

## 京都産業大学インターネット利用に関するガイドライン

### 1. はじめに

インターネットは便利な道具であり、たくさんの利便性を持ち、様々な可能性を秘めています。大学生活や一般社会において、これをいかに使いこなすかは非常に重要な課題です。

インターネットを活用する上で、欠かせないことはルールの遵守です。便利だからと言って何でもして良い訳ではありません。パソコンやスマートフォンなどからネットワークを利用するにあたり、「京都産業大学ネットワークセキュリティ規程」および各種法令を遵守してください。京都産業大学ネットワークセキュリティ規程については、本学 Web ページ「コンピュータ環境の使い方(<http://www.kyoto-su.ac.jp/ccinfo/>)」内、「情報センター規程一覧」に掲載していますので、必ず確認してください。

このガイドラインでは、そのうち特に重要な項目について具体的に説明します。

なお、違反行為をした利用者については、本人に通知することなく、当該行為の停止、利用停止等の処置を行うことがあります。

### 2. 法律・規則による遵守事項

インターネットの世界でも法律は適用されます。利用者が相互に権利を尊重し合い、ルールを守って気持ちよくネットワークを利用してください。

#### 2.1. 人権（人格権，プライバシー権，肖像権等）について

日本国憲法第 3 章第 13 条には「すべて国民は、個人として尊重される。生命、自由及び幸福追求に対する国民の権利については、公共の福祉に反しない限り、立法その他の国政の上で、最大の尊重を必要とする。」と定められており、民法第 709 条には「故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う。」と定められています。

当然のことですが、他人の悪口や個人情報、プライバシーを言いふらしてはいけません。これらの行為は他人の人権を侵害します。ブログや Twitter などのネット上であっても同じことです。写真をブログに載せる場合などでも、写り込んでいる人に、ネットに載せることに不都合がないか許可を求める必要があります。

#### 2.2. 著作権について

著作権は、産業財産権と共に知的財産権に含まれる権利の一つです。「知的財産権」とは、知的な創作活動によって何かを創り出した人に対して付与される、「他人に無断で利用されない」といった権利です。著作権は、手続きを一切必要とせず、著作物が創られた時点で「自動的」に付与されることが、国際的なルールとなっています。

簡単に言えば、著作者の許可なしに著作物を複製したり、二次利用してはいけない、ということを決めています。

	著作権	.....	著作者の権利，著作隣接権
知的財産権	産業財産権	.....	特許権，実用新案権，意匠権，商標権
	その他	.....	回路配置利用権，育成者権，営業秘密等

身近な例では，次のような行為が著作権侵害となります。

- ・ インターネットに不正に置かれたビデオや音楽等をダウンロードする行為
- ・ 著作権の存在するビデオや音楽等をコピーして人にあげる行為
- ・ 雑誌を立ち読みして，気に入ったページを写真に撮る行為
- ・ 二次利用が許可されていない画像を自分のブログに使う行為

著作権を侵害すると刑事罰（著作権法に定められた懲役や罰金）の他，民事訴訟による損害賠償請求を受ける可能性があります。

著作権には，許諾なしに複製を可能とする条件も定められています。私的利用に限って複製を認める条項（著作権法第 30 条）と，学校での教育現場に限って複製を認める条項（著作権法第 35 条）がありますが，何れも条件を拡大解釈しないよう注意してください。一言で言えば，著作者から訴えられるような利用の仕方をしてはいけません。引用（著作権法第 32 条）についても同様です。なお，学校の機材を用いて行う複製は私的利用とは認められません。

### 2.3. 本学規程について

個人に発行されたユーザ ID とパスワードは，それぞれが責任を持って管理する義務があります。ネットワーク上で何らかのトラブルが発生した場合は，それに用いられたユーザ ID の所有者に責任が問われます。ユーザ ID を人に貸す行為は認めていませんので，パスワードを他人に教えてはいけません。なお，どのような場合でも，大学がパスワードを尋ねることはありません。言葉巧みにパスワードを聞き出して悪用する事例がありますので注意してください。

また，本学の ID は教育・研究を目的として発行されています。教育研究の目的にそぐわない利用方法は慎んでください。例えば，学習に必要な画像・音楽・動画ファイルを大学のサーバに保存することや，政治・宗教活動などを行ってはいけません。

自分の情報を自分で公開することは法律上禁じられていませんが，本学ネットワークセキュリティ規程では，不要なトラブルを避けるため，自己の情報をみだりに公開することを禁じています。ストーカー被害などに遭わないためにも，不用意に情報を出さないようにしてください。

なお，スマートフォン等 GPS 付機器で撮影した写真には位置情報が埋め込まれている場合があります。自宅で撮影した写真をブログ等に掲載すると，その写真から自宅の位置が分かることとなりますので，位置情報を削除してから掲載するなど，注意が必要です。

### 3. マナー，心得

インターネットは単なる道具・テクノロジーではなく，手紙や電話と同様に社会性をもった通

信手段であり、一種の社会的空間です。文字のみのコミュニケーションもあり、相手の意図することを誤解したり、こちらの意図することが理解してもらえなかったりして、互いに不快な思いをすることがあります。この様なことを避けるためにも、マナーを身に付けて、全ての人が快適に利用できるように心掛けましょう。

### 3.1. 名乗る

インターネットで電子メールの受送信や Web を介した問い合わせなどを行う際は、まず所属と本名を名乗りましょう。気心の知れた相手でない限り、それが礼儀です。

### 3.2. インターネットは匿名ではない

必要に応じて、本名の代わりに匿名性のあるハンドル（ネーム）という別名を用いる場合があります。自分で考えたニックネームを本名の代わりに利用することで、ネットワーク上でプライバシーを守りながら活動を行うことができます。

しかし、しばしば匿名だからと無責任な発言がされることが見受けられます。「匿名でなければ情報発信できない」と思うような内容は発信してはいけません。高い人格を持ってインターネットを利用してください。

そして、一見、匿名性がありそうに見えるインターネットですが、大抵の場合、個人を特定することが可能です。警察が調べれば、いつどのパソコンからアクセスしたかが分かりますし、ブログの書き込みや写真などに含まれるヒントを集めて解析することでも個人を特定できることがあります。

### 3.3. インターネットへ発信した情報は取り消しができない

インターネット上の情報はどんどんコピーされます。検索サイトが取り込んだり、誰かがブログに引用したりする他、インターネット上の全てのデータを定期的に収拾しているサイトもあります。このため、一度ネット上に出した情報は取り消すことができないと考えてください。

### 3.4. 文字だけではニュアンスは伝わらない

インターネット上での情報交換の多くは、文字によって行われます。文字だけでは互いの顔が見えないため、表現のニュアンスを意図したとおり伝えることができない、もしくは相手の持つ文化的背景が違うなどの要因から、誤解やトラブルが発生することがあります。

情報を発信する際は相手のことをよく考え、意図することが間違いなく相手に伝わる内容であることを確認しましょう。

### 3.5. 反社会的な情報を発信しない

「未成年だが酒を飲んだ」「高速道路で 150km 出した」など、反社会的な内容を発信すると、大勢からバッシングを受けるでしょう。たとえ冗談でもそのような内容を書き込むべきではありません。

### 3.6. ブログや Facebook などは友達以外の人も見ている

ブログや Facebook などに書き込んだ内容は、世界中の誰もが見ることができます。たとえあな

たが友達限定にしているとしても、友達の誰かがシェア（引用して発言）すると、その発言は制限なしに誰でも見ることができます。

「友達グループしか見ていない」、または「自分の発言なんて誰も見ていない」と思うのは大きな間違いです。ネットへの書き込みは、誰に見せても問題のない内容に留めましょう。

### 3.7. 郷に入っては郷に従え

インターネットには独特の文化があります。例えば質問サイトでは、質問を行う際には既に同じ質問がされていないか調べてから行う、早く回答を貰おうとたくさんの掲示板にマルチポストしてはいけない、質問のタイトルには「質問」とだけ書いたりせず何の質問かわかるようにする、などがあります。

これらの文化はサービス、サイト毎に少し違っていますので、新しいサービスを利用する際は、まずその雰囲気慣れることから始め、マナーを学んでから本格的に利用しましょう。

### 3.8. 情報を鵜呑みにしない

どのようなメディアにも言えることですが、メディアが発信する情報は正しいものばかりではありません。間違いや思い込みで誤った情報が書かれていることもありますし、情報操作を目的に、わざと事実と違うことを書いている場合もあります。特にインターネットは誰でも手軽に情報発信できるため、誤った情報が多く含まれます。

情報の真偽を見極める目が必要です。例えばステルスマーケティングと呼ばれる、消費者に気付かれないように宣伝する（桜が個人の口コミを装ってある商品を褒めるなどの）行為があり、近年問題となっています。

重要な情報は、複数のメディア（ネット、新聞、雑誌、書籍、テレビ、聞き込みなど）を用いて、総合的に判断しましょう。

## 4. 安全対策

セキュリティの意識を持たずにインターネットを利用すると、自分自身または第三者が不利益を被る事件に巻き込まれてしまう場合があります。また、コンピュータウィルスなどに感染したコンピュータをそのまま利用してしまうことで、意図せずトラブルを拡大させてしまうことも考えられます。

必要な知識と意識を持って、全ての人が快適に利用できるように心掛けましょう。

なお、学内ネットワークで、自分のユーザ ID を知らない間に他人が使用しているのではないかという形跡がある場合や、ウイルス、マルウェアに感染した形跡がある場合は、速やかに情報センターに連絡してください。

### 4.1. パスワード管理

昨今、新聞やTVなどのマスメディアでも報道されるように、ネットワークに不正侵入したり、他人のユーザ ID を不正に使用して混乱させたり、情報を不正に入手したりする人々がいます。ユーザ ID を不正に使用されないために最も単純で確実な方法は、自分のユーザ ID に適切なパスワードを設定することです。

パスワードを盗む手法の一つに「コンピュータを用いて総当りで順に試す」というものがあります。この攻撃では、短時間で効率よく解析するために、短い桁数から試す、数字だけの組み合わせから試す、辞書に載っている単語や個人情報を組み込んで試すといったことが行われます。従って、適切なパスワードは次のようなものになります。

- ・自分だけが知っているオリジナルの文字列である
- ・英大文字・英小文字・数字・記号を全て含んでいる
- ・長さが10文字以上である
- ・書き留める必要がなく覚えることができる
- ・誰かに覗かれても覚えられないように、素早くタイプすることができる

また、インターネット上のサービスを利用すると、そのサービス専用のユーザIDの作成を求められることが多く、サービスの利用に応じて管理するユーザIDが増えます。その際、全て同じIDとパスワードに設定した場合、管理は簡単になりますが、どこか一箇所でもパスワードが漏えいしてしまった場合、他の全てのサービスに不正アクセスされかねないリスクが伴いますので、それぞれ違うパスワードを付けてください。

万が一、パスワードが漏洩したとしても、それに気付くことは困難です。これに対しては、パスワードを定期的に変更することで被害を最小限に留めることができます。

#### 4.2. パソコンのセキュリティ対策

現在のコンピュータウイルスには、犯罪者が遠隔操作をするために作成されているものが増えています。犯罪者は迷惑メールの代理送信や、特定サイトへの攻撃代理などを請け負うアンダーグラウンドビジネスに利用するため、世界中に遠隔操作ができるパソコンを増やしています。金儲けができるので、その足がかりとなるウイルスはプロを雇って、極めて高度なプログラムテクニックを用いて作成されています。

ウイルスは、感染すると犯罪者からの指示があるまで何もせず潜伏します。犯罪者からの指示により実行される内容は、大抵の場合他のサイトへの攻撃であり、感染したパソコン自体には何も破壊活動を行わないため、感染に気付くことは極めて困難です。警察から、「あなたのパソコンから不正アクセスが行われた」と指摘され、初めて気付くことになるでしょう。平成24年に起きた、遠隔操作による掲示板書き込みの冤罪逮捕事件は正にこのパターンであり、誰もが冤罪逮捕される危険があります。

また、ウイルスの種類が爆発的に増えており、ウイルス対策ソフトをインストールしていても、全てのウイルスを検知することはできません。特に「標的型攻撃」と呼ばれる特定の組織を狙って配布されるウイルスは、一般に出回らないためにウイルス対策ソフトのメーカーが標本を採取することができず、パターン検出での対策が取れません。

かなり絶望的ともいえる現状ですが、ウイルスが感染する経路はだいたい決まっています。次にあげる対策を行うことでウイルス感染の可能性をかなり下げることができますので、必ず実行してください。なお、セキュリティ更新がされなくなった古いOSやソフトウェアは危険ですのでネットワークにつないではいけません。

(1) OS のセキュリティを最新にする

ウイルスは、OS の脆弱性について感染します。発見された脆弱性は、Microsoft や Apple など、OS メーカーから提供されるセキュリティパッチを適用することで解消します。常に最新の状態に保ちましょう。

(2) アプリケーションソフトのセキュリティを最新にする

Word や Excel、PDF などの文書ファイルに感染するウイルスがあります。これらは Word や Excel、Adobe Reader など、アプリケーションソフトの脆弱性について感染を広げます。発見された脆弱性はメーカーから提供されるセキュリティパッチを適用することで解消します。常に最新の状態に保ちましょう。

(3) ブラウザのバージョンを最新にする

ウイルスは、ブラウザの脆弱性について感染します。発見された脆弱性は、ブラウザメーカーやプラグインソフトメーカーから提供されるセキュリティパッチを適用することで解消します。常に最新の状態に保ちましょう。Flash や JAVA は狙われやすいので特に注意が必要です。また、ウイルス感染を目的に開設されている Web ページもありますので、怪しいサイトに近寄らないことも大切です。

(4) ウイルス対策ソフトをインストールする

全てのウイルスは止められませんが、一般的に出回っているかなりのウイルスを防いでくれます。ウイルス対策ソフトのふりをしたウイルス付き偽ソフトも存在するので、信頼のおけるものを使ってください。ウイルス対策ソフトはパターンファイルと呼ばれる、ウイルス判定データを最新にしておかないと役に立ちません。パソコン購入時に付属するウイルス対策ソフトは大抵の場合ライセンス期限付きです。期限が切れるとパターンファイルが更新されなくなります。注意してください。

(5) USB メモリ等の自動実行を止める

USB メモリや DVD を挿入すると自動的に再生を始めたり、プログラムを起動する仕組みを悪用してウイルス感染プログラムを自動実行させて繁殖するウイルスがあります。少し不便になりますが、自動実行は停止させておく方が無難です。

(6) 自宅のインターネット接続にはブロードバンドルーターを用いる

1 台しかパソコンを使わない場合は、ブロードバンドルーターを用いずともインターネットに接続することができますが、この接続方法はインターネットからパソコンに直接アクセスが可能な状態であり、一瞬で不正アクセスを許してしまう可能性があります。ブロードバンドルーターを間に挟むことで、インターネットからパソコンへの直接アクセスが不可能になります。

(7) P2P ファイル共有システム等、不正な経路で手に入れたプログラムを実行しない

P2P ファイル共有システムや Web サイトなどで、高価なソフトやゲームソフトを不正に無料

配布している違法行為があります。これを手に入れて使いたいと思う心理を利用して、犯罪者は正規ソフトに見せかけてウイルスを配布しています。P2P ファイル共有システムなどで配布されているソフトはほとんどがウイルス付きだと思ってよいくらい、ウイルス感染の温床となっています。なお、この理由により、本学では P2P ファイル共有ソフトの利用を禁じています。

#### (8) メール添付ファイルに気をつける

迷惑メールについてくる添付ファイルだけでなく、友人から届いたメールであっても、友人のパソコンに感染したウイルスが、友人のふりをしてメールを送ってきていることがあります。

### 4.3. スマートフォン等のセキュリティ対策

スマートフォンの中身はパソコンと同じです。パソコンのウイルス対策と同様の対策がスマートフォンにも必要です。料金を徴収する仕組みや連絡先、メールなどの情報がある分、パソコンより危険だともいえます。

iPhone 系は比較的安全な仕組みがありますが、Android 系はウイルスが入り込みやすい仕組みになっています。Android でアプリをインストールする際には、アクセスする情報の確認画面が表示されます。単なる電卓アプリなのに連絡帳にアクセスを求めているなど、不審なアプリはインストールしてはいけません。

### 4.4. クラウドサービスの利用に関する注意

Dropbox や Evernote など、クラウドにデータを預けるサービスがありますが、これらの物理的な保存先はインターネットの向こう側にある、それぞれの会社が保有するサーバです。大抵の場合、十分なセキュリティ監視の下に運用されていると思われませんが、システムトラブルによる情報漏えい、倒産による情報売却など、想定外の事案により情報が流出するリスクがあります。G-mail などのメールサービスも同様です。

個人情報や機密情報が含まれるデータを取り扱う場合は、十分に注意してください。

### 4.5. 防犯知識

インターネットを利用した犯罪が増加しています。特に近年は、詐欺の手口も非常に巧妙化しており、気が付かない間に被害に遭うケースも少なくありません。被害を未然に防ぐため、次に代表的な犯罪の手法を挙げますので参考にしてください。また、いつも最新の情報を収集して、防犯対策をしてください。なお、これらの勧誘は、悪質な業者などが不特定多数に電子メールを発信しているものがほとんどです。もし、このような電子メールが届いた場合、たまたまあなたに届いた程度と捉えて、無視することがよいでしょう。電子メールに返信したり、電話で連絡することは、更に個人情報を相手に与え、事態が悪化することが考えられますので注意してください。

もし、犯罪の事例に遭遇した場合や犯罪に巻き込まれてしまった場合は、速やかに大学や警察、消費者センターなどに相談してください。

#### (1) フィッシング (phishing)

主に金融機関などを装って電子メールを送信し、偽の Web サイトに誘導して暗証番号やクレジットカード番号などの個人情報をだまし取る詐欺です。金融機関へは、メールに書かれ

た URL に直接アクセスせず、普段から Bookmark している信頼できる URL からアクセスするなどの手法が有効です。

## (2) 架空請求

主にアダルトサイトなどを名乗って架空の利用料金を請求する電子メールを送信し、金銭を振り込ませる詐欺です。無視することが一番です。例外として、裁判所から特別送達（原則手渡し）で送られてくる「支払督促」などは対応が必要ですが、支払督促を装った郵送物という手口もあるようです。

## (3) ワンクリック詐欺

Web サイトでクリックした拍子に、「会員登録を受け付けました」などと表示して金銭を請求する詐欺です。契約は双方の合意が必要であり、無関係のボタンをクリックしただけで一方的に契約が成立することはありません。無視することが一番です。

## (4) その他

インターネットでも現実社会と同様に、甘い言葉や法律的な難しい言葉で巧みに金銭を奪い取ろうとする悪徳業者や犯罪者がいます。

世の中うまい話はありません。本当にうまい話があれば、それは人に教えず自分だけで実施することでしょう。少額の出資で多額の利益が出るように思わせる「ネズミ講」や「マルチ商法」など、騙されないように十分に注意してください。

## 5. 常に最新のセキュリティ情報を

セキュリティ事案は対策が取られれば、新たな手口が生まれます。最新の攻撃手口を知ることが、トラブルに巻き込まれないために有効です。次のような情報サイトを利用して、定期的に調べるとよいでしょう。

本学 moodle 上「INFOSS 情報倫理」

<http://cclms.kyoto-su.ac.jp/>

本学では、1 年次生に情報倫理教育を実施しており、e-Learning 教材「INFOSS 情報倫理」を提供しています。内容は事例を中心に毎年更新されていますので、2 年次生以上の人も毎年再確認するとよいでしょう。

総務省「情報通信白書」

<http://www.soumu.go.jp/johotsusintokei/whitepaper/>

経済産業省「インターネット安全教室」「チェック PC」

<http://www.checkpc.go.jp/>

経済産業省、日本ネットワークセキュリティ協会（JNSA）「インターネット安全教室」

<http://www.net-anzen.go.jp/>

NISC 内閣官房情報セキュリティセンター「国民を守る情報セキュリティサイト」



<http://www.nisc.go.jp/security-site/>

日本ネットワークセキュリティ協会（JNSA）

<http://www.jnsa.org/>

警察庁「セキュリティポータルサイト」

<http://www.npa.go.jp/cyberpolice/index.html>

独立行政法人 情報処理推進機構（IPA）「ここからセキュリティ」

<http://www.ipa.go.jp/security/kokokara/quiz/index.html>

一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）

<http://www.jpCERT.or.jp/>

独立行政法人 国民生活センター「インターネットトラブル」

<http://www.kokusen.go.jp/topics/internet.html>

ウイルス対策ソフトメーカー各社

シマンテック，マカフィー，トレンドマイクロ，etc.

## 6．免責

本学におけるネットワークの利用は，基本的に自己の責任に基づくものとし，次の事項について大学は責任を負いません。

- (1) 天災やテロ等の不慮の事故，システム管理上の予測できない事故によるネットワークの停止やデータの損失
- (2) 本学のインターネット接続サービスや利用者が提供するサービス，またはそれらを通じて他のネットワークサービスを利用することで発生した一切の損害

学校法人京都産業大学ネットワークセキュリティ委員会