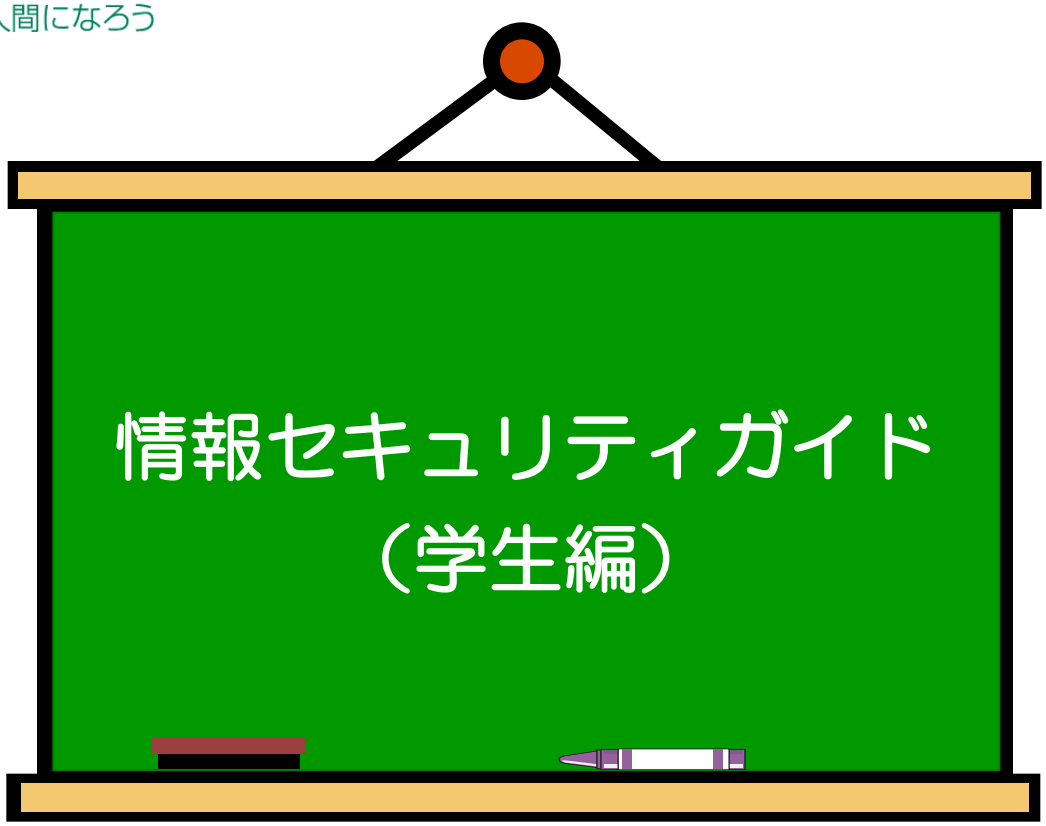
Sugiyama
人間になろう



情報セキュリティガイド（学生編）

情報セキュリティガイドについて

　この情報セキュリティガイドは、スマホ／パソコン等を安全に利用するため学生の皆さんに最低限守ってほしいことや注意してほしいことをまとめています。

　情報には、プライバシーのように慎重に取扱う必要があるものがあります。そのセキュリティを考えた際に、注意すべきこともまとめました。

　このガイドをよく読み、情報セキュリティへの理解を深め、事故を起こしたり巻き込まれないようにしましょう。

目　次

スマホ／パソコン等の利用時に注意すること

インターネット利用時の注意

≪インターネットの利便性と危険性≫

インターネットは、大変便利なツールです。しかし、利用方法を誤ったり適切な管理を行わないと、被害者になるばかりか加害者にもなる危険性があります。十分理解し便利な情報ツールとして活用しましょう。

日常における情報セキュリティ対策〔独立行政法人情報処理推進機構 （IPA）〕
https://www.ipa.go.jp/security/anshin/measures/everyday.html

◆怪しいサイトへのアクセス

怪しいサイトへは、近づかないようにしましょう。
もし、おかしいと感じたら直ぐ離れましょう。
不確かで怪しいサイトの情報は、ダウンロードしないようにしましょう。

- コンピュータウイルスの感染やスパウェア※等の不正なソフトがインストールされてしまう恐れがあります。

◆ スパウェア

スパウェアとは、知らないうちに勝手にインターネットに情報を送信するソフトウェアのことです。怪しいサイトで不正にインストールされてしまう以外に、インターネットからダウンロードしたソフトウェアに付属しているものもあります。インストール時に目的以外の機能が含まれていないか確認しましょう。

◆ブラウザソフトのセキュリティ設定

インターネットブラウザ（ 、 、 、 ）は、セキュリティを確保するためアップデートの適用を常時行い利用しましょう。

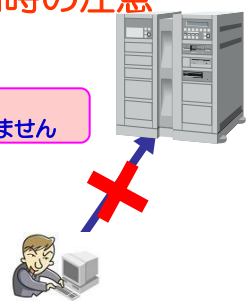
◆不特定の人が利用するパソコンの使用について

インターネットカフェ等では、キー入力を盗聴するプログラムが組み込まれている危険性があります。

- 学園の重要な情報へのアクセスでIDやパスワードの操作が必要な時は、インターネットカフェ等の不特定の利用者のあるパソコンでは行わないようにしましょう。

◆SNS（Line・YouTube・X・Instagram・TikTok等）の利用時の注意

個人情報を書き込んだり誹謗中傷などはしないようにしましょう。
また記載された情報を鵜呑みにしないように注意しましょう。
所謂、闇バイトに気を付けましょう。
（インターネット上の情報が全て正しいとは限りません）



◆不正アクセスの禁止

他人のパスワード等を無断で使用したり、他人に教えたりしてはいけません。

- ハッキングツール等を使用し、侵入する行為も絶対に行ってはいけません。

スマホ／パソコン等の利用時に注意すること

パスワード管理

≪パスワードの重要性≫

パスワードは、本人を証明するものであり大変重要です。
- パスワードが他人に知られてしまえば、あなたに「なりすます」ことで悪用されてしまうかもしれません。

◆パスワードの変更

パスワードを受け取ったら、速やかに変更しましょう。
- 他人にパスワードが知られた可能性がある場合も速やかに変更しましょう。

◆適切なパスワード管理

パスワードの取り扱いには、注意しましょう。
- 他人に教えないようにしましょう。
- 入力時は人に見られないように、また他人の入力時は目をそらすなど配慮しましょう。
- 大学で使用するパスワードは、１２桁以上必須で推測されにくいものを推奨します。
  - 自分や身近な人の名前、誕生日、電話番号、辞書に載っている単語など推測されやすいものは避け アルファベット大文字、小文字、数字、記号から３種類以上を織り交ぜる必要があります。
  - 英単語の組合せ等で、15文字以上をフレーズを用いるという考え方もあります。
- 忘れないようにしましょう。メモするときは見える場所に書いてはいけません。

◆多要素認証を使用しましょう！

- S*map、Gmail、Microsoft365は、シングルサインオン時に多要素認証を必須としています。 スマホアプリを主に、SMSを副として利用環境を整備してください。
- 多要素認証は「なりすまし」「のっとり」を防止できる有効な対策です。個人でも活用しましょう。

セキュリティ対策

◆セキュリティ被害の防止

自分が使うスマホ/パソコンでは次のことに注意しましょう。
- OSやアプリケーションは、アップデートを行い常に最新にしましょう。
- セキュリティ対策ソフトを導入し、継続的に更新しましょう。
  - 購入時に付属しているセキュリティ対策ソフトは、有効期間を確認しましょう。 期間が切れていると、内容が更新されず危険です。契約更新（有償）が必要です。
  - Windows10/11の場合、無償で添付されたWindows Defenderを使用することができます。
- フリーWi-Fiや、学園内無線ＬＡＮサービスの利用時は、不特定多数の人が使用する環境になります。 特にセキュリティ対策やアップデートが必須です。

◆セキュリティ被害が発生した時の対応

ウイルス検出など、セキュリティに関するメッセージが表示された時は、 表示を読み、その内容を理解した後、一旦ネットワークから物理的に切り離し、 原因の駆除、隔離など処置を行いましょう。
- 処置ができない場合は、学園情報センターに報告し指示を 仰ぎましょう。その際は表示内容や症状をきちん伝えましょう。
  - ウイルス感染等の兆候は機器の故障や、アプリケーションのトラブルと見分けが つきにくいものです。おかしいなと感じたら、対策ソフトでチェックしましょう。

スマホ／パソコン等の利用時に注意すること

◆電子メール利用時の注意事項

電子メールを送る時は、サブジェクト（題名、件名）を付けしましょう。
宛先間違いや、ドメイン名の誤りに注意が必要です。

- Cc（Carbon Copy）、Bcc（Blind Carbon Copy）の使い方を間違えないようにしましょう。
- 宛先は（To）へ、その内容を知らせたい相手は（Cc）です。
  （Bcc）は、（To）（Cc）で送る相手に、メールの送信先に（Bcc）が含まれることを知らせたくない時に使います。

添付ファイルは開く前に、不審な点が無いか確認しましょう。

- 送信者が知らない相手の場合や、知人でも文書内容等が変だと思ったら、十分注意し、不用意に開けないようにしましょう。
  ウイルス感染は、添付ファイルからも多く発生しており注意が必要です。

電子メールに記載されているリンク先を不用意にクリックしないようにしましょう。ワンクリック詐欺やフィッシング詐欺の手口かもしれません。文面の日本語は既に十分自然になっています。

- 大学からパスワードの再設定や、ログインを促す内容は、メールで送信しません！
  うっかり自分のユーザーID、パスワードを促されるまま入力しないようにしましょう。
  GmailやMicrosoft365は、乗っ取り被害が他大学で発生しています。
- 心当たりの無い送信元からの案内メールなどは、興味を引く言葉や楽しそうな雰囲気に惑わされ、安易にリンクをクリックしないようにしましょう。
  オークションやインターネットショッピングでも注意が必要です。

チェーンメールに加担しないようにしましょう。

- 複数の人に転送を求めるチェーンメール（不幸の手紙など）へ加担することはやめましょう。
  重要で緊急を装ったデマメールへも内容を確認して対応することが大切です。

◆個人のWebサイト、Blog、 SNS、ファンサイト等開設時の注意事項

著作権の侵害に注意しましょう。

- 著作権者の了解を得ないで勝手に複製しホームページ上に掲載することなどは、著作権の侵害になるので注意が必要です。

個人情報の取扱いは慎重に行いましょう。

- 個人情報の公開については、慎重に考えましょう。後述のページを参照してください。

パスワードは、厳重に管理しましょう。

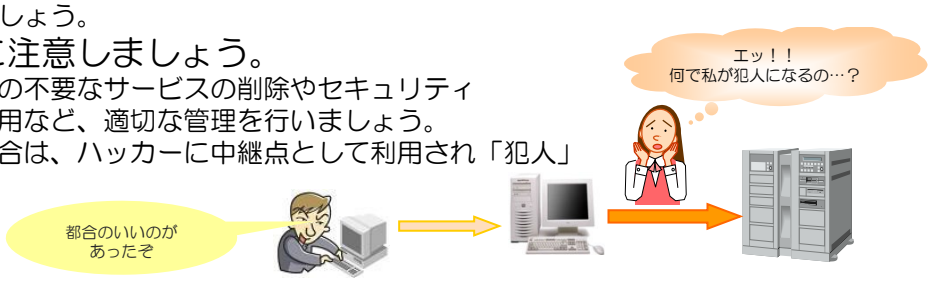
- 管理するパスワードが漏えいすると、他人に改ざんされてしまいます。

開設したサイト等への嫌がらせ、個人情報の掲載へは管理者として適切に対応しましょう。

- 「迷惑行為の禁止や不適当と思われる発言は削除します」といった旨の規約を明記し、管理者として責任と権限を理解し対応しましょう。

踏み台にされないように注意しましょう。

- スマホ／パソコン（サーバ）の不要なサービスの削除やセキュリティパッチ等修正プログラムの適用など、適切な管理を行いましょう。
- 適切な管理がされていない場合は、ハッカーに中継点として利用され「犯人」にされる恐れがあります。



スマホ／パソコン等の利用時に注意すること

Webシステムの利用

≪システムへのログインについて≫

大学では、S*mapやGmail等へのログインを、まとめて一回で可能なシステム（シングルサインオン）が使われています。パスワードの漏えいは全てを乗っ取られる危険性があるため、取り扱いに注意すると共に、多要素認証（P.3参照）を使用するなどセキュリティ強化に努めましょう。

◆Gmail（Google Workspace for Education Fundamentals）に関する注意事項

Googleには、Gmailをはじめ、様々なアプリケーションがあります。設定を間違えると、想定しない相手にも情報やファイルの共有をしてしまうため、以下の点には注意しましょう。

- 「ドライブ」は、クラウドストレージです。インターネット上にファイルの保存や共有ができます。インターネットURLを作成し、それを知っている人に対して、ファイルやフォルダを共有（公開）することが可能です。公開範囲は「意図的な世間一般への公開」を除いて、次の範囲に「リンクの共有」を設定するなど気を付けましょう。
  - ➢ オフ－特定のユーザー
    生成されたリンク（URL）を知っている
    指定したメールアドレスを持つユーザーに共有します。大学内、大学外のメールアドレスが指定可能です。
  - ➢ オン－リンクを知っている椙山女学園の全員
    生成されたリンク（URL）を知っている
    G-suiteを利用可能な学生教職員に共有します。
- 「フォト」は、写真に特化したクラウドストレージです。共有をかけた場合、生成されたリンク（URL）を知っているユーザーのみに共有します。

◆Microsoft365 利用時の注意事項

Microsoft365には、OneDriveをはじめ、様々なアプリケーションがあります。設定を間違えると、想定しない相手にも情報やファイルの共有をしてしまうため、以下の点には注意しましょう。

- 「OneDrive」は、クラウドストレージです。インターネット上にファイルの保存や共有ができます。インターネットURLを作成し、それを知っている人に対して、ファイルやフォルダを共有（公開）することが可能です。公開範囲は「意図的な世間一般への公開」を除いて、次の範囲に「リンクの設定」を設定するなど気を付けましょう。
  - ➢ 特定のユーザー
    生成されたリンク（URL）を知っている
    指定したメールアドレスを持つユーザーに共有します。大学内、大学外のメールアドレスが指定可能です。
  - ➢ リンクを知っている学校法人椙山女学園のユーザー
    生成されたリンク（URL）を知っている
    Microsoft365を利用可能な学生教職員に共有します。
- 「Teams」や「SharePoint」は、チャットとWebサイト等を介して情報共有が可能です。アクセス許可については取り扱うファイルの内容に応じて、しっかり判断してください。

スマホ／パソコン等の利用時に注意すること

スマホを安全に使うために

スマホを買ったら、アプリのインストールの前にまず「情報セキュリティ」に関する対策を行いましょう。
スマホユーザーとして最低限知っておきたい５項目を紹介します。

◆スマホを落とした！

購入後すぐにロックを！

プライベートの大切な情報がいっぱい詰まったスマホをなくして、もし悪意のある人に拾われて中をのぞかれたら・・・！！
そんな場合に有効なのがセキュリティロック。スマホは、顔、指紋、ジェスチャー、文字列等をロック（鍵）にすることができます。買ったらすぐに設定しましょう。万が一、スマホをなくしてしまった場合に備えて、「端末を探す」設定をしておくことも大切です。遠隔操作で、スマホの位置を特定したり、中のデータを消去できる場合もあります。
場合によっては、速やかに購入店やサポートに相談しましょう。

◆アプリのインストール！

アプリは信頼できるサイトから

スマホで使用するアプリは、アプリの審査や不正アプリの排除を実施している信頼できる所からインストールしましょう。iPhoneであれば「App Store」、Androidであれば「Google Play」です。
Android系スマホの場合は、「提供元不明のアプリ」は原則インストールしない設定にしておきましょう。

◆謎のアクセス許可？

不自然なアクセス許可は拒否！

Android系スマホの場合、アプリをインストールする際に表示される「アクセス許可」は必ず目を通してから承認してください。壁紙アプリにも関わらず「連絡先データを読み取り」の許可を求めるアプリにウイルスが仕掛けられていた例もあります。アプリの機能からすると不自然なアクセス許可が1つでもあったらインストールを中止した方が安全です。疑問点はアプリの開発元や、ITに詳しい人に確認しましょう。

スマホ／パソコン等の利用時に注意すること

◆最新版で体力アップ！

OSやアプリのバージョンは
常に最新に

スマホの基本ソフトであるOSのバージョンが旧い（ふるい）と、ウイルス感染や悪意のある攻撃に遭う危険性が高まります。OSの脆弱性を修正するためのデータが携帯電話会社から提供されたら速やかにアップデートしましょう。

アップデートは「設定」などのメニューからできます。

自分でインストールしたアプリが古い場合でも、同様にウイルス感染や悪意のある攻撃に遭う危険性が高まります。常に最新の状態に保つよう、こまめにチェックしましょう。

また最新版OSに対応できなくなったスマホは残念ですが買換えましょう。

Androidのアップデート期間は2～７年。
iPhoneのアップデート期間は5～6年

◆安全な回線を利用する！

通信は安全な環境で

スマホで、街中などのフリーWi-Fi（無線LANスポット）を利用する方法がありますが、安全な通信が確保できるかは不明です。不特定多数の利用者がいる（無償の）Wi-Fi環境では、盗聴の危険性があります。ネットバンキングなど、重要な情報の送受信には、安全な回線を利用するようにしましょう。

VPNの利用も考えましょう。

◆安全なサイトを閲覧する！

表示内容の真贋を見分ける

Webを閲覧している際に、突然「ウイルスに感染しています」といった警告が表示される場合があります。

そのような表示はセキュリティ対策ソフトを装った悪意のあるアプリをインストールさせようとするものです。怪しい警告や、広告が表示されるWebサイトは閲覧しないようにしましょう。

《参考にした資料》

・独立行政法人 情報処理推進機構 （IPA）、【スマホを安全に使うための6項目】
https://www.ipa.go.jp/security/love_smartphone_life/mini_book/index.html

スマホ／パソコン等の利用時に注意すること

SNS利用にあたっての注意

SNS（Social Network Service）とは、インターネット上でのコミュニケーションツールであり、今や広く社会に浸透し、利活用されるようになってきました。しかし、扱い方を間違えば、 LINE、X、Instagram、TikTok、Facebookなど、親しい友人・知人に向けて発信した個人的な意見や近況報告が、そのような意図とは大きく離れてインターネット全体に伝達・拡散し、思わぬ重大な事態に発展することがあります。発信者が特定され、家族や友人、大学、就職の内定先等まで巻き込まれる事例も発生しています。

学生の皆さんは、SNSを利用するにあたって、その特性を十分に理解したうえで利用してください。

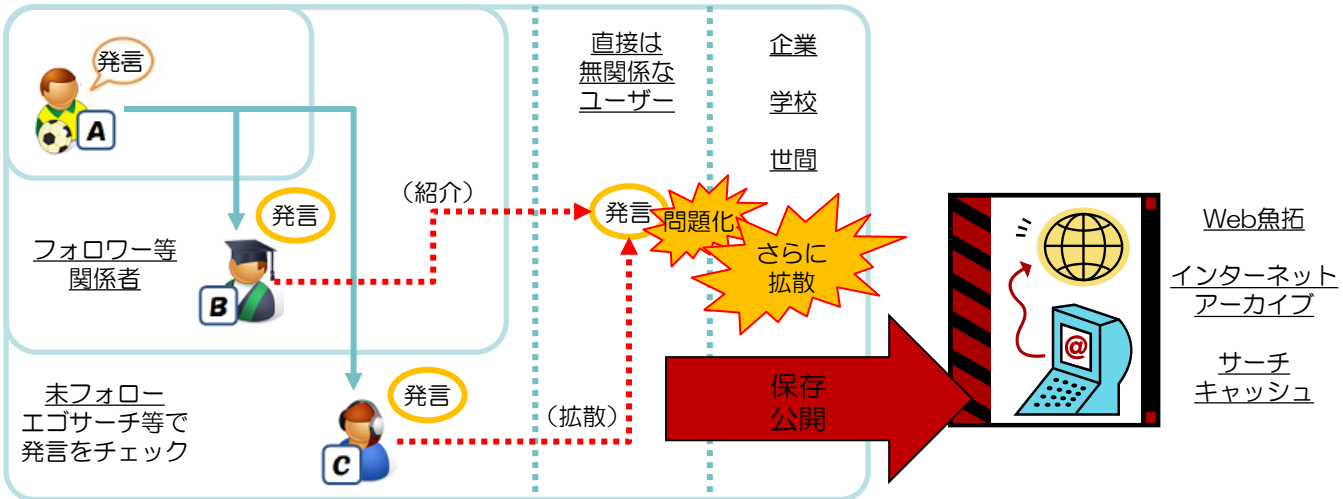
◆SNSへの書き込みは独り言や友達とのおしゃべりではない

発言（書込み）を非公開設定（アクセス制限）していないアカウントは、全世界に向かって情報を発信しています。

◆見られていないと思い込んでいるのは“あなただけ”

日常的に発言（書込み）をしていると、身近な人にしか見られていないと思いがちですが、発言した内容から個人が特定されているケースもあり、先生や先輩、バイト先や企業など多数の関係者の目に触れてしまう事例が発生しています。

世界に向かって公開されている以上、まったく無関係な人が発言（書込み）を発見して、それを拡散することも考えられます。過去の発言も遡って検索され拡散されることもありますし。一度拡散した情報を完全に削除することは不可能です。今の軽率な発言が、将来をつぶす可能性があることを重々認識しましょう。



スマホ／パソコン等の利用時に注意すること

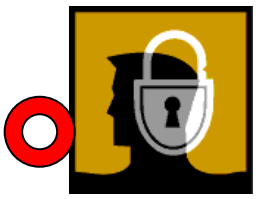
◆ネット上に完全な匿名性やセキュリティはない

非公開設定（アクセス制限）をしていても、システムエラーや、つながりのある友達のミス、あるいは悪意により、内容が漏えいされる可能性はあります。

犯罪や反社会的行為など何らかの問題が発生した場合、法律によって被害者には発信者の情報を開示請求することが認められています。アクセス制限していることに対して安全を過信することなく、発言には十分注意しましょう。

◆個人情報とプライバシーの保護

自分自身だけではなく、本人に断りなく個人名や写真などの個人情報を不用意に掲載することは絶対にやめましょう。あなたが公共の場で表現しないようなことは、Web上でも同じように表現しないようにしましょう。



◆他者の尊重

他者の人格・性格を否定するなど、誹謗中傷することは人権侵害・名誉毀損になる可能性があります。他者への配慮を十分に心がけましょう。

《参考にした資料》
・聖心女子大学におけるソーシャルメディア扱いのガイドライン
・独立行政法人 情報処理推進機構 （IPA）ここからセキュリティ！ 情報セキュリティ・ポータルサイト
https://www.ipa.go.jp/security/kokokara/study/

情報の取扱いについて

著作権の侵害

◆正規ライセンスの利用

ソフトウェアを使用する際は、利用規約をよく確認しましょう。
ライセンス規約違反とならないよう、注意が必要です。

- ソフトウェアを利用する権利の貸与や譲渡を認めていない場合があります。借りたソフトのインストールや、パソコンを譲ってもらった場合には気を付けましょう。
- インストールできるパソコンや台数が制限されている場合があります。自分のパソコン等へのインストールは良く確認して行い違反の無いようにしましょう。
- また研究室等に設置された共用のパソコンであっても、ソフトのインストールは管理者の了承と、ソフトウェアのライセンスを確認してからにしましょう。

◆著作権の意識

インターネット上の文章、イラスト、音楽、写真などを権利者に無断で複製し、インターネット等に掲載して誰にでもアクセス可能な状態にすることは、著作権侵害にあたります。
（レポートに引用する場合は引用元を明記する必要があります。）

- 音楽や映像等のダウンロードを目的として、違法にアップロードされたと認識してWebサイトからダウンロードすることも違法です。
- ファイル共有ソフト（Winny、PerfectDark、Share等）を使用した結果、ウイルス感染により個人情報が漏えいする事件が過去にありました。このような違法となる行為及びその目的のためにファイル共有ソフトを利用することは、絶対にやめましょう。

個人情報の保護

◆個人情報の取扱い

氏名、住所、電話番号、写真などの個人情報は、本人に断り無く、電子メールでの発信やWebページ、掲示板、SNSへ公開することは絶対にやめましょう。

- 親しい友達同士や先輩・後輩の関係であっても、同意を得ないで勝手に公開してはいけません。公開に際しては、必ず同意を得ましょう。
- 集合写真などで本人が識別できる場合も、同意を得る必要があり十分注意が必要です。

サークル等でメンバーリストを作る場合は、一人一人が安全に管理し、そのリストの使用目的の範囲内で利用しましょう。

- Twitter等SNSへの書き込みにふさわしい情報であるかの判断や、個人情報の扱いは、各自で慎重に考えて責任を持って行動しましょう。

情報の取扱いについて

情報のバックアップ

◆バックアップの重要性

課題や卒論等の大切なデータは、複数個所に保存することでバックアップを作成し、誤削除や破損に備えておきましょう。

- バックアップとは、大切なデータを複数の場所に、途中経過毎にコピーしておくことです。ハードディスク（HD）、CD等のメディア、USBメモリに定期的にバックアップするようにしましょう。
- バックアップのコピー先（USBメモリ等）も消耗品です。バックアップ先が一つでは、故障や経年劣化によるトラブルでデータが消えて復旧できなくなることがあります。複数のバックアップ先を用意して使いましょう。
- クラウドにデータを保存することでもバックアップしておきましょう。
  Google Worksapceや、Microsoft365が使用できます。
- 個人使用のパソコンも、定期的にバックアップしておきましょう。
- 個人使用のスマホは、iCloudやGoogle標準のバックアップでクラウドへバックアップしておきましょう。

情報の消去

◆買い替え、廃棄、譲渡時の注意事項

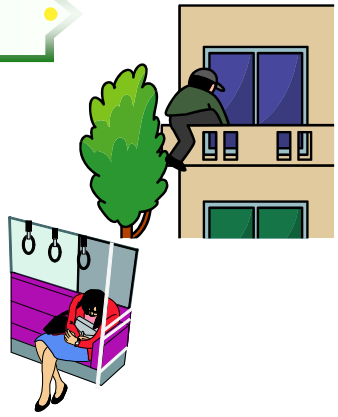
スマホ／パソコン等の中に保存された情報は、専用の消去ツールなどを使い、完全消去するか物理的に破壊し読み出せないようにしましょう。

- 買い替え等では、販売店側で情報消去サービスを行っていることもあります。下取りでは、販売や廃棄時に保存されていた情報がどう処理されるか確認しておきましょう。
- 拾った第三者が、データを読み出して悪用するかもしれませんので、USBメモリ等の情報記憶媒体も判読不能にしてから廃棄しましょう。
  物理的にキズをつけたり、破壊するなどしてから自治体の指定した廃棄物として処理しましょう。

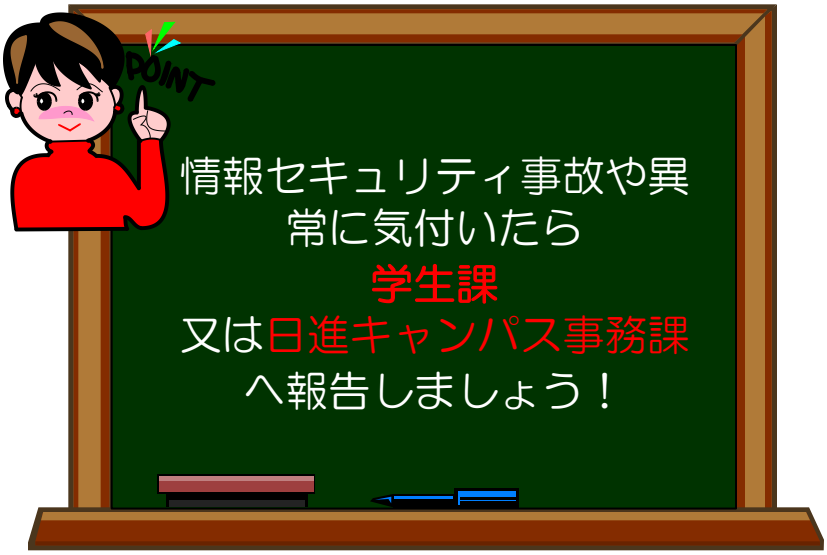
盗難対策

◆情報の盗難対策

重要な情報が入ったノートパソコンや情報記憶媒体は、施錠できる場所に保管するといった盗難対策をしましょう。
移動の時は、置き忘れによる紛失や盗難に注意しましょう。



事故の発生や異常に気づいたとき



報告する事故など

- コンピュータウイルス等の感染
- データの破壊・改ざん・紛失
- スマホ／パソコン等や情報記憶媒体※1の紛失、盗難
- 情報通信媒体※2の不正使用
- 個人情報の漏えい※3、紛失、盗難
- 情報セキュリティ上、重要と思われること

※1　HD、USBメモリ、CD、DVD等の電磁的・光学的記憶媒体
※2　電子メール、電子ニュース、Webシステム、SNSなど
　　インターネットを介してサーバ等を使用する通信手段
※3　個人情報の拡散など、自身では制御が不可能な場合も含む

《報告相談窓口》

学生課　星が丘キャンパス　学園センター２階
TEL　０５２－７８１－６４７５

日進キャンパス事務課　日進キャンパス　人間関係学部１号館２階
TEL　０５６１－７４－１１９２

椙山女学園情報セキュリティポリシー

平成１９年　４月２７日

学校法人椙山女学園（以下「学園」という。）は、「人間になろう」という教育理念の達成や、グローバル情報社会の一員として情報活用を促進するとともに、社会からの厚い信頼に応えるため、学園内外と安全に情報交換できる環境を構築することを目指し、教育研究機関にふさわしい情報セキュリティポリシーをここに策定する。

１　学園の教育事業運営における情報セキュリティの重要性を正しく認識し、学園の学生生徒等を含む構成員に対して基本的事項の理解及び適切な行動を促すように努める。

２　学園における情報セキュリティ適用範囲及び境界を定義し、管理対象を明確にすることで、適切な管理体系を構築する。

３　セキュリティ目標を設定する。設定目標は、達成可能なものであり客観的に評価可能なものとする。

４　学園に、前項の目標を達成するために必要な組織及び規則を整備する。

５　情報セキュリティ事項を周知徹底するため、学園の職員等に対して適切な研修及び啓発活動を実施する。学生生徒等に対しては、情報セキュリティポリシーの遵守は情報化社会における重要な責務であることを認識するよう、教育及び啓発に努める。

６　情報セキュリティの適正な運用及び有効性を維持するために、定期的に監査を実施する。

付録：情報セキュリティに関する法律

「不正アクセス行為の禁止等に関する法律」（不正アクセス禁止法）

不正アクセス行為を禁止し、罰則を定める法律。電気通信回線を通じた犯罪防止を目的とし、アクセス制御機能の保護を図る。他人のIDやパスワードを無断で使用する行為を抑制します。

- 他人のIDやパスワードを無断で使用してSNSに不正ログインする行為
- システムの脆弱性を突いてコンピュータに侵入する行為

「個人情報の保護に関する法律」（個人情報保護法）

個人情報の適正な取扱いを義務付け、個人の権利利益を保護する法律。事業者に対し、個人情報の収集、利用、提供のルールを定める。個人情報の無断収集や不正利用を抑制します。

- 企業が顧客の個人情報を無断で第三者に提供する行為
- 従業員が個人情報を不正に持ち出し、外部に漏洩させる行為

「電子署名及び認証業務に関する法律」（電子署名法）

電子署名の法的効力を認め、認証業務の基準を定める法律。電子商取引の信頼性を向上させる。電子文書の改ざんやなりすましを抑制します。

- 認定を受けていない事業者が電子署名を提供する行為
- 利用者が認定認証事業者に虚偽の証明をさせる行為

「情報流通プラットフォーム対処法」（情プラ法）

SNS事業者に誹謗中傷や権利侵害情報の迅速な対応を義務付け、削除基準の明示と運用状況の公表を求める。インターネット利用者の誹謗中傷やなりすまし、闇バイトの勧誘などの行動を抑制することを目的としています。

- SNS上での誹謗中傷投稿を放置する行為
- 削除申請に対して適切な対応を行わない行為

「その他の情報セキュリティに関わる法律」

- 高度情報通信ネットワーク社会形成基本法（IT基本法）
- 不正競争防止法
- 電気通信事業法
- サイバーセキュリティ基本法
- 著作権法
- 刑法・コンピュータ犯罪
- 電波法

発　行：学校法人椙山女学園
　　電子情報セキュリティ委員会

【 変更履歴 】

1. Ver 1.0	2007年10月26日	新規発行
2. Ver 1.1	2010年 4月 1日	改訂
3. Ver 1.2	2012年 4月 1日	改訂
4. Ver 2.0	2014年 4月 1日	第2版発行
5. Ver 2.1	2017年 4月 1日	改訂
6. Ver 3.0	2019年 4月 1日	改訂
7. Ver 3.1	2023年 4月 1日	改訂
8. Ver 3.2	2025年 4月 1日	改訂

椙山女学園大学