社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2006－DPS－126 (2)
2006－CSEC－ 32 (2)
2006／3／16

電子メールからの接続先企業検出による フィッシング詐欺対策の提案

柴田 賢介† 荒金 陽助† 塩野入 理† 金井 敦†
† 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所

概要 近年のインターネットの普及により，電子メールによるエンドユーザ間のコミュニケーションが増加する一方で，これを悪用し，エンドユーザの個人情報を狙うフィッシング詐欺が多発している．フィッシング詐欺は，金融機関等を装った偽装メールを契機とするものが多く，フィッシングメールの多くはソーシャルエンジニアリングによってエンドユーザを巧みにフィッシングサイトへ誘導しようとする．我々は，エンドユーザに送られてきたメールが正当なものであるか否かを検証するために，「メールがどの企業に接続させようとしているのか」という情報に注目している．本稿では，メール本文を解析することによって，メールの接続先企業に関する情報を抽出し，得られた接続先情報とハイパーリンクをホワイトリストと比較して，接続先の正当性を検証する方式を提案するとともに，プロトタイプを用いた接続先企業検出の精度に関する評価について述べる．

キーワード フィッシング詐欺，ホワイトリスト，電子メール，形態素解析，ソーシャルエンジニアリング

An Anti-Phishing Method by Detecting Hijacked Brand Names in Spoofed Emails

Kensuke Shibata† Yosuke Aragane† Osamu Shionoiri† Atsushi Kanai†
† NTT Information Sharing Platform Laboratories, NTT Coporation

Abstract In recent years, many people use email and various online services by the wide use of Internet. In that context, phishing attacks which aim at users' personal information become a serious threat. In this paper, we propose an anti-phishing method. This proposal method has a function of URL verification by using white list of legitimate web sites. To counter the social engineering technique, we focus attention on the hijacked brand name in spoofed emails. We show the prototype system of our method and the evaluation about precision in detecting the hijacked brand names.

Keywords Phishing Attack, White List, Email, Morphologic Analysis, Social Engineering

1 背景

1.1 フィッシング詐欺の現状

近年のインターネットの普及により，エンドユーザは電子メールやWWW(World Wide Web)によって様々なオンラインサービスを利用することが可能となっている．例えば，オンラインショッピングやオンラインバンキングなどの電子商取引などが挙げられ，これらのサービスは，利用者に対する利便性を大きく高めるものである．しかし，このようなオンラインサービスが普及する一方で，インターネット上でやりとりされる個人情報を狙う犯罪が多発している．このような犯罪の1つに，フィッシング詐欺がある．フィッシング詐欺対策について取り組んでいる米国の団体 Anti-Phishing Working Group (APWG) によれば，フィッシング詐欺は以下のように定義されている [1].

「フィッシング詐欺とは，詐称メールを用いて受信者を偽装 Web サイトに誘導し，クレジットカード番号やアカウント名，パスワード，社会保障番号などの個人財務情報を一般消費者を騙して漏洩させる行為である.」

図1は，フィッシング詐欺の典型的な実行手順を示したものである．まず，信頼のおける金融機関等の企業を装ったメール (フィッシングメール) がエンドユーザの元へ届く (1)．次にユーザはメール本文中に含まれるハイパーリンクによってメールと同じ企業を装った Web サイト (フィッシングサイト) へと誘導される (2)．フィッシングサイトはフォーム等によって個人情報の入力を求めるものが多く，ユーザがこのフォームに個人情報を入力して送信すると，その情報が詐欺師の手に渡ってしまうことになる (3).

フィッシング詐欺は“Phishing”と綴るが，これは

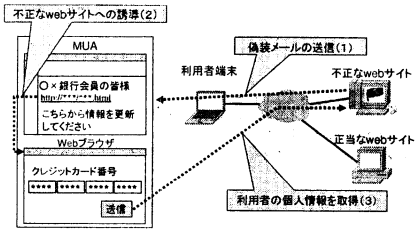

図 1: フィッシング詐欺の概要

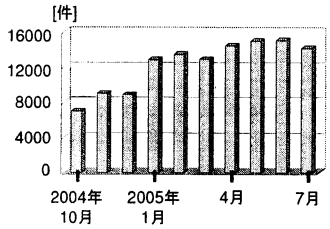

図 2: フィッシングサイトの件数の推移

詐称メールという餌で被害者を釣り上げる手法が従来の詐欺と比較して洗練されていることから，洗練された (Sophisticated) 釣り (Fishing) を語源とする説が有力である．

1.2 フィッシング詐欺の現状

現在，フィッシング詐欺の件数は増加の一途を辿っている．APWG において発表されている，2004 年 10 月から 2005 年 7 月までのアクティブなフィッシングサイトの件数を図 2 に示す．2005 年 6 月の件数は 15,000 件を超えており，2004 年 10 月に比べて倍以上となっている [1][2]．また，フィッシング詐欺の特徴として，フィッシングサイトの平均稼動日数が 5.6 日と非常に短いことが挙げられている．フィッシング詐欺師は，主に米国やアジア諸国の脆弱性のある Web サーバを乗っ取って金融機関等のフィッシングサイトを立ち上げ，個人情報を収集する．そしてフィッシングサイトが発見される前に削除し，証拠を隠滅するのである．

表 1 に，日本国内における主なフィッシング詐欺被害の具体例を示す．日本国内においても被害は増加する傾向にあり，フィッシング詐欺の標的にされた事例だけでなく，公的機関の Web サイトが乗っ取られ，フィッシングサイトの踏み台として使用された例も存在する．

表 1: 国内におけるフィッシング詐欺被害の具体例

対象	時期	内容
クレジットカード会社 A	2005 年 2 月	カード番号，有効期限などの窃盗から偽造カードを作成．
公共機関 B	2005 年 2 月	Web サーバが乗っ取られ，フィッシングサイトの踏み台に使用される．
ポータルサイト C	2005 年 6 月	見た目が酷似したフィッシングサイトを作成し，ID，パスワードを詐取．著作権法違反と不正アクセス禁止法違反の疑いで犯人を逮捕．初の摘発
公共機関 D	2005 年 7 月	Web サーバが乗っ取られ，フィッシングサイトの踏み台に使用される
金融機関 E	2005 年 7 月	見た目が酷似したフィッシングサイトを作成される
ポータルサイト F	2006 年 2 月	オークションに利用される ID，パスワードを入手し，不正に利用．フィッシング詐欺での摘発としては国内初の事例．

2 フィッシング詐欺の手口と電子メールの利用

2.1 フィッシング詐欺の手口

本節では，フィッシングメールやフィッシングサイトにおいて，情報を偽装するために使われている代表的な手口について説明する．

(1) 本物に酷似したフィッシングメール，サイトの作成 フィッシングメール，フィッシングサイトの両者とも，偽装の対象となる企業を装い，利用者を視覚的に騙そうとするものが多い．過去の事例では，企業のロゴマークや，使用するフォントを似せることによって，本物の企業と酷似したメール，Web サイトを使ってフィッシング詐欺を試みるケースが多く存在する．背景には，企業のロゴや画像，フォント等を集めた，「フィッシングサイト作成用ツール」が詐欺師の間で流通しているという事情がある．

(2)HTML メール フィッシングメールの多くは，HTML メールによって記述されている．これは，メールの本文中に含まれるハイパーリンクによって利用者をフィッシングサイトへ誘導する際に，ユーザが目にするリンクの文字列と，リンクをクリックした際に遷移する URL を異なる文字列にすることが可能なためである．例えば，メールの本文中に ○×銀行

 と記述しておけば，○×銀行にリンクしていると見せて，http://www.phishing_site.com/というまったく別のサイトへ誘導することが可能である．

(3) アドレスバー偽装 (1) において述べた企業と酷似したWebサイトの場合は，Webブラウザのアドレスバー(URLが記述されている部分)を確認することによって，当該サイトが偽装されたものであると判定することが可能である．しかし，詐欺の手口は洗練されており，フィッシング詐欺のターゲットとなる企業と類似したドメイン名を取得して利用者の目を欺こうとするものや，Javascriptを利用してブラウザのアドレスバーにポップアップを上書きし，本来接続しているURLを隠して偽のURL情報をポップアップ上に表示するといった手口が存在する．

現在フィッシング詐欺において頻繁に利用されている手口は以上の3種類である．これらの他に，トロイの木馬と呼ばれる手法を用いて悪意のあるプログラムをエンドユーザのPCにダウンロード，実行させてフィッシング詐欺を行なう手口も存在するが，被害件数としては未だ少ない[3]．

2.2 フィッシング詐欺対策における課題

2.2.1 フィッシング詐欺とソーシャルエンジニアリング

2.1節において述べた手口は，Javascriptなどの技術的な手法を用いてはいるが，一方でソーシャルエンジニアリング的な要素が含まれると考えられる．電子メールやWebサイトの見た目を偽装し，情報を受信した側にとって「メールやWebサイトの送信元は常に利用している(信頼できる)企業である」と思い込ませることにより，フィッシングサイトに個人情報を入力して送信するように「仕向けて」いる．つまり，企業と顧客という人間関係を巧みに利用して個人情報を詐取しようとする「ソーシャルエンジニアリング」であると言える．

現在，技術的な側面から様々なアプローチで対策を行なうフィッシング詐欺対策製品が販売されているが，フィッシング詐欺がソーシャルエンジニアリング的な側面をもっている以上，技術的な側面からの対策のみによってこれを防ぐことは難しい．

2.2.2 フィッシング詐欺における電子メールの利用

本論文では，フィッシング詐欺の契機となるのは金融機関等を装ったフィッシングメールであると述べてきた．欧米諸国においては，電子メール以外にもチャットソフトを利用してチャットの相手にフィッシングサイトのURLを送りつけるものや，ブログを利用してURLを貼り付け，フィッシングサイトへ誘導しようとするなど，フィッシング詐欺の入口としてメール以外の手段を用いるケースも見られる．しかし，フィッシング詐欺においては，下記の理由において今後も電子メールが利用され続けると考えられる．

- 金融機関から顧客への新サービスの通知，ECサイトにおける宣伝，オークションサイトにおける落札の通知など，現在すでに電子メールを用いたサービスが定着しており，その手軽さから，企業側が好んで利用しているため，詐欺の対象となりやすいこと
- HTMLメールが利用できること
  - 企業のロゴ等の画像ファイルを多用することによりメールの送信元を偽装することが可能
  - 2.1節に述べたように，HTMLのAタグによって実際の遷移先URLを隠すことが可能
  - Javascriptを埋め込むことにより，正当なWebサイトの上にフィッシングサイトのポップアップウィンドウを表示するなど，様々な偽装が可能

既存のフィッシング詐欺対策には，Webブラウザにおいて URLの検証を行なうものや，個人情報の送信をブロックするものなど，フィッシング詐欺の出口となる部分において対策を施す製品が多くみられる．電子メールにおける対策としては，従来行なわれてきたスパムメールフィルタリングによって，エンドユーザがフィッシングメールを受信する前の段階で対策を行なうものが主流であり，フィッシングサイトへの誘導を防ぐための対策として十分であるとは言えない．

3 提案するフィッシング詐欺対策

3.1 提案手法のアプローチ

2.2節において，フィッシング詐欺にはソーシャルエンジニアリングの側面がある点，そして，詐欺の

入口として電子メールが頻繁に利用されている点を述べた．既存技術による対策のみではこれらの手法に対して決して万全であるとは言えない．

我々は，フィッシング詐欺の入口となる電子メールと，出口となるWebブラウザの両方において，ホワイトリストを用いたフィッシング詐欺対策を提案している．Webブラウザにおけるフィッシング対策に関しては，文献[3][4]において述べている．ホワイトリストを用いたフィッシング詐欺対策とは，正当なWebサイトのURLをリスト化しておき，エンドユーザがこれに該当しないURLにアクセスした場合に警告を表示するというものである．

本論文において提案する，詐欺の入口となる電子メールにおける対策では，エンドユーザの元に届く電子メールが「どの企業を騙ろうとしているのか」というソーシャルエンジニアリング的な情報に着目した．フィッシングメールの場合，メールの見た目や文面によって，フィッシング詐欺の対象となる企業を騙るはずであり，提案手法によってメールからブラウザへ誘導しようとする接続先の企業名を取得することにより，当該企業に絞って効果的にホワイトリストのチェックを実施することが可能となる．

3.2 システムアーキテクチャ

本節では，電子メールからの接続先企業検出によるフィッシング詐欺対策を実現するシステムのアーキテクチャと動作について述べる．図3に，システムのブロック図を示す．電子メールからの情報取得を行なうため，大部分のモジュールはMUA(Mail User Agent)のプラグインとして実装する．メール本文から企業名を抽出するための企業名リスト，正当なWebサイトのURL情報を格納するホワイトリスト，接続先企業を抽出する際に使用するキーワードリストについては，エンドユーザの端末に格納されており，必要に応じてに最新版へのアップデートが行なわれる．

以下に，エンドユーザがMUAにおいてメールを受信し，メール中のリンクをクリックしたことを想定した処理手順を示す．

1. メールの受信と同じタイミングで，メールのヘッダ，本文を取得．HTMLメールの場合には，本文をテキスト化する．
2. エンドユーザがリンクをクリックした時点でクリックされたメールのヘッダ，本文に対して形態素解析を行なう．

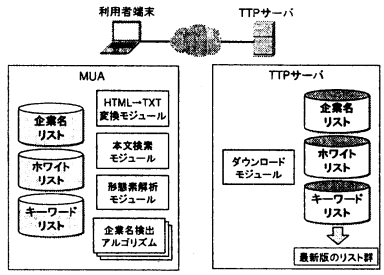

図3: 電子メールにおけるフィッシング詐欺対策システムのブロック図

3. 企業名リストに含まれる企業名を，クリックされたメールのヘッダ，本文において検索．マッチした企業名とその位置(行，列)を取得．
4. 同様にキーワードリストに含まれるキーワードを検索．マッチしたキーワード名とその位置(行，列)を取得．
5. 検出された企業名，キーワードに対して企業名検出アルゴリズムを適用し，各企業名に得点を付与．
6. 企業名ごとに得点の総和を算出し，閾値を超えた企業名を接続先企業名の候補としてユーザに提示し，接続先企業名の選択を求める(図4)．
7. ユーザが選択した企業名のホワイトリストにクリックしたURLが含まれるか否かを検証．含まれない場合にはユーザに対して警告を表示．

ここで，手順5に記述した企業名検出アルゴリズムとは，我々が企業からの広告メール約100通を分析して考案したものであり，例えば，「メールのFrom，Subjectフィールドに含まれる企業名は○○点を付与」「特定のキーワード(格助詞『から』etc.)と隣接している企業名に△△点を付与」といったルールが複数含まれる．

以上の手順により，エンドユーザが受信し，URLをクリックしたメールの接続先となる企業名を抽出し，当該企業のホワイトリストを用いてクリックされたURLの正当性を検証し，正しいURLであると判断されれば，ユーザは安全にWebブラウザでのアクセスを行なうことが可能となる．

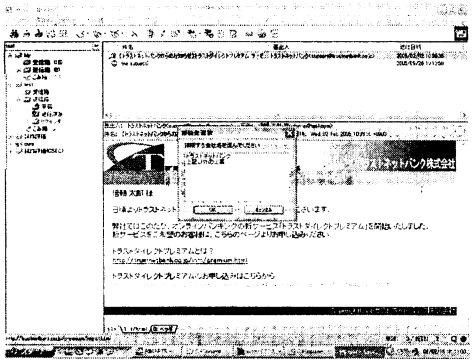

図 4: プロトタイプシステムにおける，企業名選択画面のスクリーンショット

4 プロトタイプによる評価と考察

4.1 プロトタイプによる提案手法の評価

我々は，3 章において述べた提案手法のプロトタイプを，代表的な MUA である Becky![5] のプラグインとして実装した．提案手法では，企業名の抽出に失敗してしまうと，正しいホワイトリストとの照合が行なえないため，企業名を正しく抽出できるか否かが非常に重要である．そこで，本節では，実装したプロトタイプを用いて，企業名の抽出に関する評価を行なった．

評価の際に注目したのは，以下の 2 点である．

1. エンドユーザに提示する接続先企業名候補の中に抽出すべき企業名は含まれるか．
2. 抽出すべき企業名が企業名検出アルゴリズムによって最高得点を獲得し，ユーザに提示される際にリストの先頭となっているか．

後者は，本プロトタイプにおいて，エンドユーザに提示する接続先企業名が複数ある場合，得点が高い企業名順にユーザに提示するという機能に起因するものである．UI の観点から，複数の企業から 1 つをエンドユーザに選択させる場合，最も先頭にある企業名が一番選択しやすいと考えられるため，抽出すべき企業名が最高得点を獲得することが好ましい．これらの点において本プロトタイプが優れているか否かを評価する．

表 2 として，本評価に使用したメールの内容を示す．評価に使用したのは，企業からの広告メール 300 通である (3.2 節において述べたアルゴリズムの考案時に用いた 100 通のメールとは別に用意したものである)．メール送信元企業には，金融機関，EC サイト，ポータルサイト，ショッピングモール等が含まれる．これらのメール中に含まれるハイパーリンクをランダムに選択し，企業名抽出を行なった．評価項目 1 に関する評価結果を表 3 に示す．今回の評価では，評価対象のメールの中で，現在フィッシング詐欺のターゲットとして頻繁に狙われている金融機関からのメールについて，別途評価結果を取得した．評価項目 1 については，抽出すべき企業名が正しく検出される率は全メールを対象とした場合 99.2% であり，金融機関からのメールのみを対象とすると検出率は 100% となった．表 4 は，評価項目 2 の評価結果を示しており，抽出すべき企業名が最高得点を獲得する率は 99.0% となり，金融機関からのメールのみを対象とすると最高得点の獲得率は 98.2% となった．

表 2: 評価に使用した電子メール

分類	メールの数	リンクの数
評価対象となるメールの総数	300 通	3696 リンク
HTML メールの数 (300 通中)	122 通	2716 リンク
金融機関からのメール (300 通中)	70 通	332 リンク

表 3: 企業名の検出率に関する評価結果

評価対象メール	正しく検出されたリンク数	検出率
メール全体	3938 リンク	99.2%
金融機関のメール	332 リンク	100%

4.2 考察

今回の評価では，企業名の検出及び検出の際の順位について，かなり高い結果を得ることができた．このような結果が得られた理由として，以下が挙げられる．

- 評価対象となったメールの中には，本文中に複数の企業の製品や，他社の宣伝をする内容のものも含まれるが，EC サイトやポータルサイトからのメールでは，他社製品へのリンクについても，当該 EC サイト，ポータルサイトを介して接続するようになっており，EC サイトやポータ

表 4: 企業名の提示順位に関する評価結果

評価対象メール	最高順位を獲得したリンク数	獲得率
メール全体	3658 リンク	99.0%
金融機関のメール	326 リンク	98.2%

ルサイトの企業名はヘッダや本文中に繰り返し出現するため，検出が容易であったこと．

逆に，今回検出に失敗もしくは最高得点の獲得に失敗した原因としては，以下が挙げられる．

- 企業名の検出に失敗した原因
  1. メール中に複数のドメインへのリンクが含まれるようなメールの場合，当該リンクの近くに接続先となる企業名が配置されることが多い．このような企業名に得点を付与するアルゴリズムは3.2節において述べた企業名検出アルゴリズムに含まれているが，この場所以外に企業名が現れない場合，当該企業の得点が閾値を超えず，接続先企業名の候補として抽出できなかった．
  2. 今回は企業名を対象として検出を試みたが，企業の中には，サービス名と企業名を使い分けているケースが見られた．(例:「フレッツ」と「NTT東日本」) メール中でサービス名が多用され，企業名の出現回数が少なかった場合に，これを接続先企業名の候補として抽出できなかった．
- 最高得点の獲得に失敗した原因
  1. メール中に複数のドメインへのリンクが含まれる場合に，企業名の検出に失敗したことと同様の理由で，得点が下がってしまった．
  2. ショッピングモール等のメールにおいて，メールのSubjectに他社の製品名，企業名を記載している場合があり，Subjectに記載された企業名の得点が高くなってしまった．

企業名の検出に失敗した原因に関しては，それぞれ以下のような対処によって容易に検出が可能となる．

1. ハイパーリンクの近くで検出された企業名に付与する得点を高くすることにより，リンクの近くに企業名が存在した場合には接続先企業として検出することが可能．
2. 企業名リストに，各企業の名称に加えてサービス名，ブランド名，Webサイトの名称等を含めていくことにより，現在のアーキテクチャに変更を加えることなくサービス名等の検出が可能．

以上のような対処によって，今回検出に失敗した企業名を抽出させることは容易に可能である．但し，前者のようなパラメータの変更は，選択肢となる企業数の増加につながるため，パラメータ変更後に再度評価を実施する必要がある．

5 まとめと今後の課題

フィッシングメールによってエンドユーザを巧みに誘導し，フィッシングサイトにおいてユーザの個人情報を狙うフィッシング詐欺の件数は年々増加する傾向にあり，その手口も洗練されたものとなってきている．

本稿では，フィッシング詐欺対策として，フィッシング詐欺の入口となる電子メールを利用し，ソーシャルエンジニアリングへの対策を考慮したフィッシング詐欺対策を提案した．また，提案手法を実装したプロトタイプの評価では，本手法の核となる接続先企業名の検出において，高い性能を持つことが示された．

今後は，4.2節において述べたとおり，接続先企業名の検出率をさらに高めるために，接続先企業名検出アルゴリズムと検出に使用するパラメータ群の改良を行なう．また，正当なWebサイトから送られるメールだけでなく，フィッシングメールを対象とし，当該メールが騙る企業名を確実に抽出することが可能であるか否かの評価を行なうことにより，本手法のフィッシングメールへの有効性を示す必要があると考えている．

参考文献

[1] Anti-Phishing Working Group:
Phishing Activity Trends Report - July 2005,
http://www.antiphishing.org/APWG_Phishing_Activity_Report_Jul_05.pdf (2005).

[2] 荒金陽助, 柴田賢介, 金井敦: フィッシング詐欺対策に向けた一考察, マルチメディア, 分散, 協調とモバイル (DICOMO 2005) シンポジウム, pp. 481–484 (2005).

[3] 柴田賢介, 荒金陽助, 塩野入理, 金井敦: フィッシング詐欺の現状とアドレスバー偽装手口に対する一考察, グループウェアとネットワークサービスワークショップ 2005, pp. 19–24 (2005).

[4] 柴田賢介, 荒金陽助, 金井敦: フィッシング詐欺対策のための URL 検証方式の提案, マルチメディア, 分散, 協調とモバイル (DICOMO 2005) シンポジウム, pp. 485–488 (2005).

[5] : Becky! Internet Mail.
http://www.rimarts.co.jp/index-j.html.