

ARP偽装の恐怖！

～ ネットワークを学ぼう(1/3) ～
Ethernetを知る

2008/7/17 sasimi

今日のテーマ

- ARPの偽装というものがあることを知る
- ARPが何かちょっとだけ知る
- Ethernet(イーサネット)について学ぶ
 - 3つの特徴
 - スイッチとはなにか
- 「ちょっとだけ」ネットワークに興味を持つ

ARP偽装(ARP Spoofing)って？

ARPを書き換えて**デフォルトゲートウェイ**を偽る

知らない単語

- ARP ???
- デフォルトゲートウェイ？

次回に詳しく説明します

ARP偽装はなにが怖い？#1

WEBコンテンツを改ざんしたりできます

例えば

- openlab見たら怪しい海外のサイトに飛んだ
- openlab見たらアンチウィルスの警告が出た

ということが起こりうる、これは怖いです

ARP偽装はなにが怖い？#2

- WEBサーバ上のファイルは問題ない(正常)
- でも、ブラウザでアクセスすると変

つまり、WEBサーバはなににも悪くない

→WEBサーバのファイルチェックだけではダメ

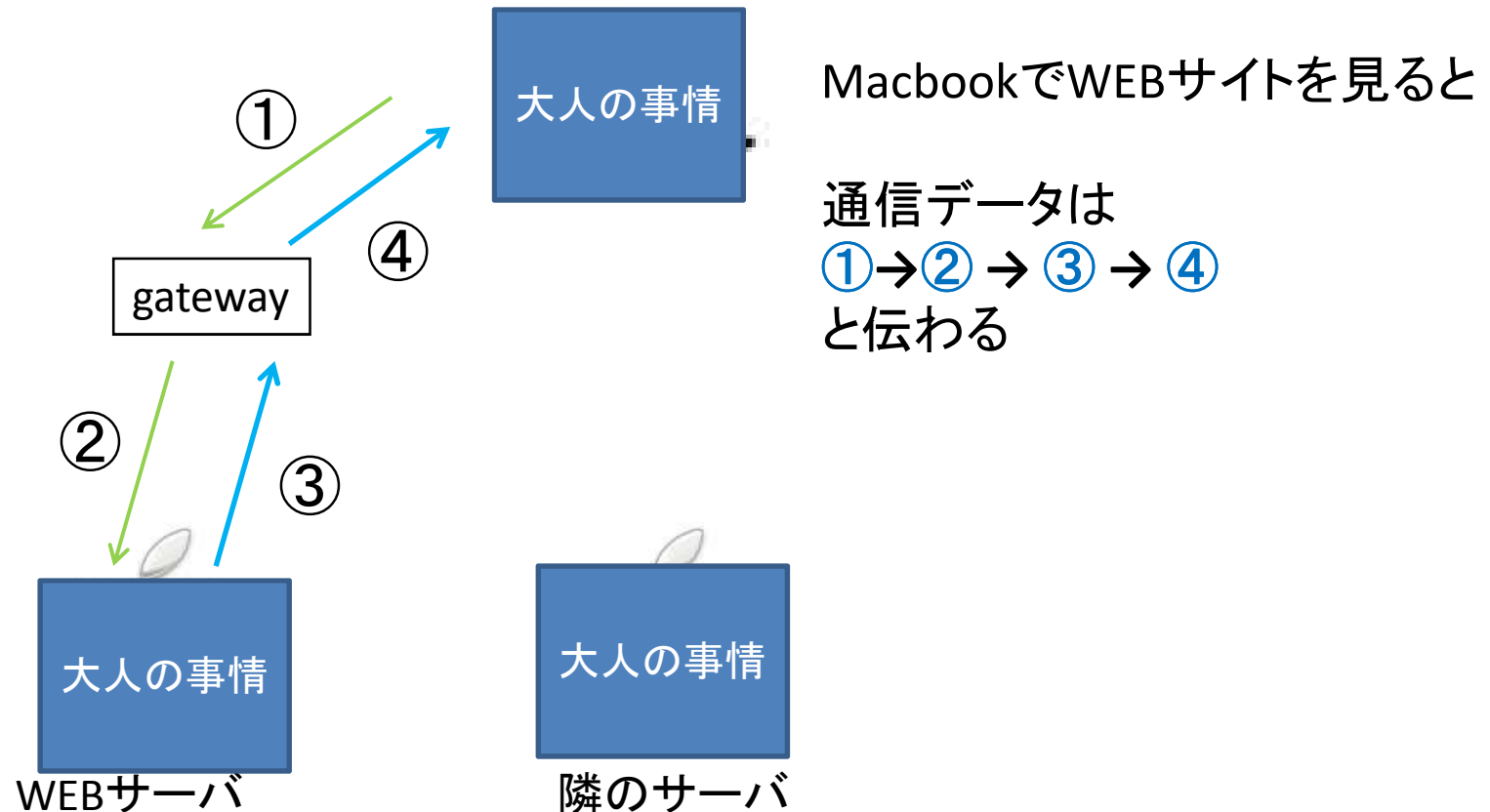
→Tripwire オワタ！？ \ (^o^) /

注： Tripwireはファイルの改ざんなどを監視するツール

では、ARP偽装の概要を紹介します

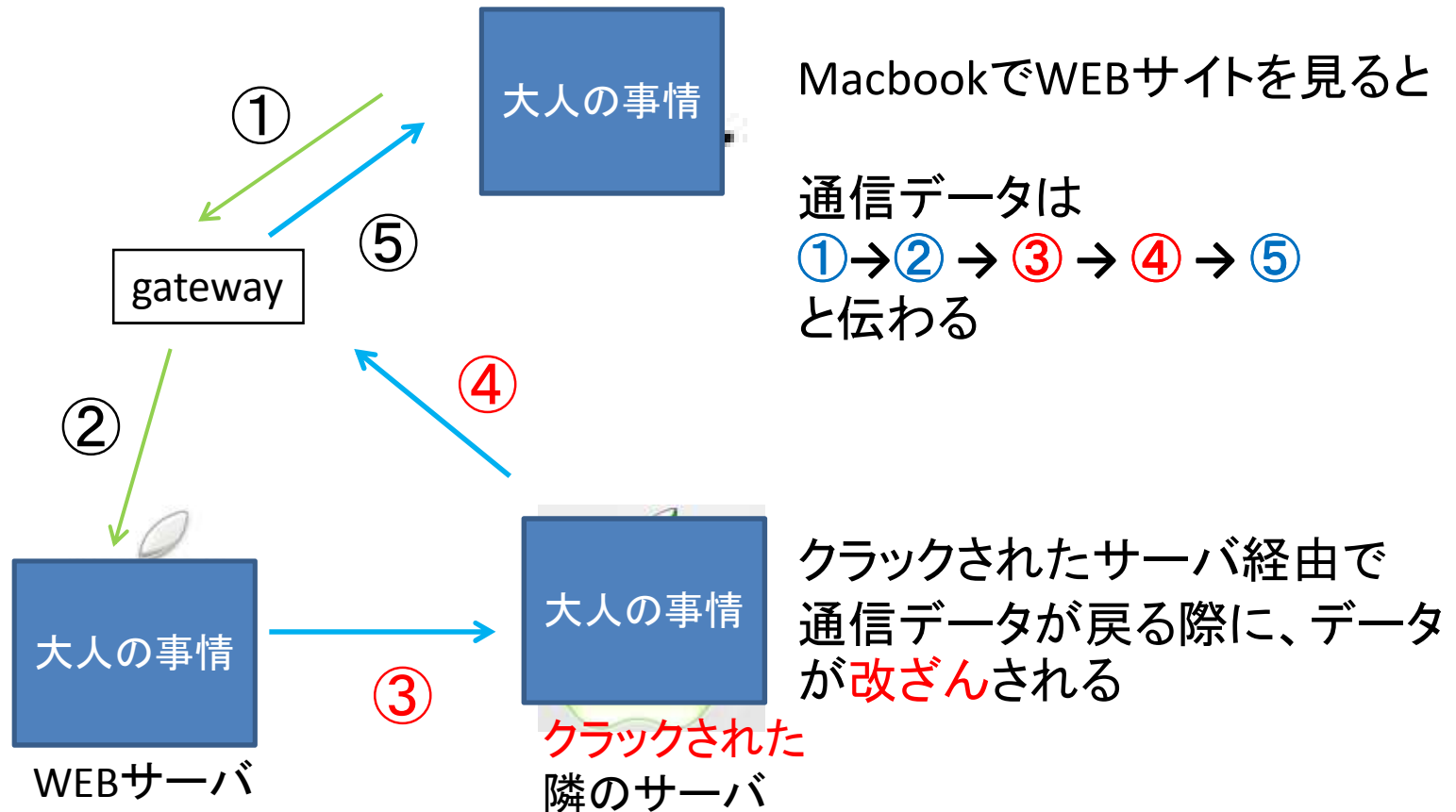
ARP偽装の概要#2

正常な状態



ARP偽装の概要#2

ARPが偽装された状態



ちょっとした疑問(1)

- なんでこんなことが起こるの？
- 対策ってあるの？
- そもそもARPってなに？
- ゲートウェイってなに？

3回の講義でこれら全てを説明していきます

ARP (Address Resolution Protocol) とは

IPアドレスからMACアドレスを解決する仕組み

また知らない単語が...

- IPアドレスって??
- MACアドレスって??

さて

- 残念ながらARPの詳細は次回
- IPアドレスやゲートウェイも次回
- MACアドレスはこれから話します

では本題

- ネットワークを理解すればARP偽装のキャラクリがわかります
- 今日はEthernetを学びます

Ethernet(イーサネット)とは

- 1973年誕生、1983年にIEEE 802.3として標準化
- 社内ネットワーク(LAN)でも使っています
- TCP/IPのリンク層に該当する実装の1つ

TCP/IPの階層

各層の実装例

TCP/IPの階層	各層の実装例
アプリケーション層	http, smtp
トランスポート層	tcp, udp
インターネット層 (IP Layer)	IP
リンク層 (Link Layer)	Ethernet, ISDN, ppp

Ethernetの3つの特徴

- 通信機器は**MACアドレス**で識別
- ネットワークの形態は**バス型**
- 通信の制御は**コリジョン**(衝突)検出で行う

では、それぞれを説明していきます

Ethernetの特徴 1 / 3

MACアドレス (Media Access Control Address)

- Ethernet機器それぞれ固有の物理アドレス
- Ethernetでは48ビットの値

MACアドレスの例:

00-1C-C4-36-E6-9C

上位24ビット:

メーカー固有の値

下位24ビット:

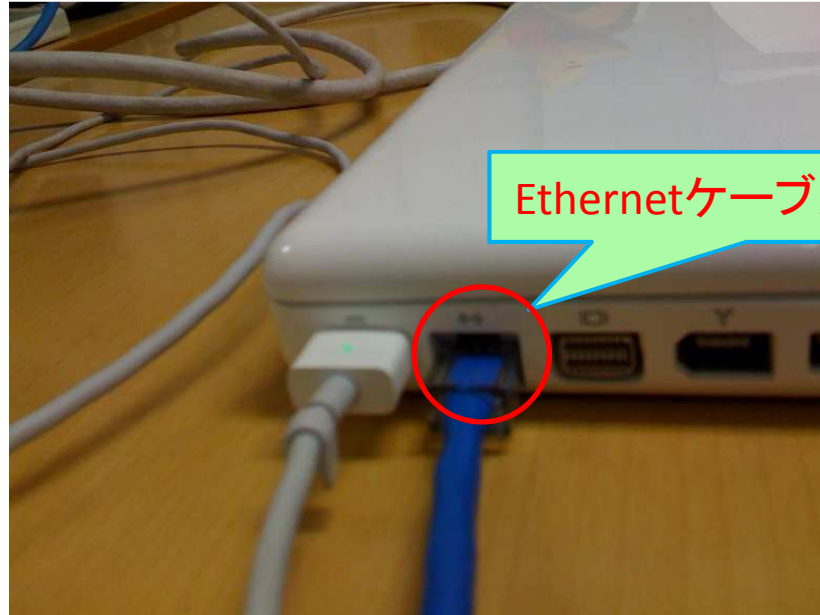
メーカーの機器内で重ならない値

つまり、同じMACアドレスは世界に存在しない

MACアドレス-補足#1

PCについでるEthernet機器ってどんなの？

MacBookでの例：



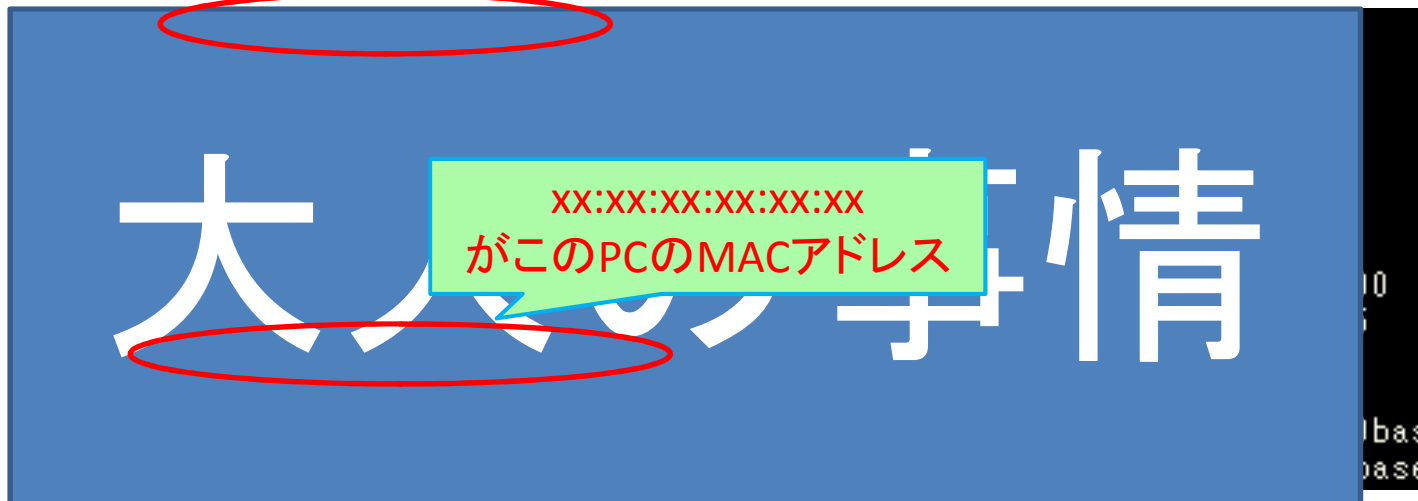
Ethernetケーブルを挿すコレ

MACアドレス-補足#2

ではそのMACアドレスは見られるの？

MacOSでの例

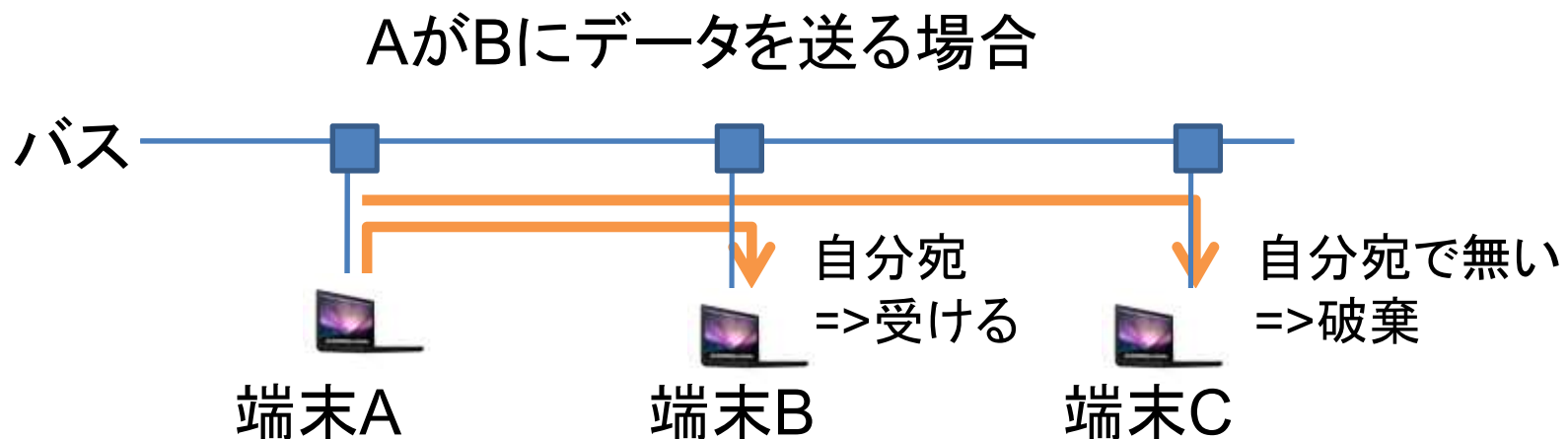
ifconfigコマンドを実行



Ethernetの特徴2/3

バス型 (bus topology)とは

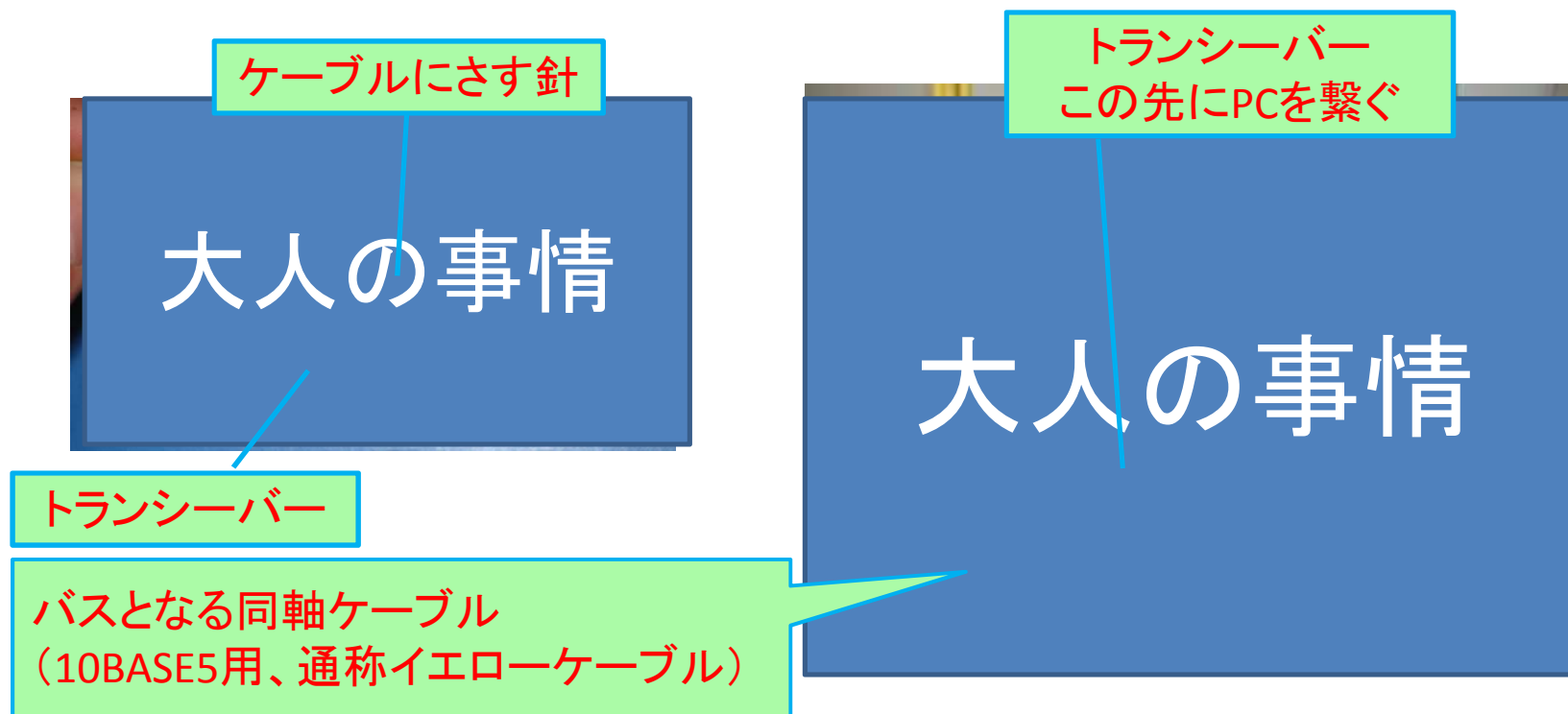
- 一本のケーブル(バス)に端末がつながる
- 通信データはつながる端末全てに届く
- 自分が送信先となっているデータだけ受ける



バス型-補足#1

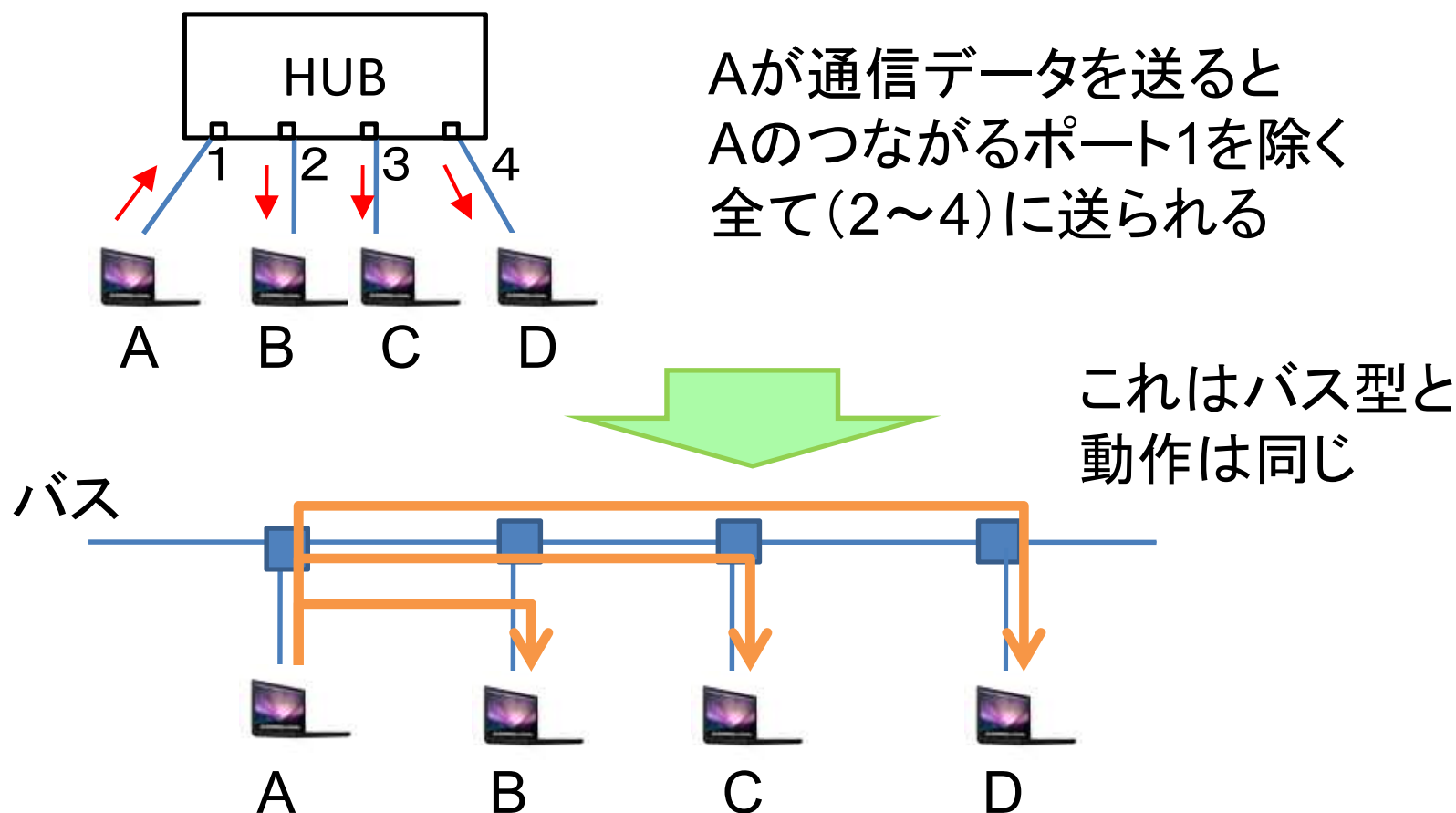
バス型って社内では見かけないですが？

そうですね、でも昔(1990年代前半)はこれが普通でした



バス型-補足#2

ハブ(リピーターHUB)でつないでもバス型



Ethernetの特徴3/3

コリジョン (collision) とは

- 同時に2台以上の端末がデータ送信して衝突すること

線路の両側から電車がきたら衝突するよね

コリジョン-補足#1

コリジョンが発生したら？

- 送った通信データが壊れるため、しばらく待って端末は再度データを送る

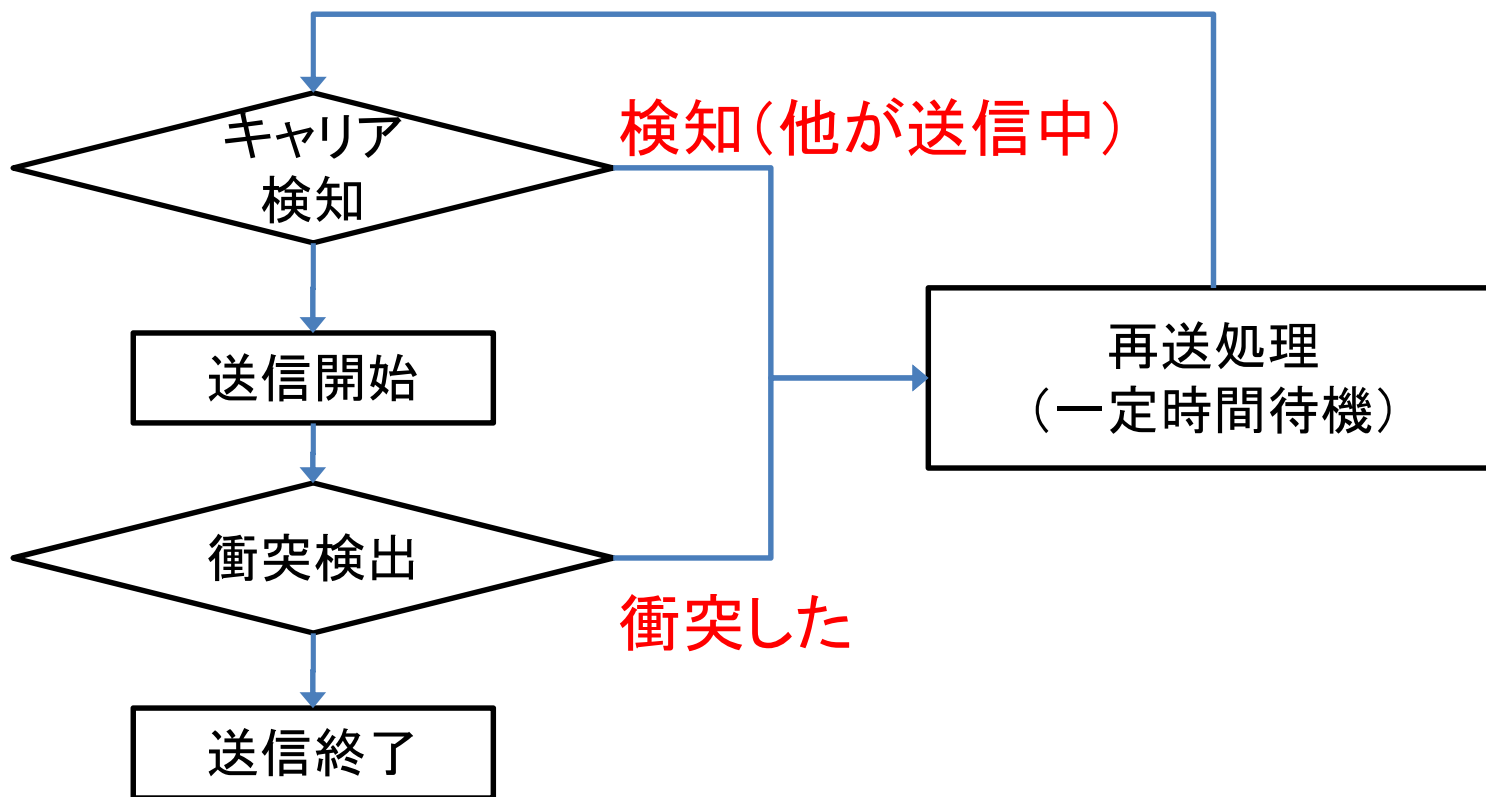
その仕組みをCSMA/CD

(Carrier Sense Multiple Access/Collision Detection)

と呼ぶ

コリジョン-補足#2

CSMA/CDの仕組み



ちょっとした疑問(2)

これって

- コリジョンがコリジョンを呼ぶ??
- 他人宛の通信データも見られるんじゃない?
(盗聴できる??)

その通りです

バス型はだめ？

なんかバス型って無駄が多くない？

確かに～

大人の事情

バス型の良いところ

でもバス型にも良いところはあるよ

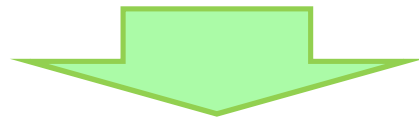
- 構造が簡単 ⇒ 機器が安い

それと

同軸ケーブルはノイズに強く、ケーブルを
長距離引ける(工場とかにもいいよ)

スイッチの誕生

でも、バス型はやっぱり不便

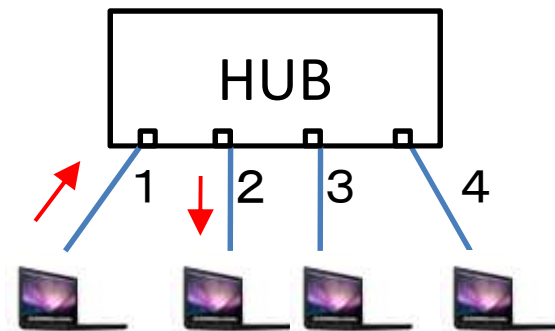


スイッチ(ブリッジ)の誕生

スイッチとは

スイッチ(ブリッジ)とは

- 送信先MACアドレスを解釈しその端末が繋がるポートだけにデータを送る機能を持つ



スイッチ機能付きのHUBでは

AがB宛に通信データを送ると
Bのつながるポート2だけに送る

スイッチ-補足#1

スイッチの利点

- 通信したい端末だけにデータを流すので無駄がない
 - ⇒ コリジョンが防げる
- 他の端末の通信が終わるまで待たなくてよい
 - ⇒ ネットワークを有効に使える

スイッチ-補足#2

大人の事情

スイッチの場合には

- (1) AからD宛
- (2) BからG宛
- (3) CからF宛
- (4) EからH宛

を同時に送信が可能

スイッチ-補足#3

コリジョンが起きないなら全てスイッチへ置き換えればよいのでは？

- でもスイッチは構造が複雑 ⇒ 高い

というのは昔の話

今はスイッチが安価で買えるため

HUB＝スイッチ機能付き(スイッチングHUB)

では、まとめておきます

まとめ

- ARP偽装の概要を知りました
- Ethernetについて以下を学びました
 - Ethernetの3つの特徴
 - MACアドレスで機器を区別
 - 全端末が1本につながるバス型の接続
 - コリジョンを検出して通信を制御
 - バス型の欠点と利点
 - 通信の無駄が多い、が仕組みが簡単で安い
 - スイッチとは
 - 通信の無駄がない、装置も今は安くなった

おわり

以上です

ご清聴ありがとうございました