

SIGN 利用ライセンス 制度の理解に向けて



産業能率大学 情報センター
2024 年度

(目次)

I	はじめに (インターネットの世界)	-1-
	1. インターネットとは	-1-
	2. インターネットの特性とリスク	-2-
II	SIGN 利用ライセンス制度とは?	-3-
	1. 産業能率大学の情報教育環境	-3-
	2. SIGN 利用ライセンス制度の目的	-3-
	3. SIGN 利用ライセンス制度の概要	-4-
III	SIGN の利用ルール	-5-
	1. 利用マナー	-5-
	2. SIGN への接続 (機器)	-6-
	3. 設備の利用	-7-
	4. 不正アクセスの禁止	-8-
	5. 著作権侵害、商標の無断使用、肖像権侵害等の行為の禁止	-10-
	6. 公序良俗に反するメールやコンテンツの配信の禁止	-10-
	7. 犯罪と認定される行為の禁止	-13-
	8. システム資源の大量消費に繋がる行為の禁止	-15-
	9. 売買行為、営利目的の行為の禁止	-16-
	10. 携帯パソコンの利用ルール	-16-
IV	SIGN 利用ライセンス制度に関わる規則	巻末

SIGN 利用ライセンス制度の理解に向けて

I はじめに(インターネットの世界)

1. インターネットとは

①インターネットの利用

インターネットとは、世界規模のコンピュータ・ネットワークです。地球上には、会社、大学、その他、様々な組織があり、その中でコンピュータを接続するためのネットワークが作られています。このような組織のネットワーク同士を接続するもの、それがインターネットだとされています。しかし、インターネットが普及した現代では、その仕組みすら、意識することなく利用している場合も多く、メール送受信、ホームページの閲覧、オンラインゲームなど、パソコンやスマートフォンで日常的に行っているのではないのでしょうか。電車の中でも、本や新聞、漫画を読むのではなく、スマートフォンを操作している人が多くなってきました。2025年卒の大学生の殆どは、スマートフォンを所持していて、就職活動に利用しています。

(マイナビ 2025年卒大学生のライフスタイル調査結果詳細 2024年1月25日より

https://www.mynavi.jp/news/2024/01/post_40729.html)

インターネットは、1960年代後半のアメリカ国防省のARPANETを発祥として、研究者間で利用、育成されてきた研究用のネットワークとして出発しました。その後、通信規約であるTCP/IPが公開されたため、パソコンからでも簡単に接続できるようになりました。最初は研究者やその卵である情報科学の学生たちによって利用されていましたが、パソコンの普及とともに次第に普及し、1990年代に入って商用プロバイダ(インターネット接続業者)が出現したことにより、間口が一気に広がることとなりました。今では、プロバイダに加入していなくても、Wi-Fiやスマートフォン(4G回線など)を通して、誰でもすぐにインターネットが使えるようになっています。



その成立の経緯から明らかなように、インターネットは特定の開発管理者の下で計画的・実務的に作られたものではなく、参加する研究者達がボランティア精神に基づいて自発的に発展させてきたのが特徴です。その結果、規制の緩い、ある意味で自由なものとなりましたが、反面、専門研究者のように理性ある善意の人たちしか利用しないことを前提にして設計されていますので、誰もが利用できる状況では、「悪意」の侵入を招きやすく、いろいろな問題を抱えていることも事実です。

②インターネットでできること

インターネットの利用方法として代表的なものは、WWW(World Wide Web)や電子メール(E-mail)です。電子メールは、スマートフォンでも使っている人は多いでしょう。文字通り、インターネットを通じて電子的に手紙(mail)を送り受けする技術です。昔は文字情報だけでしたが、今では、写真その他ファイル、電子化できるものなら何でも送り受けすることができます。



WWWとは、文字・画像・音声で構成された情報をサーバ上にWebページ(よく「ホームページ」と呼ばれます)という形で置いて、インターネットを通じてそれを閲覧させ

るものです。これを利用すると、世界中から情報を集めることができます。また、逆に、自分のホームページを作って情報を発信したり、電子掲示板や電子会議室という形で、遠く離れた人同士で話し合いをしたりすることができます。さらに、最近では、これらの応用として、電子商取引、インターネット電話、eラーニング、ネット対戦型ゲーム、テレビ会議、チャット、ブログ、動画共有といったような様々な利用方法が実現されています。

しかし、WWWや電子メールにも様々な問題があります。後に述べるように、電子メールはコンピュータ・ウイルスをばらまくためのチャンネルになっていますし、SPAMメールの増加により、「使いやすさ」が損なわれ、その対策のために巨額のコストが必要となっています。

また、インターネット上の情報には「不正確なもの・悪意のあるもの・公序良俗に反するもの」が多く混在しており、情報の確実性・信頼性は保証されません。「インターネットの情報をすべて鵜呑みにせず自己責任で判断する」——それも、インターネットを利用するとき大切なことの一つです。

また、コミュニケーションツールとして利用されているものの中で、ブログのようにコメントやトラックバックをやり取りするもの、チャットのように同時に複数の人とその場で文字による会話ができるものなどはルールやマナーをしっかりと守らないとトラブルが発生しやすいツールでもあります。更に、ブログやプロフに記載された個人情報の流出や悪用によるトラブルも多発しています。したがって、このあたりのルール、マナー、エチケットはしっかり身につけておく必要があります。

2. インターネットの特性とリスク

① World Wide ということ

インターネットの最大の特徴は、World Wide ということです。インターネット上の情報は、国境に関係なく行き来しています。皆さんも情報の収集だけでなく YouTube や Twitter、Facebook を利用することで海外のサーバにアクセスすることもあるでしょう。日本にいながら世界中の情報にアクセスできるインターネットの環境は、いろいろな面での可能性を大きく拡大したといえるでしょう。

しかし、その利用にあたっては、World Wide であることのリスクを認識することが必要となります。

世界には様々な文化があり、良きにつけ悪きにつけ、それぞれの価値基準で社会が形成されています。そこにインターネットが普及し、情報が自由に駆け巡ると、どうなるでしょうか。不必要な文化間の摩擦が発生することも考えられます。

さらに、国家や企業の活動にインターネットが利用される比重が高まると、いったんネットワーク機能が停止した場合、莫大な損害が発生します。もちろん、これが単なる事故ならば防ぐのはそう難しいことではないかも知れませんが、インターネットに悪質なデマを流したり、システムの機能を停止するコンピュータ・ウイルスを送りつけたりという、意図的な悪意の攻撃が現実に行われる状況が発生しています。

自分のパソコンが、いつの間にか、このような攻撃の踏み台（経由地）にされ、その一端を担っていたということも十分にありえるのです。

② まだ秩序が定まっていない、自己責任の世界だということ

社会の一員として生活していくためには、自分の属する集団で決められた最低限の約束事があります。各人が他者を尊重し、お互いの約束事を守ることによって初めて社会は有効に機能します。身近な例で



言えば、日本に住む以上、日本国の法律に従う必要がありますし、家庭内には家庭内の、暗黙の約束事があります。

通常、これらの規則は、家庭での躰や、学校等の集団生活の中で自然に身につけていきます。しかしインターネットの世界は、まだ発展途上であるため、約束事が定まりきっていない状況です。このため、近年、インターネット犯罪と呼ばれる様々な犯罪が次第に増加してきました。それは、国内だけでなく、国境を越えて広がるほどのものになっています。

これに対し、政府は関連法令の新設・改正を実施しています。また、「サイバー犯罪条約 (Convention of Cybercrime)」のような国際的な取り決めも進められています。

しかし、法律や条約で定めたからと言って、直ちにインターネット上の犯罪がなくなるわけではありません。残念ながら、悪意のある人間はどこにでもいますし、人類にとって未体験の世界であるため、まったく想像もできないような犯罪が引き起こされる可能性も考えられます。

インターネットの世界は急激に拡大しており、日本においてもインターネットの利用を含む IT 技術の発展によるイノベーション(革新)は、国家規模で語られています。しかし、インターネットは無害で安全な、保護された秩序ある空間ではありません。場合によっては、刑法の処罰対象になったり、莫大な損害賠償を請求されたりする可能性もあります。また、ホームページ上に自分のプライバシーや顔写真を掲載することは、世界中にそれらの情報を知らせることになります。発信した情報に対して、予想もしない反応が返ってくることもあります。

このような状況下においてインターネットを真に活用するためには、インターネットにまつわる約束事やリスクを理解し、自己責任において利用していくことが重要となります。

II SIGN 利用ライセンス制度とは？

1. 産業能率大学の情報教育環境

産業能率大学では、情報機器を利用した教育を行うために、いつでも、どこでも情報サービスやインターネットにアクセスできるよう無線LAN（全教室、図書館、ラーニングコモンズ、ラウンジ）を提供しています。



※無線LANは、携帯パソコンの他、スマートフォンやタブレットも接続できます。その他、情報コンセント（有線LAN／電源コンセント）を設置している教室があります。

これらをSIGNという名称のネットワークで結んでいます。SIGNとは、**S**anno **I**nformation **G**alaxy **N**etwork の頭文字をとったもので、学生教育と利用者に対する情報サービスを目的とした、学部・大学院のキャンパスネットワークです。

SIGNを通じて、インターネットへのアクセスや電子メールの送受信も可能です。

2. SIGN 利用ライセンス制度の目的

SIGN は、全ての教室からのインターネット利用を可能とする他、学生所有の携帯パソコンの接続等、様々な情報サービスを提供してきました。しかしながら、インターネットを介した利用方法の多様化が進み、従来の使用ルールの想定を越えた状況が発生し

ています。具体的には、不正アクセスやウィルスによるネットワークへの脅威、電子情報による各種ハラスメントや犯罪行為の発生等のリスクが急激に高まっています。また、実習室使用マナーの悪化も目立ち始めました。

このため、本学では、「SIGN 利用ライセンス制度」を制定し、ネットワーク利用における危機管理を図ることとしました。

更に、情報化社会の進展と共に、技術面のみでなく、「情報」と「社会」との関係を理解し、真の情報化を担える人材が必須となっています。産業能率大学では、そのような人材の育成に全学を挙げて取り組んでいます。SIGN 利用ライセンス制度は、学習環境を維持することに加え、そのための取り組みの一環となるものなのです。

SIGN 利用ライセンス制度の目的は次の通りです。

- ・産業能率大学の全ての利用者が、快適に学習できる環境を維持すること。
- ・学生が「知らない」ことにより被害・加害の当事者となることを防止すること。
- ・在学中に「情報倫理」を体得し、社会での実践に結び付けること。

3. SIGN 利用ライセンス制度の概要

SIGNライセンス制度とは「SIGNを利用するにあたり必要となる利用ルールの理解や携帯パソコンのセキュリティ対策の実施を条件として、SIGNの利用を許可する制度」です。運転免許をイメージすれば理解しやすいと思います。



① ライセンスの付与手続きについて

- (1) 1年次生には、産業能率大学入学時にライセンスを付与します。具体的には、ライセンス制度に関するガイダンスの受講、SIGN 利用ライセンス制度を遵守する旨の誓約書の提出となります。この有効期間は半年で、仮ライセンス期間とも呼ばれます。
- (2) 後学期のガイダンス期間に情報倫理に関するガイダンスを行い、その段階で一定の基準を満たしていると判断された場合には、1年次生のライセンスの有効期間をさらに半年延長します。
ここで言う一定の基準とは、講習会の受講、利用知識の確認（理解度テストの正解率 80%以上）、携帯パソコンのセキュリティ対策の実施等となっています。
- (3) 2年次以降は、ライセンスは年度毎の更新となります。
年度当初のガイダンス期間に、ライセンス更新ガイダンスを実施しますので、これに出席のうえ、一定の基準を満たしていることを条件に、ライセンスを更新します。更新手続きまでの間は、前年度のライセンスが有効となりますが、正当な理由なく更新を怠った場合は利用資格が停止されることがあります。注意してください。

② 違反行為と処分について

SIGN の利用ルールに違反した場合、違反の程度に応じて、情報センター長が学生賞罰委員会に連絡します。そして学内での審議を経て、「SIGN ライセンスの停止」、「SIGN ライセンスの取り消し」などの処分がされます。また違反内容によっては、損害賠償の対象になる場合もあります。更に、違反が法律に触れるものであった場合は、刑事・民

事の対象となります。

とはいえ、良識を守り普通に利用していれば、ルール違反を犯すことはないはずです。処分にまで発展するのは、軽微な反則行為を何度も繰り返した場合や、明らかに悪質、もしくは法律に違反する行為を行った場合となります。

SIGNは本来、皆さんが積極的に利用し、学習していただくための設備です。臆することなく有効に活用してください。

*ただし、「やってはいけないこと」を知らずに被害・加害の当事者になってしまうことがありますので、本書を熟読すると共に、センター主催の説明会等に参加し、ネットワーク社会での常識や決まり事を身に付けるようにしましょう。

③ 情報センター主催の説明会について

情報センターでは、必要に応じ、セキュリティや情報倫理に関わる説明会を、更新時以外にも実施する予定です。Ca-In (SANNŌ Campus Information) や掲示で、その都度ご案内しますので、進んで参加してください。

④ SIGN利用ライセンス制度の運用組織と問い合わせ窓口

SIGN 利用ライセンス制度は、産業能率大学の情報教育を支援することを目的として設置された「産業能率大学情報センター」の所長の下で、情報センターに属する教職員を中心に運営されます。また、違反行為に対する処分や運用方法についての審議は、「学生賞罰委員会」で行われます。

SIGN 利用ライセンス制度の制定にともない、相談窓口を設けていますので、質問等があれば、湘南キャンパスでは情報センター棟 3F 学生情報サービスセンター窓口に、自由が丘キャンパスでは1号館 1Fの学生情報サービスセンター窓口に、代官山キャンパスでは事務室に来てください。

Ⅲ SIGN の利用ルール

この章では、SIGN の利用ルールを具体的に説明します。その中には、SIGN を使うための産業能率大学独自のルールだけでなく、インターネット社会に参加するための普遍的なルールも多く含まれています。

新聞等に掲載される最近のインターネット関連の事件を見ると、「法律に違反することを知らないでやってしまい加害者になってしまった」事例や、「リスクに関する知識がなかったために、用心を怠り被害者になってしまった。」事例が多く見られます。

冒頭にお話したように、インターネットの社会は未だ未成熟な世界です。そこには、有る可能性と想定のできないリスクが同居しています。

皆さんも、この世界の約束事を良く知り、安全かつ有効に活用するようにしてください。

1. 利用マナー

大学の設備は、学生・教職員が共同で利用するものです。一人のマナー違反のため、設

備が使用できなくなったり、授業の進行が妨げられたりすると、他の利用者に迷惑がかかります。

ここでは、情報設備のある教室でのマナーに関する取り決めについて説明します。

① 対象となる教室

実習室、共同利用室等、実習用のデスクトップパソコンが配備された教室はすべて対象となります。

② 利用ルール

(1) 飲食物の持ち込みは全て禁止です。飲食物をこぼすと機器の故障や施設が稼働しなくなる恐れがあるからです。

ただし、ここで「持ち込み」とは、「直ちに飲食できる状態になっていること」を言います。弁当、菓子、ペットボトル等は、蓋を閉め、あるいは包んでカバン等に収納してください。取り出し、あるいは机の上に置いた時点で、「飲食」とみなされますので注意してください。



(2) 当日の使用・不使用に関わらず、原則として傘の持込は禁止です。廊下の傘立てを使用してください。傘立てがなく持ち込む場合は必ず傘袋を使用してください。(水気は電子機器の大敵です)

(3) ゲームは全て禁止されます。これらの教室は学習のための施設だからです。



(4) 不必要な席取り、大声でのおしゃべりや騒いだりすること、スマートフォン、携帯電話等の使用等で、他の利用者の学習を妨害してはいけません。

(5) 他人の ID を借りて、SIGN に接続してはいけません。ID の貸し借りをしないことは、ネットワークを使う上での第 1 歩です。自分の ID を人に貸すのは、印鑑を貸すのと同等の危険があります。

2. SIGN への接続 (機器)

SIGN は、学習のためのネットワークであり、ここで提供される各種サービスを利用した授業が多数組まれています。また、事務局情報を含め、利用者の利便性を向上させるための情報提供が行われています。

従って、SIGN の運用にあたっては、安定してサービスを供給することが重要な指針となっています。

このため、SIGN に接続する機器についてはすべて把握されており、勝手に自分の機器 (端末等) を接続することは許されていません。

先生方が教育・研究のために、支給された以外のサーバやパソコン等の機器を繋ぐ時にも、情報センター長への申請が必要です。これは、ウィルス対策の実施状況やネットワークでの使用方法を確認して、SIGN の安定稼働を守るためです。

一方で、2001 年度から開始された携帯パソコン制度により、学生が自分の携帯パソ

コンを SIGN に接続することができるようになりました。

しかし、この制度の下においても、学生が自分のパソコンを自由に SIGN に接続することを許しているわけではありません。

入学時に本学が斡旋したパソコンについては、初年度は、許可基準を満たしていると情報センター長が接続を承認したものとして扱われています。これに対し、斡旋機以外の携帯パソコンを希望する学生については、申請書の提出が義務付けられ、審査が行われます。

そして、どちらのパソコンであれ、次年度以降は、SIGN ライセンスの更新時に、セキュリティ対策が正しく取られているかといったパソコン内部のソフトウェアの設定状況もチェックされ、接続許可が更新されることとなります。

したがって、学生が接続できる携帯パソコンは、情報センター長の許可を得た 1 台だけになります。

3. 設備の利用

設備は大事に使ってください。前項でも記した通り、SIGN は利用者全員が学習のために使う設備です。ネットワーク全体に支障をもたらせば、授業やサービスの提供が不可能になりますし、実習室の機器が故障すれば、授業に参加できない学生が出る可能性があります。



とはいえ、情報設備も機械ですから、故障する場合がありますし、トナー等の消耗品が切れてしまう場合もあります。こういった場合の対応の仕方を下記に列記しますので、放置することなく連絡してください。

ただし、意図的、もしくは明らかに本人の過失で大学に設置してある情報機器やソフトウェアを壊した場合は、処分や弁済請求の対象となることがあります。また、機器を勝手に移動した場合も同様です。（移動が必要な場合は担当の先生を通じて学生情報サービスセンターに申請してください。）

① プリンタのトナー、インク切れ

学生情報サービスセンターに連絡してください。

② プリンタの紙詰まり

基本的に自助努力で解決してください。ただし、機器の損壊等の危険があると判断した場合には、無理をせず、学生情報サービスセンターに連絡してください。

③ パソコン本体、プリンタの故障・破損

直ちに学生情報サービスセンターに連絡してください。そのまま放置することは厳禁です。

④ その他の使用上の疑問点やトラブル

学生情報サービスセンターにて対応します。（自由が丘キャンパス）1 号館 1F / （湘南キャンパス）情報センター棟 3F の窓口まで来てください。

なお、原則はあくまで自助努力ですので、予め了解してください。

4. 不正アクセスの禁止

不正アクセスとは、ネットワーク上の情報に対して、自分に与えられた権限を越えてアクセス（コンピュータを動かし利用する）しようとする行為であり、不正アクセス禁止法では、①なりすまし（他人の ID・パスワードを使用してアクセスする行為）②権限のないファイルへのアクセス（プログラムの弱点を利用して権限外の情報にアクセスする行為）を規定し、3年以下の懲役・100万円以下の罰金の罰則を規定しています。また、同法では、他人の ID・パスワードを第3者に譲り渡す行為も、不正アクセスを助長する行為として禁止し、1年以下の懲役または50万円以下の罰金としています。

これらの行為は、他の違反行為の入り口となることが多く、その結果として、不正が拡大していくことになります。軽い気持ちやゲーム感覚で行ったことが、重大な結果をもたらすことがありますので注意が必要です。

① 権限外のファイルへの不正アクセス及び、不正な権限取得を目的とした行為

インターネット上に存在するネットワークには、それぞれのセキュリティポリシーに従い、ネットワークの安全を確保するための制限がかけられています。また、ネットワーク上のファイルには、ほとんどの場合、アクセス権（そのファイルを読み書きできる者を指定する設定）が設定されています。プログラムの弱点について、自分に許可されていないファイルにアクセスしたり、そのファイルの権限自体を書き換えてしまおうとすることは、例えて言えば、鍵の掛っている家に無断で上がりこむようなものです。



② パスワード解読、ポートスキャン等のプログラムの実施、持ち込み

他人のパスワードを解読しようとしたり、内外のネットワークにポートスキャン（コンピュータシステムのポートを探り、侵入できる弱点を探ること）をかける行為は、不正アクセスの準備といえます。現実の行為に置き換えれば、他人の家の鍵穴にいろんな鍵を差し込んでみるのが前者で、鍵がかかっているかどうか手当たり次第にドアノブをまわして歩くのが後者です。

最近では、これらを行うためのソフトがインターネット上に流れている場合があります。しかし、好奇心からであれ、このようなソフトを使うことは許されません。

これらの行為をすると、対象にされたサーバにアクセスログ（記録）が残ります。したがって、サーバ管理者は自分の管理するサーバが攻撃を受けたことに気づき、徹底的な調査を行います。そして本人が特定されてしまうのです。こうなってしまうと、出来心や悪戯といった言い訳は一切通用しません。厳重な処罰の対象となってしまいます。

③ なりすまし行為

メールやインターネット上で、他人の ID を使用して通信を行うことを「なりすまし」といいます。

他人の名を語って、ありもしないことを流したり、インターネット上での売買をしたりすると名誉毀損罪、詐欺罪等の対象となるばかりでなく、民法上の不法行為となり、損害賠償請求を起こされることもあります。

また、セキュリティの管理が不十分な場合、自分が被害者になる可能性があります。買ってもしない商品や身に覚えのない請求が届いたり、知らないうちに悪者にされていたりと、被害を受けた場合のダメージは多大なものになります。

これを防ぐためには、ID、パスワードの管理をきちんと行うことが最低限必要です。パスワードの設定方法については、「利用の手引き」に記載がありますので、確認してください。

④ 認められたもの以外のネットワーク資源・ソフトのダウンロード

SIGN 上には、情報を利用するためのいろいろなフォルダやファイルが置かれています。また、一方で、情報環境の整備用に一般の学生がアクセスできないものも多数存在します。

これらの資源を不正な手段を使ってダウンロードすると、著作権違反等に問われることとなります。例えば、実習室のデスクトップパソコンにインストールされたソフトは、多くの場合、ソフト会社と大学とがライセンス契約を結び、厳重な管理の下で運用されています。これを不正な手段により、自分の携帯パソコンや記録媒体にダウンロードすると、ライセンス契約に対する違反行為となり損害賠償を請求されることもあります。

⑤ コンピュータ・ウィルスの作成、持ち込み

コンピュータ・ウィルスとは、メールの添付ファイルや Web 上に仕掛けられた特殊なプログラムで、コンピュータの機能を阻害したり、ソフトウェアを破壊したりするものです。

従来は、メールの添付ファイルを開くことにより感染するのがほとんどでしたが、最近は、USB フラッシュメモリを媒体とした感染や汚染されたホームページを開くだけでの感染等、感染経路が多様化しています。

また、最近ではワーム型のウィルスが多く流れています。これは自分で自分自身をばらまく能力を持ったコンピュータ・ウィルス的一种でインターネットに流れているウィルスの大半はこのワーム型のウィルスに分類できるものが増えていきます。メールに添付されているファイルを実行させる事でウィルスが起動し、自分自身をメールや P2P ソフト、chat ソフトなどを利用してばらまいていきます。

コンピュータ・ウィルスに感染すると、ファイルが消されてしまったり、コンピュータの動作が異常に遅くなったりするだけでなく、そのコンピュータがネットワーク上にウィルスを垂れ流すことにより、接続したネットワーク全体を機能不全に陥らせることとなります。現に、新種のコンピュータ・ウィルスが流行する度に、社会に大きな影響を与えることが繰り返されています。

産業能率大学では、2001 年度より携帯パソコン制度を開始しました。この制度では、家庭でインターネットに繋いだ携帯パソコンを大学のネットワーク (SIGN) に直接繋ぐこととなります。もし、家庭でコンピュータ・ウィルスに感染した携帯パソコンを SIGN に接続してしまうと他のパソコンに感染させてしまったり、ネットワークをストップさせてしまうことにもなりかねません。

☆コンピュータ・ウィルスに感染しないために、次のことに注意してください。

*ウィルス対策ソフトのデータを最新の状態にする。

*メーカーより提供されるパッチファイルをこまめに当てる。



- *情報センターより発信されるウィルス情報に注意する。
- *不審なメールは開封しない。
- *出会い系サイトやアダルトサイト等の危険なサイトにアクセスしない。
- *フリーソフトのダウンロード、インストールは慎重に対処する。

5. 著作権侵害、商標の無断使用、肖像権侵害等の行為の禁止

著作権についての細かい解説は、別の機会に譲りますが、要は、「創作物（具体的な有体物である必要はない。）には、創った人の権利がある。従って、勝手に使ってはいけない。」ということです。

特に、コンピュータの世界においては、デジタル情報の複製の容易さとインターネットの World Wide という特性が、この問題に大きな影響をもたらすこととなります。デジタル化された情報は簡単にコピーが可能であり、品質の劣化もないため、簡単に複製できるからです。

例えば、自分のホームページに、これらをダウンロードできるコーナーを作ったとすれば、世界中の人間が自由に利用することが可能になってしまいます。しかし、音楽やソフトウェア、デザイン等の創作物には、作者の権利が及んでいますので、無断でこのような行為を行えば、著作権を侵害することになります。

また、会社のロゴ等の商標には商標権が存在しますし、個人の写真には肖像権が存在します。

日常、コンピュータを扱っている際、これらの権利についての配慮をつい忘れがちですが、最近では著作権その他の知的所有権についての意識が高まっています。

無知や不注意から莫大な損害賠償を請求されることもありますので、注意してください。特に、ホームページから著作物を全世界に配信した場合の推定被害は、莫大な金額になる可能性があります。

著作権についての主な注意事項は次のとおりです。

- *他人のソフトウェアや音楽をコピーして利用しない。
- *漫画のキャラクターや企業のマーク等をホームページに利用しない。
- *自作ホームページにソフトウェアや音楽のダウンロード機能を置かない。
- *ファイル交換ソフト等を利用して他人の著作物の共有をしない。
- *他人の写真や個人情報を許可なくホームページで公開しない。
- *インターネット上の画像や情報を利用する時は、必ず著作権についての確認を行う。
- *著作権の及んでいる情報を利用するときには、著作権者の承認を得る。

6. 公序良俗に反するメールやコンテンツの配信の禁止

① 他人に対する誹謗・中傷や他人の社会的評価に関わる問題の記載

他人に対する誹謗・中傷や他人の社会的評価に関わる問題を記載してはいけません。パソコンに一人で向かっていると、相手の顔が見えないため、通常のコミュニケーションを逸脱した表現をしてしまう場合があります。また、会議室等に匿名で参加できる場合もあり、面と向かっては言わないような事まで書いてしまうケースも見られます。

しかし、これは禁物です。

インターネットの世界は、「開かれた社会」です。あなたが書いた情報が多くの不特定の人たちに見られる状況にあることが多くなります。議論に熱くなって、不用意な発言をしたり、安易に人（組織）の悪口を書き連ねたりすると、名誉毀損罪、侮辱罪、信用毀損罪、業務妨害罪等に該当したり、民法上の不法行為に該当し、損害賠償を求められたりします。また、そこまで行かなくても、大事な人間関係を壊してしまったりします。

インターネット上では、必ず現実の世界に照らして、冷静に判断・発言するようにしましょう。

* もし、被害に遭ったら…

被害に遭った状況を説明できるよう準備し、ホームページの URL 及び印字、電子メールの印字、振り込みや送付の控え等を用意して、学生サービスセンターか最寄りの警察署に相談してください。



【コラム】コミュニティサイトのリスクについて

インターネット上でのコミュニケーションといえば、以前はメール、チャット、電子掲示板等が主なものでしたが、近年では、ブログ、SNSが中心となり、これらの機能が、動画やゲームのサイトに付加されるようになり、パソコンからだけでなく携帯電話やスマートフォンを利用して気軽に利用できるようになってきました。

そうした中で、学校裏サイトでのいじめの問題や、SNSサイトでの飲酒運転やアルバイト先での悪戯の告白等、社会問題に発展するケースも発生しています。こういった不法・不正行為を行わないことはもちろんですが、（その事実がなく）本人は冗談のつもりで書き込んだことが原因で批判の対象とされたり、周囲を巻き込んだ問題となることがあります。（不注意な発言によりサイトが「炎上」したという話はよく聞きます。）

更に、こういった問題が起きると、「まとめサイト」といって、その「事件」だけでなく、書込者の過去の情報まで調べ上げ、「晒す」サイトも存在しています。高校時代に投稿したいじめの話が後になって炎上し、社会人になってから別のサイトに乘せた顔写真や勤務先の情報まで公開されたような例もあります。

インターネット上に書き込んだデータは、（他者によるコピーも可能であり）データの自己管理が不可能となり削除することができない場合が多々あります。「気軽に書き込める」と「社会的責任」は別であることを十分に認識する必要があります。

詳細につきましては、本学の「ソーシャルメディア利用ガイドラインを参照願います。（URL：<https://www.sanno.ac.jp/students/snsguide.html>）

② 他人のプライバシーの侵害

他人のプライバシーの侵害をしないようにしましょう。

人間は、「自分に関する情報の流れをコントロールする権利」→「プライバシー権」を持っています。この権利は、近年の情報技術の発達とともに、その保護の重要性が叫ばれ、日本においても、個人情報保護法は 2003 年 5 月 30 日の公布後、直近

では改正法が 2023 年 4 月に施行されました。

ここで言う、個人情報とは、「生存する個人に関する情報であつて、次の各号のいずれかに該当するものをいう。一 当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他の知覚によっては認識することができない方式をいう。次項第二号において同じ。）で作られる記録をいう。第十八条第二項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」と定義されています。

身近な例を言えば、名前や住所、電話番号、顔写真等、個人を特定できる情報を本人の承諾なくホームページ等に掲載した場合がこれにあたります。インターネットは開かれた場ですから、それを見た第三者が、その情報をどう利用するかわかりません。最悪の場合、ストーカーや犯罪行為に利用される場合もあるわけです。（掲示板に本人が推定できる氏名、イニシャル等を載せるのも同様です）

逆に、自分の個人情報を安易にネット上に載せるのにも注意しなくてはなりません。インターネットは、個人情報を収集する様々な仕組みを備えています。

ホームページ上での各種アンケートや懸賞応募、ホームページを使った会員登録、電子掲示板、電子商取引等、個人情報を送信する機会が増えてきています。「身に覚えのないダイレクトメールが多数送られてくるようになった。」「知らない人からメールが届くようになった。」等、思い当たることはありませんか？ もしかすると、自分がインターネット上で入力したデータが使われているかもしれません。個人情報誌の投稿も業者によりデータベース化されているという話もあります。

また、コミュニケーションツールとして利用されているブログやチャットなどのように、誰でも匿名で投稿できるものや、ある程度メンバーを絞ってメンバー以外には公開も投稿もさせないものもあります。このような場所でも、電話番号や住所、本名などの個人情報を書き込むことは望ましくありませんし、コミュニケーションの相手に質問することも失礼です。

たとえば、集められた個人のメールアドレスは、インターネット上で売買され、思わぬところからダイレクトメールや、スパムメール、チェーンメールに利用されることがあります。

インターネットの世界はルール等が正式に定まっていない自己責任の世界です。思わぬトラブルに巻き込まれないように注意してください。

③ 風俗営業に関わる情報、ねずみ講に関する情報の配信

風俗営業に関わる情報、ねずみ講に関する情報を配信してはいけません。

風俗営業とは、「風俗営業等の規則及び業務の適正化に関する法律」に規定されている業種を言います。特に 1999 年 4 月改正後の同法では、ネット上でポルノ映像を有料で提供する行為を「映像送信型性風俗特殊営業」と位置づけ、規制の対象としています。

【注】風営法に規定されている業種

- ・接待飲食等営業（キャバレー、照明の暗いバー・喫茶店他）
- ・遊技場営業（パチンコ店、麻雀荘、ゲームセンター営業）
- ・店舗型性風俗特殊営業（ソープランド、個室マッサージ、ストリップ劇場、ラブホテル・モーテル、アダルトショップ、出会い系喫茶）
- ・無店舗型性風俗特殊営業（派遣型ファッションヘルス、アダルトビデオ等通信販売）

ねずみ講とは、後順位の加入者が支出した金品を、先順位の加入者が受領することを内容とする配当組織で、親>子>孫と加入者が無限に増加することにより莫大な儲けが出ると言われて勧誘されます。

ところが、現実には、この計算は必ず破綻します。（一人が二人の子を勧誘するとしても、2の27乗＝134,217,728と27世代目には1億人を突破してしまいます）

このため、「無限連鎖講の防止に関する法律」により、開設、運営、加入勧誘等、無限連鎖講に関わる全ての行為が禁止されています。

最近では、インターネット上で、マネーゲームと称して、ねずみ講の勧誘が為される場合が増加しています。この時、「先に入った者がある時点で抜けるのでネズミ講ではない。」とか、様々な誘い文句がありますが、加入者が抜けるシステムであるかどうかということは、ねずみ講の要件ではありません。これに参加することは、明らかな違法行為となるだけでなく、友達をなくし、社会的信用を失墜することに繋がります。

【参考】 マルチ(まがい)商法

ねずみ講と似た形態のものとして、マルチ商法があります。これは、販売組織の加盟者が商品を販売しながら会員を勧誘し、ネズミ講式に消費者を販売員にすることにより、組織をピラミッド式に拡大していく商法をいいます。この商法自体は、販売方法のひとつとして禁止されてはいませんが、実際にはねずみ講と同様に会員の獲得が困難になり人間関係が崩れたり、会員が不良在庫を抱えたりと、問題が生じるケースが続発しています。

このため、「特定商取引に関する法律」により「連鎖販売取引」として規制されており、広告規制、契約書面の交付義務、クーリングオフ制度等が設けられています。最近では、インターネット上のホームページや電子メールでの勧誘が増加しています。

7. 犯罪と認定される行為の禁止

犯罪を犯してはいけないことは、普段の生活でも、インターネット上でも当たり前の事です。しかし、何が犯罪とされるのかを知らないと、軽い気持ちで知らずに、犯罪を犯してしまう事にもなりかねません。軽い気持ちであれ、犯罪は犯罪です。刑法犯として処罰されたり、社会的な立場を無くすことになりかねません。

また、インターネットには詐欺などの犯罪を目的としたサイトが多数存在しています。これらのサイトの危険性を判断できないと、詐欺被害や不正請求の被害に遭いかねません。ここでは、いくつかの事例をあげます。皆さんの参考にしてください。

① インターネット詐欺、不正請求等

インターネットの普及とともに激増しているのが、詐欺や不正請求といった経済事犯です。インターネット上のショップやオークションで、〇〇売りますと出品し、希望者に代金を振り込ませ、商品は送らない。また、見本と著しく異なる商品を送ってくるケース等がインターネット詐欺の代表的なものです。インターネットでは、相手が直接見えませんので、対面販売であれば見破れるウソも見逃してしまいがちです。最近では、手口が巧妙化し、実際に存在するサイトそっくりの画面に銀行口座の情

報を入力させたり、キーボードの操作履歴を盗んだりして、被害者口座から預金を根こそぎ奪取するケースや、サイトのリンクをクリックしただけでアダルトサイトに誘導され会費の入金を請求されるケースなど、お金に絡むインターネット上の犯罪は多様化しています。

情報センターでは、ライセンス制度のガイダンス等でインターネット上の経済事犯の動向や注意点の解説を行っていますので、必ず参加し、このような被害に遭わないようにしてください。また、万一、不安な状況が発生した場合には、情報サービスセンターに相談してください。

② 脅迫、嫌がらせ、恐喝

「××しないと、家族に不幸が起きる。」といった直接的な脅迫のメールを送る行為の他、最近では、「◆◆を殺せば 10 万円の懸賞金を出す。」といったインターネットの匿名性を悪用した事件も発生しています。動機は振られた腹いせといった単純なものが多いですが、どんな人間が見ているかわかりません。悔し紛れの一言が重大な事件を引き起こすことにもなるのです。

また、脅しやゆすりのメールを送りつけて金品を要求すると恐喝になります。

この場合、メール上であろうと、直接の行為であろうと、手段は問われません。

③ わいせつ物陳列

わいせつの概念は、国や文化により異なります。また、時代によっても変わってきます。日本においては、最高裁の判例で「いたずらに性欲を興奮または刺激させ、かつ普通人の正常な性的な羞恥心を害し、善良な性的道義的概念観念に反するもの」と定義されていますが、実際に取り締まりの対象となる基準は変わってきています。

いずれにせよ、対象となるようなモノをインターネット上に載せた場合は、公然化したものとしてわいせつ物陳列罪に問われることとなります。

④ 淫行勧誘

出会い系サイトやメール・掲示板等を使った買春・売春行為は禁止されています。SIGN は学習のためのネットワークですので、こういった書き込みが禁止なのは当然ですが、インターネットや携帯電話の世界では、この種の情報が氾濫しているのも事実です。

恋人やメル友募集を謳って、実体はお金絡みだったりするものも多くあります。

その他にも、インターネットや携帯電話の出会い系サイトをきっかけにした、殺人、強姦、恐喝、脅迫、児童買春等の事件が全国で多発しています。

出会い系サイトには、相手の素顔が見えず、しかも、どんな人間も参加できるため、こうした危険性も潜んでいることを認識してください。

【参考】 以下は、神奈川県警のホームページでの注意です。

- 「こんなことをしても大丈夫だろう」等という軽い気持ちで行った行為が犯罪になってしまうこともあるので、自分の行動に責任を持ちましょう。
- 出会い系サイトに限らず、インターネットで知り合った者と実社会で会うと、犯罪に巻き込まれる危険性があるので、絶対にやめましょう。

⑤ ストーカー行為

平成12年11月24日から「ストーカー行為等の規制等に関する法律」が施行されました。これは、「特定の者に対する恋愛感情などの好意の感情またはそれが満たされなかったことに対する怨恨の感情を充足する目的で特定の相手に付きまったり、執拗に嫌がらせを繰り返す行為」を規制し、罰則などを設けたものです。

具体的には、「付きまとい、待ち伏せ、押しかけ、監視していると告げる行為、面会、交際の強要、乱暴な言動、無言電話等、汚物等の送付、名誉の侵害、性的羞恥心の侵害」が対象行為となります。

例えば、

- ◆『昨夜 Aさんと渋谷で映画を見ていましたね。』というような監視をしていることを告げるメールを送りつける。
- ◆会ってくれとか、つきあってくれという内容のメールを繰り返し送りつける。
- ◆意味のない、もしくは嫌がらせのメールを大量に繰り返し送りつける。
- ◆掲示板に、相手のプライバシー情報を載せ、不名誉な書き込みを行う。

等が、インターネットを使用したストーカー行為の代表的なものです。

とにかく、相手が、「身体の安全、住居などの平穏もしくは名誉が害された」と感じたり、「行動の自由が著しく害される不安を覚え」たりした場合には、ストーカー規制法の対象となる場合があります。「情熱」と「暴走」は紙一重のところにあることを覚えておきましょう。

⑥ 犯罪を目的とした受発信

例えば、銀行強盗の打ち合わせをメールで行ったり、実際の犯罪に繋がるやり取りを、ネットワークを使って行ったりすることです。いずれも犯罪を準備する行為ですから、厳しく禁止されます。

8. システム資源の大量消費に繋がる行為の禁止

ネットワークを構成する資源は、残念ながら無限ではありません。ネットワーク上を流れるデータ量が過大になると、回線や処理の遅延が発生します。大量データの保存など、サーバのハードディスクを占有する行為も、自分以外の利用者にも迷惑がかかる場合があります。（誤って2つのシステムの間で、相互にメールを転送する設定を行うと、「無限に」メールが転送され続け、莫大なデータがネットワーク内に流れることとなりますので、注意が必要です）

SIGNは、産業能率大学の学生・大学院生が学習のために共同利用する環境です。システム資源を大量に消費し、授業ができなくなったり、ネットワーク自体が機能しなくなったりするような行為は全て禁止されています。

① チェーンメールの発信・転送

チェーンメールとは、「不幸の手紙」のように、他の人にメールを送るように仕向ける内容のメールであり、「これを・・・人に転送しないと…」といった文面で送られます。

チェーンメールが流通すると、ネットワーク上で飛び交うメールがねずみ算式に増

え、ネットワークに渋滞をもたらします。中には、ウイルスに対する警告情報や倒産したペットショップのペット救済のように、善意を装う内容のものもありますので注意してください。「(不特定の) 何人に転送せよ」とか、「みんなに教えてあげて」といった内容のメールには対応しないことが大事です。疑わしいメールを受け取った場合は、学生情報サービスセンターに連絡してください。

② 認められたもの以外の FTP

FTP とは、ファイルのダウンロードを行うための仕組みで、インターネット上で FTP によるダウンロードを実施した場合、大学のインターネット回線に渋滞を引き起こし、他の利用者に影響を与える場合があります。SIGN では学外のサイトからの FTP は、原則として認めていません。FTP を行うことが必要な場合には、担当の先生を通じて学生情報サービスセンターに相談してください。

③ 25MB（総容量）を超えるメールの送受信

産業能率大学では、25MB（総送受信容量）を超えるメールは送受信できないようにシステムで制限しています。

これは、大量の文書や添付ファイル（作成したファイルをメールに添付できる機能）の送受信により、通信回線の遅延など、学内・学外でトラブルを引き起こす可能性があるからです。例えば、デジタルカメラで撮影した画像ファイルを課題や論文で使用し、添付ファイルとしてメールを送信した場合、メール送信容量の制限によりメールを送信できないことがあるので注意してください。

ファイルを添付したメールの送信時には、総容量に注意し、分割・圧縮ソフトの利用など、添付ファイルの容量を小さくするよう習慣を付ける事が重要です。

注意：添付ファイルを送信する場合、メール総容量は元のファイル容量より大きくなります。例えば 1MB（+文書の容量）のファイルを添付した場合、1.4MB 程度（+文書の容量）になりますので注意してください。なお、メールを受信する相手先によっては、25MB を下回る容量のメールしか受け取れない場合もあります。

④ DOS 攻撃

DOS 攻撃とは、インターネット上に接続された特定のコンピュータに対して大量の不要な情報を送付することをいいます。標的にされたコンピュータは、送りつけられた情報への対応を行うことにより、性能低下を招き、本来のシステムが動作しなくなったり、利用者がアクセスできなくなります。

9. 売買行為、営利目的の行為の禁止

SIGN 上で「売ります、買います」をしないでください。

SIGN は、教育目的に限定されたネットワークです。したがって、個人のホームページやメール等で、SIGN 上の資源を利用して、売買行為を行ってははいけません。

10. 携帯パソコンの利用ルール

本学では、携帯パソコン制度を2001年度より導入し、(許可された)自分の携帯パソコンを大学構内でSIGNに接続することが可能となっています。

このことは、従来の大学主導によるセキュリティ管理だけでなく、学生自身がセキュリティ管理に責任を負うことの重要性がますます高まったことを意味します。

以下の項目は、携帯パソコンの利用にあたって、特に注意しなくてはならない事項ですので厳守してください。(知らずに行ってしまった場合でも処罰の対象となります。)

- ①他人の携帯パソコンを無断で使用(貸し借り)しないこと。
- ②指定されたコンピュータ名を改変しないこと。
- ③公序良俗に反する目的で作成されたファイル・ソフトをインストールしないこと。
- ④ウイルスに感染したパソコンをSIGNに接続しないこと。
- ⑤ウイルスの感染が判明した場合には、すぐに学生情報サービスセンターに届け出る
こと。
- ⑥ウイルス対策ソフトを最新の状態に更新すること。
- ⑦その他、情報センターより発信されたセキュリティ対策を速やかに行うこと。
- ⑧ パソコンロッカー(自由が丘キャンパス)を不正に使用しないこと (割当外のロッカーの使用、禁止物の収納、非施錠、落書き、不許可掲示、他人のロッカーの解錠等)



V SIGN利用ライセンス制度に関わる規則

産業能率大学 情報教育ネットワーク (SIGN) 利用規程

(目的)

第1条 本規程は、産業能率大学情報センター規程第7条に基づき、情報教育ネットワーク（以下「SIGN」という）の利用に関する事項を定める。

(利用目的)

第2条 SIGNの利用目的は、本学の教育、利用者に対する情報サービスの提供、およびこれに準ずるものに限定する。

(利用資格)

第3条 SIGNの利用資格を有する者は、次のとおりとする。

- (1) 本学の学生（大学院、短期大学を含む通信教育課程、および聴講生、委託生、研究生を含む）
- (2) 本学の教職員（嘱託を含む）
- (3) 兼任教員
- (4) 客員教授
- (5) 派遣研究員
- (6) 非常勤職員
- (7) マネジメントスクール受講生
- (8) その他情報センター長が適当と認めた者

2 SIGNの利用資格を有する者は、SIGN利用ライセンスの交付を受けることにより、SIGNを利用目的の範囲で利用することができる。

(SIGN利用ライセンスの付与)

第4条 SIGNの利用資格を有し、必要な手続きが完了した者には、SIGN利用ライセンスを付与し、利用IDを発行する。通信教育課程、マネジメントスクールについては利用の都度の申請に基づく付与とする。

2 SIGNを利用する者は、情報センター長にSIGN利用ライセンスの付与を申請し承認を得なければならない。申請の具体的な方法については別に定める。

3 情報センター長は、前項の申請を適当と認めたときは、これを許可し、SIGN利用ライセンスを付与する。

(SIGN利用ライセンスの有効期間)

第5条 SIGN利用ライセンスの有効期間については別途定める。

(利用時間)

第6条 SIGNの利用時間は別に定める。

(機器の貸出)

第7条 SIGNに係る機器の貸出を受けようとする者は、情報センター長に申請をしなければならない。情報センター長は、申請内容が正当かつ情報センター運

営に支障をもたらさないと判断した場合これを許可する。

(経費の負担)

第8条 情報センター長は、利用者に対してSIGNの利用に係る経費の一部を利用負担金として求めることがある。負担の具体的な内容については別に定める。

(遵守事項)

第9条 SIGNの利用者は、その利用にあたっては定められた事項を遵守し、システムの秩序を乱し或いは資源を毀損するような使用をしてはならない。具体的な遵守事項については別に定める。

(利用者責任)

第10条 SIGNの利用により利用者が損害を受けたり、他者に損害を与えた場合、それは利用者の責任に帰せられるものとする。

(利用状況の調査)

第11条 情報センター長は、ネットワークの保全、秩序維持を目的として、ネットワーク資源の使用状況について調査を行うことができる。

2 情報センター長は、利用者に対して、SIGN利用に係る報告書の提出を求めることができる。

(弁済請求)

第12条 遵守事項の違反、又は重大な過失により、SIGN設備・データ等の各種資源を損壊した場合、利用者に対し弁済を求めることがある。

(利用の停止、制限)

第13条 情報センター長は、本規程に違反する行為、別に定める規則に違反する行為、SIGNの運営に重大な支障をきたす行為、または重大な支障をきたす恐れがあると認められる場合は、当該利用者のSIGN利用ライセンスの取消しや停止をすることができる。

2 前項において、学生懲罰委員会の審議を経て教授会に諮り、当該処置の要否及びその内容を決定する。

3 情報センター長は、必要に応じて利用者に対しSIGNの利用を制限することができる。なお、この制限を越えて利用する場合は、情報センター長の許可を得なければならない。

(報告)

第14条 情報センター長は、本規程に則し行った処分については、意見を付し大学学長に報告する。

(免責)

第15条 本学は、SIGNによるサービスの提供の遅延、中断、

又は提供された情報に関連して生じた損害について利用者に対し、責任を負わないものとする。

(その他)

第16条 本規程に定めるもののほか、SIGNの利用に関して必要な事項は別に定める。

産業能率大学 SIGN利用ライセンス制度 運用内規

(目的)

第1条 本学の情報教育ネットワークであるSIGNを本来目的に沿い、円滑、快適な運用環境を供することを目的として、「大学 情報教育ネットワーク (SIGN) 利用規程」(以下、「SIGN利用規程」という)第4条に基づき、SIGN利用ライセンス制度を制定する。

(ライセンスの付与)

第2条 SIGN利用規程に規定された利用資格を有する者からの申請に対し、情報センター長の承認が行われた時点で、SIGNの利用を許可しSIGN利用ライセンスを付与する。

(ライセンスの付与手続き)

第3条 通学課程の学生、及び大学院生については、産業能率大学入学後、SIGN利用及び情報論理に関するガイダンスの受講により、SIGN利用ライセンスを付与する。

- 2 その他の利用資格者については、所定の申請書の提出による申請手続きにより、情報センター長の承認をもってSIGN利用ライセンスを付与する。
- 3 SIGN利用ライセンスの付与を受ける者は、所定の誓約書を提出しなくてはならない。

(有効期間)

第4条 SIGN利用ライセンスの有効期間は、原則発効年度内とする。

- 2 通学課程の学生で、初回にSIGN利用ライセンスを付与されてから6ヶ月間は仮ライセンス期間とし、有効期間も6ヶ月間とする。
- 3 第1項および第2項で定める有効期間満了後も、第5条に定める更新の手続き期間にあつては暫定的に使用を許可する。

(更新)

第5条 有効期間満了後も利用資格を有し、SIGN利用ライセンス更新ガイダンスに出席し所定の手続きを行い、許可基準を満たしていると判断された場合はSIGN利用ライセンスを更新する。

- 2 更新を許可する基準については、年度毎に基準の見直しを行い、情報システム運営委員会で決定する。

(取消し)

第6条 SIGN利用ライセンスは以下の場合に取消される。

- (1)所持者が、「SIGN利用規程」に定める利用資格を喪失した場合
- (2)所定の更新手続きを怠った場合
- (3)「大学 SIGN利用の規制に関する内規」に定める違反により、SIGN利用ライセンス取り消しの処分を受けた場合。
- (4)その他、情報センター長が、SIGN利用ライセンスの取消しを決定した場合

(ライセンス証の発行)

第7条 SIGN利用ライセンスが付与された通学課程の学生には、SIGN利用ライセンス証を交付する。

(ライセンス証の返還)

第8条 SIGN利用ライセンスが取消された通学課程の学生は、SIGN利用ライセンス証を速やかに情報センター長宛返還しなくてはならない。

(ライセンス証の再発行)

第9条 SIGN利用ライセンス証を紛失した場合は、速やかに学生情報サービスセンターで再発行申請を行わなければならない。

(ライセンス証の提示義務)

第10条 SIGNの利用中に、SIGN利用ライセンス証の提示を教職員より求められた場合には、速やかにこれを提示しなくてはならない。

(組織)

第11条 SIGN利用ライセンス制度の運用は以下の組織により行われる。

- (1) 情報システム運営委員会
SIGN利用ライセンス制度の運用における具体的な検討、提案を行う。
- (2) 情報センター
SIGN利用ライセンス制度の実運用(ライセンスの付与手続き、周知活動等)を行う。

(情報センター長の取消し・停止権限)

第12条 情報センター長は、以下の手続きにより、利用承認の取消しや停止を行うことができる。

- (1) 情報センター長は違反の程度により直ちに学生賞罰委員会に申し入れるとともに、情報システム運営委員会に報告する。
- (2) 学生賞罰委員会の審議を経て、学長が教授会に諮り決定した処分内容に従い情報センター長が取消しや停止の指示を行う。

(違反行為に対する緊急処置)

第13条 情報センター長は、緊急でやむを得ない事情がある時は、緊急処置として、資格停止、利用制限の仮処置を行うことができる。ただし、その内容に関して大学学長に速やかに報告しなければならない。

(再申請)

第14条 情報センター長は、SIGN利用ライセンスの取消しを受けた者からの申請が新たにあった場合、取消日より1年間、これを受理することができる。

(情報倫理教育の義務)

第15条 当該制度の運用にあたり、情報センターは、ガイドブックの配布、ガイダンスの実施等、情報倫理に関する知識の普及に関わる活動を実施しなければならない。

産業能率大学 SIGN利用の規制に関する内規

第1章 総則

(目的)

第1条 本内規は、「大学 情報教育ネットワーク (SIGN) 利用規程」第9条に基づき、SIGN利用ライセンス制度において利用者が遵守すべき項目について定める。

(処分の種類と範囲)

第2条 処分の原則は以下のとおりとし、その適用は遵守事項ごとに学内外への影響を考慮のうえ決定する。

- (1) 第2章で定める軽微な違反については、教職員の都度による注意をもって、その処分とする。ただし、違反行為を繰返すなど改善が認められない等の場合や悪質な場合に関しては、この限りではない。
- (2) 第3章で定める重度な違反については、「大学 SIGN利用ライセンス制度運用内規」第12条に従い利用の取消しまたは停止処分とする。

第2章 軽微な違反

(利用マナー)

第3条 実習室、共同利用室、IT&コミュニケーションルーム、大学院学生共同研究室等、実習用のデスクトップパソコンが配備された教室、及び、指定された場所において、下記の行為を禁止する。

- (1) 飲食物の持ち込み (ペットボトルについては、蓋を閉め、カバン等に収納すること。弁当、菓子等も同様の扱いとする。)
- (2) 濡れた傘の持込 (傘立てがない場合は所定のビ

ニール袋に入れること)

- (3) 未届出での教室AV設備機器等の利用および移動
- (4) SIGN利用ライセンス証の不携帯での情報教育ネットワーク (SIGN) の利用

2 前項で定めた以外の教室において、以下の行為を禁止する。

- (1) 教室設備 (AV機器やネットワーク機器等) に影響を及ぼすような飲食物や傘などの取扱い (飲食を可能とするが、その扱いには十分注意を払うこと。)
- (2) 未届出での教室AV設備機器等の利用および移動
- (3) SIGN利用ライセンス証の不携帯での情報教育ネットワーク (SIGN) の利用

3 パソコンロッカールームにおいて、以下の行為を禁止する。

- (1) 飲食物の持ち込み (ペットボトルについては、蓋を閉め、カバン等に収納すること。弁当、菓子等も同様の扱いとする。)
- (2) パソコンロッカーの不正使用 (割当外のロッカーの使用、禁止物の収納、非施錠)
- (3) 本人以外のパソコンロッカーの解錠、施錠
- (4) パソコンロッカー上やパソコンロッカールーム内への物品の放置等
- (5) パソコンロッカールームにおける落書き、不許可掲示
- (6) パソコンロッカールーム内の設備の損壊

(携帯パソコンの利用ルール)

第4条 携帯パソコンのSIGNへの接続にあたっては、利用ルールを遵守しなければならない。

- 2 以下に定める事項については禁止する。
 - (1) 所有者未許諾での他人の携帯パソコンの使用
 - (2) 指定されたコンピュータ名の改変
 - (3) 公序良俗に反する目的で作成されたファイル・ソフトのインストール、および起動
 - (4) ウイルスに感染したパソコンのSIGNへの接続
 - (5) Windows Update、ウイルス対策ソフトの更新等、情報センターより発信されたセキュリティ対策の不履行

(認められた機器以外の接続)

第5条 申請に基づき接続が承認された情報機器以外の機械装置をSIGNに接続してはならない。

第3章 重度な違反

(設備の破壊)

第6条 設置された情報機器のハードウェア、ソフトウェアを損壊してはならない。この場合において、故意、または重大な過失が認められた場合、処分対象とする。

(不正アクセス)

第7条 内外のネットワークに対し、以下に示すような不正アクセス、及び侵害行為を行ってはならない。

- (1) 権限外のファイルへの不正アクセス及び、不正な権限取得を目的とした行為
- (2) パスワード解読、ポートスキャン等のプログラムの実施、持ち込み。
- (3) なりすまし行為 (他人のIDでの接続を含む)
- (4) 認められたもの以外のネットワーク資源・ソフトのダウンロード
- (5) コンピュータウィルスの作成、持ち込み
- (6) その他、情報センターが禁止した不正アクセス行為

(知的財産権侵害)

第8条 著作権侵害、商標の無断使用、肖像権侵害等の行為を行ってはならない。

(公序良俗違反)

第9条 以下に示す公序良俗に反するメールやコンテンツの配信を行ってはならない。

- (1) 他人に対する誹謗・中傷
- (2) 他人の社会的評価に関わる問題の掲載
- (3) 他人のプライバシーの侵害
- (4) 風俗営業に関わる情報、ネズミ講に関する情報の配信
- (5) その他、情報センター長が公序良俗に反すると認めたもの

(犯罪と認定される行為)

第10条 詐欺・脅迫・恐喝・薬物使用促進・わいせつ物陳列・淫行勧誘・嫌がらせ・ストーカー行為等、犯罪と認定されるような行為を行ってはならない。また、犯罪を目的とした情報の受発信をしてはならない。

(システム妨害)

第11条 以下に示すシステム資源の大量消費に繋がる行為を禁止する。

- (1) チェーンメールの発信・転送や大量のメール送受信
- (2) 未承諾の大量データのダウンロードおよびアップロード
- (3) システム妨害となるような不正データの送込み
- (4) その他、情報センター長が指定した行為

(営利行為)

第12条 商品の売買、その他営利を目的とした利用を禁止する。

産業能率大学 SIGNのID、パスワード管理に関する内規

(目的)

第1条 本内規は、「大学 情報教育ネットワーク(SIGN)利用規程」(以下、「規程」という)第4条に基づき、SIGN利用ライセンスを付与された者に対し、SIGNを利用するためのIDを発行する手順と遵守すべき事項を規定するものである。

(IDの管理)

第2条 IDは、附表の基準にしたがい、情報センター長が学生情報サービスセンター長にID、暫定パスワードの付与、停止、削除を指示することにより管理する。

(パスワードの管理)

第3条 利用者はパスワードの管理について一切の責任を負う。

- 2 利用者は、付与された暫定パスワードを自己の定めるパスワードに速やかに変更しなくてはならない。
- 3 パスワードは、次の規準を満たして設定しなくてはならない。
 - (1) パスワードは6文字以上8文字以内とする。
 - (2) パスワードは英数字や記号などを混在させる。

(パスワードの再発行)

第4条 利用者は、パスワードを忘れた等の理由によりパスワードの再発行が必要な場合には、学生情報サービスセンターの窓口に設置したパスワード再発行申請用端末に必要事項を記入し、学生情報サービスセンター長に申請する。

- 2 学生情報サービスセンター長は、パスワードの再発行を承認した場合、学生情報サービスセンター担当者にパスワードを再発行するよう指示する。
- 3 学生情報サービスセンター担当者は、暫定パスワードを発行し、当該利用者にパスワードの再発行完了の連絡を行い、学生の場合には学生証、教職員の場合には本人であることを確認のうえ、引き渡しを行う。
- 4 利用者は、暫定パスワードを受け取り、直ちに暫定パスワードを変更しなくてはならない。

(遵守事項)

第5条 利用者は、本サービスの利用に際し、本規程、並びに関連する各規程に定める事項について遵守しなければならない。

(IDの停止)

第6条 学生情報サービスセンター長は、利用者が教職員で休職または留学する場合、人事発令に基づき当該利用者のIDを停止し、復職後に再開する。

- 2 学生情報サービスセンター長は、利用者が学生で休

学する場合、教授会に付議され承認された学籍異動一覧に基づき当該利用者のIDを停止し、復学後に再開する。

(IDの削除)

- 第7条 情報センター長は、教職員が退職、またはSIGN利用対象部門から異動した時に学生情報サービスセンター長にIDの削除を指示する。
- 2 情報センター長は、学生が卒業、退学および除籍された場合、学籍異動決定後、学生情報サービスセンター長にIDの削除を指示する。

(本サービスの管理)

- 第8条 学生情報サービスセンター長は、本サービスの適正な運用の維持に必要な事項について記録管理する。

【附表】 情報教育ネットワーク (SIGN) のID付与、停止、削除基準				
	対象	IDの付与	IDの停止、再開	IDの削除
(1)	大学通学課程、大学院の正課生	入学をもって付与	休学する場合、学籍異動決定後の異動一覧に基づき停止し、復学後に再開	卒業、退学および除籍された場合、学籍異動決定後の異動一覧に基づき削除
(2)	短大、大学、大学院の専任教員	人事発令に基づき付与	休職、留学時、人事発令に基づき停止(復職後再開)	退職時及び、短大、大学、大学院の専任教員を外れた時、人事発令に基づき削除
(3)	大学、大学院の兼任教員	人事発令に基づき付与	---	大学、大学院の兼任教員契約を解除した時、人事発令に基づき削除
(4)	職員	所属長の申請に基づき付与	所属長の申請に基づき停止、再開	所属長の申請に基づき削除
(5)	その他の者	所管部署の所属長の申請に基づき付与	所管部署の所属長の申請に基づき停止、再開	所管部署の所属長の申請に基づき削除

産業能率大学 携帯パソコン制度に関する規程

(目的)

- 第1条 産業能率大学(以下「本学」という)の携帯パソコン制度(以下「本制度」という)は、本学の学生が専用の携帯型パソコン(以下「携帯パソコン」という)を所持し、「学生ひとりひとりがパソコンを道具として使いこなす」ことにより、現代において求められる情報リテラシーを修得することを目的とする。

(携帯パソコンの活用推進)

- 第2条 本学は、学生が情報リテラシー修得にあたり必要となる各種サービスの提供や授業での利用を積極的に推進することとする。
- 2 この場合における施策や周辺機器の配備等は、学長が別に定めるところにより行う。

(適用)

- 第3条 本制度の対象者は、学部通学生およびその他の学生で情報センター長の許可を得た者とする。

(ネットワークへの接続)

- 第4条 第1条の目的を達成するため、学生は、所持する携帯パソコンについて、大学の情報ネットワークに接続する許可を受けなくてはならない。

(学生の遵守義務)

- 第5条 学生は、携帯パソコンの利用にあたっては、関連諸規程に定められた規則を遵守しなくてはならない。

(運用規則)

- 第6条 携帯パソコン制度の運用ルールについては、「大学携帯パソコン制度の運用に関する内規」に定める。

(管轄部署)

- 第7条 本制度の運用は、情報センターが主体となって行う。
- 2 携帯パソコンの利用に関する事務は情報サービスセンターが行う。

産業能率大学 携帯パソコン制度の運用に関する内規

第1章 総則

(目的)

- 第1条 本内規は、学生が専用の携帯パソコンを有効に利用するための運用制度について規定する。

(SIGN接続を許可するパソコンの数)

- 第2条 SIGNへの接続を許可される携帯パソコン(以下単に「携帯パソコン」という)は、学生1名につき1

- 台を原則とする。
- 2 SIGNに接続しないパソコンの学内持込みについては第4章に定める。

(携帯パソコンの仕様)

第3条 利用可能な携帯パソコンの仕様、及び携帯パソコンにインストールするソフトウェアについては、情報システム運営委員会の答申を受け、学長が年度毎に定める。

(大学標準機の斡旋)

- 第4条 大学は、携帯パソコンに関して、大学標準機(以下、「大学斡旋パソコン」という)を設定し、入学時に学生に斡旋する。
- 2 大学斡旋パソコンの選定に際しては、情報システム運営委員会において審議し、稟議に付したうえで、大学学長が決裁を行なう。
 - 3 編入生については、編入する年度の新生と同機種の案内を行う。

(大学斡旋パソコンに対するサービス)

第5条 大学斡旋パソコンの利用に際し大学が提供するサービスについては、第2章に定める。

(個人購入パソコンの利用)

- 第6条 大学斡旋パソコン以外の個人で所有する携帯パソコン(以下、「個人購入パソコン」という)の利用については、情報センターにて事前に審査を行い、情報センター長が許可をした場合にSIGNへの接続を許可する。
- 2 個人購入パソコンの利用に関する運用ルールについては、第3章に定める。

(パソコン専用ロッカーの貸与)

- 第7条 大学は、所有する携帯パソコンのSIGNへの接続を許可された学部通学生に対し、携帯パソコン専用ロッカーを貸与する。
- なお、このロッカーの利用において紛失・盗難等の被害が発生した場合、本学はその責を負わない。
- 2 学生情報サービスセンターは、貸与したロッカーを施錠した鍵の紛失などの場合、貸与者本人からの申し出により学生情報サービスセンター長が許可のうえ、鍵を壊して開錠することができる。
 - 3 学生情報サービスセンターは、貸与者以外による不正利用、貸与者の学籍異動による利用資格喪失、違反物品格納等の場合は、学生情報サービスセンター長の許可により鍵を壊して開錠することができる。その際のロッカー内の物品については拾得物と同様の扱いとする。

(遵守事項)

第8条 本制度の利用者は、関連諸規程に定められた規則の他、次に定める事項について遵守しなければならない。

- (1) 大学指定のウィルスワクチンソフトをインストールし、常に最新データに更新すること。
- (2) 接続を許可されたパソコンに、所定のシールを貼ること。
- (3) 機器を変更する場合は、速やかに変更の申請手続きを行うこと。

第2章 大学斡旋パソコン

(目的)

第9条 本章は、大学斡旋パソコンの運用に関わる事項について定める。

(適用)

第10条 本章は、大学斡旋パソコン利用者に適用する。

(利用申請)

第11条 大学斡旋パソコンを利用する学生は、別途設定する申込期間内に、携帯パソコン購入申込書を情報センターの定める提出先に提出し、支払いの手続きが完了することにより申請が完了したものとす。

(携帯パソコンの引渡し)

- 第12条 大学斡旋パソコンの引渡しは、次のとおりとする。
- (1) 大学は前条の手続きが完了した学生に対し、大学の指定する日および指定する場所で大学斡旋パソコンの引渡しを行う。
 - (2) 学生は、受取りの際には、本人確認ができる学生証などを持参しなければならない。
 - (3) 学生は、受取り後に実施の講習会に必ず出席しなくてはならない。やむを得ず欠席する場合は、事前に学生情報サービスセンターに連絡しなければならない。

(故障、障害時の対応)

第13条 本制度の利用者は、一般的な使用環境で使用中にパソコンの動作に障害が発生した場合、学生情報サービスセンターにて障害内容の確認及び調査・対応を受けることができる。

(大学斡旋パソコンに対するサポートサービス)

- 第14条 大学は、大学斡旋パソコンの安定利用を目的として、以下のサービスが享受できるよう納入業者等に手配する。
- (1) 大学斡旋パソコン引渡し日より指定期間の動産保険サービス。
 - (2) 大学斡旋パソコンおよびその付属品の修理に関するサービス。

(修理申込および返却の手続)

- 第15条 大学斡旋パソコンの修理申し込みおよび返却の手続きは、次のとおりとする。
- (1) 本制度の利用者は、「携帯パソコン修理申込

書」に必要事項を記載し、学生情報サービスセンターに現品と共に提出する。

- (2) 学生情報サービスセンターは、修理品の預かりが必要な場合には、現品と引替えに「修理品引換書」を利用者に渡さなければならない。
- (3) 修理の完了後は、「修理品引換書」の提出および「学生証」の提示と引替えに修理済現品を返却する。

(修理期間中の代替機貸出し)

第16条 本制度の利用者は、修理期間中については、授業で利用する場合に限り、次の要領で代替機の貸出しを受けることができる。

- (1) 修理申込時に受領した「修理品引換書」と「学生証」を持参し、学生情報サービスセンターに申し出る。
- (2) 貸出しは授業の行われる時限単位を原則とし、授業終了後の自習利用や自宅への持ち帰りは不可とする。ただし、課題等の提出に支障がある場合は、担当教員との調整により、時間延長を行う場合がある。

(紛失・盗難時の処置)

第17条 大学斡旋パソコンを盗難、または紛失した場合、学生は速やかに学生情報サービスセンターに報告しなくてはならない。

- 2 警察への届出を行った場合には、盗難受理番号など必要事項を学生情報サービスセンターまで連絡しなくてはならない。

(盗難・紛失時の代替機および備品の貸出しについて)

第18条 盗難・紛失時の代替機および備品の貸出しについては、次のとおりとする。

- (1) 学生情報サービスセンターに連絡後の1週間を、捜査期間とし、この期間は代替機および備品の貸出しを受けることができる。ただし、この場合においても、貸出しの単位は授業時間ごととする。学生情報サービスセンター長の判断により、この時期を延長することができる。
- (2) 捜査期間終了後、個人で購入するか、大学経由で購入するか意思決定を行わなくてはならない。なお、時期によっては、大学経由での購入が不可能である場合もある。
- (3) 大学経由での購入を選択した場合には、機器の引渡しが完了するまでの期間、代替機の貸出しを受けることができる。
- (4) 個人での購入を選択した場合には、購入準備期間の2週間(届け出より3週間)まで代替機の貸出しを受けることができる。

(卒業・退学後の取り扱い)

第19条 卒業・退学後の、大学斡旋パソコンの障害及びトラブルについてのサポートは大学では一切行わない。

第3章 個人購入パソコン

(目的)

第20条 本章は、個人購入パソコンの運用に関わる事項について定める。

(適用)

第21条 本章は、個人購入パソコン利用者に適用する。

(利用申請)

第22条 個人購入パソコンの利用を希望する学生は、大学が案内する申し込み期間または募集期間中に、所定の接続申請書に必要事項を記入し学生情報サービスセンターに提出しなくてはならない。

(利用の許可)

第23条 情報センター長は、利用申請が適正と認められた場合には、個人購入パソコンの利用を許可する。

(許諾の通知と指導)

第24条 学生情報サービスセンターは、情報センター長の許可の通知を基に、学生に対し、インストール作業の方法や、手続関連の指導を行う。

- 2 学生情報サービスセンターは、学生のインストール作業状況を把握・管理しなくてはならない。

(環境の同期)

第25条 利用許可を得た学生は、学生情報サービスセンター指定の説明会に参加し、学内の指定された場所で、大学指定のソフトウェアのインストール作業及びネットワークの設定を行わなければならない。

- 2 設定内容については、説明会ごとに別途定める。

(自己責任の原則)

第26条 「個人購入パソコン」の利用にあたっては、すべて自己責任を原則とする。

自己責任の範囲とは、例えば次のとおりとする。

- (1) 授業や情報サービス、大学設置の周辺機器(プリンタ、マルチメディア機器など)の利用での不具合
- (2) ネットワーク接続に関する不具合
- (3) 必要な周辺機器(LANカード、LANケーブル、DVDドライブなど)の購入
- (4) 故障、または障害などによる不具合
- (5) アプリケーションソフトの作動に関する不具合

- 2 前条に基づき実施した大学指定のソフトウェアのインストールや設定変更などによる不具合の発生について、大学では責任を負わない。

(代替機の貸出し)

第27条 故障、紛失、盗難等、個人購入パソコンが使用不能に陥った場合であっても、大学は代替機の貸出し

はしない。

(紛失・盗難時の処置)

第28条 個人購入パソコンについても紛失・盗難時には、情報サービスセンターに届けなくてはならない。

第4章 SIGNに接続しないパソコン

(目的)

第29条 本章は、接続未許可パソコンを学内に持ち込む際の運用に関わる事項について定める。

(適用)

第30条 本章は、全学生に適用する。

(利用の原則)

第31条 情報コンセントの設置された教室(実習室、情報化教室、図書館等)、およびプリンタルームに、接続未許可パソコンを持ち込む場合、および情報コンセントに接続する場合には、予め許可を受けなければならない。

- 2 接続未許可パソコンの指定された場所以外での利用については、自由とする。

(利用申請)

第32条 指定場所での接続未許可パソコンの利用を希望する学生は、所定の接続申請書の必要事項を記入し、学生情報サービスセンターに提出しなくてはならない。

(利用の許可)

第33条 情報センター長は、利用申請が適正と認めた場合には、接続未許可パソコンの利用を許可する。学生情報サービスセンターは、情報センター長の許可通知を元に、学生に対し通知する。

- (1) 持込を許可されたパソコンに、所定のシールを貼ること。
- (2) 機器を変更する場合は、速やかに変更の申請手続きを行うこと。

(許可の有効期限)

第34条 許可の有効期限は当該年度内とする。

(自己責任の原則)

第35条 接続未許可パソコンの利用にあたっては、すべて自己責任を原則とする。自己責任の範囲とは、例えば次のとおりとする。

- (1) 故障、または障害などによる不具合
- (2) アプリケーションソフトの作動に関する不具合
- (3) 盗難・紛失時の処置

(遵守事項)

第36条 学生の違反が発見された場合には、持込許可を取り消すと共に、「大学 SIGN利用の規制に関する内規」に基づき処分する。

ここに記載されている規定は、
2022年4月1日現在のものです。

インターネットの利用について

(参考ホームページ一覧)

「神奈川県警察 サイバー犯罪」

https://www.police.pref.kanagawa.jp/index2.htm#cyber_hanzai

「警視庁」

<https://www.keishicho.metro.tokyo.lg.jp/>

「警察庁」

<https://www.npa.go.jp/>

「一般財団法人インターネット協会」

<https://www.iajapan.org/>

「独立行政法人 情報処理推進機構」

<https://www.ipa.go.jp/>

「Microsoft Windows Update のページ」

<https://www.microsoft.com/ja-jp/safety/protect/musteps.aspx>

SIGN 利用ライセンス制度の理解に向けて

2024年4月1日 発行（第24版）

産業能率大学 情報センター