

さようなら、 意味のない暗号化 ZIP 添付メール



編集にあたって

—儀式セキュリティ PPAP：日本のセキュリティ・ルネサンスに向けて—

崎村夏彦 | NAT コンサルティング

見世物小屋セキュリティ

セキュリティ・シアターという言葉がある。筆者は見世物小屋セキュリティと呼んでいるものだ。米国の著名なセキュリティ研究者である Bruce Schneier によって 2003 年頃に使われ始めた単語で、その意味するところは「セキュリティが向上したというお茶の間の安心感のために、実質的なセキュリティ向上には寄与しない対策に投資する行為」のことを意味する。

アメリカで作られた単語であるから、アメリカでもこうした意味の疑わしい対策はある。よく引き合いに出されるのは、空港におけるむき出しの銃を抱えた武装州兵のパトロールである。事情をよく知らない一般消費者からすれば、彼らはテロリストから自分たちを守ってくれていると思うのであろうが、実は州兵の銃には銃弾が装填されていないので、テロリストの来襲には対応できない。まさに、「安心」対策であって「安全」対策にはなっていない例と言えよう。

こうしたセキュリティ・シアターでとられる対策の大きな特徴に、芝居の脚本で出てきそうな脅威を扱うという点がある。芝居で扱う脅威は、現実それが大きな影響を持つかどうかよりも感情に訴えることを旨とする。たとえば、テロリストが靴底に爆弾を隠して持ち込んで、自分の乗る飛行機が爆破されるなどだ。確かにその可能性はあるかもしれない。しかし、そこだけ塞いでも、他の道を塞がなければ、単に迂回されるだけなので意味がない。セキュリティ対策は包括的に行われなければならない。あまりに狭い範囲の対策で安心するのは、誤った安心感というべきものであろう。そして、このような誤った安心感を得るための対策は有害である。

有害である理由はいくつかある。

1. 安心感を得たために、本来すべき対策をしなくなる。
2. 安心感を得るために不必要な費用をかけ、本来の対策にまわす費用が少なくなる。

などがその代表例だ。

一歩進んだ儀式セキュリティ

しかし、靴底爆弾のチェックというのは、一応科学的な根拠があることはある。これに対して、怪しげな宗教の壺やら儀式などには科学的根拠はない。さらに、最近では「新型コロナウイルスを消毒する」として、信者の口に塩水でスプレーを吹きかける儀式をして集団感染を起こす教団まである始末である。こうした科学的根拠のない心の平安のための対策のことを、セキュリティ・シアターを一歩進めて、筆者は儀式セキュリティと呼んでいる。そして、日本にはこうした儀式セキュリティが多い。こうした儀式セキュリティの代表例が、昨今、情報漏えい対策として日本でのみよく見られるようになった「PPAP」である。

PPAPについては、第1章以降で詳しく触れるが、ざっくりいうと、パスワード付き暗号化ファイルを作って添付ファイルとしてメールで送り、同じメールアドレスに今度はパスワードを送るという対策である。途中の経路の情報漏えい対策や誤送信防止対策として行われるようであるが、元のメールを受け取れる人ならば、次のパスワードも受け取れるので意味はない。つまり、科学的根拠はない。それどころか、受け取り手は、メールゲートウェイでのウイルスチェックなどができなくなるところなど、上記の新型コロナウイルス拡散儀式的ですらある。

儀式セキュリティと日本人

さて、このPPAPであるが、海外ではほとんど見ることができない、印章（ハンコ）と並ぶ日本に特徴的な慣行である。紙+印鑑というのも、原本性と本人同意の確認を目的としているのだからセキュリティ対策と言えるだろうが、PPAP同様科学的根拠はない。

はじめからなかったわけではない。かつては、目の粗い紙にインクや墨など連続的に濃度が変わり、

書いたあとは酸化が進み経時の変化を反映できる手段で内容を染み込ませて記録し、毎回ランダム性が付与されるために複製が難しいとされる手掘りのハンコで印章を押すことにより改ざん検知と作成者認証をしていたのだから科学的なセキュリティ対策になっていた。

しかし、現代で紙とハンコを要求する人たちは、このことをきちんと考えているだろうか？ 外見だけを儀式としてなぞっているのではないだろうか？ 現状は、表面にコーティングが施されたコート紙に、均質かつ安定的なトナーで表面に着色、印影から3Dプリンタで安価に複製できる印章を使って印影をつけているわけだが、内容は表面に均質に付着しているだけなので修正は可能だし、寸分たがわぬ印章をつけることも容易である。紙+印章というセキュリティ手段は完全に危殆化してしまっているのだ。科学的根拠はない。あるのは儀式としての意味だけである。そして、これを非難するものは異端として糾弾される。

日本における セキュリティ・ルネサンス

実はパスワード付きファイル送付も、紙に文を記載して朱肉を付けるという行為も、正しく行えば効果はある。問題は、どのような脅威に対応しようとしているかを考えるのをやめてしまい、儀式として行い続ける行為である。

本特集では、第1章でPPAPが生まれた経緯、第2章、第3章でそれぞれの立場からのPPAPの評価と大対策、第4章で「社会からPPAPをなくすには？」と題し座談会を行い、より良い方策を検討している。

本特集が、科学的根拠のない儀式を盲信する中世的セキュリティ感から日本を脱却させる「セキュリティ・ルネサンス」成立の一助となれば幸いである。

(2020年4月15日)