熊本大学
情報セキュリティ
ポケットマニュアル
（学生用）

発行者　総合情報統括センター情報セキュリティ室

パソコンやスマートフォン等の利用

■パソコンやスマートフォン等の利用において様々な問題が発生しています。このポケットマニュアルでは皆さんが注意すべき事項をまとめました。

1 個人のID･パスワードは適切に管理！

ID･パスワードは本人であることを証明する大切な情報です。盗まれたり他人に使用させないようにしましょう。

また、容易に推測されるパスワード（例：誕生日）や複数のサイトで同じパスワードを使う「使い回し」はやめましょう。

※ 本学では、英大文字･英小文字･数字･記号のうち3種類を組み合わせた8文字以上を推奨しています。

2 セキュリティ対策の徹底！

パソコンやスマートフォンではセキュリティ対策が必要です。個人のパソコンには必ずセキュリティ対策ソフトを導入しましょう。なお、本学在学中はセキュリティ対策ソフトである「F-Secure」の無償利用が可能です。また、OSやアプリケーションも定期的にアップデートしましょう。

3 不審なメールは無視（削除）！

金融機関等からのパスワード変更や個人情報入力を促すメール、知人等を装った不審なメールが届いた場合には無視（削除）しましょう。

安易に情報を入力したり添付ファイルを開いたりすると、情報が搾取されたり、マルウェア感染する可能性があります。

パソコンやスマートフォン等の利用

熊本大学 Kumamoto University

4 OneDrive、DropBox等のクラウド・ストレージに注意！

DropBox等のクラウド・ストレージに保存した情報は、サービス提供業者の所有物になる可能性があります。必ず利用規約を確認しましょう。また、利用する場合は公開の範囲を限定しましょう。

5 個人情報の重要性を意識！

個人情報を悪用されて事件に巻き込まれるなどのトラブルが多発しています。個人情報詐取目的のアプリもあるので、公式サイト以外からのアプリのダウンロードは控えましょう。また、スマホで撮影された写真には位置情報が埋め込まれている場合があります。写真提供やネットに掲載する場合は、その情報を削除しましょう。

6 アプリのダウンロードは正規のサイトで！

アプリの不正コピーは違法であり、民事だけでなく、刑事処罰の対象になります。大学においても不正行為により懲戒処分の対象となりますので、海賊版をダウンロードはしてはなりません。また、ファイル共有機能を有するP2P通信ソフトウェアの使用は禁止です。

7 Twitter、LINE等のソーシャルメディアでの不必要な発言は控える！

ソーシャルメディアでの発言は一瞬で世界中の人に伝わります。違法行為（未成年の飲酒・喫煙等）や迷惑行為（アルバイトでの不適切な行動等）を投稿して問題となったケースも多く見受けられます。また、こういった事件を発生させたことで本人の将来（就職）にも悪影響を与えます。

自分の情報は自分で守ろう！

熊本大学 Kumamoto University

8 スマホ決済の利用に注意！

スマホ決済アプリ事業者を装った偽のSMS（ショートメッセージサービス）から、フィッシングサイトに誘導される事例が報告されています。誘導先のフィッシングサイトでは認証情報と、クレジットカード情報などの入力を求められます。誘導先で情報の入力などを促すメッセージを受信した場合は安易に信用せず、正規の案内かどうか真偽を確認するようにしましょう。

9 ネット上の誹謗・中傷・デマに注意！

他人や団体、会社などを誹謗中傷するような書き込みはやめましょう。悪質な書き込みは、刑罰（名誉毀損罪・侮辱罪等）に当たることがあります。

また、ネット上には誤った情報や偽の情報もたくさん掲載されていますので、安易に信じたりせず、また、むやみに拡散するようなことはやめましょう。

10 インターネット上の情報の活用、レポートの作成には著作権に留意！

レポートや研究論文等において、活用する情報をインターネットや書籍から引用する場合には、著作権に留意してください。不正に利用した場合には著作権違反で訴訟を起こされる可能性があります。

USBメモリや印刷物等の利用

熊本大学 Kumamoto University

11 USBメモリやSDカードの利用後は速やかにデータを削除！

携帯電話やスマートフォン等に比べて、USBメモリやSDカードは不用意に扱われる傾向があります。携帯する場合は肌身離さず持つことは当たり前ですが、もしもの場合に備えて、使用後のデータは削除しましょう。

12 印刷物もしっかり管理！

デジタルのデータだけでなく、印刷物の紛失・盗難も個人情報の漏えい等において問題になります。
印刷した場合には速やかに回収してください。また、机の上等に置きっぱなしにしないようにしましょう。

13 インシデント発生時は速やかに報告！

インシデントとは、「マルウェア感染、パソコンやUSBメモリ・印刷物の紛失等情報漏えいなどに繋がる可能性のある事柄」をいいます。
こういった事象を学内で発見した場合には、直ちに指導教員(又は教務担当)と総合情報統括センターヘルプデスクに報告してください。

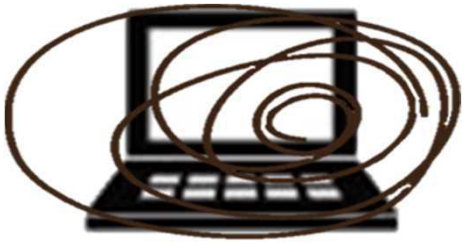
情報セキュリティインシデント発生時

熊本大学 Kumamoto University

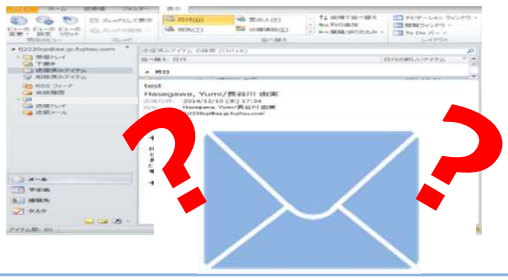
インシデントかな？　と思ったら…

セキュリティ対策ソフトからの通知

パソコンが誤動作する



身に覚えのないメールの送信履歴がある



緊急時の対応方法（パソコン室）

① パソコンをシャットダウンする
② 直ちに教務担当とヘルプデスクに報告し、指示に従う

緊急時の対応方法（研究室パソコン）

① パソコンは、LANケーブルを抜く
② 直ちに指導教員とヘルプデスクに報告し、指示に従う

【通報窓口】
- **総合情報統括センター　（ヘルプデスク）**
  096-342-3949（security@kumamoto-u.ac.jp）

2020年10月発行