第3章　情報倫理

この章について

この章では、情報倫理、マナー、ガイドライン、規約、ルール、法律といった概念を扱います。最初に情報倫理とは何か、また情報化社会に参画するにあたってなぜ情報倫理が重要であるかということについて述べます。

また「危機管理」という観点から、コンピューターとネットワークを利用する際に注意すべき点について解説を行います。危機管理はリスクマネジメントと言い換えても構いませんが、どのようなリスクがあるかということを知ることで、無用なトラブルから身を遠ざけることができるようになります。

また法律、特に著作権法について知るのも重要です。コンピューターを利用するということは、情報を生産するか消費するかしているわけですが、どちらにしても扱っているのは情報という著作物です。情報を生み出すといってもゼロから生み出すのは至難の業です。アイザック・ニュートンは「If I have seen further it is by standing on the shoulders of Giants. （私がより遠くを見渡すことができたとしたら、それは巨人達の肩の上に立ってのことだ)」と書簡で述べたそうです。実際のところは膨大に積み上げられた先人の知見を勉強するので精一杯、といったところかもしれませんが、新たな知見を付け加える前に、まず巨人の肩の上に立つ方法を学ぶことにしましょう。

3.1　情報倫理とは

「情報倫理」と聞くと、どのような印象を持つでしょうか。あれをしてはいけないとか、これをしてはいけないといった規則を集めた、「ダメダメ集」を想像する方が多いかもしれません。学者同士が行っている机上の議論に過ぎない何かで、自分には何の関係もないものであると考えるでしょうか。または、高校で勉強した（かもしれない）倫理の授業と重ね合わせて、情報と倫理がどうやって結びつくのか疑問に思うかもしれません。

「倫理」とは、「道徳規範」とされます。広辞苑第 6 版によれば、道徳とは「人のふみ行うべき道。ある社会で、その成員の社会に対する、あるいは成員相互間の行為の善悪を判断する基準として、一般に承認されている規範の総体。法律のような外面的強制力を伴うものでなく、個人の内面的な原理」とされます。

情報倫理も倫理という名が付いているようにこの定義を応用したもので、したがってある種の規範であるということになります。具体的には、情報化社会における規範を考える学問であるということができます。

ただし、「ある社会で」という点に注意が必要です。つまり、時代や前提とする条件によって倫理は変わり得るということです。過去において、例えばギリシャ・ローマ時代の倫理学者が述べてきたことは現代に通じる点もあるかもしれませんが、それがそのまま現在も妥当性を保ち続けているとは限りません。情報倫理も同じで、「情報」という言葉に含意される事柄が変化すれば、倫理上検討すべきであると認識される状況も、またその解答も（あるとすれば）変化するのです。

まとめると情報倫理は「情報化が進展している社会において、その情報化の進展に即しながら、社会的規範について考える学問である」と考えることができます。

ある行為の社会的規範といっても実際にはあまり難しいことではなく、コンピューターでキーを押して何かを入力する、クリックするといった程度のことでしかありません。従って、我々が何気なく行っている日常的なコンピューターの利用がどのような意味を持っているのかということについて、改めて考え直すといった程度に考えてもらって構いません。

情報倫理のもう 1 つの特徴が、その技術的な側面です。例えば、コンピューター教室において利用者が電子メールを受信したとすると、そのメールの内容は、情報としてはその教室の他のコンピューターにも届く可能性があり、単に破棄されているに過ぎず、その気になれば盗聴することもできる可能性があります（機器や設定の方法によっては届かないこともあります）。このようなネットワークの技術的な特徴は、通信の秘密という、憲法にも明記されている重要な規範に関する再検討が必要であることを意味しています。ここで重要なのは、そもそもその倫理的状況の理解に技術的な理解が必要であるという点です。

前述のように、情報倫理は情報化社会の進展に合わせて変化する可能性のあるものです。技術的な要件が変化すれば、その要件に合わせて行動規範も変化する可能性があり、そこで情報技術に関する原理的な理解が不可欠です。しかも、やっかいなことに情報技術の進展は非常に速いのです。しかし、コンピュータやネットワークの技術的な側面を仕事や研究の対象にしていない方がほとんどであると思いますので、必要に応じて技術の原理的な理解とその含意を学んでいくことにしましょう。

3.2　ガイドライン、ネチケット、マナー等と情報倫理の違い

情報倫理と混同されやすいのが、ガイドラインやネチケット、マナーといったものです。これらと情報倫理の違いはどのようなところにあるでしょうか。

例えば 1990 年代では、電子メールは 50KB 未満とし、これを超える場合は分割しなければならないということがよく言われていました[1]。これは、受け取る側がイライラせず受け取ることができる

[1] 50KB という容量は、ネチケットガイドライン（RFC 1855）の影響が強いものと思われます。過去の特定の環境において 50KB という基準がそれなりの意義を持っていなかったとは言えませんが、このガイドラインにも書いてあるように 50KB と

最大のメール容量かもしれません。この場合、これはマナーといえるでしょう。または、メールの受信者に関する何かしらの（主として通信設備やサーバー等の）事情を前提にしている場合は、一種のガイドラインであるとも言えます[2]。

しかし、これは情報倫理であるか、ということには疑問が残ります。コンピューターやネットワーク資源を過度に利用することは慎むべきですが、倫理といった場合、それは一律に決まるものではなく、状況に応じて個々人が合理的に価値判断して決めなければならないものです。

もちろん、これはネチケット、マナー、ガイドライン、ルールといわれるものを軽視してよいということではありませんし、この章の大半はこれらの解説に費やされます。しかし、情報倫理とは単なるルール集ではなく、自己の中にそのルールを形成するプロセスであり、このような自己責任による自己決定こそが、情報倫理とガイドラインの大きな違いなのです[3]。

情報倫理について理解するためには、技術的な背景の原理的な理解が不可欠であることは前述の通りです。知らなかったでは済まないのがこの社会の基本であるため、自覚のあるなしに関わらず、無知であることは社会との摩擦を生じかねないということになります。あるいは、犯罪の加害者や被害者になってしまうこともあり得ます。

逆に言えば、このような自己決定に基づく自己責任の原則が成立するには、社会的に見て一定水準の教育が確保されている必要があるとも言えます。また変化する社会状況に対応するため、情報収集とスキルの習得が適時適切に行われる必要もあります。

簡単に言えば、コンピューターやネットワークを利用し続ける限り、その技術的な背景とそれが含意するものについて勉強を続けなければならないということです。

本章では、このような考え方を前提にして、理解しておくべき基本的な技術的原理とともに、コンピューターやネットワークを利用する上で注意すべきいくつかの項目を提示します。いくつかはガイドラインであり、いくつかはマナーやモラルの範疇に入り、またいくつかは読者の倫理的な判断を必要とするものがあるかもしれません。

いずれにしても、これらの項目については、既に述べたように執筆時点で言えることばかりであって、将来に向かって正しいことは保証されていないことに注意してください。情報社会に自主的に、自らの合理性をもって向かっていくことこそが情報倫理において重要なのであり、それは誰かが押し付けるものではなく、仮に押しつけられたところで実際の活動に結びつかないでしょうから、そこには何の意味もないのです。

3.3 マナー：無用な摩擦を回避する

ここでは、マナーについて述べます。法律や学内規則で決められてはいいませんが、無用な摩擦やトラブルを回避するために知っておいた方がいいことです。ここでは、「ネチケットガイドライン」（RFC1855）[3] に沿って、1 対 1 の通信、1 対多の通信、情報サービスの利用の 3 つに分類して解説します。

3.3.1 1 対 1 の通信：電子メール

1 対 1 の通信の多くは、電子メールかチャットで行われます。ここでは、電子メールについて取り上げます。

いう数字はガイドラインが書かれた当時における経験則に過ぎません。

[2] Waseda-net が学生向けに用意しているメールの保存容量は 1GB ですので、これは決して他人事ではありません。Word や Excel 等のファイルを添付すると、メールのサイズは一気に膨れあがりますので、十分な注意が必要です。

[3] 自己責任による自己決定の結果、海賊版ソフトウェアをネット上で販売することになっては困りますから、その自己決定が社会的にみて望ましい価値を持っているべきでもあります。

電子メールに限らないことですが、誰かと情報をやり取りするときに注意すべき事は「送るときは慎重に、受け取るときは寛容に」です[4]。送るときにはマナーに忠実に、受け取るときは多少マナーや一般的な流儀から外れていても許す気持ちが大切です。全体的に、相手の立場になって考えるという、コミュニケーションに関する、ごく常識的な思考方法が重要なのです。

電子メールでは、まず形式的な要件を整えることが重要です。具体的には、メールを出す前にまず宛先（To）、カーボンコピー（Cc）、題名（Subject）[5]などのヘッダ情報を重点的にチェックしてください。

宛先 To は宛先です。Cc も同じようにメールが届くのですが、Cc は参考までに送信することを意味しています。意味上の違いはありますが、同じように届くことには変わりありません。To や Cc をしっかり確認しないと、意図しないメールアドレスへ情報を送信してしまうことになりかねません。いったん自分の手を離れた電子メールは、もはや自分でコントロールすることはできないことを覚えておきましょう。また、Cc とほぼ同じ機能だがメールの受信者一覧には載らないという Bcc（Blind Carbon Copy）という機能も利用することができます。多くの宛先に対して同時にメールを出したいが、全員がお互い顔見知りでない（例えば転居を知らせるメールなど）という場合などに使うと良いでしょう。

名を名乗る あなたが誰であるか、メールアドレスだけで判断できない場合がほとんどです。授業関連の連絡なら、授業名、学部や学籍番号も書いておくべきでしょう。また、仲の良い友人や家族を除き、自分の通称（あだ名）を名乗りつつメールを書くのは大変失礼なことです。

題名 学生諸君がよく忘れてしまうのが、Subject（題名）です。電子メールを 1 日数通しか受け取らない人ばかりではありません。数十から数百通のメールを受け取る人にとって、題名が適切に入力されていないメールは不親切であり、よって処理が後回しになる傾向が高いようです。また「こんにちは」とか「お願い」といった Subject はほとんど意味がないことも覚えておきましょう。

メールはすぐには読まれない すぐにメールを読んで対応してくれるだろうことを期待するかのようなメールも、よく見かけます。電子メールは非同期型の通信で、相手にメールが届くかどうか、また実際に読んでくれるかどうかすら保証されていないことを理解しておきましょう。

添付ファイル 添付ファイルの容量の大きさは今や相対的なもので、受け取る人の環境によって上限がまちまちですが、送ろうとしているファイルが少し大きいな、と思ったら相手にまず受け取れるかどうかを聞いてから送ると良いでしょう。

鵜呑みにしない 「ガセネタ」の電子メールが国会で話題になったことがありましたが、現在広く利用されている電子メールシステムでは送信時に偽装できない情報はほとんどありません。電子メールは、はがき程度の秘匿性・信頼性しか持ち得ないことを理解し、本当に重要な情報はメールでは送らないで手紙や電話にする、メールでなければならないのであれば暗号化するというように、通信手段を適切に使い分けることを考えましょう。

チェーンメール いわゆる「不幸の手紙」のようなものがチェーンメールと呼ばれているものです。以前は、ねずみ算のように送信されるメールを増大させるのでシステムに負荷をかけるため、チェーンメールはいけないこと、と言われていました。昨今はその程度の負荷よりも迷惑メールの方がよほど深刻ですので、負荷を気にする必要はないでしょう。チェーンメールを思わず転送してしまうのが問題なのは、そこに書いてあることを無批判に受け入れて、転送して

[4]ただし、教員については話が別です。教員は、学生諸君を指導する立場にありますので、学生諸君のメールについて批判的にならざるを得ません。

[5]要件、用件、件名など呼び方は様々なものがあります

しまうというところであると考えられます。2011 年 3 月 11 日に発生した東日本大震災時に、チェーンメール等の形で数多くのデマが拡散されたことも記憶に新しいところです。

転送設定に注意 メール転送機能を用いると、あるメールアドレスに届いたメールを、他のメールアドレスに自動的に転送できます。しかし、自動転送の設定内容を間違えると、見知らぬ第三者へメールが転送されるとか、２つのメールアドレスの間でメールを転送しあって、いわゆるループ状態になるなど、他人への被害を引き起こします。ループとは、メールサーバ間でメールが転送され続ける現象を指します。例えば図 3.1 のように設定してしまうと、携帯電話のメールアドレスに届いたメールは Waseda-net に転送されますが、Waseda-net ではそのメールを携帯電話に転送してしまい、これが延々と繰り返されてしまいます。このようなループは、システムに大きな負荷をかけますので、メールの転送設定を行ったら、必ず意図した通りに転送されているか確認を行いましょう。

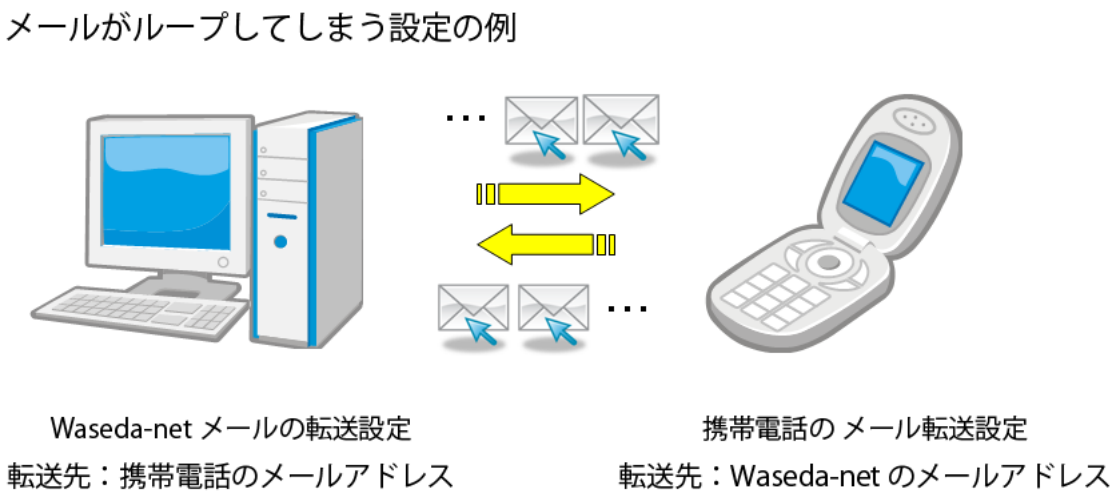

図 3.1: メールループの例

3.3.2 1 対多の通信

1 対多の通信では 1 対 1 で必要な配慮はすべてそのまま必要です。加えて、いくつか注意すべきことがあります。

相手が多数の場合、たいていの場合そこには何かしらのルールが存在しています。それが明文化されているか不文律であるかは関係ありません。そのルールから外れてコミュニティに参加し続けることは不可能です。メーリングリストや掲示板など、様々なツールがありますが、いずれの場合でも無用な摩擦を避けつつ参加するには、そのコミュニティのルールを良く知るのが重要です。

なお、1 対多のサービスとしてよく利用されるようになったのが、Twitter、Facebook、Mixi といった、SNS（Social Networking Service）がよく利用されています。これらのサービスを利用する 2010 年以降、これらのサービスを利用している、学生と思われるユーザーがカンニング、窃盗、盗難（万引き）、不倫、痴漢、飲酒運転、キセル（無賃乗車）といった違法行為を告白し、それがインターネット上で大きく取り上げられ、大学等に通報が行われる[6]ということが散見されるようになりました。

[6]いわゆる「電凸」です。

また、様々な SNS を横断的に調査して、問題の行為を行った者の実名、住所、所属などをインターネットの掲示板上に掲示する[7]ということも行われています。

これらのサービスを利用すること自体は問題がありません。また、犯罪的な行為が許されないのは言うまでもないことですが、それをインターネット上で開陳すると、それが事実かどうかは別として、それは当面の間、色々な方法で電子的に保存されてしまうということを理解して下さい。

つまり、コミュニケーションの対象が多数になった時点で、その対象は日本全体、あるいは世界全体であるということです。

3.4　リスク管理：被害者にならないために

3.4.1　インターネット上の詐欺行為

インターネットは、以前は商業利用することができなかったのですが、一般に開放され、またショッピングなどの経済活動が活発に行われるようになり、それにつれて犯罪者も増加しました。必要以上に恐れる必要はありませんが、高度な技術を持って真剣に、仕事としてコンピューター犯罪を行っている者がいるということは覚えておきましょう。ここでは特に詐欺行為に注目して説明します。

フィッシング詐欺

fishing（魚釣り）をもじった、phishing[8]という種類の詐欺です。これはインターネット上において企業や組織の名前・Web サイトを偽装し、ユーザが入力した個人情報を盗み取ろうとする行為です。つまり、ユーザを騙して釣り上げてやろうということです。

大学や企業を装い「ユーザアカウントの有効期限が近づいていますので、登録内容の再入力をお願いします」などのメールを送信し、企業の Web サイトを装った偽の Web サイトへ誘導し、個人情報などを入力させるというのが典型的な手口です。

対策としては、メールで個人情報を送信しないということと、Web ブラウザーで ID やパスワードを含む個人情報を入力する際には、次の 2 点を確認して下さい。

- URL が自分の意図しているサイトかどうか
- SSL により暗号化されているか

フィッシング詐欺の場合、相手は例えば Yahoo!そっくりの Web サイトを用意し、そこに ID とパスワードを入力させようとします。そこで、自分がアクセスしているサイトが本当に Yahoo!のものかどうかをしっかり確認して下さい。Web ブラウザーが SSL を利用していれば、暗号化と相手先の確認の両方が同時に達成することができますので、個人情報を入力させるサイトでは必ず SSL を使いましょう。逆に言えば、正しく SSL を利用していないのに、個人情報や ID・パスワードの入力を求めるような Web サイトは、使うのを止めましょう。

ワンクリック詐欺

ワンクリック詐欺は、ブラウザー上で 1 回クリックしただけで（勝手に）サービスの申し込み（契約）が完了したと主張し、料金を請求してくるという詐欺です。次のような実例が報告されています。

[7] いわゆる「曝し上げ」です。

[8] 固定電話に特定の周波数の音を流すことによって電話システムを操作し、例えば無料で長距離電話をかけるという、ネットワーク犯罪の先祖のようなことが 1950 年代頃から行われていたようで、これを phone と freak を掛け合わせて作られた造語、phreaking と呼んでいました。「phishing」はこの造語を語源にしていると思われます。

- 興味本位でいかがわしい広告をクリックしたところ、突然「有料サイトに入会した」と表示された
- 「個人を特定した」とのメッセージとともに、いろいろな情報が表示され、怖くなったので不本意ながら支払った
- 携帯電話からインターネットに接続し、いろいろなサイトを見ているうちに、突然アダルト（出会い系）サイトにつながり、料金請求の画面が表示された

基本的な対策として、まずいかがわしい情報が書き込まれているようなサイトは閲覧しないということです。また、不特定多数の人が書き込める掲示板などには、このような詐欺行為を行うためのWebサイトへのリンクが設置されている場合があります。リンクを無自覚にクリックするのではなく、リンク先のURLをよく見て良く分からなければ安易にクリックするのは止めましょう。

実例のように「個人を特定した」としてIPアドレスやプロバイダ名が表示される場合がありますが、一般的に、ネットワーク管理者やプロバイダではない第三者がこれらの情報から個人を特定することはできないことを覚えておきましょう。同様に、携帯電話の機種名や個体識別番号などからも個人を特定するはできません。架空請求のWebページやメールの内容はもっともらしく書かれていますが、これを信じて支払いや返信をしないようにしましょう。

もし個人情報を入力してしまった場合や、しつこく何度も請求が来る場合は、決して料金の支払いや振込みを行わず、早稲田ポータルオフィスや都道府県の警察サイバー犯罪相談窓口に相談しましょう。

インターネットオークション詐欺

インターネットオークションは，店頭販売より安い値段で商品が購入できたり、販売が終了になった商品が購入できたりと大変便利ですが、詐欺行為もまた多く行われています。

- インターネットオークションで商品を落札後、代金を相手の指定口座に振込んだが、品物が届かず連絡も取れなくなった
- 品物は届いたが、中身が偽物またはガラクタだった

こうしたオークションについては、次のような対策が考えられます。

出品者の身元・連絡先を必ず確認する 名前・メールアドレス、振込口座だけではなく、住所や電話番号など身元をしっかり確認しましょう。また被害にあったときのことを考え、銀行振込み時の控え、取引を記録したメールなどをしっかり保存しておきましょう。

「エスクローサービス」業者を利用する エスクローサービスとは、売り手と買い手の間に入り、品物と商品の受け渡し確認を行い取引の安全を確保するサービスです。大手のオークションサイトではこのサービスを提供していますので、なるべく利用するようにしましょう。

高額な商品，ブランド品についてはオークションでの購入を避ける PCやオーディオ製品などの高額商品は自転車操業などの取引商品として扱われることが多いです。またブランド品は贋作の販売が多く行われています。これらの商品をオークションで購入することはお勧めしません。

3.4.2　オンラインプライバシーを守るための 12 の方法

詐欺行為以外に注意すべきなのは、プライバシーです。ここでは、Electronic Frontier Foundation（EFF）による「オンラインプライバシーを守るための 12 の方法（EFF's Top 12 Ways to Protect Your Online Privacy）」[9]を紹介します。

ネットワーク上でやり取りされる情報の経済的価値が高まり、またネットバンキングやクレジットカードを用いたショッピングのように、直接貨幣価値を取引する機会が増えています。これに伴ってコンピューター犯罪も、単なる愉快犯から金銭を目的とした犯罪へと大きくシフトしています。コンピューターやネットワークの正しい理解が無いまま無自覚に利用してはならないのです。

リスク管理の第 1 歩は、そこにどのようなリスクがあることを知ることから始まります。この点で、コンピューターやネットワークのセキュリティは広範で深い知識が必要です。コンピューターやネットワークを利用し始めたばかりの利用者にとっては、そもそもコンピューターで何ができるのかということすら分からないはずで、ここがコンピューターおよびネットワークのセキュリティの難しいところです。

しかし、この「12 の方法」はあまりコンピューターの知識が無くてもすぐに実践できることが多く書かれています。一部、技術的な解説が必要な点については後述します。

1. 個人情報を不用意に開示してはいけません。
2. Web ブラウザのクッキー警告表示を有効にし、クッキー管理ソフトを使いなさい。
3. 「クリーンな」電子メールアドレスを用意しておきなさい。
4. 見知らぬ相手や会ったばかりの「友人」に個人情報を公開してはいけません。
5. 職場では監視されているかもしれないと考えなさい。メーリングリストに個人的なメールは送ってはなりません。重要なファイルは自宅のコンピューターに保存しなさい。
6. 連絡先や個人情報と引き替えに賞金や賞品を提供するサイトに注意しなさい。
7. いかなる理由があっても迷惑メールに返事してはいけません。
8. Web セキュリティを意識しなさい。
9. 自宅のコンピューターセキュリティを意識しなさい。
10. プライバシーポリシーと保証のシールを吟味しなさい。
11. 自分の個人情報を、いつ・なぜ・だれに対して公開するのかを決めるのは他ならぬ「自分自身」であることを忘れてはいけません。
12. 暗号を使いましょう！

1、4、6、10、11 あたりにちりばめられていますが（それだけ繰り返したいことなのです）、最初に強調しておくべき事は「自分の個人情報を守るのは自分自身」という当たり前のことです。インターネットを利用していると、様々な場面で個人情報の提供を求められます。

ネット上では、サービスの提供を有償・無償で受ける際に個人情報の提供を求められるケースがほとんどです。有償の場合でも、サービスの提供に不必要な個人情報を求められる場合があります。ここで考えて欲しいのは、その後の自分の個人情報の行方と、そのサービスは個人情報を提供してまで利用したいものかどうか、ということです。

[9] http://www.eff.org/wp/effs-top-12-ways-protect-your-online-privacy を参照のこと。

それを考える際に参考になるのが、各社の掲げているプライバシーポリシーや保証のシール（プライバシーマーク等）です。プライバシーポリシーを設定していない企業のサービスは、どれだけ有用に見えても使うべきではありません。また、できるだけプライバシーマークや TRUSTe など、外部機関により認証を受けた会社であるかどうかを確認しましょう。

個人情報を考えるときに重要なのは、説明責任を前提とした自己決定です。なぜ、その個人情報を入力する必要があるのか、そのサイト (会社) は説明しているでしょうか。例えば、ショッピングサイトで住所を入力せずに購入したものを自宅に届けてもらうことは不可能です。では、生年月日を求められた場合、どう判断すべきでしょうか。例えば、そのサイトは顧客の年齢層を考慮した商品を勧めてくれるサービスを利用できるという説明をするかもしれません。実際のところ、そのようなマーケティング的な分析に利用されるはずですが、そのような情報を提供しても問題ないでしょうか？ここで問題があるか無いかは、自分で決めなければなりません。

これは懸賞のような、自分が何かしらの金銭的な支払いをしないときでも当てはまることです。自分自身の個人情報を対価として、一定の確率で当選するかもしれない賞品を得ようとするのが本質であることを理解しておきましょう。

また、個人情報である氏名や電話番号を入力することが求められていたとしても、必ずしも正しい氏名と電話番号を入力するべきではないケースもあるかもしれません。決して Web サイトの不正な利用を勧めているわけではありません。しかし、前述のように個人情報として提供すべき範囲もまた、利用しようとしているサイトの運営会社が決めることではなく、自分自身で決めることです。

Web サイトの入力フォームに何も書き込まなければ、自分の個人情報が何らかの形で流出する危険性はかなり減ります。しかし、それだけが個人情報ではありません。例えば、どのようなサイトを閲覧したかという履歴もまた、重要な個人情報です。インターネット上のコンピューターには、それぞれ IP アドレスという電話番号のように世界に 1 つしかない番号が付与されています。どの IP アドレスからのアクセスであるかということは、アクセス先に記録として残ります。

また、Web ブラウザには Cookie という仕組みが用意されています。Web は、ブラウザー（クライアント）がサイト（サーバー）に対して情報を送信するように要求し、サーバーからクライアントに情報が送られてくる（応答）ことで成り立っています。ここでは、ブラウザは主に情報のリクエストを行い、サーバーは専ら情報を送信します。つまり、情報はサーバーからブラウザに流れるのが主です。フォームもこのリクエストの一種なのですが、フォームさえ使わなければ情報が漏れないのかというと、そういうわけではありません。もう 1 つ、ブラウザからサーバーに情報が渡る道が用意されており、それが Cookie なのです。これは、おおよそ次のように動作します。

1. ブラウザがサーバーに情報を要求する
2. サーバーはブラウザに Web ページを送信すると共に、Cookie を送信する
3. Cookie の中には特定が可能なように大きな桁の、ユニークな番号が書いてある
4. ブラウザが同じサーバーにアクセスする
5. ブラウザからサーバーに Cookie が渡される

つまり、Cookie を用いると特定のコンピューターからのアクセスかどうかを特定することができるということです。不便なことばかりではなく、ID とパスワードを利用しなくてもログイン状態になるなどの利点もあります。このように便利な仕組みである一方で、プライバシー上の問題になりやすいので、きちんと管理しようというのがここでの趣旨です。

クリーンなメールアドレスとは、知人にしか教えないようなメールアドレスという意味です。ショッピングに利用したり、Web サイトに掲載したりするメールアドレスとは別のメールアドレスを用意しましょうということです。

最後に暗号化ですが、インターネットの基本的な特徴として、特に指定しなければデーターは暗号化されない状態で流れます。盗聴するのは必ずしも容易ではありませんが、暗号化には色々な意味で利点があります。可能な限り暗号化通信を利用するよう心がけてください。

3.5　ルール：加害者にならないために

無人島などで一人気ままに生きていくのでない限り、社会生活を送らなければならず、それはルールを守らなければならないことを意味しています。ルールとしては法律やガイドライン、規約など様々なものを考えることができますが、ここでは早稲田大学の関連規約で禁止されている行為を紹介します。

3.5.1　各種システムに共通した禁止行為

規約に定められた禁止行為は、各システムでほぼ共通しています。21 種類ほどの行為が共通して禁止されていますが、主なものを以下に挙げておきます[10]。

1. 自らのユーザ ID およびパスワードを貸与、販売、譲渡等により第三者に使用させる行為
2. 他の利用者のユーザ ID およびパスワードを不正に使用する行為
3. 他人を詐称する行為
4. システムの不正な利用またはそれを助ける行為
5. 営利を目的とした行為
6. 他の利用者、本大学または第三者の著作権その他の知的財産権を侵害する行為
7. 他の利用者、本大学もしくは第三者を誹謗、中傷しまたは名誉もしくは信用を傷つけるような行為
8. 他の利用者もしくは第三者の名誉、財産またはプライバシー等を侵害する行為
9. 詐欺等の犯罪に結びつく行為
10. その他法令および社会慣行に反する行為、または公序良俗に反する行為

禁止行為に関する記述は改訂される場合がありますので、MNC の Web ページを随時参照して、最新の規約を確認してください。

各規約に違反した行為があったと判断された場合、MNC では内容に応じて情報サービスの一時利用停止などの処分を行います。この処分とは別に、所属学部において学則に基づく処分が行われる場合があります。詳しくは、以下の Web ページを参照してください。また、ネットワークの利用に関して今までに学部が下した最も重い処分は退学であることを付記しておきます.

MNC 規約違反による処分について

`http://www.waseda.jp/mnc/LOCAL/RULES/breaking.html`

MNC では利用者がコンピュータやネットワークを使って何をしているのか利用履歴を記録し、一定期間保存しています。これにより，早稲田大学のネットワーク上での不正な行為があれば、MNC は行為者を特定できます。また、もし Waseda-net ID パスワードの貸与や盗難により、他者が不正行為を行ったとしても、それはその Waseda-net ID の持ち主の行為として責任を問われる場合がありま

[10] 詳しくは `http://www.waseda.jp/mnc/rules.html` を参照。

す。利用履歴の保存は早稲田大学で定められている「個人情報の保護に関する規則」に則って行われ、適切に利用している学生のプライバシーが損なわれることはありません.

個人情報の保護に関する規則

http://www.waseda.jp/kyomubu/new/kitei.html

以下では、禁止行為 21 項目のなかでも特に重要性が高いものについて、まとめて解説を行います。

パスワードの管理

学内ネットワークの利用は早稲田大学の学生および教職員に対して認められた特権です。これを大学の関係者以外に利用させる権限は、一般の利用者にはありません。利用者に交付されたユーザ ID は、その利用者のみが利用できるものです。パスワードは「他者の記憶は読み取れない」という事実に依拠した認証手段です。世界中で利用者本人のみが知っているという状態がパスワードを認証手段として利用する必要条件であり、他者に知られてはいけないものです。

このため、パスワードは適切に管理する必要がありますが、そのポイントは次の通りです。

パスワードは誰にも教えてはいけない たとえ知人や家族などであっても、パスワードは教えてはいけません。また聞いてもいけません。

パスワードは他人が見られる状態にしてはいけない パスワードをメモをした瞬間、他人の目に触れる可能性が生まれます。また、パスワードを入力しているところを他人に見られるのもリスクがあります。逆に、他の人がパスワードを入力しようとしている時は、マナーとして顔を背けましょう。

脆弱なパスワードを利用してはいけない 8 文字未満、文字種としてアルファベットの大文字・小文字・数字・記号を混ぜて使っていない、辞書に載っているような単語を使う、単純な規則の文字列を使うなどしてはいけません。

2009 年、アメリカで大規模なパスワード流出事故がいくつかありましたが、この時流出したパスワードを解析したところ、16%がそのユーザーの名前、14%がキーボードの並び（12345678 とか qwerty など）、4%が password という文字列ないしこれを少々いじったもの（passw0rd など）、5%がポップカルチャーの関連単語（pokemon など）やその改変、4%が身の回りで目に付いた単語（dell や apple など）、その他 iloveyou やスポーツ関連などだったという分析が行われています[11]。また、パスワード長で最も多かったのが 6 文字、ほとんど（約 95%）の人は 8 文字以下となっています。

「良いパスワード」を定義するのは非常に難しいのですが、こういった「悪いパスワード」は決して利用してはいけません。

一方で、良いとされるパスワードは文字種が入り交じって長いものです。これは、覚えられないパスワードを覚えろといっているようなものではありますが、できるだけ覚えやすくするような工夫を考えることができます。例えば、次のような文章からパスワードへの変換法則を作るのも 1 つの方法でしょう。

1. 自分の好きな適当な文を考える	寿司と言えばマグロ
2. ローマ字に変換する	sushitoiebamaguro
3. 適当にローマ字を数字や記号で置き換える	su410>mag6!
4. 適当に小文字と大文字を入れ替える	Su410>Ag6!

パスワードによる認証は様々な Web サイトでも利用されており、それぞれで違う ID とパスワードを登録しなければならないことが多いのが現状です。多くの ID とパスワードを使っていると 1 つずつの扱いが粗末になりがちですが、重要な ID とさほど重要でない ID にわけて管理しても良いで

[11] http://www.darkreading.com/blog/archives/2009/02/phpbb_password.html

しょう。Waseda-net のパスワードは履修登録から授業の課題提出にまで利用する重要なものであることを認識して、厳重に管理して下さい。

匿名と情報発信の責任、詐称

著作権法上、匿名でいる権利は保障されています。自分の作成した著作物について、氏名を公表するかどうかは著作者の自由に任されているということです（著作権法第 19 条)。匿名でもなお著作権は保護されますが、保護を受けにくくはなります。

一方で、匿名性にはいくつかの種類とレベルがあります。代表的なところでは日本国憲法第 15 条に規定されている秘密投票などを挙げることができます。このように、ある種の匿名性は民主主義の基礎をなすものであると考えられる、重要なものです。インターネット上でも、匿名で議論を行うことがある程度可能であり、それが自由で忌憚のない情報の交換を可能にしている側面があります。

しかし、ここで注意したいのが匿名性のレベルです。匿名であるはずのインターネット上の掲示板で、殺人予告などをして逮捕されたり名誉毀損で損害賠償請求されたりといったケースが後を絶たないことを考えれば、インターネットでは表面的な匿名性しか得られないことがほとんどであることが分かります（コラム参照)。

匿名を前提とした言動は、得てして無責任になりやすいようですが、思わぬところで足をすくわれて後悔することが多いようです。逆に、自覚的に真の匿名状態で発言したい場合は、それなりに準備して取り組む必要があるということです。

なお、他人を詐称することは匿名と異なり、どのような場合であれ一切認められません。これは、他人の ID を剽窃してなりすますことや、他人のふりをしてネットワーク上の活動を行うことが含まれます。

コラム インターネットと匿名性

「インターネットの匿名掲示板」「匿名の学校裏サイト」「匿名性の高いファイル交換システム」といった旨の説明がマスコミでよく取り上げられています。しかし、殺人予告を行って逮捕された者は枚挙にいとまがありませんし、Winny 等の「匿名性の高い」はずのソフトウェアを利用して著作権法に違反したファイル共有をしていると、国内外からあっという間に通報を受け、刑事・民事の責任を問われることになり、この例も枚挙にいとまがありません。
第 2 章で簡単に触れましたが、インターネットに接続されたコンピュータには、IP アドレスと呼ばれる、電話番号に相当する世界で固有の番号が割り振られています。コンピュータ同士で通信を行う際にはこの番号が必ず利用されます。そうでなければ、通信が成立しません。そして、多くの場合で通信相手は誰と通信を行ったのかという記録（これをログといいます）を残しています。
次に、その IP アドレスは誰が割り当てるかというと、大学やインターネット・サービス・プロバイダ（ISP）のような、末端のユーザにインターネットへの接続サービスを提供している組織です。そのような組織は、ユーザに IP アドレスを割り当てるにあたって、誰にその IP アドレスを割り当てたかというログを収集します。
この 2 つの情報と、問題の行為が行われた日時とを結びつけることで、最終的に誰が何をしたのかということが特定できるというわけです。
このように、インターネットは決して匿名性の高いシステムではないということを理解しましょう。

著作権関連

各種法令のなかで、大学において学生諸君が特に注意すべきものに、著作権関連の法律を守らなければならないということがあります。言論の府であるところの大学は、研究や教育を通じて広い意味でのソフトウェアコンテンツを生み出すことを目的とした機関であるからです。

著作権（Copyright）は、文字通り複製（copy）する権利（right）のことをいいます。見方や立場によって著作権については様々なトピックスがありますが、特にここでは大学における論文やレポートを格上で注意すべき点について解説します。実際には、他人の著作物をまったく利用することなく、新たな作品を生み出すというのは、ほとんど不可能です。ただし、誰かの著作物を利用するにあたっては、守らなければならないルールがあるのです。

ここで取り上げる著作権については、主なトピックが 2 つあります。1 つはソフトウェアとそのライセンス、つまり使用許諾契約です。もう 1 つが、文章の作成に関連したものです。

ソフトウェアの違法コピー

ソフトウェアは無償のものも有償のものもありますが、いずれの場合でもそのソフトウェアそのものを譲り受けるわけではありません。あくまでも、利用する権利を譲り受けます。使用の許可（許諾）に当たっての条件を契約としてまとめたものが、使用許諾契約であり、ライセンスとも呼ばれます。

契約は当事者の合意に基づいて決定されます。本人に自覚がないケースが多いので問題が起きることもあるのですが、あるソフトウェアを利用しているということは、そのソフトウェアの使用許諾契約に合意していると見なされるのです。

このように、ソフトウェアは、必ずライセンス契約に従って利用して下さい。例えば、次のような行為は禁止です。

- 研究室の PC に、ソフトウェアの購入ライセンス数以上の本数のインストールを行う
- サークル活動のために、市販されているアプリケーションソフトをコピーした CD を配布する
- 友人にコピーしたソフトを譲り渡す
- 著作権侵害にあたるファイル交換を行うために P2P ソフトウェアを使う

一般的に、有償で販売されているソフトウェアは、1 台の PC にのみインストールして利用できるという場合がほとんどです。職場と自宅で 1 台ずつインストールできるという場合もありますし、ファミリーパックという形態で 3 台や 5 台までというケースも見受けられます。販売形態によって異なりますので、確認が必要です。

2010 年 1 月から、違法コピーであるソフトウェアをダウンロードしただけで違法とされるようになりました。罰則はありませんが、場合によっては強制捜査の対象にもなり、また民事責任を免れるのは難しくなったと言えます。違法コピーのソフトウェアを利用して損害賠償請求の訴訟を提起された場合、過去の判例によれば、その請求額はおおよそソフトウェアの正規小売価格の 2 倍程度です[12]。

文書作成と著作権

大学では、レポートや論文などで文章を作成します。Web ページで情報発信するということもあるでしょう。研究成果についてプレゼンテーションを行うということも考えられます。

レポートや論文で他人の文章を勝手に引き写せば、それは複製ということになり、権利を侵害したことになります。Web ページで情報発信すれば、それは複製したことになり、Web サーバーにその文書を設置した時点で公衆送信可能化し、不特定多数に向けて配信すれば公衆送信したことになります。プレゼンテーションで他人の著作物を勝手に使うと、上演や上映を行ったということになります。

ここで複製（転載）とは、上に述べた記事や画像データなどの著作物の全部または一部などをそのまま抜き出して利用することを言います。これらを利用するためには著作者や登録者に転載の許可を得る必要があります。もし許可を得ずに転載した場合には著作権侵害で訴訟にすらなる可能性もありますので、十分注意してください。

一方、著作権は無制限に認められるのかといえばそうではなく、著作権の及ばない利用（著作権法第 30 条から第 47 条の 4）というものがあります。これらは著作権法上認められた行為であり、利用に当たって著作権者の許可は必要ありません。

ただし、日本の著作権法は著作権の及ばない範囲について個別具体的に列挙していますので、それぞれのケースについて著作権法をよく理解をしてから利用する必要があります。

例えば、文章について、他者の書いた文章を自分の文章の中に取り込むことは、引用という方式なら認められています (著作権法第 32 条)。ただし、引用として認められるには以下の条件をすべて満たしている必要があります。

- その著作物を引用する必然性がある。

[12] 2001 年 5 月における東京地裁の判決では、被告に対して正規小売価格の賠償金支払いを命じています。被告は既に違法コピーの利用が発覚した後に正規品を購入しており、合わせて正規価格の 2 倍を支払ったことになります。

- 自分の著作物と引用部分が明確に区別できる。
- 引用された著作物の出典、著作者名などが明記されている。
- 自分の著作物と引用する著作物の主従関係が明確にされている。
- 原則として原形を保持し、改変して使用する場合はその旨を明記する。

「必然性がある」とは、脈絡なく引用していいわけではないということです。引用する必然性もなしに、これは引用だと言い張れば、何でも複製できることになってしまうからです。

「自分の著作物と引用部分が明確に区別できる」とは、例えば短い文章であれば括弧でくくる、という方法が良いでしょうし、少々長い文章であれば段落を変え、字下げをして前後の段落から少し引用文章の段落を離してやるといった方法がよくとられます。百聞は一見にしかずですので、例として、日本国憲法の前文を一部引用してみます[13]。

> 日本国民は、恒久の平和を念願し、人間相互の関係を支配する崇高な理想を深く自覚するのであつて、平和を愛する諸国民の公正と信義に信頼して、われらの安全と生存を保持しようと決意した。われらは、平和を維持し、専制と隷従、圧迫と偏狭を地上から永遠に除去しようと努めてゐる国際社会において、名誉ある地位を占めたいと思ふ。われらは、全世界の国民が、ひとしく恐怖と欠乏から免かれ、平和のうちに生存する権利を有することを確認する。

さて、出所の明示ですが、最後にまとめて参考文献としてあげるのでは不十分です。それぞれの引用部分に対応して出所を明示する必要があります。つまり、文章のうちどの部分が、どの文献から引用されているのかが明らかになっていなければいけません。この表示の仕方は学問分野や学会によって様々に異なります。本書では 85 ページの第 6 章「レポート・論文作成の基礎」でこの方法を解説していますので、参考にしてください。

一方、出所を明示しなければならないという時点で、参考にした文献リストを作成する必要があることが分かります。また、この文献リストはばらばらのやり方で作ればいいというものではなく、統一的な方法で作成する必要があります。早稲田大学では Refworks という文献管理システムを全学の学生が利用できるように提供していますので、ぜひこれを活用してください。本書では 96 ページの「Refworks による文献管理」でこれを詳しく紹介しています。

また主従関係が明確ということは、文章の質や分量から見て、主役はあくまでも自分自身の書いている文章であるということです。質が意味するのは、引用された文章というのはあくまでも付随的なものでなければならず、量という意味では引用した文章の方が多かったというのでは、なかなか引用とは主張しづらいだろうと考えられます。

早稲田大学では、このような引用という手続きにきちんと則っていないレポートや卒業論文、修士論文、博士論文等については、剽窃ということで定期試験における不正行為（いわゆるカンニング）と同じ扱いとすることとなっています。不正行為ということは、その学期のすべての単位を失い、また停学処分が下されるということです。

ハラスメント

本学では「早稲田大学ハラスメント防止委員会」を設置し、ガイドラインを設けています。ハラスメントは人権侵害であり、コンピューターやネットワークの利用を通じてであったとしても、このガイドラインに抵触する言動を行うことは、やはり人権侵害となります。

詳しくは「早稲田大学ハラスメント情報委員会」の Web ページ

[13] 憲法その他の法令は、著作権法の対象外です（著作権法第 13 条）。

http://www.waseda.jp/stop/

に掲載されています。無意識のうちに誰かを傷つけてしわないように、ぜひ一度は目を通してください。

3.6　演習問題

1. 自らのパスワードが強度という点で妥当かどうか、再検討しなさい。強度が足りないと考えたら、パスワードを変更しなさい。強度の確認のためには、例えば、
   https://www.microsoft.com/japan/protect/yourself/password/checker.mspx
   のような Web ページで提供されているサービスを利用しても良い。ただし、その場合はパスワードが詐取されないことを十分注意して確認すること。

2. 「中古ソフトウェア」を売買することは合法か違法か調べなさい。特に、ゲームソフトウェアとビジネスソフトウェアを区別する必要があることに注意すること。

3. 違法にコピーしたソフトウェアを組織的に利用していることが発覚し、訴訟に至ったケースが日本であるが、その事件の概要と判決内容を Web 検索で調べなさい。

4. Web の掲示板で名誉毀損が行われたとして掲示板の運営者に対して裁判で損害賠償請求が行われ、損害賠償が認められたケースと認められなかったケースがある。Web を検索して、それぞれ 1 つずつ例を挙げなさい。

5. P2P（Peer to Peer）によるファイル共有ソフトとして、Winny や Share、BitTorrent などを利用する人がいるが、利用中に誤って自らの個人情報を漏洩させてしまう場合がある。どのような経緯で流出が起こり、どのような被害が発生したか具体的なケースを Web 検索により調査しなさい。