JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

中小企業向け個人情報保護対策WG 活動報告

市川　順之
伊藤忠テクノサイエンス株式会社

2006 年 5月30日

目次

- 個人情報保護法施行元年の世の中の動向
- WG が目指したもの
- WG活動の詳細
- まとめ
- 今後の中小企業の課題
- 最後に

個人情報保護法施行元年の
世の中の動向

この一年の状況

JNSA

個人情報保護法完全施行後、
この1年間の世の中の動向

個人情報漏洩事故

・多発したP2Pソフトによる情報漏洩事故

個人情報の取扱い

・昨年　5月20日　M銀行に対し金融庁が個人情報保護法に基づく是正勧告

・JR西日本　尼崎脱線事故での安否情報をめぐる大混乱

WG が目指したもの

WG概要

中小企業向け個人情報保護対策 WG

WG発足のきっかけ

- 2005年4月、個人情報保護法完全施行に対して中小企業がどのような状況に陥るのか？また、大企業と比較しできる対策は何があるのか？という疑問を純粋に追求するために発足。

WGの目的

- 法律施行後の中小企業の現状について調査し、中小企業に適した対策について研究する。

スケジュール (2005年度)

２００５年

- 2月　　WG発足
- 6月　　モニタ企業コンサルティング開始
- 10月　 中間発表
- 12月　2社目モニタ企業コンサルティング

２００６年

- 3月　　成果発表

月一回の定例ミーティング開催
コンサルティングについては随時

WG活動の当初に考えたこと

JNSA

個人情報保護対策というと．．．．

個人情報保護宣言の作成
個人情報保護　ポリシー策定
組織的、技術的、人的、物理的対策の検討

中小企業向けが
できたらいいな

安全管理の実装

監査

対策見直し

活動内容

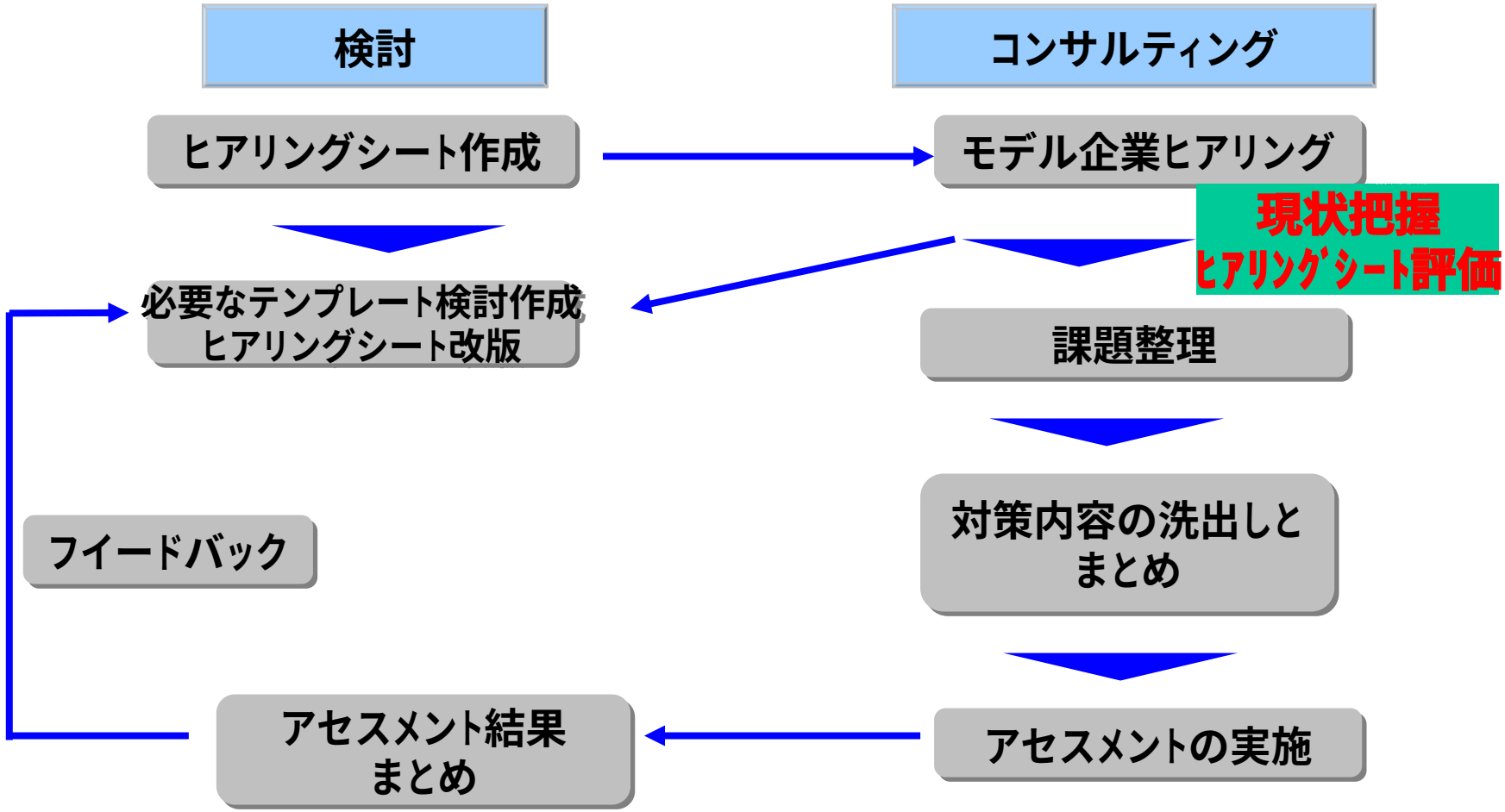
- 中小企業における個人情報保護法による影響の把握
- 中小企業における個人情報保護対策の検討、実地検証

・中小企業の運用に適した形のﾃﾝﾌﾟﾚｰﾄの検討（JNSA提供の雛型も参考）

・モニタ企業へのコンサルティングを通じて実地検証　（2社）

・作成したﾃﾝﾌﾟﾚｰﾄ（ﾁｪｯｸﾘｽﾄ）によるモニタ企業ヒアリング
・モニタ企業に対する経済産業省ガイドライン（4つの基準）のセキュリティアセスメントとアドバイス

WG活動プロセス



WG活動の結果としては

個人情報保護対策というと．．．．

個人情報保護宣言の作成
個人情報保護　ポリシー策定
組織的、技術的、人的、物理的対策の検討

中小企業が自主的にこの流れを運用するための仕組みを考えたほうが有効

ヒアリングシートをベースにしたチェックシートへのブラッシュUP

安全管理の実装

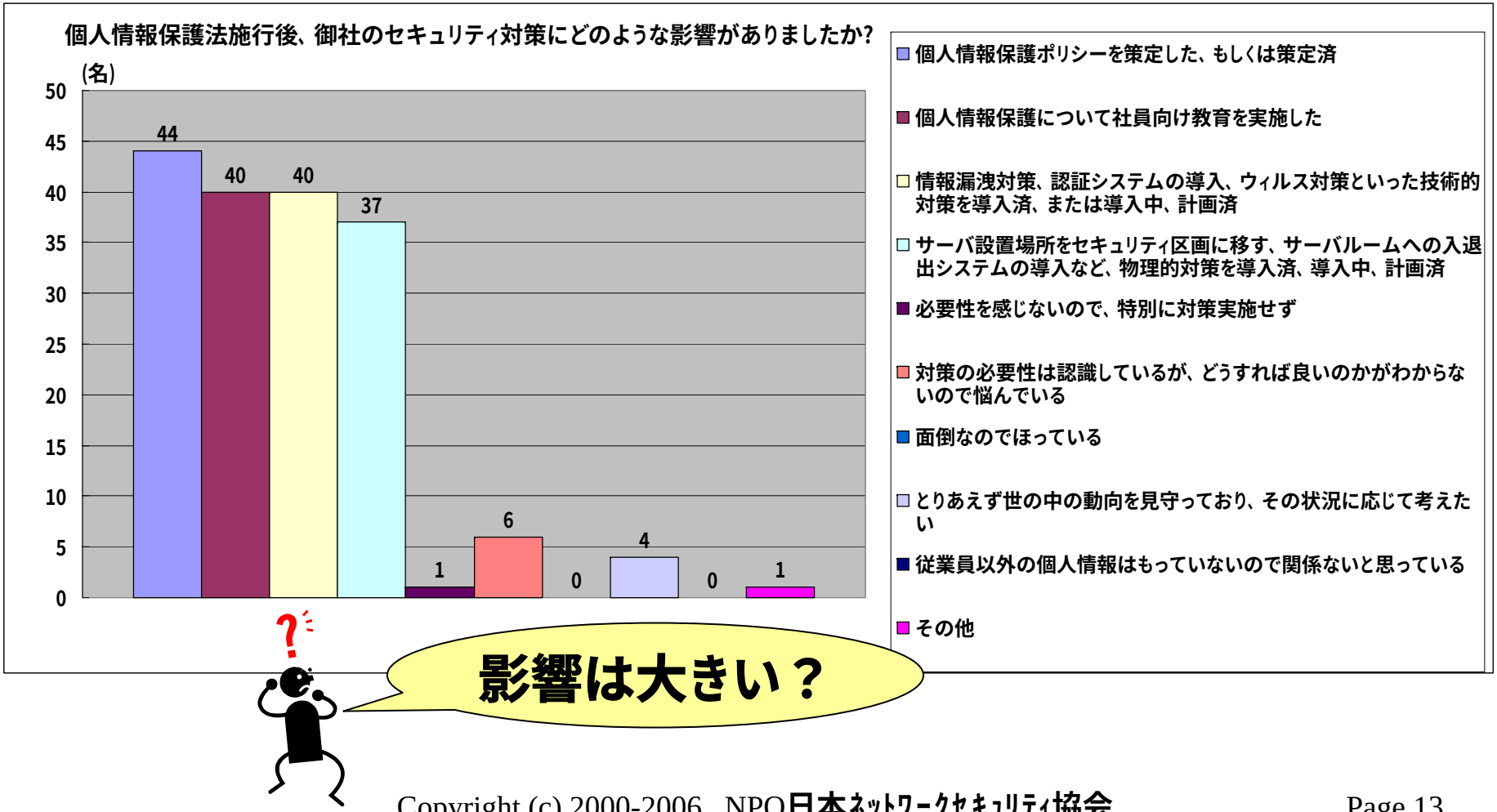
監査

対策見直し

WG活動の詳細

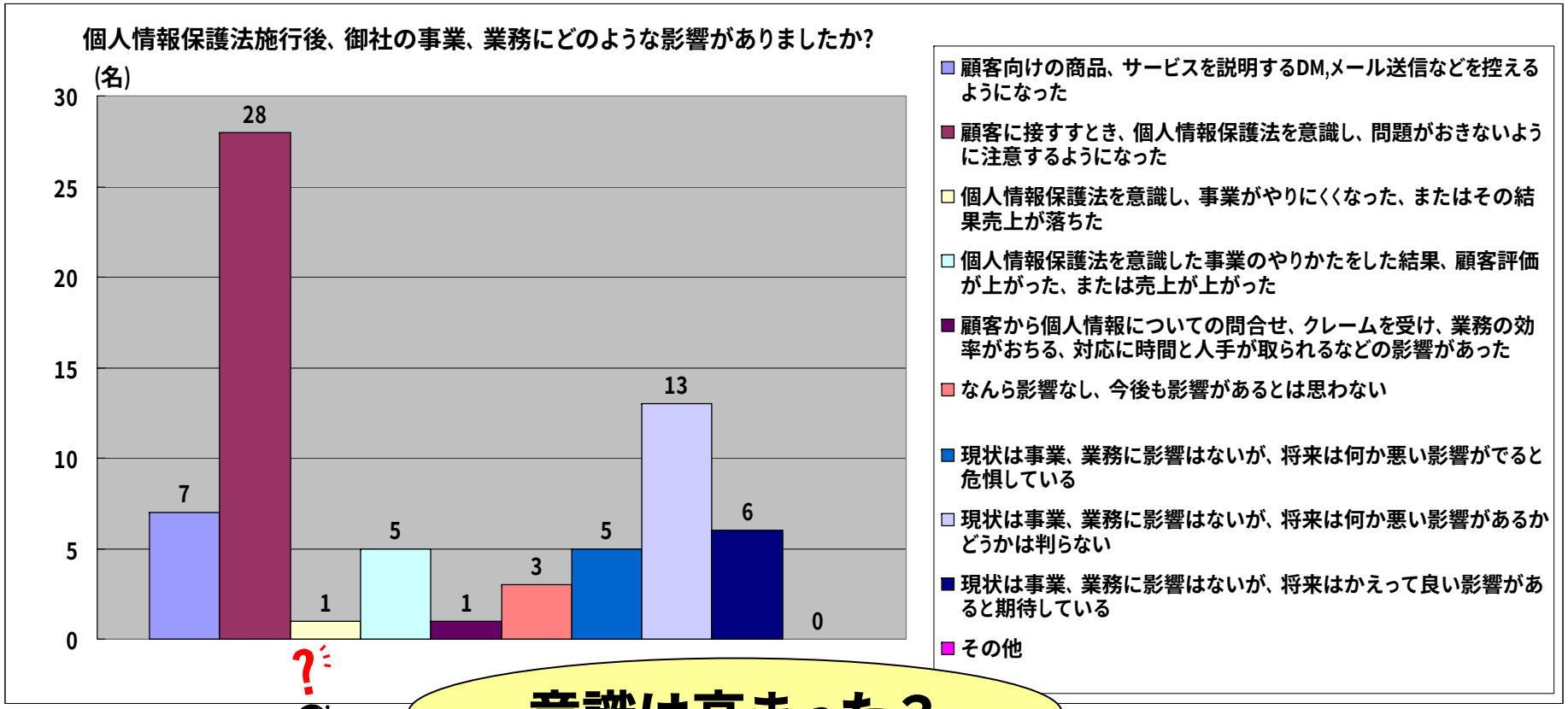
ＪＮＳＡセミナーのアンケート結果

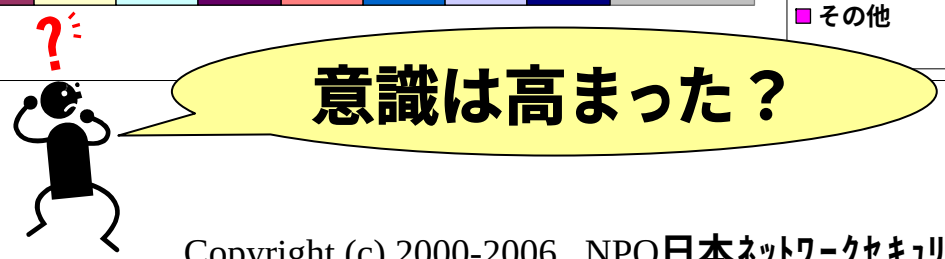
昨年１０月　ＪＮＳＡセミナーでのアンケート結果



ＪＮＳＡセミナーのアンケート結果

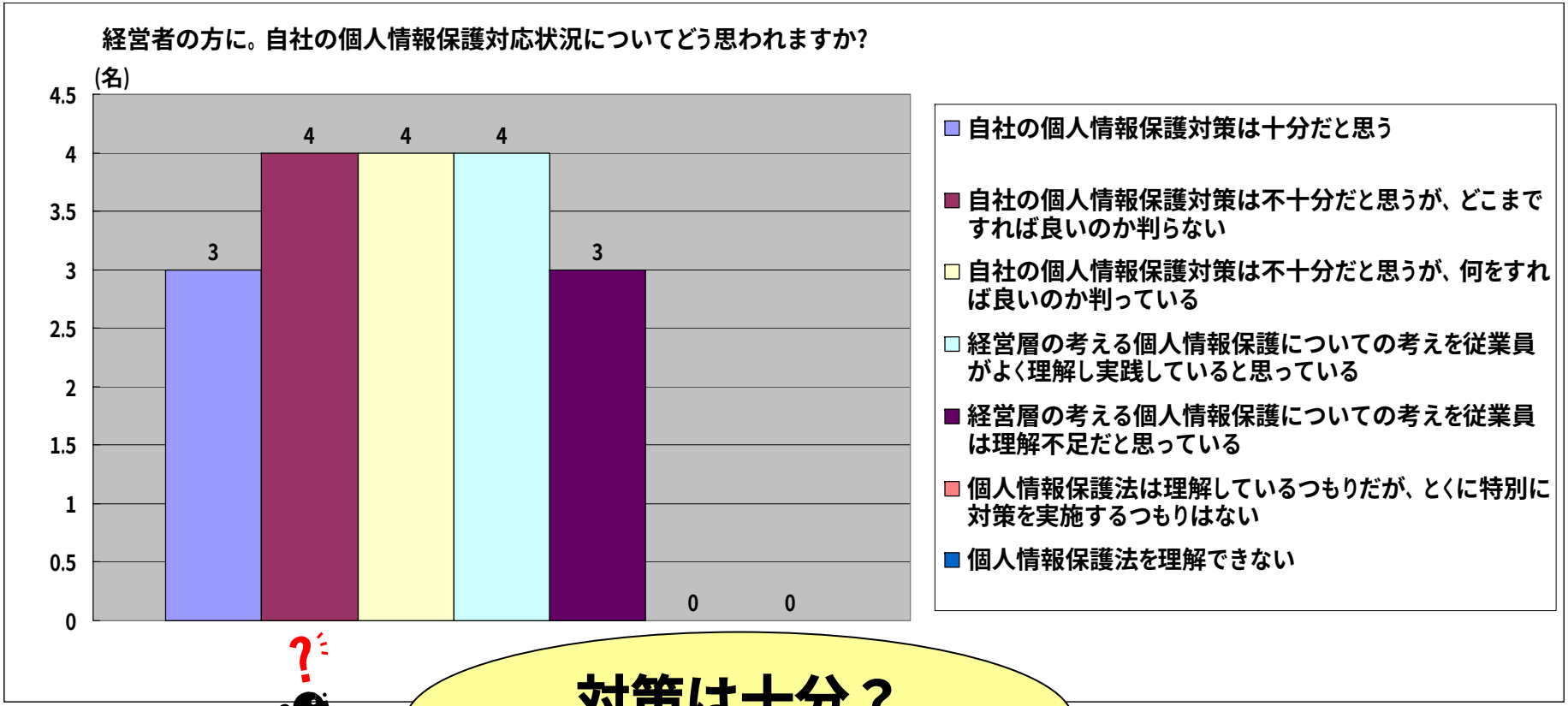
昨年１０月　ＪＮＳＡセミナーでのアンケート結果

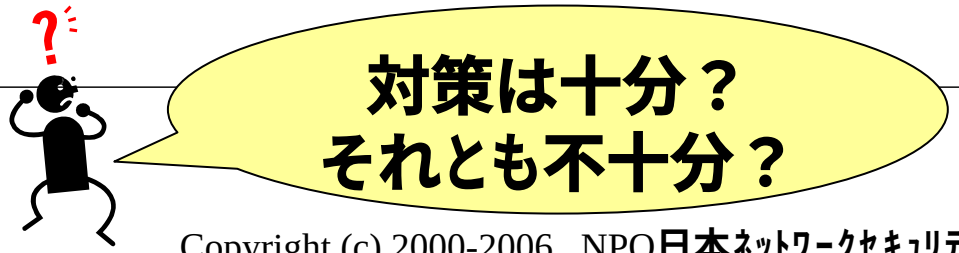




ＪＮＳＡセミナーのアンケート結果

昨年１０月　ＪＮＳＡセミナーでのアンケート結果

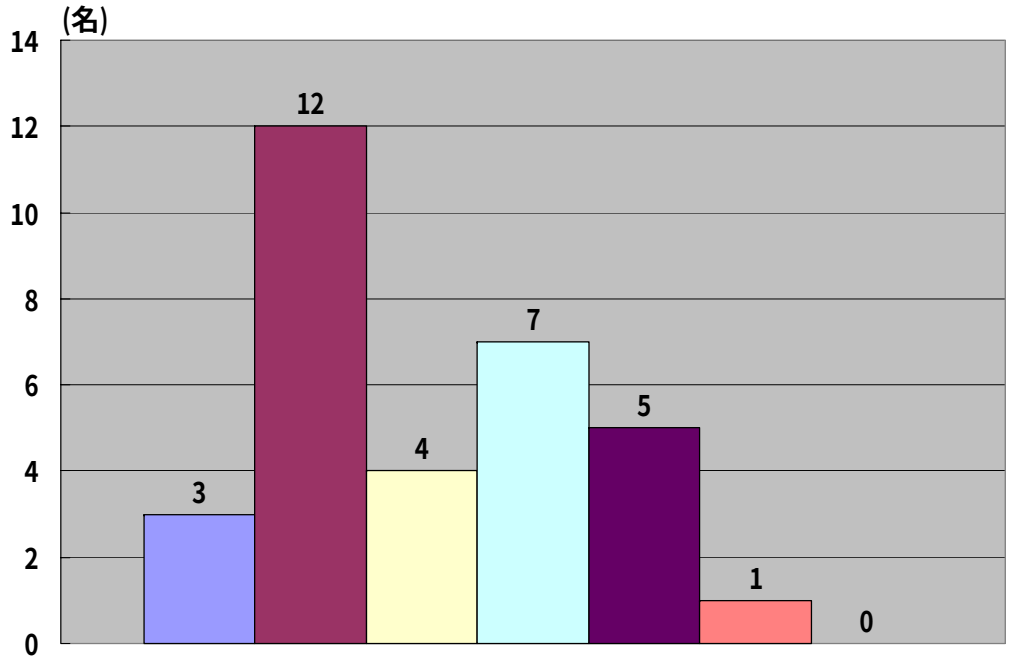




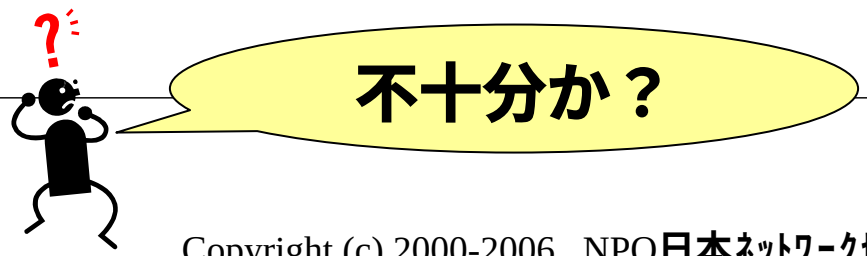
ＪＮＳＡセミナーのアンケート結果

昨年１０月　ＪＮＳＡセミナーでのアンケート結果

情報システム部門の方に。自社の個人情報保護対応状況についてどう思われますか?



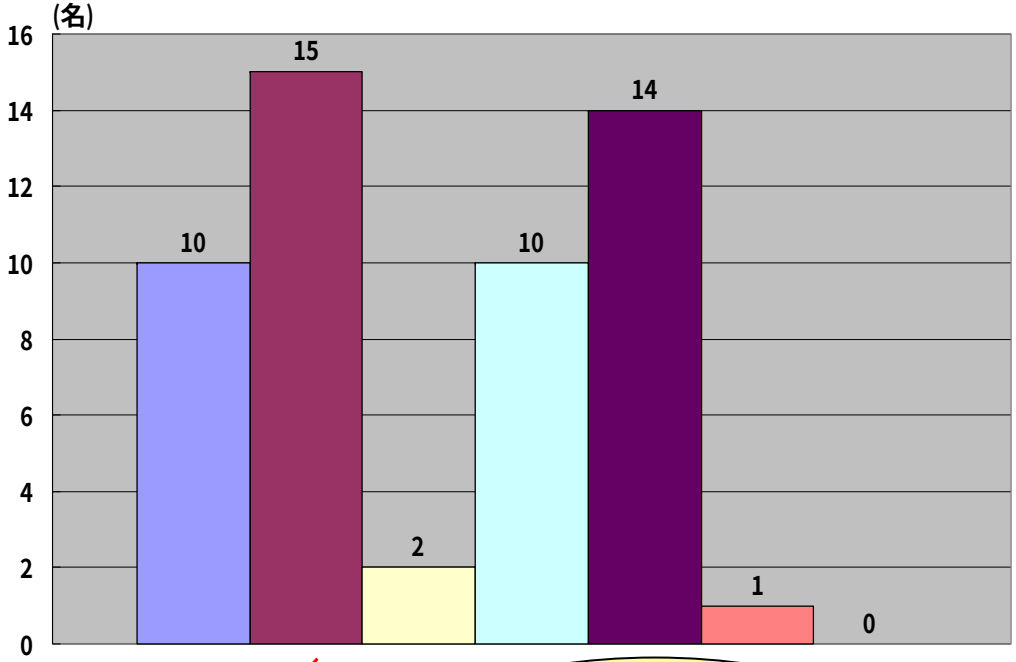
- 自社の個人情報保護対策は十分だと思う
- 自社の個人情報保護対策は不十分だと思うが、どこまですれば良いのか判らない
- 自社の個人情報保護対策は不十分だと思うが、何をすれば良いのか判っている
- 経営層が個人情報保護対策についてよく理解し、前向きだと思う
- 経営層が個人情報保護対策について理解不足、積極性がないと思う
- 個人情報保護法は理解しているつもりだが、とくに特別に対策を実施するつもりはない
- 個人情報保護法を理解できない



ＪＮＳＡセミナーのアンケート結果

昨年１０月　ＪＮＳＡセミナーでのアンケート結果

情報システム部門以外の従業員の方に。自社の個人情報保護対応状況についてどう思われますか?



- 自社の個人情報保護対策は十分だと思う
- 自社の個人情報保護対策は不十分だと思う
- 自社の個人情報保護対策は現場の実態とマッチしていると思う
- 自社の個人情報保護対策は現場の実態と合わない
- 自社の個人情報保護対策について社内教育をうけ、対策の目的、効果を理解している
- 自社の個人情報保護対策について社内教育をうけたことがないので、対策の目的、効果を理解していない
- 個人情報保護法を知らない

ＪＮＳＡセミナーのアンケート結果

昨年１０月　ＪＮＳＡセミナーでのアンケート　ご意見

- プライバシーと個人情報の混同
- 個人情報に対し過剰な反応
- 個人情報ひとくくりではなく機微性の考慮も
  （例：氏名とカード情報を同じレベルで扱うのは変）
- 個人情報は守るために持っているのではなく使うため
- 適切に対応できているか不安
- 対策が不徹底
- 取り組みが難しい、どう対策していいのか判らない
  対策の基準って？

中小企業の現状

・アンケート、モニタ企業から見えた現状

技術的対策の現状

・どこまでやれば良いのか？
・現状の対策が十分なのか、不十分なのか自信がない
・システムに対する知識不足

物理的対策の現状

・事務所の制約
　セキィリティ区画としてサーバルームの独立もスペース、事務所環境により困難

中小企業の現状

JNSA

・アンケート、モニタ企業から見えた現状

組織的対策の現状

・担当者まかせで管理できていない
・社員と外部要員・バイトの区別がない
・委託先についての管理方法に不安要素がある
・セキュリティに対する意識はあるが文書化されていない
・実態とルールとの間にギャップ
・就業規則等の規程がない
・監査をしたことがない

人的対策の現状

・教育をしたことがない
→そもそも教育すべきルールがない
・教育はしたが効果が不明

中小企業の現状

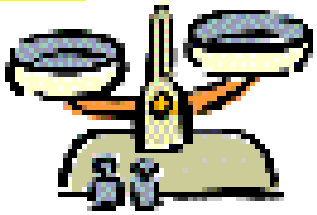
重視

技術対策

軽視

組織対策
人対策

技術対策をすれば充分かな
組織、人については. . .



技術対策を重視するが、どこまですべきか判らない

中小企業の問題

問題

・技術対策の目標レベルを自分で決められない
　→ 課題、問題を把握できていないので、目標が決まらない
　　課題、問題を抽出しても充分かどうか自信がない
・監査をしていないのでＰＤＣＡサイクルをまわせない

マネジメントの問題！

WGから提示した対策案

- まずは現状把握から

  ヒアリングシートの書き方の工夫
  対策項目とレベル、ＰＤＣＡとの対応の記述により、課題と目標を把握

- 組織、人的対策への雛形提示
  - 保護方針
  - 各種契約書の雛形
  - 就業規則に盛り込む事項
  - 社内教育用のテキスト

ヒアリングシート

全体構成

資産確認シート

個人情報取扱確認シート

技術的対策確認シート

人的対策確認シート

物理的対策確認シート

組織的対策は．．

それぞれに分散し盛り込み

技術、人、物理対策はそれをチェックする組織的な対応もないと意味がない、組織的対策は独立せず、各対策に盛り込み

ヒアリングシート

ヒアリングシート例

技術的対策　不正ソフトウェア対策　抜粋

4		個人データを取り扱うシステムについての不正ソフトウエア対策		
4-1	D	ウイルス対策ソフトウエアを導入しているか	1	□0 □1 □2 □3
4-2	D	OS、アプリケーション等に対するセキュリティパッチを適用しているか		
		- 自動的にセキュリティパッチの適用が行われる設定にしている	2	□0 □1 □2 □3 □☆ □★
		- セキュリティパッチの適用は人の行動に任せている	1	□0 □1 □2 □3 □☆ □★
4-3	D	ウィルス対策ソフトのパターンファイル更新をしているか		
		- 新しいパターンファイル更新は自動的に行う仕組みを導入している	2	□0 □1 □2 □3 □☆ □★
		- 新しいパターンファイル更新は人の行動に任せている	1	□0 □1 □2 □3 □☆ □★
4-4	C	パターンファイルやセキュリティパッチの更新の確認をおこなっているか		
		- 更新の確認は自動的に行う仕組みを導入している	2	□0 □1 □2 □3 □☆ □★
		- 更新の確認は人の行動に任せている	1	□0 □1 □2 □3 □☆ □★

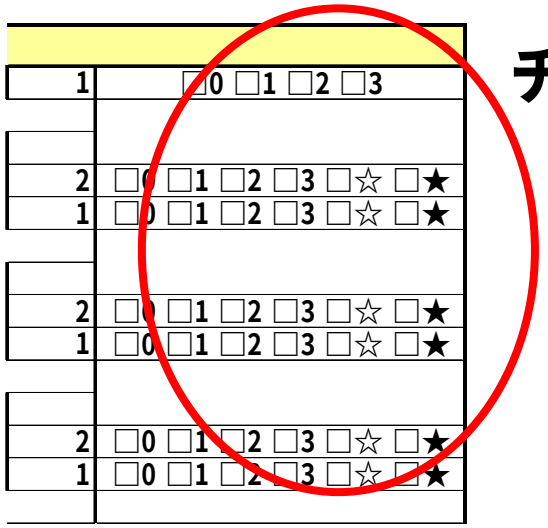
PDCAサイクルのどこにあたるか
D：実施　C：監査

対策レベル　3段階
(軽度) 1　2　3 (高度)

ヒアリングシート

ヒアリングシート例

技術的対策　不正ソフトウェア対策　抜粋



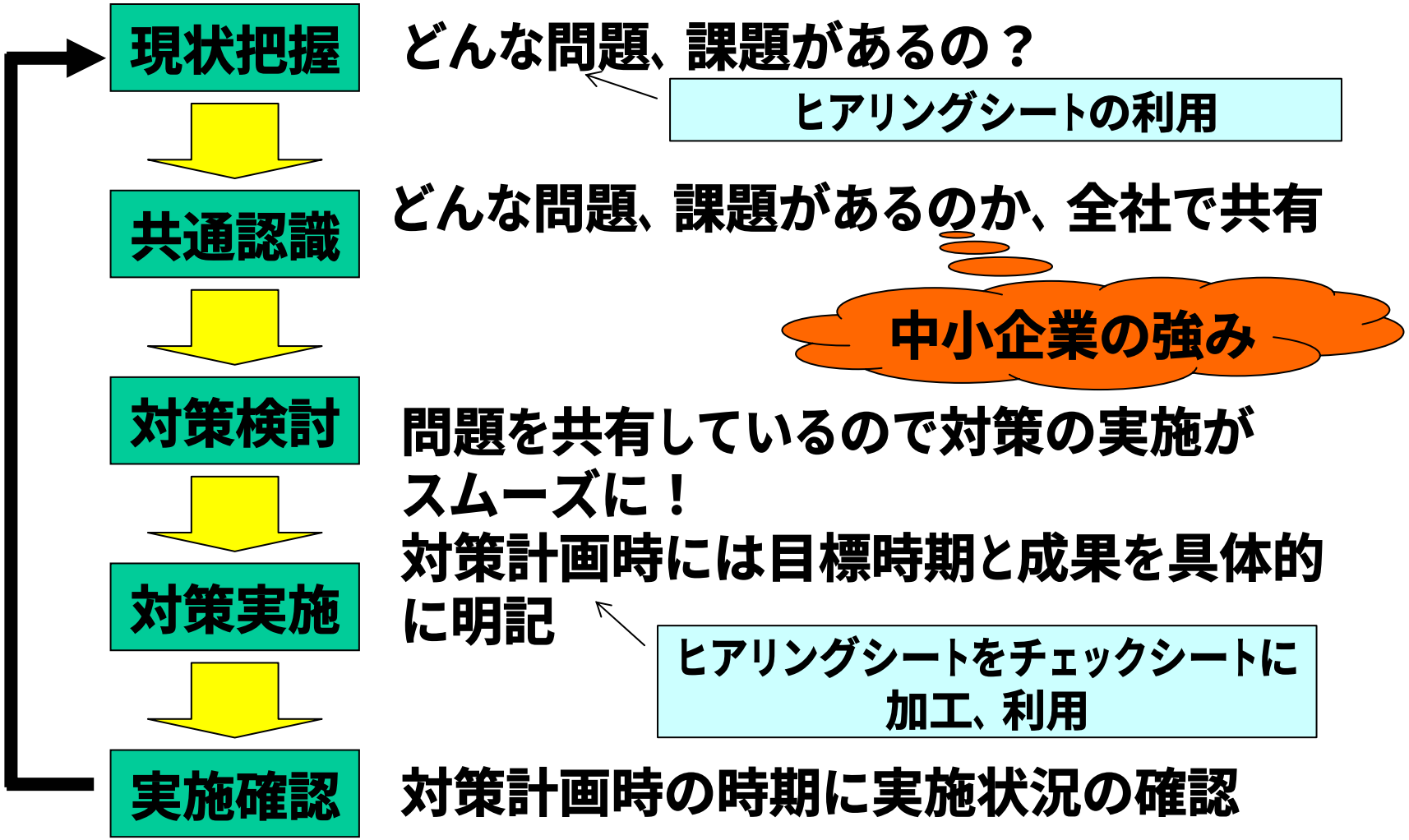
1	□0 □1 □2 □3
2	□0 □1 □2 □3 □☆ □★
1	□0 □1 □2 □3 □☆ □★
2	□0 □1 □2 □3 □☆ □★
1	□0 □1 □2 □3 □☆ □★
2	□0 □1 □2 □3 □☆ □★
1	□0 □1 □2 □3 □☆ □★

チェック欄
- 0・・・なし
- 1・・・認識はしているが対策してない
- 2・・・とりあえず対策している
- 3・・・問題なくやれている
- ☆・・・必要がない（脅威がない）
- ★・・・リスクとして許容している

☆、★がないところは、絶対対策すべき、と考えたところ

まとめ

中小企業における対策推進方法



中小企業における対策推進方法

ヒアリングシート　ー＞　チェックシートへ

1	規程･マニュアル･ルール集/ドキュメント	目標		
1-2	個人情報管理台帳(利用目的、保管場所、保管方法、アクセス権限者、利用期限等)を作成しているか			
	P 台帳を作成している	ｘｘｘまでに台帳を作成する	1	□0 □1 □2 □3
	D 台帳に基づいた運用をしている	台帳で管理外の個人情報をもたない	1	□0 □1 □2 □3
	D 台帳を定期的に更新している	作成した台帳はxx月毎に内容のﾁｪｯｸを行う	3	□0 □1 □2 □3 □☆ □★
	C 台帳に基づいた運用をしているか定期的に監査している	台帳で管理外の個人情報をもっていないかxx月毎に部門でﾁｪｯｸ、ｾｷｭﾘﾃｨ責任者に報告	3	□0 □1 □2 □3 □☆ □★
	A 運用･監査･経営環境に基づき台帳の項目を見直している	xxx毎にﾁｪｯｸした内容に基づき、ｾｷｭﾘﾃｨ管理者は改善をするためｾｷｭﾘﾃｨ委員会議を開催し,見直しを図る	3	□0 □1 □2 □3 □☆ □★

現状把握した結果から目標の立案

目標をチェックシートにすることで、チェックシートそのものが規程もかねる

今後の中小企業の課題

今後の課題

情報セキュリティの大きな変化

不正侵入対策 → **内部情報漏洩対策** → **個人情報保護法/情報セキュリティ対策**

- FW
- IDS,IPS
- ｱﾝﾁｳｨﾙｽｿﾌﾄ

- 暗号化
- 操作ﾛｸﾞ
- 媒体抑止

- コンプライアンスルールを守る

企業価値の向上

- 情報ｾｷｭﾘﾃｨｶﾞﾊﾞﾅﾝｽ
- 保証型監査

- 日本版ＳＯＸ法
- 新会社法

中小企業にとって？

WGも個人情報からセキュリティ全般へ

最後に

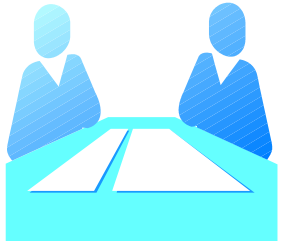
チームメンバー

- コンサルティングチーム
  - 株式会社ウェブエージェント
    - 臼井　義美
  - アイネット･システムズ株式会社
    - 元持　哲郎
  - アイネット･システムズ株式会社
    - 水田　雅樹
  - 富士通関西中部ネットテック株式会社
    - 嶋倉　文裕
- アドバイザリ
  - JNSA西日本支部のメンバ
- 研究チーム
  - 株式会社アイ･ソリューションズ
    - 谷口　星彦
  - 伊藤忠テクノサイエンス株式会社
    - 市川　順之
  - 伊藤忠テクノサイエンス株式会社
    - 西村　祥

順不同、敬称略

お願い

- JNSA会員企業の皆様へ
  - チェックシートを使っていただいてご意見をいただきたい
  - より良くする為に、辛口評価をいただきたい
- 本日来場された皆様へ
  - ご協力いただける方はこの後、私までお声掛けください



ご清聴ありがとうございました。