

ネットワーク技術を悪用した個人情報の漏えいに注意

1 はじめに

本年 4 月 1 日に「個人情報の保護に関する法律」が完全施行されてから、約半年が過ぎようとしている。JNSA セキュリティ被害調査 WG が発表している「2004 年度情報セキュリティインシデントに関する調査報告書¹」によると、個人情報の漏えいは、盗難によるものが約 36%で最も多く、次いで紛失・置き忘れが約 22%となっており、不正アクセスやワーム・ウイルスといった、ネットワーク技術の悪用を原因とするものは 3%と非常に少ない。しかし、最近になって「フィッシング」、「ファームング」、「悪魔の双子」が個人情報漏えいの原因として認識され始めている。これらの原因による個人情報漏えいは、現在のところあまり発生していないが、手口がますます巧妙化しつつあるため、今後、被害が増加する可能性は十分考えられる。

これらのネットワーク技術を悪用した個人情報の漏えいについて、その手法、対策について述べる。

2 フィッシング (phishing)

フィッシング(phishing)という言葉は、「釣り」を意味する「fishing」と「(手口が)洗練されている」を意味する「sophisticated」を組み合わせで作られたと言われている。アメリカ合衆国では 2003 年から被害が発生しており、2004 年 6 月に警察庁ホームページ (<http://www.npa.go.jp/>)において、注意喚起²を行ったところである。



図 1 にフィッシングの代表的な手口を示す。フィッシングの流れは次のとおりである。

攻撃者は、発信元を実在する金融機関などに詐称した偽のメールを送信する。メール本文の内容は、ウェブページ上での個人情報の入力を促すような文面とともに、個人情報入力用のウェブページへのリンクが書かれている。ただし、リンク先として書かれている URL は、メールの発信元となっている金融機関などの URL によく似たものとなっている。

メールを受信したインターネット利用者は、メールの案内に従って本文内のリンクをクリックする。

¹ http://www.jnsa.org/active/2004/active2004_1a.html

² http://www.npa.go.jp/cyber/warning/chuikanki/160604_1.htm

リンク先のページは、メールの発信元となっている金融機関などの個人情報入力用ページによく似た偽のページ（フィッシングページ）となっており、ここに個人情報を入力した場合、データが攻撃者に不正に窃取されることになる。

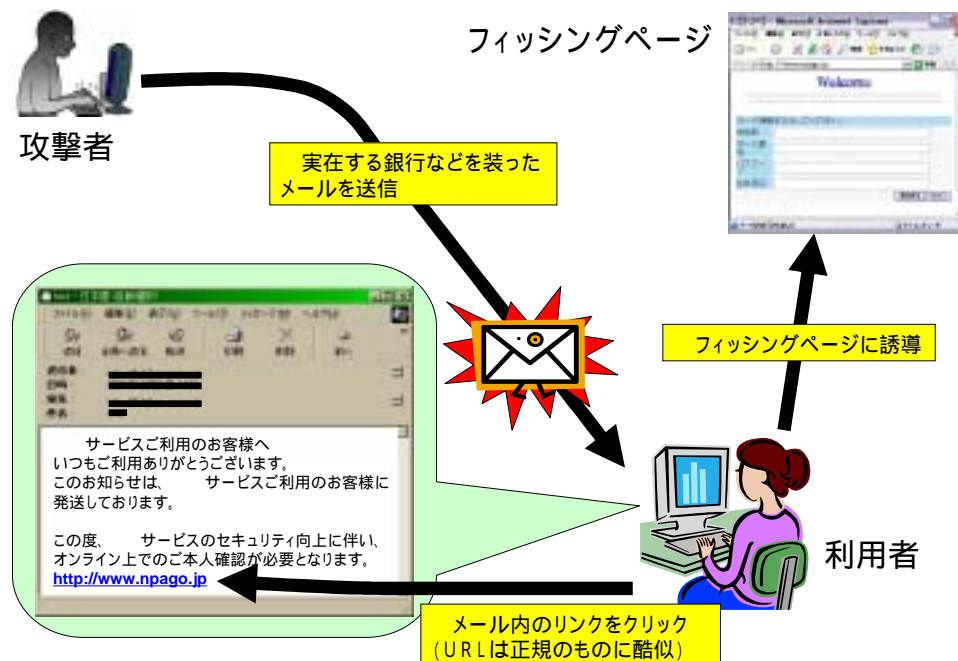


図1 フィッシング

最近では、ブラウザのアドレスバーの表示をごまかし、正規のウェブページに接続していると見せかけるなど、悪意のあるウェブページにアクセスさせる手口も巧妙化している。また、フィッシングを行う場合に送信されるメールは、ウイルスメールではないため、受信側のウイルスチェックソフトでも検出できない。

フィッシングに使用される技術は、特に難しいものではなく、ソーシャルエンジニアリング³によるところが大きい。フィッシングの語源にもあるように、偽の電子メールを「餌」に個人情報という獲物を「釣る」という手口である。

³ 管理者や社員、取引先などになりすましてパスワードを聞き出す、ごみ箱からパスワードが書かれたメモをあさるなどの「社会的手段」を使って個人情報を盗み出す方法のこと。防止のためには、安易にパスワードを教えたり、重要な書類を読み取ることのできる状態で廃棄したりすることのないよう、組織全体でセキュリティに関する意識を高めることが必要である。(@police 用語集より引用)

3 ファーミング(pharming)

(1) 概要

ファーミング(pharming)という言葉は、フィッシングの「釣り」の代わりに「農場」を意味する「farming」を用いて作られたと言われている。これはファーミングがインターネットにおいて基幹となる技術である名前解決を悪用するため、「農場」=「基幹となる技術」に「種」=「ファーミングの仕掛け」を植え付けるということで「pharming」という単語が用いられたと考えられる。

名前解決とは、インターネットにおいてホスト名を IP アドレスに変換することであるが、その方法には、一般的に hosts ファイルによる方法と DNS サーバによる方法の 2 つがあり、ファーミングはいずれの方法も悪用することが可能である。

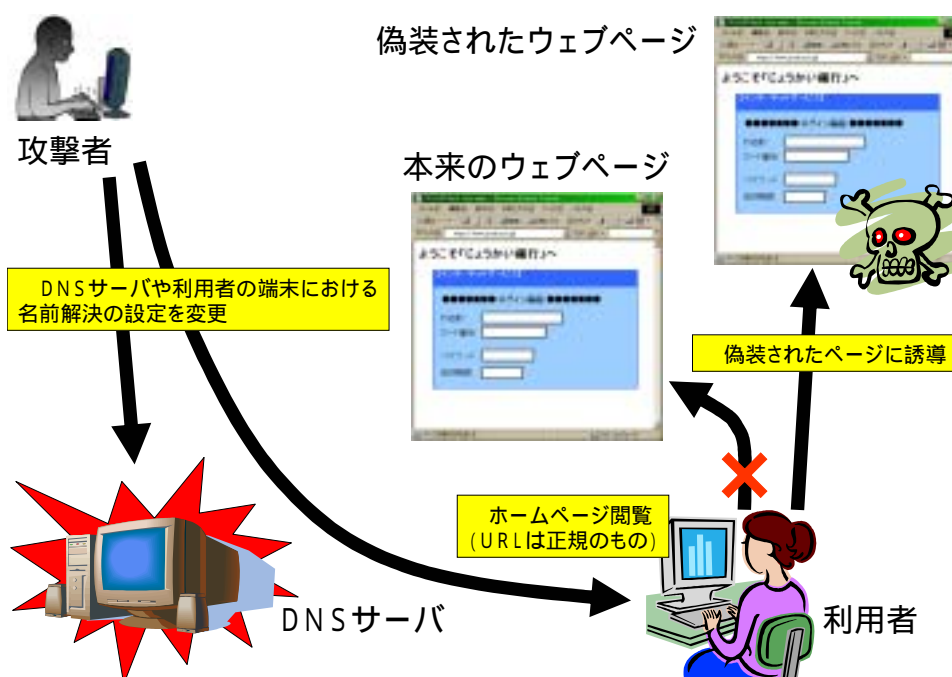


図2 ファーミング

図2にファーミングの手口を示す。

攻撃者は、DNS サーバや利用者の端末における名前解決の設定を変更する。名前解決の設定を変更する手口については、後述する。

インターネットの利用者は、ホームページを閲覧するために URL を入力する。

名前解決に関する設定が変更されているため、正しい URL を入力しても誤った IP アドレスに変換され、正規のウェブページではなく、まったく別のウェブページ（偽装されたウェブページ）を閲覧することになる。もし、この偽装されたウェブページが、個人情報の窃取を目的に攻撃者によって開設されたものである場合、このウェブページに入力された個人情報は、攻撃者に不正に窃取される。

ファーミングは、個人情報の窃取を目的に偽のウェブページに誘導する点において

フィッシングと同じであるが、名前解決の設定が変更されているため、正規の URL を入力しても偽のウェブページに誘導される点に注意してほしい。

4 ファーミングに悪用される手口～名前解決に関する設定を変更する手口

ファーミングは、名前解決に関する設定を変更するため、通常のウェブページの閲覧と区別がつかず、インターネット利用者が無意識のうちに被害に遭ってしまう可能性がある。ここで、名前解決に関する設定を変更する手口について整理しておく。

(1) ウイルスやワームなどによる hosts ファイルの書き換え

hosts ファイルは、DNS サーバを使用せずに名前解決するために設定されているファイルで、次のような内容のファイルである。

```
127.0.0.1 localhost
192.168.1.2 webserv.hoge**.com
192.168.1.3 mailserv.hoge**.com
```

図3 hosts ファイルの例

このファイルにより、ホスト名 webserv.hoge**.com の IP アドレスは 192.168.1.2、ホスト名 mailserv.hoge**.com の IP アドレスは 192.168.1.3 であると関連付けられる。

一般に名前解決は、まず hosts ファイルを参照し、hosts ファイルに該当のデータがない場合は DNS サーバに問い合わせるため、優先して参照する hosts ファイルをウイルスやワームなどによって書き換えることで簡単に偽のウェブページに誘導することができる。

(2) DNS キャッシュポイズニング

DNS キャッシュポイズニングは、DNS キャッシュ汚染とも呼ばれ、攻撃対象の DNS サーバに偽のキャッシュ情報を書き込ませて、正規のウェブページとは異なるウェブページに誘導させるものである。

偽のキャッシュ情報を「毒」に見立てて、攻撃対象の DNS サーバに「毒」を注入するという意味で、このような言葉を使用している。

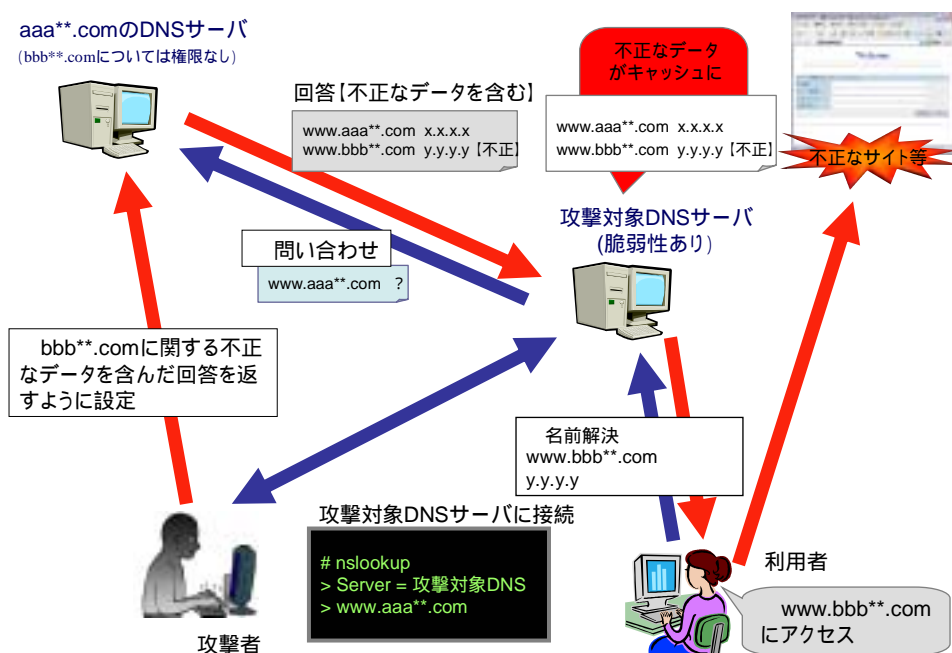


図4 DNSキャッシュポイズニング

図4にDNSキャッシュポイズニングの仕組みを示す。

攻撃者は、aaa**.comドメインを管理するDNSサーバに対し、権限のないbbb**.comドメインに関する不正なデータを回答するように設定を変更する。

次に攻撃者は、nslookupコマンドやdigコマンドを用いて、攻撃対象であるDNSサーバに接続し、www.aaa**.comに対する問い合わせを行う。

攻撃対象のDNSサーバは、aaa**.comドメインを管理するDNSサーバに、www.aaa**.comのIPアドレスを問い合わせる。

aaa**.comドメインを管理するDNSサーバは、www.aaa**.comに関する回答を返すとともにwww.bbb**.comに関する不正な回答も返す。

攻撃対象のDNSサーバはキャッシュ汚染に対して脆弱であるため、www.aaa**.comに関する回答とwww.bbb**.comに関する不正な回答をキャッシュしてしまう。

インターネット利用者がwww.bbb**.comを閲覧する。

利用者端末は、攻撃対象のDNSサーバにwww.bbb**.comのIPアドレスを問い合わせ、そのIPアドレスy.y.y.yを回答する。

y.y.y.yはwww.bbb**.comの正しいIPアドレスではないため、不正なウェブページに誘導される。

この場合、攻撃対象となっているDNSサーバは、問い合わせた結果をキャッシュしているだけであるので、脆弱性はあるものの悪意はないという点に注意を要する。

(3) 偽のDNSサーバの設置 (DNSサーバの管理上の問題)

DNSは、多数のDNSサーバがそれぞれのドメインを管理し、インターネットにおける

名前解決を実現している。しかし、DNS サーバの管理が不適切であると、偽の DNS サーバが設置されて、偽のウェブページに誘導されてしまう。

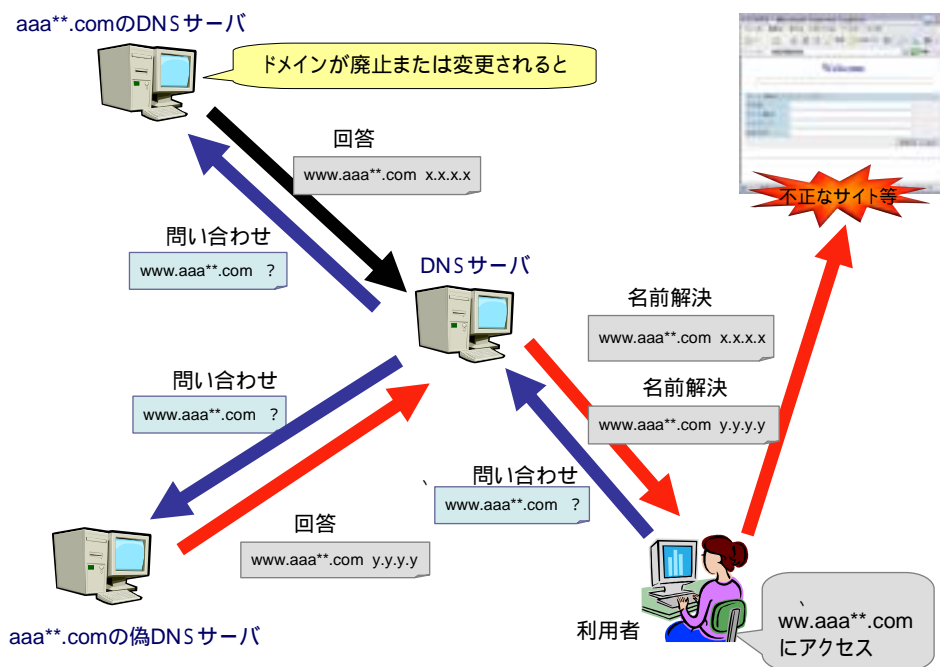


図5 偽のDNSサーバの設置

図5は、あるドメイン名の廃止または変更が、信頼関係のあるDNSサーバの設定情報に反映されなかったためにファームウェアに悪用される例を示している。正常な名前解決の流れは、

インターネットの利用者は、ホームページ `www.aaa**.com` を閲覧するため、URLを入力する。利用者の端末は、設定されているDNSサーバ(以下、「設定DNSサーバ」)に対し、`www.aaa**.com` の名前解決を要求する。

設定DNSサーバは、`www.aaa**.com` に関するIPアドレス情報がキャッシュにない場合、`aaa**.com` ドメインを管理するDNSサーバに対して、名前解決を要求する。

`aaa**.com` を管理するDNSサーバから、設定DNSサーバに対し `www.aaa**.com` のIPアドレス `x.x.x.x` が回答される。

設定DNSサーバは、利用者の端末に `www.aaa**.com` のIPアドレス `x.x.x.x` を告げる。

インターネット利用者は、`www.aaa**.com` を閲覧する。

となる。

ところが、`aaa**.com` が廃止または変更になった時、悪意のある第三者が `aaa**.com` を取得し、そのドメインを管理するDNSサーバを設置した場合、名前解決は図5におい

て次のようになる。

インターネットの利用者は、ホームページ `www.aaa**.com` を閲覧するため、URL を入力する。利用者の端末は、設定 DNS サーバに対し、`www.aaa**.com` の名前解決を要求する。

設定 DNS サーバは、`www.aaa**.com` に関する IP アドレス情報がキャッシュにない場合、`aaa**.com` ドメインを管理する DNS サーバに対して、名前解決を要求するが、`aaa**.com` は一度廃止または変更されたため、`aaa**.com` は悪意のある第三者が設置した別の DNS サーバで管理されている。

`aaa**.com` を管理する DNS サーバから、設定 DNS サーバに対し `www.aaa**.com` の IP アドレス `y.y.y.y` が回答される。

設定 DNS サーバは、利用者の端末に `www.aaa**.com` の IP アドレス `y.y.y.y` を告げる。

インターネット利用者は、`www.aaa**.com` を閲覧するが、以前のウェブページとは異なる悪意のあるウェブページに誘導される。

これは、ドメイン名が廃止または変更されたという情報が、DNS サーバに正しく反映されていないことが主な原因であるが、DNS サーバの設定におけるタイプミスでも同様のことが発生する。

5 悪魔の双子 (Evil Twin) ~ 偽の無線 LAN アクセスポイントの設置

「悪魔の双子」(Evil Twin)とは、偽のアクセスポイントを設置した無線 LAN であり、コーヒーショップなどの公衆無線 LAN を不正に利用する目的で設置される。

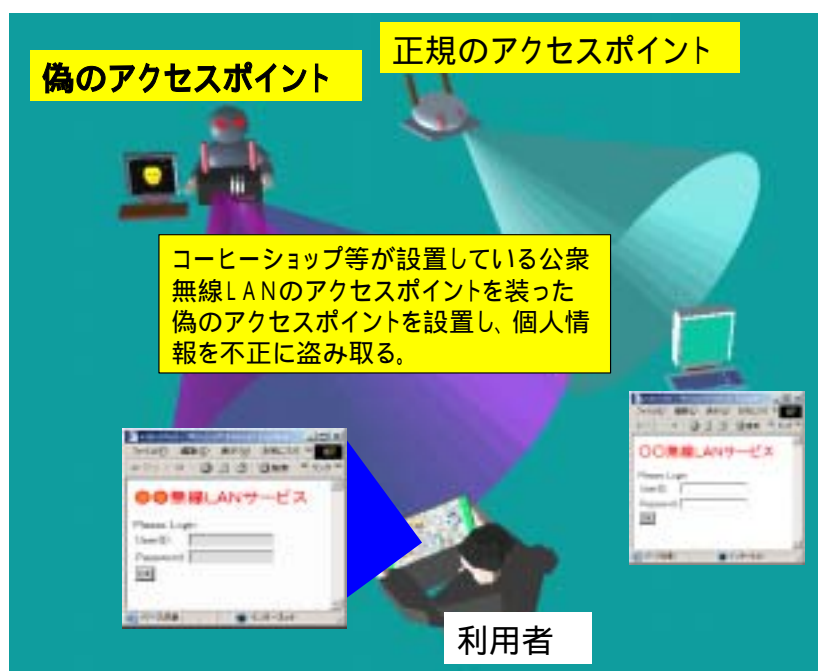


図6 悪魔の双子

図6に「悪魔の双子」(Evil Twin)についての概要図を示す。通常、無線 LAN 機能が搭載されているノートパソコンなどで公衆無線 LAN サービスを利用する場合、アクセスポイントに接続後、そのサービスを利用するためのユーザ ID 及びパスワードを入力する必要がある。この「悪魔の双子」は、公衆無線 LAN サービスを利用するときに、利用者が入力する個人情報を窃取することを目的として設置されるもので、中には、正規のログイン用ウェブページとまったく同じものを準備しているものもあると言われている。

特に、WindowsXP を用いて公衆無線 LAN サービスを利用する場合、アクセスポイントを自動的に探し出して自動接続するため、意図しないアクセスポイントに接続され、個人情報が不正に窃取されることが多い。

偽の無線 LAN のアクセスポイントの設置は、公衆無線 LAN に限ったものではなく、企業や個人で開設している無線 LAN についても同様の脅威が存在し、スパムメールの送信や DoS 攻撃などに悪用される場合がある。

6 対策

これまで説明したネットワーク技術を悪用した個人情報漏えいの手口について、その対策を述べる。

(1) フィッシング

ア 不自然なメールに注意する

フィッシングの手口の多くは、個人情報の入力を促す内容のメールを送りつけるものである。一般にメールで個人情報の入力を促すことはあり得ないため、そのような内容のメールやメール本文内のリンクは信用しない。また、スパムメールをフィルタリングするソフトウェアを導入し、適切に運用することも有効な手段といえる。

イ URL 及びウェブページの確認

フィッシングページの URL は、実在するウェブページの URL と非常によく似ており、また、フィッシングページ自体も実在するウェブページに似せて作られていることが多いので、よく確認する。

ウ SSL⁴証明書の確認

一般的に個人情報を入力させるウェブページは、SSL を使用しているので、証明書の発行元などが正規のものであるかよく確認する。

エ フィッシングページのフィルタリング

フィッシングページをブラックリスト化しフィルタリングなどのソフトウェアを導入し、不審なウェブページへのアクセス制限を行う。

⁴ Web 上でデータを暗号化して通信を行う技術。認証機能によるなりすまし防止と、暗号化による盗聴防止に有効である。多くのオンラインショッピングサイトでクレジットカード番号入力時に利用されている。Secure Sockets Layer の略。(@police 用語集より引用)

(2) ファーミング

ア 利用者による対策

(ア) アンチウイルスソフトの導入

アンチウイルスソフトを導入し、パターンファイルの定期的な更新により、hosts ファイルを書き換えるウイルスやワームなどの感染を防ぐ。

(イ) 脆弱性の解消

ウイルスやワームなどのほかにも外部からの攻撃により hosts ファイルが書き換えられる可能性があるので、セキュリティ修正プログラムを適用する。

(ウ) SSL 証明書の確認

一般的に個人情報を入力させるページは、SSL を使用しているので、証明書の発行元などが正規のものであるかよく確認する。

イ サーバ管理者による対策

(ア) 脆弱性の解消

DNS サーバの脆弱性を解消することで、不正なレコードをキャッシュすることがなくなる。

(イ) サーバ管理者間の連絡

偽の DNS サーバの設置を防ぐため、ドメイン名の廃止や変更が発生した場合は、必ず、信頼関係のあるドメインの DNS サーバの管理者へ連絡し、廃止または変更の情報を反映させる。

(3) 悪魔の双子

ア 必要時にのみ、無線 LAN 機能を有効にする

意図しないアクセスポイントへの接続を防ぐため、無線 LAN 機能は必要時にのみ有効にする。

イ SSL 証明書の確認

一般的に個人情報を入力させるウェブページは、SSL を使用しているので、証明書の発行元などが正規のものであるかよく確認する。

7 おわりに

インターネットの利便性が高まる一方で新たな脅威が顕在化しつつある。今回紹介した手口は、脆弱性の解消やアンチウイルスソフトの適正な運用などといった、これまで言われている情報セキュリティを確保する上での基本的な事項を守っていれば防げるものが多い。今後、この種の手口はますます巧妙化すると思われる、また、新たなサイバー犯罪に直結するような攻撃手法が編み出されるかもしれない。インターネット利用者並びにサーバ管理者にあっては、今後とも、基本的な情報セキュリティ対策の徹底を願いたい。