個人情報保護法と ISMS 認証基準

情報技術試験場

2005 年 4 月から施行される個人情報保護法について知っておきたいポイントと中小企業における情報セキュリティ面からどのように対策すればよいかについて、ISMS（情報セキュリティ管理システム）との関係から解説させていただきます。

■個人情報保護法のポイント

・企業が漏洩事故を起こした場合等の責任が大きく変り、従来のプライバシー権侵害による責任のほかに個人情報保護法違反の責任が追加され責任が重くなった。

・違反すると最高で刑罰（6 月以下、30 万円以下）が科せられる実効性のある法律だが、個人が訴えない限り実効性はない。

・両罰規定（違反行為をした者だけでなく、その法人自体も処罰対象とする制度）の対象。

・対象は「個人情報データベース等」（５千件を越える個人情報がコンピュータであれ紙であれ整理され、容易に検索できる状態にあるものをいう）を事業活動に利用している事業者（「個人情報取扱事業者」という）。

■ 中小企業において施行前にすべきこと

1) どんな個人データがあるかすべて把握する。

2)「個人情報」、「個人データ」、「保有個人データ」を区別する。（ガイドライン[1)] を参照）

3) 「個人情報取扱事業者」に該当するかどうかを判断する。

該当する場合は、早急に対策が必要です。担当機関にご相談ください。

■ ISMS とは

情報セキュリティマネジメントシステム(Information Security Management System: ISMS) は、情報セキュリティ管理システム仕様の国際規格です。図１に示すように元は英国の規格(BS7799)ですが、国際規格(ISO/IEC17799)や国内規格(JIS X 5080)の情報セキュリティ管理実施基準と用語互換性があります。

ISMS 適合性認定制度があり、認定が受けられます。詳細は、JIPDEC[2)]に問い合わせ下さい。

■情報セキュリティ対策

企業にとって個人情報保護法の施行は、自社の情報セキュリティについて見直すよい機会ですし、

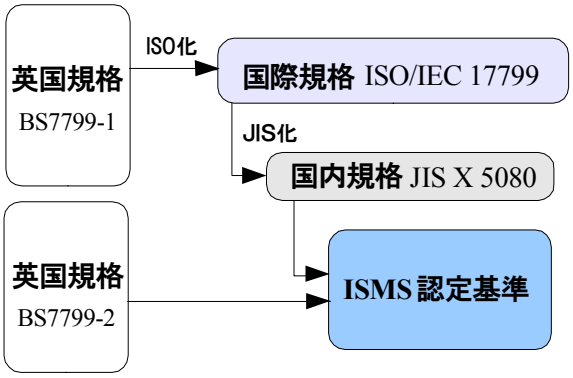

図１　セキュリティ規格の関係

「個人情報取扱事業者」でなくても何らかの対策が必要です。

ISMS は、その対策の足掛かりとして認定を受けないにしても取組んで見ては如何でしょうか。その考え方（PDCA サイクルのスパイラルアップ）や構築手順は大変参考になります。

詳細については、文献２）の認定基準の補足・ガイド等をご覧下さい。

■　まとめ

個人情報保護法対策として ISMS の利用をお勧めしましたが、なにより関心をもって事業を見直す機会にして頂ければよいと思います。

今回は、事業者を対象に解説しましたが、それぞれ該当する担当省庁からガイドラインがでていますので、それらを参照してください。

■　参考文献

1)　個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成１６年１０月２２日厚生労働省経済産業省告示第４号）

2)日本情報処理開発協会:http://www.isms.jipdec.jp/

情報技術試験場　ソフト開発部　青木久夫
TEL 0263-25-0778　FAX 0263-26-5350
E-mail　aoki@nagano-it.go.jp