摂南大学
情報システム利用ガイドライン

2019 年 3 月 18 日改訂

情報メディアセンター

改訂履歴

版数	発行日	改訂内容
第一版	2011 年 9 月 30 日	初版発行
第二版	2019 年 3 月 18 日	・3.3 「掲示板、SNS（Social Networking Service）などの利用」を「ソーシャルメディアガイドライン（掲示板・SNS など）の利用」に変更 ・3 3.3 (3) 「SNS（mixi など)」を「SNS（Twitter、Instagram など)」に変更 ・4 4.1 マルウェアに関する記述を追記 ・4 4.3 ファイル交換（情報漏洩・著作権）の記述を修正 ・4 4.4 「Wiki」を「Wikipedia」に修正

1. はじめに

1.1 情報システムの目的

摂南大学（以下「本学」という。）の情報システムは、本学の教育理念である「人間力・実践力・統合力を養い、自らが課題を発見し、そして解決することができる知的専門職業人を育成する」ことを実現するために、本学のすべての教育・研究活動および運営の基盤として設置されています。したがって、情報システムを秩序と安全性をもって安定的かつ効率的に運用することが不可欠です。このためには、本学情報システムを利用するすべての人が、利用に関する規則を遵守せねばなりません。

1.2 情報システム利用者の心構え

法令に違反しないことは当然ながら、本学の情報システムを円滑に運用するためには、各利用者が本学構成員の一員であるという認識をもって、十分な注意を払ってコンピュータを操作することが必要です。まず、このことをよく理解してください。

1.3 利用についての原則

(1) 利用の精神

本学情報システムの利用にあたっては、つぎのことに留意するとともに、基本的な社会常識に従い、他の利用者や通信先に対する配慮をもって利用してください。

・言論の自由、学問の自由
・他者の生命、安全、財産を侵害しない
・他者の人権、人格の尊重
・公共の福祉、公の秩序

(2) 法令の遵守

本学情報システムでの行為は治外法権ではありません。日本国内においては日本国内法が適用されます。場合によっては海外の法律の適用をうける可能性もあります。法令や公序良俗に反する行為を行ってはいけません。

(3) 目的外利用の禁止

本学情報システムは、教育・研究活動および運営の基盤として設置・運営されているものです。これらの目的に該当する範囲で利用してください。

(4) 利用規程と罰則

「摂南大学情報メディアセンター規定および利用内規」などの学内規定に違反する行為をした場合には、警告、利用制限、所属部局への通報などの措置がとられることがあります。また、不正利用の発生とその対処について、利用者の氏名を含め公表されることがあります。

2. 法令および利用規則の遵守

2.1 法令および利用規則に違反する行為

関連する法令としては、憲法はもちろんのこと、刑法、民法、商法をはじめとして、不正アクセス禁止法、著作権法、プロバイダ責任制限法、その他多くのものがあります。また、外国に影響を及ぼす場合は外国法の適用を受ける可能性があることにも留意せねばなりません。その他、他人の犯罪行為の手伝いをした場合は、幇助罪(ほうじょざい)または従犯として処罰されることがあります。以下の禁止事項および遵守事項に留意してください。

禁止事項

(1) 基本的人権・プライバシーの侵害

本学情報システムの利用に限らず、基本的人権を尊重せねばなりません。人種・性別・思想信条などに基づく差別的な発言をネットワークで公開すると、基本的人権の侵害となることがあります。誹謗(ひぼう)中傷は名誉毀損(きそん)で訴えられることがあります。

本学情報システム利用者のプライバシーは尊重されますが、利用者は他人のプライバシーも尊重しなければなりません。他人のプライバシーを勝手に公開してはなりません。

(2) 利用権限の不正使用

利用権限は正しく使用しなければなりません。また、パスワードを盗まれて不正行為が行われないようパスワードを厳格に管理することは、利用者の責務です。利用者は、以下のような行為をしてはなりません。

(a) 他者のアカウントを使う

利用者は、他者のログイン名を用いてログインしてはいけません。この行為は不正アクセス禁止法で犯罪とされています。また、利用者は、自分のアカウント(利用権限)を他人に使わせてはなりません。本人のログイン名で他者に本学情報ネットワークを使用させたり、ファイル格納領域などの資源を他者に使わせることもこれに含まれます。

(b) 他者の名前やログイン名を騙(かた)る

他者の名前やログイン名を騙って、電子メールを送ったり掲示板に書き込みを行ってはいけません。

(3) 他組織への侵入

セキュリティホール等を利用して情報システムに侵入する行為も不正アクセス行為です。本学情報システムの内外を問わず、利用資格のないコンピュータを使用してはなりません。本学情報システムから他組織の情報システムへ不正に侵入した場合、本学全体が外部のネットワークとの接続を切られるだけなく、場合によっては国際問題に発展する可能性があります。また、他組織への侵入を試みるようなことも絶対にしてはなりません。

自分で不正アクセスをしなくても、他人に不正アクセスをさせるような行為をしてもいけません。たとえば、電子掲示板に他人の ID とパスワードを載せるような行為や、友人に自分の ID とパスワードを貸し与える行為などがあてはまります。また、コンピュータウイルスの中には、感染すると他のコンピュータへの不正侵入を試みるものもあります。感染したコンピュータの所有者が知らないうちに、不正侵入や攻撃を行うことになりますので注意が必要です。

(4) 知的財産権の侵害

知的財産権は、人間の知的創作活動について創作者に権利保護を与えるものです。絵画・小説・ソフトウェアなどの著作物、デザインの意匠などを尊重することを心がけて下さい。著作物の無断複製や無断改変はしてはなりません。例えば、本・雑誌・ウェブページなどに提供されている文章・図・写真・映像・音楽などを、無許可で複製あるいは改変して、自分のウェブページで公開したり、Twitter やネットニュースに投稿したりしてはいけません。他人の肖像や芸能人の写真については、肖像権やパブリシティ権の侵害になることがあります。

(a) 著作権

著作物（小説、音楽、絵画、動画、写真、プログラム、データベース等）には著作権があります。著作権は、著作物の作者が自分の作品を勝手に公開されたり改変されたりすることで気分を害することがないようにする働き（著作者人格権）と、著作物を勝手にコピーされたりして作品の価値が下がってしまうということのないようにする働きがあります。著作権のある著作物を著作権者の許可なくコピーして他人に渡したり、ウェブページなどで公開すると、著作権法によって罰せられるだけでなく、著作権者から損害賠償を要求されることもあります。著作物の一部を利用したり、改変、翻訳、編曲、翻案することも、著作権者に無断で行ってはいけません。

意識的に公開したつもりがなくても、コンピュータがウイルスに感染していたり、ファイル交換ソフトの設定によっては、著作物が外部に公開・共有されてしまうことがありますので、十分な注意が必要です。また、ディジタル著作物には、コピーできないように制限がかかっているものもありますが、その制限を無効にしてコピーができるようにする装置やソフトウェアを販売したり配布すると、たとえ自らはコピーや公開をしていなくても罰せられることがあります。

(b) 肖像権、パブリシティ権

本人に無断で写真を撮ったり、その写真をインターネットに公開してはいけません。写真を撮られたり、その写真を公開されることで、嫌悪感をもつ人も多く、人格権の侵害であると考えられるからです。このような行為をすると、肖像権の侵害として訴えられ損害賠償を請求されることがあります。

また、タレントやスポーツ選手など有名人の写真は、それだけで経済的な価値がありますので、パブリシティ権の侵害として、経済的な損失について賠償請求されることになります。

(5) 有害情報の発信

違法な情報はもちろんのこと、公序良俗に反する情報や有害情報を発信してはいけません。本学情報システムを用いてわいせつな文書・画像などを公開してはいけません。また、それらへのリンクを提供してはいけません。このほか、次のような情報の公開も、研究上必要な場合を除き、禁止します。

(a)情報自体から違法行為を誘引するような情報（銃器や爆発物などの情報、禁止薬物や麻薬の情報等）

(b)人を自殺等に勧誘・誘引する情報

(c)ネズミ講やマルチ商法の勧誘

(d)セクハラ、アカハラに関する記述を伴うような情報

遵守事項

(6) 個人情報・機微(センシティブ)情報の保護

以下に挙げるような、個人情報や機微(センシティブ)情報をパソコンで取り扱う場合は、これらの情報が不必要に流出しないように細心の注意を払う必要があります。

(a) 氏名、住所、生年月日、電話番号、メールアドレスなど、個人を特定できる情報
(b) 病歴、持病、血液型などの医療情報
(c) 家族・親族関係や出身地などの情報
(d) 個人の趣味や嗜好などに関する情報
(e) 借金の有無や残高などに関する情報
(f) 銀行口座番号やクレジットカード番号、健康保険証番号など

(7) 本学情報システムのセキュリティ保持への協力

上記(1)～(6)のほかに、セキュリティを保持するために、利用者自身が注意すべきことがあります。例えば、コンピュータウイルスを持ち込まない、不信な発信元からのメールを開かない、自分の管理しているコンピュータにウイルス対策ソフトを導入しウイルス検知パターンを常に最新状態に保つ、本学情報システムの故障や異常を見つけたら速やかにシステム管理者（情報メディアセンターなど）に通報するなどが、これに該当します。

大学のネットワークは、多くの管理者によって支えられています。ネットワークでは、一部の利用者の自分勝手な行為や心無い行為によって、ネットワークの利用が著しく制限されたり、大学全体の信用が失われたりすることがあります。一人一人のネットワーク運用への協力が、より良い教育・研究環境の構築につながることを自覚してください。ネットワークの利用中に、ネットワークの安定運用に関わる問題点に気づいたらシステム管理者（情報メディアセンターなど）に報告してください。

2.2 教育・研究目的に反する行為

本学情報システムは、教育・研究活動および運営の基盤として設置されています。教育・研究活動および運営という設置目的から逸脱する以下のような行為は、利用の制限や処分の対象になることがあります。

(1) 政治・宗教活動

特定の団体に利便を供するような活動に用いてはいけません。

(2) 営利活動の禁止

広告・宣伝・販売などの営利活動のためにウェブページや電子メールを用いてはいけません。

(3) 運用妨害

物的な加害の有無に関わらず、本学情報システムの運用を妨害する行為は禁止します。例えば、本学情報システムに悪影響を与えたり、他の利用者に迷惑をかけるような利用はしてはいけません。

(4) 目的外のデータの保持

個人に与えられたファイル領域やウェブページ領域に、教育・研究の目的に合致しないものを置いて

はいけません。

3. マナーの遵守

3.1 ネットワークを快適に利用するために

法令や公序良俗に反せず、教育研究目的に合致した利用であっても、注意すべきことがいくつかあります。ここでは簡単に触れておきます。

(1) 品位をもって利用する

本学の構成員としての品位を保って利用すべきことは言うまでもありません。品位に欠けるメッセージの発信は謹んでください。

(2) 他人を思いやって利用する

大量のデータを送受信すると、本学情報システムを利用している他人に迷惑をかけることになりますので、十分注意してください。また、情報演習室のように共同で利用するコンピュータ設備は、ネットサーフィンやゲームで占有したりせずに、他人に対する思いやりをもって利用してください。

(3) パスワードを適正に管理する

パスワードはあなたが正規の利用者であることを確認するために大切なものです。自分のパスワードを友人に教えたり、友人のパスワードを使ってコンピュータを利用してはいけません。パスワードを教えた人、教えてもらって利用した人の双方が責任を負うことになります。

パスワードの文字列を工夫し、自分の頭にだけに覚えておいて、パスワードを他人がわかるような状態で手帳や携帯電話などにメモしないでください。他人がパスワードを入力するときには、顔をそむけるという配慮も必要です。

アカウントを盗用されても、直接的な経済的不利益は被らないかもしれません。しかし、例えば、パスワードを知られたために、自分のアカウントから他人を侮辱(ぶじょく)する内容の電子メールが発信された場合、あなたが侮辱行為者として扱われます。また、あなたのアカウントを利用して他のコンピュータへの侵入行為が行われた場合(これを踏台アタックと呼びます)、アカウントを盗用された被害者が、まず最初に犯人として疑われるのです。

パスワードは、各システムの運用ルールに従い英小文字・英大文字・数字・記号を含めるようにしてください。

(4) 個人情報やプライバシー情報を守る

共用のサーバコンピュータに置かれたファイルには、他の利用者から読まれないようにアクセス権限を設定できることが多いので、適切に設定しましょう。誰からも読める、または誰からも書き込めるという状態は非常に危険です。また、他人のファイルが読めるようになっていたとしても、無断でその内容を見ることはやめましょう。ウェブページ・ニュース・掲示板などに、個人情報やプライバシー情報を提供することも危険な行為です。

ウェブページやブログ等に書いて公開すること以外に、情報を保存してあるパソコンやメモリカード

などを放置したり紛失することで、意図せずに情報が流出することがあります。同様に、ファイル交換ソフトを使用している場合に、これらの重要な情報が外部に対して公開されてしまっていることもあります。

懸賞応募のウェブページ等に個人情報を入力する際は十分に注意する必要があります。懸賞を口実に個人情報の収集を行っている場合があり、後日大量の迷惑メールが届くようになってしまうこともあります。

また、パソコンのセキュリティ対策が不十分であると、コンピュータウイルスなどの悪性プログラムに感染し、これらによって情報が自動的に外部に送信されたり、ファイル交換ソフトで共有されることがあります。

いずれにしても、いったん流出した情報は、たとえ後で公開を取りやめたとしても、既に第三者にコピーされていることが多く、回収することは困難です。自分自身の個人情報や秘密情報を流出させてしまった場合には、自分自身に、肉体的、精神的、金銭的な被害が生じますし、他人の個人情報や機微(センシティブ)情報を流出させてしまった場合には、法的に訴えられる可能性が生じますので、十分な注意が必要です。

3.2 メールの利用に関して

(1)メールの信頼性を過信しないようにしましょう

電子メールは、複数のコンピュータを中継して配送されますので、相手に届かないこともまれですがあり得ます。また、宛先アドレスが変更になっていたり、迷惑メールと間違われて配送されないこともあります。重要な用件をメールのみに頼るのは避けて、状況に応じて他の手段を併用しましょう。

(2)あいさつ、自己紹介など、手紙としてのマナーを守りましょう

親しい友人へのメールであれば、用件のみを伝えることもありますが、そうでない人へのメールは、あいさつや自己紹介などを忘れないようにしましょう。

(3)宛先を間違えないようにしましょう

メールの宛先を間違えると、メールシステムに余計な負担をかけ、管理者に迷惑をかけることがあります。また、大切なメールが意図しない人に届き、個人情報などが漏洩することもあります。メーリングリスト等で届いたメールに対して返事を出すと、メーリングリストの登録者全員にメールが届いてしまいます。メールを送信する前に宛先を確認するようにしましょう。

(4)Cc、Bcc の使い方

本来の宛先ではない人にメールのコピーを送っておきたいときには Cc (Carbon Copy)や Bcc (Blind Carbon Copy) を使います。メールの返事を書くときは、Cc に書いてある人にも返事を出す必要があるかどうかを考えましょう。メールの宛先(To)や Cc に書いたアドレスは、メールが届いた人全員が見ることができます。他に誰に出したメールかを知られたくない場合は、Bcc に宛先を書きましょう。

(5)サブジェクト（題名もしくは件名）をつけましょう

多くのメールが届く人は、サブジェクトを見てメールを整理します。内容を簡潔に表すサブジェクトを付けるようにしましょう。

(6)機種依存文字、HTML メールに関する注意

記号や罫線、絵文字等の中には、特定の機種でしか表示できないものがあります（ローマ数字（時計文字）や、丸数字（マルの中に数字）など)。また、いわゆる半角カナも使用してはいけません。HTML 形式のメールは、使用しないでください。これは、受信した側のセキュリティ水準の低下を招くおそれがあるからです。

(7)添付ファイルに関する注意

添付ファイルを使用する場合は、ウイルス等と間違われないように、どのようなファイルを添付するのか、必ず本文中で説明をするようにしましょう。また、特にサイズの大きな添付ファイルは、メール配送システムに大きな負担をかけます。他の方法がないか検討し、相手先に確認をしてから送りましょう。

(8)チェーンメール（chain mail)、デマメールの禁止

複数人へのメールの転送を求めるチェーンメール（不幸の手紙などのように、同じ内容を別の人に転送するように要請するもの）は、メールの配送システムに大きな負担をかけ、システム管理者にも迷惑をかけますので、加担してはいけません。メールの内容が重要かつ緊急を要すると思われてもデマの可能性もありますので、よく確認をして、必要であればマスコミ等、他の手段での伝達を考えるようにしましょう。

(9)迷惑メールやフィッシングメールへの対策

迷惑メールやフィッシングメールが届いても、配送中止の依頼も含めて返事を出してはいけません。メールが確実に届いていることを相手に知らせることになります。迷惑メールやフィッシングメールの本文には特定のサイトへのリンクが設定されていることが多いですが、それらをクリックしてはいけません。また、自分のメールアドレスをウェブページや掲示板に掲載すると、迷惑メールが多く届くようになりますから、メールアドレスの取り扱いは慎重に行いましょう。

(10)パソコンのメールと携帯電話のメールとの違い

パソコンのメールでは携帯電話のメールと異なり、すぐに返事ができるとは限りません。すぐに返事が来ないことも想定しておいてください。

(11)メールアドレスの扱い

メールアドレスはウェブページなどで不用意に公開しないことが望ましいでしょう。しかし、講演会の連絡先等のために公開する必要が生じることもあります。そのような場合には、次のような方法をとるのがよいでしょう。

(a) メールアドレスをロボットで機械的に収集されないように、メールアドレスの全部あるいは一部を画像にしたり、アドレスの一部の@記号を --atmark-- のように別の文字列に置換したりしてウェブページに掲載する。
(b) 講演会への参加申し込みなどのように、掲載期間が限定されている場合は、申込み専用の期限アドレスを使用する。

3.3 ソーシャルメディア（掲示板、SNS など）の利用

(1)誹謗(ひぼう)・中傷をしない

実名の場合はもちろん、匿名の掲示板であっても、誹謗・中傷をしてはいけません。名誉毀損(きそん)などで訴えられることがあります。相手が特定できなくても、人種差別など許されない発言があります。一般社会で許されないことはネットワークでも許されません。

(2)フレーミング（炎上）に注意

ネットワークでは、些細(ささい)なことから議論が白熱し、誹謗中傷の応酬や水掛け論になってしまうことがよくあります。冷静かつ誠実な対応を心掛けましょう。

(3)掲示板毎のルールに従う

掲示板や SNS（Twitter、Instagram など）には、そのコミュニティ毎に個別のルールが設けられていることがよくあります。いくつかの記事を読んで雰囲気を理解してから、発言するのがよいでしょう。

(4)ソーシャルメディアガイドラインを守りましょう

本学ではソーシャルメディアを利用するにあたっての基本的なルールを定めた、ソーシャルメディアガイドラインを策定しています。ソーシャルメディアの利用においてはソーシャルメディアガイドラインを守り、良識ある行動を心掛けてください。

ソーシャルメディアガイドライン
http://www.setsunan.ac.jp/gakusei/guideline/

3.4 ネットワークの過度の利用による悪影響

パソコンや携帯電話によるネットワーク利用は便利ですが、長時間にわたって過度な利用をすると、以下にあげるような心身面に様々な影響が生じることが指摘されています。十分な休息と適度な運動を心掛けましょう。

(1)生活リズムが不規則になることによる心身障害
(2)姿勢や視力への悪影響
(3)対人関係などコミュニケーション能力の阻害
(4)学業成績の低下

4. 情報セキュリティの基礎的知識

4.1 コンピュータウイルスとワーム、Spyware（感染兆候と予防対策、事後対策）

ソフトウェアは人間に役立つように設計されているものですが、一般的に害を及ぼすことを目的に作成されたソフトウェアをマルウェア（malware）と呼びます。マルウェアにはコンピュータウイルス、ワーム、スパイウェア、アドウェア、ランサムウェアなど、広範な種類のソフトウェアが含まれます。

コンピュータウイルスは、自己伝染機能（自己を複製し他のコンピュータに感染を広げる機能)、潜伏機能（特定の条件がそろうまで活動を待機する機能)、発病機能（データの破壊・システムを不安定にする・バックドアを作成するなどの機能）を特徴としたプログラムです。コンピュータウイルスには、ウイルス、トロイの木馬、ボットなどがあります。

ウイルスは宿主となるプログラムに寄生するのが特徴で、様々な不利益（ハードディスクを消去するなど）をもたらします。トロイの木馬は一見有益ないし無害に見えるプログラムが、実は不正な動作をするというものです。スパイウェアは、トロイの木馬とほとんど同じですが、特にユーザに関する情報を収集するのに利用されるものをいいます。

ボットは、メールやネットワークを通じて感染範囲を広げ、感染したコンピュータにバックドア（正規の手続きを踏まずに内部に入る事が可能な侵入口）を仕掛けるというものです。このバックドアにより感染したコンピュータは不正に操られ、著名なサイトなどを（数千、数万台の PC から）一斉攻撃するのに利用されます。

ワームは独立したプログラムで宿主を必要としないことからウイルスとは異なるとされていますが、ネットワークを媒介として増殖し、コンピュータやネットワークに過大な負荷をかけます。

いずれにしても感染経路、ファイルの種類（アプリケーション、Microsoft Office のファイル、ウェブ Cookie など)、被害など、どのような側面で切ってもマルウェアには様々なものがあり、この対策だけ取っていればよいということはありません。

最も重要なのは、アンチウイルスソフトウェア（ウイルス対策ソフトウェア）を導入しておく、ということです。アンチウイルスソフトウェアには、無償で利用することができるものもあります。

なお、アンチウイルスソフトウェアを導入しても、ウイルス検出のパターンファイルなどを定期的に更新しなければ意味がありません。自動でパターンファイルを更新するように設定することができますので、良く確認しておきましょう。

4.2 フィッシング、架空請求等

フィッシング（phishing）は「釣り」の fishing にかけた言葉ですが、ウェブや電子メールを利用した詐欺の一種です。典型的には、「ユーザアカウントの有効期限が近づいています」であるとか「登録情報の確認をしてください」などといった電子メールが届きます。電子メールにあるリンクをクリックすると本物そっくりのサイトが表示されるのですが、実際にはそれは犯罪者が仕立てたニセ物のサイトで、そこで銀行の口座番号や ID、パスワード、クレジットカード番号等の情報を収集しているというものです。

ポータルサイトと呼ばれる統合的なサービスを提供しているサイトでは、オークションや小口決済機能を 1 つの ID で統合しているケースもあり、ID やパスワードを盗まれることで何重にも被害に遭い、また間接的に加害者になるケースもあるようです。

また、電子メールで利用してもいないサービスについて料金を請求されたり、またその請求が恐喝的な手口で行われることもあるようです。

このようなフィッシングや架空請求等への対応は、次のようなものを挙げることができます。

(1) ウェブブラウザのフィッシング詐欺対策機能を有効にすること

(2) 正しい電子メールの知識を持ち、HTML メールを利用しない、リンクを安易にクリックしないこと

(3) ウェブページの URL（特にオーソリティのドメイン名）を良く確認すること

インターネットが普及するにつれ、インターネット上の経済活動も活発に行われるようになっており、それにともなって犯罪者もまたインターネットを活動の場にするようになっています。

フィッシング詐欺は様々な手口で行われていますが、最終的にはウェブを通じて情報収集が行われることが多いため、ウェブの安全な利用が鍵となります。ショッピングや銀行等だけでなく、ウェブを利用していて個人情報を入力しなければならないような場合は、とにかく慎重になる必要があります。

4.3 ファイル交換（情報漏洩、著作権）

ファイル交換ソフトとは、インターネットを利用した P2P（Peer to Peerーピア・トゥー・ピア）でファイルをやり取りするソフトウェアのことです。現在では数多くのファイル交換ソフトが存在し、日本では Winny、Share などが有名です。

ファイル交換ソフトは、自動的にファイルを送受信する仕組みであるため、違法なファイルのやり取りに利用されたり、ウイルスの感染によって、公開するつもりのないファイルがインターネット上に流れてしまったりといったトラブルが数多く発生しています。つまり、ファイル交換ソフトを利用しているコンピュータでは、通常のホームページの閲覧や電子メールの利用に比べて、情報漏洩の危険性が格段に高くなるというわけです。

もうひとつ理解しておかなければならないのは、著作権侵害に対する問題です。多くのファイル交換ソフトは、収集したファイルを再度インターネットに公開する仕組みを持っています。最初は収集したファイルであっても、後からそれらのファイルを自分のコンピュータから公開することにより、著作権侵害で訴えられる可能性があるということです。このような被害を防ぐもっとも確実な対策は、公私ともにファイル交換ソフトを使わないことです。

4.4 情報発信

インターネットは、だれもが気軽に情報発信ができるのがその特徴の 1 つです。以前から気軽に行うことのできた情報発信ですが、ブログや Wikipedia、匿名掲示板などの普及によって、敷居の高さはより低くなっています。

インターネットへの情報発信として注意しなければならないのは、それが不特定多数への情報発信であることが多く、またコンピュータを利用しているため情報の再利用が簡単である、ということです。特定少数への発信であったとしても、一度自分の手を離れた情報がどのように再利用されるかコントロールするのは難しいので、情報の発信にあたっては、特に慎重になってください。

特に慎重を期すべきなのは、個人情報です。自分の個人情報以上に、他者の個人情報の扱いについては、極めて慎重に行ってください。

また、文字のみのコミュニケーションでは真意が伝わらずに嫌な思いをすることもあるでしょう。基

本的には情報の送り手としては真意が伝わるよう厳密に、誠意を持って対応し、情報の受け手としてはおおらかな気持ちで接するのが基本です。インターネット上のコミュニケーションで嫌な思いをしたら、相手が誰であれ、誹謗や中傷をやり返すのではなく、単にその場から離れるのが良いでしょう。

なお、近年の傾向として、インターネット上の情報発信について責任を問われるケースが増えています。無責任あるいは反社会的な言説については社会的な制裁が加えられる可能性が高くなっています。またそうなった場合に、インターネットは発信者を特定するのがそれほど難しくないことから、民事や刑事上の責任を負う可能性があることを自覚しておく必要があります。

インターネットというすばらしい道具を得て、私たちの情報空間はこれまでとは桁違いに広いものとなりました。この広大な情報空間にどのように対応していくのかということを、技術的な面から、また社会的な面からも学ぶ必要があるのです。

以上

摂南大学　情報メディアセンター