# 情報処理概論

**コンピュータ・ウイルス**

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの

自己伝染機能、潜伏機能、発病機能

**マルウエア**　（「マル」は Malicious、悪意のあるという意味）

マルウエアの症例

画面の表示がおかしく　データの破壊　異常な動作　情報流出　ネットワークからの侵入可能に

以前は愉快犯的なもの、今は情報入手や金銭獲得、組織活動の妨害などより悪質なものに

- ランサムウェア

ファイルを勝手に暗号化したり、PC をロックするなどで使用不能に

⇒ 元に戻すことを条件に金品を要求

- ボット

ボットに感染した多数の PC に対し一斉に攻撃指示を出し、企業等のサーバにアクセス（DDoS 攻撃）

DDoS 攻撃：特定のメールサーバや Web サーバに大量のアクセスを行い、そのサーバの機能を麻痺させる攻撃を DoS（Denial of Service）攻撃という。更に、これを多数の PC 等から同時に行うのが DDoS（Distributed DoS）攻撃

- バックドアの設置

**マルウエアの感染**

何らかの形で悪意のあるプログラムが実行（それ以外の場合も）

● 危険なファイル

・内容がプログラムであるファイルには注意が必要（拡張子が exe、pif、scr、bat、com）

お知らせ.doc
お知らせ.exe
お知らせ.doc　　.exe

・マクロウイルス

Word や Excel 等にも、その上で実行される特殊なプログラム（マクロ）が存在する。

マクロを含む Word 文書ファイル
マクロなし　docx、マクロあり　docm（Word 2007 以降）

・pdf ファイルでもウイルスが

pdf ファイル：ワープロソフトや表計算ソフトなどのデータを、印刷のイメージで圧縮したファイル
pdf ファイルを見るには Adobe Reader というソフトが必要。Adobe Reader の脆弱性を突く。

・画像ファイル（拡張子は jpg 等）でも同様の危険性

・RLO（Right-to-Left Override）ウイルス

filefdp.exe　を　file[RLO]fdp.exe とすることにより fileexe.pdf　に

・ショートカットウイルス


ショートカットファイル：ダブルクリックすると、アプリケーション・ソフトが起動
実態は、ショートカットファイルと呼ばれる拡張子 lnk のファイル
コンピュータに対する簡単な操作を指示するスクリプトが含まれ、それが実行

**様々な感染経路**

● USB メモリ等からの感染

● メールからの感染

メールの形式

基本的にはテキスト形式で

HTML 形式の場合は、後述する Web の場合と同様の危険性が

リッチテキスト形式程度ならば大丈夫？

● Web からの感染

・安易なダウンロードは危険

トロイの木馬

アドウェア、スパイウェア

クッキー（Cookie）とは

Web サイトを訪れた際、ブラウザを通じて記憶される情報

トラッキング・クッキーはどの Web ページを訪れたかなどの情報 ⇒ これを集めれば個人情報？

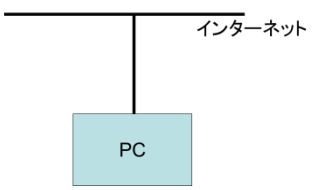
・Web ページを表示しただけで感染

Gumblar（2010 年頃）

正規の Web サイトを改ざんし、不正な Web サイトに誘導（改ざんされた Web ページで感染も）

偽の警告も大流行

● ネットワークに接続しただけで感染




**対策**

● データのバックアップ

● PC を感染しにくい状態に

・OS やアプリケーション・ソフトの問題点（脆弱性）を修正

開発元の提供するセキュリティ・パッチの利用

Windows の場合は Windows Update

通常はシャットダウンメニューに「更新してシャットダウン」等と表示

手動の場合は、①スタートボタン、②設定、③更新とセキュリティ、

④Windows Update を選択、⑤更新プログラムのチェック

再起動が必要な場合も

詳細オプションで「自動（推奨）」に、

「Windows の更新時に他の Microsoft 製品の更新プログラムも入手します。」にチェック

Update には期限が

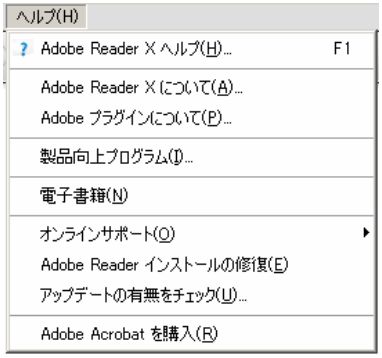
・Windows XP 以前は既にサポート終了

・Vista は 2017/10/10 まで、7 は 2020/1/14 まで、8/8.1 は 2023/1/10 まで

アプリケーション・ソフトでも更新作業（セキュリティ・パッチ）が必要

多くのソフトで自動更新機能

手動で行いたい場合は、ヘルプのメニューに




今危ないのは drive-by download

利用しているソフトの脆弱性を突いて

勝手にマルウエアをダウンロードする手口

OS、ブラウザ、Adobe Reader、Adobe Flash Player など

中には OS 等の自動アップデート機能を無効にするものも

⇒ 定期的に手動でアップデートを（これがうまくできない場合は感染の可能性）

ゼロデイ攻撃も

脆弱性が判明してから、修正プログラムが提供される間に感染

脆弱性に対する回避策の提示 ⇒ メールマガジンを利用

マイクロソフト http://technet.microsoft.com/ja-jp/security/cc307424.aspx

情報処理推進機構 http://www.ipa.go.jp/about/mail/

・ウイルス対策ソフトの導入

利用することは当然の義務

ウイルス情報を最新のものに更新、定期的なスキャンも

ウイルス対策ソフトの契約期間を過ぎると最新情報の入手ができなくなるので、その場合は契約更新もしくは新規導入が必要

ウイルス作成ツールなども存在し、ウイルス情報が間に合わない場合も

ウイルス対策ソフトを欺くこんな手口も（ZIP ファイルの利用）

・ZIP ファイル

複数のファイルを一つのファイルにまとめ、更にその容量が小さくなるように圧縮ということを行ったファイル（この講義で使っている「練習用ファイル.zip」もこれを利用）

単にマルウエアを ZIP ファイル化するだけならばウイルス対策ソフトも対応できるが

そうは言っても

● 日常的な対策

・メールの場合は添付ファイル（送信元の偽装にも注意）

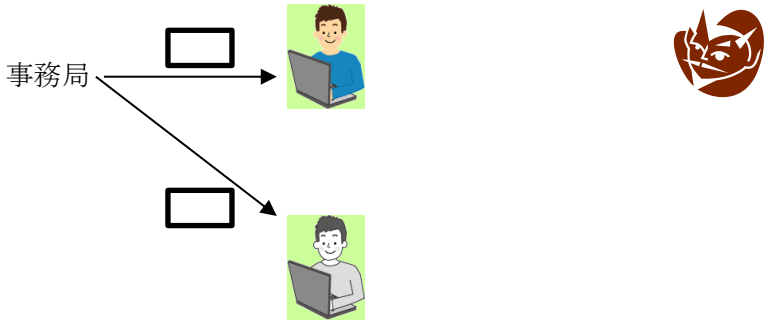
・メールの利用はテキスト形式で

・怪しげなプログラムやファイルを開かない（有用なファイルや、有名なファイルを装うことも）

・怪しげなホームページを見ない

など、常にマルウエアに対する注意を（ただし、この部分はドンドン巧妙化）

● 持続的標的型攻撃



・水飲み場型攻撃

標的とする企業・組織の従業員がアクセスしそうな Web サイトを改ざん

標的とする企業・組織の従業員の場合だけ、ウイルスをダウンロード（それも 1 回だけ？）

巧妙なメールによる攻撃あるいは水飲み場型攻撃とゼロデイ攻撃を組み合わされると

対応は不可能？

侵入を前提とした社内ネットワーク作り

企業側の対策

・サンドボックス

・クラウド型

**不正なアクセス**

・マルウエアだけでなく、様々な外部からの不正なアクセスに対応する必要

⇒ ファイア・ウォールの設置（PC レベルではパーソナル・ファイア・ウォールソフトの導入）

ウイルス対策ソフトには、この機能を併せ持っているものが多い

（ウイルスバスター、 Norton Internet Security など）

ブロードバンド・ルータ（家庭内にある複数の PC がインターネットに接続する際に用いる装置）

の設置も有効（ファイア・ウォールの機能も併せ持っている）

**パスワードの設定も重要**

全てのユーザ アカウントにはパスワードの設定を（特に管理者の権限があるものは必須）

パスワードは、8 文字以上で、大文字・小文字・数字・記号の混入

簡単に類推されないもの

定期的に変更するのが有効

**もしマルウエアに感染したら**

まずは感染の拡大防止

・ネットワークの切断（ケーブルを引き抜く、無線 LAN 機能を off、ダメなら親機を off）

・その PC で利用した USB メモリ等は利用しない

・電源はそのままで、コンピュータに詳しい人、ウイルス対策ソフトメーカ等に連絡

**マルウエアには感染しないことが一番重要**

ウイルス対策ソフトは、感染した状況に対応するものではなく、感染しないようにするもの

**フィッシング（phishing）**

実在する企業の Web サイトに見せかけたサイトへ、メールなどを使ってユーザーを誘導し、クレジットカード番号などを入力させて盗む

（詳細はフィッシング対策協議会 http://www.antiphishing.jp/などで）

**スピアフィッシング（spear phishing）**

**今までの話は現時点で分かっているもの　　今後は更に別の手口も**