一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
ICM2024-19,LOIS2024-52(2025-01)

組織ネットワーク管理のための DNS 通信分析による RPZ を利用した不正通信検知手法の検討

一瀬 光† 金 勇‡ 飯田 勝吉††

†大分大学 情報基盤センター
‡東京科学大学 情報基盤センター
††北海道大学 情報基盤センター

E-mail: †ichise-hikaru@oita-u.ac.jp, ‡yongj@cii.isct.ac.jp, ††iida@iic.hokudai.ac.jp

あらまし 昨今、不正な DNS 通信を行うマルウェアが急激に増えている。そのようなマルウェアに感染した PC は組織の DNS フルリゾルバを経由せずに直接外部に DNS クエリを送る。これまでの研究ではその直接外部クエリを検知・遮断するために NS レコードとそれに対応する A レコードを分析し、DNS の RPZ(Response Policy Zone)に登録した。SDN を利用してパケット操作を行い、RPZ に登録されていない IP アドレス宛の DNS クエリは不正な通信として遮断するシステムを構築した。しかしながら、これまでの研究では RPZ を登録するのに 40 分以上かかり、大規模な組織ネットワークでは利用することが難しい。そこで本研究ではその RPZ を登録する処理時間を短縮することに着目する。DNS 通信を既存研究よりも高速に分析できる方法を実装し、RPZ を利用した検知・遮断システムを構築した。更には実際の組織ネットワーク環境において利用できる方法を検討する。

キーワード 不正通信，DNS，RPZ, SDN，ネットワーク管理.

A Consideration for Deployment of Abnormality Detection System by DNS Traffic Analysis using RPZ

Hikaru ICHISE† Yong JIN‡ Katsuyoshi IIDA††

† Information Technology Center, Oita University
‡ Center for Information Infrastructure, Institute of Science Tokyo
†† Information Initiative Center, Hokkaido University

E-mail: †ichise-hikaru@oita-u.ac.jp, ‡yongj@cii.isct.ac.jp, ††iida@iic.hokudai.ac.jp

Abstract Recently, the number of malwares using abnormal DNS communication has been increasing. The PC infected in such malware sends DNS queries non-via DNS full resolver (direct outbound DNS query) in organization network. In our previous research, we analyzed NS records and the corresponding A records and stored them in DNS RPZ in order to detect and block the direct outbound DNS queries. However, our system had difficulty in being deployed in a large-scale network environment, since it took more than 40 minutes to register the NS records and the corresponding A records in the RPZ. Therefore, in this paper, we focus on shortening the processing time of registration in the RPZ. We implement the method to analyze the DNS traffic faster than the previous system, and construct the detection and blocking system using RPZ. Moreover, we consider the deployment of our system in real network environment.

Keywords Abnormal communication, DNS, RPZ, SDN, Network management.

1. はじめに

昨今、DNS を利用したマルウェアは急激に増加している。文献[1]のインターネットイニシアティブ（IIJ）社の DNS フィルタリングレポート（2024 年 4 月～6 月）によれば、PC は DNS を利用して C&C サーバと言われる怪しいサーバと通信し、PC に命令を送り、遠隔で操作、情報取得する報告されている。本報告ではフィルタリング対象のマルウェアのドメインは 2024 年現在でも増加している。それ以外にも、DDoS 攻撃、バックドアのマルウェアでも DNS を利用している。このような DNS を利用したマルウェアを検知することは急務であり、大きな課題でもある。

DNS はクライアント PC が Web サーバ、メールサーバのようなアプリケーションにアクセスするた

めに予めドメイン名と IP アドレスを変換するためのシステムである。図 1 は DNS の挙動を示す。初めクライアント PC は DNS フルリゾルバに問い合わせをする（矢印①：DNS クエリと呼ぶ。）。次に DNS フルリゾルバは権威 DNS サーバにメールサーバ、Web サーバの IP アドレスの問い合わせを行い、通信を行うための宛先 IP アドレスを取得する（矢印②、③）。その後、情報を取得した DNS フルリゾルバはクライアント PC にその結果を返し（矢印④：DNS レスポンス）、最終的にクライアント PC は Web サーバやメールサーバ等のアプリケーションサーバとの間で通信を行う（矢印⑤）。このような手順に基づき、クライアント PC は様々なアプリケーションを利用する。しかしながら、DNS を利用したマルウェアに感染したクライアント PC は本手順（矢印①～⑤）に従って、通信を行わない。図 2 はマルウェアに感染したクライアント PC の挙動を示す。マルウェアに感染したクライアント PC（ボット感染 PC と呼ぶ。）は DNS フルリゾルバを経由しないで不正なサーバ（C&C サーバと呼ぶ。）に直接 DNS クエリを送り、通信を行う（矢印①、②）。その後、ボット感染 PC は他の正常な PC やサーバに DoS 攻撃や不正なメール配送を行う挙動を行う。そこで、本研究ではボット感染 PC を検知、遮断することに着目し、我々は研究を行ってきた。

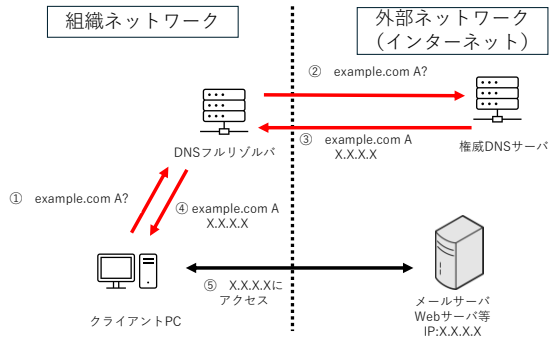


図 1 ：正当な DNS の挙動

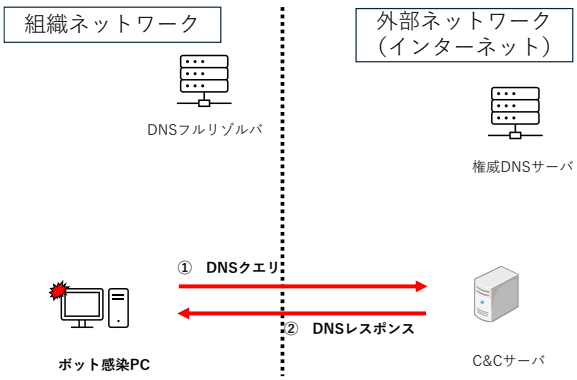


図 2 ：ボット感染 PC の挙動

これまでの我々の研究ではこのような直接外部クエリを利用したボット感染 PC を検知するために、初期段階では東京工業大学（東工大と呼ぶ。）の学内 LAN とインターネットに接続しているボーダルータから、DNS クエリと DNS レスポンス（DNS 通信）を取得して、直接外部クエリを約 100 日間の分析を行い、怪しい通信を抽出した。その結果、約 20%が不正な DNS クエリであると判明した[2]。この結果に基づいて、次の段階では直接外部クエリを検知、遮断するシステムを検討した。正常な名前解決方法では DNS フルリゾルバと権威 DNS サーバ間の DNS 通信では必ず、NS（Name Server）レコードを取得する。そのため、研究の初期段階で取得した DNS 通信を利用して、NS レコードとそれに対応する A レコードを取得し、照合したデータベースを創る。次にそのデータベースをホワイトリストとして利用する。そのホワイトリストと SDN(Software Defined Network)[3]を図 3 のように利用することによって、直接外部クエリの検知、遮断するシステムを提案した。更にはその提案システムを設計、構築、実装することによって、実際に直接外部クエリを検知できることを示し、そのシステムの性能評価を行った。その結果、本提案システムは 2 時間 200MB の DNS 通信の pcap ファイルを利用し、約 60 分の処理時間でデータベースに NS レコードとそれに対応する A レコードを保存し、そのような DNS 通信を取得できる組織ネットワーク環境では充分に利用できるシステムであることを示した[4]。次の段階として、DNS の機能の一つである RPZ（Response policy Zone）[5]を利用したシステムに変更した。その際に DNS 通信の分析するプログラム、RPZ に登録するプログラム複数プログラムを作成した。先行研究と同様の pcap ファイルを利用して作成したプログラムを実行した結果、処理時間が約 40 分かかった。データベースとのネットワーク遅延を比較した結果、充分に RPZ でも利用できることを示した[6]。しかしながら、既存の研究ではデータベース、RPZ を用いても巨大な組織ネットワーク上では 2 時間毎に 200MB 以上の DNS 通信を取得できるようなネットワーク環境ではよりリアルタイムに DNS 通信を分析することが求められるため本システムでは難しいことが課題である。

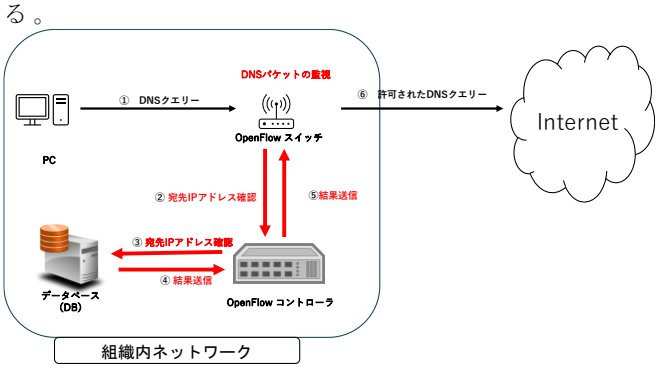


図 3 ：直接外部クエリ検知・遮断システム

そこで、更なる段階として、本研究では大規模組織においてもこれまで検証してきたシステムを利用できることを目的として、DNS 通信の分析処理時間を短縮し、よりリアルタイムに近い直接外部クエリを検知・遮断できるシステムに拡張すること

が狙いである。つまり、多くの DNS 通信を取得できる環境において、既存システムよりも高速に DNS 通信を処理できるシステムにすることに着目している。そこで本研究ではデータベースを利用する代わりに DNS の BIND9 以降に実装された RPZ を利用する。更には DNS 通信の分析、RPZ に登録するプログラムを 1 本のプログラムに修正することによって、DNS 通信の処理時間を 7 分まで高速に処理できる方法を示した。更には DNS 通信の取得時間や TTL (Time To Live) とゾーン情報を入れることにより、データの更新できるような仕様に拡張した。

2. 関連研究

これまで多くの DNS の不正通信に関する研究が多くなされている。本節では本研究と関連の深い研究を紹介する。

文献[7]では Chen 氏は DNS トンネリングの検知方法についての問題に取り組み、解決方法として新しい LSTM 技術を使って 99.38%の検知率で検知できることを示した。しかしながら、この論文では分析手法は分析するための時間がかかるため大規模なネットワーク環境では実装することが難しいと考えられる。

このように DNS を利用したマルウェアを検知するために機械学習を用いる方法もあるが、本研究では、DNS の直接外部クエリに着目し、大規模ネットワーク環境でも利用できるように DNS 通信を高速に分析し、RPZ に登録する方法を検討した。

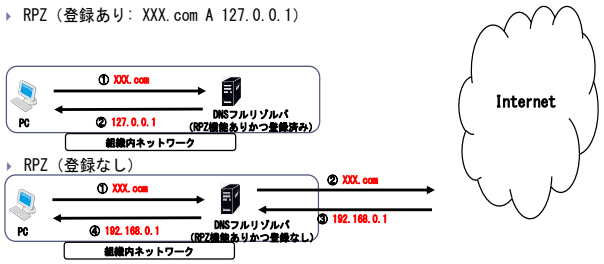
3. 直接外部クエリの RPZ を利用した検知・遮断システムの処理時間の短縮方法と実装

前節では DNS を用いた不正通信の検知システム関する関連研究を述べた。本節では本研究の目的である大規模なネットワーク環境ための処理時間の短縮方法について述べる。

3.1. 概要と修正方法

本システムでは組織内の PC が直接外部クエリを利用するマルウェアに感染した際、組織内の DNS フルリゾルバを利用せずに外部に DNS クエリを送る。そのため、事前に DNS フルリゾルバと権威 DNS サーバから NS レコードとそれに対応する A レコード (glue A レコード) を取得することはない。その観点から、NS レコードとそれに対応する glue A レコードを既存の研究ではデータベースに保存してきた。しかしながら、データベースを用いた保存方法では TCP 接続し、保存するため、多くの遅延が発生する。それを解決するために本研究では UDP を利用した DNS の機能の一つである RPZ[5]を利用することによって、遅延を大幅に改善させて、より高速に NS レコードとそれに対応する A レコードを保存することができるシステムを提案する。

RPZ の目的はクライアントから送信された悪意のある DNS 名前解決に対して故意に失敗させたり、クライアントに返したりすることができる。図 4 は RPZ の挙動を示す。図 4 に示すように RPZ に「XXX.com A 127.0.0.1」を RPZ のゾーンファイルに登録している場合、外部のインターネットに問い合わせすることなく、PC は RPZ の情報 (127.0.0.1) のみ取得し、不正な IP



アドレスにアクセスできないようにすることができる。

図 4 : RPZ に挙動

一方で、RPZ に何も登録されていない場合は通常通り、名前解決をするような挙動となっている。

この機能とこれまで利用していた SDN を組み合わせることによって、検知・遮断システムを構築する。

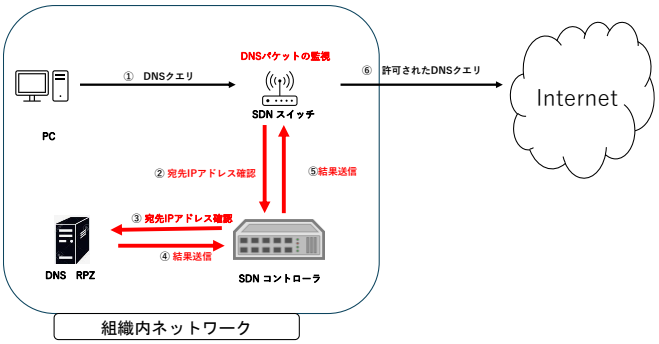


図 5 : システムアーキテクチャ

SDN[3]はデータプレーンとコントロールプレーンからなるシステムである。データプレーンとはスイッチやルータのようなネットワーク機器であり、それらをコントロールプレーンで制御できる仕組みとなっている。従来のネットワーク機器ではこのデータプレーンとコントロールプレーンが一体となっており、ルータ、スイッチにアクセスして、コントロールする必要があった。この SDN 機器を利用することによって、コントロールプレーンで配下にあるデータプレーンのスイッチを制御することが可能である。更に、コントロールプレーンではプログラマブルな仕様になっており、管理者側でプログラミング言語を利用することによって、パケットを自由に転送や遮断することが可能である。

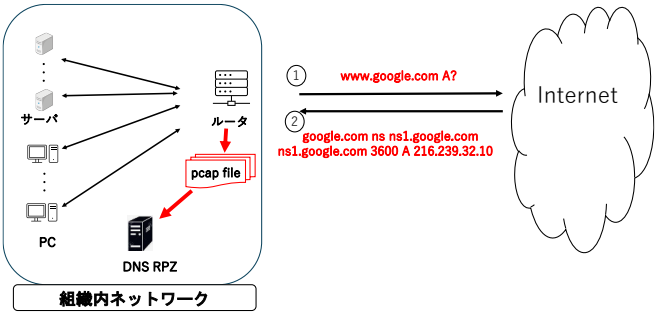


図 6 : 取得情報と RPZ の登録

図 5 はシステムアーキテクチャを示す。PC は SDN スイッチに DNS クエリを送る（矢印①）。次に SDN スイッチの送られた DNS クエリは SDN コントローラに転送され、宛先 IP アドレスを RPZ に問い合わせチェックする（矢印②、③）。そのチェックした結果を SDN コントローラから経由して SDN スイッチに返す（矢印④、⑤）。その結果、RPZ に登録されている IP アドレスは正当な宛先 IP アドレスとして正常に SDN スイッチを通過し、RPZ に登録されていない IP アドレスは不正な宛先 IP アドレスとして遮断できるようなシステムである。

ここで重要となるのは RPZ をホワイトリストとして扱うので、いかに高速に RPZ に正当な IP アドレスとそれに付随する情報を登録できるかである。RPZ のホワイトリストの作成方法は図 6 に示すように予め組織内ネットワークとインターネットに接続する境界ルータから pcap フォーマットでインターネットに通信する DNS 通信（矢印①、②）を取得する。その後、pcap ファイルから①と②を照合し、NS レコードとそれに対応する glueA レコード、更には取得時間（UNIXTIME）、TTL（Time To Live）、ゾーン情報を DNS の TXT レコードで登録することにより、RPZ のホワイトリストを作成する。RPZ に登録した 1 レコードとしては“ 216.239.32.10.rpz.example.com TXT 166247324_3600_google.com”となる。

以前の我々の研究 [6]において、東工大のボーダルータから多くの DNS トラフィックの pcap ファイルを入手した。約 200MB の DNS トラフィックの 1 塊の pcap ファイルを利用し、本システムを評価した結果、1 つの pcap ファイルを処理し、RPZ に登録する時間は約 40 分かかった。前の研究では登録するのに Python ベースで分析し、RPZ に登録する際に、perl を利用していたため、約 40 分もの時間が必要となった。そこで全てのプログラムを Python ベースで修正し、更にはプログラムを再度見直し、RPZ の登録プログラムを高速に処理できる方法を提案する。

3.2. 実装とネットワーク環境

3.1 節で述べたような提案手法に基づいて、本節ではプログラムを作成し、実装とそのネットワーク環境を説明する。pcap ファイルから RPZ に登録するプログラムである。

pcap ファイルの処理プログラムである。プログラム言語は python3.9 を利用し、dpkt モジュール、pcap-ct モジュール、Pygments モジュールを利用して pcap ファイルを解析した。DNS クエリをリストで保存し、メッセージ ID でそれに対応するレスポンスを照合する。そのレスポンスに NS レコードとそれに対応する glueA レコードがある、もしくは NS レコードと対応する A レコードがある場合、RPZ に A レコードの IP アドレスを“<IP アドレス>.rpz.example.com TXT UNIXTIME_TTL_Zone”登録する。この RPZ に登録する際に、RPZ の設定として、TSIG(Transaction SIGnatures)キー[8]を生成し、named.config ファイルに設定と処理プログラムの中にその TSIG キーを組む込むことによって、RPZ を動的に更新できる仕様とした。そうすることで一連の処理を全て python で 1 本のプログラムにして、作成することが可能となる。

また、ネットワーク環境としては図 7 に示すように、1 つのホストサーバに 3 つの KVM(Kernel Virtual Machine) を構築し、各 KVM にそれぞれプログラムを実装して、各 OS は RockyLinux8.10 を利用し、ネットワーク環境を構築した。更に本研究環境では SDN としてコントローラーとして Ryu[9] を利用し、データプレーンとして OpenVswitch[10]を利用した。

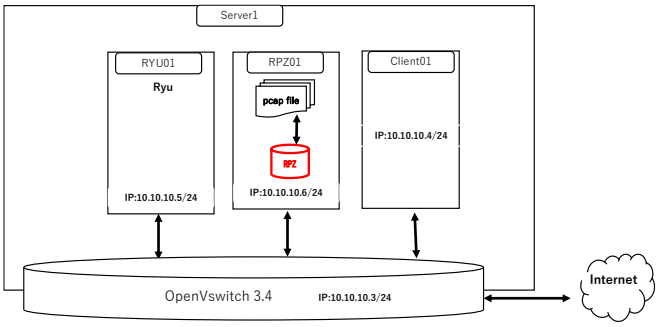


図 7:ネットワーク環境

4. 機能評価

提案システムの機能を確認するために 3.2 の実装とネットワーク環境において、評価する。構築したネットワーク環境上で以前の我々の研究 [6]において、東工大のボーダルータから多くの DNS トラフィックの pcap ファイルを取得した。その一部 200MB の pcap ファイルを利用する。

実験用のネットワーク環境において RPZ を構築したあと、実装したプログラムを利用して、pcap ファイルから RPZ に登録する。その結果、表 1 に示すようにデータベースと既存の研究で利用した 2 本のプログラムによる RPZ の登録方法、今回の改修により 1 本のプログラムによる登録結果、大幅に改善したことがわかる。これにより大規模なネットワーク環境において多くの DNS 通信を取得できる環境でも負荷なく高速に RPZ に登録できることを示す。更には UNIXTIME と TTL を取得しているため、その期限によって、削除処理も可能である。

表 1 ：処理時間結果

データベース登録時間	複数プログラム RPZ 登録	1 本プログラム RPZ 登録
60(minutes)	40(minutes)	7(minutes)

本研究により大規模な組織ネットワーク環境のような多くの DNS 通信を取得できる環境でも高速に分析し、RPZ に登録することはできるが、本実験環境では

SDN 環境であるため、実際のネットワーク環境では利用が難しい。そのため、実環境として組織内ネットワーク環境では次世代ファイアウォールをカスタマイズすることにより、本システムの RPZ を次世代ファイアウォールから常に参照することにより実社会でも利用可能である。具体的には図 8 は RPZ を利用した組織ネットワークの直接外部クエリの検知・遮断方法の管理を示す。組織内の PC から送られてくる全ての DNS クエリは次世代ファイアウォールで必ずチェックする（矢印①）。次に次世代ファイアウォールは DNS クエリの宛先 IP アドレスを RPZ にチェックする（矢印②）。その結果、RPZ に存在している場合、正常な通信として判断、存在しない場合は怪しい通信とし、遮断する（矢印③）。そして、正常な DNS 通信のみ外部のインターネットに送る方法である（矢印④）。

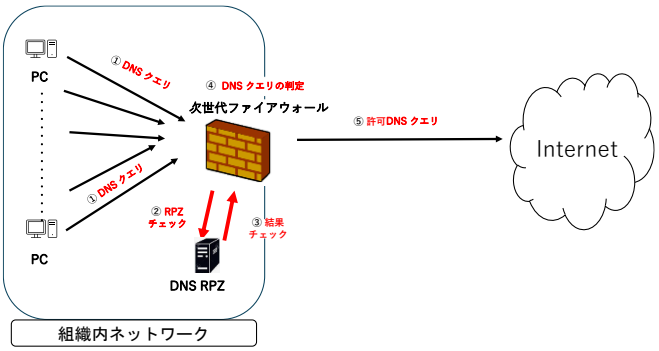


図 8 ：組織ネットワークの RPZ を利用した検知・遮断方法

5. おわりに

これまでに我々は DNS に関する直接外部クエリに着目して、不正な通信の検知・遮断方法について研究してきた。既存の研究の課題として DNS 通信の分析と RPZ の登録時間が 40 分かかる。そこで、本研究ではその課題解決するために Python プログラムの改修による処理時間の短縮と組織ネットワーク環境における RPZ の利用方法の検討をおこなった。その結果、NS レコードとそれに対応する A レコードを RPZ に登録する時間は 7 分と大幅に短縮することが可能となった。そのため、大規模な組織ネットワークでも利用できることを示した。更にその組織ネットワークで RPZ の利用方法について検討した。

今後は本大学で実際に次世代ファイアウォールを利用しているので、カスタマイズすることにより現実的なネットワーク環境でも本システムの有効性を明らかにする必要がある。

文　献

[1] 株式会社インターネットイニシアティブ ：「DNS フィルタリング定期レポート 2024 年 4 月～2024 年 6 月」、 2024 年 7 月 31 日.

[2] H. Ichise, Y. Jin, and K. Iida, “Analysis of DNS TXT record usage and consideration of botnet communication detection,” *IEICE Trans. Commun.*, vol. E101-B, no. 1, pp. 70–79, Jan. 2018. DOI: 10.1587/transcom.2017ITP0009

[3] Open Networking Foundation: SDN Architecture (online), https://www.opennetworking.org/ (accessed 2024-12-16).

[4] H. Ichise, Y. Jin, K. Iida, and Y. Takai, “NS record history based abnormal DNS traffic detection considering adaptive botnet communication blocking,” *IPSJ J. Information Processing*, vol. 28, pp. 112-122, Feb. 2020. DOI: 10.2197/ipsjjip.28.112

[5] Internet Systems Consortium, https://www.isc.org/rpz/ (accessed 2024-12-16).

[6] H. Ichise, Y. Jin, and K. Iida, “Policy-based detection and blocking system for abnormal direct outbound dns queries using RPZ,” *Proceedings of International Conference on Future Computer and Communication (ICFCC 2022)*, 2022.

[7] S. Chen, B. Lang, H. Liu, D. Li, and C. Gao, “DNS covert channel detection method using the LSTM model,” Computers & Security, vol. 104,art. 102095, 15 pages, May 2021.

[8] P. Vixie, O. Gudmundsson, D. Eastlake, B. Wellington, “Secret Key Transaction Authentication for DNS (TSIG),” *IETF RFC2845*, May. 2000.

[9] NTT, inc., “Ryu: Getting Started,” https://osrg.github.io/ryu-book/en/html/, (Accessed 2024-12-16)

[10] Open vSwitch: Open vSwitch, https://www.openvswitch.org/ (Accessed 2024-12-16)