情報セキュリティハンドブック

ITを使った、安全で楽しいキャンパスライフを送るために

法政大学

学校法人 法政大学　総合情報センター

ユーザーIDとパスワードは
不正に利用されないようにしましょう

□ 他人はもちろんのこと、家族や友人であってもユーザーIDやパスワードを教えたり、共有することは絶対にやめましょう。

□ 初期パスワードは速やかに変更し、強度の高い複雑なパスワード（英字大小文字、数字、記号を組み合わせる）を設定しましょう。また、生年月日など他人が容易に推測できるパスワードはやめましょう。

□ 過去に使用したパスワードや類似したパスワードは使用しないようにしましょう。また、利用するサービスごとに異なるパスワードを設定しましょう。

□ 図書館やネットカフェなど不特定多数の人が利用する共用PCや街中にある無料で利用できるWi-FiでユーザーIDやパスワードを入力したり、新規ユーザー登録をしないように注意しましょう。

□ 二段階認証や生体認証など、よりセキュリティ強化した認証システムを活用しましょう。

対応サービスでは、パスワードに頼らない「パスキー」（生体認証）や、FIDO2対応の「セキュリティキー（外付け型の認証デバイス）」を設定しましょう。偽サイトでは通用しない仕組みのため、安全性が大きく向上します。

また、学内向けサービスでも以下のように設定ができますので、ぜひ活用しましょう。

https://netsys.hosei.ac.jp/settings/mfa_settings.html

不審なメールやWebサイトを開かないようにしましょう

□心当たりのないメールは開封せずに削除しましょう。メールを開封しただけでウイルスに感染してしまうことがあります。

□万一メールを開いてしまった場合は、本文に記載されているリンクや添付ファイルを開かないようにしましょう。

□金融機関や企業などを装ったメールが送られ、本物そっくりな見た目のページに誘導し、個人情報やクレジットカード番号を騙し取る詐欺が相次いでいます。安易に個人情報を入力しないようにしましょう。

□インターネット上には様々なWebサイトがあり、ウイルスに感染したファイルやアプリが置かれていることがあります。信頼できるWebサイトやアプリ以外でのファイルのダウンロードはやめましょう。また、よくアクセスするサイトはブックマークをしておくと安心です。

□メールやSNS、Webサイトの画面上で「ウイルスに感染しています！」などの脅迫メッセージや、「続きが気になったらクリック！！」のリンク先から金銭を要求されることがあります。慌てて電話をかけたり、リンク先にアクセスしないようにしましょう。

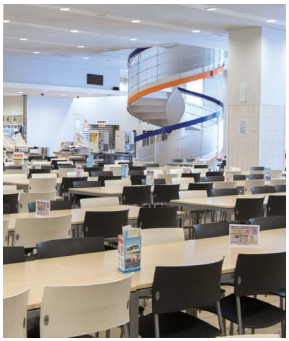
ソフトウェアを更新したり、ウイルス対策ソフトを導入しましょう

- □ PCやスマートフォン、タブレットのOS（Windows、MacOS、Android、iOSなどの基本ソフト）やアプリケーションに脆弱性（ぜいじゃくせい）が発見されることがあります。提供される修正プログラムを速やかに適用し、最新の状態に保ちましょう。
- □ ウイルス対策ソフトを導入して、外部から送られるデータをチェックしたり、インターネット・USBメモリなどからPCがウイルスに感染するのを防ぎましょう。
- □ サポートの切れたOSやアプリケーションを利用していると、ウイルスに感染しやすい状態になります。また、ライセンス違反に該当する場合もあります。定期的にアップデートやライセンスの更新を行いましょう。

脆弱性（ぜいじゃくせい）とは

PCのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生したサイバーセキュリティ上の欠陥のこと。
脆弱性を放置していると、外部から悪意を持った第三者（攻撃者）によって、不正アクセスをされたり、ウイルスに感染する危険性があるため、OSやソフトウェアの更新情報が届いたら、できる限り迅速にアップデートを行う必要があります。

大切な情報を適切に管理しましょう



□ PC、USBメモリの置き忘れ、紛失、盗難には十分に注意しましょう。大切な情報を含むPCやUSBメモリ等は肌身離さず持ち歩きましょう。

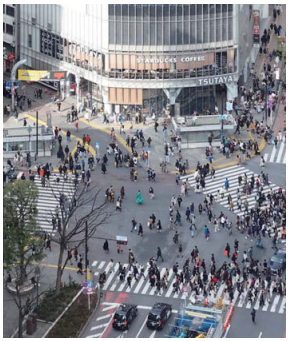
□ 友人やサークル、ゼミのメンバーの住所、電話番号などの個人情報を含むデータ等は、用途が済み次第速やかに削除しましょう。

□ 不特定多数の人が使用する共用PCを利用した際には、自分が保存・記録したデータを必ず削除し、残っていないか確認しましょう。

□ 大学が提供しているクラウドストレージがあります。ここにデータを保存すれば、持ち歩きによる紛失リスクを防ぐことができます。積極的に活用しましょう。

□ 大切なデータはあらかじめ、クラウドサービスやUSBメモリ、外付けハードディスクなどにバックアップを取っておきましょう。

大学外の団体と共同で活動するときは情報の取り扱いに十分注意しましょう



- □ 相手先から受け取った情報は、公開の可否を確認しましょう。迷う場合は公開しないことを原則にしましょう。
- □ 自分や友人、教職員などに関する個人情報や、大学が管理する重要な情報は、必要最小限で共有し、第三者への提供・転送は避けましょう。
- □ 相手先から受領したデータは、パスワード設定や施錠保管を徹底し、PCやUSBメモリの持ち歩きは最小限にしましょう。
- □ 相手先に情報を送るときは宛先を再確認し、相手先のアドレス開示に配慮してTo／Cc／Bccを使い分けましょう。機密性の高いデータは大学のクラウドストレージを利用しましょう。
- □ 共同事業の内容をSNS等で発信する前に、相手先の合意と公開範囲を確認し、位置情報や画像の写り込みにも注意しましょう。
- □ 万が一情報を流出させた場合は、学内フローに従ってHOSEI-CSIRT（P10参照）に連絡しましょう。

Wi-Fi（無線LAN）を安全に利用しましょう

□ 街中にあるWi-Fi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が存在します。安全性が保障されない提供元の不明なWi-Fiにはアクセスしないようにしましょう。

□ 自宅にWi-Fiが設置されている場合は、無断で他人に接続されないよう、セキュリティ設定を確認しましょう。

□ PCやOSと同じように、Wi-Fiルーターにもセキュリティ上の問題点（脆弱性）が発見されることがあります。提供される修正プログラムを速やかに適用し、最新の状態に保ちましょう。

SNSや匿名掲示板は
注意を払って楽しみましょう






- □ インターネット上に公開した情報は、一瞬で世界中へ拡散します。匿名でも、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。一度発信したものは後に消去したくなっても、完全には消去することができません。よく考えて公開しましょう。
- □ 他人を傷つける発言・行為や誹謗中傷などは人権侵害です。お互いの人権を尊重しましょう。
- □ 有名人や友人など、他人の情報や写真を許可なく公開することはプライバシーの侵害となります。
- □ 流れてきた情報を鵜呑みにせず、必ず発信元を確認しましょう。デマやフェイクニュースを拡散させることになりかねません。
- □ スマートフォンなどから投稿した場合、GPS情報から生活圏や自宅、個人を特定される恐れがあるので、位置情報を埋め込まないようにしましょう。
- □「高額バイト」などの情報は犯罪に巻き込まれる可能性があります。安易に連絡を取らないようにしましょう。

著作物の不正な利用はやめましょう

- □ 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かかわっています。無断でコピーしたり、コピーしたものを配布・共有しないようにしましょう。
- □ 不正にコピーされたものを入手・再配布することも違法になります。
- □ 論文やレポート作成時は引用のルールを守り、安易にネット上の情報をコピー＆ペースト（コピペ）をするなど、剽窃（ひょうせつ）・盗用をしないようにしましょう。

メールの宛先を確認しましょう

○メールを送信するときは、間違った相手に送信しないように、入力したメールアドレスをよく確認しましょう。

○Ccに入力したメールアドレスはメールを受け取った全員が見えてしまうので、To（宛先）、Cc（Carbon Copyの略：Toの宛先へ送る内容を共有したい相手がいるとき）、Bcc（Blind Carbon Copyの略：To、Ccへ送る相手を知られずに共有したい相手がいるとき）の違いを理解し、他の人のメールアドレスが知られては困る場合にはBcc を使いましょう。

情報セキュリティ事件・事故に遭遇したら

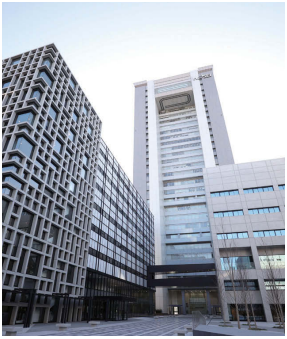
HOSEI-CSIRT連絡フォーム
（24時間受付）

「使用しているPCがコンピュータ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」
「重大な情報を保存しているUSBメモリを紛失した」
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「**HOSEI-CSIRT（シーサート）**」に連絡をして下さい。

「**HOSEI-CSIRT**」とは本学の情報セキュリティインシデント（以下、「インシデント」という）対応チームの名称で、インシデントを未然に防止すること、インシデントが発生した際の被害を最小限にすることを第一に、対処・対応等の活動を行っています。

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

法政大学 情報センターのご案内



市ケ谷、多摩、小金井の各キャンパスに設置されている情報センターには、PCを備えた情報実習室や自習用の情報カフェテリア、貸出ノートPC、無線アクセスポイントなどが設置されています。
本学のネットワークは、国立情報学研究所が提供するSINET回線によりインターネットへ接続しており、安定的かつ高速なデータ送受信を実現しています。

■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/

■多摩情報センター（総合棟3階）
TEL：042-783-2143
https://tedu.ws.hosei.ac.jp/

■小金井情報センター（管理棟4階）
TEL：042-387-6089
https://kedu2025.ws.hosei.ac.jp/

初期パスワードの変更方法や大学提供のクラウドストレージ（Boxなど）に関する利用方法はこちらで案内しています。

■法政大学 全学ネットワークシステム ユーザ支援WEBサイト
https://netsys.hosei.ac.jp/

情報セキュリティに関する情報

情報セキュリティに関する最新の情報は以下を参照してください

セキュリティ項目	情報提供機関／URL
セキュリティ全般	**独立行政法人情報処理推進機構（IPA）** https://www.ipa.go.jp/security/
サイバー犯罪への対策	**警察庁　サイバー警察局** https://www.npa.go.jp/bureau/cyber/index.html
注意喚起や脆弱性など セキュリティ最新情報	**JPCERT コーディネーションセンター** https://www.jpcert.or.jp/
サイバーセキュリティ 対策のための基本情報	**総務省　国民のためのサイバーセキュリティサイト** https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html

独立行政法人情報処理推進機構（IPA）

警察庁　サイバー警察局

JPCERT コーディネーションセンター

総務省　国民のための情報セキュリティサイト

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、PC 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。

＜法政大学学術情報ネットワーク規程＞
https://netsys.hosei.ac.jp/protected/acceptable_use_policy.pdf