NPO ISEF
Not-for-Profit Organization of Information Security Forum

特定非営利活動法人
NPO情報セキュリティフォーラム

NPO-ISEF 情報セキュリティレポート：2011-No.04
ソーシャルエンジニアリング攻撃の今と昔

株式会社日立製作所
寺田 真敏（Terada Masato）

【著者経歴】
横浜研究所と HIRT（Hitachi Incident Response Team）に所属。中央大学大学院客員講師、JPCERT/CC 専門委員、IPA セキュリティセンター研究員、テレコム・アイザック推進会議運営委員、日本シーサート協議会の副運営委員長を務める。

2011 年、ハッカー集団による一連の攻撃活動、防衛産業や官公庁系を対象とした標的型攻撃など、サイバー攻撃による脅威が身近なものとする出来事が多数発生した。サイバー攻撃の過程において、人間の心理的な隙や人間の行動上の隙をつく攻撃、いわゆるソーシャルエンジニアリング攻撃が重要な役割を果たしている。ここでは、電子メールなどで利用されてきたソーシャルエンジニアリング攻撃の手法を年代毎に振り返ってみたい。

1 ソーシャルエンジニアリング攻撃とは

ソーシャルエンジニアリング攻撃は、社会工学的な観点から発生する脆弱性（人間の心理的な隙や行動上の隙）を利用した攻撃方法である。人間の心理的な隙を利用する事例としては、『システム管理者になりすまして、「（システム管理上）あなたのパスワードを送ってほしい」というメールを送り、パスワードを聞き出す』、『電話や面と向かって何気なく個人情報を聞き出す』などがある。また、人間の行動上の隙を利用する事例としては、『ゴミ箱に廃棄された紙ゴミから重要情報を探し出す（重要な情報が記載された紙の資料を何気なくゴミ箱に捨ててしまう）』、『肩越しに画面や利用者の手の動きを見てパスワードを盗み見る（まわりから見られているという意識がない）』などがある。

2 手法の今と昔

電子メールなどで利用されてきたソーシャルエンジニアリング攻撃は、人間の心理的な隙を利用するもので、電子メールの件名にユーザが開封したくなるような見出しを記載するだけではなく、見た目を本物に近づける、本物を再利用するなど、年々巧妙化している。その手法の変遷を事例と共に紹介する。

2.1 1991 年

- **メッセージにより誘導する**

1991 年 4 月、米国のコンピュータ緊急対応チーム CERT/CC から「CA-1991-03：Unauthorized Password Change Requests Via Mail Messages」という注意喚起が発行された。ここで報告された攻撃は、システム管理者を装って「パスワードを変更して欲しい！」という電子メールを送りつけるという手法であった（図 1）。

SAMPLE MAIL MESSAGE as received by the CERT (including spelling errors, etc.)
:
{mail header which may or may not be local}
:
This is the system administration:
Because of security faults, we request that you change your password to "systest001". This change is MANDATORY and should be done IMMEDIATLY. You can make this change by typing "passwd" at the shell prompt. Then, follow the directions from there on.

Again, this change should be done IMMEDIATLY. We will inform you when to change your password back to normal, which should not be longer than ten minutes.

Thank you for your cooperation,

The system administration (root)

END OF SAMPLE MAIL MESSAGE

出典：CERT Advisory CA-1991-03 Unauthorized Password Change Requests Via Mail Messages
http://www.cert.org/advisories/CA-1991-03.html

図 1：CERT/CC が発行した注意喚起で紹介された事例

2.2 1999 年

- **添付ファイルを開きたくなるメッセージを利用する**

ソーシャルエンジニアリング攻撃は、管理者を装ったパスワード変更依頼だけではなく、電子メールにウイルスファイルを添付して自己伝搬していく、いわゆる電子メール型ウイルスにも利用されている。図 2 は、1999 年頃に流布したウイルスが利用した件名／本文である。いずれの場合も、思わず添付ファイルを開きたくなるようなメッセージとなっている。

名称	利用されたメッセージ
W97M/Melissa 【1999年2月】	件名：Important Message From “ユーザ名” 本文：Here is that document you asked for ... don't show anyone else ;-) 頼まれていたﾄﾞｷｭﾒﾝﾄです。誰にも見せないように;-)
VBS/Loveletter (ラブレター) 【2000年5月】	件名：ILOVEYOU. 本文：kindly check the attached LOVELETTER coming from me. 私からのラブレターです。どうぞ読んでみて下さい。
VBS/OnTheFly 【2000年8月】	件名："Here you have, ;o)" 本文：Hi: Check This! 添付："AnnaKournikova.jpg.vbs"

図 2：電子メール型ウイルスで使用された件名／本文の例

2.3 2000 年

- **添付ファイルを安全なファイルであると勘違いさせる：二重拡張子**

2000 年代には、メッセージだけではなく、見た目を騙す手法が出始めた。2000 年 5 月に出現したラブレターウイルス（VBS/Loveletter）は、添付ファイルをテキストファイルと勘違いさせるた

めに、「.TXT」という文字列を入れた「LOVE-LETTER-FOR-YOU.TXT.vbs」という添付ファイル名を使用した（図 3）。この添付ファイルは、拡張子が vbs であるが、その前に「TXT」が付いていたために、テキストファイルと勘違いして多くのユーザが開いてしまったと言われている。

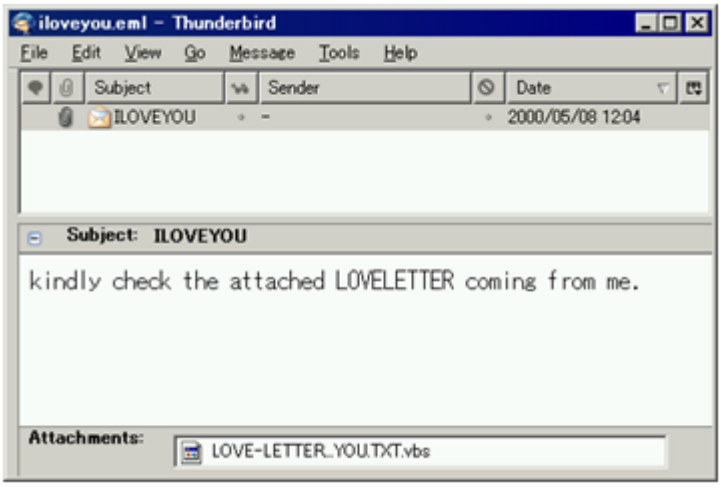

図 3：二重拡張子を利用した添付ファイル名の例

2.4 2004 年

- **本物と勘違いしてしまう電子メールやウェブサイトを利用する：フィッシングメール＆フィッシングサイト**

2003 年に入ると欧米でフィッシングによる被害が出始め、2004 年には国内でもフィッシング詐欺による被害が発生した。ここでは、本物と勘違いしてしまう電子メールやウェブサイトが利用されていた。図 4 の事例は、フィッシングサイトを日本語で作成しているだけではなく、（偽物の URL を隠すために）JavaScript を使ってブラウザのアドレスバー上に本物の URL を表示させるというものであった。

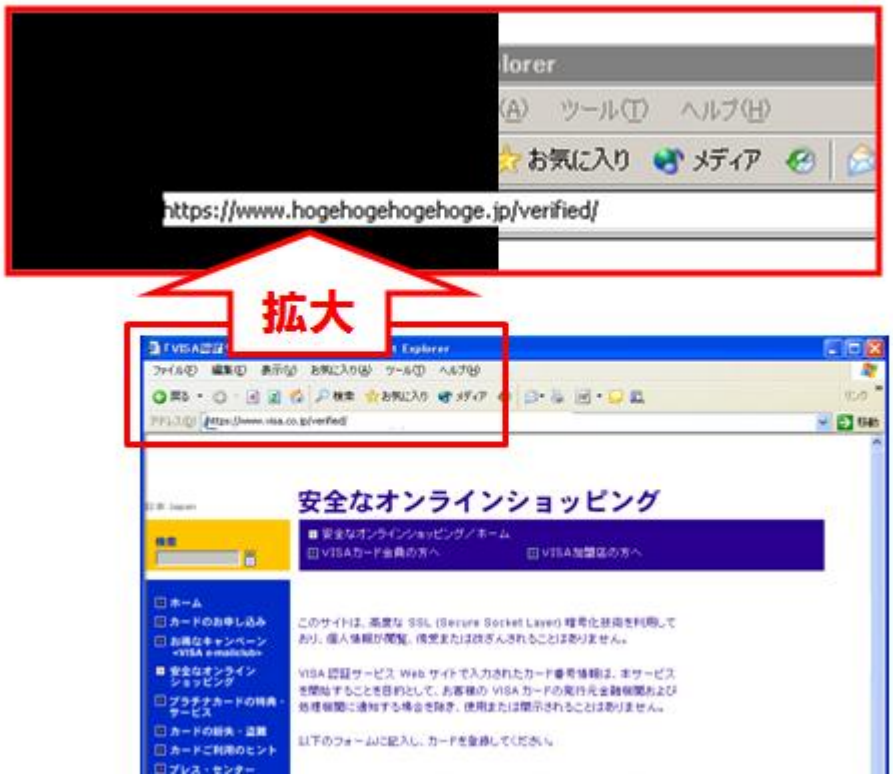

図 4：フィッシングサイトの再現例

- **問題のない操作であると勘違いさせる：アイコン偽装**

情報漏えいウイルスとも呼ばれ、Winny での情報漏えい被害を発生させ続けているアンティニィウイルス（Antinny）は、実行可能ファイル（＝ウイルス本体）をアイコン偽装していた。図 5 は、アイコン偽装を再現したものである。右側のアイコンは一見フォルダに見えるが、実はフォルダと同じアイコンを表示する、非常に長いファイル名（コピー～新しいフォルダ２　・・・空白文字・・・　.exe）を使って偽装された実行可能ファイル（＝ウイルス本体）である。

さらに、アンティニィウイルスでは、ダウンロードした LZH などの圧縮ファイルに、アイコン偽装したファイルをひとつだけ格納するというソーシャルエンジニアリング攻撃が併用されていることもあった。これは、ユーザがアイコン偽装されたフォルダをクリックしなければならない状況を作り出すために考えられたものであろう。

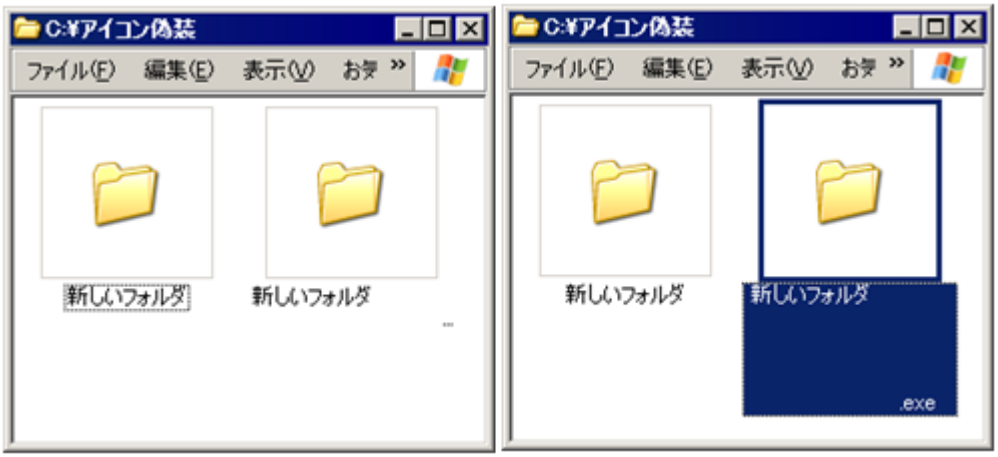

図 5：アイコン偽装の再現例

2.5 2008 年

- **問題のない操作であると勘違いさせる：USB メモリの自動再生／自動実行**

2008 年 11 月頃から出現したコンフィッカーウイルス（Conficker）には、2008 年 12 月にはいってから、USB メモリの自動再生／自動実行を利用して感染する機能が追加された。ここで利用されたソーシャルエンジニアリング攻撃は、USB メモリの持つ物理的な媒介手段としての利便性と Windows 環境が提供する USB メモリの自動再生／自動実行である。特に、USB メモリの自動再生／自動実行は、見た目を問題のない操作であると勘違いさせるために利用された。

図 6 は、Windows XP パソコンに USB メモリを接続した直後の状態で、USB メモリの自動再生／自動実行を利用して騙す手法を再現したものである。この事例の場合、ダイアログの「OK」ボタンを押すと、上段にある「USB メモリを開く」が選択され、USB メモリに格納された実行可能ファイル（＝ウイルス本体）が起動することになる。

図 6：USB メモリの自動再生／自動実行の再現例

- **本物を活用する：カット＆ペースト**

2008 年あたりから、「怪しいメールには気をつけなさい」という注意喚起では通用しなくなる事例が出始めた。この頃から、サイバー攻撃の活動基点が「怪しい」から「怪しくない（怪しさを感じさせない）」に切り替わり始めた。

図 7 は、コンピュータセキュリティシンポジウム 2008（CSS2008）の募集要項を装ったウイルス添付された電子メールである。受信した電子メールの本文に記載されているメッセージは、ウェブサイトに掲載されていた募集要項から切り貼り（カット＆ペースト）して作成された文面であり、怪しさをまったく感じさせない。もちろん、この電子メールに、ウイルスファイル（ウイルスが埋め込まれた PDF ファイル：css2008-cfp.pdf）が添付されていたことは言うまでもない。

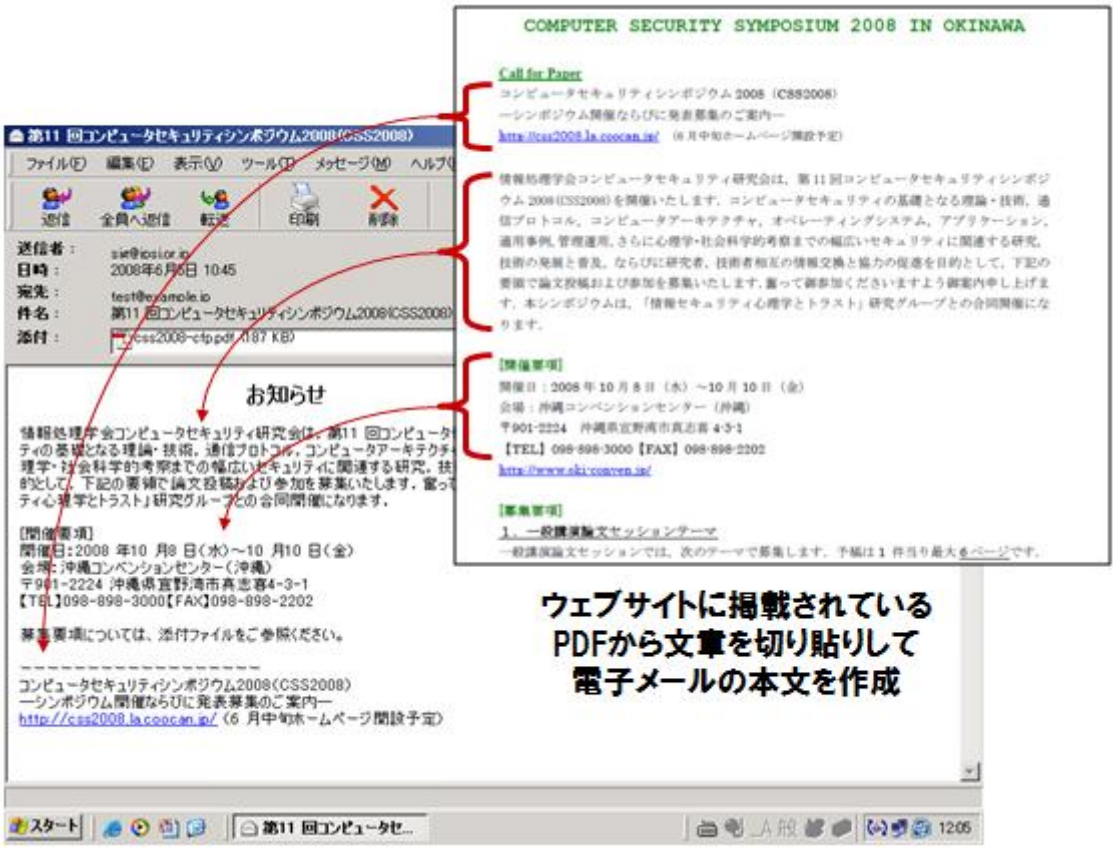

図 7：怪しさを感じさせないウイルス添付された電子メールの例

2.6 2009 年

- **本物から誘導する**

2009 年に入ると、電子メールだけではなく、ウェブサイトにおいても、「怪しいウェブサイトには気をつけなさい」という注意喚起だけでは通用しなくなった。2009 年 5 月に出現したガンブラー（Gumblar）は、一般的なウェブサイトの一部を改ざんして、図 8 に示すようなブラウザ上には表示されない誘導コードを蔵置する。このため、ユーザは一般的なウェブサイトにだけアクセスしていると思い込む。しかし、ブラウザは蔵置された誘導コードにより、一連の攻撃活動（ウイルスをダウンロードするサイトにアクセスした後、脆弱性を悪用されてウイルスに感染する）の渦中に巻き込まれてしまうことになる。

ソーシャルエンジニアリング攻撃という点では、怪しいサイトにアクセスしていなければ大丈夫であろうという心理的な隙を利用していることになる。

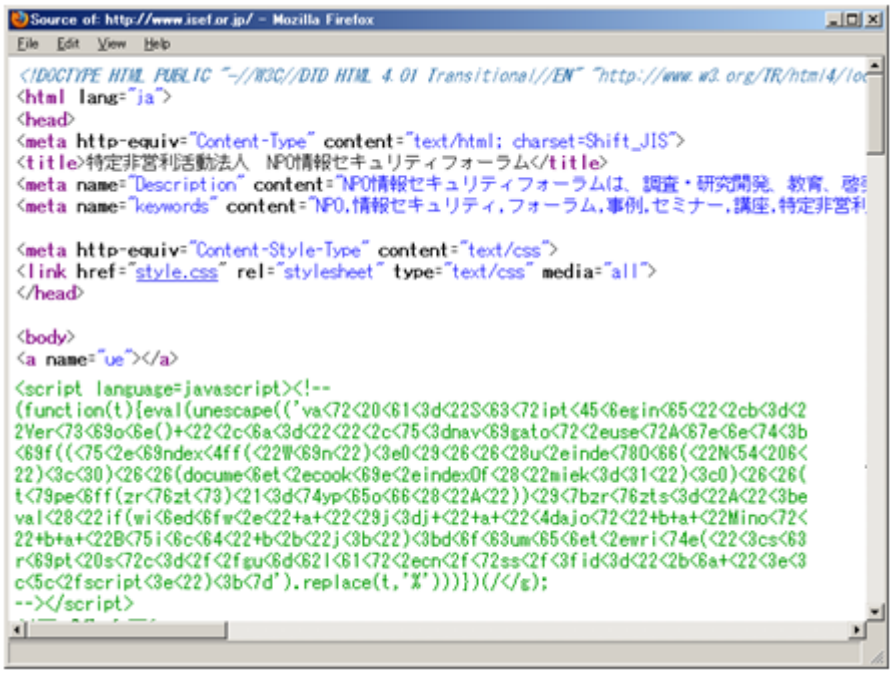

図 8：ウェブサイトを改ざんした誘導コード蔵置の再現例

2.7 2011 年

- **<u>問題のない操作であると勘違いさせる：アイコン偽装＋ファイル名偽装</u>**

2011 年 9 月に出現したアールエルトラップウイルス（RLTrap）は、Unicode 制御文字の RLO（Right-to-Left Override）を利用してファイル名偽装した。RLO は、アラビア文字など右から左に記述する文字のために書字方向を変更するための制御文字である。この RLO の制御文字をファイル名の途中に挿入することにより、画面に表示されるファイル名の右端に来る文字列を pdf などの無害な拡張子に見せかけることができてしまう。図 9 は、PDF ファイルのアイコン偽装と RLO を利用したファイル名偽装を再現したものである。

問い：どちらが PDF ファイルか？

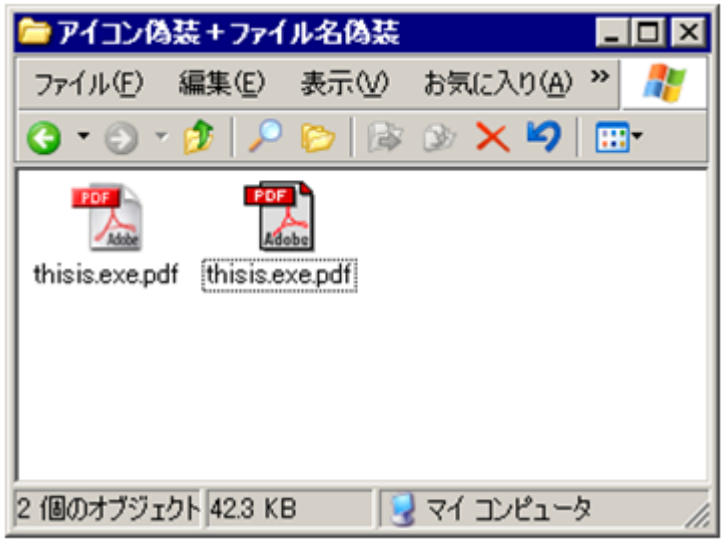

図 9：RLO を利用したファイル名偽装の再現例

答え：左側のファイル名は「thisis.exe.pdf」であり、右側のファイル名は「thisis.」と「fdp.exe」の間に RLO 制御文字の入った「thisis.[RLO 制御文字] fdp.exe」となっている。「PDF ファイルは左側である」が答えである。

- **本物を活用する：再送**

2011 年の標的型攻撃の電子メールでは、電子メール（オリジナル）を搾取した後、その電子メールに添付されているファイルをウイルスファイルに入れ換えて再送するという高度なソーシャルエンジニアリング攻撃が行われている。

図 10 は、その攻撃を再現したものである。再送された電子メール（右）には、本文に「メール送信に失敗したかもしれませんので、再送いたします。」という文章が追記され、添付ファイルのひとつがウイルスファイルに入れ換えられている。もし、電子メールの発信元パソコンが遠隔から操作可能なウイルスに感染していたならば、このようなことも実現可能であることは容易に類推できる思う。

図 10：2011 年の標的型攻撃のメールの再現例

3 さいごに

電子メールなどで利用されてきたソーシャルエンジニアリング攻撃を年代毎に振り返った。すべての手法を提示できているわけではないが、技術は継承され、いろいろな工夫が取り込まれていくことにより、年々巧妙化する手法の変遷を感じとって頂けたのではないかと思う。

標的型攻撃の電子メールの中にも、巧妙なものもあれば、明らかに怪しいもの（文字化けしたメッセージ、体裁がくずれたメッセージ、応募もしていないキャンペーン当選メールなど）もある。まずは、ユーザ自身が、明らかに怪しいものを見分ける努力をしなければならないと思う。そして、ここまで巧妙になってくると、明らかに怪しいものでもクリックしてしまうユーザの数を減らすための注意喚起や教育などの施策だけではなく、技術的にユーザを守るための施策でかためていく必要性がある。

情報セキュリティに携わる者にとって、これからもサイバー攻撃との戦いは続く。

2012 年3月２８日発行

特定非営利活動法人　NPO 情報セキュリティフォーラム
〒221-0835
神奈川県横浜市神奈川区鶴屋町 2-17　相鉄岩崎学園ビル
TEL(045)311-8777　　FAX(045)311-8747
E-Mail: isef@isef.or.jp　　URL: http://www.isef.or.jp