IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

セキュリティ評価と
情報セキュリティ対策ベンチマーク

2007年3月5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/

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

本日の内容

1. IPAセキュリティセンターの紹介
2. セキュリティ評価
3. 情報セキュリティ対策ベンチマーク
   1) 背景と概要
   2) 利用状況
4. セキュリティ評価の目的と活用

IPAセキュリティセンターの紹介
－ 最近の調査報告書から －

IPAセキュリティセンターの概要

IPAセキュリティセンター（IPA/ISEC）

情報システムの信頼性・安全性に係わる基盤整備

情報化社会における見えない脅威から社会を守るため、ウイルス・不正アクセス対策、暗号技術、セキュリティ評価　・認証等、情報セキュリティに関する情報収集・研究開発・調査分析・普及啓発活動・脆弱性情報の発信・緊急事態発生時の対応等、他に類を見ない一貫した情報セキュリティ対策事業を実施

■情報セキュリティ技術ラボラトリー

✧　情報システム脆弱性分析の充実及び調査・研究

■情報セキュリティ認証室

✧セキュリティ評価・認証
（2004年4月からIPAが認証機関）

■企画グループ

✧　調査研究・研究開発

■ウイルス・不正アクセス対策グループ

✧ ウイルス、不正アクセスの届出と相談

■暗号グループ

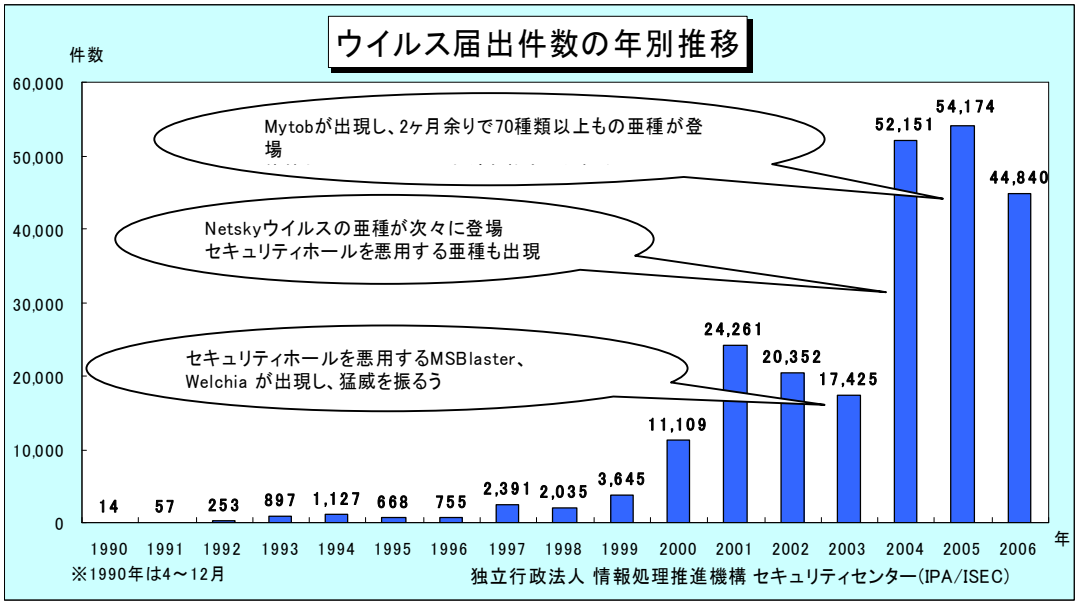
✧ 暗号技術評価プロジェクト

■普及グループ

✧　国内外のセキュリティ関係機関との連携

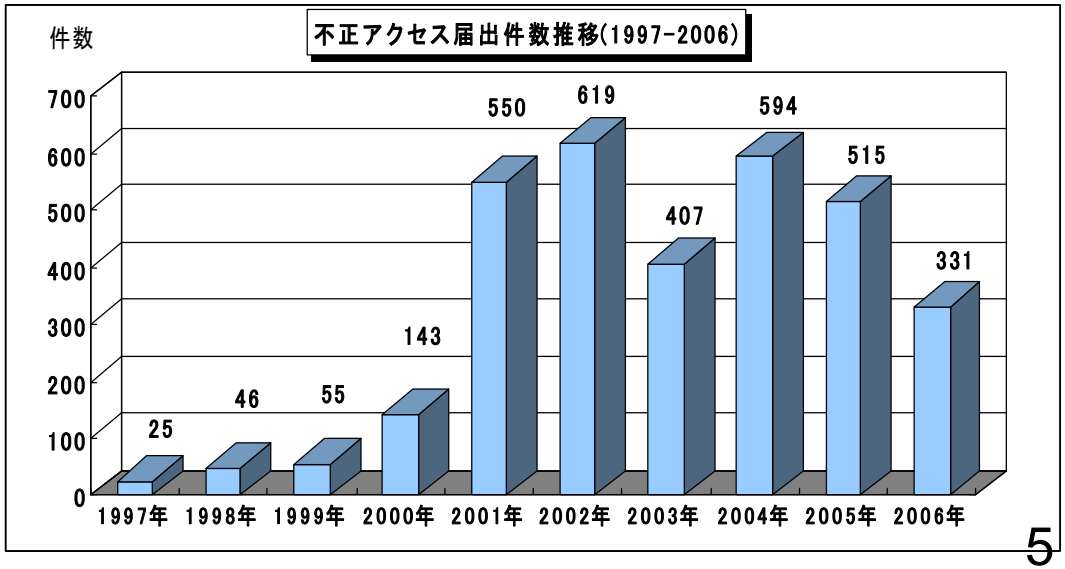
✧　情報セキュリティ対策の普及啓発

近年の情報セキュリティに関わる脅威の傾向



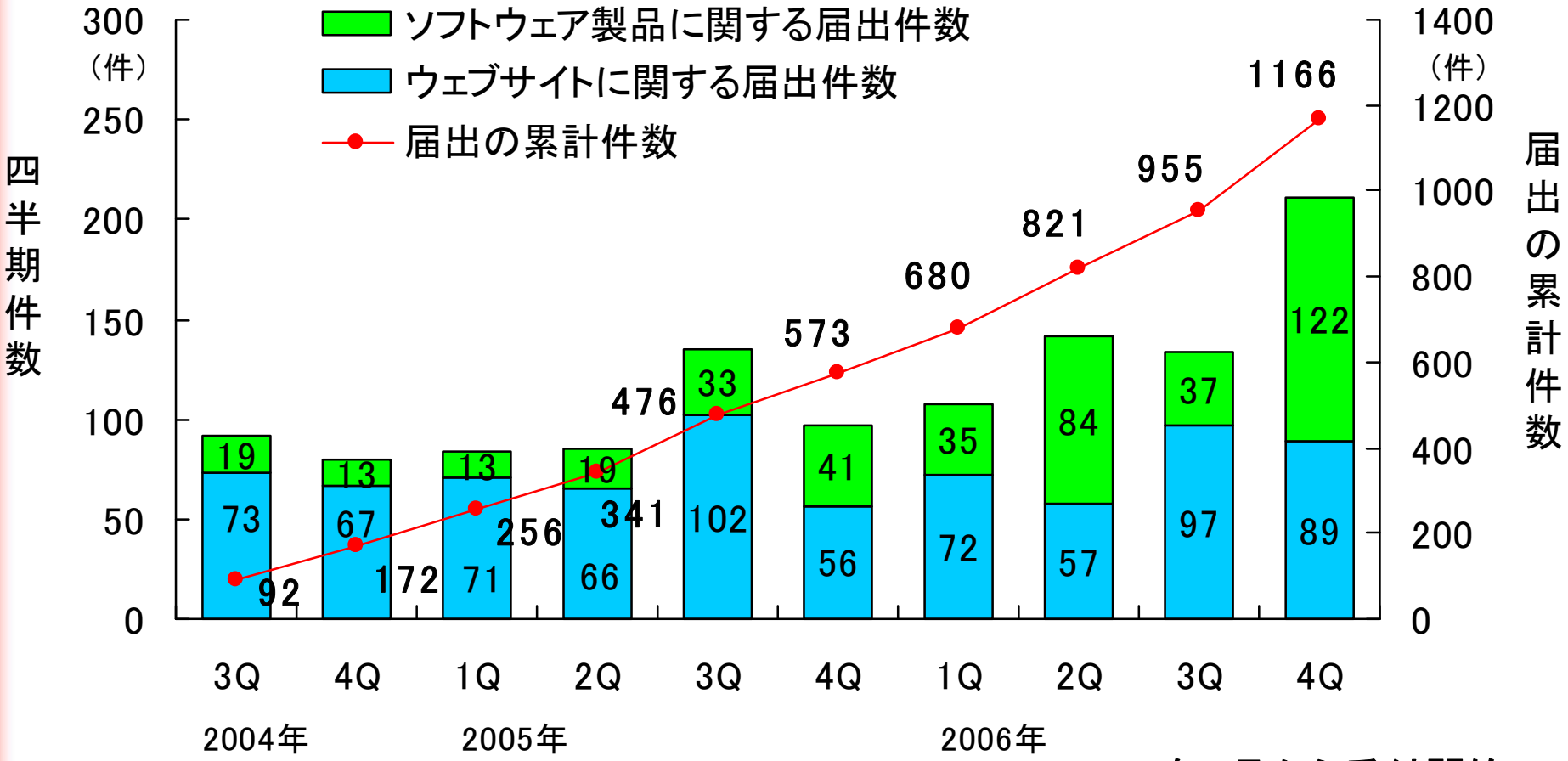
- 発生する問題の量的増加
  - コンピュータウイルス、不正アクセスの届出の増加
- 脅威の質的変化
  - 愉快犯的行為から経済的利得目的化、組織化・分業化

出典：IPA
コンピュータウイルス届出状況
http://www.ipa.go.jp/security/txt/list.html
不正アクセス届出状況
http://www.ipa.go.jp/security/ciadr/txt/list.html



脆弱性の現状：脆弱性関連情報の届出件数の推移

脆弱性の届出件数の四半期別推移
2006年10月24日に1000件に達した。



2004年7月から受付開始

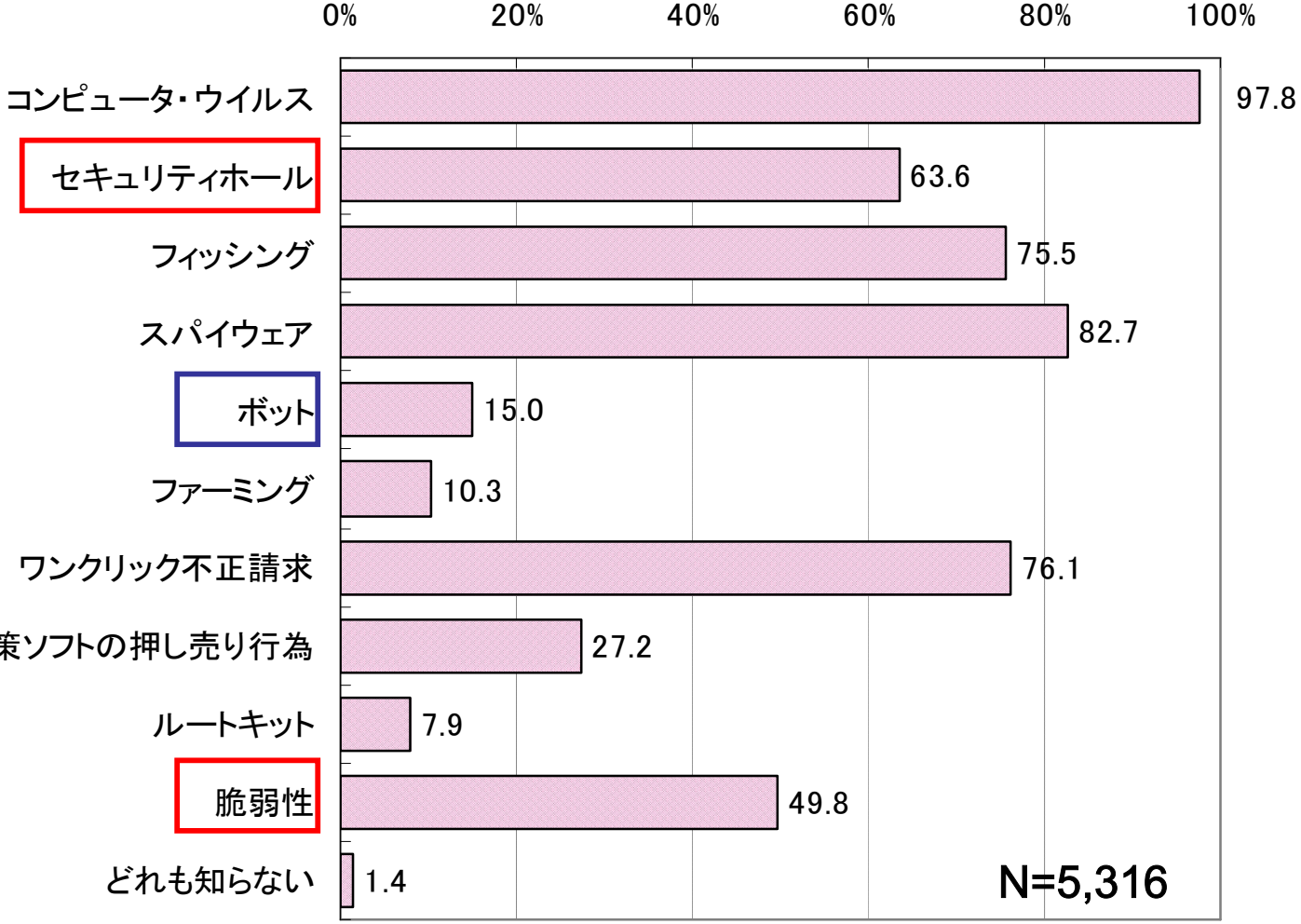
情報セキュリティに関する新たな脅威に対する意識調査

http://www.ipa.go.jp/security/fy18/reports/ishiki01/index.html

（N=5,316）

情報セキュリティに関する言葉の認知度

聞いたことがあるものをすべて選んで回答。最も認知度が高いのは「ウイルス」97.8%、次いで「スパイウェア」が82.7%。「ボット」は15.0%で低い。



「セキュリティホール、脆弱性」聞いたことがあるのはインターネットユーザのほぼ半分

2007年2月7日公開

情報セキュリティに関する言葉の認知度 ［回答者全体］（複数回答）

調査方法 ： ウェブアンケート調査　　調査期間 ： 2006年11月15日～11月16日

調査対象 ： 15歳以上のPCインターネット利用者

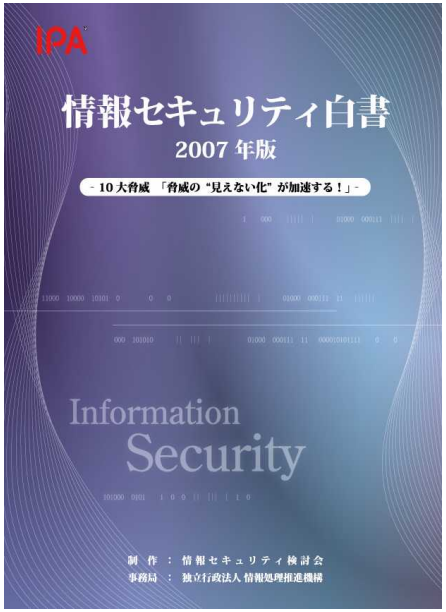
情報セキュリティ白書 2007年版

「脅威の“見えない化”が加速する！」

- 社会的影響の大きさから10大脅威を列挙
- 利用者、管理者、開発者それぞれの立場での対策

情報セキュリティ白書 2007 年版　編集: 情報セキュリティ検討会　事務局: IPA
http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.html

第1位　漏えい情報のWinnyによる止まらない流通
第2位　表面化しづらい標的型（スピア型）攻撃
第3位　悪質化・潜在化するボット
第4位　深刻化するゼロデイ攻撃
第5位　ますます多様化するフィッシング詐欺
第6位　増え続けるスパムメール
第7位　減らない情報漏えい
第8位　狙われ続ける安易なパスワード
第9位　攻撃が急増するSQLインジェクション
第10位　不適切な設定のDNSサーバを狙う攻撃の発生



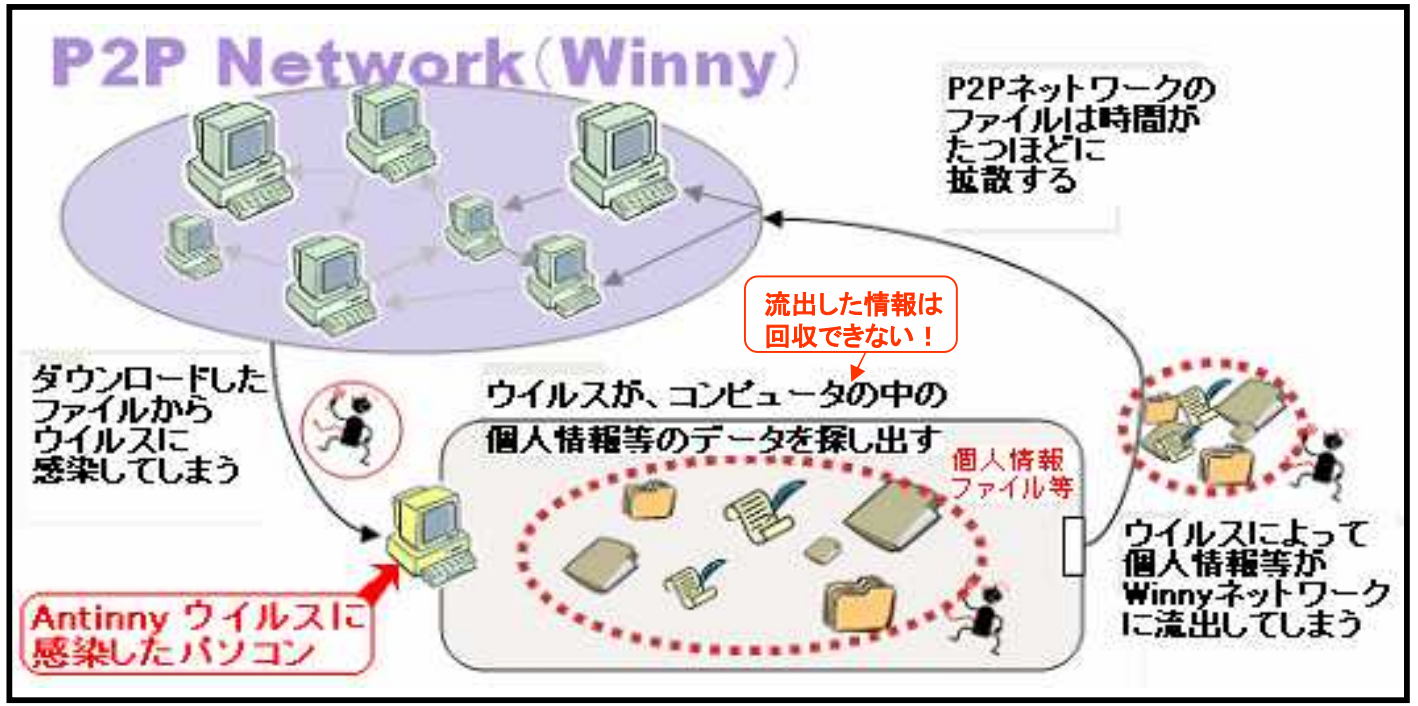
企業における情報セキュリティ事象被害額調査

- ウイルス、不正アクセス、情報漏えいなどの情報セキュリティ事象が発生した場合の企業に与えるインパ クトをどの程度の被害額が発生するのかの観点から調査
- 被害額算出モデルを用い、ウイルスによる感染被害が発生した際の、復旧費用・逸失売上を推計し算出
- 不正アクセスにより Web サービスを停止せざるを得なくなった事象、Winny を介した情報漏えい事象については、事象の発生した企業にヒアリング等を実施し（計10社）、その状況を取り纏めて推計

http://www.ipa.go.jp/security/fy17/reports/virus-survey/index.html

2006年11月29日公開

Winnyを通じたウイルス感染による情報漏えいの多発



予防策

- 漏えいして困る情報を取り扱うパソコンには　Winnyを導入しない
- 職場のパソコンに許可無くソフトウエアを導入しない
- 職場のパソコンを外部に持ち出さない
- 職場のネットワークに、私有パソコンを接続し　ない
- 自宅に仕事を持って帰らなくて済むよう作業量を適切に管理する
- 職場のパソコンからUSBメモリやCD等の媒体に情報をコピーしない
- 漏えいして困る情報を許可なくメールで送ら　ない
- ウイルス対策ソフトを導入し最新の定義ファイ　ルで監視する、不審なファイルは開かない

情報セキュリティ白書 2006 年版　- 10 大脅威「加速する経済事件化」と今後の対策 –　から
http://www.ipa.go.jp/security/vuln/20060322_ISwhitepaper.html

Winnyを介した情報漏えい被害対応の実態【ヒアリング調査の結果】

①事象の顕在化

第三者からWinnyのネットワーク上に企業情報が流れているとの通報により情報漏えいが発覚。直ちに、事実確認及び対応を実施する体制を構築。

②被害状況の調査

流出元となったPCに保存されていたデータと、Winnyネットワーク上に流通しているデータの照合、漏えいしたデータの影響範囲について分析。必要に応じて、Winnyネットワークの監視を行い、データの拡散範囲の特定を実施。

③対外説明等

漏えいしたデータに顧客情報が含まれていた場合、当該顧客への事情説明を実施。コールセンターを設置するケースもあった。

④再発防止策

社員すべてを対象として、自宅PCに業務データが保存されていないかのチェックを実施。また、情報の持ち出しルールの再徹底、Winny等のファイル交換ソフトの使用を自粛・禁止する通知を発信。

Winnyを介した情報漏えいによる被害額【ヒアリング調査結果】

推計される被害額（事例からの推計）：

被害状況の調査

・漏えいしたデータの分析　90万円～ 180万円
（社員が数十名で対応した人件費）

・流出元となったPCの調査、Winnyネットワークでの拡散状況調査
500万円～600万円
(専門業者による調査費用)

対外説明　　問合わせ窓口等　　45万円～1,600万円
(顧客への謝罪対応、問合わせ窓口設置)
※約3ヶ月間、10名体制で対応したケースも有

以上の人件費・外注費で総額2,000万円を越えるケースも有り

セキュリティ評価

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

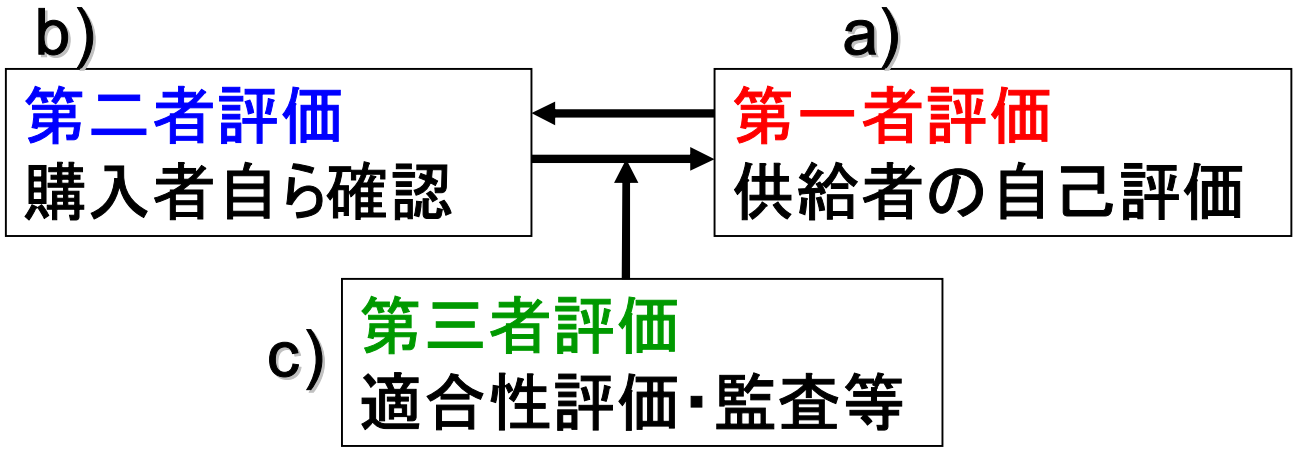
●製品等のセキュリティ実装状況の評価

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には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

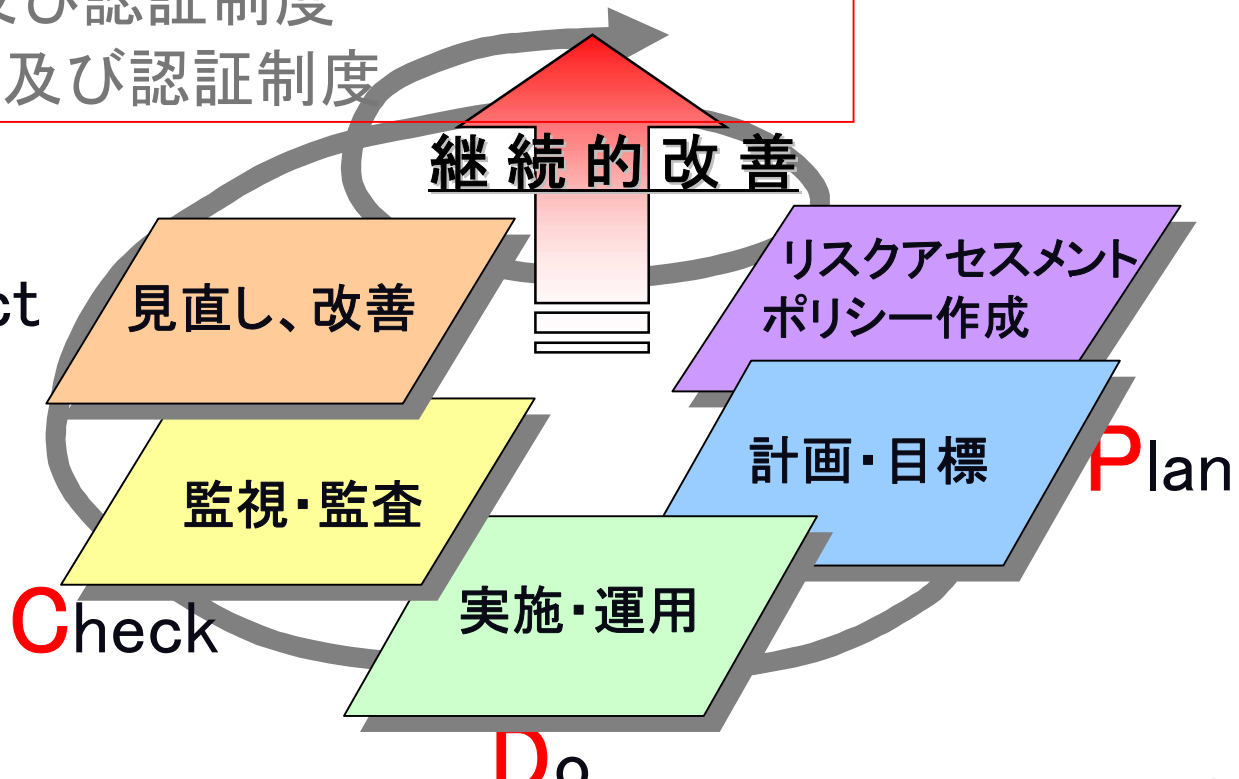
自己評価（セルフアセスメント）

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

PDCAサイクルとセキュリティ評価の活用

ISMS適合性評価制度
情報セキュリティ監査
情報セキュリティ対策ベンチマーク
自己点検
==========
ITセキュリティ評価及び認証制度
暗号モジュール試験及び認証制度

PDCAサイクルによるセキュリティレベルの向上



図は(財)日本情報処理開発協会の資料を基に作成

情報セキュリティ対策ベンチマーク
背景と概要

組織の情報セキュリティ対策状況の自己診断ツール

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

背景:「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

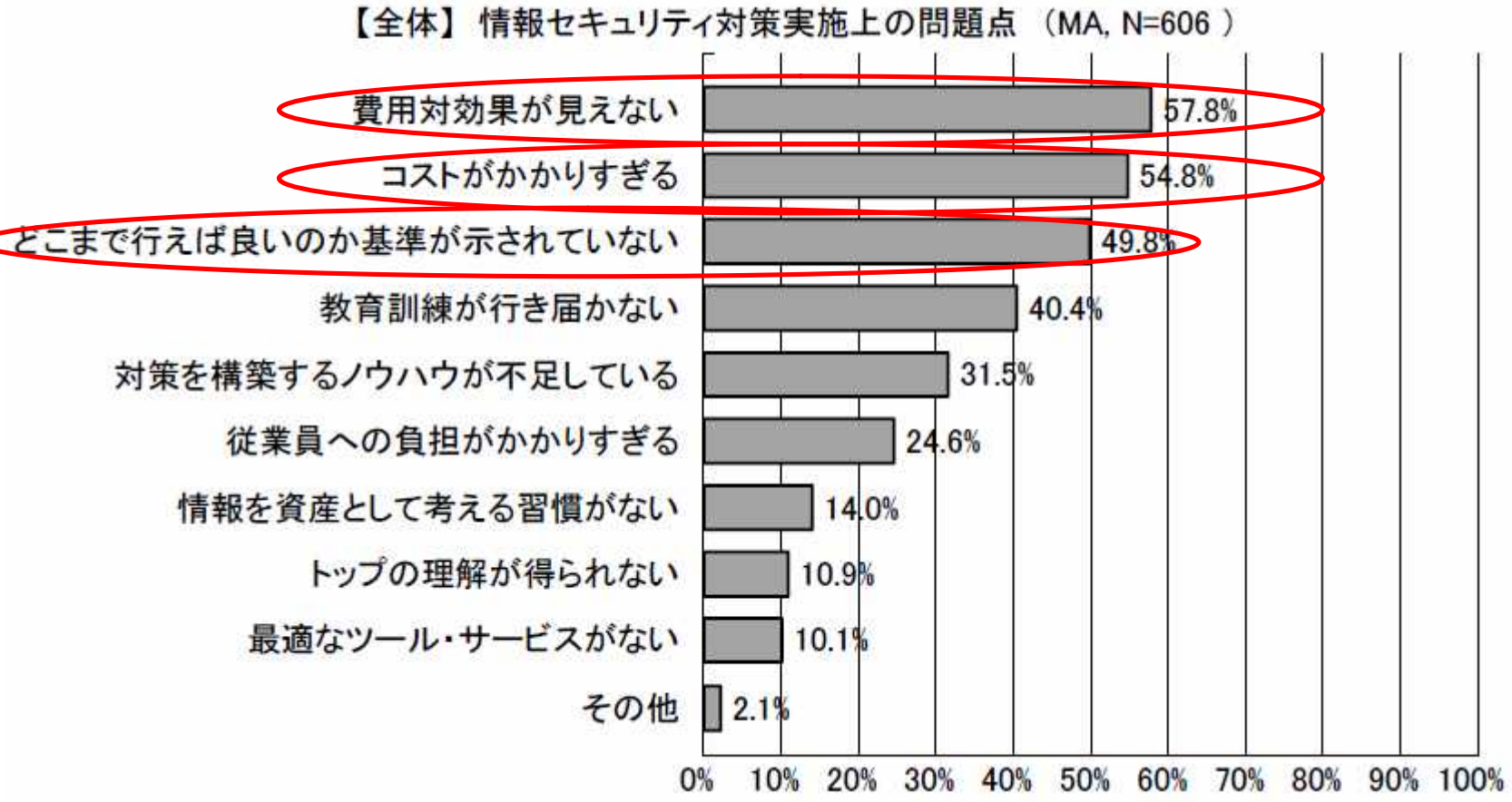
- ① 情報セキュリティ対策ベンチマーク

  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

（参考）情報セキュリティ対策実施上の問題点

➢企業が情報セキュリティ対策を行う上で障害と感じる主な要因は、
①費用対効果が見えない（57.8%），コストがかかりすぎる（54.8%）
②どこまで行えばよいか基準が示されていない（49.8%）



出典：平成17年度「不正アクセス行為対策等の実態調査」(警察庁) http://www.npa.go.jp/cyber/research/h17/countermeasures.pdf

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/index.html

- 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

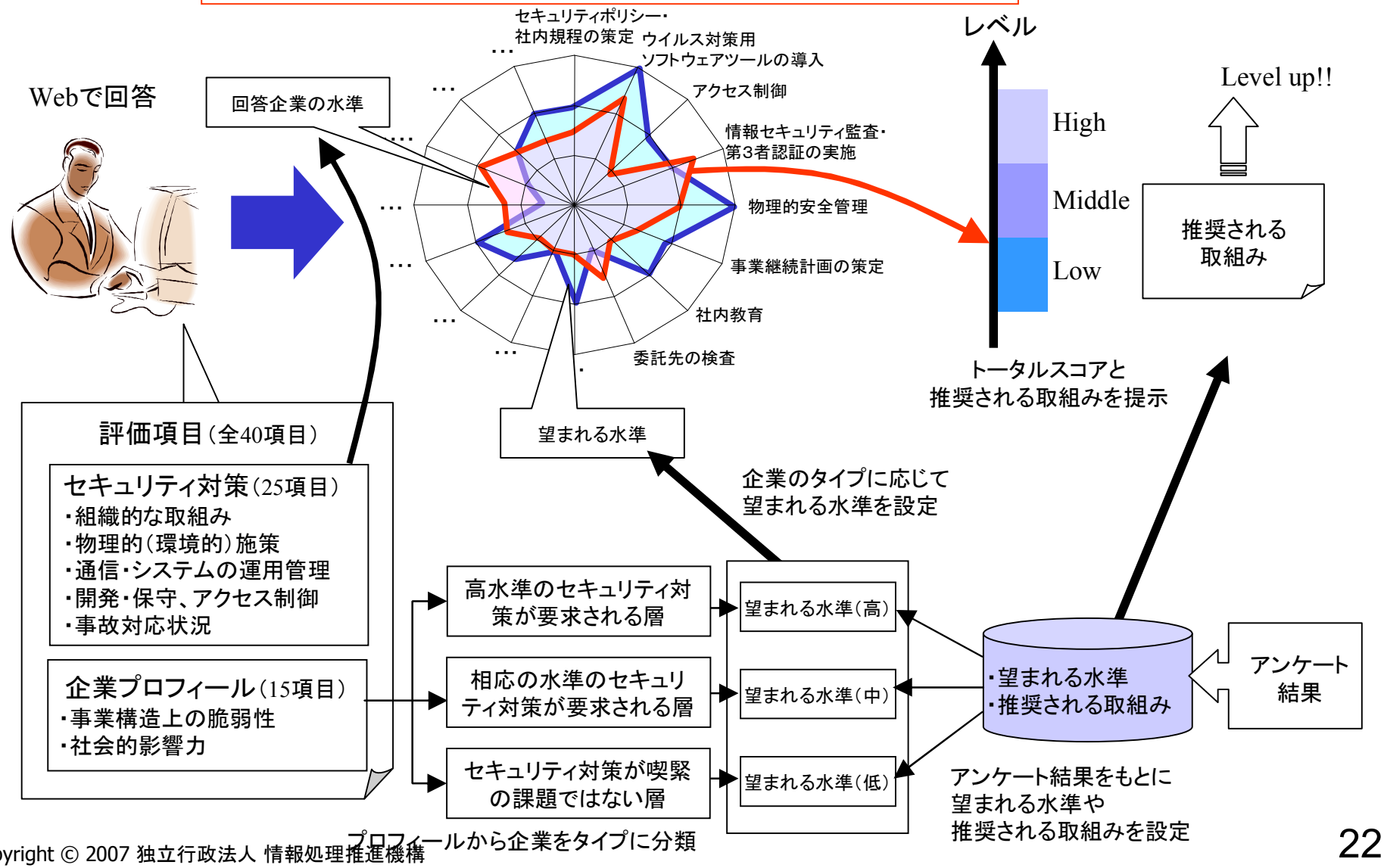
ある指標（ベストプラクティス）を探し出し、それと比べて自社のレベルを評価し、足りない部分を改善していく経営改善の手法

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

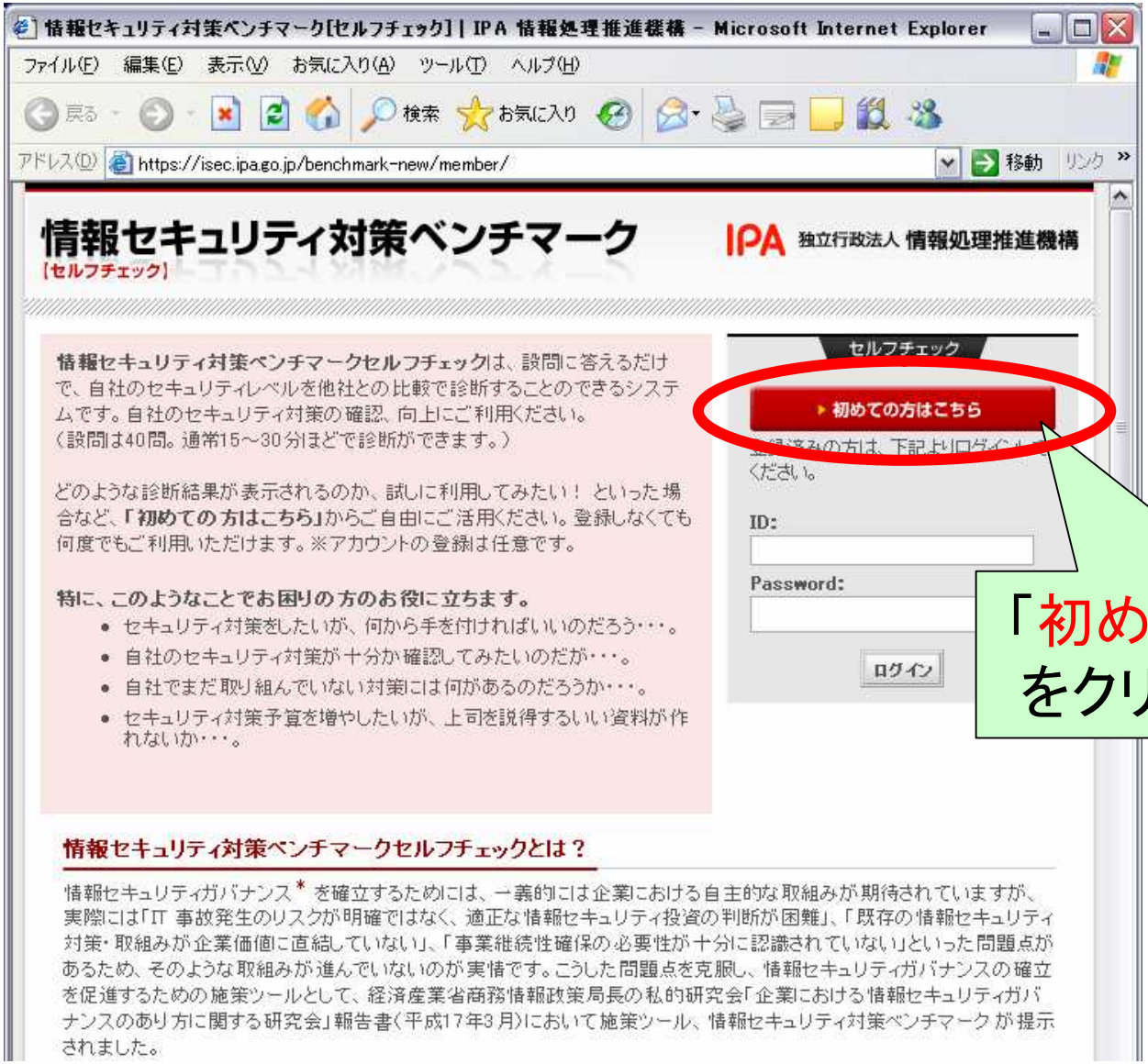
情報セキュリティガバナンス推進には経営陣の積極的関与が不可欠

情報セキュリティ対策ベンチマーク システムの概要

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

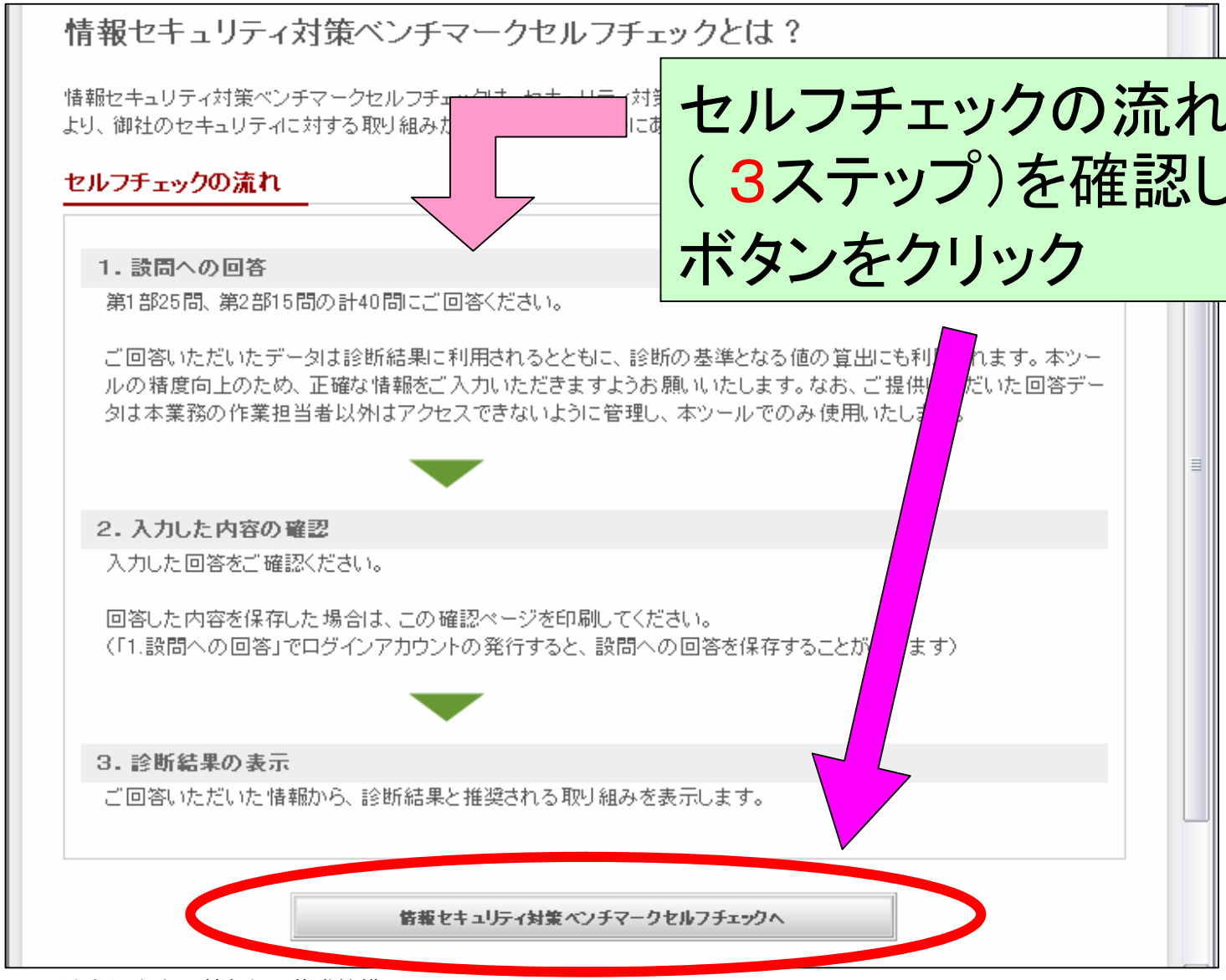


情報セキュリティ対策ベンチマークシステムの利用方法①



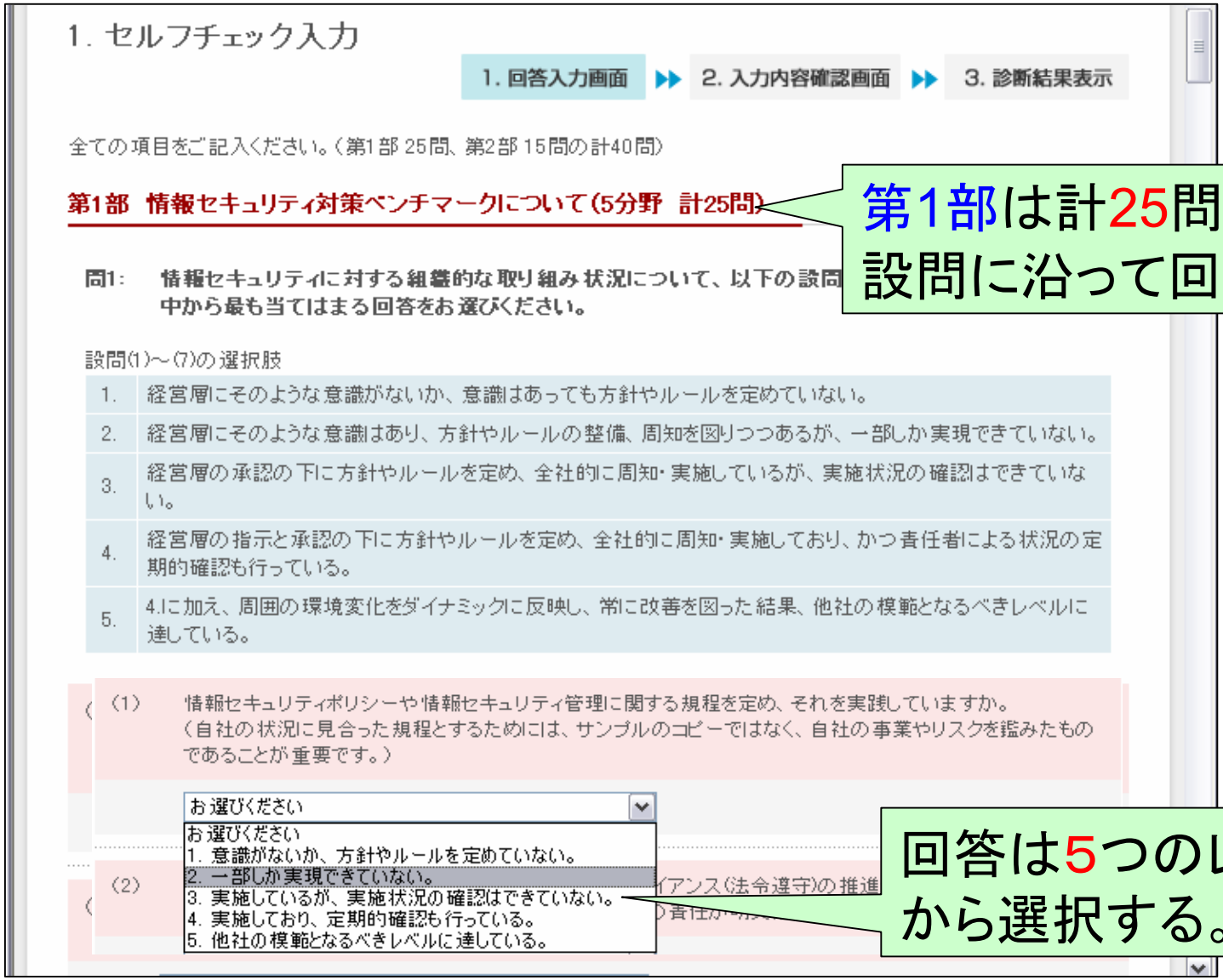
「初めての方はこちら」
をクリックしてスタート

情報セキュリティ対策ベンチマークシステムの利用方法②



セルフチェックの流れ（３ステップ）を確認しボタンをクリック

情報セキュリティ対策ベンチマークシステムの利用方法③



情報セキュリティ対策ベンチマークシステムの利用方法④

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 （5項目）
(c) 通信ネットワーク及び情報システムの運用管理 （5項目）
(d) 情報システムの開発、保守におけるセキュリティ対策
　及び情報や情報システムへのアクセス制御の状況 （5項目）
(e) 情報セキュリティ上の事故対応状況 （3項目）

ISMS認証基準Ver.2.0の詳細管理策がベース
- 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。

情報セキュリティ対策ベンチマーク
セキュリティ対策の取組み状況　評価項目 (a) 7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）

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定とするには・・・・・

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・・・・・

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。

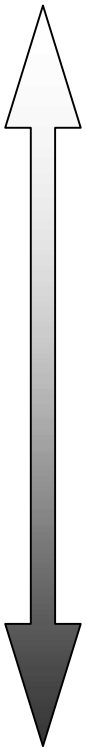
オ） 貴社では、社外の組織に業務を委託する際の契約書に、セキュリティ上の理由から相手方に求めるべき事項を記載していますか。セキュリティ上の理由とは・・・・

カ） 貴社では、従業者（派遣を含む）に対し、入社、退職の際に機密保持に関する書面を取り交わすなどして就業上のセキュリティに関する義務を明確にしていますか。

キ） 貴社では、従業者（派遣を含む）に対し、情報セキュリティに関する貴社の取組みや関連ルールについての計画的な教育や指導を実施していますか。

第1部の選択肢

できていない

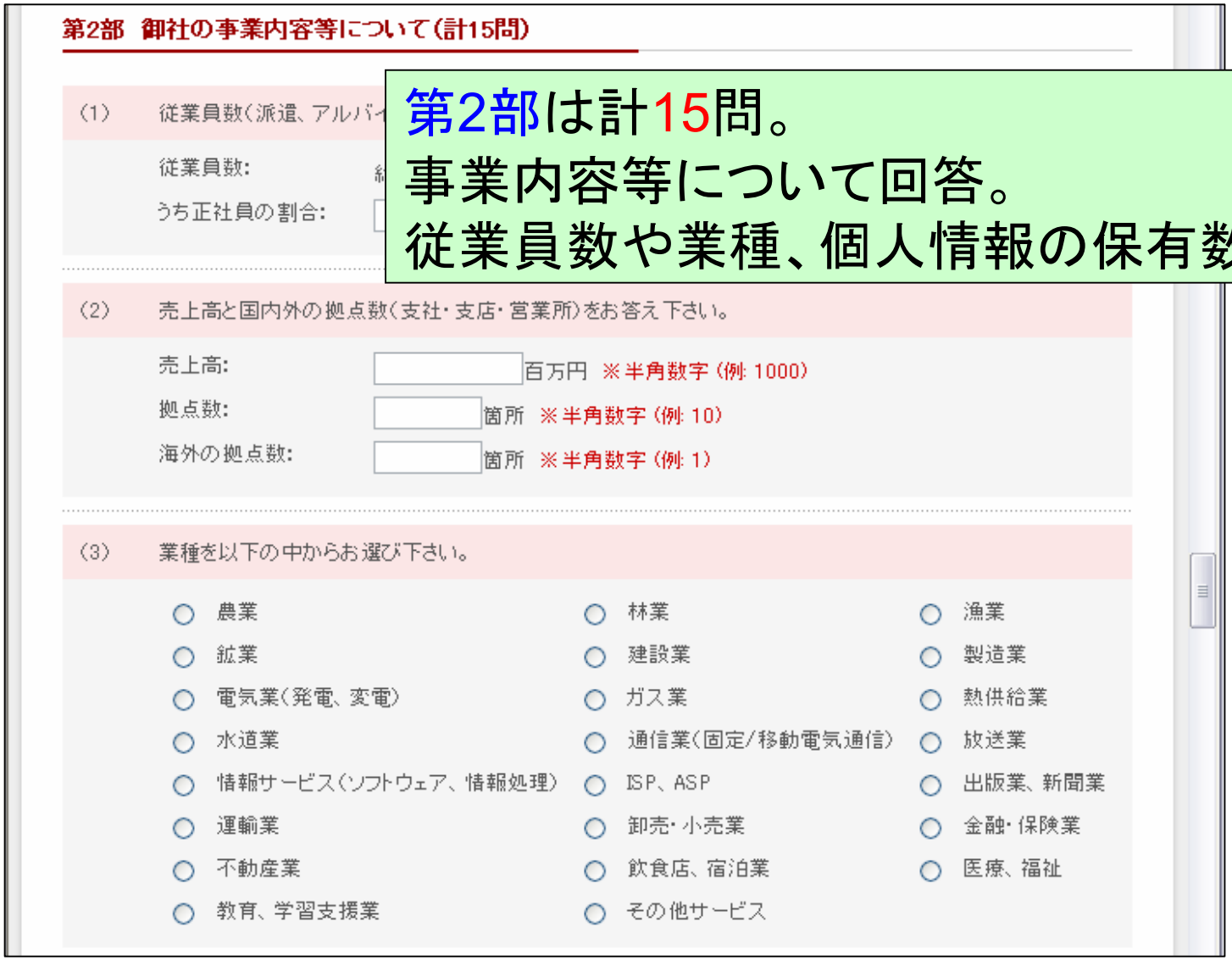


1	経営層にそのような意識がないか、意識はあっても方針やルールを定めていない
2	経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3	経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4	経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5	4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

できている

2. 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システムの利用方法⑥



第2部は計15問。
事業内容等について回答。
従業員数や業種、個人情報の保有数など。

情報セキュリティ対策ベンチマーク

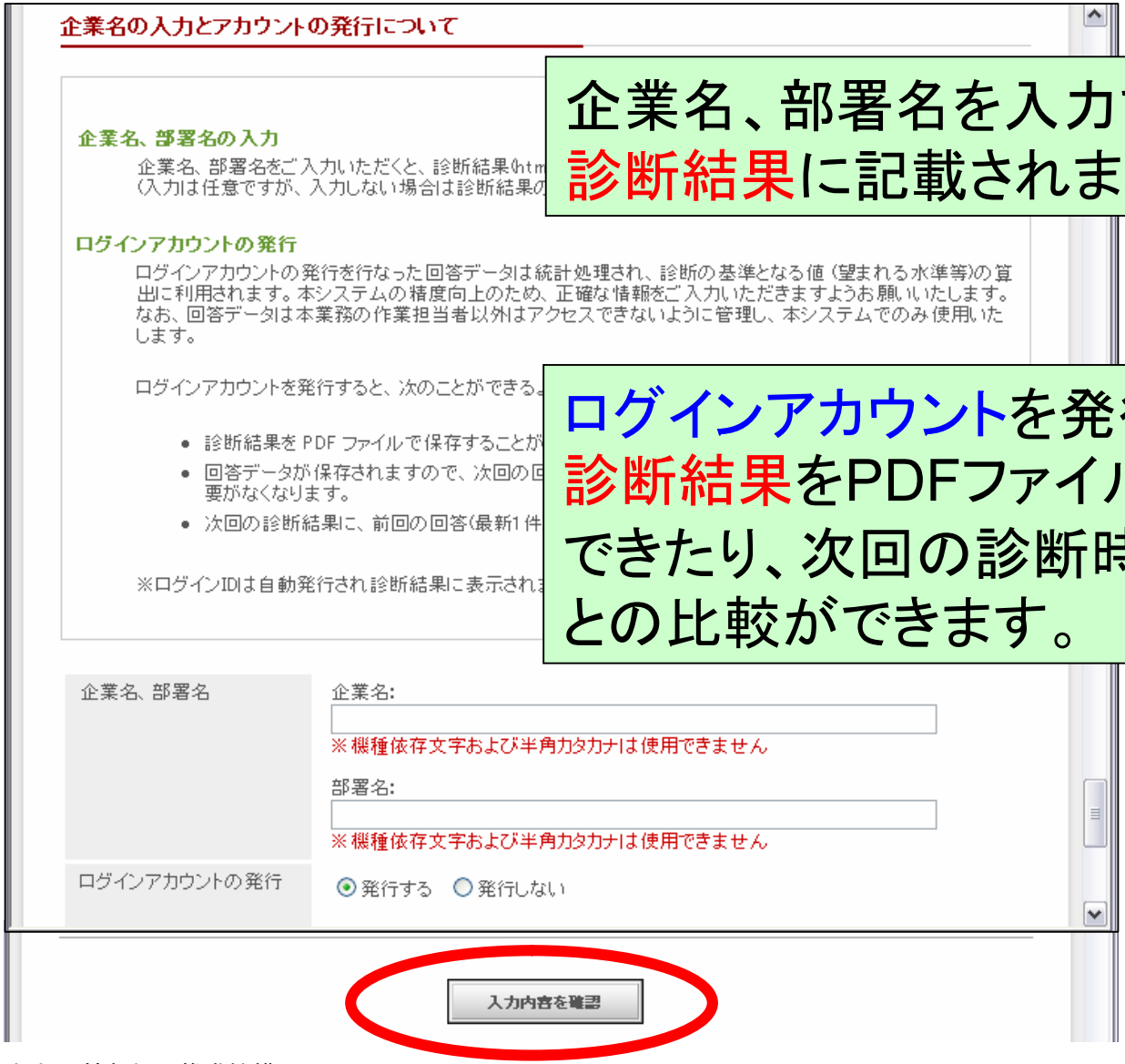
企業プロフィール

一般的な企業属性、事業構造上の脆弱性や社会的影響力により構成

(a) 従業者数（派遣、アルバイトを含む）及びそのうちの正社員の割合
(b) 売上高、国内外の拠点数（支社・支店・営業所）
(c) 業種
(d) 国家や社会基盤、経済基盤に与える影響の観点から見た公益性
(e) 事業が、顧客の生命・身体・財産・名誉等に与える影響の大きさ
(f) 主要業務のうち、情報システム（社外のシステムを含む）に依存している割合
(g) 主要な業務に関わる業務プロセスのうち、インターネットに依存している割合
(h) 主要情報システムの、（月間）売上高に影響を及ぼさない許容停止時間
(i) 主要情報システムが営業日に24時間停止の場合、当該日売上高への影響
(j) 情報セキュリティ事故が発生した場合のブランド（企業イメージ）への影響
(k) 元請や代理店、フランチャイジー等のビジネスパートナーへの依存度
(l) 重要情報（国家機密・営業機密・プライバシー情報等）の保有・管理・使用状況
(m) 個人情報の取扱量
(n) 離職率（直近の１年間に退職・転職された従業者の割合）
(o) 事業活動に影響を与えるような情報セキュリティ関連の事故の発生経験

2. 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システムの利用方法⑦

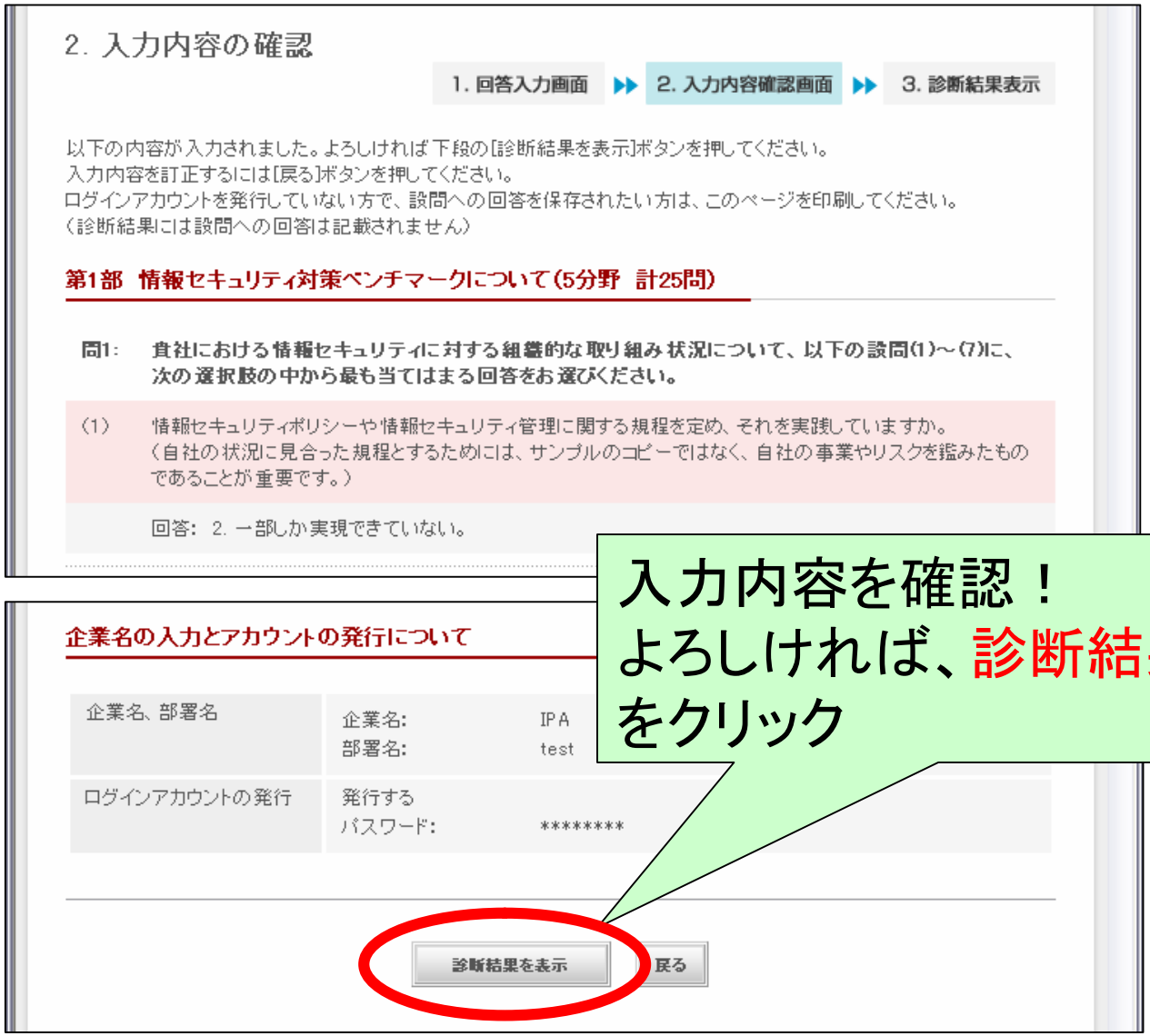


企業名、部署名を入力すると、診断結果に記載されます。

ログインアカウントを発行すると診断結果をPDFファイルで保存できたり、次回の診断時に前回との比較ができます。

2. 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システムの利用方法⑧



2. 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システムの利用方法⑨

ログインアカウントを発行していると、診断結果をPDFで保存できます。

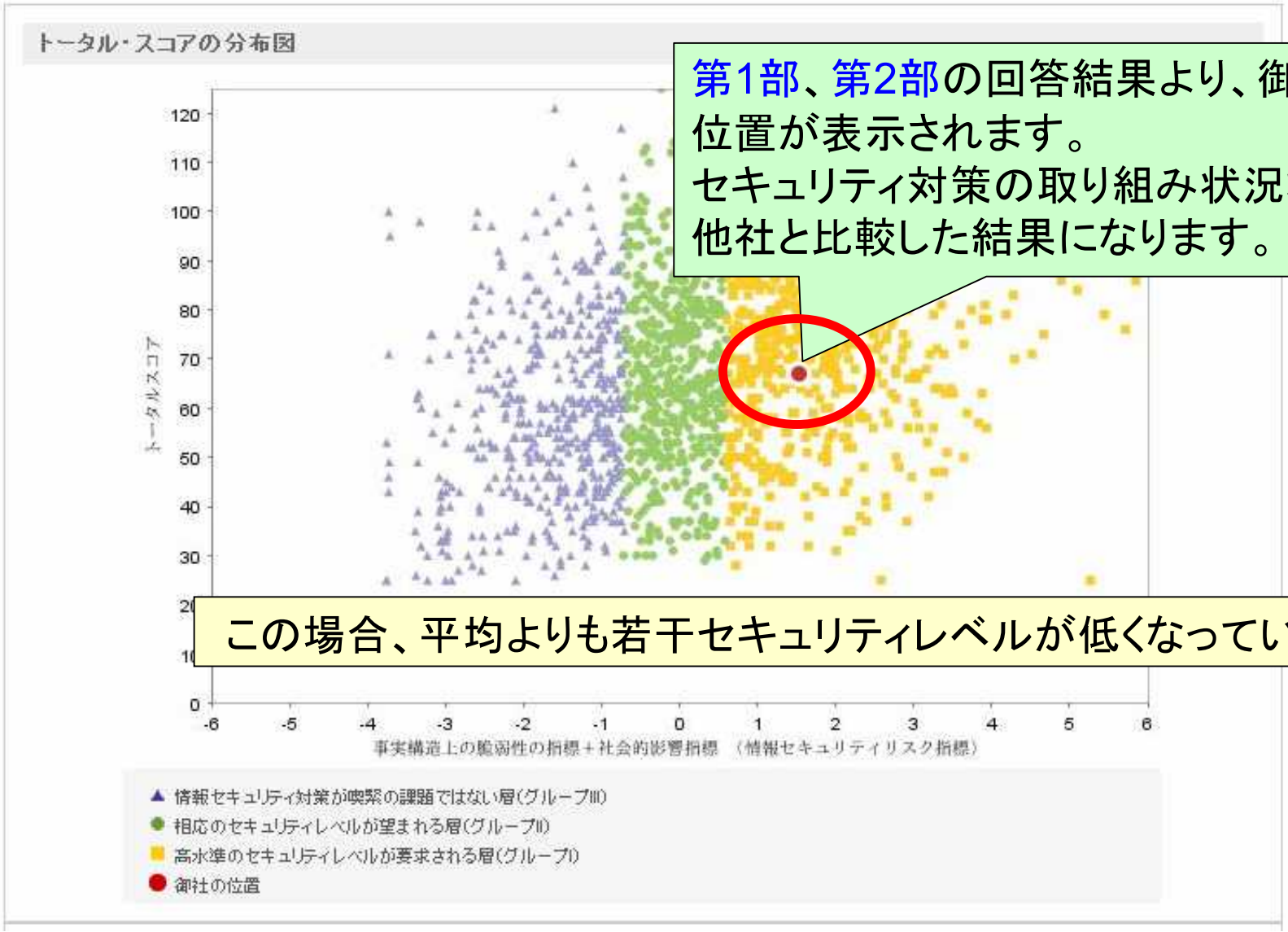
情報セキュリティ対策ベンチマーク

企業分類

企業プロフィールから [1]事業構造上の脆弱性、[2]社会的影響力を分類軸として以下の3グループに分類

①高水準のセキュリティレベルが要求される層
②相応の水準のセキュリティレベルが望まれる層
③情報セキュリティ対策が喫緊の課題でない層

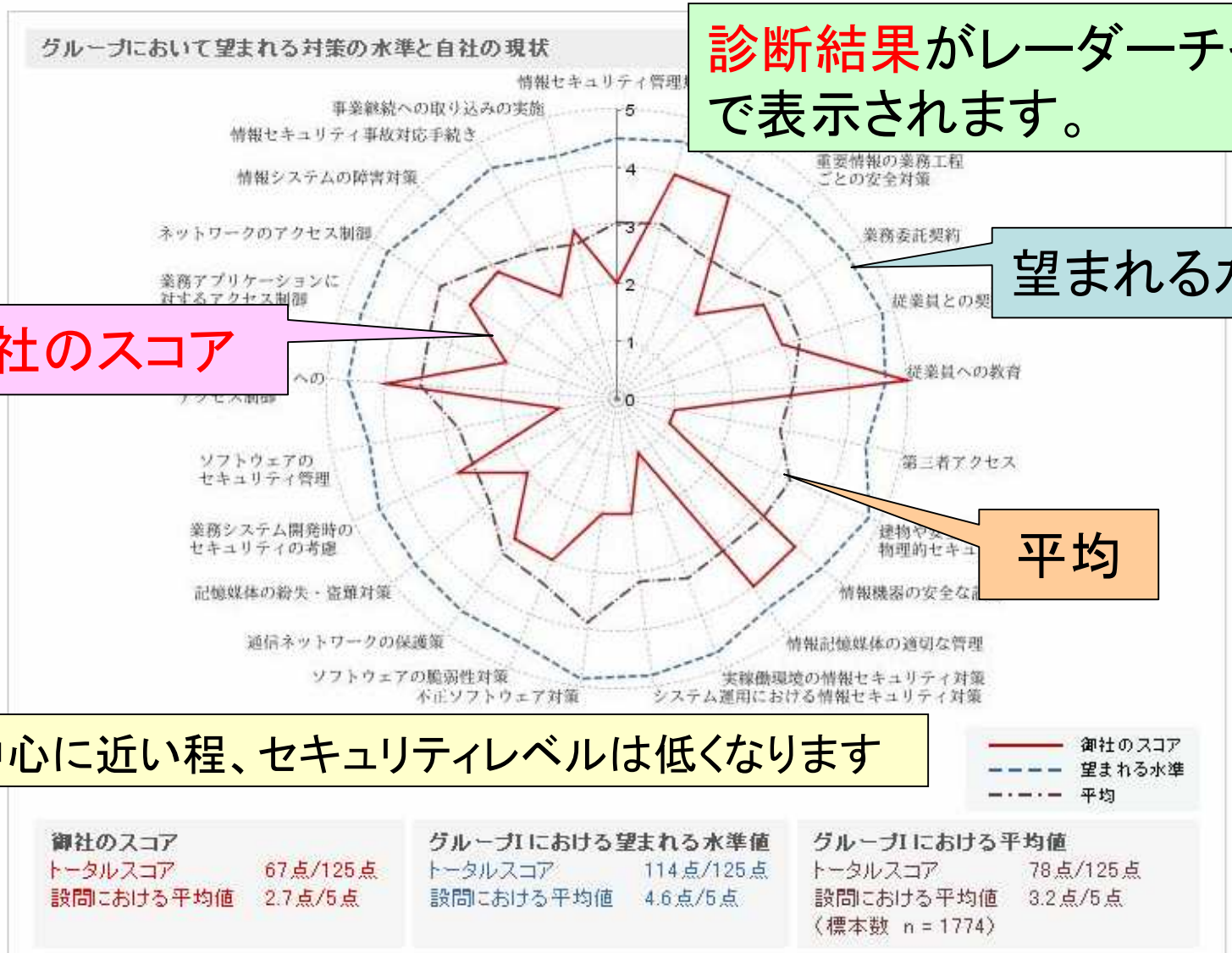
情報セキュリティ対策ベンチマークシステムの診断結果①



第1部、第2部の回答結果より、御社の位置が表示されます。
セキュリティ対策の取り組み状況など、他社と比較した結果になります。

この場合、平均よりも若干セキュリティレベルが低くなっています

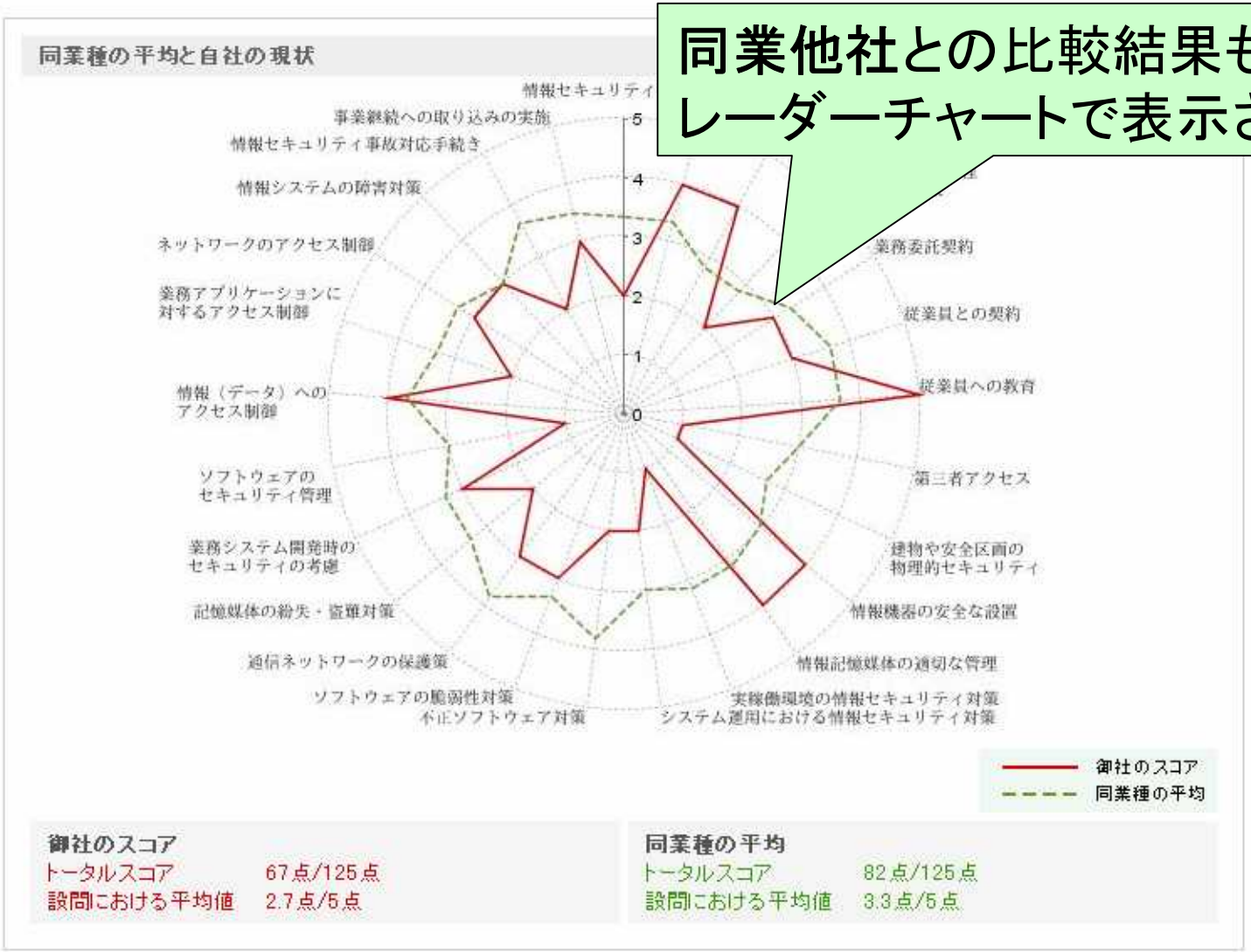
情報セキュリティ対策ベンチマークシステムの診断結果②



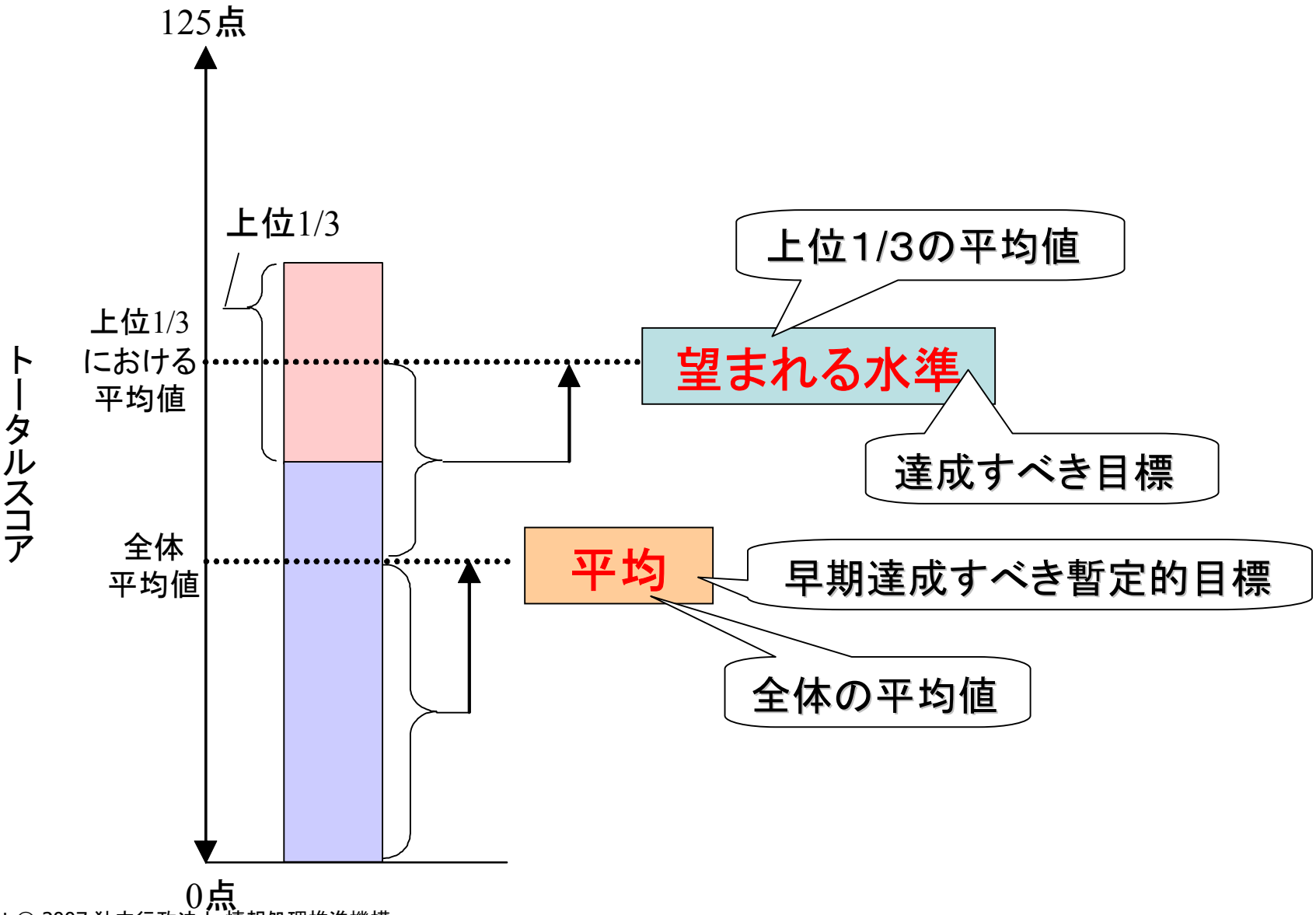
情報セキュリティ対策ベンチマークシステムの診断結果③

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。



情報セキュリティ対策ベンチマークシステム：望まれる水準



情報セキュリティ対策ベンチマーク
セルフチェックの結果：推奨される取組み例

IPA®

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が選択
すので、今後の対策や改善への取り組みの参考

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、作業責任者や手順の

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。

説明:
個人情報保護法の規定やガイドラインに
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。

情報セキュリティ対策ベンチマーク
セルフチェックの結果：推奨される取組み例

大項目1. 貴社における情報セキュリティに対する組織的な取組状況についてうかがいます。

質問① 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。

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。

対策のポイント：

- ●情報セキュリティポリシーや管理規程が策定されているか
- ●ひな形、サンプル、他社事例等のコピーではなく、社内で十分な討議を経て、自社の状況に見合った内容となっているか
- ●ポリシーは全社をカバーしているか
- ●社長ないし上級役員が承認しているか
- ●全従業者（派遣を含む）に対して通知・公表済みか
- ●定期的に見直すための手続きを定めているか
- ●既に見直し時期が到来していた場合、見直しを実施したか
- ●改訂結果について、社長ないし上級役員の承認を得て、再度通知・公表したか
- ●従業員がポリシーや関連規程類を遵守し、率先垂範を確認するための手続きを定めているか
- ●ネットワーク検査や侵入テストを定期的に実施し、ポリシーの実装状況を確認しているか

解説： 効果的な情報セキュリティ対策を実現するためには、情報セキュリティに関する・・・・・・・・・

情報セキュリティ対策ベンチマーク
評価項目と対策のポイント

評価項目：5グループ、グループ毎に3～7項目　**計25項目**
対策のポイント：各項目毎に3～10個　**計127**

(a)情報セキュリティに対する組織的な取組状況（①～⑦）
①10+②12+③5+④5+⑤4+⑥4+⑦5 = 45

(b) 物理的（環境的）セキュリティ上の施策（①～ ⑤）
①4+②6+③3+④4+⑤5 = 22

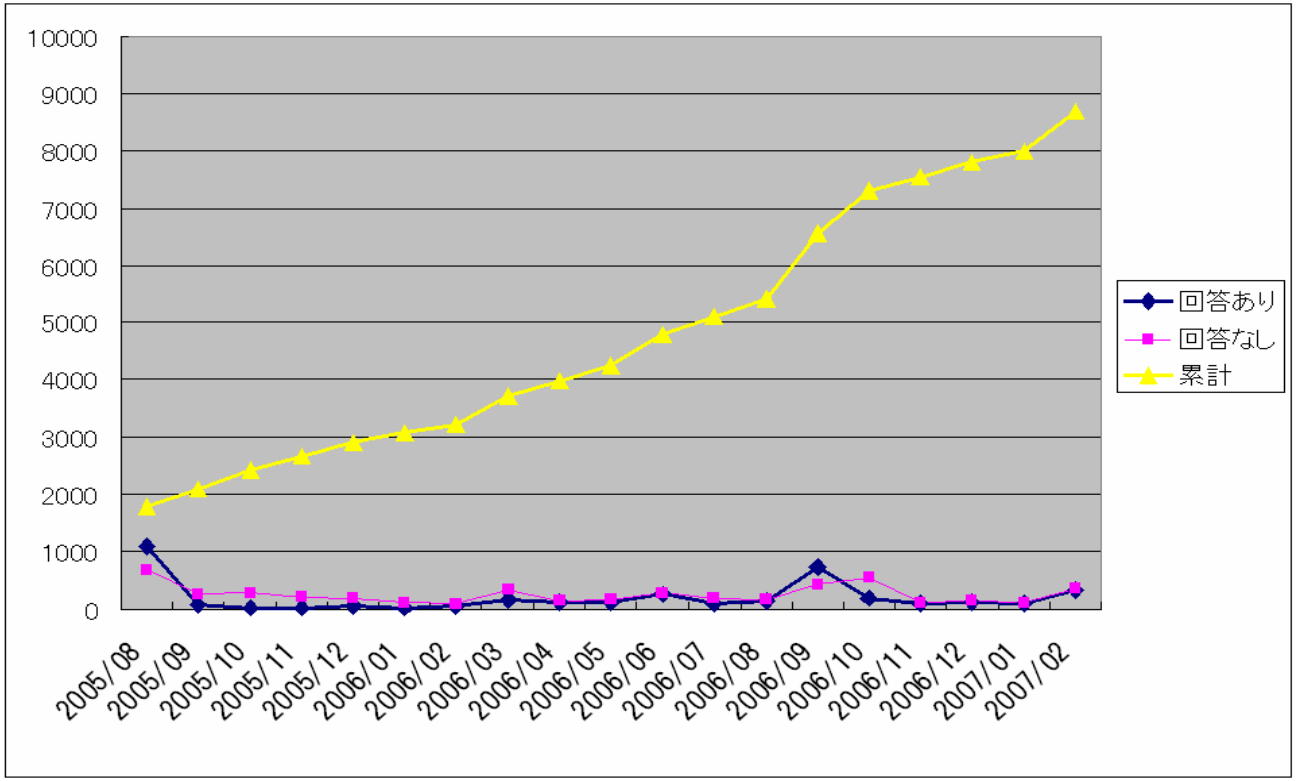
(c) 通信ネットワーク及び情報システムの運用管理（①～⑤）
①4+②5+③3+④3+⑤6 = 21

(d) 情報システムの開発、保守におけるセキュリティ対策
及び情報や情報システムへのアクセス制御の状況（①～⑤）
①5+②5+③5+④2+⑤6 = 23

(e) 情報セキュリティ上の事故対応状況（①～ ③）
①7+②4+③5 = 16

情報セキュリティ対策ベンチマーク
利用状況

情報セキュリティ対策ベンチマーク
利用状況



ベンチマーク利用件数は8,500件を超える

2007年2月25日現在

※ 3,816件の提供データの内の885件は、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（H17.3)におけるデータ 。

回答データ提供有り	回答データ提供無し	合計
3,816※件 （300人以下の企業 2,083件（55%）を含む）	4,871件	8,687件

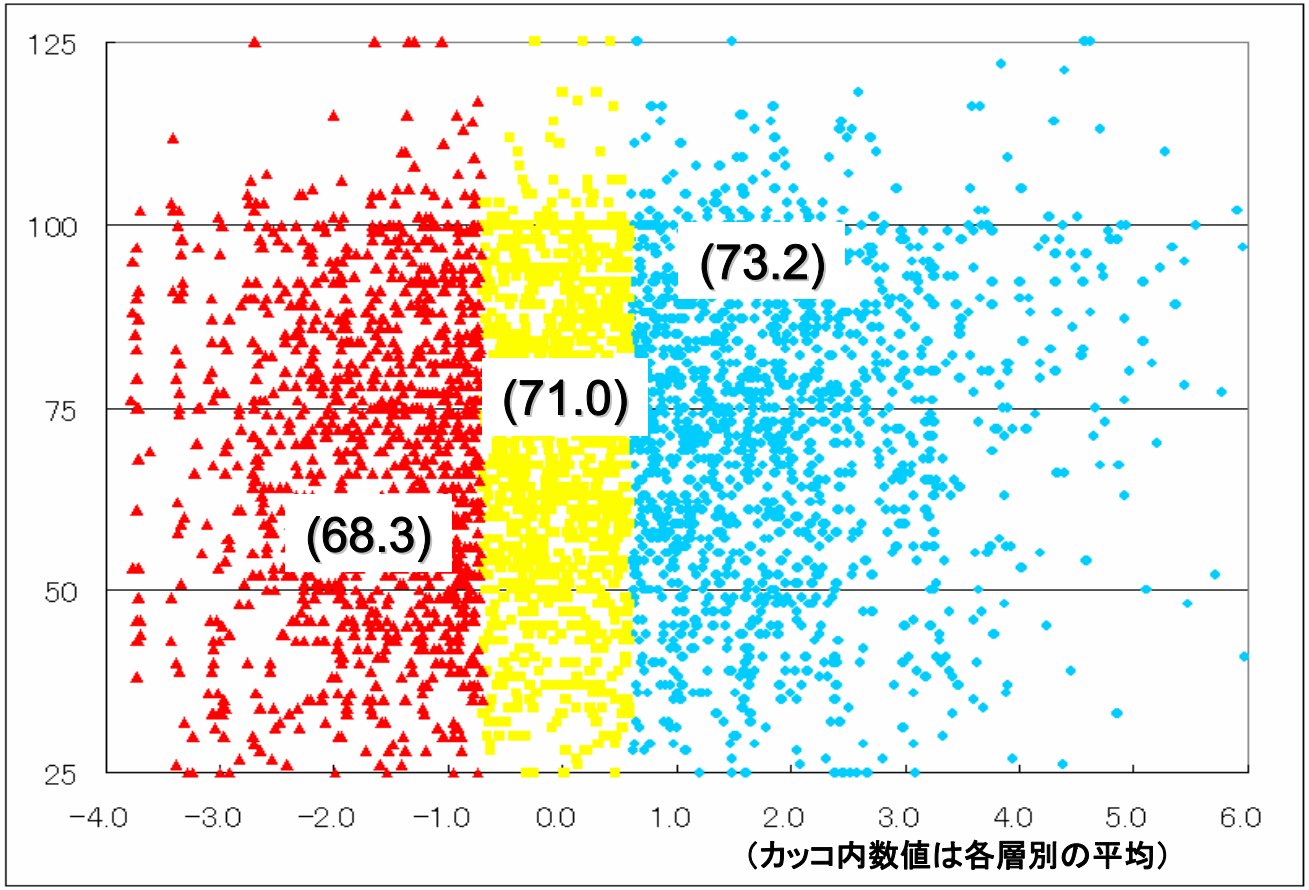
情報セキュリティ対策ベンチマーク
トータルスコアの分布

IPA

全企業 （3,816件より）

2007年2月25日現在

30.9%　30.2%　38.9%　← 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 70.8

業構造上の脆弱性指標＋社会的影響力指標
（情報セキュリティリスク指標）

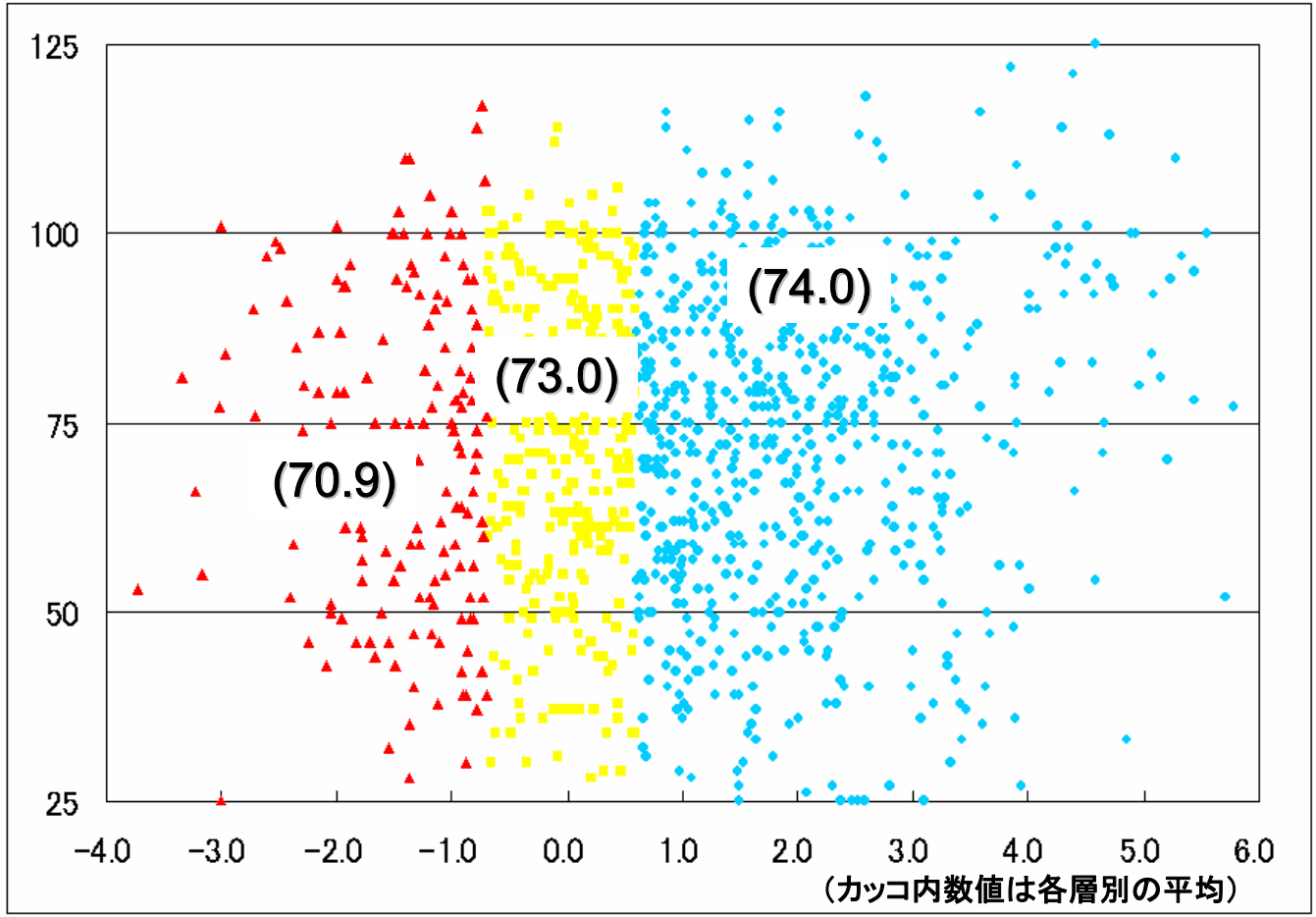
注：縦軸はセキュリティ対策スコア、横軸は情報システム依存度や個人情報の保有数などの業態で決定。

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

重要インフラの企業 (N=1165)

2007年2月25日現在

13.6%　27.6%　58.8%　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
72.6

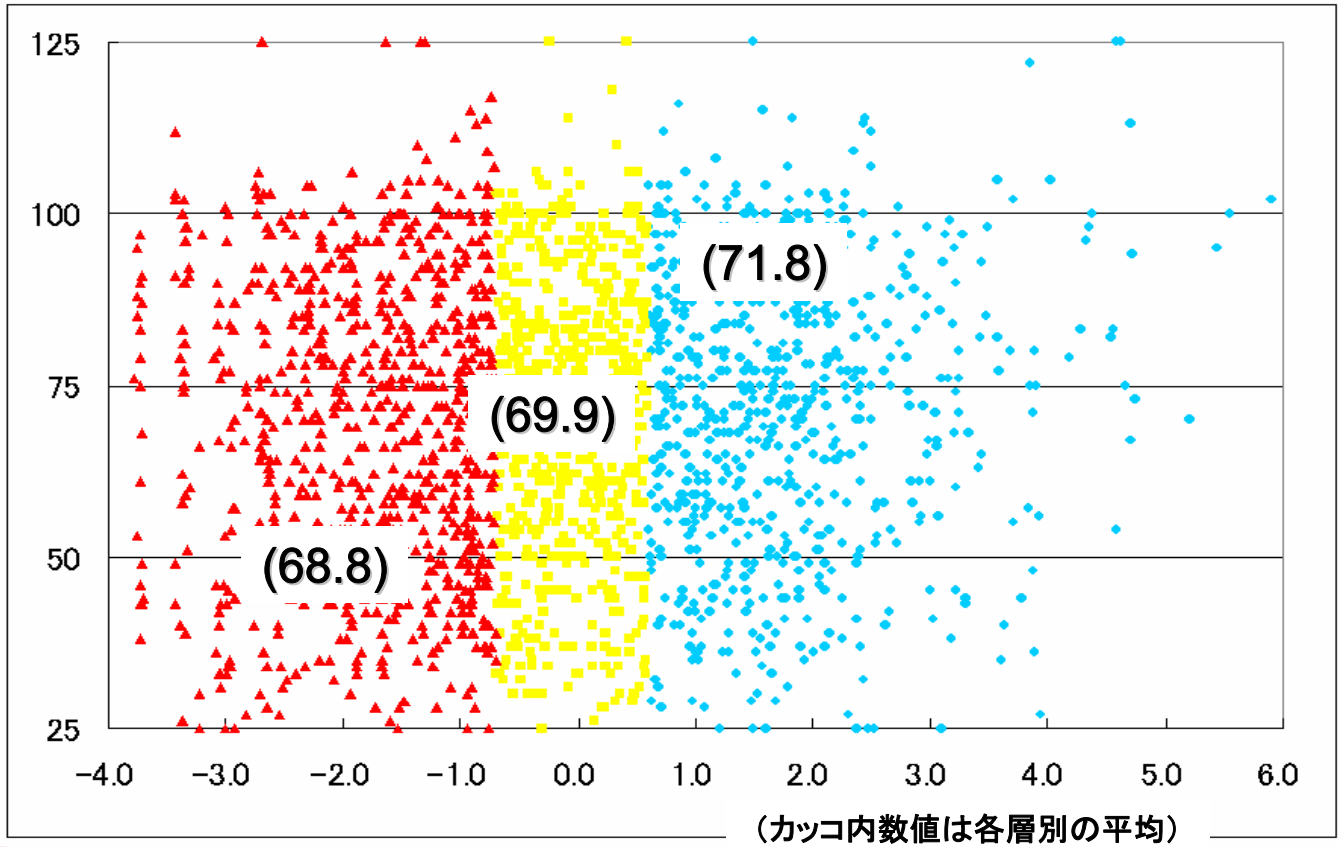
情報セキュリティ対策ベンチマーク
トータルスコアの分布

300人以下の企業でも高いセキュリティが求められる

従業員数300人以下の企業 (N=2083)

2007年2月25日現在

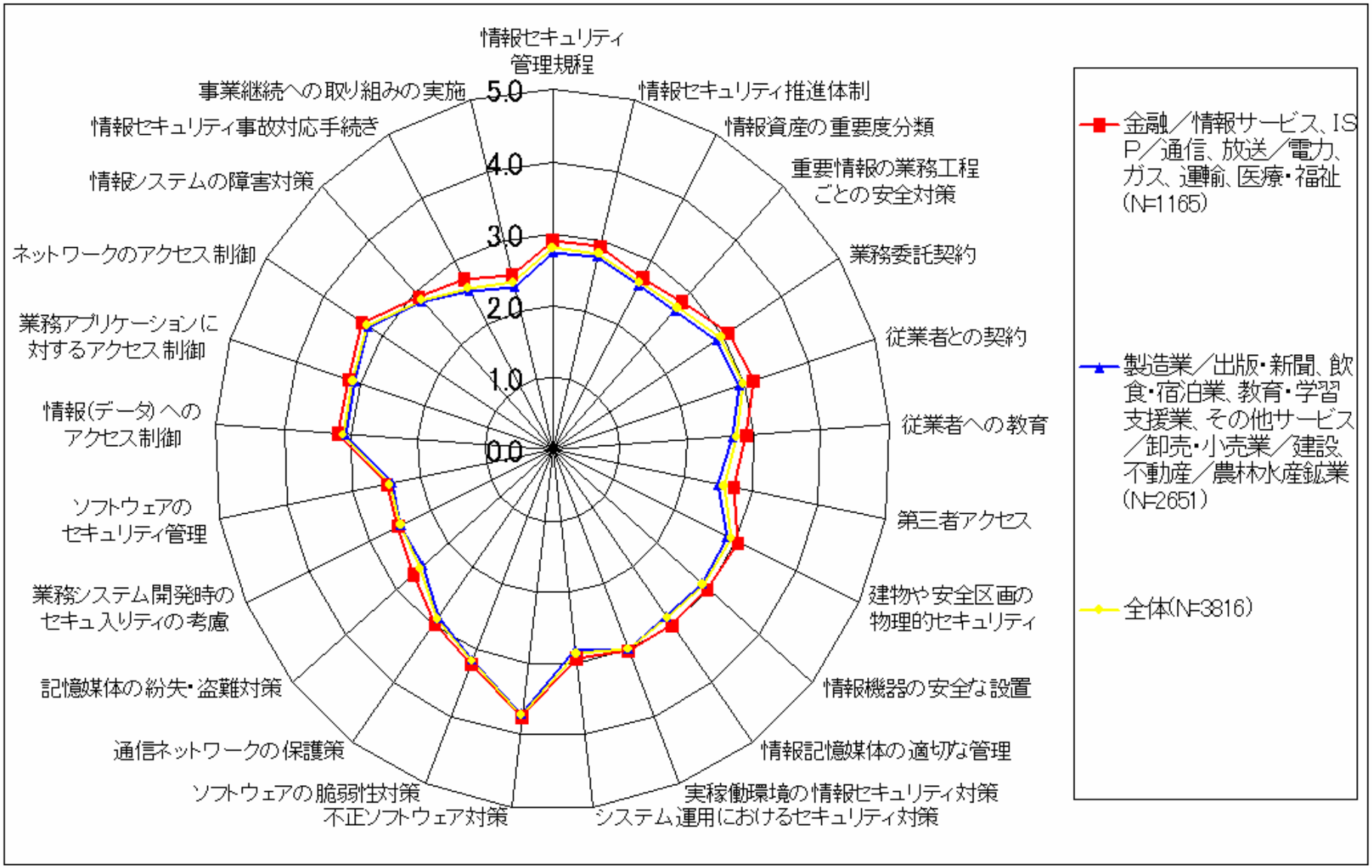
38.6% 28.7% 32.7% ← 各層の構成割合



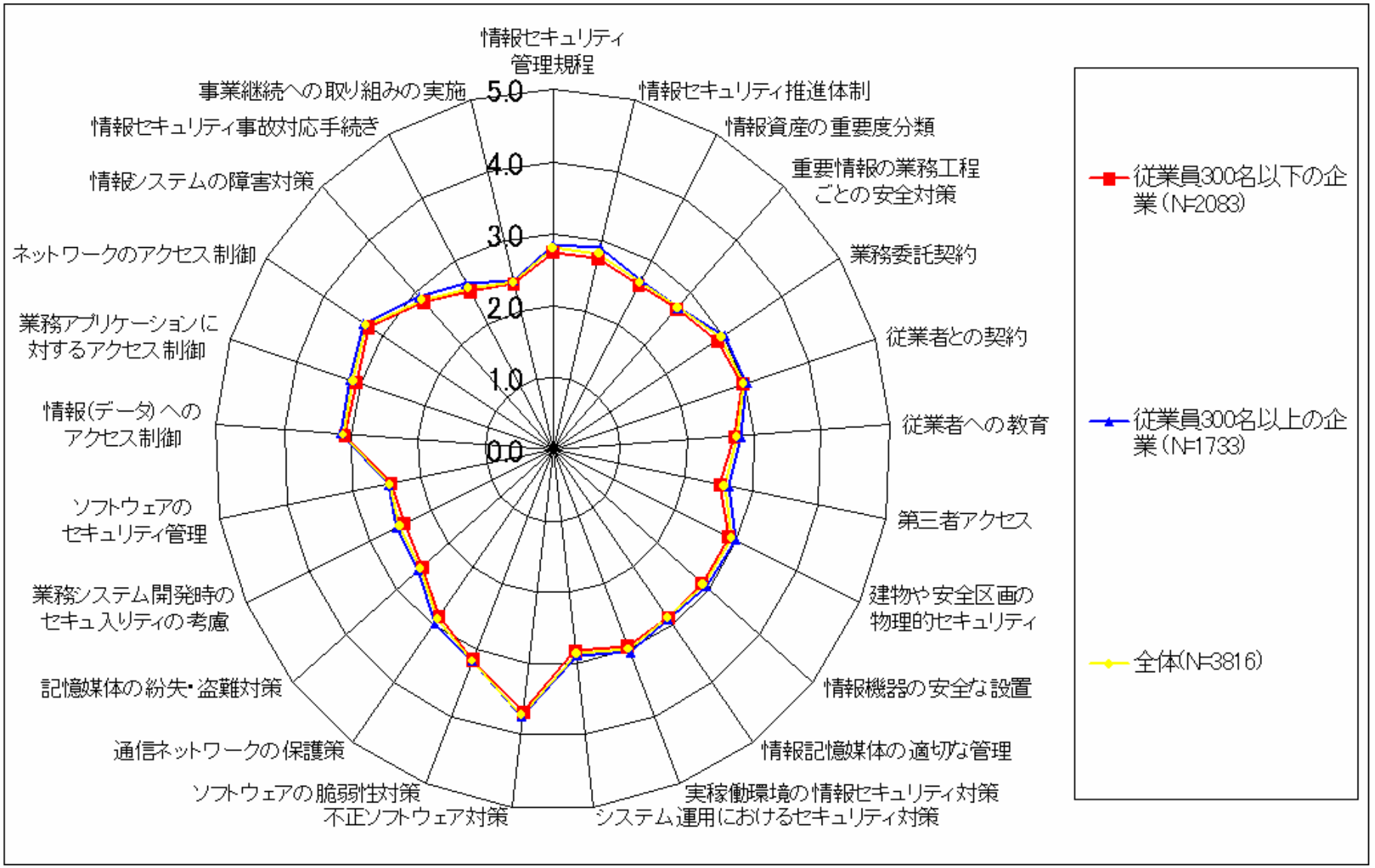
- 高水準のセキュリティレベルが要求される層
- 相応のセキュリティレベルが望まれる層
- 情報セキュリティ対策が喫緊の課題でない層

平均点
70.2

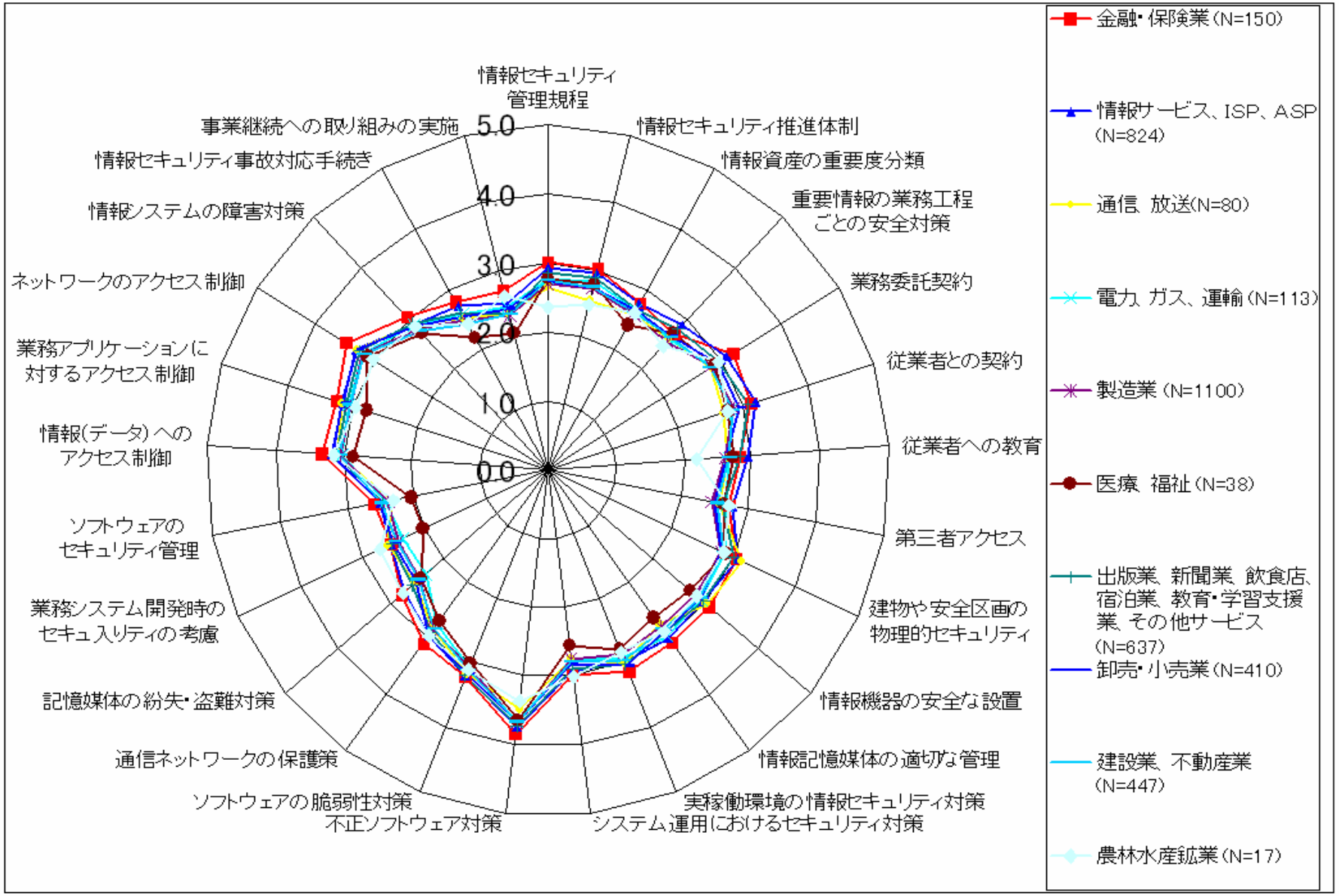
情報セキュリティ対策ベンチマーク
重要インフラ関連／その他の平均



情報セキュリティ対策ベンチマーク
企業規模別の平均



情報セキュリティ対策ベンチマーク
業種別平均



セキュリティ評価の目的と活用

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

セキュリティ評価の活用例

- **セキュリティ対策取り組み状況の外部への説明資料に活用**

  ※　ベンチマークでは、評価結果の表示がHTML方式とPDFの両方で表示されるため、PDF版を印刷してそのまま提出も可

- **外部委託をする際の評価指標のひとつとして活用**

  「政府機関の情報セキュリティ対策のための統一基準」（解説書p.115）

  (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。

  解説：(前略) 評価方法の整備には、**ISO/IEC 17799 等に基づく認証制度**の活用や、国際規格を踏まえ、**情報セキュリティガバナンスの確立促進のために開発されたセルフチェックベースのツール**等の応用が考えられる。

情報セキュリティ対策ベンチマークシステム

ISMS適合性評価制度

政府機関統一基準　http://www.nisc.go.jp/active/general/kijun01.html

（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
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
外部委託における情報セキュリティ対策実施規程　雛形

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**

(2) 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。
(5) 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 」より

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

●準拠する評価基準: 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

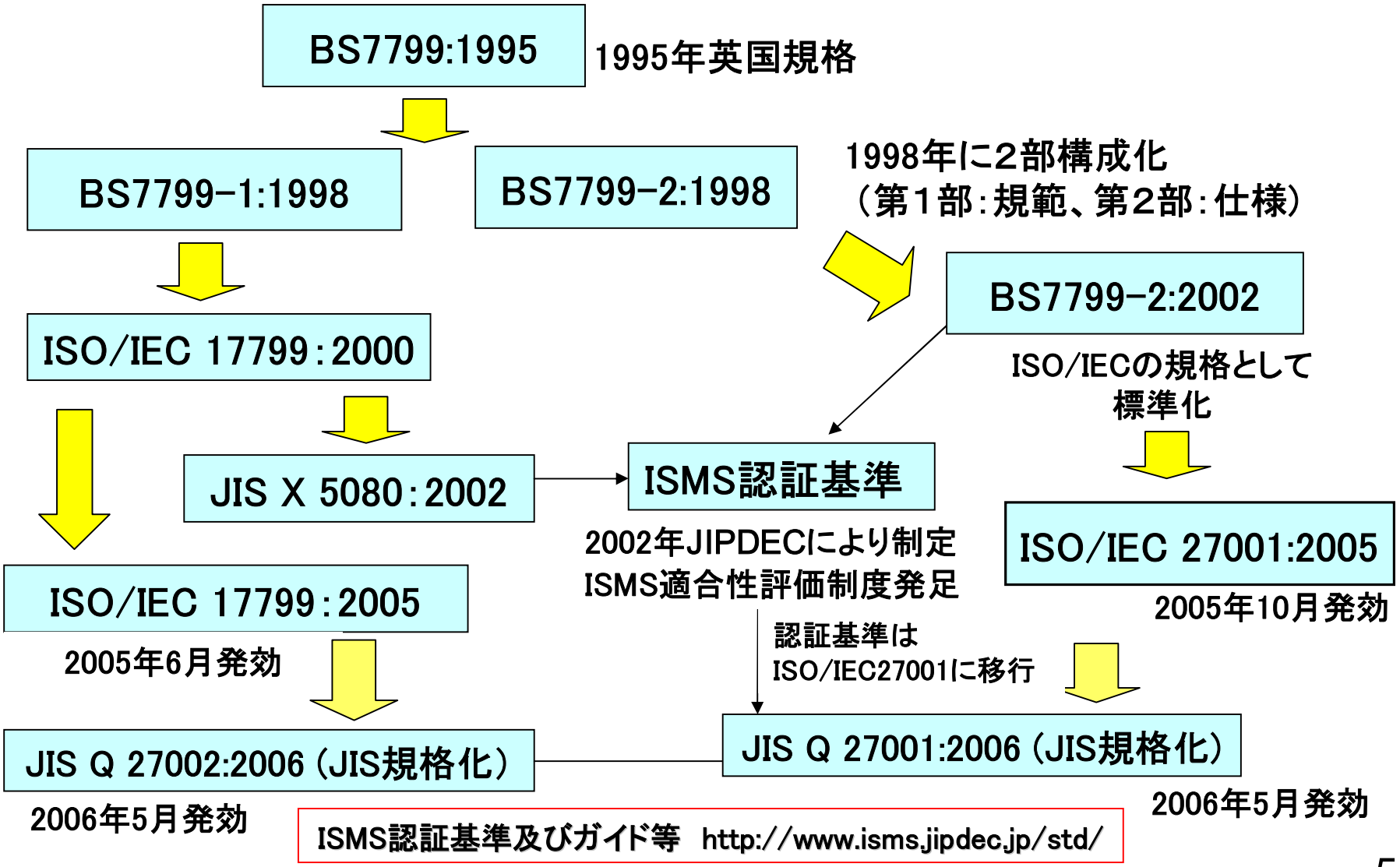
付属書A　管理目的及び管理策

個々の管理策は合理的理由があれば適用除外可能

●(財)日本情報処理開発協会(JIPDEC)により運用
様々なガイドブックがJIPDECのホームページよりダウンロード可能
(http://www.isms.jipdec.jp/std/index.html)

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

■（参考）情報セキュリティマネジメントの規格



ISO/IEC 27000ファミリ

- ISO/IEC 27000 Principles and vocabulary
- ISO/IEC 27001 ISMS Requirements
  - ISMS認証のための要求事項
- ISO/IEC 27002 (ISO/IEC17799:2005が名称変更し2007年成立予定)
  - ISMSベストプラクティス集(管理策集)
- ISO/IEC 27003 ISMS Implementation guidelines
  - ISMS導入のガイドライン
- ISO/IEC 27004 ISM Measurements
  - ISMの測定方法
- ISO/IEC 27005 Information Security Risk Management
  - リスクマネジメントのためのガイドライン
- ISO/IEC 27006 Requirements for bodies providing audit and certification of information security management systems
  - ISMSの審査及び認証機関に対する要求事項

（参考）JIS Q 27001:2006とJIS Q 27002:2006

JIS Q 27002:2006
(ISO/IEC 17799:2005)

（情報セキュリティマネジメントの実践のための規範）

管理領域(箇条)	カテゴリ	管理策
5. 情報セキュリティ基本方針	1	2
6. 情報セキュリティのための組織	2	11
7. 資産の管理	2	5
8. 人的資源のセキュリティ	3	9
9. 物理的及び環境的セキュリティ	2	13
10. 通信及び運用管理	10	32
11. アクセス制御	7	25
12. 情報システムの取得、開発及び保守	6	16
13. 情報セキュリティインシデントの管理	2	5
14. 事業継続管理	1	5
15. 順守	3	10
合計	39	133

JIS Q 27001:2006
(ISO/IEC 27001:2005)

0.1 序文
0.2 ISMSの採用
（ISMSに適用されるPDCAモデル）
1. 適用範囲
2. 引用規格
3. 用語及び定義

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

付属書A(規定）
管理目的及び管理策

※上記の日本語表現は暫定的な仮訳

登録証と適用範囲定義書の確認

ISMSの適用範囲

事業・組織・所在地・資産・技術の特徴の見地から，ISMSの適用範囲及び境界を定義する。この定義には，適用範囲からの除外について，その詳細及びそれが正当である理由も含めるものとする.（JIS Q 27001:2006)

企業全体、1事業部、複数の部門などを適用範囲とすることが可能

委託先の選定にISMS 認証を活用する際には次の文書を確認

①登録証：認証を取得したことを証する登録証

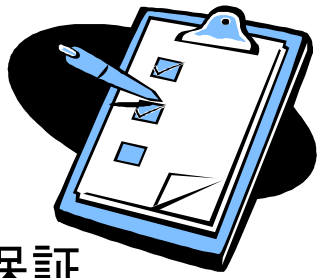
②適用範囲を定義した文書（適用範囲定義書）：
　どのような範囲（組織、部門、業務、プロセス、サービス等）で
　認証を取得したかを定義した文書

③適用宣言書：どのような管理策を実施しているかを宣言している文書

外部委託におけるISMS適合性評価制度の活用方法
http://www.isms.jipdec.jp/doc/JIP-ISMS117-10.pdf

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:外部監査人の選定

- 経済産業省の情報セキュリティ監査企業台帳
  - 情報セキュリティ監査を行うことを自ら宣言し証明する企業・組織を登録
  - 情報セキュリティ監査企業概要、情報セキュリティ監査実施の実績
  - 情報セキュリティ監査従事者の概要(氏名、情報セキュリティ監査

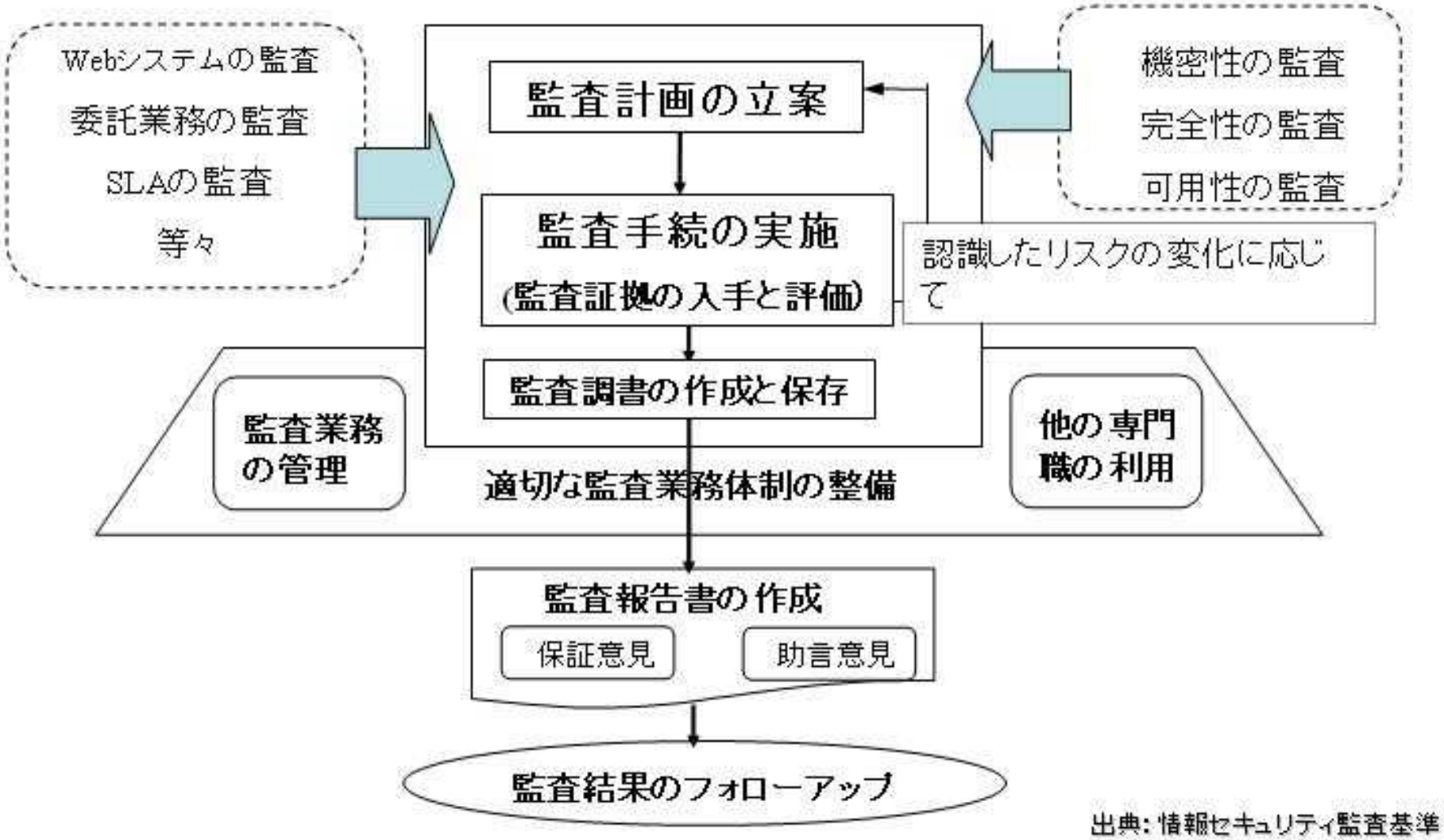
  URL: http://www.meti.go.jp/policy/netsecurity/is-kansa/

- JASAの公認情報セキュリティ監査人資格制度

  JASA(特定非営利活動法人日本セキュリティ監査協会)
  - 情報セキュリティ監査ガイドの整備や公認情報セキュリティ監査人資格制度、審査委員会制度などの取り組みを行っている。
  - 公認情報セキュリティ主任監査人、公認情報セキュリティ監査人、情報セキュリティ監査人補、情報セキュリティ監査アソシエイト
  - 資格登録者名簿は、JASAのホームページ上で閲覧可能

  URL: http://www.jasa.jp/cais/

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

（参考）JIS X 5080 (ISO/IEC 17799:2000)と情報セキュリティ管理基準との対比表

情報セキュリティ監査制度(経済産業省)　情報セキュリティ管理基準【Excel形式】
http://www.meti.go.jp/policy/netsecurity/audit.htm

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
1.1	情報セキュリティ基本方針	情報セキュリティのための経営陣の指針及び支持を規定するため	1) 基本方針文書は、経営者によって承認され、適当な手段で、全従業員に公表し、通知すること	1) 基本方針文書には、経営陣の責任を明記すること	3.1.1
				2) 基本方針文書には、情報セキュリティの管理に対する組織の取組み方法を明示すること	3.1.1
				3) 基本方針文書には、情報セキュリティの定義を含めること	3.1.1
				4) 基本方針文書には、その目的を含めること	3.1.1
				5) 基本方針文書には、適用範囲を含めること	3.1.1
				6) 基本方針文書には、情報共有を可能にするための機構としてのセキュリティの重要性を含めること	3.1.1
				7) 基本方針文書には、情報セキュリティの目標を支持する経営陣の意向声明書を含めること	3.1.1
				8) 基本方針文書には、原則を支持する経営陣の意向声明書を含めること	3.1.1

JIS Q 27002:2006の発効に伴い
情報セキュリティ管理基準の見直しが
行われています

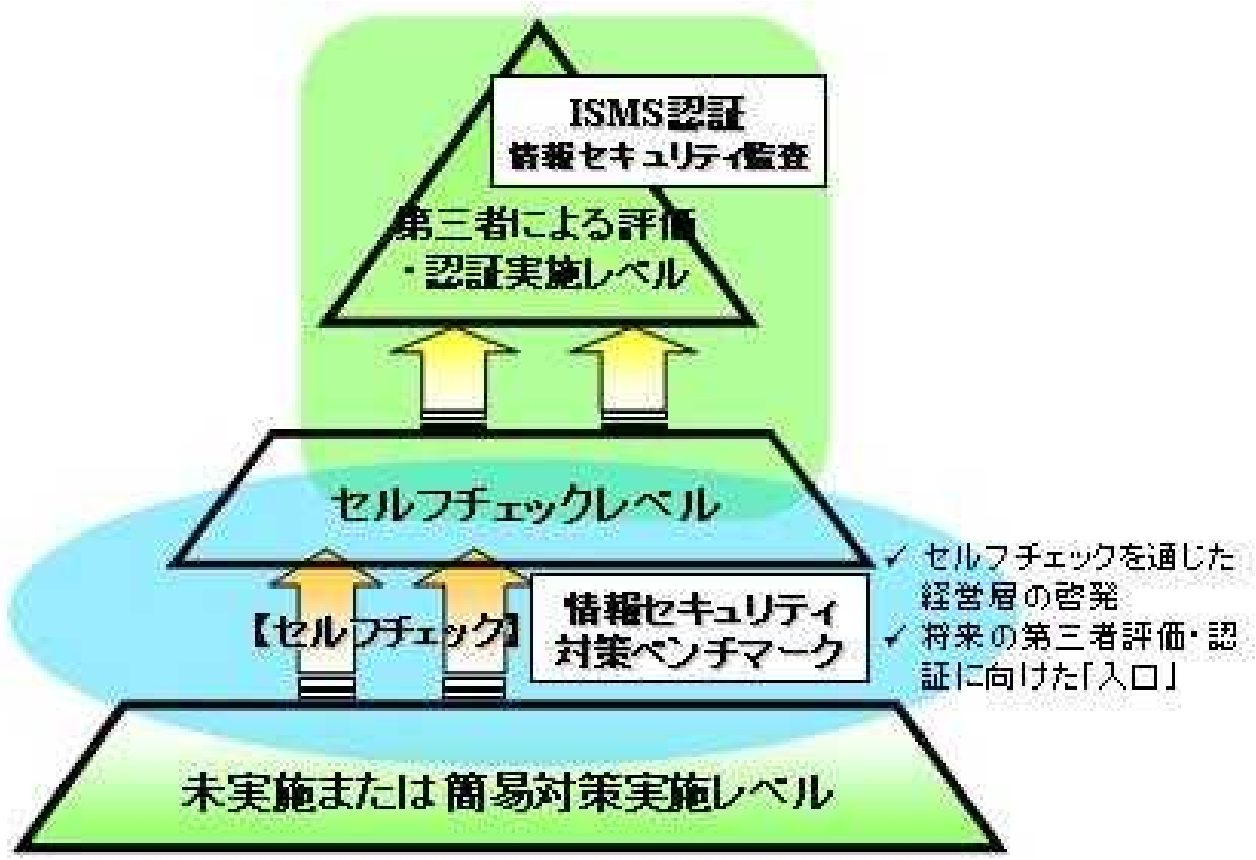
ISMS適合性評価制度と情報セキュリティ監査

- ISMS適合性評価制度
  - JIS Q 27001:2006の要求事項への適合を評価
  - 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
  - 監査目的は、監査依頼者の要求に応じて設定
  - 状況に応じ「個別管理基準」を利用することが可能
    （個別管理基準（監査項目）策定ガイドラインVer1.0）
  - 監査目的と監査対象により、組織の情報セキュリティマネジメントシステムの監査、技術的対策の監査など様々な監査がある
  - 助言型監査：監査対象の組織と監査人の2者関係
  - 保証型監査：監査報告書を活用する第3者の存在

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

情報セキュリティ対策ベンチマークと ISMS認証等との関係

情報セキュリティ対策ベンチマークは
第三者評価・ISMS認証の実施への「入口」の役割を担う



経済産業省の資料を基に作成：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

情報セキュリティ対策ベンチマーク：活用方法

PDCAサイクルの各段階での活用が可能

・Plan(計画)段階での活用- 不足な取り組みをチェック
・**ベンチマークを繰り返し活用**することで、徐々にレベルを上げていけるためDo(実行) - Check(点検)での活用は特に効果的
・セルフチェック後の改善活動はAct (処置)にあたる
・対策の取組み状況25項目は、ISMS認証基準Ver.2.0 の詳細管理策をベースに作成。ISMS認証取得の準備段階としての活用も可能
・セキュリティ対策取り組み状況の外部への説明に活用

状況に応じたカスタマイズ

対策の取組み状況25項目と対策のポイントの活用
JIS Q 27002 の管理策、実施の手引き、関連情報の参照
情報セキュリティ管理基準のサブコントロールの参照
必要に応じ、脆弱性検査などと併用

対策の取り組み状況25項目はJIS Q 27001:2006対応となるよう現在検討中

情報セキュリティ対策ベンチマーク
今後の展開

JIS Q 27001:2006 (ISO/IEC 27001:2005) 対応など

- 25項目の質問の見直し
- 対策のポイントの見直し
- 解説や回答項目（5段階の成熟度）の見直し
- 表示結果について
  （業種別の望まれる水準の表示など）
- その他

新しい動き

- 英語版の作成と公開（作成進行中・近日公開予定）
- その他

情報セキュリティ教本（2007年4月刊行予定）

【目次】
第1章　はじめに
第2章　情報セキュリティの組織
第3章　情報セキュリティポリシーのつくり方
第4章　情報の分類と管理
第5章　リスクマネジメント
第6章　技術的対策の基本
第7章　セキュリティ製品とセキュリティサービス
第8章　導入と運用
第9章　セキュリティ監視と侵入検知
第10章 セキュリティ評価
第11章 見直しと改善
第12章 法令遵守

【付録】
政府機関統一基準の構成と本書の関係
URL集

1　セキュリティ評価とは

1.1 セキュリティ評価の目的
1.2 誰が誰を評価する？

2　情報セキュリティ対策
　　実施状況の評価
2.1 自己点検
2.2 情報セキュリティ対策ベンチマーク
2.3 情報セキュリティ監査
2.4 ISMS適合性評価制度

3　製品調達における
　　セキュリティ評価の活用
3.1 ITセキュリティ評価及び認証制度
3.2 暗号モジュール試験及び認証制度

4　適合性評価
4.1 適合性評価制度の概要

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/