令和6年度医療情報セキュリティ研修 及び
サイバーセキュリティインシデント発生時初動対応支援・調査等事業

【システム・セキュリティ管理者向け研修】
連携Aコース
～ ネットワーク基礎編 ～

大阪大学　D3センター　教授　CISO
猪俣　敦夫
Ph.D, RISS, CISSP

自己紹介（いのまたあつお）

大阪大学　教授

D3センター、大学院情報科学研究科

情報セキュリティ対策室室長, OU-CSIRT隊長

- (一社)　公衆無線LAN認証管理機構　代表理事
- (一社)　ライフデータイニシアティブ(LDI)　理事
- (一社)　大学ICT協議会（AXIES）理事
- (一社)　JPCERTコーディネーションセンター　理事
- 京都女子大学、東京薬科大学、慶應義塾大学、NAIST、東京電機大学　他
- 経済産業省　ソフトウェアセキュリティTF委員
- 総務省　公衆無線LANセキュリティ委員会座長
- 2025大阪・関西万博サイバーセキュリティ有識者会議委員
- (株)カプコン　セキュリティ監督委員
- 阪急阪神HD (株)　サイバーセキュリティ顧問
- (株)ベネッセHD　情報セキュリティ監視委員
- NEXCO東日本・中日本・西日本　ETC開発委員、　他多数
- IPA 情報処理安全確保支援士　特定講習講師
- 大阪府警、奈良県警察サイバーセキュリティアドバイザ
- NTT西日本情報漏洩事案内部調査委員会 委員
- 大阪急性期・総合医療センターインシデント調査委員会委員長、他

はじめに　連携コースについて

医療機関では、情報システムの調達においてセキュリティ要件を提示せず、ベンダーに対策を依存している傾向があります。

ベンダー側としても医療情報システム全体の構成やセキュリティ要件に関して、顧客からの具体的な指示がなければ、提案に盛り込む機会を逸し、提案時にはセキュリティ要件が検討されず調達が済んでしまう状況です。

連携コースは、以下のA・B・Cの3コースで構成しています。（各コース　単体での受講可能）

- **連携Aコース**
  連携Bコース（ワークショップ）、連携Cコース（机上演習）に必要な前提スキルとなるネットワーク基礎、セキュリティ基礎について学習
- **連携Bコース（ワークショップ）**
  ネットワーク更改にむけて、RFP（提案依頼書）、RFI（情報提供依頼書）に必要な要素について学習
- **連携Cコース（机上演習）**
  インシデントハンドリングに使用できるネットワーク構成図の作成・管理について学習

はじめに　連携コースについて

目的

連携Bコース(ワークショップ）では情報システム調達時に実施するRFP（提案依頼書）、RFI（情報提供依頼書）作成について、連携Cコース(演習）はインシデントハンドリング時において有用となるようなシステム構成図の作成を学ぶことで、**ベンダーに対するセキュリティ対策の依存関係を改善する目的としています。**

そこで連携Aコースでは、システムセキュリティ管理者の方が、上記を作成するうえで技術的に理解が必須な知識として、ネットワーク基礎でのプロトコル、そのプロトコルがOSI参照モデルのどのレイヤーに関わるかなどを学びます。

医政局参事官室0

今日のゴール
連携Aコース　ネットワーク基礎編

- ベンダー任せで自組織のネットワークがブラックボックスになっていないでしょうか
- ベンダーと技術的な視点でやり取りできるようになるためには、ネットワークのどのような知識をえておけば良いでしょうか
- もちろん、全てを網羅して理解することはそれなりの時間がかかりますが、今日はその中でも特に知っておいてほしい部分のみを取り上げます

スライド 5

医政局参事官室0 →SAJ様

今回の研修内容は連携B,Cコースにつなげる内容になるかと思いますが、どのようにつながるのでしょうか。その辺りの意図も含めて頂いた方が良いかと思います。

それに付随して、医療機関でなぜこの知識を持っていればよいかが伝わりずらいので、

まず初めにどういう風に医療機関で使えるのか、役立つのかがイメージとして分かりずらいので、ご説明をお願いできますでしょうか。

また、最後の方で、医療機関で使うイメージや例を紹介いただけますと伝わりやすいかと思います。

医政局参事官室, 2024-11-20T06:50:44.122

理解してほしい知識

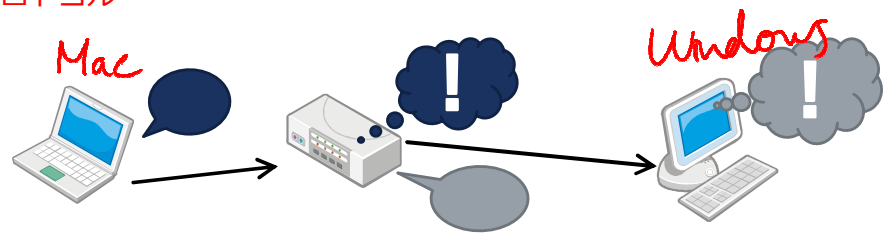
- プロトコルとOSI参照モデル
- レイヤ1 物理層：信号とケーブル
- レイヤ2 データリンク層：MACアドレス
- レイヤ3 ネットワーク層：IP、ICMP、ルータ、グローバルアドレス
- レイヤ4 トランスポート層：TCP、UDP、VPN
- レイヤ7 アプリケーション層：C/S（クライアントサーバ）、HTTP

1. プロトコルとOSI参照モデル

プロトコル（PROTOCOL）

- コンピューターを接続するには何かしらの規格（取り決め）を決めておく必要がある
  - どの参事官室0ーブルでつなごうかな？
  - 開始と終わりはどうしようかな？
  - どのぐらいの大きさにデータを分割してパケットにしようかな？
  - 分割したモノを組み立て直すときはどうしようかな？
- 人間の会話に言語が存在するのと同じで、コンピュータ同士でもルールが必要

  ➔これがプロトコル



スライド 8

参事官室0　コンピュータのことでしょうか？
参事官室, 2024-11-20T01:12:30.270

美和0 0　コンピューターに変更しました。
和田 美恵, 2024-11-22T09:48:14.805

参事官室0

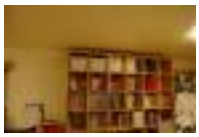
階層化という考え方（とっても重要）

- 通信プロトコル
  - コンピューター同士が通信するための手順、取り決め
  - みんなバラバラだったらどうだろう

→内容ごとに階層化（レイヤーに分けて）して仕事をすれば？

→OSI(Open Systems Interconnection)参照モデル

引っ越しの時は
荷物がバラバラ



引っ越しした先では、
きれいに階層化して
整理してみたら？

スライド 9

参事官室0　コンピュータ？
参事官室, 2024-11-20T01:12:58.323

美和0 0　コンピューターに変更しました。
和田 美恵, 2024-11-22T09:48:40.333

OSI参照モデル

- 仕事の分業モデルをうまく取り入れた
- プロトコルを役割毎に分類
  - 別の階層の処理については関知しない！

第○層とかレイヤ○
とか呼ばれる

Web(HTTP)、メール、
文字コードなどのそれぞれ
のアプリケーションに使う
フォーマットなど

宛先までの転送経路、
パケットが失われたときの再
送の仕組みなどなど

UTP(イーサネットケー
ブル)、光ファイバ、
無線などなど

第7層	アプリケーション層
第6層	プレゼンテーション層
第5層	セッション層
第4層	トランスポート層
第3層	ネットワーク層
第2層	データリンク層
第1層	物理層

異国の人同士がおしゃべりするためには

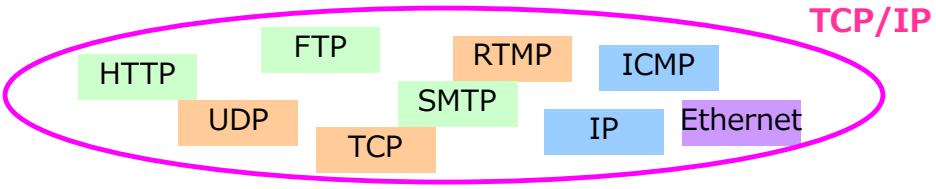
- 異なるシステムコンピュータ同士で会話をしたい

どんなケーブルをつなげられるかな？
どんな方法でデータ送ったらいいかな？
どういった流れに沿って送ればいいかな？

TCP/IPという決まりごと
に従ってみようよ！

TCP/IP

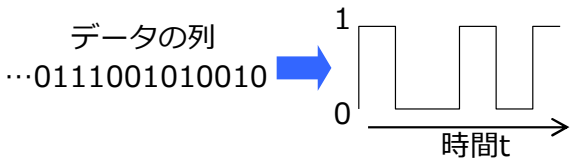
- Transmission Control Protocol / Internet Protocol
  - 通信プロトコルの集合体
  - OSI規格よりシンプル→大きく普及
  - インターネットでは、TCP/IPのプロトコルスイートに含まれる色々なプロトコルが使われている



2. レイヤ1 物理層：信号とケーブル

レイヤ１：物理層

- 階層化モデルの最下層を支える
  - コンピュータのデータ（0と1からなる符号）とネットワーク媒体上を流れる電気信号を変換する
- データを流すための物理媒体
  - 有線
    - 同軸ケーブル、イーサネット(LAN)ケーブル、光ファイバ　など
  - 無線
    - 802.11a/g　など
  - リピータ
    - 中継器



3. レイヤ2 データリンク層：MACアドレス

レイヤ２：データリンク層

- 送信元ハードウェア（NICなど）から送信先ハードウェア（NICなど）にデータを伝送する
- 伝送誤りを見つける（修復はしない）
- 伝送路内でデータを制御する
  - 例：速度の速い送信者が、受け取りの遅い受信者にどんどんデータを送りつけてあふれさせないようにする

データの交通整理

レイヤ２：データリンク層

- 1つの物理媒体（有線や無線）上の通信
  - 1本のケーブル（ないし無線）を共有するので端末ごとに区別できるように何らか固有のIDが必要
- 特定できたらようやく端末間で通信できるようになる
  - 例：ホストA-ホストC

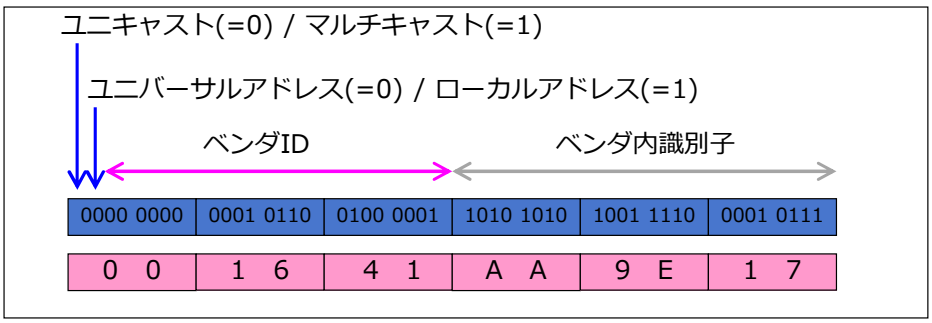
レイヤ２：フレーム化

- 物理層を流れるビット列(01001・・・)を適当な長さに区切った塊
  - どこが区切りか分からない
  - ノイズによって誤りがあるかも分からない
- フレームのメリット
  - 連続したビット列をいくつものフレームに分けてフレームごとに制御する
    - 区切ることで扱いやすくなる例（＾－＾）
    - allworkandnoplaymakesjackadullboy

All work and no play makes Jack a dull boy.

レイヤ２：
MACアドレス(MEDIA ACCESS CONTROL ADDRESS)

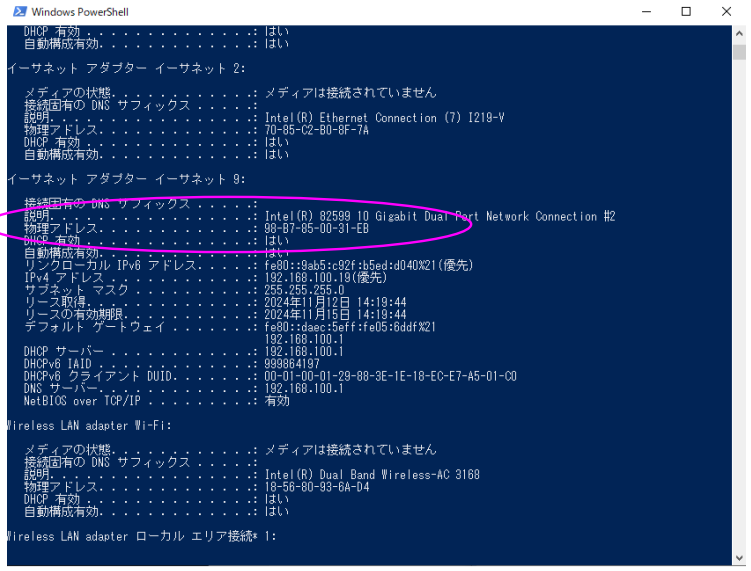
- ハードウェアの識別番号
  - ベンダ(製造メーカ)ごとにIDが決められており、製品1つ1つに重ならないようにMACアドレスの割り当てを行っている
- 先頭1ビット目、2ビット目は通信の種類
- 長さは48ビット
  - 2進数で48桁＝16進数で6桁
  - コロン(：)で区切って表記する、通例アルファベットは大文字



MACアドレスを調べてみよう

- Windows
  - Windows Powershellやコマンドプロンプトcmd.exe を起動
  - コマンド:　ipconfig /all
- MacやLinuxなどUNIX系OS
  - ターミナルからコマンド:　ifconfig –a

- 練習：皆さんのスマホに搭載されているWi-FiデバイスおよびBluetoothデバイスのMACアドレスを確認してみてください



4. レイヤ3 ネットワーク層：IP、ICMP、ルータ、グローバルアドレス

レイヤ３：ネットワーク層

- データリンク・物理層(L2, L1)
  - 実際の配送を行ってくれるトラックや貨物列車
- ネットワーク層(L3)
  - 荷物の発送所、貨物ターミナルでの作業
- L3プロトコル
  - IP(Internet Protocol)
    - 荷物が近くから遠くまで宛先住所に届くよう手配する
    - 上位層から預かった大きな荷物(データ)は分割して発送(パケットに分割)
  - ICMP(エラー処理、制御)
    - どのようなエラーが起こったか? その理由

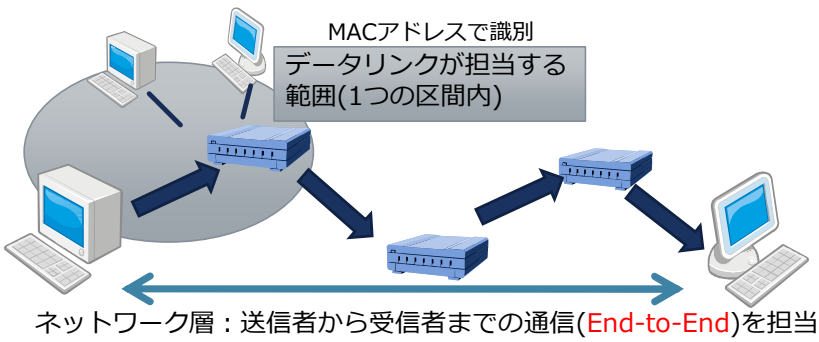
貨物列車

貨物ターミナル駅

今一度整理：L2とL3の担当は？

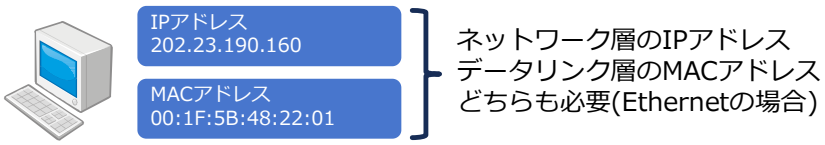
- データリンク
  - 1つの小さなネットワーク区間内(たとえば研究室内など)の通信ができるようにする
- ネットワーク層
  - 送信者から受信者まで(End-to-End)の通信ができるようにする

宛先にたどり着くまでにはどちらも必要



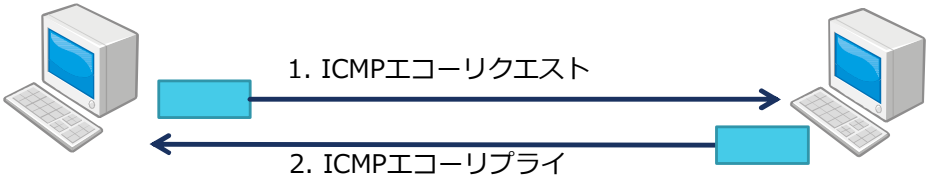
レイヤ３：IPアドレス

- データリンク層のMACアドレスとの違い
  - MACアドレス
    - 小さな1つのネットワーク(同一リンク)内の計算機識別に利用
      - もちろん、誰もが重複することの無いようにアドレスは世界で唯一つ
      - Ethernet以外のデータリンクとしてFDDIやATMなどにはMACアドレスはない
  - IPアドレスはデータリンクの種類にかかわらず同じ形式



ICMP(INTERNET CONTROL MESSAGE PROTOCOL)
事例：生存確認：PING (ICMP ECHO)

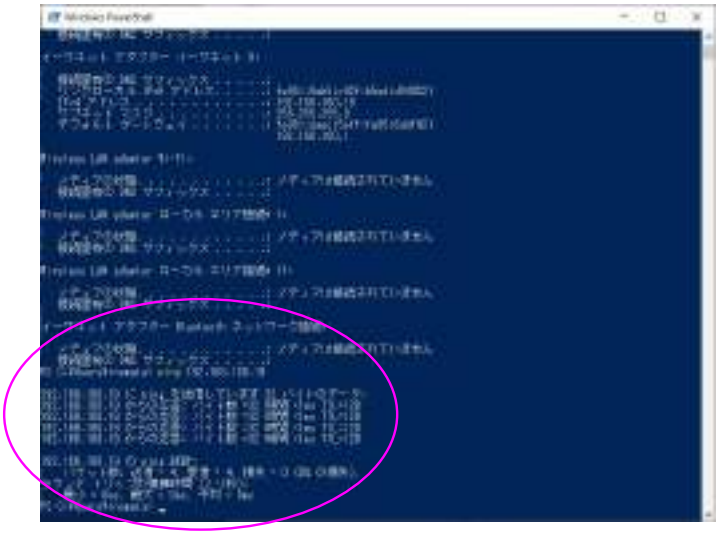
- コマンド: ping hostname or IP address
  - # ping www.osaka-u.ac.jp
  - 生存確認だけでなくRTT(Round Trip Time: 往復時間)を計測



  - セキュリティの理由からpingの返事をしないこともある
    - これは何故でしょうか

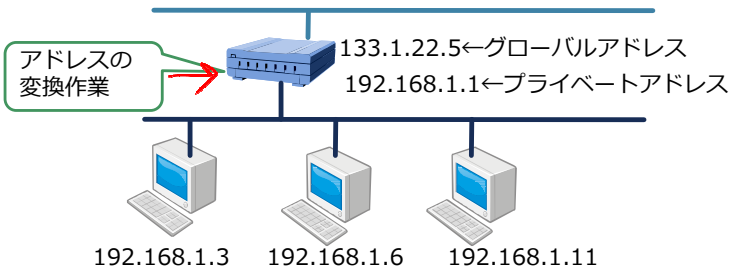
IPアドレスを調べてみよう

- Windows
  - Windows Powershellやコマンドプロンプトcmd.exe を起動
  - コマンド:　ipconfig /all
- MacやLinuxなどUNIX系OS
  - ターミナルからコマンド:　ifconfig –a
- 練習：皆さんのPCのIPアドレスを調べてpingコマンドを自分自身に打ってみよう



プライベートアドレスとグローバルアドレス

- NAT(Network Address Transition)
  - 1つのグローバルアドレスを複数のプライベートアドレスで共有
    - プロバイダ(ISP)と契約しているネットワークなど
      - 個々のPCはプライベートアドレスだが、インターネットに接続できるようになる
    - 利点：ISPから1つだけグローバルアドレスをもらえれば、家庭内のプライベートネットワークから何台でもアクセスが可能
    - 欠点：通信トラヒックが多くなるとルータの負荷が高くなりやすい



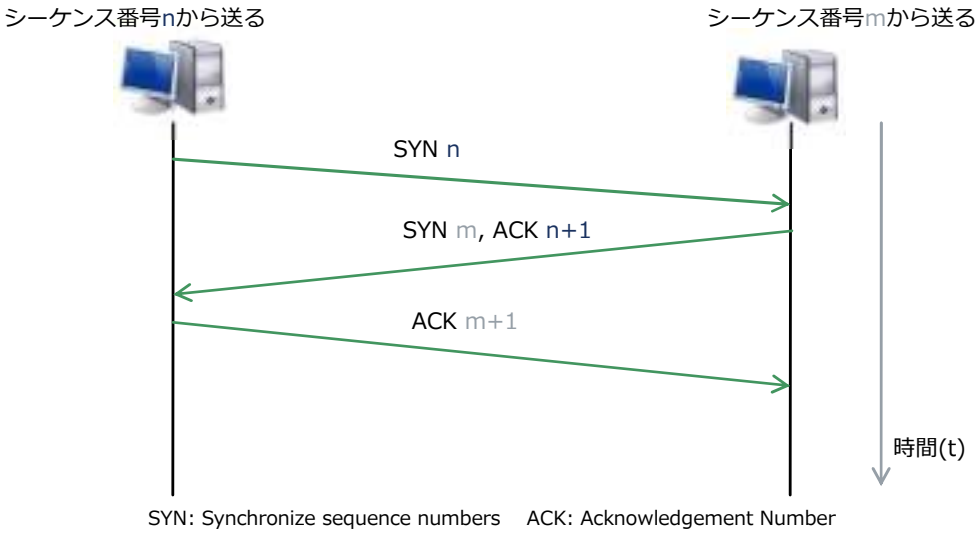
5. レイヤ4 トランスポート層：TCP、UDP、VPN

レイヤ４：トランスポート層

- それぞれのホスト上で動いているプロセス(アプリ)間の通信を担う
  - プロセスとはプログラム命令のこと
  - ホスト上では多くのプロセスが実行されている
- TCP(Transmission Control Protocol)
  - コネクション型(Connection-Oriented)
  - プロセス間でVirtual Circuit(Connection)：トンネリング
  - 多くのプログラムで使われているプロトコル
    - Webとかメールとか
- UDP(User Datagram Protocol)
  - コネクションレス型
  - Datagram
  - リアルタイムアプリケーションなど
    - 動画ストリーミングとか、テレビ電話とか

TCP：3WAY HANDSHAKE

- 通信開始時に手続きに従ってコネクションを確立する

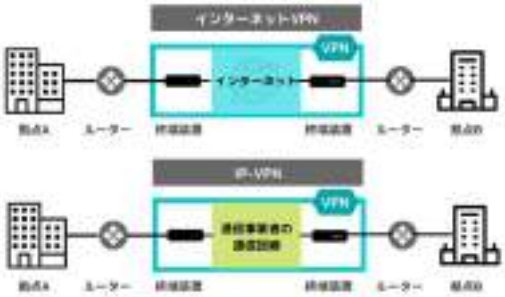


UDP

- TCPのように、信頼性、フロー制御、輻輳制御などの仕組みを持たない
  - 余分な処理をしないので簡単
- 何故UDPで良いの？
  - 応答確認がいらない、データ量が多い、かつリアルタイム性の高いアプリケーション
    - 音声、映像など次々に大量のパケットが送られてくる
    - 少々パケットがロストしても良く、とにかく処理が速い

トンネリング？

- 仮想のトンネル(Virtual Circuit)とは
  - 公園にある土管のこと覚えてますか
  - 土管＝VPN(Virtual Private Network)
    - 入り口に入れば一直線に出口までたどり着ける
    - 周りが堅牢なコンクリートなので安全、しかも中が見えない（カプセル化）
- VPNには色々なタイプが存在
  - インターネットVPN
    - 通常のインターネットを利用するので容易に構築可能、ベストエフォート
  - エントリーVPN
    - 通信事業者専用の閉域網に接続され、セキュリティがインターネットVPNより高い



Rworks社のHPより引用
https://www.rworks.jp/system/system-column/sys-entry/21285/

通信の中身を見てみよう

- Wireshark
  - Windows、Mac、Linuxで動作する無料ソフトウェア

参事官室0

スライド 33

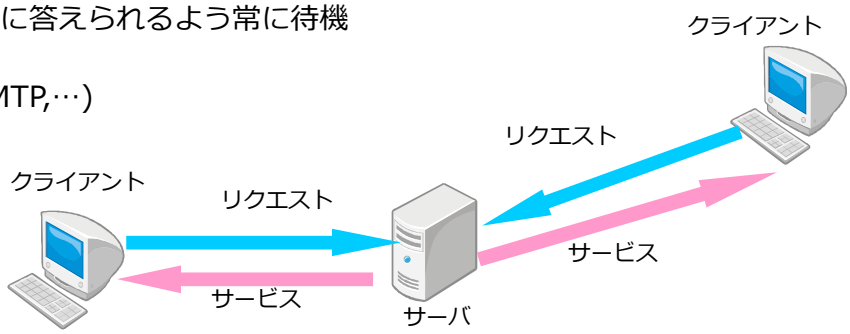
参事官室0　Wiresharkはあまり基礎的な内容ではないかとおもいますが、話しますか？
参事官室, 2024-11-20T01:31:53.837

美和0 0　基礎ではありませんが、システムセキュリティ管理者向けなので、知っていただきたいToolの1つとして紹介したいです。
和田 美恵, 2024-11-22T09:49:49.981

6. レイヤ7 アプリケーション層：C/S（クライアントサーバ）、HTTP

レイヤ7：アプリケーション層
C/S クライアントサーバモデル

- ほぼインターネットのサービス全てがC/Sモデルで動作
- サービスモデル
  - 提供者とサービスの受け手を定義
    - 提供者＝サーバ
    - 受け手＝クライアント
- サーバはクライアントからの要求に答えられるよう常に待機
  - Webサーバ(HTTP, HTTPS)
  - メールサーバ(POP, IMAP, SMTP,…)
  - etc….



DNS(DOMAIN NAME SYSTEM)

- インターネットではIPアドレスでホストを特定
  - グローバルIPアドレスは(基本的に)世界で唯一のアドレス
  - End-to-End通信を確保
  - IPアドレスのように人間にとって数字の羅列は覚えにくい
    - 単なる数字の羅列は覚えるのが大変

例

- 133.1.138.144 ←→www.osaka-u.ac.jp.
- 正引き
- 逆引き

IPアドレスと名前の対をどこかに記録しておいて、
必要に応じて取り出せばよい

ホスト名とドメイン名

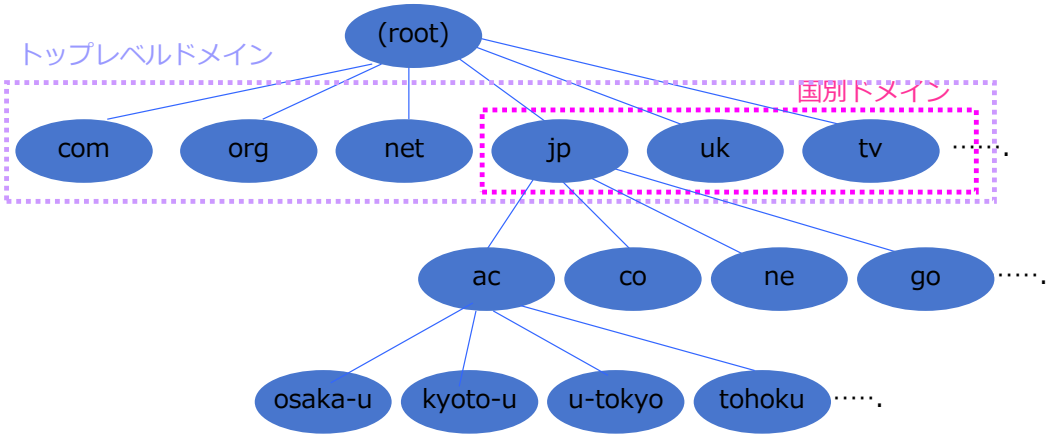
- IPアドレスと同じく、世界に1つのホストを示す
  - www.osaka-u.ac.jp
    - ホスト名
    - ドメイン名
  - 英語での住所表記と同じく、小区分→大区分
    - 例) 1st Ave., Between 42nd St. & 48th St., New York, NY 10017
  - ホスト名
    - 左の最初のピリオドまでの文字列で表す
  - ドメイン名
    - osaka-u.ac.jp
      - 第３レベルドメイン
      - 第２レベルドメイン
      - トップレベルドメイン

一番右がトップレベルドメイン、以下右から順に第○レベルドメインと呼ぶ

ドメイン名の階層構造

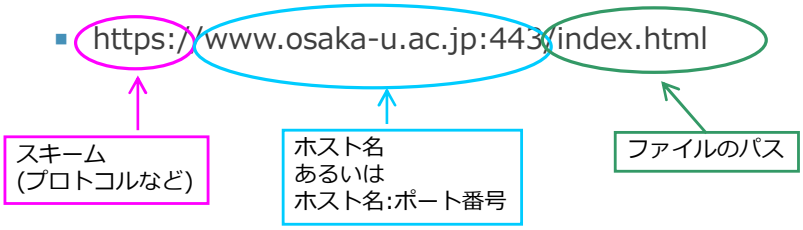
- 木構造(ツリー)と根(root)
- 例： **www.osaka-u.ac.jp.**

[.] というroot(根)が隠れている



HTTP(HYPERTEXT TRANSFER PROTOCOL)

- HTTP=WWWを実現するためのプロトコル
  - ハイパーテキスト(HTML, XML)を想定
    - テキストデータのみならず、音声や画像・音声等バイナリデータも含め様々なデータのやり取りが可能
  - トランスポート層(L4)プロトコルにはTCPを利用
- URL (Uniform Resource Locator)
  - インターネット上の資源の場所を示す
  - https://www.osaka-u.ac.jp:443/index.html



HTTPステータスコード

ステータスコード	意味	内容
200	OK	正常に処理された
301	Moved Permanently	指定のURLは恒久的に移動した
403	Forbidden	アクセスが禁止されている
404	Not Found	リソースが見つからない
500	Internal Server Error	サーバ内部でのエラー
503	Service Unavailable	サービスが一時的に利用できない

おわりに

セキュリティ対策の技術はシステム・セキュリティ管理者の専門外だからとベンダーに任せるのではなく、
ベンダーから状況を聞いて**自分で理解**できるだけで、
インシデント対応がよりスムーズに進めることができます

そして習うより、慣れろ！です

ありがとうございました。