エッセイ	「白拍子」

神尾 博

標的型攻撃の第一ステップは、不正プログラムや不正リンクを埋め込んだフィッシングメールである事が多い。巧みにたぶらかした後はバックドアを仕組んだり、PCやサーバを支配したりすることで、内部の重要情報の詐取や、データの破壊活動等の悪事を働く。

悪質メールの侵入阻止には、偽装メールアドレスをSPF（Sender Policy Framework）等の送信者ドメイン認証でフィルタリングする事が一定の有効性を持つが、相手の送信側でも導入されていなければ無意味である。また攻撃メールを模した電子メールを組織員に送信するといった演習も役立つが、2012年のNISCの公表では、訓練で添付ファイル開封が10.1%、リンククリックが3.1%とあり、なかなか万全とはいかない。

実際、偽装メールには手の込んだソーシャルな手法が用いられる。SNSでターゲットを探し、素性を徹底的に調査する。その後、綺麗どころ やイケメンを装い組織のキーパースンに近付いたりするから、たちが悪い。

架空の美女を使った「ロビン・セージ実験」の結果報告は衝撃的だ。彼女の虚偽のプロフィールはMIT卒で25歳、現在は海軍のサイバー攻撃の脅威に関する分析官というもので、写真はアダルトサイトから拝借している。１ヶ月弱の間にSNSで作った「友人」には、軍や政府の関係者も含まれていて、個人情報のやり取りや有名企業への勧誘まであったという。

こちらはあくまで研究目的だが、趣味で演じる「ネカマ」の歴史は古い。インターネットの黎明期から出現し、2000年発刊の文献にも「ネカマ道」という老舗サイトが紹介されている。当時から「本格的なネカマを見分けるのは一筋縄ではいかない」とされているから、状況は変わっていないどころか、ますます熟達しているようだ。一方の男子への扮装は、平安時代末期からの、女性による男装の歌舞「白拍子（しらびょうし）」を髣髴する。芸能者、そして遊女であり、平清盛や源義経といった、当時の権力者の寵愛を受けた祇王や静御前が有名である。

標的型攻撃に持続性（執拗）を加えたものが、一般的に「APT（Advanced Persistent Threat）」と定義されている。執拗と言えば、歌舞伎や能には清姫の扮した白拍子が登場する。この乙女もなかなか粘着質だ。約束を反故にして、いつまでも結婚に煮え切らない山伏をストーキングの挙句、ついには大蛇に変身し、道成寺の鐘の中に隠れた男を情念の炎で灰にしてしまったという過去を持つ。

ネットでも相手を騙せば、当然ながら報復のリスクが発生する。品行方正でもネットストーカーに付きまとわれる可能性だってある。蛇のような妄執は巳年に限らず、これからも「持続的」にネットの中を徘徊し続けるに違いない。

「白拍子」葛飾北斎・画（江戸時代）