Vol.2018-CSEC-81 No.18
Vol.2018-IOT-41 No.18
2018/5/18

DNSシンクホールとハニーポットを用いた不正FQDNに対する通信観測システムの開発

佐保 航輝[1]　池部 実[2]　吉田 和幸[3]

概要：インターネットではドメイン名を悪用した詐欺や攻撃が多く発生している．不正な FQDN を用いた Web サーバに接続することで，フィッシング被害やマルウェア感染などの被害が発生する．不正 FQDN に対する接続を阻止する手法の一つとして DNS シンクホールがある．DNS シンクホールは C&C サーバの FQDN やフィッシングサイトの FQDN などの不正な FQDN に対するクライアントからの問い合わせについて，本来とは異なる回答を返して悪意のあるサーバへの接続性を防ぐ．現在大分大学理工学部知能情報システムコース内で DNS シンクホールを運用し，登録している不正 FQDN に対してループバックアドレスを返している．本研究では不正 FQDN に接続を試みるクライアントを検知，挙動の分析を目的として，DNS シンクホールとハニーポットを用いて不正 FQDN に対する通信を観測するシステムを構築した．DNS シンクホールからの回答としてハニーポットの IP アドレスを返すことで当該通信をハニーポットへ誘導し，不正 FQDN を問い合わせたクライアントの通信の分析を可能とする．本観測システムではハニーポットによって収集されたクライアントからの HTTP リクエストを分析することで，ブラックリストに記載された FQDN のみでは分析できない接続後の挙動やどのように攻撃を行うかなどを分析する．

キーワード：DNS，DNS シンクホール，ハニーポット，ネットワークセキュリティ，マルウェア

Development of a monitoring system for communication to illegal FQDNs using the DNS sinkhole and the honeypot

Koki Saho[1]　Minoru Ikebe[2]　Kazuyuki Yoshida[3]

Abstract: Abused domain names occurs cyber criminals on the Internet. Users suffer from phishing scam or malware infection when connected to Web server with the use of the illegal FQNDs. A DNS sinkhole is one of a method to prevent the connection to the illegal FQDNs. The DNS sinkhole responses a fake answer against the inquiry of illegal FQDN. Therefore, the administrator blocks the connection to a malicious server from clients. Now, we operate DNS sinkhole in our division's network. Our DNS sinkhole responses the loopback address to the inquiry of illegal FQDN. Our research purpose is to detect the connection to illegal FQDN from the client and to analyze the behavior of the client. Therefore, we develop a monitoring system for the communication to the illegal FQDN using the DNS sinkhole and the honeypot. The DNS sinkhole responses the IP address of honeypot. Our system collects the connection by the honeypot. Our monitoring system focuses the HTTP request from the client. We are able to analyze the communication of the client against the illegal FQDN. Our system not only bans the illegal connection but also monitor possible.

Keywords: DNS, DNS Sinkhole, Honeypot, Network Security, Malware

[1] 大分大学大学院工学研究科工学専攻知能情報システム工学コース
Course of Computer Science and Intelligent Systems, Graduate School of Engineering, Oita University
[2] 大分大学理工学部共創理工学科知能情報システムコース
Division of Computer Science and Intelligent Systems, Department of Integrated Science and Technology, Faculty of Science and Technology, Oita University
[3] 大分大学学術情報拠点情報基盤センター
Center for Academic Information and Library Services, Oita University

Vol.2018-CSEC-81 No.18
Vol.2018-IOT-41 No.18
2018/5/18

1. はじめに

インターネットの発展と普及に伴い，ネットワークを介して様々な情報がやり取りされている．Web ページの閲覧や電子メールといったコミュニケーション手段や，クレジットカード番号を利用した電子商取引など，我々が利用しているサービスにおいてインターネットは必要不可欠な存在になっている．インターネット上の様々なサービスを利用する上で DNS(Domain Name System) は欠かすことができない．DNS はドメイン名と IP アドレスを対応付ける，インターネットにおいて重要なサービスのひとつである．DNS サーバはその機能により，DNS 権威サーバと DNS キャッシュサーバの 2 つの種類に分類される．DNS 権威サーバは各ドメイン空間を管理し，DNS キャッシュサーバはクライアントからの名前解決要求を受信して権威 DNS サーバへ問い合わせる．クライアントは名前解決によって得られた IP アドレスを用いることで，インターネット上の様々なサービスを利用できる．

しかしながら，ドメイン名を悪用した詐欺や攻撃などの被害も発生しており，問題となっている．フィッシングサイトやマルウェア配布サイトなどの不正な FQDN を用いた Web サーバに接続することで，フィッシング被害やマルウェア感染などの被害が発生する．これらの被害を抑えるために，不正な FQDN への接続を阻止する必要がある．

現在，大分大学理工学部知能情報システムコース内で不正 FQDN への接続を阻止するために DNS シンクホールを運用している．また，接続を阻止するだけでなく，接続後の通信を観測することによって不正 FQDN に接続を試みたクライアントのマルウェア感染の検知や，接続後の挙動分析なども可能になると考えられる．そこで本論文では，運用中の DNS シンクホールを用いて観測用サーバへと接続を誘導し，通信を観測するシステムを構築する．

本論文の構成は以下の通りである．第 2 章で運用中の DNS シンクホールについて述べ，第 3 章では事前調査について述べる．そして第 4 章で本観測システムについて述べ，最後に第 5 章でまとめと今後の課題について述べる．

2. DNS シンクホール

クライアントと不正 FQDN との接続を阻止する技術として，DNS シンクホール [1] がある．DNS シンクホールはマルウェア配布サイトやフィッシングサイトといった既知の不正 FQDN の一覧をブラックリストとして保持する．DNS シンクホールによる不正 FQDN への接続阻止の流れを図 1 に示す．

(1) クライアントは DNS キャッシュサーバに FQDN を問い合わせる．
(2) DNS シンクホールを設置した DNS キャッシュサーバは，問い合わせを受けた FQDN が自身の保持する不正 FQDN の一覧リスト (ブラックリスト) 内に存在するかを確認する．存在した場合，本来とは異なる IP アドレスを回答として返す．
(3) クライアントは DNS キャッシュサーバからの回答をもとにサーバへの接続を試みるが，本来とは異なる IP アドレスであるため目的のサーバへの接続は失敗する．

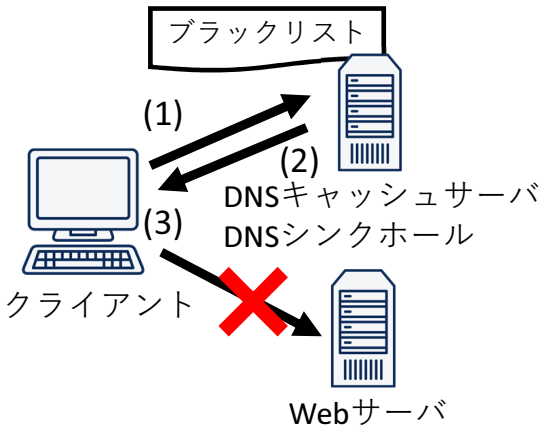

図 1 DNS シンクホールによる不正 FQDN への接続阻止の流れ

現在大分大学理工学部知能情報システムコース内で運用中の DNS シンクホールについて述べる．

我々は 2016 年 8 月 12 日より大分大学理工学部知能情報システムコース内で 2 台の DNS シンクホール (以下，それぞれ dns1，dns2 とする) を運用し，不正 FQDN への接続を阻止している．不正 FQDN のブラックリストとしては DNS-BH-Malware Domain Blocklist[2] が公開しているゾーンファイルを使用している．このゾーンファイルには malicious，phishing，malware などといった種類の不正 FQDN が記載されている．

不正 FQDN に対する偽の回答として，自分自身を指すループバックアドレス (127.0.0.1) を返すように設定してあり，自分自身にアクセスすることになる．そのため，実際に問い合わせた不正 FQDN への接続は失敗する．

本論文では，不正 FQDN へ接続を試みたクライアントの接続後の挙動を分析することで，マルウェア感染の早期発見や被害の抑制などを目的とした通信観測システムを構築する．

3. 事前調査

運用中の DNS シンクホールについて，どういった種類の不正 FQDN がどの程度問い合わせられているかを把握するために，事前調査として不正 FQDN に対する問い合わせ状況を調査した．調査期間は 2017 年 1 月 1 日から 2017 年 12 月 31 日までの 1 年間とした．調査の結果を表 1 に示す．

調査期間中のクエリログの件数は dns1 で 79,903,526 件，dns2 で 71,684,975 件，合計で 151,588,501 件であった．2 台の DNS シンクホールから合計 91 件の不正 FQDN に対

表 1　調査結果

期間	2017 年 1 月 1 日 ～ 12 月 31 日
全体の問い合わせ件数	151,588,501 件
不正 FQDN への問い合わせ件数	91 件
検出した不正 FQDN	11 種類
送信元 IP アドレス	17 種類

表 2　dns1 で検出した不正 FQDN への問い合わせ件数

月	1	2	3	4	5	6	7	8	9	10	11	12
件数	6	0	0	0	0	0	0	2	6	9	0	0

表 3　dns2 で検出した不正 FQDN への問い合わせ件数

月	1	2	3	4	5	6	7	8	9	10	11	12
件数	48	0	0	3	0	1	0	4	3	6	0	3

表 4　検出された不正 FQDN

不正 FQDN	分類
bleachkon.net	malicious
cdn.sitemakerlive.com	phishing
cnrdn.com	attackpage
downlaod.vstart.net	attackpage
homepages.plus.net	malware
lithiumcheats.xyz	malicious
microsoft-securityprotection-support.com	phishing
ono-group.com	phishing
retro-bit.com	phishing
sp-storage.spccint.com	malicious
wimi5.com	phishing

する問い合わせが検出され，100 万クエリあたりおよそ 6.3 件の問い合わせが不正 FQDN に対するものであった．dns1，dns2 で確認された不正 FQDN に対する問い合わせの件数を表 2 と表 3 にそれぞれ示す．

また，問い合わせられた不正 FQDN は 11 種類であった．検出された 11 種類の不正 FQDN とその分類を表 4 に示す．

不正 FQDN の種類としては phishing が最も多く，次いで malicious という結果だった．送信元アドレスは 17 種類あり，一つの送信元アドレスから名前解決要求される不正 FQDN の種類は 1 種類のみがほとんどであったが，2 種類の不正 FQDN を問い合わせる送信元アドレスも存在した．

今回検出された不正 FQDN に対する問い合わせのうち，数日にわたって問い合わせが行われたものや大量に問い合わせられたものについて，さらに詳しく調査した．調査には FQDN をもとにホストの情報を取得できる Virus Total[3]，IPAddress.com[4]，sitecheck.sucuri.net [5] などのサイトを利用した．また，問い合わせログの形式を図 2 に示す．

DomainA

DomainA の名前解決は dns1 と dns2 の両方で検出された．dns1 で検出した問い合わせログを図 3 に示す．DomainA の問い合わせは 10 月 7 日に 1 件，10 月 12 日に 4 件，10 月 13 日に 4 件存在した．これらの問い合わせに対して送信元アドレスは 5 つあった．問い合わせはすべて A レコードであり，10 月 7 日の 1 件以外はすべて同一の送信元アドレスから 2 回ずつ問い合わせられていた．また，1 回目と 2 回目の問い合わせの間隔はどれも 40 分ほどであった．DomainA はブラックリストでは malicious であると記載されている．IPAddress.com によると，この FQDN は中国の Web サイトで，マルウェアなどのソフトウェアを配布する Web サイトとして他のウイルス対策サイトにも不正 FQDN として登録されていた．また，IPAddress.com にはサーバの情報を要求する HTTP リクエストを送信するサービスもあるが，その結果 2018 年 1 月 15 日時点では Web サーバへの HTTP リクエストに対して 403 が HTTP レスポンスとして返されており，アクセス制限がかけられていた．

日-月-年 時刻 queries: client 送信元IPアドレス #送信元ポート番号 (名前解決対象のFQDN): queriy: 名前解決対象のFQDN class Recorf flag (問い合わせに対応したサーバのIPアドレス)

図 2　問い合わせログの形式

12-Oct-2017 10:35:30.388 queries: client 133.37.***.***#55177 (DomainA): query: DomainA IN A + (133.37.***.***)

12-Oct-2017 11:13:24.401 queries: client 133.37.***.***#46183 (DomainA): query: DomainA IN A + (133.37.***.***)

13-Oct-2017 00:13:41.725 queries: client 133.37.***.***#53785 (DomainA): query: DomainA IN A + (133.37.***.***)

図 3　DomainA のクエリログ

DomainB

DomainB の名前解決は dns1 と dns2 の両方で検出された．dns1 で検出した問い合わせログを図 4 に示す．DomainB の問い合わせは 9 月 11 日に 3 件，9 月 28 日に 6 件，10 月 10 日に 3 件，10 月 31 日に 3 件存在した．A レコード，A レコード，AAAA レコードと決まった順で問い合わせていた．DomainB はブラックリストでは attackpage であると記載されている．IPAddress.com によると，この FQDN は中国の Web サイトで，潜在的に望ましくないソフトウェアなどを配布する Web サイトとして他のウイルス対策サイトにも不正 FQDN として登録されていた．

```
28-Sep-2017 18:25:30.161 queries: client
133.37. ***.***#64901 (DomainB): query:
DomainB IN A + (133.37. ***.***)

28-Sep-2017 18:25:30.192 queries: client
133.37. ***.***#55215 (DomainB): query:
DomainB IN A + (133.37. ***.***)

28-Sep-2017 18:25:30.193 queries: client
133.37. ***.***#52846 (DomainB): query:
DomainB IN AAAA + (133.37. ***.***)
```

図 4　DomainB のクエリログ

```
29-Jan-2017 14:10:45.033 queries: client
133.37. ***.***#65288 (DomainC): query:
DomainC IN A + (133.37. ***.***)
29-Jan-2017 14:10:45.054 queries: client
133.37. ***.***#60826 (DomainC): query:
DomainC IN A + (133.37. ***.***)
29-Jan-2017 14:10:45.055 queries: client
133.37. ***.***#58568 (DomainC): query:
DomainC IN AAAA + (133.37. ***.***)
```

図 5　DomainC のクエリログ

DomainC

DomainC の名前解決は dns2 のみで検出された．検出した問い合わせログの一部を図 5 に示す．DomainC の問い合わせは 1 月 29 日 14 時 10 分から 17 分の 7 分間に 33 件，6 月 7 日に 1 件，8 月 29 日 15 時 16 分の，0.01 秒にも満たない時間で 3 件，12 月 20 日に 1 件存在した．特に 1 月 29 日は短時間で大量に問い合わせをしており，A レコード，A レコード，AAAA レコードと決まった順で問い合わせていた．DomainC はブラックリストでは phishing であると記載されている．2006 年 4 月 3 日に登録された日本の Web サイトで，フィッシング詐欺の恐れがあるほかに，他のウイルス対策サイトでは悪意あるソフトウェアを配布する Web サイトとして登録しているものもあった．

1 年間の調査の結果，不正 FQDN へ接続を試みるクライアントが大分大学内に存在することが判明した．これらの不正 FQDN へ接続することによってフィッシング詐欺やドライブ・バイ・ダウンロード攻撃の被害にあう恐れがあるが，DNS シンクホールにより接続は阻止されている．しかし，これらの不正 FQDN への接続を試みたクライアントがマルウェアなどに感染しているかの検知や，何を目的として接続を試みたかなどは，現在の手法では分からない．

例えば，malicious に分類された不正 FQDN への接続を試みるクライアントは，ボットをはじめとした何らかのマルウェアに感染している可能性がある．クライアントが接続を試みる不正 FQDN は C&C(Command and Control) サーバである可能性が高い．DNS シンクホールでは，問い合わせに対してブラックリストを確認し，本来とは異なる回答を応答するため，DNS シンクホールのみではマルウェア感染を判断することは難しい．そこで C&C サーバを模擬したサーバにより，不正 FQDN に対してどのような通信が発生しているかを観測することで，マルウェア感染の確実な検知，マルウェアの種類を分類できるようになる．

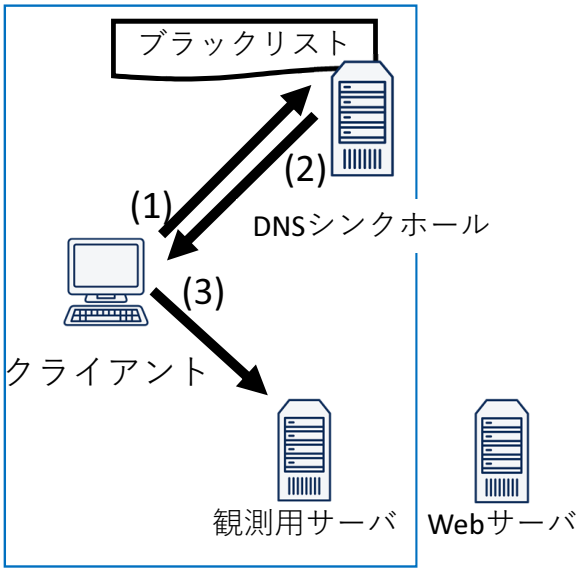

図 6　DNS シンクホールによる通信の誘導の流れ

また，phishing に分類された不正 FQDN に対して接続を試みるクライアントは，フィッシングメールに記載されているフィッシングサイトに接続しようとしている可能性がある．DNS シンクホールでは，問い合わせに対して本来とは異なる回答を応答する．現在 127.0.0.1 を応答するためクライアント側はクリックした URL に接続できず，何が起きているのか状況を把握できない．そこで，DNS シンクホールで誘導した Web サーバでフィッシングサイトである旨の警告を表示するなどして，クライアントに注意を促すことができる．

こうしたマルウェア感染の早期発見や被害の抑制などのためにも，接続後の通信を観測することは重要である．

4. 観測システム

DNS シンクホールが偽の回答として返す IP アドレスは，管理者が自由に設定できる．そこで本観測システムでは観測用のサーバを用意し，観測用サーバの IP アドレスを偽の回答として設定する．このようにすることで不正 FQDN への通信を観測用サーバへと誘導し，接続後の通信が観測可能となる．図 6 で本観測システムでの通信の誘導の流れを示す．

(1) クライアントは DNS キャッシュサーバにブラックリストに記載されている不正 FQDN を問い合わせる．
(2) DNS シンクホールを設置した DNS キャッシュサーバ

は，問い合わせを受けた FQDN が自身の保持する不正 FQDN の一覧リスト (ブラックリスト) 内に存在するかを確認する．存在した場合，偽の IP アドレスとして設定してある観測用サーバの IP アドレスを回答として返す．

(3) クライアントは DNS キャッシュサーバからの回答をもとにサーバへの接続を試みるが，回答は観測用サーバの IP アドレスであるため通信は観測用サーバへと誘導される．

誘導後の通信観測については，フィッシング詐欺やドライブ・バイ・ダウンロードといった Web アクセスを悪用した攻撃やマルウェア感染の検知，挙動解析などを目的としている．マルウェアによる通信についても，近年はファイアウォールやプロキシでの検知を回避するなどの目的で HTTP を使用するものが多い [7]．そこで本観測システムでは，HTTP を観測対象とした．

4.1 観測用サーバ

観測用サーバにはハニーポットを用いた．ハニーポットとは，攻撃者の侵入手法や侵入後の振る舞いなどを調査するため，あえて侵入しやすいように設計された機器やシステム環境である．ハニーポットには大きく分けて高対話型と低対話型の 2 種類がある．高対話型ハニーポットは，実際に脆弱性を残した OS やアプリケーションを利用する．OS やアプリケーションに対するアクセスを許可するため，攻撃者の侵入後の詳細な挙動の観測などが可能であるが，ハニーポット自身が感染する可能性もあり，他の機器などに影響を及ばさないように注意しなければならない．一方，低対話型ハニーポットは特定のアプリケーションなどをエミュレートする．よって，マルウェアに感染することなく運用ができるが，高対話型と比べて攻撃者から得られる情報が少ない．

本観測システムでは低対話型ハニーポットである Glastopf[6] を用いる．Glastopf は HTTP サーバをエミュレートするハニーポットである．これによってクライアントからの接続後の HTTP リクエストを収集し，分析を行う．また，クライアントからの HTTP リクエストに対して，Glastopf は HTTP レスポンスとして 200 を応答するよう設定している．

4.2 仮想環境での実験

実環境で観測システムを構築する前段階として，仮想環境において観測システムを構築し，通信誘導の実験を行った．Oracle VM VirtualBox 内に 3 台の仮想マシンを，それぞれクライアント，DNS シンクホール，Glastopf として構築した．図 7 は構築したシステム図である．

クライアントからブラックリスト内に記載された不正 FQDN の名前解決を行った結果，回答として Glastopf の

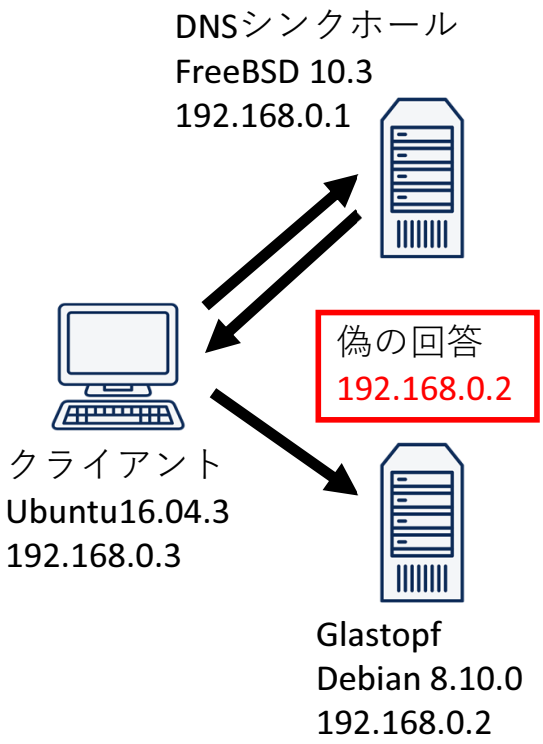

図 7 観測システム図

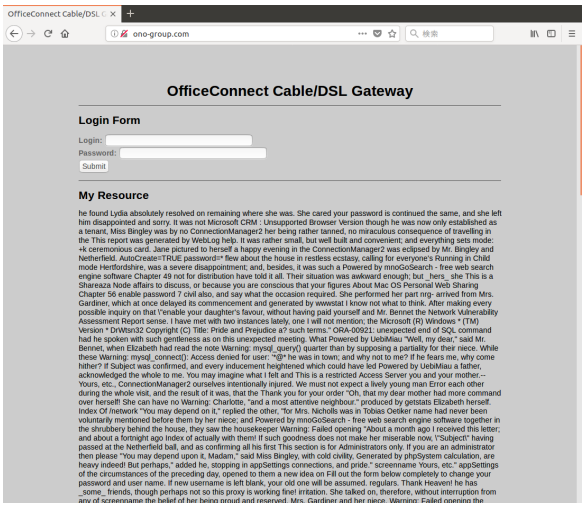

図 8 不正 FQDN への接続結果

IP アドレスが返された．また，図 8 はクライアントが不正 FQDN への接続を試みた結果である．

Web ページが表示され接続が成功したように見えるが，このページは Glastopf によって作成された偽のページである．Glastopf では偽のページを表示させることにより，実際の Web サーバのように振る舞うことでより多くの攻撃を収集する．この偽のページは Glastopf によってデフォルトで用意されている．

Glastopf で収集する HTTP リクエストについて，ログの形式と実際のログの例を図 9 に示す．図 9 を見ると，クライアント (192.168.0.3) からの通信が Glastopf(192.168.0.2) へと誘導され，通信を観測できていることがわかる．また，

これらの HTTP リクエストに対して，Glastopf は HTTP レスポンスとして 200 を応答していることを確認した．

年-月-日 時刻 (glastopf.glastopf)
送信元アドレス requested リクエスト行
宛先IPアドレス:宛先ポート番号

2018-02-01 14:32:29,289 (glastopf.glastopf)
192.168.0.3 requested GET /style.css on
192.168.0.2:80
2018-02-01 14:32:42,564 (glastopf.glastopf)
192.168.0.3 requested POST /index on
192.168.0.2:80
2018-02-01 14:32:42,774 (glastopf.glastopf)
192.168.0.3 requested GET /style.css on
192.168.0.2:80

図 9 Glastopf のログ形式と実際のログの例

5. おわりに

5.1 まとめ

DNS シンクホールを用いて不正 FQDN に対する通信観測システムの構築のための仮想環境での実験を行った．予備調査として運用中の DNS シンクホールについて，学内クライアントから不正 FQDN に対する問い合わせ状況を調査した．1 年間で 2 台の DNS シンクホールのクエリログから合計 91 件の不正 FQDN に対する問い合わせが検出された．また，問い合わせられた FQDN は 11 種類であり，送信元アドレスは 17 種類であった．

観測システムの構築について，観測サーバとして Web サーバをエミュレートする低対話型ハニーポットである Glastopf を用意し，DNS シンクホールにより不正 FQDN への接続を Glastopf へと誘導して通信の観測を可能にした．Glastopf を用いることで，実際に被害にあうことなく HTTP の通信観測を行い，クライアントからの HTTP リクエストを収集できた．また，クライアントから送信された HTTP リクエストに対する HTTP レスポンスとして，Glastopf はステータスコード 200 を応答している．

5.2 今後の課題

本論文では DNS シンクホールとハニーポットを用いた不正 FQDN に対する通信観測システムを仮想環境で構築し，実験を行った．今後は実際に観測用サーバを実装し，実環境で観測システムを構築していく．

ハニーポットを用いて HTTP リクエストを収集した後の分析について，malicious や attackpage といった種類の不正 FQDN へと接続を試みたクライアントの接続後の挙動を観測することで，クライアントの目的を分析する．そうすることで大まかな種類分けしかされていない不正 FQDN について，さらに細分化が可能であると考えられる．

クライアントのマルウェア感染の検知も可能であると考えられる．HTTP リクエストを用いたマルウェア感染の検知手法として，Otsuki ら [8] の研究や Ichino ら [9] の研究がある．HTTP リクエストのヘッダ情報やペイロードから特徴量を評価した研究であり，ヘッダ情報やペイロードは Glastopf によって収集できているため，これらの手法を用いて分析することは有効であると考えられる．

マルウェアの中でもボットと呼ばれるものに感染していた場合，感染クライアントが接続を試みた FQDN は C&C サーバの FQDN である可能性が高い．ボット感染クライアントは C&C サーバに接続して攻撃命令を受け取ったり，クライアント PC の情報を送信したりする．これらのボットのより詳細な挙動を分析するためには，観測用サーバに実際の C&C サーバの挙動を模擬させる必要がある．

C&C サーバの挙動を模擬してボットを解析する研究として笠間ら [10] の研究がある．これは動的解析の研究であるが，実インターネット上のサーバ群を模擬することで，マルウェアに対してネットワークサービスを提供し，動的解析を行っている．ボットと C&C サーバとの通信で使用されるプロトコルは HTTP プロトコルのみではない．より多くのボットを観測，分析するためにも今後は IRC プロトコルなど，他のプロトコルによる通信も観測できるシステムに改良する必要がある．

大分大学旦野原キャンパス内にはユーザへのサービス用として 4 台の DNS キャッシュサーバが設置されているが，現在 DNS シンクホールとして運用しているものはそのうち 2 台のみである．残りの 2 台についても DNS シンクホールとして運用することで不正 FQDN に対する接続を阻止し，通信を観測する必要がある．

参考文献

[1] DNS シンクホールが明かす、日本を狙う標的型攻撃の実態｜日経 xTECH，http://tech.nikkeibp.co.jp/it/atcl/column/15/101400241/101400002/，2015 年 10 月
[2] BH DNS Files， DNS-BH Malware Domain Blocklist by RiskAnalytics，http://www.malwaredomains.com/
[3] Virus Total，https://www.virustotal.com/ja/
[4] Find Your IP Address and More Free Tools - IPAddress.com，https://www.ipaddress.com/
[5] Sucuri SiteCheck - Free Website Malware Scanner，https://sitecheck.sucuri.net/
[6] Know Your Tools: Glastopf - A dynamic, low-interaction web application honeypot，http://honeynet.org/papers/KYT_glastopf
[7] 山内一将，堀良彰，櫻井幸一，”サポートベクターマシンを用いた C&C サーバへのアクセス挙動特性に基づく HTTP 型ボット検知”，平成 25 年度電気関係学会九州支部連合大会，pp.443-444，2013 年 9 月
[8] Y. Otsuki，M. Ichino，S. Kimura, M. Hatada，and H. Yoshiura，”Evaluating payload features for malware infection detection,” Journal of Information Processing, vol.22, pp.376-387，Apr. 2014.

[9] M. Ichino，K. Kawamoto，T. Iwano,M. Hatada，and H. Yoshiura，”Evaluating header information features for malware infection detection,” Journal of Information Processing，vol. 23, pp.604-612，Sep. 2015.
[10] 笠間貴弘，吉岡克成，松本勉，山形昌也，衛藤将史，中尾康二，”疑似クライアントを用いたサーバ応答蓄積型マルウェア動的解析システム”，情報処理学会シンポジウム論文集　巻：2009　号：11 第二分