Vol.2016-IOT-32 No.39
2016/3/4

NAT環境に対応した DNS・SDN連携型動的ファイアウォールシステム

藤巻 伶緒[1,a)]　大塚 友和[2,b)]　山井 成良[3,c)]　北川 直哉[3,d)]　岡山 聖彦[4,e)]

概要：近年，組織外ネットワークから組織内ホストへ不正アクセスが後を絶たず，その対策は急務である．対策の一つとしてファイアウォール製品が広く用いられているが，線密な検査を行うと負荷が高くなり，スループットの低下を招く．これを回避するためには，管理者が信頼できる通信相手とそれ以外の相手を手動で設定する必要がある．我々はこれまでに，問い合わせ元のクライアントに応じて，動的にファイアウォールの検査内容を決定するシステムを提案した．この手法は，通信の殆どが，事前に DNS による名前解決を行う点に着目し，DNS キャッシュサーバにクライアントの IP アドレスを通知する機構を組み込むことで実現した．しかし，NAT ルータを用いた環境では，クライアントの IP アドレスがグローバル IP アドレスに変換されて通信を行った場合，検査内容の決定が不可能になるという問題があった．本論文では，DNS キャッシュサーバから通知されるクライアントの IP アドレスを，変換後のグローバル IP アドレスに書換える機能を実装することで，NAT ルータを用いた環境に対応する手法について述べる．

Proactive firewall system in cooperation with DNS and SDN applicable to NAT environment

Reo Fujimaki[1,a)]　Tomokazu Otsuka[2,b)]　Nariyoshi Yamai[3,c)]　Naoya Kitagawa[3,d)]
Kiyohiko Okayama[4,e)]

Abstract: Recent years, unauthorized accesses from the external network to the internal host are sharply increasing. Although many firewall products are widely utilized as one of the countermeasures, its throughput decreases when it perform detailed inspection of packets. In order to prevent this problem, administrator must configure manually whether the communication partner is reliable or not. In the past, we have proposed a system for determining the dynamic examination content in accordance with the inquiring client. This method focused on the point that the most kinds of communication performs a name resolution using DNS in advance, and this system has achieved by notifying the client IPaddress to the DNS cache server. However, this system cannot determine the inspection content when a client IPaddress is converted into a global IP address. In this paper, we describe about a system that corresponds to the environment using a NAT router by using the function of rewriting from the client IPaddress to the converted global IPaddress.

1. はじめに

近年，組織外ネットワークから組織内ホストへ不正アクセスが後を絶たず，その対策が急務となっている．不正アクセスの一般的な対策として，ファイアウォール装置を導入し，組織の対外接続点での通信を検査する方法が広く利

1 東京農工大学工学部情報工学科
Department of Computer and Information Sciences, Tokyo University of Agriculture and Technology
2 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
3 東京農工大学大学院工学研究院
Institute of Engineering, Tokyo University of Agriculture and Technology
4 岡山大学大学情報統括センター
Center for Information Technology and anagement, Okayama University
a) reo@net.cs.tuat.ac.jp
b) otsuka.net@s.okayama-u.ac.jp
c) nyamai@cc.tuat.ac.jp
d) nakit@cc.tuat.ac.jp
e) okayama@cc.okayama-u.ac.jp

用されている．ファイアウォールにおいて，大量の不正アクセスやウィルスの検査をまとめて行うような運用を行う場合，機器に大きな負荷がかかり，スループットの低下を招く．その運用に耐えうるような機器は非常に高価であり，導入が難しい場合が多い．この問題を回避するため，監視対象となる通信を限定したり，負荷の高い検査を行わないようにしたりするなどの設定を行う必要がある．しかし，このような構成のほとんどは管理者が手動で行わなければならないため，管理者の負担が大きくなるという問題がある．

この問題に対して，本研究グループはこれまでに，ファイアウォールが送信元ホスト（以降，クライアントとする）と送信先ホスト（以降，サーバとする）を通信が行われる前に把握して，検査内容を動的に決定するシステムを提案した [1]．一般的に，あらゆる通信が行われる前に，予め DNS[2][3] による名前解決が行われる点に着目し，クライアント側 DNS サーバ（以降，DNS キャッシュサーバとする）がクライアントの IP アドレスをサーバ側 DNS サーバ（以降，DNS コンテンツサーバとする）に通知する機構を組み込む．この機構によって，DNS コンテンツサーバがクライアントの IP アドレスとサーバの IP アドレスを事前に把握することができる．このシステムでは，一般的に SDN[4] の代表的な技術である OpenFlow[5] を用いて，事前に把握したクライアントとサーバに基づき，パケットの転送先を動的に決定するシステムを提案している [6]．

この手法では，たとえば送信元が信頼できる場合には，ファイアウォールを迂回させたり，負荷の高い検査を行わないようにする．一方，通信相手が信頼できない場合には通信帯域を制限したり，負荷の高い厳しい検査を行ったりする．また，ボットを発信源とする通信に多く見られるような，事前に名前解決を行わない通信については，不審なアクセスとみなして厳しい検査を行ったり，遮断したりすることが可能である．この仕組みにより，信頼できる通信と疑わしい通信を分離し，信頼できる通信の高速化と，管理者の負担軽減を図ることができる．

しかしこれらの手法では，クライアント側で NAT[7] によって，送信元 IP アドレスが変換されて通信を行った場合，DNS キャッシュサーバから通知された送信元 IP アドレスはプライベート IP アドレスのため，これに基づいて検査内容を動的に決定することができなくなるという問題がある．この問題を解決するために，DNS キャッシュサーバで通知される送信元のプライベート IP アドレスを，NAT により変換可能なグローバル IP アドレスに書換える機構を NAT ルータに組み込む必要がある．そこで本稿では，DNS キャッシュサーバから通知されるクライアントのプライベート IP アドレスを，変換後のグローバル IP アドレスに書換える機能の設計と実装および動作確認を行う．これにより，クライアント側で NAT ルータを利用した環境に対応した，DNS と SDN の連携による動的ファイアウォールシステムを提案する．

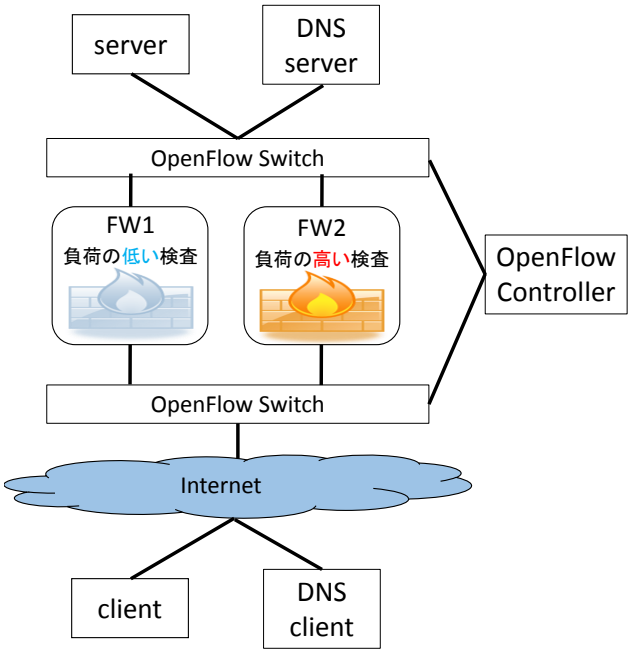

図 1　システム全体の構成例
Fig. 1　An example of the system structure

2. 動的ファイアウォールシステム

我々の研究グループはこれまでに，DNS キャッシュサーバにクライアントの IP アドレスを DNS コンテンツサーバに通知する機能を組み込むことにより，クライアント・サーバ間の通信に利用する IP アドレスを事前に把握して，ファイアウォールの検査内容を動的に変更するシステムを提案した．このシステム全体の構成を図 1 に示す．このシステムでは，スイッチで通信の動的な振り分けを行うために OpenFlow 技術を導入し，DNS コンテンツサーバ，OpenFlow スイッチおよびファイアウォールの相互連携による効率的な不正アクセス防止システムを実現している．なお，この図において，FW1 は信頼できる相手との通信用で負荷の高い検査を省略したファイアウォールであり，FW2 はそれ以外の相手と通信するときに用いられるファイアウォールを表す．

このシステムを実現するため，本研究グループでは，まず DNS キャッシュサーバにクライアントの IP アドレスを通知する機能を用いた [10]．通知方法として，EDNS0[8] のクライアントサブネットオプション [9] を利用している．なお，DNS キャッシュサーバではセキュリティ対策のため，通知するクライアントの IP アドレスをサーバの IP アドレスを管理する DNS コンテンツサーバにのみ通知する機能が必要になる．また，DNS のキャッシュ機能により IP アドレスの通知が行われない場合が生じるため，キャッシュ

を一部無効化機能が必要である．このため，DNS キャッシュサーバの実装である BIND とは別に，上述した 2 つの機能を実現するプログラム（以降，新規 DNS キャッシュサーバ）を DNS キャッシュサーバとして実装している．新規 DNS キャッシュサーバは，BIND に付属してある問い合わせ用プログラムである dig を用いて，問い合わせメッセージにクライアントサブネットオプションを付加して通知を行うものである．

2.1 従来システムの問題点

動的ファイアウォールシステムでは，組織内のネットワークに対して通信を行うネットワークが NAT ルータを利用していた場合，DNS キャッシュサーバで通知する問い合わせ元 IP アドレスは，内部用（プライベート）IP アドレスとなる．そのため，OpenFlow コントローラは内部用（プライベート）IP アドレスを取得するため，クライアントが外部側（グローバル）IP アドレスを利用して通信を行った場合，OpenFlow スイッチは信頼できる相手からの通信であるにもかかわらず，これらのアドレスを持つホストが同一ホストであることを判断することができないため，負荷の高い検査を行うファイアウォールに振り分けてしまうという問題がある．

2.2 解決策の検討

2.1 節で述べた問題点への解決策として，DNS キャッシュサーバで通知するクライアントの IP アドレスを，NAT ルータで変換される IP アドレスに変更する方法が考えられる．この方法は，2 節で述べたように，新規 DNS キャッシュサーバで実行する dig プログラムのクライアントサブネットオプションに，変換後の IP アドレスを指定することで実現できる．これは，新規の DNS キャッシュサーバのプログラムを 1 行変更するだけでよく，容易に実現可能である．なお，問い合わせメッセージに付加できる IP アドレスは 1 種類である．ゆえに，変換後の IP アドレスが 2 種類以上ある場合には，通知された IP アドレスと同じ IP アドレスを用いてクライアント・サーバ間の通信を行うことができない．この問題に対して，新規 DNS キャッシュサーバに，クライアントの IP アドレスとその変換後の IP アドレスを管理しておき，その対応関係に基づいて通知する送信元 IP アドレスを変更する方法が考えられる．しかし，NAT ルータの設定が変更された場合，新規 DNS キャッシュサーバで管理する IP アドレスを更新する必要があり，管理者の負担が大きくなるという問題がある．

もう一つの解決策として，NAT ルータ上で DNS キャッシュサーバから通知される送信元 IP アドレスを，変換後の IP アドレスに変更する方法が考えられる．これは，問い合わせメッセージに付加された IP アドレスを，NAT ルータ自身が予め設定した変換後の IP アドレスに書換える．その後，クライアント・サーバ間でも同じ IP アドレスを用いて通信を行うように NAT ルータで変換する．これにより，変換後の IP アドレスが 2 種類以上ある場合にも対応できる．また，NAT ルータの設定を変更しても対応できる．

本研究では，NAT ルータに問い合わせメッセージに含まれるクライアントの IP アドレスを書換える機能を組み込むこととした．

3. 動的ファイアウォールシステムにおける NAT ルータ

3.1 NAT ルータの設計

本システムでは，クライアント側に NAT 機能を併用することを想定している．そこで本研究では，NAT ルータに DNS キャッシュサーバの問い合わせメッセージに含まれるクライアントサブネットオプションを書換える機能を組み込む．なお，この機能はシステムの保守性を高めるため，既存の NAT 機能とは別に実装する必要がある．

3.2 NAT ルータの実装

NAT ルータは，DNS 問い合わせメッセージに含まれるクライアントサブネットオプションを書換えるとともに，その送信元 IP アドレスを外部側（グローバル）IP アドレスに変換する処理を行う．既存の NAT 機能によるアドレス変換とは別に，クライアントサブネットオプションを書換えるプログラムを処理させる機能が必要である．このことから本研究では，FreeBSD 10.2-RELEASE を採用し，FreeBSD の ipfw(8) と divert(4) を利用する．これは ipfw(8) のルールを設定することで，特定の条件のパケットをプログラムに迂回させることができる．また NAT 機能には，FreeBSD の natd(8) を利用した．

3.3 NAT の設定

本研究では，簡単化のため NAT ルータによって変換される IP アドレスが 2 種類あると想定した実装を行う．このため，外部用インターフェース (msk0) の NIC(Network Interface Card) に 2 つの IP アドレスを持たせる．NAT の設定を図 2 に示す．この図のように，/etc/natd.conf という natd(8) の設定ファイルに内部 IP アドレスと外部 IP アドレス 2 つの組を設定する．たとえばこの図において，client1 の内部 IP アドレス（192.168.a.2）は外部 IP アドレス (165.93.b.c) にアドレス変換される．

3.4 NAT ルータのシステム構成

システム構成例を図 3 に示す．NAT ルータの構築にあたり，以下のように ipfw(8) のルールを設定した．

以下のルールにより，宛先 TCP/UDP ポート 53 番の内部用インターフェース (re0) を通るパケットは，DNS の問い合わせメッセージと判断され，クライアントサブネット

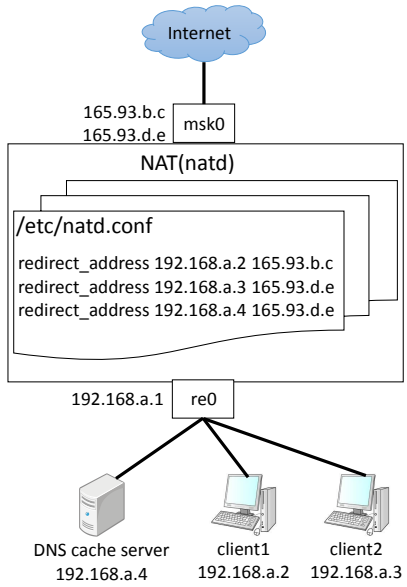

図 2　NAT の設定例
Fig. 2　A configration example of NAT

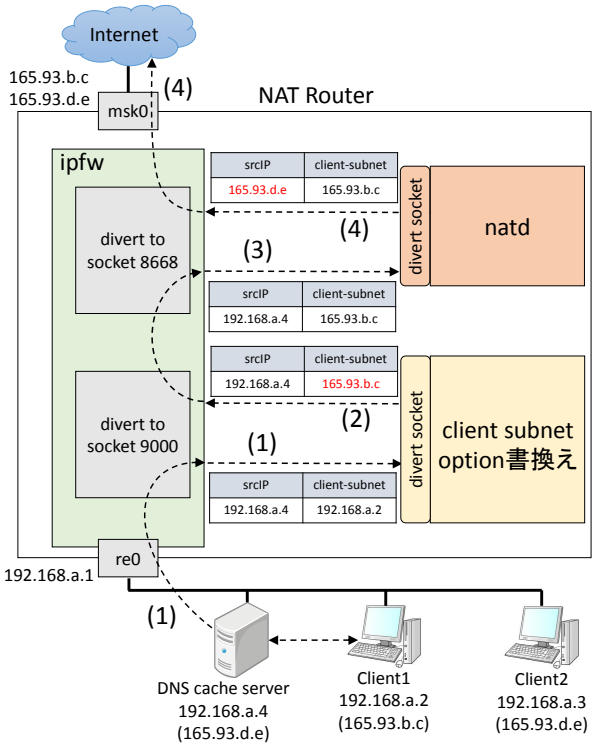

図 3　システムの構成例
Fig. 3　A configuration example of the system

オプションを書換えるプログラムに迂回する．

```
00060 divert 9000 ip from any to any dst-port 53 via re0
```

また以下のルールにより，外部用インターフェース（msk0）を通るパケットは，アドレス変換を行う natd(8) に迂回する．

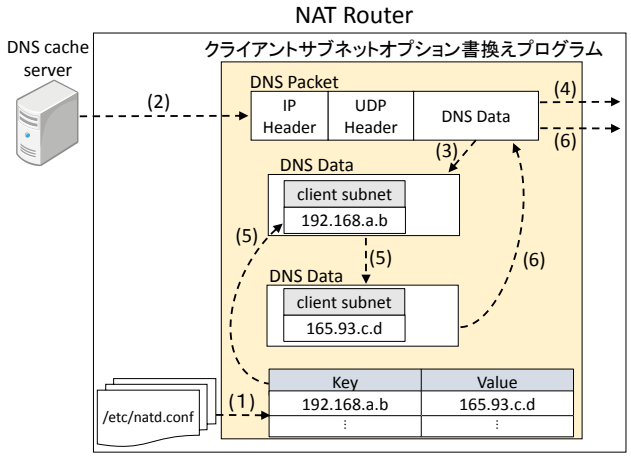

図 4　クライアントサブネットオプション書換え機能の動作
Fig. 4　Behavior of the client subnet option rewriting function

```
00050 divert 8668 ip4 from any to any via msk0
```

例として，NAT ルータがクライアントサブネットオプションを含むパケットを DNS キャッシュサーバから受信した場合の動作を図 3 に示す．以下の番号は図 3 中の番号に対応している．

(1) NAT ルータは DNS キャッシュサーバの問い合わせパケットを受信し，ipfw(8) のルールに従い，クライアントサブネットオプションの書換えを行うプログラムにパケットを送る．
(2) クライアントサブネットオプションを書換えたパケットを IP パケットのストリームに再注入する．
(3) ipfw(8) のルールに従い，ネットワーク変換デーモンである natd(8) にパケットを送る．
(4) パケットの送信元 IP アドレスのアドレス変換を行ったパケットをインターネットに送出する．

3.5　クライアントサブネットオプション書換え機能

クライアントサブネットオプション書換え機能の動作例を図 4 に示す．クライアントサブネットオプション書換え機能の実現には，CPAN の Perl モジュール Net::Divert[11] を利用した．このモジュールは，ipfw(8) のルールに設定したポート番号とソケット通信を行うためのものである．また，DNS の問い合わせメッセージに含まれるクライアントサブネットオプションの書換えには，CPAN の Perl モジュール Net::DNS::Packet[12] を利用した．以下に，クライアントサブネットオプション書換え機能の動作例を示す．なお，以下の番号は図 4 中の番号と対応している．

(1) クライアントサブネットオプションの書換えを行うプログラムを起動する．その後，natd(8) の設定ファイルを読み込む．読み込んだファイルから内部 IP アドレスと外部 IP アドレスを取出し，内部 IP アドレスをキーに，外部 IP アドレスを値とした連想配列を作成

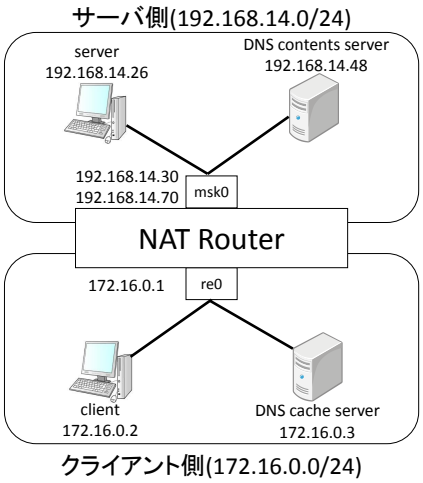

図 5　実験環境
Fig. 5　Experiment environment

する．
(2) NAT ルータは，DNS の問い合わせパケットを受信する．ipfw(8) のルールにより，プログラムはそのパケットを取得する．
(3) パケットから DNS データを抽出する．
(4) 抽出したデータにクライアントサブネットオプションが付加されているか確認し，含まれていなければ，取得したパケットをそのまま送出する．付加されていれば (5) に進む．
(5) (2) で作成した連想配列を利用して，クライアントサブネットオプションを書換える．
(6) クライアントサブネットオプションを書換えた DNS データを書き戻して，パケットを送出する．

4. 動作確認実験

実験方法として，クライアントの Web ブラウザでサーバのドメイン名を入力する．その後，DNS キャッシュサーバはクライアントサブネットオプションを付加した問い合わせを DNS コンテンツサーバに行う．

4.1 実験環境

本研究のために構築した実験環境を図 5 に示す．図中において，クライアント側 (172.16.0.0/24) をローカルネットワークと想定し，サーバ側 (192.168.14.0/24) をグローバルネットワークと想定する．また，クライアント (172.16.0.2) からの通信はグローバル IP アドレス (192.168.14.30) に変換され, DNS キャッシュサーバ (172.16.0.3) からの通信はグローバル IP アドレス (192.168.14.70) にアドレス変換する設定をしている．DNS コンテンツサーバ (192.168.14.48) はサーバ (192.168.14.26) のゾーン情報を管理し，DNS キャッシュサーバからの問い合わせに対して応答する．

```
query 26126 : www.reo.net.cs.tuat.ac.jp IN A
Received query from 192.168.14.70 to 192.168.14.48
;; HEADER SECTION
;; id = 26126
;; qr = 0 aa = 0 tc = 0 rd = 1 opcode = QUERY
;; ra = 0 z = 0 ad = 1 cd = 0 rcode = NOERROR
;; qdcount = 1 ancount = 0 nscount = 0 arcount = 1
;; do = 0
;; EDNS version 0
;; flags: 0000
;; rcode: NOERROR
;; size: 4096
;; option: CLIENT-SUBNET 00012000ac100002

;; QUESTION SECTION (1 record)
;; www.reo.net.cs.tuat.ac.jp. IN A

;; ANSWER SECTION (0 records)

;; AUTHORITY SECTION (0 records)

;; ADDITIONAL SECTION (1 record)
;; EDNS version 0
;; flags: 0000
;; rcode: NOERROR
;; size: 4096
;; option: CLIENT-SUBNET 00012000ac100002

——Display of destination IP address——
192.168.14.26
——Display of source IP address———
172.16.0.2
```

図 6　クライアントサブネットオプション書換えを行わない場合の結果
Fig. 6　Result in the case of without rewriting of the client subnet option

4.2 動作結果

動作確認方法に従って動作確認を行った結果，図 6 より，DNS コンテンツサーバでクライアントサブネットオプションが付加された DNS 問い合わせとその応答メッセージから，クライアントのローカル IP アドレス (172.16.0.2) とサーバの IP アドレスを抽出できていることが分かる．また図 7 より，NAT ルータによって変換されるクライアントのグローバル IP アドレス (192.168.14.30) とサーバの IP アドレスを抽出できていることが分かる．なお，DNS コンテンツサーバに対して問い合わせを行った DNS キャッシュサーバの IP アドレスは，グローバル IP アドレス (192.168.14.70) に変換されていることが確認できる．以上のことより，NAT ルータ自身が予め設定した変換ルールに基づいて，DNS キャッシュサーバから通知される IP アドレスを書換えていることが確認できる．この NAT ルータを，動的ファイアウォールシステムのクライアント側に設置することで，通知する IP アドレスと実際にクライアントが通信に利用する IP アドレスを同一のものとすることができる．これにより，DNS コンテンツサーバは，クラ

```
query 58780 : www.reo.net.cs.tuat.ac.jp IN A
Received query from 192.168.14.70 to 192.168.14.48
;; HEADER SECTION
;; id = 26126
;; qr = 0 aa = 0 tc = 0 rd = 1 opcode = QUERY
;; ra = 0 z = 0 ad = 1 cd = 0 rcode = NOERROR
;; qdcount = 1 ancount = 0 nscount = 0 arcount = 1
;; do = 0
;; EDNS version 0
;; flags: 0000
;; rcode: NOERROR
;; size: 4096
;; option: CLIENT-SUBNET 00012000c0a80e1e

;; QUESTION SECTION (1 record)
;; www.reo.net.cs.tuat.ac.jp. IN A

;; ANSWER SECTION (0 records)

;; AUTHORITY SECTION (0 records)

;; ADDITIONAL SECTION (1 record)
;; EDNS version 0
;; flags: 0000
;; rcode: NOERROR
;; size: 4096
;; option: CLIENT-SUBNET 00012000c0a80e1e

――Display of destination IP address――
192.168.14.26
――Display of source IP address―――
192.168.14.30
```

図 7 クライアントサブネットオプション書換えを行う場合の結果
Fig. 7 Result in the case of rewriting of the client subnet option

イアント・サーバ間の通信で利用される IP アドレスを事前に把握して，ファイアウォールの検査内容を動的に変更するシステムを実現することができる．

5. おわりに

動的ファイアウォールシステムを機能させるには，DNS キャッシュサーバで通知する IP アドレスと同一の IP アドレスを用いて，クライアントは通信を行う必要がある．そのため，クライアント側で NAT ルータを利用した環境では，通知される IP アドレスと通信に利用される IP アドレスが異なり，動的ファイアウォールシステムが機能しないという問題があった．そこで本論文では，動的ファイアウォールシステムのクライアント側に設置する NAT ルータを設計し，実装および動作確認を行った．この NAT ルータは，予め設定した変換ルールに基づいて，DNS キャッシュサーバから通知されるプライベート IP アドレスをグローバル IP アドレスに書換える機能を持つ．これにより，動的ファイアウォールシステムのクライアント側で NAT ルータを用いる環境に対応することが可能となった．また，従来のシステムでは，クライアント側で NAT ルータを利用した環境において，変換後の IP アドレスが 2 種類以上ある場合に対応できなかった．しかし本研究により，NAT ルータ上に DNS から通知される IP アドレスを変換後の IP アドレスに書換える機能を組み込むことで，変換後の IP アドレスが 2 種類以上でも対応することが可能となった．

本研究では，変換後の IP アドレスが 2 種類あると想定して実装を行ったが，今後の課題として，2 種類以上の IP アドレスを用いた場合の動作確認を行うことが挙げられる．また，開発された動的ファイアウォールシステムに，実装した NAT ルータを設置した状態の実証実験を行う必要があると考える．

謝辞 本研究の一部は平成 25〜27 年度科学研究費補助金（基盤研究（C），課題番号 25330205）の補助を受けている．ここに記して感謝の意を表する．

参考文献

[1] 岡山聖彦, 山井成良, ガーダ, 大塚友和: DNS と OpenFlow スイッチとの連携による動的ファイアウォール, インターネットと運用技術シンポジウム 2013(IOTS2013) 論文集, pp95-98, 2013.
[2] P.V. Mockapetris: Domain Names - Concepts and Facilities, RFC1034, IETF, 1987.
[3] P.V. Mockapetris: Domain Names - Implementation and Specification, RFC1035, IETF, 1987.
[4] E.Haleplidis, K.Pentikousis, S.Denazis, J.Hadi Salim, D.Meyer and O.Koufopavlou: Software-Defined Networking (SDN): Layers and Architecture Terminology, RFC7426, IETF, 2015.
[5] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker and Jonathan Turner: OpenFlow: Enabling Innovation in Campus Networks, In Proceedings of SIGCOMM 2008, pp.69-74, 2008.
[6] 大塚友和, ガーダ, 山井成良, 岡山聖彦: DNS と OpenFlow との連携による動的ファイアウォールシステムの構築, 第 17 回 IEEE 広島支部学生シンポジウム論文集, pp140-143, 2015.
[7] P.Srisuresh and K. Egenang: Traditional IP Network Address Translator (Traditional NAT), RFC3022, IETF, 2001.
[8] P.Vixie: Extension Mechanisms for DNS(EDNS0), RFC2671, IETF, 1999.
[9] C. Contavalli, W. van der Gaast and D. Lawrence, W. Kumari: Client Subnet in DNS Queries, Work in Progress, IETF, 2015. https://tools.ietf.org/html/draft-ietf-dnsop-edns-client-subnet-06
[10] 大塚友和, 山井成良, ガーダ, 岡山聖彦: 動的ファイアウォールシステムのための DNS によるクライアント IP アドレスの通知機能, マルチメディア, 分散, 協調とモバイル（DICOMO2014）シンポジウム論文集, pp184-189, 2014.
[11] S.Wehner: Net::Divert, 2001. https://metacpan.org/source/ATRAK/Net-Divert-0.01/Divert.pm
[12] N.Labs: Net::DNS::Packet, 2015. https://metacpan.org/source/NLNETLABS/Net-DNS-1.04/lib/Net/DNS/Packet.pm