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

＜２００４年版＞

平成１７年５月

(財)日本情報処理開発協会

はじめに

情報化の広がりに伴って、情報セキュリティ対策の不備による影響は個々の企業だけの問題に止まらず、相手企業や消費者などにも大きな影響を与えるものとなっている。企業あるいは組織が情報セキュリティを確保するためには、技術と運用面でバランスのとれた総合的なセキュリティ対策を実施する必要がある。特に組織全体のセキュリティ対策を実施するためには、情報セキュリティマネジメントシステム（ISMS）の構築が有効である。

このような観点から、平成 14 年に当協会より報告書「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」が発行された。その後、約 2 年半が経過し、ISMS を取り巻く国内外の状況は大きく変化した。特に、わが国の認証取得数は 2005 年３月現在 500 件を超え、世界各国との比較においても、その数字は突出している。また、2005 年 4 月の個人情報保護法の完全施行に伴い、企業等の組織による情報保護への関心も一層高まっている。このような背景を受け、ISMS に関する規格等のガイドラインが示すフレームワークを、いかにして日々の活動の中で実現していくのかが大きな課題となっている。

本報告書は、ISMS の構築やその実践に取り組んでいる組織に参考にしていただけるよう、海外の先進的な取り組みを紹介する。特に、欧米においてコーポレートガバナンスの重要性が指摘され、関連する法規制が整備されたことによる情報セキュリティマネジメントへの影響と関連性など、ISMS を取り巻く環境変化も視野にいれた形でまとめることとした。

本調査研究を実施するにあたり、ご協力頂いた富士ゼロックス㈱ビジネスイノベーション事業部に対し厚く御礼申し上げるとともに、本報告書が情報セキュリティマネジメントへの取り組みの一助となれば幸いである。

2005 年 5 月

財団法人　日本情報処理開発協会

KEIRIN この事業は、競輪の補助金を受けて実施したものです。

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　情報セキュリティマネジメントのための実践規範」と「BS7799-2　情報セキュリティマネジメントシステム仕様」に分かれ、BS7799-1 が国際規格である「ISO/IEC17799　情報技術‐情報セキュリティマネジメントのための実践規範」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)は、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、要求事項が書かれている。BS7799-2 は、1999 年に発行された後、2002 年に改訂された。また、これをベースにしてわが国では、2002 年に ISMS 適合性評価制度が確立された。同制度の認証基準は、2002 年に Ver.1.0 が発行され、2002 年の BS7799-2 の改訂を受けて、2003 年に Ver.2.0 が発行されている。

ISO/IEC 17799 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ある。ISO/IEC 17799 は、2000 年に発行された。なお、ISO/IEC 17799 は、2002 年に JIS X 5080 として国内規格化がなされている。

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。

わが国における ISMS 適合性評価制度と同様、この英国の認証制度をモデルにして、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。

また、ISO/IEC 17799 や BS 7799-2 等の規格は、現在も見直し作業が進められており、進化を続けている。ISO/IEC 関連の規格は、5 年ごとに見直されるのが通例であるが、ISO/IEC 17799 は、これをまたずに見直し作業が行われており、2005 年末までには改訂版が発行される見込みである。

ISO/IEC 17799 や BS 7799-2 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。また、近年、ISO/IEC17799 や BS7799-2 以外にも、情報セキュリティのマネジメントに関する規格やガイドラインが、さまざまな視点で開発されている。これらの中には、ISO/IEC17799 や BS7799-2 との関連性について記述しているものもある。ISMS（もしくは情報セキュリティマネジメント）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。表1に、2005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。

表 1 各国におけるISO/IEC17799及びBS7799-2の国内規格化

国名	ISO/IEC17799の国家規格化	BS7799-2の国家規格化
日本	○(JISX5080)	×
米国	×	×
カナダ	×	×
英国	○(BS7799-1)	○BS2299-2
ドイツ	×	×
オランダ	○(SPE 20003)	○(SPE 20003)
オーストラリア	○(AS/NZS ISO/IEC 17799:2001)	○(AS/NZS ISO/IEC 7799.2:2003)
ニュージーランド	○(AS/NZS ISO/IEC 17799:2001)	○(AS/NZS ISO/IEC 17799:2001)
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	○(SS ISO/IEC 17799:2001)	○(SS 627799.2:2003)
ノルウェー	○	○
イスラエル	○(SIISO17799)	×
デンマーク	×	×
ポーランド	×	×
ハンガリー	×	×
シンガポール	×	×
インド	○IS:15150:2002	

○：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を表2に示す。なお、これらの最新情報は、国際的民間組織である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ウェブサイト（http://www.xisec.com/）で公表している。

表 2　各国の BS7799 認証数

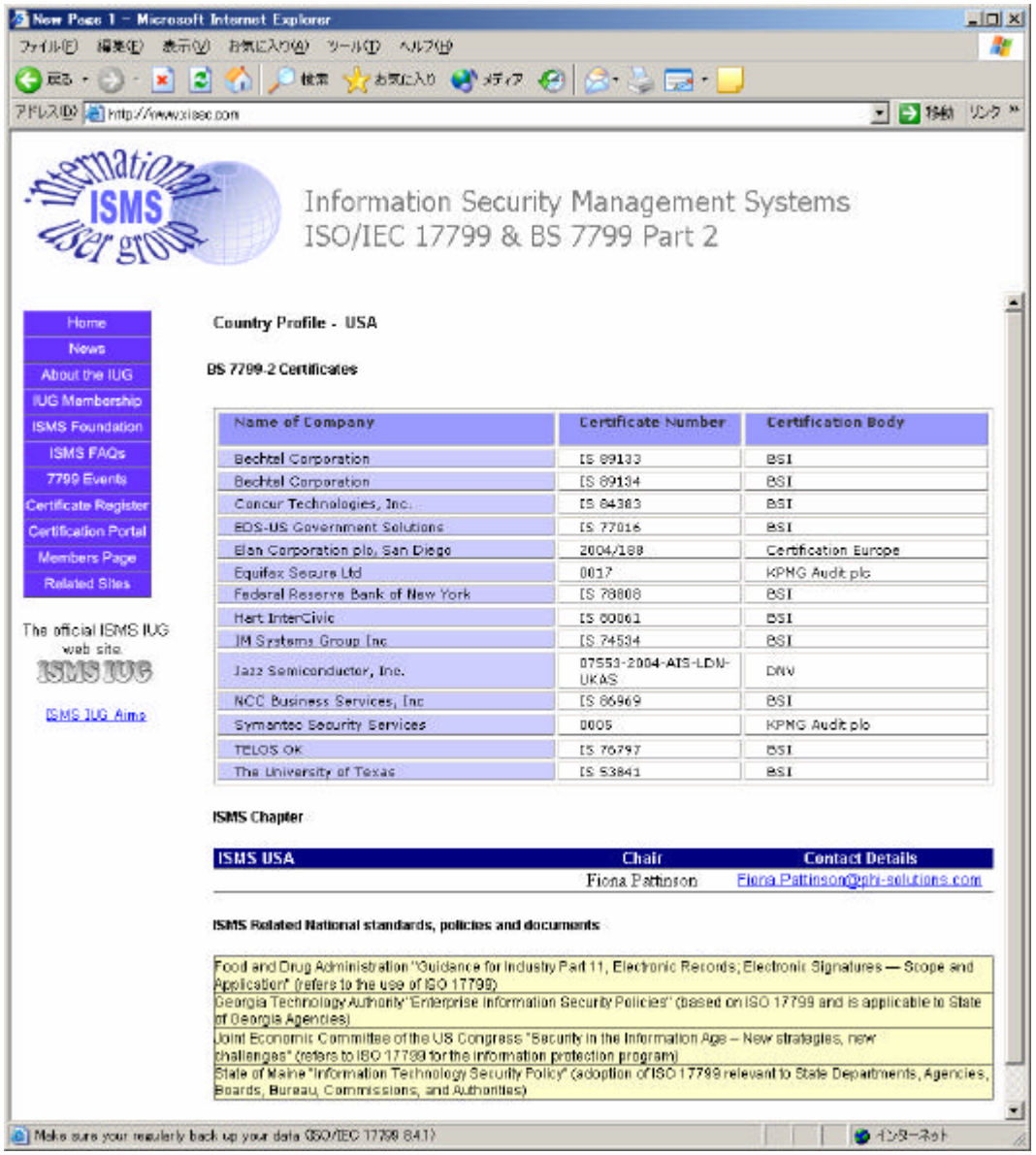
国名	認証数	国名	認証数	国名	認証数
日本	510	シンガポール	11	デンマーク	2
英国	185	ノルウェー	9	マン島	2
インド	82	スウェーデン	6	マレーシア	2
台湾	45	オーストリア	5	コロンビア	1
ドイツ	36	スイス	5	チェコ共和国	1
韓国	31	アイスランド	4	エジプト	1
イタリア	23	ポーランド	4	レバノン	1
オランダ	18	ブラジル	3	ルクセンブルク	1
香港	17	ギリシャ	3	マカオ	1
米国	15	メキシコ	3	マケドニア	1
フィンランド	12	サウジアラビア	3	モロッコ	1
オーストラリア	11	スペイン	3	カタール	1
中国	11	アラブ首長国連邦	3	スロバキア	1
ハンガリー	11	アルゼンチン	2	スロベニア	1
アイルランド	11	ベルギー	2	南アフリカ	1
				合計	1102

*2005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/

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最新情報は、国際的民間組織である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ウェブサイト（http://www.xisec.com/）で公表している（図１）。

図 1　認証取得企業(事業所)名の一覧（米国の例）



（出典：http://www.xisec.com）

1.5　世界の認証機関

世界の認証機関の最新情報は、国際的民間組織である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ウェブサイト（http://www.xisec.com/）で公表しており、2005年3月現在36の機関が認証業務を行っている(表 3)。

表 3　世界の認証機関

認証機関名
BM TRADA CERTIFICATION LIMITED
BSI
BVQI (Bureau Veritas Quality International)
Certification Europe
CIS (Austria)
DNV (Det Norske Veritas)
DQS GmbH (Germany)
DS Certification
JACO-IS (Japanese Audit and Certification Organisation)
JICQA
JMAQA
JQA (Japanese Quality Assurance)
JSA
JUSE-ISO Center
KEMA Quality BV
KPMG Audit plc
KPMG Certification
KPMG RJ
KPMG SA
LRQA
National Quality Assurance
Nemko (Norway)
PSB Certification (Singapore)
RINA S.p.A. (Italy)
RWTUEV Systems GmbH (Germany)
SAI Global Limited (Australia)

SEMKO-DEKRA Certification AB
SFS-Inspecta Certification (Finland)
SGS ICS Limited
SQS (Swiss Quality System)
STQC IT Certification Services (India)
Teknologisk institutt Sertifisering AS (Norway)
TÜV Rheinland Group (Germany)
TÜV SÜD Gruppe (TÜV Management Service GmbH) (Germany)
UIMCert (Germany)
United Registrar of Systems Limited

（出典：http://www.xisec.com/）

1.6 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 関連の報告書を作成する。

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、2002 年９月に改訂版が発行された。BS7799-2 の改訂版が、ISO 規格として提案され国際規格化されるかどうかについては、今後の動向を見守る必要があるが、BS7799-2 に基づく認証取得が世界規模で普及しており、デファクト・グローバル・スタンダードとなりつつある現状から、ISO 化に賛成する国が増加している。

IUG の活動は、インターネット上のウェブサイト（http://www.xisec.co.uk/）で公開されている。

日本 ISMSユーザグループ（J-ISMS UG）

2004 年 7 月に、IUG への窓口としての役割を果たす日本 ISMS ユーザグループが設立された。同グループの設立及び活動に関しては、経済産業省、財団法人　日本情報処理開発協会（JIPDEC）が支援しており、以下の活動を行う予定である。

（１） 会員に向けて、ISMS 構築、運用等に関わる国内外の標準化情報、経験情報を迅速に日本語で提供します。本情報提供のために J-ISMS UG 専用のポータルサイトを立ち上げます。

（２） ISMS 構築、運用に関わる課題、問題点について、広く意見交換・議論ができる場を提供します。定期的に研究会やセミナーなどを開催し、会員の抱えている問題点などの解決に向け、情報交換を進めます。

（３） 会員間の意見交換の結果、ユーザの視点から必要と考えられる意見をまとめ、ISO（国際標準化機構）などの ISMS に関する国際標準化活動の場へ提言します。

（出典：http://www.j-isms.jp/pdf/release040729.pdf）

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、国際規格 ISO/IEC17799 になった。現在、JTC1/SC27 で開発中の規格は、表４のようになっている。

表 4　JTC1/SC27 の TC で開発中の規格

規格番号	規格名称
ISO/IEC FCD 9796-3	Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms
ISO/IEC FDIS 9798-6	Information technology -- Security techniques -- Entity authentication -- Part 6: Mechanisms using manual data transfer
ISO/IEC FCD 10116	Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
ISO/IEC FCD 11770-4	Information technology -- Security techniques -- Key management -- Part 4: Key establishment mechanisms based on weak secrets
ISO/IEC WD 13335-2	IT security techniques -- Management of information and communications technology security -- Part 2: Techniques for information and communications technology security risk management
ISO/IEC FCD 15408-1	IT Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
ISO/IEC FCD 15408-2	IT Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements
ISO/IEC FCD 15408-3	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements
ISO/IEC DTR 15443-2	Information technology -- Security techniques -- A framework for IT security assurance -- Part 2: Assurance methods
ISO/IEC WD TR 15443-3	Information technology -- Security techniques -- A framework for IT security assurance -- Part 3: Analysis of assurance methods
ISO/IEC FDIS 17799	**Information technology -- Security techniques -- Code of practice for information security management**
ISO/IEC WD 18028-1	Information technology -- Security techniques -- IT network security
ISO/IEC FCD 18028-2	Information technology -- Security techniques -- IT network security -- Part 2: Network security architecture
ISO/IEC FCD 18028-3	IT security techniques -- IT network security -- Part 3: Securing communications between networks using security gateways
ISO/IEC 18028-4	Information technology -- Security techniques -- IT network security -- Part 4: Securing remote access
ISO/IEC CD 18028-5	Information technology -- Security techniques -- IT network security -- Part 5: Securing communications across networks using Virtual Private Networks
ISO/IEC FCD 18031	Information technology -- Random number generation
ISO/IEC FCD 18033-2.2	Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers
ISO/IEC FDIS 18033-3	Information technology -- Security techniques -- Encryption

	algorithms -- Part 3: Block ciphers
ISO/IEC FDIS 18033-4	Information technology -- Security techniques -- Encryption algorithms -- Part 4: Stream ciphers
ISO/IEC NP 18043	Information technology -- Deployment and operation of Intrusion Detection Systems
ISO/IEC FCD 18045	Information technology -- Security techniques -- Methodology for IT Security Evaluation
ISO/IEC FCD 19790	Information technology -- Security techniques -- Security requirements for cryptographic modules
ISO/IEC CD TR 19791	Information technology -- Security techniques -- Security assessment of operational systems
ISO/IEC WD 19792	Information technology -- Security techniques -- Framework for Security Evaluation and Testing of Biometric Technology
ISO/IEC NP 24742	Information technology -- Information security management metrics and measurements
ISO/IEC FCD 24743	Information technology -- Security techniques -- Information security management systems requirements specification
ISO/IEC NP 24745	Information technology -- Biometric template protection

(http://www.iso.org/iso/en/CatalogueListPage.CatalogueList?COMMID=143&scopelist=PROGRAMME)

- FCD･･･Final Committee Draft(最終委員会原案)
- FDIS･･･Final Draft International Standards（最終国際規格案）
- WD･･･Working Draft（規格原案）
- DTR･･･技術報告書原案（Draft Technical Report）:
- TR･･･技術報告書（Technical Report）:
- CD･･･委員会原案（Committee Draft）

JTC1/SC27の情報は､以下のインターネット上のウェブサイトで見ることができる。

http://www.jtc1.org/FTP/Public/JTC1/DOCREG/BerlinPresentations/SC27BerlinPresentation.ppt

なお、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

1.7 Metrics＆Measurement（M&M）

ISO/IEC17799 や BS7799-2 を開発し、改訂などの作業を続けている ISO の担当部署である JTC1 SC27 では、いくつかの新作業項目（NP）への取り組みを始めている（開発中の作業項目の一覧は、表４　JTC 1/SC 27 の TC で開発中の規格を参照）。その中でも 2004 年 10 月に NP になった、「NP24742　Information Security Management Metrics and Measurement(Oct 2004)」(以下、M&M と呼ぶ)は、ISMS のマネジメント・レベルを図る方法を提示する規格につながる重要な作業項目である。M&M は、今後 SC27 の会合で審議される予定である。

M&M の課題

M&M の目的は、ISMS 実施の効果とパフォーマンスを図ることにある。そのためには、以下のような課題がある。

- パフォーマンスをどのような項目で規定するか
- 何を計測するか
- どう計測するか
- 何時、計測するか　等

M&M の内容

まず記録を取る必要がある。以下のような例が上げられる。

- アンチウィルスのログ
- 従業員の作業報告書
- 利用者訓練の証拠
- インシデントの記録　等

M&M の計測

セキュリティ管理策の効果、効率、もしくは成熟度を評価するのに有用な数値データには以下のようなものがあげられる。

- アンチウィルス・ツールのための予算
- セキュリティの訓練を受けた従業員
- ウィルス障害から回復するのに要した時間
- アンチウィルスにより保護された機器
- 不正なコードによりサービスが提供できなかった時間

- 報告されたインシデント数
- 昨年ウィルスが原因で起こったインシデントのコスト
- アンチウィルスにより止められた攻撃
- フィルタリングされた電子メール
- 世界規模で出現した新種のウィルス　等

このような計測指標については、米国の NIST、カーネギーメロン大学が開発した SSE-CMM(Systems Security Engineer-Capability Maturity Model)、ISO/IEC15939 Software Measurement Process、ISO14030 Environmental Performance Evaluation など、既存のさまざまな手法が参考となるであろう。

1.8　まとめ

世界の認証取得数に基づく考察

2005 年 3 月時点で、世界全体で認証を取得している企業(事業所)は、1000 件を超えている。その内約半数が日本における認証取得であり、その数字は突出している。4 年前の調査結果と同様、インド、台湾、韓国、中国、シンガポールなどのアジア諸国による認証取得数が多い。日本を含むアジア圏で認証取得が多い理由としては、政策展開による推進活動が積極的に行われており、また産業界もそれを受けて積極的に推進していることが指摘できる。

一方で、香港や米国のように産業界における認知度の向上とマーケティング上のメリットなどから認証取得が徐々に伸びてきている国もある。

認証取得の動機の分析

近年の認証取得の動機を分析すると以下にまとめられる。

1　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する。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。

2　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、認証を取得する。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

調査は、政府関係者、コンサルタント、企業等の情報セキュリティマネージャーなどに対する電子メールを使用したアンケートとヒアリングにより実施した。なお、認証取得数や認証取得事業所名は、IUGのホームページを参照した。また、特に今回の調査では、米国における取り組みに重点を置いた。

2.1　スウェーデン

- スウェーデンでは、SWEDAC（Swedish Board for Accreditation and Conformity Assessment）が認証機関を認定している。
- SWEDACは、2005年3月時点でDNV Certification 、SEMKO-DEKRA、SFS-Inspecta Certificationの3つの認証機関を認定している。
- スウェーデン国内での認証取得数は、調査時点で6件である。

表 5　スウェーデンにおける認証（SAI Globalによる認証）

組織名	認証番号	認証の種類
ABB Facilities Management AB	0001-2000-AIS-SKM-SWEDAC	DNV
C2 Management AB	0002-2000-AIS-SKM-SWEDAC	DNV
GESAB Engineering AB publ.	0003-2001-AIS-SKM-SWEDAC	DNV
Posten Sverige AB Corporate Security Group	32638	BVQI
Primärvården Falkenberg, Falkenberg, Slöinge, Ullared and Vessigebro	120004	SEMKO-DEKRA Certification AB
TietoEnator Oyj, Processing and Networks	1930-06	SFS-Inspecta Certification

（出典：http://www.xisec.com/sweden.htm）

- SEMKO-DEKRAは、2005年1月19日に認定されたばかりで、調査時点での認証取得数は1件であった。
- スウェーデンでは、BS7799-2は国家規格化され、SS 62 77 99.2:2003と

なっている。また、ISO/IEC17799 は SS ISO/IEC 17799:2001 である。

- 認証制度は、国際的でありヨーロッパ域内で合意されたものに基づいて構築された。認証制度の基盤は、EN45012 及び EA-7/03 ガイドである。

- SWEDAC の ISMS 関連の URL：
  http://www.swedac.se/sdd/System.nsf/(GUIview)/index_eng.html

2.2 ポーランド

- ポーランドでは、BS7799:-2:2002 の採用が公表されるのを待っているところである。
- したがって、オフィシャルな形での認定制度はまだ確立されていない。
- しかしながら、近い将来採用が公表されることを前提として、いくつかの準備が進められている。すでに、ひとつの認証機関が申請をする運びとなっており、国内での認定に向けての作業が進められている。
- 認定機関として Polish Accreditation Centre (Polskie Centrum Akredytacji - PCA)が設置されている。PCA は、政府のエージェンシーで、マネジメントシステムを含むあらゆる認定制度について責任を有している。
- 調査時点では、国際的に認証ビジネスを展開している DNV と KEMA の 2 認証機関のポーランド支店が、認証業務をポーランド国内で行っている。
- ポーランド国内での認証取得は 4 件である。

表 6 ポーランドにおける認証

組織名	認証番号	認証の種類
Doradztwo Gospodarcze DGA S.A	07507-2003-AI-LDN-UKAS	DNV
LUMENA Sp. z o.o.	07541-2004-AIS-LDN-UKAS	DNV
Pern Przyjazn, Plock		KEMA Quality BV
The Office of the Polish Securities & Exchange Commission	07532-2004-AIS-LDN-UKAS	DNV

（出典：http://www.xisec.com/poland.htm）

- ISO/IEC17799 は、2003 年に国内規格化されており、規格番号は PN-I-17799 である。
- 現在、BS7799-2 の国内規格化の作業が進められており、その作業が終了し PN-I-07799-2 の出版を待っているところである。
- ISO/IEC13335 の part1～3 をすでに国内規格化しており、規格番号は PN-1-13335-1～3 である。

- 給与支払い機関に関する EU 規則に、ISO/IEC17799 を参照しているものがある。ポーランド国内でも関係があるが、ポーランドの法律で直接 ISO/IEC17799 や BS7799-2 を参照しているものはない。
- ISMS の市場は、今まさに出現しつつあるという状況である。ポーランド企業における情報セキュリティのアウェアネスは低いが、近い将来成長すると思われる。最も重要な要素は、ポーランド企業ならびにポーランド国内で活動する外国企業に影響を与えるような競争とグローバリゼーションの成長である。
- ISMS に興味を持っている産業は、IT 企業である。特に、銀行などに対してアウトソーシング・サービスを提供することに特化している企業の関心が高い。IT コンサルティング企業も同様である。
- ISMS は、常にそうであるというわけではないが、QMS の導入に専門性を有する人たちによって適用された方法にかなり影響を受けている。
- 普及啓発のために、多くのセミナーやコンファレンス、巡回興行を主催したり参加している。
- 現状での主な障害は、英国の規格に基づいて行わなければならないことである（文書を 2 カ国で準備し、外国人の監査人に認証を受けなければならない）。英国の規格をベースとした国際標準を採用するという認識は、広く普及させるためには最も良い方法であるが、BS7799-2:2002 をポーランド標準として採用すれば、この問題の大半は解決すると思われる。
- IT コンサルタント企業、政府のエージェンシー、自動車工場などで ISMS の導入に成功した事例がある。
- ISMS は、組織の種類や大きさに係らず、導入できる最初の役に立つアプローチとして有効だと考える。

PCA の URL：www.pca.gov.pl

2.3 香港

- 香港には、認定機関は存在しない。
- 認証機関は、海外の認定機関により認定され活動している。香港における認証取得数は、17件である。

表 7 香港における認証

組織名	認証番号	認証の種類
Cascade Ltd Netvigator Internet Service Operation Center (i-Center)	IS 79908	BSI
Cascade Ltd. (e.Center)	IS 77647	BSI
CLP Power Hong Kong Ltd, Information Technology Business Group	IS 77670	BSI
Doctor A Security Systems (HK) Ltd	IS 75486	BSI
e-Cop.net Ltd	ISMS-2002-0005	PSB Certification
Fugro Technical Services Limited	07509-2003-AIS-LDN-UKAS	DNV
GIPS LTD	07510-2004-AI-ROT-UKAS	DNV
Hong Kong Cyberport Management Company Ltd	IS 79189	BSI
Hutchison GlobalCenter Ltd	31927	BVQI
NEC Hong Kong Ltd, Business Solutions and Service	IS 77654	BSI
PCCW Unihub Ltd HK	IS 67432	BSI
PCCW Powerbase Data Center Services	IS 66182	BSI
Singapore Telecom Hong Kong Limited	ISMS-2003-0009	PSB Certification
Technic Employment Service Centre Ltd.	07575-2004-AI-LDN-UKAS	DNV
TQM Consultants Ltd	IS 57846	BSI
Tseung Kwan O Hospital, Department of Radiology	IS 80265	BSI
Vhsoft Technologies Co. Ltd	02015-2001-AIS-LDN-UKAS	DNV

（出典：http://www.xisec.com/hong%20kong.htm）

- 現在、香港で認証業務を行っている機関は、BSI、PSB Certification、DNV、BVQIの4機関である。
- それぞれの認証数は、表8のとおりである。

表 8　香港の認証機関と認証数

認証機関名	認証数
BSI	10
PSB Certification	2
DNV	2
BVQI	1
計	15

- 認証活動は、他国の制度を活用する形で行われている。香港では、政府は非常に無干渉であり、企業は自力で認証を取得する方法を模索しなければならない状況である。
- ISO/IEC17799 の国内規格化はなされておらず、その予定もない。
- BS7799-2 の国内規格化はなされておらず、その予定もない。
- ISO/IEC17799、もしくは BS7799-2 に変わるような規格はない。
- 法規制において、ISO/IEC17799 もしくは BS7799-2 を参照しているものはない。
- 主に、商業組織により鼓舞される形で認証取得へと進んだ産業界のリーダー的企業が、ここの組織やさまざまな産業セクターの関心を高めているというのが現状である。
- 中央政府による、この分野のセントラリゼーションやコントロールといった動きはない。
- 現時点で ISMS 認証に興味を持っている業界としては、ISP や Data Center ビジネスなどに進出している通信会社が上げられる。公的に提供するサービスのセキュリティを産業として推進している。
- 認証取得数は、かなり安定基盤にのってきた。このことは、発行された認証取得数の増加率が失速していることからも伺える。
- ISMS の認知度向上に関しては、2 日間のセキュリティコンファレンスやさまざまな組織によるセキュリティイベントなどが開催されていることがあげられる。
- 香港では、一つ一つの組織による取り組みを通して普及しているため、そのスピードはかなり遅く、いまだ産業界のリーダーが取り組んでいるだけという状況である。
- ISMS を普及させるモチベーションとしては、競争の激化が考えられる。

企業が、「認証を取得しなければビジネスを失う」という考え方をするようになれば普及すると考える。

2.4 オーストラリア

- オーストラリアの認定機関は、JAS・ANZ（Joint Accreditation System of Australia and New Zealand）である。
- 2005年3月時点で、JAS・ANZにより認定された認証機関は、SAI Global（SAI Global Certification services Pty Ltd.Trading as SAI Global）のみである。
- オーストラリアにおける認証取得数（SAI Globalによる認証）は、13件である。

表 9 オーストラリアにおける認証（SAI Globalによる認証）

組織名	認証番号	認証の種類
(ICAC)	ISM20003	AS/NZS 7799.2:2000
ANZ Banking Group Ltd t/a	ISM00001	AS/NZS 7799.2:2000
Bridge Point Communications Pty Ltd	ISM20009	AS/NZS 7799.2:2000
Central Corporate Services Unit	ISM20017	AS/NZS 7799.2:2003
CITEC	ISM20011	AS/NZS 7799.2:2003
Fujitsu Aust Ltd & Fujitsu N.Z. Ltd	ISM00002	AS/NZS 7799.2:2003
Independent Pricing & Regulatory Tribuna	ISM20002	AS/NZS 7799.2:2000
Justice Technology Services	ISM20018	AS/NZS 7799.2:2003
NEC Business Solutions Ltd	ISM20029	AS/NZS 7799.2:2003
Office of the Ombudsman	ISM20007	AS/NZS 7799.2:2000
Request Broadband Pty Ltd	ISM20008	AS/NZS 7799.2:2003
Telstra Corporation Limited	ISM20016	AS/NZS 7799.2:2003
Yarra Valley Water Limited	ISM20014	AS/NZS 7799.2:2003

（出典：http://www.xisec.com/australia.htm）

- オーストラリアの認証制度は、EA/7-03に基づいて構築されている。
- ISO/IEC17799は、オーストラリアで国内規格化されている。規格番号は、AS/NZS ISO/IEC 17799:2001 (ISO/IEC Edition 2000)である。
- BS7799-2は、オーストラリアで国内規格化されている。規格番号は、

AS/NZS 7799.2:2003 (BS 7799.2:2002)である。

- ISO/IEC17799 ならびに BS7799-2 に関連する規格やガイドラインとして以下のものがある。
  - 情報セキュリティリスクマネジメントに関するオーストラリア規格：Handbook 231 (HB 231)
  - リスクマネジメントに関するオーストラリア規格：AS/NZS 4360:2004 及びそれに付随するハンドブック：Handbook 436 (HB 436)
- ほとんどの州政府は、内部の情報セキュリティマネジメントプログラムとして ISMS に高い興味を示している。**New South Wales 州では、全ての部署に認証取得を義務付けた。**
- 産業界においても興味は高い。多くの企業がこの規格をセキュリティ・プログラムの基盤として社内的に活用している。しかしながら、認証取得数は少ない。
- 規格の普及啓発は、5 年前から幅広い産業界や政府機関に対するプレゼンテーションを行うといった形で行われている。

- JASANZ の URL：
  http://www.jas-anz.com.au/showpage.php
- SAI Global の ISMS 関連の URL：
  http://www.saiglobal.com.au/assuranceservices/certification/InfoSecurityManagement
- オーストラリアにおける認証（SAI Global による認証）の詳細情報の URL:
  http://register.sai-global.com/SuppliersSearch.asp?firsttime=True

2.5 インド

- **インドでは、**Quality Council of India (QCI)**が現在認定のための制度を構築している途中である。したがって、現在インド国内で認定業務は行われていない。**
- **オランダの** RvA（Raad voor Accreditatie）**により認定された** STQC（Standardization Testing Quality Certification）**が、現在認証業務を行っている。インド国内での認証取得数は、**80 **件(情報公開している事業所のみ)である。**

表 10　インドにおける認証

組織名	認証番号	認証の種類
Accenture Services Private Limited	IS 87690	BSI
Accurum India Private Limited	IS 85437	BSI
AFL Pvt. Ltd. Logistics Division	07542-2004-AIS-LDN-UKAS	DNV
Arsin Systems Pvt. Ltd, Hyderabad	ISMS/04/1019	STQC IT Certification Services
BAeHAL Software Ltd	ISMS/03/1015	STQC IT Certification Services
Business Process Outsourcing (India) Private Limited, Bangalore	01 153 10001	TÜV Rheinland Group
Cable & Wireless (India)	07550-2004-AIS-LDN-UKAS	DNV
CAPGEMINI Consulting India PVT. Ltd.	IS 86507	BSI
Capita Mastek BPO Private Limited	IS 92564	BSI
Churchill India (P) Ltd, New Delhi	ISMS/01/1002	STQC IT Certification Services
Churchill India (P) Limited, Gurgaon	IS 87556	BSI
Cognizant Technology Solutions, Chennai, Kolkata, Hyderabad, Bangalore and Pune	ISMS/01/1006	STQC IT Certification Services
Computer Sciences Corporation, Noida	ISMS/04/1020	STQC IT Certification Services
Datamatic Technologies Ltd	ISMS/03/1014	STQC IT Certification Services
DSL Software Ltd., BPO Division	07504-2003-AIS-LDN-UKAS	DNV
eMR Technology Ventures Private Limited	IS 85013	BSI

Epicenter Technologies Pvt. Ltd.	IS 90090	BSI
exl Service.com (India) Private Limited, Noida	ISMS/04/1018	STQC IT Certification Services
Fortune Infotech Ltd	45	KPMG Audit plc
GAVS Information Services Private Limited	IS 83211	BSI
GE Capital International Services	07504-2004-AIS-LDN-UKAS	DNV
HCL Comnet Ltd	ISMS/01/1011	STQC IT Certification Services
HCL Technologies BPO Services Limited	IS 83208	BSI
HCL Technologies BPO Services Limited	IS 88970	BSI
HCL Techologies Limited - NTD	47	KPMG Audit plc
HCL Technologies Limited - BSC	48	KPMG Audit plc
HCL Technologies Limited - CTD	49	KPMG Audit plc
Hexaware Technologies Ltd	07503-2004-AIS-LDN-UKAS	DNV
HTMT	40	KPMG Audit plc
Hughes Software System, Gurgaon (Haryana)	ISMS/01/1004	STQC IT Certification Services
ICICI Bank Limited-Global Trade Services Unit(GTSU)	IS 89521	BSI
ICICI OneSource Limited	ISMS/03/1008	STQC IT Certification Services
iGate Global Solutions	8	KPMG Audit plc
Immaculate Interactions (India) Limited	IS 81026	BSI
Infosys Technologies Ltd.	07516-2004-AIS-LDN-UKAS	DNV
Infotech Enterprises Ltd, Hyderabad and Bangalore	141669	BVQI
Integral Media Services India Private Limited	IS 89519	BSI
ITC Infotech India Limited	IS 85445	BSI
IVY Comptech Pvt. Ltd., Technology Division	IS 91899	BSI
IVY Computech Private Limited	IS 87796	BSI
Larsen & Toubro Ltd, Engneering and construction division, Mumbai and Vadodara	ISMS/01/1001	STQC IT Certification Services
L & T Infotech	43	KPMG Audit plc
Mphasis BFL Ltd	ISMS/03/1012	STQC IT Certification Services
M/s Bechtel India Pvt. Ltd	07551-2004-AIS-LDN-UKAS	DNV
MsourcE India Pvt Ltd	ISMS/03/1010	STQC IT Certification Services

Mumbai Police Call Centre	IS 87715	BSI
Network Solutions Pvt Limited	IS 84018	BSI
Patni Computer Systems Limited	46	KPMG Audit plc
P & O Ports India Pvt Limited	IS 82277	BSI
Polaris Software Lab Ltd, Chennai	ISMS/04/1022	STQC IT Certification Services
PricewaterhouseCoopers Pvt Ltd	07506-2003-AIS-LDN-UKAS	DNV
Progeon Ltd	07517-2004-AIS-LDN-UKAS	DNV
Rapidigm (India) Ltd.	07527-2004-AIS-LDN-UKAS	DNV
RelQ Software Pvt. Ltd.	2004/137	Certification Europe
Rolta India Ltd.	IS 91193	BSI
Sasken Communication Technologies Limited	IS 90155	BSI
Sasken Network Systems Limited	IS 90134	BSI
Satyam Computer Systems, Secundrabad	ISMS/01/1005	STQC IT Certification Services
SecureSynergy Private Limited	IS 88604	BSI
Shipara Technologies Ltd	ISMS/02/1007	STQC IT Certification Services
Siemens Shared Services, Bangalore	ISMS/02/1021	STQC IT Certification Services
SIFY Ltd	IS 81027	BSI
Sobha Renaissance IT Private Limited	IS 84145	BSI
Software Technology Parks of India, Noida	145477	BVQI
ST Microelectronics Ltd, Noida	ISMS/01/1003	STQC IT Certification Services
Syntel Ltd, Mumbai, Pune and Chennai	151503	BVQI
Tata Consultancy Services	07508-2003-AIS-LDN-UKAS	DNV
Tata Iron and Steel Company Ltd	ISMS/03/1009	STQC IT Certification Services
Tata Technologies Ltd	07552-2004-AIS-LDN-UKAS	DNV
Technovate eSolutions Private Ltd, New Delhi	4.47	BVQI
Telesource Management Consulting Pvt Ltd.	IS 86879	BSI
Tricom Information & Technology Lim	IS 89652	BSI
Vanguard Info-Solution Ltd.	IS 91590	BSI
Vinciti Networks Private Limited	IS 84140	BSI
vMoksha Technologies Private Ltd	IS 79064	BSI
Wipro Ltd – 01 Markets	ISMS/03/1016	STQC IT Certification Services

Wipro Technologies	02186-2002-AIS-ROT-UKAS	DNV
WNS Global Services Private Limited	IS 87746	BSI
Xansa India Ltd	02072-2002-AIS-LND-UKAS	DNV
Xerox Modicorp Ltd, Software Services Division	ISMS/03/1013	STQC IT Certification Services

（出典：http://www.xisec.com/india.htm）

- DNV, BSI, KPMG などもインド国内の組織に対して認証を行っており、全体で 50 件を超える認証が取得されている。
- ISO/IEC17799 は国内規格化され、その規格番号は IS 15150 である。
- BS7799-2 は、国内規格化されていない。
- ISO/IEC17799 ならびに、BS7799-2 に類似した規格やガイドラインは特にない。
- IPR、Cyber Security、digital signatures などについての法規制である Indian IT Act 2000 が施行されているが、ISO/IEC17799 や BS7799-2 は参照していない。
- 情報や情報資産が保護されているという信頼感をあたえるために、BS7799-2 の認証取得の達成は重要なことであると認識されている。
- 普及啓発のために、BS7799-2 のアウェアネス・プログラムを定期的に展開するなどの施策を実施している。すでにその結果は、認証取得数という形で現れている(現在でも 5 件の認証業務が進行中である)。
- 情報は資産であり、機密性、真正性、可用性を確保することは最大の要求事項である。ISMS は、今日コンピュータを活用するあらゆるビジネスにとって欠かすことのできないものであると認識している。

- QCI の URL：http://www.qcin.org/
- STQC の URL：http://www.stqc.nic.in/

2.6 米国

- **米国の公的機関では、**BS7799-2 **をベースとした認証制度の確立や普及支援は行っていない。**NIST **により推進されているのは、連邦システムのための規格作りと推進策である。産業界は、これらの選択肢から個々の組織の判断により適切な規格やガイドラインを参照するというアプローチになっている。**
- ISMS **のための規格、**BS7799-2 **のための認定機関というものは米国には存在しない。**
- NIST **により開発された連邦システムのための国家規格に関する活動は行われている。**
  - NIST **の制度では、**「NIST Special Publication 800-37; Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004」**を規定しており、これに基づいて認証制度が運用されている。**
- BS7799-2 **に基づく認証取得数は、約** 12 **件である。**

表 11 米国における認証

組織名	認証番号	認証の種類
Bechtel Corporation	IS 89133	BSI
Bechtel Corporation	IS 89134	BSI
Concur Technologies, Inc.	IS 84383	BSI
EDS-US Government Solutions	IS 77016	BSI
Elan Corporation plc, San Diego	2004/188	Certification Europe
Equifax Secure Ltd	17	KPMG Audit plc
Federal Reserve Bank of New York	IS 78808	BSI
Hart InterCivic	IS 80061	BSI
IM Systems Group Inc	IS 74534	BSI
Jazz Semiconductor, Inc.	07553-2004-AIS-LDN-UKAS	DNV
NCC Business Services, Inc	IS 86969	BSI
Symantec Security Services	5	KPMG Audit plc

（出典：http://www.xisec.com/USA.htm）

- **認定機関としては、**ISO9001 **等の米国認定機関** ANAB**（正式名** ANSI-ASQ

National Accreditation Board[1]）がある。

- ISO/IEC17799 は、コントロール・リスト（管理策の一覧）に関する国際標準であり、米国で採用されているという認識である。
- 連邦システムのために使われるコントロール・リストは、NIST SP 800-53 にまとめられている。
-

Recommended Security Controls for Federal Information Systems, February 2005

Annex 1: Consolidated Security Controls-Low Baseline

Annex 2: Consolidated Security Controls-Moderate Baseline

Annex 3: Consolidated Security Controls-High Baseline

- BS7799-2 に基づく認証制度に関する検討については、同規格の国際規格化を待っている状況である。
- サーベインス･オックスレイ法は、内部のコントロールに関する要求事項を有しているが、特定の規格について言及しているわけではない。
- 認証を取得している企業の傾向を見ると、ほとんどがグローバル企業である。このようなグローバル企業では、業務遂行上、全体の調和を図ることができ、国際的に認知されている規格である BS7799-2 を選択しているものと思われる。
- ISMS の普及活動などに、公的支援はなされてはいない。関係者間で ISMS 関連の情報を交換するメーリング･リストなどは持っている。
- 普及については、米国は広大な国であり、急速な推進は難しいと考えている。
- 米国企業が、ISO/IEC17799 や BS7799-2 を積極的に採用していくような動きは現状では見られない。その理由として、米国企業にとってこの他にも実施しなければならないことが多くあり、そちらのほうが優先順位が高いということが上げられる。また、これらの規格を参照することで、市場におけるメリットを享受できるとは今のところ見受けられない。2～3 年の間は、大きな変化は見られないであろう。
- 米国企業が BS7799-2 の認証を取得する目的は、主に“証明してもらう”ことにある。特に、サービスを提供している場合などは、顧客の要求事項を全て満たしていることをひとつずつ示す代わりに、認証取得の証明書を

[1] ANAB は、RAB(正式名 ANSI-RAB National Accreditation Program)が 2005 年 1 月 1 日に組織改変とともに、改名したもの。

見せることで代替できるというメリットがある。

- 認証取得理由をまとめると以下のようになる。
  - 情報セキュリティの効果の改善
  - 市場での差別化
  - 顧客の要求事項の満足
  - 新しい/既存の顧客及びビジネス･パートナーの信頼に対するインパクト
  - 世界的規模で普及している唯一の規格であること
  - 保険料率が低くなる可能性
  - スタッフの責任の明確化
  - 規格が IT と同様に、組織、人、施設もカバーしていること
  - 法規制対応（HIPAA, Privacy Act of 1974, Computer Security Act of 1987, National Infrastructure Act of 1996, Gramm-Leach-Bliley Act of 1999 , Government Information Security Reform Act of 2001 など）
- 米国企業が認証取得に向けて努力しているといった傾向は見られないが、投資家たちの満足度を維持・向上させ、自社の社会的信用を失墜させないように、事故を未然に防ぐことに注力している。
- 米国企業は現在、HIPAA, Sarbanes-Oxley Act, Safe Harbor, California privacy Law, or the Common Criteria など、延々と続く法規制に準拠するため、かなりのプレッシャーを受けている。問題として、このような政府の規制は企業に係わってくるものであるが、ほとんどの企業では法規制要求事項に対応できる準備ができておらず、導入するためだけに非常に多くの努力をしなければならない。これらの法規制に対して、継続的に監査されることによって準拠するための時間と資金を投入している。監査と認証に係る努力にもまた、時間、資金、人手を要し、その他のプロアクティブな計画を立て展開することができなくなっている。現在、ほとんどの企業は、直近の米国政府の要求事項に対応することに追われているというのが現状である。
- このような新しい規制が一段落した後には、数年の間、レビュー・プロセスと実践が繰り返され、米国企業はリラックスしてより賢くよりプロアクティブにこれらを実践する方法を見出すことになるであろう。
- ISMS は、このような規制を全て満足するために参考になるであろうし、支援するものであると考えられる。しかしながら、ほとんどの企業はそれ

程プロアクティブではない。ある企業では、5 年以上前からモデル・セキュリティ・コンプライアンス・プログラムを持ち運用している。他の企業もまた、同様のセキュリティ・コンプライアンス・プログラムを持っている。しかしながら、そういったプログラムは ISMS とは呼ばず、認証についても取得しようとしないだけである。確立されたセキュリティ・コンプライアンス・プログラムを有する企業でさえ、これらの(新しい)法的要求事項に対応するために多くの資金が注ぎ込まれている。もし、ISMS を持っていたならば、どれほどより賢く、より早い方法で政府の規制に準拠できたかを後になって気づくことになるであろう。

- 米国で認証取得が増えない理由のひとつは、それがまだ英国規格 BS7799-2 をベースにしていることがあげられる。将来的に、BS7799-2 が国際規格になった場合、認定機関である ANAB が ISMS の認定制度を確立し、展開することになると予想される。この際には、米国における需要の扉が開かれ、一気に認証取得が普及し始める可能性がある。
- 認証取得が進まないもうひとつの障害は、米国では法規制においてセキュリティ・マネジメント・システムを持つことを義務付け、そしてそのシステムが BS7799-2 に基づく認証取得を要件とすることを言及しているものがないことである。
- 普及を促す要素としては、国際企業が特定の市場や特定の地域でビジネスを展開するために認証を取得するように要求されるということが考えられる。
- ISO 9000 では、認証を取得することにより、何らかの財務上の利益が得られるということが明確になるまで、その普及の速度は非常に遅かった。現時点では、BS7799-2 の認証を取得することに関して、財務上のインセンティブというものがない。これが、米国企業において認証取得が進まないもうひとつの理由である。
- ただし、サービス･プロバイダー事業を展開している企業や国際的な要求を受けている企業については、認証取得のインセンティブがある。
- ひとつの企業内でも、認証を取得することにより顧客の要求事項を満足していることを他社に先駆けて証明でき、競争に勝つことができるビジネスを展開しているセクションでは、認証を取得する財務上のインセンティブが働いているが、それ以外のセクションでは働かないといった違いがある。
- また、ISO15408(Common Criteria)のように政府などの調達基準として採用された場合は、シェアを伸ばしたり現状のシェアを確保するために認

証を取得するといったインセンティブが働くであろう。

- BS7799-2 が、セキュリティ・コンプライアンスを確かなものにするというのは自明であるが、認証取得をすることにより財務上の利益が確保できるということが明確にならない限り、時間と努力を投入し認証取得に取り組むというインセンティブは働かない。むしろ、目の前に迫っている法規制への準拠を続けるというのが現実的である。
- 米国企業は、現在、市場シェア・収益・株主の信頼を失うことがないように、Safe-Harbor や Sarbanes Oxley 及びその他の法規制に準拠しようと努力している。コンプライアンスの枠を超えた対応をするというのは、高くつきすぎるのである。ISO への準拠についての考え方と価値観は、それは企業経営にとって負担増となる販売促進を目的とした仕事として行われているという認識がある。
- BS7799-2 について、米国の情報セキュリティマネージャーの多くはその内容を知っており、必要に応じて参照しているが、認証取得はコストがかかりすぎると考えている。
- 情報セキュリティマネジメントの実践において参照している ISO/IEC17799 及び BS7799-2 以外の規格やガイドラインとして以下のものがあげられる。
  - ISF の Standard of Good Practice
  - COBIT （Control Objectives for Information and Related Technology）
  - NIST 規格
- 取引先などの管理をするためには、監査報告書を活用し、四半期ごとに特定のテーマについてのセルフ・レポートを各事業単位で作成するなどの方法で、ビジネス･ネットワーク全体の情報セキュリティマネジメントを行っている(独自に開発した管理手法を使用)。リスクアセスメント手法についても、独自に開発したものを使用している。管理策は、ISO/IEC17799 に記載されている管理策の約 75%程度を実践している。
- 情報化投資は、売上の 10%程度でそのうち約 4%が情報セキュリティ投資（ウィルスチェック、IP ネットワークセキュリティ、人件費等）である。
- 情報セキュリティ担当者の中で、技術系バックグラウンドを持つ人材の割合が約 3 分の 2、戦略系（マーケティングなどを含む）のバックグラウンドを持つ人材が約 3 分の 1 である。戦略系を担当する人材は、コーポレートフィロソフィーと情報セキュリティマネジメント活動をつなぐ業務を

遂行しており、非常に重要な役割を担っている。実践は、個々の部署の管理職を調整役として展開している。根気強くこれらの管理職における情報セキュリティ・アウェアネスを高めたことにより、情報セキュリティ実践の必要性についての共感を得ることができるようになった。これには数年を費やした。また、このことにより、近年は情報セキュリティ予算の確保にもそれ程苦労することがなくなった。

- 多くの米国企業では、ISO/IE C17799 を自社のセキュリティ対策レベルを図る物差として利用している。一方、BS7799-2 が要求するマネジメントシステム、すなわち管理の方法については、それが法規制にならない限り普及するのは難しいであろう。また、政策の監督よりも独自性（クリエイティビティ）を好むという米国企業の管理職における傾向も普及を遅らせていると思われる。
- 米国におけるある調査によると、1990 年代情報化投資は売上の約 1%程度であった。その情報化投資のうち、約 0.5%が情報セキュリティ投資であった。2005 年では、情報化投資が約 23%、情報セキュリティ投資は、5～15%にまで上昇している。このように、情報化投資及び情報セキュリティ投資の売上にしめる割合が高くなったため、経営層は ROI（投資効率）についての説明を CIO[2]や CISO[3]に求めるようになりつつある。その要求に対応するために、Metrics & Measurement の開発に取り組んでいるが未だ有効な手法は開発されていない。
- 情報セキュリティマネージャーのバックグラウンドについて、その歴史的な背景を追うと、1950 年代は IT の専門家という形で単一のカテゴリーであった。その後、役割がプログラミングとコンピュータ・オペレーティングに二分された。さらに、データベース、意思決定支援、トランザクション、ネットワーク、メインフレーム、デスクトップといった形で細分化された。1995 年頃からは、ウェブ・デザイナーという分野が生まれ、これらの人々の中から主にネットワーク、メインフレーム、デスクトップ、ウェブ・デザイナーといった人々が、個々の役割の業務の一部としてセキュリティに取り組み始めた。1999 年には、大学に情報セキュリティの専門課程が設置されるなどの影響もあり、コーポレート･(情報)セキュリティについてのグループといったものが設置されるようになり今日に至っている。

[2] CIO (chief information officer) IT 担当役員
[3] CISO: Chief Information Security Officer 企業内で情報セキュリティを統括する担当役員

- 米国で優先順位が高くなっている情報セキュリティ関連の政策は、大きく 3 つある。
  - 企業財務に係る問題
  - 個人情報保護に係る問題
  - 重要なインフラストラクチャーに係る問題
- 企業財務に係る問題は、非常に社会的インパクトが大きかったエンロンやワールドコムの不正及び倒産事件により成立したサーベインス･オックスレイ法（SOX 法）への対応である（SOX 法については、詳細を後述する）。
- 個人情報に係る法規制としては、ヘルスケア分野における HIPPA（Healthcare Insurance Portability and Accountability Act）がある。HIPPA は、カルテなどの医療情報を医療機関が適切に管理することを求めている。この法規制のセキュリティに関す規則は、2005 年 4 月 25 日に発効する。また、金融機関については、GLBA (Gramm-Leach-Bliley Act：グラム･リーチ･ブライリー法)が制定されている。GLBA 法は、銀行、証券会社、保険会社などの金融機関に課せられているもので、1999 年 11 月 12 日に成立した。金融機関は、この法律が求める顧客情報の保護に準拠しなければならない。
- 電力、石油、ガス、化学、鉄道などの重要なインフラストラクチャーについては、連邦政府のホームランド･セキュリティ政策において高い優先順位が付けられ、対策が推進されている。たとえば、石油及びガス分野では、2004 年 11 月 2 日に「A Comparison of Cyber Security Standards developed by the Oil and Gas Segment」が公表されている。この報告書では、「ISO/IEC17799」、「API1164」、「AGA Report No. 12 Draft 3 August 14, 2004」の 3 規格の内容が比較され、企業が適切な規格を参照できるようになっている。電力分野でも、2004 年 11 月 2 日に「A Comparison of Electrical Sector Cyber Security Standards and Guidelines」が公表されている。この報告書では、「ISO/IEC17799」、「IEEE1402」、「NERC Security Guideline for the Electricity Sector」、「NERC 1200」、「NERC1300 Draft 1.0 September 15, 2004」の 5 規格の内容が比較されている。たとえば、「IEEE1402」はより物理セキュリティに重点が置かれ、「NERC」は、サイバー・セキュリティに重点が置かれているといった違いが指摘されている。

NIST の URL：http://www.nist.gov/

- ANAB の URL：http://www.anab.org/
- ISF の Standard of Good Practice ：
  http://www.isfsecuritystandard.com/index_ie.htm
- 「A Comparison of Cyber Security Standards developed by the Oil and Gas Segment」の URL：
  http://csstc.inel.gov/pressroom/reports/comparing_oil_and_gas_sector_cyber_security_standards.pdf
- 「A Comparison of Electrical Sector Cyber Security Standards and Guidelines」：
  http://csstc.inel.gov/pressroom/reports/comparing_electric_utility_cyber_security_standards.pdf

2.7　まとめ

ISMS 認証取得数は 1,000 件を超えたが、その約半数は日本での認証取得であり、世界的なレベルで日本と同様の普及段階にあるとは言い難い。個々の国や地域で、それぞれ異なる普及段階にある。その中で、前回と同様にインドやシンガポールといった IT の振興に重点を置いた政策を展開している国々での認証取得数の増加がひとつの特徴と言える。3 年前の調査においてもその兆候は見られたが、現在の取得数と比較すると積極的なポリシー・イニシアチブが ISMS の普及を促していることがわかる。

一方で、欧州でもスウェーデンやポーランドなどで、認証スキームが着実に作られつつあるということも調査の結果明らかになった。

一方、今回の調査で重点を置いた米国では、その認証数が 14 件と未だ非常に少ない。ヒアリングによる調査で明らかになったのは、ISMS への認知度はかなり高いということである。CISO や情報セキュリティ担当者は、その内容についても精通しており、必要に応じて参照している。多くの企業では、申請すれば認証取得は難しくない状況にあると推測される。このような企業に対し、認証を取得している企業には、以下のような明確な動機があると思われる。

① 認証取得のインセンティブ―たとえばサービスビジネスを提供しており、顧客の信頼性を得るために第三者認証を取得するなど―がある
② グローバルなビジネス展開の中で、全体の調整をするために認証を取得する

認証は取得していないが、ISMS を活用している企業における規格の活用方法は、ISO/IEC17799 を管理策のベスト・プラクティスとして組織の現状とのギャップ分析に使うというものであった。一方、BS7799-2 が提示するマネジメント・サイクルについては、以前から実施していることであり、すでに独自の管理手法を作成し運用の中で自社に合った形に変えてきているという状況があった。

現在の米国企業の情報セキュリティ関係者の関心は、次々に施行される法制度への対応である。特に SOX 法は、直接的に経営層の責任が問われかねない要

求事項であり、高い優先順位で人手と費用を投入している。しかしながら、このように法制度対応に追われている現状に疑問を持っている CISO や情報セキュリティ担当者も少なくない。このような専門家たちは、将来的には ISMS が提示するプロセスを踏んで、自社の組織の実情にあった対策になっているかを見直す必要があると考えている。

3 ISMS に関連するその他の動き

3.1 ITIL

ITIL は、IT Infrastructure Library の略で IT サービス・マネジメントに関するベストプラクティスである。1980 年代に英国政府機関で開発が始まり、1989 年に初版が発行された。「IT サービス」は、「1 つまたは複数の事業領域をサポートする IT システムが提供する一組の関連する機能で、換言すればソフトウェア、ハードウェア、通信設備により構成されている [4]」と定義される。現在、ITIL は、ヒューレット・パッカード、IBM、マイクロソフトといった「IT サービス」を提供する組織に参照されている [5]。

ITIL 関連の組織

ITIL は、英国政府の中央コンピュータ技術庁により作成され、現在は OGC（Office of Government Commerce）が所有者となっている [6]。

また、itSMF（IT サービスマネジメントフォーラム）は、IT サービスマネジメントに関する国際的な会員制ユーザ・グループで ITIL の普及促進を行っている。なお、itSMF ジャパンは、2003 年 5 月に設立されている。

- itSMF ジャパンの URL: http://www.itsmf-japan.org/index.html

ITIL の概要

「IT サービスマネジメント－ITIL 入門」に以下のように記述されていることからわかるように、ITIL の内容を知るためにはそれを構成する書籍を見ていくのがわかりやすい。

[4] IT サービスマネジメント用語集、itSMF ジャパン、2003 年 3 月（日本版発行） pp. 43
[5] IT サービスマネジメント－ITIL 入門、itSMF、2004 年 7 月（日本語版発行）pp. 11
[6] 同上 pp. 31

『ITIL は元々、IT インフラストラクチャの保守、運用という特定分野について記述した書籍の集大成からなっていました。[7]』

ITIL 関連書籍は、以下の 7 冊で構成される。

1. サービスデリバリ
2. サービスサポート
3. セキュリティ管理
4. ICT インフラストラクチャ管理
5. アプリケーション管理
6. サービスマネジメント導入計画立案
7. 事業の展望

ITIL の示すフレームワークの中心は、「サービスデリバリ」と「サービスサポート」の２つである。この 2 つを合わせたものを「サービスマネジメント」と呼ぶ。

「サービスデリバリ」は、以下の内容を含んでいる。

- サービスレベル管理
- IT サービス財務管理
- キャパシティ管理
- IT サービス継続性管理
- 可用性管理

「サービスサポート」は、以下の内容を含んでいる。

- サービスデスク
- インシデント管理
- 問題管理
- 構成管理
- 変更管理
- リリース管理

[7] IT サービスマネジメント－ITIL 入門、itSMF、2004 年 7 月（日本語版発行）pp. 33

ITIL と ISMS

ITIL は、サービス・プロバイダのためのフレームワークを提供するものである。したがって、セキュリティ管理の基本は、顧客とのサービスレベルアグリーメント（SLA）におけるセキュリティ条項ということになる。顧客は、リスク分析を行い、セキュリティの要求事項を決める。最終的には、顧客とサービス・プロバイダの間で合意したセキュリティ条項が作られる。このセキュリティ条項の要件が、サービス･プロバイダが基本的に提供するセキュリティ（セキュリティ・ベースライン）よりも高いものを要求している場合は、サービスの提供において実現するセキュリティ対策を見直すことになる。

ITIL と ISMS の関係について、「IT サービスマネジメント－ITIL 入門」には以下のような記述がある。

> 「情報セキュリティ管理は、IT 組織におけるセキュリティをサービス・プロバイダの観点から統合したものです。情報セキュリティ管理実施基準（BS7799） は、セキュリティ対策の開発、導入、評価のガイダンスを提供しています。[8]」

この記述から、ITIL はサービス･プロバイダのためのフレームワークを提供しているというのが ISMS と大きく異なる点であることがわかる。ITIL のプロセスのインプットは、顧客からの SLA のセキュリティ条項であり、アウトプットは SLA に準拠していることを顧客に報告するという形になっている。

ITIL の全体フレームの中で、セキュリティ管理は他のプロセスと切り離して実践することはできない。この関係を「IT サービスマネジメント－ITIL 入門」では以下のように表現している。

> 「セキュリティ管理は他の ITIL プロセスと関連性があります。これは他のプロセスがセキュリティに関する活動を行うからです。これらの活動は書くプロセスやプロセス・マネージャの責任において、決められた方法で行われますしかし、セキュリティ管理はセ

[8] IT サービスマネジメント－ITIL 入門、itSMF、2004 年 7 月（日本語版発行）pp. 175

キュリティ関連の活動の体系について他のプロセスに指示を出します。通常、これらの合意はセキュリティ・マネージャと他のプロセス・マネージャとが相談した後で設定されます。[9]」

たとえば、以下のような管理プロセスが関連性があるとしている[10]。

- サービスデリバリ
  - サービスレベル管理
  - 可用性管理
  - キャパシティ管理
  - IT サービス継続性管理

- サービスサポート
  - 構成管理
  - リリース管理
  - インシデント管理
  - 問題管理
  - 変更管理

ITIL では、IT の急速な変化に対応できるプロセスの必要性が強調されている。計画、実行、評価、維持向上のプロセスを繰り返すというのは ISMS のマネジメント・サイクルに似ているが、そのプロセスの目的は「SLA セキュリティ要件の実装」にある。

ITIL の場合、顧客との SLA のセキュリティ条項に確かに準拠していることを示すことができなければならない。したがって、「セキュリティ管理についての測定可能な重要業績評価指標（KPI）と判断基準[11]」について合意しておくことが重要である。

ITIL は、IT サービス・プロバイダのために開発された BS7799-2 と類似したマネジメントのベストプラクティスである。この ITIL をベースに作成された

[9] IT サービスマネジメント－ITIL 入門、itSMF、2004 年 7 月（日本語版発行）pp. 178
[10] 同上、pp.178-181
[11] 同上、pp.183

英国規格 BS15000-1 では、ISO/IEC17799 が参照されている。また、規格中には「BS15000-1 の要求事項を実践したとしても、BS7799-2 を基準とする認証を得るために必要なすべての要求事項を満たすとは限らない。BS7799-2 の認証を取得した組織は、BS15000-1 のセキュリティ要求事項を満たすことになる」という内容の記述がある。

3.2 サーベインス･オックスレイ法（SOX 法）

米国では、エンロン やワールドコム の不正事件を受けて、2002 年 7 月に制定された企業改革法(サーベインス・オックスレイ法；SOX 法)への対応が最重要課題として取り組まれている。特に、SOX 法は財務情報の真正性を要求しているため、CISO や CIO にとって重要な経営課題となった。

SOX 法とは

企業改革法の目的は、開示制度の正確性と信頼性の改善と投資家保護である。その目的は、財務関連情報の内容に関する責任が上級経営者にあることを明確にすることにより、上級経営者による不正や粉飾決算を防ぐことにある。

対象となるのは、SEC（米国証券取引委員会）に登録している企業で、その中には約 30 社の日本企業も含まれる。米証券取引委員会（SEC）は、2003 年 6 月に企業改革法の要求事項をより具体的に明らかにした内容を提示している。

ポイントは、以下のようにまとめられる。

- 取締役・経営幹部の財務報告・開示の関する責任（コーポレート･ガバナンス）
- 監査人の独立および監査・監査法人規制
- 企業の開示の強化
- 証券アナリストの利益相反
- 法執行・調整・罰則強化

企業改革法で重要な条項は、第 302 条「財務報告に関する会社の責任（経営者の民事責任）」、第 404 条「経営者による内部統制の評価」および第 906 条「財

務報告に関する会社の責任（経営者の刑事責任）」への対応の 3 条項と言われている。特に第 404 条は、どこまで実践すれば内部統制を適切に実施していると判断できるか難しい課題を抱えている。

表 12　企業改革法のポイント

第 302 条	財務報告書に対する企業責任→年次・四半期報告・内部統制の確立維持
第 404 条	経営者による内部統制の評価→内部統制の有効性評価に使用されたフレームワークの特定、内部統制評価の合理的な証拠の作成が必要
第 906 条	違反→最長 10 年の禁固刑か 100 万ドル以下の罰金、あるいはその両方の刑事罰。 故意に違反→最長 20 年の禁固刑か 500 万ドル以下の罰金、あるいはその両方の刑事罰。

内部統制

第 404 条に規定している内部統制を適切に実施するための参考となるのが、COSO フレームワークである[12]。COSO の「内部統制モデル」は、1992 年に作成され、2004 年にはより経営活動に関する視点を取り入れた「ERM モデル」が作成された。COSO フレームワークでは、リスクを評価しそれに基づいて対策を策定し、それが適切に実施されているかどうかを監視するといった一連の内部統制活動のプロセスを規定している。

[12] COSO は、トレッドウェイ委員会組織委員会（Committee of Sponsoring Organizations of Treadway Commission）の略称で、米公認会計士協会（AICPA）、米内部監査人協会（IIA）などにより設立された団体。

表 13　COSO　ERM フレームワーク

SO法404条の要求事項を整理するために有効なフレームワーク

「内部統制の目的」
- Strategy（戦略）
- Operation（事業活動）
- Reporting（財務報告＋非財務報告）
- Compliance(法令順守）

「内部統制の構成要素」
- Internal Environment(内部環境)
- Objective　Setting（目的の設定）
- Event Identification（事象の特定）
- Risk　Assessment（リスク評価）
- Risk　Response（リスクへの対応）
- Control　Activity（コントロール活動）
- Information＆Communication（情報と伝達）
- Monitoring（モニタリング）

「組織レベル」
- Entity-Level（全社レベル）
- Division（部門）
- Business　Unite（ビジネスユニット）
- Subsidiary（子会社）

個々の組織では、この COSO フレームワークなどを活用し、財務システムを変更するなどの対策を実施する。マネジメントに関しては、規定した管理方法に従って実践している記録を残さなければならない。また、その記録が改ざんされていないことを保証する必要がある。たとえば、適切なアクセス権限の付与や履歴の保存などが具体的な対策としてあげられる。図 2 は、SOX 法に合致するように既存の内部統制を見直し、改善したプロセスを表す事例である。この一連のプロセスは、内部統制活動を表すものとして文書化することが重要である。また、テストの内容や結果、改善内容などは記録として残す。また、内部統制監査の実施や報告は、監査報告書にまとめる。このような一連の作業は、経営層の責任の下で実施され繰り返される。

図 2　　SOX 法対応の内部統制の実践プロセス

SOX 法と ISMS

多くの米国企業は、すでに SOX 法対応として、要求事項に合致した具体策

を一通り策定し終わったという状況である。不備があった場合、経営者の責任が問われることから、これまでかなりの人手とコストをかけて対策を実施してきた。しかしながら、今後はコストの適切性などを含めた見直しをする第 2 フェーズに入っていくことになる。

一方、日本版企業改革法の導入も検討されている。たとえば、東京証券取引所では有価証券報告書等において、不実の記載がないことを代表者が確認することなどを盛り込んだ報告書を公表している。

米国での先行事例は、わが国の企業の実践において大変参考になるであろう。

SOX 法の目的と ISMS の目的とは基本的に異なっているものの、いくつかの類似点も見られる。まず、ISMS ではセキュリティの 3 要素に情報資産の真正性を含んでいる。この点は、ISMS のために確立したいくつかの管理策は、SOX 法の要求を満足させることができるものと思われる。また、実践のためのプロセスにおいては、どちらもリスク評価を含んでおり（COSO フレームワークを参照した場合ではあるが）、すでに ISMS に取り組んでいる企業には馴染みのあるアプローチであると言える。

SOX 法の要求する内部統制のレベルについては、まだ解釈が定まらないところがある。しかしながら、最終的に経営者や役員が自社にふさわしいセキュリティのあり方について、自己の責任において意思決定（これは経営方針に密接に関連する）を行わなければならないという事実を明らかにした意味は大きい。そのために必要な一連のマネジメント・プロセスを実施するために、COSO フレームワークと同様 ISMS もまた CISO や情報セキュリティマネージャー達に有用な情報を提供するものである。