業務改善のプロフェッショナル

❶ リスクマネジメント

約400社をコンサルティングした専門家のノウハウを公開
情報セキュリティ対策の強化と業務スピードの向上は両立できる

情報セキュリティに対する社会の意識が高まるなか、多くの企業が認証を取得しようとしている※ISMS。しかし、取得企業の情報漏えい・流出が多発している。なぜ事故が起きてしまうのか。大手から中小・ベンチャー企業まで、約400社のコンサルティングを行っているLRM代表の幸松氏に聞いた。

コンサルタントへの依存は禁物

――ISMSを取得する企業が増えていますが、情報流出事故も少なくありません。なぜですか。

認証を取得することが目的化しているからです。どんな企業でも、従業員の不注意や認識の甘さから情報が流出する可能性はある。ISMSは、そのリスクを継続的に評価するためのフレームワークにすぎません。しかし、多くの経営者は情報流出を防ぐ〝お墨つき〟のように思いがちです。

本来、ISMSは運用が大切。それによって情報流出を防いだり、被害を軽減できるからです。でも、多くの企業は取得当時の仕組みを維持するだけになっています。

――なぜ、効果的な運用ができないのでしょう。

認証取得までのプロセスを、コンサルタントにまかせっきりにしてしまうからです。彼らは企業のISMS取得を支援しますが、現場に深く入らない。運用マニュアルも定型的で、業務の実態にあっているとは限りません。

――具体的に教えてください。

たとえば、私物の情報端末を社内に持ち込むルール。「携帯電話はOKだがノートパソコンはダメ」。こんな規定を認証取得時に作成したとします。4半期に1回、セキュリティ担当者が現場責任者に「ルールを守っているか」と聞く。「はい」。これで、経営者にはいつも「セキュリティレベルは維持されている」という報告があがる。

ところが、持ち込んでいる〝携帯電話〟が問題。規定作成時にはガラケーだったのが、いまはスマートフォンです。情報端末としての機能はパソコン並み。セキュリティリスクが高くなっているのに、だれも気づかない。外部コンサルタントが作成した運用マニュアルでは、現場の変化を察知できないのです。

実効性のある対策は現場から生まれる

――では、どうすればいいのですか。

現場主導の対策を行うことです。現場のメンバーにセキュリティ上の不安要素をリストアップさせ、それぞれについて効果的な対策を議論してもらう。外部コンサルタントはそのサポート役に徹するのです。

たとえば、「業務で作成・改訂したデータについて、つねにバックアップをとる」というルールをつくるとしましょう。現場メンバーに対策を考えさせると、実効性の高いアイデアが出てきます。バックアップをそのつど手動で取得すると仕事の邪魔になるので、自動バックアップの仕組みを導入する、といった案です。

外部コンサルタント主導だと、「データ変更の際には、各自がバックアップをとるように注意する」といった、形式的なものになりがちです。

――しかし、認証を取得・更新するにはどの企業も同じルールを定めなければいけませんよね。

いいえ。それは誤ったイメージです。外部コンサルタントが主導するから形式的なことが多くなる。現場業務にあった自社独自の対策をつくってかまわないのです。

当社のコンサルティングでは、業務全般の改善の一環として、情報セキュリティ強化を進めることが多い。そうすれば業務効率を向上させながら情報流出リスクを低減できます。一社でも多く、実効性のあるセキュリティ対策づくりを支援したいですね。

LRM
代表取締役
幸松 哲也
ゆきまつ てつや

1976年 兵庫県生まれ。2001年に徳島大学を卒業後、TIS株式会社に入社。大規模システム開発プロジェクトに携わり、企画・提案から開発、運用・保守まで一貫して担当。その後、外資系IT企業、システム会社を経て、2006年にLRM株式会社を設立。代表取締役に就任。ISMS認証審査機関の主任審査員も務めている。

認証を取得するだけでは不十分
おもな情報流出・漏えい事例

事例1 システム会社
従業員数／約40名　年商／約20億円　ISMSとPマーク取得

- 概要：大手メーカーから、技術の特許にかんする情報システムの運用を受託。**「機密情報がある最重要データにはアクセスしない」という契約条件**だったが、社員がそのデータにアクセスした。その事実がメーカー側のログで判明する。
- 原因：**契約条件の詳細が現場の担当者に伝わっていなかった。**そのため、担当者は「セキュリティを強化するために必要だから」と最重要データにアクセスしてしまった。
- 結果：3年契約で10億円の大型プロジェクトだったが、**取引停止**に。本件の売上を前提に経営計画を立てていた**システム会社は倒産危機に陥り、協力会社の社員約40名が全員解雇**される。担当社員は責任をとって退職した。

事例2 広告代理店
従業員数／約70名　年商／約50億円　ISMS取得

- 概要：本社オフィスで開催したパーティーの様子を社員が撮影し、Facebookにアップ。**その画像にクライアントの新製品の模型が映っている**ことを、Facebookを閲覧したクライアントの社員が発見。
- 原因：**模型を片付けずにパーティーを開き、撮影してしまった。**また、Facebookの画像にタグ付けした社員の友人が「全体公開」の設定にしていたため、誰でも画像を閲覧できる状態になっていた。
- 結果：画像に映った模型が、どんな製品かわからない初期段階のものだったことが幸いし、実害はなし。そのため**取引停止にはならなかったが、厳重注意を受ける。**

エキスパートが教える

ISMS取得後の運用法
3つのポイント

1 文書からISO用語をなくす

コンサルタントの主導で作成されたISMSの文書は、独特の表現が多い。たとえば「完全性が損なわれた場合」という言葉をISMSでは使う場合が多いが、この言葉ではどんな場合かわからない。**「間違ってしまった場合」と表現を変えるだけで、現場の社員にわかりやすくなる。**

2 業務全般の改善と同時に行う

ISMS運用のPDCAサイクルを回すときに、セキュリティ対策以外の業務改善を同時に行う。ある会社では、文書管理体制の改善策として、ICタグの認識装置を内蔵する書庫を導入。ICタグ付のファイルを決められた順に並べなければ、アラートが鳴る仕組みに。その結果、**文書整理による業務効率向上と、セキュリティ強化が同時に実現**した。

3 ISOのためだけの活動をなくす

ISMSを維持するために必要な作業は、案外少ない。やらなくてもよい作業をしている場合は多い。「この作業はISMSがなくてもやる意味はあるのか？」と見直し、意味がないと思った作業は積極的に廃止する。**「ISOのためでなく自社のための仕組み」にしていく。**

10秒Check

情報セキュリティ対策で経営者が陥りがちな
6つのカン違い

- □ ISMSを取得したので自社のセキュリティは万全だ
- □ 情報漏えいリスクの評価は事務局にまかせているから安心
- □ 取得当初の基準どおりに何度も更新しているからセキュリティ体制は維持されている
- □ コンサルタントが作成した文書にのっとって運用しているので、リスク管理は万全
- □ 多額のシステム投資をしたのでセキュリティレベルが向上した
- □ セキュリティを強化すると業務に支障が出る

3つ以上あてはまる会社は情報セキュリティマネジメントを早急に見直すべき

※ISMS：企業などの組織が情報を適切に管理し、機密を守るための包括的な枠組み。ISMSの構築の仕方と認定基準は国際規格（ISO27001）になっている。