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（SHS）の開発

菊池研b4　井窪 竜矢

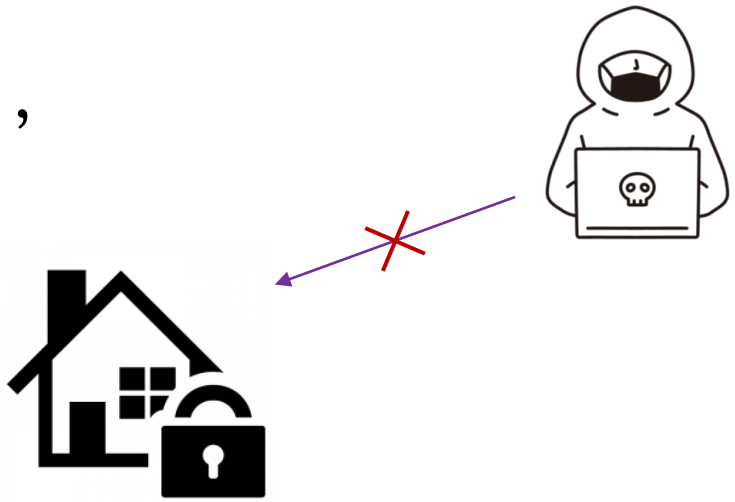
研究背景

背景

- COVID-19の影響によるオンライン作業の増加
- ホームネットワークを運用する上で，危険性の理解が不可欠

目的

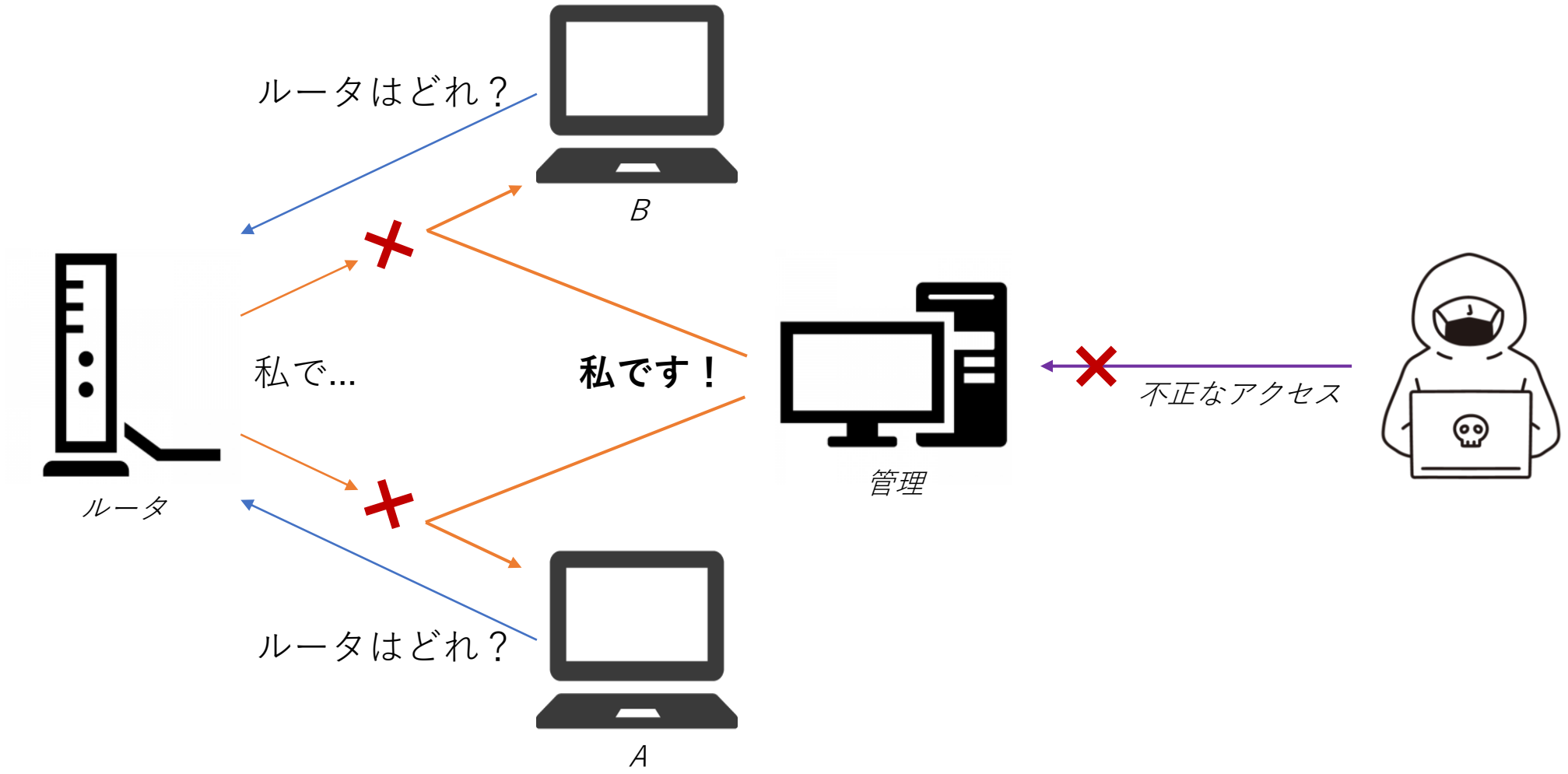
ホームネットワークが危機に晒されないよう，
セキュリティシステムSHSを開発する



ホームネットワークの危険性

	オフィス	ホーム
ファイアウォール	各オフィス専用	簡易的
セキュリティに対する理解	専門の部署	基本的に理解はなく，意識が低い
危険性（盗聴，改竄，マルウェア等）	上記2つのセキュリティ対策により減少	家族の不用意なインストールにより増加

解決方法：ARPスプーフィング



ARPスプーフィング

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

ルータRが所有するARPテーブル

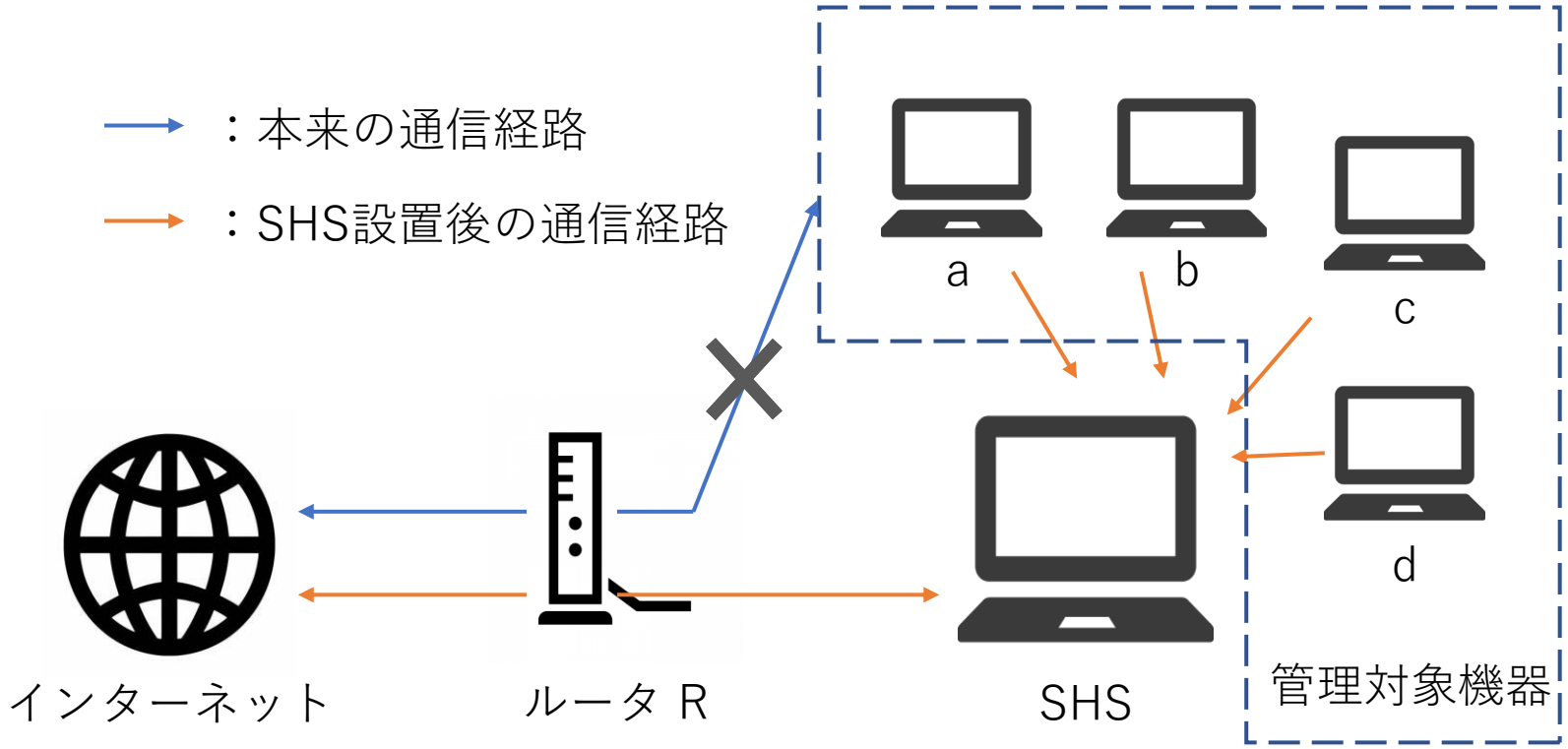
	IPアドレス	macアドレス
SHS	10.2	02
a	10.101	11
b	10.102	12
c	10.103	13
d	10.104	14

ARPスプーフィング後のARPテーブル

	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

SHS設置後のローカルネットワーク

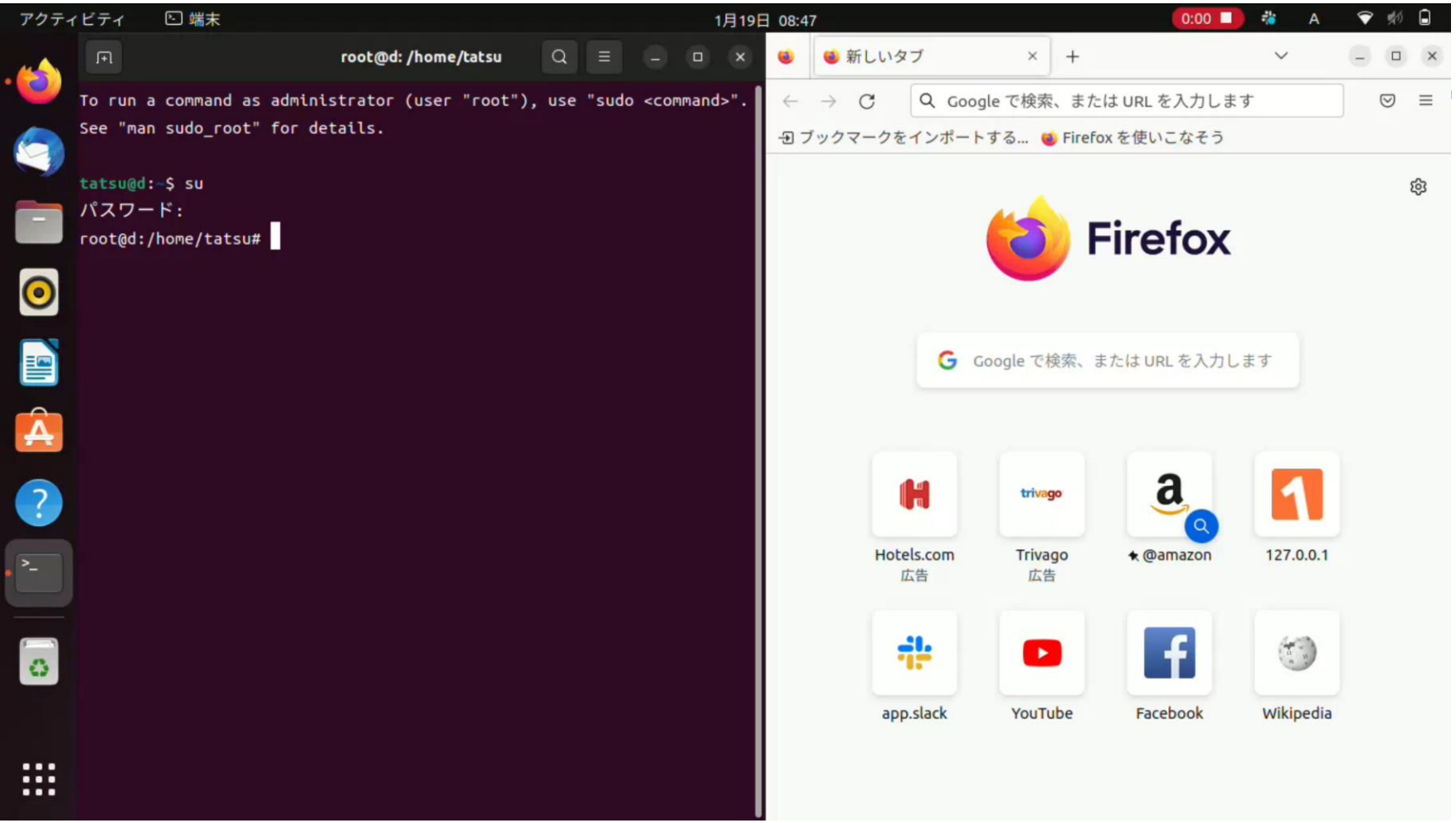
- Node.js
  - python-shell
  - body-parser
  - express
- Python
  - scapy



SHSの内容

SHSでできること

- 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



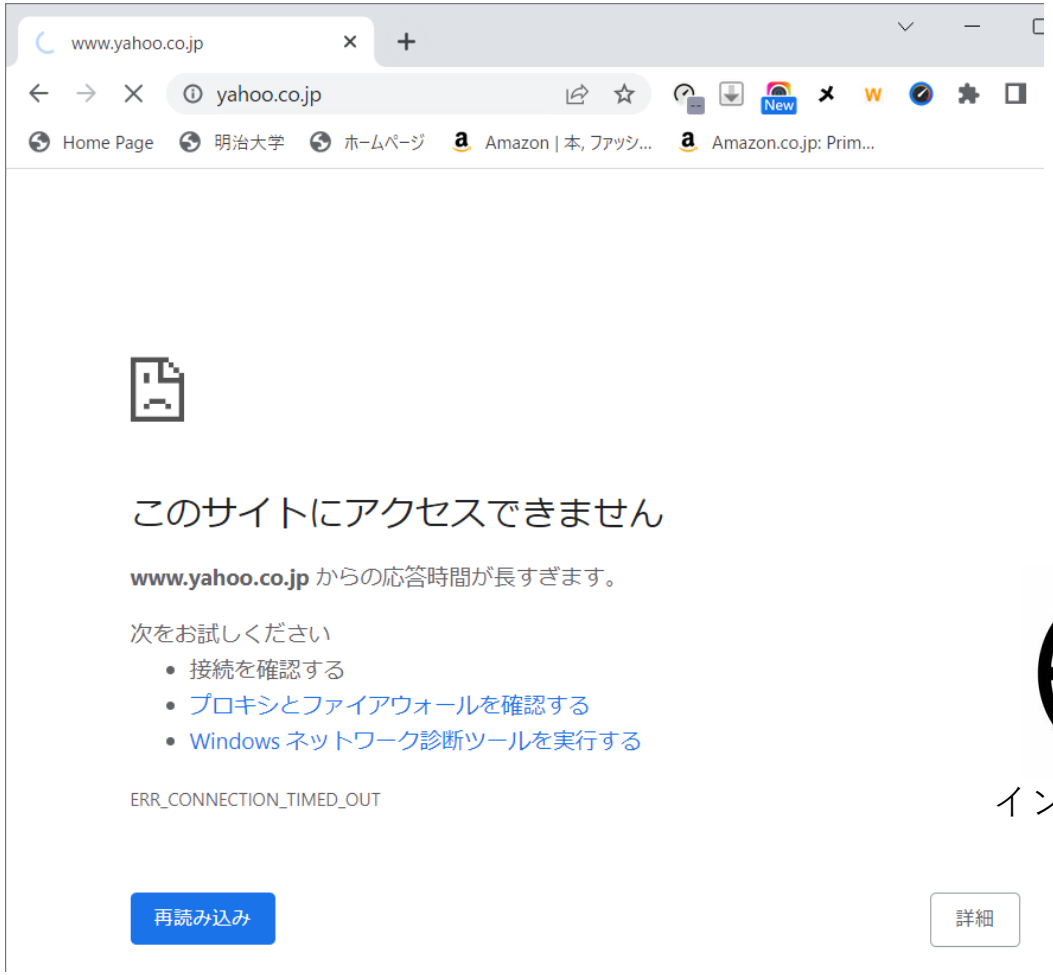
0:07　初期情報の自動取得
　　ARPテーブルの取得（30秒毎）

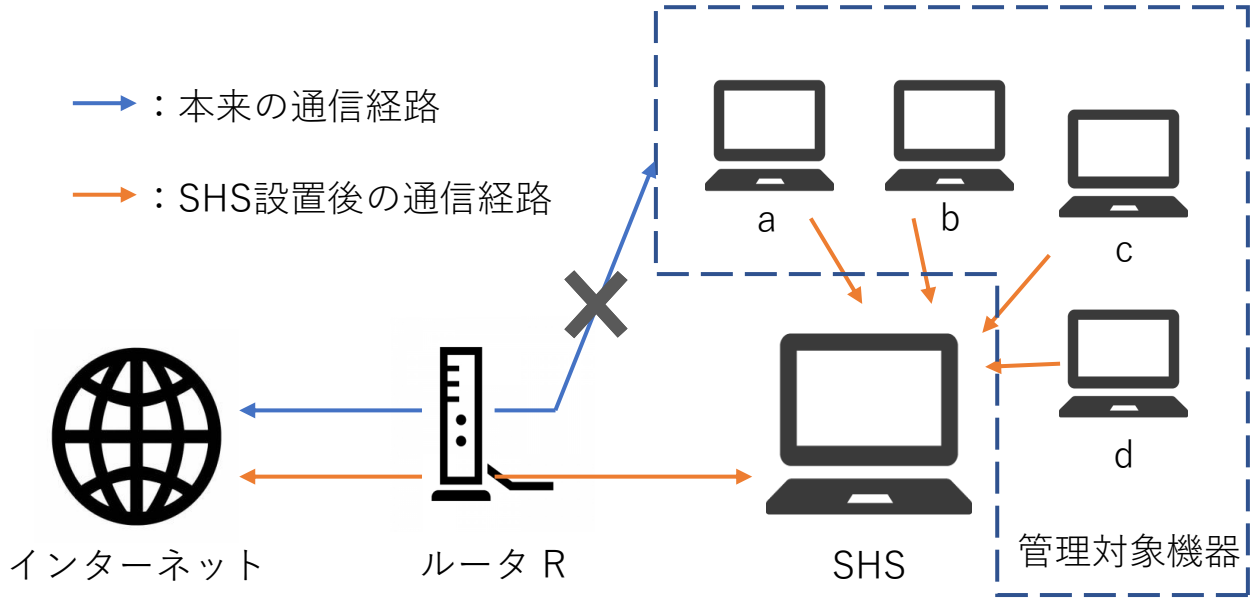
0:23　管理webサイトへのアクセス

1:03　管理対象機器に変更
　　ARPスプーフィング実行

1:23　フィルタの追加方法
　　URLからIPアドレスを取得
　　フィルタの削除，再追加

ARPスプーフィングによる影響





被験者実験：目的

目的

開発したSHSがどの環境においても正確に動作することを確認するため

実験内容

菊池研究室のメンバに各家庭でSHSを実行してもらう

被験者実験：結果

各世帯におけるデバイスベンダーの統計

ベンダー	A	B	C	D	E	F	G	H	I	J	K	合計
BUFFALO	1				2	1	1				1	6
AmazonTechnologies	1				1		1			1	1	5
Nintendo	1	1				2						4
Apple	1			1		1					1	4
NEC Platforms		1		1						1		3
TP-LINK TECHNOLOGIES			1	1					1			3
⋮						⋮						⋮

ベンダー情報の説明

ベンダー	主に取り扱っている電子機器
BUFFALO	ルータ
AmazonTechnologies	映像出力
Nintendo	ゲーム
Apple	スマホ，PC
NEC Platforms	ルータ
TP-LINK TECHNOLOGIES	IoT機器全般

結論

- ARPスプーフィングを応用することで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
- 実証実験により，11人/11人（100%）の家庭でホームネットワークにおいてSHSが稼働することがわかった

今後

SHSはUbuntuでの実装を想定しており，windowsで実装できている機能は機器の検出のみのため，windowsでのアクセス制御の実装を課題とする