IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

情報セキュリティ対策ベンチマーク 構成、役割、利用傾向、意義について

2006年3月2日

独立行政法人　情報処理推進機構
研究員　菅野　泰子

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

本日の内容

1. IPAとIPAセキュリティセンターの紹介
2. 情報セキュリティ対策ベンチマーク：構成と役割
   1) 背景
   2) 構成と役割
      概要、評価項目と対策ポイント、
      成熟度の構成、企業分類と望まれる水準
3. 情報セキュリティ対策ベンチマーク：利用傾向等
   1) 利用傾向
   2) 新バージョンの改善点
4. セキュリティ評価における自己評価の意義
   1) 様々なセキュリティ評価
   2) 自己評価（セルフアセスメント）に関するガイドライン
   3) 海外の自己評価ツールの紹介

IPA の概要

独立行政法人　情報処理推進機構（IPA）

情報処理促進に関する法律（昭和45年5月22日法律第90号)に基づき1970 年10月に設立された「情報処理振興事業協会」を前身として、同法の一部改正（平成14年12月11日法律第144号）により、2004年1月5日　「独立行政法人　情報処理推進機構」　として発足

国家情報戦略をソフト面から担う総合的な情報化政策を推進

■ソフトウエア開発
- ✧ 次世代ソフトウエア開発事業
- ✧ 中小ITベンチャー支援/ 債務保証 等

■オープンソースソフトウエア・センター
- ✧ ｵｰﾌﾟﾝｿﾌﾄｳｪｱ活用基盤整備事業
- ✧ OSSに関する情報の集約と発信 等

■ ｿﾌﾄｳｴｱ・ｴﾝｼﾞﾆｱﾘﾝｸﾞ・ｾﾝﾀｰ
- ✧ ソフトウエア産業の国際競争力強化
- ✧ 海外の有力機関との連携

■セキュリティセンター
【情報セキュリティ対策】
- ✧脆弱性対策、ウイルス・不正アクセス対策
- ✧セキュリティ評価認証、暗号技術、調査研究

■ 情報化人材の発掘・育成
- ✧ ITスキル標準
- ✧情報処理技術者試験
- ✧未踏ソフトウエア創造事業
- ✧地域の人材育成支援

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

本日の内容

1. IPAとIPAセキュリティセンターの紹介

2. ***情報セキュリティ対策ベンチマーク：構成と役割***
   - ***1) 背景***
   - ***2) 構成と役割***
     概要、評価項目と対策ポイント、
     成熟度の構成、企業分類と望まれる水準

3. 情報セキュリティ対策ベンチマーク：利用傾向等
   - 1) 利用傾向
   - 2) 新バージョンの改善点

4. セキュリティ評価における自己評価の意義
   - 1) 様々なセキュリティ評価
   - 2) 自己評価（セルフアセスメント）に関するガイドライン
   - 3) 海外の自己評価ツールの紹介

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
    自己評価用ツール
  - 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**

背景：ベンチマークとは？

一般に、計測の基準となる指標のこと

IPA

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
コンピュータのハードやソフトの性能比較に使われる指標をベンチマークとも言う

情報セキュリティ対策ベンチマーク

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
IPAのWeb上で、Webベースのセルフチェックサービスを公開
各評価項目の質問に答えると、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

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

自社が望ましい水準とどの程度のギャップがあり、どこまで対策すれば良いか示されないと、実際の行動には結びつきにくい

→ **情報セキュリティ対策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【セルフチェックシステム】の公開

第1部：情報セキュリティ対策状況に関する設問　25問
第2部：事業内容に関する設問　15問

設問のサンプル

- ✓ 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。
- ✓ 導入しているソフトウェアに対して適切な脆弱性対策を実施していますか。
- ✓ 主要な業務に関わるプロセスのうち、インターネットに依存している割合はどの程度ですか。

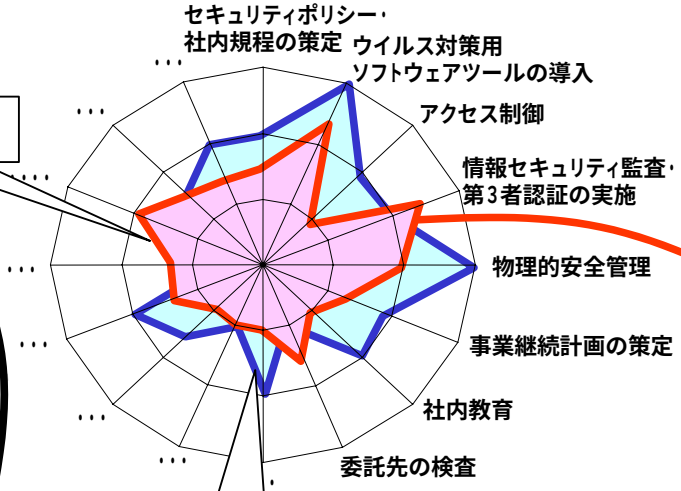
情報セキュリティ対策ベンチマークシステム
http://www.ipa.go.jp/security/benchmark/

情報セキュリティ対策ベンチマーク

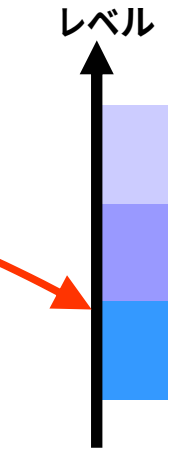
システムの概要

Webで回答

回答企業の水準



望まれる水準



トータルスコアと
推奨される取組みを提示

Level up!!

推奨される
取組み

評価項目（全40項目）

セキュリティ対策（25項目）
- 組織的な取組み
- 物理的（環境的）施策
- 通信・システムの運用管理
- 開発・保守、アクセス制御
- 事故対応状況

企業プロフィール（15項目）
- 事業構造上の脆弱性
- 社会的影響力

企業のタイプに応じて
望まれる水準を設定

高水準のセキュリティ対策が要求される層

相応の水準のセキュリティ対策が要求される層

セキュリティ対策が喫緊の課題ではない層

プロフィールから企業をタイプに分類

望まれる水準（高）

望まれる水準（中）

望まれる水準（低）

・望まれる水準
・推奨される取組み

アンケート
結果

アンケート結果をもとに
望まれる水準や
推奨される取組みを設定

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状況　評価項目

IPA

評価項目の策定

ISMS認証基準Ver.2.0の詳細管理策をベース
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る

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)
(b) 物理的 (環境的) セキュリティ上の施策 (5項)
(c) 通信ネットワーク及び情報システムの運用管理 (5項)
(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)
(e) 情報セキュリティ上の事故対応状況 (3項)

(参考) ISMSに関する標準化動向と認証基準

2006.3.1 現在

BS7799:1995 1995年英国規格

BS7799-1:1998

BS7799-2:1998

1998年に2部構成化
(第1部：規範、第2部：仕様)

BS7799-2:2002

ISO/IEC 17799：2000

ISO/IECの規格として
標準化

JIS X 5080：2002

ISMS認証基準

2002年JIPDECにより制定
ISMS適合性評価制度発足
V2.0 付属書「詳細管理策」
はJIS X 5080:2002 を参照

ISO/IEC 27001:2005

2005年10月発効

ISO/IEC 17799：2005

2005年6月発効

JIS Q 27001 としてJIS規格化

JIS Q 27002 としてJIS規格化

ISMS認証基準及びガイド等
http://www.isms.jipdec.jp/std/

(参考) ISO/IEC 17799:2000 vs ISO/IEC 17799:2005

IPA

【127の管理策】

ISO/IEC 17799:2000 →JIS X 5080

Security policy セキュリティ基本方針	(2)
Security organization 組織のセキュリティ	(10)
Asset classification & control 資産の分類及び管理	(3)
Personnel security 人的セキュリティ	(10)
Physical & environmental security 物理的及び環境的セキュリティ	(13)
Communications & operations management 通信及び運用の管理	(24)
Access control アクセス制御	(31)
Systems development & maintenance システムの開発及び保守	(18)
Business continuity management 事業継続管理	(5)
Compliance 適合性	(11)

【133の管理策】

ISO/IEC 17799:2005 →JIS Q 27002

Security policy (仮訳) セキュリティ基本方針	(2)
Organizing information security (仮訳) 情報セキュリティのための組織	(11)
Asset management (仮訳) 資産の管理	(5)
Human resources security (仮訳) 人的資源のセキュリティ	(9)
Physical & environmental security (仮訳) 物理的及び環境的セキュリティ	(13)
Communications & operations management (仮訳) 通信及び運用管理	(32)
Access control (仮訳) アクセス制御	(25)
Information systems acquisition, development and maintenance (仮訳) システムの取得、開発及び保守	(16)
Information security incident management (仮訳) 情報セキュリティインシデントの管理	(5)
Business continuity management (仮訳) 事業継続管理	(5)
Compliance (仮訳) 順守	(10)

※上記の日本語表現は暫定的な仮訳

(参考) JIS X 5080:2002と管理基準との対比表

http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex01_2.xls

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

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

IPA

(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。

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

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

評価項目に対する取組みの成熟度の構成

IPA

できていない

各評価項目に関する自社の取組みの「成熟度」

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

経営層向けに平易な言葉を使用し、ガバナンスの観点から見た対策の取組状況（成熟度）を評価の基準としている。

情報セキュリティ対策ベンチマーク

企業プロフィール

IPA

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

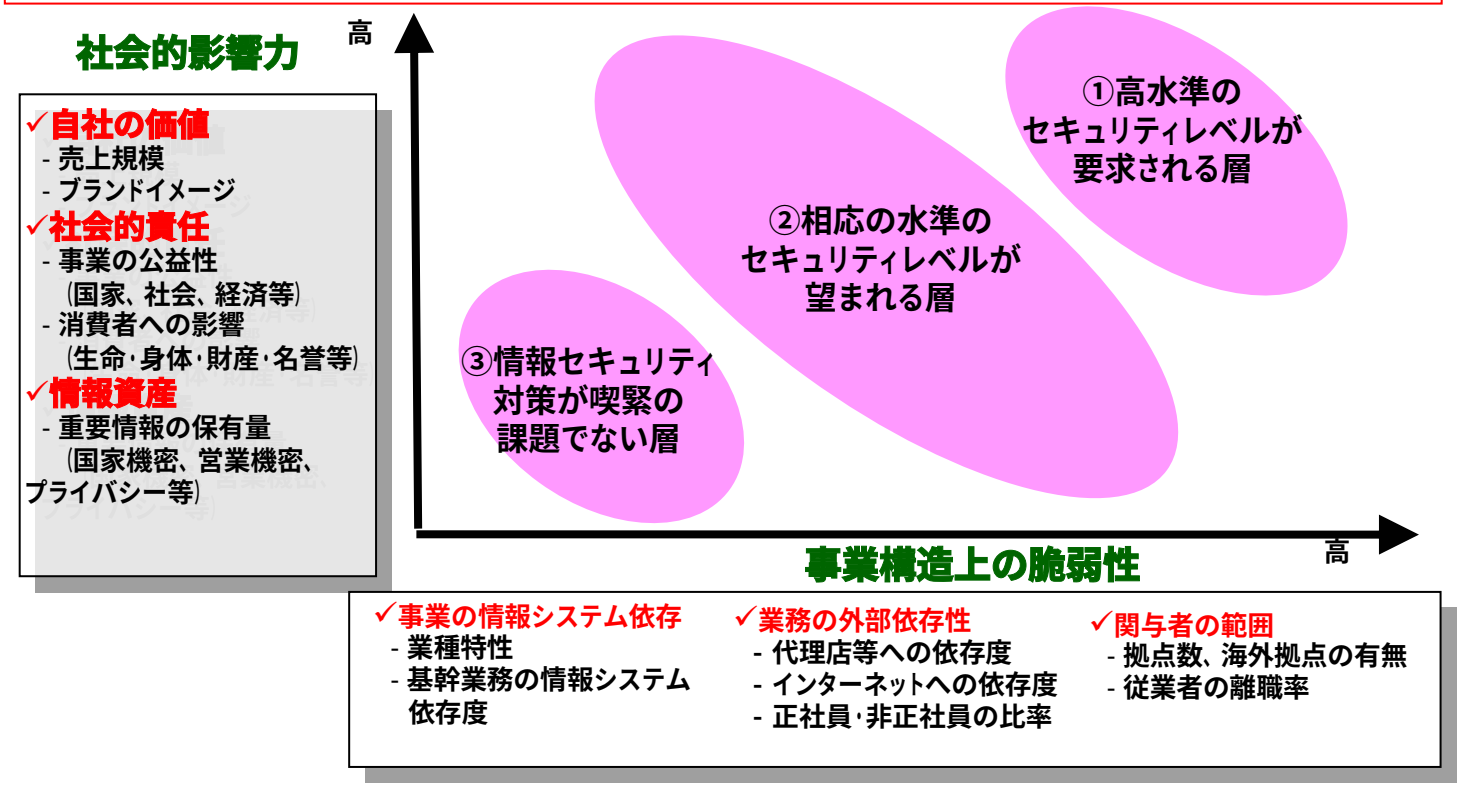
(a) 従業者数（派遣、アルバイトを含む）及びそのうちの正社員の割合
(b) 売上高、国内外の拠点数（支社・支店・営業所）
(c) 業種
(d) 国家や社会基盤、経済基盤に与える影響の観点から見た公益性
(e) 事業が、顧客の生命・身体・財産・名誉等に与える影響の大きさ
(f) 主要業務のうち、情報システム（社外のシステムを含む）に依存している割合
(g) 主要な業務に関わる業務プロセスのうち、インターネットに依存している割合
(h) 主要情報システムの、（月間）売上高に影響を及ぼさない許容停止時間
(i) 主要情報システムが営業日に24時間停止の場合、当該日売上高への影響
(j) 情報セキュ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

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

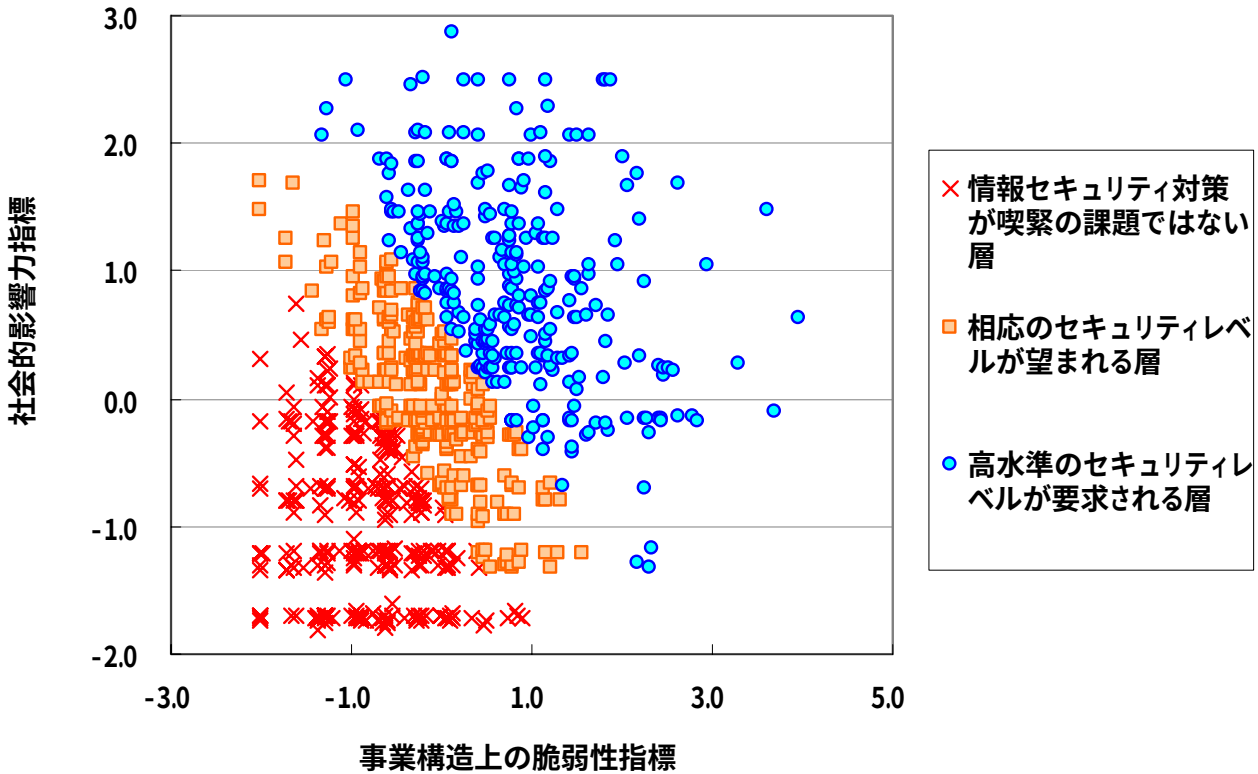
望まれる水準：回答企業の分類

事業構造上の脆弱性指標

= -0.0018×正社員割合+ 0.0710 x 総拠点数+ 0.5389× IT依存度 + 0.5326 x インターネット依存度+ 0.3588×ビジネスパートナーへの依存度 - 0.0302×年間離職率

社会的影響力指標

= 0.1331×売上高 + 0.2764×公益性 + 0.3082×顧客への影響 + 0.3044×ブランドへの影響 + 0.3214×機密情報の保有度 + 0.2212×保有個人情報数



アンケート回収企業1,633件中、全設問に回答の885件（大手企業474社、中小企業411社）を活用

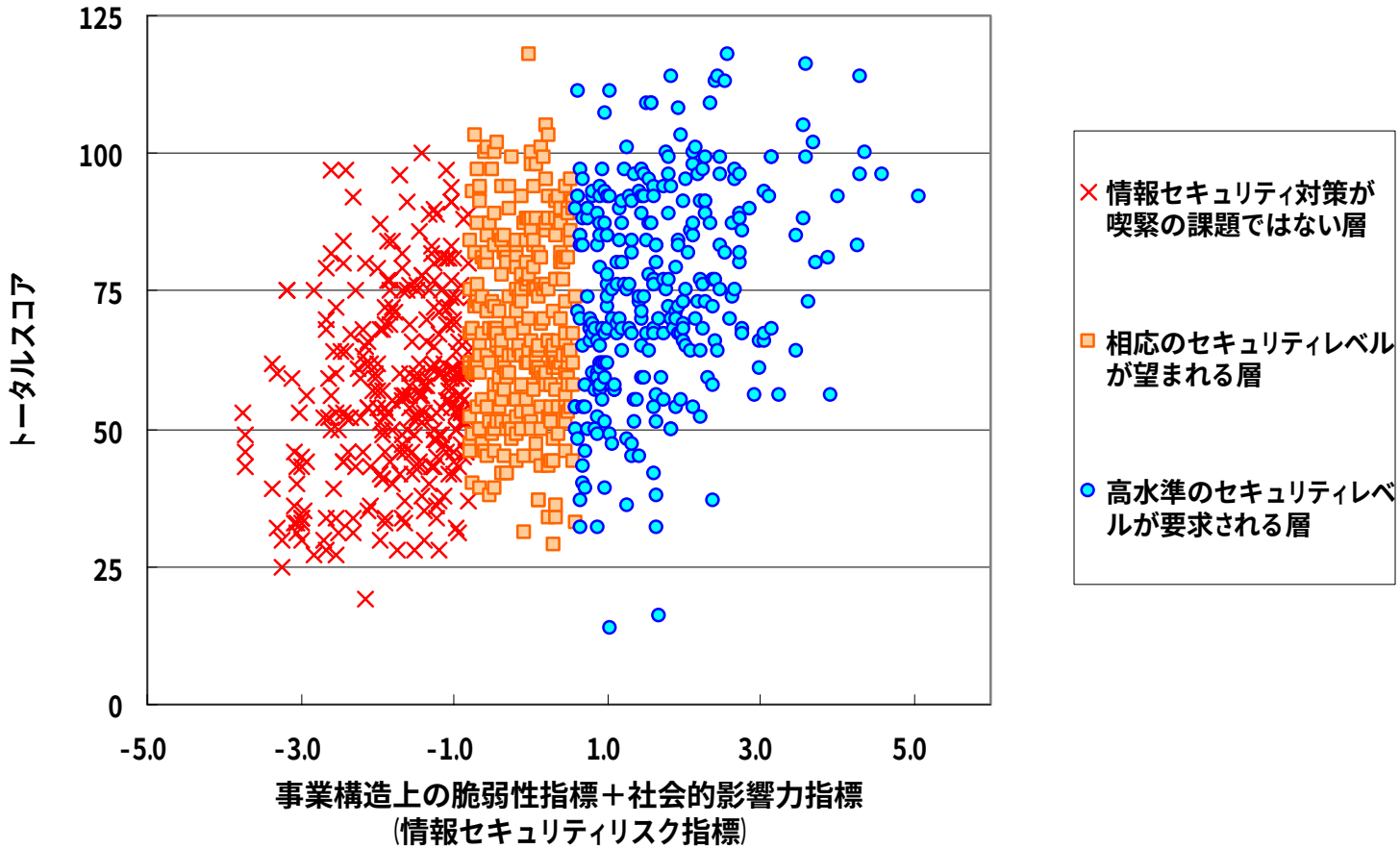
回答者数が均等になるよう、3つのグループに分類（各295社）

情報セキュリティ対策ベンチマーク

望まれる水準：トータルスコアの分布

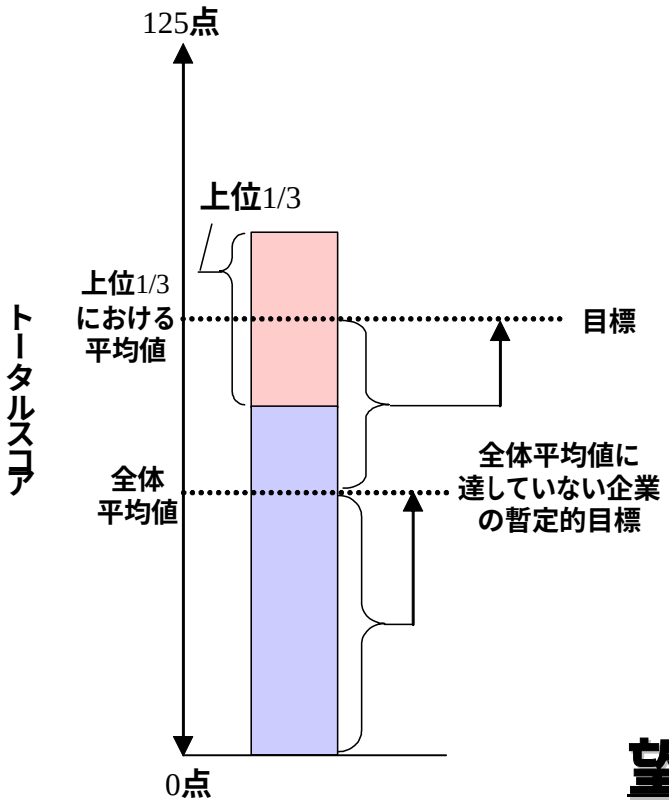
情報セキュリティリスク指標と対策取組状況トータルスコアの関係

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
トータルスコア＝評価項目全25項目 x 5 (5段階評価を点数に換算)、合計125点



望まれる水準値の決定

望まれる水準の設定



望まれる水準

- 各層の上位1/3の平均値を目標
- 各層における全体平均値に達していない企業は、各層における全体平均値を、早期達成すべき暫定的目標として設定

注：「望まれる水準」は、企業の業務内容・IT依存度の変化という内的要因だけではなく、社会全体のネットワーク化の更なる進展などの外的要因によっても変動していくものであることに留意。

望まれる水準の具体的な値

	全体	高水準のｾｷｭﾘﾃｨﾚﾍﾞﾙが要求される層	相応のｾｷｭﾘﾃｨﾚﾍﾞﾙが望まれる層	情報ｾｷｭﾘﾃｨ対策が喫緊の課題ではない層
上位1/3の平均値	88(3.5)	96(3.8)	87(3.5)	76(3.1)
全体平均値	67(2.7)	75(3.0)	68(2.7)	57(2.3)

注：( ) 内の数値は、企業における取組みの成熟度に換算したもの。

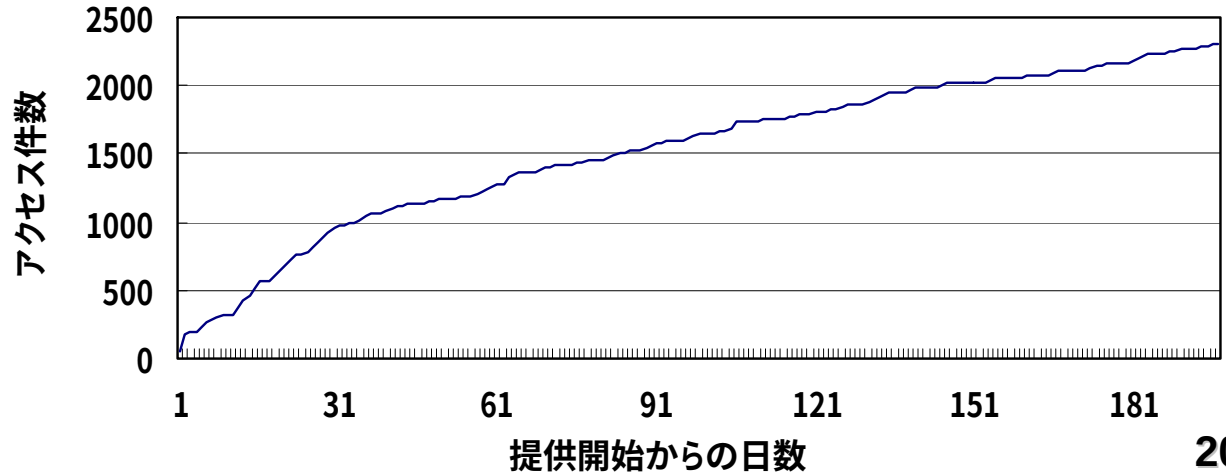
本日の内容

1. IPAとIPAセキュリティセンターの紹介
2. 情報セキュリティ対策ベンチマーク：構成と役割
   1) 背景
   2) 構成と役割
      概要、評価項目と対策ポイント、
      成熟度の構成、企業分類と望まれる水準
3. ***情報セキュリティ対策ベンチマーク：利用傾向等***
   1) 利用傾向
   2) 新バージョンの改善点
4. セキュリティ評価における自己評価の意義
   1) 様々なセキュリティ評価
   2) 自己評価（セルフアセスメント）に関するガイドライン
   3) 海外の自己評価ツールの紹介

情報セキュリティ対策ベンチマーク
利用状況

2005年8月4日公開以来約6ヶ月余りで2,300件を超えるアクセス

ベンチマーク利用件数推移



2006年2月17日現在

回答データ提供有り	回答データ提供無し	合計
451件 (19.6%)	1,855件 (80.4%)	2,306件

基礎データ： 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で
ベンチマークにより実際に自己採点した協力企業のデータ (885件)

IPA Webでの回答データ： ご協力のお願い ○提供する ○提供しない

ご提供の回答データは、本業務の作業担当者以外はアクセスできないよう管理し、本ツールでのみ使用

情報セキュリティ対策ベンチマーク: Q & Aより

Q: なぜ会社名、部署名、電話番号の入力が必要なのか？（なぜ必須？）

（注：会社名、部署名、電話番号は、「回答データを提供する」にチェックを付けた場合のみ必須項目）

A: いたずら目的のデータ送信防止の抑止効果を期待して、会社情報入力をお願いしています。

Q:「回答データを提供しない」にチェックした場合は、IPA殿ではデータは使用されず、IPA殿の誰も見られないのか？(試しに使いたい)。試しで使った結果は、電子データで入手でるか？

A: IPA担当者でも見ることはできません。診断結果はWEB上に表示されます。

Q: ベンチマークの質問を自社のE-mailで提供しお客さの回答を代理入力するのは可能か？

A: ベンチマークは診断を行いたい企業様が、当機構サイトにて、ご自身で入力し、
ご自身で診断結果を確認することを目的として公開致しています。

Q: 弊社は、47社ほどグループ会社を保有。入力を一括して、グループ内IT組織で行いたい。

A: 問題ありません。セキュリティ対策の参考にご活用下さい。

Q:「ガバナンスの・・報告書」を参考に業務方針等を作成した場合に著作権等侵害にあたるか?

A: 報告書を参考に、業務方針を策定するなどの利用は、著作権には触れないと思います。当該報告書を引用して外部に公開する資料を作成する等においては、出典元を明記するなどが必要になります。

Q: 製薬業界の他社事例を元に、自社がどの程度進んでいるか確認したいが可能か？

A: ベンチマークでは 9業種の業種別対策平均値を出していますが、製薬業界のみのデータはありません。

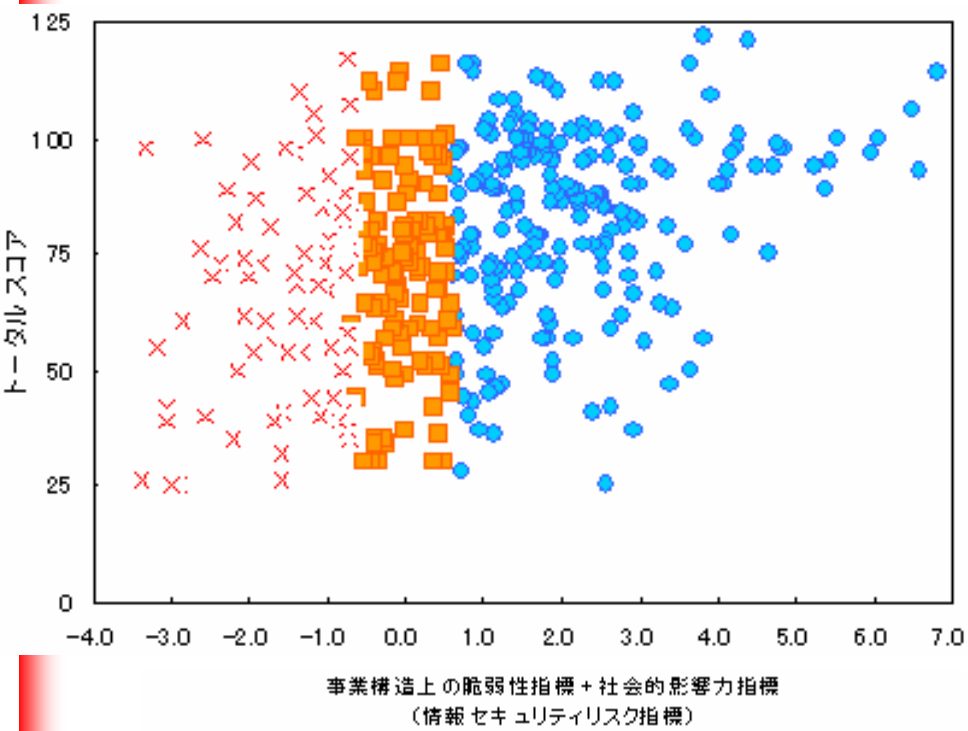
Q: 利用状況、利用傾向は？ 新バージョンのリリースは？ 改良のポイントは？

A: → **これからお話します。**

情報セキュリティ対策ベンチマーク

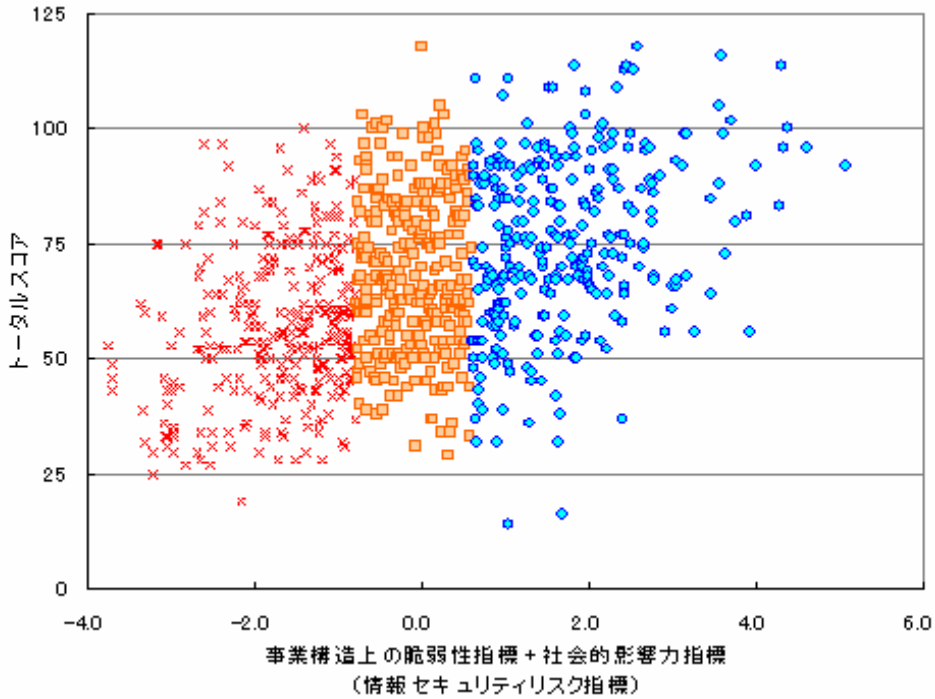
既存データ（報告書ベース）と新規データ（Web公開ベース）の比較

新規データ



回答データ提供　451件より

既存データ



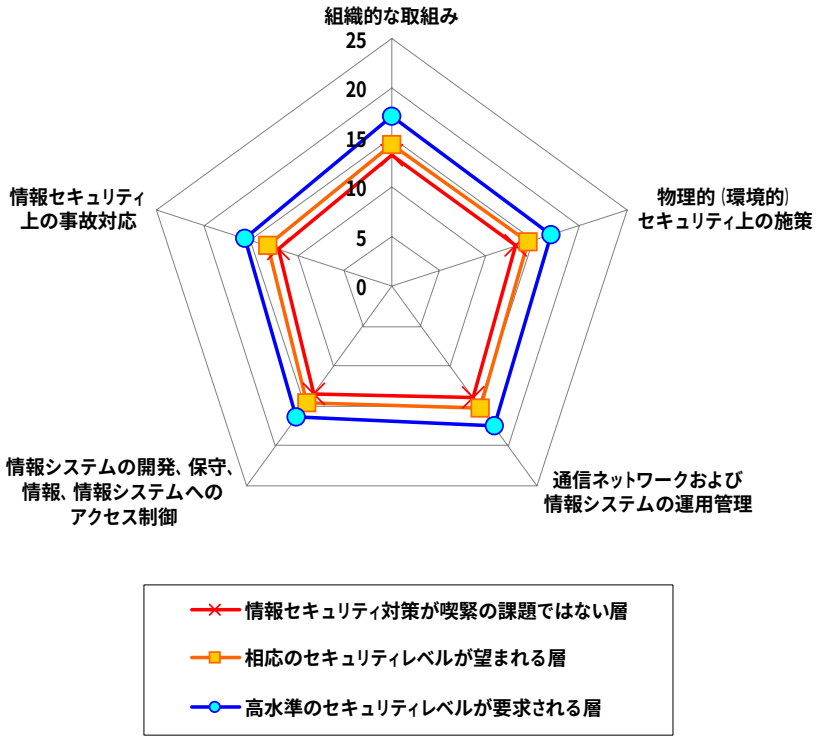
既存データ　885件より

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。

新規データは高い水準に分布が見られる。

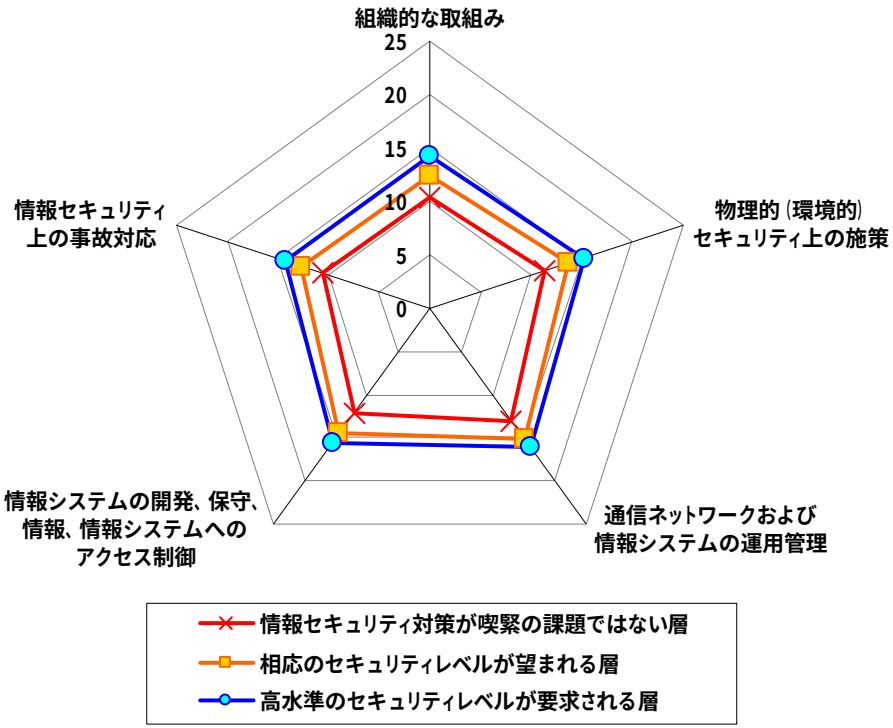
2006年2月17日現在

情報セキュリティ対策ベンチマーク
設問グループごとの回答層別平均



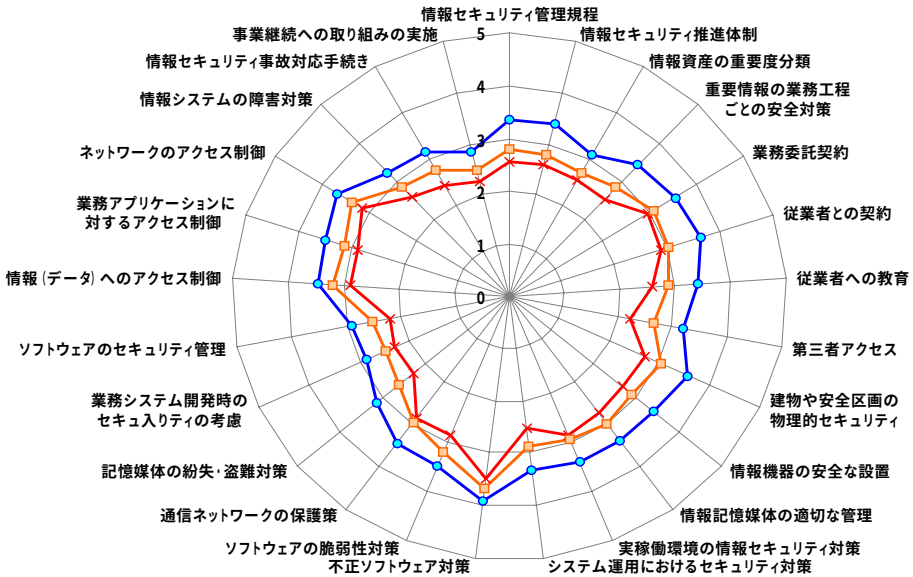
回答データ提供　451件より

既存データ　885件より



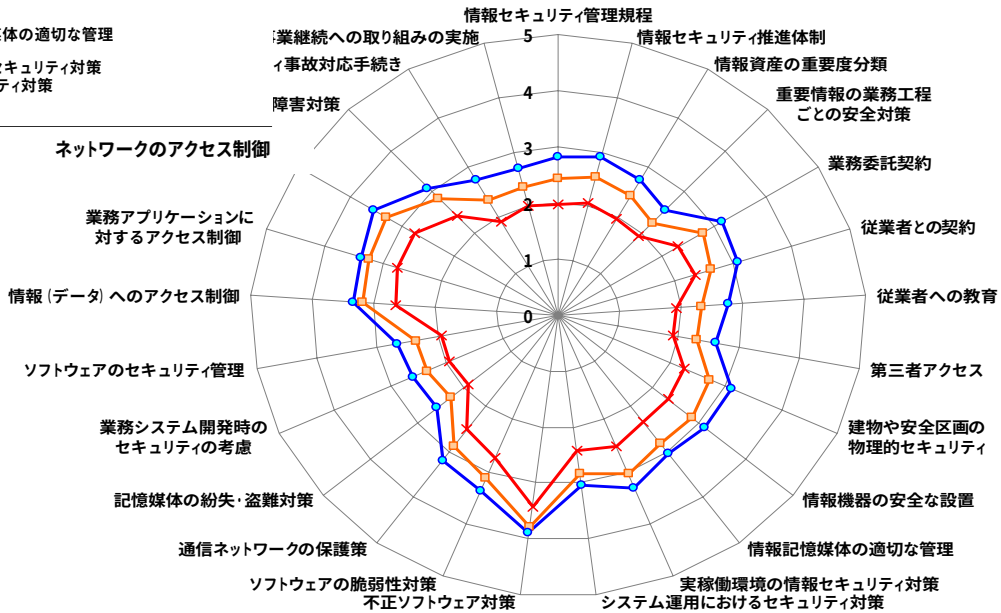
2006年2月17日現在

情報セキュリティ対策ベンチマーク
小問ごとの回答層別平均



既存データ　885件より

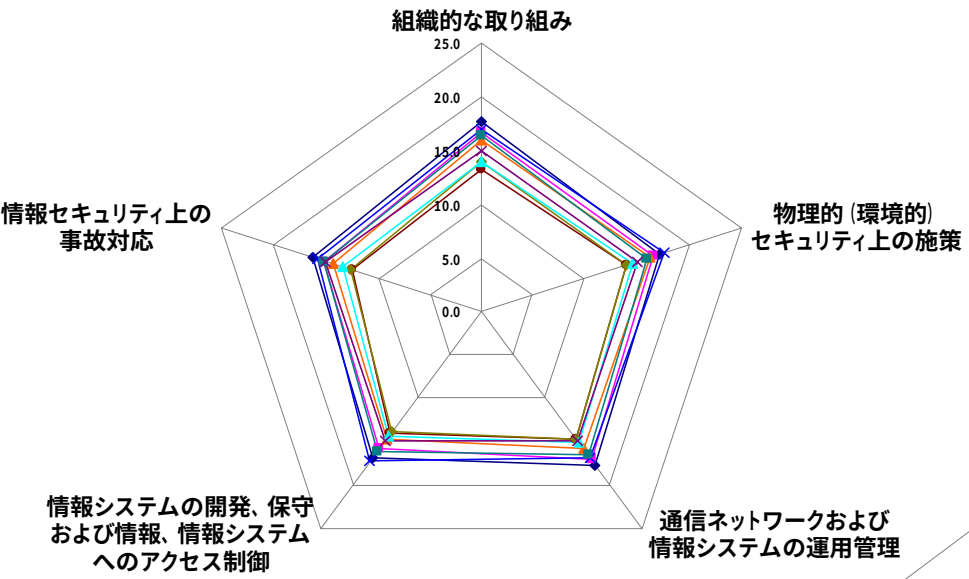
回答データ提供　451件より



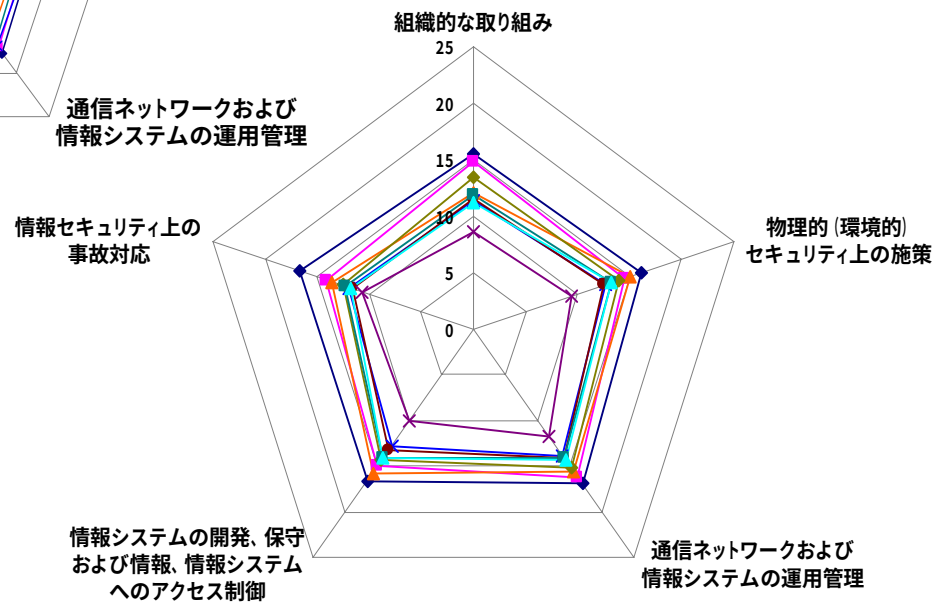
2006年2月17日現在

情報セキュリティ対策ベンチマーク
設問グループごとの業種別平均

回答データ提供　451件より



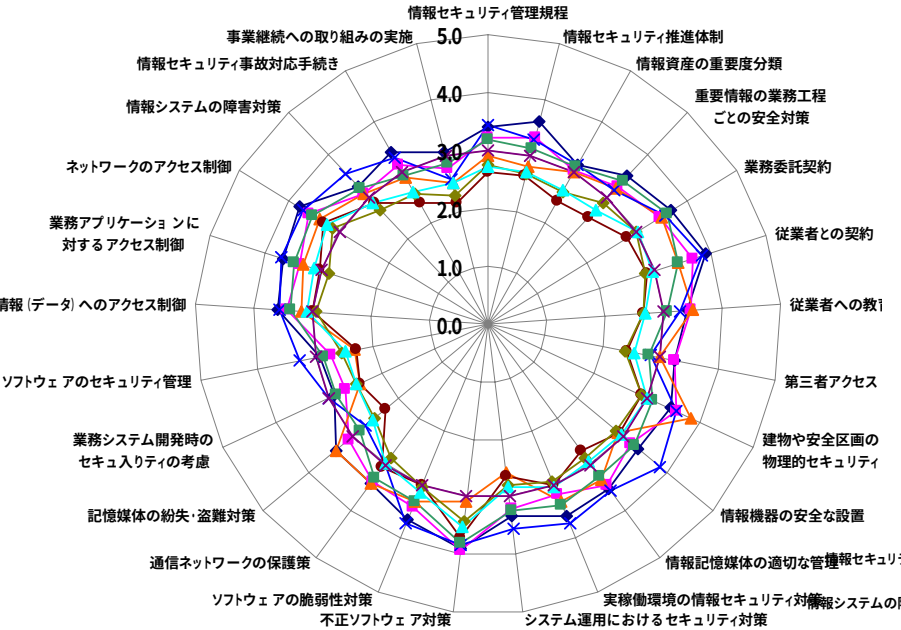
既存データ　885件より



2006年2月17日現在

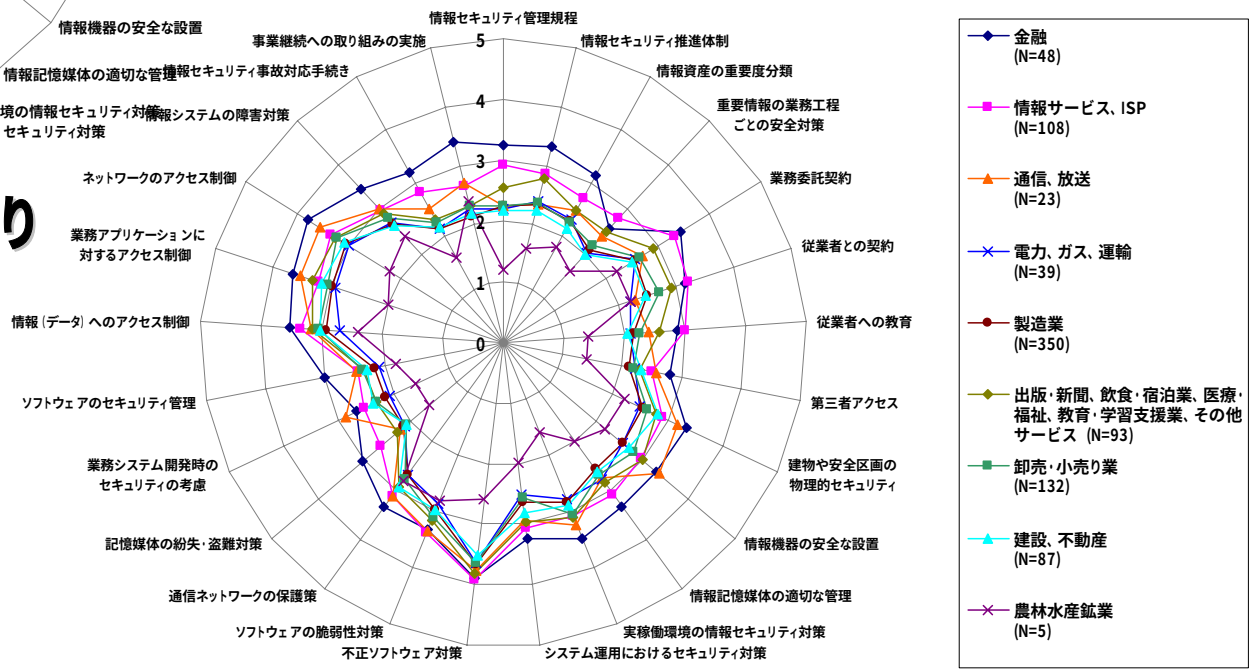
➢**金融業の水準が高レベルとなっている**

情報セキュリティ対策ベンチマーク
小問ごとの業種別平均



既存データ　885件より

回答データ提供　451件より



2006年2月17日現在

情報セキュリティ対策ベンチマーク 新バージョンの改善点（概要）

主な改善点

- インターフェースの改善
  → *利便性の向上*

- データベースの整備
  → *比較対象データの増加による診断精度の向上*

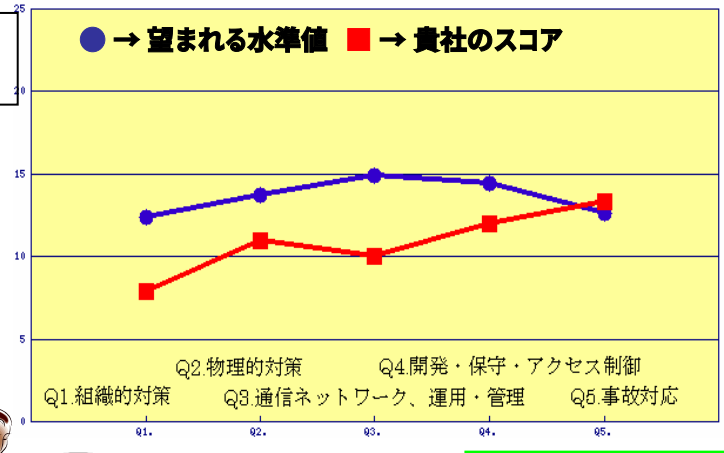
診断結果の活用方法

- セキュリティ対策取り組み状況の外部への説明資料
- 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）に掲載

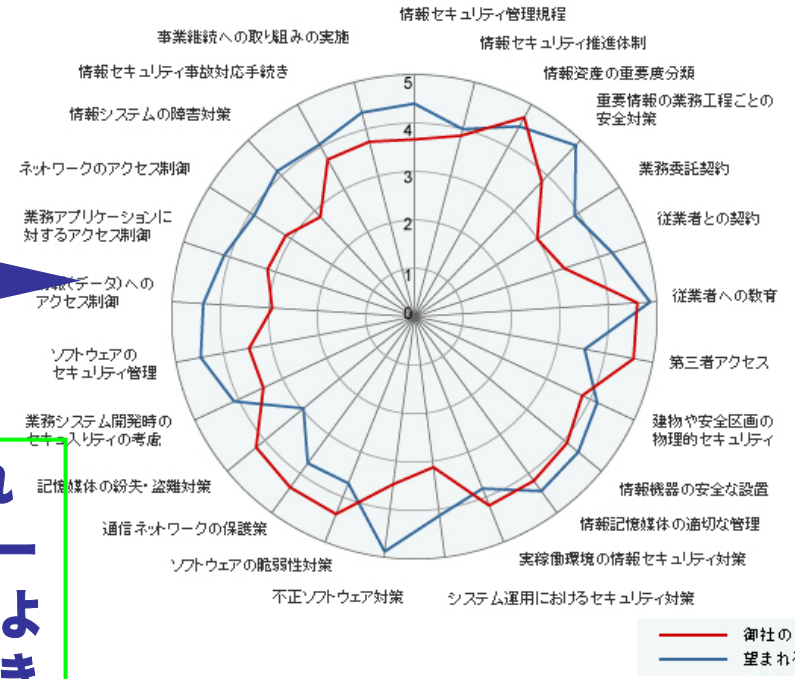
情報セキュリティ対策ベンチマーク 新バージョンの改善点 (1)

IPA

旧



新



Webで回答

評価項目 (全40項目)

セキュリティ対策 (25項目)
- 組織的な取り組み
- 物理的 (環境的) 施策
- 通信・システムの運用管理
- 開発・保守、アクセス制御
- 事故対応状況

企業プロフィール (15項目)
- 事業構造上の脆弱性
- 社会的影響力

1.各項目の望まれる水準値をレーダーチャートで表示し、より視覚的に認識できるよう改善。

企業のタイプに応じて望まれる水準を設定

利用者の回答データを蓄積

- 望まれる水準値の算出データ

2.データの絶対数を増加
望まれる水準値や統計データとしての正確性の向上、時間経過とともに推移していく水準の変化への対応を図る

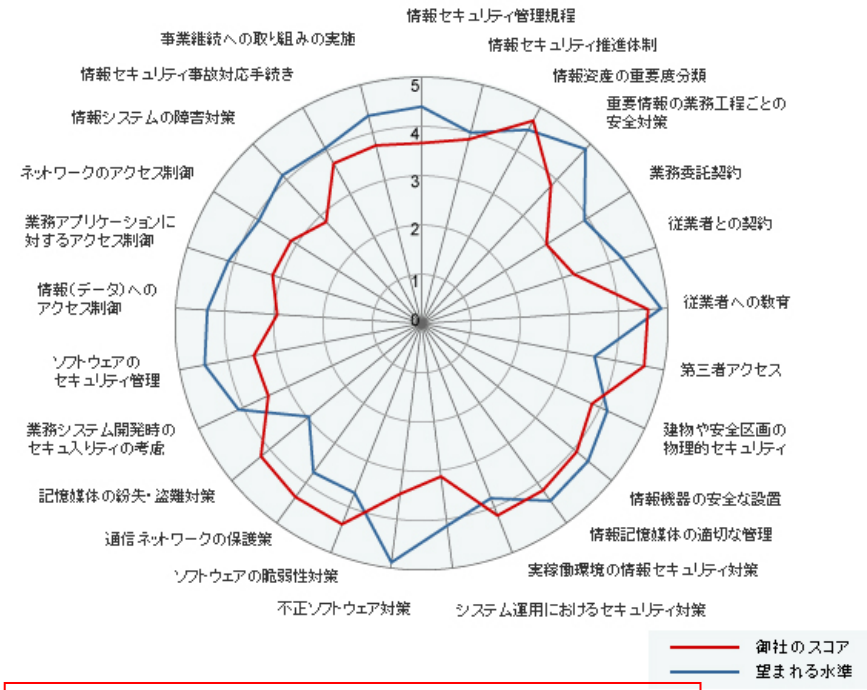
データベース (開発部分)

診断結果　サンプル：

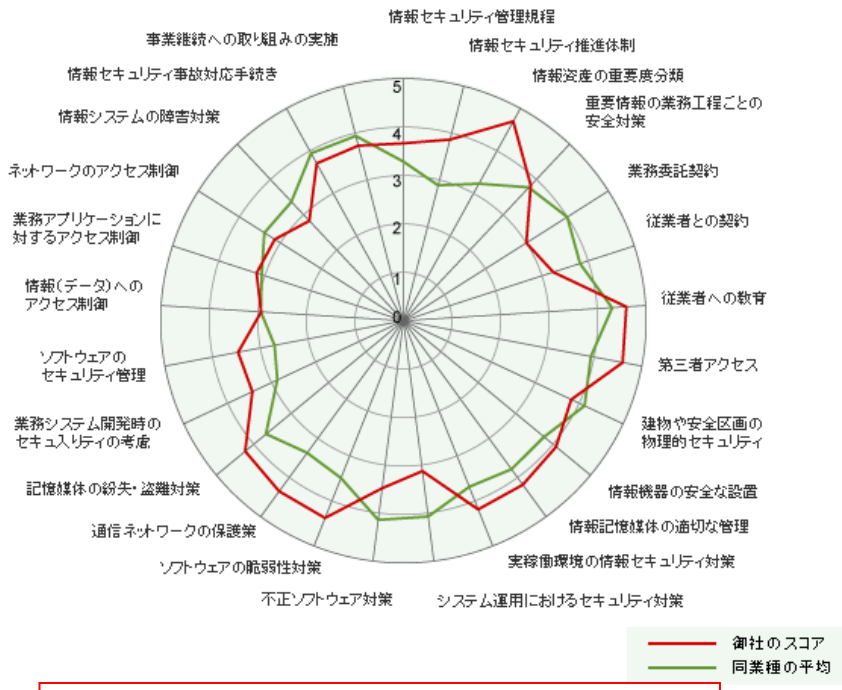
御社は、高水準のセキュリティレベルが要求される層（グループⅠ）に分類されます

グループⅠの中において御社のスコアは、上位41～50%以内 に位置付けられました。
（各グループを合わせた全体での位置付けは、上位31～40%以内 となっています。）

グループにおいて望まれる対策の水準と自社の現状



同業種の平均と自社の現状



御社のスコア
トータルスコア　　75点/125点
設問における平均値　3.0点/5点

同業種の平均
トータルスコア　　75点/125点
設問における平均値　3.0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　　96点/125点
設問における平均値　3.8点/5点（標本数 n=1235）

情報セキュリティ対策ベンチマーク 新バージョンの改善点 (2)

IPA

診断結果の活用方法

- 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
  ※ 評価結果の表示がHTML方式とPDFの両方での表示
  印刷して提出しやすい体裁に
- 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。**
- スコアの変化をチェック:希望者は、結果の履歴を参照できる
  希望者にID/パスワードを発行
  次回評価時に履歴を表示する際には、ID/パスワードを入力

経年変化のチェック：診断結果サンプル

企業名、部署名の入力（ログインアカウント発行希望者のみ入力）
企業名、部署名を入力いただくと、診断結果に記載されます。（入力は任意）

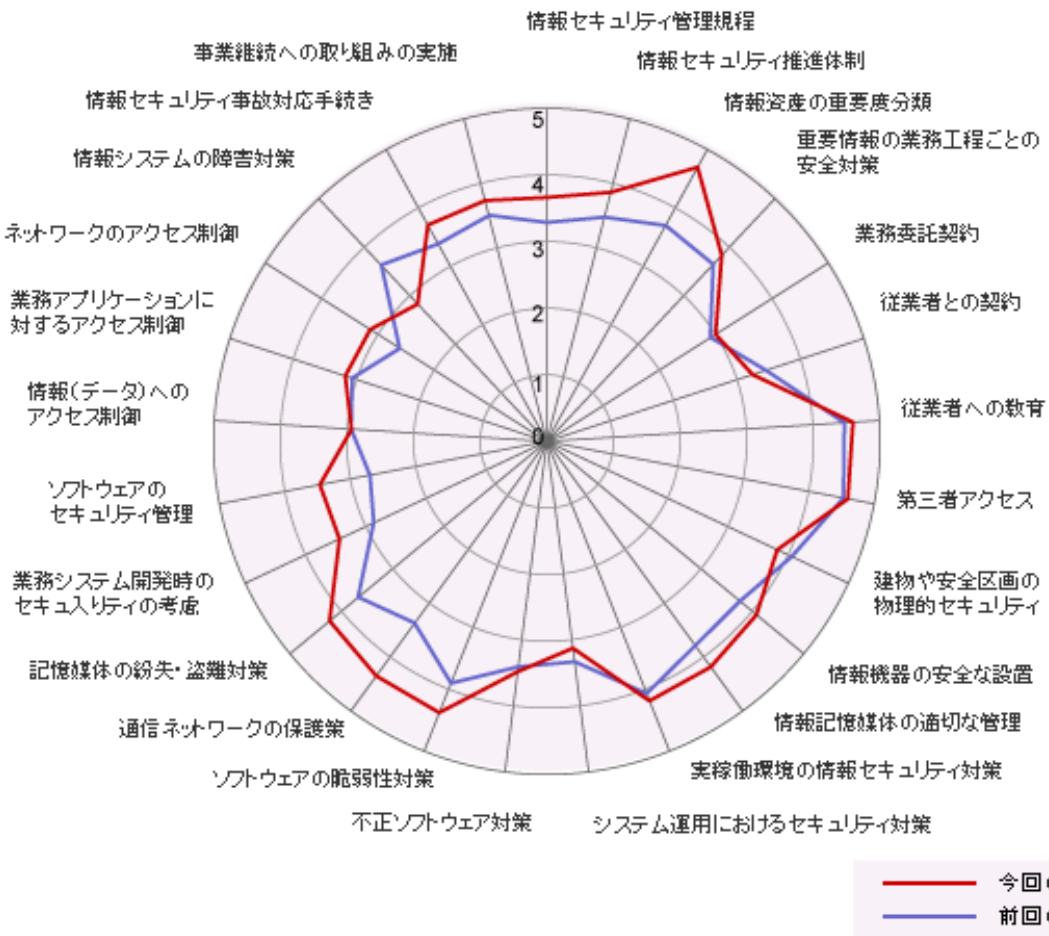
ログインアカウントの発行

※ ログインIDは自動発行
診断結果に表示される
（希望者にのみ発行）

ログインアカウントを発行すると、次回診断の際、企業プロフィールの入力の手間を軽減できる。
設問への回答最新1件が保存され、前回との比較が表示される。
（診断結果のPDFは各自保存）

本システムではご回答いただいたデータを統計処理し、その都度、対策の「望まれる水準」を見直しています。このため情報処理推進機構(IPA)では、日々変わる「望まれる水準」と御社の現状とをご理解いただくためにも、本システムを継続してご利用いただくことをお勧めしています。

今回のスコアと前回のスコアをグラフ表示



本日の内容

1. IPAとIPAセキュリティセンターの紹介
2. 情報セキュリティ対策ベンチマーク：構成と役割
   1) 背景
   2) 構成と役割
      概要、評価項目と対策ポイント、
      成熟度の構成、企業分類と望まれる水準
3. 情報セキュリティ対策ベンチマーク：利用傾向等
   1) 利用傾向
   2) 新バージョンの改善点

4. セキュリティ評価における自己評価の意義

1) 様々なセキュリティ評価
2) 自己評価（セルフアセスメント）に関するガイドライン
3) 海外の自己評価ツールの紹介

様々なセキュリティ評価

情報セキュリティ監査
ISMS適合性評価制度
ITセキュリティ評価・認証制度
脆弱性検査（または脆弱性診断、脆弱性監査）
情報セキュリティ対策ベンチマーク

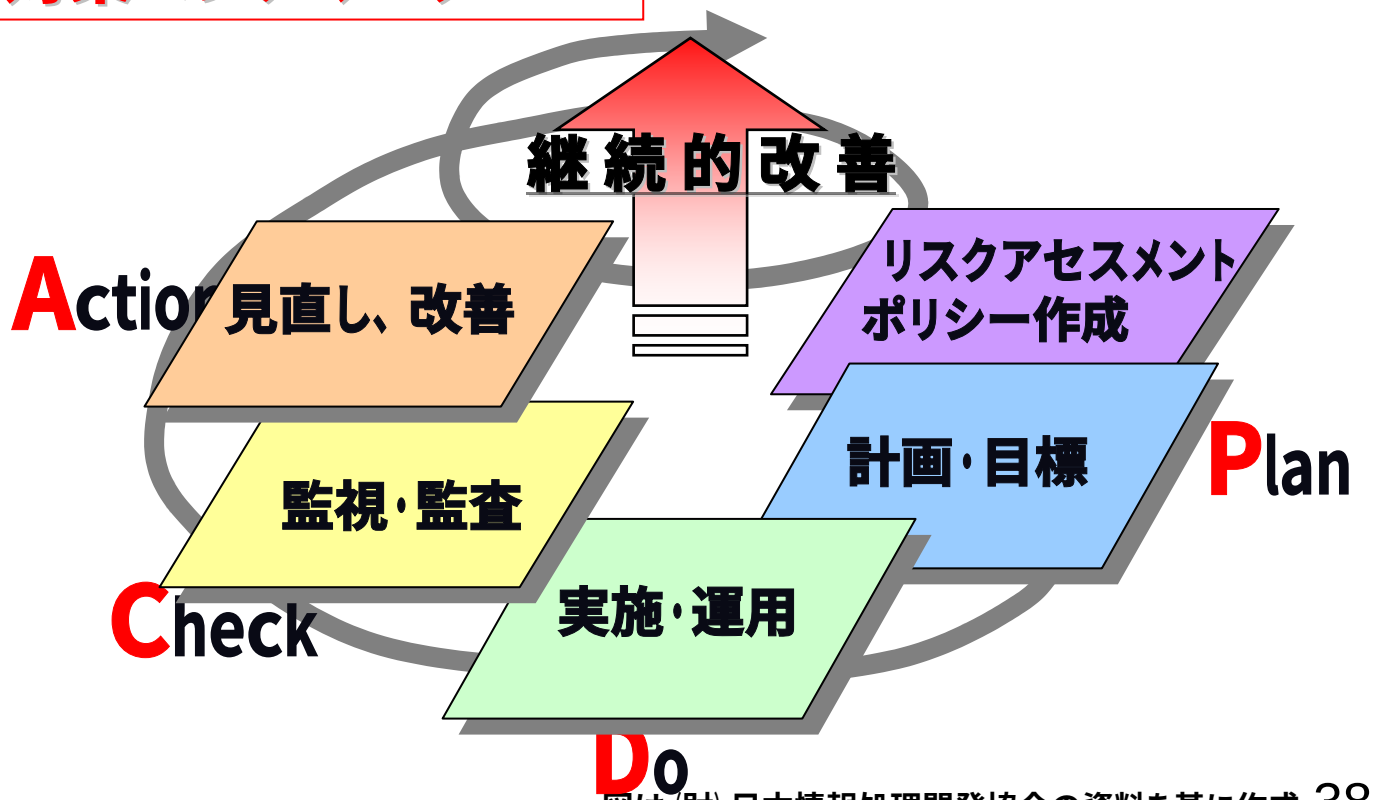
第三者評価と自己評価

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

PDCAサイクルとセキュリティ評価の活用

情報セキュリティ監査
ISMS適合性評価制度
ITセキュリティ評価・認証制度
脆弱性検査（脆弱性診断、脆弱性監査）
情報セキュリティ対策ベンチマーク

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

PDCAサイクルのPlan(計画)-Do(実施)- C(点検)各段階での活用が可能

- 自社の現在のレベル、望ましい水準とのギャップ、不足している対策がスコアとして示されるため、Plan(計画)段階での活用は、特に有効
- **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(実施) - C(点検)での活用も十分に効果的
  (新バージョンでは、履歴によるスコアの変化のチェックも可能)
- セルフチェック後の改善活動はA (Act:見直し)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

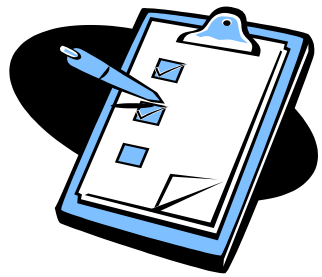
状況に応じたカスタマイズ

対策の取組み状況25項目と対策のポイント127項目の活用
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

情報セキュリティ監査

PDCAサイクルではC(check:点検)にあたる

- 情報セキュリティ対策の**有効性・実施状況**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**・・・不備な点を示す
  - **保証型監査**・・・不備は無かったことを示す
- 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

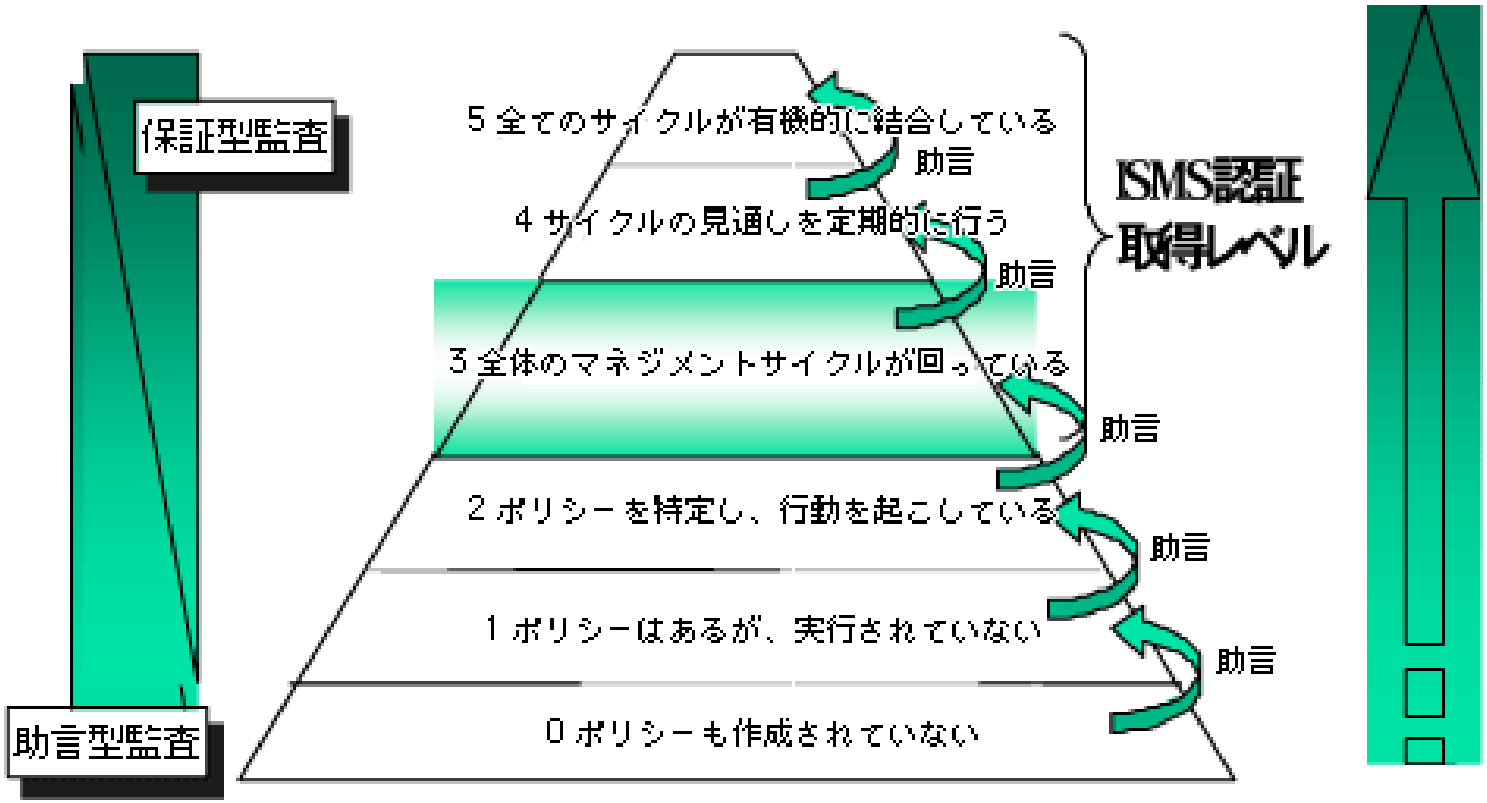


経済産業省の情報セキュリティ監査企業台帳 http://www.meti.go.jp/policy/netsecurity/is-kansa/

情報セキュリティ監査

■保証型監査と助言型監査の関係（イメージ図より）

情報セキュリティ監査の普及による
情報セキュリティマネジメントの向上



※上記0～5は単なるイメージであり、正式な定義等ではない。

出典：http://www.jasa.jp/isec-kansa/about02.html

ISMS適合性評価制度による認証

ISMS適合性評価の認証を受けるには、C(Check:監査/点検)の段階を経てPDCAサイクルを最低でも一回はまわしている必要がある

- ISMS（情報セキュリティマネジメントシステム）が適切に構築運用されていることを、正式に認定された審査登録機関と審査員が評価し、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：ISMS認証基準。
- ISMS認証基準の「第4 情報セキュリティマネジメントシステム」「第5 経営者の責任」「第6 マネジメントレビュー」「第7 改善」に記載の要求事項は、認証を受けるためには必須。

  付属書の「詳細管理策」に関しては、除外は認められるが、除外する場合、リスクアセスメントの結果に基づき、経営陣や責任者が判断して正式に残留リスクの受容が決定されたことを示す証拠を、適用宣言書に残す必要がある。
- 財団法人日本情報処理開発協会（JIPDEC）により運用。
- この制度を支える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/)

【参考】政府機関統一基準と ISO/IEC17799:2005, SP800-53との対応（自己点検）

出典：内閣官房情報セキュリティセンター
政府機関統一基準とISO/IEC17799:2005等との対応について
http://www.bits.go.jp/active/general/pdf/rel2005_iso.pdf

				ISO/IEC17799	SP800-53
2.3 評価					
2.3.1. 情報セキュリティ対策の自己点検					
（1） 自己点検に関する年度計画の策定					
	2.3.1.(1) (a)	基本	最高情報セキュリティ責任者は、年度自己点検計画を策定すること。	15.2.1	CA-2
（2） 自己点検の実施に関する準備					
	2.3.1.(2) (a)	基本	情報セキュリティ責任者は、行政事務従事者ごとの自己点検票及び自己点検の実施手順を整備すること。	15.2.1	CA-2
（3） 自己点検の実施					
	2.3.1.(3) (a)	基本	情報セキュリティ責任者は、最高情報セキュリティ責任者が定める年度自己点検計画に基づき、行政事務従事者に対して、自己点検の実施を指示すること。	15.2.1	CA-2
	2.3.1.(3) (b)	基本	行政事務従事者は、情報セキュリティ責任者から指示された自己点検票及び自己点検の実施手順を用いて自己点検を実施すること。	15.2.1	CA-2
（4） 自己点検結果の評価					
	2.3.1.(4) (a)	基本	情報セキュリティ責任者は、行政事務従事者による自己点検が行われていることを確認し、その結果を評価すること。	15.2.1	CA-2
	2.3.1.(4) (b)	基本	最高情報セキュリティ責任者は、情報セキュリティ責任者による自己点検が行われていることを確認し、その結果を評価すること。	15.2.1	CA-2
（5） 自己点検に基づく改善					
	2.3.1.(5) (a)	基本	行政事務従事者は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善し、情報セキュリティ責任者にその旨を報告すること。	15.2.1	CA-2
	2.3.1.(5) (b)	基本	最高情報セキュリティ責任者は、自己点検の結果を全体として評価し、必要があると判断した場合には情報セキュリティ責任者に改善を指示すること。	15.2.1	CA-2
2.3.2. 情報セキュリティ対策の監査					
（1） 監査計画の策定					
	2.3.2.(1) (a)	基本	情報セキュリティ監査責任者は、年度情報セキュリティ監査計画を策定し、最高情報セキュリティ責任者の承認を得ること。	15.3.1	CA-2

【参考】ISO/IEC17799の管理策(評価関連)

IPA

ISO/IEC 17799:2005

Security policy セキュリティ基本方針
Organizing information security 情報セキュリティのための組織
Asset management 資産の管理
Human resources security 人的資源のセキュリティ
Physical & environmental security 物理的及び環境的セキュリティ
Communications & operations management 通信及び運用管理
Access control アクセス制御
Information systems acquisition, development and maintenance システムの取得、開発及び保守
Information security incident management 情報セキュリティインシデントの管理
Business continuity management 事業継続管理
Compliance 順守

11の管理領域と133の管理策

15 Compliance (順守)

15.2 セキュリティ方針及び標準の順守，並びに技術的順守

15.2.1 セキュリティ方針及び標準の順守

管理策： 管理者は，セキュリティ方針及び標準類への順守を達成するために，自分の責任範囲におけるすべてのセキュリティ手順が正しく実行されることを確実にすることが望ましい。
(自己点検･セルフアセスメント)

15.2.2 技術的順守点検

管理策： 情報システムを，セキュリティ実施標準の順守に関して，定めに従って点検することが望ましい。
(技術者自身、ツールによる検査など)

15.3 情報システムの監査に対する考慮事項

15.3.1 情報システムの監査に対する管理策

15.3.2 情報システムの監査ツールの保護

6.1.8 情報セキュリティの独立したレビュー

※日本語訳は暫定的な仮訳

【参考】ISMS関連国際標準動向（27000シリーズ）

- 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 Measurement
  - **セルフアセスメントのための指標及び測定方法**
- 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**

【参考】SP800-53の管理策 (CA:評価関連)

CA: Certification, Accreditation, and Security Assessments

IPA

クラス*	ファミリ	識別子
管理	リスクアセスメント	RA
管理	計画	PL
管理	システムおよびサービスの調達	SA
管理	認定、認可、およびセキュリティアセスメント	CA
運用	人的セキュリティ	PS
運用	物理的および環境的な保護	PE
運用	緊急時対応計画 (Contingency Planning)	CP
運用	構成管理	CM
運用	保守	MA
運用	システムおよび情報の完全性	SI
運用	記録媒体の保護	MP
運用	インシデント対応 (Incident Response)	IR
運用	意識向上および訓練	AT
技術	識別および認証	IA
技術	アクセス制御	AC
技術	監査および責任追跡性	AU
技術	システムおよび通信の保護	SC

17のファミリと163の管理策

(管理策、補足ガイダンス、管理強化策)

- CA-1 認定、認可、及びセキュリティアセスメントの方針と手順
- CA-2 セキュリティアセスメント
  [管理策が正しく導入され、意図したとおりに運用され、期待した成果が得られているか判断するために、定期的にセキュリティ管理策を評価]
  (自己評価及び第三者評価)
- CA-3 情報システムの接続
- CA-4 セキュリティ認定
- CA-5 活動計画とマイルストーン
- CA-6 セキュリティ認可
- CA-7 継続監視

* 各ファミリに含まれる管理策の主な特性に基づいて管理・運用・技術のクラスに分類されているが、セキュリティ管理策の多くは複数のクラスに関連付けることができるため、クラス分けは便宜的なもの。

【参考】FISMA導入プロジェクト リスクマネジメントフレームワーク(RMF)

IPA

開始点 (FIPS199/SP800-60)

セキュリティのカテゴリ化

情報資産に対する潜在的な脅威の影響度に基づき、情報システムを低位・中位・高位に分類する。

(FIPS200/SP800-53)

セキュリティ管理の選択

情報システムを保護するための最低限のセキュリティ管理策を低位・中位・高位の分類に応じて選択する。

(SP800-53/ FIPS200/SP800-30)

選択したセキュリティ管理の調整

リスクアセスメント行い、個々の状況、脅威への対策要件、各政府機関に特有の要件に基づき、先に選択した管理策を調整する。

(SP800-18)

セキュリティ管理策の文書化

情報システムのセキュリティ要件の概要及び計画された又は既存のセキュリティ管理策をシステムセキュリティ計画書に記載し、文書化する。

(SP800-70)

セキュリティ管理策の導入

新／旧情報システムへセキュリティ管理策を導入する；
セキュリティ設定用チェックリストの使用

(SP800-53A/SP800-26/ SP800-37)

セキュリティ管理策の評価

セキュリティ管理策が正しく導入され、意図した通りに運用され、セキュリティ要件に見合う成果を上げているかを判断する。

(SP800-37)

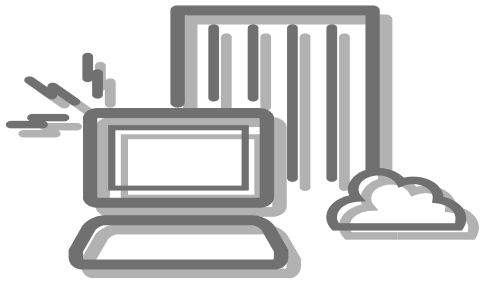
システム運用の承認

政府機関の運用管理リスク、情報資産または個人へのリスクを判断した上で、情報システムの運用を承認する。

(SP800-37)

セキュリティ管理策実施状況の監視

セキュリティ管理に影響を及ぼす情報システムへの変更を監視し、管理策の有効性を継続的に評価する。



監査（自己評価と第三者評価）

Draft SP800-26 Rev1, Guide for Information Security Program Assessments and System Reporting Form
(SP 800-26 Security Self-Assessment Guide for Information Technology Systems (November 2001))
ITシステムのためのセキュリティ自己アセスメントガイド
Draft SP 800-53A: Guide for Assessing the Security Controls in Federal Information Systems
連邦政府情報システムにおけるセキュリティ管理策アセスメントガイド

【参考】NIST文書などの翻訳・調査研究プロジェクト

http://www.ipa.go.jp/security/publications/nist/index.html
http://www.nri-secure.co.jp/news_alert/report/nist/nist_report.html

NIST :
National Institute of Standards and Technology
米国国立標準技術研究所

SP800シリーズ:
SP=Special Publications
NIST CSD (Computer Security Division)
が発行するITセキュリティ関係のガイドライン
NIST CSD: http://csrc.nist.gov/

FIPS:

Federal Information Processing Standards
米国商務長官の承認を受けて、NISTが公布した情報技術関連の連邦政府基準

シリーズNo.(原文発行年月)	タイトル	掲載(予定)
SP 800-26 ※ (2001年11月)	ITシステムのためのセキュリティ自己アセスメントガイド Security Self-Assessment Guide for Information Technology Systems	2005年8月
SP 800-33 (2001年12月)	ITセキュリティのための基本テクニカルモデル Underlying Technical Models for Information Technology Security	2005年8月
SP 800-35 (2003年10月)	ITセキュリティサービスガイド Guide to Information Technology Security Services	2005年8月
SP 800-42 (2003年10月)	ネットワークセキュリティテストにおけるガイドライン Guideline on Network Security Testing	2005年8月
SP 800-50 (2003年10月)	ITセキュリティの意識向上およびトレーニングプログラムの構築 Building an Information Technology Security Awareness and Training Program	2005年8月
SP 800-55 (2003年07月)	情報技術システムのためのセキュリティメトリクスガイド Security Metrics Guide for Information Technology Systems	2005年8月
SP 800-61 (2004年01月)	コンピュータインシデント対応ガイド Computer Security Incident Handling Guide	2005年8月
SP 800-64 (2004年06月)	情報システム開発ライフサイクルにおけるセキュリティの考慮事項 Security Considerations in the Information System Development Life Cycle	2005年8月
[更新 05/12/28] SP 800-34 (2002年06月)	ITシステムのための緊急時対応計画ガイド Contingency Planning Guide for Information Technology Systems	2005年11月
NEW! SP 800-30 (2002年07月)	ITシステムのためのリスクマネジメントガイド Risk Management Guide for Information Technology Systems	2006年1月
SP 800-53 (2005年02月)	連邦政府情報システムにおける推奨セキュリティ管理策 Recommended Security Controls for Federal Information Systems	2006年2月

【参考】その他のセルフチェックツール

海外でも、ベンチマークと同趣旨のセルフチェックツールが公表

アメリカ：ISG (Information Security Governance) Program
民間団体The National Cyber Security Partnership (NCSP)
「Information Security Governance　A Call to Action」を2004年4月発表。
資料：経営陣が情報セキュリティを評価する簡易な評価法が添付
http://www.cyberpartnership.org/InfoSecGov4_04.pdf

イギリス：e-Security Health check
政府機関DTI（Department of Trade and Industry）**提供のセルフチェックツール**
BS7799をベースに作成した質問項目に回答すると、企業のステータスが体重計の形式で表示される　http://www.dti-bestpractice-tools.org/healthcheck/

フランス：EBIOS（Expression of Needs and Identification of Security Objectives）
フランス政府機関で情報セキュリティを担当するDCSSI (Central Information Systems Security Division)**が提供する無料のリスク評価ツール**

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報告書　（参考3）より
http://www.meti.go.jp/report/downloadfiles/g50331d01j.pdf

【参考】その他のセルフチェックツール

イギリス：e-Security Health check http://www.dti-bestpractice-tools.org/healthcheck/

Please answer the following

Does your organisation have an information security policy?	Yes ◉	Pa
Are staff allocated with specific security responsibilities, e.g. locking the building, allocating passwords?	Yes ◉	Pa
Do you know what your organisation's main assets are, do you have a list of them, and does this list include information?	Yes ○	Pa
Are specific personnel measures, such as training users or including security in their job descriptions, taken with respect to security?	Yes ◉	Pa
Does your organisation take steps to prevent unauthorised access to your premises?	Yes ◉	Pa
Have you implemented operational controls and procedures to safeguard your information, e.g. use of back-ups, anti virus software, firewalls?	Yes ◉	Pa
Do you control access to information through the effective use of user ids and passwords, e.g. making sure users don't share passwords, write their passwords on post-it notes?	Yes ◉	Pa
Have steps been taken to ensure that security requirements are defined and incorporated during system development or met by packaged software solutions?	Yes ◉	Pa
Do you have any business continuity plans?	Yes ○	Pa
Do you ensure that you meet all your legal requirements/obligations, e.g licensing, copyright, data protection?	Yes ◉	Pa

Submit | Proceed To Main Questionnaire

Summary Of Results From Short Survey

Needs improvement

The Main Questionnaire

In order to assess your information security health more accurately, you may now wish to move on to the main questionnaire. This is broken down into 10 sections. You may answer any, or all of the following sections, with individual results being available at any stage.

If you complete all 10 sections you will be given an overall rating.

Section	No. of Questions	Completed?
1. Security Policy	5	No
2. Security Organisation	9	No
3. Asset Classification & Control	8	No
4. Personnel Security	9	No
5. Physical & Environmental Security	11	No
6. Communications & Operational Mgt.	19	No
7. Access Control	24	No
8. System Development & Maintenance	10	No
9. Business Continuity Mgt.	3	No
10. Compliance	8	No

106 questions

情報セキュリティ対策ベンチマーク
～ 貴社のセキュリティレベルは？ ～

IPA

こんなときに！

我が社の
セキュリティ対策は
十分だろうか？

セキュリティ対策
予算を増額したいが、
上司を説得できる資料、
作れないかなぁ？

まだ取り組んでいない
セキュリティ対策には
何があるだろう？

自社の対策レベル、望ましい水準との
ギャップ、どの対策が不足かをチェック

何度も活用して
継続的に改善

情報セキュリティ対策ベンチマークシステムの活用
http://www.ipa.go.jp/security/benchmark/

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/