JQAインタビュー

わが国の情報セキュリティ政策と日本情報処理開発協会の取り組み


経済産業省 井土和志氏


JIPDEC 小林正彦氏


JIPDEC 高取敏夫氏

1990年代後半から社会のIT化が急速に進展し、産業や社会、個人の生活のすみずみまでITが浸透している。それに伴って情報システムに対する脅威も複雑化し、情報セキュリティ事故が企業価値に与える影響は増大する一方であるため、情報セキュリティ対策には、その場しのぎでない総合的・根本的な考え方が求められるようになった。以来今日まで、日本政府も、情報セキュリティ対策には継続的な取り組みを続けており、それを受けて財団法人日本情報処理開発協会（JIPDEC）などの公益法人が積極的に活動している。それらの取り組みについて、経済産業省の井土和志氏、JIPDECの小林正彦氏、高取敏夫氏にお話をうかがった。

JQA マネジメントシステム情報誌
ISO NETWORK

Contents
2009 vol.17

■ わが国の情報セキュリティの始まり

――ISMS（情報セキュリティマネジメントシステム）は2002年から正式な運用が開始されていますが、その導入が決断された頃の話をしていただけますか。特にその当時の情報セキュリティに関する状況はどういうものだったのでしょうか？

井土　わが国へのISMSの導入は、2000年に決断されました。1994年頃から本格利用され始めたインターネットの影響もあり、90年代後半になると、情報セキュリティに関して大きな環境変化が起こり始めていました。コンピュータシステムはクライアントサーバスタイルが主流となり、コンピュータウイルスや不正アクセスの問題が無視できなくなりつつありました。このような変化を背景に、当時の通商産業省（現経済産業省）は、俗に「安対制度」と呼ばれていた「情報システム安全対策実施事業所認定制度」の大幅見直しを課題として抱えていました。この見直しの一環として、ISO/IEC17799の前身であるBS（英国規格）7799についても海外調査を実施し、検討をしていました。このような中で、2000年の1月に霞が関の中央省庁の多くが連続的にホームページ不正改ざんの被害を受けたことも1つの契機となり、情報セキュリティ対策の官民あげての抜本的な取り組み強化が急務であるとの認識が政府の中で浮上していました。

ISMSは、廃止する安対制度の受け皿としても、また国を挙げての情報セキュリティ対策強化のためにも期待できる制度として、早急に導入しようということになったのです。

――そこで、財団法人日本情報処理開発協会（JIPDEC）の出番となったのですね。

小林　JIPDECは中立的な公益法人として、経済産業省をはじめ、国の情報化政策との密接な連携のもとで日本の情報化の発展に貢献するため、ISMS適合性評価制度やプライバシーマーク制度の運用など、さまざまな事業を行っています。

ISMSの導入にあたって、JIPDECは認定機関としての役割を担うこととなりました。井土さんのお話にあった経済産業省の調査でわかったのは、企業や組織における情報セキュリティ対策は、ウイルスや不正アクセスなど、気がかりな問題に対して場当たり的に対策を実施するだけではうまくいかない。もっと総合的な枠組みで進めるべきであるということでした。そのための処方箋として、欧米で本格的に定着してきているISMSが非常に有効であることもわかりました。安対制度に比べて幅広い事項をカバーできるだけでなく、PDCAに基づき企業の業種・規模・

経済産業省 商務情報政策局情報セキュリティ政策室 課長補佐
井土和志氏
2001年、外務省入省。2007年より現職。現在、主に企業の情報セキュリティ対策の推進に向けた諸制度の整備・運営、国際動向の把握等を担当。

財団法人日本情報処理開発協会 常務理事・情報マネジメント推進センター センター長
小林正彦氏
1979年、通商産業省（現経済産業省）入省。前経済産業大臣官房付・内閣官房情報セキュリティセンター内閣参事官。

状況に応じた柔軟な対応が可能であるなど、それまでの日本の企業に不足していた情報セキュリティ対策の推進エンジンの役割が大いに期待できるものでした。

高取　ＪIPDECがISMS第三者認証制度を立ち上げたのは2002年のことでしたが、当時はISOには対応する情報セキュリティの認証規格がありませんでした。正確にいうと、ISO/IEC17799というガイドライン規格はあったのですが、それはまだ認証の規格ではなかったのです。

そこで認証のための規格として、BS7799のPart2をベースとして、JIPDECが独自にISMS認証制度を立ち上げました。それがバージョン1.0から2.0へと進化し、最終的にはISO/IEC27001に移行しました。その間に約5年かかっていますが、認証登録をする事業者はIT関連から製造業やサービス業に広がり、日本が世界のISMS認証取得の過半数を占めるほどに普及しました。現在でもわが国は、ISMS認証取得の非常に多い国になっています。

■ 情報セキュリティ政策の4つの柱

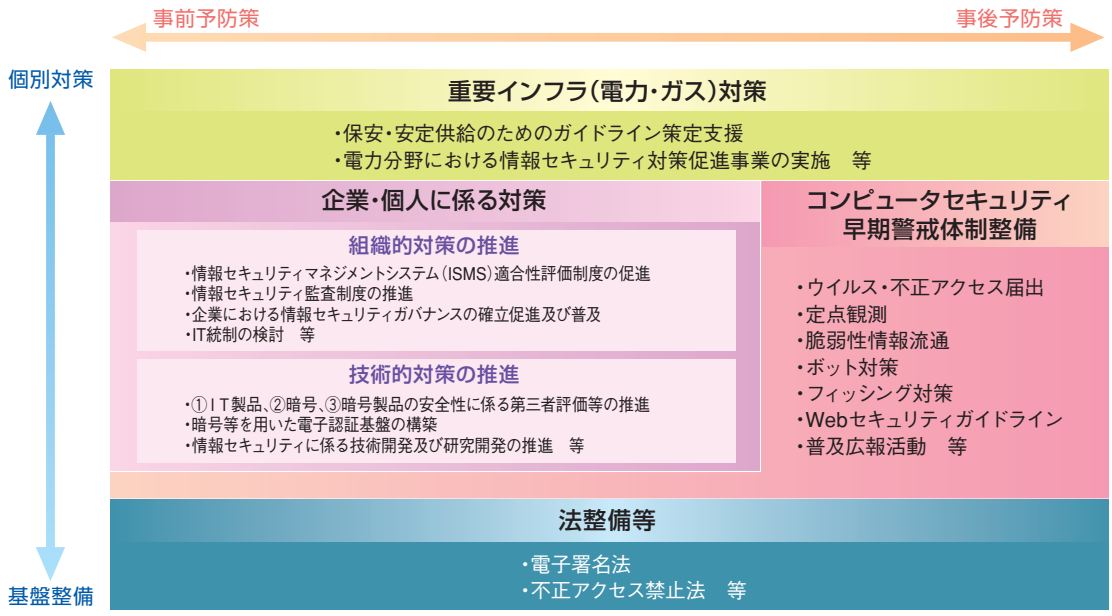
――経済産業省では、「情報セキュリティガバナンス」という言葉を使われていますが、これは現在の情報セキュリティ政策の中でどのように位置づけられるものなのですか？

井土　経済産業省の実施している情報セキュリティ政策は、大きく4つの柱から成り立っています。1つめは情報セキュリティの重要性を周知する普及啓発。2つめは暗号や認証システムの技術開発等を推進していく技術的対策。3つめは組織が適切に情報を管理していくための方策を検討する組織的対策。4つめが情報セキュリティに関する脅威が日々進化する中で、脅威に対応した対処策を検討する早期警戒体制の整備です。

この中で、ISMSは組織的対策の1つの例に含まれてくるものといえます。

ご質問の「情報セキュリティガバナンス」は、現在、経済産業省が組織的対策の推進事業の中心として進めているものです。これは、簡単にいえば、情報セキュリティ対

経済産業省の情報セキュリティ対策の全体像



策をコーポレートガバナンスの一環として実施すべきという考えに立っています。企業などの組織においてITを使う割合が急速に大きくなっていることに加えて、個人情報保護法や金融商品取引法などの新しい法制度に対応する必要も生じているため、もはやIT担当者だけでは最適化ができません。したがって、経営者が全体の観点から物事を捉え、どの情報が大事でどの情報がそれより優先度が劣るのかを決めた上で、コーポレートガバナンスの中に含まれるリスク管理の一環として情報を管理する必要があります。

このように、情報セキュリティ対策に組織全体できちんと取り組まなければいけないという基本原則のもとで、それを推進していくために、何ができたらいいのか、何をしていくべきなのかを考え、各種ガイドラインの整備等に取り組んでいるというのが、経済産業省が進めてきた情報セキュリティ政策の2005年以来の流れです。

ただし、これまでの情報セキュリティ政策はどちらかといえば大企業主導であり、中小企業の情報セキュリティ政策については、正直なところ未だ課題が多いと考えています。

――JIPDECはISMSに続いてITSMS（ITサービスマネジメントシステム）認証制度にも取り組まれ、そして昨年にはBCMS（事業継続マネジメントシステム）の実証運用も始められていますね。これはどういう経緯からでしょうか？

高取　2007年に、JIPDECはITSMS第三者認証制度の運営をスタートしました。情報セキュリティの分野に続いて、ITサービス運用の品質を向上させようと考えたからです。JIPDECとしては、IT分野に特化したともいえますし、事業の裾野を広げたともいえるでしょう。

小林　ISMSには15個の目的別に総計133の管理策が示されており、これらを検討して実施しなさいという構造になっているのですが、その目的の14番目に「事業継続管理」があり、それについても何かできることがあるなら実施するようにとなっています。しかし、他の情報セキュリティ管理策項目については、何をなすべきかがかなり具体的に詳しく書かれているのに対して、事業継続についてはその点があまり示されていません。詳細は企業や組織にほとんど任されている状態です。

これはITSMSについても同様で、（ITサービスの継続性という面から）事業継続は重要な項目とされているのに、同じく具体性がない。つまり、ISMSもITSMSも事業継続については「やりなさい」と明確に書かれているのにそのための虎の巻がないという状況でした。

一方、世の中では事業継続に対する社会的な関心が高まってきていました。アメリカの9.11テロ事件では、被災

財団法人日本情報処理開発協会 情報マネジメント推進センター　副センター長
高取敏夫氏

1970年、財団法人日本情報処理開発協会に入社。
2000年に同協会情報セキュリティ部で、情報セキュリティの調査研究、不正アクセス検査ツール実証、ISMS適合性評価制度の創設を歴任。

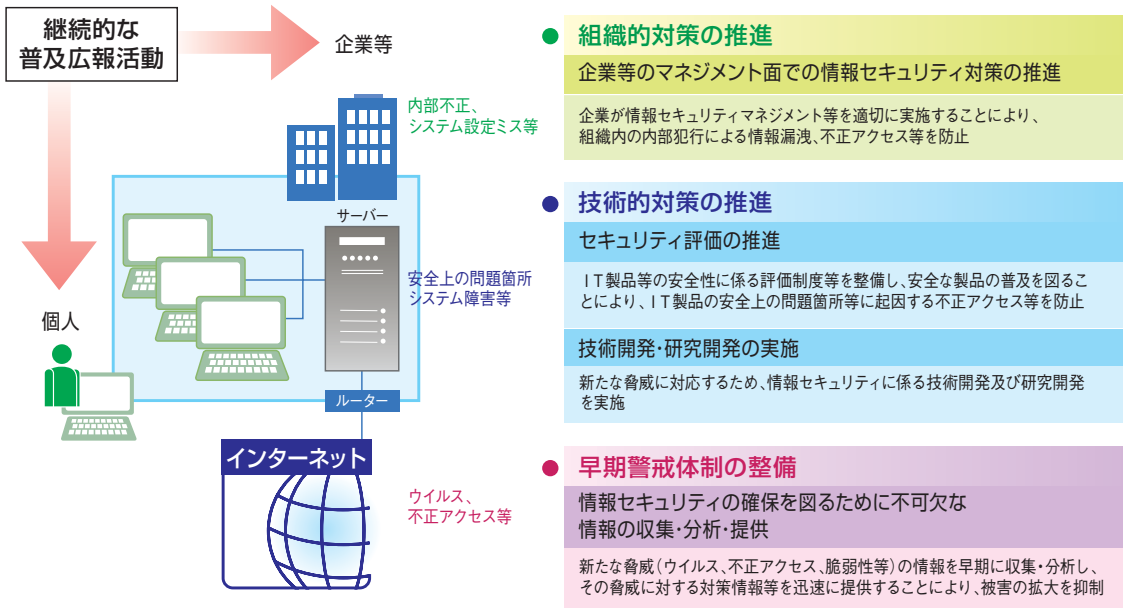
した企業のいくつかはバックアップセンターを備えていたために事業継続に成功し、2005年のハリケーン・カトリーナ災害では、行政の対策不備が指摘されました。日本でもかねてから首都圏や東海地方で大地震の発生が懸念されており、それらを背景として、政府から「事業継続計画策定ガイドライン」が出されました。

高取　ISMSやITSMSを十分にやりきるためには、事業継続にきちんと対応しなければなりません。そして社会の関心として事業継続はニーズが高まっている。それらを勘案して、JIPDECがBCMSにも領域を広げた理由の一つというわけです。

――BCMSが事業に加わってきた経緯はわかりましたが、BCMSというのは情報産業や情報領域に関わらない部分も多くあります。従来のISMSやITSMSといったJIPDECの事業範囲から一歩広げたのでしょうか？

小林　話の流れからいうと、ISMSやITSMSの中の事業継続の項目に対する具体策というか、処方箋ということでBCMSが浮上してきたわけですが、実際のところはBCMSのほうが考える対象が大きなものになっています。情報セキュリティやデータの安全性だけではない部分がたくさんありますから。その点では、逆「入れ子」構造とでもいうべき関係です。

脅威に対応するための情報セキュリティ対策（イメージ）



ただし、近年の企業経営はITを抜きにしては考えられませんから、情報セキュリティも事業継続も、現実的には不可分の関係になりつつあります。情報の管理が重要であることに関してはどちらも同じです。

一般的にいえばBCMSにはIT関連以外の業種や領域も対象となるわけですが、実効性のあるBCMSを考える場合には、情報の安全性確保は欠かせません。したがって、JIPDECの手がけているISMSとITSMS、BCMSは皆つながっていることになります。

■ 事業継続マネジメントシステムの広がり

――経済産業省では「事業継続計画策定ガイドライン」を発表されていますが、この背景をうかがえますか。

井土　数年前、事業継続という言葉がクローズアップされてきた頃に、日本企業のBCP（事業継続計画）策定率が非常に低く、海外に比べて大きく遅れているという状況が判明しました。こういった事情を受け、2005年、主にITの観点から事業継続に取り組んだ経済産業省と、防災という観点から取り組んだ内閣府がほぼ同時にガイドラインを策定しています。それからも事業継続の普及に関する調査は行っていますが、数字は上向いてはいるものの、まだ欧米等とは差があるというのが現状です。

BCMSの国際標準化については、ISOの場で検討が行われており、経済産業省の「事業継続計画策定ガイドライン」と、内閣府のガイドラインを統合し、日本案として提出しました。その後、今日まで議論が続いていますが、当初見込んでいたほどのスピードでは進展してはいないという状態です。

高取　2005年に出された経済産業省の「事業継続計画策定ガイドライン」は、JIPDECにとって非常にインパクトがありました。それから内閣府の「事業継続ガイドライン」や中小企業庁の「BCP策定ガイドライン」と、次々と政府からのガイドラインが出てきました。

ちょうどそのころ、JIPDECはISMSのために事業継続管理についての調査研究を始めていました。諸外国の現状に比べて日本が非常に遅れていることがわかり、BCPやBCM（事業継続マネジメント）だけではなく、マネジメントシステムとして考えていこうと決めたのもそのためです。

――BCMSではどのような対象を脅威として考えればいいのでしょうか？

高取　企業を襲う脅威には、さまざまなものが想定できます。大規模災害（地震など）や新型インフルエンザのパンデミック（感染爆発）、そして現在の世界を覆っている世界的な不況など、いろいろな脅威が思いもよらない方向から襲ってきます。それに企業や組織としてどう対応すればいいのか。実はパンデミックのように、あらゆる企業が直面する脅威に対する対応と、自組織だけが直面する深刻なIT事故のようなものに対する対応の両面からの検討が必要です。そのためにはまず、事業継続計画を作ること。そしてそれを形骸化させないために、有効な仕組みの中に取り込むこと。さらには、その仕組みの有効性を継続的に改善しながら維持すること。これがBCMSの基本的な考え方です。

日本の企業の方々は、QMSやEMSでマネジメントシステムには馴染みがあります。単なる事業継続計画の策定だけでは、そこで止まってしまう可能性がありますが、計

画を実行して、監視して見直すPDCAサイクルにすることができれば、有効に活用できるはずです。

小林　BCMSを大地震対策のような、100年に一度起きるかどうかわからない災害のためのものと考えている人がいますが、めったに起きないことに対する計画や備えというのは形骸化してしまいがちです。そうではなくて、起こる可能性のある脅威のうち、企業価値を大きく損ねるようなものに対する備えを仕組みとして管理するのがBCMSなのです。

――現在BCMSはISOの規格ではありません。ISOの規格になってから対応すればいいという企業もあるのではないでしょうか？

高取　確かにBCMSについては、まだISOの認証規格は存在していません。そのためにJIPDECは、BS25999という英国の規格を採用しています。ISOの規格としては2010年から2011年ころに、何らかのものが出てくると聞いています。

しかし、企業の事業継続はISOに基づくかどうかは関係なく、今すぐに対策すべきものです。それを独自で手探りでやるか、現時点で最も完成度の高いBS25999を使ってやるかは、企業を経営する方の判断すべきことですが、JIPDECは後者の方法が総合的かつ体系的な取り組みができる点で有利と考えています。

小林　仮に将来ISOの規格が出てきたとしても、BS25999の血筋をまったく引いてないものになるとは思えません。どの程度BS25999要素が入ってくるかは予想できませんが、少なくとも無縁のものにはならない、むしろかなり色濃く引き継がれると見ています。だとすれば、今からBS25999で事業継続に取り組んでも無駄にはならないでしょう。

高取　とりあえず、BCMSがどんなものであるかを知っておくことは、企業の方たちに有用と思います。そのために、昨年7月にJIPDECは『BCMSユーザーズガイド』を作成して頒布しています。自分たちの企業や組織でBCMSをどのように作り込んでいったらいいかを考えるときの参考になると思いますので、ご一読いただければ幸いです。

BCMSユーザーズガイド
―BS 25999-2：2007 対応―（JIPDEC発行）
入手先：財団法人日本情報処理開発協会
情報マネジメント推進センター

――BCMSに関して最後にひとことお願いできますか。

井土　経済産業省としては、企業における事業継続計画の策定が進展し、事業継続が企業の経営にとって非常に重要な考えであるということがきちんと認識されることが望ましいと思っています。BCMSに関するJIPDECの取り組みが、事業継続の重要性に対する理解が社会全体に浸透する一助として、有益なものとなることを希望しています。

小林　日本人というのは、取り組み始めるとすごく完成度の高いものを目指してしまう傾向があります。そのために、あれもこれも取り込もうとして行き詰まってしまう。また、それが予想されるので取り組みが始められないとなりがちです。しかし、最初の時点から頂点を目指す必要はありません。それぞれの企業や組織に合った地点からスタートし、自分たちのペースでレベルアップしていけばいいのです。事業継続の問題についても同様だと思います。BCMSは、このような漸進的な対応を可能にする仕組みであって、BCMSのこの考え方が世の中に早く普及してほしいと思っています。

本年1月19日から、JIPDECのWebサイトにてBCMS認証機関の認定条件や
BCMS審査員の条件などの実施要領等を含むBCMSに関するページが公開されています。
URL　http://www.isms.jipdec.jp/bcms.html