情報セキュリティ対策ベンチマーク活用集

ISMS認証取得や情報セキュリティ監査の
準備段階での活用を含む多彩な活用例を紹介

情報セキュリティ対策ベンチマーク普及検討会編

はじめに

21世紀に入り、本格的な情報社会への動きがますます鮮明になってきました。企業活動は、まさしく情報活動そのものといっても過言ではなく、企業業績は情報技術の活用力に左右されるようになり、国民生活もまた、ほとんどが情報技術に支えられた社会インフラに依存しています。企業の価値も、これまでの物を中心とした価値から情報や知識を中心とした価値に主軸が移りつつあります。

今後も私たちの社会が継続的に発展していくには、社会を発展させる情報や知識がさまざまな脅威から保護され、社会を支える情報技術が信頼に足るものでなければなりません。これはつまり、企業規模にかかわらず、情報セキュリティが社会の継続的な発展に必要欠くべからざるものになってきたことを意味しています。

しかしながら、企業や団体の情報セキュリティの取り組みは、まだ望まれるほどの効果を発揮しているとは言えません。残念ながら、重要情報や営業秘密の流出は止まらず、消費者の機微な個人情報の漏えいも続いています。

必要な情報セキュリティ対策やそのマネジメントについての国際的な標準化は進み、多くの企業や団体が取り組み始めてはいるのですが、まだその効果が大きく表れているところまでには至っていません。このような中にあっては、情報セキュリティ対策の評価が欠かせません。

情報セキュリティ対策ベンチマークは、このような背景の中で迷っている経営者に、現状を踏まえたうえで、情報セキュリティ対策にどこからどのように取り組むか、どこまでやらなければならないか、などを理解し意思決定する際の指針を提供することを目的としたツールです。

他の企業の平均等との相対比較ができるなどで、発表以来多くの企業に利用され歓迎されていますが、まだこのツールの多彩な使い方の一部しか活用されていないのが実情です。

情報セキュリティ対策の推進を目的とした制度には、ISMS適合性評価制度や情報セキュリティ監査制度が既にありますが、ベンチマークはこれらと肩を並べて、企業の規模や状況に応じて使い分けていただくべきものです。

本書が、これから情報セキュリティ対策に本格的に取り組もうとする企業の経営者や担当者に有効に活用いただけることを期待しています。

2008年1月
情報セキュリティ対策ベンチマーク普及検討会
座長　**大木　栄二郎**

Contents

本書の概要

1 背景

情報セキュリティ対策ベンチマークは、2005年3月に経済産業省が公表した「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」の中で提言された施策ツールである。独立行政法人情報処理推進機構（以下、IPAという）が、企業の情報セキュリティ対策実施状況を自動的に診断するツールとして開発を進め、2005年8月よりWeb上で提供している。

内閣官房情報セキュリティセンターが公表している政府機関統一基準適用個別マニュアル「外部委託における情報セキュリティ対策に関する評価手法の利用の手引き」では、外部委託先の情報セキュリティ対策の実施状況を評価する方法として、「情報セキュリティ対策ベンチマーク」が、「ISMS適合性評価制度」、「情報セキュリティ監査」とならんで紹介されるなど、「情報セキュリティ対策ベンチマーク」は、組織の情報セキュリティ対策を評価する方法として定着してきている。

「情報セキュリティ対策ベンチマーク」は、情報セキュリティ対策の計画段階においても、運用段階においても、組織の情報セキュリティ対策を向上させるために使うことができる。また、ISMSの認証取得や情報セキュリティ監査などの準備段階で活用することもできる。しかし、具体的な活用例が少ないことから、チェックツールとしての活用が多いと思われる。「情報セキュリティ対策ベンチマーク」の有効活用を促進するためには、利用者のニーズに応じた活用例や、ISMS認証取得や情報セキュリティ監査の準備段階として使うためのノウハウなどの提供が必要となる。

このような状況に鑑み、ユーザにわかりやすい「情報セキュリティ対策ベンチマーク」の活用例を作成し、もって、情報セキュリティ対策の向上に寄与するために、各分野の専門家が集まり検討する場として、2007年4月に、「情報セキュリティ対策ベンチマーク普及検討会」が設立された。

本書は、「情報セキュリティ対策ベンチマーク普及検討会」により作成されたものである。

2 対象とする読者と本書の目的

本書は、情報セキュリティ対策ベンチマークの利用者を対象として書かれているが、中小企業、大企業、利用者（使う側）、コンサルタントや委託元など（使わせる側）というように対象者を限定していない。また、実例を参照した、さまざまな活用例を挙げて、情報セキュリティ対策ベンチマーク利用者の裾野が広がる活用法を想定している。

なお、初めて利用する人に、情報セキュリティ対策ベンチマークの使い方を指南するものではなく、既に情報セキュリティ対策ベンチマークを利用した人に、更なる活用のアイディアを提供することを意図している。たとえば、毎年定期的に自組織の情報セキュリティ対策状況を評価することによりステップアップする、委託先や関連会社などの情報セキュリティ対策状況の確認にも発展させる、というような、展開の可能性を示している。

また、組織の情報セキュリティ対策状況の評価を初めて実施する場合には、ISMS適合性評価制度や情報セキュリティ監査はハードルが高いかもしれない。そこで、本書では、情報セキュリティ対策ベンチマークとこれらの関係性を具体的に示し、情報セキュリティ対策ベンチマークをISMS認証取得や情報セキュリティ監査の準備段階で活用するにはどのようにすればよいかの具体的な手引きとなることも想定している。

3 本書の概要

組織の情報セキュリティ対策は広範囲にわたり、その評価については専門的な知識や多くの手順が必要なことから、難しいというイメージがある。そこで、本書では、「情報セキュリティ対策ベンチマーク」の活用という視点から、情報セキュリティ対策状況の評価について、具体的に、わかりやすい説明をこころがけた。また、実際のビジネスシーンを想定した活用例を示すことにより、現場での応用がしやすいように配慮している。

1章では、情報セキュリティ対策状況を評価する「**情報セキュリティ対策ベンチマーク**」、「**ISMS適合性評価制度**」、「**情報セキュリティ監査**」について、それぞれの評価手法を比較し、その特徴や位置づけを説明する。

2章では、「**情報セキュリティ対策ベンチマーク」の活用例**として、次の3つのケーススタディを示す。

1. 自社の情報セキュリティ対策状況の把握
2. 情報セキュリティ教育への応用
3. 共通の尺度によるグループ内統制

3章では、「情報セキュリティ対策ベンチマーク」では高得点であった企業が、次のステップとして、ISMS認証取得への挑戦を通じて、「**情報セキュリティ対策ベンチマーク」をISMS認証取得に活用するケーススタディ**を示す。

4章では、「**情報セキュリティ対策ベンチマーク」の「情報セキュリティ監査」への活用例**として、次の4つのケーススタディを示す。

1. 地方公共団体における助言型情報セキュリティ監査の利用例
2. 政府機関統一基準に基づく保証型情報セキュリティ監査の利用例（被監査主体合意方式）
3. 一般企業における保証型情報セキュリティ監査の利用例（利用者合意方式）
4. グループ企業における保証型情報セキュリティ監査の利用例（利用者合意方式）

付録には、「情報セキュリティ対策ベンチマーク」、「ISMS適合性評価制度」、「情報セキュリティ監査」**それぞれの評価**について説明を記した。

情報セキュリティ対策
ベンチマーク活用集

1章
情報セキュリティ評価について

1 情報セキュリティ評価について

情報セキュリティ対策ベンチマーク、ISMS適合性評価制度、情報セキュリティ監査は、いずれも、組織が構築した情報セキュリティマネジメントを評価するものである。本項では、これらの情報セキュリティ評価について、その概要や特徴について述べる。

これら評価の準拠する規格は、情報セキュリティマネジメントの国際規格であるJIS Q 27001（ISO/IEC 27001）やJIS Q 27002（ISO/IEC 27002）[*1]である。ただし、評価方法や評価項目の量、評価の詳細さには大きな違いがある。情報セキュリティ対策ベンチマークは、他の評価に比べ、評価項目が少なく、自己診断であることから、作業量や評価に要する時間は比較的少なくてすむ。一方、中立の立場の専門家に評価を依頼する情報セキュリティ監査やISMS適合性評価では、より詳細な評価を行うことから、多くの作業や、時間、費用を必要とする。また、情報セキュリティ対策ベンチマークは、経営者の関与を考慮して評価を行い、ISMS適合性評価制度は、規格への適合性を評価し、保証型情報セキュリティ監査は、利用者が期待する水準を満たすかを評価する。

なお、ISMS適合性評価制度の準拠する規格は、経営者の視点から情報セキュリティマネジメントについて記載したものであり、その意味で、いずれの評価も、経営者の視点からの評価であると言える。

本項では、これらの評価の概要や特徴について、箇条書きや図表により、簡潔に比較した。また、詳細な説明は、付録に掲載した。

1 各評価の特徴

▶ 情報セキュリティ対策ベンチマーク

組織の情報セキュリティ対策実施状況を、自らが評価し、望まれる水準に対する自組織の達成レベルや他組織との相対比較ができる自己診断ツールである。

Webサイト上の質問に答えることで、組織の情報セキュリティ対策状況についてISMS適合性評価制度よりも簡便に自己評価することが可能である。何千件もの現実の診断データに基づき、望ましい水準及び他社の対策状況と自社の対策状況を比較することができる。

▶ ISMS適合性評価制度

組織が構築した情報セキュリティマネジメントシステムが、適切に組織内に整備・運用されていることを、認定された審査登録機関と審査員が、ISMS認証基準（国際規格と同等の規格であるJIS Q 27001）への適合性という観点から評価し、その結果に基づき認証を与える制度である。

▶ 保証型情報セキュリティ監査

組織が構築した情報セキュリティマネジメントの整備・運用状況が、監査結果を利用する者（委託元など）の期待する水準にあるか否かについて、独立かつ専門的な立場の監査人が、一定の基準に照らし、保証意見を表明する監査形態である。

---

*1 本書では、JIS Q 27001:2006、JIS Q 27002:2006を、それぞれJIS Q 27001、JIS Q 27002と、また、ISO/IEC 27001:2005、ISO/IEC 27002:2005をそれぞれISO/IEC 27001、ISO/IEC 27002と表記する。

▶ 助言型情報セキュリティ監査

組織が構築した情報セキュリティマネジメントの整備・運用状況について、独立かつ専門的な立場の監査人が、一定の基準に照らして不十分な点を検出し、必要に応じて検出事項に対応した改善提言を表明する監査形態である。

2 各評価に用いる基準

▶ 情報セキュリティ対策ベンチマーク

評価項目は、情報セキュリティ対策状況に関する25項目（設問）である。これらは、JIS Q 27001附属書Aの情報セキュリティ管理策133項目をもとに作成されている。

▶ ISMS適合性評価制度

適合性評価の基準は、JIS Q 27001である。また、JIS Q 27001の要求に基づき、リスクアセスメントを行った結果として、組織自身が選択するセキュリティ基準を追加することも可能である。組織自身による基準の選択肢として、JIS Q 27001の付属書AやJIS Q 27002の情報セキュリティ管理策、及び公的な基準あるいは業界基準など、さまざまなベストプラクティスを利用することができる。

▶ 情報セキュリティ監査

情報セキュリティ管理基準、及び公的な基準あるいは業界等の基準を取捨選択しあるいは追加することにより策定された個別管理基準が評価に用いる基準である。

2 各評価の比較

情報セキュリティ対策ベンチマーク、ISMS適合性評価制度、情報セキュリティ監査を、目的、対象範囲、評価に用いる基準、評価者、評価のアウトプットなどにより比較した一覧を、**表1.1**（次頁）に示す。

情報セキュリティ対策ベンチマークの評価項目は、JIS Q 27001付属書Aの管理策（133項目）をもとに、組織的対策、物理的対策、技術的対策など、組織に必要な主要な情報セキュリティ対策を網羅し、25項目に整理されている。また、評価結果の利用者や目的に応じて、それぞれの評価項目に付随している対策のポイントとして146項目の利用が可能であり、より詳細な評価や分析をしたい場合などに有効である。

ISMS適合性評価制度は、ISMS認証基準であるJIS Q 27001の要求事項に適合しているかどうかが評価され、認証取得する側の状況に応じてこの基準を作り変えることは出来ない。なお、ISMS認証を取得するための要求事項には、必須のものと除外可能なものがあり、その際にはなぜ必要で、なぜ不要かを、経営陣や責任者が判断に関与し、残留リスクとして受容されたことを示す証拠を文書（適用宣言書）に記載する必要がある。

表1.1　各評価の比較

評価区分	診 断	認 証	監 査	
評価名称	**情報セキュリティ対策ベンチマーク**	**ISMS適合性評価制度**	**助言型情報セキュリティ監査**	**保証型情報セキュリティ監査**
利用の目的	組織の情報セキュティ対策の整備・運用状況の自己評価	情報セキュリティマネジメントシステムの認証	組織が目指す情報セキュリティマネジメントの整備・運用状況の評価	顧客等が期待する情報セキュリティマネジメントの整備・運用状況の保証
目指すべきセキュリティ水準	経営者が目指す水準（望まれる水準や平均値を参照）	経営者が目指す水準	経営者が目指す水準	顧客等が期待する水準
対象範囲	組織体*1	組織体*1・特定業務サービスなど	特定業務・サービス、組織体*1	
評価に用いる基準	JIS Q 27001を参照し作成された25の評価項目（網羅的・簡易的・固定的）	JIS Q 27001（網羅的）	情報セキュリティ管理基準等を参照し作成された個別管理基準（個別的）	
評価者	経営者、管理者（自己評価）	審査員（第三者評価）	監査人（第三者評価）	
評価のアウトプット	散布図 レーダーチャート スコア 助言	ISMS認証　登録証	助言意見	保証意見
費用	無料	有料	有料	

＊1 組織体とは、組織の全部・一部・複合組織を指す。複合組織とは、複数の連携した組織群をグループとして評価するケースである。

一方、保証型情報セキュリティ監査の評価に用いる基準は、顧客など監査報告書利用者の期待する情報セキュリティ水準に応じて被監査組織などが作成した個別管理基準である。監査では、これに対応した個別の監査手続きが作成され、ぜい弱性対策やアクセス制御などに対するより専門的・技術的な監査や、業界特有の個別管理基準に対する監査など、顧客など報告書利用者の目的や期待に応じて、さまざまな利用ケースが想定されている。

評価の対象範囲は、組織全体のことも、一部（特定部門）のことも、また、複合組織のこともある。複合組織とは、複数の連携した組織群をグループとして評価するケースである。さらには、インターネット・

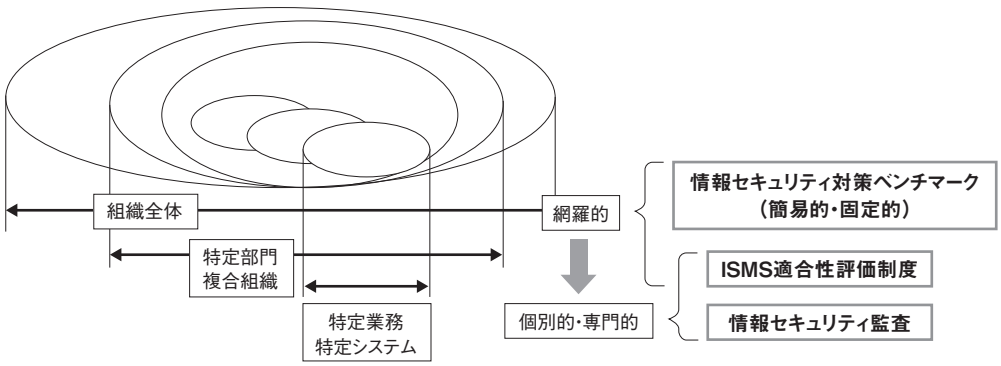


図1.1　評価の対象範囲と評価内容

キャッシングなどの特定業務や情報検索システムなどの特定システムを評価対象とする場合もある。一般に、特定業務や特定システムを評価対象範囲とする場合、その業務の専門性や技術に特化した詳細な評価が求められる。

情報セキュリティ対策ベンチマークは、特定部門または全組織を対象範囲とし、25項目を自己診断するので、簡易な評価であると言える。ISMS適合性評価制度は認証を与えることを目的に、特定業務・特定システムから全組織までを対象範囲としており、JIS Q 27001付属書Aの133項目の管理策のみならず、マネジメントシステムの要求事項を中心に評価している。一方、情報セキュリティ監査、特に保証型情報セキュリティ監査は、保証意見を表明することを目的に、対象範囲を特定業務や特定システム、特定部門などに絞っている。そのため、情報セキュリティ管理基準やそれを参照して作成された個別管理基準を評価尺度とし、対象範囲のすべての項目をより細分化して詳細な評価を実施することに特徴がある。

つまり、情報セキュリティ対策ベンチマークの評価項目は網羅的、簡易的、固定的であることから、より詳細に多くの項目を評価したい場合は、ISMS適合性評価、情報セキュリティ監査を利用することになる。

3 評価結果の利用方法と留意点

1 評価結果の利用に際して

組織の情報セキュリティ対策状況の評価結果の利用目的は、おおむね次の3つが考えられる。

(1) 自社の情報セキュリティ対策の実施状況を確認する
(2) 自社の情報セキュリティ対策状況を外部へ説明する
(3) 外部委託先や子会社の情報セキュリティ対策状況を確認する

「情報セキュリティ対策ベンチマーク」、「ISMS適合性評価制度」、「情報セキュリティ監査」は、いずれも上記 (1)、(2)、(3) の利用が可能であるが、誰がどのような使い方をするか、また、その際にどの程度の情報セキュリティ対策レベルを求めるかに応じて、利用目的に最も適した評価方法を選択することになる。

情報セキュリティ対策ベンチマークは、上記 (1)、(2)、(3) の利用目的以外にも、ISMS適合性評価制度での認証取得や情報セキュリティ監査を受けるための準備段階での利用が可能である。ISMS適合性評価による認証では、国際規格への適合性が保証されるため、外部への説明においては、自社の情報セキュリティ対策状況が国際規格に定められたレベルにあることを示すことができる。また、情報セキュリティ監査においては、「保証」という概念が重要であることから、利用者の期待に応じた保証を可能にするために、保証型情報セキュリティ監査における3方式のフレームワークが策定されている。そこで、利用目的に応じて、これら3方式から自社のニーズに最も適した保証型情報セキュリティ監査方式、もしくは、助言が目的であれば、助言型情報セキュリティ監査を選択することになる。

次に、評価結果の利用という観点から、それぞれの評価方法について整理する。なお、具体的な利用例については、2章、3章、4章のケーススタディを参照されたい。

▶ 情報セキュリティ対策ベンチマーク

(1)評価結果の利用者

① 経営者、管理者、事業部責任者

② 委託元や取引先

(2)評価結果の用途

① 他社と比べた自社の位置の確認

② 全社の情報セキュリティ対策の実施状況の把握

③ 部門ごとの情報セキュリティ対策実施状況の比較

④ 定期的利用で情報セキュリティ対策の改善と向上

⑤ グループ会社、外部委託先、取引先の情報セキュリティ対策状況の把握

⑥ グループ会社、外部委託先、取引先の指導や評価

・診断結果を踏まえて、具体的な対策を促す

・診断結果の提示を取引条件に組み込む

⑦ 委託元や取引先の要求を満たすために診断結果を提示

⑧ 経営者や管理者の情報セキュリティ研修の教材として活用

⑨ ISMS適合性評価制度の準備段階で利用

・情報セキュリティ対策の継続的な改善状況を把握

・リスクアセスメント段階で利用

・マネジメントレビューにおいて利用

・運用段階で利用

⑩ 情報セキュリティ監査の準備段階で利用

・助言型情報セキュリティ監査の準備段階で利用

・保証型情報セキュリティ監査の準備段階で利用

▶ ISMS適合性評価制度

ISMS適合性評価制度の認証を取得することにより、評価の対象範囲における国際規格への適合性が保証されるため、情報セキュリティ対策状況が国際規格に定められたレベルにあることを示すことができる。

(1)評価結果の利用者

① 経営者、事業責任者など

② 委託元、取引先などの利害関係者 *2

(2)評価結果の用途

① 自社の情報セキュリティ対策レベルが国際規格に定められたレベルにあることを確認する

② 自社の情報セキュリティ対策レベルが国際規格に定められたレベルにあることをISMS認証登録証などを提示することにより、関係者、委託元や取引先などに示す

③ 委託先や取引先、グループ会社などの情報セキュリティ対策レベルが国際規格に定められたレベルにあることを確認する

---

*2「利害関係者」とは、委託元、取引先、株主、顧客、市民など、当該企業や団体に対して利害関係を持ち、評価結果や監査報告書を利用する者を指す。

▶ 情報セキュリティ監査

情報セキュリティ監査には、自組織の情報セキュリティ対策に対する助言を求める助言型情報セキュリティ監査と、顧客など監査報告書利用者の期待する水準にあることの保証を求める保証型情報セキュリティ監査がある。また、保証型情報セキュリティ監査では、被監査組織のリスクマネジメントに利害関係者 *2 が当事者としてどの程度関与するかによって監査方式が異なり、以下の3方式がある。

(1)被監査主体合意方式

利害関係者が被監査組織のリスクマネジメントに当事者として直接関与し、具体的に要求した管理策の実装状況を確認することを目的に監査するケース

(2)利用者合意方式

利害関係者が被監査組織のリスクマネジメントに当事者として関与するも、被監査組織の主体的なリスクマネジメントに依存し、管理策の設計並びに実装状況を確認することを目的に監査するケース

(3)社会的合意方式

利害関係者が被監査組織のリスクマネジメントに当事者として関与せず、被監査組織の主体的なセキュリティ管理の出来栄えを確認することを目的に監査するケース

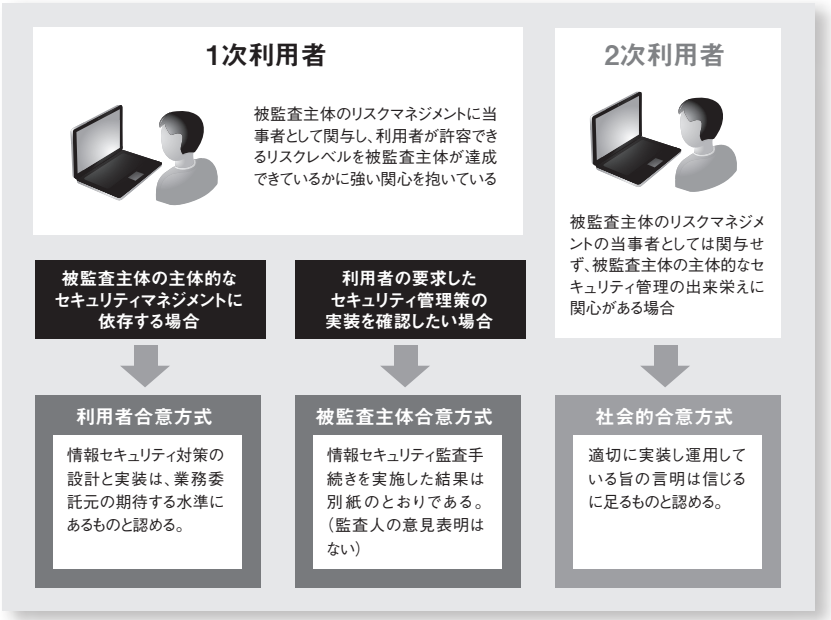


図1.2　利用者にとっての保証型監査3方式の意味と使い分け

以上3方式のどれを選択するかは、利害関係者の監査報告書を利用する目的やその結果がもたらす効果によって異なる。

2 情報セキュリティ対策ベンチマークの利用から他制度への展開

「情報セキュリティ対策ベンチマーク」の評価結果をもとに、さらに情報セキュリティレベルを向上させ、ISMS適合性評価制度の認証や情報セキュリティ監査にステップアップするプロセスとして、**図1.3**の「情報セキュリティ対策ベンチマークから他制度への展開」で示す4つのケースが想定される。

(1)ISMS適合性評価制度の準備段階で利用するケース

(2)ISMS適合性評価制度の認証取得後に、委託元などから個別に情報セキュリティ水準確保の確認要請などがあり、保証型情報セキュリティ監査を利用するケース

(3)助言型情報セキュリティ監査の準備段階で利用し、さらに委託元などから個別に情報セキュリティ水準確保の確認要請などがあり、保証型情報セキュリティ監査を利用するケース

(4)保証型情報セキュリティ監査の準備段階で利用するケース

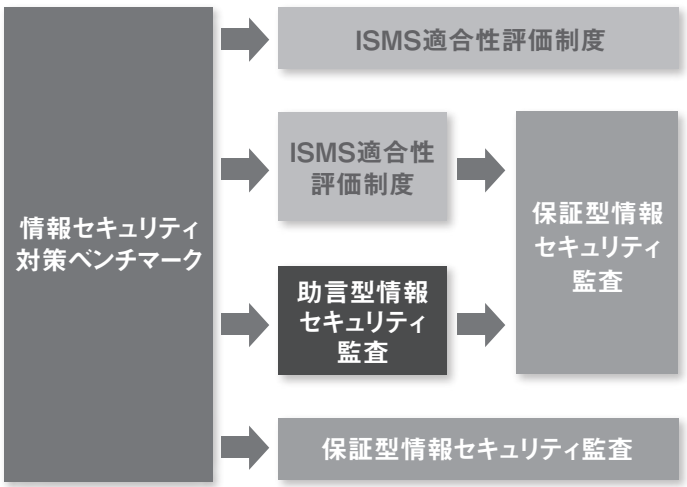


図1.3　情報セキュリティ対策ベンチマークから他制度への展開例

3 外部委託において評価結果を利用する際の留意点

外部委託をする場合に、その企業を選ぶべきか否かの判断材料のひとつとして「情報セキュリティ対策ベンチマーク」、「ISMS適合性評価制度」、「情報セキュリティ監査」の評価結果を使う場合は、委託する業務に関係する部署や業務が評価の対象範囲であるかどうか、また、評価項目や評価手続きが業務遂行にあたって必要なセキュリティを確保するのに十分であるかどうかを確認する必要がある。

内閣官房情報セキュリティセンターが公表している、政府機関統一基準適用個別マニュアル「外部委託における情報セキュリティ対策に関する評価手法の利用の手引」（2007年10月）には、府省庁において情報処理業務を外部委託により行う場合には、外部委託先の情報セキュリティ対策の実施状況を評価する方法として、ISMS適合性評価制度、情報セキュリティ対策ベンチマーク、

情報セキュリティ監査の各評価手法が紹介されている。また、これらの評価の利用に際しての留意点が記載されている。

【参考URL】政府機関統一基準適用個別マニュアル群
http://www.nisc.go.jp/active/general/kijun_man.html

▶ 情報セキュリティ対策ベンチマーク

委託先の選定や、委託先に求める情報セキュリティ対策等を確認する手段として情報セキュリティ対策ベンチマークを利用する場合には、委託業務遂行に際して委託先に実施させる情報セキュリティ対策の内容が、情報セキュリティ対策ベンチマークの25項目の評価項目で十分に評価できると判断される場合であることに留意する必要がある。なお、25項目それぞれに付随する対策のポイントが全部で146項目あることから、これらの項目をチェック項目として活用することも考えられる。

情報セキュリティ対策ベンチマークの評価においては、対策を「実施している」／「実施していない」ではなく、1から5までの成熟度で評価していることから、どのレベルを要求水準として設定するかにも留意する必要がある。委託先に対して一定の情報セキュリティ対策の実施を求めるのであれば、基本的には成熟度3（実施しているが、実施状況の確認はしていない）を求める。しかし、基本的な対策に加えPDCAサイクルが実施されている事を求める場合は成熟度4（実施しており、定期的に確認している）を求める。（成熟度に関しては、p.86、図付1.2参照）

▶ ISMS適合性評価制度

委託先の選定にISMS認証を活用する際に確認する文書は、ISMS認証登録証、適用宣言書、適用範囲定義書である。登録証は、認証を取得したことを証明するもので、適用範囲を示す法人及び部門名、登録範囲内の活動（業務プロセスやサービス）が記述されている。「適用宣言書」は、どのような管理策を実施しているかを宣言している文書であり、そこでは、要求される管理策の採用、不採用及びそれらの理由について説明している。また、適用範囲を定義した「適用範囲定義書」では、認証を取得している業務やサービス内容を記載しているほか、それを運用している組織やシステム等について、組織図やネットワーク構成図を用いて説明している。そのため、適用範囲定義書の取り扱いには注意が必要である。

【参考URL】外部委託におけるISMS適合性評価制度の活用方法
http://www.isms.jipdec.jp/doc/JIP-ISMS117-10.pdf

▶ 情報セキュリティ監査

委託先の選定時には、委託先の情報セキュリティ水準を評価する基準として、ISMS認証の取得結果または情報セキュリティ対策ベンチマークの実施結果を利用することが原則であるが、委託先の情報セキュリティ管理策（及び詳細管理策）が利害関係者の要求事項を満たしていることを確認するには、情報セキュリティ水準の監査を実施することが最も有効な手段である。

情報セキュリティ監査は、監査結果が被監査対象（委託先）の利害関係者（委託元など）に利用されることを想定して実施される監査であるため、監査対象、利用する管理基準などが利害関係者における監査結果の利用目的に合致していることの確認に留意する必要がある。

また、委託先の内部監査や助言型情報セキュリティ監査では、監査結果は被監査対象の改善を目的としているため、利害関係者が確認したい事項が監査結果に記載されない可能性がある。従って、委託先の情報セキュリティ対策の履行状況を確認することを目的に実施する監査では、保証型情報セキュリティ監査が適している。前述の「図1.2 利用者にとっての保証型監査3方式の意味と使い分け」で示した様に、委託先のリスクマネジメントに当事者としてどの程度関与するかによって監査方式が異なるが、利用に際しては以下の点にも留意されたい。

(1)委託元（利害関係者）と委託先（被監査主体）が1対1の関係にある場合
- ・大組織から小組織へ具体策を要求するケース → 被監査主体合意方式
- ・対等な関係で期待する水準などを提示するケース → 利用者合意方式

(2)利害関係者が多数おり多対1の関係の場合 → 社会的合意方式

	被監査主体合意方式	利用者合意方式	社会的合意方式
利害関係者と被監査主体の関係	1対1	1対1（多対1）*	多対1
利害関係者の影響力（関与の度合い）	大	中	小
利害関係者の期待	自組織に合わせて、被監査主体の情報セキュリティマネジメントが実施されること	自組織の情報が期待する情報セキュリティマネジメント水準で管理されること	自分の情報が社会的に容認された情報セキュリティマネジメント水準で管理されること
個別管理基準	要求事項として提示された管理手続	言明書記載の管理手続	言明書の根拠となる社会的に合意された管理手続
監査結果の利用目的	管理手続が的確に実装され、運用されていること		
適用イメージ	重要情報の提供が必要な作業を外部委託する場合（先端技術など）	重要情報を提供してサービスを得たいが、相手の詳細を知ることができない場合（ASP、データセンターなど）	個人情報などを提供して、電子的なサービスなどを得る場合（地方自治体、電子商取引など）

＊ 委託先（被監査主体）が監査報告書を他の利害関係者に積極的に開示するケースなど。

情報セキュリティ対策
ベンチマーク活用集

2章
情報セキュリティ対策ベンチマーク活用例

■ 2章で紹介する3つの活用例

この章では、実際のビジネスシーンを想定した次の3つの活用例を紹介する。

1 自社のセキュリティ対策状況の把握（A社の場合）

情報漏えい事故を起こしてしまった企業が、情報セキュリティ対策の見直しのために、情報セキュリティ対策ベンチマークを利用するケースである。

A社は社員数50名の中小企業。2003年夏に蔓延した、ブラスターウイルスに感染したことから、ウイルス対策は行っているが、その他の対策はまだ進んでいない。

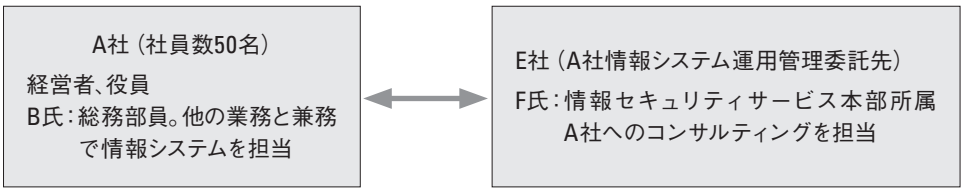
そんな時、顧客情報の漏えい事故を起こしてしまう。この事故をきっかけに全社的に情報セキュリティ対策を見直すことになり、情報システム担当のB氏は、2週間以内に現状の情報セキュリティ対策状況を把握し、改善提案を行うことになった。

B氏は、2週間でこの課題を実行できたのだろうか？

2 情報セキュリティ教育への応用（F氏の場合）

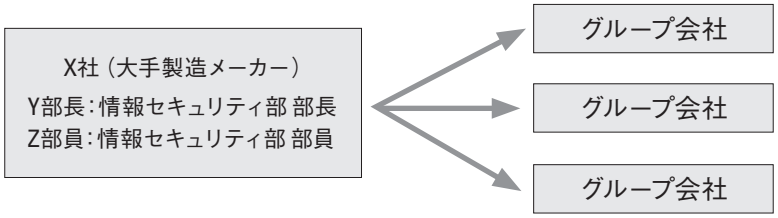
A社では、情報漏えい事故を起こしたことから、情報セキュリティへの関心が高まっている。そこで、役員みずから情報セキュリティ教育を受講することになった。その教育を担当したのがA社に情報セキュリティ対策のコンサルティングを行っているF氏。

F氏は役員に対して、どのような教育を実施したのだろうか？



3 共通の尺度によるグループ内統制（X社の場合）

100社を超えるグループ子会社を傘下にかかえる、大手製造メーカーのX社。これらのグループ会社に業務を委託することも多く、委託に際しては、会社の重要な技術情報を提供することもある。法令順守の観点からも、企業秘密の保全という観点からも、グループ会社の情報セキュリティ対策状況の把握や、その対策状況の改善は、X社にとって、重要な課題である。X社はどのようにして、100社を超えるグループ会社の情報セキュリティ対策状況を把握したのだろうか？



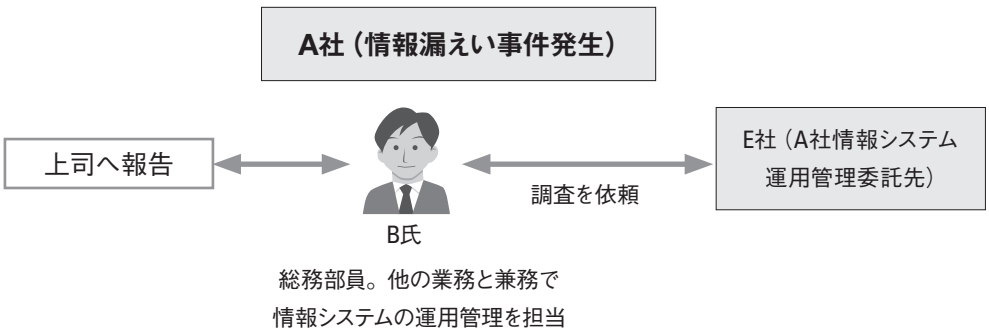
1　A社の場合―自社の情報セキュリティ対策を把握する

1 情報漏えい事件の発生

A社の強みは、海外からあまり知られていない商品を発掘し、販売するという商品探索能力にある。時には、海外の会社と提携して、日本向けの商品開発をすることもある。販路は、商品紹介セミナーなどによるフランチャイズ展開や、お得意様への直販を主としている。最近は、Web販売も開始した。社員数50名ほどの小さい会社だが、業績は好調である。4、5年前に比べると社内のIT化も進み、社員1人に1台のパソコンを設置するなど、IT環境は整っている。業務は情報システムに依存することが多く、商品管理も総務・人事管理も、情報システムなしには動かない。

A社では、ウイルス対策ソフトやファイアウォールは導入しているが、情報セキュリティポリシーの策定や、情報セキュリティ教育などはまだ行っていない。総務部のB氏は他の業務と兼務で情報システム関連の担当をしており、以前、組織として情報セキュリティに取り組む必要性を、社長に進言したことがあった。しかし、売上げに直結するシステム開発と違い、「すぐに効果が確認できるわけではない」との社長判断で、組織運営や人的管理にかかわる情報セキュリティ対策は、優先順位が低いと判断された。

そんなある日、気になるメールが届いた。顧客情報が漏れているようだ、という匿名のメールだった。メールを受けた担当者は、新聞でも連日報道されている「情報漏えい」と聞いてあわてふためいて、すぐに上司に相談した。このメールについては、上司を経由して、社長まで報告が上がった。社長からは「すぐに事実を確認するように」との指示もあったが、メールは匿名であり、クレーム用フォームからの連絡であることから、素性はまったくわからない。困っていたところ、Web販売サイトの利用者から、自分の情報が漏えいしているようなので何とかしてほしい、というメールが届いた。同様のクレームは他にも届いた。利用者からの情報とWebサイトの登録情報を突き合わせると一致したことから、これはWebサイトからの情報漏えいだと特定した。しかし、何が原因で漏れたのか、内部の者による持ち出しなのか、ウイルスによるものなのか、不正アクセスによるものなのか、見当がつかない。B氏は、応急措置をするとともに、情報システムの管理を委託しているE社に調査を依頼した。



調査の結果、Webサイトにぜい弱性があり、そのぜい弱性を利用した不正アクセスにより、顧客情報が漏れていたとわかった。いったんセキュリティ事故が起こると、お客様にも迷惑をかけ、会社の信用にも傷がつき、業務にも影響が出る。収束するまでは大変な労力がかかる。*3

*3 情報漏えい発生時の対応については「情報漏えい発生時の対策ポイント集」（IPA）参照

2 社長の決意と指示

情報漏えい事件も一段落し、A社の社長は、情報セキュリティ対策について、もっとしっかり取り組む必要性を感じていた。今回の事件で、情報セキュリティは、会社の事業にも大きな影響を与えるビジネスリスクであると認識したのである。

B氏は、社長の命を受けて、自社の情報セキュリティ対策の洗い出しをすることになった。何が足りなくて、どこを改善すべきか、2週間後に社長に報告しなければならない。2週間後というのは、厳しい。B氏は、情報システム担当ではあるものの、他業務との兼務で、情報セキュリティの専門家でもない。しかし、組織全体を視野に入れた情報セキュリティ対策というのは、広範囲に及ぶことくらいは知っている。普通に考えても、対策の一覧を作成し、それと自社の対策をマッピングして、提案書らしきものを作成するのは、専門的知識も必要だし、かなりの労作業になる。

困ったB氏は、E社の情報セキュリティコンサルタントのF氏に相談したところ、耳寄りな情報を得ることができた。F氏によれば、自社の情報セキュリティ対策状況を手軽に評価できる良いツールがあるという。それは、IPAがWebサイト上で提供している「情報セキュリティ対策ベンチマーク」というもので、何でも30分ほどで、自社の情報セキュリティ対策状況を自己診断することができるというのである。

3 情報セキュリティ対策ベンチマークへのトライアル

B氏は、早速URLを教えてもらい、「情報セキュリティ対策ベンチマーク」のWebサイトにアクセスした。Webサイトには、「こんなときに！」とある。それは；

「我が社のセキュリティ対策が十分か確認してみたいのだが…。」

「セキュリティ対策をしたいが、何から手をつければいいのだろう…。」

「自社でまだ取り組んでいない対策には何があるのだろうか…。」

といったものだった。これは、まさに、B氏が今困っていることである。

こんなときに！

情報セキュリティ対策ベンチマークでは、アカウントを発行すると、次回の診断の入力作業を低減するなどの便利な機能があるらしいが、まずは、アカウントを発行せず、トライアルで診断をすることにした。

質問は、情報セキュリティ対策についての25項目のほかに、企業プロフィールについての質問がある。実際に質問に答えようとすると、組織的対策、物理的対策、技術的対策を網羅しているため、事前の準備が必要なことがわかる。しかも、単にYes、Noを問うものではない。「1. 実施していない」、「2. 一部しか実現できていない」、「3.実施しているが、実施状況の確認はしていない」、「4. 実施しており、定期的に確認している」、「5. 他社の模範となるレベル」の5段階での回答である。

「これは、もしかしたら、PDCAサイクルを念頭に置いた質問ではないか？」とB氏は思った。「4のレベルなら、PDCAが回っていると言えるのではないか？」、これはなかなか奥が深い。社長の指示は、自社の情報セキュリティ対策の洗い出しをして、何が足りなくて、どこを改善すべきか、ということだったから、これらの質問には、自社の実施状況をきちんと調べてから答えるべきであろう。ざっと見ただけだが、このツールは、まさに、B氏のニーズにあっていると言える。

表2.1　情報セキュリティ対策ベンチマーク（ver.3.0）における評価項目一覧

連番	（大項目1）情報セキュリティに対する組織的な取組状況	
1	①	情報セキュリティ管理規程
2	②	情報セキュリティ推進体制
3	③	情報資産の重要度分類
4	④	重要情報の業務工程ごとの安全対策
5	⑤	業務委託契約
6	⑥	従業者との契約
7	⑦	従業者への教育
	（大項目2）物理的（環境的）セキュリティ上の施策	
8	①	建物や安全区画の物理的セキュリティ
9	②	第三者アクセス
10	③	情報機器の安全な設置
11	④	書類、記憶媒体の適切な管理
	（大項目3）情報システム及び通信ネットワークの運用管理	
12	①	実稼働環境の情報セキュリティ対策
13	②	システム運用におけるセキュリティ対策
14	③	不正プログラム対策
15	④	情報システムのぜい弱性対策
16	⑤	通信ネットワークの保護策
17	⑥	記憶媒体の紛失・盗難対策
	（大項目4）情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況	
18	①	情報（データ）へのアクセス制御
19	②	業務アプリケーションに対するアクセス制御
20	③	ネットワークのアクセス制御
21	④	業務システム開発時のセキュリティの考慮
22	⑤	ソフトウェアの導入・開発時のセキュリティ管理
	（大項目5）情報セキュリティ上の事故対応状況	
23	①	情報システムの障害対策
24	②	情報セキュリティ事故対応手続き
25	③	事業継続への取組みの実施

4 B氏のアイディア

B氏は、情報セキュリティ対策ベンチマークの質問を一覧表にして、自社がどこまで行っているかを書き込むことで、社長報告用の資料ができると考えた。B氏は、診断はせずに、質問をざっと眺めてからログアウトした。幸いなことに、情報セキュリティ対策ベンチマークのサイトには、診断の準備をするための資料が掲載されている。B氏は、まず、「情報セキュリティ対策ベンチマークの質問一覧」と、「情報セキュリティ対策ベンチマーク質問と対策のポイント」をダウンロードした。これらの資料をベースに、B氏は、エクセルで次のような一覧表を作成した。

表2.2　B氏作成のA社対策一覧表

質問（評価項目）	回答（日付）	回答（日付）	現状	行うべき対策	行動計画	実行記録
大項目1　組織的						
①情報セキュリティ.....						
（対策のポイント）.....						
:	:	:	:	:	:	:

B氏は、25項目の質問を大項目ごとに記載した。こうすることで、対策を考える時に、各項目を、組織的、物理的、技術的というようなまとまりで整理することができる。また、自社にあった対策を網羅しようと考え、自社に必要な対策のポイントを付け加えた。さらには、時系列的な管理ができるようにと、回答欄を複数設けた。半年とか1年の間をおいて、繰り返し診断を行うと、段階的に自社の情報セキュリティ対策状況を改善できるし、対策の進捗状況も管理できる。B氏は、診断の度に、その時々の回答や状況を書き込んでおこうと考えた。

しかし、この表に書き込むのは、診断を行った後でよいと考え、まずは、ダウンロードした「情報セキュリティ対策ベンチマーク質問一覧」の回答欄に社内の状況を調査しながら、自分の答えを書き込んだ。その際、情報セキュリティポリシーのコピーや、情報システムの台帳など、回答の根拠となるものも、自分なりに集めておいた。これらの資料は、2週間後に、この表をもとに社長に報告する時に、詳細を聞かれたら、対策の現状を示す根拠として見せることができる。

5 情報セキュリティ対策ベンチマークで自己診断

いよいよ自己診断である。今度は、トライアルではないので、アカウントの発行をすることとした。回答は事前に調査して記録しているものを入力するだけなので、診断結果を表示するまで5分もかからなかった。診断結果では、散布図やレーダーチャートが示され、グラフィカルで直感的に自社の対策状況が把握できる。

診断企業は、情報セキュリティリスク指標に応じて、3つのグループのいずれかに分類される（**表2.3**）。情報セキュリティリスク指標は、従業員数、売上高、重要情報の保有数、IT依存度などから計算される企業のかかえるリスクを表す指標である。

表2.3　リスク指標による企業分類

分類	特徴
I	高水準のセキュリティレベルが要求される層
II	相応の水準のセキュリティレベルが望まれる層
III	情報セキュリティ対策が喫緊の課題でない層

散布図は、全体と、従業員数300名で分けた企業規模別の2種類がある。いずれも、情報セキュリティリスク指標によって分類されたグループを色別に表示し、診断企業は自分が分類されたグループと、全体の中での自社の位置とを把握することができる。レーダーチャートは、リスク指標によるグループ別、企業規模別、業種別の3種類が示される。同業他社との対策状況の比較は、社長にとってもインパクトがあるのではないかとB氏は考えた。

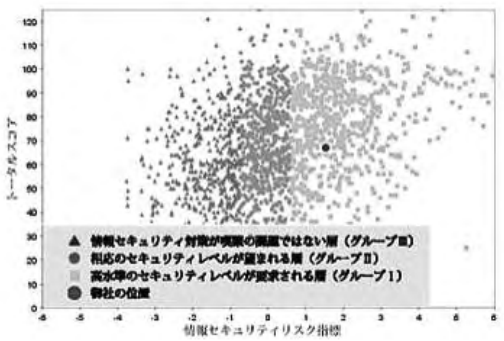


図2.1　診断結果の例（散布図）

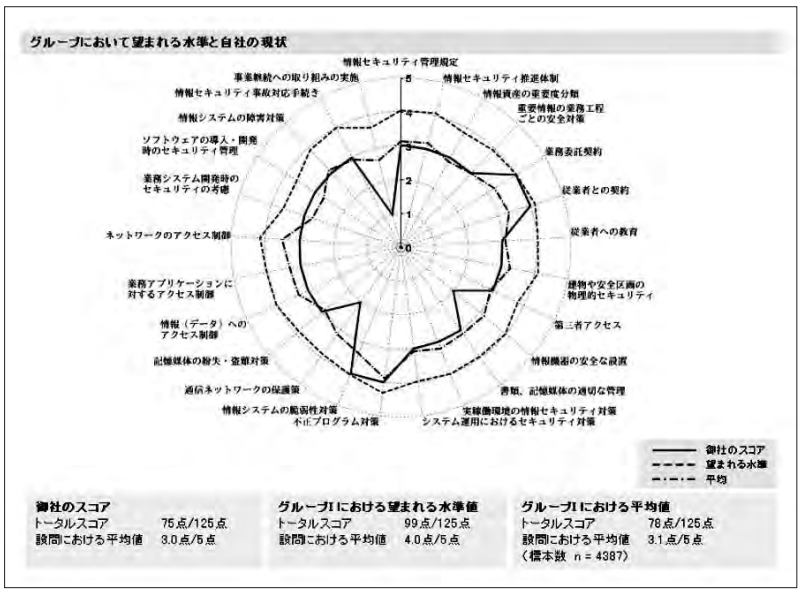
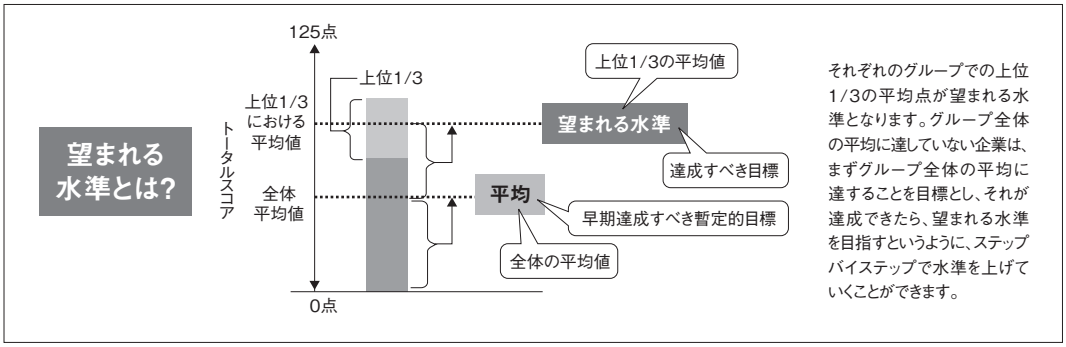


図2.2　診断結果の例（レーダーチャート）

A社はIIIグループに分類された。実施していない対策があるため、トータルスコアは50点とかなり低い。初めてのトライアルなので、これもいたしかたない。診断結果には、**望まれる水準**というものも示される。さらには、一定の水準に達していない場合は、**推奨される取組**が表示される。推奨される取組には解説もあるが、これはあとで読むことにした。



6 総務部長への報告と診断の訂正

B氏が、診断結果を上司の総務部長に報告したところ、総務部長より、不正プログラム対策は、B氏の回答した3ではなくて、4ではないかとの意見があった。A社では、ウイルス対策ソフトはすべてのパソコンに導入し、パターンファイルの更新、定期的なウイルス検査、ぜい弱性対策を行っている。また、全員がウイルス対策を実施しているかを確認し、必要に応じた見直しも行っている。

2003年の夏に、W32/Blasterというネットワーク経由で蔓延するウイルスが流行した時に、A社はこのウイルスに感染してしまい、大騒ぎになったことがあった。そのため、ウイルス対策は進んでいる。

B氏は、ウイルスだけではなく、スパイウェアやボットなどの新しい脅威やそれらによって引き起こされるフィッシング詐欺や、情報漏えい、踏み台の脅威などについては、対策が十分とはいえず、まだ4には達していない、という気持ちはあったが、ここは、総務部長の意見に従うこととした。

情報セキュリティ対策ベンチマークには、回答の修正を行える機能がある。ログインIDとパスワードを入力すると「Myページ」が表示される。

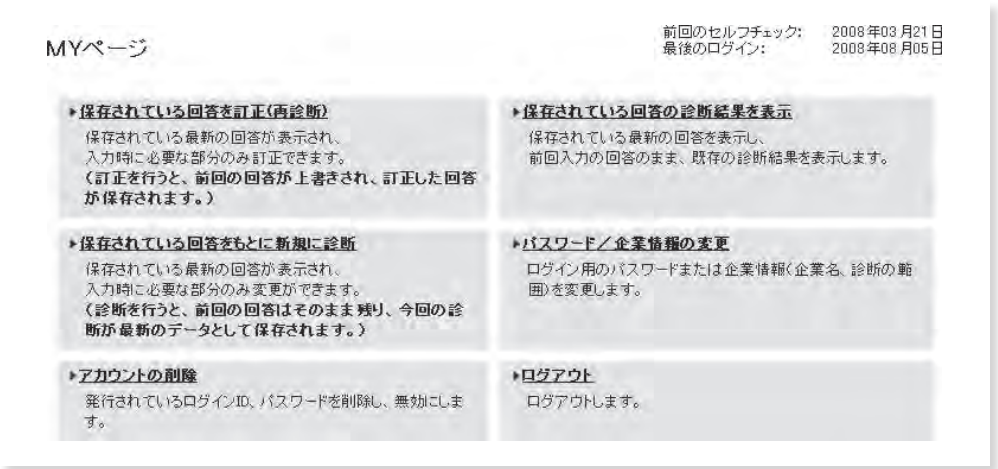


図2.3　情報セキュリティ対策ベンチマークのMyページの画面

このページには、「保存されている回答を訂正」という機能があり、この項目をクリックすると、保存されている回答が表示され、必要な部分の訂正だけで診断ができるという手軽さである。

診断の訂正も終了し、いよいよ社長への報告の準備である。B氏は、対策の一覧表に、今回の診断の結果、自社の対策状況、行うべき対策、行動計画を記し、報告用の一覧表を完成させた。

しかし、もうひとつ大事なことが足りない。それは、対策を行う時にかかるコストの検討である。どの程度の労力と費用がかかるか、概算でも準備しておかないと、次に進めない。B氏が、F氏の助力も得ながら、やっとこれらの作業を終えたのは、社長への報告の前日であった。

7 社長への報告

いよいよ、社長への報告である。例の一覧表と情報セキュリティ対策ベンチマークの診断結果を中心に説明を進めることにした。社長への報告会には、役員や部長も出席した。

最初に診断結果の説明をした。社長も役員も、見やすい散布図やレーダーチャートにより自社のセキュリティレベルを認識できることに驚いていた。また、スコアが表示されるのもわかりやすいと好評だった。しかし、自社のセキュリティレベルが他社と比べて思ったよりも低かったことにショックを受けていたようだった。

次に、対策一覧表について説明したところ、短時間によく整理したと感心する役員もいた。診断結果では、どこがどの程度不足なのか提示されていたため、対策の必要性については、社長も役員も納得したようであった。今後の対策について議論したのち、一度にすべての対策を行うことはできないので、段階的に対策を向上させていこうということに落ち着いた。

情報漏えい事件の影響もあり、情報セキュリティへの関心は高い。そこで、後日、もう少しまとまった時間を取って、社長、役員、部長などの幹部クラスを対象とした、情報セキュリティ教育を実施してはどうか、ということになった。役員クラスへの情報セキュリティ教育となると、B氏には荷が重い。結局は、E社のF氏に教育をお願いすることとなった。

2 F氏の場合 ― 情報セキュリティのコンサルティング

1 F氏とA社と情報セキュリティ対策ベンチマーク

E社では、情報システムの構築運用サービスとともに、情報セキュリティマネジメント構築のコンサルティングや情報セキュリティ教育も手がけている。E社の情報セキュリティサービス本部に所属するF氏は、情報セキュリティコンサルティングや情報セキュリティ教育を担当している。F氏は、ITコーディネータでもある。仕事柄、中小企業とのおつきあいも多い。最近、F氏の担当するA社では、情報漏えい事件を引き起こしてしまい、それを機に、情報セキュリティ対策への関心が高まっているようである。

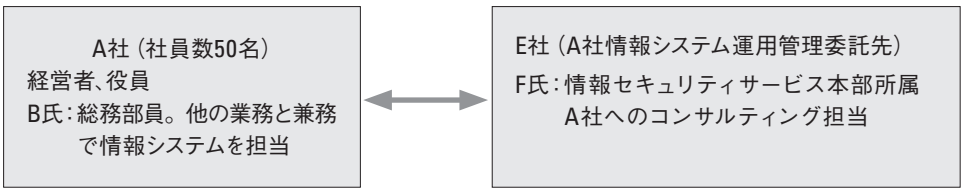
情報システムを利用している企業であれば、情報セキュリティ対策は必須である。しかしながら、中小企業には、情報セキュリティ対策に人やお金を十分に割けないという事情もある。売上げに直接結びつかない情報セキュリティ対策にお金をかけることは、かなり厳しい。もちろん、昨今は、情報セキュリティ対策を行っていることをセールスポイントにする会社も増えているようだが、A社の場合は、そこまで行っていない。

そんなA社の事情を知っていたため、この前の情報漏えい事件で、情報セキュリティ対策の見直しをA社が行った際には、F氏は、IPAの情報セキュリティ対策ベンチマークを紹介した。情報セキュリティ対策ベンチマークはこんな点が良いとF氏は考えている。

(1)時間や費用がかからず、専門的な知識がなくても自己診断ができる。
(2)情報セキュリティ対策として網羅的に何をすべきか理解しやすい。
(3)解説書を読むより、自己診断をすることで理解が深まる。
(4)対策を実施していない会社にとっては、良いきっかけになる。
(5)散布図やレーダーチャートなどで自社の位置を知ることができる。
(6) 他社と比較できるので、他社より遅れている場合は、経営層の危機意識が高まり、結果として情報セキュリティ対策が加速する。

2 情報セキュリティ教育の準備

A社では、情報セキュリティ対策ベンチマークの診断結果の報告を契機として、幹部クラスへの情報セキュリティ教育が行われることになり、その教育をF氏は依頼された。



情報セキュリティ対策は、経営者の関与が必須である。それは、ひとつには、人や費用などを投入するための経営的判断が求められるためでもある。しかし、それにとどまらず、経営者のコミットメントとリーダシップが無ければ、組織的な対策を展開することが難しいためでもある。経営者自らが、情報セキュリティ対策の意義やその実施方法の概略を知ることにより、組織的取組みを推進しやすい環境が整うことになる。

B氏との打合せで、F氏は、教育資料は情報セキュリティ対策ベンチマークの質問や対策のポイントをベースに作成しようと考えた。情報セキュリティ対策ベンチマークの質問は、25項目ながら網羅性があり、またPDCAサイクルの考え方を取り入れている。そのため、情報セキュリティ対策ベンチマークの質問の内容を理解すれば、基礎知識の習得には十分であると考えたのであった。

情報セキュリティ対策ベンチマークの情報セキュリティ対策に関する25項目の質問は、ISMS適合性評価制度の認証基準であるJIS Q 27001の附属書Aの管理策133項目をベースに作成されている。この133項目は、情報セキュリティ対策として行うべきことを網羅的かつ具体的に纏めたものである。それを、情報セキュリティの専門家が集まり、平易な言葉を使用して、25項目に整理している。また、質問に付随する対策のポイントを見ることで、具体的に何をどのように行えばよいかが理解できる。対策のポイントは全部で146項目あり、やはり133項目の管理策を参照して作成している。対策のポイントについては、全て考慮するというのではなく、自社の状況に応じて取捨選択をすればよい。

表2.4　JIS Q 27001の管理領域と情報セキュリティ対策ベンチマークの評価項目

JIS Q 27001		情報セキュリティ対策ベンチマーク（大項目と質問・対策のポイント）		
情報セキュリティ管理領域	管理策数	大項目名称		
1. 情報セキュリティ基本方針	2	1. 情報セキュリティに対する組織的な取組状況		7
2. 情報セキュリティのための組織	11			
3. 資産の管理	5			50
4. 人的資源のセキュリティ	9			
11. 順守	10			
5. 物理的及び環境的セキュリティ	13	2. 物理的（環境的）セキュリティ上の施策		4 / 22
6. 通信及び運用管理	32	3. 情報システム及び通信ネットワークの運用管理		6 / 33
7. アクセス制御	25	4. 情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況		5
8. 情報システムの取得開発及び保守	16			25
9. 情報セキュリティインシデントの管理	5	5. 情報セキュリティ上の事故対応状況		3
10. 事業継続管理	5			16
11領域	133	大項目5	質問数	25
			対策のポイント数	146

F氏は、JIS Q 27001の11の管理領域と、情報セキュリティ対策ベンチマークの評価項目との関連を示す表を作成した（**表2.4**）。こうすることで、情報セキュリティ対策の全体像を知るとともに、対策をカテゴリごとに整理できる。さらには、国際規格との関連について理解してもらうことができる。

情報セキュリティ対策ベンチマークの質問には、役員クラスが把握すべき項目もあれば、詳細は担当者に任せて、概要のみ理解すればよいものもある。そこで、情報セキュリティ対策ベンチマークの構成にあわせて、教育項目、達成目標、教育内容を整理し、教育に必要な時間を整理した（次頁 **表2.6**）。

役員クラスは受講にあまり時間が割けないことを考慮し、教育の所要時間は2時間として、それぞれの項目の教育に必要な時間を考えた。

表2.5　教育項目、達成目標、教育内容

分類	到達レベルと教育内容
重点教育項目	十分な理解が必要な項目（質問・説明・対策のポイント、解説を理解する）
標準教育項目	相応の理解が必要な項目（質問・説明・一部の対策のポイントを理解する）
概要教育項目	概要のみ理解すればよい項目（質問、説明を理解する）

対策を行う上では、単に実施している実施していないではなく、PDCAサイクルを考慮する必要がある。そこで、情報セキュリティ対策ベンチマークの5段階の回答の選択肢とPDCAサイクルを対応させて教育することとした。

表2.6　教育項目、達成目標、教育内容

情報セキュリティ対策ベンチマークの25項目		役員への教育	教育時間
1	1．情報セキュリティ管理規程	重点教育項目	40分
	2．情報セキュリティ推進体制、コンプライアンス		
	3．情報資産の重要度分類	標準教育項目	30分
	4．重要情報の業務工程ごとの安全対策		
	5．業務委託契約		
	6．従業者との契約		
	7．従業者への教育		
2	8．建物や安全区画の物理的セキュリティ		
	9．第三者アクセス		
	10．情報機器の安全な設置		
	11．書類、記憶媒体の適切な管理		
3	12．実稼働環境の情報セキュリティ対策	概要教育項目	30分
	13．システム運用におけるセキュリティ対策		
	14．不正プログラム対策		
	15．情報システムのぜい弱性対策		
	16．通信ネットワークの保護策		
	17．記憶媒体の紛失／盗難対策		
4	18．情報（データ）へのアクセス制御		
	19．業務アプリケーションに対するアクセス制御		
	20．ネットワークのアクセス制御		
	21．業務システム開発時のセキュリティの考慮		
	22．ソフトウェアの導入・開発時のセキュリティ管理		
5	23．情報システムの障害対策	標準教育項目	20分
	24．情報セキュリティ事故対応手続き		
	25．事業継続への取り組みの実施		

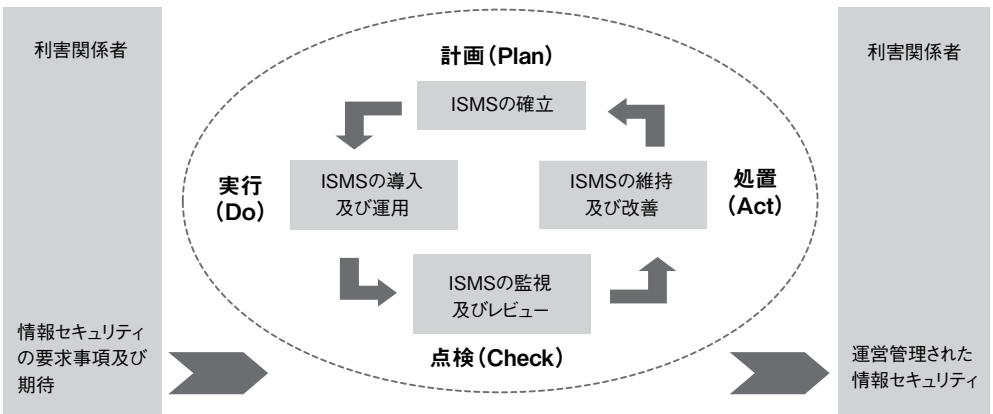


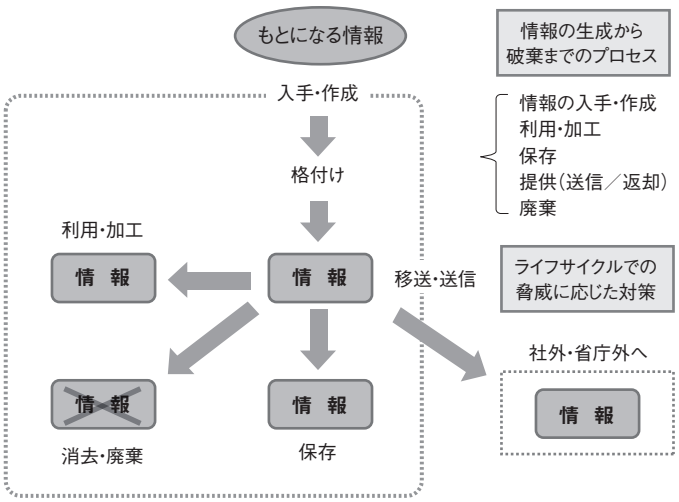
図2.4　ISMSプロセスに適用されるPDCA（出典：JIS Q 27001:2006）

表2.7　5段階の回答基準とPDCAサイクル

1	経営層にそのような意識がないか、意識はあっても方針やルールを定めていない	計画（Plan）以前
2	経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない	計画し、一部のみ実施（Plan及び一部Do）
3	経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない	実施している（Doの段階）
4	経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている	確認を行っている（Checkの段階）
5	4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している	他社の模範レベル

経済産業省やIPAのWebサイトから情報セキュリティ対策ベンチマークの25項目の質問、説明、対策のポイント、解説が記載された資料がダウンロードできる。そこで、配布する教材は、これらの資料を使うこととした。まず、事前に幹部全員にアンケートを取り、自身の所管する部門の情報セキュリティ上の問題点や課題を提出してもらい、さらには、情報セキュリティ対策ベンチマークの質問の中の不明な用語や内容を把握した。不明な用語として回答のあったものは、簡単な用語解説の資料を作成した。図や絵で内容を説明すると、直感的に理解できることから、IPAの情報セキュリティセミナーの資料を参考にしながら、プレゼン資料を作成した。たとえば、「4.情報の業務工程ごとの安全対策」の評価項目のところでは、図のような情報のライフサイクルの図を使って説明することとした。

教育資料は、情報セキュリティ対策ベンチマークやIPAの資料を参照して作成したため、出典を明記した。



出典：（独）情報処理推進機構　情報セキュリティセミナー（2007年度）資料

図2.5　情報のライフサイクルと取扱い

3 情報セキュリティ教育の実施

A社で、情報セキュリティ教育に参加したのは、社長以下4名の役員・部長とB氏の計6名だった。F氏は、淡々と教材をこなす教育ではなく、質疑応答の時間も取り、雑談の中でセキュリティのポイントが理解できるようにと考えた。25の評価項目だけでは、個々の対策に焦点があたりがちなので、基本的な考え方として、次の点を追加した。

(1)情報セキュリティ対策はトップダウンで行うため、経営層のリーダシップが必要である。
(2)情報セキュリティリスクだけではなく、全体のビジネスリスクを考えて、必要な情報セキュリティ対策を行うべきである。
(3)そのためには、部分的ではなく、全体を見据えたバランスの良い対策が必要である。
(4)対策にかけられる人も費用も限られている中では、対策の優先順位付けが必要である。
(5)情報セキュリティ対策を事業にどう結びつけるかの視点も必要である。

情報セキュリティ管理規程の項目では、次の点を強調した。

(1)情報セキュリティポリシーの策定だけして、実施されていない場合がある。いわば、絵に描いた餅の状態では、策定した意味がない。
(2)情報セキュリティに関連する規程には、情報セキュリティポリシー以外にも、業務規程、組織規定、文書規程、個人情報保護規定などがある。関連する規程と整合性が取れていること、上位文書は何であるかなどが明確であることが必要。
(3)情報セキュリティポリシーは、策定にも負荷がかかるが、本当に大変なのは、それをどう現場に浸透させ、定着させるかということ。
(4)情報セキュリティポリシーに定められたルールを現場へ浸透、定着させるには、情報セキュリティ教育や対策の実施状況の点検が有効である。

事故対応状況の項目では、情報漏えい事件があったこともあり、活発な質疑が行われた。この項目では、特に事前の準備が事故対応の成否を分けることを強調した。また、全般的なポイントとして、次の点を強調した。

(1)組織の情報セキュリティ対策の定期的な点検には、情報セキュリティ対策ベンチマークが使える。
(2)診断結果を整理して、対策の改善を行う際に、できることと無理なことを整理して、アクションプランを作成する。
(3)アクションプランを作成した後は、計画が実施されているか確認する。
(4)経営層が改善の音頭を取ることで、改善が進む。

A社の役員にとって、このような情報セキュリティ教育は初めてのことであり、日頃の疑問への答えも得ることができ、満足しているようであった。

情報セキュリティ教育は、本来は全社員に対して行うべきである。そうしないと、ルールはあっても、そのルールが守られず、結果としてセキュリティ事故につながってしまう。F氏は、今後早い時期に社員対象のセキュリティ教育を行うことを勧めて、役員向けの教育を締めくくった。

4 情報セキュリティ対策ベンチマークの活用方法

F氏は、常々、情報セキュリティ対策ベンチマークはさまざまな使い方ができると考えている。たとえば、今回は教育に使ったが、情報セキュリティポリシーの策定や見直しにも利用できる。

表2.4のJIS Q 27001の管理策は、情報セキュリティポリシー策定の際によく参照されてきた管理策である。133項目もの詳細なポリシーを作成する必要のない中小企業にとっては、まずは情報セキュリティ対策ベンチマークの25項目と、自社にあった対策のポイントをピックアップすることによって、情報セキュリティポリシーを作成することも可能であろう。すでに情報セキュリティポリシーを作成している会社であれば、25項目の質問や自社の情報セキュリティポリシーを比較して、不足な部分をチェックすることもできる。

情報セキュリティ対策ベンチマークはPDCAの各段階で、次のように活用することができる。

▶ Planの段階での活用

(1) そのグループでの自社の位置を散布図やレーダーチャートで確認する。
(2) 望ましい水準からどの程度不足かチェックする。
(3) 他社と比べてどの程度の差があるかチェックする。
(4) 「推奨される取組」を参照し、どこから対策を始めるかチェックする。
(5) 情報セキュリティポリシー策定の参考にする。

▶ Do & Check & Actの段階での活用

(1) 日ごろの対策状況をチェックし、日々の改善に役立てる。
(2) 情報セキュリティ対策の取り組み状況を外部へ説明する際に活用する。
(3) 外部委託先の情報セキュリティ対策状況を評価するために活用する。
(4) 情報セキュリティ教育に活用する。

▶ ISMS認証取得や情報セキュリティ監査などの準備段階で活用

F氏は、情報セキュリティ対策ベンチマークは、職場診断にも使えると考えている。たとえば、複数の部門の管理職に、それぞれ情報セキュリティ対策ベンチマークによる自己診断を実施してもらい、その結果を比較することにより、意識の違いを横並びで比較することができる。またグループ会社での、セキュリティレベルを揃えるために情報セキュリティ対策ベンチマークの診断を使うことも可能である。

情報セキュリティは、情報セキュリティリスクを事業経営上どのように位置づけ、そのリスクに経営者としてどのように対応するかという経営上の問題でもある。経営層が情報セキュリティ対策の必要性を実感した場合に、情報セキュリティ対策ベンチマークは、自社の情報セキュリティ対策状況を把握するのには良いツールである。その際、コンサルタントのアドバイスが必要な場面もあるだろう。F氏は、これからも、情報セキュリティ対策ベンチマークをコンサルティングに取り入れていきたいと考えている。

3 X社の場合―グループ会社の情報セキュリティ対策状況の把握

1 X社の情報セキュリティ対策上の課題

大手製造メーカーのX社では、資本関係のあるグループ子会社は100社を超え、グループ企業内の業種は、製造を専業とするもの、販売を専業とするもの、金融や出版を行うものなど、その業種もさまざまである。これらのグループ会社にX社より直接業務を委託することも多いが、外部委託先の情報セキュリティ対策状況の把握は、法令順守の観点から必須である。また、内部統制の観点から、本社、子会社を問わず、グループ企業総体として足並みを揃えて情報セキュリティ対策を行う必要性を感じている。さらには、X社の技術情報を託す子会社もあり、企業秘密の保全という観点からも、グループ会社の情報セキュリティ対策状況の把握及びその改善は重要な課題である。

X社としては、情報セキュリティ対策の必要性は十分認識しており、全社対応の情報セキュリティを担当する部署を設け、情報セキュリティ対策を進めている。X社では、3～4年前は、個人情報保護法対策について作業を進めた。その際、経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」を参照して対策を行った。また、企業秘密を守るという意味で、不正競争防止法の要求事項や顧客からの要求に基づき、情報漏えい防止対策も行ってきた。情報漏えい防止については、社員ひとりひとりの意識も重要であると考え、「情報を許可無く持ち出すべからず」とか「私物のパソコンを許可無く持ち込み、社内のネットワークに繋ぐべからず」とか、これをすると事故につながりやすいことをまとめ、「べからず集」のようなものを作成して社員に配布をするとともに、情報セキュリティ教育にも注力している。

このような個別の対策を積み重ねてきた結果、X社社内での情報セキュリティ意識の向上はみられたが、グループ会社全体の情報セキュリティ対策状況の把握は、まだできていなかった。本社の情報セキュリティ対策は進んでいるものの、グループ子会社の情報セキュリティ対策状況となると、まだ心もとないところもある。まずは、これらグループ会社の情報セキュリティ対策状況を把握し、何ができて、何ができていないのか、情報セキュリティ対策の浸透度を含めて実態を把握し、不足なところがあれば改善を促す作業が必要だ。しかし、100社以上のグループ会社を抱えるとなると、情報セキュリティ対策状況の把握だけでも作業負荷もコストもかかる。また、どのような基準に基づき、どのような方法で状況を把握するかも問題である。情報セキュリティ監査の実施やISMS認証取得をすべての子会社に要求するわけにもいかない。

そんな中、X社情報セキュリティ部の部長Y氏はIPAの情報セキュリティ対策ベンチマークのサイトを発見し、これが、グループ会社の情報セキュリティ対策状況の把握に使えるのではないかと考えた。

2 提案と協議

Y部長は、全体を視野に入れた場合、共通の基準に則った対策が必要であると考えていた。情報セキュリティ対策ベンチマークの情報セキュリティ対策に関する質問のもととなったのは、情報セキュリティマネジメントの規格であるJIS Q 27001であり、この規格を整理軸として対策状況を評価するのは妥当と考えた。Y部長は、早速部内のスタッフを集め、情報セキュリティ対策ベンチマークが使えるかどうかについて協議を行った。

情報セキュリティ対策ベンチマークの概要を説明したところ、部内のスタッフの反応は、情報セキュリティ対策ベンチマークをグループ会社の情報セキュリティ対策状況を把握するためのツールとして使うことについては、おおむね好意的であった。情報セキュリティ対策ベンチマークを採用しても良いという理由をまとめると次のような意見に集約された。

▶情報セキュリティ対策ベンチマークを採用しても良いと考えた理由

(1)経済産業省より公表された施策ツールを、IPAがWebサイト上で使える自動化ツールとして開発し、提供しているため、Webサイト上の質問に答えることで、組織の情報セキュリティへの取組状況についてISMS適合性評価制度よりも簡便に自己評価することが可能である。

(2)情報セキュリティ対策に関する25項目の質問は、JIS Q 27001付属書Aの管理策をもとに作成されており、国際標準に基づいた網羅性のあるものである。

(3)JIS Q 27001付属書Aの管理策133項目を、専門家により25の質問項目に整理しているので、回答するための時間と手間はそれほど多くない。

(4)25項目の質問に対応している対策のポイントは146項目あり、対策のポイントに見合った対策を順次講じることで、段階的な情報セキュリティ対策の向上が見込まれる。

(5)企業プロフィールからセキュリティ水準の要求レベルに応じて3つのグループに分けられ、そのグループごとに求められるセキュリティ水準があるため、会社の状況にあわせたセキュリティ投資を考えることができる。

(6)何千件もの現実の診断データに基づき、望ましい水準や同業他社の対策状況と自社の対策状況を比較することができる。

(7)診断結果の表示は、散布図やレーダーチャートを使って可視化された、直感的にわかりやすいものである。

(8)政府機関統一基準においても、外部委託先の情報セキュリティ対策の実施状況を評価する方法として、「ISMS適合性評価制度」、「情報セキュリティ監査」と並んで、「情報セキュリティ対策ベンチマーク」が紹介されている。

(9)100社の診断データが集まれば、各子会社を資本の大きさや業種に応じてグループ分けし、資本の額ごと、業種ごとに対策状況の違いを比較できる。

(10)情報セキュリティ対策ベンチマークの使用は無料であり、労力と費用の両方を省力化できる。

情報セキュリティ対策ベンチマークの採用については、部員の意見はおおむね好意的ではあったが、情報セキュリティ対策状況の評価については次のような、さらに踏み込んだ議論もなされた。

▶自己評価についての質疑

Q: 情報セキュリティ対策ベンチマークは自己評価であり、評価者によるばらつきがあるのではないか?

A: 自己評価なので、評価のばらつきが大きいとか、精度が低いとは一概に言えない。わが社で情報セキュリティ対策ベンチマークの診断をする時には、ヒアリングをする、文書を見るなど裏づけを取ってから質問に答えるべきと考える。情報セキュリティ対策ベンチマークの質問には、実態を調査しないと答えられない。情報セキュリティ監査でもヒアリングや文書調査、現場の調査をするのであり、調査項目が簡易か詳細かの差こそあれ、同様の作業が必要と考えている。また、他社で情報セキュリティ対策ベンチマーク診断を行っているところに聞いてみると、診断をいったん行った後でも、自分の答えが正しかったかどうかを各部署にヒアリングし、修正をしていると聞く。評価の精度を上げるのは、取り組み方によるのではないか。

Q: グループ会社によっては、自分の組織の評価を上げたいので、実際より良い点数をつけることもあるのではないか?

A: 見ず知らずの人に自己診断してもらうわけではなく、誰がどこで何をしているかがわかっているので、実態とかけ離れた診断をすれば、それを把握することはできる。記録やログによる検証もできるので、現実とかけ離れた診断かどうかの判断はできると思う。

Q: 他者による評価に比べ、自己評価の利点はどこにあると考えるか？

A: 自己評価の良さは、質問に答えることで、自分に何が求められているのか、自分が何をすべきかがわかるところにある。自ら気づくほうが、他者に指摘されるより、対策に取り組もうという意欲が湧くのではないか。

▶相対評価と絶対評価について

Q: 情報セキュリティ対策ベンチマークは他社との比較による相対評価だが、比べる対象が低すぎたり、高すぎたりするリスクがあるのではないか？

A: もちろん、そのようなリスクはあるが、母数が集まれば、そのようなリスクは低減されると思う。相対評価にも絶対評価にもそれなりの良さがあるが、特にまだ対策が進んでいないところは、相対評価により、自社の位置を知り、まずは他者の対策レベルに追いつくというように、回りを見ながら対策を順次向上させるという道筋のほうが取り組みやすいのではないか？情報セキュリティ対策ベンチマークの診断においては、5段階評価の4はPDCAが回っているレベルである。ある目標を決めて、その目標に適合しているかどうかを評価する絶対的評価であれば、4のレベルを目指すべきなのだろうが、最初からハードルが高いとあきらめてしまう可能性もある。このあたりに、絶対値を決めての評価の難しさがある。さらには、グループ会社の対策状況の評価に情報セキュリティ対策ベンチマークを使うのであれば、比較する対象は、情報セキュリティ対策ベンチマークに蓄積された診断データだけではなく、各グループ会社間でその情報セキュリティ対策状況の比較ができる。そういう意味では、比べる対象が高すぎる、低すぎるというような懸念は無用ではないか？

情報セキュリティ対策ベンチマークの良さは、自社は相当情報セキュリティ対策が進んでいると思っていたが、診断結果を見て、他より遅れていたことにショックを受け、対策を進めなければという意識付けが強烈にできるところにもあるのではないかと考える。

このような議論を経て、情報セキュリティ対策ベンチマークの採用を決定した。Y部長は、Z部員を担当者に任命し、情報セキュリティ対策ベンチマークをグループ会社の対策状況の評価のために使うことに関する社内稟議書及び、各グループ会社に配布する、情報セキュリティ対策ベンチマークの概要説明書と診断結果を報告するフォーマットの作成を指示した。

3 情報セキュリティ対策ベンチマークによる診断の実施

社内稟議の承認も済み、概要説明と報告用フォーマットもできあがり、グループ会社100社に対して、情報セキュリティ対策ベンチマークの診断を実施することとなった。概要説明書と報告用フォーマットは、エクセルで作成された2ページ見開きの簡潔なもので、1ページ目に概要説明、2ページ目の報告用フォーマットにはその会社の診断点数を書き込むことができるようになっている。X社は、情報セキュリティ対策ベンチマークの診断では、グループⅠ（高水準のセキュリティレベルが要求される層）に分類される。報告用フォーマットには、各グループ会社が診断点数を入れると、グループⅠでの比較はもとより、X社グループ全体での平均、望まれる水準との比較もできるような工夫がなされていた。

X社のグループ子会社は、製造、販売、金融（クレジット）、商社、出版など、10程度の業種がある。企業規模も10,000名を超すものから、20名以下の小規模事業者までさまざまである。これらの会社には、業務を委託することも多いので、グループ子会社は、外部委託先と同様の位置づけである。セキュリティに対する意識も会社によって温度差があり、高いものから低いものまであるため、これらの会社に対して、最初に情報セキュリティ対策の重要性と、今回、情報セキュリティ対策ベンチマークの診断を依頼する背景についての説明を行い、協力を要請した。

情報セキュリティ対策ベンチマークの診断については、手間、時間、費用がかからないことから、あまり抵抗もなく、すんなりと各グループ会社に受け入れられ、概要説明書と報告用フォーマットを配布する運びとなった。なお、診断結果の回収にあたっては、報告用フォーマットとともに、IPAのWebサイトで提供している、PDF出力した診断結果もあわせて提出させることとした。

グループ子会社各社に情報セキュリティ対策ベンチマークの診断を依頼するに先立って、X社では、まず自らが情報セキュリティ対策ベンチマークの診断を行うこととした。その際、情報セキュリティ部で把握している事柄に加え、従業員へのヒアリングを行ったり、他部署の文書を閲覧したり、対策実施状況の裏づけを取る作業を行い、さらには、回答内容について、情報セキュリティ委員会の同意を得た上で、診断を行った。

情報セキュリティ対策ベンチマークの診断のように簡易なものでも、グループ会社全体で行うとなると、それを実施する情報セキュリティ部では、それなりの準備が必要であり、時間もかかる。概要説明と報告フォーマットの作成、配布と回収、回収した診断結果の分析などに、担当のZ部員もかなりの時間を割くこととなった。さらには、概要説明の配布から回収までに、およそ1ヶ月の期間を要することとなった。このような状況を見て、情報セキュリティ対策ベンチマークによる診断の実施を提案したY部長は、いまさらながら、この方法を選択したことのメリットを実感するのであった。

4 情報セキュリティ対策ベンチマークによる診断結果の分析と考察

Y部長は、100社より回収した診断結果をZ部員に分析させ、分析結果の報告を指示した。情報セキュリティ対策ベンチマークでは、散布図とレーダーチャートで次のような診断結果を見ることができる。

▶散布図

(1) 自社が3つのグループのどのグループに分類され、その中でどの位置にあるかを散布図で確認。
(2) 従業員数300名以下、301名以上の企業規模によるグループ分けと、各グループ内での自社の位置の散布図による確認。

▶レーダーチャート

(1) リスク指標に応じて分類されたグループ内での、平均や望まれる水準と自社のレベルとのレーダーチャートによる比較。
(2) 従業員数により分けられた各グループ内での平均、望まれる水準と自社のレベルのレーダーチャートによる比較。
(3) 業種ごとにわけ、同業種内での平均、望まれる水準と自社のレベルのレーダーチャートによる比較。

▶その他

(1) 自社の過去の診断結果と現在の診断結果の比較。
(2) PDFに出力した診断結果では、「情報セキュリティ対策ベンチマーク確認票」も表示される。

Z部員は、100社にのぼるグループ会社の診断データがあることから、IPAのWebサイト上で提供される診断結果に加え、次のような分析を試み、Y部長に結果を報告した。

▶診断データ分析の内容

(1) トータルスコア及び25項目ごとのスコア平均それぞれについて、グループIでの全国平均とグループ会社全体の平均の比較。

(2) 25項目ごとのスコアの全国平均と比較して特に高い対策項目と低い対策項目の抽出。

(3) グループ会社を資本の大きさごとにABC区分に分け、これらの区分でトータルスコアの平均と25項目ごとのスコアの平均それぞれについて比較。

(4) グループ会社を従業員規模で、1000名以上、300名から1000名、300名未満にわけ、企業規模によるトータルスコア及び25項目ごとのスコア平均それぞれについての比較。

(5) グループ会社を業種ごとにわけ、業種ごとのトータルスコアの平均及び25項目ごとの対策のスコアの平均それぞれについて比較。(X社においては、グループ子会社は、各事業部の配下にあるため、業種ごとの分類は、事業部ごとの分類と同義)。

(6) 情報セキュリティ対策項目の5段階の回答の分布をグラフにより図示し、どの業種グループがどの項目で遅れているか、または進んでいるかの分析。

▶診断データ分析結果の考察と改善提案

(1) 診断データの分析内容により、全国平均と比較して特に低い対策項目については、改善提案 (原因の分析とどのような改善が可能かの提案) を作成。

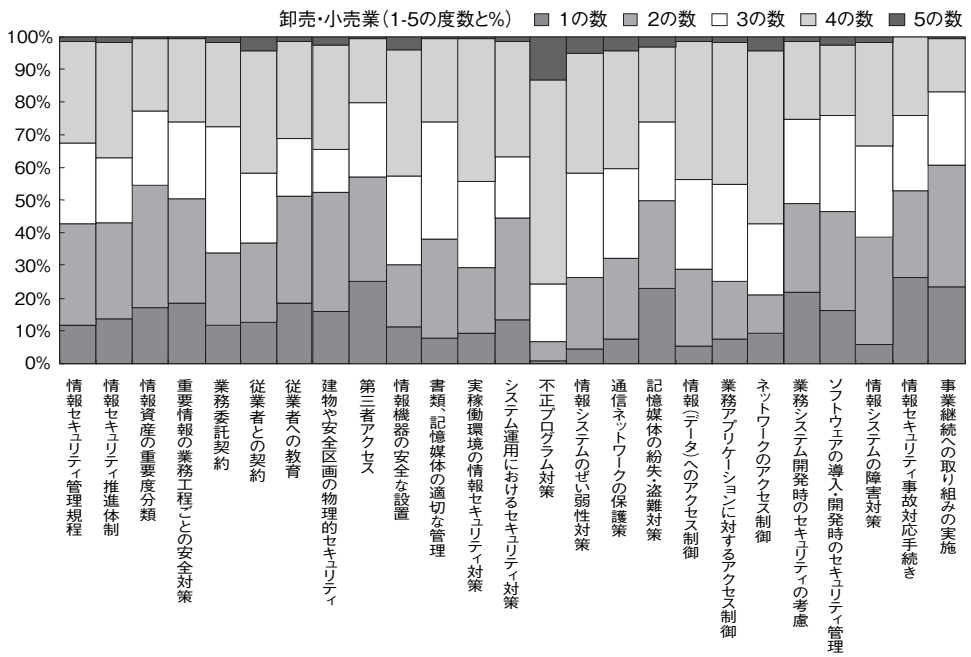


図2.6　Z部員の分析結果のグラフの例示 (業種別1-5の回答数 (%) の比較)

(2)診断データの分析内容により、業種ごと（事業部ごと）に対策状況に差があったものは結果を事業部に伝え、弱い部分の改善を提案。
(3)診断データの分析内容により、遅れている対策項目を抽出し、改善を提案。

5 今後の課題

Y部長は、Z部員からの報告を受け、報告の準備を始めた。準備をしながら、今回の診断により見えてきた課題と今後の展開に思いを馳せた。

▶Y部長の所感

(1)情報セキュリティについて良く知らないところは、高い点数をつけ、反対に情報セキュリティについて良く知っているところは、シビアに点数をつける傾向がある。今回の診断では、わが社が診断前に行ったような準備作業を各グループ会社に要求したわけではなかったために、このような差が見られたのかもしれない。今後は、情報セキュリティについて良く知らないところへの教育や、診断前の準備作業に関しての意識付けが必要である。
(2)情報セキュリティ対策ベンチマークは、大項目で答える以外にも、対策のポイントで細かく見ていくことができる。そこで、対策のポイントの実施目標を年ごとに決めて、段階的にスパイラルアップでしていきたい。
(3)小規模企業においては、点数の高い低い以前に対策を考えていない領域がある。そこで、小規模企業が情報セキュリティ対策を始めるきっかけにするような使い方もできる。一般に、大企業はスタッフがいて、対策も進む。中小企業の中には、社長以下数名の規模のところもあり、対策が難しい。
(4)今回の診断に当たっては、わが社では、従業員へのヒアリングを行った。情報セキュリティ対策ベンチマークの設問に対応した従業員向けのヒアリングをWebサイト上で提供してくれれば、この作業はかなり軽減できる。また、そのようなツールをうまくアレンジすれば、小規模企業向けの診断ツールになるかもしれない。小規模企業は、個人の延長のような規模の企業も多く、その情報セキュリティ対策については現在打つ手が無い。業務委託の孫請けが、小規模企業である場合もあり、小規模企業の情報セキュリティ対策は看過できない問題である。しかし、小規模企業向けに情報セキュリティ対策ベンチマークほどの網羅性を求めて良いものかどうかの課題は残る。
(5)情報セキュリティ対策は、自律的なボトムアップの活動に落とし込めたら良いと考えている。QCの小集団活動は、何十年も続いて、この活動を行うことが習慣になっている。安全衛生運動は、労働安全衛生法の要求事項を踏まえた活動が定着している。情報セキュリティ対策に関する活動も、仕事の中に自然に入り込み、続けていけるようになれば良いと思う。
(6)全社で同じ考え方、基準に則って対策をするのは、内部統制にも通じる。
(7)情報セキュリティ対策ベンチマークは、情報セキュリティ対策の底辺を広げるには、とても良いツールだと思う。

このようにして、X社の第1回目の情報セキュリティ対策ベンチマークによる診断は終わった。数々の成果もあり、今後の課題も見えてきた今、Y部長は、この診断を毎年の定例行事にしようと考えている。また、英語版の情報セキュリティ対策ベンチマークが公開されたことでもあり、海外の子会社へ情報セキュリティ対策ベンチマークの診断を広めることを考えている。

情報セキュリティ対策
ベンチマーク活用集

3章 情報セキュリティ対策ベンチマークからISMS認証取得へ

1 情報セキュリティマネジメントシステムの構築

1 J社の情報セキュリティ対策上の課題

J社では、各種のセンターサービス業務を行っており、アウトソーシングサービス、特にＡＳＰサービスなどが伸びている。これらのサービスは、顧客の基幹業務に大きな影響を与えるため、サービス業務の信頼性、安全性などを確実なものとしなければならなかった。しかしながら、外部委託先の情報セキュリティ対策状況の把握が不十分であり、顧客からの要求事項に対応できるかどうか不安があった。また、他社のデータセンターが顧客情報の漏えい事故を起こすなど、社会的信用にも大きな問題となっていた。J社では、2005年より情報セキュリティ対策ベンチマークを利用して、全社的に情報セキュリティ対策の実態を時系列で把握することとしていたが、このようなセキュリティ事故発生を契機に社内の情報セキュリティ対策を見直すこととなった（**図3.1**参照）。

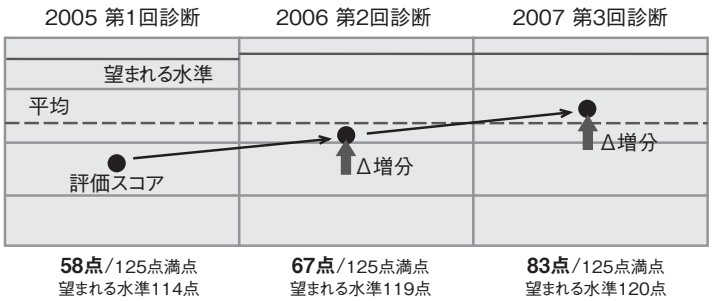


図3.1　情報セキュリティ対策ベンチマークによる時系列比較

その結果、情報セキュリティ対策は技術だけではなくそれをどう運用・管理するか、社内の制度・ルールなどが重要であると認識させられた。特に、情報セキュリティに対する危機意識が低いために起因する人的なミスを無くすためには、現場レベルにおける個人それぞれの情報セキュリティに対する認識を向上させることが重要であり、繰り返して教育・訓練活動を実施する必要があった。

このような状況から、情報セキュリティを確保するための企業の経営基盤として情報セキュリティマネジメントシステム（ISMS）の導入を検討することとなった。さらに、ISMS適合性評価制度の認証基準であるJIS Q 27001の要求事項に適合させることによって、顧客に対して組織の情報セキュリティ対策への取り組み姿勢をアピールすることにつながるとともに、情報セキュリティを維持・向上させる仕組みとしてISMS認証取得は有効と判断したからである。

2 ISMS導入の準備

▶情報セキュリティ対策推進会議の設置

J社では、情報セキュリティ管理活動や関連する規程は存在するが、情報セキュリティに関する統一的な活動が不足しているとの認識から、データセンター事業部部長を中心として、「情報セキュリティ対策推進会議」を設置し、全社的な情報セキュリティ対策について検討することとした。その際、JIS Q 27001の要求事項のほか、ISMSの実践規範であるJIS Q 27002、及びJIPDEC発行のISMSユー

ザーズガイド（平成18年12月発行）を参考にした。

その結果、データセンター事業部部長は、情報セキュリティマネジメントの仕組みを確立することの重要性を認識した。データセンター事業部部長が、検討成果を社長に報告した結果、「会社として情報セキュリティマネジメントの仕組みを確立するように」との指示が下った。検討成果の報告の際に、データセンター事業部部長は、社長に対して、情報セキュリティマネジメントの仕組みを確立するためには、各部との連携が不可欠である旨を説明し、各部門からの支援とコンセンサスを得る必要性から、「情報セキュリティ対策推進会議」を設置した。関係する各部門のメンバーを集めて検討することについては、取締役会の承認を得た。「情報セキュリティ対策推進会議」は、運用部門担当の役員（常務取締役）が責任者となり委員（関連部署の部長クラス）を任命し、通常の組織運営に組み込んだ。

「情報セキュリティ対策推進会議」のメンバー（部門）を**表3.1**に示す。

表3.1　情報セキュリティ対策推進会議のメンバー（部門）一覧

部門名	役　割	参加メンバー	選定理由
総務部	ルールを決める側として参加	総務課長 人事課長	・全社規程類の発行の管理責任部門である。 ・人の採用の責任部門である（外注を含む）。 ・社内のトラブル案件の相談窓口であり、情報セキュリティに関する対応も今後必要となる。 ・施設面に責任を負う部門である。 ・プライバシーを守るべき部門である。 ・懲罰等に関する部門である。 ・教育に関する部門である。
内部監査室	ルールを決める側として参加	監査室長	・内部監査を行う部門である。 ・情報セキュリティ監査の主管部門となる。
法務部	ルールを決める側として参加	法務部長	・契約関連及び法務面に関連する事項を担当する部門である。
データセンター事業部	ルールを決める側として参加	事業部長 A課長 B課長 C課長	・事業所の運用管理に責任をもつ部署である。 ・システムの企画・開発・運用の管理責任部門であり、情報システムのセキュリティ対策を実施している。 ・事業所内のLANに責任を負っている。

▶検討すべき課題と実施方針

「情報セキュリティ対策推進会議」における検討の結果、JIS Q 27001の要求事項に対して、下記の検討すべき課題について、その対策を実施する方針案が取締役会に報告され、承認された。

(1) ISMS基本方針の策定及びISMS適用範囲と境界の定義
(2) 情報セキュリティに関する管理組織の整備
(3) 情報セキュリティ基本方針に関する規程類の整備
(4) リスクアセスメント方針と手順の策定及びリスクアセスメントの実施
(5) 情報セキュリティインシデント管理
(6) 事業継続計画の作成
(7) 法的要求事項の順守
(8) 情報セキュリティに関する教育・訓練規程の策定とその実施
(9) 情報セキュリティ対策の運用及び記録
(10) 内部監査または情報セキュリティ監査に関する規程の策定とその実施
(11) マネジメントレビュー

(1)～(11)の課題に対する対策の実施については、3 ～ 13を参照のこと。

3 ISMS基本方針の策定及びISMS適用範囲と境界の定義

ISMS基本方針は、事業上の要求及び法的要求事項やリスクアセスメントなどから導かれる情報セキュリティへの要求事項を考慮し、リスクマネジメント環境、ISMSを確立し維持する組織環境、情報セキュリティの全般的な方向性及び行動指針を確立するためのものであり、情報セキュリティ基本方針のさらに上位の方針を示すものである。

そこで、「情報セキュリティ対策推進会議」では、その最初の作業として、ISMS基本方針を策定し、取締役会の承認を得た。

ISMSの適用範囲とは、合理的なマネジメントシステムの構築が可能で、外部とのインターフェースが明確にできる範囲のことであり、そのため、事業、組織、所在地、資産、技術の特徴の見地から、ISMS適用範囲及び境界を定義する必要がある。

適用範囲については、情報セキュリティマネジメントの構築を行う際に、業務手順の変更が必要となる場面も想定されるため、第一ステップとして機動的に業務手順の変更等が行える特定の部門を対象とした。将来的には、情報セキュリティマネジメントの実践を行った結果をもとに全社的な体制へと拡張することとした。具体的には、「情報セキュリティ対策推進会議」が以下の2点を考慮してISMSの適用範囲の原案を作成し、取締役会にて承認された。

(1)会社にとって情報セキュリティが特に重要な資産を含むデータセンター事業部内の業務を適用範囲とする。また、データセンター事業部の情報セキュリティについて重要な関わりを持つ部署、データセンター事業部の業務に関連する部分についても適用範囲とする。

(2)組織の活動と情報セキュリティの関係から、守るべき資産についてどのように関係するかを考慮し、適用範囲内の情報セキュリティマネジメントを構築することで一定の効果をあげられるところを適用範囲とする。

今回定めたISMS適用範囲を次頁 **表3.2**に示す。

4 情報セキュリティに関する管理組織の整備

情報セキュリティに関する管理組織及び管理責任者として情報セキュリティ対策室及び情報セキュリティ責任者を設置、任命することとした。また、情報セキュリティ対策室の上位組織として、組織全体のリスクを管理する危機管理室を新たに設置した。ドキュメントとしては「情報セキュリティに関する組織規程」に詳細を記述することとした。J社の社内組織図は、**図3.2** (P41)に示す通りである。

▶ 情報セキュリティ対策室

情報セキュリティ対策室は、情報セキュリティに関する検討・承認及び重要事項について危機管理室に事案を発議する組織としての機能及び情報セキュリティに関する各部門の調整を行う機能を持つ。

(1)情報セキュリティ対策室の責務

①情報セキュリティ基本方針のレビュー・改定案作成

②情報セキュリティ関連各種ガイドラインの策定

③情報セキュリティリスク評価の承認

④情報セキュリティリスク管理の実施

⑤情報セキュリティ事故の統括管理
⑥事業継続に関する課題の監視及び報告
⑦情報セキュリティに関する各部の指導
⑧情報セキュリティに関する社外組織との連携
⑨その他、必要に応じ、情報セキュリティに関する重大な意思決定及び危機管理室への起案を行う

(2)情報セキュリティ対策室長

情報セキュリティ担当役員（CISO:Chief Information Security Officer相当）を情報セキュリティ対策室長とした。情報セキュリティ対策室のメンバーは、適用範囲内の各部門の部門長が兼任し、さらに事務・運営要員として専任スタッフを置くこととした。

表3.2　適用範囲

No.	カテゴリ	対　象	内　容	関連する文書
1	事　業	データセンター事業部の行う事業全体に関する情報セキュリティマネジメント	・データセンター事業 ・運用監視事業 ・運用委託事業	ISMSの文書
2	組　織	データセンター事業部	業務を行う部門	組織図 職務分掌
		情報セキュリティ対策室	情報セキュリティ協議会及びクロスファンクショナル協議会の機能を持つ組織	
		総務部	以下の業務を範囲とする。 ・人事採用（外注含む） ・施設管理 ・従業員教育 ・その他データセンター事業部（大手町）の情報セキュリティマネジメントに関わる業務	
		法務部	以下の業務を範囲とする。 ・法律に関連する業務 ・データセンター事業部の契約に関する業務 ・その他データセンター事業部の情報セキュリティマネジメントに関わる業務	
		内部監査室	以下の業務を範囲とする。 ・データセンター事業部のセキュリティ監査に関する業務 ・その他データセンター事業部の情報セキュリティ管理に関わる業務	
3	所在地	大手町事業所	データセンター事業部	フロアレイアウト（空調ダクト等の設備の構成も含む） 電源・電話の配線図
		本社（右部分）	情報セキュリティ対策室 総務部 法務部 内部監査室	
4	情報技術	ハードウェア・ソフトウェア	大手町事業所内で管理されるハード・ソフトウェアを適用範囲とする。	機器構成図 ネットワーク構成図
		ネットワーク	大手町事業所からの対顧客・対インターネット接続のルータを含む。	
5	資　産	上記1～4に所属するすべての情報資産を適用範囲とする。 各部の作成する資産管理目録にて詳細が定義される。		資産管理台帳

▶情報セキュリティ責任者及び情報セキュリティ管理者

適用範囲内の各部門に情報セキュリティ責任者を任命することとし、各部門の部門長を情報セキュリティ責任者に任命した。また、情報セキュリティ責任者を補佐する情報セキュリティ管理者（課長職相当）を各部門から2名任命した。

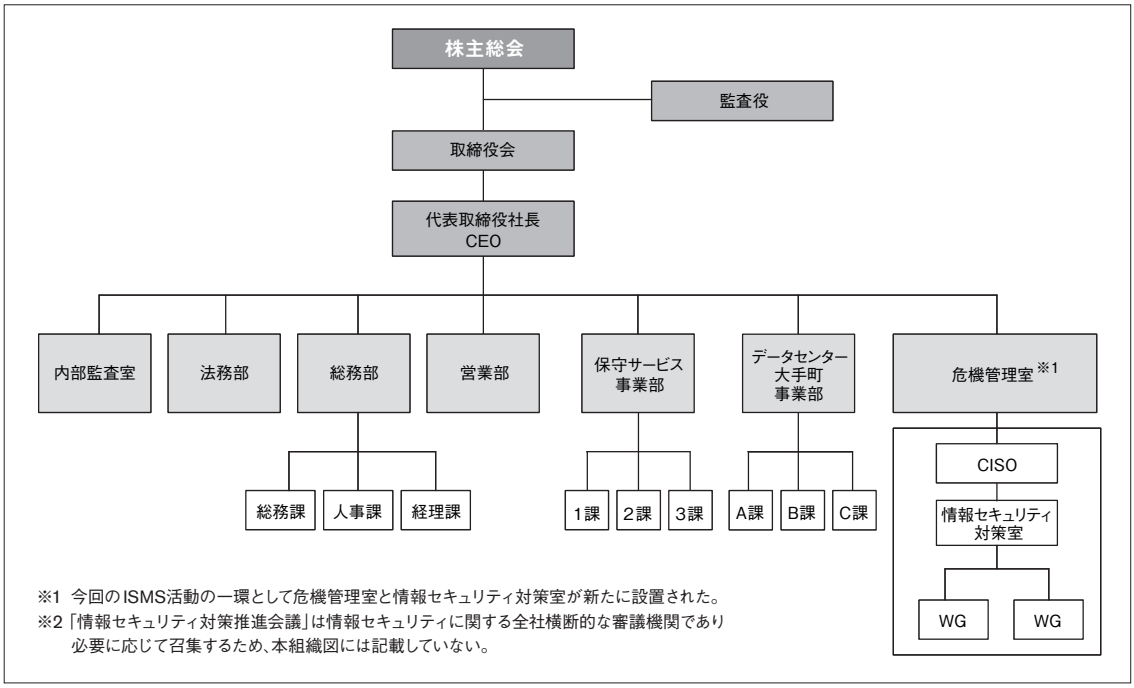


図3.2　J社の社内組織図

5 情報セキュリティに関する規程類の整備

情報セキュリティに関する規定類の整備に関しては、現在の情報セキュリティ基本方針及び既存の情報セキュリティに関連する各種の文書を活用した。さらに必要なドキュメントとして、適用範囲内向けの各種情報セキュリティガイドラインを作成し、それに従ってルール・手順書等を作成した。情報セキュリティ基本方針については、J社として考えるべき情報セキュリティ上のポイントを、現場に理解しやすい表現とすることで、現場への浸透を図ることを重視した。

▶情報セキュリティ関連のドキュメント類

情報セキュリティ基本方針に基づくドキュメント類は次の通りである。

(1)情報セキュリティ基本方針

情報セキュリティの目的とその考え方等について定義した文書である。当社の情報セキュリティに関する全社的な規程として存在する。

(2)情報セキュリティ関連全社規程

全社規程は、情報セキュリティに関連するか否かにかかわらず、その適用や周知について全社員が対象となっている規程の総称である。情報セキュリティ関連全社規程は、適用範囲内の資産に関連して情報セキュリティを守る管理・対策として適用可能なものを、情報セキュリティ対策室が選択したもので、情報セキュリティ基本方針から引用される規程である。なお、今回のISMS活動の一環として新たに危機管理室や情報セキュリティ対策室が設置されたが、これらの組織に関しては、「情報セキュリティに関する組織規程」に詳細を記述した。

(3)情報セキュリティガイドライン

情報セキュリティマネジメントを行うために必要であり、かつ上記(1)、(2)に含まれないものについて、対策の指針を示すものとして新たに適用範囲内のみの情報セキュリティガイドラインとして作成する。

(4)ルール・手順書等

(1)～(3)に基づいて作成され、部門内のルール及び手順書として作成する。

情報セキュリティ基本方針に基づくドキュメント体系を**図3.3**に示す。

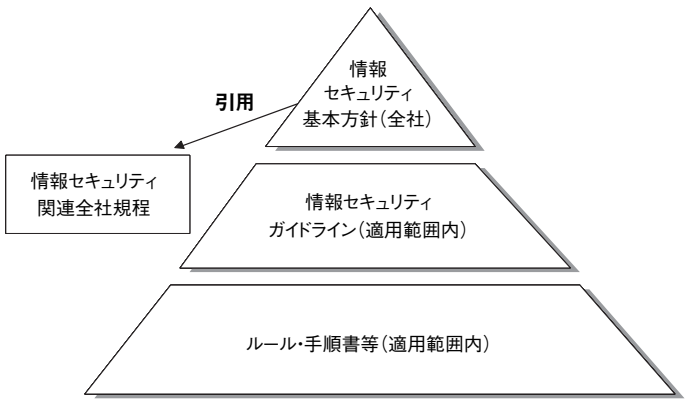


図3.3　ドキュメント体系

ドキュメント体系に対応するドキュメントの例示を**表3.3**～**表3.7**に示す。情報セキュリティ関連全社規程とは、J社に既に存在する情報セキュリティ関連規程である。

表3.3　情報セキュリティ基本方針(全社)

No.	ドキュメント名	内容	承認者	実施責任者
1	情報セキュリティ基本方針	全社の情報セキュリティ 基本方針	取締役会	役員・従業員等

表3.4　情報セキュリティ関連全社規程（全社）

No.	ドキュメント名	内容	承認者	実施責任者
1	文書管理規程	文書管理に関する規程	取締役会	従業員等
2	危機管理室規程	危機管理室の役割、メンバ及び責務に関する規程		危機管理室
3	営業秘密管理規程	不正競争防止法に対応し、企業における営業秘密を管理するための規程		役員・従業員等
4	内部監査規程	内部監査に関する規程		内部監査室
5	就業規則	社員の就業に関する規則		従業員等
6	システム開発規程	システム開発に関する規程		関連部門
7	契約締結に関する規程	ユーザと契約を締結する際の規程		
8	データセンター内ネットワーク管理規程	データセンターの有線、無線LANの構成管理等		
9	データセンターの環境整備に関する規程	耐震設備、耐火設備、電力供給、電話回線の維持等に関する規程		
10	顧客情報保護規程	顧客情報保護に関する規程		役員・従業員等
11	携帯電話の使用に関する規程	携帯電話の使用に関する規程		

表3.5　情報セキュリティ関連規程（適用範囲内）

No.	ドキュメント名	内容	承認者	実施責任者
1	情報セキュリティに関する組織規程	情報セキュリティ管理体制及び責任に関するガイドライン	取締役会	役員・従業員等
2	リスクマネジメント規程	リスクアセスメント及びリスク対応実施に関するガイドライン	危機管理室	情報セキュリティ対策室及び関連部門

新たに作成する必要がある情報セキュリティガイドライン（適用範囲内）及びルール・手順書等（適用範囲内）の例示を**表3.6**～**表3.7**に示す。

表3.6　情報セキュリティガイドライン（適用範囲内）（抜粋）

No.	ドキュメント名	内容	承認者	実施責任者
1	情報セキュリティ教育・訓練ガイドライン	情報セキュリティ教育に関するガイドライン	情報セキュリティ対策室長	総務部及びデータセンター事業部の情報セキュリティ責任者
2	情報セキュリティ監査ガイドライン	情報セキュリティ監査の計画実施及び報告に関するガイドライン		内部監査室の情報セキュリティ責任者
3	情報セキュリティ事故管理ガイドライン	情報セキュリティ事故管理に関するガイドライン		各部の情報セキュリティ責任者
4	コンプライアンスガイドライン	法律等への準拠に関するガイドライン		
5	事業継続計画作成ガイドライン	事業継続計画作成に関するガイドライン		データセンター事業部の情報セキュリティ責任者
6	物理的アクセス管理ガイドライン	入退室に関するガイドライン		総務部及びデータセンター事業部の情報セキュリティ責任者
7	論理的アクセス管理ガイドライン	オペレーションシステム、アプリケーションシステム、データベース等の論理的アクセスを設定する際のガイドライン		

表3.7　ルール・手順書等（適用範囲内）

No.	ドキュメント名	内容	承認者	実施責任者
1	ルール・手順書等（ここでは詳細は記述しない）	**表3.6**のドキュメントに従って各部門で作成する	情報セキュリティ対策室長	各部の情報セキュリティ責任者

6 リスクアセスメントの実施

▶リスクアセスメント方針と手順の策定及び実施部門

(1) リスクアセスメントの方針と手順の策定

リスクアセスメントの目的は、ISMSの適用範囲において特定した資産に対して、情報セキュリティに与える影響を考慮し、実際に情報セキュリティマネジメントの対策を講じる対象となるリスクを洗い出すことにある。リスクアセスメント方針及びその手順は、ISMS基本方針に従って、資産価値、脅威、ぜい弱性等を評価するための構造、仕組みとして定義し、文書化する必要がある。

リスクアセスメントは、リスク分析からリスク評価までの全てのプロセスと定義される。リスク分析においては、それぞれの資産に対する脅威とぜい弱性からリスクのレベルを算定し、リスク評価ではリスク受容基準及びリスク受容可能レベルを決定する。そして、リスク評価の結果に基づきリスク対応を実施することとなる。

J社では、ISMSユーザーズガイドを参照し、自社に適した方式を検討した。その結果、ベースラインアプローチと詳細リスク分析手法に基づき、資産とそれに関連する脅威をリストアップし、リスクアセスメントを実施する方法を採用することとした。

ベースラインアプローチは、大きく分けると「ベースラインの決定」と「ギャップ分析の実施」の2つの手順で実施される。ベースラインは、情報セキュリティ管理について、組織の定める独自の対策基準であるが、J社では、この基準にJIS Q 27001付属書Aの管理策を準用することとした。また、ギャップ分析の際は、情報セキュリティ対策ベンチマークの25項目の質問と対策状況を把握することにより、ギャップ分析結果として活用することとした。

(2) リスクアセスメントの実施項目及び実施部門

リスクアセスメント実施項目と実施部門を**表3.8**に示す。

表3.8　リスクアセスメント実施項目と実施部門

No.	実施項目	実施部門	承認
1	リスクアセスメント手法の決定	情報セキュリティ対策室	危機管理室
2	情報セキュリティリスクアセスメント手順書作成	情報セキュリティ対策室	危機管理室
3	リスクアセスメント実施	データセンター事業部	情報セキュリティ対策室
4	リスク評価結果を情報セキュリティ対策室へ報告	データセンター事業部	情報セキュリティ対策室
5	リスク対応の決定（管理策の決定）	情報セキュリティ対策室	危機管理室
6	ガイドライン等の作成	情報セキュリティ対策室	危機管理室
7	基本方針及び関連規程の見直し	情報セキュリティ対策室	危機管理室
8	リスク対応より対策の決定	データセンター事業部	情報セキュリティ対策室
9	対策の実施・運用	データセンター事業部	情報セキュリティ対策室

情報セキュリティリスクアセスメント手順書や関連するガイドラインは、リスクアセスメントを実際に行う部門が実施可能なように、平易な表現で記述することとした。方針、手順、実施部門が決まったところで、第一段階としてギャップ分析を、第2段階として詳細リスク分析を行うこととなった。

▶リスク分析の実施

(1)第1段階：ギャップ分析の実施

ギャップ分析の目的は、現状の管理策の適用状況の把握にある。ギャップ分析は、一般的に推奨される管理レベルと組織の現状の管理レベルを比較し、「大きな差が認められる箇所」、「明らかに管理策の適用を必要としている箇所」を発見し、より詳細なリスク分析の実施を検討することにある。

ISMSの適用範囲で定義した資産は、すべてギャップ分析の対象である。この段階では、資産を一つひとつ個別に比較するのではなく、対象となる資産をまとめたグループを一つのまとまりと見て分析を実施することが望ましい。

JIS Q 27001の管理策の適用状況を初期段階でチェックする際に、情報セキュリティ対策ベンチマークによる診断結果をもとに、組織における管理策の適用状況、問題の所在等を、25項目の情報セキュリティ対策状況を確認したり、146項目の対策のポイントを利用して確認した。

(2)第2段階：詳細リスク分析の実施

ギャップ分析により発見された問題箇所の重大なリスクの存在を明らかにした後に、詳細リスク分析を実施した。

詳細リスク分析の対象は、ギャップ分析の結果、「基準に適合していない」、「基準に一部適合していない」と判断された箇所のみとする。そこで、ISMSが対象とする資産のうち、すでに適切な管理策が適用されていると判断された項目については、詳細リスク分析の対象から除外し、基準への適合が疑わしい項目に関連するものについて、資産ごとに詳細リスク分析を実施した。

▶リスク対応

詳細リスク分析の評価結果から、リスク受容基準を超える場合のリスク対応として、情報セキュリティ対策（選択した管理策）を実施することとなる。

J社では、「情報セキュリティリスクアセスメント手順書」に従い、データセンター事業部にてリスクアセスメントを実施した。その結果、明らかとなったリスクについて、情報セキュリティ対策室がリスク対応策の検討を行った。

リスク評価およびそれに続くリスク対応の方針は下記の通りである。

(1) 情報セキュリティ対策チェックシートを作成し、チェックシートに現状を記述し、記入者がリスクを評価する。

(2) 実現できない対策については、情報セキュリティ対策室の検討メンバーが対策チームとなり、評価の上、リスクを受容する判断をくだす。

リスク評価シート　　No.

基準目的	【基準目的の番号】
基準項目	【基準項目の内容】
当社状況	【当社にとっての該当内容】

関連する資産

番号	内容	ビジネスへの影響
A1	【該当する情報資産1】	【ABCで記入】

関連する脅威

番号	内容	備考
T1	【該当する脅威の内容】	

関連する対策

番号	内容	対策済	備考
P1	【当社における基準対策】	□ 済の場合（■）	対策状況、不備内容等

リスク

A	T	P	内容	リスク	備考
資産	脅威	未実施対策	【リスク内容】	ABCで記入	理由等

図3.4　リスク評価シート

リスクアセスメントとリスク対応は、以下の手順で実施された。

(1)情報セキュリティ対策室がリスク評価シート（**図3.4**参照）の「当社状況」、「関連する脅威」、「関連する対策」を記述する。

(2)リスクアセスメントを行う部門は、次の作業を実施する。

①「関連する資産」に、該当する資産を記述し、事業への影響を記入する。

②「関連する対策」の「対策済」欄を記入する。

③「リスク」を記入する。

④すべてのリスク評価シートに対して①～③を行った後、結果を情報セキュリティ対策室に提出する。

(3)情報セキュリティ対策室は、提出されたリスク評価シートをもとにリスク対応を行う。

▶規程類・ガイドライン及び適用宣言書の見直し

リスク対応の結果、規程・ガイドライン等の見直しが必要になる場合がある。これらの見直しについても順次行うこととした。

また、リスク対応の結果、選択した管理目的及び管理策、並びにそれらを選択した理由について見直しを行い、適用宣言書の改訂版を作成した。

リスク対応計画フォーマットを**表3.9**に示す。

表3.9　リスク対応計画フォーマット

				ISMS 管理責任者	実行責任者
管理No.	×××××××	優先順位	①		
資産		管理策		対策費用	
				想定損害額	
現状の問題点					
改善策と 予想改善効果				リスクのレベル （前）	リスクのレベル （後）

実施項目		担当者						
1								
2								
3								
4								
5								
6								
7								
8								
		確認						

7 情報セキュリティインシデント管理

情報セキュリティインシデントの発見・報告・対応及び再発防止策を速やかに行うためには、事前に情報セキュリティインシデント管理に関する手法や手順を定める必要がある。そこで「情報セキュリティインシデント管理ガイドライン」を策定し、手法と手順を詳細に記述した。また、事故が起こった際は、「情報セキュリティインシデント対策報告書」を記録として保存することとし、報告書の雛形も作成した。

通常の情報セキュリティインシデント管理の系統については、次頁 **図3.5**に示す。

▶情報セキュリティインシデントの定義と特例

(1)情報セキュリティインシデントの定義

次頁 **表3.10**のいずれかを情報セキュリティインシデントとして定義した。

(2)情報セキュリティインシデントの特例

情報セキュリティインシデントの特例となる重大な情報セキュリティインシデントについて定義し、特例については、別途「危機管理規程」にて定めることとした。

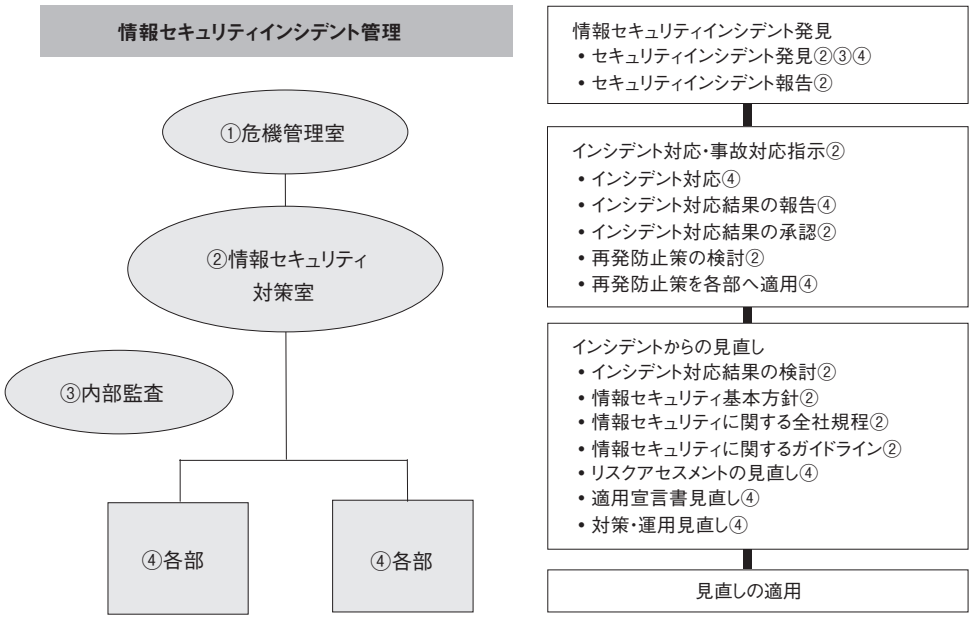


図3.5　通常の情報セキュリティインシデント管理の系統

表3.10　情報セキュリティインシデントの例示

No.	分類	内容	原因
1	業務障害	業務の継続が困難	天災、人災、公共インフラ停止、機器破壊等
2	サービス障害	正常なサービスの継続が困難	ハード・ソフト障害、スタッフの緊急入院等
3	情報障害	守るべき情報の不全	情報漏えい、情報改ざん、情報破壊等
4	セキュリティ侵害	（実害とは関係なく）情報セキュリティ対策が破られる	不正アクセス、ウィルス発生、パスワード漏洩等
5	セキュリティ障害	情報セキュリティ対策が実施されないまたは効果がない	ファイアウォール設定不備、鍵管理不備等
6	インシデントの疑い	上記1 ～ 5への重大な疑い	

表3.11　情報セキュリティインシデントの特例（例示）

No.	分類	内容	原因
1	重大事故	経営に関わる事故	大災害、事件、多くのスタッフの緊急入院、大量の顧客情報流出等

▶情報セキュリティインシデント対応

(1)情報セキュリティインシデント発生時の連絡体制

情報セキュリティインシデント発生時の連絡体制を定めておくことで、発見者は、情報セキュリティインシデントまたは情報セキュリティインシデントに関する重大な疑いがある場合に遭遇した場合に、速やかに報告することが可能になる。インシデント発生時の連絡体制は、**表3.12**のように定められた。

表3.12　インシデント発生時の連絡体制

No.	連絡元	連絡先	内容
1	発見者	所属部門の情報セキュリティ責任者	情報セキュリティインシデントの種類・状況 発見者氏名及び発見者への連絡方法等
2	所属部門の情報セキュリティ責任者	情報セキュリティ対策室長	情報セキュリティ責任者の判断で、必要時に連絡
3	情報セキュリティ対策室長		情報セキュリティ対策室長が重大事故と判断した場合、「危機管理規程」に従い連絡

(2)情報セキュリティインシデントの調査及び対応

情報セキュリティインシデントの調査及び対応は、情報セキュリティ責任者の指示により、各部門が行うものとした。ただし、緊急性のある場合はこの限りではない。

(3)情報セキュリティインシデントの記録

情報セキュリティインシデント対応後、情報セキュリティ責任者は、情報セキュリティインシデント報告書を作成し、情報セキュリティ対策室に提出することとした。

(4)情報セキュリティインシデントからの学習

情報セキュリティインシデント発生の際は、速やかな対応が必要であるが、再発防止のために、情報セキュリティインシデントより学ぶことは重要である。そこで、対策の見直しや再発防止策について以下の通り定めた。

- 情報セキュリティ対策室は、情報セキュリティインシデント報告書をもとに、情報セキュリティマネジメント及び対策に関する全社的見直しを行う。
- 情報セキュリティ対策室は、情報セキュリティインシデント報告書をもとに、再発防止策の全社への適用を検討する。

8 事業継続計画の作成

データセンター事業部が中心となり、事業継続計画を作成した。ドキュメントとしては、「業務継続計画作成ガイドライン」に事業継続の目的、枠組み、事業継続対応組織などの詳細を記述した。また、「事業所業務継続計画」には、対応手順等の詳細を記述した。

▶災害・事故の想定

事業継続計画策定にあたっては、想定される災害及び事故について、業務への影響を分析した。

- 天災　　：地震、水害、火災、落雷等
- 人的災害・障害　　：テロ、犯罪、誤用等による事故等
- 公共インフラの不全　：電力、水道、ガス、公衆回線等
- 情報セキュリティ侵害：情報の改ざん、破壊、漏えい、サービス 妨害等

▶リスクアセスメントと危機管理の実施

想定する災害・事故に対し、リスクアセスメント手順書に従ってリスクを評価し、危機管理によるエスカレーションモデルを確立することとした。

事業継続計画はJ社にとって重要度が非常に高いため、情報セキュリティ基本方針に明確に事業継続管理について記述することとなった。また、リスクアセスメントの結果明らかになった事業継続上の不備については、その改善点を検討した上で、情報セキュリティ規程へ反映させることとなった。

▶訓練及び試験の実施

実際に事業の継続を脅かすような事態が発生した場合に、現実の対応が滞りなく行われるよう、事業継続要員の訓練も必要である。そこで、「事業所業務継続訓練計画」を定め、危機管理によるエスカレーションモデルにもとづいて、訓練及び試験を実施する。訓練結果は、「事業継続訓練・試験結果」としてその記録を保存することとした。

9 法的要求事項の順守

法務部が中心となり、法的要求事項の順守プログラムを作成した。ドキュメントとして「コンプライアンスガイドライン」に枠組みや体制等の詳細を記述した。また、「法的要求事項の順守プログラム」には対応手順等の詳細を記述した。さらには、「法的要求事項の順守プログラム」に従い、各種記録を保存することとした。

▶法的要求事項の順守プログラム策定にかかわる作業

以下に、法的要求事項の順守プログラム策定にかかわる作業を列記する。

(1)関連する法規のリストアップ

法務部は、当社業務に関連する法律、条例、業界ガイドライン等（以下、法令等）の一覧を作成する。

(2)責任部門及び実施部門の明確化

情報セキュリティ対策室は、関連する法令等に対し、順守すべき責任部門を割り当て、責任部門の情報セキュリティ責任者をその責任者とする。

(3)法的要求事項の順守プログラムの作成

各法律等の責任者が法的要求事項の順守プログラムを作成する。この際、責任者は必要に応じ法務部の助言を受ける。

(4)社内規程及び契約のチェック

法務部は、社内規程及び契約について、関連法令等への準拠をチェックする。

10 情報セキュリティに関する教育・訓練規程の策定と実施

J社では、継続的な教育・啓蒙活動を重視し、すべての役員・従業員等に対し、初期及び定期的な情報セキュリティ教育を行うことを定めている。教育は、集合教育に加え、シフト勤務者、協力会社要員も多いことから、e-ラーニングを各部署単位で導入し、活用・実施することとした。ドキュメントとして「情報セキュリティ教育・訓練ガイドライン」に教育計画の策定方法、教育対象、実施に関する事項を記述した。また、「情報セキュリティ教育教材」及び「情報セキュリティ教育出席簿」を記録として保存することとした。

▶全社的な情報セキュリティ教育

全社的な情報セキュリティ教育については、総務部が担当部署となり、ISMS適用範囲内の全役員・従業員等に対する情報セキュリティ教育計画を策定し、教育の実施および実施記録の作成と保管を行うこととなった。教育は、毎年4月に定期的に行うこととし、これ以外の時期に新たに任命される役員、新たに就業する従業員等については、個別に教育を行うものとした。

教育実施時には教育受講者の記録を作成し、全役員・従業員等が教育を受講したことを確認することとした。

情報セキュリティ教育は、実施時期や実施方法により次の場合が考えられる。

(1) 初期情報セキュリティ教育

役員の新規任命時、従業員等の就業開始時に初期情報セキュリティ教育を実施する。また、ISMSの導入時に対象となる役員及び従業員等に対して情報セキュリティ教育を行う。

(2) 定期情報セキュリティ教育

役員・従業員等に対し、定期的な情報セキュリティ教育を実施する。

(3) 社内イントラによる随時の教育

情報セキュリティ教育のフォローアップとして、社内イントラにて教材を公開し、社員がいつでも参照可能な状態とする。

▶情報セキュリティ教育の内容及び教材

全社を対象とした教育内容を以下の通り定めた。

(1) 情報セキュリティに関する一般的な啓発

(2) 情報セキュリティ基本方針・全社的な情報セキュリティ関連規程及び情報セキュリティに関するガイドラインの内容の説明等

教材については、情報セキュリティ対策室が原案を作成し、総務部が教材として整理した。

▶部門による情報セキュリティ教育・訓練の方針と教育内容

部門内の情報セキュリティ教育については、各部門が担当部署となり、教育計画の策定、教材の作成、教育・訓練の実施・記録を行うこととした。

(1) 情報セキュリティ教育・訓練の対象及び実施時期

関連する各部門にて業務を行う全スタッフに対し、着任時及び定期的に情報セキュリティ教育・訓練を実施する。

(2)教育・訓練内容

教育・訓練内容を以下とする。教育マニュアルは各部門で作成する。

①業務及び情報取り扱い時のルールに関する教育・訓練

②事業継続計画実施に関する教育・訓練

③情報セキュリティ事故対応に関する教育・訓練

(3)情報セキュリティ教育・訓練の計画及び記録

部門内の全スタッフに対する情報セキュリティ教育計画を作成し、実施する。実施時には教育受講者の記録を作成し、部門内の全スタッフが教育を受講したことを確認する。

▶データセンター事業部での情報セキュリティ教育・訓練の実施

(1)情報セキュリティ教育・訓練計画

今回ISMS適用範囲と定めたデータセンター事業部では、部門内情報セキュリティ教育・訓練のための教育・訓練計画を策定した。

(2)情報セキュリティ教育・訓練の実施

データセンター事業部の部門内情報セキュリティ教育・訓練は、計画に従って順次実施した。教育・訓練の結果は「教育・訓練出席者名簿」に記録した。全社的教育及び部門情報セキュリティ教育の効果について、「教育アンケート」により出席者からアンケートを収集し、改善を行った。「教育アンケート」は記録として規定の期間保存することとした。

表3.13にデータセンター事業部の教育・訓練計画を例示する。

表3.13　教育・訓練計画

No.	内容	ドキュメント	周期
1	情報システム運用技術教育・訓練	運用手順書	1回／年
2	情報セキュリティインシデント 発見時の訓練	情報セキュリティインシデント 管理ガイドライン	1回／年
3	障害・セキュリティ欠陥発見時の 教育・訓練	障害対応 手順書	1回／年
4	業務継続に関する教育・訓練 災害発生時の連絡 ハード・ソフト障害時の切り替え バックアップからのリストアップ	事業所業務 継続計画	各項目に関する周期は業務継続計画に従う

※新規スタッフへの教育は、着任時に行う

11 情報セキュリティ対策の運用及び記録

▶情報セキュリティ対策の実施

情報セキュリティのリスク評価結果により見直された情報セキュリティ基本方針、情報セキュリティに関する全社規程／情報セキュリティに関するガイドラインをもとに、データセンター事業部にて情報セキュリティ対策を実施した。

この段階における情報セキュリティ対策ベンチマークの診断結果は、日頃の情報セキュリティ対策の実施状況をチェックし、日々の改善に役立てる場合などに活用することができる。

▶情報セキュリティ対策に関する記録の収集とチェック

情報セキュリティ対策に関する記録について、定期的にチェックを行う。利用者アクセスの管理に関する記録の収集とチェックについて、**表3.14**に例示する。

表3.14　記録の収集とチェック

No.	記録	周期	管理者	記録チェックの観点	対応するドキュメント
1	施設の予約 及び訪問者の記録	1回／月	施設管理者	予約者と訪問者の一致 不必要と考えられる訪問	物理的アクセス管理ガイドライン 入退管理手順書
2	施設内のセキュリティドア等の利用記録	1回／月	施設管理者	入室と退室の整合性 過度に頻繁な入退室	物理的アクセス管理ガイドライン
3	IDカード配布台帳 IDカード貸出し記録	1回／月	施設管理者	貸出し期限を越えた貸出し	物理的アクセス管理ガイドライン
4	情報処理機器保守記録	1回／月	システム管理者	定期的な保守の実施 臨時保守の理由	運用手順書
5	保守時のID貸出し記録	1回／月	システム管理者	マシン保守記録との一致	運用手順書
6	情報処理関連設備保守・試験記録	1回／月	施設管理者	定期保守及び緊急保守	事業継続計画

▶情報セキュリティ対策の実施状況の把握

ISMS適用範囲内において適用している管理策の実施状況、要員に対する情報セキュリティ対策の周知度などを把握することとした。

たとえば、実際にはリスク対応計画（**表3.9**参照）により管理策を実施することになっていても、情報セキュリティ対策ベンチマークを用いた診断結果からは実施していないと読み取れる場合、その管理策について具体的に何が問題だったのかを判断し、改善に役立てることができる。

また、教育・訓練の実施の際に、適用しているはずの管理策を、個々のスタッフが実践していないことを発見できる場合がある。その場合、スタッフに対しては順守しなければいけない規定ルールはこれであると明示することで、情報セキュリティ対策の周知度を深めることができる。

12 内部監査または情報セキュリティ監査の実施

内部監査室の監査の一環として、内部監査または情報セキュリティ監査を実施する。監査は、最低でも年1回を原則として実施する。ドキュメントとして、「内部監査ガイドライン」または「情報セキュリティ監査ガイドライン」に詳細を記述する。「内部監査報告書」または「情報セキュリティ監査報告書」を記録として保存する。特に情報セキュリティに関する監査を重視している。

▶内部監査または情報セキュリティ監査

内部監査または情報セキュリティ監査は、内部監査室が監査計画を立案し、各部門の監査を行う。各部門が半年に1回以上の情報セキュリティ監査を受けるものとする。内部監査または情報セキュリティ監査は下記の内容とする。

(1)情報セキュリティ基本方針・情報セキュリティに関する全社規程及び情報セキュリティに関するガイドラインへの準拠に関する監査

(2)関連する法律、条例、業界ガイドライン、契約等への準拠に関する監査

(3)情報システムのセキュリティに関する技術的な監査（内部監査室の判断により、外部セキュリティ監査を実施している会社を利用できる。）

▶監査の報告とレビュー及び考察

(1)内部監査または情報セキュリティ監査結果の報告

監査報告書は、内部監査室長が作成し、社長、情報セキュリティ対策室長及び監査対象部門を統括する部長に報告する。

(2)監査結果によるレビュー

情報セキュリティ対策室は、情報セキュリティ対策室長の指示により、監査結果を参考にして現在の情報セキュリティ対策等をレビューする。

(3)監査結果の反映

情報セキュリティ対策室は、監査結果によるレビューを受け、情報セキュリティ対策についての指示を出す。実行については、各部門の責任者が実施する。

(4)監査の有効性に関する考察

内部監査というと一般的には被監査部門と独立した第三者による監査を意味する。したがって、内部監査室の要員がすべて他部門との兼務であれば、有効な内部監査が実施できる可能性は低いと思われる。

J社の現状では、内部監査室の要員のうち内部監査室長を含めすべてネットワーク運用管理部門、施設管理部門との兼務である。コスト削減のおり、内部監査室の専任者を要することは困難である。また、ネットワーク運用管理部門を監査するスキルを持っている要員が現在不足しており、やむを得ずネットワーク運用管理部門との兼務により実施している。要員不足は否めないが、監査の実施において有効性を確保するよう注意深く監視するとともに、独立した監査が可能な体制を早急に整えることとした。

▶監査員の教育訓練

情報セキュリティ教育・訓練ガイドラインでは、各部門で部門内の全スタッフに対する情報セキュリティ教育計画を作成し、実施することになっている。しかしながら、情報セキュリティ監査が始まったばかりであり、内部監査室では具体的な教育計画の作成がされていない。

また、実際の監査の教育も実施されていない。そこで、計画を作成し、早急に教育を実施し、効果の確認をすることとした。

13 マネジメントレビュー

経営陣は、組織の情報セキュリティマネジメントの導入および実施の最高責任者であり、その意味からも、組織の情報セキュリティマネジメントシステムが適切であり、有効に機能していることを確認する必要がある。また、確認の結果必要となった是正措置や改善を行わなければならない。

J社の社長及び役員は、情報セキュリティ基本方針及び情報セキュリティ目標を含むISMSの導入状況や改善の必要性について、監査報告書によりマネジメントレビューを行った。

また、導入した管理策がどの程度有効に機能しているかについては、導入前の情報セキュリティ対策ベンチマークの診断結果と、導入後の診断結果を比較し、管理策の有効性測定の一助として活用した。

2 ISMS認証取得

1 認証登録までの流れ

▶審査準備

J社では、ISMS認証取得のために追加の情報セキュリティ関連の設備投資は実施していないが、毎年の設備投資計画にデータセンターのセキュリティの強化を組み込んでいる。

審査登録機関（認証機関）は、J社からの見積依頼書を受理し、対象範囲のビジネスの内容、組織の規模等を考慮し、審査の工数の算定に基づく費用を見積書として提示した。

審査登録機関は、J社へ見積書を提出し、双方が同意のもと、認証契約を行った。

▶審査実施

審査登録機関は、審査員を決定し、審査チームを編成し、審査日程の調整を行った。

J社の審査実施にあたって、審査チームには審査をマネジメントするチームリーダーが配員された。さらに、十分な審査をするために審査チームが確保すべき専門性としては、データセンターの経営・運営に関する事項、施設、設備に関する要求事項、利用しているサーバ、ネットワーク等の技術的事項、適用される法規制等があげられた。

申請が受理され、審査登録機関との認証契約等の締結後、審査チームの編成や審査の日程等が調整された後、審査が開始される。

審査登録機関は、審査チームにデータセンターでの業務経験及び関連する業務に携わった経験のある審査員をアサインした。審査チームは、審査業務計画を作成し、審査を実施した。

▶審査登録

審査は、文書審査（ステージ1ともいう）と実地審査（ステージ2ともいう）の2段階で行われた。文書審査の目的は、組織のセキュリティ基本方針及び目標に照らして、当該ISMSを理解し、また当該審査に対する組織の準備状況を理解することにより、実地審査の計画に焦点を定めることにある。実地審査の目的は、組織が自ら定めた基本方針、目標、及び手順を順守していること、当該ISMSが認証基準又は規準文書のすべての要求事項に適合していること、並びに当該ISMSが組織の基本方針及び目標を実現しつつあることを確認することにある。

審査日数や審査工数は、ISMSの適用範囲、受審組織の規模、事業所数、リスクの程度、プロセスの複雑さなどによって異なってくる。また、申請から登録までの期間は、審査日数のほか、審査の不適合（注：不適合とは、マネジメントシステムが基準に適合していないか、システムが実行されていない場合である）の状況によっても異なってくるが、規模があまり大きくなく、特に問題が無い場合には3〜4ヶ月程度と思われる。

J社では、審査の結果、2007年に無事に認証を取得することができた。認証登録の情報は、審査登録機関から認定機関に報告されるが、報告時期により1ヶ月程度ずれる場合がある（**図3.6**参照）。認証登録は、初回審査から3年間有効となる。認証登録後、通常1年を超えないサイクルで維持審査（サーベイランス）が実施される。

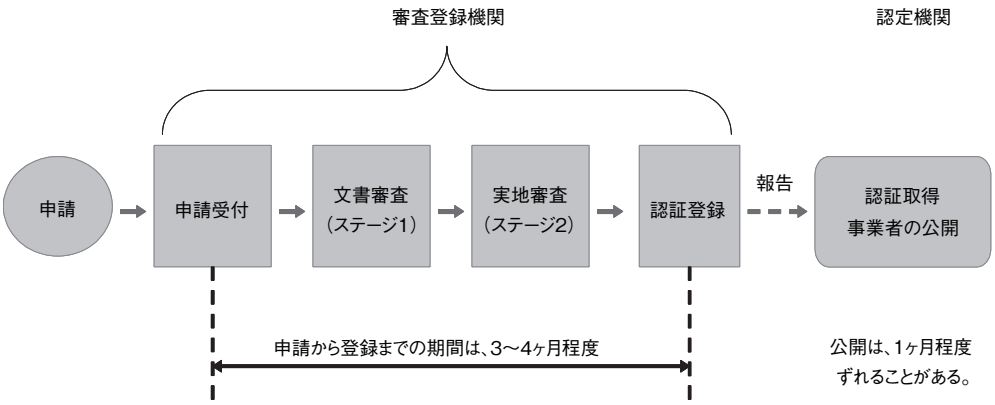


図3.6　審査登録の流れ

2 今後の課題

J社では、今回のISMS認証取得後に、情報セキュリティマネジメントの構築・導入・運用における今後の課題を、次の通り整理した。

(1) ISMS構築に際しての特別な設備投資は行っていない。ただし、情報セキュリティは日々変化していくため、将来に亘って現状のままで十分とは思っていない。リスク評価や事業継続管理といった面について、PDCAサイクルの中で順次向上させていく必要がある。

(2) トップダウンによる推進が重要である。ある程度作業が進んで、ISMS構築が自分達のためになることの理解が得られれば、その後は関係者が自ら進んで始めるようになる。こうしたステップをうまく進めるためには、具体的な推進組織体制が必要である。また、情報セキュリティは、経営の最重要事項であること、そのために経営資源を投入する必要があるとのメッセージを繰り返し発信する必要がある。

(3) ISMSの構築のポイントは、既存コンプライアンスの整理・活用、教育・啓発活動の推進、現場の仕事に合わせた手続き策定などである。教育については、社員・協力会社要員にはe-ラーニングを実行している。e-ラーニングはこれからも続けていくが、内容はISMSの重要なポイント（現場としてやるべきこと）のみに限定しており、ISMS基本方針全体を詳細に説明するための教育は、今後の課題として考えている。

(4) 従来は、データセンター業務の重要性をなかなか理解してもらえなかったが、ISMSを構築することで、情報セキュリティの重要性についての認識が広まり、その結果データセンター業務の重要性を理解してもらうことができた。データセンターのスタッフも業務自体に自信を持てるようになった。

(5) 規程・ルールを明確にすることで、個人の対策実施状況のバラツキを抑えることもできるようになった。今後は、ISMSの改善活動をどのように有効性の測定につなげていくかが課題である。

(6) 情報セキュリティマネジメントの運用においては、日常の活動に無理なく組み入れることで、現場の負担を少なくすることが肝要である。たとえば、現場の業務手順にISMSの手順を組込み、業務手順を参照することで自然にISMSが要求する手順を実施し、記録を残せるようにすることである。

(7) 今後は、ISO 9001等の既存のマネジメントシステムとの融合をいかに進めるかが課題である。

情報セキュリティ対策
ベンチマーク活用集

4章 情報セキュリティ対策ベンチマークから情報セキュリティ監査へ

■ 4章で紹介する4つの活用例

この章では、情報セキュリティ監査が用いられる実際のビジネスシーンを想定した、情報セキュリティ対策ベンチマークの活用例を4件示す。

1 助言型情報セキュリティ監査を活用し、よりよい情報セキュリティマネジメントの形成を進めた地方公共団体の例

情報セキュリティ対策ベンチマークを活用した自己評価を生かし、職員の意識改革等を果たした地方公共団体が、システムトラブルを契機として、市民に納得してもらえる情報セキュリティ水準を確保するために、本格的に専門家を活用して助言型の情報セキュリティ監査を受けることになった。助言型情報セキュリティ監査とは実際どのようなものなのだろうか。そして、その効果は？

2 政府機関統一基準に従い政府機関から受託業務を行う民間企業における保証型情報セキュリティ監査の利用例（被監査主体合意方式）

情報セキュリティ対策ベンチマークを活用した自己評価結果が良かったことからS社は、T独立行政法人から情報システム開発業務を受託することになった。受託に当たりS社は、政府機関統一基準に基づきT独立行政法人が定めた情報セキュリティ要求事項に従った対策を整備し、運用する必要がある。実際に業務を開始した後、その要求事項に適正に従っているかを監査することになった。この監査は被監査主体合意方式と呼ばれる保証型の情報セキュリティ監査であった。一体、被監査主体合意方式とはどのような監査なのだろうか？

3 情報セキュリティ対策が顧客の期待水準に達していることの保証を受けた民間企業の例（利用者合意方式）

情報セキュリティ対策ベンチマークを活用して比較的早期にISMS認証を取得したU社が事業拡大のために大手V社に販売活動をしたところ、利用者合意方式の保証型情報セキュリティ監査を受けるよう求められた。利用者合意方式とはどのような監査なのか。そしてU社の準備とは？

4 グループ企業の情報セキュリティ水準を向上させるために情報セキュリティ監査を利用するようになった例（利用者合意方式）

100社を超えるグループ会社を情報セキュリティ対策ベンチマークという共通の尺度で評価し、グループ全体の底上げを図ったX社が次に打った手は？

情報セキュリティ監査を上手に活用して、グループ企業の情報セキュリティ水準の底上げを行うにはどうしたら効果的か？

1　地方公共団体における助言型情報セキュリティ監査の利用例

1 情報セキュリティ対策ベンチマークの利用と効果

P市は人口10万人、地方の中核都市に隣接する小規模工業都市として栄えてきた。事業所数は5,000弱、うち約10％が工業事業所である。

P市では「地方公共団体における情報セキュリティポリシーに関するガイドライン（平成15年版）」を参照し、2004年度中に情報セキュリティポリシーの策定作業を行い、2005年4月より施行した。また、2005年には副市長が情報化推進担当責任者となり、情報政策課が情報セキュリティ対策に取り組むことになった。

しかし、情報政策課では、それまで主に業務システムの電算化を目的に業務を進めており、情報セキュリティに詳しい人材が少なかった。情報セキュリティポリシーの策定もガイドラインを常に参照しながら、専門家の手を借りずに策定した経緯がある。PDCAサイクルは一応回ったものの、Cの段階に不安が残っていた。

その一方、業務系の窓口業務システムにおいて、一昨年、昨年と続いてコンピュータシステムの不具合が見つかり、市民からの問い合わせが相次いだことから、本格的に情報セキュリティ対策の見直しを行うことになった。

昨年度までは、情報セキュリティ対策の予算が組まれていなかったため、まずは無料で実施でき、望ましい水準と、自組織の現状を比較できる情報セキュリティ対策ベンチマークを利用して市の現状を把握し、内部の資料としていた。情報セキュリティ対策ベンチマークの設問への答えを考える中で、情報政策課職員の中に情報セキュリティに関するより深い理解が得られたという者が数人出てきた。

2 助言型情報セキュリティ監査の利用へ

今年度は、昨年度の窓口業務システムの不具合をきっかけに、情報セキュリティ対策の取り組み状況を市議会に報告するよう副市長から指示が出た。このため、民間企業を想定した情報セキュリティ対策ベンチマークの自己診断結果だけでなく、専門家である第三者が評価した結果を提出する必要が生じた。

市民に分かりやすい形で評価結果を示す必要があるため、ISMS認証の取得も検討したが、現状では認証取得レベルにあるか判断できず、また、予算措置もなかった。そこで、当面ISMS認証取得を断念し、情報セキュリティ監査を受ける方向で検討することになった。

当初は、総務省の「地方公共団体における情報セキュリティ監査ガイドライン（平成15年版）」を参考に、内部監査の実施を検討したが、現在の体制ではすぐに内部監査を実施できる状況ではなかった。このため、専門家に助言型情報セキュリティ監査を委託し、あるべき姿と現状のギャップについての指摘を受けるとともに、改善の方向性について助言を得ることにした。

情報政策課では、今年度の監査対象を情報セキュリティポリシーの適切性の評価と昨年不具合の見つかった基幹システムとした。外部監査人の調達様式は、公募型プロポーザル方式（企画提案書を評価・判断して事業者を選定）とし、要求仕様を作成し公募したところ、数社より応募があった。

検討の結果、特定非営利活動法人日本セキュリティ監査協会（JASA）の公認情報セキュリティ監査人（CAIS）資格を保有し、また地方公共団体セキュリティ対策支援フォーラム（LSフォーラム）の主催する自治体業務知識研修を終了した監査人が所属するR社に助言型監査を依頼することにした。監査技量とともに自治体特有の業務知識があり、さらに監査の品質に万一問題があった場合は、申し立てにより、JASAの審査委員会で紛争審査が行われることから、非常に信頼性の高い監査が実施できると考えたためである。

R社の監査人との契約締結にあたっては、改めて以下の項目を確認した。

＜監査内容＞

- 監査の目的、対象、範囲
- 準拠する基準
- 監査のポイント

＜監査人の権限＞

- 監査人の権限
- 注意義務
- 倫理
- 監査人の責任
- 機密保持
- 監査結果の管理方法

＜監査スケジュール＞

- 監査実施期間
- 事前打合せの時期と回数
- 監査計画書作成
- 予備調査
- 本調査
- 監査報告書作成
- 監査報告会

＜監査実施体制＞

- 監査責任者、監査人、アドバイザを含む監査体制
- P市情報政策課との役割分担

＜成果物＞

- 納入物一覧

特に報告会については、情報政策課への報告会のほか、市長への報告会を追加した。確認の結果は非常に納得のいくものであったため、正式にR社と契約を締結した。契約に際しては、R社の監査チーム全員に守秘義務契約を課し、また監査結果の管理方法についても明示した。

3 監査の実施とその成果

契約に際してR社との間で充分な確認をしたため、監査自体は非常にスムーズに行われた。

特に予備調査では、総務省の地方公共団体情報セキュリティ管理基準をもとにR社が作成したアンケートを使用した。R社では、同じ管理基準について、「情報システム管理担当者用」と「窓口職員（システム

オペレータ）用」の二通りのアンケートを使用し、システムに詳しくない現場の職員にも分かりやすい形になっていた。また、R社の提案に従い、監査手続き開始に先立って、監査を受ける側の部署の職員に「説明会」を開いた。その結果、「情報セキュリティとは何か」「何のために情報セキュリティ監査を行うのか」について、職員の理解が得られ、その後のアンケート、ヒアリングがスムーズに実施できるようになった。

情報セキュリティ監査の結果は、下記の報告書にまとめられ、情報政策課での報告会のほか、市長への報告とも非常に分かりやすく、満足のいくものであった。

発行日　：200X年XX月XX日
報告書No.：XXXXXXXXXXX

P市市長　○○　○○　殿

発行責任者：R株式会社　代表取締役社長
○○　○○　印
審査者　：R株式会社 セキュリティ事業部
上席スタッフ
○○　○○　印
作成者　：R株式会社　監査チームリーダー
○○　○○　印

情報セキュリティ監査報告書

「地方公共団体情報セキュリティ管理基準」に照らして、200X年XX月XX日から200X年XX月XX日における貴市の情報セキュリティ活動の実施状況について監査を実施いたしました。

当監査は、「地方公共団体情報セキュリティ管理基準」及び監査依頼者・監査実施者双方で同意した「情報セキュリティ管理基準」の一部項目（別紙1参照）に基づいて監査を行い、情報セキュリティに関わるリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づいて適切なコントロールが採用されているか否かを確かめ、さらに成熟度モデルを活用して、問題点を検出し提示するという観点から実施いたしました。

監査の結果、以下の検出事項とその改善提言を報告いたします。

当監査報告書は内部利用を目的として作成したものであるとともに、監査依頼者と、監査実施者または監査人との間には、記載すべき利害関係はありません。

― 記 ―

Ⅰ. 監査の概要

1. 個別管理基準の作成

「地方公共団体情報セキュリティ管理基準」の中から、個人情報保護と密接な関係があるコントロール項目に基づき、貴市の監査を実施した。

なお、上記コントロール項目については、貴市よりご提示の17項目の他、さらに当監査チームが重要と判断した20項目を追加し、貴市固有の個別管理基準を作成した。

情報セキュリティ管理 における各領域	貴市よりご提示の コントロール項目数	監査チームが追加した コントロール項目数	合計
セキュリティ基本方針	1 項目	1 項目	2 項目
組織のセキュリティ	―	1 項目	1 項目
資産の分類及び管理	2 項目	―	2 項目
人的セキュリティ	3 項目	1 項目	4 項目
物理的環境的セキュリティ	4 項目	4 項目	8 項目
通信及び運用管理	6 項目	1 項目	7 項目
アクセス管理	―	10 項目	10 項目
システムの開発及び保守	―	1 項目	1 項目
事業継続管理	―	1 項目	1 項目
適合性（コンプライアンス）	1 項目	―	1 項目
合計	17 項目	20 項目	37 項目

2. 成熟度モデルの適用

上記1.で作成した個別管理基準に基づき監査を実施するにあたり、COBIT 4.1の成熟度モデルを適用した。成熟度は、すべての項目共通とし、以下の6段階により評価を行った上で、成熟度レベル「3」に基づく監査意見を述べている。

成熟度	レベル
5	最適化されている
4	管理され、測定が可能である
3	定められたプロセスがある
2	再現性はあるが直観的
1	初期／その場対応
0	実施していない

3. 監査実施期間

200X年XX月XX日からXX月XX日

4. 監査体制

(1)監査チーム

監査人氏名	役　割	所持資格
○○　○○	監査チームリーダー	公認情報セキュリティ主任監査人
○○　○○	監査チームメンバー	公認情報セキュリティ主任監査人
○○　○○	監査チームメンバー	公認情報セキュリティ監査人
○○　○○	監査チームメンバー	公認情報セキュリティ監査人

(2)監査品質管理体制

監査チームから独立した品質管理者を以下の通り設けた。

氏　名	所属・役職	所持資格
○○　○○	セキュリティ事業部 上席スタッフ	公認情報セキュリティ主任監査人

Ⅱ. **監査意見**

200X年XX月XX日から200X年XX月XX日までの期間に係るXXXを対象とした情報セキュリティ対策の実施状況は、監査手続きを実施した範囲内において以下に記載する検出事項が「情報セキュリティ管理基準」に照らして不適切であると判断される。

Ⅲ. **検出事項**

領域（部署名）	項目（コントロール及び サブコントロール）	検出された個別事象
・・・・・	・・・・・・・・・	・・・・・・・

Ⅳ. **改善提言**

緊急改善事項	領域：○○○ 項目：・・・・・・・・ 提言内容：・・・・・・・・・
	領域： 項目： 提言内容：
通常改善事項	領域： 項目： 提言内容：
	領域： 項目： 提言内容：

※「緊急改善事項」、「通常改善事項」の区分は、監査チームの判断による。

Ⅴ. **特記事項**

・・・・・・・・・・・

以上

ただし、報告書の市民への公開については、P市のぜい弱性を公開することにもつながるので、市の広報誌及びWebサイトにて、下記のように公開するにとどめた。

P市の情報セキュリティ対策実施状況について

200X年XX月XX日
P市市長　○○　○○

「情報セキュリティ管理基準」に照らして、200X年XX月XX日から200X年XX月XX日における情報セキュリティ活動の実施状況について監査を実施いたしました。

当監査は、「地方公共団体情報セキュリティ監査基準」及び監査依頼者・監査実施者双方で同意した「情報セキュリティ管理基準」の一部項目（別紙1参照）に基づいて監査を行い、情報セキュリティに関わるリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づいて適切なコントロールが採用されているか否かを確かめ、さらに成熟度モデルを活用して、問題点を検出し提示するという観点から実施いたしました。

監査人の選定に当たっては公募型プロポーザル方式とし、応募社の提案を検討の結果、R社と決定し、契約を結びました。

監査の結果、R社より○件の検出事項とその改善提言が報告されました。改善提言中、△件につき改善対策実施済み、▽件について対策を実施する予定です。

当監査報告書は内部利用を目的として作成したものであるとともに、監査依頼者と、監査実施者または監査人との間には、記載すべき利害関係はありません。

助言型情報セキュリティ監査を実施したことで、情報政策課の職員に情報セキュリティ監査のノウハウが蓄積されたばかりでなく、監査を受けた職員の間にも情報セキュリティに対する意識が浸透したことが最も大きな収穫であった。

これを機に、全システムに対し、内部監査を2年に1度、外部監査を3年に1度実施するサイクルを構築し、運営していくことが市議会において承認された。

2 政府機関統一基準に基づく被監査主体合意方式の保証型情報セキュリティ監査の利用例

1 情報セキュリティ対策ベンチマークの利用と効果

S社はT独立行政法人から、情報検索システムの運用を受託している。海外からの利用も想定し、運用は24時間体制で、障害の緊急対応などを含むフルアウトソーシングの形態である。

このシステムはWebサイトによりT独立行政法人が保有する知識データベースを検索するシステムである。個人情報等の機密性の高い情報を取り扱うことはないが、知識データベースへのアクセスを行わせることは、T独立行政法人にとって情報セキュリティ上のリスクになる。また、利用者にとり、自身の検索行動について第三者が知りうることは好ましくない。これらのことから、機密性・完全性の要素において、高い水準の情報セキュリティ対策を必要としている。また海外からの利用のため、24時間安定稼働が必要であり、可用性についても配慮が求められる。

T独立行政法人は、情報検索システムの運用を外部委託するに当たり、運用委託業者選定委員会を中

立的な委員により組織し、選定作業を行うこととした。運用委託業者選定委員会は、内閣官房情報セキュリティセンター(NISC)が公表した「外部委託における情報セキュリティ対策実施規定」を参考に、情報セキュリティ対策ベンチマークの結果を指標として、委託先候補の情報セキュリティ対策の遂行能力と取り組み状況を評価した。

その結果、運用委託業者選定委員会では、情報セキュリティ対策ベンチマークの結果で多くの項目で望ましい水準にあり、同業グループ内でも高い結果を示し、かつ提案書の内容が優れていたS社を情報検索システムの運用業務の委託先の第一候補とすべきとの結論を得た。

2 保証型情報セキュリティ監査の利用へ

T独立行政法人の情報セキュリティ責任者はさらに、S社の情報セキュリティ対策の履行状況を確認するために、定期的に自己点検の結果を報告するとともに、S社において実施すべき情報セキュリティ管理手続と情報セキュリティ監査の実施を要求した。具体的には、調達仕様書の中で、調達条件として次の項目を記述した。

(1) 定期的な自己点検の結果報告。
(2) 外部委託する情報検索システムの運用において、実施すべき情報セキュリティ管理手続き。
(3) 年1回の被監査主体合意方式による保証型情報セキュリティ監査の実施及び監査結果の報告。

S社は、T独立行政法人が提示する情報検索システム運用外部委託仕様書に対し、具体的な情報セキュリティ対策をとりまとめ、T独立行政法人に提案した。

(1) 自己点検の報告は、情報セキュリティ対策ベンチマークの結果を定期的に報告する。
(2) 管理手続きは、S社が現状で実施している情報セキュリティ管理手続きをそのまま実施する。
(3) 被監査主体合意方式の保証型情報セキュリティ監査については、情報セキュリティ監査企業台帳に登録されており、JASAの会員企業でもあるY監査会社に依頼する。

T独立行政法人は、S社からの提案内容を高く評価し、S社を外部委託企業として採択した。T独立行政法人とS社は、情報検索システム運用外部委託に関する条件を詰め、合意内容に基づき外部委託契約を締結した。

委託契約にもとづき、S社は毎年1回、次の流れにより被監査主体合意方式の保証型情報セキュリティ監査を実施することとなった。

3 監査手続の合意

被監査主体合意方式の保証型情報セキュリティ監査の流れは、下記のとおりである。

(1) S社は、提案書で提示したY監査会社と監査契約を締結する。
(2) S社とY監査会社は、合議により、監査テーマ及び監査手続を決定し合意する。
(3) S社は、(2)でY監査会社と合意した監査テーマ及び監査手続の内容を、T独立行政法人に報告し、T独立行政法人の確認をとる。
(4) Y監査会社は、(2)でS社と合意した監査テーマ及び監査手続に従い、S社に対する監査を実施し、監査報告書をS社に提出する。
(5) S社は、Y監査会社から提出された監査報告書を、T独立行政法人に提出する。

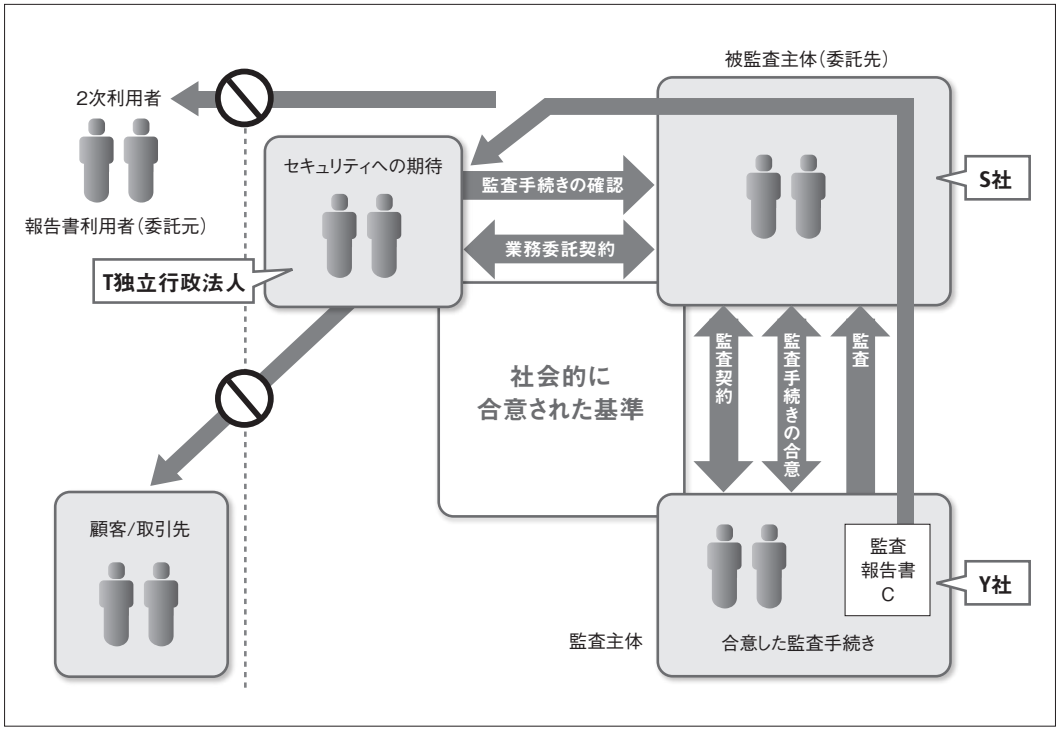


図4.1　被監査主体合意方式の保証型監査

S社とY監査会社とは、初年度の情報セキュリティ監査の実施における監査テーマを次の3領域とすることで合意した。

(1) 物理的及び環境的セキュリティ
(2) 通信及び運用管理
(3) 情報セキュリティインシデント管理

また、これら3領域において対象とする情報セキュリティ管理手続きとその監査手続きについては、次頁 **表4.1**の内容で合意した。

S社は、Y監査会社とのこれら合意内容について、T独立行政法人の確認を得た。

表4.1　合意した情報セキュリティ監査手続き

監査領域	情報セキュリティ管理手続	情報セキュリティ監査手続
物理的及び環境的セキュリティ	セキュリティを保つべき領域が許可されたものだけにアクセスを許すことを確実にするための、適切な入退管理策により保護されていること。	【閲覧】入退室管理規定、入退室手順が確立されているかを確認する。 【再実施】正しい入退室方法、不正な入退室方法の両方を試す。
	装置の可用性及び完全性を継続的に維持するための作業が実施されていること。	【閲覧】定期的な保守作業が正しく行われているか、事故発生時の対応が正しく行われているかを、保守作業記録を閲覧して確認する。
	・ ・	・ ・
通信及び運用管理	悪意のあるコードから保護するために検出、予防及び回復のための管理策が実施されていること。	【閲覧】ウイルス対応手順などを閲覧し、悪意のあるコードから情報資産を保護するために、検出、予防及び回復のための管理策が実施されているかを確認する。
	情報及びソフトウェアのバックアップが合意されたバックアップ方針に従って定期的に取得されていること。	【閲覧】バックアップ方針及びバックアップ記録等を閲覧し、情報及びソフトウェアのバックアップが合意されたバックアップ方針に従って定期的に取得されていることを確認する。
	監視活動の結果が定めに従ってレビューされていること。	【閲覧】ログ解析結果等を閲覧し、監視活動の結果が定めに従ってレビューされていることを確認する。
	・ ・	・ ・
情報セキュリティインシデント管理	情報セキュリティインシデントに対する責任体制及び手順が確立されていること。	【閲覧】情報セキュリティ関連規程を閲覧し、情報セキュリティインシデントに対する責任体制及び手順が確立されていることを確認する。
	情報セキュリティインシデントの発生に対して、規模及び費用を定量化し監視できるようにする仕組みが備えられていること。	【閲覧】情報セキュリティインシデントの記録を閲覧し、規模及び費用を定量化し監視できるようにする仕組みが備えられていることを確認する。
	・ ・	・ ・

4 監査の実施とその成果

Y監査会社は、3において示したS社と合意した監査テーマ及び監査手続きにより、S社に対する被監査主体合意方式の保証型情報セキュリティ監査を実施し、次の監査結果報告書をS社に提出した。

平成19年○○月○○日

S株式会社
代表者　○○　○○　殿

Y監査会社
代表者　○○　○○　印

情報セキュリティ監査結果報告書

当社は、T独立行政法人殿が貴社に運用を委託している情報検索システム運用業務の情報セキュリティ対策の順守状況を確かめることを目的として、貴社が、T独立行政法人殿と貴社の経営者との間で定めた情報セキュリティに係る管理手続（以下「情報セキュリティ管理手続」という。）を平成×年×月×日から平成×年×月×日までの期間において履行していることを確認するために、「被監査主体合意方式」による保証型情報セキュリティ監査を実施した。

情報セキュリティ管理手続は、T独立行政法人殿から平成○年○月○日に要求された情報セキュリティ管理基準に基づいて貴社がその対策を記載した管理手続であり、平成×年×月×日から平成×年×月×日までの期間において、情報検索システム運用業務に対してこの情報セキュリティ管理手続が実施されていることの責任は、貴社の経営者にある。また、貴社の情報セキュリティ管理手続の十分性については、貴社及び貴社がT独立行政法人殿から得た確認に従ったものであり、本書に掲載されていない情報セキュリティ管理手続については、今回の情報セキュリティ監査の範囲には含まれていない。

当社は、「情報セキュリティ監査基準」に準拠して、下記に掲載した貴社と合意した情報セキュリティ監査手続を実施した。この情報セキュリティ監査手続を実施した結果は下記の通りである。ただし、当社が実施した情報セキュリティ監査手続は、貴社及び当社との間で合意し、T独立行政法人殿の確認を得た情報セキュリティ監査手続に限定して監査手続を実施している。

（確認した情報セキュリティ監査手続とその結果は、ここ又は別紙に記載する。）

なお、この報告書は、T独立行政法人殿のための情報利用を意図したものであり、T独立行政法人殿及び貴社以外の第三者の利用を意図したものでなく、また、他の第三者にこの報告書を利用させてはならない。

以上

— 別　紙 —

確認した情報セキュリティ監査手続とその結果

監査領域	情報セキュリティ管理手続	情報セキュリティ監査手続	結果	発見事項
物理的及び環境的セキュリティ	セキュリティを保つべき領域が許可されたものだけにアクセスを許すことを確実にするための、適切な入退管理策により保護されていること。	【閲覧】入退室管理規定、入退室手順が確立されているかを確認する。 【再実施】正しい入退室方法、不正な入退室方法の両方を試す。	○ 実施していると認められる	－
	装置の可用性及び完全性を継続的に維持するための作業が実施されていること。	【閲覧】定期的な保守作業が正しく行われているか、事故発生時の対応が正しく行われているかを、保守作業記録を閲覧して確認する。	○ 実施していると認められる	－
	・ ・	・ ・		
通信及び運用管理	悪意のあるコードから保護するために検出、予防及び回復のための管理策が実施されていること。	【閲覧】ウイルス対応手順などを閲覧し、悪意のあるコードから情報資産を保護するために、検出、予防及び回復のための管理策が実施されているかを確認する。	○ 実施していると認められる	－
	情報及びソフトウェアのバックアップが合意されたバックアップ方針に従って定期的に取得されていること。	【閲覧】バックアップ方針及びバックアップ記録等を閲覧し、情報及びソフトウェアのバックアップが合意されたバックアップ方針に従って定期的に取得されていることを確認する。	○ 実施していると認められる	－
	監視活動の結果が定めに従ってレビューされていること。	【閲覧】ログ解析結果等を閲覧し、監視活動の結果が定めに従ってレビューされていることを確認する。	○ 実施していると認められる	－
	・ ・	・ ・		
情報セキュリティインシデント管理	情報セキュリティインシデントに対する責任体制及び手順が確立されていること。	【閲覧】情報セキュリティ関連規程を閲覧し、情報セキュリティインシデントに対する責任体制及び手順が確立されていることを確認する。	○ 実施していると認められる	－
	情報セキュリティインシデントの発生に対して、規模及び費用を定量化し監視できるようにする仕組みが備えられていること。	【閲覧】情報セキュリティインシデントの記録を閲覧し、規模及び費用を定量化し監視できるようにする仕組みが備えられていることを確認する。	○ 実施していると認められる	－
	・ ・	・ ・		

S社はこの報告書をT独立行政法人に提出し、T独立行政法人は、Y監査会社がS社に対して行った情報セキュリティ監査によって、S社の情報セキュリティ対策が、T独立行政法人の要求するセキュリティ事項を満たしていることを確認した。

3 一般企業における利用者合意方式の保証型情報セキュリティ監査の利用例

1 情報セキュリティ対策ベンチマーク利用とISMSの取得

U社は、Webシステムを用いた顧客管理を行うアプリケーション提供サービスを行う企業である。従業員総数は60人と小さいが、系列のデータセンターを利用して、堅実なサービスを提供し、徐々に大口の顧客を獲得しつつあった。

情報セキュリティサービスが付加価値サービスであり、ネットワークやサーバに対するセキュリティの設定と監視を顧客に提供している。セキュリティを独学で学んだ部長が、独自のセキュリティポリシーを作成し、それに基づき情報セキュリティ対策を施していた。

近年、同業他社がISMS認証の取得等を通じて、情報セキュリティの優位性をアピールしている。これに対抗するために、社長からISMS認証の取得を行えないかとの打診があった。ただ、社長の要求は厳しく、残された期間は半年に満たないものであった。

既にポリシーを作成し、運用しているので、ISMS認証の取得も無理ではないと考えた専務は、この少ない期間でISMS認証の取得が可能かを検討するように部長に指示した。部長は独自の情報セキュリティ対策でISMS認証取得が可能であるかを確認するために、情報セキュリティ対策ベンチマークを利用することとした。

情報セキュリティ対策ベンチマークの結果は、上位21%から30%の範囲であり、かなりの項目で望ましい水準にあった。一方、情報資産の取り扱いやシステムの障害対策などいくつかの項目で、望ましい水準に達していないことが判明した。これらの弱点についての対策の大部分は、現在行っている管理策の徹底などで対応できるものがほとんどだったことから、短期でISMS認証の取得が可能との見通しが立った。

ISMS認証の取得は、当初思ったよりは苦労した。また、審査のタイミングがあわず、多少、時間を要したが、半年あまりで認証を取得した。

2 保証型情報セキュリティ監査の利用へ

ISMS認証の取得が功を奏したのか、その後、優良顧客に恵まれ、U社の業績は順調に伸びていった。U社は更なる業容拡大のため、インターネット・キャッシングを開始しようとしている大手金融機関のV社に営業を行った。V社のインターネット・キャッシングは、24時間365日サービスを行うものである。キャッシングというサービスのため、顧客の機微情報も取り扱う。このため、機密性・可用性のいずれの要素においても高い水準のセキュリティを必要とする。

U社は営業資料等に、最大停止時間15分以内のサービスレベルとISMSの認証取得を掲載している。V社は、U社のISMS認証取得は評価したものの、U社に対し、自社の情報に対するセキュリティ面での十分な対策を施し、さらにその内容が着実に行われていることを客観的に証明するよう求めた。そこでU社は、V社と秘密保持契約を締結した上で、自社が実施している情報セキュリティマネジメントシステムの詳細管理策を開示し、その実施を外部機関による情報セキュリティ監査で客観的に評価して貰うことで対応することを提案した。

V社がこの提案を受諾したため、約1ヶ月で詳細管理策を提示し、その後、3ヶ月以内に監査報告書を提出することとなった。

3 言明書の作成

U社は、V社と相談し、情報セキュリティ監査企業台帳に登録されており、JASAの会員企業でもあるZ監査会社に依頼することを決定した。

U社で行なわれる保証型情報セキュリティ監査は、利用者合意方式と呼ばれるものである。この方式では、最初に、U社がV社の情報セキュリティ上の期待水準に基づき、実施する情報セキュリティ管理手続を言明書として取りまとめ、V社に提示する。

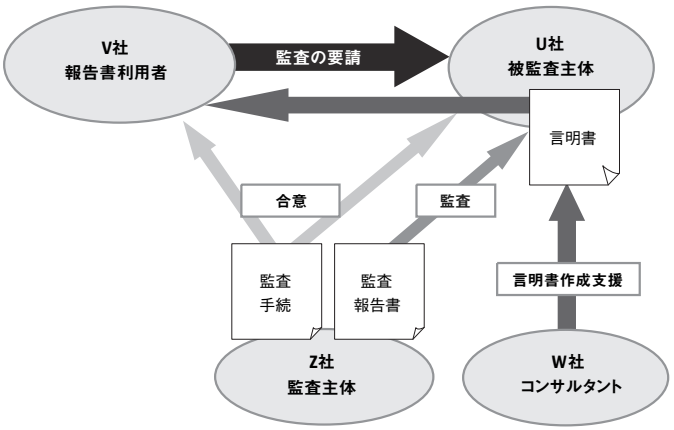


図4.2　保証型監査の主体間の関係（利用者合意方式）

V社がその内容で自らの期待する情報セキュリティが確保できると判断すると、この言明書が適正であるか否かについて、監査主体であるZ監査会社が情報セキュリティ監査の結果に基づき意見を述べる。Z監査会社が行う監査手続で、V社が期待する保証に足る監査ができるかについては、報告書利用者であるV社とZ監査会社が事前に合意する必要がある。

情報セキュリティ監査に先立ってZ監査会社は、U社の状況を聞き取った。その結果、以下の点をU社に伝えた。

(1) ISMS認証取得の全ての分野にわたった詳細管理策を監査するには、時間的にも費用的にも膨大になること。

(2) U社がISMS認証を取得しており、基本的なマネジメントシステムはできていることから、リスクの大きい分野に絞った情報セキュリティ監査であれば比較的安価な費用で行えること。

U社はISMS認証取得に用いたリスク分析を再検討したが、すべて許容リスク以下のため、対象を絞ることができなかった。そこで、コンサルタントのW社に助言を求めた。

W社がU社の業務フローとデータフローを把握し、統制上のクリティカルポイントを分析した結果、顧客○○情報データベースに、最も多様な人々がアクセスし、作業に用いていることが明らかになった。U社の情報セキュリティ設計もそれを意識しており、多重のシステム的な防御策をとっているが、それでもなお人的要因を排除できず、そのことが最も大きなリスクであると判断された。

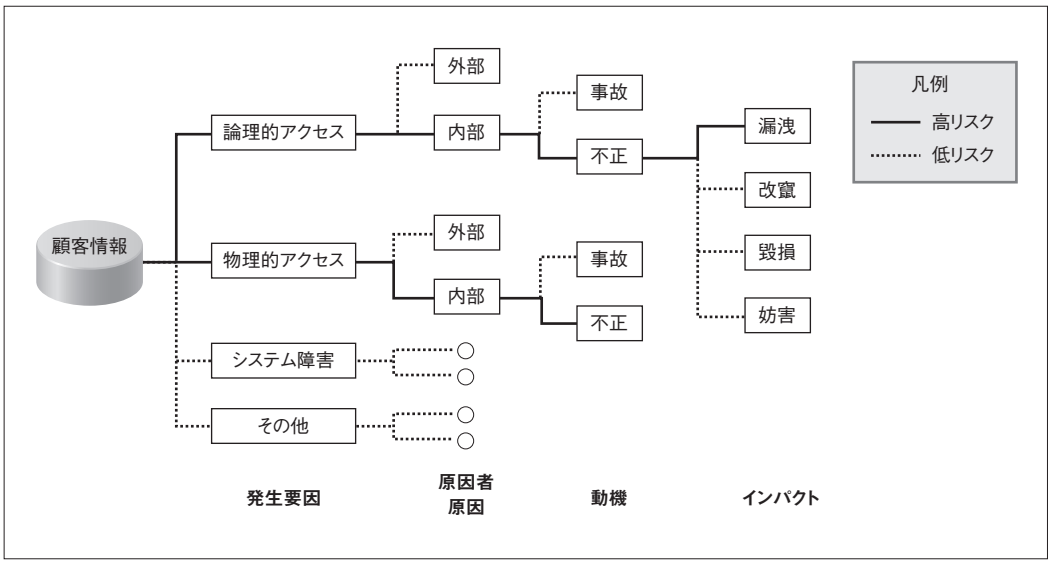


図4.3　リスク分析のイメージ

W社は、分析結果に基づき、アクセス制御の管理に焦点を当てるべきであるとU社のトップに提言した。

提言を受け、U社はアクセス制御に関わる管理手続きについて言明書を作成し、V社に提示した。言明書は、以下のとおりである。

20XX年MM月DD日

V株式会社　殿

顧客の情報を取扱う業務の情報セキュリティマネジメントに関する言明

U株式会社
代表取締役社長　○○　○○

1. 当社は、200X年XX月XX日にV株式会社殿から以下の要求を受けました。
   当社が提供する＊＊＊＊サービス（以下、対象業務）では、V株式会社殿から委託された情報（顧客の情報）を確実に管理すること。
2. 当社は、リスクアセスメントの結果、前項の要求を実現するに足る管理策を下記の範囲で整備し、運用しています。

当社の対象業務を担当する部門は、公的な基準に基づく情報セキュリティマネジメントシステムを運用しています。

Ⅰ　対象範囲及びリスク管理方針	
1. 対象範囲	① 対象業務に係る＊＊システムと、当該システムの運用部門、＊＊センター、当該センターに入室する全ての人（システムの利用者、関係する社員及び部外者など）を対象とする。 ② 【参照資料】 ③ 対象システム範囲：付属資料1に図面で表示。 ④ ＊＊センター詳細：付属資料2に図面で表示。
2. リスク	① 対象業務に係る各プロセスのリスクを評価した結果、顧客＊＊データベースに係る不正アクセスリスクが非常に大きい。 ② 対象業務においては、事業継続上顧客の信頼が不可欠であり、信頼維持のために、顧客の情報の機密性確保が最も重要である。 ③ 機密性確保を問われる顧客の情報の中では、顧客から受託する顧客＊＊情報の価値が最も高い。これを処理する＊＊管理システムの機密性に関するリスクが最大である。 ④ ＊＊管理システムの中についてみると、ネットワーク上を流れる部分的な顧客＊＊情報よりは、データベースに蓄積された顧客＊＊情報全体の機密性に関するリスクが大きい。 ⑤ 顧客＊＊データベースの機密性確保の観点においては、技術的（システムぜい弱性リスク・システム運用リスク等）・物理的セキュリティリスクに比較して、不正アクセスリスクが非常に大きい。
3. リスク管理方針	当社は、下記の方針で重要な情報資産を管理している。 ① 従業員等による不正を防止するため厳格なアクセス管理策を講じる。 ② アクセス管理策は、合理的な範囲で行う。 1 ＊＊システムに過大な負荷をかけない範囲で実装する。 2 ライセンス契約に抵触するシステム改変は行わない。 3 アクセス管理サービス価格に影響を与えない範囲で行う。
Ⅱ　管理策	
(1) 9.1.2* 物理的入退管理策	① ＊＊センターへの入退室は、以下の方針で行っている。 ② センター入り口には、許可された者のみが入退室できるよう、ビデオ監視装置つきの導入路を設け、その導入路の前後に扉を設置し、制御している。 ③ 業務に従事する者すべてに、顔写真入りのIDカードを配布し、入室時には常に着装させている。なお、入館証はICカードとし、入退室及び機器へのアクセス管理の認証のためにも利用している。 ④ センターの扉はICカード及び指紋認証装置により制御し、許可された者以外の入室を阻止している。なお、指紋認証装置の読取不全の時は、パスワードでの認証を併用している。 ⑤ 室内での工事等により役員・社員等以外の者が立ち入る必要がある場合には、事前に情報セキュリティ管理者に届け出し、許可を受けさせている。許可をした場合には、臨時のIDカードを貸与した上で、２名以上の社員が常時付き添い作業に従事させている。なお、臨時のIDカードは毎日回収している。 ⑥ ビデオ監視及び入退室のログを記録し、3年間安全に保存している。
(2) 10.1.3* 職務の分割	① 対象業務に関わる区画及び重要情報資産へのアクセス権限は、職務及び責任範囲を明確にした職務定義書に基づき設定している。 ② 職務定義においては、一人が複数の権限を保有しないよう、・・・の作業を分離するよう設定している。 ③ 各職務について、・・・、各々に対するアクセス権限の内容を明確にする。また、緊急の必要により、・・・場合の管理策をあらかじめ定め、これに基づき作業を行っている。 ④ 全ての役員・社員等には、・・・権限以外のアクセスを禁止している。 ⑤ ・・・組織・人事の異動の際にも権限の重複がないようにしている。 ⑥ 情報セキュリティ管理責任者が・・・年1回定期的に見直している。
・ ・	・・・ ・・・

＊ 9.1.2、10.1.3は、情報セキュリティ管理基準などの番号である。

4 監査手続の合意

Z監査会社は、U社が提示した言明書をもとに、監査手続きの検討に入った。監査手続は、設計監査と実装監査の2つに分けられる。

設計監査では、対象業務に関するリスクの把握が適正に行われ、言明書に必要十分な管理策が組織的に検討されていることを確認する。

実装監査では、言明書の管理策が言明書どおりに実施されていることを確認する。監査手続きを策定するに当たって、情報資産の重要度や監査リスク（ルールと実態が乖離しやすい）などを考慮し以下の4つに類別した。その結果をもとに監査規模の見積りなどを行い、必要十分な監査手続をとれるようにした。

類別	概要	具体的な例
L (Logical)	ルール（基準や運用手順、システム仕様書など）の存在を閲覧などにより確認する。	・パスワード管理システムの仕様確認。 ・モバイルコンピュータの設定ルール確認。
G (Governance)	ルールが周知徹底されているかを、部分的なエビデンスの閲覧や質問などにより検証する。	・アクセス管理方針の運用状況などを質問により確認。 ・教育の受講記録を確認。
D (Document)	ルール通りに運用されているかを、記録の閲覧や質問・視察などにより整合性を検証する。	・ID削除依頼書とサーバのID設定内容及びID削除の実行に関係するログとの整合性確認。 ・送付者と受け取り者のドキュメントの整合性確認。
P (Physical)	ルールに基づいて保存されている記録の信憑性を、閲覧・質問・視察や再実施により検証する。	・2人同時に入室していないかなど物理的な入退室の状況を目視確認。 ・入退室ログと勤務実態があっているかなど入退室ログと実地の目視確認。 ・実物の運用状況の目視確認。

以上の検討結果に基づき、Z監査会社は以下に示す監査手続きをU社及びV社に提示した。

V社はこの監査手続により、監査で十分な成果が得られると判断し、監査手続きについて合意した。

監査手続（平成○○年○月○日作成）　Z監査会社

U株式会社　情報セキュリティ監査チームリーダ
××　××

【設計監査】管理策の必要性・十分性	
言明書作成の 正当性	【質問】言明書作成の目的、言明の根拠に関し、経営者に質問を行い、明確な根拠があることを確認する。 また、言明書の作成に関わった社内の責任者・担当者、及び外部委託先（コンサルティング会社W社）責任者及び担当者に質問し、経営者の質問と整合性があることを確認する。 【閲覧】言明の根拠となる、言明書作成の経緯を記録した文書を閲覧し、経営者の回答と整合性が取れていることを確認する。 文書としては、以下のものを対象とする。 ・言明書作成に関わる会議の記録（情報セキュリティ委員会議事録、経営会議議事録、その他打合せ記録等）。 ・言明書作成の資料として用いたW社のコンサルティングの結果報告書。 ・ISMSなど公的な認証取得の文書を閲覧し、経営者が情報セキュリティマネジメントを的確に運用していることを確認する。

リスク把握の適切さ	【閲覧】対象業務フローに係るリスク分析を確認し、リスクが漏れなく、的確に洗い出されていることを確認する。 【視察】業務の現場を確認し、リスク分析で記述された脅威・ぜい弱性が十分であることを確認する。 【質問】業務現場の担当者に質問し、リスク分析が的確であることを確認する。 【質問】経営者にリスクに関して質問し、リスクが正しく認識されていることを確認する。 【質問】言明書の作成に関わった社内の責任者・担当者、及び外部委託先（コンサルティング会社W社）責任者及び担当者に質問し、経営者の質問と整合性があることを確認する。
管理策の適切さ	【閲覧】情報セキュリティ管理基準を参照して作成した個別管理基準に照らして、リスク分析によって洗い出されたリスクに対し、言明書において必要な管理策が網羅されていることを確認する。 【質問】経営者に管理策の内容を質問し、管理策として行うべきことが的確に記述されていることを確認する。 【質問】言明書の作成に関わった社内の責任者・担当者、及び外部委託先（コンサルティング会社W社）責任者及び担当者に質問し、経営者の質問と整合性があることを確認する。
【実装監査】　言明書どおりに運用が行われていることの確認	
言明書の運用の確認	【質問】経営者と業務管理責任者に質問し、言明書に基づく管理を実施していることを確認する。 【閲覧】言明書どおりに管理策が組織全体で運用されていることを示す文書を閲覧し、組織的管理が行われていることを確認する。 ・情報セキュリティ委員会等の議事録。 ・詳細管理策策定後の運用状況を記録した文書。 【閲覧・質問】内部監査報告書を閲覧すると共に、内部監査人に質問し、適正な運用が行われていることを確認する。 ・詳細管理策運用に関する内部監査報告書。
・ （略） ・	
職務権限定義の適正さ	【閲覧】職務定義及び職務任命に関する文書を閲覧し、適正な運用がなされているかを確認する。 ・対象業務に関わる区画及び重要情報資産へのアクセス権限を規定する職務及び責任範囲を明確にした職務定義書は適正な手順により作成・承認されているか。 ・職務定義書の内容は、以下の条件を満たしているか。 ・辞令で確実に職務権限の発令、停止が行われているか。 ・権限のたな卸しは、年1回経営者の責任において行われているか。 【質問】業務責任者・現場担当者に質問し、記録が正しく行われていることを確認する。 ・一人が複数の権限を保有しないか。 ・一つの職務で同一の重要データに対する読取、書込み・変更、監視・監査の作業が分離されているか。 ・各職務について、業務遂行上アクセスが必要な情報資産が全て網羅されているか。 ・各職務の情報資産に対するアクセス権限の内容が明確か。 ・緊急の必要により、職務定義書に定められた以外の作業や他の人の作業を兼務することが生じた場合の管理策があらかじめ定められているか。 ・職務定義書に定められた以外の作業においては、あらかじめ定められた管理策に基づき作業が行われているか。 ・全ての役員・社員等に、定められた権限以外のアクセスが禁止されているか。 ・組織・人事異動の際にも権限の重複がないよう運用されているか。 ・情報セキュリティ管理責任者が職務権限の設定と付与を行っているか。 ・情報セキュリティ管理責任者が権限の付与状況を少なくとも年1回定期的に見直しているか。
・ （略） ・	

5 監査の実施と効果

情報セキュリティ監査手続きの合意を受けて監査が実施された。

その結果、U社は、下記に示す報告書により、委託元（顧客であるV社）の期待する水準にあるとの保証意見を得ることができた。

情報セキュリティ監査の保証意見により、V社はU社との契約を締結することになった。その後U社は、最大停止時間15分以内のサービスレベルとISMS認証を取得していることに加え、保証型情報セキュリティ監査で保証を得ている点を同業他社との差別化ポイントとして、V社と同等の情報セキュリティ水準を期待している大手金融機関なども対象として、更なる業容拡大をはかることとした。

情報セキュリティ監査報告書

200X年XX月XX日

委　託　元　　V株式会社　殿
被監査主体　　U株式会社　殿

監査主体
Z監査株式会社
代表者　○○　○○印

情報セキュリティ監査報告書

監査主体は、被監査主体との200×年●月●日付情報セキュリティ監査契約にもとづく「利用者合意方式」による保証型情報セキュリティ監査の結果を下記のとおり報告する。

― 記 ―

監　査　結　果

●●作成の200X年●月●日付言明書記載のシステムの運用管理サービスに対する情報セキュリティ対策の実装は、委託元の合意を得た情報セキュリティに係る監査手続を実施した限りにおいて、□□□□によって示されている同業務委託元の期待する水準にあるものと認める。

理　　由

監査人は、主任監査人○○、監査人△△、監査人補××からなる監査チームを組織し、情報セキュリティ監査基準及びU株式会社作成の詳細管理策に基づく個別管理基準に準拠して、200X年●月●日から200X年●月●日までの間、監査報告書利用者たる○○業務委託元と合意した以下の監査の範囲及び監査手続きにより、U株式会社代表取締役○○　○○作成の200X年●月●日付言明書記載に対する情報セキュリティ対策の実施状況を監査した結果、監査結果表明のための合理的な証拠を得た。

委託元と合意した監査の範囲及び情報セキュリティ監査手続き：別紙

実施した監査手続		結果
【設計監査】管理策の必要性・十分性		—
言明書作成の正当性	【質問】言明書作成の目的、言明の根拠に関し、経営者に質問を行い、明確な根拠があることを確認する。 また、言明書の作成に関わった社内の責任者・担当者、及び外部委託先（コンサルティング会社W社）責任者及び担当者に質問し、経営者の質問と整合性があることを確認する。 【閲覧】言明の根拠となる、言明書作成の経緯を記録した文書を閲覧し、経営者の回答と整合性が取れていることを確認する。 文書としては、以下のものを対象とする。 ・言明書作成に関わる会議の記録（情報セキュリティ委員会議事録、経営会議議事録、その他打合せ記録等）。 ・言明書作成の資料として用いたW社のコンサルティングの結果報告書。 ・ISMSなど公的な認証取得の文書を閲覧し、経営者が情報セキュリティマネジメントを的確に運用していることを確認する。	実施していると認められる
リスク把握の適切さ	【閲覧】対象業務フローに係るリスク分析を確認し、リスクが漏れなく、的確に洗い出されていることを確認する。 【視察】業務の現場を確認し、リスク分析で記述された脅威・ぜい弱性が十分であることを確認する。 【質問】業務現場の担当者に質問し、リスク分析が的確であることを確認する。 【質問】経営者にリスクに関して質問し、リスクが正しく認識されていることを確認する。 【質問】言明書の作成に関わった社内の責任者・担当者、及び外部委託先（コンサルティング会社W社）責任者及び担当者に質問し、経営者の質問と整合性があることを確認する。	実施していると認められる
管理策の適切さ	【閲覧】情報セキュリティ管理基準を参照して作成した個別管理基準に照らして、リスク分析によって洗い出されたリスクに対し、言明書において必要な管理策が網羅されていることを確認する。 【質問】経営者に管理策の内容を質問し、管理策として行うべきことが的確に記述されていることを確認する。 【質問】言明書の作成に関わった社内の責任者・担当者、及び外部委託先（コンサルティング会社W社）責任者及び担当者に質問し、経営者の質問と整合性があることを確認する。	実施していると認められる
【実装監査】	言明書どおりに運用が行われていることの確認	—
言明書の運用の確認	【質問】経営者と業務管理責任者に質問し、言明書に基づく管理を実施していることを確認する。 【閲覧】言明書どおりに管理策が組織全体で運用されていることを示す文書を閲覧し、組織的管理が行われていることを確認する。 ・情報セキュリティ委員会等の議事録。 ・詳細管理策策定後の運用状況を記録した文書。 【閲覧・質問】内部監査報告書を閲覧すると共に、内部監査人に質問し、適正な運用が行われていることを確認する。 ・詳細管理策運用に関する内部監査報告書。	実施していると認められる
・ （略） ・		

職務権限定義の適正さ	【閲覧】職務定義・及び職務任命に関する文書を閲覧し、適正な運用がなされているかを確認する。	実施していると認められる
	・対象業務に関わる区画及び重要情報資産へのアクセス権限を規定する職務及び責任範囲を明確にした職務定義書は適正な手順により作成・承認されているか。	実施していると認められる
	・職務定義書の内容は、以下の条件を満たしているか。	実施していると認められる
	・辞令で確実に職務権限の発令、停止が行われているか。	実施していると認められる
	・権限のたな卸しは、年1回経営者の責任において行われているか。	実施していると認められる
	【質問】業務責任者・現場担当者に質問し、記録が正しく行われていることを確認する。	実施していると認められる
	・一人が複数の権限を保有しないか。	実施していると認められる
	・一つの職務で同一の重要データに対する読取、書込み・変更、監視・監査の作業が分離されているか。各職務について、業務遂行上アクセスが必要な情報資産が全て網羅されているか。	実施していると認められる
	・各職務の情報資産に対するアクセス権限の内容が明確か。	実施していると認められる
	・ 緊急の必要により、職務定義書に定められた以外の作業や他の人の作業を兼務することが生じた場合の管理策があらかじめ定められているか。	実施していると認められる
	・職務定義書に定められた以外の作業においては、あらかじめ定められた管理策に基づき作業が行われているか。	実施していると認められる
	・全ての役員・社員等に、定められた権限以外のアクセスが禁止されているか。	実施していると認められる
	・組織・人事異動の際にも権限の重複がないよう運用されているか。	実施していると認められる
	・情報セキュリティ管理責任者が職務権限の設定と付与を行っているか。	実施していると認められる
	・情報セキュリティ管理責任者が権限の付与状況を少なくとも年1回定期的に見直しているか。	実施していると認められる
・ （略） ・		

4 グループ企業における利用者合意方式の保証型情報セキュリティ監査の利用例（2章 3 のX社の場合）

1 X社における保証型情報セキュリティ監査への取り組み

200X年に入り、X社グループ各社の情報セキュリティに関する理解度は深まり、情報セキュリティ対策ベンチマークの回答もブレが少なくなってきた。

3つのグループごとにみると、いずれのグループでもしっかりとした情報セキュリティマネジメントが行われていると考えられるトップ集団と、十分なマネジメントが運用できない企業とに二分されている状況にあった。

また、いくつかの企業で、評価を気にするあまり診断を甘めにする動きも生じているのではないかとの懸念が生じた。

このような状況から、更なる情報セキュリティ対策の向上を図るために、情報セキュリティ部長のY氏は、情報セキュリティ監査を行うことを企画した。具体的には、3グループのうち、中位以上のクラスの企業の中から数社を選び、保証型情報セキュリティ監査により、自己診断の結果が適正であるかを判断すること、及び、下位に低迷する企業については、助言型情報セキュリティ監査により対策の強化を図ることとした。

企業の選定についてどのように行うかが議論され、結果として、自ら情報セキュリティ監査を望む企業を3グループ各々から保証型情報セキュリティ監査・助言型情報セキュリティ監査各1社を選ぶと共に、無作為抽出で上位から1社保証型情報セキュリティ監査を、下位から1社助言型情報セキュリティ監査を行うことが決定された。

このY部長の提案は、グループ経営ミーティングで今年度の活動として認められ、年度の初めに各社に通知された。この通知を受けた後、自己診断が開始され、上半期に各社の診断結果が情報セキュリティ部に報告されてきた。

昨年度と比較すると数社で厳しめの診断をした跡が見える企業もあったが、全体的な傾向はそれほど変わらないものであった。

情報セキュリティ監査を依頼する企業は当初の想定よりも多かったため、抽選で各グループから各々2社を選定した。また、無作為抽出により各グループから2社ずつ抽出し、合計12社に対する情報セキュリティ監査を実施することとなった。

2 X社における保証型情報セキュリティ監査の導入

監査実施に当たって、X社は、監査目的を以下のように定めた。

(1)保証型情報セキュリティ監査にあっては、グループとして情報セキュリティ対策ベンチマークの項目ごとに客観的な評価基準を設け、それに達しているかを判断することにより、適正な自己診断が行えていることを明らかにする。

(2)助言型情報セキュリティ監査においては、3以下の水準にある項目について、情報セキュリティ管理基準に照らして、適切でない項目を検出し、どのような点を改善するのがよいかを明らかにする。

また、保証型情報セキュリティ監査は利用者合意方式とするが、被監査主体となる各社の顧客と合意をとるのは時間的に余裕がないことから、X社が利用者代表として監査手続きについて監査会社と合意することにした。

この目的のために、情報セキュリティ対策ベンチマークの項目を情報セキュリティ管理基準及びCOBIT 4.1[*4]など関連する基準を参考に、個別管理基準を作成し、情報セキュリティ監査を実施することが方針として決定された。

X社は、情報セキュリティ監査企業台帳に登録されており、JASA会員企業でもある監査会社の中から、実績のある数社にRFPを送付し、提案書作成を依頼した。その結果、個別管理基準の作成方法や監査手続きについて、すぐれた提案をした6社を選定し、各々のグループごとに、保証型情報セキュリティ監査と助言型情報セキュリティ監査を分けて監査を依頼することにした。

＊4 COBIT 4.1：COBIT（Control Objectives for Information and related Technology）はITGI（IT Governance Institute：ITガバナンス協会）が発行しているITカバナンス確立のための一連の資料やツールである。2008年9月現在のバージョンは4.1。

選定された6社は各々担当する被監査主体を訪問し、事前調査を踏まえてテーマを絞り、自社の情報セキュリティ強化に結びつく分野に重点を置いて情報セキュリティ監査を行うことになった。

情報セキュリティ監査が開始されてから、報告書を取りまとめるまでは、ほぼ順調に作業が進み、予定通り監査は終了した。

保証型情報セキュリティ監査を受けた6社のうち、4社は自己診断の結果とほぼ変わらない水準にあることが確認できた。

残りの1社は、自社が定義していた手順にあいまいな部分があった。現状は現場の責任者の判断で一見問題なく運用されていたが、マネジメント上では不備と指摘され、保証意見は留保された。また、残りの1社は、是正処置が手順どおりに行われていない事象が検出され、保証意見は述べられなかった。

助言型情報セキュリティ監査を受けた6社は、大きく2つのグループに分かれた。第一のグループは情報セキュリティマネジメントそのものの設計に問題のあるグループで、PDCAサイクルの理解が不十分であったため、基本的な規定・体制について改善提言を受けた。

第二のグループは基本的なフレームワークはできているが、管理策が不十分なため、ぜい弱性が残っている点について改善提言を受けることになった。

3 グループ全体の情報セキュリティの向上

情報セキュリティ監査を受ける各社の経営者や担当者は、当初、相当緊張し、また、監査人の判断に厳しく抵抗する姿もあった。

監査が進んでいくにつれて、監査人がどのような点を見るかが分かり、これら経営者や担当者は、情報セキュリティマネジメントに関する深い理解を得るようになってきた。

保証型情報セキュリティ監査により保証意見を得た企業は、情報セキュリティ報告書を作成し、保証された内容を可能な範囲で開示した。

情報システム部は、保証を受けた4社の情報セキュリティ責任者を講師とした勉強会をグループ内企業の情報セキュリティ責任者に対して開催した。この中で、情報セキュリティ対策の立案、言明書の作成、監査を受けるプロセス等について、突っ込んだ質疑応答がなされ、情報セキュリティマネジメントに対する理解をより一層深めることができた。

さらに、情報セキュリティ部は、助言型情報セキュリティ監査報告書に基づき、「情報セキュリティマネジメントの構築のコツ」を作成し、陥りやすい誤りを事例として整理した。企業名が分からないように、内容を架空の会社の話に置き換えているが、ドキュメンタリータッチで仕上げたものが好評で、一般社員にも広く読まれるようになった。

これらの活動を通じて、情報セキュリティマネジメントに対する全グループを通じた理解が深まった手ごたえを、Y部長は感じている。

情報セキュリティ対策
ベンチマーク活用集

付録

付録 1　情報セキュリティ対策ベンチマークの概要

付1.1　情報セキュリティ対策ベンチマークの概要

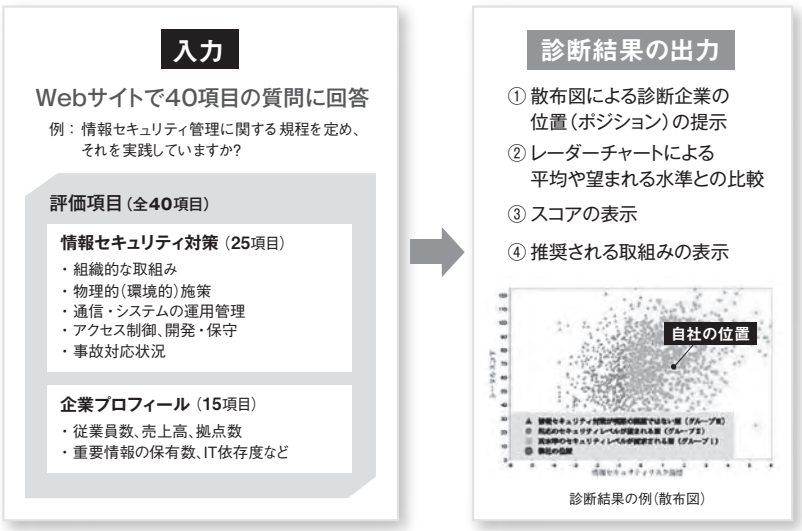
情報セキュリティ対策ベンチマークは、組織の情報セキュリティ対策状況を自らが評価するための自己診断ツールである。経済産業省より公表された情報セキュリティガバナンス推進のための施策ツールを、IPAが自動診断システムとして開発し、2005年8月よりIPAのWebサイト上で提供している。

情報セキュリティ対策の実施には経営者のリーダシップが重要なことから、経営者の気づきと積極的な関与を促すためにも有効だとされている。

自己診断ツールといわれるものは多くあり、チェックリストに○や×をつける、段階的評価に基づき点数をつけるなどの方法で診断するものがある。Webベースで質問に答えていくと、点数が表示されるものもある。情報セキュリティ対策ベンチマークも、これらの自己診断ツールの要素を持っているが、他と大きく違うのは、何千件もの実データに基づいて、望まれる水準を設定しており、望まれる水準や他社の対策状況と自社の状況を比較できる点にある。

情報セキュリティ対策ベンチマークは一般に、計測の基準となる指標のことを言う。ベンチマーキングは、ある指標（ベンチマーク）を探し出し、それと比べることで自組織のレベルを評価し、不足部分を改善していく経営改善の手法としても知られている。「情報セキュリティ対策ベンチマーク」は、この自己評価と業務改善の手法を情報セキュリティ対策に応用したものである。

情報セキュリティ対策ベンチマークによる自己診断はWebベースで行われる。IPAのホームページ（http://www.ipa.go.jp/security/benchmark/）にアクセスし、第1部 情報セキュリティ対策への取組みに関する25問と、第2部 企業プロフィールに関する15問、計40問に回答すると、診断結果と推奨される取組みが表示される。



図付1.1　情報セキュリティ対策ベンチマークの概要

診断企業は情報セキュリティリスク指標に応じて、**表付1.1**に示す3つのグループのいずれかに分類される。情報セキュリティリスク指標は、従業員数、売上高、重要情報の保有数、IT依存度などから計算される企業のかかえるリスクを表す指標である。

表付1.1　情報セキュリティリスク指標による企業分類

分　類	特　徴
グループⅠ	高水準のセキュリティレベルが要求される層
グループⅡ	相応の水準のセキュリティレベルが望まれる層
グループⅢ	情報セキュリティ対策が喫緊の課題でない層

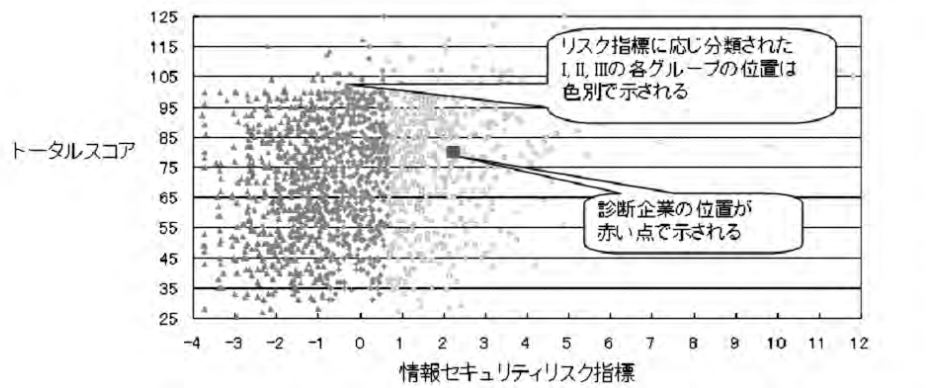
第1部の情報セキュリティ対策に関する25項目では、自組織の取組みの状況を**図付1.2**に示す5段階の成熟度により自己評価する。成熟度1は取り組みができていない状態であり、段階が上がるにつれて、取組みができていることになる。1問5点（5段階）として、トータルスコアは125点である。

できていない

1	経営層にそのような意識がないか、意識はあっても方針やルールを定めていない
2	経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3	経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4	経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5	4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

できている

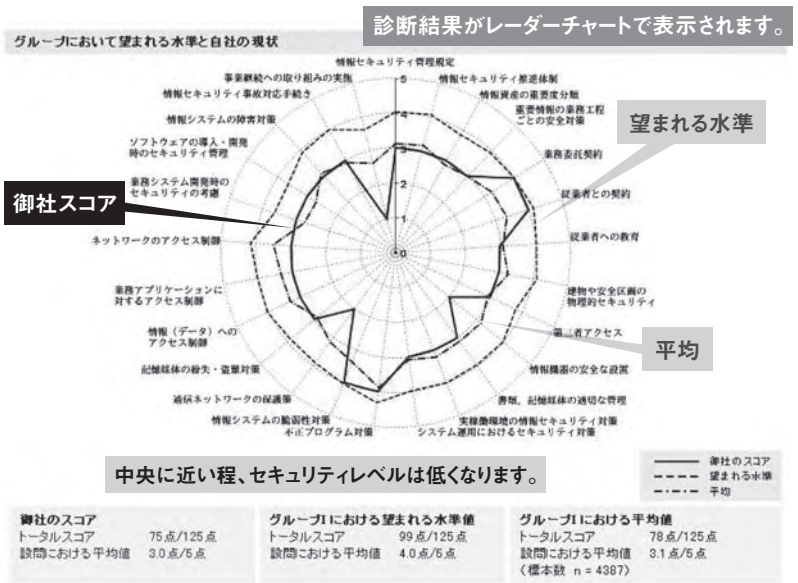
図付1.2　成熟度で答える5段階の回答



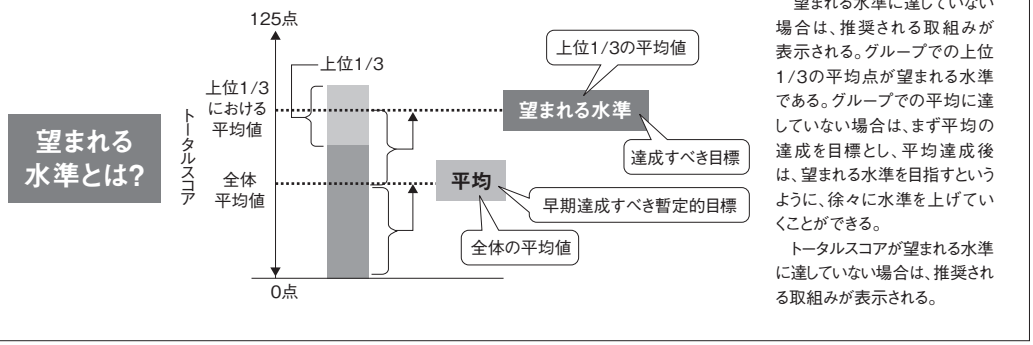
図付1.3　診断結果例（散布図）

自組織がどのグループに分類され、その中でどの位置にあるかは、散布図（**図付1.3**）やレーダーチャート（**図付1.4**）で示される。散布図の縦軸はトータルスコア、横軸は情報セキュリティリスク指標である。散布図は、全体と、従業員数300名で分けた企業規模別の2種類があり、いずれも、リスク指標によって分類されたグループを色別に表示し、診断企業は自分が分類されたグループと、全体の中での自社の位置を把握することができる。

25項目の各スコアの比較は、レーダーチャートで示される。レーダーチャートは、情報セキュリティリスク指標によるグループ別、企業規模別、業種別の3種類が示され、望まれる水準や、グループでの平均値と自社のスコアの差を比較することができる。



図付1.4　診断結果例（レーダーチャート）



図付1.5　望まれる水準

望まれる水準は比較するグループごとに設定されており、これを目安に、必要なレベルの対策が検討できるため、セキュリティコストの適正化につながる。
第1部の25問は、ISMS認証基準であるJIS Q 27001の附属書Aの管理策133項目をもとに作成されている。経営層の利用を想定し、平易な言葉を使い、25問に絞り込んだため、簡便に組織の取り組み状況を確認できる。また、質問ごとに「対策のポイント」があり、それらをあわせると全部で146項目となる。

質問に答える際に、その根拠を確認することで、より客観的で信頼性の高い診断結果として活用できる。たとえば、「経営層を含めた情報セキュリティの推進体制やコンプライアンス（法令順守）の推進体制を整備していますか？」という質問なら、体制図や各担当者の責任を記載した文書などが根拠となる。

付1.2 改訂版の公開と新機能

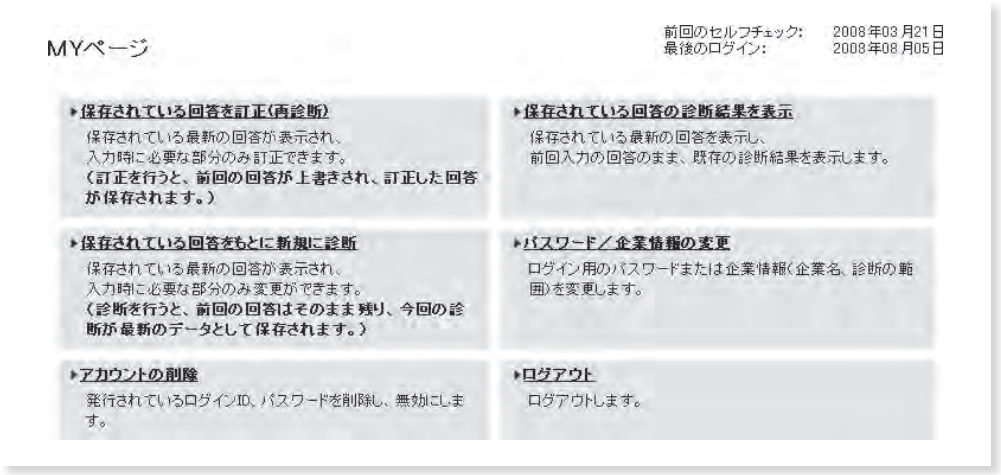
2005年3月の「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」の発表より2年半が経過し、経済産業省より「情報セキュリティ対策ベンチマーク改訂版」が2007年8月24日に公開された。これは、この間に企業が抱える事業リスクも多様化・複雑化したことに対応し、施策ツールの見直し・改善が検討されたことの成果である。

IPAでは、この改訂版に示された、JIS Q 27001への対応、及び、ユーザからの要望に基づいた新機能を追加し、2007年12月には情報セキュリティ対策ベンチマークver.3.0を、2008年4月にはver.3.1を公開した。次に改善のポイントを示す。

(1)ISMS認証基準（JIS Q 27001）への対応
- 質問構成、質問内容、推奨される取り組みを新しいISMS認証基準に対応して変更。その際、既存の診断データを継続して使えるように、新旧バージョンでの質問の整合性に配慮した。
- 平易な言葉を使用するとともに、曖昧な表現をなくし、丁寧な説明をつけた。

(2)MYページのユーザビリティの向上

MYページは、アカウントを発行したユーザがログインできる固有のページで、保存されている回答



図付1.6 MYページの画面

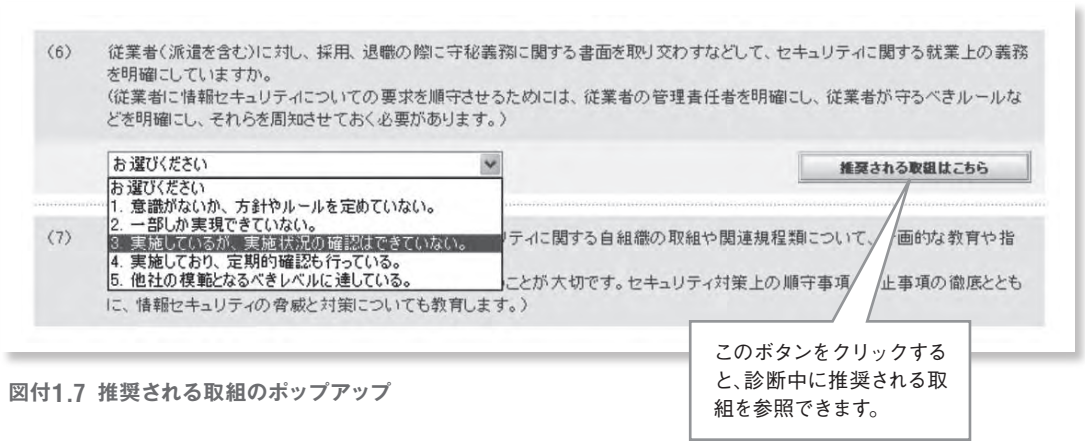
の訂正、保存されている回答をもとにした新規の診断、パスワードの変更などができる。このページでは、次の改良を行った。

- 修正か新規の診断かを選べる機能を追加。
- MYページからの診断では、保存されている最新の回答が表示され、変更部分の入力だけで診断ができる機能を追加。

(3)診断用のツールを提供

- 診断前に回答を記載して準備できる質問一覧を提供（情報セキュリティ対策ベンチマークポータルサイトよりダウンロード可能に）。
- 診断中に、評価項目の「推奨される取組み」を直接参照可能。

【「推奨される取組」の参照】



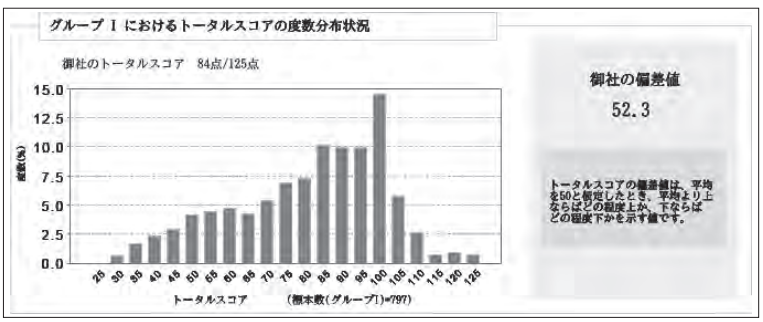
図付1.7 推奨される取組のポップアップ

(4)診断の基礎データと統計情報

- 情報セキュリティを巡る環境変化やレベルの変化を勘案し、情報セキュリティ対策ベンチマークver.3.1より、診断の基礎データは、最新2年分のデータを適用することとした。具体的には、毎年12月末で集計を区切り、統計情報をまとめ、翌年4月より新しいデータセットでの診断を開始する。(統計情報掲載のURL：http://www.ipa.go.jp/security/benchmark/benchmark_tokuchover31.html)

(5)トータルスコアの度数分布状況と偏差値を表示

- 情報セキュリティ対策ベンチマークver.3.1より、診断結果にトータルスコアの度数分布と偏差値が表示される。トータルスコアは、情報セキュリティ対策状況の回答から得られる総得点であり、偏差値は、グループの総得点の平均値を50と仮定した時、平均よりどの程度上か、またはどの程度下かを示す値である。



付1.3 政府機関での利用（外部委託先の評価）

政府機関が外部委託先の情報セキュリティ対策状況の確認をするために情報セキュリティ対策ベンチマークを使用する際、業務の性質に応じて要求水準を設定することがある。政府機関統一基準適用個別マニュアル「外部委託における情報セキュリティ対策に関する評価手法の利用の手引」は、要求水準を設定する際には成熟度4を求める場合と成熟度3を求める場合の2通りあるとしている。成熟度4は、「経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている」段階で、トータルスコア125点満点の100点以上ということになる。成熟度3は「経営層の承認のもとに方針やルールを定め、全社的に周知・実施している」段階で、トータルスコアで75点以上ということになる。

自己診断結果提出の際には、確認書と項目ごとの確認結果を提出する。確認結果は、IPAのWebサイト上から印刷されるPDF出力結果の提出でも可能である。

付1.4 情報セキュリティガバナンスと3つの施策ツール

2005年3月に発表された経済産業省の「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」では、「情報セキュリティガバナンス」という考え方が提唱されている。報告書の中で「情報セキュリティガバナンス」は「社会的責任にも配慮したコーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」と定義されている。コーポレートガバナンスとは、企業経営を規律するための仕組みのことをいい、それを支えるメカニズムである内部統制の仕組みとしては、企業理念・行動規範等にもとづく健全な企業風土の醸成、法令順守の仕組みの構築、監査環境の整備、企業経営に重大な影響を及ぼすリスクの管理などが挙げられる。そして、これらの仕組みにより情報セキュリティを企業内に構築・運用する際、「自身が被害に遭わない、被害に遭った場合には被害をできるだけ局限化する」という基本原則に加えて、社会的責任も踏まえた上で情報セキュリティ対策に取り組むことが求められている。

「情報セキュリティガバナンス」が台頭してきた背景には、情報セキュリティ対策が企業の社会的責任を果たすという観点からも必要不可欠になっているという状況がある。情報セキュリティ事故が起きると、企業の存続が脅かされるだけでなく、その事故が社会全体に波及する可能性があること、企業が保有する情報の価値が高まっていること、法令順守が大きな課題となっていることなどから、情報セキュリティは経営課題となっているためである。

しかし、特に中小企業においては、情報セキュリティ対策が進んでいないという現実がある。対策が進まない理由として、IT事故発生のリスクが明確でなく、適正な情報セキュリティ投資の判断が困難、既存の情報セキュリティへの対策や取組みが企業価値に直結していない、事業継続性確保の必要性が十分に認識されていないの3点が挙げられ、これらの問題を解決して「情報セキュリティガバナンス」を確立するツールとして、次の3つの施策ツールが公開された。

(1)情報セキュリティ対策ベンチマーク
(2)情報セキュリティ報告書モデル
(3)事業継続計画策定ガイドライン

情報セキュリティ対策ベンチマークは、「IT事故発生のリスクが明確でなく、適正な情報セキュリティ投資の判断が困難」という問題に対してのひとつの答えと考えることもできる。

付録２　ISMS 適合性評価制度の概要

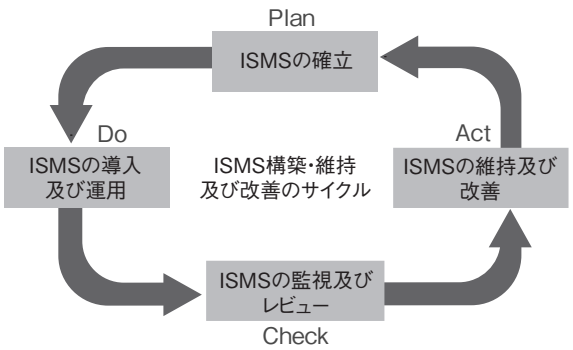
付2.1　ISMSの確立及び運営管理

1 一般要求事項

JIS Q 27001（ISO/IEC 27001）の一般要求事項では、「組織は、その組織の事業活動全般及び直面するリスクに対する考慮のもとで、文書化したISMSを確立、導入、運用、監視、レビュー、維持及び改善しなければならない」としている（**図付2.1**参照）。

ISMSの要求事項は、ISMSプロセスにおけるPDCAサイクルに従いまとめられている。ISMSを構築するためには、組織における情報資産を識別、分類し、これらの情報資産に対する脅威、ぜい弱性、発生頻度をベースにリスクアセスメントを実施し、リスク対応計画に基づきリスク低減のための情報セキュリティ対策を実施する。また、ある時点で情報セキュリティ対策を講じたとしても、技術の進展や環境の変化に合わせた改善を行う必要がある。そのための活動が内部監査や経営陣によるマネジメントレビュー、見直し、継続的改善・処置である。

また、その組織のISMSに関わる方針や記録を文書として作成、保管することが求められている。



図付2.1　ISMSプロセスにおけるPDCAサイクル

付2.2　ISMSの確立

ISMSを確立するには、組織における情報資産を識別、分類し、これらの情報資産に対する脅威、ぜい弱性、発生頻度をベースにリスクアセスメントを実施し、リスク対応計画に基づきリスク低減のための管理策を決定し、実施しなくてはならない。

1 ISMSの確立ステップ

ISMSを確立するためのステップは、**図付2.2**に示す通りである。

図付2.2　ISMSの確立のステップ

(1) ISMSの適用範囲及びISMS基本方針を確立する（STEP1～STEP2）

まず、ISMSの適用範囲は事業、組織、その所在地、資産及び技術の各特徴の観点から定義する。ISMS基本方針は、事業上及び法的要求事項やリスクアセスメントなどから導かれる情報セキュリティに対する要求事項を考慮し、リスクマネジメント環境、ISMSを確立し維持する組織環境、情報セキュリティの全般的な方向性及び行動指針を確立することである。なお、ISMS基本方針は、情報セキュリティ基本方針のさらに上位の方針を示すもので、組織全体のマネジメントシステムの観点からISMSをどのように位置づけるかを示したものである。

(2) リスクアセスメントに基づいて管理策を選択する（STEP3～STEP7）

上記 (1) で決定したISMSの適用範囲及びISMS基本方針に基づき、リスクアセスメントの取組み方法を策定する。リスクアセスメントは、比較可能で再現可能な結果を導き出すことを確実にする。

リスクの識別では、保護すべき情報資産に対して機密性、完全性、可用性を喪失させる脅威、ぜい弱性及びそれらが事業に及ぼす潜在的な影響の大きさを識別する。すなわち、「リスク」とは現実に脅威を受けたときに想定される「資産が被る影響（資産価値）」と、その資産に対する「脅威の頻度」及びその脅威が侵入してくる可能性のある資産の「ぜい弱性の程度」の組合せである。

リスクアセスメントでは、セキュリティ障害による事業上の損害及び発生可能性を評価した結果でリスク水準を算定し、リスクを受容するための基準と比較してリスク受容できるか、リスク対応が必要かどうかを決定する。リスクの受容ができない場合、リスク対応として管理策の採用、リスク保有、リスク回避、リスク移転の選択をする。リスクアセスメントの具体的方法については、ISMSユーザーズガイド（JIS Q 27001対応　平成18年12月 JIPDEC発行）を参照されたい。

リスク対応の結論に従って、JIS Q 27001 附属書A「管理目的及び管理策」のリストから適切な管理目的と管理策を選択する。管理策の選択には、リスク受容基準、法令又は規制要求事項、契約上の義務、及び事業上の要求事項を考慮する。また、附属書Aのリストの選択だけでなく、組織の必要に応じて追加の管理目的と管理策を採用することもできる。

(3) リスクについて適切に対応する計画を策定する (STEP8～STEP10)

経営陣は、選択した管理目的及び管理策についての残留リスクを承認し、ISMSの導入及び運用について許可を与える。

選択した管理目的及び管理策並びにこれらを選択した理由と除外の理由を記載した適用宣言書を作成する。なお、適用宣言書には、現在実施されている管理目的及び管理策も含める。

2 リスクアセスメント

ISMSを確立するステップにおける「リスクアセスメント (リスクを分析し評価する)」の段階として、「ギャップ分析」、「詳細リスク分析」の2段階で実施することが可能である。

リスクアセスメントの方法である「ベースラインアプローチ」、「詳細リスク分析」及び「組合せアプローチ」について説明する。

(1) ベースラインアプローチ

ベースラインアプローチとは、後述する詳細リスク分析とは異なり、情報資産ごとにリスクそのものを評価しない。

一般の情報セキュリティに関する基準や、業種・業界で採用されている標準やガイドラインなどを参照し、組織全体で共通の情報セキュリティ対策を実施する。実現可能な水準の管理策を採用し、組織全体で情報セキュリティ対策に抜け、漏れが無いように補強していくアプローチである。

ベースラインアプローチは、大きく分けると以下の2つの手順で実施される。

①ベースラインの決定

②ギャップ分析の実施

ベースラインアプローチでは、組織の達成する情報セキュリティ管理について独自の「対策の標準」を作成する。一般に、この対策の標準のことを「ベースライン」と呼ぶ。

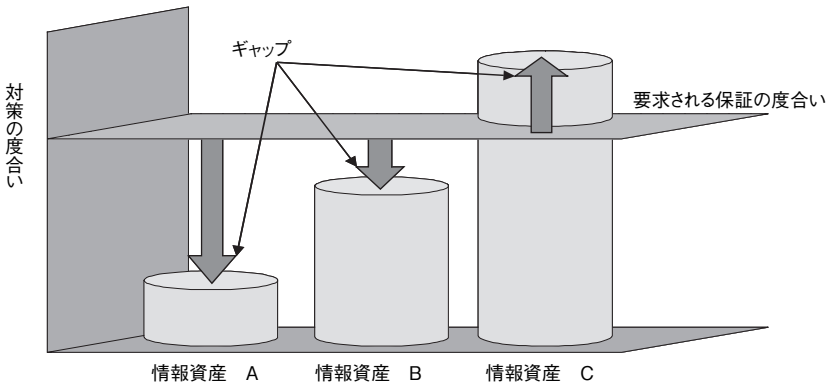
実際にどのようなコントロールを導入するのか、「出来る、出来ない」の判断をする前に広く管理策についての情報を収集し、組織が要求する情報セキュリティの管理水準が、達成可能なベースラインであるかを検討されたい。たとえば、他の企業と比較して情報セキュリティの管理水準が必要なレベルであるかを調べるのも効果的である。

次に、ギャップ分析について説明する。

ギャップ分析実施の目的は、組織の定める基準への準拠状況の把握にある。

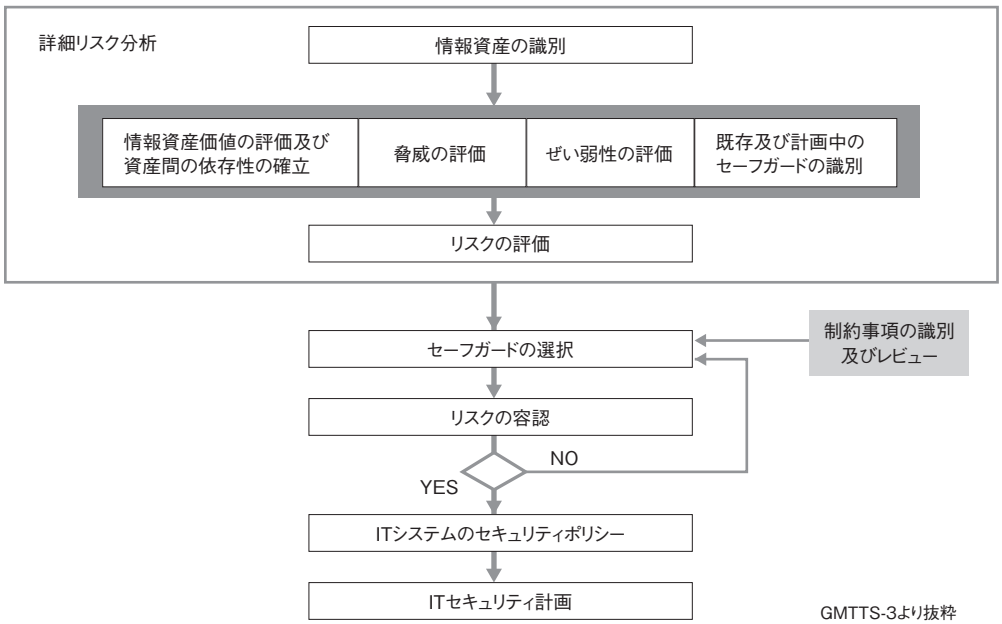
基準で要求される管理レベルと事業者の管理レベルの現状を比較し、「大きな差が認められる個所」、「明らかに管理策の適用を必要としている個所」、「過度に管理策が適用されている個所」等を確認する。

図付2.3は、それぞれの資産を対象に、現状の対策の度合いと組織によって定められる「要求される保証の度合い」との乖離を示している。図付2.3の要求される保証の度合いはひとつの平面として表現されているが、本来、要求される保証の度合いは一律ではなく、資産の属性や性質、組織における重要度により情報資産ごとに決定される。



図付2.3　要求される保証の度合い

(2)詳細リスク分析



図付2.4　詳細リスク分析を含むリスクマネジメント

詳細リスク分析では、資産ごとの関連するリスクの識別を個別に実施する（**図付2.4**参照）。

リスクが顕在化する頻度は、脅威が発生する（顕在化する）可能性、管理上の弱点につけ込まれる可能性（ぜい弱性）の他に、資産が攻撃者から見てどれほど魅力的なものであるのか等にも依存する。

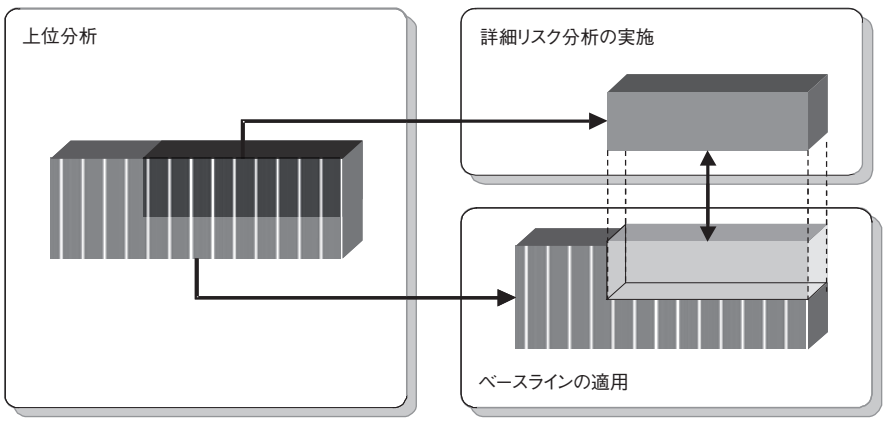
まず、リスク分析の対象範囲の定義付けをしなければならない。プロセスが密接に絡み合っているにもかかわらず、安易に範囲を狭め、慎重な定義付けを怠ると、後に不必要な作業が増えたり、抜けが見られたりすることに繋がるからである。

(3)組合せアプローチ

一般には、ベースラインアプローチと詳細リスク分析を併用する組合せアプローチを採用することが効率的であると紹介されている。

どのような場合にどのアプローチを採用するかは一概には決定できない。適切なアプローチの採用のための判断材料は、資産に求められるセキュリティ要求事項（前述の事業上の要求事項、法的又は規制要求事項、契約上のセキュリティ義務など）に依存する。組合せアプローチには、それぞれの資産を取り巻くリスク環境を確認し、適切なリスク分析のアプローチを採用し、それぞれのアプローチの弱点を相互に補完し合うことにより、ISMS適用範囲全体のリスク分析を効率的に実施する目的がある。「ベースラインアプローチ」のみでは、高い水準で情報セキュリティ対策が実装されるべきリスクの高いシステムについて対応策が不充分になる可能性があること、また、「詳細リスク分析」をすべてのシステムに適応することは効率的な観点から現実的でないことが大きな理由である。

図付2.5は、組合せアプローチの例である。



図付2.5　組合せアプローチ

付2.3　ISMSの導入及び運用

1 ISMSの導入及び運用ステップ

ISMSの導入及び運用のステップは、**図付2.6**に示す通りである。

(1) リスク対応計画の実施（STEP1～STEP2）

リスク対応計画は、情報セキュリティについてのリスクを管理するためのものである。すなわち、受容できないリスクを低減するためにとるべき活動と、選択した管理策の実装に関する計画を明らかに

することである。このリスク対応計画により、組織が識別したリスクに対する管理策の実施状況と、残留リスクが受容可能な水準以下に低減されていないリスクへの追加的対策の進捗状況を容易に把握することができる。

次に、管理目的を達成するためにリスク対応計画を実施する。実施するとは、ISMSを構築し実装することを意味する。そのため、経営陣はリスクマネジメントに必要な経営資源を割当てる責任がある。

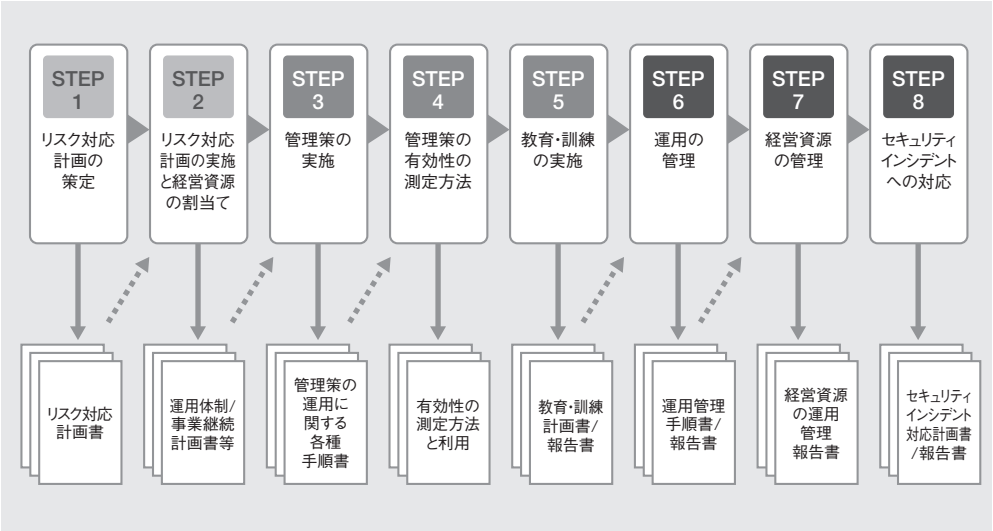
(2)管理策の実施と有効性の測定 (STEP3～STEP5)

管理策の運用に関する手順や情報セキュリティインシデントの発生した際の手順などを文書化し、管理策を実施する。計画された管理目的が管理策によってどの程度達成されているかを判断するため、選択した管理策又は一群の管理策の有効性を測定する方法について定義する。また、比較可能で再現可能な結果を出すための管理策の有効性を評価するために、この測定方法をどのように利用すべきかを規定する。管理策が有効であるかどうかは、管理策の導入が対象とするリスク及び目的への適切な対策として機能するかどうかである。

また、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ためには、要員全てが要求される業務に対する力量をもつことを確実にするため、教育・訓練を実施する。

(3)運用管理と情報セキュリティインシデントへの対応 (STEP6～STEP8)

導入した管理策が適切に運用、管理されるための手順書を策定するとともに、各手順書には、運用管理者、利用者などの関係者の責任を明記する。経営陣は、ISMSの運用管理に必要な経営資源を決定し提供する。リスク対応計画では、適正な資金の拠出範囲を明確にする。情報セキュリティインシデントに対する被害を最小限に抑えるため、情報セキュリティインシデントに対応するための手順書を策定し、その内容を定期的に検証するとともに、セキュリティ事象を検出するための管理策を実施する。



図付2.6　ISMSの導入及び運用のステップ

付2.4 ISMSの監視及びレビュー

1 ISMS監視及びレビューのステップ

ISMSの監視及びレビューのステップは、**図付2.7**に示す通りである。

(1)管理策の有効性の測定 (STEP1～STEP3)

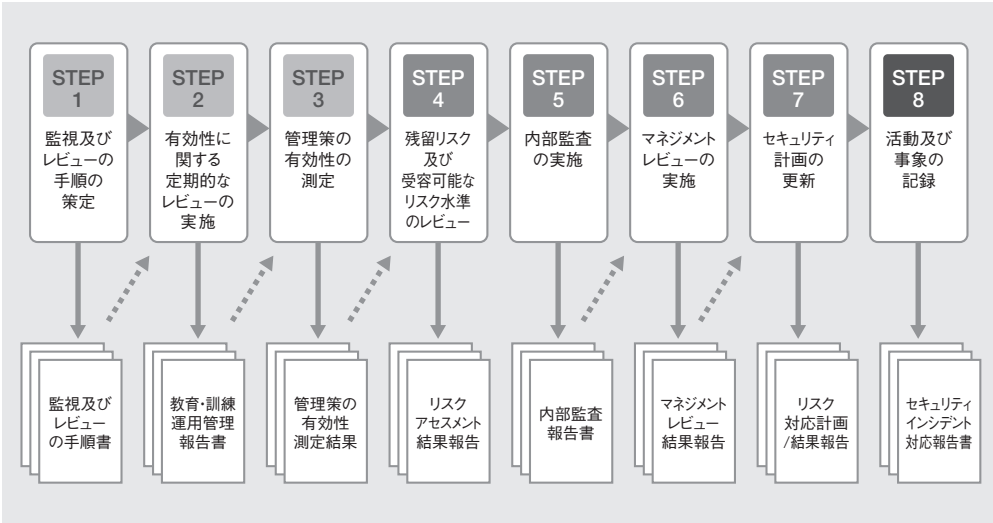
組織は、セキュリティ上の違反行為、情報セキュリティインシデントの防止、及びセキュリティ違反に対する処置の有効性を判断するため、監視及び見直しの手順を文書化するとともに、監視のための管理策を実施する。ISMSの有効性に関して定期的なレビューをする。有効性の評価は、目標に対する達成度を確認する。そのため、セキュリティ要求事項が満たされていることを検証するために、導入した管理策がどの程度有効に機能しているかを測定する。

(2) セキュリティ計画の更新 (STEP4～STEP7)

組織は、実施された管理策の有効性やリスクアセスメントに生じる変化 (組織変更、技術革新、事業の目的及びプロセスの改善、脅威の認識、外部事象) を考慮し、残留リスク及び識別された受容可能なリスク水準をレビューする。ISMSのプロセス及び手順が定められた通りに実行されているか否かの内部監査を実施する。経営陣は、組織のISMSのプロセスが適切で妥当でかつ有効であることを確実にするため、定期的にマネジメントレビューを実施し、ISMSの維持や継続的な改善を行う。組織が策定したあらゆる情報セキュリティに関するセキュリティ計画 (リスク対応計画も含む) を更新する。

(3)活動及び事象の記録 (STEP8)

ISMSの有効性又はプロセスの実施状況に重大な影響を与える可能性のある活動及び事象を記録する。記録は、要求事項への適合性及びISMSの有効な運用の証拠を提供するために作成し、維持する。



図付2.7 ISMSの監視及びレビューのステップ

付2.5 ISMSの維持及び改善

1 ISMSの維持及び改善のステップ

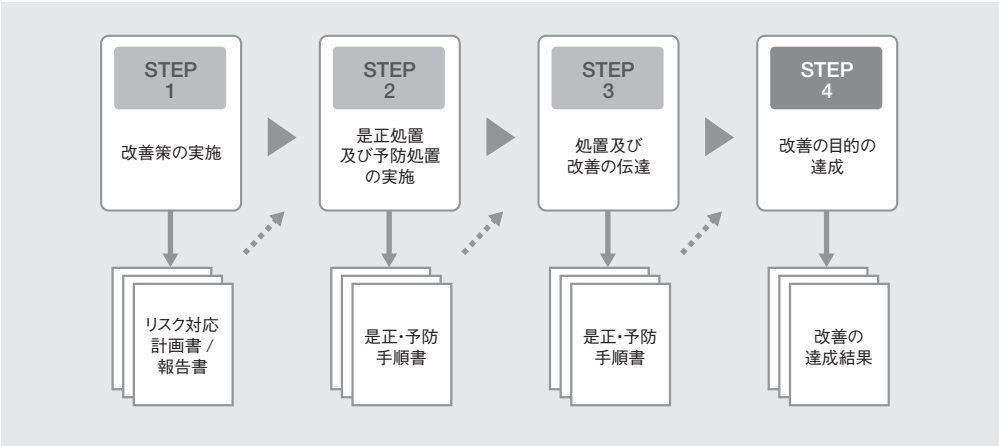
ISMSの維持及び改善のステップは、**図付2.8**に示す通りである。

(1)改善策及び是正・予防処置の実施 (STEP1～STEP3)

経営陣が責任をもって、ISMSの改善策を確実に実施する。この改善策は、前述のISMSの監視及びレビューを通じて得られたものだけでなく、外部からの改善要求事項なども考慮する。組織は、再発防止のため、ISMS要求事項への不適合の原因を除去するための是正処置及びISMS要求事項への起こりうる不適合の発生を防止するための予防処置を実施する。利害関係者全てに対し、状況に応じた適切な詳しさで処置及び改善策を伝達し、処置及び改善策の進め方について合意を得る。利害関係者は、組織の内部だけでなく外部の利害関係者も含めて配慮する。

(2)継続的改善 (STEP4)

組織は、改善の目的を確実に達成するよう監視し、必要によりレビューする。継続的改善は、機会あるごとに改善を行うことである。



図付2.8 ISMSの維持及び改善のステップ

付2.6 ISMSのマネジメントプロセス

1 経営陣の責任

ISMSの内部監査が実施されることを確実にするため、経営陣のコミットメント (約束、関与) が要求されている。ISMSに関連する活動すべてを含む内容であり、リスクを受容するための基準及び受容可能なリスク水準を決めることが要求されている。また、経営陣はISMSの必要性を理解し、その為に必要な経営資源の提供を行うとともに、要員の教育・訓練、意識向上及び力量が要求されている。

2 ISMS内部監査

ISMSの管理目的、管理策、プロセス及び手順が定められたとおりに実行されているか否かを評価するため、内部監査を実施することが要求されている。特に、ISMSが有効に実施され、維持され、期待通りに実施されていることを確認する必要がある。

3 ISMSのマネジメントレビュー

マネジメントレビューは、経営陣がISMSの効果を把握し、改善するための意思決定をする一連のプロセスである。マネジメントシステムの有効性を確保するために、経営陣の責任を明確化し、あらかじめ定められた間隔（少なくとも年1回）で実施することが要求されている。

経営陣は、組織のISMSが引き続き適切で妥当かつ有効であることを確実にするため、情報セキュリティ基本方針及び目的を含むISMSの変更の必要性を評価する。また、マネジメントレビューからのアウトプット（改善すべき事項の決定及び処置）として、リスクアセスメント計画及びリスク対応計画の更新、契約上の義務、管理策の有効性を測定する方法を改善することが要求されている。

4 ISMSの改善

ISMSの要求事項への不適合（ISMS認証基準に適合していないか、マネジメントシステムが実行されていない場合）が発生することを防止するために、その原因を除去すること、及び不適合発生の予防処置の必要性を評価することが要求されている。情報セキュリティの継続的な改善に経営陣が責任を持つことにより、情報セキュリティ対策が確実に実施され、組織の情報セキュリティ水準も継続して向上することが期待できる。

付2.7 管理目的及び管理策

「管理目的及び管理策」は、附属書A（規定）として記載されている。この規定は、ISMSの確立プロセスにおけるリスク対応として適切な管理目的及び管理策を選択するためのものである。また、すべてを網羅してはいないので、組織は必要に応じて追加の管理目的及び管理策を選択することもできる。

ISO/IEC 27001では、A.5～A.15に記載する管理目的及び管理策のリストは、ISO/IEC 17799の5から15を参照している。ISO/IEC 27001規格の第3章 2 1 で規定されたISMSのプロセスの一部としてこのA.5～A.15のリストから管理目的及び管理策を選択することとしている。

すなわち、「管理目的及び管理策」は、ISO/IEC 27002（JIS Q 27002　情報セキュリティマネジメントの実践のための規範）との整合性が完全に図られており、11の管理領域と39の管理目的及び133の管理策が記載されている。

A.5～A.15までに規定されている管理目的及び管理策の概要は、次の通りである。

(1) セキュリティ基本方針

情報セキュリティ基本方針は、事業上の要求事項や目的、関連する法令及び規制に対する取り組みなどを示したものであり、経営陣の指針及び支持を規定する。情報セキュリティ基本方針が妥当及び有効であることを確実にするためのレビューをする。情報セキュリティ基本方針のさらに上位の方

針を示すものとしてISMS基本方針があるが、これは組織全体のマネジメントシステムの視点からISMSをどのように位置づけるかの方針を示したものである。

表付2.1　管理領域別の管理目的及び管理策の数

対策	附属書A（規定）の管理領域	管理目的	管理策
組織的 人的	A.5　情報セキュリティ基本方針	1	2
	A.6　情報セキュリティのための組織	2	11
	A.7　資産の管理	2	5
	A.8　人的資源のセキュリティ	3	9
物理的 技術的	A.9　物理的及び環境的セキュリティ	2	13
	A.10　通信及び運用管理	10	32
	A.11　アクセス制御	7	25
	A.12　情報システムの取得、開発及び保守	6	16
組織的	A.13　情報セキュリティインシデントの管理	2	5
	A.14　事業継続管理	1	5
	A.15　順守	3	10
合　計		39	133

(2)情報セキュリティのための組織

情報セキュリティを確保するための組織としては、内部組織と外部組織に分けて考える。内部組織では、経営陣は情報セキュリティ基本方針を承認し、セキュリティに対する役割を割当て、組織全体にわたるセキュリティ活動を調整し、独立したレビューを実施する。情報セキュリティインシデント（事件・事故）に対処するときの適切な連絡窓口を確保するため、関係当局（監督官庁など）を含む外部のセキュリティ専門組織との連絡体制を維持する。外部組織による組織の情報及び情報処理施設へのアクセス、並びに情報の処理及び通信を管理する。組織の情報または資産への顧客のアクセス、あるいは顧客以外のビジネス活動の取引先である第三者との契約は、関連するすべてのセキュリティ要求事項を考慮する。

(3)資産の管理

組織の資産を適切に保護し、維持するため、すべての資産を明確に識別し、重要な資産について目録を作成・維持する。組織の中に資産の管理責任者を指定し、資産の利用の許容範囲に関する規則を文書化する。情報の適切なレベルでの保護を確実にするため、情報の必要性、優先順位及び保護の程度により情報を分類し、情報に対するラベル付け及び取扱いに関する手順を規定する。

(4)人的資源のセキュリティ

組織の情報セキュリティに影響を与える者を、従業員、契約相手及び第三者の利用者に区分する。雇用に関する事項は、雇用前（組織が関係を開始する前のこと）、雇用期間中（この関係が継続している期間）、雇用の終了または変更（この関係が終了または変更した後）の3段階に大別する。

雇用前では、従業員、契約相手及び第三者の利用者がその責任を理解し、求められている役割を確実にするため、セキュリティの役割及び責任について文書化し、職務定義書及び雇用条件において十分に審査する。

雇用期間中では、組織内の構成員全体にセキュリティの適用を確実にするため、経営陣の責任を明確にし、すべての従業員、契約相手及び第三者の利用者にセキュリティ手順及び情報処理設備の利用

方法について適切な意識向上のための教育・訓練を実施し、セキュリティ違反の取扱いに関する正式な懲戒手続を設ける。

雇用の終了または変更では、従業員、契約相手及び第三者の利用者の組織からの離脱を管理し、組織のすべての資産の返却及びアクセス権の削除を確実にする。

(5)物理的及び環境的セキュリティ

組織の情報及び情報処理施設のある領域を保護するため、物理的セキュリティ境界を設ける。セキュリティが保たれた領域では、入退管理、オフィス、部屋及び施設に対する物理的セキュリティ、外部及び環境の脅威からの保護、受渡し場所の隔離などがある。装置（構外で用いるもの及び移動するものを含む）については、環境上の脅威、認可されていないアクセスのリスクを低減し、損失または損傷から情報を保護する。物理的な脅威からサポート設備（電源、ケーブル配線など）を保護する。記憶媒体を内臓した装置は、装置の設置場所及び処分についても考慮する。

(6)通信及び運用管理

情報処理設備の正確、かつセキュリティを保った運用を確実にするため、すべての情報処理設備の管理及び運用のための責任体制及び手順の確立、運用システムの変更管理、職務の分割などを実施する。第三者が提供するサービスの管理は、提供されるサービスの合意の実施状況、順守状況を監視及びレビューする。

システム故障のリスクを最小限に抑えるため、必要とされるシステム性能を満たす十分な容量・能力の計画作成、新しいシステムの受入れなどを確実にする。悪意のあるコード及び認可されていないモバイルコードの侵入を防止し、検出するための予防対策を実施する。情報及びソフトウェアのバックアップは、合意されたバックアップ方針に従って実施するために、日常の作業手順を確立する。

ネットワークを脅威から保護するために、ネットワークのセキュリティ管理及びすべてのネットワークサービスについてセキュリティ特性、サービスレベル及び管理上の要求事項を特定する。取外し可能な媒体を管理する手順を確立し、媒体が不要になった場合には、正式な手順を用いて安全に処分する。情報の取扱い及び保管の手順を確立し、システム文書は認可されていないアクセスから保護する。組織間での情報及びソフトウェアの交換は、正式な交換方針に基づき情報交換に関する合意に沿って実施する。いかなる関連法令をも順守する。配送中の情報及び情報を格納した物理的媒体を保護するための手順及び標準を確立する。

電子商取引サービス（オンライン取引を含む）の利用に関連する情報は、不正行為、契約紛争及び情報の露呈または改ざんなどから保護する。認可されていない変更を防止するため、公開システム上で利用可能な情報の完全性を保護する。情報セキュリティ事象を記録した監査ログを取得する。システム使用状況を監査する手順を確立し、システム運用担当者の作業ログ及び障害ログを取得する。

(7)アクセス制御

情報へのアクセスを制御するため、アクセス制御方針は業務上及びセキュリティ要求事項に基づいて管理する。情報システム及びサービスへのアクセス権の割当て（特権の割当て及び利用、パスワードの割当て、利用者のアクセス権）を管理するための正式な手順を備える。

認可されていない利用者のアクセス、並びに情報及び情報処理設備の損傷または盗難を防止するため、利用者にパスワード及び利用する装置のセキュリティに関してその責任を認識させる。認可されていないアクセスまたは損傷のリスクを低減するために、クリアデスク・クリアスクリーン方針を適用する。内部及び外部のネットワークを利用したサービスへの認可されていないアクセスを防止するため、外部から接続する利用者の認証、ネットワークにおける装置の識別、ポートの保護、ネットワークの領域分割、接続制御、ルーティング制御を実施する。

オペレーティングシステムへの認可されていないアクセスを防止するため、ログオン手順、利用者の識別及び認証、パスワード管理システム、システムユーティリティの使用、セッションのタイムアウト、接続時間の制限などを利用する。業務用ソフトウェアシステムが保有する情報への認可されていないアクセスを防止するため、アクセス制限、システムの隔離などを行う。モバイルコンピューティング及び通信設備を用いた場合のリスクから保護する。テレワーキングのための方針、運用計画及び手順を策定し、実施する。

⑻情報システムの取得、開発及び保守

情報システムのセキュリティ要求事項は、設計、開発及び実装する前に特定し、合意した上で文書化する。業務用ソフトウェアにおける入力データ、内部処理、メッセージの完全性、及び出力データの妥当性確認を含める。情報を保護するための暗号の利用に関する方針を策定し、実施する。

組織における暗号技術の利用を支持するために鍵管理を実施する。

システムファイルのセキュリティを確実にするため、運用システムに係わるソフトウェアの導入を管理する手順を備える。システムファイル及びプログラムソースコードへのアクセス制御を実施する。業務用ソフトウェアシステムのソフトウェア及び情報のセキュリティを維持するため、プロジェクト及びサポート環境は厳しく管理する。変更によってシステムまたは運用環境のセキュリティが損なわれないことを点検するために、提案されているすべてのシステム変更のレビューを確実にする。情報の漏えいの可能性を抑止する。組織は、外部委託したソフトウェア開発を監督し、監視する。

利用中の情報システムの技術的ぜい弱性の管理は、効果的、体系的及び再現可能な方法で、その効果を確かめるための測定を伴って実施する。利用しているオペレーティングシステム及びあらゆる業務用ソフトウェアに適用する。

⑼情報セキュリティインシデントの管理

情報セキュリティインシデントに対する迅速、効果的で整然とした対応を確実にするため、責任体制及び手順を確立する。情報セキュリティインシデントの形態、規模及び費用を定量化し監視する。情報セキュリティインシデント後の個人または組織への事後処置が法的処置に及ぶ場合は、証拠を収集、保全及び提出する。

⑽事業継続管理

情報システムの重大な故障または災害の影響からの事業活動の中断に対処するとともに、それらから重要な業務プロセスを保護するため、組織全体を通じた事業継続管理手続きを策定し、維持する。事業活動及び重要な業務プロセスの時機を失しない再開を確実にするために、事業継続計画を策定し、実施する。すべての計画が整合したものになることを確実にするため、単一の事業継続計画策定の枠組みを維持する。事業継続計画が最新で効果的なものであることを確実にするため、定めに従って試験・更新する。

⑾順守

法令、規制または契約上のあらゆる業務、及びセキュリティ上の要求事項に対する違反を避けるため、各情報システム及び組織の取組み方を明確に定めて文書化し、最新に保つ。組織の記録の保護、個人データ及び個人情報の保護、情報処理施設の誤用防止、暗号化機能は、関連する協定、法令及び規制を順守する。組織のセキュリティ方針及び標準類へのシステムの順守を達成するため、セキュリティ手順が正しく実行されることを確実にする。情報システムをセキュリティ実施標準の順守に関して点検する。情報システムに対する監査手続きの有効性を最大限にするため、情報システム監査中には運用システム及び監査ツールを保護する。情報システムを監査するツールの誤用または悪用を防止するためにツールへのアクセスを抑制する。

付録３　情報セキュリティ監査の概要

付3.1　一部の保証と全体の保証

情報セキュリティ監査においては、情報セキュリティマネジメントシステムの一部を対象とした監査と全体を対象とする監査がありえる。

情報セキュリティマネジメントシステムのPDCAサイクルが、組織として有効に回っていることをみる場合には、対象となるマネジメントシステムの全体を対象として監査を行わなければ意味を成さない。ISMS認証の取得のために、組織の情報セキュリティマネジメントシステムを助言型情報セキュリティ監査により監査する場合などが、これに相当する。

対象となる情報セキュリティマネジメント全体を、情報セキュリティ管理基準をそのまま用いて監査する場合、用いる管理策の数は約130、詳細管理策レベルの数は約1000に達する。保証型情報セキュリティ監査で全体を保証する場合には、これらをすべて詳細に監査する必要があるため、監査費用の負担は少なくない。監査の経済合理性を考慮すると、範囲を限定することが望ましい。

一般的に保証型情報セキュリティ監査では、範囲を限定した一部の保証が行いやすい。たとえば、ISMS認証を取得し、PDCAサイクルが定着して情報セキュリティマネジメントシステムがある程度成熟してきた組織では、顧客の要請に基づいて保証型情報セキュリティ監査を行うニーズが生じてくる。この場合、マネジメントシステムの基本骨格が完成しているため、顧客の要請する範囲を絞り、より詳細な監査を行う。これが部分を対象とする情報セキュリティ監査である。

範囲の絞り方は情報セキュリティ監査目的によりさまざまである。例えば、リスクが大きい分野に絞って監査することで、全体のリスク管理レベルをより詳細に把握することなどが考えられる。

情報セキュリティ監査において、全体を対象とするか部分を対象とするかは、あくまでも監査目的をどのように設定するかに係るものであり、目的に対して最も合理的な監査手続きを選択する必要がある。

付3.2　保証型情報セキュリティ監査

現在、情報セキュリティ監査として行われる監査は主に助言型監査である。保証型監査については、経済産業省の情報セキュリティ監査研究会報告書に必要性が簡略に述べられているが、まだ概念や具体的手法に関して社会的に共通な理解があるわけではない。ここでは、日本セキュリティ監査協会において策定された「当面行うべき保証型情報セキュリティ監査」を中心に、概略を述べる。

1 保証型情報セキュリティ監査の必要性

情報セキュリティマネジメントシステムが正しく設計され、運用されているかを評価するためにISMS適合性評価制度がある。当該制度で審査に合格すると、情報セキュリティマネジメントシステムについて国際規格に適合していることが認められる。この制度があるにもかかわらず、なぜ保証型情報セキュリティ監査が必要とされるかを、ここでは述べることにする。

保証型情報セキュリティ監査の必要性は2つある。一つは、ISMS認証取得企業または同程度以上の

水準の情報セキュリティマネジメントシステムを行っている企業が、より精緻なリスク低減を顧客から要求され、実施している場合に、実際に高度なリスク管理を実施していることを顧客に保証する場合である。他の一つは、ISMSの認証は不要だが、顧客と必要な情報セキュリティ対策を約束し、その実施を顧客に保証する場合など、特定の管理策の実装と実施を保証する場合である。

(1)高度なリスク管理の保証

情報セキュリティマネジメントシステムにおいてはPDCAサイクルを確立し、情報セキュリティマネジメントの継続的改善を行うことが重要である。ISMS適合性評価制度の審査では、JIS Q 27001を基準として、これらの点を確認し、さらに、JIS Q 27002の管理策のうち、任意の項目をサンプルで確認し、的確な運用が行われていることを評価する。この審査で重大な不適合がなければ、認証が行われる。また、軽微な不適合については改善指摘を行い、継続的なマネジメントの向上を促している。

情報セキュリティマネジメントの継続的な向上により、ISMS認証取得後、ある程度の期間を経た企業では、顧客からリスク低減をより精緻に求められることが生じる。

ISMS適合性評価制度は、当該組織の情報セキュリティマネジメントシステムがJIS Q 27001というベストプラクティスの規格に適合しているかを評価するが、どの程度のリスク低減策を、どの程度精緻に行っているかを評価するものではない。

保証型情報セキュリティ監査が必要とされる第一の理由がこの部分にある。保証型情報セキュリティ監査では、顧客が期待する情報セキュリティの要求水準に対して、被監査主体が適正に管理策を実装し、運用しているかを監査し、監査人としての意見を表明するものである。

(2)特定の管理策の実装と実施の保証

ISMS認証取得には、時間と費用と労力が必要である。これらの制約から、ISMS認証取得を行わない、あるいは行えない企業がある。これらの企業でも、情報セキュリティマネジメントについての保証が必要な場合がある。

たとえば、委託業務において委託者が受託者に情報セキュリティの要求事項を提示し、受託者がそれを順守する義務を負う契約を締結する場合である。その際に、委託者が受託者を監査する、あるいは受託者から第三者監査報告の提出を求める場合がある。これらの場合に、保証型情報セキュリティ監査が必要となる。

(3)保証型情報セキュリティ監査の対象

保証型情報セキュリティ監査の保証対象は、4つの点に分けて考えることができる。

第一は、全体を保証するか、部分を保証するかという範囲に関わる点である。

論理的には被監査主体の情報セキュリティマネジメント全体を対象とする場合と、ある部分を対象とする場合が考えられる。ここで考えなければならないのは監査の経済合理性である。情報セキュリティマネジメントに保証を与えるためには、少なくとも情報セキュリティ管理基準の詳細管理策レベルで項目を検証することが必要である。これらの検証のためには、技術的な検証も欠かせない。そのために、さらに、検証する項目が増えることがある。被監査主体の情報セキュリティマネジメント全体を対象とする保証型情報セキュリティ監査では、少なくとも詳細管理策レベルである約1000項目を、十分な証拠を収集して検証することになる。このための情報セキュリティ監査の手間は膨大なものにならざるを得ない。そのための費用負担までして、保証を求める必要性がどこまであるかということが問われる。

高度なマネジメント水準の保証を受けようとする場合、被監査主体の情報セキュリティマネジメント全体については、少なくともISMSの認証を受けることで、ベストプラクティスを実装していることまで保証される。もちろんISMS認証取得によってもリスクは残留する。高度なマネジメント水準はこのような

残留リスクに対するマネジメントに対して必要となる。この中で、リスクの大きい部分に対象を絞って保証すれば、全体を保証することと結果が大きく異なることはない。情報セキュリティのリスクの大きい部分に対象範囲を限定し、保証型情報セキュリティ監査を実施することが経済合理性をもつといえよう。
一方、低度のマネジメント水準を保証する場合には、そもそも対象が限定されているので、全体を保証するということはない。これらのことから、保証型情報セキュリティ監査は、監査目的にあわせて、重要事項が欠落しないよう配慮しつつ合理的に範囲を設定する、部分を保証する情報セキュリティ監査が現実的である。

第二は、言明を保証するか、実態を保証するかという点である。
通常、情報セキュリティ監査は、被監査企業の経営者の言明を保証し、経営者の言明（Assertion；主張とも訳される）に対して信頼性を付与することを目的として行われる。会計監査においては、財務諸表が会計原則に則っている、あるいは企業の内部統制がとれていることを経営者が言明（主張）していると捉え、その言明の適正さを監査によって保証するという構図が描かれている。監査対象の情報セキュリティマネジメントシステムに責任を有する者（経営者など）が、その設計や運用において求められる水準を満たしているという言明が行われ、それが保証の対象となる。
情報セキュリティ監査では、言明を「被監査主体の経営者が、監査報告書の利用者に対して行う、『被監査組織において情報セキュリティに関するマネジメントとコントロールを適切に行っている旨』を内容とする主張」と定義している。また、言明の要件は次の3つである。
（1）言明の主体が示されていること
（2）監査の対象組織が一義的に定められていること
（3）監査人が監査するに足る内容の事実に関する主張が存在すること
言明という概念を用いるのは、監査主体が保証する対象を明確にすることと、監査主体と被監査主体の責任区分を明確に示すことの二つのためである。
上述のように、組織の情報セキュリティマネジメントのある部分を対象とした場合、その範囲で何を対象に保証するかを明確にしなければならない。監査主体、被監査主体、そして利害関係者という監査に関わる三当事者で共通の理解ができる対象がないと、保証が困難になる。情報セキュリティマネジメントには、会計原則のような社会的に合意され、確立した原則は存在せず、リスク対応についても組織の自主性に委ねられているため、三者間の共通理解が容易ではない。被監査主体の経営者が対象範囲のマネジメントについて、三者間で共通理解ができる内容の言明を行うことで、保証対象を明確にすることができる。
また、監査人の責任と経営陣の責任とは区別されなければならない。監査人は、監査対象が管理基準を満たしているかを判断することに責任があり、被監査主体の経営者が負うべき情報セキュリティ対策の実施責任は負っていない。経営者が言明によって実施責任を明確にすることで、その言明が信じるに足るとするか否かを判断する監査人の責任が明確になる。
なお、言明を対象としても、その言明が明らかに不適切である場合は保証型監査を実施しないなど、情報セキュリティの専門家である監査人として当然行うべき行為が求められる。
実態を保証する場合、あるいは言明を明記しない場合には、監査報告書に監査対象に対する経営者の責任を記述することが必要である。

第三は、設計と実装のどれを監査するかという点である。情報セキュリティ監査では、この二つに対して、設計監査と実装監査という用語を用いている。

設計監査は、情報セキュリティ対策の設計を対象とするもので、「情報セキュリティ対策設計監査」を短くしたものである。この設計監査は、設計されたコントロールの整備状況について保証するものであり、整備状況の監査ともいう。
実装監査は、組織が定めた（設計した）情報セキュリティ対策が設計どおりに行われていることを保証の内容とするもので、「情報セキュリティ対策実装・運用監査」を短くしたものである。運用状況の監査ともいう。
設計監査と実装監査のうち、どの監査を行うかは、監査目的などにより異なる。設計については了解が取れている場合は実装監査のみでよい。

第四は、ある時点について保証を与えるか、ある期間について保証を与えるかである。
ある時点における状況を監査結果として報告するものを時点監査という。この監査をする場合であっても、その時点よりも前の期間において情報セキュリティ対策の有効性について検証する必要がある。
ある期間の監査対象について、観察した事実あるいは言明などに対する意見を監査結果として報告するものを期間監査という。
情報セキュリティ監査においては過去の一定期間にわたって情報セキュリティのマネジメントとコントロールが有効に機能していたかどうかを保証の対象とするには、その証跡の確保が一部のコントロールには難しいなど、期間監査の実現にはまだかなり検討を要する事項が残されている。このため、当面は時点監査を中心に進めるのが妥当である。

2 保証型監査の概念フレームワーク

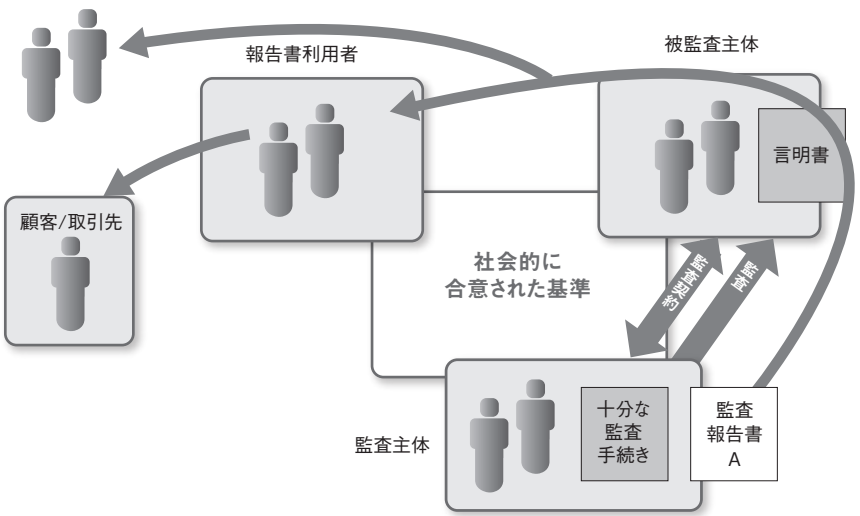
保証型監査では、監査主体、被監査主体、そして利害関係者という監査に関わる三当事者の間でどのような共通理解がなされるかによって、監査の方式が異なる。監査の方式には、社会的合意方式、利用者合意方式、被監査主体合意方式の三つがある。以下に、この三方式の概要を示す。

(1)社会的合意方式

社会的合意方式とは、社会的に合意された情報セキュリティ管理基準や監査基準に沿って、すべての利害関係者たり得る利用者にその結果を報告する方式である。監査は本来、この前提で構築されており、保証型の情報セキュリティ監査が目指すべき方向もここにあると考えられる。社会的合意方式における保証の対象は、被監査主体の経営者による言明である。この言明について、監査意見を表明する（監査意見表明方式）ものである。社会的合意の内容により、設計監査と実装監査の両者に基づき意見表明を行う場合と、実装監査のみで意見表明が可能な場合が考えられる。
監査人は、監査目的に適った監査範囲を対象として、監査人が必要と考える適切かつ十分な監査証拠を収集できる監査手続きを実施する。その結果を記載した監査報告書は、利用者を限定せず公開される。なお、監査報告書には、監査意見として「信じるに足る」という表現を用いることが検討されている。社会的合意方式は、現在の会計監査と同様の利用のされ方が想定される。被監査主体の情報セキュリティマネジメントに対する保証が必要な場合に、この監査が行われることになる。ただし、情報セキュリティマネジメントの水準に社会的な合意ができていなければ、保証の意味がないばかりか、いたずらに社会的混乱を招く恐れもある。社会的な合意形成のためには、情報セキュリティに関する共通の水準が意味を持つ、業界などの社会的に認められ組織が利用者との間で明確なセキュリティ要求事項を合意するなどのことが必要となる。

表付3.1　保証型監査の三方式

	社会的合意方式	利用者合意方式	被監査主体合意方式
適用可能な具体例	委託先の監査結果を広く利害関係者に公表したい場合	委託部分は全体の一部で、委託先に期待する水準が明確な場合	受託者に求められる事項の順守について保証を得たい場合
保証の内容	設計監査または実装監査	設計監査または実装監査	実装監査
保証の方法	意見表明方式	意見表明方式	結果報告方式
保証の対象	言明方式	言明方式	非言明方式 ※「同意された管理手続き」が経営者の言明に該当すると解釈できる
保証の対象とする期間	時点監査（期間監査も条件を満たせば可能）	時点監査（期間監査も条件を満たせば可能）	時点監査または期間監査
監査の対象範囲	監査の主題にかかわる重要部分を欠いていないこと	監査の主題にかかわる重要部分を欠いていないこと	被監査主体と合意し、利用者の確認を得た部分
監査報告書の利用者	不特定	特定された一次利用者に限定	特定された一次利用者に限定
監査手続き	監査人が必要と考える手続き	特定の監査報告書利用者と同意した、期待にこたえられる監査手続き	被監査主体と合意し、利用者の確認を得た監査手続
報告書の記載	信じるに足る	期待する水準にある	結果を報告する



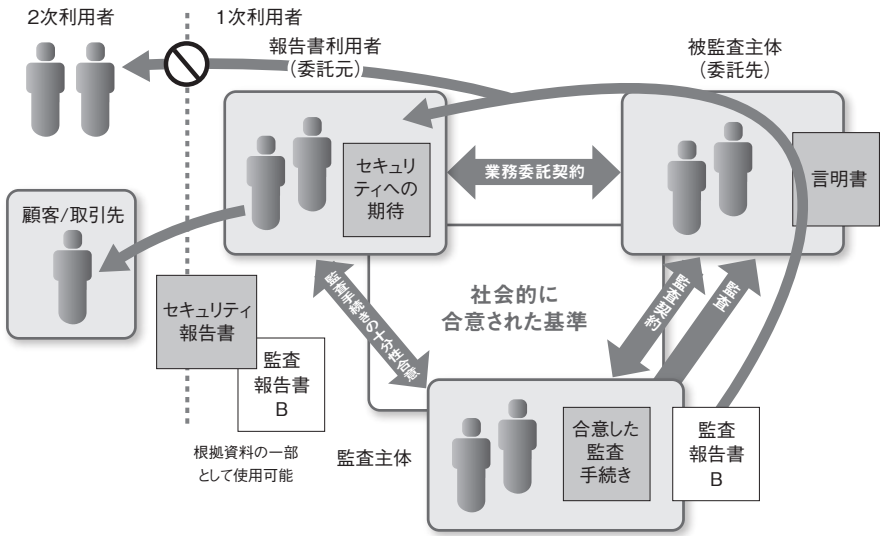
図付3.1　社会的合意方式

(2)利用者合意方式

利用者合意方式は、監査報告書の利用者が、被監査主体の情報セキュリティ対策に直接の利害関係を持ち、その適否や有効性に特定の期待や要求水準を示している場合に、監査人が利用者の期待する水準を満たしているかどうかを監査する方式である。業務委託関係にある委託元が委託先の監査において、委託元として期待している水準が満たされているかどうかに焦点を絞って行う監査に典型的に現れる方式である。

この場合の監査報告書利用者は、被監査主体と特定の利害関係を持つ利用者（1次利用者）に限定される。監査人は、1次利用者の期待する情報セキュリティ確保の要求水準を満たすかどうかを確認するに十分な監査手続きを実施し、その結果を意見として報告書に記載する。報告書の記述は、「期待する水準にある」という方向で検討されている。委託元の期待水準が明確で、設計に関して被監査主体と共有されている場合には、実装監査のみでよいが、そうではない場合には、設計監査と実装監査をあわせて行う必要がある。

監査報告書には、利用者と被監査主体との同意に基づくこと、及び報告書利用者が1次利用者に限定されることを明確に示さなければならない。

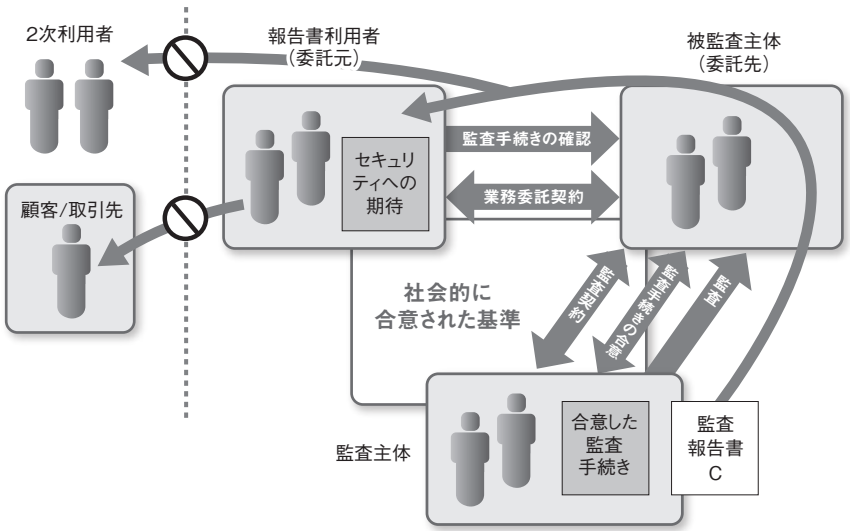


図付3.2　利用者合意方式

(3)被監査主体合意方式

被監査主体が、利害関係者に向けて説明するために、特定の監査テーマを定め、その監査手続きを監査人と相談し、合意の上で定める場合で、かつ、監査テーマと監査手続きについて監査報告書の利用者の確認が取れている場合の保証型監査の方式を、被監査主体合意方式という。監査人は、被監査主体の依頼を受けて、監査テーマに関して被監査主体と合意した監査手続きに従って、被監査主体が定めた情報セキュリティマネジメントの実態が存在するかどうかを主眼に監査を実施し、監査結果を報告する形をとる。

この場合、監査テーマと監査手続きが三当事者で了解されているため、被監査主体の経営者が自らの情報セキュリティを言明しなくても、監査結果について三当事者間で誤解が生じることはない。このため、非言明方式となることが想定される。この方式では、監査テーマや監査手続きが、被監査主体と監査主体の合意及び監査報告書1次利用者の確認により限定される。このため、内容を詳細に理解した当事者以外に監査報告書が開示されると誤解を生むことになる。報告書の取扱いは、厳正に管理しなければならない。このような監査は、開かれた市場において非常に突出した委託者が、情報セキュリティマネジメントについて大枠をガイドライン等で開示し、市場に参加する多数の受託候補企業がこれらを理解している状況において、適用されると想定される。受託候補企業が、その業務に対してガイドライン等に沿った情報セキュリティ対策の設計を自主的に行う。委託契約が締結された後の適切な時点で、ガイドライン等の設定趣旨に沿った対策が実際に行われているかを監査する。監査手続きについては、受託者と監査人との間で取り決める。この時に、委託者が監査手続きとガイドライン等を設定した趣旨に乖離がないかを確認することで、監査結果が有効性をもつ。ガイドライン等が共有されているので、監査はガイドライン等の項目ごとに監査手続きを実施し、適切に行われている事項、必ずしも十分でない事項を事実として、結果のみを報告書に記載することになる。



図付3.3　被監査主体合意方式

3 保証型監査の実施にあたって

保証型監査は、監査報告書利用者が被監査主体の企業以外であることが多いと考えられる。このため、誤った監査結果がもたらす社会的な影響が助言型監査に比較して大きい。保証型監査を実施するにあたっては、この点を十分に認識して対応することが肝要である。

第一に、監査リスクをより厳しく評価しなければならない。監査に適さない組織や意見表明が行えないことが十分に予想される場合には、監査を実施しないことが重要である。

第二に、監査人の独立性を、助言型監査以上に厳しく守ることが必要である。

第三に、監査チームの編成にあたって、専門性を十分に発揮できるようにする必要がある。情報セキュリティ監査で保証を与えるためには、技術的な検証が重要な役割を担うと考えられる。情報セキュリティに関わる技術は非常に細分化され、また深いので、各々に合わせた専門家を結集することに配慮すべきである。

第四に、監査証拠は質・量共に適切かつ十分になるようにしなければならない。収集した事象について証拠能力を吟味し、保証するに足る証拠に基づき、誤りのない意見形成を行うことが必要である。

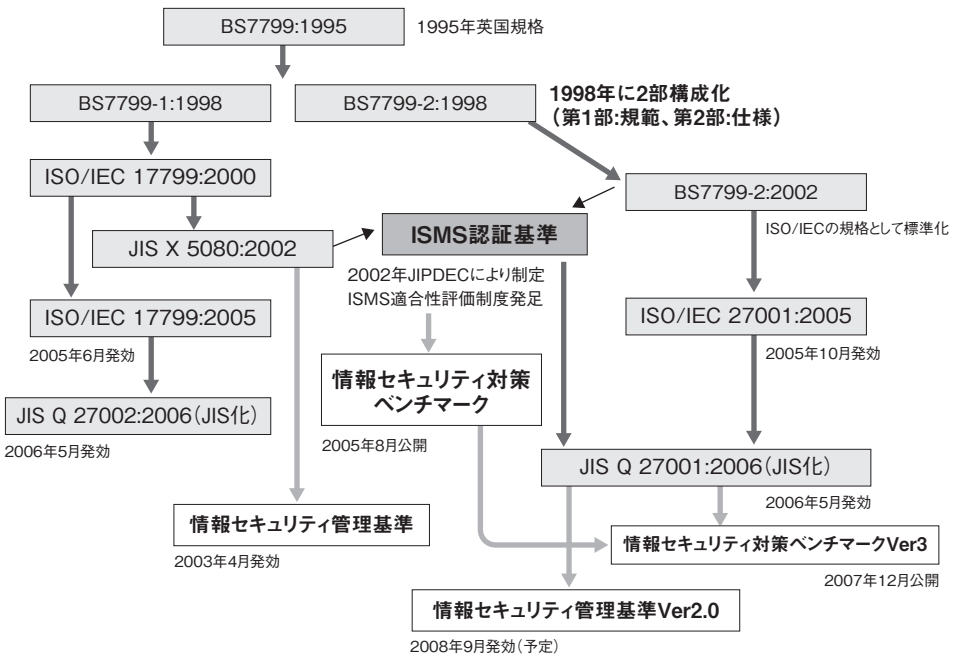
この他、監査品質を高く保つために、しっかりとした体制で適確な監査を実施することも必要である。

付録 4　情報セキュリティマネジメントに関する規格類

付4.1　情報セキュリティマネジメントの規格

情報セキュリティ管理策の選定にあたってよく参照されるのは、JIS Q 27002である。この規格は、ISO/IEC17799として2000年に初めて国際標準化されたのち、2005年に改訂された。その規格がJIS化されたのがJIS Q 27002：2006である。この規格は、情報セキュリティ対策を行う際の実践の模範となるベストプラクティスを記したものであり、さまざまな推奨管理策が記載されている。一方、ISMS適合性評価制度の認証基準であるJIS Q 27001：2006は、国際規格のISO/IEC 17799：2005をJIS化したものである。(両規格とも2006年5月に発効)。

これら2つの規格は、もとはBS7799というひとつの規格であった。**図付4.1**にBS7799からJIS Q 27002：2006、情報セキュリティ管理基準までの流れを示す。



図付4.1　情報セキュリティマネジメントの規格

BS7799は、1995年にBSI (British Standards Institution：英国規格協会) により制定された情報セキュリティマネジメントシステムの英国規格である。BS7799は、1998年にはBS7799-1 (Part1)、BS7799-2 (Part-2)の二部構成となり、2000年にはPart1がISO/IEC 17799：2000として国際標準化され、それに伴い英国規格もBS7799-1:2000として改正された。Part2はその後、プロセスアプローチ、PDCAサイクル、継続的改善等の考えを盛り込み、BS7799-2：2002となった。

日本では、ISO/IEC 17799：2000はJIS X 5080：2002としてJIS化された。一方、BS7799-2：2002をもとにISMS認証基準Ver.1.0が策定され、2002年4月にはこの基準にもとづくISMS適合性評価制度が稼動し始めた。その後、2003年4月にはこの基準はISMS認証基準Ver.2.0として改定された。同じ2003年4月に、JIS X 5080：2002に準拠した情報セキュリティ管理基準が経済産業省より告示された。また、2005年にBS7799-2：2002がISO/IEC 27001：2005として国際規格化され、さらにJIS Q 27001：2006としてJIS化されたのに伴い、この規格がISMS適合性評価制度の準拠する規格となった。準拠する規格の変更に伴い、情報セキュリティ管理基準も情報セキュリティ管理基準Ver.2.0に改定される（2008年9月予定）。

これらの規格のほかに、27000シリーズとしてISMS実装のガイダンス（ISO/IEC 27003 ISMS Implementation Guidance）やISMSリスクマネジメント（ISO/IEC 27005 ISMS Risk Management）などの規格が策定中である。

なお、2006年8月に公開された情報セキュリティ対策ベンチマークの25の評価項目は、ISMS認証基準Ver.2.0をもとに作成され、2007年12月に公開された情報セキュリティ対策ベンチマークVer.3の25の評価項目は、JIS Q 27001：2006をもとに作成されている。

付4.2 JIS Q 27001とJIS Q 27002

1 JIS Q 27001とJIS Q 27002

「JIS Q 27002：2006情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範」には、11の管理領域と133の管理策が記載されている。管理策はcontrol（コントロール）の訳語であり、そのため、管理策を「コントロール」と呼ぶこともある。**図付4.2**にJIS Q 27002：2006の構成を示す。

管理領域（箇条）	カテゴリ	管理策
5. 情報セキュリティ基本方針	1	2
6. 情報セキュリティのための組織	2	11
7. 資産の管理	2	5
8. 人的資源のセキュリティ	3	9
9. 物理的及び環境的セキュリティ	2	13
10. 通信及び運用管理	10	32
11. アクセス制御	7	25
12. 情報システムの取得、開発及び保守	6	16
13. 情報セキュリティインシデントの管理	2	5
14. 事業継続管理	1	5
15. 順守	3	10
合計	39	133

JIS Q 27002（ISO/IEC 17799：2005）の構成

11の管理領域と133の管理策

各領域にセキュリティカテゴリがあり、各セキュリティカテゴリには、管理策、実施の手引き、関連情報が含まれる

【例】

14.事業継続管理：1つのカテゴリと5つの管理策

14.1	事業継続管理における情報セキュリティの側面
14.1.1	事業継続管理手続への情報セキュリティの組込み
14.1.2	事業継続及びリスクアセスメント
14.1.3	情報セキュリティを組み込んだ事業継続計画の策定及び実施
14.1.4	事業継続計画策定の枠組み
14.1.5	事業継続計画の試験、維持及び再評価

図付4.2　JIS Q 27002：2006の構成

11の管理領域にはそれぞれセキュリティカテゴリがあり、各セキュリティカテゴリには、39の管理目的と133の管理策のほかに、実践の手引きや関連情報が含まれる。実践の手引きなどを参照し、133の管理策を、さらに1000近くのサブコントロールに詳細化できる。

これらは、さまざまなベストプラクティス（実践の模範となる管理策）の集大成であり、網羅的、汎用的である。組織によっては、採用する必要のないコントロール（またはサブコントロール）がある反面、特定の業務にとっては、追加の管理策が必要な場合もあり、組織は、これらの管理策から自組織にあったものを適宜取捨選択したり、別途必要な管理策を追加したりする。

ISMS適合性評価制度の認証基準である「JIS Q 27001：2006情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項」には、ISMS認証取得のための要求事項や手引きが記載されている。ISMS認証を取得するための要求事項には、必須のものと除外可能なものがある。JIS Q 27001の「4．情報セキュリティマネジメントシステム」「5.　経営陣の責任」「6. ISMS内部監査」「7. ISMSのマネジメントレビュー」「8. ISMSの改善」に記載の要求事項は、認証取得には必須であり、除外することはできない。

JIS Q 27001附属書Aには、JIS Q 27002と同じ管理目的と管理策が記載されているが、その取捨選択は利用者の自由裁量に任されているJIS Q 27002のスタンスとは違い、JIS Q 27001においては、その選択は基本的には任意だが、除外する場合、その管理策がなぜ必要で、なぜ不要かの根拠をリスクアセスメントの結果に基づき示すことが求められる。また、経営陣や責任者が判断して正式に残留リスクの受容が決定されたことを示す証拠を、文書（適用宣言書）に記載する必要がある。さらに、個々の組織の状況に応じて管理策を追加する場合には、JIS Q 27002の実践の手引きや関連情報、及び公的基準あるいは業界基準など、さまざまなベストプラクティスを利用する。**図付4．3**にJIS Q 27001とJIS Q 27002の関係を示す。

なお、管理目的と管理策の概要は、「付2.7 管理目的及び管理策」を参照されたい。

JIS Q 27002：2006
(ISO/IEC 17799：2005)
（情報セキュリティマネジメントの実践のための規範）

管理領域（箇条）	カテゴリ	管理策
5. 情報セキュリティ基本方針	1	2
6. 情報セキュリティのための組織	2	11
7. 資産の管理	2	5
8. 人的資源のセキュリティ	3	9
9. 物理的及び環境的セキュリティ	2	13
10. 通信及び運用管理	10	32
11. アクセス制御	7	25
12. 情報システムの取得、開発及び保守	6	16
13. 情報セキュリティインシデントの管理	2	5
14. 事業継続管理	1	5
15. 順守	3	10
合計	39	133

JIS Q 27001：2006
(ISO/IEC 27001：2005)

0.1 序文
0.2 ISMSの採用
（ISMSに適用されるPDCAモデル）
1. 適用範囲
2. 引用規格
3. 用語及び定義

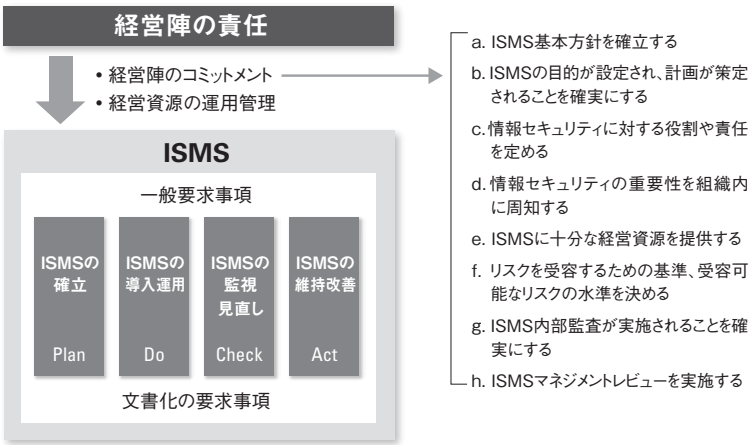
4. 情報セキュリティマネジメントシステム
5. 経営陣の責任
6. ISMS内部監査
7. ISMSのマネジメントレビュー
8. ISMSの改善

附属書A（規定）
管理目的及び管理策

図付4．3　JIS Q 27001とJIS Q 27002の関係

2 JIS Q 27001の要求事項

ISMS適合性評価制度では、組織が構築した情報セキュリティマネジメントシステムが、ISMS認証基準であるJIS Q 27001の要求事項に適合しているかどうかが評価される。JIS Q 27001の要求事項については、「付録2 ISMS適合性評価制度の概要」に詳しい説明があるため、ここでは、そのコンセプトを図示するに留める。



図付4.4　JIS Q 27001の一般要求事項と経営陣の責任

JIS Q 27001では、情報セキュリティに対する経営陣のコミットメントと責任が強く求められる。また、一般要求事項は、ISMSにおけるPDCAサイクルに従いまとめられており、組織は、ISMSに関わる方針や記録を文書として作成、保管することが求められる。**図付4.5**に、PDCAサイクルの各段階における一般要求事項の細目を示す。

ISMSの確立	ISMSの導入運用	ISMSの監視見直し	ISMSの維持改善
1. 適用範囲と境界の定義	1. リスク対応計画の策定	1. 監視・見直しの手順実施	1. 改善策の実施
2. 基本方針の策定	2. リスク対応計画の実施	2. 有効性の定期的見直し	2. 是正措置・予防措置の実施
3. リスクアセスメントの取り組み方法	3. 管理策の実施	3. 管理策の有効性測定	3. 利害関係者への処置の伝達
4. リスクの識別	4. 管理策の有効性評価	4. リスクアセスメントの見直し	4. 改善による意図した目的の達成
5. リスクの分析・評価	5. 教育訓練及び認識プログラム	5. 内部監査の実施	
6. リスク対応の選択肢の評価	6. ISMSの運用管理	6. マネジメントレビューの実施	
7. 管理策の選択	7. ISMS経営資源の管理	7. セキュリティ計画の更新	
8. 残留リスクの承認	8. インシデント対応	8. 活動・事象の記録	
9. ISMSの承認			
10. 適用宣言書の作成			
P	D	C	A

図付4.5　PDCAサイクルの各段階における一般要求事項

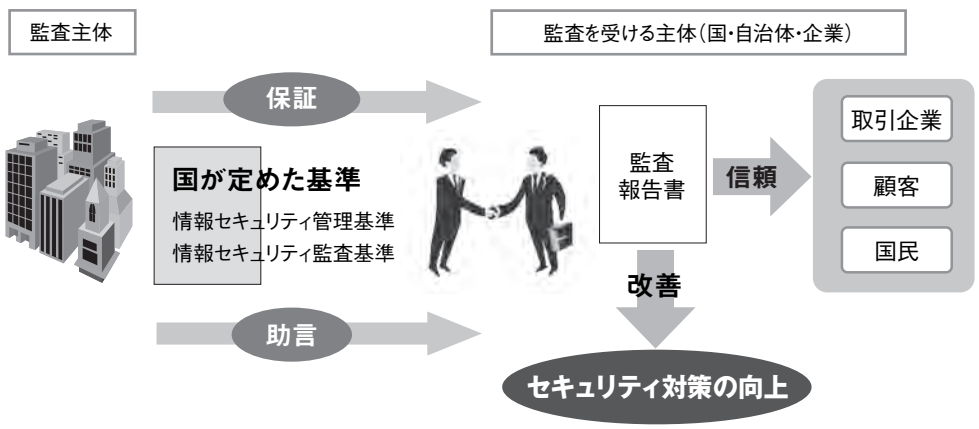
3 情報セキュリティ対策ベンチマークの25の評価項目

情報セキュリティ対策ベンチマークの評価項目は、JIS Q 27001附属書Aの管理策（133項目）をもとに、25項目に整理されている。また、組織的対策、物理的対策、技術的対策など、組織に必要なセキュリティ対策を網羅している。それぞれの評価項目に付随している対策のポイントは、合計で146項目あり、情報セキュリティ対策ベンチマークを使ってより詳細な評価をしたい場合は、これらの対策のポイントを利用することもできる。

表付4.1　JIS Q 27001の管理領域と情報セキュリティ対策ベンチマークの評価項目

JIS Q 27001附属書A		情報セキュリティ対策ベンチマーク（大項目と質問・対策のポイント）		
情報セキュリティ管理領域	管理策数	大項目名称		
1. 情報セキュリティ基本方針	2	1. 情報セキュリティに対する組織的な取組状況		7
2. 情報セキュリティのための組織	11			
3. 資産の管理	5			50
4. 人的資源のセキュリティ	9			
11. 順守	10			
5. 物理的及び環境的セキュリティ	13	2. 物理的（環境的）セキュリティ上の施策		4 22
6. 通信及び運用管理	32	3. 情報システム及び通信ネットワークの運用管理		6 33
7. アクセス制御	25	4. 情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況		5
8. 情報システムの取得開発及び保守	16			25
9. 情報セキュリティインシデントの管理	5	5. 情報セキュリティ上の事故対応状況		3
10. 事業継続管理	5			16
11領域	133	大項目5	質問数	25
			対策のポイント数	146

4 情報セキュリティ管理基準

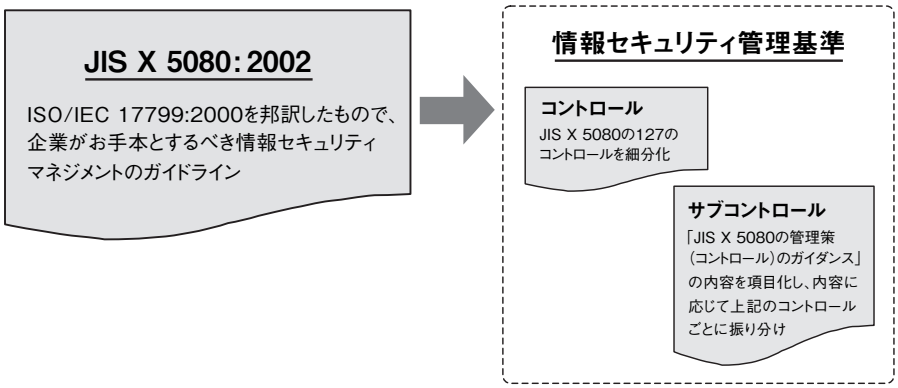


図付4.6　情報セキュリティ監査制度の概要

2003年4月、情報セキュリティ監査制度が経済産業省の告示として公表された。(1) 企業等の情報セキュリティ対策（外部からの不正アクセス防止の設定をしているか、情報管理責任者を任命しているか等）について、(2) 客観的に定められた国の基準に基づいて、(3) 独立した専門家が、(4) 評価（保証または助言）する制度であり、「情報セキュリティ管理基準」及び「情報セキュリティ監査基準」からなる。なお、監査主体は「情報セキュリティ監査企業台帳」に登録され、毎年7月に更新される。**図付4.6**に情報セキュリティ監査制度の概要を示す。

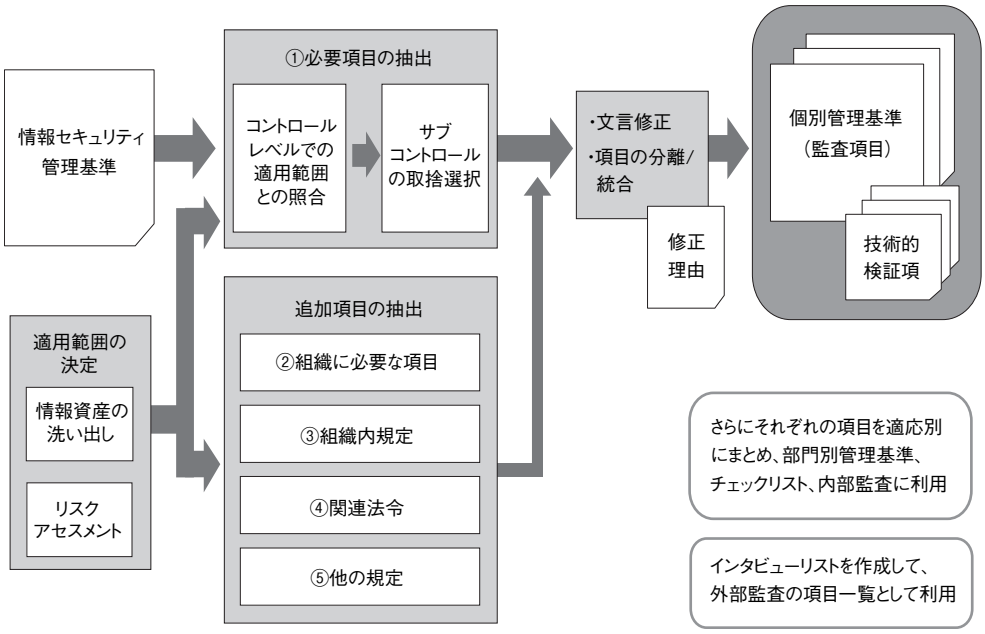
この情報セキュリティ監査制度における根幹となる基準の一つである情報セキュリティ管理基準は、組織体が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロールを整備、運用するための実践規範である。情報セキュリティマネジメントは、第一義的には、組織体における必要性と組織体の責任において果たされるべきものであり、情報セキュリティマネジメントの基本的な枠組みと具体的な管理項目を規定することによって、組織体が情報セキュリティマネジメント体制の構築と、適切なコントロールの整備と運用を効果的に導入できるように支援することを目的としている。

本管理基準は、情報セキュリティに係るマネジメントサイクル確立のための国際標準規格であるISO/IEC 17799：2000（JIS X 5080：2002）をもとにしており、情報資産を保護するための最適な実践慣行を帰納、要約し、情報セキュリティに関する、マネジメント及びコントロールの項目を規定したものであり、全体で127のコントロール（管理策）及びそれを詳細化した952のサブコントロールから構成されている。**図付4.7**に情報セキュリティ管理基準の構成を示す。



図付4.7　情報セキュリティ管理基準の構成

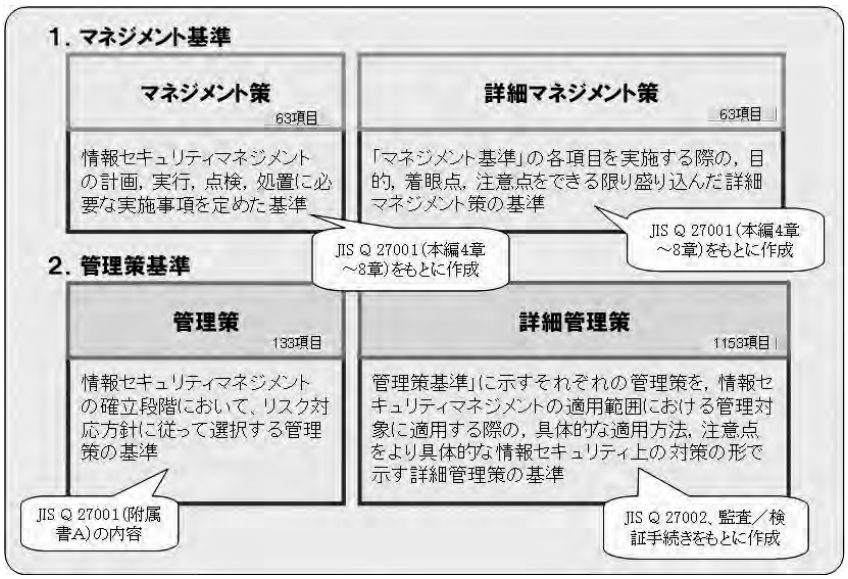
本管理基準は、組織体の業種及び規模等を問わず適用できるよう汎用的なものとなっている。組織体においては、本管理基準を基礎として、リスクアセスメントの結果等に基づき、独自に必要とする項目を追加、あるいは削除して、個別管理基準を作成することができる。ただし、情報セキュリティは、個々のマネジメント及びコントロールの項目が相互に結びつき合ってはじめて有効に機能するものであり、また、計画、実施、評価、是正を通じたマネジメントサイクルとして機能するように留意しなければならない。次頁 **図付4.8**に、個別管理基準作成までの流れを示す。



図付4.8　個別管理基準作成までの流れ

なお、本管理基準は、準拠する規格がJIS X 5080:2002からJIS Q 27001:2006に変更されたことに伴い、情報セキュリティ管理基準Ver.2.0へ改定される（2008年9月予定）。

図付4.9に情報セキュリティ管理基準Ver2.0の構成を示す。



図付4.9　情報セキュリティ管理基準Ver2.0の構成

情報セキュリティ対策
ベンチマーク活用集

資料

資料１　情報セキュリティ対策ベンチマークの質問一覧

情報セキュリティ対策ベンチマークver.3　25項目の質問一覧

大項目1．情報セキュリティに対する組織的な取組状況	
①	情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。
②	経営層を含めた情報セキュリティの推進体制やコンプライアンス（法令順守）の推進体制を整備していますか。
③	重要な情報資産（情報及び情報システム）を、その重要性のレベルごとに分類し、さらにレベルに応じた表示や取扱いをするための方法を定めていますか。
④	重要な情報（たとえば個人データや機密情報など）については、入手、作成、利用、保管、交換、提供、消去、破棄などの一連の業務プロセスごとにきめ細かくセキュリティ上の適切な措置を講じていますか。
⑤	外部の組織に業務や情報システムの運用管理を委託する際の契約書には、セキュリティ上の理由から相手方に求めるべき事項を記載していますか。
⑥	従業者（派遣を含む）に対し、採用、退職の際に守秘義務に関する書面を取り交わすなどして、セキュリティに関する就業上の義務を明確にしていますか。
⑦	経営層や派遣を含む全ての従業者に対し、情報セキュリティに関する自組織の取組みや関連規程類について、計画的な教育や指導を実施していますか。
大項目2．物理的（環境的）セキュリティ上の施策	
①	特にセキュリティを強化したい建物や区画に対して、必要に応じたセキュリティ対策を実施していますか。
②	顧客、ベンダーや、運送業者、清掃業者など、建物に出入りする様々な人々についてセキュリティ上のルールを定め、それを実践していますか。
③	重要な情報機器や配線などは、自然災害や人的災害などに対する安全性に配慮して配置または設置し、適切に保守していますか。
④	重要な書類、モバイルPC、記憶媒体などについて適切な管理を行っていますか。
大項目3．情報システム及び通信ネットワークの運用管理	
①	情報システムの運用に際して、運用環境や運用データに対する適切な保護対策が実施されるよう、十分に配慮していますか。
②	情報システムの運用に際して、必要なセキュリティ対策を実施していますか。
③	不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウェアなど）への対策を実施していますか。
④	導入している情報システムに対して、適切なぜい弱性対策を実施していますか。
⑤	通信ネットワークを流れるデータや、公開サーバ上のデータに対して、暗号化などの適切な保護策を実施していますか。
⑥	モバイルPCやUSBメモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などを想定した適切なセキュリティ対策を実施していますか。
大項目4．情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況	
①	情報（データ）や情報システムへのアクセスを制限するために、利用者IDの管理、利用者の識別と認証を適切に実施していますか。
②	情報（データ）や情報システム、業務アプリケーションなどに対するアクセス権の付与と、アクセス制御を適切に実施していますか。
③	ネットワークのアクセス制御を適切に実施していますか。
④	業務システムの開発において、必要なセキュリティ要件を定義し、設計や実装に反映させていますか。
⑤	ソフトウェアの選定や購入、情報システムの開発や保守に際して、セキュリティ上の観点からの点検をプロセスごとに実施するなど、適切なプロセス管理を実施していますか。
大項目5．情報セキュリティ上の事故対応状況	
①	万が一システムに障害が発生しても、必要最低限のサービスを維持できるようにするため、情報システムに障害が発生する場合をあらかじめ想定した適切な対策を実施していますか。
②	情報セキュリティに関連する事件や事故が発生した際に必要な行動を、適切かつ迅速に実施できるように備えていますか。
③	何らかの理由で情報システムが停止した場合でも、必要最小限の業務を継続できるようになっていますか。

情報セキュリティ対策ベンチマークVer.3 質問と対策のポイント

大項目1. 情報セキュリティに対する組織的な取組状況

①情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。

ポリシーや規程は、サンプルのコピーではなく、自組織の事業やリスクを鑑みた内容であることが重要です。また、そうしたポリシーや規程を実践するためには、定めた規程類を関係者に十分に周知させると共に、規程類の順守状況を点検し、必要に応じて見直すことが大切です。

説明 ポリシーや規程を組織にとって有効なものとするためには、自組織の状況に見合った内容にする必要があります。そのためには、サンプルのコピーではなく、自組織の事業やリスクを鑑みた内容とすることが重要です。また、対策の実効性を確保するためには、定めた規程類を役員や全従業員に対して十分に周知すると共に、規程類の順守状況を適宜点検し、必要に応じて見直すことが大切です。

対策のポイント

1. 情報セキュリティポリシーや管理規程が策定されているか
2. ひな形、サンプルなどのコピーではなく、組織内での十分な討議や検討を経て、自組織の事業やリスクに見合った内容となっているか
3. ポリシーは全組織をカバーしているか
4. 組織の長ないし上級役員が承認しているか
5. 全従業者（派遣を含む）や関連する外部関係者に対して周知させているか
6. 定期的に見直すための手続を定めているか
7. あらかじめ定められた間隔、または重大な変化が発生した場合に、見直しを実施したか
8. 改訂結果について、組織の長ないし上級役員の承認を得て、再度周知したか
9. 従業員がポリシーや関連規程類を順守していることを点検・監査するための手続を定めているか
10. 組織内の情報セキュリティ対策や情報システムに関する点検や監査の実施を推進しているか
11. 情報システムが、業務以外の目的で利用されることを防止するための措置を講じているか
12. 情報システムに対し、いわゆるネットワーク検査やモニタリングを行うなどして、ポリシーの実施状況を確認しているか

②経営層を含めた情報セキュリティの推進体制やコンプライアンス(法令順守)の推進体制を整備していますか。

推進体制を整備するためには、経営層がリーダシップを発揮すること、各担当者の権限と責任を明文化することなどが重要です。また、法令順守のためには、順守すべき法令を正確かつ網羅的に把握することが必要です。

説明 推進体制を整備するためには、経営層がリーダシップを発揮すること、各部署の活動を調整する組織を整備すること、各担当者の権限と責任を明文化することなどが重要です。また、法令順守のためには、順守すべき法令などを正確かつ網羅的に把握することが必要です。さらに、組織の活動に関する説明責任を果たすため、種々の活動に関する記録を残すと共に、特に法令などによって保存が求められる文書については、記録を適切に保護することが求められます。

対策のポイント

1. 組織内の情報セキュリティのあり方を決定したり、各部署の活動を調整したりする組織が整備されているか
2. その組織の責任者は経営層の人間が担当しているか
3. その組織において、情報セキュリティに関する適切な責任や資源配分を検討しているか
4. 単独行動による不正行為をけん制するため、職務や権限を適切に分離しているか
5. 関係当局や情報セキュリティの専門家との連絡体制を構築しているか
6. 事業を遂行する上で順守すべき法令、基準、規制などを網羅的に、かつ正確に把握しているか
7. 他者の知的財産権を保護するための手続を定め、それを実践しているか（たとえば、ソフトウェアの不正コピーを予防するための手当てなど）
8. 個人情報を保護するために必要な対策を定め、それらを実施しているか
9. 不正競争防止法で保護される情報の要件を把握しているか
10. 自組織が実施した様々な活動について、それらを記録する仕組みはあるか
11. 特に法定の保存文書について、厳格な管理を実施しているか

③重要な情報資産（情報及び情報システム）を、その重要性のレベルごとに分類し、さらにレベルに応じた表示や取扱をするための方法を定めていますか。

情報資産をその重要性に応じて管理するためには、レベル分け、レベルに応じた表示や取扱方法などの指針及び情報の管理責任者を定める必要があります

説明 情報セキュリティ対策を効率的に、かつ高いコスト効果をもって実施するためには、重要な情報資産をあらかじめ把握するとともに、その情報資産の重要度に応じて管理することが必要です。また、情報資産の管理責任者や利用できる人の範囲などを情報資産の重要度に応じて、あらかじめ定めておくことで、取扱がずさんになることを防ぎます。その際、管理すべき情報資産には、情報システムだけでなく情報そのものも含むこと、また情報は、電子媒体に限らず紙媒体などについても管理が必要であることに留意する必要があります。

対策のポイント

1. 重要な情報資産の目録を作成しているか
2. 情報資産の管理責任者を明確に定めているか
3. 情報の重要性に応じた分類及び取扱いの指針を定めているか
4. 情報システムから出力した情報についても、重要性のレベルや取扱いが明確になっているか
5. 分類及び取扱いの指針に従って情報を分類した上で、重要性のレベルに応じた表示と取扱いを行っているか
6. 情報資産を利用できる部署や人などの範囲を定めているか

④重要な情報（たとえば個人データや機密情報など）については、入手、作成、利用、保管、交換、提供、消去、破棄などの一連の業務プロセスごとにきめ細かくセキュリティ上の適切な措置を講じていますか。

適切な措置とは、業務プロセスごとの作業責任者や作業手順の明確化、取扱者の限定、処理の記録や確認などを指します。また、業務プロセスは、手作業で行うか、情報システムに依存するかを問いません。

説明 重要情報の入手、作成、利用、保管、交換、提供、消去、破棄などに当たっては、そうした一連の業務プロセスごとの作業責任者や作業手順の明確化、取扱者の限定、処理の記録や確認などが必要です。

対策のポイント

1. 各業務プロセスにおける作業責任者や作業手順を明確化し、その手順に基づいて作業を実施しているか
2. 各業務プロセスにおける作業を適切な担当者のみに限定し、その作業担当者の認証や権限付与の状況を確認しているか
3. 重要情報に対するアクセスの記録・保管、権限外作業の有無の確認など、対策の実施状況を把握しているか
4. 組織内外での情報の交換について、ルールと手順を定め、その手順に基づいて作業を行っているか
5. 重要な情報が消失、変更、誤用されないよう、操作ミスを考慮した運用方法を定めているか
6. 重要な情報について、漏えいや不正利用を防ぐために、保護対策を実施しているか

⑤外部の組織に業務や情報システムの運用管理を委託する際の契約書には、セキュリティ上の理由から相手方に求めるべき事項を記載していますか。

セキュリティ上の理由とは、たとえば情報の漏えいや消失、情報あるいは情報システムの誤用などの防止を指します。

説明 外部の組織に業務を委託する際の契約書には、情報の漏えいや消失の防止、情報あるいは情報システムの誤用の防止を徹底するために、それらに関する条件を記載しておく必要があります。記載すべき条件には、委託先が実施すべき業務の内容、委託先が提供するサービスに関するサービスレベルの保証、委託先が委託業務に関して実施すべき安全管理措置などがあります。さらに、そうした契約条件に沿って適切に業務が遂行されていることを確認するため、報告や記録を求めることも大切です。

対策のポイント

1. 委託業務に際して締結する契約書に、業務内容、サービスレベル及び委託先に提供する重要な情報に関する安全管理措置や機密保持などの責任などを明確に定め記載しているか
2. 委託業務の確実な実施や委託先でのセキュリティ対策実施状況を報告や記録により確認しているか
3. 委託業務内容の変更について把握し、記録しているか

⑥従業者（派遣を含む）に対し、採用、退職の際に守秘義務に関する書面を取り交わすなどして、セキュリティに関する就業上の義務を明確にしていますか。

従業者に情報セキュリティについての要求を順守させるためには、従業者の管理責任者を明確にし、従業者が守るべきルールなどを明確にし、それらを周知させておく必要があります。

説明 すべての従業者に対して、採用や退職の際に、セキュリティ上の義務や、退職後の守秘義務など、セキュリティ上の順守事項を誓約させることで、注意義務を自覚させるとともに、就業規則や服務規律などに明示するなどして、情報セキュリティ対策に実効性を持たせます。さらに、退職や異動に際しては、貸与した資産の返却を確認すること、付与したアクセス権限を削除することも大切です。

対策のポイント

1. 従業者（派遣を含む）を採用する際に、経歴、資格などが職務にふさわしいかを十分に審査し、さらに守秘義務契約を締結しているか
2. 雇用契約時に、セキュリティ上の義務を明示しているか
3. 就業規則ないし服務規律に、従業員が順守すべき事項を明示しているか
4. 退職に際して、情報資産の返却確認やアクセス権限の削除を確実に行っているか
5. 退職に際して、退職後における守秘義務を退職予定の従業者に再確認しているか
6. セキュリティ違反を犯した従業員に対する懲戒手続を整備しているか
7. 採用から雇用、退職まで、従業員の管理を行う体制と責任が明確になっているか

⑦経営層や派遣を含む全ての従業者に対し、情報セキュリティに関する自組織の取組や関連規程類について、計画的な教育や指導を実施していますか。

情報セキュリティ教育は、全員に漏れなく定期的に行うことが大切です。セキュリティ対策上の順守事項、禁止事項の徹底とともに、情報セキュリティの脅威と対策についても教育します。

説明 従業者に対する教育は、情報セキュリティ対策の有効性を向上させるために必要不可欠です。関係者全員に対する教育を適切に実施し、その効果が得られていることを確認することによって、技術的なセキュリティ対策との相乗効果を期待できます。特に、保護すべき情報資産へのアクセス管理を確実なものとするために、パスワードや鍵の管理の徹底はとても大切です。

対策のポイント

1. ポリシー及び関連規程を従業者（派遣を含む）が理解し、実践するために必要な教育を実施しているか
2. パスワードの管理や暗号鍵の管理について教育を行なっているか
3. 単に出来合いの教材だけでなく、自組織の状況に即した適切な教材を用意しているか
4. 教育は、定期的に、従業者全員に漏れなく実施しているか
5. 教育が有効であることを確認するための手立てを用意しているか

大項目2. 物理的（環境的）セキュリティ上の施策

①特にセキュリティを強化したい建物や区画に対して、必要に応じたセキュリティ対策を実施していますか。

特にセキュリティを強化したい建物や区画については、ゲートや間仕切りを設けるなどして、境界を明確にし、入退館や入退室管理を実施する、あるいは警報装置の設置などを行います。また、荷物の受渡し場所や外部者の作業場所を確保するなど、セキュリティを考慮して物理的に区域を分けるようにします。

説明 重要な情報や関連する設備が数多く存在する場所については、セキュリティ対策として特段の配慮が必要となります。このような場所（建物や区画）については、入室可能な人をできるだけ制限したり、外部からの侵入者に対する防護策を強化したりすることが必要です。対策としては、ゲートや間仕切りを設けるなどして、境界を明確にし、入退館や入退室管理を実施する、あるいは警報装置の設置などを行います。また、荷物の受渡し場所や外部者の作業場所の確保、外来者の来訪履歴の保管も大切です。

対策のポイント

1. 特にセキュリティを強化したい物理的区域を定め、この区域の内外において順守すべきセキュリティ上の規程を整備しているか
2. 侵入を防止するために必要な建物や警報設備などの基準を設定しているか
3. 敷地及び建物に入ることができる人を制限しているか
4. その制限の対象になる人を識別できるようにしているか
5. 入退館（室）の履歴を記録し、その記録を適切に管理しているか
6. 訪問者や清掃業者などの立ち入りできる区域が明確になっているか

②顧客、ベンダーや、運送業者、清掃業者など、建物に出入りする様々な人々についてセキュリティ上のルールを定め、それを実践していますか。

自組織の建物や事務所には、思ったよりも多くの外来者が出入りしている事があります。そうした外来者に守って頂くべきルールをあらかじめ定めておくことが重要です。

説明 建物や事務所の中には、数多くの情報や関連する設備が所在しています。これらの情報や設備に触れる機会のある外来者に対しては、それぞれのリスクの状況を踏まえたルールの制定と、それに従った運用を行うことが必要です。

対策のポイント

1. 外部の人々の出入りによって、どのようなリスクが生じるかを検討し、その結果、明らかになったリスクについて適切な対策を実施したか
2. 外来者が建物内や室内で作業する場合、適切な管理の下で作業を行わせているか
3. 立ち入りを許した区域内で訪問者や清掃業者などへの応対を実施しているか
4. 顧客との打合せ場所や案内時の導線などにおいて、セキュリティ上の配慮を行っているか

③重要な情報機器や配線などは、自然災害や人的災害などに対する安全性に配慮して配置または設置し、適切に保守していますか。

安全性に配慮した配置または設置とは、たとえば、重要なシステムの安全な場所への設置、盗み見の防止や盗聴防止などに配慮した設置、配線類の地下や床下への埋設、浸水、火災、地震などを考慮した配置などを言います。

説明 重要な情報機器や配線については、偶然の事故による損壊や外部の者による盗み見や損壊を防ぐなど、安全上の配慮が必要です。偶然の事故に対しては、機器の転倒防止、漏水被害対策、周辺での飲食禁止、踏みつけや引っ張りによる断線の防止など、設備本体や周辺で起こりうる事故を洗い出し、それらに備えた対策を行うことが重要です。また、外部の者による盗み見や損壊に対しては、機器や配線などに、容易に接触できないようにすることが重要です。

対策のポイント

1. 基幹業務システムや機密情報を保有する情報システムを、許可された者だけが立ち入ることのできる安全な場所に設置しているか
2. 執務室の入口から見えないように情報処理設備を配置または設置しているか
3. 使用中に画面を盗み見されないように配置を工夫しているか
4. 不用意な損傷、傍受による盗聴などに配慮して、電源コードや通信ケーブルを配置しているか
5. 重要な情報システムについて、地震などによる転倒の防止、水漏れなどによる被害の予防、停電時の代替電源の確保などを実施しているか

④重要な書類、モバイルPC、記憶媒体などについて適切な管理を行っていますか。

適切な管理とは、たとえば、保管キャビネットの施錠やプリント出力の放置禁止、記憶媒体の粉砕廃棄などを言います。また、重要な書類には、情報システムに関する文書を含みます。

説明 書類や電子的な記憶媒体などによって情報が漏えいする事故が数多く発生しています。保管キャビネットの施錠やプリント出力の放置禁止、記憶媒体の粉砕廃棄など、重要な情報が記録されている書類や記憶媒体を適切に管理することが必要です。また、重要な書類などが他の物品に紛れてしまう事によって不適切な取扱が起きないように、日ごろから、事務所や会議室の整理整頓に心がけることも大切です。

対策のポイント

1. 重要な書類、モバイルPC、記憶媒体などを適切に管理しているか
2. 重要な書類、モバイルPC、記憶媒体などは、物理的に破壊するなどしてから処分しているか
3. 重要なデータやライセンス付きのソフトウェアなどを格納した装置や記憶媒体を破棄する際は、中のデータを確実に消去しているか
4. 事務所内の机上、書庫、会議室などの整理整頓を実施しているか
5. 事務所、机、保管キャビネットなどの施錠管理を実施しているか
6. 郵便物、FAX、印刷物などの放置禁止や保護を実施しているか
7. 情報システムに関する情報も重要書類として取扱い、施錠保管などを実施しているか

大項目3. 情報システム及び通信ネットワークの運用管理

①情報システムの運用に際して、運用環境や運用データに対する適切な保護対策が実施されるよう、十分に配慮していますか。

適切な保護には、開発環境、テスト環境と運用環境の分離、変更管理の実施、開発での本番データの使用制限などが含まれます。

説明 システム開発には、多数の作業者が関与するなど、大きなリスクが潜在しています。そのため、システム開発から本番運用への移行を踏まえ、十分な受け入れテストの実施、運用システムと開発システムの分離、運用システムの変更管理手順の策定、個人情報などの重要なデータを含む本番データの使用制限などの対策が重要となります。

対策のポイント

1. 情報システムの運用環境を開発環境やテスト環境から隔離しているか
2. 個人情報などの重要なデータを不用意にテストに用いないためのルールを定めているか
3. 運用環境の変更について規程を定めているか
4. 運用環境の変更を規程に沿って行うと共に、その過程や結果を記録しているか
5. 必要な場合、情報システムの性能や容量の管理を行っているか
6. 情報システムの受け入れについて、十分なテストを行っているか

②情報システムの運用に際して、必要なセキュリティ対策を実施していますか。

必要なセキュリティ対策には、各種手順書の作成、ルールに従った運用、監視、ログの取得と分析などが含まれます。

説明 情報システムや通信ネットワークの運用管理に必要な情報セキュリティ対策には、セキュリティの確保に必要な事項を含む各種手順書の作成、手順書などのルールに従った運用の実施とその監視、ログの取得と分析などが含まれます。また、運用システムを安定して稼動させるためには、情報システムの性能や容量を監視することも大切です。

対策のポイント

1. システム運用におけるセキュリティ要求事項を明確にしているか
2. 情報システムの運用手順書を整備しているか
3. 日々のシステム運用に不手際が生じないようにするための工夫をしているか
4. システムの運用状況を点検しているか
5. セキュリティ関連のイベントのログを取得しているか
6. 設備の使用状況を記録しているか
7. イベントログや設備の使用状況に関する記録を定期的に点検しているか
8. 不正行為の証拠を隠蔽するなどの目的で、システムログや各種の記録が、改ざんや消去などされないように配慮しているか
9. システム内のサーバや端末などの機器類について、常に時刻が同期するよう設定しているか

③不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウェアなど）への対策を実施していますか。

不正プログラム対策には、ウイルス対策ソフトの導入や、パターンファイルの更新を適時行うこと、ぜい弱性を解消することなどが含まれます。

説明 不正プログラム対策には、ウイルス対策ソフトを導入し、パターンファイルの更新を適時行うことなどが含まれます。また、定期的なウイルス検査を実施し、万が一問題が生じた場合にとるべき処置を周知しておくことも大切です。

対策のポイント

1. ウイルス対策ソフトを適切に配置しているか
2. パターンファイルの更新を適切に行っているか
3. 各サーバやクライアントPCについて、定期的なウイルス検査を行っているか
4. 情報システムの利用者は、ウイルス対策や問題が生じた場合における必要な処置について十分に認識しているか
5. 外部で使用したモバイルPCを内部ネットワークに接続する前に、ウイルス駆除などの（検疫）処理を行っているか
6. 不正プログラムによる攻撃などに悪用されないよう、ぜい弱性の解消（修正プログラムの適用）を行っているか

④導入している情報システムに対して、適切なぜい弱性対策を実施していますか。

適切なぜい弱性対策には、セキュリティを考慮した設定や、パッチ（修正プログラム）の適用、バージョン管理や構成管理、変更管理などが含まれます。

説明 適切なぜい弱性対策には、ぜい弱性情報や脅威情報の定期的な入手、不要なサービスの停止といったセキュリティを考慮した設定、パッチ（修正プログラム）の適用、バージョン管理や構成管理、変更管理などを含みます。

対策のポイント

1. ぜい弱性情報や脅威情報を定期的に収集しているか
2. ぜい弱性や脅威に大きな変化があった場合には、リスクを改めて評価し、ソフトウェアへのパッチ（修正プログラム）適用などの必要な措置を実施しているか
3. パッチについてテスト・適用が適切になされているか
4. 情報システムの導入に際して、不要なサービスを停止するなど、セキュリティを考慮した設定を実施しているか
5. Webサイトの公開にあたっては、不正アクセスや改ざんなどを受けないよう、適切な設定やぜい弱性の解消を行っているか

⑤通信ネットワークを流れるデータや、公開サーバ上のデータに対して、暗号化などの適切な保護策を実施していますか。

適切な保護策には、VPNの使用や重要な情報のSSLなどによる暗号化があります。

説明 適切な保護策には、VPNの使用や重要な情報のSSLなどによる暗号化があります。また、重要な情報を電子メールでやりとりする場合には、情報を暗号化しておくことも効果的です。

対策のポイント

1. 外部のネットワークから内部のネットワークや情報システムへアクセスする場合に、VPNなどを用いて暗号化した通信路を使用しているか
2. Webにアクセスする際、必要に応じ、SSLなどを用いて通信データを暗号化しているか
3. 電子メールをやり取りする場合に、重要な情報を暗号化しているか

⑥モバイルPCやUSBメモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などを想定した適切なセキュリティ対策を実施していますか。

モバイルPCやUSBメモリなどの記憶媒体の使用場所には、外部のパブリックスペースやリモートオフィス、自宅などを含みます。外部のセキュリティの脅威は内部よりも高いことを考慮して対策を行う必要があります。

説明 モバイルPCやUSBメモリなどの記憶媒体の使用場所には、外部のパブリックスペースやリモートオフィス、自宅などを含みます。外部では、内部での利用に比べて盗難や紛失のリスクが高いことを考慮し、外部持ち出しに関する規程を定めたり、強固な認証や暗号化などの対策を検討したりします。

対策のポイント

1. モバイルPCやUSBメモリ、CDなどの使用や記憶媒体の外部持ち出しについて、規程を定めているか
2. 外部でモバイルPCやUSBメモリ、CDなどの記憶媒体を使用する場合の紛失や盗難対策を講じているか
3. モバイルPCにログオンする際に、利用者IDとパスワードなどによる認証を実施しているか
4. モバイルPCなどに保存されているデータを、その重要度に応じて暗号化しているか

大項目4. 情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況

①情報（データ）や情報システムへのアクセスを制限するために、利用者IDの管理、利用者の識別と認証を適切に実施していますか。

適切な利用者IDの管理には、利用者IDの定期的な見直しによる不要なIDの削除や共用IDの利用制限、単純なパスワードの設定禁止などがあります。

説明 適切な利用者IDの管理には、利用者IDに関する規程の整備、利用者IDの定期的な見直しによる不要なIDの削除や共用IDの利用制限、本来必要ではない特権を設定したIDの発見と見直し、見破られやすい単純なパスワードの設定禁止などがあります。

対策のポイント

1. 利用者IDの登録や削除に関する規程を整備し、利用者のIDを定期的に見直しているか
2. 不要になった利用者IDの無効設定漏れがないか、IDの不正利用がないかなどを定期的に点検しているか
3. 空白のパスワードや単純な文字列のパスワードを設定しないよう、利用者に求めているか
4. 利用者ごとにIDとパスワードを割当て、そのIDとパスワードによる識別と認証を確実に実施しているか

②情報（データ）や情報システム、業務アプリケーションなどに対するアクセス権の付与と、アクセス制御を適切に実施していますか。

適切なアクセス権の管理には、アクセスできる情報システムを利用者ごとに限定すること、利用できる機能を制限すること、利用者のアクセス権をレビューすることなどがあります。

説明 適切なアクセス権の管理には、あらかじめ方針を定めておき、その方針に基づいてアクセスできる情報システムを利用者ごとに限定すること、利用できる機能を制限すること、利用者のアクセス権をレビューすることなどがあります。

対策のポイント

1. アクセスを管理する方針を定め、利用者ごとにアクセス可能な情報（データ）、情報システム、業務アプリケーション、サービスなどを適切に設定しているか
2. 適切な権限付与が行われているか、必要以上の権限付与がないかなど、利用者に与えたアクセス権を定期的にレビューしているか
3. 特に重要な情報を格納した情報システムについては、一度のアクセスでの利用時間の制限などのアクセス条件による制御を行っているか

③ネットワークのアクセス制御を適切に実施していますか。

適切なネットワークのアクセス制御には、たとえばネットワークの分割や外部からの接続時の認証などがあります。

説明 ネットワークへの接続に伴って、接続したネットワーク経由で侵入されるといったリスクが増大します。そのようなリスクを低減するためには、ネットワークへの適切なアクセス制御が不可欠です。ネットワークのアクセス制御には、たとえばネットワークの分割や外部からの接続時の認証などがあります。

対策のポイント

1. 外部のネットワークから内部のシステムへアクセスする際（モバイルPCを使用する場合を含む）に、利用者認証を実施しているか
2. サービスや情報システムにアクセス可能な利用者を制限するために、ネットワークを論理的に切り離したり、接続を制限したりしているか
3. 許可されていないワイヤレスアクセスポイントの設置を禁止しているか
4. 外部の無線LANを利用してネットワークにアクセスする場合に、セキュリティ対策を実施しているか
5. 内部のネットワークに接続する端末機器について、接続時に認証しているか

④業務システムの開発において、必要なセキュリティ要件を定義し、設計や実装に反映させていますか。

自組織での開発、外部委託による開発を問わず、開発の際に必要なセキュリティ対策としては、仕様書にセキュリティ上の要求事項を盛り込むこと、設計や開発に際してぜい弱性を作り込まないように配慮すること、ぜい弱性を残さないための適切なシステム試験を実施することなどがあります。

説明 業務システムは、完成してしまった後に改変を加えることは困難で、コストも嵩みます。企画、設計などの初期の段階から情報セキュリティについて配慮することが必要です。そのためには、自組織での開発、外部委託による開発を問わず、仕様書にセキュリティ上の要求事項を盛り込むこと、設計や開発に際してぜい弱性を作り込まないように配慮すること、ぜい弱性を残さないための適切なシステム試験を実施することなどが重要です。

対策のポイント

1. セキュリティ上の要求事項を仕様書に盛り込んでいるか
2. 入力データに対するチェック機能を適切に実装しているか
3. 業務処理プロセスを適切に実装しているか
4. 情報の保護機能を適切に実装しているか
5. 出力データの妥当性や表示メッセージの正しさなどに関するチェックを適切に行っているか
6. ぜい弱性を作り込まないために、プログラミング上の配慮がなされているか

⑤ソフトウェアの選定や購入、情報システムの開発や保守に際して、セキュリティ上の観点からの点検をプロセスごとに実施するなど、適切なプロセス管理を実施していますか。

選定や購入、開発や保守を外部委託している場合は、セキュリティ上の観点からの点検が可能かどうかを回答してください

説明 ソフトウェアにセキュリティ上の問題を混入させないための管理が重要です。たとえば、選定や購入に際しては、ソフトウェアの開発元を確認すること、開発や保守に際しては、ソースコードへのアクセス管理といったセキュリティ対策の実施状況の記録やレビューの記録などを確認できることが大切です。

対策のポイント

1. 運用に供しようとする情報システムのソフトウェアの導入や変更に関する手順を整備しているか
2. ソースコードへのアクセスを制限しているか
3. 構成の変更に関する手順を整備し、厳重に管理しているか
4. トロイの木馬などの不正プログラムが組み込まれていないかどうかをチェックしているか
5. 外部委託によるソフトウェア開発を行う場合、使用許諾、知的所有権などについて取り決めているか
6. 外部委託によるソフトウェア開発を行う場合、品質や作業範囲、標準となる契約書や合意書を用意しているか
7. 開発や保守を外部委託する場合に、セキュリティ管理の実施状況を把握できるか

大項目5. 情報セキュリティ上の事故対応状況

①万が一システムに障害が発生しても、必要最低限のサービスを維持できるようにするため、情報システムに障害が発生する場合をあらかじめ想定した適切な対策を実施していますか。

適切な対策には、たとえばシステムの二重化、バックアップと運用記録の取得、障害対応手順の明確化、外部委託先とのサービスレベルの合意などがあります。

説明 情報セキュリティの重要な要素の一つである可用性に影響を与える事象のうち、影響の度合いが最も大きいのは、情報システム関連機器の障害であると言っても過言ではありません。情報システムに求められる可用性の条件を満たすためには、可用性に関する要求に対応した適切な障害対策機能の情報システムへの組込みが欠かせません。

対策のポイント

1. 情報システムの可用性に関する要求は明確で妥当なものか（可用性とは、情報システムを使う権限のある人がいつでも使えるようにすることをいいます）
2. 障害対策の実行に必要なバックアップ情報の取得や、運用記録などの確保を適切に行っているか
3. 障害部分の切り離し、縮退運転、情報の回復や情報システムの復旧など、障害発生時に必要となる機能を情報システムに組み込んでおり、それらが適切に機能することを検証しているか（縮退運転とは、提供する機能やサービスの対象者の絞り込みなどにより、障害時でも、必要最低限のサービスを提供できるようにすることを言います）
4. 障害発生時の対応手順や、障害対策処理の実施要領を策定しているか
5. 障害対応のスキルに関する教育や訓練を実施しているか
6. 情報システムの運用を外部に委託している場合、障害発生時にも所定のサービスレベルが維持されることを、委託先との間で相互に確認しているか
7. システムの各種ログを取得できているか

②情報セキュリティに関連する事件や事故が発生した際に必要な行動を、適切かつ迅速に実施できるように備えていますか。

事件や事故への備えには、そうした万が一の場合にとるべき行動をあらかじめ検討しておくこと、検討した結果を文書にまとめて関係者に周知しておくこと、緊急の連絡網を整備すると共に、必要な要員や資機材を揃えられるようにあらかじめ手配しておくことなどがあります。

説明 情報セキュリティに関連する事件や事故が発生した場合に、被害の拡大を防ぎ、局所化するためには、事件や事故に必要な対応を組織全体で適切かつ迅速に実施できなければなりません。そのためには、事件や事故を想定し、実施すべき作業やその実施要領を確立するとともに、現場の要員がいざというときに対応作業を円滑に実行できるように準備しておくことが必要となります。また、個人情報などの漏えいが発生した場合に、影響を受ける可能性のある本人への連絡、主務大臣などへの報告、事実関係や再発防止策の公表などを円滑に進めるため、手順などを整備しておくことも重要です。

対策のポイント

1. セキュリティにかかわる出来事、事件や事故の発生時の対応について、実施要領を定めているか
2. セキュリティにかかわる出来事、事件や事故に関する対応要領を関係者に徹底しているか
3. セキュリティにかかわる出来事、事件や事故の発生時の連絡網を含む対応体制を構築しているか
4. セキュリティにかかわる出来事、事件や事故への対応に必要なリソースやツールを適切に準備しているか（ここでのリソースやツールとは、障害対応要員、障害を記録するためのディスク領域、障害報告機能や分析機能などを指します）

③何らかの理由で情報システムが停止した場合でも、必要最小限の業務を継続できるようになっていますか。

万が一、情報システムが停止してしまった場合に備えて、普段は情報システムで行っている業務をたとえば手作業で代替できるように、そうした業務の手順書や様式類をあらかじめ用意しておくこと、またそうした手作業を実施できる場所や資機材を確保しておくこと、さらに手作業で代替できるように要員を訓練しておくことなどが重要です。

説明 地震、台風、水害などの自然災害による施設、システム機器、業務アプリケーション、業務データの損壊や、そのほか情報システムに生じた重大事故によって、情報システムが停止し、短期間での復旧の目処がたたなくなるような事態の発生が考えられます。このような状況においても事業の継続ができるようにするためには、情報システム全体をカバーするバックアップセンターの準備や、ソフトウェア資産や業務データのバックアップとその安全な保管、さらには手作業により業務の遂行ができるようにしておくなどの準備が必要となります。事業活動の多くを情報システムに依存している組織においては、事業継続への取組は十分に検討しておくべきです。

対策のポイント

1. 情報システムが停止した場合に、自組織の業務に及ぼす影響について検討した事があるか
2. 各業務の重要度や、業務システムのトラブルがそうした業務に及ぼす影響について把握しているか
3. 情報システムの停止が長期になる場合に備え、業務を継続するための方針やシナリオを策定しているか
4. 情報システムの長期停止時に必要となる、バックアップセンターへの切り替えや業務の手作業への切り替えなどは、何時でも実施できるよう、手順の策定や関係者への周知と訓練を実施しているか
5. 外部への連絡など、情報システムが長期停止に陥った場合に必要となるその他の措置についても検討し、実施要領を策定しているか

注：各項目の解説については、「情報セキュリティ対策ベンチマーク（改訂版）」に記載されています。この資料は、以下のURLよりダウンロードすることができます。

http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html

資料2 JIS Q 27002：2006 箇条、セキュリティカテゴリ、管理策（タイトル）一覧

注：JIS Q 27001:2006 付属書Aの管理目的及び管理策はJIS Q 27002:2006の箇条5-15までに掲げられているものをそのまま取り入れて配列したものです。

箇条/セキュリティカテゴリ	管理策（タイトル）
5. セキュリティ基本方針	
5.1 情報セキュリティ基本方針	5.1.1 情報セキュリティ基本方針文書 5.1.2 情報セキュリティ基本方針のレビュー
6. 情報セキュリティのための組織	
6.1 内部組織	6.1.1 情報セキュリティに対する経営陣の責任 6.1.2 情報セキュリティの調整 6.1.3 情報セキュリティ責任の割当て 6.1.4 情報処理設備の認可プロセス 6.1.5 秘密保持契約 6.1.6 関係当局との連絡 6.1.7 専門組織との連絡 6.1.8 情報セキュリティの独立したレビュー
6.2 外部組織	6.2.1 外部組織に関係したリスクの識別 6.2.2 顧客対応におけるセキュリティ 6.2.3 第三者との契約におけるセキュリティ
7. 資産の管理	
7.1 資産に対する責任	7.1.1 資産目録 7.1.2 資産の管理責任者 7.1.3 資産利用の許容範囲
7.2 情報の分類	7.2.1 分類の指針 7.2.2 情報のラベル付け及び取扱い
8. 人的資源のセキュリティ	
8.1 雇用前	8.1.1 役割及び責任 8.1.2 選考 8.1.3 雇用条件
8.2 雇用期間中	8.2.1 経営陣の責任 8.2.2 情報セキュリティの意識向上,教育及び訓練 8.2.3 懲戒手続
8.3 雇用の終了又は変更	8.3.1 雇用の終了又は変更に関する責任 8.3.2 資産の返却 8.3.3 アクセス権の削除
9. 物理的及び環境的セキュリティ	
9.1 セキュリティを保つべき領域	9.1.1 物理的セキュリティ境界 9.1.2 物理的入退管理策 9.1.3 オフィス、部屋及び施設のセキュリティ 9.1.4 外部及び環境の脅威からの保護 9.1.5 セキュリティを保つべき領域での作業 9.1.6 一般の人の立寄り場所及び受渡場所
9.2 装置のセキュリティ	9.2.1 装置の設置及び保護 9.2.2 サポートユーティリティ 9.2.3 ケーブル配線のセキュリティ 9.2.4 装置の保守 9.2.5 構外にある装置のセキュリティ 9.2.6 装置の安全な処分又は再利用 9.2.7 資産の移動
10. 通信及び運用管理	
10.1 運用の手順及び責任	10.1.1 操作手順書 10.1.2 変更管理 10.1.3 職務の分割 10.1.4 開発施設、試験施設及び運用施設の分離
10.2 第三者が提供するサービスの管理	10.2.1 第三者が提供するサービス 10.2.2 第三者が提供するサービスの監視及びレビュー 10.2.3 第三者が提供するサービスの変更に対する管理
10.3 システムの計画作成及び受入れ	10.3.1 容量・能力の管理 10.3.2 システムの受入れ
10.4 悪意のあるコード及びモバイルコードからの保護	10.4.1 悪意のあるコードに対する管理策 10.4.2 モバイルコードに対する管理策
10.5 バックアップ	10.5.1 情報のバックアップ
10.6 ネットワークセキュリティ管理	10.6.1 ネットワーク管理策 10.6.2 ネットワークサービスのセキュリティ
10.7 媒体の取扱い	10.7.1 取外し可能な媒体の管理 10.7.2 媒体の処分 10.7.3 情報の取扱手順 10.7.4 システム文書のセキュリティ
10.8 情報の交換	10.8.1 情報交換の方針及び手順 10.8.2 情報交換に関する合意 10.8.3 配送中の物理的媒体 10.8.4 電子的メッセージ通信 10.8.5 業務用情報システム

10.9　電子商取引サービス	10.9.1　電子商取引 10.9.2　オンライン取引 10.9.3　公開情報
10.10　監視	10.10.1　監査ログ取得 10.10.2　システム使用状況の監視 10.10.3　ログ情報の保護 10.10.4　実務管理者及び運用担当者の作業ログ 10.10.5　障害のログ取得 10.10.6　クロックの同期
11．アクセス制御	
11.1　アクセス制御に対する業務上の要求事項	11.1.1　アクセス制御方針
11.2　利用者アクセスの管理	11.2.1　利用者登録 11.2.2　特権管理 11.2.3　利用者パスワードの管理 11.2.4　利用者アクセス権のレビュー
11.3　利用者の責任	11.3.1　パスワードの利用 11.3.2　無人状態にある利用者装置 11.3.3　クリアデスク・クリアスクリーン方針
11.4　ネットワークのアクセス制御	11.4.1　ネットワークサービスの利用についての方針 11.4.2　外部から接続する利用者の認証 11.4.3　ネットワークにおける装置の識別 11.4.4　遠隔診断用及び環境設定用ポートの保護 11.4.5　ネットワークの領域分割 11.4.6　ネットワークの接続制御 11.4.7　ネットワークルーティング制御
11.5　オペレーティングシステムのアクセス制御	11.5.1　セキュリティに配慮したログオン手順 11.5.2　利用者の識別及び認証 11.5.3　パスワード管理システム 11.5.4　システムユーティリティの使用 11.5.5　セッションのタイムアウト 11.5.6　接続時間の制限
11.6　業務用ソフトウェア及び情報のアクセス制御	11.6.1　情報へのアクセス制限 11.6.2　取扱いに慎重を要するシステムの隔離
11.7　モバイルコンピューティング及びテレワーキング	11.7.1　モバイルのコンピューティング及び通信 11.7.2　テレワーキング
12．情報システムの取得、開発及び保守	
12.1　情報システムのセキュリティ要求事項	12.1.1　セキュリティ要求事項の分析及び仕様化
12.2　業務用ソフトウェアでの正確な処理	12.2.1　入力データの妥当性確認 12.2.2　内部処理の管理 12.2.3　メッセージの完全性 12.2.4　出力データの妥当性確認
12.3　暗号による管理策	12.3.1　暗号による管理策の利用方針 12.3.2　かぎ（鍵）管理
12.4　システムファイルのセキュリティ	12.4.1　運用ソフトウェアの管理 12.4.2　システム試験データの保護 12.4.3　プログラムソースコードへのアクセス制御
12.5　開発及びサポートプロセスにおけるセキュリティ	12.5.1　変更管理手順 12.5.2　オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー 12.5.3　パッケージソフトウェアの変更に対する制限 12.5.4　情報の漏えい 12.5.5　外部委託によるソフトウェア開発
12.6　技術的ぜい弱性の管理	12.6.1　技術的ぜい弱性の管理
13．情報セキュリティインシデントの管理	
13.1　情報セキュリティの事象及び弱点の報告	13.1.1　情報セキュリティ事象の報告 13.1.2　セキュリティ弱点の報告
13.2　情報セキュリティインシデントの管理及びその改善	13.2.1　責任及び手順 13.2.2　情報セキュリティインシデントからの学習 13.2.3　証拠の収集
14．事業継続管理	
14.1　事業継続管理における情報セキュリティの側面	14.1.1　事業継続管理手続への情報セキュリティの組込み 14.1.2　事業継続及びリスクアセスメント 14.1.3　情報セキュリティを組み込んだ事業継続計画の策定及び実施 14.1.4　事業継続計画策定の枠組み 14.1.5　事業継続計画の試験、維持及び再評価
15．順守	
15.1　法的要求事項の順守	15.1.1　適用法令の識別 15.1.2　知的財産権（IPR） 15.1.3　組織の記録の保護 15.1.4　個人データ及び個人情報の保護 15.1.5　情報処理施設の不正使用防止 15.1.6　暗号化機能に対する規制
15.2　セキュリティ方針及び標準の順守、並びに技術的順守	15.2.1　セキュリティ方針及び標準の順守 15.2.2　技術的順守の点検
15.3　情報システムの監査に対する考慮事項	15.3.1　情報システムの監査に対する管理策 15.3.2　情報システムの監査ツールの保護

内容に関するお問合せ先

■情報セキュリティ対策ベンチマーク

独立行政法人 情報処理推進機構　セキュリティセンター

〒113-6591 東京都文京区本駒込2-28-8 文京グリーンコート センターオフィス16階
TEL：03-5978-7508　　FAX：03-5978-7518
e-mail：isec-info@ipa.go.jp
URL：http://www.ipa.go.jp/security/benchmark/

■ISMS適合性評価制度

財団法人 日本情報処理開発協会
情報マネジメント推進センター ISMS制度推進室

〒105-0011　東京都港区芝公園3-5-8　機械振興会館3階
TEL：03-3432-9386　　FAX：03-3432-6200
e-mail：it-info@tower.jipdec.or.jp
URL：http://www.isms.jipdec.jp/

■情報セキュリティ監査

特定非営利活動法人 日本セキュリティ監査協会　事務局

〒103-0025 東京都中央区日本橋茅場町2-8-4 全国中小企業会館5階
TEL：03-5640-7060　　FAX：03-5640-0666
e-mail：office@jasa.jp
URL：http://www.jasa.jp

■情報セキュリティガバナンス等の情報セキュリティ政策について

経済産業省　商務情報政策局　情報セキュリティ政策室

〒100-8901 東京都千代田区霞ヶ関1-3-1
TEL：03-3501-0397　　FAX：03-3501-6639
e-mail：it-security@meti.go.jp
URL：http://www.meti.go.jp/policy/netsecurity/

情報セキュリティ対策ベンチマーク普及検討会　名簿

【座長】	大木　栄二郎	工学院大学情報学部　教授
【構成員】	山田　安秀	独立行政法人 情報処理推進機構 セキュリティセンター長
	石井　　茂	独立行政法人 情報処理推進機構 セキュリティセンター　普及グループリーダー
	菅野　泰子	独立行政法人 情報処理推進機構 セキュリティセンター　調査役
	高取　敏夫	財団法人 日本情報処理開発協会 情報マネジメント推進センター　SMS制度推進室　室長
	星　　昌宏	財団法人 日本情報処理開発協会 情報マネジメント推進センター　審査グループリーダー
	下村　正洋	特定非営利活動法人 日本セキュリティ監査協会 理事・事務局長
	沓澤　　徹	特定非営利活動法人 日本セキュリティ監査協会 事務局次長
	永宮　直史	特定非営利活動法人 日本セキュリティ監査協会 保証型監査促進プロジェクト・コアメンバー 資格認定委員会委員、資格維持プログラム小委員会委員長
【オブザーバ】	清水　友晴	経済産業省　商務情報政策局 情報セキュリティ政策室　課長補佐
	和田　浩明	経済産業省　商務情報政策局 情報セキュリティ政策室
	井口　新一	財団法人 日本適合性認定協会　専務理事
	本山　佳奈	財団法人 日本適合性認定協会　認定審査員
	川口　修司	株式会社 三菱総合研究所 情報セキュリティ研究グループ　主席研究員
【事務局】	独立行政法人 情報処理推進機構	

情報セキュリティ対策ベンチマーク普及検討会 作業部会 名簿

【構成員】	菅野　泰子	独立行政法人 情報処理推進機構 セキュリティセンター　調査役
	高取　敏夫	財団法人 日本情報処理開発協会 情報マネジメント推進センター　ISMS制度推進室　室長
	星　　昌宏	財団法人 日本情報処理開発協会 情報マネジメント推進センター　審査グループリーダー
	沓澤　　徹	特定非営利活動法人 日本セキュリティ監査協会 事務局次長
	永宮　直史	特定非営利活動法人 日本セキュリティ監査協会 保証型監査促進プロジェクト・コアメンバー 資格認定委員会委員、資格維持プログラム小委員会委員長
	高橋　さぎり	特定非営利活動法人 日本セキュリティ監査協会 事務局
【オブザーバ】	清水　友晴	経済産業省　商務情報政策局 情報セキュリティ政策室　課長補佐
	本山　佳奈	財団法人日本適合性認定協会　認定審査員
	川口　修司	株式会社 三菱総合研究所 情報セキュリティ研究グループ　主席研究員

注：構成員、オブザーバの記載は、組織名のあいうえお順に記載しています。

情報セキュリティ対策ベンチマーク活用集

2008年1月　初版　第1刷発行
2008年3月　第2版　第1刷発行
2008年9月　第3版　第1刷発行

著作編者　独立行政法人 情報処理推進機構
財団法人 日本情報処理開発協会
特定非営利活動法人 日本セキュリティ監査協会

連絡先　独立行政法人 情報処理推進機構
セキュリティセンター
TEL：03-5978-7508　E-mail：isec-info@ipa.go.jp

http://www.ipa.go.jp/security/benchmark/