科学研究費助成事業　　研究成果報告書

平成　２６　年　　５　月　１３　日現在

機関番号：　１５３０１
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５００１２２

研究課題名（和文）手口の巧妙化に対応可能な迷惑メール対策手法

研究課題名（英文）An anti-spam method against sophisticated techniques

研究代表者
山井　成良（YAMAI, NARIYOSHI）

岡山大学・情報統括センター・教授

研究者番号：９０２１０３１９

交付決定額（研究期間全体）：（直接経費）　　4,000,000円、（間接経費）　　1,200,000円

研究成果の概要（和文）：よく用いられている迷惑メール対策手法として，宣伝や詐欺のためのURL（誘導先URL）に着目したフィルタリング技術がある．ところが，最近では誘導先URLの頻繁な変更など，同技術を回避する手法が横行し，その対処が急務となっている．本研究では誘導先URLに含まれるドメインの登録日やそのドメインを管理するDNS（ドメイン名システム）サーバの挙動など，迷惑メール送信者が本質的に回避しにくい特徴に基づく迷惑メール対策手法を確立した．

研究成果の概要（英文）：As an anti-spam method, a filtering technology based on URLs for advertisement, phishing, and so on (target URLs) is frequently used. Recently, however, to avoid this technology, spammers use a sophisticated countermeasure such as frequent change of target URLs. Therefore, a new method against this countermeasure is required. In this research, we established an anti-spam method based on basically unforgeable characteristics such as the registration date of the domain in a target URL, the behavior of the DNS (Domain Name System) server of the domain related to the target URL, and so on.

研究分野：　総合領域

科研費の分科・細目：　情報学、メディア情報学・データベース

キーワード：　電子メール　迷惑メール　DNS　ブラックリスト　ホワイトリスト

１．研究開始当初の背景

近年，迷惑メールやこれに伴う不正行為の蔓延が大きな社会問題となっている．その対策として大部分の迷惑メールに含まれている宣伝や詐欺などのための URL（誘導先 URL）に着目したフィルタリング技術が現在広く使われている．ところが，特に最近では攻撃者の手口が巧妙になり，従来の対策が有効に機能しなくなってきている．たとえば FastFlux と呼ばれる手口では，

(1) 迷惑メール毎に内容の一部，特に誘導先 URL のドメイン部分（誘導先ドメイン）を変更する．
(2) 上記の誘導先ドメインに対して複数のボットを偽 Web サーバとして構成し，DNS サーバの応答でこれらを切り替える．
(3) 上記で用いられる DNS サーバ自身も複数のボットから構成され，親ドメインの DNS サーバの応答でこれらを切り替える．

という方法が取られている．現在主流となっている，URL や IP アドレスに基づく判定(ブラックリスト）や登録済み迷惑メールとの同一性に　基づく判定（署名ベースフィルタリング）ではこれらの手口により回避されているのが現状である．

２．研究の目的

上記のような手口に対応するため，本研究では以下の各項目の実現を目指した．

(1) DNS サーバの挙動に基づくフィルタリング手法の確立

迷惑メール毎の誘導先ドメインの変更を実現するためには，迷惑メール送信者が仕立てた DNS サーバは 1 台で多数の誘導先ドメインに対応していると推測され，実際に予備調査では任意の問合せに同じ応答を返す DNS サーバの存在が確認されている．そこで本研究では DNS サーバの挙動を効率よく調査し，その結果に基づいて迷惑メールをフィルタリングする手法を確立する．

(2) ドメイン登録情報に基づくフィルタリング手法の確立

特に詐欺などの犯罪行為に利用される誘導先ドメインについては，使い捨て用として次々に取得され，登録費の支払いに不正取得したクレジットカード情報が使われる場合が多い．その結果，このようなドメインは登録費の未払い，あるいは犯罪行為の発覚などにより短期間で閉鎖され，存在期間が短いと予想される．そこで本研究ではドメインの登録情報（whois 情報）のうち特に登録時期に着目し，登録して間もないドメインが誘導先として含まれるメッセージを高い確率で迷惑メールと判定する手法を確立する．

(3) DNS サーバのブラックリストに基づくフィルタリング手法の確立

上記(1)のように迷惑メール送信者が仕立てた DNS サーバ 1 台が多数の誘導先ドメインに対応していると推測され，DNS サーバの台数は誘導先ドメインの種類より大幅に少ないと予想される．これが事実なら，DNS サーバの IP アドレスに基づくブラックリストが有効に機能する可能性がある．そこで本研究では特に変更が比較的制限される，レジストリに登録された DNS サーバを対象としたブラックリストを作成し，その有効性を検証する．

３．研究の方法

本研究では，まずハニーポット等を用いて迷惑メールを収集し，その中に含まれる誘導先ドメインについて DNS サーバの挙動やドメイン登録情報を分析した．次に，分析結果に基づき，迷惑メール判定基準やブラックリストへの登録基準を決定した．さらに，試作システムの設計・実装を行い，有効性を検証した．各年度に行った研究内容は以下のとおりである．

(1) 平成 23 年度

① 迷惑メールの収集・分析

主に迷惑メール収集用ハニーポットが受信した迷惑メールや利用者が判定した迷惑メールを分析し，特に DNS サーバの挙動と照らし合わせて迷惑メールの判定基準を分析・検討した．

② DNS サーバ挙動判定プログラムの設計・実装

上記の調査により，誘導先ドメインに対応する DNS サーバは通常の DNS サーバとは異なる挙動を行うものが多いことが確認できた．そこで，DNS サーバの挙動を判定するプログラムを設計・実装した．

③ 優先配送システムの設計・実装

上記の DNS サーバ挙動判定プログラムは，多くの URL を含む迷惑メールを受信するとオーバヘッドが無視できない問題が新たに判明した．この問題に対処するため，信頼できるメールサーバから受信したメールを専用のメールサーバで受信する，優先配送システムの設計・実装を行った．

(2) 平成 24 年度

① DNS サーバ挙動判定プログラムの評価

前年度に開発した DNS サーバ挙動判定プログラムを迷惑メールフィルタリングプログラム SpamAssassin にプラグインとして組み込み，正しく動作することを確認した．

② DNS サーバ用ブラックリストの設計・実装

DNS サーバ用ブラックリストの設計・実装を行い，上記①と同様に迷惑メールフィルタリングプログラム SpamAssassin にプラグインとして組み込んだ．

③ whois 情報判定プログラムの設計・実装・検証

ドメイン情報を提供するサーバ（whois サーバ）は迷惑メール判定のための利用を想定しておらず，頻繁な情報収集が制限されている．そこで，whois サーバに依存することなくドメイン登録日を調査・検索するシステムを開発した．

④ 優先配送システムの評価

前年度に開発した優先配送システムの性能評価として，同時に 500 セッションを受け付けた場合の動作を検証した．

(3) 平成 25 年度

① ドメイン登録日に基づく迷惑メール判別システムの開発

前年度に開発したドメイン登録日検索システムを迷惑メールフィルタリングプログラム SpamAssassin にプラグインとして組み込み，迷惑メール判別システムとして動作させた．

② 優先配送システムの改良

前年度までに開発した優先配送システムでは，たとえば転送などによりホワイトリストに登録されているメールサーバから迷惑メールを受信した場合，簡単な検査しか行われないため迷惑メールと判定できない可能性があるという問題があった．そこで，この問題へ対処できるように優先配送システムの改良を行った．

③ パスワード不正取得による迷惑メール発信に対する対策手法の開発

平成 25 年度はパスワードを不正取得して迷惑メールを発信する行為が頻発した．この手口では正規のユーザ認証を行ったうえで迷惑メールを発信するため，従来の迷惑メール対策手法が有効に機能しない．そこで，その手口への対策手法を開発した．

４．研究成果

(1) 研究の主な成果

本研究課題で得られた主な研究成果を以下に示す．

① 頻繁に変更される誘導先URL に対応するDNS サーバの挙動

誘導先 URL を頻繁に変更する手口において，誘導先 URL に対応する DNS サーバの挙動を調査した結果，トップレベルドメインが同じであれば任意のドメインに関する A（Address）レコードの問合せに対して同一の応答を返し，また誘導先ドメインに関する SOA（Start of Authority）レコードの問合せに対して応答を返さない，という通常の DNS サーバとは異なる挙動を行うものが多いことが確認できた．

② DNS サーバの挙動に基づく迷惑メール判定手法の確立

上記(1)の結果をもとに，誘導先 URL に対応する DNS サーバに random.tld（random はランダムな文字列，tld は誘導先 URL と同じトップレベルドメイン）に対する A レコードと誘導先 URL のドメインに対する SOA レコードを同時に問い合わせ，先に受信した応答を調べることにより，タイムアウトを待たずに素早く DNS サーバの挙動を調査することが可能になった．これにより，誘導先 URL を頻繁に変更する手口に対して，ブラックリストに依存することなく対抗することが可能となった．

③ ドメイン登録日に基づく迷惑メール判定手法の確立

whois 情報のうち特にドメイン登録日については，迷惑メールや悪性ウェブサイトとの関連に関する多くの調査研究がおこなわれているが，これまでは whois サーバのアクセス制限のためにドメイン登録日を迷惑メール判定に用いることが困難であった．本研究では，比較的よく使われているトップレベルドメインである com，net，org の 3 つを対象として，これらのゾーン情報（当該トップレベルドメインに含まれるドメイン名の一覧）を毎日受信し，前日との差分に基づいてドメイン登録日を調査・検索するシステムを開発した．また，最近は短い URL でアクセスするとリダイレクト機能により本来の URL にアクセスすることができる短縮 URL サービスが多数存在しているため，既存の短縮 URL サービスに対してはダイレクト先の URL を取得し，その URL に対してドメイン登録日を取得するようにした．なお，たとえばメーリングリストの退会など，一度アクセスしただけで副作用が生じる URL が存在するため，全ての URL についてリダイレクトが生じるかどうかをアクセスして試す方法は採用できないことが判明した．

④ 優先配送システムの実用化

1 通のメッセージ中に含まれる URL が多くなると，DNS サーバの挙動調査に要する時間が無視できなくなることから，信頼できるメールサーバから送られる電子メールについては，別途用意したメールサーバで受信することができる，優先配送システムを開発した．同様の仕組みはたとえば PC ルータでも実現可能であるが，信頼できるメールサーバの数が多くなると優先配送対象かどうかを判別するために要するオーバヘッドが無視できないため，レイヤ 3 スイッチの設定を動的に変更することにより高速に配送できるシステムを開発した．また，信頼できるメールサ

ーバから迷惑メールと疑われるメールを受信した場合，強制切断を行うなどの方法で一時エラーを発生させ，一般用メールサーバに配送させる手法を考案し，優先配送システムに実装した．性能評価の結果，添付ファイル付メッセージなど指定した条件を満たすメッセージを比較的早い段階で強制切断して一般用メールサーバで受信するように動作することが確認された．

⑤　パスワード不正取得による迷惑メール発信に対する対策手法の開発

パスワードを不正に取得して迷惑メールを大量に送信する手口を分析した結果，送信者は多数のクライアントを用いて送信するが，個々のクライアントの送信量はそれほど多くないことが判明した．これは，これまでよく用いられてきた，1 つの IP アドレスに対する送信量規制が有効に機能しないことを意味する．一方，クライアントの所在国を調べたところ，多数の国に分散していることが判明した．そこで，送信元 IP アドレスをもとにクライアントの所在国を求め，現実的には異動が不可能な頻度で短時間に多数の国からメール送信を試みられた場合にパスワードが不正取得されたと判断してアカウントを停止する対策手法を開発した．

(2) 今後の展望

特にドメイン登録日に基づく迷惑メール判定手法は，研究当初はゾーン情報を公開しているトップレベルドメインがそれほど多くはなかったが，最近では手続きを行えば多くのトップレベルドメインがゾーン情報を公開するようになったため，今後は本研究の成果の有効性が大きく向上することが予想される．また，現在は入手したゾーン情報を他者に公開することができないため，作成したドメイン登録日検索システムを第三者が利用することはできないが，本研究の有効性が広く認められ，公式サービスとして提供できるように Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG) などの関連団体に提案を行う予定である．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１３件）

① Nariyoshi Yamai, Masayuki Matsuoka, Kiyohiko Okayama, Keita Kawano, Motonori Nakamura, Masato Minda: Domain Registration Date Retrieval System for Improving Spam Mail Discrimination, Journal of Information Processing, 査読有, Vol.22, No.3, 2014. 掲載確定.

② ガーダ，山井成良，岡山聖彦，河野圭太，中村素典：レイヤ 3 スイッチによる動的ホワイトリストを用いた電子メール優先配送システム，情報処理学会論文誌，査読有，Vol.55, No.3, 2014, pp.1151-1159. URL:<http://id.nii.ac.jp/1001/00099466/>

③ 山井成良，藤原崇起，河野圭太，大隅淑弘，岡山聖彦：パスワード不正取得による迷惑メール発信に対する対策，情報処理学会研究報告，査読無，Vol.2014-IOT-24, No.9, 2014, pp.1-6. URL:< http://id.nii.ac.jp/1001/00098592/>

④ 山井成良，ガーダ，松岡政之，須藤亨，岡山聖彦，河野圭太，中村素典：電子メール優先配送における信頼できる MTA からの spam メール処理，インターネットと運用技術シンポジウム 2013 論文集，情報処理学会，査読無，Vol.2013, 2013, pp.99-102. URL:<http://id.nii.ac.jp/1001/00096446/>

⑤ Gada, Nariyoshi Yamai, Kiyohiko Okayama, Keita Kawano, Motonori Nakamura: E-mail Priority Delivery System with Dynamic Whitelist in the Layer 3 Switch, Proceedings of 2013 IEEE 37th International Conference on Computer Software and Applications (COMPSAC 2013) Workshops, 査読有, 2013, pp.581-586. DOI: 10.1109/COMPSACW.2013.78

⑥ Masayuki Matsuoka, Nariyoshi Yamai, Kiyohiko Okayama, Keita Kawano, Motonori Nakamura, Masato Minda: Domain Registration Date Retrieval System of URLs in E-mail Messages for Improving Spam Discrimination, Proceedings of 2013 IEEE 37th International Conference on Computer Software and Applications (COMPSAC 2013) Workshops, 査読有, 2013, pp.587-592. DOI: 10.1109/COMPSACW.2013.79

⑦ 松岡政之，井上達貴，山井成良，岡山聖彦，河野圭太，中村素典，民田雅人：メッセージ中 URL に基づくドメイン登録日検索システムを用いた迷惑メール判別機構，マルチメディア，分散，協調とモバイルシンポジウム 2013(DICOMO 2013)論文集，情報処理学会，査読有，2013, pp.766-771. URL:<http://id.nii.ac.jp/ 1001/00097219/>

⑧ ガーダ，山井成良，岡山聖彦，河野圭太，中村素典： レイヤ 3 スイッチによる動的ホワイトリストを用いた電子メール優先配送システムの評価，情報処理学会第 75 回全国大会講演論文集，査読無，Vol.2013, No.1, 2013, pp.377-378. URL:<http://id.nii.ac.jp/1001/00093592/>

⑨ 松岡政之，山井成良，岡山聖彦，河野圭太，中村素典，民田雅人：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，インターネットと運用技術シンポジウム 2012 論文集，情報処理学会，

査読有, Vol.2012, 2012, pp.16-22. URL: <http://id.nii.ac.jp/1001/00087618/>
⑩ 山井成良,諏訪秀治,岡山聖彦,中村素典, ガーダ, 河野圭太：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, 情報処理学会研究報告, 査読無, Vol.2012-IOT-19, No.6, 2012, pp.1-6. URL: <http://id.nii.ac.jp/1001/00085783/>
⑪ Shuji Suwa, Nariyoshi Yamai, Kiyohiko Okayama, Motonori Nakamura, Gada, 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), 査読有, 2012, pp.381-386. DOI: 10.1109/SAINT.2012.68
⑫ ガーダ, 諏訪秀治, 山井成良, 岡山聖彦, 中村素典：レイヤ 3 スイッチを用いた大規模なホワイトリストに対応可能な電子メール優先配送システム, 情報処理学会研究報告, 査読無, Vol.2012-IOT-16, No.37, 2012, pp.1-6. URL: <http://id.nii.ac.jp/1001/00081151/>
⑬ Shuji Suwa, Nariyoshi Yamai, Kiyohiko Okayama, 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), 査読有, 2011, pp.439-444. DOI: 10.1109/SAINT.2011.82

〔学会発表〕(計１６件)
① 山井成良,藤原崇起,河野圭太,大隅淑弘, 岡山聖彦：パスワード不正取得による迷惑メール発信に対する対策, 情報処理学会第 24 回インターネットと運用技術研究発表会, 2014 年 2 月 27-28 日, 石川県加賀市.
② 山井成良, ガーダ, 松岡政之, 須藤亨, 岡山聖彦, 河野圭太, 中村素典：電子メール優先配送における信頼できる MTA からの spam メール処理, 情報処理学会第 6 回インターネットと運用技術シンポジウム, 2013 年 12 月 12～13 日, 広島県東広島市.
③ 山井成良：迷惑メール対策の現状と課題, 大阪市立大学創造都市研究科ワークショップ (招待講演), 2013 年 10 月 1 日, 大阪市北区.
④ Gada, Nariyoshi Yamai, Kiyohiko Okayama, Keita Kawano, Motonori Nakamura: E-mail Priority Delivery System with Dynamic Whitelist in the Layer 3 Switch, The 1st IEEE International Workshop on Architecture, Design, Deployment and Management of Networks & Applications (ADMNET 2013), 26 July 2013, Kyoto, Japan.
⑤ Masayuki Matsuoka, Nariyoshi Yamai, Kiyohiko Okayama, Keita Kawano, Motonori Nakamura, Masato Minda: Domain Registration Date Retrieval System of URLs in E-mail Messages for Improving Spam Discrimination, The 1st IEEE International Workshop on Architecture, Design, Deployment and Management of Networks & Applications (ADMNET 2013), 26 July 2013, Kyoto, Japan.
⑥ 松岡政之,井上達貴,山井成良,岡山聖彦, 河野圭太, 中村素典, 民田雅人：メッセージ中 URL に基づくドメイン登録日検索システムを用いた迷惑メール判別機構, マルチメディア,分散,協調とモバイルシンポジウム 2013, 2013 年 7 月 10-12 日, 北海道河東郡音更町.
⑦ ガーダ, 山井成良, 岡山聖彦, 河野圭太, 中村素典： レイヤ 3 スイッチによる動的ホワイトリストを用いた電子メール優先配送システムの評価, 情報処理学会第 75 回全国大会, 2013 年 3 月 6-8 日, 仙台市青葉区.
⑧ 松岡政之,山井成良,岡山聖彦,河野圭太, 中村素典, 民田雅人：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, 情報処理学会第 5 回インターネットと運用技術シンポジウム, 2012 年 12 月 13-14 日, 鹿児島県鹿児島市.
⑨ 山井成良：迷惑メール対策の概要, 迷惑メール対策セミナー[新潟] (招待講演), 2012 年 11 月 25 日, 新潟市中央区.
⑩ 山井成良：迷惑メール対策の現状と課題, 大阪市立大学創造都市研究科ワークショップ (招待講演), 2012 年 10 月 16 日, 大阪市北区.
⑪ 山井成良,諏訪秀治,岡山聖彦,中村素典, ガーダ, 河野圭太：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, 情報処理学会第 19 回インターネットと運用技術研究発表会, 2012 年 9 月 27-28 日, 島根県松江市.
⑫ Shuji Suwa, Nariyoshi Yamai, Kiyohiko Okayama, Motonori Nakamura, Gada, Keita Kawano: Spam Mail Discrimination System Based on Behavior of DNS Servers Associated with URLs, The Third Workshop on Company, Campus and Community Networking (C3NET 2012), 16 July 2012, Izmir, Turkey.
⑬ 山井成良：迷惑メール対策手法総論, 第 9 回迷惑メール対策カンファレンス (招待講演), 2012 年 5 月 27 日, 東京都港区.
⑭ ガーダ, 諏訪秀治, 山井成良, 岡山聖彦, 中村素典：レイヤ 3 スイッチを用いた大規模なホワイトリストに対応可能な電子メール優先配送システム, 情報処理学会第 16 回インターネットと運用技術研究発表会, 2012 年 3 月 15-16 日, 札幌市北区.

⑮ 山井成良：迷惑メール対策の現状と課題，大阪市立大学創造都市研究科ワークショップ（招待講演），2011 年 11 月 8 日，大阪市北区．
⑯ Shuji Suwa, Nariyoshi Yamai, Kiyohiko Okayama, Motonori Nakamura: DNS Resource Record Analysis of URLs in E-mail Messages for Improving Spam Filtering, The 2nd Workshop on Company, Campus and Community Networking - Technology, Management and Ethics - (C3NET 2011), 20 July 2011, Munich, Germany.

〔その他〕
○表彰（計　３件）
① 松岡政之，井上達貴，山井成良，岡山聖彦，河野圭太，中村素典，民田雅人：メッセージ中 URL に基づくドメイン登録日検索システムを用いた迷惑メール判別機構，マルチメディア，分散，協調とモバイルシンポジウム 2013（DICOMO2013）優秀論文賞，情報処理学会 DICOMO2013 実行委員会，2013 年 8 月．URL: <http://www.dicomo.org/2013/commendation.html>
② ガーダ（指導学生）：レイヤ 3 スイッチを用いた大規模なホワイトリストに対応可能な電子メール優先配送システム，2012 年度山下記念研究賞，情報処理学会，2013 年 3 月．URL: < http://www.ipsj.or.jp/award/yamashita2012.html>
③ 松岡政之，山井成良，岡山聖彦，河野圭太，中村素典，民田雅人：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，第 5 回インターネットと運用技術シンポジウム(IOTS2012)優秀論文賞，情報処理学会インターネットと運用技術研究会，2012 年 12 月．URL: <http://iot.ipsj.or.jp/iots/2012/award>

６．研究組織
(1)研究代表者
山井 成良（YAMAI NARIYOSHI）
岡山大学・情報統括センター・教授
研究者番号：90210319

(2)研究分担者
岡山 聖彦（OKAYAMA KIYOHIKO）
岡山大学・情報統括センター・准教授
研究者番号： 20252588
河野 圭太（KAWANO KEITA）
岡山大学・情報統括センター・准教授
研究者番号： 40397899

(3)連携研究者
中村 素典（NAKAMURA MOTONORI）
国立情報学研究所・学術基盤推進部・特任教授
研究者番号： 30268156

(4)研究協力者
民田 雅人（MINDA MASATO）
株式会社日本レジストリサービス