平成１７年度（第２０回）
学術及び総合情報処理センター長会議基調講演における質問への回答

（１）「情報セキュリティマネジメントの重要性」

（質問１）

何に対するセキュリティを重要視するのか。規準はありますか。（自分で考えよですか。）

（回　答）

組織にとって情報そのものが価値のある場合、情報を犯罪や災害等から適切に保護することが重要である。情報を保護する上では、情報そのものだけでなく、それを利用するシステムや人なども保護対象となる。情報セキュリティの目的は、単に情報を守るだけでなく、適切な利用環境を維持することも含まれており、必要な時、必要な情報を活用しながらいかに情報を保護するかということである。組織の情報セキュリティを確保するためには、保護すべき情報資産ごとにリスクアセスメントを行い、リスクを低減させるためのセキュリティ対策を実施し、監視し、継続的に改善することである。

情報セキュリティマネジメントの国際規格として、ISO/IEC 17799:2000（JIS X 5080:2002）**が制定され、その改訂版が２００５年６月１５日に発行されている。この規格は、先進的企業のベストプラクティスをカテゴリー別に区分し、情報セキュリティの実践規範としてまとめたものであり認証規格ではない。認証規格は、英国規格** BS 7799-2:2002 **をベースに** ISMS **認証基準（**Ver.2.0**）が２００３年４月に制定されており、情報セキュリティマネジメントシステムの要求事項がまとめられている。このように国際規格** ISO/IEC 17799 **及び** ISMS **認証基準（**Ver.2.0**）は、情報セキュリティマネジメントについて理解する上での共通言語となっている。**

（質問２）

セキュリティレベルの決め方について、合理的方法はあるのか。

（回　答）

セキュリティレベルの決め方について、特に合理的な方法があるわけではない。ISMS **の特徴は、組織自らがそれぞれの自己責任においてセキュリティレベルを決めることができる。このことは、一定レベルの基準をクリアすることを要求していないので、各組織の事業内容はもちろん、運用形態、事業規模などの条件によって、情報セキュリティの重点項目も異なっている。このように、環境が異なるところへ同じレベルの対策を求める必要はなく、対象とするリスクの程度やどのように対策を講じていくかなどは、各組織の判断に任せており、リスクアセスメントの結果に応じたセキュリティレベルは、各組織で検討するのがベストだという考え方である。また、リスクアセスメントには様々な手法があり、個々の手法の種類とそれらの長所・短所を知り、その上で組織の特徴に合わせたリスクアセスメント手法を選択することが重要である。**

（質問３）

リスク評価は主観的なもので良いのか。人によって評価が異なるときにそれをどう集約するのか。万が一、情報がもれた場合のリスク(損害)と投資との兼ね合いをどう考えるのか。

（回　答）

リスク評価は、必ずしも定量的に算定することができるわけではないが、関係者が納得できる合理的な指標を用いて、統一的な視点で相対的な比較が可能となるように実施されることが望ましい。また、リスクを定性的にしか把握できない場合には、経験等に基づく推測に

より評価することも考えられる。その場合には、評価者の判断のバラつきについても、リスク評価の初期の段階から具体例を用意し、評価者に十分な説明をすれば、結果をある程度標準化することは可能になるであろう。また、あくまでリスク評価実施時のリスク環境であるため、情報資産の資産価値や脅威、ぜい弱性等の環境に変化が生じた場合は、適宜リスク評価の見直しをすることが重要である。その結果、リスク（損害）が発生した場合の損失の回避・軽減を図ることが可能となるからである。

このようなことから、組織が求めるセキュリティレベルによっては、もっと簡易なリスク評価方法でもよい場合や、逆にもっと厳密かつ詳細にリスク評価する必要もある。必ずしもこうしなければいけないということではないが、その組織に合ったリスクアセスメント手法を選択することが重要である。リスクアセスメントの実施で期待されることは、個々の情報資産が持つリスク、リスクに対する適切なセキュリティ対策、及びセキュリティ対策に投じるべきコストを識別できることである。リスクは時間の変化や環境要因などで動的に変化するものなので、適宜リスク評価を行いセキュリティ対策の実装状態などのレビュー及びその有効性を評価するための手段も必要となる。

（質問４）

認定機関を誰が審査しているのか。経産省？

（回　答）

ISMS 制度は民間の任意分野として存在しており、特に認定機関の審査はない。しかしながら制度を運営する認定機関は、一定の品質をもつことを保証するための要求事項である国際規格の ISO/IEC 17011:2004（JIS Q 17011:2005）に適合させる必要がある。そのことにより、国際的な認定機関の集まりである IAF（International Accreditation Forum：国際認定フォーラム）では、各国の認定プログラムの同等性を促進するとともに、認定機関間の相互承認協定（MLA：Multilateral Recognition Arrangement）を締結することを要件としており、相互の認定プログラムが同等であることを相互審査（Peer Evaluation）により担保している。

（質問５）

この認証制度は品質保証や環境マネジメント認証などとアプローチにおいてどう異なるのか。PDCA という観点では全く同じであるが、情報セキュリティという点でＩＳＯ９０００や１４０００の制度設計と異なるのはどういう点であるのか。

（回　答）

ISMS 制度は、情報セキュリティマネジメントを対象とした第三者による認証制度であり、アプローチにおいて ISO 規格をベースとした品質マネジメントシステム（ISO 9001）や環境マネジメントシステム（ISO 14001）などと同様の制度である。ISMS における管理手法としてプロセスアプローチを採用し、それを実現するための考え方として PDCA モデルを提示している。すなわち、ISMS プロセスは PDCA サイクルを継続的に繰り返すことにより、改善を加えながらそのスパイラルアップによって情報セキュリティレベルの維持・向上を目指し続けることにある。ISMS では、リスクアセスメントの結果により、必要なセキュリティレベルを決め、プランを持ち、資源を配分してシステムを運用することが要求されており、対象とするリスクの程度やどのように管理策を講じていくかなどは、各組織の判断に任されており、具体的な対策は 127 項目の「詳細管理策」から適宜選択することができるのが特徴である。

（質問６）

情報系センターなどの大学職員が審査員研修を受ける(審査員になる)ことに対しご意見を伺いたい。また、そのような事例や相談の有無についても支障のない範囲で教えていただきたい。

（回　答）

ISMS 認証取得は、あくまでも情報セキュリティ対策における出発点である。ISMS の確立、導入、運用及び維持等を行うのは人である。所定の審査員研修コースを終了することにより、初回は審査員補として登録申請が可能である。ISMS 審査員の資格基準として、教育レベル、実務経験、業務経験、研修、個人的資質、推薦などが規定されており、ISMS の審査実績により審査員あるいは主任審査員として登録できる。ISMS は、認証したからよいのではなく、PDCA サイクルを継続的に繰り返し、情報セキュリティレベルの維持・向上を目的としているので、３年間に２回以上の審査に対応する上でも内部監査人としての役割が重要となる。その際審査員補の資格は、組織における ISMS を維持するための内部監査人としての役割がある。組織の各個人が情報セキュリティに関連する責任を果たし、期待される役割を実行する必要がある。そのためには、全ての要員が要求される業務を実施する力量を持つことを確実にするために、教育・訓練の実施が要求されている。特に経営陣は、ISMS の必要性を理解し、経営資源の提供をしなければならない。

（質問７）

個人情報保護法に伴う法規遵守のしくみとの適合性(適合度)を伺いたい。(ユーザーズガイドに具体的なしくみ構築例があるのでしょうか。)

（回　答）

ユーザーズガイドとして、特に具体的な構築例は記載されていないが、個人情報保護法の法規順守性（法規適合性）については、組織あるいは企業にとって不可欠な要求事項であり、ISMS を構築するための有効な出発点である。このことから、組織として法的リスク、経営リスクについて対処する基本方針を策定し、経営に対する影響、重要度に応じてリスクアセスメントし、経営上の観点からリスク対策を実施する必要がある。すなわち、情報資産を洗い出す際に、管理すべき個人情報、関係する法令を特定し、システムに自社の立場、業務を折り込み、法令も　反映した実効性のあるマネジメントシステムを構築する必要がある。

（質問８）

他人メールアドレスの”のっとり”に対処するためには、他人メールアドレスの問い合わせに応えるために組織の認証が必要と思われますが ISMS との関係はあるのでしょうか。

（回　答）

メールアドレスに関する対策としては、ネットワークのアクセス制御や情報システムのアクセス権の管理などがあげられる。情報システムのアクセス権については、利用者登録、特権管理、利用者のパスワードの管理、利用者のアクセス権の見直しといった対策などがあげられる。これらの対策は、組織のリスクアセスメントの結果により、適宜選択することが重要である。

次に、ISMS 制度との関係では、ISMS 認証は情報セキュリティ強度の認証（保証）をすることではなく、組織が適切な情報セキュリティマネジメントを実施していることに対し、第三者である審査登録機関が認証（保証）することである。すなわち、その組織が必要と認めた範囲内の情報セキュリティ対策が適切に実施されている可能性が高いことであり、対外的には組織の情報セキュリティの信頼性をアピールするための重要な手段と考えられる。

（質問９）

情報セキュリティマネジメントと個人情報保護関連マネジメントとの統合化または包含関係は。二重のマネジメントになるか。

（回　答）

個人情報保護法に対応したコンプライアンス（法令順守）を実現するためには、単に個人情報保護法やそのルールに従うだけでなく、多数の準拠すべきルールに従って組織を運営する必要がある。ISMS では、個人情報保護法一つだけを守るというわけではなく、組織にとって様々な法律に対応することが要求されており、個人情報保護関連のマネジメントを包含するものと考えられる。

また、ISMS は体系的で全経営活動に統合されたマネジメントシステムであり、コンプライアンスプログラムの基盤として構築することが可能である。このことは、実質的には ISO 9001、ISO 14001 と共通のマネジメントシステムとの整合化を図ることができる。

（質問 10）

ISMS と P2-7 との相異についてご説明いただければと存じます。

（回　答）

ISMS と P マークとの相異について説明する。

ISMS と P マークは、それぞれ独立した制度であるが、両制度の共通点としては、組織がマネジメントシステムを構築するプロセスは共通しており、PDCA サイクルを継続的に実践し、運用体制を見直し改善することが求められている点である。

ISMS 制度は、組織が構築した ISMS が、ISMS 認証基準の要求事項に適合しているかどうかを第三者機関によって評価・認証する制度である。ISMS の適用範囲は、組織自らの意思により決定することができるので、組織全体あるいは特定の部門・事業所（大学の場合は、学部や特定の事務組織など）を単位として認証を取得することが可能である。また、ISMS の対象となるのは、情報資産であり、情報資産を適切に保護するため、技術的なセキュリティのほか、人的セキュリティを含む組織全体のマネジメントとして取組む必要がある。

P マーク制度は、個人情報の取扱いについて適切な保護措置を講ずる体制を整備している事業者などのコンプライアンスプログラム（方針、組織、計画、実施、監査及び見直しを含むマネジメントシステム）が JIS Q 15001：1999 に適合しているかどうかについて評価・認定を受け、その旨を示すものとして P マークのロゴを付与される制度である。P マーク制度の目的は、個人情報保護に関する消費者の意識の向上を図る。事業者が個人情報を適切に扱っているかどうかの判断材料を消費者に与える、民間事業者の個人情報保護措置に対してインセンティブを与えることである。P マークの適用範囲は、原則として組織全体であり、一定の要件を満たさない限り部門ごとや事業所単位での取得は認められていない。対象となる資産は、個人情報であり、個人情報を対象としてコンプライアンスプログラムを確立し、その後も組織のコンプライアンスプログラムの継続的な見直しを実施する必要がある。

（質問 11）

認証を受けるためのコスト的な面はどの程度でしょうか。

（回　答）

ISMS 認証取得に係わる直接的な費用としては、審査登録機関に支払う審査費用、セキュリティ対策費、教育費、ISMS 構築に係わる人件費、コンサルタントなどの支援業務委託費用などが考えられる。これらの費用は、認証取得する組織の方針や状況(適用範囲、規模、セキュリティ保証の程度など)によって異なる。認証審査に係わる審査工数は、審査の種類（初

回審査、サーベイランス審査、更新審査、臨時の審査、フォローアップ審査等）や審査対象となる ISMS の状況（組織の人数、関連部門の数、組織の業務特性、サイト・事務所の数、情報処理設備の量、技術の複雑さ、セキュリティ要求の程度、法的要件の程度等）によって異なってくる。審査費用の詳細については、審査登録機関に問合せされたい。

（質問 12）

認証に要する費用は初回審査時いか程必要か。毎年のサーベイランス時いか程必要か。

（回　答）

ISMS 制度は、品質や環境の認証制度と同じように国際規格に基づいて審査が実施される。審査内容は二段階審査で行われ、第一段階の審査は ISMS の構築状況及び基本文書・手順書類等について審査がある。第二段階では、ISMS 運用の有効性などを記録などの証拠によって確認する審査である。審査工数は、人員、サイト、インフラなどの適用範囲やリスクの大きさに依存している。ISMS 認証に要する費用は、適用範囲、審査対象規模や審査日数によって異なってくる。審査登録機関の初回の審査料は、審査工数にもよるが一般的にはおよそ 100 万～200 万円程度である。毎年のサーベイランス時は、初回審査のおよそ１／３程度、３年後の更新時にはおよそ２／３程度である。

（２）「静岡大学における情報セキュリティマネジメントの取り組み」

（質問１）

情報資産の評価とリスク対応計画の全学的な検討での問題点、ポイントはなんでしょうか。（静岡大学における）･･･この点については，お答えの中で一部おうかがいできましたのでご参考まで。

（回　答）

全学を適用範囲として考えるのにはかなりの労力を要すると思われます。私どもは、とにかく適用範囲をセンター内の情報資産にとどめ、管理の行き届いた中での基準作りに焦点を絞りました。ですが、認証を受けた後の全学的な影響は徐々によい効果が見られてきていると思います。CIO は徐々に適用範囲を有意味な形で拡張していくことをお考えですし、認証を受けないまでもその基準に則って運用を整備すること自体が重要であると考えます。

（質問２）

仕事量の増加はいかほどでしょうか。

（回　答）

まず、情報資産を洗い出して、それを管理できる形にするまで、そして管理のための手続きを文書化するまで換算はできませんが、かなりの仕事量があることは事実です。しかし、そうした仕事がセンター内の大きなかつ重要な仕事であると位置づけることで、その他の運用よりも時間をかけるという意志決定もできます。

（質問３）

マニュアル化のようですが、どの程度のマニュアルが配布されるのでしょうか。

（回　答）

手順書レベルのものまで含めるとかなりの数ですが、それは適用範囲内の人間が常に最新版を参照できる形にしておけばよいので、電子版を共有ディスクフォルダーにおいて管理しています。

（質問４）

学内の理解を得るための努力の KEY はなんですか。

（回　答）

「今後の大学の危機管理の最重要課題である。」ことを常日頃から役員会などでお話ししておくことだと思います。時間はかかります。しかし、ご理解いただけたものと思っております。

（質問５）

ISMS はセンターとして取得しているのか。あるいは大学として取得しているのか。

もし、センターとしている場合、他のセキュリティレベルの高い学務情報(学生関連)等を扱う部局で ISMS 取得の計画はあるのか。

（回　答）

現在は、総合情報処理センターだけで認証を受けております。これを徐々に拡張する計画は CIO がお考えでありますが、今は明確なものではありません。

（質問６）

最近の公共端末へのフィルタリングソフトの導入については、どう考えているのか。

（回　答）

教育研究とは関連しないサイトへアクセスして利用することは、それ自身大学としてはある意味脅威となり得る可能性がございます。それをふまえ、平成 18 年度にリプレースされる

情報基盤では、フィルタリングソフトを基本仕様の中に位置づけました。

（質問７）

情報セキュリティ委員会とセンター長との関係はどうなっているのか。

（回　答）

情報セキュリティ委員会の委員長は、学術・情報担当理事であり、総合情報処理センター長は、情報セキュリティ委員会の委員となっており、学術・情報担当理事からその権限のある部分を委任されております。

（質問８）

セキュリティポリシーの下での具体的な手順やパラメータ設置について全学的な取り組みが行われているのか。それともセンターのテリトリー範囲内での ISMS の構築にとどまっているのか。

（回　答）

センター範囲内での構築にとどまっております。

（質問９）

サーベイランスのための資料作成に時間がかかりすぎるという問題はないのか。

（回　答）

時間はかかります。かなりの労力ではあると思いますが、いったん作成してしまうとその後の修正はそれほど苦にはならないと思います。さらに、管理が行き届くので心配は減ります。

（質問 10）

具体的な適用範囲は。(センターが管理する機器システム以外を含むのか。)

（回　答）

センターの事務室及び実習室と学内ネットワークの主線の部分を、主な物理的な適用範囲としています。

（質問 11）

対象にした具体的な情報資産は。(支障のない範囲で結構です。)

（回　答）

かなり細かくリストアップしていますが、全部で今のところ 150 程度の項目になっております。

サーベイランスのときにご示唆をいただいたのは、これはかなりまとめて管理する方策を考えた方がよいということでした。物理的な資産、その中の情報、カテゴリーには大きくそのようなものがございます。

（質問 12）

センターの取り組みと学内各部門での取り組みについて、少し説明を補足していただきたい。（参考のために）

（回　答）

現在のところ、総合情報処理センターとして認証を受けてそれがどのような意味を持っているのかを機会あるごとに他部局へ広報している次第です。また、運営委員会など各部局の委員の方がお集まりいただける場では、非常に有意義な意見交換ができます。

（質問 13）

（もしさしつかえなければ）審査にあたって必要となった費用の概略をお教え願えませんでしょうか。（組織の規模、受審内容により異なるであろうことは当然承知しています。）

（回　答）

数百万円単位でお考えください。コンサル料も含めてですが。

（質問 14）

貴重な取り組みの報告と感心しました。ただし、PDCA という言葉の意味を聞きそこないました。お教えいただければ幸いです。

（回　答）

Plan，Do，Check，Action の略です。

（質問 15）

認定（認証）に必要な費用（認定機関へ支払う費用です。）初年度と２、３年目を教えてください。機関によって違うのでしょうか。

（回　答）

料金体系は正確には記憶しておりませんが、初回審査時が百数十万、サーベイランスは数十万単位です。

（質問 16）

情報資産の洗い出しがセンターの職員だけでできるのですか。学部等でさまざまな情報が発生します。これらの洗い出しが大変だと思います。

当初、職員会議はどのような頻度で、どの程度の長さで行ったのですか。

静大の職員構成で検討には充分でしたか。

（回　答）

様々な問題を検討した上で、センター内の情報資産だけに限定して認証を受けております。ですので、管理すべき情報さらにそれを運用する者、どちらも限定されています。全学的な情報資産の洗い出しは非常に大きな作業ですので、これには手を付けていません。職員構成的には正直かなり苦しい部分もありますが、なんとかやりくりしています。

（質問 17）

Ｐ４、サーベイランスにおいて、導入されたデータベースのコスト、規模の概略をお教えください。

このデータベースは学内の最も重要な情報が蓄えられています。学内からの利用の快適性と外部侵入の排除で困難が伴うと思いますが、どのようにバランスを取られたのですか。

（回　答）

今回導入した groupware は百数十万円でした。また、学外との通信は切られています。ですので、職員は学内の自分の PC でアクセスします。

（質問 18）

情報担当理事とセンター長の権限について知りたい所です.

（回　答）

学術・情報担当理事から、総合情報処理センター長は、かなりの権限を委任されていることは事実です。しかし、ISMS の運用に関しては最終的に必ず CIO の management review を受けることが義務づけられています。

（質問 19）

ノート PC に対する特に行っている対処方法があればお聞かせください。

（回　答）

今回の適用範囲で言えば、職員の利用している notebook PC とその中に入っている情報資産が対象となります。これらに対する脅威はかなり大きなものがあります。管理策としては、

内部の HD には重要度の高い情報資産は保存せずに、暗号化されパスワード管理された外付け HD を利用するようにしています。