熊本大学 情報セキュリティポリシー

ポイントセレクション 2014

私たちの日常生活の中で、今やパソコンやスマートフォンは必要不可欠なものとなり、
インターネットを使わない生活は考えられなくなりました。
しかし、インターネットには、便利であるが故に**情報漏洩**をはじめとする
さまざまな**情報セキュリティのリスク**も潜んでいます。
また、パソコン等を使用する際に利用しているUSBメモリーや電子メールなども、
便利なアイテムですが、使い方を一歩間違えると**ウイルスの侵入経路**となり、
私たちを脅かすものへと変わります。
本学では、本学情報システム及び情報資産を適切に管理・運用して、
情報セキュリティインシデントの脅威から私たちを守るために
「熊本大学情報セキュリティポリシー」を平成22年5月21日に策定しております。
今回は情報セキュリティポリシーの中でも
皆さんに特に守っていただきたい項目をピックアップしましたので、
是非実行して楽しいインターネット生活を送りましょう。

1 アカウント・パスワードは、他人に知られないよう注意しよう！

（情報システム利用規則第6条）

重要

★自分のアカウントを他者に使用させないこと
★他者のアカウントを使用しないこと
★パスワードを適切に管理すること

ポイント

パスワードに使用する文字列（利用者パスワードガイドライン）

1. **８文字以上が大原則！** 一文字増えると格段に強固になる。
2. **英大文字**（Ａ～Ｚ）、**英小文字**（ａ～ｚ）、**数字**（０～９）、**記号**（@!#$%&=-+*/.,:;[]¦~<>?等）を**３種類以上組み合わせる。**
3. 有名人の名前、辞書の見出し語はそのまま使わない。
4. 自分や家族の名前・生年月日、自分のユーザIDは使わない。

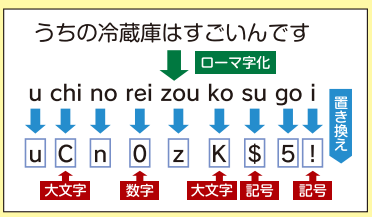
ちょっと参考

安全なパスワードの作り方

1. システム毎に異なるパスワードを自分で作る。
2. パスワードの使いまわしはしない！

（例）① 元となる文章を考える。
② ローマ字で書き出す。
③ 母音を抜く、数字や記号におきかえる。
④ システム毎の略称を付加する。

uCn0zK$5!Fb（facebookのパスワードだから最後にFb）
kPuCn0zK$5!（熊大ポータルのパスワードだから最初にkP）



IC学生証・IC職員証について

- IC学生証・IC職員証を紛失した場合、他者に使用された場合は、所属の学部、部局等の事務室に届け出て下さい。
- IC学生証・IC職員証を拾った場合は、最寄りの事務室等に届けて下さい。

ICカードの被害について

IC学生証、IC職員証に限らず、ICチップが組み込まれたカードには、たくさんの情報が書き込まれていて、これを読み取られる被害（スキミング被害）も報告されています。銀行ATMカード、クレジットカード、電子マネーカード等も同様です。なりすまして使用された場合の被害は大きなものになりますから、取り扱いには注意しましょう。

2 情報セキュリティ研修は必ず受講しよう！

（情報システム利用規則第8条）

重要 ★本学情報システムの利用に関する教育を、毎年必ず受講すること

ポイント

今年も実施！

情報セキュリティeラーニング研修

教 職 員：**平成26年8月25日(月)開講予定**

学　　生：**平成26年10月6日(月)開講予定**

受講方法：eラーニングシステムにアクセスして受講してください。

「熊本大学ポータル」→「全学LMS (e-Learning System) Moodle」→「研修(14後)」→「熊本大学 情報セキュリティ 2014」

※開講期間、注意事項等は、別途メールにてお知らせします。
なお、**受講率は、学部や部局毎に集計して公表**します。

ちょっと参考

情報漏えいの傾向

情報漏えいの約80%は、管理ミス、誤操作、紛失・置き忘れなどの「ヒューマンエラー(人の不注意)」が原因で発生しており、発生経路の約70%は、技術的な対策が講じにくい場面(人が守らなければならないこと)で発生しています。

つまり、セキュリティポリシーを遵守していれば、発生しなかった漏えいと言えます。

情報漏えいの原因	
1位	**管理ミス**
2位	**誤操作**
3位	**紛失・置き忘れ**
4位	盗難
5位	不正な持ち出し

情報漏えいの経路	
1位	紙媒体
2位	可搬記憶媒体
3位	電子メール
4位	インターネット
5位	PC本体

3 ハラスメント、個人情報保護及び守秘義務に違反しないように注意しよう！

（情報システム利用規則第11条）

重要 ★差別、名誉毀損、侮辱又はハラスメントにあたる情報の発信をしないこと
★個人情報又はプライバシーを侵害する情報の発信をしないこと
★守秘義務に違反する情報の発信をしないこと

事例 **ブログへのコメント書き込みについて**

本学でも、学生がブログに不適切な書き込みをしたとして、学外から謝罪を求められた事案がありました。

インターネットの世界は、匿名性が通用すると思っていませんか？ でも、サーバのログをたどれば、IPアドレスは簡単に判りますし、プロバイダは司法機関からの要求があれば、誰がそのIPアドレスを使って通信したのかを特定して、その利用者の情報を提供します。 あなたの身元は、難なく特定されることでしょう。

価値観は人ぞれぞれ。 何でもないと思っていることが、人によっては心に暗くのしかかるようなことだったりします。ましてや、明らかに誹謗中傷するような内容はいけません。

情報の発信は、あなたの人生に深刻な爪痕を残すかもしれませんから、後々の影響を考えて、くれぐれも慎重に！

ポイント

熊本大学ソーシャル・メディア・ガイドラインから

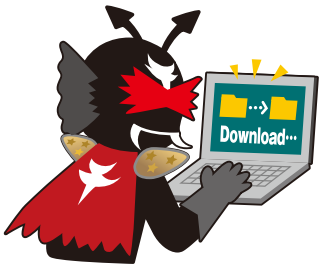
本学の構成員(学生・教職員)であることを明示してソーシャル・メディアを使用する場合、**発信内容は個人の見解であり、本学の立場や意見を代表するものではない旨を記載**して下さい。

4 著作権を侵害しないように注意しよう！

（情報システム利用規則第11条、第12条）

重要

★著作権等の財産権を侵害する情報の発信をしないこと
★通信の秘密を侵害する行為をしないこと
★正規のライセンスを受けていないソフトウェアの利用及びこれを助長する行為をしないこと
★P2Pソフト（ファイル共有ソフト）を使用しないこと



事例

日本音楽著作権協会（JASRAC）からの苦情

Bit Torrent、Share、迅雷、Cabos等のP2Pソフトをインストールして使用していると、自分が知らない間に音楽著作物を違法に送信する場合があります。これを発見した日本音楽著作権協会（JASRAC）から、本学に著作権侵害の苦情が寄せられたことがあります。

違反者は、IPアドレスなどから容易に特定され、悪質な場合には損害賠償や著作権法違反による摘発の対象になる可能性もあります。注意しましょう。

ポイント

バンドル（抱き合わせ）ソフトに注意！

P2Pソフトウェアは、他のソフトウェアをダウンロードした時にいっしょにダウンロードされることがあります。インストールの時に、ついつい「OK」を押してしまうとインストールされてしまいます。「OK」を押す前に、十分注意しましょう。

また、**常に自分のPCのソフトウェアの状況を把握**しておいてください。

5 知らないメールに注意しよう！

（情報システム利用規則第14条）

重要

★電子メールの利用に際しては慎重に行い、マナーについても配慮すること

ポイント

電子メールの怖いところ

とっても便利な電子メール。これがないと生きていけないという人も、大袈裟ではなくいますよね。でも、使い方を間違えるととんでもないことになります。

まず、個人情報の漏えいは、電子メールの誤送信のような単純なミスで起きてしまうことも多いのです。また、ウイルスの侵入経路となりがちなのが「添付ファイル」。そして、ついついクリックしてしまうのが「リンクURL」。フィッシング詐欺サイトなど危険なサイトに誘導されることもめずらしいことではありません。

「何か変だな」と思ったら直ちにマウスから手を離し先に進むことを止めましょう！落ち着いて考えることが大切です。

ちょっと参考

標的型メール攻撃に注意！

最近のサイバー攻撃の中で、特に注意を要します。知り合いや関係者を装い、いかにもありそうな内容のメールを送りつけてきます。

わずかでも不審な点があったら、一切反応しないことが重要です。知り合いや関係者の連絡先をあらかじめはっきりと知っている場合は、必要に応じてメールとは別の手段（電話等）で不審な点を確認するなど、慎重に対処しましょう。

6 モバイルPCはウイルスに注意しよう！

（情報システム利用規則第16条）

ちょっと参考

重要

★モバイルPCを本学情報システムに接続する場合は、ウイルス対策ソフトを必ず導入すること

★OS（オペレーティングシステム）の更新を必ず行うこと

ポイント　ウイルスに感染したと感じたら

1. **ネットワークケーブルを抜く、無線LAN機能をOFFにする**など、PCを接続しているネットワークから切り離す。
2. **PCをシャットダウンしたり、再起動したりせずに、そのままの状態で総合情報統括センターに連絡**する。

F-Secure（エフセキュア）が無料で使えます

F-Secureは、本学の学生・教職員が無料で利用できるウィルス対策ソフトです。

熊本大学がサイトライセンス契約を結んでいるので、学内でも、自宅でも、個人所有のＰＣを含めて利用できます。

F-Secureは、「熊本大学ポータル」→「サイトライセンスソフト・ダウンロードシステム」からダウンロードできます。

Windows 用以外に、Mac OS用やLinux用もダウンロードできます。

F-Secure（ウィルス対策ソフト）に関するお問い合せは、総合情報統括センターヘルプデスク（内線3949）まで。

ポイント　PCは最新の状態に

1. Windows等の**OS**、Internet Explorer等の**ソフトウエア**、ウィルス対策ソフトの**パターンファイル**などは、**常に最新の状態**にしておきましょう。
2. **アップデートは、設定を「自動更新」**にしておくと安心です。

事例　個人用PCが利用されて加害者に

「熊本大学から大量の迷惑メールが来ている!!」、「サーバに不正アクセスを受けた!!」と、被害を受けた個人や団体より本学に苦情が寄せられた事例がありました。

本学では、全学無線LANに接続したPCのアクセス記録を調べ、１台の個人用PCにたどり着きました。ＰＣはウイルス対策ソフトが導入されておらず、これが原因となってウイルスに感染し、大量のメールやサーバへの不正アクセスをくり返していました。

PCの所有者は、「自分が加害者になるとは夢にも思っていなかった」と呆然としていましたが、当然ＰＣの所有者には厳重な注意が言い渡されました。

本人に悪気はなくても、意思とは関係無く不特定多数の人々に多大な迷惑をかけることにより加害者となります。セキュリティ対策は、一人ひとりの社会的責任と考えましょう。

インシデント通報窓口　（情報システムにおけるインシデント対応手順3）

通報窓口

総合情報統括センター

内線3949（ダイヤルイン096-342-3949）平日／9:00～17:00

e-mail による連絡は、security@kumamoto-u.ac.jp

※学生は、まず最初に各学部等の窓口に通報してください。

熊本大学 Kumamoto University

発行／総合情報統括センター
情報セキュリティ室
2014.8