総　論

最近のセキュリティ脅威の動向と企業における情報セキュリティマネジメントの在り方

情報セキュリティ大学院大学
内田 勝也

はじめに

情報セキュリティという言葉を聞くと直感的に、技術的な問題での解決を考える人達が数多くいる。しかし、現在のネットワークの爆発的な普及や企業内での一人一台のパソコン利用の環境が達成され、多くの人々が関係していることを考えると、情報セキュリティの問題は、人間の問題が多くを占めるのではないかと考えても不思議ではないであろう。

実際、2006年に世界各国で発生した情報流出事件のうち、1回でもメディアに取り上げられた145件についての調査※1がある。情報流出は、過失によるものが77%と圧倒的に多く、業種や地域による偏りは見られず、大企業や中小企業、政府機関、軍などで流出が起こっている。

また、2006年3月に内閣府の国民生活局が実施した「個人情報の保護に関する事業者の取組実態調査※2」でも、表1に示すような結果になっている。

どこまでを過失と考えるかによるが、1から4までを過失と考え、5、6を故意と考えると、過失91%、故意9%となる。また、1から3までを過失と考えると、過失と故意の割合は65%と35%となるが、過失が故意を大きく上回っている。

現在の情報セキュリティ対策を単に技術的な対策だけでなく、人間的な問題として考えることも大切と思われる。

目的の明確化

2005年4月の個人情報保護法の完全施行以来、多くの企業等では、ノートパソコン等の持ち出しを制限したり、ファイルの暗号化を行っている。

特に、ノートパソコンの持ち出しを禁止しているケースでは、それで全ての従業員が問題なく業務を遂行できるのであろうか？

ノートパソコンの持ち出し禁止の目的を考えると、電車の中に置き忘れたり、自動車を使っている場合に車上荒らしに遭うこと等を危惧していると思われる。

単に禁止をするのではなく、従業員の特質を考えた管理方法もあるのではないだろうか？

電車等に置き忘れる人の多くは、以下の様な人が多いと考えている。

①普段、何も持たない
②電車内で荷物を網棚に上げ、座っても荷物を膝上に置かない
③パソコンを持っているのに、お酒を飲んで帰る

表1　内閣府国民生活局の調査

漏えい発生原因	回答割合(%)		
1. 従業者の置忘れ、施錠忘れ等の過失	21.3	61.7	65.0
2. 従業者のインターネット利用上の過失(メール誤送信、HPへの誤掲載等)	8.6		
3. 従業者(含 退職者)が盗難にあった(含 車上荒し等)	14.2		
4. 委託先・運送業者の漏えい等	17.6		35.0
5. サーバ／PCへの攻撃(ハッキング・ウイルス感染等)	2.8	6.4	
6. 従業者の個人情報持出し、売却・譲渡・漏えい等	3.6		
7. 原因不明／その他／無回答	31.9	−	−

④荷物を２つに分けて持つ

普段から何も持たない人は荷物を持っても、それに注意が向かないことが多い。電車で座席に座り居眠りをしていて、目的の駅に着いて急いで降りる場合、網棚に上げた荷物を忘れても不思議ではない。

座席に座ったら、荷物は必ず膝の上に置く習慣や荷物を２つ以上に分けて持たない工夫が、置き忘れや置き引きに遭う可能性を低くすることになるのではないだろうか。

また、車上荒らしに遭う場合では、以下のようなことが考えられる。

①パソコン、アタッシュケース、重要そうな封筒等を助手席や後部座席に残している

②大きな駐車場では、人気のない隅の方に駐車する

車上荒らしを行う犯罪者にとって、車内を覗いても何も置いてないようであり、そばを頻繁に人が通る車より、車内に価値がありそうなものが置いてあり、周りに人気がない車の方が車上荒らしを行い易いであろう。

パソコンやアタッシュケース等の重要なものは、ダッシュボードやトランクに保管し、駐車場でも人気のない隅の方に駐車しないようにするだけでも犯罪を防止できる可能性が高くなる。

普段からこの様な問題を職場で話題にすることができれば、セキュリティ意識（セキュリティ文化？）を醸成することが可能であろう。

肩肘をはって情報セキュリティ教育を行うだけでなく、問題の本質を十分考えて、関係者全員が周知できる仕組みを考えることが大切であろう。

教育の難しさ

（1）駐車禁止マークはどちら

図１をみて、駐車禁止マークが左か右か分かるだろうか？

「正しいと思うものを左か右で回答せよ」との質問であれば、二者択一であるので50%の確率で正答を指摘することができる。しかしながら、「いずれが正しいか

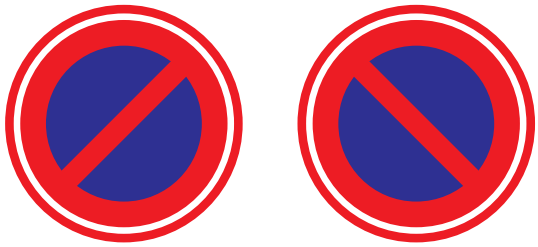

図１　駐車禁止マークはどれか？

を指摘し、その理由を述べよ」と質問をすると多くの人は回答できないであろう。

これは、駐車禁止マークの由来を聞いたことがないため正答できないものと思われる。マークの由来は、「No Parking」のNとOをもとにして作成したと教えられていれば、右のマークが正答であることは自明であろう。

またこの先、この質問をされても、大部分の人は正答することができるであろう。

何気ないものでも、質問に正答できない場合でも、その由来と共に正答を教えられれば、記憶に深く残り、以後は間違えることがなくなる可能性が高い。

（2）交通信号はどちらか

同様の問題は日本の交通信号でもある。

図２で、日本の交通信号は左か右のどれかという質問である。

これも、信号機の役割を理解させることができれば、簡単な問題で、正答は左である。

信号機は交差点で車が止まってくれることが期待して作成してあると考えれば、左側通行で右ハンドルの運転手に「赤（止まれ）」が良く見えるようにするには、

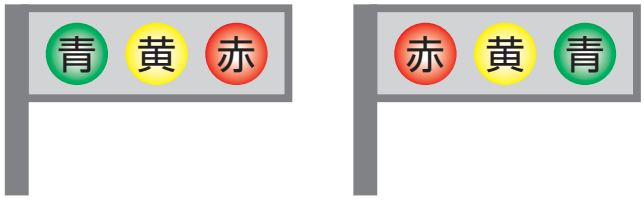

図２　日本の信号機はどれか？

左の信号が正答になる。ちなみに、歩行者信号は、赤が青よりも上にある方がよいことは容易に想像がつく。

（3）渦巻きですよ！

図３を見て、渦巻きになっていると思った方は、今までこの図を見たことがない方だと思われる。

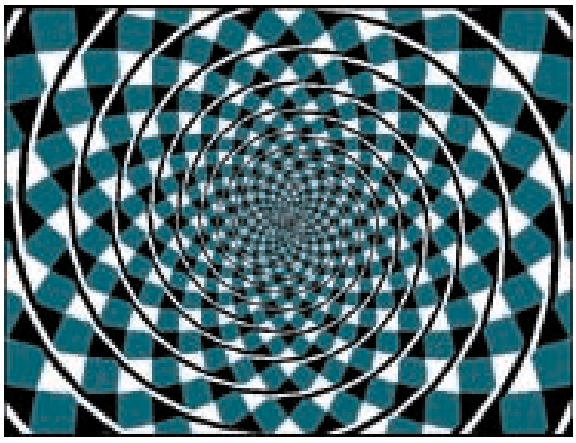

図３　渦巻き

渦巻きに見える部分を鉛筆かボールペンでなぞって見れば明らかであるが、同心円になっている。

この図は、「フレーザーの錯視」と呼ばれ、人間の五感は簡単に騙されやすいことを示している。

過去にこの様な図を見たことがある方は、「渦巻きになっている」と言われると、実際に自分でなぞることにより、錯視かどうかの判断をするであろう。

（4）三ない運動

かつて、高校生のバイク事故に対応するため、「バイクの三ない運動」と言うのがあった。これは高校生に、「免許を取らない、バイクに乗らない、バイクを買わない」という３つの「ない」からこう呼ばれた。

バイク事故から高校生を守るには、危険なもの（バイク）から高校生を遠ざけることが良いと考えた結果から出た運動であった。しかし、この運動は事故撲滅に繋がらなかった。交通安全教育を行い、安全運転意識を育むことが事故減少に繋がるとの考えが実践されると事故は大きく減った。

問題の本質を考えず、「臭い物には蓋をする」といった考えだけでは、問題が解決しない例である。

■ 総合的な対策を ■

（1）組織・個人と違反

個人が違反を犯す場合、その個人が属する組織風土を考えることも大切で、企業・組織における組織風土と違反は密接に関係しているとの研究※３がある。

組織風土の違いにより、個人的違反が容認され易い組織風土と、組織違反が容認され易い組織風土があるが、それらは異なっている。これらをまとめたものを図４に示す。

このような組織の特徴を考えると組織に属する個人への対策だけでなく、組織風土も含めて、どの様な対応を行うかが大切であることが理解できるであろう。

（2）Winny等の暴露ウイルス

少し前の話題であるが、2006年初に、官公庁、企業から情報流出が相次いだ。多くはWinny等のP2Pソフ

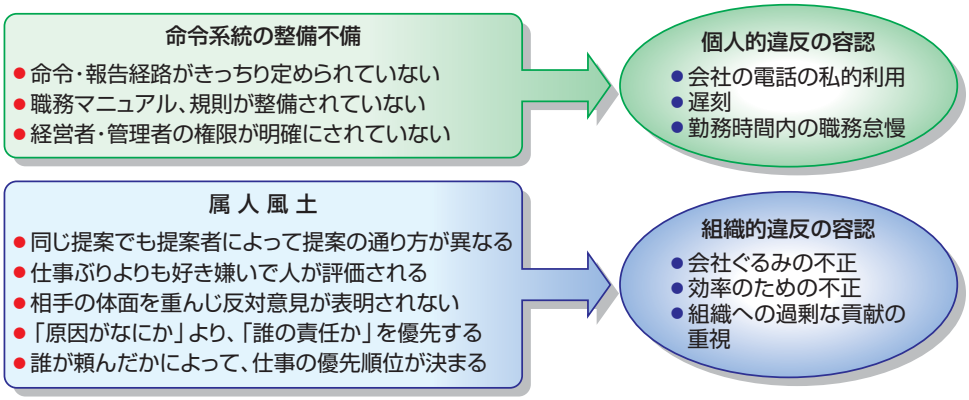

図４　組織風土による違反の相違

トの利用者が、Winny等を狙ったウイルスに感染したパソコンで個人情報や機密情報を扱ったため、それらの情報が漏えいしたものである。

特に県警や自衛隊から、重要情報の漏えいが発生したため、2006年3月、当時の官房長官が「情報漏えいを防ぐ最も確実な対策は、パソコンでWinnyを使わないこと。私（官房長官）からも国民の皆さんにお願いしたい」との声明を出した。

しかしながら、情報漏えいは止まることはなかった。考えてみれば当然であり、この様な声明をだして情報漏えいがなくなれば、総合的な情報セキュリティ対策は不要であろう。

この声明を聞いて感じたことは、前項の「教育の難しさ」（4）で述べた「三ない運動」に似ている感じがした。Winny等のP2Pソフトを使うなと言っても自宅でこっそり利用していたり、個人情報や機密情報の外部持ち出しを禁止しても、職場でパソコンを利用できる環境が十分でなければ、必ず自宅で仕事をする職員はおり、その職員がWinnyのウイルスに感染したパソコンを使って情報漏えいを起こす可能性は高い。

官房長官の声明の直後に、某官庁の情報セキュリティの担当者と話をする機会があった。「情報セキュリティ担当になるまで、情報セキュリティについて考えたことなどなかった。勿論、個人のパソコンにお金を払ってウイルス対策ソフトを導入すること等を考えたこともなかった。導入済みの『お試し版』のワクチンソフトで十分であると思っていた」と述べていた。

実際、官房長官声明後も、自衛隊、警察や日銀・支店などから情報漏えいは続いている。

組織やそこで働く人達を考えた教育・啓発が必要であることを示しているのではないだろうか。

■ ISMS適合性評価制度について ■

（1）ISMS制度の概要

ISMS※4制度は、国際的に整合性のとれた情報セキュリティマネジメントシステムに対する第三者適合性評価制度（第三者認証制度）で、国内では2001年4月から1年間のパイロット期間を経た後、2002年4月から本格運用され、2008年6月20日現在、2,677事業所が認証を取得している。第三者認証制度には、ISO9000※5（1994年に運用開始、現在、約43,400事業所が認証を取得）やISO14000※6（1996年に運用開始、現在19,800事業所が認証取得）等がある。ISMSは本格運用から既に6年以上経過しているが、これらに比べ、まだ認証取得事業所数も少ないが、確実に増加している。

しかしながら、ISMS認証取得事業所においても、情報セキュリティマネジメントシステムが十分に機能していないとの話もある。それらを踏まえ、筆者の研究室で2007年2月に、住所を公開している1,400余りの事業所に対して、郵送によるアンケートを実施し、その実態について調査を行った。

詳細は、(財)ニューメディア開発協会のウェブで公開している「ISMSの維持管理における実態調査※7」を参照して頂きたい。

この調査からISMSだけでなく、他の認証制度を含めて、幾つかの課題に明らかになった。

（2）監査概念の重要性

ISMSでは、PDCAモデルによるプロセスアプローチを基本にマネジメントシステムの構築を行っていると述べているが、第三者認証制度やISMSの確立（表2）を見る限り、監査（厳密には、業務監査：表3）の考え方が根底にある。

しかしながら、調査結果を見る限り、審査機関、審査員だけでなく、認証取得事業所担当者やコンサルタント等、ほとんど全ての関係者が、監査概念を理解できていない。

（3）リスク概念の重要性

表2で述べたISMSの確立をみてもわかるように、ISMSでは、常にリスクを考えることが大切であるが、リスクを考えていないのではないかと思われるケースが多い。

表２　JISQ27001 ISMSの確立

ISMS の確立

●**リスク対応のための、管理目的及び管理策を選択する**
管理目的及び管理策は、リスクアセスメント及びリスク対応のプロセスにおいて特定した要求事項を満たすために**選択し、導入**しなければならない。
選択は、法令、規制及び契約上の要求事項と同じく、**リスク受容基準も考慮**する。
このプロセスの一部として、特定した要求事項を満たすために適切なように、管理目的及び管理策を選択しなければならない。
管理目的及び管理策は**全てを網羅していないので、追加の管理目的及び管理策を選択**してよい。

●**適用宣言書の作成：適用宣言書は以下の項目を含むように作成する**
1) 選択した管理目的及び管理策とそれらの選択理由
2) 現在実施している管理目的及び管理策
3) 適用除外とした管理目的・管理策と適用除外が正当である理由

JIS Q 27001：2006 より

表３　検査と監査の相違

検査と監査の相違

●**検査**：決まったルールに基づいて事務手続きが行われているかどうかをチェックする。
●**監査**：ルール自体がリスクを防ぎ、内部統制上、望ましい内容かどうかをチェックする。

先端内部監査研究会 「これが金融機関の内部監査だ」（第１版）金融財政事情研究会より

本来、管理策は認証取得事業所のリスクを考慮して取捨選択されることになっている（表２）が、管理策を唯一絶対的なものと考え、審査を行う審査員が一部にいる。このため、表４の⑥や⑦の様な声が認証取得事業所側からでてくるのであろう。

本来、リスクをゼロにすることは不可能であるが、種々な方法でリスクを小さくすることが、あるレベルに達すれば、表２で述べているように、「リスクを受容」することになる。

（４）制度の運用体制の重要性

表４ アンケート回答等の例

① ISMSの要求レベルは、顧客などのステークホルダーの要求を満たしていない。さらに高いレベルの対応が必要
② 顧客先で顧客の指示に従ってシステム開発を行っている場合のISMS適用形態がわからない
③ 管理策全ての対応を要求される
④ 非常に優秀な審査員で、指摘事項に対する対策まで考えてくれた
⑤ J-SOXには、ITIL（ISO/IEC 2000）で対応する必要がある
⑥ 審査員の質、現場、経営者の立場での視点の欠如、技術を知らない
⑦ 審査員は管理策を杓子定規的に適用するだけで、付加価値のある審査が望めない

昨年、アンケート調査を行ったこともあり、複数の審査機関の方々や認証制度に関心のある方々との意見交換では、「海外の制度は日本に馴染まない」といった制度自体の課題を指摘する方々もいる。しかし、筆者は、制度運用上の課題の方が重要な感じがある。

少なくても、ここで述べた、「監査概念」や「リスク概念」を多くの関係者に啓発し、理解を得るだけでも大きく違ってくる。

しかしながら、一度、確立した制度を変更することは非常に困難が伴うから不可能だとの指摘もあるが、時間の経過や環境の変化で、当初策定した制度や仕組みに多くの課題がでてくる可能性は十分ある。 制度検討時点で全ての課題を考えて構築できなければ、一定期間後に見直しをすることは当然であろう。

また、そうは言っても社会的に大きな問題にならないと変更は難しいとの指摘もあるが、小さな問題への対処が、結果的に、制度自体を長期に安定化できるのではないか。これは、「割れ窓理論」の実践で、安全な町になったニューヨーク市の例を考えれば明らかであろう。

※１ ロシア企業の調査
http://www.itmedia.co.jp/news/articles/0702/17/news011.html
※２ 内閣府国民生活局の調査
http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20070425kojin2.pdf
※３ 鎌田晶子 「『組織風土』とヒューマンエラー」（大山正・丸山康則 編「ヒューマンエラーの科学」）
※４ ISMS: Information Security Management System（情報セキュリティマネジメントシステム）の略
※５ QMS： Quality Management System とも呼ばれる
※６ EMS： Environment Managemet System とも呼ばれる
※７ 以下のURLに掲載されている：http://www.pjr.jp/bs25999_special.html