10th anniversary

ISMS 適合性評価制度
Information Security Management System

座談会

10年目のISMS
～その軌跡と広がる世界～

一般財団法人 日本情報経済社会推進協会

ISMS
適合性評価制度の10年の歩み

INDEX

ISMS制度創設から10年間の歩みを回想してみると、その中でも2000年にわが国の中央省庁のホームページが連続して改ざんされるという情報セキュリティ事件が記憶に残っているが、これを契機として情報セキュリティ対策への抜本的な取り組みが強化されるようになった。このような状況の中で、情報セキュリティポリシーを軸とした情報セキュリティ対策の重要性が認識され始め、特に情報セキュリティマネジメントの国際規格であるISO/IEC 17799の制定が注目を集めた。JIPDECとしてもISMSとの係わりを持った年でもあった。これをベースとしたISMS適合性評価制度を創設し、わが国全体の情報セキュリティ強化のため、また安対制度廃止後の受け皿として、早急にISMSを導入することとなった。JIPDECでは、2001年に約1年間のパイロット運用を実施した後、2002年4月から本格運用を開始した。

その当時は、情報セキュリティに対する意識が低かったため、人的な不注意で情報を漏洩したり、ウイルス付きメールを開けてネットワークを麻痺させたり、不正アクセスによる情報の改ざんなどの被害が相次いで起きてきていた。このような情報セキュリティ事故を防止するためにも、単にセキュリティ技術の導入だけでは難しく、組織全体のリスクマネジメントの仕組みが重要となっていた。また、人的なミスにより情報セキュリティ事故を無くすためには、個人それぞれの情報セキュリティ意識を向上させるとともに、繰り返して教育・訓練活動を実施するなど、企業文化としてのセキュリティを醸成させることが重要である。このような背景からISMSが着実に実績を伸ばし、2013年1月現在、4,209の組織が認証を取得している。

さらなるエポックとしては、2005年10月にISMSの国際規格としてISO/IEC 27001が発行され、それに伴いISMS認証基準（Ver.2.0）を国内規格JIS Q 27001に移行することとなった。また、このISO/IEC 27001の制定に伴い、認定機関の認定システムに対する国際的な標準（ISO/IEC 17011）に適合させるため、認定スキームの変更を行った。具体的には、JIPDECで実施していた審査員評価登録業務及び審査員研修機関の認定については、（一財）日本規格協会のマネジメントシステム審査員評価登録センター（JRCA）に移管された。

次に、ISMSに関する国際連携は海外の認定機関との相互連携を図ることであり、JIPDECは2006年4月にPAC（太平洋認定協力機構）、2007年10月にはIAF（国際認定フォーラム）にそれぞれ加盟し、ISMS認証の信頼を確保させるとともに、ISMSの相互承認協定（MLA）の実現に向けて国際貢献を果たすこととしている。

これまでにISMS制度の定着に必要な普及活動として、業種別ガイドラインの策定、ISMSに関する国内外の最新動向、及びISMSの重要性を周知させ、意識を高めるための説明会を全国主要都市において実施した。2007年3月の説明会において、延べ参加者が10,000人を超え、ISMSの普及に大いに貢献することとなった。

最後に、今後のISMS制度の展開であるが、ISMSの27000シリーズにおいてセクター分野ごとの国際的なガイドラインが発行されるに伴い、ISMSの認証拡大を進めるとともに、他のマネジメントシステムとの統合化を図り、エンドユーザーのためのマネジメントシステムを確立させ、ISMS認証の信頼性を向上させる制度として進化させていく所存である。

ISMS適合性評価制度に関する年表

制度普及 第一期

制度普及 第二期

2000	1	中央省庁ホームページ連続改ざん事件
	7	「情報セキュリティ管理の国際的なスタンダードの導入及び安対制度の改革」※を公表
	12	ISO/IEC 17799 が制定
2001	3	安対制度の廃止
	7	ISMS 適合性評価制度パイロット事業の実施
2002	2	ISMS 適合性評価制度の確立
	4	JIPDEC、ISMS　適合性評価制度正式運用開始
2003	4	OECD の情報セキュリティガイドラインの見直し
2004～		ファイル交換ソフト Winny による情報流出事件
2005	4	個人情報保護法施行
	6	ISO/IEC 17799 改訂版の発行（2007.7にISO/IEC 27002へ規格番号の変更）
	10	ISO/IEC 27001（ISMS 認証基準）の発行
2006	4	PAC（PACIFIC　ACCREDITATION　COOPERATION）加盟
	5	ISMS 認証基準（Ver.2.0）から JIS Q 27001への移行開始
2007	3	審査員評価登録業務及び審査員研修機関の認定業務の移管
	10	IAF（INTERNATIONAL　ACCREDITATION　FORUM）加盟
2008	5	医療機関向け ISMS ユーザーズガイドの発行（初版は、2004.11発行）
	6	ISMS の相互承認（MLA）の検討開始
2009	3	クレジット産業向け PCIDSS/ISMS ユーザーズガイドの発行（初版は、2006.3発行）
2009～2010		ISMS 審査員評価登録センターの認定
2011	8	ISMS 認証取得組織が 4,000 を超える
2011～		標的型サイバー攻撃深刻化
2012	5	制御システムのセキュリティマネジメントシステム（CSMS）の制度の検討開始
	10	ASEAN 情報セキュリティ政策会議

※正式名称「情報セキュリティ管理に関する国際的なスタンダードの導入及び情報処理サービス業情報システム安全対策実施事業所認定制度の改革について」

2012年にISMS（Information Security Management System：情報セキュリティマネジメント システム）適合性評価制度は10周年を迎えました。
10周年を記念し、2012年末にISMS制度の創設や現在の運用を支える関係者の皆様にお集まりい ただき、これまでを振り返るとともに、現在の課題や今後の展開について座談会形式でお話を伺いました。
企業にとってなぜISMS認証を取得する必要があるのか。標的型サイバー攻撃対策としても有効な のか。会話は真摯に、ときに熱を帯びて行われました。

創設の経緯:
ネットワーク時代の情報セキュリティを確立するために

情報セキュリティの安全対策としてISMS適合性評価制度(以下、ISMS制度)以前の制度はどのようなものでしたか?

土居　通商産業省が昭和56年(1981年)からスタートさせた「情報処理サービス業情報システム安全対策実施事業所認定制度」(以下、安対制度)がありました。安対制度は主に施設や設備の物理的な対策に重点が置かれていて、データセンターを所有する情報処理サービス業を対象としていました。
インターネット接続完全商業化やWindows95の登場など1990年代にコンピュータのネットワーク化が大きく進む中、安対制度は抜本的に見直す時期にきていました。誰もがネットワークにアクセスし情報を活用できる時代では、安対制度のように情報処理サービス業のみを対象にしていてはセキュリティを保つことはできません。

三角　通商産業省内でも、安対制度に代わる新しい制度では情報処理サービス業だけでなく、対象をもっと広げないといけないという議論をしていました。

2000年当時、日本政府は電子政府実現のための整備を進めるなどネットワーク社会到来への期待が高まる一方で、セキュリティ対策の不備による事件も続発しました

土居　2000年1月末、省庁や政府機関のホームページの改ざん事件が相次いだのは衝撃的でした。この事件後、官民あげて情報セキュリティ意識が高まりましたが、ネットワーク時代の情報セキュリティを確立するためには、技術的なセキュリティ対策と組織全体のマネジメントの両面から取り組むことが必要です。
もうひとつ重要な観点は国際標準化の潮流です。安対制度は我が国のローカルな制度でしたが、新しい制度となるISMS制度では、品質マネジメントISO 9001(1987年発行)やISO 14001(1996年発行)のようにグローバルスタンダードも重要なテーマでした。

ISMS制度をつくるうえで海外の制度を参照しましたか?また苦労したのはどのような点ですか?

駒瀬　BSI(英国規格協会)が平成7年(1995年)に規定した英国規格BS7799を参照しました。情報セキュリティ対策を行う際のCode of Practice（実践規範）を記したPart1と、組織のISMS構築、運用に関する第三者認証のための要求事項を記したPart2の両方ですね。Part1は2000年にISO/IEC 17799(現在、ISO/IEC 27002)、Part2は2005年にISO/IEC 27001になりました。2006年には2つともJIS化されました。

土居　ISMS制度の第三者認証に関わるBS7799 Part2がISO化される5年も前でしたが、ISO化されるだろうと見込んでいましたから、通商産業省も先取りしていこうと。同省とISMS制度を運用するJIPDEC、認定機関としてのJIPDEC情報マネジメント推進センター、学識経験者や業界団体の有識者によって構成される運営委員会と技術専門部会が一体となって進めました。皆さんとても進取の精神に富んでいましたね。

駒瀬　BS7799 Part2に基づきながらも日本独自にアレンジした部分もあります。例えば人事採用に関して採用前に身元調査をしなければならないという記述は、日本風土における身元調査が困難なことも踏まえて人員の資質や職能を明確にするという表現に変更しました。頭を悩ませたのは単語解釈の要素が多かったですね。英語の直訳ではなく、日本語ではこう書いた方がわかりやすいだろうと。しかし認証基準づくりよりも苦労したのは、安対制度とISMS制度の違いや、なぜ必要なのかを説明することです。

土居　品質や環境は対象とするものがよくわかりますが、情報セキュリティは対象が見えているようで見えていない。

駒瀬　安対制度のときは自社の物理的な設備を守ればよかったのですが、ISMS制度ではネットワーク上を行き交う情報も守らなければならず、守備範囲もパートナー先にまで及ぶこともあります。その点をなかなか理解していただくのが難しくて…。

三角　ISMSはマネジメントシステムですが、そもそも当時はマネジメントシステム自体が理解されていませんでした。ISO 9001もそうですが、仕組みができているから品質管理ができているのではなく、品質管理をするために仕組みを導入し目標を設定し達成していく。そのための認証制度なのですが、モノの規格との違いを理解していただくという面でISMS制度も同様に苦労されたと思います。

土居　通商産業省は平成13年(2001年)3月31日をもって安対制度の廃止を決定していましたから、受け皿となるISMS制度をスタートするために、時間がない中で評価者を育てなければならないなど課題は山積していましたが、どうにか2001年度のパイロット運用にこぎつけることができました。

10年の歩み:
ISMS認証取得が調達条件に盛り込まれるなど社会的に認知

ISMS制度は平成14年(2002年4月)から本格運用を開始しました。その後、順調に普及は進みましたか?

土居　金融、流通、製造業などいろいろな業種から突破口となる企業や地方自治体がISMS認証を取得することで少しずつ裾野が広がっています。安対制度は20年間で認証取得した企業が200社だったのに対し、ISMS制度は10年間で取得している組織が4,000以上です。ISO 14001の取得数が20,000、ISO 9001取得数が40,000ですから、情報セキュリティの重要性の観点からも普及拡大は今後の課題となります。

駒瀬　ISMS認証取得数はなだらかに上昇を続けていますが、急激に伸びたのは2004年から2005年にかけてです。この時期はファイル交換ソフトWinnyを通じて官庁や企業の内部情報が流出するケースが相次ぎました。Winnyによる情報流出事件を契機に、入札条件にISMS認証取得を盛り込むケースが増えてきました。

三角　建設業界においてISO 9001の認証取得数が急増したのと同じですね。入札条件になることでISMS制度の社会的な認知度も高まります。

駒瀬　振り返ってみると、2005年はISO/IEC 27001の国際規格化や個人情報保護法の全面施行など情報セキュリティにおけるエポックメイキングな年となりました。

土居　情報セキュリティへの関心が高まり、ISMS制度が社会的に認知されるのに伴い、ISMS認証取得を対外的に公表することが信頼性の向上につながるようになってきました。また企業や組織がISMSを導入して改善活動を継続することで、企業はもとより国全体、そして世界全体が安心安全の方向に向かっていきます。こうしたISMS制度の考え方に対する理解はこの10年で着実に広がっています。

ISMSを太い幹にしながら
クラウドセキュリティなどをプラスアルファして
時代のニーズに応えていければと思います

上村 昌博（うえむら まさひろ）氏
経済産業省　商務情報政策局
情報セキュリティ政策室 室長
JIPDEC IMS運営委員会 オブザーバ

コンピュータセキュリティ早期警戒体制の整備事業、企業・個人の情報セキュリティ対策促進事業を通して情報セキュリティ政策を推進する情報セキュリティ政策室の室長。2012年4月からJIPDEC IMS運営委員会 オブザーバとして参加。政府の視点でISMS制度の支援や、本制度とクラウドセキュリティなどとの関わりについての意見を集約する役目を担っている。

新たな脅威への対応:
ISMSは標的型サイバー攻撃など新たな脅威にも有効

ISMSが10周年となる2012年と、その前年の2011年は国際関係が緊張し標的型サイバー攻撃といった新たな脅威が日本国内を襲いました。新たな脅威に対する備えとしてISMS制度の果たす役割はどのようなものでしょうか?

駒瀬　標的型攻撃は人間の弱点やミスを誘因するなど手口が巧妙で、技術だけで社内システムへの侵入を止めようとしても難しい。標的型攻撃に対しては1つの対策ではなく総合的な観点が求められます。企業活動のさまざまなシーンで点検機能が働き、組織的に管理できるISMSは標的型攻撃への対策としても有効です。

三角　しかし管理面だけでも標的型攻撃には対応しきれないのが現状です。いまの攻撃手法は、仕事上で知り合いになっておいてメールを送り、業務上、開かないといけないところに追い込んできます。人的対策では対応しきれず、ファイルを開いた後の技術的対策をとることが必要です。標的型攻撃に対しては管理と技術のバランスが重要なポイントになります。またISMS認証を取得しているからといって標的型攻撃の対策がとれているわけではないということも大事な視点です。

駒瀬　ISMS制度は採用する管理策が決まっているわけではありません。企業が標的型攻撃のリスクを認識し、管理と技術の両面から対策を充実させる目標を立てたら、何が効果的な管理策であるかを特定し、それがきちんと実行され効果を上げているかどうかを審査する制度です。ISMSの要求事項と133の管理策を適切に運用していれば、標的型攻撃への対策を実行に移す場合も、既に管理面における基盤があることから、最初から仕組みを作る必要はありません。PDCA（Plan-Do-Check-Act）サイクルを上手くまわしながら、リスクを認識・評価し、役割と責任を明確にしながら対策を強化していくことで、新たな脅威にも対応できます。

この10年間、急速に進む技術革新にISMS制度ではどのように対応してきましたか?

駒瀬　モバイルの普及などによって情報セキュリティを取り巻く脅威も大きく変わります。ISMS制度の中のどのような要件を守っていれば新しい脅威に対処できるのかといった解説を行うことは技術専門部会の重要な役割となっています。また、データセンターのアウトソーシングサービスやクラウドサービスの利用などさまざまな運用手段に適したISMS制度の要件を紹介することも多くなりましたね。

上村　顧客からの信頼獲得や社内セキュリティの抜本的改革、社員のセキュリティ意識の向上などISMS認証の取得目的は企業によって様々です。どんなに優れた制度も利用されなければ価値をもたらしません。ISMS制度誕生から10年間、企業の声に耳を傾けて制度としてより良いものにしてきたわけですが、今後もその点は重視していきたいと思います。

ISMS導入を成功するポイントにはどのようなことがありますか?

三角　ISMS制度では何をどこまでやるかを企業が自ら決めなければなりません。企業によって経営戦略やシステム環境、リスクは異なるためです。ISMS制度の管理策に記述されている通りに行うのではなく、なぜこの管理策が必要なのかといった背景を理解したうえで自社の組織に合ったものに噛み砕いて対策をたてることが大切です。

上村　ISMS制度は企業それぞれがどれだけ大事な情報をもっているのか、それはどのような脅威にさらされていて、万一情報流出などの事故があった場合の被害はどれくらいか。また被害を最小化するためにどのような対策をとるか。企業自らが考える最初の一歩になるという点も重要です。

土居　事業継続管理や内部統制などの経営上の課題とITの結び付きが強まっている現在、ISMSに対する企業トップの理解と決断も欠かせません。

上村　2012年5月、土居先生を代表に民間企業が集まり情報セキュリティガバナンス協議会がスタートしました。経営層を対象とする情報セキュリティガバナンスとは「社会的責任にも配慮したコーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」と定義されています。情報セキュリティガバナンスはISO/IEC 27014として国際規格化の方向にあります。

広がるISMS:
ISMSという幹にプラスアルファしてセキュリティを強化

ISMS認証の取得により他の認証を効率的に取得できるといったことはありますか?

土居　個人情報保護法が施行されたときも、技術専門部会が中心になってISMSの管理策の中で個人情報保護法に必要なものは何かを列記したガイドをつくりました。

駒瀬　カード業界におけるグローバルセキュリティ基準「PCI DSS」のときもそうですね。

上村　ISMS認証を取得している企業の立場で考えると、何か新しい認証制度ができてきたときにISMSと重複する項目があった場合、その項目に関してすでに適合していることを認めてほしいという思いはあるでしょう。
現在、制御システムにおけるセキュリティマネジメントシステムCSMS(Cyber Security Management System)の制度化を図っていますが、ISMSと重複する項目が100項目くらいあります。重複しない項目だけを行うことでCSMSの認証を取得するようにできないだろうかという議論を進めています。

駒瀬　効率的な認証取得とは視点が異なりますが、ISO/IEC 27000シリーズの中で10番以降は、通信事業(ISO/IEC 27011)、医療(ISO 27799)など業種に即した規格がつくられ、いまも金融(ISO/IEC TR 27015)など次々と準備されています。

上村　現在、準備している規格の中で高い関心を集めているのがクラウドセキュリティの規格です。この規格も新たに制度をつくるのではなくISMSにプラスアルファするかたちで行うことを検討しています。いろいろな業種業態でISMSを太い幹としながら時代のニーズに応えてセキュリティの強化を図っていくという方向に進んでいければと思っています。

ISMSの今後:
日本企業が海外で信頼を築くための大きな拠り所に

情報セキュリティの要としてISMS制度がより役割を果たしていくうえでの課題はありますか?

土居　まず、審査のレベルを均一にすることですね。誰が評価

ISMSの仕組みのもと管理と技術の両面で対策を立て
PDCAサイクルをまわすことは
標的型サイバー攻撃にも有効です

駒瀬 彰彦（こませ あきひこ）氏
株式会社アズジェント
営業統括本部 コンサルティング担当部長
兼 セキュリティセンター フェロー
シニアコンサルタント
JIPDEC ISMS 技術専門部会 主査

平成13年(2001年)に実施されたISMSパイロット事業にて運営委員会の下部委員会である、ISMSパイロット事業技術委員会 委員。ISMS適合性評価制度(ISMS制度)では制度創設から現在までISMS技術専門部会 主査(平成15年度より)を務める。株式会社アズジェント社内のISMSの管理責任者として、またISMS導入のコンサルタントとして活躍している。

しても同じというわけにはいかないでしょうが、それに近いようなかたちにもっていかないと。

三角　ISMS認証制度は信頼が命なので評価者のレベルは重要ですね。信頼が揺らぐと制度そのものの有効性が疑われることになります。

土居　日本企業全体のセキュリティを向上するという観点では中小企業のためのISMSを考えることも大切です。匠の技を持った町工場には世界中から仕事の依頼がくるわけですが、「機密情報を小規模な企業に扱わせて大丈夫なのか」という海外企業の疑問に応えるために「ISMS認証を取得したい」という中小企業のニーズは大きいです。しかし133の管理策をとるためのコストも人員も不足しています。

上村　その点は欧米でもホットな話題になっています。サプライチェーンにおけるセキュリティを考えたとき、中小企業のセキュリティマネジメントは重要な課題です。欧米でもまだ明確な答えはでていないようですが、本当に大事な論点だと思います。

三角　中小企業のセキュリティ向上を目的に、レベルを下げるのではなく汎用性を高め、中小企業に特化したバージョンをつくることが大切ではないでしょうか。ドキュメントをはじめとする事務の簡素化なども考える必要があります。ASEAN諸国にISMS制度を普及する際にも中小企業向けといった視点は重要ですね。

上村　2012年10月、東京で開催した日・ASEAN情報セキュリティ政策会議ではASEAN諸国から「ISMS制度に取り組みたいので協力してほしい」という話がありました。

三角　日本品質のISMSを世界に広げていきたいですね。日本企業の営業担当が海外の企業に名刺を差し出すとき、ISMSのマークが名刺についていると、セキュリティの仕組みを持っていることが認識され、信頼の最初のステップになります。

ISMS制度の相互承認は進んでいますか?

土居　ISMS制度の相互承認については、IAF(International Accreditation Forum, Inc. :国際認定フォーラム)、PAC(Pacific Accreditation Cooperation:太平洋認定協力機構)ともに、従来のISO 9001、ISO 14001に加えて、ISMS(ISO/IEC 27001)を新たに含めるための作業を進めています。2013年前半にもISMS MLA(相互承認)の申請受付が開始される可能性もあります。

海外に進出する日本企業は急増していますから、相互承認はとてもメリットが大きいですね。

土居　日本のISMSを世界で通用させてほしいという日本企業のニーズは以前から大きなものがありました。グローバルに展開している日本企業は、日本でISMS認証を取得することで相互承認に加盟している他国にも通用します。相互承認は、ISMSが日本だけでなく世界で信頼を築くための大きな拠り所となります。

上村　世界各国のISMS認証取得登録発行数をみると、日本は4,000以上と圧倒的です。日本企業のセキュリティに対する関心の高さ、理解の深さが窺えます。二番目の英国、三番目のインドが500台、中国は急増していますが400近くです。さきほどASEAN諸国のお話をしましたが、ISMSのグローバルでの普及のためにISMS制度に関する豊富な実績やノウハウを活かし世界各国のセキュリティ向上に貢献することが日本に求められています。

メッセージ:
「a Culture of Security(セキュリティ文化)」の具現化を目指して

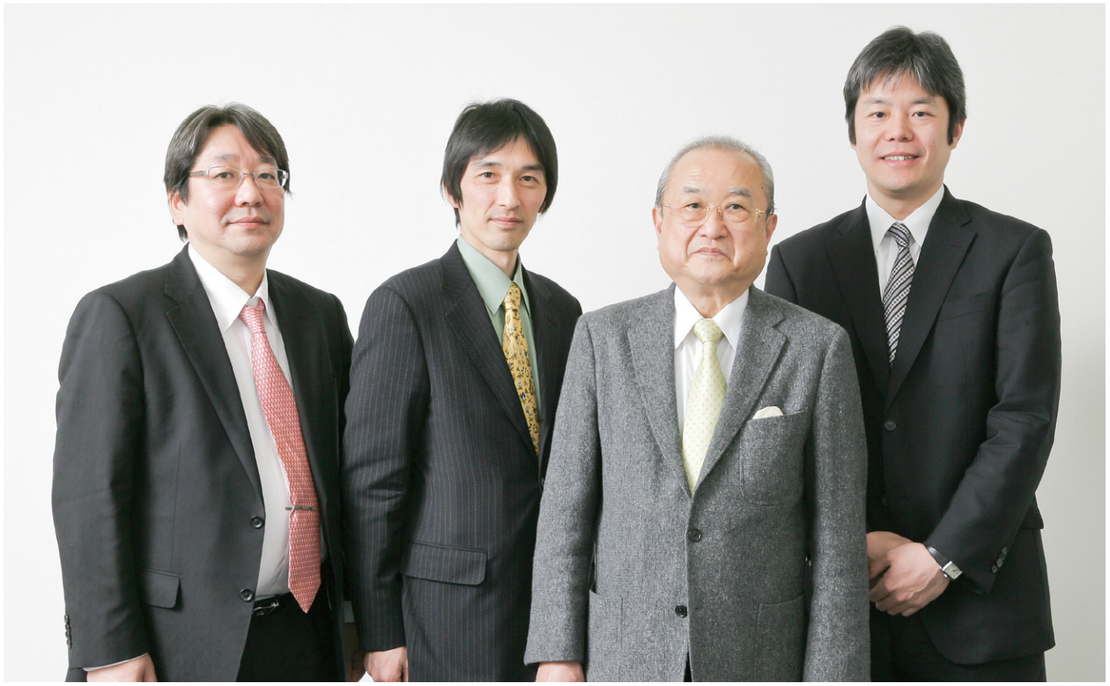
座談会の締めくくりとして、ISMS認証を取得している企業、また取得を検討している企業にメッセージをお願いします。

三角　繰り返しになりますが、ISMSはマネジメントシステムなので、運用者次第で有効な対策も打てるし、逆に無効な対策となってしまうこともあります。マネジメントシステムであるということを理解したうえで、マネジメントと合わせて技術面もしっかりと対応することが大切です。

駒瀬　企業としてISMS導入によるメリットを追求するなら、機密性だけでなく完全性や可用性にも着目すべきです。例えばWebサービスでサービス停止が起きないように完全性と可用性に着目した仕組み作りを目的とし、運用上の不備がサービス停止の要因であれば、その点を改善する管理策を強化し継続的に改善していく。ISMSは情報リスクに柔軟に対応できるため、事業継続など、もっといろいろな視点で活用することも考えていただきたいと思います。

上村　ISMS認証の取得は、個々の企業はもとより日本全体のセキュリティの底上げにつながります。セキュリティの文化をつくっていくという観点から、ISMSをより良くしていくために企業の皆さんの意見もお聞きしたいと考えています。またISMSという大きな幹を大切にしながらプラスアルファで何ができるのかといった議論も重要なポイントになると思います。相互承認が進めばISMSは海外市場で日本企業が信頼を築くベースとなりますから、もっと多くの企業に関心をもっていただきたいですね。

土居　2001年9月11日、アメリカの同時多発テロ事件の後、OECD(Organisation for Economic Co-operation and Development：経済協力開発機構)の情報セキュリティガイドラインの大幅な見直しが行われました。大きなポイントは、情報セキュリティの重要性を幅広く認識させる「a Culture of Security(セキュリティ文化)」という概念を導入したことです。
この概念には世界中の人々がセキュリティを文化として受け入れて安心な世界にしていこうというメッセージが込められています。ISOにしろ、各国のセキュリティ関連の制度はOECDの情報セキュリティガイドラインを踏まえています。ISO/IEC 27001にも冒頭にこの言葉がでてきます。上村室長からもお話がありましたが、国民ひとりひとりが文化としてセキュリティを身につけていく。ISMSは「a Culture of Security」を具現化していく1つの柱となるものです。



ISMSの昨日、今日、明日

日本マネジメントシステム認証機関協議会（JACB）
代表幹事　小林 憲明 氏

ISMS適合性評価制度の本格運用から１０周年を迎えるにあたり、心からお祝い申し上げます。此処に至るまでの、一般財団法人日本情報経済社会推進協会（JIPDEC）および関係者のご尽力に対し、改めて敬意を表します。
JACB傘下の認証機関は認定機関であるJIPDECのご指導のもと、ISMS規格の普及、審査・認証に努めて参りました。
１０周年に際して、ISMS制度の変遷を振り返ってみたいと思います。

平成12年7月31日より、既に実施されていた「情報システム安全対策実施事業所認定制度」(以下、安対制度という)を引継ぐ形でJIPDECによるISMS適合評価制度が開始されました。
安対制度は情報処理設備・施設をもつデータセンタの経済産業省による認定制度として普及し、200近い組織が認定を受けていました。
この認定を受け継ぐ形でISMS適合性評価制度がスタートしたお陰で、当初の認証に弾みがつき、普及して行きました。

安対制度は認証機関側から見ると、審査というよりも要求事項検査であり、また、国内基準として、日本で特に大きなリスクである地震に対する対策をはじめ、設備面と運用面について詳細な基準が設けられていました。また、検査の対象も、情報処理設備、施設を提供するデータセンタ側の基準が中心でありました。すなわち、情報処理設備を利用する組織のための基準ではなく、提供する側の基準であったと評価することができます。

ISMS適合性評価制度が開始されるにあたって、認証機関はISO 9001で行っていたプロセスアプローチを活用して、要求事項項番のチェックではなく、業務の流れの中で情報資産が適切に扱われているかを試行錯誤しながら審査をするようになっていきました。
また国際標準は責任と権限をより重視しており、日本人には理解が難しい、経営者のコミットメントなどの概念にも取り組みながら、日本の組織の特性を加味して国際標準に対応して参りました。

当初はITサービス提供者に対してデータセンタを中心にした審査をしていましたが、徐々にITサービスを利用する組織にもISMS制度は浸透しております。
現在4000社余りの組織が認証され、ISO 9001やISO 14001と並んだメインの規格に成長し、IT産業のためだけの規格ではなく、組織が情報を扱う時の規格へと理解されつつあります。また、これらの動きに伴い、ISO 9001やISO 14001と同時にマネジメントシステムの審査をする複合、統合審査の件数も多くなってきております。
認証機関と致しましては、規格があって審査をするのではなく、組織があり、その課題解決のために規格を組み合わせて使用し、その有効性を審査しようとの基本姿勢を堅持しております。

また、この流れにそったのが今ISO/IEC 27001の改訂として取り組んでいるハイレベルストラクチャー（HLS）をベースとした規格の改訂です。これが行われることにより、より一層課題解決のための規格の位置付けが明確になり、他の規格と一体となって、組織の情報を扱うための規格として拡大、成長していくと思われます。

これら世の中のながれにあった規格の適用推進のため、認証機関の協議会であるJACBはJIPDECと緊密に協力して努力して行く所存であります。ISMS制度の普及に際してJIPDECの役割は今後益々大きくなってくるものと期待しております。

ISMS適合性評価制度の今後の発展に向けて

日本ISMSユーザグループ
代表　中尾 康二 氏

近年、IT化の進展にともない、企業等において扱われる情報（資産）が多様化し、それらの資産管理が複雑になってきている中、不正アクセスやコンピュータウイルスによる被害、および内部不正者や外注業者による情報漏えい事件など、情報資産を脅かす要因（脅威）が著しく増加しています。これらの脅威に対して適切にリスク（資産に対する想定脅威による影響度）を算定し、導出されたリスクレベルの低減を実施し、企業における総合的な情報セキュリティ確保を遂行するためには、経営層の主導による「情報セキュリティマネジメントシステム（以下、ISMS）」の迅速な構築、円滑な運用が必達事項となっています。

ISMSの構築・運用を実施する企業の目線から、2004年7月29日、任意団体「日本ISMSユーザグループ（J-ISMSUG）」が設立されました。日本ISMSユーザグループは、ISMSの既認証取得企業を中心に、今後ISMS認証取得の予定企業、ISMSコンサルティング企業、ISMS標準化賛同企業などが密に連携することにより、ISMSの構築・運用など広範囲に渡るISMS関連技術（経験と知恵）を共有し、意見交換を進め、日本における健全かつ効果的なISMS普及・促進に貢献することを目的としています。なお、本設立においては、経済産業省、一般財団法人日本情報経済社会推進協会（JIPDEC）のご支援を頂いておりました。

ISMSユーザグループは、日本だけではなく、ISMSの構築・運用を積極的に推進する国々（英国、ドイツ、豪州、ブラジル等）に存在し、ISO/IEC 17799（情報セキュリティマネジメントの実践のための規範）の国際規格化（2000年)の後にそれらの設立が開始され、その活動が活発化されました。欧州やアジアなど世界20カ国以上のISMSユーザグループが国際ISMSユーザグループ（IUG）としてまとまり、ISMSの国際的な普及を促進しております。

日本においても、ISO/IEC 17799の国際規格化成立を起点として、2002年度からJIPDEC主管のISMS適合性評価制度の運用が開始され、2003年には、ISMS認証取得企業数は世界第1位となり、国際的にもISMS認証に関わる最先進国と認められるようになりました。このような背景から、日本においては2004年に日本ISMSユーザグループの設立を決定し、国際規格化への協力、研究会、セミナーの開催などの活動を精力的に実施して参りました。具体的な活動、成果については、Web（http://j-isms.jp/）を参照ください。

これまで日本ISMSユーザグループでは、国際規格化、ユーザ目線での課題解決などの観点から、日本における企業がISMSを適正かつ効率的に運用するためのガイドライン的な成果物をまとめてきており、結果的には、ある意味ISMS適合性評価制度の推進役として、制度活動の拡大などに貢献できていると自負しております。

しかしながら、近年の脅威の多様化/複雑化、クラウド、サプライチェーンなどを含めた企業が直面するビジネススタイル変化などの多くの外部要因の変化に鑑みても、ISMSに対する新たな考え方の整理が必要な時に来ていると考えます。具体的には、１）ISMSの基盤であるISO/IEC 27001を基本的に踏襲すべきであること、２）外部要因の変化に適切に、迅速に対応するためのISMS関連のガイドライン規格化、参考資料の充実化が必須であること、３）さらに、管理策のお手本となるISO/IEC 27002においては、外部要因対策に関連する記述をわかりやすく包含すること、４）プライバシー管理など、他施策との関係を整理することなどが今後の検討の方向性として重要になると考えます。

最後に、日本における「ISMS適合性評価制度」は他国とは比較にならないほど、制度運用面、管理体制面、推進体制面において卓越しています。上記の方向性なども視野に入れながら、日本ISMSユーザグループとしては、本制度のさらなる発展、及びより実践的な活用を目指して今後とも継続的な協力をさせていただく所存です。

●ISMS制度に関する問合せ先●

〒106-0032　東京都港区六本木一丁目9番9号 六本木ファーストビル内
一般財団法人 日本情報経済社会推進協会（JIPDEC）情報マネジメント推進センター
TEL.03-5860-7570　FAX.03-5573-0564
URL http://www.isms.jipdec.or.jp/

文書番号 JIP-ISMS130-1.0

一般財団法人　日本情報経済社会推進協会

〒106-0032　東京都港区六本木一丁目9番9号 六本木ファーストビル内
TEL.03-5860-7551　FAX.03-5573-0560
URL http://www.jipdec.or.jp/

発行年月　2013年2月