ウイルスバスター for Home Network に関する調査研究

平山 夏輝 †

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 †

1　はじめに

近年のネットワークの普及に伴い利用者の多様化がすすみ, 小さい子供から年配の方まで, 誰でも簡単にネットワークを活用できるようになっている.

しかしながら, 誰でも簡単にネットワークを活用できるようになっている反面, 子供のアクセス管理や, 危険なサイトへのアクセスなどのセキュリティ面での問題がある. 企業のネットワークであれば専用のファイアウォール (FW) を導入して, すべてのパケットを検査すればよいが, 商用のプロバイダから借りているルータを用いて接続している家庭内ネットワークで, それを FW に置き換えて自分で管理することは技術的に困難である.

そこで, トレンドマイクロ社は, 家庭内ネットワークの単一のノードとして接続するだけで, 全ネットワークのノード管理を実現する製品であるウイルスバスター home Security[1] (以下, VBHS とする) を開発している.

本稿では, VBHS がどの様な仕組みで専用の FW なしで家庭内ネットワークのパケットを中断検査しているのか, いくつかの実験を行い, その仕組みを解析し, その課題を検討する.

2　ウイルスバスター for Home Network

2.1　概要

VBHS は, トレンドマイクロ株式会社が販売している家庭内ネットワーク保護用デバイスである. 保護対象となるネットワーク端末に VBHS の 1 台を接続し, 所有しているスマートフォンに管理アプリをインストールするだけでそのネットワーク端末につながっている全ての端末を管理する. 次の様な様々な機能を有しており, 家庭毎にカスタマイズすることができる.

1. 家庭内ネットワークに新しく参入してきたデバイスに対して, ネットワークに接続させるか否かを確認する機能 ［アクセス管理機能］
2. 家庭内ネットワークの中にある不審なデバイスをネットワークから遮断する機能 ［デバイス遮断機能］
3. ネットワークブラウザのフィルタリング機能 ［ペアレンタルコントロール］

2.2　ARP Spoofing

VBHS の原理は ARP Spoofing[2] により実現されていると考えられる. 全ての IP アドレスはデータリンク層で ARP(Address Resolution Protocol) によって動的に構成される ARP テーブルに従って MAC アドレスに変換される. VBHS は, これを利用して各種フィルタリング機能を実現していると考えられる.

2.3　機能の動作確認

本稿では, VBHS のフィルタリング機能について動作を確認する.

2.3.1　URL フィルタリング

ネットワークブラウザを閲覧している時の機能として特定のサイトへの通信を拒否する URL フィルタリングがある.

管理アプリに接続を拒否したいサイトの URL を入力すると, そのサイトへの通信が遮断される. URL の入力には, 文字, 数字および －(ハイフン) なので, https 通信はフィルタリングできない欠点がある.

実際にフィルタリングを指定して, http://windy.mind.meiji.ac.jp/ をブロックした結果を図 1 に示す.

図 1　URL フィルタリングの適用結果

フィルタリングを行った web サイトの画面が「この

†Department of Frontier Media Science, School of Interdisciplinary Mathematical Science, Meiji University, Kikuchi Laboratory.

ページは見られません」という特定の記述に変わっている. この機能は, 後述するカテゴリフィルタリングのようにカテゴリ毎ではなく, 任意の URL を自由に指定できるという点で自由度は高い.

2.3.2 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 サイトの表示をなくす機能にカテゴリフィルタリングがある. 「アダルト」, 「薬物」, 「不適切な広告」などのカテゴリが用意されており, フィルタリングしたいカテゴリを選択するとそのカテゴリに属する web サイトがブロックされる. 実際に「お酒」というカテゴリを選択し, 朝日ビールのサイトである https://www.asahibeer.co.jp/ へアクセスした結果を図 2 に示す.

図 2 カテゴリフィルタリング「お酒」の適用結果

3 調査

3.1 実験環境

本研究には Windows10 が搭載された PC *C* を有線ネットワーク内に設置し, VBHS *B* を接続した.

実験環境図を図 3 に示す.

3.2 実験目的と方法

VBHS *B* がいかにしてデバイスの遮断を行っているのかを調べるために, フィルタリングされる対象である PC *C* が属するサブネットにおける ARP パケットを Wireshark を用いて観測し, VBHS *B* の接続前後の ARP テーブルの変化を調べる. もしも, VBHS *B* がルータ *A* への MAC アドレスをスプーフィングする ARP を送信していれば, ARP Spoofing を用いている証拠である.

3.3 実験結果

VBHS *B* にて PC *C* を遮断対象に指定したところ, 任意に開いたウェブサイトである https://www.google.com/

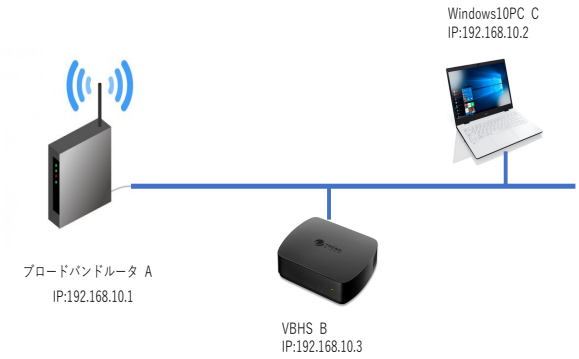

図 3 実験環境図

が図 4 のような表示になり, 対象 PC *C* はウェブのフィルタリング接続フィルタリングが行われている挙動を見せた.

図 4 遮断対象 PC *C* のウェブ画面

まず, ネットワーク内に VBHS *B* が接続されていない通常時の PC *C* から観測した ARP パケットを図 5 に示す.

図 5 の時間の単位は秒であり, 初めのパケットが観測されてからの相対時間を表している. ホスト名である AsixElec は PC *C* を, NECPlaff はルータ *A* を示している. 図 5 から, 約 30 秒毎にルータ *A* から PC *C* に ARP パケットが送信されていることがわかる.

次に, VBHS を接続した時の ARP パケットの観測結果を図 6 に, ARP テーブルの変化を表 1 に示す.

ARP Spoofing が攻撃対象に行われると, 不正な ARP パケットがブロードキャストされ, その対象の ARP テーブルが書き換えられる [3].

表 1 から, PC *C* の ARP テーブルのルータ *A* の IP アド

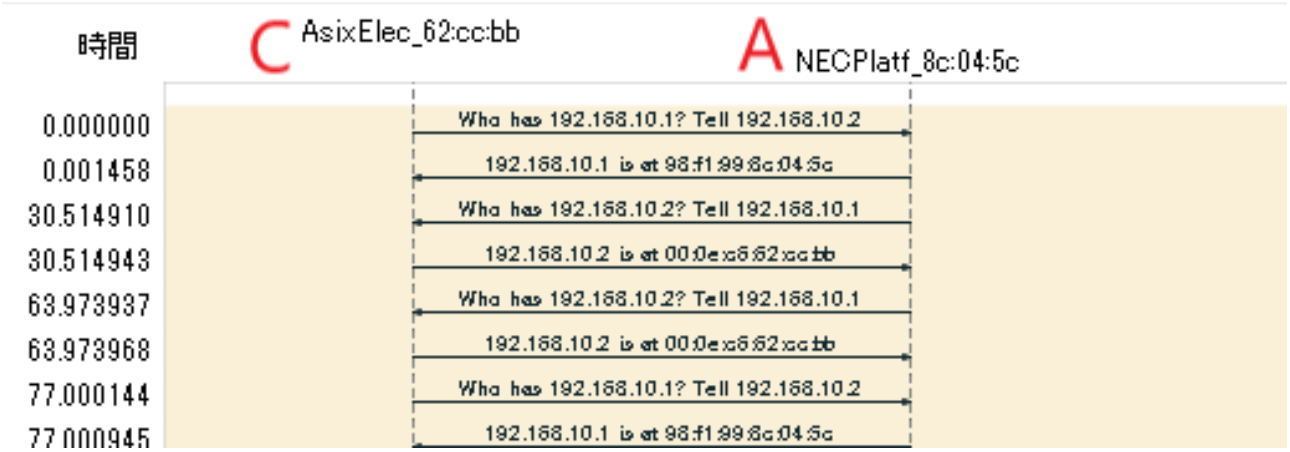

図 5　VBHS *B* 接続前の PC *C* から観測した ARP パケット (通常時)

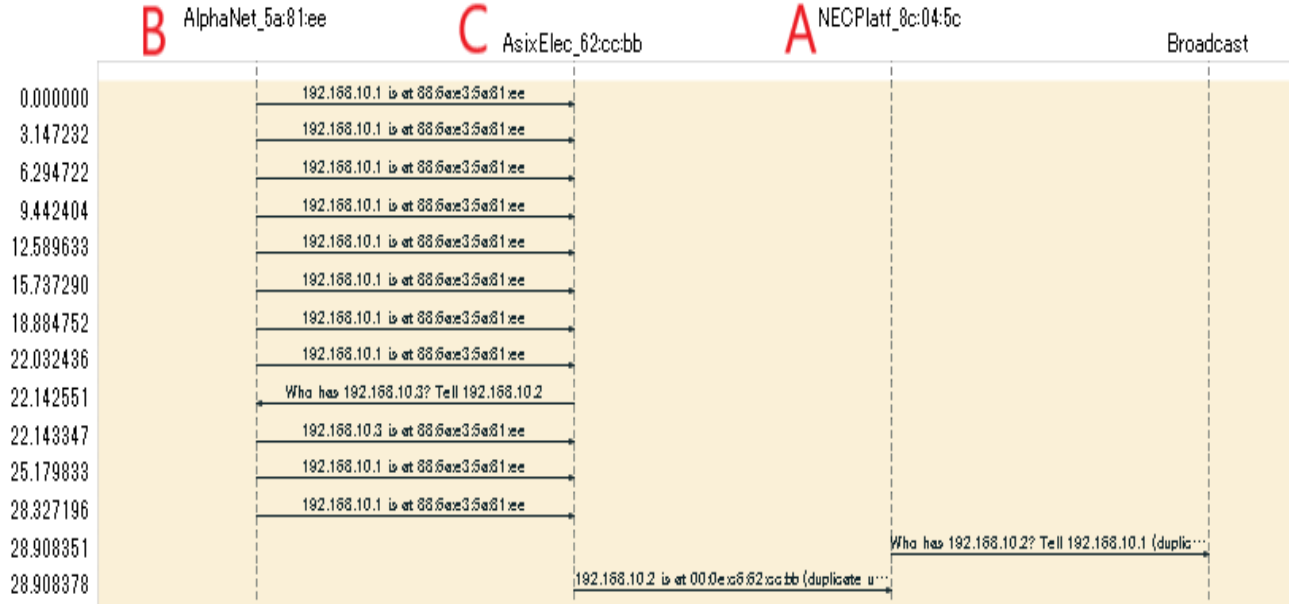

図 6　VBHS フィルタリングの時に遮断対象 PC *C* から観測した ARP パケット

表 1　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

レス 192.168.10.1 の MAC アドレスが VBHS *B* の MAC アドレスである 88-6a-e3-5a-81-ee に変化していることがわかる. VBHS *B* の IP アドレスである 192.168.10.3 が追加されており, ARP テーブルが書き換えられている.

図 6 の AlphaNet は VBHS *B* を示している. 図 6 で遮断対象である PC *C* に 10 個以上もの ARP パケットが約 3 秒毎に送信されている. このパケットの送信元は VBHS *B* であり, ルータ *A* の IP アドレスであった 192.168.10.1 の MAC アドレスは VBHS *B* の MAC アドレスである, という ARP パケットを PC *C* に送り続けている. 28.908 秒後にルータ A から正しい ARP パケットが送信されている. しかし, 正規は約 30 秒おきなのに対して, VBHS は 3 秒おきであり, ほとんどの場合 *B* のアドレスに書き換えられてしまう.

以上の結果から VBHS は ARP Spoofing を用いてデバイスの管理を行っていることがわかった.

4 おわりに

本研究では VBHS を使用し, その機能を調査し, その原理を明らかにした. 本研究では, VBHS の機能である URL フィルタリング機能において, https 通信を遮断できなかったので, その通信の解析を今後の課題とする.

参考文献

[1] Trendmicro, (https://www.trendmicro.com/ja_jp/forHome/products/vbhn.html , 2020 年 12 月参照).

[2] 松藤央, 落合秀也, 江崎浩, “無線端末による ARP を用いたセグメント内の通信妨害攻撃とその対策”, マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO), pp.210-213, 2018.

[3] Mahendra Data “The Defense Against ARP Spoofing Attack Using Semi-Static ARP Cache Table”, Sustainable Information Engineering and Technology(SIET), pp.206-210 , 2018.