

2-9 情報倫理と自己防衛

インターネットを上手に利用するには、法律などの規制がまだ十分でなく匿名性が高いなどの独特な側面を持つインターネットの世界で、加害者にならないための情報倫理と被害者にならないための自己防衛に通じている必要があります。ここでは、情報倫理と自己防衛に関する概要を学び、様々な実例を皆さん自身がインターネットの中から収集し、できる限り自分自身で実感してもらいたいと思います。

2-9-1 情報倫理

インターネットに代表されるコンピュータネットワークは、人類が初めて手にする可能性を開き、産業革命に匹敵する変化を社会にもたらすと考えられています。このような新しい可能性を意義あるものとし、物心ともに豊かな社会を建設していくには、各自が以下のような情報倫理（法律、ルール、マナー）を守り、加害者にならないように心する必要があります。ここでは、基本的なことに止めますので、詳細は学内用ホームページの情報倫理を参照してください。

①基本事項…自己責任の世界

インターネットを利用して情報を受信したり発信したりするときには、それによって生じるリスクや社会的責任や法的責任を自身が負わなければなりません。

②セキュリティ

利用権限のないシステムに不正にアクセスすることは、不正アクセス防止法で禁止されています。また、個人情報保護の観点から、個人情報の取り扱いは慎重に行う必要があります。特に以下の事項に注意しましょう。

- ・他人のユーザIDやパスワードを盗用しない。
- ・コンピュータウイルスを作成・流布しない。
- ・内部情報を部外者に漏らさない。
- ・個人情報（名前、住所、電話番号、メールアドレス、勤務先、等々）は、本人の承諾なしに公表したり、第三者に伝えたりしない。顧客名簿等の持ち出しなどは法律で禁じられています。
- ・個人情報を収集するときは、その目的と利用範囲を事前に明確にし、本人（未成年者の場合はその保護者）の承諾を得る。

③違法行為はしない

インターネットの世界では、自分の名前を隠して様々な行為をしたり、現実の自分とは全く別の人間のように振舞ったりすることが可能のように思いがちです。実際には、違法行為に匹敵する内容をもつホームページや掲示板は、通信記録の追跡などから違法行為者が特定される可能性が高いのですが、匿名性があるように見えることが普通の人を違法行為へいざなうことがあります。2011年には、法務省は、プロバイダなどに対して、一定期間(90日間)の通信記録の保全を求めることができるとする法案を国会に提出し可決されました。

また、知識がないためまったく悪いことをしているという意識無しに、法律に反する行為をする人たちも増えてきています。ぜひ皆さんも、自分は大丈夫と高をくくらずに注意して下さい。以下、代表的な違法行為についてみていきましょう。

著作権の侵害

文章や写真、音楽、ソフトウェアなどの著作物に関する権利は、著作権者だけがもっており、無断でこれを複製、転載、改変したりすることは禁じられています。インターネットでの著作物の利用に際しては、以下のような行為が著作権の侵害に当たるので注意するように。

- ・ホームページ、書籍、新聞、論文などの記事や写真を無断で転載すること
- ・テレビやビデオから取り込んだ画像やデータを無断で掲載すること
- ・芸人や著名人の写真やキャラクターをまねて描いた絵の画像データを、無断で掲載すること
- ・他人が作成したソフトウェアやそれを改変したプログラムを無断で掲載すること
- ・音楽や歌の歌詞またはCDなどから取り込んだデータを無断で掲載すること
- ・他人の電子メールを無断で掲載すること

なお、引用は出典を明記すればOK。2011年には、著作権法が改正され、海賊版の音楽や映画などインターネット上の違法配信と知りながら、そのファイルをダウンロードした場合も罪になることが決まりました。更に、2012年には、違法ダウンロードにも罰則が与えられる法案が可決されました。インターネットに流布しているソフトやデータを当たり前で使用しただけでも、罪に問われることもあるわけなので正確な法律知識を身につける必要があります。

インターネット上の情報はマルチメディア情報であるため、複数の著作権が複雑に絡み合っている場合がほとんどです。このような場合の著作権処理は容易ではないので、最近、マルチメディア情報の著作権処理を主な目的とする組織の形成やビジネスモデルが考案され、実験的活動が始まっています。

また、学術論文についても、そのオリジナリティが大変に重要になります。従って、無断転載や剽窃は絶対にしてはなりません。

商標の使用

商品やサービスを識別されるために付けられている文字、図形、記号などを商標といい、法律によって保護されています。他人の商標をあたかも自分の商品やサービスのものであると誤解を招くような使い方をしてはいけません。

肖像権

本人の許可無く、その顔や容姿などを撮影し、その写真をホームページなどで公表すると、肖像権の侵害として訴えられ、損害賠償を請求される可能性があるので注意。

プライバシーの侵害と個人情報の保護

他人の私生活にかかわる各種の情報を本人の了解無くインターネットでみだりに公開すると、プライバシーの侵害として訴えられ、損害賠償を請求される可能性があるので注意。また、他人の個人情報を収集するときは、本人の（未成年の場合は保護者の）承諾を得る必要があり、合意した利用目的以外の使用はしないように。特に、名簿の扱いには気を付け、第3者に売却したり渡したりしないようにしましょう。「個人情報保護法」が施行され、法的にも罰せられる

ようになりました。このような個人情報（名前、住所、電話番号、メールアドレス、勤務先、等々）は、本人の承諾なしに公表したり、第3者に伝えたりしないのが原則です。

個人情報は一度インターネット上で公表されると、取り戻すことは不可能であり、不特定多数に行き渡るため、大変な結果につながることもあります。例えば、イラク人質事件（2004年4月）の当事者3名の住所がインターネット上の掲示板に書き込まれただけで、個人を誹謗中傷する郵便が彼らのもとに多数届き、札幌法務局が掲示板の管理者に書き込みの削除を依頼した件などはその一例です。

違法商法

ねずみ講、未承認医薬品の販売・広告、違法通信販売等の法律で禁止された商業活動は行わないこと。

有害情報の発信

猥褻な文書や画像、爆薬や毒薬などの製法等、他人を害する情報は発信しないこと。インターネット上の掲示板のいたずら書きも、内容によっては犯罪行為とみなされる場合があります。例えば、国内最大の掲示板群「2ちゃんねる」に2011年9月に小田急電鉄が走るトンネルを爆破すると書き込んだとして、偽計業務妨害容疑で神奈川県が男性が逮捕されたこともあります。

誹謗・中傷

特定の個人をネット上で誹謗したり中傷したりしないこと。特に、自分の名を明かさず他人を非難するような卑怯な振る舞いは、絶対避けること。事件化し、裁判沙汰になって、誹謗中傷した者が（場合によっては舞台となったネットワークサービスの管理責任者も）罰金や禁固刑に処せられた例も多いのです。本学でも、外部から本学の学生に誹謗・中傷されたという苦情がきたことがあります。注意しましょう。

④ネットワークエチケット

違法行為にならなくても、他人を不快にさせることはなるべく避けるようにします。たとえば、他人の電子メールを見たり、ネット上で他人を困惑させたりしないように。インターネットの利用者として、良きエチケットとルールを守るようにしましょう。

2-9-2 自己防衛

インターネットの利用者が上記の情報倫理（法律、ルール、マナー）を守り、利用者の自由にまかせてもインターネットの世界の秩序が保たれるのであればそれに越したことはありません。しかし現実には、インターネットの利用者がすべて善人とは限らず、様々な違法行為や悪意に満ちた行為を行うものが後を絶たず、実際に多くの被害者が出ています。このような現状では、被害者にならないために自分を自分で防衛する方法を知っておく必要があります。

①基本事項…自己責任の世界

インターネットを利用することによって生じるリスクは、自身が負わなければなりません。そのため、自分を守るのも自分の責任で行わなければならないのです。

②組織の一員としての自己防衛

不正アクセス

予防：ネットワークユーザとして個人のパスワードとユーザIDをしっかりと管理するのが最重要。内部セキュリティに関する情報を外部者に漏らさないようにします。

対処：不正アクセスを疑わせるようなシグナルを感じ取ったら、直ちにネットワーク管理部門に知らせること。クラッカーが内部の誰かになりすましている場合などは、なりすまされた本人か親しい者が気づきやすいので、注意を怠らないように。

コンピュータウィルス

予防：何よりも、最新のウィルス情報（ウィルスデータファイル）をもつアンチウィルスソフトを使用するのが最善。組織やプロバイダで提供されているものは必ず活用するようにしましょう。本学の場合は、本学 LAN の入り口ですべての出入りするメール（添付ファイルも含めて）に対しウィルスチェックを実施しており、端末機にも最新のウィルス情報を持つアンチウィルスソフトを無償で提供しています。

対処：感染に気づいたら、まずネットワーク管理部門に知らせ、ウィルスを特定し、有効なワクチンで端末内を駆除します。そして、管理部門と協力して、必ず感染範囲とルートを調査し、今後の予防に役立てます。

③個人としての自己防衛

個人情報の流出

インターネットでは、個人情報やメールは送信時に盗聴される可能性があります。また、各種アンケートに答えても、個人情報を収集されている場合が多いのです。個人情報が流出すれば、以下のパスワード盗用、プライバシー侵害、詐欺、スパムメール、爆弾メール、チェーンメール等に悪用されたり、無断でアダルトサイトに登録されたりするなど、様々な被害を受ける可能性があるため注意を要します。

予防：他のホームページに個人情報を書き込んだり、アンケートに答えたりした場合は個人情報が漏れているものと覚悟し、注意を怠らないように。ユーザ ID やパスワードの管理に注意を払うこと。自分の住所や電話番号をネット上で公開することは極力避けましょう。

対処：被害を受けたら、ユーザ ID、パスワード、電話番号などの変更できるものは、直ちに変更します。必要なら警察に相談すること。

パスワードの盗用

他人にパスワードを盗用されたら、自分名でインターネットを利用されたり、コンピュータ犯罪を起こされたりする可能性があります。

予防：他人のしている前でパスワードを打ち込まないように。また、パスワードのメモなどを放置するなどのずさんなパスワード管理をしないこと。

対処：直ちにパスワードを変更するように。

プライバシー侵害

電子掲示板などに勝手に私生活に関する情報を公開される場合や、メールで親しくなった相手に名前や住所などを教えたならストーカー行為に及ばれるような場合です。

予防：自分からは無意味に個人情報公開しないように。

対処：プライバシーを侵害するメッセージなどを、プロバイダに連絡して削除するように要求したうえで、警察に相談します。ストーカー行為は、直ちに警察に訴えます。

著作権侵害

自分の著作物（著作権侵害）やホームページに掲載した顔写真（肖像権侵害）などを無断で転載されるような場合です。

予防：ホームページに顔写真などを公開することは極力避けること。公開する場合は、そのメリットとデメリットをよく考え、自己責任において判断するように。

対処：無断転載者に削除要求をします。要求に応じない場合は、当該ホームページを管理するプロバイダに対応を依頼します。

詐欺

インターネットで見た相手に対して送金したが品物が届かない、あるいは身に覚えのない請求がくるなどの場合です。

予防：個人間の売買では、品物の引き渡し方法と代金の支払方法を双方が納得できる方法で決めることが大切。「他に希望者がいるので先にお金が振り込まれた方に譲る」などというのは詐欺の典型的な手口なので注意。特に、インターネットオークションでは盗品の売買など、トラブルが多いことを肝に銘じて参加することが大切です。

対処：やりとりしたメールの写しおよび銀行振込の控えをもって、直ちに警察に届けます。

オンラインショッピング

オンラインショッピングで購入したものが違っていたり破損していたので、返品しようとしたが、受け付けてもらえなかったり、そのショップが存在していなかったような場合です。

予防：代金決済の方法としてクレジットカード番号の送信を必要とする場合は、よほど暗号システムがしっかりしているショップ以外は避けるようにします。FAX等の別の手段で送信できるかどうか問い合わせるのがよいでしょう。信頼できる目安として、販売価格、送料、代金支払時期と方法、商品引き渡し時期、返品可否と条件、販売業者名、住所、電話番号、責任者・担当者氏名等の項目が明示されているかに注意すること。

対処：ショップが個人商店のような場合は、解決が困難。ショップ全体を管理するモールがあればそこに相談します。また、消費者センターなどに相談するのもよいでしょう。

ねずみ講とマルチ商法

予防：現実世界と同じように、うまい話には気をつけること。会員を増やすことが目的の場合は、特に気をつけるように。ねずみ講の場合は、参加した者も罰せられるので注意が必要。このような誘いのメールには反応せず、返信も転送もしないように。本学でも、まれですが実害が出ています。

対処：しつこい場合は、消費者センターや警察に相談するように。

スパムメールと爆弾メール

知らないところから届くダイレクトメールをスパムメール、一度に大量のメールが送信される場合を爆弾メールと呼んでいます。これらのメールは、本来必要としているメールを探す邪魔になり、メールボックスを満杯にしてしまうので迷惑なものです。

予防：加入しているプロバイダによっては、そのようなメールの受信を拒否できる場合があるので、問い合わせてみましょう。

対処：スパムメールの場合は、メール本文とヘッダ一部分を保存し、発信元プロバイダに連絡します。爆弾メールの場合は、自分のプロバイダに連絡して、自分のメールボックス内の削除と受信拒否を設定してもらいましょう。ただし、最近は頻繁にメールアカウントを変えて送付してくるケースも多く、アドレスに対する受信拒否は余り効果が出ないようです。

チェーンメール

幸福の手紙のようなメールが届き、複数の他人に転送するように要求してくるようなメールのこと。架空の緊急事態を装い、多数に転送するよう指示するデマメールも同じです。最近は少なくなってきましたが、注意する必要があります。

予防：自分のところで断ち切る勇気をもつこと。

対処：このようなメールは他人に転送すると、ねずみ算式に増加し、メールサーバ障害や通信混乱を招く恐れがあります。転送せず、直ちに削除すること。

誹謗中傷

誹謗・中傷は突然発生するというより、ある経緯があって発生する 경우가ほとんどです。インターネットでは、世界中の人とコミュニケーションできる反面、主義主張、思想信条、慣習等の異なる背景をもつ人々との議論になるので、一方的な価値観の押しつけはしないように注意が必要です。

予防：相手の意見に激高したり、過激な要求を突きつけたりしないこと。通常の議論以上に、一歩引き、冷静に話し合う姿勢を失わないことが大切。

対処：当事者同士で、もう一度冷静に話し合っ解決方法を探るように。ときとして、沈黙を守ることも役に立ちます。告訴もできますが、それは最後の手段です。

インターネット中毒

1日に8時間も10時間もインターネットに向かい、家族や友人との人間関係を無視し、仕事を無視し、インターネットから離れるとイライラして落ち着かなくなったら、インターネット中毒を疑わなければなりません。

予防：現実の生活を常に優先するという鉄則を守り、中毒によって失うものの大きさを常に心することです。心配なら、一度ヤングの提唱する「インターネット中毒度テスト」（ヤング著「インターネット中毒」毎日新聞社、本学の図書館にあり）をやってみるとよいでしょう。

対処：ただちに専門の精神科医か心理カウンセラーに相談しましょう。

電磁波

すべての電子機器や通信機器は電磁波を出しています。パソコンも例外ではありません。電磁波の人体への影響については、現在、動物実験や免疫実験による研究が進められていますが、ガン発生などに影響ありとする結果と影響無しとする結果が相半ばしていて、まだはっきりした結論には至っていません。もっとも、日本電子工業振興会（JEIDA）は一定の安全ラインを決め、市販のパソコンや携帯電話などはその指標を満たしているので安全だと主張しています。しかし、パソコンや携帯電話が飛行機の操縦機器や心臓に埋め込まれたペースメーカーなどに影響を与えることは知られており、複数機器の同時使用などの場合、場所によっては電磁波が局部的に強まることも考えられるので注意が必要です。また、携帯電話の発する電波は、金属壁で囲まれている電車内などでは全反射され、そのほとんどが車内に閉じ込められて充満することが知られています。すなわち、電子レンジと同じ現象が起こることになります。

予防：電磁波は電流が曲げられると生じるのでコードはなるべく巻くように束ねては使用せず、電磁波グッズなどを利用しましょう。ただし、磁界は遮蔽が困難。なるべく長時間端末に向かうことも避けましょう。インターネット中毒や眼精疲労、それに起因する肩こりなどの予防にもなります。携帯電話は、上記の理由から電車やバスの中では電源を切るようにしましょう。

対処：できれば電磁波の強度測定をし、必要ならば電子機器の配置を変えたりしましょう。

最後に、このような情報倫理と自己防衛は表裏一体の関係にあることに注意しておきましょう。すなわち、他人にこのような自己防衛を強いるような行為をしないというのが、情報倫理の真髄であることを。

[課題1] インターネットにおける被害の実例

以上の情報倫理と自己防衛に述べられている内容に関係する実例（被害か加害かを問わない）をインターネットの中から収集して、レポートにまとめて提出します。実例はカテゴリーの異なる5例以上とし、レポートの形式（ワープロ清書、手書き、メール形式など）、提出の仕方や締め切りなどは担当教員の指示にしたがってください。ただし、ホームページなどのコピーは不可。自分の言葉で説明することが重要です。

ヒント：サーチエンジンなどを駆使してそのような実例を掲載しているホームページを見つけるのが近道です。その場合、必ず参照したホームページの URL 等を参考文献として最後にまとめて掲載するようにします。そうでないと、盗作になりますからね。