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。

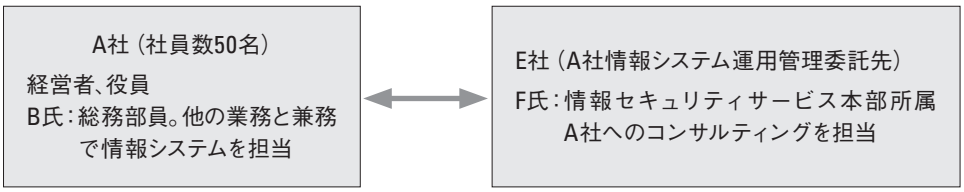
そんな時、顧客情報の漏えい事故を起こしてしまう。この事故をきっかけに全社的に情報セキュリティ対策を見直すことになり、情報システム担当のB氏は、2週間以内に現状の情報セキュリティ対策状況を把握し、改善提案を行うことになった。

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）

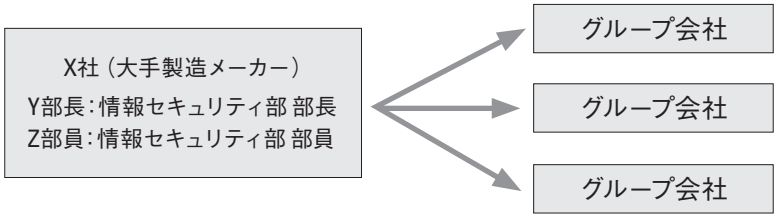
A社では、情報漏えい事故を起こしたことから、情報セキュリティへの関心が高まっている。そこで、役員みずから情報セキュリティ教育を受講することになった。その教育を担当したのがA社に情報セキュリティ対策のコンサルティングを行っているF氏。

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？



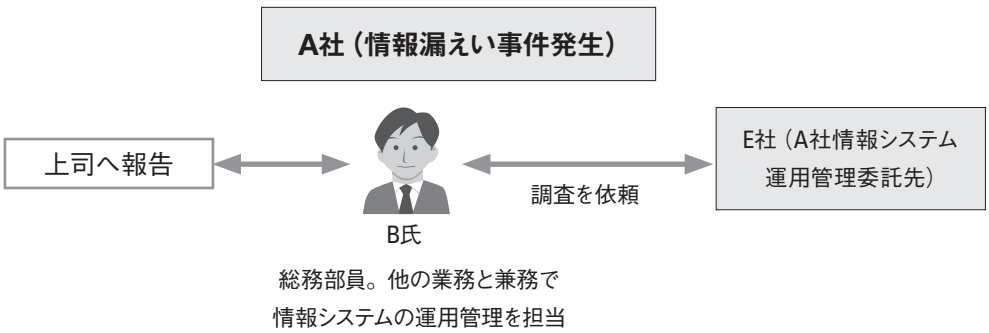
1　A社の場合―自社の情報セキュリティ対策を把握する

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。

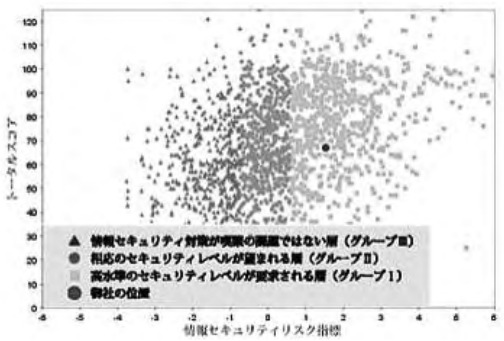


図2.1　診断結果の例（散布図）

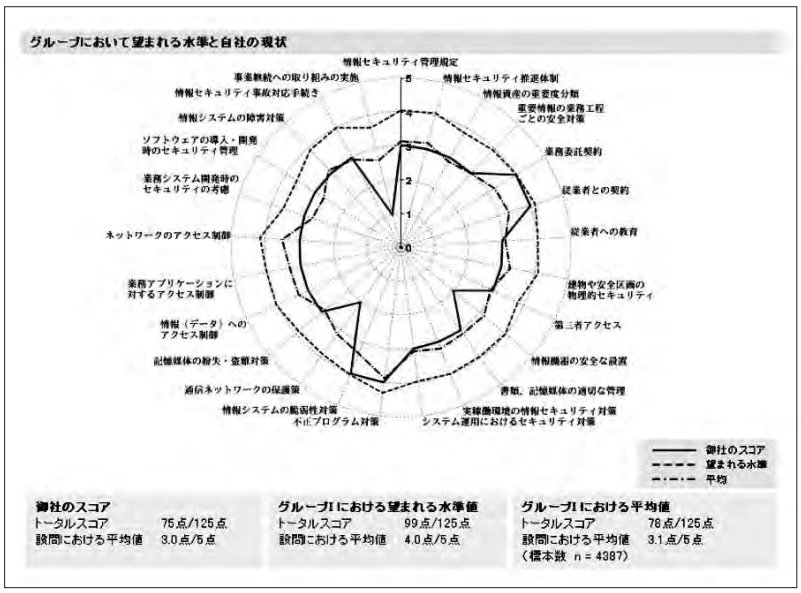
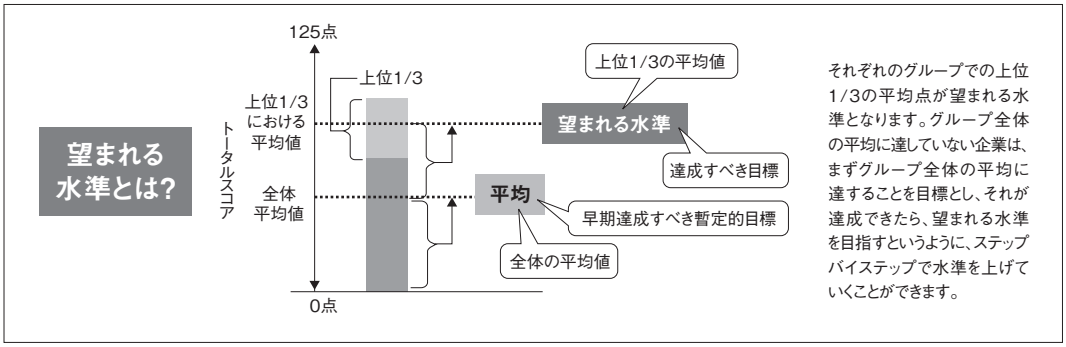


図2.2　診断結果の例（レーダーチャート）

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。

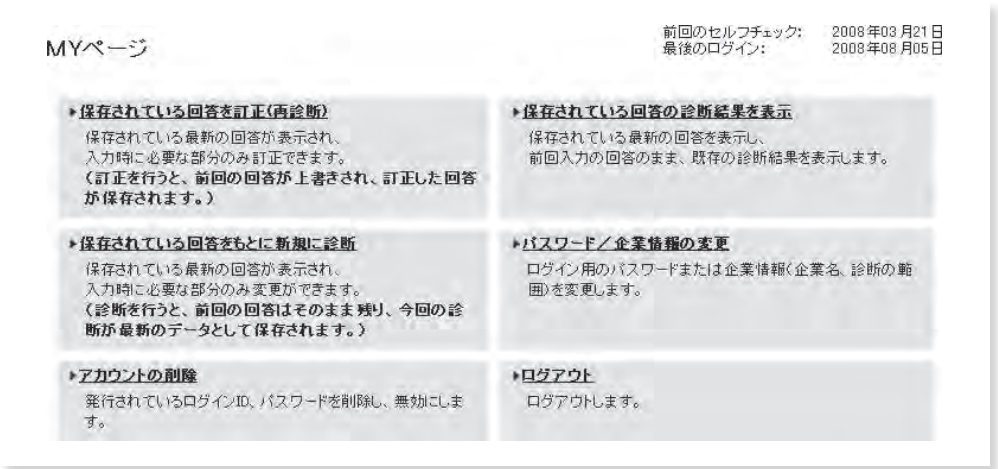


図2.3　情報セキュリティ対策ベンチマークのMyページの画面

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。

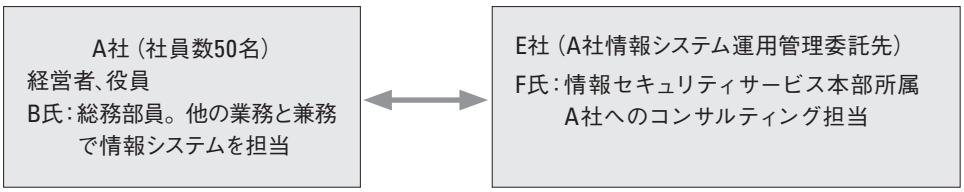
情報システムを利用している企業であれば、情報セキュリティ対策は必須である。しかしながら、中小企業には、情報セキュリティ対策に人やお金を十分に割けないという事情もある。売上げに直接結びつかない情報セキュリティ対策にお金をかけることは、かなり厳しい。もちろん、昨今は、情報セキュリティ対策を行っていることをセールスポイントにする会社も増えているようだが、A社の場合は、そこまで行っていない。

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		

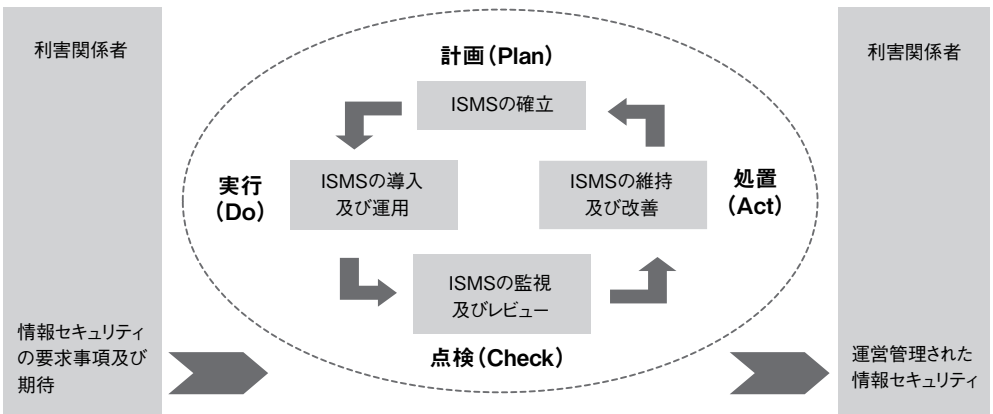


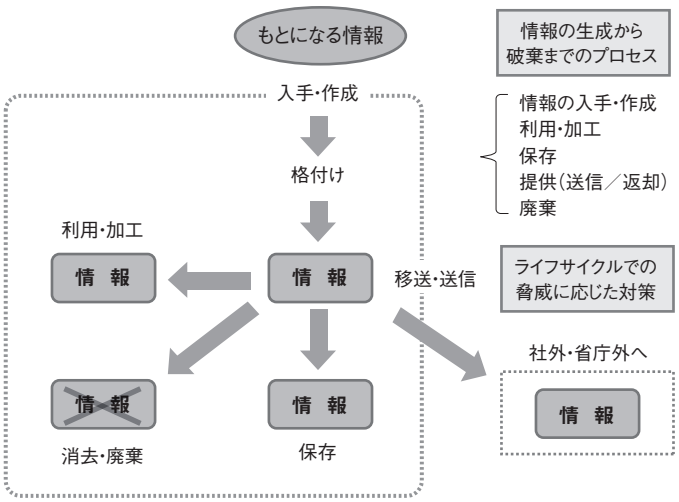
図2.4　ISMSプロセスに適用されるPDCA（出典：JIS Q 27001:2006）

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。

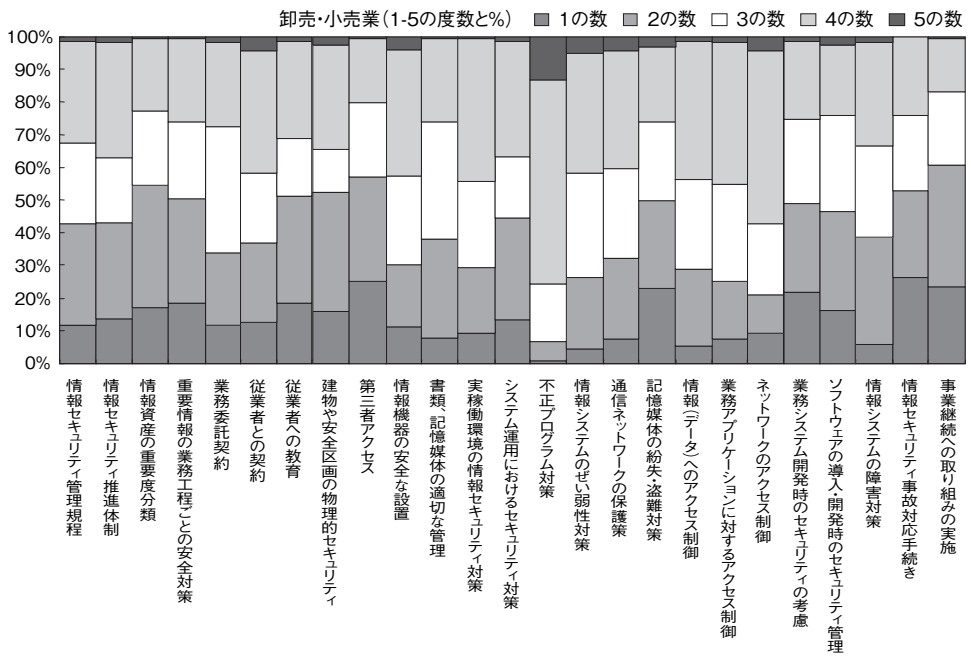


図2.6　Z部員の分析結果のグラフの例示 (業種別1-5の回答数 (%) の比較)

(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。