情報倫理と情報セキュリティ

はじめに

■情報倫理とは、

ネット社会での適正な考え方、ルールやマナーを守った**適切な行動の規範**のことです。

順守しなければならないインターネットに関係する規約やガイドライン、さらには、罰則のある法律もありますので十分注意してください。

■情報セキュリティとは、

インターネットを利用する際に注意する**危機管理対策**（リスクマネージメント）のことです。

自分が被害者になる場合だけでなく、犯罪者に利用されることにより、意図せず加害者になってしまうケースもあります。

十分な知識を身に付けて、適切な対策・対応を心がけてください。

■Contents■

1. 情報を発信する際の注意

1-1. 個人情報を安易に公開しない

1-2. 発言や投稿は慎重にする

2. 情報を利用する際の注意

2-1. 著作権・肖像権に注意する

3. セキュリティ対策

3-1. 脆弱性対策

3-2. ウイルス感染対策

3-3. 不正アクセス対策

3-4. 初期設定の見直し

3-5. 脅威の手口を知る

※本マニュアルは情報の要約です。 詳細は、各ページ内のアンダーライン部分をクリックして、各サイトの内容を閲覧してください。

Copyright © Meiji Gakuin University All Rights Reserved.

■本学における規則・注意事項■

※各リンク先を開き、必ず読んでください

▼PCとネットワークにおける規則や手引き

◆情報センターHP掲載事項

- 明治学院大学 情報ネットワーク規程
- 明治学院大学 情報ネットワーク研究・教育利用細則
- 情報センターオリエンテーション（動画）
- 明治学院大学 コンピュータ・ネットワーク 利用の手引き

▼ソーシャルメディアに関する注意事項

◆「ソーシャルメディアについて」HP掲載事項

- ソーシャルメディアの利用に関するガイドライン
- ソーシャルメディアアカウント利用要綱
- 明学生が考えた SNSのための５つの合言葉

・本ガイドラインに関するお問い合わせ：広報課
・SNS等で、トラブルに巻き込まれたら：学生部

明学生が考えた SNSのための **５つの合言葉** ～再考で最高のSNSライフに～

みんな見てる、
オレのプライベート!?

友だちは、フリー素材じゃありません。

みんな！ オレの
勇姿を見てくれ！

その個性の出し方、間違っていませんか？

騙されるわけないじゃん。
もう大学生だぜ？

デマの中継所にならないでっ！

起きて『既読』、お昼『なう』、
寝る前『いいね！』、
それが私の日常

昨日、SNSで何を見たか、思い出せますか？

ちょっと見るだけだから
だいじょうぶ！

歩きスマホは、歩く武器。

(2014年度学生広報委員制作)

Copyright © Meiji Gakuin University All Rights Reserved.

1．情報を発信する際の注意

■個人情報とは、

◆個人情報保護委員会HPより

氏名、顔写真、住所、生年月日、家族構成など、単一およびそれらの組み合わせにより、
【個人を特定できる情報】のことです。

■個人情報保護法の５つの基本チェック

① **取　得　：　無断で取得しない**

・利用目的を特定して、本人にわかるように取得してください。

② **利　用　：　流用しない**

・取得時に特定した利用目的の範囲内でのみ利用してください。

③ **保　管　：　漏洩・紛失しない**

・USBメモリーに入れたデータなど、紛失しないように安全に管理してください。

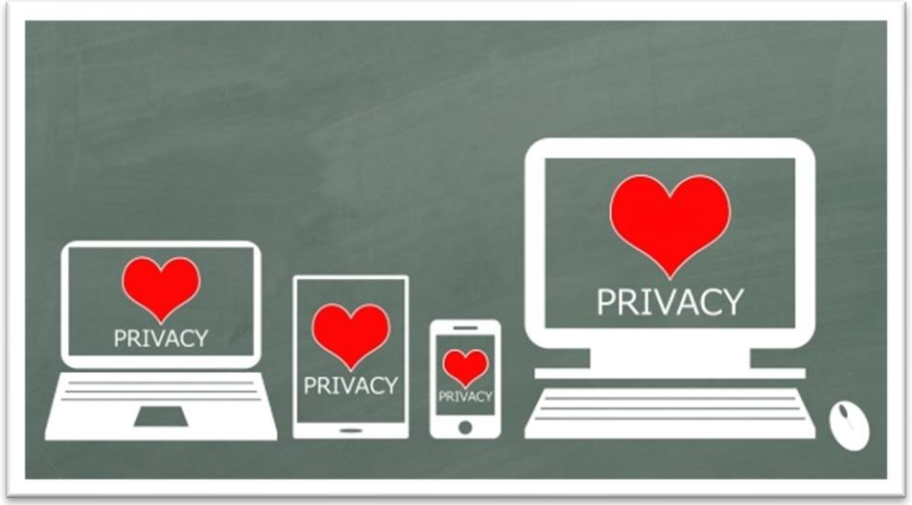
・クラウドに保管する際には、パスワードをかけ、公開条件に注意してください。

④ **提　供　：　他人に提供しない**

・第三者に提供する場合は、本人の了解を得てから提供してください。

⑤ **対　応　：　要求に対応する**

・本人からの開示・訂正・利用停止等の申し出があった際は、
迅速に対応してください。



Copyright © Meiji Gakuin University All Rights Reserved.

1． 情報を発信する際の注意

1-1. 自分や知人の個人情報を安易に公開しない

1-2. 相手が不快に思うような発言はしない

◆警視庁「情報セキュリティ広場」
◆「守っていますか？ルールとマナー」より

- ネット上で、円滑な活動を行うには、現実社会と同じマナーを守ることが大切です。
- ネット上に情報を公開するときに、それによって生じるリスク・社会的責任、法的責任を負うことは、現実社会以上に深刻になる場合があります。 安易な情報発信が、他人に不快な思いをさせたり、思わぬところで加害者や被害者になってしまうおそれもあります。

■インターネット利用　７か条

1. インターネット社会でも、実生活と同じルールとマナーを守る
2. 他人のプライバシーを尊重する
3. 住所・氏名などの個人情報を入力する時は、十分注意する
4. ID・パスワードの管理を徹底する
5. 他人のミスを大げさに指摘しない
6. メールを送る前に、内容をよく確認する
7. 面と向かって言えないことは書かない

慎重な情報発信を心がけてください

Copyright © Meiji Gakuin University All Rights Reserved.

2．情報を利用する際の注意

■著作権とは、

作品を創作した者が有する権利で、**知的財産権**の一種です。

◆文化庁HP「著作権」より

◆著作権情報センターHPより

2-1.著作権、肖像権に注意する

- ネット上に公開されている文章や画像を、そのままコピーして自分のレポートに利用すると、**【著作権法】**に抵触するおそれがあります。
  レポート等に引用する際には、正しい著作物引用方法のルールを守ってください。 ※１参照
- 漫画、小説、写真、論文などが違法にアップロードされたコンテンツ（海賊版）と知りながらダウンロードすることは違法です。※２参照
- インターネット経由でコンテンツを共有する際にもルールがあります。 ※３参照
  授業でコンテンツを利用する際には、特例ルールがあります。範囲内で利用してください。
- 出版された著作物・配布物や、インターネット経由で取得した授業の動画や資料などにも著作権があります。Webサイトにアップする、SNSに投稿する、友人にコピーを譲渡するなど、不適切な再配布をしないよう注意してください。
- 人物の背景に小さく映り込んだポスターは著作権侵害になりませんが、映画のポスターなどをメインに撮影してSNSに掲載するのは違法になります。

Copyright © Meiji Gakuin University All Rights Reserved.

2．情報を利用する際の注意

■著作権に関する情報

詳細は、下記の【各機関のホームページ】にて確認してください。

※2021年1月に著作権法が改正されました。

※１ 「著作権」 ◆文化庁

※２ 「侵害コンテンツのダウンロード違法化」について（政府広報オンライン）

「ちょっと待って！そのダウンロード、違法かも？」（リーフレット）
「著作権広報大使」ハローキティの【大切にしようね著作権！】」（YouTube）
「海賊版はキライ！byハローキティ」（YouTube）

※3 「学校における教育活動と著作権」
「学校教育と著作権」 「著作権テキスト」

もっと詳しく CRIC公益社団法人著作権情報センター
「みんなのための著作権教室」「青少年向けの著作権関連ウェブサイト」

インターネットからの情報は、ルールを守って利用してください

※1 著作物の正しい引用方法

① 公表された著作物からの引用であること
② 引用を行う必然性があること
③ 自分の文章と引用との違いが明確に区別できる表現であること
④ 自分の文章がメインで、引用は参考程度であること
⑤ 出典を明記すること

Copyright © Meiji Gakuin University All Rights Reserved.

3．セキュリティ対策

■情報セキュリティとは、

パソコンやスマートフォンは単なる電子機器ではなく、大学生活に欠かせない重要なアイテムですが、保存されている情報が盗まれてしまったり、勝手に変更されてしまうことで、自分や関係者が犯罪や被害にあうことがあります。

また、ウィルスに感染した自分のパソコンが犯罪者に乗っ取られ、第三者への攻撃の中継点とされて、自分が加害者になってしまうといったケースも多発しています。

ネット詐欺やサイバー攻撃の手口は、時とともに変化していきます。しかし、情報セキュリティ対策の基本は、大きく変わるものではありません。 基本対策でしっかりガードして、安全にインターネットを利用しましょう。

■基本のポイント

3-1.　脆弱性対策
3-2.　ウイルス感染対策
3-3.　不正アクセス対策
3-4.　初期設定の見直し
3-5.　脅威の手口を知る

■詳しく学びたい方は、

こちらのテキストを参照してください。

内閣サイバーセキュリティセンター発行

【インターネットの安全・安心ハンドブック】
（PDF:23MB）

英語版 English version（2017）

Copyright © Meiji Gakuin University All Rights Reserved.

3．セキュリティ対策

■情報セキュリティ対策の基本

3-1．脆弱性対策 【アップデート】

「**OSやソフトウェアは、常に最新の状態に！**」（YouTube）

- パソコンやスマートフォンのOS、ソフトウェア、アプリは、いつも最新のバージョンにしておきましょう。※1
- 古いままにしておくと、セキュリティに弱点（脆弱性）がある状態になってしまい、とても危険です。
- 最新のバージョンにアップデートをすると、脆弱性を悪用する攻撃への守りが強くなります。
- アップデートは、パソコンやスマートフォンだけではなく、ネットワークにつながるすべての機器に必要です。（ルーターやネットワークカメラ、スマートスピーカーなど、様々な機器についてもお忘れなく！）

◆参考ページ

●インターネット接続機器のセキュリティ対策について
家庭教師が教えるネット家電セキュリティ対策！（YouTube）

※1 OSのバージョンをアップグレードする際の注意！

アップデートではなく、バージョン名が変更になる大きな変更「アップグレード」をする際には、セキュリティソフトなどが対応しているかどうかを、本学のHPにて確認してから行ってください。

●例： Windows 10 → Windows 11
macOS Big Sur → macOS Monterey

●アップグレード手順 ：Windows / Mac

●確認は、「情報センター」(こちら)から

Copyright © Meiji Gakuin University All Rights Reserved.

3．セキュリティ対策

個人のパソコン・スマートフォンには、必ずセキュリティ対策を！
本学では、セキュリティソフト【**ESET**】のライセンス契約をしています。 学生・教職員は、無償で利用することができます。 詳細は、「**ウィルス対策ソフト無償貸与サービスについて**」から

3-2．ウイルス感染対策

「ウイルスへの対策意識を持ちましょう」（YouTube）

- パソコンには、ウイルス対策ソフトを入れましょう。ウイルスに感染しにくくなります。常にアップデートも忘れずに！
- パソコンやスマホがウイルスに感染したり、不正アプリをインストールしたりすると、お金や情報を盗まれてしまいます。
  感染に気づかずに、乗っ取られた状態のままパソコンを使用し続けると、被害が増大してしまいます。
- アプリは、原則として公式ストアから入手しましょう。不正アプリの被害にあいにくくなります。
- メールの添付ファイルやリンク（URL）にウィルスが潜んでいるかもしれません。慎重に本物かどうか確かめましょう。

◆参考ページ

●パソコンのウイルスについて

ウイルスはあなたのビジネスもプライベートも狙っている！（YouTube）

●スマートフォンのウイルスについて

スマホがウイルスに感染!? 不安に思ったら試したい5つの方法

あなたのスマートフォン、ウイルスが狙っている！（YouTube）

Copyright © Meiji Gakuin University All Rights Reserved.

3-3．不正アクセス対策

1）パスワードの設定について

「パスワードは長く、複雑に、使いまわさない」（YouTube）

- 短いパスワードや、誕生日や名前、電話番号、辞書にある単語、「1234」など単純なパスワードでは、簡単に推測や解析をされてしまいます。
- 同じパスワードを複数のサービスで使うと、ハッキングされてしまった時に、ほかのサービスにも不正にログインされることがあります。
- パスワードは他人に教えないで大切に保管しましょう。

パスワードのチェックポイント

◆チョコっとプラスパスワードより

- □ 8文字以上の文字数で構成している
- □ 数字や、記号も混在している
- □ アルファベットに大文字と小文字を混在している
- □ サービスごとに違うパスワードを設定している

2）Wi-Fi の利用について

「Wi-Fi利用者向け簡易マニュアル」（リーフレット）

- 接続するアクセスポイントをよく確認し、信頼性のないWi-Fiの利用は避けましょう。偽のアクセスポイントに騙されないよう、メールアドレスやID・パスワードの入力も慎重に！
- 正しいURLでHTTPS通信をしているか確認しましょう。
- 自宅に設置しているWi-Fiルーターなどのネットワーク機器の設定を確認しましょう

◆参考ページ

- 自宅のWi-Fi環境で押さえておきたいセキュリティ対策
- 野外でWi-Fi接続をする時のセキュリティの基礎知識

Copyright © Meiji Gakuin University All Rights Reserved.

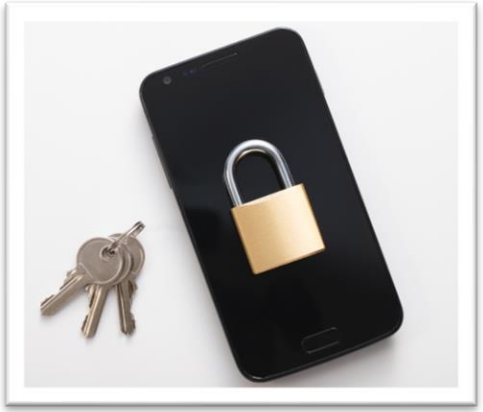
3-4．初期設定の見直し

「スマホを買ったら画面ロックを設定しましょう」（YouTube）

- 新しくパソコンやスマホなどの電子機器を買ったり、ソフトウェアやアプリを入れたりしたときは、初期設定から変更してセキュリティを高めましょう。初期設定では、セキュリティが弱かったり、データ共有などの思ってもみない機能がオンになっていたりします。
- 初期パスワードを変更し、生体認証などで画面ロックを設定することで、セキュリティを強化できます。
- データ共有など、情報を渡したり連携させたりする機能の設定を確かめておくことで、予想外のトラブルを防ぐことができます。
- 複数の人たちと機器を共有するときは、アカウント（ログインID）をわけましょう。
- ルーターやネットワークカメラなどのID、パスワードは、必ず出荷時設定から変更しましょう。

◆参考ページ

- 他者が勝手に操作できないようスマートフォンには必ず画面ロックの設定を
- スマホをなくした！というときに取るべき行動とは？
- LINEアカウントを乗っ取られないためにできること



Copyright © Meiji Gakuin University All Rights Reserved.

3-5. 脅威の手口を知る

「常に最新の手口を知っておきましょう」（YouTube）

- ネット詐欺やサイバー攻撃などの、最新の手口を知っておきましょう。
- インターネット上の罠は、テクニックがますます巧妙に、そして多様に変化しながら、あなたの心のスキをつこうと企んでいます。 流行している手口を前もって知って、備えておけば、被害にあう可能性を低くできます。
- 相談できる人や相談窓口を確かめておくこともおすすめです。

◆参考ページ

- NISC「サイバーセキュリティ・ポータルサイト」
- IPA「情報セキュリティ安心相談窓口」
- Canon「サイバーセキュリティー情報局」

■マルウェア

悪意のある（malicious）ソフトウェア（software）を合わせた造語。感染対象に対して有害な作用をもたらすことを目的に作成されたソフトウェアの総称。

■踏み台

サイバー攻撃者が、関係のない第三者のコンピューターやサーバーを乗っ取り、攻撃の拠点として利用すること。

■DDoS攻撃

複数の端末から標的となる通信機器や端末に対して大量の通信を行い、サービスを妨害する攻撃の一種。

マルウェアに感染して乗っ取られたコンピューターを「踏み台」として利用し、それら多数の端末から一斉に標的を攻撃するケースも増えている。その場合、踏み台にされた機器は、所有者の知らぬ間に攻撃に悪用され、結果的にDDoS攻撃に加担してしまうケースも少なくない。

◆サイバーセキュリティ情報局「キーワード辞典」より

Copyright © Meiji Gakuin University All Rights Reserved.

3．セキュリティ対策

情報セキュリティ対策のPOINT！

1．OS やソフトウェアは、常に最新の状態にしておこう

新たに広まるコンピュータウイルスに対抗するため、製造元から無料で配布される最新の更新プログラムにアップデートしましょう。

2．パスワードは貴重品のように管理しよう

パスワードは自宅の鍵と同じく大切です。パスワードは他人に知られないように、メモをするなら人目に触れない場所に保管しましょう。

3．ID・パスワードは、他人に絶対教えない

金融機関を名乗り、銀行口座番号や暗証番号、ログインIDやパスワード、クレジットカード情報の入力を促すような、身に覚えのないメールが届いた場合、入力せず無視しましょう。

4．身に覚えのない添付ファイルは開かない

身に覚えのない電子メールにはコンピュータウイルスが潜んでいる可能性があります。添付されたファイルを開いたり、URL（リンク先）をクリックしないようにしましょう。

5．ウイルス対策ソフトを導入しよう

パソコンはもちろん、スマートフォンやタブレットにもウイルス対策ソフトをインストールしましょう。ウイルス定義ファイルのアップデートも忘れずに。

6．ネットでは信頼できるお店を選ぼう

ネットショッピングでは、詐欺などの被害に遭わないように信頼できるお店を選びましょう。身近な人からお勧めのお店を教わるのも安心です。

アプリのダウンロードも信頼できるサイトから行いましょう。

7．大切な情報はバックアップしておこう

思い出の写真や様々な記録など、大切な情報がパソコンの初期化や故障によって失われることのないよう、別のハードディスクなどに複製しておきましょう。

8．外出先では紛失・盗難・ネットワークに注意しよう

大切な情報を保存したパソコン、スマートフォンなどを自宅から持ち出すときは機器やファイルにパスワードを設定し、なくしたり盗まれないように注意して持ち歩きましょう。

市中のWi-Fiに接続するときも十分注意しましょう。

9．困ったときはひとりで悩まず まず相談

架空請求のメールが届く。ウイルスに感染した。などの被害に遭遇したら、ひとりで悩まず各種相談窓口に相談しましょう。

Copyright © Meiji Gakuin University All Rights Reserved.

引用、出典、参考資料一覧

◆文化庁
「著作権」

◆政府広報オンライン
「侵害コンテンツのダウンロード違法化」について

◆CRIC【公益社団法人著作権情報センター】
「みんなのための著作権教室」
「青少年向けの著作権関連ウェブサイト」

◆PPC【個人情報保護委員会】

◆警視庁サイバーセキュリティ対策本部
「情報セキュリティ広場」
「サイバーセキュリティー対策」（YouTube）
「サイバーセキュリティーについて」（YouTube）

◆警察庁サイバー犯罪対策プロジェクト
「インターネット安全・安心相談」
「鷹の爪団のサイバー犯罪撲滅大作戦」（動画）

◆JCCA【日本クレジット協会】
「ID・パスワード～使いまわし絶対ダメ！」(YouTube)

◆Canon【サイバーセキュリティ情報局】
「キーワード辞典」

Canon | ESET SPECIAL SITE
キヤノンMJがお届けする安全なデジタル活用のためのセキュリティ情報
サイバーセキュリティ情報局

◆NISC【内閣サイバーセキュリティセンター】
「インターネットの安全・安心ハンドブック」
twitter: https://twitter.com/nisc_forecast

NISC 内閣サイバーセキュリティセンター 注意警戒情報

◆IPA【情報処理推進機構】
情報セキュリティ
情報セキュリティ普及啓発映像コンテンツ (YouTube)
twitter: https://twitter.com/IPA_anshin

IPA 情報セキュリティ安心相談窓口

【情報倫理と情報セキュリティ】 明治学院大学情報センター
2022年1月 Ver. 1.1作成

Copyright © Meiji Gakuin University All Rights Reserved.