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、単独ではなく、他のファイルに寄生し、自己増殖機能を持つもの

ワーム（ウイルスのように寄生はせず、単独で増殖）

トロイの木馬（他のアプリになりすまし、自己増殖はしない）

マルウェア　（「マル」は Malicious、悪意のあるという意味）

マルウェアの症例

データの破壊　情報流出　ネットワークからの侵入可能に　仮想通貨等のマイニング

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

感染した PC に何かをするのではなく、ネットを通じて外部からの指示により活動

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

ネットワークを通じて、自由にその PC に入り込めるようにすること

マルウェアの感染

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）

マクロを含む文書ファイル等を開くと、警告

・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。
マルウェアに感染した pdf ファイルを表示する際に、勝手にファイルをダウンロード
Adobe Reader の脆弱性を突く。

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

もっとも危ないのは添付ファイル

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 ページを見ただけで感染

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

Web の閲覧をしている際に「警告 あなたのコンピュータでウイルスが検出されました。」

などの警告メッセージが

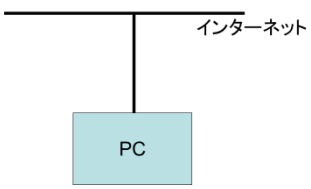
● ネットワークに接続しただけで感染

通常は、外部から侵入できない（鍵がかかっている）

ある入口について鍵の壊し方が判明

それを利用して PC に侵入

感染（Blaster、Sasser）



Windows Update、ファイア・ウォール

対策

- データのバックアップ

  常時バックアップと離散的バックアップ

- 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

以前の Windows では Update に期限が（Windows Vista 以前は既にサポート終了）
・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ェ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、修正プログラムが提供されるまでに行われる攻撃

脆弱性等の情報のブローカーや市場も

・セキュリティソフト（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
セキュリティ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

Windows Defender は？

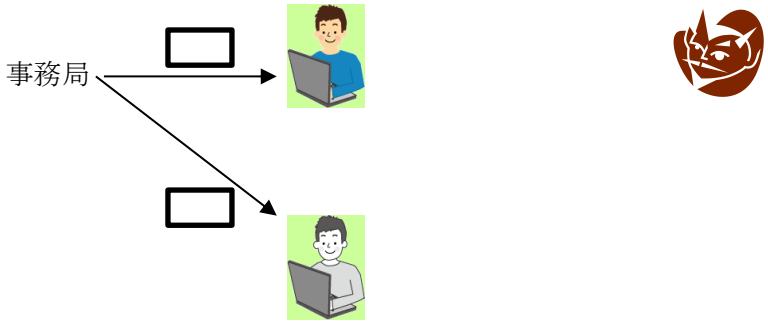
● 日常的な対策
・メールの添付ファイル（送信元の偽装にも注意）
・怪しげなプログラムやファイルを開かない
・怪しげなホームページを見ない
など、常にマルウェアに対する注意を（ただし、この部分はドンドン巧妙化）

マルウェア「EMOTET」被害が昨年 10 月頃から拡大
・バックドアの設置や情報漏洩
・勝手にファイルをダウンロードする機能もあるため、ランサムウェア等への感染も
・内部データを使って他者への感染拡大
・メールの添付ファイルが中心（マクロを含む Word の文書ファイル）
・知人が感染すると、その知人宛のメールに対する返信という形で送られてくることも

● 持続的標的型攻撃

バラマキ型ではなくターゲット型

ターゲットを狙うのに、何段階も経て



・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？

最近は RAT（Remote Access Tool）を使った手口も

企業側の対策

・サンドボックス

外部から受け取ったプログラムを特定の保護された領域で動作させ、マルウエアか否かを判断

・クラウド型

メールや Web の閲覧を、必ずセキュリティ会社のコンピュータを介して行うという方法

侵入を前提とした社内ネットワーク作り

不正なアクセス

・マルウェアだけでなく、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）

セキュリティ対策ソフトには、この機能も

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つ）

ただし、新たな問題も（ブロードバンド・ルータそのものがターゲットに）

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）

ブロードバンド・ルータや IoT 機器にも

パスワードは人に教えたり、使い回しをしない

パスワード管理機能の利用も（セキュリティソフト、Edge 等）

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

もしマルウェアに感染したら

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、セキュリティソフトメーカ等に連絡

マルウェアには感染しないことが一番重要

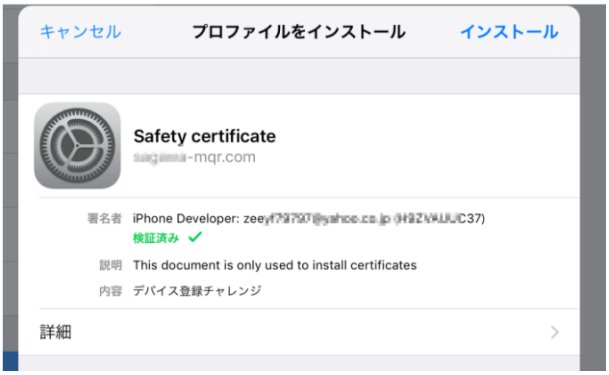
ウイルス対策ソフトは、感染した状況に対応するものではなく、感染しないようにするもの

フィッシング（phishing）

- 悪意ある人物が特定の Web サービスや金融機関にそっくりなニセサイトを用意し、この URL をメールで送りつける。
  - ・ユーザ　アカウントの有効期限が近づいています。
  - ・新規サービスへの移行のため、登録内容の再入力をお願いします。
  - ・セキュリティ強化のため、ログインをお願いします。
  - ・第三者によるログイン試行を確認したので、ログインをお願いします。

- メール上のリンクをクリックすると、本物のサイトのような入力画面へ
- Google や Yahoo!の検索で、上位に表示されるものがフィッシングサイトという場合も
- 本物そっくりのニセアプリや、実在するアプリの便利機能などをよそおったニセアプリ
  SNS へのログイン、個人情報の入力をさせ情報を盗む。

携帯電話事業者サイトを偽装し、iOS 端末に対し不正な構成プロファイルをインストールさせて端末の固有情報を盗む手口の例
サイバー犯罪者がスマートフォン全体を対象として幅広く攻撃している。



スピアフィッシング（spear phishing、spear は槍）

特定の人物を対象としたフィッシング
持続的標的型攻撃などの一環として

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