情報セキュリティマネジメントシステム(ISMS)の
国際動向と取り組みの実際

平成 14 年9月

(財)日本情報処理開発協会

目次

図表目次

図

表

1　世界の動き

1.1　ISMS を取り巻く歴史的背景と経緯

歴史的背景

ISMS は、情報セキュリティを管理する一連の仕組みを指す言葉である。品質管理システムを QMS(Quality Management System)と呼び、環境管理システムを EMS(Environment Management System)と呼ぶが、その情報セキュリティ版のことを ISMS(Information Security Management System)と呼ぶ。

情報通信技術の普及に伴い、安全性の問題が社会的に重要な問題であるという認識が高まる中、各国や国際機関等で、安全性に関するさまざまな取り組みが始まり、現在も続けられている。そのような動きの中で、英国では、この問題に関心の高い産業界の人々が集まり、1993 年に、「Code of Best Practice, Information Security Management」が作成された。これが、1995 年に、英国の ISMS に関する国家規格「BS7799:1995　A Code of Practice for Information Security Management」になった。BS7799:1995 は、その後、「BS7799-1　情報セキュリティ管理実施基準」と「BS7799-2　情報セキュリティ管理システム仕様」に分かれ、BS7799-1 が国際規格である「ISO/IEC17799　情報技術‐情報セキュリティ管理実施基準」になった。

認証と ISMS を取り巻く現状

現在、世界各国では、この BS7799-2 及び ISO/IEC17799(BS7799-1)が、ISMS を実践する際に参照する規格として、注目されている。BS7799-2 は、認証を取得するために参照する規格で、『～しなければならない(shall)』という形で、要求事項が書かれている。ISO/IEC17799(BS7799-1)は、管理策（情報セキュリティ対策）を策定する際に参照するガイドラインで、『～するとよい(should)』という表現形態が使われている。

BS7799-2 をベースにした、認証制度を最初に開発したのは、英国である。この英国の認証制度をモデルにして、その後、英国以外の国々で、同様の認証制度が作られ、運用されている。認証制度は、基本的に各国でひとつずつ整備されているが、それぞれの国で作られた認証制度のもとで認定された認証機関は、国内はもとより、国境を越えて、認証ビジネスを展開している。従って、認証制度

が確立されていない国でも、国際的に認証ビジネスを行っている認証機関から認証を取得することが可能であり、世界全体で認証取得が進んでいる（認証制度を取り巻く状況の変化）。また、ISO/IEC17799 や BS7799-2 等の規格は、現在、見直し作業が進められており、進化を続けている（内容の変化）。このように、ISO/IEC17799 および BS7799-2 をベースにした ISMS を取り巻く状況は、その認証取得と内容という 2 つの側面で、複雑なグローバル・ダイナミクスの中で、変化している。認証取得という視点で見た場合、ISO/IEC17799 や BS7799-2 の内容の変化と認証取得の国際動向を捉えておくことが重要である。

ISO/IEC17799 や BS7799-2 等の規格は、枠組みを示す規格と言われている。これらの規格では、ISMS を構築し、情報セキュリティマネジメント（ISM）を実践するための基本的な要求事項を記述してあるが、具体的に実施していく際には、さらに多くの知識が必要となる。たとえば、物理的セキュリティにおいて、ドアの施錠という管理策を策定する場合は、どのような手段があり、どのような考えでそれらを選択していけばよいかを知っておかなければならない。各国では、このような管理策策定に役立つガイドライン等も作成されている。

ISMS（もしくは ISM）に取り組む組織は、このような各国の関連するガイドラインについても、情報を収集しておくと有益である。

1.2 ISO/IEC17799 と BS7799-2 の国内規格化の現状

ISO/IEC17799 や BS7799-2 を、自国の国家規格として採用する動きが広まっている。以下に、2002 年 3 月時点での調査結果に基づき作成した各国の状況を示す。

国名	ISO/IEC17799 の国家規格化	BS7799-2 の国家規格化
日本	○	×
米国	×	×
カナダ	×	×
英国	○	○
ドイツ	×	×
オランダ	○	○
オーストラリア	○	○
ニュージーランド	○	○
ブラジル	○	○
チェコ共和国	○	○
フィンランド	○	○
アイスランド	○	○
アイルランド	○	○
スウェーデン	○	○
ノルウェー	○	○
イスラエル	×	×
デンマーク	×	×
ポーランド	×	×
ハンガリー	×	×
シンガポール	×	×

○：すでに国家規格として発行している国

×：検討中もしくは未検討の国

1.3 各国の認証取得の現状

各国での認証取得数（表 1）を以下に示す。なお、これらの最新情報は、国際的民間組織、インターナショナル・ユーザ・グループが、インターネット上の以下のサイトで公表している。

http://www.xisec.com/Register.htm

表 1 各国の BS7799 認証数

国名	認証数	国名	認証数
英国	52	ギリシア	2
インド	6	香港	2
シンガポール	5	アイルランド	2
ドイツ	4	イタリア	1
日本	4	オランダ	1
韓国	3	ノルウェー	1
スウェーデン	3	エジプト	1
台湾	3	スペイン	1
米国	2	アラブ首長国連邦	1
中国	2	オーストラリア	1
フィンランド	2	オーストリア	1
		合計	100

*2002 年 3 月時点の調査結果に基づき作成。
*参照したサイト：http://www.xisec.com/Register.htm

1.4 世界の認証取得企業(事業所)

世界の認証取得組織と認証機関の名称(表 2)を以下に示す。なお、これらの最新情報は、国際的民間組織、インターナショナル・ユーザ・グループが、インターネット上の以下のサイトで公表している。

http://www.xisec.com/Register.htm

表 2 認証取得企業(事業所)リスト

No.	認証取得企業(事業所)	国名	認証機関
1	ABB Facilities Management AB	Sweden	DNV
2	Accordis Acetate Chemicals Ltd, Derby	UK	BSI
3	Alenia Marconi Systems Ltd, Dorchester	UK	BSI
4	American Society of Quality	USA	BSI
5	AMOUN Pharmaceutical Co, Cario	Egypt	BSI
6	Attenda Ltd, Staines and Heathrow	UK	BSI
7	Baltimore Technologies, Dublin	Ireland	LRQA
8	Bank SinoPac, Information Technology Division	Taiwan, ROC	DNV
9	Britannic Money plc	UK	KPMG Certification Services
10	Brite Voice Systems Group	UK	SGS ICS Limited
11	BSC Consulting	UK	DNV
12	BT Exact Technologies, Ipswich	UK	LRQA
13	BT Group Security, Milton Keynes	UK	LRQA
14	Business Coach IT Management, Swansea	UK	BSI
15	C2 Management AB	Sweden	DNV
16	CADWEB Ltd, London	UK	BSI
17	CAMELOT Group plc, Watford and Aintree	UK	BSI
18	Chatham Archive Ltd	UK	SGS ICS Limited
19	Churchill India (P) Ltd, New Delhi	India	STQC Certification Services
20	Citibank N.A, Asia Pacific Processing Center	Singapore	PSB Certification
21	Consignia plc	UK	DNV
22	DAI-ICHI KANGYO BANK Ltd, London	UK	BSI
23	DBI Consulting, Kenilworth	UK	BSI
24	DeTeCSM GmbH Deutsche Telekom Computer Service Management GmbH, Krefeld, Bielefeld,	Germany	DQS

	Darmstadt, Regensburg, Kronshagen, Münster, Bonn, Hamburg, Frankfurt am Main, Selb, Magdeburg, Griesheim, Bonn/Bad Godesberg, Berlin, Bad Kreuznach, Norden/Norddeich		
25	ABB Facilities Management AB	Sweden	DNV
26	Detica Limited	UK	DNV
27	DNP Facility Services Co Ltd	Japan	BSI
28	Eastlands Benefits Administration, Basingstoke	UK	BSI
29	e-Cop.net	Singapore	PSB Certification
30	Energis UK, Reading	UK	LRQA
31	Ericsson ESPA A S.A	Spain	BSI
32	Foreign and Colonial Management Ltd	UK	DNV
33	GESAB Engineering AB publ.	Sweden	DNV
34	GLAXO WELLCOME Manufacturing	Singapore	BSI
35	GLAXOSMITHKLINE, Montrose and Speke	UK	BSI
36	GTECH Ireland Corporation	Ireland	DNV
37	HackersLab Taiwan Co Ltd	Taiwan, ROC	BSI
38	Hanvit Bank Info Tech Unit	Korea	BSI
39	Hays Commercial Services	UK	BVQI
40	HM Government Communications Centre	UK	LRQA
41	Huangdao Power Plant of Shandong	China	DNV
42	Hughes Software System, Gurgaon (Haryana)	India	STQC Certification Services
43	IMServe Europe, Milton Keynes	UK	LRQA
44	Insight Consulting Limited	UK	DNV
45	Insurance Technology Solutions plc, Leeds	UK	LRQA
46	International Integrated Systems Inc	Taiwan, ROC	BSI
47	Intermail plc, Newbury	UK	LRQA
48	Kensington Mortgage Co, London	UK	BSI
49	KPMG	UK	BVQI
50	Larsen & Toubro Ltd, Engneering and construction division, Mumbai and Vadodara	India	STQC Certification Services
51	LEDU	UK	SGS ICS Limited
52	Link Interchange Network ltd	UK	KPMG Certification Services
53	Logic Systems Management	UK	BSI
54	Logica UK Limited	UK	DNV
55	Luton Borough Council, I.M. Div	UK	National Quality Assurance
56	Marconi Secure Systems	UK	DNV
57	McCarthy & Associates	UK	SGS ICS

			Limited
58	Mcquarie Corporation	Australia	BSI
59	MIDAS-KAPITI International, London	UK	BSI
60	Mitsue Links Co Ltd	Japan	BSI
61	NDS Corporation, Seoul	Korea	DQS
62	Netstore plc, Berkshire	UK	DQS
63	Netstore plc, Berkshire	UK	BSI
64	Nihon Unisys Ltd	Japan	KPMG Certification Services
65	Norsk Informasjonssikkerhet AS	Norway	DNV
66	Novotrust Oy	Finland	SFS Certification
67	NTT DATA ITSC Group	Japan	BSI
68	One2One plc,Hatfield, Herts	UK	LRQA
69	Panacea Services Ltd, London	UK	LRQA
70	Panafon S.A.	Greece	National Quality Assurance
71	Panafon Vodafone	Greece	National Quality Assurance
72	Paramount Computer Systems, Dubai Internet City	UAE	BSI
73	PICC, Xiamen Branch	China	DNV
74	Property Search Agency Ltd, London	UK	BSI
75	S-Cube Inc, Seoul	Korea	BSI
76	Satyam Computer Systems, Secundrabad	India	STQC Certification Services
77	Serco Consultancy, Malvern	UK	BSI
78	Siemens Aktiengesellschaft Österreich A-1211 Wien	Austria	DQS
79	Siemens Business Services GmbH & Co. OHG Siemens IT Service Region Deutschland D-81739 München	Germany	DQS
80	Siemens Business Services Trust Center, Munich	Germany	BSI
81	S.I.A Spa	Italy	DNV
82	Sony Information System Solutions (Asia Pacific) (A divisional company of Sony Electronics (S) Pte. Ltd.)	Singapore	PSB Certification
83	ST Microelectronics Ltd, Noida	India	STQC Certification Services
84	Stonewood Electronics	UK	BVQI
85	Syan Ltd, High Wycombe	UK	BVQI
86	Synstar International	UK	DNV
87	Terrington Systems Limited	UK	SGS ICS Limited
88	The Co-operative Bank plc, Lancashire and Salford	UK	BSI
89	The University of Texas	USA	BSI

90	TietoEnator Oyj	Finland	SFS Certification
91	Total Network Solutions Ltd, Oswertry	UK	BSI
92	TQM Consultants Ltd	Hong Kong	BSI
93	Trustis Limited, London	UK	LRQA
94	Unilever GIO Asia	Singapore	PSB Certification
95	Unisys Ltd, Milton Keynes	UK	BSI
96	Vhsoft Technologies Co. Ltd	Hong Kong	DNV
97	Vodafone Telecommerce GMBH, Ratingen	Germany	BSI
98	Volex Group plc, Warrington	UK	BSI
99	Wellance, Amsterdam	Netherlands	LRQA
100	Whyte & Company	UK	National Quality Assurance

*2002 年 3 月時点の調査結果に基づき作成。
*参照したサイト：http://www.xisec.com/Register.htm

1.5 国際組織

インターナショナル・ユーザ・グループ（IUG）

インターナショナル・ユーザ・グループ（IUG）は、情報セキュリティマネジメントのベストプラクティスにおける一般的な興味を共有するための世界規模のコミュニティである。

その目的は、以下にまとめられる；

① **プロモーション**
ベストプラクティス、ISO/IEC17799 や BS7799-2 をベースとした適切な情報セキュリティマネジメントのノウハウの適用を促進したり普及させる。

② **アウェアネス**
世界的規模でビジネスの利益に供するために、ISMS 規格、認証、開発のアウェアネスと理解を促進する。

③ **ネットワーキング**
IUG のメンバーが互いに情報交換するフォーラムを提供する。

④ **情報交換**
IUG のメンバーが情報交換するプラットフォームを提供する。

⑤ **研究活動とコラボレーション**
ISMS のソリューションを構築するための研究や ISMS 関連のペーパーを作成する。

具体的な活動としては、国際コンファレンスやセミナー、オンライン・ディスカッション・グループの管理などがある。全世界で ISMS の認証を取得している企業や認証機関名の情報も、IUG で集められ公開されている。また、BS7799-2 の改訂作業は IUG を中心として行われている。BS7799-2 は、すでにドラフトが作成され、パブリック・コメントが求められている。今後は、このドラフトに基づき BS7799-2 の改訂版が正式に発行される予定となっている。この BS7799-2 が ISO 規格として提案されるか否か、またもし提案されるとしたら、そのタイミングはいつになるのかについては、未定である。

IUG の活動は、インターネット上の以下のサイトで公開されている。

http://www.xisec.co.uk/

ISO/IEC　JTC1/SC27（ISO/IEC17799 規格を制定する委員会）

ISO において、情報セキュリティ関連の規格策定を議論しているのは、「JTC1/SC27：情報技術：セキュリティ・テクニック」と呼ばれる委員会である。日本もこの委員会のメンバーとして規格作成に参加している。BS7799-1 は、2000 年 10 月に開かれたこの JTC1/SC27 の会合で、3 分の 2 の賛成票を獲得し、ISO/IEC17799 になった。現在、JTC1/SC27 では、ISO/IEC17799 改訂のための議論が展開されている。2002 年 4 月の会合では、各国から多くのコメントが提出され、改訂版が発行されるのは、数年先になるという見方もある。

JTC1/SC27 の情報は、以下のインターネット URL で見ることができる。
http://www.din.de/ni/sc27/

日本の窓口は、以下のとおりである。

Japan (JISC)
Address:
JISC
c/o Standards Division
Industrial Science & Technology Policy and Environment Bureau - METI
ISO/IEC JTC 1/SC 27 "P-Member"
1-3-1, Kasumigaseki, Chiyoda-ku
Tokyo 100-8901
Japan
Telephone: + 81 3 35/01 92 87
Telefax: + 81 3 35/80 86 25
E-Mail: 27japan@itscj.ipsj.or.jp

JTC1/SC27(情報通信セキュリティ)の活動状況は、以下のアドレスにまとめて紹介されている。
http://web.sfc.keio.ac.jp/~naemura/sc27.html

1.6 まとめ～国際的認証取得数、認証取得業種に基づく考察と認証取得の動機の分析

世界の認証取得数に基づく考察

2002 年 8 月時点で、世界全体で、認証を取得している企業(事業所)は、約 140 件である。この数字から、ISMS 認証は、まだ普及が始まったばかりという現状が推測できる。各国の ISMS 認証の現状については、まず、この規格の元になっている規格 BS7799 を作成した英国での認証が最も多く約 70 件である。この背景には、英国の経済省にあたる DTI(Department of Trade and Industry)と産業界による、推進活動があるのは言うまでもない。DTI によると、1999 年には両者が協力して実施したワークショップなどに 450 を超える機関が参加したということである。また、DTI では、企業の情報セキュリティ担当者向けに、先進的に、ISMS を構築し実施している企業が、実際に、何故 ISMS に取り組み始めたか、何をどのように実施しているのかなどを、わかりやすく事例紹介するパンフレットを作成したり、同じ情報をインターネット上で公開するなどの推進活動を行っている。シンガポールでも、英国などから ISMS のスペシャリストを招いて講演会を行うなどの活動を実施している。インドでも、情報技術省(Ministry of Information Technology) が、BS7799 認証を推進している。このような政策的な後押しが認証数の増加に繋がっていると思われる。

全体的な認証数が少ないため、現時点で判断するのは難しいが、官民ともに、情報セキュリティマネジメントの重要性を認識し、推進している国において認証取得数が増えているといえる。また、欧米、アジアといった経済エリアによる特徴はなく、全世界で同じように立ち上がりつつあると見られる。特に、アジアの IT 先進国と見られるインドやシンガポールでの認証取得が進んでいる点が注目される。

世界の認証取得業種に基づく考察

2002 年 8 月時点、全世界で BS7799-2 に基づく認証を取得している企業と認証機関の一覧を見ると、認証を発行した機関として突出しているのは、英国の BSI で、全体の約 40%の認証を行っている。全般的に、現時点では、世界的規模で認

証事業を展開している機関による認証が多い。これは、英国の認定機関である UKAS に認定された認証機関による活動が、全世界的規模で以前から展開されてきた結果と言える。

認証を取得している組織の傾向を見ると、全般的に、IT 関連の事業を行っている企業、たとえば IT コンサルティング会社、テレコミュニケーション・サービス会社、IT セキュリティ関連会社などの認証が多い点が指摘できる。また、最も認証取得が進んでいる英国の状況等を概観すると、IT 関連を中心とした企業に加え、金融関連（銀行の情報通信部門、オンライン・バンク、保険等）、医薬品、ファシリティ・サービス、認証ビジネス、ビジネス・コンサルティング、EC ビジネス等の事業者などが含まれる。また、政府機関などによっても認証が取得されているといった現象も起きている。たとえば、英国の郵便を取り扱っている Consignia などが認証を取得している。

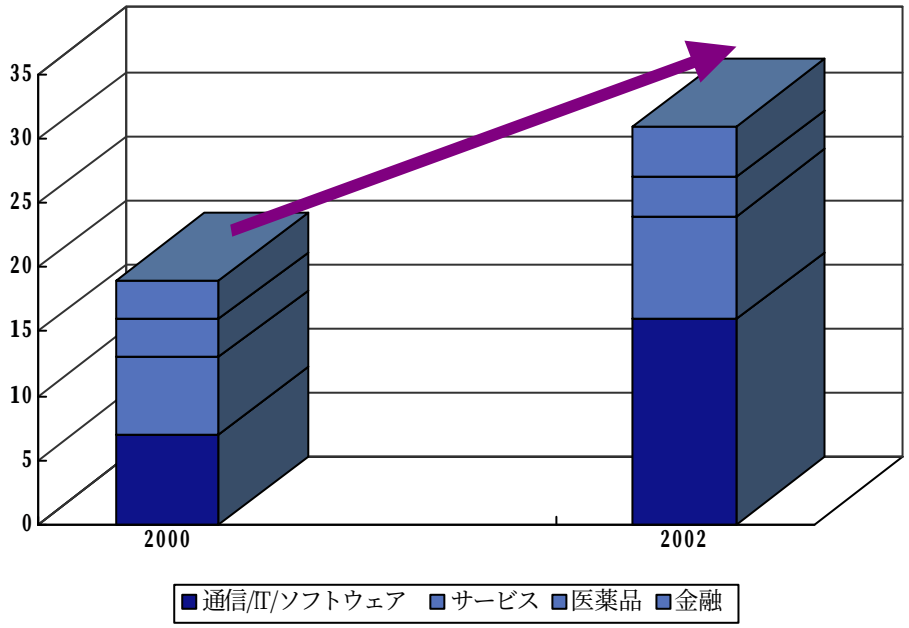


図 1　認証取得業種の変化

図 1 は、認証取得数の最も多い、BSI による 2000 年 11 月時点での認証数と 2002 年 2 月時点での認証数を業種別に比較したグラフである。一認証機関のデータですが、全体の動向を推測するに足る情報を提供していると考えられる。

このグラフによると 2 年前の 2000 年に 20 件だった認証取得数が 2002 年には 34 件と約 1.5 倍になっている。認証取得企業の内容を見ると、IT 関連業者が多く、2 年間の比較をしても、この IT 関連企業の認証取得の伸びが最も大きくなっている。顧客情報が経営上重要な資産になるサービス業に加え、医薬品関連や金融関連業種の認証取得が多い点が注目される。特に金融関連は、銀行の情報通信部門やオンライン・バンクなどで認証が取得されている。

認証取得の動機の分析

認証取得企業の業種や規模などから、認証取得の動機を分析すると以下にまとめられる。

1　　重要な情報があり、それを保護する手段として認証を取得

データが漏洩した場合のダメージ（損害賠償、企業イメージの低下など）を考え、事業を行っていく上で、データの信頼性の確保が重要と考える業種の認証取得。このような業種の例としては、金融関連、人材派遣、宝くじビジネスなどを実施している企業があげられる。

2　　IT 関連サービスを提供する上で、知見が必要

まず、自分で体験する必要があると考える業種の認証取得。このような業種の例としては、IT 関連サービス、ファシリティ・サービス、コンサルティング等があげられる。

3　　自社のサービス品質向上の一環として認証を取得する

認証を取得することにより、自社のサービスは十分情報セキュリティに配慮した上で実施されている点を明確に示すために認証を取得。顧客から重要な情報を提供してもらわなければビジネスそのものができない、他社との差別化の材料として認証取得が有効な企業が多い。このような業種の例としては、EC ビジネ

ス、インターネットバンク、認証サービスなどがあげられる。

4　国際企業で、他の拠点での認証取得が進みチェーンプレッシャーがかかった

同一の企業グループの中で、情報共有がされており、その結果チェーンプレッシャーが働き、認証を取得。この現象は、特定の業種に限らずに起こっている。

2 各国の動きと取り組みの特徴

2.1 英国

BS7799 開発の歴史に見る官民協力体制の実態

BS7799 の開発は、「情報セキュリティマネジメントの基準が必要」と考えた産業界の情報セキュリティ・マネージャーたちが、英国の経済産業省にあたる DTI(Department of Trade and Industry)に働きかけたのがきっかけで始まった。これは、DTI にとっても、初めてのケースであった。DTI は産業界の声を聞き、開発の手助けをすることにした。1990 年から 91 年にかけて、DTI と産業界は協力して、”Code of Best Practice, Information Security Management”を開発し、1993 年に発行した。これは、BSI における検討を経て、国家規格 BS7799 として発行された。

BSI での検討において、重要な役割を果たしたのは、産業界のメンバーで構成されるグループ、BDD（Business Development Group）のひとつである、BDD/2 である。BDD/2 は、BSI の関連組織である BSI/DISC Committee の一種である。DISC は、産業界とコラボレーションするスキームを開発してきた組織で、産業界のメンバーで構成されるグループ（BSI/DISC Committee という）をマネジメントするという役割(ビジネス)を担っている。BS7799 は、この DISC を中心としたスキームに乗っ取って作成された。現在、BS7799 のガイドラインとして DISC PD シリーズが発行されているが、これらもこのような産業界のメンバーが作成したものである。

アウェアネス向上のための推進策

DTI では、ISMS のアウェアネス向上のために、いくつかの活動を実施している。そのひとつは、セミナーの後援である。1999 年の時点で、すでに 450 機関がワークショップ、もしくはセミナーを受講した。DTI が支援したこのようなセミナーにおいて、講師として講演するのは、ISMS に取り組んだ企業の情報セキュリティ・マネージャー等である。

また、認証取得企業等の取り組み内容をケーススタディとして、インターネ

ット上で公表したり、小冊子を作成し配布したりしている。これから、ISMS に取り組む組織は、これらの情報から、実際の取り組みの様子を知ることが可能である。

DTI のインターネット上のアドレスは、以下のとおり。
http://www.dti.gov.uk/

認証取得組織に学ぶ ISM 実践のポイント

◎ 従業員のアウェアネスを同じレベルにする

ある英国の金融関連企業では、ビジネスに必要なソフトウェアの開発、開発者の人材管理、および会社全体の情報資産を管理するトップマネージャーがいた。そのマネージャーは、以前から社員全員に情報セキュリティの重要性に気づいてもらう必要を感じていた。そこで、BS7799 の認証取得を決意した。ISM の実践では、アウェアネスの向上や教育が要求されていたからである。やはり、ISM の実践において、苦労したのは、IT 関係者以外の従業員の理解を得ることであった。情報セキュリティの重要性を認識してもらうために、その主旨を説明することによりアウェアネスの共有を図った。

◎ 従業員のアウェアネス向上や教育を継続的に実施する

◎ ISM の実践において、最も難しいのは、アウェアネス向上や教育を継続的に実施することだという。ある認証取得組織では、社内ネットワークを使ったｅ-ラーニング・システムを開発し、社員のアクセスを自動的に記録できるようにしたということであった。

◎ アウェアネスツールの開発

アウェアネスツールとして、コースター(図 2)、ハンドブック(図 3)、カレンダー、などが使われている。

表

裏

図 2　　コースターを使ったアウェアネス

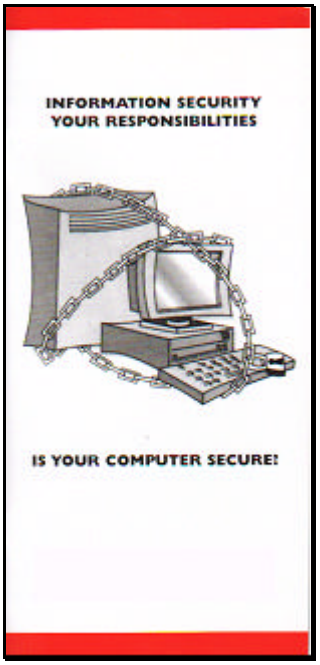


図 3　　パンフレットを使ったアウェアネス

◎　　既存の情報セキュリティ対策を見直すための ISMS

英国で、ISMS に取り組んでいる組織では、ISMS を採用する以前から、さまざまな情報セキュリティ対策を実施している組織が多い。ある組織では、以前から社内監査等を実施しており、情報を資産として捉えそれを保護するというマインドは十分あったといえる。別の組織では、十年も前から、情報セキュリティ・マネージャーという役職を設置し、アウェアネス向上への取

り組みや社内教育などを実施してきている。このような組織には、情報資産を管理者や情報セキュリティの担当者といった、社内の専門家が存在していた。このような人々が、最終的に選択したのが、ISMS というアプローチだったのである。ISMS は、既存の情報セキュリティ対策を見直す手段として有効なツールといえる。

◎ 情報セキュリティ・スコープの明確化とポリシー

ある組織では、ISMS に取り組むにあたって、情報セキュリティ・スコープを『顧客情報の保護』と『サービスのアベイラビリティ』に決めたということであった。これが、結果的に目的、すなわち何を達成すべきか明らかにし、情報セキュリティポリシーに明記した。このことにより、ISM の実践を容易にした。

2.2 ドイツ

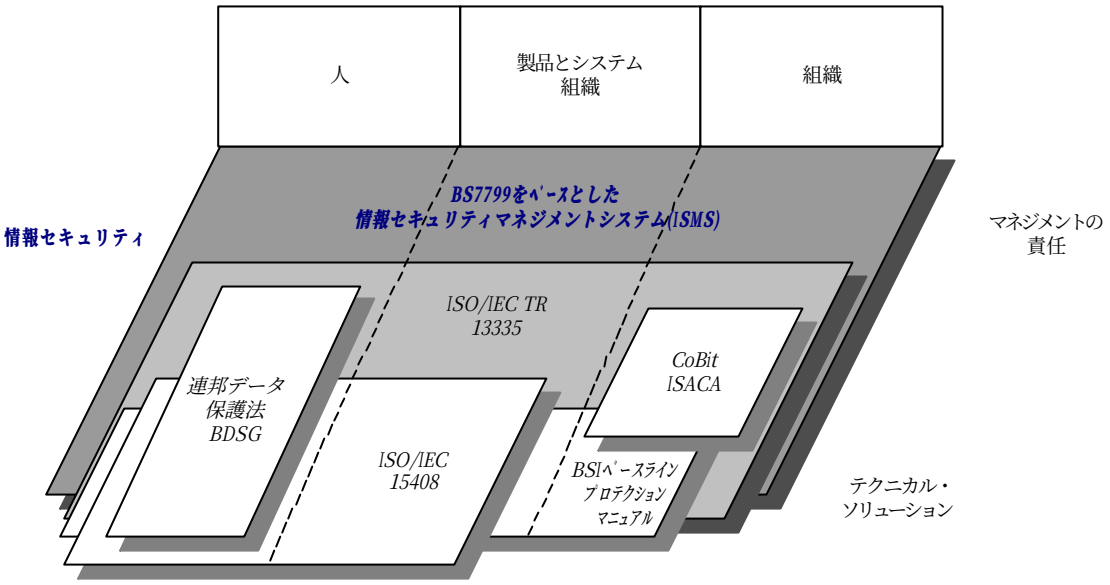
ISMS 関連の 2 つの取り組み

ISMS に関連するドイツ国内の取り組みには、2 つの流れがある。ひとつは、BS7799-2 に基づく認証取得である。もうひとつは、「ドイツ BSI」と呼ばれる独立行政法人のガイドライン策定である。

BS7799-2 に基づく認証取得

ドイツの認証取得数は、2002 年 3 月時点で、4 件である。そのうち、2 件が Siemens により取得されている。また、各認証機関の認証数は、DQS（ドイツ品質保証機構；Deutsche Gesellschaft zur Zertifizierung von Managementsystemen mbH）が 2 件、BSI が 2 件となっている。DQS は、1985 年にドイツで最初のマネジメント規格の認証機関として設立された。設立にあたって German Institute for Standardization (DIN)、German Society for Quality (DGQ)が出資している。DQS では、1998 年に ISMS の認証を行うことを決定し、2000 年 12 月に TGA[1]の認定を受けた。

[1] TGA(Trägergemeinschaft für Akkreditierung GmbH)は、ドイツの認定機関で、ISMS の他に、ISO9000、ISO14000 などに関する認定を行っている。2002 年 3 月時点で、BS7799－2 に関する認定を行った機関は、DQS と UIMCert GmbH である。



*CoBit ISACA[2]･･･Governance, Control and Audit for Information and Related Technology; Information Systems Audit and Control Association

図 4　DQS の考える BS7799 と他の規格との関係

図 4 に示すように、DQS では、BS7799 をマネジメントの責任から技術的なソリューションまで、広範な分野をカバーする規格と捉えている。このような理解の元で、グローバルスタンダードを適用することのメリットを認め、認証取得を積極的に推進している。

DQS の情報は、以下のインターネット HP で見ることができる。
http://www.dqs.de/

ドイツ独自のガイドライン「IT ベースライン・プロテクション・マニュアル」

ドイツで IT セキュリティの普及、及び e-Government のサポートを実施す

[2] CoBit ISACA については、http://www.isaca.org/cobit.htm を参照。
http://www.isaca.gr.jp/homepage_j.htm
CoBit ISACA については、http://www.isaca.org/cobit.htm を参照。

るために、1991 年、BSI 法に基づき、「ドイツ BSI」(Bundesamt fur Sicherheit in der Informationstechnik が、設立された。ドイツ BSI は、Ministry of Interim の下部組織で、独立行政法人である[3]。

ドイツ BSI では、「IT ベースライン・プロテクション・マニュアル」を作成し、その活用を推進している。「IT ベースライン・プロテクション・マニュアル」は、ISO/IEC17799 の内容を包含しているというのがドイツ BSI の認識である。「IT ベースライン・プロテクション・マニュアル」は、表 3 に示すような目次で構成されている。

表 3　「IT ベースライン・プロテクション・マニュアル」の目次

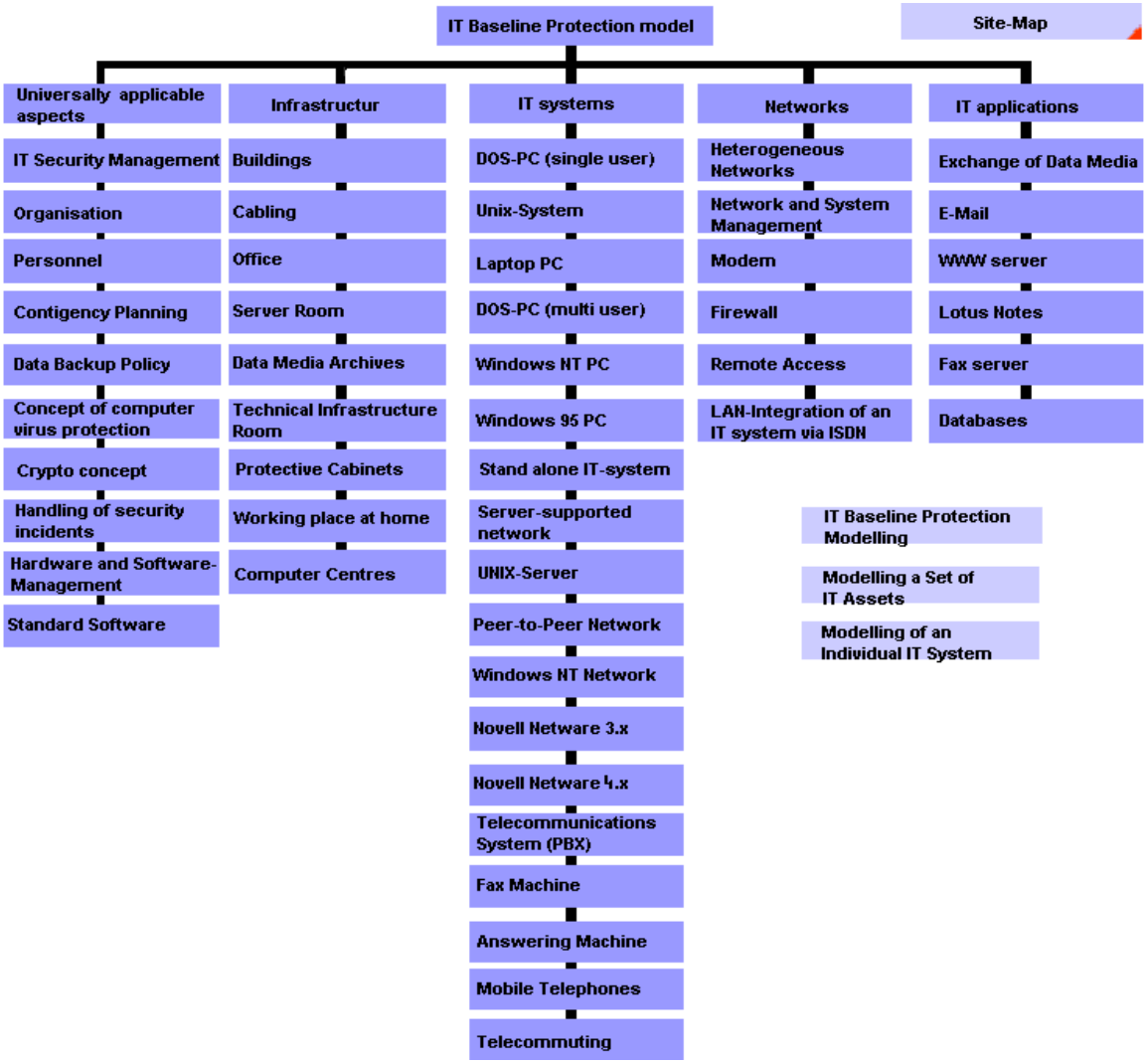
- 概要
- 使い方
- 一般的事項
- インフラストラクチャー
- 非ネットワークシステム
- ネットワークシステム
- データ伝送システム
- テレコミュニケーション
- その他の IT コンポーネント
- 保護対策一覧
- 脅威一覧

「IT ベースライン・プロテクション・マニュアル」の内容は、以下のサイトで見ることができる。

http://www.bsi.bund.de/gshb/english/menue.htm

上記のアドレスで、「IT ベースライン・プロテクション・モデル」を選択すると、図 5 に示すように、全体の枠組みが表示される。個々の項目を選択すると、詳細なガイドラインを見ることができる。

[3] ドイツ BSI は、その名前から英国の規格協会である BSI と混同しがちであるが、両組織は無関係である。ドイツ BSI については、以下のページに日本語の詳しい記述がある。
http://www.ipa.go.jp/security/ccj/ninshou/german.htm
また、ドイツ BSI のホームページは、以下のとおりである。
http://www.bsi.bund.de/index.htm



http://www.bsi.bund.de/gshb/english/menue.htm より

図 5　「IT ベースライン・プロテクション・モデル」の構成

認証取得企業に学ぶ ISM 実践のポイント

ギャップ分析とリスク評価

まず、既存のセキュリティ対策を使うことを考え、残存リスクを評価した。これに対して、セキュリティ上の管理策を策定した後の残存リスクを評価した。これらの作業は、情報資産の所有者が責任を持って行っている。また、リスク評価にはISO TR13335-34、RA Software Tool5、BSI PD3005等が使用されている。

従業員のアウェアネスが成功の鍵

従業員のアウェイアネスが成功の鍵と認識し、それを向上させるために、「セキュリティを意識的に体験する」というスローガンを掲げ、目に見える形でのアウェイアネス・シンボルを使って、実践している。具体的には、ポスター(図 6)やパンフレット（図 7）の作成、社内誌や社内ネットワークへの記事掲載、セキュリティのコンプライアンス違反についてのステッカー（図 8） 、CD を使用したインタラクティブ・ゲームの開発、主な情報セキュリティ問題をまとめたカード（図 7）などを、作成し実践している。

---

[4] ISO TR13335-3 は、「情報技術－情報技術セキュリティ管理指針パート 3：情報技術セキュリティの管理技法」という ISO 規格である。リスク評価の手法を解説している。

[5] BSI により発行された BS7799 用のリスク評価ツールである。内容の説明やデモ版のダウンロードは、http://www.c-cure.org を参照。コンタクト先は、c.cure@bsi-global.com。日本語化の予定もある。

図 6　　情報セキュリティ・マネージャーとポスターの原版

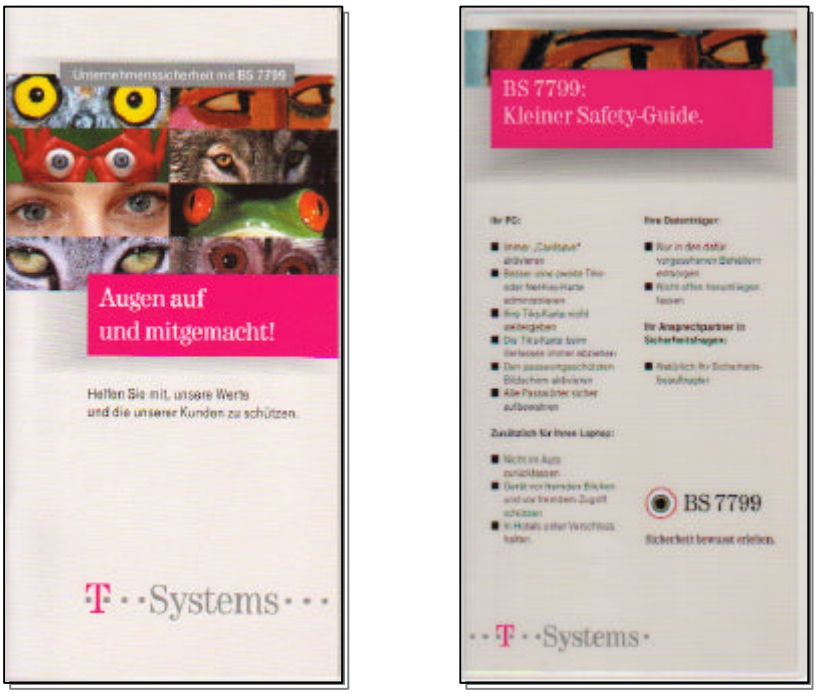


図 7　　パンフレットとカード

図 8　　ステッカー

以下のサイトにドイツ企業の取り組み事例のプレゼンテーション資料が提示されている。

http://www.xisec.com/BS7799Certification.pps

また、リスク評価については、以下に解説（プレゼンテーション資料）があり、参考になる。

ISO/IEC 17799 Risk Assessment

2.3 シンガポール

情報通信セキュリティ政策

シンガポール情報通信当局（iDA:the Info-communication Authority of Singapore[6]）は、情報通信セキュリティ（iSec: the Infocom Security）に、国際的な注目が集まっていることを受け、2001 年 11 月 30 日に、アニュアル・インフォコム・セキュリティ・デー・キャンペーン(annual Infocomm Security Day/ Campaign)を開始している。キャンペーンの目的は、コンピュータ・ユーザのセキュリティ・アウェアネスを高め、適切な iSec の習慣を身に付けることの価値をコンピュータ・ユーザに教え込むことであった。

シンガポール生産性規格委員会(PSB:Singapore Productivity Standards Board)も同様に、情報セキュリティマネジメント（ISM:Information Security Mangement）を調査するシンガポール企業を支援するためのプログラムを開始した。そのひとつのキーとなるプログラムは、PSB Certification Pte ltd により管理される「PSB 情報セキュリティマネジメントシステム認証スキーム(the PSB Information Security Management System(ISMS) Certification Scheme)」である 。2001 年 11 月 20 日の時点で、以下のシンガポールの４企業が、このスキームのもと BS7799:1999(Part2)認証を取得している 。

- Unilever－Global Infrastructure Organization Asia
- Sony－Electronics (S) Pte Ltd　Information Systems and Solutions Asia Pacific
- e-Cop.net (S) Pte Ltd
- Citibank, N.A. －Asia Pacific Processing Center

認証取得企業の傾向

シンガポールにおいて、BS7799:1999(Part 2)認証普及の鍵となる推進力としては、以下の 2 つが上げられる。

[6] http://www.ida.gov.sg/Website/IDAhome.nsf/Home?OpenForm

①内部的　－ 社内のセキュリティ基準への適合（特にマルチナショナル企業）
②外部的　－ 主要な顧客やビジネス・パートナーによる要求が増えている。特に、ネットワーク・アクセスが、許されているか、または、取り引きがオンラインで実施されている場合が多い。

このことは、シンガポールで認証を取得している企業の多くが国際企業であることから明らかである。さらに、どの企業も、リーディング・カンパニーである。

データ保護法の影響

現時点(2002 年 3 月 18 日)で、シンガポールでは、ISMS 規格を採用するように企業に義務付けている法規制はない。しかしながら、海外企業のデータ保護法準拠が、2 つの方法でシンガポールの企業に影響を与えている：1)データ保護法は、シンガポール内の企業に対して、駐在員の個人情報を流すことを禁止している；2)データ保護法は、第 3 者の国に存在する部署が同様の個人情報をシンガポール国内の企業に流すことを制限している。

小売業者(特に、e-テイラー)、直接市場で売買する人や店、金融機関、通信業者、情報通信サービスプロバイダー、製造業者、大学、病院などが、海外企業のデータ保護法により影響を受ける可能性があるデータの利用者である。

国家規格の動向

ISO/IEC17799 及び BS7799-2 の国内規格化の検討はすすんでいるものの、BS7799-2 が国際規格化されるのを待っている状況である。

PSB Certification Pte Ltd により運営されている ISMS 認証スキームとは別に、PSB と iDA は、「**シンガポール標準 SS 493 (Part1)**」と称する国内の IT セキュリティ標準フレームワークを開発するための情報技術標準委員会(Information Technology Standards Committee[7])を有している。

SS 493 (Part1)は、以下の 4 つのパートで構成されている：

[7]情報技術標準委員会のウェブサイトは、http://www.itsc.org.sg

Part1　概要(An Overview)
Part2　セキュリティ・サービス(Security Services)
Part3　構造とメカニズム(Architecture and Mechanisms)
Part4　プロセスと手法(Processes and Methods)

2002 年 3 月 18 日時点では、「Part1　概要」のみが公開されており、それ以外の標準及び SS 493 を受けた認証スキームは、未だ開発されていない[8]。

SS 493(Part1)は、以下の分野をカバーしている。

1. SS 493(Part1)文書で使われる一般的な用語の定義
2. IT セキュリティ標準フレームワークのコンセプトへのイントロダクション
3. フレームワークの目的
4. フレームワークのための設計分類
5. フレームワークの解説
6. フレームワークの利用方法

情報技術標準委員会のウェブサイトは、以下のとおり。
http://www.itsc.org.sg

SS493 の情報は以下のサイトで見ることができる。
http://www.itsc.org.sg/sg_it_stds/abstract_ss493_1.html

認証取得企業に学ぶ ISM 実践のポイント

セキュリティ・トレーニングとアウェアネス

セキュリティ・トレーニングは、3 時間のコンパルソリ・トレーニングを全従業員に受講させた。方法は、セミナー方式を採用した。アウェアネスの目標を、「ISMS にかかる責任とは何かを知らせる」こととした。パンフレットの作成、ポ

[8] 2002 年 3 月 18 日に、現地の調査機関が PSB に電話で問い合わせた結果得た情報による。

スターの掲示などをおこなった。たとえば、プリンターの脇に、「出力したデータを置きっ放しにしてはならない」という警告を表示したり、ドアに「開けたままにしてはならない」という警告を表示している。

プロセスマネジメントへの取り組みと ISMS

シンガポールのある企業では、ISMS を構築する際に、CMM-SW(Capability Maturity Model for Software)と関連付けて取り組んでいる。CMM-SW は、組織の『ソフトウェアプロセス』の成熟度を評価するためのモデルである。『ソフトウェアプロセス』は、「ソフトウェアおよび関連成果物（例えば、プロジェクト計画、設計文書、コード、テストケース、およびユーザマニュアル）の開発と保守に使用する活動、手法、プラクティス、および変換作業の集合[9]」として定義されている。CMM-SW では、継続的にプロセスを改善し、組織におけるソフトウェア成熟度レベルを上げることを目的として実施されている。CMM-SW への取り組みを続けている同社では、ISMS の構築及び実践のために、従業員へのトレーニングや教育の中で、ISMS についてだけではなく、組織としての総合的な取り組みとして説明し、理解を促している。

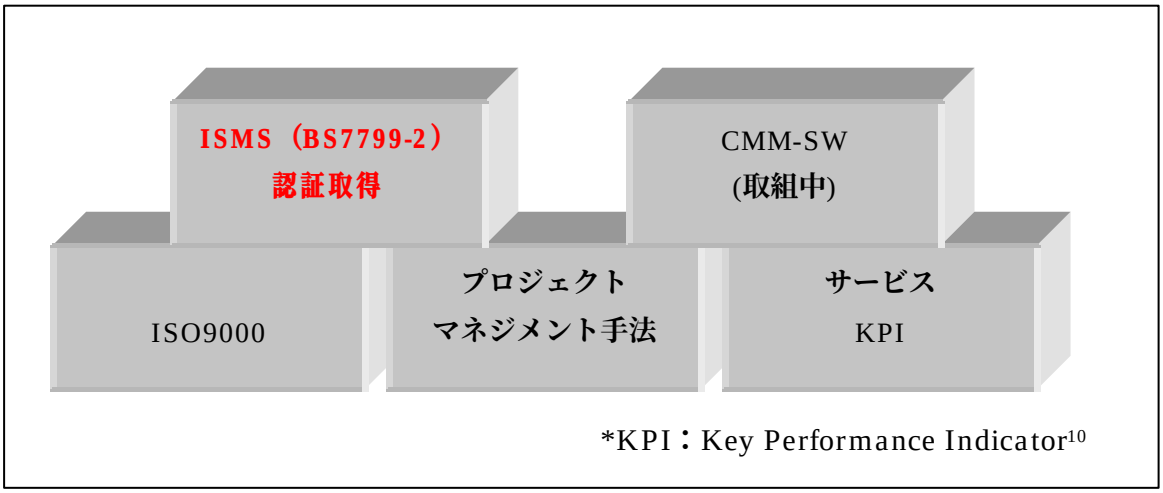


図 9　品質及びセキュリティ管理の関係図の例

[9] ソフトウェア能力成熟度モデル 1.1 版, 1993, pp.3
[10] KPI とは、重要業績評価指標のことである。(http://www.tokyo-biso.co.jp/n_ifm02/n_ifm02.html より)

CMM(能力成熟度モデル)については、以下のサイトをご参照ください。

http://www.iijnet.or.jp/sea/CMM/publish/CMM-J99.html
http://www.sei.cmu.edu/cmm/cmm.html

2.4 オーストラリア・ニュージーランド

関連する国家規格

オーストラリアでは、1995 年から、BSI により開発された BS7799 を受け入れ、“変更することなく”、AS/NZS4444(現在、AS/NZS ISO/IEC17799:2000)という国家規格として採用した。さらに、2000 年には BS7799-Part2 を AS/NZS4444:2(現在、AS/NZS 7799.2:2000)としている。これに伴い、同年、認証スキームが導入された。また、これに関連するハンドブックとして、「HB 231:2000 Information security management guidelines」が 2000 年に作成され、現在中小企業向けのハンドブックが作成されている。

オーストラリアには、汎用的に使用できるリスクマネジメント規格「AS/NZS 4360:1999 Risk management」が存在する。これは、ISMS 構築を始めるにあたって参考となる規格と考えられている(図 10)。

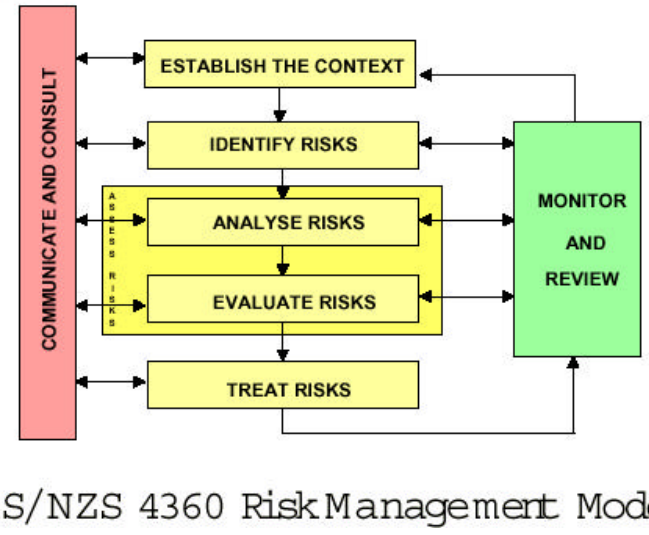


図 10 オーストラリアのリスクマネジメントモデル規格（AS/NZS 4360）

オーストラリアの規格は、以下のサイトからアクセスできる。
http://www.standards.com.au/catalogue/Script/search.asp

認証制度の動向

オーストラリアにおける規格を管理しているのは、豪州規格協会(Standards Australia)である。その下部組織である「品質保証サービス(QAS:Quality Assurance Services)」が、規格へ適合している組織の認証に責任を持っている。AS/NZS7799 Part 2:2001 及び BS7799.2:1999 に対する認証の提供も、この QAS により行われている。

QAS の認定は、オーストラリアとニュージーランドの合同認定機関(Joint Accreditation System of Australia and New Zealand(JASANZ))により行われた。

ISO/IEC17799 は、大手銀行などに採用され、企業における認知度は徐々に高まっている。また、政府の電子商取引セキュリティ・ガイドラインにも含まれており、州政府の中には、これをもとにポリシーや標準を書き直しているところもある。

セキュリティ・サービスを提供している企業によると、顧客は、ISO/IEC17799 をベースにしたサービスを志向しているということである。ただし、現時点では、セキュリティの重要性を十分に認識している大規模組織における取り組みに限られており、中小企業への普及は次の段階と考えられている。

普及の速度が遅いのは、産業界における認知度が低いのが原因と思われる。そのため、JASANZ が開始した認定制度において、認証機関として認定された組織が QAS のみに留まっている。これに対して、JASANZ では、ISMS の普及を促進するため、アウェアネス・プログラムを展開していく計画があるということであった。

ニュージーランドに関しては、関連規格および認定システムもオーストラリアと合同で実施されており、ISO/IEC17799 もこの分野におけるキーとなる規格として位置付けられている。政府関係者（eGovernment unit）によると、ニュージーランドは、限られた政府資源しか持たない非常に小さな国であるということが理由として挙げられている。

QAS の ISMS 関連情報は、以下のサイトで入手できる。
http://www.qas.com.au/SECTIONS/InfoSecurityManagement/

JASANZ の ISMS 関連情報は、以下のサイトで入手できる。
http://www.jas-anz.com.au/homeframe.htm

2.5 米国

政府関連機関 NIST の公表文書

米国国立標準技術局(NIST:National Institute of Standards and Technology)[11]は、米国商務省の技術管理本部の部局で、標準の開発と適用を行っている。NIST の ISO/IEC17799:2000 に関する考え方を、「International standard ISO/IEC 17799:2000 Information Security Management, Code of Practice for Information Security Management Frequently Asked Questions, December 2001」（ここでは、NIST FAQ 文書と呼ぶ）をもとに、以下にまとめる[12]。なお、この文書には、正式な米国政府の見解を述べたものではないという但し書きが付記されている。

ISO/IEC17799:2000 の捉え方

NIST FAQ 文書では、ISO/IEC17799 は一般的な組織に関する情報セキュリティマネジメントのガイドとして捉えられている。

従って、ISO/IEC17799:2000 のカバーする範囲は、同規格は、決定的な詳細もしくは“ハウツー“を提供することを意図したものではなく、ポリシーや一般的な「グッドプラクティス(推奨策)」についてのトピックスを表記したものと説明している。

さらに、ISO/IEC17799 がカバーしていない範囲に関する説明の中では、セキュリティの広い範囲の話題(トピック)について触れているが、深いところまでは追求していないと評している。そこで、詳細な組織上の情報セキュリティレビュー、もしくは認

[11]米国商務省の技術管理本部の部局名。当初、1901 年に The National Bureau of Standards として設立されたが、議会によりミッションが拡大強化され、1988 年に名称も現在の NIST に改称された。現在の年間予算は 8 億ドル、職員は 3,330 名にのぼる。

NIST は、技術、計測、標準の開発と適用を通じて、産業界と深くかかわりながら、米国経済の発展と生活の質の向上に貢献している。NIST の活動は、次の４領域に大別される。

*Measurements and Standards Laboratories：米国産業界強化の為のインフラ整備
*Advanced Technology Program：民間企業とタイアップしての先端技術開発の推進
*Manufacturing Extension Partnership：中小企業への技術、事業支援
*Baldrige National Quality Award：企業、各種団体向けの品質向上表彰制度

[12] http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf

証プログラムをサポートするに足る情報を提供していないというのが NIST の考え方である。ISO/IEC17799 は、上級管理者がセキュリティのさまざまな分野に含まれる基本的な問題を理解するのには役立つものとしている。

さらに、暗号に関しての ISO/IEC17799 の全表記を引用し、より詳細なガイドラインが NIST で開発（NIST Special Publication(SP)800-21）され、ウェブからダウンロードできるとコメントしている[13]。

ISO/IEC17799:2000 と BS7799 の捉え方

BS7799 は、BS7799（Part1）と BS7799（Part2）から構成されている。ISO/IEC17799 は、BS7799-1 は、組織的な情報セキュリティマネジメントプログラムのための仕様ではなく、認証に使うことはできない。BS7799-2 は、ISMS のための仕様であり認定された認証のための基盤として使うことができる。BS7799-2 は、ISO/IEC17799 とは、直接的な関係はない。

ISO/IEC17799:2000 と ISO/IEC15408:1999(Common Criteria)との関係

この 2 つの規格には、内容及びアプローチに関して、密接な関係はない。両者は、同じもしくは似通った事柄をカバーしているわけではない。

“Common Criteria”は、製品における IT セキュリティ機能の使用及び技術上の評価をすることを意図している。これに対し、ISO/IEC17799:2000 は、技術上の規格ではなく、IT システムの導入に関連して非技術的な課題を評価するマネジメント規格である。このような課題は、人事、手続き、物理セキュリティ、セキュリティマネジメントなどとともに取り扱うべき事柄である。

“Common Criteria”により評価された IT 製品やシステムを使用することにより、組織が直面するセキュリティ・リスクを軽減するために有効である。この点についての参考資料として、

[13] http://csrc.nist.gov/publications/nistpubs/index.html

“NIST Special Publication 800-23, Guide to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products[14]”がある。

認証システムについて

ISO/IEC17799 は、認証とは関係なく、現在は、BS7799-2 の認証があるのみである。いくつかの国では、ISO/IEC17799 の一部が国の法律、特にプライバシーに関する法律と矛盾するということを表明してきている。

ISO/IEC17799:2000 は、ISO/IEC JTC 1 SC 27(IT Security Techniques)で、セキュリティ標準に積極的に参加している国の中にも反対国があった。

2000 年 6 月に提出された米国の見解は、かなりの技術的な理由で採用に反対するものであった。米国の”ISO/IEC JTC 1”と”ISO/IEC JTC 1 SC27”の”Technical Advisory Group(TAGs)”のメンバーのほとんどは、米国の産業界を代表するものである。正式な米国政府の見解は表明されていないが、”Commerce Department(via NIST)” 及び ”Department of Defense(via DISA)”から参加している US TAG メンバーは、米国の見解を支援している。現時点(2001 年 12 月)での米国の興味は、2000 年に提出した技術上のコメントを考慮してもらうべく、大規模な改定を行うことである[15]。

NIST の見解

NIST は US NB の見解を支援している。米国政府、米国の”ISO/IEC JTC 1”と”ISO/IEC JTC 1 SC27”の”Technical Advisory Group(TAGs)”の産業界のメンバーの大多数は、この見解を支持している。

---

[14] http://csrc.nist.gov/publications/nistpubs/index.html

[15] 米国が 2000 年に提出したコメントは、添付資料「International standard ISO/IEC 17799:2000 Information Security Management, Code of Practice for Information Security Management Frequently Asked Questions, December 2001」を参照。

加えて、ISO/IEC17799:2000 は有料であるが、NIST は、有益な文書を無償で提供している。

どのような NIST 文書が、ISO/IEC17799 の変わりに使えるか？

NIST が提供している組織的情報セキュリティマネジメントに役立つ文書には以下のものがある。

- SP 800-12, Computer Security Handbook
- SP 800-14, Generally Accepted [Security] Principles & Practices
- SP 800-18, Guide for Developing Security Plans

- SP 800-23, Guide to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- SP 800-26, Security Self-Assessment Guide for Information Technology Systems

ISO/IEC17799 の現状

ISO/IEC17799 は、2000 年のファースト・トラックで持ち出された多くの技術的課題にについて、JTC1/SC27 内で始まっている。ジョイント・プロジェクト・エディターは、ドイツの Oliver Weissman と英国の Angelika Plate である。

標準化に関する米国の組織

ISO/IEC JTC 1 SC 27 に対する TAGs は、”National Committee for Information Technology Standards(NCITS), Technical Committee T4, Security Techniques” である。”Technical Committee T4, Security Techniques”は、情報技術セキュリティのための一般的な方法の標準化に参加している。これは、セキュリティ技術とメカニズム；セキュリティガイドライン；セキュリティ評価分類；情報技術システムセキュリティサ

ービスに対する一連の要求事項の特定などのために作業を行っている。ISO/IEC JTC 1 SC27 に対する US TAG として、T4 は、JTC 1 TAG に対して米国の見解に関する推奨事項を提供している。

NCITS 技術委員会における投票メンバー及びアドバイザリー・メンバーになるための費用(1 名の代理人を含む)は、年間 800 ドルである。NCITS 技術委員会 T4 の委員長は、Rowena Chester, University of Tennessee(roc2@cornell.edu)である。

NCITS 技術委員会 T4 のウェブサイトは、
http://www.ncits.org/tc_home/t4.htm

NCITS 及び JTC 1 TAG へのメンバーシップ情報は、以下のウェブサイトで入手できる。
http://www.ncits.org/

米国の JTC 1 (JTC 1 TAG)に対する技術アドバイザリー・グループのウェブサイトは、以下のとおり。
http://www.jtc1tag.org/

NIST FAQ 文書によると、米国の政策として、広義の ISMS（これを組織的情報セキュリティマネジメントと呼んでいる）は推進しているが、ISO/IEC17799 については、改善すべき点があるというのが大方の意見である。従って、本調査において、積極的に認証制度を確立し推進するといった英国に見られるような動きは認められなかった。しかしながら、NIST が 1996 年 9 月に発行した「Generally Accepted Principles and Practices for Securing Information Technology Systems[16]」では、BS7799 を参照しており、その内容を全面的に否定しているというわけではない。

[16] http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

民間活動の実態

産業界では、徐々に ISO/IEC17799 への認識が高まりつつある。しかしながら、そのスピードは遅く、始まったばかりといえる。現在は、コンサルタントが企業などのセキュリティシステムの全般的な評価を行う際に、フレームワークとして ISO/IEC17799 を使っているというのが主な動きである。

米国の政府機関や ANSI は、ISO/IEC17799 の作成に積極的に関与してこなかったため、ISO/IEC17799 に関して、個人を訓練したり、認証することができる組織は、米国には存在しない。従って、米国のコンサルタントのほとんどは、国外で訓練を受け資格を取得している。必要な資格を取得した後、ISMS の審査を行うために米国の機関に雇用されているというのが現状である。

米国においても、特に、国際企業が BS7799-2 の認証取得に強い興味を示している。これは、グローバルスタンダードになりつつある BS7799-2 に準拠して、情報セキュリティマネジメントシステムを構築していること、さらに第三者による認証を取得しているということを対外的に示すことのメリットを理解しているためである。このような事実は、米国政府が ISO/IEC17799 にあまり関心を示していない現状においても、米国の市場に存在する事実である。

このような産業界のニーズを受けて、業界団体も動き出している。業界団体の動きとしては、IT 関連企業のコンソーシアムである「Software Productivity Consortium」が、ISO/IEC17799 教育事業を開始した。同コンソーシアムでは、ISO/IEC17799 及び BS7799-2 の認証制度に関する情報収集を行ったり、担当者が BSI の審査員コースを受講するなどの準備をしていた。2002 年 10 月には、「ISO 17799 Information Security Management Systems Implementation」という 5 日間の教育コースをオープンする[17]。このような活動を通して、米国における ISO/IEC17799 の認知度は加速することが予想される。

[17] http://www.software.org/pub/training/course.asp?id=800

2.6 カナダ

行政当局の考え

カナダの標準化機関(”Canadian National Standards Body”)の見解は、米国と同様、ISO/IEC17799 は、国際標準にするのは、時期的に早すぎたというものである。カナダの行政当局では、いくつかの ISO 標準やガイドラインは採用しているが、受け入れていないものもある。ISO/IEC17799 もそのひとつという考え方が主流である。現在、法規制の整備と、特定の詳細部分に関して、法規制を補完するさまざまな 2 次的出版物について作業を行っているが、その中に ISO/IEC17799 は含まれていない。カナダにおいては、連邦政府が制定した法律が、産業界や政府全体を拘束する。連邦政府が実施していない分野に関して、州政府などが独自に法規制を実施するということはない。従って、現状の行政当局の動向としては、ISO/IEC17799 を積極的に推進していこうというものではないというのが大方の意見と推測される。ただし、保健省が発行した「GOOD PRACTICES FOR COMPUTERISED SYSTEMS IN REGULATED "GXP" ENVIRONMENTS[18]」(ドラフト)では、データ管理に関するセクションで、ISO/IEC17799 が参考になると記述しているなど、米国と同様、必ずしも、全ての行政当局の見解が一致しているわけではない。

民間の動向

現在、カナダでの認証取得は、ゼロである。ISO/IEC17799 の改訂作業が終了するには、さらに 1 年以上かかると考えられている。その影響もあり、米国の民間セクターとは異なり、カナダでは、ISO/IEC17799 はそれ程普及しないだろうと予測している。カナダでも、大規模企業が、ISO/IEC17799 を自分の評価のための基礎情報として活用することはあると思うが、米国のコンサルタントが行っているほど多くは ISO/IEC17799 はカナダのコンサルタントには利用されていない。

カナダの情報セキュリティへの取り組み

ISO/IEC17799 への取り組みは消極的であるが、カナダにおける情報セキュリティへの取り組みが遅れているわけではない。むしろ、政府機関の情報セキュ

[18] http://www.hc-sc.gc.ca/hpfb-dgpsa/inspectorate/goodprac_comp_syst_pics_entire_e.html#20

リティへの取り組み等は、他の国々よりも進んでいる。

関連文書は、カナダ大蔵省 Treasury Board of Canada-Secretariat の Policies and Publication のサイト[19]で見ることができるが、特に、Security Policy[20]等は、ISMS に取り組む際に参考になる。

また、規格としては、リスクマネジメントの規格である CAN/CSA-Q850-97 Risk Management: Guideline for Decision Makers も参考になる。カナダの規格は、以下のサイトからアクセスできる。

http://www.csa.ca/language/default.asp?thisUrl=%2FDefault%2Easp

19 http://www.tbs-sct.gc.ca/pubpol_e.html
20 http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/siglist_e.html