情報処理学会論文誌 Vol. 49 No. 9 3104–3111 (Sep. 2008)

Web of Trustの導入による コンテンツベースフィッシング検知方式の改良

西垣正勝[†1] 長谷巧[†2] 原正憲[†3]

検索エンジンを活用することによって，インターネット上に定常的に存在しているWebページのすべてをホワイトリストとして活用するコンテンツベースのフィッシング検知方式が提案されている．この手法によるフィッシングサイトの検知精度は，検証したいWebページの特徴を用いてインターネット検索を行う際の検索精度に依存する．そこで本論文では，Web of Trustの概念を導入することによりインターネット検索の検索精度を高め，コンテンツベースのフィッシング検知方式の検知精度の向上を果たす．

An Improvement of Content-based Phishing Detection Using Web of Trust

Masakatsu Nishigaki,[†1] Takumi Nagaya[†2] and Masanori Hara[†3]

Recently a content-based phishing detection has been proposed, in which Internet search engine is a key mechanism which allows us to use the existing all websites as white list. In this scheme, accuracy of phishing site detection depends on the performance of Internet search by the characteristics of the website to be checked. Here in this paper, by introducing the concept "Web of Trust" to improve the accuracy of Internet search, we try to achieve higher performance of the content-based phishing detection.

†1 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University
†2 静岡大学大学院情報学研究科
Graduate School of Informatics, Shizuoka University
†3 株式会社KDDI研究所
KDDI R&D Laboratories, Inc.

1. はじめに

インターネットの普及により，インターネットバンキングやオンラインショッピング等の電子商取引に代表される様々なオンラインサービスが登場している．しかし，それにともない新たにフィッシングという犯罪が台頭し始めた．フィッシングとは，インターネットバンキングサービスやオンラインショッピング等を提供する正規サイトを模倣したサイトを作成し，そこへ利用者を誘導して正規サイトと勘違いさせることで不正に個人情報やクレジットカード番号，各種サービス利用のためのID・パスワード等の重要な情報を詐取することである．年々，フィッシングの被害は急増しており技術的な対策が求められている．

既存のフィッシング検知手法の中で，最近になって，コンテンツベースのフィッシング検知方式[1),2)]が提案された．これに関し，吉浦らは「インターネット上に蓄えられている大量かつ多様な知識をセキュリティ技術に応用する」というヒューマンコミュニケーションセキュリティに関する構想を提案しており，効率的にインターネット上の知識を活用するためにインターネットの検索技術を利用することをあげている[3)]．コンテンツベースのフィッシング検知方式はヒューマンコミュニケーションセキュリティ構想のフィッシング検知への応用と位置付けられ，「インターネット上に定常的に存在しているWebページのすべてをホワイトリストとし，検索エンジンによるインターネット検索を利用することで，検査対象のWebページがこの巨大なホワイトリストに含まれるか否かを効率的に照合することによってフィッシングサイトを検出する」という究極のホワイトリスト型フィッシング検知技術であると見なすことができる．

すなわち，コンテンツベースのフィッシング検知方式の検知精度は，検査対象のWebページの特徴を用いてインターネット検索を行う際の検索精度に依存する．いい換えれば，コンテンツベースのフィッシング検知技術の実用には，高い精度でインターネット検索が行えるという大前提が必要である．しかし，現在の主流であるGoogleやYahoo等の検索エンジンによるインターネット検索には限界がある．そこで本論文では，Web of Trustの概念[4)]の導入によってインターネット検索の検索精度を高め，インターネット上の知識をより効果的に検索することを可能とし，これによりコンテンツベースのフィッシング検知方式の検知精度の向上を達成する．

2. 既存研究

コンテンツベースのフィッシング検知方式は，Zhangら[1)]および中山ら[2)]により提案されている．これらの方式は，検査対象のWebページからTF-IDFを用いて特徴的な単語を抽出し，それを検索キーワードとしてGoogleでインターネット検索を行うもので，検索結

果の中に当該ページが含まれていれば正規サイト，含まれていなければフィッシングサイトと判定する．なお，ここで，検査対象の Web ページのドメインが検索結果の上位 n ページのいずれかのドメインと一致した場合に「含まれる」と判断される．

Zhang らは 100 件のフィッシングサイトに対して検知率 97%の検知を実現している．これは各種 Anti-phishing Toolbar の検知精度[5] と比較して，非常に高い精度であるといえる．しかし，100 件の正規サイトを用いた誤検知実験では，10%の誤検知率を発生させている[1]．中山らの 39 件のインターネットバンキングサービスサイトのみを用いた誤検知実験においても誤検知率は 23%であり[2]，コンテンツベースのフィッシング検知方式は特に誤検知（false positive）においてはまだ改善の余地が残されている．

この理由として，我々は以下の 2 つの要因が原因であると考える．

要因 1)　検索エンジンで検索できないサイトが存在する：

たとえば Google では，meta タグや robots.txt によって，特定の Web ページを検索対象から除外できる[6]．また，作成されて間もない Web ページは，Google に登録されるまでは検索対象に含まれない．コンテンツベースのフィッシング検知方式は，インターネット検索によって検索されうるすべての Web ページをホワイトリストとして活用する方式であるため，検索エンジンにて検索できない正規サイトはホワイトリストから漏れてしまう．

要因 2)　同じサイト内の複数の Web ページにおいても URL のドメインが異なることがある：

ある Web ページ α に含まれるキーワードを用いて検索した場合に，その Web ページが含まれる Web サイト内の他のページ（たとえばその企業のポータルページ）β が得られることも多い．このため文献 1)，2) では，検査対象の Web ページ α と検索結果の Web ページ β のドメインが一致するか否かによって α が正規サイトであるのかフィッシングサイトであるのかを判定するという方法をとっている．よって，ページ α とページ β の URL のドメインが異なっているような正規サイトがあった場合，ページ α はフィッシングサイトであると判定されてしまう．

より詳しく述べると，要因 1 に該当する Web ページ α に関しては，当該ページ α はインターネット検索では直接見つからないため，関連する Web ページ（たとえばその企業のポータルページ）β がインターネット検索で見つかり，かつ，α と β のドメインが一致する（要因 2 には該当しない）場合のみ，既存方式で検知可能である．また，要因 2 に該当する Web ページ α は，当該ページ α が要因 1 に該当しなければ，「インターネット検索によってページ α を検索することができる検索キーワード」を適切に指定することができた場合のみ，既存方式で検知可能である．そして，要因 1 と 2 の両方に該当する Web ページ α は，インターネット検索で直接見つけることができず（要因 1），関連するページ β がインターネット検索で見つかったとしても，α と β のドメインが一致しない（要因 2）ため，既存方式では検知することが不可能である．

表 1　国内インターネットバンキングサービスの認証ページ 119 件の調査結果
Table 1　# of authentication pages of domestic Internet banking sites.

要件 1 に該当する	要件 2 に該当する	両方の要件に該当する	どちらも該当せず
40 件(33.6%)	100 件(84.0%)	28 件(23.5%)	7 件(5.9%)

以上のように，正規サイトが要因 1 または要因 2 のいずれかを満たしている場合，当該サイトの正当性をコンテンツベースのフィッシング検知方式により判定するにあたって false positive が発生する可能性があり，正規サイトが要因 1 と要因 2 の両方を満たしている場合には，当該ページの正当性をコンテンツベースのフィッシング検知方式により判定する際に false positive の発生が避けられない．

上記の要因 1 および要因 2 を要件として，要件 1 および要件 2 に該当する Web ページがそれぞれどれくらい存在するかに関して我々が簡易な調査したところ，Web ページ全体を見た場合には，実際に上記の 2 つの要件に該当する Web ページの割合は低かったが，日本のインターネットバンキングサービスの認証ページ[⋆1] 119 件に限定した場合には多くのページがこれらの要件に該当していることを確認した[⋆2]．その結果を**表 1** に示す．

この理由としては，以下のことが考えられる．

- インターネットバンキング等の電子商取引を行うサイトでは，センシティブな顧客情報等を取り扱っているため，セキュリティ上，認証等の重要な Web ページへはその銀行のポータルページからしかアクセスを許さないというポリシで運用されることも多い．

⋆1 本論文では，Wikipedia の日本の銀行一覧[13] に記されている「都市銀行」，「第一地方銀行」，「第二地方銀行」，「ネット銀行」に該当する 119 の銀行が提供する「インターネットバンキングの個人向けの認証ページ」を「インターネットバンキングサービスの認証ページ」として選出した．ただし，119 行のうち，インターネットバンキングを提供していない 1 行は除外した．また，1 行は 2 つのインターネットバンキングサービスを個別のサイトで提供していたため，その両ページを対象とした．なお，本論文では，ID とパスワードの入力を促すページを「認証ページ」と定義している．

⋆2 諸外国においては国ごとに特徴が異なり，イギリス，カナダ等の銀行は日本と同様の傾向であったが，アメリカの銀行に関してはこの傾向は顕著ではなかった．

この場合，検索エンジンから直接アクセスできないような設定を施しているサイトは要件 1 に該当することになる．

- 同様の理由で，顧客情報等を扱うための重要な Web サーバと公開情報を扱うための一般 Web サーバを分離するというポリシで運用されるサイトも多い．そして，その際，銀行が重要な Web サーバの運用を外部の専門的な ASP に委託するケースがある．その場合には銀行のポータルページ等と ASP による認証ページの URL のドメインが異なることになり，要件 2 に該当することになる．

さらに重要なのは，これらの認証ページはヒューリスティックを用いたフィッシング検知手法においても false positive の温床となっているという事実である．フィッシングサイトは認証ページを模擬しているため，フィッシングサイトらしさを判定するための特徴（たとえば，「ユーザ ID やパスワードの入力フォームを備える」という特徴）は，当然，正規の認証サイトにも見受けられることが多い．実際，今回の国内インターネットバンキングサービスの認証ページ 119 件に対して，ヒューリスティックベースのフィッシング検知ソフトである spoofguard [7] を用いて誤検知実験を行ったところ，109 件をフィッシングサイトと誤検知した（誤検知率 92%）[⋆1]．

特にインターネットバンキング等の電子商取引サイトの認証ページはフィッシングの対象になりやすい．よって，このような Web ページこそ，フィッシング検知の必要が問われる．しかし，既存のコンテンツベースのフィッシング検知技術では，このようなサイトを的確に真贋判定することができていない．かつ，この問題は，ヒューリスティックを用いたフィッシング検知との併用を試みたとしても解決できない．そこで我々は，電子商取引サイトの認証ページに焦点を当て，コンテンツベースのフィッシング検知方式の誤検知（false positive）を改善し検知精度を向上させる方策を検討する．

3. 提 案 方 式

3.1 Web of Trust の導入

「インターネット検索により，インターネット上に大量に存在する知識の中から必要な知識を探し出し，活用する」という吉浦らの構想[3] は理論的には非常に有効であると考えられる．しかし，前章で述べたように，既存のインターネット検索においては十分な検索結果を得ることは困難である．吉浦らの構想を真に実用的なものにするためには検索精度の高い検索技術が必要不可欠である．そこで我々は，インターネット検索に Web of Trust の概念[4] を導入することを提案する．

Web of Trust とは OpenPGP [8] で広まった信頼性を保証するモデルの 1 つである．このモデルは「自分の知らない相手が信用できるか否か判断したい場合に，その相手が多数の人から信用されている場合や，自分の信用している第三者がその相手を信用している場合には，その相手は信用できると判断する」という考え方に基づいている．

我々は，インターネット検索と Web of Trust を併用することで，2 章に示した 2 つの要件に起因する問題を克服できると考える．コンテンツベースのフィッシング検知方式により，インターネットバンキングサービスの認証ページ α の正当性を検査する場合を例にとり，これを説明しよう．ここで α は，検索エンジンによって検索できないように設定されており（要件 1），かつ，その銀行のポータルページ β とは異なるドメインの URL が付されている（要件 2）とする．認証ページ α は要件 1 に該当するため，α 内に含まれるキーワード（銀行名や，「ログイン」という単語等）を用いてインターネット検索を行っても，検索結果の中に α は含まれない．しかし，銀行名が検索キーワードとなっているため，この銀行のポータルページ β は検索結果に含まれるだろう．よって，Web of Trust の概念に基づき，ポータルページ β からリンクが張られている Web ページを次々にたどることによって，当該インターネットバンキングサービスの認証ページ α に至ることができる．直接的なリンクをたどるため，α と β の URL が異なっていても問題ない．こうして，ページ α がホワイトリスト（インターネット上に定常的に存在している Web ページのすべて）に含まれるということが確認できれば，このページがフィッシングサイトではないと判定できる．

3.2 Web of Trust を導入したコンテンツベースフィッシング検知

図 1 に Web of Trust を導入したコンテンツベースフィッシング検知方式の処理フローを示す．

まず，従来のコンテンツベースのフィッシング検知と同様，(1) 検査対象の Web ページの中から，TF-IDF 等を活用し，特徴的な語句を選択したうえで，その語句をキーワードとしてインターネット検索を行い，(2) 検索結果の上位 n サイトの中に検査対象の Web ページが含まれるか否かを検査する．手順 (2) の検査が真であれば，当該ページを正規サイトと判定して終了である．

検索結果の中に検査対象ページが含まれなかった場合は，Web of Trust に基づく探索が開始される．すなわち，(3) 手順 (1) における検索によって得られた上位 m サイトを「アンカ

⋆1 インターネットバンキングサービスの認証ページに限らず正規サイト全体から無作為抽出した Web ページに対する誤検知率は 38%である[5]．

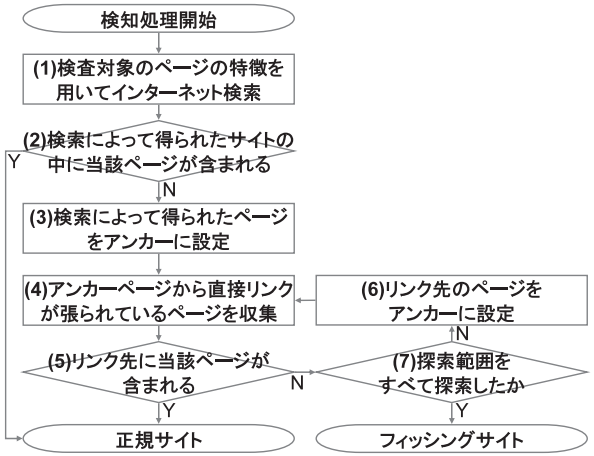

図 1　提案方式の処理手順
Fig. 1　Flow of phishing site detection.

ページ」としてセットしたうえで，(4) 各アンカページのそれぞれから直接リンクが張られている Web ページ（アンカページから 1 ホップ先のリンク）をすべて収集し，(5) 収集されたページの中に検査対象の Web ページが含まれるか否かを検査する．手順 (5) の検査が真であれば，当該ページを正規サイトと判定する．手順 (5) の検査が偽であった場合は，(6) 収集されたすべての Web ページを新たに「アンカページ」としてセットしたうえで，手順 (4) に戻る．(7) 手順 (4)〜(6) は，探索範囲の Web ページの探索が尽くされるまで繰り返される．

ここで，手順 (2) および (5) における包含検査においては，URL 一致（検索/収集された Web ページの中に，検査対象の Web ページと同じ URL のページが含まれている），ディレクトリ一致（検査対象の Web ページと同じディレクトリのページが含まれている），ドメイン一致（検査対象の Web ページと同じドメインのページが含まれている）等のオプションが考えられる．また，手順 (6) における探索範囲は，「リンクホップ数限定（手順 (1) の検索結果から p リンク先の Web ページまでを探索対象とする）」，「リンク範囲限定（手順 (1) の検索結果のページのドメイン内へのリンクのみを探索対象とする）」等の制限を指定することができる．

Google の検索結果はページランクによって順位付けされている[9]．よって，手順 (1) のインターネット検索の結果，上位にランキングされたサイトは，定常的に多数から参照されている「信用できるサイト」だといえる．すなわち，手順 (3)〜(6) のリンク探索は『「信用できるサイト」からリンクが張られているサイトも「信用できるサイト」として信用する』という信頼の連鎖をたどる作業であるということが分かる．コンテンツベースのフィッシング検知方式におけるインターネット検索はホワイトリスト（信用できるサイト）との照合に相当する操作である．このため，Web of Trust の導入による「信用できるサイト」の増大が，コンテンツベースのフィッシング検知方式におけるホワイトリスト照合の精度を改善し，この結果，誤検知（false positive）の発生が抑えられる．

4. 実　　験

4.1 実　　装

今回は提案方式と既存方式との差異を明らかにすることに焦点を置き，簡易的ではあるが，以下の仕様でプログラムを作成した．

「既存方式」

1. 3.2 節の手順 (1)〜(2) によるフィッシング検知を行う．
2. 手順 (1) のインターネット検索では，文献 2) と同様の TF-IDF 計算ルーチンを用い，検査対象の Web ページの中から特徴的な語句をキーワードとして選出し，Google によって検索を行う．また，SEO（検索エンジン最適化）の文献には「インターネット検索で上位に表示されるために最重要視される項目はページのタイトルである」という記載もある[12] ため，TF-IDF を利用せずに，検査対象の Web ページのタイトルを検索キーワードに用いて Google 検索を行う方法も試す．
3. 手順 (2) においては，検索結果の上位 10 件に対して検査する（$n = 10$）．
4. 手順 (2) の包含チェックは，URL 一致，ディレクトリ一致，ドメイン一致の 3 種類を試す．

「提案方式」

1. 3.2 節の手順 (1)〜(7) によるフィッシング検知を行う．
2. 手順 (1) のインターネット検索では，検査対象の Web ページのタイトルをキーワードに用い，Google によって検索を行う．今回は，提案方式においては，TF-IDF による検索キーワードの選出は行わない[⋆1]．

⋆1 表 3 から分かるように，TF-IDF を利用して検索キーワードを選出した場合の既存方式の検知率は，タイトルを検索キーワードとして使用した場合の既存方式の検知率よりも低いという結果であった．これは，文献 2) にも記されているように，形態素解析における分かち書きの失敗がその主な原因であった．すなわち，現時点の計算機による自然言語処理能力に鑑みるに，TF-IDF の利用は，残念ながら，処理時間を大きく増大させてしまうというデメリットのみが前面に現れてしまう．このため，提案方式においては TF-IDF の採用を見送り，ページタイトルを検索キーワードとして利用する方法のみを試すこととした．

表 2　フィッシングサイト 100 件の検知件数（検知率）と検知時間（平均，分散，最大値，最小値）
Table 2　Experimental results of true positive for 100 phishing sites and time taken for detection.

	検知件数（検知率）			検知時間			
	URL 一致	ディレクトリ一致	ドメイン一致	平均	分散	最大値	最小値
既存方式 (ページタイトル)	100 件(100%)	100 件(100%)	100 件(100%)	1 秒	0	1 秒	1 秒
提案方式 (ページタイトル)	100 件(100%)	100 件(100%)	100 件(100%)	1972 秒	64870253	37805 秒	1 秒

3. 手順 (2) においては，検索結果の最上位 1 件に対して検査する（$n = 1$）．
4. 手順 (3) においても，検索結果の最上位 1 件のみをアンカページとする（$m = 1$）．
5. 手順 (2) および (5) の包含チェックは，URL 一致，ディレクトリ一致，ドメイン一致の 3 種類を試す．
6. 手順 (7) の探索範囲に関しては，探索対象となるドメインを「検査対象の Web ページの URL のドメイン」および「手順 (2) の検索結果最上位の Web ページの URL のドメイン」に限定する．
7. 手順 (4)〜(5) の検査は，アンカページの HTML ファイルを先頭行から走査していき，リンク先 URL が出現するたびに，当該ページに対する検査を行う．また，手順 (7) の階層チェックにおいては，幅優先探索に従う順序で検査を行っていく．

4.2 実験対象

誤検知実験には 2 章で調査したインターネットバンキングサービスの認証ページ 119 件を正規サイトとして利用する．また，PhishTank [10] から任意に選んだフィッシングサイト 100 件を利用し検知実験を行う．

4.3 実験結果

フィッシングサイトに対する検知実験の結果を**表 2**，正規サイトに対する誤検知実験の結果を**表 3** に示す．

表 2 より，提案方式においても既存方式と同様に高い検知率を達成できていることが分かる[⋆1]．これは，フィッシングサイトはインターネット上に定常的に存在しておらず（平均存続期間は 4 日[11]），インターネット検索を用いても検索できないためである．また，フィッシングサイトはその性質上，他サイトからリンクが張られている可能性も稀有である．よって，リンクをたどるという改良を加えた提案方式においても，検知精度の低減がなかったと考えられる．

⋆1 既存方式においては，TF-IDF による検索キーワードの選出を行うまでもなく，ページタイトルをキーワードとしてインターネット検索を行うことによりフィッシングサイトが検知できている．このため，既存方式によるフィッシングサイトの検知実験においては，TF-IDF による実験は割愛した．

表 3　正規サイト 119 件の誤検知件数（誤検知率）と検知時間（平均，分散，最大値，最小値）
Table 3　Experimental results of false positive for 119 legitimate sites and time taken for detection.

	誤検知件数（誤検知率）			検知時間			
	URL 一致	ディレクトリ一致	ドメイン一致	平均	分散	最大値	最小値
既存方式 (TF-IDF)	73 件(61.3%)	67 件(56.3%)	60 件(50.4%)	51 秒	2611	255 秒	5 秒
既存方式 (ページタイトル)	55 件(46.2%)	53 件(44.5%)	43 件(36.1%)	1 秒	0	1 秒	1 秒
提案方式 (ページタイトル)	23 件(19.3%)	16 件(13.4%)	16 件(13.4%)	135 秒	464457	3636 秒	1 秒
提案方式 (銀行名)	6 件(5.2%)	0 件(0%)	0 件(0%)	5 秒	287	145 秒	1 秒

表 4　両要件に該当する正規サイト 28 件に対する誤検知件数（誤検知率）
Table 4　Experimental results of false positive for 28 legitimate sites that meet both conditions 1 and 2.

	誤検知件数（誤検知率）
	ドメイン一致
既存方式(TF-IDF)	28 件(100%)
既存方式(ページタイトル)	28 件(100%)
提案方式(ページタイトル)	1 件(3.6%)
提案方式(銀行名)	0 件(0%)

また表 3 より，既存方式と比較して提案方式の誤検知（false positive）の低さが示されている．特に**表 4** に示すように，2 章に記した要件 1 と要件 2 の両方に該当するサイト 28 件に限定すると，既存方式ではこれらのサイトを正規サイトとして判定することができないが，提案方式では十分な検知精度が得られていることが確認できる．

これらの結果は，インターネット検索のみを用いる既存方式の問題点を，リンクをたどるという Web of Trust の概念を導入した提案方式が解決していることを示している．両実験結果から，提案方式が既存方式の改良を達成していることを確認した．

しかし，提案方式においてもまだ誤検知（false positive）が発生してしまっている．これは，今回の実験では検索キーワードを Web ページのタイトルとしたために，3.2 節の手順 (1) におけるインターネット検索が適切に機能しなかった場合があったためだと考えられ

る．そこで，提案方式に対し，銀行名[⋆1]を検索キーワードとして手動で設定した場合の実験を行った．表 3，表 4 にはその結果も併記してある．この結果より，計算機による自然言語処理が発達し，ページの内容から銀行名を抽出することができるようになった際には，提案手法は非常に高い検知精度を達成できることが期待できる．一方，既存方式の場合，2 章で説明したように，たとえ十分な検索キーワードの選定が行えたとしても，要件 1 と要件 2 の両方に該当するサイトに対しては誤検知（false positive）を回避することは不可能である[⋆2]．

5. 検知時間に関する考察

提案方式は，既存方式の検知精度の改良を達成した．しかし提案方式は，1 つの Web ページの検査を行うために大量のリンクをたどる必要があるため，検査に要する時間が激増するという非常に大きな問題をかかえている．

表 2，表 3 においては，4 章でのそれぞれの実験における提案方式および既存方式の検知時間の平均，分散，最大値，最小値が併記してある[⋆3]．ここで，実験環境は，PC は OS：Windows XP SP2，CPU：Pentium4 2.6 GHz，メモリ：512 MHz，インターネット回線は下り 100 Mbps である．検知実験と誤検知実験の平均検知時間（表 2 と表 3 の平均検知時間の平均）は，既存方式ではページあたり 1 秒なのに対して，提案方式は 974 秒を要してしまっている．

検知時間を増加させている一番の原因として考えられるのは，リンクをたどるホップ数が増えるとリンク先のページ数が指数関数的に激増してしまうことがあげられる．提案方式においては，すべてのリンク先を探索し終わっても検査対象の Web ページが見つからなかった場合に初めて当該ページをフィッシングサイトと判定する．このため，4 章の実験ではリンク範囲限定方式を採用している（探索範囲を「検査対象の Web ページの URL のドメイン」または「インターネット検索結果最上位の URL のドメイン」に限定している）ものの，それでもなお，フィッシングサイトであるとの判定を下すにあたっては当該ドメインに含まれる Web ページのすべてに対してのリンクをたどることになる．Web サイトの規模が小さい場合はさほど問題とはならないかもしれないが，大規模なサイトの場合，これは検知時間の大幅な増大に直結する．

表 5　国内銀行におけるポータルページから認証ページまでのリンクのホップ数
Table 5　# of hops of link from portal page to authentication page in domestic banks.

1 ホップ以内	2 ホップ	3 ホップ	4 ホップ以上
43 件(36.1%)	68 件(57.1%)	8 件(6.9%)	0 件(0%)

そこで，提案アルゴリズムの探索範囲をさらに限定することを考える．具体的には，4 章の実験において採用していたリンク範囲限定方式に加え，リンクホップ数限定方式（インターネット検索によって得られたページから p リンク先の Web ページまでを探索対象とする）による制限も追加することにより，たどるべきリンクの数を減らし，検知時間の減少を図る．ただし，リンクをたどる探索範囲を狭めることは，同時に誤検知（false positive）の増加を招き検知精度が低下してしまう恐れがある[⋆4]．そこで，誤検知を増加させないためにはどの程度の深さまでリンクの階層（ホップ数）をたどるべきかに関する目安を調べるために，4 章の実験で用いた国内インターネットバンキングサービスの認証ページ 119 件に対して，それぞれの銀行のポータルページから当該認証ページに至るまでのリンクのホップ数を調査した．その結果を**表 5** に示す．

表 5 より，（少なくとも今回の実験対象のサイトに対しては）4 階層以上のリンクホップ数を持つサイトは存在しない．これは，ポータルページから 3 ホップ先までのリンクをたどれば認証ページに到達することを示し，逆に，それ以上の深さまでリンクを探索しても検知精度には影響しないことを意味している．したがって，「3.2 節の手順 (1) におけるインターネット検索によって銀行のポータルページを得ることができる」という前提が成り立つのであれば，探索範囲をホップ数 $p = 3$ に限定することにより，検知精度を低下させることなく検知時間を減少させることができると考えられる．

これを確かめるために，表 3 の実験（対象：国内インターネットバンキングサービスの認証ページ 119 件，検索キーワード：銀行名を手動で入力，探索範囲：検査対象の Web ページの URL のドメインとインターネット検索結果最上位の URL のドメインに限定）および表 2 の実験（対象：フィッシングサイト 100 件，検索キーワード：ページタイトル，探索

⋆1 検査対象ページのインターネットバンキングサービスを提供している銀行の「銀行名」を指す．
⋆2 実際に，既存方式に対しても手動で銀行名を検索キーワードに設定して表 4 の実験を行ったところ，誤検知件数 28 件のままであった．また，同様に表 3 の実験を行ったところ，既存方式においては，銀行名を検索キーワードにしてしまうと，TF-IDF やページタイトルを利用した場合よりも誤検知件数が大きく増加する結果となった．銀行名を検索キーワードにすると，その銀行の認証ページ以外のページがインターネット検索の上位に多くランクインすることになり，認証ページが上位 10 位以内に含まれなくなってしまうことが，この精度劣化の主要因であった．
⋆3 厳密には「1 秒」の記載は「1 秒以内」を示す．
⋆4 リンクホップ数の制限はホワイトリストを削減することに相当するため，false negative は増加しない．

表 6　表 2 の実験に対しリンクホップ数の限定を追加した場合のフィッシングサイト 100 件の検知数（検知率）と検知時間（平均，分散，最大値，最小値））
Table 6　Experimental results of true positive for 100 phishing sites and time taken for detection, with limited hops of link.

	検知件数（検知率）			検知時間			
	URL 一致	ディレクトリ一致	ドメイン一致	平均	分散	最大値	最小値
提案方式 (ページタイトル)	100 件(100%)	100 件(100%)	100 件(100%)	253 秒	496451	2915 秒	1 秒

範囲：検査対象の Web ページの URL のドメインとインターネット検索結果最上位の URL のドメインに限定）に対して，さらにリンクホップ数限定方式（ホップ数 $p = 3$）を追加した場合の検知数と検知時間を調べた．以下，前者を追実験 1，後者を追実験 2 とする．

追実験 1 の結果は表 3 と同等であった．今回の検査対象サイト（国内インターネットバンキングサービスの認証ページ 119 件）はホップ数 p が 3 以上であれば認証ページまでリンクをたどることが可能であるため，検知率が低下することはない．また，ホップ数の限定の有無にかかわらず，認証ページまでリンクがたどれた時点で検査は終了するため，正規サイトに対しては検知時間は変化しない．一方．追実験 2 の結果を**表 6** に示す．表 6 より，探索範囲を適切に限定することができれば，検知率を低下させることなく，フィッシングサイトに対しての検知時間を減少させることが可能であることが確認できた．

6. ま と め

本論文では，Web of Trust の概念を導入することによってインターネット検索の検索精度を補い，コンテンツベースのフィッシング検知方式の検知精度の向上を果たす方式を提案した．既存のコンテンツベースフィッシング検知方式が有効に機能しない国内インターネットバンキングサービスの認証ページに対する検知実験を通じ，本改良方式の有効性を検証した．

今後は，銀行名を自動的に検索キーワードとして設定する方法，効率的なリンク探索範囲の限定の仕方等を検討したうえで，多種多様なサイトを対象とした大規模な検証実験を行っていく予定である．また，Web of Trust には「信頼度（trust）」として，ultimate，full，marginal，none，unknown という 5 つの指標がある[4]．本方式にさらに信用度を導入するようなことも検討していきたい．

謝辞　株式会社 KDDI 研究所三宅優様，窪田歩様には方式に関しての有益なる助言をいただいた．4 章における既存方式との比較実験に関しては，文献 2) の著者であられる電気通信大学吉浦裕教授，中山心太氏にご援助をいただいた．ここに深く謝意を表する．

参 考 文 献

1) Zhang, Y., Hong, J. and Cranor, L.: CANTINA: A Content-Based Approach to Detecting Phishing Web Sites, *Proc. 2007 International Conference on World Wide Web*, pp.639–648 (2007).
2) 中山心太，吉浦　裕：模倣コンテンツの特性に基づくフィッシング検知方式，情報処理学会研究報告，2007-CSEC-38-57, pp.387–392 (2007).
3) 吉浦　裕，片岡春乃，中山心太：多様化するメディア環境に適応するヒューマンコミュニケーションセキュリティの構想，情報処理学会研究報告，2007-CSEC-38-19, pp.125–132 (2007).
4) The GNU Privacy Guard. http://www.gnupg.org/（2007 年 11 月確認）
5) Cranor, L., Egelman, S., Hong, J. and Zhang, Y.: Phinding Phish: An Evaluation of Anti-Phishing Toolbars, CMU-CyLab-06-018 (2006).
6) Google ウェブマスター向けヘルプセンター：Google のインデックスにコンテンツが登録されないようにする，またはインデックスからコンテンツを削除する方法を教えてください．http://www.google.co.jp/support/webmasters/bin/answer.py?answer=35301&topic=8459（2007 年 11 月確認）
7) Chou, N., Ledesma, R., Teraguchi, Y., Boneh, D. and Mitchell, J.C.: Client-side defense against web-based identity theft, *Proc. 2004 Network and Distributed System Security Symposium* (2004).
8) OpenPGP.org. http://www.openpgp.org/（2007 年 11 月確認）
9) Google Technology. http://www.google.com/technology/index.html（20007 年 11 月確認）
10) PhishTank. http://www.phishtank.com/（2007 年 11 月確認）
11) Anti-phishing Working Group: APWG Phishing Trends Activity Report for February 2007. http://www.antiphishing.org/reports/apwg_report_february_2007.pdf（2007 年 11 月確認）
12) 株式会社アイレップ SEM 総合研究所：図解 SEO 対策がわかる，技術評論社 (2007).
13) Wikipedia，日本の銀行一覧．http://ja.wikipedia.org/wiki/%E6%97%A5%E6%9C%AC%E3%81%AE%E9%8A%80%E8%A1%8C（2008 年 3 月確認）

(平成 19 年 11 月 30 日受付)
(平成 20 年 6 月 3 日採録)

西垣　正勝（正会員）

1990 年静岡大学工学部光電機械工学科卒業．1992 年同大学大学院修士課程修了．1995 年同博士課程修了．日本学術振興会特別研究員（PD）を経て，1996 年静岡大学情報学部助手．1999 年同講師，2001 年同助教授．2006 年より同大学創造科学技術大学院助教授．2007 年より准教授．博士（工学）．情報セキュリティ，ニューラルネットワーク，回路シミュレーション等に関する研究に従事．

長谷　　巧

2007 年静岡大学情報学部情報科学科卒業．現在，同大学大学院修士課程．情報セキュリティに関する研究に従事．

原　　正憲

1981 年生．2003 年名古屋大学工学部電気電子情報学科卒業．2005 年同大学大学院工学研究科電子情報工学専攻修了．同年 KDDI 株式会社入社後，（株）KDDI 研究所出向，現在に至る．