Web 世界を安全にする試み

インターネットが生み出した WWW の世界は，21 世紀の「大いなる西部（Wild Wild West）」だといわれてきたが，最近ますます現実味を帯びてきた．未開拓の西部と同じように限りないビジネスチャンスとアウトローによる危険に満ちている現在の Web 世界で，秩序と安全がいつ確保されるのか？　今回は Web 世界でのホットな出来事をとり上げる．

◆スパムメールの洪水

世界中で問題になっているが，最近のスパムメールの多さには辟易とさせられる．この 1 年での増加は著しく，私でも 1 日に平均数十通も受け取るようになった．多くは勧誘のメールだが，詐欺目的のメールもかなり混じっている．勧誘もお国柄を反映しているようで，米国では薬価の安いカナダからの処方薬のオンライン販売など健康医療関係がほぼ半数を占める．その他はローンや学位取得，出会い系などさまざまな勧誘である．昨年末に大統領が署名して成立したスパムメール規制法（CAN-SPAM 法）が今年 1 月から施行されているが，規制が緩いこともあって，その効果はあまり見られず，スパムの数は増大し続けている．現在では電子メールのトラフィックの 64% から 83% を占める．

とりあえずの対処法として，大手の ISP がフィルタリングサービスを提供しているし，対策ソフトも出回ってはいるが，なかなかうまく機能しない．フィルタリングを難しくしているのは，出す側がさまざま悪知恵を使っているからだ．スパムメールを調べると，それらの工夫の跡が見える．

送信元や返信先の成りすましは，電子メールのプロトコル SMTP（Simple Mail Transfer Protocol）の弱点を使って早くから行われてきた．メールの内容でチェックするために，Bayes 統計を使ってメール中の特定単語の出現頻度パターンで識別する方法が導入された．すると，送り手は出現頻度を変える細工を凝らして，フィルタの働きを無効にした．たとえば，背景と同色の文章を文面に埋め込んだり，判読不能なほどの小さな文字の文章を追加したりする細工が使われている．また，単語の綴り文字を別な文字や記号に変え，人間には単語の意味が連想できるが機械には認識できなくしてフィルタをすり抜ける．まさにイタチごっこだ．人間の悪知恵に対抗できる強力な適応性の高いフィルタがぜひともほしいが，なかなか難しそうだ．そこで，現実的な対処法として大手の ISP で構成された ASTA（Anti-Spam Technical Alliance）が，スパム対策のベストプラクティスを 6 月に発表した．当面はそこに書いてあるような対処療法で凌ぐしかなさそうだ．

◆フィッシング詐欺

今年の春に急激に増えたこの詐欺を私も早々に経験した．取引銀行であるシティバンクを装ったメールを受け取ったのは 4 月だった．トラブルが起きたので，書かれてある Web サイトにアクセスして対応してほしいと書いてあった．対応しないと口座が利用できなくなるとも警告していた．そのメールはロゴも含め本物のメールそっくりで，指定された Web サイトの URL も本物そっくりだった．指定サイトにアクセスすると，個人情報や銀行口座番号や暗証番号の入力を求められ，指示通りすると情報をそっくり盗まれるという按配だ．幸いにも私はこのような詐欺の手口を知っていたので，引っかからずに済んだ．eBay からというメールも受け取った．それにしても，メールや Web サイトがあまりにもうまく偽装されていたので，こんな手口を知っていなければきっと騙されてしまう．事実，騙された人も多いようで，米国では年間 24 億ドルもの被害になるという．クレジット社会の米国では個人の信用履歴が重要な信用基準になっているので，個人情報を盗まれ悪用された被害者は，金銭的な被害に加え，失墜した信用履歴を簡単に回復できず，実生活で大変な苦労を背負うことになる．

この詐欺のたくらみを検知する方法はあるという．メールや Web サイトをうまく偽装するために，本物のサイトに長時間アクセスして詳細に調べるので，それを検出しようというわけだ．これも簡単に裏をかけそうで，

米国富士通研究所
松尾 和洋　*kmatsuo@fla.fujitsu.com*

どれだけ有効かまだはっきりしない．

◆ソーシャルエンジニアリング

インターネットにおけるセキュリティ対策としては，ウイルス対策技術，暗号技術や認証技術，安全なネットワーク接続技術などの技術的な課題が主に考えられてきたが，それだけで十分ではない．人々の普段の行動がネットワークを通して世界に広がっているので，そこにセキュリティリスクが生じる．それをどう減らすかも重要だ．フィッシングは安全なネットワーク接続ができれば防御できるというわけではない．

ソーシャルエンジニアリングとは，社会工学という学問分野を意味し，大学の学科名にも使われている．ところがセキュリティの分野では別な意味で使われる．人と社会的に接触することにより重要な秘密情報を搾取する技法やその研究のことを指す．先に述べたフィッシングもこの類である．ところで，フィッシングは phishing と綴り，釣りと同じではない．sophisticated fishing に由来するともいうが，真偽のほどは知らない．

メールや Web サイトをそっくりに偽装することは比較的簡単だ．発信元の名前も Web サイトの URL も簡単に成りすませるのなら，いったい何を信じればいいのだろう．送り手は最初は無差別に送りつけていたが，最近は確実な相手に的を絞るようになっている．ますます巧妙になり，危険度も高まっている．このまま放置すれば，電子メールはゴミの山になり，インターネットは情報をサーフィンするだけに使われ，誰も E コマースに参加しなくなってしまう．

◆では，どうする

「大いなる西部」とは異なり，Web 世界はインターネット技術を基盤にしている．適切な技術を開発し，その技術を利用したシステムをみんなが受け入れれば，「秩序と安全」は早急に確立できるはずだ．スパム対策を含め，電子メールを安全で確実なものにするためには，まずメールの発信元の認証をしっかりすることである．6 月に開かれた電子メール技術会議でもインターネットプロトコルの発明者の一人である V. Cerf 博士が同様の発言を基調講演で行っている．

今春，IETF（The Internet Engineering Task Force）はスパム対策の標準技術を策定すべく，ASRG（Anti-Spam Research Group）というワーキンググループを設置して，DNS（Domain Name System）ベースのメール認証システムの確立を進めることにした．また，米国の主要なプロバイダもいくつかの対策技術を考えている．Yahoo ではメール送信者の身元確認のために暗号化された鍵をすべてのメールに添付するシステム（DomainKeys）を支持している．AOL や Google は IETF が検討している SPF（Sender Policy Framework）と称する DNS データベースを変更して送信元を認証するシステムを試験導入することを考えている．Microsoft も Caller ID を使った独自のシステムを開発してきたが，SPF との技術統合に動き出した．ともかく一刻も早く標準となる技術を確立して，現実に運用できるようにする必要がある．

メールの発信元が管理できれば，メールの発信に従量制の課金システムを導入することも考えられる．通常利用者には小額で，多量のメール発信には高額な料金を徴収すればいい．課金については，たぶん社会的な抵抗が大きいだろうが，安全を確保するシステムを早期に導入するためには，何かうまいビジネスモデルが必要だ．Web の場合も情報発信元の URL を偽証できるというセキュリティホールをなくさなければならない．現在のインターネットの匿名性はある程度制限されるが，健全なプライバシ保護の仕組みをうまく造って，皆が安心して使えるようにすることが何より大切だ．

◆やっと本気

現在でも Web 世界は秩序と安全がまだ確立できていなく，最近の状況はますます危うくなっている．でも，ほとんどの人は Web 世界のない社会には後戻りしたくないはずだ．そうだとすると，多少の犠牲を払ってでも Web 世界に秩序と安全を確立する仕組みを入れていくことになる．技術的には難しい問題ではないだろうが，これだけ普及した仕組みを変えるとなると大事になる．まず，産業界が協調して技術の標準化を早急に進め，その技術を使ったシステムを Web 世界に試験導入して，人々が納得できる新しい社会的な仕組みを造りあげる．重要な社会基盤なので社会的コンセンサスを確保することがとても大切だ．これにはずいぶん時間がかかりそうだ．でも，現在の危機的な状況を前にして，みんなやっと本気でなんとかしなければと動きだしたようだ．

参考文献，参考 URL
1）CAN-SPAM 法 : http://www.spamlaws.com/federal/108s877.html
2）スパム対策の提案書 : http://docs.yahoo.com/docs/pr/pdf/asta_soi.pdf
3）ソーシャルエンジニアリング :
http://www.securityfocus.com/infocus/1527
4）電子メール技術会議での V. Cerf 博士の講演 :
http://news.com.com/2100-1024-5238202.html
5）スパム対策技術 : http://news.com.com/2102-7349_3-5176415.html
（平成 16 年 8 月 4 日受付）