分断サブシステムと統合認証基盤

北　原　宗　律

（受付　2006 年 10 月 11 日）

は　じ　め　に

大学も，今様の「ユビキタスコンピューティング」や「ユビキタスネットワーキング」への対応に迫られている。学生の方は，すでに，「ケイタイ」を使用した「ユビキタス社会」を体験している。大学は，「学内ユビキタス」の実現のため，関係者全員に自分のノート PC の持ち込みを許可し，無線 LAN ネットワークを構築し，無数のアクセスポイントを設置し，IC カードの携帯を許可している。

通学中の電車やバスの中で，駐車中の車の中で，あるいは，アルバイト先の休憩時間に，学生達が，パソコンを使って，余習・複習をする姿が見られるかも知れない。「ユビキタス勉強」の環境も整いつつある。

2007年 4 月から，学部の約1,300名の新入生全員に「ノート型パソコン」を持たせることを決定し，同時に，無線 LAN ネットワークと IC カード学生証の導入も決定した大学もある。学生は，「自分のノート PC」であるから，学外のどこでも，そのノート PC を使用してもよく，手近のネットワークに接続してもよい。ただ，不正プログラムや不正コードを送り込まれたり，ウイルスに感染したりする危険性や，ある種のファイル共有ソフトや情報事故を惹起するようなソフトなどをインストールしているという心配はないのだろうか。また，PC 本体の盗難等の危惧もある。

大学内では，多くのサブシステムが稼働している。ユーザは，複数の「ユーザ ID」と「パスワード」を持たざるを得ない。つまり，サブシステム間の分断の中で，ユーザ認証も分断されているのである。複数の識別符号を持つことの危険性も指摘されている。そもそも，それでは「大学ユビキタス」とはほど遠いだろう。

このような問題意識から，本小論において，大学キャンパス内のサブシステムについて述べ（1），キャンパスのネットワーク，ワイヤレスネットワークについて述べ（2），先進大学の統合認証基盤を紹介する（3）。

1 大学サブシステム

1.1 出席管理システム

［図 1 ］は，大学のサブシステムの全体像を表したものである。「出席管理システム」は，通常の授業における出欠の管理を行うものである。教室のドアに「非接触型 IC カードリーダ／ライタ」を設置する。学生は，教室のドアに設置されたカードリーダに自分の IC カード学生証をかざすことによって，出席情報が記録される。Felica ケイタイをかざすことで出欠が確認できるものもある。出欠データはサーバに転送され，担当者は全学年の出席状況を確認することができる。学生は，IC カード学生証内のデータで自分の出欠状況を確認することができる。もちろん，一つの授業で複数回出席をとることや補講授業にも対応していなければならない。

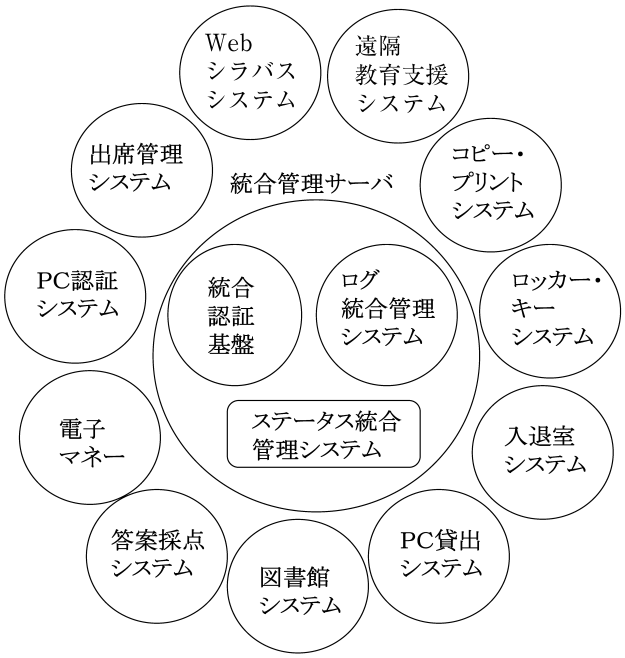


図 1 大学サブシステム

1.2 PC 認証システム

大学の LAN 環境について，「ユーザにとっての簡便な仕組みの確保」と「不正アクセスの確実な防止」という二つの相反する課題を考慮する必要があるという[1)]。「大学では対象ユー

1） 飯田勝吉「東京工業大学の情報通信基盤整備」『ネットマークスソリューションセミナー（2006・10・5）報告書』

ザの数が極めて多く，新入生の中には十分な IT リテラシを持たないユーザがいる可能性もあるため，アクセスに複雑な手続が必要な環境では，事前教育に多大な労力と時間がかかってしまう」。「アクセスの簡便性」と「セキュリティ」を両立させるのが，「ウェブキャプティブポータル」と「MAC アドレス認証」とを組み合わせた，いわば複合方式であるといわれる。ウェブキャプティブポータルとは，Web ブラウザで最初に外部サイトへのアクセスを行う際に強制的に認証ページが表示される仕組みのことである。

1.3 電子マネー

1.3.1 Felica

Felica（フェリカ）は，SONY が開発した非接触 IC カード技術方式の一つである。フェリカの IC カードをリーダ／ライタにかざすと，リーダ／ライタのアンテナからの電磁波を受けて，IC カード内に電力が発生し，この電力で起動した IC カードとリーダ／ライタが相互に通信を行い，データの読み取りと書き込みが可能になる。IC カードをリーダ／ライタが検出後，相互認証を行い，データの読み書きを行う一連の動作を，約0.1秒のスピードで実現した。また，IC カードシステムのデータの通信速度は 212 kbps を達成した。そのため，駅やコンビニなどでの決済に欠かせないものとなっている。リーダ／ライタとコントローラ，リーダ／ライタとカード間の通信は暗号化されている。さらにデータを相互認証するごとに乱数を発生させ，鍵を変えることで，秘話性を向上させたり，データの改ざんの防止処理を行っている。

1.3.2 SAFETY　PASS

SAFETY PASS（セーフティパス）とは，NTT コミュニケーションズが提供する IC カードを使用したサービスである。パソコンに IC カードを接続することによって，ネット上での支払いやサービス利用時のセキュリティを確保することができる。ネット上のサービス利用時は，名前や住所などの面倒な入力も不要で，ショッピングやオークションなど，セーフティパス機能があれば，ネット上のサービスをもっと安全に，教職員の方は，経費精算システムへのアクセスが可能となる。

1.4 プリント管理システム

学生の一人ひとりのプリンタの使用枚数をコントロールするシステムである。学生の使用枚数を制限することによって，無駄なプリントアウトやミスプリントを防止することにある。コンピュータよりプリントコマンドを流し，プリンタに，IC カード学生証をかざすことによって，ハードコピーが出力される仕組みになっている。制限枚数を超過する場合には，Web 上の管理窓口において，制限枚数超過の申請をしなければならない。

1.5 答案採点システム

答案用紙の採点欄に，IC タグラベルが貼付されている。その下に，点数を書き込む欄がある。答案の提出時，または回収前に，学生は，自分の IC カード学生証を IC タグに重ねると，その学籍番号が IC タグに記録される。教員は，点数欄に点数を書き込む。リーダ／ライタを用いると，学籍番号と点数が同時に読み取られ，データとして成績管理サーバに送られる仕組みになっている。採点ミスの防止と成績表への転記ミスの防止が目的である。もちろん，採点時間の短縮と採点作業の省力化につながる。

1.6 入退出システム

教職員が，大学の，教室，実験室，コンピュータ室，演習室，研究室，共同研究室等の入退室の際に「IC カード身分証」を使用するシステムである。入室時に，IC カードをかざすことで，教室等の施錠が解除され，そして，退室時に，IC カードをかざすことで，教室等の施錠ができる。入退出データはシステムのサーバに記録される。

1.7 遠隔教育支援システム

学生が Web 教材を使用して学習できるシステムである。教材の形態として，テキスト文，ビデオ映像，スライドなどがある。教室での授業を Web 上に再現したものである。インターネットに接続できるコンピュータを持っていれば，学内外の両方でこのシステムを利用することができる。また，Web テストをアップすることによって，テストの自動採点が可能となり，授業出席データを追加することによって，成績評価の自動作成も可能となった。

1.8 Web シラバスシステム

Web 上で担当授業のシラバスを作成するシステムである。教員識別番号を記入すると，すべての担当授業のシラバスフォーマットが現れ，それに従って記入するだけでよい。ただ，必須項目について，フォーマットからはずれると，エラー表示が出る。もちろん，学生も，同じシラバスを閲覧することになる。

2 キャンパス公衆 LAN

2.1 大学ユビキタスとセキュリティ

教室，図書館，食堂，セミナーハウス，ロビーなど，大学内のさまざまな場所で，いや，トイレも含めて，あらゆる場所で，「情報コンテンツ」にアクセスすることができる，いわゆる「キャンパス公衆 LAN」の導入を積極的に進めなければならない。つまり，大学ユビ

キタスの実現である。「情報コンセント」をわざわざ用意しなくてもよい。「電気コンセント」から高速ネット接続が現実になりつつある。電力線を利用したインターネット接続の性能は，ケーブルモデムや電話回線利用のデジタル加入者線（DSL）で接続する場合と変わらないといわれている。大学ユビキタスによって，学生の方の利便性が高まり，学習スタイルの自由度も広まるからである。学生に，無線 LAN 内蔵のケイタイパソコンを持たせるのであるから，24時間，何処にいても，勉強ができる環境を用意しなければならない。通学途中のアストラムライン（広島市の新交通システムの愛称）の中で，電車の中で，バスの中で，自家用車の中で，アルバイト先等で，「ユビキタス的に」パソコンが使える環境が望ましいに違いない。ひょっとしたら，本家の「ケイタイ」（すなわち，「携帯電話」）の地位を揺るがす存在になって欲しい。通信料金だけを考えれば，パソコンの方が格段に安くあがると思うからである。また，「IT を自在に活用できる能力を育成することも，現在の社会では基本的なリテラシのひとつになっている。キャンパス公衆 LAN の導入は，IT 教育の側面でも重要な意味を持っている」と言われている[2)]。

2.2 自己防衛型ネットワーク戦略

今や，「ネットワークの境界」を明確に定義することは困難になってきている。ユーザの機器は多くの場合複数のネットワークに接続され，周辺領域はあたかも動く標的のようなものになってきたからである[3)]。顧客パートナー間のエクストラネット通信が日常的となり，ワイヤレスやモバイル，リモートアクセス VPN によって実現された生産性向上も，さらに複数のネットワークへの接続状況を加速させている。

ユーザが自分のノート PC をホームオフィスや公共のホットスポット，あるいはホテルの客室などで他のネットワークやインターネットに接続することによって，ウイルスなどに感染してしまうところに現在のセキュリティの課題が潜んでいる。ユーザはその後で会社や大学に戻り，イーサーネットやワイヤレス LAN のアクセスポイントを通じて，直接社内・学内ネットワークに接続する。そうすると，気づかないうちに不正プログラムや不正コードを送り込んでしまうことになる。それと同時に，ネットワークで最初に異常が発生してから社内・学内ネットワーク全体に伝播し，深刻な結果を招くまでに要する時間は急速に縮まっている。ネットワーク管理者がウイルス，ワーム，トロイの木馬，その他望まれざる侵入者を検出して修復を試みた時点では，時はすでに遅い。ネットワーク機能やサービスのダウンタイムが避けられない事態となっている[4)]。

2） 飯田，同上。
3） PACKET，2005年秋号，シスコシステムズ，2 頁。
4） 同上。

現在のネットワークには分散型のセキュリティ機能，ネットワーク全体にわたってホストの振る舞いやステータスの変化に応じたエンドポイントのクレデンシャル（認証保証書）の文脈自体を認識する力，さらにそれらのクレデンシャルが信用できるものであることを確認する認証メカニズムが必要となっている。

これらの要求に応えられるのが，「自己防衛型ネットワーク戦略」（SDN: ”Self-Defending Network）である[5)]。SDN 戦略の第一段階は，ルータ，スイッチ，ワイヤレスアクセスポイント，および単独のネットワークアプライアンスなど，ネットワークエレメントにセキュリティ機能・サービスを統合することである。SDN 戦略の第二段階は，侵入防衛システム（IPS: Intrusion Prevention System）がアクセス制御リスト（ACL: Access Control List）に対して特定の接続へのアクセス拒否を伝えるなど，協調的な手法で相互連携を図るセキュリティ対応のネットワークエレメントに深く係わっている。これは，他のネットワークへの接続によって，社内・学内ネットワークへの感染源となる可能性を秘めたユーザのエンドポイント機器にまでセキュリティ機能を拡張するものである。そして，第三段階は，適応型防御システム（ATD: Adaptive Threat Defence）と呼ばれるもので，その狙いは，ネットワーク上にあるすべてのパケットとそのフローを守り，その根源で攻撃を断つ能力を持っている。通信に HTTP のポート80を使う Web 対応のアプリケーションの内部から行われるセキュリティ攻撃が増えているので，すべてのパケットとフローの保護が必要なのである。

ATD の段階を加えることによって，複数のレイヤに組み込まれたネットワークセキュリティがイーサーネットポートから Web アプリケーションの内部まで行き届いている。セキュリティの脅威があらゆる角度からネットワークシステムに襲いかかる現在，もはやポイントごとの単体製品では十分な防御を図ることはできない。急速に伝播する攻撃の影響に備えて守りを固めるためには，統合された多層型のシステムによる自己防衛型ネットワークが形成されていなければならない[6)]。

2.3 ワイヤレス侵入防衛システム

ワイヤレスネットワークは，画期的なモビリティと柔軟性・生産性の向上をもたらす一方で，ユーザ自身がネットワークの放送局的役割を果たしセキュリティの新しい脅威のベクトルを自分のネットワークに招き入れてしまう可能性も生み出している。Windows ベースのワイヤレス対応ノート PC は，デフォルトとしてそのアクセスポイントが認可されているか否かにかかわらず，Wi－Fi 接続が可能なあらゆるアクセスポイントを探し回るのが実情である。

そこで，ネットワーク侵入防衛システム（IPS：Intrusion Prebention System）に必要な機

5） PACKET，同上，3 頁。
6） PACKET，同上，8 頁。

能は，1）アクセスポイントの認証，2）無認可アクセスポイントの無効化，3）クライアントの包囲的防御，4）クライアントポリシーの実施，5）ロケーション・ベースの侵入検知，の，5つである[7)]。

アクセスポイントはIPSセンサーとして働き，不正を発見した場合はワイヤレス制御機器／管理機器に報告する。それを受けた機器群は，ネットワーク管理ポリシーに基づいて，ネットワークに接続されている無許可の不正な機器を自動的に排除する。センサーは，不正なアクセスポイントの抑制によって，ワイヤレス機器の情報を検出・集約し，関連づけと実行が可能なネットワークの要素として許可する[8)]。

ワイヤレスLANへの侵入によってもたらされる脅威は，空中を飛び交う無線電送が組織の壁という物理的境界をスルリと抜けてしまうこと，さらにワイヤレスのクライアント機器が，見つけた信号の中で最も強力なものに自動的に接続する性質を持っていることが原因となっている[9)]。

クライアント同士が直接つながれた場合，一時的に特別なネットワークを形成する。このようなピア・ツー・ピア接続で，無認可のクライアントが機密データを記憶している正当なクライアントと自動的につながってしまった場合，その機器のハードディスクドライブにアクセスすることができるため，重大なリスクが発生する。その結果，更に，あるクライアントが別のコネクションに便乗して学内の固定回線に接続されたネットワークリソースに入り込む可能性もある。

IPSのワイヤレス監視システムは，いかなるネットワークプロトコルでも大学の境界外の空間に漏れれば，それを検知してネットワーク・マネージャに是正措置をとるための知識を提供する。最も厳重な安全監視ソリューションは，すべてのワイヤレスLAN機器の存在と活動を検知できるネットワークセンサーを展開することである[10)]。

3　統合認証基盤

3.1　キャンパスシステムの現状

ITの活用領域が拡大するとともに，システム全体の整合性が失われてしまうことが少なくない。大学も，行政機関と同じで，「縦割り」が未だに残っている。各々の部局毎に情報化・ネットワーク化を実施したことによって，統合性が失われてしまっている。予算という制約

7）　同上，14頁。
8）　同上，15頁。
9）　同上，16頁。
10）　同上，17頁。

がある以上，それは避けられないことかも知れない。また，新しい機能が追加されたシステムが出回ることで，従来のシステムが数年で陳腐化してしまい，年次的な情報化，あるいは段階的な情報化ということが困難な時代になっている。情報機器の方は「IT スピード」で進化し，大学の情報化計画が「ペーパスピード」で実施されるのであるから，それらの両者の間隔は広がることこそあれ，絶対に狭まることはない。情報機器が居眠りすることも考えられないのである。

「新たな機能が次々に追加されるということで，システムが“つぎはぎ”だらけになったり，サブシステム間が分断されてしまう可能性が高くなるのだ。特に複数の OS を利用しているシステムではこの傾向が高くなる。これによってシステムの運用負担が増大し，ユーザの利便性も損なわれてしまうのである」[11]。このような“分断されたサブシステム”の中でも特に大きなデメリットをもたらすのが，ユーザ認証の分断である。複数の認証サーバが利用されている環境では，当然，ユーザは複数の ID とパスワードを使用する必要がある。これらすべてを覚えておくことは至難の業である。そのためユーザはパスワードをメモするようになり，メモの紛失などによってパスワードの漏洩の危険性も高くなる。また，ユーザ情報の管理作業にも時間がかかるようになり，ユーザ管理の徹底も難しくなる。単に利便性が損なわれるだけでなく，セキュリティ上の問題も引き起こすことになってしまう。

3.2 統合認証基盤の必要性

3.2.1 東京経済大学の統合認証基盤［図 2］[12]

認証システムとしては LDAP と Active Directory が導入されており，UNIX 系システムの認証は LDAP サーバ，Windows 系システムの認証は Active Directory によって行われる。これらの認証システム上の情報は MIIS2003 によって同期化される。管理者がユーザ情報の登録や変更を行うと，MIIS によって LDAP と Active Directory の両方に情報が送られるようになっている。さらにホームディレクトリやメールボックスの作成・削除なども，MIIS とアプリケーションサーバ（UNIX）との連携によって自動化されている。管理用ツールは Web ブラウザで利用できるようになっている。

このような統合認証基盤を導入したことによるメリットは計り知れない。管理者の負担が大幅に軽減したことが最大の効果であるように思われる。管理用ツールの Web 化もその負担軽減に大きく貢献している。管理者側の負担軽減は，同時に，ユーザ側の利便性の向上とも連動しているのである。すなわち，パスワードの変更やメールの転送などのユーザ機能も，Web ブラウザで利用できるようになっているのである。その上，基幹系を含めて PC 教室ま

11） http://www.netmarks.co.jp/case/pdf/user_report_tokyokeizai.pdf
12） 同上。

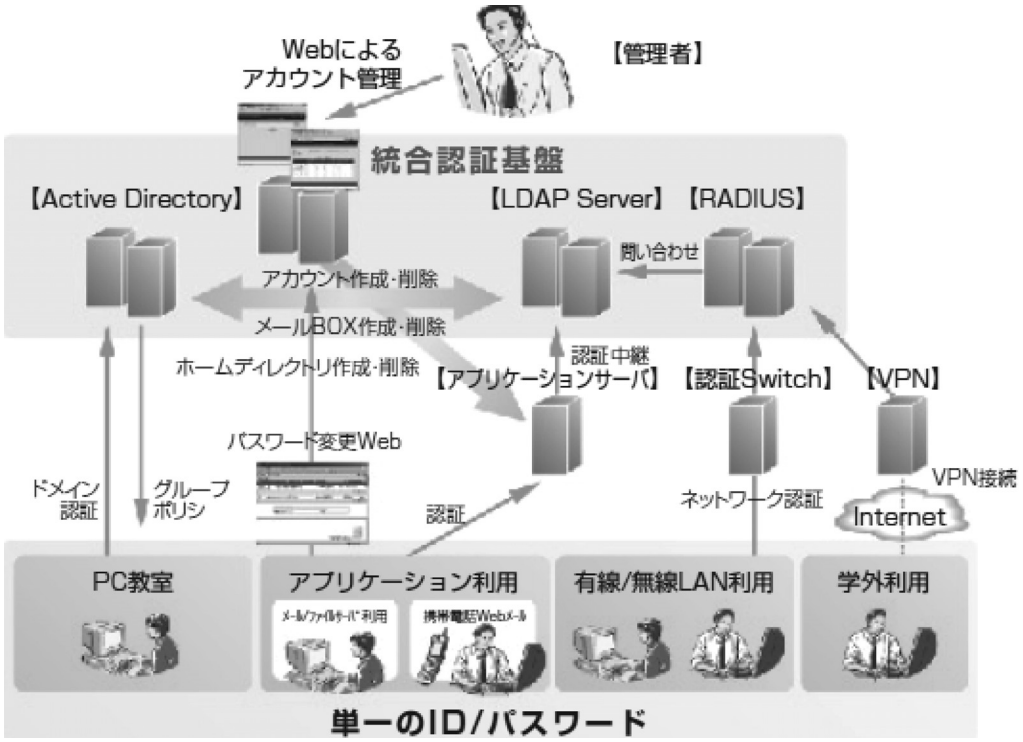


図 2　東京経済大学の統合認証基盤

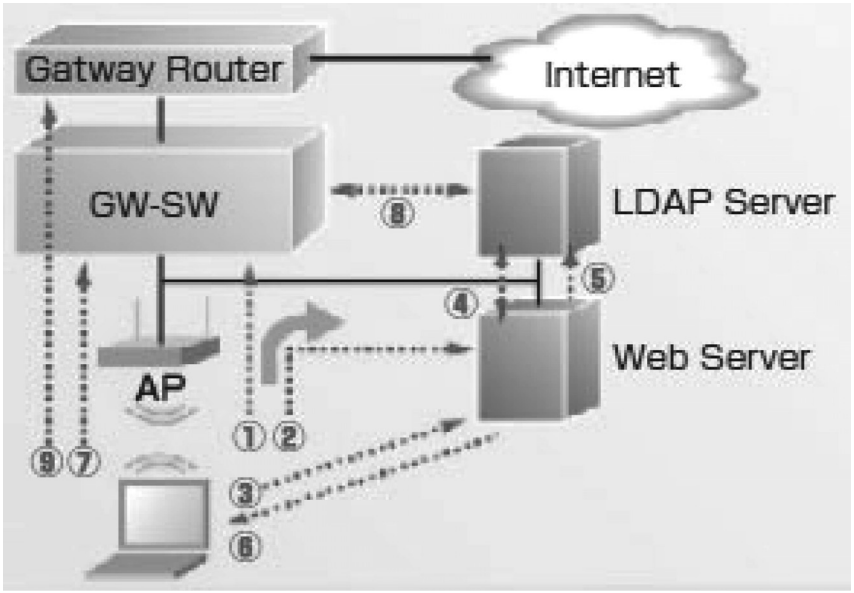
でをもギガビットネットワークで構築するなど，通信スピードも高められており，システム停止のリスクも冗長化設計によって低下している。インフラ再構築後も，計400台以上設置している PC 教室でのネットワークに関するユーザからのクレームはほとんど発生していない，ということである。

また，統合認証基盤の構築により，むしろ，サブシステムの導入が容易になったともいえる。同基盤上で，「就職支援システム」，「印刷枚数管理システム」や「Web メール」のサービスが実現されており，さらに，学外から学内ネットワークにアクセスできる VPN サービスも開始したが，そのサービスにおける認証も同じ基盤によって一元的に管理されているのである。

3.2.2　東京工業大学の統合認証基盤［図 3］[13)]

パスワードと MAC アドレスによる複合型認証方式によるユーザ認証はつぎのような手順で行われる。まず，ユーザは無線 LAN アクセス可能な PC から，ネットワークへのアクセスを行う。このファーストアクセスは無線 LAN スイッチから外部のウェブキャプティブポー

13）　http://www.netmarks.co.jp/case/pdf/user_report_tokyo_tech.pdf



認証プロセス

① ユーザは端末をLANに接続し、DHCPによりIPアドレスを取得
② 外部Captiveportalにリダイレクトし、ユーザに認証画面を表示
③ ユーザ名とパスワードをHTTPSを用いて送信
④ LDAPサーバに問い合わせを行い、ユーザ名、パスワード、MACアドレスを確認
⑤ ユーザ名、パスワード、MACアドレスをLDAPサーバに登録
⑥ GWスイッチのセッションキーを含むページを生成し、ユーザに表示
⑦ ユーザ名とセッションキーをHTTPSを用いてGWスイッチにアクセス
⑧ LDAPサーバに問い合わせし、アクセスされたユーザ名と
セッションキーの正当性を確認
⑨ セッションキーの正当性を確認後、GWスイッチは端末の通信遮断を解除

図 3　東京工業大学の統合認証基盤

タルサーバ（外部サーバ）にリダイレクトされ，外部サーバからユーザ ID とパスワードを入力する画面がユーザの PC に送られる。ユーザはここでユーザ ID とパスワードを入力する。MAC アドレスが未登録の場合には「MAC アドレス登録画面」も表示される。ユーザが MAC アドレスを登録すると，外部サーバはその情報を LDAP サーバに登録する。さらに，ユーザ PC に対して無線 LAN スイッチの認証機能に強制ジャンプするように指示する。ユーザ PC はこの指示に基づいて無線 LAN スイッチにアクセスし，その無線 LAN スイッチは LDAP サーバと連携したユーザ認証を行う。ここで正規ユーザであると認識されると，キャンパス公衆ネットワークにアクセスできるようになる。「ユーザ ID とパスワードだけの認

証では，パスワードが漏洩した場合にユーザ本人に知られることなく，無制限に不正アクセスが繰り返される」[14]。しかし，これに MAC アドレス認証を組み合わせることで，不正アクセスに制限を加えている。正規ユーザが使用するものとは異なる PC からアクセスされた場合，その PC の MAC アドレスが LDAP サーバに登録されるため，不正使用を即座にチェックすることが可能である。また，不正な MAC アドレスの登録を防止するため，ユーザ毎に登録可能な MAC アドレスは 2 個までに制限し，登録 MAC アドレスの変更も 1 日 1 回までにしている。

3.2.3　青山学院大学の統合認証基盤［図 4］[15]

このネットワークで特徴的なのは，認証 VLAN を利用した，高度な認証システムを導入したことにある。ネットワークを利用するときに，ユーザは，ユーザ ID とパスワードによって認証を受けるが，ここで認証されなければネットワークにアクセスすることすらできない。

認証に必要なユーザ情報や権限情報は，LDAP サーバによって一元的に管理されている。学生，教員，職員などのユーザの権限に応じて，アクセスできる VLAN をあらかじめ定義し，グループ単位，個人単位で VLAN リソースへのアクセスを制限することができる。さらに，「ネットワークの利用履歴も記録され，誰が，何時，どのスイッチから，どの MAC アドレ

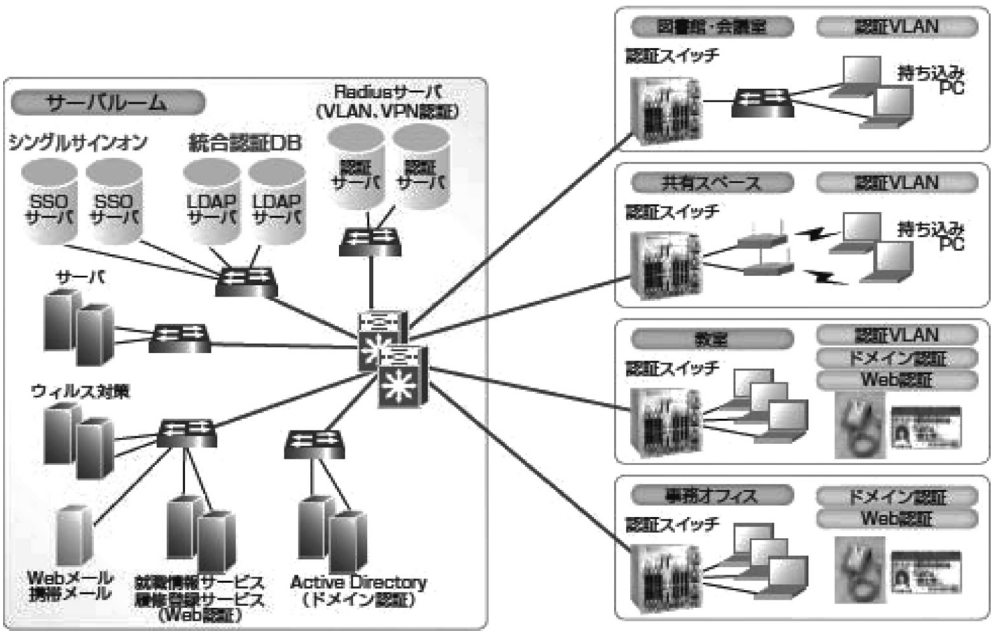


図 4　青山学院大学の統合認証基盤

14）　同上。
15）　http://www.netmarks.co.jp/case/pdf/user_report_aoyama.pdf

スでネットワークにアクセスしたのかを追跡することも可能」になっている。

学内に設置されたパソコンだけではなく，教員や学生が持ち込んだパソコンもネットワークに容易に接続することができるようになっている。このほか，学内には，学生用の共用端末も設置されており，ここから授業スケジュールの参照や履修登録などを行うことが可能である。これらの端末では，「ユーザ認証に，IC が組み込まれた学生証を近づけるだけで，アクセス可能なリソースにシングルサインオンできる」。

以前は学内に複数の認証システムが存在し，ユーザに混乱を招く事態が生じていた。つまり，一人のユーザが複数の ID やパスワードを管理しなければならないため，かえってセキュリティが甘くなる傾向があった。「今回のネットワーク構築で統合認証を導入したことで，これによって，ユーザ側の利便性と管理者側の管理性という相反する特性を同時に向上させることができた」[15a)]。

3.2.4 獨協大学の統合認証基盤［図 5］[16)]

獨協大学は，バックボーンに ATM を利用した IP ネットワーク（“DAINET”）を構築している。全教室の PC 約1,300台がこの DAINET を介してインターネットに接続されている。2003年 3 月から，ATM ネットワークは，ギガビットイーサーネットワークにリプレイスされ，バックボーンの高速化・広帯域化がはかられた。同時に，認証 VLAN が導入され，ネットワークレベルの認証システムが稼働中である。

「認証 VLAN」によって，ネットワークスイッチがユーザ ID とパスワードを確認するた

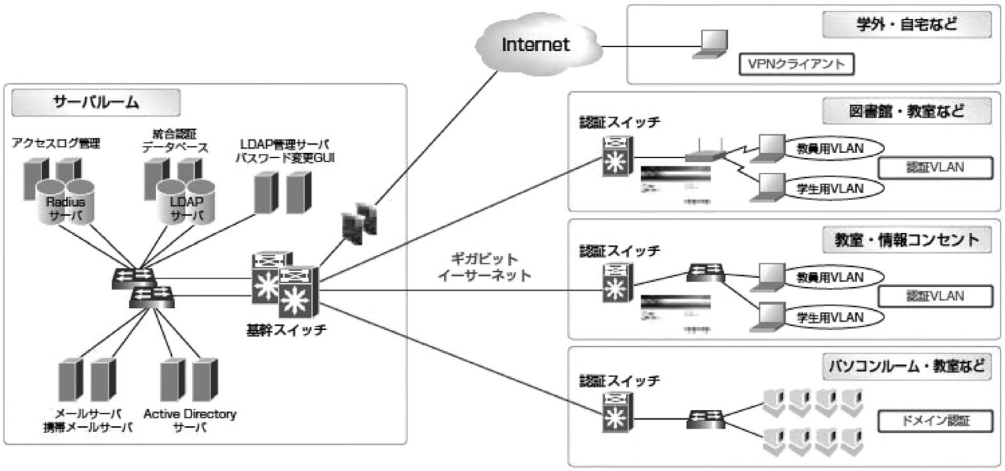


図 5　獨協大学の統合認証基盤

15a）http://www.netmarks.co.jp/case/pdf/user_report_aoyama.pdf
16）　http://www.netmarks.co.jp/case/pdf/user_report_dokkyo.pdf

め，ネットワークの入口で不正アクセスをシャットアウトでき，複数の OS にも対応可能である。従来では，ユーザ認証に Windows ドメインが利用されていたため，Windows レベルのセキュリティが確保できても，ネットワークレベルのセキュリティの確保や，Macintosh や Linux のユーザ認証には対応できていなかった。

また，認証 VLAN の導入により，十分なセキュリティを確保できるため，「無線 LAN」の導入も可能になった。学生ラウンジをはじめ，各棟の各フロアに無線 LAN のアクセスポイント（AP）を設置しているため，ISP 的なサービスも学内ネットワークから提供されている。この無線 LAN の導入によって，ユーザはどこからでもネットワークを利用できるようになった。そういう意味では，「学内ユビキタスネットワーク」の実現といえるのではないだろうか。

従来は，LAN のポートを一般に開放していなかった。ネットワークのセキュリティの確保に不安があったためである。ネットワークに接続できる PC も固定的であった。しかし，現在では，教員や学生が自分で持ち込んだ PC を自由にネットワークに接続できる環境になっている。ただ，ネットワークの一般開放と不正利用の防止とを両立させるため，アクセス情報は記録として残さざるを得ない。

そのほか，学外からのインターネット経由で安全にアクセスできる VPN サービスの提供，アカウントの統合，ディレクトリサービス（LDAP）と連携した認証情報管理なども実現されており，その結果，ユーザ側の利便性の向上と同時に，管理者側の負担も大幅に軽減されたといえる[17)]。

お　わ　り　に

先進大学として紹介したシステムは短期間で導入されたものではない。多くのサブシステムの稼働中に，認証の分断の不便性，ユーザ側の高負担，セキュリティ確保における管理者側の高負担に直面してきた。一方で，教職員や学生の私有 PC の持ち込み，無線 LAN ネットワークの構築，IC カード学生証の導入等，学内ユビキタスへの対応に迫られていた。東京工業大学は「キャンパス公衆 LAN に独自の複合認証方式の採用，簡便さとセキュリティを両立した無線 LAN 環境の実現」，東京経済大学は「学内ネットワーク全体のユーザ認証を統合，多様なサブシステムのための共通基盤の確立」，青山学院大学は「認証 VLAN を利用した統合認証システムや IC カード連携でインフラの確立」，獨協大学は「既存 ATM のギガビットイーサネットへ移行，認証 VLAN の活用による安全性と利便性の両立」というよう

17）　http://www.netmarks.co.jp/case/pdf/user_report_dokkyo.pdf

に，それぞれ，大きなテーマを掲げて，検討委員会を立ち上げ，そこで，数年にわたって議論・検討を重ねてきた。その成果が紹介した各大学のネットワークシステムにおいて実現したものと思われる。

大学の分断されたサブシステムを利用する際の個人認証の方策として，総合認証基盤の構築が最も合理的と思われる。一見，トレード・オフの関係にある「利便性」と「管理性」の問題を解決してくれたからである。ただ，従来型・旧型システムが持っていた機能性・利便性等のメリットを継承できるものにすべきである。