

（株）ケー・シー・エス ISO 事業部
技術顧問 田嶋忠志

話題のPマーク認証 取得のための4ステップ

個人情報漏洩の怖さ

これまでは「国際規格」であるISOの内容・認証取得・失敗例・成功例などを説明しましたが、今号では話題の「情報管理システム」に焦点を当てて説明します。

最近「企業情報が漏洩した」「個人情報情報が漏れた」というようなニュースを耳にしない日はないくらいです。コンピュータを中心とするIT技術の発展に伴い、多量の情報を保管・管理し、かつ容易にコピーし、送受信できる時代になりましたが、逆に他人に漏れ出す機会も飛躍的に増大。これが基で大きなトラブルに進展するケースが多く見られます。

まず、表を見て下さい。これは03年におこった代表的なトラブルとその解決費用です。

当然ながら、これは一例ですから

水面下ではもっと多くのトラブルが存在すると想定されます。この表を見るといかに「個人情報管理」が大切で、企業の生命線につながるかが分かっていただけだと思います。

05年4月1日には個人情報保護を目的とした「個人情報保護法」が完全施行されることになっており、個人情報扱った企業にとっては法律違反という責任リスクが高まること予想されています。

この種のトラブルは、単に損害賠償のみならず、企業イメージの低下、信用失墜による株価下落、顧客離れから、ひいては経営不振に進展する可能性もあります。最悪の場合、企業倒産にまで進展することもあり得ますので非常に重要です。

漏洩防止の管理システム

二つした情報漏洩トラブルの防止

めのために浮上したマネジメントシステムが二つあります。ISO化はされていませんが、ISOと同様の思想で構築されたシステムです。

一つ目は企業全体の業務に関する「情報セキュリティ・マネジメント・システム（ISMS/インフォアームーション・セキュリティ・マネジメント・システム）」で、二つ目が個人情報管理を主目的にした「Pマーク（プライバシー・マーク）」です。

ISMSは企業全体に関わり、やや大がかりで認証取得にはかなりの労力と時間を要します。

一方のPマークは個人情報管理に特化しており、比較的容易に取得できることから、大企業から中小企業まで認証取得に殺到。現在は認証取得審査の順番待ちという状況です。今回は一般的なPマークに焦点を絞り説明したいと思います。

認証取得の主な対象企業としては電子商取引を行なう企業、通信販売企業、宅配・運輸業、教育機関など。さらには人材派遣業、マーケティングリサーチ業、学習塾、印刷業、銀行・金融業、医療機関など広範囲に及んでいます。

認証取得の大まかな手順は次の4つのステップです。

業務を通して得られる個人情報社外から預かる（社外に預ける）個人情報、従業員や会員の情報などを企業として特定する。

どの様に外部漏洩を防止するかを検討する。

検討結果を基に規格に則って社内マニュアル、規程、手順書を作成し、システムを構築する。

システムを実際に運用し、その内部監査を実施。さらに、外部からの審査を受け、認証を得る。

このように一連のISO管理システムの構築手順とまったく同じです。ISO、ISMS、Pマークの最終目標は同じで「企業リスクを減らし、改善改革を実践するための管理システム」といえます。トラブルの予防システムです。ISO9001や14001を取得されている企業は、システムへの理解がやさしく、構築にもさほど時間がかかりません。

03 - 04年の情報漏洩事例とその解決費用

ケース	漏洩事例とその解決	内容	解決費用
A	カード会員情報571人分が漏洩した事が発覚した(2004年09月)	個人情報管理システム作成の委託先元社員が顧客情報(氏名・住所・電話・生年月日・カード番号・有効期限など)を売却し、1350万円が悪用された。	被害額肩代わり
B	カード会員情報48万人分漏洩(2004年08月)	社内から顧客情報が流出した。犯人は特定されていない。	金券×48万人分
C	通販会社の顧客情報10万件漏洩(2004年03月)	元社員2名が6年前の顧客情報を流出させた。	通販番組1カ月自粛
D	情報通信企業保有の顧客情報140万件漏洩(2004年03月)	顧客情報漏洩経路は特定できていない。	誠意を持って対応
E	電子通信販売企業保有の個人情報466万件漏洩(2004年02月)	加入者の個人情報が発見。経路は特定できていない。	500円金券 ×466万人分
F	雑誌購読者顧客情報(2003年10月)	架空名義の債権回収業者から請求書や督促状が送付され、誤って送金した事件。経路は特定されていない。	1000円金券 ×18万人分
G	全115万のコンビニカード会員情報のうち56万人分漏洩(2003年06月)	加入者顧客名簿情報漏洩。経路は特定されていない。	500円金券 ×115万人分

「Pマーク」認証の取得法

ISOと同じようにPDCA(プラン・計画 実行 チェック アクション)経営者の評価と指示)のサイクルで改善していくシステムで、まず自社の実態に合うように、Pマーク規格に沿ってシステムを構築していきます。

このため、マニュアル 規程 手順書を作成し、内部監査 経営者のマネジメントレビュー、外部からの審査を受けて認証を取得。さらに2

年ごとのサーベイランス(監視制度)とその流れは、先行しているISOと同じです。

ただ、ISOよりも対象とする範囲が狭いため、比較的短期間で費用も安く、要する手間も少なく認証取得が可能です。

認証取得までの構築期間は、コンサルティングの支援を得て、システム構築・試運転・実績に約六カ月、審査を受けるための順番待ちが四六カ月(審査自体は一二日間)と、合計約一年を要します。現状では、

順番待ち解消のために審査機関増が検討されており、近く順番待ち期間が短縮される見通しです。

費用はコンサルティング、審査登録料、維持費用等が必要ですが、大まかにはISO認証取得の六〇七〇%ほどと考えておけばよいと思います。

現時点で日本国内では約一〇〇〇社が取得済みです。審査機関は「JIPDEC(日本情報処理開発協会)」が担当しており、ISOの審査機関とはまったく別の機関です。

最近のISO改訂・新設の話題

最後に最近のISO規格改訂と新ISOの話題を紹介します。

ISO14001(環境管理マネジメントシステム)

現行の96年版から改訂版04年版への移行が、国際投票を経て04年11月15日に発効しました。日本国内では日本語翻訳版を12月中に作成し、改訂JIS Q14001:2004となる予定です。

今の見通しでは、運用期間六カ月を確保せねばならないことから、発効から六カ月後の05年5月中旬までは現行96年版のみで、新規審査・サーベイランスを行ない、05年5月中旬06年5月中旬までの一年間で04年版対応に移行する必要があります。

06年5月中旬以降は、04年版に統一

一し、現行96年版は廃版となります。すべての既取得企業は、この一年間に移行審査(サーベイランス審査時)を受審し04年版対応に切り替えます。

問題は移行規格の内容とその程度ですが、それほど大きな改訂ではない、従来に比べ解釈や運用の面で明確でなかったところが、より厳密に規定されているという感じですが。

ISO22001(食品関係のISO)制定の動き

今まで、食品製造や加工などでは国内法はありましたが、管理システムについては、特殊なHACCP以外にはありませんでした。これを一般的なISOにして広く適用させる動きがあります。見通しでは05年中はISO化の具体案が決まると見られています。

ISO13485

(医療機器製造・輸入等へのISO国際基準)について

これはすでに発効して、多くの企業が認証取得に取り組んでいます。05年には国内法の薬事法改定によりISOと共通化する部分もあり、認証取得の動きが活発化すると予測されています。

もしご質問があれば下記に連絡下さい。わかる範囲で回答申し上げます。

㈱ケー・シー・エス ISO事業部
E-mail: isojigy@kcsweb.co.jp
URL http://www.kcsweb.co.jp

「ISO / 経営改革への道」は今回で終了させていただきます。ご愛読いただきまことにありがとうございました。