

情報セキュリティと情報倫理

第9回 ネットワークセキュリティ技術

2022/12/02

2022年12月2日

1

概要

- ①全学共通科目1年生後期
- ②金曜日五時限 (16:10-17:40)

③担当:

☆植田秀夫・永井孝幸・森真幸 (情報科学センター)

④評価方法 (予定)

☆毎回のミニレポート (20%)

△出席を前提とした課題内容 (予定)

☆1回程度の課題レポート (30%)

☆期末テスト (50%)



2

- ⑤参考書: 情報のセキュリティと情報倫理 (山田
☆ISBN978-4-595-31897-9 C1355 ¥26

- ⑥参考書: IT社会の法と倫理 第二版 (サラ・バ
☆ISBN978-4-89471-430-4 C3032 ¥3900E

2022年12月2日

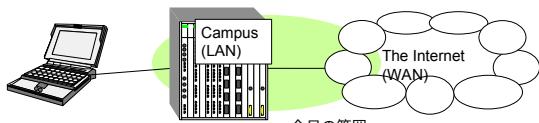
ネットワークセキュリティ技術

シラバスより

- ①インターネットにおける通信の仕組みと不正通信の事例を取り上げ、ファイアウォールやネットワーク侵入検知システムなど不正通信からの防御手段について議論する。

第8回 ホストセキュリティ技術

- ②パスワードによるユーザ認証やファイルに関するアクセス制御など、計算機を不正利用から防御する技術について議論する。



2022年12月2日

4

サイト(組織)の保護の方法

①ホスト・セキュリティ

☆個々のホストを個別に強化する

☆環境の複雑さと多様性

△バージョンの差、OSの差 etc...

☆アクセス権を持つユーザの善意と技能に依存

☆高いレイヤでの制御が比較的容易

△アプリケーションレベル

②ネットワーク・セキュリティ

☆サービスへのネットワークアクセスを管理

△ファイアウォールの構築

△強力な認証手段

△暗号化機能の使用

2022年12月2日

5

インターネットの基礎

キーワード

- ①サーバ・クライアントモデル
- ②パケット交換方式
- ③ゲートウェイ(ルータ)とホスト
- ④IPアドレス (IPv4)
- ⑤ISOのOSI階層モデル
- ⑥TCP/IP

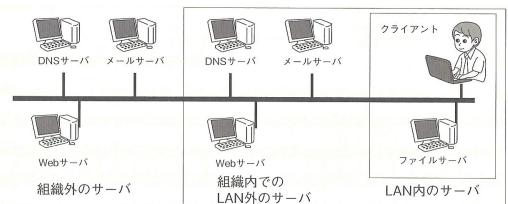
2022年12月2日

6

サーバ・クライアントモデル

- ①ホスト: インターネットに接続している機器
- ②サーバ: サービスを提供するホスト (常時稼働)
- ③クライアント: サービスを受けるホスト

サービスを、2種類のホストに分けて整備利用する方式



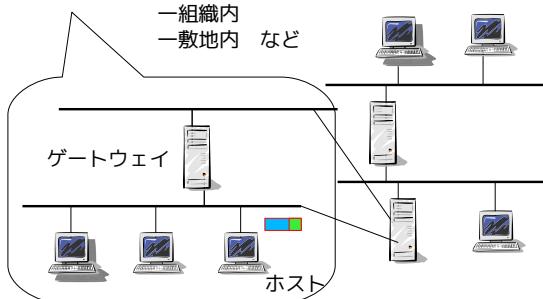
2022年12月2日

7

ホストとゲートウェイ

- ② ホップバイホップ型の通信

③ LAN (Local area network) WAN (Wide area network)



2022年12月2日

10

通信相手の識別

- ④ アプリケーション同士が通信をする

例: Web ブラウザと Web サーバ
 コンピュータ IP アドレス
 アプリケーション ポート番号

住所のようなもの
同居人の区別

IPAddr: 192.168.0.10



port: 49153

IPAddr: 133.16.240.10



port: 80

2022年12月2日

11

IPv4 (Internet Protocol version 4)

- ⑤ アドレス表記: 4 オクテット (32 ビット)

☆ 8 ビット (0 ~ 255) の数値を .(ドット) で 4 つ並べる

例 133.16.240.10 (10000101 00010000 11110000 00001010)

△ 次世代 (?) の IPv6 では 128 ビット

▼ 2001:02f8:0031:0000:0200:f8ff:fe71:7581

☆ ネットワーク部分とホスト部分に分かれる

△ ネットマスク (24 ビット長 or 255.255.255.0 等)

▼ 133.16.240.10 / 24 → .1 ~ .254 のホストが同居可能

△ ホスト部のビットがすべて 0 → ネットワーク自身

△ ホスト部のビットがすべて 1 → ブロードキャスト

▼ 当該ネットワークに属するすべてのホスト宛

→ 両端が使えない

[考えてみよう] : ネットマスク長 /28, /29, /30, /31, /32
実際のホストの存在できる最大数は ?

2022年12月2日

12

TCP/IP による通信

- ⑥ IP アドレスとポートによって通信が識別される

☆ ポートが異なれば別の通信 (コネクション)

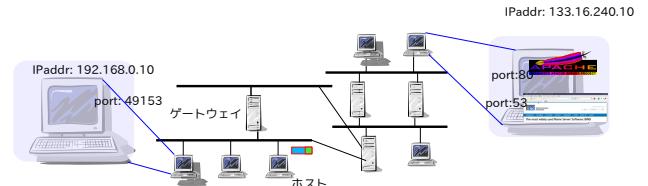
- ⑦ 途中の転送経路はゲートウェイ毎に自律的に決定

☆ 行きと戻りが同じ経路とは限らない

- ⑧ 双方向にパケットがやりとりできると通信可能

☆ 一方通行だけパケットが通っても通信自体は不成立

△ それでもある種の攻撃は可能な場合がある



2022年12月2日

15

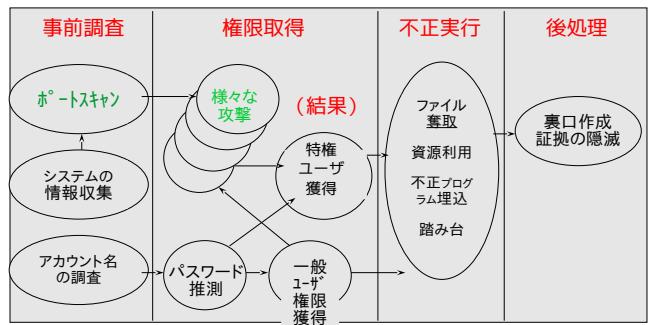
ネットワークへの攻撃と防御

2022年12月2日

17

1) 侵入の手口

- ⑨ 一般的な侵入は次の 4 つの段階を経て行われる



2022年12月2日

18

2. ポートと脆弱性（1）

② ポート（番号）

☆ インターネットで特定のサービスを通信させるための識別番号（1～65535まで）

③ プロトコル（HTTP、SMTP、POP3等）

☆ サービスを提供するための約束ごと（手順）

☆ Well-Known Port（標準ポート）の例：

⇒ WWWプロトコル（HTTP）→ ポート80番

⇒ メール送信プロトコル（SMTP）→ ポート25番

⇒ メール受信プロトコル（POP3）→ ポート110番

→ ポートスキャン

☆ 当該ホストで動いているサービスの調査

2022年12月2日

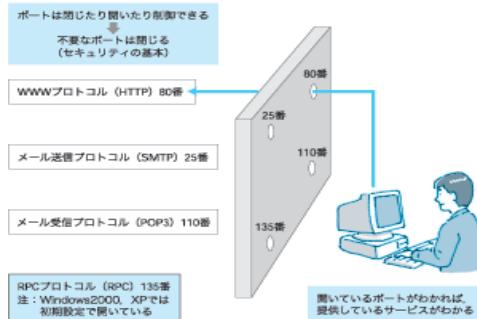
19

ポートスキャンの実例

```
# nmap -v -A 133.16.240.10
Starting Nmap 5.00 ( http://nmap.org ) at 2009-12-01 14:36 JST
NSE: Loaded 30 scripts for scanning.
NSE: Loaded 30 scripts for scanning.
Initiating ARP Ping Scan at 14:36
Scanning 133.16.240.10 [1 port]
Completed Parallel DNS resolution of 1 host at 14:36; 0.24s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 14:36; 5.53s elapsed
Initiating SYN Stealth Scan at 14:36
Scanning dsm02.dsm.cis.kit.ac.jp [133.16.240.10] [1000 ports]
Discovered open port 25/tcp on 133.16.240.10
Discovered open port 433/tcp on 133.16.240.10
Discovered open port 53/tcp on 133.16.240.10
Discovered open port 8080/tcp on 133.16.240.10
Discovered open port 993/tcp on 133.16.240.10
Discovered open port 80/tcp on 133.16.240.10
Discovered open port 22/tcp on 133.16.240.10
Discovered open port 110/tcp on 133.16.240.10
Discovered open port 587/tcp on 133.16.240.10
Increasing send delay for 133.16.240.10 from 0 to 5 due to 11 out of 34
Increasing send delay for 133.16.240.10 from 5 to 10 due to 11 out of 1
Increasing send delay for 133.16.240.10 from 10 to 20 due to max_send_size
Increasing send delay for 133.16.240.10 from 20 to 40 due to max_send_size
Increasing send delay for 133.16.240.10 from 40 to 80 due to max_send_size
Increasing send delay for 133.16.240.10 from 80 to 160 due to max_send_size
Increasing send delay for 133.16.240.10 from 160 to 320 due to 11 out of 1
MAC Address: 00:00:5E:00:01:D2 (USC Information Sciences Inst)
Device: generic purpose
Operating System: NetBSD 5.X
OS details: NetBSD 5.9.5
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=214 (Good luck!)
IPID Sequence Generation: All zeros
Service Info: Host: xen02.dsm.cis.kit.ac.jp; OS: NetBSD
Read data files from: /usr/pkg/share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 328.35 seconds
```

2. ポートと脆弱性（2）

ポートとプロトコル



2022年12月2日

21

2. ポートと脆弱性（3）

④ ポートが開いていると…

☆ 提供しているサービスがわかる

☆ 開いているポートを悪用して侵入・攻撃

☆ 脆弱性があると、さまざまな被害を受ける

（ウイルス感染、操作権限の奪取、DoS攻撃を仕掛けるプログラムの埋め込みなど）

⑤ 対策：

☆ 使わないポートは閉じる

☆ パッチを適用し脆弱性をなくす

Denial of Service
(サービス不能化攻撃)

検査ツール（例）

nmap (<http://www.insecure.org/nmap/>)

Nessus (<http://www.nessus.org/>)

2022年12月2日

22

ファイアウォール

1. ファイアウォールとは？
2. ファイアウォールの構成
3. パケットフィルタリング、
アプリケーションゲートウェイ、
プライベートアドレス
4. ネットワークアドレス変換技術（NAT）
5. DMZ
6. ファイアウォールの落とし穴
7. パーソナルファイアウォール

2022年12月2日

23

1) ファイアウォールとは？

インターネットと内部ネットワーク（LAN）の境界線上で、アクセス制御を行う装置

【ファイアウォールの主な機能】

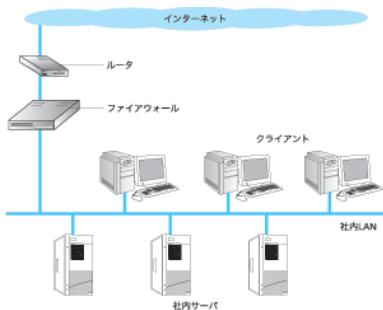
- ☆ 外部との出入口を絞る（例：特定のポートのみ通過）
- ☆ 内部ネットワーク（LAN）の構造を外部に見せない
- ☆ 外部からの不正なアクセスを排除
- ☆ 必要なアクセスだけを通過させる

2022年12月2日

24

2) ファイアウォールの構成

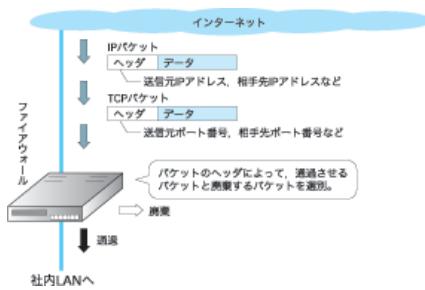
基本的なファイアウォールの構成



2022年12月2日

25

3) パケットフィルタリング



- ・パケットの情報に基づいて、通過させるパケットと通過させないパケットを選別すること。
☞ 通常は「通過を許可するパケットだけを指定」。

2022年12月2日

26

3) アプリケーションゲートウェイ

- ① アプリケーションプロトコルに基づいてアクセスを制御する
 - ☞ HTTP (Web アクセス)
 - 例: ☞ FTP (ファイル転送)
 - ☞ POP (メール受信)
 - ☞ SMTP (メール送信) など
- ② アプリケーションプロトコルごとに許可 / 禁止を制御可能
 - ☆ IP パケットレベルよりも詳細に制御可能
 - ☆ ログ記録が残しやすい
 - ☆ 複雑 (プロトコルの中身の知識が必要)

2022年12月2日

27

3) プライベートアドレスの割り当て

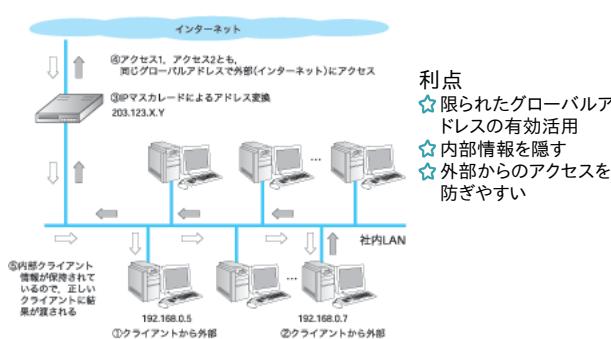
- ① グローバルアドレス
 - ☆ インターネットに接続する各機器に一意に割り当てられた IP アドレス
- ② プライベートアドレス (RFC1918 での規定)
 - ☞ 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
 - ☆ 組織や会社内の閉じられた空間で独自に割り当てられた IP アドレス
 - ☆ グローバルアドレスの不足を補う
 - ☆ そのままではインターネットにアクセスできない
☞ 変換作業が必要 (NAT など)
 - ☆ 外部からアクセスされない利点もある
- ③ リンクローカルアドレス (RFC3927 での規定)
 - ☞ 169.254.0.0/16 (AutoIP とも呼ばれる)

2022年12月2日

28

4) ネットワークアドレス変換技術(NAT)

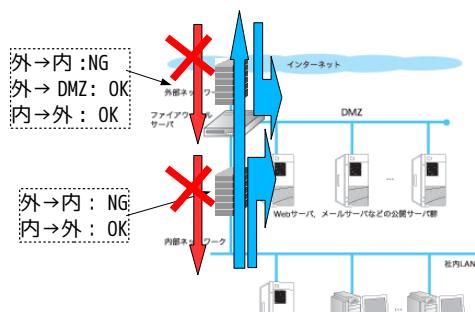
ネットワークアドレス変換 (NAT : Network Address Translation)
・内部の(プライベート)アドレスを外部の(グローバル)アドレスに変換し、
インターネットへのアクセスを可能にする技術



2022年12月2日

29

5) DMZ (DeMilitarized Zone: 非武装地帯)



外部のインターネットと内部の LAN の間に緩衝地帯を設け、公開サーバを設置

2022年12月2日

30

6) ファイアウォールの落とし穴

② ファイアウォールも万全ではない

- ☆ 例: DoS 攻撃やウイルスは防げないこともある
- ☆ 通信可能にしてある Web サーバへの DoS 攻撃
- ☆ メールに添付されているウイルス

③ NAT はファイアウォールではない

- ☆ NAT 機能付ルータ ≠ ファイアウォール
- ☆ 通信ポートを塞いでいるわけではない
- ☆ NAT 機器自体が狙われている

④ 過信せずにあらゆるセキュリティ対策を行うことが肝要

- △ 例) ファイアウォールがあるからアンチウィルスソフトは不要
.....、というわけではない!

2022年12月2日

31

家庭用ルータが狙われている

・ 安易な設定のものが多数存在

The screenshot shows a network diagram with a router, a computer, and a mobile device connected. Below it is a screenshot of a software interface with various configuration options and a search bar.

http://blog.trendmicro.co.jp/archives/11200

2022年12月2日

33

参考 : NOTICE (<https://notice.go.jp/>)

The ACTIVITIES section shows a flowchart where NICT (情報通信研究機構) performs '機器調査' (device investigation) and '情報提供' (information provision) to 'インターネットプロバイダ' (Internet Service Provider), which then triggers '注意喚起' (warning notice) to '機器の利用者' (device user). The user can then contact 'NOTICE サポートセンター' (NOTICE support center) for 'ユーザサポート' (user support).

<https://www.nict.go.jp/press/2019/02/01-1.html>

2022年12月2日

34

参考事例：古い機器を使い続けられる？

② 使えるうちは使い続けてしまうのが人情

- ☆ 何が通信機器なのか判りにくい

③ 古い通信規格 (WEP) にしか対応していない

- ④ 容易に悪用可能な脆弱性がある

The page discusses the discontinuation of the 'Nintendo-Wi-Fi USBコネクタ' and 'Nintendo-Wi-Fiネットワークアダプタ'. It states that these products have been discontinued since 2005 and 2008 respectively, and that users should stop using them due to security risks. It also notes that the WEP protocol is easily exploitable.

<https://www.nintendo.co.jp/support/information/2022/0720.html>

2022年12月2日

35

4. サーバへの攻撃(サービス妨害)

1. DoS 攻撃(サービス妨害攻撃)

- DoS: Denial of Service

2. DDoS 攻撃(分散 DoS 攻撃)

- DDoS: Distributed DoS

3. メール攻撃

2022年12月2日

36

1) DoS 攻撃 (Denial of Service)

② サーバに過大な負荷をかけ、パフォーマンスの低下やサービス停止に追い込む攻撃

③ ping の悪用など、さまざまな攻撃手法がある

- △ ping = ネットワーク検査ツールの一つ
到達性の確認など

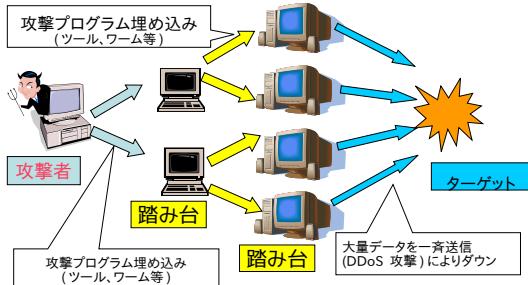
④ DoS 攻撃を行うコード (プログラム) を仕込むウイルスも登場している

2022年12月2日

37

2) DDoS 攻擊 (Distributed DoS)

- ⑤ 密かに攻撃プログラムを埋め込まれて DoS 攻撃に加担することがある



2022年12月2日

38

DDoS 攻撃の実例

The screenshot shows a news article from Ars Technica. The headline reads "Record-breaking DDoS reportedly delivered by >145k hacked cameras". Below the headline is a sub-headline: "Ars Technica security / 2016/09/29/hacked-or-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/". The main text discusses a massive DDoS attack originating from over 145,000 hacked cameras. The article includes a quote from a researcher at the University of California, Berkeley, and a link to a GitHub repository containing the exploit code. The background of the page features a large image of a city street at night with a person walking in the foreground.

39

3) メール攻撃

- ② メールサーバに大量のメールを送り付ける
☆ メールサーバのパフォーマンス低下や機能停止

- ⑤ 第三者中継機能を悪用
 - ☆ スパムメールの踏み台として利用される
 - ⑥ バウンスメール（エラー通知）を悪用
 - ⇒ バックスキャッター

2022年12月2日

2022年12月2日

2022年12月2日

40

4) ボットネット (botnet)

- ⑤ 悪意のある攻撃者によって構築され、インターネット経由の指令によって遠隔操作を可能としたコンピュータ群
 - ☆ ウィルスプログラムで感染
 - ☆ 数百台から数千、数万台のものもあると言われている
 - ☆ 感染 PC はゾンビ PC とも呼ばれる
 - ⇒ 知らぬ間に加害者側にまわることに
 - ☆ DDoS 攻撃だけでなく、大量 SPAM 発信やアカウント破りにも使用
 - ⇒ みかけ上の計算パワーが大きい
 - ⇒ 足が付きにくい
 - ⇒ アンダーグラフナーの温床？

関連記事：<http://www.itmedia.co.jp/news/articles/1003/04/news019.html>

2022年12月2日

42

IDS (Intrusion Detection System)

- ③ 侵入検知システム (IDS)
 - ☆ ファイアウォールで防げないものに対応
 - ⇒ http (80/tcp) を塞いではサービスできない
 - ☆ 「やばい」アクセスを検知→報告 (アラート)
 - ⇒ シグネチャベース (特徴一致)
 - ⇒ アノーマリティテクション (異常判定)
 - まだまだ研究の余地あり(いたちごっこ?)
 - ④ IPS (Intrusion Prevention/Protection System)
 - ☆ 侵入予防・保護システム
 - ☆ IDS に、防御機能を付加したもの
 - ⇒ フォールスポジティブ (誤検知)
 - ⇒ フォールスネガティブ (見過ごし)

2022年12月2日

43

無線 LAN の問題

- ② 通信傍受、
不正な利用、
プライバシー
☆ Evil Twin
- ② 技術基準適合証明
(技適) 問題



2022年12月2日

総括

② ネットワークセキュリティ技術

2022年12月2日

47