## はじめに

明治大学内のコンピューターからインターネットにアクセスするためには、この「**MIND 利用講習会**」を受講しなければなりません。

明治大学のネットワークの総称を MIND（マインド）と呼びます。明治大学内からネットワークに接続する場合は、どのような状況であれ「MIND」を利用していることになります。

皆さんは既に携帯電話やスマートフォン、自宅のパソコンなどから、インターネットを利用したことがあると思います。しかし、大学には大学のルールがあります。明治大学のネットワーク＝MIND を利用するためには、そのルールを知り、守る必要があります。この講習会には、まずはこれらのルールを理解するという大きな目的があります。

また、インターネットを利用する際には、大学のルール以外にも注意しなければならないことがあります。この講習会では、おもに以下のことを説明します。

### （1）この講習会の目的

・明治大学には、ネットワークを利用するためのルールがあります。ルールを守らないと利用停止などの措置を受けることになります。大学内のネットワーク利用のルールを学習しましょう。
・インターネット利用上の注意・マナー・エチケット等を学習し、安全かつ快適に利用しましょう。
・自宅など、大学外でインターネットを利用する際にも、明治大学の一員として心がけるべきマナーを学習しましょう。
・近年、インターネット上のトラブルが多くなっています。インターネット上のトラブルは、「原因はささいなことである場合が多い」、「巻き込まれていることに気づきにくい」、「意図せず自分が加害者になることがある」、「どのようなトラブルが多発しているのかを自分で知る必要がある」などの特徴があります。このような特徴を理解し、トラブルを回避しましょう。
・被害者にならないためには、自分で自分を守る必要があります。「パスワードの適切な管理」、「コンピューターの保護」、「最近の事例を知ること」について学習しましょう。
・コンピューターウィルスやスパイウェアなど情報セキュリティについて学習しましょう。

### （2）この講習会を受講するとできるようになること

・明治大学内のコンピューターからインターネットへのアクセスが可能になります。
・MIND モバイル接続サービス（後述）が利用できるようになります。

# 1．明治大学のネットワーク

## （1）MIND とは

「MIND」とは、**明治大学のネットワークの総称**です。「**Meiji University Integrated Network Domain**」の略で、「マインド」と読みます。明治大学内の施設・設備からインターネットに接続する場合は、どんな状況であれ「MIND」を利用していることになります。

MIND では、皆さんの学生生活を支える便利な情報サービスが、数多く提供されています。

- **Oh-o! Meiji システム**
  明治大学の全学的な教育支援システムで、授業の検索や資料の閲覧、レポートの提出、大学からのお知らせの確認、個人スケジュールの登録・管理などを行うことができます。
- **Meiji Mail**
  明治大学の全学生が利用できるメールシステムです。
- **図書館オンラインサービス**
  図書館で提供しているサービスで、学内外の資料所在情報を検索したり、外部データベース・電子ジャーナル、図書の予約申込や貸出延長、配送依頼などができます。

## （2）MIND のルール

MIND の利用について、明治大学が定めるルールがあります。MIND を利用するには、これらのルールを遵守しなければなりません。

**・MIND 関連規程**

大学が定める「MIND 関連規程」は、MIND のウェブサイト上に公開されています（http://www.meiji.ac.jp/mind/rule/index.html）。利用者に関連するところでは、「MIND 利用基準」、「MIND 運用基準」、「MIND 審査委員会要綱」などがあります。これらの中でもすべての利用者に関係するのが「MIND 利用基準」です。

**・MIND 利用基準**

「MIND 利用基準」は、利用者のための規程です。「第 7 条（遵守事項）」に MIND 利用上の大原則が定められています。MIND は以下のような利用方針に則って利用しなければなりません。大前提なのでよく読み、遵守してください。

①教育・研究及びその支援に関連する目的以外に使用しないこと。
②営利を目的に利用しないこと。
③通信の秘密を侵害しないこと。
④プライバシー、名誉等の他人の権利を不当に侵害する情報や公序良俗に反する情報を取り扱わないこと。

⑤知的財産権により保護された情報の取り扱いには注意すること。
⑥MIND の適正かつ正常な運用のために協力し、運用に支障を来すような利用をしないこと。
⑦その他情報基盤本部長が必要と認める事項。

**・「MIND 利用上の遵守事項ガイドライン」について**

本テキスト最終ページの[資料]・「MIND 利用上の遵守事項ガイドライン」は、MIND 利用基準第 7 条をわかりやすく説明したものです。安全で快適なネットワークの利用のために、MIND 関連規程に定められていることの中から特に重要なものを抜粋しました。必ず熟読し、遵守してください。

## ２．MIND 過去の違反事例

残念なことに、大学のネットワーク、コンピューター利用における利用違反がこれまでに何回か発生しています。その違反の内容と違反者に対する厳しい措置について紹介します。

ルールを遵守することが、学生生活を送る上で大変重要であるということが理解できると思います。

### （1）過去の違反事例

#### ① 違反事例１： ユーザーID／パスワードの貸し借り

ユーザーID／パスワードを貸し借りすると、貸した側、借りた側の両者が不正利用とみなされます。

「自分のユーザーID を使用して、隣にいる友人に利用させる」ことも、実質的に代人利用ですので不正です！

友人に貸してくれと頼まれたとしても、毅然とした態度で断りましょう。

また、学内の共有パソコンを使用後、うっかり終了するのを忘れてしまい、後から来た人がそのまま利用してしまうというケースがあります。この場合、後からパソコンを利用する人は、あなた自身のユーザーID でパソコンを利用することになり、結果的にユーザーID の貸し借りと同じ危険性があります。パソコン利用後は忘れずに終了するようにしてください。

#### ※ パスワードの取り扱いについて

ユーザーID とパスワードは、あなたがコンピューターの正当な利用者であることを証明する役割をもっています。

パスワードを紛失したり、盗難に遭ったりすると、そのアカウントで利用できるサービスすべてを不正に行使されるおそれがあります。他人のアカウントを盗み見したり、何らかの形で知り得たりしたものを不正に行使することは、不正アクセス禁止法により禁じられていますが、利用者側は自衛手段を講じて被害に遭わないようにしなければなりません。紛失、盗難に気づいたら、当該アカウントの管理者や発行者に至急報告し、アカウントを停止してもらいましょう。大学内のアカウントであれば、所定の事務室に申し出てください。

また、パスワードは以下の点に留意して設定するようにしましょう。

・予測されにくいものを設定する。（誕生日や電話番号はNG!!）

・定期的な変更を心がけること。

・数字とアルファベットを混ぜる。なるべくアルファベットは大文字と小文字を混ぜる。

### ② 違反事例２： 外部ホームページへの不適切な書込み

・掲示板へのトピックとは関係のない情報

・他人の個人情報

・ねずみ講勧誘まがい

・特定個人に対する誹謗中傷

学内のネットワーク、コンピューターを利用し、外部ホームページの掲示板にアクセスすることができます。決してルールに反した不適切な書込みはしないようにしてください。場合によっては犯罪行為とみなされ、法的な措置を取られる場合があります。

学内のコンピューターではいつ・誰が・どのコンピューターを利用して、どのホームページにアクセスしていたかはすぐにわかります。

外部のホームページに不適切な書込みをした場合、そのホームページ管理者からの通報があれば、すぐに誰の行為か割り出すことができます。

匿名だから大丈夫だと安易な判断をしないでください。

### ③ 違反事例３： 不適切なホームページの公開と掲示板の管理不足

・不適切画像の貼りつけ

・掲示板の放置による不適切な書込みの長期間の掲載

学内に自分のホームページを立ち上げることができます。しかし注意しなければならないのは、そのホームページは全世界に向けて公開されるということです。

自分で不適切な書込みをするのは言語道断ですが、不特定多数が参加できる掲示板を開設した場合は、世界中から書込みができるということを認識してください。誰がどんな書込みをしてくるかわかりません。定期的に掲示板の書込み内容をチェックし、不適切な書込みを発見したら、速やかに削除するようにしてください。

## （２）違反者に対する措置

違反をした者に対しては、MIND 関連規程に則り、利用停止や利用資格取消等の厳しい措置がとられます。これらの措置を受けたものは、MIND が利用できなくなり、単位取得、進級、卒業、就職に大きな影響を及ぼしてしまうことになる以下のような深刻な事態に陥ります。

① 教室や自習室に設置してあるパソコンが利用できなくなる。

① 図書館のパソコンが利用できなくなる。

① 学内の無線 LAN や情報コンセントが利用できなくなる。
① Web での履修申請ができなくなる。
① 証明書自動発行機が利用できなくなる。
① Oh-o! Meiji システムが利用できなくなる。
① 大学の電子メールが利用できなくなる。

## ３．インターネット利用時の注意とマナー

インターネットには全世界で数億台ものコンピューターが接続されており、きわめて公共性の高いシステムであると言えます。不特定多数が参加する仕組みだからこそ、個々がモラルと節度を持って利用しなければなりません。公共の場におけるマナーをよく意識して利用してください。「自分だけなら何をやっても迷惑にならない」、「自分さえ良ければいい」、「ネット上なら許される」というような安易な考え方はトラブルのもとになります。

インターネットを利用するときには、守らなければならないルール（法律や規則）と、守るべきマナー（エチケット）があります。ルール違反は罰則の対象となり処罰されます。マナー違反は批判され、ネットワークの利用やコミュニケーションに大きな支障を来すことがあります。自分の責任は自分で取る覚悟が必要です。

また、インターネット上でのトラブルは「ほんのささいなこと」が原因になることがままあります。しかし「ほんのささいなこと」でも、知っていなければ気をつけることはできません。どんなトラブルが流行しているのかを、常に知っておく必要があります。

### （１）不用意なコピーに注意

#### ① 関連法規

インターネットを利用する上でのルールには、「明治大学で定めるルール（＝MIND 利用基準)」以外にも、法律により定められたものがあります。法律を犯せば、犯罪として法の下に処罰されます。以下に関連する事項と法規を紹介します。

・不正利用・不正アクセス（不正アクセス行為の禁止等に関する法律） ※1
・わいせつ物の頒布等（刑法第 175 条「わいせつ物頒布等」等）
・ネズミ講（無限連鎖講の防止に関する法律）
・マルチ商法（無限連鎖講の防止に関する法律・刑法第 246 条「詐欺」等）
・違法薬物の販売（薬事法・大麻取締法・覚せい剤取締法・麻薬及び向精神薬取締法等） ※2
・ネットワークストーカー（ストーカー行為等の規制等に関する法律等）
・脅迫・詐欺 （刑法第 222 条「脅迫」・第 246 条「詐欺」等）

・犯罪予告（刑法第 222 条「脅迫」・刑法第 233 条「信用毀損及び業務妨害」・刑法第 234 条「威力業務妨害」）

※１　他人のアカウント（ユーザーID やパスワード）を盗んで、あるいは何らかの経緯で知り得て、ログインするだけでも、「不正アクセス行為の禁止等に関する法律」に抵触します。遊び半分だからといって許されるわけではありません。

※２　違法薬物は、インターネット上でも、言葉巧みな誘い文句のもとでやりとりされています。法律で禁止されているのはもちろんのこと、乱用した者の心身を例外なく破壊するものです。絶対に手を出してはいけません。

### ② 諸権利を侵害する行為

インターネット上では、さまざまな情報がやりとりされています。その中には、法律で保護される権利が含まれていることがあります。

・知的財産権
・プライバシーに関する権利
・個人情報の取り扱い
・肖像権等

パソコン上では、簡単な操作で文章や画像、動画などの情報を複製（コピー）することができます。とても便利なことですが、権利で保護された著作物や情報をやりとりする際には、十分な注意が必要です。マウスを操作するだけでやりたいことができてしまうぶん、うっかり、あるいは軽率に、他人の権利を侵害してしまう可能性があるということです。自分の操作や行為に責任をともなうことを念頭に置いておきましょう。

### ③ 引用と盗作

レポートや論文を作成する際にも注意が必要です。インターネット上に公開されている他人の著作物（文章や画像等）をそのままコピー&ペーストしたものを、自分の著作物として提出することは、著作権法に抵触するばかりか、レポートや論文、課題の意義から鑑みても問題です。

引用には引用のルールがあります。他人の著作物を引用する際には、次の点に留意しましょう。
・引用はあくまでも、その目的および分量において、正当と認められた範囲内に限られます。
・引用の際は、引用箇所がはっきりと分かるようにカギカッコで括るなどの区別をした上で、
　出典・タイトル・著作権の所在
などを明示しましょう。

## （2）<u>文字によるコミュニケーションのマナー</u>

マルチメディアという言葉のとおり、インターネット上では様々な形態のコンテンツや情報がやりとりされています。コミュニケーションの手段も、音声チャットやテレビ（動画）電話などが手軽に利用できるようになってきました。

しかしながら、いまだ「文字によるコミュニケーション」が多くやりとりされています。電子メールや電子掲示板（BBS)、インスタントメッセンジャー、ブログやSNS（facebookやtwitterなど）など、これらはすべて「文字」を中心にやりとりされているものです。

文字でのやりとりは、面と向かってコミュニケーションするときに比べて、発言のニュアンスや趣意がうまく伝わらないことがあり、ときとしてネガティブな誤解を招くことがあります。自分は何気なく書いたつもりのメールやメッセージも、相手が不快に思っていたり、あるいは相手を傷つけていたり、意図しない誤解を生んでいたりすることがあります。ほんのささいなことがきっかけで、大きなトラブルになることも少なくありません。普段のコミュニケーション以上に注意する必要があります。

親しい友人関係でさえ、注意しないとあらぬ誤解を招くことがあります。また、特に不特定多数が閲覧する可能性のある電子掲示板や、顔見知りでない相手とのやりとりには、以下のような点に注意すべきです。

・感情的な表現や否定的な表現など、相手を刺激するような言い回しは避ける。
・意味不明な表現やスラングの使用には注意する。
・冷静に判断する。

**・メールのマナー**

メールは私たちにとって大変身近なものですが、そのぶん、マナーに対する意識が軽薄になっていることがあります。時と場合をわきまえて正しく利用しないと、マナー違反だと思われるばかりか、必要な情報がきちんと伝えられず、コミュニケーションに支障を来す場合もあります。

・宛先に注意。間違えて送信してしまっても、取り戻すことはできない。
・件名は的確に。なるべく用件がわかりやすいように。長すぎず、短すぎず。携帯電話では「無題」のまま送ることがあっても、パソコンのメールでのやりとりではマナー違反とされることが多い。
・仕事等プライベート以外のやりとりでは、必要事項（宛先、自分の名前、用件）を明確にするよう心がけること。例)「○○様　明治大学の△△です。××の件について・・・」
・署名をつける。凝ったものでなくてよい。必要な情報（所属・氏名・連絡先等）が伝わるように。相手によって内容を変更することも必要。
・メールを送ったからといって、すぐに相手の手元に届くとは限らない。メールサーバやネットワークのトラブル等により、届かないこともある。

## （3）情報発信の落とし穴

**・SNS でのトラブル（嫌がらせ・ストーカー被害など）**

「twitter」や「facebook」に代表されるようなサービスのことを「SNS（Social Network Service）」といいます。一般に、人と人とのつながりをサポートする、登録制のウェブサイトやそのサービスのことを指します。同じ趣味や趣向、居住地、出身校などを持つ者同士が、ウェブサイト上で集まり、気軽にコミュニケーションをとることができます。

しかし、この SNS をめぐるトラブルも少なくありません。後述する「炎上」の問題や、配慮のない書き込みなどによって、友人との信頼関係にひびが入ってしまうこともあります。また、住所や誕生日、よく訪れる場所といった自分のプロフィールを詳しく公開することで、それらの情報をもとにストーカー的な被害に遭うおそれもあります。個人を特定できる顔写真などを掲載する場合にも注意が必要です。インターネット上に公開するものは、全世界から閲覧される可能性があるということを念頭に置く必要があります。

**・炎上（フレーミング）－ブログ・SNS・電子掲示板（BBS）など**

ブログや SNS、BBS に何気なく書き込んだ冗談であっても、冗談では済まされないことがあります。インターネット上で発言するということは、世界中から閲覧される可能性があるということを意味しています。その影響力を意識しておく必要があります。

BBS で犯罪予告をすれば、威力業務妨害などの罪に問われ、検挙されます。インターネットは匿名性があると思われていますが、それはユーザー同士が互いにそうであるだけであって、アクセスした記録や書き込みをした記録は残ります。匿名性はないものと思ってください。

反社会的な行為、犯罪行為などを、実際には行っていないにもかかわらず、あたかも自分がやったかのように自慢気に書き込みをして、大きなトラブルにつながるというケースは後をたちません。ほんの冗談のつもりで「やってもいないこと」を書いたとしても、「やっていない」では済まされなくなります。世界中から閲覧されるということは、「真剣に事実だと思い込んで批判する者」、「嘘だとわかっていながらはやし立てる者」、「ただおもしろがって火に油を注ぐ者」等々、様々な閲覧者がいるということを意味しています。

また、一度インターネット上に公開した情報は、回収して「なかったことにする」のはたいへん困難です。したがって、たとえば自分や友人の個人情報や、個人が特定できるような顔写真等、コンテンツの取り扱いには十分注意しなければなりません。ブログや SNS などで皆さんが行った不注意な発言や投稿が、将来の就職活動などで不利に働いてしまうこともあるかもしれません。

インターネット上に情報を公開する際には、その内容について十分配慮し、皆さん自身が責任を持って行うようにしましょう。

## ４．情報セキュリティ

インターネットは大変便利なシステムですが、安全で快適に利用するためには、自分で気をつけなければならないことがあります。ここでいう「情報セキュリティ」は、インターネット上の罠に巻き込まれないための自衛手段としてとらえてください。

## （1）コンピューターウィルス

「コンピューターウィルス」とは、なんらかの経路で外部から侵入する、悪意をもったプログラムのことを指します。

**・感染経路**

主な感染経路は、電子メールの添付ファイル、ウェブ（インターネット）上からダウンロードしたファイル、外部記憶媒体などです。**最近ではホームページを閲覧するだけで感染するウィルスも多数出現しています**。

**・症状**

症状は、パソコンが起動しない、頻繁にフリーズする、画面表示が乱れる等コンピューターの異常な動作のほか、ファイルやデータが削除される、保存したファイルやデータを無作為にばらまく、システム自体を破壊するなど、多種多様です。中には、感染したパソコンのアドレス帳等を参照して、ウィルスに感染したファイルをメールに添付して勝手にばらまいたりするものもあります。さらにはコンピューター自体を乗っ取り、他のコンピューターに攻撃を仕掛けるものもあります。つまり、**ウィルスに感染したパソコンやユーザーは、被害者であると同時に、加害者になってしまう可能性が高い**のです。

ウィルスの中には、「バックドア」と呼ばれる仕掛けを残すものもあります。感染したコンピューターに「隠し穴」を作っておき、その穴を利用していつでもそのコンピューターに攻撃できるようにしたり、不正なプログラムを仕掛けたりできるようにするものです。

「トロイの木馬」といわれるタイプは、先述のようなコンピューターウィルスの症状がないものが多く、ウィルスに感染していることをユーザーに気づかせないまま、ひそかに活動を続けます。たとえば「キーロガー」と呼ばれるものは、ユーザーが入力したキーボードのボタンをすべて記録して、その履歴から ID やパスワードを検出し、不正に詐取する恐ろしいウィルスです。

**・対応法**

感染経路や不正活動、症状が多種多様になっています。ウェブサーフィンをしているだけでも、ウィルスに冒される危険があるわけですから、ユーザーが自分で気をつけるには限界があります。**ウィルス対策ソフトを導入することが、一番の防衛策**です。逆にいえば、ウィルス対策ソフトが入っていないパソコンはかなり危険だといえます。

そして、ウィルス対策ソフトが常に最新の状態に保たれるよう、自動アップデート機能などは有効にしておきましょう。最新の状態を維持しないと、せっかくウィルス対策ソフトを導入していても、日々現れる新種のウィルスに対応できず、被害を受ける可能性があります。

また、ウィルス対策ソフトは万能ではありません。新種のウィルスに対応するまでに時間を要する場合もあります。少しでもウィルスに感染するリスクを減らすために、怪しいサイトを閲覧したり、不審なファイルを開いたりしないよう、普段から気をつけましょう。

## （2）ネット詐欺

**・フィッシング詐欺**

利用者を本物そっくりの偽物サイトに誘導し、アカウント（ユーザーID・パスワード）を盗み取り、悪用するものです。銀行のオンラインサービスのアカウントや暗証番号を盗まれ、預金を不正に引き出されるなどの被害を受けるケースがあります。ブラウザの URL を確認することが有効な防御策とされてきましたが、最近では URL 欄を偽装する手口も確認されているため、ウィルス対策ソフトに含まれる「フィッシング詐欺防止機能」等で対策を講じる必要もあるでしょう。

**・ワンクリック詐欺**

ワンクリック詐欺とは、アダルトサイトや出会い系サイトに張られたリンク、送られてきた電子メールの URL をクリックすると、「入会ありがとうございます」、「登録が完了しました」等、一方的に契約したようなメッセージが表示され、「サービス利用料」などと称して不当に料金を請求されることをいいます。法律に則った正しい手続きがないかぎり契約は成立しませんので、料金を支払う必要はありません。表示されている連絡先に確認の連絡をしてしまうと、新たな詐欺被害につながることもあります。どうしても不安な場合は、みだりに行動せず、まずは大学や行政機関（国民生活センターや消費生活センター）に相談してください。

**・インターネットオークション詐欺**

インターネットオークションで商品を落札し、出品者に支払いをしたにもかかわらず、商品が送られてこないなどの被害が発生しています。出品者の過去の評価に問題がある場合や、商品説明があいまいだったり、画像が実物ではなくメーカーサイトのイメージ画像の流用だったりする場合は、その商品（特に高価なもの）には入札しない、というような心がけが必要です。出品者が過去の評価をねつ造している可能性もあるので、入札は慎重に行うようにしましょう。

**・チェーンメール・デマ情報**

チェーンメールと呼ばれる、いわゆる「不幸の手紙」のようなメールが出回ることがあります。チェーンメールには「このメールを受信したら 10 人の人に転送してください」といった文言が含まれています。このようなメールを受信しても、転送してはいけません。ネットワーク回線に不必要な負荷をかけるばかりか、風説の流布にもつながりかねません。携帯電話のメールでも同様のものが出回ることがあります。受け取った場合はそのまま破棄しましょう。

デマ情報も同様です。「○○というコンピューターウィルスが出回っています。パソコン内の○○というファイルがあったらそれはウィルスです。すぐに削除しましょう」といった内容のチェーンメールが出回ります。実際には「うそ」の情報であることがほとんどです。「○○というファイル」が重要なシステムファイルであり、鵜呑みにして削除するとパソコンが起動しなくなる、など悪質ない

たずらであることもあります。ウィルスやセキュリティに関する情報は、専門のベンダなどの信頼性の高い情報源から得るようにしましょう。

### ※ SSL 通信で自分の個人情報を盗聴から守ろう

ネットショッピングやチケット予約、会員制サイトなどの各種オンラインサービスを利用する際、ユーザーID やパスワード、自分の住所、氏名、電話番号などの個人情報をインターネット経由で送信することがあります。このとき通常の通信方法で送信すると、データが送信先に到着するまでの間に、盗聴されたり改ざんされたりする可能性があります。個人情報を送受信する場合、これらの被害を防ぐために、「SSL 通信」を利用するのが一般的です。SSL は、公開鍵暗号や共通鍵暗号（秘密鍵暗号)、デジタル証明書、ハッシュ関数などの技術を用い、データを暗号化して盗聴を防ぐほか、改ざんやなりすましを検出することができるセキュリティ技術です。

利用中のウェブサイトが SSL 通信に対応している場合、ブラウザのアドレス欄右側など、どこかに「鍵」のマークが表示されます。個人情報を送信するときには確認しておきましょう。

## さいごに・・・登録までの流れ

この講習会の終了時に、誓約書・MIND 利用講習会出席票を回収します。これをもとに講習会の受講登録処理を行います。処理には数日間かかります。なお、この登録処理の完了と同時に利用可能となるサービスは以下のとおりです。

・大学内のコンピューターからインターネットへのアクセス
・MIND モバイル接続サービス（VPN 接続/無線 LAN 接続/モバイル情報コンセント接続）
・図書館オンラインサービス（外部データベース/電子ジャーナル）

## 参考資料

**・「MIND リーフレット」**
明治大学の主な情報サービスやアカウントの種類、問い合わせ先などをご案内しています。

**・「ソーシャルメディアガイドライン」**
ソーシャルメディアを利用する際の考え方や留意点をまとめたガイドラインです。

いずれも、MIND ホームページから確認できます。

http://www.meiji.ac.jp/mind/