ホームネットワークにおける全ホストを管理する Simple Home Security の開発

井窪 竜矢 †
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

2020 年以降流行している COVID-19 により，オンライン学習や在宅勤務の利用が増えた．今後もオンラインを用いる作業への需要は残ると考えられる．

しかしながら，専門知識を持つ管理者がいないホームネットワークにおいては気づかないうちに個人情報を盗まれたり，自身の所有する機器が乗っ取られることもある．特に，専用のファイアウォールがないため，知識のない家族が勝手に導入したスマートフォンのアクセス制限ができない．

そこで，本研究は，ホームネットワークにおいて家族が危険なサイトにアクセスしないように，Wi-Fi に接続している全ての機器を自動検出し，特定サイトへのアクセス制御を施すことを目的とする．しかし，ホームネットワークには通常専用のファイアウォールがなく，危険なサイトへのアクセスを遮断するのが困難である．そこで，本研究では，IP アドレスと mac アドレスを対応付ける ARP（Address Resolution Protocol）[3] に注目する．ARP を代理で送信する良性の ARP スプーフィングを応用することで，ファイアウォールを代用することを提案する．本稿では，システム開発と各家庭で行った実証実験の結果を報告する．

2　提案システム構成

2.1　ホームネットワークの危険性

家庭内で運用するネットワークにおいて注意すべき事項について３つ挙げる．

１つは専用ファイアウォールの有無だ．ファイアウォールはインターネットを通してローカルネットワークに侵入する不正なアクセスを防止するためのセキュリティシステムである．企業ではセキュリティ対策として専用のファイアウォールを設けているが，ホームネットワークにおいては高度なセキュリティ対策はなされていない．

次に，利用する人の知識不足が挙げられる．セキュリティやネットワークに対し，知識や関心が無い場合，不正なアクセスに気づかない場合も多い．

最後は，家族がアプリを勝手にアプリをインストールできることだ．ホームネットワーク内において，接続端末が不用意にインストールし，ウイルスに感染した場合，ホームネットワーク全体が危機に晒られる．

これらの問題を解消するため，ローカルネットワーク内のアクセスを制御するシステムを提案する．

2.2　ローカルネットワーク内のアクセス制御

図 1 に，ローカルネットワーク内で行われている通信と，本研究で実現するアクセス制御を示す．通常，家庭内にある各機器 A，B，C はルータ R を通し外部と通信するのに対し，Simple Home Security（SHS）設置では，A，B，C から R への通信を全て獲得し，SHS 経由で中継する．これを設置し，SHS の内部で各ホストからの特定のサイトへの通信を遮断することができる．

2.3　目標とするセキュリティ対策

以下のセキュリティ対策を目的とする．

- Wi-Fi に接続している全ての機器の自動検出
- 各機器が所有する以下の情報の自動検出
  - IP アドレス
  - mac アドレス
  - ベンダー情報
- サイトのアクセス制限

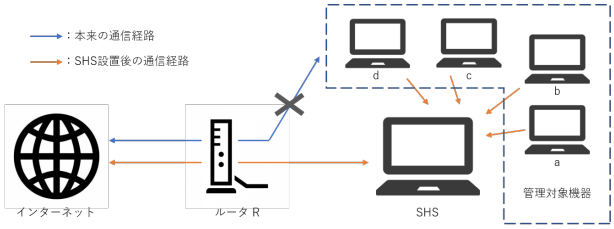

図 1　SHS 設置後のシステム構成図

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

2.4 ARP スプーフィング

ARP テーブルは IP アドレスと mac アドレスの対応表であり，通信に必要な mac アドレスを IP アドレスからスムーズに変換する役割を担っている．ARP スプーフィングは，ARP テーブルを書き換え本来の通信経路を強制的に変更することである．

表 1 に図 1 におけるルータ R，SHS，機器 a，機器 b の ARP テーブル，表 2 に，R が持つ ARP テーブル，表 3 に書き換えられた ARP テーブルを示す．ARP テーブルの書き換えによる影響は図 1 の通信経路の変化に該当する．

表 1　各機器の IP アドレスと mac アドレス

	IP アドレス	mac アドレス
ルータ R	10.1	01
SHS	10.2	02
機器 a	10.101	11
機器 b	10.102	12
機器 c	10.103	13
機器 d	10.104	14

表 2　R が所有する ARP テーブル

	IP アドレス	mac アドレス
SHS	10.2	02
a	10.101	11
b	10.102	12
c	10.103	13
d	10.104	14

表 3　R が所有する ARP テーブル：変化後

	IP アドレス	mac アドレス
SHS	10.2	02
a	10.101	02
b	10.102	02
c	10.103	02
d	10.104	02

3　先行研究

北原が報告 [1] した単独ツールでの ARP スプーフィングの実験結果をまとめた表 3.1 では，パケットの送信間隔に関わらず，高い割合で ARP スプーフィングが成功したことが分かる．2 台同時で実験を行った表 3.2 によると，2 種類のツールを用いて同時に ARP スプーフィングを実行する場合，パケットの送信間隔が短いツールが，より長く ARP テーブルを占有している．

村上らが報告 [2] したセキュリティ設定の不備に対する注意喚起の検証では，注意喚起を行わない場合に比べ 5 週間で 3 倍以上のポート開放状況の改善が確認された．

4　SHS の開発

4.1 ローカル Web サーバ

SHS はホームネットワークに接続する機器を管理するために，ローカル Web サーバを起動する．図 2 に作成した web サイト，表 4 に図 2 における各項目の説明を示す．

表 4　設定画面の機能

ipv4	IP アドレスの確認
access	Wi-Fi への接続権限の設定
control	管理対象の設定
mac	mac アドレスの確認
vendor	ベンダー情報の確認
name	ホスト名の確認
filter	制限されている IP アドレスの確認
config	制限するサイトを追加（URL を入力）
	ホストネームの変更
submit	config の送信
initialize	登録されている機器の初期化

4.2 主要な機能の仕組み

SHS のデバイス検知と ARP スプーフィング，閲覧制限について説明する．

家族が無許可で接続したデバイスを検知するには，デバイスがルータに向けてブロードキャストした ARP リクエストを検知することで実現できる．しかしこの方法では，図 3 のように初回のブロードキャストしか検知できない．

そこで，新たなデバイスの検知は，ローカルアドレス全てに ARP リクエストを送信し，返答される ARP テーブルから IP アドレスと mac アドレスを取得している．これにより，勝手にルータに接続している機器を検知することができる．

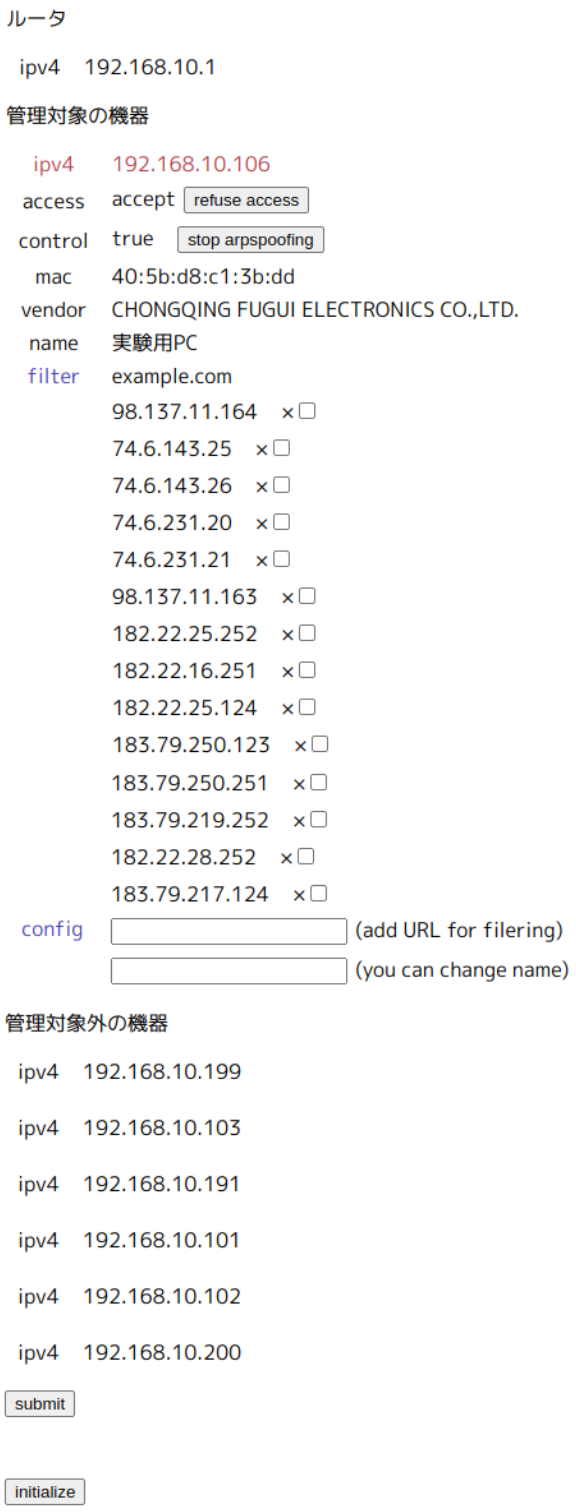

図 2　設定画面（Web サイト）

ARP スプーフィングは，Python にて scapy[4] を用いて 2 秒おきに ARP リプライを送信することで実現している．40 秒に一回 ARP リクエストを送信し，応答がなかった場合，ARP スプーフィングを停止する．

閲覧制限については，nftables[5] を利用している．

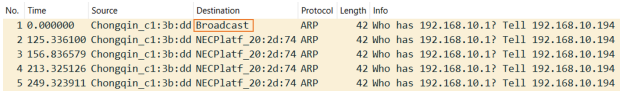

図 3　ARP リクエスト

nftables はファイアウォールで，特定の通信を遮断する．図 4 に nftables に記載した内容を示す．図 4 において，1 に作成した遮断する IP アドレスのリストを 2 で宣言し，読み込む．最後に 3 で IP アドレスのリスト全てに対し，通信を遮断する．

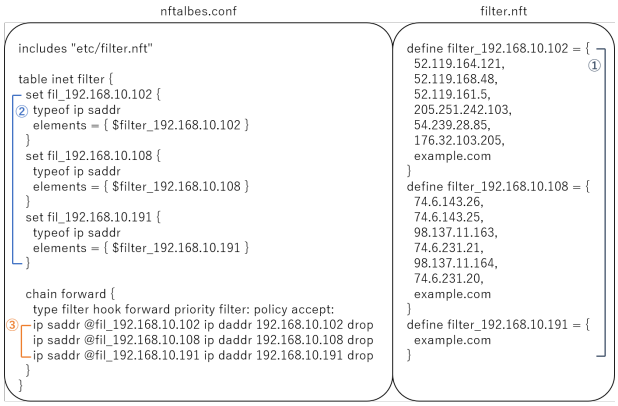

図 4　nftables

4.3　SHS の実行

表 5 に実行画面と説明を示す．通常は 30 秒毎に ARP テーブルを取得しており，その際に管理対象に設定された機器にのみ ARP スプーフィングを実行する．

4.4　課題

実際にルータに接続している全てのデバイスが検知できない．計測した結果，10 の機器に対し，SHS では 8 つしか検出できなかった．検知できなかった IP アドレスに ping を送信したところ「Destination host unreachable.」と出力されたため，宛先ホストに到達できていないことが分かる．このメッセージには宛先ホストがそもそもない，ルータが宛先を知らない等の意味がある．

5　SHS の利用方法

5.1　SHS の起動方法

SHS には Node.js と Python のプログラム言語を使用している．SHS 起動に向けた事前準備として以下のライブラリのインストールが必要となる．

表 5　実行画面の説明

t(s)	意味	実行画面
0 ～ 30	① ARP テーブルを 30 秒毎に取得	count: 0 192.168.10.106: 40:5b:d8:c1:3b:dd 192.168.10.199: 76:f0:98:c9:27:fc 192.168.10.200: 48:a5:e7:4e:07:56 192.168.10.101: 7a:93:2d:b9:62:b3 192.168.10.102: f0:67:28:6b:20:73 192.168.10.103: ca:3f:7f:58:78:f8 192.168.10.1: 08:10:86:20:2d:74
	名前の変更	name_192.168.10.106: 実験用 pc
	ARP スプーフィング の対象に設定	run arpspoofing on 192.168.10.106
30 ～ 60	①と同様	count: 1 （省略）
	ARP スプーフィング実行	192.168.10.106 Start ARPspoofing...
60 ～ 90	①と同様	count:2 （省略）
	url（yahoo.co.jp）の IP アドレスの取得, ブラックリストへの追加	filter_192.168.10.106: yahoo.co.jp 182.22.25.252 stored success 182.22.16.251 stored success 182.22.25.124 stored success 183.79.250.123 stored success 183.79.250.251 stored success 183.79.219.252 stored success 182.22.28.252 stored success 183.79.217.124 stored success refer:25-33

- Node.js
  - python-shell
  - body-parser
  - express
- Python
  - scapy

SHS は配布したフォルダ内にある「nd.js」を実行するため，カレントディレクトリの移動後，ターミナルで「node nd.js」を入力すると起動する．

5.2　サイトへのアクセス制限

SHS の起動後, 任意のブラウザで「http://127.0.0.1:8000/」と入力すると図 2 のサイトにアクセスする．表 4 に記載したように，config の入力欄に制限するサイトの URL を入力し，「control」を true の状態にすると，アクセス制限が完了する．

6　被験者実験

自作したプログラムが正確に動作することの確認するため，2022 年 11 月 16 日から 12 月 18 日に菊池研究室に所属する大学院生，学部生を対象として実験を行った．本実験は参加対象者へのプログラムの配布，各家庭においてプログラムの実行，機器の情報が登録された json ファイルの提出という手順を踏んでいる．表 6 に実験で明らかにされた各世帯におけるデバイスベンダ―の統計を示す．ルータや PC の他にゲーム，映像出力，プリンターを販売している Nintendo，Amazon，Epson 等の機器を検出した．

mac アドレスからベンダー情報が判明しなかったものを「不明」と表記している．ベンダー情報が取得できない原因として mac アドレスのランダム化 [6] が考えられる．これにより，企業ごとに決まっていた mac アドレスに統一性がなくなり，プライバシー保護が期待できる．

7　おわりに

本研究では，ARP スプーフィングを応用することで，子供が危険なサイトにアクセスしないよう，ホームネットワークを安全に管理するシステム SHS を開発した．しかし，本プログラムは Ubuntu での実行を想定しており，windows で実装できている機能はデバイスの検出のみのため，今後は windows でのアクセス制御の実装を課題とする

参考文献

[1] 北原，“ARP テーブルスプーフィング攻撃のリスク評価”，2021 年度明治大学卒業論文，2021.

[2] 村上ら：セキュリティ設定に不備のある IoT 機器の所有者に対する専用アプリを介した注意喚起の効果検証, コンピュータセキュリティシンポジウム 2021, pp.183-190, 2021

[3] IT 用語辞典 e-Words，“ARP【Address Resolution Protocol】アドレス解決プロトコル”（https://e-words.jp/w/ARP.html，2022 年 4 月参照）

[4] Scapy, “Packet crafting for Python2 and Python3” (https://scapy.net/，2022 年 6 月参照)

[5] wiki-nftables，“Main Page” (https://wiki.nftables.org/wiki-nftables/，2022 年 6 月参照)

[6] Wi-Fi Column, “進む MAC アドレスのランダム化。影響や切り替え方法をご紹介”（https://www.ntt-bp.net/column/blog/2021/12/post-64.html，2023 年 1 月参照）

表 6　被験者実験の結果：ベンダー情報

	A	B	C	D	E	F	G	H	I	J	K	合計
BUFFALO	1				2	1	1				1	6
ELECOM			1			1						2
NEC Platforms		1		1						1		3
AlliedTelesis								1				1
HonHai Precision Ind	1								1			2
Nintendo	1	1				2						4
AmazonTechnologies.	1				1		1			1	1	5
Apple	1			1		1					1	4
TP-LINK TECHNOLOGIES			1	1					1			3
Liteon Technology			1									1
INNONET			1	1								2
Seiko Epson		1		1								2
OkiElectric Industry					1							1
HUAWEITECHNOLOGIES					1							1
SonyCorporation						1						1
ASRockIncorporation								1				1
GUANGDONGOPPO[a]		1										1
不明	2	2	1	4	2	6			4			21
合計	7	6	5	9	7	12	2	2	6	2	3	61

[a] GUANGDONGOPPO MOBILE TELECOMMUNICATIONS の略