IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

情報セキュリティ対策ベンチマークの活用と情報セキュリティ評価について

2008年2月12日

独立行政法人　情報処理推進機構
セキュリティセンター　菅野 泰子

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

本日の内容

1. 情報セキュリティ対策ベンチマーク
   背景と概要
2. セキュリティ評価の目的と活用
3. 情報セキュリティ対策ベンチマーク
   活用集と活用例

■情報セキュリティガバナンスの確立に向けて

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
http://www.meti.go.jp/policy/netsecurity/sec_gov_report.html

- **問題**
  - **IT事故発生のリスクが不明確、適正な情報セキュリティ投資の判断が困難**
  - **既存の情報セキュリティへの「対策」「取組」が、企業価値に直結していない**
  - **事業継続性確保の必要性が十分に認識されていない**

↑

- **「情報セキュリティガバナンス」を確立するツール**
  - **①情報セキュリティ対策ベンチマーク**

    情報セキュリティガバナンス推進のための
    組織の情報セキュリティ対策状況の自己診断用ツール
  - **②情報セキュリティ報告書モデル**
  - **③事業継続計画策定ガイドライン**

情報セキュリティガバナンスと自己診断テストの活用

情報セキュリティ対策ベンチマーク（自己診断テスト）

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

- Web上で自社の現状を入力すると、自動的に結果を表示
- トータルスコアと自社のレベルが示され、望ましい水準とのギャップや、どのような対策が不足かをチェックできる

「どこまで行えばよいか基準が示されていない」「コストがかかりすぎる」という問題へのひとつの答え

ベンチマーキング

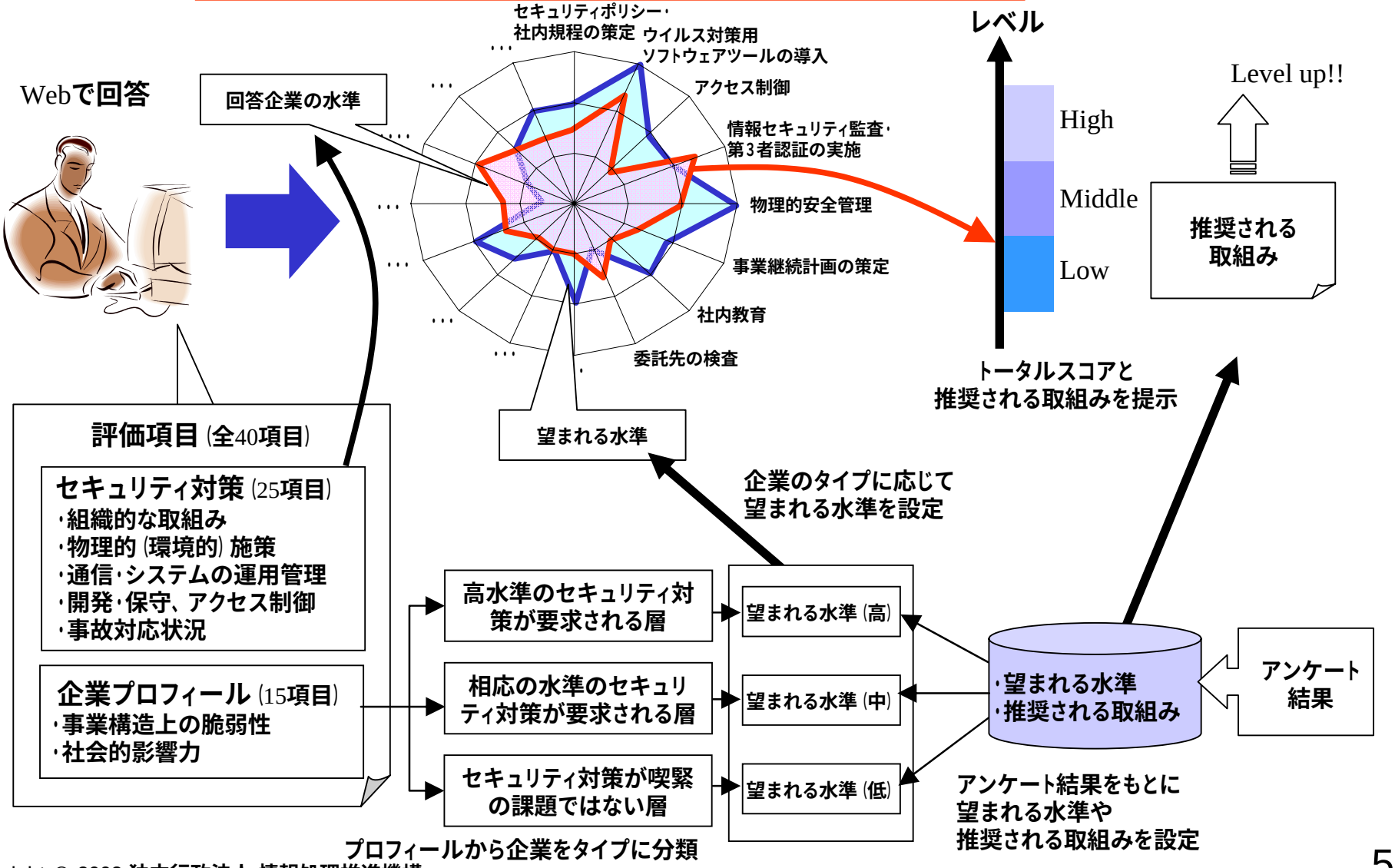
ある指標（ベストプラクティス）を探し出し、それと比べて自社のレベルを評価し、足りない部分を改善していく経営改善の手法

この**自己評価と業務改善の手法**を情報セキュリティ対策に応用

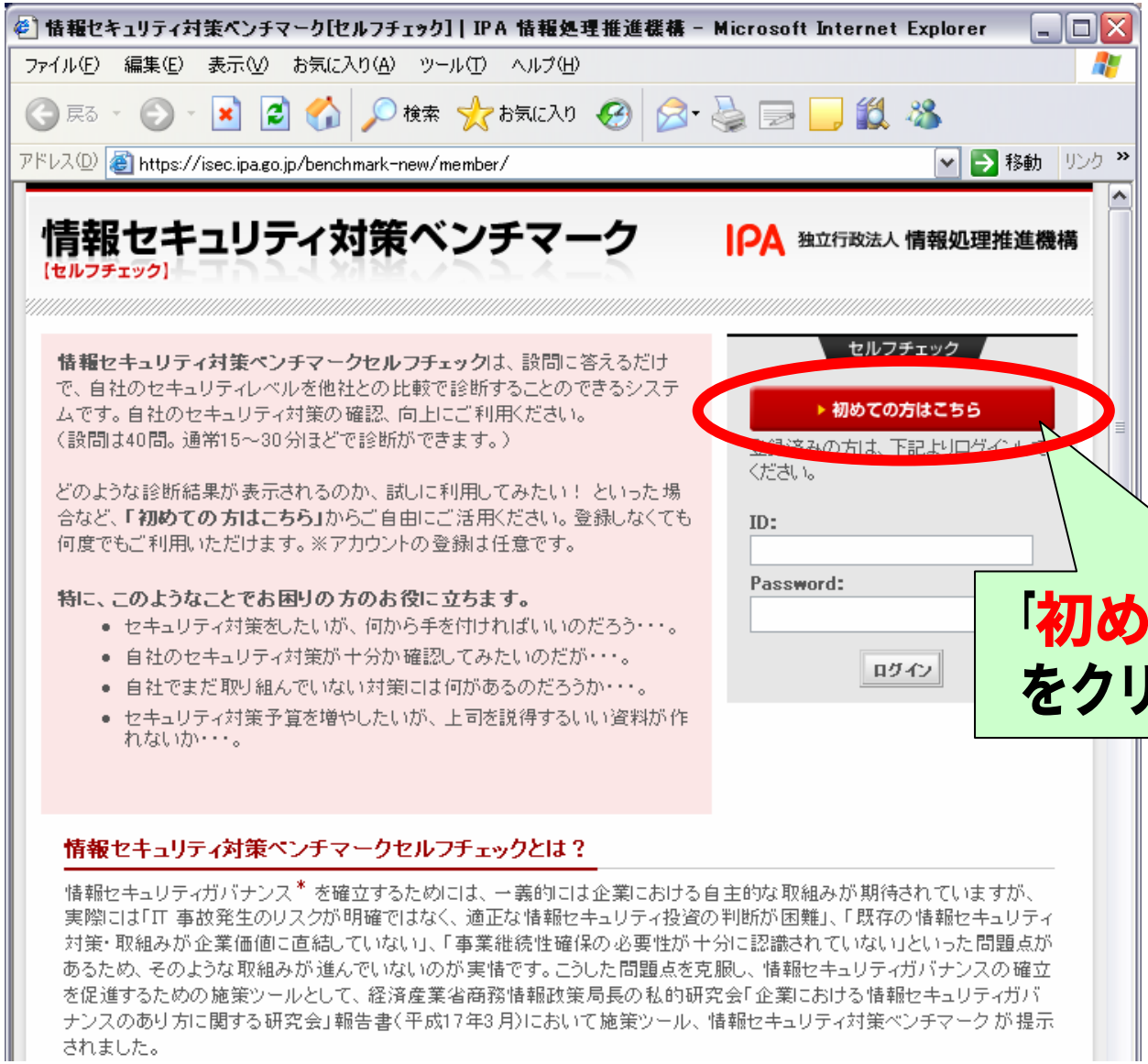
情報セキュリティガバナンス推進には経営陣の積極的関与が不可欠

■情報セキュリティ対策ベンチマークの概要

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



情報セキュリティ対策ベンチマークの利用方法



「**初めての方はこちら**」
をクリックしてスタート

■ セキュリティ対策に関する質問

第1部の設問（評価項目）

5 グループ構成、グループ毎 3～7 項目　計 25 項目

(a) 情報セキュリティに対する組織的な取組状況　（7項目）
(b) 物理的（環境的）セキュリティ上の施策　（4項目）
(c) 情報システム及び通信ネットワークの運用管理　（6項目）
(d) 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項目）
(e) 情報セキュリティ上の事故対応状況　（3項目）

JIS Q 27001(ISMS認証基準) の
付属書Aの管理策（133項目）がベース
- 専門家によるWGの検討を経て策定。
- 平易な言葉でわかりやすく表現。
- 評価項目の量を抑えている。

■ セキュリティ対策に関する質問の回答（選択肢）

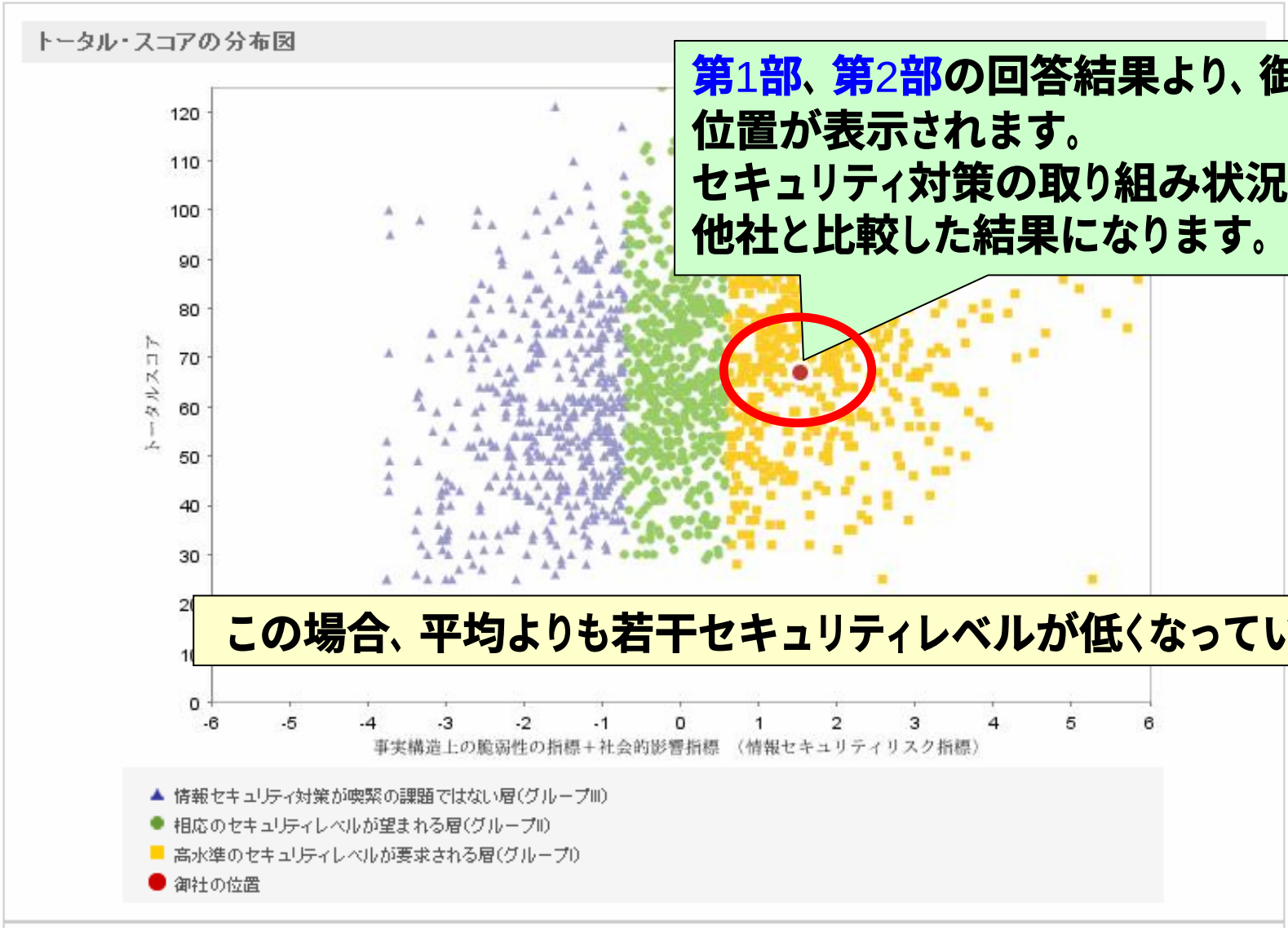
第1部の質問へは5つの選択肢より回答

できていない

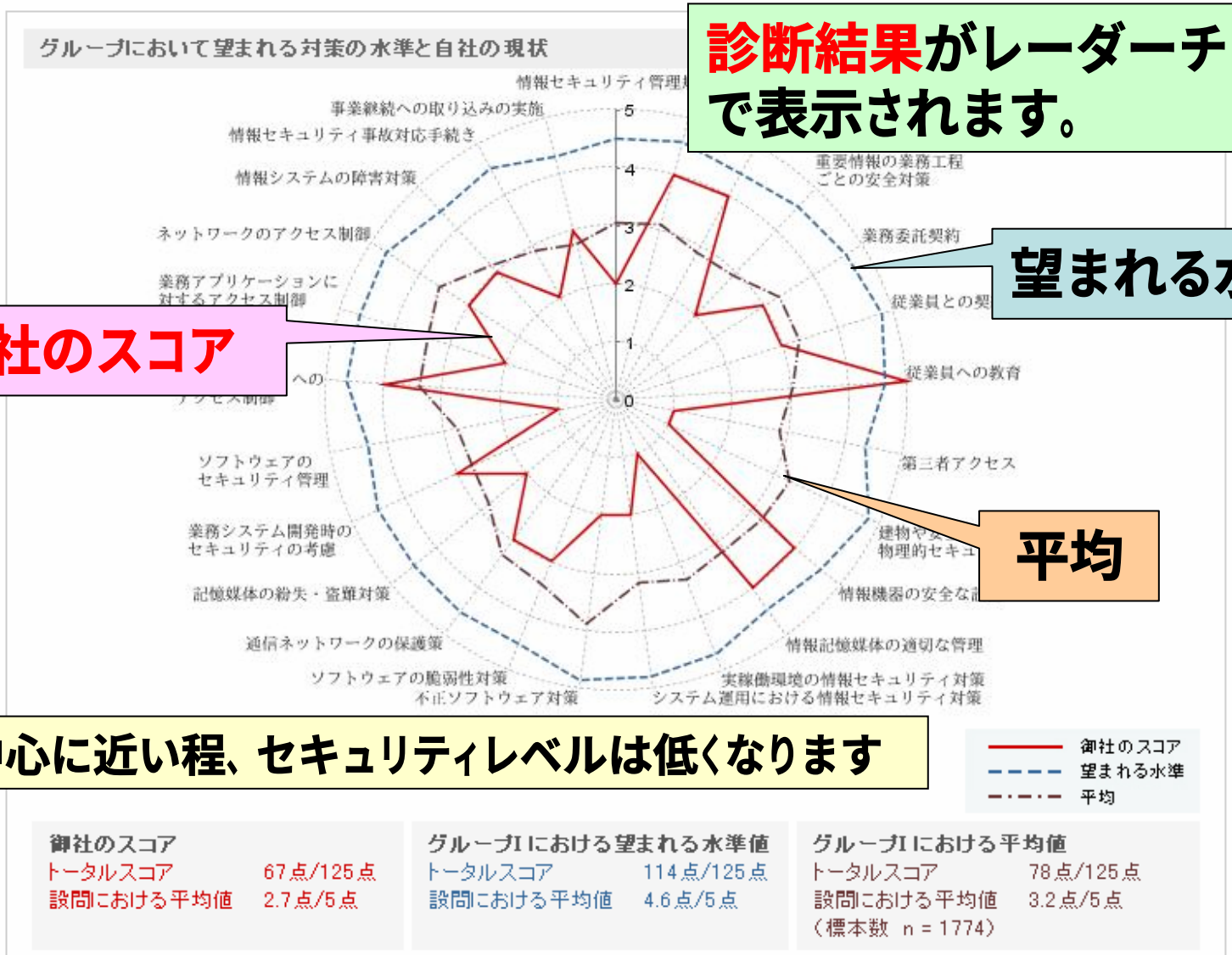
1	経営層にそのような意識がないか、意識はあっても方針やルールを定めていない
2	経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3	経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4	経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5	4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

できている

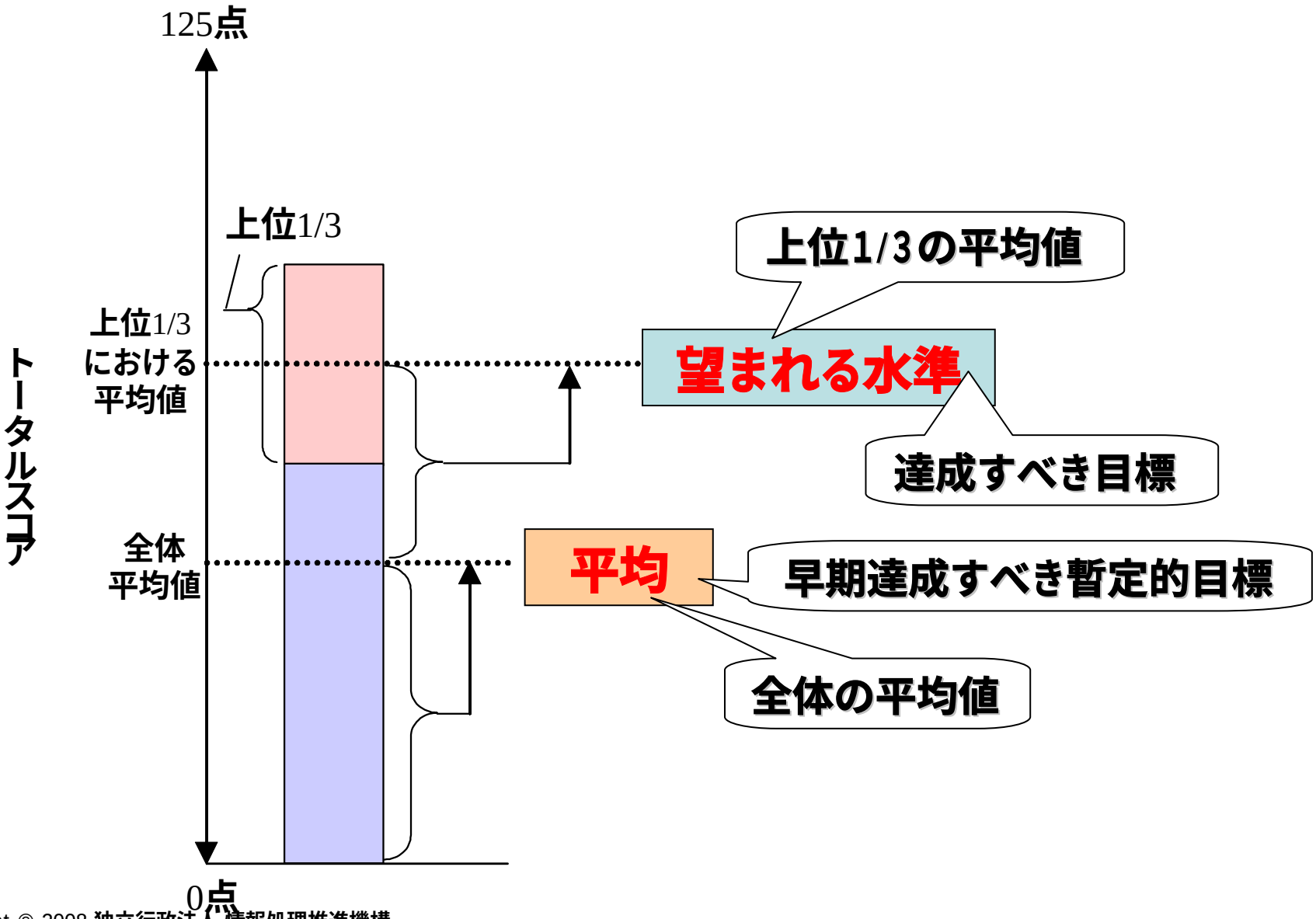
■情報セキュリティ対策ベンチマークの診断結果



■ 診断結果（レーダーチャート）



■ 望まれる水準とは

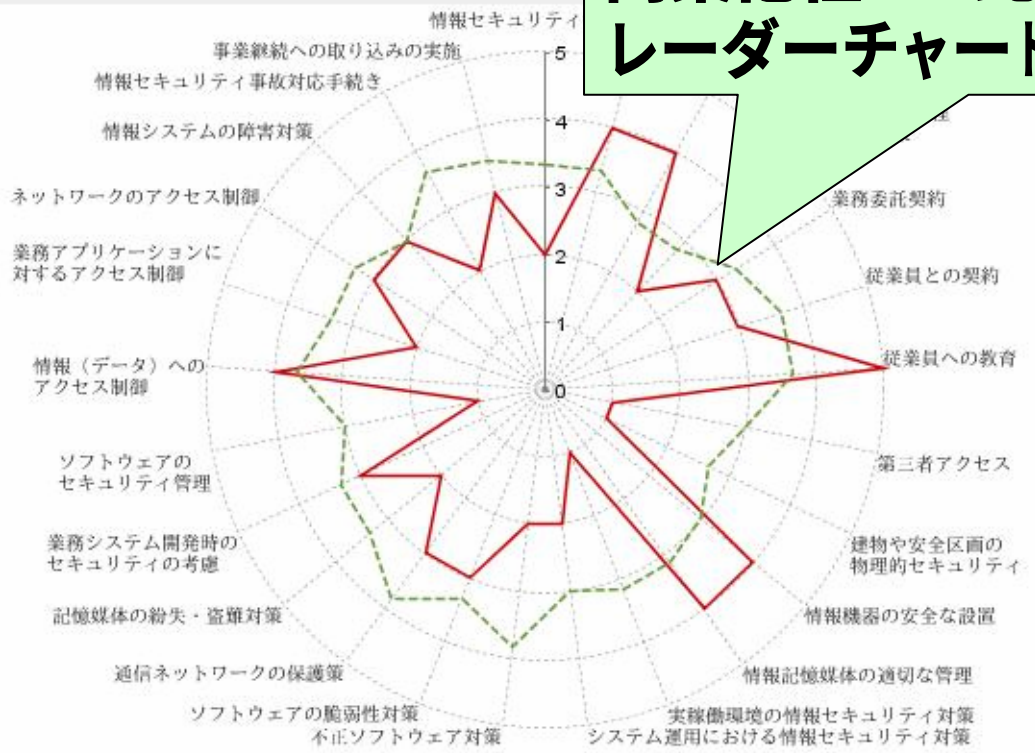


■診断結果（同業他社との比較）

また、同じ業種の平均と比べると次のようになります。

同業他社との比較結果も
レーダーチャートで表示されます。

同業種の平均と自社の現状



御社のスコア		同業種の平均	
トータルスコア	67点/125点	トータルスコア	82点/125点
設問における平均値	2.7点/5点	設問における平均値	3.3点/5点

■推奨される取り組み例

推奨される取り組み事例

第1部の設問に対し、選択肢の1もしくは2が選
すので、今後の対策や改善への取り組みの参

セキュリティ対策が弱い項目について、推奨される取り組み事例（必要な対策情報）を参照できます。

1: 情報セキュリティに対する組織的な取組状況について

（1） 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。）

説明:
ポリシーや規程が有効なものであるためには、それらが自社の状況に見合ったものである必要があります。ポリシーや規程は、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。
詳細はこちらを参照ください。

（4） 個人データ等の重要な情報については、取得、利用、保管、開示、消去等の一連の業務工程毎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

説明:
個人情報保護法の規定やガイドライン
責任者や手順の明確化、取扱者の限定や処理の記録、確認などが必要です。
詳細はこちらを参照ください。

この情報を参考にして、ワンランク上のセキュリティ対策を実施していきましょう。

デモ 1 **デモ 2**

情報セキュリティ対策ベンチマークポータルサイト
http://www.ipa.go.jp/security/benchmark/

自己診断サイトへは
Enterをクリック

ベンチマークポータルサイトに掲載の資料

- 情報セキュリティ対策ベンチマークの概要
- 情報セキュリティ対策ベンチマークver.3.0 の特徴
- 情報セキュリティ対策ベンチマークの使い方
- 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の質問一覧
- 推奨される取り組みのページ
- 情報セキュリティ対策ベンチマークに関するFAQ
- 情報セキュリティ対策ベンチマークに関する資料など

ポータルサイトには、
様々な情報が
掲載されています。

質問一覧や対策のポイント一覧

http://www.ipa.go.jp/security/benchmark/benchmark-question.html

診断の際には、「情報セキュリティ対策に関する25問」と「企業プロフィールに関する15問」にご回答いただきます。事前に質問内容をチェックしたい場合には、このサイトより、質問一覧をダウンロードすることができます。

情報セキュリティ対策ベンチマークの質問一覧

独立行政法人 情報処理推進機構
セキュリティセンター
isec-info@ipa.go.jp

情報セキュリティ対策ベンチマークの質問一覧

BM Ver.3 Questions.doc（220KB、Doc ファイル）

このファイルには、ベンチマークの診断で質問される「情報セキュリティ対策に関する 25 問」と、「企業プロフィールに関する 15 問」の設問の内容と、回答欄があります。このファイルをダウンロードして、質問項目を確認し、事前に回答してみることで、自己診断の準備ができます。

質問と対策のポイント一覧表

25questions_points Ver.3.0.pdf（72KB、PDF ファイル）

ベンチマーク ver.3.0 より、診断中に、推奨される取組がポップアップ画面により確認できるようになりました。このファイルには、「情報セキュリティ対策に関する 25 問」の一覧と、それぞれの質問に対する対策のポイントが記載されています。このファイルをダウンロードすると、診断中のポップアップ画面の「対策のポイント」が事前にご確認いただけます。

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

活用方法について知りたい場合は、活用集を参照下さい。

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。
- ニーズにあった活用例を見出せるよう、実例を参照した、さまざまな活用例を挙げています。
- 情報セキュリティ対策ベンチマークと ISMS 認証取得や情報セキュリティ監査の関係を具体的に示し、これら評価の準備段階で活用するための具体的な手引きとなります。
- 付録では、情報セキュリティ対策ベンチマーク、ISMS 認証、情報セキュリティ監査それぞれの評価について、その概要を説明しています。

本活用集の構成

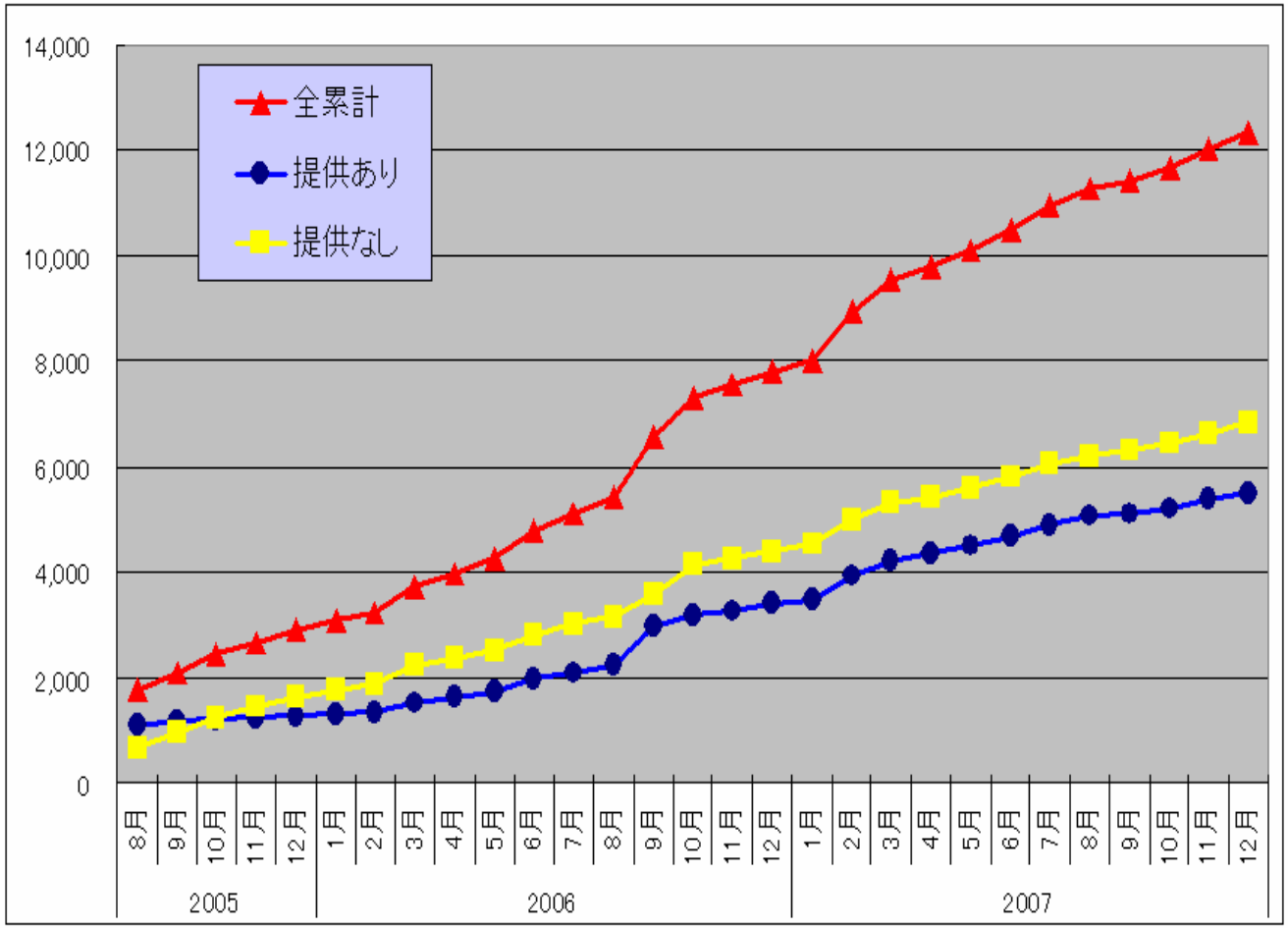
- 第1章　情報セキュリティ評価について
- 第2章　情報セキュリティ対策ベンチマーク活用例
- 第3章　情報セキュリティ対策ベンチマークからISMS 認証取得へ
- 第4章　情報セキュリティ対策ベンチマークから情報セキュリティ監査へ
- 付 録　情報セキュリティ対策ベンチマーク、ISMS 認証、情報セキュリティ監査　それぞれの評価について、その概要を説明

◇ 情報セキュリティ対策ベンチマーク活用集　目次はこちら (63KB、PDF ファイル)

◇ 本活用集(全128ページ)のダウンロード (3.17MB、PDF ファイル)

◇ プレスリリースの全文は、以下のPDF をご覧ください。
プレスリリース全文 (38KB、PDF ファイル)

■ 情報セキュリティ対策ベンチマークの利用状況



ベンチマーク利用件数は12,000件を超える

2007年12月31日現在

***注** 5,498件の提供データの内の885件は、ベンチマークシステムの基礎データに使用する為、協力していただきました企業のデータになります。

回答データ提供有り	回答データ提供無し	合計
5,498*注件	6,828件	12,326件

本日の内容

1. 情報セキュリティ対策ベンチマーク
   背景と概要
2. セキュリティ評価の目的と活用
3. 情報セキュリティ対策ベンチマーク
   活用集と活用例

■セキュリティ評価の目的

- 自社の情報セキュリティ対策の有効性や実施状況を確認
  - 自社のセキュリティレベル維持改善のため
  - 意図した通りに実行されているか
  - 対策の効果は上がっているか
  - 不足なところ、実情にあわないところは無いか
- 自社のセキュリティ対策状況の外部への説明資料に活用
  - 取引先への説明
  - 製品やサービスの購入者への説明
  - 情報セキュリティ報告書へ記載（説明責任を果たす）
- 外部委託先や子会社のセキュリティ対策状況の確認
  - 製品やサービスを購入する際に評価結果提出を求める
  - 子会社のセキュリティ対策状況を確認する
- 製品等の購入の際にセキュリティ実装状況について確認

■様々なセキュリティ評価

●組織のセキュリティ対策状況の評価

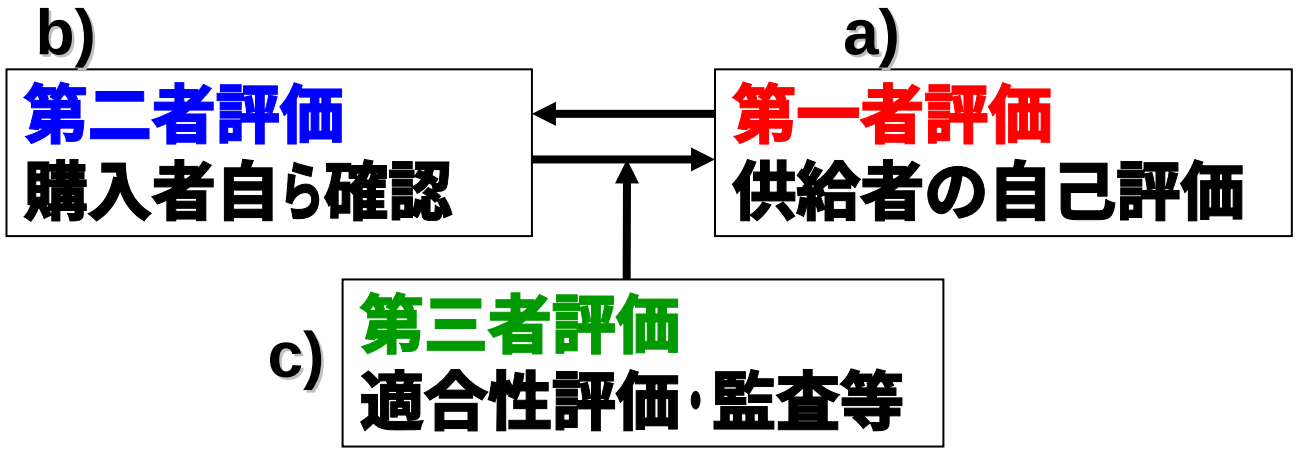
1) ISMS適合性評価制度
2) 情報セキュリティ監査
3) 情報セキュリティ対策ベンチマーク
4) 自己点検

●製品等のセキュリティ実装状況の評価

1) ITセキュリティ評価及び認証制度
2)暗号モジュール試験及び認証制度（JCMVP）

■誰が誰を評価する？(製品やサービスの購入時)

製品やサービスなどを購入したり、選択しようとする時、購入者や選択者が、その製品やサービスなどが、規格や基準を満たしているかどうかを確認するための評価は、評価者という観点からみると3種類ある。



a) 第一者評価：　製品やサービス提供者の規格、基準を満たしているとの主張を信じる
b) 第二者評価：　購入者や選択者が自ら確認する
c) 第三者評価：　中立の第三者に依頼し、その製品などが規格・基準などを満たしているかどうか確認してもらう。

■組織のセキュリティ対策状況の評価

第三者評価：被評価者と独立の立場の専門家による客観的評価
手間、時間、費用がかかる
実施時期を決めて、計画的に行う

自己評価　：情報システム部門の責任者や担当者が、導入した
個々の管理策の効果や効率を自己評価する
第三者評価に比べ手間、時間、費用が少なくて済む

第三者評価

ISMS適合性評価制度
情報セキュリティ監査
ITセキュリティ評価・認証制度　など

自己評価
(セルフアセスメント)

情報セキュリティ対策ベンチマーク
(IPAの情報セキュリティ対策自己診断ツール)
チェックリストによる自己点検　など

(参考) 政府機関統一基準適用個別マニュアルより

【参考URL】 **政府機関統一基準適用個別マニュアル群**
http://www.nisc.go.jp/active/general/kijun_man.html
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
(DM6-06-071)

外部委託において利用できる評価手法：主に以下の3 つの制度
- **情報セキュリティマネジメントシステムに関する適合性評価制度**
- **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**

委託先の選定：委託先候補が情報セキュリティマネジメントシステムに関する適合性評価制度　に基づく認証を取得していること、又は情報セキュリティ対策ベンチマークの結果が求める成熟度に達していることを、選定における評価の要素に含めることができる。また、将来的には、情報セキュリティ監査の結果を選定における評価の要素に含めることも想定される。
履行状況の確認：業務における定常的な確認に加えて、委託先における当該情報処理業務を対象にした情報セキュリティ監査が活用できる。

これらの制度は特徴に応じて適切な場面で有効に活用することが重要
「**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** 3.各種制度と利用場面」より

■3つの評価方法の比較

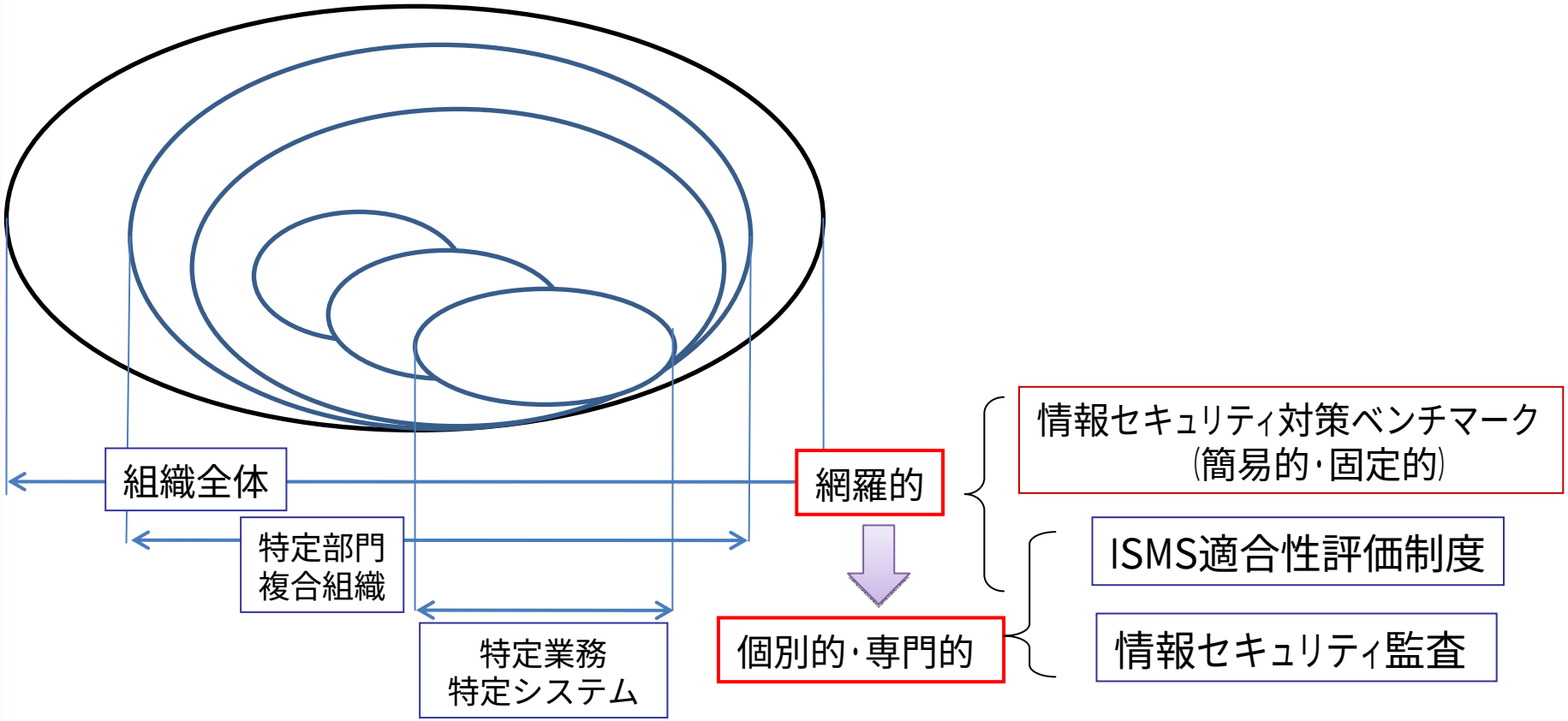
■ベースとなる規格は、情報セキュリティマネジメントの規格：JIS Q 27001やJIS Q 27002

■評価方法や評価項目の量、評価の詳細さは大きく違う

	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	ISMS適合性評価
利用目的	情報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の整備・運用状況の評価	情報セキュリティマネジメントシステムの認証
対象範囲	組織体	組織体、特定業務・サービスなど	組織体、特定業務・サービスなど
目指すべきセキュリティ水準	経営者が目指す水準	顧客が期待する水準（保証型） 経営者が目指す水準（助言型）	経営者が目指す水準
評価者	経営者、管理者 (自己評価)	監査人 (第三者評価)	審査員 (第三者評価)
評価法	相対的評価、定量的評価	監査	審査
評価に用いる基準	JISQ27001をベースに作成した25問 (網羅的・簡易的・固定的)	JISQ27001, 27002等を参照し作成された個別管理基準 (監査毎に個別)	JISQ27001 (網羅的)
評価結果	散布図, レーダーチャート, スコア, 助言	助言意見、保証意見	ISMS認証登録証
費用	無料	有料	有料

出典：情報セキュリティ対策ベンチマーク活用集を基に作成

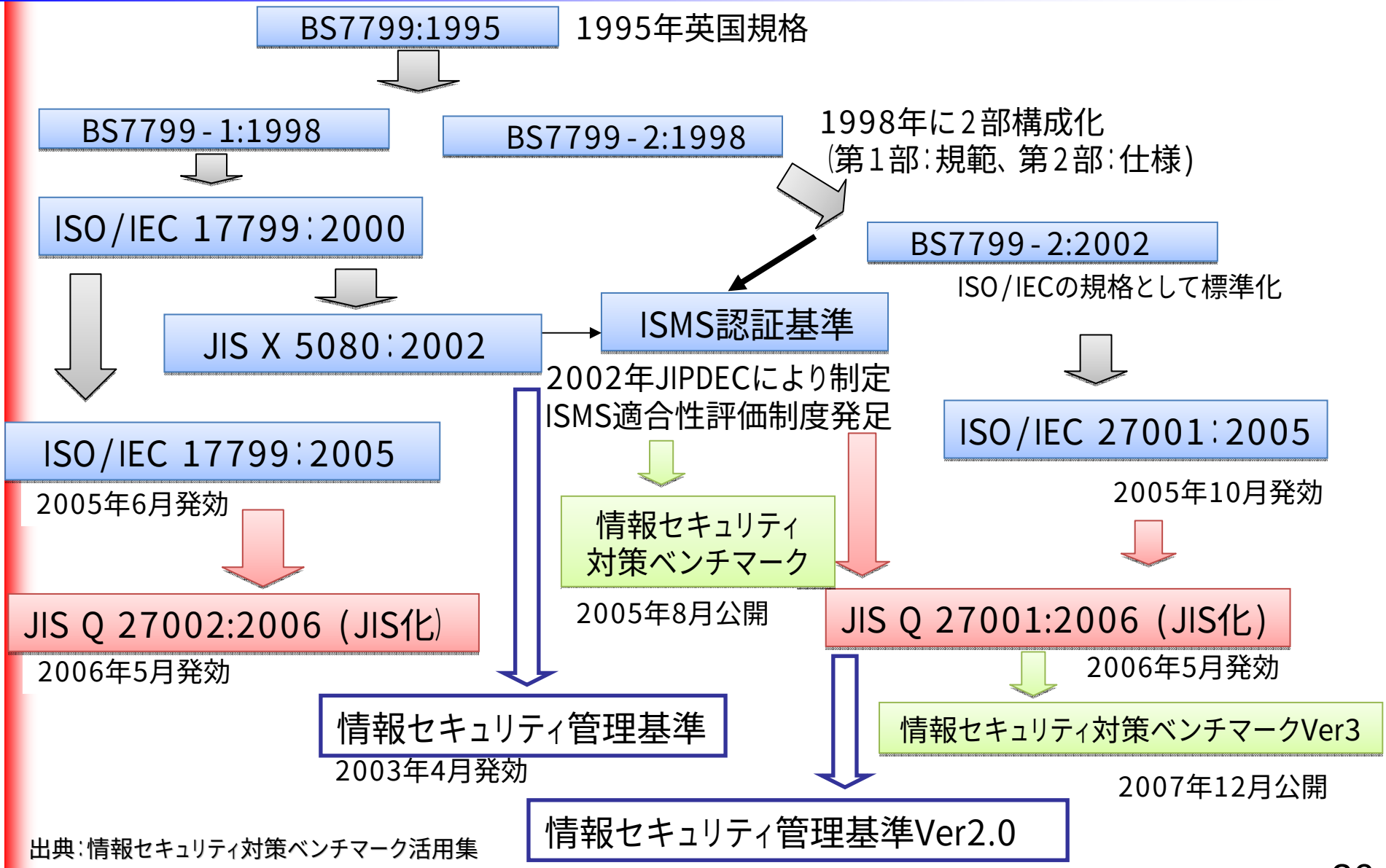
■各評価方法の評価の対象範囲と評価の程度



□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
□より詳細に多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できる。

出典：情報セキュリティ対策ベンチマーク活用集

■情報セキュリティマネジメントの規格



出典:情報セキュリティ対策ベンチマーク活用集

■JIS Q 27001管理策とベンチマークの質問

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 / 50
2. 情報セキュリティのための組織	11			
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 / 25
8. 情報システムの取得開発及び保守	16			
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 / 16
10. 事業継続管理	5			
11 領域	133	大項目 5	**質問数**	**25**
			対策のポイント数	146

出典：情報セキュリティ対策ベンチマーク活用集

■ ISMS適合性評価制度

●ISMSが構築運用されていることを、審査登録機関が評価
→適合していると認められた場合、認証を付与し登録する制度

●準拠する基準: JIS Q 27001:2006 (ISO/IEC 27001:2005)

・4　情報セキュリティマネジメントシステム
・5　経営陣の責任
・6　ISMS内部監査
・7　ISMSのマネジメントレビュー
・8　ISMSの改善

必須の要求事項(文書化)

付属書A　管理目的及び管理策

個々の管理策は合理的理由があれば適用除外可能

● JIPDEC（(財)日本情報処理開発協会　http://www.isms.jipdec.jp/）
JAB（(財)日本適合性認定協会http://www.jab.or.jp/）

により運用

適合性評価(Conformity Assessment)：　製品、プロセス、人、組織などが、要求される規格、基準を満たしているかどうかを評価

■ ISMSの要求事項

ISMSの確立	ISMSの導入運用	ISMSの監視見直し	ISMSの維持改善
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	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	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	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
P	D	C	A

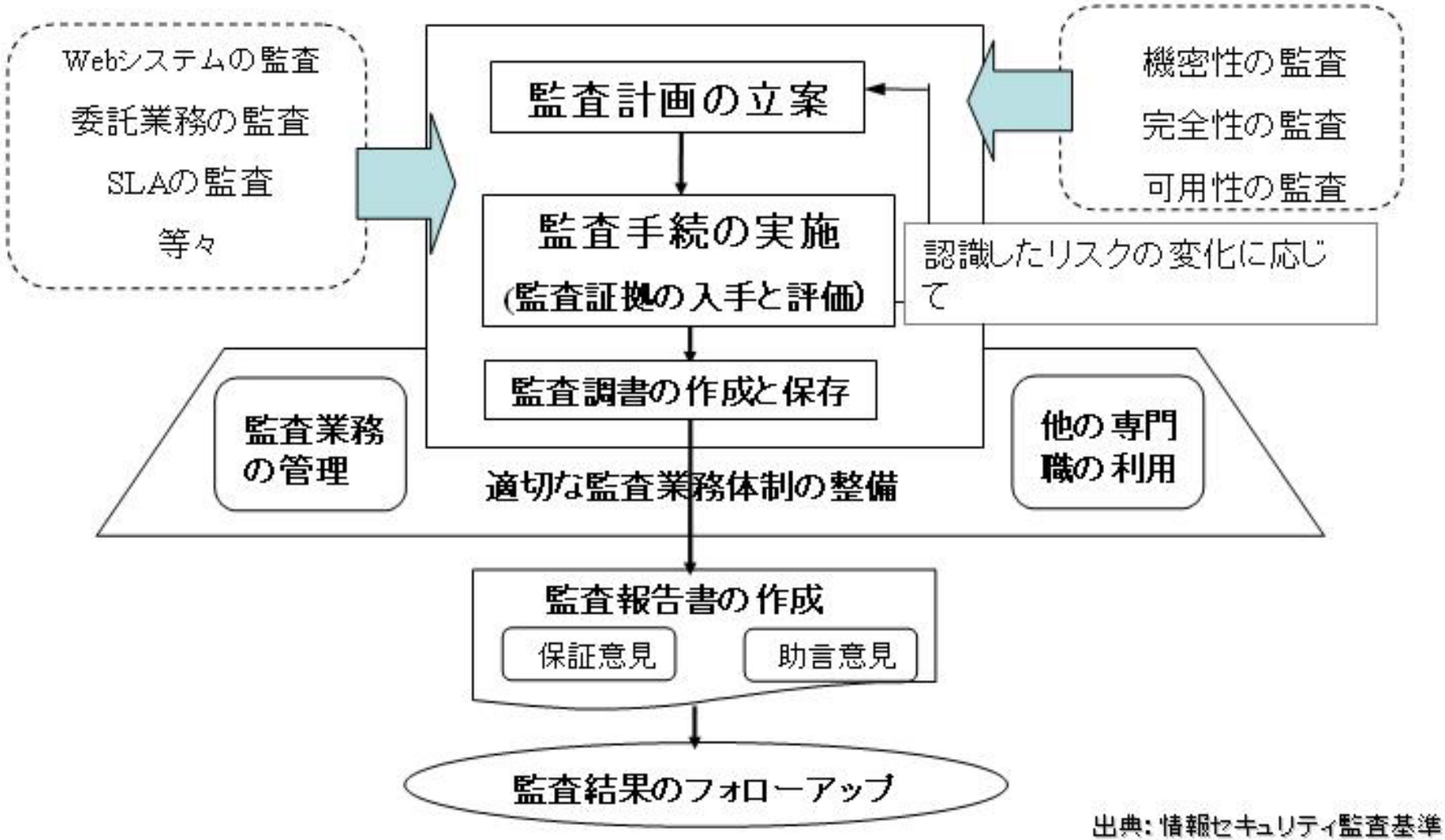
出典：IPAフォーラム2007　大木栄二郎先生のプレゼン資料より

■情報セキュリティ監査

- **情報セキュリティ対策の有効性・実施状況を評価**
  情報セキュリティ対策が適切に実施され、期待通りに機能しているか、
  情報セキュリティに係るリスクマネジメントが適切に行われているかを評価
- **準拠する基準**
  - 情報セキュリティ監査基準・・・監査人の行動規範
  - 情報セキュリティ管理基準・・・監査上の判断基準
- **助言型監査と保証型監査**
  - 助言型監査・・・不備な点を示し是正措置を助言
  - 保証型監査・・・基準に従い評価した結果不備は無いと保証
- **独立の監査人によって行われる第三者評価**
  - 外部監査・・・専門の監査会社
  - 内部監査・・・組織内部の監査部門
    被監査部門との独立性
- **監査時期：1年に1回などの割合で定期的に行う**
  - 監査の実施は、Check(点検・監査・見直し)にあたり
  - 助言に従って改善を行うのはAct(処置)にあたる

経済産業省主導のもと、2003年3月に運用開始

■情報セキュリティ監査実施のフレームワーク



出典: 情報セキュリティ監査基準

■保証型情報セキュリティ監査の3方式

1次利用者

被監査主体のリスクマネジメントに当事者として関与し、利用者が許容できるリスクレベルを被監査主体が達成できているかに強い関心を抱いている

2次利用者

被監査主体のリスクマネジメントの当事者としては関与せず、被監査主体の主体的なセキュリティ管理の出来栄えに関心がある場合

被監査主体の主体的なセキュリティマネジメントに依存する場合	利用者の要求したセキュリティ管理策の実装を確認したい場合	
利用者合意方式	**被監査主体合意方式**	**社会的合意方式**
「‥‥情報セキュリティ対策の設計と実装は、業務**委託元の期待する水準にあるもの**と認める。‥‥」	「‥‥情報セキュリティ監査手続きを実施した結果は別紙のとおりである。‥‥‥‥‥‥‥‥」 (監査人の意見表明はない)	「‥‥‥‥適切に実装し運用している旨の言明は**信じるに足る**ものと認める。‥‥‥‥‥‥」

出典：情報セキュリティ対策ベンチマーク活用集（情報セキュリティ監査より）

■ ISMS適合性評価制度と情報セキュリティ監査

- **ISMS適合性評価制度**
  - JIS Q 27001:2006の要求事項への適合を評価
  - ISMS認証取得により、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
  - 認証を受ける側の状況に応じて基準を作り変えることはない
  - 適用範囲は、認証依頼者により選択可能
- **情報セキュリティ監査**
  - 監査報告書利用者の目的に応じて、多様な監査が選択できる
    (助言型監査、保証型監査、網羅的監査、一部の監査、技術的より詳細な高水準の監査、またその組み合わせ等が可能)
  - 評価 (監査) の基準は、JIS Q 27002ベースの詳細管理策を網羅した情報セキュリティ管理基準等を参照し、監査目的に対応して作成された個別管理基準
  - 委託先に預託する機微な自社情報のセキュリティ対策状況を評価するには、保証型監査が適している

違いを踏まえた上で、自組織のニーズに合った評価を選択

本日の内容

1. 情報セキュリティ対策ベンチマーク
   背景と概要
2. セキュリティ評価の目的と活用
3. 情報セキュリティ対策ベンチマーク
   活用集と活用例

■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

【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 (IPA)
	財団法人 日本情報処理開発協会 (JIPDEC)
	特定非営利活動法人 日本セキュリティ監査協会 (JASA)
【オブザーバ】	財団法人日本適合性認定協会 (JAB)

● 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可能
- 実例を参照した、さまざまな活用例を記載
- 情報セキュリティ対策ベンチマークと ISMS 認証取得や情報セキュリティ監査の関係を具体的に示し、これら評価の準備段階で活用する具体的な手引きに

本活用集 (全128ページ) のダウンロード

http://www.ipa.go.jp/security/benchmark/benchmark-katsuyou.html

■情報セキュリティ対策ベンチマーク活用集

● 目次

- 第1章　情報セキュリティ評価について
- 第2章　情報セキュリティ対策ベンチマーク活用例
- 第3章　情報セキュリティ対策ベンチマークからISMS 認証取得へ
- 第4章　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
- 付 録　情報セキュリティ対策ベンチマーク、ISMS 認証、情報セキュリティ監査　それぞれの評価について、その概要を説明

情報セキュリティ対策ベンチマークから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特徴と活用例

特　徴

- 時間･費用がかからず、専門的な知識がなくても自己診断できる
- 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
- 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
- 情報セキュリティ対策を始める良いきっかけになる
- 散布図やレーダチャートなどで自社の位置を知ることができる
- 他社との比較により、経営層の危機意識が高まり、対策が加速する。

活　用　例

- 他社と比べた自社の位置の確認
- 全社の情報セキュリティ対策の実施状況の把握や部門ごとの比較
- グループ会社、外部委託先などの対策状況の把握や評価、指導
- 委託元や取引先の要求を満たすために診断結果を提示
- 経営者や管理者の情報セキュリティ研修の教材としての活用
- ISMS適合性評価制度や情報セキュリティ監査の準備段階での利用

■自社の情報セキュリティ対策状況の把握

情報漏えい事故を起こしてしまった企業が、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。

A社は社員数50名の中小企業。2003年夏に蔓延した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。

■情報セキュリティ教育への応用

A社では、情報漏えい事故への反省から、情報セキュリティ教育への関心が高まっている。経営陣自ら教育を受講する。

A社(社員数 50 名)
経営者、役員
B氏:総務部員。
他の業務と兼務で
情報システムを担当

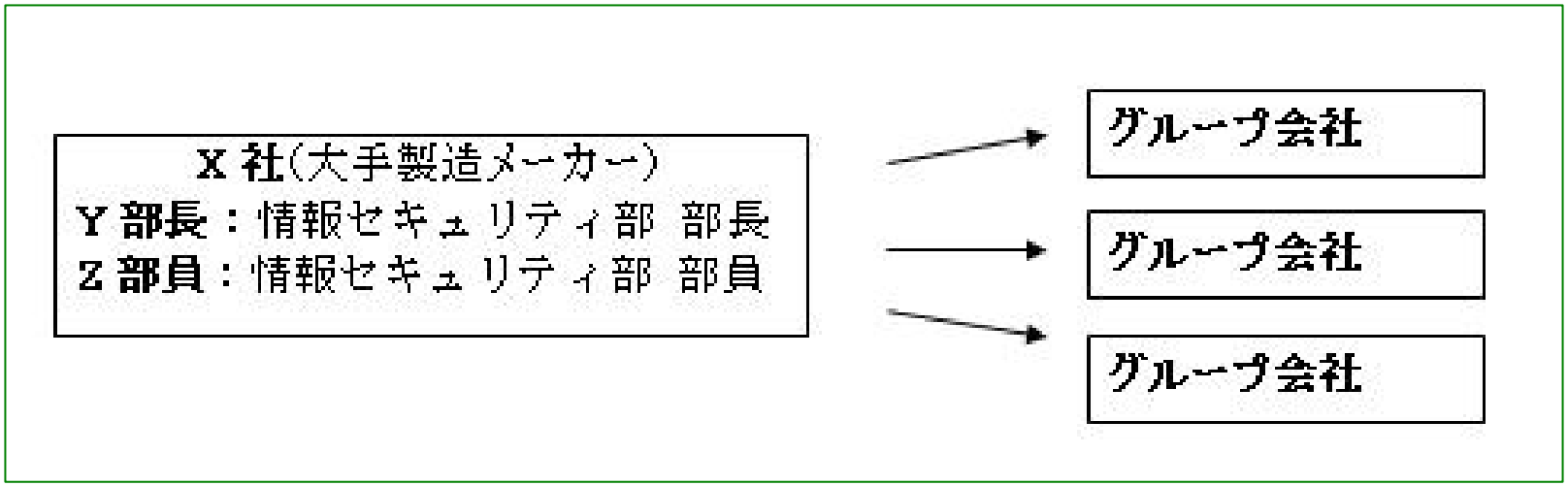
⇔

E社(A社情報システム運用管理委託先)
F氏:
情報セキュリティサービス本部所属
A社へのコンサルティング担当

教育を担当したのは、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、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教育資料を作成しようと考えた。

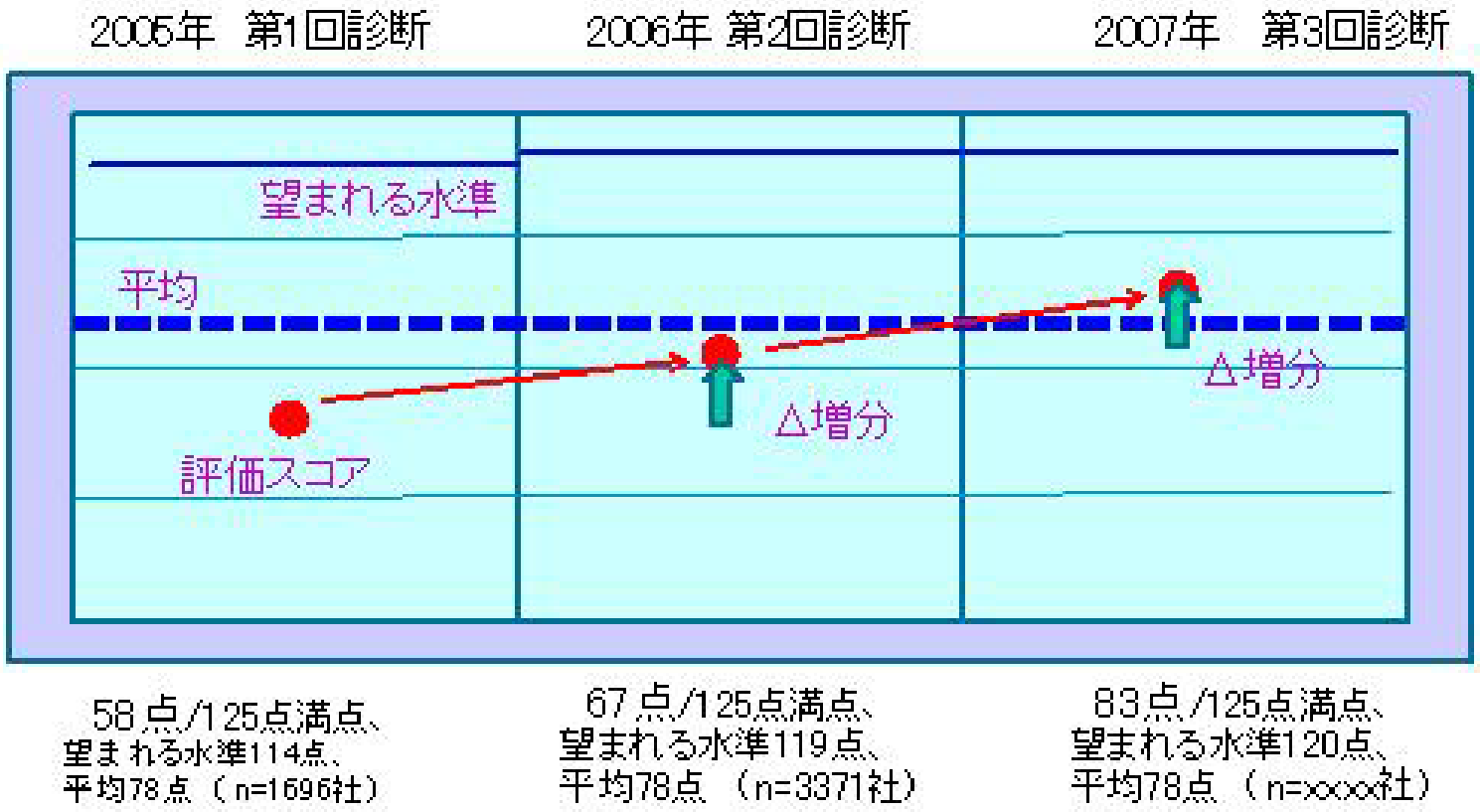
■共通の尺度によるグループ内統制

X社では傘下にかかえるグループ子会社が100社を超える。
これらの会社の情報セキュリティ対策状況の把握は重要な課題



大手製造メーカーX社では、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、会社の重要な技術情報を提供することもある。法令順守や企業秘密の保全という観点から、グループ会社のセキュリティ対策状況の把握や、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？

■ISMS認証取得の準備段階での活用例



- **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。**
- **セキュリティ事故を契機に社内の情報セキュリティ対策を見直すことに。**
- **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。**

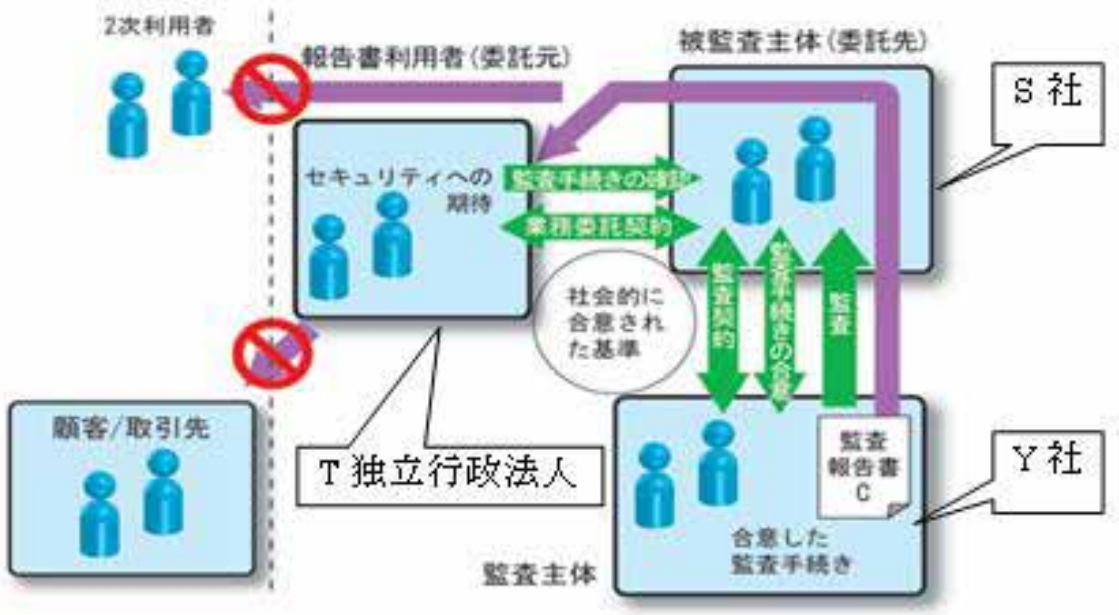
■情報セキュリティ監査への活用例

■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。

■ 政府機関統一基準に基づく民間企業における保証型情報セキュリティ

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。



被監査主体合意方式の保証型監査

■ (参考) 情報セキュリティ教本 (2007年4月刊行)

【目次】

独立行政法人　情報処理推進機構
セキュリティセンター（IPA/ISEC）

〒113-6591
東京都文京区本駒込２－２８－８
　文京グリーンコートセンターオフィス１６階
ＴＥＬ　０３（５９７８）７５０８　　ＦＡＸ　０３（５９７８）７５１８
電子メール　isec-info@ipa.go.jp
ＵＲＬ　http://www.ipa.go.jp/security/