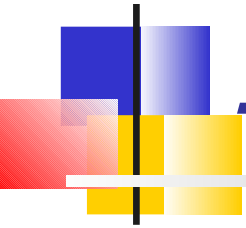


コンピュータウイルス

渡辺研究室

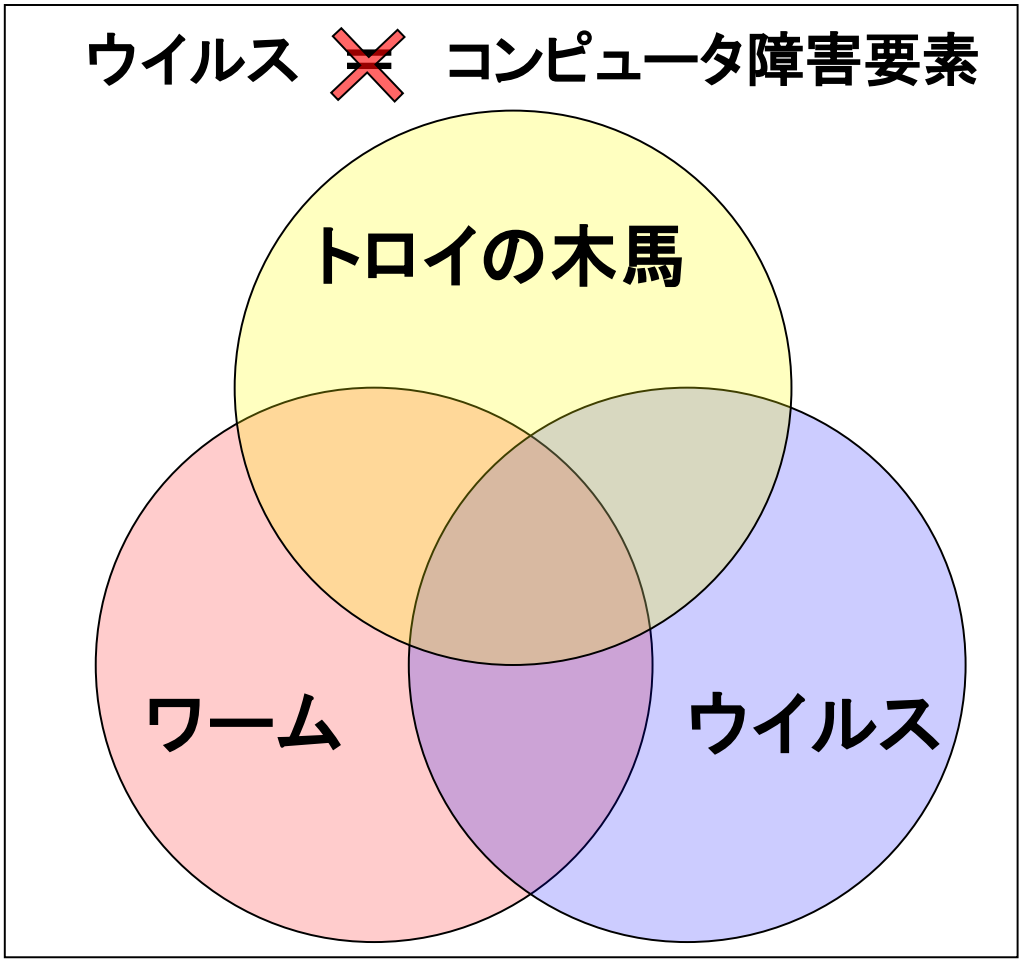
040427362　　樋口　豊章

参考資料

- 本資料は下記論文を基にして作成されたものです。文書の内容の正確さは保障できないため、正確な知識を求める方は原文を参照してください。

  - 書名　：　コンピュータ・ウイルスが伝染るのはなんでだろう！？
  - 著者　：　武井純孝
  - 発行年月日　：　2003年5月20日
  - 出版社　：　小学館

コンピュータ病原体



•バグ

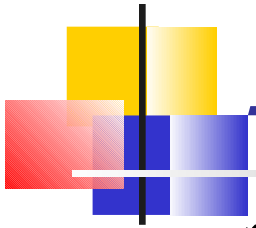
プログラムのミスにより、データに対して間違った加工を行うこと。

•セキュリティホール

コンピュータセキュリティの欠陥で、バグの一種。

コンピュータ病原体の分類

- **ワーム**
  - ワームの本質は自己増殖を繰り返すこと
- **ウイルス**
  - ウイルスの最低条件はファイルに寄生すること
- **トロイの木馬**
  - コンピュータの内通者
  - ワームやウイルスの補助ツールのようなもの

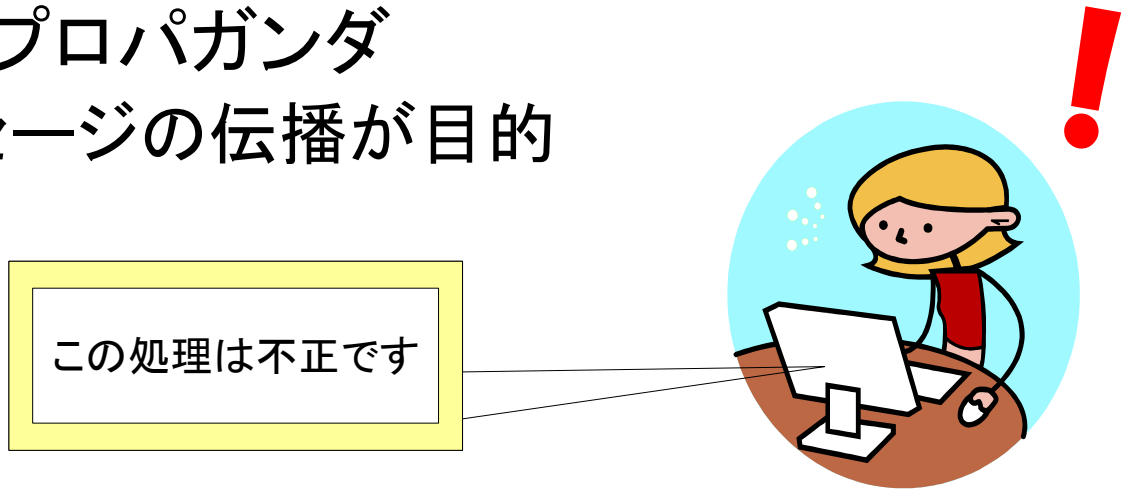


コンピュータ障害の症状の分類

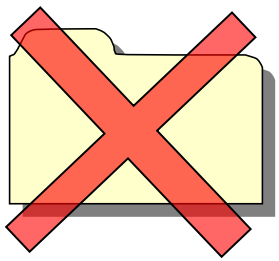
- グループ1：感染先のコンピュータが被害を受ける場合
  - 啓蒙／プロパガンダ
  - 破壊／ディストラクション
  - 悪戯／トリック
  - 資源占拠／リソースオキュペイション
  - 改変／オルタレーション
  - 創造／クリエイション
  - 裏口／バックドア
  - 漏洩／リーク
  - 防御物破壊／ディヘッジ

コンピュータ障害の症状の分類
―感染先のコンピュータが被害を受ける場合―

- 啓蒙／プロパガンダ
  - メッセージの伝播が目的

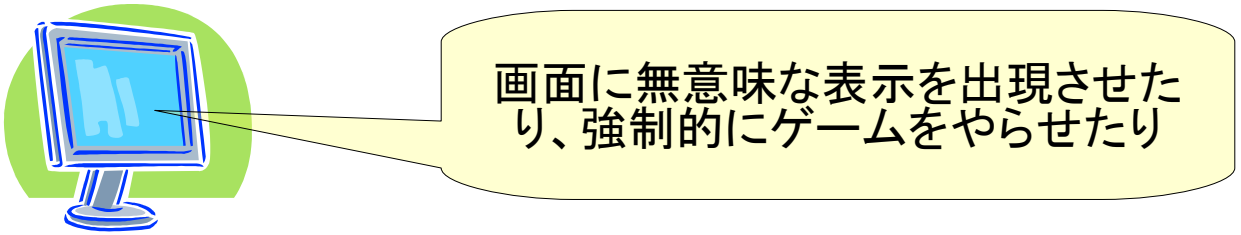


- 破壊／ディストラクション
  - ファイルやディレクトリィを消去する

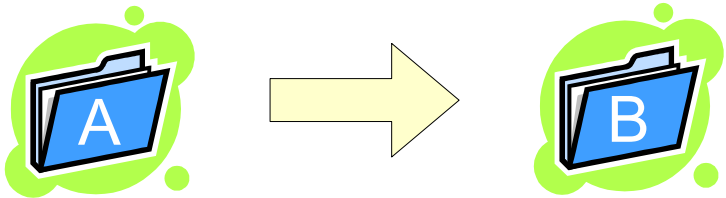


コンピュータ障害の症状の分類
ー感染先のコンピュータが被害を受ける場合ー

- 悪戯／トリック
  - 驚かせたりする事（悪戯）が目的

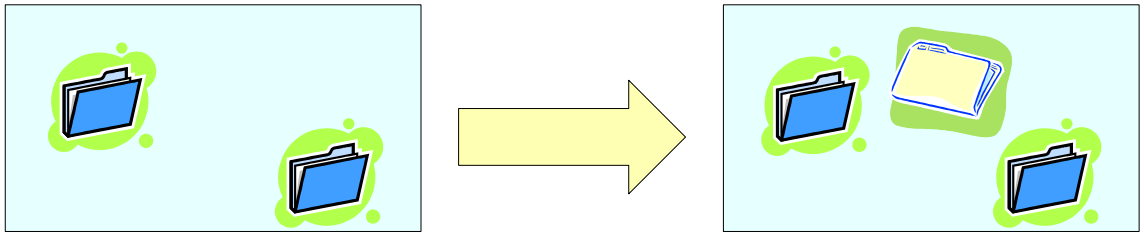


- 改変／オルタレーション
  - データを書き換える症状
  - ホームページの内容を書き換えてしまう事もある



コンピュータ障害の症状の分類
―感染先のコンピュータが被害を受ける場合―

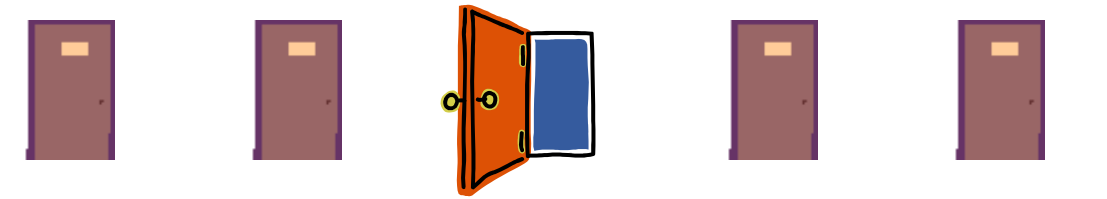
- 創造／クリエイション
  - 勝手にファイルが作成される症状



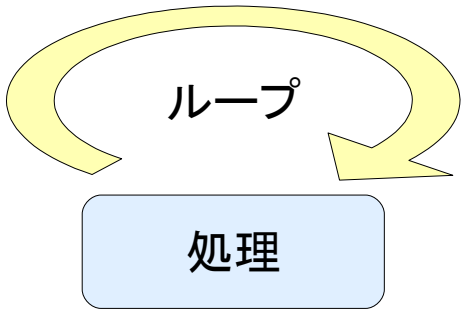
- 防御物破壊／ディヘッジ
  - セキュリティソフトを無力化される症状
    - セキュリティソフトで検知できれば発症しない
    - 「改変」と「破壊」を組み合わせ

コンピュータ障害の症状の分類
―感染先のコンピュータが被害を受ける場合―

- 裏口／バックドア
  - ポートが勝手に開かれる症状

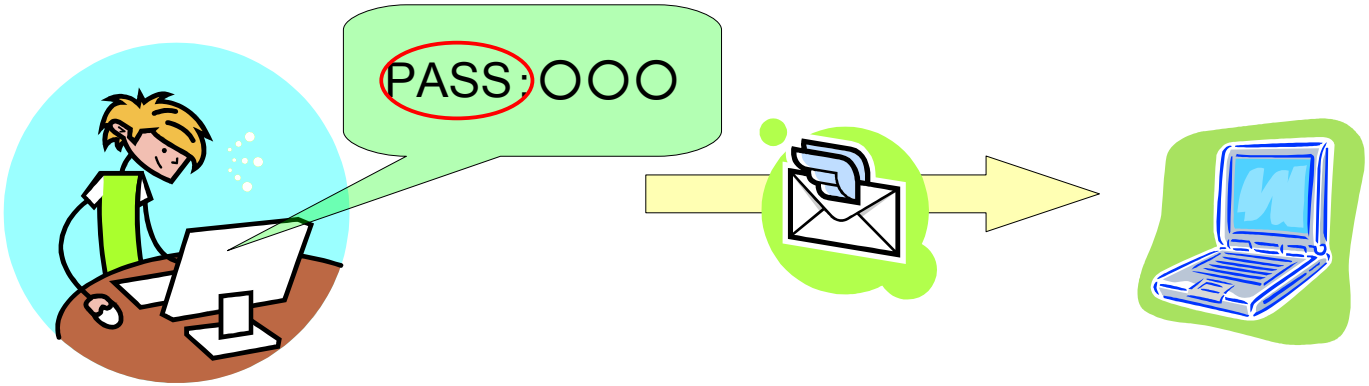


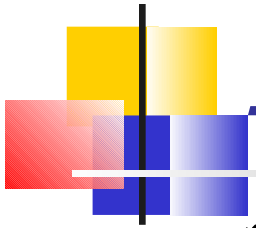
- 資源占拠／リソースオキュペイション
  - メモリやCPUなどを食い尽くす症状



コンピュータ障害の症状の分類
―感染先のコンピュータが被害を受ける場合―

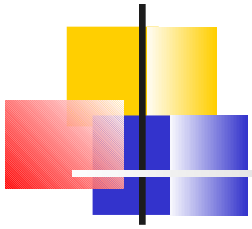
- 漏洩／リーク
  - コンピュータ内部の情報を外部に送信する症状
    - バックドアは開かない
    - 通信内容を監視し、特定の文字列を見つけ次第、記録して特定のメールアドレス宛に送信する
    - トロイの木馬ではない





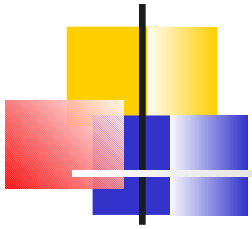
コンピュータ障害の症状の分類

- グループ2：感染先のコンピュータから他のコンピュータが被害を受ける場合
  - 帯域占拠／バンドオキュペイション
  - 攻撃／アタック
    - ポートスキャン
    - DoS
    - PoD
    - メールボム　……など



コンピュータ障害の症状の分類
ー他のコンピュータが被害を受ける場合ー

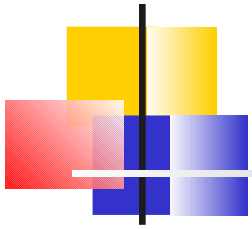
- 帯域占拠／バンドオキュペイション
  - 感染先のコンピュータから大量のパケットがネットワーク上に溢れ、通信が麻痺してしまう症状
  - この症状を目的としたコンピュータ病原体は少なく、副次的に起こる症状である
- 攻撃／アタック
  - 何らかのネットワーク攻撃が行なわれる症状
  - セキュリティホールがなくてもパンクさせる事が可能



「攻撃」の例

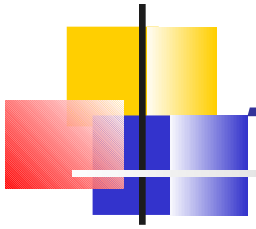
- ポートスキャン
  - サーバのポートを逐次検索する行為
  - セキュリティホールがないか調べる

- DoS（Denial of Services　サービス妨害）
  - 不正なデータや、大量のデータを送信することで、相手のコンピュータやネットワークを麻痺させる攻撃



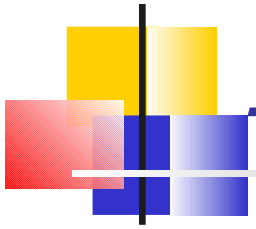
「攻撃」の例

- PoD（Ping of Death　死のピング）
  - 規定より遥かに大きなパケットを送信することで、相手のコンピュータをリセットしなければならない状態にする攻撃
  - 現在では殆ど全てのOSで対処されているか、パッチ(修正プログラム)が配布されている
- メールボム
  - 膨大な数の大容量メールを送ることで、相手のメールボックスをパンクさせる攻撃
  - 副次的に「帯域占拠」がおこる



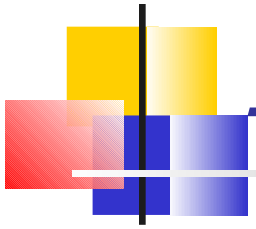
コンピュータの病態の分類

- ネットワーク発症
  - DDoS　……など
- ロジック発症
- ポリモーフ発症
- コンパニオン発症



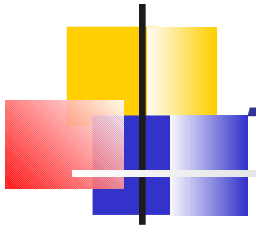
コンピュータの病態の分類

- ネットワーク発症
  - 複数の感染されたコンピュータが連携を取って第三者のコンピュータに「攻撃」を行なう病態
  - DDoS
    - 「Distributed Denial of Services」の略語
      （分散型サービス妨害）
    - ユーザに気づかれないよう「トロイの木馬」を仕掛け、攻撃を開始する時に予め仕掛けたトロイに対して一斉にパケットの送出命令を発行するというもの



コンピュータの病態の分類

- ロジック発症
  - 常にシステムを監視し、条件にあった動作が行なわれたときに発症するような病態
  - 「潜伏型」のコンピュータ病原体に見られる
- ポリモーフ発症
  - コンピュータ病原体の本体を暗号化して、セキュリティソフトに発見されにくくする働き



コンピュータの病態の分類

- コンパニオン発症
  - 正規のプログラムのファイル名と同じ名前のファイル名を持つコンピュータ病原体の本体を用意し、本物より先に実行させる病態
  - WindowsがexeファイルよりComやbatファイルを実行したり、実行ファイルを探すディレクトリに順番がある事を利用