独立行政法人 情報処理推進機構

組織の情報セキュリティ対策自己診断テスト

情報セキュリティ対策ベンチマーク活用のご案内

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

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

http://www.ipa.go.jp

2008年1月

情報セキュリティ対策ベンチマーク

情報セキュリティ対策は、ウイルス対策や脆弱性対策、暗号化や認証などの技術的対策にとどまらず、組織的対策、物理的対策、人的対策から法令順守まで実に多種多様です。たとえば、情報セキュリティポリシーの策定や対策推進体制の整備、情報の分類とライフサイクルに応じた取扱い、従業員の管理、外部委託先の管理、入退出管理、セキュリティ事故対応など多岐にわたります。情報セキュリティ対策が多様化する中、対策に漏れはないか、他社と比べて自社の対策がどのレベルにあるのかチェックしたいと考える企業や組織も多いことでしょう。組織として必要な対策を体系的に網羅し、チェックできるツールがあるなら、とても便利に違いありません。

独立行政法人 情報処理推進機構（IPA）のWebサイトでは、自組織のセキュリティ対策状況を自己診断できる「情報セキュリティ対策ベンチマーク」を提供しています。情報セキュリティ対策ベンチマークは、経済産業省公表の施策ツールを、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上で提供しているもので、公開以来、多くの企業に利用されています。診断結果は、自組織や委託先の情報セキュリティ対策の実施状況の確認に活用できます。また、ISMS認証取得の準備段階や、情報セキュリティ監査の準備段階での活用も可能です。

情報セキュリティ対策ベンチマーク活用集

これまで、本システムを様々なケースに応じて活用するための具体的な活用方法等が示されていないことからIPA、特定非営利活動法人 日本セキュリティ監査協会（JASA）、財団法人 日本情報処理開発協会（JIPDEC）をはじめとする団体および専門家により構成される**「情報セキュリティ対策ベンチマーク普及検討会」**では、情報セキュリティ対策ベンチマークの更なる普及、活用を目指して、ケースに応じた活用例や、ISMS認証取得や情報セキュリティ監査などの準備段階で本システムを活用するためのケーススタディなどを「情報セキュリティ対策ベンチマーク活用集」としてまとめました。

本活用集の特徴

- 対象者を限定せず、中小企業、大企業、コンサルタントや委託元など広く活用していただけます。
- 現場での応用を考慮し、実際のビジネスシーンを想定したケーススタディを示しています。
- 情報セキュリティ対策ベンチマークと、ISMS認証や情報セキュリティ監査との関係を具体的に示し、これらの評価を受ける準備段階での手引きとしても活用していただけます。

本活用集（全128ページ）の公開場所

IPAのWebサイト（下記URL）よりダウンロードいただけます。

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

組織の情報セキュリティ対策状況を評価する

情報セキュリティ評価には、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があります。これら評価のベースとなる規格は、情報セキュリティマネジメントの規格であるJIS Q 27001やJIS Q 27002です。しかし、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ります。

- 情報セキュリティ対策ベンチマークは、全組織や特定部門を対象範囲としたWebベースの自己診断システムです。情報セキュリティ対策の取組状況の評価項目は、ISMS認証基準 附属書Aの管理策（133項目）をもとに、組織的対策、人的対策、物理的対策、技術的対策を網羅し、25項目に整理されています。
- ISMS適合性評価制度は、認定された審査登録機関と審査員による第三者評価です。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することができます。評価にあたっては、JIS Q 27001附属書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ます。
- 情報セキュリティ監査は、中立の専門家である監査人による第三者評価です。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、特定部門などに絞り、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、より詳細な個別的、専門的な評価を実施することに特徴があります。

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ができます。

表　情報セキュリティ対策を評価する3つの評価方法の比較

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	組織の情報セキュリティ対策の整備・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	JISQ27001を参照し作成された25の評価項目（網羅的・簡易的・固定的）	JISQ27001（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・複合組織を指します。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す。

情報セキュリティ対策ベンチマーク活用集　第1章より

情報セキュリティ対策ベンチマークの活用例　>> 診 断

情報セキュリティ対策ベンチマークの概要

図　情報セキュリティ対策ベンチマークの概要

入力

Webで40項目の質問に回答

例：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?

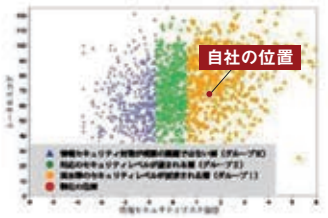
評価項目（全40項目）

情報セキュリティ対策（25項目）
- 組織的な取組み
- 物理的（環境的）施策
- 通信・システムの運用管理
- アクセス制御、開発・保守
- 事故対応状況

企業プロフィール（15項目）
- 従業員数、売上高、拠点数
- 重要情報の保有数、IT依存度など

診断結果の出力

① 散布図による診断企業のポジショニング提示
② レーダーチャートによる平均や望まれる水準との比較
③ スコアの表示
④ 推奨される取組の表示



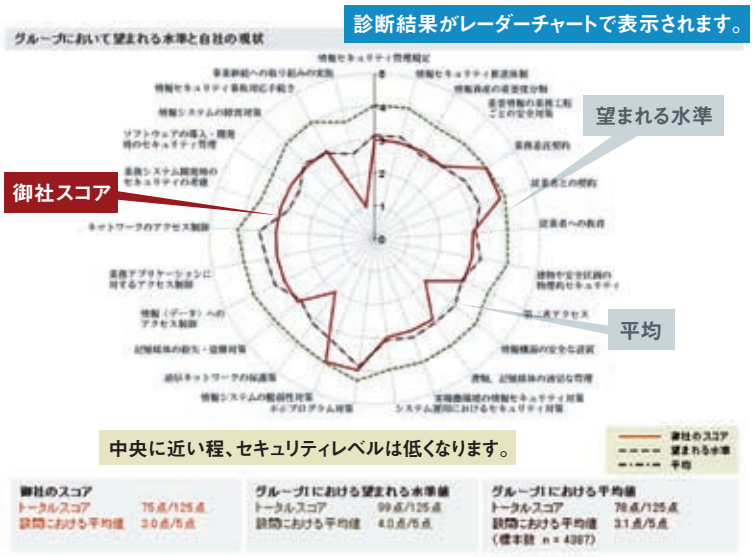
診断結果の例（散布図）

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の取組状況（25項目）と企業プロフィール（15項目）を回答することにより、セキュリティ対策の取組状況がどのレベルに位置しているかを確認できる、Webベースの自己診断システムです。診断結果では、情報セキュリティ対策の取組状況がスコア（点数）で表示されるほか、散布図により、他社と比較した診断企業の位置の確認や、レーダーチャートによる平均値や望まれる水準との比較ができます。

情報セキュリティ対策ベンチマークの特徴

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情報セキュリティ対策に関する理解が深まる。
4. 対策を実施していない会社にとっては、セキュリティ対策を始める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. 他社との比較により、経営層の危機意識が高まり、情報セキュリティ対策が加速する。

図　レーダーチャートによる診断結果の例



評価結果の利用

評価結果は、自組織の情報セキュリティ対策の実施状況の確認、自組織の対策状況の外部への説明、外部委託先や子会社の対策状況の確認など、様々な局面で利用することができます。また政府機関が外部委託先の情報セキュリティ水準を評価する方法として、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」では、「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ています。

情報セキュリティ対策ベンチマークの活用例

a）他社と比べた自社の位置の確認
b）全社の情報セキュリティ対策の実施状況の把握
c）部門ごとの情報セキュリティ対策実施状況の比較
d）定期的利用で、情報セキュリティ対策の改善と向上
e）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や指導
f）委託元や取引先の要求を満たすために診断結果を提示
g）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
h）ISMS適合性評価制度の準備段階で利用
i）情報セキュリティ監査の準備段階で利用

情報セキュリティ対策ベンチマーク活用集（第2章）には次のケーススタディが紹介されています。

▶ 自社のセキュリティ対策状況の把握（A社の場合）

A社は社員数50名の中小企業。ウイルス対策などは行っているが、その他のセキュリティ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セキュリティ対策を見直すことになり、情報セキュリティ対策ベンチマークを利用して、全社のセキュリティ対策状況の把握と改善を行う。

▶ 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？

▶ 共通の尺度によるグループ内統制（X社の場合）

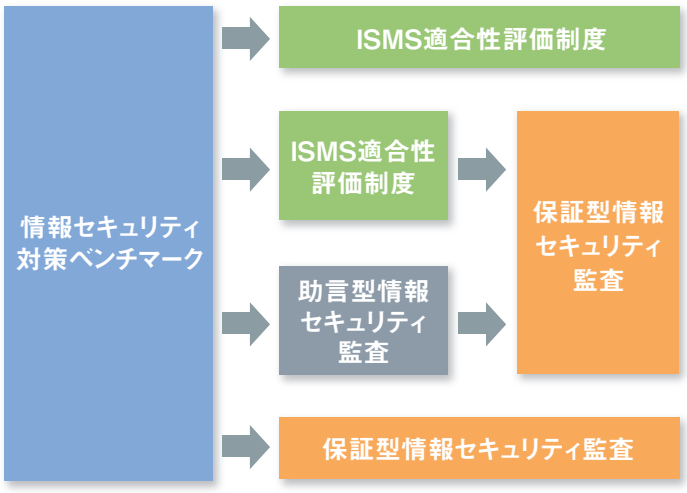
100社を超えるグループ子会社を傘下にかかえる、大手製造メーカーのX社。これらのグループ会社に業務を委託することも多く、委託に際しては、会社の重要な技術情報を提供することもある。法令順守の観点からも、企業秘密の保全という観点からも、グループ会社のセキュリティ対策状況の把握や、その対策状況の改善は、X社にとって、重要な課題である。X社はどのようにして、100社を超えるグループ会社のセキュリティ対策状況を把握したのだろうか？

他の制度への展開例

情報セキュリティ対策ベンチマークの評価を基に、更に情報セキュリティレベルを向上させ、ISMS認証取得や情報セキュリティ監査にステップアップする展開例として、次の4つのケースが想定されます。

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のセキュリティ水準確保の確認要請があり、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、更に委託元などから個別のセキュリティ水準確保の確認要請があり、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　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



情報セキュリティ対策ベンチマークからISMS適合性評価制度へ >> 認 証

ISMS適合性評価制度の概要

ISMS適合性評価制度は、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、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評価し、その結果に基づき認証を与える制度です。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ます。認証を受ける範囲は、保護すべき情報資産を考慮して組織自身が定めることができます。

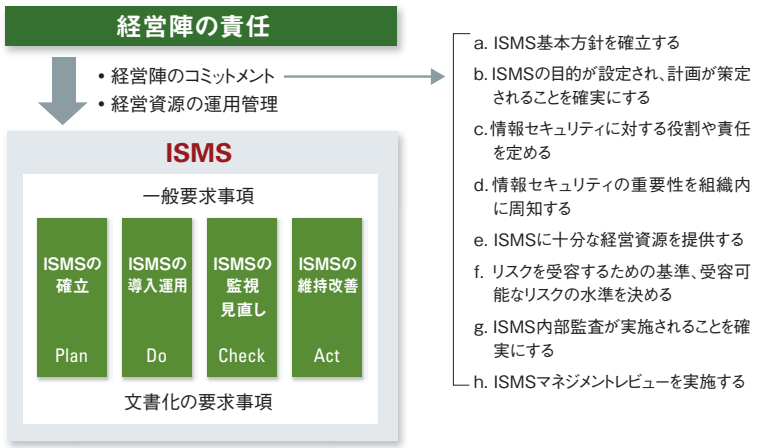
ISMS適合性評価制度の特徴

1 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求められる。

2 JIS Q 27001の一般要求事項は、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。

3 この審査に合格し認証取得すると、情報セキュリティマネジメントについて国際規格に定められたレベルにあることが保証される。

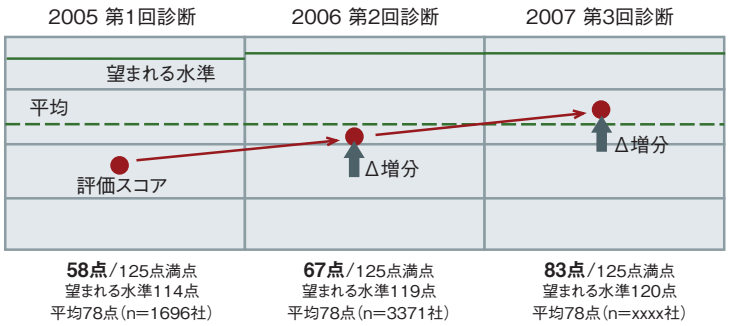
図　ISMS適合性評価制度の概要



情報セキュリティ対策ベンチマークのISMS認証取得への活用例

情報セキュリティ対策ベンチマーク活用集（第3章）には次のケーススタディが紹介されています。

図　情報セキュリティ対策ベンチマーク診断結果の時系列での比較



58点/125点満点
望まれる水準114点
平均78点（n=1696社）

67点/125点満点
望まれる水準119点
平均78点（n=3371社）

83点/125点満点
望まれる水準120点
平均78点（n=xxxx社）

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、全社的に情報セキュリティ対策の実態を時系列で把握していたが、ある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。そこで、情報セキュリティ対策ベンチマークの診断結果を踏まえ、ISMS構築およびISMS認証取得の検討を行った。

ISMS認証取得へ活用するポイント

1 ギャップ分析における活用

ギャップ分析実施の目的は、現状の管理策の適用状況の把握にある。JIS Q 27001の管理策の適用状況を初期段階でチェックするためにベンチマークを利用することが可能である。

2 マネジメントレビューにおける活用

たとえば、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、当該管理策を導入する前に実施したベンチマークの診断結果との比較は有効である。

3 情報セキュリティ対策の運用及び記録段階での活用

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。

1、2、3 いずれの場合も対策のポイントを含め参照することが推奨される。

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　>>監 査

情報セキュリティ監査の概要

情報セキュリティ監査は、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、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参照して策定された個別管理基準に照らし、保証意見や改善提言などの助言を表明する、第三者評価です。

情報セキュリティ監査の特徴

1 助言型監査と保証型監査

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監査と、委託元など利害関係者が、委託先などが期待するセキュリティ水準にあることの保証を求める保証型監査がある。

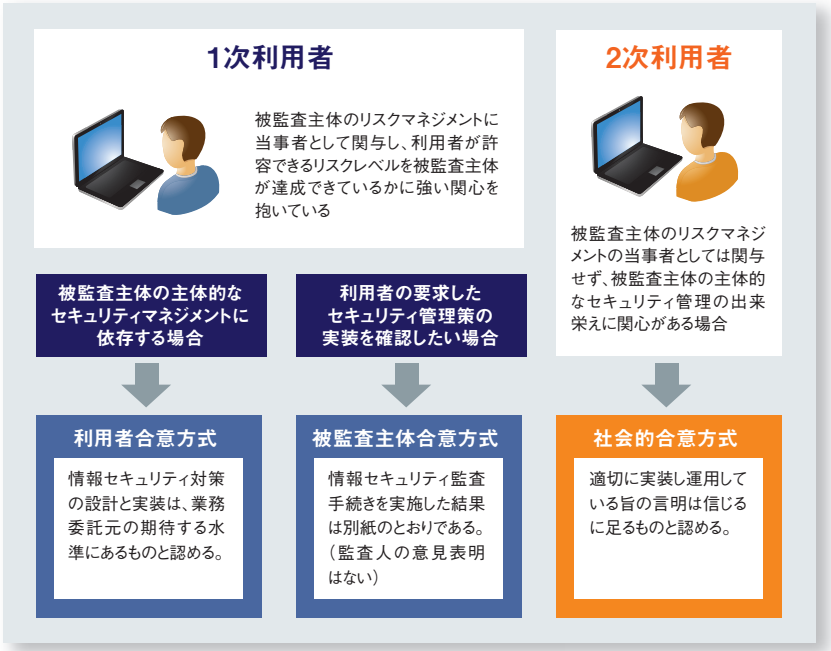
2 保証型監査の有用性

委託先の選定時に、ISMS認証や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は有効であるが、情報セキュリティ対策（コントロール）が、期待する水準や要求事項に対して適正に行われているかを評価するには、保証型監査が最も適切な手段である。

3 保証型監査の3方式

被監査組織のリスクマネジメントに対して、委託元など利害関係者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、右図の3方式がある。

図　保証型情報セキュリティ監査の3方式



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

情報セキュリティ対策ベンチマーク活用集（第4章）には次のケーススタディが紹介されています。

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

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、助言型の情報セキュリティ監査を受けることになった活用例を紹介。

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）

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り、政府機関統一基準に基づきT独立行政法人が定めたセキュリティ要求事項に対して、被監査主体合意方式と呼ばれる保証型情報セキュリティ監査を受けることになった活用例を紹介。

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）

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、保証型情報セキュリティ監査を受けるよう求められ、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ことになった活用例を紹介。

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）

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、保証型情報セキュリティ監査を上手に活用しながら、グループ企業の情報セキュリティ水準の底上げを図った利用者合意方式の活用例を紹介。

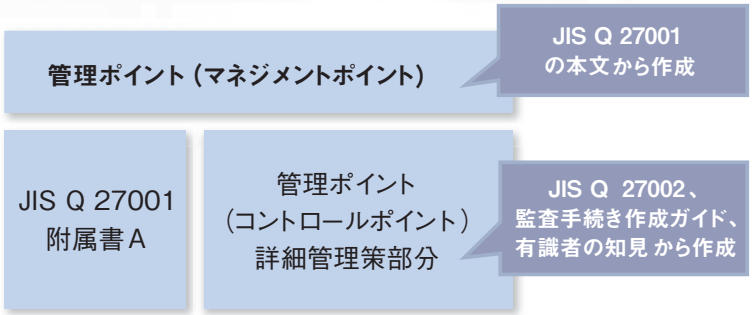
各評価の準拠する基準

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化したものです。
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状況を評価する25項目は、JIS Q 27001:2006の附属書Aの管理策をもとに作成されています。また、それぞれの評価項目に付随す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す。

表　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. 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			50
3. 資産の管理	5			
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

図　情報セキュリティ管理基準Ver2.0の構成



情報セキュリティ監査で使用する情報セキュリティ管理基準は、ISO/IEC 17799:2000をJIS化したJIS X 5080:2002に準拠しています。この規格がJIS Q 27001:2006に改定されたのに伴い、情報セキュリティ管理基準Ver.2.0への改定作業が進んでいます。

情報セキュリティ対策ベンチマーク活用集　付録より抜粋

IPA　Japan information processing JIPDEC Development Corporation　JASA

情報セキュリティ対策ベンチマーク活用集(情報セキュリティ対策ベンチマーク普及検討会編)は、IPAのWebサイト(下記URL)よりダウンロードいただけます。

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

情報セキュリティ対策ベンチマーク普及検討会　メンバー

座　長	大木 栄二郎　工学院大学情報学部 教授
メンバー	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
オブザーバ	財団法人日本適合性認定協会
事務局	独立行政法人 情報処理推進機構