ISMS Journal (Issue 1)

（日本語版）

出典：http://www.xisec.com

財団法人 日本情報処理開発協会

ISMS Journal

第 1 号　2002 年 10 月（仮訳）

第１号発行について

このたび IUG ISMS ジャーナル第１号を発行いたしました。このジャーナルは季刊誌であり、毎回、ISO/IEC 17799、BS 7799 Part 2 や関連規格に関するニュースを、地域ニュース、国際ニュース、世界における認証の動向、実施に関する問題、規格の要素を解釈する際の手引きや支援、その他多くの重要な関心事などにわたって提供致します。

このジャーナルは、IUG（International User Group）のリサーチ部門にあたる本協会が発行いたします。IUG は、国際的にも、地域レベルでも現在活動を展開しております。昨年には、従来のオーストラリア、スウェーデン、英国に加え、カナダ、ドイツ、香港、台湾などにも IUG の地域支部を設置致しました。

このジャーナルでは今後、例えば、この第１号掲載の「在宅勤務者とセキュリティ」、その他監査と認証の詳細、リスクマネジメントの実体、Plan、Do、Check、Act 方法による ISMS 構築など、BS 7799 の適用に関する特定の領域に焦点をあてた多くの連載記事を掲載する予定です。また標準化や認証についての最新情報や、世界各国の IUG 支部による報告から最新情報をお届けする予定です。

この第１号が皆様にとって有益で役立つものであり、また次号も興味をもってご一読頂ければ幸いです。

Ted Humphreys（編者）

ハイライト

News from IUG Chapters（IUG 支部ニュース）

The Canadian Landscape（カナダの状況）

カナダの ISO 17779 ユーザーグループの初回会合が、８月８日トロントで開催された。カナダでは ISO/IEC 17799 と BS 7799-2 規格に対する支持が強まってきており、これら規格に対する信用も高まってきている。またカナダのいくつかの行政府部門だけでなく、銀行や様々な商業組織も関心を示している。カナダ IUG 支部は 8 月末にも、ISO/IEC 17799 のギャップ分析に関する最近の実際経験を検討する目的で会合を開いた。カナダグループの次回会合は 10 月 10 日に予定されており、この会合では "Enforcing Corporate Governance Using ISO/IEC 17799, Turnbull Report and NSA Infosec Assessment Capability Maturity Model"（ISO/IEC 17799 を用いた企業統治の実施、Turnbull による報告、及び NSA 情報セキュリティ評価能力完成モデル）という議題について話し合う予定である。このプレゼンテーションの目的は、公認会計士、CFO、CEO、CIO、CSO や、全ての経営管理を統合し、効率的な企業統治を行うために提示されるビジネスツールを適切に適用するようにすることである。

これは、素晴らしい、意欲的なスタートだが、しかし今だなすべきことが多くある。カナダユーザーグループの最初の取組みの一つには、ISO/IEC 17799 を使用する便益について認識を高め教育を進めることが挙げられる。

カナダ ISO 17799 ユーザーグループのコーディネーターへの連絡は、lj@scienton.com.へお願い致します。

The German Club（ドイツのクラブ）

7799 利害関係者グループによって、ドイツでも IUG クラブが開設された。これは、いくつかのドイツ企業において認証ルートに対する関心が高まっていることを受けたものである。現在、既に認証を取得している企業の例としては、T-Systems、Siemens、Vodafone などがある。ドイツ IUG クラブのメンバーには、このような認証取得企業、現在取得準備中の企業、ドイツ認証機関である DQS、行政府代表者、セキュリティ実践者が含まれている。

ドイツ IUG クラブの初回の議題は、以下のとおりである。

- BS 7799-2 の新版、この規格のドイツ市場への適用可能性、及び統合マネジメントシステムへ向けた今後の動向の推進。
- ISO/IEC 17799:2000 及び BS 7799-2:2002 の適用において SME（Small and Medium-sized Enterprise = 中小企業）に対する支援方法の検討。
- ドイツ産業及び商業における ISO/IEC 17799:2000 及び BS 7799-2:2002 に対する理解の向上、及び 7799 に関する事項を協議し展開できる場であるフォーラムの開催。

The German Information security Agency（略称：ドイツ BSI）は、'A Comparative Study of IT Security Criteria'（IT セキュリティ基準に関する包括的調査）を発行した。このなかでは、次の文書が比較されている。

- IT Baseline Protection Manual（IT ベースライン保護マニュアル）
- ISO/IEC 17799 及び BS 7799 Part2
- ISO TR 13335 (GMITS)
- ITSEC/Common Criteria
- ISO 9000
- Control Objectives for Information and related Technology (CobiT®)（情報技術及び情報関連技術の管理目的）
- ドイツにおける他の文書

この文書の目的は、ユーザーが自らの目的に最も適したものを選択するのに役立つよう、IT や情報セキュリティに関して馴染みのある文書に対する入門的なガイドを構築することである。この文書では、以下のような事項が検討されている。

- 目的、対象者（targeted audience）、適用されるアプローチは何か？
- 規格の更新方法、及び完成方法は？
- 入手方法の容易さは？価格は？
- 認証、及び国際化については？

上記の事項に関しての表形式による詳細な比較に加え、この調査ではこれらの文書の組み合わせという興味深い問題について議論しており、うち 2 つのシナリオには（以下に示すように）ISO/IEC 17799 が含まれている。

1） ISO/IEC 17799 と IT ベースライン保護マニュアル（の組み合わせ）。ISO/IEC 17799 は「ベストプラクティス」の管理の一覧を提供するものであることから、より詳細な技術的説明を IT ベースライン保護マニュアルから取り入れることによって、これらの包括的な推奨事項を実施する助けとなり得る。

2） ISO/IEC 17799 と ISO 9000（の組み合わせ）。ISO 9000 には特定の情報セキュリティ考慮事項が含まれていないことから、ISO/IEC 17799 を情報セキュリティマネジメントに関する範囲を拡大するために使用することが可能となる。特に、ISO/IEC 17799 には、作成プロセスを網羅した方法も記載されており、その為 2 つの規格は補完し合うことができる。

ISO/IEC 17799 とコモンクライテリアの組み合わせは十分興味深いのだが、この 2 つの文書は目的と方向性が異なるため、この組み合わせは考慮されていない。この文書全体については、ウェブサイト www.bsi.de. で閲覧することができる。

ドイツにおける ISO/IEC 17799:2000 及び BS 7799-2:2002 に関する今後の開発やニュースに興味のある方は、IUG クラブのウェブサイト www.aexis.de. を閲覧ください。

Dr. Angelica Plate
(AEXIS Security Consultants
& IUG Germany Chair)

Certification in Hong Kong －Out off the Blocks （香港における認証 － 障害を越えて）

シンガポール、韓国、日本、インドなどのアジア太平洋地域の他の国々と異なり、香港特別行政地域 HKSAR（Hong Kong Special Administration Region）の行政府は、現在のところ、BS 7799-2 を含む地域的又は国際規格を正式には認めていない。しかしながら、HKSAR が正式に公的な関心を示していないからといって、香港の民間企業における BS 7799-2 認証取得に対する関心レベルの着実な高まりが妨げられているといったことはない。2001 年以来、5 つの組織が香港において BS 7799-2 の認証を受けている。これらの組織名称は以下の通りである。

- Icfox International (BSI-IS 67394)
- PCCW Business eSolusions HK (BSI-IS 67432)
- PCCW Powerbase Data Center Services (BSI-IS 66182)

- TQM Consultants Ltd (BSI-IS 57846)
- Vhsoft Technologies Co. Ltd (DNV-02015-2001-AIS-LDN-UKAS)

2002 年 7 月 18 日現在、香港は、英国（69）、日本（7）、インド（6）、韓国（6）、ノルウェー（6）に続いて、ドイツ、シンガポールと並び世界で 6 番目に認証発行数の多い国（5）となっている。

現在、香港では、少なくとも、他にも 8 つの組織が正式に BS 77799-2 認証を取得するための手続きに入っている。うち、少なくとも 2 組織が今年末までに BS 7799-2 認証を取得すると思われる。

香港には、情報リスクマネジメントに関する主眼点を組み合わせた BS 7799 研修コースを実施する主な機関が 2 つある。ある地元の大学がうち１つのコースを運営しており、もう一方のコースは認定された BS7799-2 認証機関が運営している。2001 年以来、約 200 名の学生が様々な BS 7799 研修コースを地元香港で受講している。

地元大学の実施した地域調査によると、BS 7799 規格を知っていたのは調査を行った学生中約 20%に止まっている。結果として、調査を行った大学生の間では、BS 7799 の認識レベルは、他の情報セキュリティを基礎とした制度と比べて引き続き低い割合に止まっていることがわかった。

BS 7799-2 認証に対する関心レベルが地域で高まっているという事実を確認するため、IUG 香港支部が 2001 年後半に設置された。この HKIUG は少数の個人から成るが、彼らは皆 BS 7799-2 認証プロセスの異なる面に直接関わった経験がある者達である。HKIUG の初めの取組みは、各地に固有の性質を反映したコメントを提出する場である、最近行われた BS 7799-2 に対するパブリックコメントによるレビュープロセスに自らが貢献する方法を見出すことだった。

HKIUG は、現在、HKSAR 行政府に対して BS 7799-2 などの情報セキュリティマネジメント規格をより正式に認める必要性や、そのような規格に対する認証を取得した結果として達成できる便益をさらに推し進める案を募っている。

Dale Johnstone
(IUG Hong Kong Chair)

This Month's Articles（今月の特集）

Spotlight on Incidents（事件・事故に着目する）（Part 1）

この記事は 2 部構成であり、今回の第 1 部では、Dr. David Brewer が BS 7799 Part2:2002 新版の観点からセキュリティ事故に関して馴染みのあるテーマを考察する。

The 2002 DTI Security Breaches Report（2002 年度 DTI セキュリティ違反報告書）によると、昨年中に英国企業の 44%が少なくとも 1 つの悪質なセキュリティ違反の被害に遭ったとのことである。また、セキュリティ事件・事故にかかった平均費用は 30,000GBP（British Pound = 英国ポンド）で、なかにはこの費用が 500,000GBP 以上に上ったと報告した企業もあるということである。主な攻撃方法として報告されたのは、ウイルスだった。全世界的に見ると、他にもインターネットビジネスに対する深刻なサービス妨害攻撃、顧客のアカウント詳細情報の盗難、国家防衛システムへの侵入、セキュリティ事件・事故に対する企業の対応についての敵意をもった報道、会計疑惑、主要企業の倒産に関するケースなどが報告されている。

こういったケースはあなたの会社でも起こり得るのだろうか？その場合、問題となるだろうか？

新 BS 7799-2:2002 は、これらの疑問に答えるのに役立つ。この新規格は、情報セキュリティマネジメントシステム（ISMS）を構築、使用、維持、改善する方法について説明するものである。つまり、どのようなリスクが生じた状況でも効果的に運用が行えるよう、経営陣（management）が組織の情報セキュリティ防衛を整備する手段なのである。この ISMS の動力源（powerhouse）は、50 年以上前に Deming が初めて考案した Plan、Do、Check、Act サイクルである。

チェック行為の目的は、ISMS 適用範囲内において管理策が実施されているか、効果的に運用されているか、他の管理策を導入する必要はないかをチェックすることである。とりわけ、何らかの新たなリスクが生じた場合、現在の管理策でそのリスクを処理できるのか、もしくは新たな防御策（defense）を設けるべきなのか？また実際、他の防御策を現在安全に移すことができるのだろうか？BS7799-2:2002 の附属書 B では、チェック行為を成し遂げることのできる様々な方法が推奨されている。この方

法は、例えば、IT ネットワークのセキュリティが破られていないかどうかチェックするなどの侵入検出から、ISMS の総合効果を評価するために ISMS 全体のマネジメントレビューの実施にまで及ぶ。前者は本質的に主として技術的なものであり、一方後者はほとんど全て人によって実施される。この 2 つの両極は、このように実施手段が全く異なるだけでなく、実施頻度においても異なっている。前者は、ネットワークが稼動している間中行われるリアルタイム活動であり、多くの場合その実施時間は 24 時間×7 日である。一方、後者は、年に一度実施すればよい。

この両極の中間の事例としては「他者からの学習」（”learning from others”）と呼ばれるものがある（他にも一つあるが、これは実質的にセキュリティ事件・事故の結果必要となる活動に関するものであり、つまり規定要求事項である。これについては次号で述べる。－新規格[BS 7799-2:2002]の 4.2.2(g)項を参照）。「他者からの学習」項における助言は、もともと、米国のコンピューター緊急対応チーム（CERT = the Computer Emergency Response Team）やパーデュ大学（Purdue University）などの国際機関が定期的に発信する、IT の脆弱性に関する警告を取り扱うことのみを対象としたものだった。しかしながら、いったん新規格にこれを含めるという提案が承認されると、編集チーム（the Editing Team）はこの定義を全種類の報告を含めるというものに拡大した。これによって我々は他者の経験から学ぶことによって自らの防御策をチェックすることができるようになった。この規格では、会議、専門家の会合、利用者グループ、技術や運営管理に関連する出版物にみられる様々な記事について言及している。DTI セキュリティ被害報告は、単にこれらのうちの一つにすぎない。

従って、チェック活動は、いかにして他者の経験について学ぶか、またいかにして他者が経験したのと同様の問題に取り組むか、もしくはそのような問題の発生を防ぐかを我々に教えてくれるものなのである。さて、何が自身の会社に起こり得るかはわかった。となると、それは大問題となり得るのだろうか？この疑問に対する回答は、Plan 活動、とりわけリスクアセスメントのなかに見出される。他者に起こった事項を識別する際、「それは問題となり得るか？」という疑問に対する回答を得るための活動は、我々自身のリスクアセスメントに即して行うべきである。そうはいってもやはり水平思考が、常套手段（byword）である。というのも、我々自身の行うリスクアセスメントは、リスクアセスメント実施時に我々がリスクとみなしたものだけに限られてしまう可能性があるからである。つまり、チェック活動を適切に実施することによって、視野を広げ、幅広い考えをもつことができるのである。

被害を受けた会社にあなたの会社と同様のタイプの脅威が存在し、また同様の資産価値があり、かつこの会社が同じような技術を使用していた場合、明らかに、あなたの会社にもこの被害会社と同様のリスクが存在するだろう。そのためその被害会社に対する攻撃が成功したという事実を要因として、自らの状況を再検討するための優先活動を緊急に行うべきである。その際、攻撃が成功したかもしれない他の方法を考えてみてほしい。これらは、あなたの会社にも当てはまるだろうか？これはただ単に水平思考の例の一つにすぎない。何千ものクレジットカード詳細情報の盗難に関する報告がいくつかある。このような窃盗を行ったのはハッカーかもしれないが、しかし不満を抱いている従業員が詳細情報を CD にコピーし、それを持ち出しても、全く同様のことが起こり得るだろう。これは水平思考の別の事例である。映画産業の情報セキュリティ愛好家は、ジュラシックパーク 1 をみて、電源のスイッチを再び入れるために主役の男女をヴェロキラプトルと対戦せざるを得ない状況に追い込んだ、復旧モード付きのセキュリティシステムは設計すまいと思わせる、あの最後のシーンを好むかもしれない。が、しかしこの冒険は全て、（Richard Attenborough 氏演ずる）John Hammond が、（Wayne Knight 演ずる）Dennis Nedry の行った IT に関する取組みに対して適当な賃金を支払えなかったことから始まったことを思い起こして欲しい。内部者による攻撃（Insider attacks）はおそらく、外部者による攻撃よりも重要であろう。しかし実際の要因は影響であり、ジュラシックパークはこの影響が非常に大きなものとなり得ることを示している。Barings と Enron は両方とも内部管理が原因で倒産したのが、もし BS 7799-2:2002 アプローチを適用していればその利益を得ていたであろう。リスクアセスメントは、セキュリティ事件・事故を取り上げて発生可能性と影響度からこの事件・事故を評価するよう教えてくれるのである。

この特集の第 2 部では、この 2 つめの疑問により詳しく答えるためにリスクアセスメントの利用を考察する。同様に、セキュリティ事件・事故について、規格として特に何を言及しなければならないかについても考察する。

Dr. David Brewer (Gamma Secure Systems Ltd)

Audit and Certification（監査{審査}と認証）（part 1）－ So You Have An Audit（監査{審査}の受審）

ある組織は BS 7799-2:2002 に適合した ISMS を保持しているが、認証は受けていない。この組織内で新たに任命されたセキュリティ担当役員（Security Officer）は、月曜に監査（審査）員が来るという連絡を上司から受けた。このセキュリティ担当役員はいったい今から何をす

ればよいのだろうか？

セキュリティ担当役員は、どのタイプの監査（審査）員が来るのか、そしてその目的は何なのかを知っておく必要がある。そうすることによって、他にも切迫した業務がある中で監査（審査）に必要な準備を終わらせることができるのである。

どのタイプの監査（審査）員が来て、何を行うのだろうか？来る可能性のある監査（審査）員グループには、以下のものがある。

The Internal auditors（内部監査員）

内部監査員は、組織の内部管理（Internal Control）手順の様々な側面について監査を行う、組織内の独立した者達からなるチームである。この活動を、大抵の場合は会計監査員についてだが、外部組織に委託している組織もある。この内部監査員達は、上層部経営者の合意を得た期間中に検討事項全体を網羅するよう作業実施計画を立てる。その業務の一部には、ISMS 内部監査の実施が含まれる。その際の適用範囲については、BS 7799-2:2002 の 6.4 項に規定されており、また手引き B 5.4 項に詳述されている。この業務は、定期的に一度に全てを対象として実施されることもあれば、年間で全体を網羅するような、部分的なもののこともある。

内部監査員は、例えば、ライン部門においてプロセスを実施した結果に見られる誤りを識別するための手順と、ISMS 内部の事件・事故報告プロセスとの関係についてなど、ISMS 範囲外の問題についてセキュリティ担当役員と話し合いたいと望むかもしれない。彼ら内部監査員の行うどのような訪問についても、その正確な業務範囲を明らかにしておく必要がある。

IT 内部監査員は、たいてい、ISACA（The Information Systems Audit and Control Association = 情報システムコントロール協会）や内部監査人協会といった自身の属する団体が発行している手引きに関する業務を行う。この手引きとは、CobiT®や e-SAC のことである。この手引きについて説明している文書は、ウェブ上にて無料で入手できる。例えば、http://www.itgovernance.org/ を閲覧ください。

The external (financial) auditors（外部{会計}監査員）

この監査員は組織にとって外部の者である。これには、政府省に対するものとしては NAO（National Audit Office = 英国会計検査院）、地方・保険機関に対するものとしては区域監査サービス、そして会計事務所が含まれる。この外部監査員らの検討事項の大半は組織の会計報告書の誠実性を扱うことだが、政府の監査員は公的資金の使用に関してその効果及び効率に関する検討事項も扱う。業務の一部として、通常、監査員らは情報セキュリティを含む被監査者の手順の品質についての評価に務める。監査組織は通常、IT 専門家を職員として採用しており、こういった専門家が情報セキュリティの監査に携わるであろうと思われる。

外部監査員は、会計機関の発行した規格に関して業務を行う。これらの規格及び関連する手引きは、特に ICAEW（The Institute of Chartered Accountants in England and Wales = イングランド・ウェールズ勅許会計士協会）の IT 学会から得られるいくつかの IT 資料も含め、概して組織に関する一般的なものである。会計事務所からの外部監査スタッフはまた、他の目的のために業務を行うこともある。これには例えば、監督機関に関する業務、特定の基準を満たすための特定活動の監査業務などがある。

セキュリティ担当役員は、こういったスタッフの手助けを適切に行えるよう、外部監査の目的について明確にすべきである。

Certification auditors（認証審査員）

認証審査員とは、規格に従って認証登録証を発行することを認められた認証機関の外部審査員のことである。英国には、BS 7799-2:2002 について認証登録証の発行を認められている機関が数多くある。これらの審査員は ISO 及び IAF の発行する規格やガイドラインに関して業務を行う。

Other auditors（他の監査員）

組織は、例えば、税関局（HM Customs）（付加価値税(VAT)について）、内国歳入庁（Inland Revenue）（源泉課税(PAYE)について）、また健康安全局（the Health and Safety Executive）といった、他の機関による監査（又は検査）を受けることがある。これらの監査は、情報セキュリティの調査を伴うこともある。

Other activities, which may be called audit.（監査と呼び得る、他の活動）

このような活動の一例としては、当該活動と無関係な組織内の者が実施する ISMS 内部監査がある。このケースは、組織内に内部監査員がいないか又は、内部監査員が他の運営上の優先事項があるため多忙な場合に起こり得る。

他の例としては、例えば、侵入テスト（penetration tests）など、情報セキュリティの特定の様相に関してのコンサルタントによる外部監査がある。

Conclusion（結論）

セキュリティ担当役員は、監査（審査）員が何を目的としているかを明らかにし、必要に応じて ISMS について当該監査（審査）員に適切な説明を行い、彼らが調査したいと望む記録や文書を見つける手助けをすべきなのである。

Willie List

Towards A Culture of Security（セキュリティ文化の普及に向けて）

OECD は、今年 7 月、情報システム及びネットワークのセキュリティためのガイドラインを発行した。このガ

イドラインは、OECDが1992年に初めてセキュリティに関するガイドラインを定めて以来、IT環境全体に起こった劇的変化を反映したものとなっている。実際、この10年間にわたって、動力技術の発達、これらの技術使用の普及、相互接続ネットワークの増加、ネットワークトラフィック容量の拡大がみられた。

2002年版のガイドラインは､セキュリティ文化という概念の普及を目的としている。これには、リスクについての意識向上、これらリスクの管理方法、情報システム及びネットワークの使用に対する信頼の構築、セキュリティ問題を理解するうえで助けとなる参考文献の枠組みの作成、セキュリティの実践やその手順についての協力及び情報共有の推進、規格作成の際に考慮すべき重要な側面としてのセキュリティの推進などが含まれる。これらの目的は、セキュリティ文化の構築に役立つ次の9つの原則を導入することによって支援される。

- 認識（Awareness）
- 責任（Responsibility）
- 対応（Response）
- 倫理（Ethics）
- 民主主義（Democracy）
- リスクアセスメント（Risk Assessment）
- セキュリティの設計及び実装（Security design and implementation）
- セキュリティマネジメント（Security management）
- 再評価（Reassessment）

このガイドラインに関する詳細情報については、OECDウェブサイト www.oecd.org. をご覧下さい。新BS 799-2:2002では、これら多くの原則を実施するためのプロセスの枠組みが示されている。

Ted Humphreys（XiSEC）

Applying ISO/IEC 17799 （ISO/IEC 17799の適用）－

Homeworkers and Security（在宅勤務者とセキュリティ）

情報改革の最も大きな影響のうちの一つに情報労働者の増加があげられる。情報は有形資産ではないため、情報を主に取り扱う仕事に携わる者は事務所や工場といった特定の場所に縛られる必要はない。そのような者達は、必ずしも従来の事務所的環境に対する物理的セキュリティ対策によって守られているとは限らないことから、彼らに関する情報セキュリティは特に重要であり、また特有のリスクを呈している。組織の通常のセキュリティ基本方針の多くは適用できないかもしれなく、また標準的な保護手段の多くは欠落しているか又は効果がないかもしれない。

やはり、ISO/IEC 17799には特にこのような労働者を対象とした助言があり、これは9.8項に記載されている。ISO/IEC 17799では、２つのタイプのリモート作業（remote working)、すなわち移動型計算処理（mobile computing)と遠隔作業(teleworking)を区別している。移動型計算処理は、持ち運びのできる機器（portable device）の使用を対象としているが、一方遠隔作業は固定された場所からのリモート作業を対象としている。遠隔作業（teleworking）という言葉は、あまり洗練されていない用語であるのはもちろん、この項の2つめの小項目（9.8.2項）に含まれているタイプの管理策を正確に描写するのに十分なものとはいえない。というのも、遠隔作業（teleworking）とは組織の他の部分と何らかの通信接続の型式があることを示すものなのだが、しかし実際にはこの手引きはそのような接続のあるなしに関わらず、一様に適用できるからである。おそらく、在宅勤務（homeworking）の方がより正確な用語だと思われるが、この在宅勤務という用語は情報産業以外にはあまり芳しくない響きがある（ので採用しなかった)。それでも、ISO/IEC 17799では、遠隔作業（teleworking）であるなしに関わらず、在宅勤務者（homeworker）の保護手段について考察するためのすばらしい出発点を提供しているのである。

しかしながら、在宅勤務者の保護手段を評価しようとする場合､BS 7799-2の引用附属書はあまり有用でない。管理策は一つしかなく、これも単に在宅勤務者のポリシー、手順、及び規格の構築を要求するものにすぎない。BS 7799-2:2002の有益性が十分明らかになるのは、PDCAモデルを適用した場合のみなのである。

PDCAプロセスのPlan段階では、リスクアセスメントを策定・実施する際に、在宅勤務（homeworking）と通常のビジネス環境の主な違いを明らかにすべきである。在宅勤務の環境のみにしか当てはまらないであろう、一連の脆弱性全てが付加されるからである。これには、物理的セキュリティが均一でなくなり、たいていの場合弱くなってしまうといった脆弱性だけでなく、監督やレビュープロセスという人的側面が変化し、多くの場合マネジメント間の相互作用があまり頻繁でなくなり、より形式的なものとなってしまうといった脆弱性が含まれる。従って必然的に、在宅勤務のための特別な管理策を実施しなければならない。チェック活動もまた重要である。通常の事務所環境における官僚的なプロセスは別として、ポリシーや管理策の日常的な変更が行えなくなるかもしれないし、或いは既存の管理策が使用できないか又は適切でなくなるかもしれない。効果的な在宅勤務者のセキュリティを確保するために、種々の非標準的なプロセスが必要となるのは必須である。

最後に、在宅勤務に関するより幅広い様相の一部として、在宅勤務者のための情報セキュリティを考察しなければならない。例えば英国では、殆どの組織は、在宅勤務の許可に先立ち、サイト訪問調査を含む健康安全の分析が必要だと考えるであろう。このリスクアセスメントを、セキュリティを網羅するものにまで拡大し、また例えば単一の活動又はレビュープロセスの一部としての物理的セキュリティの向上に関する決定や助言を管理する

ものにまで拡大するのは、単純な問題であるべきである。このことは、BS 7799-2:2002 と他のプロセス管理規格とをより完全に統合することによって大いに促進される。

もし在宅勤務セキュリティに関心がおありならば、推奨可能な資料が数多くあり、これらの資料にはより詳細な情報が掲載されており、かつ無料である。英国貿易産業省（DTI = the UK Department of Trade and Industry）は、"Working anywhere: exploring telework for individuals and organizations"（場所を問わず働く：個人及び組織における遠隔作業の検討）という素晴らしい冊子を発行している（DTI reference 00/867)。この包括的なガイドには、データ保護及び情報セキュリティに関するセクションがある。これはオンラインで注文できるが（http://www.dti.gov.uk/publications/)、現在はウェブから直接ダウンロードはできない。多くの産業団体や組合は、在宅勤務（homeworking）や遠隔作業（teleworking)の意味するところについて役立つ助言を提供できる。実際、英国通信労働組合 (UK)（The Communication Workers Union)（http://www.cwu.org）では、英国の情報源の範囲をリストアップした包括的なリサーチノート（RD 98/044/2）を提供しており、これは Web 上からダウンロードできる。

Dr. Mike Nash (Gamma Secure Systems Ltd)

Tao-Zen Practice and The Art of Information Security Management [1]（Tao-Zen プラクティスと情報セキュリティ管理術）

新たに改訂された BS 7799-2:2002 は、ISMS の継続的改善プログラムの実施を支援して、効果的な情報セキュリティを確保するための PDCA（Plan、Do、Check、Act）モデルを採用している。以下の事項は最近の２つの冊子から抜粋した見解であり、近代マネジメントシステムの考え及び手法と組み合わせた、いくつかの東洋哲学の考え及び原則を適用している。ここに掲載の記事は、Ted Humphrey が BS 7799:Part 2 新版（2002 年版）の観点から ISMS プロセスアプローチの異なる側面を考察した 5 つの記事のうち、最初のものである。

セキュリティが保てない部分が常にある程度存在することを認める一方で、必要最低限のセキュリティを実現するための適正なバランスがとれるように、我々は自身のビジネスシステムを運営管理する必要がある。これは、我々のシステムが「目的に適った」("fit for purpose") ものとなる保証水準（level of assurance）を確立し、かつセキュアな方法でサービスや製品を届けるという我々の能力に対する信頼を顧客、ユーザー、依頼者及び取引相手先に与えるために、この保証を適切に管理する必要があることを意味する。つまり情報セキュリティマネジメントシステム（ISMS）が、まさに必要とされているのである。これを達成するうえで、我々は以下の事項を行うべきである。

- 保護したいビジネス環境を全体的な視野からみる。
- その保護を実現するうえでプラス及びマイナスとなる影響力を理解する。
- 必要最低限の保護レベルを達成するために必要な、適正なバランスをとる。
- 保護レベルの維持に影響を及ぼす変化を理解する。
- ただ単に情報セキュリティマネジメントシステムを確立するだけでなく、変化を監視・レビューし、適正なバランスをとり、マネジメントシステムを継続的に改善するのに適した行動もとるために、循環的な思考法を養う。

Realizing an holistic approach（全体的アプローチに対する認識）

必要なセキュリティについて効果的に調べようとする場合には、ビジネス環境をより幅広く全体的に捉えることが必要となる。我々のビジネス環境は多くの異なる資産によって構成される。他の資産より重要なものもあれば、他よりも実用性の高いものもある。また他に依存している資産もあれば、他と連動したり相互運用したりしなければならないものもある。これらの資産には、情報、人、ブランド名・登録商標、知的所有権、イメージや評判、所有物、ハードウエア・ソフトウエアアイテムなどが含まれる。これらには全てビジネス環境のなかで果たす役割があり、あらゆる資産がどのように関連し依存しあっており、また全体と調和しているかを知ることは、セキュリティの観点から重要である。つまり、保護すべき必要のあるものは何かを知り、また、そのような保護を行うことを可能にする制約、依存、影響を知る必要があるのである。

Understanding the realities of the opposing forces（マイナスの影響力の実体把握）

情報セキュリティ実現のための探求は、自身のビジネスに関連する脅威、強み、そして弱みを理解することから始めるべきである。その結果、自身のビジネスに対する影響とリスクの実体を把握する、より良い体制が整う。つまり、適切な保護を達成する上で、我々にとってプラスとなる影響力或いはマイナスの影響力を十分理解しなければならない。こういった理解に基づいてマネジメン

[1] "Tao-Zen Practice and The Art of Information Security Management"（Ted Humphreys、2001 年 XiSEC 発行）からの抜粋。

トの決定を行う必要があるのだが、その際、これは明瞭な科学ではなくリスクの算定なのであり、保護したいビジネス環境についての知識なのだということに配慮しなければならない。なぜなら、不確かで未知なものは常に存在するからである。

“The unknown is what it is.”（John Lennon より）

Achieving a realistic balance（実際的バランスの達成）

ビジネス上のあらゆる所有物や活動については、経済的に意味があり有用なものとなるように適正なバランスをとる必要がある。企業は、自らをどのように組織し、マネジメントスタイルを運用し、どのような専門的技術を必要とし、かつ資産や資源を運営管理し保護するかといった、自身が確立するポリシーと戦略間の適正なバランスをとることを目指すべきである。リスクマネジメントとは、バランスをとる活動なのである。つまり、影響の及ぼすプラス面とマイナス面を判断し、資産に対する脅威が発生した場合の影響の性質及び度合いについて何を受け入れ維持することができるかについての決定を行い、及びリスクレベルを許容できる影響範囲内に保つための管理システムの実施と維持にかかる費用を決定するといったことである。その際、経済的制約や他のビジネス上の制約は重要な役割を果たす。保護する資産の価値以上にセキュリティに費用をかけても、経済的には意味をなさない。セキュリティ技術を管理し運用するための適切な資源を確保せずにその技術に対して費用をかけるのもまた、経済的にもセキュリティ上においても意味をなさない。保護とリスクの実際的なバランスをとろうとするならば、全体的な視野からビジネス環境を正しく考慮してリスクマネジメントを確立し、企業の直面しているビジネスを脅す影響力や強化する影響力と、リスクを弱める影響力や高める影響力を理解することが必須なのである。

Realising changes（変化の自覚）

あらゆるものは絶えず変化しており、不変なものなどない。脅威レベルは変化し、その脅威が及ぼす影響も変化することがある。また、強みが弱みに変化してより簡単に利用されてしまうこともあり、誤ったマネジメントの決断がなされることもある。これら全てが我々の直面するリスクの潜在レベルを引き上げている。現状を維持できるものなど何もないのであり、これは協力することが必要な外部のビジネス環境のセキュリティと同様、内部のビジネス環境のセキュリティにも当てはまる。組織構成は変化するのである。実際、職員の役割や機能は変化し、従業員も変化し、また従業員数も変化する。そしてこれらは全て企業のセキュリティに影響を及ぼし得るのである。企業は拡大し、縮小し、また多様化することもある。企業の属する市場も変化にさらされている。この市場も競争力が強まったり弱まったりする可能性があり、また繁栄したり崩壊したりする可能性もある。技術も変化するため、技術変化をどのように受け入れるのかを識別する必要がある。また、取引相手先、顧客、供給者に関連した変化にも同様のことがいえる。

このようなあらゆる変化と、その変化に対する企業の対応法に応じて、脅威のタイプやレベル、我々のビジネスの弱み又は強み、そしてリスクと影響の結果は変化し得る。我々のビジネスに合ったセキュリティレベルを達成し維持するためにより良い状況をつくるには、変化の対応に関するマネジメントの予定案にセキュリティを入れるようにしなければならない。ビジネス上の変化を取り扱うマネジメントの予定案に沿って、自身のビジネスのセキュリティを監視、識別、理解、レビューしなければならないのである。

Ted Humphreys (XiSEC)

Standardisation update（標準化最新情報）

BS 7799 Part2：2002

2002 年 9 月 5 日に BS 7799 Part2 新改訂版（2002 年版）が発行された。この新版は、ISO 9001 など、他のマネジメントシステム規格との整合を図るため、また Plan（ISMS の確立）、Do（ISMS の実施）、Check（ISMS の監視及びレビュー）、Act（ISMS の改善）モデルとこのモデルを実施するためのプロセス一式を盛り込むために改訂されたものである。

Revision of the PD Series of Guides（PD シリーズの改訂）

ガイドである PD 3000 シリーズは、現在、BS 7799-2:2002 新改訂版を考慮に入れた改訂作業が進められている。5 部構成の PD 3001～PD 3005 は、ユーザーが BS 7799-2:2002 規格に記載されている様々なプロセスや要求事項を実施する手助けとなるようなテーマを網羅している。例えば、3002 ではリスクアセスメントに関するガイダンス的枠組みを、3005 は管理策の選択に関する助言とガイダンスが提供されており、また 3003 では Part2 規格への準拠をチェックするためのワークブックがいくつか示されている。これらガイドの改訂版は初秋にも発行される予定である。

Ted Humphreys
（BS 7799 Part2:1999 年版及び 2002 年版編者）

ISO/IEC 17799:2000

一方、ISO/IEC 17799 は現在改訂中である。次回会合は今年 10 月に開かれ、この改訂版について議論される予定である。

この改訂目的は以下のようなものである。

- 管理策の実施に関するガイダンスの改善及び拡大
- 必要な場合にはさらなる管理策の追加
- 記載されている助言の明確性及び読みやすさの改善
- 旧版を導入している組織が簡単に新版にアップグレードできるよう、"backwards compatibility"（旧版との互換性）の維持

この改訂は ISO/IEC JTC1 SC27 で行われており、会合に出席したりコメントを提出するといった方法で世界中から少なくとも 20 カ国がこの改訂に参与している。このように非常に大きな関心が寄せられているため、そして数多くのコメントが寄せられたため、新版の発行は 2004 年以降になるものと思われる。

Revision of GMITS Part 1, 2 and 3（GMITS Part 1、2、3 の改訂）

ISO TR 13335 （GMITS – Guidelines for the Management of IT Security）の Part1 及び Part 2 は、現在 ISO/IEC JTC1 SC27 のもとで改訂作業が行われている。この改訂版では、Part1 と Part2 をあわせて一つのテクニカルレポートにすることに加え、現在の版に記載されている助言を改善・改正する予定である。現在、改訂版ドラフトに対する投票が行われており、2003 年中に最終版が発行されると思われる。

GMITS Part3 の改訂は、現在進行中である。Part3 は、リスクアセスメントとリスクマネジメント面を対象としたものであり、現在 Part1 と Part2 の改訂やリスクマネジメントを扱った他の開発にあわせて改正中である。

Dr. Angelica Plate
（AEXIS Security Consultants & international coeditor of ISO/IEC 17799:2000）

Certification Update（認証最新情報）

BS 7799 Part2 認証取得事業者数は、増加の一途をたどっている。The international register（国際認証登録事業者リスト）は、認証を取得した企業を記載したものであり、www.xisec.com/Register.com. で閲覧できる。同じサイト上にこれら認証の ISMS 適用範囲のいくつかが掲載されている。現在、認定された認証機関は世界中に 12 機関あり、認証審査を実施している。大陸ごとの認証事業者数を示した世界地図は www.gammassl.co.uk/bs7799 で閲覧できる。

What is the Foundation?（本協会について）

The International 7799 Foundation（国際 7799 協会）は、IUG の企業調査部門である。ここでは、各種の調査や共同ネットワーク化作業を通して IUG の目的を支援する役割を果たしている。本協会では IUG を代表して ISMS ジャーナルを発行している。本協会ではまた、規格の解釈に関する全ての事柄に対して無料の仲裁サービスを提供している。

Future Issues（次号案内）

このジャーナルは、今後四半期ごとに発行される予定です。このジャーナルの定期購読を希望する方は、件名に SUBSCRIBE と入力して journal@xisec.com へ e-mail をお送りください。定期購読を解除される場合は件名に UNSUBSCRIBE と入力して journal@xisec.com へ e-mail をお送りください。今後の発行に関する詳細情報は以下の URL で入手できます。

- www.xisec.com/IUGN.htm
- www.aexis.de
- www.gammassl.co.uk
- www.itsystemsplus.com

第 2 号では以下のテーマを扱う予定です。

- 事件・事故に着目する（Part 2）
- 監査（審査）と認証（Part 2）
- ISO/IEC 17799 の適用 – 移動型計算処理（mobile computing）
- Tao-Zen プラクティスと ISMS の確立

Events（行事）

最近では、次の行事が開催されました。

- ISO/IEC 17799/BS 7799 に関する初回ワールドサミットが 8 月 13/14 日シンガポールで開催された（詳細については www.tech-world.sq.com 参照)。
- 7799 Goes Global カンファレンスが 9 月 4/5 日ロンドンで開催された（詳細・カンファレンスレポートについては www.xisec.com 参照)。
- ISO/IEC 17799/BS 7799 に関するプレゼンテーションと 1 日間の tutorial を主に扱った、ISACA Asia CACS 2002 カンファレンスが 9 月 9/11 日開催された（詳細については www.isaca.or 参照)。

今後は、次の行事の開催を予定しています。

2002 年 10 月 2 日	BS 7799 ISMS ワークショップとセミナー（スロヴェニア、Ljubjana）
2002 年 10 月 7-15 日	ISO/IEC JTC1/SC 27 会議（ポーランド、ワルシャワ）
2002 年 10 月 23-24 日	BS 7799 2 日間コース（オスロ、Institute of Technology）
2002 年 11 月 11-12 日	IFIP TC-11 Working Group 11.5 on IICIS 2002（ドイツ、ボン）
2002 年 12 月 3 日	IUG 会議（英国、ロンドン）
2002 年 12 月 4 日	UK ユーザーグループ クリスマススペシャルワークショップ（英国、ロンドン）
2002 年 12 月 9-11 日	BSI-DISC BS 7799 リスクマネジメント 3 日間コース（英国、Gatwick）
2002 年 12 月 11-13 日	“Information security in the public sector”（公共部門における情報セキュリティ）（英国、ロンドン）
2003 年 3 月 17/18/20/21 日	7799 Goes Global カンファレンス（中国、北京・上海）
2003 年 4 月 28 日～5 月 6 日	ISO/IEC JTC1/SC27 会議（カナダ、ケベック）
2003 年 10 月 20-24 日	ISO/IEC JTC1/SC27 ワーキンググループ会議（フランス、パリ）

Journal Contacts（ジャーナル連絡先）

ご意見、情報セキュリティや BS 7799 に関する経験等を当協会までお送りください。すばらしい投稿につきましては次号以降で掲載させていただきますので、他の読者とご意見を共有することができます。

次号以降及び標準化問題への投稿は

tedxisec@aol.com Ted Humphreys まで、

本ジャーナルへの広告掲載については

dbrewer@gammassl.co.uk David Brewer まで、

情報セキュリティ及び BS 7799 に関するご質問は

aexisap@aol.com Angelika Plate までお送りください。

編集チーム（Editing Team）が最善を尽くしてご質問にお答えします。