# A-2.
# マルウェアの脅威と事例

青山学院大学
根本　貴弘





## このセッションの目的

⑩マルウェアの分類と動作を理解する
⑩サイバー攻撃の実例を知る

マルウェアに感染したときの影響をいち早く想像できる

# マルウェアとは？

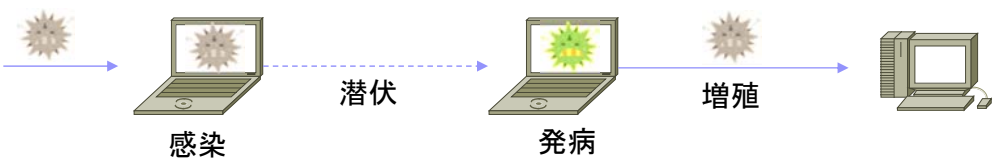
- 不正な動作をすることで，コンピュータやプログラムに対して被害を加える悪意あるソフトウェアの総称
- **malware** = **mal**icious(悪意ある) + soft**ware**
- 様々な種類がある
  - ウイルス
  - ワーム
  - トロイの木馬
  - スパイウェア
  - ランサムウェア等





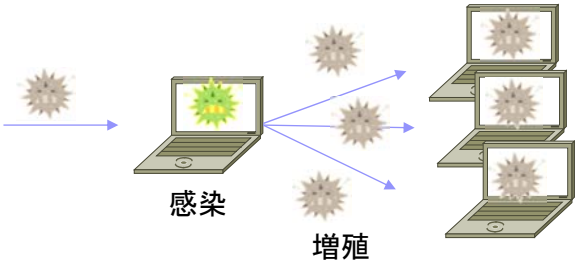
# ウイルス概要

- **自己増殖機能**を持ち，コンピュータやプログラムに対して被害を加えるように作成されたマルウェア
- 特徴
  - 自己増殖
    - 感染PCの機能を用いて（もしくはプログラムを書き換えて），他のPCにウイルスをインストールする
  - 潜伏
    - 感染PC内で一定時間ないし特定の時刻になるまで不正な挙動を示さない
  - 発病
    - 感染PC内の情報の消去，改ざん，外部流出等，利用者の意図しない挙動を行う



# ワーム概要

- **単独**で自己増殖可能で，他のプログラムの動作を妨げたり，利用者の意図しない挙動を示すマルウェア
- 特徴
  - 完全に自己完結したプログラム
    - ホストプログラムやユーザの操作を必要としない
  - 自己増殖
  - データの改ざんや削除等を行うものが多い
  - ウイルスやトロイの木馬と比較して感染速度が早い

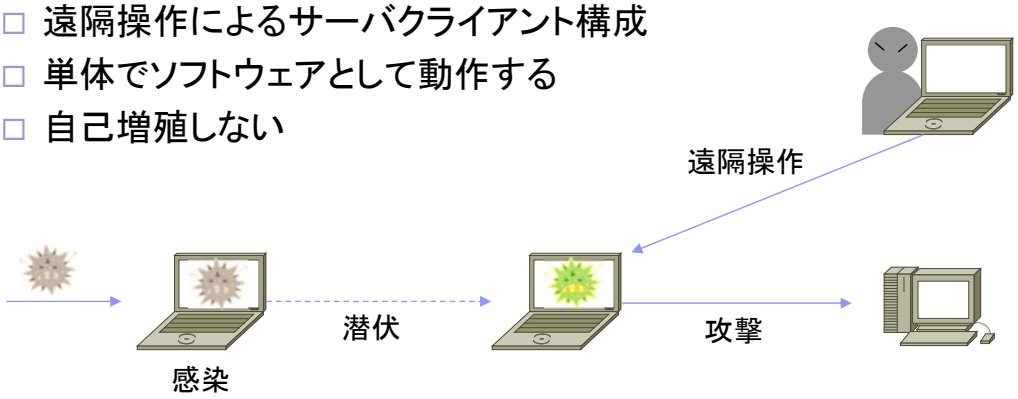







# トロイの木馬概要

- 利用者にとって**有用なソフトウェアを装い**感染PCに潜伏し，破壊活動や情報窃取を行うマルウェア
- 攻撃者による**遠隔操作**によって行動するものもある
  - RAT(Remote Access Tool)と呼ばれることがある
  - 攻撃者側クライアントを**C&C(Command & Control)サーバ**と呼ぶ
- 特徴
  - 遠隔操作によるサーバクライアント構成
  - 単体でソフトウェアとして動作する
  - 自己増殖しない



# トロイの木馬の種類

- **バックドア**型(RAT)
  - インターネット経由で標的PCを不正操作するためのソフトウェア
- **パスワード窃取**型
  - IDやPWなどの情報摂取を目的としたソフトウェア
- **ダウンローダー**型
  - バックドアとなる不正プログラムをダウンロードするソフトウェア
- **ドロッパー**型
  - 不正プログラムが内包されたファイルを感染PCにドロップする
  - ダウンロード型に比べてファイルサイズが大きい傾向にある
- **プロキシ**型
  - ルータやDNSを改変し，PC上に踏み台用プロキシサーバを構築する



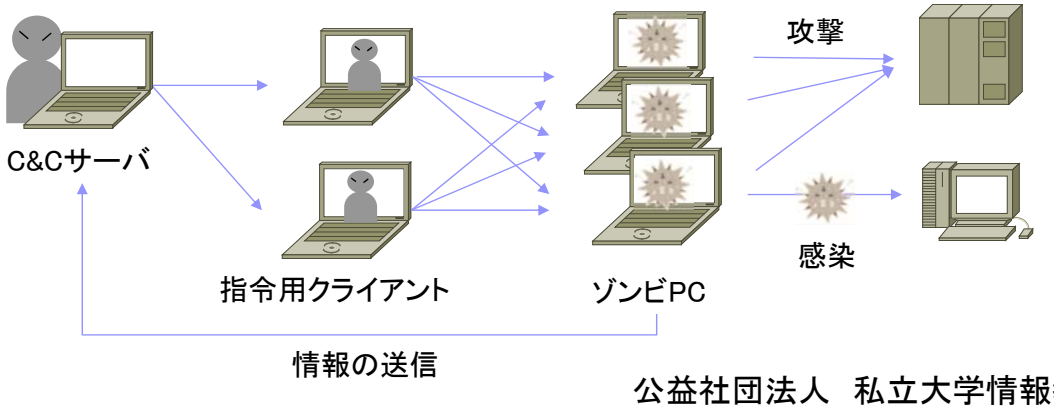


# スパイウェア概要

- 利用者の情報を収集し，**収集した情報を攻撃者に送信するための不正プログラムの総称**
- 特徴
  - 利用者が気づかないようにバックグラウンドで情報収集行う
  - 正規のソフトウェアにも混入している場合がある
    - 利用者情報の収集のため
  - 収集する情報は，ID/PWやプライバー情報等
- 種類
  - システム・モニタ
  - トロイの木馬
  - アドウェア
  - トラッキングクッキー

# ボットネット概要

- ボットと呼ばれるマルウェアに感染したPC等で構成されるネットワーク
  - トロイの木馬等で乗っ取られたゾンビPCで構成されたネットワークも含まれる場合がある
- 数百～数万台で規模で，攻撃者の指示で動作する
  - DDoS攻撃を用いたサイバー攻撃やスパムメール，スパイウェア等に悪用されることがある

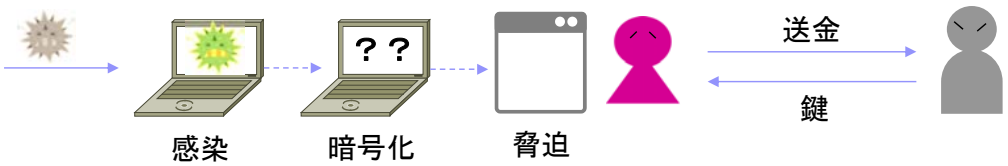






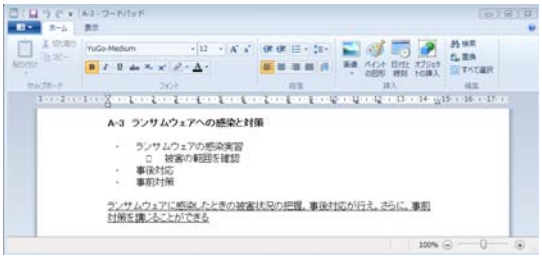

# ランサムウェア概要

- 感染PCの利用に**制限**をかけることで，**身代金の要求**をすることを目的としたマルウェア
- Ransomware = Ransom(身代金) + Software
- 特徴
  - PC利用に制限をかける
    - ファイル暗号化型
    - 端末ロック型
  - 制限解除のためのメッセージが表示される

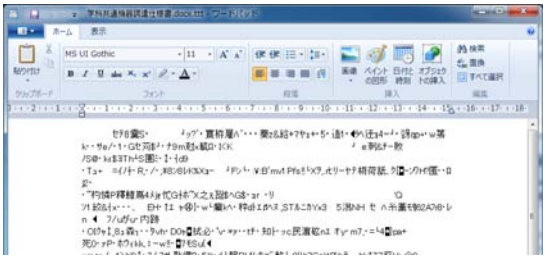


# ランサムウェアによる暗号化

- ランサムウェアの中には感染するとファイルを暗号化するものがある




暗号化前



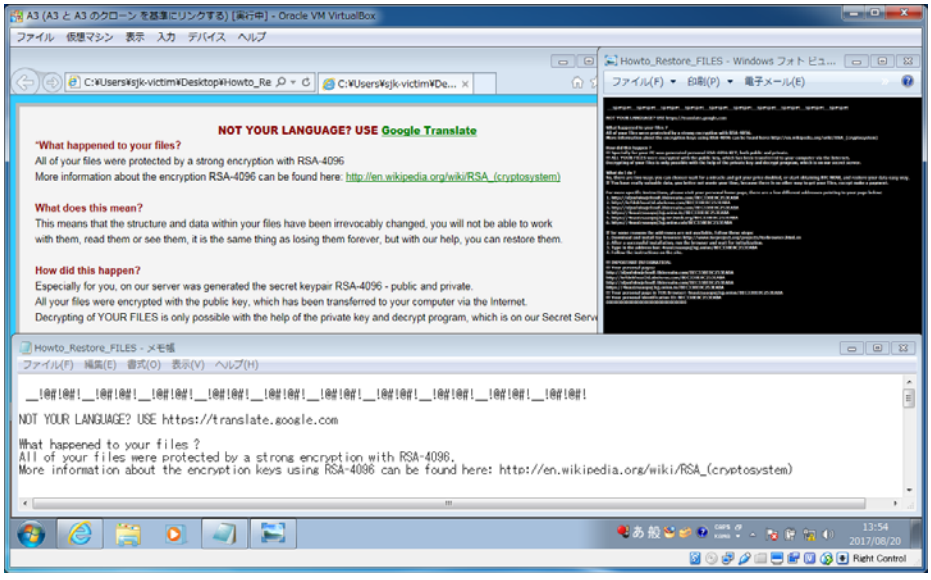
暗号化後





# ランサムウェアの脅迫文

- ランサムウェアに感染すると身代金を要求するための脅迫文が表示される




TeslaCryptによる脅迫文

# ランサムウェアの種別

| No. | 相談初出時期 | 名称 | タイプ | ファイル拡張子 | 日本語対応 |
|---|---|---|---|---|---|
| 1 | 2015年4月 | Crypt0L0cker | ファイル暗号化型 | .encrypted | ○ |
| 2 | 2015年12月 | CryptoWall | ファイル暗号化型 | ランダム文字列 | × |
| 3 | 2015年12月 | TeslaCrypt | ファイル暗号化型 | .vvv | × |
| 4 | 2016年2月 | Locky | ファイル暗号化型 | .locky | ○ |
| 5 | 2016年3月 | Android端末のランサムウェア | 端末ロック型 | - | ○ |
| 6 | 2016年6月 | Zepto | ファイル暗号化型 | .zepto | ○ |

[引用]ランサムウェアの脅威と対策 – IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/files/000057314.pdf





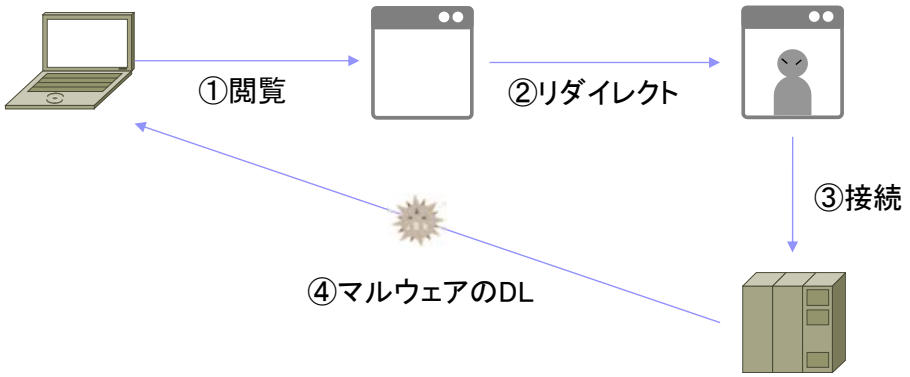
# ランサムウェアの感染経路

- **ウェブサイト**
  - 改ざんされた正規のウェブサイトを閲覧することで感染
  - 不正広告を閲覧することで感染
  - ダウンロードしたファイルを開くことで感染
- **メール**
  - メール本文に記載されたURLからアクセスすることで感染
  - メールの添付ファイルを開くことで感染
- **ドライブ・バイ・ダウンロード**による感染

[引用]ランサムウェアの脅威と対策 – IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/files/000059576.pdf

# ドライブ・バイ・ダウンロード概要

- インターネット経由で，標的PCにマルウェア等をダウンロードさせるための攻撃手法








# マルウェアの感染経路

- Web閲覧
  - 閲覧したWebページにマルウェアが埋め込まれており，Webページを閲覧した際にダウンロードされる
- Web誘導
  - メールに記載されたURLのWebページにアクセスするとマルウェアがダウンロードされる
- ネットワーク
  - ソフトウェアの脆弱性やPCの設定不備をついて感染させる
- メール添付
  - 添付ファイルにマルウェアが埋め込まれており，添付ファイルを開くと感染させられる
- 外部記憶装置
  - USBメモリ等の外部記憶装置経由で感染する
- 共有ディレクトリ
  - 共有ディレクトリ経由で感染する

# ランサムウェアの事例：WannaCry

- 2017年03月に明らかとなった暗号化型ランサムウェア
  - 世界150カ国以上で20万件以上の被害が出た
  - タイプのファイルを暗号化
    - 「.txt」「.doc」「.ppt」「.jpeg」「.zip」など150種類以上ファイルが暗号化の対象
    - 暗号化後は「.WCRY」という拡張子を追加
- ワームタイプのマルウェアで，自身のプログラムを他のコンピュータに複製し自己増殖する
- Windowsの脆弱性「EternalBlue」を突いたもので，Windows Updateを行なっていない端末が被害にあった


WannaCry感染画面
[出典]https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html