情報処理学会
グループウェアとネットワークサービス研究会
2005年11月10日, 11日

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

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 ブロードバンド環境の普及により，さまざまなネットワークサービスにおいて ID やパスワードを用いた認証，電子商取引が行なわれ，多くの個人情報がネットワーク上でやりとりされている．現在，これらの情報を狙う犯罪としてフィッシング詐欺が多発している．世界的にはフィッシング詐欺のターゲットは金融機関にとどまらず，今後は日本においても社会／行政サービスへの影響が懸念される．本稿では，フィッシング詐欺の現状と今後の傾向について述べるとともに，代表的なフィッシング詐欺の手口であるアドレスバー偽装を検知する手法を提案する．提案手法の評価では，アドレスバー偽装の手口を用いたフィッシングサイトに対し，高い検知率を示すことが確認された．

キーワード 情報セキュリティ，フィッシング詐欺，ネットワークサービス，社会／行政サービス

Recent Trend of Phishing and a Study for Address-bar Spoofing

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

Abstract In recent years, electronic commerce has become more popular and many people use online shopping, banking, etc. 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 against address-bar spoofing attack which is one of the typical methodologies of phishing. We confirm that our method detects address-bar spoofing sites with a high rate.

Keywords information security, phishing, network services, social/governmental services

1 フィッシング詐欺とは

インターネット技術の発展により，各家庭にブロードバンド環境が普及し，多様なオンラインサービスが提供されている．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や，電子政府への取り組みなどが挙げられる．これらのサービスの普及により，利用者に対する利便性が高まる一方で，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，フィッシング詐欺がどのようにして実行されるかを示したものである．その流れはまず，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) が利用者の元へ届く (1)．次に利用者はメール本文中に張られたハイパーリンクによって不正サイト (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に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，利用者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．

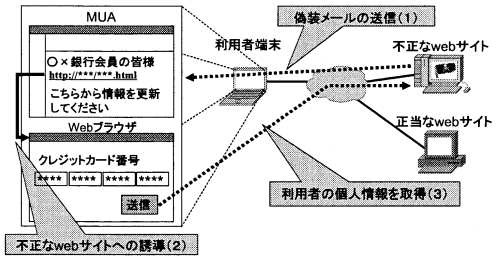

図 1: フィッシング詐欺の概要

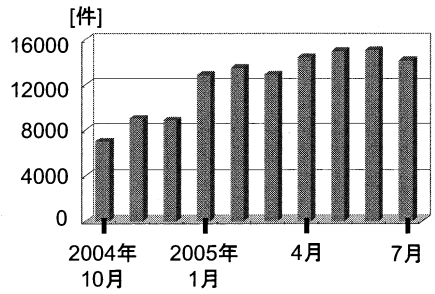

図 2: フィッシングサイトの件数の推移

2 フィッシング詐欺の現状と傾向

2.1 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 [2]．図 2 として，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示す [1]．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．国別の統計では，オンラインでのショッピングや，クレジットカードの利用が普及している米国における被害が最も多い．また，フィッシング詐欺のターゲットとなる企業は少数に集中する傾向があり，フィッシングサイトの総件数のうち，80% を 6 社が占めている．フィッシング詐欺のターゲットとなる企業の内訳は，85% が金融機関を狙ったものであり，オンラインバンキングにおける口座番号，個人情報やクレジットカード番号を詐取しようとするものが大部分を占めている．金融機関を狙ったフィッシング詐欺では，オンラインバンキングの会員向けのフィッシングメールを送付し，「こちらのリンクから情報を更新しなければアカウントを停止します」といった内容で利用者を不安にさせ，フィッシングサイトに誘導するケースが多い．表 1 に，日本国内における 2005 年のフィッシング詐欺被害の具体例を示す．金融機関が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ある．日本においてもフィッシング詐欺の件数は増加する傾向にあり，早期の対策が望まれる．

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
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
銀行 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

2.2 フィッシング詐欺の今後の傾向

2.1 節において，フィッシング詐欺のターゲットの大部分が金融機関であると述べた．しかし，海外ではフィッシング詐欺の件数が多くなり，その認知度が上昇しているため，フィッシング詐欺の成功率が下がっていると推測される．このような現状を受けて，新たなターゲットを狙ったフィッシング詐欺が話題となっている．表 2 として，金融機関以外を狙ったフィッシング詐欺の事例を示す．

事例 1 は，オンラインゲームのアカウントを停止したという旨のフィッシングメールを送り，アカウントの再開のためにログインデータを入力させるというものである．詐欺師は詐取したログインデータを利用してゲームにログインし，ゲーム上の仮想世界で流通する武器や通貨を不正に入手する．ゲーム上の仮想アイテムは，オークションサイトなどで現金で取引されているケースがあるため，入手したアイテムを販売する目的があったと推測される．

事例 2 は，サッカーのワールドカップを主催する機関を装い，くじに当選したので賞金を振り込みたいといった形で銀行口座の情報を聞き出そうとするものである．本事例はヨーロッパ各国において展開されており，大規模な詐欺集団による犯行である可能性が高い．

事例 3 は，中国に特有のフィッシング詐欺であると

表 2: 金融機関以外をターゲットとしたフィッシング詐欺の事例

事例	時期	内容
事例 1	2005 年 9 月	オンラインゲームのアカウントを狙うフィッシング詐欺．ID，パスワードを詐取
事例 2	2005 年 9 月	ヨーロッパにおいて，サッカーくじに当選したことを知らせるフィッシングメールにより，銀行口座の情報を詐取しようとする
事例 3	2004 年	中国において，日本の文部科学省にあたる教育部のフィッシングサイトを立ち上げ，大学を卒業した学生の ID を詐取

言える．中国では，大学を卒業した学生の情報を日本の文部科学省にあたる教育部が一括で管理しており，卒業した学生には卒業証明書が紙媒体で発行されるとともに，自身の卒業証明書の画像を文部科学省において確認するための ID，パスワードが払い出される．学生を採用しようとする企業に対しても卒業証明書の画像参照用の ID が払い出され，企業は電子的な卒業証明書と学生が持参する紙媒体の卒業証明書を照合することにより，正当な学歴を持つ学生であることを確認している．フィッシング詐欺師は，教育部のフィッシングサイトを作成し，学生の ID，パスワードを詐取することにより，卒業証明書の画像を参照し，偽造卒業証明書を作成する．偽造された卒業証明書は学歴のない学生に対して販売され，企業は学歴のない学生を高学歴の学生として採用してしまう可能性がある．

事例 3 に見られるように，海外においては公的機関の Web サイトは他の企業のフィッシングサイトの踏み台として使用されるだけでなく，フィッシング詐欺のターゲットとなる傾向がある．日本においてもさらなるブロードバンドの普及により，今後は行政等を含めたさまざまな分野においてもオンラインサービスが浸透していくことが予測されるが，このようなサービスがフィッシング詐欺のターゲットとなる可能性は十分にあり，サービスの普及への脅威もしくは，サービス導入への障壁となる恐れがある．

3 フィッシング詐欺の技術的手口

3.1 フィッシング詐欺手口の種類

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技術的手口について説明する．

(1)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．

(2) 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．

(3) アドレスバー偽装 上述した企業と酷似した 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．後者の手口については，3.2 節で詳しく述べることとする．

(4)DNS Poisoning 大部分の利用者が利用している OS である Windows，Linux などには，hosts ファイルといってインターネット上のホスト名と IP アドレスの対応付けを記述し，DNS(Domain Name System) による名前解決を行なう前に参照させるためのファイルが存在する．フィッシング詐欺においては，これを悪用し，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利用者の PC にダウンロード，実行させる．このプログラムは，hosts ファイルを書き換え，金融機関などの Web サイトのドメイン名に対し，

フィッシングサイトのIPアドレスを対応付ける．これにより，利用者をフィッシングサイトへと誘導することが可能となる．類似した手口には，DNSサーバを攻撃し，テーブルを書き換えてフィッシングサイトへ誘導する手口も存在する．

(5) キーロガー　本手口もDNS Poisoningと同様に，トロイの木馬の手法を用いるものであり，利用者に悪意のあるプログラムをダウンロード，実行させる．このプログラムは，利用者のキーボード操作のログを取得し，特定のサーバに送信する機能を持つ．オンラインバンキングなどにおいてキーボードからパスワード，口座番号などの個人情報を入力すると，すべての情報が詐欺師の手に渡ってしまうという手口である．

フィッシング詐欺に用いられる主な手口は以上の5種類に集約される．2005年6月〜9月にかけて，文献[3]やSPAMメールを元にフィッシング詐欺手口に関する調査を行なった結果，上記の手口のうち，頻繁に使われているのは手口(1)，(2)，(3)の3種類であり，これらの手口が使われる割合は90％を超えていた．

3.2　アドレスバー偽装手口

3.1節では，フィッシング詐欺手口の種類とその概要について述べた．本節では，手口の中でも頻繁に利用されている，Javascriptを用いたアドレスバー偽装手口について詳しく説明する．

Javascriptを利用したポップアップは，従来Webサイトを表示する際に，利用者に注目させたい広告等を表示する目的で，Webサイト運営者に利用されてきた．しかし，このポップアップは，以下のような特徴を持つために，フィッシング詐欺に悪用されている．

- Webサイト運営者が画面上の任意の位置に配置できる
- URLを示すアドレスバーや，ツールバーを持たないポップアップを作ることができる

図3として，アドレスバー偽装のポップアップを表示したサンプルのWebサイトのスクリーンショットを示す．図では，ポップアップの存在を分かりやすくするため，少しずらして表示したものを示している．このように，枠線やアドレスバーを持たないポップアップに，偽装対象となるWebサイトのURLを記述しておき，ブラウザのアドレスバーに重ねて配置することによって，アドレスバーの偽装が可能となる．実際にブラウザのアドレスバーに重なるようにポップアップを配置すると，本物のWebサイトとフィッシングサイトとの区別はつきにくく，フィッシングサイトを判別することは非常に困難である．このように，フィッシング詐欺の手口は洗練されたものであり，必ずしもコンピュータリテラシの低い利用者のみに被害の危険があるというものではなくなっている．

図3: アドレスバー偽装サイト

4　提案するフィッシング詐欺対策

4.1　ホワイトリストを用いたフィッシング詐欺対策

本研究では，ホワイトリストを用いて，Webサイトの正当性を検証し，利用者をフィッシング詐欺の被害から守るための対策技術を提案している．現在，フィッシング詐欺対策は，ブラックリスト方式とホワイトリスト方式の2種類に分けることができる．ブラックリスト方式は，フィッシングサイトが見つかると，当該サイトのURLをリストに登録し，以降利用者がブラックリストに掲載されたURLにアクセスした場合には，警告を表示する．しかし，APWGの報告によると，現在のフィッシングサイトの平均寿命は5.7日とされており[1]，フィッシングサイトが発見され，ブラックリストに掲載された時にはフィッシングサイトにアクセスできなくなってしまうといったケースも見られ，掲載されるまでの間に被害が発生してしまう可能性が高い．

ホワイトリスト方式では，TTP(Trusted Third Party)が正当なWebサイトのURLを管理し，利用者はブラウザでWebサイトにアクセスする際に，当該サイトが正当なものであるか否かをホワイトリストと比較し，URLの検証に失敗した場合には正当なWebサイトではない可能性があるとして利用者に対して警告を表示する．図4として，提案手法のアーキテクチャを示す．ホワイトリスト方式は，Webサイトの運営者がサイトの構成を変更した場合に，ホワイトリストに対しても変更を加えなければならないという欠点があ

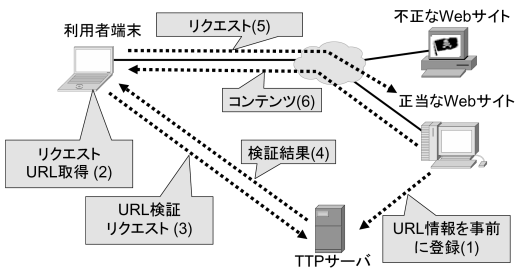

図 4: ホワイトリストを用いたフィッシング詐欺対策

るが，本手法では，ディレクトリレベルという概念を導入し，ホワイトリストに掲載される URL を構造化して管理することにより，柔軟かつセキュアなホワイトリストの運用を可能としている [4].

また，フレーム構成を持つ Web サイトに対し，一部のフレームのみを乗っ取るといった手口が存在することから，ホワイトリストにはトップページの URL だけでなく，フレームを構成する URL や，HTML の form タグの action 属性に含まれる，フォームの送信先 URL を含めて，Web サイト全体を URL 検証の対象としている.

本方式は，ホワイトリストに掲載されていない Web サイトについては警告を発するという構造になっており，ブラックリスト方式と比べて安全側に倒れるフェールセーフを基本コンセプトとしている.

4.2 アドレスバー偽装検知

4.1 節において，ホワイトリストを用いたフィッシング詐欺対策について述べたが，現在，我々は本方式にアドレスバー偽装を用いたフィッシングサイトの検知機能を追加し，フィッシング詐欺に遭う危険性をさらに抑える手法を検討している.

図 5 に，アドレスバー偽装検知機能の概略を示す．本機能は，フィッシングスクリプトテーブルを備えており，アドレスバー偽装に利用される Javascript の関数名等をテーブルとして保持しておく．利用者が Web サイトにアクセスした際に，ブラウザ内で HTML ソースを取得し，テーブル内のスクリプトとのパターンマッチングを行なう．HTML ソースにアドレスバー偽装と思われるスクリプトが検知された場合には，ブラウザ上に警告ダイアログを表示することにより，利用者に通知する.

本機能の特徴は，以下の 2 点である.

1. パターンマッチング時に，ポップアップの表示位置を考慮

2. Javascript の unescape 関数を用いたパターンマッチング回避手口への対策

前者は，Javascript の関数名をキーとした文字列のパターンマッチングを行なうだけでなく，関数のパラメータを考慮し，アドレスバー偽装を目的としたポップアップを表示する場合にのみ警告を表示するというものである．本方式では，アドレスバー偽装を用いた複数のフィッシングサイトの HTML ソースを解析し，ポップアップ表示のための関数の，位置を調節するパラメータの傾向を分析した結果をフィッシングスクリプトテーブルに含めている．よって，ポップアップ表示のための関数が HTML のソースに含まれており，かつ関数のパラメータがテーブルに記述された範囲内にある場合にのみ，アドレスバー偽装サイトとして検知することが可能となる.

後者は，アドレスバー偽装フィッシングサイトの中に，Javascript の unescape 関数を用いて，HTML ソースの中の Javascript の部分を unicode 化し，ウィルス検知プログラムや，我々が提案しているパターンマッチングから逃れようとするものが存在するため，これに対処する機能として追加したものである.

提案しているアドレスバー偽装検知機能は，フィッシングサイトに利用されるスクリプトを検知するというブラックリスト的なアプローチとなっているが，本手法は以下のような理由で有効であると言える.

- 3.1 節でも述べたとおり，フィッシングサイト作成用ツールが出回っており，アドレスバー偽装サイトの中には共通する Javascript のパターンを持つものが存在する

- フィッシングサイトの URL をブラックリスト化して URL のマッチングを行なう手法とは異なり，HTML のソースレベルでのマッチングを行なっているため，フィッシングサイトの寿命とは無関係に，同様の手口が使われる限りフィッシングサイトを検出することができる

5 プロトタイプによる評価

本章では，4.2 節で述べたアドレスバー偽装検知機能を搭載したプロトタイプを作成し，偽装サイトの検知率に関する評価を行なった結果を示す．評価では，3.1

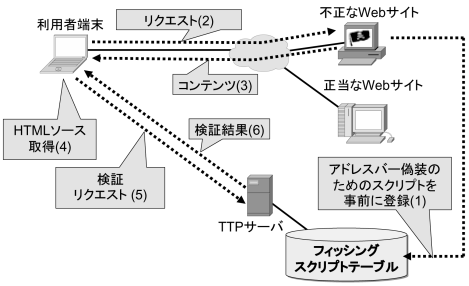

図 5: アドレスバー偽装検知機能

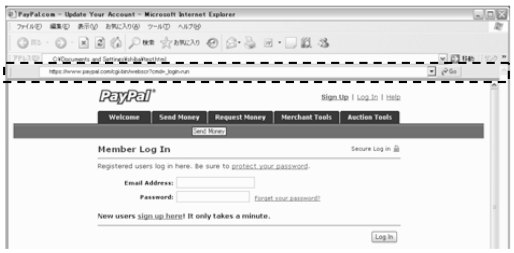

図 7: アドレスバー全体を偽装するフィッシングサイト

節と同様のフィッシングサイトに関する調査を行ない，発見されたサイトのうち，アドレスバー偽装手口を用いているものを対象とし，偽装サイトにアクセスした場合に，正しく検知が行なえるか否かの検証を行なった．評価の結果を図 6 として示す．今回評価の対象となったアドレスバー偽装サイトは 15 件であり，そのうち Javascript を用いて単純にポップアップを表示しようとするものが 11 件，Javascript の unescape 関数を用いているものが 3 件，それ以外のものが 1 件であった．評価の結果としては，15 件中 14 件のフィッシングサイトを検知することに成功し，検知率は 93.3% となった．検出に失敗した 1 件のフィッシングサイトは，図 7 に示すように，アドレスバーの URL 部分だけでなく，ブラウザのアドレスバー全体を偽装するものであり，Javascript の構造がかなり複雑なものとなっていたため，正しく検知することができなかった．しかし，現在出回っているアドレスバー偽装手口については，かなりの確率で検知できるという結果を得ることができた．

6 まとめと今後の課題

利用者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．今後はオンラインバンキング，オンラインショッピングなどの電子商取引だけでなく，公的機関における電子行政サービスなどへの影響も懸念される．本稿では，フィッシング詐欺対策として，ホワイトリストを用いた URL 検証を行なう手法を提案するとともに，フィッシング詐欺の手口として頻繁に利用されるアドレスバー偽装を検知するための手法について述べた．また，本手法を実装したプロトタイプを評価し，その実現可能性を示すとともに，高い偽装サイト検知率を持つことを示した．今後は，アドレスバー偽装フィッシングサイトに対するさらなる検知率のアップを図るだけでなく，新しいフィッシング詐欺手口への対策について取り組んでいく予定である．

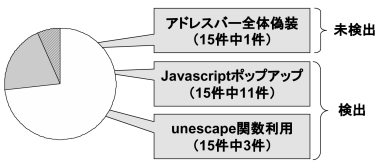

図 6: アドレスバー偽装検知機能に関する評価結果

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] : フィッシング詐欺サイト情報. http://www.rbl.jp/phishing/.

[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).