電脳講座（最終回）

裏ネット･セキュリティ講座

2003 年 1 月 8 日

基礎演習Ⅰ鎌田ゼミ電脳省

〔目次〕

1. 「2ちゃんねる」講座

――新しい情報コミュニティとメディアリテラシーについて

URL: http://www.2ch.net

■「２ちゃんねる」とは何か？

「２ちゃんねる（２ちゃん）」というのは、インターネットの一つのウェブサイト（ホームページ）です。このサイトには掲示板しかありませんが、しかし掲示板は鎌田ゼミホームページのように一つだけあるのではなくて、膨大な量の掲示板があります。それぞれの掲示板は「政治・経済」「芸能」「ゲーム」といった具合にジャンル分けがされていて、それぞれの掲示板ではそのジャンルに沿った話題のみが繰り広げられています（ジャンルと関係ないことを書き込んだら板違い・スレ違いなどと言って怒られます）。

■２ちゃんのどこが新しくて、何がすごいのか（諸刃の剣）

「２ちゃん」の革命的なのは、ひとつには上に書いた通り「膨大なテーマの掲示板が一つのサイトにまとめられている」ということです。もうひとつは「匿名で書き込み」という点です。勿論、どんな掲示板でも本名で書き込まなくてよい以上、匿名であると言えるわけですが、ハンドルネーム（インターネット専用のニックネーム）を使うことが多いで

す。しかし２ちゃんではハンドルネームすら使わないことが普通で、そこに書き込まれている情報は文責を持った誰の意見でもない「名無しさん」の独り言であると言うことが、２ちゃんの「すごい」ところなのです。普通は誰それが書きましたという文責を負ってこそ、まともで有用な情報であると考えられるのですが、逆に２ちゃんでは、その情報を提供するとき、文責という社会的な責任を負う必要はない。そのため各テーマに関して自由な意見を言い合えるのです。ここではIPアドレス（どこからアクセスしているかを示す「住所」のようなもの）も管理者以外が割り出せないようになっており、ほぼ完全な「言論の自由」が保証されています。あまりに革命的なために、企業から「不当な誹謗中傷を受けた」と提訴され、賠償命令の判決が下された事件がありましたが、それを読んだひとはもちろん、書き込んだひとも賠償金を支払う必要はありませんから、安心して利用しましょう。（ただし、警察沙汰になった場合、２ちゃん管理人は書き込み者のIPアドレス等を提出する場合があるとのことです。当たり前ですが無根拠な誹謗中傷はやめましょう）

■２ちゃん用語の解説

・板、スレッド、レス

まず大きなジャンル分け（といってもかなり細かくわかれていますが）がされているのが「**板**」です。例えば、２ちゃんの左のフレームに表示されている赤字のジャンル名の「政治・経済」の下に青字で並んでいる「政治思想」「ゴーマニズム」「金融」というのが、それぞれ「板」と呼ばれるものです。それぞれの「板」の名前をクリックして表示された画面をスクロールすると、ゾロゾロと「1: 議論の効果ってあるのか？ (24)　2: 天皇制　に賛成しる！！（.ㅁ∀ㅁ ）(631)　3: ここはコヴァ人口とサヨ人口どちらが多いんだい？ (62)……」といったような（必ずしもこうではないと思うが）ことがらが書いてある部分が出てきます。これがそれぞれ「**スレッド**」になっています。スレッドのタイトルの青字をクリックすると、実際のスレッドが表示されます。それぞれのスレッドでは、ジャンルに関連するトピックで問題提起や質問し、そこに「**レス**」のかたちで色々な人がどんどん意見を述べていきます。

・age/sage

２ちゃんでは膨大な板があり、またそれぞれの板には膨大な数のスレッドがあります。このスレッドは、人気の良し悪しで順番が入れ替わるようになっています。あるスレッドでレスを書き込むとそのスレッドは上に上昇します（age＝あげ、と言う）。また、順位を下げたい場合には、書き込み画面のメール欄に「sage」と書き込むと、そのスレッドは「下がり」ます。

・逝ってよし、鬱だ氏のう、禿同

２ちゃんは今でこそ誰でも使うお茶の間コミュニティ化していますが、それでもやはりオタク（＝geek）たちの臭いがのこる特殊なコミュニティであるといえます。オタク・コ

ミュニティに付き物なのは特有の隠語です。もちろん２ちゃんも例外ではなく、様々な「２ちゃん語」が発明されてきました。黎明期には「ｷﾞｺﾊﾊﾊ（＝「ギャハハハ」の意。親指シフトという特殊なキーボードで誤入力したものが元になっているらしい)」や、「逝ってよし（＝「逝去」の逝く、だがバカとかアホとかいうニュアンスに近い)」といったものが使われましたが流行り廃りがあり、２ちゃん語は日々つくられています。詳しくは２ちゃんの書き込みや２ちゃん用語集を参照し、習得してください。日常会話での２ちゃん語の使用は程々に。(例えばここ→http://majiwota.hp.infoseek.co.jp/dictionary.shtml)

■利用するときに気をつけること

・情報をうのみにしない。

誰が書いたのかわからない情報です。組織に隠匿された真実を暴こうとする人の書き込みもあれば、そういう正義感溢れるひとの勘違い発言もありますし、また誰かを陥れようとするウソの情報もしばしば書き込まれます。これらの情報を見分ける目を養ってください。言葉のプロレスのごとき暴言の数々に、最初は見ていてストレスがたまり、見るのも嫌になるかも知れません。しかし話半分の気持ちで見ればなかなかに有用な、他では得られないような情報が得られることも多いです。

・無駄な書き込みをしない、そういう書き込みを見つけたら放置プレイ。

自由と野放図をはき違えないでください。ストレス解消のはけ口として少々２ちゃんを使うのは悪いとは言いませんが、過度の破壊行為はいけません。また、上に書いたとおり２ちゃんは「言論のプロレス」とも言うべきある程度のルールに基づいて攻撃しあっているところもあります（最近はそのようなマニアックな使われ方は以前より減ってきてはいますが)。プロレスはスポーツです。悪ノリはやめましょう。怪我します。

また、アスキーアートと言って文字列だけで絵を表現する、大変な芸術作がよく書き込まれていますが、これも無駄に他人のつくったアスキーアートを掲示板に貼り付けまくったりするのはやめましょう。いたずらするのにもセンスが必要なのです。センスのない人はいたずらなどするのはやめましょう。遊び心のない人は真面目に生きるよりほかに道はありません。

・個人攻撃されたら

これはどこの掲示板で攻撃された場合にも言えることですが、相手がいわゆる「荒らし（掲示板の雰囲気を損なわせることが目的の書き込み者)」の場合、相手はあなたが激昂する様を見て楽しみたいがためにあなたを攻撃している場合が多いです。この場合、あなたがどんなに冷静に客観的に反論を書き込んでも、ほとんど無駄だと思ってください。言うなれば相手はガキ（厨房＝中坊という言葉もあります）なのであって、まともにとりあうだけ時間の無駄です。放置しましょう。悪質な場合には、管理人に連絡してください。

2. 「WinMX」講座

――P2P ファイル共有と著作権のありかたについて

URL: http://www.winmx.com

■「WinMX」とは何か？

「WinMX」というのは、ひとことに言うと「ファイル共有ネットワーク」です。WinMX のサービスを利用しているユーザー同士が直接、いろいろなファイルの交換をすることができるサービスなのです。大変素晴らしいシステムなのですが、多くの問題を抱えています。歴史的にも紆余曲折があり、また今後もごたごたが予想されます。

■WinMX サービスの使い方

まず、WinMX のホームページ（www.winmx.com）にアクセスすると、「NEW! Version 3.31 Available Now!」という青い文字の表示が出てきます。ここをクリックするとダウンロードページに進み、WinMX をダウンロードすることができます。ダウンロードできたら保存したファイルのアイコンをダブルクリックしてインストール手順に従ってください。インストールが完了しソフトを立ち上げたら、まず接続する画面が出てきてここで接続できたら（Connection Status のところが「Ready」と表示される）接続完了です。画面上の方の「search」をクリックして、後は好きにしてください。

■何が問題なのか？

WinMX のような P2P 型ファイル交換サービスの元祖として、Napster というのが昔（3 年くらい前）ありました。Napster は音楽ファイルだけを交換するものだったのですが、ちょっと工夫することで、実質どんなファイルでも交換することができました。この元祖 P2P ファイル交換システムはアメリカの大学で大流行しましたが（あまりに流行りすぎて、大学のネットワークを圧迫したために「禁止令」が出た大学もあるほど)、メタリカとかいうバンドや全米レコード工業会(RIAA)に提訴され敗訴して去年消滅しました。

問題なのは、このシステム自体なのではなくて、ここで著作権の発生するデータを公開することが、現行の法律では違法であると言うことです。つまり、WinMX コミュニティで一般的に行われている営みのほとんどは違法行為であるということです。そのことが倫理的あるいは哲学的に問題であるかというのはまた別の話ですが、ソクラテスも云々言った通りです、注意しましょう。

■ふぐは食いたし……

WinMX はとても魅力あるツールです。このシステム自体は合法ですが、ここで著作権を

伴うファイルを他人に公開することは、著作権法で禁止されています。実際違法ソフトやわいせつ画像を公開した WinMX ユーザーの中から逮捕者がでています（見せしめの印象も強いですが)。一般に P2P サービスは取り締まりのしようがないと言われていますが、使い方によってはこれが違法であり、また処罰の対象にもなりうることを知っておいてください。

■別の危険性

WinMX で共有されているファイルの中には、zip という形式で交換されているものも多いです。これは、いくつかのファイルを一つにまとめて、合計サイズも小さくするといういわゆる「圧縮ファイル」なのですが、この zip ファイルの中にウィルスが混入している危険性が非常に高いです。ウィルスの詳細については後の章で詳しく紹介しますが、ウィルスに感染したら、簡単に言うと、あなたのコンピュータは破壊されます。つまり、データがめちゃくちゃにされて起動できなくなるばかりでなく、あなたが今までつくったレポートやデジカメで撮った写真やインターネットからダウンロードしてきたデータ全てが、復元不可能なかたちに破壊し尽くされます。ウィルス対策法についても後述しますが、基本的な対策としてはウィルスの発生源に近づかないことが肝心です。WinMX もまた然りで、著作権云々の問題のまえに、ウィルスによってあなたのコンピュータがダメになる可能性が高いのです。注意してください。というより、我々電脳省は WinMX の使用をまったくお勧めしません。

3. その他、〈アングラ〉というもの

――危険がいっぱいのアンダー･グラウンド(まったく非推奨)

■アンダー・グラウンドとは何か？アングラがアングラであるわけ。

アンダー・グラウンド（アングラ）というのは、その名の通りインターネット社会の影に隠れて生きるコミュニティのことです。アングラの巣窟はウェブサイト（ホームページ）であるとか、先ほど紹介した WinMX などです。そこでは、いろいろな「やばい」モノ・情報が取り引きされています。アングラがアングラである所以は言うまでもなく、それが違法なことだからです。ここで取り引きされているヤバいものをいくつか、参考程度に紹介しておきます。

■エミュレータ

エミュレートというのは、何かの疑似動作という意味です。一般的にエミュレータと言うと、いにしえのコンピュータや機械をソフトウェアで再現して動かすということなのですが、アングラにおいてこれは、ゲーム機器のエミュレータのことを指します。古くはファミコンからプレステ（２はあったのかなかったのか不明）まで、あらゆるゲーム機のソフトをパソコン上で再現してみせます。エミュレータ自体合法のモノもあるのですが（ばっかりではないが)、ソフトのデータに著作権法違反のファイルが多々存在します。このエミュレータしかり、下に紹介する「割れず」なり MP3 なり、インターネットのアングラで流通するものは著作権がらみのものが多いです。

■割れず(Warez)

コンピュータのソフトをパッケージの CD-ROM からコピーして、インターネットで公開できるようにしたものです。昔は Warez サイト（Warez.com）などで公開されているものが多かったのですが、最近では WinMX で交換されています。ウィルスが混入している場合があり、非常に危険です。

■MP3(もせ)

CD などの音楽ファイルを変換して作る、インターネットで公開できるような小さいサイズのファイルです。昔はホームページやホットラインというシステムで公開・交換されていたことが多かったのですが、最近ではもっぱら WinMX が主流です。これも著作権がらみで違法です。

■注意

はっきり言っておきますが、ここで仕入れた程度の知識でアングラに踏み込むと、取り

返しのつかないことになります。おどしで言う訳じゃありませんがかなり危険なことです。人間の欲望につけ込む罠がアングラサイトには数知れずあります。興味本位でこれらのサイトに立ち入るのはやめましょう。何か起こってからではどうにもなりませんし、また仮に何かあっても当方は一切責任を負いません。

■だから何？

さあ……。

4. セキュリティ講座･オンライン編

――ウィルス･クラッキングから自分のパソコンを守る

■「オンライン」であることの恐怖

オンラインとは、ネットワークでつながれていけいけの状態のことを言います。オンラインであることは大変素晴らしいことです。それと同時に、大変危険なことです。素晴らしいのは、ネットワークを介して私たちが情報のやりとりをできるからです。危険なのは、見ず知らずの人間に情報を盗まれたり、とんでもないファイルを送りつけられたりする可能性があるからです。便利さには危険が伴うことは当然のことで、私たちはネットを利用してその便利さを享受するかぎり、安全について考え自衛しなければなりません。それは、無人島にでも住まない限り、自分の家に鍵を付けなくてはいけないのと同じことです。一般的な対策について、これから紹介します。

■ウィルスとは何か

ウィルスと言うと、どうしてもインベーダーや小学校の時に見せられた虫歯菌のイラストを思い浮かべてしまいますが、コンピュータウィルスはそういう姿をしていません。一見、普通のソフトやファイルと同じような姿をしています。ただし、普通とちがうのはそのソフトなりファイルなりが破壊的な振る舞いをするという点です。例えば、あなたのハードディスクのファイルを全部消去してしまったり、あなたの個人情報をメールで知人に勝手に送りつけてしまったりするのです。

ウィルスを作るのには特別な知識は要りません。例えば、私たちが秋学期に勉強したVisual Basicのマクロで簡単に作れるものなのです。つまり、ごく簡単なプログラミングの知識さえあればウィルスの作成は可能なのです。ちょっと大きな本屋に行ってコンピュータ書のコーナーに行けば、「ウィルスの作り方」などと書かれた黒表紙の本がたくさん平積みにされています。ですから、逆の立場から言えば、こういったウィルスに感染しない

ようにするために十分に対策をとっておく必要があるのです。

■ウィルス対策にはどうすればよいか

まず何よりも大切なのは、メールで送られてきたりやダウンロードしてきた、怪しいファイルをやみくもに開いてみないことです。特に、「(ファイル名) .vbs」というファイル名のものはかなり危険です。まったく知らない人からそういうファイルが送られてきた場合、99%ウィルスだと言ってもよいでしょう。それ以外の形式のファイルでも危険は伴います。見ず知らずの外国人がジェニファー・ロペスのプライベートショットを送ってきてくれるはずがありません。迷わず削除しましょう。

それでも避けられない場合もありますので、インターネットに接続しているコンピュータには、ウィルス対策ソフトというのを導入しておいた方がいいです。市販のものでは「ノートン。アンチウィルス（http://www.symantec.com/）」や「ウィルスバスター（http://www.trendmicro.co.jp)」が一般的です。実際ウチのパソコンもノートンのおかげで何度となく救われています。パソコンの中にはこういったソフトがあらかじめインストールされているものも多いようですが、しかし「半年限り」などといった期限付きのものが多いようです。期限が切れた場合はすぐに継続利用を申し込むようにしましょう。持ってないと言う人は購入を検討してください。

お金がないという人は、無料のウィルス対策ソフトとして、AVG 6.0 Free Edition（www.grisoft.com）というものもあるので、これでもいいかもしれません。このソフトの日本語の説明についてはこちら→（http://ryulife.com/net/avg.html）を見てください。

■マイクロソフトが危ない

Windows ははっきり言って、バグだらけのとんでもないソフトです。セキュリティの面でも非常に怪しい。これが家ならば欠陥住宅なのですが、ソフトウェア界というフロンティアにおいては、だれもビル（ゲイツ）に攻撃しないのです。

Windows では「Windows Update」といって、自動的にバージョンアップする機能が搭載されています。インターネットに接続しているなら、新しいバージョン（修正版）を自動的にダウンロード、インストールすることができます。普通はパソコン起動時に自動的にチェックするようになっていますが、こまめに確認するようにしましょう。

また、Windows に付属のメールソフト Outlook Express(OE)や、ブラウザ（ホームページ閲覧ソフト）Internet Explorer(IE)もまた危険です。できることなら、別のソフトに乗り換えることをお勧めします。メールに関しては、Becky!（www.rimarts.co.jp、4000 円）や無料の EdMax（www.edcom.jp）がお勧めです。ブラウザでは、Opera（jp.opera.com）や Mozilla（www.mozilla.gr.jp）があります。

■ファイアウォール

ファイアウォールというのは、「語源は炎を防ぐ壁という意味ですが、転じてセキュリティなどの防御システムのことを指します。パソコンで言えば、クラッキングを防ぐプログラムのことを指しています。本来の役割はパソコンへの外部からの不正進入を防ぐことです。それを実現するための仕組みとして・パケットフィルタリング・不正アクセスの監視の二点を主におこないます」ということだそうです（ryulife.com/net/firewall.html）。

WindowsXP ではファイアウォール機能が搭載されているのですが、それ以外の OS でファイアウォール機能を導入したい場合は、市販ソフト「McAfee.com インターネットセキュリティ（www.sourcenext.com）」や「ノートン・インターネットセキュリティ」を購入してください。

■プロクシ

プロクシというのは「代理」という意味で、あなたのパソコンの代わりにネットの情報を取得してくれるサーバのことです。あなたがどこかのホームページを訪問するとき、そのページには IP アドレスというものが記録され、どこからアクセスしたのか等が、ホームページ管理者に知れてしまいます。ここから様々な個人情報が流出する危険性もあるのですが、プロクシを利用することで、情報の漏洩を防ぐことができます。

プロクシサーバはあなたが契約しているプロバイダに用意されているものもありますが（各自確認してください）個人情報を知られないようにするためには、「公開プロクシ」というものを使うことをお勧めします。Yahoo!などで「公開プロクシ」と検索してください。そこで見つけてきたプロクシを、インターネットブラウザで設定します。Internet Explorer を使っている場合には「ツール」メニューから「インターネットオプション」で設定できます。「インターネットオプション」ウィンドウの「接続」を選択して、「設定」をクリックすると、プロクシのアドレスを入力をするところが出てきますので、そこで抜かりなく設定してやってください。

最後になりますがこんな素人の文章よりもこっちの方が余程役に立つかと思われますので紹介しておきます。「竜の情報館」http://ryulife.com/net/index.html

5. セキュリティ講座･オフライン編

――大学･自宅でのトラブルを防ぐための心掛け

■渡る世間は……

オンラインでの危険性とその対策については前の章で書いた通りです。しかし、あなたの安全を脅かす者は、必ずしもネットワークの向こうにいるわけではありません。ごく原始的で、しかし実に様々な方法でトラブルに巻き込まれる危険性があります。例えば、ハッキングと言っても専門的な知識でネットワークに侵入するばかりではなく、あなたがコンピュータでメールを読んでいるところを、後ろの席から盗み読みされているかも知れません（これを「ショルダー・ハッキング」と言います)。こういったオフラインでのセキュリティに関しても十分に注意し対策する必要があります。

■大学でトラブルに遭わないために

・パスワードをこまめに変更する

春学期の最初に口うるさく言われたことですが、実際にやっている人はほとんどいないように思います。人がたくさんいるコンピュータ教室や大学図書館で毎日同じパスワードを使い続けることは危険です。少しでもリスクを軽減させたいのなら、こまめにパスワードを変更するべきです。

・パスワード付きスクリーンセーバを設定する。

図書館で座席を確保するつもりなのか、カバンをおきっぱなしログオンしっぱなしにして､長時間退席している人が多いですが､普通に考えてこんなに危険なことはありません。三田キャンパスの異常な治安の良さがあってこそなのですが、いつトラブルが起こっても不思議ではない状態です。できれば対策をしておくべきでしょう。

大学のコンピュータには Windows2000 がインストールされていますが、これには標準機能として「スクリーンセーバ」というものが搭載されています。スクリーンセーバというのは本来、ずっと同じ画面を表示し続けてモニタ画面が焼き付かないようにするためのソフトなのですが、これをセキュリティ目的に利用することができます。

スタートメニュー（画面右下にある「スタート」と書いてあるところ）から「設定」さらに「コントロールパネル」を選択します。するとアイコンがずらずらっと並んだウィンドウが出てきます。「画面のプロパティ」をダブルクリックして開き、「スクリーンセーバー」を選択して、「待ち時間（席を離れて何分でロックがかかるか)」と「パスワードによる保護」を設定してください。

・印刷しようとしたものの行方を追え

特にプリンタのトラブルが多いⅡ号館の 108 教室で見られるのですが、印刷を実行したあと、エラーでプリントできなかったときに別のプリンタで印刷して、失敗した方はほっ

たらかしにするのは、結構危険なことです。特に、レポートなどの印刷でこれをやるのはかなり危険だと言えます。なぜなら、エラーが復旧したときにはあなたの印刷しようとしたものがプリントされ、それが第三者の目に触れてしまう可能性が高いからです。これも今の三田の状況では考えにくいかも知れませんが、悪用されないとも言い切れません。自分でプリントしようとしたものは、全て自分で始末するようにしましょう。

エラーで印刷できなかった書類のキャンセルの仕方は次の通りです。まず、画面右下（時計表示の左となり）に並んでいるアイコンの中から、プリンタの絵柄のアイコンをダブルクリックします。そこで開いたウィンドウの中から、自分の印刷しようとしていたファイルをクリックし選択して、メニューから「キャンセル」（もしくは「削除」。どっちだったかな）を選んでください。これで印刷は完全にキャンセルされます。

・メールアドレスについて

セキュリティ自体とはあまり関係のないことですが、大学のメールアドレス（xxx@ksc.kwansei.ac.jp）を大事に使いたいのなら、あまりこれをやたらに他人に公開しすぎない方がいいです。どこのだれだか分からない人とやりとりする場合には、なるべくなら大学のアカウントは使わないようにして、別のアドレスを取得した方がいいと思います。例えば、MSN の Hotmail（http://www.hotmail.com/JA/）では簡単に無料の Web メールのアカウントを取得することができます。どうでもよい用途に使うことも多いので「捨てアドレス」等とも言われますが、便利ですのでどんどん利用しましょう。

■自宅のパソコンでの対策

私の高校の恩師が言っていたことですが「人間誰しも何か事情を抱えて生きている」ものです。あなたが家族に何を隠さなければいけないのかは分かりませんが、見られて困るプライバシーもひょっとしたらあるかもしれません。これをあなたのいない隙に家族に見られないために自衛する手段はあります。

・とにかくパスワード

これに尽きます。ただし相手は家族です。誕生日をパスワードにするなどという愚かしいことはやめましょう。

具体的には、WindowsXP を使っている場合、ログインでパスワードをかけることが考えられます。XP では起動したときにまずログイン画面があらわれます。多くの場合これをすっ飛ばして自動的にログインするようになっているのですが、ここでログインするユーザーとパスワードを入力しないとそのユーザーの領域を使用できないようにすることができます。一台のパソコンを何人かで共有している場合には便利な機能です。

設定方法は次の通りです。コントロールパネル（開き方は上記「スクリーンセーバ」のところと同じ）を開いて、そこから「ユーザーアカウント」を開く。「新しいアカウントを作成する」をクリックして、名前を入力して、「次へ」。アカウントの種類を「制限」に選

択して、「アカウントの作成」。この後、作成されたアカウント（コントロールパネル「ユーサーアカウント」の画面に新しい自分の名前が表示されてるはず）をクリックすると新しい画面が表示されます。そこで「パスワードを変更する」をクリック。「現在のパスワード」欄以外のところを記入して、「パスワードの変更」をクリック。これで完璧です。鉄壁です。

他にも、メールソフト（Outlook Express）の使用者選択でパスワードをかけることができたり、Internet Explorer の特定の「お気に入り」だけを隠蔽することができたり（これは Favorites 忍者、www.aa.alpha-net.ne.jp/wooky/というツールが必要。無料）します。というより基本的に、お互いのことを詮索しあわない良い関係を家庭で築きたいものです。