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

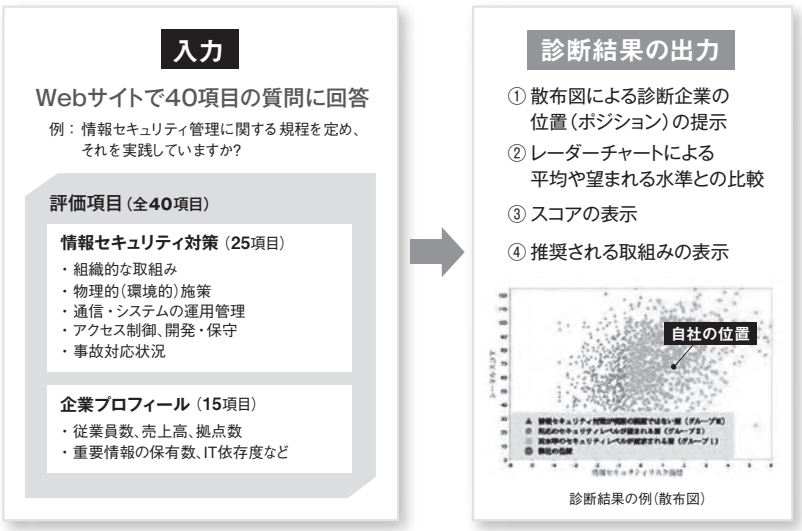
情報セキュリティ対策ベンチマークは、組織の情報セキュリティ対策状況を自らが評価するための自己診断ツールである。経済産業省より公表された情報セキュリティガバナンス推進のための施策ツールを、IPAが自動診断システムとして開発し、2005年8月よりIPAのWebサイト上で提供している。

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

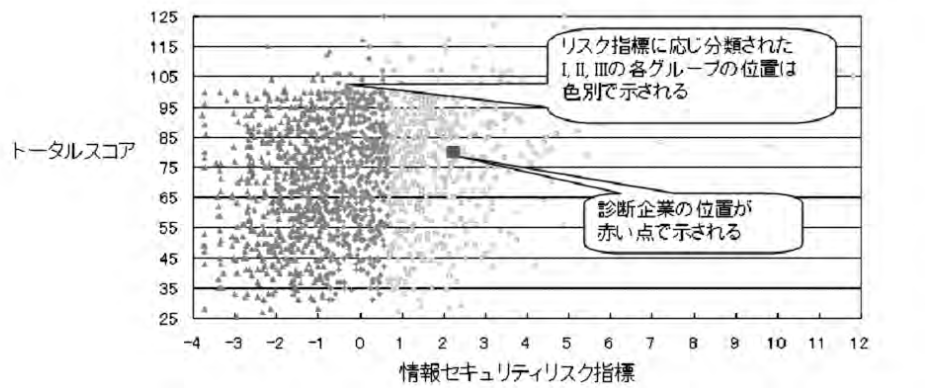
第1部の情報セキュリティ対策に関する25項目では、自組織の取組みの状況を**図付1.2**に示す5段階の成熟度により自己評価する。成熟度1は取り組みができていない状態であり、段階が上がるにつれて、取組みができていることになる。1問5点（5段階）として、トータルスコアは125点である。

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

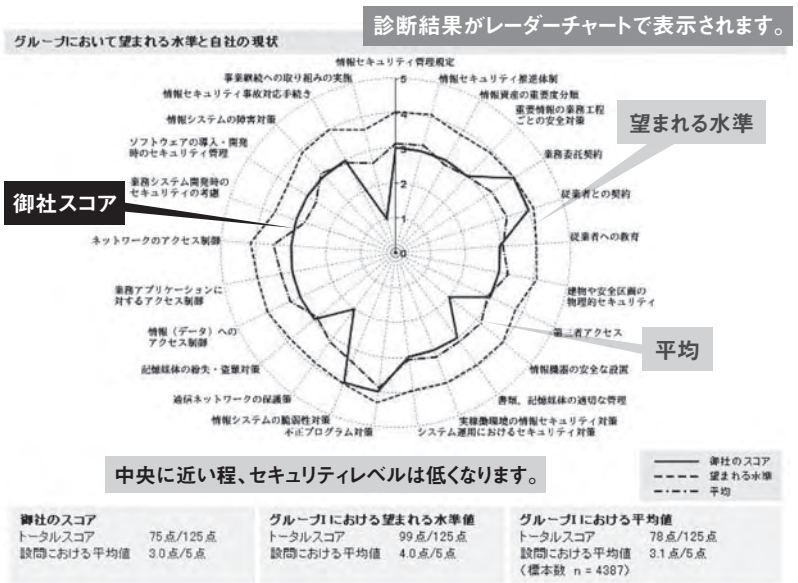
図付1.2　成熟度で答える5段階の回答



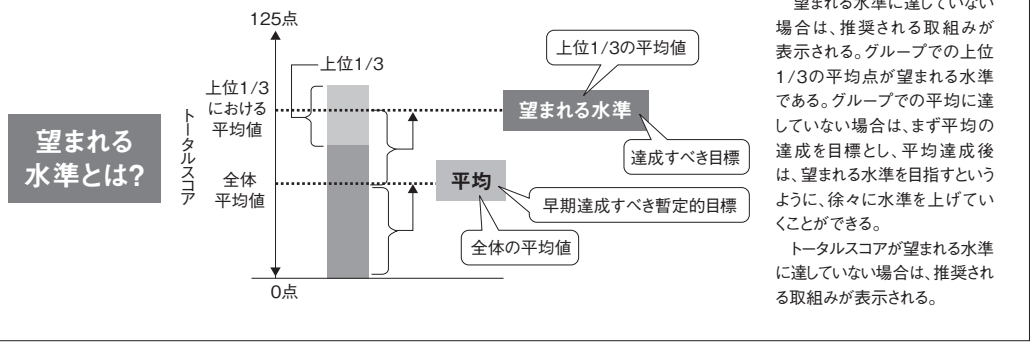
図付1.3　診断結果例（散布図）

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

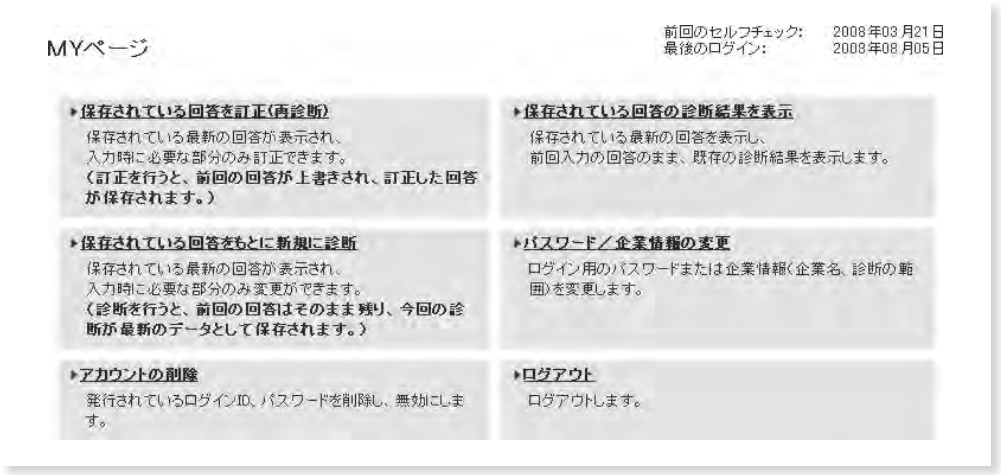
2005年3月の「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」の発表より2年半が経過し、経済産業省より「情報セキュリティ対策ベンチマーク改訂版」が2007年8月24日に公開された。これは、この間に企業が抱える事業リスクも多様化・複雑化したことに対応し、施策ツールの見直し・改善が検討されたことの成果である。

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

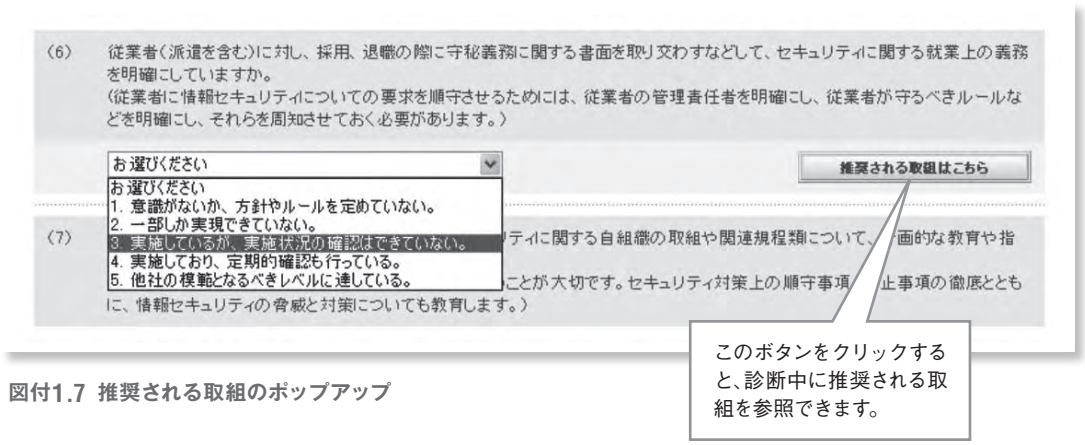
の訂正、保存されている回答をもとにした新規の診断、パスワードの変更などができる。このページでは、次の改良を行った。

- 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】



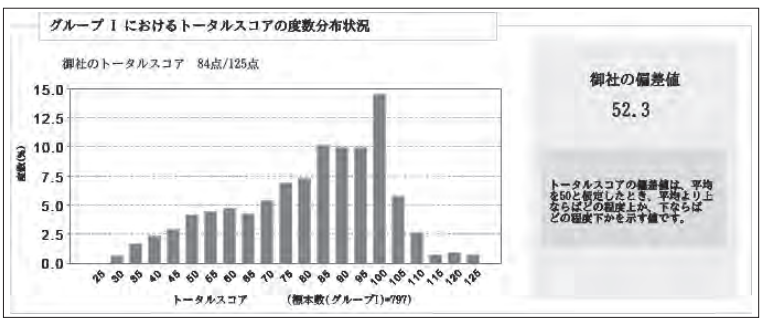
図付1.7 推奨される取組のポップアップ

(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

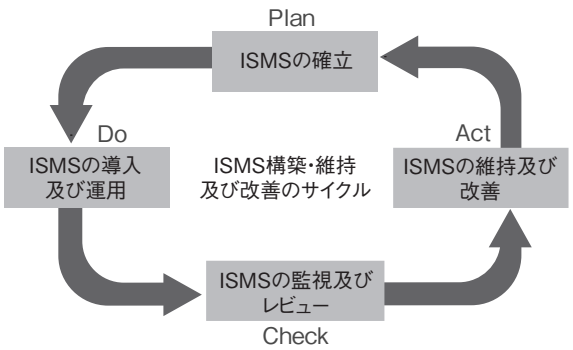
付2.1　ISMSの確立及び運営管理

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。

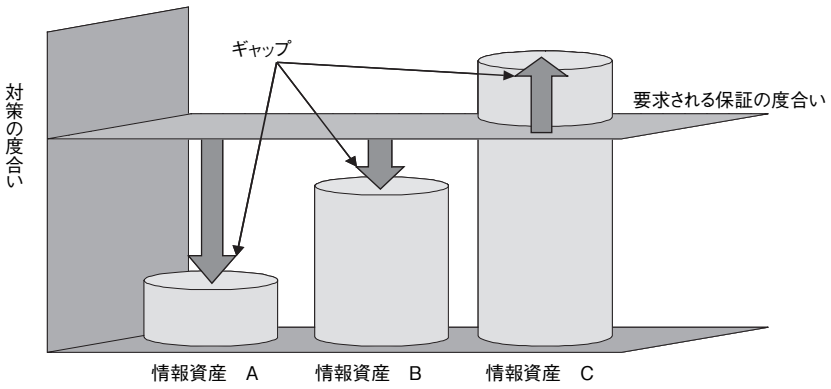
実際にどのようなコントロールを導入するのか、「出来る、出来ない」の判断をする前に広く管理策についての情報を収集し、組織が要求する情報セキュリティの管理水準が、達成可能なベースラインであるかを検討されたい。たとえば、他の企業と比較して情報セキュリティの管理水準が必要なレベルであるかを調べるのも効果的である。

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。

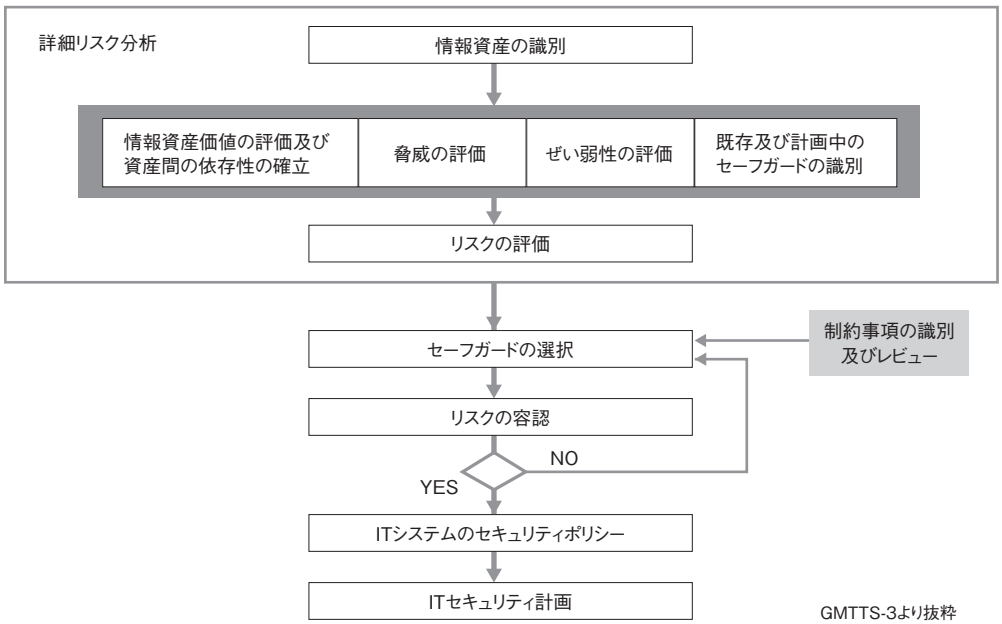
基準で要求される管理レベルと事業者の管理レベルの現状を比較し、「大きな差が認められる個所」、「明らかに管理策の適用を必要としている個所」、「過度に管理策が適用されている個所」等を確認する。

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。

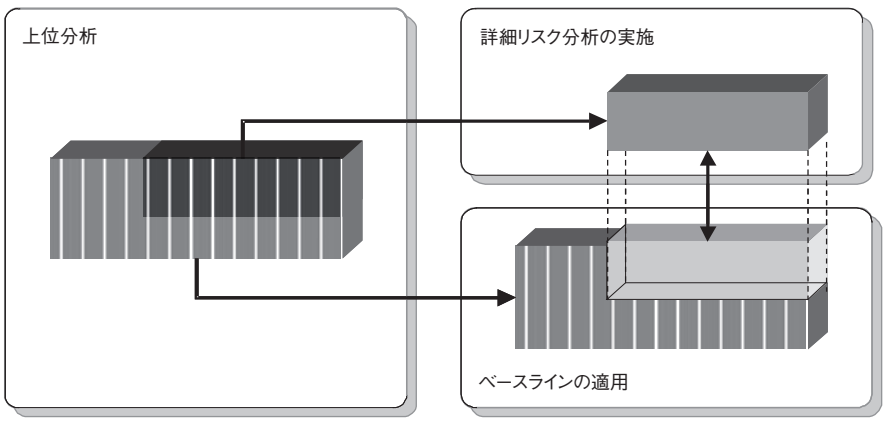
まず、リスク分析の対象範囲の定義付けをしなければならない。プロセスが密接に絡み合っているにもかかわらず、安易に範囲を狭め、慎重な定義付けを怠ると、後に不必要な作業が増えたり、抜けが見られたりすることに繋がるからである。

(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。

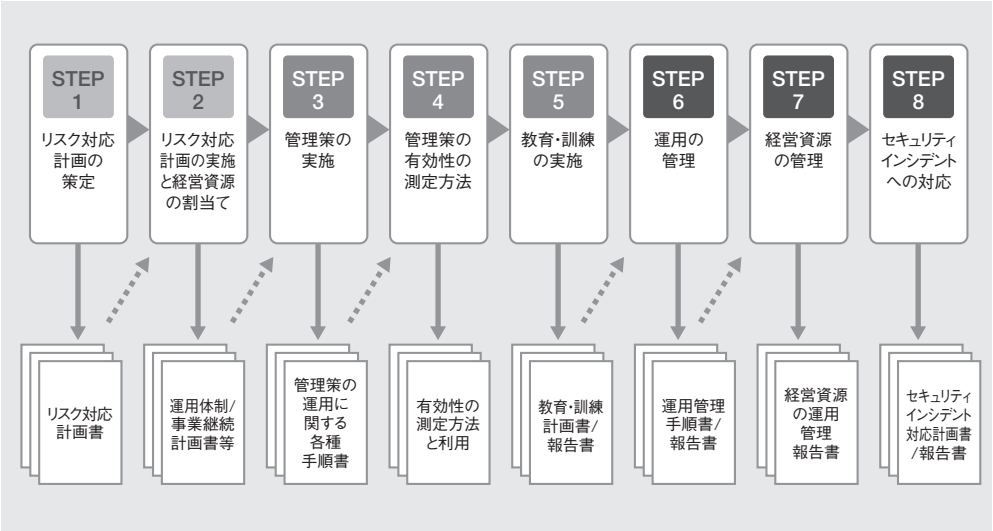
(2)管理策の実施と有効性の測定 (STEP3～STEP5)

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)

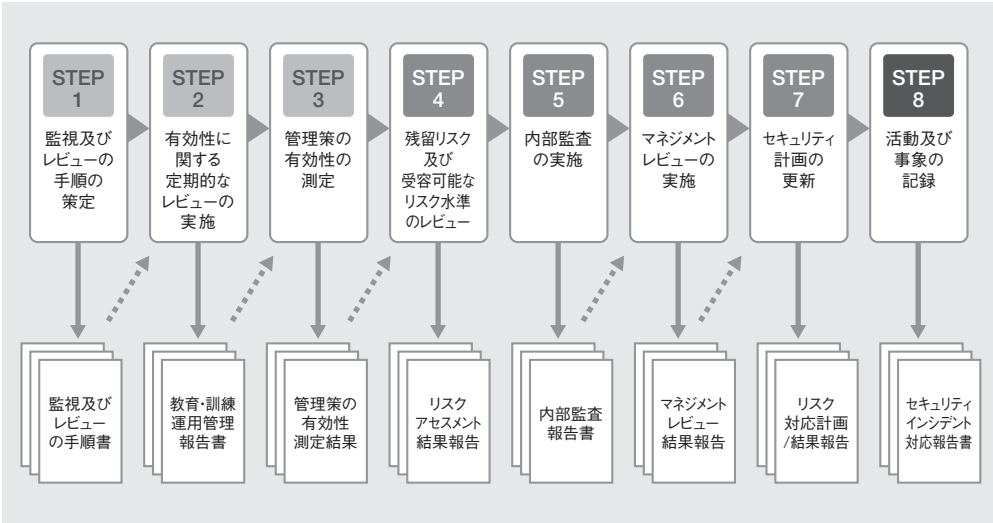
組織は、セキュリティ上の違反行為、情報セキュリティインシデントの防止、及びセキュリティ違反に対する処置の有効性を判断するため、監視及び見直しの手順を文書化するとともに、監視のための管理策を実施する。ISMSの有効性に関して定期的なレビューをする。有効性の評価は、目標に対する達成度を確認する。そのため、セキュリティ要求事項が満たされていることを検証するために、導入した管理策がどの程度有効に機能しているかを測定する。

(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

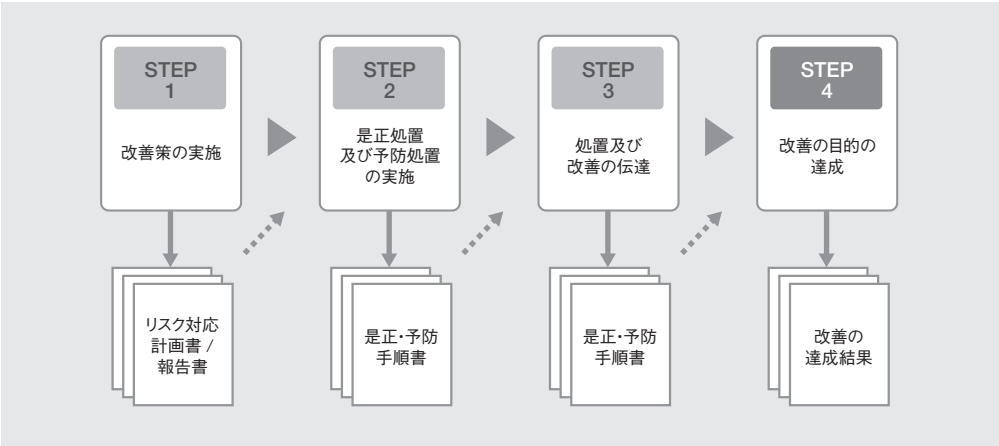
ISMSの維持及び改善のステップは、**図付2.8**に示す通りである。

(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

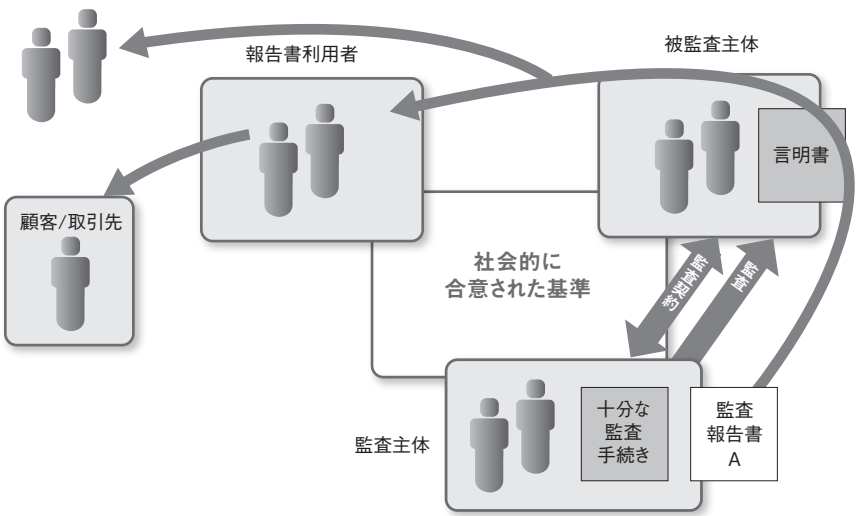
保証型監査では、監査主体、被監査主体、そして利害関係者という監査に関わる三当事者の間でどのような共通理解がなされるかによって、監査の方式が異なる。監査の方式には、社会的合意方式、利用者合意方式、被監査主体合意方式の三つがある。以下に、この三方式の概要を示す。

(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



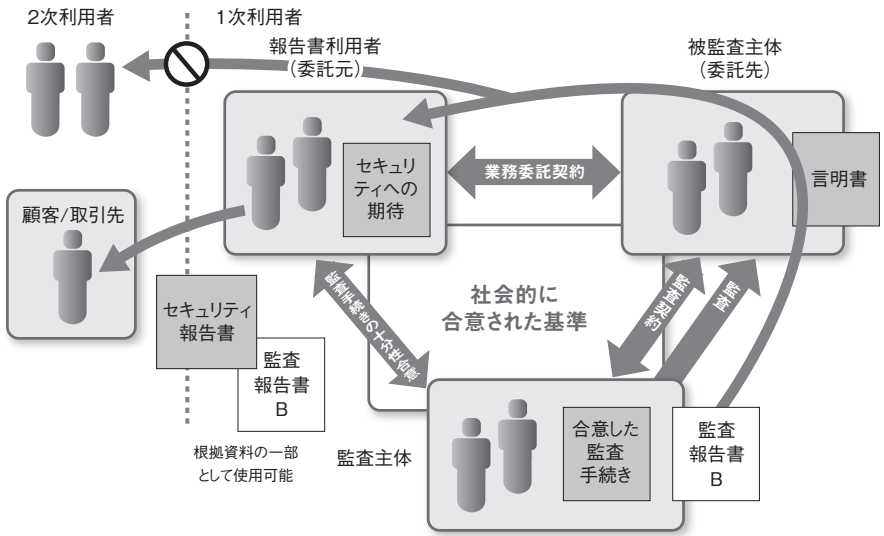
図付3.1　社会的合意方式

(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。

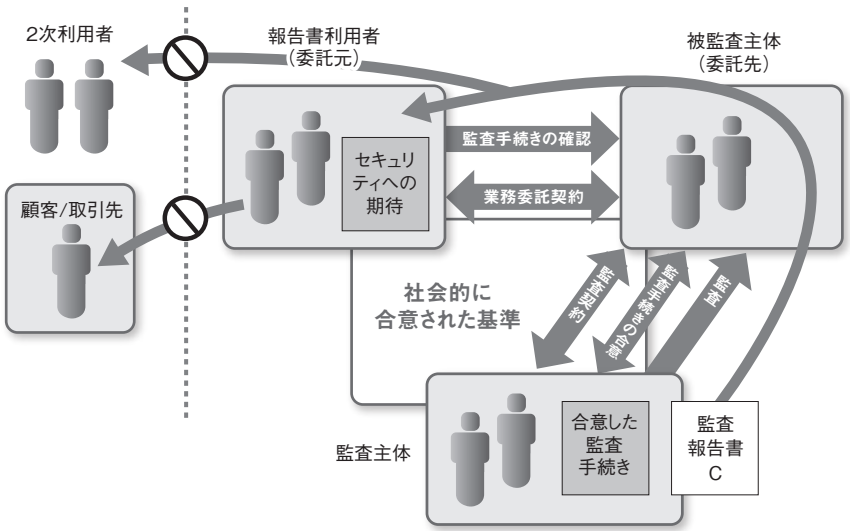


図付3.2　利用者合意方式

(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。

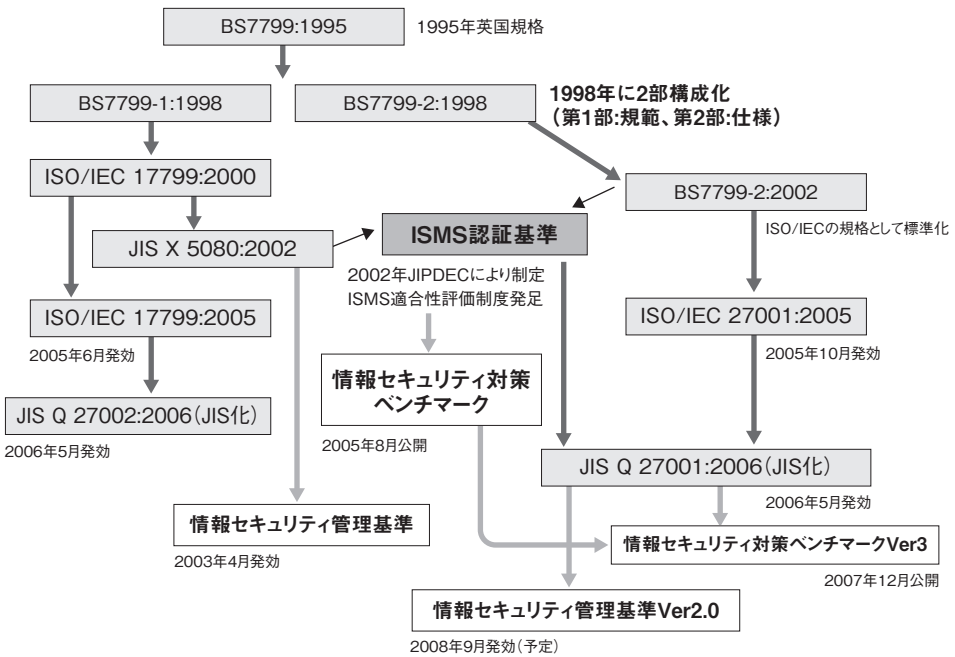
この他、監査品質を高く保つために、しっかりとした体制で適確な監査を実施することも必要である。

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

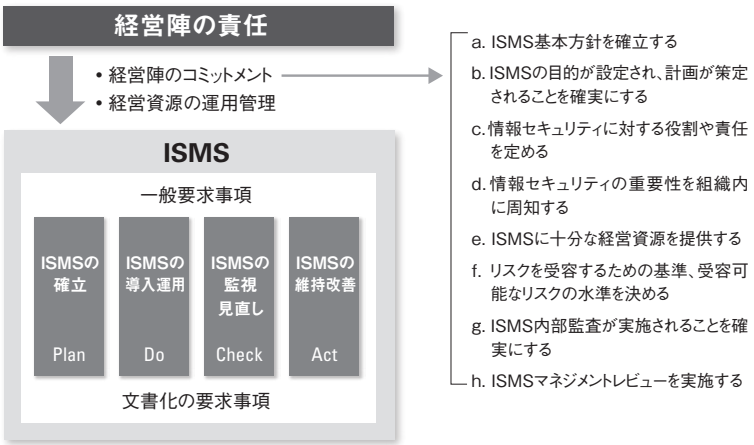
4. 情報セキュリティマネジメントシステム
5. 経営陣の責任
6. ISMS内部監査
7. ISMSのマネジメントレビュー
8. ISMSの改善

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

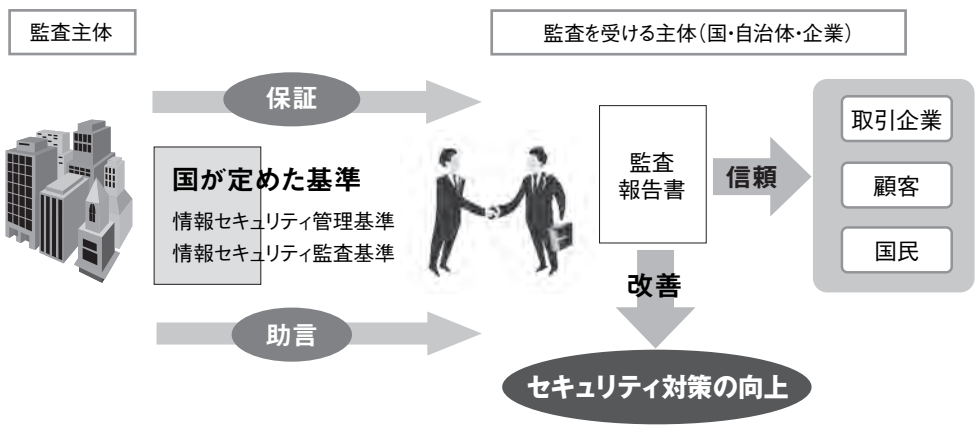
3 情報セキュリティ対策ベンチマークの25の評価項目

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

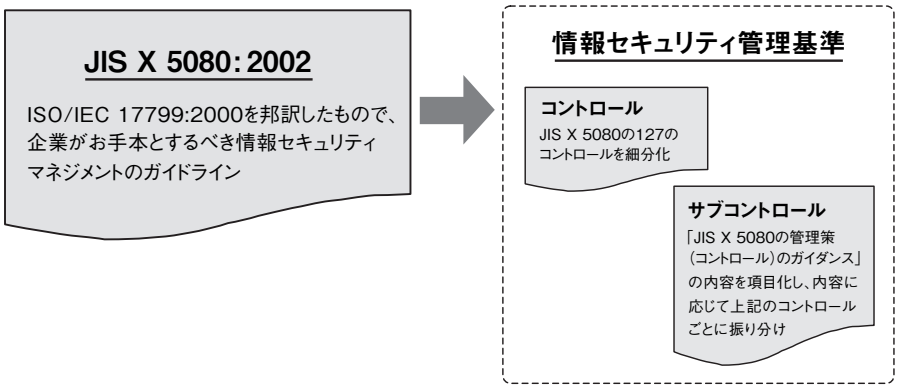


図付4.6　情報セキュリティ監査制度の概要

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。

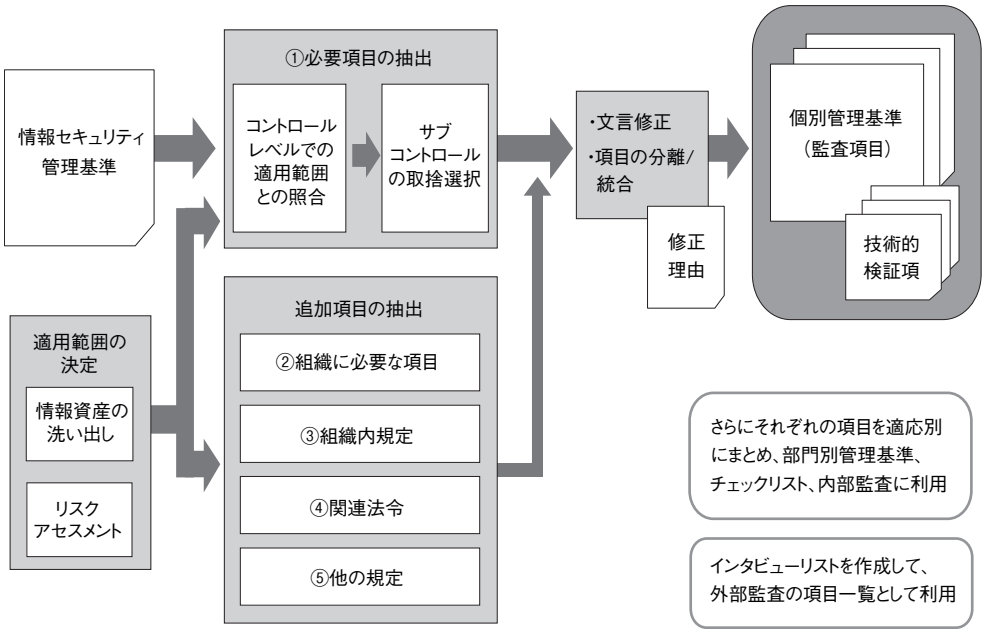
この情報セキュリティ監査制度における根幹となる基準の一つである情報セキュリティ管理基準は、組織体が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロールを整備、運用するための実践規範である。情報セキュリティマネジメントは、第一義的には、組織体における必要性と組織体の責任において果たされるべきものであり、情報セキュリティマネジメントの基本的な枠組みと具体的な管理項目を規定することによって、組織体が情報セキュリティマネジメント体制の構築と、適切なコントロールの整備と運用を効果的に導入できるように支援することを目的としている。

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

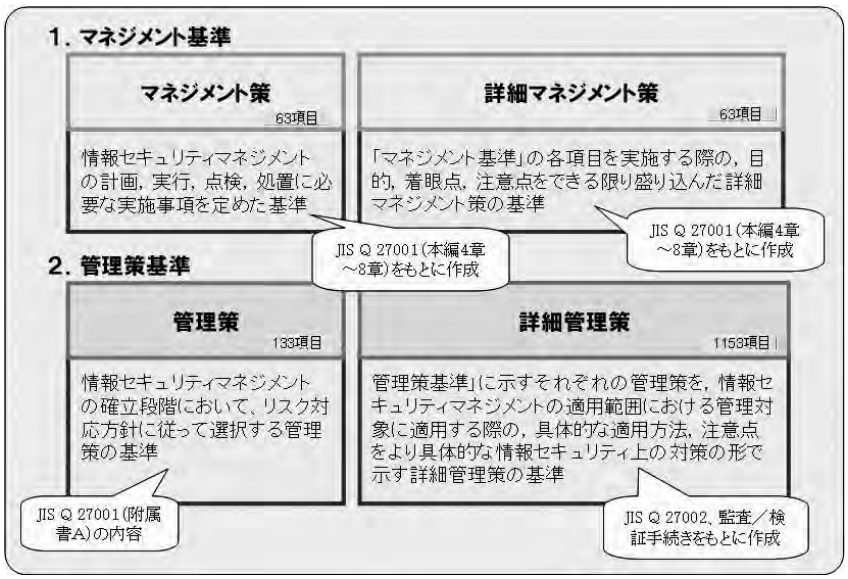
本管理基準は、組織体の業種及び規模等を問わず適用できるよう汎用的なものとなっている。組織体においては、本管理基準を基礎として、リスクアセスメントの結果等に基づき、独自に必要とする項目を追加、あるいは削除して、個別管理基準を作成することができる。ただし、情報セキュリティは、個々のマネジメント及びコントロールの項目が相互に結びつき合ってはじめて有効に機能するものであり、また、計画、実施、評価、是正を通じたマネジメントサイクルとして機能するように留意しなければならない。次頁 **図付4.8**に、個別管理基準作成までの流れを示す。



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