ISMS Journal (Issue 3)

（日本語版）

出典：http://www.xisec.com

2004 年 8 月 9 日

財団法人 日本情報処理開発協会

第 3 号　2004 年 4 月（仮訳）

ISMS　Journal

目次

本 ISMS ジャーナルは、ISMS International User Group により発行されています。

ISMS 認証（ISMS CERTIFICATION）

ISMS 認証の市場は拡大を続けており、現在では 37 ヶ国 600 以上の企業が「認証クラブ（“certification club”）」に参加している。また International Register（各国認証取得事業者一覧）にみられるように、様々な産業セクターの事業者が認証を取得している。このなかには金融、保険、通信、IT、製造、小売、政府セクターの多くの有名企業も含まれており、また中小企業の認証取得数も増加している。ISMS 認証を目的とした BS7799 Part 2 の適用が世界的に増加していることは、事業者らが自らの直面しているリスクを認識し、ビジネス保護の目的でこれらのリスクをマネジメントするための行動を起こす準備をしていることを示している。

認証取得のビジネス上の理由・便益は様々である。例えば、契約上の義務、コーポレートガバナンス、顧客や他の利害関係者らに対する情報保証の提供、法令への適合、供給者に BS 7799-2 への適合を要求する入札文書他、多数ある。

認証を取得した世界各国の企業の多様性については、ISMS International User Group ウェブサイト掲載の International Register of Certificates（各国認証取得事業者一覧）を参照下さい。

US ニュース（US NEWS）

米国では、ニューヨーク連邦準備銀行、EDS エンタープライズサービス GSOC、TELOS－OK など、多くの企業が最近 BS 7799-2 の ISMS 認証を取得している。

また、ISMS International User Group の米国支部が最近設置された。この支部は、定期的な ISMS 構築とその利用法のワークショップ、カンファレンス、ユーザーグループウェブサイト、刊行物などによって、ISO/IEC 17799 や BS 7799-2 などの ISMS 規格の利用を促進・支援していく予定である。この支部は設置後数週間で急速に発展しており、5 月 6 日、7 日にはカリフォルニア州のプレサントンにて初のイベントとなるセミナーを開催予定である。この支部に参加をご希望の米国の方は www.us-isms.org を参照ください。

ISO/IEC 17799 の改訂（REVISION OF ISO/IEC 17799）

ISO/IEC 17799 の維持に責任をもつ委員会、ISO/IEC JTC 1/SC 27 の次回会議が 4 月にシンガポールで開催される。現行の ISO/IEC 17799 は 2000 年に発行されたものでこれは現在改訂中であり、シンガポールでの会議はこの改訂をより一層進める機会となるだろう。

ISO/IEC 17799 規格の次版では、多くの更新や追加を含め、内容を拡充するために新たな事項が考慮されている。この例としては、「人員に関する」章（”Personnel” section）が挙げられる。この章では、雇用前、雇用中、及び雇用終了後に生じる、異なる要求事項が規定される予定である。事件・事故処理や第三者サービスなどの項目にも、こういった改善や更新が盛り込まれる予定である。これらの項目は、第三者サービスのマネジメントに関連する最近の要求事項をカバーするよう、かなり範囲が広げられた。また他にも新項目として、モバイルコード、ぜい(脆)弱性、パッチ管理に関連するセキュリティ側面などが加えられた。この規格の新版は、情報セキュリティ界における変化や進展を考慮した最新規格となるべきである。またそれと同時に既存の規格との整合のとれた規格となるべきである。

またこの改訂では、（管理策と管理策の実施に関する助言を分離することにより）インターフェースが改善され、利用しやすくなっている。これによって、リスクマネジメントに適切な管理策と、そのような管理策の実現方法を識別しやすくなるだろう。この規格の新版は、2005 年に発行される見込みである。

Angelika Plate（AEXIS Security Consulting/ISO/IEC 17799 改訂共同編者）

HIPAA と ISO/IEC 17799（HIPAA AND ISO/IEC 17799）

はじめに（Introduction)

The Health Insurance Portability and Accountability Act (1996) (HIPAA：医療保険の携行性と責任に関する法律）が、2003 年 4 月から米国で発効された。HIPAA の目的は「グループ及び個人加入の健康保険の携行性と継続性の改善、健康保険及び医療給付における無駄、不正行為、及び悪用の防止、医療用貯蓄口座の利用促進、長期医療サービスの利用・補償範囲の改善、並びに医療保険の管理の簡素化他」を図ることである。

この HIPAA の目的の焦点は、個人データの収集・伝送の認可規則に関する European Data Protection Directive（欧州データ保護指令）（以下指令という）の要求事項とはやや異なっている。

この特集では、この 2 つの法令の要求事項を考察し、その要求事項に対応するためには ISO/IEC 17799 規格をどのように利用すればよいかについて、また検討すべき制約について考察する。

全般的な考察（General considerations)

HIPAA 及び指令のどちらにも、準拠する為に実施しなければならない具体的な対策については明確に記述されていない。指令には、個人データのなかには法的な認可なしでは収集できないものがあり、またデータ項目のなかには他よりも強力な保護を必要とするものもある、という注釈がある。しかしながら、より強力な保護とは何を意味するのか、については何ら明確な定義はない。

また HIPAA は、米国規格協会認定の機関（National Council for Prescription Drug Programs [全米処方薬プログラム協議会]など）の規格導入の可能性も示唆している。

「HIPAA の目的の一つは、・・・健康保険及び医療給付における無駄、不正行為、及び悪用の防止である。」

一方、指令では規格については直接触れていないが、欧州規格機関の CEN には法令を支援するために必要な規格を作成する権限がある（実際に、デジタル署名指令を支援する多くの規格を作成している。しかし、これらの規格は、現在のところ全面実施はされていない）。

これまでのところ、どちらの法令においても準拠を保証する方法・手法の充足度（又はその他）については、法的決定はなされていないようである。

ではこれらの法令では何が要求されるのか？（So what does the legislation require?)

技術スタッフにとってはつい忘れがちなことかもしれないが、これらの法令には達成すべき目標を定めている部分もある。しかし、どちらの法令もその目標達成のためにとらなければならない具体的なセキュリティ対策は定めていない。

HIPAA には、保護すべき情報の定義として、下記の通り記載されている。

第 6 章 個人の特定が可能な保健情報

『個人の特定が可能な保健情報』という用語は、個人から収集された人口統計学的情報を含む、下記の情報全てを意味する。

a) 医療機関、健康保険、雇用者、又は医療決済機関が作成又は受領した情報、及び
b) 個人の過去、現在、又は未来の肉体的／精神的な健康又は状態、個人への医療提供、あるいはまた個人へ提供された医療の過去、現在、又は未来の支払状況に関するもので、下記の事項を満たすもの。
   ｉ）個人を特定する情報、又は
   ii）その情報が個人の特定に利用可能だと信じるに足る根拠のある情報

また、次を含む。

a) 第（2）段落に記載の金融・管理上の取引（administration)、及び
b) 医療システム運用を改善し管理コストを削減するという目標に合致し、長官（Secretary）により適切と判断された他の金融・管理上の取引

これは、データ範囲の点からすると、よりいっそう幅広い指令のアプローチとは対照的である。しかし医療に関する章においては非常に似通っている。HIPAA では個人データよりはるかに広範なデータを対象としているため、ある意味 HIPAA の方が指令よりも強力だといえる。そのデータは、生存している個人についてだけのデータよりも多くの確認を必要とすることもある。

固有の要求事項（Specific requirements）

HIPAA の適用範囲は、実施者に下記の事項を満たすよう要求している。

a) 次の事項を考慮する。
   ｉ）保健情報の維持に利用される記録システムの技術力
   ii）セキュリティ対策費用
   iii）保健情報にアクセスする人員訓練の必要性
   iv）コンピュータ化された記録システムにおける監査証跡の価値
   v）小規模の医療機関と地方の医療機関のニーズ及び能力（このような機関は長官により定義される）
b) 医療決済機関がより規模の大きな機関の一部である場合、情報の処理に関して、この規模の大きな機関からの情報への無認可のアクセスを防ぐ方法で医療決済活動を分離するポリシー及びセキュリティ手順を有していることを確実にする。

指令にも、全ての記録管理システムに適用される、（コンピュータを運用している組織ではなく）個人に対する損害や使用した対策のコストと効果を十分考慮しなければならない、という要求事項があり、上記の HIPAA の要求事項はこの指令の要求事項と似ている。

要求される手順（Required procedures）

HIPAAには、実施しなければならない個別の活動が定められており、これらは原則と同様に非常に明確である。

第2章　保護手段（SAFEGUARDS）

保健情報を維持又は伝送する、第1172(a)章に記載の各人員は、次の事項を満たすために妥当で適切な管理的、技術的、及び物理的保護対策を維持しなければならない。

a） 情報の完全性及び機密性を確保する。
b） 当然予期される次の事項全てから保護する。
　ⅰ） 情報のセキュリティ又は完全性に対する脅威又は危険、及び
　ⅱ） 情報の認可されていない使用又は開示
c） 或いはその役員又は従業員がこの項目へ準拠することを確実にする。

一方、指令は、保管データについて閲覧、説明、遮断、又は消去を受けられるというデータ対象者の権利の原則を確立するものであるため、その要求事項のなかで上記についてさらに踏み込んでいる。この指令の消去の要求事項は、HIPAAで言及されている『記録管理システムの技術的要求事項』の一部と見なされるかもしれないが、消去に関しての明確な要求事項はない。

要求事項の分析（Analysis of requirements）

前述したように、HIPAAと指令のどちらも、遵守しなければならない特定の対策を義務付けていない。また、機密性及び完全性に関する要求事項については、どちらも言及している。可用性については明確には言及していないが、しかし価値がある場合には、ビジネスシステムは時宜に即して機能していなければならない。このことは、特に医療システムが時宜に即した運用に失敗し、そのためその管理者が訴訟の対象となる恐れのある場合に当てはまる。

他の要求事項、例えば業務の復旧などについては、明確に取り扱われていない。情報の完全性と復旧は同じというわけではないが、完全性の継続に関する要求事項ではバックアップ記憶装置サービスのことが示唆されている。

また、認可された者だけが情報を入手できることや、適切な監査が行われていることを確実にすることの可能な要求事項がある（しかし、この文脈で監査とは何を意味するのかを考慮しなければならないかもしれない）。reasonable（妥当な）という用語を要求事項に含める趣旨は、やはりここでもあまり明確ではない。reasonable（妥当な）は、固定用語（fixed term）ではなく、技術能力の変化、また流行の変化の影響を受ける用語である。ここでは技術能力が優先されるべきだが、しかしある一つの具体的な結果を導くための方法が複数ある場合、実際の有効性に関わらず一つの特定のアプローチが他よりも一般的だとみなされることもある。

HIPAAと指令のどちらも費用効果的な手順の使用について言及している。

準拠は常に基本である。準拠の確保は技術的要求事項ではなく、また技術的な方法だけでは実現することはできない。セキュリティ上の技術的な観点からでは、最も実現可能なものは、技術的検査に限られる。一方準拠の多くは社会的・行動的なものである。これらは、本質的にマネジメントの問題であり、技術規格よりもマネジメント規格の方により適している。

要求事項とISO/IEC 17799の整合（Matching requirements and ISO/IEC 17799）

HIPAAと指令どちらにおいても、費用効果的な対策が要求されている。これは、リスク分析に関するISO/IEC 17799の要求事項と完全に合致している。リスク分析のアプローチは、機構構築（mechanism）のための費用の妥当性を示すためにも、また機構構築費用が実現見込みのある利益に比べてはるかに高い場合にその妥当性を示すためにも利用することができる。なぜ対策が実施されないのかを明示するため、特に対策が小規模企業にとってその規模や能力を考慮して適切でない場合にその理由を明示するために、正式なリスク分析が求められることもある。

機密性、完全性、可用性実現のための機構（mechanism）が要求されているが、ISO/IEC 17799では何ら特定の管理策の実施を義務付けていない。この規格には多くの管理策が記載されているが、それらはすべて規制的なものではないのである。また、個々の状況においてどの管理策が適しているか決定するための正式な機構についての記述はない。リスク分析の要求事項は、管理策が目的に適している場合にのみ、その管理策を選択できるということを意味している。

このような方法で、ISO/IEC 17799は、たとえある特定の状況において利用可能な、最も強力な技術的セキュリティ機構があるかもしれない場合でも、特定の管理策が費用効率的なものとして選択された理由を明示する、優れた方法となっている。

ISO/IEC 17799は、非常に柔軟な規格となるよう作られており、小規模の医療行為から大規模の病院業務にまで及ぶ様々な規模の組織に適用することができる。この規格は、あいまいな規則書（rule book）ではなく、組織のビジネスに適した費用分析に基づき、組織のビジネス要求事項に適切な要素と妥当なものを選択できる強固な枠組みを提供しているのである。

実際にISO/IEC17799は、コーポレートガバナンスの要求事項を取り扱うための、今日入手可能なセキュリティ規格のなかでおそらく最も適切な規格だろう。ガバナンスはプラクティスとプロセスを取り扱う管理者及び経営者に対して義務を課している。これは技術的要素のものではなく、組織が自らのセキュリティを適切にマネジメントしていることを証明しようとする際に、まさに必要とされるものなのである。

「ISO/IEC 17799は、非常に柔軟な規格となるよう作られており、小規模の医療行為から大規模の病院業務まで及ぶ様々な規模の組織に適用することができる。」

Steve Mathews

7799 GOES GLOBAL イベント ? 2003（7799 GOES GLOBAL EVENTS ? 2003）

2004 年イベント

・シンガポールワークショップ
2004.04.28
・プレサントンワークショップ（米カリフォルニア州）
2004.05.06/07
・ストックホルムカンファレンス&チュートリアル（スウェーデン）
2004.10.05/06
・サンパウロカンファレンス(ブラジル)
2004.10.25
・ロンドンカンファレンス&チュートリアル（英国）
2004.12.01

上記イベントの詳細については、ISMS International User Group のウェブサイトを参照下さい。

京都（KYOTO）

ISMS International User Group と日本情報処理開発協会（JIPDEC)の国際的な連携により、2003 年 11 月 18-19 日に、日本における初の”7799 Goes Global” カンファレンスが開催された。このカンファレンスは、7799 ベストプラクティスに対する関心が日本国内の様々な事業者のあいだで高まっていることを反映し、このカンファレンスは大成功を収めた。

開催地は、数多くの「世界遺産」のある世界的に有名な都市、京都市だった。またこのカンファレンスは日本情報処理開発協会（JIPDEC）主催で開催され、経済産業省（METI：Ministry of Economy, Trade and Industry）及び京都府から寛大なご支援を頂いた。

ロンドン（LONDON）

昨年の英国 7799 Goes Global カンファレンスは、9 月 18-19 日にロンドン塔で開催された。この開催地は、言うまでもなく情報セキュリティというテーマに非常に関連のある場所である。このカンファレンスは、DTI と International User Group の支援を受けて BSI によって開催された。

カンファレンスでは、ガバナンスの重要性、リスクマネジメント、ISMS の導入や認証取得事例などといった、様々な重要課題について活発で白熱した議論が展開された。また、このカンファレンスでは CISM 委員会議長による ISACA CISM 名誉賞授賞式も行われた。

この京都カンファレンスとロンドンカンファレンスのレポートは、ISMS International User Group のウェブサイトで閲覧できる。

パリ（PARIS）

7799 Goes Global ワークショップ、”Manager vos risques de l’information:7799?” が、INFOSEC 博覧会開催期間中の 11 月 27 日にパリで開催された。このワークショップは、企業にとって様々なリスクマネジメント問題に取り組むために集まり、Ernest & Young、France Telecom Transpac、CSC、Certplus、Alstom から ISO/IEC 17799 利用経験について話を聞くことのできる絶好の機会となった。

7799 Goes Global
ISMS International User Group

業務処理上の誤り（PROCESSING BUSINESS ERRORS）

「業務処理上の誤りを防止したいならば、ISO/IEC 17799 の管理策適用によって業務用ソフトウェアの安全を確保しなさい。」

ISO/IEC 17799 では、業務用システムのセキュリティについてどのように記載しているのだろうか。より正確に言えば、この規格では、業務プロセスへ入力される情報の検証や、またこれらの業務プロセスからのアウトプットのチェックについてどのように記載しているのだろうか。折しも、この規格には例えば 10.2.1、10.2.2、10.2.4 など、この分野について記載した一連の管理策がある。では、このようなインプットとアウトプット検証の為の管理策があるということは、どの程度重要なのだろうか？その答えは、非常に重要、である。つまり、これらの『管理策』は、業務が依存している実際のデータ処理において発生した誤りを識別するためのものである為、非常に重要なのである。特に、これらの管理策は次を検出することを目的としている。

- インプットにおける誤り／手違い
- ソフトウェア処理時の誤り／手違い
- 最新のビジネス要求事項とソフトウェアの非両立性
- 起こりえない処理結果
- 保管データの改ざん

業務用ソフトウェアへのインプット情報には、数多くの種類がある。例えば、次のようなものがある。

- 会計・支払請求システム内：氏名及び住所、信用限度、顧客参照番号、請求料金、通貨の換算
- 製造及び生産システム内：設計、生産方法・手法、生産ラインのタイミングデータ

組織は、プロセスにインプットされる情報とそのプロセスから生じる結果の正確さ、完全性、一貫性、及び適時性を管理していることを確実にする必要がある。これらを管理していない場合、次のような結果が生じ得る。

- 業務或いは取引先や顧客に対する不正行為
- 誤って送付された請求書やインボイスを受け取った顧客の不満、又は契約上のサービスや商品提供能力の欠如
- 法律又は会計法規に規定する記録管理及び／又は提示に関する要求事項への適合能力の欠如

ISO/IEC 17799 は、こういった実際のビジネスリスクに対し、ベストプラクティス的な管理策を適用するための良い出発点となる。今回の記事は、業務処理上の誤りを回避するのに役立つ、ISO/IEC 17799 を探っていくシリーズの第一部なのである。

2004年度違反調査（2004 BREACHES SURVEY）

最新の情報セキュリティ違反調査は2004年4月27日に公開予定である。PriceWaterhouseCoopers (PWC)プロジェクトが2004年度の調査を実施し、またMicrosoft、Computer Associates、Entrustがこのプロジェクトの共同支援を行った。

この調査報告書とともに、下記を含むファクトシート一式も公開されている。

- 識別マネジメント
- 侵入防止
- スパム
- リモートアクセス
- スタッフによるインターネット誤用
- バックアップ及び復旧
- ウイルス及び悪質なコード

また、このファクトシートでは、こういった問題に関連のあるいくつかのベストプラクティス的推奨事項が、読みやすく、使いやすいかたちで記載されている。

この報告書とファクトシートのコピーは、DTIのウェブサイト、http://www.dti.gov.uk/industries/information_security/downloads.html からダウンロードできる。

1991年以来、英国貿易産業省（Department of Trade and Industry）は、英国企業の直面しているリスクについて企業の理解を深めるために情報セキュリティ違反調査を後援している。この2004年情報セキュリティ違反調査（Information Security Breaches Survey: ISBS 2004）は第7回目であり、PriceWaterhouseCoopersにより実施された。

この調査結果によると、あらゆる規模の企業がインターネット利用を取り入れており、今や英国は完全に情報時代に入っていることが示されている。これによって事業の運営方法が変化し、その効率性や顧客サービスが改善されている。

しかしながら、ネットワーク化の拡大によって、情報セキュリティ問題の増加という悪影響も生じている。事実、この調査結果は、セキュリティ問題が今や他人事ではなく、ビジネスライフの避けがたい現実となっていることを示している。つまり、組織はこういった脅威を必死に抑制しようと努力しているが、セキュリティ事件・事故数は増加の一途を辿っているのである。

しかしながら、幸いなことに取締役会レベルでは情報セキュリティは継続して優先度が高い。これまでにないほど数多くの企業がセキュリティポリシーを導入しており、BS 7799を採用した企業は、この規格が真の利益をもたらすものだということに気づいている。

また、企業自らの情報セキュリティ問題への対処を支援する目的で政府、特に私の所属する省から発行されたガイダンスが多くの企業に利用されているのも喜ばしいことである。この分野での我々の活動は今後も継続し、英国における e-ビジネス促進のための政府アジェンダの主要な一部となるだろう。

情報セキュリティの脅威を抑制するための戦いは長期にわたると思われ、現時点では勝利には程遠い。しかしこれは、英国企業が決して負けることのできない戦いなのである。

Stephen Timms MP
エネルギー、電子商取引、及び郵政事業担当大臣
2004年4月

「不適切なものをダウロードするスタッフは、それを電子メールによって共有する傾向がある。経営者が気づく前に、その企業は他の組織に対して不正な物を送っているのである。評判を脅かすリスクは重大である。」2004年違反調査より

ファクトシート記載の推奨事項例

SPAM

- スタッフ間でのスパムの認識を高め、スタッフがスパムを受け取る危険度の高い作業を行わないようにする。
- スパムフィルタリングツールの使用を検討する。
- ISPとよりスパムのソースに近い所でスパムを阻止する方法について協議する。
- 業務がスパム関連規制を意識していることを確実にする。
- 電子メールサーバーが安全であり、スパムに利用されていないことを確実にする。

識別マネジメント

- 自社のITシステムへアクセスできる者について慎重に検討する。
- システムへのアクセスは必要に応じてのみ認め、またこれを定期的に見直す。
- 多くのシステムにアクセスするユーザーが数多くいる場合、自動化を検討する。
- パスワード以上のものが必要かどうかを検討する。

スタッフによるインターネット誤用

- インターネットの容認可能な利用方法について明確なポリシーを定める。
- このポリシーをスタッフに周知させる。
- インターネット利用状況を監視し、不適切なウェブサイトをブロックするためのソフトウェアを導入する。
- 業務において事件・事故が生じた場合に何をすべきかについての、明確な危機管理計画を定める。

フォーレンジックの準備 ― 事件・事故対応計画の一部
(FORENSICS READINESS ? A PART OF THE INCIDENT RESPONSE PLAN)

この記事は、コンピュータフォーレンジックとISO/IEC 17799関連シリーズの第1弾である。

ISMSとコンピュータフォーレンジック (ISMS and Computer Forensics)

年齢差別に対する訴訟である Wright 対 AmSouth Bancorp、2003 WL 245588 (2003年2月5日、第11巡回区連邦控訴裁判所) では、原告は被告の従業員5名が2年半の期間に「作成、修正及び/又はアクセスした文書処理ファイル全て」を記録したコンピュータディスク及びテープの証拠開示を求めた。裁判では「..全て..」の妥当性について被告の弁護人から異論があるかもしれないが、一方でこの事例は組織において有効なISMSを維持することの重要性を示している。

コンピュータフォーレンジックは、ハッカー特定などの刑事訴訟や障害の発生したコンピュータの原因究明のためだけではなく、特に法的な意義及び/又は懲戒処分を検討する場合において、組織のISMSとも非常に関連がある。

ISO/IEC 17799:2000 の 12.1.7.1.c)記載の「提示されるべき証拠がシステムによって保管及び処理された期間をとおして, 管理策が正しく, かつ, 一貫して働いていたという十分な証拠 (すなわち, プロセス管理の証拠)」は、証拠の「受け渡し記録の管理」の維持において、証拠を取り扱う者全てが権限を与えられ、その後も追跡記録がとられていることを確実にするのに重要である。また一方、「・・・管理策が正しく, かつ, 一貫して働いて・・・」いることは、「・・・文書処理ファイル全て・・・」の提出を求める裁判所の要請への対応の際にも重要である。訴訟の間に提出された証拠は十分ではなくいくつかのファイルが欠けている、と原告が主張することもあり得るのである。

ISO/IEC 17799:2000 ― 「提示されるべき証拠がシステムによって保管及び処理された期間をとおして, 管理策が正しく, かつ, 一貫して働いていたという十分な証拠 (すなわち, プロセス管理の証拠)」

被告の最良の戦略は、データ検出ポリシー、バックアップポリシー等を伴う、信頼に足るISMSを確立することである。同様に、重要なのは、一貫した実施状況を証明する明確な記録が入手可能なことである。明確なポリシーと記録があることにより、被告側の信頼性は非常に高まるだろう。

証拠の許容性 (Admissibility of Evidence)

ウェブサイト中の全ウェブページが失われたというある一つの事例がある。この事例では、そのウェブサイトのウェブページは全てバックアップされていたが、ウェブサイト運営管理者 (the management) はそのウェブサイトのシャットダウンを決定し、またコンピュータフォーレンジック調査実施のために専門家が呼ばれた。専門家らが現場で環境の簡単な検査と関連スタッフ全員に事情聴取を行った結果、ウェブページの消去は2日前に発生し、システムはウェブページの消去が検出された直後にバックアップのウェブページによって復旧され、そのまま運用が継続されていたことがわかった。

システム管理者がこの復旧を実施していたが、その際に組織の運営管理者に報告していなかった。そのため運営管理者は 2 日後に初めてこの状況を知ったのである。このシステムのハードディスクのイメージはビット単位でフォーレンジックデータ収集ノートブックにコピーされ、そのイメージのチェックサム (ちょうど指紋のようなもの) は現場で顧客担当者によって記録・検証された。このイメージを記録したハードディスクは正式に署名されて保護包装に密封された。

受渡し記録の管理 (Chain of Custody)

電子形式の証拠は簡単に修正及び/又は消去できることから、BS7799-2:2002 の A.12.1.7 における重要なポイントは、証拠の許容性と、証拠の品質及び完全性についてである。証拠の許容性 (ISO/IEC 17799:2000 12.1.7.2) について、主要な問題の一つは、要請のある場合には、その証拠がオリジナルであり、後にこの証拠へ修正を加えることは不可能だったということを法廷で証明することである。前述したように、ハードディスクのイメージについて記録されたチェックサムは、法廷で提示した証拠がオリジナルであるとの証明に役立つ。

証拠保管のため、イメージを記録したハードディスクは複製され、オリジナルコピーのハードディスクの方は安全に保管された。複製されたコピーの方がコンピュータフォーレンジック調査に使用された。さらに、証拠の取扱い、特にオリジナルの取扱いは、認可された要員によって行われ、各アクションについて記録をとらなければならない (ISO/IEC 17799:2000、12.1.7.3 b)。

フォーレンジックの準備 (Forensic Readiness)

このコピーの方のハードディスクに記録されたイメージのレビューに際してフォーレンジック調査を行った結果、システム障害が発生した可能性を明らかに示していたのは、ログの欠落だった。ほとんどのログファイルは消去か、無効化されていた。さらに調査を進めた結果、多くの「有名な」トロイのコードとバックドアがインストールされていたことがわかった。

ほとんど全てのログが入手不可能だったため、原因と侵入方法の特定は不可能ではないにしても、非常に難しいものになった。そのなかで調査員の行える作業の一つは、消去されたファイルの復旧だった。しかし、2日後に調査員が到着した時点では、サーバーが非常にアクティブになっていたため、消去されたファイルが元々保存されていたハードディスクの部分は上書きされており、復旧は全く行えなかった。セキュリティ上の事件・事故は避けられないものである。この事件・事故からの学習は、明らかにセキュリティ事件・事故への対応に際しての主な目的の一つなのである (BS7799-2:2002、A.6.3.4)。

このフォーレンジック調査を通して得られた実際的経験から、より首尾よくフォーレンジックの準備に取り組むには次が必要だといえる。

ログ ―これはほとんどの人が思っている以上に重要である。主要サーバーのログは敷地外に保管するか、又は少なくとも他のシステムに、できればリアルタイムで保管しなければならない。

データ収集ツール ― バックアップと復旧設備は、殆どの事件・事故対応計画において常に主要な要素である。しかしながら、通常バックアップと復旧設備はファイルを基にしており、従って最後にバックアップされたファイルの復旧を目的としている。その為、消去されたファイルについてはバックアップも復旧もなされない。しかし、この消去されたファイルの検索こそが、コンピュータフォーレンジック調査員がまず最初に行う作業のなかで最も主要な作業の一つなのである。ハードディスク、メモリー、他の格納デバイス内のイメージを転送可能な、十分にテストされたデータ収集ツールとその他必要な装置（大型ハードディスクなど）は、事件・事故対応チームにとって必須のツールである。このようなツールによって、調査完了までの間システムをシャットダウンして待機しなければならない時間が大幅に短縮されるだろう。

タイミング ― 「事件・事故」が疑われる場合には、その最初の段階で適任な事件・事故対応チームを呼ぶべきである。

個人からコンピュータ利用侵害の報告を最初に受けるのは、おそらくシステム管理者だろう。しかし、システム管理者は、そのような状況を的確に処理する訓練を受けていないかもしれない。短時間で対応する為に、組織内部又は外部の適切な訓練を受けた者を、最初の対応者（First Responder）として確保可能にしておくべきである。コンピュータ侵害行為のあった可能性が発見された後に最初の対応者がとる処置は、調査、コンピュータシステムのフォーレンジック調査や、将来的に起こり得る訴訟又は管理活動において極めて重大な役割を果たすだろう。最初の対応者の必要性は、次回ジャーナル掲載予定のパート 2 でさらに論じる。

Norman Pan
Doctor A Security Systems (Hong Kong) Ltd

編者記：記録の収集及び許容性に関する法令・用語は国によって異なり、従ってこの記事のアドバイスが有効でない国もある。ISO/IEC 17799 の 12.1.1では、適用される関連法令を明確に定めることが望ましい、と記載されており、また 12.1.7 では、この 12.1.1で明確に定められた法令に適用される証拠の収集に関するベストプラクティスについて述べられている。

情報セキュリティガバナンス（Information Security Governance）

情報セキュリティガバナンスとは（What is it?）

多くの企業は、事業運用のために情報システムをますます使用するようになってきている。その為 IT と情報セキュリティ（IS）に付随するリスク、利便性、機会の検討を余儀なくされている。つまり、今やIT&ISガバナンスは、より広範な企業のコーポレートガバナンスの一部を形成していなければならないのである。

一連の技術的対策、組織的対策、人的対策によって保護は提供される。これが、*入手可能な資源と予算に基づく『適正な保護バランス』*を発見できる鍵となる。

『IS ガバナンス』アプローチによって、企業は自らを賢く保護することができるようになる。というのも、ビジネスニーズやリスクの合理的な評価に基づいて、必要で適切なレベルで保護できるようになるからである。また2003年には次の３つのリスク領域が新たにみられるようになった。

- 情報及び信頼システムの可用性に関する要求事項の増加
- 情報の誤用／悪用の潜在的可能性の増大 ― プライバシー問題に影響。
- ハッカーによる、外部からの危険性 ― サービスの妨害、ウイルスの攻撃、さらには場合によっては恐喝の恐れ。

このようなことから、今や次の質問を企業が自らに問いかけてみる時期にきている。

現在の情報セキュリティプラクティスの程度は？

- セキュリティが適切に取り扱われているという確信があるか。
- 最新のセキュリティ問題やベストプラクティスを認識しているか。
- 競合他社は情報セキュリティについて何を実施しているか、またそれを自社とどのように比較するか。
- 情報セキュリティに関する事業上の要求事項について概略を描いているか。
- 情報セキュリティにどの程度投資するかについて、見解をもっているか。
- セキュリティリスクや入手可能なテクニカルソルーションについて、迅速に対応しているか。
- セキュリティ状況やセキュリティプロジェクトについての経過報告書を入手しているか。
- 自身の情報セキュリティ体制の独立レビューを実施したことはあるか。

2004年は重要な年（MILESTONE YEAR）

Butler Group社によれば、2004年ではガバナンスの全領域が明確になっており、同社によると、次の５つが最重要課題となると予測されている。

1.準拠 ― プライバシー問題及び米国企業改革法などの法令
2.ガバナンス ― 大企業の多くは、IT ガバナンスプラクティスの実施に意欲的である*。
3.情報収集 ― 企業の多くは投資収益を得る方法を検討している。
4.集積 ― 過去の投資からの論理的向上
5.アウトソーシング

*このプラクティス開発は、リスクマネジメントから始まり、枠組みモデルとして ISO/IEC 17799 を導入した情報セキュリティガバナンスに至ると予想されることから、情報セキュリティガバナンスはこの開発において必須の要素となるだろう。

IT Governance Institute の詳細情報については、vernon.poole@sapphire.net までお問い合わせください。

Vernon Poole, IT Governance Institute
and Sapphire Technologies

「一連の技術的対策、組織的対策、人的対策によって保護は提供される。これが、入手可能な資源と予算に基づく『適正な保護バランス』を発見できる鍵となる。」

内部監査の実施（DOING AN INTERNAL AUDIT）

このシリーズの第１回（ISMS ジャーナル第１号）では、情報セキュリティ問題の取扱者が一連の業務のなかで関連をもつ可能性のある、様々な監査員のタイプについて説明した。第２回（ISMS ジャーナル第 2 号）では、認定第三者審査のプロセスについて説明した。今回は、内部監査に初めて取り組む新人の観点から監査のプロセスの概観を説明する。

監査とは何か？（What is an audit?）

監査とは、内部の影響を受けない者（コンピュータプログラムの場合もある）が行う、活動の調査のことである。これは、人は自らを監査することはできず、また所属するチームの業務や委任元の業務の監査も行えない、ということを意味している。しかし、BS 7799-2（と ISO 9000 シリーズ）には、自身の業務をチェックし、全活動に対する有効なマネジメントレビューを確立することを求める要求事項がある。

「自分自身の業務に対する監査でなければ、誰でも監査を実施することができる。組織のなかには『内部監査員』と呼ばれるグループを置いているところもあり、このグループは通常、全ての内部監査業務を委任されている。」

同様に、多くのセキュリティソフトウェア製品やコモンクライテリアではログの作成プロセスを『監査』として説明しているが、例えばログ維持活動など、いかなる形式であれログの作成は監査ではない。

監査の実施は過去又は現在の活動に基づいており、監査結果は監査報告書にまとめられる。監査報告書を読んだ人のなかには、通常、監査員が監査に基づき業務に『問題なし』としている場合には、大幅な変更のない限り今後も引き続き『問題なし』だろうと思う人がいる。しかし、この考えは、場合によっては間違っている。

監査は頻繁に実施する活動ではない。その為、活動が日々正確に実施されていることを確認するためにより頻繁に実施される、有効なマネジメント管理策の代わりとはならない。

事件・事故や他の例外事項のための特別調査は、内部監査員が実施しても、通常、監査として分類されない。

監査は誰が実施するのか？（Who may perform an audit?）

自分自身の業務に対する監査でなければ、誰でも監査を実施することができる。組織のなかには『内部監査員』と呼ばれるグループを置いているところもあり、このグループは通常、全ての内部監査業務を委任されている。しかし、時として、ある業務を実施するのに必要な能力がこのグループになかったり、このグループが忙しく組織内の他の者（又はチーム）が監査業務を実施するよう要請されたりすることもある。

専任の内部監査員に対しては、監査協会、内部監査人協会（IIA：Institute of Internal Auditors)、国際セキュリティ監査コントロール協会（ISACA：International Security, Audit and Control Association)、国際認定審査員登録機関（IRCA：International Register of Certified Auditors）などの組織発行の監査資格の取得を奨励すべきである。

ある特定の状況、特に監査の実施が規制要求事項の場合は、その監査を担当する監査員のうち少なくとも１人が監査実施前にこれらの資格を取得しておくのが最も良い。

監査目的（Audit Objectives）

すべての監査には目的がなければならず、この目的の種類によって実施作業の内容と目的達成法が決まる。

監査目的には、次の基本的な 2 つの種類がある。

a）手順（又はプロセス）が、この手順を定めたマニュアルに従って、適正な人員及び／又はソフトウェアによって実施されていることを確認する。例えば、

- システムのアクセス権が適切な管理者によって認められている、
- リスクアセスメント文書に記載の通り、リスク分析が実施されている、等である。

この種の監査は、よく順守監査（Compliance audit）と呼ばれる。

b）活動の結果が想定通りであることを確認する。例えば、

- 許可又は拒否されたアクセスが関連業務／人員（ソフトウェア）にとって適切である。
- リスク分析で全てのリスクが識別されている、等である。

この種の監査は、よく実体監査（Substantive audit）とよばれる。

監査では何が行われるのか（What does do on an audit?）

最初の業務は、監査の範囲と目的を設定することである。また、必要な場合には、総合目的を実施すべき個々の監査や業務に分類する。この後、作業のためのプログラムと時間割を作成し、必要な資源を割り当てるべきである。このプログラムは、例えば、毎年全ての側面を監査できるように ISMS 全体を対象としたものかもしれないし（これは BS 7799 Part 2:2002 の要求事項)、また例えばアクセスコントロールといった１つの側面のみを対象としたものかもしれない。

一般に、個々の監査は次のステップで実施される。

a）計画策定
- 範囲と目的の確認
- 費用効果的な業務実施方法の決定
- 実施業務の取り決め
  - ○ 作業実施のための資源割当て
  - ○ 監査対象（被監査者）との日程調整

b）必要な管理上の取り決め

c）作業実施
- 計画した業務の実施
- 実施状況の証拠の記録
- 被監査者の実施状況が不十分なところの特定

・ 活動において改善の必要な領域の特定

d) 結論のための証拠の記録

e) 作業のレビュー

・ 結論が証拠によって適切に裏付けられていることを確認する。

・ 計画が全て実施されたことを確認する。

f) 報告及びフォローアップ

・ 経営陣に所見を報告する。

・ 経営陣への提言についてフォローアップを行う。これはたいてい次回の監査で実施する。

・ 要求に応じて監査プログラム全体を修正し、監査プロセスの改善事項を明確にする。

注：『監査プログラム』と『監査計画』という用語については、マネジメントシステム監査のための指針である EN ISO 19011:2002 の定義に従って使用した。他の監査文書では、これらの用語を反対の意味、つまり、プログラムとは個々の監査における詳細な作業、また計画とは全体的な監査計画という意味で使用されている。

作業の実施（Performing the Work）

手順への準拠を確認することが目的の場合、監査作業では通常、その手順の使用状況のサンプルを選択し、規則が守られているかどうかを判断するために実施業務全てに沿って追跡する。しかし、手順そのものの改善の必要性や、その手順では目的が達成されていない可能性もあることを監査員は知っておくべきである。その結果、たとえスタッフが規則に従っていても、こういった理由から監査員が改善の必要な領域の報告を希望することもある。

プロセスの結果を確認することが目的の場合、上記の手順は最も費用効果的な監査方法ではない可能性がある。例えば、

・適切な権限なしにある特定の資産にアクセスできるかどうかを確認することが目的の場合、権限なしでアクセスを試みるのが一番簡単なテストかもしれない（侵入テストは専門的な監査法である）。

・人員によるアクセスが職務明細書及びアクセスコントロールポリシーに合致しているかどうかを確認することが目的の場合、関連する権限事項を含むアクセス表のチェックが適切かもしれない。

相違や誤りが発見された場合、監査員は使用されている手順の改善方法に関する提言を検討すべきである。

多くの場合、改善は見解の問題であり、実際に発生した誤りについての具体的事実がその事例改善のために役立つ。

監査員へのアドバイス（Some tips to auditors）

全てを監査するのは不可能であり、従って効果的な監査の秘訣は最小の時間でチェック可能な最大の範囲の作業を行うことである。そのためには、全体のなかから効果的なサンプルを選択することが必要となる。

監査員にとって現状を 100%把握するのは不可能であり、その為監査員は、スタッフが理解していることや何故その業務を行っているかについて彼らが説明する際に、いつも注意深く話を聞く。例えば、『もし予想通りに業務が進まない場合どうなりますか。』といった説明の必要な回答を導き出す積極的な質問をするとよい。そのような回答からは、単なるはい／いいえといった回答よりも多くの情報を得ることができる。

ある問題について監査員がスタッフとは異なった見解をとった場合、その違いを明確に説明し、両者ともこの違いについて理解することが重要である。多くの場合、協議の間に問題は解決され、適切な処置について監査員とスタッフの間で合意することが可能である。これが不可能な場合、見解の異なる正確な理由を経営陣に提示することが可能である。このプロセスによってスタッフと監査員によるフォローアップへの取り組みを最小化することができる。

改善のために監査員が行う提言が全て建設的、実際的、費用効果的で、かつ関連スタッフに歓迎されるものとなるよう努力するとよい。注：認定第三者監査員は、システム改善のための提言を行うことはできない。

監査ガイダンスはどこで入手できるのか（Where can a person obtain audit guidance?）

監査ガイダンスは様々なところから入手できる。いくつかを次に示す。

・EN ISO 19011:2002 － 英国規格協会（及び他の規格協会）

・英国規格協会 PD3000 シリーズ（www.bsi.org.uk）

・ ISACA （International Security Audit and Control Association：国際セキュリティ監査コントロール協会）？ www.isaca.org

・IIA（Institute of Internal Auditors：内部監査人協会） － 英国内 www.iia.org.uk、海外 www.theiia.org

・イングランド・ウェールズ勅許会計士協会（www.iceaw.co.uk）

・管理会計士協会（www.cima.org.uk）

・スコットランド勅許会計士協会（www.icas.org.uk）

・公共財務会計協会（www.cipfa.org.uk）

・米国公認公共会計士協会（www.aicpa.org）

「全てを監査するのは不可能であり、従って効果的な監査の秘訣は最小の時間でチェック可能な最大の範囲の作業を行うことである。そのためには、全体のなかから効果的なサンプルを選択することが必要となる。」

リスクの伴うビジネス－人的資源（A RISKY BUSINESS ? HUMAN RESOURCES）

ISO/IEC 17799 と BS7799-2 では、かなり広範な脅威やリスクが取り扱われている。このなかには、ビジネスプロセスやアプリケーションに関連するリスクや、法的適合・規制への適合、第三者供給者によるアクセスや外部委託協定などが含まれる。この記事ではこの 2 つの規格に沿って、情報セキュリティの人的資源面に関連するリスクを考察する。

主要な資源（A Critical Resource）

スタッフや従業員は組織内の最も価値ある資源の一つである。適切な能力のあるスタッフなくしては、組織を効率的かつ有効に運用することはできない。一方、人的資源は組織に最も深刻なリスクをもたらす可能性もある。これらのリスクは、偶発的な事故、人的な誤り又は手違い、あるいは計画的／意図的な攻撃に関係する可能性がある。組織は、スタッフが日常業務を行うために、機密情報及び／又は重要な情報に対する様々なレベルのアクセス権をこれらスタッフに与えている。これらの権限は適切に用いられているかもしれないが、誤用されておりその結果個人的利益及び／又はビジネスの消失を目的として悪用されているかもしれない。人的資源のマネジメントは、情報セキュリティの確立と維持に密接に関連しているのである。

資源管理（Resource Management）

それでは、情報セキュリティ保護に関して人的資源面が管理されていることを確実にするために、組織は何をすべきなのだろうか。ISO/IEC 17799 には、人的資源に関連するベストプラクティスも記載されている。次に示すのは、ISO/IEC 17799 ベストプラクティスに基づく検討すべき重要な質問のチェックリストである。

「スタッフや従業員は組織内の最も価値ある資源の一つだが､最も深刻なリスクをもたらす可能性もある。」

- 例えば、応募者の資格、照会先、能力のチェックといった、適切な人員募集手順を実施していますか。
- スタッフに対し適切な研修や意識向上を行っていますか。
- その仕事の業務要求事項に従って、一連の適切なアクセス権限及び責任を割り当てていますか。
- 例えば、インターネットサービス、又は業務用アプリケーションやプロセスのスタッフによる誤用・悪用を防ぐための管理策を実施していますか。
- 有効なスタッフ手順を導入していますか。
- 情報セキュリティに関して、十分な支援とコミットメントをスタッフに提供していますか。
- 適切な雇用終了手順を実施していますか。

リスクのアセスメント及びマネジメント（Assessing and Managing the Risks）

組織の成功と安定にとって人的資源は非常に重要なことから、資源管理に関してリスクアセスメントを行うのは重要である。このリスクアセスメント実施後に、ISO/IEC 17799 のベストプラクティス実施を含め、これらのリスクを取り扱うための経営陣の適切な活動を実施すべきである。

同様に、実施されている経営陣の活動や管理策の有効性を定期的にレビュー・監視するために行う必要のある、継続的なマネジメントプロセスも重要である。この実施、監視、レビューのライフサイクルを示す事例は数多くある。業務システムや情報へのアクセス権は、個々の職務権限に基づいて割り当てるべきである。これらの権限は、業務や個人の職務権限の変更を考慮する為に定期的にレビューすべきである。また、人員が組織を離れる際のことも忘れるべきではない。全アクセス権限を取り消し、業務システム上の全アカウントを閉じ、その人員が在籍時に使用していた組織の財産を返却するようにしなければならない。これらの処置は、適時、実施しなければならない。

偶然又は意図的な行動や意思決定によって起こる、スタッフ・従業員の日常業務に関連するリスクや影響は数多い。

- 人的な誤りは、情報の処理時や業務用ソフトウェア使用時に起こり得る。これらによって、組織へのリスク度が変化する結果となる可能性があり、また実際そうなっている。このような誤りは、研修や意識不足、あるいは従業員がプレッシャーを受けてストレスがたまったり、超過労働していたり、あるいは行うのに適切な資格のない業務を与えられたことが原因で起こり得る。
- また、組織は個人的利益を得たいと望む従業員によるリスクにもさらされている。これには、詐欺行為、偽造記録、その他の活動などがある。
- 従業員は不満を抱いたり、幻滅したり、あるいはまた不公平な取扱いを受けていると感じているかもしれず、こういった感情によって組織に対し否定的な行動をとる可能性がある。これは、出世に関する不満や、又は職務権限や作業割当てについての決定に対する不満によることもある。
- 従業員による組織の IT やネットワーキング資源の悪用や誤用は、ビジネスに対する深刻なリスクとなる可能性がある。

これらのリスク全てや他のリスクに対してはアセスメントを実施し、組織がビジネスに対する損失、消失、損害に直面するのを回避するために、状況を管理する為の経営陣の適切な活動を実施する必要がある。どのような管理策を実施するにしても、これら管理策によって継続して組織のリスクがマネジメントされていることを確実にするために、その管理策を定期的にレビュー・監視しなければならない。

BS 7799-2 及び ISO/IEC 17799 関連のリスクアセスメント方法や手法、BS 7799-2 及び ISO/IEC 17799 の要求事項の実施を支援するリスクアセスメント／マネジメントツールについての詳細情報については、www.aexis.de を参照ください。

Angelika Plate（ドイツ ISMS 支部議長）

国際規格概要－SC27（INTERNATIONAL STANDARD PROFILE SC27）

国際規格概要シリーズを今号から始めた。この最新シリーズの初回となる今回は、ISO/IEC JTC 1/SC 27 の業務を概観する。

SC 27 は、セキュリティ規格分野における専門家の集まる国際的な委員会ある。SC 27 は、現在既に商取引や産業界で利用されている、数多くの規格を作成した委員会である。また最近では、企業の成功と安定に必須の資産保護を将来的に世界的レベルで改善することを目指した規格作成プログラムが策定されている。この委員会には３つのワーキンググループ（WG）があり、各 WG にはそれぞれ独自の業務プログラムがある。

WG 1（Security Management：セキュリティマネジメント）

このワーキンググループでは、セキュリティマネジメントに関して、ベストプラクティス的なアドバイスや仕様を組織に提供する規格を作成している。これらの規格には、ビジネスが直面するリスクを管理するためのマネジメント的管理策について、その枠組みを確立する方法が記載されている。例えば、セキュリティポリシーや手順、リスクアセスメントのプロセスや情報システム、業務アプリケーション、プロセス、ネットワークへのアクセスや、これらの安全な利用のための日常的な業務運用に採用されるプラクティスなどについて記載されている。WG1 の業務の例としては次のようなものがある。

・情報セキュリティマネジメントの実践のための規範 [ISO/IEC 17799]

・ICT セキュリティマネジメント（MICTS － 以前の GMITS）[ISO/IEC 13335]

・IT ネットワークセキュリティ [ISO/IEC 18028]

・情報セキュリティ事件・事故マネジメント [ISO/IEC 18044]

・侵入検出[ISO/IEC 15947 及び ISO/IEC 18043]

・信頼できる第三者機関[ISO/IEC 14516]

WG 2（Cryptographic Techniques：暗号技術）

SC 27 規格の相補的なファミリー規格は、個々の IT セキュリティポリシーや手順実施のための手法及びメカニズムの分野を担当するワーキンググループ、WG2 によって作成されている。例えば、情報の機密性を保護するための暗号技術、システムへの許可されたアクセスを実施するための識別及び認証メカニズム、電子取引や電子文書の完全性及び真正性を保護する為のデジタル署名技術などである。WG2 の業務の例としては次のようなものがある。

・デジタル署名[ISO/IEC 9796 及び ISO/IEC 14888]

・認証[ISO/IEC 9798]

・暗号化アルゴリズム [ISO/IEC 18033]

・鍵管理 [ISO/IEC 11770]

・否認防止

このグループ作成の規格は、スマートカードへの暗号手法の埋め込み、様々なソフトウェアアプリケーションの導入、通信機器や装置の開発など、様々なタイプの技術分野に及んでいる。

WG 3（IT 製品及びシステムのセキュリティ評価：Security Evaluation of IT Products and Systems）

このワーキンググループでは、IT システムの定義・配付と製品の評価・保証に関する規格を作成している。例えば、製品導入のための個別のセキュリティ要求事項を定める手順や IT セキュリティ保証に関するガイダンス、セキュリティを提供する IT 製品評価のための基準や方法論などである。この基準は、スマートカード、オペレーティングシステム、データベース、ファイアウォールなどの製品やシステムを評価するために使用される。WG3 の業務の例としては次のようなものがある。

・IT セキュリティ評価基準（コモンクライテリア）[ISO/IEC 15408]

・保護プロファイル[ISO/IEC 15446 及び ISO/IEC 15292]

・暗号化モジュールのセキュリティ要求事項（この業務は WG 2 と共同で進められている）

・セキュリティ評価の枠組み及びバイオメトリック技術検査（この業務は WG 2 と共同で進められている）

連係（Liaisons）

SC 27 とその３つのワーキンググループは、規格作成や、また今後の要求事項の特定に関して、他の規格作成組織・委員会と共同で作業を進めている。連係先としては、ITU-T（電気通信標準）、ISO TC68（銀行業標準）、SC 37（バイオメトリクス）、SC 6（ネットワーク標準）などが挙げられる。

SC 27 委員（SC 27 Membership）

SC 27 には、投票権をもつメンバー31 カ国、オブザーバーメンバー9 カ国が参画している。SC27 業務への寄稿は 31 か国の規格作成機関（National Standards body）から寄せられており、また上記の連係グループからも寄せられている。

Ted Humphreys
SC27 PR Officer、SC27/WG 1 議長

「SC 27 は、セキュリティ規格分野における専門家の集まる国際的な委員会ある。」

ISMS International User Group ウェブサイト www.xisec.com を参照下さい。

情報セキュリティマネジメントのベストプラクティスとその認証を求める国際社会からの過去 12 年間にわたる要望に応え、ISO/IEC 17799 と BS 7799 Part2 という 2 つの規格が作成されました。これら規格の適用及び使用は、情報セキュリティマネジメントの「共通語（common language）」として世界中の多くの国々で組織の規模の大小を問わず受け入れられています。ISMS International User Group は、ビジネス主導の、ISO/IEC 17799 と BS 7799 Part 2 ユーザーの国際的なネットワークです。BS 7799 規格の国際的な普及を促進するために、ISMS International User Group は、この規格の利用に関する経験を共有する手段を円滑にすることを目的として 1997 年に DTI（Department of Trade and Industry：英国貿易産業省）によって設立されました。1997 年以来、International User Group は成長を続け、今では 3000 人以上の専門家らの参画する国際的なネットワークとなっています。この専門家らの多くは、International User Group 支部に所属しており、この支部は、現在、オーストラリア、ブラジル、カナダ、ドイツ、香港、日本、韓国、シンガポール、スウェーデン、米国、英国の、世界 11 カ国に設置されています。

ジャーナル ― 次号案内（JOURNAL ? FUTURE ISSUES）

投稿（Contributions）

次号以降に投稿をご希望の方、又はトピックやテーマについてご提案のある方は、編集者までご連絡ください（7799@xisec.com）。

解釈（Interpretations）

ISO/IEC 17799 と BS 7799-2 についてのご質問のある方、又はこれらの規格の要求事項について ISMS Foundation の正式な解釈をご希望の方は、7799@xisec.com までご連絡ください。

ISMS 事例（ISMS Experiences）

ISO/IEC 17799 と BS 7799-2 についての見解やご経験をお寄せください。

- aexisap@aol.com
- dbrewer@gammassl.co.uk
- 7799@xisec.com

定期購読／定期購読の解除（Subscribe/Unsubscribe）

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 JOURNAL 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 JOURNAL と入力して journal@xisec.com へ電子メールをお送りください。

第 4 号の特集

- フォーレンジックの準備 ― パート 2：最初の対応者の必要性
- 国際規格規格概要 ― ITU-T
- GBLA、SOX、及び ISO/IEC 17799
- 危険の伴うビジネス パート 2 ― 事業資源の可用性及び継続性
- 業務処理上の誤り ― パート 2