日本福祉大学　ICT サポートデスク

情報倫理ガイドライン

ネットワーク社会のルールとマナー

Nihon Fukushi University
ICT Support Desk

2019/04/01　ver.7

はじめに

情報機器やインターネットの普及により、パソコンやスマートフォンから、世界中の様々な情報にアクセスしたり、自ら情報発信することが可能になりました。また、SNS やオンラインゲームなどで、現実社会とは違うコミュニケーションが行われています。

便利になる一方で、情報漏えいや不正アクセス、ネット上の誹謗中傷や著作権法違反など様々な事件・事故が発生しています。

このような事件・事故の当事者とならないために、情報を扱う上でのルールやマナーを身に付けておかねばなりません。

本学では、「情報セキュリティの基本ポリシー」を定め、学内の情報セキュリティを維持・管理するための仕組みやルールの整備を進めてきました。この取組みが第三者機関にも評価され、国際規格（ISO27001）に基づく認証を取得しています(2018 年 4 月 1 日現在)。

本ガイドラインは、学内の情報セキュリティを維持・管理するための仕組み・ルール整備の一環として作成しました。内容を十分に理解し、日々の学習や就職活動などで情報機器やインターネットを活用してください。

インターネットの光と影

インターネット上では個人が自由に情報発信、または収集することが可能ですが、多様な形で発信される情報の中には、高い信頼性を備えた情報、信頼性に乏しい情報、誤った情報や、内容が古くなった情報など、様々な情報が混在しています（情報の価値基準は個人ごとに異なります）。

こうした情報の中から、①自分の必要とする情報を迅速に探し当て、②正しい情報を的確に選別し、③それを実際に活用する能力を身に付けてこそ、インターネットを価値あるデータベースとして利用することが可能になります。

情報を取捨選択する能力を養うとともに、不審な Web サイトや不審なメールは無視する、安易にクレジットカード番号など個人情報は入力しないなどの自己防衛が大切です。

アカウントの管理は慎重に!!

入学(編転入)・入職時に付与されるアカウント(ID とパスワード)は、本学の情報システムを利用する時のみ使用するようにしてください。プライベートで利用するサービス(SNS、ネット通販など)で同じ ID とパスワードを使用すると、学外のサービスで情報漏えいが発生した際に、漏えいした ID とパスワードを利用して本学の情報システムに不正アクセスされるリスクが高まります。

パスワードは、利用者本人であることを証明するための文字列です。自分に付与されたアカウント(ID とパスワード)を人に貸さないのはもちろんですが、パスワードを他人と共有したり、安易に人に教えないよう十分に注意してください。

パスワードの設定条件

① 文字数:8 文字以上 32 文字以内
② 文字種:半角の英文字／数字／記号(特殊文字)から二種類以上
③ 使用可能な文字:A-Z、a-z、0-9、! @ # $ % ^ & * + - _ =
④ 同じ文字の繰り返しやわかりやすい並びの文字列は使用しない
⑤ 他者が推測可能な文字列(例:ID、氏名、電話番号、誕生日など)は使用しない
※ID と同じ文字列、若しくは逆の文字列を含む文字列は設定できません。
⑥ 他のシステムと同じパスワードは使用しない

Q. 自分に付与されたIDとパスワードを友人に貸与しました。どうなりますか？
A. 本学の規程では、ID の貸し借りを禁止しています。そのため、ID の利用停止処分となることがあります。なお、ID を使用した友人が、利用中何らかのトラブルを引き起こした、あるいは巻き込まれた場合、貸与した者の責任も問われることになります。

不正アクセス行為は禁止されています

不正アクセスとは、正規の利用権限を持たない者が情報資源にアクセスする行為を指します。例えば、他人の ID・パスワードの盗用やセキュリティーホール(プログラムの欠陥)を悪用した情報資源へのアクセスが該当します。平成 12 年に「不正アクセス禁止法」が制定され、これに違反した場合には罰則規定が設けられており、法令に従って処罰されます。

マルウェア（ウイルス・スパイウェアなど）に注意しましょう

マルウェアとは、ウイルスやスパイウェアなど、コンピュータに感染し、寄生して「悪さ」をする「悪意あるソフトウェア」の総称です。

ウイルスの最も大きな特徴は、この「悪さ」をするプログラムが「感染」するということです。自分自身だけではなく、周囲の人にもウイルスの影響が及ぶ可能性があることを覚えておきましょう。

スパイウェアは、利用者の個人情報やアクセス履歴などの情報を収集します。ウィンドウなどを表示せずに動作するため、すぐには気づかない場合が多いことが特徴です。スパイウェアのうち、キーボード入力を監視し入力情報（パスワードなど）を取得するものを、キーロガーといいます。これらに感染した場合、クレジットカードや銀行口座などを不正に利用される恐れがあります。

マルウェアに感染しないために（対策）

① パソコンにウイルス対策ソフトを導入し、定義ファイルを定期的に更新する。
② OS やソフトウェアのセキュリティアップデートが公開された際は、更新を行い常に最新の状態を保つ。（特別な事情が無い限り自動更新にすることを推奨）
③ インターネットカフェなどでパソコンを利用する場合は、個人情報を入力しない。
④ 心当たりの無い送信者や、不審な件名のメールは閲覧せずに削除する。
⑤ インターネット上で公開されているソフトやデータは、不用意にダウンロードしない。
⑥ メールに添付されたファイルは、例え知人からであっても不用意に開かない。
⑦ 万が一感染した場合に備え、重要な情報は定期的にバックアップを取る。

携帯情報端末からの情報流出に注意しましょう

スマートフォン、タブレット PC などの携帯情報端末は、パソコンと同様に多くの情報を取り扱うことができます。例えば、スマートフォンに含まれる情報には、以下のようなものがあげられます。

1) 自分自身の電話番号、メールアドレス、指紋などの個人情報
2) カメラで撮影した写真や動画
3) 登録した連絡先や発着信履歴、送受信したメール
4) 各サービスのアカウント（ID・パスワード）やインターネットの閲覧記録
5) 位置情報（GPS 機能を ON にしている場合）
6) その他、スマートフォンにダウンロードしたファイル・データなど

これらの情報を、より手軽に持ち運びできることから、紛失・盗難による情報流出が問題となっています。また、パソコンと同様にマルウェア感染する危険があるため、携帯情報端末には紛失・盗難対策とともに、マルウェア対策を行うようにしてください。

携帯情報端末のセキュリティ対策

① 画面ロックを有効にする（パターン、パスコード、PIN、指紋登録等）
Andoroid：パターン、PIN、パスワード、指紋認証等
iOS：パスコード、指紋認証、顔認証等
※端末がロックされていても SD カードは抜き取り可能なため、SD カードには個人情報を保存しないよう留意する。

② 端末を探す機能を有効にする（紛失時にリモートから端末ロックやデータ消去が可能）

③ サービス利用での対策
クラウドサービスなどを利用する場合は、サービスの利用規約や、通信が暗号化されている事を確認すると共に、ID（アカウント）・パスワードを厳重に管理する。

④ 設置元が不明な無線 LAN のアクセスポイント接続への対策
誰が、またはどのような業者が設置したか分からない無線 LAN のアクセスポイントには接続しない。

著作権を守りましょう

著作権制度とは「他人の著作物を利用する際には、著作権者の了解を得てください」という制度で、著作物を保護することにより、創作者を含めた著作権保持者の経済的・人格的利益を確保し、創作活動に対するインセンティブ（動機付け）を与えようとするものです。

最近の情報技術の革新により、音楽・静止画・動画・ソフトウェアなどのデジタル情報を劣化させることなくコピーすることが可能となり、インターネットの急激な普及とあいまって、著作権の保護が重要なテーマとなっています。著作権法に違反した場合、法令に従って処罰されるとともに、損害賠償などの訴訟を起こされる場合があります。違法と知りつつ著作物をコピーするなどの行為は、絶対にしてはいけません。具体的には、以下のような例があります。

1) 文章、画像、動画、音楽、コンピュータプログラムなどを無断で転載すること。
2) スキャナなどを使って、データ化した書籍や雑誌の情報を無断で掲載すること。
3) コンピュータソフトウェアを無断でコピー（複製）すること。

レポートなどに利用する場合は、引用（部分掲載）にとどめ、出典元（掲載の元となった資料の出所（本のタイトルや Web サイトのアドレスなど）を参考文献として掲載するようにしてください。

ソーシャルメディアを利用する際の一般的な注意事項

ソーシャルメディア（SNS、動画共有、電子掲示板、ブログなど）は、多様なコミュニケーションのツールとして大変便利ですが、一方で多くのリスクが潜んでいます。利用にあたっては、ツールの特性をよく理解し、思わぬトラブルに巻き込まれないよう、あるいは当事者とならないよう、以下の事項を守って利用してください。

1. **規程・規約を遵守すること**

   本学の諸規程に反する行為は慎んでください。また、学外のサービスを利用する際は、各サービスの利用規約をよく確認するよう努めてください。

2. **個人情報・プライバシー情報の保護**

   自分自身の個人情報を登録・公開する際は、事前に利用するサービスの特性や公開範囲をよく確認してください。他人の個人情報を本人に無断で公開してはいけません。

   一度インターネット上に発信した情報は、本人が削除しても、第三者によりコピー・保存され、半永久的に利用される恐れがありますので十分に注意してください。

3. **情報発信は正確かつ慎重に**

   発信する情報は正確かつ最新のものであるよう留意してください。単なる噂やチェーンメールなどの不確実な情報、嘘や不適切な行為を扇動する情報を発信してはいけません。誤解を招かない表現に努め、万が一、誤りや誤解などが生じた場合には、速やかに訂正しましょう。

4. **知的財産権を侵害しない**

   著作権・肖像権・商標権・特許権などの権利を侵害してはいけません。

   （例）

   - お気に入りのキャラクターの画像を無断で自分のブログに転載する行為は、著作権法違反です。
   - 本人に無断で写真や動画を撮ったり SNS で公開する行為は、肖像権の侵害になります。

5. **誠実で責任ある行動を**

   自分の発言・投稿には自分で責任を持ちましょう。一般的なモラルやマナーを守り、円滑なコミュニケーションに努めてください。

6. **トラブルには冷静に**

   対面ではないコミュニケーションは、しばしば誤解から思わぬトラブルに繋がることがあります。自分だけで解決できないようであれば、第三者に相談しましょう。また、自分に非があった場合には、相手を無視せず誠心誠意対応してください。

2001 年 4 月　第 1 版発行
2004 年 4 月　第 2 版発行
2005 年 4 月　第 3 版発行
2007 年 4 月　第 4 版発行
2011 年 4 月　第 5 版発行
2013 年 4 月　第 6 版発行
2019 年 4 月　第 7 版発行

編者　　日本福祉大学 総務課（ICT 推進室）
発行　　日本福祉大学 総務課（ICT 推進室）
〒470-3295 愛知県知多郡美浜町奥田
URL: https://www.n-fukushi.ac.jp/mec/

日本福祉大学 ICT サポートデスク