SDNを利用したセキュアなホームネットワーク方式

Matsunaga, Kazuya / 松永, 和也

(出版者 / Publisher)
法政大学大学院理工学研究科
(雑誌名 / Journal or Publication Title)
法政大学大学院紀要. 理工学研究科編
(巻 / Volume)
63
(開始ページ / Start Page)
1
(終了ページ / End Page)
7
(発行年 / Year)
2022-03-24
(URL)
https://doi.org/10.15002/00025387

SDN を利用したセキュアなホームネットワーク方式

Secure Home Networking method using SDN

松永和也
Kazuya Matsunaga
指導教員　金井敦

法政大学大学院理工学研究科応用情報工学専攻修士課程

As the number of devices connected to the network in households becomes more and more diverse, cybercriminals are shifting their focus from traditional network devices to IoT devices, which are vulnerable to malware and other attacks due to their insufficient security measures. IoT devices are vulnerable to malware and other attacks. If a device is infiltrated by such an attack, it will be able to freely access other devices in the home network, and the spread of malware will be missed. However, using conventional firewalls and anti-virus software for protection is difficult due to the complexity of the home network itself and the specifications and cost of IoT devices. Therefore, in this research, we propose a system that minimizes the damage caused by attacks by dividing the network segments according to the policies of the devices and users connected to the network in the home network. Specifically, we propose a flexible network configuration by using the concept of SDN, in which the network is centrally managed by a program. From the verification results, we have shown that it is possible to divide the devices connected to the network within the home network and control their communication. In the future, we will need to continue to implement communication outside the home network and isolation of malicious terminals.

***Key Words** : Software Defined Network, OpenFlow, Home Network*

１．はじめに

近年, IoT をはじめとした多種多様な機器がホームネットワーク内に混在する．しかし，これまでネットワークに接続されていないモノが接続されることにより，セキュリティのリスクも高まる．特に IoT 機器はセキュリティ対策が十分に行われていない事が多くマルウェアを始めとした攻撃の対象になりやすい．

従来はファイアウォール等によりパケットフィルタをネットワークに適用する際，一つのセグメントにて構成されるホームネットワークの特性により，その効果がすべての端末に及ぶ欠点があり，結果として，それは正常な通信までを遮断するものとなっている．さらに，ホームネットワークのユーザーはコンピューターの知識に関して精通しているわけではなく，加えてホームネットワークに繋がる機器が増加の傾向にあり，よりホームネットワークの管理は複雑になり，一般ユーザーにはホームネットワークの管理が難しくなりつつある．またこうした IoT 機器のセキュリティ対策の既存研究[1]-[4]では，悪性端末の通信を検知したら，機器に関わらずただ通信を完全に遮断することで，ホームネットワークへの不正アクセスの被害の最小限，および IoT 機器などがマルウェアに感染した場合にその端末が攻撃を行った場合などの被害の最小化を図っている．しかしこれでは，テレビなどといった普段の生活に影響を与えている度合いが高く，また日常的に常にネットワークに繋がっていないと機能が完全に停止してしまう機器の通信までもを完全に遮断してしまうと，それだけで生活に支障が出てしまい，利便性の低下に繋がる．

よって，本研究ではホームネットワークへの不正アクセスの被害を最小限にしつつ IoT 機器などがマルウェアに感染した場合にその端末が攻撃を行った場合などの被害を最小化するシステムの提案を行う．パケットフィルタがすべての端末に及ぶ問題については，ホームネットワークを複数のセグメントに分割しセグメント間の通信制御を Software Defined Network(以下：SDN)[5][6]を用いて行うことで，それぞれの端末間の通信に固有の制御を行い正常な通信までを遮断することを防ぐ．ホームネットワークの管理の難しさについては，ユーザーがネットワーク制御を簡単に行えるような抽象化を図ることで解決する．そして，端末の隔離の仕方については，ネッ

トワークに繋がっている IoT 機器の機能・普段の生活に影響を与えている度合いに応じて SDN を用いて柔軟に変更する．IoT 機器がマルウェアに感染した時，それらを隔離用ネットワークに隔離し，そこの中でネットワークの制御を行う．例えばテレビなどといった日常的に常にネットワークに繋がっていないと機能が完全に停止してしまう機器がマルウェアに感染した場合，同じホームネットワーク内に存在する他の機器への通信は遮断しつつ，外部への通信は許可する．また普段の生活に影響を与えている度合いが低く，完全に機能が停止しても生活に支障が出ない IoT 機器がマルウェアに感染した場合は他の機器への通信や外部への通信も完全に遮断する．このように IoT 機器の機能・普段の生活に影響を与えている度合いによって段階的にネットワークの制御・隔離を行うことで，生活の利便性を損なうことなくホームネットワーク内の被害を最小限に抑える．

２．ホームネットワークの問題点

ホームネットワークがより便利になっていくにつれ，ホームネットワーク上で扱う情報が複雑化し，機器ごとに QoS 制御やセキュリティなど適切な管理が必要となる．しかし，接続する機器数の増加によりその管理コストは大きくなる[1]．

しかし管理コストが大きくなる一方で，ホームネットワークの様々な制御を実装するための構成やホームネットワークユーザーの間の技術的知識の欠如などもまた問題である． IoT 機器を購入するユーザーは，メーカーが適切なプライバシー・セキュリティ保護をデバイスに組み込んでいることを想定しているが，既存の研究では様々な脆弱性が存在していることがあり，実際これらのデバイスの多くは攻撃者のほとんどの努力を必要とせずに侵害される可能性がある[7]．

従来のホームネットワークでは，パソコンやスマートフォンのみがネットワークに接続される場合，エンドポイントでの端末のみを守るセキュリティ対策が中心だった．このようなエンドポイントのセキュリティ対策では，アンチウイルスソフトやファイアウォールが用いられる．アンチウイルスソフトは，マルウェアの特徴や振る舞いを記録したファイルから検知を行う．またファイアウォールは，端末への不必要なアクセスを遮断するための仕組みである．これら双方の組み合わせにより，許可されていないアドレスや端末からの不正アクセスを遮断できる他，ホームネットワークに攻撃者が侵入しても端末を守ることができる．しかし，アンチウイルスソフトに関しては，新種のマルウェアや既存のマルウェアの亜種に対して検知が難しいという欠点を持つため，脆弱性の多い IoT 機器とは相性が悪い．また IoT 機器が普及し，スマートホームなどの考えが生まれると，エンドポイントでのセキュリティだけでは困難であった．IoT 機器であるカメラやスマート家電では，機器の処理能力が低く，エンドポイントでのセキュリティ対策に求められる要件を満たさないからである．さらに独自の組込み用 OS が使われているものもあり，そもそもセキュリティソフトなどが動作しないものがあることや，ホームネットワーク内のすべての端末にこれらの仕組みを導入するのは非常にコストが高いと言える．

従って，こうした仕組みが導入できない端末へのセキュリティ対策も同時に必要である．

また，現在，家庭のネットワークからインターネットに接続すると時は，一般に NAT と呼ばれる LAN 内の IP アドレスからインターネットのグローバル IP アドレスに変換することを無線 LAN ルーターを介して互いに通信し，インターネットに繋がるホームネットワークが構築される．この NAT によって，インターネット上からホームネットワークへの攻撃を防ぐことができる．これは NAT ではホームネットワーク側のプライベート IP アドレスからインターネット上のグローバル IP アドレスが識別できるが，インターネット上からでは NAT を行われていないため，変換前のプライベート IP アドレスを識別できないためである．しかし近年の IoT 機器はファームウェアの更新などで，NAT を無視してインターネットから直接アクセスできるインターフェースを持つ場合がある．結果として，このインターフェースから侵入され攻撃を受ける可能性がある． さらに，ホームネットワークの要となるルーターに対する攻撃も増加している．これはホームネットワークに繋がる IoT 機器がインターネットの出入口となるルーターを乗っ取ることによって，様々な不正活動を行えるためである．実際にルーターの脆弱性を悪用する攻撃を受けルーターの侵入に成功すると，例えばルーターに繋がるパソコンやスマホ，スマートテレビなど様々な機器がサイバー犯罪者が用意した危険なサイトに誘導されフィッシングを行われたり，ルーターの DNS が書き換えられスマートテレビのファームウェア更新サイトを不正サイトへ差し替えることでスマートテレビがランサムウェアに感染するなどの例もある．

またスマートホームの普及などによって，IoT 機器数が増加している中で， OWASP IoT Project[8]は， IoT Top10 を発表した中で，脆弱なパスワードでの侵入やデータのプライバシー保護が不十分であることや安全でないデータの転送などが挙げられており，IoT 機器のセキュリティソフト対策不足について言及されている．

上記の脆弱性から，IoT 機器が機器への感染や攻撃に悪用され，侵入や感染などの被害によってデータ流出や外部サービスへの攻撃などの悪用されるため，予め侵入を前提にセキュリティ対策を考えなければならない．このことから，ホームネットワークセキュリティ対策として必要なものは侵入感染後の被害の最小化である．

３．関連技術と関連研究

第２節で述べた，IoT 機器の接続により管理が複雑になりつつあるホームネットワークにおいて攻撃の被害を最小化させる方法の一つとして，SDN と呼ばれるソフトウェアにより仮想的なネットワークを構築する概念がある．SDN により，利用状況に応じて動的にネットワーク制御を行うセキュアなネットワークを構築できる．

OpenFlow は SDN を具体化する技術仕様の一つであり，従来のネットワーク機器が持つデータ伝送部と制御部をそれぞれ OpenFlow スイッチ(以下：OFS)と OpenFlow コントローラー(以下：OFC)に分離した構成となっている．OpenFlow はフローと呼ばれる単位で通信を行い，条件(ヘッダフィールド）にマッチしたパケットに対して，アクションで指定された動作を行う．このフローは，OFC 上のプログラムにより生成され，OpenFlow を使って OFS へと送られる．送られたフローは OFS のフローテーブルに格納され，以降これを用いてパケットが制御されるようになる．OpenFlow の動作モデルを図１に示す．

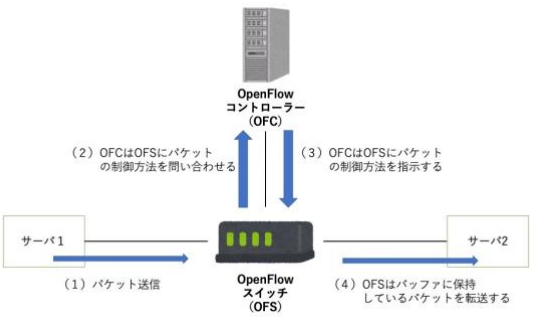

図１　OpenFlow の動作モデル

また関連研究としては，ホームネットワークをネットワーク上の機器・サービスごとに分けて，帯域制御を行うネットワークスライシングと呼ばれる研究がある． 長谷らは，単にホームネットワーク上での情報のやり取りを最適化するだけでなく，機器の増加や機能の高性能化に伴って複雑になるホームネットワークの構築・管理をネットワーク仮想化技術の１つであるスライスを用いることで自動で行い，ネットワーク知識の浅い人物であっても容易に管理を行うことができる手法を提案している[1]．ホームネットワークに接続している各機器をその機器の持つ機能ごとに OpenFlow を用いてスライスを割り当てることによって，機器の追加などのホームネットワークの管理を容易にし，新たに機器が追加された際にもその機器の持つ役割を把握し自動で適するスライスに割り当てる．スライスごとに帯域などを保障することにより，通信品質を向上させ，通信量の増加により発生する通信品質の低下という問題の解決を行っている．

Yiakoumis らは，ユーザーがトラフィック制御などのネットワーク制御のみを行い，その制御操作を通じてインフラが自動で設定される手法を提案している[2]．この提案手法では，ネットワーク操作の抽象化を行うことで，ユーザーが容易にネットワークを構築および構成の変更をすることが可能となっている．

Dangovas らは，SDN を用いてユーザーとデバイスをトポロジに緊密にし，認証を行うことを提案している[3]．提案手法では，認証プロセスがすべてのエンドユーザーにとって使いやすいようにするため，Web ベースの認証インターフェースを実装している．この研究での SDN コントローラーは，クライアントネットワークデバイスとそのメンバーのポリシーグループへの関連付けを管理し，転送の決定を下してこれらのポリシーを適用する．上記の認証が完了することで，通常の転送プロセスが行われるように，認証によるネットワーク制御手法を提案している．

Frank らは，各デバイスの最小許容ポリシーを自動的に構築し，感染したデバイスが攻撃するのを防げる OpenFlow 対応アクセスポイント(AP)を使用したホームネットワークを保護するための新しいモデルを提案している[4]．この研究で実装されている Flow Policy Enforcer(FPE)と呼ばれるホームネットワークを保護するソリューションにより，IoT 機器は通常時は意図した通りに動作するが，攻撃を受けた場合はネットワーク機能が制限され，攻撃者が IoT 機器を踏み台としてさらなる攻撃を仕掛けることを防いでいる．また FPE はデバイスが AP に接続するとトラフィックを監視し，最小のポリシーを自動的に学習し，学習したポリシーが適用されるシステムである．このシステムはホームネットワーク内で完結することでクラウドベースのソリューションで問題となるプライバシーや可用性について保証している．

４．提案手法

（１）提案手法のコンセプト

前項で述べた関連研究より，ホームネットワークをセキュアにし安全に使用できるようにするためには，端末やユーザーごとのネットワークポリシーを設定し，端末ごとの認証システムを導入し，SDN との連携させ，ポリシーごとにネットワークを分け，柔軟に端末をポリシー別ネットワークに移動させることができる構成にし，ネットワーク制御や端末の認証をユーザーにわかりやすくし，コンピューターの制御の抽象化が必要である．そこで本研究では，ホームネットワークへの不正アクセスの被害を小さくしつつ，IoT 機器などがマルウェアに感染した場合にその端末が攻撃を行った場合などの被害を最小化するシステムの提案およびプロトタイプの実装を目的とする．また認証技術により，MAC アドレスだけでなく利用者や端末の種類を登録することで端末のネットワークのセキュリティ強度を操作し，その強度に応じたネットワーク制御を OpenFlow を中心とした SDN 技術によって実現する．

（2）提案モデル

第 1 節の項で述べた通り，ホームネットワークのユーザーはコンピューターの知識に関して精通しているわけではなく，加えてホームネットワークに繋がる機器が増加の傾向にあり，より複雑になるホームネットワークの管理は一般ユーザーには難しいため，ユーザーがネットワーク制御を簡単に行えるような抽象化を行う．

さらに昨今，脆弱なパスワードによる情報流出の被害や IoT のマルウェア感染による DDoS 攻撃の被害があることから，侵入されることを前提としたネットワーク構成にする．そのため，接続時にはすでに感染している，もしくは無線ネットワークに入るためのパスワードが脆弱であるために侵入されるのを防ぐために，認証を SSID/パスワードだけでなくホームネットワークの管理者自身が接続されるマシンを承認することでホームネットワークを使用できるようにする認証プロセスを実装する．そこで提案モデルでは，OpenFlow，認証サーバ，IP アドレスを付与する DHCP，ホームネットワークとインターネットの境界にあたるルーターをシステムの提案のために実装し，ホームネットワーク内に導入する．

ホームネットワーク内の利用者は，認証サーバに端末の登録を行う．登録する情報は，端末を一意に識別できる MAC アドレス，その端末のタイプもしくは利用者によって識別するタイプである．登録した情報からネットワークのポリシーに従って，登録した端末に割り当てる IP アドレスを持つ端末がホームネットワーク内外においてどの程度アクセス権限を許容するかをネットワークポリシーから OpenFlow で設定を行う．これにより，意図せずにすべての IoT 機器やホームネットワーク全体の機器にマルウェアが拡散するリスクや外部への攻撃を軽減することができる．また，端末の登録や通信などを認証サーバを通すことによって，不正アクセスの脅威に対しても有効なシステムとなる．

またこのシステムはホームネットワーク内に物理マシンを設置することで導入する．これによりクラウドベースのソリューションで問題となるプライバシーや可用性についての問題を解決する．提案モデルの概要図を図 2 に示す．

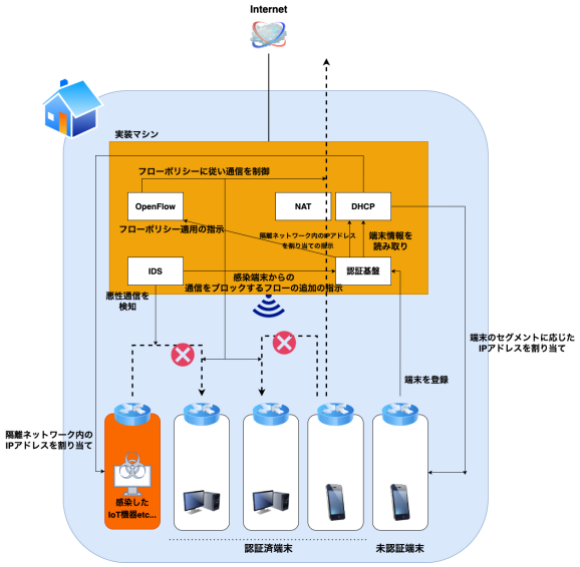

図 2　提案モデルの概要図

また環境として想定したホームネットワークは，端末や利用者ごとに「未登録端末」「PC/携帯」「家電」「IoT 機器」「その他」「親」「子」「高齢者」「ゲスト」「隔離ネットワーク」の 10 種類のネットワークセグメントで区切る．表 1 にセグメント間，セグメント外への通信制御をまとめたものを示す．

表 1　セグメント間，セグメント外への通信制御（○：許可，×：遮断，△：一部許可）

NW_ID	機器	セグメント内への通信	別セグメントへの通信	外への通信
1	未登録端末	○	×	×
2	PC/携帯	○	○	○
3	家電	○	△(NW_ID=2,6,7,8)	○
4	IoT機器	○	△(NW_ID=2,6)	○
5	ゲスト	○	×	○
6	親	○	○	○
7	子	○	△(NW_ID=2,3)	○
8	高齢者	○	△(NW_ID=3)	○
9	その他	○	×	○
10	隔離ネットワーク	○	×	×

さらに本研究では SDN を用いる．SDN では，仮想ネットワークを生成・削除したり，ネットワーク構成の変更や動作状態の監視などを全てソフトウェアで行う．この SDN を導入することにより，IoT 機器の普及やサーバーやストレージの仮想化が進む中でホームネットワークのようにネットワーク構成要素が急速に複雑になっていくにも関わらず，ネットワークは物理的な制約に縛られていたことを，簡単かつ柔軟で迅速なネットワーク構成を変更可能にする．

さらに従来のホームネットワークでは無線 LAN ルーターがホームネットワークの境界に位置していたが，この提案モデルにおいては実装マシンがその役割を果たす．実装マシンは無線 LAN ルーターのように DHCP の役割を行

うと同時に，認証技術，SDN による通信制御，これらを操作する基盤をホームネットワーク内に提供する．

５． プロトタイプ実装

プロトタイプの実装環境についてシステムは一台の RaspberryPi4[9]上に OpenFlow とその他のサービスから構成される SDN ネットワークを構築する．OFS と OFC，NAT はホストマシン上で動作させ，DHCP や Redis，Web サーバは仮想化上で動作させる．RaspberryPi4 のスペックは表 2 に示し仮想マシンについては表 3，4 に示す．

表 2　RaspberryPi4 のスペック

構成要素	スペック
CPU	quad-core Cortex-A72 (ARM v8) 64-bit
メモリ	8GB
ホスト OS	Ubuntu 20.04LTS
仮想化	Docker
動作サービス	OFC，OFS，NAT

表 3　仮想マシンのスペック

構成要素	Web サーバ	DHCP	Redis
仮想化	Docker	Docker	Docker
動作サービス	WebUI	DHCP，DB	KVS

表 4　仮想マシンのスペック

構成要素	DNS
仮想化	Docker
動作サービス	DNS サーバ

実装する SDN ネットワークの全体像を図 3 に示す．wlan0 および eth0 はそれぞれ OFS となる OpenVSwitch と接続し，NIC，無線 LAN アダプタと連携する．これによって wlan0，eth0 のトラフィックを NAT や OpenFlow によって制御を行い，ホームネットワークの SDN を構築する．

現在の進捗としては IDS の構築および外部との通信以外まで完了している．これにより，コンピューターの知識に関して精通しているとは限らないホームネットワークのユーザーでも端末の認証やネットワーク制御を簡単に行うことができ，SDN により利用者と機器のポリシーに応じて分割されたホームネットワーク内のネットワーク間の通信制御を行える．また，もし未登録端末がマルウェアに感染していても，いきなりマルウェアの感染拡大につながる危険性は無い．

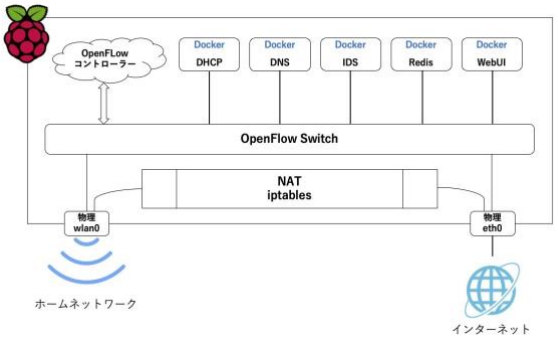

図 3　SDN ネットワークの全体像

６． 考察

現在実装しているプロトタイプに対して，2 つの実験を行った．検証環境としては，図 4 のように機器を設置し，登録者のみ IoT 機器を通信可能，来訪者は内部の端末と通信不可，未登録端末は内部の端末と通信不可といった固定ルールで端末と利用者に応じたセグメンテーションで分けた．

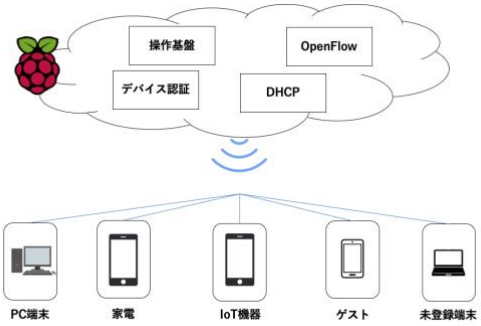

図 4　評価実験環境

1 つ目は，ホームネットワークで細かく分けたマイクロセグメンテーションと OpenFlow によって意図した通りにアクセス制御が行われているかを確認した．実験内容は，セグメント毎の疎通の実験と認証済み端末のみが許可されたセグメントに通信できるかの確認を行った．結果は表 5 に示す．

2 つ目は，ユーザビリティの評価において，プロトタイプの実装において，接続要求端末が登録を行い，登録を行ったアドレスが適用されるまでの時間を計測した．結果は図 5 に示す．

表 5　アクセス制御の評価

内容	PC	家電	IoT	ゲスト	未登録端末
from PC	○	○	○	×	×
from 家電	○	○	×	×	×
from ゲスト	×	×	×	○	×
from 未登録	×	×	×	×	○

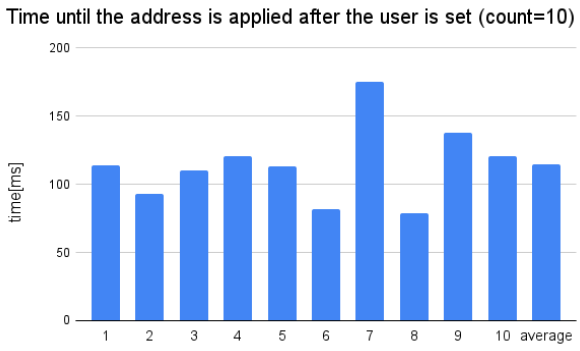

図 5　アドレス適用までの時間

アクセス制御について，IP アドレスとフローにおけるアクセス制御ではそれぞれ定義した通りに動作していることが確認できた．未登録端末の動作確認では，登録端末が接続されていることを確認できなかったことから，もし未登録端末がマルウェアに感染していても，いきなりマルウェアの感染拡大につながる危険性は無くなったと考えられる．

ユーザビリティについては，図 5 に示すように、アドレス適用までに時間で評価した．これはバックエンドの API での応答時間を見ているだけであるため，ユーザーが多少の時間はかかると考えられる．この点を踏まえると，接続要求端末が登録を行い，登録を行ったアドレスが適用されるまでの時間はおよそ 50〜60 秒ほどかかると考えられる．従って端末の登録の実験よりユーザーが快適に設定できるシステムになったと考えられる．

また，本手法では，ホームネットワークにおいて、特にマルウェア感染に注目して，攻撃の被害を最小化する方法としてセグメント分割を行い，セグメント間の通信を制限する手法を提案した．

本研究では今後ルールベースの IDS を導入することによって既存のマルウェアや怪しい通信を検知することは可能となる．しかし，新しいマルウェアなどの出現や新しいソフトウェアの脆弱性を利用した攻撃を検知することは難しい点は，今後の課題である．

さらに，OWASP IoT Project[8]は IoT デバイスが直面する課題としてあげている，データのプライバシーにおいてこの提案手法は LAN 内で制御していることから，クラウドベースのソリューションとは異なり データのプライバシーとクラウドサービスが落ちた場合の可用性などの問題を回避できる．

昨今のホームネットワークでは，ストリーミングサービスやスマートホームの発展により，トラフィックの種類やトラフィック量の増大により，ネットワークが遅くなるなどの可能性があるため，それぞれのセグメントをサービスごとにより細かく区切り，ネットワーク上で提供するサービス品質である QoS(Quality of Service)を利用して，ある特定の通信を優先して伝送させたり，帯域幅を確保することでより快適なホームネットワークが提供できる．

本提案手法は，ホームネットワーク内の端末や接続形態に対応しつつ，今後さらに増えるであろう IoT 機器それぞれにセキュリティ製品導入が難しいことや脆弱であることによるセキュリティ被害を防ぐために，SDN を導入した．今後スマートホーム発展によるホームネットワークの形態の多様化が進んだ場合にも対応できる．

7． 結論

本研究では，SDN を利用したシステムからマイクロセグメンテーションという端末や利用者のセキュリティポリシーからホームネットワーク内でネットワーク分割を行い，その上で OpenFlow によるネットワーク制御およびセキュリティ対策である IDS，OpenFlow のフロールールを利用した感染や二次被害を防ぐためのマイクロセグメンテーションをホームネットワークに適用する手法を提案した．

また，この手法を利用したプロトタイプを実装し，実際にホームネットワーク内の端末と利用者に応じた端末間の通信制御の動作を確認し，ユーザビリティの評価を行った．

その結果，新しく登録しようとした端末がマルウェアに感染していてもいきなりマルウェアの感染拡大につながる危険性は無くなったことが確認できた．また端末の登録の評価実験より，ユーザーが快適に設定できるシステムであることが確認できた．

今後の課題として，引き続きプロトタイプの実装を進める必要がある．今後実装する必要がある機能として具体的には，ホームネットワーク外への通信処理や，IDS と SDN を連携させた悪性端末の隔離，トラフィックの種類やトラフィック量の増大によりネットワークが遅くなる可能性への対策としての QoS 制御などである．また端末の隔離の仕方について，IoT 機器と生活の利便性を考慮した隔離の仕方を具体的に精査する必要もある．

謝辞

本研究を進めるにあたり，ご指導して頂いた指導教員の金井敦教授に感謝致します．また，ご協力頂いた皆様，研究室の方々に厚く感謝を申し上げます．

参考文献

1) 長谷錦，吉村悠，今野裕太，佐藤健哉，″NFV を利用したホームネットワーク管理手法の提案″，FIT2016，2016
2) Y. Yiakoumis, M. Bansal, S. Katti, and N. McKeown, "SDN for Dense Wi-Fi Networks," in Presented as part of the Open Networking Summit 2014 (ons 2014), 2014
3) V. Dangovas and F. Kuliesius, "SDN-Driven Authentication and Access Control System," The International Conference

on Digital Information, Networking, and Wireless Communications (DINWC2014), no. June, pp.20-23, 2014

4) M. Frank and M. Ghaderi, "Securing Smart Homes with OpenFLow," Science, Oct 2019

5) Bruno Astuto A. Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti. A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. IEEE Communications Surveys & Tutorials. 13 February 2014

6) D.S Rana, S. A. Dhondiyal, and S.K. Chamoli, "Software Defined Networking (SDN) Challenge, issues and Solution," International Journal of Computer Sciences and Engineering, vol. 7, no. 1, pp.884-889, Jan. 2019

7) V. Sivaraman, H. H. Gharakhili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-levelsecurity and privacy control for smart-home IoT devices," in 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications, Wimob 2015, 2015, pp.163-167

8) OWASP, “NFVOWASP Internet of Things Project,”FIT2016, 2016.28/04/2018, vol.64, no.9, pp.2489–2509, 2018

9) RaspberryPi, "Teach, Learn, and Make with Raspberry Pi," 2020. [Online]. Avaliable: https://www.raspberrypi.org/