BS7799-2をベースにISO27001
ISMS要求事項の国際規格化で認証制度の使い勝手が向上
情報セキュリティマネジメント標準化の最新動向

企業の情報資産は、ウイルスだけでなく、外部からの不正アクセスやデータ流失などのさまざまな脅威にさらされている。あらゆる業種の企業において、情報セキュリティマネジメントの重要性が高まる中、情報セキュリティマネジメントシステム（ISMS）の要求事項を規定した規格であるBS7799-2がISO／IEC27001として国際規格化されることになった。その経緯や狙いについて、ISO／IECの情報セキュリティ分野を管轄するJTC1／SC27／WG1の、国内対応委員会の中尾康二主査（KDDI株式会社・技術開発本部情報セキュリティ技術部長）に話をお聞きした。

ISO／IEC JTC1／SC27／WG1 国内対応委員会
中尾康二主査
（KDDI株式会社・技術開発本部情報セキュリティ技術部長）

今年11月にもISO27001が発行へ

――今年は、ISO／IEC17799（情報セキュリティマネジメントのための実践規範）の改訂版が6月に発行されたのに続き、BS7799-2（情報セキュリティマネジメントシステムの要求事項）がISO／IEC27001として国際規格化される見通しと伺っております。本題に入る前に、まず情報セキュリティマネジメントに関する国際規格化の背景についてお聞かせください。

中尾●ITの急速な進展に伴い、企業の情報資産がウイルスや不正アクセス、DoS攻撃などの被害に遭う危険性は、今まで以上に高まっています。いったんこうした被害に遭うと、カスタマーからの信用は大きく失墜し、企業イメージの低下、さらには企業収益の悪化も免れません。こうした背景から、情報セキュリティマネジメントの重要性は日に日に高まっている状況です。ISO／IEC JTC1／SC27／WG1（以下、WG1）では、情報セキュリティマネジメントの普及・発展をめざし、国際規格化を推進しています。

情報セキュリティマネジメントの国際規格化は、英国規格BS7799を基に進められてきました。この規格は「BS7799-1」と「BS7799-2」の二部構成になっており、このうちBS7799-1は2000年にISO／

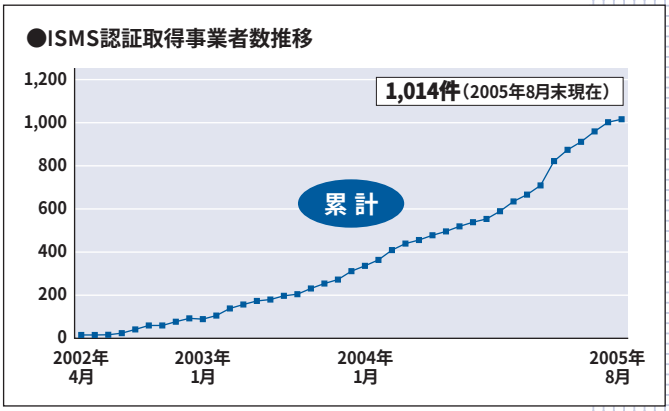
IEC17799として国際標準化されています。一方、情報セキュリティマネジメントシステム（ISMS）の要求規格であるBS7799-2については、これまで各国のISMS認証のベースとして活用されるにとどまっていましたが、ここに来てようやく国際規格化されることになったのです。

――BS7799-2がISO／IEC27001として国際規格化されるまでの経緯について、ご説明いただけますか。

中尾●世界各国のＩＳＭＳ認証動向を見ると、BS7799-2を自国の規格として導入している国がある一方、この規格をベースに独自の規格を策定している日本のようなケースもあります。ご承知のように、日本では2002年より（財）日本情報処理開発協会（JIPDEC）が運営する「ISMS適合性評価制度」に基づいて、ISMS認証のための基準が制定されました。このように、内容はBS7799-2とほとんど変わらないにもかかわらず、表面的に異なる規格が世界に複数存在していたわけです。

ISO／IEC JTC1／SC27では、こうした混沌とした状況を鑑み、ISMS要求事項に関わる国際規格化の妥当性について検証を重ね、2004年より国際規格化に向けた作業がスタートしました。ただ、規格化作業がスムーズに進んだかというとそうではありません。米・仏など一部の国から、「GMITSやNISTなどのドキュメントからよいと思われる部分を寄せ集め、新たな規格を制定してはどうか」などの意見が出されたためです。

当然のことながら、日本をはじめBS7799-2をベースにISMS認証を行っている国としては、そのような意見は受け入れられるものではありません。「BS7799-2をベースにした国際規格にするべき」というスタンスで各国に働きかけを行った結果、われわれの主張が認められ、ようやく具体的な作業に着手することができたのです。こうして、2005年4月にウィーンで行われたISO／IEC JTC1／SC27会合において、ISMS要求事項規格案のFCD（Final Committee Draft）が承認され、FDIS（最終国際規格案）への移行も確認されました。FDIS投票による承認が得られ次第、早ければ今年11月にもISO／IEC27001として新たな国際規格が発行される見通しです。



財団法人 日本情報処理開発協会（JIPDEC）発表資料より

セキュリティレベルをグローバルにアピールできる

――こうしてお話を伺っていると、今回の国際規格化において日本が果たした役割は大きかったように感じますが、いかがでしょうか。

中尾●そうですね。日本のISMS認証の取得件数は世界でも突出しており、海外から一目置かれる存在であることは確かです。具体的には、世界全体のISMS認証件数が1,600件弱であるのに対し、日本は1,000件を超え世界の半数以上を占めている状況です。このため、認証制度の構築・運営ノウハウを持った“ ISMS先進国 ”として高く評価されており、われわれの主張も少なからず受け入れられたのではないかと思います。

――新たにISO／IEC27001が発行されることによって、ISMSの認証制度はどのように変わっていくのでしょうか。

中尾●ISO／IEC27001の規格化作業は、BS7799-2との整合性や移行の容易さなどを念頭に進められたため、若干の修正点はあっても、それほどドラスティックな変更はないということを、ご理解いただきたいと思います。

今回の国際規格化による大きなポイントは、ISOと

して国際的に認知されたISMS要求事項に則って、クロスボーダーで認証を展開できるようになること。すなわち、ISMSの認証を取得した企業は、自社の情報セキュリティレベルについて、グローバルにアピールすることができるようになります。これは、おそらく多くの企業が待ち望んでいたことなのではないでしょうか。

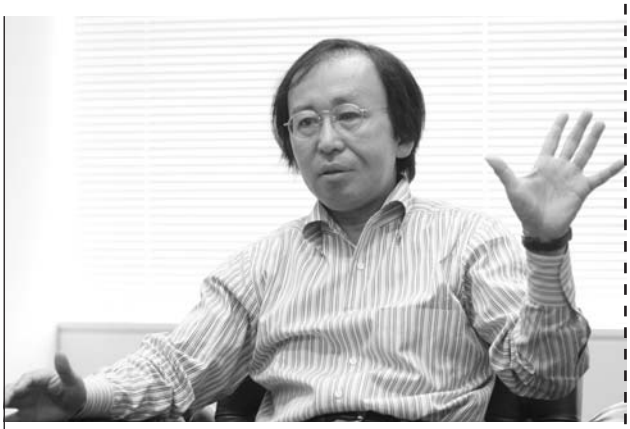
ISO／IEC27001の発行によって、今後はJIS X 5080（ISO／IEC17799）のような、国際規格に対応したJISを発行する必要が出てきます。現在、27001の番号をそのまま用いて、「JIS Q 27001」として発行できるように準備作業を進めており、これが実現すればISMS認証の裾野はさらに広がっていくでしょう。

現状のISO17799は2年後にISO27002へ移行

――情報セキュリティマネジメントのための実践規範であるISO／IEC17799の位置付けは、今後どうなりますか。

中尾●ISO／IEC17799については、2007年のISO／IEC JTC1／SC27会合において、ISO／IEC27002への完全移行を承認・確認する予定です。なぜ2年後なのかというと、ISO／ITC17799という規格番号が、現状のISMS認証において一般的に使用されており、突然変更してしまうと混乱を招く恐れがあるためです。従って、今年6月に発行されたISO／IEC17799の改訂版にも、17799から27002に移行する可能性のあることが注記されています。

このほかWG1では、情報セキュリティマネジメントに関わる国際規格として、「情報セキュリティマネジメントのためのリスクマネジメント」、「情報セキュリティマネジメントの計量、測定」、「情報セキュリティマネジメントシステムのための実施の手引」に関する検討・審議を進めているところです。これらは別々の規格番号とはせずに、ISO9000シリーズやISO14000シリーズと同様に27000シリーズとして体系的な規格群とすることが決定しています。



――最後に、これから情報セキュリティを確立したいと考えている企業に対して、ぜひアドバイスをいただけますか。

中尾●まず守るべき情報資産を特定し、情報セキュリティの3大要素であるC.I.A.(※)と照らし合わせて、どんなリスクがあるのかをきちんと評価することが大切です。そうすれば、どんな対策を講じればよいか、おのずと見えてくるでしょう。そして、セキュリティポリシーに基づいて具体的な計画・目標を策定して実行し、点検、見直しを行うというPDCAサイクルを繰り返し回すことによって、情報セキュリティのレベルは強化されるはずです。

以前は「直接的にビジネスとは関わり合いがない」という理由から、情報セキュリティに着目する企業はそれほど多くありませんでしたが、ここ数年間で企業情報の漏洩などによる“負の効果”について、かなりの経営者が意識するようになってきています。このことは、ISMSの認証取得件数が増加傾向にあることからも明らかです。今後、ISMSの重要性に対する認識がさらに高まることによって、社内にセキュリティ風土を確立される企業が増えるものと期待しております。

――本日は貴重なお話をいただき、ありがとうございました。

※ Confidentiality、Integrity、Availabilityの略。それぞれ、認可された者だけが情報にアクセスできるようにする「機密性」、情報および処理方法が正確かつ完全であることを保証する「完全性」、認可された者が必要な時に確実に情報にアクセスできるようにする「可用性」を指す。