

情報セキュリティに関する第三者認証の効果

小川陽平 ●株式会社コスモスモア ファシリティ事業部 部長

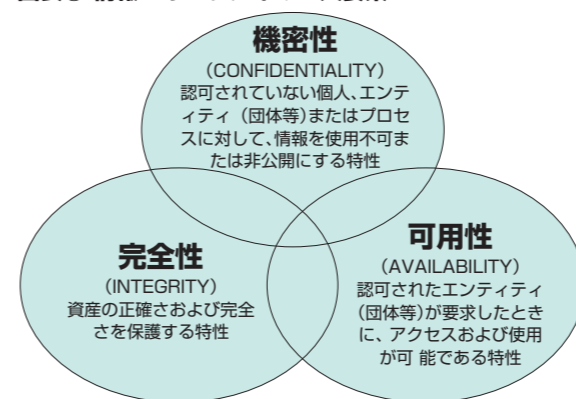
1986年、株式会社リクルートコスモス入社（現、株式会社コスモスインシア）、その後株式会社コスモスモアに転籍、約11年にわたり総務、人事、情報IT、経営企画などのスタッフ部門の責任者として従事。自社オフィス施策でコンクール等入賞。2008年にファシリティ事業部の部長に就任し、年間700件以上のFMに携わる。

今回は、全国四七九社総務部門アンケートの中で、「総務部門の役割として重要になると思ふこと」の第四位「情報セキュリティ」についてお話しいたします。

情報セキュリティは重要でも進まないのはなぜ？

情報セキュリティの定義は、情報システムの「機密性」「完全性」「可用性」を確保することを目的とし、自然災害、機器障害、故意、過失等の人的障害等のリスクを未然に防止し、また、発生したときの影響を最小限に抑え、回復の迅速化をはかることとされています。

図表① 情報セキュリティの3大要素



出所: JIS Q 13335-1:2006

第三者認証の取得で迷いを払しょく

企業の業種や業態、規模、従業員数等により情報資産の量はまちまちです。情報セキュリティへの投資もそれによって異なります。情報セキュリティ先進企業の総務部門の方の課題は複雑化された問題の場合が多いですが、いまだ本格的に取り組んでいない企業の総務担当の方に対しアドバイスをするなら、第三者認証の取得をおすすめします。情報セキュリティを推進するには、ほとんどの場合「従業員にとって今より面倒」なことが多くなり、トレードオフの関係性です。情報セキュリティの重要性を問い、総務部門でルール等を内製化するパワーを考えると、他者（お

ます（図表①）。また、情報資産の主要な一部が「個人情報」です。二〇〇五年四月に個人情報保護法が施行され、どの企業でも例外なく対応を求められています。情報セキュリティを高めるためには、自社の保有する情報のみならず、お客さまから預かった情報や、委託先に預けた情報も含め、全体で考えなくてはなりません。万一漏えいした際の、企業が負う責任や影響はいわずもがなです。総務部門の重要な事項としてみなさんが認識をされていると同時に、総務としてどこまで対応するべきか悩みも多いと聞きます。次にご紹介するのは会社全体で情報セキュリティに取り組む、大きな成果を上げている企業の成功例です。

富士ゼロックス株式会社の場合

情報は作成、伝達、共有、保管、廃棄というライフサイクルそれぞれの段階にリスクが存在しますが（図表②）、富士ゼロックス株式会社では情報セキュリティの「重大事故をゼロにする」という目標を明確に定めました。そのため重大事故につながる軽微な事故の把握と分析にも力点を置き、予防策を多重化して講ずることで、目標を達成しています。

① 情報セキュリティ専門部署を設置／分散していた部署をまとめたことで、従業員からの問い合わせが増え、意識向上を実現。

客さま）からも認知される「第三者認証」を取得することを経営とコミットされた方が、情報セキュリティレベルの推進力が格段にアップすると考えます。個人情報管理と機密情報管理とのプロセスの違いはほとんどなく、プライバシーマーク（以下Pマーク）はITに特化した内容ではないため、IT投資をすぐに決断しなくとも社内体制の強化や従業員教育のベースができるなどのメリットも多く、特におすすめです。今回は本来のファシリティマネジメント（FM）の内容から大きく離れたようですが、FMは手段であるため、次回以降ご紹介したいと考えます。

◆

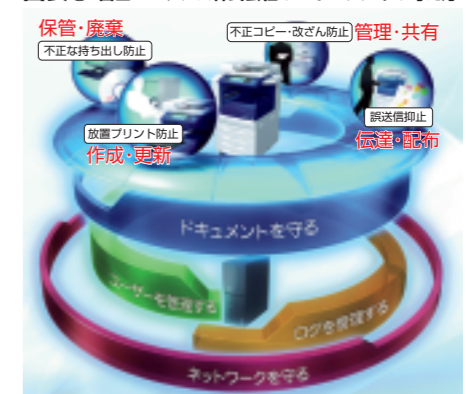
今回は「組織変革」についてFMの観点からお話ししたいと思います。

図表③ 情報セキュリティに関する認証制度の例

制度	プライバシーマーク	ISMS適合性評価制度	ITSMS適合性評価制度
規格	JISQ15001	ISO27001 JISQ27001	ISO20000 JISQ20000
目的	適切な個人情報の取り扱い	情報の機密性を担保した運用の維持	提供するITマネジメントを効率的・効果的に運営管理すること
対象	企業内のすべての個人情報（自社のみならず、社外から預かったものも含む）	適用範囲内のすべての情報資産（ハード、ソフト、個人情報も包含する）	適用範囲内のすべての情報資産（ハード、ソフト、個人情報も包含する）
単位	企業全体	事業所・部門単位などが可	事業所・部門単位などが可
更新	2年ごと	3年ごとおよび、毎年の継続審査	3年ごとおよび、毎年の継続審査
取得企業数	1万2,063社	3,806組織	150組織

出所：一般財団法人日本情報経済社会推進協会（JIPDEC）

図表② 富士ゼロックス株式会社のセキュリティの考え方



出所：富士ゼロックス株式会社

- ② 事故報告の徹底／「事故」を「情報を一瞬でも手放し第三者の目に触れる可能性のある状態」と定義付け、発生したら二時間以内で第一報を入れるルールとした。報告を徹底したことで当初報告件数が増えたが、従業員への意識の浸透に伴い、ここ数年は数が減少。
- ③ 「情報セキュリティ報告書」を発行／言行一致の考えに基づき二〇〇六年より発行。
- ④ 分析に基づくくわつかり紛失の予防／片手で持てるものはなくしやすいため、会社貸与のUSBメモリには本体よりはるかに大きいストラップを付ける。
- ⑤ 年一度のeラーニング、セキュリティ委員会の設置、ポスター設置などの啓発策を複数実施