情報セキュリティ技術:
不正アクセス対策とコンピュータウィルス

情報社会とセキュリティ
2024 年度前期

佐賀大学理工学部 只木進一

不正アクセス: Unauthorized Accesses

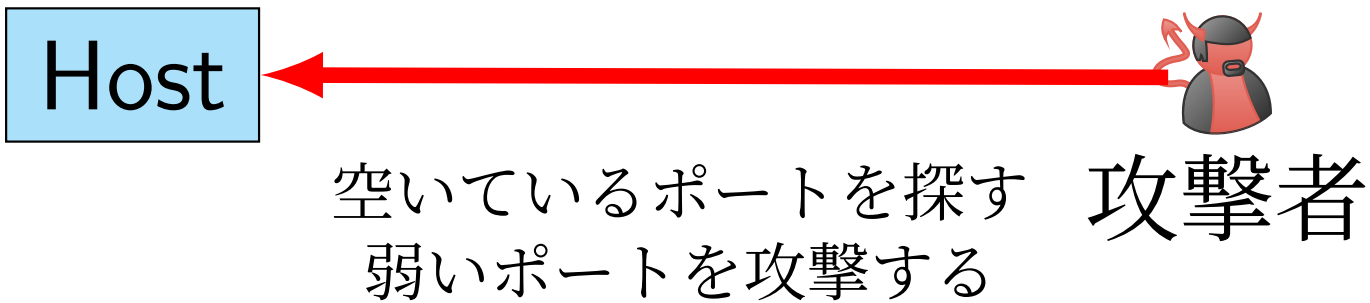
- 権限のない資源 (コンピュータ、サービス) への接続
  - ログイン権限のないサービスへの侵入
  - 与えられた権限以上の権限の取得
    - ID/PW の窃取
    - 脆弱性を狙った攻撃
  - 重要情報の窃取
- 正当な利用者の資源利用の妨害
  - 共有コンピュータの資源を独占する
  - 他人の PC の資源を勝手に利用する
  - 大量の通信を送って、サーバを停止させる

攻撃者の類型

- hacker: 高いコンピュータ技術を有する者
  - hacker 自体は、攻撃者ではない
- cracker: hacker のうち、悪意をもって攻撃する者
- しかし、攻撃用ツールはインターネット上に存在
  - script kiddie: 攻撃用ツールを使って興味本位で攻撃する者
- かっては、愉快犯が多かった
- 最近は、プロによるお金目当ての攻撃が増えている

ポートスキャン: Port Scans

- 攻撃の準備として脆弱な部分を探す
- ポート: TCP/UDP において、サービスとの紐づけ
  smtp:25, DNS:53, http:80, NetBIOS:137, SQL:156, etc.
- 応答するポートを調べ、その後で脆弱性を調べる
  - 80 番に応答 ⇒ バージョンを調べる ⇒ 脆弱性を突く



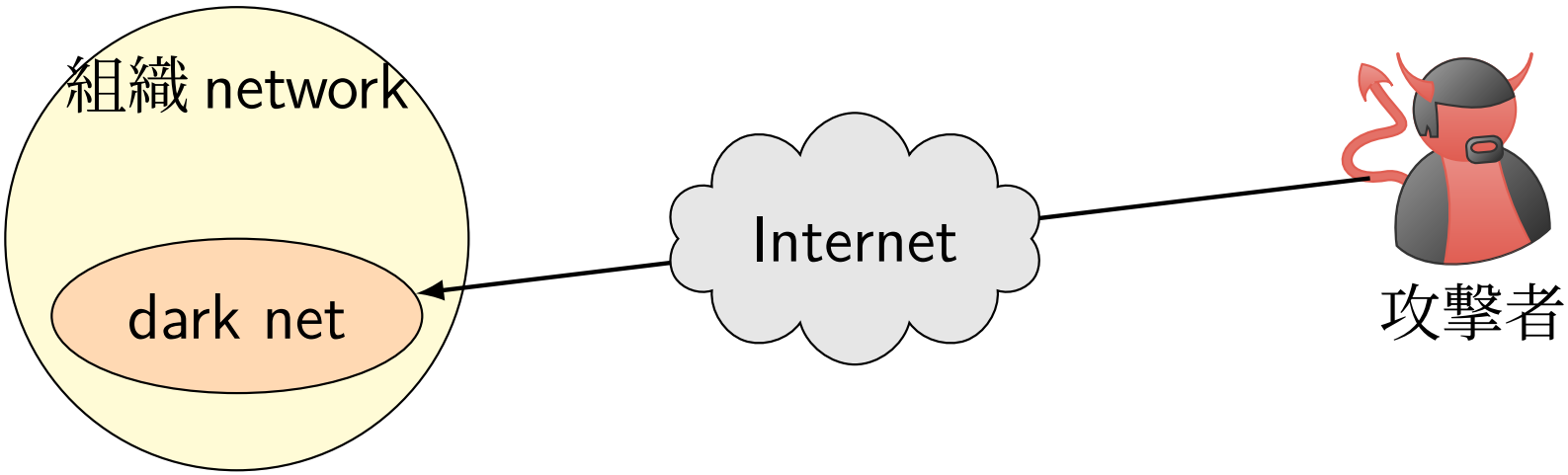
ポートスキャンへの対策

- ファイアウォールにてポートを閉じる
  - FW で、送信先のアドレス・ポートの組を拒否
  - 外部からは、許可されたポートだけを開けるのが基本
- サーバ等は、不要なサービスを停止する
  - ポート向け接続要求を拒否
- FW 及びサーバで、通信をモニタリングする

ポートスキャンの状況

- ポートスキャンは、使用していないアドレスにも到着
  - 攻撃者は、攻撃対象を探している
- ダークネット: 使用していないアドレス空間
- ポートスキャン数の推計: IP アドレスあたり 183 万件 (2022 年)
  https://www.nict.go.jp/press/2023/02/14-1.html
- Web カメラなどの IoT 機器やホームルータが狙われている
  - IoT: Internet of Things: インターネットに接続された様々な機器

ダークネット: Dark Nets



- 使用していないアドレス領域へポートスキャン
- ダークネットを使って、攻撃状況の傾向を知ることができる。

質問

使用していない領域へのアクセス状況を知ることで、攻撃の傾向を知ることができるのはなぜでしょう。

コンピュータウィルス: Comupter Viruses

- malware: ウィルス、スパイウェア、ボットなど悪意あるプログラムの総称
- computer virus
  - 伝染機能: ファイルにコピーを付ける、あるいは通信機能を使ってコピーを送信する
  - 潜伏機能: 見つからないように潜伏する
  - 攻撃機能: ファイルの破壊、ファイルの持ち出し

virus: [ˈvaɪrəs]
mal: bad or badly; not correct or correctly

- spyware
  - コンピュータの操作や通信内容を盗み見る
  - 通信機能を使って、外部に送信
  - key logger: キーボード操作を記録する
  - web spyware: Web の閲覧履歴を記録する
- bot
  - 外部からの指令、あるいは特定の時刻に起動
  - 攻撃先に一斉に通信

- Trojan horse: 便利なアプリケーションを偽装した malware
  - ファイルの持ち出し
  - 侵入用裏口の設置
  - 他の malware をダウンロード

ランサムウェア: Ransomware

- 感染すると、PC 内のファイルに暗号がかかる
- 金銭を要求、特に電子通貨を要求
- 払っても、解除されるか不明
- 企業への大規模攻撃の事例: 事業継続への脅威
- 病院システムへの攻撃事例: 診療継続への脅威

https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html
https://www.asahi.com/articles/ASP592PNYP58ULFA008.html

ランサムウェアの被害例: 病院

- 2021 年 10 月: 徳島県つるぎ町立半田病院
  https://www.asahi.com/articles/ASQ6N6QFPQ6NPTLC01W.html
- 2022 年 10 月: 大阪府立大阪急性期・総合医療センター
  https://www.asahi.com/articles/ASQB075DWQB0OXIE022.html

マルウェアの感染経路

- 添付ファイル: メールサービス側の対策が強くなり、減少傾向
- Web: 閲覧しただけで感染することがある
- USB 等の媒体
- ネットワーク

マルウェアへの対策

- ウィルス対策ソフトの導入
- メールサーバへのウィルス対策の導入
- IDS/IDS における対策
  - sandbag: 添付ファイルやダウンロードファイルの挙動を検査
  - マルウェアが行う通信の検知
- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System

標的型攻撃: Targeted Attacks

- メール受信者の特性を考慮して、開封されやすいメール等を送る
- 目的は多様: マルウェア配布、IP/PW 窃取、個人情報窃取
- 「至急」、「重要」などのキーワードで、受信者の判断を迷わす
- 送信元アドレスの詐称
- 最近の例: 宅配便到着の偽装、返信メールの偽装
- 機械翻訳性能の向上: 自然な日本語になっていることに注意

質問

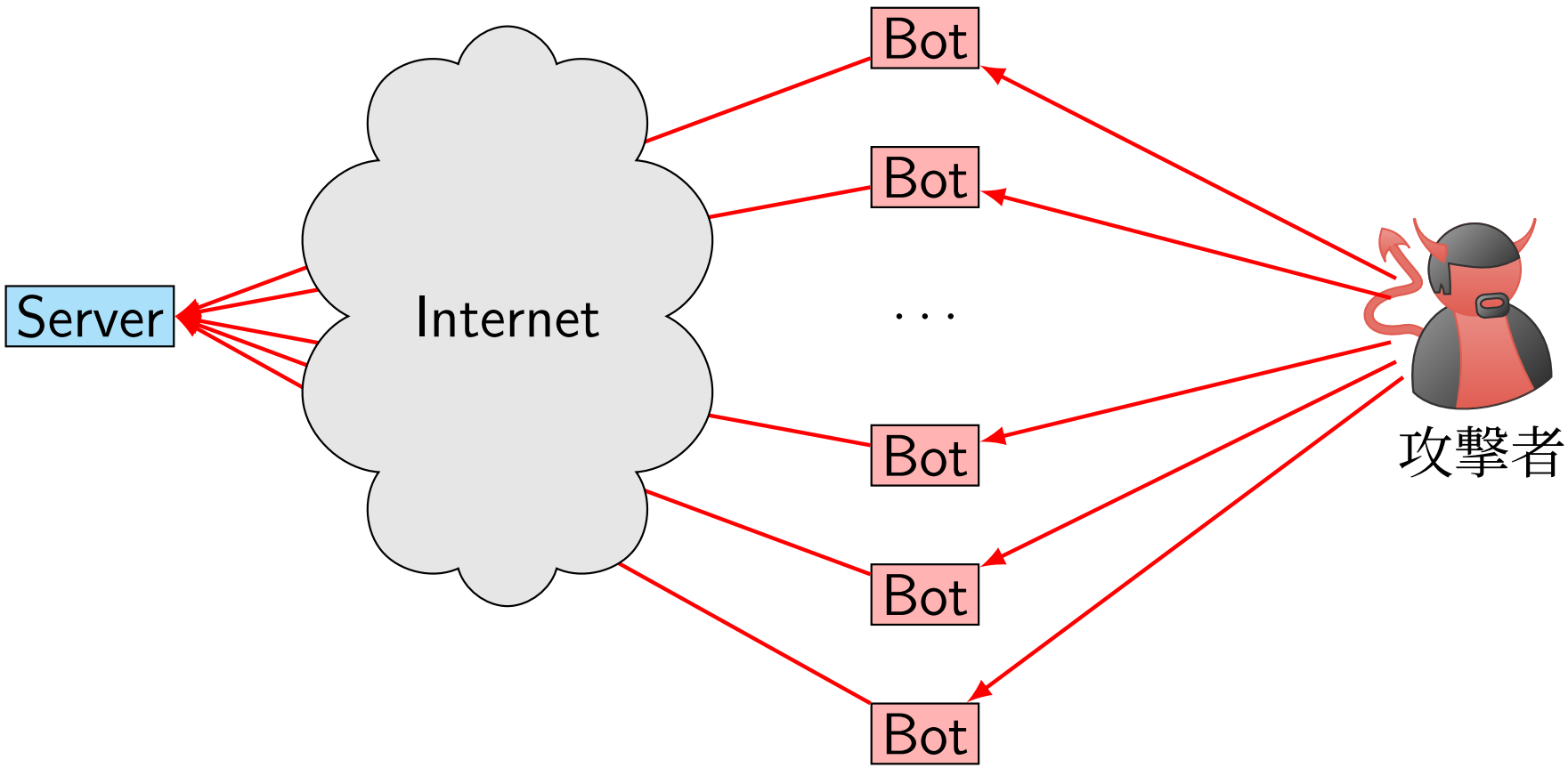
標的型攻撃メールを受信したことはありますか。

DoS (Denial of Service) 攻撃

- 攻撃によって、サーバの機能低下・停止を狙う
- マルウェアを使った攻撃
- 大量通信を使った攻撃
  攻撃する PC の能力も必要
- 一点から攻撃してくる場合には、FW 等で防ぐことができる

DDoS 攻撃: Distributed DoS

- bot を多数の PC へ伝染させる
- bot のネットワークを構築する
- bot が、一斉に対象となるサーバへ攻撃する
- インターネットの多数の点から攻撃してくるため、FW 等で防ぐことが困難


Server
Internet
Bot
Bot
. . .
Bot
Bot
Bot
攻撃者

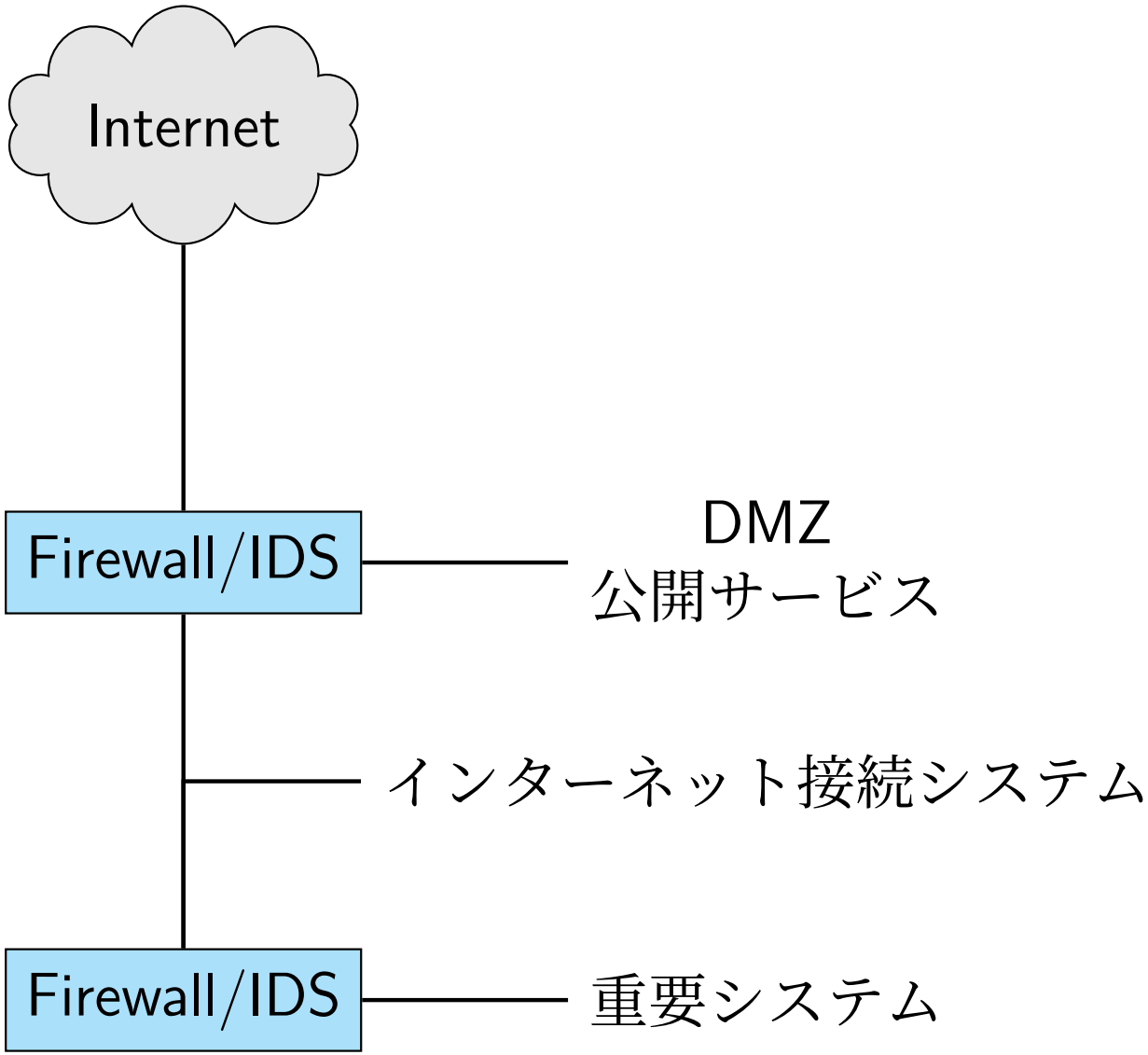
ネットワークからの不正侵入

- 脆弱なサーバへの侵入
  - ソフトウェア脆弱性
  - 設定不良
- 脆弱な通信装置: VPN 等
- パスワード窃取による侵入
- Trojan horse などのマルウェア

不正侵入対策

- ネットワークの分離
  - 重要情報を持つネットワークを切り離す
  - DMZ (DeMilitarized Zone) の設置
- サーバ、サービスにおけるアクセス制限
  - 接続元の制限
  - ユーザ制限

- Firewall
  - 送受信元、サービスで通信を制限
- IDP (Intrusion Detection System)
  - 侵入の兆候を検知して遮断
  - 接続時の振る舞いを分析等
  - サンドバック
    - 添付ファイル・ダウンロードファイルの振る舞いをシミュレーション


Internet
Firewall/IDS
DMZ
公開サービス
インターネット接続システム
Firewall/IDS
重要システム

ゼロトラストネットワーク: Zero Trust Networks

- モバイルデバイスの急速な普及
  - 組織のデバイスを外部で使用
  - 個人デバイスを内部へ持ち込む
- 境界での防衛ではもはや不十分
- 全てのデバイスを信用しない (zero trust)
  - デバイスの挙動をモニタリング
  - 不審なデバイスを検知し隔離

物理的不正侵入対策

- 部屋への立入り制限
- 入退室管理
  - IC カード等による施錠・開錠
  - 記録
- 監視カメラ
- 名札、服装
- デバイスの持ち込み制限

課題

adware について調べ、そのリスクを考察しなさい。