全学ネットワークアクセス認証システムの導入

浜元信州[†1] 青山茂義[†1] 三河賢治[†1]

新潟大学において，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の構築と運用状況を報告する．認証を導入したことにより，不正ネットワーク利用者の排除，利用者の追跡が可能になり，キャンパスネットワークの信頼性が向上した．システムの運用開始から現在に至るまで，サービス停止等の重大な問題はなく，安定した稼働を続けている．本稿では，全学規模での導入を行なうにあたって，認証システムの設定や問題点，現在の利用状況について述べる．

Installation of Network Access Authentication System for the Campus Network

NOBUKUNI HAMAMOTO ,[†1] SHIGEYOSHI AOYAMA [†1]
and KENJI MIKAWA[†1]

We report the operation of the autheticated network installed for the new campus network of Niigata university. The new campus network is safer than before because the users of the network can be identified and unauthrized persons can not access to the network. We did not experienced any network failure since the new network was installed.

In this report, we describe settings of the installed switches and servers. The problems of the new campus network is also described in this report.

1. はじめに

新潟大学は，9学部，7研究科，附属病院，及び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．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，運営は，著者らの所属する情報基盤センターが行っている．

近年ブロードバンド環境の整備が進み，ネットワークは，電気，ガス，水道等の公共インフラとしての役割のみならず，ビジネス，教育，研究，娯楽等，社会基盤の中心的な役割を果たすようになった．一方で，ネットワークを利用した著作権侵害やコンピュータウイルスの拡散，不正アクセス等の加害活動の事例も増加している．このような状況の中，本学においても，セキュリティ対策の啓蒙活動と併せて，学内ネットワークの不正利用に対して現実的な対策の必要性が高まっている．

本学では，ネットワークの不正利用対策の一環として，情報基盤センターが中心となり，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．これまでに全学の無線LANシステムや情報基盤センター内の情報コンセントでユーザ認証システムを導入しているが，ほとんど全ての本学構成員が日常的に利用するような大規模なネットワークアクセス認証システムの運用実績がなかった．以下，本学における全学規模のネットワークアクセス認証システムの導入から運用に至る経過を報告する．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，本認証システムの構築や管理・運用面を検討する上で非常に参考になった．

†1 新潟大学 情報基盤センター
Center for Academic Information Service, Niigata University

2. 要件の設定

ネットワークアクセス認証にも様々な方式があり，単純なIPフィルタリングを利用した認証方式から，DHCPを利用したMACアドレス認証，認証スイッチを利用したユーザ認証，MACアドレス認証，IEEE802.1X認証，さらには，検疫システム等，端末のセキュリティ状態の確認まで含んだ方式も存在する．本認証システムの導入の目的を，ネットワークの不正利用に対して，その利用者を明確にできることに設定し，多様な認証システムの中から最適な認証システムの検討を行った．

2.1 全学へ対応可能な認証方式の検討

本学は，主たるキャンパスを新潟市内の二地区（五十嵐地区，旭町地区）に構えるが，その他に附属農場，

演習林，臨海実験所，附属学校（新潟市，長岡市），新潟駅前キャンパス等が佐渡島を含めて近隣の市町に分散している．今回，市内及び遠隔地の全てのネットワークの更新に合わせて，ネットワーク認証システムを導入することになったが，キャンパス毎の差異を与えず，同等の要件を設定する方針で，導入の検討を行った．

本学では，組織毎にネットワークの利用セグメントを分割し，例外もあるが，基本的には組織の代表管理者（以下，部局管理者）の責任において IP アドレスの払い出しを行い，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，払い出した（もしくは回収した）IP アドレスや機器の情報を管理用データベースに登録し，情報基盤センターでは，この管理用データベースに基づいて全学の IP アドレスの払い出しや設置機器の状況を把握している．

しかしながら，このような管理体制の弱点を突き，部局管理者の許可を得ずに不正に IP アドレスを機器に設定し，学内ネットワークに接続する事例が全学の様々な部局にて報告されている．このような場合には，IP アドレスから機器の利用者を特定できず，セキュリティインシデントの際，問題となっていた．このため，ネットワークアクセス認証システムの導入にあたり，特定のシステムや教室ではなく，全学でネットワークアクセス認証を実施することとした．

前述の通り，情報基盤センターでは特定のシステムで認証システムを導入しているが，全学に対して認証サービスを行っている認証システムはない．つまり，本学構成員全員にユーザ ID とパスワードが配布されていない．そこで，認証方式については，ユーザ ID とパスワードによる認証（以下，ユーザ認証）に加えて，機器を直接認証する方式が必要である．また，基本的に固定 IP アドレスでの運用を行っているため，DHCP は利用せず，認証スイッチを利用した方式を採用することとした．

2.2 多種多様な機器への対応の検討

大学という組織は，官庁や企業と異なり，多種多様な機器が設置されている．例えば，一般の事務機器（コンピュータやネットワークプリンタ）の他に，ブロードバンドルータ，NAS，特定の OS で動作する実験機器等，新旧の多彩な機器がネットワーク上で共存している．

本学に設置されているこれら全ての機器に対してネットワークアクセス認証を行える仕組みが必要となるため，IEEE802.1X のようなサプリカントを必要とする認証システムの利用は難しい．最近の認証スイッチでは，サプリカントを利用せず，ウェブブラウザを利用してユーザ認証する仕組みが備わっていることが多い．近年は，ほとんどの OS でウェブブラウザの利用が可能であり，この方式での認証が問題なく動作するため，今回の導入で採用することとした．

新潟大学のネットワークはイーサネットで構築されているため，ネットワークを利用する機器には MAC アドレスが設定されている．そこで，大学特有と思われる多様な機器への対応を考慮して，ネットワークアクセス認証は MAC アドレスによる認証（以下，MAC アドレス認証）を基本とした．ユーザ認証が利用可能な端末であっても，利用者にとって，ユーザ認証手続きは煩雑と感じられることが予想されたため，端末の移動がなく，利用者が決まっているコンピュータについては，MAC アドレス認証を利用することとした．ノートパソコンや携帯用ネットワークデバイス等を，一時的に，学内有線ネットワークに接続する場合は，ユーザ認証でネットワークに接続することを基本とした．

2.3 多段接続された機器への対応の検討

本学の場合，ネットワークに接続する機器は，L2 スイッチに直接収容されている場合もあるが，L2 スイッチに直接収容されずスイッチングハブ等でポートを分岐して収容されていることが多い．古い建物によっては，子ハブ，孫ハブといった多段構成で接続されている箇所も見受けられる．このため，L2 スイッチの 1 個のポートを複数の機器が共有している接続の形態を考慮しなければいけない．

このような多段接続であってもネットワークアクセス認証を行える仕組みが必要となるため，1 個の MAC アドレス，もしくは 1 個のユーザ ID がポートを占有してしまうような認証の方式は本学では利用できない．

3. システム構成

本節では，ネットワークアクセス認証システムを構成するネットワーク機器，認証サーバを紹介し，ネットワークに接続する具体的な機器の認証方針について解説する．

3.1 機器構成

本学のネットワーク構成は次の通りである．エリアスイッチ及びコアスイッチとしてシスコシステムズ合同会社製 Catalyst 6500 を設置している．コアスイッチ，エリアスイッチはメッシュ構成の配線とし，冗長性を高めることで通信の安定化に配慮している．エリアスイッチとコアスイッチは，主たるキャンパスにおよそ 20 台設置している．フロアスイッチは，一部の例外を除き，同じくシスコシステムズ合同会社製 Catalyst 2960 を建物の各階に設置している．フロアスイッチは，遠隔キャンパスを含めておよそ 260 台設置している．本学のネットワーク構成の概要を**図 1** に示す．

ネットワークアクセス認証は，最もエンドユーザ側に近い Catalyst 2960 で行うこととした．本学の例では，ユーザ認証と MAC アドレス認証を併用して運用するため，Catalyst 2960 からの認証要求を一旦，窓口となる「認証サーバ」で受理し，ユーザ認証用

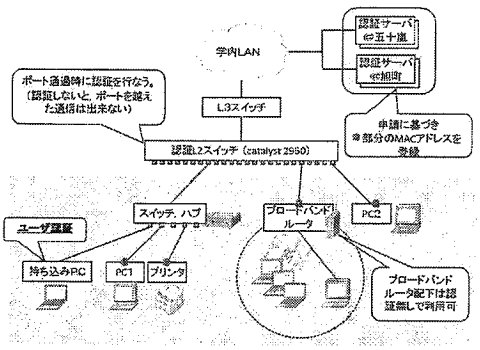

図 1 ネットワークアクセス認証システムの概要
Fig. 1 The overview of the network authentication system.

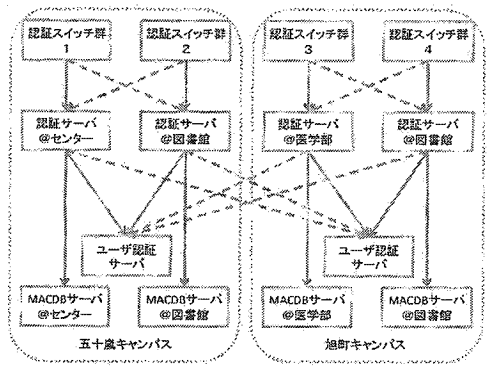

図 2 ネットワークアクセス認証システムに関連するサーバの冗長構成
Fig. 2 Redundant configuration of the authentication servers.

の「ユーザ認証サーバ」及び MAC アドレス認証用の「MAC 認証サーバ」に問い合わせる構成となっている．各サーバの機器構成を**表 1** に示す。

本システムにおいて，認証サーバは大変重要な役割を果たしており，認証サーバが停止した場合，大学全体の業務に甚大な支障をきたす．そこで，認証サーバは論理的にも物理的にも別になるように複数の建物に分散して配置し，停電や機器故障等の不慮の事故に備えている．認証サーバの論理的な構成を**図 2** に示す．

catalyst の認証機能では，認証スイッチに，プライマリとセカンダリの 2 台の認証サーバを登録出来，プライマリの認証サーバへの接続が失敗した場合に，セカンダリの認証サーバへと問い合わせる仕様となっている。プライマリの認証サーバには 5 秒間隔で問い合わせを行ない，5 回応答がない場合に，プライマリ認証サーバには接続できないとみなし，セカンダリ認証サーバへと切り替わる設定とした。また，セカンダリ認証サーバの利用時間は 60 分に設定し，切り替わってから 60 分経過後に，再度，プライマリ認証サーバへの接続を試みるようにしている。認証サーバから MAC 認証サーバへ問い合わせる際には，両サーバはネットワーク的にも物理的にも近くに設置されているため，冗長構成を取らないこととした。仮に，MAC 認証サーバが停止した場合には，認証サーバから正常な結果が返らないため，セカンダリの認証サーバへと切り替わる．認証サーバからユーザ認証サーバの問い合わせの際には，認証サーバ用ソフトウエアの Cisco Secure ACS において，プライマリのユーザ認証サーバとセカンダリのユーザ認証サーバが切り替わるよう設定した．プライマリサーバへ 3 回問い合わせて応答のない場合にはセカンダリに切り替わる．4 台の MAC 認証サーバ，2 台のユーザ認証サーバにある MAC アドレス，ユーザのデータは Active Directory でマルチマスタ構成として設定し，15 分間隔で互いに同期するよう設定した．

3.2 認証機能と設定

本学で導入したネットワークアクセス認証のプロセスは，図 2 に示したように，認証スイッチ，問い合わせの窓口となる認証サーバ，ユーザ認証用の認証サーバ，MAC アドレス認証用の認証サーバが連携して行う．手順の概略を下記，及び，**図 3** のフローチャートに示す．

(1) 配下の機器から認証スイッチに通信が発生する．
(2) 当該の機器が未認証の場合，認証スイッチから問い合わせの窓口となる認証サーバに MAC アドレスが送信される．問い合わせ窓口となる認証サーバは，MAC アドレス認証用の認証サーバ（MAC 認証サーバ）に当該の MAC アドレスを問い合わせ，登録済みである場合は，通信を許可するアクセスリストを認証スイッチに設定して終了する．
(3) MAC アドレスが未登録の機器が接続され，その機器から HTTP または HTTPS でアクセスが発生した場合，当該機器にユーザ認証ページを返信する．当該機器でユーザ ID とパスワードの入力後，問い合わせ窓口の認証サーバは，ユーザ認証用の認証サーバにユーザ ID とパスワードを問い合わせ，正しい組み合わせである場合は，通信を許可するアクセスリストを認証スイッチのポートに設定する．

以上の通り，認証スイッチは，認証に関わる MAC アドレス，ユーザ ID，パスワード等の情報を窓口となる認証サーバに問い合わせる．窓口の認証サーバ自身には，認証を評価する情報は一切なく，ユーザ認証用，MAC アドレス認証用の各サーバに問い合わせを行う．認証が許可されると，窓口の認証サーバから通信を許可するアクセスリストが認証スイッチに送信されて，認証スイッチで当該機器の通信が許可される仕組みである．

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

	認証サーバ	MAC 認証サーバ	ユーザ認証サーバ
機器名	NEC Express5800/110Ri-1	NEC Express5800/110Ri-1	Dell PowerEdge 2850
CPU	Intel Xeon X3350 2.66GHz	Intel Xeon X3350 2.66GHz	Intel Xeon 3.2GHz
メモリ	2GB	2GB	3GB
HDD	73.2GB×2 (RAID1)	73.2GB×2 (RAID1)	73.2GB × 3 (RAID5)
OS	Win2003 Server Standard R2 SP2	Win2003 Server Standard R2 SP2	Win2003 Server Standard R2 SP2
主なソフトウエア	Cisco Secure ACS	Active Directory	Active Directory

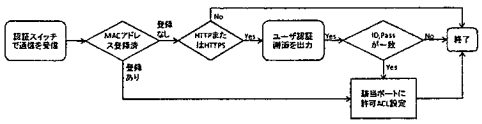

図 3　ネットワークアクセス認証手順
Fig. 3　Flowchart for the network authentication

Catalyst 2960 では，認証情報に関して幾つかのパラメータを設定することができるが，本学では，ユーザ認証，MAC アドレス認証の方式に関わらず，以下の設定を行った．

(1)　認証スイッチは，認証が許可されている機器に対して，認証開始から 1 週間後に認証を強制的に解除する．
(2)　認証スイッチは，認証が許可されている当該機器がネットワークから切断後，25 分後に認証を強制的に解除する．
(3)　認証スイッチは，認証に失敗した機器に対して，認証失敗後，2 分間，当該機器からの再認証を受け付けない．
(4)　認証スイッチは，DHCP，DNS で利用するポートの通信をあらかじめ許可する．

設定 (1) について，MAC アドレス認証の場合は，認証が切断されても機器側から通信が発生すると自動的に再認証される．ユーザ認証の場合は，認証が切断されると，機器側から通信が発生しても認証スイッチで通信が遮断されるので，再度，ユーザ認証を行う必要がある．この設定により，MAC アドレスまたはユーザ ID が認証サーバから削除されても，当該機器が既に認証されている場合は，最長 1 週間利用可能となる．新潟大学では今までネットワークアクセス認証が導入されていなかったため，認証に伴う制限に対して，ユーザからの反対が予想された．このため，認証による制限は極力緩める形で導入を行うという方針とし，1 週間という若干長めと思われる値を採用している。

設定 (2) について，機器を 25 分以上，ネットワークから切断した状態の場合は，再度認証プロセスが実行される．ネットワーク切断後，認証が解除されるまでの経過時間を 25 分として設定したが，運用状況を確認しながら，最適な経過時間を設定する予定である．認証スイッチでは，定期的に ARP 要求を送ることで機器の接続を確認している．本設定は，ARP 要求に対する応答がないため機器が切断されたとみなしてから，認証を解除するまでの時間である．ARP 要求を 5 分おきに発生させ，5 回応答がない場合には，認証を解除する設定とした．

設定 (4) について，本学特有の事情により，認証スイッチを越えて，DHCP による IP アドレスの配布が行われているので，DHCP で利用するポートを開放する必要がある．また，ユーザ認証を行う場合，ウェブブラウザによるアクセスを前提としているので，名前解決ができなければそもそも認証ページを表示することができない．このため，DNS で利用するポートもあらかじめ開放しなければいけない．

ネットワークアクセス認証で使用される MAC アドレス，ユーザ ID，パスワード等の認証情報は隠蔽されるべきであるが，以下の方針に基づき，認証情報を保護している．本システムでは，認証要求端末と認証スイッチとの通信，認証スイッチと認証サーバとの通信で認証情報が流れる．MAC アドレス認証の場合，認証要求端末と認証スイッチとの通信で MAC アドレス，認証スイッチと認証サーバとの通信で MAC アドレスとパスワードが流れる．TCP/IP 通信であれば，MAC アドレスは常時平文でネットワークを流れているので，特に隠蔽の必要はない．一方，認証スイッチと認証サーバとの通信では，RADIUS プロトコルを利用して，ダイジェスト情報のみが流れるように設計している．ユーザ認証の場合，両方の通信において，ユーザ ID とパスワードが流れる．このため，ユーザ認証ページの表示に HTTPS を利用して暗号化し，認証スイッチと認証サーバとの通信では，MAC アドレス認証と同様に RADIUS もしくは LDAPS を利用して認証情報を隠蔽した．

3.3　各種機器への対応方針

前節で述べたように，大学には多種多様な機器が設置されている．ネットワークに接続する全ての機器の認証に対応できるように，ネットワークアクセス認証は MAC アドレス認証を基本として，ユーザ認証を併用する．以下に機器の対応状況を述べる．

パーソナルコンピュータ

パーソナルコンピュータに関しては，ユーザ認証，MAC アドレス認証ともに認証動作に問題なく利用可能である．デスクトップ型のように教室や研究室を移動せずに使用する固定端末は原則 MAC アドレス認証

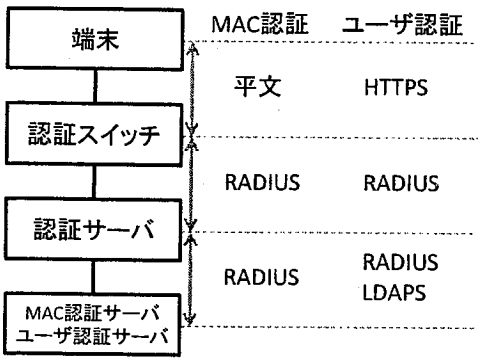

図 4　ネットワークアクセス認証情報の暗号化方式
Fig. 4　The encryption method for the network authentication

を行う方針とした．一方，学内を持ち運んで利用するような携帯端末であっても使用責任者が明確な場合には原則 MAC アドレス認証を行い，学生や教職員による自宅 PC の持ち込みや一時的な利用の場合にユーザ認証を行う方針とした．

ネットワークプリンタ，スキャナ，NAS 等

ネットワークプリンタや NAS 等，ウェブブラウザを表示できない機器に関しては，MAC アドレス認証で対応可能である．

ブロードバンドルータ

ブロードバンドルータに関しては，MAC アドレス認証で対応可能である．ブロードバンドルータの MAC アドレスが認証サーバに登録されている場合には，ブロードバンドルータ自身が認証を許可されるので，配下の機器は個々に認証する必要なく自由にネットワークにアクセス可能となる．一方，ブロードバンドルータの MAC アドレスが認証サーバに登録されていない場合には，配下の機器はユーザ認証を要求される（ただし，ウェブブラウザによるアクセスでなければ単に通信できないだけである）．配下の機器からのユーザ認証で通信が許可された場合，認証サーバは，ブロードバンドルータの MAC アドレスと IP アドレスに紐づけて通信を許可する（すなわち，認証サーバからは，ブロードバンドルータがユーザ認証によって通信を許可されているように見える）ため，配下の他の機器は個々に認証する必要なく自由にネットワークにアクセスできる．このため，ブロードバンドルータの管理責任者は，ブロードバンドルータの配下に接続されている全ての機器に対して責任を持って管理するという方針とした．

シンクライアント

本学特有の事情として，授業用コンピュータと事務職員用コンピュータがシンクライアントで運用されている．授業用コンピュータは，本体に固定ディスクを搭載しないネットワークブート方式の構成，事務職員用コンピュータは，リモートデスクトップを利用した画面転送方式の構成である．

画面転送方式の端末では，機能限定された OS 上のリモートデスクトップ機能によってサーバから転送された画面のみ表示することができるが，端末本体のウェブブラウザからユーザ認証することはできない．このため，画面転送方式のシンクライアントでは，ユーザ認証は不可能，MAC アドレス認証のみ可能である．

本学のネットワークブート方式の端末では，端末の起動時に DHCP によって IP アドレスが与えられるように設計されている．このため，認証スイッチ上であらかじめ DHCP で利用するポートの通信を許可しておく必要がある．ネットワークブート方式では，一旦，端末が起動すると，端末自身のウェブブラウザからユーザ認証を利用可能である．本学の場合，授業用コンピュータにログオンするときにユーザ認証を行っているので，二重のユーザ認証は行わず，MAC アドレス認証を行う方針とした．

4. 導入計画

全学規模でネットワークアクセス認証システムを導入するにあたり，先ず始めに利用者の混乱が予想された．本システムの認証方式として，MAC アドレス認証，ユーザ認証を選択可能であるが，前者の場合は，利用者が機器の MAC アドレスを調査しなければならず，後者の場合は，ユーザ ID とパスワードを本学構成員全てに配布しなければいけない．そこで本学では，**表 2** に示すようなタイムスケジュールに基づき，ネットワークアクセス認証システムの導入を計画した．具体的には，以下の作業を行い，事前に十分な評価を行った上で，実際にネットワークアクセス認証を導入するに至った．

(1)　情報基盤センターで MAC アドレスの収集を開始する．
情報基盤センターで管理する全ての L3 スイッチの ARP テーブルを毎時間 SNMP で収集し，MAC アドレスと IP アドレスの対応表の一覧を作成した．

(2)　部局担当者に MAC アドレスの照会を開始する．
本学の場合，IP アドレスは組織毎に管理されている．そこで，情報基盤センターから部局管理者に，担当する IP アドレスと対応する MAC アドレスの一覧表を送付し，対応表に誤りがないか確認を依頼した．当然，MAC アドレスを調べられないことも予想されたので，オペレーションシステム毎の MAC アドレス調査マニュアルを用意し，依頼時にマニュアルを送付した．

(3)　認証サーバを稼働する．
収集した MAC アドレスを MAC 認証サーバに登録し，MAC 認証サーバを稼働させた．MAC

表 2　ネットワークアクセス認証システム構築スケジュール
Table 2　Time schedule for the introduction of network authentication system.

スケジュール	作業内容
導入 8ヶ月半前	情報基盤センターで MAC アドレスの収集を開始する.
導入 7ヶ月前	部局担当者に MAC アドレスの照会を開始する.
導入 5ヶ月前	部局担当者に MAC アドレスの照会を終了する.
導入 4ヶ月前	認証サーバを稼働する.
導入 3ヶ月半前	情報基盤センターでネットワークアクセス認証の先行導入を開始する.
導入 2ヶ月前	一部の組織でネットワークアクセス認証の先行導入を開始する.

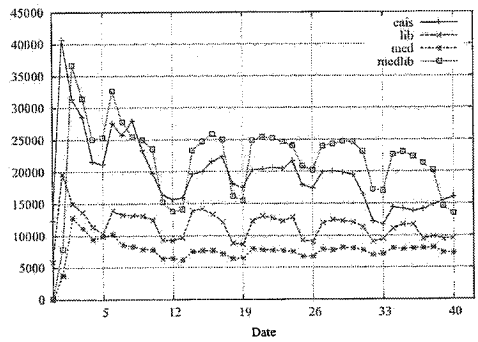

図 5　認証サーバへのアクセス数
Fig. 5　The number of accesses to the authentication servers.

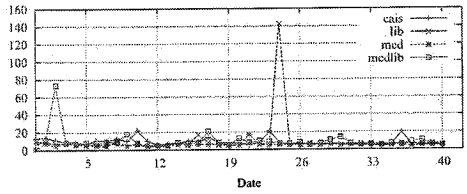

図 6　認証サーバへの 1 秒あたりのアクセス数の最大値
Fig. 6　The number of peak accesses per second to the authentication servers.

認証サーバへの MAC アドレス登録，削除などの運用手順の調整や，MAC 認証サーバと窓口の認証サーバとの連携設定についての評価を行った．

(4)　情報基盤センターでネットワークアクセス認証の先行導入を開始する．
情報基盤センターで事前にネットワークアクセス認証を開始して，システムの調整や不具合等の確認を行った．この時点で，利用者からの想定される質問や回答案，利用者マニュアル等を整備し，運用開始のための実質的な準備に入った．

(5)　一部の組織でネットワークアクセス認証の先行導入を開始する．
一部の組織に協力してもらい，ネットワークアクセス認証の導入時に起こりうる問題等について，事前に十分な評価を行った．

5. 運用の評価

全学規模のネットワークアクセス認証システムを稼働するため，運用開始前には様々な困難が予想されたが，比較的スムースに運用を開始することができたと思われる．本節では，運用の状況や本学で実施した救済措置等について報告する．

5.1 運用状況

混乱を避けるため，五十嵐地区と旭町地区で 1 日ずらして，2 日間でネットワークアクセス認証を開始した．各キャンパスに設置した 4 台の認証サーバへのアクセス数を**図 5** に示す．図中，横軸は，五十嵐地区の認証開始日からの経過日数，縦軸は，認証サーバへのアクセス数である．各グラフについて，'+' は情報基盤センター（cais），'×' は附属図書館（lib），'∗' は医学部（med），'□' は医歯学図書館（medlib）に設置した認証サーバへのアクセス数となっている．ここで，情報基盤センターと附属図書館は五十嵐地区，医学部と医歯学図書館は旭町地区に所属する．7 日周期で，アクセス数の谷間があるが，これは土曜日と日曜日に対応している．認証フロアスイッチから認証サーバへの問い合わせが均等になるように，各認証サーバで受け持つ認証フロアスイッチの台数がほぼ同数になるように，学部を単位として割り振ったが，実際のアクセス数は均等に分散せず，およそ 3 倍の差が発生していることが分かる．結果，認証サーバへのアクセス数は，1 日あたり高々40,000 件程度であり，平均して，最大 2 秒に 1 件程度のアクセスに抑えられている．

次に，1 秒あたりの最大アクセス数を**図 6** に示す．図から，毎日の 1 秒あたりの最大アクセス数は 10 件程度の日が多いことが分かるが，認証開始から 24 日目に医学部設置の認証サーバで 1 秒間に 143 件ものアクセスを記録した．このような場合でも，特に認証サービスが停止することなく稼働を続けている．以上の結果，図 5 と図 6 で示すように，認証サーバにとって，認証フロアスイッチからの問い合わせが大した負担になっていないことが分かる．

最後に，MAC アドレス認証，ユーザ認証が成功した回数をそれぞれ**図 7** の上段と下段に示す．図 5 と同様に，横軸は，五十嵐地区の認証開始日からの経過日

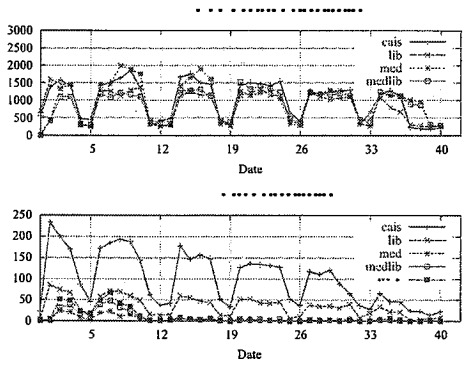

図 7　認証サーバでの認証許可接続数

Fig. 7　The number of authorizations under Mac/User authentication.

数，縦軸は，認証サーバへのアクセス数である．MAC アドレス認証について，ほぼ全ての認証サーバでアクセス数が均等に分散している．一方，ユーザ認証について，情報基盤センターの認証サーバへのアクセス数が最も多く，他のサーバへのアクセス数は少ない．また，図 7 の下段から，五十嵐地区のユーザ認証の成功回数と比較して，旭町地区の成功回数が極端に少ないことが分かる．これは，旭町地区において，ユーザ ID とパスワードの周知が十分でないことを示している．本システムの運用に関しては，特に問題とはならないが，ユーザ ID とパスワードの周知については今後の課題である．

また，ユーザ認証の成功数が，認証開始後，徐々に減少している．これは，認証開始当初，MAC アドレスを間違えて登録する等，ユーザ認証せざるを得ない機器が多数存在したためと考えられる．その後，登録内容を正確な MAC アドレス値に訂正することで，徐々にユーザ認証の利用が減っていったと思われる．図 7 と図 5 を比較すると，実際の認証サーバへのアクセス数と，認証が成功した回数の差がとても大きい．これは，MAC アドレス認証に失敗しているにも関わらず，認証サーバにアクセスし続けている機器が存在しているためである．一つの情報コンセントをハブで分岐し，認証スイッチのポート配下でのみ通信を行う場合（室内利用のプリンタ等）には，認証を行う必要がないため，この様な機器が認証サーバに負荷をかけている可能性がある．管理上、すべての機器について登録をお願いしているが，この例のように通常の利用に問題のないケースでは，未登録機器が残っている可能性が高い．未登録機器からのアクセスにより，認証スイッチ，認証サーバには負荷がかかっていると思われるが、現時点では問題なく稼働している．

5.2　暫定アカウントの発行

認証開始当初は，利用者への周知が不十分であったこともあり，ネットワークアクセス認証が始まること自体を知らない利用者も多数存在していた．このような事例は，多数の構成員を抱える総合大学において，全構成員に十分周知するということの難しさを改めて実感させられる出来ごとであった．このため，認証開始当初は，ユーザ ID が分からない上，MAC アドレス登録も行っていない利用者からの問い合わせが多数寄せられた．

本学では，認証開始から 3 週間は，利用期限を定めた暫定 ID を 1 個だけ用意し，問い合わせのあった利用者に暫定 ID でユーザ認証してもらい，暫定 ID の利用期限が切れるまでに，MAC アドレス登録の申請をお願いした．暫定 ID によるユーザ認証の成功回数の推移は，図 7 の下段の，'■' で示す．認証開始後，3 週間以内に暫定 ID の利用者数は徐々に減少し，ほぼ 2 週間で利用者がいなくなった様子が伺える．

6. 問 題 点

ネットワークアクセス認証の運用開始後，利用者，部局管理者等から苦情を含めて，いくつか問題点を指摘された．今後の改善すべき点として，認証システムのハードウェアに関する問題，運用に関する問題に分けて，以下にまとめる．

6.1　ハードウェアに関する問題点

表 3 に示すように，現在のところ，Catalyst 2960 は，MAC アドレス認証の場合，IP アドレスを，ユーザ認証の場合，MAC アドレスを，ログの項目としてそれぞれ出力できない．本学の場合，MAC アドレス認証を基本としているため，セキュリティインシデント等の発生時に，当該機器の追跡にやや困難を伴う．一方で，Catalyst 2960 は，Device Tracking テーブルという現在の IP アドレスと MAC アドレスの組のデータを保持しているので，このテーブルを定期的に出力し，ログ上の MAC アドレスと対応付けて，当該機器を追跡している．

次に，Catalyst 2960 の配下にルータもしくは L3 スイッチが接続されている場合に，Catalyst 2960 でルータ配下の機器を認証できない事例が報告された．ブロードバンドルータのように，LAN 側の IP アドレスを NAT している場合には問題が発生しないが，ルーティングしている場合に MAC アドレス認証，ユーザ認証ともに利用できない．現在のところ，ルータが接続しているポートの認証設定を解除することで問題を回避している．

最後に，ユーザ認証時のサーバ証明書エラーが挙げられる．本学では，ユーザ認証ページを表示する際，認証要求端末と認証フロアスイッチとの通信を HTTPS で暗号化しているが，認証要求端末側から見ると，ウェブブラウザで入力した URL とは異なる，認証サーバの証明書が送られてくるため，ウェブブラウザによっては，セキュリティ警告画面を表示してしまい，利用

表 3　取得可能な認証サーバ上のログ
Table 3　Available log information on authentication server

	時刻	認証結果	端末 IP	端末 MAC	スイッチ IP	ユーザ ID
MAC アドレス認証	○	○		○	○	N/A
ユーザ認証	○	○	○		○	○

者がユーザ認証をあきらめてしまう場合が多かった．MAC アドレス認証が主に利用されているため，大きな問題にはなっていないが，現時点では，根本的な解決に至っていない．

6.2　運用に関する問題点

本学では，部局管理者の責任において IP アドレスの払い出し（もしくは回収）を行い，IP アドレスや機器の情報を管理用データベースに登録していたが，ネットワーク認証の運用開始に伴い，管理用データベースに MAC アドレスの項目を追加し，機器，IP アドレス，MAC アドレスの対応表を構築することとなった．利用者は，MAC アドレスを調査し部局管理者へ申請を行ない，部局管理者は管理用データベースに MAC アドレスを登録する．MAC アドレスを MAC 認証サーバに登録する作業は，情報基盤センターの管理者権限で行っているため，部局管理者は，MAC アドレスに関して，管理用データベースに登録する作業と，MAC 認証サーバへの登録依頼を情報基盤センターに提出する二つの作業を行うこととなった．このため，情報基盤センターでは，管理用データベースと認証サーバを連携するツールを作成し，登録依頼を廃止することで部局管理者の負担軽減を行った．しかし，IP アドレスと異なり MAC アドレスは機器の入れ替えに伴い頻繁に更新されるので，依然として部局管理者の業務負担が増大しているという問題がある．また，ユーザが機器の MAC アドレスを調査後，MAC 認証サーバに登録されるまでの間は，ユーザ認証を利用して機器をネットワークに接続する．しかし，プリンタ等のユーザ認証が利用出来ない機器は，この期間，全く利用出来ない．部局管理者が不在などで，登録までに時間がかかる場合には，情報基盤センターへ直接連絡が来ることもあり，随時，直接 MAC アドレス登録することで回避している．現在のところ件数が多くないため大きな問題にはなっていないが，より良い解決策を検討中である．

7. おわりに

本報告では，本学における全学ネットワークアクセス認証システムの導入とその後の運用状況について述べた．運用開始前には様々な困難が予想されたが，導入後は大きな問題もなく比較的スムースに移行できたと思われる．認証を導入したことにより，不正なネットワーク利用者の排除や，利用者の追跡ができるようになり，キャンパスネットワークの信頼性が向上したと言える．

運用面では，MAC アドレス未登録の機器がネットワークに接続することで，認証サーバに繰り返し負荷をかけることが分かったが，機器の特定が容易になったこともあり，ネットワークの安定性に影響を与えるほどではない．運用開始後，法定点検による停電を除いて，本システムは連続稼働を続けている．

現在は，認証システム導入後に指摘されたいくつかの問題点について，回避策を検討している段階である．今後，改善策及び新規ツールの導入を予定しているが，結果については別途報告したい．

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).