～ 新たに岡山大学の一員となられた皆様へ ～

安心・安全のための情報セキュリティガイド

岡山大学
OKAYAMA UNIVERSITY

岡山大学では、情報漏洩やウイルス感染、情報セキュリティ・インシデントの防止などのために、岡山大学情報セキュリティポリシー及び実施規程・実施手順を定めています。このパンフレットは、新たに岡山大学に入学、編入、着任された皆様のために、大学等の情報システムやネットワークを利用する際に遵守すべき必要最低限の事項をまとめたものです。これらを遵守するとともに、情報セキュリティ教育の受講や、公表されたセキュリティ情報の収集を通じて、情報セキュリティについて日々学習し、適切な情報利用に努めましょう。

1．OSやセキュリティ対策ソフトはいつも最新にしましょう

2．ID、パスワードを適切に管理しましょう

3．メールの送信に注意しましょう

4．モバイル端末や記憶媒体の持ち運びに注意しましょう

5．不審なメールやwebページを開かないようにしましょう

6．インターネットのサービス、SNSの利用に注意しましょう

7．ソフトウェアインストールの注意点、
P2Pファイル交換ソフトの使用禁止

8．情報セキュリティ・インシデント発生時の対応

9．その他の注意

- 情報機器や記憶媒体の廃棄
- web利用の注意点
- 離席時の画面ロック

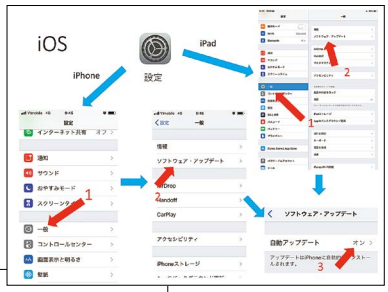
〈参考〉情報セキュリティポリシー【学内限定】
http://www.citm.okayama-u.ac.jp/citm/security/securitypolicy.html

目の届く場所に貼って普段から注意喚起しましょう。

1. OSやセキュリティ対策ソフトは いつも最新にしましょう

ウイルスなどの不正なプログラムは、オペレーティングシステム（以下OS）やその他のソフトウェアの弱点（脆弱性）によって活動します。脆弱性のほとんどは、更新プログラムをインストールすることで修正されます。更新しないOSやソフトウェアは非常に危険です。

- OSのアップデートを自動更新にして、いつも最新の状態で使用してください。ネットワークに接続していない場合にも、定期的に確認して更新をしてください。
- ソフトウェアも必ずセキュリティアップデートをしてください。
- 更新プログラムが提供されなくなったOSやソフトウェアを使わないようにしてください。



Windows

macOS

新種のウイルスや不正なプログラムは、2015年の平均で1日100万件以上が発見されています。セキュリティ対策ソフトがインストールされていても、ウイルス定義ファイルが更新されていなかったり、セキュリティ対策ソフトが旧バージョンであったりすると、ウイルスを適切に検出できません。

- ウイルス定義ファイルは頻繁に更新してください。また、週に1回程度はパソコン内のファイルをセキュリティ対策ソフトでチェックしましょう。
- セキュリティ対策ソフトは最新バージョンを使用してください。

※岡山大学では、トレンドマイクロ社との包括契約により、大学所有の機器であればウイルスバスターを台数の制限なく利用できます。教職員・学生が岡山大学に持ち込む可能性のある個人所有の機器には1人につき3台まで利用することができます。**学内のネットワークに接続する機器には、必ずセキュリティ対策ソフトを使用してください。**

2. ID、パスワードを適切に管理しましょう

メールや各種サービスでパスワードを盗まれて不正行為を受ける被害が多発しています。短いもの、ユーザ名と似ているもの、本人に関する情報、辞書の単語などは危険です。

- 推測されにくいパスワードを設定してください。岡山大学統合認証管理システムでは、**英大文字、英小文字、数字またはシステムで使用可能な特殊文字を各最低1文字以上含む8文字以上16文字以内**を使用するよう定めています。
- 複数のサービスで同じパスワードを使わないでください。新たな環境に移った機会に、以前使用していたパスワードから一新することをお勧めします。

3. メールの送信に注意しましょう

電子メールは、通信経路やサーバで盗聴される危険があります。また、複数の相手にtoやccでメールを送ると、宛先のメールアドレスが他の人にも知られてしまい、不正行為や迷惑メールの原因になることがあります。

- 機密情報や業務の情報などをメールでやりとりする場合には、必要に応じて重要な情報を添付ファイルにし、暗号化して送信するようにしてください。
- 複数の人にメールを送る場合は、Bccで宛先を追加するか、面倒でも1件ずつ送るようにしましょう。

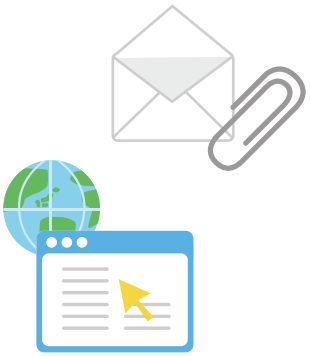
4. モバイル端末や記憶媒体の持ち運びに注意しましょう

モバイル端末やUSBメモリなどの記憶媒体の持ち運びは、盗難や紛失の危険があります。もし機密情報が保存されていたら情報漏洩事件につながります。

- 暗号化していない機密情報は持ち運ばないようにしましょう。
- モバイル端末や記憶媒体は、電車の棚に置かないようにしましょう。飲食の場に持ち込む際には特に注意しましょう。
- 以前に使用していた記憶媒体にも、機密情報が残っていないか確認しておきましょう。

5. 不審なメールやwebページを開かないようにしましょう

標的型攻撃メールの被害が深刻な問題となっています。重要な連絡であるように偽り、メールの添付ファイルやURLを開くように仕向けてウイルスに感染させる手口です。感染するとファイルを暗号化したり、情報漏洩事件を起こしたりします。また、インターネット上には閲覧しただけでウイルスに感染するような危険なwebページが多数あります。



- 心当たりのある相手や業務に関するようなメールでも、少しでも不自然だと感じた添付ファイルやリンクは、安易に開かずに電話やその他の方法で相手に確認しましょう。特に環境が変わった直後は、岡山大学の関係者を装った第三者が不正なメールを送り付けることが考えられます。メールの送信者が関係者かどうかはっきりしないときは、周囲の人に確認してください。
- 業務に関係ないサイトは閲覧しないようにしましょう。
- 検索サイトで見つけたwebページには、危険なものがありますので十分に注意しましょう。

6. インターネットのサービス、SNSの利用に注意しましょう

インターネットのサービスには、メール、翻訳、ファイル共有等々、便利なサービスが多数ありますが、その特性を十分に理解して利用してください。例えば、翻訳サイトは、入力した内容を翻訳サイト管理者が見ることができます。またファイル共有サービスの設定が不適切であれば、ファイルがインターネットに公開されることがあります。

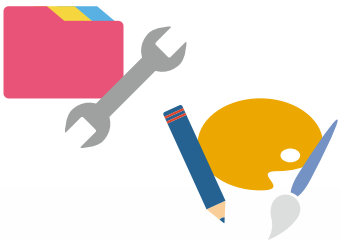
- 特にフリーのサービスなど、厳密な秘密保持が保証されないサービスでは、機密情報を扱わないようにしてください。
- 教職員の方は、異動などでデータ移行が必要な場合等も含め、ファイルの配送は岡山大学のファイル配信サービスを利用しましょう。学外とのデータのやりとりも可能です。利用方法は情報統括センターwebページを御覧ください。
- ファイル共有サービスでは、アクセス可能範囲と保存期間を設定しておきましょう。

FacebookやTwitterなどのSNSは便利で楽しい反面、投稿内容や設定の不備でトラブルになることがあります。投稿した内容は公開、引用されることを前提に利用しましょう。

- 業務上の利用の際は「国立大学法人岡山大学におけるソーシャルメディアに関する要項」、私的利用に関しては「岡山大学ソーシャルメディアガイドライン」を参照してください。
- 私的な利用では、業務情報に関する投稿は止めましょう。**特に異動や引っ越し、新しい環境などについての話題をSNSに投稿する場合は、業務に関する情報が含まれないよう注意してください。**
- SNSの怪しい投稿のリンクに注意しましょう。

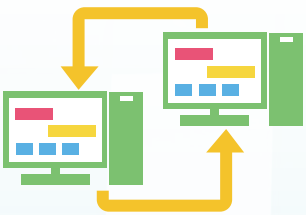
7. ソフトウェアインストールの注意点、P2Pファイル交換ソフトの使用禁止

パソコンやスマートフォン等にソフトウェアをインストールする際は、ライセンスや、不正なプログラムに注意してください。



- 業務で使用するパソコンにソフトウェアをインストールする際は、システム管理者や情報セキュリティ管理者の承諾を得てください。
- P2Pファイル交換ソフトは、著作権侵害やウイルス感染の危険があるため使用禁止です。個人所有のパソコンであっても使用しないようにしてください。

※岡山大学では、マイクロソフト社との包括契約により、同社のソフトウェアを無償で利用することができます。利用対象と、利用できるソフトウェアについては、下記ページをご覧ください。



〈参考〉マイクロソフト包括ライセンス【学内限定】
http://www.citm.okayama-u.ac.jp/citm/license/msbp.html

8. 情報セキュリティ・インシデント発生時の対応

情報セキュリティ・インシデントとは、事業運営に影響を与えたり、情報セキュリティを脅かしたりする事件や事故のことをいいます。例えば、コンピュータウイルス感染による情報漏洩や、ホームページの改ざんなどです。インシデントの発生をゼロにすることはできません。インシデントが発生することを前提に被害が最小限になるように心がけてください。インシデントの可能性があるときは次の対応をしてください。

- 情報端末の電源を切らずにネットワークから切り離してください。そして、スリープか休止状態にしてください。
- 冷静にどんな異常なことが起きたのかを把握し、直ちに情報統括センターのwebページから［情報セキュリティ通報フォーム］で連絡してください。また、所属部局の担当者にも連絡してください。その後、対処方法の連絡をお待ちください。

9. その他の注意

■情報機器や記憶媒体の廃棄や譲渡

- 紙媒体はシュレッダーにかけましょう。CDやDVD等は切断しましょう。
- パソコンやUSBメモリは、完全消去のソフトウェアでデータを消去するか、情報を復元できないようにしてから処分しましょう。タブレット端末、スマートフォン、携帯電話なども同様です。
- また個人情報や研究情報などの機微情報を扱うパソコンでは、普段から情報を暗号化しておくようにしましょう。WindowsではBitLocker、macOSではFileVaultを利用して自動的に暗号化が可能です。iPhoneやiPadではパスコードを設定することで、内部の情報を暗号化することができます。Androidでは、標準で暗号化されている場合もありますが、手動で設定が必要なものもあります。

■web利用の注意点

- webページで情報を入力する際には、httpsで接続されている（URLが「http」ではなく、「https」で始まっている）ことや、サーバ証明書で正規のサイトであることを確認しましょう。
- webブラウザ（インターネットエクスプローラーやChrome等）は、セキュリティレベルが低下するような設定やアドインのインストールを行わないようにしましょう。

■離席時の画面ロック

- パソコンを不正に使用されたり、画面を覗き見されたりしないように、スクリーンセーバーとパスワードロックを使用してください。

岡山大学 情報統括センター CSIRT

問い合わせ先

■利用者相談窓口（ヘルプデスク）

情報統括センター１階　TEL：086-251-7232

■情報統括センター鹿田担当

岡山大学病院外来診療棟３階　TEL：086-235-7075

URL：https://www.citm.okayama-u.ac.jp/citm/index.html

2020年3月発行