ウイルスバスターfor Home Networkの調査研究

明治大学　総合数理学部
先端メディアサイエンス学科
菊池研究室 4年 平山夏輝

研究背景

ネットワーク利用者の多様化

- 子供から年配まで

ホームネットワークにおいてアクセス管理の問題あり

- 東芝やNECなどの企業はイントラネットの外にFWを導入すればよいが,
  個人の家庭ではブロードバンドルータの関係で困難

- 小さいお子様の無自覚な不正サイトの利用による
  料金請求などネットワーク利用の懸念

ウイルスバスターHome Security(VBHS)

トレンドマイクロ社は家庭ネットワーク向け管理機器を開発

- 家庭のネットワークを脅威から守るために開発
  1. 不審な機器の接続を遮断
  2. フィルタリング機能

どのような仕組みで家庭内ネットワークのパケットを検査しているのか仕組みを解析し, 課題を検討

VBHSの機能

1. URLフィルタリング
   - 特定のURLのネットワークブラウザへの通信を拒否する機能

2. カテゴリフィルタリング
   - ある特定のカテゴリに属するwebサイトの表示を拒否することが可能

VBHSはどのようにしてデバイスの遮断を行っているのか?

ARP(Address Resolution Protocol)

ARPリクエストとARPリプライというパケットからなり, 宛先IPアドレスを持つノードのMACアドレスを得る.

これらのやりとりをARPキャッシュとして一定時間保存しているものを「ARPテーブル」という

ARPSpoofing

ARPスプーフィングは、正規のクライアントからのARPリクエストに対して、別のクライアントが「不正なARPリプライ」をブロードキャストする

多量なARPパケットの送受信やARPテーブルの変化がみられる

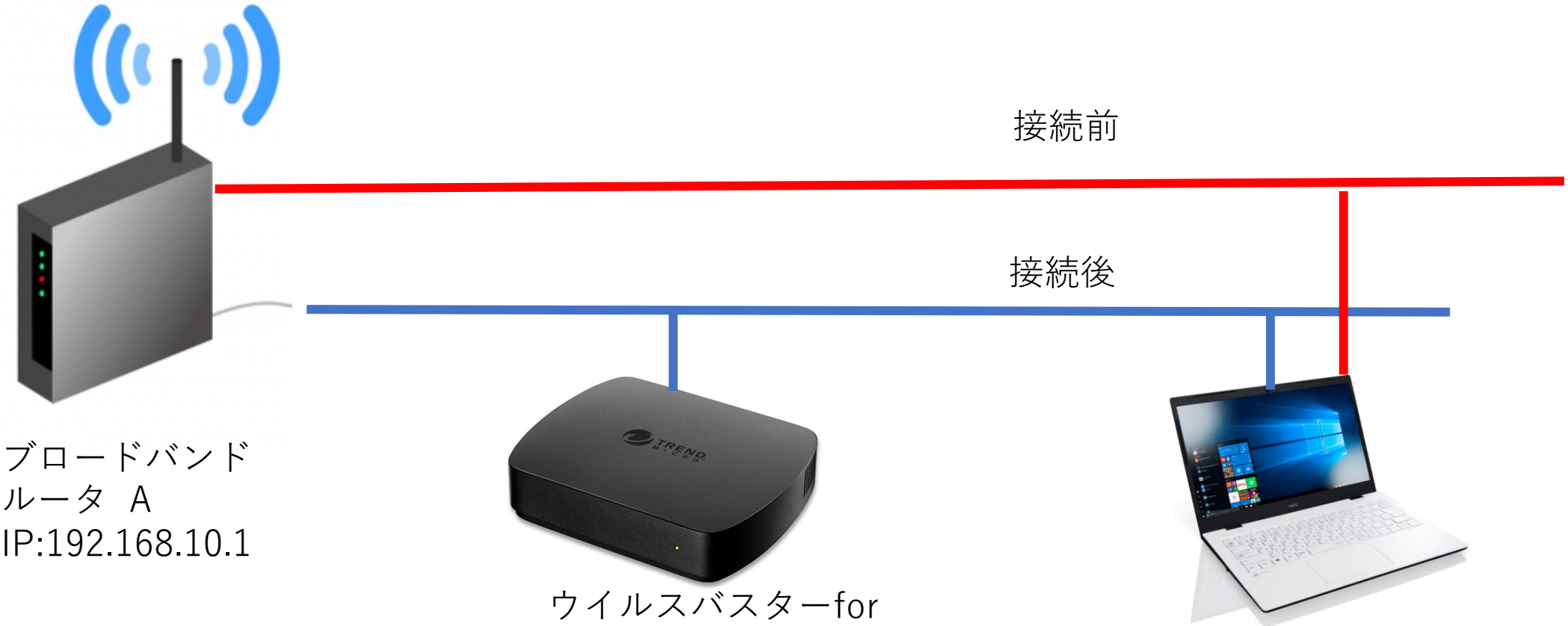
調査目的と方法

目的：VBHSがARPSpoofingを用いてデバイスの遮断を行っているのかを調べる

方法：遮断対象であるPC CにてARPパケットをWiresharkを用いて観測し, ARPテーブルの変化をVBHSの接続前後で調べる

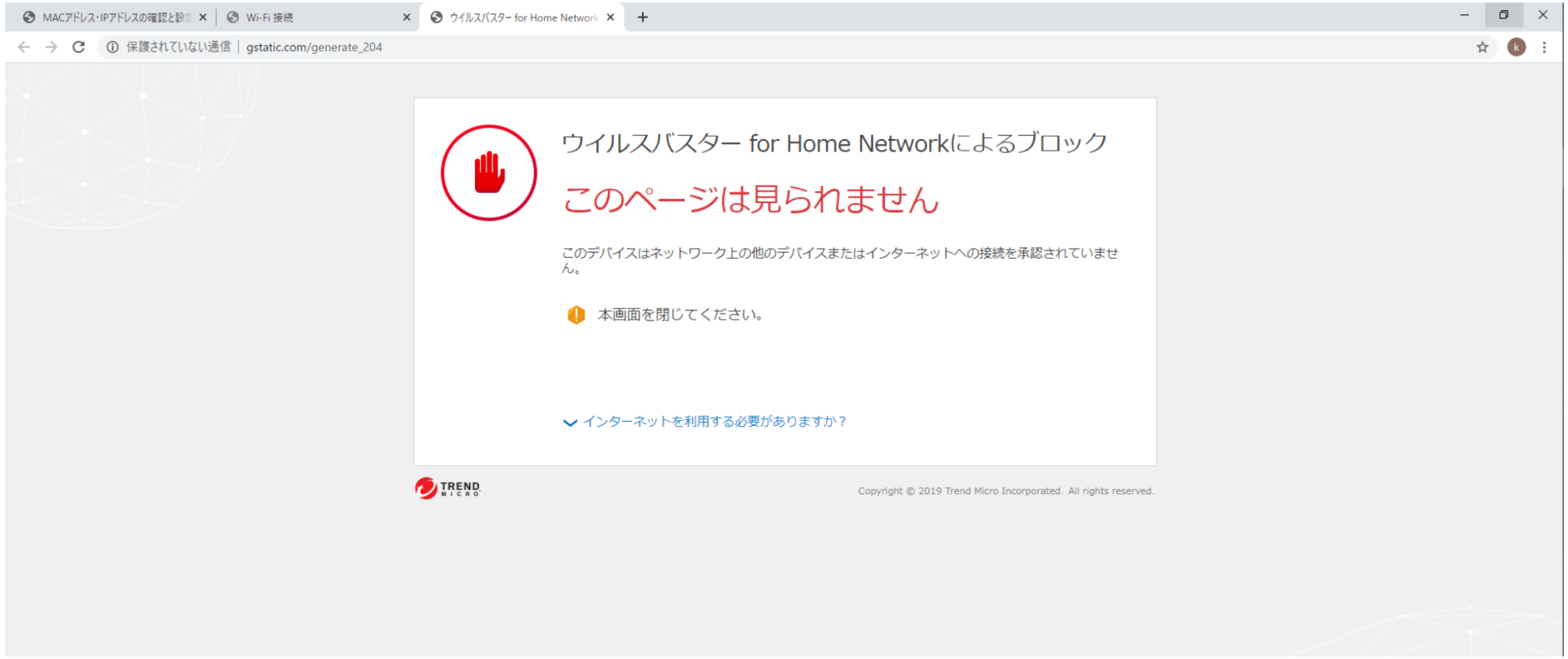
→ARPSpoofingを用いているなら多量なARPパケットの送受信やARPテーブルに変化がある

調査環境


接続前
接続後
ブロードバンド
ルータ　A
IP:192.168.10.1
ウイルスバスターfor
Home Network　B
IP:192.168.10.3
Windows10PC　C
IP:192.168.10.2

調査結果

PC Cをネットワーク内から遮断

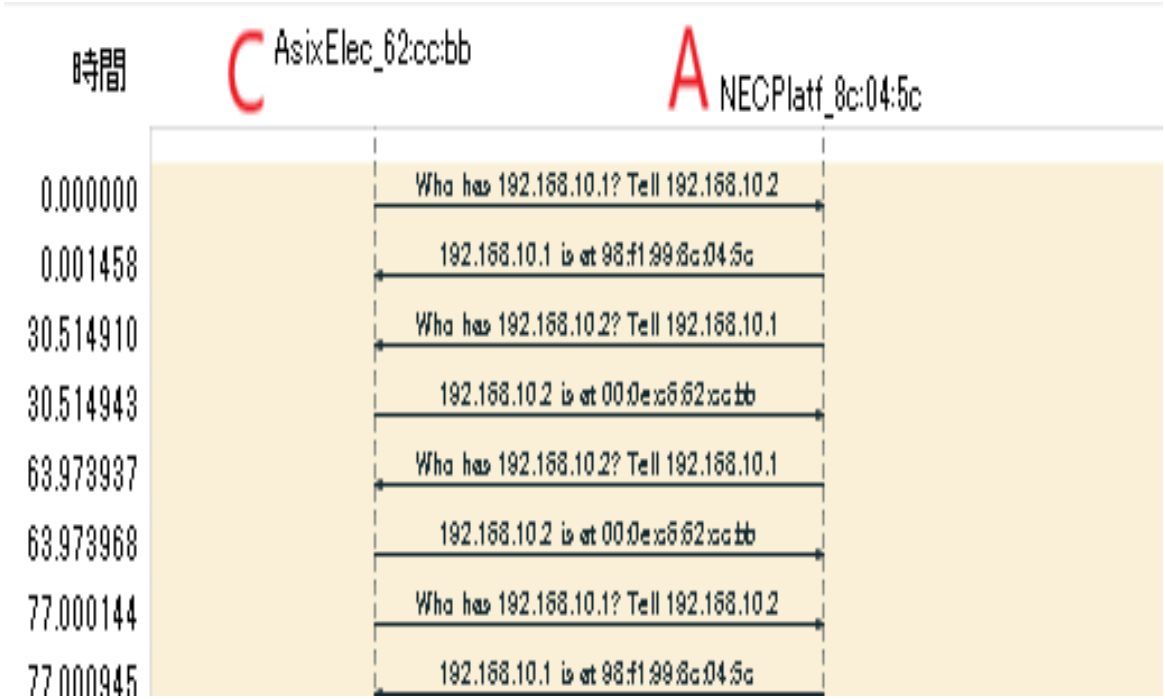


調査結果

B　　C　　A

ARPパケットの観測

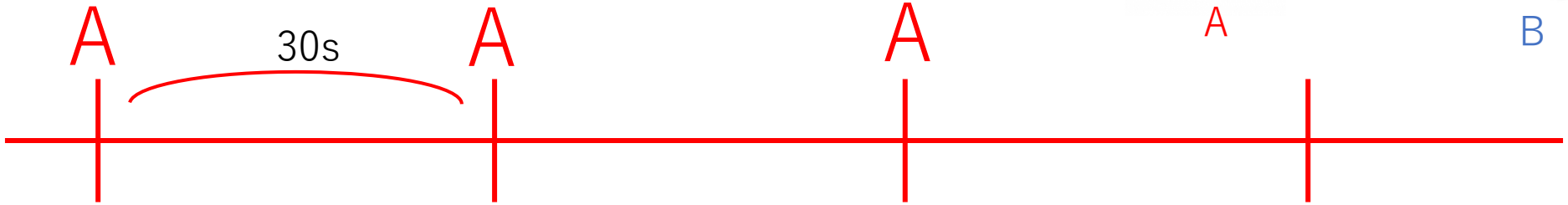
接続前



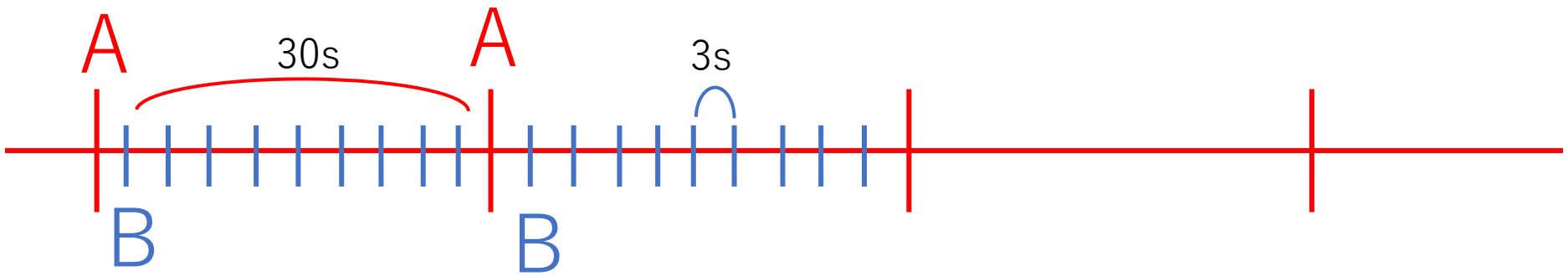
接続後

ARPの間隔

接続前



接続後



ARPテーブルの変化

	接続前			接続後		
ホスト	IPアドレス	MACアドレス	種類	IPアドレス	MACアドレス	種類
ルータ A	192.168.10.1	98-f1-99-8c-04-5c	動的	192.168.10.1	88-6a-e3-5a-81-ee	動的
PC C	192.168.10.2	00-0e-c6-62-cc-bb	動的	192.168.10.2	00-0e-c6-62-cc-bb	動的
VBHS B				192.168.10.3	88-6a-e3-5a-81-ee	動的
ブロードキャスト	192.168.10.255	ff-ff-ff-ff-ff-ff	静的	192.168.10.255	ff-ff-ff-ff-ff-ff	静的

まとめ

VBHSは遮断対象PCに3sおきにARPリプライを送ることにより，
ARPSpoofingを用いてネットワークデバイスの制御を行っている