コンピュータ科学III

担当：武田敦志　<takeda@cs.tohoku-gakuin.ac.jp>

http://takeda.cs.tohoku-gakuin.ac.jp/

悪意のあるソフトウェア(1)

- 悪意のあるソフトウェア「マルウェア」

  malicious software の略

  一般的には「コンピュータウィルス」と呼ばれる

マルウェアの分類

- 広義のコンピュータウィルス
  - 狭義のコンピュータウィルス
  - ワーム
  - トロイの木馬
- 悪意のあるソフトウェアツール
- 悪意のあるデータ

悪意のあるソフトウェア(2)

- マルウェアの目的

  コンピュータシステムを「攻撃」する

  - データの破壊

    記録されているデータの消去・改竄を行う

  - バックドア

    コンピュータの不正な操作を可能にする

  - スパイウェア

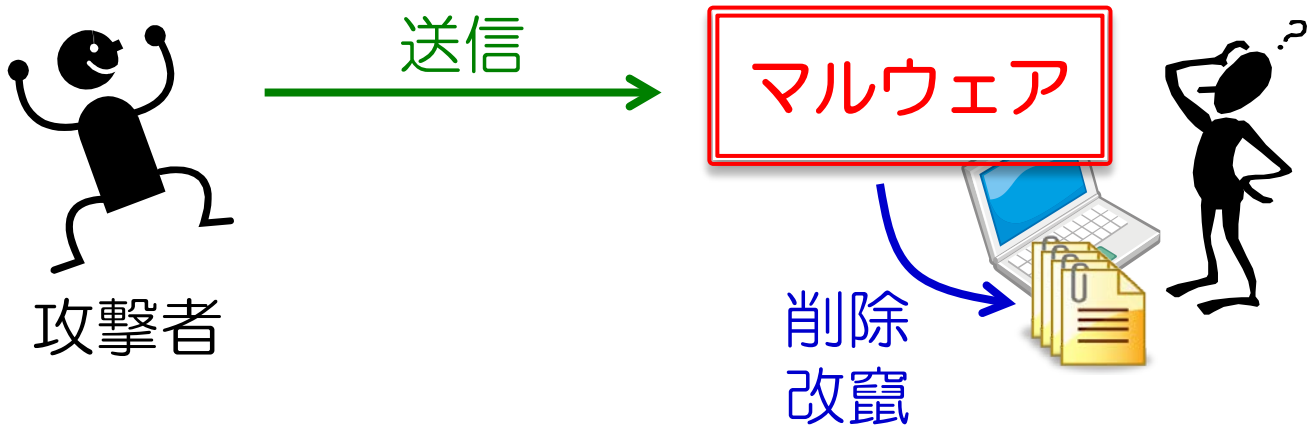
    利用者の秘密の情報を盗聴する

悪意のあるソフトウェア(3)

- データの破壊

  他人のコンピュータを**破壊**するためのマルウェア

  - コンピュータに記録されているデータの消去・改竄
  - ハードディスクのフォーマット

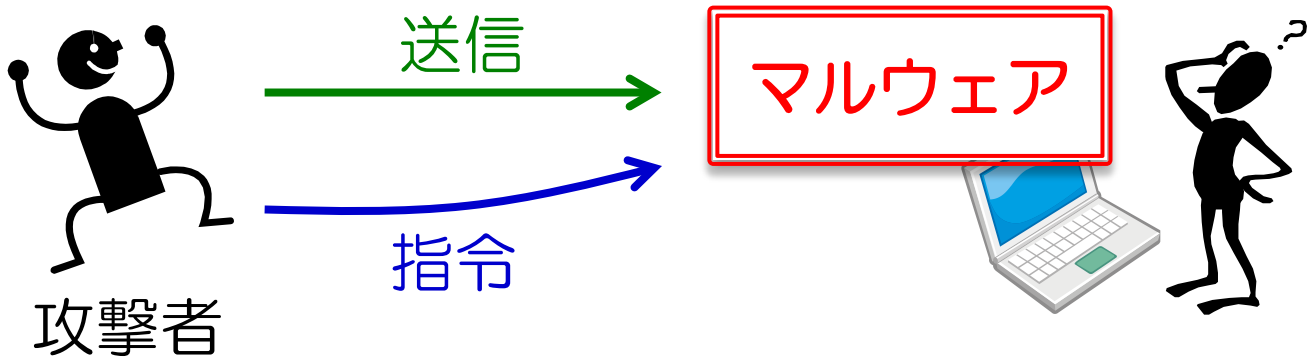


悪意のあるソフトウェア(4)

- バックドア

  他人のコンピュータに**侵入**するためのマルウェア

  - インターネットを介して操作できるようにする
  - 盗聴・改竄・踏み台攻撃に使用されることが多い

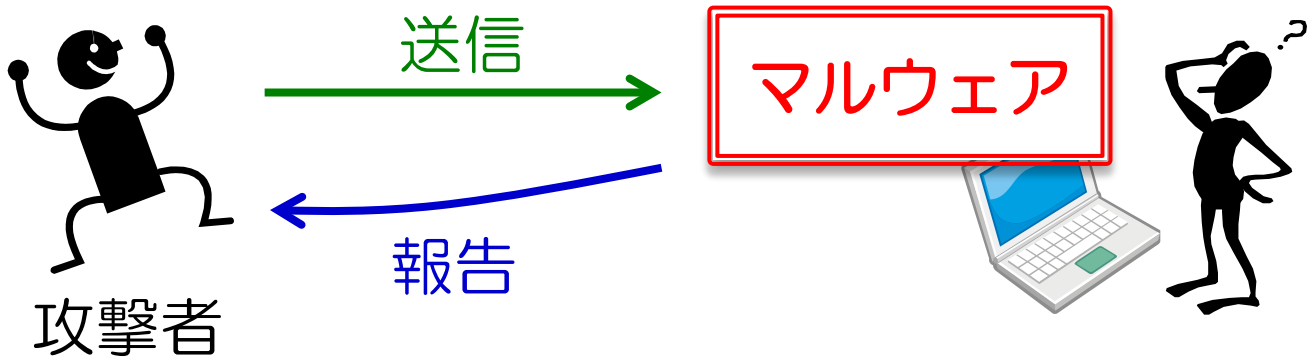


悪意のあるソフトウェア(5)

- スパイウェア

  他人のコンピュータを**盗聴**するためのマルウェア

  - コンピュータに記録されている個人情報を盗聴する
  - コンピュータの操作内容を盗聴する

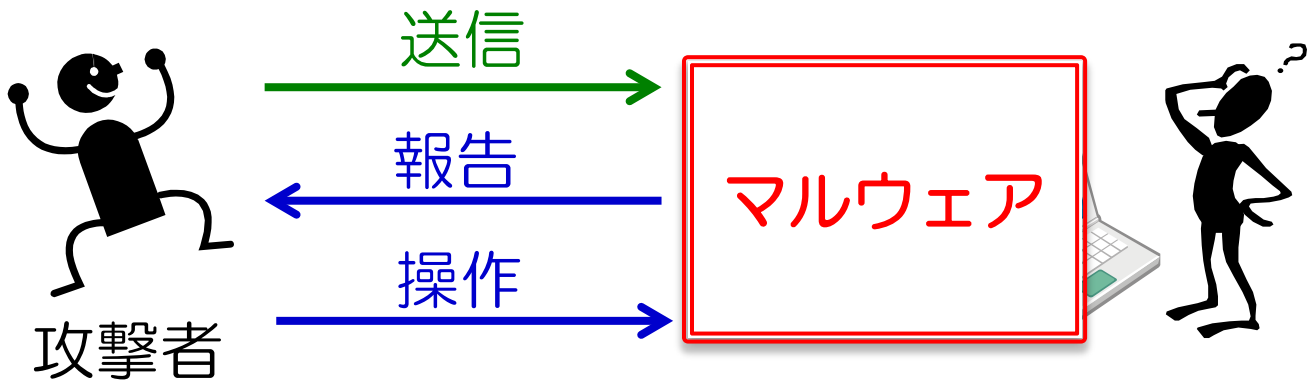


悪意のあるソフトウェア(6)

- 複数の性質を持つマルウェア

  コンピュータを**破壊**・**操作**・**盗聴**するマルウェア

  - コンピュータに記録されている情報を**盗聴**する
  - 盗聴の結果に従って、そのコンピュータを**操作**する
  - 操作が終わったら記録（ログなど）を**破壊**する



悪意のあるソフトウェア(7)

- 通常のソフトウェアとマルウェア

  マルウェア：**悪意のある動作を行う**ことを除くと
  通常のソフトウェアと同じ

  - 機械語などで書かれたプログラム
  - メモリにロードされて実行される

  実行されて初めて効力を発揮する

  ⇒ 実行されないなら「ただのデータ」

マルウェアの種類(1)

- 狭義のコンピュータウィルス
  - 他のソフトウェアに「寄生」する

    他のプログラムの一部に自分を潜り込ませる

    ⇒ コンピュータウィルスに感染した状態

    宿主のプログラムに一部として実行される
  - 実行と同時に増殖する

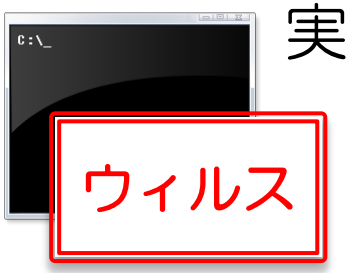
    感染していないプログラムに複製を潜り込ませる

    ⇒ 他のプログラムファイルに書き込む

マルウェアの種類(2)

- コンピュータウィルスの動作

① 何らかの方法で
実行させる



② 他のプログラムに
感染する

③ プログラムを実行すると
ウィルスも実行される

マルウェアの種類(3)

- ワーム
  - 単一のプログラムとして実行される

    ワームそのものが完結したプログラム

    自身を実行してもらえないと効力を発揮できない

    ⇒ 通常は「自動実行プログラム」として登録する
  - 実行と同時に増殖する

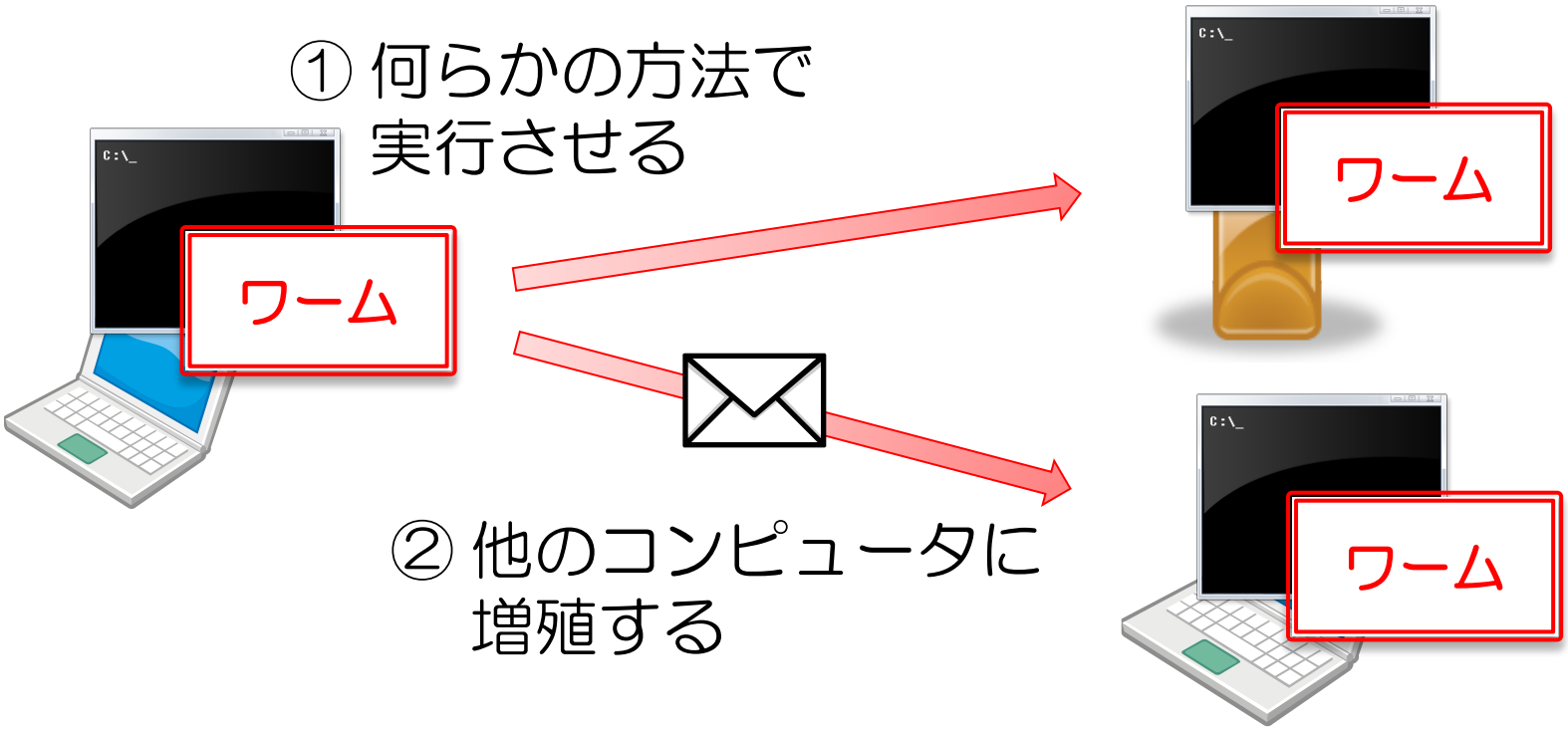
    外部メディア（USBなど）に増殖する

    ネットワークを介して増殖する

    ⇒ 自身を添付したメールを送ることもある

マルウェアの種類(4)

- ワームの動作



マルウェアの種類(5)

- トロイの木馬
  - 他のソフトウェアに組み込まれた状態で**配布**される
    ソフトウェアを実行するとトロイの木馬も**実行**される
    ⇒ 役に立つソフトウェアのように**見せかける**
  - （通常は）実行しても増殖しない
    ソフトウェアを何度も実行させるように仕向ける
    ⇒ 目立った動作をしないタイプが多い

マルウェアの種類(6)

- トロイの木馬の動作

① 通常のソフトウェアに見せかけて配布する

② ソフトウェアを実行するとトロイの木馬も実行される

マルウェアみたいなプログラム

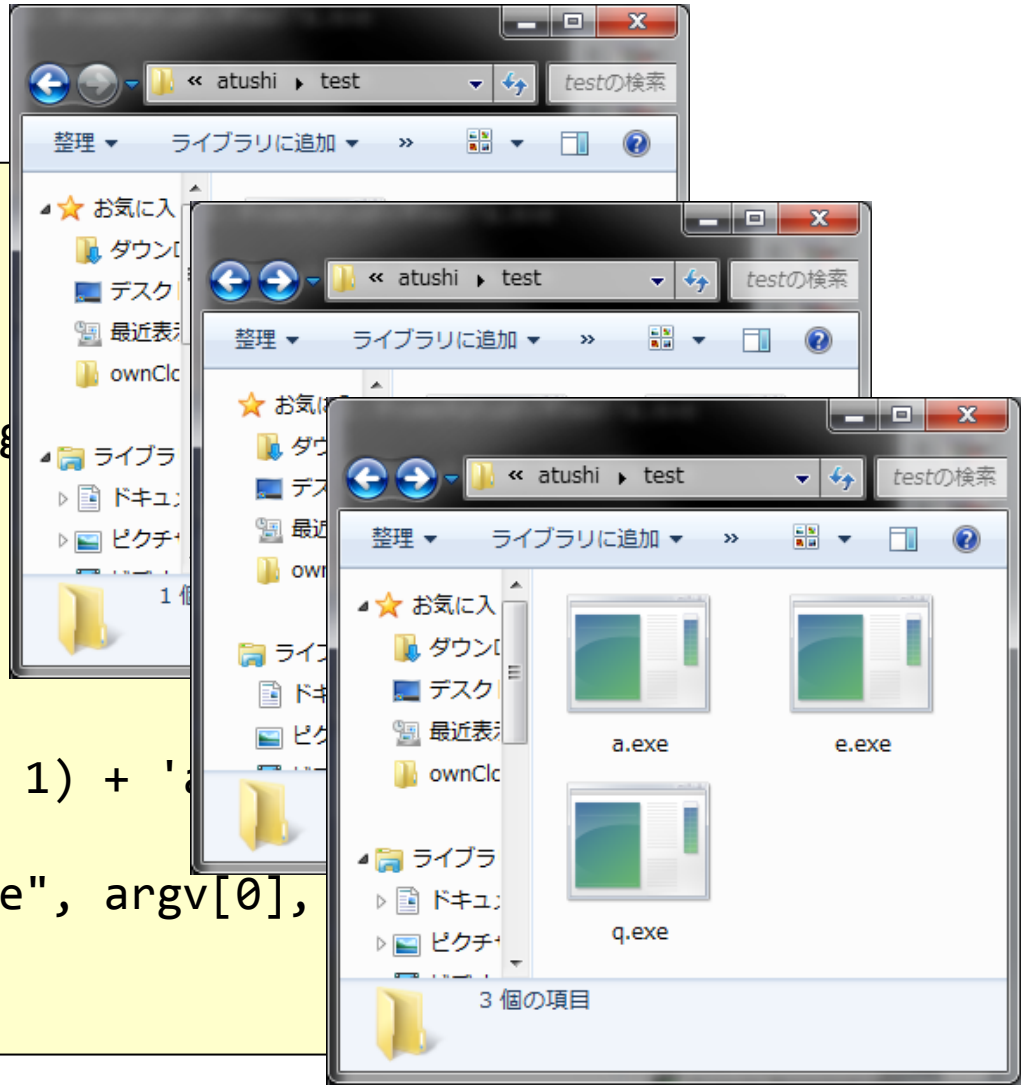
- 増殖するプログラム

```
#include <stdio.h>
#include <stdlib.h>
#include <time.h>

int main(int argc, char *arg
{
  char cmd[15];
  char c;

  srand(time(NULL));
  c = rand() % ('z' - 'a' + 1) + '

  sprintf(cmd, "cp %s %c.exe", argv[0],
  system(cmd);
}
```



コンピュータへの侵入(1)

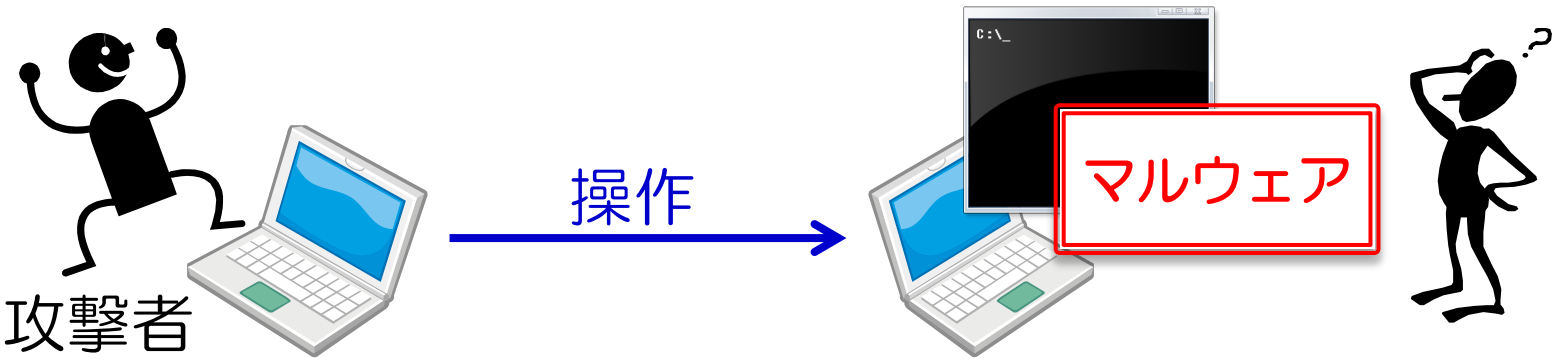
- マルウェアの実行による侵入

  最も基本的な侵入方法

  - ウィルスの実行
  - ワームの実行
  - トロイの木馬の実行

  } 対象のコンピュータを遠隔操作可能な状態にする

  マルウェアは攻撃者の指示に従って動作する



コンピュータへの侵入(2)

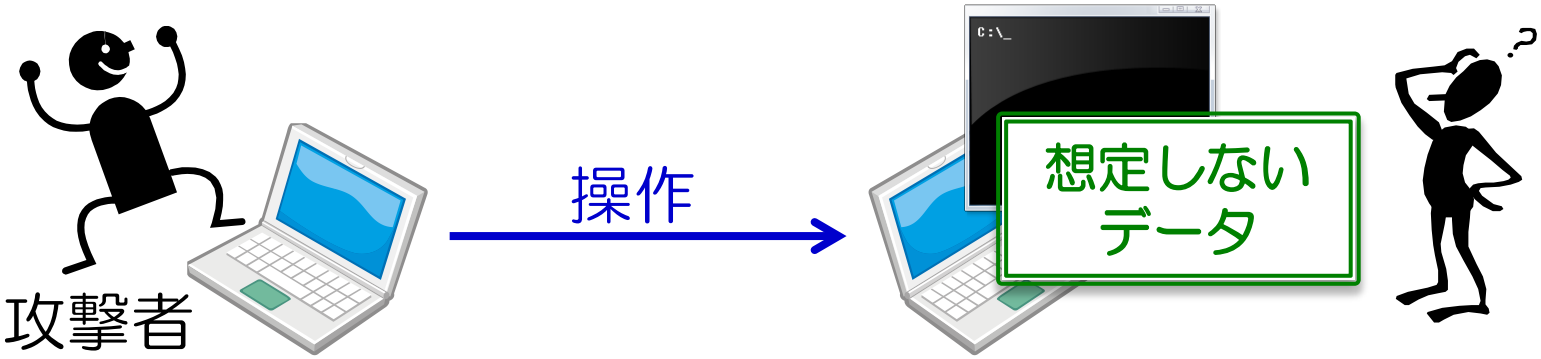
- セキュリティホールをついた侵入

  ソフトウェアの不具合をついて侵入する

  - ソフトウェアが想定していないデータを送りつける
  - ソフトウェアは想定外の動作をする

    ⇒ データを用いてソフトウェアを制御

（SQL Injection, Cross Site Scripting も同じ発想の攻撃）



コンピュータへの侵入(3)

- 不正侵入と攻撃

攻撃者がコンピュータの操作権を乗っ取る

コンピュータのデータを盗聴

他のコンピュータを攻撃

他の人や組織を攻撃

乗っ取られたコンピュータが**攻撃者**となる

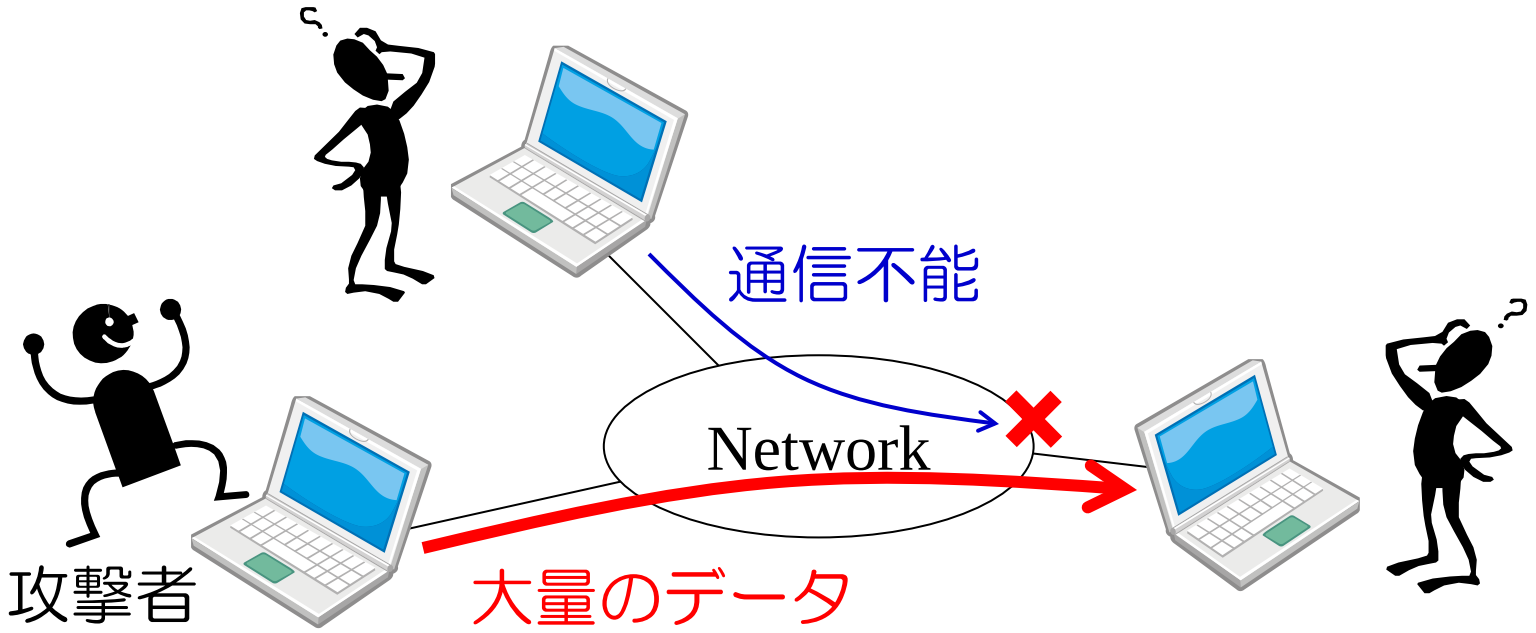
パソコン遠隔操作事件（2012年）
マルウェアに乗っ取られたパソコンによって犯罪予告が行われ、
これらのパソコンの所有者が逮捕（誤認逮捕）された。

コンピュータへの侵入(4)

- DoS攻撃（Denial of Service attack）

  特定のコンピュータに対して大量のデータを送信する

  ⇒ そのコンピュータの機能を停止させる

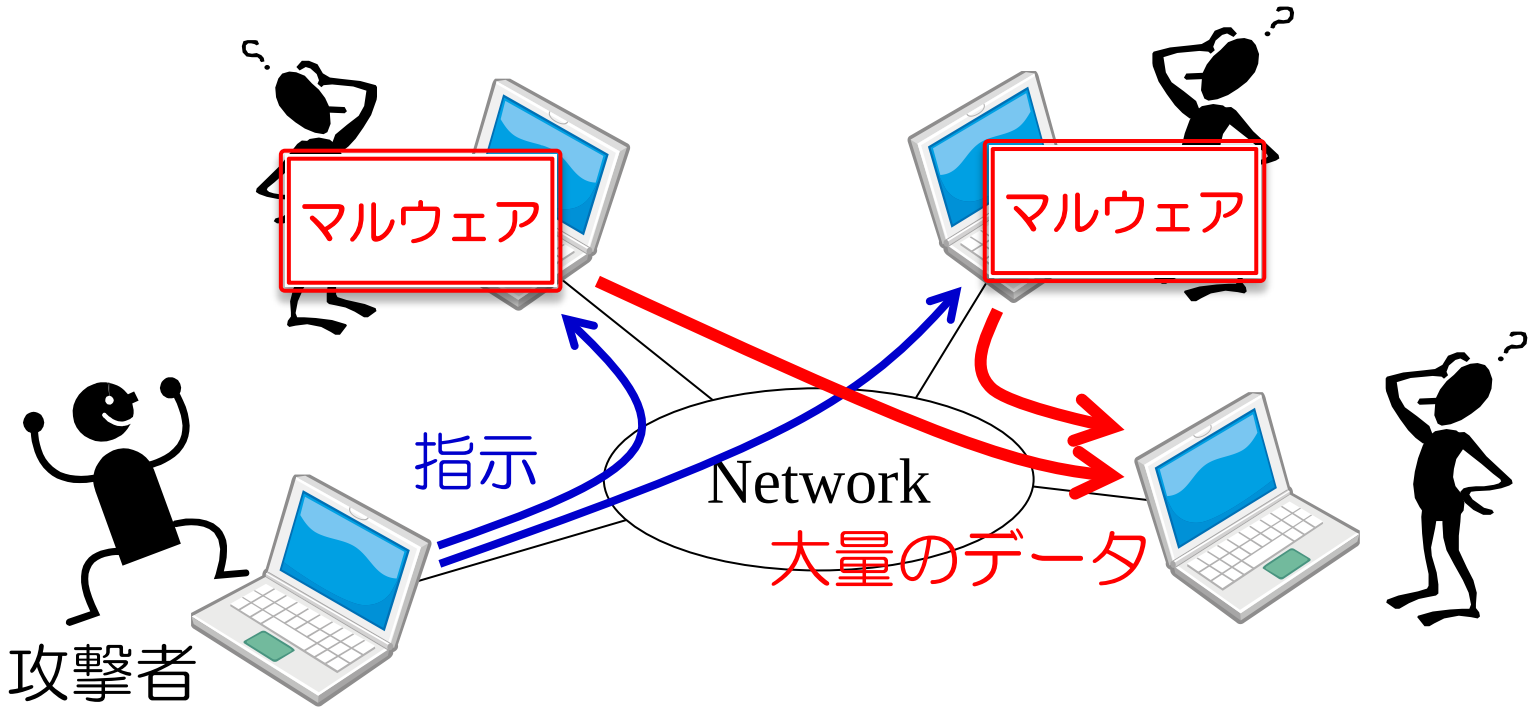


コンピュータへの侵入(5)

- DDoS攻撃（Distributed Denial of Service attack）

  特定のコンピュータに対して大量のデータを送信する

  ⇒ 侵入した複数のコンピュータを利用する



コンピュータへの侵入(6)

- 侵入されないための対策
  - マルウェアを**実行しない**

    実行者は**コンピュータの利用者**（攻撃者ではない）

    ⇒ よくわからないプログラムを実行しない
  - セキュリティホールへの対策をする

    ソフトウェアは**可能な限り最新**の状態にする

    「最新だから安全」というわけでもないので注意
  - パスワードなどの秘密情報は**厳重に管理**する

    簡単なものにしない・紙にメモしない など

それでも、ダメなときはダメ・・・

コンピュータへの侵入(7)

- 侵入された後の手続き

① ネットワークから**物理的に切断**する
侵入されたコンピュータは有害であることを理解する

② 侵入経路と影響範囲の**特定**
侵入経路（マルウェアなど）を特定
影響範囲（他のコンピュータへの攻撃）を特定

③ 担当責任者に**報告**
侵入経路と影響範囲を**必ず**報告すること
⇒ これを怠ると訴訟問題になる可能性がある

④ システムの**再インストール**
システムは諦めましょう。データは保全できるかも？