Vol.2019-IOT-44 No.48
2019/3/8

OpenFlowを用いた利用者にとって利便性の高い大規模組織向け仮想ネットワーク構成方式の提案

古賀 歩[1,a)]　石橋 勇人[2,b)]

概要：現在の組織内ネットワークは，主に管理上あるいはセキュリティ上の理由によって，いくつかのネットワークに分割して構築される．これは通常 VLAN の形で実現されるが，VLAN 間のアクセスを目的に応じて制限することによってセキュリティを高めたり，1 つのネットワークに接続される機器台数を制限することによって管理を容易にしたりすることができる．しかし，ネットワーク間のアクセス制限の敷居を高くしてしまうと，セキュリティ上は安心であるが，複数のネットワークへの接続を必要とするユーザの利便性が下がってしまう．また，大規模組織においてネットワークの細分化を徹底すると，IEEE 802.1Q に基づく VLAN 技術ではネットワークの数が不足する場合がある．本稿では，SDN(OpenFlow) を用いることによってこういった問題を解決可能なネットワーク構成方式を提案する．

Design of a User-Friendly OpenFlow-based Virtual Network Architecture for Large-Scale Organizations

1. はじめに

現在，大学や企業内で使用されている組織内ネットワークは，ごく小規模の場合を除いて，設置部署やユーザの属性など何らかの要因に基づいて分割された形で設計，運用されている．これは，ネットワークの仕様，管理上の要求，セキュリティ対策など様々な要因から必要とされることである．この際，ネットワークの分割は VLAN 技術によって実現されていることが一般的である．

一方，ネットワークの管理を十分に行う上において，端末の認証はもはや必須の要件であると言って良い．

ところが，現状の主要な方式では，3 章で述べるように，ユーザの利便性を損ねたり，特に大規模組織においては機能が不十分であったりといった問題が発生する．

本稿では，それらの問題に対して SDN 技術 (OpenFlow [1]) を用いた解決手法を提案する．

[1] 大阪市立大学大学院創造都市研究科
Graduate School for Creative Cities, Osaka City University, Osaka 558-8585, Japan
[2] 大阪市立大学大学院工学研究科
Graduate School of Engineering, Osaka City University, Osaka 558-8585, Japan
[a)] ayumukoga@gmail.com
[b)] h-ishibashi@osaka-cu.ac.jp

2. 関連研究

近堂ら [2] は大規模組織内ネットワークを対象とし，利用者からの申請に基づくネットワーク構成管理とスイッチの自動設定を行うネットワーク管理システムの設計と実装を行なった．ネットワークの利用形態が多様化する中で管理システムの自動化は主要な課題である. この研究ではネットワークスイッチに対する設定内容を抽象化することで機種に依存しない制御を行い，利用者からの申請に基づいた設定の自動化を実現している．

また，近堂ら [3] は外部からの不正侵入アクセスによる情報漏洩・データ改ざん等のセキュリティインシデントに対する対策として，キャンパスネットワークの IP アドレスや VLAN 等の資源を一元管理することにより，ネットワークに接続されるホストの把握を行った．さらに，ホストに対するアクセス制限機能をネットワーク側で提供することで，簡易な操作設定でアクセス制限を適用することを可能にした．この研究ではインターネットに公開されるグローバルホストのセキュリティ対策を実装したが，ローカルホストに対するセキュリティ対策を実装してはいなかった．

橋下ら [4] はアプリケーションと連携したネットワーク制御の一つとして，認証基盤と OpenFlow コントローラが

連携してネットワークレベルでのアクセス制御を行う実例を示した．実現した機能としては，正規のアドレスを持たない端末のアクセスを著しく制限すること，ログイン，ログアウトによってネットワークアクセスの不可避を制御することの二点であり，これによって単体のネットワークについてアクセス制御は実現した．

浜元ら [5] が提案したネットワークは，幹線機器の高速化，冗長化を施した安定で高速なネットワークである．このネットワークの導入により，接続機器の管理者が明確となり，セキュリティインシデント時の機器特定も容易にした．また，動的 VLAN を利用することにより，場所単位から，人単位でのサブネット構成へと管理を変更した．サブネットはユーザの性質毎に分離され，適切なアクセス制御を行うことでネットワークの安全性を向上させている．

3. 提案方式

3.1 現状の問題点

3.1.1 ネットワーク分割の得失

冒頭で述べたように，大学や企業の組織内ネットワークは，通常幾つもの部分に分割されている．ネットワークを分割することによってトラフィックをネットワーク的に分離し，アクセス制御することで，セキュリティレベルを高めることができるという利点がある．具体的には，人事，財務，研究開発といった部門毎にネットワークを分離し，関係のない部門へのアクセスを禁止するようなケースである．

このように業務やサービスに対応してネットワークが分離されている場合，1 人の人が複数の業務に関わろうとすると，業務によってネットワークを使い分ける必要が出てくる．このためには，

(1) それぞれのネットワークに接続された複数の端末を用意し，使い分ける
(2) 1 台の PC に複数のネットワークインターフェースを装備し，複数のネットワークに接続する
(3) (ユーザを認証する際の ID によって接続先のネットワークを切り替えている場合[*1]) 業務によって ID を使い分けてログインし直す
(4) 何らかの遠隔アクセス手段 (VPN，リモートデスクトップ等) を用いる

などの方法が考えられる．

(1)，(2) はハードウェアの増設を必要とするため，コスト面で不利である．また，特にノート PC では実現が困難なことも多い．(3) は追加のハードウェアは不要であるが，毎回ログインの操作を伴うことがユーザの利便性を損なう．(4) は追加のサーバ等を要し，コスト的にも利便性的にもデメリットがある．

また，ネットワークを分離することには，別の利点もある．端末がマルウェアに感染したり侵入を受けた場合に，同一のネットワーク内への攻撃はより容易であるため，その範囲を絞っておく方が有利である．さらに，攻撃を受けた端末の周辺部分をネットワーク単位で切り離すなど，その後の対応を柔軟に行うことができる．

この際，特に大学においては研究室やプロジェクト単位で活動が行われるため，それぞれを分離しようとすると非常に多数のネットワークを作成する必要がある．しかし，通常ネットワークを分離するために使用されている IEEE 802.1Q ベースの VLAN 技術では，最大でも 4094 個のネットワークにしか分割することができないため，大規模な組織ではネットワーク数が不足するという問題がある．

3.1.2 ネットワーク認証時の問題

ネットワークに参加する際の認証には，captive portal による Web 認証，IEEE 802.1X による認証，MAC アドレスによる機器単位の認証など，いくつかの方法が用いられる．1 つの認証方式に頼らず様々な認証方式を用いることで，サーバや IoT デバイスなど対話的な認証が適さない機器にも対応できる．

ユーザに対するわかりやすさの点では，Web 認証が有利である．現在一般に使用されている Web 認証方式では，ユーザの端末がネットワークに参加した際に，まず認証前 VLAN というアクセスコントロールの厳しいネットワークに所属させる．次にユーザが認証を行い，認証が成功すると，ID に基づいて適切な VLAN に所属させる．この際，認証前後の VLAN の切り替えにともなって IP アドレスの変更が必要となるため，IP アドレスの再配布を行なっており，このための時間が 1~2 分程度必要となることが利用者の利便性を損ねている．

IEEE 802.1X による認証では IP アドレスの再配布を伴わないためにこの問題は生じないが，一般に認証情報を保存して使用するため，ID の切替には手間がかかる．

3.2 提案システムの方針

提案システムの設計方針は次の 3 つである．

(1) 複数のネットワークへの同時アクセス
業務ごとに異なる複数のネットワークに対し，認証のやり直しを伴わない方式を実現する．これは，SDN 技術によるパケットヘッダの IP アドレス書き換えによって行う．

[*1] いわゆるユーザベースの動的 VLAN

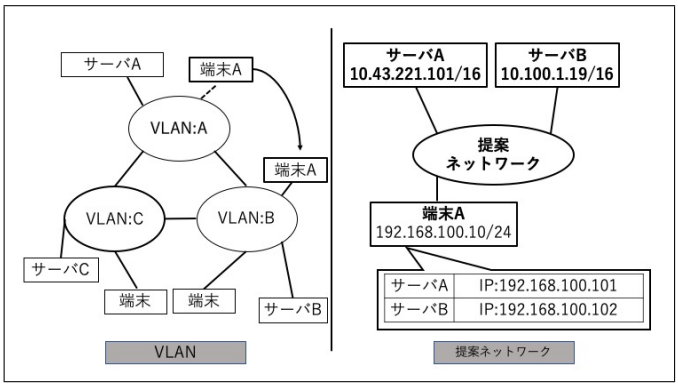

図 1　提案手法と VLAN の違い

図 1 のように，VLAN 技術を用いたネットワークでは，自己 (端末 A) の所属する VLAN(VLAN: A) の外 (VLAN: B) に利用したいサービスがある場合，所属する VLAN を切り替える必要があった (ここでは，セキュリティ上の理由によって VLAN A から B へはアクセスできないものとする)．

提案手法ではシステムがパケットのヘッダフィールドの情報を書き換えることで，端末の LAN の中にユーザが必要なすべてのサーバが存在しているように見せかける．このため，利用するサーバ (サービス) によって VLAN を使い分ける必要はない．

(2) 大規模組織への対応

上で述べたように，SDN 技術を用いた新たな方式で仮想ネットワークを構成することにより，4094 個の制限を受けない仮想ネットワークを提供する．

(3) 認証を伴うネットワーク接続に要する時間の短縮

端末の持つ IP アドレスを認証前後で付け替え不要とし，認証後は SDN スイッチにおいて IP アドレスを書き換えることで IP アドレスの再配布に要する時間を不要とする．

3.3　提案ネットワークの概要

図 2 は提案ネットワークの概要図である．

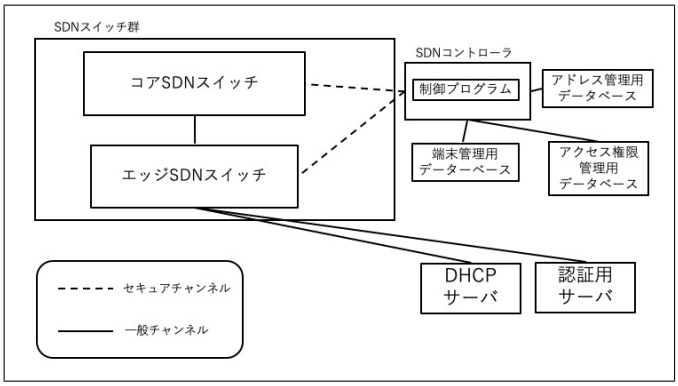

図 2　提案ネットワーク

ここで，端末の接続される SDN スイッチをエッジ SDN スイッチ，エッジ SDN スイッチ間を接続する SDN スイッチをコア SDN スイッチと呼ぶことにする．今回の提案方式では，必要な制御をすべてエッジ SDN スイッチにおいて実現しており，コア SDN スイッチはフレームの転送のみを行っている．したがって，コアの部分は必ずしも SDN スイッチである必要はない．

端末がエッジ SDN スイッチに接続されると，提案システムはその端末に対して IP アドレスを配布する．認証前の端末は認証サーバとのみ通信可能である．

端末が認証に成功すると，提案システムは “ユーザの持つ認証後の全ての端末” と “ユーザがアクセス可能なサーバ” で構成される仮想的な LAN を作成する．この際，VLAN タグは用いずにエッジ SDN スイッチでパケットのヘッダフィールドを書き換えることによって，これを実現する．

提案システムが提供するユーザごとに作成される仮想的な LAN を，以下では **vNet**(virtual Net) と呼ぶことにする．この vNet では，既存の VLAN 技術とは異なり，サーバから端末に向けて送信されるパケットのヘッダフィールドを SDN スイッチで書き換えることによってユーザの端末と同じ LAN にサーバが存在しているように見せかけている (図 3)．また，サーバ側ではサーバと同じ LAN に端末がいるように見えている (図 4)．

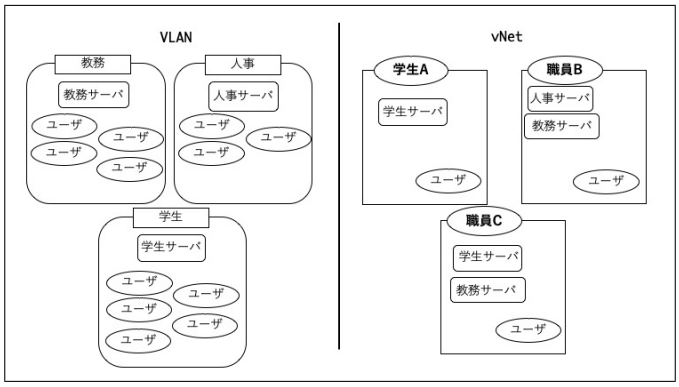

図 3　vNet と VLAN の違い

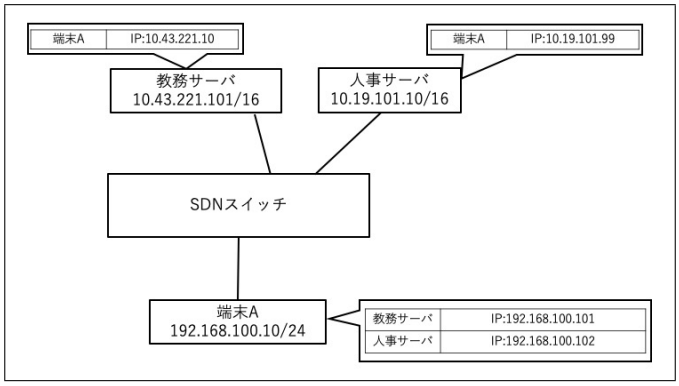

図 4　vNet の動作例

3.4 提案ネットワークの設計

提案システムは端末管理用データベース，アドレス管理用データベース，アクセス権限管理用データベースを持つ．

システムは起動時に物理的なネットワークのトポロジを認識し，データとして持つ．

端末 A がネットワークに接続した際のシステムの処理は次のようになる．端末 A が情報コンセントに接続しネットワークへ参加すると、提案システムは DHCP サーバから IP アドレスを配布する．提案システムは端末管理用データベースに新たな端末を追加し，認証前に取得可能な情報を取得してその情報を書き込むとともに，認証状態を未認証としておく．未認証端末は認証サーバへのアクセスのみを許可するように制御する．端末が認証に成功した場合は，端末管理用データベースに登録されている情報にユーザ ID と論理アドレスの情報を追加し，認証状態を認証済みに変更する．

本システムでは，端末に配布される IP アドレスおよびサブネットマスクは全て同一である．エッジ SDN スイッチにおいてパケットの送信元 IP アドレスを変更するため，コアネットワーク部分ではそれぞれが異なる論理 IP アドレスを持っており，物理 IP アドレスが同一であっても問題ない．認証前の状態では DHCP サーバと認証サーバのみにアクセスできるように制御する．

提案システムは認証後にユーザの持つ端末同士とアクセス可能なサーバとの通信する可能にするために，ブロードキャストパケットとユニキャストパケットを同じユーザ持つ端末とサーバに到達するように制御する必要がある．

3.5 管理データベース

提案システムは端末管理用のデータベース，アドレス管理用データベース，アクセス権限管理用データベースの 3 つを持つ．端末管理用データベースは端末の MAC アドレス，ユーザ ID，接続しているエッジのスイッチの ID，接続しているポート番号，認証状態，認証後に変換される IP アドレス (以下，論理アドレス) を保持する．アドレス管理用データベースは，ユーザごとに用意する．このデータベースには，vNet 内の各端末から見えている他の端末やサーバの IP アドレスと論理アドレスの組合せを保持している．アクセス権限管理用データベースはサーバ毎にアクセス可能なユーザの一覧を登録する．

3.6 認証前の制御

認証前の端末に対して必要以上の権限を与えることはセキュリティ上好ましくない．そのため，認証前の端末は認証だけを可能としておく．具体的には

- DHCP サーバからの IP アドレスの受領
- 認証サーバへのアクセス

の 2 点のみを可能とするように制御を行う．

3.6.1 DHCP サーバとの通信

端末が DHCP サーバとの通信を行えるよう制御するために，端末から発信されたパケットのプロトコルを判定し，DHCP に関連するものであった場合はパケットをコア SDN スイッチ側のポートに出力する．

本システムではユーザの端末に配布される IP アドレスのサブネットマスクを/24 に設定しているが，これは 1 人のユーザが使用する端末やサーバ等を収容するに十分な大きさであり，かつ，必要な数の仮想ネットワークが用意できるように自由に定めて良い．ただし，サーバについてはより広いサブネットマスクを設定する．これはサーバであれ端末であれ，全ての端末が同じ LAN にいるように見えるように設計しているため，端末と違い同じ LAN の中にいる端末の数が多いサーバでは，端末と同じサブネットマスクでは対応しきれない可能性があるためである．

3.6.2 認証サーバへのアクセス

未認証端末が他端末へのアクセスを試みた場合，エッジの SDN スイッチでパケットを他端末へ到達しないように，システムがデータベースに登録されている端末の MAC アドレスから認証状態を確認し，未認証端末であった場合パケットを破棄するように制御する．

3.6.3 認証機能

本システムでは，端末の接続時に原則としてユーザ ID を用いた認証を行う．認証に成功すると，端末管理用データベースの，対応する MAC アドレスをキーとして持つレコードに，ユーザ ID と認証後に変換される IP アドレスを追加し，認証状態を認証済みする．認証後に変換される IP アドレスは，割り当て済みの IP アドレスとは重複しないアドレスを選択して割り当てる．このアドレスは，実際に端末に配布されている IP アドレスとは異なるサブネットの IP アドレスとする．

3.7 認証後の制御

認証後の端末に対して許可するのは，同じユーザの端末同士の通信と認められたサーバへのアクセスである．よって認証後は

- 端末同士のユニキャストパケットの制御
- ブロードキャストパケットの制御
- 端末とサーバのユニキャストパケットの制御

この 3 点の制御が必要である．

3.7.1 端末同士のユニキャストパケットの制御

同じユーザの端末同士は通信を可能にする．ここで同じユーザの持つ端末を端末 A，端末 B とする．両方の端末の認証が終わり，ARP による MAC アドレスの解決を終えた後にユニキャストで通信を行う際は次のような流れになる (図 5).

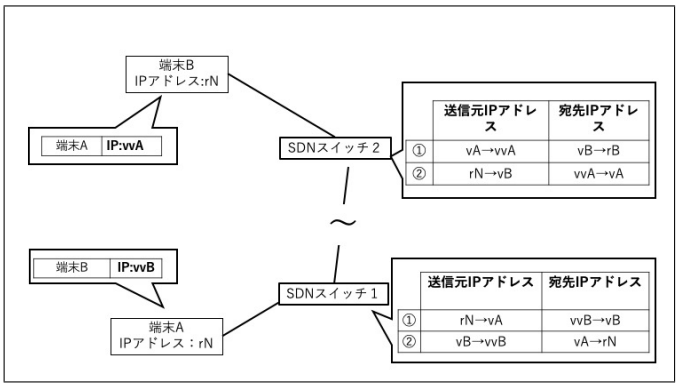

図 5 端末同士の通信におけるアドレス変換

端末 A に配布されている IP アドレスを rA，端末 A の論理アドレスを vA，端末 A から見えている端末 B の IP アドレスを vvB，端末 B の IP アドレスを rB，端末 B の論理アドレスを vB，端末 B から見えている端末 A の IP アドレスを vvA とする．ただし，端末 A と端末 B に配布れている IP アドレスは仕様上同じなので両端末の IP アドレスを rN とする．

端末 A から出たパケットは SDN スイッチ 1 の①のルールに基づき，送信元 IP アドレス (rN) は端末 A の論理アドレス (vA) に変換される．また宛先 IP アドレス (vvB) は端末 B の論理アドレス (vB) に変換し，コア SDN スイッチが接続されているポートへ出力する．その後，パケットはコア SDN スイッチでルーティングされ，端末 B のエッジの SDN スイッチである SDN スイッチ 2 に到達する．SDN スイッチ 2 は宛先 IP アドレスを端末 B の実際の IP アドレス (rN) に変換する．また，送信元 IP アドレス (vA) は端末 B における端末 A の IP アドレス (vvA) に変換される．その後，パケットを端末 B が接続されているポートに出力する．端末 B から端末 A に向かうパケットについても SDN スイッチ 1，2 で同様の処理を行うことにより，実際に同じ IP アドレスが配布されていてもスイッチで適宜書き換えることにより，通信を可能とする．同じユーザの端末でなかった場合のユニキャストパケットはエッジの SDN スイッチで破棄するように設定することにより，到達しないように制御する．

3.7.2 端末のブロードキャストパケットの制御

ブロードキャストパケットは同じユーザの端末にのみ到達するように制御を行う (図 6).

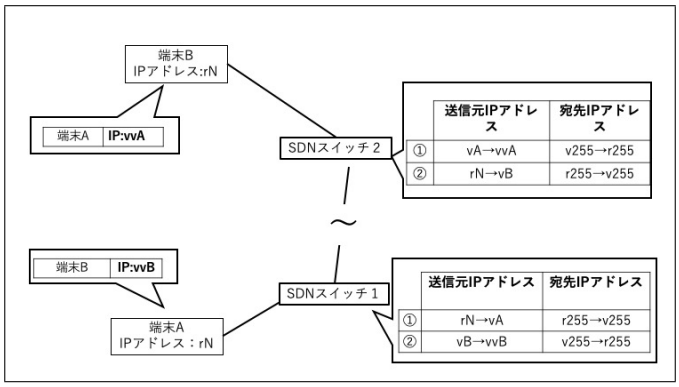

図 6 ブロードキャストパケットのアドレス変換

ブローキャストパケットを同じユーザの端末のみに到達させるために，ブロードキャストパケットの送信元 MAC アドレスを用いる．また，ブロードキャストパケットはコアの SDN スイッチでフラッディングするように設定する．端末 A から発信されたブロードキャストパケットは SDN スイッチ 1 の①のルールに基づきパケットの中身を書き換える．その後，コア SDN スイッチでフラッディングされ，端末 B のエッジ SDN スイッチ 2 にブロードキャストパケットが到達する．この時，SDN スイッチ 2 はシステムにブロードキャストパケットを出した端末のユーザと同じユーザの端末が自己のポートに接続されているかを問い合わせる．同じユーザの持つ端末が存在すれば SDN スイッチ 2 の①に基づきパケットを書き換え，端末 B が接続されているポートにパケットを出力する．同じユーザの端末が存在しない場合はパケットを破棄する．以上の制御によりブロードキャストパケットは同じユーザの端末にのみ到達するように制御可能である．

3.7.3 端末対サーバの通信制御

認証後，特定のサーバへアクセスを行おうとした場合，以下のような手順でサーバと通信する (図 7).

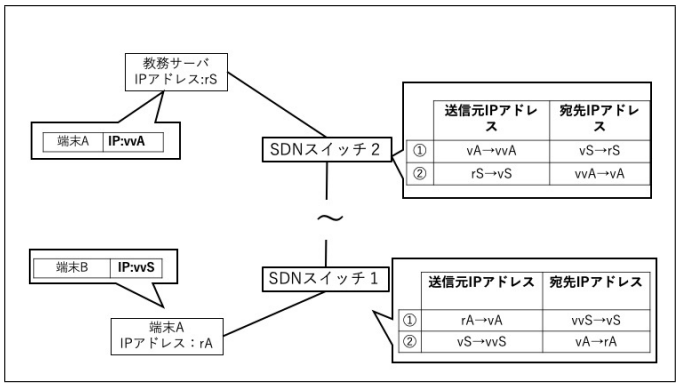

図 7 対サーバのアドレス変換

端末 A に配布されている IP アドレスを rA，端末 A の論理アドレスを vA，端末 A から見えている教務サーバの IP アドレスを vvS，教務サーバの IP アドレスを rS，教務

サーバの論理アドレスを vS，教務サーバから見えている端末 A の IP アドレスを vvA とする．端末とサーバの通信はエッジの SDN でパケットのヘッダフィールドの値を適宜書き換えることによる通信を実現する．端末 A から教務サーバに向けて出たパケットの送信元 IP アドレスは rA，宛先 IP アドレスは vvS となっている．SDN スイッチ 1 で①のルールに基づき変換される．その後，SDN スイッチ 2 の①のルールに基づき、ヘッダフィールドが変換し，教務サーバにパケットが到達する．教務サーバから端末 A に向かうパケットは，それぞれの SDN スイッチの②のルールに基づきパケットのヘッダフィールドの値を変換する．これにより，サーバ，端末はそれぞれの LAN 内に，通信相手が存在しているように見える．この際に使用する IP アドレスの変換ルールは提案システムが管理する．

4. 実装

提案システムは OpenFlow 1.3 に基づいており，OpenFlow 構築フレームワークである Ryu [6] 4.28 を用いて Python 言語で実装している．

システムの構成は図 8 の通りである．ここで，DHCP サーバはコントローラの機能として実装しており，必要なデータベースもコントローラ内部に持っている．

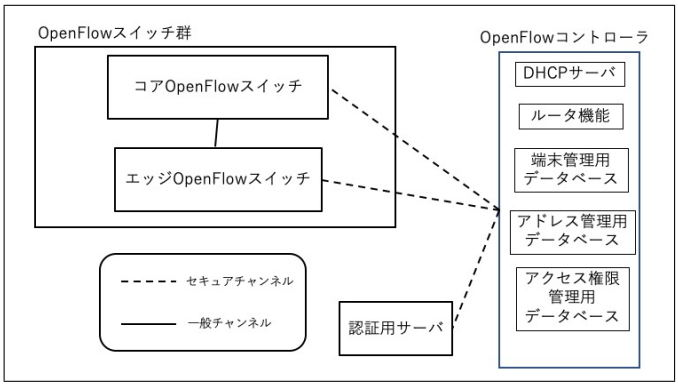

図 8 提案ネットワークの実装

試作システムは Mininet [7] 上に実現しており，基本的な機能についての動作を確認した．

5. おわりに

今後の課題として本論文ではエッジ OpenFlow スイッチに書き込まれるフローエントリの数を充分に検討できていない．よって現在の提案システムでスイッチのスケーラビリティに対応可能かを検証する必要がある．また認証前の状態で WindowsUpdate などの OS のアップデートだけを可能にするような制御を実現することで端末のセキュリティを向上できると考えられる．

参考文献

[1] Mckeown, N.: OpenFlow: Enabling innovation in campus networks, *SIGCOMM Computer Communication Review*, Vol. 38, pp. 69–74 (2008).
[2] 近堂 徹，田島浩一，岸場清悟，岩田則和，相原玲二：自動構成機能を有する大規模キャンパスネットワーク管理システムの実装と評価，情報処理学会論文誌，Vol. 57, No. 3, pp. 998–1007 (2016).
[3] 近堂 徹，田島浩一，吉田朋彦，岸場清悟，岩田則和，西村浩二，相原玲二：アクセス制限機能を提供するキャンパスネットワークの実装と評価，学術情報処理研究，Vol. 21, No. 1, pp. 36–43 (2017).
[4] 橋本直樹，園生 遥，牛込翔平，菊田 宏，永園 弘，廣津登志夫，新村正明：OpenFlow による認証基盤と連携したネットワークアクセス制御の実現 (技術と社会・倫理)，電子情報通信学会技術研究報告， Vol. 113, No. 442, pp. 133–138 (2014).
[5] 浜元信州，井田寿朗，齋藤貴英，酒井秀晃，小田切貴志，横山重俊：動的 VLAN を利用した全学認証ネットワークの構築，学術情報処理研究，Vol. 20, No. 1, pp. 65–74 (2016).
[6] Ryu SDN Framework Community: Ryu SDN Framework, (online), available from ⟨https://osrg.github.io/ryu/⟩ (accessed 2019-01-31).
[7] Mininet Team: Mininet, Octopress (online), available from ⟨http://mininet.org⟩ (accessed 2019-01-31).