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。