

情報セキュリティ対策の 9 項目

1 情報通信機器



OS やソフトウェア、セキュリティソフトは、常に最新の状態で利用しましょう。またパスワードロックをかけましょう。



2 パスワード



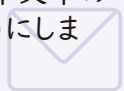
推測されにくいように 10 文字以上で、無関係な（文章にならない）複数の英数字をつなげ、その間に数字列を挟むようにしましょう。また使いまわしは控えましょう。

3 メール



アカウントに 2 段階認証（ワンタイムパスワード）を設定しましょう。

また心当たりのないメールは極力開かず、不明なメールの添付ファイルや本文中の URL は開かないようにしましょう。



4 外部メモリ



外部メモリは極力使わず、使う場合は個人情報を入れないようにしましょう。使用する場合はパスワードロックをかけられるものをおすすめです。



5 ファイル共有サービス (クラウドサービス)



アクセス権を限定しましょう。不要になった場合は速やかに共有を解除しましょう。

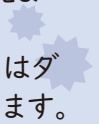


6 フリー Wi-Fi や フリーソフト



アクセスやダウンロードによりサイバー攻撃、ウイルス感染の恐れがあるため、フリー Wi-Fi の利用やフリーソフトのダウンロードは控えましょう。

※「GoogleChrome」はダウンロードをお願いします。



7 SNS



SOBA マナベル 支援 > 学生支援センター > 各種規程に掲載された「ソーシャルメディア利用ガイドライン」を遵守し、SNS の特性を理解した上で利用しましょう。



8 バックアップ



不測の事態に備え、定期的にバックアップを取りましょう。



9 情報の削除



目的を終えた情報は削除しましょう。またパソコンを廃棄する場合は専門業者へ依頼しましょう。



情報セキュリティ侵害等を発見した場合は、八洲学園大学 学生支援センターへご連絡ください。

【八洲学園大学 学生支援センター】

電話：045-410-5454 メール：u-info@yashima.ac.jp

（受付時間：平日 9:00～18:00 / 土日祝 9:00～17:00）



1. 情報通信機器の OS やソフトウェアは、常に最新の状態で利用しましょう。



OS やソフトウェア、セキュリティソフトを更新せず古いバージョンのまま使用していると、悪意あるサイバー攻撃を受けたりウイルスに感染する恐れがあります。常に更新を行い、最新の状態で利用してください。

またパソコン自体にパスワードを設定して、パソコン内の情報を見られないようにしましょう。

2. パスワードは複雑なものにし、使いまわしは控えましょう。



短いパスワードは見破られやすく不正にログインされ悪用される恐れがあります。パスワードを10文字以上にすると、推測や解析されにくくなるため、「無関係」「複数の単語」「数字列を挟む」「使いまわさない」ようにして安全性を高めましょう。

3. 2段階認証を設定しましょう。心当たりのないメールは開かないようにしましょう。



アカウントに2段階認証（ワンタイムパスワード）を設定すると、本人確認を2回するため不正なアクセスをより効果的に防ぐことができます。

近年、ウイルス付のメールや巧妙な偽メールが増えています。心当たりのないメールは極力開かず、添付ファイルや本文中の URL は開かないようにしましょう。

4. 外部メモリは極力使わず、使う場合は個人情報を入れないようにしましょう。



外部メモリは、盗難や紛失による情報漏洩やウイルス感染のリスクがあります。使用する場合は「個人情報を入れない」「重要な情報は持ち出さない」ようにしましょう。

※メモリ自体にパスワードロックをかけられるものだと、盗難や紛失時にデータを読み取られる可能性が低くなります。

5. ファイル共有サービス（クラウドサービス）のアクセス権を限定しましょう。



ファイル共有サービス（クラウドサービス）は、オンライン上でデータを保存・管理できるサービスです。ファイルを共有する際は、必要に応じてアクセス権を付与しましょう。不要になった場合は情報の流出を防ぐためにも共有を解除し、適切にアクセス権を管理しましょう。

6. フリー Wi-Fi やフリーソフトのダウンロードは控えましょう。



セキュリティ対策が行われていないフリー Wi-Fi やフリーソフトを利用すると、第三者に通信内容を覗かれ個人情報の流出や ID・パスワードの悪用、ウイルス感染の恐れがあるので、注意しましょう。

※「GoogleChrome」はダウンロードをお願いします。安全性があり、不正なサイトやウイルス感染の恐れのあるサイトから保護してくれます。

7. ソーシャルメディアは責任をもって利用しましょう。



ソーシャルメディアを利用する際は、八洲学園大学「ソーシャルメディア利用ガイドライン」を遵守し、責任をもって情報発信を行いましょう。基本的人権、肖像権、プライバシー権、著作権、商標権などを侵害しないように注意しましょう。

8. 不測の事態に備え、定期的にバックアップを取りましょう。



定期的にバックアップを行っている、データの消失や破損が起きても復元することが可能です。パソコンの故障や人為的ミス、ウイルス感染などの不測の事態に備えましょう。

9. 情報の削除をしましょう。



情報漏洩を防ぐために、目的を終えた情報は削除しましょう。紙の書類はシュレッダーにかけてから破棄してください。

パソコン自体を廃棄・譲渡する場合は、削除や初期化するだけでは復元される恐れがあります。完全に削除できるデータ消去ソフトを使用したり、専門業者へ依頼し復元できないようにしましょう。