

特 集

個人情報の取扱いにフォーカスした ISMS-PIMS 認証がいよいよ始動

一般社団法人情報マネジメントシステム認定センター（ISMS-AC）

事務局長 星 昌宏氏 認定審査員 郡司 哲也氏

ISMS（情報セキュリティマネジメントシステム:ISO/IEC 27001）規格を拡張し、個人情報の取扱いにフォーカスしたISMS-PIMS 認証（ISO/IEC 27701に基づく適合性評価）に向けての取り組みが、2020年12月、始動した。国内企業においても個人情報の取扱いへの関心は高く、その動向が注目されている。一般社団法人情報マネジメントシステム認定センター（以下、ISMS-AC）事務局長の星氏と、認証基準の策定に携わった郡司氏に、ISMS-PIMS 認証の概要、取得のメリット、認証取得にかかわる今後のスケジュールなどについて伺った。



星 昌宏氏(左) 郡司 哲也氏(右)

高まる情報セキュリティへの関心 国内6,000以上の組織がISMSを取得

— 2020年12月に、いよいよ個人情報の取扱いに特化したISMS-PIMS 認証（ISO/IEC 27701に基づくプライバシー情報マネジメントシステムの適合性評価）の認証機関の認定が始まりました。ISMS-PIMS 認証は、ISMS（情報セキュリティマネジメントシステム:ISO/IEC 27001）の取得を前提とした認証であるということです。まずはISMS 認証取得の現状についてお聞かせください。

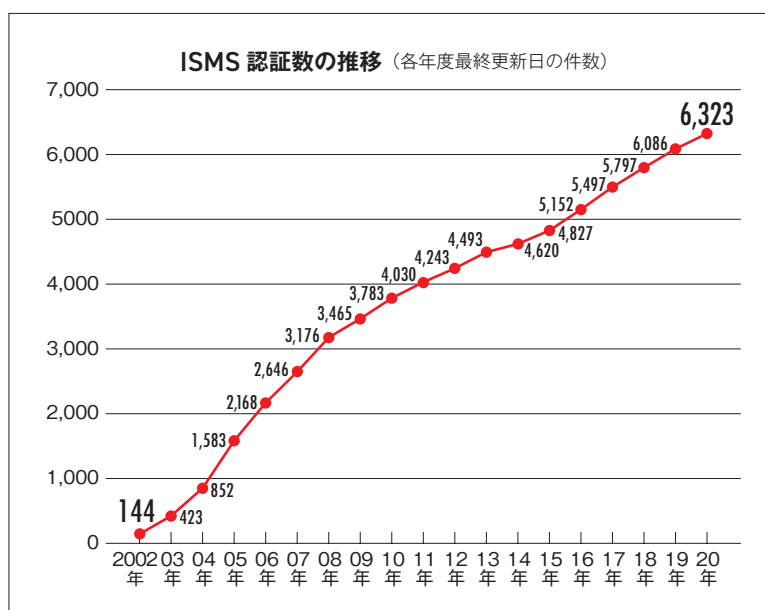
星 ISMSの認証は2002年にスタートしました。国内の認証取得組織は2019年11月に6,000を超え、2021年1月13日現在で6,323となっています。ISMS認証は必ずしも全社での取得とは限らず、1つの企業内の異なる部署等で複数取得されている場合もありますので、企業数ではこれより少なくなります。

— ISMS 認証を取得しているのは、どのような業種の企業が多いのでしょうか？

星 ISMS 認証の取得について、特に事業分野は指定していません。情報セキュリティはITシステムを活用していれば必ず必要になり、ITはいまや特定分野に限らずほぼすべての分野で使われているからです。

郡司 Amazon Web Services（AWS）、Google、中国のファーウェイなど世界的にメジャーな企業も、率先してISMS認証を取得しています。

星 国内の状況については、ISMS-ACが認証取得組織を対象にアンケート調査を行っており、これによってある程度業種を把握しています。最新のアンケートは2018年3月に実施したもので、有効回答数は1,180。これによりまずと「情報技術」が半数以上を占めており、さらにその内訳を見ると、システムインテグレーションやソフトウェア開発などが挙がっています。



個人的な印象ですが、出版・印刷業は全体で見ると2.4%と小さな割合でありながら、近年増加傾向にあるように思います。同じく増加しているのが廃棄物処理業です。古紙やOA機器などを取り扱いますので、ISMSへの関心が高いのでしょう。

ISMS取得を前提に個人情報の取扱いに特化した管理策を追加

— ISO/IEC 27701とはどのような規格なのでしょう？

郡司 ISMSの管理対象が組織の資産全般であるのに対し、ISO/IEC 27701はISMSを拡張し、PII（Personally Identifiable Information:個人識別可能情報）の取扱いにフォーカスしたマネジメントシステムです。PIIを個人情報と読み替えて、個人情報保護のためのマネジメントシステムと捉えていただいてもよいと思います。

もともとISMSの中にも個人情報（PII）保護に関する項目が存在しているのですが、それは一般的でざっくりしたものです。そのため個人情報（PII）の取扱いに特化した管理策が必要だろうということで、まずガイドラインとしてISO/IEC 29151（個人を特定できる情報保護のための実施標準）が作られました。ISO/IEC 29151は、ISMSクラウドセキュリティ認証の基準となるISO/IEC 27017と同様、ISMSのセクター別ガイドライン規格です。さらにその後、ガイドラインだけではなく要求事項も含む規格が必要ではないかということで検討が進められ、2019年8月に、要求事項とガイドラインを1つにまとめたISO/IEC 27701が発行される運びとなりました。ISO/IECの規格のタイトルが「プライバシー情報マネジメントのためのISO/IEC 27001及びISO/IEC 27002への拡張—要求事項及び指針」であることからわかる通り、あくまでもISMSがベースにあり、その上に個人情報を取り扱う上で留意

すべき具体的な要求事項や管理策が追加されたという建て付けです。

ちなみに“ISMS-PIMS（アイエスエムエス ピムス）”は、ISMS-ACが定めた呼称です。ISMS認証ファミリーの1つであり、個人情報に配慮した保護対策ができていますISMSであるという意味で、ISO/IEC 27701に対する適合性評価制度のことを「ISMS-PIMS認証」と呼んでいます。

——個人情報保護の方策として、日本では1998年からプライバシーマーク制度の運用が行われています。プライバシーマーク制度（以下、Pマーク）とISMS-PIMS認証の違いはどこにあるのでしょうか。

郡司 同様の質問をよくいただきます。決定的な違いは、ISMS-PIMS認証に用いられる認証基準（ISO/IEC 27701）は国際規格であり、Pマークの場合は国内規格（JIS Q 15001）だということです。

JIS Q 15001の本文には、個人情報に関する法規制、すなわち、日本の個人情報保護法に従いなさいということが明示されています。JIS Q 15001は、日本の法規制と密接にリンクしています。ですからPマークを取得していれば、個人情報保護法をはじめとする日本の法令に順守しているということを、顧客や取引先に対してアピールすることができます。

一方、国際規格であるISO/IEC 27701は、特定の法とリンクしているわけではありません。ですから認証を取得する組織は、ISO/IEC 27701に加えて、事業を行う国や地域のガイドラインや法令を確認し、それに則って業務を遂行することになります。例えば日本では個人情報保護法のほか、PPC（個人情報保護委員会）が発行しているガイドライン、米国であればNIST（National Institute of Standards and Technology）のサイバーセキュリティのガイドライン、欧州であればGDPR（General Data Protection Regulation:一般データ保護規則）などですね。

また、Pマークは法人単位で付与される認証なのに対して、ISMS-PIMS認証は必ずしも全社での認証ではないという点も、違いのひとつです。事業所、あるいは部署ごとに認証の取得が可能です。



——ISOが個人情報の取扱いに特化した規格が必要だと判断した背景には、どのような事情があったのでしょうか。

郡司 SNSの利用拡大などによって個人情報を含む大量の情報が流通するようになったという背景があります。例えば米国大統領選では以前からSNSが活用されていますが、それに伴う社会問題も起きました。このような状況下で欧州では、消費者の人権保護を組織に対して強く求めるGDPRが、

2018年5月に発効されました。これをきっかけに、世界的にプライバシー保護の動きが加速したと考えられます。ISO/IEC 27701はこのGDPRをかなり意識して作られています。

個人情報の取扱いに関して具体的管理策に踏み込んだ審査を実施

郡司 ISO/IEC 27701の特徴には、個人情報(PII)を取り扱う役割としてPII管理者とPII処理者という2つを定義しているという点もあります。日本の個人情報保護法では、個人情報を取り扱う会社を個人情報取扱事業者としてひと括りに定義しているのに対し、ISO/IEC 27701ではPII管理者とPII処理者という役割を別々に定義して、それぞれに個別の手引きを提供しています。世界的には、この2つを分けて定義するのがスタンダードになっています。

個人情報の取り扱いにおいて最も重要なポイントは、利用目的と利用方法、それらに対する個人からの同意です。どのようなパーソナルな情報を収集し、どのように使って、どのようなアウトプットをするのか。それを決める組織がPII管理者です。PII管理者は、個人情報を提供した人々に対する責任をとる立場にあります。

PII処理者はそれらを自分たちでは決めずに、PII管理者の指示や依頼に基づいて実行する組織です。PII管理者から氏名や住所のデータを渡されて、ダイレクトメールを送付する事業者などは、PII処理者ということになります。PII処理者であることを積極的にアピールして、業務委託につなげたいという事業所もあるでしょう。しかし、PII管理者はPIIの処理をしないということではなく、PII処理者も兼ねている(役割として包含している)ケースが多いのではないかと思います。

星 ダイレクトメールの発送代行を請け負うという立場ではPII処理者だけれども、自社の社員の個人情報を取り扱っているという面ではPII管理者だというケースもあるでしょうね。

——企業にとってISMS-PIMS認証を取得するメリットは何でしょうか？

郡司 認証基準となるISO/IEC 27701は国際規格ですので、特に海外で事業を展開している組織、海外企業と取引がある組織にとっては、信頼性の高さをアピールするために有効だと思います。

すでにISMSを取得している組織であれば、これに追加するかたちで個人情報の取扱いに対する管理体制を整えればよいので、一から構築するよりはるかに短期間・低コストでISMS-PIMS認証を取得することが可能です。逆に言いますと、ISMS (ISO/IEC 27001)を取得していないセクションを含めてISMS-PIMS (ISO/IEC 27701)認証を取得したいという場合には、まずISMSの適用範囲をそれらのセクションにも広げる必要があります。まだISMS認証を取得していないという場合には、ISMS認証とISMS-PIMS認証の同時取得を目指すことも可能です。

星 ISMS認証では、主に法順守の仕組みができているかという観点からの審査を行います。ISMS-PIMS認証ではさらに具体的な管理策に踏み込んで審査しますから、個人情報の取扱いに関す

るリスクマネジメントを明確な基準に則って実施しているということを、対外的に証明することができるようになりました。

ISO/IEC 27701には個人情報の取扱いに関する具体的な対応策が示されていますから、すでにISMS認証を取得している、あるいは個人情報を取り扱っている組織は、必ずしも認証を目的としなくても、マネジメントシステムをブラッシュアップするために、一度この規格の内容を確認しておかれるとよいと思います。

事業の海外展開を図る企業を中心に国内300組織の取得を見込む

— ISMS-PIMS 認証はどういった組織で取得が進むと想定していच्छいますか。

星 ISMS-PIMS 認証の認証基準であるISO/IEC 27701がグローバルスタンダードであることを考えると、やはり最も関心が高いのは、事業を海外展開している企業ではないかと思ひます。

先ほど紹介したISMS 認証取得組織を対象としたアンケート調査では、ビジネスの海外展開についても聞いています。それによると、ISMS 認証取得組織のうち海外展開しているところは20.4%と、約5分の1です。さらにこの20.4%の組織に対して、ISMSについて過去に海外の取引先からどのような評価を受けたかについて尋ねた設問では、「ISMS 認証の取得を確認されてプラス評価を得た」が20.7%、「特にプラス評価はされなかったがISMS 認証の取得を確認された」が13.7%、「確認されたことはない」が65.6%となっています。プラス評価をされたところ、つまりISMS 認証取得全組織のうち4~5%の組織は、ISMS-PIMS 認証に最も高い関心を示すと考えられます。ISMS 認証取得組織は現在6,000以上に上りますので、それに当てはめれば、約300の組織が直接的な候補になると考えています。

郡司 ISMS-PIMS 認証がいよいよ始まるらしいという情報が出始めた当初から、すでに何件かお問い合わせをいただひています。電気通信事業者やネット通販など、もともとISMS 認証への関心が高かつ

たところは、先陣を切ってISMS-PIMS 認証取得への取り組みを始めていると思ひます。

将来的には、例えば海外の通販モールの出店の条件として、ISMS-PIMS 認証の取得が義務付けられるといったケースが出現する可能性もあると思ひます。国内でも、例えばPII 処理者としての業務を受託するような場合においては、ISMS 認証にプラスしてISMS-PIMS 認証の取得を検討する組織が出てくるかもしれません。



ISOの認定基準発行を前に世界各国で認証がスタート

— ISMS-PIMS 認証に関するスケジュールは？

星 ISMS-AC では12月15日にISMS-PIMS認証を行う認証機関の認定について申請受付を開始し、その旨のニュースリリースを出しました。同時にISMS認証の認定を受けている認証機関には、認定基準と認定を受けるための手順等を記した文書をお送りしております。

実はISO/IEC 27701の適合性評価を実施する認証機関に対する認定基準については、ISOではまだ審議中なのです。当初の予定では、認定基準は2020年12月1日に発行される予定と聞いていましたが、修正コメント対応等により、発行が後ろ倒しになりました。世界では、英国の認定機関であるUKAS（ユーカス United Kingdom Accreditation Service:英国認証機関認定審議会）などが先行して独自の基準で認定を始めています。ISMS-ACでもISOの規格策定状況を注視しつつ、先行する各国の認定基準も参考にしながら、独自基準によって、認証機関の認定を開始いたしました。

— ISMS-PIMS 認証の周知を図るためのキャンペーン展開等は計画されていますか。

星 ISMS-ACは認定を専門に行う機関であり、自らキャンペーン展開やユーザーズガイドの作成・発行、セミナーの開催等の普及啓発活動は行っていません。ISMS認証に関しては、JIPDEC（一般財団法人日本情報経済社会推進協会）がそれらの普及啓発活動を行ってきていますので、ISMS-PIMS認証に関しても同様の扱いとなる見込みであり、ISMS-ACもこれに協力してまいります。

— 今後に期待しております。われわれベターリビングもISMS-PIMS認証機関の認定を受けるべく準備を進めているところであり、この認証を通じて企業の皆様のより安全かつ有意義な個人情報の取り扱いを支援していく所存です。本日はありがとうございました。