さいたま

埼玉大学情報メディア基盤センター年報

VOL.18　2010　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。

センターから

「雲」をつかむような話

情報メディア基盤センター長　吉田 紀彦

この1年の間にIT業界で最も流行った言葉は、おそらく「クラウド」（Cloud Computing）と「つぶやき」（Twitter）であろう。では、「クラウド」、つまり「雲」とは何なのか。「どこでもネットワーク」な社会に向けての一つの大きな動きではあるが、実は、その定義は明確ではない。

「Cloud Computing」の語を最初に使ったのは、2006年にGoogle社のCEOが、というのが定説になっている。なお、「クラウド」というのは、IT業界では元々インターネットのイメージ図を、具体的通信経路を捨象する意味でモヤモヤした雲の形で描くので、そこから来ている。旧来は利用者が必要とするソフトウェアやデータを自分のコンピュータ上に置いていたのに対して、「クラウド」ではそれらをインターネット上のどこかに置いて、利用者はブラウザなど最低限だけを用意すればいい、というのが大かたの共通認識だろう。その背景に、高速大容量ネットワークの普及、そして分散計算技術の飛躍的進歩があるのは、間違いない。

しかしながら、ネットワーク上にソフトウェアやデータを分散させるという考え方そのものは少しも新しいものではなく、すでに1960年代から活用されてきている。考えようによっては、当時主流であった「大型計算機＋端末群」というコンピュータ構成が、現代のインターネットという基盤の上に「クラウド」として蘇ったと言えなくもない。現実にプロバイダが「クラウド」と称して提供しているサービスは、サーバ上の単なるディスク領域、データセンター、遠隔実行できるソフトウェア、利用者が自分の必要なソフトウェアをサーバ上で実行するための環境など、ピンからキリまで千差万別である。ただ、最先端の技術では、例えば別々のプロバイダが提供する複数のソフトウェアパーツをネットワーク上で一つに統合して単体サービスに見せることなどまで可能だが、いわゆる「クラウド」でそれが前面に出てくることはない。

このような現状を見ると、極端な言いかたをすれば言葉だけの独り歩き、特に企業や組織に向けて商用プロバイダが展開しようとしている「クラウド」とは、企業や組織が必要とする様々な業務・様々なサービスについて、ホスティングやアウトソーシングを一括してそのプロバイダに囲い込もうとするビジネス、と言い切ってもいいくらいに感じられる。「クラウド」で主張されている利点はコスト削減と管理効率化にあり、それには疑問の余地はない。しかし一方で、企業や組織の機密情報を外部に置いてネットワーク利用することのセキュリティ的な問題、信頼性の問題、企業や組織ごとの独自カスタマイズが極めて難しい問題など、慎重に考慮しなければならない要素も多々内包している。

「アカデミック・クラウド」と称する教育機関向けのサービスが登場したり、学内情報基盤システムを全面的に「クラウド」化する大学が現れてきた中、情報メディア基盤センターでも、業界全体の動向や他大学の動きなどを逐一チェックしつつ、注意深く分析と検討を進めている。月並みな言いかたになるが、「適材適所」「臨機応変」な利用が肝心であろう。それを通じて、学内の教育・研究・業務の情報サービス基盤をより充実させていきたいと考えている。

埼玉大学の各種ホスティングサービスの紹介

田邊 俊治*[1]，小川 康一*[1]，齋藤 広宣*[1]

*[1] 埼玉大学情報メディア基盤センター

Abstract

埼玉大学情報メディア基盤センターでは､Web ホスティングを初めとした各種ホスティングサービスを提供している。利用者の利便性が向上し、またセンターの稼働率上昇にもつながる一方で、利用者の増加に伴って性能上、また運用上の課題も出てきている。本稿ではその課題を整理し、また今後の展望についても言及したい。

1. 経緯

埼玉大学は平成 19 年度の情報システム更新で FTTL(Fiber To The Laboratory)と認証 VLAN・事後検疫システムを導入した。大学で用いるサーバ・システムについては、旧来は各学部・部局にてサーバやセキュリティ機器を整備してきた経緯があったが､前述の各システムを導入する際の予備調査でサポートが終了している古いサーバ OS やファイアウォールが利用されていたり管理者がはっきりしないものが多く、各学部・部局の管理にまかせることは、セキュリティ的に不安もあった。そこで、十分な管理がされていないサーバに関して、情報システム更新にあわせてセンター管理下のホスティングサービスへの誘導を図った。

2. ホスティングサービスの種類と概要

2.1 Web ホスティング（利用数：約 150）

Linux サーバ上で Apache を動作させ、またユーザにディスク領域を割り当てている。URL はこのサーバに由来するものが割り当てられるが、ユーザが希望する独自のホスト名を利用することもできる。

2.2 DNS ホスティング（利用数：正引き 17 ゾーン、逆引き 110 ゾーン）

Infoblox アプライアンスを用いて提供している。ユーザはクラス C 未満の逆引き設定についても GUI によってそれぞれの DNS を設定することができる。

2.3 Mail ホスティング（利用数：11 ドメイン、490 アドレス）

Linux サーバ上で HDE controller を利用してサービスを提供している。本来はバーチャルドメインによる各種ホスティング機能を実現するソフトウェアであるが､各管理者がバーチャルドメイン内のユーザを管理するためにこのうちメール機能のみを利用している。

2.4 DB ホスティング（利用数： 4）

Web ホスティングの提供をしている中、CMS(Content Management System)を利用するために DB を使いたいという要望が出てきたため、DB ホスティングのサービスを行っている。Web ホスティングとは別の Linux サーバ上で MySQL と PostgreSQL をサービス提供している。

3. ホスティングサービスの現状について

サービス当初（情報システム更新時）からのユーザのほか、自前のサーバの老朽化やクラッキング被害のためにホスティングに移行してくるユーザもいて、利用数は増加してきている。また特に Web ホスティングは、研究成果の掲載や講義資料の配布の用途にも便利であるようで、個人や研究室という比較的小さな単位で利用されるケースも増えている。

DNS ホスティングや Mail ホスティングでは、学部・部局のサーバ管理者にあたる人がユーザであり、サービスの開始

や継続段階において大きな問題は起こっていない。一方 Web ホスティング・DB ホスティングの方はユーザの裾野が広がってきており、中には“CMS を使いたい、しかし CLI があまり使えない”という、スキルに不安のあるユーザも現れている。

4. サービス運営上の問題点

特に Web ホスティング・DB ホスティングのサービスにおいて、ユーザの性質や利用形態の変化などによって、いくつかの問題点が浮上してきている。

【サーバの負荷増大】…利用ユーザ数の増加に伴い、ユーザのディスク領域が不足するなどの弊害が出てきている。サーバの増強によって対処する予定である。

【利用用途の多様化】…ホームページ上で模擬講義をビデオ配信したり、自作のアプリケーションのデータ置き場として利用したり、研究室のファイルサーバとして利用したりなど、ユーザごとにさまざまな使い方をしている。一部の目的外使用に対しては、是正をお願いするレベルの対応しかとることができていない。

【容量制限に対するユーザの不満】…Web ホスティングでは、ユーザあたりの使用量を 500MB に制限しているが、これを増量してほしいとの要望も出ている。

【重要度の高いコンテンツの存在】…Web ホスティングには、大学本体のホームページから個人のものまでさまざまなレイヤーのものが増えてきて、監視や障害対応の優先度をつける必要が生じてきた。また、入学試験の合格発表をホームページ上で行っており、この時は特別な監視態勢をしく必要がある。

【サーバの監視】…サーバの死活監視（ping 監視）は行っているが、サーバが動いていてもホームページは見られないという事象が何度か発生している。今後はサービス監視も必要と考えられる。

【サーバソフトウェアのアップデート運用】…本 Web ホスティングでは Perl や PHP も使用できるようになっているが、これらのバージョンアップ要望が出てきている。しかし、文字コードの問題や現バージョンを前提に作られている Web アプリの存在などのため、アップデートのためには相当の準備と調整が必要と思われる。

5. 今後について

現状、各ホスティングサービスはそれぞれ 1 台のサーバのみで提供しているため、保守運用やサービスレベルなどがどうしても画一化されたものとなっている。当面の対策としては、サーバの増強を行うとともに仮想サーバの構築を行い、リソースの柔軟な利用を図りたいと考えている。また新たなサービスとして、ファイルサーバを提供することも思案しているところである。平成 24 年度からは次のシステムに更新となるので、このタイミングで監視運用機能やユーザの利便性を高めた新しいホスティングサービスを開始することを目指したいと考えている。

光ファイバケーブル接続技術の習得

－FTTL を支える光インフラメンテナンス手法の確立に向けて－

情報メディア基盤センター*　　技術部第２技術系**　　技術部第４技術系***
○小川康一*　　田邊俊治*　斎藤広宣*　原正史**　南雲浩二**　　佐藤甲輔***

※本寄稿は「第 20 回技術部研修発表会予稿集」の原稿をもとに加筆修正したものです。

1. まえがき

近年、IT 技術の向上とともにインターネットを用いた情報の伝達は目覚ましい発展を遂げている。ネットワークでやり取りする情報量の増加に伴い、より高速で大容量の帯域を必要とするようになった。

このような情勢を受け、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することとなった。

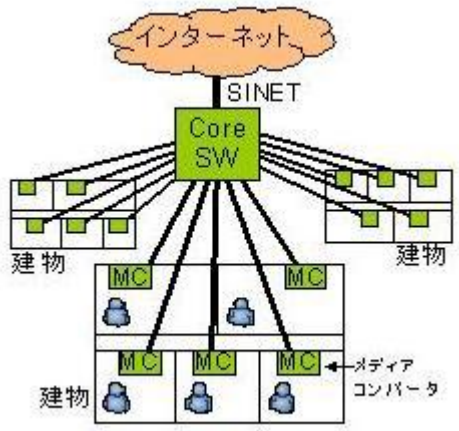

図１　FTTL ネットワーク構成

実際の配線としては、部屋にシングルモードファイバー2心、合計で約3600 心を配線、サーバ室側で48 ポートパネル(2U) を用いて42U ラック5 本のパッチパネルへと収容し、42U ラック6 本分の集合メディアコンバータ（１ユニット1.5U で16 台収容）に接続している。各光コンセントについては9 桁のコンセント番号を付与して管理をしている。

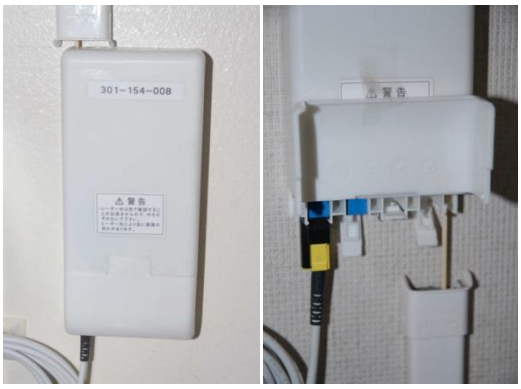

写真１ 本学光コンセントの例
（2 心のファイバが部屋まで来ている）

写真２ 光ファイバラック群

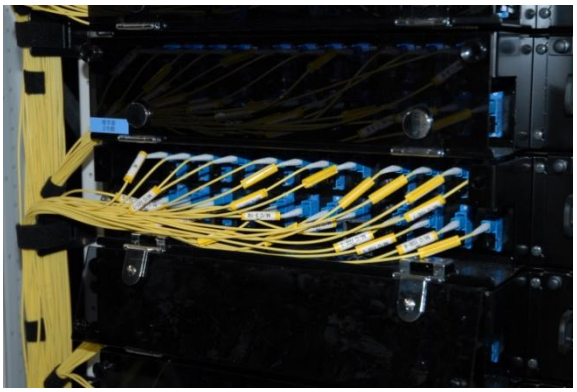

写真３ 光ファイバ収容トレイ

一般的なイーサネットLANケーブルの施工は使用する機器や部材も入手しやすく、比較的容易な施工方法で構築、メンテナンスが可能である。一方で光ファイバケーブルの取り扱いは専門知識が必要であり、かつハードルが高いものである。また光ファイバは今後10年程度、保守・運用、維持管理が必要である。また学内からの要望に応じて、今後も必要箇所への光配線の敷設が増加していくものと考えられる。

現在運用中のネットワークも開始から3年目を迎え、研究室での模様替えや引っ越しなどで光コンセントの設置箇所に物をぶつけたりして欠損するなどの事故や不具合が多くなってきた。

これらの背景をもとに光融着技術の必要性を感じ、研修テーマとして選ぶに至った。ここでは光融着講習を受講し、習得した技術について報告するとともに、今後の展開についても検討したい。

写真4 光融着講習会の様子（講習）

写真5　光融着講習会の様子（実習）

2. 光ファイバとは

光ファイバ（Optical Fiber）とは通信に使用されるケーブルの一種で、データを光信号に変換して伝送するケーブルのことである。データ伝送速度の速さ、一度に伝送できるデータ量の大きさ、共に非常に優れていることを最大の特徴とする。

光通信に利用されている光ファイバは基本的に屈折率のことなる2重のガラス層でできている（図2)。中央部のコア（core）は屈折率が大きく、外周部のクラッド（cladding）は屈折率が小さい。

光は、コアとクラッドの境界面で全反射を繰り返しながら伝搬する。クラッド部には光は通らない。

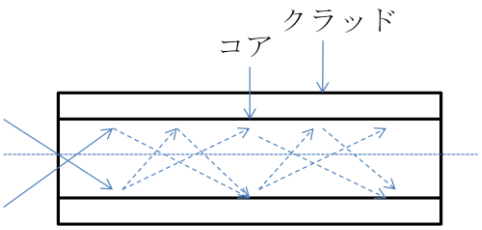

図2 マルチモード光ファイバの構造の例

光ファイバの材質は主に石英系ガラスが用いられているが、加工の容易さや安価な光素子が利用できることからプラスチック光ファイバの利用も増えてきている。講習会で講師に確認したところ、本学でも研究室などに施工されている部位ではプラスチック光ファイバが採用されている。

3. 光ファイバ融着接続

現在、光ファイバ通信網の建設において、光ファイバを接続する融着には代表的な3つの接続方法がある。講習会ではこれら3つの接続法について実習した。

3.1　融着接続

「光融着」の一般的な接続方法で、永久接続であり、一度接続すると脱着は不可能である。接続損失は小さく、無反射である。接続部の強度は大きく、長期信頼性も高い。融着

機と融着部を保護する補強スリーブが必須となる。

昨今は融着機の性能が向上し、融着そのものは自動化が行われており、操作自体は昔に比べて容易になった。融着作業の手順は図 3 の通りである。

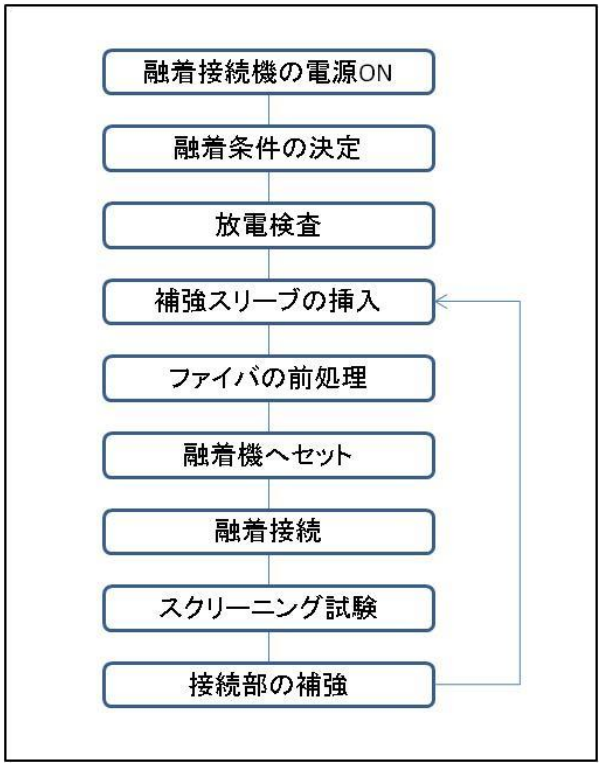

図 3　融着接続作業の手順

3.1.1 融着接続に必要な機器・部材

光ファイバの融着接続には以下のような機器・部材が必要である。

① 補強スリーブ
② ベンコット（塵が出にくい脱脂綿）
③ アルコール（純度 99.9%、工業用）
④ ファイバカッター
⑤ ストリッパー
⑥ 融着機

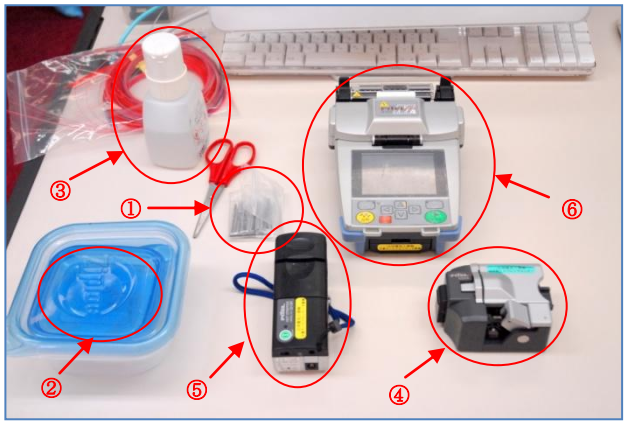

写真 6 融着接続に必要な機材・部材

3.1.2 接続前の準備段階の注意点

接続の準備段階の洗浄が十分でないとうまく融着ができない。このため洗浄は光ファイバの軸上に平行に脱脂綿を 3～4 回程度移動させて、「キュッ、キュッ」と音が出るくらいに拭く必要がある。ただしファイバ心線はガラスであるため、簡単に折れてしまうので取り扱いに注意が必要である。

写真 7 清掃後のテープ心線

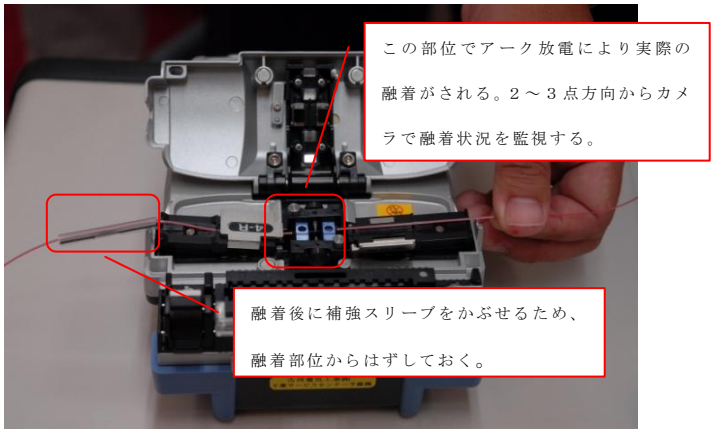

写真 8 融着直前のテープ心線の様子

3.1.3 補強スリーブについて

光ファイバの融着接続部は表面の被覆が全段階の作業で除去されているため、曲げなどに弱く、被覆除去時や融着機にセットした際に生じる表面傷、接続時に発生する熱歪み等によって引っ張り強度が約 1/10 に下がるといわれている。そこで接続部位を保護する目的で補強スリーブを用いることで光ファイバ表面の保護、機械的強度を持たせている。

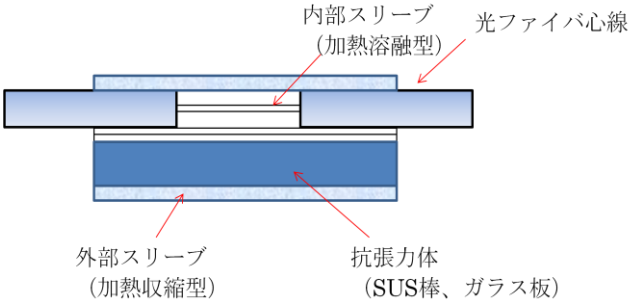

図 4　補強スリーブの内部構造

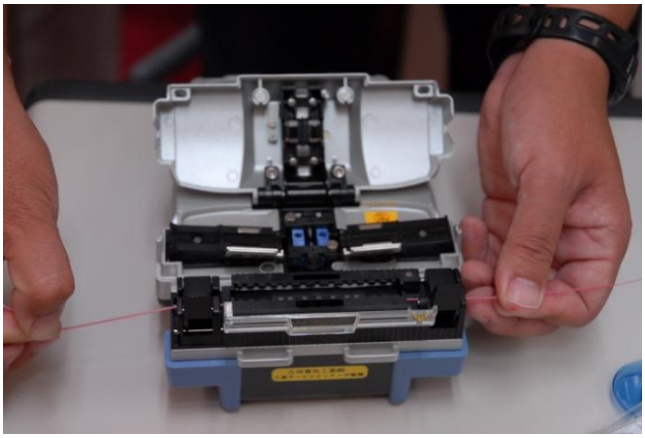

写真 9 補強スリーブの加熱収縮工程

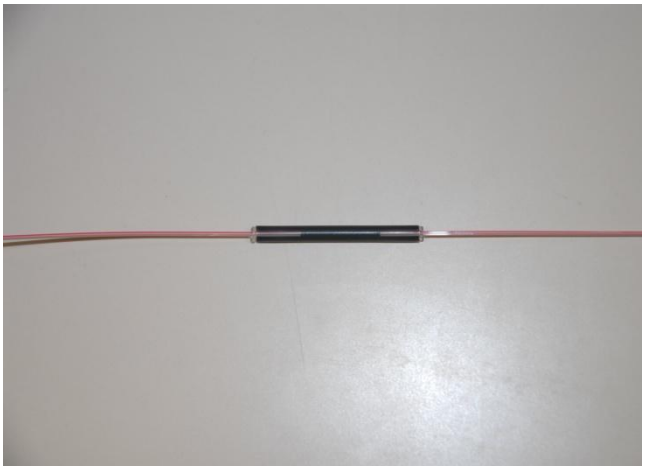

写真 10 加熱収縮後のファイバ

3.2 メカニカルスプライス

スプライスユニットに接続スリーブをセットし、ファイバを差し込んでクサビを食い込ませることで接続が完了する。特徴として接続損失は小さい。また、整合剤が内部に充填されており､ある程度の反射を軽減している。手動工具であるため、電源などは必要ない。ただし、接続スリーブの一つあたりの単価が高く、大量の場所を接続するのにはコスト高である。

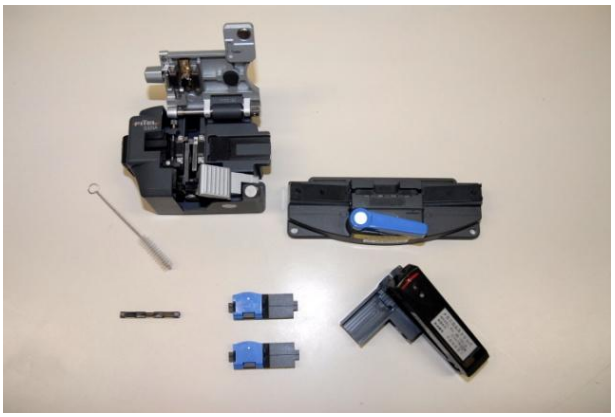

写真 11 メカニカルスプライス法の機材

写真 12 接続スリーブ

写真 13 メカニカルスプライスの施工

3.3　光コネクタ接続

講習では古河電工（㈱成和技研工業製品）の「かんたん SC コネクタ」と呼ばれる現場即席のキットを用いた。施工方法は容易で、ファイバを部材に差し込み、クサビ型の突起部をはめ込めば完成である。3.2 のメカニカルスプライスと同様に整合剤が内部に充填されており、反射を軽減している。

ただし、部材単価が高く大量の場所を施工するには不向きであると思われる。

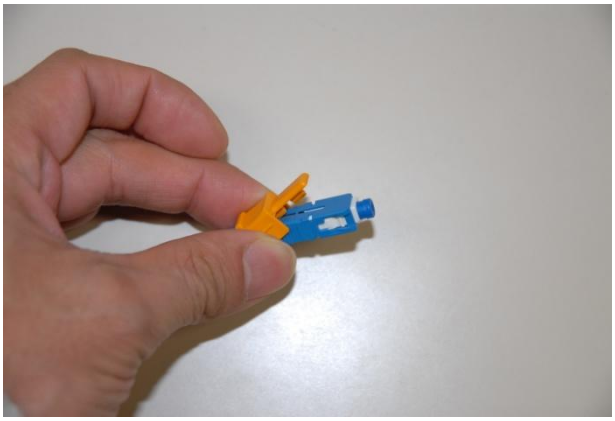

写真 14　かんたん SC コネクタの施工

3.4　融着時の注意点

補強スリーブを加熱収縮させるときに気泡等が混入すると、四季の温度変化により気泡内で光ファイバが収縮を起こし、最悪の場合には破断に至る。そのため補強スリーブの加熱収縮後はスリーブの全周を十分に検査する必要がある。

また、融着に利用するアーク放電の検査が必須である。これは環境条件（気温や湿度など）によって変化するので作業毎に確認が必要である。

今回講習で利用したテープ心線はファイバをねじったままで補強する危険性は少ない。補強後の目視による検査も容易であるが、単心線については捻れの有無の判別が困難であり、補強後は特に注意が必要である。

今回の講習でも実施したが、単心線の融着時には黒マジックで表面をマーキングして捻れを防ぐことが必要である。

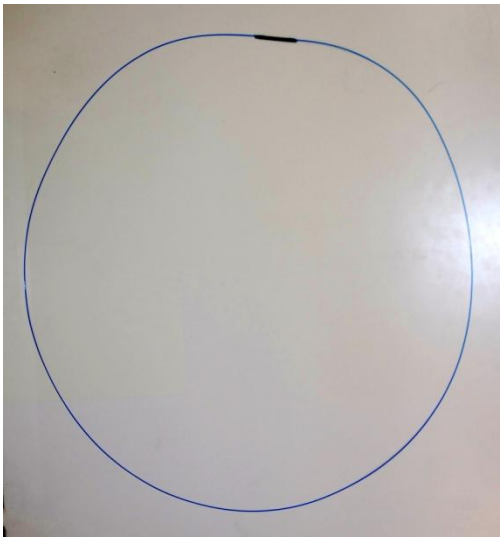

写真 15 正しい融着によるファイバ
（捻れのない融着のため、円を描く）

3.5 融着接続のまとめ

講習では代表的な３つの接続方法を習得することができた。メカニカルスプライスやコネクタなど比較的容易な接続方法も選択できるようになったが、総合的に判断した場合には融着接続が良いようである。

表 1　光ファイバ接続方法一覧

種類	タイプ	損失 [dB]	反射 [dB]	コスト（部材）
融着接続	永久	0.05～0.10	なし	数百円
メカニカルスプライス	永久	0.10	40～50	1000 円
コネクタ	簡易	0.50	40	2000 円

4.　まとめ

今回、技術部の研修と情報メディア基盤センターの理解を得て、基本的な融着技術を習得する機会に恵まれた。光を取り扱っていく上での注意点なども再度見直していきたい。光ネットワークは本学にとって今後もインフラを支える重要な基盤である。継続利用には保守メンテナンスが必要となる可能性がある。建物間で利用する集合ファイバケーブルについては施工が難しく、業者に任せる必要があるが、建物内での不具合や保守に関しては内

部で対応することできめ細やかな対応やコスト削減につながると考えている。

今回の講習後に保守メンテナンスにおいて実際に光融着を実施した実績は残念ながらない。しかし、今後大学内で管理体制を構築し、効率的な保守メンテナンスを実施できるよう進言していきたい。融着機の導入や付随設備の採用などの検討も模索しているが、高価であるため現状はレンタルによる利用が望ましいと考えている。

また、これまで情報メディア基盤センターでは光ネットワーク導入に伴い OTDR（Optical Time Domain Reflectometer）などの計測機器の導入についても尽力してきた。今回は融着技術が中心であったが、是非これらの計測器を用いた融着後の測定方法や不具合時の原因究明の方法についても理解を深めたいと考えている。

また、今後技術部はもちろんのこと、関連部局の担当者も含めた上で、融着技術の勉強会を実施し、融着技術の確認と知識の伝播を続けていきたい。

参考資料・引用文献

1) 光講習会テキスト（古河電気工業株式会社情報通信カンパニー光技術トレーニングセンター）

2) 光商品総合カタログ（古河電工、2009-A）

3) 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

4) 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

5) 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

6) 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

Access Control List に関する話

吉浦紀晃

情報メディア基盤センター

1　はじめに

インターネットが使われ始めたころから、ネットワークを介したサーバ等への攻撃はあった。攻撃に対する防御方法として最もシンプルであるが効果があるのはアクセス制御を行うことである。ここでいうアクセス制御とは、ネットワーク機器が、機器を通過する通信パケットの通信プロトコル、送信先や送信元 IP アドレス、送信先や送信元のポート番号等に基づき、そのパケットを通過させるか捨て去るかを行うことである。

このアクセス制御をどのように行うかをネットワーク機器に設定するときに利用されるのが、Access Control List (ACL) である。ACL は通信の許可不許可を決める規則であり、ネットワーク管理業務において重要なものの 1 つである。筆者はこれまで 3 つの大学において大学全体のネットワーク管理組織 (Network Operation Center) に携わってきたが、筆者のこれまで実際運用の体験に基づいて ACL の設定に関する話を書いていきたい。

アクセス制御には様々な方法が考えられると思うが、なぜ、ACL の設定の話を書こうとしたかというと、「アクセス制御を行うのは、Firewall 等の専用機器であり、Layer3 スイッチ等で設定することはない。また、一カ所で設定するものである。」という認識をシステムインテグレータ等の人々から度々聞くことが多かったからである。本稿で示すものが一般的かどうかは何とも確証がないが、これまで実際に運用してきた ACL の設定に関して示すこととする。

2　Access Control List とは

ACL とはどのようなものであるかを具体例を利用して説明する。図 1 は ACL の一例である。

ネットワーク機器にパケットが到着したときに、ネットワーク機器はそのパケットが、ACL に書かれているいずれかの規則に該当すれば、その規則に記述されている処理、つまり、通過させるか捨てされるかのいずれかの処理を行う。

```
1 deny ip from 192.168.0.0/16 to 133.38.202.224/28
2 allow tcp from 133.38.202.192/26 to 133.38.202.200 22
3 allow tcp from 133.38.202.200 22 to any
4 allow tcp from any to 133.38.202.200 80
5 allow ip from 133.38.202.192/26 to 133.38.202.192/26 53
6 allow ip from 133.38.202.192/26 53 to 133.38.202.192/26
7 deny tcp from any to 133.38.202.200 1-1023
8 deny udp from any to 133.38.202.200 1-1023
9 allow ip from any to 133.38.202.241
```

表 1: Access Control List (ACL)

図 1 の場合、パケットがネットワーク機器に到着後、最初の規則にパケットが該当するかどうか調べる。つまり、送信元 IP アドレスが 192.168.0.0/16 に該当するか、送信先 IP アドレスが 133.38.202.224/28 に該当するかを調べる。該当すれば、１番目の規則では、”deny”と書かれているためこのパケットは廃棄される。該当しなければ、次の規則を用いて同様の処理を行い、該当する規則が現れるまで ACL に書かれている規則を順次参照していく。また、該当する規則に”allow”と書かれていれば、パケットを通過させる。該当する規則が無い場合も想定し、パケットを破棄するか通過させるを予め決めておく。

アクセス制御を行うネットワーク機器では、全てのパケットに対してこの操作を行うため、パケットの数が多くなるとまた ACL の規則数が増えるとネットワーク機器の負荷が増加する。

ここで述べた処理手順は、ACL の基本的な処理方法であり、初期の頃のルータや Firewall、現在でも安価なルータや家庭用のブロードバンドルータで採用されている方法である。この方法は基本的にルータの farmware などのソフトウェアによって処理されるものである。

このような処理方法では大きなネットワークのアクセス制御を行うのは無理であり、大学等のネットワークのアクセス制御を行おうとすると処理能力に限界がある。そこで、大規模な Layer 3 スイッチや Firewall 専用器では図 1 に示すようにハードウェアにより ACL 処理を行っている。

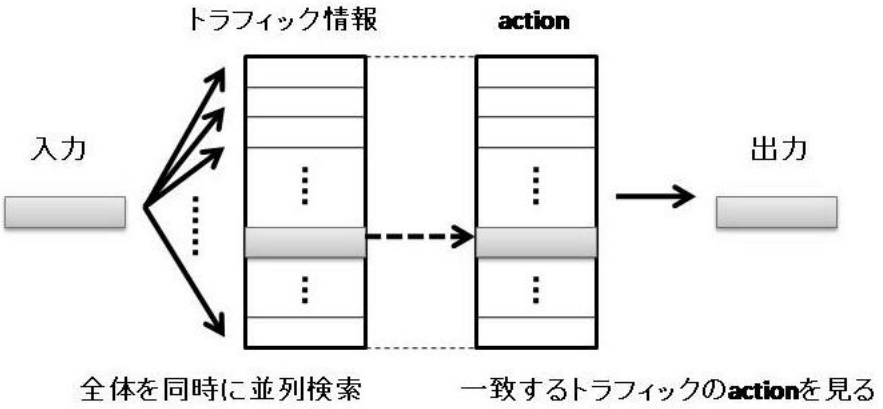

図 1: ACL のハードウェア処理の概要

ハードウェアで処理を行う場合、ネットワーク機器には予め専用の回路を用意しておき、ACL の各規則を各回路が処理を行う。この処理は並列に行われ ACL の規則の数に因らず一定の時間で処理が終わる。また、ハードウェア処理のため、大量のパケットの処理も短時間で終了する。ただし、ネットワーク機器にある ACL 処理用の回路数によって ACL の規則数が制限される。

3　大学におけるネットワーク管理

大学に限らないと思うが、ある組織のネットワークにおいてアクセス制御を行う場合、一カ所で集中して制御を行う方法と組織内のネットワーク機器で分散して行う方法が考えられる。大学においては両方考えられるが、私自身は後者、つまり、機器毎に ACL を設定することしか経験したことがない。この理由を考えてみると、以下のような大学のネットワークの特殊な事情があると思われる。

1. 大学では部署毎にサブネットワークアドレスが与えられ、ほぼ独立して運用される。サーバも存在する場合もあれば、存在しない場合もある。

2. 一方、各部署にはネットワーク管理が存在しないことが多い。よって、サーバ管理に不備が

あったり、Firewall が設置されていない場合があったり、設置されたとしても適切な Firewall の設定が行われるとは言いがたいなど様々な問題がある。

3. いくつかの部署は、部署間の関連が強いため相互で通信を行うことが多く、ファイル共有やプリンターの共有を行うなどネットワークの相互の通信が多くなる。

最初の項目に関して言えば、大学の NOC[1]からみると、各部署へのネットワークを提供しているプロバイダー業務であるように思われる。また、関連のない部署が同じ建物に入っているということも多々あり、物理的な近さが部署間の親密さに繋がらないことがある。

2 番目の項目から各部署にアクセス制御までまかせることはできない。各サブネットワーク毎に ACL の設定を大学の NOC が行うことになる。ただし、大学の NOC は各サブネットワークにあるサーバ等を管理することはないので、ゲートウェイとなるネットワーク機器において ACL を設定することになる。インターネットサービスプロバイダーはこのようなサービスを提供しないが[2]、大学では提供する必要がある。この時点で、一般のインターネットサービスプロバイダー業務とは異なっている。

3 番目の項目は、研究室毎にネットワークを利用していて、その研究室同士でファイル共有等を行いたい場合などが該当する。これは、ACL の設定に関連するので 2 番目の項目にも該当するが、インターネットサービスプロバイダーであれば具体的な設定内容である IP アドレスやポート番号を利用者から指定してもらえるが、大学では「どこそこの研究室とファイル共有したいのだが」といった要望しか上がってこないので、どのように設定するかまでを検討することが 3 番目の項目に含まれる。ファイル共有ぐらいだとそれほど難しくないが、一般的ではないソフトウェアの利用の場合、通信に必要なポート番号が明確になっていないことが多く、これを見つけだすだけでも結構な労力を必要とする。必要そうなポートを多めに開けておけば解決するのだが、それではセキュリティレベルが低下してしまう。

以上のことをまとめると、大学の NOC の業務は、ネットワーク管理とユーザに対する簡単なコンサルティングということになる。コンサルティングをどの軽減することは可能かも知れないが、ネットワーク管理業務を軽減するというのは難しく、ネットワーク管理業務の中でも ACL は重要なものである。管理業務を軽減してくれるツールが登場すれば話は別だがそれはかなり夢物語のような気がしている[3]。

4 アクセス制御をどこで行うか

一般にアクセス制御を行うとなると、Firewall 専用器などを想定する人も多いが、専用器がまだ存在しないか高額だったころにはルータでアクセス制御を行っていた。キャンパスネットワークと呼ばれるネットワークが大学に引かれたころに導入された CISCO の AGS[4]といった古いルータでもアクセス制御を行っていた記憶がある。今では、Firewall 機器も広く利用されているため、Firewall 機器でアクセス制御を行うのが理想なのかも知れないがネットワーク毎に Firewall 機器を用意したり、また、大学ネットワーク全体のアクセス制御を行う大規模な Firewall 機器を導入することはコスト面や管理運用面から考えると重荷となる。図 2 に 1 つの Firewall 機器でアクセス制御を行う場合のネットワーク図を示す。この場合、全てのネットワークが直接 Firewall に接続している必要がある。実際にこのようなネットワークを構成するは難しいが、TagVlan を用いるなどす

[1] Network Operation Center の略

[2] お金を払えば ACL を設定してもらうこともできるが、結構な金額になる

[3] ちまたには、ネットワーク管理が楽になりますよ言ったうたい文句で販売されているものもあるが、助けにはなるかも知れないが、軽減にはならない。コストに見合うようなものは私自身はであったことがない。

[4] 実際に取り扱った AGS のインターフェースの構成は 10base の AUI を 5 個に FDDI インターフェースを 1 つなどであった。

れば、仮想的には図 2 にあるネットワーク構成は可能ではある。しかし、Firewall 機器の要求される性能を考えるとコスト面で見合わないと思われる。

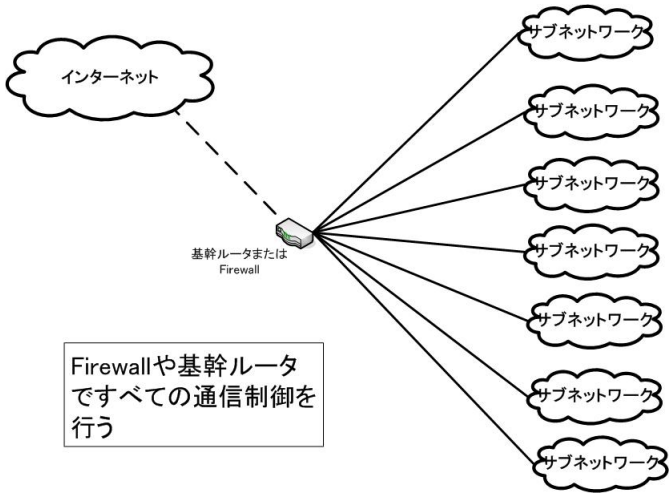

図 2: Firewall 専用器 1 台でネットワーク全体のアクセス制御を行う場合のネットワーク図

そこで、アクセス制御を行う方法としては、各サブネットワークが接続している末端のルータで行うか、または、末端のルータでアクセス制御を行うとともに大学のネットワークの出入口に設置した Firewall またはルータでもアクセス制御を行うかのいずれかが考えられる。

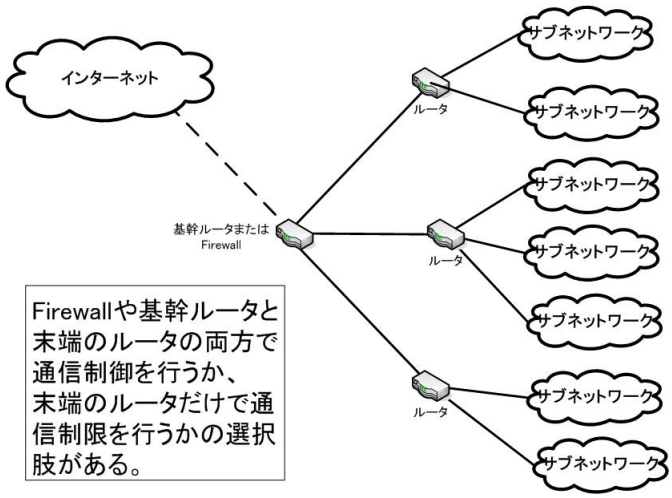

図 3: ルータで機能させるアクセス制御の範囲

それぞれ利点と欠点をあげると

- 末端のルータでのみアクセス制御を行う場合

  1. 各サブネットワーク毎の要求にあったアクセス制御をかけることが容易になる。
  2. パケットのアクセス制御の処理が末端のルータに分散される。
  3. 大学外のネットワークとのアクセス制御も末端のルータで行う必要があるため、ACL が大きくなる。
  4. 類似の ACL の記述が各末端のルータに増える。よって、大学外と大学内のネットワー

クのアクセス制御の方針が変るとすべての末端のルータの ACL の書き換えを行う必要が出てくる。

- 出入口の Firewall またはルータと末端のルータでアクセス制御を行う場合

  1. 各ネットワーク毎の要求にあったアクセス制御を行う場合が出てくる。
  2. アクセス制御の処理が末端のルータと出入口の Firewall 等に分散されるが、大学外と大学内のネットワークのアクセス制御の処理は出入口の Firewall 等に集中する。
  3. 大学外のネットワークとのアクセス制御は Firewall に集約されるため末端のルータの ACL が小さくなる。
  4. 大学内と大学外のネットワークのアクセス制御に関する ACL が出入口の Firewall 等だけに設定されるため、アクセス制御の方針変更に対応しやすくなる。

管理面から考えると ACL の維持管理が問題になるが、どちらも一長一短である。出入口の Firewall 等でアクセス制御を行う場合、大量のトラフィックによる DoS 攻撃を考慮する必要がある。実際、大量のパケットを送りつけられそのアクセス制御の処理のために Firewall がダウンしたり、正常な通信であってもそれが大量であるために Firewall がダウンするということが実際に起る。よって、出入口の Firewall でアクセス制御を行うことは DoS 攻撃の危険性を常にはらんでおり、セキュリティ面を考えると余り望ましくないのかも知れない。

「望ましくないのかも知れない」と弱めの主張をしたのは、それににも関わらず、ほとんどの大学では、Firewall を設置しているという事情があるからである。この理由を考えると、上記に関連したものとして、ACL のメンテナンスが非常に大変になること、末端のルータの処理能力を越えるような ACL を書かなければならないことなどがあげられる。それ以外の理由としては、Firewall の高機能化があげられる。単純にアクセス制御をするだけではなく、通信のセッション情報を保持したり、パケットのヘッダーだけではなくその内容を参照することでアクセス制御を行うなどの stateful inspection を行うことで、ウィルスの検出、P2P 通信の制御、様々な攻撃の防御などの機能があり、Firewall は単純に ACL の設定通りのアクセス制御を行うだけではない。

また、大学外の特定の IP アドレスの通信を禁止したい場合には、大学の出入口で通信制限を行うのが最も簡単である。結局のところ、現状では、ACL を大学の出入口の Firewall 等と末端のルータで行うというのが一般的ではないかと思う。

5　ACL のトラブル

アクセス制御のトラブルは ACL の設定ミス等によって起きることが多い。単純な設定ミス以外の設定ミスとしては次のことが考えられる。

1. アクセス制御の管理者の誤解による設定ミス

   設定する人間、つまり、管理者が設定する内容を誤って理解している場合、ACL を意図通り設定していても設定内容自体に誤りがあるので、アクセス制御も誤ったものになってしまう。

2. ACL がネットワーク機器においてどのように処理されるに関する誤解による設定ミス

   ACL がネットワーク機器においてどのように処理されるかということを誤解している場合、誤ったアクセス制御を行う可能性が高い。これは、ネットワーク機器のマニュアルの内容を十分理解することで防ぐことができる。

3. ACL が多数の規則からなることによる設定ミス

   ACL の規則数が増えれば管理者が設定を誤る可能性が高くなる。また、設定の誤りも見つけることが難しくなる。

4. 複数のネットワーク機器でアクセス制御を行うため、設定すべき ACL が複雑になることによる設定ミス

   例えば、2 つのネットワーク機器で特定の通信を両方とも禁止している状況でその通信を許可するとなると、2 つのネットワーク機器の ACL を変更している必要があり、管理が非常に煩雑になる。管理者が良くやる間違いは 1 つの機器の ACL の変更を行ってもう一つの機器の ACL の変更を行わないといったことがある。

ACL の設定ミスで特に問題なのは設定ミスに気づかないことである。許可している通信が通信できない場合には、ACL の設定ミスであるということを気づきやすいが、許可していない通信が通信可能になっている場合、気づくことが極めて少ない。気づくのは大抵の場合、何らかの攻撃や不正侵入を受けたときにはじめて気づくことが多く、手遅れになったりもする。

一方、ネットワーク構成、特に経路制御が ACL に関連してくるのは、経路の行きと帰りの経路が異なる場合である。

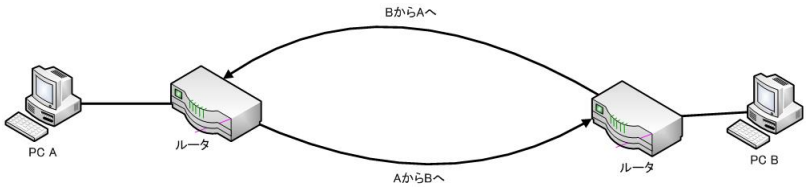

図 4: 行きと帰りが違う経路の場合

図 4 において、行きと帰りの経路の途中でアクセス制御が行われている場合、ACL の設定と確認が難しくなる。例えば、何らかのトラブルが発生した場合、行きのパケットによるのか帰りのパケットによるのかを判断する必要がある。また、図 4 のような経路を設けているのは、一方の経路に障害が発生した場合に、他方の経路で行きも帰りもパケットを送信することができるためである。また、ACL を設定しても正しいかどうかを確認するのが難しい。というのも、トラブル時に一方の経路だけを行きと帰りの両方で利用されることがあるがそのときに正しくアクセス制御ができているかどうか正常時には確認できないからである。

6　攻撃防御

外部からの攻撃を防ぐ方法として、攻撃元を検出しアクセス制御することは有力な方法の 1 つである。今では、攻撃を防ぐ方法としては、Intrusion Protection System(IPS) を用いることで、攻撃元の検出とアクセス制御を自動で行う方法や、攻撃元の検出に Intrusion Detection System(IDS) を用い、ACL の設定を手動で行うなどいくつかの方法が考えられる。

IPS を用いる場合、攻撃を検出後、攻撃であるかどうかに関わらず攻撃元からの通信すべてを止める方法もあり、または、攻撃と考えられる通信だけを止める方法もある。前者であれば、ACL の設定を自動で行うということになるが、後者は ACL の設定を行わず、常時パケットの中身を検査することになり、IPS の負荷が大きくなる。ちなみに、最近 Google が中国からの撤退を表明したが、中国でのインターネットでの検閲の方法は前者の方法に類似した方法がとられている [4]。

外部からの攻撃を防ぐために ACL を管理者が設定する場合には、大学外と大学内のネットワークの出入口に Firewall を設置し、この機器で ACL の設定を行うことになる。前述したように、末

端のルータでこの ACL を設定することは管理者の相当な負担になるとともに、攻撃への早急な対応を考えると一カ所のネットワーク機器の ACL の設定で組織全体のネットワーク防御に効果があることが望ましい。ただし、大学全体の Firewall では、DoS 攻撃をうけないような工夫が必要となる。

攻撃の検出で問題となるのはその検出の確度である。筆者は、簡単な Darknet を利用して攻撃の検出を行っている。規模としては、32 個の連続した IP アドレスを利用したネットワークである。この Darknet による攻撃検出方法であるが、上記 32 個の IP アドレスを 1 台の PC のインターフェースに設定し、この PC で Firewall ソフトウェアを稼働させ、すべての通信情報をログに残し、そのログに基づいて攻撃があるかどうかを常時調べることで、攻撃の検出を行っている。この方法自体は特別難しい方法でもなく、また、それほど負荷も大きくない。類似のことは、大学外との入り口に設置された IDS や IPS でも行われているはずであり、実際、大学のネットワークの出入口には IPS が設置されている。この IPS と Darknet を用いた検出を比較すると次のようになる。

1. IPS は Stateful inspection により様々な攻撃を検出することができる。
2. Darknet では検出できたが、IPS で検出できなかったものも多数ある。

IPS で検出できる攻撃は多数にわたり、専用器であるので検出できて当然である。一方、Darknet で検出できて IPS で検出できなかったものとしては、ポートスキャンである。これは、Darknet で検出できるものは ipfilter、ipchain、ipfw などの firewall ソフトウェアで得られる通信ログでありこのログ情報から得られるのはポートスキャン等の攻撃しか得られないからである。IPS でもポートスキャンなどの攻撃を検出するものだと思っていたが、かなりの頻度で検出できなかった。検出できなかったものは、ポートスキャン数が少ない攻撃、ハイポートつまり、ポート番号が 4 桁や 5 桁のポートスキャンの攻撃、スロースキャン攻撃つまり、ポートスキャンの間隔 (数秒から数時間) が広い攻撃などが主なものであった。IPS のように大学のすべての外部との通信を検査する場合、スロースキャンなどを監視するには数十秒単位でのパケットの履歴を監視する必要があり、かなりの高性能な機器が必要になる。このようなポートスキャンが検出可能な IPS が実際に商品として存在するのか、また、コスト面から見たときに十分見合うものなのかを考えると、IPS でスロースキャン等を検出することは難しいのではないかと思う。

7 Access Control List に関する研究

最後に筆者が行っている ACL に関する研究 [8] について述べる。前述したように ACL の処理方法はハードウェアによるかソフトウェアによるかのいずれかになる。ACL をソフトウェアで処理する場合、参照される規則をリストの上から順番に探す直列処理で行われる [6, 3]。基本的に読み込むことのできる ACL のサイズに制限はないが、処理に要する時間は ACL のサイズにより変化してしまう。なお、その処理に最適な ACL を構築することは NP 完全であることが知られている [5]。それに対し ACL をハードウェアで処理する場合は、連想メモリ (Content Addressable Memory,CAM) などを用いるために規則を参照する際、並列処理が可能で一律の時間により実行できる [2, 1]。ただし、ハードウェアのサイズに収まるような大きさの ACL でなければ実行できない。すなわち、ACL サイズはハードウェアのサイズに制限される。加えて CAM は参照される規則を検索するときすべての回路を動作させることになるため電力コストが大きくなってしまう。その関係上 CAM そのものも小さいサイズのもので済むよう、ACL はより小さいサイズのものが好ましい。

仮に ACL がハードウェアの制限に収まっていたとしても、ACL のサイズを小さくすることが必要な場合がある。筆者の研究で扱っている Layer 3 スイッチである OmniSwitch では、利用できる ACL のサイズがマニュアルに記載されており、ACL 関連以外の利用できる限界値、例えば、VLAN 数、dynamic VLAN やユーザ認証による VLAN の利用者数の上限なども記載されている。しかし

表 2: 処理前の ACL の一部

policy network group G1 44.8.53.192 mask 255.255.255.224
policy network group G2 44.8.7.0 mask 255.255.255.192
policy network group G3 44.8.22.192 mask 255.255.255.192
policy condition c1 source network group G1 destination network group G3
policy condition c2 source network group G2 destination network group G3
policy action NG diposition drop
policy action OK
policy rule r1 precedence 10 condition c1 action OK reflexive
policy rule r2 precedence 10 condition c2 action OK reflexive

表 3: 処理後の ACL の一部

policy network group G1 44.8.53.192 mask 255.255.255.224 **44.8.7.0 mask 255.255.255.192**
policy network group G3 44.8.22.192 mask 255.255.255.192
policy condition c1 source network group G1 destination network group G3
policy action NG diposition drop
policy action OK
policy rule r1 precedence 10 condition c1 action OK reflexive

ながら、これらの機能を同時に上限まで利用できるとは限らず、ACL 関連以外の機能を最大限利用したときに、ACL の機能が上限まで利用できない可能性がある[5]。よって、ACL のサイズがハードウェアの制限に収まっていたとしても、出来るだけ小さくした方が管理運用上も好ましい。

一方、ネットワークの管理運用の立場から考えると、何らかのトラブルやセキュリティ上の問題への対応、ネットワークの新設や廃止など様々なオペレーションが ACL の更新を必要とすることもある。そのときに、ネットワーク管理者がサイズを考慮して ACL の更新を行うことは難しい。よって、管理者は自身が管理したい ACL をそのまま記述し、ACL のサイズを自動的に短縮することができると、ネットワークの管理コストを下げることができる。

以上のような背景を受けて、[8] では ACL を書き換えそのサイズを特定のハードウェアのサイズまで短縮するようなプログラムの開発を行っている。ACL の最適化が NP-完全であるため、実際に最適な大きさ ACL を短縮化するアルゴリズムを考案しても、それが実用的かどうかは分からない。そこで、ACL を局所的に見て、短縮する規則をするようなアルゴリズムを作成し、それを実装したプログラムを作成している。このプログラムにより、ACL はハードウェアのサイズにとらわれず構築することもでき、ハードウェア処理におけるデメリットを克服することができる。[8] で作成したプログラムでは、例えば、表 2 にある ACL を表 3 のように変換することができる。これらの ACL は Alcatel 社の Omni Switch 用のものである [7]。

[8] で示しているプログラムではこのような短縮化が可能であるが、最短にすることは保証されない。よってこのプログラムにはできるかぎり短縮化することはできるがまだ不十分なところもあり、改良の余地が多々ある。

[5]OmniSwitch のログやマニュアル等を見ると OmniSwitch での ACL の処理は、CAM で行われているわけではなく、pseudo CAM (PCAM)、つまり擬似的な CAM が利用されているようである。よって、他の機能に PCAM が多く利用されると ACL の処理に必要な PCAM が足りなくなる可能性があるのではないかと推測している。

8 まとめ

本稿では、ACL の設定体験に基づき、ACL の設定方法や問題点を議論した。TagVLAN の利用が当たり前になってきており、Layer3 や Layer2 スイッチの高機能化などに伴い、ACL をどこにどのように設定すればいいのかなどいろいろ考えなければいけなくなるのではないかと想像している。

参考文献

[1] 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.

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

[3] Subrata Acharya,Mehmud Abliz,Bryan Mills,Taieb F.Znati,Jia Wang,Zihui Ge,Albert Greenberg:”OPTWALL : A Hierarchical Traffic-Aware Firewall”,NDSS Symposium,2007.

[4] R.Clayton, S.J.Murdoch, and R.N.M.Watson, Ignoring the Great Firewall of China, Proceedings of 6th International Workshop of Privacy Enhancing Technologies, LNCS 4258, pp.20–35, 2006

[5] Vic Grout,John McGinn,John Davies:”Real-time optimisation of access control lists for efficient Internet packet filtering”,J Heuristics,2007.

[6] Hazem Hamed,Ehab Al-Shaer:”Dynamic Rule-ordering Optimization for High-speed Firewall Filtering”,ASIACCS,2006.

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

[8] 石川拓道、吉浦紀晃、ハードウェア処理される Access Control List の短縮化、第 2 回インターネットと運用技術シンポジウム (IOTS2009) 論文集、pp.101-108, 2009