「気付かない」が恐ろしい！

長崎大学では，学生のパソコン必携化が平成 26 年 4 月からスタートして，私たちの勉強に，趣味に，生活に，パソコンやスマートフォンが活躍の場を広げています。しかし，その裏で私たちが気付かない間に，いろいろな脅威が忍び寄っています。
たとえば，スマートフォンに保存した個人情報が外部に送信されたり，自分のパソコンやスマホが遠隔操作されたりなど，ひとたび起これば，自分だけでなく，色々な人に迷惑をかけてしまいます。そうならないために，日々の生活の中で情報セキュリティ対策を実践することが重要です。このパンフレットでは，すぐに始められる 7 つの対策を紹介します。

このパンフで紹介する７つの対策

1. セキュリティホールをふさごう
2. セキュリティ対策ソフトは最新に
3. ID とパスワードを適切に使おう
4. フィッシング詐欺への対策
5. サポート詐欺への対策
6. 生活上の盲点に気をつけよう
7. SNS，気をつけて使おう

それでも困ったときにはココに相談

ICT 基盤センター（center☆ml.nagasaki-u.ac.jp）
☆を@に変更して下さい。

1. セキュリティホールをふさごう

現実 **ウイルスなどは OS やアプリの脆弱性が大好き**

これまで世間を騒がせたマルウェア[*1]は，オペレーティングシステムやアプリケーションソフトの脆弱性をついてきますが，その多くはパッチ[*2]をキチンと適用していれば防げたといわれています。最近は無線 LAN のアクセスポイント等の機器の脆弱性もよく狙われています。

対策 **OS やアプリ等を確実に最新の状態にしましょう！**

この対策はパソコン，スマートフォン，タブレット他ネットワークに接続される機器に共通です。パソコンの場合，自動的にアップデートが行われるものもあります。

- Windows Update（毎月第 2 水曜日もしくは第 3 水曜日）
- Adobe Acrobat Reader など Adobe 製品（不定期）
- Google Chrome や Mozilla Firefox などのブラウザ（不定期）

どのソフトが最新の状態にあるか，よく分からない人は，MyJVN バージョンチェッカ[*3]を利用しましょう。
スマートフォンやタブレットの場合は，App Store や Play ストアにアクセスして，アップデートがないかをチェックするようにしましょう。

[*1] マルウェア（Malware）：有害な機能をもったプログラムの総称。ウイルス，ワーム，トロイの木馬などに分類されます。

[*2] パッチ：ソフトウェアのベンダー（開発元）から配布される修正プログラム

[*3] MyJVN バージョンチェッカ：Windows のパソコンを対象に，脆弱性を悪用されやすいソフトが最新かどうかをチェックするアプリです。以下のサイトからアクセスできます。
https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html

2. セキュリティ対策ソフトは最新に

現実　**セキュリティ対策ソフトをインストールしているのに，定義ファイルの更新などがいい加減**

セキュリティ対策ソフトをインストールしたのに，定義ファイル[*4]が日々更新できていなかったり，自 PC 内をまったくスキャンしていなかったり，ましてや定義ファイルの更新可能な期限を過ぎてしまっているケースがあります。これでは，残念ながらセキュリティ対策になっていません。

対策　**毎日定義ファイルを更新しましょう！**
週に１回以上はウイルスチェックしましょう！

パソコンは言うに及ばず，スマートフォンやタブレット（特に Android）も必須です。
Windows8.1 以降であれば，Windows Defender で最低限の対策をとることができます。

注意　**スマートフォンやタブレットのセキュリティ対策**

（特に Android の）スマートフォンを購入したときには，セキュリティ対策の契約[*5]をしているかチェックしましょう。契約していなければ，迷わずスグに市販のセキュリティ対策ソフトを買ってインストールしてください。タブレットの場合もスマートフォンと同様の対策が必要です。

[*4] 定義ファイル：マルウェアの特徴を書いたファイルで，日々新たなマルウェアが登場するので，毎日更新しなければなりません

[*5] スマートフォンのセキュリティ対策サービスの例：安心ネットセキュリティ（au），あんしんセキュリティ（ドコモ），セキュリティパックプラス（ソフトバンク）など

3. ID とパスワードを適切に使おう

現実　**数種類のパスワードを使いまわしたり，簡単なパスワードを使ったりと，管理がいい加減**

ID とパスワードが第三者に知られて，成りすましにあう事件が数多く起きています。脆弱な Web のサービスから ID・パスワードが漏えいして，他のサービスにログインするパスワードリスト攻撃も盛んです。

対策　**多要素認証が利用できる場合でも，同じパスワードを使い回さず，他人に分かりにくいものを使うようにしましょう**

以下を参考にパスワードを適切に管理・利用するようにしましょう。

（1） 推測しにくいパスワードを使う

- 大文字・小文字・数字・記号の組み合わせ
- 長いパスワード（マイクロソフト社は 14 文字以上を推奨）
  - 自前の変換ルールを作ってパスフレーズを変換

（2） 管理ツールや自分だけのメモを用いパスワードを適切に管理する

（3） パスワードは絶対に人に教えない（知られたら直ちに変更）

（4） パスワードの使いまわしをしない（サイトごとに異なるパスワードを）

注意　**簡単なパスワードは一瞬で解読されます**

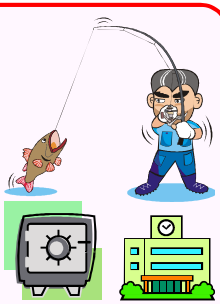
右表はパスワードの解読時間です。文字の種類が多く，桁数が長い方が安全です。

パスワードの桁数	4桁	6桁	8桁	10桁
英小文字　(26字)				
ZIP	1秒以下	1秒以下	46秒	9時間
ZIP(256bitAES)	1秒以下	5分	2日	4年
DOC	1秒以下	26秒	5時間	136日
DOCX	20秒	44分	105日	195年
英大小文字＋数字　(62字)				
ZIP	1秒以下	13秒	13.5時間	6年
ZIP(256bitAES)	14秒	15時間	7年	26千年
DOC	1秒以下	1時間20分	211日	2,218年
DOCX	10分42秒	29日	301年	1,158千年
英大小文字＋数字＋記号　(93字)				
ZIP	1秒以下	2分24秒	14日	341年
ZIP(256bitAES)	1分11秒	7日	169年	1,462千年
DOC	6秒	15時間	15年	128千年
DOCX	55分	326日	7,800年	66,726千年

4. フィッシング詐欺への対策

現実 昔からありますが，今も被害が後を絶ちません

最近では，手口や文章が巧妙化しています。大手銀行や大学のメールシステム管理者をかたる**メール本文のリンクから，フィッシングサイトに誘導して ID やパスワードなどの情報を盗み取るケースが知られています。**フィッシングサイトには，公開されているサイトの画像を利用して，本物とよく似たものもあります。



対策 メールの中身を一度疑う！
メールの送信元を安易に信用しないこと！

多くのケースでは，メールや SNS 上のリンクをクリックするなどしてフィッシングサイトに誘導します。少なくとも，以下の点に注意しましょう。これも**パソコンとスマートフォン共通です。**

（1） メールの内容を安易に信用しない

- 緊急，重要，期間限定，あなた限定などと書いてあれば疑った方がいいでしょう

（2） リンクを安易にクリックしない

（3） 入力前に本物のサイトかどうか確認する

- 紛らわしい文字を見分けましょう（lと1，oと0など）
- URL が「https://･･･」となっているか見分けましょう

注意 それでも被害にあった場合

一人で抱え込まずに，家族や大学関係者（教職員や ICT 基盤センターなど），国民生活センター，警察などに相談しましょう！

5. サポート詐欺への対策

現実 近年被害にあう人が増えています

パソコンやスマートフォンで Web サイトの閲覧などをしていると，突然「ウイルスに感染しています」などのニセ警告画面やニセ警告音が出て，それらをきっかけに電話をかけさせ，**有償サポートやセキュリティソフトなどの契約を迫る詐欺行為が増えています。被害者の中には，プリペイド型電子マネーで何回も支払わされたケースもあります。**

対策 まずは落ち着きましょう

（1） 「警告画面や警告音は偽物ではないか？」と疑いましょう

- 警告画面に表示された指示（電話連絡やアプリのインストールなど）に従ってはいけません。

（2） ブラウザの通知機能を許可せずに，ブラウザを終了させましょう

（3） スマホアプリのカレンダー（主に iPhone）への不審な書き込みがあったら，照会をタップしないでください

- (2)と(3)表示にしたがってリンクをクリックすると，不審なサイトに誘導されるかもしれません

（4） 一人で対応するのが難しい場合には，周りの人に相談しましょう

注意 それでも被害にあった場合

一人で抱え込まずに，家族や大学関係者（教職員や ICT 基盤センターなど），国民生活センター，警察などに相談しましょう！

6. 生活上の盲点に気をつけよう

現実

ニセの電話からゴミ収集まで，生活上のスキをついて情報が盗まれる被害が起きています

情報を盗む手法は様々ですが，私たちの日常生活で，いつどこで起きてもおかしくありません。日常生活では，下図の例のように様々なやり方で，不正に知られる可能性があります。

他人に成りすまして電話

ごみ収集等を装う

貼紙を覗き見る

対策

日々注意して生活することが大事です！

- 電話の場合，「折り返し電話する」などと言って電話を切り，その場で対応しない
- ゴミを捨てる場合，書類をシュレッダーにかけたり，大事な情報が書かれた箇所を黒く塗りつぶしたりして，読めないようにしてから捨てる
  - ✧ 特に個人を特定できそうなものを捨てる時は確実に処置することを強くお勧めします
- 覗き見防止のため，大事な内容が書いたメモを人目につくところに貼らない
- USB メモリは紛失に気をつけるとともに，重要な情報を保存しない

7. SNS，気をつけて使おう

現実　**SNS でのプライバシー設定の不備や不適切なやりとりから，トラブルや犯罪に発展することがあります**

Facebook や twitter を利用するとき，公開設定が不適切だと，自分だけでなく家族や友人のプライバシー情報をネットに晒して，思いもよらないトラブルに巻き込まれます。また，最近では SNS 上で「高収入で簡単なバイト」などと称して犯罪の共犯者を募集する，「闇バイト」が増えています。

対策　**情報の公開範囲に関する設定を確認しましょう。また，不審な情報や誘いに乗せられないようにしてください**

以下に日常生活に役立つ注意点[*7]を紹介します。特に**スマートフォンから気軽に利用できるので，より注意を払うようにしましょう。**

(1)　常に公開・引用・記録されることを意識して利用しましょう
(2)　複雑なパスワードを設定し，セキュリティを高める工夫を行いましょう
(3)　公開範囲を設定し，不必要な露出を回避しましょう
(4)　知らない人とむやみに“友達”にならずに，知っている人でも本人かどうか確認しましょう
(5)　SNS の“友達”に迷惑をかけない設定を行いましょう
(6)　“友達”からの削除は慎重にして，制限リストなどの利用も考えるようにしましょう
(7)　写真の位置情報やチェックインなど，技術的なリスクを正しく理解しましょう
(8)　むやみに”友達”のタグ付けや投稿をしないようにしましょう
(9)　「闇バイト」など，不審な情報を見たら身近な人や警察に相談しましょう

[*7] (1)～(8)は日本ネットワークセキュリティ協会，「ＳＮＳの安全な歩き方～セキュリティとプライバシーの課題と対策～」（公開 2012 年 11 月 1 日）より引用しました。