Vol.2010-IOT-10 No.10
2010/7/16

迷惑メール判定精度向上を目的とした メッセージ内 URL の DNS レコード解析

諏訪秀治[†1]　山井成良[†2]
岡山聖彦[†2]　中村素典[†3]

近年，ワンクリック詐欺やフィッシング詐欺などを目的とする迷惑メールが増加している．これらの迷惑メールの対策技術に，本文内の URL や，URL の示す IP アドレスに注目して迷惑メール判定を行う DNSBL が存在する．しかし，迷惑メール送信者は Web サイトの構築にボットネット，fast-flux や DNS ワイルドカードといった手口を使用し，既存の DNSBL では迷惑メールと判定できないものが存在する．そこで，本研究ではメッセージ内 URL に関連した迷惑メール判別手法の判定精度向上のために，実際に迷惑メールのメッセージ内 URL から DNS レコードを取得し，特徴の解析を行った．その結果，DNS ワイルドカードの不正な使用の特徴が迷惑メール判定の基準として効果を示すことを確認した．

DNS Resource Record Anlysis of URLs in E-mail Messages for Improviing Spam Discrimination

Shuji Suwa,[†1] Nariyoshi Yamai,[†2]
Kiyohiko Okayama[†2] and Motonori Nakamura [†2]

In recent years, spam mails intending for “One click and charge claim”, “Phishing” and so on have become increasing. As one anti-spam technology, DNSBL based on the URLs or their corresponding IP addresses in the messages is well used. However, some spam mails that cannot be discriminated by conventional DNSBLs get appearing since the spammers create web sites using various techniques such as botnet, fast-flux and Wildcard DNS record. To improve the accuracy of discrimination of spam mails using these techniques, we analysed DNS record charasteristics corresponding to the domain name from the URLs in actual spam mails. According to the result of this analysis, we confirmed that improper use of Wildcard DNS record is one effective criterion for discrimination of spam mails.

1. はじめに

電子メールは WWW と並んで，社会的な活動を支える通信手段としてもはや必要不可欠な存在となっている．しかし，電子メールはセキュリティ面で問題の多いサービスでもあり，特に，宣伝や広告を目的として不特定多数の利用者に向けて送信される迷惑メールが社会問題となっている．米 Symantec 社によると，2010 年 4 月では迷惑メールは全電子メールの 90.1%を占めており[1)]，また，2009 年全体では迷惑メールの 90.6%で Web サイトの広告を目的とした URL の記載が見られたという[2)]．このような広告は一般の利用者にとって不要な情報であるうえに，これらの URL に対してアクセスを行うことで，(1) 個人情報の流出，(2) 不正ソフトウェア (マルウェア) への感染，(3) ワンクリック詐欺や通信販売を装った詐欺といった被害に遭う可能性がある．以降，本稿ではこのような悪質な Web サイトを構築し，迷惑メールを送信する者のことを攻撃者と呼ぶことにする．このような迷惑メールによる被害によって，利用者が便利に電子メールを使用できない状況になることを回避するために，迷惑メールへの技術的な対策が重要となっている．この対策手法の 1 つに電子メールに記載されているメッセージ内容を見ることで迷惑メールの判定を行う手法があり，その中でも，メッセージ内 URL を迷惑メール判定に使用する手法がある．しかし，近年では攻撃者も迷惑メールをフィルタリングされないために，より一層手口の巧妙化を進めている．

URL を利用した Web サイトの閲覧をさせるためには DNS の利用が不可欠である．そこで，本研究ではメッセージ内 URL の DNS レコードに注目した．迷惑メール内 URL で攻撃者が使用する手口としては，URL をメール毎に変更するものや，ユーザにアクセスさせる Web サーバを短時間に変更するものが挙げられる．また，攻撃者は Web サイトの構築にあたって，ボットネットを使用している可能性が高い．このような手口を使用した Web サイトの DNS レコードでは A レコードの生存時間が比較的短かく，また，応答される A レコードの数が通常のものに比べて多いと考えられる．また，DNS サーバがボット PC である場合，DNS サーバとしての動作が，通常の DNS サーバとは異なる部分があると思わ

†1 岡山大学 大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
†2 岡山大学 情報統括センター
Center for Information Technology and Management, Okayama University
†3 国立情報学研究所
National Institute of Informatics

れる．そこで，本研究は実際に迷惑メールのメッセージ内 URL から取得した DNS レコードの解析を行った．本稿ではその解析結果を報告する．

2. URL に基づく迷惑メール対策と攻撃者の対抗策

2.1 URL に関連する迷惑メール対策

迷惑メールの判定手法の一つに，メール本文に含まれる URL を使用する方法がある．URL が悪質かどうかを判断するためのブラックリストを DNSBL(DNS Block List) と呼び，SURBL(SPAM URL Realtime Black List)[3]，URIBL(URI Black List)[4]，ivmURI[5] といったものが存在する．メッセージ内の URL が示しているドメイン名やその IP アドレスが DNSBL に含まれていた場合，そのメールは迷惑メールであると判断される．迷惑メールの多くはメッセージ内に URL が付与されていることから，DNSBL は高い効果を期待できる．

しかし，DNSBL を使用するにはデータの更新が必要不可欠である．よって，次節で述べるように迷惑メール内の URL や使用されるホストの IP アドレスが頻繁に変更される場合，これらの URL が回避すべき URL かどうかを判定できない可能性がある．

2.2 URL に関連する攻撃者の手法

攻撃者は 2.1 節で述べた対策手法を回避するために URL に関した様々な手法を用いている．以下に，その方法についての説明をする．

URL の変化

攻撃者は不正に取得した個人情報により多数のドメインを次々と取得しているといわれ，[7] このため攻撃者の Web サイトの URL は様々に変更可能である．また，メッセージに毎回同じ URL を記載すると，ブラックリストによって迷惑メールと判断されるため，メール送信毎にサブドメイン以降の部分をランダムな名前に変更しているものがある．

IP アドレスの変化

サーバの負荷を分散するために使用される技術に DNS ラウンドロビン[6] がある．近年では，攻撃者がこの手法を利用した fast-flux[7] と呼ばれる手口を用いることで，Web サイトとして使用されるサーバの IP アドレスを短時間で変化させている．さらに攻撃者は所有するネームサーバに登録するリソースレコードそのものも短時間で変更している．よって，ユーザがこのような Web サイトアクセスし，しばらく時間が経過した後でそのサイトが悪質なものであると判明した場合，攻撃に使用されたサーバの IP アドレスを突き止めることが困難となる．また，これにより IP アドレスベースのブラックリストの効果が低減されることとなる．

3. メッセージ内 URL の DNS レコード解析方法

2.2 節で述べたように，攻撃者は悪質な Web サイトをインターネット上で活動させるために様々な手段を用いており，2.1 節で挙げたような URL に関する迷惑メール判定手法を使用しても，それを回避するものが存在する．しかし，攻撃のために構成された Web サイトに関する DNS レコードからは，通常とは異なる傾向が見られると考えられる．そこで，メール内 URL から得られる FQDN(Fully Qualified Domain Name) をもとに各種 DNS レコードを収集し，迷惑メール判定に活かせるような特徴の発見を目指した．

3.1 解析方法の検討

迷惑メール内の URL から DNS レコードを取得し，解析することで，通常の Web サイトにおける DNS レコードとは異なる特徴が現れると思われる．本節では，攻撃者が 2.1 節で述べた手口を使用する場合に現れる可能性の高い特徴と，それらを検証するために必要な情報について説明する．

応答される A レコード数

攻撃者が用意した Web サイトでは，2.1 節で述べたような fast-flux 手法が使用されている可能性がある．この場合，ネームサーバには同じ FQDN に対して多数の A レコードを保持している．したがって，迷惑メールに記載されている FQDN の A レコードを取得すると，比較的多数の A レコード応答が応答されると考えられる．そこで，各 FQDN 毎に取得できる A レコード数を調べ，迷惑メール内 URL の特徴を検証する．

A レコードの生存時間の値

攻撃者は短時間で FQDN に対する IP アドレスを変更し，クライアントに古い IP アドレスをキャッシュさせないように，A レコードの TTL 値を小さく設定していると考えられる．したがって，迷惑メール内の URL で使用される A レコードの TTL 値は比較的小さいと思われる．そこで，各 FQDN の A レコードの TTL 値を調べ，このような特徴が現れるかどうか検証を行う．

ネームサーバの異常動作

攻撃者はボット PC をネームサーバとして動作させている場合があり，このとき，ボット PC を既存のネームサーバと同じように振る舞わせる何らかのツールを使用していると思われる．これらのツールが，通常のネームサーバには見られない動作をしている

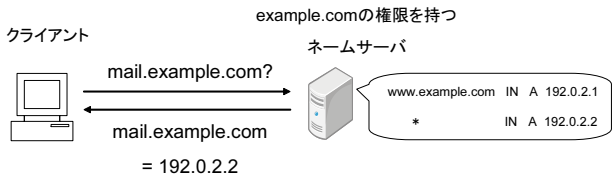

図 1 DNS ワイルドカードを使用したネームサーバの例
Fig. 1 An example of the name server using Wildcard DNS record

可能性がある．例えば，通常得られるはずのレコードが応答されない，あるいはネームサーバとして応答を行わない，DNS ワイルドカード[8] の使用範囲が管理権限を逸脱しているなどが挙げられる． DNS ワイルドカーとは，ネームサーバが管理する名前空間において，設定しておいた名前以外に対して IP アドレスを応答する機能である．図 1 にその動作の一例を示す． example.com というドメイン名を管理するネームサーバで www.example.com には IP アドレス 192.0.2.1 を，サブドメインに www 以外を持つ FQDN に対しては 192.0.2.2 を応答する．2.1 節で，メール毎に URL のホスト名部分が異なるメールが存在すると述べたが，この手口の場合，ホスト名の変更とネームサーバで管理するリソースレコードの変更を連動させる必要がある．この処理を簡略化させるために，攻撃者は DNS ワイルドカード，あるいは異なるドメイン名に対しても同じ IP アドレスを応答するような仕組みのネームサーバを使用していると考られる．そこで，攻撃者が使用するネームサーバの特徴を検証するために，各 FQDN 毎に DNS ワイルドカードを使用したネームサーバが応答を行っているかどうかを調べる．

3.2 DNS レコード収集方法

迷惑メールのメッセージ内 URL は時間が経過すると，使用サーバやドメイン名が各関連団体 (国，ISP，ドメインの登録機関など) によって検挙され，DNS を使用してもリソースレコードが得られないことがある．そのため，メッセージ内 URL に対する DNS レコードの取得はメールを受信した直後に行う必要がある．そこで，各メール受信時に DNS レコードやワイルドカード使用に関する情報を取得するようにした．メール受信時における，これらの情報取得の流れを以下に示す．

(1) 電子メールを受信する．
(2) メールサーバは，メール受信時に，自作プログラム (以降，プログラムと呼ぶ) を起動させる．このプログラムはメール本文を入力とする．
(3) プログラムは，メール本文から URL を抜き出し，これらから FQDN 部分を取得する．
(4) プログラムは，取得した FQDN 毎に，DNS キャッシュサーバを使用して情報を取得し，保存する．
- FQDN に対する A レコード，NS レコード，SOA レコードを DNS キャッシュサーバに問合せて取得する．また，NS レコードに示されているネームサーバの IP アドレスもキャッシュサーバにより取得する．
- 後述する方法で，各ネームサーバ毎の DNS ワイルドカード使用の情報を調べる．

(5) DNS キャッシュサーバは，プログラムの代わりにネームサーバ群に対して問合せを行う．なお，各問合せ結果をプログラムへ渡した後，キャッシュ内容を破棄する．
(6) まだ調べていない FQDN があれば 4 へ，無ければ終了する．

上記の手順 4 で述べたように，プログラムでは DNS レコードに加えて，各 FQDN を管理しているネームサーバの DNS ワイルドカード使用の有無と DSN ワイルドカードが適用される範囲を調べた．これは，ネームサーバに対して，FQDN をランダムなアルファベットに変更した際の応答を調べることで判定できる．メッセージ内 URL の FQDN 部分が www.example.com の場合を図 2 に示す． まず，www.example.com の A レコードを取得し，IP アドレスを得る．次に，サブドメイン部分 (www 部分) をランダムなアルファベットの文字列（図 2 中では random と記述）に変更し，www.example.com の A レコードと同じ IP アドレスが応答されるかどうかを調べる．ここで，同じ IP アドレスが応答された場合，DNS ワイルドカードがサブドメイン以降で使用されていると判定できる．さらに，ランダムな文字列単体でも A レコードを問合せ，ここでも同じ IP アドレスが応答された場合，トップレベルドメイン以降で DNS ワイルドカードを使用していると判定できる．

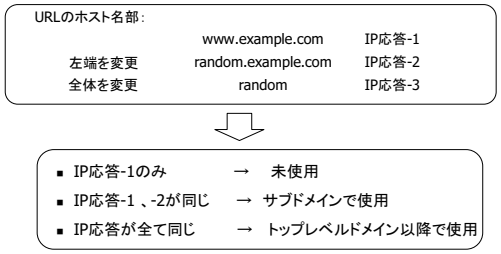

図 2 DNS ワイルドカード使用範囲の判定
Fig. 2 Classification of the range of using Wildcard DNS record

Vol.2010-IOT-10 No.10
2010/7/16

4. メッセージ内 URL の DNS レコードの解析結果

まず，3.2 節で述べた方法を使用して筆者が DNS レコードの取得を行ったときの環境と，サンプルとして使用したメールについての説明を 4.1 節で行う．続いて，4.2 節で 3.1.2 節で述べたような傾向について検証，考察を行う．

4.1 実験環境

まず，本実験で使用したメールサンプルについて説明する．迷惑メールのサンプルとしては，迷惑メールでありながらも，従来の迷惑メール判定手法によって非迷惑メールと判断されてしまうようなものを扱うべきであるが，このようなメールを多数取得することが困難であったため，従来手法で迷惑メールだと判定されたものを使用した．また，URL をメッセージに含む非迷惑メールのサンプルとして，メールマガジンサービスにより配送される電子メールを使用した．本実験でサンプルとして使用したメールは以下の 3 種類である．

(1) 本研究室で使用しているメールサーバ (以降，メールサーバ A と呼ぶ) に届いたメールの内，既存のフィルタリングツールを用いて迷惑メールと判断されたもの，あるいは，メーリングリストに存在しないユーザーに宛てられたもの

(2) 個人の所有するあるメールサーバ (以降，メールサーバ B と呼ぶ) に届いたメールの内，SpamAssassin[9] によって迷惑メールと判断されたもの

(3) メールマガジンサービスによって配送されたもの

これらのメールを受信するにあたって，筆者が実際に使用した環境を図 3 に示す．

サンプルとして受信した電子メールの件数と，その本文中に含まれていた URL より抽出した FQDN 件数を表 1 に示す．

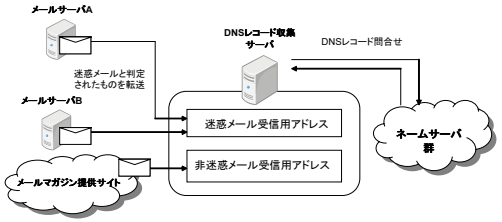

図 3 DNS レコード解析を行った環境
Fig. 3 Environment for DNS record analsys

表 1 受信メール件数とメッセージ内 FQDN 数
Table 1 Counts of received e-mails and included FQDNs

	迷惑メール	非迷惑メール
受信メール (件)	10395	1062
FQDN(件)	7035	732

4.2 解析結果

本節では，4.1 節の環境で取得したデータを元に検証，考察を行う．3.1 節で述べた各項目を検証する前に，本実験でサンプルから得られた，FQDN，ドメイン名，ホスト IP アドレス，ネームサーバ名，ネームサーバ IP アドレスの総数を表 2 に示す． 表 2 を見ると，迷惑メール側では FQDN 数 7035 件に対して，誘導先ホストの IP 数が 329 件と少ない結果となった．この結果と DNS ラウンドロビンの使用に関しては，4.2.1 節と 4.2.2 節で詳しく述べることにする．また，IP アドレスの数に対して URL の数が多数確認されたことについては，4.2.3 節で DNS ワイルドカードの使用に関する結果とともに述べることにする．

4.2.1 A レコード数

本節では，メールに含まれる FQDN の A レコード数の結果を元に考察を行う．各メールの FQDN 毎の A レコード数を表 3 に示す． 表 3 を見ると，迷惑メール側の FQDN では A レコードを 1 件しか持たないものが 99.59%，複数の A レコードを持つものが 0.41%という結果となった．したがって，今回のサンプルのからは，ネームサーバに多数の A レコードを登録し IP アドレスの変更を行う手口が少数しか見られなかったといえる．また，表 1 に示した迷惑メール側の FQDN の総数とそれらに対して使用されていたホスト IP アドレスの総数を見ると，後者が極端に少なく思える．このような結果になったのは，攻撃者が IP アドレスはあまり変更せず，FQDN あるいはその一部分を頻繁に変更して Web サイトを運用していたためだと考えられる．一方で，非迷惑メール側では 1 件の A レコードを持つのものが 82.24% 複数の A レコードを持つものが 17.76% という結果となり，非迷惑メール

表 2 各種データの総数
Table 2 The total count of various data

	迷惑メール	非迷惑メール
FQDN(件)	7035	732
ドメイン名 (件)	1705	533
ホスト IP アドレス (件)	329	758
ネームサーバ名（件）	2297	1078
ネームサーバ IP アドレス（件）	539	989

表 3 FQDN 毎の A レコード数
Table 3 Counts of A-record per FQDN

A レコード数	迷惑メール内 FQDN		非迷惑メール内 FQDN	
	件数	割合 (%)	件数	割合 (%)
1	7006	99.59	602	82.24
2	24	0.34	88	12.02
3	0	0.00	10	1.37
4	2	0.03	9	1.23
5	0	0.00	2	0.27
6	2	0.03	11	1.50
7	0	0.00	7	0.96
8	0	0.00	2	0.27
9	0	0.00	0	0.00
10 以上	1	0.01	1	0.14

側の FQDN が多数の A レコードを持つという結果になった．この結果については 4.2.2 節で A レコードの TTL 値について検証する際，あわせて考察を行うことにする．

4.2.2 A レコードの生存時間

表 4 に各 FQDN で設定されていた TTL 値の割合を示す．迷惑メール側では TTL 値が 0 秒〜3600 秒の FQDN は 96.26%を占めており，中でも，TTL 値が 1801 秒〜3600 秒のものが 89.24%と集中していた．一方で，非迷惑メール側でも TTL 値が 0〜3600 秒の FQDN が 70.36%存在し，この内，43.58%が 0〜900 秒と非常に短時間に設定されていた．4.2.1 節で述べたように，非迷惑メールでも複数の A レコードを使用している FQDN が存在していることから，非迷惑メール内の URL においても DNS ラウンドロビンが使用されている場合があるとわかる．この場合，DNS ラウンドロビンは本来の目的である，サーバの負荷分散のために使用されていると考えられる．すなわち，使用するユーザの多いサイトほど，DNS ラウンドロビンの特徴が大きく現れる可能性が高い．したがって，A レコードが多い，あるいはそれらの TTL 値が短いというだけでは迷惑メールの判定をすることは難しいと思われる．しかし，TTL 値が 3600 秒を超える FQDN が，迷惑メール側では 3.47%，非迷惑メール側では 29.64%であったことを考えると迷惑メール内 FQDN の TTL 値は比較的小さいということがいえる．

表 4 A レコード毎の TTL 値
Table 4 TTL of each A-record

TTL 値	迷惑メール内 FQDN		非迷惑メール内 FQDN	
	件数	割合 (%)	件数	割合 (%)
0〜900	433	6.15	319	43.58
901〜1800	61	0.87	30	4.10
1801〜3600	6278	89.24	166	22.68
3601〜10800	20	0.28	35	4.78
10801〜21600	35	0.50	63	8.61
21601〜43200	14	0.20	10	1.37
43201〜86400	190	2.70	105	14.34
86401〜172800	2	0.03	3	0.41
172801〜	2	0.03	1	0.14

4.2.3 DNS ワイルドカードの使用範囲と SOA レコードの有無

4.2.1 節，4.2.1 節で述べたように，今回のサンプルからは IP アドレスを多数運用し，DNS ラウンドロビンによって使用させる IP アドレスを変更させる手口はあまり見られなかった．しかしながら，迷惑メール毎で URL のホスト名部分を変更している手口が多く確認できた．これに関連して，DNS ワイルドカードの使用について検証を行う．3.1 節で述べたように各ネームサーバ毎に図 2 に示した方法で DNS ワイルドカードの使用されている範囲を調べた．各 FQDN 毎の NS レコードに現れるネームサーバの内，DNS ワイルドカードの使用範囲が最も大きかったものをその FQDN の DNS ワイルドカード使用範囲とみなした．表 5 は各 FQDN 毎の DNS ワイルドカード使用範囲を示している． まず注目すべき点は，迷惑メール側でのみトップレベルドメイン以降で DNS ワイルドカードを使用する FQDN が多数存在していた点である．つまり，3.1 節で述べたような DNS ワイルドカードを使用したネームサーバが存在しており，これらを使用してメール毎で FQDN を変更していたと考えられる．また，サブドメインでの使用は非迷惑メール内の FQDN でも使用されていた．

次に，各ネームサーバ IP 毎の DNS ワイルドカード使用範囲を表 6 に示す． 表 6 によると，実際トップレベルドメインでの DNS ワイルドカードを使用していたネームサーバの IP アドレスは 34 件であった．表 5 でトップレベルドメイン以降で DNS ワイルドカードが使用されていた FQDN が 5948 件であったことを考えると，この数値は極端に少数である．また，SOA レコードの有無と DNS ワイルドカードの使用範囲には関連性があることが判っ

表 5 FQDN 毎の DNS ワイルドカード使用範囲
Table 5 The range of using Wildcard DNS record of each FQDN

	未使用	サブドメイン以降	トップレベルドメイン以降
迷惑メール内 FQDN（件）	336	751	5948
非迷惑メール内 FQDN（件）	637	95	0

表 6 ネームサーバ IP アドレス毎の DNS ワイルドカード使用範囲
Table 6 The range of using DNS Wildcard record of each name server IP

	未使用	サブドメイン以降	トップレベルドメイン以降
迷惑メール側ネームサーバ IP（件）	364	141	34
非迷惑メール側ネームサーバ IP（件）	810	179	0

た．表 7 に各 FQDN 毎の SOA レコードの有無と DNS ワイルドカード使用の範囲を示す．迷惑メール側では，通常であれば得られるはずの SOA レコードを得られない FQDN が存在した．さらに，トップレベルドメインで DNS ワイルドカードを使用している FQDN からは，SOA レコードを得られないことが多いという結果となった．このような結果が現れたのは，攻撃者が Web サイトの構築にあたって，DNS サーバとして振舞うようなツールを使用しているためだと考えられる．迷惑メール側で DNS ワイルドカードを使用していない，あるいはサブドメイン以降で使用している FQDN で，SOA レコードが欠如しているものも存在した．これは DNS ワイルドカード使用範囲の判定の際に，ネームサーバのリソースレコードが変更されたり，一時的なネットワーク障害などによりネームサーバの応答の待ち時間が増加し，正しく範囲を測定できない FQDN が存在したためであった．

以上の結果より，FQDN をメール毎に変更する手口を使用している場合，攻撃者は DNS ワイルドカードを使用している可能性が高く，また，FQDN に対して SOA レコードが欠如している場合，その FQDN は高い割合で有害なものであると考えられる．したがって，これらを調べることで，攻撃者によって URL や IP アドレス，ネームサーバなどが頻繁に変更されるような場合でも，有害な URL か判定するための要素として機能し，最終的には，迷惑メール判定にも活用できると考えられる．

5. おわりに

本論文では，迷惑メール判別の精度を向上するために，メッセージ内 URL の DNS レコード解析を行った．従来の迷惑メール判別手法によるフィルタリング回避や，攻撃元の隠蔽を目的として攻撃者が使用している様々な手法が DNS レコードに特徴として現れるか検証した．その結果，本実験で取得したサンプルの場合，A レコード数とレコード生存時間に関して，攻撃者が使用する fast-flux 手法と同じ特徴が非迷惑メール側にも現れた．したがって，この二つの項目だけでは，迷惑メールの判別を行うことが困難であるとこと判った．しかし，攻撃者の使用しているネームサーバは，任意のホスト名の IP アドレス解決要求に対して同一の IP アドレスを応答する場合があり，加えて，これらは SOA レコードの応答を行わない可能性が高いという特徴を発見した．また，このようなネームサーバの IP アドレスが変更される頻度は極めて少ないことが判った．

今後の課題として，ハニーポットを設置し，従来の迷惑メール判別手法によって判別可能な迷惑メールと不可能な迷惑メールを分類して評価することが必要である．また，各 URL 毎の，時間経過による DNS レコードの変化，各ドメイン名の登録時期などの検証を行い，より詳細な DNS レコードの解析を行う必要がある．

表 7 FQDN 毎の SOA レコード有無別 DNS ワイルドカード使用範囲
Table 7 The range of using Wildcard DNS record based on the existence SOA record of each FQDN

	SOA レコード有無	未使用	サブドメイン以降	トップレベルドメイン以降
迷惑メール内	有り	311	750	1
FQDN(件)	無し	25	1	5947
非迷惑メール内	有り	637	95	0
FQDN(件)	無し	0	0	0

参 考 文 献

1) Symantec, “‘Behind the Scenes’ of Spam URLs; New Internet in Africa Attracts Spam Botnets; Soccer World Cup Themed Malware, ” MessageLabs Intelligence Reports, May 2010
http://www.messagelabs.com/mlireport/MLIReport_2009_05_May_FINAL.pdf
2) Symantec, “2009 Annual Security Report, ”MessageLabs Intelligence Reports , 2009
3) “SURBL, ”http://www.surbl.org/
4) “URIBL.COM, ”http://www.uribl.com/
5) ivmURI , “a URI blacklist, ”http://dnsbl.invaluement.com/ivmuri/
6) RFC 1794 ,DNS Support for Load Balancing
http://tools.ietf.org/html/rfc1794
7) 日経 BP 社，ITpro, “攻撃の高度化,「Fast-Flux」から「RockPhish」まで，”
http://itpro.nikkeibp.co.jp/article/COLUMN/20071211/289199/
8) 株式会社日本レジストリサービス，森下泰宏，“DNS ワイルドカードに関する技術的特徴と課題– Site Finder サービスを中心に–， ”
http://jprs.jp/tech/material/DNS-wildcard-20031008.pdf
9) Apache Software Foundation, The Apache SpamAssassin Project
http://spamassassin.apache.org/