

第三回：マインドマップで学ぶ、技術者のためのシステムセキュリティ対策入門

梅原 伸行¹

前回は、「情報資産」を蝕む「脅威」のうち、「盗聴」に対するシステムセキュリティ対策のポイントを取り上げました。今回は、近年、日本でも大きな被害を及ぼしている「なりすまし」に対するシステムセキュリティ対策のポイントを取り上げていきたいと思います。

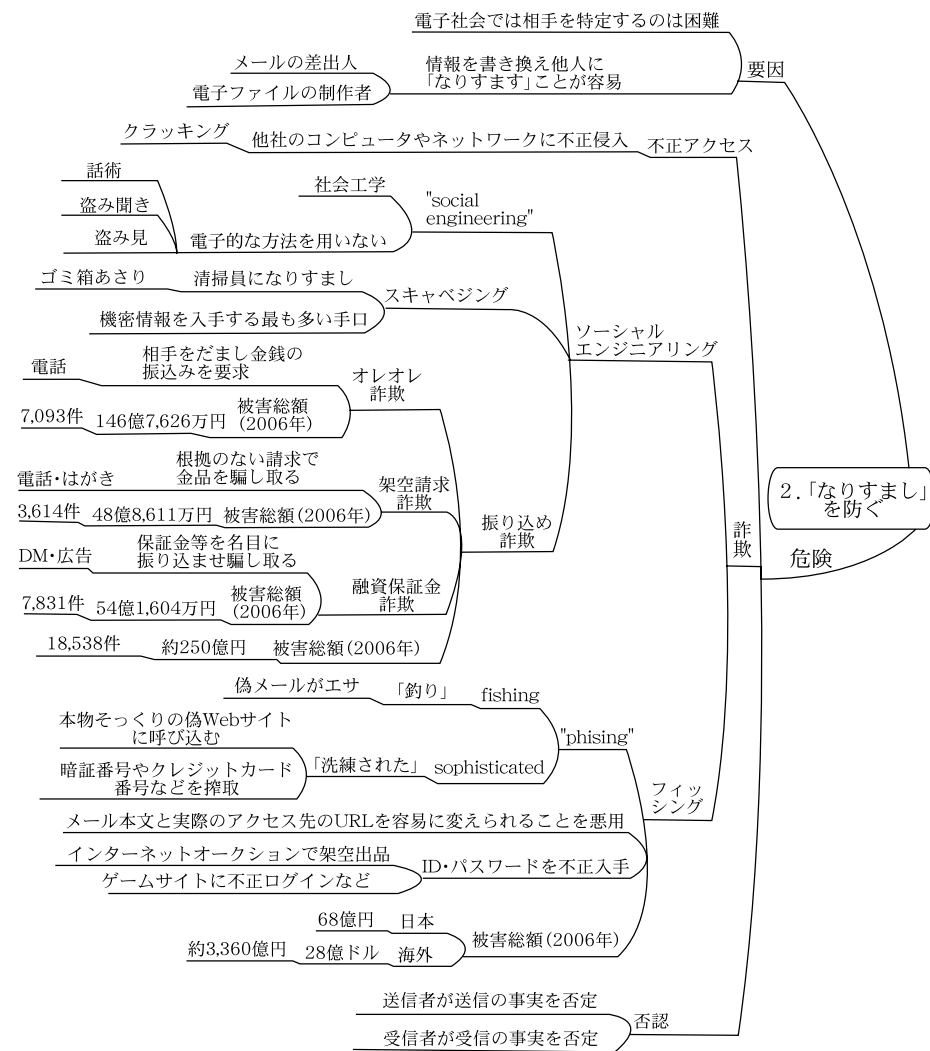
人が「なりすまし」を行う目的は、主に「お金」にあります。一昔前であれば他人に「なりすまし」するためには、手の込んだ「変装」を行わなければならなかったかもしれませんが、今は家に居ながら「なりすまし」ことが可能です。

「なりすまし」には、大きく分けて「電子的な方法を用いないもの」と「用いるもの」がありますが、「電子的な方法を用いないもの」は、「ソーシャルエンジニアリング」と呼ばれる従来の「変装」型詐欺になります。「振り込め詐欺」がこの代表格ですが、昨年だけでも被害総額は約 250 億円²にも上っており、電話やハガキなどアナログな手口が依然有効であることを示しています。この対策は「人的セキュリティ」の方に入ってしまうので本連載の範囲外となりますが、罨にかからないための日頃の心がけが重要になります。³

次に「電子的な方法を用いる

もの」ですが、様々な手口のうち、最も広く知られているのは、やはり「フィッシング」でしょう。「フィッシング」とは、エサで魚をおびき寄せて釣り上げる (fishing) ように、偽メールをエ

サにして本物そっくりのサイトに誘い込み、暗証番号やクレジットカード番号などを盗み取る手口のことですが、HTML メールの場合、メール本文と実際のアクセス先の URL を変えることができるという



1. JIPDEC ISMS ISO27001 審査員補, SAAJ システム監査人補
2. <http://itpro.nikkeibp.co.jp/article/NEWS/20060927/249160/?ST=security>

3. オレオレ詐欺対策についてはこちら
<http://www3.nhk.or.jp/gatten/archive/2006q2/20060517.html>

ことを悪用する手法が「洗練されている」(sophisticated) という
ことで「Phising」と名付けられました。しかし、実際のところ高度な技術は必要なく、Webサイトの基本的な知識があれば中学生⁴でも実現可能なため、被害が後を絶たない状況となっています。

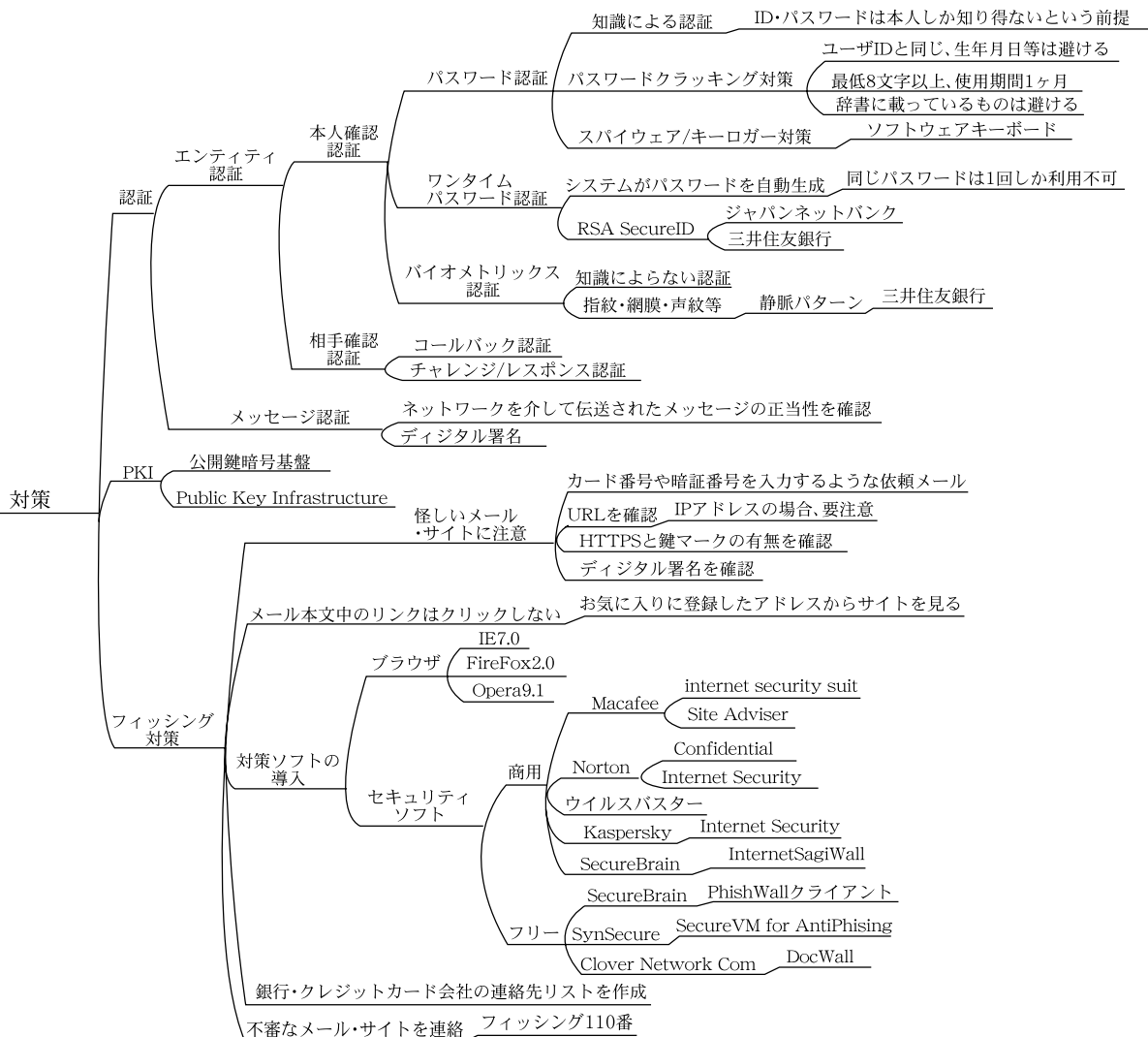
「フィッシング」詐欺による被害総額は、昨年68億円⁵に達し、セキュリティ強化策が取られるようになってきました。例えば、銀行やインターネットバンキングで

は、本人しか知り得ないことを前提として「ID・パスワード」による照合を行っていましたが、それが他人に知られてしまった場合、いとも簡単になりすまされてしまう危険があるため、「ソフトウェアキーボード」(ID・パスワード盗聴防止)、「ワンタイムパスワード」(パスワードの複雑化)、「バイOMETRICS認証」(知識によらない認証)などの対策が取られるようになってきました。

個人レベルの対策としては、「怪

しいメール・サイトに注意する」のが一番ですが、有償・無償のフィッシング対策ソフトを導入する手もあります。IE・FireFox・Operaの最新バージョンは既に「フィッシング対策」機能を備えているので、これを機に乗り換えるのも良いかもしれません。(開発者の場合、なかなかそうもいかないのですが。)

今回は、「改ざん」に対するシステムセキュリティ対策のポイントを取り上げたいと思います。



4. https://www.netsecurity.ne.jp/1_6806.html
5. <http://itpro.nikkeibp.co.jp/article/COLUMN/20070218/262323/>