やさしいネットワーク・セキュリティ(2)

フィッシング詐欺への対策技術

連載 IT技術

村山　純一
MURAYAMA　Junichi
東海大学大学院情報通信学研究科
情報通信学専攻主任教授

セキュリティはいたちごっこの世界

前回，盗聴対策として，暗号通信技術について紹介した。しかし，ネットワーク・セキュリティの世界は，いたちごっこである。残念ながら，盗聴対策だけでは万全とはいえない。例えば，盗聴が難しい固定電話も，オレオレ詐欺に利用されている。同様の詐欺は，インターネットの世界でも多発している。偽装されたオレオレ店舗ウェブサーバが顧客を騙すのである。

このような詐欺はフィッシング詐欺と呼ばれる。個人情報が不正に入手され，不正送金などの被害が発生する。被害者には，個人だけでなく法人も含まれる。文献1）によれば，昨年度の被害額はおよそ16億円である。様々な対策により，被害額は減少傾向にある。それでも莫大な金額と言わざるを得ない。

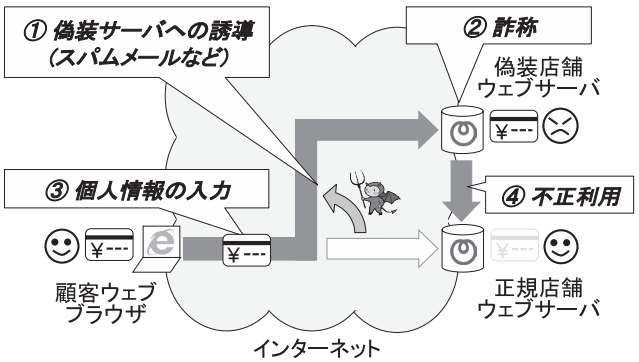
今回は，このフィッシング詐欺の手法とその対策技術について，やさしく紹介する。

オレオレ店舗ウェブサーバに要注意！

フィッシング詐欺では，正規店舗になりすました偽装店舗ウェブサーバが使用される。このサーバは本物そっくりであり，顧客は簡単に騙されてしまう。まさに，オレオレ店舗ウェブサーバである。たとえ暗号通信を行っていたとしても，個人情報が漏えいしてしまう。顧客のウェブブラウザが，偽装サーバから通知された鍵で，通信データを暗号化してしまうためである。

偽装サーバの構築は簡単である。例えば，文献2）のような，サーバのコンテンツを複製・保存するツールを使用すれば良い。見かけが同じため，正規サーバと偽装サーバを見分けることは難しい。

フィッシング詐欺の手順は，図－1の通りである。詐欺師は，あらゆる手段を駆使して，偽装ウェブサーバへ店舗の顧客を誘導する（図－1－①）。本物そっくりの偽装サーバに誘導された顧客は，正規サーバにアクセスしたものと騙されてしまう（図－1－②）。この結果，店舗を利用するための顧客識別情報やパスワード情報を入力してしまう。クレジットカード番号などの個人情報を直接入力してしまうこともある（図－1－③）。詐欺師は，偽装サーバに入力された顧客情報を読み出すと，これを不正に利用する（図－1－④）。



図－1　フィッシング詐欺

スパムメールに要注意！

インターネットでメールを利用していると，様々な広告メールや，怪しげな文章のメールも送られてくる。

このようなメールは，スパムメールと呼ばれている。スパムメールの多くは，店舗ウェブサーバへのアクセスを誘うものである。この中には，偽装サーバへ誘うメールも含まれている。

例えば，「あなたのパスワードが漏洩しました。一刻も早くパスワードを変更してください。ホームページは，こちらのリンクです。」といったメールが送られてくる。危機感を煽られた顧客は，慌ててリンクをクリックする。ところが，このリンクは，正規サーバではなく，偽装サーバに接続されているのである。

この結果，顧客は偽装サーバにアクセスしてしまう。偽装を見抜けないと，個人情報を入力してしまうことになる。

ウェブサーバの名前をチェック！

ウェブブラウザの画面上部には，アドレスバーと呼ばれる領域がある。ここには，閲覧中のウェブサーバの名前（注1）が表示される。例えば，「www.ntt.co.jp」と言ったように，企業や国の省略名がアルファベットで羅列される。中には，文献3）にあるように，「日本語.jp」などと，漢字や平仮名で記載されることもある。

正規サーバか偽装サーバかを見分ける基本は，アドレスバーに注意することである。ウェブサーバの名前をよく確認することで防げる詐欺も多い。アドレスバーを気にかけないことも多いと思うが，よく注意されたい。また，ホームページのリンクを利用して，他のホームページへジャンプすることも多いことだろう。この場合もアドレスバーには気を付けたい。

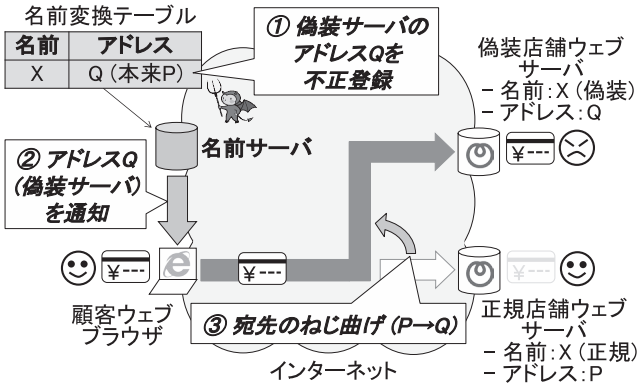
攻撃される名前サーバ

ウェブブラウザのアドレスバーに，ウェブサーバの名前を手入力してアクセスすることもあるだろう。実は，インターネット上では，ウェブサーバの所在がインターネットアドレス（注2）で識別されている。このアドレスは32ビットあるいは128ビットの2進数データである。この数値データは，人間には覚え難く，入力も面倒である。そこで，インターネットアドレスの代わりに，ウェブサーバの名前が利用されている。

ウェブブラウザは，ウェブサーバにアクセスする際，ウェブサーバの名前から，インターネットアドレスを導き出す必要がある。この際に，名前サーバ（注3）が利用される。このサーバは，固定電話での番号案内サービス104を連想させるものである。

名前サーバの多くは，プロバイダが提供しており，基本的には信頼性が高い。一方で，名前サーバは，技術的には，様々な攻撃の踏み台にされやすい特徴を持つ。ある攻撃（注4）では，図－2に示すように，偽インターネットアドレス情報が，名前サーバに不正登録されてしまう（図－2－①）。以後は，ウェブブラウザに正規サーバの名前を入力しても，偽装サーバのインターネットアドレスが通知されてしまう（図－2－②）。宛先インターネットアドレスがねじ曲げられるため，多くの顧客が集団的に偽装サーバに誘導されることになる（図－2－③）。

このような攻撃を利用した詐欺は，ファーミング詐欺と呼ばれている。現在は，名前サーバの監視など，プロバイダ側での対策も進んでいる。このため，集団で被害に遭うことは稀である。しかし，インターネットに異常がないか，日頃からニュース等で注意することは必要である。



図－2　ファーミング詐欺

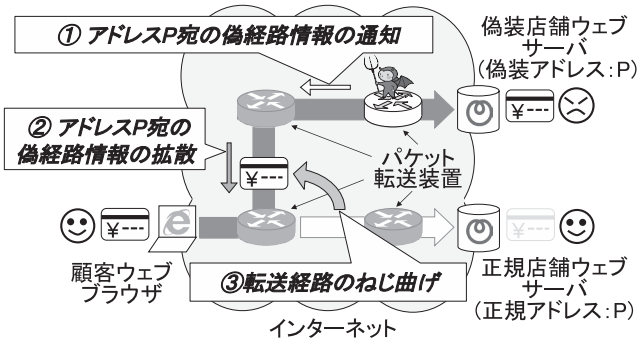
攻撃されるパケット転送装置

インターネットでは，多数のパケット転送装置（注5）が互いに連携して，世界中にパケット形式の通信データを送り届けている。パケット転送装置の間では，自分が誰にパケットを配送できるのかという経路情報が常に交換されている。また，この経路情報から，宛先毎に最適なパケット転送経路が導き出されている。

ところで，図－3に示すように，攻撃を受けたパケッ

ト転送装置が，偽の経路情報を通知することがある（図－３－①）。すると，その情報がたちまち多くのパケット転送装置に拡散してしまう（図－３－②）。この結果，特定サーバに向けた通信パケットの転送経路だけがねじ曲げられる（図－３－③）。すなわち，正規サーバのインターネットアドレス宛に送ったはずの通信パケットが，偽装サーバへ送り届けられることになる。

このような攻撃は，経路ハイジャック攻撃と呼ばれる。現在では，プロバイダのネットワークが適切に監視されており，滅多に発生しない。しかし，海外プロバイダによる設定ミスなどが原因で，通信パケットの転送経路がねじ曲げられることもある。このため，プロバイダから提供されるお知らせなどについても日頃から注意されたい。



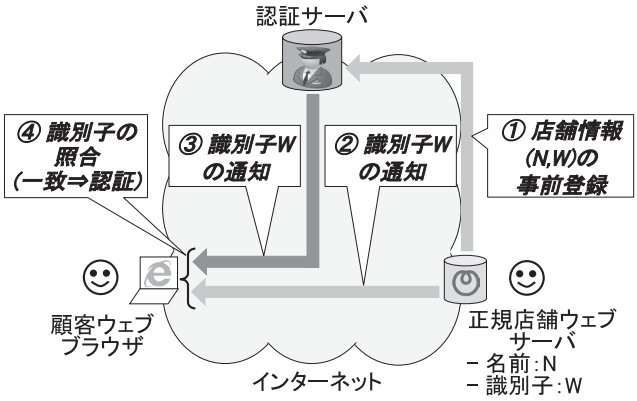
図－３　経路ハイジャック攻撃

ウェブサーバは本物か？

フィッシング詐欺では，オレオレ詐欺と同様に，偽装サーバが自分は正規サーバであると主張する。これが本物かどうかを判断するためには，信頼できる第三者の協力が必要である。インターネットの世界では，図－４に示すように，第三者として認証サーバ（注6）がこの判断を手助けしてくれる。

認証サーバには，多数の店舗ウェブサーバの情報が登録されている。店舗ウェブサーバは，店舗（企業）情報として，サーバの名前と識別子を，予め認証サーバに登録申請する（図－４－①）。認証サーバは，店舗（企業）が実在するかどうかを審査する。実在すれば申請情報を登録する。実在しなければ申請を却下する。

一方，顧客のウェブブラウザは，店舗ウェブサーバにアクセスすると，最初にサーバ識別子と認証サーバのアドレスを通知してもらう（図－４－②）。この後，認証サーバへも問い合わせ，登録されている店舗ウェブサーバのサーバ識別子を通知してもらう（図－４－③）。ウェブブラウザは，通知されたサーバ識別子同士を照合する（図－４－④）。一致すれば，アクセス中のウェブサーバを認証された正規サーバと判断する。一致しない場合は，偽装サーバと判断する。

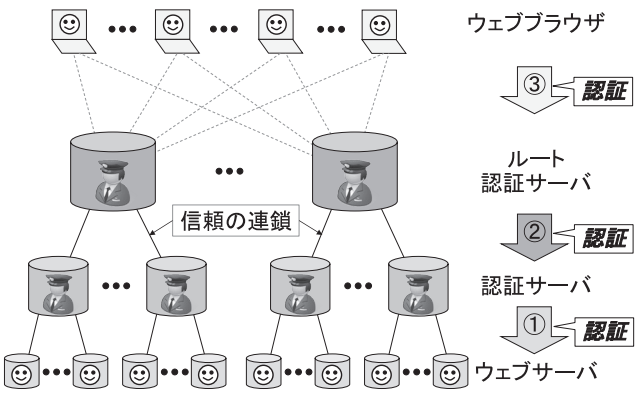


図－４　ウェブサーバの認証

認証サーバは本物か？

オレオレ詐欺も高度化すると，詐欺師が集団となり，本人だけでなく，警官にもなりすますことがある。このことは，フィッシング詐欺でも同様である。そこで，図5に示すように，認証サーバも本物かどうかを判断することが重要となる。この判断を手助けしてくれるのが，ルート認証サーバである。

店舗ウェブサーバが本物であることは，認証サーバが証明してくれる（図－５－①）。同様の手段で，認証サーバが本物であることは，ルート認証サーバが証明してくれる（図－５－②）。ルート認証サーバは，



図－５　認証サーバの認証

多数の認証サーバの情報を保有するため，信頼の連鎖が階層的に形成される。この連鎖により，世界中のウェブサーバの信頼性が高められている。

実はウェブブラウザも重要！

世界中には無数のウェブサーバが散らばっている。これら全てのサーバ認証を手助けするため，ルート認証サーバも複数のサーバに分散化されている。ところで，ルート認証サーバが本物であることを，どのように判断すれば良いのだろうか？

実は，ルート認証サーバの認証は，ウェブブラウザが行う（図－5－③）。ウェブブラウザには，全てのルート認証サーバの識別子が初期設定されている。ウェブブラウザは，ルート認証サーバから識別子を通知されると，これらの設定済みの識別子と照合する。いずれかと一致する場合は，正規のルート認証サーバと判断する。一致しない場合は，偽装されたルート認証サーバと判断する。

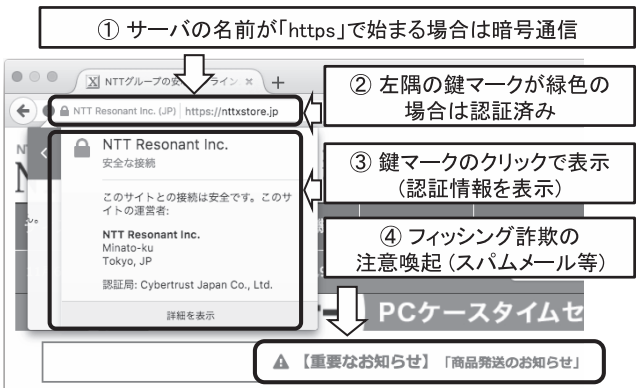
このことから，ウェブブラウザとして，信頼できるソフトウェアを利用することが大変重要である。特に，自分でウェブブラウザをインストールする場合には，正規のサーバからダウンロードしたか，また正規のソフトウェアをダウンロードしたかなど，充分に注意されたい。さらに，ウェブブラウザにウイルスが寄生している場合には，サーバ認証にも支障を来す恐れがある。このため，日頃からウイルス対策ソフトウェアなども活用したい。

個人情報を入力する時に注意すること

ウェブブラウザに個人情報を入力する際には，暗号通信とサーバ認証が共に行われていることを確認してもらいたい。暗号通信は通信経路上での情報漏えい対策，サーバ認証は宛先サーバでの情報漏えい対策である。いずれも図－6に示すように，ウェブブラウザのアドレスバーを確認されたい。

暗号通信時には，サーバの名前の左側に，httpsの文字列が現れる（図－6－①）。また，その左側に鍵マークも現れる。さらに，サーバが正規であると認証されると，この鍵マークが緑色に変化する（図－6－②）。鍵マークをクリックすると認証情報も確認できる（図－6－③）。個人情報を入力する前には，確認する癖をつけておきたい。また，詐欺が多発すると，本文中に店舗からの注意情報が示されることもある（図－6－④）。

ポップアップウィンドウが現れる場合は，さらに要注意である。背景ウィンドウが正規サーバ，ポップアップウィンドウが偽装サーバの場合もある。個人情報の入力を促される場合には，ポップアップウィンドウ自身のアドレスバーに特に注意されたい。



図－6　ウェブブラウザのアドレスバー

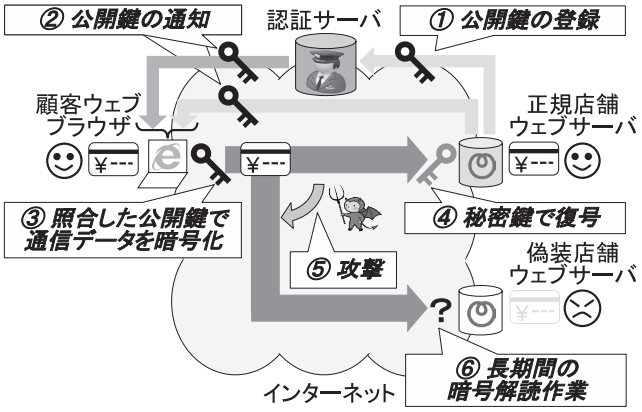
サーバ認証でも公開鍵／秘密鍵が活躍

説明が複雑になるので省略したが，実は，図－7に示すように，サーバ認証時のサーバ識別子には，暗号通信の公開鍵が使われている。すなわち，認証サーバには，店舗ウェブサーバの公開鍵がサーバ識別子として登録される（図－7－①）。ウェブブラウザには，この公開鍵が店舗ウェブサーバと認証サーバの双方から通知される（図－7－②）。ウェブブラウザは，公開鍵の照合で認証を行った後，この公開鍵で通信データを暗号化する（図－7－③）。正規の店舗ウェブサーバは秘密鍵を保有するため，暗号データを簡単に復号できる（図－7－④）。

何らかの攻撃が行われると，この暗号データが偽装サーバへ届くかもしれない（図－7－⑤）。この場合でも，偽装サーバは暗号データを復号できない。正規サーバの秘密鍵を入手できないためである。この結果，暗号解読には天文学的な時間が必要となる（図－7－⑥）。すなわち，個人情報の漏洩が阻止できることになる。

インターネットショッピングを安心・安全に行うた

めには，暗号通信とサーバ認証の組み合わせが必須である。公開鍵/秘密鍵は，この両者において，とても重要な役割を果たす非常に画期的な技術なのである。



図－7　公開鍵を識別子としたサーバ認証

【参考文献】

1）“ネットバンク不正送金16億円 警察庁，昨年の被害集計”，朝日新聞デジタル
<http://www.asahi.com/articles/ASK3Q3WK3K3QUTIL010.htm>
2）“ScrapBook”，firefoxアドオン拡張機能，
<https://addons.mozilla.org/ja/firefox/addon/scrapbook/>
3）“日本語.jp”，JPRS，
<http://日本語.jp/>

（注1）正確には，「URL（Uniform Resource Locator）」
（注2）正確には，「IP（Internet Protocol）アドレス」
（注3）正確には，「DNS（Domain Name System）サーバ」
（注4）正確には，「カミンスキー攻撃」
（注5）正確には，「ルータ」
（注6）正確には，「認証局」

非開削技術講習会

■ 福岡会場

日　　時：平成30年2月16日（金）　10：00～17：00
会　　場：TKPガーデンシティ博多新幹線口 3-A
　　福岡市博多区博多駅中央5-14　福さ屋本社ビル　☎092-432-7250
募集人員：45名
内　　容：❶10：00～10：05　はじめに
　　❷10：05～12：05　HDD（誘導式水平ドリル）工法について
　　伊藤靖氏他（JSTT HDD工法委員会委員長）
　　❸12：05～13：00　休憩
　　❹13：00～14：00　非開削地下探査技術適用の手引き（案）について
　　齋藤秀樹氏（JSTT 地下探査技術委員会委員長）
　　❺14：00～14：10　休憩（昼食）
　　❻14：10～15：10　地下管渠工事の社会的費用―算定の手引き―（案）について
　　宮武昌志氏（JSTT ソーシャルコスト検討委員会委員長）
　　❼15：10～15：20　休憩
　　❽15：20～16：20　管路更生工法の変遷について
　　佐藤敏明氏（㈱日本管路更生工法品質確保協会理事）

お問い合わせ先
JSTT 一般社団法人日本非開削技術協会　【事務局】 小谷，近藤（Tel：03-5639-9970　E-mail：office@jstt.jp）