パケット解析

2024/11/09

GDGoC 大阪大学

低レイヤー講演会 in Osaka

Tam

アンケート

唐突ですが、

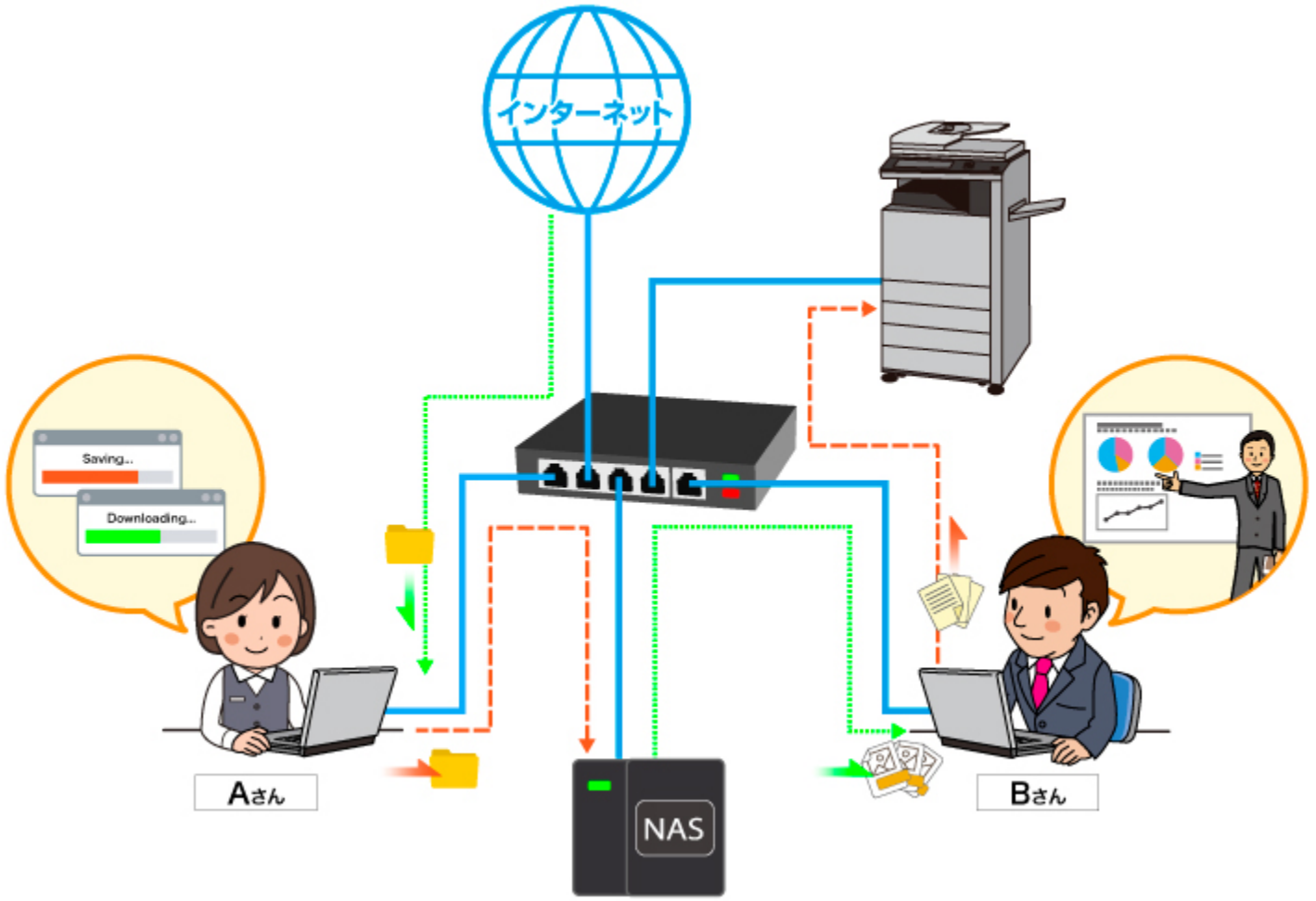
自分が使ってるネットのデータ、覗かれたら嫌ですか？

残酷な現実

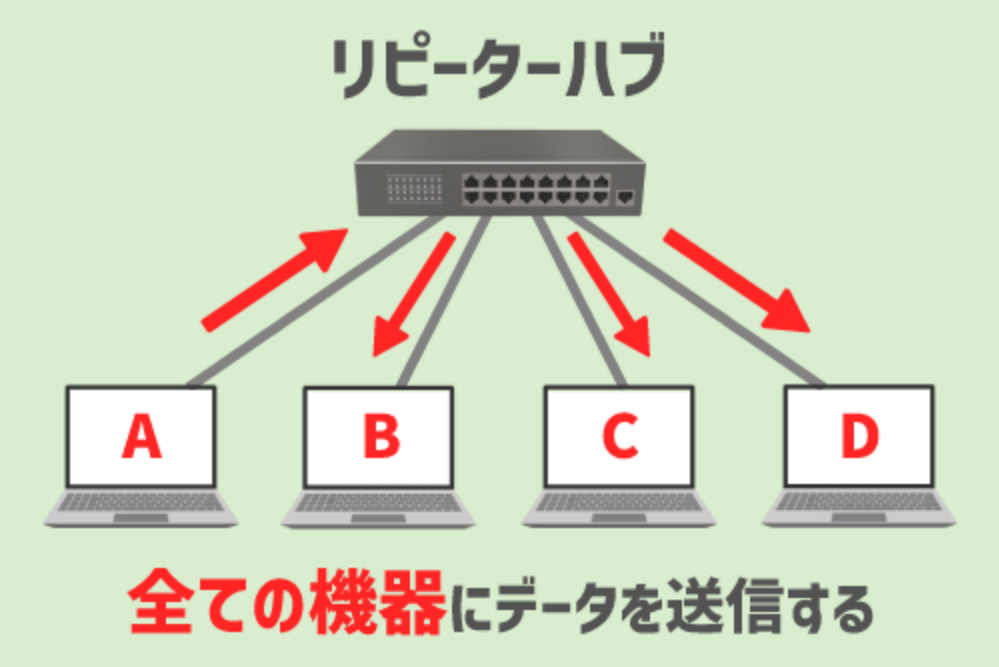
WiFi でも有線LAN でも、

データは見られています。

有線LAN の場合

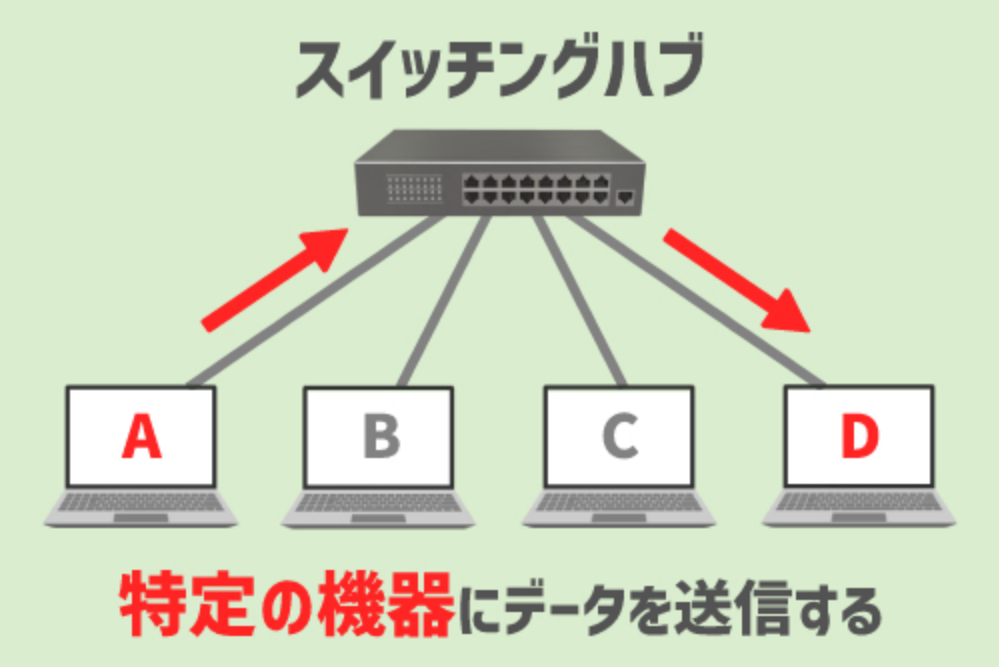


バカHUB



※ノジマ の HP より抜粋

スイッチングHUB



※ノジマ の HP より抜粋

無線LAN の場合

- 繋ぐためには SSID とパスワードが必要。
- パスワードが必要なんだから、他の人には見えないんじゃね？

⇨同じ WiFi を使ってる人は、全員データが見えます。
⇨スイッチングHUB みたいな構造も少ないので、余計簡単に見えます。

WireShark や TCPDump

- データを覗き見るための専用のソフトがあります。
- 違法性はありません！（よく誤解する人が居ます。）
- 固定電話の盗聴と言った概念ではありません。
- データは誰でも見れます。
- 逆に見られているという認識で使用する必要があります。

実演

- 見えちゃいけないデータが見えちゃうとマズイので、詳細はボカシます。
- 昨今の通信料は膨大なので、そのまま覗き見ると、データが大量にありすぎます。
- フィルタを掛けることにより、目的のデータのみに絞ることが出来ます。

潜水

- WireShark では「パケット」ごとにデータが出力されます。
- 「パケット」とは、 WiFi や有線LAN のデータ通信の最小単位です。

パケットの構造

- 有線LAN と無線LAN ではパケットの構造が若干違います。
- 有線LAN のパケットのほうが、入門としては都合がいいです。
- ここでは、会場の設備の都合で、 WiFi のパケット構造を見ていきます。

OSI参照モデル

※明確に層分けできない場合が結構あります。

モデルの上から下に向かって順番に見ていきます。

セッション層、プレゼンテーション層、アプリケーション層

HTTP や SMTP 、 DNS と言ったプロトコルが使われます。

トランスポート層

TCP, UDP, ICMP といったプロトコルが使われます。

TCP

ネットワーク層

IP 通信が行われます。

ここの定義により、グローバルな通信が行えるようになります。

物理層、データリンク層

各物理デバイス間の通信が行われます。

ここでは、主にローカルネットワーク内での通信しか行われません。

なんの役に立つの？

- 低レイヤー（機械）に近い方のコード
- OS やライブラリの用意されてない IoT 機器
- VPN などのプロトコル作成
  など。