迷惑メール判定精度向上のための メッセージ中URLのドメイン登録日検索システム

松岡 政之[1,a)]　山井 成良[2]　岡山 聖彦[2]　河野 圭太[2]　中村 素典[3]　民田 雅人[4]

概要：
近年，ワンクリック詐欺やフィッシング詐欺などの悪意あるWebページへの誘導などを目的とした多くの迷惑メールが送信されている．迷惑メール対策の技術的な手法の一つとして，迷惑メール内のURLをブラックリスト化して照合を行う，URLブラックリストと呼ばれる手法が存在する．しかし，攻撃者はドメインを使い捨てとし，新たに取得したドメインを宣伝または攻撃用Webページに用いることによって，メールメッセージ内のURLを変更する手口を使用し始めており，既存のブラックリストでは迷惑メールと判定できないものが現れている．本研究は，迷惑メール本文中のドメイン登録日に注目し，迷惑メール判定手法の判定精度向上を目的とするものである．そこで，各ドメインごとにその登録日を収集・記録するシステムの設計と実装を行った．このシステムによりDNSを用いてドメインの登録日を検索することが可能になった．

キーワード：電子メール，迷惑メール，ドメイン，whois，DNS

Domain Registration Date Retrieval System of URLs in E-mail Messages for Improving Spam Discrimination

Matsuoka Masayuki[1,a)]　Yamai Nariyoshi[2]　Okayama Kiyohiko[2]　Kawano Keita[2]
Nakamura Motonori[3]　Minda Masato[4]

Abstract: In recent years, many spam mails intending for “One-click fraud” or “Phishing” have been sent to many unspecified e-mail users. As one anti-spam technology, URL Blacklist based on the URLs in the spam mails is well used. However, spammers have been avoiding this technique by getting many new domains, using them only in a few spam mails, and throwing them away. In this paper, we focus on the domain registration date related to the URLs in the messages in order to improve the discrimination accuracy of spam mails. Thus, we address design and implementation of the domain registration date retrieval system which obtains domain lists from some Top Level Domain registories and records registration dates for each domain in the lists. With this system, we can retrieve the registration date of a domain by DNS.

Keywords: E-main, spam mail, domain, whois, DNS

1. はじめに

近年，インターネット利用者の増加に伴い，WWWと並んで電子メールは非常に多く人に利用され，社会的な活動を支える通信手段として必要不可欠なものとなっている．

1 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology Okayama Uniersity
2 岡山大学情報統括センター
Center for Information Technology and Management Okayama Univercity
3 国立情報学研究所
National Institute of Informatics
4 株式会社日本レジストリサービス
Japan Registry Services Co., Ltd.
a) matsuoka@dist.cne.okayama-u.ac.jp

しかし，電子メールのサービスにはセキュリティ面での問題が多く，特に，宣伝や広告を目的をした不特定多数の利用者に送信される迷惑メールが社会問題となっている．Symantec Intelligence Report の 2012 年 7 月の発表によると，全電子メールトラフィックの 67.6%を迷惑メールが占めている [1]．これらの迷惑メールによって，(1) 通信資源や計算機資源，通信費用や通信時間などを無駄に消費する．(2) 迷惑メールの区別に多大な労力を必要とし，また正当なメールを迷惑メールと共に誤って削除したりする．(3) 迷惑メールの送信元などとして名前を騙られた場合や，迷惑メールの中継に組織内のメールサーバが使用されることによって，その組織が迷惑メールの送信に関与していると疑われる．などの深刻な問題が発生している．また，迷惑メールの多くはメッセージ中に URL が記述してあり，その URL にアクセスすることによって悪質なサイトに誘導され，コンピュータウィルスに感染したりフィッシング詐欺やワンクリック詐欺などの詐欺行為の被害にあうなどの問題も深刻である．

このような問題に対して，現在様々な対策が施されている．その一つとして，電子メールに記載されているメッセージの内容を基に迷惑メールを判別する方法があり，その中でも URL のブラックリスト[*1]を作成し，受信メールメッセージ内の URL と照合することによって迷惑メールを判別する方法がある．迷惑メールの多くはメッセージ内に URL が記述されているため，この手法は高い効果を期待できる．しかし，近年では攻撃者はこの方法に対抗するために新たなドメインを頻繁に取得し，メッセージ内の URL に使用するドメインを使い捨てにする手口を使用し始めている．これによって，迷惑メールに記述する URL が頻繁に変更され，URL のブラックリストが無効化されてしまう．

新たなドメインを次々に使用するには，頻繁に新たなドメインを取得していかなければならない．そこで本研究では，迷惑メールに使用されるドメインの登録日に注目した．迷惑メール中に含まれる URL に現れるドメイン（以下，誘導ドメイン）の登録日は比較的短いことが先行研究 [2] により知られており，この特徴を用いれば誘導ドメインの登録日を迷惑メール判定指標の一つとして用いることで迷惑メール判定精度の向上が見込める．

ところが，先行研究でドメイン登録情報の検索に使用している WHOIS サービスの多くでは，頻繁な検索に対する制限が設けられているため，これをそのまま迷惑メール判定に用いることができない．そこで，本稿では代表的な TLD (Top Level Domain）レジストリが提供しているゾーン情報に基づき，含まれている各ドメインについてその登録日を収集・記録し，与えられたドメイン名に対してその登録日を検索できるシステムを提案する．

以下，2 章では迷惑メールの現状の対策とその問題点を述べ，3 章でその問題点を解決する提案システムの実現方針について述べ，4 章では提案システム実装について述べ性能を評価する．最後に，5 章で本論文をまとめ，今後の課題について述べる．

2. 迷惑メールと対策の現状

2.1 迷惑メールの手口とその対策手法

迷惑メール送信者は，自身や攻撃に使用される Web サーバを突き止められることを防いだり，より多くのメールがブロックされずに送信先へ届くようにするために，さまざまな手法を用いている．

2.1.1 迷惑メールの送信手法と対策

古くから用いられてきた方法として，設定の不十分なメールサーバを利用することにより自身の用いるネットワークの特定をしづらくする方法や，送信元を偽って送信者を特定しづらくする方法がある．これらの攻撃方法には，迷惑メールの送信元の IP アドレスやドメインのブラックリストを用いる DNSBL(DNS Blacklist) や，正当なメールサーバからの送信か否かを確認する送信ドメイン認証が用いられている．

また，10 年ほど前から一般ユーザの PC を大量にコンピュータウィルス等の悪意のあるソフトウェアに感染させることによって，外部ネットワークから操作し，迷惑メールの送信などに用いるボットネットと呼ばれる手法が使われ大きな問題となっている．

2.1.2 DNSBL の問題点

DNSBL では送信元に基づくブラックリストによってメールをフィルタリングする．しかし，正当なメールサーバが迷惑メール送信の中継として利用されることによって不正な送信元だと判断されてブラックリストに登録されたり，誤ってブラックリストに登録されてしまった場合，正当なメールも受信することができなくなってしまう．

また，一般に提供されている DNSBL の一覧にはポリシーが不明確なものもあり，必ずしも信頼できないものが存在する．

2.1.3 メール本文に基づく迷惑メールフィルタリング

上記の対策以外に，メールの内容に関して迷惑メールフィルタを用いて受信を抑制する対策も講じられている．多くの迷惑メールは宣伝や，悪意ある Web サイトへの誘導，ウィルスの配布などを主目的としており，その内容に共通点や同様の特徴が見られる．そこで，迷惑メールに多く使われる内容を統計的に処理して，迷惑メールを判定する．

また，メッセージ内の URL に関して，URL ブラックリストと呼ばれるものが存在する．これは，メッセージ内 URL が悪質かどうかを判断するためのブラックリストであり，

[*1] 実際にはドメイン部のブラックリスト

代表的なものとして SURBL[5] や URIBL[6]，ivmURI[7] がある．これらのブラックリストは，迷惑メールメッセージ内のクリック可能なリンクにあるドメインを一覧にしたものである．迷惑メールメッセージ内から全 URL を抜き出し，それをブラックリストと比較し，一致すれば迷惑メールと判断してブロックできる．この手法は，迷惑メール送信者が送信元を偽っても有効であり，また，多くの迷惑メールがメッセージ内に URL の記述を持つため，高い効果を期待できる．

2.1.4 URL ブラックリストの問題点

迷惑メールの送信元や誘導先などに不正に使用されたドメイン（悪性ドメイン）は，一般的には不正使用が判明するとレジストリによって停止される．その対抗手段として，攻撃者は不正に入手した個人情報によって次々と新しいドメインを取得する．こうして取得したドメインを使用し，攻撃用サイトを活動させることにより，迷惑メールメッセージ内の URL も頻繁に変更することができる．

このような手口で取得，使用されたドメイン（使い捨てドメイン）は大量に存在し，また使用頻度が比較的少ないため，URL ブラックリストへの登録が追い付いていない．また，このようなドメインは長期間使われることがないため，たとえ URL ブラックリストへ登録されたとしても実際に使い捨てドメインが検索される機会は少ないと思われる．

これらのことから，URL ブラックリストは使い捨てドメインに対する有効性が損なわれており，迷惑メールを判別する能力に疑問が生じている．

2.2 ドメイン登録日に基づく迷惑メール判定手法

前節で述べたように，URL ブラックリストではドメインを使い捨て，URL を頻繁に変更する攻撃方法には対応できない．そこで，ドメインを使い捨てるには頻繁に新しいドメインを取得しなければならず，登録日からの経過日数の浅いドメインを URL に用いたメールほど迷惑メールである可能性が高いと考えられる．そのためには，メールメッセージ内の URL に使用されている各ドメインの登録日を調べる必要がある．

先行研究において JWSDB というブラックリストに登録されているドメインに関して，そのドメインの登録情報を調べたものがある [2]．それによると，約半数の登録者は一つしかドメインを所持していないが，割合的に少数の登録者が複数のドメインを所持している．また，93%のドメインがそのような登録者によって同じ日にほかのドメインと共に登録されており，80%のドメインが 10 個以上のまとまりとして登録されている．このことからも，ドメインの登録日を迷惑メール判定の指標に用いることは多くのドメインに対して有用であると考えられる．

そこで，ドメインの登録日を調べる方法に WHOIS を用いる方法がある．WHOIS とは IP アドレスやドメインの登録者などに関する情報を，インターネットユーザが誰でも参照できるサービスである [8]．WHOIS を用いることで，ドメイン名やレジストラ名，ドメインの登録年月日などさまざまな情報を参照することが可能である．レジストラが提供する情報は，IP アドレスやドメイン名などのインターネット資源を管理する ICANN という組織によって規定されている [9]．これらの情報は，(1) ネットワークの安定的運用を実施する上で，技術的な問題発生の際の連絡のために必要な情報を提供．(2) ドメイン名の申請届出時に，同一ドメインや類似ドメインの存在を確認するために必要な情報を提供．(3) ドメイン名と商標等に関するトラブルの自立的な解決のために必要な情報を提供．といった目的で公開されている．

しかし WHOIS は，マーケティングなど本来の目的外で使用されることを避けるため，検索頻度の高いユーザを一時的に制限したり，検索時間に間隔を持たせるなど，WHOIS 情報への大量アクセスを避ける対策がなされている．また，WHOIS はそのフォーマットが定められていないため，提供団体によってフォーマットが不均一であり，プログラムによる解析が非常に困難である．そのため，迷惑メール判定のためにメールメッセージ内 URL のドメインに関して WHOIS 情報の検索を行う場合，すべての受信メールに関して検索を行うことは事実上不可能である．

3. ドメイン登録日収集方法の提案

2.3 節で述べたように，迷惑メール判定のために WHOIS を用いてドメインの登録日を調べることは不可能である．そこで，本章ではドメインの登録日を容易に検索できるようにするための提案手法について述べる．

3.1 実現方針

WHOIS を使用せずドメインの登録日を直接調べる方法はない．しかし，一部のトップレベルドメインに関しては現在登録されているドメインの一覧を取得することが可能である．そこで，この一覧を用いて 1 日ごとの登録されているドメインの一覧を比較することによって，新しく登録されたドメインを見つけることが可能であり，新しいドメインの登録が確認された日を登録日とすることで，各ドメインの登録日を調べることができる．この方法では大量のアクセスなどは必要なく，ドメイン数に関わらず登録日を調査することが可能である．厳密には，WHOIS で得られるドメインの登録日とゾーン情報への登録日は必ずしも一致するとは限らない[*2]が，迷惑メールの判定には大きな影響を与えないと思われる．

また，受信メールを判別するたびにそのドメインの登録

[*2] ドメイン名の不正使用を防ぐため，登録はされているが使用されてないドメインが存在する．

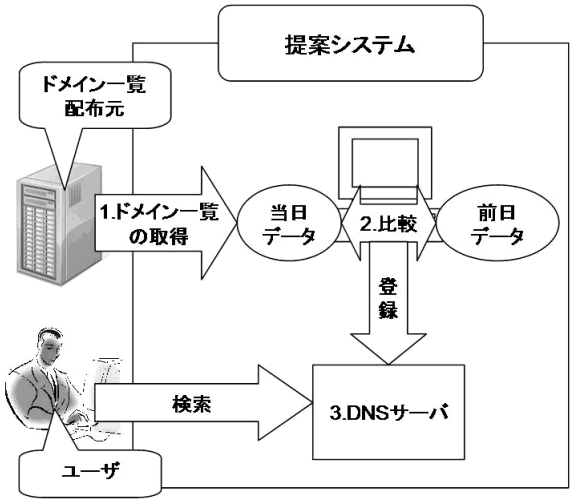

図 1 提案システムの構成
Fig. 1 The layout of the proposal system.

日を問い合わせる必要があるので，WHOIS のように登録日を容易に問い合わせることができるような機能が必要である．そこで，同様にドメイン名を用いて問い合わせを行う DNS のシステムに注目した．DNS の正引きではドメイン名を用いて問い合わせを行い，それに対応した IP アドレスを返す．それを利用し，応答に用いる情報を IP アドレスではなく登録日とすることで，ドメイン名から容易にその登録日を問い合わせることが可能になる．よって，実装システムには DNS サーバとしての機能をもたせる必要がある．

以下，本章ではこの方針を実現するための提案システムの設計について述べ，次章で実装について述べる．

3.2 システムの設計

提案システムは図 1 に示す構成となっており，各ブロックでは次に示すような機能を持つ．

(1) ドメイン一覧の取得
毎日 1 度，ドメイン一覧の配布元から最新のドメイン一覧をダウンロードし入手する．また，入手したドメインの一覧から必要な情報のみを抽出し，データを処理しやすくしておく．

(2) ドメイン一覧の比較
前日のドメイン一覧と入手した最新の一覧の比較によって，新規に登録されたドメインと削除されたドメインを割り出し，差分情報を生成する．

(3) DNS サーバ
DNS サーバとして検索が可能になるよう，ドメインとその登録日のデータを DNS ゾーンファイルとして記録するため，前の処理で作成された差分情報から登録日を記録したゾーンファイルを更新する．
また，通常の DNS の問い合わせと同様に dig や nslookup といったコマンドで，ドメイン名からそのドメインの登録日を検索できる．

表 1 トップレベルドメイン名に基づくスパム URL 分布 [1]
Table 1 Spam URL Distribution based on Top Level Domain Name.

ドメイン	迷惑メールに占める割合 (%)
com	63.9
ru	8.3
net	6.9
br	3.7

4. システムの実装と性能評価

本章では，3 章で示したシステム構成の実装方法について述べ，本システムを実行した場合の性能について評価する．

4.1 システムの実装と処理手順

実装システムでは以下に示す処理を毎日 1 度行うことによって，常に最新のデータを参照できるようにする．

4.1.1 ドメイン一覧の入手

多くの TLD ではゾーン情報を提供するサービスがあり，今回はそのうち com，net，org を対象とした．com，net は Verisign[11] より，org は PIR[12] より入手した．

入手するゾーン情報はこれらの団体によって毎日更新されており，これは日付によって判定を行う本システムにおいて有用な更新頻度である．

本研究を開始した当初はこれらは迷惑メールに使用されるドメインの上位を占めていたため，これらのドメインを対象としている．Symantec Intelligence Report の 2012 年 7 月の発表によると，迷惑メールに用いられているトップレベルドメイン上位 4 つの割合は表 1 に示すとおりである．また，表 1 にはないが org も高い割合にあり，これらの割合は日々変動している．表 1 より，これらのトップレベルドメインは迷惑メールに用いられるドメインとして代表的なものであり，これらに関して調査することは非常に有効だとわかる．ただし，ru や br に関しては同様のサービスを見つけることができなかったため今回は対象としていない．また，info や biz は今回対象としていないが，ゾーン情報を提供するサービスがあるため以下に説明する方法を同様に適用可能である．

これらの団体からのドメイン一覧のダウンロードには FTP を用いた．ただし，ファイルサイズが大きく途中でコネクションが切断されてしまうことが多かったため，レジューム機能を持つ wget というコマンドを用いた．ダウンロードするファイルは各 TLD のネームサーバのゾーン情報を記述したファイルであり，図 2 に示すような内容である．このままではデータとして扱いにくいため，awk や uniq のコマンドを用いてドメインの部分のみ重複なく抽

```
$ORIGIN NET.
$TTL 900
@ IN SOA a.gtld-servers.net. xxx.verisign-grs.com. (
                          1309579858 ;serial
                          1800 ;refresh every 30 min
                          900 ;retry every 15 min
                          604800 ;expire after a week
                          86400 ;minimum of 15 min
                          )

EXAMPLE0 NS NS1.XXY
EXAMPLE1 NS NS17.NAMESERVER1.COM.
EXAMPLE1 NS NS18.NAMESERVER1.COM.
EXAMPLE2 NS A.NS1
(以下，省略)
```

図 2 ダウンロードしたゾーンファイル
Fig. 2 A downloaded zone file.

出する．awk，uniq は共に UNIX のコマンドであり，awk はデータが規則的に並んだテキストファイルを簡単なスクリプト記述で処理するスクリプト言語，uniq はソート済みのファイルから重複する行を削除するコマンドである．この処理では，図 2 を例に挙げると，EXAMPLE0, EXAMPLE1，EXAMPLE2 の部分のみを抽出することとなる．

4.1.2 ドメイン一覧の比較

現存するドメインとその登録日の一覧を保持するためにはデータベースを用いた．ここでデータベースを用いた理由は，後に示す Bind DLZ を利用するためである．この機能を利用することで，最も普及している DNS サーバである BIND を用いながらもゾーン情報をメモリに保持しておく必要がなくなるため，大量のメモリを必要とせずに数十 GB に及ぶゾーンファイルを管理することが可能となる．また，サーバを起動する場合やゾーン情報を更新した場合にも大量のゾーン情報を読み込む必要がなくなるため迅速にサービスを提供することも可能になる．なお，データベースには MySQL を使用した．

ここでの機能は，以下の手順でダウンロードして抽出したデータと前日のドメインの抽出データを比較してデータベースを更新する．

(1) 入手した最新のドメイン一覧と前日のドメイン一覧を UNIX の diff コマンドによって比較し，差分情報を抽出する．
(2) diff コマンドによって抽出された追加および削除の差分情報を元にデータベースを更新する．追加分のドメインはその日の日付を TXT レコードとして記録する．

この一連の操作によってデータベースは常に現存するドメインのみを保持し，各ドメインに対してその登録日も共に記録している．

当初はこの作業をすべてデータベース上で行おうとしていたが，数十 GB，約 1 億件にも及ぶデータをデータベースを用いて比較しているとその処理に数日要してしまう．一方 diff コマンドはデータの順序がそろい，差分の少ないもの同士の比較であれば高速に処理することが可能である．例として，com ドメインは 1 億件近く存在するのに対し，日々 10 万〜20 万件程度しか追加および削除されていない．また，ドメインの登録順序について調べたところ，日によって大きく変化しないことが確認できた．そのため，diff コマンドを用いて比較することとした．

4.1.3 検索用データの更新

ドメイン一覧の比較結果を用いて DNS サーバのゾーンファイルを更新するのだが，現存するドメインの一覧を用いてゾーンファイルに変換を行うと，ドメインの数が非常に多く時間がかかってしまう．それに加え，新規に登録および削除されるドメインは前日から引き続き存在するドメインに比べれば非常に数が少ないため，更新のないドメインを含むゾーンファイルを作成することは非常に無駄が大きい．また，更新したゾーンファイルを DNS サーバに読み込ませるにはサーバをリロードしなければならず，ドメインの数が増えるほどリロードに時間がかかり，リロード中は DNS のサービスを利用できないためサービスが長時間中断されることとなり非常に不便である．

そこで，Bind DLZ (Dynamic Loadable Zones)[13] と呼ばれる機能を利用した．これは BIND のバックエンドとしてデータベース等を用いることが可能になるものである．そのため，従来すべてメモリ上に格納していたゾーン情報をデータベース上で管理することができるようになるため，大量のメモリがなくとも巨大なゾーンファイルを扱うことが可能となる．

今回はデータの扱いやすさから MySQL をバックエンドとして使用した．よって，前項で示したデータベースの更新によって検索用データである DNS のゾーンファイルも更新されたこととなる．

この一連の流れは図 3 に示すとおりである．

今回使用した，com，net および org ドメイン以外のデータを今後本システムで扱うことになった場合，上記の 4.1.1 項の手順でデータからドメインのみを抽出して適切な形にすれば，以下ほとんどプログラムを変更することなく用いることが可能である．

4.1.4 ドメイン登録日の検索

このシステムを用いたドメインの登録日の検索方法は，通常の DNS 問い合わせと同様に dig や nslookup を用いて TXT レコードの問い合わせによって行うことができる．ただし，”example.net.zone” のように末尾に”.zone” をつ

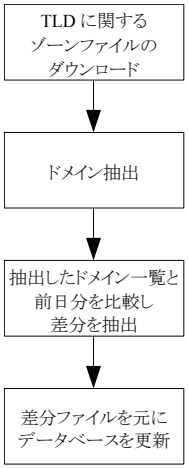

図 3 試作システムの処理の流れ
Fig. 3 The processing flow of the prototype system.

表 2 実行環境
Table 2 The environment of the prototype system.

ホスト計算機

OS	VMware ESXi5
CPU	Intel(R) Xeon(R) E5620
メモリ	18 GB
HDD	1 TB

仮想計算機

OS	FreeBSD/amd64 8.2-RELEASE
割当 CPU	2.40GHz 8 コア
割当メモリ	18GB
割当 HDD	256GB

けて問い合わせを行う必要がある[*3]．これは，このシステムを用いた登録日の問い合わせを通常の DNS 問い合わせと区別するためである．dig コマンドを用いたこのシステムに対する問い合わせ及びその応答の一例を図 4 に示す．

4.1.5 システムの運用

試作システムはすべての処理を自動で行うため，十分なディスク領域が確保されていれば，運用においては定期的にバックアップを取るなどをすればで十分である．よって，本システムの運用に当たっては管理者に大きな負担はないと考えられる．

4.2 性能評価

4.2.1 システム実行環境

本研究で実装したシステムの実行環境は表 2 に示すとおりである．なお，本研究では仮想環境を用いている．

4.2.2 使用データ

実験に用いたデータは com，net および org ドメインのゾーン情報であり，それぞれ表 3 に示すドメイン数であった．ただし，ドメインの新規登録及び削除によって日によって多少データ数が異なるので概数で示す．

[*3] 将来は”.local” 等のドメインに変更予定.

表 3 各 TLD のドメイン数
Table 3 The number of domains registered in each TLD.

TLD 名	ドメイン数
com	約 10500 万
net	約 1500 万
org	約 920 万

表 4 データ処理時間
Table 4 Data processing time

TLD 名	処理時間
com	約 120 分
net	約 15 分
org	約 10 分

4.2.3 データ処理時間

本システムを用いた一連のアップデート処理の時間は表 4 に示すとおりであった．

当初 32bitOS を用いた場合はメモリの問題，また，データベースのみを用いた場合はディスクのアクセス速度の問題から，処理不可能または処理に数日かかってしまうなどの問題があった．しかし，diff コマンドや Bind DLZ などをあわせて使用することにより，より高速な処理が可能となり，実運用が可能な処理性能を達成することができた．

5. むすび

本論文では，ドメインの登録日を収集・記録し，検索できるシステムを提案し，そのシステムの設計・実装および性能の評価を行った．

従来のブラックリスト方式では，メールメッセージ内の URL が頻繁に変更される攻撃手口には対応できなかった．また，迷惑メール判別の指標としてメッセージ内 URL のドメインの登録日を調べるために，従来から存在する WHOIS を使用した場合，大量のアクセスができないため，すべての迷惑メールに関して調べることは不可能であった．しかし今回の研究で，ブラックリストでは対応できなかった電子メールが迷惑メールであるかを判定するための指標の一つとして，メッセージ内 URL に用いられているドメインの登録日を使用するために，容易にドメインの登録日を調べることが可能となった．

今後の課題として，本システムを用いて，メールメッセージ内 URL に用いられているドメインの登録日からの日数とそのメールが迷惑メールであるかどうかの相関関係の追加的な調査や，本システムを実際に迷惑メール判別ソフトと連携させ，迷惑メール判定精度の向上を目指すなどの事項が挙げられる．

また，調査によって本システムの有用性を証明し主張していくことで，現在ドメイン一覧の入手ができない TLD に関しても，今後入手できるように働きかけていく必要も

```
$ dig @150.46.47.206 example.net.zone txt
; <<>> DiG 9.6.-ESV-R3 <<>> @150.46.47.206 example.net.zone txt
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12040
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;example.net.zone.                  IN      TXT

;; ANSWER SECTION:
example.net.zone.           3600    IN      TXT     "20110623"

;; AUTHORITY SECTION:
net.zone.               86400   IN      NS      net.zone.

;; ADDITIONAL SECTION:
net.zone.               86400   IN      A       150.46.47.206

;; Query time: 1879 msec
;; SERVER: 150.46.47.206\#53(150.46.47.206)
;; WHEN: Tue Jan 24 16:53:30 2012
;; MSG SIZE  rcvd: 81
```

図 4 試作システムを用いたドメイン登録日検索の例
Fig. 4 An example of the domain registration date retrieval with the prototype system.

ある．

謝辞 本研究の一部は日本学術振興会より科学研究費助成事業（基盤研究 (C)23500122）の支援を受けている．ここに記して感謝の意を表する．

参考文献

[1] Symantec Corporation: シマンテックインテリジェンスレポート: 2012 年 7 月 (online), 入手先 ⟨http://www.symanteccloud.com/ja/jp/mlireport/sr_wp_spam_report_1207.pdf⟩ （参照 2012-9-20）.
[2] Felegyhazi, M., Kreibich, C. and Paxson, V.: *On the potential of proactive domain blacklisting*, Proceedings of the 3rd USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET'10), pp. 99-107 (2010).
[3] T. Bereners-Lee, L. Masinter and M. McCahill: Uniform Resource Locators (URL), RFC 1738, IETF (1994).
[4] P. Mockapetris: DOMAIN NAMES - CONCEPTS AND FACILITIES, RFC 1034, IETF (1987).
[5] SURBL: SURBL(online), available from ⟨http://www.surbl.org/⟩ (accessed 2012-9-20).
[6] uribl: URIBL.COM(online), available from ⟨http://www.uribl.com/⟩ (accessed 2012-9-20).
[7] PowerView Systems: ivmURI "a Domain/URI Blacklist"(online), available from ⟨http://dnsbl.invaluement.com/ivmuri/⟩ (accessed 2012-9-20).
[8] JPRS：Whois とは (online), 入手先 ⟨http://jprs.jp/info/whois/⟩ （参照 2012-9-20）.
[9] ICANN: Registrar Accreditation Agreement(online), available from ⟨http://www.icann.org/en/registrars/ra-agreement-17may01.htm⟩ (accessed 2012-9-20).
[10] Internet Systems Consortium: BIND 9 Administrator Reference Manual(online), available from ⟨http://ftp.isc.org/isc/bind9/cur/9.8/doc/arm/Bv9ARM.pdf⟩ (accessed 2012-9-20).
[11] Verisign: Verisign(online), available from ⟨http://www.verisigninc.com/⟩ (accessed 2012-9-20).
[12] Public Interest Registry: PIR(online), available from ⟨http://www.pir.org⟩ (accessed 2012-9-20).
[13] SOURCEFORGE.NET: Bind DLZ(online), available from ⟨http://bind-dlz.sourceforge.net/⟩ (accessed 2012-9-20).