NPO ISEF
Not-for-Profit Organization of Information Security Forum

特定非営利活動法人
NPO情報セキュリティフォーラム

NPO-ISEF 情報セキュリティレポート：2012-No.01

IPA 情報セキュリティ対策ベンチマーク

独立行政法人 情報処理推進機構（IPA）
技術本部 セキュリティセンター 普及グループ
内山 友弘（Tomohiro Uchiyama）

【著者経歴】

情報システムの SI ベンダーにおいて情報システムの開発、情報セキュリティ対策業務の経験を経て現職。IPA ではインターネット定点観測や情報セキュリティ対策ベンチマークの運用、情報セキュリティ対策の普及・啓発活動を通じて講演や情報発信を行う。情報セキュリティ「対策のしおり」シリーズ（Vol.1～10）の著者でもある。

1 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マネジメントシステム（ISMS）の実施状況を、自らが評価する自己診断ツールである。

ツールの初公開は、2005 年であるが、2007 年には、JIS Q 27001:2006 への対応等多様なニーズへの対応や、ユーザへのヒアリングに基づき、ツール自体を大幅に改訂し、ver3.0 として公開した。

さらに、2008 年からは、診断結果の表示項目の追加と、情報セキュリティをめぐる環境変化や対策レベルの変化を勘案し、最新 2 年間のデータを基準(診断基礎)データとして採用し始めた(ver.3.1 以降)。

また、2011 年からは、当ツールの国際(アジア圏）展開を踏まえ、情報システムを取り巻く環境の変化に伴う組織の情報セキュリティ対策の取り組み状況に関して ERIA(東アジア・ASEAN 経済研究センター)*1の提言を取り入れ、新たに 2 項目の参考質問を追加した。この参考質問が正式質問になるのは次期バージョン（ver.4.0）以降(2012 年度内公開予定)である。

*1) ERIA(東アジア・ASEAN 経済研究センター)

ERIA のアジア共通ベンチマークに関する提言により、アジア地域での情報セキュリティ対策の普及･標準化等に、IPA が運用する情報セキュリティ対策ベンチマークシステムが利用できることを確認し、アジア地域でのセキュリティ診断項目として 2 つの質問事項の追加を要請された。

2 診断方法および診断結果

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 問＋参考質問 2 問）と企業プロフィール（15 項目）を回答することにより、他社と比較して、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自己診断ツールである。

各設問については、以下のサイトを参照されたい。

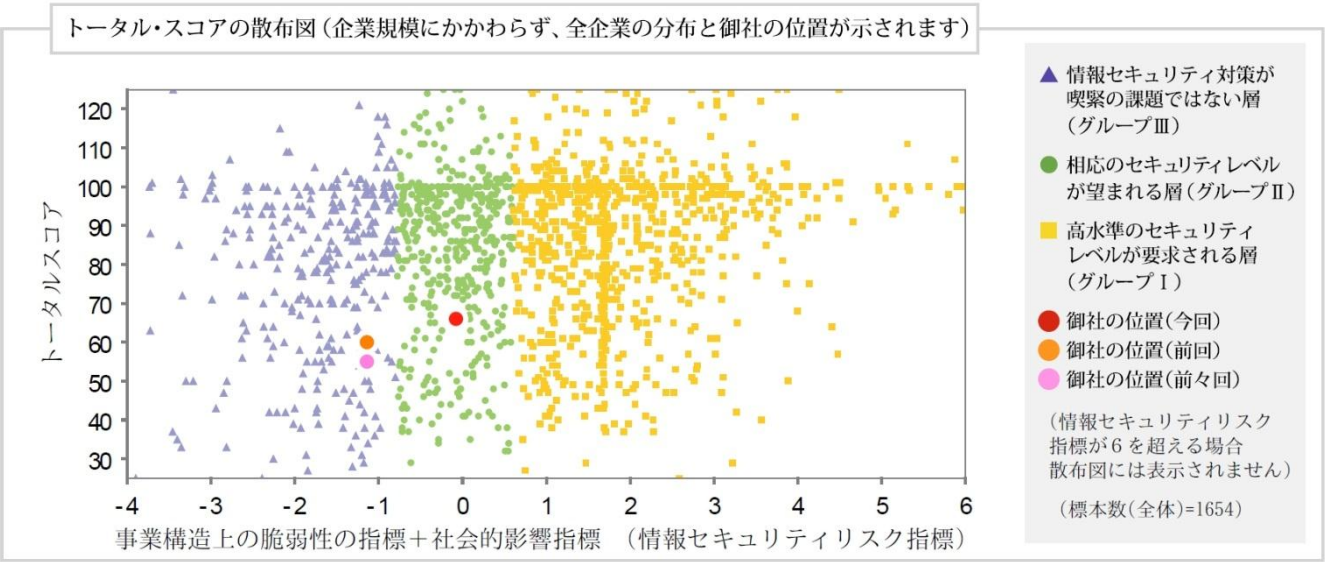
■ 情報セキュリティ対策ベンチマークの質問一覧
http://www.ipa.go.jp/security/benchmark/benchmark-question.html

企業プロフィール(15 項目)からは、情報セキュリティリスク指標*2の値が算出され、診断企業はその指標に応じて、

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

の３つのグループのいずれかに分類される。

【診断結果のサンプル】



企業プロフィールに関する 15 項目の回答から、自社が高・中・低のどのグループに属するかがわかる。

情報セキュリティ対策への取組状況に関する 25 問（参考質問 2 問は除く）の回答から対策状況のスコアが計算される。

- 情報セキュリティに対する組織的な取り組み状況（7 問+参考質問）
- 物理的（環境的）セキュリティ上の施策（4 問）

- 情報システム及び通信ネットワークの運用管理状況（6 問＋参考質問）
- 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 問）
- 情報セキュリティ上の事故対応状況（3 問）

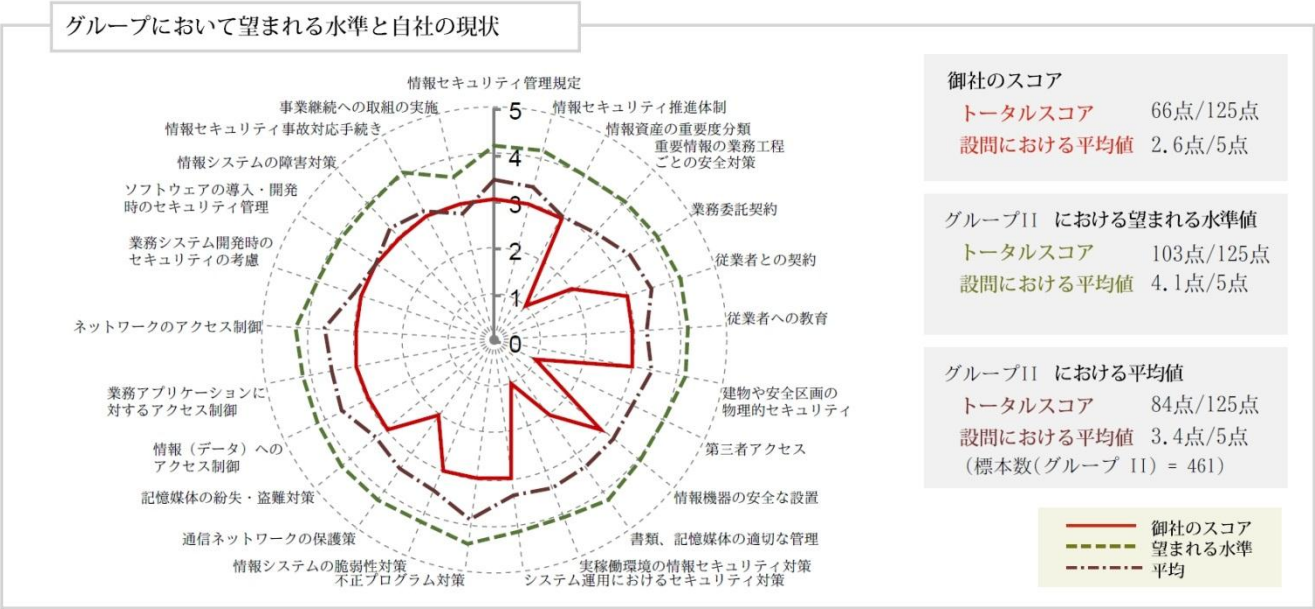
自己診断では、1 から 5 の 5 段階で回答し、これがスコアとなる。

（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

(1)は取り組みができていない状態、(5)は他社の模範となるまで取組みが進んでいるレベルである。各項目は 5 点、トータルスコアは 125 点である（参考質問は除外）。

ちなみに、参考質問を除く 25 問は ISMS 認証基準である JIS Q 27001:2006 付属書 A の管理策（ 133 項目）をベースに作成されている。

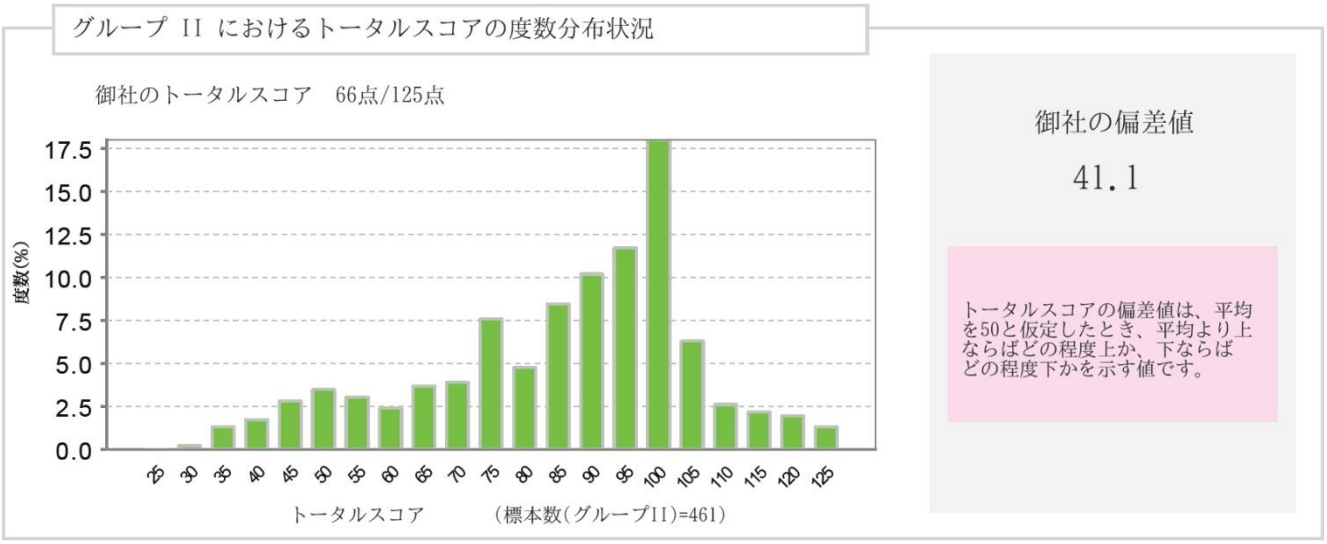
【診断結果のサンプル】



上記のサンプルでは、同じグループ内における自社と他社との比較により、セキュリティ対策の取り組み状況がわかる。つまり、情報セキュリティ対策の取組状況に関する 25 問の回答から、自社がグループ内や同業他社との比較でどのレベルにあり、望ましい水準*3とどの程度のギャップがあるかわかる。

さらに、トータルスコアの度数分布状況と偏差値を表示する。

【診断結果のサンプル】



トータルスコアの度数分布と偏差値は、分類されたグループの中での比較である。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。

表示される診断結果をまとめると以下のようになる。

（1）　トータルスコアの分布と自社の位置を散布図で表示
- 散布図は、全体と企業規模別の 2 種類を表示
- 散布図中の自社の位置は最新の位置と過去 2 回分までの比較が可能

（2）　レーダーチャートによるスコアの比較は 4 種類を表示
- 情報セキュリティリスク指標に応じたグループ別のスコアの比較
- 企業規模別によるスコアの比較
- 業種別によるスコアの比較
- 自組織の最新のスコアと過去 2 回分までのスコアの比較

（3）　トータルスコアの度数分布状況と偏差値を表示

（4）　診断結果を資料として活用可能（PDF で保存・印刷）

（5）　スコアー覧の表示（PDF）

（6）　推奨される取り組みの表示

*2) 情報セキュリティリスク指標

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 依存度などから算出される企業のかかえるリスクを表す指標である。情報セキュリティリスク指標の算出方法は、「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」参考資料 情報セキュリティ対策ベンチマーク p. A1-30 「企業分類に係わる指標の算出方法」を参照されたい（http://www.meti.go.jp/report/downloadfiles/g50331d01j.pdf）。

情報セキュリティリスク指標＝事業構造上の脆弱性指標＋社会的影響力指標

事業構造上の脆弱性指標＝-0.0018×(正社員割合-77.673)/23.249
+ 0.0710×(総拠点数-36.133)/288.791
+ 0.5389×(IT 依存度-2.797)/1.054
+ 0.5326×(インターネット依存度-1.611)/0.858
+ 0.3588×(ビジネスパートナーへの依存度-2.028)/0.892
- 0.0302×(年間離職率-6.037)/8.305

正社員割合は%の値
総拠点数は国内拠点数+海外拠点数
IT依存度は%ベースの1(25%以下)～4(75%以上)の点数
ビジネスパートナーへの依存度は%ベースの1(25%以下)～4(75%以上)の点数
年間離職率は%
※(上記の値-平均値)/標準偏差に係数をかけて合算する

社会的影響力指標＝0.1331×(売上高-61526.4)/127537.8
+ 0.2764×(公益性-2.354)/0.913
+ 0.3082×(顧客への影響-2.203)/0.865
+ 0.3044×(ブランドへの影響-2.598)/0.803
+ 0.3214×(機密情報の保有度-2.256)/0.899
+ 0.2212×(保有個人情報数-249308.1)/822664.5

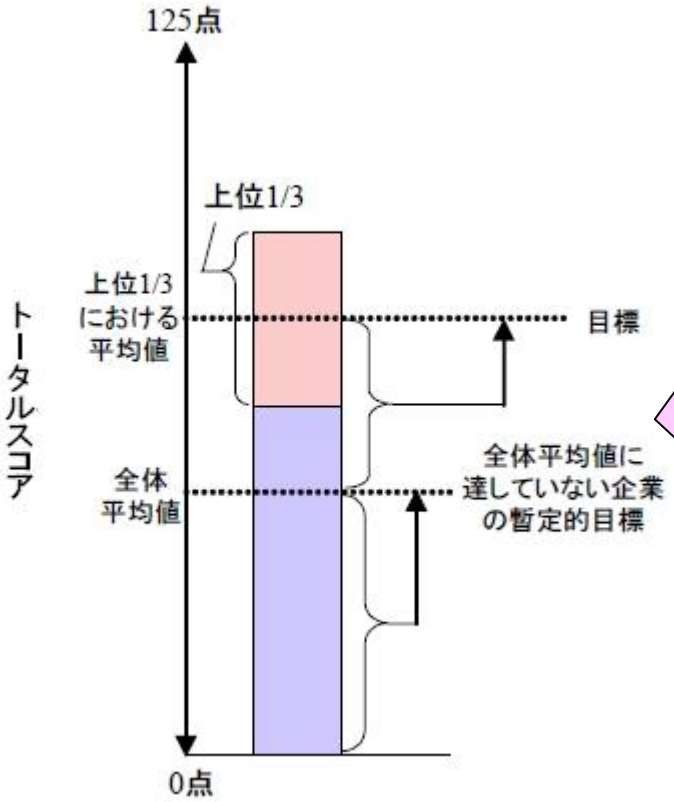
売上高は百万円単位の金額
公益性は、1点(ほとんどない)、2点(少ない)、3点(他の業種に比べると高い)、
4点(事業の性質上極めて高い)の点数
顧客への影響は、1点(ほとんどない)、2点(少ない)、3点(大きな影響がある)、
4点(極めて大きな影響がある)の点数

参考までに、グループⅠとグループⅡの境界となる情報セキュリティリスク指標の値は0.6で、グループⅡとグループⅢの境界となる情報セキュリティ指標の値は-0.79である。

グループⅠ：情報セキュリティリスク指標 >= 0.6
グループⅡ：情報セキュリティリスク指標 < 0.6 and 情報セキュリティリスク指標 > -0.79
グループⅢ：情報セキュリティリスク指標 <= -0.79

*3) 望まれる水準

望まれる水準（目標値）は、トータルスコア順に並べた診断データの上位1/3の診断データの平均値である。



望まれる水準（目標値）の算出

トータルスコア順に並べた診断データの上位1/3に位置するトータルスコアを求め、そのトータルスコアを**超える**トータルスコアを持つ診断データの平均値を「望まれる水準(目標値)」とする。

3 情報セキュリティベンチマークの活用

情報セキュリティ対策ベンチマークの活用方法については，まず評価結果そのものの活用がある。これらは、説明不要だろう。

評価結果の利用

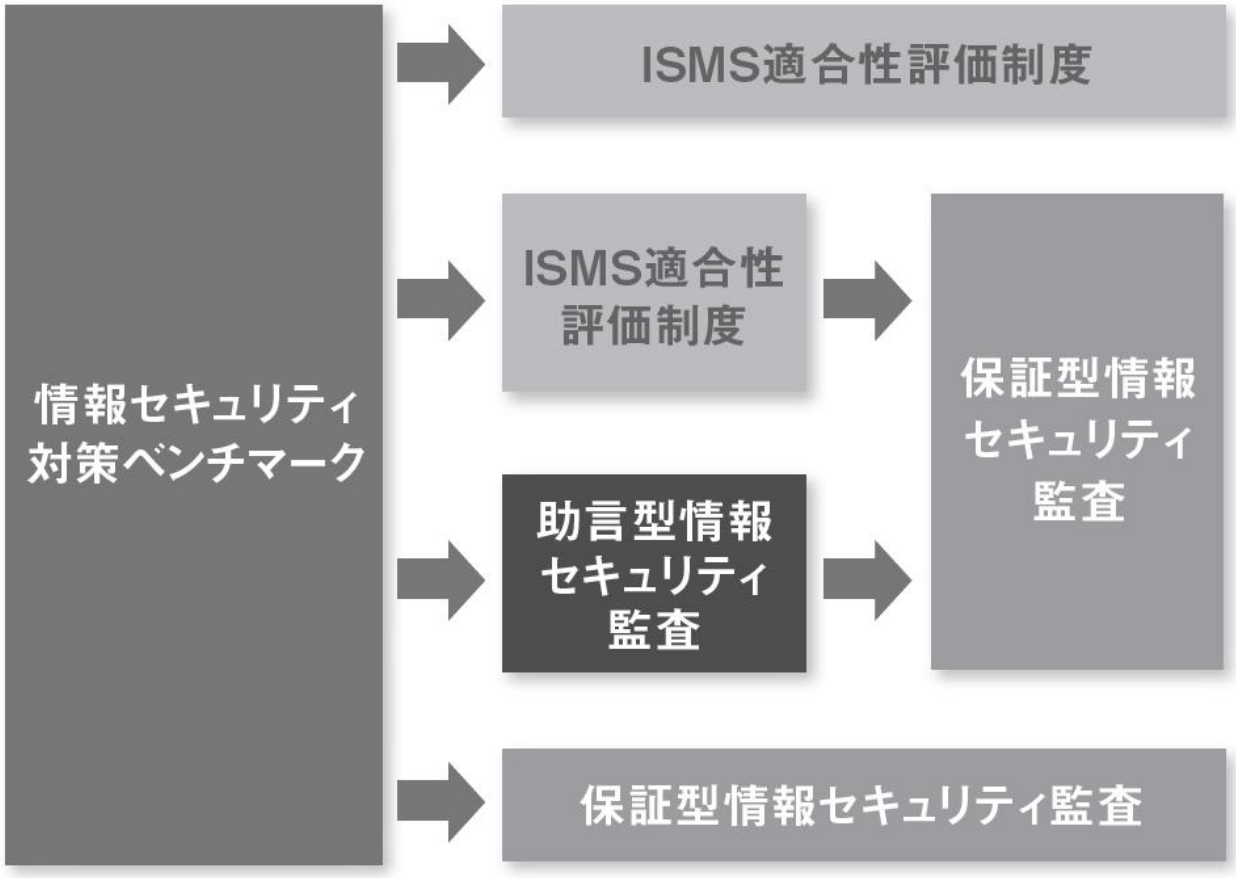
（1） 自社の情報セキュリティ対策の実施状況を確認する
（2） 自社の情報セキュリティ対策状況を外部に説明する
（3） 外部委託先や子会社の情報セキュリティ対策状況を確認する

次に考えられるのは、ステップアップである。

情報セキュリティ対策ベンチマークの利用からの他制度への展開

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、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



情報セキュリティ対策ベンチマークの活用に関する詳細は、以下のWebサイト(PDF)を参照されたい。

■ 情報セキュリティ対策ベンチマーク活用集
http://www.ipa.go.jp/security/benchmark/benchmark-katsuyou.html

以上

2012 年8月1日発行

特定非営利活動法人　NPO 情報セキュリティフォーラム
〒221-0835
神奈川県横浜市神奈川区鶴屋町 2-17　相鉄岩崎学園ビル
TEL(045)311-8777　　FAX(045)311-8747
E-Mail: isef@isef.or.jp　　URL: http://www.isef.or.jp