Vol.2012-EVA-39 No.6
Vol.2012-IOT-19 No.6
2012/9/28

DNS問合せの応答に基づくspamメール判別システムの設計と実装*1

山井 成良[1,a)]　諏訪 秀治[2,†1]　岡山 聖彦[1]　中村 素典[3]　ガーダ[2]　河野 圭太[1]

概要：
最近，URL に基づく spam メールフィルタを回避するため，spam メールに含まれる URL 中のドメイン部を 1 通毎に変更する手口が横行している．これに対して，我々はこのような spam メールで用いられる URL では，ドメイン部に対する権威 DNS サーバが通常とは異なる挙動を示すことを明らかにした．そこで本稿では権威 DNS サーバへいくつかの問合せを行って挙動を調査し，その結果に基づいて迷惑メールを判別するシステムの設計と実装について述べる．

キーワード：迷惑メール，URL, DNS

Design and Implementation of Spam Mail Discrimination System Based on Response of DNS Queries

Nariyoshi Yamai[1,a)]　Shuji Suwa[2,†1]　Kiyohiko Okayama[1]　Motonori Nakamura[3]　Gada[2]
Keita Kawano[1]

Abstract:
Recently, spammers often use techniques of using different domain names in URLs for every message so that they can avoid a kind of spam filter based on URL. In our previous research, we found that many authoritative DNS servers associated with URLs in spam mails were irregular in terms of their behavior. In this paper, we address the design and implementation of a a spam mail discrimination system based on the behavior of DNS servers.

Keywords: spam mail, URL, DNS

1. はじめに

電子メールは WWW と並んでネットワーク上で最も普及しているサービスの一つであり，現代社会では，社会的な活動を支える必要不可欠な通信手段である．しかし，電子メールは様々なセキュリティ上の問題を抱えており，spam メールの蔓延も見過ごすことのできない大きな社会問題となっている．最近では Rustock，Waledac などの大規模なボットネットの活動停止により，spam メールの量は減少してきているが，2012 年上半期の電子メール全体の約 2/3 は spam メールであり [1]，また 2012 年 3 月中旬では spam メールの 70–80% が URL を含んでいたことが示

[1] 岡山大学情報統括センター
Center for Information Technology and Management, Okayama University
3-1-1, Tsushima-naka, Kita, Okayama 700–8530, Japan
[2] 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
3-1-1, Tsushima-naka, Kita, Okayama 700–8530, Japan
[3] 国立情報学研究所
National Institute of Informatics
Tokyo, 101-8430, Japan
[†1] 現在，NEC ネッツ SI
Presently with NEC Network & System Integration Corp.
[a)] yamai@cc.okayama-u.ac.jp
[*1] 本論文は SAINT2012 での発表内容 [12] を一部修正したものである．

されている [2]．このような URL にアクセスすると，利用者にとって不要な広告が表示されるだけではなく，(1) 個人情報の流出，(2) 悪性ソフトウェア（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の被害，などの実質的な被害に遭う可能性があるため，その対策は重要である．

spam メールへの対策方法はいくつかの種類に分類できるが，その主流の一つにメッセージの本文の内容に基づいて判別する方法であるフィルタリングがある．その中でも，メッセージ中の URL に着目し，spam メールによく含まれる URL を登録したブラックリスト [3], [4], [5] がよく用いられている．ところが，最近では 1 通毎に spam メールに含まれる URL を変更する手口が横行しており，これにより URL のブラックリストが無効化される事態が多発している．これに対して，我々はこのような手口で用いられる URL では，その URL のドメイン部（以降，誘導先ドメイン）に対する権威 DNS サーバ（以降，関連権威サーバ）は挙動が通常の DNS サーバとは異なるものが多いことを突き止めた [6], [7]．

そこで本稿では関連権威サーバにいくつかの問合せを行い，その応答に基づいて spam メールの判別を行うシステムの設計と実装について述べる．本システムでは同時に複数の DNS 問合せを行い，また異常な動作を行う DNS サーバのブラックリストを持つことにより高速化を図っている．

2. URL に基づく spam メール対策手法およびその対抗手法

2.1 URL に基づく spam メール対策手法

メッセージの内容に基づく spam メール対策であるフィルタリングには，ヒューリスティックフィルタリング，ベイジアンフィルタリング，分散協調フィルタリング（シグネチャベースフィルタリング）など，いくつかの方法に分類できる．このうち分散協調フィルタリングは，同一内容のメールが多数の受信者に送られるという spam メールの特徴を利用した対策法で，一定数以上の受信者から spam との報告を受け取ったメールは，シグネチャと呼ばれるメッセージの同一性を判定するための値がブラックリストに登録され，今後の判定に用いられる．

このシグネチャとして URL やその一部（特にドメイン部）を用いている spam フィルタも多く存在する．これは URL 中の誘導先ドメインは比較的変更が難しかったためである．また，このようなシグネチャを集めたものをブラックリストとして DNS の仕組みを用いて公開しているサービス（DNSBL:DNS Black List）もいくつか存在し，たとえば SURBL(Spam URL Realtime Black List)[3], URIBL(URI Black List)[4]，ivmURI[5] などが知られている．これらの DNSBL では誘導先ドメインやそれに対する IP アドレス（誘導先 IP アドレス）が登録されており，ドメイン名や IP アドレスをキーとして問合せを受けると，登録の有無によって異なる応答が返されるようになっている．spam メールには多くの URL が含まれるため，このようなブラックリストの有効性を高めるには多くの URL を出現後短時間のうちに登録する必要がある．

2.2 spam メール送信者側の対策手法

前節で述べた URL に基づくフィルタリングを回避するため，spam メール送信者は様々な手口を用いている．本節ではこれらの手口のうち代表的なものを説明する．

2.2.1 誘導先ドメイン名の頻繁な変更

spam メール送信者は不正な手段で入手したクレジットカード情報などを用いて大量のドメイン名を取得し，これらを用いて同一のサーバに対する URL を頻繁に変更して spam メールを配送するような手口が知られている [8]．さらに，我々の調査 [6], [7] でも，spam メール中に含まれる URL の誘導先ドメイン名とこれらに対応する IP アドレスについて，異なるものの数を比較した結果，前者のほうが約 6 倍多いことが判明している．

この技術により，誘導先ドメイン名に基づくブラックリストは，新規ドメインの登録が追い付かず，その有効性が低下することになる．

2.2.2 誘導先 IP アドレスの頻繁な変更

逆に，spam メールの URL では，1 つの誘導先ドメイン名に対して複数の IP アドレスが対応している，fast-flux と呼ばれる手口が用いられる例が報告されている [8]．これは DNS サーバにおいて 1 つのドメイン名に対して複数のアドレスを登録し，問合せを受ける度にこれらを順に応答することにより実現しており，本来であれば複数のサーバ間で負荷分散を行う場合に用いられる技術である [9]．しかし，spam メールの誘導先ドメインでは，資源レコードのキャッシュ有効時間（TTL: Time To Live）を短くし，また資源レコードを頻繁に入れ替えることにより，稼働中のボットに確実に誘導し，また誘導先のボットの特定を困難にする目的で用いられている．

この技術により，誘導先 IP アドレスに基づくブラックリストも，次々に登録されるボットを登録できず，その有効性が低下することになる．

3. 誘導先 URL の関連権威サーバの挙動

我々の調査では，spam メールに含まれる URL の関連権威サーバは通常の DNS サーバでは見られない異常な動作を行うことが判明している．本章ではこの異常動作の詳細について述べる．また，前回の調査以降に行った 2 回目の調査結果についても述べる．

3.1 ワイルドカード資源レコードの不正使用

ワイルドカード資源レコード（以下，ワイルドカード）

[10] は問合せに合致する資源レコードが他にない時に用いられる特別な資源レコードである．通常の DNS サーバの運用では，ワイルドカードの使用は権威が委譲されているドメイン内に限られる．一方，spam メールに関連する DNS サーバの中には，権限が委譲されていないドメインについても不正にワイルドカードを使用するものがある．

たとえば，誘導先ドメイン www.example.com に対する権威サーバが example.com の権限の委譲を受けている場合を考える．この場合，*random*.example.com に関する問合せ（*random* は任意のサブドメイン名）に対してワイルドカードを用いるのは正常な使用であるが，*random*.com や *random* に関する問合せに対してワイルドカードを用いるのは不正な使用に該当する．このため，通常の DNS サーバは権威を委譲されていないドメインに関する問合せに対して Non-Existent Domain(NXDOMAIN) エラーを返すか，あるいは単に問合せを廃棄する．一方，spam メールに関連する DNS サーバの中には，このようなワイルドカードの不正使用を行っているものが多数存在する．このような DNS サーバでは，上記のような問合せに対しても同一のアドレスを返す動作を行う．これは誘導先ドメイン名の頻繁な変更に対しても 1 台の DNS サーバで設定を変えずに応答できるようにするためと思われる．

3.2 SOA レコード問合せに対する無応答

SOA(Start of Authority) レコードは，権威を持つゾーンの先頭で 1 つだけ定義されるレコードである [11]．したがって，通常の DNS サーバであれば SOA レコードの問合せに対して回答セクションあるいは権威セクションに SOA レコードを含む応答が返される．

一方，我々の調査では，spam メールに関連する DNS サーバの中には，SOA レコードの問合せには全く応答がないものが多数存在することが判明している．これはこのような DNS サーバは SOA レコードの問合せを想定していないか，あるいは簡略化を目的として問合せを無視するように設計されているためと推測できる．

3.3 前回以降の調査結果

前回の調査では，2009 年 11 月，12 月に我々が受信した電子メールについて様々な統計量を解析した．その後，2010 年 12 月から 2011 年 3 月にかけても同様の調査を行った．本節ではその結果を簡単に示す．

まず，調査対象となった電子メールの様々な統計量を**表 1** に示す．この表において ham は spam メールではない電子メールを指す．また，**表 2** 及び**表 3** では各誘導先ドメインおよび各誘導先 IP アドレスについて関連権威サーバの SOA 問合せの反応とワイルドカード使用範囲の関係をそれぞれ示したものである．表中の各値は，異なる誘導先ドメインあるいは誘導先 IP アドレスのうち，SOA 問合せに対する反応とワイルドカードの使用範囲との組合せに対応するものの個数を示している．

表 1 調査対象電子メールの統計量

調査項目	spam	ham
受信メール数	14,829	5,250
異なる誘導先ドメインの数	4,480	1,722
異なる誘導先 IP アドレスの数	747	1,704
異なる関連権威サーバ名の数	1,767	2,052
異なる関連権威サーバアドレスの数	1,046	2,014

表 2 誘導先ドメインに対する関連権威サーバの SOA 問合せの反応とワイルドカード使用範囲の関係

メール種別	SOA 問合せ	ワイルドカード使用範囲				合計
		不使用	*.dom.tld	*.tld	*	
spam	応答	830	1,118	687	2	2,637
	無応答	79	11	1,751	2	1,843
ham	応答	1,497	224	0	1	1,722
	無応答	0	0	0	0	0

表 3 誘導先 IP アドレスに対する関連権威サーバの SOA 問合せの反応とワイルドカード使用範囲の関係

メール種別	SOA 問合せ	ワイルドカード使用範囲				合計
		不使用	*.dom.tld	*.tld	*	
spam	応答	733	261	2	1	997
	無応答	28	6	10	5	49
ham	応答	1,687	325	0	2	2,014
	無応答	0	0	0	0	0

表 1 より，spam メールについては，異なる誘導先 IP アドレスの数は異なる誘導先ドメインの数，異なる関連権威サーバ名の数，異なる関連権威サーバアドレスの数と比較して大幅に少ないことがわかる．一方，ham メールメールについては，異なる誘導先ドメインの数と異なる誘導先 IP アドレスの数，ならびに異なる関連権威サーバ名の数と異なる関連権威サーバアドレスの数はほぼ等しいことがわかる．これらのことより，ham メールについては 1 台の誘導先 WWW サーバに対してほぼ 1 つの誘導先ドメイン名が対応するのに対して，spam メールについては 1 台の誘導先 WWW サーバに対して多数の誘導先ドメイン名が割り当てられていることが推測できる．

また，表 2 より，spam メールではワイルドカードを SLD(Second Level Domain)（表中の “*.tld”）で用いている DNS サーバに関連付けられている誘導先ドメインが多いのに対して，ham メールではそのような誘導先ドメインが全くないことがわかる．前回の調査では，spam メールではワイルドカードを TLD(Top Level Domain)（表中の “*”）で用いる DNS サーバに関連付けられた誘導先ドメインを含むものが多かったが，今回の調査ではワイルドカードを用いるレベルは異なるもののワイルドカードの不正利用という観点では前回の調査と同じといえる．また，

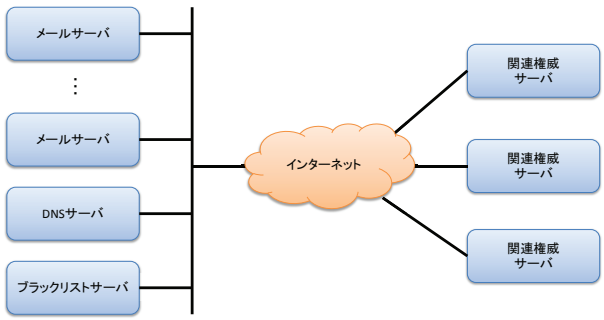

図 1 spam メール判別システムの構成

SOA レコードの問合せに対して無応答の関連権威サーバが spam メールでは見られたのに対して ham メールでは見られなかった．これらの結果により，関連権威サーバにおけるワイルドカードの不正利用に基づく spam メール判定は現在でも有効であると言える．

さらに，表 2 と表 3 を比較すると，SOA レコードの問合せに応答を返さない 49 台の関連権威サーバが 1843 個の異なる誘導先ドメインに関連し，SLD でワイルドカードを不正利用する 12 台の DNS サーバが 2,438(=687+1,751) 個の誘導先ドメインに関連していることがわかる．これらの結果より，DNS サーバの IP アドレスに基づくブラックリストが有効であると言える．

4. spam メール判別システムの設計

前節で示した調査結果より，誘導先 URL の関連権威サーバが異常な動作を行うのであれば，このような誘導先 URL を含む電子メールは spam メールである可能性が非常に高い．そこで，関連権威サーバに対していくつかの問合せを行い，その応答をもとに spam メールの判別を行うシステムの設計を行った．

4.1 システムの概要

本システムは**図 1** に示すように何台かのメールサーバ，DNS サーバ，およびブラックリストサーバから構成される．メールサーバはメッセージを受信するとその中から URL を取り出してその関連権威サーバの挙動を調査し，その結果に基づいて spam メールの判別を行う．ブラックリストサーバは関連権威サーバが異常であればメールサーバから報告を受け，その報告回数に基づいて spam メール判別に用いられるスコアを提供するためのサーバであるが，本稿では誌面の都合上説明を省略し，詳細は [12] に譲る．

4.2 spam メール判別方法

3.3 で述べたように，URL の関連権威サーバがワイルドカードを SLD で用いているか，あるいは SOA レコードの問合せに応答を返さない場合，そのような URL を含む電子メールは spam メールである可能性が非常に高い．このような異常な動作を検出するには，spam メール判別プログラム（以下，判別プログラム）が関連権威サーバに対して “*random*.tld” ドメイン（tld は誘導先ドメインの TLD と同じ）の A レコード問合せを行い，またその権威ドメインの SOA レコード問合せを行えばよい．しかし，通常の DNS サーバは前者の問合せに対して応答を返さない場合が多く，また異常な DNS サーバは後者の問合せに対して応答を返さないため，単純な調査方法ではタイムアウトを待つ必要が生じる．

そこで，本システムでは両方の問合せを同時に行い，先に返された応答を用いて判別するようにした．判別基準を以下に示す．

(1) 先に SOA レコードが返された場合，DNS サーバが正常であると判定する．
(2) 先に SOA レコード問合せに対して “Non-Existent Domain” エラーが返された場合，DNS サーバが異常であると判定する．
(3) 先に A レコードが返された場合，返されたアドレスが誘導先 IP アドレスと同じであれば DNS サーバが異常であると判定する．そうでなければ正常と判定する．
(4) 先に A レコード問合せに対して “Non-Existent Domain” エラーが返された場合，DNS サーバが正常であると判定する．

この判別基準では，ほとんどの通常の DNS サーバは (1) か (4) に該当し，ほとんどの異常な DNS サーバは (3) に該当する．したがって，タイムアウトを待つ必要なく spam メールの判別を行うことが可能になる．なお，(2) は本来であれば通常の DNS サーバでも異常な DNS サーバでも起こらないが，念のために含めた．

4.3 全体の動作手順

システムの動作手順を以下に示す．なお，ブラックリストサーバに関連する動作は一部省略する．

(1) 判別プログラムはメール中に含まれる各 URL について誘導先ドメイン名を取り出して，DNS サーバに対して A レコードを問い合わせ，その応答より誘導先 IP アドレスだけでなく，関連権威サーバ名とその権威ゾーン名を得る．
(2) 次に，判別プログラムはブラックリストサーバに関連権威サーバ名が登録されているかどうかを問い合わせ，登録されていればそのスコアを得る．
(3) 次に，判別プログラムは DNS サーバに対して関連権威サーバの A レコードを問い合わせてその IP アドレスを得る．
(4) 次に，判別プログラムはブラックリストサーバに対して各関連権威サーバアドレスが登録されているかどうかを問い合わせ，登録されていればそのスコアを得る．
(5) 次に，判別プログラムは各関連権威サーバの挙動調査

を行う．まず，判別プログラムが持つキャッシュを検索し，もしヒットすればキャッシュされた以前の調査結果を用いる．そうでなければ前節で述べた方法で調査を行い，その結果をキャッシュする．キャッシュのヒット，ミスにかかわらず，調査結果が「異常」であれば関連権威サーバの FQDN（Fully Qualified Domain Name）および IP アドレスをブラックリストサーバに送る．

(6) 判別プログラムは上記 (2)，(4)，(5) の結果に基づいて総合的なスコアを各関連権威サーバについて算出し，そのうち最もスコアが大きいものが管理者の定めた閾値を超えていれば spam メールと判定する．

5. spam メール判別システムの実装と評価

前章で示した動作に基づいて，我々は試作システムを実装した．また，試験運用を行い，その機能や性能を確認した．本章では実装方法と試験運用の結果について述べる．

5.1 試作システムの実装

試作システムは 1 台のメールサーバとブラックリストサーバ（DNS サーバと兼用）の計 2 台で構成した．このうち，メールサーバにおける判別プログラムの実装方法について以下に述べる．

判別プログラムは SpamAssassin[13] のプラグインモジュールとして Perl で実装した．SpamAssassin はメッセージ中の URL を取り出し，判別プログラムに誘導先ドメインを渡す．判別プログラムは各関連権威サーバの挙動調査を行い，その結果を次の各変数に格納する．

NSNAMEBL_CHECK ブラックリストサーバへの関連権威サーバ名の問合せ結果．登録時は登録頻度に応じた値（2 ～ 255）となり，それ以外は 0 となる．

NSIPBL_CHECK サーバ名の代わりに IP アドレスを用いる点を除いて上記と同じ．

IRREGULAR_NS_CHECK 関連権威サーバの挙動調査結果．異常であれば 1，それ以外は 0 となる．

これらの変数は spam メール判別のスコアとしても用いられ，たとえば NSNAMEBL_CHECK の値が 50 未満の場合にはスコアは 2 点，50 以上の場合にはスコアは 5 点，のような柔軟な設定が可能である．

なお，関連権威サーバの挙動調査においてどちらの問合せに対しても応答がなかった場合には最大で 10 秒間待ち，タイムアウトを通知するようにした．

5.2 試作システムの評価

2011 年 12 月 27 日から 2012 年 1 月 7 日までの間に受信した電子メールを対象に試作システムの評価実験を行った．評価対象の電子メールは以下の 3 種類である．

表 4 試作システムによる spam メール分別結果

	spam1	spam2	ham
電子メール数	4,390	511	1,008
spam 判定メール数	76	7	2

表 5 判別プログラムの処理時間

測定項目	spam1	spam2	ham
判別時間 (sec)	0.48	1.35	2.51
挙動調査時間 (sec)	0.25	0.82	1.35

表 6 処理対象電子メールの統計量

	spam1	spam2	ham
平均誘導先ドメイン数	0.97	1.03	5.11
平均関連権威サーバアドレス数	2.50	3.18	19.05
キャッシュミス率 (%)	4.5	11.3	12.1

spam1 著者の一人に送られ，ツールにより自動的に spam メールと判定されたもの．

spam2 個人の所有する，現在は使用されていないアドレス宛に送られたもの．

ham 数種類のメールマガジンサービスから配送されたもの

この評価実験ではメールサーバは 1 台しかないため，ブラックリストサーバは用いず，IRREGULAR_NS_CHECK の結果だけを用いて判定した．

5.2.1 判別能力の評価結果

試作システムによる spam メール分別結果を**表 4** に示す．残念ながら，この評価実験では spam メールと判別された電子メールは spam1，spam2 とも少なかった．この結果は表 2，表 3 と大きく異なっている．その原因として，2011 年 3 月に巨大ボットネット Rustock が解体され [14]，受信する spam メールの内容が大きく変化したことが挙げられる．

spam と判定されたメールを詳しく調べると，spam1 中の 76 件は誘導先ドメインが全てレジストラ「お名前.com」により登録されたものであった．したがって，これらは既に摘発されて使われなくなったドメインであると推察できる．一方，spam2 中の 2 件はいずれも誘導先 URL にアクセスすると Pharmacy Express のページが表示された．ham 中の 2 件のうち，1 件は SpamAssassin が誤って URL でない部分を判別プログラムに渡したためであり，またもう 1 件は「お名前.com」により登録されたものであった．

5.2.2 処理時間の測定結果

次に，試作システムの処理時間の測定結果を**表 5** に示す．この表において，判別時間，挙動調査時間はそれぞれプラグイン自身の平均実行時間および IRREGULAR_NS_CHECK の平均実行時間を示す．また，処理対象電子メールの統計量を**表 6** に示す．さらに，1 台の DNS サーバに要する挙動調査時間を**表 7** に示す．

表 7　DNS サーバ 1 台の平均挙動調査時間

	spam1	spam2	ham
キャッシュミス (sec)	0.50	1.32	0.27
キャッシュヒット (sec)	0.008	0.018	0.004

表 5 に示すように，spam2 の判別時間は spam1 と比較して約 2.8 倍長い．表 6 によると，この理由は spam2 のキャッシュミス率 (11.3%) が spam1(4.5%) と比べて約 2.5 倍大きく，また平均関連権威サーバアドレス数も少し大きいためであると推測できる．一方，ham の判別時間は spam2 と比較すると約 1.9 倍となっている．両者のキャッシュミス率に大きな差はないが，関連権威サーバアドレス数は約 5.7 倍，また関連権威サーバの調査時間が約 1/5 であることを考慮すると，妥当といえる．

表 7 により，キャッシュヒット時の調査時間はミス時と比較して 70 分の 1 程度の時間に収まっており，キャッシュが調査時間の短縮に大きな役割を果たしていることがわかる．また，キャッシュミス時の調査時間を比較すると，ham に比べて spam1，spam2 の時間が大幅に長いことがわかる．これはいずれの問合せにも無応答であったためタイムアウトが生じた関連権威サーバが合計で 31 台確認されたことから，その影響によるものと推測できる．

6. まとめ

本稿では，誘導先 URL の関連権威サーバにいくつかの問合せを行い，その応答に基づいて spam メールの判別を行うシステムの設計と実装について述べた．本システムでは同時に複数の DNS 問合せを行い，また異常な動作を行う DNS サーバのブラックリストを持つことにより高速化を実現した．本システムでは誘導先ドメインではなく，関連権威サーバを調査対象としているため，多数のドメインを使って URL に基づくブラックリストを回避するような手口に対しても有効に機能する．本システムだけで判別できる spam メールは評価実験では少なかったため，有効性を確認するまでには至らなかったが，このような手口を用いた spam メールは一時的に減少している可能性があり，再び増加した場合には本システムの有効性を確認できると思われる．また，現状でも誤検出率（false positive rate）が小さいため，従来技法と組み合わせることによりその判定精度向上に貢献できる．

今後の課題としては，多数のメールサーバを用いて挙動調査結果を共有し，ブラックリストサーバの有効性を検証することが挙げられる．

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] シマンテック: シマンテックインテリジェンスレポート: 2012 年 6 月 (online), available from ⟨http://www.symantec.com/content/ja/jp/enterprise/white_papers/sr_wp_spam_report_1206.pdf⟩ (accessed 2012-08-27) (2012).
[2] Eric Park: 一撃離脱スパムの増加 (online), available from ⟨http://www.symantec.com/connect/blogs-258⟩ (accessed 2012-08-27) (2012).
[3] SURBL(online), available from ⟨http://www.surbl.org/⟩ (accessed 2012-08-27) (2012).
[4] URIBL.COM(online), available from ⟨http://www.uribl.com/⟩ (accessed 2012-08-27) (2012).
[5] ivmURI: a URI blacklist(online), available from ⟨http://dnsbl.invaluement.com/ivmuri/⟩ (accessed 2012-08-27) (2012).
[6] 諏訪秀治，山井成良，岡山聖彦，中村素典：“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”，情報処理学会インターネットと運用技術研究会研究報告，また，また Vol.2010-IOT-10，No.10，pp.1–6 (2010).
[7] Shuji Suwa, Nariyoshi Yamai, Kiyohiko Okayama, and Motonori Nakamura: “DNS Resource Record Analysis of URLs in E-mail Messages for Improving Spam Filtering”, Proceedings of 2011 11th Annual International Symposium on Applications and the Internet (SAINT 2011), pp.439–444 (2011).
[8] McAfee, Inc.: 攻撃の高度化，「Fast-Flux」から「RockPhish」まで (online), available from ⟨http://itpro.nikkeibp.co.jp/article/COLUMN/20071211/289199/⟩ (accessed 2012-08-27) (2012).
[9] T. Brisco: “DNS support for load balancing,” RFC 1794, IETF(1995).
[10] P. Mockapetris: “DOMAIN NAMES - CONCEPTS AND FACILITIES,” RFC 1034, IETF(1987).
[11] P. Mockapetris: “DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION,” RFC 1035, IETF(1987).
[12] Shuji Suwa, Nariyoshi Yamai, Kiyohiko Okayama, Motonori Nakamura, Gada, and Keita Kawano: “Spam Mail Discrimination System Based on Behavior of DNS Servers Associated with URLs”, Proceedings of 2012 12th Annual International Symposium on Applications and the Internet (SAINT 2012), pp.381–386 (2012).
[13] Apache Software Foundation: SpamAssassin: Welcome to SpamAssassin(online), available from ⟨http://spamassassin.apache.org/⟩ (accessed 2012-08-27) (2012).
[14] MessageLabs Intelligence: MessageLabs Intelligence: March 2011(online), Symantec Corporation, available from ⟨http://www.symanteccloud.com/mlireport/MLI_2011_03_March_Final-EN.pdf⟩ (accessed 2012-08-27) (2011).