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・

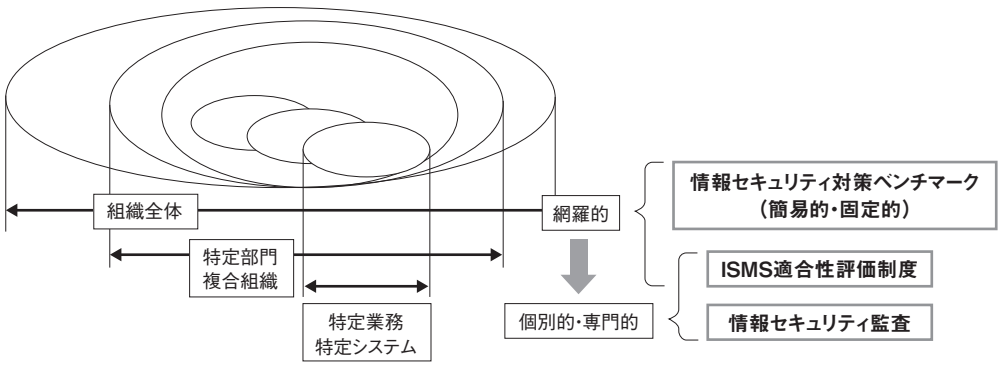

図1.1　評価の対象範囲と評価内容

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

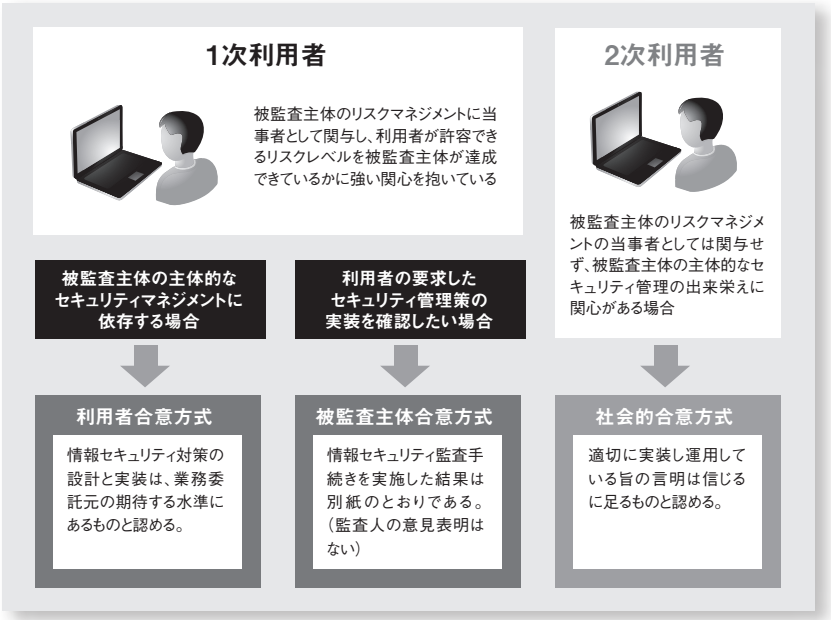

図1.2　利用者にとっての保証型監査3方式の意味と使い分け

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

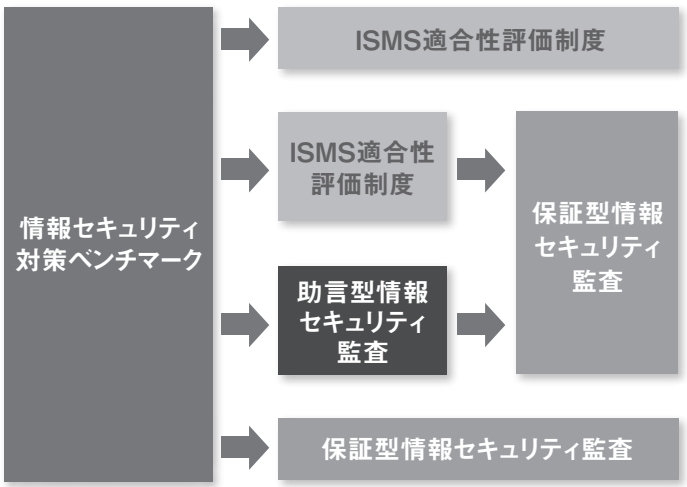

図1.3　情報セキュリティ対策ベンチマークから他制度への展開例

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。