは，認証サーバに問い合わせを行う．**図 1** に外部サーバを含む認証サーバの概要を示す．認証サーバには，MAC アドレス，ユーザアカウント情報（ユーザ ID，パスワード）などの認証情報はなく，外部サーバに問い合わせて認証情報を得る．MAC アドレスは，MACDB サーバ，ユーザアカウントはユーザ認証サーバにそれぞれ登録されている．

認証サーバの OS，ハードウエア情報の機器構成を**表 1** に示す．管理用 GUI が標準搭載されているため，ユーザ認証サーバ，MACDB サーバともに Win2003 Server 上で Active Directory を用いた管理を行っている．Active Directory は，元々MAC アドレスを管理するために作られているわけではないため，MACDB サーバでは，**表 2** に示したように属性を読み替えて利用している．また，OU は分割せず，全学の MAC アドレスを一つの OU として管理している．表中にある sAMAccountName と name は両方共 MAC アドレスと読み替えたが，両者が必須項目となっているため，やむを得ず同じ意味で読み替えた．新潟大学では，MAC アドレス一つにつき，基本的に IP アドレス 1 つを与えている．しかし，複数の場所で同一の PC を利用したい場合などには，MAC アドレスは 1 つだが IP アドレスを複数登録したいという要望がある．このため，displayname, description ともに IP アドレスであるが，主に使う IP を displayname に，その他の IP アドレスは description に記

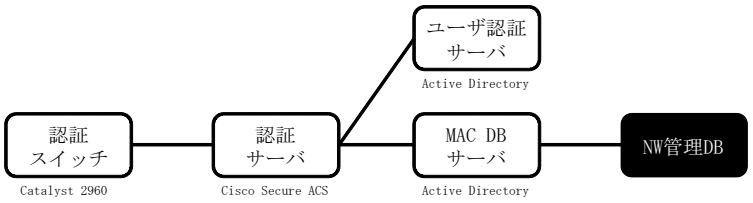

図 1 ネットワークアクセス認証関連のサーバ
Fig. 1 Servers for the network access authentication.

表 2 MACDB サーバ上の AD の属性値の意味
Table 2 Meanings of the attributes of the Active Directory on the MACDB server.

属性	意味
sAMAccountName	MAC アドレス
name	MAC アドレス
displayname	IP アドレス
description	2 つめ以降の IP アドレス
mail	登録作業者メールアドレス

述している．

3. 運用上の問題点

本学では，部局管理者が利用者の申請に基づき IP アドレスを払い出し，管理用 DB サーバに登録している．情報基盤センターでは，このデータベースの情報から全学の 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．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．情報基盤センターでは，ネットワークアクセス認証の導入以前に，次のように DNS の一元管理を行っていた．IP アドレスの払い出しと同様に，部局管理者が利用者の申請に基づき，DNS 情報を管理用 DB サーバに登録し，同時に情報基盤センターに申請を行う．情報基盤センターは，申請内容とデータベースの情報に間違いがないことを確認の上，DNS サーバに申請内容を反映する．

ネットワークアクセス認証の導入にあたり，MAC アドレスをどのように管理するかが問題となったが，導入当初は，管理用 DB サーバに “MAC アドレス” の属性を追加した．MAC アドレスの登録の流れは，DNS 登録と同様に，部局管理者が利用者の申請に基づき，MAC アドレスを管理用 DB サーバに登録し，同時に情報基盤センターに申請を行う．情報基盤センターは，申請内容とデータベースの情報に間違いがないことを確認の上，MAC

DB サーバに申請内容を反映する．しかしながら，次のような問題が発生したため，新たにデータベースアプリケーションの構築が必要となった．

問 題 点 1

本学の場合，ネットワークアクセス認証の方式として MAC アドレスによる認証を基本としたため，第一の問題は，利用者からの MAC アドレス申請が DNS 申請と比較して格段に多いことに起因する．MAC アドレスを認証サーバに登録する作業は，職員の手作業で行っているため，登録の遅延を引き起こす一因となった．MAC アドレスの登録を完了するまでの代替手段としてユーザ認証を行っているため，利用者からのクレームをある程度，回避できていると考えているが，ネットワークプリンタやブロードバンドルータのようにユーザ認証できない機器に関する要望が多い．

問 題 点 2

第二の問題は，管理用 DB サーバで使用していたソフトウェアの仕様に起因する．データベースの属性型として，数値型，文字型等を選択することができるが，管理用 DB サーバで使用したソフトウェアでは，MAC アドレスに特化した型が存在せず，また適切な入力制約をかけることができなかった．このため，様々な表現形式で申請された MAC アドレスの登録時に多くの誤入力が発生し，登録の遅延を引き起こす一因となった．

問 題 点 3

第三の問題は，一つの IP アドレス（MAC アドレス）に複数の MAC アドレス（IP アドレス）の登録を許可したことに起因する．MAC DB サーバは，MAC アドレスをキーとして管理を行っているが，管理用 DB サーバは，IP アドレスをキーとして管理を行っていた．管理用 DB サーバでは，部局を横断しての検索が難しく，部局管理者が，ネットワーク管理データベース上で，MAC アドレスに対応する IP アドレスを検索することが難しくなってしまった．このため，部局管理者自身が MAC アドレスの新規登録か，MAC アドレスに対する IP アドレスなどの情報の更新かが分からず，不正確な申請が届くことになってしまった．MAC DB サーバへの登録作業時に，改めて，MAC アドレスに対応する IP アドレスを検索し直すことが多くなることで，複数の IP アドレス（MAC アドレス）を登録する作業自体が煩雑となり，登録の遅延を引き起こした．

4. ネットワーク管理用データベース

前節で述べたように，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．そこで，新たに管理用 DB サーバを構築するにあたり，旧版の管理用 DB サーバと同様，ユーザインタフェースとしてウェブブラウザを利用することとした．データベース管理システムは，PHP を介して，ウェブアプリケーションと親和性が高い PostgreSQL を採用した．PostgreSQL の特徴として，豊富なデータ型を備えていることが挙げられる．IP アドレスは，inet 型で定義すると，‘aaa.bbb.ccc.ddd’ といった IP アドレスの入力を直接受け付けることができる．MAC アドレスは，macaddr 型で定義すると，‘aa:bb:cc:dd:ee:ff’，‘aa-bb-cc-dd-ee-ff’，‘aabbcc:ddeeff’，‘aabbcc-ddeeff’，‘aabb.ccdd.eeff’，’aabbccddeeff’ といった MAC アドレスのほとんどの表現形式を網羅しており，これらの入力を直接受け付けることができる．PostgreSQL の採用により，問題点 2 で述べた，誤入力を防ぐことができる．管理用 DB サーバのハードウェア及びソフトウェアの詳細を表 1 に示す．

管理用 DB の属性を**表 3** 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．また，部局管理者と情報共有するために必須となる項目は，旧版の管理用 DB から引き続き属性として定義している．表中，更新日と更新者は，本システムで自動的に登録される項目である．

4.1 ホーム画面

管理用 DB サーバのホーム画面を**図 2** に示す．本学では，クラス B のネットワークをクラス C 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．管理用 DB サーバでは，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．

ホーム画面は，上段，中段，下段の構成となっており，上段には「検索」「登録」「確認」の各機能へのリンクが張られている．中段には，ログイン ID の所属するグループに応じたサブネットの一覧が表示される．このため，割り当てられたサブネット以外の情報を操作することも閲覧することもできない．下段は，中段のサブネットのボタンをクリックすると，サブネットに登録された機器情報の一覧を表示する領域である．各レコードをクリックすると，**図 3** に示す登録画面に遷移し，レコードの詳細を閲覧できるとともに，登録内容を変更したり，削除したりすることが可能となる．

4.2 登 録 機 能

登録画面（図 3）では，必須項目を入力し登録ボタンを押すことによって情報が登録される．実際にデータベースに登録する前には，**図 4** に示すように，本当に登録するか確認画面を表示している．同時に，入力された IP アドレスまたは MAC アドレスと一致するレコー

表 3 ネットワーク管理データベースの管理情報
Table 3 Information registered on the network management database.

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

図 2 ネットワーク管理データベースホーム画面
Fig. 2 The main screen of the network management database.

ドが部局のサブネットに存在する場合，該当するレコードの一覧を表示し，これらのレコードを残すか確認している（残す場合はチェックを外す仕様となっている）．

本学の場合，利用者は登録申請を忘れずに行うが，削除申請を忘れてしまうことが多い．本機能は，重複する IP アドレスまたは MAC アドレスの一覧を部局管理者に示すことによって，利用者の削除申請忘れを防ぐことも目的のひとつである．

4.3 CSV ファイルとの連携機能

申請件数が多い場合には，申請内容を一括登録可能な機能が必須であるため，部局管理者からのこの機能に対する強い要望があった．本管理用 DB サーバでは，CSV ファイルによる一括登録機能，CSV ファイルの内容とデータベースの内容を完全に一致させる同期機能を提供し，部局管理者の利便性の向上を図っている．

また，登録されたレコードの一覧を CSV ファイルに出力する機能も提供している．ホーム画面上の「全管理データを CSV ファイルに書き出し」による全レコードの一覧や，検索結果画面上の「CSV 書き出し」による検索結果の一覧を CSV ファイルに出力することが可能である．

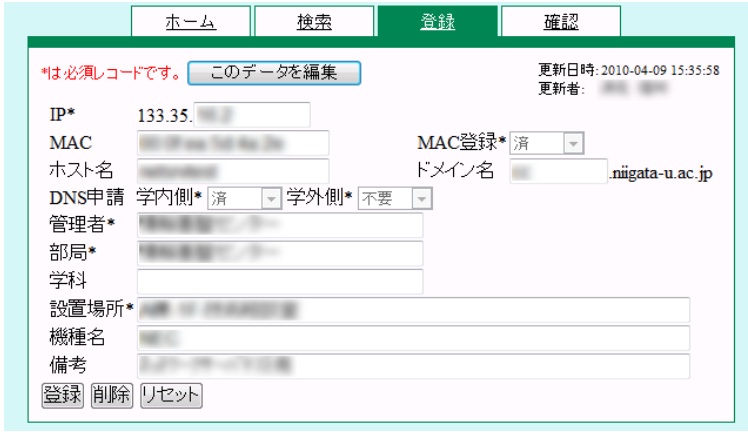

図 3 ネットワーク管理データベース登録画面
Fig. 3 The registration form of the network management database.

図 4 ネットワーク管理データベース登録確認画面
Fig. 4 The confirmation of the registration form of the network management database.

4.4 その他の機能

管理用 DB サーバには，その他，検索機能や，パスワード変更機能等を実装している．サーバ管理者向けには，ユーザ作成機能と部局（グループ）作成機能が実装されている．ユーザ ID 毎に 1 つの所属部局を割り当てることが可能であり，部局毎に複数の管理サブネットを割り当てることが可能である．これらの機能を組み合わせると部局毎に複数の部局管理者を登録することができる．

4.5 MAC DB サーバとの連携

本学のネットワークアクセス認証の構成では，管理用 DB サーバに登録された 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，管理用 DB サーバ上の 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は大変重要である．特に，管理用 DB サーバでは PostgreSQL が稼働しているが，MAC DB サーバでは Active Directory が稼働している．異なる DBMS 間で確実に MAC アドレスを連携するため，本システムを稼働させた当初は，手動で両データベースを連携していたが，登録の遅延を引き起こす一因となった．そこで，連携を自動化するために次の 2 つの方法を試みた．

(1) 同時登録システム

管理用 DB サーバ上での MAC アドレスの登録と同時に，MAC DB サーバに通信を行い登録を行うシステムである．管理用 DB サーバから MAC DB サーバに LDAPS で通信し，MAC アドレスの登録及び削除を同時に行う．

(2) 定期同期システム

管理用 DB サーバと MAC DB サーバとの同期を定期的に行うシステムである．定期的に管理用 DB サーバは，MAC DB サーバから登録されているレコードの一覧を取得し，レコードの差分を MAC DB に返送する．MACDB サーバでは，定期的に差分データを反映することによって管理用 DB サーバとの同期を実現する．

同時登録システムは，MAC アドレスの登録後，即座に MAC DB サーバに反映される利点があるが，MAC DB サーバの故障や通信異常等の障害により同期に失敗した場合の回復手段を別途用意しなければいけない．また，MAC DB サーバに対して，リモートでレコードの登録や削除を行うので，同期用 ID とパスワードが漏洩した場合の被害は甚大である．そのため，同期用 ID とパスワードの管理には，当然であるが，十分な配慮が必要となる．一方，定期同期システムは，MAC DB サーバのレコードを読み取るための権限のみ必要であるため，パスワードの漏洩等による不正登録の危険性を回避できること，定期的に全レコードのマッチングを行うため，通信障害等により同期に失敗しても次回の同期で回復が可能で

図 5 ネットワーク管理データベースログ確認画面
Fig. 5 The log view screen of the network management database.

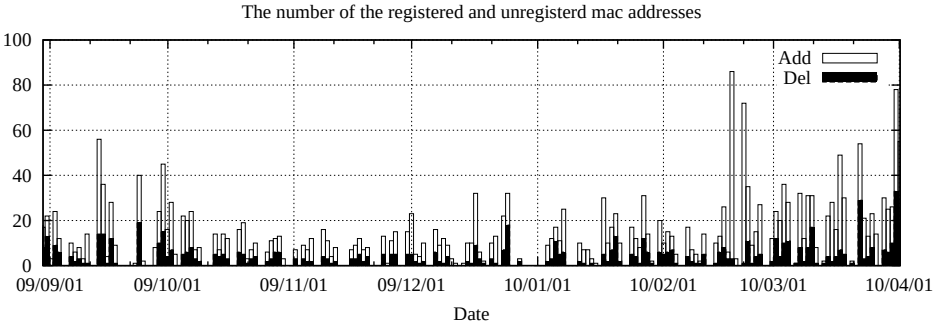

図 6 MAC アドレス登録状況
Fig. 6 Status of MAC address registration

あるというメリットがある．このため，現在稼働中の管理用 DB サーバでは，定期同期システムを採用している．データベース間の同期を 1 時間毎に行い，同期結果は**図 5** に示す画面で確認することができる．

また，MAC DB サーバに申請された MAC アドレスが本当に登録されているかを部局管理者が確認するための，MAC アドレス登録確認機能を実装している．この機能は，管理用 DB サーバのウェブインタフェース上で MAC アドレスを入力すると，MAC DB サーバに直接問い合わせ，MAC アドレスが本当に登録されているかを表示する機能である．問い合わせの際には，データ読み取り専用のユーザ ID で問い合わせることによって，セキュリティに配慮している．

5. 運用状況

管理用 DB サーバを開発後は，情報基盤センターでの登録作業に対する負荷は著しく減少した．以前は手動で行っていた管理用 DB サーバと MAC DB サーバとの連携を自動化することにより，情報基盤センター側での登録作業が無くなったことが大きい．現在まで，特に登録に関する問題は生じていない．また，問題となっていた入力ミスは，入力の制約を与えることができたため，ほぼ全滅したと言ってよい．

図 6 に管理用 DB サーバ導入後 6ヶ月間の MAC アドレス登録，及び，削除の状況を示す．登録と削除を合計すると，1 日あたり平均 12.7 件であるが，日によってかなりばらつきがある．9 月末から 10 月初めにかけては，後期が始まるためか登録や削除が多くなっている．また，2 月の後半から 4 月にかけては，年度末のため登録や削除される MAC アドレスが多く，最大では 1 日あたり 80 件を超える日もある．一方で，11 月頃には，登録される MAC アドレスは少なく，ほとんど登録，削除のない日もあることがわかる．手動登録の場合，特に登録，削除が多い 2 月末から 4 月にかけては，作業の遅れが発生することが懸念されるが，本システムの導入により迅速に作業を行うことが可能となり，部局管理者，情報基盤センター担当者の両者から好評である．

全体として，登録件数が削除件数より多いことが分かる．単純に機器の数が増えている可能性も考えられるが，廃棄の際に，削除申請を忘れている機器が多いという可能性も否定できない．不必要な登録があると，データベースが膨れ上がる等の問題を引き起こす．不必要な MAC アドレス登録を防ぐための，適切な運用方法を見つけることは，引き続き，今後の課題である．

6. おわりに

新潟大学でのネットワークアクセス認証システム導入に伴う，ネットワーク運用状況の変化と，管理用 DB サーバについての概要を述べた．認証システムを導入するにあたっては，認証情報の管理という新たな業務が発生し，管理者にとっては大きな負担が発生する可能性がある．今回は，管理用 DB の構築により，その管理負担増大を軽減することが出来た新潟大学での事例を紹介した．

利便性の高いウェブインタフェースと，自動登録により，ネットワーク管理業務を大きく軽減することが出来た．今回は MAC アドレスの自動登録を行ったが，管理用 DB サーバを利用して DNS の管理も行っているため，今後は，DNS サーバとの自動連携についても検討する予定である．

参考文献

1) 田島浩一，西村浩二，近堂徹，岸場清悟，相原玲二：ホスト登録を用いたネットワーク認証システムの実装と評価，学術情報処理研究，No.11, pp.42-49 (2007).
2) 志村俊也，徐浩源：横浜国立大学「認証ネットワーク」: 運用管理方法の改良，学術情報処理研究，No.10, pp.81-84 (2006).
3) 徐 浩源，大山 清，志村俊也：IP アドレス管理システムの開発と運用，学術情報処理研究，No.8, pp.79-82 (2004).
4) 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).