2011.1.21

情報セキュリティニュース ＜2010 No.4＞

情報管理におけるヒューマン・エラー対策

１．　はじめに

あるお客様から、ヒューマン・エラーによる情報漏えい事故が止まらないので何か対策はないかという相談を受けたことがあった。事業者の情報漏えい対策においては、多くの場合は情報の盗難など不正対策に重点が置かれているものの、個人情報の誤送付など些細な人的ミスが引き起こすヒューマン・エラー対策が後手になっていることが多かった。このお客様は事務処理を中心とした事業者で、ほとんどの職員が業務の一環で個人情報に接している。ヒューマン・エラーによる事故が頻発しており、このお客様はその対策にも重点を置きたいとのことであった。結論からお伝えすればヒューマン・エラーは完全に無くすことはできない。一方で、何らかヒューマン･エラーを少しでも減らす対策があるのではないのか、今回はヒューマン・エラーによる情報漏えい防止策について考えたい。

２．ヒューマン・エラーについて

ヒューマン･エラーとは、JIS 規格では「意図しない結果を生じる人間の行為」という定義である。ここでは情報管理上の行為におきかえて、重要情報の誤送付、誤送信、置き忘れ、紛失、設定ミスなどの情報漏えいを対象とする。

ヒューマン・エラーの一般的な研究については、交通関係、原子力関係、医療関係、製品製造関係などの業種で先行して進んでいる。特にこのような業種では、些細なヒューマン･エラーから重大な事故（特に人命に影響を与える事故）に発展するケースが多く、軽視ができないため、ヒューマン・エラー対策に関する取り組みが進んでいる。

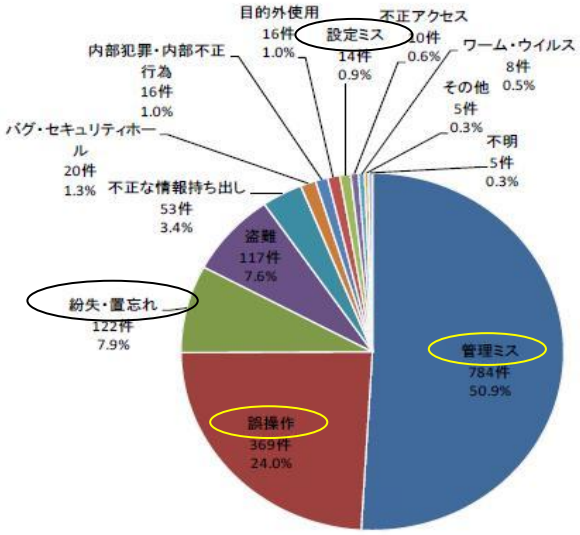
一方、ヒューマン･エラーによる重要情報の漏えい事故は人命に直接的に影響を与えることはなく、深刻な事態まで発展するケースは稀である。漏えい後の再発防止策では、FAX 送信前に二人で「二重チェック」をし、電車の網棚に個人情報の入った鞄を置かないといった「ルールの追加・再確認」、それらを徹底するための「社員教育」といったことをするのではないだろうか。確かに、そのような対策でも十分に効果はある。これも重大な事故に至っていないため、このような対策で十分と考えられていることが多い。

しかしながら問題は、ヒューマン･エラーによる単発の漏えい事故ではなく、その頻度である。ひとつひとつが軽微な漏えい事故であっても、同一事業者がそれを頻繁に繰り返せば、いつかは信用失墜や深刻な事故にも繋がるおそれがある。

今回は、ヒューマン･エラーによる情報漏えい防止策で考えられるうち、根本的なところに焦点を当ててみる。また、ここでは比較的どの業種にも適用できそうな話に限定する。

３．情報漏えい事故の傾向

NPO 日本ネットワークセキュリティ協会が 2010 年夏に発表した「2009 年情報セキュリティインシデントに関する調査報告書」に情報漏えい事故の傾向が記載されている。当該調査報告書によると、個人情報漏えいでマスコミやホームページなどで発表された事故から調査した結果、「漏えい原因比率（件数）」は図１のとおりである。



出典：NPO 日本ネットワークセキュリティ協会

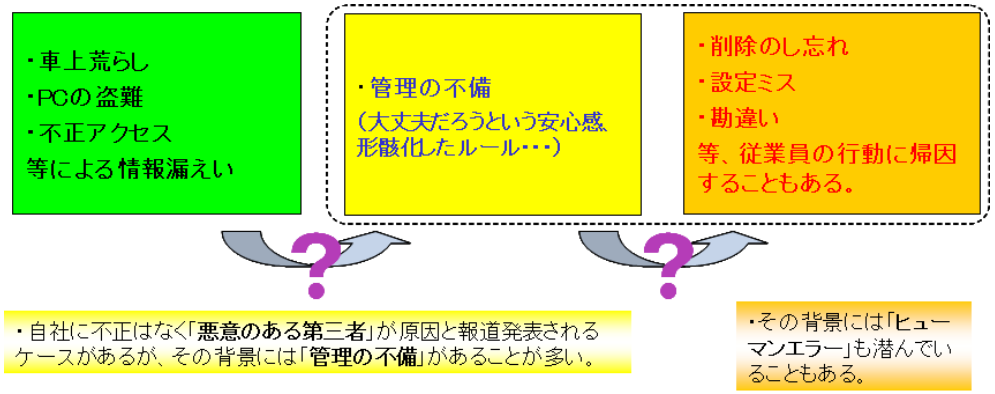
（図1）漏えい原因比率（件数）

当該調査報告書に記載されているとおり、『「管理ミス」の次に「誤操作」「紛失・置忘れ」が続く。「誤操作」は、郵送やメールの宛先を誤ることが多く、「紛失・置忘れ」は、外出中や帰宅中のUSB メモリ、ノートパソコンおよび紙ファイルの紛失が多い。これらは個人情報を取り扱う担当者のヒューマン・エラーである』ということである。ここで「管理ミス」とは、社内調査をした結果、紛失が判明した、誤って廃棄していたなどのことが後から発覚した幅広いケースを含んでいる。この図から見てもわかるとおり、事故原因のほとんどがヒューマン･エラーに属する。この種の漏えいは、今後もゼロにすることはできない。

ここで注意したいのは、調査報告書の対象は個人情報漏えいに限定しており、かつマスコミやホームページで発表されたものに限られていることだ。つまり、ヒューマン･エラーによる非公表の情報漏えい事故は水面下では相当数ある可能性が高いということである。

４．どのような対策をとればよいか

一見してヒューマン･エラー以外が原因と考えられる情報漏えいについても考えてみる。例えば、「盗難」や「不正アクセス」などである。マスコミやホームページ上の報道ベースでは、第三者の悪意による結果とされることがある。しかしながら、その背景には「管理の不備」がかなりあるのではないかと推察される。例えば、持ち出しても大丈夫だろうという安心感や、形骸化したルールなどである。さらにそれらの背景には、削除忘れ、設定ミス、勘違いなど職員の行動（ヒューマン･エラー）に起因することもあるのではないだろうか（図２）。逆から考えれば、ヒューマン･エラーが引き金となり、「盗難」や「不正アクセス」に至る可能性もゼロとも考えにくい。



（図2）情報漏えい事故の背景

そこで、「ヒューマン･エラー」の対策に限定せず、「管理の不備」の対策にも注意しておく必要がある。

４－１．「管理の不備」の対策

最初に着手したいのが「管理の不備」対策の方である。個人情報保護法が 2005 年に施行されてから、事業者の情報セキュリティ全般に対する意識が一層向上してきたものと思われる。しかしながら、最近、弊社が様々な事業者に対して監査（現場の実態調査）を実施すると、ルールが形骸化していることがよく発見される。また、個人情報についてはルールが一定整備されているものの、それ以外の重要情報、例えば設計書や企画書などの営業機密情報の取扱ルールが未整備であることが多い。

そこで改めて情報管理の実態調査を行うことを推奨する。可能な限り現場を巡回して職場内を確認することが望ましい。規模が大きな事業者は部門長に一任することも一つの方法である。社内ルールが守られているかを調査することが重要であるが、特に注目して頂きたいのは、

① 職員が帰宅した後、机の上に重要情報が残されていないか。
② 職員が帰宅した後、机の引き出しやキャビネットが施錠されているか。
③ 誰もがアクセスできる共有フォルダーに保管すべきではない重要情報はないか（アクセス権限が特に設けられていないフォルダーに、削除されずに残されているケースがある）。
④ PC のハードディスクに重要情報がないか（例えば、持出用 PC に必要以上の重要情報が保管されているケースがある）。
⑤ USB メモリ等記録媒体に重要情報がないか

などである。おそらく多くの事業者でこのようなルールがあるのにもかかわらず、実際に調査すると意外と守られていないことが多い。これらの５点は簡単に調査できることであるため、是非とも実施して実態を把握して頂きたいことである。

「社内ルール上定められていることを遵守させる」のが鉄則であることは言うまでもない。これを 1 回限りではなく、遵守させるために違反者をしつこく注意をして、強制していくことが重要である。そのために、部門長などに責任と権限を与えることで、部門長が自覚を持った上で、社内ルールの遵守についてリードしていかなければならない。特に“整理整頓”ともいえる上記①～⑤は、実は重要な項目である。重要情報を取り扱う事業者は、管理の不備を点検・是正すると同時に、ヒューマン･エラー対策にも効果のある整理整頓を徹底するのがポイントである。

一例を挙げて考えてみる。昨今では、機密情報がインターネットに流出する事件も多発している。ある事件では、共有フォルダー上におかれた機密情報を関係者が持ち出して、インターネット上に

公開するということであった。まさに前述の③が徹底されていれば、こういうこともなかったのではないだろうか。弊社が毎年監査しているあるお客様においても、共有フォルダーにおかれている重要情報に神経を尖らせている。それは、メールに添付するには容量オーバーという理由で、他部門と共有するために一時的に共有フォルダーに置かれた情報が大量に削除し忘れられたことがあったからだ。

この③の対策として考えられるのは、共有フォルダー上にある電子ファイルの定期的削除をする機会を設けることである。そのためには、共有フォルダー上の電子ファイルを一斉削除する旨を事前に伝え、他部門や他人がアクセスできないフォルダーに保管するなど、必要な電子ファイルは一度待避させる。時期が来たら、“持ち主が不明”となった電子ファイルを一斉削除する。一斉削除直前に共有フォルダー上に電子ファイルが一つも残っていなければもちろん優秀であるが、持ち主が不明な電子ファイルが多数残っていることに気づくかもしれない。

また、④⑤の調査については調査の負担がかかるが、隣人とクロス・チェックさせる（互いにPCのハードディスク内や、使用しているUSBをチェックし合う）ことを実践している事業者もある。

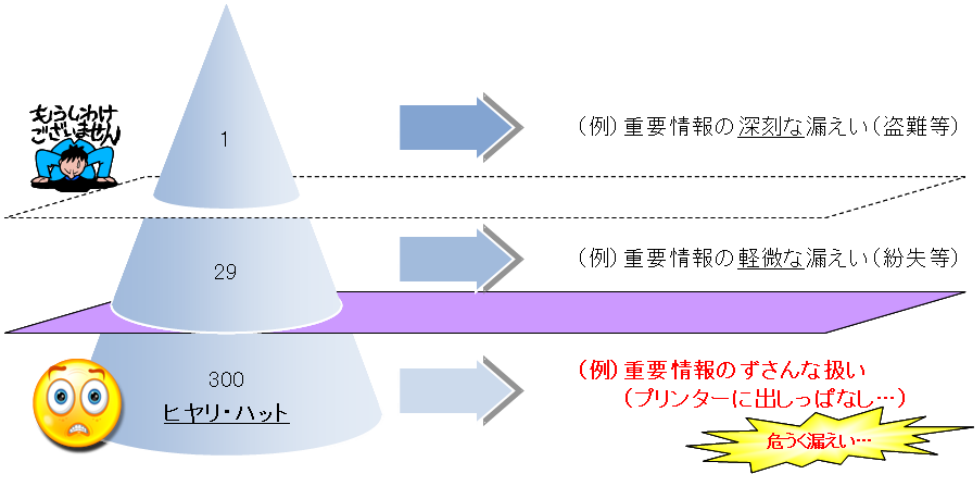
４－２．「ヒューマン･エラー」の対策

ここで、次のヒューマン･エラーによる情報漏えい防止策を検討する前に、ポイントを２つほど紹介したい。

４－２－１．ヒヤリ・ハット事例

ハインリッヒの法則というのがある。これは安全技術者のハインリッヒが見いだした法則であり、1:29:300の法則とも呼ばれる。説明すると、1件の深刻な事故の背後に、29件の軽微な事故があり、その背後に300件のヒヤリ・ハットがあると言うことである。ヒヤリ・ハットとは、「事故につながりそうなミスや事象にヒヤリとしたり、ハッとしたりすること」である。

これを情報漏えいに適応してみると、例えば深刻な漏えい事故１件（例えば大量・機密の情報の漏えいなど）に至るまでに、軽微な情報漏えい事故（例えば紛失や誤送付など）が29件ある。そしてその背後に、プリンターに重要情報が置き去りなっているのに気づいた、二重チェックでミスを発見した、などヒヤリ・ハットが300件あると考えられる（図３）。



（図3）　ハインリッヒの法則

事業者は情報漏えい事故が発生したら、その事象だけ着目することが多いが、それだけでなく、背後に隠れているヒヤリ・ハットにも着目するのが第一のポイントである。ヒヤリ・ハット事例を収集し、そこから考えてみる。そして、情報漏えい頻度をできるだけ減らすことを目標としたい。

４－２－２．個人周辺の影響

一般的に事業者では、「人が過ちを犯してしまう」ということが前提で、モニタリングを強化している。モニタリングというのは、例えばシステムチェックによるアラートの表示、二重チェックによる二人での検証作業、チェックシートや指差し確認などによるセルフ・チェックなどが該当する。このような対策は非常に有効であるが、事故が起こる度にこのようなモニタリング項目を増やしているというのが現状ではないだろうか。

ここで、さらに一歩進んで「何故、人は過ちを犯すのか」について焦点を当てる。人が過ちを犯す理由は、能力や熟練度、集中力など“個人の要素”であるため、解決は困難であると考えられやすい。実はそれだけではなく、その“周辺環境”にも要因があると考えられている。ご参考までに、その代表的なモデルが東京電力原子力研究所ヒューマンファクター研究室による m-SHEL モデルを簡単に紹介する。

これは、ヒューマン・エラーは「個人の要素」と「周辺環境が個人に及ぼす要素(頭文字をとって m、S、H、E、L)」があると示される。例えば、情報漏えい事故に適応させてみると、個人の要素の周辺は、

m（management）･･･部門長など上長による指導力不足など
S（software）･･･わかりにくい手順書・ルール・指示など
H（hardware）･･･誤操作をしやすいシステムなど
E（environment）･･･資料が散乱など
L（liveware）･･･周りの人たちからの圧力など

と考えてもよいだろう。

これらの１つ１つの詳細な分析はさておき、要は「周辺環境も個人に影響を与える」ということを認識しておくのが第二のポイントである。すなわち、当事者のみならず、その周辺環境にも眼を向けてみて、そこに問題があるようであれば改善をしてみるということである。

４－２－３．職員目線での取り組み

さて、ここから上記２つのポイントを押さえ、職員にアンケートをまず実施してみる。アンケートでは、ヒヤリ・ハットの収集と、本人の問題及び周辺環境に関する問題を収集すること、他に職員が日頃している工夫や疑問も併せて収集するとよい。それを元に、ルール策定サイド側の目線ではなく、職員目線でヒューマン・エラーを少なくする環境に変えていこうというのが趣旨である。

では、実際に取り組んだ例をご紹介する。重要情報を取り扱う職員からアンケートで収集した情報とは、例えば、「お客様がいらっしゃると、作業中の書類を放置してしまう職員が多い。担当を分けた方がいいのではないか」、「●●の時に、危うく漏えいしそうになる。そういうときに当部では○○している」、「これはよく注意して操作しないと間違えてしまう。だから私は△△しないようにしている」、などのヒヤリ・ハット事例や職員の工夫・疑問である。特に、既存ルールとは別の、職員が現場で考えている工夫などが多く収集できた。職員の方は現場においても、独自に工夫しながら作業をしていたのである。

次に、そのアンケート結果を整理したうえで、その情報を職員で共有し、集合研修の中でディスカッションさせてみた。職場によくあるヒヤリ・ハット事例や、周辺環境の問題、個人の工夫などはこのような機会がないとなかなか共有されない。そこで他の職員の工夫や疑問などを共有することにより、「なるほど、それは明日から実践できそうだ」、「こうしてみたらどうか」、「それをルール化しよう」など職員の自発的な行動がみられた。また、個人の IT リテラシーが一定レベルに揃っていないことも明確になった。例えば、Excel などの通常使うツール類のオプション設定ひとつで作業

負担が変わる（作業ミスを減らすきっかけとなる）ことを知らなかったなどである。

このように、アンケートとディスカッションをしていくうちに、意外な発見ができた他に、そこで自発的な行動が生まれたことは興味深い。通常は、情報管理を統括する責任部門などがルールを定め、職員にそれを従わせているはずである。それだけではなく、ルール策定側では気づかないことを摘み取り、新たに職員目線でもルールを見直してみる、必要に応じて改善をする、というのはヒューマン・エラー対策には有効ではないだろうか。

５．具体策例

ここでは、現場で生まれたルールの実践など興味深い取り組み事例についてご紹介したい。

（１） 合わせ技

もともとは環境 ISO の一環でこのような運営をしていた企業で、そこに情報漏えいの観点でもチェック項目を追加した“合わせ技”をした例である。これはある職場で生まれたルールを全社的に適用した例だ。

『４－１.「管理の不備」の対策』でも触れたように、机上等の整理整頓はヒューマン・エラー対策として効果が期待できる。ご紹介するのは、職員各自が帰宅前にチェックシートを用いて、整理整頓等をした旨を掲示するというやり方だ。チェックシートの内容は、

- 机の上・机の下を片付けたか（重要な情報が放置されていないか）
- 机やキャビネなどを施錠したか
- PC のハードディスクに余計な情報はないか
- PC の電源をオフにしたか
- ゴミ箱のゴミは捨てたか

などである。

それだけではなく、最終帰宅者は帰社した職員の机にチェックシートが掲示されたか、共用プリンター等の電源をオフにしたかなどについても別にチェックをする。チェックシートが掲示されていない職員がいた場合は、最終帰宅者は当該職員の机上にレッドカードを置き、警告するという運営である。

（２） 間接技

机の上・下を整理しろと指示してもなかなか改善されない、という悩みもよく聞く。このような場合は、そこに梃子を直接入れるのではなく、間接的にやらせるというのも一手である。例えば、ある事業者は、職員の作業場所を強制的に引っ越しさせていた。そうすることで、机周りの片付けが期待され、自ずと不要な情報を廃棄させるというのが狙いである。

（３） 情報漏えいゼロ運動の実施

工場などでは、過去の事故から「無事故日数連続〇日」という掲示をして、そこの従事者に安全を心がけるよう促している。ある事業者では、これを応用し社内ホームページで「情報漏えい無事故〇日」ということを職員に通知している。こうすることで、記録を伸ばすことに全員一丸となり、一人一人の意識を向上させるという効果が期待できる。

（４） 好取組事例の全社的紹介

情報セキュリティ担当者が定期的に職場を訪問（面談や現場調査）している事業者もある。主に、情報管理上の問題点を指摘することが主でもあるが、それと同時にその職場の好取組事例についても調査を実施している。この事業者では、情報セキュリティ担当部門が社内報を定期的に発行して

おり、そこで職場の好取組事例を紹介している。各職場の工夫は情報セキュリティ担当者のような第三者でないと気づかないことが多い。ここでの狙いは、重要情報の管理状況を点検し、問題があれば是正させるだけでなく、好取組事例を社内報で紹介し、他の職場でも参考にして頂こうということである。社内報で紹介された職場のモチベーションアップにも繋がっているという。

６．まとめ

以上、重要情報管理におけるヒューマン･エラー対策について考察してきた。ヒューマン･エラーはそう簡単に取り除くことはできない。しかしながら、ヒューマン･エラーの削減を積極的に取り入れている業種の工夫を情報漏えい対策にも応用することで、その効果も期待できるのではないだろうか。そのためには、地道な整理整頓、ヒヤリ・ハット事例の収集はもとより、職員の目線も取り入れ、ルールを見直してみるというのもよい。情報管理におけるヒューマン･エラー対策はこれだけではないが、まずは基本的なところから実践し、情報漏えい対策に少しでもお役に立てば幸いである。

以上

株式会社インターリスク総研
マネジャー・上席コンサルタント　石丸　英治

［参考文献］

・小松原明哲著『ヒューマンエラー 第２版』丸善（2008 年）