ISMS Journal (Issue 2)

（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 2 号　2003 年 2 月（仮訳）

第 2 号発行について

このたび ISMS ジャーナル第 2 号を発行いたしました。このジャーナルは ISMS IUG(International User Group）の季刊誌であり、ISO/IEC 17799、BS 7799 Part 2 や関連規格に関するニュースを、各国の活動・国際的な活動の双方を含めて提供致します。またこのジャーナルでは、認証の世界で起こっている事柄に注目し、実施上の問題について議論し、これら規格の解釈においてガイダンスや支援を提供致します。

このジャーナルは、個々の ISMS IUG 支部から編集上の独立性を保つために、ISMS IUG のリサーチ部門にあたる本協会が発行いたします。ISMS IUG（www.xisec.com）は、国際的にも、また地域レベルでも現在活動を展開しています。

第 1 号の発行後、様々な出来事が起こりました。KAB は BS 7799 Part 2 に基づいた韓国認証制度（Korean certification scheme）に着手し、IRCA は ISMS Auditor Certification Criteria（ISMS 審査員評価・登録基準）を公開しました。また、BS 7799Part2 の 2002 年版のフランス語翻訳版とドイツ語翻訳版も現在作成中であり、一連のガイドである BSI PD 3000 シリーズも公開されました。種々の 7799 Goes Global（7799 国際化）カンファレンスも、2003 年には世界各地で開催される予定です。世界各国での ISMS 実施に関する認証も、引き続き増加しております。今号では、7799 に関する連載記事の他に、これらの事柄や他のニュースについてお伝えします。

この第 2 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）

IUG Meeting of European Experts（欧州専門家の IUG 会合）

IUG の地域会合が、12 月 3 日ロンドンで開催された。この会合には、フィンランド、ドイツ、アイルランド、オランダ、ノルウェー、スウェーデン、英国の専門家らが出席した。またこの会合では、ユーザーの申請（user application）、認証、7799 Goes Global カンファレンス、このジャーナルや最新の標準化活動など、世界各地から ISO/IEC 17799／BS 7799 の導入や採用についての報告や最新情報を得るための機会が提供された。

この会合ではまた、「BS 7799 Part 2: 2002 – Back to the Future: What next strategy?」の表題のもと、今後の作業についても協議した。ユーザーや ISMS 構

築者を支援するため、実施ガイドラインの分野でいくつかの意見がだされている。このような意見としては、継続的な ISMS 改善、ISMS 監査、ISMS 実施についてのプログラム実施に関する指針などが挙げられた。また、BS 7799 Part 2 に関する標準化及びガイドラインの分野では今後どのような作業が必要かを調査する目的で、全 IUG メンバーと他の利害関係者らに対してアンケートを発行することが決定された。

他の議題として、特定の ISMS 作業要求事項と目的を満たす申請者の選定に際して、組織・企業を支援するための ISMS 実践者に対する資格基準（competency criteria）について議論された。スウェーデンのユーザーグループがこの議題について検討しており、この目的のために基準案を作成した。IUG におけるこれと同等の基準の必要性についてコメントを募るため、このスウェーデンの基準を IUG メンバーに回付することが決定された。

IUG 欧州専門家グループの次回会合は今年 5 月 19/20 日にノルウェーのオスロで開催される予定である。

Ted Humphreys. IUG Chair

Promoting Information Security in Hong Kong（香港における情報セキュリティ促進）

香港経済は、よりいっそう情報技術に依存するようになってきている。この依存が高まった結果として、公共・民間の両セクターから情報セキュリティ全般に対して関心が寄せられ、これとともに情報セキュリティマネジメントは引き続き香港社会の主要な一部となっており、確実に改善されつつある。

香港企業や一般社会全体にわたって情報セキュリティ意識レベルの高まりが勢いをみせる中、この勢いを維持する目的で、香港政府はビジネスや地域社会全般のセキュリティをより良く改善する必要性を識別しこれを認識している。この改善は、国際的に認められている主要な情報セキュリティマネジメント規格（ISMS）や、このような規格に付随可能な、関連する認証プロセスを採用する重要性がよりいっそう認められつつあることに見受けられる。

香港における情報技術を代表する Legislative Councillor は、最近、ビジネスや地域社会セクターにわたって情報セキュリティマネジメントをより良く促進するには、次の事柄を行うために関連組織と連携する必要があると提案した。

- 多くの情報技術ユーザーや中小企業では、自らの情報技術施設をセキュアにするために必要な資源を充当することができないといったことから情報セキュリティの知識、専門的知識、ガイダンスが不足している。このような情報技術ユーザーや中小企業が直面している、共通の問題を取り扱う。
- ISMS/ISO 17799 の研究を実施する。
- 香港産業に適した、国際的に認められたセキュリティ規格を推奨する。
- 情報セキュリティマネジメントを採用する利点をより一層普及する。
- 小規模企業のニーズに最も適した情報セキュリティマネジメントのスキームを導入する。
- 国際レベルの包括的な情報セキュリティマネジメント戦略を採用することによって、香港政府のセキュリティレベルを高める。

現在、香港の政府、ビジネス、地域社会セクター全体にわたって情報セキュリティ規格に対する意識の向上が進んでおり、このことから今後の見通しは非常に有望だと思われる。

香港では ISMS ユーザーグループに対してより強い関心を示す人々は確実に増加しており、また正式に BS 7799 認証を取得した組織数も増加している。このことから、情報セキュリティに対する意識は、香港全体にわたって今後も順調に高まっていくと期待される。

Dale Johnstone
(IUG Hong Kong Chair)

Canada（カナダ）

ISO 17799 ユーザーグループは、Scienton と CNC Global の支援を受け、専門家らがセキュリティ規格、企業統治（corporate governance）、リスクマネジメント、信頼関係について会合を開き意見を交換する場にまで発展した。以下はトロントで開催された最近の 2 つの会合からのニュースである。どちらの会合においても、CNC Global が会合設備の提供を行った。

Scienton がスポンサーとなり、BSI の Mr. Craig Heier をトロントに招いた。Mr. Heier はこの会合で ISO 17799 規格に関する BSI の見解についてプレゼンテーションを行った。このプレゼンテーションは、この会合に出席した、カナダの主要な金融・州政府機関のマネージャーや CSO の興味を大いに引いた。

CIO 情報セキュリティ顧問であり、またこのテーマに関しての様々な興味深い記事の執筆者でもある Mr.

Mark Duez は、「今日、最も重要な企業の課題は、新たなビジネストラストを生成し、企業の決定に対する投資家の信頼を回復することである。」と述べた。また、ビジネスプロセスにおける新たなトラストパラダイムについての見解を示した。

本ユーザーグループの議長である Mr. Zivic は両方の会合の司会進行を務め、またプレゼンテーションを行って ISO 17799 と SSE-CMM の価値を比較した。このプレゼンテーションでは、ある一つの規格を実施する際、他の規格を意識して慎重に行えば ISMS を複数の規格に適合させることができるため、マネジメントシステム実施全般に付加価値をつけることができるという事実が挙げられた。

前回の会合の終わりに際して、Mr. Zivic はトロントにおける世界的な IUG カンファレンスを取り巻く進展について発表した。会場に興奮が沸き起こり、これは 2003 年における最も重要な情報ガバナンス行事として受け止められた。

カナダユーザーグループの活動については、www.scienton.com/7799ug/をご覧下さい。

Germany（ドイツ）

ドイツ IUG の初回会合は、2002 年 12 月 6 日ボンの T-Systems で開催された。この会合は、全出席者らにとって 7799 関連の重要な事項について議論する機会となった。この会合には、T-Systems、DQS（ドイツの 7799 認証機関）、BSI（ドイツ情報セキュリティ機関）、AEXIS からの代表者らが参加した。他にも著名な来賓講演者数名が出席し、7799 に関する重要な事柄についての最新情報や興味深い見解を提供した。この会合では、最初に Angelika Plate が講演を行い、ISO/IEC 17799 改訂についての最新情報や最近開始された ISMS Study Period（ISMS 検討期間）についての情報を含む、ISO からの最新ニュースを紹介した。続いて、下記の来賓講演者によるプレゼンテーションが行われた。

- Ted Humphreys：IUG や 12 月 3 日に開催された会合についての最新ニュース、新 BS 7799 Part 2、BS 7799 Part 2 認証、『7799 Goes Global』（7799 国際化）カンファレンス、ISMS ジャーナル、及び本協会についての最新ニュースなど、重要なトピックについての最新情報の紹介。
- David Brewer：内部監査及び 7799 認証審査についての情報を含む、「監査員への対応法」についての説明。また、記録、面接、ISMS 適用範囲、机上監査、監査員の科学技術の知識、管理策の選択とビジネスセンス間のバランスなどを網羅した、実際の事例に基づいた監査経験も紹介された。
- Mike Nash：7799 とコモンクライテリアは対立するのか、それとも補完的に作用することができるのかという問題の提起。また、この 2 つの規格が運用されている異なる状況、『システム』についての異なる内容と異なる見解、2 つの認証モデル、またリンクや相互運用の可能性についても検討された。

これらのプレゼンテーションについて、ドイツ IUG のメンバーらの間で激しい議論が行われた（これらのプレゼンテーションは全て、www.aexis.de のドイツ IUG のページから入手できる）。ドイツ IUG メンバーは、次回会合の日程について、ISO SC27 会議と次回の IUG 会議開催直後に開催を予定することに合意した。

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

Certification Launch in Korea（韓国での認証開始）

Korea Accreditation Board（韓国認定機関）（KAB）は、2002 年 11 月 19 日、BS 7799 認証のための認定制度に着手したと発表した。地域産業や政府において ISMS と BS 7799 規格に対する関心が高まる中、この認定制度によって、セキュリティ意識と ISMS を金融、通信、IT セクターなどの企業へと広めると同時に、認定された認証機関の認証プロセスの開発が期待される。

KAB はまた、BS 7799 認証機関の認定に関する文書、審査員研修コースの認定や審査員登録に関する文書を含む認定文書類を公開した。

認証機関に対する認定基準は、ISO/IEC Guide 62 に基づいており、また EA 7/03 「*Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems*」と同等である。この基準では、認定された機関に対し、認証の守秘性、客観性、公平性を確保する、組織構造、適格な要員、及び認証プロセスをもつことを要求している。

BS 7799 審査員については、ISMS 審査プロセスへ参加する（審査は行わない）ことに加えて、6 年の IT 実務経験を有し、このうち 2 年は情報セキュリティの職務であることが要求されている。さらに、該当する水準の学歴及び審査員研修コースの修了が要求されている。

これらの基準は、国際的に整合のとれた方法による第三者認証システムへの基本的なアプローチであるため、この制度の重要な要素である。

この KAB の制度はパイロット事業として 2003 年 12 月 31 日まで実施される。その後この認定・認証制度全体を最新の状態に維持するために必要に応じて見直し改訂される。

パイロット事業において認定を申請している機関は、認証機関では KFQ、KSA、K-QA、審査員研修機関では KSA、Neville Clark、BSI である。

これは、ISMS 構築を促進する活動と BS 7799 認証を実施するための様々な韓国内での活動を調整する、非常に効果的なアプローチである。例えば、ISMS フォーラム（IUG の韓国支部）が結成された。この支部では今後、ISMS と ISO/IEC 17799 及び BS 7799-2 の利点を積極的に広めていく予定である。

また、KS X17799（ISO/IEC 17799）、KS X 13335（ISO TR 13335）、及び BS 7799-2:2002 の韓国語翻訳版が公開された。これにより、関係者らが容易にこれらの規格の入手・研究を行えるようになった。

Hyun-Sic Won
Korea Accreditation Board

UK User Group（英国ユーザーグループ）

2002 年 12 月 4 日に開催された前回の英国ユーザーグループの会合では､7799 審査がどのように進められるのか、また認証取得に向けて何を想定すべきかを実際に示すために審査のロールプレイ（実演）が行われた。この実演での審査対象企業は､「Trust-4U」という名称の架空の信託サービス会社で、その設定は次の通りである。

Trust-4U は、ロンドン本社とリバプール支社の 2 つのオフィスをもち、従業員数は 200 名だが、現在拡張を計画している。この企業のビジネスタイトルである「Trust」という語に示すとおり、この会社は次の 3 タイプのサービスを提供している。それは、デジタルキーパッドを組み込んだ特別設計のドアロックのような物理的セキュリティ機器の開発・導入・維持、現地警備員や現地外の警備要員といった形でのセキュリティスタッフの提供、保管サービスの提供である。

Trsut-4U は､ある主要顧客から強い要望があったため、またCEO が 7799 の認証は市場において優位となるとみなしたため、認証を取得することにした。

この審査のロールプレイの実演者

- Trust-4U チーム
  - **CEO（Willie List）**
  - **Head of Security（警備責任者）（Vernon Poole）**
  - **Head of IT Services（IT サービス責任者）（David Brewer）**
  - **Head of Human Resources（人事責任者）（Jason Parker-Smith）**
- 認証機関チーム
  - **Lead Auditor（主任審査員）（David Watson）**
  - **Auditor/Technical Expert（審査員／技術専門家）（Angelika Plate）**

この実演は、既にステージ 1 審査は実施され、認証機関が Trust 4U はステージ 2 審査を受ける準備が十分整っているという結論に達したと仮定して始まった。またこの実演は、7799 審査の代表的な 3 つの場面に分けて行われた。

場面 1 － The opening meeting（初回会議）

始めに、どのように審査が実施されるのかについて審査員が説明的なプレゼンテーションを行い、Trust-4U の CEO が企業説明と 7799 認証取得を決定した理由の説明を行った。

審査員は、CEO がどれだけ ISMS の適用範囲を理解しているかについてと､ISMS 実施に対する CEO のコミットメントについて確認を行った。また、ISMS 基本方針の完成度について議論し、ISMS の適用範囲を確認した。ここで明確にされた重要なポイントは、ISO 9001 登録証が、検討される ISMS の適用範囲の全てを含んではいない場合に、どの程度 ISO 9001 認証に頼ってよいか、ということである。

場面 2 － The audit walk about and interviews（訪問審査と面談）

続いて､IT グループと人事部のセキュリティ体制に

関しての審査が行われた。

この部分の審査において、次のポイントが浮上した。それらは、管理策の完全な実施、全体的なセキュリティ解決策に関連して Trust-4U 内の特定の場所のために実施されているセキュリティ体制の関連、職務分離の適切な実施、リスクアセスメントと実施される管理策との関連、及び従業員の Web の使用状況と email 使用状況の合法的な監視である。また審査のこの場面では、Trust-4U が大きく依存している、様々な第三者セキュリティ対策を定めた重要な契約書の所在が確認できなかったことが明らかにされた。

場面 3 － The closing meeting（終了会議）

この場面は、調査結果に関する、審査員と技術専門家間との協議から始まった。この協議では、いくらかの軽微な不適合（不完全な ISMS 基本方針など）や観察事項と、ある契約書が見つからないという重大な不適合がとりあげられた。次に、これらの調査結果について当該組織と協議し、この協議中に CEO がその契約書をブリーフケースにしまっていたことが分かり、この重大な不適合は文書の取扱いに関する改善についての観察事項に変更された。

審査員らは、認証機関に対し、Trust-4U がこれらの不適合の処理方法についての詳細な計画を明示した後に、Trust-4U に対して登録証を授与すべきだと提言するという結論に達した。

このセッションの最後では、このセッションで生じた問題が議論された。特に鋭い質問として、「審査員が、不適合を立証するために策を講じることは許されるのか？」というものがあった。識者ら（Panel）の回答は、圧倒的に「できない（No）。」だった。この最終セッションでは、聴衆が 7799 審査の情報を、こういった形で提供することを高く評価していることが示された。また、2003 年ロンドン開催の 7799 Goes Global カンファレンスに先行して実施されるものなど今後のマスタークラスでは、この好評を博した形式を採用してく予定である。

Dr. Angelika Plate (AEXIS Consulting, Germany)

THIS MONTH'S ARTICLES（今月の特集）

Spotlight on Incidents（事件・事故に着目する）(Part 2)

この特集は 2 部構成であり、今回この第 2 部では、Dr. David Brewer が新たに改訂された BS7799 Part 2:2002 の観点から、セキュリティ事件・事故について馴染みのあるトピックの分析をまとめる。

他の組織に影響を及ぼしている事件・事故については、ニュースグループや the 2002 DTI Security Breaches Report（2002 年度 DTI セキュリティ違反報告書）などの出版物を通してよく知られている。前回は、「では、そのようなことはあなたの会社にも起こり得るのか？もしそうならば、それは問題となり得るか？」という疑問を提起した。今回は、この２つめの質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。

BS 7799-2:2002 の 4.2.2(g)では、セキュリティ事件・事故を迅速に検出し、これに対処できる手順や他の管理策を実施するよう組織に要求している。一方、ISO/IEC 17799:2002 では、事件・事故への対処についてのみしか言及していない（例えば、6.3、8.1.3、11 等）。その為、セキュリティ事件・事故とは、たまたまそれらに気づいた者によって単に観察されるにすぎない事象なのだと見なされているように思える。ここでは、一度も検出されたことがないために誰も対処していない事件・事故は存在し得るのだろうか、という問題がたくみに避けられている。「イエス」という答えは、完全犯罪を意味する。それどころか、Barings、Enron、Allied Irish Bank など、顕著なケースでみられるように、一度も検出されたことのない軽微な事件・事故は数多くあり、ついにはこれらが誰も無視することのできないだろう一つの壊滅的な事件・事故となるのである。従って、BS 7799 Part 2 新版が事件・事故を検出し、かつそれらを迅速に検出する必要性に着目しているのは、非常に適切なことなのである。

事件・事故を検出するための手順や他の管理をもつには、何を探すのかを知っていることが前提である。これは非常に困難な仕事のように思われるが、極めて重要なことであり、実際に少々の事前の考慮と水平思考を行うことによって多くの場合達成されているのである。確かに、このセキュリティ事件・事故にはどのようなものが考えられるかが明確にされていない場合、あなたの会社のリスクアセスメントが不完全なものだということが激しく議論される可能性がある。他者に起こっていることに注意することによって、この分野における自らの考えを広げることができるのである。

会合へ公文書を持っていくための「セキュアな」レザー・ブリーフケースについて、「このレザーケースを

破るのは簡単だ。－ 鋭いナイフがありさえすればいい。」という見解があったのを覚えている。しかし、この場合ナイフで切ったという事実を隠すことは不可能だろう。別の例は James Bond の映画「Dr. No」にみることができる。この映画のなかでは、有名なスパイが自分の髪の毛を 1 本抜いて、鍵をかけたブリーフケースのしまってあるクローゼットの枠とドアの間にこの髪の毛を貼り付けていた。どちらのケースでも、セキュリティ設計者は、予防、検出、抑止、復旧という従来のサイクルを、検出を最初に持ってきて配列し直している（図 1 参照）。ここでの原則は、もし検出できないならば、セキュリティが損なわれたかどうか知りえない、ということである。セキュリティ侵害を確実に検出できるようにするというステップの次には、予防策を講じるというステップがくる。この予防策とは、例えば上記の 2 つの例の場合では、より強固な鍵やより硬い素材のブリーフケースを使用するといったものである。

上記のことは、計画段階の初期において、我々は「事件・事故が起こったことをどのようにして検出できるか」と問うべきだということを示唆しているのだ。

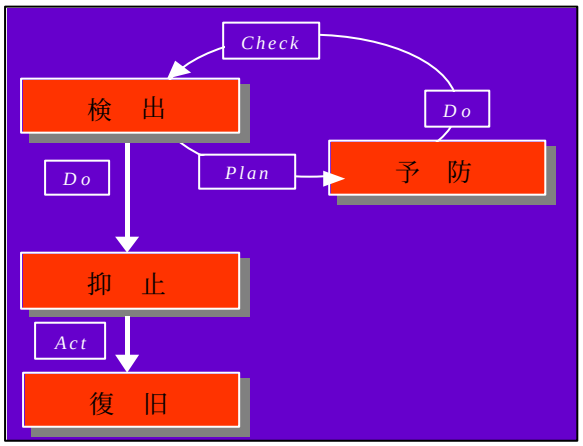

図 1： 予防の前に検出を考える

私が初めて ISMS のための審査スケジュール案作成に取り組んだ時、これがソフトウェア設計と似ていることに気づいた。ソフトウェアエンジニアとしての訓練の一部には、設計の早い段階で試験実施について考えるというものがあった。ここでは、「V」モデルが使用され、このモデルによって要求事項仕様が作成され、顧客受け入れ試験仕様が作成された。次の改良段階では、システム設計、システム試験仕様、顧客許容試験手順（少なくとも草案の形で － 「V」モデルは低い層で設計や試験を行った際に検出された、高い層における障害を修正するための反復を可能にする）が作成された。要するに、試験は追加部分というよりもむしろ、設計の不可欠な構成要素となっているのである。この概念を用いて、各節を自身の ISMS 基本方針に取り入れ、基本方針の表明が満たされていることを確認するために何をすべきかを引き出した。この結果、次の事項が得られた。

- 基本方針の表明と直接的に対応する審査要求事項
- いくつかの手順又は他の管理があるという論拠。
- これらの手順や他の管理策が実施され、有効に作用していた、又はしていなかったことを証明するのに必要な証拠。

この結果は図 2 に示されている。

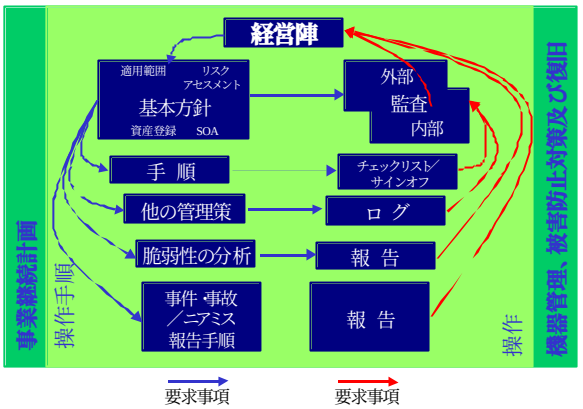

図 2： 事件・事故検出の計画

脅威分析（vulnerability analysis）と事件・事故／ニアミス報告（incident/near miss reporting）という優れた手順に注目して欲しい。この 2 つは両方とも、「他者からの学習」（Learning from Others）（この記事の Part1 参照）と事件・事故の検出（incident detection）についての BS7799-2:2002 要求事項の作成に大きな影響を与えた。また、セキュリティ手順（security procedures）が運用手順（operational procedures）に組み込まれ、その結果事業継続計画（Business Continuity Plan）に組み込まれていることに注目して欲しい。ここでの目的は、情報セキュリティをビジネスの不可欠な部分とすることであって、何らかの補足的な追加部分とすることではない。

話はリスクアセスメントまで戻るが、BS7799-2:2002（例えば 4.2.1 項）では、識別した各リスクをリスク対応計画で採用した手段によって受容可能なレベルまで低減するよう要求している。これは、管理策の導入、リスクの回避、リスクの移転、又は単にリスクの意識的な受容を行うことによって等、様々な方法で達成することができる（4.2.1(f)参照）。The Institute of Chartered Accountants in England and Wales (ICAEW)（イングランド・ウェールズ勅許会計士協会）は、企業統治に関する自身の見解を説明するうえで、「inapplicable risk」（適用外リスク）という概念を導入している。「inapplicable risk」とは、及ぼす影響は壊滅的だが起こりそうにないリスク、又は頻繁に発生するがその影響はさして重要でないリスクのことである（図 3 参照）。ICAEW は、ある企業が、決して総勘定元帳に転記されることのない、用途を問わない現金払い用の償却費を年間 £5,000 用意している

という一つの事例[1]を挙げている。この企業は、これは inapplicable risk（すなわち受容されたリスク）だと強く主張しており、従ってさらにリスクアセスメントを考慮する際にはこれを除外している。結果的に、このリスクに対処するための管理策は実施されていない。この誤りは、やはり例にもれず、正しい質問を行わなかったことにある。このケースでは、正しい質問とは、「£5,001 を失うリスクは受容できるか？」である。私の考えでは、この答えは「ノー」だと思う。でなければ、受容できるリスクのためにより高い上限を設けておくべきだった。それ故、£5,000 という限界値に至った場合を検出するための管理策が必要なのである。この手段を含めることができなかったということは、受容できるリスクが突然、受容できないリスクになった場合にそれを検出できないことを意味するのである。

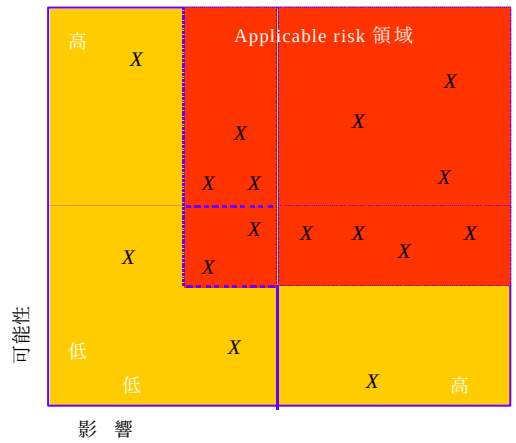

図 3：Applicable risk と inapplicable risk

要約すれば、セキュリティ事件・事故の検出を実施する必要があり、かつこれを効果的に行うためには、このセキュリティ事件・事故が実際に起こった場合のための計画を立てなければならないのである。計画の立案は、リスクアセスメントの段階で行われる。管理策が実施されており、かつ有効に作用していることを確実するために必要な証拠を識別するには、「V」モデル概念を使用すべきである。また、受容リスクが受容できないリスクに変わった時点を決めるための管理策を実施していることを確実にすべきである。

ISO/IEC 17799:2000 では、たとえ事件・事故を検出するという目的に特化した手順があったとしても、その事件・事故に対処するのは常に人間なのだ、ということが示唆されている。これは、必ずしもいつもそうであるとは限らない。というのは、対処は自動化できるからである。例えば、技術的な事例として、攻撃を防ぐためにルーターやファイアーウォールのプログラムを作り直すことのできるネットワークの侵入検出システムがある。また混合型の事例としては、「trouble tickets」を適切な支援チームに送り、修復作業を要請し、この作業が行われ問題が解決されたかどうかを追跡するネットワークのマネジメントシステムがある。問題が解決されていない場合には、さらに trouble ticket を送り、問題は自動的により高いマネジメント権限へあげられていく。他にも、2002 年 9 月にロンドンで開催された 7799 Goes Global カンファレンスにおける atsec GmbH の Helmut　Kurth で報告された Vodafone の「ISMS Security Monitor」では、この両方の技術に関する優れた事例が紹介されている。これら３つは全て自警手順（self-policing procedures）の事例であり、これらには段階的拡大の概念が取り入られている。自警手順（BS 7799-2:2002　B4.3 参照）とは、これを実行している間に生じた誤りや障害を、迅速に検出できるよう構築された管理策のことである。従って、自動化された是正処置では、上述した侵入検出器の場合のように、次に起こるかもしれないもの全てのリスクを受容可能なレベルまで低減するのに、そのような処置を講じる必要があるか否かが問題となる。これは、たとえ事件・事故の対処にあたるのが人間の場合でも、常にそうでなければならない。処置は、同じ事件・事故の再発を含む、次に起こるかもしれないリスクを受容可能なレベルにまで低減するためにだけ必要とされる。

次号の ISMS ジャーナルでは、自警手順についてさらに深く掘り下げて議論する。

Dr. David Brewer (Gamma Secure Systems Ltd)

Audit and Certification　（監査{審査}と認証）(Part 2) － Accredited 3rd Party Audits（認定を受けた第三者認証）

この監査（審査）に関する連載の第一回目では、様々な種類の監査（審査）、監査（審査）の範囲、監査（審査）に関するビジネス上の背景など、監査（審査）全般を概観した。今回第二回目では、認定を受けた BS 7799 認証に関する第三者審査の詳細について述べる。

Certification Bodies（認証機関）

認証機関（Certification Body = CB）は、BS 7799 の第三者認証審査を行う。ISMS 認証サービスを実施するためには、認証機関（CB）は国際的な要求事項及び基準に従って、認定機関（例、英国では UKAS、スウェーデンでは SWEDAC、ドイツでは TGA。－ 欧州の認定機関リストは

[1] “The Auditing Practice Board – Briefing Paper – Providing Assurance on the Effectiveness of Internal Control” 2001 年 6 月、ISBN なし。ABG Professional Information (PO Box 21375 London WC1N 1QP)より入手可能。

http://www.european-accreditation.org を、世界各国の認定機関リストは www.iaf.nu を参照）による審査を受けて認定されなければならない。現在、ISMS 認証サービス実施について認定された認証機関は、世界中で 23 機関以上ある（最新版リストについては www.xisec.com 参照)。

ISO Guide 62（及び EN 45012）は、認定についての一般要求事項及び基準を定めたものである。これらの文書は、ISO 9001 品質マネジメントシステム、ISO 14001 環境マネジメントシステム、BS 7799 Part 2 ISMS、及び他のマネジメントシステムを規定する審査基準となり得る規格について認証審査を実施する認証機関（CB）に適用される。

また、ガイドラインである EA 7/03 では、特に ISMS 審査との関連において Guide 62（EN45012）の要求事項を解釈し、拡充している。これらのガイドはまた、認証機関（CB）に雇用されている審査員に対し、審査プロセスの計画、実施、運営方法を定めた ISO 19011 規格に記載の、審査に関する関連ガイドラインに適合するよう要求している。

Auditor Competence and Qualifications（審査員の力量及び資格）

認証審査プロセスに対する信頼や信用は、審査を実施する審査員の力量にかかっている。Guide 62 及び EA 7/03 は、認証機関（CB）に対し、審査を効果的かつ均一的に実施できるようにするために、自らが保有していなければならない情報セキュリティマネジメントの必要な力量を分析し、かつこのような力量を有する審査員を選定できる適切なシステムをもつことを要求している。審査員の力量に関する一般基準は ISO 19011 に規定されており、これは学校教育、業務経験、審査員研修、審査経験から得られる各種の知識や技量を活用する能力の証明に基づいている。

審査員は、継続的専門能力開発（continual professional development）プログラムを通して、また定期的に ISMS 審査に参加することによって、自らの力量を高め、維持し、かつ改善していくことが期待される。

IRCA は、ISO 19011 に基づいて審査員認証に関する一連の基準を定めた。この基準は、ISMS 審査員又は ISMS 主任審査員として認定されるために、学校教育、業務経験、審査員研修、及び審査経験の点から審査員が満たさなければならない必要最低限の要求事項を定めている。

Certification Scope（認証範囲）

ISMS の適用範囲は、認証取得希望組織が定める。この適用範囲が、当該組織のビジネスに合致しているかということ、またリスクアセスメントと関連する規制要求事項によって定めたセキュリティ要求事項を満たす情報セキュリティの提供についての、組織の能力及び／又は責任に影響を及ぼす、組織の運用を何も除外していないかということをチェックするのが、認証機関（CB）の役割である。

従って、認証機関（CB）は、BS 7799 Part 2 規格に定めるように組織の情報セキュリティリスクアセスメントが当該組織の活動を適切に反映しており、かつ組織の活動範囲全体に及んでいることを確実にすべきである。また、認証機関（CB）は、これが組織の適用宣言書の中に反映されていることを確認すべきである。

ISMS が適用範囲内に完全には含まれていないサービスや活動と連動している場合、この連動に関連するリスクも、やはり当該組織の情報セキュリティリスクアセスメントに含めるべきである。

Audit Process（審査プロセス）

組織の BS 7799 Part 2 規格の情報セキュリティマネジメントシステム（ISMS）認証には、２つの審査プロセスがある。

Stage 1（ステージ1）

この審査ステージ期間では、認証機関（CB）は ISMS の設計及び実施に関する文書の審査を行う。これには、少なくとも ISMS 適用範囲の定義、ISMS 基本方針、リスクアセスメント報告、及びリスク対応計画、適用宣言書、並びに ISMS の核を成す要素（core elements）を含めるべきである。この審査によって、審査員らは組織の ISMS の適用範囲、基本方針、及び設計を理解することができ、従って審査計画において何に焦点をあてるべきかがわかる。またこの審査によって、当該組織では審査に対する準備がどれだけ整っているか目安をたてることができる。この文書審査が終了し審査報告書が作成された後、認証機関（CB）はステージ２審査へ進むかどうか決定する立場にたつ。次のステージに進む前に、認証機関（CB）は組織固有の ISMS 適用範囲の審査を処理するために必要な力量を有する

審査チームを召集しなければならない。

Stage2（ステージ2）

この審査ステージ期間では、認証機関（CB）の審査チームは ISMS 適用範囲内の組織の事業所（site）を訪問する。この審査ステージの目的は、当該組織が独自の基本方針、目標、及び手順をもち、維持していることを確認すること、また当該組織の ISMS が BS 7799 Part 2 規格の全ての要求事項に適合しており、かつ組織の基本方針目標（organization's policy objectives）を達成していることを確認することである。

これらの目標が満たされていることをチェックする際、審査チームは、組織の情報セキュリティに関連するリスクのアセスメント、その結果として生じる ISMS の設計と適用宣言書に重点を置く。審査チームはまた、このプロセスから得られる目標及び目的、並びにこれら目標及び目的に照らした業務の監視、測定、報告、レビューを行うために何を実施しているかを考慮に入れる。この審査には、セキュリティ及びマネジメントレビューが確実に実施されるようにするために、また内部 ISMS 監査プロセスが確実に実行されるようにするために、何が運用されているかについての審査も含まれる。また、情報セキュリティ基本方針に関して、どのようなマネジメントの責任が定められ、履行されているかも含まれる。

この審査の重要な側面は、情報セキュリティ基本方針、リスクアセスメント結果、セキュリティ目標及び目的、情報セキュリティに対する責任、そして管理策及び手順のシステム間のつながりを明示するため、かつ業務の監視及びセキュリティレビューの実施のために何が行われているかを明示するために、客観的証拠を提示させ調査することである。

Nonconformities（不適合）

BS 7799 Part 2 の場合、不適合とは、一つ又は複数の要求される ISMS 要素が欠落しているか若しくはこれを実施・維持することができないこと、あるいは組織のセキュリティ基本方針及び目標を達成する ISMS 能力に関して、客観的な証拠に基づいた重大な疑問が生じることである。

認証機関（CB）は、不備（deficiency）のレベルと改善領域を定義することができる（例えば、Major [重度] 又は Minor [軽微] な不適合、Observations [観察事項] 等）。しかしながら、このような不備のレベルは全て、不適合の定義と同じであり、Guide 62 及び EA 7/03 基準の規定に従って処理すべきである。

Audit Report and Decision on Certification（審査報告及び認証に関する決定）

審査チームは、BS7799 Part 2 規格の全ての要求事項に対する組織の ISMS の適合について、調査結果の報告書を認証機関（CB）へ提出するよう要求される。BS7799 Part 2 規格の全要求事項に適合するために是正すべき不適合全てについて、速やかに当該組織に通知すべきである。認証機関（CB）は、組織に対し、報告書について意見を述べ、かつ不適合を改善するために定められた期間内に組織が実施を予定している特定の是正処置、又は組織が実施を予定している計画について、説明するよう求めなければならない。このようなフォローアップ処置の終了には、ISMS の全体的な再審査又は部分的な再審査が必要なこともあり、あるいはサーベイランス期間中に書面による宣言を確認することが適切だとみなされることもある。

この報告書には、審査した ISMS 要素の識別、評価を実施した審査対象の ISMS 適用範囲、不適合について明確な記述のある規格の要求事項に対しての組織の ISMS の適合に関する意見、及び適切な場合には、当該組織の前回の審査結果との有用な比較を含めるべきである。

当該組織の ISMS に対して登録証を授与するか否かの決定は、審査中に収集した情報、審査報告書、及び他の関連情報に基づいて認証機関（CB）が行わなければならない。認証決定者は、当該 ISMS 審査に参加した者であってはならない。

Award of Certificate（登録証の授与）

組織に授与される登録証には、当該認証機関（CB）を認定した認定機関のロゴ及び認証機関（CB）のロゴが記載される。

Surveillance Audits（サーベイランス審査）

認証機関（CB）は、認証された組織の ISMS が継続して BS7799 Part 2 規格の要求事項に適合していること、及び当該 ISMS が組織の情報セキュリティ基本方針の目標を達成するのに引き続き有効なことを検証するのに十分に近い間隔で、定期的なサーベイランス審査を実施する。またこの審査では、前回の審査期間中

に識別された不適合に対して組織のとった処置を審査すべきである。

サーベイランス審査期間中に不適合が発見された場合、これらの不適合を認証機関（CB）の合意した期間内に有効に是正しなければならない。不適合の是正がこの合意期間中になされなかった場合、認証は縮小、一時停止、また時には取消さなければならないこともある。是正処置実施のために与えられた期間は、不適合の深刻度に合致しているべきである。

ISMS 規格 BS7799 Part 2 では、管理策、プロセス及び手順の ISMS システムが、当該規格や関連する法令及又は規制の要求事項に適合しているか、識別された情報セキュリティ要求事項に適合しているか、有効に実施されているか、有効に維持されているか、そして予測通りに機能しているかを判断するために、あらかじめ定められた間隔で ISMS の内部監査を組織が実施することを求めている。審査プログラムは、審査対象の ISMS プロセス及び領域の状態と重要性のほかに、前回の審査結果を考慮に入れて作成しなければならない。

Re-certification（認証の更新）

認証の更新は、通常、3 年に 1 回行われる。その目的は組織の ISMS が全般的に BS7799 Part 2 規格の要求事項に継続して適合しているか、及びその ISMS が適切に実施され維持されているかを検証することである。

認証の更新及びサーベイランス審査プログラムには、通常、次の事項を含めるべきである。

- 認可された ISMS が継続して実施されていることの検証。
- 組織の運用を変更した結果として生じる、管理策の ISMS システムに対する変更の影響の検討、及び運用の変更の点から ISMS の有効性全般を完全に確保すること。これには、ISMS の文書化されたシステムに対する変更を含む。
- BS 7799 Part 2 の要求事項に継続して適合していることの確認、及び ISMS の有効性と全 ISMS 要素間の有効な相互作用を維持しているというコミットメントの明示。
- ISMS 内部監査、内部セキュリティレビュー、マネジメントレビュー、予防処置及び是正処置という、システム維持の側面。

BS 7799 Part 2 規格の規定する PDCA モデルに基づいた ISMS プロセスは、継続的改善のプログラムを理解するために、組織に対しマネジメントの枠組みを提供するものである。これよって、組織が、ビジネスにおける共通の利益及び統治に関して有効であり、かつ上述した認証の更新及びサーベイランス審査活動の目的にもあった ISMS をもてるようにすべきである。

Ted Humphreys

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

Mobile Computing（移動型計算処理）

前回は、情報革命によって情報労働者－主に実体のない情報を扱う仕事に従事する者や必ずしも事務所や工場などの特定の場所に縛られる必要のない者－の膨大な増加がどのように生じたかについて論じた。そのような者達は、必ずしも従来のオフィス環境におけ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。

ISO／IEC 17799 の 9.8 項では、遠隔作業（teleworking）と移動型計算処理（mobile computing）という２つの主題に分けて、特にこのような労働者を対象とした助言を提供している。前回は、遠隔作業 －決まった場所で働いているが、組織の通常の管理下にない者のための情報セキュリティ－ について述べた。今回は、この規格のなかで移動型計算処理と呼ばれている、持ち運びのできるコンピュータ機器を取り扱った、9.8 項中のこのもう一つの主題を考察する。

ISO／IEC 17799 の定義では、移動型計算処理は、組織の敷地内外、ネットワークへの接続の有無を問わず、あらゆる形式の輸送できる情報機器の使用を含む。従って、この移動型計算処理は、一般に移動型計算処理として理解されている意味（第三者の供給する無線リンクを通して組織のインフラに接続される、持ち運びのできる機器{portable device}の使用）のほかに、ワイヤレスコンピューティング（一般に、その支援インフラの全要素が組織の管理下にある、あらゆる形式

の固定されていない連結ネットワークとして定義されている）を含む。特に、公共の場所でのスタンドアローンの機器の使用や輸送が、この移動型計算処理のなかに含まれる。

このように広範な範囲に及ぶにも関わらず、ISO/IEC 17799 は、あらゆる形の移動型計算処理から考慮するのに有効なリスクチェックリストを提供しており、様々な管理策が個々の状況のために識別されている。公共の場所では、実際には重大な脅威は、状況に関係なく、通常、設備の盗難やその結果であることに留意して欲しい。盗まれた設備の代わりを設置しなおさなければならないだけでなく、消失した情報をもう一度作成するために時間と労力がかかり、何よりも悪いことには、パスワードや他のネットワークアクセス管理が危険にさらされるからである。

しかしながら、BS7799-2:2002 の引用附属書のなかには、移動型計算処理についてはたった一つの管理策、すなわち正式な基本方針及び適切な管理策を実施すること、としか規定されていない。これはもちろん、ほぼ間接的な要求事項に近い！そのため、情報セキュリティ管理者（Information Security Manager）には２つの選択肢しかない。持ち運びのできる機器を禁止しなければならないか、そうでなければ特別な管理策を必要とする特別なリスクを識別するために、特別なリスクアセスメントを実施しなければならないかである。この他に何が適切かを見出す方法はない。

悲しいことに、未だにモバイル機器の多くには内蔵する情報を保護するための適切なセキュリティが備わっておらず、また多くの組織はそのため、内蔵のセキュリティモデルが改善されるまでは携帯情報端末（PDA－Personal Digital Assistants）などの機器の業務上の使用を全面的に禁止することを望んでいる。また、線（wires）がないことによってあたかもセキュリティ上の脆弱性が見えなくなったかのように、システムアドミニストレーターがワイヤレスネットワークのセキュリティ上の特徴を無視するか、又は無効にするという残念な傾向もある。ここでもまた、組織の多くはデジタル携帯電話以外のワイヤレステクノロジー全てを全面禁止することを望むだろうと思われるのである。

これは BS 7799-2:2002 の PDCA モデルにどのような影響を与えるのだろうか。*計画*段階（*Planning* stage）においては、望ましいモバイルテクノロジーや環境を識別し、特別なリスクアセスメントを実施する必要がある。*実施*段階（*Do*）においては、特別な管理策を実施しユーザー慣習（user practice）を確立する必要がある。例えば、ワイヤレス LAN の到達距離を試験し、コンフィギュレーションデータが適切に隠されているかチェックする必要があるかもしれない。*点検*（*Check* ）活動は管理策が継続して適切であることを確実にするのに不可欠である。すなわち作成者は、メンテナンス技術者がパスワードやアクセスオプションを初期化して初期値に戻ってしまったりしたことによってセキュリティが破壊されている箇所について移動業務（mobile services）を調べる。最後に、*処置*段階（*Act*）においては、リスクアセスメントが無効であるか又は無効になったことが、文書化された、移動に係るセキュリティ違反数やその性質によって示された場合、予防処置が必要となることもある。

これら全てには、豊かな良識を伴うことが必要となる。移動型計算処理は、依然として、セキュリティ意識とベストプラクティスに関するユーザー訓練が最良な分野である。また、盗難や関連設備の再購入費を減少させることによって、失った情報セキュリティ費を考慮しなくてもおそらく迅速な費用対効果（payback）が得られるであろう分野でもある。ラップトップコンピュータ、電話や他のモバイル機器は通常、内蔵されている情報ではなく、これらを消去して機器自体を売る目的から盗まれる。また、ネットワークのパスワードは、ワイヤレス妨害や WEP 暗号クラッキングよりも、盗まれたラップトップのケースの中にあったメモが見つかることや公共の場所でネットワークにエントリーするところを誰かに見られることによって損なわれる可能性の方がはるかに高い。

多くのモバイル製品は、安全でない「out of the box」であるか、又はこれら製品にはユーザーや切羽詰ったセキュリティ実施者やネットワーク維持技術者によって、簡単に、多くの場合故意でなく停止され得るというセキュリティ上の特徴がある。製造者の多くは、今なお元々それ自体がセキュアでなく、ユーザーや IT（情報技術）部の行為に関係なく安全を確保できないモバイル機器を提供している。多くの組織は、たとえ固定リンクからの無許可の外部アクセスを防ぐために膨大な資源を投入している場合でも、ワイヤレスを対象とした攻撃（compromise）に対しては、最も単純なものに対してさえ依然として脆弱なままなのである。移動型計算処理は、潜在的なアキレス腱なのであり、そのように取り扱われなければならない。これを特別のリスクアセスメントとせよ！

Dr. Mike Nash (Gamma Secure Systems Ltd)

Tao-Zen Practice and The Art of A Holistic Balanced View[2]（Tao-Zen practice [道教・禅思想の実践]と全体的な、バランスのとれた物の見方）

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 つの記事のうちの、第２部である。

The business environment（ビジネス環境）

PDCA モデルの計画（Plan）段階は、各組織のビジネス状況に適した ISMS の確立に関するものである。BS 7799 Part 2 に規定するプロセスでは、ISMS を実現するための計画について述べている。ISMS を自らのビジネスに適切なものとするためには、この ISMS を、存在する連動（interface）、外部依存や満たすべき要求事項、内部及び外部のリスク状況の十分な情報に基づいた世界的な観察情報、ビジネス状況の客観的見方といった、自身のビジネス環境を全体的に観察した適用範囲とともに定める必要がある。組織の ISMS はおそらく他のシステムと連動しており（interface）、これらのシステムを通してリスクが自らのビジネスにもたらされるかもしれない。ネットワークインターフェースはごく一般的な例だが、他にも毎日の操作インターフェースがあり、これも検討する必要がある。ISMS は組織の一部のみにすぎないかもしれなく、そのため他の事業体との連動（interface）が存在する可能性がある。ISMS はまた、顧客や供給者のシステムと連動させる（interface）必要があるかもしれない。ISMS のインターフェースのセキュリティは、ネットワーク管理、SLA、契約や他の手段によって実現される。リスクアセスメントが適切で組織のビジネス状況に合うようにするには、リスク環境を全体的な視点からみることが必要なのである。

何を保護する必要があるかについてさらに調べるためには、情報それ自体を含む、自身のビジネス情報に関連する ISMS の適用範囲内の資産全てを識別すべきである。こういった資産には、情報処理やストレージシステム、ビジネスプロセス、商標名・登録商標、知的所有権、イメージや評判、組織の労働者、配備されている情報システムに関連する物理的資産、使用又は提供されているサービス、及び自身の ISMS に固有の他の資産全てが含まれる。

自らのビジネスが所有する資産のなかで何が最も重要な資産かを決めるために、資産の実用性又は価値を識別する必要がある。この「価値」（”value”）は、当該資産のもつ財政的価値、有用性及び他の利便性を示すべきものである。資産評価の方法は千差万別であり、ここで留意すべきことは自らの組織に最も適した方法を選択するということである。

Opposing forces（マイナスの影響力）

ISMS の適用範囲と基本方針表明を定めて作成し、当該 ISMS における資産を識別した後、このプロセスにおける次のステップは、自らのビジネス環境に対するマイナスの影響力（opposing forces）を調べることである。これには、当該 ISMS 資産に対するリスクの識別（identifying)、アセスメント（assessing)、及び評価（evaluating）が含まれる。ビジネス情報が直面するかもしれないリスクは数多く、また組織ごとに異なる。そのため、情報セキュリティを適切で自身の組織のニーズに十分に合ったものにするためには、自らのビジネスに固有かつ関連のあるリスクを識別することが必要となる。

当該 ISMS の適用範囲に固有の脅威及び脆弱性は、マイナスの影響力を調べる際に重要な役割を果たす。自らのビジネスを妨害するかもしれない作用について調べるためには、資産を脅かすものやそういった脅威の発生を可能にするもの、つまり脆弱性を理解することが重要なのである。脅威及び脆弱性を識別する際には、これら全てはマネジメントの実践であり、過度の技術的詳細はアセスメントには役立たないであろうことに留意して欲しい。ISMS の適用範囲に固有の様々な脅威や脆弱性に対して先入観をもたないこと、かつ当てはまる技術的、人的、手順的、物理的脅威及び脆弱性に関して、一貫したアセスメントを保有していることが、より重要である。

マイナスの影響力を調べる際の他の重要な要素は、事件・事故の発生頻度を調べることである。ここでもまた、これらの脅威と脆弱性が一体となってセキュリティ事件・事故を引き起こす可能性について評価を試みる方法は様々である。処理が楽で自身の ISMS の適用範囲内で容易に適用できるアプローチは全て選択すべきである。脅威及び脆弱性に関するアセスメントへの有益なインプットとは、ユーザーインタビュー、事件・事故報告書、審査報告書、監視活動の結果、及びそれ以外の自身の ISMS における個々のセキュリティ状況について情報を与えてくれるもののことである。

[2] “Tao-Zen Practice and The Art of Information Security Management”を扱った一連の記事（Ted Humphreys、2001 年 XiSEC 発行）からの抜粋。

Making a Management Decision（マネジメントの決定）

正しいマネジメントの決定を行うためには、ISMS の適用範囲における資産が直面している、最も深刻なリスクについての概念をもっておく必要があり、これまでに収集した情報がこのために使用できる。これらのリスクについては、自身の資産の重要性と事件・事故が起こる可能性に基づいてリスクアセスメントを行うことができる。これらの価値を組み合わせる方法は様々であり、自らの ISMS に関連する方法を選択すべきである。これらのリスクは、その後、深刻度に従って分類できるため、これによって高い優先順位で処理すべき、最も深刻なリスクの優れた概観が示される。

リスクアセスメントの実施後は、当該 ISMS において最も効率的に様々なリスクを処理する方法を決める。リスク対応には次の 4 つの選択肢がある。

- 適切な管理策を適用することによってリスクを低減する（下記でも更に詳しく述べる）。
- 他のリスク対応の可能性を考慮したうえでの意識的な決定だという条件のもとで、リスクを受容する。
- 例えば、リスクを伴うある特定のビジネス活動を行わないことによって、リスクを回避する。
- 関連ビジネスリスクを、例えば保険業者、供給者といった他者に移転する。

識別された各リスクについて、適切な選択肢（又は選択肢の組合せ）を識別すべきである。リスク対応について考える場合、完璧なセキュリティは存在しないのであり、また多くの場合それは最も望ましい解決策でさえない（というのもそのためには妥当な度合いをはるかに越える、多くの資金と資源がかかる可能性があるからである）ことに留意すべきである。

Selecting Controls（管理策の選択）

あるリスクへの対応にあたってリスクの低減がもっとも良い選択肢だと決定した場合、そのリスクを受容可能なレベルまで低減するための管理策を識別すべきである（この受容可能なレベルは ISMS の適用範囲に関して定めるべきであり、経営陣はこれに同意すべきである）。これがいつも可能とは限らないことに気づくだろうが、しかし特定のケースにおいては少なくとも実現可能な程までにセキュリティを改善することができる。

適切な管理策を見出すには、リスクアセスメントの結果から有益な情報を得ることができる。リスクアセスメントは、なぜある特定の資産が保護を必要とするのか（その重要性、有用性、又は価値）、どういった事件・事故（特定の脅威と脆弱性が一緒になった）がリスクを引き起こすのかを教えてくれる。この情報に基づいて、BS 7799 Part 2 の附属書 A、あるいは資産の保護や脆弱性の低減に役立つか、又は脅威の起こる可能性を低減する他の資料から、管理策を選択することができる。

管理策を選択するにあたって、自身の ISMS の適用範囲内で一貫した総合的なセキュリティを実現する唯一の方法は、異なる管理策を適切に組み合わせてそれを維持することである。例えば、完全な保護を実現するためには、

- 技術的管理策（例、ファイアーウォール製品）。
- 手順上の管理策（例、ファイアーウォールへのアクセス権及び規則の実施、運用、更新手順）。
- 人的管理策（例、そのファイアーウォールを実施する能力のある人員育成訓練）。
- 物理的管理策（例、ファイアーウォールのアクセス権の物理的保護）。

といった管理策を組み合わせなければならない。

Linking it all together（全情報の関連づけ）

全てのマイナスの影響力を評価した（assess）後、次に情報全てを関連づけ、適用宣言書（the Statement of Applicability）のなかに集約する。適用宣言書（SoA）には、選択した管理策全て（BS 7799 Part 2 の附属書 A から選択したもの、及びその他の規格等から選択された他の管理策全て）が記録される。これに加え、適用宣言書（SoA）には BS 7799 Part 2 の附属書 A に記載の管理目的及び管理策の除外も盛り込むべきである。

しかし管理策及びその除外の記載よりも重要なことは、これらの情報を、資産やリスク、それに ISMS 基本方針案の作成の際に行った決定と、リスクアセスメント後に行った決定に立ち戻って関連づけることである。選択した管理策の場合は、その管理策がどの資産のために選択されたのかとその理由、すなわちどのリスクを低減すべきなのか、そしてどのリスク対応の決定がなされたのかを示すべきである。同様に、選択しなかった管理策の場合は、なぜ特定の管理策が必要でないのか、リスクアセスメント結果を用いてこの除外の正当性を示すべきである。

Balance（バランス）

バランスは動的なビジネスプロセスであるべきで、静的なものであるべきではない。安全性（security）と非安全性（insecurity）という 2 つの分離された部分は、一つの物を構成する 2 つの要素－「1 枚の硬貨の表と裏」－なのである。こういった正反対のもののバランスをとることは、リスクのマネジメントに関連したビジネス上の問題である。我々が実現すべきバランスは、我々のビジネス環境に特有の流動性や変化を

反映した、これら２つの面の名もなき統一体なのである。変化というものは何らかのかたちで至る所にあり、かつ防ぐことができない。これを理解し受容することによって、変化に内在するバランスを得ることができ、そしてこれによって脅威と対策、脆弱性と是正処置といった、これら相反するもののエネルギーを調和し、その結果マイナスの影響力の効果を調和することができるのである。

Ted Humphreys (XiSEC)、 Dr Angelika Plate

STANDARDISATION UPDATE（標準化最新情報）

Information Security Incident Management（情報セキュリティ事件・事故マネジメント）

我々のシステム、運用プロセス、及び重要な資産は、ビジネスに深刻な影響を及ぼしかねない様々な事件・事故にさらされている。今日のビジネス環境に存在する、この様々なセキュリティ事件・事故に関連したリスクのマネジメントを実施できる重要性を意識して、SC27 は、「Information Security Incident Management」（情報セキュリティ事件・事故マネジメント）（ISO/IEC 18044）という表題の規格の開発に着手した。事件・事故が起こった場合に、その事件・事故が引き起こし得る損害を最小限に抑えるために、その事件・事故に対して迅速、効果的、かつ整然とした対処を行えるようにするために、管理策を実施する必要がある。この潜在的な損害は、事件・事故の深刻度と対処・復旧のためのマネジメントシステムの有効性によって異なる。

ISO/IEC 18044 規格の開発には、報告、検出・識別、分析・評価、対処・復旧、学習・改善という、完全な事件・事故マネジメントライフサイクルが考慮に入れられている。

ISO/IEC 17799:2000 Revision（ISO/IEC 17799 の改訂）

国際規格 ISO/IEC 17799:2000 の維持作業は ISO/IEC JTC1 SC27 が行っている。JTC1SC27 はまた、ISO/IEC 17799 の改訂作業も行っている。この改訂は、必要な改善を目的としているが、一方で現在 ISO/IEC 17799 の適用に投資している全ての組織が資金・資源を無駄にすることのないよう、『backwards compatibility』（現行規格との互換性）を保つことも目指している。

SC27 は、合意の意思決定プロセスを用いて、各国の機関からの寄稿に基づいて改訂文書のレビュー・編集作業を行っている。これらコメントに関する決議に従って、新案が発行される。そしてある一定の状態に達した後には、その文書は数段階の投票を経て、最終的にこの規格の次版公開に至る（現段階では、2004 年末又は 2005 年と推測される）。

IMPORTANT(重要)： この改訂プロセスは現在進行中であり、いまだ終了してはいない。従って、2000 年に公開された版が現在有効なバージョンであり、その為これが他の文書内で引用・参照されている。

改訂の最終過程では、最近、約 700（！）もの発展的なコメントを頂いた。前回の SC27 会議ではこれらのコメント全てについて議論することはできなかったため、残りのコメントについて議論するために（次回の SC27 会議に合わせて）2003 年 4 月 24 日～26 日にケベックで特別会議（ad hoc meeting）を開催することを予定している。

改訂の詳細については、詳細な改訂報告書に記載されており、この報告書は www.aexis.de で入手できる。この報告書を一読される際には、この報告書は SC27 による次版の改訂文書作成（つまり 2003 年 5 月）までの期間においてのみ有効だということに留意してください。

ISMS Study Period（ISMS 検討期間）

2002 年 4 月に開催された SC27 のベルリン会議では、ISO/IEC 17799 の改訂について議論され、組織が必要とするかもしれない ISO/IEC 17799 の種々の使用法に関しての重要な議論に発展した。これについてさらに詳しく調べるために、National Bodies（各国の機関）に対して質問を行い、その回答（feedback）について 2003 年 10 月に開催された SC27 のワルシャワ会議で議論した。

各国の機関から寄せられた主な結果は、次の通りである。

- ISO/IEC 17799 に定める個々の利用法があり、組織は自らに最も適する方法で ISO/IEC 17799 を使用することができ、またそうすべきである。
- 管理目的及び管理策の記述にある『should』という語は、そのまま残す。
- ISO/IEC 17799 では、いかなる認証事項についても言及しない。

上記のほかにも、フランスは、ISO 9001 などの他のマネジメントシステム規格と同様に、情報セキュリティマネジメントシステム（ISMS)に関する規格に対しても強い市場ニーズがあることを示した。このような寄稿を踏まえて、SC 27 WG1 は Study Period on ISMS（ISMS に関する検討期間）を設け、BS 7799 Part

2、ISO 9001、ISO 14000、ガイド 72 及び 73、ISO/IEC 17799、TR 13335、他の SC27 規格などの、他の既存の規格を考慮に入れて ISMS 規格制定の実現可能性を検討することを決定した。

Guidelines on IT Security GMITS（IT セキュリティガイドライン、GMITS）(ISO/IEC 13335)

ISO TR 13335（GMITS – Guidelines for the Management of IT Security）のパート１及びパート２については、現在 ISO/IEC JTC1 SC27 内で改訂中である。この改訂作業として、この２つのパートを統合して１つの文書にすること、現行の版に記載されている助言や指針を改善・改正すること、そしてこの２つのパートの初公開後に行われた規格の開発を考慮するのに必要ならば新たな資料を追加することが挙げられる。

GMITS パート 3 の改訂も、現在進行中である。パート 3 は、リスクアセスメント面とリスクマネジメント面を対象としたもので、パート 1 とパート２の改訂及びリスクマネジメントを扱う他の規格の開発に合わせて改正が行われている。

GMITS のこの 3 つのパートを、テクニカルレポートから完全な国際規格に移行してはどうかとの提案がなされている。この件は現在、投票にかけられている。

PD 3000 Series（PD3000 シリーズ）

BSI 発行のガイド、PD3000 シリーズは、Part 2 の新版（2002 年版）を考慮するために、最近改訂・改正された。このシリーズは、以下の通りである。

Preparing for BS 7799-2 certification（BS 7799-2 認証の準備）（PD 3001）

これは、BS 7799-2:2002 と、実践規範 BS 7799-1:2000（ISO/IEC 17799）のユーザーに対する指針である。

このガイドには、『Plan, Do, Check, Act』モデルと、ISMS のプロセス要求事項、認証プロセス、及び認証取得準備に関する指針が記載されている。

Guide to BS 7799 Risk Assessment（BS 7799 リスクアセスメントへのガイド）（PD 3002）

このガイドは、BS 7799、特に BS 7799 情報セキュリティマネジメントシステムの構築・認証の観点からリスクアセスメント及びリスクマネジメントのテーマを取り扱ったものである。また、リスクアセスメントとリスクマネジメントの基本的概念についての共通の基礎及び理解、使用される用語、そしてリスクアセスメント及びリスクマネジメントのプロセス全般とその選択肢を提供することを目的としている。

Are you ready for a BS 7799 audit? A compliance assessment workbook（BS 7799 の監査の準備はできていますか？ － 適合性評価ワークブック）(PD 3003)

このガイド PD 3003 の内容は、7799 管理策に関する ISMS プロセスチェックとギャップ分析の両方を盛り込んだ、適合性評価ワークブックを提供するものとなるよう拡充された。

Guide to the implementation and auditing of BS 7799 controls （BS 7799 管理策の実施及び監査へのガイド）(PD 3004)

このガイドの内容には、BS 7799 Part 2:2002 の認証取得を考えている組織が処理すべき ISMS 管理要求事項が含まれている。このために、このガイドの第 2 章では、BS 7799 Part 2:2002 の各管理策を、次の 2 つの異なる側面から検討している。

- **Implementation guidance（実施に関する指針）**：ここでは、BS 7799 Part 2:2002 附属書 A の管理策の実施にあたり、管理要求事項を満たすために何を考慮する必要があるかについて説明している。この指針は、BS 7799 Part 2 管理策の実施に関する助言を記載した、ISO/IEC 17799:2000 と整合がとられている。
- **Auditing guidance（審査に関する指針）**：ここでは、BS7799-2:2002 の管理策の実施が本質的な ISMS 管理要求事項を網羅していることを確実にするために、この実施について審査する際に何をチェックすべきかについて説明している。

Guide on the selection of BS 7799 controls（BS 7799 管理策選択のガイド）（PD 3005）

このガイドでは、ユーザーに対し、以下の事項に関する指針を提供している。

- 選択プロセス － ここでは、識別されたセキュリティ要求事項をとりあげ、一連の関連するビジネス上の決定を通して実施する必要のある管理策を定める。これには、『要求事項の評価』、『選択プロセスへのアプローチ』、及び『選択プロセスの概要』が含まれる。
- 管理目的及び管理策の選択 － これには『セキュリティ要求事項と BS 7799 管理策』と『セキュリティ上の問題と BS 7799 の管理策』が含まれる。
- 選択上の要因及び制限
- 情報セキュリティマネジメントシステム（ISMS）認証、適用宣言書、及び ISMS 要求事項
- リスクアセスメント－概要（詳細な情報は PD 3002 に記載されている）。ここでは、『リスクのアセスメント』、『リスクアセスメントの構成要素』、『リスクアセスメントプロセス』、及び『リスクアセスメント』について記載されている。

ガイド PD 3000 シリーズについての詳細な情報については、c.cure@bsi-global.com まで電子メールにてお問合せください。

AUDITOR CERTIFICATION（審査員の評価・登録）

IRCA（International Register of Certified Auditors）は、ISMS 審査員評価・登録基準を公開した。この基準では、審査員には次の４つのタイプある。

- ISMS Provisional Auditor（ISMS 審査員補）
- ISMS Auditor（ISMS 審査員）
- ISMS Lead Auditor（ISMS 主任審査員）
- ISMS Principal Auditor（ISMS プリンシパル審査員）

評価・登録プロセスの一部として、IRCA は申請者を要求事項に照らして評価する。この要求事項は、力量を定める主要な技量、知識、及び経験を反映したものであり、ISMS 審査員はこれらをもっていなければならず、かつ審査においてこれを保有していることを実証しなければならない。

この評価基準では、申請者が各タイプの審査員登録のために満たさなければならない教育、業務経験、審査員研修、審査経験を定めている。

このスキームは次の者達を対象としている。

- ISMS 審査員。例えば、第三者審査登録機関に雇用されているか又はこれら機関と契約している者、第一者又は第二者 ISMS 審査に携わる者。
- 情報セキュリティ実践者。例えば、情報セキュリティコンサルタント、IT セキュリティマネージャー、IT 要員。
- 組織内における ISMS 監査、すなわち ISMS の内部監査を実施する従業員。

この ISMS Auditor Certification Scheme（ISMS 審査員評価･登録スキーム）は、次に示す主要な規格及びガイドラインに関する知識及び経験に基づいている。

Certification Specifications（認証仕様）
- BS 7799-2:2002 情報セキュリティマネジメントシステム - 仕様及び利用の手引
- ISO 9001:2000 品質マネジメントシステム - 要求事項

Auditing Standards（監査に関する規格）
- 品質及び／又は環境マネジメントシステム監査のための指針

Accreditation Standards（認定規格）
- EA 7/03, ISMS 審査登録機関の認定に関するガイドライン

Control Standards（管理規格）
- ISO/IEC 17799: (最新版), 情報セキュリティマネジメントシステム - 仕様及び利用の手引

全登録審査員の詳細については、登録簿に記載されている。この登録簿は IRCA が発行・公開している。

IRCA は、認定 ISMS 研修コースに関する基準も発行している。この分野に関しては、次の 2 つの文書を発行している。

- IRCA 2060 ISMS Auditor Conversation Training Course
- IRCA 2061 ISMS Auditor/Lead Auditor Course

これらの文書は、研修機関が IRCA/2060, Information Security Management Systems (ISMS) Auditor Conversion Training course の認定を取得するのに役立つものとなるよう作成された。

IRCA の ISMS 審査員評価・登録を希望する審査員は、認定された IRCA ISMS 研修コースか、又は IRCA がこれと同等なものとして認めた代替研修を申請前 3 年以内に修了し、これに合格していなければならない。

CERITIFCATION UPDATE（認証最新情報）

BS 7799 Part 2 の認証取得事業者数は、継続的に増加している。認証を取得した事業者の一覧である International Register は、www.xisec.com/Register.com でみることができる。また、これら認証の ISMS 適用範囲についても、このサイト上でみることができる。この International Register に Certification Portal が新たに加えられた。これは、ISMS 認証に関する情報センターに発展する予定であり、このサイトでは認証プロセスには何が関連するか、誰が認証に関連するのかなど、ISMS や他の関連最新トピックを取り上げる。

現在、認定された認証機関は世界各地に 23 機関あり、認証審査を実施している。大陸別認証取得事業者数を示す世界地図は、www.gammassl.co.uk/bs7799 でみることができる。

7799 GOES GLOBAL CONFERENCES（7799 国際化カンファレンス）

2002 年 9 月 4、5 日から、情報セキュリティマネジメントシステムに関する一連の International User Group カンファレンスが始まった。これは、「7799 Goes Global」（7799 国際化）カンファレンスと呼ばれる。9 月 4、5 日のカンファレンスはロンドンで開催され、産業界や商業界らの第一人者が企業統治、ISMS の認証と実施、e-biz、そして ISMS 統合及び ISMS の法的側面の処理に関する最新動向と発展について示すために一堂に会した。

2003 年には、素晴らしい一連の 7799 Goes Global 行事が開催される。これは、6 月 9、10 日中国の上海に始まり、その後は 7 月上旬にメキシコシティでの開催が計画されている。今秋には、9 月 17～19 日にロンドンの有名なロンドン塔で開催される予定であり、またできれば 9 月初旬にスリランカでも（現在の予定では 9 月 4、5 日に）開催される。

WHAT IS THE FOUNDATION?（本協会について）

The ISMS Foundation（本 ISMS 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キング活動を通して 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。本協会はまた、規格の解釈に関して、全ての者に対し無料仲裁サービスを提供している。

INTERPRETATIONS & READER FAQS（解釈＆読者からの FAQ）

このコラムでは、BS 7799 規格の解釈や、また次号以降では読者から寄せられた FAQ を紹介する。BS 7799 Part 2 又は ISO/IEC 17799 の適用に際に生じる問題の解釈については、ISMS 協会が提供する。そのような解釈の最近の例を以下に示す。

これらの FAQ は、Web を通して収集される、このジャーナルの読者からのご意見（feedback）です。

これらの問題を取り扱う担当者に対するご質問、解釈のご要望につきましては、「7799 Interpretation」と記した電子メールを aexisap@aol.com までお送りください。

例えば、BS 7799 の解釈は次のようなものである。

Interpreting risk acceptance in BS 7799-2:2002（BS 7799-2:2002 におけるリスク受容の解釈）

BS 7799-2 では、4.2.1.e)(4)において次のように規定している。

- *4.2.1 c)で確立した基準を使用して、当該リスクが受容できるか、又は対応が必要かを決める（4.2.1 c)参照)。*

BS7799-2 4.2.1 f)の選択肢(2)では、考えられるリスク対応活動の 1 つとして次のように規定している。

- *リスクが組織の基本方針及びリスクの受容基準を明らかに満たしている場合、意識的かつ客観的に当該リスクを受容する（4.2.1 c)参照)。*

通常、リスク対応活動の検討段階までには、その際残っているリスクについては受容できないとの決定が既になされている。では、ここで、いかにしてさらにリスクを受容すると決定できるのだろうか？

リスクアセスメントは、通常、我々のビジネスが直面するリスクレベルの指標となる。我々のビジネスは、そのビジネスが耐え得るリスクの閾値（threshold）を定めるべきである。この閾値を超えるリスクについては、どのようにこれを取り扱うか定める必要があり、またこの閾値以下のリスクについては、このリスクを受容可能だとする（4.2.1 e) ステップ(4)の解釈)。ここでは、たとえリスクのレベルが定めた閾値を超えたとしても、そのリスクを受容しなければならないという状況が生じる可能性がある（4.2.1 f) 選択肢(2)の解釈)。

そのような状況において特に必要なのは、閾値を超えるリスクの受容に対してマネジメントの承認を得ることであり（4.2.1.i)も参照のこと)、またできるだけ早くその状況の変化を識別するためにこれらのリスクを監視するということである。

Dr. Angelika Plate（AEXIS Security Consultants）

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

電子メールをお送りください。

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 へ電子メールをお送りください。詳細情報については以下の URL で入手できます。

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

第 3 号では以下のテーマを扱う予定です。

- 連載シリーズ「監査（審査）と認証」Part 3
- 連載シリーズ「ISO/IEC 17799 の適用 Part 3。認識に関する重要なトピックを取り上げます。
- 連載シリーズ「Tao-Zen Practice と ISMS の実施」Part 3
- 新シリーズ － HIPAA（Health Insurance Portability and Accountability Act：医療保険の携行性と責任に関する法律)、指令、及び 17799 について
- 新シリーズ－ ISMS Forensics（ISMS の科学捜査)－Part 1 ではこのテーマについて説明します。

今後の ISMS ジャーナルで検討されるトピックとしては、保険や保険と情報セキュリティ及びリスクマネジメントとの関連が挙げられます。「insurance survey」（保険検査）に参加を希望される方は、www.gammassl.co.uk/bs7799/insurance.html をご覧下さい。

また、認証を取得した事業者がどのようにしてセキュリティ監視の問題を処理したかについての記事を掲載したいと思っております。この記事では、この第 2 号に掲載のセキュリティ事件・事故に関する記事に続いて、セキュリティの監視に関する実例を提供いたします。このセキュリティの監視についての記事は、大規模なネットワーク化されたシステムにおいて、Plan、Do、Check、Act モデルをいかにして自動化できるかに関する事例について説明する予定です。

このジャーナルに広告掲載をご希望の方、又は投稿をご希望の方は、当協会までご連絡ください。連絡先の詳細については、このページの Journal Contacts をご覧下さい。

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。

EVENTS（行事）

2003 年には以下の行事の開催を予定しています。

3 月 5～7 日	BS 7799 リスクマネジメントコース（英国、ロンドン）
4 月 2～3 日	ISO/IEC 17799 実施コース（オスロ、Norwegian Institute of Technology）
4 月 28 日～5 月 6 日	ISO/IEC JTC1/SC27 会議（カナダ、ケベック）
5 月 8／9 日	7799 Goes Global カンファレンス（カナダ、トロント）
5 月 19～20 日	IUG 欧州専門家会議（ノルウェー、オスロ）
5 月 29～30 日	ISO/IEC 17799 実施コース（英国、Sunningdale、Civil Service College）
6 月 9 /10 日	7799 Goes Global カンファレンス（中国、上海）
7 月 7～8 日	7799 Goes Global カンファレンス（メキシコ、メキシコシティ）
9 月 17～19 日	7799 Goes Global カンファレンス（英国、ロンドン）
10 月 20～24 日	ISO/IEC JTC1/SC27 ワーキンググループ会合（フランス、パリ）