C3301 教育テキスト作成ガイドライン（一般利用者向け）

国立情報学研究所 学術情報ネットワーク運営・連携本部  
高等教育機関における情報セキュリティポリシー推進部会

**改定履歴**

|  |  |  |
| --- | --- | --- |
| 日付・文書番号 | 改定内容 | 担当 |
| 2007年2月15日  A3301 | 新規作成（教育テキスト） | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2007年10月31日  A3301 | 「教育テキスト作成ガイドライン（一般利用者向け）」として、内容を一般利用者向けに見直し | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2015年10月9日  C3301 | 高等教育機関の実態に合わせた内容の見直し | 上田浩（京都大学）  須川賢洋（新潟大学）  中西通雄（大阪工業大学） |

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。

sp-comment[at]nii.ac.jp　（[at]を＠に置き換えてください）

担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

解説：本文書は独立した形で利用可能な、一般利用者向けの教育テキストです。内容はできるかぎり正確な記述とするよう心がけましたが、記述の簡潔さを優先したために一部不十分な表現になっていたり、逆に記述が重複しているところもあります。また、自習用のテキストではなく、講師が一般利用者の立場やスキルに応じて適切な助言を行いつつ講義を行うことを前提として、その講習用テキストとして作成してあることにご留意ください。

　このテキストは、「C2301 年度講習計画」に従って、60分ないし90分の基礎講習用として作成したものです。受講対象は、本学情報システムを新たに利用することとなった学生・教職員です。テキストの内容は、本学情報セキュリティポリシー（の各規程）に基づいて、できるだけ具体的にわかりやすい形で説明しています[[1]](#footnote-1)。

# **1. はじめに**

## 1.1 情報システムの目的

　本学情報システムは、本学の理念である「研究と教育を通じて、社会の発展に資する」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、運営されています。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、本学のセキュリティポリシー（運用基本方針、運用基本規程）や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

　「コンピュータ教室で、ログインされたままのパソコンを何者かが操作した。」、「他人の著作物を無許可でウェブサーバに置いて公開し、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てしまった。」、「研究室のウェブサーバがフィッシングに利用された。」などの事件が発生しています。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

**（利用の精神）**

(1) 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

**（法令の遵守）**

(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なりません。

**（目的外利用の禁止）**

(3) 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。

**（利用規程と罰則）**

(4) 「C2201 情報システム利用規程」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。なお、個々の部局等ネットワークの利用については、それぞれ規則が定められていますので、個別のルールに従ってください。

　以下、2章で具体的に説明しますが、1.3(1),(2)は本学情報システムに限らず一般の広域ネットワークの利用でも共通する事項であることに留意してください。

# **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、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、不正競争防止法、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とき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。例えば、次のような行為をしてはなりません。また、他人の犯罪行為の手伝いもしてはなりません。幇助罪として処罰されることがあります。

### (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。誹謗中傷は名誉毀損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。私信の無断開示などもそれにあたります。慰謝料の請求を受けることがあります。

他者の名前やログイン名をかたって、電子メールを送ったりSNSに書き込みを行うこともしてはなりません。

### (2) 不正アクセス行為

　利用権限は正しく使用せねばなりません。また、パスワードを盗まれて不正行為が行われないようにするため、パスワードを厳格に管理することは、システム管理者および利用者の責務です。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、自分の利用権限(アカウント)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。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。

(c) 不正アクセスを助長する行為

　直接に不正アクセスを行わなくとも、不正アクセスの用に供する目的で他人のパ

スワードを取得したり提供したり保管したりする行為も、同様に不正アクセス禁

止法違反として罰せられます。その為のフィッシングサイト、フィッシングメー

ルを作成・送信する行為も同様です。

### (3) 知的財産権の侵害[[2]](#footnote-2)

　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に心がけて下さい。 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、SNS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、映画、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されることのないようにするという働き（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。ただし、著作物の利用を永久に禁止すると、文化の普及や発展に悪影響を及ぼしますので、一定期間経過後は自由に利用してもよいことになっています。

　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、著作権者から損害賠償を要求されたり、罰せられることもあります。海賊版(違法に複製 された著作物)の音楽や映像を大学や自分のパソコン、スマートフォンなどにダウンロードすることも違法で罰せら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[[3]](#footnote-3)。

　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、ファイル共有ソフトウェアの設定によっては、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、ファイル共有ソフトを使ってはいけません[[4]](#footnote-4)。また、ディジタル著作物には、アクセス（利用）が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対象機器以外でゲームをできるようにしたりする装置やソフトウェアを販売したり配布すると、罰せられることがあります。

　また、コピーガードが外された著作物をコピーした場合にも著作権侵害に問われることがありますので、注意が必要です。

### (4) 肖像権、パブリシティ権の侵害

他人の肖像を本人に無断で写真に撮ったりインターネットに公開したりしてはいけません。写真を撮られたり公開されたりすることが、嫌悪感につながることも多く、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) 個人情報・機微(センシティブ)情報の漏えい

　以下に挙げるような、個人情報や機微(センシティブ)情報をパソコンやスマートフォ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。

1. 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
2. 個人の所在地などの位置情報

(c) 病歴、持病、血液型などの医療情報

(d) 家族・親族関係や出身地などの情報

(e) 個人の趣味や嗜好などに関する情報

(f) 借金の有無や残高などに関する情報

(g) 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

### (6) 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・図画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[[5]](#footnote-5)。詳しくは、「C3254 情報発信ガイドライン」を参考にしてください。

・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など）

・人を自殺等に勧誘・誘引する情報

・ネズミ講やマルチ商法の勧誘

## 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

　本ネットワークは本学の財産ですから、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。塾のプリントを作成したりすることもこれに含まれます。

(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たりするような過剰な利用は避けねばなりません。

(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くべきではありません。

# **3. 利用心得**

## 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下さい。

(2) 他人を思いやって利用する

　動画など大量のデータを送受信したりすると、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から、十分注意してください。また、共同で利用するコンピュータ設備は、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。

解説：ネットワーク帯域やチャネルを占有する行為との例として以下があります。

YouTubeなどの動画を長時間視聴する

ゲーム機やスマートフォンなどを学内無線LANに不必要に接続する

(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用いてはいけません。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。

　パスワードを他人に分かる状態にしないでください。メモが必要な場合は、自分なりに工夫して一目見ただけではそれがパスワードであることが分からないようにしましょう。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よく行われています。

　本学情報システム以外にもSNSやショッピングサイト、学外のメールサービスなど様々なサービスを利用するためにパスワードが必要となりますが、サービスごとに違うパスワードを設定するようにしましょう。パスワードを共通のものにしていると、万が一パスワードが漏えいした場合、それらのサービスが不正に利用されるだけでなく、あなたの学務情報などへの不正アクセスが行われるかもしれません。

　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計算機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。

強い(破られにくい)パスワードの例 : パスワードには、辞書に載っているような単語を避けること、および、英小文字だけでなく、英大文字・数字・記号を含めるようにしてください[[6]](#footnote-6)。

(4) 自己の情報を守る

　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・・SNSなどに、自分の個人情報やプライバシー情報、位置情報を提供することも危険につながります。

ウェブページやブログ・SNS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スマートフォン、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、ファイル共有ソフトウェア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。

このように、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、ファイル共有ソフトウェア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[[7]](#footnote-7)。

(5) 本学情報システムのセキュリティ保持に協力する

　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、不審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管理者に通報するなどが、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。ひとりひとりのネットワーク運用への協力が、よりよい教育・研究環境の構築につながることを自覚しましょう。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定められた窓口に報告してください。

## 3.2 メールの利用に関して[[8]](#footnote-8)

・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、遅れて届いたり、相手に届かないこともまれですがあり得ます。また、宛て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。

・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。

・宛て先を間違えないようにしましょう

メールの宛て先を間違えると、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、個人情報などが漏えい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うことがあります。メールを送信する前に宛て先を確認するようにしましょう。

・Cc、Bccの使い方

本来の宛て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。メールの宛て先(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知られたくない場合は、Bccに宛て先を書きましょう。

・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。

・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(リッチテキスト)形式のメールは、原則として使ってはいけません。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。

解説：当事者同士の合意を得た上でHTMLメールが使われる場合があります。

・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。

・メールの転送設定に関する注意

メールを自動転送している場合には、携帯電話などのアドレスを含め、転送先のアドレスが有効かどうか定期的に確認してください。届かないアドレスへの転送は、大学のメール配送システムに大きな負担をかけることに加え、授業に関するものなど、あなたへの重要な連絡が届かないことになります。

解説：スマートフォン等で直接メールシステムにアクセスできる環境が整備されている場合には、転送設定を推奨しない方が良いと考えられます。

・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す。

・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[[9]](#footnote-9)。また、自分のメールアドレスをウェブ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。

・PCのメールと携帯電話のメールとの違い

PC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。たとえ、すぐに返事が来なくても、怒ったりしてはいけません。

・メールアドレスの扱い

メールのアドレスはウェブ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。

(i) 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に掲載する。

(ii) 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、申込み専用の時限アドレスを使用する。

## 3.3 グループウェアサービスの利用

研究室や研究グループなどの情報共有にグループウェアサービスを利用することがあるかもしれません。情報漏えいを避けるため、利用にあたり公開設定、共有設定、情報の格付けが適切になされるよう留意してください。また、機密情報や機微情報を掲載することについての判断は慎重に行ってください。

解説：A大学では情報の格付けの対象は教職員のみを想定していますが、グループウェアサービスを研究に参加する学生が利用する場合には教職員の監督のもと、情報の格付け関連規定を学生にも遵守させる措置を取るなど各大学の判断が必要となります。

## 3.4 掲示板、SNS (Social Networking Service) などの利用

・誹謗中傷をしない

実名の場合はもちろん、匿名の掲示板であるからといって、誹謗・中傷をしてはいけません。名誉毀損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[[10]](#footnote-10)。

・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よくあります。冷静かつ誠実な対応を心掛けましょう。

・掲示板毎のルールに従う

掲示板や、SNS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。

## 3.5 ネットワークの過度の利用による悪影響

　パソコンやスマートフォンなど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、以下にあげるように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。

・対人関係などコミュニケーション能力の阻害

・学業成績の低下

・生活リズムが不規則になることによる心身障害

・姿勢や視力への悪影響

# **4. 情報セキュリティの基礎的知識**

## 4.1 インターネットのしくみ（IPアドレス、URL、HTTP）

(1) IPアドレス

PCをインターネットに接続して利用するためには、そのPCをインターネット上で一意に識別できるよう、住所や電話番号に相当する「アドレス」が必要となります。インターネットでは、「IPアドレス」と呼ばれるアドレス体系を利用します。具体的には32桁の2進数で表現されますが、それでは分かりづらいのでこれを8ビット毎に切って10進数で表現します[[11]](#footnote-11)。つまり、「192.168.0.1」のように0～255までの数字を4つ、ピリオドで区切って並べたものになります（図１参照）。

11000000.10101000.00000000.00000001

11000000101010000000000000000001

192.168.0.1

図１：IPアドレスの例

このようなIPアドレスは基本的にインターネット上で固有のものでなければなりませんが、様々な理由から「プライベートIPアドレス」と呼ばれるものも利用されています。

インターネットにおいて、データは「パケット」という形式により共有回線上でやりとりされます（パケット交換方式）。パケットは、元々送信しようとしていたデータ（例えば電子メールのデータ）にヘッダ（小包の表書きのようなもの）等を加えたものです。

すべてのパケットについて、ヘッダに発信元および宛先のIPアドレスが書き込まれます。従って、基本的にインターネットにおける通信は匿名ではないと考えるべきです。また、たとえどのような暗号化を行ったとしても、「どのコンピュータから情報が発信されたか」「どのコンピュータ宛てに情報が送信されたか」という記録は残ります。暗号化しなければ基本的に万人が観察可能な状態で通信が行われますので、インターネットは安全であることを仮定することができない通信手段ということができます。電子メールにしてもウェブにしても、せいぜいはがき程度の秘匿性しか持ち合わせていません。機密性の高い情報は必ず暗号を利用するべきです。

(2) ドメイン名

さて、このようなIPアドレスを覚えるのは現実的ではありません。そこで、コンピュータにニックネームを与え、そのニックネームをIPアドレスに変換するシステムを考えます。これをDNS（Domain Name System）と呼びます。これにより、例えばwww.kantei.go.jpという「ドメイン名」をIPアドレスに変換することができます。ドメイン名は階層的な構造を持っており、ある程度類推をすることもできるといった特徴があります。

このドメイン名は安全なウェブの利用で重要なポイントとなりますので、どのドメイン名がどの企業や大学等の組織（のサービス）のものであるか、重要なものについては覚えておくようにしましょう。特に金銭や個人情報等の取り扱いに注意が必要な情報のやり取りを伴うサイト、つまり銀行等の金融機関、ショッピングサイトなどについては重要です。

(3) URLとHTTP

ウェブでは、URL（Uniform Resource Locator）という形式で情報の入手元を指定します。これは、図２のような構造を持ちます。

スキーム　オーソリティ　　　　　　　　パス

http://www.example.com/jp/link.html

図２：URLの構造

一番左の「http://」が「スキーム」で、情報（正確にはリソースといいます）にアクセスするための方法を指定します。次が「オーソリティ」で、そのリソースを管理しているコンピュータを指定します。オーソリティにはドメイン名やIPアドレスを利用することができます。最後がパスで、そのオーソリティのどこにリソースがあるのかを指定します。ここでは「jp」というディレクトリ（フォルダ）の中にある「link.html」というファイルを指定しています。

ここで利用されているスキームはHTTP（Hyper Text Transfer Protocol）です。これは文字通り「転送」のためのプロトコル（決まり事）です。ウェブブラウザはURLに書かれているオーソリティにアクセスし、パスをたどってファイルを取得して表示等を行います。つまり、ウェブブラウザは基本的にダウンロードのためのシステムであるということができます。ここは重要なポイントです。ウェブはテレビ放送のように一方的に送りつけられている情報を受動的に画面に映しているわけではなく、あくまでも自分でリクエストした情報をダウンロードしているのです。IPアドレス等の情報がリクエスト先に残りますし、自分が望まないデータ（コンピュータウイルスなど）をダウンロードしてしまうこともあり得るのです。

HTTPでは、ダウンロードだけでなく情報を送信することもできます。これによって、通信が双方向となり、より様々なサービスを受けることが可能になりますが、逆に言えばウェブを通じた自覚・無自覚の情報漏えいというものも起こりえますので注意しましょう。

## 4.2 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あって宿主を必要としないところが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[[12]](#footnote-12)。ここではIPA（情報処理推進機構）による「パソコンユーザのためのウイルス対策 7 箇条[[13]](#footnote-13)」を紹介しておきます。

最も重要なのは、アンチウイルスソフトウェアを導入しておくことです。本学ではアンチウイルスソフトウェアの全学ライセンスを取得していますので利用してください。

解説：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。次の3種類のソフトウェアを紹介しておきますので、検討して「自分の」パソコンに導入しておきましょう(無料で利用できる条件として、非営利の条件がついているものもありますので注意)。

avast! [[14]](#footnote-14)

Avira[[15]](#footnote-15)

AVG® Anti-virus Free Edition[[16]](#footnote-16)

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。これらのソフトウェアはいずれも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。

## 4.3 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、クレジットカードの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. ウェブブラウザやアンチウイルスソフトウェア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

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。

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。

## 4.4 ファイル交換（情報漏えい、著作権）

BitTorrent, Shareなどのファイル共有ソフトウェアの利用には常に著作権侵害とウイルス感染による情報漏えいがつきまといます。本学では、利用規程でBitTorrent, Share, WinnyなどのP2Pソフトウェアの利用を禁じていますので、それらのソフトウェアを利用してはなりません。

## 4.5 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SNS、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ですから、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、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。最近の事例としては、SNSで、学生が遊園地のアトラクションで業務妨害を行ったこと、飲酒運転などの違法行為を告白し、社会的に非難を浴びたことなどがあります。真実かどうかは別として、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、インターネットで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すら負う可能性があることを自覚しておく必要があります。

## 4.6 関連情報

IPA、NISC、JPCERT/CC、@Police(警察庁) などが情報セキュリティに関する最新情報を発信しています。これらを日々チェックするようにしてください。

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。

1. 教育を担当される教員の方へ : 学生に対して「情報リテラシー」などの講義の中で実施する場合には，一回ですべてを教えてしまうのではなく，毎回の講義の中で関連する部分をとりあげていくのがよいでしょう(マイクロインサーション)。例えば，個人のウェブサイト作成の授業ときに著作権に関することを教えるなどして，工夫してください。 [↑](#footnote-ref-1)
2. 著作権侵害とならない引用や私的使用については，講義時間に余裕がある場合は触れておくのがよいでしょう。特に，引用については，ウェブによる情報発信方法の講義や，レポートの書き方の講義で説明すべきです。 [↑](#footnote-ref-2)
3. 受講対象者によっては，著作権法違反になりうる具体例を挙げて説明するのもよいでしょう。 [↑](#footnote-ref-3)
4. 「情報システム利用規程」(C2201)の第十条十五項で、教育研究目的以外でのP2Pソフトウェアの利用は禁止されています。 [↑](#footnote-ref-4)
5. 各大学で発信する情報をどこまで禁止しているかに依存します。 [↑](#footnote-ref-5)
6. これらの文字を含まないようなパスワードは設定させないようにしているシステムもあります。 [↑](#footnote-ref-6)
7. ここでは，主に個人的なレベルの個人情報の取り扱いに関する注意を述べています。業務として，一定規模以上の個人情報を収集し取り扱う場合は，個人情報保護法（国立大学法人の場合は、独立行政法人等個人情報保護法）の規定や，本学情報格付け規定に従う必要があります。 [↑](#footnote-ref-7)
8. 詳細は、C3252 電子メール利用ガイドラインを参照のこと。 [↑](#footnote-ref-8)
9. フィッシングメールは，その内容が非常に巧妙なものもあり，利用者がフィッシングメールであることに気づかずに対応してしまう危険性もあるので，必要に応じて具体例をあげて解説を行うとよいでしょう。 [↑](#footnote-ref-9)
10. 匿名の掲示板等であっても，捜査機関等からの要請があれば，ログ情報から利用者が特定されます。 [↑](#footnote-ref-10)
11. IPv4 の場合。 [↑](#footnote-ref-11)
12. マルウェア(malware, malicious software) とは，悪意的なソフトウェアという意味の造語で、ネットワークやコンピュータに何らかの被害をもたらすように作られたソフトウェアの総称。 [↑](#footnote-ref-12)
13. http://www.ipa.go.jp/security/antivirus/7kajonew.html [↑](#footnote-ref-13)
14. http://www.avast.com/jpn/download-avast-home.html [↑](#footnote-ref-14)
15. http://www.avira.com/ [↑](#footnote-ref-15)
16. http://free.grisoft.com/ [↑](#footnote-ref-16)