# インターネットとネットワークに関する基礎知識—情報モラルとセキュリティ—

担当：笹原・匂坂・佐藤・清水・千葉・宮脇

## 本日の内容

- インターネットのしくみと利用上の注意点（モラルとセキュリティ）を把握する
- コース管理システム Moodle の授業コースにアクセスする

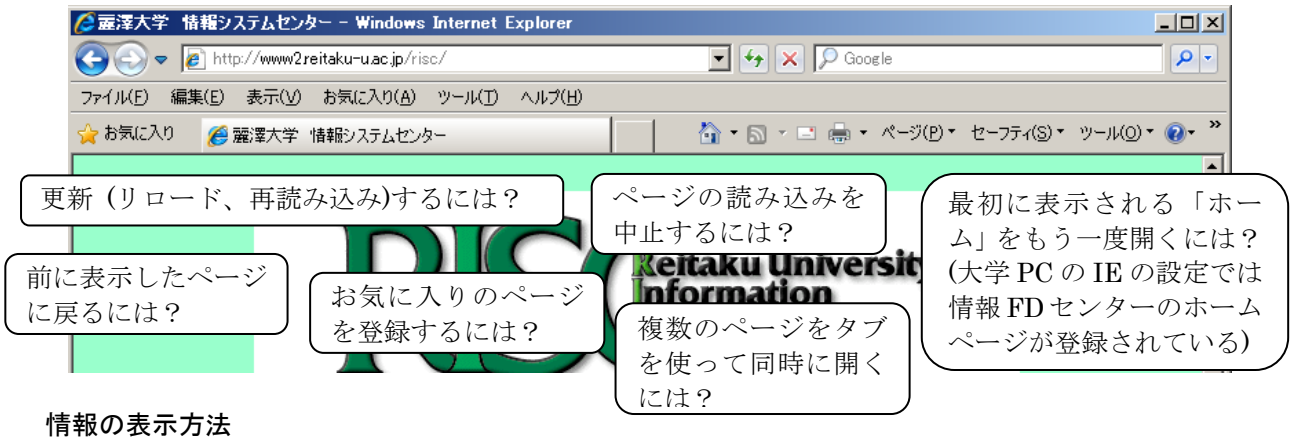
## 1. WWW ブラウザの使い方の基本

WWW ブラウザを使うと、インターネット上に接続されている世界中のコンピュータで公開されている情報を閲覧することができる。
WWW ブラウザの種類：**Internet Explorer**／Mozilla Firefox／Opera／Google Chrome／Safari …

WWW ブラウザの起動（Internet Explorer, Mozilla Firefox, Opera）：


※ Firefox, Opera は [スタート]→[プログラム] から起動

※ Internet Explorer (IE) の主な操作方法を確認しよう




### 情報の表示方法

(1) 情報をたどって探していく (ハイパーリンク hyperlink の利用)。
(2) アドレス (URL) を指定する。
(3) 検索エンジンを使う。

**実習 1：上記 (1) の方法で以下のホームページを閲覧しよう**

- 麗澤大学のホームページ（情報 FD センターのホームページにリンクがある）
- 麗澤大学　図書館ホームページ（麗澤大学のホームページにリンクがある）
- 情報 FD センターのホームページ（ブラウザの「ホーム」ではなく、麗澤大学のホームページから探してみよう。見つけにくい！）
- 「コンピュータ・リテラシー」の全クラス共通のページ（情報 FD センターのホームページの「麗澤大学授業教材集」にリンクがある） ※ URL: `http://www.FL.reitaku-u.ac.jp/lit/`
- 「コンピュータ・リテラシー」の各クラスのコースページ（Moodle）※別配布の資料参照
- 「IT 用語辞典 e-Words」（授業ホームページにリンクがある）

**実習 2：上記 (3) の方法で以下のホームページを探してみよう (キーワードはスペースで区切って複数入力することができる。入力すべきキーワードを考えよう)。たとえば、大学の外にあるパソコンからこれらのページを探すことを考えよう。**

- 情報 FD センターのホームページ（ブラウザの「ホーム」ではなく、検索エンジンで探そう）
- 外国語学部「コンピュータ・リテラシー」の全クラス共通のページ

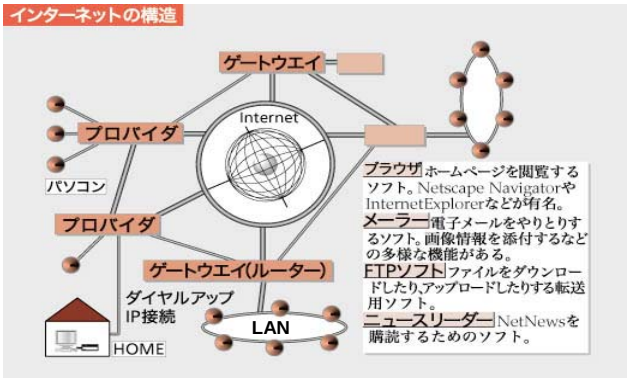
**実習 3：検索エンジンの「イメージ(画像)検索機能」を使って画像を検索してみよう**

**実習 4：「コンピュータ・リテラシー」の各クラスのコースページ (Moodle) を、すぐに開けるよう「お気に入り」(Internet Explorer の場合。Firefox, Opera の場合は「ブックマーク」) に登録しよう (登録内容はあとで整理・編集することができる)。授業外の時間に学生 PC で WWW ブラウザを開き、登録**

したアドレスが参照できることを確認しよう。
実習 5:「コンピュータ・リテラシー」の各クラスのコース（Moodle）を開き、第 4 回授業の課題（Journal「日誌」の記入と保存）をおこなおう。

## 2. インターネットの基本

インターネットは、ネットワークとネットワークを相互に接続することによって世界中に広がったネットワーク環境である。今日のコンピュータはネットワークに接続されることでより力を発揮する。各組織のコンピュータは、LAN（Local Area Network）と呼ばれるコンピュータ・ネットワークに接続される。各組織では、このネットワークを自律的に管理・運用している。こうした自律ネットワークが複数組み合わされ、世界的な規模のネットワークに発展したものがインターネットである。「インターネット」というネットワークサービス組織が存在するわけではない。世界中に散在するネットワーク（商用サービス、地域ネットワーク、企業や大学などのLAN、WAN）が相互接続されインターネットが構成されている。




日経BP社『日経BPデジタル大事典 2001-2002 年版』より

インターネットの利用は、電子メール、WWW（World Wide Web）による情報検索や収集と情報発信、FTP（File Transfer Protocol）によるファイル転送、インターネット電話やデータストレージなど、さまざまなサービスが存在している。

現在では、このインターネットを情報収集や情報発信の道具として使いこなす能力「インターネット・リテラシー」を身に付けることが、コンピュータ・リテラシー能力の一つとして欠かせない。インターネット・リテラシー能力には、インターネットを使いこなせること以外に、危険に対処する能力やネットワーク上での正しいマナー（ネチケット）を身に付けていることが重要となる。

## 3. インターネットを利用する上での注意点

上の項でも説明したとおりインターネットはネットワークを相互接続した世界規模の巨大なネットワークであるものの、情報を伝達する経路にすぎない。いわば情報の道路であり、現在提供されているWWWサービスやメールなどはそれを利用する方法のひとつでしかない。今後もその特徴を活用した様々なサービスが出現することになるはずである。インターネットを固定的に考えるのはその活用の妨げになる可能性がある。

インターネットを利用することで、多くの情報を効率良く収集することができ、同時に情報を発信することも容易である。その利便性を大いに活用したいところであるが、同時にその背後に隠れた危険な側面にも留意しておく必要がある。その利便性は善良な利用者だけでなく、悪意を持った利用者や犯罪組織などにとっても有用だからである。

また、当人に悪意がなくても、誤った使い方をしてしまうことで、法に触れたり多くの人の迷惑となったりするような行為を行うことも簡単である。

ここでは、他人に不利益を与えることなく、また自分自身が不利益をこうむることなくインターネットを便利に活用するための注意点について簡単に述べる。

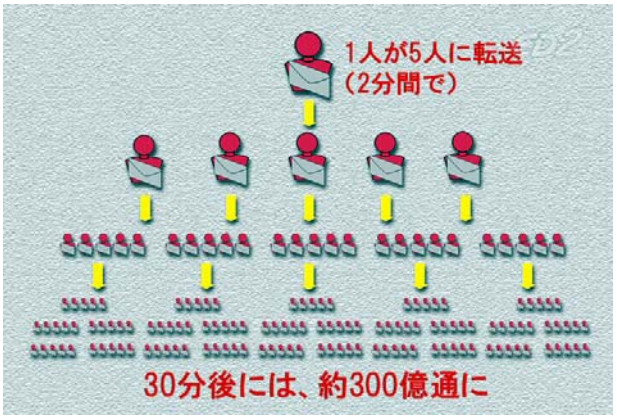

グリーンコミュニティ「ひいらぎ Cafe」の SSL 情報

### (1) 通信の暗号化

まず最初に、電子メールを送る場合であれ、Webページのフォームに入力して送信する場合であれ、情報は暗号化しない限りインターネット上に流れる情報はいつでも傍受される可能性があることを意識しよう。電子メールにパスワードなど重要な情報を書き込んで送信することは絶対に避けなければならない。

暗号化されていないプロトコル（HTTP）では情報はそのまま文字として流れる。ログイン情報を入力する場合や、ネットショップなど個人情報を入力する場合には、WWWブラウザとWWWサーバーの間でデータを暗号化するSSL（Secure Socket Layer, プロトコル名はHTTPS）が使われていることを必ず確認しよう（右上図参照）。SSLを使うと、通信をおこなっているブラウザとサーバー以外は情報を読み取ることができない。

当然だが、暗号化をおこなって通信するのは信頼できる相手でなくてはならない。初めてやり取りをするサーバーの場合、公式の認証局による認証を受けているかなどを確認して判断するのが普通である（右上図）。




チェーンメールはデマや中傷、詐欺などといった情報でさえ、すばやく拡散させてしまう性質がある。善意の内容であっても情報を制御できなくなる可能性が高く、他の方法を使うべきである。
（図は『情報機器と情報社会のしくみ素材集』から）

### (2) ネット上の情報の信頼性

マスメディアから発信される情報の多くは専門家によるチェックを経ている。しかしながら、インターネットでは個人でも容易に情報発信できるため、過失または故意により誤った情報が公開されていることも少なくない。また犯罪目的で虚偽の情報発信が行わ

れることもある。インターネットを用いた情報収集などには、その真偽を見分ける能力が必要となる。

不確かな情報がメールで送られ、転送を求められることもある(チェーンメール)。安易に転送するとデマの情報を拡散させてしまう可能性がある。チェーンメールなどによるデマの情報は、喫緊性の高い内容(差し迫った内容、不安になる内容)で、現実的で(さもありそうな話で)、不特定多数の人が対象となり、しかもあいまいさに包まれていて真偽の検証が難しい場合に拡散しやすくなる。

### (3) 情報発信を行う際の注意点【次回詳しく扱う】

ネット掲示板やブログ、SNS(ソーシャルネットワーキングサービス)などを用いて日本全国あるいは世界各国の人々へ情報発信したり意見交換を行ったりすることも簡単である。しかしながら、インターネット上で情報発信を行うということは、都会の駅前の雑踏などでメッセージを書いたプラカードを掲げる行為と同じ性質がある。友人同士の気軽なメッセージ交換の場として利用していたとしても、大勢の第三者が読んでいるという意識が常に必要であり、実際にそうであることが多い。悪意のない仲間内の軽口のつもりで書き込んだ内容が事件に発展することもある。また内容の正当性や正確性への配慮も求められる。

インターネットでの情報発信は、都会の雑踏でプラカードを掲げるのと同じ性質がある

### (4) 著作権【次回詳しく扱う】

インターネットとパソコンを使えば、他者の著作物をコピーして利用することも簡単である。日本の著作権法と、日本を含む多くの国が署名するベルヌ条約では、個人的な用途であれば他者の著作物であっても自由に利用することができる。しかしながら、ネット上での公開という行為は個人的な行為に当たらないため、許可や権利を得ていない公開(自動公衆送信)は著作権法に違反する行為となるので注意が必要である。

文章の引用については、引用部分が量的にも内容においても本文(主)に対して従の位置づけになっていて、引用部分が本文と明確に区別されていること、出典の明記があることなどが必要となる。限度を超えた引用は盗用となり、法的な処罰を受けるだけでなく社会的な信用を失うことにつながってしまう。

互いの権利を尊重しあうことで社会は成り立っているが、インターネットもまた同様である。

### (5) ネット上での匿名性

通信の秘密は法により守られているため、インターネット上では匿名の状態で情報収集したり情報発信したりすることができる。また、これを隠れ蓑(みの)にして悪意を持った行為を行う者も残念ながら存在する。しかしながら、通信に関する記録は接続事業者や通信事業者、サービス提供者などのコンピュータ上で一定期間保存されているため、強迫や誹謗中傷、著作権の侵害などといった法に触れる行為については、捜査機関などによって発信者を特定することは難しくない。

不満のはけ口などとしてインターネットで他人を中傷したり強迫したりといった行為を行うと、多くの人を不快にするだけでなく、本人にとっても不本意な結果が待ち構えていることになる。匿名性は善良な利用者にのみ与えられている。

### (6) 個人情報を守る

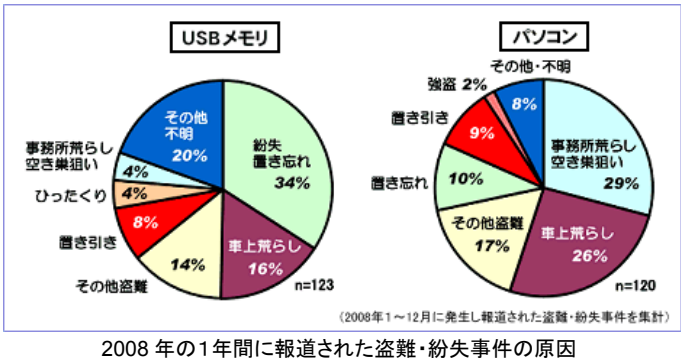
氏名や年齢、住所、電話番号、病歴、顔写真、銀行の口座情報、クレジットカード番号など個人を特定できる内容を総称して個人情報と呼ぶ。これらの内容がインターネットなどを通じて流出するようなことがあると、悪用されたり致命的な被害を受ける恐れがある。ひとたびインターネット上に流出・拡散した情報は消去することができないことを忘れてはならない。その取り扱いには充分な注意が必要である。個人情報収集が目的の懸賞サイトや占いサイトなどもあり、登録してしまうと詐欺目的の迷惑メールが多量に届いたりアダルト系サイトの会員にさせられてしまうこともある。


本人を特定できるような個人情報をインターネット上で公開するのは危険な行為である。地図サービスサイトで設定を誤り、多くの個人情報を公開してしまうといった事故も多発している
(『情報機器と情報社会のしくみ素材集』から)

またオークションサイトのアカウント情報(ユーザIDとパスワード)が盗まれ悪用されることで、たとえば架空出品や落札詐欺などにより無関係な第三者に多大な被害をもたらす可能性がある。金融サービスのアカウント情報なども含めて、厳重な管理が求められている。

もちろん他者の個人情報を扱う場合は当人の許可を得るなど慎重に行うべきである。携帯電話の電話番号やメールアドレスも個人情報のひとつである。

ノートパソコンの軽量化や高性能化、USBメモリの大容量化や低価格化が進んでいるが、同時に紛失や盗難などに遭った際の情報流出リスクも増大している。個人情報や機密情報を保存する際には暗号化を行ったりパスワードを設定したりするなど、万一の事態に備えて事前の対策を行っておくことが肝要である。




2008 年の1年間に報道された盗難・紛失事件の原因

個人情報保護法（個人情報の保護に関する法律）が2004年に施行されたが、大まかに言えばこれは個人情報の悪用を罰する法律ではなく、企業や自治体などでの個人情報の取り扱い方法について規定した法律である。個人情報は自身で守る必要がある。

### （7）マルウェアへの対策

当初は多くが“いたずら目的”で作成されていたマルウェア（ウイルスやスパイウェアなどの悪意のあるソフトウェアの総称）も、現在では金銭や犯罪が目的で大量にばらまかれるようになっている。パソコンやインターネットを利用する際には、セキュリティ対策ソフトをインストールしておかなければ、自分自身が被害に遭うだけでなく、まわりの人にも多大な迷惑をかけてしまう可能性が非常に高くなる。

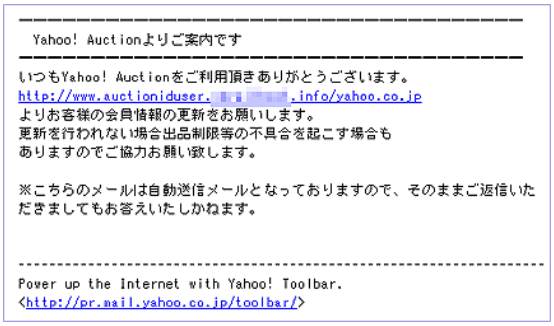
また、現状の対策ソフトでは「定義ファイル」を最新のものに更新しておかなければ新種のマルウェアの検出・駆除を行うことができず、役に立たなくなってしまう。期限切れになると更新できなくなるので注意が必要である。

マルウェアには、ウイルス、ワーム、スパイウェア、キーロガー、アドウェア、ランサムウェア、トロイの木馬、ボットなど感染活動や動作内容などが異なる多くの種類がある。スパイウェアやキーロガーは、パソコンに保存されたファイルやキーボード操作から機密情報や個人情報、アカウント情報を盗むことが目的である。トロイの木馬やボットは感染したパソコンを外部から乗っ取り、さまざまな悪意のある行為が行われる。ランサムウェアはパソコン内のファイルを勝手に暗号化し、元へ戻すために金銭を要求するものである。

感染原因の多くは、迷惑メールの添付ファイルのクリック、迷惑メールから誘導される悪意のあるWWWサイトでのうかつなクリック（ダウンロードが自動で行われることもある）などとなっている。最近では他者のUSBメモリをパソコンに差すことで感染するといった事例も多い。信頼できる団体や企業のWWWサイトが書き換えられてマルウェア感染してしまうことも少なくない。インターネットに接続しただけで感染することもある（ワーム）。したがって対策ソフトの利用が不可欠である。

### （8）迷惑メールへの対処

情報漏えいや推測などにより勝手に送られてくる広告・宣伝のメールを迷惑メールと呼ぶ。国内業者による許可のない（オプトインされていない）商用メールの送信は「特定商取引法」と「特定電子メール適正化法」により禁止されている。しかしながら、海外の送信業者から、あるいは海外のサーバーを用いた迷惑メールは増え続ける一方という現状がある。インターネット上に流れるメールの8～9割が迷惑メールとするセキュリティ関連団体の報告もある。


Yahoo! Auctionよりご案内です

いつもYahoo! Auctionをご利用頂きありがとうございます。
http://www.auctioniduser.[redacted].info/yahoo.co.jp
よりお客様の会員情報の更新をお願いします。
更新を行われない場合出品制限等の不具合を起こす場合も
ありますのでご協力お願い致します。

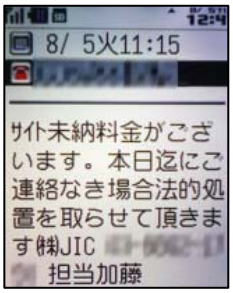
※こちらのメールは自動送信メールとなっておりますので、そのままご返信いただきましてもお答えいたしかねます。

Power up the Internet with Yahoo! Toolbar.
<http://pr.mail.yahoo.co.jp/toolbar/>

フィッシングメールの例。このように手続きしないとアカウントを停止するなどと脅す内容が書かれることも多い

迷惑メールには、詐欺やマルウェア感染を目的とするものも少なくない。またメールを表示しただけで感染したり、読んだことが送信者へ伝わる仕組みになっているものもある。したがって知らない送信元からの迷惑メールは読まずに削除するのが一番安全である。添付ファイルをクリックしたり、リンクをクリックしたりする行為は非常に危険である。

これらの危険性を回避するために、インターネット接続事業者（プロバイダ）や携帯電話会社などが迷惑メールをブロックするサービスを提供している。できるだけこれらを利用するとよいが、現状のシステムでは正規のメールもブロックしてしまう可能性があり、ブロックされた迷惑メールリストの中に正規のメールが入っていないかは定期的に確認する必要がある。



架空請求のメール例

迷惑メールには、キャンペーン当選、無料プレゼント、芸能人のゴシップ情報、新型インフルエンザウイルスなど時事的なニュース、アダルト系の情報などメール受信者の興味を引くような内容のもの、コンピュータウイルス感染やメール送信エラーの通知を装うもの、宛先間違いのメールを装うものなど、あの手この手で受信者のクリックを誘うことが多い。迷惑メールはあらゆる犯罪行為に巻き込まれる最初の第一歩になる可能性が高いことを知っておくべきである。

#### ・フィッシング詐欺

銀行やオークションサイトなどになりすましたメールに「更新手続きをしないとアカウントを停止」といった内容が書かれている場合がある。これをフィッシング詐欺メールと呼ぶ。書かれた偽のリンクをクリックして個人情報を入力してしまうと悪用されることになる。個人情報の入力を求めるメールを受け取った際は、電話帳などで調べた企業の番号に直接電話をかけるなどして真偽を確認するほうが安全である。

#### ・架空請求詐欺

最近では、携帯電話のショートメール（SMS、Cメール）などを使った架空請求詐欺の被害が増加している。「有料サイトの料金が未納」「本日中に連絡がなければ法的措置」などと脅す文面で、うっかり連絡してしまうと何度も高額な送金を要求されることになる。不安な場合は、消費者生活センターや警察署の窓口で相談するとよい。どちらの窓口もWWWページに連絡先などが記載されている。

ワンクリック詐欺のメール例。メールなどに書かれたリンクアドレスをクリックすると、このような画面が表示される

#### ・ワンクリック詐欺

迷惑メールなどに書かれた「無料サービス」の言葉にだまされクリックする

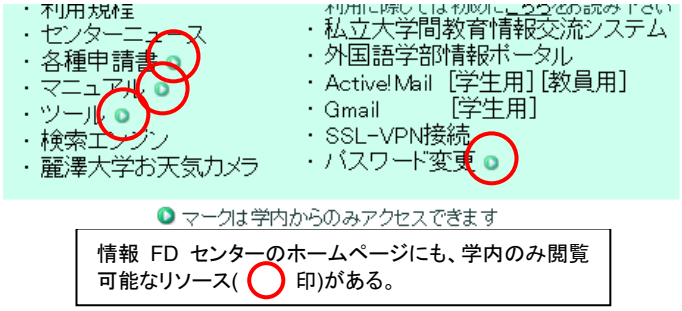
と、会員登録したとして会費を請求される詐欺の総称。現状では業者が個人を特定することは不可能なので無視すればよい。ただし、メールアドレスを特定する仕掛けによって請求書のメールが送られてきたり、マルウェアをダウンロード・実行して請求画面が消えなくなるといった被害に遭うこともある。

## 4. 学内 LAN の活用

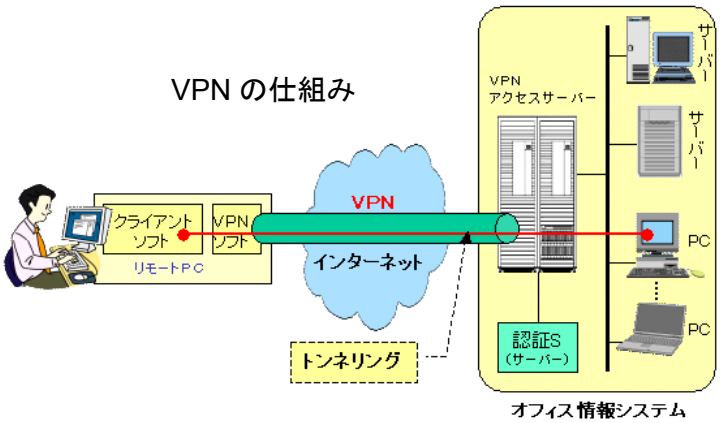
§2. で述べたとおり、麗澤大学を含む教育機関や企業などは、LANを構築して複数のコンピュータを接続し、ユーザー認証のしくみを使って正当なユーザーがコンピュータを利用できるようにしている。ユーザーはLANに接続したコンピュータにログオンし、プリンターなどのハードウェアを使ったり、データを保存したファイルサーバにアクセスする。ハードウェアやデータなどの資源（リソース）を共有することで、多数のユーザーが効率よく情報システムを利用することができるとともに、プリンターやディスクの購入コストを削減することができる。

LANは殆どの場合、インターネットに接続されている。ユーザーはLANの中のリソースを使うだけでなく、インターネット上のサービスにもアクセスすることができるが、内部の情報を守るため、外からLANの内部にアクセスすることは厳しく制限されている。LANとインターネットの接続部分には、ファイアーウォール(firewall, 防火壁)と呼ばれるシステムが常時稼働しており、外部からの侵入や攻撃を検知し防御するとともに、LANの内部からウィルスなどマルウェアのダウンロードがおこなわれないよう監視しているのである。

もちろん、サービスの中には学外から直接アクセスする必要があるものもある。例えば、Webページを公開するWWWサーバーや電子メールの送受信をおこなうメールサーバーは、LANの外に置かれる場合もあるし、LANとインターネットの中間に「非武装地帯(DMZ)」というインターネット側からもアクセスできる特別な場所を作り、そこに置かれる場合もある。(麗澤大学の場合、外部公開用のWWWサーバーのほか、「学生用Webシステム」などがDMZに置かれ、LANの外からもアクセスできるようになっている。なお、LANの内側に置かれている内部用のWWWサーバーはLANの外からアクセスできない）これらのシステムは常に外部からの攻撃にさらされるため、LAN内部とは区別して厳しく管理されている。また、外部公開用のWWWサーバーにある内部用のWebページはLANの外側からアクセスできないように設定されている（右上図参照）。




一方で、学外からLANの内部のリソースにアクセスしたい場合がある。例えば、自宅のパソコンからファイルサーバの[user-id]（Xドライブ）に保存されているレポートファイルを開きたい、学内LANの中で利用できる語学学習システムで学習したい、といった場合である。

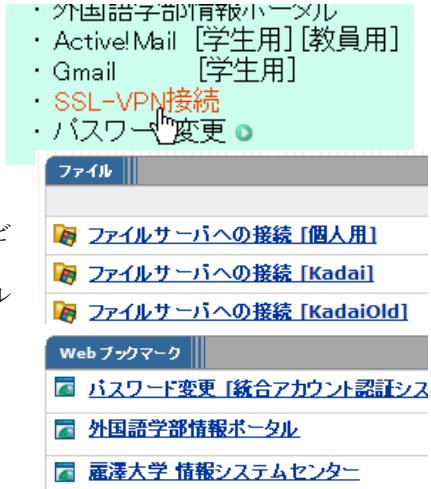



IPA「リモートアクセス環境におけるセキュリティ」より

さらに、最近、新型インフルエンザや鳥インフルエンザなどの感染症の流行(いわゆる「パンデミック」)の発生により、大学が長期にわたり閉鎖されるなどの事態が起こる可能性がある。このような場合、学生が自宅PCなどから学内の資料を閲覧し、授業に代わる課題を実施することで、学習の中断を最小限にとどめることが期待される。

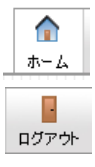
このような要求に対応するには、インターネット上から情報が不正に読み取られたり、不正にLANにアクセスされることを防ぐ、セキュリティ対策を施したリモートアクセスシステムを導入する必要がある。

麗澤大学情報FDセンターでは、外部からLANにアクセスするためのVPN（Virtual Private Network）を使ったトンネリングのしくみを提供しており、暗号化の仕組みである SSL (§2参照）を使い、学内むけに公開されたWebページやファイルサーバを安全に閲覧・利用することができる。




**実習 6：SSL-VPN 接続**サービスを使って、Xドライブをはじめとする学内のリソースにどのようにアクセスするかを確認しよう。

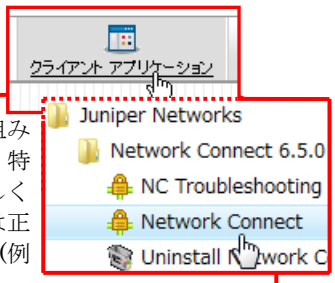
1. 情報FDセンターのホームページを開く
2. 「SSL-VPN接続」をクリックし、アカウント情報を入力してSSL-VPNサービスにログインする
3. Webブラウザに学内のファイルサーバの接続リストが表示される。「ファイルサーバへの接続[個人用]」を開き、Xドライブの内容が表示されることを確認しよう
4. 「ホーム」ボタンでSSL-VPNサービスの最初の画面に戻る
5. 「Webブックマーク」にある情報FDセンターのリンクを開く
   ※ このやり方で開いた情報FDセンターのホームページの



URLはVPNを経由しているため特殊なアドレスに変換されている（ブラウザのアドレスバーを参照するとよい）

6. 「ログアウト」ボタンを押してログアウトし、SSL-VPNを終了する

※ 自宅PCなどで情報FDセンターのホームページを開き、SSL-VPNを使って学内むけマニュアルやMoodleの各クラスのコースページにアクセスできることを確認しよう。




**注意**：SSL-VPN は、簡単な手続きで学内 LAN にあるリソースを閲覧するための仕組みである。学内の WWW サーバーが提供する Web ページは、SSL-VPN で閲覧する際、特殊な URL に変換されて表示される。このため、ページによっては SSL-VPN では正しく利用できない(例えば学内の TOEIC 学習システム「NetAcademy」は SSL-VPN では正しくアクセスできない。また Moodle でも一部機能が正しく表示されないことがある(例えばテキストのリッチテキスト編集ができない(テキストの編集・保存はできる)など)。

学内にあるこれらのリソースを学外から利用するためには、SSL-VPN ではなく Network Connect というサービスを使う必要がある。Network Connect を使うにはヘルプデスクに「リモート接続サービス利用申請書」を提出する(ノート PC やスマートフォンを学内無線 LAN に接続するサービスとは別の申請書となる)。

## 5. 参考になる WWW ページ

「ネット社会の歩き方」 http://www.cec.or.jp/net-walk/

「ネチケットホームページ」 http://www.cgh.ed.jp/netiquette/


（一般財団法人 コンピュータ教育推進センター）


（千葉学芸高等学校）

「インターネットを利用する方のためのルール&マナー集」 http://www.iajapan.org/rule/

「情報社会の光と影 IT リテラシー」 http://www.e-kokoro.ne.jp/m-literacy/

「国民のための情報セキュリティサイト」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/


（財団法人インターネット協会）




（文部科学省）


（総務省）

情報処理推進機構（IPA）セキュリティセンター「リモートアクセス環境におけるセキュリティ」
http://www.ipa.go.jp/security/awareness/administrator/remote/

（以上）