SCIS 2006 The 2006 Symposium on Cryptography and Information Security
Hiroshima, Japan, Jan. 17-20, 2006
The Institute of Electronics, Information and Communication Engineers

フィッシング攻撃対策ツールの有効性評価のためのスキャナの提案
A Proposal of Scanner for Evaluating Anti Phishing Tools

宮本 大輔 * 鈴木 未央 * 櫨山 寛章 * 門林 雄基 *
Daisuke Miyamoto Mio Suzuki Hiroaki Hazeyama Youki Kadobayashi

あらまし フィッシング攻撃は，インターネットを利用する個人を標的として行われており，各個人の持つ機密情報を盗むことを目的とする攻撃である．フィッシング攻撃による被害は急増しており，フィッシング攻撃対策技術は社会的な重要性を増しつつある．しかし，フィッシング攻撃に用いられる手法は多様化しており，既存のフィッシング攻撃対策ツールの有効性は疑わしいとされている．本研究では，個々のフィッシング攻撃対策ツールがどのような攻撃手法に対して有効であるか，あるいは有効性の高いフィッシング攻撃対策ツールの組み合わせ方の明確化を目的としたスキャナを提案する．本システムは，擬似的なフィッシング攻撃を行うスキャンノードと，擬似的な機密情報を保有するデータノードによって構成される．スキャンノードはデータノードに対し，実際のフィッシング攻撃に用いられる手法を用いて，データノードの持つ情報を送信させるように促すことによってスキャンを行う．これにより，個々のフィッシング攻撃対策ツールがフィッシング攻撃をどの程度阻止できるかを検査する．さらに，本提案手法がフィッシング攻撃者に悪用されないための設計や運用についての考察を行い，今後の課題について述べる．

キーワード フィッシング対策, セキュリティ, スキャナ, エミュレータ

1 はじめに

近年，インターネットにおいてフィッシング攻撃が猛威をふるっている．フィッシング攻撃とは，インターネットを利用するエンドユーザを騙すことにより，ユーザの個人情報を盗む攻撃である．Anti-Phishing Working Group の報告 [1] によれば，フィッシングによる被害報告は 2004 年 10 月には 6,957 件であったが，2005 年 6 月では 15,050 件に増加している．また，Gartner は調査期間となった 1 年間に，約 120 万人が 929 万ドルの損失をフィッシング攻撃により被ったと報告 [2] しており，フィッシング攻撃の対策技術は社会的な重要性を増しつつある．

フィッシング攻撃が増加する背景として，エンドユーザがクレジットカード番号や預金番号などの個人情報を，銀行や電子商取引を行うウェブサイトに対して送信することが一般的となっている事象が挙げられる．フィッシング攻撃者 (以下，単に攻撃者と記す) はエンドユーザのこのような慣習につけこみ，個人情報を盗もうと試みる．

フィッシング攻撃には，大きく分けて誘致，取得の 2 つの段階がある．まず誘致の段階においては，攻撃者はエンドユーザのメールアドレスを収集する．

そして，フィッシングサイトと呼ばれる，銀行や電子商取引を行うウェブサイトと非常によく似た外観を持つウェブサイトを作成する．さらに攻撃者は，フィッシングメールと呼ばれる，フィッシングサイトを閲覧するよう促す内容の電子メールを収集したエンドユーザのメールアドレスに送信する．攻撃者は，フィッシングサイトを閲覧したエンドユーザに個人情報を入力させることにより，エンドユーザの個人情報を取得する．

現在，攻撃者からエンドユーザを防衛するフィッシング攻撃対策ツール (以下，単に対策ツールと記す) も開発されているにも関わらず，フィッシング攻撃による被害は増加し続けている．また，フィッシングサイトを自動的に識別し，エンドユーザに警告を行う対策ツールが盛んに開発されているが，このような対策ツールの有効性は疑わしいとされている [3]．また，フィッシングサイトの URL をフィルタリングにより判別し，対策を行う手法も考えられている．しかし，フィッシングサイトの作成は容易であり，攻撃者は URL を短時間で何通りにも変更できるため，フィッシングサイトのフィルタリングは効果が期待できない．フィッシングサイトではない，社会的に信頼のおけるサイトの URL を収集し，その URL に対するアクセスのみ許可するようなフィルタリングも考えられる．しかし，フィッシングサイト以外のサイトの URL の数は膨大な量であり，このフィルタリングによる対策の実現は極めて困難である．その他，ウェブサイトの外観やコンテンツの内容，URL の類似性からフィッシングサイトを判別する方法や，メールの

* 奈良先端科学技術大学院大学, 奈良県生駒市高山町 8916-5, Nara Institutee of Science Technology, 8916-5 Takayama Ikoma Nara

内容からフィッシング攻撃を検出する手法が提案されているが，どの対策手法もフィッシング攻撃を解決するには至っていない．

このように，既存の対策ツールにはそれぞれ利点と欠点があり，またフィッシング攻撃を防止できる領域も限定的である．従って，エンドユーザをフィッシング攻撃から守るためには，このような既存の技術を組み合わせた対策が必要である．このためには個別技術の対策可能な領域，不可能な領域を明らかにし，その上で個別技術を組み合わせた環境が攻撃を防御可能であるか否かを評価するシステムが必要である．

翻ってコンピュータセキュリティの分野では，脆弱性スキャナによる検査や侵入テストなどにより，コンピュータシステムの欠陥を調べ，その箇所を修復する手法が用いられている．このような手法を用いると，システムがどのような攻撃に対する対策がなされているかを検査でき，どのような対策ツールがどのような攻撃に対して有効であるかを検査できる．

そこで本研究では，対策ツールの有効性評価のためのスキャナを提案する．本システムの目的は，各対策ツールがどのような攻撃に対して有効であり，どのような攻撃に対して脆弱であるのかを明確にすることである．これにより，対策ツールの開発者は欠陥を修正しやすくなり，エンドユーザは自分が十分なフィッシング対策を行っているか判断しやすくなる．また本研究では，検査において特別なテスト環境を用意する必要を省き，エンドユーザの利用する環境をそのまま検査できるような設計を目指す．

本システムは，フィッシング攻撃の手法を用いて検査を行う SN (Scan Node: スキャンノード) と，擬似個人情報を保有する DN (Data Node: データノード) によって構成される．本システムの検査手順としては，まず DN が SN に対して検査を依頼する．SN は DN の依頼に対して，例えばランダムに生成した情報を DN に発行する．本研究では，このデータを擬似個人情報と定義する．さらに SN は，実際のフィッシング攻撃と同じ手法を用いて，DN に疑似個人情報を送信させようと試みることにより検査を行う．DN はこの検査に対し，SN に疑似個人情報を送信しようと試み，対策ツールはこの試みを阻止する．本研究ではこのような検査により，対策ツールの有効性を示す．

対策ツールを検査し，有効性を評価するという試みは頻繁には行われていなかった．これは，既存の攻撃がコンピュータシステムを標的とし，そのシステムの欠陥につけ込んだ攻撃であるのに対し，フィッシング攻撃がコンピュータシステムを利用する人間を標的とし，その錯覚につけ込んだ攻撃であることが原因であると考えられる．このため，フィッシング攻撃に関しては，コンピュータシステムによる自動的な検査が難しかった．

そこで本研究では，エンドユーザは攻撃者のフィッシング攻撃に対して個人情報を公開しようとする，という仮説のもと，エンドユーザの行動をエミュレートするエージェントを提案し，このエミュレータを NUE (Novice User Emulator: 初心者エミュレータ) と定義する．NUE は本システムの検査に対して，あたかも攻撃者の思うままに騙されている初心者のように，なるべく個人情報を送信しようと試みる．この試みを，対策ツールが防止できるか検査することにより，対策ツールの有効性を評価できると考える．

以下， 2 章に関連研究を延べ， 3 章に本システム及び本システムの実施する検査の概要について述べる．さらに 4 章において本システムの有効性や運用方法に関する考察を行い， 5 章では今後の課題について述べる．

2 関連研究

これまで多くのフィッシング攻撃に関する研究がなされており，その手口についてもいくつかの文献 [4, 5] にまとめられている． 1 章で述べたとおりフィッシング攻撃には誘致と取得の 2 つの段階がある．本章ではそれらの手口のさらなる詳細と，本研究の先行研究で行われている対策について述べる．

誘致の段階において，まず攻撃者はフィッシングメールを送信する宛先となるメールアドレスを入手する．この手法としては，数多くのウェブサイトを巡回し，その中に含まれているメールアドレスを抽出するクローリングと呼ばれる手法が挙げられる．クローリングの根本的な対策としては，ウェブサイトにメールアドレスを公開しないことである．また HoneySpam [6] では，クローリングの有効性を減らすため，特別なメールアドレスをウェブサイトに混入することを提案している．フィッシングメールの送信者が，クローリングによって抽出したこの特別なメールアドレスにフィッシングメールを送信した場合，エンドユーザからフィッシングメールの送信者を追跡するのが容易になるとされる．

さらに，エンドユーザの ISP にフィッシングメールが到着することを防ぐ技術も盛んに開発されている．Sender ID [7] はメールの発信者の照合を行い，メールサーバへのフィッシングメールの配送を防止する．さらにフィッシングメールがエンドユーザの ISP に到着したとしても，フィッシングメールであるか否かを判別することにより，通常のメールと隔離する技術もある．例えば IronPort [8] は過去のフィッシングメールから生成したシグネチャに一致するメールを隔離する機能を持つ．しかし，攻撃者が全く新しい内容のフィッシングメールを用いた場合，メールの内容のみによって正確にフィッシングメールを判別することは難しい．また，エンドユーザが到着したフィッシングメールを受信しても，S/MIME [9] などの電子署名を用いて，メールの送信者を確認し，フィッシ

ングメールを識別するような方法も考えられる．ただし現在，日常的に使用されているメールのほとんどは電子署名がされておらず，この手法のみを用いてフィッシングメールを判別することは不可能である．このため，届いたメールがフィッシングメールであるか否かの判定は，エンドユーザに委ねられることが多い．

攻撃者は，フィッシングメールの内容に騙されたエンドユーザにスパイウェアをダウンロードさせたり，クロスサイトスクリプティング脆弱性のあるウェブサイトを閲覧させたり，あるいはフィッシングサイトを閲覧させようと試みる．このような個人情報の取得の段階におけるフィッシング攻撃に対し，アプリケーションファイアウォール [10,11] は，ダウンロードやクロスサイトスクリプティング脆弱性による攻撃を防止できる．しかし，アプリケーションファイアウォールでは，フィッシングサイトを用いた攻撃を防止するのは難しい．この原因としては，フィッシングサイトの作成が容易であり，攻撃者はフィッシングサイトの URL を短時間で何通りにも変更できるため，フィッシングサイトを URL によってフィルタすることは効果が期待できないことが挙げられる．フィッシングサイトではない，社会的に信頼のおけるサイトの URL を収集し，その URL に対するアクセスのみを許可するようなフィルタも考えられる．しかし，このようなフィルタでは全く新しいウェブサイトはフィッシングサイトと誤認識され，ウェブサイトの閲覧が不可能となってしまう．そこで SPS [12] では，フィルタによりウェブサイト全体を閲覧できなくするのではなく，ウェブサイトの個人情報を入力する部分のみ取り除くことを提案している．ただし，有効性を示すためには，大規模な運用実験の結果が必要であると考えられる．

また，エンドユーザがフィッシングサイトを閲覧した後に動作する対策ツールを考える．フィッシングサイトではない正式なウェブサイトの場合，個人情報を入力するページにおいてサイト証明書が用いられていることが多い．そこで，このサイト証明書の有無や，内容が正規の認証局から発行された証明書であるかを検査することにより，ウェブサイトがフィッシングサイトであるか否かを判別する手法がある．ただし，全てのウェブサイトで個人情報の入力にサイト証明書が用いられている訳ではなく，この方法だけでは全てのフィッシングサイトを正確に判別し，個人情報の入力を防止することは難しい．

さらに，サイト証明書だけではなく，ウェブサイトの URL や内容，デザインを基に，フィッシングサイトであるか否かを識別するツール [13,14] もある．これらのツールは，エンドユーザがフィッシングサイトに対して個人情報を送信する際に警告を表示し，攻撃者に対する個人情報の送信を阻止する．しかし，Wu [3] らの実験では，このような対策ツールを用いてもなお 34% のユーザはフィッシングサイトに個人情報を漏洩するという結果が示されている．この実験によると，エンドユーザはフィッシングサイトが本物であるように錯覚した場合に警告を無視し，また本物のウェブサイトが貧弱な構成である時に，対策ツールが十分に動作しなかったとしている．

その上，攻撃者はこのような対策ツールを回避しようと試みる [15,16]．その多くは，対策ツールの実装上の欠陥を利用して，対策ツールの無力化を目指す．

以上のように，対策ツールが数多く開発されているにもかかわらず，個々の対策ツールは限られた場面でしか利用できず，その有効性も評価されていないことが多い．

3　対策ツールの有効性評価のためのスキャナ

2 章で述べた問題を解決するため，本研究では対策ツールの有効性を評価するスキャナを提案する．従来のスキャナはコンピュータシステムの脆弱性を検査し，修正すべき箇所を明らかにすることにより，システムの安全性を高める目的で利用されている．本システムも攻撃者が用いる技術を駆使して，エンドユーザの環境がフィッシング攻撃に対して脆弱であるか否かを検査する．

本章では本研究の提案するシステムに必要な機能を整理し，その上で実施する検査及び NUE の概要について述べる．

3.1　要件定義

本システムが保持すべき機能を以下に示す．

- 個々の対策ツールを検査する機能があること
  個々の対策ツールの有効性を評価する能力である．本研究では，エンドユーザの利用するコンピュータにおける対策についても，ISP における対策についても個別に評価する．これに対して，どちらか片方の対策だけ評価するという手法もある．例えばフィッシングメールをフィルタする機能は，エンドユーザの利用するメールクライアントでも，ISP におけるメールサーバにおいても利用可能である．エンドユーザがフィッシングメールを閲覧できなくすることを目的とするならば，どちらか片方の対策がなされていれば十分である．しかし ISP においてのみフィルタが行われている場合，エンドユーザが ISP を変更した時に，フィッシング攻撃に対し脆弱になる危険性がある．このため，エンドユーザにおける対策，ISP おける対策を個別に評価する必要があると考えられる．

- 拡張性が高いこと
  本システムに必要な検査項目は，新しい攻撃手法が発見されたり，既存の対策ツールに問題が発見される毎に増加する．このような新しい検査項目を容易に追加しうる拡張性が必要である．

- エンドユーザの本物の個人情報を漏洩しないこと
本システムがエンドユーザの本物の個人情報を漏洩しない機能が必要である．これは，検査の時にエンドユーザの本物の個人情報を取り扱うのではなく，擬似個人情報を取り扱うことによって解決できる．

- 自動的に検査を行えること
対策ツールの欠陥をコンピュータシステムが自動的に検査する機能である．フィッシングメールの内容や，閲覧しているウェブサイトがフィッシングサイトであるか否かをエンドユーザ本人に判断させた場合，検査項目が増えるにつれエンドユーザの負担が増える．そこで，エンドユーザのシステム上で動作するエージェントが，自動的に検査に対して応答する．

- 攻撃者に悪用されないこと
本システムが，攻撃者に悪用されないような機構が必要である．従来の脆弱性スキャナは，コンピュータの管理者が安全性を高める目的だけでなく，攻撃者がシステムに侵入し，犯罪を行う目的でも用いられる．このため，本システムでは，フィッシング検査を行う SN と，脆弱性を検査する対象である DN を分離する．そして，DN から SN に対してフィッシング検査を依頼しない限り，検査が行われないよう制御する．さらに，SN 単体ではいかなる脆弱性検査もできないよう制御する．これらの制御構造により，本システムの悪用を防止する．また，たとえ攻撃者が中間者攻撃を行ったとしても，検査を実施していることが発見されなかったり，検査結果が改ざんされないような機構も必要であると考える．

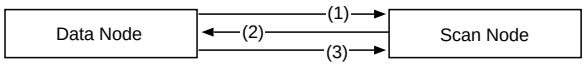

図 1: 検査の準備

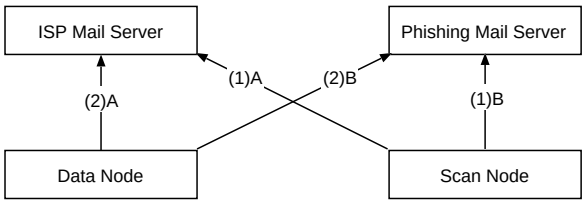

図 2: 誘致の段階における検査

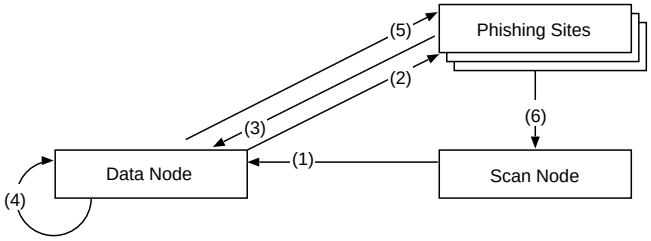

図 3: 取得の段階における検査

3.2 本システムが実施する検査の概要

本システムが実施する検査の概要について述べる．図 1 に検査を行うための準備について示す．まず DN は SN に検査を依頼する (図 1-(1))．SN は依頼を受け付け，ランダムかつ一意な疑似個人情報を生成し，DN に対し送信する (図 1-(2))．DN は，この情報を記憶し，準備が完了したことを SN に伝達する (図 1-(3))．また，検査を行う際に必要な情報があれば，この準備段階で SN に対して通達する．

次に，SN によりフィッシング攻撃の誘致の段階における検査を行う．SN はエンドユーザの ISP にフィッシングメールを送信し (図 2-(1)A)，DN にメールが到着するか否かを確認させる (図 2-(2)A)．ISP のメールサーバにフィッシングメールが到着していなかったり，メールをフィッシングメールであると認識し，フィルタにより削除されていた場合はフィッシング攻撃に対して安全であると判断できる．さらに，ISP における対策がなく，エンドユーザのシステムにおいて対策がなされている状況を想定した検査を行う．手法としては，SN でメールサーバを動作させ，フィッシングメールを配備し．(図 2-(1)B)，DN をこのメールサーバに接続させる (図 2-(2)B) ことにより，フィッシングメールフィルタの有効性を検査する．なお本研究では，攻撃者がメールアドレスを収集する段階においては省略している．その理由としては，エンドユーザのメールアドレスがすでに攻撃者に漏洩しているか否かを確認する有効な手法がないからである．

さらに，フィッシング攻撃の取得の段階における検査を行う．SN はフィッシングサイトを生成し，DN に対しそのフィッシングサイトを閲覧するよう指示する (図 3-(1))．また同時に，SN は DN で稼働している NUE に対して，閲覧していたフィッシングサイトのどのフォームに個人情報を入力し，どのボタンをクリックするかを指示する．次に DN はフィッシングサイトを閲覧するよう要求し (図 3-(2))，フィッシングサイトのコンテンツを受信する (図 3-(3))．フィッシングサイトを閲覧できた DN は，個人情報を入力し (図 3-(4))，その内容をフィッシングサイトに送信する (図 3-(5))．個人情報の送信が完了した場合，フィッシングサイトから SN に対して対策ツールの欠陥が発見されたことを通知する．図 3 の (2)

〜 (5) のいずれかにおいて個人情報の漏洩を防止できた場合，対策ツールが有効であると判断する．

このように，これまでのフィッシング攻撃の手法を利用した検査により，対策ツールの有効性を評価できると考える．

3.3 NUE の概要

NUE は，SN の命令を受け，擬似個人情報を送信しようと試みる，DN で稼働するエージェントである．NUE はフィッシングサイトを閲覧する際に，DN 上でウェブブラウザを起動する．これは，ウェブブラウザのアドインとして組み込まれているフィッシング攻撃対策ソフトウェアについて有効性を評価するためである．フィッシング攻撃対策ソフトウェアには，特にフィッシングサイトと検知したページを表示するか否かをエンドユーザにダイアログボックスを表示することにより警告し，ページを表示するか否か確認させるものもある．NUE はフィッシング攻撃に騙されてしまうようなエンドユーザの行動をエミュレートするエージェントであるため，警告の内容を無視するような挙動を行う．このため，ダイアログボックスに総当たり方式で応答するなど，警告を無視するような選択肢を調査し，フィッシングサイトをブラウザに表示するよう試みる．

さらに，NUE は指示されたフィッシングサイトのフォームの部品に個人情報を入力する．フィッシングサイト毎にフォームの形状は異なるため，SN はどのような手順で個人情報を入力するフォームに移動し，どのようにして個人情報を送信するのかを，フィッシングサイト毎に NUE に通達する必要がある．例えば代表的なフィッシングサイトの場合，フォームのテキストボックスに個人情報を入力し，送信ボタンなどのボタンにより個人情報を送信する．この場合， NUE からキーボードやマウスなどの入力装置を制御させ，フォーカスを適切な位置に移動させることにより，個人情報の送信が行われる．NUE が個人情報の入力や送信の際に，フィッシング攻撃対策ソフトウェアが警告を表示する可能性がある．これに対してもフィッシングサイトを閲覧するときと同様に，警告を無視するよう試みる．

このようにして，NUE が個人情報をフィッシングサイトに漏洩するよう試みることが可能となる．

4 考察

本章では，本研究の提案するシステムについて有効性を定性的に評価し，さらにその運用方法について考察する．

4.1 本システムの有効性

フィッシング攻撃の手法は変化し続けており，本研究で提案するシステムには，その変化に対応できる拡張性が求められる．しかし，従来の脆弱性スキャナと同様に，本システムは既知のフィッシング攻撃に用いられる手法についてのみ検査可能である．仮に攻撃者が毎回異なる手法でフィッシング攻撃を行うことが可能なら，本研究で提案するシステムの有効性は疑わしい．なお，この場合においては，既存の全ての対策ツールの有効性も疑わしくなり，フィッシング攻撃はエンドユーザのセキュリティ意識によってのみ対策せざるを得ない．このため，本研究にも，対策ツールにも，新しいフィッシング攻撃の手法を素早く収集し，たとえ攻撃者が新しい手法で攻撃を行っても被害を最小限にする機構が必要である．この機構は，Honeypot による対策を参考とすることにより実現できると考える．すなわち NUE が動作するホストに様々な手段でフィッシング攻撃をおびき寄せ，その手口を分析することにより検査項目を追加する．この分析が自動化でき，フィッシング攻撃の伝達速度よりも早く対策が行えるのであれば，本システムは十分に有効性が高いと言える．

また，本研究では疑似個人情報を用いて検査を行っているが，本当の個人情報が流出する際でないと警告を表示しない対策ツールも存在すると考えられる。従って，疑似個人情報にも一定の本物らしさが求められる．例えば，疑似個人情報としてクレジットカード番号を入力するのであれば，その値や長さ，あるいは生成アルゴリズムなどを同一にする必要がある．また，NUE に二要素認証やマトリクス認証を用いた個人情報を送信をさせる場合には，SN から DN で稼働する NUE に対し疑似個人情報入力の操作手順を通達する必要がある．さらに NUE がキーボードやマウスを制御するだけでなく，指紋読みとり装置や IC カードリーダのようなデバイスを操作可能になれば，生体認証や IC カード認証が用いられている場合にも検査が可能となる．

4.2 本システムの運用

本システムは，SN と DN が協調して動作することにより，対策ツールの有効性を評価する．仮に，SN が悪意ある第三者に乗っ取られた場合には，DN が SN の指示に従ってスパイウェアをダウンロードさせられるなどの被害が起こりうる．このため，SN の運用には注意が必要である．とりわけ，DN が第三者の SN を利用している場合は，その第三者が信頼のおける機関であることが保証されなければならないと考える．本研究では Spoofer Project [17] を参考とした運用を提案する．Spoofer Project は，ISP がエンドユーザの IP アドレスを偽造した通信を制限しているか否かを検査する目的のプロジェクトである．Spoofer Project では検査用のアプリケーションをエンドユーザにダウンロードさせ，エンドユーザのシステム上で実行し，IP アドレスを偽造した通信が特定のサーバに到達するか否かを検査する．す

なわち Spoofer Project では，一元的に管理されたサーバノードと，エンドノードで動作するエージェントが協調して動作することにより，プロジェクトの目的を達成している．

本研究についても，SN を一元的に管理し，DN 上で動作するエージェントを配布するような運用形態が考えられる．これにより，SN を新規に設置することなく検査を行うことが可能となり，利便性が増す．また，新しい検査項目が増えた場合も，一元的に管理されている SN に項目を追加するだけで対応可能となり，拡張性の面でも利点がある．なお，SN を一元的に管理することにより，SN が生成するフィッシングサイトの URL が指定しやすくなり，フィルタ等による対策手法が有効かどうか検証しやすくなる．このため，対策ツールの開発者らと協力し，この SN の生成する URL を対策ツールに登録してもらい，各フィルタの有効性をさらに細かく検査するような環境も実現しうると考えられる．

5 おわりに

本研究では，フィッシング攻撃の手法を踏まえ，対策ツールの有効性を評価するためのスキャナを提案した．本システムが実現できた場合，対策ツールの問題点の修正が容易になったり，エンドユーザにどのような対策が必要であるかを指摘しやすくなる．さらに，どのような対策ツールの組み合わせが良いか簡単に評価でき，フィッシング攻撃に対する安全性が高いエンドユーザの環境の構築が期待できる．また，本研究では本システムが悪用されないための制御機能などに関して基礎的な設計を行い，動作の概要について延べた上で，その有効性及び運用について考察した．

今後の課題としては，さらなる設計の詳細化が挙げられる．SN と DN における通信手法やメッセージフォーマットなどを定め，実装を行う．さらに，有効性評価の基準となる指標を策定し，本システムが単に欠陥の有無だけでなく，より粒度の細かい検査結果を出力できるような実装を目指す．

参考文献

[1] Anti-Phishing Working Group. Phishing Activity Trends Report - June, 2005, Jun. 2005.

[2] Tom McCall and Radley Moss. Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce, Jun. 2005.

[3] Min Wu, Rovert Miller, and Simson Garfinkel. Do Security Toolbars Actually Prevent Phishing Attack? In *Proceedings of SOUPS 2005, poster session*, Jul. 2005.

[4] Abhishek Kumar. Phishing - A new age weapon. Technical report, Open Web Application Secuirtry Project (OWASP), 2005.

[5] Gregg Tally, Rshan Thomas, and Tom Van Vleck. Anti-Phishing: Best Practices for Institutions and Consumers. Technical report, McAfee Research, Mar. 2004.

[6] Mauro Andreolini, Michele Colajanni, Francesca Mazzoni, and Luca Messori. HoneySpam: Honeypots fighting spam at the source. In *Proceedings of SRUTI 2005*, December 2005.

[7] J. Lyon and M. Wong. Sender ID: Authenticating E-Mail. Technical report, Internet Engineering Task Force, May 2005.

[8] IronPort Systems, Inc. The Leader in Network Security for Email - IronPort.

[9] B. Ramsdell. S/MIME Version 3 Message Specification. RFC 2633, Internet Engineering Task Force, June 1999.

[10] Blue Coat Systems, Inc. spyware prevention - Blue Coat Systems. Inc. - proxy servers, 2005.

[11] F5 Networks, Inc. TrafficShield Application Firewall, 2005.

[12] Daisuke Miyamoto, Hiroaki Hazeyama, and Youki Kadobayashi. SPS: A Simple Filtering Algorithm Thwart Phishing Attacks. In *Proceedings of AINTEC 2005*, Dec 2005.

[13] R. Dhamija and J.D. Tygar. The Battle Against Phishng: Dynamic Security Skins. In *Proceedings of SOUPS 2005*, Jul. 2005.

[14] Amir Herzberg and Ahmad Gbara. TrustBar: Protecting (even Naïve) Web Users from Spoofing and Phishing Attacks. Cryptology ePrint Archive, Report 2004/155, 2004.

[15] Eileen Zishuang Ye, Yougu Yuan, and Sean Smith. Web Spoofing Revisited: SSL and Beyond. Technical report, Department of Computer Science Dartmouth College, Feb 2002.

[16] Cristine E. Drake, Jonathan J. Oliver, and Eugene J. Koontz. Anatomy of a Phishing Email. In *Proceedings of CEAS 2004*, Jul. 2004.

[17] ANA Spoofer Project. http://spoofer.csail.mit.edu/.