Vol.2016-DPS-166 No.29
Vol.2016-CSEC-72 No.29
2016/3/4

OpenFlow を用いたホームネットワークへの接続端末制御による不正アクセス防御手法の提案

村上萌[†1]　中村嘉隆[†2]　高橋修[†2]

概要：近年，モバイル端末や情報家電などの普及によりホームネットワークの形態が多様化している．一方で，異なるネットワークや様々な端末が混在することによる，多数のセキュリティ脅威からホームネットワークを保護することが必要とされている．それらの中でも，特に不正アクセスの発生件数は年々増加傾向にあるため，早急な対策を取るべきであると考える．本稿では，端末がホームネットワークへの接続時に認証システムを設けることで不正アクセスを防止する方法を提案する．具体的には，SDN 技術の一つである OpenFlow を用いた認証システムを構築し，同ネットワーク内へと接続できる端末を制限することで，脅威からの被害を防止する．

キーワード：ホームネットワーク，セキュリティ，OpenFlow，認証

Proposal of unauthorized access defense technique by the connection terminal control to the home network using the OpenFlow

MEGUMI MURAKAMI[†1]　YOSHITAKA NAKAMURA[†2]
OSAMU TAKAHASHI[†2]

Abstract: In recent years, the form of the home network is diversified by spread of mobile terminals and information appliances. On the other hand, due to the fact that the different networks and various terminal are mixed, it is possible to protect the home network from a large number of security threats are needed. Among them, for in particular incidents of unauthorized access are increasing every year, think that it should take immediate measures. In this paper, the terminal is to propose a method to prevent unauthorized access by providing the authentication system at the time of connection to the home network. Specifically, to construct an authentication system using OpenFlow which is one of the SDN arts, by limiting the terminal that can be connected to the same network, to prevent damage from threats.

Keywords: Home network, Security, OpenFlow, Authentication

1. はじめに

近年，IoT (Internet of Things) が注目を集めるようになり，今後あらゆるものがネットワークに接続され利用されることが予想される．それに伴い，ネットワーク内には様々な端末や機器が混在することになる．企業内ネットワークはもちろん，特に家庭内のネットワーク (以下：ホームネットワーク) は情報家電などの普及も加わり，その形態が多様化していくと考えられる．

図 1 にホームネットワークのモデル[1][2]を示す．ホームネットワークは一般的に有線ネットワーク，無線ネットワーク，センサネットワークなどの異なるネットワークで構成されている．それらのネットワーク内に配置される端末に関しては，パソコン，モバイル端末，それらに搭載されるアプリケーションが存在している．また，近年の技術の発達により情報家電など，これまでネットワークに接続されずに使用されてきた端末や機器も存在している．

一方で，異なるネットワークや端末が混在することで，それぞれに関わる様々なセキュリティ上の脅威が顕在してしまう可能性がある．

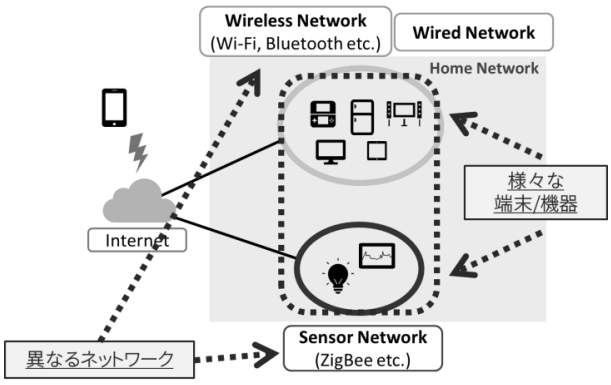


図 1　ホームネットワークのモデル

セキュリティ上の脅威の例として，不正アクセス，盗聴，サービス妨害･拒否攻撃，ウィルス攻撃などが挙げられる．これらが各種端末やネットワークごとに顕在した場合，個別に対処するとコストや時間がかかってしまうという問題がある．そこで，それぞれの脅威に対し一括に対処する必要がある．

また，顕在するセキュリティ上の脅威に関して，特に近

†1 公立はこだて未来大学大学院システム情報科学研究科
†2 公立はこだて未来大学システム情報科学部

年では不正アクセスによる被害が多発している[3][4]. また, 不正アクセスの発生件数別で考えると，一時は減少傾向が見られたが，ここ数年で再び増加傾向が見られる[5]．そこで本稿ではこれを踏まえ，多数存在するセキュリティ上の脅威の中でも不正アクセスに焦点を当てる．

2. 関連研究

2.1 ホームネットワークのセキュリティ

Kim ら[6]はホームネットワークを安全に利用するためにはいくつかのセキュリティ技術があるが，それらの中で認証技術は不可欠であると述べ，ホームネットワーク内に認証システムの設置を提案している．認証システムの役割は既知の端末と未知の端末を区別し，既知の端末のみ通信を行わせることである．ホームネットワーク内に設置された認証システムを利用して，端末がホームネットワーク内外と通信する前に認証を行う．認証に成功した端末は既知の端末であるとみなされ，ネットワーク内では既知の端末同士でのみ通信を行うため，結果としてネットワーク内の安全を保つことができる．

2.2 認証技術

認証技術の既存研究として吉田[7]は認証情報を利用した不正アクセス検出法を提案している．一般的に認証は正規ユーザが認証システムにアクセスし, ID やパスワードなどの情報を入力後，その情報がシステムに保存されている情報と比較され，一致した場合にはアクセス許可，一致しない場合にはアクセス拒否という処理が行われる．この処理内でシステムに対し，正規ユーザが行わない特殊なアクセスや，正規ユーザのアクセスパターンから大きく外れたパターンが検出された場合に不正アクセスがあったとみなす．しかし，不正ユーザは不正アクセスの発生を検出されないように特殊なアクセスを避ける傾向にある. そのため, 認証システムにおけるアクセスにおいて必ず発生する認証処理や, 認証確認処理時に得られる情報を元にすることで, 特殊なアクセスパターンを用いずに不正アクセスの検出を可能としている．

具体的な動作として，正規ユーザが認証時成功した際, 認証サーバが発行する認証情報に加え認証成功時に得られるユーザ識別情報（認証成功時刻や回数など）をシステム内に登録し, 認証情報と共にそれを正規ユーザに付与する．正規ユーザはアクセス時に付与された情報を利用してアクセスする．認証サーバの持つ情報とそれが一致した場合，アクセスが許可される．また，その際にユーザ識別情報が更新され，ユーザに再び付与される．両者が持つ情報が一致しなかった場合，認証情報は無効化されアクセスも拒否される．ユーザ識別情報が更新される仕組みによって，認証情報を盗聴されたあるいは，正規ユーザよりも先に不正ユーザによる不正アクセスが発生した場合でも，次に正規ユーザがアクセスした際に不正アクセスがあったことを検出できる．

以上の手法を用いることでホームネットワーク内に対する不正アクセスを検出することが可能だと考える．しかし，ホームネットワーク内には異なる規格のハードウェアやそれに搭載される様々なアプリケーションが混在しているため，それらすべてに対応したシステムの構築や更新を続けるのは困難である．従って，システムをすべての端末や規格に対応したソフトウェアとして構築するのではなく, ホームネットワーク内で通信するのであれば，どの端末も必ず利用するネットワークを利用したシステムを構築することが望ましいと考えられる．さらに，端末数の増加に伴い認証処理の手間も増大すると考えられるため，ネットワークの状況に合わせて動的に認証情報を管理できるシステムを構築する必要がある．

2.3 OpenFlow

本稿では前項で述べた問題を解決するために OpenFlow を利用する[8]．OpenFlow とは SDN (Software Defined Network) を具体化する技術仕様の一つであり, ネットワークの機能をソフトウェアで制御する技術である．従来のネットワーク機器が持つデータ伝送部と経路制御部をそれぞれ OpenFlow スイッチと OpenFlow コントローラに分離した構成となっている．

2.3.1 フロー

OpenFlow はフローと呼ばれる単位で通信を行っており, その情報は OpenFlow スイッチが持つフローテーブルに蓄積される．フローはヘッダフィールド，アクション，統計情報の 3 要素で構成されており, OpenFlow スイッチが通信を受信した際，その通信を条件で判別 (マッチング) し，決められた動作 (アクション) を行う．マッチング条件には従来のスイッチがルーティングに利用していた IP アドレス，MAC アドレスだけでなく，TCP や UDP のポート番号など複数のレイヤをまたがる様々なものを利用することができ，さらにこれらのマッチング条件を複数組み合わせて転送先を指定できる. アクションには通信の転送, 破棄, パケットの書き換えなどが指定できる．統計情報では，フローテーブルに登録されているフロー数やマッチング処理回数などを管理している．以上のことから OpenFlow を利用することで従来と比べ柔軟な経路の構築・管理が可能となる．

2.3.2 OpenFlow プロトコル

フローは OpenFlow コントローラにより生成され，OpenFlow スイッチへと送られる．この間の通信に OpenFlow コントローラとスイッチ間の通信に用いられる

Vol.2016-DPS-166 No.29
Vol.2016-CSEC-72 No.29
2016/3/4

のが OpenFlow プロトコルである．プロトコルで定義されている代表的なメッセージとして，Packet In,メッセージ，Packet Out メッセージ，Flow Mod メッセージなどがある．Packet In メッセージは, OpenFlow スイッチからコントローラに対し，パケットを受信したことを通知するメッセージである. OpenFlow コントローラはこの通知の内容を解析することで，通信の振る舞いを決定する．Packet Out メッセージは OpenFlow スイッチからパケットを送出されるために OpenFlow コントローラからスイッチに対して送信するメッセージである．ポートやパケットの種類については自由に指定できる．Flow Mod メッセージは，OpenFlow スイッチで記述されているフローを書き換える場合や，スイッチに新規のフローを追加する場合に用いられるメッセージである．

2.3.3 OpenFlow の動作概要

図 2 のようなネットワーク構成を例として OpenFlow の動作概要を述べる．

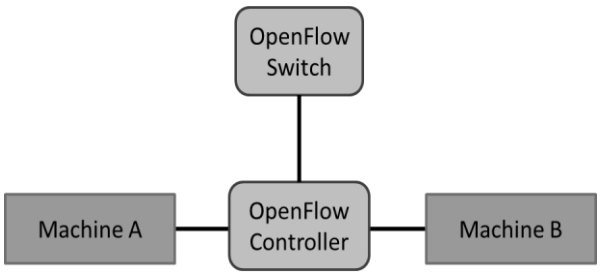


図 2 OpenFlow のネットワーク構成の例

(1) コントローラとスイッチ間の接続

OpenFlow スイッチは OpenFlow コントローラの IP アドレスを宛先として，スリーウエイハンドシェークを開始し，TCP コネクションを確立する．OpenFlow コントローラと OpenFlow スイッチはメッセージを送受信し合い，互いのバージョン情報，スイッチの情報，パケットのサイズ指定，スイッチの状態の情報をやり取りし，接続を確立する．

(2) あらかじめフローを登録しておいた場合の通信手順

コントローラとスイッチ間の接続が成立した段階でコントローラがフローの登録・変更・削除をスイッチに対し要求する．コントローラは Flow Mod メッセージを送り，複数のフローエントリの登録をまとめて指示する．マシン A か OpenFlow スイッチにマシン B の IP アドレス宛とした ping コマンドを実行する．OpenFlow スイッチはフローテーブルから先ほどの動作に該当するフローエントリを確認する．確認後フローエントリに従いパケットを転送し，マシン B にパケットが到着する．

(3) あらかじめフローを登録していない場合の通信手順

マシン A から OpenFlow スイッチにマシン B の IP アドレス宛とした ping コマンドを実行する．フレームを受け取った OpenFlow スイッチはフローテーブルのエントリを確認し，条件に該当する情報がないということが判明する. OpenFlow スイッチは受け取ったフレームをバッファに保存した上で，Packet In メッセージで OpenFlow コントローラにフレームの内容を通知する．コントローラはフレームの内容をもとに, フレームの処理を決定する．OpenFlow コントローラは，OpenFlow スイッチに対し Flow Mod メッセージでフローエントリの追加，Packet Out メッセージで転送を指示する．これでマシン B にフレームが到着する．

3. 提案方式

関連研究で述べた認証技術は，インターネットなどの一般的なネットワークでの利用を想定したものであることから，ホームネットワークの環境には適していないと考えられる．そこで本稿では OpenFlow を利用することにより，ホームネットワークに適した形で認証技術を実現する．OpenFlow を利用して認証する端末を限定し, 動的に接続を管理することで，不正アクセスによる被害を軽減するようにしたのが本提案方式の特徴である．

3.1 想定環境

本稿では，正規ユーザである端末がホームネットワーク外から内へ通信を開始する状況を想定する．ホームネットワーク内から外への通信については, 想定外とする. また，端末数は一般的に利用されているルータの推奨接続台数である 5~10 台を想定する．

3.2 提案方式の概要

本提案方式では OpenFlow と認証技術を組み合わせることにより, ホームネットワークに接続する端末を制限する．端末に接続制限を設けることで，既知の端末と未知の端末を区別し, 不正アクセスそのものを事前に防止する. また，認証時にやり取りされる情報を利用した不正アクセスの検出方法についても検討する．以上を実現するにあたって，本提案方式では下記のステップを行う．

- 端末の登録
- 端末の判別
- 接続の許可・不許可
- 不正アクセスの検出

また，本提案方式のシステムは以下で構成されている．

- 接続要求端末
- 登録端末
- OpenFlow スイッチ・コントローラ

3.2.1 端末の登録

接続要求端末)はネットワーク上に存在する登録端末を利用して MAC アドレスや機器の接続優先度などの機器を判別するための情報 (機器情報) を登録する．(図 3 ①) 登録端末は登録された機器情報と認証成功時刻，成功回数といった認証処理時頻繁にやり取りする情報（識別情報）を接続要求端末と外部データベースの両者に登録情報として保存する．(図 3 ②) 以上で接続要求端末の登録は完了となる．

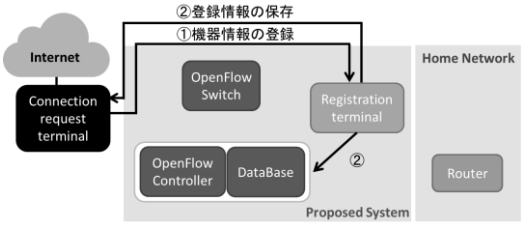


図 3 端末登録時の動作

3.2.2 端末の判別

接続要求端末は通信を開始するにあたり，まず前述の登録端末で登録情報の照合を要求する. (図 4 ①) 要求を受け取った登録端末は，接続要求端末と外部データベースに保存された両者の登録情報を用いて照合する. 照合した結果，両者の登録情報が一致したら，その結果を受けて，外部データベースの登録情報を更新し，OpenFlow を用いて端末に対する接続制限を行えるようにする．(図 4 ②)

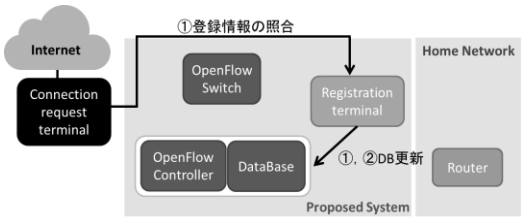


図 4 通信判別時の動作

3.2.3 接続の許可・不許可

登録情報照合後．接続要求端末は OpenFlow スイッチに対し接続を開始する. (図 5 ①) 通信要求を受け取ったスイッチは Packet In メッセージとして，OpenFlow コントローラ に経路の振り分け先の問い合わせを行う．(図 5 ②) Packet In メッセージを受け取った OpenFlow コントローラは外部データベースと連携して，通信の経路の振り分け先を Flow Mod メッセージとして OpenFlow スイッチの持つ経路表を更新するよう指示する. (図 5 ③) 指示を受け取った OpenFlow スイッチは指示通り経路表を更新し, 接続要求端末からの通信をホームネットワーク内に通す. (図 5 ④) 以上により，接続要求端末はホームネットワークに接続可能となる．接続成功後は，登録端末と接続要求端末の持つ登録情報の更新を行う．(図 5 ⑤)

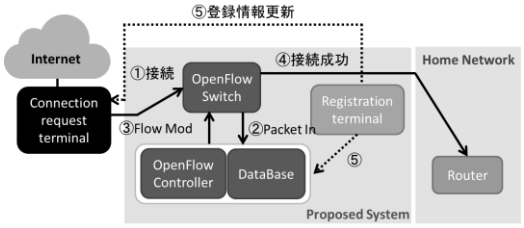


図 5 接続許可時の動作

3.2.4 不正アクセスの検出

第三者による不正アクセスがあった際の動作について述べる．不正端末は OpenFlow スイッチに対して接続を開始する. OpenFlow スイッチは不正端末からの前項の正規端末時と同様に Packet In メッセージとして, 経路を OpenFlow コントローラに問い合わせを行う．その返答として，OpenFlow コントローラはスイッチに問い合わせを返すが，第三者による不正端末は端末情報を登録していないため，外部データベースは更新されていない．そのため，登録情報が一致せず，結果としてホームネットワーク内への通信はできず遮断されることとなる．また，万が一接続要求端末が持つ登録情報が盗聴され，不正端末が認証に成功してしまった場合 (図 6 ①，②) には，認証成功時に正規端末が接続した際と同様に，登録情報も更新される．(図 6 ③) そのため，正規端末が接続時に自身の持つ情報では登録情報が一致せず (図 6 ④), 自身より前に接続されたことが判明し，不正アクセスを検出することが可能となる．

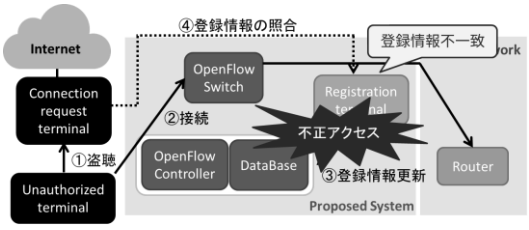


図 6 不正アクセス検出時の動作

4. 実験と評価

4.1 実装

提案方式は OpenFlow コントローラのフレームワークのひとつである Trema を利用して実装した．また，実験の比較対象となる関連研究の方式は，同等の環境や条件が良いと考えたため, Trema を構成する言語と同じ Ruby を利用して実装した.

4.2 実験環境

実験を行うにあたり，Linux ディストリビューションのひとつである Ubuntu[9] を利用して, OpenFlow コントローラ，OpenFlow スイッチ，ネットワーク内に存在する端末となるシミュレーションサーバを複数台構築した．提案方式での詳細な実験環境を表 1 として下記に示す.

Vol.2016-DPS-166 No.29
Vol.2016-CSEC-72 No.29
2016/3/4

表 1 実験環境

	ソフトウェア	OS	台数
OpenFlow コントローラ	Trema[10]	Ubuntu 12.04 desktop	1
OpenFlow スイッチ	Open vSwitch	Ubuntu 12.04 server	1-2
他端末		Ubuntu 12.04 server	5-10

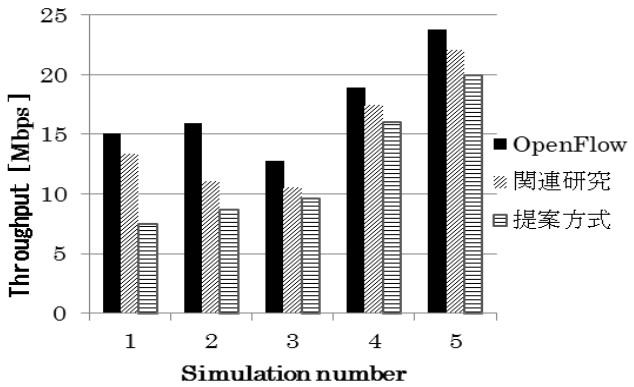
4.3 基礎実験

本実験は，提案方式における想定環境の基本性能評価のために行った．実験の内容として，本提案方式を実装した環境，OpenFlow を実装した通常のネットワーク，関連研究で述べた認証技術を適用したネットワークの 3 つの環境のスループットをそれぞれ測定し, 結果を比較した. また，シミュレーションの試行回数は 10 回，測定時間は 10 秒とし，その平均を各環境のスループット値として算出した．また，表 2 に示した通りネットワーク内の端末同士の通信のシミュレーションを複数用意し，各場合によるスループットの差を測定した．

表 2 通信のシミュレーション

番号	内容
1	同じ OpenFlow スイッチ（関連研究の場合はスイッチ）に繋がれた端末間
2	異なる OpenFlow スイッチ（関連研究の場合はスイッチ）に繋がれた端末間
3	隣接する端末間
4	ホームネットワーク外の端末と内の端末間
5	ホームネットワーク外の端末と OpenFlow スイッチ間

5. 結果と考察



実験結果を下記に図 4 として示す.

図 4 スループットの測定結果

実験結果から，通常の OpenFlow を適用したネットワークとの比較では，関連研究，提案方式ともにスループットが低い値となった．これは関連研究のネットワークと提案方式ともにネットワーク内に認証システムを設置したことにより，その負荷が増加したためだと考えられる．また，関連研究と提案方式との比較では，ホームネットワーク内でのスループットに多少差が現れたものの，ホームネットワーク外から内へのスループットにはほぼ差が現れなかった．この結果から，提案方式によって，通常のネットワークと比べ (この場合は OpenFlow ネットワーク) ネットワーク内に多少の負荷はかかるものの，関連研究とはほぼスループットに差が見られないことから，認証を適用したネットワークには大きな影響を与えることはないと考えられる．

性能評価としては大きな差異はないものの，提案方式が劣る結果となった．しかし，不正アクセスを防止・検出できるという面では提案方式，関連研究の方式共に同等のレベルである．また，提案方式は OpenFlow を利用しているためその特性から，機器や規格にとらわれず利用できるということ, OpenFlow コントローラによるネットワークの集中管理ができるということがメリットとしてあげられる．よって，今後ホームネットワークの形態の多様化が進んだ際でも対応できるということがいえる．

6. おわりに

本稿では，ホームネットワークの形態の多様化からセキュリティ上の課題として，近年増加傾向が見られる不正アクセスに着目した．その対策として, OpenFlow を用いてホームネットワーク内に動的な認証システムを構築し，不正アクセスによる被害を軽減する手法を提案した．本提案方式では認証時に頻繁に利用される情報を用いることで，ネットワークに接続する端末を制限すると共に，万が一認証が突破された場合でも不正アクセスが検出できるシステムを構築した．また，シミュレーションサーバによる仮想環境を構築し，本提案方式によるネットワークへの影響としてスループットを測定した．測定したスループットを通常の OpenFlow ネットワーク, 関連研究の方式を比較した所. OpenFlow ネットワークとではやや差が現れ, ネットワーク内に認証システムを設置することにより多少の負荷がかかることが判明した. しかし, 関連研究の方式との比較では，大きな差が現れなかったことから，認証を適用したネットワークとして考えるとネットワーク内に大きな負荷を与えることはないと考えられる．また，不正アクセスを防止・検出するという面では提案方式，関連研究の方式共に同等のレベルであることから， OpenFlow を利用した集中管理により，提案方式の方がホームネットワークの形態の多様化に伴うセキュリティの向上に対応できると考えられる．

Vol.2016-DPS-166 No.29
Vol.2016-CSEC-72 No.29
2016/3/4

7. 今後の課題

今後は，性能評価としては端末の登録から認証までの処理時間を計測し，認証によりどの程度遅延が発生するのか定量的な実験を行いたいと考えている．また，セキュリティ面としては提案方式と関連研究の方式共に不正アクセスを防止・検出できるという面では同等レベルであったが，評価として正規アクセスと不正アクセスをどれほど正確に判別できるか定性的な実験を行い，セキュリティの観点からの本提案方式の有用性をあらためて示したい．と考えている．また，OpenFlow のセキュリティ面での課題についても対策を検討していきたい

参考文献

[1] J.-B. Hwang, and J.-W. Han, ”A Security Model for Home Networks with Authority Delegation,” Proceedings of 2006 international conference on Computational Science and Its Applications(ICCSA'06), pp.360-369,2006.
[2] G.W.Kim, D.G.Lee, J.W.Han, S.C.Kim, and S.W. Kim,”Security framework for home network: authentication, authorization, and security policy,”
[3] 日本経済新聞, “東大に不正アクセス、氏名など３万 6000 件流出か”, http://www.nikkei.com/article/DGXLASDG16H3W_W5A710C1000000/ ,2015
[4] CNET Japan, “タミヤのウェブサーバに不正アクセス--最大 10 万件の個人情報流出の可能性”, "http://japan.cnet.com/news/society/35067696/", 2015
[5] ITpro, “2013 年の不正アクセス件数は過去最多、不正送金が 1000 件超に”, http://itpro.nikkeibp.co.jp/article/NEWS/20140328/546848/
[6] G.W.Kim, D.G.Lee, J.W.Han, and S.W.Kim,”Security technologies based on home gateway for making smart home secure,” Proceedings of the 2007 conference on Emerging direction in embedded and ubiquitous computing(EUC'07), pp.124-135, 2007.Proceedings, pp.124-135, 2007.
[7] 吉田剛,“認証情報を利用した不正アクセス検出手法の提案”, 電子情報通信学会総合大会講演論文集 2011 年 通信(2), p.139, 2011.
[8] “Open Network Foundation”, https://www.opennetworking.org/ja/.
[9] Ubuntu, “The world's most popular free OS”, http://www.ubuntu.com/
[10] “Trema”, https://trema.github.io/trema/