さいたま

埼玉大学情報メディア基盤センター年報

VOL.17 2003 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 20 年度活動報告

センターから

卷　頭　言

ネットワークの「砦」

情報メディア基盤センター長　吉田 紀彦

現代ネットワーク社会は悪意に満ちている。最重要課題として真っ先に必ず「セキュリティ」が挙がってくるのが、悲しい現実だ。悪意は、ウィルスやワーム、盗聴、パスワード割出し、スパイウェア、キーロガー、ボット、DoS（ブログ炎上に似た攻撃）、迷惑メール（SPAM）、なりすまし（フィッシング）など、ありとあらゆる思いつく限りの形で、また時には思いもよらない形で、気づかない内に襲ってくる。例えば、無線LANで数年前まで使われていたWEPという暗号化規格はとっくに破られている。やみくもな機械入力を防ぐために、わざと歪めた英数字を表示して、それを入力させる「キャプチャ」と呼ばれる仕掛けが多用されているが、画像理解技術など何も使わずにそれを破る極めて巧妙な手口がすでに考案されている。被害にあったPCを隔離と証拠保全のためにネットワークから切り離すのは対策の基本だが、その瞬間に自らの痕跡を跡形もなく消し去ってしまうウィルスもすでに存在する。悪意の目的は破壊活動、機密情報や個人情報の窃取、詐欺、脅迫など様々だが、PCの持ち主が被害を被るにとどまらない。いつの間にかPCが悪用されて加害者に加担させられることも少なくない。

回顧談をすれば、20年くらい前までのインターネットの黎明期は平和な時代だった。元々お互いに顔見知りの人たちだけが使っていたためもある。インターネットの仕組みや規約には当時の性善説の名残りがまだ残っていて、それが今では弊害を引き起こしているのも事実だ。例えば、メールの基本的な仕組みにはセキュリティはないに等しく、それを悪用した様々な迷惑メールがインターネット中に溢れている。インターネットは表社会だけでなく、裏社会にも根底から革新をもたらした。

どうすればいいか。まず第一に利用者各人の自覚が欠かせない。ウィルス対策ソフトウェアを必ず使用する、パスワードは解読されにくい文字列を使ってしかも定期的に変更する、怪しいメールは開かない、怪しいウェブページは見ない、怪しいソフトウェアやデータはダウンロードしない（もっとも「怪しい」かどうかの見極めは実は難しいが）などが真っ先に挙げられる。しかし、悪意の側の進歩は文字通り日進月歩であって、残念ながら、もはや自覚に頼るだけでは追いつかない。特に大学という組織では、年ごとに多数の利用者（学生）が入れ替わることもあり、教育や啓蒙に加えて、全体としての技術的な対応も重要になってくる。

情報メディア基盤センターでは平成19年春の全学基幹ネットワーク更新に合わせ、一つには、迷惑メール自動フィルタを導入して到来メール総量の7割以上にも達する迷惑メールのブロックにかなりの効果を挙げている。本年度は学内システムへの学外からのアクセスについて、盗聴・漏洩や不正使用を防止しつつ実現するために、暗号化に基づく仮想的な専用回線のネットワーク技術を活用して、まず学務関係で運用を開始した。このようなセキュリティ技術も着実に進歩してきており、今後もそれらを積極的に検討していく。全学ネットワークの「砦」をより一層堅固なものにして、教育・研究・業務の情報基盤インフラストラクチャをさらに安全・安心な形で安定して提供することを、引き続き目指していきたい。

情報基盤の整備と課題

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

Administration and Operation of Campus Network based on Fiber to the Laboratory

田邊俊治† 小川康一† 吉浦紀晃‡ 伊藤和人‡ 重原孝臣‡ 前川仁‡

†埼玉大学 情報メディア基盤センター
‡埼玉大学 大学院理工学研究科 数理電子情報部門

概 要

埼玉大学では平成 19 年 3 月にキャンパスネットワークを更新した．この新しいネットワークは，全学の全ての部屋をコアスイッチに光ファイバで接続するという完全スター型光直収ネットワークである．また，ユーザ数約 14,000 人の大規模認証 VLAN，クライアントにソフトウェアを必要としない検疫システムなどの特徴を有しており，埼玉大学情報メディア基盤センターが管理運用を行っている．稼動後一年あまりが経過してこの新ネットワークでのトラブル対応・運用を通じて浮上してきた問題点について，レイヤー別および，レイヤーを越えた観点から分析し，運用における改善点について考察を行った．

キーワード：ネットワーク運用，光ファイバー，ダイナミック認証 VLAN，検疫ネットワーク，P2P 規制

1 はじめに

埼玉大学では平成 19 年 3 月にキャンパスネットワークおよび情報システムを更新した．この更新にあたっては，FTTL(Fiber To The Laboratory) と称し学内のほぼ全ての部屋に光ファイバーを張り巡らせ，コアスイッチに直収するようにネットワークを構成した [1, 2, 3]．また，セキュリティと利便性を確保するためにダイナミック認証 VLAN(以後，認証 VLAN) を運用することとした．管理運用は埼玉大学情報メディア基盤センター (以後，センター) が行っている．サーバ群についてはホスティングサービスを提供し，一元管理を行うという集中型へとデザインの転換を行った．本論文では，新ネットワークの立ち上げや，稼動後一年あまりが経過してこの新ネットワークでのトラブル対応・運用を通じて浮上してきた問題点について報告する．

このような光ファイバーにより各部屋とコアスイッチを結ぶネットワークの先行例としては千葉工業大学のものがあり，約 1000 部屋に光ファイバーが敷設されている．一方，埼玉大学での FTTL の設置では，ファイバーを敷設することによって利用が可能となった認証 VLAN や検疫システムについて重点を置いている．さらに，ネットワークトポロジーの変更に伴い，従来のネットワーク管理体制の変更も行った．これまで，ネットワークの管理体制は多くの問題を抱えていたにも関わらず簡単には変更できなかったが，ネットワークトポロジーの変更を機会することで，管理体制の見直しを行った．

2 更新前のネットワークとネットワーク更新の目的

図 1 に更新前のネットワークと更新後のネットワークを示す．埼玉大学の新ネットワーク以前のネットワークは，リング状の基幹ネットワークを Ethernet で構築し，リンクを構成する各ルータ同士は Layer 3 レベルで接続し，RIP により経路制御を行っていた．また，ルータは主要な建物にのみ配置され，そこから各建物へとネットワークが繋がっていた．各学部・学科には，クラス C の大きさを最小単位としてサブネッ

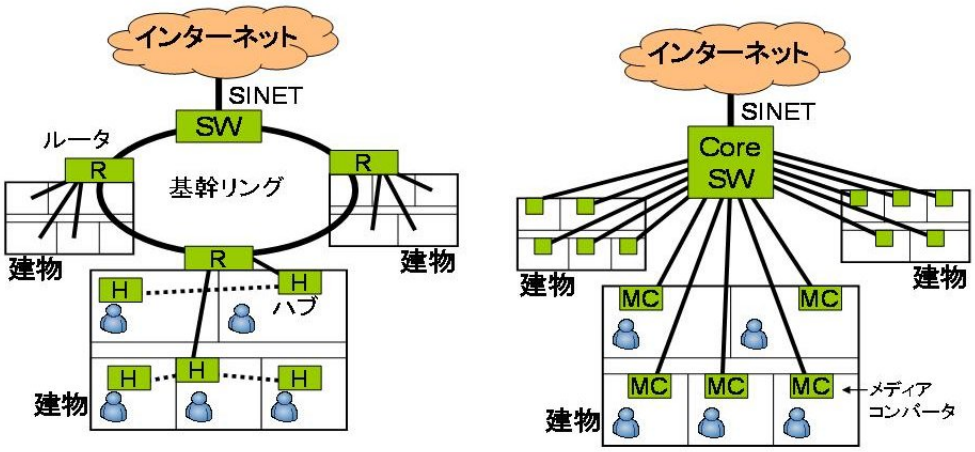

図 1: 従来の基幹ネットワークとスター型ネットワーク

トワークが提供されていた．その上で各学部・学科でそれぞれ独自にサーバを運用し，DNS サーバや Mail サーバを利用しており，大学全体としてみると，サーバの分散管理が行われていた．

このため，ある部屋，特に，基幹ネットワークを構成するルータがある部屋や建物のネットワークの入り口となる機器がある部屋などでトラブルがあると，建物全体のネットワークに波及するといった問題がたびたび起き，センターでは対応に多くの時間を要することとなった．

各学部や学科、事務組織のネットワークや各種サーバの管理は，その組織が行っていたため，ネットワーク管理の専門家ではないが，多少でもネットワークの知識がある人間に管理が任され，長年固定化してしまい，特定の教職員が半ばボランティア的に致し方なくネットワーク管理を任されてしまうケースが多かった．これは管理者にとって過大な要求であると同時に，各組織のネットワーク管理が属人的管理となってしまうこととなってしまった．このことは，管理者が変更になる場合に大きな問題となっており，また、セキュリティポリシーやそのための実施手順書を作る上で大きな問題となっていた．

別の問題として，建物の新築・改築や組織の改組により学部・学科，事務といった組織が横断的に共用する建物が増加し 1 フロアに複数の組織が展開する一方で，1 つの組織が複数の建物・フロアにまたがって分散するといった例が増えていた．

これ以外にも情報セキュリティインシデント対応やセキュリティポリシーに基づく運用なども求められており，埼玉大学のキャンパスネットワークや情報システムの管理運用には数多くの課題が山積みであった．

そこで，ネットワークの更新にあわせて，FTTL を導入することで，同一フロアに異なる組織があったとしても，また，同一組織が異なる建物にあったとしても，1 つの組織が 1 つのネットワークを他の組織と共有しないで利用できるようにした．さらに，新システムのサービスを新ネットワークにおいてのみ適用することで，旧ネットワークからの移行を促進し，またホスティングサービスを利用するように誘導することにより，分散型の管理体制から一元集中型への管理体制への移行を図った．これにより，当初の目的の大部分は達成できたが，ほぼ一年の運用の間にさまざまな課題がみえてきた．

3　新ネットワークの構造・サービス

新ネットワークシステムの構造はレイヤー別に次のようになっている．なお，ネットワークの規模は，ユーザ数が約 14000，部屋数が約 1800，VLAN 数は認証 VLAN が 150，固定 VLAN が 250 である．ネットワークに接続している PC 等の数は，各サブネットワークの管理を各組織に任せているために正確には把握できていない．

3.1 Layer 1

今回の更新にあたっては，学内 44 棟・約 1800 部屋に光コンセントとメディアコンバータを配置して情報ネットワーク機器室（以下サーバ室）に設置されたコアスイッチのポートと 1 対 1 対応したスター型ネットワークを形成している．図 2 は実際の光コンセント，図 3 はメディアコンバータである．メディアコンバータを利用した理由は，各部屋に設置されるネットワーク機器にはほとんどの場合，光ファイバーが接続可能なインターフェースを有しておらず，UTP ケーブルによる接続だけが可能であるため，メディアコンバータによる変換を行う必要があるためである．

実際の配線はサーバ室パッチパネルから各建物のパッチパネルへ集合光ケーブルを敷設し，そこから各部屋の光コンセントまで個別配線を行っている．部屋には末端として光コンセントが設置されておりメディアコンバータまで曲げフリー光ケーブルで接続している．部屋毎にシングルモードファイバー 2 心，合計で約 3600 心の配線はサーバ室側で 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，それを 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．図 4 はサーバ室のパッチパネル，図 5 はサーバ室の集合メディアコンバータである．

運用を開始してみると図面と配線の間違いが発見され，ケーブル不良か接続の間違いかを判別するために，可視光源による接続調査をおこなわなければならない事態になった．このほかに建物改修工事や部屋の用途換えに伴う改装工事などの際に断線事故を起こすなどのトラブルがあった．このような場合には，利用心線の変更や周辺の部屋からの振替を必要とするが，これも接続ミスか断線事故かの判別がつきにくいため，最終的には OTDR(Optical Time Domain Reflectometry) を利用して断線箇所を特定することが必要となった．このように光ファイバーの管理についての問題が明らかになり，いったん問題が起きるとその原因を突き止めるまでにかなりの手間と時間がかかった．また，本来は正しいはずの図面に誤りがあることがあるので，実際に光ファイバーの接続が確認できる体制や設備が必要である．

図 2: 光コンセント

図 3: メディアコンバータ

3.2 Layer 2

コアスイッチについては Alcatel-Lucent 社の OmniSwitch7800 を 6 台用いて，1 つの部屋から引かれた光ファイバーを，これらいずれかのスイッチの 1 ポートに収容した上で認証 VLAN150 個，固定 VLAN250 個を稼動させている．図 6 はコアスイッチである．図 7 に示すように，Alcatel-Lucent 社の認証 VLAN は，同じポートに接続しても MAC アドレス単位で接続を制御するので，1 つのポートで複数の VLAN を利用することが可能である．また，固定 VLAN とはポート単位で 1 つの VLAN が利用可能であり，認証の必要がない VLAN である．各部屋の光ファイバーが接続しているコアスイッチ 1 ポート毎に，その部屋が固定 VLAN を利用する場合には，VLAN を固定的に割り振る．また，その部屋が認証 VLAN を利用する場合には，そのポートを認証 VLAN として稼動させる．認証 VLAN は，機器の性能上，256 個までしか利用できないため，学科や講座毎に学生・教員・研究室・学科内向け・外向けの 5 種類の認証 VLAN を用意し，認証に使う ID 毎にどこの VLAN に所属するかがあらかじめ設定されている．なお，ID は大学の全ての教職員や学生に与えられている．

以前はブロードキャストストームが発生すると建物全体でネットワークが使えなくなるというトラブルが起きていた．しかし，このように大学内のサブ

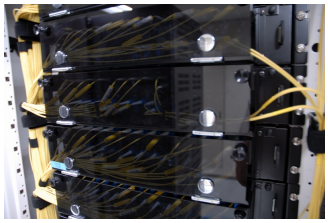

図 4: パッチパネル

図 5: 集合メディアコンバータ

ネットワークを細かく切ることにより，このような問題はなくなった．しかし，最近では認証 VLAN の処理における負荷が大きいことによると思われるが，OmniSwitch7800 に取り付けられているネットワークモジュールに接続している 1 つのポートで大量のパケットが発生する状態になると，モジュールに収容されているすべてのポートで通信が不安定になる状況が見られた．コアスイッチに限らず無線 LAN でも VLAN の数が多いために負荷が高く認証不能やルーティング不能のトラブルなどが見られており，動作を確認しながらベンダーと調整を行っている．

3.3 Layer 3

VLAN 毎に/22〜/28 の IP アドレスを割り当てて運用を行っており，個別の希望がない限りすべて DHCP でアドレスを割り振る設定としている．新ネットワークへの移行の際に，DHCP の全面的な適用を行えなかったために旧来からの管理者の中には IP アドレスについてネットワーククラスの知識しかなく，また，移行前に利用していたサブネットマスクはほとんが/24 であったため，CIDR 表記などになじみのない人が多くいた．そのため，新ネットワークへの移行の際には，説明用資料などが必要になるなど，各学部学科のネットワーク管理担当者への十分な説明が必要不可欠であった．また，新ネットワークを管理する立場であ

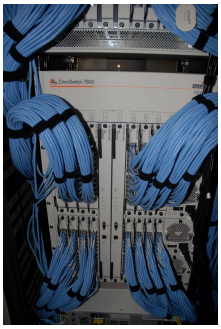

図 6: コアスイッチ

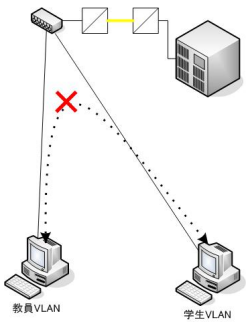

図 7: ダイナミック認証 VLAN

るセンターでは，VLAN 同士の ACL(Access Control List) をこれまでの経緯を踏まえた上で提供しているが，そのアクセス関係についても明解な説明資料が必要であった．図 8 は，実際に説明の際に用いたアクセスコントロールの図である．また，図 9 では，研究室 VLAN、サーバ VLAN、教員 VLAN、学生 VLAN に所属するネットワーク機器の例を示している．この図に示すように，プリンタなどの人が直接 web 認証することが出来ない機器もいずれかの VLAN に所属させる必要があり，この作業のトラブルが多く発生した．

3.4 Layer 4〜7

この項目とセンターが提供するサービスについては重複部分もあるが，一般的に利用されるネットワーク上のサービスとネットワーク接続を利用するのに基本的に必要なものについて説明する．基本的ネットワークサービスとして NTP サービスとメールのみ提供をしており，POPS / IMAPS / SMTP Auth に対応

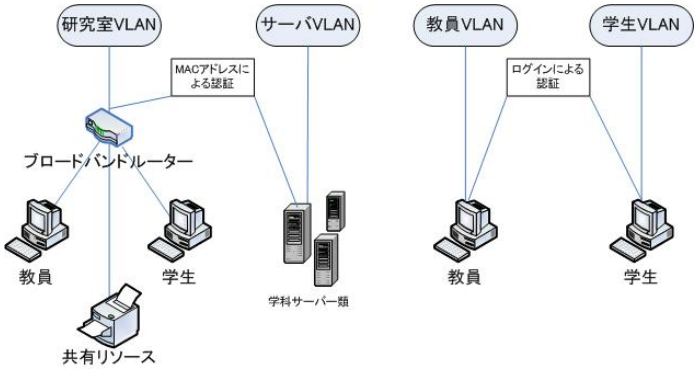

図 9: VLAN に所属する機器の例

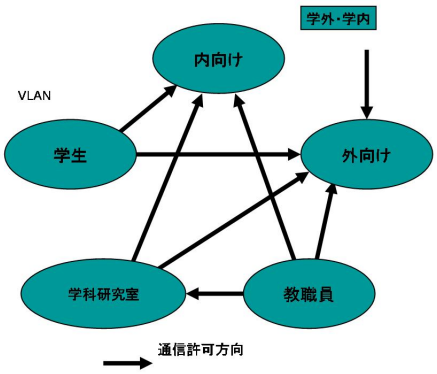

図 8: VLAN 関係図

しているほか，web メールとして Active!Mail が利用できるようになっている．

有線 LAN では認証後の所属 VLAN の IP アドレスを取得させるために Java Applet を利用しているが，セキュリティ強化対策を行った WindowsVista ＋ Internet Explorer 7 や JRE(Java Runtime Environment) のバージョン違いなどで個々の対応を迫られることが多い．

無線 LAN については Trapeze 社製 [9] の 802.1X 認証を行う無線 LAN スイッチ型の機器を導入したが不慣れな利用者が設定に手間取る事例が非常に多かった．PC や LAN カードに添付される各種サプリカントの扱いに苦慮したため手順書では Windows の機能によるもののみを対象とした．しかし，WindowsXP ではレジストリに ID・パスワードを記録してしまうために，パスワードを変更した場合にはレジストリの編集が必要になる．これは一般の利用者には難しい操作を強いる結果となってしまった．

3.5 サービス

更新されたネットワークの上に各種システムを構築しセンターとしてサービスを行っている．これらは単に技術的な提供というだけでなく，センターの方針をもとに行っている．

3.5.1 統一認証システム

大学には，教職員や学生が情報端末を利用するための認証システム，教員が業績を登録するための認証システム，シラバスを入力するための認証システム，学生の授業の履修登録のための認証システムなど多くの認証システムが乱立していた．これらの認証システムを統一することを目的として，統一認証システムを用意した．具体的には，OpenLDAP[7] により実現している．このシステムの稼働開始時は，情報端末やキャンパスネットワーク利用する際の認証システムとして利用されていた．その後，教員のシラバス登録ための認証システム，学生の授業の履修登録のための認証システムにも利用されており，徐々に学内の認証システムが統一されつつある．

この認証システムでは，大学の教職員と学生に対してアカウントが発行される．この認証システムにもとづいて，大学が提供するメールアドレス (全学用メールアドレス) も配布される．

3.5.2 検疫システム

認証 VLAN により個々の機器が判別され，直収ネットワークによりダイレクトな接続のコントロールが

行えることから，ネットワークに接続されている機器を監視し異常な通信を行ったものをネットワークから切り離して安全な状態に保つ検疫システムが稼動している．

ネットワークの最上位にある IPS(Intrusion Protection System) が通信内容を解析し，そのログからコアスイッチに当該機器の MAC アドレスの通信を遮断させることでこれ実現している．これは個々の通信機器にエージェントを導入することなくネットワーク上の振る舞いを見て判別するので大学のような持込端末を制御しづらい環境に向いている．ポリシーの問題から現在は P2P ファイル共有ソフトの規制のみを行っている．

3.5.3 各種ホスティングシステム

センターでハードウェアと基本システムを用意し利用者へ機能のみを提供するホスティングを Web・Mail・DNS で提供している．過去に各部局へ配布されたインターネットアプライアンスで，メーカー保守が終了しているものを現在でも利用している部局がある．このような機器を撤廃するための受け皿として用意したものである．また，大学内のサーバを減らすことによるセキュリティの向上も目的である．

1. Web ホスティングサービス

   共用の Web サーバを提供し各部局･研究者の Web ページを収容する webhosting サービスである．リプレース前は Web サーバの提供という名前で www.saitama-u.ac.jp 以下をディレクトリで分けて提供していたがホスティングサービスとして DNS の設定が可能であれば部局のサブドメインやホスト名のついた URL も利用できるようにした．これらは個々のホスト名でサーバ証明書も利用できるように Apache HTTP Server [6] による IP アドレスベスのバーチャルドメインとして提供している．

2. Mail ホスティングサービス

   各学部などで独自にメールサーバを運用してきたが，機器の老朽化や平文パスワードの利用などのセキュリティ上の問題へ対処するために Mail ホスティングとしてドメイン毎のユーザ管理を利用申請者で行えるものを提供することとした．これにより，セキュリティを確保した上で，各学部などの組織で独自にメールアドレスの利用や発行を行うことができる．例えば，大学に教職員ではないが，大学のメールアドレスを必要とする人に対して，各組織が独自にアドレスの提供を行うことができる．

   Mail ホスティングサービスの利用を促進するために，全学用メールアドレスだけに適用していた spam ファイアーウォールを，Mail ホスティングサービスにも適用した．

3. DNS ホスティングサービス

   ネットワークの移行にともない多数の VLAN が設定されたが，ほとんどが旧来クラス C と呼ばれていた/24 に満たない大きさである．このため逆引きについては，CIDR に対応している必要があり，これまで学内で行ってきた DNS の運用では対応できない．そこで，DNS ホスティングサービスをセンターとして提供することとした．これは Infoblox 社 [10] の DNS アプライアンスを導入し，GUI で設定･操作が行えるようになっている．

3.6 管理と運用階層

運用においては情報メディア基盤センターが利用実態の全てを把握するのは不可能なので，ネットワークリソースの管理については各学部または学科毎の担当者からの申請に基づいて設定を行っている．この窓口となる担当者については技術を理解し責任を負えるものが望ましいのが，学部によってはそのような状態にないことがある．システムの改善や利用者へのナレッジマネージメントのためにこれらの役割をもつ人々を効率よく組織化していくことが必要である．これらは，全学サービスを提供するということで大学全体としての業務効率化や学内へのアピールに有用であると考えられる．

3.7 教育用 PC

本ネットワークの更新に合わせて，教育用 PC の更新も行い，345 台の MacOSX を導入した．これは，11 台のブートサーバによる Netboot を利用している．トラフィックやサーバによる障害は発生しなかったが，各 PC にログインする際に，LDAP への問い合わせが

多数発生し，ログインに 5 分以上かかるという問題が当初発生した．これは，ログイン時の LDAP の問い合わせの回数を減らすように設定を変更することで解決した．これ以外では特に問題は起きていない．

4 考察

4.1 適切なレイヤー選択と問題解決

情報メディア基盤センターへ持ち込まれる相談やトラブル解決依頼は様々あるが，相談者の持ってくる解決法がベストとは限らないものが多い．また，技術的に解決可能な問題であっても規定・規則で縛られる場合もあるので注意が必要である．たとえば学務部の企画により電子シラバス・履修登録・成績入力を行う学務システムが別に稼動していたがこれらのアカウントをこのシステムの ID と統一することになった．従来の学務システムでは便宜上事務が教員に代わり各種入力を行うこともあったが，それを知らされず統合となったために事務が教員のパスワードを求めるなど，運用上の問題が発生した．また，教員が自宅から各種入力を行えるようなシステム改善を求めてきたが，個人情報の持ち出しに関する適切なルールが未だに作成されていないので，対応するかどうかも含めて未解決のままである．

これらのトラブルを未然に防ぐためには技術的な部分以外への配慮が必要であり，その部分についてはそれを職務としている適切な部署との連携と情報提供を行っていくことが必要である．

4.2 LDAP の問題

ユーザ管理を LDAP により行っているが，ユーザ数が 14,000 を超えており，大規模なものとなっている．ユーザ数の多さによるものか各種サービスからの参照回数などによる負荷に起因するかは調査中であるが，データベース破損で認証不能になることがこの 1 年間で 5 回発生している．このため，現在のマスター＋スレーブ構成からマルチマスター＋スレーブ＋ロードバランサ構成への変更を検討しているところである．LDAP によるユーザ管理についてはいくつか研究があるが [4, 5]，規模に関する報告はあまりない．

4.3 認証 VLAN

認証 VLAN を利用する場合，その OS と方法としては Windows ＋ web 認証が最も多い．この方法の場合，認証後に IP アドレス再取得をさせる必要があり，これは JavaApplet で実現される．しかしながら，JavaApplet が動かないトラブルが発生し，認証 VLAN が使えないという事態があった．これは JRE の特定のバージョンが原因と思われる．実際に，Java1.6 update5 でトラブル報告があり自動で Java のアップデートを行うと認証 VLAN が利用できないといった事態になった．このような事態を避けるために，不用意にアップデートをかけないように一般利用者に注意喚起を行う必要があった．

4.4 検疫

新ネットワークシステムでは検疫システムが稼動しているが，自動的に検出して通信遮断しているものとして現状では，P2P による通信だけである．他のものについては，検疫は行っているが自動的に遮断せずに，手動による対策を行っている．自動化は今後の課題である．

P2P プロトコルを対象に検疫と自動遮断を行ったところ，通信できないのは，PC に原因があると思い，再インストールをしてしまうといった事例があった．また，ホームページからファイルをダウンロードしようとしたときに，それが P2P プロトコルを利用したダウンロードの方法だとは知らずに行ってしまい，通信ができなくなってしまうという事例もあった．この場合は他のダウンロードの方法を選べば問題はなかったが利用者にはそのような知識がないために通信ができなくなってしまった．このように，一般利用者にある程度の知識を持ってもらわないとネットワークが非常に使いにくいものになり，また，管理自体も手間がかかってしまうという問題がある．

4.5 国立大学固有の問題

3.1 章でも述べたように，実際の運用では，光ファイバーの図面と配線の間違いや建物改修工事や部屋の用途換えに伴う改装工事などの際に断線事故を起こすなどのトラブルが起きた．これらのこの原因の 1 つとして，ネットワークの運用に複数の部署がかかわり合っていることがあげられる．つまり，ファイバー

の敷設自体は施設部署の担当であり，電源は電気通信担当，実際のネットワーク運用はセンターとなっており，何らかの作業や変更を行う場合に，1つの部署だけで行うと問題が発生する．国立大学法人特有の問題とも考えられるが，工事などの際には，施設部署の電気通信担当や実際に利用する部局の担当者と連絡を密にし，利用実態を把握する必要がある．

4.6 IPv6への対応

IPv4のアドレス枯渇などから，今後はIPv6の利用も検討する必要がある．今回のネットワーク更新では，コアスイッチと部屋がメディアコンバータのみを介して接続されており，コアスイッチでIPv6に対応するか，IPv6ルータをコアルータと独立に用意することで，ネイティブなIPv6ネットワークを独立して提供できる．これは，コアスイッチと部屋の間にLayer 3スイッチが存在しないため容易に行うことができる．

4.7 各VLANに関する監視

各ネットワークの利用方針については，それを利用している組織や研究室によるため，各VLANでどのようにPC等のネットワーク機器が接続されているのかといったことがわからない．例えば，各VLANでNATを使って接続ノード数を増やすことが可能であり，このような場合には接続ノード数をネットワーク全体を管理運用しているセンターでは把握できない．また，独自に無線LANのアクセスポイントを設置することも可能であり，これについても把握できない．これらのことは，利用者の責任で行うことを運用上のルールとしていることで責任の所在は明らかにしているが，接続ノード数や無線LANアクセスポイントの把握はセキュリティ上必要なので何らかの対応は必要であると考えている．

5 最後に

社会情勢・大学を取り巻く環境の変化などのパラダイムシフトにより旧態依然とした属人的・慣習的・個人責任といった体制は変革を迫られている．新システムやサービスの導入といった技術的なもので解決できるものはあるが，ポリシー・運用などのシステムがあってこそはじめて大学の情報系センターとして周囲から求められているものを担うことができるであろう．今回のダイナミックな変化の中で得られたものを踏まえて次期システムの構想や現行の運用体制の変革に取り組んでいきたい．

参考文献

[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No.11，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] 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

[4] 平塚紘一郎，大垣内多徳，田中光也，長期運用を考慮した認証システムの設計と運用，情報処理学会 インターネットと運用技術，No.2007-DSM-047，pp.13–18，2007

[5] 前田香織，河野英太郎，北村俊明，キャンパスネットワークへの認証システムの導入情報処理学会 インターネットと運用技術，No.2007-DSM-047，pp.19–24，2007

[6] Japan Apache User Group, http://www.apache.jp/

[7] OpenLDAP，http://www.openldap.org/

[8] アルカテル・ルーセント OmniSwitch 7800, http://www1.alcatel-lucent.com/com/en/appcontent/opgss/OS700_br_tcm228-288021635.pdf

[9] Trapeze 無線LANスイッチ http://www.macnica.net/trapeze/index.html

[10] Infoblox, DNSアプライアンス http://www.infoblox.com/

第9回インターネットテクノロジーワークショップ発表論文に加筆

学外アクセスサービスについて

木村雄一

情報メディア基盤センター

1. まえがき

情報メディア基盤センターでは、平成 20 年度前期の成績登録より、Web 成績登録システムへの学外アクセスサービスを開始しました。これは、非常勤講師の方が学外から直接 Web 成績システムに成績登録作業を行ってもらうことで、これまで他の教職員が非常勤講師の成績登録作業を代行していたのを解消するのが大きな目的でした。また、常勤の教員についても学外から成績登録をできるようにして欲しいとの過半数代表の要望を受けたものでもあります。Web 成績登録システムをはじめとして、学内ネットワーク上に存在するシステムはセキュリティ上の観点から、学外から一切アクセスできないようにされていました。これは言うまでもなく、膨大な個人情報を取り扱う学内ネットワークの運用はセキュリティの確保に最大限の配慮をしなければならないからです。そこで、本年度は「試行」と位置付け、学内ネットワークと学外のインターネットに接続された PC とを安全にかつ簡便に接続するための方法について慎重に検討を進めました。なお、Web 成績登録システムへの学外アクセスサービスの開始に向けて、情報メディア基盤センターと研究協力部情報基盤課は、学務部全学教育課と定期的に打ち合わせを開催し、情報交換を行いました。

インターネット等の公衆回線を用いて離れた場所に存在する LAN 同士を接続するための技術として、VPN (Virtual Private Network) という技術があります。これは企業内ネットワークの拠点間接続などに使用され、専用回線を用いるより低コストで実現できるのがメリットです。VPN では、インターネット上にデータを送信する際に認証技術やトンネリング・プロトコルと呼ばれる特殊なプロトコルを用いた暗号化によって、インターネット上に仮想的な通信トンネルを構成することでできます。この通信トンネルは利用するアプリケーションを問わないため、VPN による接続ができれば Web 成績登録システムだけでなく、教員活動報告書 Web 入力システムにも利用することができるようになります。VPN は利用されるプロトコルの違いからいくつかの種類がありますが、平成 20 年 7 月にスタートした学外アクセスでは「PPTP」、平成 21 年 1 月からは「SSL-VPN」と呼ばれる方法がそれぞれ採用されました。

2. PPTP による学外アクセス

平成 20 年 7 月に供用が開始された「PPTP」による学外アクセスサービスは、学外からの非常勤講師による成績登録を主な目的としてスタートしました。「PPTP」とは、

Microsoft 社によって提案された暗号通信のためのプロトコルで、Point to Point Tunneling Protocol の頭文字をとったものです。Windows98 以降の Microsoft 社製の OS には標準で搭載されていたため、多くの利用者が追加投資をすることなく利用可能と判断したためです。また、情報メディア基盤センターに設置された PPTP サーバーにはフリーソフトウェアを活用し、既存のサーバーに間借りする形で導入されました。さらに、導入作業は情報メディア基盤センターの技術職員の小川康一氏が中心となり担当しました。このため、導入費用はゼロという点も PPTP を採用した大きな理由でした。ただし、このような間借り状態の PPTP サーバーでは同時接続数が多数となった場合に正常に動作できるかという問題があったため、平成 20 年度前期の学外からの成績登録は原則として非常勤講師の利用に限定させていただきました。

PPTP による学外アクセスでは、延べ 406 人の非常勤講師から利用実績があり、概ね順調に学外からの成績登録が行われました。また、心配された同時接続数はたいしたことになりませんでした。というのは、多くの利用者はファイルのアップロードにより成績登録を行うため、短時間のうちに作業を終えられるためです。しかし、問題点も見受けられました。PPTP を利用するには PC にダイアルアップ接続と同様な設定をする必要があり、PC に不慣れな方にとっては設定作業が困難となる場合があったこと、PC を利用するネットワーク環境によっては PPTP による通信が許可されていない場合があったこと、PPTP で Web 成績登録システムに接続すると切断しない限り他の web サイトを閲覧できないこと（セキュリティの点からそのような設定としていました）、など主に利便性の面で問題がありました。また、過半数代表からは常勤教員についても学外からの成績登録を認めて欲しい、さらに「教員活動報告書 Web 入力システム」にも学外から入力できるようにして欲しいとの強い要望を受けるようになりました。教員活動報告書の入力作業は成績登録と比較して長時間に及ぶため、同時接続数が増加する可能性が高いと考えられます。また、入力途中で接続が切れることがあれば折角入力したデータが消失することになりかねないため、学外との接続を担うサーバーにはより高い安定性が求められます。となると、間借り状態の PPTP サーバーに対する懸念は払拭できません。そこで、新たに「SSL-VPN」装置を導入することになりました。なお、PPTP サーバーの運用は平成 21 年 3 月で終了する予定です。

3. SSL-VPN による「埼玉大学リモートアクセスサービス」

平成 21 年 1 月に学外接続サービスのための「SSL-VPN」機器が導入されました（図 1）。「SSL-VPN」とは VPN の暗号化プロトコルとして、”https://～”でおなじみの SSL（Secure Sockets Layer）を利用した VPN 技術です。ほとんどの Web ブラウザは SSL 通信に対応しているため、学外の利用者はインターネットが利用できる環境であれば SSL-VPN を利用することができます。PC にこれといった設定をする必要はなく、インターネットに接続された PC で Web ブラウザを起動し、埼玉大学へ接続する場合はブラウザのアドレス欄に”https://vpn.saitama-u.ac.jp/”と入力すれば SSL-VPN に接

続できるという利便性の良さが最大のメリットです（図 2）。図 2 の画面が表示されましたら、統一認証アカウントのユーザー名とパスワードを入力して、ログインしてください。このように、SSL-VPN は非常に簡単に VPN を利用することができるため、現在は”リモートアクセス”と言えば SSL-VPN を利用することが定番となっています。

他方、SSL-VPN のサーバー側については、サーバーの安定性、長期的な拡張性やサポート面を考慮して、専用の機器を導入することが一般的です。加えて、平成 21 年度からは教員活動報告書 web 入力システムへの学外接続も開始される予定です。そこで、情報メディア基盤センターでは F5 ネットワークス社製の SSL-VPN 機器を購入しました。なお、購入には学長裁量経費の支援を頂きました。SSL-VPN の稼動を機に、「埼玉大学リモートアクセスサービス」と称しています。

平成 20 年度後期の成績登録から、常勤教員についても所属部局長の許可を得た上で学外からの成績登録が利用できるようになりました。SSL－VPN の稼動後、間もない段階ですが、これまでのところ大きなトラブルの報告はなく、順調に稼動しています。また、「PPTP より接続が簡単になった」とのご感想も伺っています。

4. おわりに

情報メディア基盤センターでは、今年度よりスタートしました学外アクセスサービスを含め、学内ネットワークの安定した運用とセキュリティの確保に努めていますが、社会では情報流出事故のニュースが後を絶ちません。その多くは個人のちょっとした不注意によるものです。学外から成績登録を行うことは必然的に個人情報を学外に持ち出すことになり、その取り扱いについては平成 21 年 2 月 3 日付け埼大全機（総）第 43 号で定められています。学外から成績を登録する際は個人情報の取り扱いに十分ご注意の上、「埼玉大学リモートアクセスサービス」をご利用ください。

図 1 SSL-VPN 装置の外観

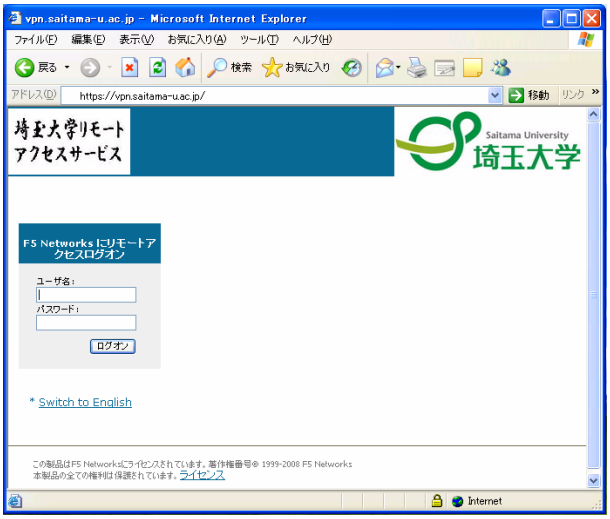

図 2 埼玉大学リモートアクセスサービス画面

P2P検疫について

吉浦紀晃

情報メディア基盤センター

1　P2Pとは

P2Pとはpeer-to-peerの略です。それではpeer-to-peerとは何かというと、端末同士でデータのやり取りを行う方式ということです。これだけだと何のことか分かりませんが、P2Pという言葉が出てくる以前のコンピュータネットワークの通信方式であるサーバクライアントに対抗した言葉がP2Pであり、サーバクライアント方式を説明しないと説明できません。

サーバクライアント方式の通信は、図1にあるように、1つのコンピュータが他のコンピュータと通信する方式であり、サーバとクライアントが通信することで、サーバにあるデータをダウンロードすることができます。ここで、中心になるコンピュータのことをサーバ、このサーバと通信をする他のコンピュータをクライアントと呼びます。この方式では、クライアント同士のやり取りも可能であり、このやり取りは一旦サーバを経由して行われることになります。2ちゃんねるなどの多くの掲示板などではこの方式がとられています。

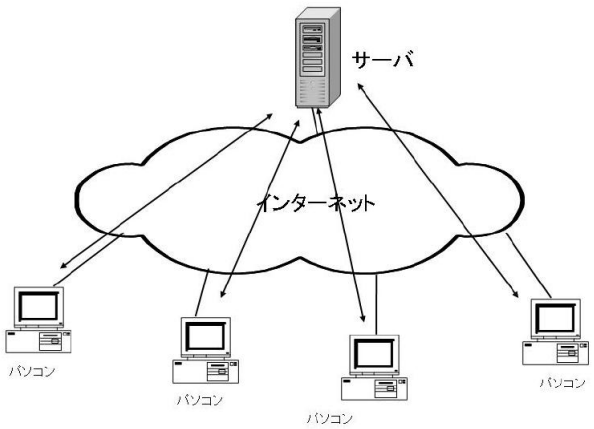

図1: サーバクライアント方式

一方、P2P方式での通信は、図2に示すように、クライアント同士が相互に直接接続してデータのやり取りを行います。この方式の利点として第一にあげられるのが負荷分散です。サーバクライアント方式の通信では、多数のクライアントが利用する場合に、サーバに負荷が集中してしまい、通信遅延や通信ができないといったトラブルが起きますが、

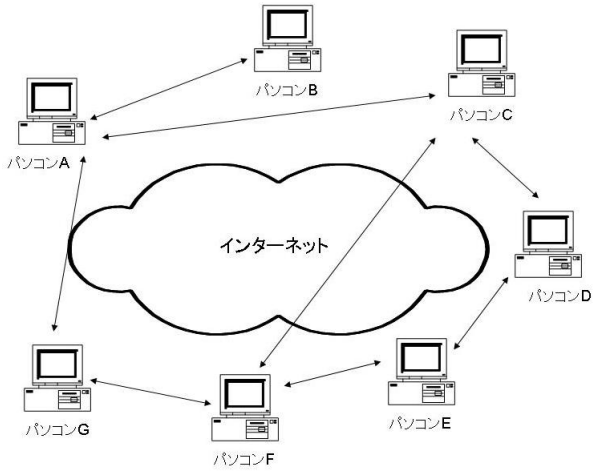

図 2: P2P 方式

P2P 方式ではサーバにあたるようなコンピュータは存在しないため、一カ所に負荷が集中することがなく通信遅延などの問題が起きにくくなっています。このため、ファイルのダウンロード等を行うのには都合のよい通信方式であり、この通信方式を利用した多くのソフトウェア (P2P ソフトウェア) が作られてきました。代表的な P2P ソフトウェアとしては以下のようなものをあげることができます。

Winny　WinMX　Cabos　LimeWire　BitTorrent　FlashGet　BitComet
eMule　Share　PPLive　PPStream　TvAnts　QQLive

日本で有名な P2P ソフトウェアとしては Winny があげられると思いますが、国や地域によっては、よく利用される P2P ソフトウェアは違ってきます。例えば、南米などでは、eMule が良く利用されていたりします。多くの P2P ソフトウェアの中でどれを利用するかといったことは、そのソフトウェアの特徴よりも、そのソフトウェアで共有できるファイルにより決められるといった傾向があります。また、1 つのコンピュータで複数の P2P ソフトウェアを利用するといった利用者もいます。

P2P 自体は 1 つの通信技術ですので、様々な研究も行われていますし、実際に多人数が利用するネットワークアプリケーションでは P2P 技術により構築されているものもあります。例えば、Linux などのオペレーティングシステムの DVD イメージなどは数ギガバイトになるので、1 つのサーバからダウンロードすると時間がかかる、サーバに負荷が集中するなどの問題があります。そこで、P2P 技術を利用して、分割された DVD イメージを複数のクライアントからダウンロードするといった手法がとられており、これにより、ダウンロードの高速化と負荷分散が実現されています。

2　なぜ、P2P ソフトウェアは利用に注意が必要なのか

これまで述べたように、P2P はファイルのダウンロード等には有効な技術ですが、その一方で、様々な問題もあります。

1. P2P によるウィルスの感染の危険性

コンピュータではほとんど全てのものがファイルの形式になっています。よって、ウィルスも P2P ネットワーク上で伝搬する可能性があります。メールや Web アクセスの場合にはウィルス検出ソフトが機能しますが、それ以外のファイルへのアクセスの場合には検出ソフトが機能しないといった場合もありますので、感染の危険度が高くなります。

2. 情報漏洩

「暴露ウィルス」という言葉が一時期流行ったりしましたが、ウィルスによってコンピュータにある様々な情報が P2P ソフトウェアによりインターネットに漏洩してしまう可能性があります。また、P2P ソフトウェアによってはユーザが共有するつもりではないファイルまでもが漏洩してしまう可能性があります。

この種の情報漏洩は社会問題化しています。実際、自衛隊の機密情報や生徒の成績が P2P ソフトウェアでインターネット上に漏洩されたといった報道があるように情報漏洩は数多く起きています。

これは役所や企業の問題である場合が多いわけですが、大学生であれば以下のような問題が考えられます。

(1) 教育学部の学生のパソコンから教育実習のレポートが漏洩し、その電子ファイルにはそのファイルに児童の個人名とその児童の様子が書かれていた。
(2) 医学部の保健学科の学生のパソコンから介護実習のレポートが漏洩し、その電子ファイルには介護した患者の病状などが書かれていた。
(3) 工学部の学生のパソコンから卒業研究用実験データが漏洩した。そのデータは非常に重要であり、漏洩したためにそのデータに関連した特許出願ができなくなってしまった。

などいろいろな問題が考えられます。特に、個人名などの個人情報が含まれている場合には、訴えられる場合もあり得ます。

3. 著作権侵害

P2P ソフトウェアで最も話題となっているのが著作権侵害です。あくまでも憶測ですが、P2P ソフトウェア利用者の目的のほとんどは、何らかのファイルが欲しいということなのではないかと思います。そして、そのファイルの多くが音楽、映像、ソフトウェアなどの著作物であることが多く、その多くは著作権侵害により作られたファイルなのではないかと思っています。当然ですが、著作権侵害はいけないことです。

4. 児童ポルノ

P2P ソフトウェアで海外で特に問題にされていることとして、児童ポルノ画像を P2P を利用して送受信していることがあります。著作権侵害は親告罪であり、誰かが訴えないと捜査等が始まりません。よって、著作権侵害していてもだれかに訴えられない限りは、問題が表面化することはありません。一方、児童ポルノ等は親告罪ではありませんので、捜査当局が捜査をして、犯罪者を逮捕起訴することがあります。実際、P2P を利用して児童ポルノなどのやり取りをしたため逮捕されたという報道を目にすることもあります。

5. 加害者となる可能性

   P2P ソフトウェアではダウンロードしたファイルを他のパソコンからダウンロードできるようにしてしまうものもあります。例えば、著作権法に違反して作られたファイルをダウンロードした場合、法律上は問題にならないかも知れませんが、これを他者へダウンロードさせると法律違反になります。ですので、利用者は無意識のうちに違反行為を行っていることになります。

   また、P2P 方式の通信では、ファイルを直接ダウンロードしなくてもファイルがパソコンに保存されるということもあります。例えば、図 2 において、パソコン A がパソコン D からファイルをダウンロードする場合、直接接続していないので、一旦パソコン C を経由してファイルのダウンロードが行われます。このとき、パソコン C にはダウンロードされたファイルが保存され、パソコン C の利用者が直接ダウンロードしていないファイルもパソコン C に保存されることになります。もし、このファイルが違法ファイルならば、パソコン C の利用者に何らかの処罰などが課されないとも限りません。

6. 帯域の浪費

   P2P ソフトウェアはファイル共有をすることが主な目的ですから、ダウンロードするだけではなくアップロードする役割、つまり、他のユーザからファイルをダウンロードされることもあります。多くのユーザから大量のファイルをダウンロードされたり、大量のファイルをダウンロードすれば、大量のデータがネットワーク上に流れることになります。これは他のネットワーク利用者にとっては迷惑になります。大学のネットワークやインターネットは多人数で共有しているものであり、特定の利用者が大量のデータを流すと、他の利用者のデータが遅く届いたり届かなくなったりしてしまいます。

   大量のデータのやり取りは他の利用者の迷惑になりますが、上記のように特に P2P ソフトウェアは大量のデータの送受信を発生させやすいので注意する必要があります。

3　法律の話

P2P ソフトウェアについては、Winny の開発者が「著作権法違反の幇助罪」で逮捕起訴され、一審判決では有罪判決が出ています。この判決に対して賛否様々な意見がありますが、P2P ソフトウェアを安易に利用すると是非は兎も角として、不必要な騒動に巻き込まれてしまう可能性があります。

一般に P2P ソフトウェアにより著作権違反であるファイルをダウンロードすることは、著作権違反にならないと解釈されています。しかしながら、Winny の裁判のように、当初法律違反にならないと思われた事柄であっても裁判で有罪判決を受けるなど、インターネットの利用に関する法律は実体に追いついておらず、明確に決まっていないことがいろいろありますので注意が必要になります。

当然ですが、このようなファイルを他者へダウンロードをさせると著作権法違反になります。前述したように、P2P ソフトウェアがダウンロードしたファイルを他者へダウンロード可能にすることもありますので注意が必要です。また、最近では、違法ファイルをダウンロードしただけでも違法とするように法律の改正を行う動きもあります。

このように法律の解釈や法律自体が変るということもありますので、「違法なファイルをダウンロードするのは違法ではない」という認識は改めた方がいいでしょうし、現状でも場合によっては、逮捕等のトラブルに巻き込まれてしまう可能性も認識したほうが良いでしょう。さらに、インターネットには国境はありませんので、海外から突然警告が送られてくると言ったこともあり得ます。

法律の話をしましたが、違法であるかどうか以前に、音楽ファイルや画像ファイルなど、本来金銭を出して購入すべきものを無料で利用できるということはすべきではなく、問題がないかどうかを良く考えてからこのようなファイルをダウンロードしたり利用したりすべきです。違法な方法で作られたファイルをダウンロードすることは違法な行為に手を貸しているといえなくもありません。

4　プロバイダの話

インターネットは様々なネットワークをつなぎ合わせた「ネットワークのネットワーク」であり、プロバイダはインターネットを構成する重要な要素です。多くの人が家から利用するときにはプロバイダを利用してインターネットを利用していると思います。

プロバイダの悩みの 1 つが、インターネットを流れる大量のデータです。ネットワーク上に大量のデータを流すためには、回線を増強する、機器を更新するといった対応が必要であり、そのためにはそれなりのコストがかかります。一方、家でインターネットを利用するときの費用は定額であることが多いと思います。そのため、プロバイダは回線の増強などでコストをかけたからといって一般ユーザから費用を徴収するわけにもいきません。そして、データ量の 9 割近くが約 1 割の利用者によるものであるとの調査結果もあり、特定の利用者が大量のトラフィックを発生させています。このことから、プロバイダによってはトラフィック制限を行うなど、P2P ソフトウェアによるトラフィックへの対策を実行や検討しているところもあります。

5　埼玉大学での対策

このように P2P ソフトウェアの利用には多くの問題があることから、埼玉大学では次のような対策をとっています。

1. 埼玉大学のネットワークでは、P2P ソフトウェアを利用するとパソコンがネットワークから自動的に遮断され、ネットワークが利用できなくなります。

   遮断されたパソコンで再度ネットワークを利用するためには、情報メディア基盤センターで遮断解除の手続きを行う必要があります。

2. 研究等で P2P ソフトウェアを利用する場合には、事前に申請するとネットワークから遮断されません。

この対策では、健全な P2P ソフトウェアの利用も阻害してしまう可能性がありますが、前述した問題点を考えると、上記の対策をとらざるを得ないというのが現状です。例えば、P2P ソフトウェアを大学のネットワークで利用して違法ファイルを公開した場合、その P2P ソフトウェアの利用者のみならず、大学の管理責任も問われてしまうためです。

また、P2P ソフトウェアを利用しているつもりでなくとも遮断されてしまう場合もあります。例えば、何かファイルをダウンロードするためにクリックしたところ P2P ソフトウェアによりファイルがダウンロードされるといった場合には、ネットワークから遮断されてしまいます。

このように、むやみやたらとクリックすると問題を起してしまったりしますので、クリックするとどのようなことが起きてしまうのか、自覚しながらネットワークを利用するのが重要になります。これは何も P2P だけではなく、クリックしただけで、ウィルスに感染するといった危険なものもありますので、十分に注意する必要があります。

6　インターネットを正しく利用しましょう

本来インターネットは、その初期の段階では、何の制限もなく自由に利用できるようにというコンセンサスがあり、性善説に基づいて利用されてきました。しかし、ウィルスの出現など様々な要因でインターネットの自由な利用が徐々に制限されています。そして、P2P 自体も有益な技術であるにも関わらず、著作権侵害といった違法行為を行う利用者が多数いるために、P2P 技術自体の利用も制限されるといったことが様々なところで検討されつつあります。ネットワーク利用に制限を設けざるを得なくなるのは、利用者によるところが大きいということを自覚して、ネットワークを利用する必要があるのではないかと思います。