情報モラル・セキュリティについて

Contents

京都教育大学 KYOTO UNIVERSITY OF EDUCATION

大阪教育大学 OSAKA KYOIKU UNIVERSITY

奈良教育大学 Nara University of Education

情報モラル・モデル

情報社会の倫理

■ 情報社会への参画において、責任ある態度で臨み、義務を果たす
■ 情報に関する自分や他者の権利を理解し、尊重する

約束、プライバシー、モラル、肖像権、個人の尊重

法の理解と遵守

■ 情報社会の活動に関するルールや法律を理解し、適切に行動する
■ 契約の内容を正確に把握し、適切に行動する

著作権、情報セキュリティポリシー、規範意識

公共ネットワーク社会の構築的な

■ 情報社会の一員として、公共的な意識を持ち、適切な判断や行動ができる

ステマ、マツリ、デジタル・デバイド

日常モラルの側面
心を磨く

カリキュラムの概要

安全への知恵

■ 危険を予測し被害を予防するとともに、安全に活用する
■ 情報を正しく安全に活用するための知識や技術を身につける
■ 自他の安全や健康を害するような行動を抑制できる

SPAM、脆弱性（ぜいじゃくせい）、依存、スマホ老眼

情報セキュリティ

■ 情報セキュリティに関する基礎的・基本的な知識を身につける
■ 情報セキュリティの確保のために、対策・対応がとれる

ID、認証、ペアレンタルコントロール、フィルタリング、暗号化

安全の側面
知恵を磨く

文部科学省発行「教育の情報化に関する手引」より引用

大学側がしていること

外部（インターネット）との通信制限（ファイアウォール）

大学の共同利用PCは、直接インターネットにアクセスできないよう、間に「壁」を設けています。これは、大学の外からの様々な攻撃から、皆さんの情報を守るためです。皆さんが利用するPCがコンピュータウイルス（以下ウイルス）などに感染した場合に、大学の外に伝染させ迷惑をかけてしまうことを防止するためでもあります。
このため、大学のネットワークとインターネットの間に「ファイアウォール」という仕組みを準備して、必要な通信だけを通過できるようにしています。

ウイルスへの対応

写真などのデータを友人とメールで交換することも多いと思いますが、友人や知人を装って、ウイルス等の不正プログラム（マルウェア）が送られてくることがあります。ウイルスに感染すると、自分のコンピュータが使えなくなるだけでなく、他の利用者に迷惑をかけることにもなります。
大学では、そのような事態を防ぐために、ウイルス対策ソフトを導入し、定期的に最新のウイルス定義ファイルに更新して、新種や変種のウイルスにも対応できるようにつとめています。しかし、未知のウイルスは、検出できませんので、皆さんの所に届いてしまうこともあります。メールの添付ファイルや実行形式（EXE形式等）のファイルは、むやみに開かない習慣をつけてください。

アクセスログの収集

大学の共同利用PCにログオン・ログオフしたことや、印刷したこと、どのサイトにいつアクセスしたかなど、様々なネットワーク利用に関する履歴を、大学では収集・蓄積しています。これを「アクセスログ」と呼んでいます。アクセスログは、不正な利用がないかを点検することで、皆さんや大学が不利益にならないようにするために収集しているものです。むやみに公開するものではありませんが、問題のある利用があった場合など、必要に応じて適切な機関にアクセスログを提供することがあります。

情報セキュリティポリシーによる明文化と周知

大学における情報システム利用の基本ルールとなるものを情報セキュリティポリシーと呼びます。その組織に属する全ての人が理解し、遵守することで、組織として安全・安心して活動できるように策定しているものです。網羅的に記載されている情報セキュリティポリシーを教員や学生などの対象者にあわせ、メールやWebなどのサービス別にまとめて、より判り易くしたものをガイドラインと呼んでいます。
皆さんがこれらの明文化されたものに沿って行動できるように、大学は周知と点検を行なっています。

CSIRT（シーサート）

コンピュータやネットワークに関して、セキュリティ上の問題（インシデント／事案）が発生したときに、対応の中核となる組織を、CSIRT(シーサート)と呼び、大学や政府・行政機関で設置がすすんでいます。災害時に備えて日常生活で避難経路を確認することや、110/119などの通報のしかたを知っておくことと同じように、学生生活やアルバイト・ボランティア活動など、それぞれの活動シーンごとに、セキュリティ上の問題が起きた時にどこに連絡すればよいのかを確認しておきましょう。

情報モラル・セキュリティについて
私たちが気をつけるべき
9つの大切なこと

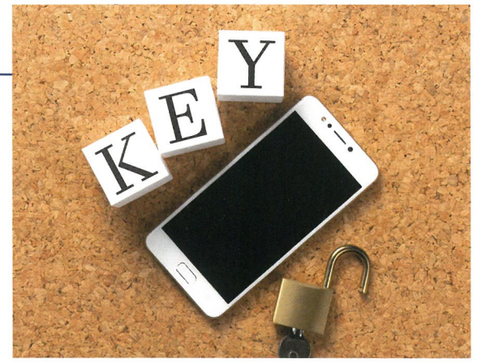
情報セキュリティって何？

「守るべき情報」へのアクセスを「認められた人だけ」が、その「正確な情報」を、「必要な時に使うことができる」状態を維持することを指しています。情報セキュリティは、

- ネットワークやシステムによる技術的なセキュリティ
- パソコン、USBメモリ等の適切な管理や部屋の施錠といった物理的なセキュリティ
- 規則の遵守や適切な運用といった人的なセキュリティ

のそれぞれについて考える必要があります。特に人的なセキュリティでは、「USBメモリを落とさないように」といった注意喚起だけではなく、「人は必ずミスをする」という前提で被害を最小限にする発想で考えていくのが基本です。

アカウントの適切な利用



アカウントとは、コンピュータ・ネットワークの利用資格のことで、組織から一人に対して1つずつ割り当てられます。利用時にアカウントをチェックすることを認証といい、通常、利用者IDとパスワードを入力することで行われます。

大学が発行するアカウントは、大学生活の中でメールなどの各種サービスの基本となっているとともに、大学外のサービスとも『認証連携』と呼ばれる仕組みによって、利用できるようになっています。

パスポートや運転免許証を他人に貸すことが極めて危険なことであるのと同じように、自分のアカウントを他者に使わせたり、他者のアカウントを使ったりするのは、良くない行為です。

他人のアカウントを使う行為は、「なりすまし」と呼ばれます。ずさんなパスワード管理が原因で「なりすまし」をされてしまい、それにより誰かが不利益を受けた場合、損害賠償を請求されることがあります。

パスワードは決して他人に知らせてはいけません。また、簡単に推測できるような単純なパスワードは使わないようにし、他人に知られないよう適切に管理してください。

また、SNSなどの大学と連携していない企業や機関が運営している外部サービスに、大学の発行したアカウント情報（利用者IDとパスワード）をそのまま登録して使ってはいけません。そのサービスからアカウント情報が漏えいした場合、芋づる式に大学のアカウントを悪用されてしまう危険性が高まります。

多要素認証による自衛

パスワードのみによる認証は、パスワードが漏洩するとただちに不正アクセスされる恐れがあり危険です。メール等の重要なサービスは、複数の要素を使って認証を行なう多要素認証が採用され、パスワードに加え、指紋や虹彩、顔などの生体情報、スマホなどのデバイスといった所有機器情報など、本人以外が持つことが難しいものを要素として認証できるようになっています。最初の準備が面倒ですが、取り返しがつかないことになる前に備えておくといいでしょう。

著作権・著作物について

「引用」という言葉を聞いたことがありますね。大学生活ではレポートなどで文献から引用してまとめることが多くなってくるかもしれません。この「引用」には以下のようなルールがあります。

- 自分の文章が「主」で、引用部分が「従」となる文章量と扱いであること
- 引用部分が明らかに本文と区別できること（「」などで囲む、字体を変えるなどといったことです）
- どこから引用したのか、出典を明らかにすること（そのために、引用されるものは既に公表されている著作物であること）

これらのルールが守られないと「盗用」となり、不正行為となります。

他人の著作物を利用する場合、「権利者の了承を得る」というのが基本ですが、その手続きを省略できる例外として、「引用」や「私的利用のための複製」などがあります。

これらのことは、「著作権法」などの関連法令で定められているのですが、これらは情報化の進展に伴って年々改訂されています。最新の法令について知っておくことも大事ですが、「著作者に迷惑をかけない」「自分の著作物はちゃんと主張する」ということを意識して行動していくとよいでしょう。

大切なデータを守る

他人の個人情報が大量に保存されているスマートフォンを落とした際、拾った人が勝手に中の情報を読めたり、メールやLINEなどが使えたり、といった状態にならないように、「ロック」機能を設定していますよね。

同様に、PCなどを利用するときも、離席する際には必ずロック状態にするようにしましょう。

重要なデータをネットワークでやりとりするときには、途中で第三者に覗き見されるリスクを軽減するよう心がけましょう。メールは通常暗号化されずにやりとりされるので、重要なデータを添付ファイルで送ってはいけません。Webを用いてやり取りする場合は、暗号化された通信方式(https)かどうかを必ず確認するようにしましょう。メールや、暗号化されていないWeb(http)など、安全でない方法でデータをやり取りせざるを得ない場合、ファイルそのものを暗号化してから送るなどの対策をとりましょう。

個人情報の取り扱い

個人情報保護法などの施行後、個人情報の取り扱いに対する皆さんの関心も高くなっていると思います。しかし、一部には間違った解釈も広がっていて混乱しているケースも見受けられるようになってきました。大学において、皆さんを「顧客」と考え、民間企業と同じように、顧客保護のために、事前に利用目的の特定や明示を行い、必要な情報のみを収集すべき、といったものがそうです。

教育現場という所は、学生や教員が相互に自由な情報交流を保障することで初めて教育目的が達成されるところです。また、学生同士が共に影響しあいながら学ぶことができるように教員が動くためにも、不断の情報共有も必要でしょう。

そのため、大学は、教育を実現して行くために必要と判断した場合には「教育のため」という利用目的で情報を求め、大学内で共有していくことを行います。皆さんも、大学内の情報共有には、積極的に関与してください。

しかし、大学の外に向けての情報発信については事情が違います。ホームページなどに掲載する場合は、たとえ新聞などで表彰などの事実が公表されたことでも、事前に本人（未成年の場合は保護者も）に公開に関する同意を得る必要があります。また、クラブなどで集合写真を公開する場合などは、写っている人全てに事前に同意を取らないと「肖像権の侵害」となってしまいます。「大学からの情報発信」という社会的責任の一翼を担うことになりますので、判断に迷った場合は関係部署に相談してください。

端末(PC,スマートフォン,タブレット等)を守る

基本ソフト(OS)やアプリケーションなどのソフトウェアは、利用が保証されている（サポートがある）ものを選ぶとともに、脆弱性対策等で提供される更新プログラムを随時適用し、常に最新状態にしておきましょう。特にフリーソフトをインストールする際には、マルウェアやアドウェア（不快な広告を表示するソフト）が含まれたあやしいものでないことを事前にインターネットで調査した上で導入するように心がけたほうがよいでしょう。

メール・掲示板のマナー

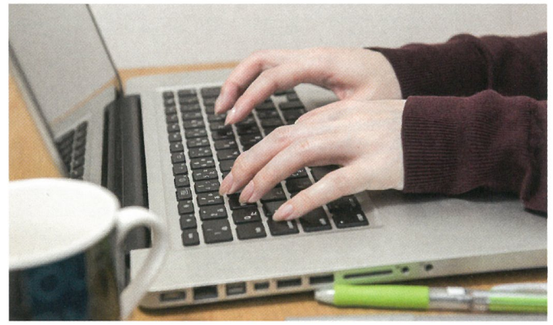
メールはとても便利なものです。メールで課題を提出することや、就職希望の企業の人事担当者とメールをやりとりすることなどもあるでしょう。

しかし、説明が足りなかったり、独りよがりな内容のメールを送ると、受け取った相手を困惑させたり、思わぬ誤解を招いてしまう恐れがあります。

また、送信先を間違ってしまうことも、よくあることです。宛先不明で返ってくればいいですが、宛先が存在した場合は、全く別の人に読まれてしまうことになります。送信する前に送信先や内容をもう一度確認しましょう。

公的なメールでは、はじめに自分のことを名乗るのがマナーです。LINEと同じような感覚で、名前も挨拶もなしに改行しない文章でメールを送ると、相手に失礼になることがあります。

1人で複数のメールアドレスを使用している人も多く、仕事用、プライベート用といった形で、用途を使い分けているケースがあります。社会人の場合、社内規定によって、仕事用のメールアドレスを仕事以外の用途で使うことが禁じられている場合がありますので、みなさんも相手のメールアドレスの用途を意識して送信先を選ぶようにしましょう。



また、「質問」「先日の件について」というような内容がわからない件名（Subject）を避け、メールの内容を示す件名をつけるように心がけましょう。特に、レポートなどの場合は、学籍番号、氏名、どの授業のものか、などの情報も記載しておくことも必要ですね。

デジタル万引き

本屋さんで、購入前の本のページを携帯電話のカメラで撮影して持ち帰ったり、メールで友だちに送ってあげたりする行為のことを『デジタル万引き』と呼んでいます。

私たちは、社会の一員となるべく、幼い頃から『他人のモノを取ってはいけない』ということを徹底されてきました。ですので、駄菓子屋さんや八百屋さんの店頭に並んでいる商品を取っていくのは良くないことと知っていますし、そういう行動をするときには、多少なりとも罪の意識との葛藤が生じているでしょう。

このような、形があって目にみえる「モノ」（有形的存在）のことを、「有体物」と呼んでいます。例えば、机や、鉛筆、隣のお家の柿などがそうですね。一方で、形がなく、目にみえない「モノ」（無形的存在）のことを「無体物」と呼んでいます。例えば、音楽や、詩、歌、におい、電波、ソフトウェアなどがそうですね。

この「無体物」を奪う行為に関しては、あまり深く考えることなく行ってしまいがちです。例えば、インターネットに違法にアップロードされた漫画や動画などを見ることに対しては、なんとなくダメなんだろうとは思いつつも、万引きのような「罪の意識」を感じるという人は少ないでしょう。

しかし、「見たからって減るものじゃないし、別にいいやん」「誰も損してないし」というような考えでこのような行為を正当化してしまって良いのでしょうか？

実は、ここで、奪ったものが「無体物」であり、その無体物に対し「対価を支払っていない」利用になっているのです。

『デジタル万引き』により、「情報」が不当に盗まれることで、出版社や著作者が不利益にならないように、私達自身で気をつけて行動していきたいですね。

役立つ情報モラル・情報セキュリティ関連サイト

次のようなサイトでは、
情報モラルや情報セキュリティに関する情報提供や教材が豊富に発信されています。

（2020年3月現在）

先生向けコンテンツ類

情報モラル教育の充実（文部科学省）
https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1369617.htm

情報化社会の新たな問題を考えるための教材<児童生徒向けの動画教材、教員向けの指導手引き>
https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1416322.htm

情報モラル指導実践ガイドブック（平成18年度文部科学省委託事業「情報モラル等サポート事業」）
http://www.kayoo.org/moral-guidebook/

やってみよう情報モラル教育（平成19年度文部科学省委託事業「情報モラル指導ポータルサイト」）
http://jnk4.info/www/moral-guidebook-2007/

情報セキュリティ啓発（IPA 情報処理推進機構）
https://www.ipa.go.jp/security/keihatsu/features.html

情報セキュリティ広場（警視庁）
https://www.keishicho.metro.tokyo.jp/kurashi/cyber/

学習コンテンツ類

著作権に関する教材、資料等(文化庁著作権課)
https://www.bunka.go.jp/seisaku/chosakuken/seidokaisetsu/kyozai.html

ネット社会の歩き方(一般社団法人日本教育情報化振興会)
http://www2.japet.or.jp/net-walk/

伸ばそうICTメディアリテラシー(総務省)
https://www.soumu.go.jp/ict-media/

情報モラル指導用に開発した教材（岩手県総合教育センター）
http://www1.iwate-ed.jp/tantou/joho/moral/

あんしんしてインターネットをつかうために 国民のための情報セキュリティサイト キッズ（総務省）
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kids/index.html

企業などで発信している教材

ミッキー&フレンズとネチケットを学ぼう（ウォルト・ディズニー・ジャパン株式会社）
https://kids.disney.co.jp/netiquette.html

情報モラル教材ダウンロード（株式会社ジャストシステムズ）
https://www.justsystems.com/jp/school/coneta/moral/index.html

本リーフレットに関する照会・お問い合わせ

京都教育大学情報処理センター
〒612-8522 京都市伏見区深草藤森町1番地
Tel (075) 644-8340
mail ipc@kyokyo-u.ac.jp

大阪教育大学情報セキュリティ
インシデント対応チーム（OK-CSIRT）
〒582-8582 柏原市旭ヶ丘4丁目698番1号 E棟
Tel (072) 978-3772
mail csirt@ml.osaka-kyoiku.ac.jp

奈良教育大学
次世代教員養成センター情報館
〒630-8528 奈良市高畑町
Tel (0742) 27-9703
mail ipc@nara-edu.ac.jp