さいたま

埼玉大学情報メディア基盤センター年報

VOL.19　2012　Information Technology Center Saitama Univ.

URL　http://www.itc.saitama-u.ac.jp/

Contents

*ＣＡＶＥ（CAVE Automatic Virtual Environment：没入型３次元可視化装置）は、米国のイリノイ大学で開発された１辺が 2.5m（埼玉大学の場合）の４面のスクリーンによる立体映像システムです。液晶シャッターメガネをかけることで映像を立体的にとらえ、観察者の位置や向きをフィードバックするヘッドトラッキングやワンド（3Dジョイスティック）による物体操作を行うことで臨場感が得られます。

平成 22 年度・平成 23 年度活動報告

センターから

震災、そして復興

情報メディア基盤センター長　吉田 紀彦

平成 23 年 3 月 11 日、出張でドイツ北部の小さな町に来ていた。朝早く目が覚めてしまったので、ホテルの部屋でテレビのニュースを眺めていたら、現地時間の朝 6 時 50 分頃、日本時間の午後 2 時 50 分頃、「日本で極めて大きな地震があったようです」との第一報が飛び込んできた。それから後、現地の一部のチャンネルでは通常の番組が全てキャンセルされ、上空から撮影した大津波の映像、そして深夜も燃えさかる気仙沼市街の映像など、何度も繰り返し放送され続けた。

埼玉大学の情報メディア基盤センターでは、地震そのものの被害はないに等しかった。しかし、直後からの計画停電の影響で、各種サービスの定常的・安定的な提供に支障をきたすようになり、学外のデータセンターに一部サービス運用を移すアウトソーシングに踏み切った。

社会的には、ソーシャル・ネットワーキング・サービス（SNS）や Twitter など、インターネットの緊急連絡手段としての効果、それを裏で支えた各種関連技術者たちの、企業や団体の枠を越えた横断的な連携なども、大きな注目を集めたが、一方で様々な問題も浮き彫りにしたと言える。

このような緊急事態に、どう対応すべきか、どう意思決定すべきか、日頃からどう備えるべきかなど、今回の大震災は極めて大きな教訓と課題を残した。他大学の情報系センターを見ても、I 大学のように、自らも甚大な被害を被りながら、地域救済とそれに向けた全国への支援の働きかけを即座に開始した事例、O 大学と Y 大学のように、地理的に離れた拠点間で相互バックアップなどシステム安定運用に向けた連携を図っている事例、その他にもクラウド化の各種事例など、様々な動きがある。1 年前の 3 月、事業継続計画（BCP）というものの重要性を、改めて眼前に突きつけられたと言ってよい。

情報メディア基盤センターでは、その後の 1 年間は、全学情報基盤システムの 5 年ごとの更新に向けた仕様の取りまとめ、そして更新の実作業に取り組んできており、教職員・学生など利用者の皆様の多大なご理解とお力添えもあって、この春になんとか更新できたものと考えている。特に事業継続計画に関しては、データセンターを引き続き活用していくとともに、今後の活動の一環として、他大学の情報系センターに向け、クラウド共同利用の提案を始めつつある。一方で、緊急時の地域貢献のありかたなど、さらに検討していかなれけばならないことも、まだ山積みになっている。

末筆ながら、平成 22 年度の年報を平成 23 年春に取りまとめることができず、今回、このように平成 22 年度および平成 23 年度の年報の合冊という形で取りまとめるに至ったが、今後ともご指導ご鞭撻のほど、何卒よろしくお願い申し上げる次第である。

大学のネットワーク運用の特徴

吉浦紀晃

情報メディア基盤センター

1　はじめに

日本の国立大学法人の情報系センター (センター) は大学の情報システムの管理を行う部門であるが、その業務は多岐にわたる。具体的には、情報教育用端末の管理、大学ネットワークの管理、メールなどの大学全体で利用する IT サービスの管理、大学内の組織に対する情報システムの技術支援、情報リテラシ教育、教育用コンテンツ作成、研究用計算機や研究用ソフトウェアといった研究用の計算機資源の管理などがあげられる。大学の事務組織の情報システムの管理は別の部署が担当している場合が多いが、センターと統合する方針を持っている国立大学法人も多い。本稿ではセンターの業務の中でもネットワーク管理について議論する。特に、大学におけるネットワーク管理の特異な点を議論し、その 1 つであるアクセス制御における問題点について議論する。

2　ネットワーク管理における情報系センターの特徴

ネットワーク管理と呼ばれる業務は大学のセンターだけの仕事ではなく、インターネットサービスプロバイダ (プロバイダ) や企業などの情報システム管理部門 (企業) においても行われている。しかし、大学でのネットワーク管理はプロバイダや企業のネットワーク管理とは異なる点が多い。表 1 は大学のセンターが行うネットワーク管理の特徴と、プロバイダや企業のネットワーク管理との比較を示したものである。表 1 の特徴とは、大学のセンターのネットワーク管理の特徴を表し、プロバイダと企業とあるのはインターネットサービスプロバイダや企業におけるネットワーク管理における特徴の有無を示す。

特徴	プロバイダ	企業
各組織にネットワーク (サブネットワーク) を持ち、ネットワーク運用ポリシーは各組織が決定する	○	×
利用する端末は利用者の自由に選べる	○	×
各組織の独立性は高い	△	△
各組織には決定したポリシーを正しく実施するネットワーク管理能力がない	×	○
利用者とネットワーク管理者との距離は近い	×	○
各組織との間に明確な取り決めがない	×	○

表 1: ネットワーク管理の特徴と他組織との比較

各特徴について以下で説明する。

(1) **各組織にネットワーク (サブネットワーク) を持ち、ネットワーク運用ポリシーは各組織が決定する**

大学内には学部、学科、講座などの様々な組織が存在する。大学のネットワークでは各組織はネットワーク (サブネットワーク) を持ち、このネットワークを各組織自身がどのように利用するかを決定する。例えば、ネットワークに端末だけを接続して利用する、サーバを設置して外部からのアクセスを許すなどの運用方針や、許可する通信や不許可する通信をどれにするかといったアクセス制御を決定する権限を各組織が有している。

この特徴はプロバイダにもある。プロバイダの場合、顧客であるプロバイダ利用者が大学における学部、学科、講座などの各組織に対応する。プロバイダ利用者はネットワークをどのように利用するかやアクセス制御などを自身で決定する。また、プロバイダは顧客に対してネットワークの利用やポリシーに干渉することはない。つまり、プロバイダ利用者に決定権があり、これは大学のネットワークとも類似している。一方、企業のネットワーク管理では企業活動のためにネットワークが利用されるため、各組織にネットワーク利用を自由に決めさせることはない。

(2) 利用する端末は利用者の自由に選べる

大学には教員、職員、学生といった構成員がいるが、利用する端末に制限があるわけではない。大学によっては利用する端末が決まっている場合がありうるが、教員や職員が対象であり、学生に対して利用する端末を制限するということはない。また、端末や利用するオペレーティングシステムが制限されていても、インストールされているアプリケーション、ソフトウェアのアップデートの状況、設定などが利用者毎に異なり、統一された端末を利用することはほとんどない。

この特徴はプロバイダにも当てはまる。一方、企業ネットワークの利用目的は企業活動であり、そのために利用する端末は決まっていることがほとんどである。また、セキュリティの確保のため端末にインストールされるアプリケーションや設定などはすべて企業の情報システム管理部門により管理されていることが多い。企業ネットワークでは端末からネットワークを利用したサービスが利用できない障害が発生した場合でも、端末の設定等を管理部門が把握しているため、障害対応が容易である。

(3) 各組織の独立性は高い

大学内の各組織は関連が強い組織もあるが独立性は高く、センターは各組織は独立したものとして扱う。関連がある組織同士においてネットワークのアクセスを双方で許可するなど組織間にまたがるネットワーク運用を行う場合にはセンターが関わる。各組織を独立したものとして扱うという点ではプロバイダも同様である。プロバイダの場合、各組織は完全に独立であり、仮に組織間で連携があったとしても各組織同士で連携を行えばよくプロバイダは関与しない。一方、企業ネットワークでは、各組織が独立性が高くはないが、組織間の連携が必要な場合には情報システム管理部門が主導的に行うことになる。この点ではセンターと企業の情報システム管理部門は類似している。

(4) 各組織には決定したポリシーを正しく実施するネットワーク管理能力がない

大学の各組織の中で、ネットワーク管理を自力で行うことができる組織は情報関連の学科以外ではほとんどない。サーバ運用を自力で行う組織もあるが、そのサーバ管理者が専門的な知識を有しているとは限らない。企業ネットワークでは各組織がネットワークを管理することはなく、企業ではこの特徴は当てはまる。企業において各組織にネットワーク管理者を配置することは高コストになるため、管理部門において集中管理される。この点では、大学のセンターは企業ネットワークの管理部門に近い。一方、プロバイダにおいてもその顧客は独自にネットワーク管理を行うことが前提である。実際にその能力があるかは別であるが、ネットワーク管理能力があるという前提がある。

ネットワーク管理能力の有無は不正侵入などのセキュリティ問題が起きた場合に重要となる。企業ネットワークでは管理部門が対応し、プロバイダ管理のネットワークでは各組織で対応することとなる。大学のネットワークにおいては、各組織で対応することが多いが、対応することができず、センターが対応することもある。

(5) **利用者との距離は近い**

大学内のネットワーク利用者はトラブルへの対処方法やネットワーク等の利用方法などが分からない場合、センターへ問い合わせを行う。大学の規模にもよるが、利用者が直接センターに来て口頭で問い合わせを行うこともあり、利用者とセンターとの距離は近い。企業ネットワークにおいても、端末を情報システム管理部門が提供していることもあり、利用者は管理部門へ問い合わせすることが普通である。一方、プロバイダにはこの特徴はない。プロバイダに利用者が問い合わせを行うことはほとんどなく、利用者の代表、つまり、プロバイダを利用する顧客のネットワーク管理者がプロバイダに対して問い合わせを行うことになり、プロバイダとネットワーク利用者の距離は遠い。

(6) **各組織と間に明確な取り決めがない**

大学内の各組織とセンターの間にネットワーク管理についての明確な取り決めがない場合が多い。これは大学の中の組織間の取り決めになるため格式ばった書面による取り決めは必要ないと思われているためである。この特徴は企業ネットワークにもあり、1 つの企業の中にある管理部門と各組織で格式ばった取り決めは必要ない。しかし、企業内の規程等が取り決めに変わるものとして利用されており、この点では大学とは異なる。一方、プロバイダとその顧客はまったく異なる組織であり、プロバイダと顧客の間では契約書面が取り交わされる。

これらの特徴からいえることは、大学のセンターは、多数の顧客を抱え、その顧客はネットワークの利用方法、利用する端末、運用ポリシーを自由に決めるが、その管理運用や障害対応はセンターが大きく関与しなければならず、ネットワーク利用者はヘルプデスクとして大学のセンターを利用するということである。このように特徴を分析すると、大学のセンターのネットワーク管理が特異であり、ネットワーク管理する立場からみると非常に扱いにくいネットワークであるといえる。

3　アクセス制御

前述のように、大学のセンターは多数の顧客を抱えその各顧客のネットワークを管理するという、他には見られない特徴をもつ。この特徴は管理技術面における特徴を引き出す。本稿ではその 1 つであるアクセス制御における特徴について述べる。アクセス制御とは IP パケットの通過の許可不許可を制御することで、この制御は IP アドレス、TCP、UDP のポート番号に基づき行われる。アクセス制御は、不正な通信を頻繁に起こす送信元からの IP パケットを遮断することでネットワークの安全性を高めること、そして、サーバへの必要ない通信を遮断することでサーバの安全性を高めることに必要不可欠なものである。

アクセス制御は Layer3 スイッチや Firewall などのネットワーク機器において行うが、このアクセス制御の方針はセンターが決めるのではなく大学内の各組織が決める。この決定された方針に基づきセンターがネットワーク機器にアクセス制御のための設定を行う。この設定はこの組織の数が少ない場合には大きな問題とはならないが、数百となると運用するだけで結構負荷が大きな業務となる。各組織で運用方針が同じであれば運用が大きな負荷なることはないが、各組織の運用方針が異なる場合、大きな負荷となる。

このような大学におけるアクセス制御の管理がプロバイダや企業において発生することは少ない。プロバイダの場合、アクセス制御を各顧客に対して行うことはほとんどなく、常に顧客に対

して通信制限のないネットワークの利用を提供する。また、企業の情報システム管理部門では各組織のアクセス制御の方針を各組織で独自で決めることはなく、情報システム管理部門が方針を決定し運用を行う。アクセス制御において多種多様な運用方針を 1 つの組織で管理するという形態は大学のセンターだけである。

3.1 アクセス制御における問題点

大学のセンターにおけるアクセス制御の管理における問題は多種多様な運用方針をセンターという 1 つの組織で管理することである。本題に入る前に、アクセス制御についてその他の運用上の問題について述べる。この問題とは、アクセス制御の方針を決めることが難しいということである。大学内の各組織がアクセス制御の方針を決めるのであるが、このためにはアクセス制御やネットワークに関する知識が必要になる。しかし、各組織にはこれらの知識を有する人がおらずアクセス制御の方針を決めることができない場合が多い。決められない場合には、センターが方針決定のための支援を行うことになる。この支援もネットワーク利用の詳細を利用者自身が把握していない場合には負荷の大きな業務になる。例えば、IP ネットワークを利用した遠隔会議システムを利用している場合、TCP や UDP のどのポート番号を利用しているかをネットワークの利用者が把握していないことが多い。ポート番号が分からなければアクセス制御をどのように行えばよいか決めることができず、遠隔会議の機器が利用するポート番号などの詳細をセンターが調べアクセス制御の方針を決定することになる。このようなことが 100 個以上の組織でおきると、アクセス制御の方針を決定するだけでも多大な負荷がセンターに押しかかることになる。

この負荷を減らす方法の 1 つとしてサーバなどの集約化がある。サーバをセンターが運用し、このサーバ上で各組織がサーバ機能を利用する。具体例としては、Web サーバの仮想ドメインや Mail サーバの仮想ドメインなどがある。この集約化により大学全体で攻撃対象となりうるサーバの台数を減少させ、セキュリティを向上させるとともに、各組織のネットワークにサーバを置かずに済ませることでアクセス制御の方針も単純になる。この集約化はクラウドの利用と似ているが、様々なサービスをクラウド上に載せることとサーバを集約化させることとは必ずしも一致しない。

3.2 Access Control List の管理

大学のセンターにおけるアクセス制御の管理における問題に話を戻す。繰り返しになるが、この問題は多種多様な管理方針をセンターという 1 つの管理組織で管理することから生じる管理の負荷の大きさである。アクセス制御は Layer3 スイッチや Firewall などのネットワーク機器において Access Control List (ACL) を設定することにより実現する。記述の仕方はネットワーク機器に依存する。表 2 は Alcatel Lucent 社の ACL の例である [5, 6]。表 2 の記述が組織毎にあり、記述量が増

```
policy network group EK 133.38.212.0 mask 255.255.252.0
133.38.211.0 mask 255.255.255.192
policy network group EKT 133.38.209.0 mask 255.255.255.192
policy condition cEK source network group EKT destination network group EK
policy action OK
policy rule rEK precedence 10 condition cEK action OK
```

表 2: OmniSwitch における ACL の例

えれば各組織の記述の間で整合性のチェックが大きな負荷となる。それ以上にチェック自体が現実的な時間で行えるかどうかという問題も起きる。また、ある組織でアクセス制御のポリシーを変

更する場合、例えば、組織内に新しいネットワークを追加する、通信できる範囲を広げたり狭くしたりする、サーバを新規に設置するなどによりアクセス制御のポリシーを変更する場合、ACL を変更する必要がある。この変更は、他の組織の ACL へ影響が及ばないように行われる必要がある。このときの変更には、ACL に規則を追加する、ACL の規則の一部を削除する、一から書き直すなどのいくつかの選択肢がある。さらに、どのように追加、削除、書き直しを行うかにも選択の余地がある。しかし、ポリシーの変更に伴う ACL の変更は局所的な場合が多く、ACL へポリシーの変更を反映させるには ACL へ規則を追加する方法を取ることが多い。この方法は、誤った作業を行ったとしても、ACL の変更部分が変更していない部分へ影響を及ぼす可能性を低く抑えることもできる。

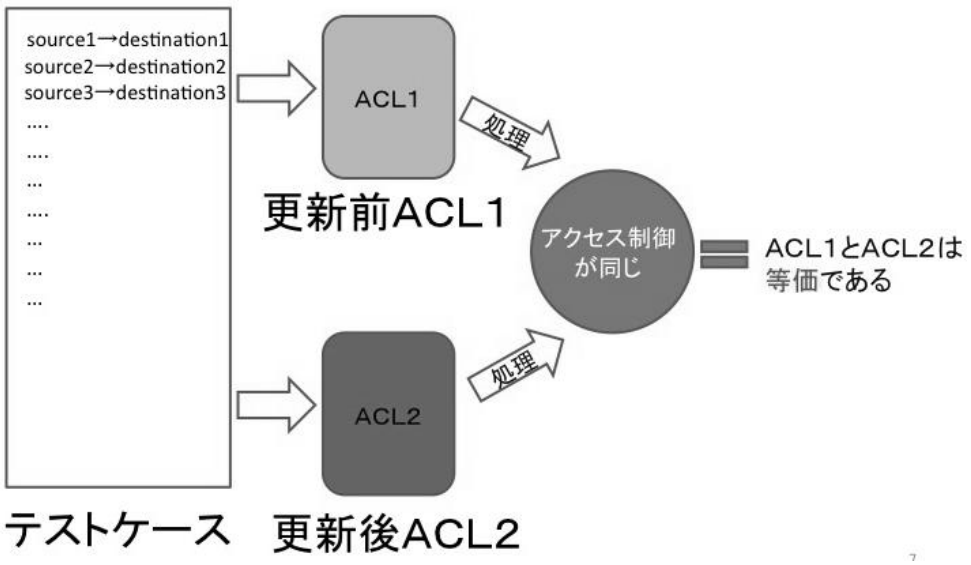


図 1: 等価性の判定

3.3 ACL の書き直し

ポリシーの変更の度に ACL へ規則の追加を行うと、ACL 全体では冗長な記述が増えていく。このことは ACL の可読性の低下させるとともに、ACL の処理の非効率化を招く。特に、処理速度の低下は利用者にとって重大な問題となるとともに、必要がないにも関わらず限界まで ACL の設定を行う可能性も生じる。ネットワーク機器では ACL の設定に上限が設けられており、同じアクセス制御を行う場合でも、より短い設定の ACL の方が処理速度や消費電力が少なく済む。さらに、設定の追加も容易になる。

よって、冗長な記述のある ACL を冗長な記述のない ACL に修正することは ACL の管理において重要である。ACL の修正は管理者が行うことになるが、修正前後の ACL の意味が変化していないこと、つまり、修正前後の ACL でアクセス制御が変化していないことが必須になる。この変化していないこと、つまり等価であることを判定するには、いくつかの方法が考えられる。例えば、ACL の記述をモデル化してそのモデルの等価性を調べる方法などが考えられる。しかし、ACL の最適化は NP-complete であることから [3]、モデル化などによる方法は計算時間を考えると現実的ではないと考えられる。

そこで、筆者は ACL の等価性を確認するためのテスト用のパケットを生成し、実際に ACL が設定されているネットワーク機器にそのパケットを送信し、そのパケットの通過や不通過を確認することで 2 つの ACL の等価性を判定する方法を提案している [4]。この方法では、実際にパケッ

トを送信し確認する作業が現実的な時間に収まる個数のテストパケットを生成する方法を提案している。次章ではこの等価性の判定方法について述べる。

4　テストパケットによる等価性判定

図 1 は本稿で説明する ACL の等価性判定の方法を示している。テストパケットは送信元 IP アドレスと送信先 IP アドレスの組である。ここでは、アドレス資源を 32 ビットで管理している IPv4 の環境下を想定しているので、送信元 IP アドレス、送信先 IP アドレスは各々最大 2^{32} 通りになる。つまり、互いを組み合わせた 2^{64} 通りのテストパケットが最大数のテストパケットとなる。しかし、このように莫大なテストパケットでは等価性判定時間が大きく、等価性を現実的な時間で収めることは出来ない。故に、2^{64} 個のテストパケットから、利用せずに済む無駄なテストパケットを出来る限り削除し、処理効率をあげることが目的達成には必要不可欠となる。そこで、[4] では ACL を構成する規則に出現する送信元 IP アドレスと送信先 IP アドレスに着目しテストパケットを少なくする。なお、[4] の方法で作成されたテストパケットについて 2 つの ACL での通過不通過が一致すれば、2 つの ACL で任意の IP パケットの通過不通過が一致する。

次に、ACL で設定されている送信元 IP アドレスと送信先 IP アドレスを利用したテストパケット生成を説明する。表 3 にある送信元 IP アドレスと送信先 IP アドレスが ACL の規則において利用されているものとする。これらの送信元 IP アドレスと送信先 IP アドレスの組み合わせの IP パケットが通過、不通過いずれであってもよい。

133.38.0.0/22→133.38.16.0/22
133.38.192.0/24→133.38.128.0/27

表 3: ACL の送信元 IP アドレスと送信先 IP アドレスの例

[4] では、表 3 から送信元 IP アドレスと送信先 IP アドレスによる 2 次元の空間を考え、各アドレスの境界とその中間点を組み合わせた送信元 IP アドレスと送信先 IP アドレスの組をテストパケットとして利用する。図 2 は表 3 からテストパケットとなる地点を示したものである。図 2 にある交点にあたる部分が全てテストパケットとして利用される。

4.1　実験

[4] では実際に 2 つの ACL からテストパケットを生成するプログラムを作成した。さらに実験として、埼玉大学で用いられている ACL とそれを修正した ACL の 2 つの ACL を入力し、実際にテストパケットを生成した。この実験で実際に使用する ACL の特徴を表 4 に示す。この実験をした環境の PC 性能を以下の表 5 に示す。実際に作成されたテストパケットの個数は 160446 であった。

	ACL1	ACL2
Maximun number of policy rules	103	176
Maximun number of policy conditions	103	176
Maximun number of policy actions	2	2
Maximun number of policy service	13	13
Maximun number of policy groups(network、MAC、service、port)	181	271

表 4: 実験で用いる ACL

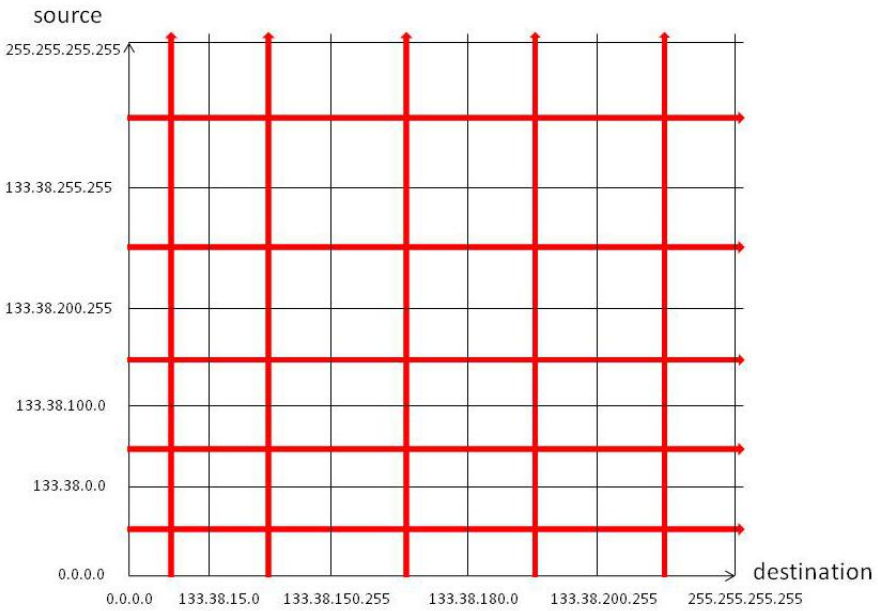


図 2: テストパケットの生成

OS	Windows Vista 32bit 版
CPU	Intel(R)Core2 Duo 2.40Ghz
メモリ	2.00GB

表 5: 実験環境

生成されたテストパケットの個数からネットワーク機器においてテストパケットの処理に必要な時間が予想できる。想定環境は 1Gbps ギガビットイーサネットを用い、ネットワーク機器が理論上の最高転送速度となるワイヤースピードで動作すると仮定する。ネットワーク機器のパケット処理速度は、スイッチが 1 秒間に処理することができるフレームの「数」を表す pps(packet per second) により表される。1Gbps のワイヤスピードの性能を有するネットワーク機器ではパケット処理速度は 1488100pps となる。1 パケットがひとつのテストパケットに対応することを考慮し、等価性判定処理の予想時間すると約 0.10781 秒となる。

4.2 問題点

予想時間は理論上の値であり、実際にこの仕組みを利用した等価性の判定にはより多くの時間がかかると推測される。仮にこの 1000 倍だとしても 100 秒程度なので現実的な時間に収まっている。生成されるテストパケットの個数次第であるが、ネットワーク機器の処理速度が高速になっていることから、等価性の判定を [4] の方法で行うことは現実的である。ただし、テストパケットをより少なくする方法を検討することは重要である。

しかし、[4] の方法を実際に利用するためには、2 つの ACL それぞれをネットワーク機器に設定した上でテストパケットの通過不通過を調べる必要があるが、いくつかの問題点がある。第一に、ネットワーク機器でのテストパケットの通過不通過を、サービスを提供したままで調べるのか、サービスの提供を停止して調べるのかという問題がある。第二に、ポート数が多数のネットワーク機器で ACL の等価性を判定する場合、多数のポートのいずれかをテストパケットが通過す

るため、これらのポート全てを、テストパケットの通過不通過を判定する機器に接続する必要がある。つまり、判定する機器は多数のポートを収容する必要がある。第三に、ネットワーク機器の特定のポートだけに設定された ACL がある場合には、各ポートのテストパケットの通過不通過を調べる必要がある。つまり、通過不通過を判定する機器はネットワーク機器のポート毎のテストパケットの通過不通過まで確認する必要がある。

このように実際に [4] の方法を利用するためには解決すべき問題があり、実際にこれらの問題を解決するのは容易ではない。これらの問題を解決するのであれば、ネットワーク機器の動作をシュミレーションするソフトウェアを作り、実際にこのソフトウェア上でテストパケットの通過不通過をテストすべきかもしれない。しかし、この場合、ネットワーク機器に応じてシミュレーションソフトウェアを作らなければならないという問題がある。

5 おわりに

本稿では、大学の情報系センターが行うネットワーク管理における特徴を述べることで、他組織のネットワーク管理とは異なることや、大学のネットワーク管理の難しさを示した。さらに、その 1 つとしてアクセス制御の管理における問題点と、解決方法について議論した。本稿の後半で述べているアクセス制御、つまり、ACL の管理も大学のネットワーク管理固有の問題である。これを解決するための 1 つの方法は、各組織のネットワーク毎に Firewall を設置することである。しかし、コストがかかるなどの理由から Firewall の設置が難しい、仮に設置できたとしても各組織では Firewall の運用ができないなどの問題が想定される。

大学のネットワーク管理は、各組織の裁量が大きいが管理はセンターが行うという、利用者には都合がよく、管理者には重労働となりうる状況にある。しかし、見方を変えると、利用者が自由に利用できるが管理しなくてもよいという、ネットワーク管理の理想的な形なのかもしれない。しかし、現状では改善が必要であり、各組織の裁量を少なくし、センターの管理運用コストを低下させるのか、それとも、管理運用技術を改良し、各組織の裁量を今のままとして、センターの管理運用コストを低下させるのかを、検討する必要がある。現状の大学のネットワーク管理を取り巻く状況では、前者の方針を取らざるを得ないであろう。

参考文献

[1] Dominique Alessandri: ”Access Control List Processing in Hardware”,Diploma Thesis,Zurich,Switzerland:ETH,Electrical Engineering Department (1997).

[2] Shingo Ata,Haesung Hwang,Koji Yamamoto,Kazunari Inoue,Masayuki Murata: ”Managment of Routing Table in TCAM for Reducing Cost and Power Consumption”, IEICE technical report.information networks (2007).

[3] Vic Gront, John McGinn, John Davies. ”Real-time optimisatoin of access control lists for efficient Internet packet filtering”, J Heuristics (2007)

[4] 吉浦 紀晃, 佐山 弘和: ”Access Control List の等価性判定のためのテストケース生成”, 研究報告インターネットと運用技術（IOT）2012-IOT-16, No.53, pp.1–6 (2012).

[5] Alcatel-Lucent:http://www.alcatel-lucent.com/wps/potal/

[6] Alcatel: ”OmniSwitch 7700/7800 OmniSwitch 8800 Network Configuration Guide”, (2005).

FTTL の運用と今後の課題
－次期システム調達に向けて－

埼玉大学情報メディア基盤センター
専門技術員　小川康一

1. まえがき

本学では 2007 年度に全学規模のネットワーク整備を行うにあたって、FTTL（Fiber To The Laboratory）と称して全学に光ファイバをはりめぐらせ、学内 44 棟・約 1800 か所にも及ぶ大規模な光ネットワークを構築した（図 1　FTTL ネットワーク構成）。本稿では本年調達する次期ネットワークを検討するにあたり、数年間の導入効果と反省を踏まえ今後のシステムの方向性を検証したい。

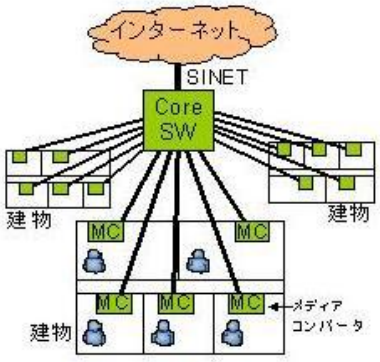


図 1　FTTL ネットワーク構成

2. FTTL を導入して

2.1　ネットワーク移行問題

本学のネットワークでは主に認証 VLAN を採用し、セキュリティが高いネットワークを目指した。現在も認証 VLAN では基本形として各部局の VLAN は機能・性質ごとに分かれており、各 VLAN 間の通信について許可・制限をしている（図 2　現在の VLAN 構成（基本形））。しかし、この VLAN 構成が便利である半面、不都合が生じることもあった。基本形そのままでは利用形態にそぐわない部分があり、ネットワーク移行時に通信ポリシー設定の見直しが多かった。

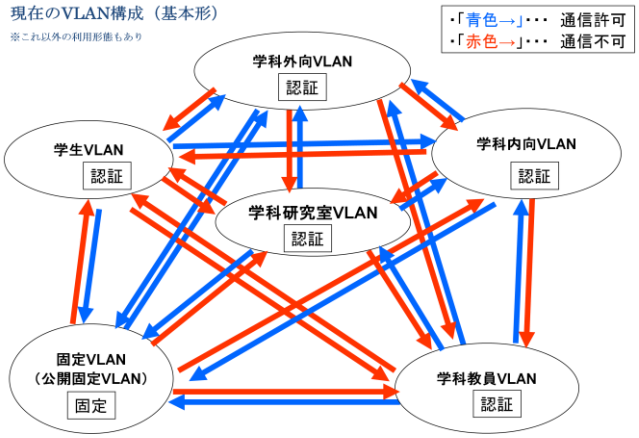


図 2　現在の VLAN 構成（基本形）

特に認証 VLAN を利用する上での難点は「ネットワークプリンタ」などの非認証端末の存在である。この場合、スイッチに対して「MAC アドレス認証」として MAC アドレス登録を行えば利用可能である。しかし実際にプリンタを利用できる VLAN をルールで定義するため、ACL などのポリシーを設定する作業が発生するなど複雑な事案が多く発生することとなった。

2.2　認証 VLAN の導入効果

導入してみて判明したことは、当初予想したより認証 VLAN の利点を生かした利用形態が存在しなかったことである。本学の認証 VLAN はダイナミック VLAN 割当方式により場所を移動してもいつでも同じネットワークを利用できることが利便性であると考えていたが、その恩恵にあずかる利用者はごく少数であった。もちろんネットワークセキュリティを考える上で、不特定多数が出入りする箇所では、必ず認証プロセスが介在するため、セキュリティリスク回避に役立っていると考えている。

2.3 不具合の発生

ネットワークが安定稼働するまでのいくつかの不具合があった。もっとも多かったのが認証 VLAN での不具合である。

１つは Web 認証で利用するブラウザで稼働する Java アプレットの問題である。利用者の環境により認証が成功せず、認証画面そのものが表示できないなどの不具合が続発した。これは Java ランタイムのバージョンにより発生するものである。現在最新の Java ランタイムを利用すれば特に問題となることはない。また、現在は Windows7 への対応を受けて Java ランタイムを利用しない方法（DHCP サーバのリースタイムの調整による）を用いて機能を実現している。

2 つ目はコアスイッチの認証 VLAN における「バッファ枯渇」問題である。当初は認証 VLAN での利用を推進したため、多くのユーザが同時に認証を行うケースがあった。このため、ネットワーク機器で認証に利用しているリソースを食いつぶした。現在はベンダーによる対応で枯渇を未然に防ぐ仕組みを導入し、問題が発生することはなくなっている。

2.4 VLAN 数の推移と今後の方針

近年実施している建物の耐震改修工事に伴う、光ファイバケーブルの再配線によりネットワークの設定についても見直すこととなった。教員の居室で入退室する人物が特定でき、責任の所在が明確化している場合には、固定 VLAN を割振ることが多くなってきた。

2010 年 2 月現在での VLAN 数は、認証 VLAN は 151 個、固定 VLAN は 358 個（管理用 VLAN17 個を含む）となっている。今後は影響などを考慮しながら、教員の居室は固定 VLAN 化を進めることになるだろう。ただし、認証 VLAN については当面現状を維持しながら、学科や部局の増加を見ながら緩やかに推移すると予想している。ユーザに影響の少ない方法での利用環境の提供が必要となるだろう。

3. ネットワーク管理

3.1 電子データによる申請管理

認証 VLAN では非認証端末への対応が必要な場合には MAC アドレスをネットワーク機器に登録する「MAC アドレス認証」という方式で対応している。

ネットワーク管理者の教職員が取り纏めを行い、電子データによる申請を行っている。理由の一つは MAC アドレス自体の転記ミスによるトラブルを防止するためである。もう一つは動作確認など管理者の手が必要になる点である。IP アドレスの割当など、各部局に沿った対応が必要となるケースが多く、管理者の対応が不可欠となる。

今後もこのような対応は認証 VLAN を運用する上で続けていく必要がある。MAC アドレス登録自体を簡易的に半自動化するシステムを導入し、運用している大学もある。本学でも今後少数で管理していくにはなんらかの管理ツールが必要となるだろう。

3.2 光コンセントの管理

本学の FTTL では「光コンセント番号」という 9 桁の番号で各部屋を管理している（写真１　光コンセント番号）。この番号と実際のネットワーク機器のポート、どのような VLAN を利用しているかの対応を把握することが重要となる。そこでは私は PHP による Web アプリケーションとして「VLAN 管理システム」（図 3 光コンセント番号検索の画面）を開発した。このシステムでは光コンセント番号をプルダウンで選択して当該の箇所の機器と VLAN を確認することができる。まだ機能面で不足があるため、今後折を見てブラッシュアップしたいと考えている。

写真 1　光コンセント番号

図 3　光コンセント番号検索の画面

4. 今後の課題

4.1　機器間をまたがる VLAN の構成

本学では棟をまたいで利用する形態がある。このため、複数のネットワーク機器で同じで VLAN を構成することになる。今後、人事異動や新規プロジェクトの創設などにより構成変更が発生することを考慮すると、柔軟に VLAN の構成を変更できることが望ましい。そのためには各機器で VLAN 数を十分に確保しておく必要がある。

4.2　ループ検知機能の搭載

ループとはイーサネットスイッチから出たケーブルを同スイッチの別のポートに接続し、「輪」のようにつないでしまうことである。これを行うと通常のイーサネットスイッチではネットワークの情報が循環してしまい、正常な通信を行うことが不可能となってしまう。現在のインテリジェントなイーサネットスイッチではループ検知機能を有することが多くなっている。もちろん、単体のスイッチだけでなく、スイッチ間をまたいだループについても検知が可能となってきている。

4.3　仮想化への対応

近年急速に採用が始まっている「仮想化」についても、ネットワークからの側面からの対応が必要である。サーバの仮想化により増大するトラフィックを効率的にさばけるかが重要となる。また仮想化にあわせたネットワーク運用も今後の課題となる。ただ単にバーチャルマシンを提供するだけでは実際の利用に耐えない。アクセスコントロールなどを柔軟に制御できるインタフェースを提供する必要があるだろう。

5. まとめ

今回の考察では現システムでの VLAN 利用を中心に現在に至る推移と対処について考察をした。これまでの運用での反省を踏まえ、今後は以下のような視点が重要と考えている。

- メーカとの強力な保守サポート体制
- ユーザ負担の少ない利用方法の提示
- スムーズな移行方法の検討
- センターの迅速な受入体制
- グリーン IT に向けての省エネルギー化
- コストの削減

今年は次期システムの調達にかかる重要な年である。ネットワーク機器はなるべく管理者にとっても安心できるものにしたいと個人的に考えている。現システム運用の反省を踏まえ、ユーザにとってより使い勝手の良いシステムを導入できるよう努力していきたい。

なお、この場をお借りして普段より当センターの運営にご理解をいただき、ネットワーク移行に多大なるご尽力をいただいた各学部の先生方、面倒な移行作業などにご協力をいただいた職員の皆様方に心より感謝を申し上げたい。

参考資料・引用文献

1) 伊藤和人、田邊俊治、小川康一、吉浦紀晃、重原孝臣、前川仁,"埼玉大学 FTTL の構築",学術情報処理研究 No11 2007,pp. 124-128,2007

2) 前川仁,"埼玉大学の次世代情報基盤の構築",埼玉大学情報メディア基盤センター年報 Vol.15 pp.2-9,2007.3

3) 伊藤和人,"新基幹ネットワークついて",埼玉大学情報メディア基盤センター年報 Vol.15 pp10-12,2007.3

4) 田邊俊治、小川康一、吉浦紀晃、伊藤和人、重原孝臣、前川仁,"光直収ネットワークによるキャンパスネットワークの管理運用"
埼玉大学情報メディア基盤センター年報 Vol.17 pp.2-9,2009.3

(平成 23 年 4 月記)

埼玉大学の情報セキュリティ対策について

埼玉大学
情報メディア基盤センター
研究協力部 情報基盤課(併)
齋藤　広宣

情報セキュリティに関する動向(1)

- 文部科学省
  - 学校における個人情報の持出し等による漏えい等の防止について(通知)　(H18.4.21)
    - 特に、下の3点への対策を示唆
    - ①個人情報等の持出し
      - 電子メールによる情報送信にも、注意を要する。
    - ②学校外で利用するパソコンのセキュリティー
      - 学校内のパソコンのセキュリティ対策も、当然に必要。
    - ③ファイル交換ソフト(Winny等)
      - 安易にインストールしないこと、など。
    - 参考URL：http://www.mext.go.jp/b_menu/koukai/kojin/info.htm

最近の情報セキュリティ事故事例

- 北海道教育大学　教員個人ホームページから個人情報流出(2010/04/21発表)
- 日本大学　ファイル共有ソフトで個人情報含む内部情報流出(2010/04/28発表)
- 島根大法科大学院、学生50人の成績が流出　職員がメール誤送信(2010/06/15報道)
- 群馬大　学生情報が保存された外付ハードディスクを紛失(2010/06/23発表)
- 川村学園女子大学　学生の個人情報を記録したハードディスクを教員が紛失(2010/06/20発表)

最近の情報セキュリティ事故事例（続）

- 昭和大学　患者情報が記録されたUSBフラッシュメモリー紛失(2010/06/25発生)
- 徳島大　教授がHPに学生情報掲載 8年間分667人(2010/07/07発表)
- 福島県立医大　教員が個人情報含むPC盗難被害(2010/08/11発表)
- 広島大学　834名分の個人情報含むUSBフラッシュメモリ紛失(2010/09/14発表)
- 立教大　学生情報が保存されたパソコンを紛失(2010/09/24発表)

※コンピュータ関連の事故が、特に目立つ

情報セキュリティに関する動向(2)

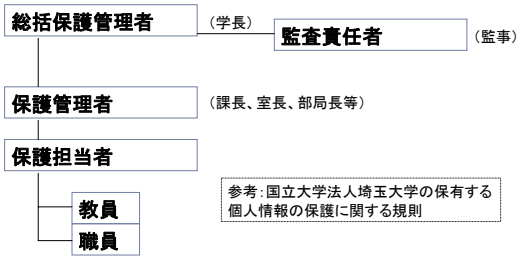
- 情報セキュリティ政策会議(政府)
  - 第1次情報セキュリティ基本計画('06～'08年)
    - 政策推進の枠組み構築
    - 事前対策の取り組み
  - 第2次情報セキュリティ基本計画('09～'11年)
    - 事前対策は当然に実施
    - 事後対応・復旧を冷静かつ迅速に推進

事故の防止
無謬性

事故の頻発
新しいセキュリティ脅威

「事故前提社会」
対応・復旧への準備
にも注力

埼玉大学の情報管理体制



保護しなければいけない情報とは

- 個人情報
  - 個人のプライバシーにかかわる情報
    - 学生・受験生・教職員の住所・氏名・生年月日、成績・健康状態ほか
    - 統一認証アカウント情報（ID・パスワード）
- 内部情報
  - 他組織に知られてはならない情報
    - 研究計画・実験データ・メモ・会話など
    - 業務上の成果物・中間成果物・マニュアル・メモ・会話など
- 共有情報
  - 外部委託先、府省庁等との共有情報
    - 担当者の氏名・役職・メールアドレス・電話番号など
    - 関係先より提供される機密情報

情報はどう保護すればいいのか

ケース・バイ・ケース

組織ごとに、適切に決める

◎関係法令
◎学内規則
◎組織の特性
◎関係先との契約
◎リスク評価

情報の重要度
利用する人・組織
利用期間
保管媒体
保管期間
保管方法
移送方法
変更管理

業務マニュアル
業務ルール

定期的な
評価・見直しも
大切

ヒューマンエラー対策

- セキュリティ事故の原因の80%は「人的ミス・エラー」
  - 管理ミス・誤操作・紛失
  - 「不正行為（内部・外部）」の割合は、案外少ない
- ヒューマンエラーに、どのように対策するか？
  - 担当者へのオペレーション教育
  - ヒューマンエラーを減らす手順や体制の整備
  - データの暗号化など、事故時の被害拡大防止策

情報システムによる対策が効果を上げる余地は、大きくない

情報システム・電磁記録情報の保護

- 「情報倫理及び情報セキュリティに関する規則」
  - 「情報倫理運用規準」
  - 「情報セキュリティポリシー」

コンピュータを使った情報利用にあたり、不適切行為の防止と、情報の改ざん、破壊、漏洩等から保護する管理策

- 情報セキュリティマネジメント体制

最高情報セキュリティ責任者（総合情報基盤機構長）
総合情報基盤機構会議
情報メディア基盤センター

コンピュータウィルス対策の例

- リスク・・・ パソコンのデータが破壊される / パソコンが使用不能になる / 情報が外部に流出する / 学内・関係先にウィルスをばらまく / 不正アクセスの足がかりにされる
- 対策

・ウィルス対策ソフトを使用する
・定期的にOS等のアップデートを行う
※「情報倫理運用規準」の遵守項目
リスク低減

・パソコンをネットワークにつながない
・パソコンで機密情報を扱わない・保存しない
・USBメモリ等の外部メディアを接続しない
リスク回避

・組織として、リスクの存在を飲む
リスク受容

※いずれの対策でも、何らかの「コスト」が必ずかかる。

パスワードの保管

- 全学統一認証アカウント
  - IDは「カード」、パスワードは「暗証番号」

IDとパスワードを書いた紙を、見やすいところに貼っている

IDとパスワードは記憶して、通知書はシュレッダーで破棄

パスワードだけをメモして、カギをかけて引き出しに保管する

ソフトウェアライセンス管理

- ソフトウェアライセンス（使用許諾）条件
  - 台数／使用人数
  - 個人向け／アカデミック／企業向け
  - 利用期間　etc.
- リスク・・・ ライセンス使用数がわからなくなる　期限切れによる機能停止　ライセンス違反による訴訟リスク
  - ⇒ **多額の賠償金につながる場合も**
- 対策・・・ ・ライセンス形態に合わせた管理表・管理ルールの策定 ・ライセンス管理ソリューションの利用

★賠償事例

法律受験予備校LEC（2001年）
Adobe社、MS社、Apple社ソフトウェアの不正コピー545本
賠償総額 約8472万円

その他のセキュリティ対策

- P2Pソフト（Winny等）をインストールしない
  - 情報漏洩の可能性
  - 違法行為につながる可能性（著作権侵害等）
- 情報の外部持ち出し時には、十分に注意する
  - パソコン・USBメモリの盗難・紛失
    - ディスクの暗号化で、ある程度対処可能
  - 電子メールの誤送信
    - 送信前に、よく確認
    - 複数人でのチェック（ダブルチェック）も有効
- 安易にサーバを設置しない
  - 管理不十分による不正侵入
  - 設定ミスによる情報漏えい

まとめ

- 情報セキュリティの確保には組織での取り組みが必要
  - 情報や組織の特性を考慮して、対策を行う。
  - 特にヒューマンエラーへの対策は不可欠。
  - 一方で、「事故前提」の考えのもと、発生時の対応にも準備しておく。
- コンピュータで情報を扱う際は、規則・ポリシーを守る
  - パソコンには必ずウィルス対策ソフトを使用する。
  - パスワードを適切に保管する。
  - ソフトウェアはライセンス違反をしないよう適切に管理する。
  - P2Pソフトをインストールしない。