フィッシング対策における技術・制度調査報告書
2007

平成１９年３月

フィッシング対策協議会

技術・制度検討ワーキンググループ

目　次

資料

フィッシング対策協議会 技術・制度検討 WG

1. はじめに

警察庁が発表した平成 18 年の不正アクセス行為の発生状況[1]によれば、不正アクセス禁止法違反による検挙件数は 703 件（うち不正アクセス行為 698 件、不正アクセス助長行為５件）で、前年と比べ 426 件増加した。また、不正アクセス行為（助長を除く）の態様は、セキュリティ・ホールを攻撃するものはなく、識別符号を窃用してアカウントを不正利用したもののみであった。識別符号入手の手口としては、フィッシングサイトを利用したものが一番多く 220 件であった。参考までに、スパイウェア等の不正なプログラムを使用して識別符号を入手したものは、フィッシングサイトにより入手したものに続き 197 件であった。

このように欧米ほどではないが日本においてもフィッシングによる被害が増加しており、フィッシングに対する技術面での対策や制度面での対策が至急望まれる。

フィッシング対策協議会の技術・制度検討ワーキンググループでは、平成１８年度、次の対処につなげるべく、現状の対策技術及び日本での制度面での調査検討を行い、課題を議論した。

2. フィッシングの定義

技術的対策及び制度面での対策を議論するに当たり、フィッシングと呼ばれるものがどの範囲に入るのかの定義を明確にする必要がある。フィッシング自身は、一般には実在する企業の偽の Web サイトを立ち上げ、その企業を装った偽のメールを送信することにより、ユーザを欺き、実在する Web サイトで使用する個人識別情報を盗む行為とされている。しかし、近年、個人識別情報を盗む方法として、従来の偽サイトを利用した方法以外の方法も広く使われてきている。例えば、米国の APWG (Anti-Phishing Working Group)では、マルウェアを使う方法や中間者攻撃など偽サイトを使わない方法もあげられている。更に、APWG のサイトで提供されている資料１「オンライン上での識別情報の盗難：フィッシングの技術、難点、および対抗策(Online Identity Theft: Technology, Chokepoints and Countermeasures)」においては、偽メールを利用した詐欺フィッシング以外にも、マルウェアベースフィッシング、DNS ベースフィッシング（ファーミング）、コンテンツインジェクション・フィッシング、中間者フィッシング、サーチエンジンフィッシングなどがをあげられてている。

さらに個人識別情報を盗むという方法においては、その情報を保存しているサーバの脆弱性を利用した方法もあり、攻撃のやり方のスコープを広げると、それに対する対策の議論も広がってしまう。

技術・制度検討ワーキンググループでは、今年度の議論を行うにあたってのフィッシングの定義を次のように定義した。

2.1 定義

フィッシング (phishing) は実在する組織を偽装した電子メールによって，ユーザネーム，パスワード，アカウントの ID，ATM の暗証番号，クレジットカードの内容のような個人識別情報をあたかも銀行や信頼できる団体に成り済まして受取人に打ち明けるように誘い込むことである。

よって、基本的に実在する組織を偽装して、ユーザを欺く特定の方法を使った攻撃をフィッシングと定義する。

2.2 今後の課題

個人識別情報に対する攻撃としては、先にあげたように、実在する組織を偽装したメールおよび偽装サイトによる方法以外にマルウェアによる方法も広く行われている。実際 2004 年に日本でも発生したインターネット・バンキングにおけるアカウントの盗み出しにはトロイの木馬が利用された。

また、最近、海外においては実在するサイトの偽装ではなく、個人識別情報を取得するためだけに、購入者の個人情報を取得する目的でオンライン販売のサイトを立ち上げ、購入者の個人情報を取得するサイトも出てきている。さらに過去の大量のクレジットカード情報の流出はほとんど脆弱なサーバに対する直接の攻撃であるか内

[1] 不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況（平成 18 年）
http://www.npa.go.jp/cyber/statics/h18/pdf35.pdf

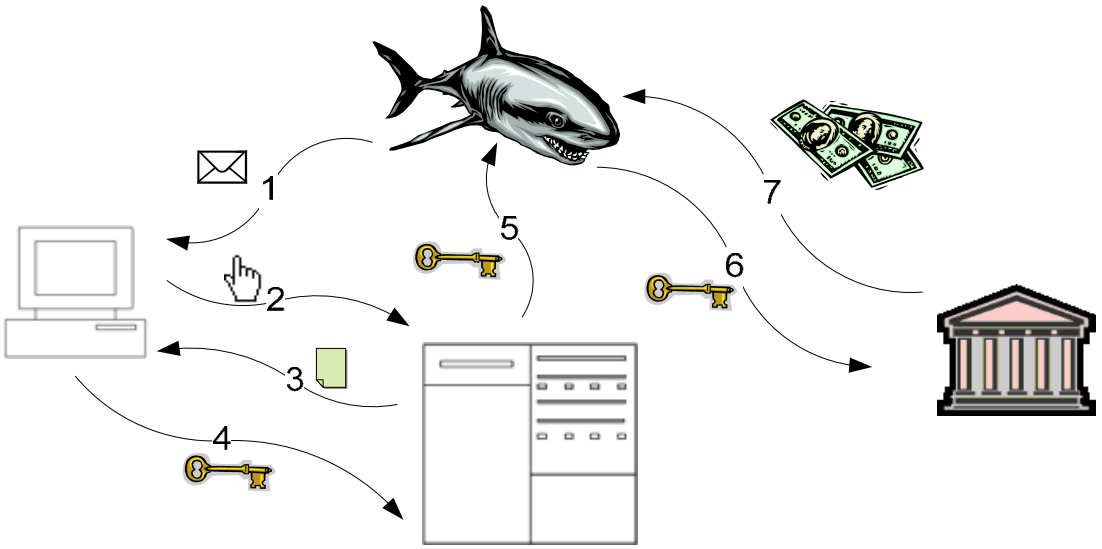
部犯行によるものである。
本報告書では（前項において）実在する組織を偽装して、ユーザを欺く特定の方法を使った攻撃と定義しているが、個人識別情報を盗まれるという被害の観点から、個別の手法を問わず、広く議論すべきではないかという意見も多く出てきた。

3. 技術面での検討

3.1 フィッシングの各攻撃段階での攻撃技術と対策の現状

資料１「オンライン上での識別情報の盗難：フィッシングの技術、難点、および対抗策(Online Identity Theft: Technology, Chokepoints and Countermeasures)」に沿って、図 3-1　フィッシング攻撃のステップのフィッシングの攻撃ステップに沿って、現時点における日本で実装可能または導入されている対策をまとめる。
フィッシングの各攻撃のステップは次の通りである。

0. フィッシングの準備段階
   攻撃ターゲットの選別や電子メール送信のためのアドレスの収集など
1. フィッシングのトリガの実行
   大量のメールの送信
2. トリガにユーザが反応
   届いたメールを開封し、URL をユーザがクリック
3. フィッシング攻撃の実行
   偽装サイトにユーザが訪問
4. 機密情報の送信
   偽装サイトでユーザが個人識別情報を入力し、漏洩
5. 機密情報がフィッシャーに送信
   偽装サイトに集められた個人識別情報をフィッシャーが取得
6. 機密情報を利用してのなりすまし
   入手した個人識別情報を利用してユーザになりすましてサービスを利用
7. 最終目的の不正行為の実行
   銀行の預金の勝手な振込みやオークション詐欺を働く



出典: Online Identity Theft: Technology, Chokepoints and Countermeasures, Aaron Emigh, 2005

図 3-1　フィッシング攻撃のステップ

3.1.1 ステップ０：フィッシングの準備段階

この段階ではフィッシャーは偽装しようとするサイトの類似ドメインの取得や偽装サイトを設置するための脆弱なサーバを探そうとする。類似ドメインの取得の禁止及び偽装サイトに利用される脆弱なサーバやクライアントを減らしていくということが対策として考えられるが、この場合技術的な面より、制度面での対策の方が有効であると考えられる。

3.1.2 ステップ１：フィッシングのトリガの実行（メールの送信）

フィッシングサイトへ誘導するために実在の組織を偽装した電子メールが送信される。偽装した電子メールがユーザに届くことを防ぐために、技術的には電子メールのフィルタリングが有効である。現在各 ISP においては迷惑メールフィルタサービスが提供されている。また、クライアントにおいても迷惑メール対策ソフトが市販されている。ただし、現時点ではフィッシングメール用ではなく、迷惑メール用のフィルタであるため、ユーザにとっては偽装したメールであるのか、実在する組織からのメールなのか判断することが難しく、迷惑メールフィルタリングの誤検知によりフィルタリングされてしまうこともある。また、偽装した電子メールを積極的に発見するためには、「おとり」メールアドレスを利用し偽装した電子メールを監視することも有効である。海外においては、偽装した電子メールの監視を行い、契約した会社に通知するサービスも存在する。

フィッシング対策協議会では参加企業でフィッシングに関する情報を共有することによって、フィッシングメールの迅速な発見、および情報共有に努めている。

メールのなりすましを防ぐためには、送信者認証も有効であるが、採用が一部にとどまっており、現時点では有効に働かない状況であると考えられる。

なお、日本の一部の金融機関においてはメールのなりすましを防ぐため、送信メールに証明書による署名メールを採用している。

3.1.3 ステップ２：トリガにユーザが反応(メールの URL に顧客が反応)

技術的な対策としては電子メールのデジタル署名技術を利用して、容易にユーザが偽装したメールを容易に判断できるようにする対策が効果的であり、現在、日本でも一部の金融機関では利用している。ただし、電子メールのデジタル署名技術はまだ広く普及していないことから、一般のユーザの認知度は低いと思われる。

この段階はフィッシングの手口や具体的被害状況などについて継続して注意喚起を行うなど、ユーザへの教育・啓発活動が大きな効果をもたらす。

3.1.4 ステップ３：フィッシング攻撃の実行

偽装されたから、ユーザのブラウザへのプロンプトの表示を防ぐことにより、フィッシング攻撃の実行を防ぐことが出来る。フィッシングサイトの構築には実在サイトに存在するクロスサイトスクリプトの脆弱性を使った方法も行われている。クロスサイトスクリプティングの脆弱性などを含む、Web アプリケーションの脆弱性を評価するサービスも数社から提供されている。また、クロスサイトスクリプティングの攻撃を検知し、ブロックする Web アプリケーションファイアウォールも提供されている。

3.1.5 ステップ４：機密情報の送信

ユーザが偽装したサイトに騙されて、機密情報を送信してしまうのをいかに防ぐかがこの段階で、多くのフィッシング対策がこのステップに焦点をあてた対策となっている。

現在、ユーザにフィッシング詐欺サイトであることを警告するために、下記のような方法を取り入れた、いくつかのフィッシング対策ツールバーが提供されている。

・ブラックリストによる方法
・ホワイトリストによる方法
・ヒューリスティックによる動的な判断

日本においても、すでにいくつかの金融機関等のサイトにおいて独自にフィッシング対策ツールバーを提供している。

また、昨年提供された Internet Explorer７、と FireFox2 では標準でフィッシング対策が組み込まれており、ユーザは容易にフィッシング対策ツールバーを導入できるようになっている。

さらに、Internet Explorer 7 では EVSSL (Extended Validation High Assurance SSL)という実在性も保証する厳密な証明書をサポートすることにより、ユーザが容易にサイトの安全性を判断できる仕組みも提供している。

それについては資料２「第三者認証について」に詳しく説明されている。EVSSL については日本においても普及を図っていくために「日本電子認証協議会」[2]が 2007 年 1 月に発足した。

Web サイト側からユーザが登録した画像情報を表示し、ユーザがサイト側を認証するサイト認証画像による方法も実用化されている。

図 3-2 のように、通常はユーザが Web サイトに認証情報を入力するが、画像による方法は、ユーザがあらかじめ登録していた画像を Web サイト側が提示し、それにユーザが認証することによって認証される。詐欺サイトはユーザが登録した画像を知らないため、ユーザに登録画像を提示できない。これにより、ユーザはサイトが本物であるかどうかを判断できる。さらにサイト画像認証の後に通常のパスワード認証を行い、サーバ側が本人を認証する方法が取られている。

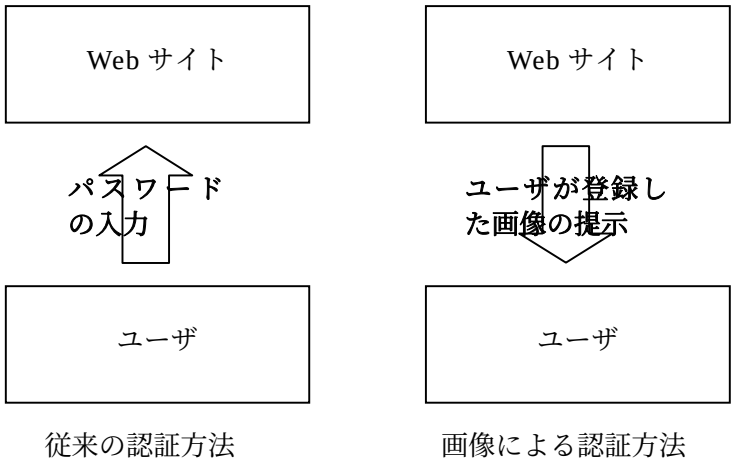


図 3-2　サイト画像認証

更に、資料３の「フィッシング対策としての画像による認証技術」に示すような、ユーザ個々人によってカスタマイズされた認証画面を表示し、ユーザが正しい画像を選択することによって、一回の画像による認証で、ユーザもサーバも相互を認証できる方法が開発され実用化されている。

3.1.6 ステップ５：フィッシャーが機密情報を入手

マルウェアであるキーロガーによる機密情報の取得から機密情報を守るため、ソフトキーボードやキー入力を

[2] http://www.jcaf.or.jp/

暗号化し、盗んだ情報が意味を持たないものにするツールも一部の金融機関等のサイトで提供されている。

3.1.7 ステップ６：機密情報を利用してのなりすまし

たとえ個人識別情報を盗まれたとしてもなりすましを防ぐ技術として、二要素認証が広く知られている。また、いくつかの金融機関等のサイトではすでに二要素認証の提供が行われている。二要素認証は一般的にコストが問題になるが、安価な方法としては乱数表を使った方法が提供されている。コストは高くなるが、より安全性の高い使い捨てパスワードのハードウェアトークンも一部の金融機関においては提供されている。

二要素認証はマルウェアによる中間者攻撃には脆弱である。そのような中間者攻撃にも安全な認証方式として、認証をオンライン以外の別ルート（たとえば電話回線を使っての認証）で実施する帯域外認証(Out of Band Authetication)も実用化されており、携帯電話を使った使い捨てパスワードによる帯域外認証もすでに製品として提供されている。具体的な方式に関しては資料４「２経路２端末・画像認証」を参照していただきたい。

また、実装レベルでは提供されていないが、記憶情報(パスワード)と記録情報(所有物)を使う二要素認証を、効率よく安全に実現する PAKE/LR-AKE という認証付き鍵共有プロトコル方式も提案されている。PAKE/LR-AKE については資料５「使いやすくフィッシングに対しても安全な通信路を作成する方法 PAKE/LR-AKE のご紹介」を参照していただきたい。

基本的にこの段階でのなりすましを防ぐ方法はすでに実装可能であるが、実装コストや運用コストのコスト面の問題により、広く一般的には利用されていないことが課題である。

3.1.8 ステップ７：最終目的の不正行為の実行

フィッシングによって取得された個人識別情報を使用し、金銭上の利益の取得を防ぐのがこの段階である。なるべくユーザの損失を可能な限り防ぐためにインターネットバンキングにおける振り込み金額を制限することなどが行われている。

クレジットカード会社では、ユーザのクレジットカード利用の異常行動から不正行為と思われるものを検知することも行われている。

4. 制度面での検討

フィッシング被害を減らすためには法律や制度面からのサポートが不可欠である。欧米、特に米国ではフィッシングを含むオンライン詐欺や犯罪を防ぐため、オンライン詐欺や犯罪のための特別な法制化も行われている。

4.1 日本と欧米(主に米国)との法制度での対応状況

日本ではフィッシング詐欺は基本的に著作権法、不正アクセス禁止法及び刑法（詐欺罪）で処罰されており、特にフィッシング詐欺を防ぐための特別な法制化は行われていない。一方、米国においては、多くの州でフィッシング対策法が提出され、一部の州では成立している。また、多くの州ではスパイウェア対策法にフィッシング対策の条項が盛り込まれており、オンライン犯罪に特化した法案が提出されている。詳しい状況に関しては資料６の「フィッシング・スパイウェアに関する法律・制度的状況－日本、米国、EU－」を参照していただきたい。

ただし、オンライン犯罪は国境を越えて行われることが多いため実効性に関しての課題も言及されている[3]。

4.2 フィッシングの各攻撃段階での法･制度面の検討

法・制度面においてもフィッシング詐欺全体ではなく、各攻撃段階における有効な現状の法・制度をマッピングすることで理解が容易になる。よって、以降、技術面での検討と同様に攻撃段階ごとに整理を行う。

4.2.1 ステップ 0：フィッシングの準備段階

この段階ではフィッシャーは偽装しようとするサイトの類似ドメインの取得を行う。JP ドメインに関しては株式会社日本レジストリサービス(JPRS)が類似ドメインの利用に対する注意[4]、および国際ドメイン名でのフィッシングの可能性について対策済みの情報[5]を提供している。

したがって、JP ドメインにおいては類似ドメインの取得については権利侵害であるとの認識が存在する。よって、JP ドメインに関しては、ある程度の抑止が行われていると考えられる。しかし、JP ドメイン以外で類似ドメインを取ることが考えられ、それについての対策は現時点では課題があると思える。

たとえば、下記の 2 つは一般の消費者にとっては区別することは難しいと思える。

www.ecom.jp
www.ecom-jp.com

また、偽装サイトのホスティングにボットが利用されていることが知られている。したがって、ボットに感染したクライアントをいかに減らすかという対策が有効である。

なお、２００６年１２月より、経済産業省と総務省が連携してボットネット対策事業を進めており「サイバークリーンセンタ」[6]というポータルサイトが開設され、対策情報が提供されている。

4.2.2 ステップ 1：フィッシングのトリガの実行

技術的対策で述べたように、技術的にはメールのフィルタリング技術の利用がこの段階の対策として有効である。なお、フィッシングのフィルタリングにおいては明らかにフィッシングと判断されるものはユーザに届く前に削除するのが有効である。しかし、ISP においてユーザのメールを無条件に削除することは禁止されており、法・制度面での検討が必要とされる。

また、送信者認証や電子署名メールの導入を加速するには制度面でサポートが必要と思われる。

現状の法制度の中では、フィッシングメールは正規の会社のブランドを偽って発信されるため、内容によっては著作権法での取り締まりも可能と思われる。

---

[3] http://www.law.duke.edu/journals/dltr/articles/PDF/2005DLTR0006.pdf
[4] http://jprs.jp/info/cyber-squatting/
[5] http://xn--wgv71a119e.jp/access/phishing.html
[6] https://www.ccc.go.jp/

4.2.3 ステップ 2：トリガにユーザが反応

偽装された電子メールにユーザが反応するのを防ぐためには、最も簡単で効果的なのがユーザに対する教育である。フィッシング対策協議会はフィッシングの事例を集めて情報提供するなど、Web 上での教育・啓発活動に力を入れている[7]。また、日本の多くの金融機関や一部のオンラインサービス業者においても教育・啓発サイトを用意したり、注意喚起を行ったりしている。また、警視庁のページや国民生活センタにおいてもフィッシングに対する啓発活動を行っている。その成果もあり、独立行政法人 情報処理推進機構による新たな脅威に対する意識調査[8]によればフィッシングについては言葉に対する認知は 80%を超えている。しかし、事象に対する正しい認知は半数に留まっており、教育啓発については更なる努力が望まれる。

米国ではフィッシングに限定せず、一般消費者の個人識別情報の盗難について連邦取引員会（FTC：Federal Trade Commission）が Web ポータルサイト[9]を立ち上げ、消費者の啓発を行っている。

オンラインでの経済活動の規模の拡大に伴い、オンラインの各種の個人識別情報が犯罪者に狙われる事例が増えており、フィッシングに限らず、個人識別情報の盗難に関する分かりやすいポータルサイトの作成が望まれる。

資料 7 の「パスワード管理とフィッシング対策」に記載されているように、一般のユーザに個人識別情報の管理方法や注意事項について広く啓発することが重要である。

なお、フィッシングメールを発見した場合は迅速にユーザへ注意喚起をすることが必要である。現在、多くの金融機関や一部のオンラインサービス業者においては自社を偽装した電子メールに対する監視を行い、発見した場合、ユーザに注意喚起を行っている。特定の会社を偽装した電子メールの監視サービスを行っている会社も存在するが、日本においては、そもそもフィッシングのターゲットとなっているブランドが少ないためか、現状そのようなサービスを採用する会社は少ないようである。

4.2.4 ステップ３：フィッシング攻撃の実行

技術面での検討で述べたようにこの段階では偽装される会社のクロスサイトスクリプトの脆弱性をなくすことがクロスサイトスクリプトの脆弱性を利用した詐欺サイト対策として有効である。現在、情報処理推進機構では脆弱性関連情報の届出[10]を受け付けており、サイトの脆弱性が未対策のまま公開されることを防ぐため調整業務を行っている。また、Web アプリケーションのセキュアな構築方法についての教育や啓発活動を行っている[11]。

4.2.5 ステップ 4：機密情報の送信

技術面の検討での検討で述べたようにこの段階においては多くの技術的な対策の提供が行われており、制度的に技術の普及を後押しできることが望ましいと思われる。

4.2.6 ステップ 5：フィッシャーが機密情報を入手

現状の法・制度ではフィッシャーが個人識別情報を入手しただけでは罰することが出来ない。

個人識別情報の利用価値の上昇とともに個人識別情報の盗難も増加している中、今後この段階を抑止するための法･制度面での検討が望まれる。

4.2.7 ステップ 6：機密情報を利用してのなりすまし

この段階においても 2 要素認証や帯域外認証など、たとえ個人識別情報を悪用されても、なりすましを防ぐ技術的な方法を実装可能であるが、コスト面等の問題から一部の導入にとどまっている。制度的に技術の普及を後押しすることが望ましいと思われる。

法的な面では、この段階では不正アクセス法により罰則を適用可能で、フィッシング詐欺の多くがこの段階で

---

7 http://www.antiphishing.jp/

8 http://www.ipa.go.jp/security/fy18/reports/ishiki01/index.html

9 http://www.ftc.gov/bcp/edu/microsites/idtheft/

10 http://www.ipa.go.jp/security/vuln/report/index.html

11 http://www.ipa.go.jp/security/vuln/event/200612.html

不正アクセス禁止法の違反として摘発されている。

4.2.8 ステップ 7：最終目的の不正行為の実行

この段階では現行の刑法によって、罰則を適用することが可能である。ただし、オンライン犯罪の特徴として国境をまたいで実行されることが考えられ、その場合に国内法による対応の限界が考えられる。

5. まとめ

フィッシングは複数の攻撃手法が組み合わせられていることから、その技術的対策および法・制度的対策の検討においても、それぞれの攻撃段階に沿って議論することが現実的であると思われる。そおため、技術的対策および法・制度的対策についてまとめたものを表 5-1 に示す。

フィッシング対策ツールバーのブラウザへの標準実装や金融機関における二要素認証の実施など、技術的対策の一部は徐々に導入が進みつつある。しかし、一方で ID の盗難という観点ではマルウェアの利用や、従来のフィッシングの範囲を超えた技術が利用されており、さらに新たな技術的対策が必要とされている。更に、技術的対策の一部については、その普及について制度的なバックアップが必要と思われる。

法･制度面においては、処罰が限定的であることから、処罰によりフィッシング行為を抑制することは期待できそうにない。米国のいくつかの州のフィッシング対策法では ID を提供させるように導く行為自身が処罰の対象となっており、フィッシング行為そのものに重い罰則を科している。日本においてもフィッシングの被害が拡大する前に、いかにフィッシングを抑制するかの法･制度面での検討が必要と思われる。また、新たなフィッシング手法が開発されているのため、それも含めた法・制度面での検討が必要と思われる。

表 5-1　技術的対策と法･制度面での対策のまとめ

ステップ	内容	技術的対策方法	法･制度面での対策
0：フィッシングの準備	攻撃ターゲットの選別や電子メール送信のためのアドレス収集。類似ドメインの取得	類似ドメイン取得の監視	類似ドメイン取得の禁止 JPRS による類似ドメイン取得に関する注意喚起の提供
1：メールの送信	フィッシングサイトに誘導するために詐欺メールの送信	ISP によるメールフィルタリング技術 送信者認証、メールの電子署名 *課題：迷惑メール用フィルタのため、フィッシングの場合フィルタの誤検知のとの見分けが付かない*	迷惑メール法、偽装メールに対する著作権法の適用 *課題：送信者認証や電子署名の技術を推進する制度が必要とされる。*
2：ユーザがメールに反応	届いたメールを開封し、URL をユーザが実行	証明書付き電子メール	教育･啓発活動によるユーザの教育 フィッシング対策協議会の Web によるフィッシングの啓発活動
3：フィッシング攻撃の実行	偽装サイトにユーザが訪れる	クロスサイトスクリプティングの脆弱性の除去	偽装 Web に対する著作権法の適用
4：機密情報の送信	偽装サイトにユーザが個人識別情報を入力する	ユーザが容易にフィッシングサイトを見分けられるようにするための技術 ･フィッシング対策ツールバー ･実在性も保証する厳密な証明書(EV SSL) ･サイト画像認証 ･画像を利用したユーザ認証	*課題：制度面での技術の普及の後押しが必要*
5：機密情報の入手	偽装サイト上の収集された個人識別情報をフィッシャーが取得	マルウェアによる識別情報の盗み取りを防止するための技術 ･ソフトキーボード、キーロガー検知	*課題：個人識別情報の入手を罰する手段がない*
6：機密情報の利用	個人識別情報を利用してユーザになりすましてサービスを利用	盗み出した個人識別情報を利用してもなりすましを出来ないようにするための技術 ･二要素認証 ･帯域外認証 *課題：コスト*	不正アクセス禁止法 *課題：制度面での技術の普及の後押しが必要*
7：不正行為の実行	クレジットカードの利用や預金の引き落としなど不正行為の実行	トランザクションの不正検知	現行の刑法に順ずる *課題：国際的な犯罪に対する国内法の限界*

6. 用語解説

・ 中間者攻撃(Man in the middle attack)：
　　通信を行う二者の間に入り込んで、途中のデータを盗聴し、改ざんする攻撃。
・ クロスサイトスクリプティング攻撃(Cross site scripting attack)：
　　Web サイトがスクリプトを利用している場合、スクリプトの脆弱性のために、他のサイトのページのスクリプトを自身のページのスクリプトとみなして実行してしまう脆弱性
・ ヒューリスティックによるフィッシングサイトの検知：
　　フィッシングサイト特有の特徴を識別してフィッシングサイトを見分ける方法
・ EV SSL(Extended Validation High Assurance SSL)：
　　証明書申請元が実際に存在することを保証する厳密で高いレベルの証明書。Internet Explorer の Version7 にて正式に採用。
・ 二要素認証(Two Factor Authentication)：
　　SYK(Something You Know 記憶)、SYH(Something You Have 所有物)、SYA(Something You Are 本人の特徴)の 3 つの認証方法のうち 2 つを組み合わせた認証方式。
・ 帯域外認証(Out of Bad Authentication)：
　　通信に利用する経路とは別の経路を使って認証を行う方式。たとえば、通信には Internet を利用するが、認証は電話回線を利用。
・ フィッシャー(Phisher)：
　　フィッシング攻撃を仕掛ける人

7. 技術･制度検討ワーキンググループ参加メンバ

(敬称略・順不同)

【委　　員】		所属	
(主査)	野々下　幸治	特定非営利活動法人　日本ネットワークセキュリティ協会	(ウェブルート･ソフトウェア株式会社)
(制度)	内田　浩示	全国銀行協会	
(制度)	山口　朗	株式会社オリエントコーポレーション	
(技術)	石田　公孝	有限会社ストーンズインターナショナル	
(技術)	國米　仁	株式会社ニーモニックセキュリティ	
(技術)	久波　健二	特定非営利活動法人日本ネットワークセキュリティ協会	(日本アイ･ビー･エム)
(技術)	西田　助宏	特定非営利活動法人日本ネットワークセキュリティ協会	(NRI セキュアテクノロジーズ)
(制度)	阿部 俊克	特定非営利活動法人日本ネットワークセキュリティ協会	(株式会社ジャパンネット銀行)
(技術)	降簱　浩司	株式会社日立製作所	
(技術)	青木　雄一	サイバートラスト株式会社	
(技術)	浅井　英里子	マイクロソフト株式会社	
(制度)	神田　祥子	マスターカード･インターナショナル･ジャパン･インク	
	内田 勝也	(情報セキュリティ大学院大学)	
(制度)	石原　智	株式会社セキュアブレイン	
	秋山　卓司	日本コモド株式会社	
	やすだ なお	特定非営利活動法人日本ネットワークセキュリティ協会　事務局	
	林　佳子	特定非営利活動法人日本ネットワークセキュリティ協会　事務局	

フィッシング対策協議会 技術・制度検討 WG

8. 資料一覧

(1) APWG 「Online Identity Theft: Technology, Chokepoints and Countermeasures」(オンライン上での識別情報の盗難：フィッシングの技術、難点、および対抗策)
　Radix Labs アーロン・エイミー
(2) 第三者認証について
　サイバートラスト株式会社認証サービス事業部
(3) フィッシング対策としての画像による認証技術
　株式会社ニーモニックセキュリティ　國米　仁
(4) ２経路２端末・画像認証
　株式会社ニーモニックセキュリティ　國米　仁
(5) 使いやすくフィッシングに対しても安全な通信路を作成する方法 PAKE/LR-AKE のご紹介
　独立行政法人 産業技術総合研究所 情報セキュリティ研究センター 主幹研究員 古原 和邦
(6) フィッシング・スパイウェアに関する法律・制度的状況－日本、米国、EU－
　株式会社三菱総合研究所　吉永京子
(7) パスワード管理とフィッシング対策
　有限会社ストーンズインターナショナル　石田公孝

資料1

オンライン上での識別情報の盗難：フィッシングの技術、難点、および対抗策

(Online Identity Theft: Technology, Chokepoints and Countermeasures)

Radix Labs
アーロン・エイミー（Aaron Emigh）
ate@radixlabs.com

2005年10月3日

謝辞

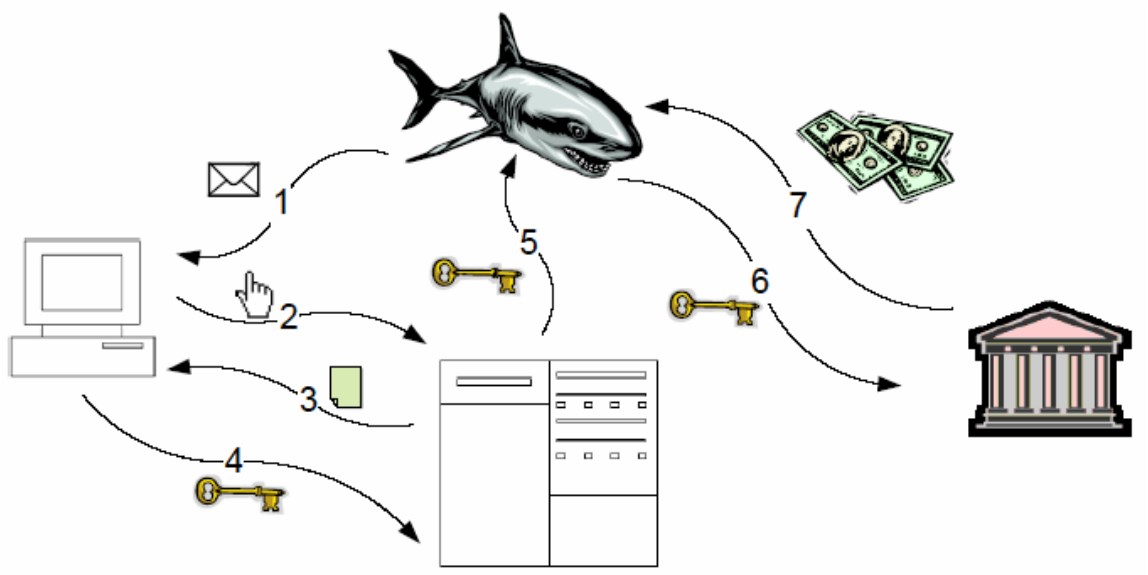
本書への財政援助について、国土安全保障省の科学技術部門（DHS S&T）に感謝する。本書に含まれる見解は著者のものであり、必ずしも国土安全保障省または科学技術部門の公式な姿勢を示すものではない。本報告書の内容は、DHS S&T、SRI International、Anti-Phishing Working Group（APWG）、民間産業などの官民の連携によるIdentity Theft Technology Councilのメンバーによってまとめられた。本書に貢献いただいたDan Boneh氏、Drew Dean氏、Louie Gasparini氏、Ulf Lindqvist氏、John Mitchell氏、Peter Neumann氏、Robert Rodriguez氏、Jim Roskind氏、Don Wilborn氏に特に感謝の意を表明する。

対象とする読者

本報告書は、セキュリティ担当者、エグゼクティブ、研究者、オンライン上での識別情報の盗難者が使用する手法やそのような犯罪を防ぐための対抗策を理解したい人々など、技術に精通した読者を対象としている。

要旨

フィッシングとは、オンライン上での識別情報の盗難によって個人の機密情報が取得されることである。フィッシングには、不正なメッセージによってユーザを騙し、情報を提供させる詐欺攻撃、悪質なソフトウェアがデータの漏洩を招くマルウェア攻撃、ホスト名のルックアップを変更し、不正サーバにユーザを導くDNSベース攻撃などがある。
ガートナー・グループでは、米国の銀行およびクレジットカード発行会社でのフィッシング関連の直接的な損失は、2003年には12億ドルだったと推定している。間接的な損失はこれよりもはるかに大きく、顧客サービス費用、口座の書き換えコスト、さらにはオンラインでの金融取引の安全性に対する不安の広まりによる、オンライン・サービスの使用の減少を原因とする費用の増加などが生じている。不正な活動によって傷つけられた信用の修復は困難なため、フィッシングは被害に遭った消費者にもかなりの苦難をもたらす。
本報告書では、あらゆるタイプのフィッシング攻撃における情報の流れを検証する。フィッシャーが使用する技術とともに、適用できる対抗策についても説明する。フィッシングを防ぐために導入できる技術に主に注目する。現在利用可能な対抗策と研究段階にある技術の両方を紹介する。



フィッシング攻撃のステップ

フィッシング攻撃は、いずれも同じ一般的な情報の流れに従っている。流れの各ステップにおいて、異なる対抗策の適用により、フィッシングを防ぐことができる。ステップは次の通りである。

0. フィッシャーが攻撃の準備をする。ステップ0の対抗策としては、フィッシング攻撃を開始前に検出するための、悪意のある活動の監視などがある。
1. 悪質なペイロードが何らかの伝搬媒介(ベクトル)を通じて届く。ステップ1の対抗策は、フィッシング・メッセージまたはセキュリティの弱点への攻撃が届くのを防ぐことである。
2. 情報漏洩に対し脆弱となるような行動をユーザがとる。ステップ2の対抗策では、フィッシング戦術を検出し、フィッシング・メッセージをより騙されにくいものにする。
3. ユーザが、リモートWebサイトまたはローカルでWeb上のトロイの木馬によって機密情報を要求される。ステップ3の対抗策では、フィッシング内容がユーザに届くのを防ぐことに重点を置く。
4. ユーザが機密情報を漏洩する。ステップ4の対抗策では、情報の漏洩を防ぐことに集中する。
5. 機密情報がフィッシング・サーバからフィッシャーに送信される。ステップ5の対抗策では、情報の送信を追跡する。
6. 機密情報がユーザになりすますために使われる。ステップ6の対抗策では、情報をフィッシャーにとって役に立たないものにすることに重点を置く。
7. フィッシャーが漏洩情報を使用して不正行為を行う。ステップ7の対抗策では、フィッシャーが金銭を受け取るのを防ぐことに重点を置く。

フィッシングは、社会的要因だけでなく技術も関与する複雑な現象である。すべてのフィッシングを防げるような単一の「特効薬」はない。しかし、技術を適切に適用すれば、識別情報の盗難のリスクを大幅に軽減できる。このような技術を適用する機会は多数ある。たとえば次のようなものである。

- Webサイトの使用やドメイン登録など、悪質な可能性のある活動を監視し、フィッシング攻撃を開始前に検出してフィッシャーの準備を妨害する（ステップ0）。
- 非認証メッセージを廃棄できるよう、電子メール・メッセージの認証を行う（ステップ1）。
- 商標、ロゴ、およびその他の専有画像の不正使用を検出する（ステップ1）。

- マルウェアへの耐性を強化するために、セキュリティ・パッチのインフラストラクチャーを改善する（ステップ1）。
- 個人情報を使用し、ユーザに対して電子メールの認証を直接行う（ステップ2）。
- 不正なWebサイトを検出し、ユーザに警告する（ステップ4）。
- 相互認証プロトコルを使用する（ステップ4）。
- 情報が対象とする受信者によってのみ使われるよう、ユーザとWebサイトの間に信頼できるパスを確立する（ステップ4および6）。
- 二要素認証を使用する（ステップ6）。
- パスワードをサイト別にするよう強制する（ステップ6）。
- 公開鍵暗号を使用して証明書をエンコードし、妥当性に制限を設ける（ステップ6）。

はじめに

フィッシングとは、オンライン上での識別情報の盗難によって個人の機密情報が取得されることである。カード・スキミングや「ダンプスター・ダイビング（ゴミ箱漁り）」などのオフラインでの識別情報の盗難や、多数の個人の情報が一度に取得されるような大規模なデータ漏洩とは区別される。フィッシングには、次のようにいくつものタイプの攻撃がある。

- 不正なメッセージによってユーザを騙し、情報を提供させる詐欺攻撃
- 悪質なソフトウェアによりデータの漏洩を招くマルウェア攻撃
- ホスト名のルックアップを変更し、不正サーバにユーザを導くDNSベース攻撃

フィッシングでは、ユーザ名とパスワード、ソーシャル・セキュリティ・ナンバー、クレジット・カード番号、銀行口座番号、さらには誕生日や母親の旧姓をはじめとする個人情報など、さまざまな機密情報が狙われる。
ガートナー・グループでは、米国の銀行およびクレジット・カード発行会社でのフィッシング関連の直接的な損失は、2003年には12億ドルだったと推定している。間接的な損失はこれよりもはるかに大きく、顧客サービス費用、口座の書き換えコスト、さらにはオンラインでの金融取引の安全性に対する不安の広まりによる、オンライン・サービスの使用の減少を原因とする費用の増加などが生じている。不正な活動によって傷つけられた信用の修復は困難なため、フィッシングは被害に遭った消費者にもかなりの苦難をもたらす。
フィッシング攻撃の頻度とその巧妙さは、いずれも劇的に向上している。最近のフィッシング攻撃や関連統計については、http://www.antiphishing.orgで紹介されている。
フィッシングは複数の国に及ぶことが多く、組織犯罪として行われるのが一般的である。影響を受ける機関は法的措置の追求が可能であり、追求をすべきだが、長期的な解決策においてはフィッシングを防ぐための技術的な措置が不可欠な要素となる。
本報告書ではフィッシャーが使用する技術を検証し、技術的な対抗策について市販のものと提案段階のものの両方を評価する。

フィッシング攻撃のタイプ

フィッシングはさまざまな方法で行われる。フィッシャーは技術的に革新的であり、技術に投資する余裕がある。フィッシャーが素人であるという考えは、よくある誤解である。専門的な組織犯罪として行われるような、最も危険なフィッシング攻撃にはこれは当てはまらない。金融機関がオンライン上での存在感を増すのに伴い、口座情報の漏洩の経済的価値は劇的に拡大してきた。フィッシャーなどの犯罪者は、犯罪によって不法に得た利益に比例して技術への投資が可能になっている。
現在のフィッシング攻撃の巧妙さと急速な発展を考えると、フィッシャーが採用する技術の包括的な目録作りは不可能である。以下では、いくつかのタイプの攻撃について説明する。攻撃のタイプ間の区別は明確なものではない。フィッシング攻撃の多くは複数の技術を採用したハイブリッド攻撃だからである。たとえば、フィッシン

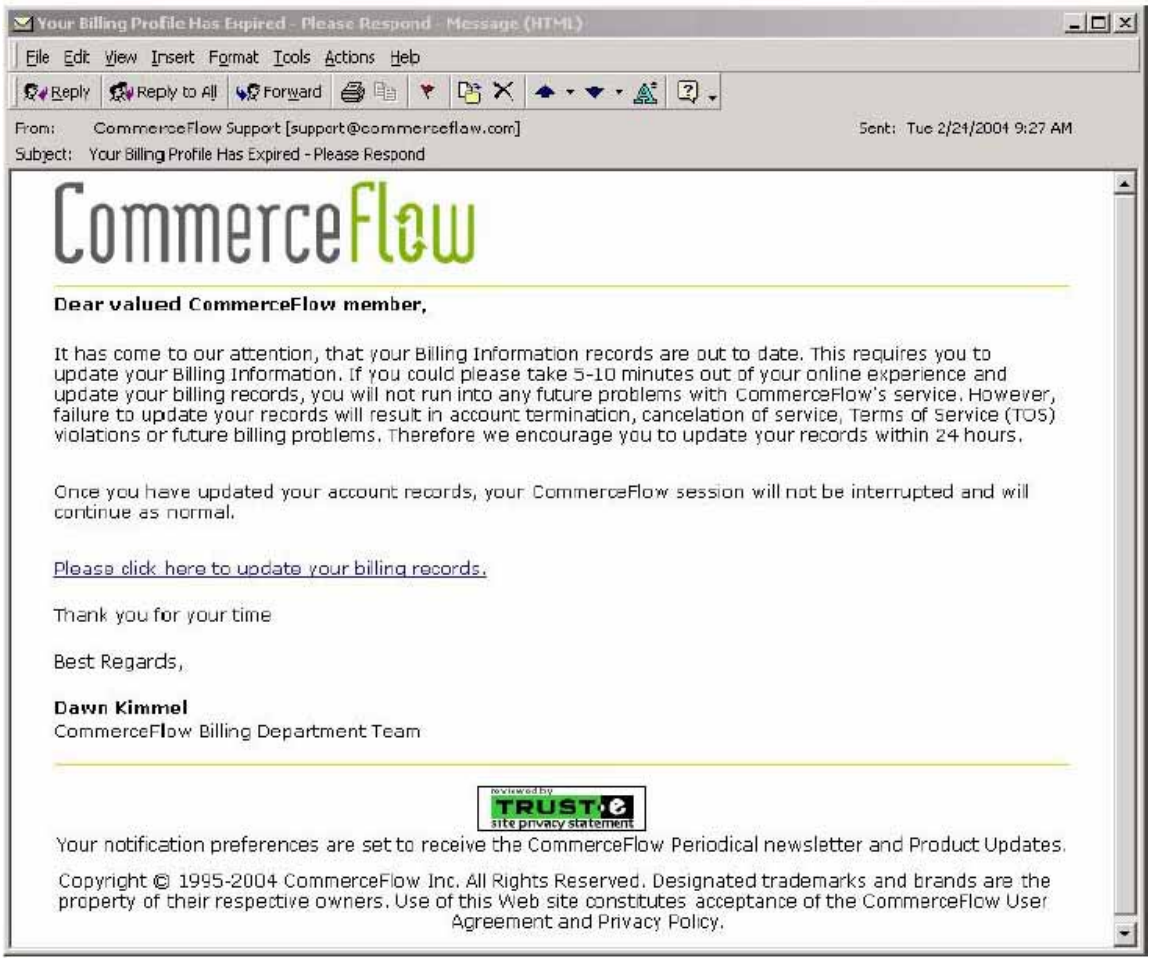
グ目的の詐欺電子メールでは、コンテンツインジェクションを受けたサイトにユーザを誘導し、そこでユーザのhostsファイルを攻撃するマルウェアをインストールする。その後正規のWebサイトにアクセスしようとするとフィッシング・サイトに転送され、中間者攻撃によって機密情報が漏洩される。

詐欺フィッシング

「フィッシング」という用語は、インスタント・メッセージによるAOLのアカウントの盗難が起源だが、今日最も一般的な詐欺フィッシングの媒介は電子メールである。代表的なシナリオでは、フィッシャーは受信者にリンクをクリックするよう求める「行動要請」の詐欺電子メールを大量に送信する。「行動要請」の例としては、次のようなものがある。

- 金融機関またはその他のビジネスにおいて受信者の口座に問題があるというメッセージ。電子メールでは、電子メール内の詐欺リンクを使用してWebサイトにアクセスし、問題を解決するよう受信者に求める。
- 受信者の口座が危険にさらされているとし、受信者に詐欺防止プログラムへの加入を勧めるメッセージ。
- 受信者が注文していない架空の商品（不快感を与えるような商品が多い）に関する請求書と、その偽の注文を「取り消す」ためのリンク。
- ユーザのアカウントへの好ましくない変更が行われたことを知らせる不正な通知と、その不正な変更に「異議を唱える」ためのリンク。
- 金融機関で新しいサービスが導入され、既存のメンバーである受信者に対し期間限定でサービスを無料で提供するという知らせ。

いずれの場合も、ユーザが誘導される先のWebサイトでユーザの機密情報が集められる。受信者が不正なWebサイトに機密情報を入力すると、フィッシャーは後に被害者になりすまして被害者の口座からの送金、商品の購入、被害者の住宅に対する2つ目のローンの申し込み、失業手当の申請などを被害者の名前で行ったり、その他の被害を及ぼす。
多くの場合、フィッシャーは経済的な損害を直接生じさせるのではなく、不法に取得した情報を二次市場に転売する。犯罪者たちは、このような情報が売買されるさまざまなオンライン・ブローカリング・フォーラムやチャット・チャネルに参加している。
詐欺ベースのフィッシング方式には多種多様なものがある。HTMLで電子メールを受信している人にはログイン・ページの複製を直接電子メールで提供できるため、リンクをクリックし、ユーザのWebブラウザーを起動する必要がない。
フィッシング・サイトへのリンクでは、ホスト名の代わりに数字のIPアドレスが使われる場合がある。そのような場合、Javascriptによってブラウザーのアドレスバーに取って代わったり、その他の方法で正規のサイトと通信しているとユーザを信じさせることが可能である。*類似ドメイン攻撃(cousin domain attack)*では、正規のドメイン・ネームと一見同じに見えるような、フィッシャーによって制御されたドメイン・ネームを使用するため、このような複雑さを回避できる。たとえば、www.commerceflow.comの代わりにwww.commerceflowsecurity.comが使われる。ユーザが悪質なサイトを訪問すると、最初の詐欺ベースのメッセージが、マルウェアのインストールへと発展することもある。



代表的な詐欺フィッシング・メッセージ

マルウェア・ベース・フィッシング

マルウェア・ベース・フィッシングとは、一般的に、ユーザのマシン上で悪質なソフトウェアを実行するあらゆるタイプのフィッシングを意味する。マルウェア・ベース・フィッシングにはいくつもの形のものがある。最も蔓延しているものを以下で紹介する。

一般的に、マルウェアはソーシャル・エンジニアリングまたはセキュリティの脆弱性の悪用のいずれかによって広まる。ソーシャル・エンジニアリング攻撃の典型的なものでは、電子メールの添付を開いたりファイルをWebサイトからダウンロードするようユーザを説得し、添付がポルノ、有名人のわいせつな写真や噂話などに関するものだとする場合が多い。ダウンロード可能なソフトウェアにもマルウェアを含むものがある。マルウェアは、セキュリティの脆弱性につけ込んでマルウェアをインストールするワームまたはウィルスの伝搬、またはセキュリティの脆弱性につけ込んだWebサイトからのマルウェアの提供のいずれかのセキュリティ攻撃によって広まることもある。サイト上に何らかの魅力的なコンテンツがあることを約束するスパム・メッセージなどのソーシャル・エンジニアリングや、クロスサイトスクリプティング脆弱性などのサイト上のセキュリティの弱点につけ込み悪質なコンテンツを正規のWebサイトに注入することなどによって、トラフィックが悪質なWebサイトに導かれることもある。

キーロガーとスクリーンロガー

キーロガーとは、自らをWebブラウザーにインストール、またはデバイス・ドライバーとしてインストールし、入力されたデータを監視して関連データをフィッシング・サーバに送信するプログラムである。キーロガーではいくつかの異なる技術が使われ、次のようなさまざまな方法で実装される。

- URLの変化を検出し、URLが指定された認証情報収集サイトになった際に情報をログに記録するブラウザーのヘルパー・オブジェクト
- キーボードとマウスからの入力とともにユーザの活動を監視するデバイス・ドライバー
- ユーザの入力と画面の両方を監視し、他のオンスクリーン入力セキュリティ対策を阻止する*スクリーンロガー*

キーロガーは、さまざまなサイトの認証情報を収集できる。キーロガーは通常、ユーザの位置を監視し、特定のサイトの認証情報のみを送信するようパッケージ化されている。金融機関、情報ポータル、企業のVPNなど、何百ものサイトが標的とされていることが多い。キーロガーの被害を受けた後には、さまざまな二次的被害が生じる可能性がある。実際に起きた例として、ポルノのスパムによってキーロガーが広まり、ある信用調査機関が巻き込まれたことで、この機関にアクセスできる50のアカウントが被害に遭い、それにより最終的に310,000組を超す個人情報が信用調査機関のデータベースから漏洩した。

セッション・ハイジャッカー

セッション・ハイジャッキングとは、主として悪質なブラウザー・コンポーネントによってユーザの活動が監視される攻撃である。ユーザが自らのアカウントにログインもしくは取引を開始すると、ユーザが正当に認証を確立した段階で悪質なソフトウェアがセッションを「ハイジャック」し、悪質な行為を行う。
セッション・ハイジャッキングは、マルウェアによってユーザのローカル・コンピュータで行われることもあれば、後に説明する中間者攻撃の一環としてリモートで行われることもある。マルウェアによってローカルに行われる場合、ユーザの自宅のコンピュータから開始されるため、セッション・ハイジャッキングは標的サイトからは正規ユーザとの対話とまったく同じに見える。

Web上のトロイの木馬

Web上のトロイの木馬は、認証情報を集めるためにログイン画面でポップアップする悪質なプログラムである。ユーザはWebサイトに情報を入力していると信じているが、実際には情報はローカルに入力され、フィッシャーに送信されて悪用される。

Hostsファイル・ポイゾニング

ユーザがURLバーにwww.company.comとタイプするか、またはブックマークを使用した場合、ユーザのコンピュータはサイトを訪問する前にそのアドレスを数値アドレスに変換する必要がある。Windowsなどの多くのオペレーティング・システムには、DNS（ドメイン・ネーム・システム）ルックアップを実行する前にホスト名をルックアップするためのショートカット用の「hosts」ファイルがある。このファイルを変更すれば、www.company.comが悪質なアドレスを参照するようにできる。ユーザがそこにアクセスすると正規のようなサイトが表示され、ユーザは機密情報を入力し、その情報は実際には意図した正規のサイトではなくフィッシャーに送られる。

システム再構成攻撃

システム再構成攻撃は、ユーザのコンピュータ上での設定を変更し、情報を漏洩させる。
あるタイプのシステム再構成攻撃では、ユーザのDNSサーバを変更し、下記のように誤ったDNS情報をユーザに提供する。
また別のタイプのシステム再構成攻撃では、Webプロキシーをインストールし、それを通じてユーザのトラフィックを受け渡す。これは別途説明する中間者攻撃の一種である。

データの盗難
悪質なコードがユーザのコンピュータ上で実行されると、コンピュータに保管されている機密情報を直接盗めるようになる。このような情報には、パスワード、ソフトウェアのライセンスキー、重要な電子メール、被害者のコンピュータに保管されているその他のあらゆるデータなどが含まれる。ソーシャル・セキュリティ・ナンバーなどのようにあるパターンに当てはまる情報を探すためにデータを自動的にフィルタにかけることで、かなりの量のセンシティブな情報を取得できる。パーソナル・コンピュータにはより厳重に保護された企業用コンピュータに保管されているのと同じ機密情報が存在することが多いため、データの盗難は、企業スパイ活動を目的としたフィッシングにも広く使われている。雇われスパイに加え、機密メモまたは設計文書が公に漏洩し、経済的損害が生じたりきまりが悪くなることもある。

DNSベース・フィッシング（ファーミング）
DNSベース・フィッシングとは、ここではドメイン・ネームのルックアップ・プロセスの完全性を妨害するあらゆる形のフィッシングを意味するものとして使用する。hostsファイルは正しくはドメイン・ネーム・システムには含まれないものの、これにはhostsファイル・ポイゾニングも含まれる。hostsファイル・ポイゾニングはユーザのコンピュータ上のファイルを変更するものであるため、マルウェアのセクションで説明している。

もう1つのDNSベース・フィッシングの形として、ユーザを間違った位置に誘導するために使用する間違った情報による、ユーザのDNSキャッシュの汚染がある。ユーザのDNSキャッシュの構成が誤っている場合、これは直接行うことができる。また、正規のDNSサーバをハッキングし、ユーザのDNSサーバを不正サーバに変更するシステム再構成攻撃、または構成が誤っている正規のDNSサーバのキャッシュの汚染によって行うこともできる。

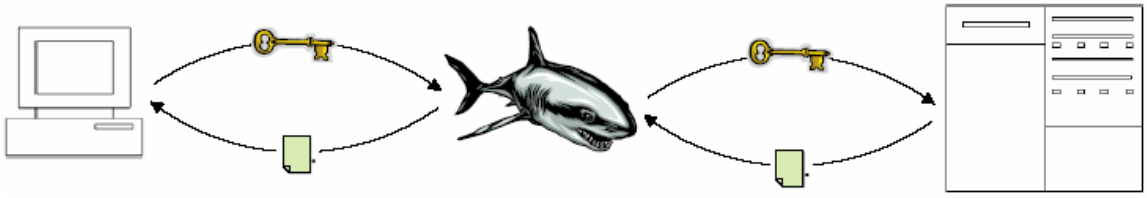
コンテンツインジェクションフィッシング
コンテンツインジェクションフィッシングとは、悪質なコンテンツを正規のサイトに注入することである。悪質なコンテンツは、他のサイトへの転送、ユーザのコンピュータへのマルウェアのインストール、またはフィッシング・サーバへのデータの転送を行うコンテンツのフレームの挿入を行う。
コンテンツインジェクションフィッシングには主に3つのタイプのものがあり、それぞれさまざまなものがある。

- ハッカーがセキュリティの脆弱性を通じてサーバを襲い、正規のコンテンツを悪質なコンテンツで置き換えまたは増補する。
- クロスサイトスクリプティング脆弱性を通じて悪質なコンテンツを挿入する。クロスサイトスクリプティング脆弱性とは、ブログ、電子商取引サイトの商品に関するユーザのレビュー、オークション、掲示板のメッセージ、検索語、Webベースの電子メールなどの外部ソースからのコンテンツに関するプログラミングの弱点のことである。このような外部から提供されるコンテンツは、悪質なスクリプトであったり、サイトのサーバでソフトウェアによって適切にフィルタで除去されていないその他のコンテンツであり、サイトの訪問者のWebブラウザー上で実行される。
- SQLインジェクション脆弱性を通じてサイトで悪質な行為が行われる。データベース・コマンドをリモート・サーバで実行し、情報漏洩を起こす方法である。クロスサイトスクリプティング脆弱性と同様に、SQLインジェクション脆弱性も不適切なフィルタリングによるものである。

クロスサイトスクリプティングとSQLインジェクションは、2つの異なる基本伝搬媒介を通じて伝搬する。1つの伝搬媒介では、悪質なコンテンツが、オークションのリスト、商品のレビュー、Webベースの電子メールなど、正規のWebサーバに保管されたデータへと注入される。もう1つの伝搬媒介では、ユーザがリンクをクリックした際に訪問するURLに悪質なコンテンツが埋め込まれる。これは、画面に表示されるURL、または検索関数の引数などのデータベース・クエリーの一部として使われるURLである場合が多い。

中間者フィッシング

中間者攻撃とは、フィッシャーがユーザと正規のサイトとの間に身を置くフィッシングの形式のことである。正規のサイトのためのメッセージは代わりにフィッシャーに送られ、フィッシャーは価値のある情報を保存してメッセージを正規のサイトに送り、応答をユーザに転送する。中間者攻撃は、漏洩させた認証情報を保管し、もしくは保管せずに、セッション・ハイジャッキングにも使用できる。中間者攻撃では、サイトは適切に機能し、何らかの問題があることを示す外的兆候がないこともあるため、ユーザに検出されにくい。



中間者攻撃

中間者攻撃はさまざまなタイプのフィッシングによって行われる。プロキシー攻撃などの一部のフィッシングの形式は本質的に中間者攻撃である。しかし、中間者攻撃は、DNSベース・フィッシング、詐欺ベース・フィッシングなど、この他の多くのタイプのフィッシングにも使われる。

通常、SSL Webトラフィックは中間者に対し脆弱ではない。SSLで使われるハンドシェークにより、サーバの証明書に記載された相手とセッションが確立され、攻撃者はセッション鍵を取得できない。また、SSLトラフィックはセッション鍵を使用して暗号化されるため、盗聴者にデコードされることもない。プロキシーはこのような暗号化されたトラフィックをトンネリングできる状態になっている。しかし、マルウェア・ベース攻撃によって新しい信頼された証明書をインストールするようシステム構成が変更されることもあり、その場合、中間者はあらゆるSSLで保護されたサイト用に独自に証明書を作成し、トラフィックを復号して機密情報を抽出し、反対側との通信のためにトラフィックを再度暗号化できる。実際には、ユーザはSSLの存在を確認しないことが多いため、中間者攻撃ではSSLをまったく使用しない。

中間者攻撃は、ハードウェア・デバイスによって生成されるワンタイム・パスコードまたは時変化パスコードなどの認証証明書を漏洩させることもある。このような盗まれた認証情報は、有効である限りフィッシャーによって認証に使われる可能性がある。

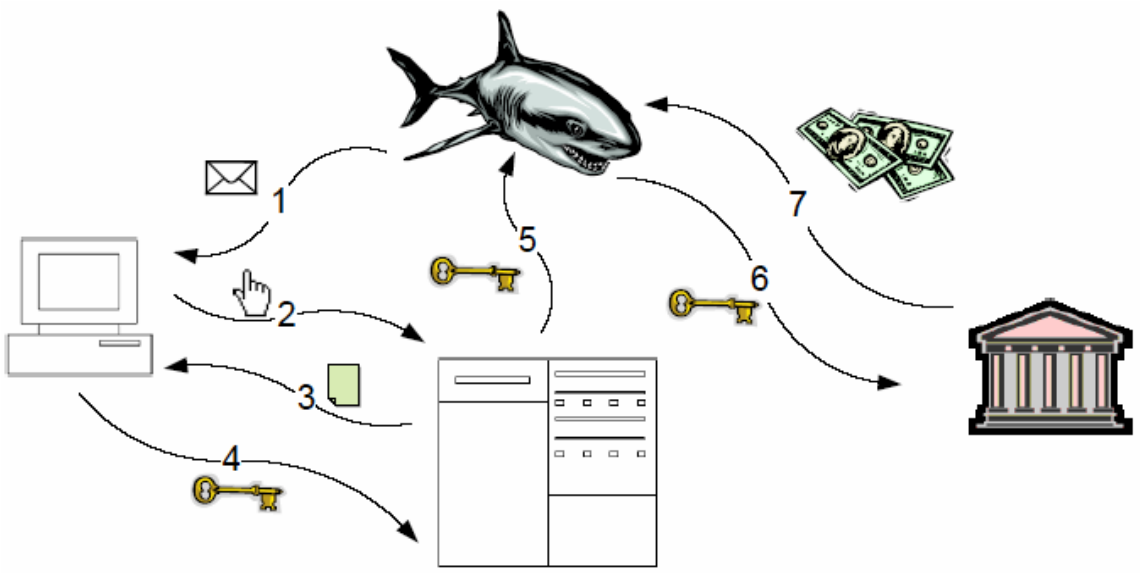
サーチエンジン・フィッシング

フィッシャーによるもう1つのアプローチとして、偽の商品のWebページを作成し、サーチエンジンにおいてそのページを索引付けし、ユーザが注文、登録、または残高の移動などの一環として機密情報を入力するのを待つ方法がある。このようなページでは、やや魅力的すぎる価格で商品を提供していることが多い。

とりわけ偽銀行による詐欺が拡大している。フィッシャーは、実在するどの銀行よりもやや高めの金利を宣伝するページを作成する。被害者たちはサーチエンジン経由でこのオンライン・バンクを発見し、新しい「口座」への「残高の移動」のために自らの銀行口座の認証情報を入力する。欲とは判断力を曇らせる強力な原動力である。「コロラド州ベッドロック」の「フリントストーン・ナショナル・バンク」にさえ銀行の口座番号を提供した被害者もいる。

技術、難点、および対抗策

技術の適用によって、フィッシング攻撃を複数の段階で防ぐことができる。技術的な対抗策については、フィッシング攻撃における下記の情報の流れの中でのステップを基準に説明する。



フィッシング攻撃のステップ
上の図でのフィッシング攻撃における情報の基本的な流れの各ステップは次の通りである。

0. フィッシャーが攻撃の準備をする。類似ドメインを使用した詐欺攻撃などでは、ドメインの登録が必要である。フィッシング・サーバが、フィッシャーが所有するものとして、または（より一般的には）ハッキングまたはマルウェアの被害に遭ったコンピュータが所有するものとして確立される。フィッシング・サーバは、Webベースのインターフェイスによってユーザから、または被害者のコンピュータのマルウェアから情報を受け取るよう構成される。
1. 悪質なペイロードが何らかの伝搬媒介を通じて届く。詐欺ベース・フィッシング攻撃では、ペイロードとは、通常、詐欺電子メールである。マルウェアまたはシステム再構成攻撃では、電子メールの添付、ダウンロードしたソフトウェアの意図せぬコンポーネント、またはセキュリティの脆弱性に対する攻撃によって届く悪質なコードがペイロードになる。DNSポイゾニング攻撃の場合、ペイロードは虚偽のIPアドレス情報である。サーチエンジン・フィッシングの場合、ペイロードは、不正なサイトを参照した検索結果である。クロスサイトスクリプティング攻撃の場合、ペイロードは、攻撃の詳細次第で、正規のサーバに保管される悪質なコードまたは電子メール内のURLに埋め込まれている悪質なコードのいずれかになる。
2. 情報漏洩に対し脆弱となるような行動をユーザがとる。詐欺ベース・フィッシング攻撃では、ユーザがリンクをクリックする。キーロガー攻撃では、ユーザは正規のWebサイトを訪問する。ホスト名のルックアップ攻撃では、ユーザは不正なサイトへと迂回する正規の名前のサイトを訪問する。
3. ユーザが、リモートWebサイトまたはローカルでWeb上のトロイの木馬によって機密情報を要求される。プロンプトを送信するリモートWebサイトは、正規のサイト（キーロガー攻撃の場合）、または悪質なサイト（詐欺ベース攻撃またはDNS攻撃の場合）、または悪質なコードを提供する正規のWebサイト（コンテンツインジェクション攻撃の場合）である。
4. ユーザが、認証情報などの機密情報を、悪質なサーバ、ローカルに実行されている悪質なソフトウェア、または正規の対話を盗聴しているソフトウェアに提供することで漏洩する。
5. 機密情報がフィッシャーに送信される。攻撃の性質次第で、この情報は悪質なサーバまたは被害に遭ったサーバ経由で送信され、キーロガーやWeb上のトロイの木馬などのローカルに実行されているマルウェアの場合は、情報は被害者のPCから送られることもある。
6. 機密情報がユーザになりすますために使われる。
7. 詐欺グループが機密情報を使用して不法な金銭収入を得る、またはその他の方法で詐欺行為を行う。

フィッシングの情報の流れの各ステップについて検証する。各ステップでは、その時点でフィッシングを防ぐために採用できる技術的な対抗策を評価する。

ステップ0：フィッシング攻撃を開始前に防ぐ

場合によっては、フィッシング攻撃を発生前に検出できることもある。また、企業は危機的状況に陥らないうちにフィッシング攻撃への対策を整えることで、対応を改善し、損失を軽減できる。

差し迫った攻撃の検出

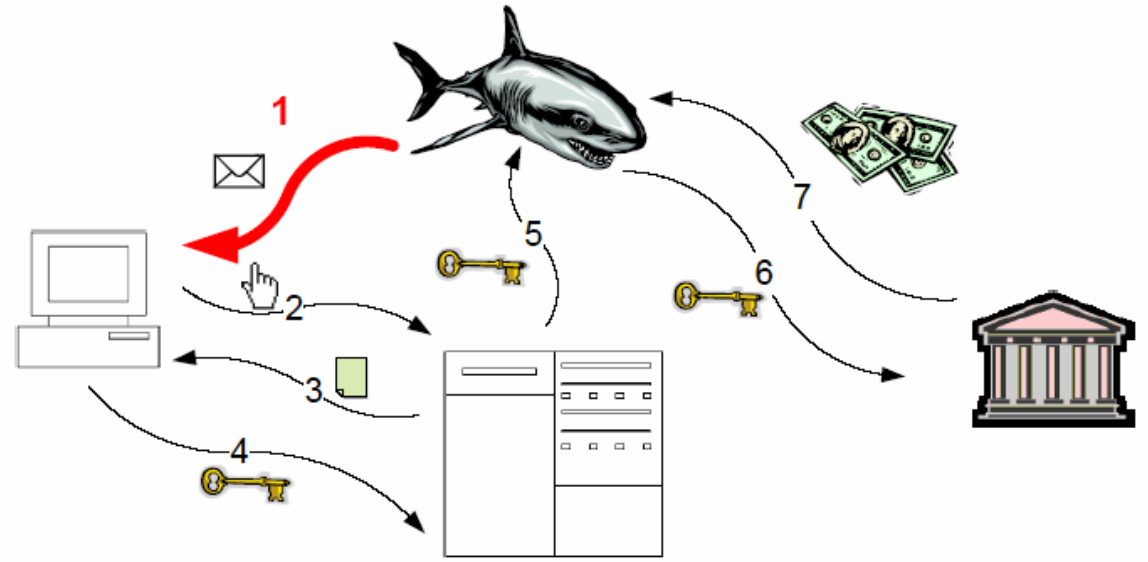
類似ドメインを使用した詐欺攻撃などの何らかのフィッシング攻撃を実施するには、フィッシャーはフィッシング・データを受け取るためのドメインを設定する必要がある。考えられるなりすまし・ドメイン・ネームを対象に先制的にドメイン登録を行えば、最も騙されやすい名前のドメインの空きを減らすこともできる。
考えられるスプーフィング・ドメインは何百万もある可能性があるため、公式なものに見えるドメインとして考えられるものをすべて登録するのは現実的ではない。スプーフ・ドメインの可能性のあるものの登録を検出し、登録者に対処すると同時にサイトでの活動を監視する登録監視サービスを提供する企業もある。
新規のドメイン登録に「保留期間」を設け、付与される前に商標保持者が新規登録に反対できるようにするという案もあった。これは類似ドメインの問題には役立つかもしれないが、フィッシャーがサイトでなりすましができることへの対策にはならない。
フィッシング・サーバを設定する際には、なりすましの対象となる正規のサイトのコピーを保存する場合が多い。正規のサイトのWebログでアクセス・パターンを分析し、フィッシャーのダウンロード活動を検出できることもある。公開Webサイトのページは最終的にはフィッシャーから遠ざけておくことはできないものの、これは攻撃への応答のリードタイムを生み、使われているIPアドレスに基づき早くから分析をしておくことで、攻撃が始まったときに捜査を迅速化できる場合もある。
「ライブ」状態に移る前に、Webを検索して新しいフィッシング・サイトを特定しようと試みるサービスもある。このようなサービスでは、フィッシング・サイトをアクティブになる前に閉鎖することになる場合が多い。しかし、多くの場合、フィッシング・サイトは検索スパイダーからはアクセスできず、収益のほとんどを運用開始の初期に得られるため、長期間アクティブである必要はない。フィッシング・サイトがアクティブである期間は平均で2日以内であり、数時間のみのことも多いにもかかわらず、それでも多大な収益を獲得するのに十分である。
フィッシャーは、フィッシング・サーバをより長期間オンラインにしておくためにさまざまな技術を導入してきた。たとえば、フィッシャーが所有するドメインを使用したフィッシングは、フィッシング・ドメインのDNSサーバで情報を更新することで任意のIPアドレスに誘導できる。フィッシャーはカスタムDNSサーバをセットアップし、それらを交替で使用し、攻撃した多くのマシンにラウンドロビン方式でIPアドレスを提供してきた。あるフィッシング・サーバが撤去されると、そのサーバはローテーションから外され、別の攻撃したマシンが追加される。DNSサーバが撤去されると、登録情報が変更され、別のものと置き換えられる。そのため、ドメインの登録機関を通じて撤去する必要があり、ISPを通じてマシンを撤去するよりも厄介で時間のかかる作業になることがある。一部のフィッシャーは、被害者が回される先の攻撃済みのマシンにロード・バランサーとして機能するようポート・リダイレクターをセットアップし、フィッシング・サーバを撤去と同時に置き換えられるようにしている。

攻撃に備える

フィッシングの標的になる可能性の高い組織は、攻撃が発生する前に攻撃に備えることができる。このような準備によって、攻撃に対する組織の対応を劇的に改善し、損失を大幅に削減できる。準備には次のようなものが含まれる。

- 顧客がなりすまし電子メールを送信できるなりすまし報告用電子メール・アドレスを提供する。これにより、通信が正規のものかについて顧客にフィードバックを提供できると同時に、攻撃が発生した場合には警告を発することもできる。
- 「バウンス(不達)」電子メールの監視。多くのフィッシャーは、標的機関の返信用アドレスを使用して、実在しない電子メール・アドレスも含む大量のリスト宛に電子メールを送る。大量のバウンス電子メールは、フィッシング攻撃が発生している兆候である。
- 電話による問い合わせの件数や、顧客サービスへの質問の性質を監視する。パスワードが変更されたなどの特定のタイプの問い合わせの急増は、フィッシング攻撃の兆候である。
- 異常な数のログイン、パスワードの変更、送金、引き出しなど、異常な動きがないか口座の動きを監視する。
- 機関の企業ロゴや図を含む画像の使用を監視する。フィッシャーは標的企業を使用して顧客を騙すための図をホストする。これは、画像の「参照者」が空または異例のものであることによりWebサーバ上で検出できることがある。
- 「ハニーポット」を設置し、同機関からとする電子メールが届くか監視する。

これらの多くのサービスを実行できる請負業者もある。標的機関が手続き上の対抗策をとったり、捜査当局と捜査を開始したり、攻撃にタイムリーに対応できるようスタッフを増やせるため、攻撃が発生したことを知ることは有用である。



フィッシングにおける情報の流れ、ステップ1

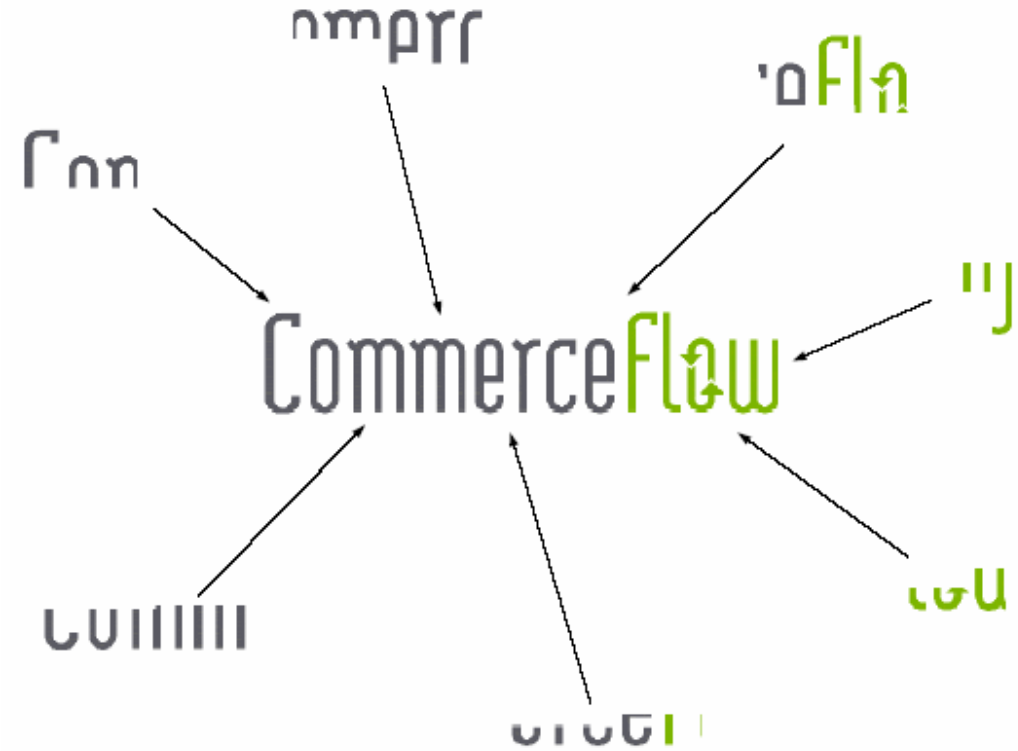
ステップ1：フィッシングのペイロードの配信を防ぐ

ひとたびフィッシング攻撃が始まると、電子メールやセキュリティ攻撃などのフィッシングのペイロードがユーザに届かないようにすることが、フィッシング攻撃を防ぐ最初の機会となる。これはフィッシングの情報の流れのステップ1の妨害を意味する。

ステップ1への対抗策：フィルタリング

スパム対策を目的とした電子メールのフィルタは、フィッシング対策にも有効な場合が多い。署名ベースのスパム防止フィルタは、特定の既知のフィッシング・メッセージを識別し、ユーザに届かないようにするために構成できる。統計またはヒューリスティックによるスパム防止は部分的にフィッシングに効果がある場合もあるが、

フィッシング・メッセージが正規メッセージに似ている場合、フィルタがフィッシングの電子メールを識別するのに足るだけセンシティブに構成されていると、正規の電子メールを誤ってブロックしてしまう危険性がある。効果的な詐欺ベース・フィッシングの電子メールや Web サイトは、まねようとしている機関と同じ外観でなければならない。カラー・スキームや画像は標的機関をまねしたものになる。そこで重要な側面となるのが企業ロゴの使用である。これにより、フィッシングの電子メールに騙される可能性が劇的に高まるからである。
対抗策の 1 つとして、電子メール内の不正なロゴの検出が考えられる。簡単な画像の比較に対抗してフィッシャーが採用し得る対抗策は多数ある。たとえば、小さなタイル状の画像を 1 つの大きな画像として表示したり、透明な画像を積み上げて複合画像を作成したりする。



複合ロゴタイプ・レンダリング

フィッシャーにこのような回避策をとらせないために、画像は分析前に完全にレンダリングする必要がある。全面的にレンダリングされた電子メールなど、大きな画像の中の変更された可能性のある商標またはその他の登録画像をいかに認識するかは、今後研究が進められる分野である。同様のアプローチをWebサイトに適用すれば、ユーザがリンクをクリックした際に役立つ可能性がある。

ステップ1への対抗策：電子メールの認証
フィッシングの電子メールは、信頼できるソースからだとされていることが多い。これには主に2つの方法がある。

- 返信用アドレスの偽造
- 類似ドメインの登録（たとえば、実際のドメインが「commerceflow.com」の企業をスプーフするための「commerceflow-security.com」）と、そのドメイン・ネームからの電子メールの送信

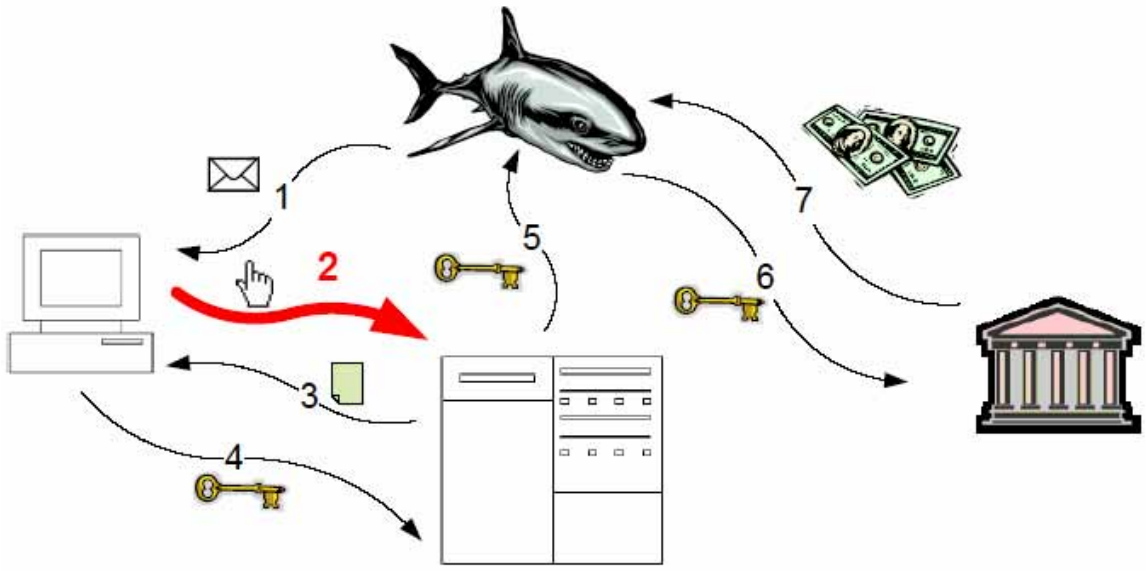
メッセージ認証技術は、フィッシング対策アプリケーションにおいて大いに期待されている。一般的に、メッセージ認証は、電子メールが送信者とされている相手から実際に送信されたものであることを保証する。幅広く展

開されれば、電子メール認証は返信用アドレスの偽造を防ぎ、不審な返信用アドレスの露呈、または公式なものに見えるドメイン・ネームの登録のいずれかをフィッシャーに強いる可能性がある。この利点としては、返信用アドレスが偽造されたアドレスよりも騙されにくいものになること、ドメイン登録がフィッシング攻撃の前に検出できること、フィッシャーをドメイン登録を通じて追跡できることなどがある。
電子メール認証技術は多数提案されている。Sender-IDとSPFは、DNSレコードを確認し、送信を行うメール転送エージェント（MTA）のIPアドレスが送信者のドメインからのメッセージの送信を許可されているかを判断することで、返信用アドレスの偽造を防ぐ。Domain KeysとInternet Identified Emailも、DNSレコードを通じて検証できるドメイン・レベルでの暗号署名を使用して、同様の認証を提供する。MTAの認可によるアプローチには実装が容易という利点があるのに対し、暗号アプローチではエンド・ツー・エンドの認証が提供される。
Sender-IDとSPFは現在IETF Experimental Standard（実験的標準）になっており、一方、MASSのワーキング・グループはDomain KeysとInternet Identified Emailの合併に取り組んでいる。この他にも、否認可能な暗号署名による電子メールや、権限者によって認定された認証トークンを受信者が解釈できるような権限ベースの電子メール認証のための提案などがある。
電子メール認証のためのもう1つのアプローチとして、送信者が受信者に電子メールを送信する権限の証明を提示する方法がある。このような方式には、送信者固有またはポリシー・ベースの電子メール・アドレスの自動生成と使用、メッセージの受信者によって発行され、送信者に送信を許可するトークンまたは証明書の使用などがある。このようなアプローチでは、追加のユーザ・インターフェイス（送信者固有の電子メール・アドレスを生成する場合）またはインフラストラクチャー（トークンの生成および／または証明書の署名および配布を行う場合）のいずれかが必要になる。
何らかの形の軽量なメッセージ認証が、将来フィッシング対策に非常に役立つ可能性がある。この潜在的な価値を実現するためには、認証されていないメッセージを即座に削除するか、またはその他の方法で不利に扱えるよう、電子メール認証技術が十分に広まり、Sender-IDなどのMTAの認可方式におけるメールの転送機能の使用に関するセキュリティの問題を解決する必要がある。
電子メールの暗号署名（S/MIME署名など）は、短期的には前向きで漸進的なステップであり、長期的に幅広く展開されれば効果的な措置となる。署名は、クライアントまたはゲートウェイのいずれかで実行できる。しかし、現在の電子メール・クライアントでは、電子メールが署名されているか否かが表示されるだけである。典型的なユーザは、電子メールが署名されていないことに気付かず、フィッシング攻撃を防げない可能性が高い。署名は、たとえばユーザが署名されていない電子メールのリンクにアクセスしようとした際に警告するなど、署名されていない電子メールの機能が制限されればより有効になる。しかし、これは、今日電子メール・メッセージの大半を占める署名されていないメッセージにとって負担となる。署名された電子メールが臨界点に達すれば、このような措置も実行可能になる可能性がある。

ステップ1への対抗策：セキュア・パッチ

マルウェアが関与するフィッシング攻撃は、セキュリティの脆弱性につけ込んでインストールされることが多い。パッチを当てていないオペレーティング・システムまたはブラウザーを実行しているユーザは、ブラウジングまたは単にインターネットに接続しているだけでもマルウェアに感染するリスクがある。
脆弱性につけ込む行為のほぼすべては、既知の脆弱性を対象にしたものである。あらかじめ知られていない脆弱性を対象とした「ゼロ・デイ」攻撃は、実際には非常にまれである。したがって、ファイアウォールの後ろに完全にパッチされたコンピュータを置くことが、脆弱性への攻撃によるマルウェアのインストールに対する最善の防御策である。
パッチは大きいことが多く、世界的な顧客ベースに配布するには長い時間を要することが多い。また、ユーザやIT部門はパッチを直ちに適用しないことも多い。パッチを適用する前に、バグが多く、コンピュータを不安定にさせる可能性のある最初のパッチが修正されるのを待つのがしばしば賢明であるという調査結果もある。
しかし、パッチの発表と配布は、パッチの対象となるセキュリティの脆弱性について犯罪者に情報を提供することを意味する。説明をあいまいにしても、パッチを分解し、それが置き換えることになるコードと比較できる。

新たに攻撃できる脆弱性が見つかると、マルウェアによる脆弱性の攻撃は事前に構築されたコンポーネントによって直ちに作成できる。パッチがリリースされてから悪質な攻撃が登場するまでの所要時間は、現在では3日未満、場合によってはわずか数時間となっている。この短い時間の後、ほとんどのコンピュータは依然として感染しやすい状態にある。
脆弱性に関する情報を漏らすことなく迅速にパッチを配布し、適用するための有望な提案の1つに、特定の脆弱性に関する集中的なセキュリティ・パッチを、パッチごとに異なる対称鍵を使用して暗号化して配布するというものがある。鍵はベンダーによって内密に保管される。パッチは暗号化された状態では適用できないが、脆弱性に関する情報を犯罪者に漏らすことなくすべての脆弱なコンピュータに配布することは可能である。パスによって修正された実際の脆弱性への攻撃が検出されると、その特定のパッチの複合鍵を直ちにインターネットですべてのコンピュータに配布し、自動的にパッチをインストールできる。脆弱性への攻撃は、パッチが修正する脆弱性への攻撃の試行を検出するハニーポット・マシンで実行されているパッチのバージョンによって検出できる。



フィッシングにおける情報の流れ、ステップ2

ステップ2：ユーザの行動の防止または妨害

フィッシングにおける情報の流れのステップ2は、ユーザを自らの機密情報が漏洩する可能性のある場所に移らせるユーザの行動に関するものである。このプロセスを妨害する対抗策にはいくつかのものがある。

ステップ2への対抗策：教育
ステップ2の対抗策として最も広く展開されているのは、ユーザ・ベースの「教育」である。具体的には、電子メールのリンクをクリックしない、SSLが使われていることを確認する、情報を提供する前にドメイン・ネームが正しいか確認するなどの手法についてユーザに指導する。
このような教育は効果的ではなく、フィッシング・メッセージへの回答率は正規の商売のための電子メールと同程度である。このような教育が効果的でなかった理由は少なくとも4つある。

- 電子メールの発信元、ページの場所、SSLの存在などの、ユーザに通常提示される情報がなりすまされる可能性がある。したがって、いかに教育されていようと、正規のメッセージとフィッシング攻撃の識別において、ユーザを頼りにすることには無理がある。

- SSLが使われていることの確認やドメイン・ネームの確認などの行動は、ユーザの通常のサイトとの対話と直接関係がないため、スキップされることが多い。
- 金融機関は、フィッシング・メッセージを正規の通信と区別するために広めてきたガイドラインから大幅に逸れてきたため、広めてきた教育のためのメッセージがむしばまれている。とりわけ、多くの金融機関は、フィッシャーが使うような意外なドメイン・ネームを使用したり、ログイン・ページでユーザが確認できるような形でSSLを使用しなかったり、電子メール通信にクリックできるリンクを含めたりしている。
- ユーザは欠陥や障害には慣れており、フィッシング関連の動きの解釈方法をよく知らないことが多い。ユーザはフィッシングの兆候をソフトウェアのバグやその他のエラーによるものだと正当化することが多い。

顧客が正規のサイトとの特定の対話のモードに慣れ、慣習から逸れたサイトを疑いやすくなるため、フィッシャーとは異なる一貫した慣習に従うことが、顧客を教育するためのおそらく最も効果的な方法である。金融機関は次のような慣習に従うことで、このような教育を促進できる。

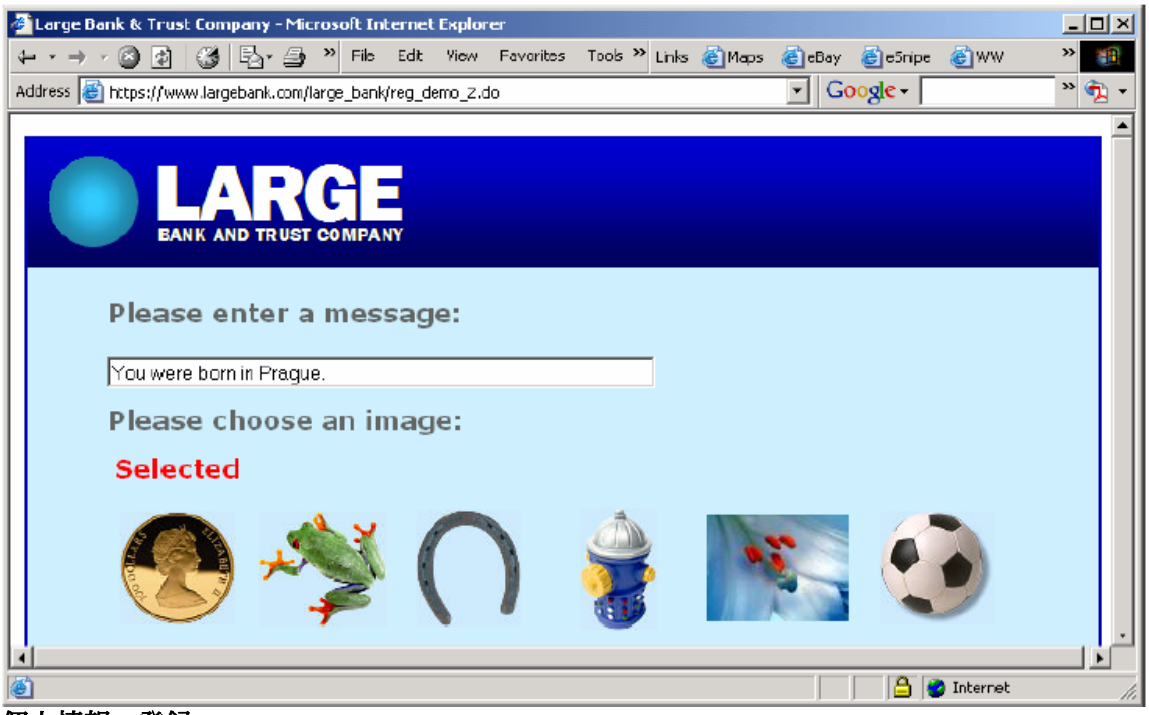
- クリック可能なリンクが実際にはマーケティングの貴重な形態となっている場合、クリック可能なリンクは決して使わないなどと顧客に言わない
- リンクにアクセスしない場合にマイナスの結果が生じると警告するような電子メールでは、「行動要請」は決して使わない
- 電子メール認証技術を使用する
- リンクを使用する場合、分かりやすい名前のリンクを使用する（虚偽的な名前のリンクは使わない）
- ログインには予想されるドメイン・ネームを必ず使用する
- ログイン・ページおよびその他のすべてのページで必ずSSLを使用する

ステップ2への対抗策：個人情報の使用

フィッシング・メッセージに騙されにくくする簡単な方法として、すべての正規の通信に個人情報を含める方法がある。たとえば、commerceflow.comからのすべての電子メールがユーザの名前で始まり、commerceflow.comがこの慣習についてユーザに教育していれば、ユーザの名前を含まない電子メールは疑わしいということになる。複数の事業部門間での連携の難しさ、提携企業によるマーケティング・プログラム、外部サービスに電子メールをアウトソーシングする慣習の拡大などにより、この慣習の導入は複雑なものになる可能性があるが、効果的な措置である。情報がパートナーと共有されたり、安全でないチャネル経由で送られることが多いため、使用する個人情報はいずれもセンシティブでないものにすべきである。

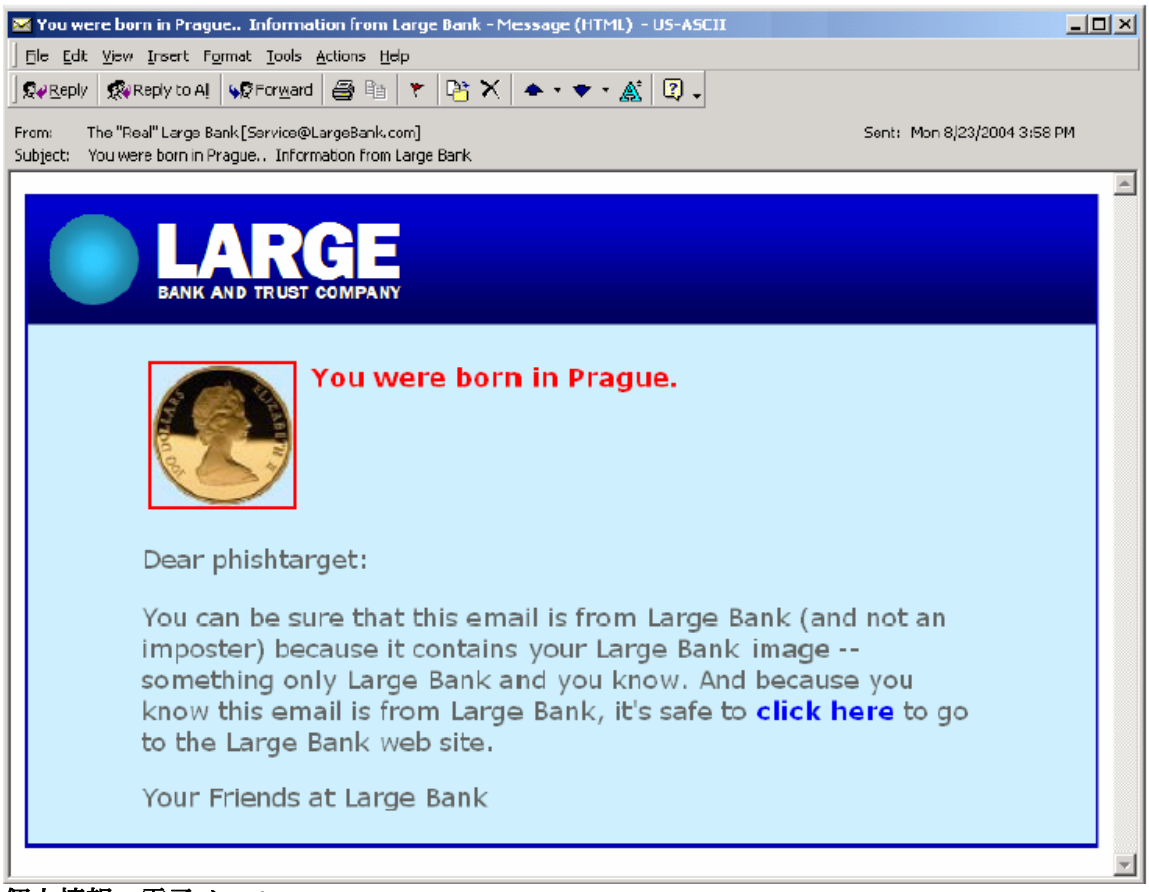
静的な識別情報以外にも、ユーザが使用を求めたテキストなどのより高度な個人情報も含むことができる。これによりユーザは、希望する情報が含まれていることを容易に確認できる。

個別の画像もメッセージの送信に使用できる。たとえば、ユーザがアカウント情報の作成または更新を行うと、そのユーザはその後個人情報として使われるテキストおよび／またはグラフィック情報の入力を許可（または要求）される。この例では、Large Bank and Trust Companyの顧客が個別テキストとして「You were born in Prague」とタイプし、カナダの1セント銅貨の画像を選択またはアップロードしている。



個人情報：登録

Large Bank and Trust Companyからのこれ以降の電子メールには、次のようにこの個人情報が含まれるようになる。



個人情報：電子メール

フィッシャーは、ユーザがどのような個人情報を選択したか知らないため、詐欺メールを偽造できなくなる。Webサイトでも、ユーザがユーザ名を入力した後、パスワードを入力する前に、同様のアプローチを使用できる。しかし、Webサイトではまず他の手段でユーザを認証する必要がある。中間者攻撃を防ぐために、二要素認証などの追加の認証を使用し、ユーザとコンピュータが正規のものであることを確認してから個人情報を表示すべきである。ユーザが確認できたら、個人用のテキストおよび／またはグラフィックが表示され、ユーザは個人情報が正しいことを確認してからパスワード情報を入力する。

このタイプのアプローチはユーザの教育に多少依存するものの、ロック・アイコンのチェック、署名のない電子メールの不信扱い、またはURLのタイプなどに関する忠告とは異なり、ユーザとメッセージまたはサイトとの間の対話に構造上の違いがある。これらの構造上の違いによって、ユーザはフィッシング攻撃と正規の対話との違いを見分けやすくなる可能性がある。

ステップ2への対抗策：詐欺コンテンツの正規表示

詐欺ベース・フィッシング電子メールでは、ユーザにリンクをクリックしてWebサイトを訪問するよう求めるものが多い。フィッシャーのWebサイトは、通常、正規の名前を持たないため、リンクの実際の宛先は偽装されていることが多い（類似ドメインを使用した攻撃、DNSのネーム解決への攻撃によるフィッシングサイトへの到達、国際化ドメイン名による同形異義語攻撃などはこの法則の例外である）。

現在では、コンテンツの作成者の指定方法に関係なくリンクを表示できる。これにより、フィッシングの電子メールで詐欺リンクが作りやすくなっている。フィッシャーはリンクの真の宛先を見えなくするために、多くの技術を採用している。たとえば次のようなものがある。

誤解を招くような名前のリンク－http://security.commerceflow.comと表示されているリンクが実際にはhttp://phisher.comに結び付いている。
覆い隠されたリンク－URLにユーザ名とパスワードが組み込まれている。これにより、リンクの実際の宛先を「覆い隠す」ことができる。たとえば、
http://security.commerceflow.com@phisher.comというURLは実際にはhttp://phisher.comに結び付いている。
リダイレクトされるリンク－あるURLへの参照を別のURLへと変換する「リダイレクト」はWebプログラミングで使われることが多い。標的機関の不注意なプログラマーが任意の場所へのリダイレクトに使用できる「オープンなリダイレクト」をアクセス可能な状態にしたままにすると、フィッシャーによってフィッシング・サイトにリダイレクトする正規のようなURLの提供に使われる可能性がある。
偽装リンク－URLにはURLの意味を隠すエンコードされた文字が含まれることがある。これは、たとえば覆い隠されたリンクやリダイレクトされるリンクのターゲットを見えなくするためなど、他のタイプのリンクと組み合わせて使われることが多い。
プログラムによって見えなくされたリンク－スクリプトの実行が許可されている場合、ユーザがリンクの宛先を見るためにマウスをリンクにかざした際にJavascriptによってステータス・テキストを変更できる。
マップ・リンク－正規のようなURLを参照するHTML「イメージ・マップ」内にリンクを含めることができる。しかし、イメージ・マップ内をクリックした場合にブラウザーが誘導される実際の場所は、ユーザには表示されない。
同形異義語URL－リンクのURLにIDN（国際化ドメイン名）の同形異義語、すなわち通常の文字と同じに表示されるものの実際には異なる文字（キリル文字など、異なるアルファベットの文字が一般的）を使用できる。現在では、これは標準外の構成のブラウザーで問題となることがほとんどである。

電子メール・クライアントまたはブラウザーへの実装への対抗策の1つとして、ユーザに疑わしいものとして明確に示せる予測可能な方法で潜在的詐欺コンテンツをレンダリングすることが考えられる。たとえば、次のHTMLフラグメントとその典型的なレンダリングの例について考えてみる。

```
<CENTER><H1>Suspicious URLs</H1></center>
<P>To go to a surprising place via a cloaked URL, click on
<A HREF="http://security.commerceflow.com@phisher.com">this link.</A>
<P>To go to a surprising place via a cloaked URL with a password, click on
<A HREF="http://security.commerceflow.com:password@phisher.com">this
link.</A>
<P>To go to a surprising place via an open redirect, click on
<A HREF="http://redirect.legitimatesite.com?url=phisher.com">this link.</A>
<P>To go to a surprising place via misleading link, click on
<A HREF="http://phisher.com">http://security.commerceflow.com.</A>
```

詐欺リンクを含むHTMLコンテンツ

詐欺リンクを含むHTMLコンテンツのブラウザ表示

ユーザは、クリックする前にステータス・バーのURLを見ても、クリックするリンクの実際の宛先を理解できないことがある。リンクのぼかしが使われている場合、特にこれが当てはまる。とりわけステータス・バーのスプーフィングへの対抗策（たとえば、URLの重要な部分を必ず表示し、URLが表示される際にスクリプトでステータス・バーを変更できないようにする）と組み合わせた場合、電子メール・クライアントまたはブラウザーの拡張機能によって、混乱を招く可能性のあるURLの宛先をアイコンで示すことで、ユーザのためにこの状況を明確化できる。上記のページは次のようにより多くの情報を提供するようレンダリングすることもできる。

詐欺リンクを含むHTMLコンテンツのレンダリング、正規表示

ステップ2への対抗策：誘導の妨害
ユーザが、覆い隠されたリンク、ぼかされたリンク、マップされたリンク、または誤解を招くような名前のリンクなどの疑わしいリンクをクリックした際に、警告メッセージを示し、リンクのトラバースの潜在的な危険についてユーザに忠告することもできる。情報は率直に示すべきであるが、単純化する必要はない。ユーザが十分な情報に基づく決定を行えるよう、リバースDNSやWHOISルックアップなどのソースからのデータを有効に含める。

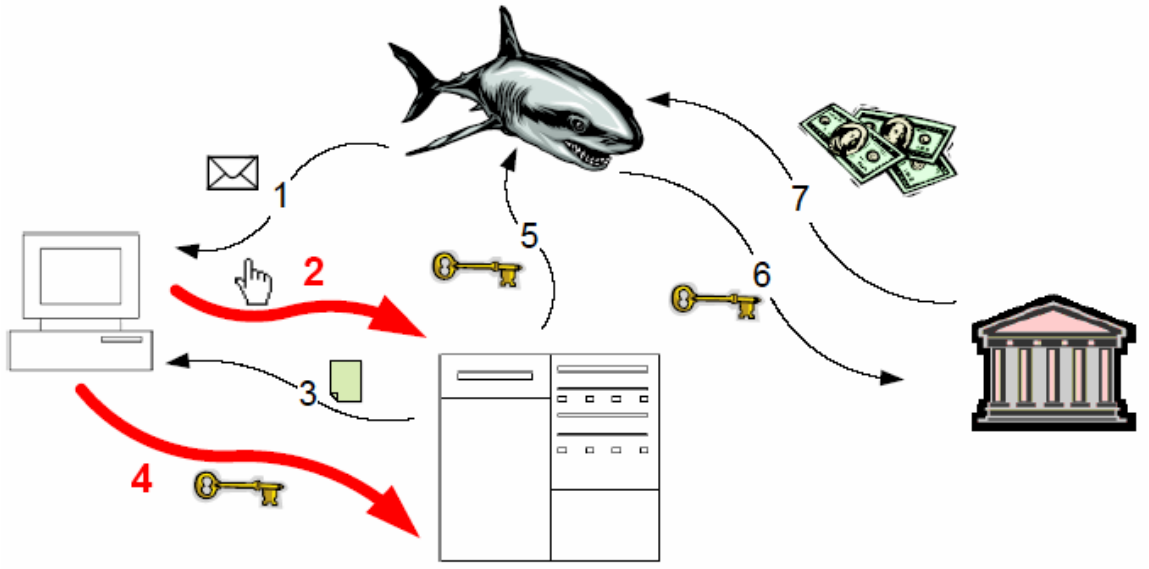
安全でないリンク・トラバーサルに関する警告メッセージ

情報を提供するような警告では、疑わしい性質の正規のリンクを許可する一方で、ユーザが適切な行動を決定するために必要な情報についてリスク評価を提供できるメリットがある。
調査によれば、このような情報は、ある動作を実現するためにユーザが実行すべき「重大な動作シーケンス」の一部になっていた方が、ユーザによってより確実に評価される。したがって、意図する選択肢をユーザがいくつかの選択肢から選択する必要のある対話の方が効果的である。

ステップ2への対抗策：一貫性のないDNS情報の検出
DNSベース・フィッシング攻撃は、ホストに誤ったDNS情報を提供できることに依存した攻撃である。このようなフィッシング攻撃は、ユーザが過去に関係を持っているサイトを訪問することが頼りのため、悪質な情報を検出できる可能性がある。過去のルックアップについて、DNSキャッシュとは別にレコードを保管できる。名前解決が別の結果をもたらした場合、信頼できるとされている外部ソースに正式な答えを求める。
また、数値IPアドレスを使用した攻撃（攻撃された自宅のマシン上のサーバのフィッシングにおいて一般的なシナリオ）において、対応するDNSルックアップが実行されていないIPアドレスへのアクセスを検出するにも効果

的な可能性がある。

ステップ2への対抗策：参照された画像の変更
フィッシャーは、標的企業によって制御されているサイト上の画像にアクセスし、正規の電子メールまたはWebサイトのルック&フィールをまねることがある。標的機関は、ある画像に対して届く要求の参照者フィールドを調べることでこの活動を検出できる。ひとたびフィッシング攻撃が始まれば、Webサーバはその画像の提供を拒否するか、またはフィッシング攻撃に関する情報提供のためのメッセージを表示した画像でその画像を置き換えることができる。
この対抗策は、電子メールから画像が参照されるようなステップ2に当てはまる。また、ステップ3で送信されたWebページが正規のサイトの画像を参照するステップ4にも当てはまる。自ら画像をホストしているフィッシャーには簡単に回避されるものの、今日まで多くの攻撃に有効となっている。



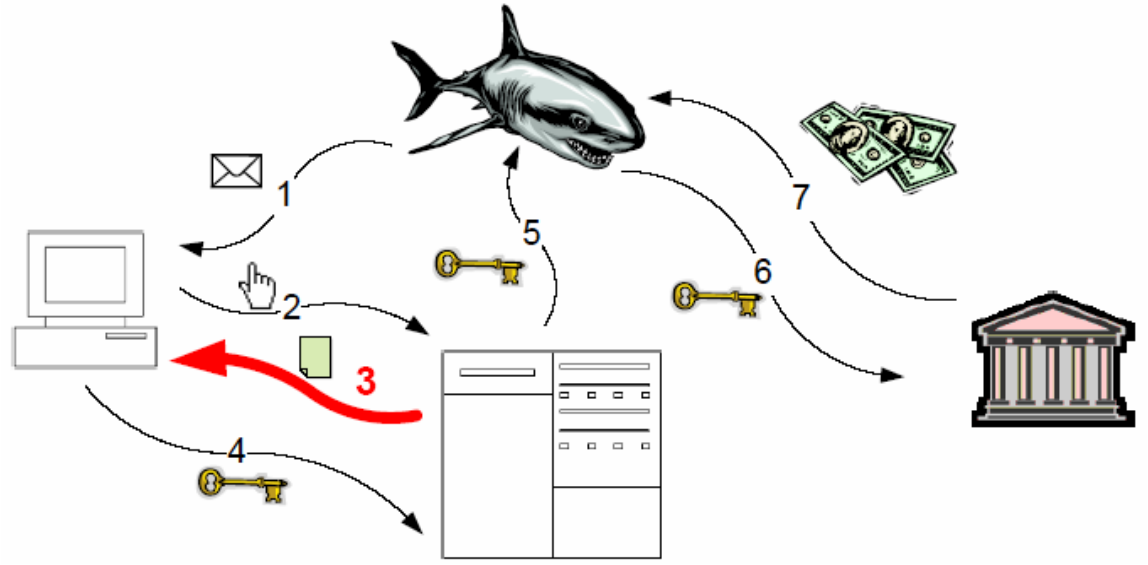
フィッシングにおける情報の流れ、ステップ2および4

ステップ2および4：誘導とデータ漏洩を防ぐ

フィッシングにおける情報の流れのステップ2は、ユーザをフィッシング攻撃に対して脆弱にするフィッシングサイトへのナビゲーションなどのユーザの行動である。ステップ4では、機密情報が漏洩する。

ステップ2および4への対抗策：アプリケーション間のデータ共有の増加
将来取り組みが進められる分野に、スパム・フィルタ、電子メール・クライアント、およびブラウザー間での情報共有の増加によるフィッシング対策がある。重要な情報はこれらのアプリケーションの境界で失われることが多い。スパム・フィルタがあるメッセージを不法扱いにしたとしても、拒否されるしきい値を下回っている限り、電子メール・クライアントでは信頼できる企業からの署名された電子メールと対等に扱われる。
メッセージの処理中に集められた情報もフィッシングの阻止に役立つ。電子メールが疑わしい場合、ユーザのホワイトリストの送信者またはBonded Sender Program（合法メール送信者の認定サービス）のメンバーからの認証されたメッセージとは別に扱うことができる。
疑わしいメッセージの視覚的な表示、スクリプトの不許可、リンクの真の名前の表示、フォームの不許可などが可能である。この対抗策は、フィッシングの情報の流れのステップ2に対応するものである。
同様に、ひとたびユーザが電子メール・メッセージ内のリンクをクリックすると、メッセージの信頼性に関する

情報が、トラバーサルを許可すべきかの判断に役立つ。リンクがトラバースされたら、信頼性が低めのメッセージで示されているリンクの機能（スクリプトの記述、フォームの送信、リンクの表示など）を制限し、フィッシングの情報の流れのステップ4の発生を防げる。
スパム・フィルタ、電子メール・クライアント、およびブラウザー間のインターフェイスは、信頼性に関する情報の送信を許可し、多くの新しいフィッシング対策法を可能にする。



フィッシングにおける情報の流れ、ステップ3

ステップ3：プロンプトの送信を防ぐ

フィッシングにおける情報の流れのステップ3は、不正な相手への機密情報の漏洩につながるユーザへのプロンプトである。ステップ3への対抗策ではこのプロンプトを攻撃し、プロンプトが届くのを防ぐか、または悪意のある相手に対し漏洩する情報が含まれるのを防ぐ。

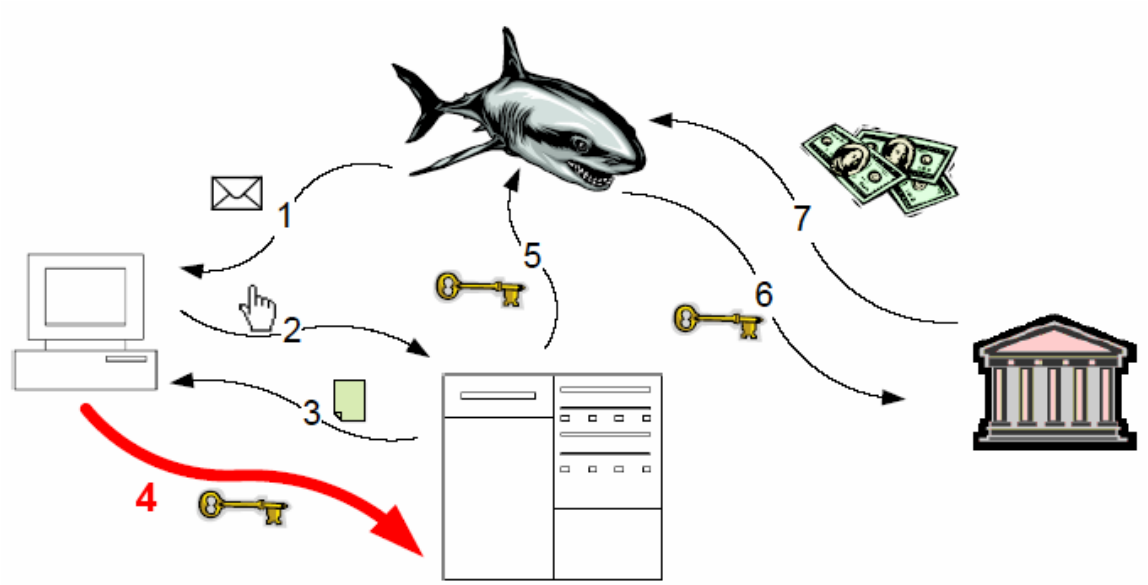
ステップ3への対抗策：クロスサイトスクリプティングの除去

クロスサイトスクリプティングは、2つある方法のいずれかによって行われるコンテンツインジェクション攻撃である。フィッシャーはフィッシングの流れのステップ1で、顧客によるレビュー、オークション、Webベース電子メール、または同様のコンテンツの一部として正規のサーバに保管することで、悪質なコンテンツを正規のWebページに注入できる。フィッシャーは、検索結果とともに表示されるスクリプトを検索クエリーに組み込むことで、ステップ1のユーザへの電子メールに含まれるURLに悪質なコードを含めることもできる。このようなURLに組み込まれたコンテンツは、ステップ2でユーザから正規のサーバに送られ、ステップ3で機密情報を求めるプロンプトの一部として戻される。
クロスサイトスクリプトは、ひとたび注入されると、ユーザがターゲットとした機関と通信していると信じるようホスト・サイトの要素を変更する。ユーザは実際にはフィッシャーに機密情報を提供することになる。
クロスサイトスクリプティングによってフィッシングの情報の流れのステップ3を妨害するには、画面に一度でも表示されたユーザ・データはフィルタにかけ、スクリプトをすべて除去する必要がある。悪意のある関係者は、Webベース電子メールのページの日付フィールドなど、予期せぬ場所にクロスサイトスクリプティング攻撃を組み込んできた。禁じられたスクリプト・要素を「締め出し」フィルタにかけて除去するのではなく、ユーザが提供したデータを「受け入れ」フィルタによって解析し、許可されたデータ・要素のみを受け入れるべきである。
クロスサイトスクリプトまたはその他のHTML要素はWebサイトの外観を損ねたり、変更したり、あるいは識別

情報の盗難とは関係のないその他の損害を招く可能性があるため、このようなフィルタリングは、さまざまな理由により適切なWebサイトの設計の一要素となっている。

ステップ3への対抗策：注入されたスクリプトの無効化
クロスサイトスクリプティングを導入する方法には多数のものがある。適切なフィルタを記述することは困難であり、コストも高く、エラーも発生しやすい。また、フィルタにかけられるべきコンテンツが不注意で見落とされることも多い。
ブラウザーの拡張により、将来クロスサイトスクリプティングに対する保護が提供される可能性がある。HTMLに含めることのできる<noscript>などの新しいタグが導入されれば、スクリプティングが一切行えない領域や、特定の機能が禁止された領域を定義できる。ブラウザーはこの動作を保証でき、十分なフィルタリングの採用は、検索結果またはオークションのリストなどのユーザが提供したテキストを適切な<noscript>および</noscript>タグで囲むだけというように簡単にできるようになる。
悪意のある関係者が有効な</noscript>タグを使用し、クロスサイトスクリプトを挿入することのないよう、<noscript>タグと</noscript>タグで一致する必要のある動的に生成されるランダム鍵を使用すべきである。このような鍵は、Webコンテンツのオーサリング・ツールによって自動的に生成できる。ユーザが提供したコンテンツはどの乱数が鍵に使われたか知るすべがないため、スクリプティングの特権を再度有効にするのに必要な情報を欠くことになる。たとえば次のようになる。

[サイトが提供したHTMLとスクリプト]
<noscript key=”432097u5iowhe”>
[スクリプト／機能が無効になっている、ユーザが提供したHTML]
</noscript key=”432097u5iowhe”>
[サイトが提供したHTMLとスクリプト]



フィッシングにおける情報の流れ、ステップ4

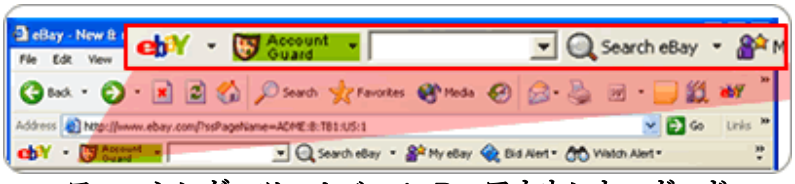
ステップ4：機密情報の送信を防ぐ
フィッシング攻撃を妨害できるもう1つの点は、ユーザがフィッシング情報の流れのステップ4で機密情報の送信

を試みるときである。詐欺フィッシングサイトが不正なものであることを対象となっている被害者に明らかにしたり、または情報の流れを妨害または変更し、機密情報をフィッシャーに利用できないようにしたり無駄なものにすることができれば、攻撃を阻止できる。
典型的な詐欺ベース・フィッシング攻撃では、フィッシャーはさまざまな技術を使用して、ユーザを正規のサイトにいると騙し続けようとする。これにも急速に変化する多数の技術が関与している。ブラウザーの場所についてユーザを騙す方法の1つに、詐欺リンクの使用がある。もう1つは、詐欺情報がURLバーに表示されるようにする方法である。たとえば、フィッシャーは、枠なしウィンドウ(borderless window)をポップアップさせてURLバーの実際のコンテンツを覆い隠し、ユーザがブラウザーのウィンドウを動かすと詐欺ウィンドウも動くようなJavascriptプログラムを作成した。これらのJavascriptプログラムは、ユーザが履歴ボックスをクリックすると、ウィンドウの履歴をまねる。
ブラウザーのロック・アイコンを見ることで、サイトへの接続が安全か（すなわちSSLを使用しているか）を判断することはできない。ロック・アイコンが信用できない理由はいくつかある。

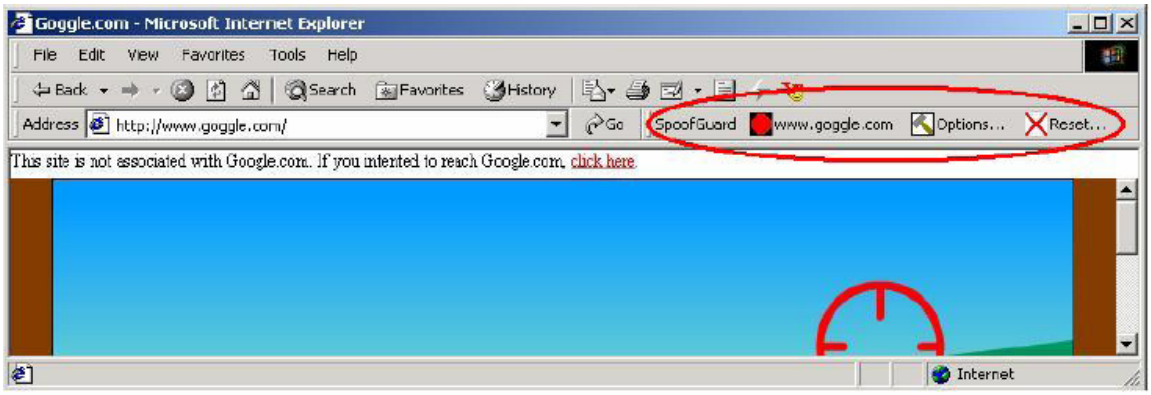
- ロック・アイコン単独では、サイトが証明書を持っているという意味しかなく、表示されている（詐欺）URLと証明書が一致することを確認するものではない。ユーザはロック・アイコンをクリックし、その意味を判断する必要があるが、これを行うユーザはわずかである。
- 特定の暗号化の設定により、自己署名証明書（有効な認証局によって発行されていない証明書）を使用してロック・アイコンを表示させることのできるブラウザーもある。
- URLバーの改竄に使われるのと同じ技術によって、ロック・アイコンをブラウザーの上に重ねることができる。この技法では、正当なものかを確認するためにユーザがロック・アイコンをクリックした際に、本物に見える証明書データを提示することもできる。

ブラウザー技術は絶えず更新され最近のフィッシング戦術に対応しているが、ブラウザーは、正規のWebサイトの設計者のニーズを満たすだけの十分な機能性と柔軟性を提供する必要のある、大規模で複雑なプログラムである。フィッシング技術に断片的に対応するだけで詐欺フィッシングの出現を完全に阻止できる可能性は非常に低い。

ステップ4への対抗策：フィッシング防止ツールバー
フィッシングサイトを特定し、ユーザに警告を試みるブラウザーのツールバーが提供されている。これらは研究プロジェクトと技術サプライヤーの双方から提供されている。フィッシング防止ツールバーは、既知のフィッシングサイトのデータベース、サイトのURLの分析、サイトの画像の分析、サイトのテキストの分析、フィッシングサイトを検出するためのさまざまなヒューリスティックなど、さまざまな技術によって安全でないサイトを見分ける。通常、サイトの安全性を示す信号機などによって視覚的に印を表示する。この場合、青は既知の良いサイト、黄色は知られていないサイト、赤は疑わしいサイトまたは既知の悪いサイトである。たとえば次のように表示される。



フィッシング・ツールバー：eBayアカウント・ガード
この例では、ユーザはeBayのサイトを表示しているため、インジケーターは青である。もう1つのツールバーの例では、ユーザは虚偽的な名前のサイトを訪問しており、危険を表示するとともに、ユーザが訪問していると信じている可能性が最も高いサイトへの容易な誘導を提供している。



フィッシング・ツールバー：スタンフォードのSpoofGuard

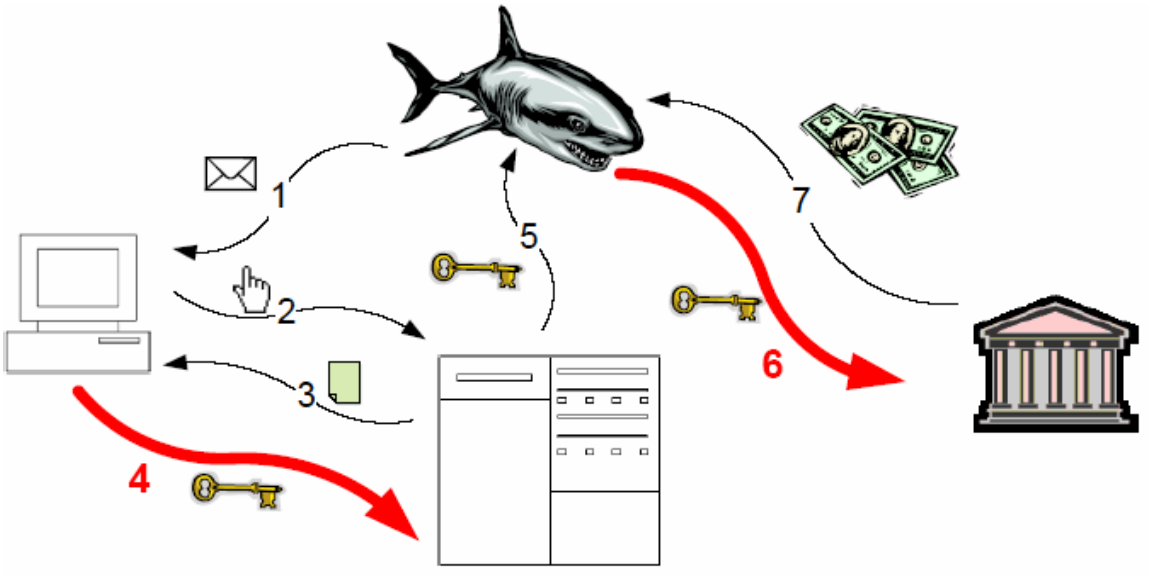
フィッシング防止ツールバーは、最新の技術を使用してなりすまされる可能性がある。画面上での場所の予約と組み合わせ、いかなるページまたはスクリプトによっても上書きされないようにすればこの危険性は回避できる。ユーザはさまざまなタイプのツールバーの表示に対し、異なる反応をすることが調査により明らかになっている。とりわけ、ある行動をとるべきか否かに関する具体的な案内を提供するツールバーは、サイトについて中立的またはプラスの情報のみを提供するツールバーに比べ、ユーザのトレーニング後には2倍以上の効果を実現することもある。しかし、最も効果的なツールバーでさえ、ユーザのトレーニングを行っていても、ユーザがフィッシングサイトを訪問した場合のフィッシングの成功率は依然として10%を超える。
フィッシング防止ツールバーによっては、ユーザが関係を持っているWebサイトに実際にアクセスした場合に、個人情報を使用して、ユーザが選択した名前または画像を表示するものもある。
アニメーション表示された境界線、ウィンドウの背景またはブラウザー・ウィンドウを囲む「クローム」のグラフィック・パターンなど、特殊なユーザ体験(experience)をブラウザー・ウィンドウごとに提供し、なりすましの防止を狙うブラウザー・プラグインもある。特殊なユーザ体験はクライアントでセッションごとに生成されるため、なりすましに対する耐性がある。このようなアプローチでは、異常なウィンドウの検出についてはユーザに依存しているため、スプーフされたウィンドウの検出の容易性と、美学的な容認可能性と押し付けがましさとのバランスが必要である。
フィッシング防止ツールバーの多くはサイトに関する情報の提供にとどまらず、フィッシングサイトと思われるサイトへのユーザの機密情報の入力の検出も試みる。ツールバーは機密情報のハッシュを保管し、発信される情報を監視して送信される機密情報を検出する。機密情報が検出されると、不正な場所に送られないよう情報の宛先が確認される。
発信データの監視には、克服すべき困難な障害がある。フィッシャーは発信情報を転送前に暗号化することがあるため、キー・ストロークは非常に低いレベルで傍受する必要がある（フィッシング・ツールバーによってはフォームの送信まで機密情報の検出を待つものもあるが、これは簡単な次善策に対して効果的でない）。同様に、Webページのスクリプトは文字がタイプされたそのままのデータを送信できる。さらに、キーロガーによる攻撃を防ぐためにアカウントとパスワード情報の順序を並べ替えてキー・ストロークを入力するユーザもおり、キーロガーの防御も無力になっている。フィッシング防止技術としての発信データの監視の長期的な実行可能性は不明だが、現時点ではほとんどのフィッシング攻撃には次善策が含まれていないため、効果的である。

ステップ4への対抗策：データ宛先のブラックリスト作成
フィッシャーと関係があるとされている特定のIPアドレスへのデータ送信をブロックする案がいくつかある。これは、フィッシングの情報の流れのステップ4を妨害する試みである。
データ宛先のブラックリスト作成には主な課題が2つある。第一に、フィッシング攻撃は、ボットネットまたは同様の構成によって多くのサーバを使用して分散型で実行されることがますます多くなっている。すべてのフィッ

シング・サーバを探すのは難題である。それが可能だったとしても、ホスト名をIPアドレスに変換するのに使われるインターネットのドメイン・ネーム・システム（DNS）を使用し、情報を内密の通信チャネルを通じて送信できるため、情報の送信を持続的に防ぐことにはならない。この簡単な例としては、フィッシャーがphisher.comのDNSサーバを制御しており、「credit-card-info」を送信したい場合、「credit-card-info.phisher.com」でDNSルックアップを行う。DNSルックアップの結果は重要ではない。データはDNS要求自体によってすでに送信されたからである。DNSはインターネットの根本的な基礎であるため、不明なアドレスについてDNSルックアップをブロックすることは実行可能ではない。
すべてのフィッシング・ドメインのDNSルックアップを何とか防げたブラックリストでさえ、DNS経由での迂回に遭う可能性は残る。フィッシャーがDNSサーバを一切制御していない場合でも、罪のない第三者DNSサーバからのDNS応答の生存時間フィールドを使用してDNS経由で情報を送信できる。
実際には、内密の通信チャネルの閉鎖は難しい問題であり、決然たる対抗者に対しては有効でない可能性が高い。

ステップ4への対抗策：画面ベースのデータ入力
重要な情報については、代わりのデータ入力メカニズムを展開している企業もある。ユーザは情報をタイプする代わりに、画面で情報を選択することで入力する。これはフィッシングの情報の流れのステップ4のキーロギング・マルウェアを妨害する試みである。
フィッシャーは次善策を展開していないため、画面ベースのデータ入力は現時点では有効である。しかし、画面ベースのデータ入力がさらに広く展開されるようになれば、マルウェアが表示を妨害し、画面に表示されたデータとユーザのそれとの対話を評価し、それによって機密情報が漏洩することも考えられる。

ステップ4への対抗策：相互認証
パスワードなどの認証のための認証情報においては、多くの場合、認証情報は双方の関係者に知られる。それを送信する代わりに、相互認証プロトコルを使用すれば、両者が認証情報を持っていることを相互に証明し合うことができ、いずれの側も認証情報を送信する必要がなくなる。
このようなプロトコルは多数ある。これらはユーザが認証情報を持っていることをサイトに対し証明すると同時に、ユーザにはサイトが認証情報を持っていることを証明できる。フィッシングへの適用は、このようなプロトコルを確実に使用する必要がある場合に限られたものになっている。フィッシャーは、認証情報を求めるだけで、プロトコルは実行しない。したがって、このような認証情報をすべてWebサイトではなく特別なプログラムに入れておくか、または後に説明するような信頼できるパスによるメカニズムを使用するべきである。相互認証プロトコルが使われることをユーザに示すもう1つの方法は、コンテンツが相互認証に使われるすべてのウィンドウに特定の画像を表示するというものである。このような画像はクライアント側に保管され、容易に詐称されることのないよう外部の関係者には秘密にされる。
相互認証プロトコルのもう1つの潜在的問題は、双方の認証情報が一致しなければならない点である。ユーザのパスワードの保管は良い慣習ではない。ほとんどの場合、パスワードはソフトでハッシュされて保管される。解釈可能なパスワードを保管する必要を避けるために、パスワードの相互認証プロトコルを、フィッシングの情報の流れのステップ6で説明するパスワード・ハッシングと組み合わせることができる。



フィッシングにおける情報の流れ、ステップ4および6

ステップ4および6：データ入力を防ぎ、役に立たないものにする

フィッシング攻撃における情報の流れのステップ4では、データが漏洩し、ステップ6では漏洩した情報が金銭上の利益のために使われる。ステップ4と6を攻撃する対抗策は、情報が漏洩する可能性を低くし、漏洩した場合にフィッシャーが情報を使えないようにする。

ステップ4および6への対抗策：信頼できるパス

インターネットの信頼モデルの根本的な欠点は、入力したデータが最終的にどこに送られるかがユーザにとって明らかでない点である。なりすまし不可能な信頼できるパスでは、重要な情報が正規の受信者にのみ届くことが保証される。信頼できるパスは、詐欺ベース・フィッシングとDNSベース・フィッシングに対する保護を提供する。オペレーティング・システムに実装されれば、アプリケーション・レベルのマルウェア攻撃からの保護も可能である。

信頼できるパスは、画面内の予約したエリアまたは傍受不可能な入力のいずれかのメカニズムを使用し、ログイン情報のために使われてきた。後者の例としては、Windows NTファミリーのオペレーティング・システムを使用したコンピュータへのログインにおけるCTRL-ALT-DELの使用がある。これは、C2認定のための米国コンピュータ・セキュリティ・センターの要件の一環として実装された。

従来型の信頼できるパスのメカニズムは、ユーザとオペレーティング・システムの間にローカル・マシン上で信頼できるチャネルを確立できる。有効なフィッシング対策のためには、悪質なサーバやプロキシーが存在する中、ユーザとリモート・コンピュータの間の信頼できないインターネット上に信頼できるパスを確立する必要がある。オペレーティング・システムは、次の2つの別々のタイプの引数によって呼び出される信頼できるパスのシステム・サービスを提供することで、センシティブな情報の入力を保護できる。

- 要求者のID、表示するロゴ、および公開鍵を含む認証局によって暗号署名された証明書
- 要求されているデータの仕様

この最も簡単な実装方法は、現在のWebページの受信に使われたアクティブなSSL接続に使われているサーバの証明書を使用し、データ入力に信頼できるパスを使用すべきだと指示するタグをHTMLフォームに含めることである。HTMLフォームは、ブラウザーからの信頼できるパスのサービスへの呼び出しにおいて、要求されたデータの仕様として使用できる。

オペレーティング・システムが信頼できるパスによる差し迫ったデータ入力について知らされると、ユーザは「セキュア・アテンション・シーケンス」として知られる傍受不可能なキー・シーケンスの入力を求められる。WindowsではCTRL-ALT-DELはセキュア・アテンション・シーケンスとなっている。これを使用するか、またはより使いやすい実装として、キーボードの特別なキーを信頼できるパスによるデータ入力専用にしておくこともできる。

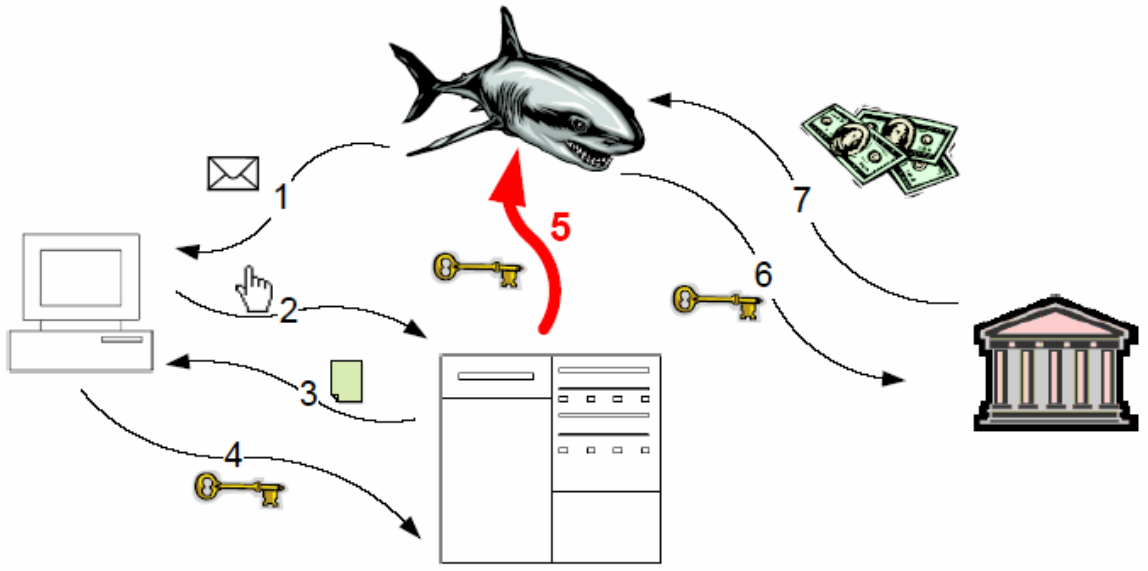
信頼できるパス：要求の通知

ユーザがセキュア・アテンション・シーケンスを入力すると、オペレーティング・システムは信頼できるパスによるデータ入力が要求されたと判断して標準入力画面を表示し、データ要求者のIDとロゴを証明書から表示し、指定された入力フィールドを表示する。

信頼できるパス：入力画面

セキュア・アテンション・シーケンスを受け取るのはオペレーティング・システムのみのため、オペレーティング・システムは確実に主導権を持つことができる。信頼できるパスによるデータ入力画面は、制御された環境にあるオペレーティング・システムによって直接表示される。このモードでは、表示を変更したり、キー・ストロークを傍受できるユーザ・プロセスはない。オペレーティング・システムによるこのレベルの制御により、管理レベルでのセキュリティ攻撃がない限り、フィッシャーによる改竄は不可能になる。フィールドが入力されると、データは証明書の公開鍵を使用してオペレーティング・システムによって暗号化されるため、対応する秘密鍵を所有する認定されたデータ受信者のみがデータを読めるようになる。暗号化されたデータは、要求したアプリケーションに提供される。
この特定の信頼できるパスのメカニズムでは、証明書を付与する前に認証局が申請者のIDとロゴを検証する必要がある。信頼できるパスの証明書は、少数の管理された権限者によって発行され、これらの権限者はIDの明確な証明を求め、不正なロゴが使われることのないよう徹底する。信頼できるパスのための信頼できる認証局になるための要件は、少なくともSSL証明書のルート認証局と同程度、おそらくはそれ以上に厳しくする必要がある。または、信頼できるパスにおいて、SSLよりも高いセキュリティのレベルの証明書を求めることもできる。
ロック・アイコンなどの勧告表示要素の確認を求める忠告とは異なり、信頼できるパスを通じてデータ入力画面にたどりつくことは、ユーザのサイトとの積極的な対話の一部である。信頼できるパスのメカニズムを必ず使用して機密情報（パスワード、クレジット・カード番号、ソーシャル・セキュリティ・ナンバーなど）を入力することにユーザが慣れると、信頼できるパスを使用しない機密情報の要求は直ちに危険信号となる。これは、信頼できないサイトへのデータ送信、または機密情報の入力を知らせる検出システムによって増補できる。
信頼できるパスは、フィッシャーがセンシティブな情報を解釈するために、その実際のIDを使用して要求するか、または信頼できるパスのメカニズムを使用せずに要求しなければならなくなるという点から、ステップ4への対抗策になる。ユーザは、信頼できるパスを使用してセンシティブな情報を入力することに慣れている場合、それを提供しない可能性が高い。信頼できるパスはステップ6への対抗策でもある。フィッシャーは証明書を盗み、盗ん

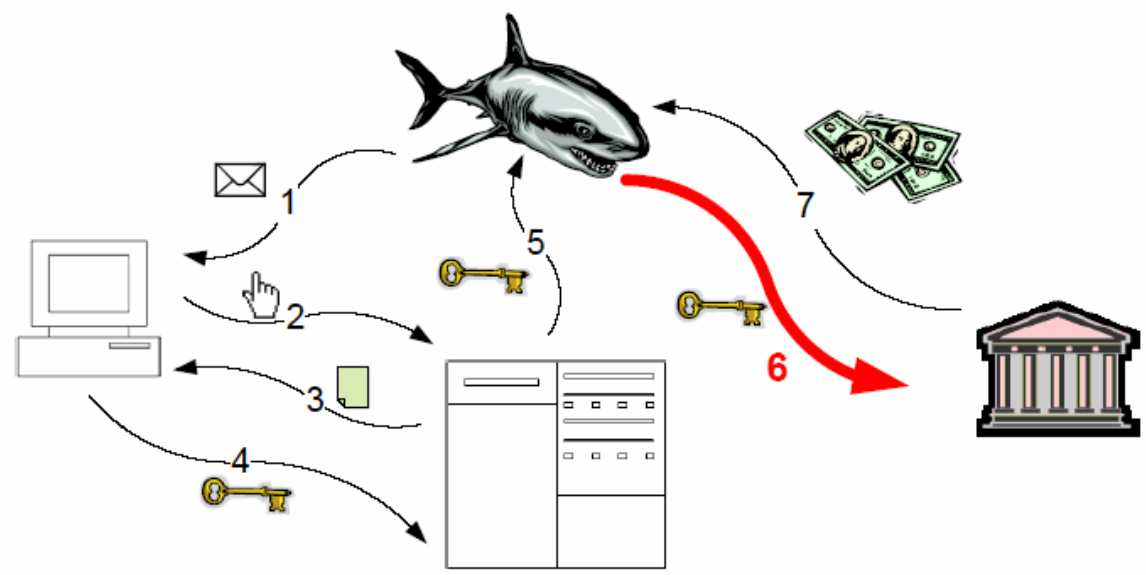
だ証明書を使用してデータを要求できる。しかし、センシティブなデータを複合するために必要な秘密鍵は正規の証明書の所有者のみが持っているため、フィッシャーはデータを解釈できない。
信頼できるパスはアプリケーション・レベルでも実装できる。スタンフォード大学のPwdHashプログラムにおける、パスワード入力のためのセキュア・アテンション・シーケンスとしての「@@」の使用は、アプリケーション・レベルでの信頼できるパスの実装である。ブラウザーに実装された信頼できるパスは、詐欺ベース・フィッシング攻撃とDNSベース・フィッシング攻撃に対する保護を提供できる可能性がある。ユーザ特権マルウェアに対する保護のためには、オペレーティング・システム・レベルでの実装が必要である。



フィッシングにおける情報の流れ、ステップ5

ステップ5：漏洩した認証情報の送信を追跡する

フィッシングにおける情報の流れのステップ5では、漏洩した認証情報がフィッシャーによってフィッシング・サーバまたはその他の収集者から取得される。Web上のトロイの木馬、キーロガー、またはローカル・セッション・ハイジャッキングなどのローカルに実行された攻撃の場合、漏洩した認証情報が取得されるフィッシング「サーバ」は、顧客のコンピュータの場合もある。
フィッシャーは、足跡を覆い、漏洩した情報の最終的な宛先を隠すために、入念な情報の流れを組み立てることがある。これらの情報の流れは、攻撃された「ゾンビ」マシン、インスタント・メッセージ、チャット・チャネル、匿名ピア・ツー・ピア・データ転送メカニズムなど、複数のメディアをまたぐこともある。学術論文では、Usenetへの投稿など公開された通信に情報を挿入できる公開鍵ステガノグラフィーなどの、最終的な証明書の利用者の検出を困難にする技法も提案されている。
一般的に、内密の通信チャネルを防ぐことは非常に難しく、現段階での対抗策は、フィッシャーへのデータの返信に先立ったフィッシング・サーバの撤去や、犯罪者を起訴するための情報の流れの追跡などを中心としたものである。



フィッシングにおける情報の流れ、ステップ6

ステップ6：漏洩情報の使用を妨げる

フィッシング対策としてのもう1つの技術ベースのアプローチは、漏洩情報の価値を下げることである。これは、フィッシングにおける情報の流れのステップ6において、フィッシャーが漏洩情報を不法収益に換えることを妨げるものである。以下の対抗策は、フィッシングの情報の流れのステップ6を攻撃する。

ステップ6への対抗策：従来型の二要素認証

データ漏洩の影響を軽減する最も一般的なアプローチは、*二要素認証*として知られているものである。これは、取引の実行を許可するために、以下の3つの基準のうちの2つの証明を必要とすることを意味する。

- 自分自身（指紋、網膜のスキャンなど網膜のスキャンなど）
- 持っているもの（スマートカード、ドングルなど）
- 知っていること（アカウント名、パスワードなど）

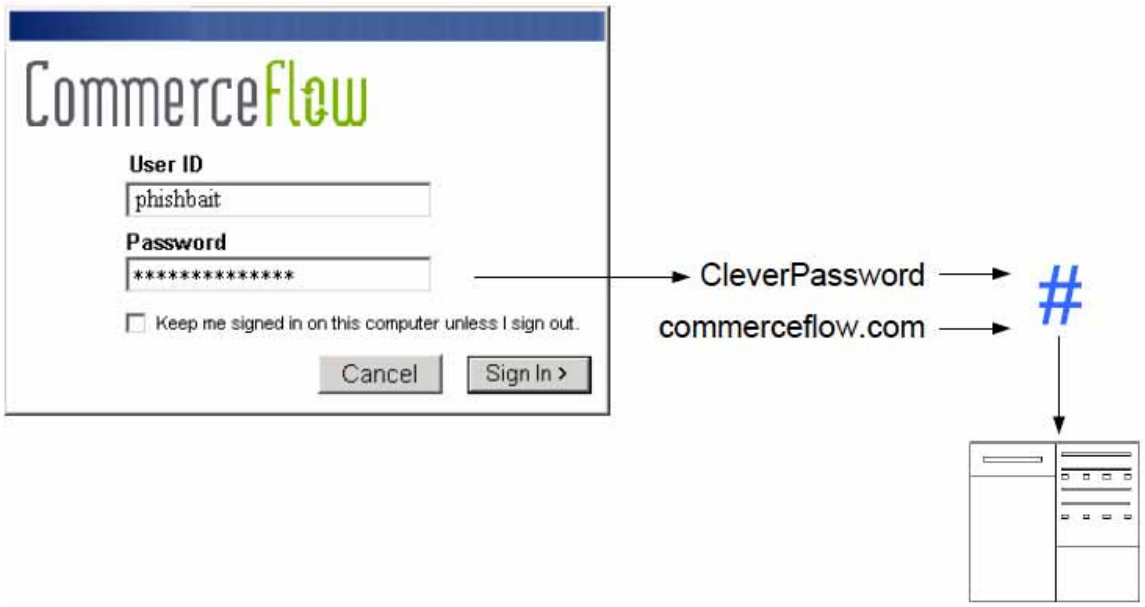
今日のフィッシング攻撃は、ユーザが*知っていること*を漏洩する場合が多い。このような情報はフィッシング攻撃によって容易に漏洩されるため、フィッシングの情報の流れのステップ6は、パスワード・タイプの証明書に加え、ユーザが*持っているもの*またはユーザ*自身*の何かを必要とすることで妨害できる。認証の追加要素は、一般的に「二要素認証」と呼ばれる。二要素認証は、アカウントにアクセスするため、または取引を実行するためのいずれかの目的で求めることができる。二要素認証はあらゆる取引に必要な場合もあれば、下記の*取引の確認*で説明するように、不正取引の可能性が高いと考えられるものにのみ必要なこともある。
米国で最も広く展開されている二要素認証デバイスは、ワンタイム・パスコード（OTP）デバイスである。このようなデバイスでは、定期的な間隔、または使われるたびのいずれかで変わるコードが表示される。ユーザがデバイスを持っていることを示すために、ユーザは、最新のパスコードの入力を求められる。このパスコードは、使われているシーケンスと最新の値を把握しているサーバによって検証される。
OTPは理解しやすく、盗まれた証明書を後で販売するための二次市場を大いに排除できる。しかし、OTPは、OTPが依然として有効な間に経済的損害が生じるようなフィッシング攻撃に対し脆弱である。OTPがフィッシングの情報の流れのステップ4でフィッシャーに渡されたときから、ステップ6で認証情報が使われるまでの間の時間が短い場合（中間者攻撃やセッション・ハイジャッキング攻撃などではこのような状況が考えられる）、フィッシャ

ーはステップ6でOTPを使用できる。
その他の形式の二要素認証には、このような攻撃に対する耐性がある。スマートカードやUSBドングルは、暗号処理を内部で実行し、盗聴者が解釈できないような手法で、認可された相手と直接認証を行うことができる。適切に実装されたバイオメトリック認証システムでは、中間者が最終的なサーバからのチャレンジに対するレスポンスを再利用できないような形で通信チャネルと結び付けられた、チャレンジ・レスポンス・プロトコルを使用する。

ステップ6への対抗策：コンピュータ・ベースの二要素認証
別のハードウェアによる二要素認証デバイスは、効果的な対抗策になる。しかし、購入、展開、サポートが高価であり、一部のもの（スマートカードなど）ではインフラストラクチャーへの恐ろしいほどの投資が必要である。さらに、不便さゆえに、顧客はハードウェアによる二要素認証デバイスの使用に抵抗を示してきた。従来型の二要素認証は、商業銀行のアカウントのような価値の高いターゲットに適しているが、今のところ米国では典型的な消費者アプリケーションにおいては広く展開されていない。
これよりコストが低い二要素認証のアプローチとして、顧客のコンピュータを*持っているもの*の認証要素として使用する方法がある。これは、顧客は自宅または職場の少数のコンピュータのいずれかからオンライン・バンキングを実行することが多いという観察に基づいている。コンピュータ・ベースの二要素認証ではこれらの認可されたコンピュータを顧客のアカウントに登録し、それらの存在を二要素認証に使用する。
これは有効なアプローチであり、ハードウェア・ベースの二要素認証と比べた場合、コストと使いやすさの面でメリットが大きい。しかし、セキュリティ上の考慮事項がいくつかある。まず、認証情報を受け取る際にDNSベース攻撃を避けるために、マシンのID情報は中間者攻撃を受けにくい方法で送信する必要がある。たとえば、ID情報の受信者を認証する特別なソフトウェア・プログラムの使用、またはSSLによって自らの認証を行ったリモート・サイトにのみ送られる安全なcookieの使用などである。
第2に、コンピュータ・ベースの認証は最終的にはローカルで実行されるセッション・ハイジャッキング攻撃またはユーザのコンピュータを使用して取引が行われるその他の攻撃を受けやすい可能性がある。ある意味、悪質なソフトウェアがひとたび顧客のコンピュータで実行されると、そのコンピュータはもはや顧客のものではなくなり、フィッシャーが所有し、認証に使えるものになる。
コンピュータ・ベースの二要素認証の主なセキュリティの問題として、新規のコンピュータの認可、または既存のコンピュータの再認可がある。ユーザは時には外部からのコンピュータまたは新たに取得したコンピュータを使用したり、認可情報が取り除かれた場合にはコンピュータを再認可する必要がある。コンピュータの認可は、ユーザにいくつかの質問に答えてもらったり、2次パスワードを提供してもらうことで行われる場合もある。この情報はフィッシングされる可能性があり、2つ目の*知っていること*要素として、コンピュータ・ベースの認証を1因子認証へと縮小する。
真の2つ目の認証要素であるためには、コンピュータ・ベースの認証は*持っているもの*を使用して新しいコンピュータを認可する必要がある。たとえば、ユーザが新しいコンピュータの認証を要求した場合、ワンタイム・パスコードがユーザの携帯電話に送信される。ユーザはこの情報を特別なプログラムにタイプし、それは適切な宛先に送られる。この場合、ユーザがパスコードを決してWebページには入力しない点が重要である。フィッシングサイトがパスコードを取得し、フィッシング・マシンの認可に使用する可能性があるためである。コンピュータの認可のための*持っているもの*もう1つの形態に、電子メール内のクリック可能な認可リンクがある。このリンクは、リンクをクリックするために使われたIPアドレスにあるコンピュータを認可する。

ステップ6への対抗策：パスワード・ハッシング
パスワードのフィッシングは、フィッシング・サーバに送られたパスワードが、正規のサイトでも有用なものでない限り無駄である。フィッシャーが有用なパスワードを集めるのを防ぐ方法の1つとして、ユーザ・パスワードを使われる場所に依存させてエンコードし、エンコードされたパスワードのみをWebサイトに送信する方法がある。これにより、ユーザは複数のサイトについて同じパスワードをタイプでき、各サイト（フィッシングサイト

も含む）は、個別にエンコードされたバージョンのパスワードを受け取る。このアイデアを実装したものを、パスワード・ハッシングと呼ぶ。パスワード・ハッシングでは、パスワード情報は送信前に送られる先のドメイン・ネームとともにハッシュされるため、実際に送信されたパスワードは、パスワード・データを受信したドメインでのみ使える。パスワード・ハッシングは、最終的には、パスワード・フィールドで自動的に実行される組み込みメカニズムとしてブラウザーで提供できる。オフライン・辞書攻撃を防ぐために、パスワード・ハッシングを使用するサイトは適切なパスワード要件も施行すべきである。パスワード・ハッシングでは、詐欺ベース・フィッシング攻撃で漏洩したパスワード・データが正規のサイトで再利用できないことから、フィッシングの情報の流れのステップ6への対抗策になる。



パスワード・ハッシング

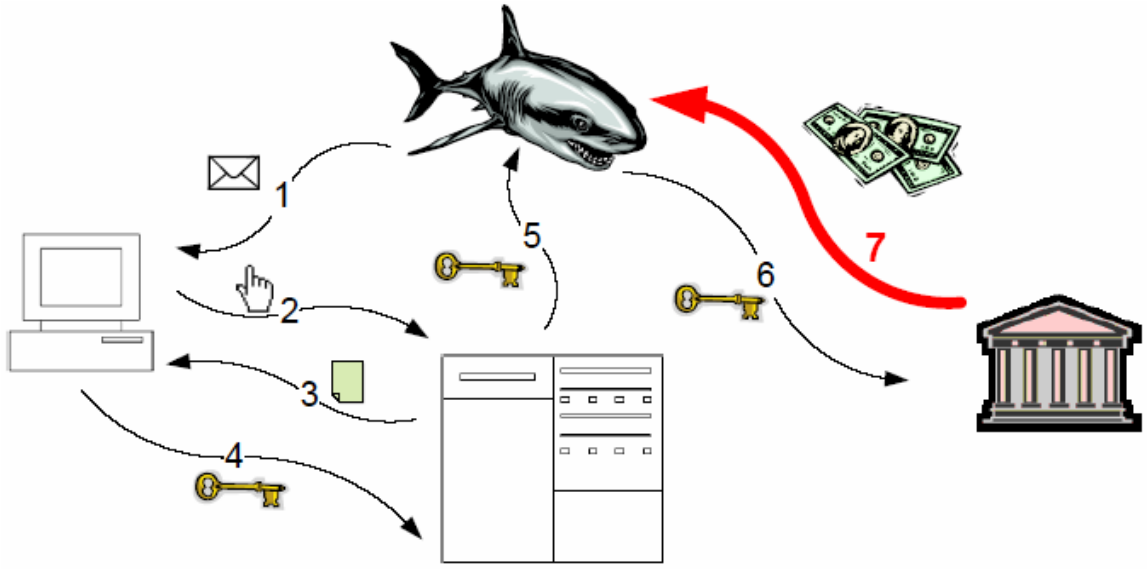
フィッシングに対するセキュリティに加え、パスワード・ハッシングは、サイトからの大規模なパスワード・データの盗難によるフィッシング以外の形態での識別情報の盗難に対する適切な保護も提供する。サイトが平文でのパスワード・データの保管を行わないことと、パスワードが別のサイトでは再利用できないことの両方を保証する。ユーザは複数のサイトで同じパスワードを使用することが多く、あるサイトで盗まれたユーザ名とパスワードが別のサイトで再利用される可能性がある。パスワードが辞書攻撃において想像されにくいものである限り、パスワード・ハッシングは盗まれた認証情報のそのようなサイト間での再利用を防げる。相互認証プロトコルと組み合わせることで、パスワード・ハッシングは、相互認証パスワードを平文で保管する必要性を除去することもできる。
フィッシャーは、パスワードを求めた後にパスワード・ハッシングを行うことはないため、パスワード・ハッシングは単独では詐欺フィッシング攻撃への保護を提供するものではない。したがって、パスワード・ハッシングを施行するために、パスワード入力を他のデータ入力と異なるものにする方法が必要である。前述の信頼できるパスがこの目的に適している。スタンフォード大学のPwdHashプログラムでは「@@」をセキュア・アテンション・シーケンスとして使用し、入力フィールドでパスワード・ハッシングが使われていることを確認する。このセキュア・アテンション・シーケンスはブラウザー・プラグインによって傍受され、プラグインはフォーカスがフィールドから離れるかまたはフォームが送信されるまでパスワード・データをスクリプトから隠す。この時点で、パスワードのハッシュされたバージョンが置き換えられる。

ステップ6への対抗策：取引の確認

フィッシングのリスクを軽減するアプローチの1つに、不正な可能性のあるオンライン取引への集中がある。これは銀行が実社会で実施しているリスク管理対策と似ている。クレジット・カードの取引はすべて評価され、疑わしい取引は顧客に確認が行われる。
オンライン取引の分析は、ユーザのIPアドレス、ユーザのマシン上でのcookieなどの認証情報の存在、取引の量、仕向先の銀行口座、仕向先の銀行口座の特徴、取引パターンの口座間分析など、さまざまな測定基準を使用して実施できる。このような分析は、銀行のオンライン・システムに統合されたソフトウェア、またはWebトラフィックを監視する「アプライアンス」で実施できる。疑わしいとして取引にフラグが立てられると、取引別の認証が顧客に求められる。
批判的に見ると、このような認証はフィッシングされるおそれのあるような「what you know(知っていること)」という質問の形で行うべきではない。強固な形の取引の認証では、電話などの信頼できるデバイスを2つ目の要素として使用する。顧客のものとして知られている番号に電話がかけられたり、SMSメッセージが顧客の携帯電話に送られると、顧客は取引を音声または返信メッセージによって確認できる。確認情報には取引自体の詳細を含めることが重要である。さもなければ、フィッシャーがセッション・ハイジャッキング攻撃を行い、ユーザが確認する取引を変更できてしまうからである。バイオメトリック・デバイスが、信頼できる状態で取引の詳細を表示できる場合、バイオメトリックスも認証に使用できる。
一部の調査によれば、顧客は確認を求められることを予想している場合、詳細をチェックすることなく取引を確認することがある。したがって、このような確認は非常にまれにするか、または確認する取引をユーザが自発的に選択することを求めるユーザ・インターフェイスを使用すべきである。
取引の分析と確認は、適切に実施されれば、管理者特権マルウェアなどのあらゆるタイプのフィッシング詐欺だけでなく、フィッシング以外によるその他の形態の識別情報の盗難におけるステップ6の効果的な軽減になる。100%の保護を提供するものではないが、オンライン取引による損害を大幅に削減できる。銀行はこのメリットを、展開コストと予想されるユーザ経験の混乱と比べて評価すべきである。

ステップ6への対抗策：ポリシー・ベース・データ
ステップ6へのもう1つの対抗策は、データを、どのようにまたは誰が使えるかを決定するポリシーと密接に組み合わせることで、第三者が使えないようにすることである。これはフィッシング攻撃のステップ6への対抗策にとどまらず、ハッキングまたはインサイダー攻撃によるデータ盗難など、フィッシング以外による識別情報の盗難にも適用できる。
この技法は、データを受信し保管するサイトが、データの最終的な利用者ではないような状況に適している。たとえば、電子商取引のサイトやISPでは、ユーザが買い物の支払いまたは繰り返し発生する請求書への支払いに便利に使えるよう、クレジット・カード番号を記録しておく必要がある。しかし、クレジット・カード取引は電子商取引会社またはISPによって行われているわけではない。実際には、支払処理会社が請求に責任を持つ。
サイトではクレジット・カード情報と、そのサイトのみが請求を行えることを定めたポリシーを組み合わせることができる。この組み合わさった情報は、クレジット・カード情報を保管する前に、支払処理会社が所有する公開鍵を使用して暗号化される。この情報は、支払処理会社のみが所有する秘密鍵なしでは復号できない。したがって、データは盗まれても盗難者にとっては役に立たない。社内でデータを保管している人が通常、復号鍵を利用でき、そのような人がわいろを受け取ったり、その他の方法で復号データが漏洩し得るような従来型の暗号化データベース方式とは異なる。
取引の実行時には、暗号化されたクレジット・カード情報が取引の詳細とともに送信される。支払処理会社はこの束を復号し、ポリシーをチェックする。取引がポリシーの下で認可されていない場合、たとえばポリシーではCommerceFlowのみがカードに請求できるとされているのに対し、PhishingEnterprisesが請求をしようとしている場合などは、請求は拒否される。
フィッシングのための対抗策とするためには、これを前述の信頼できるパスのメカニズムと組み合わせることもできる。ポリシーは、フォームに組み込み、指定した入力フィールドと組み合わせ、ID情報を画面上に表示できる指定された鍵で暗号化できる。フィッシャーが何とかサイトの主なデータにアクセスできたり、その他の方法

で情報を漏洩できたとしても、ポリシー・ベースの認証情報は依然としてフィッシャーにとって役に立たない。



フィッシングにおける情報の流れ、ステップ7

ステップ7：金銭上の利益を妨げる

フィッシングにおける情報の流れのステップ7では、ステップ6で漏洩した認証情報を使用して経済的利益が実現する。
金融機関は、フィッシング攻撃に使われている口座を検出するために、特定のタイプの送金に遅れを設けてきた。保留期間中に不正な受取口座が特定されれば、送金は無効にされ、経済的損失が防げる。
ステップ7は捜査当局もかなり関心を持っているステップである。フィッシャーは、盗まれた認証情報の使用による金銭の流れを追跡することで捕らえられることが多い。
フィッシャーは、複数の層によって金銭をフィルタにかけ、匿名の換金手段を使用することが多いものの、最終的にはフィッシャーが金銭を受け取るため、このような流れは追跡できることが多い。

技術以外のベスト・プラクティス

本報告書は、主としてフィッシング防止技術を取り上げたものである。とはいえ、フィッシングの標的になり得るすべての関係者が知っておくべき慣習がいくつかある。

- 自社のブランドに似た最も騙されやすいドメイン・ネームで利用可能なものを登録する。これは最も安価な保険である。
- ドメイン・ネームを商標登録し、一見同じようなドメイン・ネームを登録した関係者に対する償還請求に備える。
- 最近のドメイン登録を監視し、自社のドメイン・ネームと一見同じようなものを登録した関係者に対し、行動を起こす。
- DNSレコードの電子メール認証情報を公開し、顧客とのすべての通信に認証電子メールを使用する。代理でメールを送信してくれる関係者についても適用すべきである。
- 顧客宛のすべての発信メールにデジタル署名をすることを検討する。メール・サーバで実行できない場合は、電子メール・ゲートウェイで行うこともできる。

- 電子メールの慣習に関し、個人情報を決して尋ねない、またはクリック可能なリンクを決して電子メールで提供しないなど、明確なポリシーを確立する。ポリシーは、組織内のすべての利害関係者にとって受け入れられるものにする。自社に代わって電子メールを送信するすべての第三者にポリシーを徹底する。ポリシーを顧客に定期的に伝え、可能であればすべての電子メール通信、印刷物による発表などのその他のメディアでも伝える。
- 顧客への電子メールには必ず個人情報を含める。個人情報とともに、毎回そうすることが自社のポリシーだという教育的な記述を添える。
- その電子メールが本当に自社からのものかを確認するために顧客が電子メールを送れる、spoof@yourcompany.comというような電子メール・アドレスを提供する。フィッシング・メッセージの報告方法に関する明快な指示をWebサイトや自社からの通信に掲載する。
- 顧客との対話に、異常な名前や予期せぬ名前のWebサイトを使用しない。
- 自社のWebサイトがSSLを使用しており、すべての証明書が最新のものであることを確認する。
- 自社サイト上の開かれたURLリダイレクトをすべて取り除く。
- クロスサイトスクリプティングとSQLインジェクションにおいては、受け入れフィルタを使用し、ユーザが提供したデータがすべて厳重にフィルタにかけられるようにする。
- 識別情報の盗難による損失に責任を持ち、フィッシングによる損失から注意が逸れるような他の潜在的損失（不適切な貸出決定など）には責任を持たない上級職を組織内に設ける。
- フィッシング攻撃への対応に責任を持つ部門間タスク・フォースを設立する。参加する人員は上級社員で、迅速な意思決定と実行を行う権限を持つ。責任と手順を明確に描く。「防災訓練」を行い、役割が理解され、伝達が速やかであることを確認する。
- フィッシング攻撃が発生した際に送信する顧客への通信を事前に準備し、攻撃が始まったときに送信が遅れるのを防ぐ。
- 電子メールのバウンス・メッセージ、顧客からの問い合わせの件数、口座の異常な動き、疑わしい画像の使用、フィッシング・グループに関するディスカッションなど、フィッシング攻撃の兆しを監視する。
- フィッシング攻撃が発生したら署名ベースでのチェックを使用する電子メールのフィルタリング会社に直ちに通知し、フィッシング電子メールの例を提供する。これらの会社では、意図する受信者への多くの電子メールをブロックするルールを展開できる可能性がある。
- フィッシング攻撃が確認されたら捜査当局に直ちに知らせる（付録B参照）。
- フィッシング攻撃が確認されたら、Webサイトに警告を掲示し、電子メールで顧客に攻撃について知らせることを検討する。
- フィッシング・サーバを追跡し、できる限り早くシャットダウンする。この作業を支援できるサービス・プロバイダーもある。
- 大規模なフィッシング攻撃が確認されたら、顧客サービスのスタッフを増やす。
- フィッシャーを後で起訴できるよう、フィッシング攻撃の証拠を保存する。
- 第三者には、前述の慣習に反して代わりに行動をとれるような権限は与えない。

結論

フィッシングを完全に阻止できるような単一の技術はない。しかし、適切な組織と慣習、最新の技術の正しい適用、セキュリティ技術の改善などの組み合わせにより、フィッシングの普及とそれによる損失は劇的に軽減される可能性がある。特に重要なのは次のような点である。

- 価値の高いターゲットはベスト・プラクティスに従い、それらの継続的な発展について確認し続ける。
- フィッシング攻撃は、顧客の報告、バウンスの監視、画像の使用の監視、ハニーポット、管理者による行動への警告、およびその他の技法の組み合わせによって迅速に検出できる。

- Sender-IDや暗号署名などの電子メール認証技術は、幅広く展開されれば、フィッシング電子メールがユーザに届くのを防げる可能性がある。
- 画像(imagery)の分析は、フィッシング電子メールの特定について将来研究が期待される分野である。
- 暗号化されたパッチは、マルウェアの作成者にセキュリティの脆弱性を知られるのを防ぎ、脅威への迅速な対応を自動化できる。
- 個人情報はすべての電子メール通信に含めるべきである。ユーザがカスタマイズされたテキストおよび／または画像を入力または選択できるシステムは特に有望である。
- 潜在的詐欺コンテンツの表示や、安全でない可能性のあるリンクを選択した際の警告などのブラウザーのセキュリティのアップグレードは、フィッシング攻撃の有効性を大いに削減できる。
- 不正なDNS情報の検出は、有望な検討分野である。
- フィッシング攻撃に関与するコンポーネント（スパム・フィルタ、電子メール・クライアント、およびブラウザー）間での情報共有は、フィッシング・メッセージおよびフィッシングサイトの特定を改善し、疑わしいコンテンツとの危険な行動を制限できる。
- コンテンツインジェクション攻撃は拡大中の問題である。ユーザのコンテンツはすべて受け入れフィルタを使用してフィルタにかけるべきである。ブラウザーのセキュリティ強化により、クロスサイトスクリプティング攻撃が発生する可能性を小さくできる。
- フィッシング防止ツールバーは、フィッシングサイトの特定と、フィッシングサイトと思われるサイトが検出された際にセキュリティを強化するための有望なツールである。
- パスワード・ハッシングなどによるドメインごとの証明書の変更は、識別情報の盗難に対する強力な対抗策であり、信頼できるパスと組み合わせれば非常に効果的なフィッシング防止策になる。
- データの安全な入力と送信のためのOSレベルでの信頼できるパスは、不正な相手への機密データの漏洩を劇的に削減できる可能性がある。
- ハードウェア・ベースの二要素認証は、フィッシングに対して極めて有効だが、一部のアプローチは短期間でのフィッシング攻撃に遭いやすいため、価値の高いターゲットでの少数のユーザが関与する状況で推奨される。
- コンピュータ・ベースの二要素認証は、適切なセキュリティ面での特徴と低い展開コストを提供するが、特定のタイプのマルウェア攻撃を受けやすい。新しいコンピュータをどのように認可するかが、セキュリティ設計における重要な検討事項になる。
- アウト・オブ・バンドの通信チャネル経由での取引の確認は、マルウェアへの耐性のある強力な技法である。
- 可能な限り、データはフィッシャーによる使用を防ぐポリシー・ステートメントと組み合わせ、下流のデータ利用者の公開鍵で暗号化するべきである。これにより、漏洩データの不正使用が防げる。
- 捜査当局が役立てられるようなログを保管し、損失を定量化できるようにしていれば、捜査当局の対応をより効果的なものにできる。

フィッシング対策協議会 技術・制度検討 WG

資料2

第三者認証について

サイバートラスト株式会社
認証サービス事業部

フィッシング対策／企業個別対応には限界もあります。

低すぎる「身元詐称」コスト

リアル世界で身元詐称をするコストに較べ破格に低いこと、電子商取引市場の拡大に照らし、「身元詐称」犯罪は無くならないと思われます。

複製が容易であることがデジタルデータの本質にあるため、また人間は「錯覚」する生き物（リアル世界で頻発する「おれおれ」詐欺） であることからも難しいことが伺えます。

サイト保有者は被害者

- **サイト保有企業は寧ろ被害者であり、その上サイト保有企業が関知せぬところで犯罪が起こることにも問題があります。**
- **企業単体での対処には限界があると言えます。**

第三者認証が何故有効か？

ネット上に「信頼」は存在しない

- **「信頼」はリアル世界でしか確保出来ません。**
- **例えば、その会社に行ったことがある、そこの社長と会ったことがある、が信頼の源泉となります。**

すべての会社を自ら訪問することは出来ない

- **そこで、信頼できる第三者機関に対する需要が生まれます。**

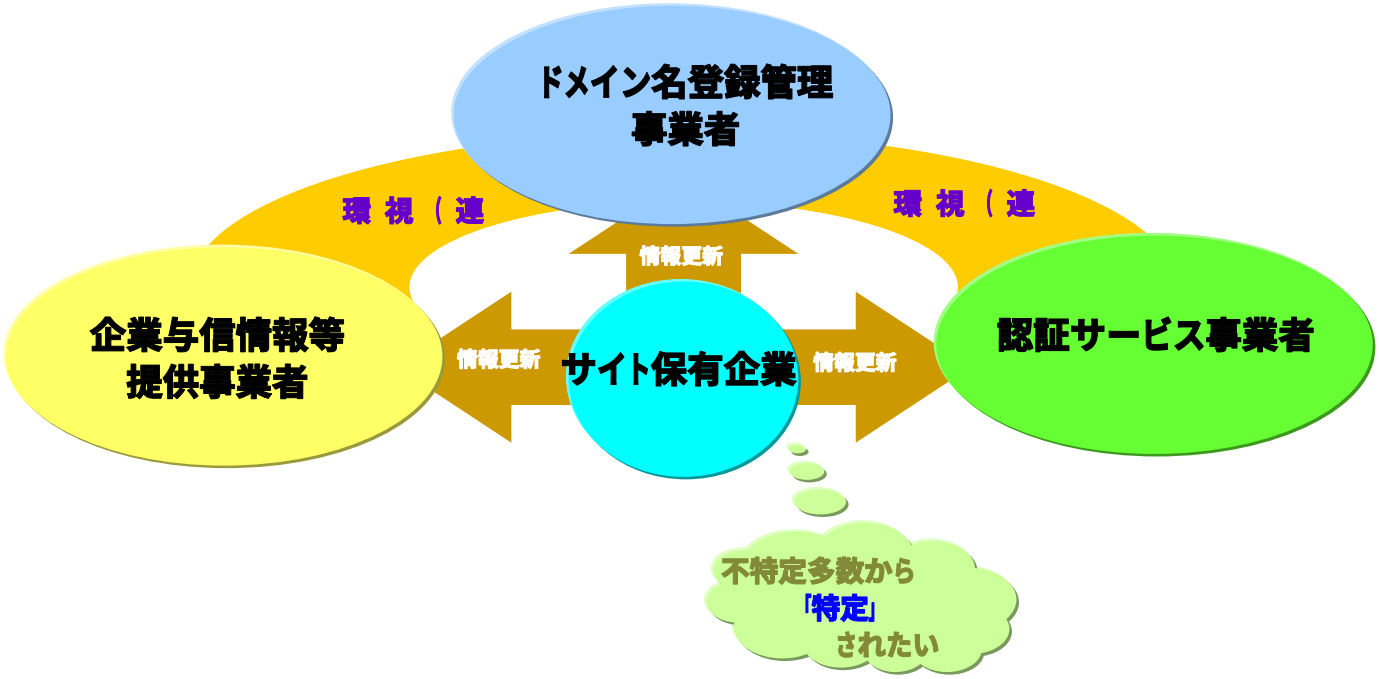
「衆人環視」という考え方

「より安心出来る」電子商取引環境の整備に利益を共有する集団的取組みが有効と考えます。

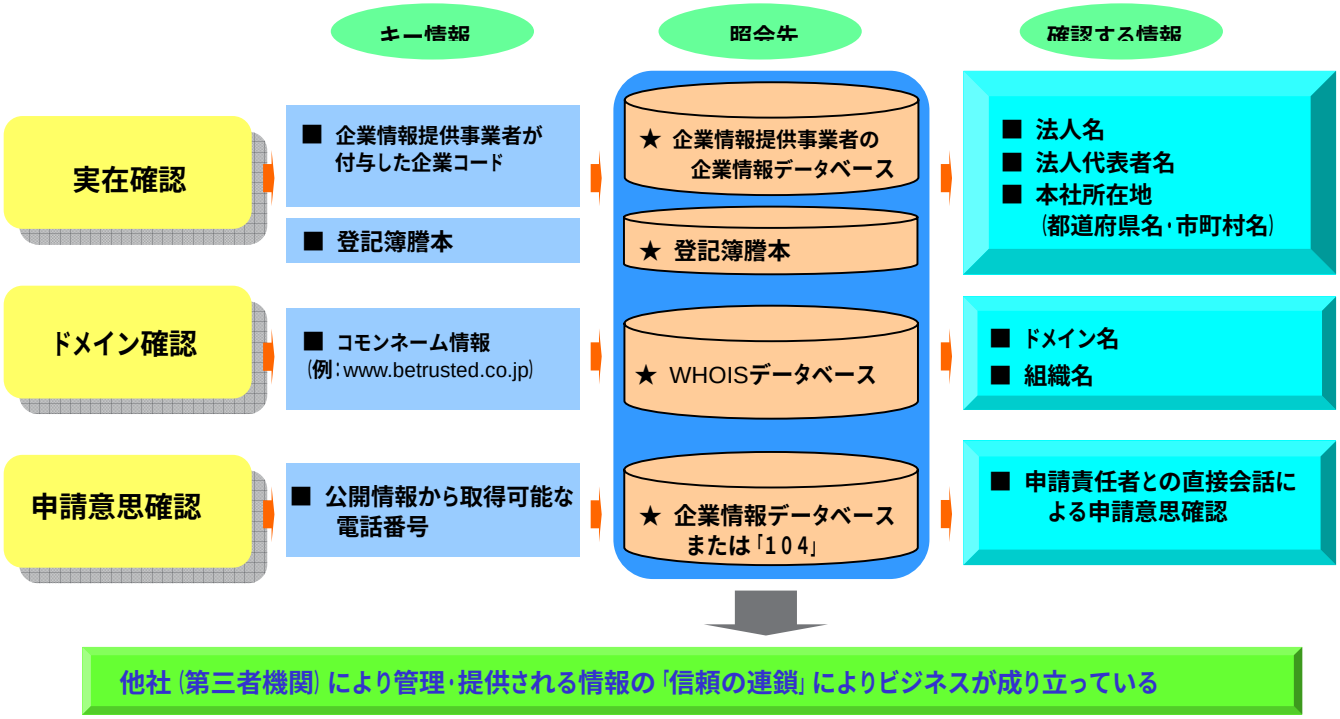
- 対面可能な「リアル」世界にも「第三者」認証という仕組みが存在（運転免許、印鑑証明、パスポート、CAFIS 、etc ） しています。
- デジタルデータは複製が容易であり、「ネット」世界では一層の精度が必要となります。

「衆人環視」という考え方－Site 保有企業の実在確認を「複数」の第三者により実現します。

- ドメイン名取得、SSL サーバ証明書取得、という汎用性ある機会が活用できるのでは？と考えています。
- 現状では、Screening （情報収集及びその確認）の精度が高いとは言えず、そこに「環視（連携）」という考え方もありません。



■ サーバ証明書＆電子メール署名用証明書 審査要



企業認証基盤としての方向性

Web Site の「信頼」だけでは不十分

- 電子メール、ダウンロードソフト、PDF 等ドキュメント情報など、「不正」Site への Gateway は多彩にあります。

- **Web Site の「衆人環視」基盤の共用が現実的**
  - 企業実在確認は共用に耐えるものであり、他方仕組みの精度向上の為にも Scalability 確保は有効だと考えています。
  - また、Web Browser 以外のネット利用環境での十分な PKI Readiness の整備が必要とも考えています。
    - 1. 携帯電話キャリア(携帯電話メールへの S/MIME 実装)
    - 2. アプリケーション開発事業者(Qualcomm, Adobe, etc)
  - 「電子署名付き電子メール」サービスの事例も徐々に顕在化 しています。
  - 「SaaS (Software as a Service 」の進展によるダウンロードソフトに対する認証需要も高まるものと想定しています。(コードサイニング証明書)

何故、PKI？

公開鍵暗号基盤（PKI）の実効性

・リアル世界でしか確保出来ない「信頼」を、ネット世界にシームレスに伝播させる仕組み

- **Web ブラウザにトラスト・アンカーとして採用された認証局が存在し、ネット上で「一意的」に信頼を連鎖する秘密鍵と公開鍵のメカニズムを提供しています。**

・ 内部犯行リスクの排除が可能であることもメリット

- **Pass word 等認証情報を Client-Server 間で共有しない為、内部犯行を防ぐことも可能です。**
- **また、内部犯行であるか否かの立証コストを PKI の利用によって削減できるものと考えています。**

Windows Vista “EV SSL Certificate (EV SSL 証明書)”の登場

■ **Windows Vista + Internet Explorer7**
- 2007 年 1 月末から Microsoft により市場投入される予定です。

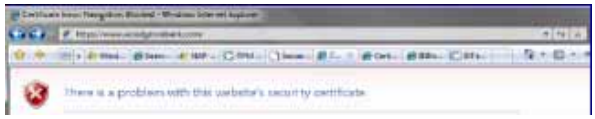
■ **Extended Validation SSL Certificate (EV SSL 証明書)**
- ユーザが「鍵」マークをクリックして証明書情報を見に行かずとも、セキュリティステータスバーが“緑”、“赤”に変色し、視覚的にストレートに証明書有効性ステータスがアピールされます。
- 併せ、企業実在確認プロセスの厳格化も行われるます。 (CA Browser Forum によって審査のガイドラインが定められています。)

☆ Extended Validation SSL Certificate (EV SSL 証明

ー グリーンバ

☆ 問題があるSSL 証明

ー 操作を続行するかの確認画



ー 続行すると、レッドバーとな

揺らぐ「鍵マーク」の信頼性

■ **ドメインの所有確認のみで発行されるサーバ証明書が Phishing を後押し!?**
- 実在証明無しの証明書はドメインさえ所有していれば誰にでも発行を許しています。
- 即ち、個人 (Phisher) に対しても発行することが可能です。
- 米金融系でドメイン所有確認のみで発行されるサーバ証明書を提示する Phishing サイトが発見されています。
- 有識者等から認証機関として、ドメイン所有認証のみのサーバ証明書の在り方が問われています。

フィッシング対策製品1

サーバ証明書 （登記簿謄本、企業コード、電話によるサーバ証明書の申請意思確認など）

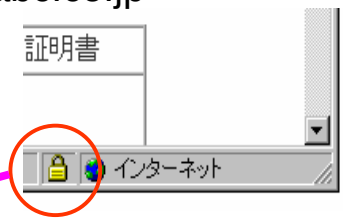
期待できる効果

1. WEB サイト運営企業･組織の実在性を保障することができます。
2. WEB サイトの運営企業･組織の実在性を確認し証明書を発行するために、フィッシングサイトのターゲットとなることを防ぐことができます。

サーバー証明書の主要な機能とは？

- SSL暗号化通信
- サイトの実在証明

https://www.abc.co.jp



PCでは

鍵マークをダブルクリックして証明書を確認！

SSL暗号化通信

個人情報、クレジットカード番号等第三者に盗み見られては困る情報を暗号化して送信

サイトの実在証明

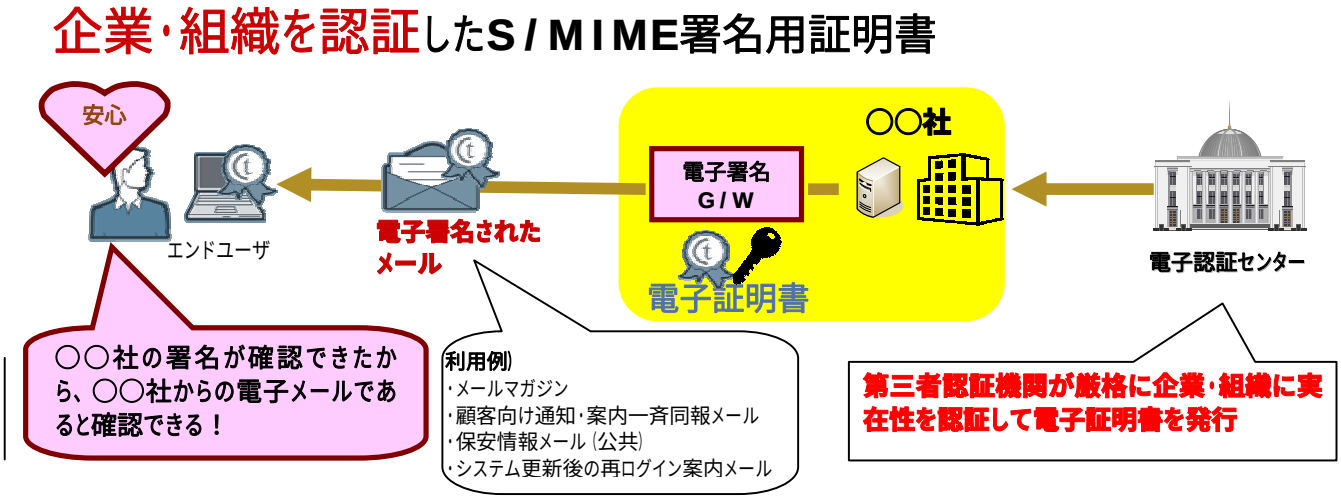
サイト運営企業が実在し、自己が所有するドメインを使用していることを第三者機関が証明

フィッシング対策製品2

メール署名用証明書 （登記簿謄本、企業コード、電話によるサーバ証明書の申請意思確認など）

期待できる効果

1. **電子メール送信元企業･組織の実在性を保障することが出来るようになります。**
2. **電子メール受信者に対して、フィッシングメールか否かを可視的に判断させることが出来るようになります。**



以上

資料3

フィッシング対策としての画像による認証技術

株式会社ニーモニックセキュリティ
國米　仁

１．ユーザ認証画面の個人別カスタマイズの効果

真正ウェブサイトのユーザ認証画面と瓜二つの偽画面をユーザに提示し、ユーザの本人認証情報を盗もうとするフィッシング犯を排除するための方法の一つとして、ユーザ認証画面の個人別カスタマイズがあります。

フィッシングの多くは著名企業の真正ウェブサイトのユーザ認証画面とそっくりの偽画面を用意しておき、偽メールやファーミングと呼ばれる偽装工作等によってユーザをこの偽画面に誘導して本人認証情報を入力させます。一般には対象とするユーザが数百万人であっても準備すべき偽画面は一組で良いのでフィッシング犯は非常に高い効率を享受しています。

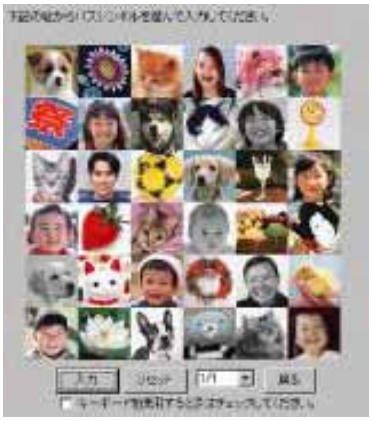
しかし、ユーザ認証画面が個人別にカスタマイズされているウェブサイトでは事情は一変します。フィッシング犯は事前に対象とするユーザのＩＤを調べ上げ、更に各ＩＤに対応する個人別カスタマイズされたユーザ認証画面とそっくりのものを準備しておかなければなりません。ユーザＩＤを悉く調べ上げ、それぞれに対応する個別の認証画面を悉く事前に用意するのは技術的には不可能ではないものの費用対効果は著しく悪いものになりますので、経済犯的なフィッシング犯はこうした経済効率の悪いウェブサイトを忌避することになります。

２．実施方法

認証画面の個人別カスタマイズには様々な方法があります。ユーザが登録したキーワードを表示するもの、ユーザが指定した色や紋様で認証画面の背景を表示するもの、ユーザが指定したアイコンを画面の一角に表示すもの、などの手法が知られています。

ユーザがそれぞれ独自に準備したオリジナル画像を認証データとして使う手法では、ユーザ認証手段そのものが自ずからフィッシング排除機能を備えています。

一例を示します。あるユーザが巧妙に偽装されたフィッシングサイトにアクセスすると右に示すようなユーザ認証画面が表示されました。この画面はユーザが自ら登録したものではありません。



ユーザが如何に迂闊であっても、自分が使っているものではない画面上で自らが準備したオリジナルの画像を選択することは不可能です。つまり、存在しないものは見つけられず、見つけられないものは選択できず、選択されないものは盗むことができないというシンプルな原理で、この画面の背後に隠れているフィッシング犯に本人認証データを盗まれることはありえません。

アクセス毎に画像配置が変る方式で運用されていると、ユーザは一度アクセスして認証画面を表示させた上でログオフし改めてアクセスした時に前回と同じ配置で表示されていれば、これは偽サイトであると判定できます。フィッシング犯としては個人別認証画面の準備に加えて画像のランダム配置機能までを盛り込んでおかねばユーザ認証データを盗むことはできないのですから、多人数を対象とするフィッシング偽画面の作成コストは更に高くなります。

このフィッシング排除効果を内在させたオリジナル画像を使うユーザ認証手法は、（これまではフィッシング排除機能を声高に謳うことはしていませんが）日本のあるオンライン決済システムの標準ユーザ認証手段として２００４年秋から運用されています。

３．メリット・効果の範囲

・不特定多数を対象とする経済犯的フィッシングに対しては全般的な有効性があると考えられます。

・ユーザ認証手段そのものがフィッシング排除機能を備えているので、ユーザが登録したキーワードを表示するもの、ユーザが指定した色や紋様で認証画面の背景を表示するもの、ユーザが指定したアイコンを画面の一角に表示すもののようなフィッシング排除目的の別手段を追加するコストは発生しません。

・サーバ認証が無力化された状況（注１）を想定しても有効性は損なわれません。

４．デメリット・効果の限界

・コスト無視の特定個人狙い撃ちの攻撃者に対しては有効ではありません。より高レベルの方策が必要です。（注２）。

・中間者攻撃を排除する機能はありません。中間者攻撃の脅威が広まってくれば中間者攻撃防止技術との組み合わせが望まれます（注３）。

・「トロイの木馬型」の悪意ソフトによる本人認証データの盗難に対する有効性はありません。別の方策が必要です。（注４）

５．課題

フィッシング被害の甚大な欧米では認証画面カスタマイズの効果は広く知られているようですが、日本ではこうした対策技術の存在自体が殆ど知られていません。フィッシング以外のネット犯罪の方が目立っている現状では一般ユーザへの広報を急ぐ必要まではないと思いますが、サービス事業者への情報提供は進めておくのが望ましいと考えます。

補注説明

注１：　サーバ認証が無力化された状態とは

例えばＡネット銀行のユーザに対するフィッシングを計画する攻撃者は先ずＡネット銀行のユーザとして登録し実際に取引を行います。そうするとアクセスから始まり取引完了までの全ての画面を自由にいくらでも見ることができます（つまり、全ての画面をキャプチャできます。キャプチャ抑止機能を備えたサイトであっても画面を高精度デジカメで撮影し後で編集することを妨げることまではできません。）

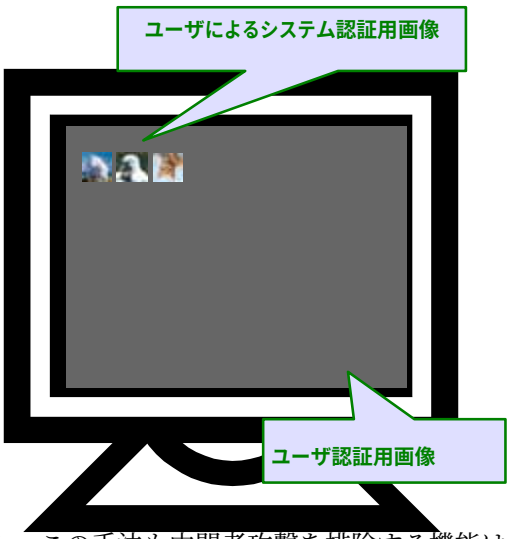
全ての画面というのは、画面右下に鍵アイコンが表示されている画面、鍵アイコンをクリックした後の証明書が表示された画面、証明書の拇印が表示された画面、更には「このサイトの安全性は確認されました」といった表示や同趣旨のマークのある画面、なども含みます。

このようにして収集した本物画面のコピーをアクセスしてきたユーザの端末に本物と同じ順序とタイミングで送出できる技能を持つ攻撃者がいると仮定します。すると、いくらサーバ認証技術が間違いのない信頼できるものであっても、画面上の表示しか頼るもののない一般のユーザには偽サーバを見分けることはできません。

端末上に常駐するサーバ認証ソフトが接続時にサーバの真贋を判定する場合も、「真」との判定はしていないのに、偽サーバから「真」と判定した時の画面を強制的に表示されてしまう可能性も考えられないことではありません。攻撃者側の急速な技量向上を考えると、現時点では考え難いことであっても先回りした対応を準備しておくことは無益ではないと考えます。

注２：　特定個人狙い撃ちのフィッシング攻撃

個人別カスタマイズされたユーザ認証画像に加えて、個人別カスタマイズされたサーバ認証画像を用意し、両者に関わる情報をキャッチボールのように多段階で双方向にやり取りすることによって特定個人狙い撃ちフィッシングを排除する手法が既に確立されています。個人別にカスタマイズされた認証画面を使ってユーザ認証とサーバ認証を交互に繰り返すと、ユーザを欺瞞する行為とサーバを欺瞞する行為を交互に繰り返す執拗な攻撃者を、繰返し回数分だけ排除する機会が発生するというものです。



A.　サーバから端末にはサーバ認証シンボルが送り出され端末画面の左上に逐次表示されています。これをユーザが見覚えのあるものとして再認できるか否かでユーザがサーバの真贋判定を行ないます。

B.　端末画面右下の認証画面からユーザの再認により選択されたユーザ認証シンボルが端末からサーバに送出され、サーバに登録してあるユーザ認証データとの照合が行なわれます。

A と B のキャッチボールによる多段階相互信頼度向上プロセスを経て相互認証に至ります。どんなに奸智に長けた攻撃者も技術以前のロジックの運用で途中で排除されることになります。

但し、この手法も中間者攻撃を排除する機能はありません。中間者攻撃を視野に入れると端末・サーバ間の相互認証・暗号化通信との組み合わせが必要となります。

注３：　中間者攻撃防止技術

サーバ上のソフトと端末上のソフトがお互いの秘密情報を知ることなくその真正性を確認し、その秘密情報と一時乱数から通信暗号化のための鍵を生成する Authentication Key Exchange　/　Establishment と呼ばれる技術などが知られています。（日本では産業技術総合研究所・情報セキュリティ研究センターなどで研究中）

注４：　「トロイの木馬」型悪意ソフトへの対抗技術

ユーザの端末に潜伏してユーザが入力する本人認証情報を取得して外部に送信する「トロイの木馬」型の悪意ソフト（マルウェア）は先ずは侵入を防止し、万が一侵入を許したものは完全に駆除できることが望ましいのですが、駆除しきれない状況も想定しておく必要があります。対策を２件ご紹介します。

使い捨て乱数を携帯電話で受信する方式：　携帯電話はマルウェアに対してＰＣよりも相対的に安全性を高く維持できることを前提にしたモデルです。暗証番号・パスワードの代わりに使い捨て乱数を照合データとして使います。使い捨て乱数は使用直後（＝攻撃者に取得された時）には既に無効になっています。使い捨て乱数を受信する携帯電話の利用者認証の強弱がシステム全体の強弱を決定することになりますので、望ましくは利用者認証をフィッシング排除効果を内在させているオリジナル画像利用本人認証手法で行います。

本人認証専用の IC カードを使用する方式：　CPU・大容量メモリー・表示/入力機能・電源制御機能のある次世代 IC カード或いは同等機能を持つ携帯デバイスに、電子証明書・暗号化通信と PKI ユーザ秘密鍵の復元・消滅機能を搭載します。悪意ソフトの潜伏する端末を想定しても、ユーザの電子証明書の内容が悪意ソフトに読み取られることがない状態を確保しながら、個々のユーザの実在確認と本人認証を行うことができるようになります。実際の運用に必要な匿名での個人情報管理方法を含め技術要素は日本国内に揃っています。

以上

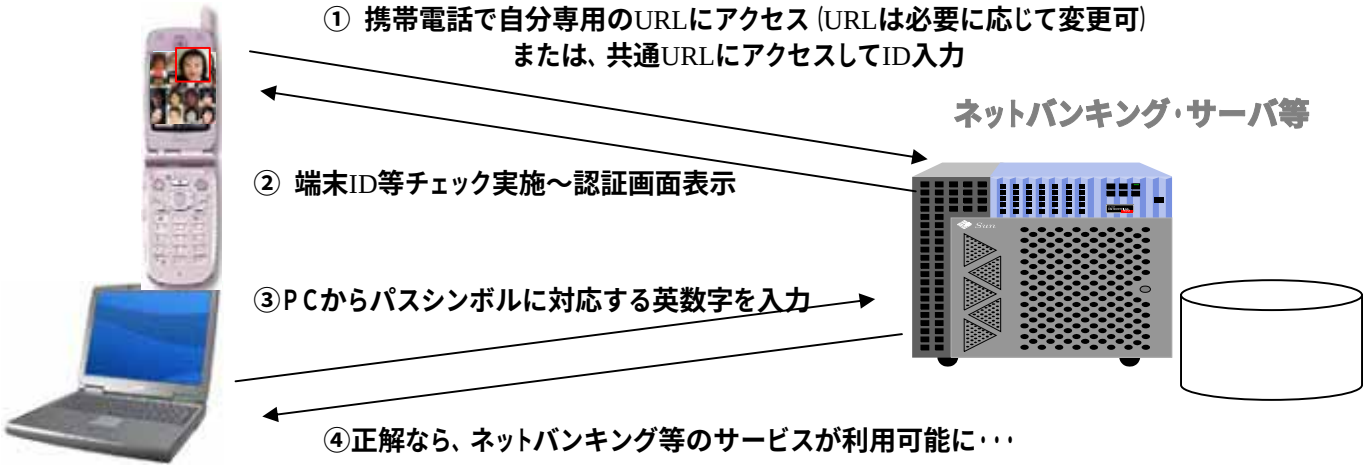
資料４

2経路2端末 画像認証
ワンタイム暗証番号携帯電話生成*方式
フィッシング･スパイウェア等を無力化

株式会社ニーモニックセキュリティ
國米　仁

ユーザ認証にはフィッシング排除機能を内在する
オリジナル画面活用型の画像認証を使用

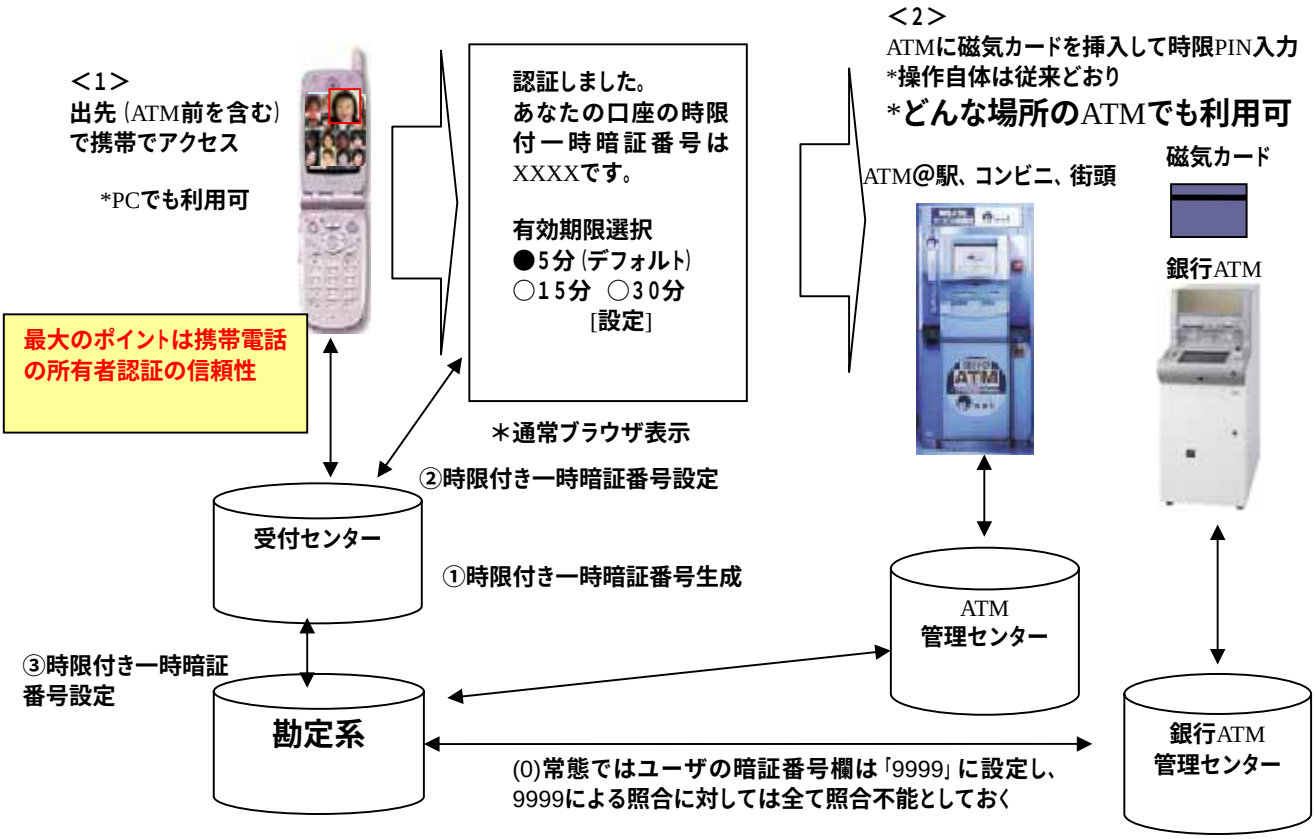
携帯電話上の
画像は毎回ランダムに表示される
画像位置の英数字は常に固定。
↓
ＰＣに入力され別経路で送信される認証データは
ユーザの記憶・意思を反映した秘密情報としての
ワンタイム暗証番号。



- 認証画像と対応する英数字は毎回変更される（画像の表示配列を毎回変更）
  → OTP 機能
- PC または携帯にスパイウェアが仕込まれていても両方同時に情報を盗まれなければ被害は防げる
  → マルウェア対策
- 盗聴システムが仕掛けられていても、両方同時に情報を盗まれなければ被害は防げる
  → 盗聴、中間者攻撃対策
- ＰＣのみならず、ＡＴＭ・ＣＡＴ・電子錠などにも対応可能。

注）ワンタイム暗証番号携帯電話生成： 携帯電話の画面に毎回配置を変えて表示される認証画像と各画像に割り振られた英数字を視認したユーザが自分の記憶と照合してワンタイム暗証番号を生成するもの

2経路2端末 画像認証
時限付きワンタイム暗証番号携帯電話受信方式
ATMなどの盗聴･盗撮を無力化



システムの動き： (0)→①→②→③→(0)
ユーザの操作： ＜1＞ → ＜2＞

ＰＣ、暗証番号対応クレジットカード支払端末、電子錠なども同様の扱いが可能

・一時暗証番号は使用時に無効となり 9999 に復帰。時限内に使わなければ 9999 に復帰。

・携帯電話によるアクセスまでは、本人・他人を問わず支払・出金は一切不可能なモデルなので、全体の強度は携帯電話の所有者認証の強度によって決定される。

・カード偽造問題は雲散霧消するので今のままの磁気カード、今のままのＡＴＭ／ＣＡＴを使い続けられる。

・受付センターの構築と勘定系ソフトの小規模な改変だけという極小のコストで暗証番号の運用に関わるセキュリティレベルを包括的に向上させることが可能。

資料5

使いやすくフィッシングに対しても安全な通信路を作成する方法 PAKE/LR-AKE のご紹介

独立行政法人 産業技術総合研究所
情報セキュリティ研究センター
古原 和邦

１．はじめに

盗聴、改ざん、なりすましなどの不正が行われる可能性のあるインターネットにおいて、インターネットバンキング、オンライントレード、有線・無線ネットワークへの接続、社外から社内ＬＡＮへのログインやリモートサーバへのログインなど、各種サービスを利用・提供する際に欠かせない技術が認証付き鍵共有技術である。認証付き鍵共有を用いれば通信相手の認証が行え、かつ、その通信相手との間に安全な通信路（暗号化および改ざん検出の施された通信路）を設立することができる。しかしながら、現在広く普及している PKI(Public-Key Infrastructure：公開鍵基盤)を用いる方式はフィッシングなどの被害を受けやすかったり、証明書の検証や管理が煩わしかったり、情報漏えいに対して脆弱であったりするなどの問題点がある。本稿では、これらの問題点を克服する１つの方法として PAKE(Password Authenticated Key-Establishment) および LR-AKE(Leakage-Resilient Authenticated Key-Establishment)を紹介する。

２．現代暗号と PKI の歴史の概略

本章では､PKI を用いた認証付き鍵共有方式が普及し問題点が明るみに出るまでの経緯を｢現代暗号および PKI 誕生の時代｣､｢PKI 普及の初期段階｣､｢PKI の実運用を踏まえた上での見直しの時代｣に分け紹介する。なお、現代暗号とは計算機の利用により可能となった複雑な演算を用いた暗号のことを指す。

２．１　現代暗号および PKI 誕生の時代

現代暗号および PKI 誕生の歴史は１９７０年代頃までさかのぼる。１９７６年に公開鍵暗号の概念および Diffie-Hellman 鍵共有方式が Diffie と Hellman により提案され[DH76]､１９７７年に RSA 公開鍵暗号が Rivest、Shamir、 Adelman により提案されている[RSA77]｡また、１９７７年には DES(Data Encryption Standard) が米国標準暗号として FIPS(Federal Information Processing Standards)化[12]されている。１９７８年には、信頼できる第三機関が公開鍵と ID などの情報に電子署名を付けることで公開鍵に対応する秘密鍵の持ち主を保障する PKI（Public-Key Infrastructure）の概念を Kohnfelder が提案している[Koh78]｡また、少し遅れて１９８５年ころに Miller および Koblitz によりそれぞれ独立に楕円曲線暗号を提案している[Mil85,Kob87]。この１９７０年～１９９０年までを「現代暗号および PKI 誕生の時代」とよぶことにする。

２．２　PKI 普及の初期段階

「現代暗号および PKI 誕生の時代」に提案された現代暗号や PKI が実際に広く普及し始めるのは、１９９０年代に入ってからである。電子メールや World Wide Web が普及し始め、暗号化や認証の重要性が一般に認識さ

[12] 残念ながら DES は鍵長が 56 ビットと短く、鍵の全数探索を受ける危険性があるため２００５年に FIPS から取り下げとなっている。現在の米国標準共通鍵暗号は２００１年に FIPS 化された AES(Advanced Encryption Standard)である。

れ始めてからである。この１９９０年～２０００年までを「PKI 普及の初期段階」とよぶことにする。この時代には、例えば、１９９１年に電子メールなどを暗号化するためのツール PGP のバージョン 1.0 がリリースされ、１９９４年にはトランスポートレイヤの通信を暗号化するため仕様 SSL（Secure Socket Layer）のバージョン 2.0 が公開されている。SSL はその後１９９６年にバージョン 3.0 が公開され、１９９９年には TLS(Transport Layer Security)バージョン 1.0 が RFC2246 として IETF において標準化されている。SSL および TLS（以下 SSL/TLS）はウェブ上において各種サービスを安全に提供する際に広く利用されていることはもちろん、VPN(Virtual Private Network)を構築する際などにおいても利用されており、現在のネット社会を支える上で欠かせない技術の１つとなっている。

２．３　PKI の実運用を踏まえた上での見直しの時代

２０００年以降は「PKI の実運用を踏まえた上での見直しの時代」とよぶことができる。インターネットが広く一般に浸透したことにより、PKI も老若男女を問わず多くの人に利用されるようになった。これに伴い PKI に対する認識不足や不適切な運用などから、問題も生じてきている。実際、２００３年ころからフィッシング詐欺や情報漏えい事件が増加してきており、PKI に対してもその適切な運用方法の見直しが求められている。

以降では、まず、第３章で PKI や PKI を用いた認証付き鍵共有方式の概要について説明し、第４章でそれらの注意点や問題点についてまとめる。そして、第 5 章でそれらの問題点を解決する方式として PAKE(Password Authenticated Key-Establishment)と LR-AKE(Leakage-Resilient Authenticated Key-Establishment) を紹介する。

３．PKI および PKI に基づく認証付き鍵共有方式

暗号方式には大別して、共通鍵暗号（対称鍵暗号や秘密鍵暗号ともよばれる）と公開鍵暗号（非対称鍵暗号ともよばれる）がある。共通鍵暗号は暗号化と復号の鍵が同じ方式であり、公開鍵暗号は暗号化鍵から復号鍵を推測することが難しい方式である。そのため、攻撃者が盗聴しか行わないと仮定した場合、公開鍵暗号の暗号化鍵は盗聴の行われている通信路を使ったとしても安全に送信することができる。しかしながら、攻撃者が盗聴以外に書き換えや成りすましを行う場合、暗号化鍵を送信するのみでは不十分である。攻撃者は自分の公開鍵を他人の公開鍵とすり変えたり、自分の公開鍵を他人のそれとして公開したりすることができるからである。これを防止する１つの方法が PKI であり、PKI では信頼できる第三機関（認証機関や認証局などともよばれる）が公開鍵とその秘密鍵の持ち主、有効期限などの情報に対して電子署名を施す。公開鍵の利用者は、予め信頼できる第三機関の署名検証鍵を手渡しなどの改ざんされない方法で入手しておき、相手の公開鍵を受け取った際にはそれに付いている電子署名を検証する（図 8-1 参照）。これにより公開鍵が誰のものであるかを確認することができる。

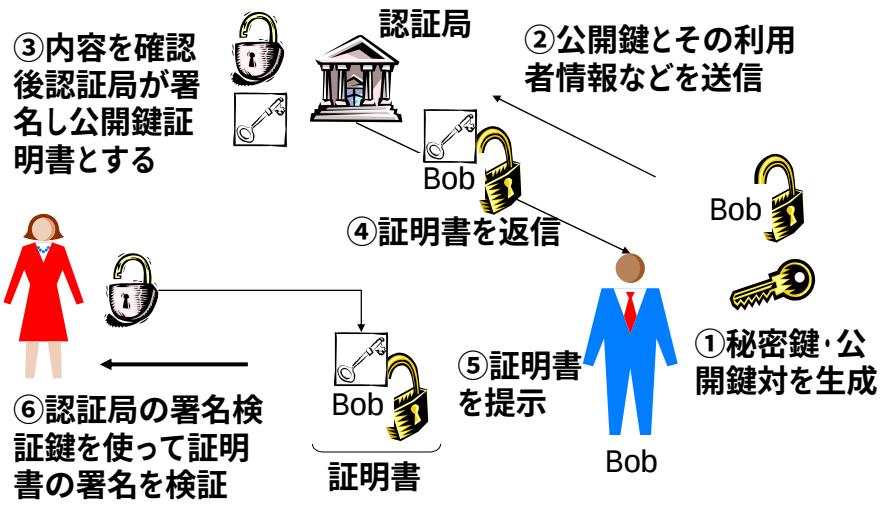


図 8-1 認証局による公開鍵証明書の発行と利用

相手の公開鍵を安全に入手できれば、それを使って相手を認証したり、鍵を共有したりできる。実際、SSL/TLS を始め多くのセキュアプロトコルでは、PKI に基づく認証付き鍵共有方式が採用されており、それらは大きく以下の２種類に分類することができる。

１）サーバ認証

２）相互認証

サーバ認証の概要を図 8-2 に示す。サーバ認証ではサーバ（と認証局）のみが秘密鍵・公開鍵対を持ち、各サーバは自分の公開鍵に対して認証局より発行してもらった公開鍵証明書を持つ。一方、クライアントは、サーバの公開鍵証明書を検証するための認証局の自己証明書を持つ。クライアントがサーバに接続すると、サーバは自分の公開鍵証明書をクライアントに送信し、クライアントは提示された公開鍵証明書の記述や電子署名に問題がないか確認する。問題がなければ、共有鍵の種となる乱数をその公開鍵で暗号化しサーバに送信する。通信相手が正しいサーバであればその送信した乱数を復号できるため、両者で同じ鍵を共有できる。共有された鍵は、暗号化や改ざん検出の施された安全な通信路を作成するために利用される。サーバ認証後にクライアント認証を行いたければ、設立された安全な通信路でクライアントがサーバにパスワードを送信しパスワード認証（Basic 認証）を行うことも可能である。

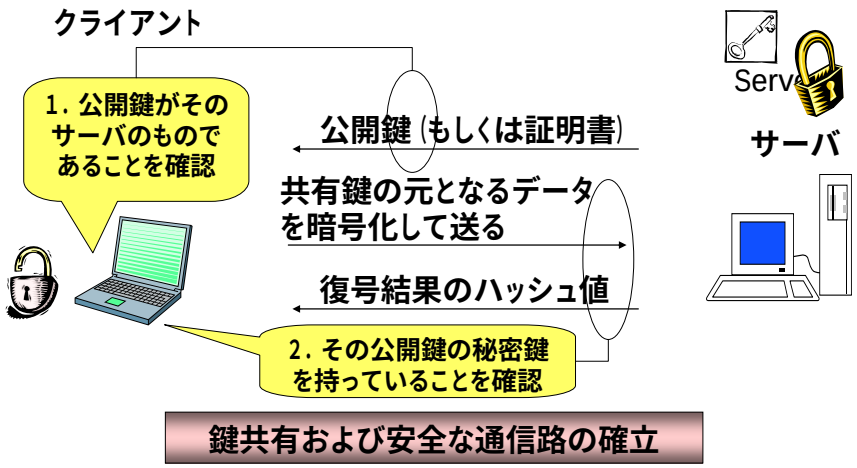


図 8-2 サーバ認証の概要

図 8-3 は相互認証の概要を示す。相互認証ではサーバとクライアントの両者（と認証局）が秘密鍵・公開鍵対を持ち、サーバ認証に加えてクライアント認証も行われる。クライアント認証はクライアントが自分の公開鍵証明書と送受信通信データに対するデジタル署名をサーバに送信し、サーバがそれらを検証することで行われる。

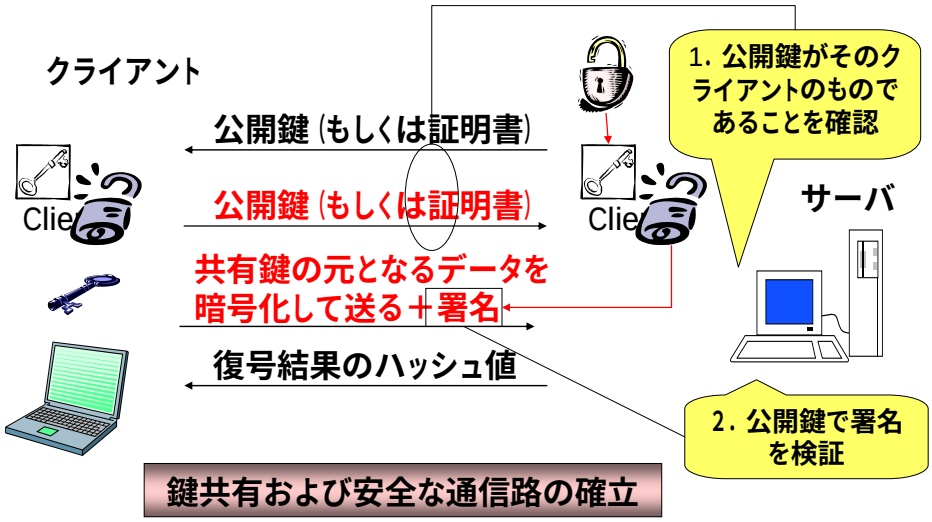


図 8-3 相互認証の概要

４．PKI に基づく認証付き鍵共有方式の問題点

前章で述べたとおり、PKI を用いれば信頼できる第三者機関が証明書を発行したサーバとの間で安全に鍵共有が行える。そのため、安全に鍵共有を行うという問題は理論的には解決されている。しかしながら、PKI が広く一般に普及するにつれ、実運用上の問題点がいくつか浮かび上がってきている。

まず、サーバ認証後に利用者のＩＤ、パスワードを検証する場合の１つ目の問題点は以下のとおりである。

問題点１：サーバの管理者の不正あるいはサーバ側からの情報漏えいに弱い。

これは、サーバに保存されているデータを解析すると利用者のパスワードが分かるという問題である。通常、利用者のパスワードはそれほど長くないため、パスワードの検証データを入手できた攻撃者は、パスワードの候補をオフラインで大量に試すことで利用者のパスワードを特定できてしまう。さらに、利用者がそれと同じＩＤ、パスワードを他のサイトでも利用していた場合、被害は他のサイトへも飛び火する可能性がある。なお、被害の飛び火は、サイト毎に異なる推測しにくいＩＤ、パスワードを設定することで回避できるが、利用者が記憶すべき情報が増えるという問題点が残り、逆に、各サイトの ID、パスワードを個人のパスワードで暗号化した場合にはその暗号文の漏洩・解析に弱くなるという問題点が残る。その上、利用者が他のサイトのパスワードを間違ってそのサイトに打ち込んだ場合、それがサーバに伝わるという問題もある。

２つ目の問題点は以下の通りである。

問題点２：証明書の発行・検証・管理等の処理が一般の方には理解しづらく、また、煩わしいこともあり、利用者が偽の証明書を受け入れてしまう可能性がある。

通常、偽の証明書が利用者に提示された場合図 8-5、図 8-4 のような警告画面（Internet Explorer (IE)の場合）が表示される。この警告は、以下のいずれか１つでも満たされると表示される。

１）提示された証明書の電子署名をクライアントの持っている信頼できるルート認証局もしくはそのルート認証局が信頼する中間認証局の署名検証鍵で検証できない。
２）証明書の有効期限が切れている。
３）打ち込んだ URL が証明書内の記述と一致していない。

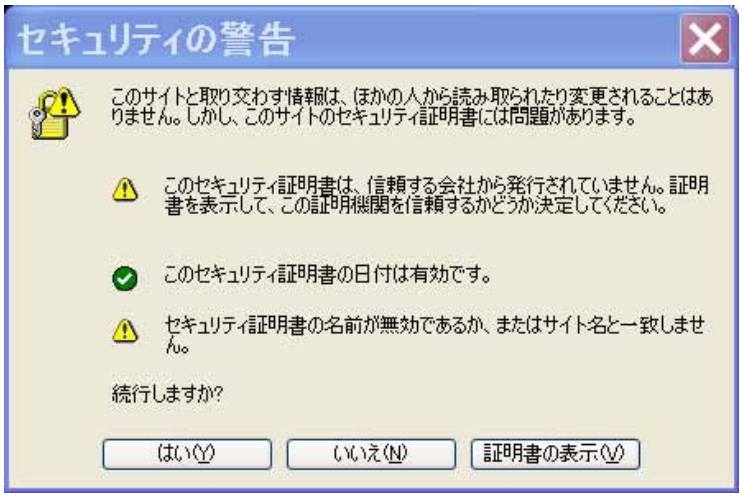


図 8-4 証明書検証時の警告画面の例（IE6 の場合）

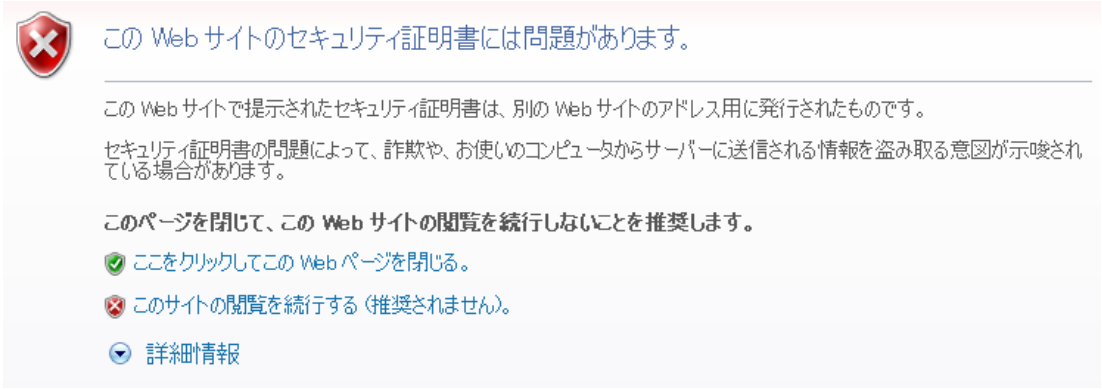


図 8-5 証明書検証時の警告画面の例（IE7 の場合）

しかしながら、多くの場合、この警告を無視して閲覧を継続すると必要なページへ接続できるため、これらの警告は無視される傾向にある。そのため、各種サイトにおいて警告を無視しないように教育や啓発が行われていたり、警告を無視してページに接続した場合には、図 8-6 のようにブラウザの見た目を変えるなどの工夫が施されたりしている。しかしながら、攻撃者の提示した偽の証明書を受け入れるかどうかの判断は最終的に利用者に任されており、サービス提供者側では確認や制御ができないという問題点が残り、また、攻撃者が警告の表示されない証明書を入手し、利用者に提示する場合もあり、警告を無視しないだけでは対処できないという問題も残る。

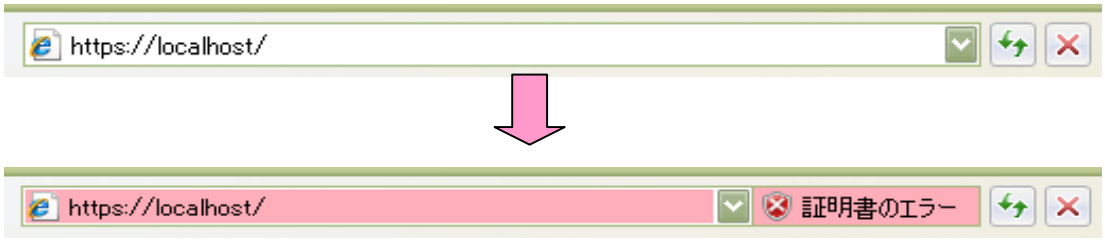


図 8-6 警告を無視してサーバに接続した場合に見た目を変える機能の例（IE7 ではアドレスバーの色が変わる）

利用者が攻撃者の提示した証明書を受け入れた場合、暗号化された通信路は攻撃者のサーバへと張られる。そのため、利用者の打ち込んだパスワードやクレジットカード番号などの入力情報は攻撃者に取られてしまう。その上、図 8-7 に示すように、攻撃者が入手した情報を使って本物のサーバへログインしその結果を利用者に転送した場合、利用者には本物のログインページが表示されるため、利用者は攻撃者のサーバにつながったことを認識できなくなる。この攻撃は、中間侵入攻撃と呼ばれている。

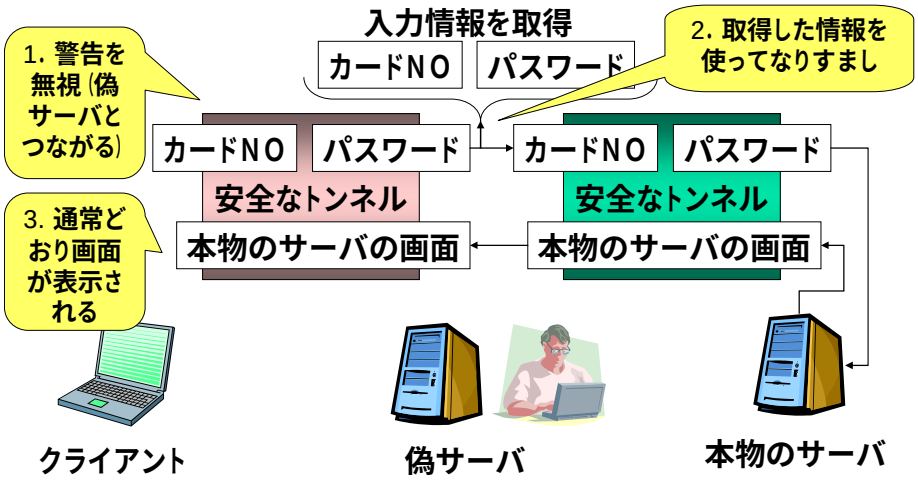


図 8-7 中間侵入攻撃の一例

なお、利用者が警告を無視してしまう背景の一つには、独自に発行した自己証明書を利用している（悪意のない）サーバが存在していることが挙げられる。本来、自前の証明書を使う場合には、それを検証するための情報（自己証明書やその拇印）を利用者に改ざんされない方法（例えば手渡しなど）で渡し、その情報を基にネットワーク経由で提示された証明書を検証させる必要がある。しかしながら、全ての利用者にこの処理を徹底させることは容易ではない。利用者の負担を軽減させるには、ブラウザにプレインストールされている信頼できる認証局の発行した証明書をサーバが利用すればよい。ただし、そのような証明書の発行にはコストが掛かるため、収益の低いサービスやボランタリーなサービスでは利用しにくい。また、証明書を低料金で発行する場合、証明書の発行基準が甘くなるという問題点がある。

PKI のもう一方の認証方式、相互認証についてであるが、これを用いると問題点１の利用者のパスワードが分かるという問題点が解決できる。相互認証では利用者の公開鍵がサーバに置かれるため、その情報が解析されたとしても秘密鍵やパスワードの情報を得ることはできない。ただし、サーバ認証と同様に利用者が偽の証明書を受け入れてしまうと、その他の入力情報（例えばクレジットカード番号など）が取られるという問題までは解決されない。その上、PKI のサーバ認証＋パスワード認証の組み合わせと比べて新たに以下の問題が生じることとなる。

問題点３：鍵を記録するための何らかのデバイスを所有しなければならない。
問題点４：その所有物の盗難や紛失に弱い。

問題４に対しては、秘密鍵を耐タンパーモジュールに格納したり、パスワードで暗号化したりすることも可能であるが、完璧な耐タンパー性を安価に実現することは容易でなく、また、パスワードで暗号化された秘密鍵を攻撃者が入手すればオフラインでパスワードの全数探索が可能となる。（これを避けるために必要となるパスワードの長さについては次章を参照のこと。）

サーバ認証＋パスワード認証、相互認証（および次章で紹介する方式）の問題点を表 8-1 にまとめる。表 8-1 からも分かるようにサーバ認証＋パスワード認証および相互認証にはそれぞれ一長一短があり、いずれも理想的な解決策となっていないことが分かる。

表 8-1 方式の比較（○：問題なし、△：多少問題あり、X：問題あり）

ヒカクコウモク / 方式	1:サーバ管理者が利用者のパスワードを知りえる問題	2:偽証明書受け入れ後に入力情報(クレジット番号など)が取られる問題	3:所有物が必要となる問題	4:盗難された所有物が悪用される問題	5:並列オンライン攻撃を受けるという問題	6:ID が平文で流れる問題	**7:送信されたごみに対してもサーバがべき剰余演算を実行しなければならない問題**
PKI(サーバ認証+PW 認証)	X	X	△*2	○	X	○	**X**
PKI(相互認証)	○	X	X	X	○	○	**X**
PAKE	X	○	○	○	X	X	**X**
LR-AKE	○	○	△*1,3	○	○	○*1	○*1

*1: 仕様書・実装版（現在準備中）で対応
*2: 正しい公開鍵を所有する必要がある
*3: 初回の接続では所有物が不要

５．使いやすくフィッシングに対しても安全な鍵共有方式 PAKE/LR-AKE

前章までで述べたとおり PKI を用いた鍵共有方式は、公開鍵を受け入れるか否かの判断が最終的に利用者に委ねられており、利用者の判断ミスがフィッシング詐欺を引き起こす原因の１つとなっている。

これに対して、公開鍵の検証をパスワードのような短い系列のみを使って行う方法が１９９２年に Bellovin と Merritt により発表されている[BM92,BM93]。この研究はその後、短いパスワードのみを使って安全に相互認証と鍵共有を実現するプロトコル PAKE (Password-Authenticated Key-Establishment)へと進化し、現在までに多くの研究が行われている。２０００年には、Bellare ら[BPR00]により安全性の形式化も行われ、また、DH(Diffie-Hellman)鍵共有をベースとする方式[Jab96,Jab97,KOY01,KI02,BCP04,Kwon05]や RSA 公開鍵暗号などの落とし戸付き一方向性関数をベースとする方式[MPS00,WCZ03,Zha04,Par07]など様々な PAKE が提案されている。２００３年には、PAKE の問題点を解決し、情報漏えいへの耐性を高めた LR-AKE(Leakage-Resilient Authenticated Key-Establishment)が提案されている。LR-AKE には DH 鍵共有ベースにした方式[SKI03]と RSA 公開鍵暗号をベースにした方式[SKI05]、さらに実装上の工夫が加わった仕様書版が存在している。

PAKE および LR-AKE を構成する際に注意しなければならない点は、秘密情報であるパスワードが短いためプロトコルの構成を誤るとオフラインでパスワードの全数探索が可能となることにある。なお、全数探索には大きく以下の３種類が存在し、適用できる全数探索の種類に応じて安全に使えるパスワードの長さが変わってくる。

１）オフライン全数探索（オフライン攻撃）
２）並列オンライン全数探索（並列オンライン攻撃）
３）直列オンライン全数探索（直列オンライン攻撃）

オフライン全数探索とは、攻撃者が通信路を盗聴したり、サーバあるいはクライアントに成りすましたりしてパスワードと関連のあるデータを入手し、それを利用してオフラインで並列かつ大量にパスワードを試す攻撃である。この攻撃は非常に多くのパスワードを試すことができ、また、そのことをサーバやクライアントに秘匿できるため非常に強力である。

一方、オンライン全数探索とは、実際に認証相手と通信を行うことによりパスワードの候補を一つずつ試す攻撃である。直列オンライン全数探索は１つのアカウントに対して連続して候補を試す攻撃であり、並列オンライ

ン全数探索は複数のアカウントに対して同時かつ並列に候補を試す攻撃である。パスワードのみを安全性の拠り所とする場合、オンライン攻撃は避けられない。

前述のとおり安全に使えるパスワードの長さは、適用できる全数探索の種類により変わってくる。オフライン全数探索が適用できる場合、非常に長いパスワードを利用しなければならないが、そうでない場合にはパスワードを短くできる。ではどこまで短くできるだろうか？1つの目安を以下に示す。まず、パスワードの長さとその探索の難しさを図 8-8 に示しておく。横軸がパスワードの長さであり、縦軸がエントロピー、つまり、パスワードが均一かつランダムに選ばれた場合の $\log_2$(パスワードの候補数)を示す。線はパスワードを構成する各文字が選ばれる集合の大きさを示している。例えば、●に対応する線は数字だけからなるパスワードを示しており、■に対応する線は大文字のみあるいは小文字のみのアルファベットからなるパスワードを示している。

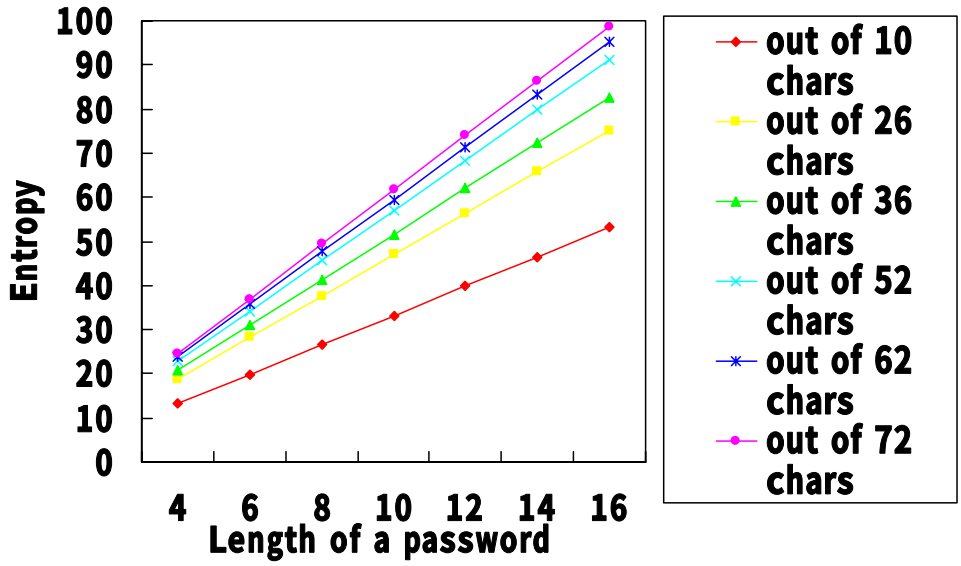


図 8-8 パスワードの種類・長さとその探索の難しさ

（パスワードが均一かつランダムに選ばれる場合）

現在、世界中でボランタリーに利用できる計算機を使って1年間に試すことのできる鍵の数は 2^{64} 程度と見積もることができる[Dis97]。また、1年間に1人の人間が許容できるリスクを 2^{-16} とする[13]と、オフライン全数探索が可能な場合に、高い安全性を満たすためには、少なくとも 80 < $\log_2$(パスワードの候補数)を満たす必要がある。ただし、オフライン全数探索に注ぎこめる計算量は年々増加しており、リスクも 1 年に限定することができないため、長期の安全性を確保するためにはこれより長いパスワードを使う必要がある。

IPsec の事前共有鍵方式や CHAP など、パスワードのみに安全性を依存する従来のパスワードベース認証あるいはパスワードベース認証付き鍵共有方式のほぼ全てがオフライン攻撃を受ける。そのため、それらを利用する際には非常に長いパスワードを利用する必要がある。これに対して、PAKE および LR-AKE ではオフライン攻撃に対して耐性を持つようにプロトコルが設計されているためより短いパスワードを安全に利用することができる。

オンラインでパスワードを試す場合であるが、仮に攻撃者が有効なアカウント ID を 1 つ入手できたとし、そ

[13] 交通事故死は1件でも許容できるものではないが、日本における平成１８年の交通事故死者数 6,352 人[Jiko]を単純に日本の総人口１億２千８百万人[Ppl]で割ると $2^{-14.3}$ となる。

のアカウントは 4 秒間に 1 回認証が行えるとすると、攻撃者は 1 年間でそのアカウントに対して最大 2^{21} 個のパスワードをオンラインで試すことができる。前の設定と同じく、1 年間に 1 人の人間が許容できるリスクを 2^{-16} とすると、直列オンライン全数探索に耐性のあるパスワードは $37 < \log_2$(パスワードの候補数)を満たすパスワードということになる。ただし、実際には、直列オンライン攻撃はサーバ側で検出可能であり、大量にパスワードが試される前に何らかの対処が可能である。そのため、直列オンライン全数探索に対してはこれより短いパスワードでも安全に利用できるようにすることができる。しかしながら、攻撃者が有効な ID を大量に入手でき、それらに対して並列にパスワードを試す場合、個人のパスワードが破られるリスクは同じでも、攻撃が成功する確率を大きくできる。例えば攻撃者が 100,000 個の有効な ID に対して高速かつ並列にパスワードを試す場合、攻撃成功確率は最大 100,000 倍となるため、それを 2^{-16} に抑えるためには、各パスワードを $56 < \log_2$(パスワードの候補数)を満たすように設定しなければならなくなる。

以上の説明を踏まえた上で、各プロトコルにおいて安全に利用できるパスワードの長さを表 8-2 にまとめておく。前述のとおり IPsec の事前共有鍵方式や CHAP などの従来のパスワードベースプロトコルは、オフライン攻撃を受けるためパスワードは非常に長いものを利用しなければならない。PAKE および PKI を用いたサーバ認証＋パスワード認証は、並列オンライン攻撃が可能なため中程度の長さのパスワードを利用する必要がある。ただし、サーバに保存してある情報が漏洩あるいは解析されると仮定した場合、それらの利用者は非常に長いパスワードを利用する必要がある。PKI を用いた相互認証の場合、利用者の所有物が盗難あるいは紛失しないと仮定するのであればパスワードは不要であるが、そうでない場合にはオフライン攻撃が可能となるため非常に長いパスワードを利用する必要がある。LR-AKE の場合、利用者の所有物が盗難あるいは紛失しないと仮定するのであればパスワードは不要であり、そうでない場合も直列オンライン攻撃が可能となるのみであるため、短いパスワードを安全に利用することができる。

表 8-2 各プロトコルにおいて安全に利用できるパスワードの長さ

プロトコル	パスワードの長さ	
	記録情報は漏洩しないと仮定した場合	記録情報が漏洩すると仮定した場合
従来のパスワードベースプロトコル	長	長
PAKE	中	長
LR-AKE	パスワード不要	短
PKI（サーバ認証+パスワード認証）	中	長
PKI（相互認証）	パスワード不要	長

長：オフライン攻撃を防げる長さ
中：並列オンライン攻撃を防げる長さ
小：直列オンライン攻撃を防げる長さ

その上、PAKE および LR-AKE では、図 8-10 に示すようにパスワードそのものを送信するわけではないため、偽サーバと通信したとしてもパスワードは相手に伝わらないことに加えて、相手が偽者であることも検出できる。また、証明書を検証したり、証明書や秘密鍵を管理したりする手間も省けるため非常に使いやすくなる。

これに対して PKI を用いたサーバ認証＋パスワード認証では、安全な通信路（トンネル）を作成するか否かの判断が最終的に利用者に委ねられており、利用者がこの判断を誤ると図 8-10 に示すように攻撃者との間に安全な通信路が張られ、結果としてパスワードやクレジットカード番号などの入力情報が取られてしまう。

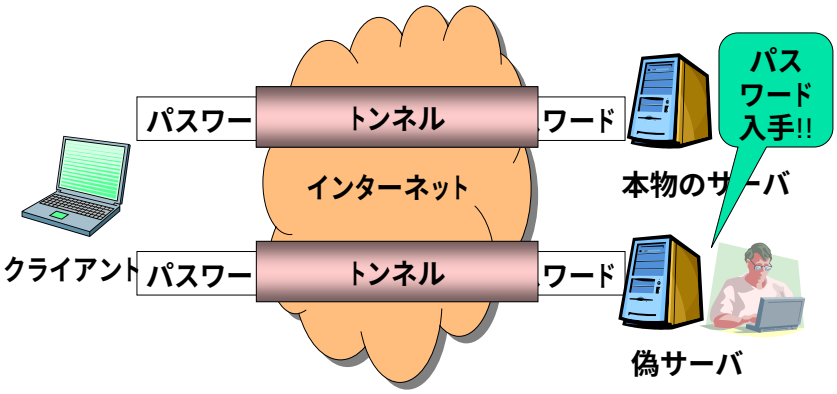


図 8-9 PKI サーバ認証におけるパスワード認証の概要（パスワードを相手に提示するため、偽サーバにつながるとパスワードやクレジットカード番号などの入力情報が盗られるという問題点がある）

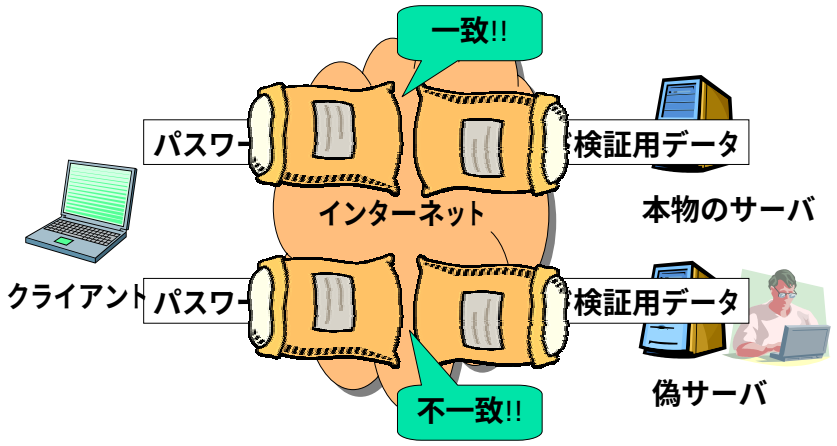


図 8-10 PAKE/LR-AKE におけるパスワード認証の概要（パスワードそのものを相手に提示しないため、偽サーバと通信してもパスワードは取られない。また、偽サーバの検出も可能）

ただし、PAKE を用いたとしても問題１は解決できないため、複数のサーバと通信を行なう場合、その数分のパスワードを覚えなければならない。加えて、PAKE には以下のような問題点がある。

問題点５：並列オンライン攻撃を受ける
問題点６：:ID が平文で流れる
問題点７：:送信されたごみに対してもサーバがべき剰余演算を実行しなければならない

問題点５は利用者がパスワードのみしか知らないという仮定の下では解決不可能であり、問題点６，７も効率のよい解決方法は知られていない。（なお、問題点６については、ID を送信せずサーバ側で ID を全数探索したり、サーバの公開鍵で ID を暗号化したりすることも可能ではあるが、両者共に計算量が増えるという問題点があり、

後者については、利用者が偽サーバの公開鍵を受け入れてしまうという仮定の元では有効な解決策となっていない。）そのため、PAKE では有効な ID が大量に攻撃者に入手される危険性があり、その分並列オフライン攻撃も適用しやすくなる。

これに対して、LR-AKE では問題点５，６，７を解決でき、また、記録情報も初回の認証時には不要となっている（表 8-2 参照)。LR-AKE はサーバへの不正侵入、記録情報の盗難いずれにも耐性を持っており、記憶情報（パスワード）と記録情報（所有物）を使う２要素認証を、最も効率よくかつ安全に実現している。さらに、RSA 公開鍵暗号ベースの LR-AKE は、PAKE や PKI ベースの認証付き鍵共有方式と比べクライアント側の処理を軽くできるという利点もあり、スマートカード、携帯電話、PDA などの小型デバイスで動作させる場合に有利である。

また、LR-AKE の仕様書版では単なる認証付き鍵共有機能だけでなく、データを安全に分散保存し、それを取り出す機能もある。近年、ビジネス継続性や災害復旧のために、データを暗号化しオンラインで遠隔地に分散保存することの重要性が増してきているが、そこで利用される認証鍵共有方式としてもデータを安全に分散保存できる LR-AKE の応用が期待できる。

LR-AKE の仕様書版および実装例等についてはいずれ（独）産業技術総合研究所、情報セキュリティ研究センターのホームページ[RCIS]で公開する予定であるので、詳細についてはそちらをご参照頂ければ幸いである。

６．まとめ

現代暗号および PKI の歴史の概略を紹介する共に、新たな潮流である認証付き鍵共有プロトコル PAKE と LR-AKE の紹介を行った。PKI は汎用的な方式であり、また、お互いに知らない２者を引き合わせる際には欠かせない方式である。しかしながら、既に知り合いとなっている２者間で利用するには必ずしもベストな解決策であるとは言えない。実際、フィッシングなどの問題も抱えており、その解決策が求められている。本稿では、既に知り合いとなっている２者間で相互認証を行いその間で安全な通信路を作成する方式として PAKE と LR-AKE を紹介した。PAKE は短いパスワードのみを利用する方式であるため、便利は良いが次のような問題点がある。１）サーバ側からの情報漏洩や管理者の不正に弱い。２）複数のサーバと通信を行なう場合、その数分のパスワードを覚える必要がある。３）アカウント ID が平文で流れてしまう。４）並列オンライン攻撃を受けてしまう。一方、LR-AKE では利用者は短いパスワードの他に記録情報を持たなければならないが、覚える情報は短いパスワード１つで済み、しかも、サーバ側、クライアント側いずれからの情報漏えいにも強くなり、また、オンライン攻撃も防ぐことができるという利点がある。

参考文献

[DH76] W. Diffie and M. E. Hellman. "New Directions in Cryptography," IEEE Transactions on Information Theory, vol.IT-22, No.6, pp.644-654, Nov, 1976.
[RSA77] R.L.Rivest,A.Shamir,and L.Adelman. “A Method for Obtaining Digital Signature and Public-key Cryptsystems,” MIT Laboratory for Computer Science, Thechnical Memo LCS/TM82, April 4,1977
[Koh78] L. Kohnfelder. “Toward a Practical Public-Cryptosystem,” Bachelor’s thesis, Dept. Electrical Engineering, MIT, Cambridge, Mass., 1978, pages 39-44.
[Mil85] V. Miller. “Use of elliptic curves in cryptography,” CRYPTO 85, 1985.
[Kob87] N. Koblitz. “Elliptic curve cryptosystems,” in Mathematics of Computation 48, 1987, pp. 203–209
[BM92] S. Bellovin and M. Merritt. ``Encrypted key exchange: Password-based protocols secure against dictionary attacks". In Proc. of IEEE Symposium on Security and Privacy, pp. 72--84, 1992.
[BM93] S. Bellovin and M. Merritt. ``Augumented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file compromise". In Proc. of the First Annual ACM Conference on Computer and Communications Security (CCS '93), pp. 244--250, 1993.
[Jab96] D. Jablon. ``Strong password only authenticated key exchange". ACM Computer Communication Review, ACM SIGCOMM, 26(5), pp. 5--20, 1996.

[Jab97] D. Jablon. ``Extended password key exchange protocols immune to dictionary attack". In Proc. of WET-ICE Workshop on Enterprise Security, 1997.
[MPS00] P. MacKenzie, S. Patel, and R. Swaminathan. ``Password-authenticated key exchange based on RSA". In Proc. of ASIACRYPT 2000}, pp. 599--613. Springer--Verlag, 2000.
[BPR00] M. Bellare, D. Pointcheval, and P. Rogaway. ``Authenticated key exchange secure against dictionary attack". In Proc. of EUROCRYPT 2000: LNCS 1807, pp. 139--155, 2000.
[KOY01] J. Katz and R. Ostrovsky and M. Yung. ``Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords" In Proc. of EUROCRYPT 2001: LNCS 2045, pp. 475-494, 2001
[KI02] K. Kobara and H. Imai. ``Pretty-simple password-authenticated key-exchange protocol proven to be secure in the standard model". IEICE Trans., E85-A(10):2229--2237, October 2002.
[WCZ03] D. S. Wong, A. H. Chan, and F. Zhu. ``More efficient password authenticated key exchange based on RSA". In INDOCRYPT 2003, LNCS 2904, pp. 375--387. Springer--Verlag, 2003.
[SKI03] S. Shin, K. Kobara, and H. Imai.``Leakage-resilient authenticated key establishment protocols". In Proc. of ASIACRYPT 2003: LNCS 2894}, pp. 166--172. Springer-Verlag, 2003.
[BCP04] E. Bresson, O. Chevassut, and D. Pointcheval. ``New Security Results on Encrypted Key Exchange". In Proc. of PKC'04, LNCS 2947, pp. 145--158, 2004.
[Zha04] M. Zhang. ``New approaches to password authenticated key exchange based on RSA". In Advances in Cryptology - ASIACRYPT'04, LNCS 3329, pp. 230--244. Springer--Verlag, 2004.
[Kwon05] T. Kwon. ``Revision of AMP in IEEE P1363.2 and ISO/IEC 11770-4
". IEEE P1363.2, June 2005.
[SKI05] S. Shin, K. Kobara, and H. Imai, “Efficient and Leakage-Resilient Authenticated Key Transport Protocol Based on RSA”, In Proceedings of the 3rd Applied Cryptography and Network Security 2005 (ACNS2005), LNCS 3531, pages 269-284, Springer-Verlag, 2005.
[Par07] S. Park. ``Efficient Password-Authenticated Key Exchange Based on RSA". In Proc. of CT-RSA 2007, Springer--Verlag, 2007.
[Dis97] ``RSA Labs' 64bit RC5 Encryption Challenge". http://stats.distributed.net/ 1997
[Acc] http://www.npa.go.jp/toukei/koutuu1/shisha.htm
[Ppl] http://www.stat.go.jp/data/nihon/zuhyou/n0200100.xls
[RCIS] AIST RCIS, http://www.rcis.aist.go.jp/index-ja.html

資料6

フィッシング･スパイウェアに関する法律･制度的状況－日本、米国、EU－

株式会社三菱総合研究所
吉永京子

１．フィッシング

(1) 日本

1)定義：

フィッシングとは、企業や組織などからの内容であると偽った電子メールを送りつけ、偽のホームページに接続させて、個人情報やクレジットカード番号、ログイン情報などを入手する詐欺行為のこと[14]。

2)我が国における事例

3)適用法令

金銭被害のないフィッシング：著作権法、不正アクセス禁止法違反

4)論点

・フィッシング詐欺というと、一見、詐欺罪に該当するかのように思えるが、金銭被害のないフィッシングは現行の刑法の詐欺罪（刑法 246 条）に該当しない。

【理由：詐欺罪は、人を欺罔して錯誤に陥れ、相手方にその錯誤に基づく処分行為（財産的処分行為）をさせて、財物（1 項詐欺）・財産上の利益（2 項詐欺）を行為者または第三者に移転させることによって成立するが、詐欺罪の客体は、財物（具体的な形をもつ固体や液体などの有体物）もしくは財産的利益であり、情報はこれに該当しない。】

⇒したがって、現在、金銭被害のないフィッシング行為については、2005 年 6 月の事案のように、著作権法や不正アクセス禁止法違反で対応されている。

・しかし、著作権法は、本来、著作者等の権利の保護を図ることを目的とする法律であり、それをフィッシングに適用するのは妥当かということ、また著作権法では、刑罰の程度を判断することができないということ、不正アクセス禁止法では、他人の ID とパスワードを入手しただけでは、同法違反に問われないなど問題がいくつか残る。

・ただし、日本では、欧米ほどフィッシング被害が出ていないこともあり、慎重な検討が必要である。

5)取組

○経済産業省－フィッシング対策協議会[15]を 2005 年 4 月に設置。
http://www.antiphishing.jp/aboutus/

○総務省－「フィッシング対策推進連絡会」[16]を 2005 年 1 月から開催。
http://www.soumu.go.jp/s-news/2005/050810_4.html

○警察庁－フィッシング 110 番[17]を設置。
http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm

---

14 総務省「国民のための情報セキュリティサイト」より。

15 http://www.antiphishing.jp/aboutus/

16 http://www.soumu.go.jp/s-news/2005/050119_4.html

17 http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm

(2) 米国

1)立法状況

・米国では、インターネット利用による ID 窃盗(identity theft)の被害件数が急増している。
・そのため、ID 窃盗抑止を目的とした様々な法案が提出されている。
・特に、 2005 年はＩD窃盗が頻発し、ID 窃盗につながるフィッシングやスパイウェアの取締りを強化する法案が連邦政府及び州政府レベルで次々に出された。[18]
・連邦レベルでは、未だフィッシング法は成立していないものの、州レベルでは、カリフォルニア州などフィッシング対策法が成立している。
・既存の法律（連邦法と州法の組み合わせ等）でも提訴できるが、フィッシング、スパイウェアに特化した法律を作ることによって、これらの問題に人々の関心を集めるという意図もあるようである[19]。

2)連邦法

3)州法

州の多くは、スパイウェア法でフィッシング対策の条項が盛り込まれているが、2006 年には少なくとも 12 州でフィッシング対策法案が提出され、7 つの州（コネチカット、ハワイ、ルイジアナ、ニューヨーク、オクラホマ、テネシー、ユタ）で成立している。

http://www.ncsl.org/programs/lis/phishing06.htm

・フィッシング対策条項を既存の州法に挿入している州：例）バージニア州
・フィッシング対策法を新たに立法する州：例）カリフォルニア州

4)取組

FTC では、消費者に、フィッシング被害に遭わないためのヒントを出すなど注意喚起している[20]。

・電子メール又はポップアップメッセージで個人情報又は金銭情報を聞いてきたら、答えたり、メッセージにあるリンクをクリックしたりしないこと
・エリアコードは間違った案内に導く。（フィッシング行為者がアカウントを更新するために電話するようにと電話番号を載せた電子メールを送りつける。 Voice Over Internet Protocol technology を使っているため、フィッシング行為者の場所は特定されない。）
・ウイルス対策又はスパイウェア対策ソフト、ファイアウォールを使い、定期的に更新すること
・個人情報や金銭情報を電子メールで送らないこと（ウェブで送る場合は、ブラウザのステータスバーで鍵のアイコンがあるか、https（s は secure の s)で始まるウェブサイトであることを確認すること。（ただ、残念なことに、いくつかのフィッシング行為者は、偽のセキュリティアイコンを持っている）
・クレジットカードと銀行口座のステートメントをチェックすること
・送信者が誰であるかに関わらず、受信した電子メールから添付資料を開いたりダウンロードしたりするときは注意すること（ウイルスやコンピュータのセキュリティを弱めるソフトウェアを含むことがある）
・フィッシングであるスパムは、spam@uce.gov とフィッシングの電子メールに記載されている当該企業、銀行又は組織に転送すること。
・詐欺に遭った(scammed)と思ったら、FTC に連絡し、FTC の ID 窃盗サイト（www.consumer.gov/idtheft）を訪問すること。

また、2006 年 5 月 10 日には、大統領令（Executive Order）により ID 窃盗タスクフォース（Identity Theft Task Force）を設立している[21]。

---

[18] 社会技術研究開発センター 「情報と社会」研究開発領域「第 1 回社会技術ワークショッツプ 複雑化する情報と社会そしてガバナンス」（2006 年 6 月 26 日）講演資料 http://www.ristex.jp/activity/joho.html

[19] Hunton & Williams LLP

[21] http://www.whitehouse.gov/news/releases/2006/05/20060510-6.html

(3) EU

EU レベルでは、フィッシングに関する立法は特にない。

取組としては、EuroISPA という EU のインターネット・サービス・プロバイダの団体が、2005 年 10 月より対フィッシングウェブサイトを eBay との協力により立ち上げ、フィッシング攻撃から消費者を守るため情報提供を行っている[22]。

2．スパイウェア

(1) 日本

1)定義

スパイウェアとは、ユーザの使用するコンピュータから、インターネットに対して個人情報やコンピュータの情報などを送信するソフトウェアのことである。一般的には、そのようなソフトウェアがインストールされていることや動作していることにユーザが気付いていない状態で、自動的に情報を送信するソフトウェアをスパイウェアと呼ぶ[23]。

2)事例

2005 年 11 月スパイウェアを使った事件の初摘発。

3)適用法令

不正アクセス禁止法、電子計算機使用詐欺罪

4)論点

現行法では、スパイウェア作成に対応できない。この点、現在、国会で、刑法を改正して、「不正指令電磁的記録に関する罪（いわゆるウィルス製造罪）」を新設することが審議されている（第 163 回国会より継続審議中）が、成立すると、スパイウェア作成に対応できる可能性はあるが慎重な検討が必要。

5)取組[24]

○内閣官房、警察庁、金融庁、総務省、経済産業省
「夏休み期間における情報セキュリティにかかる注意喚起」
http://www.meti.go.jp/press/20050720001/chuuikannki-set.pdf

○総務省「情報セキュリティサイト」
http://www.soumu.go.jp/joho_tsusin/security/enduser/ippan13.htm

○独立行政法人　情報処理推進機構
「パソコンユーザのためのスパイウェア対策 5 箇条」
http://www.ipa.go.jp/security/antivirus/spyware5kajyou.html

「スパイウェア対策のしおり」
http://www.ipa.go.jp/security/antivirus/shiori.html

(2) 米国

1)定義

米国では、法の適用対象となる技術の定義（特に、アドウエア(adware)を含むか否か）が立法作業上の難点とな

---

22 http://www.euroispa.org/antiphishing/index.html

23 総務省「国民のための情報セキュリティサイト」より。

24 社会技術研究開発センター 「情報と社会」研究開発領域「第 1 回社会技術ワークショップ　複雑化する情報と社会そしてガバナンス」（2006 年 6 月 26 日）講演資料より
http://www.ristex.jp/activity/joho.html

っている。
また、州によって定義が異なり、州をまたがって行動する企業にとって規制リスクと法遵守のコストが高くなっている。
2)連邦法（提出法案の概要は、パワーポイントを参照）
2006 年 12 月に、「S.1608 Undertaking Spam, Spyware, And Fraud Enforcement beyond Borders Act of 2005 (U.S. SAFE WEB Act)」が成立した。
目的：国境を越える詐欺、特に、スパム、スパイウェア、インターネット詐欺、欺瞞(deception)から消費者を守る。
内容：
・他国の法執行当局と一定の秘密情報のファイルを開示・共有することを許可する。
・スパイウェアやスパムに関する捜査について、FTC が他国の当局との捜査協力を可能とする権利を与える
等
参考：
http://www.ftc.gov/reports/ussafeweb/USSAFEWEB.pdf
http://www.ftc.gov/reports/ussafeweb/Summary%20of%20US%20SAFE%20WEB%20Act.pdf
3)州法
・2005 年には、12 州でスパイウェア法が成立。2006 年には少なくとも 18 の州で立法が検討されており、4 つの州（ハワイ、ルイジアナ、ロードアイランド、テネシー）で成立。
・スパイウェア対策法で訴えても良いし、 Unfair and deceptive で訴えても良い。どちらか高額のほうで訴える傾向にある。
カリフォルニア州では、スパイウェア対策法よりも Unfair and deceptive act(*注１)のほうが高額。逆に、ワシントン州とテキサス州は、スパイウェア対策法のほうが高額。
（※注１）FTC 法第 5 条の「不公正、欺瞞的な行為又は慣行(unfair or deceptive acts or practices in the marketplace)」の規定
・個人はスパイウェア対策法では訴えられない。（立証もできない）
州政府ないし検察官（attorney）が記録を求めることができる。
　平成 18 年度　技術・制度検討ワーキンググループ　特別セッション
（平成 18 年 11 月 28 日、 Ari Schwartz 氏の回答より）

（参考）
2006 年 8 月、Center of Democracy and Technology (CDT) は、州政府および連邦政府によりもたらされた事案についてレポートを出している：
CDT Spyware Enforcement Report
http://www.cdt.org/privacy/spyware/20060626spyware-enforcement.php

(3) EU
・電子通信分野におけるプライバシー保護指令(Privacy and Electonic Communications Directive)第 5 条第 3 項

・情報システムに対する非合法な攻撃に関する決定（2005 年 2 月） (Framework Decision on Illegal Attacks against Information Systems in February 2005 (FR))

資料7

パスワード管理とフィッシング対策

Stones International, Inc.
石田　公孝

1. はじめに

「山」と言えば「川」。一説によれば、この有名な合言葉は今からおよそ300年前の赤穂浪士の討ち入りの時に使われたものだという事です。考えてみればこの合言葉は当時のパスワードと言えるかもしれません。暗闇の中で、そこに居る人間が敵なのか、見方なのかを判定（認証）するために、この合言葉が必要だったわけです。ですから、まずは

パスワード　＝　認証のための何か　という風に広く捉えて考えます。

認証という作業、つまり、その人がその人であることを確認するという作業は、実は私たちの日常生活において絶えず行われているものであることに気づきます。私たちは普段、無意識のうちに相手が誰であるかを確認し、そしてその相手に応じて適切な行動を選択しています。相手が誰なのか、どのような立場の人なのかを理解することなく、行動を起こすことはできないと言ってもいいでしょう。

さて日常生活における認証作業の最も古典的な手がかりは顔や声です。一方討ち入りの例では「合言葉」という特別なものを用意しています。これは暗闇であったため顔での認証が困難であったからだと考えられます。

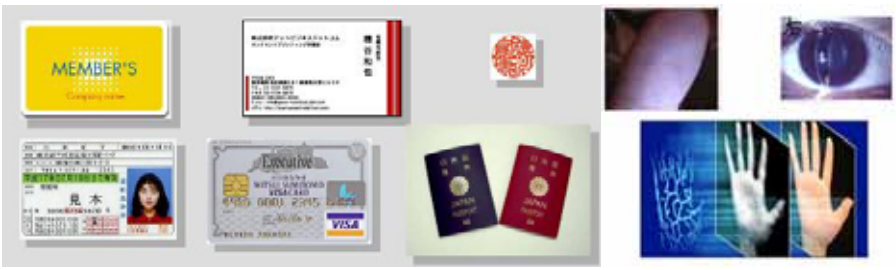
私たちの日常生活においても、顔と声では認証できない場合に対応していくつかの認証方法が採用されています。それは一般的には次の3つの方法です。

- 持っているもの

  <u>それを所有している　＝　その人である</u>

  という仮定に基づいて認証が行われます。例としてはメンバーズカード、名刺、印鑑、免許証、クレジットカード、パスポート等があります。

  なお免許証やパスポートではさらに顔写真を貼付することにより、顔での照合も可能になっています。



- その人本人であること（生体認証）

  <u>その人固有のもの　＝　その人である</u>

  という仮定により認証が行われます。具体的には指紋、虹彩、静脈等の生体の個体別の不変的な特徴を根拠にした認証方法です。

- 知っていること

  その事を知っている ＝ その人である

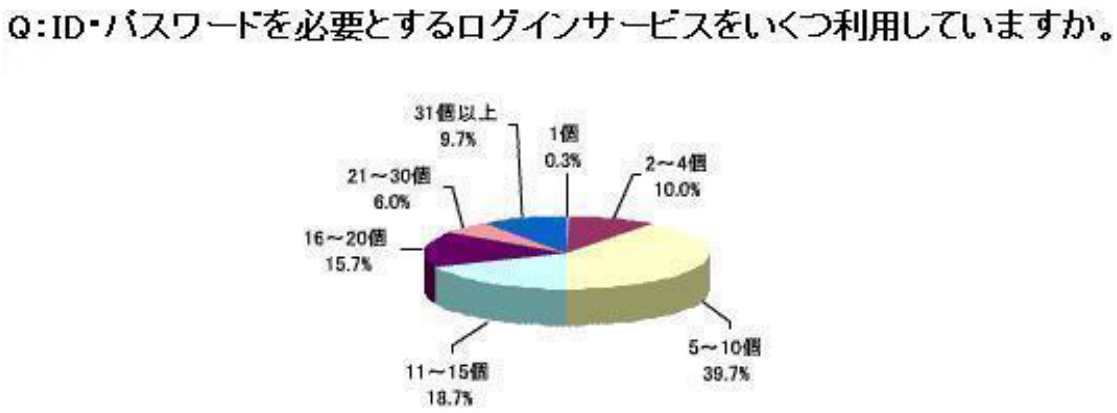
  という仮定に基づく認証です。 この例としては刑事物のドラマで犯人しか知りえない犯行現場の状況をその容疑者が知っていた、というところから犯人が逮捕されるという場面があります。

  またコンピュータ、そしてインターネット上で行われている認証として現在最も一般的に普及しているのもこの方法です。つまりユーザIDとパスワードによる認証です。

2. 増え続けるパスワード

さて、インターネットの発明により、私たちの従来の活動の多くは、インターネット上においても可能になってきています。銀行との取引、証券の取引、その他商品の売買、SNSなどインターネット上の各種サービスは益々多様化し、そして活発化しています。そして結果として認証に対する需要も増え続けています。

インターネットコム株式会社と株式会社インフォプラントが行った調査によれば、2005年時点で6割近い人が5個から15個のID・パスワードを必要とするサービスを利用しています。

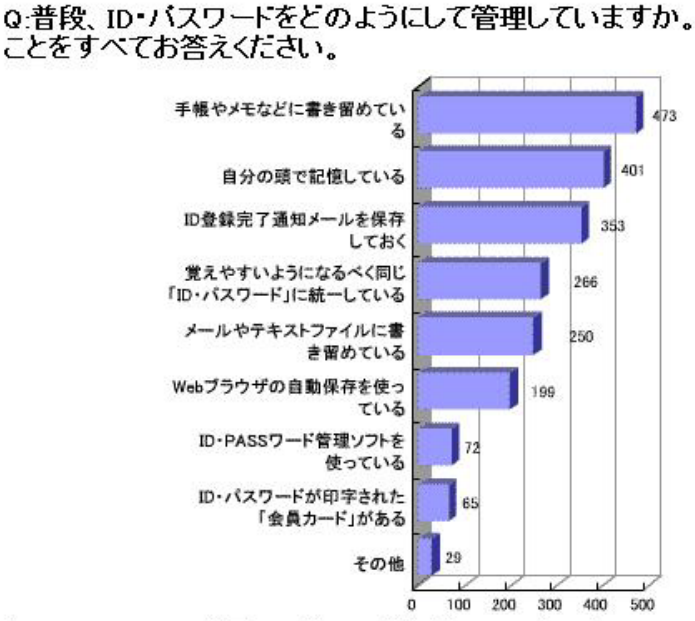


出典： 『ID・パスワードに埋もれる日々、90%以上が「忘れたことがある」』, japan.internet.com 編集部, 2005.9.9

一方、増え続けるこれらのID・パスワードをすべて記憶しておくのは容易ではありません。自分で記憶可能なパスワードの数は3個程度だという調査もあります。約6割の人が5個から15個のログインサービスを使用しているという現状において、実際に記憶可能なパスワード数が3個ということになれば、当然ながら複数のサイト向けにパスワードを流用することになります。セキュリティの観点からは、この現状は望ましいものではありません。

出典:『覚えられるパスワードは 3 つまで』, Yahoo！ニュース, 2006

次のグラフはパスワードをどの様に管理しているかを調査した結果です。この調査結果でも手帳やメモ、あるいはメールやテキストファイルに書き留めているといった方法が多数を占めています。



(2006/8/4～8/6 全国の20代～60代以上のインターネットユーザー1,091人)

出典：『「すべて違う ID・パスワードを利用」1 割以下、増え続けるログインサービス』, japan.internet.com 編集部, 2006.8.8

3. 良いパスワードとは

インターネット上のサービスにおける認証がパスワードに大きく依存している現状においては、パスワードの選定に注意が必要です。容易に推測されるようなパスワードは意味が無いからです。

良いパスワードの要件としては次のようなものがあります。さらに運用上の工夫として定期的にパスワードを変更することも重要です。

推測されにくいもの

長いパスワード（例：8文字以上）
大文字、小文字、文字や数字を混在
辞書に無い並び
自分では覚えやすい

定期的に変更

4. 利便性と安全性

推測されにくいパスワードを設定し、それらを定期的に変更しながら運用するということは、安全性を確保する上で極めて重要なことです。しかしながら実際に行うには多くの手間がかかります。

このような利便性と安全性のトレードオフを解決するためのツールとして、パスワード管理ソフトと呼ばれるソフトウェアが多数市場に存在します。これらのソフトウェアが提供する機能は以下のようなものです。

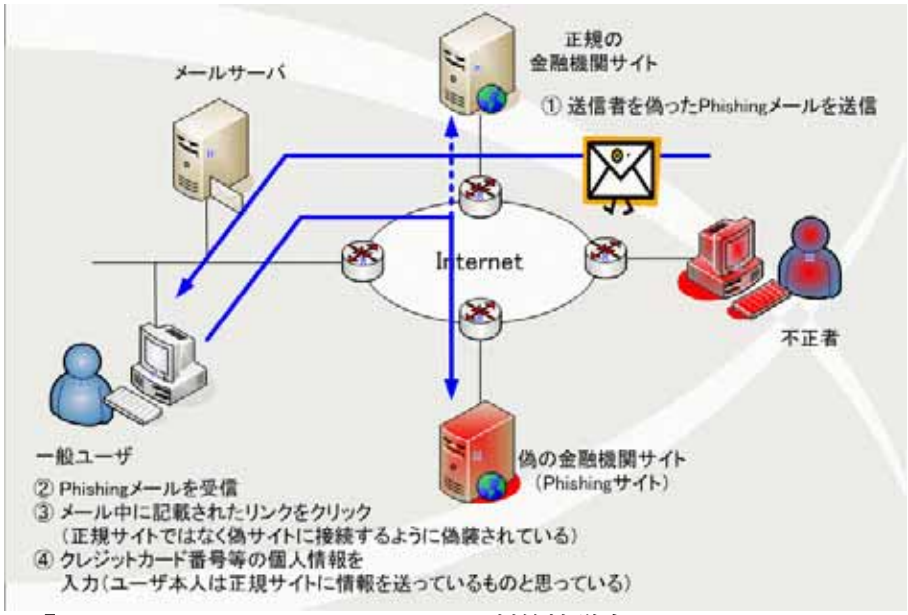
- **多数のパスワードを記憶･管理**
- **マスターパスワードで暗号化**
- **複雑なパスワードを生成**

さらにパスワードの管理機能の一部として、表示中のウェブサイトのＵＲＬを判定して対応するＩＤ･パスワードを自動的に選択するという機能性を有しています。これはフィッシング対策として「アドレスバーのＵＲＬを確認する」という動作を自動的に行うものです。その点でパスワード管理ソフトは、あるレベルにおけるフィッシング対策として有効であると言えるでしょう。

5. フィッシング対策

5.1 上流から下流へ

下図はフィッシングの典型的な流れを記載したものです。



出典： 『フィッシングとは？』フィッシング対策協議会 http://www.antiphishing.jp/, 2005

まずは発端となるメール、いわゆるフィッシングメールが送信されます。このメールが一般ユーザの手元に届いた後、ユーザは偽のサイト（フィッシングサイト）へ誘導されて、ユーザIDやパスワード、クレジットカード番号などが盗まれるという流れです。

この流れの中で、フィッシングメールはすなわちスパムメールでもあるので、スパムフィルタリング技術やメールの送信者認証技術がこれらの抑止に効果があるでしょう。これらは一般ユーザの手元へフィッシングメールが届く手前で行われるという点で、いわば上流での対策です。

一方、パスワード管理ソフトが提供するフィッシング対策は、一般ユーザにフィッシングメールが届き、フィッシングサイトに誘導された後のものであり、下流での対策と言えるでしょう。

ここではID・パスワード（ログイン情報）とクレジットカード番号の入力において、パスワード管理ソフトが提供しうるフィッシング対策について見てみます。

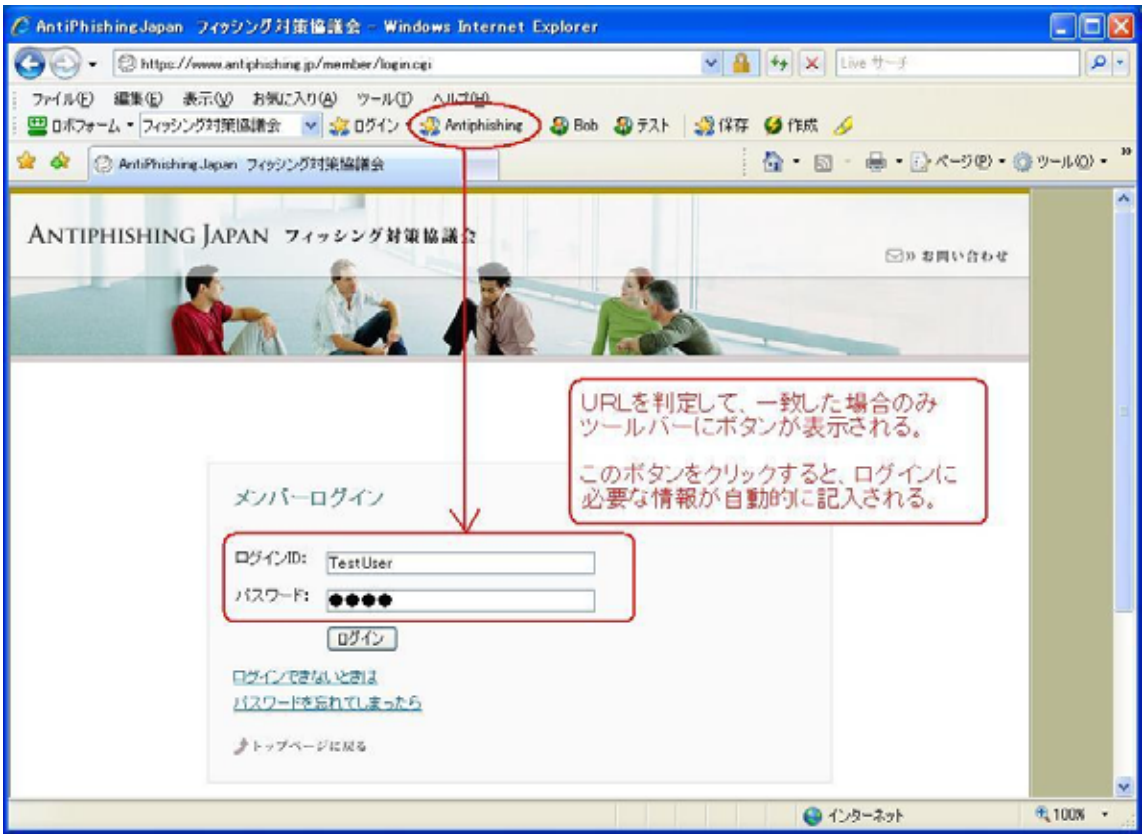
5.2 ログイン情報

下図はパスワード管理ソフトをインストールしたブラウザの画面例です。この例ではマイヤフーのログイン画面が表示されると、ツールバーには特別なボタンが自動的に表示されるようになります。

ここでは、あらかじめパスワード管理ソフトに登録してあるURLと、現在表示されているサイトのURLが比較･判定された結果に基づいて、**ログイン先 (Antiphishing)** のボタンが表示されています。そして、このボタンを押すことで、パスワード管理ソフトに登録されているログイン情報が所定の記入欄に記入されます。

ですからフィッシングメールによって誘導されたフィッシングサイトの外観が、いかに本物らしく見えても、あるいはURLが本物と酷似していても、URLの一致 (実際にはドメインの一致) が無い場合には前述のボタンは表示されません。したがって、ここにログイン情報が記入されることはありません。

一方、パスワード管理ソフトが効果をもたらすのは、あらかじめ自らがパスワード管理ソフトに登録したサイトのみです。従って初めて訪問するサイトがフィッシングサイトであるかどうかの判定を行うものではありません。しかし、今開いているサイトが自分の知っている (パスワード管理ソフトに登録してある) サイトかどうかは明確に判るようになっています。

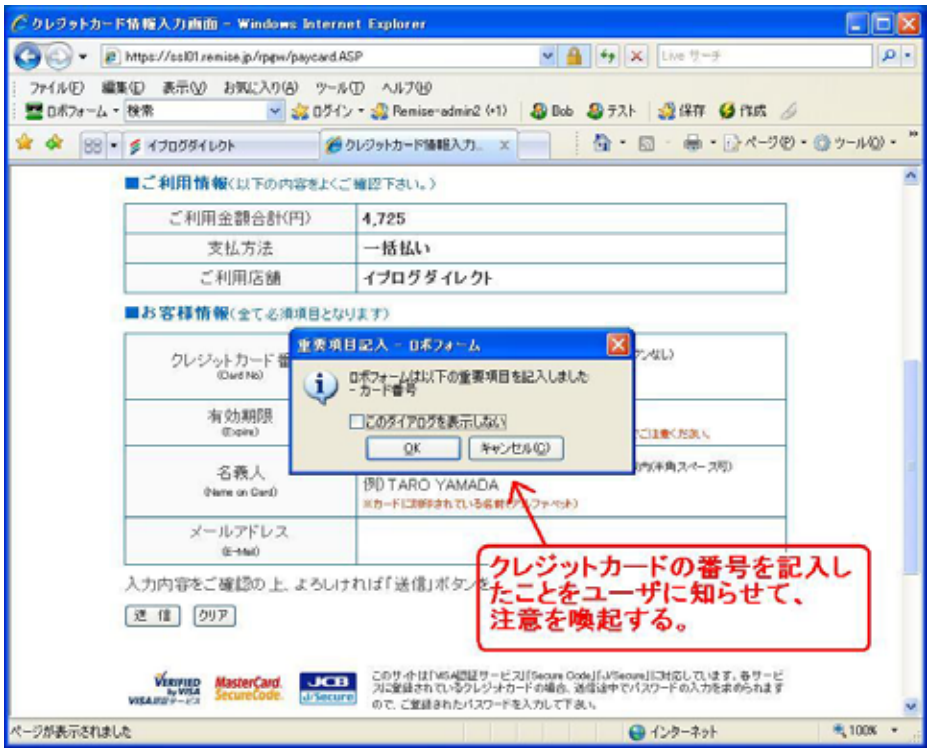


5.3 クレジットカード

ログイン情報がつねに対応するURL（あるいはドメイン）との関連の中で使用されるのに対しクレジットカード番号の場合は、あらゆるサイトでそのURLとは無関係に入力される可能性のある情報です。

一般にパスワード管理ソフトには、クレジットカードなどの個人情報を管理・記入する機能があります。しかし前述のとおり、クレジットカード番号の入力場面はURLと切り離されているため、ログイン情報の場合のようなURLの判定機能は有効ではありません。

このような場面でパスワード管理ソフトができることは下図のように、ポップアップ画面でユーザに対して重要な情報を送信しようとしていることを知らせるのみです。



5.4 多様なレベルの対応

私たちの日常の社会生活の中を見たとき、認証という作業はいたるところで多種多様な方法と、多種多様なレベルで行われていることに気が付きます。さらにそれらは複合的に用いられており、ひとつの認証をパスしても、他の認証が補間するような形で構成されています。

一方インターネットにおける認証は基本的にIDとパスワードによる認証が主流であり、一旦この認証をパスしてしまえば他に大きな関門はないという傾向にありました。

しかしながら、インターネットブラウザの最新のバージョンではフィッシング対策の機能が強化され、OSにおいてもマルウェア対策などが強化されて来ています。また、銀行等、より高いレベルでの認証が必要なサイトではID・パスワードによる認証に加えてワンタイムパスワードや生体認証などを採用するところも増えてきました。さらにパスワード管理ソフトなど、ユーザが手軽に導入できる、利便性と安全性を追求した使い易い製品も整いつつあります。

インターネットにおける人々の活動がさらに活発化するなかで、インターネットにおける認証の信頼性を確保することは極めて重要です。今後、インターネットにおける認証においても、日常の社会生活と同様に多種多様な方法、多種多様なレベルにおいて複合的に機能する認証システムの集合体、認証システム群の構築が望まれます。

出典および参考としたサイト：

ID・パスワードに埋もれる日々、90%以上が「忘れたことがある」
http://japan.internet.com/research/20050909/1.html

覚えられるパスワードは 3 つまで
http://polls.dailynews.yahoo.co.jp/quiz/quizresults.php?poll_id=122&wv=1&typeFlag=1

「すべて違う ID・パスワードを利用」1 割以下、増え続けるログインサービス
http://japan.internet.com/research/20060808/1.html

セキュリティの基本は個人のリテラシー向上にあり
http://business.nikkeibp.co.jp/article/as/20070117/117058/

「Yahoo!メール」がフィッシング対策を強化
http://profile.yahoo.co.jp/biz/press/body/4689/press7.html

マイクロソフト、新しい ID 管理技術「Windows CardSpace」を発表
http://japan.cnet.com/news/ent/story/0,2000056022,20234427,00.htm

「パスワードの終焉が見えた」--ビル・ゲイツ、InfoCard を披露
http://japan.cnet.com/news/sec/story/0,2000056024,20096500,00.htm

マイクロソフト、「InfoCard」を発表へ--デジタル ID 分野で再挑戦
http://japan.cnet.com/news/sec/story/0,2000056024,20083711-2,00.htm

ID 管理の Higgins と Bandit、MS の「Windows CardSpace」と連係可能へ
http://japan.cnet.com/news/ent/story/0,2000056022,20341768,00.htm

どうなる？ メールの送信者認証
http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20041115/152576/