6学期講義

Network Security

Introduction

総合情報学科

サービス妨害(DoS)攻撃

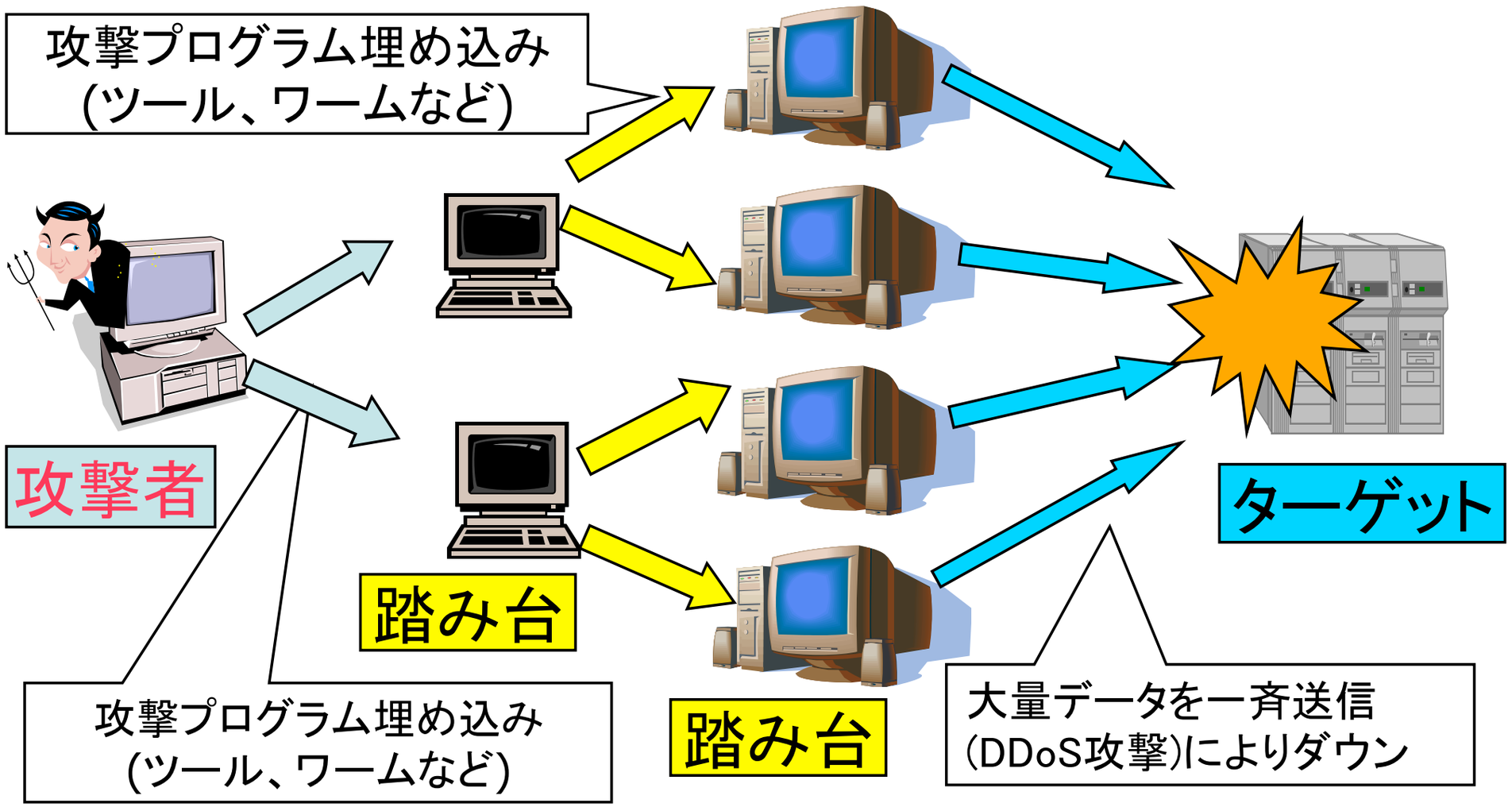
- サービス提供を困難または不能にする攻撃の総称
  - 可用性が損なわれる
    - 大量の処理要求 ⇒ 計算機/ネットワークに過大な負荷
      ⇒ サービスの正常な(提供/運用)を(困難/不能)に
  - ２つの手法：過負荷のほかに、異常終了させる手法も
- 英語: **D**enial **o**f **S**ervice Attack ⇒ 略して DoS Attack
  - いくつかの和訳: 「妨害」の他に「停止」「拒否」「不能」

DDoS攻撃

- Distributed Denial of Service攻撃の略
  ⇒ 分散処理によるDoS攻撃
- 複数台の計算機を利用して一斉攻撃 ⇒ 標的に過負荷生成
  - 攻撃側と被攻撃側の関係を「一対一」から「多対一」に
- 攻撃手法
  - Bot (Malwareの一種)、集団人力など
  - BotNet: DDoS攻撃のシステム化.
    - 簡単な命令で、多数の計算機(内のMalware)が対象を攻撃

DDoS攻撃

Malwareの感染に気づかず
知らぬ間にDDoS攻撃に加担してしまうことも



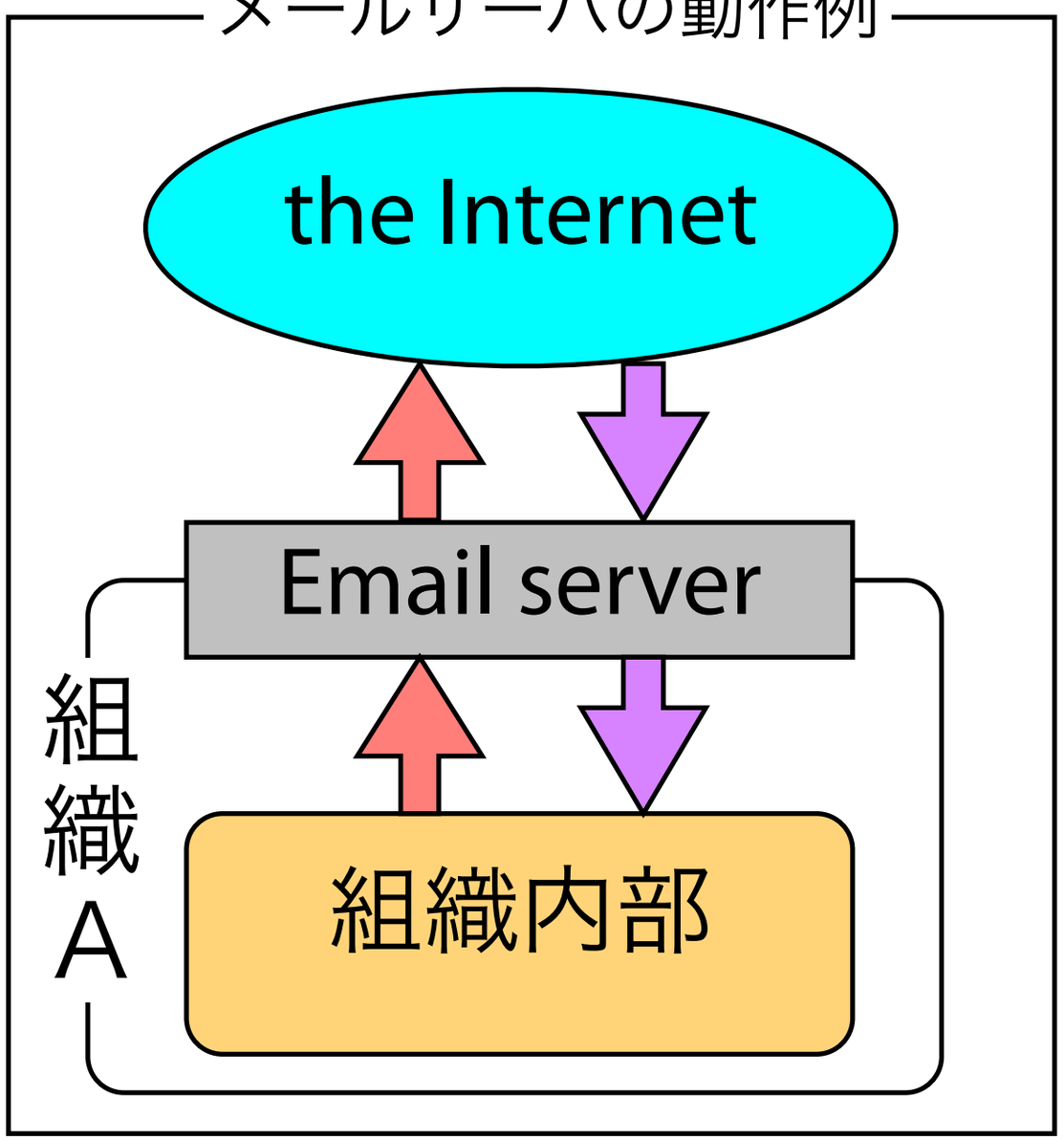
引用: IPA, https://www.ipa.go.jp/security/publications/dokuhon/ppt.html

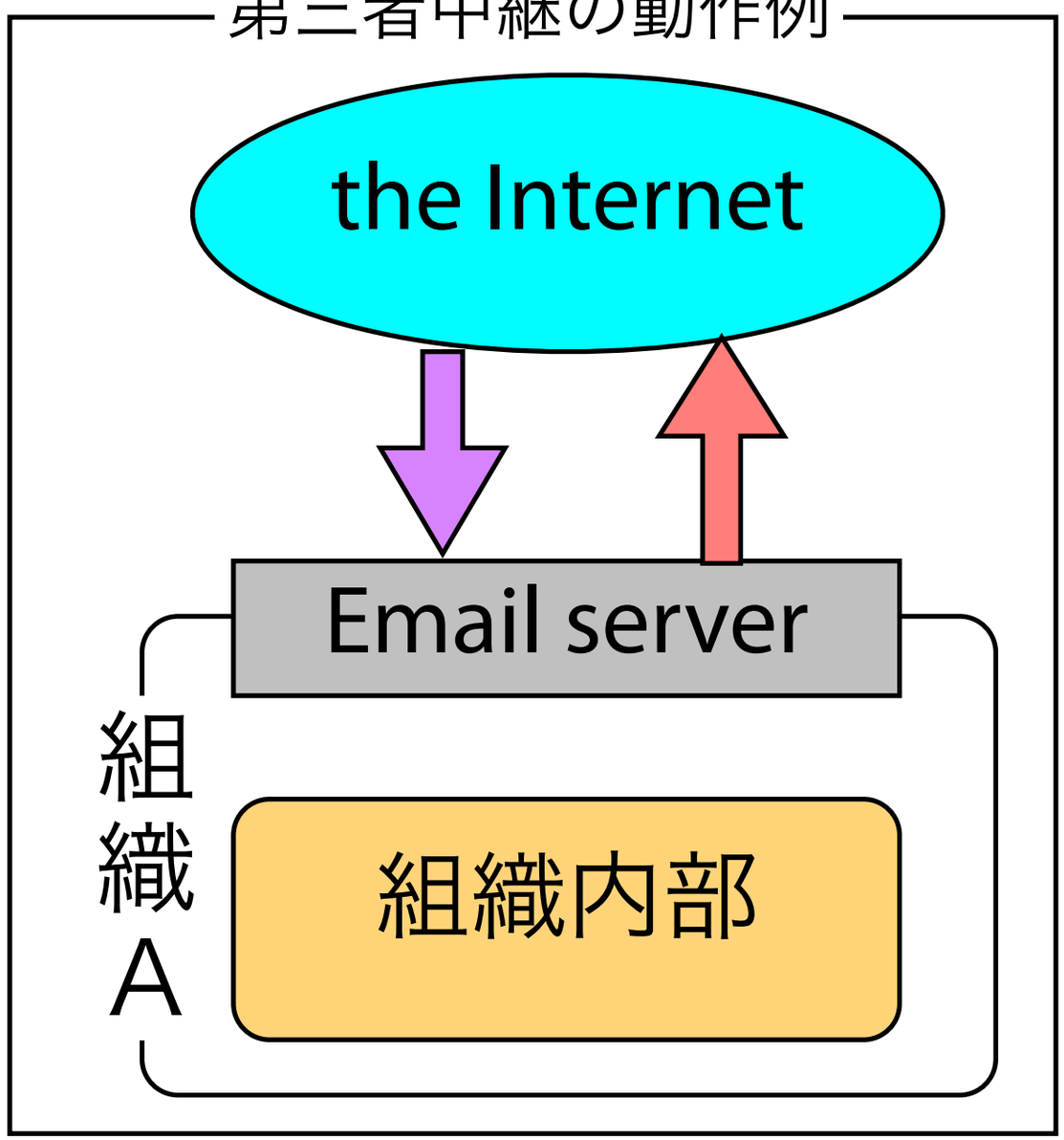
電子メール攻撃

- メールサーバに大量の電子メールを送りつける
  - メールサーバの性能低下や機能停止
    - 巨大な添付ファイル付きメールの送信
      - ⇒ file system full (記憶装置の空き容量ゼロ化)
- 第三者中継機能を悪用
  - Spam(迷惑)メールの踏み台として悪用される

第三者中継機能

- 外部から来た電子メールを別の外部へ転送する機能





F5 アタック

- 「人力」によるDoS (DDoS)攻撃
- 大量のWebページ要求を標的に送付
  - Webブラウザを起動し，F5 キーを連打するだけ (Reloadの反復実行)
    ⇒ サーバ処理能力の低下
- 誰でも実行できる攻撃方法
  ⇒ 仲間を募り、人海戦術で標的を攻撃

DoS攻撃の事例

- (2010/02/17) Game watch, “突然の大規模DDoS攻撃! その時オンラインゲーム運営はどうする?”
  - http://game.watch.impress.co.jp/docs/news/20100217_349619.html
- (2010/12/07) ITmedia, WikileaksめぐりDoS攻撃の応酬、PayPalなども標的に
  - http://www.itmedia.co.jp/news/articles/1012/07/news064.html
- (2009/08/17) ITmedia, 2ちゃんねる一部serverが長期down中 韓国からサイバー攻撃か
  - http://www.itmedia.co.jp/news/articles/0908/17/news031.html

岡崎図書館事件 (2010/3)

- 要点：情報収集処理がDoS攻撃と勘違いされ、逮捕
- 事象：図書館システムにシステム障害が発生
  - 原因調査の結果、図書館利用者の１人が逮捕
    ⇒起訴猶予処分
- 原因：1秒に1回のシステムアクセスを、DoS攻撃と誤判断
  - Web Crawlerを作成し、Webページから新着図書の情報を収集するプログラムを作成、1秒間に1回の頻度でアクセス
- さらなる調査結果：
  - Crawlerに違法性はなく、悪意による行為でもなかった
  - **図書館システムの不具合がシステム障害の原因だった**

岡崎図書館事件 関連Link

- 岡崎市立中央図書館事件 - WikiPedia
  - http://ja.wikipedia.org/wiki/%E5%B2%A1%E5%B4%8E%E5%B8%82%E7%AB%8B%E4%B8%AD%E5%A4%AE%E5%9B%B3%E6%9B%B8%E9%A4%A8%E4%BA%8B%E4%BB%B6
- **LibraHack** - マスコミ報道だけでは分からない岡崎図書館事件
  - http://librahack.jp/
- 岡崎図書館事件超解説
  - http://blog.livedoor.jp/resto/archives/51514351.html
- 岡崎図書館事件はまだ終わっていない
  - http://takagi-hiromitsu.jp/diary/20110121.html

内部のリスク要因

- セキュリティホール、脆弱性
  ⇒ 情報システムの脆弱性
- セキュリティ機能、規則の欠如
  ⇒ 組織に内在する脆弱性
- 情報リテラシーと情報倫理
  ⇒ 人為的な脆弱性

セキュリティホール(脆弱性)

- セキュリティホール(Security Hole)
  - Software上の「欠陥」。本来できないはずの操作ができてしまうことを指す
  - 「悪意ある人」により悪用される
- 脆弱性 (Vulnerability) ⇒ 弱点、欠陥
  - 欠陥だけでなく、設計(仕様)通りの動作/仕組みでも、それが攻撃に悪用される可能性がある場合も含む
    (Security Holeを含む概念)
    ⇒ 欠陥の有無を問わず、攻撃に対して〝もろい〟こと
  - Softwareや明確な欠陥以外は「脆弱性」と呼ぶ傾向

エクスプロイト(Exploit)

- 各種の脆弱性を攻撃する行為/攻略手段のことを指す
  直訳は「悪用する」「開発する」など
  ⇒ 「功績」という意味も *(Black hat*では確かに功績である*)*
- 元来、脆弱性を悪用可能にするProgramの名称を
  “Exploit code” と呼んでいた
- White hatが脆弱性検証を目的として書かれたコード
  “Proof of Concept”(PoC) (実証コード)
  脆弱性有無の確認するが、悪意のある行為はしない

脆弱性情報データベース

- 「脆弱性は全ての情報が詳細にわたって一般に公開されるべき」の具現化
  従来は”脆弱性監査ツール”などが独自に収集/集積
  - 利点: 設計/開発者が過去の失敗から学べる
  - 欠点: 悪用され、Malwareや攻撃ツール作成を支援
- 代表例: CVE, JVN, OSVDB
  - CVEを中心として、相互参照

Common Vulnerabilities and Exposures (CVE)

- 米国 非営利団体 MITREが維持しているDatabase
  ⇒ ベンダー非依存
    - URL: http://cve.mitre.org/
- CVEの目的は**識別可能性**の確保.
    - 個々の脆弱性に固有の番号を割り当て、
      それにより脆弱性を識別可能とすること
    - MalwareやExploit codeとCVEの関係性は1対1とは限らない
- 番号付与
    - CVE と CVSS

Common Vulnerabilities and Exposures (CVE)

- 日本語では「共通脆弱性識別子」
- CVEの目的は**識別可能性**の確保.
  - 個々の脆弱性に固有の番号を割り当てる
  - 各ベンダーの警告情報が同一脆弱性の指摘かどうかに利用可能
- CVE識別番号 (CVE-ID)
  - 付与番号: 「CVE-西暦年-通番 (４桁以上)」
    例) CVE-2015-0021

参考：https://www.ipa.go.jp/security/vuln/CVE.html

CVE-IDの使われ方

ご登録者各位

　このメールは、IPA Webサイトから「メールニュース配信」で「セキュリティ対策情報」にご登録いただいた方へお知らせしています。

==========セキュリティ緊急対策情報のお知らせ==========

◆お知らせリスト

　◇Microsoft Office 等の脆弱性対策について(CVE-2013-3906)

==========

■　IPAセキュリティセンターは、本日、標記の緊急対策情報を発表しました。

　◇Microsoft Office 等の脆弱性対策について(CVE-2013-3906)

　◆概要

　　Microsoft社の Microsoft Office 等にリモートからコード(命令)が実行される脆弱性が存在します。この脆弱性を悪用された場合、アプリケーションプログラムが異常終了したり、攻撃者によってパソコンが制御されたりする可能性があります。

Common Vulnerability Scoring System (CVSS)

- 日本語では「共通脆弱性評価システム」
- CVSSの目的は脆弱性の(危険度)評価**の確立**
  - ベンダー非依存
  - ３つの基準で評価：基本評価、現状評価、環境評価
- CVSS 基本値
  - 値域：(深刻度小) 0.0 ～ 10.0 (深刻度大)

参考：https://www.ipa.go.jp/security/vuln/CVSS.html

Japan Vulnerability Notes (JVN)

- JPCERT/CCとIPAが共同管理している脆弱性Database
  - 2007年4月より現在の状態に
- 日本語で記載、日本の製品に関する脆弱性情報も含まれる
  - URL: http://jvn.jp/
- 脆弱性対策情報DBもある
  - JVN iPedia - http://jvndb.jvn.jp/