自社に即したISMSの構築を目指し、半年でISO 27001の認証を取得

先端材料で世界のトップを目指し、グローバルに事業を展開している総合化学企業集団“東レグループ”。その活動を支える情報システムの企画・開発・運用を担う、株式会社東レシステムセンター。同社では会社の業務上必須といえるISMS（情報セキュリティマネジメントシステム）を構築し、2009年11月には国際規格であるISO/IEC 27001の認証を取得した。どのような考え方で進めてきたのか、社長の鹿倉尚夫氏にお聞きした。

2009年5月12日、ISO 27001の認証取得に向けたキックオフ宣言の日。東レシステムセンターの鹿倉社長は関係者に二つの“指示”を出した。

一つは、向こう半年で認証取得を果たすこと。もう一つは、自社に即したISMS（情報セキュリティマネジメントシステム）とすること。会社として守るべき業務プロセスを優先度に従って絞り込んで、身の丈に見合ったISMSを構築し、できる限り短期間で国際規格であるISO 27001の認証取得にこぎ着けたい、との趣旨だ。

“指示”の背景には、日常業務での考え方やISOに対する過去の経験がある。

システムインテグレーション・カンパニーの東レシステムセンターにとって、業務を遂行するうえで欠かせないのがプロジェクト管理の考え方だ。いくつものプロジェクトを管理していくなかでは、やるべきことを明確にしたうえで、優先度に従って一つひとつをできる限り短期間で完成させることを追求する。こうした考え方を、鹿倉社長はISMSの構築という自社のプロジェクトにも展開しようとした。

キックオフ宣言の日から半年―2009年11月13日。東レシステムセンターでは予定通り、千葉県浦安市に本社オフィスの拠点を置くネットワーク事業の一部と企画管理部の二つの部門で、ISO 27001の認証を取得した。守るべき業務プロセスと情報資産を絞り込んだ結果、必要な対策のモデルとして列挙されている133の管理策のうち122項目を適用範囲とした。

ISMSを構築しISO 27001の認証を取得した狙いは、どこにあるのか。鹿倉社長は語る。

「ISMSの構築は情報サービスに携わる企業として必要不可欠です。その上で、ISO 27001の認証を取得することを決めたのは、当社の情報セキュリティのレベルが、世間と比較してどの程度なのか確認しよう、という狙いからです。何か問題が起きてからではなく、先行することにより、お客さまはじめ、すべてのステークホルダーからより信頼を得たいとも思っていました。それに、ISO 9001の経験からもISMSの継続的な運用・改善には第三者機関の審査が必要であると考えていました」。

■ 徹底した現場の意識改革

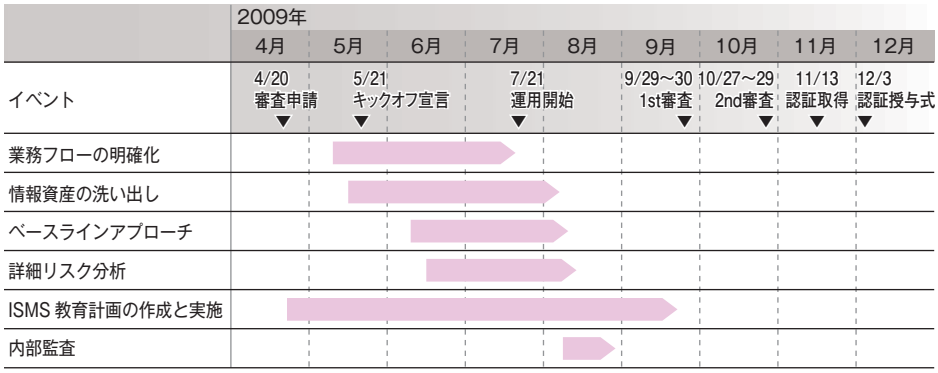
東レシステムセンターでISMSの構築に向けた第一歩を踏み出したのは、2006年7月。本社オフィスにSMO（Security Management Office）を置いたのが始まりだ。ISMSの構築に欠かせない事務局機能は、このSMOが担っている。

そして、キックオフ宣言を受けて、対象部門では、課長がISMSの管理責任者に、課員2名が推進担当者に選出された。これらの運営委員が先頭に立って、情報セキュリティに関する意識の向上を図っていくことになった。現場の意識

改革に向けた思いを鹿倉社長はこう語る。

「管理職止まりだった情報セキュリティに関する高い意識を、社員はもちろん、業務委託先や派遣社員にまで徹底していきました。いわゆるPDCAのマネジメントサイクルの中で、『C(Check)』や『A(Act)』の過程はついおろそかになりがちなだけに、そこまで徹底するよう努めました」。

■ISMS構築と認証までのスケジュール



■ 対象部門を選定し運用で社内浸透

ISMS構築の必要性は業務全般にわたっているが、そこからさらにISO 27001の認証取得まで発展させるとなると、別の視点から検討する必要が生じる。東レシステムセンターで認証取得の対象を上記二つの部門に絞ったのは、まさにそうした検討の結果だ。

では、構築したISMSの運用に会社全体としてはどのようにかかわっていくのか。鹿倉社長はこう説明する。「認証取得の対象外となる部門では、認証取得部門と歩調を合わせてISMSを自発的に運用していきます。先行していた品質マネジメントシステムの運用に関しても、取り組み方は同じです。それらが適切に運用されているか否かは、社内横断の組織として設置したITガバナンスに関する委員会でフォローしています」。

■ 提案力の向上やレベルの評価に役立つことを期待

上の表は、ISMS構築・運用の実績を示したものだ。事務局と推進担当者は週1回の割合で、情報セキュリティ運営委員会は月1回の割合で定期的に会議を開くなど、ISMSの構築・運用に向けた進捗管理を着実に実施してきた。さらに、ISMSの構築・運用に求められる教育・訓練を、対象となる役員・社員は1週間にわたって毎日の業務を終えてから受講してきた。「こうした努力が実って、通常は1年かかるといわれている認証取得をわずか半年で実現できたのです」と、鹿倉社長は満足そうだ。

東レシステムセンターにとって、ISO 27001の認証取得は、現場の実務に、どのように生かしていけるのか。

「情報セキュリティサービスを事業の一つとして手がけています。認証取得を通じてISMSが本来どうあるべきかを学んできただけに、顧客に対して本質をとらえた深みのある提案ができるのでは、と期待しています。また、認証を取得していることで、社外からは当社のSEのレベルが、わかりやすくなることも期待しています」(鹿倉社長)。

■ 経営にどう生かすかという視点で運用

このISMSとは別に、東レグループ全体で国内40社、海外60社、計100社の関係会社を対象とする「東レグループ電子情報セキュリティ対策指針」を定めている。この指針の内容に照らして、ISO 27001はどのように評価できるのか。「当社のISMSはISO 27001の認証取得を契機に第三者審査が定期的に入ることによって強化されています。ISO 27001の要求事項と指針の内容はほぼ一致しており、指針を遵守し、定着させるうえでISO 27001の認証取得を通じたISMSの強化はきわめて有効です」(鹿倉社長)。

同社では2010年度、滋賀と大阪の事業所でネットワーク事業を担当する部門を対象として、ISO 27001の認証取得に向けて動き出す予定だ。ISMS構築の推進事務局を新設して、本社オフィスで認証を取得した2部門と同じ半年での取得を目指す。

立場は異なるものの、二つの認証取得に携わった感想を鹿倉社長はこう総括する。「ISO 9001の認証を取得して以来、いい仕組みだと評価しています。マネジメントシステムが基盤になって、提供するシステムやサービスの品質は確かに高まった。ISO 27001も、マネジメントの仕組みは基本的に同じです。これらの仕組みを経営にどう生かすか、という視点で運用し、監視・レビューおよび維持・改善していきたいと考えています」。

鹿倉尚夫(しかくら ひさお)氏 プロフィール

1972年東レ株式会社入社。主に生産分野のシステム化に携わる。85年機能分社により東レシステムセンター発足とともに出向。98年同社取締役。2006年同社代表取締役社長。

■ 株式会社東レシステムセンターの概要

本社所在地	千葉県浦安市美浜1-8-1
設立年月日	1985年(昭和60年)9月24日
資本金	2億円
従業員数	270名
業務内容	情報システムの企画・開発・運用
ISO 9001初回登録	2001年9月
ISO 27001初回登録	2009年11月