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

2007－ＭＢＬ－41（14）
2007／5／18

携帯電話に対するフィッシング詐欺の可能性と対策について

荒金　陽助†　柴田　賢介†　佐野　和利†　塩野入　理†　金井　敦†

† NTT 情報流通プラットフォーム研究所　〒239-0847 神奈川県横須賀市光の丘 1-1

あらまし　オンラインショッピングなどのオンラインサービスの普及に伴い，アカウント情報やクレジットカード情報を狙ったフィッシング詐欺が多発するようになってきた．オンラインサービスにおいてクレジットカード情報や金融口座情報などの重要情報がネットワーク上でやりとりされるようになり，フィッシング詐欺の被害も甚大となってきている．この犯罪は，オンラインサービス利用時の操作に関して利用者を騙すものであり，ターゲットとするサービスや利用者に応じて様々な亜流が出現してきている．この，フィッシング詐欺がターゲットとするオンラインサービスという観点では，携帯電話によるオンラインショッピング件数も増加しており，携帯電話を狙ったウィルスの発生など，携帯電話に関わるフィッシング詐欺が増加してもおかしくない状況にある．本稿では，昨今のフィッシング詐欺の状況を概観すると共に，携帯電話を狙ったフィッシング詐欺対策を提案する．

キーワード　携帯端末，モバイルアプリケーション，モバイルコンピューティング

A Study of Phishing on Cellular Phone: Fraudulent Tricks and Solutions

Yosuke ARAGANE†, Kensuke SHIBATA†, Kazutoshi SANO†,

Osamu SHIONOIRI†, and Atsushi KANAI†

† NTT Information Sharing Platform Laboratories, NTT Coporation
1-1 Hikarino-oka, Yokosuka, Kanagawa, 239-0847 Japan

Abstract　According to the spread of online services such as online shopping, the phishing fraud have been famous crime which steals consumers' personal identity data and financial account credentials. Since important identity information such as credit card information has been sent in network, the damage caused by phishing is increasing. There are many types of phishing depending on each online services. According to the market size point of view, the online service on cellular phone should be next target of phshing. In this paper, we discuss about the aspects of phishing and propose a new anti-phshing concept.

Key words　Mobile Terminal, Mobile Applications, Mobile Computing

1. はじめに

ネットワーク環境の普及およびアプリケーション技術の開発によって，日常生活の様々な局面にオンラインサービスが浸透するようになってきた．これらオンラインサービスの普及に伴い，それらのサービスで用いられる個人を特定するためのなどの重要情報を詐取しようとするフィッシング詐欺が多発するようになってきた．フィッシング詐欺とは，クレジットカード情報や金融口座のアカウント情報など，個人の様々な重要情報を盗む犯罪であり．情報を送信させるための偽装ウェブサイトに被害者を誘導するために偽装電子メールを用いること，およびこれらの偽装ウェブサイトと偽装電子メール（フィッシングメールと呼ばれる）の手口において，心理的および技術的手段を駆使することを特徴とする [1]．これらの手段が巧妙に使われることで，多くの被害者は情報を詐取されたことすら認識することが難しいことも問題である．

主要インターネット専業銀行の預金残高及び口座数を図 1 に示す．オンラインサービスの普及と共に，サービスの決済に利用されるオンラインバンキングの利用が増加してきた．図 1 はインターネット専業銀行に関するデータであり，オンラインバンキング全てを示すデータではないが，その傾向は同様であると思われる．このようなオンラインバンキングをオンラインサービス上で利用する場合には，種々のアカウント情報をやりとりする必要が生じる．フィッシング詐欺はこのやりとりをターゲットとして情報の詐取を行う．なお，類似のやりとりは，フィッシングでない正規の手順においても発生するものであり，一般の利用者が正規の手順とフィッシングの手口とを見分けることは非常に困難である．

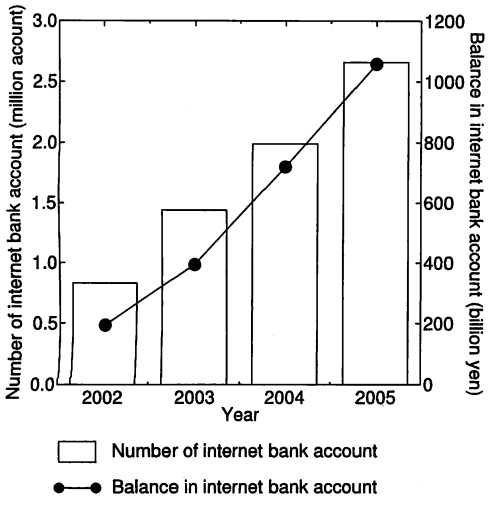

図 1　主要インターネット専業銀行の預金残高及び口座数 [2]

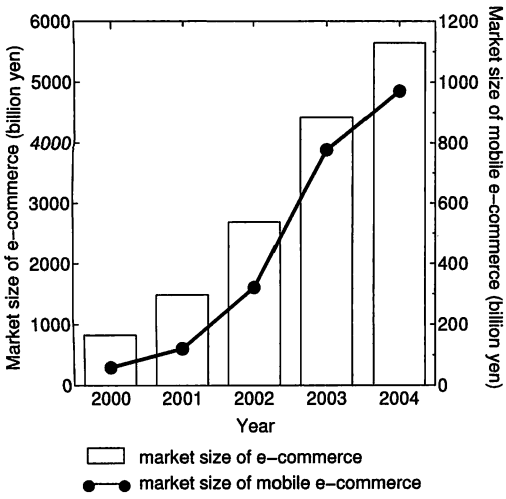

図 2　消費者向け電子商取引の市場規模の推移 [3]

フィッシング詐欺はその手口が単純であるがゆえに，様々なサービスに対して様々なタイプが発生している．あるサービスがターゲットになるかは，ひとえに犯罪の効率によって決定され，その大きな要因にサービスの規模が挙げられる．α というサービスの加入者が多いとしたときに，不特定多数に対して α を偽るフィッシングメールを送った場合に，受信者がサービス α の加入者である可能性が高まり，結果としてフィッシング詐欺に引っかかる被害者の数を見込むことが可能となる．

フィッシングがターゲットとするオンラインサービスとほぼ同様と言える BtoC の電子商取引の市場規模について図 2 に示す．ここ 5 年の推移ではあるが，急速に電子商取引が広がっていることが分かる．そのような中で携帯電話などのモバイル機器を用いたモバイルコマースの市場も着実に増加している．モバイルコマースの市場は 2004 年には 9,710 億円に達しており，2000 年の電子商取引全体の市場規模（8,240 億円）を凌駕する

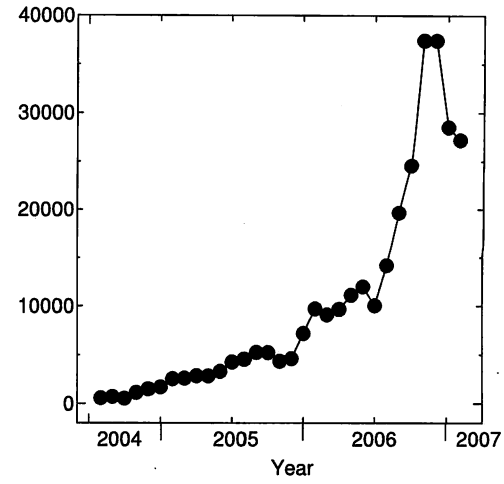

図 3　新たに発見されたフィッシングサイト数 [1]

状況となっている．従って，フィッシング詐欺のターゲットとしてのモバイルコマースの市場規模は魅力を増しつつあり，いつモバイルコマースをターゲットとしたフィッシング詐欺が多発してもおかしくない状況にある．

そこで本論文では，フィッシング詐欺について説明すると共に，モバイルコマースにおけるフィッシング詐欺の危険性を示し，携帯電話におけるフィッシング詐欺対策の一案を提案する．

2.　フィッシング詐欺とは

本章ではフィッシング詐欺の特徴とその典型的な流れについて説明する．

2.1　統計的特徴

フィッシング詐欺について様々な観点で調査を行っている Anti-Phishing Working Group (APWG) のレポートの概要を表 1 に示す．

APWG に報告されただけでも 1ヶ月間で 27000 以上のサイトが新たに発見されており，870 サイト/日以上のペースでフィッシングサイトが開設されていることが分かる．一方，フィッシング詐欺がターゲットとするブランド数は 135 ブランドであったが，そのうちの上位 80%は 10 のブランドに集中しており，1 章で述べたとおり，フィッシング詐欺の効率を追求することで，必然的にユーザの多い巨大ブランドが集中的にターゲットとなる構図が示されている．また，フィッシング詐欺がオンライン詐欺である特徴として，フィッシングサイトの短寿命化が挙げられる．2004 年の 10 月には 6.4 日であったフィッシングサイトの平均寿命が，一年後の 2005 年 12 月で 5.3 日，そしてさらに約一年後の 2007 年 1 月で 4.0 日と 2 年間で 2.4 日縮まっており，フィッシング詐欺の短期決戦化が進んでいると考えられる．

これらの中から特に新たに見つかるフィッシングサイト数に注目し，その時間推移を図 3 に示す．2004 年の 10 月には 1142 サイト/月であったものが，2005 年の 12 月で 7197，そして 2007 年 1 月で 27221 と 24 倍近い伸びとなっている．推移としては

表 1　APWG レポートの概要 (2007 年 1 月) [1]

contents	value
Number of unique phishing sites received in January 2007	27221
Number of brands hijacked by phishing campaigns in January 2007	135
Number of brands comprising the top 80% of phishing campaigns in January 2007	10
Country hosting the most phishing websites in January 2007	United States
Contain some form of target name in URL	24.5%
No hostname just IP address	18 %
Percentage of sites not using port 80	3.0%
Average time online for site	4.0 days
Longest time online for site	30 days

完全な単調増加ではないため，2006 年末からの減少が各種対策や啓蒙活動の成果なのか，誤差の範囲に過ぎないのかは予断を許さないが，サイバー犯罪の一つとして対策の緊急度が増していると思われる．

2.2 典 型 例

インターネットバンキングを対象とした典型的なフィッシング詐欺の流れを図 4 に示し，そのプロセスを説明する．犯人を M，預金者 A，銀行 B，第三者 C とする．

① サーバ乗っ取り

M は C の Web サーバの脆弱性等を利用して侵入し，自己の支配下に治める．

フィッシングサイトを構築するにあたっては，それが犯罪目的であるため，フィッシング詐欺師自身が管理をする（または借りている）サーバ上にそれを構築することはほとんど無い．多くは，ターゲットとするブランドとも全く無関係なサイトをクラックしてフィッシングサイトを開設する．わが国でも，公共機関や大学のサイトなどがクラックされ，フィッシングサイトを作成された事例が報告されている [4]．

② 偽 HP 作成

M は B の本物の Home Page (HP) に類似する偽 HP を作成する．偽 HP には「登録情報の更新」を求める記載がある．

ターゲットとするサイトと類似したサイトを作る際に，サイトの情報がデジタルデータであるため，容易にコピー可能であることもフィッシング詐欺の拡大を招いていると考えられる．

③ 偽 HP 公開

M はインターネットに接続された C の Web サーバ上で偽 HP を公開する．

ターゲットとするブランドとは無関係のサイトにフィッシングサイトを構築した場合でも，ディレクトリ名をそれらしい名称にしたりすることで，被害者を巧妙に騙すことも行われる．また，フィッシング詐欺師が自信で管理するサイトを利用することは少数例であるが，ターゲットとするブランド名と似たドメインを取得し，一見して別のサイト（ドメイン）とは思わせない手法を採用するフィッシングサイトも存在する．

④ 偽メール作成

M は偽 HP へのアクセスを誘引するメールを作成する．メールには「登録情報の更新」を求める記載がある．

様々な DM や実際の企業からの（正しい）お知らせメールが氾濫する今日において，それらの（正しい）メールの文面を参考に作成されたフィッシングメールを，その文面から偽メールだと判別するのは難しい．「メール発信者と称する企業が，クレジットカード番号を記入させることはない」，または，「重要事項を郵送ではなくオンラインで更新・確認させることはない」，などの企業の情報取り扱いポリシまで踏み込んだ高いコンピュータ/ネットワークリテラシーを必要とするからである．また，文面が正当なメールに類似していることから，スパムメールフィルタなどで排除することも一般的には困難である．

⑤ 偽メール送信

M は B を送信元と偽ったメールを特定多数または不特定多数の第三者（A を含む）に大量送信する．

メールの送信元（from フィールド）は詐称することが技術的に可能であるため，受信者のメーラーにはインターネットバンキングの銀行や，オンラインサービス会社，クレジットカード会社の名称が発信者名として表示されることとなる．

⑥ 偽メール受信

A はフィッシングメールを受信する．

上記のような送信元の詐称や，サブジェクトの文面に「緊急のお知らせ」などの注意を喚起するような文面や詐称する企業名が記載されたりしているために，受信者は詐称企業からの読むべきメールであると誤認する．その結果，メール一覧の中から本文を閲覧するようそのメールを選択してしまうことになり，より高度な詐称の手口（記述）が駆使されているメール本文に誘い込まれてしまう．

⑦ 偽 HP にアクセス

A は受信したメールの記載内容を信じてその指示に従い偽 HP にアクセスする．

フィッシングメールの発信者および内容を信頼し，メール内のリンクをクリックすることで，利用者は詐称された企業のサイトだと誤認したままフィッシングサイトに誤誘導されることになる．フィッシング詐欺師にとって，このリンクをクリックさせるまでがソーシャルエンジニアリングの勝負所であり，一方，利用者（被害者）にとっては，リンクをクリックするまでにフィッシング詐欺だと見破ることが重要となる．なぜならば，フィッシングサイトはフィッシングメールの内容を踏襲しており，フィッシングメールを信頼したユーザに対して，同様の内容を持つフィッシングサイトを信頼させることは非常に容易だからである．

⑧ 登録情報を送信

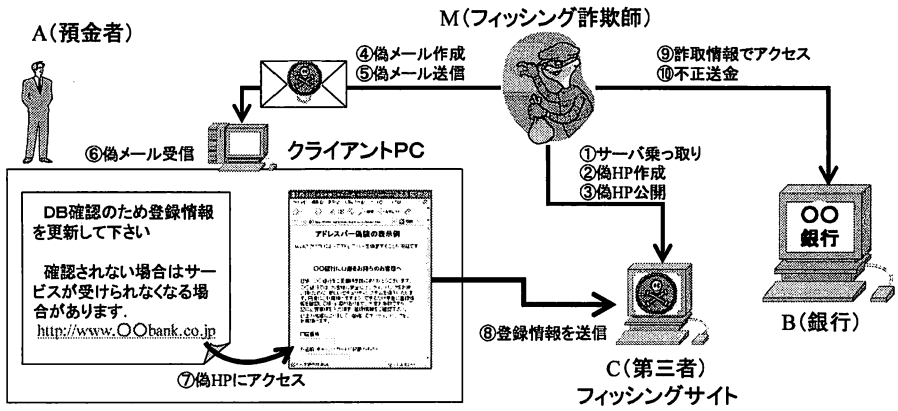

図 4　典型的なフィッシング詐欺の流れ

A は偽 HP の記載内容を信じて ID，パスワード等の A の個人情報を偽 HP に自ら入力する．

フィッシング詐欺師はフィッシングメールから自然な流れで，個人情報を入力・送信するようにし向ける．詐取対象となる情報は，オンラインサービスのアカウント情報の他に，換金性の高いクレジットカードの情報や個人を特定する情報となるソーシャルセキュリティナンバー（社会保障番号：米国）などの情報が含まれることが多い．

⑨　詐取情報でアクセス

M は B のインターネットバンキング HP にアクセスし，A の ID，パスワード等をシステムに入力する．

オンラインサービスのアカウント情報であれば，そのオンラインサービスへのログインがこれに該当する．

⑩　不正送金

B は A になりすまし，A の口座から預金を M の管理下にある他の口座等へ送金する．

3.　携帯電話に関わるフィッシング詐欺の脅威

このようにフィッシング詐欺はオンラインサービス利用者を騙すために，様々な手口を活用することで，不正な利益を上げている．今まで，フィッシング詐欺の対象は PC を用いたオンラインサービス利用者であったが，オンラインサービスの媒体として一定の利用者数を持っている携帯電話もそのターゲットとなる可能性が十分にある．事実，携帯電話をターゲットとしたフィッシング詐欺も発生してきている [5], [6]．そこで本章では，携帯電話に関わるフィッシング詐欺の脅威について説明する．

3.1　対象の拡大

詐欺という犯罪の性質を考えると，利益をより大きくするためには二つの手段が存在する．ひとつは，より多くの対象に対して詐欺行為を行って母数を確保することであり，もうひとつは，より巧妙な手口を考えだして成功確率を向上させることである．本節では前者の観点から携帯電話に関わるフィッシング詐欺について述べる．

図 2 に示したように，2004 年時点での携帯電話等から利用されるモバイル向け電子商取引の規模は一兆円規模に肉薄しており，2000 年の電子商取引全体の市場規模を凌駕している．携帯電話からのインターネットアクセスが始まった当初から，オンラインバンキングなどオンラインサービスの提供が行われていた．しかし，それらの多くは「公式サイト」と呼ばれる，メニューのトップページからたどれるサイトであり，インターネット上のオンラインサービスに直接アクセスされることは少なかった．

これにはいくつかの理由が考えられる．一つは，インターネット上に携帯電話向けのオンラインサービスを提供するサイトが少なかったことである．当初は，携帯電話からのインターネットアクセス数（ユーザ数）が限定的であり，ブラウザの表示エリア制限などによる携帯電話向け専用サイトを構築するコストと，それを利用する人数とのバランスが釣り合う状況ではなかった．また，インターネット上のサイトにアクセスすることは可能であったが，その URL を携帯電話のテンキーインタフェースを用いて入力する必要があり，ユーザビリティが悪かったことがある．さらには，携帯電話向けオンラインサービスが少ないこともあり，公式サイト以外において，携帯電話にクレジットカード番号や口座番号などの金融情報を投入することに対する心理的障壁も高かったと考えられる．

しかしながら，昨今では携帯電話からの各種オンラインサービスの利用は急激に増加している．様々な広告媒体に携帯電話向けサイトの URL を示す QR コードが記載されたり，メールマガジンのコンテンツ内にリンクが記載されていたりと，ユーザによる URL 入力の手間を可能な限り省く技術・工夫が普及してきていることも一つの理由であろう．また，Mobile Suica を始めとする携帯電話による様々な決済手法が広がり，携帯電話にクレジットカード番号などの金融情報を入力することへの心的障壁も下がってきている．

これらの要因により，フィッシング詐欺の素地としての携帯電話プラットフォームは電子商取引が活発化した頃の PC とほぼ同等となったと考えられ，最早フィッシング詐欺のターゲットとして十分な大きさを持った市場が存在していると言える．

3.2 ユーザビリティ

一方本節では，より巧妙なフィッシング詐欺の手口により，詐欺の成功率を向上させる手法について述べる．

携帯電話のインタフェースは入力・出力ともに，PC と比較してかなり限定されている．特に出力側の制限はフィッシング詐欺師にとって有利に働くことが予想される．フィッシング詐欺の多くは，フィッシングメールからフィッシングサイトに誘導される流れを取るが，それらに記載される文章は非常に巧妙に出来ており，多くのユーザにとって文章内容だけからフィッシング詐欺であると断定することは非常に難しい．そこで，PC では HTML メールの A タグで表されるリンク先のアドレスや，ブラウザのアドレスバーに現れる URL や SSL 通信を示す各種マークなど，周辺情報を総合して判断されることが多い．しかし，携帯電話では出力エリアの制限から，これらの周辺情報を確認することが容易ではない．また，PC と比較して携帯電話のメーラーと Web ブラウザの親和性が非常に高く，シームレスにメール内のリンクから Web 閲覧に移れることが多い．従って，PC 向けでは必要であった周辺情報の偽装が携帯電話向けでは不要となり，よりフィッシング詐欺を行いやすくなると共に，それを見抜くことが難しいことが予想される．

さらに，入力インタフェースの制限から，アカウント名やパスワードなどユーザに入力を要求する内容の文字数が少なかったり，入力が容易なように数字に限定したりなどのユーザビリティ向上策が採られているサイトが多い．これは，部分的な情報を盗み出すことで，他の重要な情報（パスワードなど）を類推しやすいことを意味する．また，多くのフィッシング詐欺でターゲットとされるクレジットカード番号は数字のみの組み合わせであり，携帯電話ユーザにとって入力の障壁が大きくないこともフィッシング詐欺師に有利に働く要因となる．また，携帯電話向け URL は，ユーザの入力を容易にするために非常に短い文字列から構成される傾向にあり，接続時に警告が表示されたとしても URL から接続する企業名を特定することは困難である．

4. 携帯電話におけるフィッシング詐欺対策

そこで本章では，携帯電話を対象としたフィッシング詐欺を防ぐ対策手法について提案する．

4.1 企業名によるフィッシング詐欺対策手法

筆者らは PC に対するフィッシング対策として，企業名検出による手法を提案している [7], [8]．これは，フィッシング詐欺が企業名を偽装することで利用者を騙していることから，フィッシング詐欺師が偽装している企業名と，利用者が誤認する企業名が同一であることに着目した対策手法である．その手順は以下の通りである．

準備段階として，企業名とその企業のサイトの URL の組み合わせをホワイトリストとして用意する．メールが届いた際には，メール内の企業名をホワイトリストの企業名とのマッチングから抽出し，メール内のリンク URL に関連づける．このプロセスにおいて，企業名およびリンク URL の位置関係などから，あるリンク URL に対して関連が深いと考えられる企業名を候補として，関連の深さの順でリストアップする．利用者がメール内のリンク URL をクリックした際に，そのリンク URL と関連する企業名の候補を提示し，利用者がアクセスしようとしているサイトの企業名を利用者自身に選択させる．そして，ホワイトリスト内の，利用者が選択した企業名に対応する URL と，メールに記載されたリンク URL とを比較し，異なっている場合にはフィッシングサイトであると警告する．

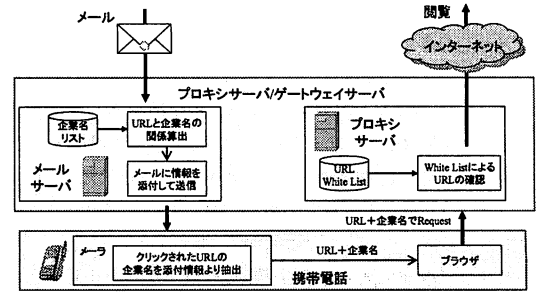

図 5 携帯電話におけるフィッシング詐欺対策アーキテクチャ

本手法の特徴は，利用者がアクセスしようとしている企業名を選択してもらうことで，「企業名」というパラメータが確実に決定されるため，ホワイトリストの URL と比較することで，フィッシングサイトを検出可能であることにある．企業名を抽出しないで正しい URL だけとの比較を行う手法では，正しい URL を検証することは可能であるが，フィッシングサイトに対しては「正しいサイトではない」という曖昧な検出にとどまる．全てのサイトがホワイトリストに登録される世界が実現した場合には，企業名を用いない URL の検証のみでフィッシングサイトを検出することが可能であるが，現実的に全てのサイトがホワイトリストに登録されることを期待するのは難しい．

以下，本章ではこの対策手法を携帯電話に適用するためのアーキテクチャを提案する．

4.2 アーキテクチャ

筆者らは PC におけるフィッシング対策として，クライアントサイドで企業名検出・ホワイトリスト照合などの処理を行う手法を提案している．しかし，PC と携帯電話では，処理能力や表示能力など様々な観点で差違が存在する．従って，PC と同様の処理を全てクライアントサイド（携帯電話）で行うことは困難である．一方，全てをサーバサイドで処理する場合には，企業名に対するユーザの意図を把握することが困難となり，フィッシング詐欺の検出が困難となる．そこで本稿では，サーバとクライアントの双方で処理を応分しつつも，可能な限りサーバ側で処理を負担するアーキテクチャを提案する．図 5 に本アーキテクチャのブロック図を示し，各機能ブロックについて以下に説明する．

メールサーバ　メールサーバでは，受信したメール内の企業名を抽出し，メール内の各リンクについてそのリンクと関連の強い企業名を尤度の順に候補としてリストアップする．このリンクと企業名候補のリストをメールヘッダなどに埋め込み携帯電話に送信する．

携帯電話メーラ　携帯電話のメーラは，受信したメールのヘッダなどからリンクと企業名候補のリストを抽出する．そして，ユーザがそのメールを閲覧し，メール内のリンクをクリックした際には，そのリンクと対応した企業名候補をユーザに提示し，ユーザがアクセスしようと思っている企業名を選択させる．選択結果として，特殊コード（プロキシサーバの URL でもよい）＋リンク URL ＋企業名の組（URI）としてブラウザに通知する．

携帯電話ブラウザ　携帯電話のブラウザは，メーラより渡された URI を用いてインターネットにアクセスする．このとき，URI の先頭がプロキシサーバの URL であった場合，その要求はプロキシサーバに伝達されることとなる．

プロキシサーバ　プロキシサーバは，携帯電話のブラウザからの要求を解析し，それが本手法に基づくものであった場合，要求されたインターネット上の URL（メールに記載のリンク先）とユーザの選択した企業名の組み合わせが妥当かどうかをホワイトリストを用いて検証する．正しく検証できなかった場合には，その URL はフィッシングサイトであるので，その旨の記載がなされたページをブラウザに送信する．

4.3 提案手法の特徴と課題

提案手法の特徴の第一は，著者らが提案している企業名を用いた検証手法を用いることで，正しいサイトを正しいと証明するだけではなく，フィッシングサイトをフィッシングサイトであると検知することが可能な点にある．

また，メールサーバおよびプロキシサーバにてリンクに関連する企業名リストの抽出およびホワイトリストとの照合が行われるため，携帯電話の負荷が少ない実装が可能である．チェックする企業名が増加した際には，URL に関連する企業候補を抽出する処理が重くなることが予想され，さらに昨今の携帯電話メールのサイズの増加により，処理対象の増加もあり，CPU への負荷は増加する傾向にある．また，ホワイトリストに登録する対象企業の増加は記憶領域へのインパクトとなり，特にアプリケーションソフトが利用可能な記憶領域が限定される携帯電話には大きな影響がある．従って，これらの処理をサーバ側で行うことで携帯電話への負荷を最小限に抑えることが可能となる．これと関連して，各種処理をサーバ側で行うことで，端末処理が必要とするデータ量を削減することが可能であり，通信費を抑えることが可能となる．

また，ホワイトリストとの照合はサーバで行われるため，企業名や URL のアップデートなどに対して適用遅延を最小限にすることが出来るという特徴も挙げられる．

一方，いくつかの課題も考えられる．提案手法では，メール受信時にメールのリンクに企業名の情報が付加されるため，メール受信後からユーザがリンクをクリックする間に企業名の登録がなされた場合，対応することが出来ない．そこで，企業名対応のないリンクをクリックした場合には，その旨プロキシサーバに通知し，最新のホワイトリストと照合を行うなどの対応が必要である．

5. おわりに

本稿では，携帯電話に対するフィッシング詐欺の可能性について述べ，その対策手法を提案した．モバイルコマースの普及によって，携帯電話を用いた金融情報などの重要情報のやりとりは活発化し，フィッシング詐欺のターゲットとして成熟した市場となりつつある．また，携帯電話特有のインタフェースにより，PC よりもフィッシング詐欺が容易な環境とも言える．そこで，筆者らが提唱している企業名によるフィッシング詐欺対策を活用しながら，携帯電話特有のインタフェースを考慮した実装方式を提案した．

提案方式は，端末（携帯電話）の負荷が少ない点や必要とする通信量が少ない点などの特徴を持つが，携帯電話のフィッシングメールに特化した処理手法や，セキュリティ強度の検証，ユーザビリティの検証については，今後，実装や評価を行う必要がある．

文　献

[1] Anti-Phishing Working Group, “Phishing Activity Trends Report for the Month of January, 2007”, APWG Web Page, http://www.antiphishing.org/, 2007.

[2] 総務省, “平成 18 年版情報通信白書”, ぎょうせい, 2006.

[3] 経済産業省・ECOM・NTT データ経営研究所, “平成 16 年度電子商取引に関する実態・市場規模調査”, http://www.meti.go.jp/press/20050628001/e-commerce-set.pdf, 2005.

[4] 三重県 総合企画局 広聴広報室, “三重県「ｅーデモ会議室」におけるサーバへの不正アクセスについて”, 三重県 Web サイト（報告書）, http://www.pref.mie.jp/TOPICS/2005070370.htm, 2005.

[5] 朝日新聞 2005 年 6 月 14 日朝刊 39 面 14 版.

[6] 日経ビジネス, “際限ない「欲望のモデル」”, Nikkei Business 2007 年 4 月 9 日号, pp.42–44. 2007.

[7] 柴田賢介, 荒金陽助, 塩野入理, 金井敦, “電子メールの解析によるフィッシングおよびファーミング対策手法の提案”, DICOMO2006, 4E3, pp.477-480, Jul. 2006.

[8] 柴田賢介, 荒金陽助, 塩野入理, 金井敦, “Web サイトからの企業名抽出によるフィッシング対策手法の提案”, 情処研報, 2006-GN-61(4), pp.17–22, Sep.2006.