第15回: 情報ネットワーク

花田 英輔
hanada@cc.saga-u.ac.jp
数理・情報部門

1

アプリケーション層

- 具体的な通信内容(データ)がやり取りされる層
- アプリケーション(サービス)によって異なる
  - 主要なサービスでは、プロトコルや利用するポート番号などが決められている
    では誰?(どこ?)が決めている?
  - 独自アプリは?
    - 自分でこれらを決めなければならない

2

プロトコル等の仕様について

- インターネットに関する多くの仕様
  - IETF(Internet Engineering Task Force)から公開
  - 専門家が話し合いなどを行い文章を公開
    - RFC(Request for Comments)
    - 基本的にテキストファイル
    - 個別に番号が振られる(例: RFC791)
  - アプリケーションに限らない
    - IPv4,IPv6, TCP等の仕様なども
      - IPv4: RFC791, IPv6: RFC1883, TCP: RFC9293 など
      - 改良があるため、一つのRFCで書かれていない場合も多い

3

プロトコル等の仕様について

- RFC による公開仕様を元にソフトウェアを作成
  - サーバ、クライアント等でお互いに通信が可能
- 自らがプロトコルを提案してRFCを公開することも可能
  - それが実際に利用されるかは別
  - プロトコルを公開しないとソフトを作ってもらえない
    - もちろんRFCとして公開しなくても良い
    - API として公開されることもある
      - Application Programming Interface

4

情報ネットワーク

ネットワークセキュリティ概要

5

ネットワークを運用する上での脅威

- 何に困るのか?
  - ネットワークが遅い
  - ネットワークが使えない
  - サーバにアクセスできない
  - ネットワークを通して攻撃を受ける
  - ネットワーク上で情報が傍受される
  - ネットワーク上に嘘の情報を流される

6

脅威への対処に向けた分類

- 脅威への対処は誰がするのか？
  - サーバが行うべきこと（ネットワークではない）
  - ネットワーク機器で行うこと
    - ユーザ認証？
    - 端末の確認？
  - アクセス権限で行うこと
    - サーバの権限？（ネットワークではない）
    - ネットワークの権限？
  - 流通するデータへ工夫すべきこと

2026/7/28 佐賀大学

7

ネットワークのセキュリティ

- セキュリティを高めるための要素
  - 接続にかかるセキュリティ
  - ユーザにかかるセキュリティ
  - データにかかるセキュリティ
  - 端末にかかるセキュリティ
  - サーバにかかるセキュリティ

2026/7/28 佐賀大学

8

ネットワーク接続にかかるセキュリティ

- 不正接続(不正侵入)の防止
  - 登録済端末のみ接続を可とする
    - MACアドレスフィルタリング
    - 証明書・ユーザ認証
  - 接続時にウイルススキャン
    - 検疫（RADIUS等）
  - 接続範囲の限定
    - ESSIDによる接続制限（無線LAN）
    - VLANによる通信範囲の制限

2026/7/28 佐賀大学

9

接続時認証と検疫

① 認証
- ネットワークへの接続の可否をID+パスワードやMACアドレスなどを確認して判断
  - RADIUS、ユーザベースVLANなど

② 検疫
- ネットワークに接続しようとする機器にコンピュータウイルス・セキュリティホールが無いかを確認してから接続させる

2026/7/28 佐賀大学

10

RADIUSを用いた接続制御

- RADIUS：Remote Authentication Dial In User Service
  - IP上のプロトコル

  (利用目的)ネットワーク上のサーバコンピュータに、ネットワーク資源の利用の可否の判断(認証)と、利用の事実の記録(アカウンティング)を一元化すること
- IEEE 802.1xと組み合わせることで、RADIUSサーバによって認証された利用者のみに対してLANを利用させることが可能
  - IEEE 802.1x：LANの利用の可否を制御する、イーサネット上のプロトコル

2026/7/28 佐賀大学

11

検疫での検査項目(Soliton社の例)

- **主な設定項目**
  - OSのセキュリティパッチ適用状況
  - ウイルス対策ソフトウェアの更新状況
  - 任意のソフトウェア/プロセスの有無
  - 任意のサービスの有無や状態
  - コンピュータ名
  - Windowsドメイン名/ワークグループ名など
- **再検疫機能**
  - ネットワークの利用開始時に加え、定期的にPCの状態を検疫条件と照合し、不適合なPCをネットワークから自動で切断可能
  - 業務時間内の使用を禁止しているソフトウェアの利用なども発見可能

2026/7/28 佐賀大学

12

（参考）検疫とは

- 本来は医学用語（法律用語でもある）
  - 全国の主要な空港・海港に設置された検疫所又は動物検疫所、植物防疫所で実施
  - 感染症が拡がるのを防ぐため、ある地域に出入りする人や物（動植物・食品）を検査し、必要な処置（診察、検査、隔離など）をとること
  - 日本における検疫の手続は検疫法などの法令による
    - 検疫法の目的：国内に常在しない感染症の病原体が国内に侵入することを防止することなど（検疫法第1条）
  - 日本における人や食品の検疫は厚生労働省が、動植物の検疫は農林水産省が担当

13

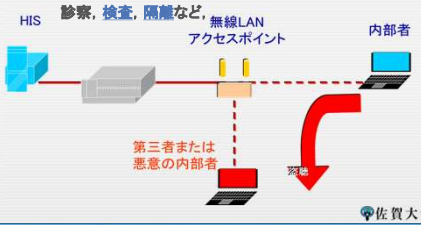
ネットワーク上のデータの暗号化

- データは傍受されることを前提に送る必要がある
  - 無線電波はアンテナさえあれば受信は可能
- 受信されても暗号化しておけば解読できない
  - 暗号化手法のセキュリティの強さに要注意
- 暗号化してもデータ自体の傍受は防げない
  - 他の技術（VPN、SSL、VLAN等）との組み合せが必要

14

無線LANの傍受対策

- 盗聴による情報流出防止対策
  - 無線LANでは暗号化は必須
    - 現時点ではWPA2による暗号化を推奨
  - 複数のSSIDを用いてVLANで分割し論理的に隔離することも可能



15

主な無線LANの暗号化方式

1 WEP：Wired Equivalent Privacy

- 無線電波自体を暗号化
  - 無線電波自体が暗号化されている状態で送信
- 暗号キーを生成する乱数列（IV）は24bitから128bitまで
  - 悪意の盗聴・解析に会わず、通常のアクセス環境であれば問題はない
- デメリット
  - WEPキー暗号化解析ソフトが出回わっている
  - 通信パケットを一定期間収集し解析ソフトを使うと乱数列（IV）解読の危険性あり

16

主な無線LANの暗号化方式

2 TKIP：Temporal Key Integrity Protocol

- Wi-Fi Alliance策定規格
- 暗号化キーを生成する乱数列(IV)を24bitから48bitに強化
  - 数ヶ月間パケット収集しても解読困難
- 暗号キーの交換を実現
- デメリット
  - ソフトウェア処理である
    - ファームウェアのバージョンアップで、既存のWEP対応機器をアップグレード可能
    - 処理スピードの低下あり

17

主な無線LANの暗号化方式

3 AES：Advance Encryption Standard

- WEP脆弱性の原因のひとつ（暗号化方式(RC4)）を抜本的に見直した方式
  - 現時点では解読手法は存在しないとされる
- 暗号キーの交換を実現
  - WEPでは暗号キーの交換ができないがWPA-PSK(AES、TKIP)はアクセスポイントとクライアント間で暗号キーの交換が可能
- デメリット
  - ハードウェア処理のため処理スピードの低下はないが、既存の機器の一部は対応不可

18

3つの暗号化方式の比較

名称	WEP	TKIP	AES
暗号の種類	RC4	RC4	AES
セキュリティ強度	△	○	◎
暗号キーの交換	×	○	○
処理形態	ハードウェア処理	ソフトウェア処理	ハードウェア処理
通信速度の低下	低下なし	低下あり（10%～20%）	低下なし
対応機器	これまで多数	ファームウェアのバージョンアップで対応可	現在の主流

Buffalo社ホームページより
http://buffalo.jp/products/b-solutions/netsecurity/wireless-security.html

※アクセスポイントと各端末に共通のキーを設定する
使い勝手はすべて同じ

2026/7/28 佐賀大学

19

無線LANの暗号化方式の主流

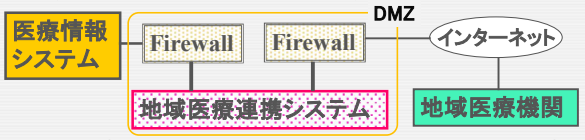
- WPA2：Wi-Fi Protected Access 2
  - 国際標準IEEE 802.11iの完成版を元にしている
  - AESを用いたCCMP（Counter mode with CBC-MAC Protocol）を採用（WPA2-AES）
  - 最長256ビットまでの強力な暗号鍵を利用可能
  - 「パーソナルモード」と「エンタープライズモード」がある
- WPA3:Wi-Fi Protected Access 3 (2018年6月発表)
  - 利用者が入力したパスワードから算出した値と乱数を用い、楕円曲線暗号によって認証を行う「SAE」（Simultaneous Authentication of Equals）方式を採用
  - WPA3対応機器はWPA2対応機器とWPA2を用いて通信可能

2026/7/28 佐賀大学

20

ネットワーク機器で実行可能な対処

- ファイヤーウォール
  - 2つのネットワークの間に挟む機器
  - 使用例（病院が持つ地域医療連携システム）



  - 医療情報システムから地域医療連携システムへは接続できるが、インターネットには接続できない
  - インターネットから地域医療連携システムへは接続できるが、医療情報システムには接続できない
  - Firewallは地域医療連携システムから外へはつながない

2026/7/28 佐賀大学

21

ファイヤーウォールで可能なこと

- 信頼できる発信源からの通信のみ通す
  - IPアドレスによる判断
- パケットの内容を確認して通す／遮断
  - プロトコル・ポート番号による判断
- 認証サーバを通した接続
  - 通信開始時に強制的に認証サーバを通させる
  - OpenFlowもこの一環
- SDN(Software Design Network)とは異なる
  - SDNの目的には含まれる

2026/7/28 佐賀大学

22

しかし不正アクセスは起きる

- 正しく接続可能な端末が乗っ取られると
  - 接続拒否ができない
  - 通信内容(パケットの中身)まではチェックしにくい

→ 不正侵入され、ウィルスが置かれる要因

- 医療機関における不正侵入例
  - 徳島県つるぎ町立半田病院(2021年)
  - 大阪急性期・総合医療センター(2022年)

→ いずれもランサムウェアによる被害

  - システム停止によって病院機能停止

2026/7/28 佐賀大学

23

ネットワークセキュリティまとめ

- セキュリティを高めるための要素
  - 通信に関する部分は以下の通り
    - 接続にかかるセキュリティ:認証・検疫
    - ユーザにかかるセキュリティ：認証
    - データにかかるセキュリティ:暗号化
    - ネットワーク機器によるセキュリティ:ファイヤーウォール

2026/7/28 佐賀大学

24

今回の課題

1. 今回の講義内容をまとめなさい。
2. ランサムウェア被害の代表例である大阪急性期・総合医療センターの被害について
   - 不正侵入の経路とそれを許した要因
   - 被害を受けて取られた対策

   を調べて記せ。
   - 本やホームページを参考にした場合は、参考文献として記述すること

   A4 2～3ページ程度にまとめること（もう少し多くてもよい）

   締切：8月3日（日）18:00 （締切厳守！）

25

定期試験について

- 日　時：8月5日(火)の3校時に実施
- 場　所：人数が多いので教養2号館3階2301講義室での実施となります
  - 自由席制にする予定です
  - 基本的にやり方は中間試験と同様です
    - （規則なので）学生証を忘れずに
- 出題範囲
  - 中間試験以降の内容がメインですが、前半部分からも出題します
    - 今回の内容からも出るかも？

26

授業評価アンケートについて

- 授業評価アンケート(Live Campus内)に協力を！
  - 8月8日(金)までに入力してください
  - 「教員ごとの指定項目」は以下の通り
    - E：毎週の課題について
      - E-1：毎週の課題の内容は適切だったと思いますか
      - E-2：課題の提出方法は適当だったと思いますか
      - E-3：課題の締切設定は適当だったと思いますか
  - アンケートへの入力内容は採点対象外です

27