# 学生のみなさんへ


# 情報セキュリティ ハンドブック

## ～情報セキュリティ事件・事故の被害者・加害者にならないために～

発行：法政大学市ヶ谷情報センター
発行日：2023 年4 月

# パソコンやスマホ、携帯電話などを使う時は…

## ユーザIDとパスワードを正しく管理しよう


- たとえ家族や友人であってもユーザ ID やパスワードを貸したり共有したりしない
- 複数のサービスでユーザ ID・パスワードを使いまわさない
- プロフィールなどの個人情報から推測されやすいパスワードを使用しない
- より安全なパスワードにするため、英大文字・英小文字・数字・記号を複数組み合わせる
- ネットカフェなど、不特定多数が利用するパソコンや、セキュリティの設定がしっかり行われているかどうかが不明なパソコンでは、極力パスワードを入力しない

## 万が一の紛失や盗難に備えよう

- 起動時や自動スクリーンロックのパスワードを設定する
- 重要なデータはバックアップを取っておく
- 遠隔操作による強制ロックや強制消去、位置情報確認サービスなどを利用する

## 情報を大切に扱おう

- 使用中のパソコンから離れるときは、ロックやログオフ、シャットダウンなどを使い分け、自分以外の人に使用させない
- 資料、パソコンなどの端末、USB メモリや CD-R などの記憶メディアは責任をもって管理する
  ※置き忘れや放置をせず、盗難の危険に晒さないよう肌身離さず持ち歩きましょう。
- 個人情報など重要なデータは、パスワードロックをかけられる保存メディアを利用する
- 資料や、CD-R、USB メモリなどの電子記憶媒体を廃棄する場合は、シュレッダーやデータ消去ソフトを使用する
- 貸出端末を返却する際は、内部にデータが残っていないか、バッグに USB メモリや CD-R 等が残っていないか確認する
- 大学から付与された個人用記憶領域（G ドライブ）も適宜活用する
  ※G ドライブに保存したファイルは、インターネット環境があれば学内の各学生用端末や自宅からでもアクセスできます。
  ※アクセス方法については市ヶ谷情報センターホームページを参照してください。

# 自分や仲間・家族の生活を守る

## ブログや掲示板、SNS（TwitterやFacebook、LINEなど）を楽しむ前に

インターネット上に公開した情報は、瞬く間に世界中へ拡散します。コピーが出回るなど取り返しがつかなくなる場合もあります。情報の公開範囲は慎重に選びましょう。

- 自分に繋がるような情報をむやみに公開しない
  ※匿名と思っていても、人間関係や過去の投稿、他サービスでの発言などを照合して本人を特定されることがあります。
- 有名人、他人・友人の情報や写真を許可なく公開しない
- 投稿内容、”いいね！”やタグの公開範囲設定をあらかじめ確認する
- 情報を鵜呑みにして拡散せず、出所を確認する
- 公序良俗に反する発言や他者への誹謗中傷、組織の機密事項などを投稿しない
- 不審なアプリを連携しない（連携する場合は承認画面の内容を確認する）

## 位置情報の公開に気をつけよう

デジカメやスマホで撮影した画像には、詳細な位置情報が記録されています（情報を見るためのソフトを使わないと見れません）。

写真に写りこんだ景色、プロフィールや発言内容、電車のダイヤなどの情報を集約することで、生活圏や自宅、個人をも特定される可能性があります。

- 位置情報を取得するアプリを使用する場合は、そのアプリを使う上で位置情報が本当に必要かを考え、むやみに取得や使用許可をしない

## オンライン授業受講に関する注意点

オンライン授業受講により、ネットワークの使用頻度が高くなります。オンライン授業で使用するパソコンやソフトウェアはアップデートを行い、常に最新の状態に保つようにしましょう。

## SNS の利用について

法政大学広報課が発行しているハンドブック「あなたの SNS の使い方、本当にそれで大丈夫？」もご活用ください。

# 怪しいサービスから身を守る

## コンピューターウイルスの感染を防ごう

コンピューターウイルスには、端末に不要なメッセージや画像を表示させる愉快犯的なものから、端末を使用できなくする、端末内の情報を盗んだり拡散させたりするような悪質なものまで様々です。まずは、1 人ひとりが感染しないよう心がけましょう。

- パソコン、スマートフォン、タブレットにはウイルス対策ソフトをインストールし、常に最新の状態を保つ
  ※記憶媒体ではない USB 機器にもウイルスが仕込まれていることがあります。挿入するだけで感染・拡散するため、ウイルス対策ソフトなどの防御策が必要です。
- OS やアプリ、ソフトウェアをアップデート ( 更新 ) し、常に最新の状態を保つ
- 配布者や作成者のわからないデータ、アプリなどをむやみにダウンロードしない
  ※アプリ本来の機能とは別に、情報を抜き取ったり遠隔操作をする機能を備えたアプリもあります。
- 心当たりのないメールの添付ファイルを開かない

## 悪意あるメールやサイトを見抜こう

企業や関係者から送信されたメールであるかのように見せかけたり、短縮 URL や偽装 URL で危険なサイトに誘導されたりすることもあります。不審なメールだと感じたら内容を鵜呑みにせず、リンク先が安全かどうか確認したり、相談したりしましょう。返信したり、リンク先にアクセスしないようにしましょう。

- 「ウイルスに感染しています！」などと危機感を煽るメッセージや、「続きが気になったらクリック！」といった誘惑にのらない
- 個人情報やカード情報を要求される場合（ネットショッピングなど）は、気軽に情報を提供せずプライバシー・ポリシーなどを確認する

## 無線 LAN（Wi-Fi）を安全に利用しよう

公衆無線 LAN の中には、通信内容の傍受や端末への攻撃を目的とした悪意あるアクセスポイントや、通信を盗聴されやすい ( セキュリティの低い ) アクセスポイントも存在します。ユーザ ID/ パスワードが不要なものや無料を謳ったもの、提供元の不明なものにはアクセスしないようにしましょう。また、そのようなアクセスポイントに自動的に接続しないよう本体側の設定も見直しましょう。

# ルールやマナーを守る

## メールを正しく使おう

- 間違った相手に送信しないよう確認する
- To.（宛先）と Cc. に入れたメールアドレスは受信者全員に見えてしまうので、用途によって Bcc. と使い分ける
- メールを送信する前に、内容が間違っていないか、その内容で相手が理解できるか確認する
- デマやチェーンメールを拡散しない

## 著作物の取り扱い方を学ぼう

音楽や映画、テレビ番組、画像、文章、ソフトウェアなどの著作物には様々な権利が係っています。

- 不正にコピーしたり、コピーしたものを配布・共有しない
- 不正にコピーされたものを入手しない

※ファイル共有を目的としたソフトやサービスは、不正コピー物配布やウイルス感染の温床となりやすいので特に注意が必要です。

- 論文やレポート作成時は引用のルールを守り、剽窃・盗用をしない

（参考）コンピュータソフトウェア著作権協会

https://www2.accsjp.or.jp/

## 情報セキュリティに関する情報

【セキュリティ最新情報の提供】
独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/

【サイバー犯罪の情報提供】
警察庁セキュリティポータルサイト@police
https://www.npa.go.jp/cyberpolice/

【セキュリティ注意喚起情報】
JPCERTコーディネーションセンター
https://www.jpcert.or.jp/

# 法政大学の情報倫理と取り組み

情報ネットワークは、生活になくてはならないものとなる一方で、個人情報など重要情報の漏えい事故・事件が多発しており、企業や国レベルの脅威（リスク）ということだけではなく、個人レベルの脅威として情報セキュリティへの注意と対策が必要となっています。

その対策には、情報倫理という概念（情報通信社会において、他人の権利との衝突を避けるために必要なマナーやモラル）を理解する必要があります。

法政大学の情報倫理は、法令順守と公序良俗を尊重し、著作権、特許及び商標等の知的財産権、名誉、信用及び肖像権、プライバシーに関する権利などの人格権を尊重し、これをみだりに侵害することなく本学の教育・研究活動にふさわしい品位を保ちながらその充実を図ることを目的としています。

法政大学では、この情報倫理の下に学生の皆さんや教職員のために安全で利用しやすいネットワーク環境を提供するとともに、安心して学内ネットワーク環境を利用できるよう「法政大学学術情報ネットワーク規程」を定めています。

これからも、全学的な情報管理の取り組みを検討し、実施することでセキュリティ対策を強化していきます。

法政大学の構成員は、コンピュータやネットワークの教育・研究利用において、学問の自由、思想・良心の自由、表現の自由をはじめとする基本的人権を最大限に尊重し、プライバシーの権利、個人情報、著作権等の知的財産権の保護にも努めましょう。

# 情報セキュリティ事件・事故に遭遇したら？

「使用しているパソコンがコンピューターウイルスに感染した」、「自分の ID やパスワードが悪用されている可能性がある」など、情報セキュリティの事件・事故が発生した、または発生した可能性がある場合は、速やかに市ヶ谷情報センターにご連絡ください。

## HOSEI-CSIRT
**（法政大学情報セキュリティインシデント対応チーム）**

csirt@ml.hosei.ac.jp

https://netsys.hosei.ac.jp/important/important20220421k01.html

## 市ヶ谷情報センター（ボアソナード・タワー4階）

TEL: 03-3264-9636　https://hic.ws.hosei.ac.jp/

**情報教育システム（パソコンやネットワーク）の使い方、各種規程はこちら**