情報システム利用ガイドライン

１．はじめに

1.1 情報システムの目的

大阪工業大学（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「教育を通じて、社会・産業界において時代の要請に応じて活躍できる専門的職業人の育成を行う」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る。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ある。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しなければならない。

1.2 情報システム利用者の心構え

「情報演習室で、ログインしたままのパソコンを他人が操作して、いたずらメールを送信された。」、「他人の著作物を無許可でダウンロードし、著作権者から注意を受けた。」、「新しいパソコンをネットワークに接続して、OS のアップデートをしている間にウイルスに感染した。」等の事件が発生している。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ある。

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、次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すること。

(a)言論の自由、学問の自由

(b)他者の生命、安全、財産の侵害

(c)他者の人権、人格の尊重

(d)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ない。日本国内においては日本国内法が適用される。場合によっては海外の法律の適用を受ける可能性もある。法令や公序良俗に反する行為を行ってはならない。

(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・運営されるものである。これらの目的に該当する範囲で利用すること。

(4)利用規程と罰則

「情報センター規定および利用内規」に違反する行為をした場合には、警告、利用制限、所属部局への通報等の措置をとることがある。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することがある。

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る。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しなければならない。その他、他人の犯罪行為の手伝いをした場合は、幇助罪または従犯として処罰されることがある。以下の禁止事項および遵守事項に留意すること。

【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、基本的人権を尊重しなければならない。人種・性別・思想信条等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る。また、誹謗中傷は名誉毀損で訴えられることがある。

本学情報システムでは、利用者のプライバシーを尊重するが、利用者も他人のプライバシーを尊重しなければならない。

(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らない。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、利用者の責務である。利用者は、以下のような行為をしてはならない。

(a)他人のアカウントを使う

利用者は、他人のユーザー名を用いてログインしてはならない。この行為は不正アクセス禁止法で犯罪とされている。また、利用者本人のユーザー名で他人に本学情報システムを使用させたり、ファイル格納領域等の資源を使わせたりすることもこれに含まれる。

(b)他人の名前やユーザー名を騙る

他人の名前やユーザー名を騙って、電子メールを送ったり掲示板に書き込みを行ったりしてはならない。

(3)他組織への侵入

セキュリティホール等を利用してコンピュータシステムに侵入する行為も不正アクセス行為である。本学情報システムの内外を問わず、コンピュータに侵入したり、侵入を試みるような行為をしたりしてはならない。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おそれがあるだけなく、場合によっては国際問題に発展する可能性がある。

また、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はならない。例えば、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等があてはまる。また、コンピュータウイルスのなかには、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がある。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るので注意が必要である。

(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ある。絵画・小説・ソフトウェア等の著作物、デザインの意匠等を尊重することを心がけること。著作物の無断複製や無断改変はしてはならない。例えば、本・雑誌・ウェブページ等に提供されている文章・図・写真・映像・音楽等を、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、ネットニュースに投稿したりしてはならない。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る。

(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）には著作権がある。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（著作財産権）がある。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、ウェブページ等で公開したりすると、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請求されることがある。著作物の一部を利用したり、改変、翻訳、編曲、翻案したりすることも、著作権者に無断で行ってはならない。

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・共有されたりすることがあるので、十分な注意が必要である。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があるが、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したりすると、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る。

(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たりしてはならない。写真を撮られたり、その写真を公開されたりすることで、嫌悪感をもつ人も多く、このような行為をすると人格権の侵害や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る。

また、タレントやスポーツ選手等の有名人の写真は、それだけで経済的な価値があるので、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がある。

(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ならない。本学情報システムを用いてわいせつな文書・画像等を公開してはならない。また、それらへのリンクを提供してはならない。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、禁止する。

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

(b)人を自殺に勧誘・誘引する情報

(c)ネズミ講やマルチ商法等の勧誘

(d)セクハラ、アカハラ等に関する記述をともなうような情報

【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こと。

(a)氏名、住所、生年月日、電話番号、メールアドレス等、個人を特定できる情報

(b)病歴、持病、血液型等の医療情報

(c)家族・親族関係や出身地等の情報

(d)個人の趣味や嗜好等に関する情報

(e)借金の有無や残高等に関する情報

(f)銀行口座番号やクレジットカード番号、健康保険証番号等

(7)本学情報システムのセキュリティ保持への協力

上記の禁止事項や遵守事項のほかに、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る。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情報センターに通報する等が、これに該当する。

大学のネットワークは、多くのシステム管理責任者（以下「管理者」という）によって支えられている。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る。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すること。また、本学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情報センターに報告すること。

2.2 教育・研究目的に反する行為

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る。

(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ないこと。

(2)営利活動の禁止

広告・宣伝・販売等の営利活動と解釈される行為は、本学ネットワークで行わないこと。

(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する。

(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かないこと。

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る。ここでは簡単に触れておく。

(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なく、品位に欠けるメッセージの発信は謹むこと。

(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るので、十分注意すること。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すること。

(3)パスワードを適正に管理する

パスワードは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ある。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たりしないこと。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る。

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等にメモしないこと。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ある。

アカウントを盗用されても、直接的な経済的不利益は被ることはないであろう。しかし、パスワードを知られたために、そのアカウントから他人を侮辱する内容の電子メールが発信された場合、侮辱行為者として扱われたり、そ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、アカウントを盗用された被害者が、最初に犯

人として疑われたりすることがある。
パスワードは、「情報センター利用者パスワードガイドライン」等の各システムの運用ルールに従い定期的に変更すること。

(4)個人情報やプライバシー情報を守る
ウェブページ・ニュース・掲示板等に、個人情報やプライバシー情報を提供することは危険な行為である。例えば、懸賞応募のウェブページのなかには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ることがある。
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の悪性プログラムに感染し、これによって重要な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によって公開されたりすることがある。
ウェブページやブログで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等を放置したり紛失したりすることで、意図せずに情報が流出することがある。
また、共用のサーバコンピュータに置くファイルは、適切なアクセス権限を設定し、誰からも読める、または誰からも書き込めるという状態にはしないこと。そして、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ないようにすること。
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ある。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たり、他人の個人情報や機微(センシティブ)情報を流出させた場合には、法的に訴えられたりする可能性があるので、十分に注意をすること。

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こと
電子メールは、複数のコンピュータを中継して配送されるので、相手に届かないこともまれにあり得る。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たりすることで配送されないこともある。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すること。

(2)あいさつ、自己紹介等、手紙としてのマナーを守ること
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るが、そうでない人へのメールは、あいさつや自己紹介等を忘れないようにすること。

(3)宛先を間違えないようにすること
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る。また、大切なメールが意図しない人に届き、個人情報が漏洩することもある。メーリングリスト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う。メールを送信する前に宛先を確認すること。

(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) を使う。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ること。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る。他に誰に出したメールかを知られたくない場合は、Bcc に宛先を書くこと。

(5) サブジェクト（題名もしくは件名）をつけること

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する。内容を簡潔に表すサブジェクトをつけるように心がけること。

(6) 機種依存文字に関する注意

記号や罫線、絵文字等のなかには、特定の機種でしか表示できないものがある（ローマ数字（時計文字）や、丸数字（マルの中に数字）等)。また、いわゆる半角カナも使用しないこと。

(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こと。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る。他の方法がないか検討し、相手先に確認をして送るようにすること。

(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、管理者にも迷惑をかけるので、加担しないこと。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るので、よく確認をすること。

(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、配信中止の依頼も含めて返事を出さないこと。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る。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が、それらをクリックしないこと。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る場合があるので、メールアドレスの取り扱いは慎重に行うこと。

(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らない。すぐに返事が来ないことも想定しておくこと。

(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で不用意に公開しないことが望ましい。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る。そのような場合には、次のような方法をとるのがよい。

(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等で、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。

(12)メールの転送について

メールを転送する場合は、メールに添付されたファイルも転送されることを想定して、メールのサイズに気をつけること。添付ファイルのサイズは、なるべく小さくすること。また、メール本文の内容だけでなく、ファイルの内容についても転送して大丈夫なものかを確認すること。

また、教職員については、成績データ等の個人情報を含むデータや大学運営に関わる重要なデータを私的メールに転送しないこと。特に、フリーメールを使用していると、そこから情報が漏洩するおそれがある。

3.3 掲示板、SNS (Social Networking Service) 等の利用

(1)誹謗・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・中傷をしないこと。名誉毀損等で訴えられることがある。相手が特定できなくても、人種差別等、許されない発言がある。一般社会で許されないことはネットワーク社会でも許されない。

(2)フレーミング（炎上）に注意

ネットワークでは、些細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ある。冷静かつ誠実な対応を心がけること。

(3)掲示板毎のルールに従う

掲示板やSNS（Facebook、Twitter、LINE等）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ある。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。

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あるが、長時間にわたって過度な利用をすると、以下に挙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る。十分な休息と適度な運動を心がけること。

(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)対人関係等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あるが、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）と呼ぶ。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、アドウェア等、広範な種類のソフトウェアが含まれる。

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等の機能）を特徴としたプログラムである。コンピュータウイルスには、ウイルス、トロイの木馬、ボット等がある。

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等）をもたらす。

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ある。

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ことが可能な侵入口）を仕掛けるというものである。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、著名なサイト等を（数千、数万台の PC から）一斉攻撃するのに利用される。

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るが、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る。

スパイウェアは、トロイの木馬とほとんど同じであるが、特にユーザーに関する情報を収集するのに利用される。

アドウェアは、広告を表示する代わりに無料で利用できるソフトウェアである。なかにはユーザーに関する情報を無断で収集するものもある。

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 等）や被害など、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、この対策だけとっていればよいというものではない。

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

なお、ウイルス対策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等を定期的に更新しなければ意味がない。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るので、良く確認しておくこと。

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 にかけた言葉であるが、ウェブや電子メールを利用した詐欺の一種である。典型的なものは、「ユーザアカウントの有効期限が近づいています」とか「登録情報の確認をしてください」というような電子メールが届き、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偽サイトが表示される。実際にはそれは犯罪者が仕立てたサイトで、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のである。

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。

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たりすることもある。

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る。

(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。

(2) 正しい電子メールの知識をもち、リンクを安易にクリックしない。

(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。

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る。

フィッシング詐欺は様々な手口で行われているが、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る。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る。

4.3 ファイル交換（情報漏洩、著作権）

代表的なファイル交換ソフト(ファイル共有ソフト、P2P ソフトウェア)には、Winny、Share、Perfect Dark 等がある。これらのソフトウェアの利用にあたっては常に著作権侵害と情報漏洩がつきまとう。また、ファイル交換ソフトを狙ったウイルスが存在するほか、ファイル交換ソフトそのものにもバッファオーバーフローという基本的な脆弱性が存在するものがある。本学では危険と判断したファイル交換ソフトの利用ができないよう制限している。

ファイル交換ソフトそのものは有望なフレームワークであると考えられるが、ファイル交換ソフトの利用を正当化する理由は 1 つたりとも存在しないことを知るべきである。

ファイル交換ソフトを通じた情報流出は、もはやニュースになっても驚かなくなるほど一般的になった。問題の背景にあるのがコンピュータを利用する者の知識と注意の不足、そしてなによりも意識の欠如であるのは明らかである。

驚くべきことに、「ファイル交換ソフトそのものは悪くない」「刃物で殺傷事件があっても刃物が悪者扱いされないのと同様に…」といった議論が一部で行われているようである。しかし、ファイル交換ソフトのネットワークに一度流出した情報は、消去するのが難しい

構造になっており、使用するユーザーが増えれば増えるほど完全に消去するのができなくなる構造になっている。ファイル交換ソフトのネットワークに参加するということは、すなわち著作権侵害に加担することといってもいいのが現状であり、それが学問の府から行われて良いはずがない。

なお、同じファイル交換ソフトウェアに該当する BitTorrent については制限対象とは、していない。

4.4 情報発信

インターネットは、誰もが気軽に情報発信できるのがその特徴の 1 つである。以前から気軽に行うことのできた情報発信であるが、ブログや匿名掲示版、さらに、Facebook、Twitter、LINE 等の普及によって、敷居の高さはより低くなっている。

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り、コンピュータを利用しているため情報の再利用が簡単ということである。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慎重に行うこと。

特に慎重を期すべきなのは、個人情報である。自分の個人情報以上に、他人の個人情報の扱いについては、極めて慎重に行うこと。

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。基本的に、情報の送り手としては真意が伝わるよう厳密に誠意をもって対応し、情報の受け手としてはおおらかな気持ちで接することが大事である。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だろう。

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る。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る。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る。

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った。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、社会的な面からも学ぶ必要がある。

2014 年 3 月 26 日作成
2018 年 3 月 19 日改版
大阪工業大学
情報センター