特集

指導と教育で安心

中小企業のための リスクマネジメント

中堅中小企業にとって、情報漏えいなどの事件は命取りとなる。
実は情報漏えいの約7割は、社員・職員の過失が原因。社員教育を見直し徹底することで、リスクを軽減することができる。
情報社会の企業をおそうリスクを洗い出し、少数精鋭で会社を守るための心構えとノウハウを紹介する。

3

実際にどう運用している？

企業の取り組み

個人のミスによる情報漏えいが多いにもかかわらず、積極的に対策を取っていない企業も少なくない。ここからは、具体的な取り組みを紹介しながら、考え方と効果のある対策を探る。

ルール作りは現場から 自社の状況に合った ルールなら継続できる

高まる企業の関心 対岸の火事ではいられない

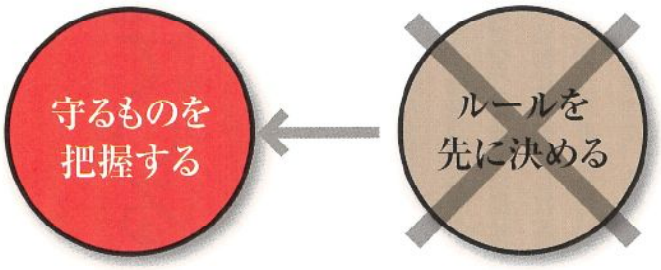
冒頭のアンケートと、あなたの会社の状況を照らし合わせてみると、いかがだろうか。現状では危ないと感じたなら、具体的な他社の取り組みや対策を押さえておきたい。

プライバシーマーク（以下Pマーク）の取得支援や情報システムの監査などを行うジャイス 代表取締役社長 梅林功氏によると、情報セキュリティに対する各社の意識は確実に高まっているという。たとえばパソコンの使用履歴。以前は、情報へのアクセス状況やプリントの有無、誰にメールしたかなどの動作をモニタリングし、何らかの確認が必要になったときに振り返る材料にしていた。それが、いまではもっと予防的に使われている。「何事か起きないためには、どの項目をチェックすれば良いのかを具体的に知りたいという声が寄せられています。本格的に取り組もうという動き、『対岸の火事ではない』という意識が高まっていることが伺えます」。

ジャイスでは、情報漏えい対策を次の4つに分類している。（1）建物の設備や入退室を管理するなどの物理的安全管理装置、（2）ネットワークやソフトウェアの管理などの技術的安全管理装置、（3）不注意や不正行為が起こらないための教育などの人的安全管理措置、（4）社内規定や体制の整備などによる組織的安全管理措置、である。盗難や紛失、メールの誤送信など、考えうる情報漏えいのほとんどに、（3）の人的問題が関連している。

一定の情報セキュリティ対策の程度を示す基準として、PマークやISOがある。他社との差異化を目的に、あるいは業界の流れや取引先か

目に見える対策から考えてはNG！



対策を、というとつい目に見える行動の部分から着手しがち。しかし、守るものを把握しないまま設けたルールは現場に適さないことが多い。

ら求められてなど、取得の理由は複数あるが、これらの取得を好機ととらえて社員教育に取り組む企業も多いという。「その際にまず必要なのは、トップが基本方針を明らかにすることです。もし業務上でPマークの取得が必要になったら、自社の状況と、なぜ必要なのかを社内に周知した上で動き始めることが肝心です」と梅林氏は話す。Pマークを取ること自体が目的になってしまうと、現場の状況に対してハードルが高い要求を押し付けることにもなりかねず、対応にストレスが生じる。結果、社員に情報セキュリティ意識を浸透させるのはずっと難しくなってしまう。

「守るべきもの」を把握することから考える

情報漏えい対策に取り組む企業によくある誤りは、行動から入ってしまうこと。熱心な企業ほど、他社の対策を見学しそれを基準として「ドアにカードキーを付ける」など、形やルールから先に決めてしまう。すると現場の状況が結果的に無視され、逆効果になる。「人間は日に見えるものに左右されてしまうものですが、行うべきことよりも『守るべきものは何か』をしっかり意識する必要があります。その上で、現場にどんなリスクが潜んでいるかを話し合って洗い出し、現場からルールを決める流れを起こせば、継続的に守れるルールができます」。

情報漏えいの問題は保護すべき対象が分かりにくく、価値を実感しにくい側面がある。まずはその価値を顕在化して、それを紛失したらどうなるかを想定し、どのような対策を取れば安心かを一つずつ考えていくことが求められる。「Pマーク取得についても、マニュアルはありますが、基本的に自社に合った形に直していくものなのです」と梅林氏。

情報セキュリティに関する対策は、広報だけでカバーするのは難しい部分もある。たとえばジャイスがPマーク取得を支援する際は、経営企画部など、ある程度経営に携わる社員一人に担当窓口になってもらうという。「サポートする側としても、現場でどのような不具合が出ているかなどを把握している方と話をしないと、守れるルールを作るのは難しい。逆に言えば、現場社員を中心とした話し合いからルールを策定すれば、ある程度は守れるのです。また、この担当者と広報との連携がうまくいけば、社員のレベルアップも見込

「守るべきものは何か」をまず考える

1　守るものを把握する

…どこにどのような情報があるのか、現場の状況を確認

▼

2　1を守るために必要なセキュリティレベルを検討する

…その情報の重要度によって、施錠したロッカーでの保管で十分なのか、それとも施錠した保管室が必要なのかを判断

▼

3　2を満たす行動やルールを策定する

…現場で守れる、継続可能な内容はどの程度なのかを確認

▼

4　3を現場に導入し、実施できているかどうか確認する

…守れないルールは意味がないので、実施が難しければ2に戻って再検討・すり合わせが必要

情報漏えい防止に取り組む際に多くの企業が誤りがちなのが、ドアにセキュリティパスを付けるなどの「行動」からルール化しようとしてしまうことだ。考える矢印を逆にし、「守るべきものは何なのか」から思考をスタートさせるべき。

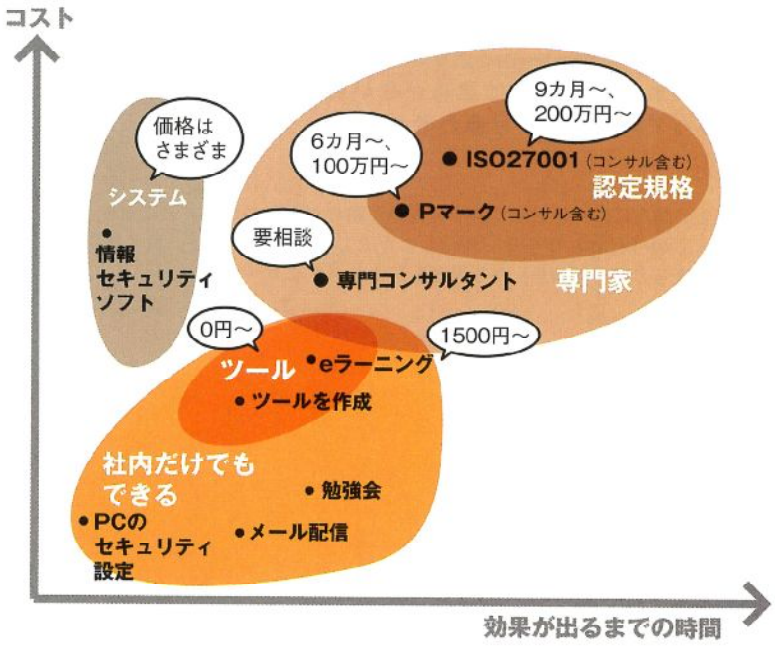
めます。周知徹底がなかなか及ばない場合には、社内ミーティングなど定例の時間を利用し、見直しや事例のチェックをすると良いでしょう」。

基準は内部にしかない 守れるルールを設定する

最終的にどのようなルールにするかは、自社の状況を踏まえた各企業の判断、つまり人の判断による。たとえば「定期的なウイルスチェックを行う」の「定期的」とはどのくらいを指すのか、チェックソフトのレベルはどの程度に設定するのかなど、あくまでも企業の扱う情報のレベルに応じた形で、自社で適正ラインを決めるしかない。どうしても、基準を求めてしまいがちだが、「その基準は企業の内部にしかないのです。Pマークに限っては、被害を受けた外部者がどう感じるかによる部分もあり、そこは社内では決められませんが、それ以外はほとんど決められます。自社の経営の中で最適最良なルールを作ったということであれば、それが一番。うまくいかなければ是正すればいいのです」。

自社が守るべき情報を把握し、どうしたら現場が守れるのかを加味してルール化した上で、状況に応じて下記のような手法を検討したい。セキュリティソフトやeラーニングは、人的チェックが行き届かない規模において補完する手段であるが、「『入れているから安心』とならないように注意が必要」と梅林氏。守るべき情報に合わせて、適切な対策を導入しよう。

自社に適した策を導入しよう



情報漏えい対策として考えられる施策を、コストと効果が出るまでの時間を軸に表した（価格と期間は参考）。「何を守るのか」を明確にした上で手法を検討するのが大前提だが、コストをかけずに取り組めるものは工夫して導入したいところだ。