IPAフォーラム2007

「情報セキュリティ対策ベンチマーク」
～事例に見る活用の広がり～

2007/10/30

大木栄二郎
工学院大学情報学部教授
IBMビジネスコンサルティングサービス顧問
公認情報セキュリティ主席監査人

目　次

1. 情報セキュリティガバナンスとベンチマーク
2. 具体的な活用事例
3. 関連諸制度との関係整理
4. 活用のヒント

情報セキュリティガバナンスとは

社会的責任にも配慮したコーポレート・ガバナンスの要素として、情報セキュリティを支えるメカニズムを内部統制の仕組みとして企業内に構築・運用すること

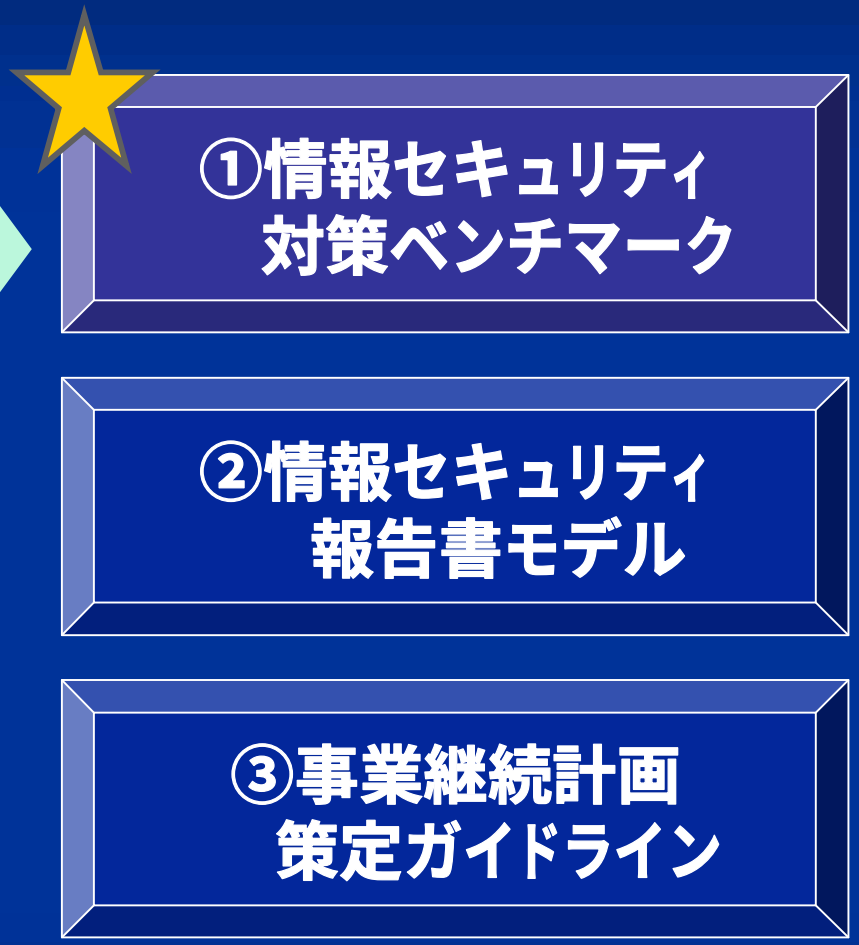
出典：経済産業省「企業における情報セキュリティガバナンスのあり方研究会報告書」平成17年3月

1）「情報セキュリティに絶対はなく、事故は起こりうるもの」との前提に立つ
2）その場しのぎの対症療法的対応から、自律的・継続的に改善・向上する仕組みへ
3）リスクに応じた合理的な対策を実施し、維持する
4）ステークホルダーに適切に開示し支持を得る

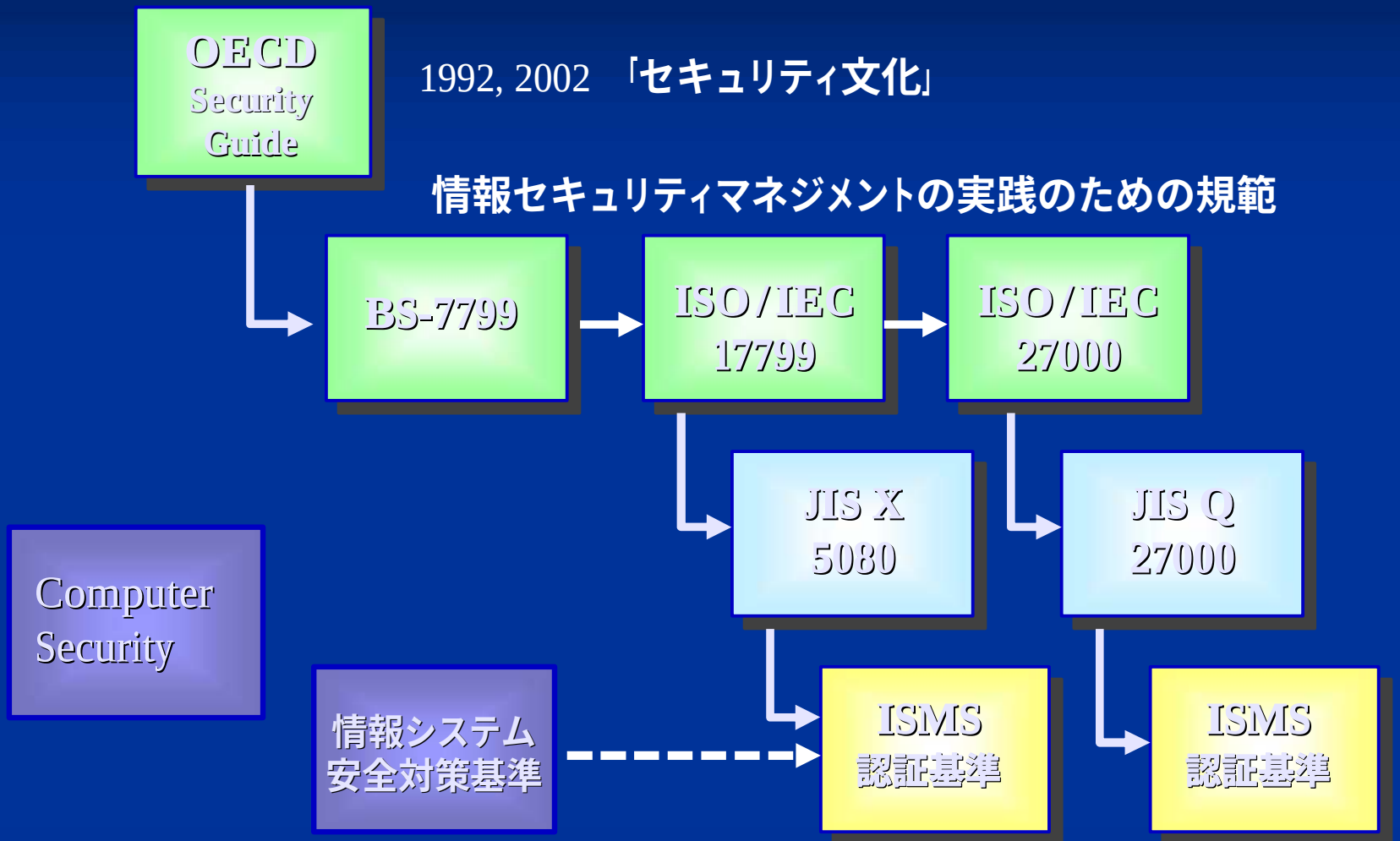
情報セキュリティガバナンス研究会の三つの施策ツール提言

問題

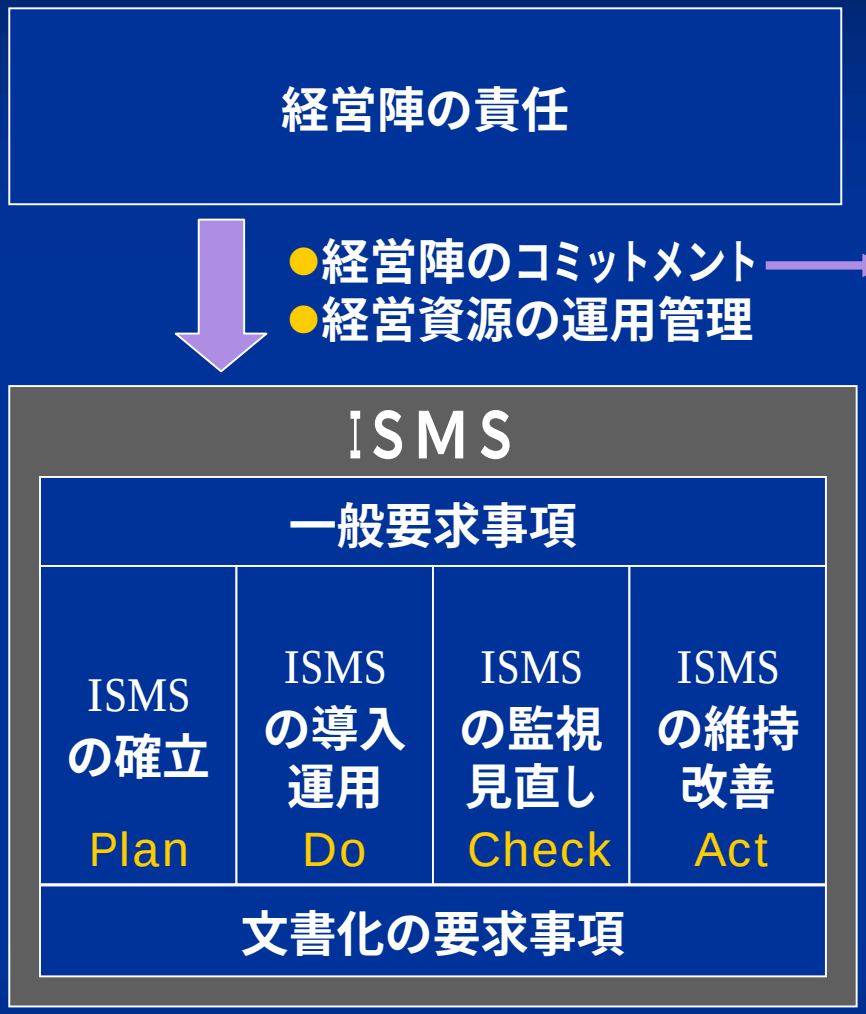
1. IT事故発生のリスクが明確でなく、適正な情報セキュリティ投資の判断が困難
2. 既存の情報セキュリティへの対策や取り組みが企業価値に直結していない
3. 事業継続性確保の必要性が十分に認識されていない



情報セキュリティマネジメント規格の発展



ISO/IEC 27001　ISMSの要求事項



a. ISMS基本方針を確立する
b. ISMSの目的が設定され、計画が策定されることを確実にする
c. 情報セキュリティに対する役割や責任を定める
d. 情報セキュリティの重要性を組織内に周知する
e. ISMSに十分な経営資源を提供する
f. リスクを受容するための基準、受容可能なリスクの水準を決める
g. ISMS内部監査が実施されることを確実にする
h. ISMSマネジメントレビューを実施する

ISO/IEC 27001 ISMSの要求事項

ISMSの確立

1. 適用範囲と境界の定義
2. 基本方針の策定
3. リスクアセスメントの取り組み方法
4. リスクの識別
5. リスクの分析･評価
6. リスク対応の選択肢の評価
7. 管理策の選択
8. 残留リスクの承認
9. ISMSの承認
10. 適用宣言書の作成

P

ISMSの導入運用

1. リスク対応計画の策定
2. リスク対応計画の実施
3. 管理策の実施
4. 管理策の有効性評価
5. 教育訓練および認識プログラム
6. ISMSの運用管理
7. ISMS経営資源の管理
8. インシデント対応

D

ISMSの監視見直し

1. 監視･見直しの手順実施
2. 有効性の定期的見直し
3. 管理策の有効性測定
4. リスクアセスメントの見直し
5. 内部監査の実施
6. マネジメントレビューの実施
7. セキュリティ計画の更新
8. 活動･事象の記録

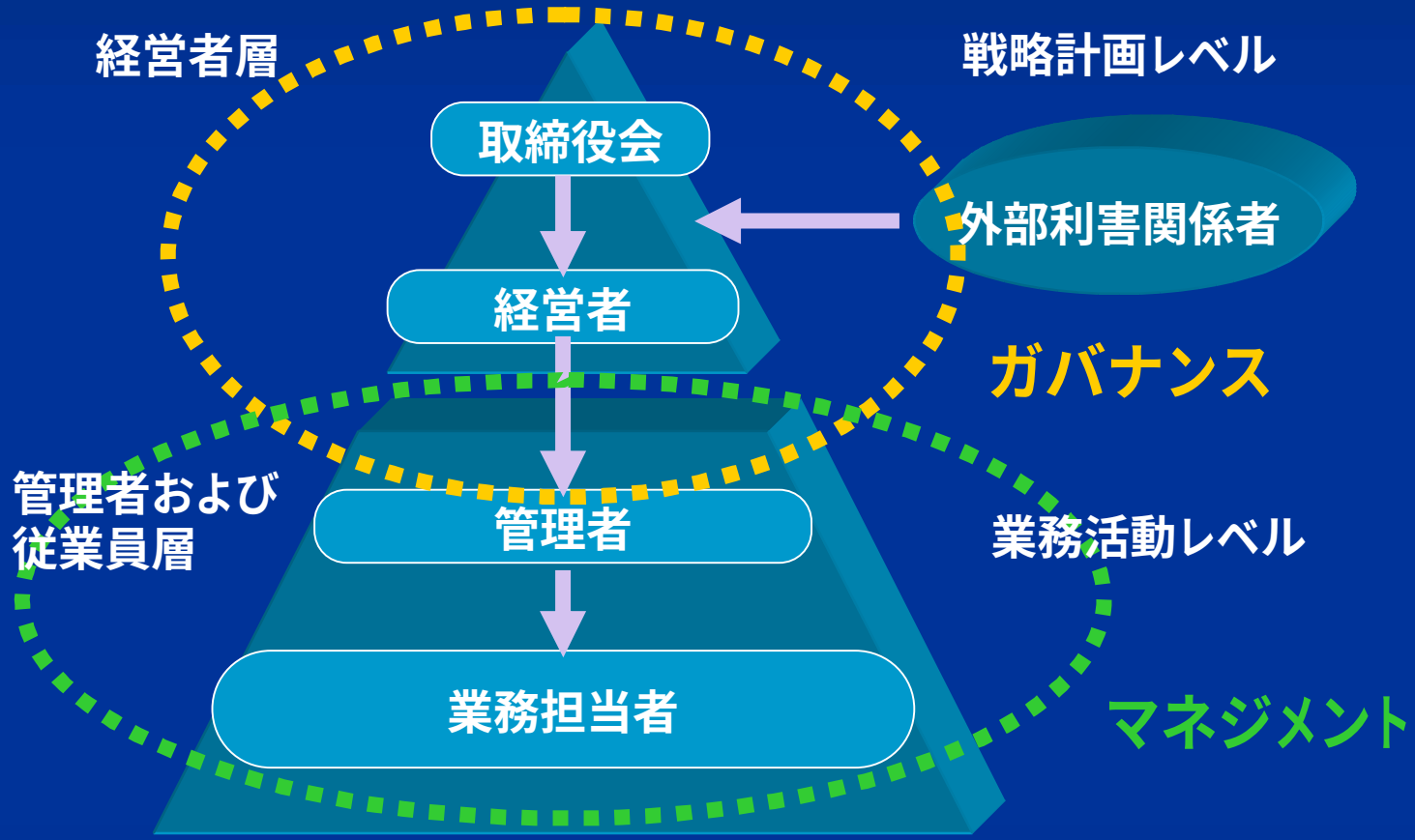
C

ISMSの維持改善

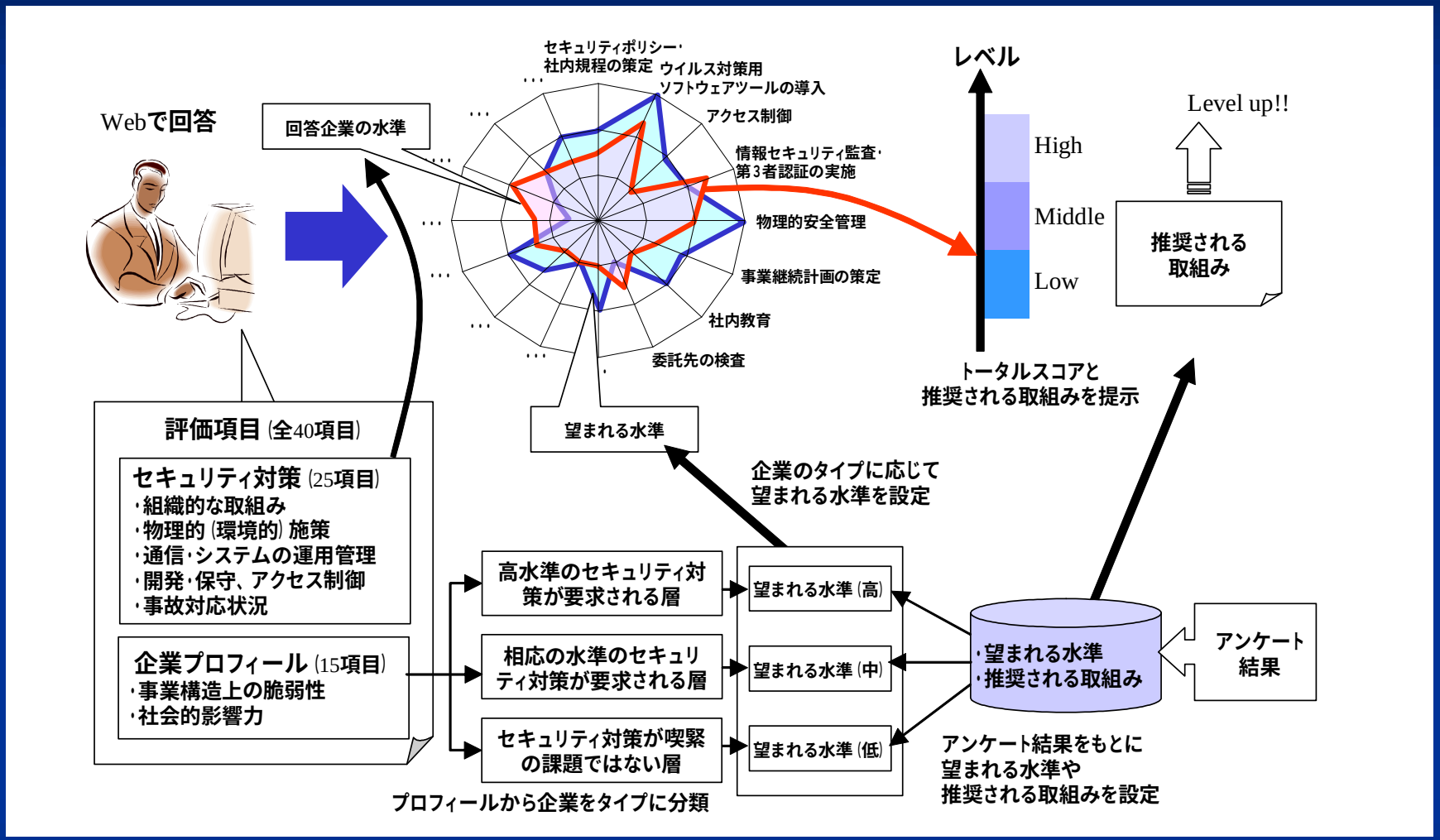
1. 改善策の実施
2. 是正措置･予防措置の実施
3. 利害関係者への処置の伝達
4. 改善による意図した目的の達成

A

マネジメントとガバナンス



情報セキュリティ対策ベンチマークのイメージ



出典：経済産業省　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

ベンチマークの質問と回答

質問(部分)

(a) 情報セキュリティに対する組織的な取組状況

ア）貴社では、情報セキュリティポリシーや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。自社の状況に見合った規程とするためには、サンプルのコピーではなく、自社の事業やリスクを鑑みたものであることが重要です。

イ）貴社では、経営層を含めた情報セキュリティの推進体制やコンプライアンス(法令遵守)の推進体制を整備していますか。

推進体制の整備のためには、監査を含めた各担当者の責任が明文化されることが重要です。

ウ）貴社では、重要な情報資産（情報及び情報システム）については、重要性のレベルごとに分け、そのレベルに応じて管理していますか。

エ）貴社では、個人データなど重要な情報については、取得、利用、保管、開示、消去などの一連の業務工程ごとにきめ細かく適切な措置を講じていますか。

適切な措置とは、作業責任者や手順の明確化、取扱者の限定や処理の記録、確認などを指します。

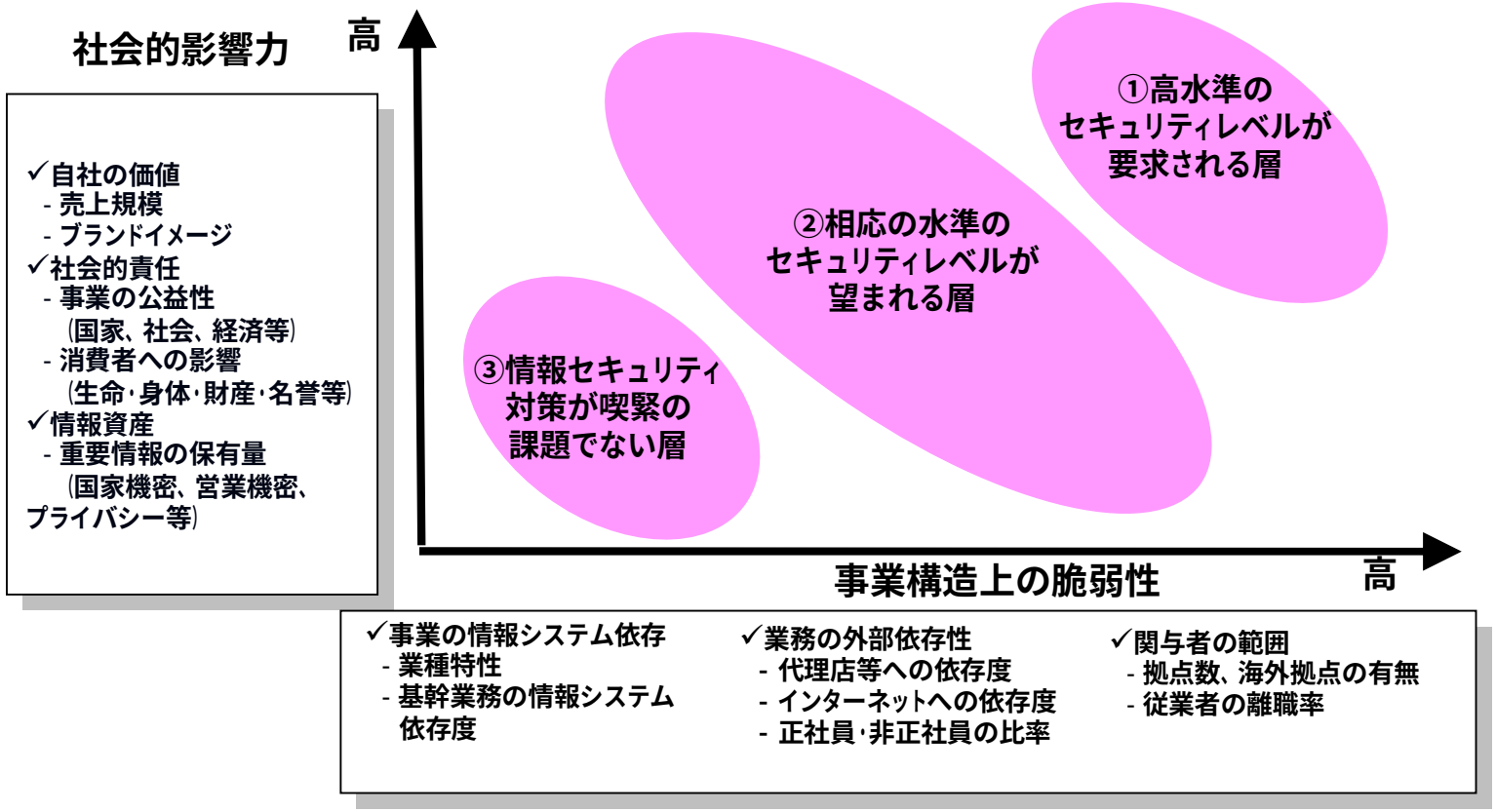
回答選択肢

できていない

できている

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

要求される情報セキュリティの水準に基づく分類



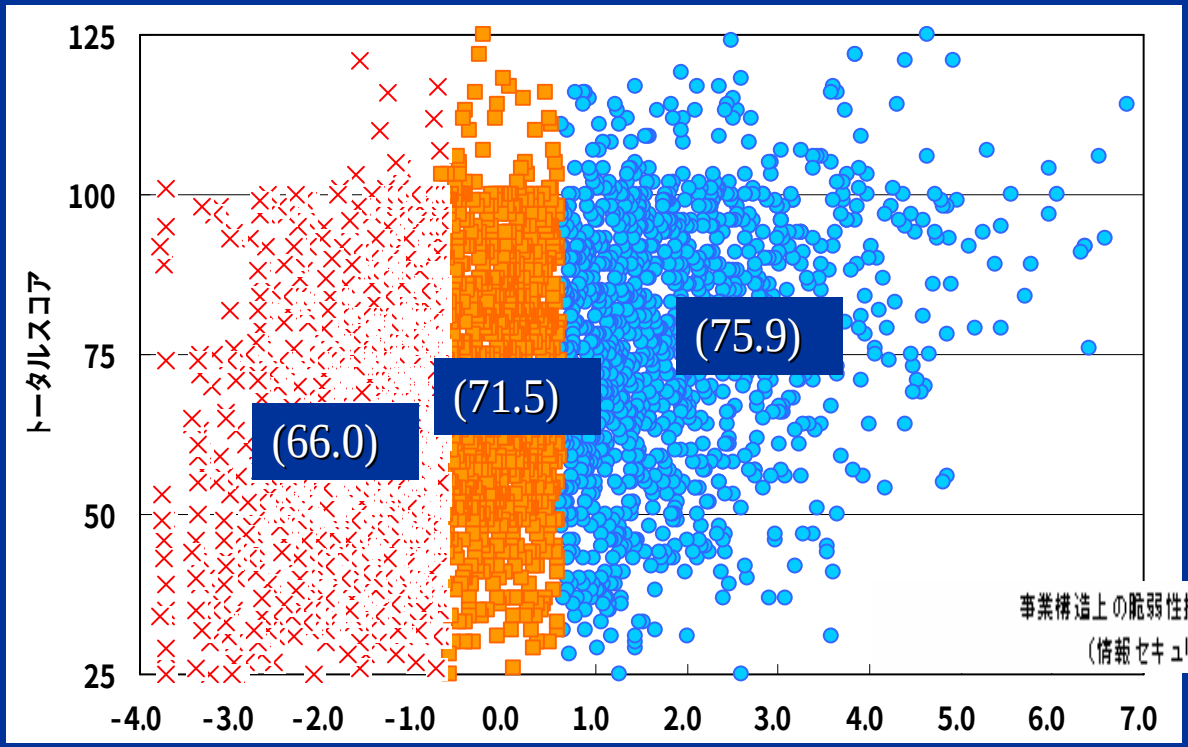
出典：経済産業省　企業における情報セキュリティガバナンスのあり方に関する研究会　報告書

情報セキュリティ対策ベンチマーク
トータルスコアの分布

2006年9月25日現在

全企業　(2,700件より)

26.3%　29.3%　44.4%　各層の構成割合



- 高水準のセキュリティレベルが要求される層
- 相応のセキュリティレベルが望まれる層
- 情報セキュリティ対策が喫緊の課題でない層

平均点　72.0

(カッコ内数値は各層別の平均)

注：縦軸はセキュリティ対策スコア、横軸は情報システム依存度や個人情報の保有数などの業態で決定。

目　次

1. 情報セキュリティガバナンスとベンチマーク
2. 具体的な活用事例
3. 関連諸制度との関係整理
4. 活用のヒント

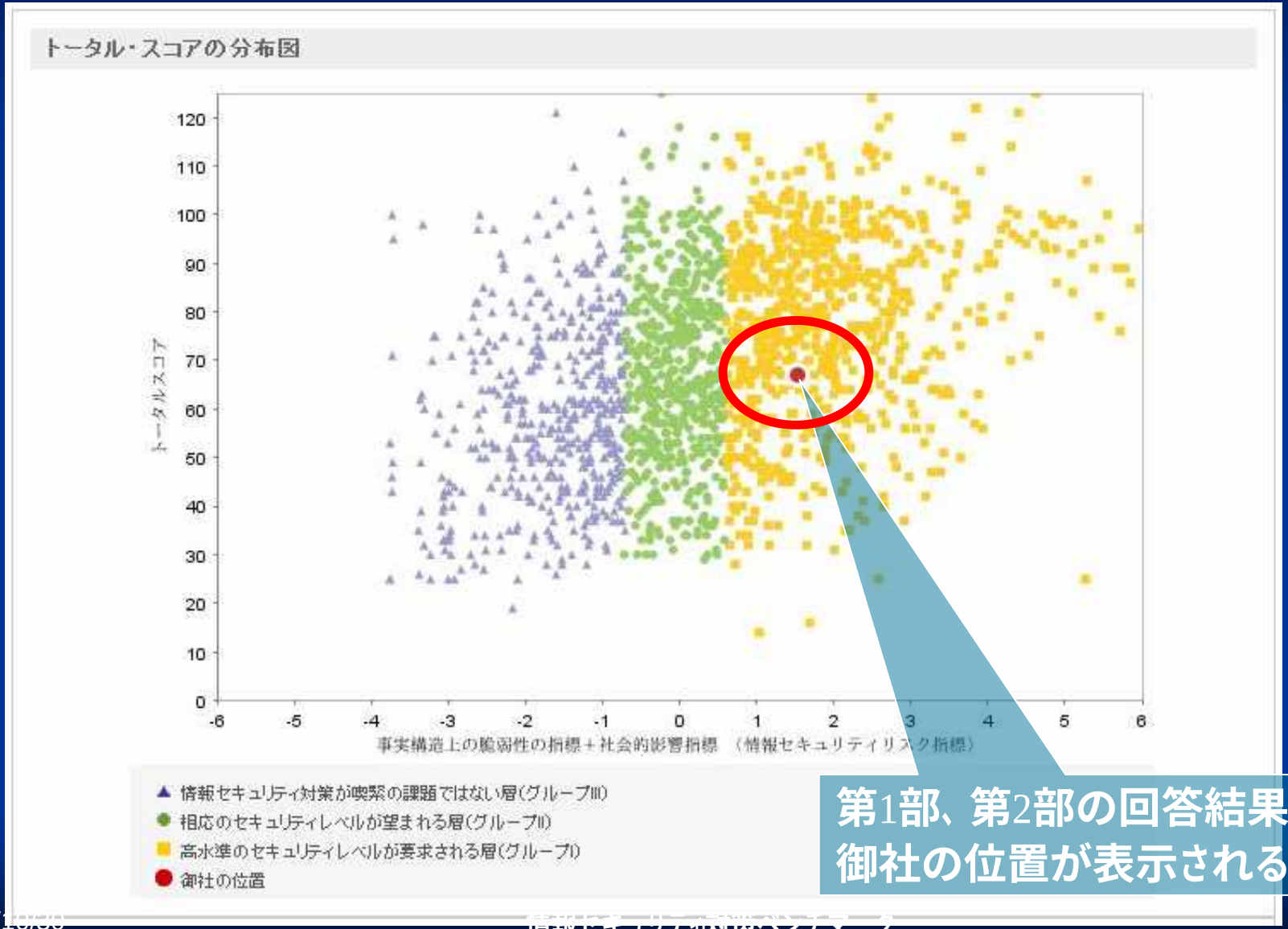
こんなときに！

「自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、何から手を付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・・・。」

活用の事例－１

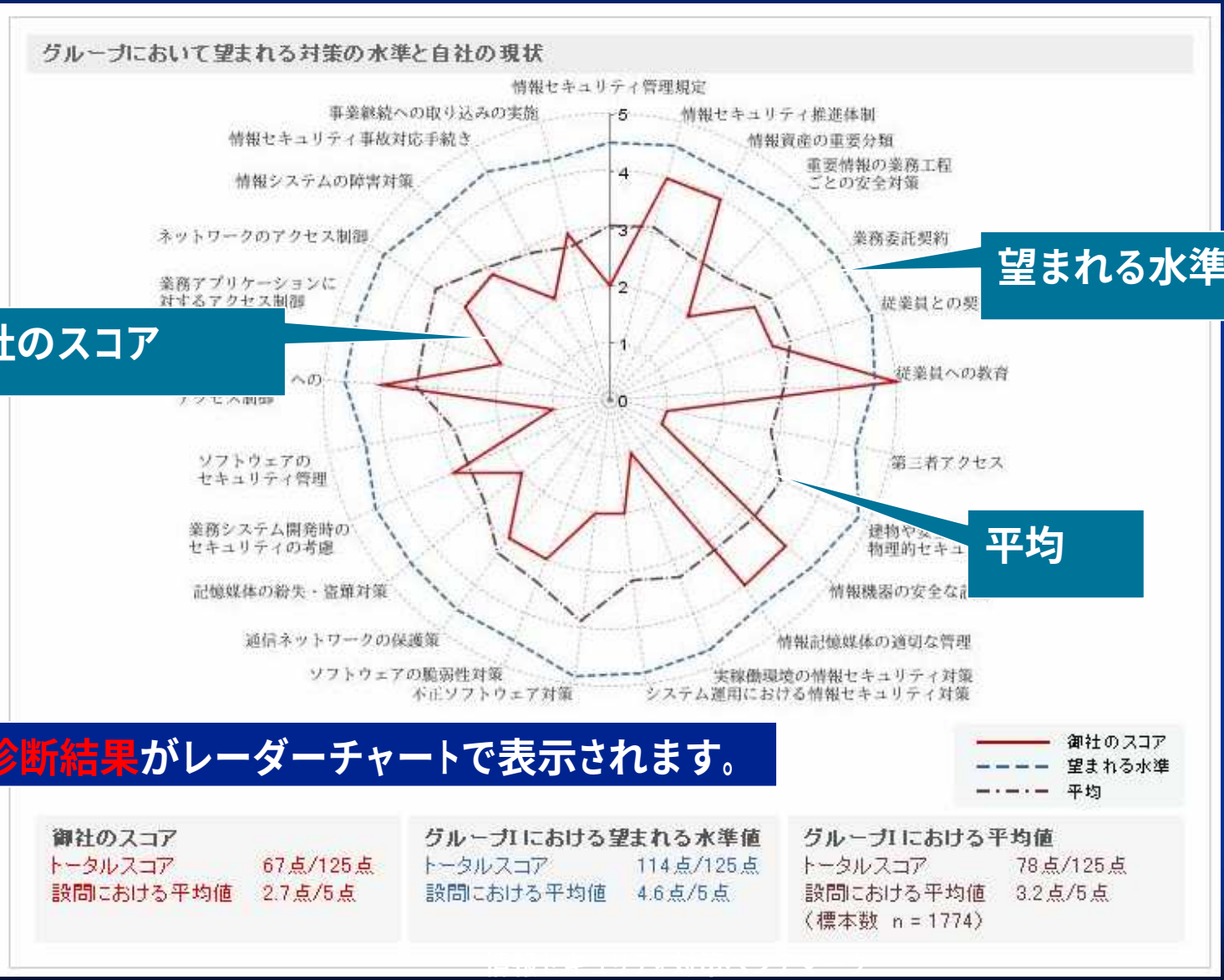
- 経営者が使う
  - 他社と比べた自社の位置を知りたい
  - リスク認識が間違っていないか確認する
- 事業責任者が使う
  - 取引相手の要求を満たす
- 管理者が使う
  - 現状を把握する、部門ごとの比較をする
  - レベルアップを図る

情報セキュリティ対策ベンチマークの利用方法



第1部、第2部の回答結果より、御社の位置が表示される。

情報セキュリティ対策ベンチマークの利用方法



診断結果がレーダーチャートで表示されます。

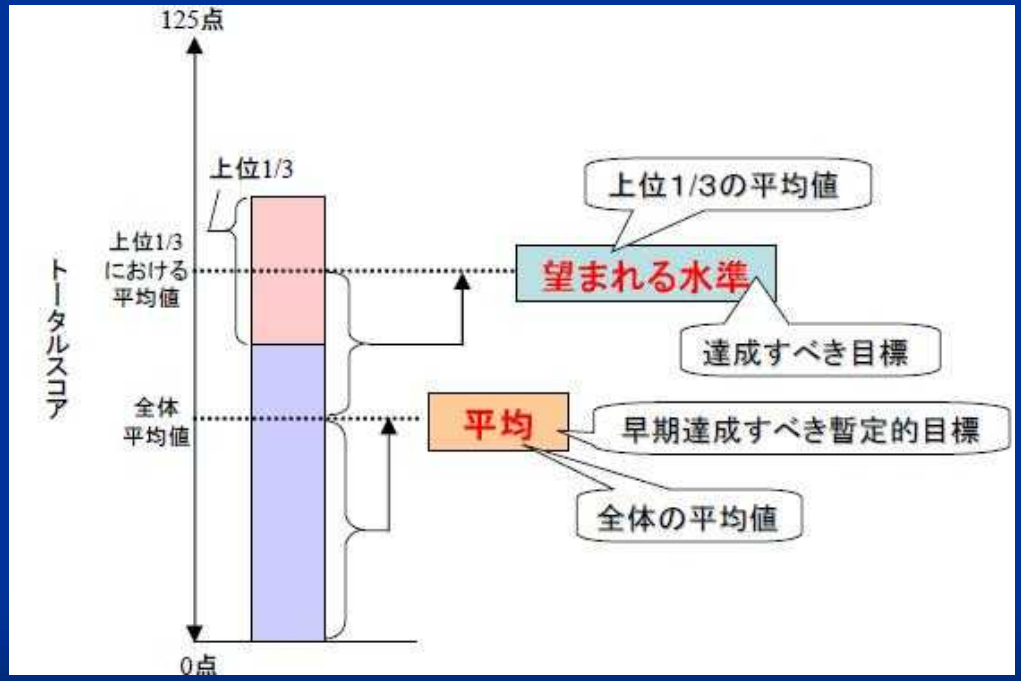
御社のスコア	
トータルスコア	67点/125点
設問における平均値	2.7点/5点

グループIにおける望まれる水準値	
トータルスコア	114点/125点
設問における平均値	4.6点/5点

グループIにおける平均値	
トータルスコア	78点/125点
設問における平均値	3.2点/5点
（標本数 n = 1774）	

望まれる水準とは？

それぞれのグループでの上位1/3の平均点が望まれる水準となります。グループ全体の平均に達していない企業は、まずグループ全体の平均に達することを目標とし、それが達成できたら、望まれる水準を目指すというように、ステップバイステップで水準を上げていくことができます。



DM6-02-061

外部委託における情報セキュリティ対策実施規程 策定手引書

内閣官房情報セキュリティセンター

9.2.2 国際規格を踏まえた委託先の情報セキュリティ水準の評価

政府機関統一基準 6.1.2 外部委託
(1)(c) 統括情報セキュリティ責任者は、委託先の選定基準策定に当たって、その厳格性向上のために、国際規格を踏まえた委託先の情報セキュリティ水準の評価方法を整備すること。【強化遵守事項】

- 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

DM6-06-061 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

4.1.2 調達仕様書の作成

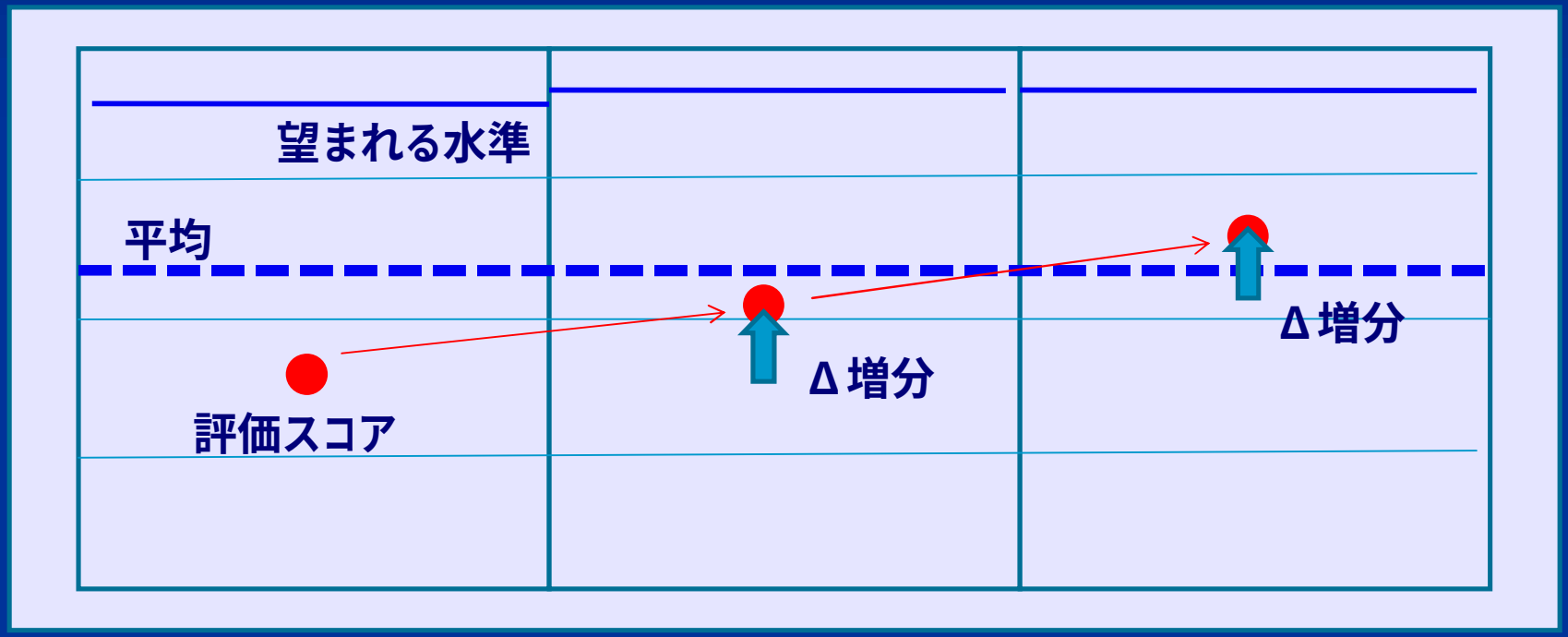
情報セキュリティ対策ベンチマークを委託先の選定に活用するためには、要求水準を定めた上で、調達仕様書等に情報セキュリティ対策ベンチマークを利用した自己評価結果を求める旨を明記する必要がある。具体的な記述例を以下に示す。

(1) 成熟度4 を求める場合

調達仕様書への記述例（1）：本調達に係る業務を行おうとする事業者は、[付録1] に従い情報セキュリティ対策ベンチマークを利用した自己評価を行い、その評価結果において、全項目に係る平均値（次項4.1.3(1)参照。）が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）に達していることを確認するとともに、[付録2] のとおり確認書を提出すること。

時系列で比較する

2005　第1回診断　　2006 第2回診断　　2007　第3回診断



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)

活用の事例－2

- グループ会社の状況把握に使う
  - グループ会社のセキュリティの現状把握
  - 診断データの分析と改善提案
- 取引先の指導に使う
  - 具体的な対策を促す
  - 取引条件に組み込む
- コンサルティングに使う
  - 経営者のセキュリティ研修の教材にする

100社を超えるグループ会社の状況の把握

- グループ子会社は100社を超え業種も様々
- 法令順守、内部統制の観点から、グループ企業総体としてセキュリティ対策を行う必要性
- 企業秘密の保全からも、グループ会社のセキュリティ対策状況の把握と改善は重要な課題
- 共通の基準に則った対策が必要
- 情報セキュリティ対策ベンチマークを採用
- 自己評価、相対評価、絶対評価

100社を超えるグループ会社の状況の把握

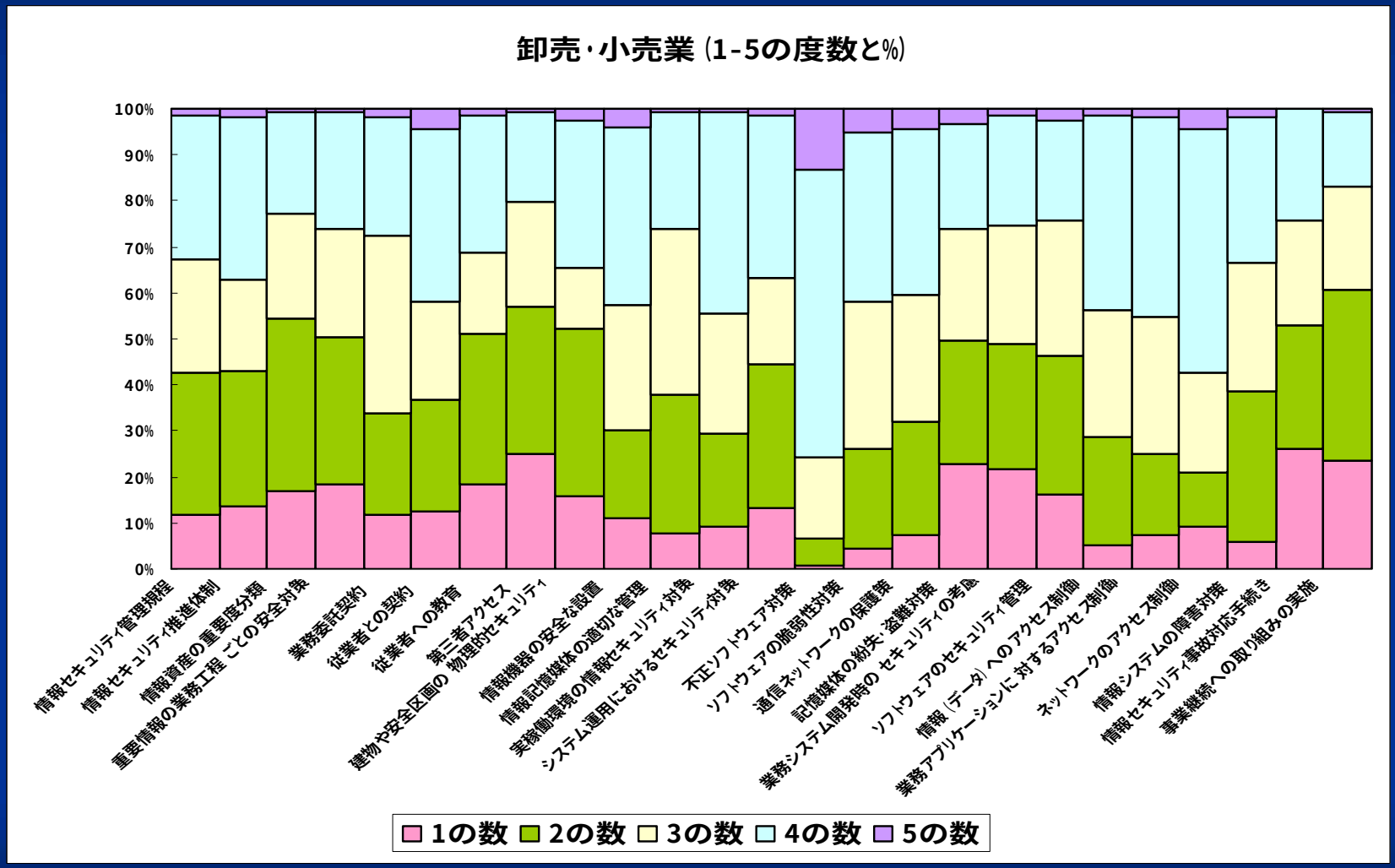
診断データ分析の内容

- 全国平均とグループ会社全体の平均の比較。
- 全国平均と比較して特に高い／低いセキュリティ対策項目の抽出。
- 企業規模別の比較
- 業種毎（事業部毎）の比較

診断データ分析結果の考察と改善提案

- 全国平均と比較して特に低い項目について、改善提案を作成
- 業種毎（事業部毎）に弱い部分の改善を提案。
- 診断データ分析内容により、遅れている対策項目を抽出し、改善を提案

100社を超えるグループ会社の状況の把握



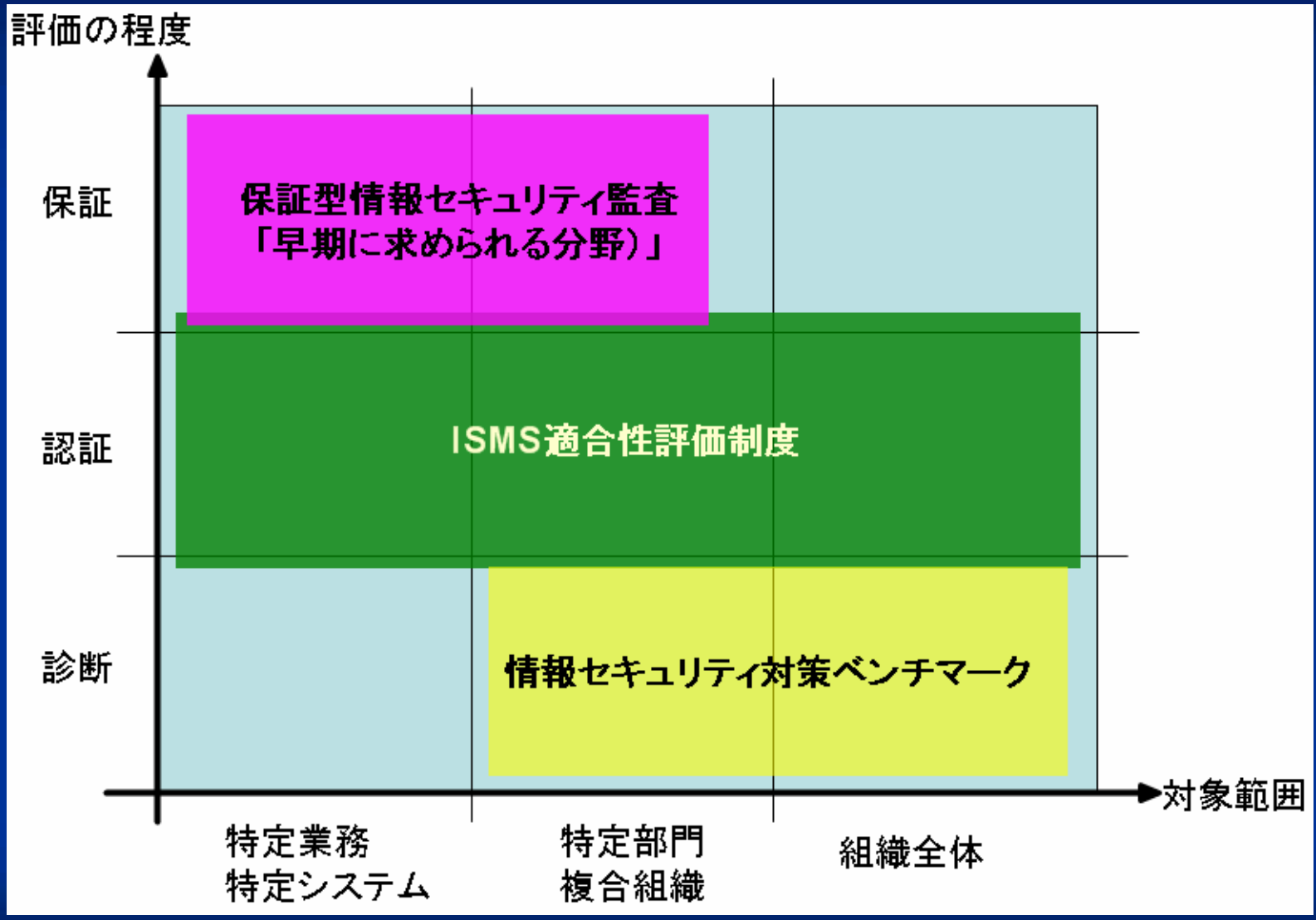
ベンチマークを役員教育に利用

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 2. 情報セキュリティ推進体制、コンプライアンス	重点教育項目	70 分
1	3. 情報資産の重要度分類 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	標準教育項目	45 分
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 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. 情報システムの脆弱性対策 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	概要教育項目	40 分
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 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	標準教育項目	25 分

目　次

1. 情報セキュリティガバナンスとベンチマーク
2. 具体的な活用事例
3. 関連諸制度との関係整理
4. 活用のヒント

三つの制度の比較


評価の程度
保証
認証
診断
保証型情報セキュリティ監査
「早期に求められる分野」
ISMS適合性評価制度
情報セキュリティ対策ベンチマーク
対象範囲
特定業務
特定システム
特定部門
複合組織
組織全体

目　次

1. 情報セキュリティガバナンスとベンチマーク
2. 具体的な活用事例
3. 関連諸制度との関係整理
4. 活用のヒント

活用のヒント

- ベンチマークは比較に意味がある
  - 平均との比較
  - 望まれる水準との比較
  - 部門間比較、グループ会社比較
- 平均や望まれる水準も変化する
- 時系列での改善の把握
  - 定期的評価
  - Δ増分の根拠の明確化
- 利害関係者への説明資料

ありがとうございました

Eijiroh Ohki

eohki@cc.kogakuin.ac.jp