DIGITAL&GLOBAL
日立ソフト

情報セキュリティ:
中堅企業にとっての本当の懸念と具体策

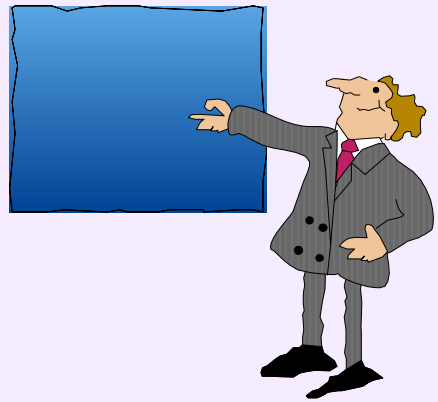
2004 01/17

日立ソフト
セキュリティビジネス部
ソリューションアーキテクト
（情報セキュリティ）
塚田 孝則

目次

情報セキュリティマネジメントの重要性

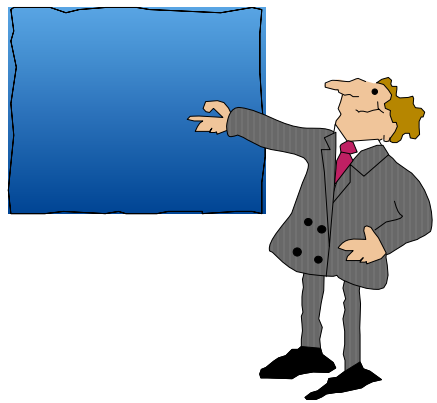
1. 経営の中でのITと情報セキュリティの位置付け
2. 情報セキュリティの必要性
3. 情報セキュリティマネジメントシステム
4. リスク評価とセキュリティ対策
5. 導入事例
6. どうしたら導入できるか
7. まとめ



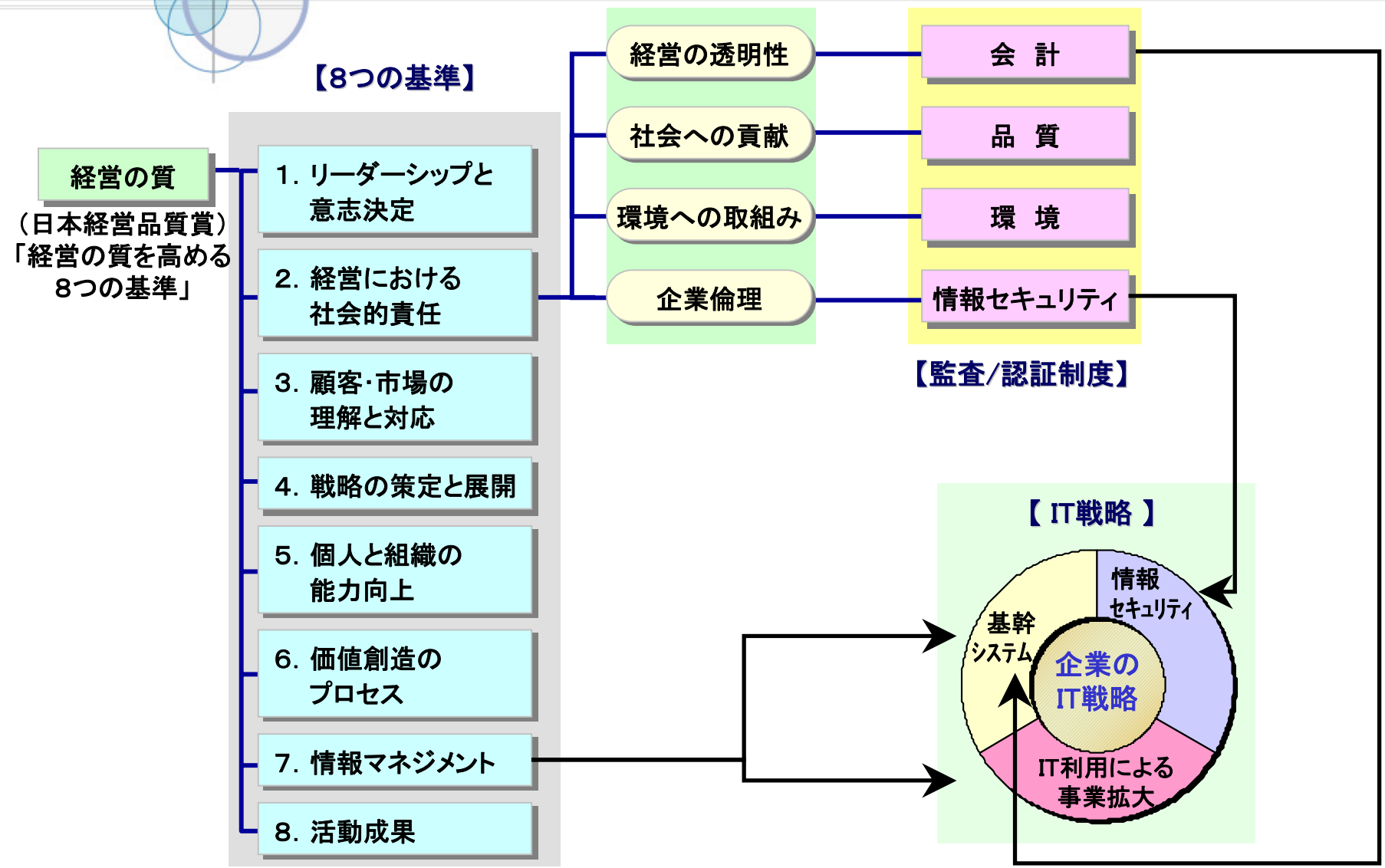
1. 経営の中でのITと情報セキュリティの位置付け

経営の中でのITと情報セキュリティ

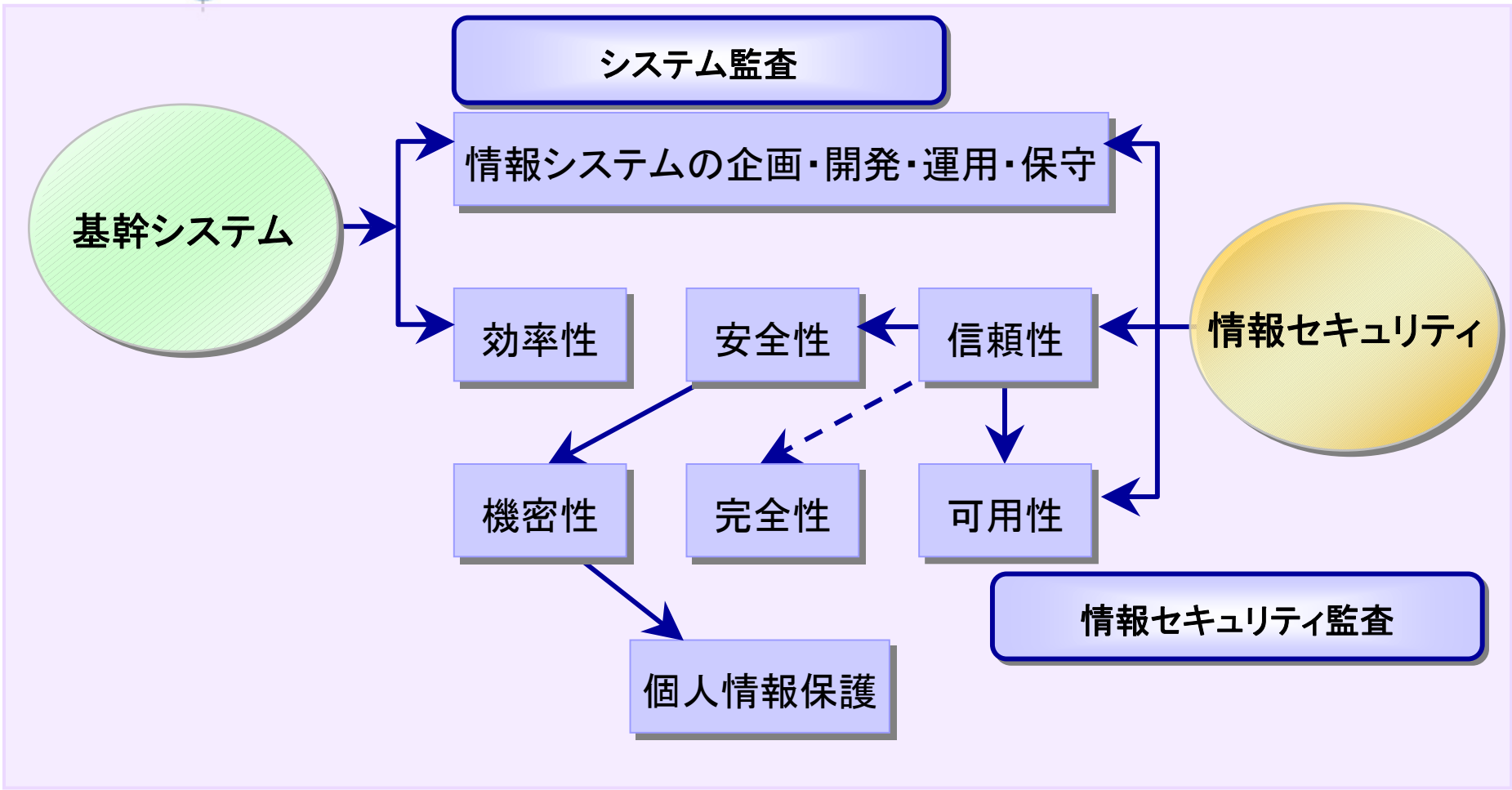
情報セキュリティ



経営の中でのITと情報セキュリティ



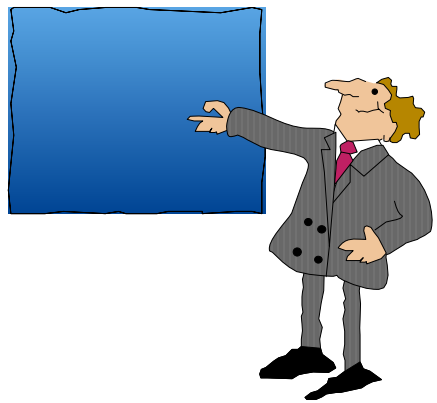
情報セキュリティ



2. 情報セキュリティの必要性

情報セキュリティ対策の必要性

組織的対策の必要性



2. 情報セキュリティの必要性

脅威

- 重要データの漏えい
  （個人情報等）
- 調達したシステムのバグ
- 災害でのITシステム停止
- 電子申請での不正
- WWWサーバ・メールサーバへの不正アクセス
- ウイルスの発生
  ・・・・・

対策

- 組織的対策
  - 手順書
  - 監査
  - 教育・訓練
    ・・・・・

＋

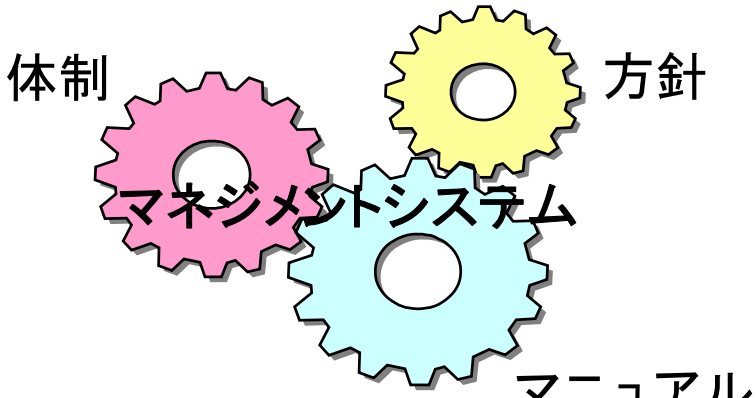
- 技術的対策
  - ファイアウォール
  - アクセス制御
  - ウイルス対策ソフト
    ・・・・・

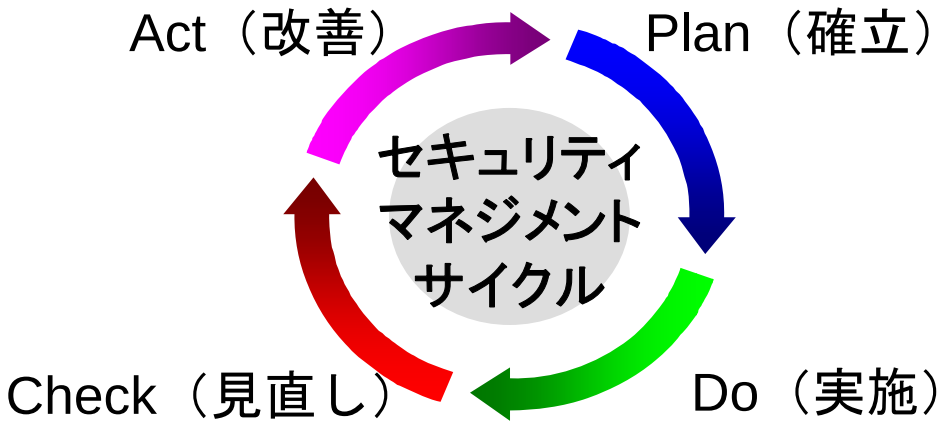
組織的対策の必要性

- そもそも人が一番のセキュリティホールである
- セキュリティソフトでは解決しない問題がある
- ソフトにはバグがある

- 情報セキュリティ対策は製品ではない。
  一連のプロセスである。

  IPA情報セキュリティ読本





3. 情報セキュリティマネジメントシステム

マネジメントシステムとは

マネジメントシステムの有効性

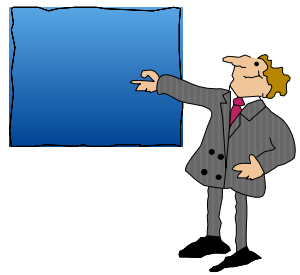
継続的改善

代表的なマネジメントシステムの規格

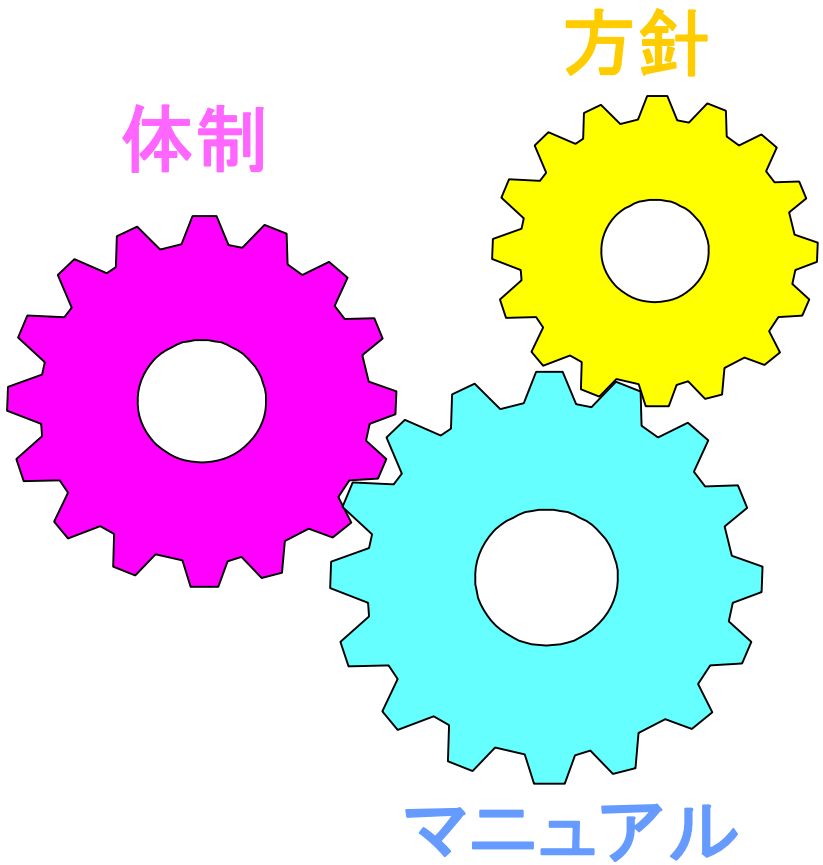
日本での認証取得状況

ISMSのサイクル

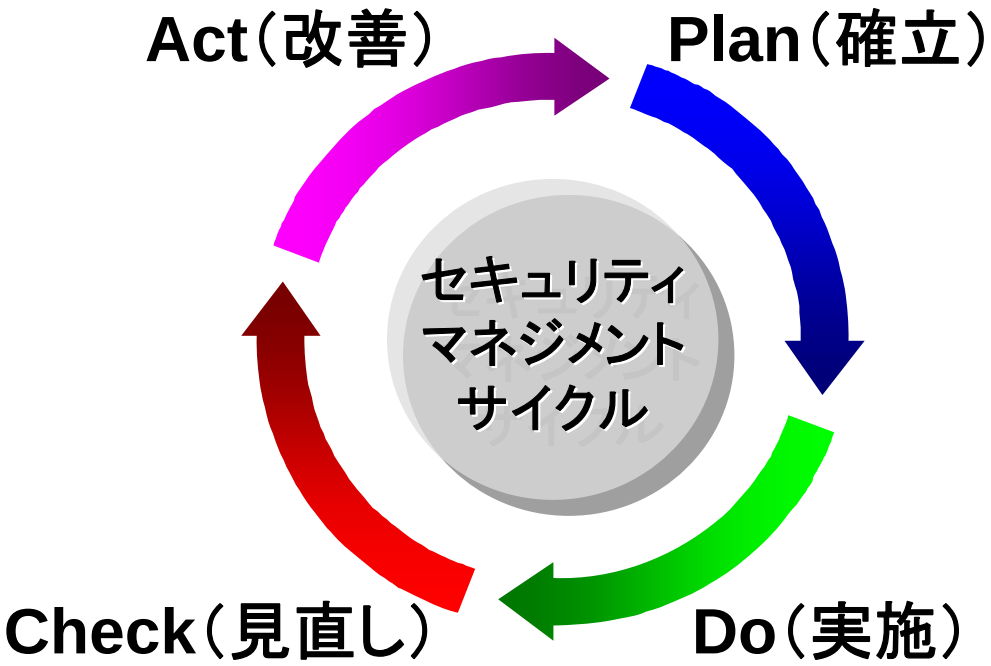
情報セキュリティ対策でのポイント



マネジメントシステムとは



マネジメントシステムとは



Plan	:	しごとのしかたを決める
Do	:	決めたことを決められたとおりやる
Check	:	ちゃんとできたか確認する
Act	:	もっと良くできないか考える

ISMSのサイクル

PDCA	項目	手順	作成文書・記録
Plan	確立	全体スケジュールの立案	ISMS活動計画
		ISMSマニュアルの作成 ・適用範囲の定義 ・セキュリティ基本方針の作成 ・体制の立案 ・マネジメントシステムの定義	ISMSマニュアルの作成 ・適用範囲 ・セキュリティ基本方針 ・体制
		文書と記録の管理手順の定義	文書管理・記録管理手順
	★	リスク評価・管理手順の作成	リスク評価・管理手順
	★	リスクの評価と管理	リスク評価・管理結果
	★	セキュリティ基準の作成	セキュリティ基準
	★	適用宣言書の作成	適用宣言書
	★	セキュリティ対策導入計画の作成	リスク対応計画
Do	導入及び運用	運用手順の作成	内部ISMS監査手順 是正処置・予防処置手順 システム運用手順など
	★	セキュリティ対策の導入	各種記録
		教育の実施	教育計画・記録
	★	運用	各種記録

ISMSのサイクル

PDCA	項目	手順	作成文書・記録
Check	監視及び見直し	ISMSの活動の監視 リスクの再評価 内部監査の実施 マネジメントレビューの実施	内部の監査計画 内部監査報告書 マネジメントレビュー報告書 他記録
Act	維持及び改善	改善 (問題の是正と予防)	是正処置・予防処置記録

マネジメントシステムのポイント

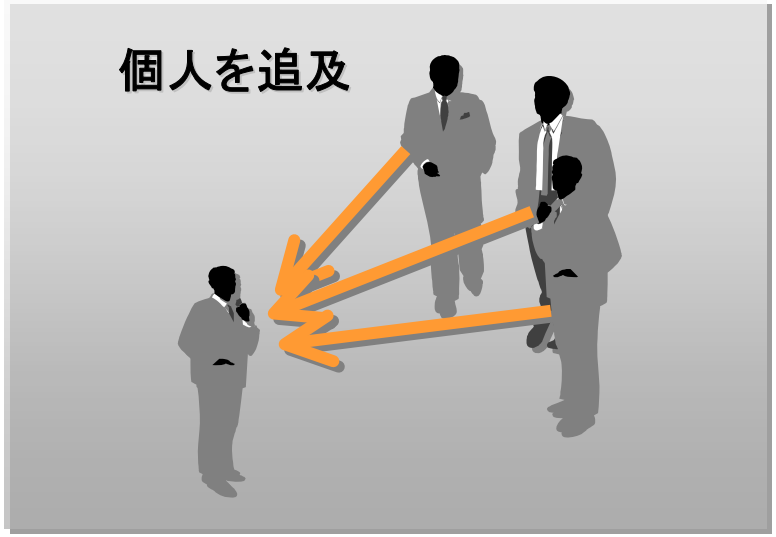
1. リスク評価
   - 「事実に基づく意思決定」（ISO9001の思想）
   - 被害額のイメージを持つ
2. 危機管理
   - 事故・天災は起こるという前提に立つ
   - 機器管理計画（事業継続計画）
3. 事故からの学習
   - プロジェクト管理、品質管理、人生、何でも同じ･･･地道に仕事の仕方を改善する
4. 継続的運用と習慣化
   - 桃栗3年柿8年
   - 教育・啓発活動
   - 認証制度の利用も有効
5. 監査
6. リーダーシップ
   - マネジメント

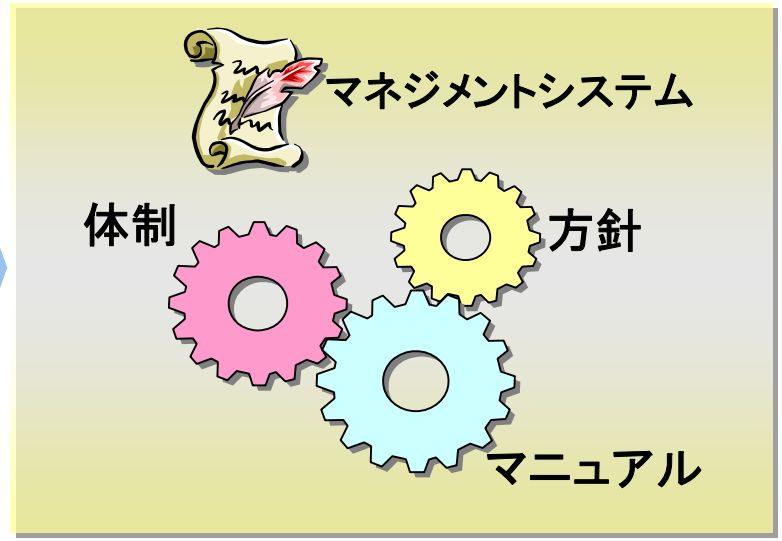
ITセレクト2002年8月号参照

事故からの学習

マネジメントシステムと問題発生時の対処

- 従来
  - 個人の責任を追及
- マネジメントシステムの導入
  - マネジメントシステムの欠点を分析し改善





代表的なマネジメントシステムの規格と認証制度

CERTIFICATION INTERNATIONAL
ISO 9001
Cert No: CI/0001

ISO9001

品質

ISO 14001 JACO JAB UKAS ENVIRONMENTAL MANAGEMENT

ISO14001

環境

マネジメント
システムの統合

BSI REGISTERED

2002年度版

BS7799

ISMS JIPDEC

Ver. 2.0

ISMS

たいせつにします プライバシー
B820016(01)

JIS Q 15001

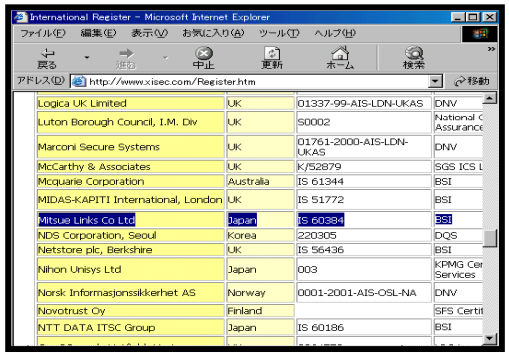
プライバシーマーク

1998年～

情報セキュリティ

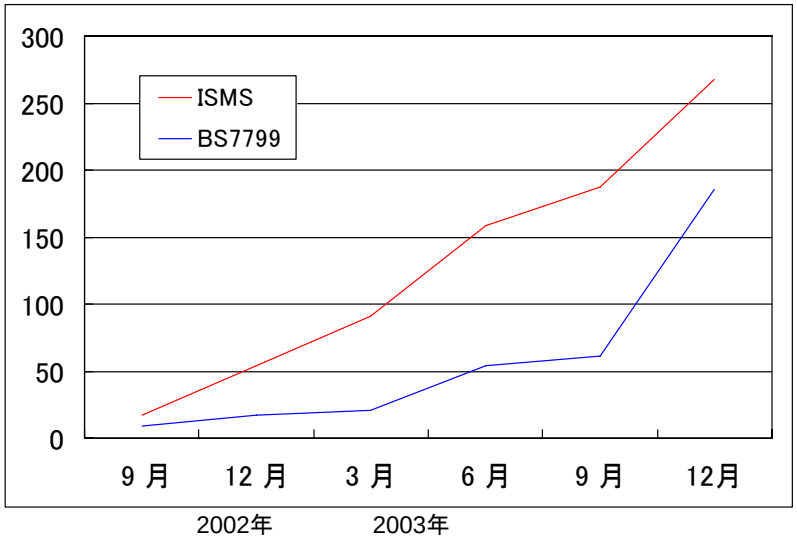
日本での認証取得状況

- BS7799
  - 英国規格、世界のデファクト
  - 2001年9月から
  - 186社取得（2004年1月現在）
    - http://www.xisec.com/



海外顧客へのアピール

- ISMS
  - BS7799と実質的に同じ
  - 日本情報処理開発協会（JIPDEC）が管轄
  - 2002年4月から
  - 268社取得（ 2004年1月現在）
    - 主にデータセンタ
    - 今後は各分野の事業者が取得
    - http://www.jipdec.or.jp/



国内顧客・官公庁へのアピール

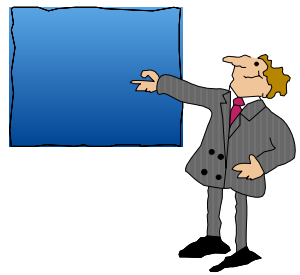
4. リスク評価とセキュリティ対策

リスク評価の必要性

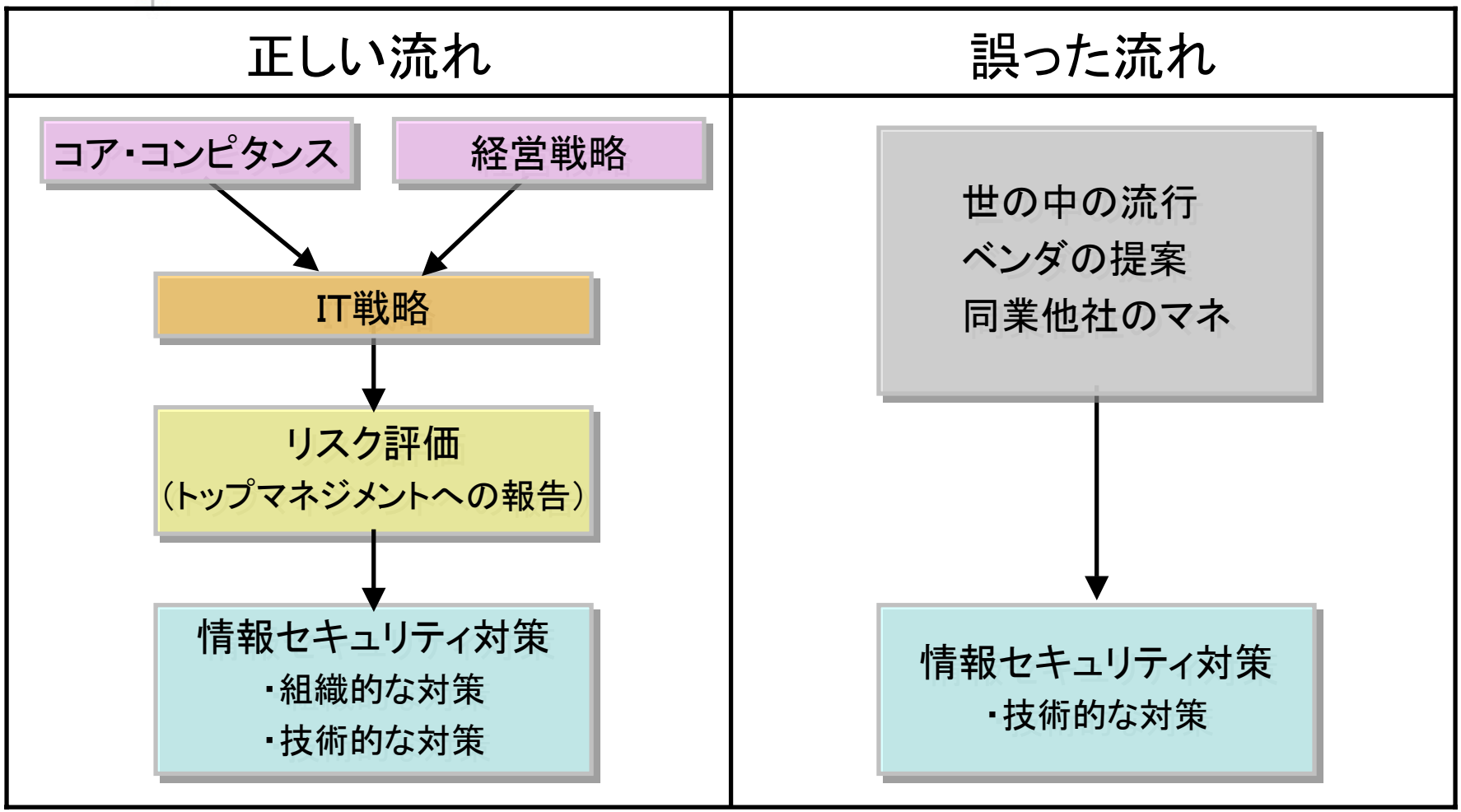
被害額のイメージを持つ

リスク評価の目的

リスク評価の手順



リスク評価の必要性

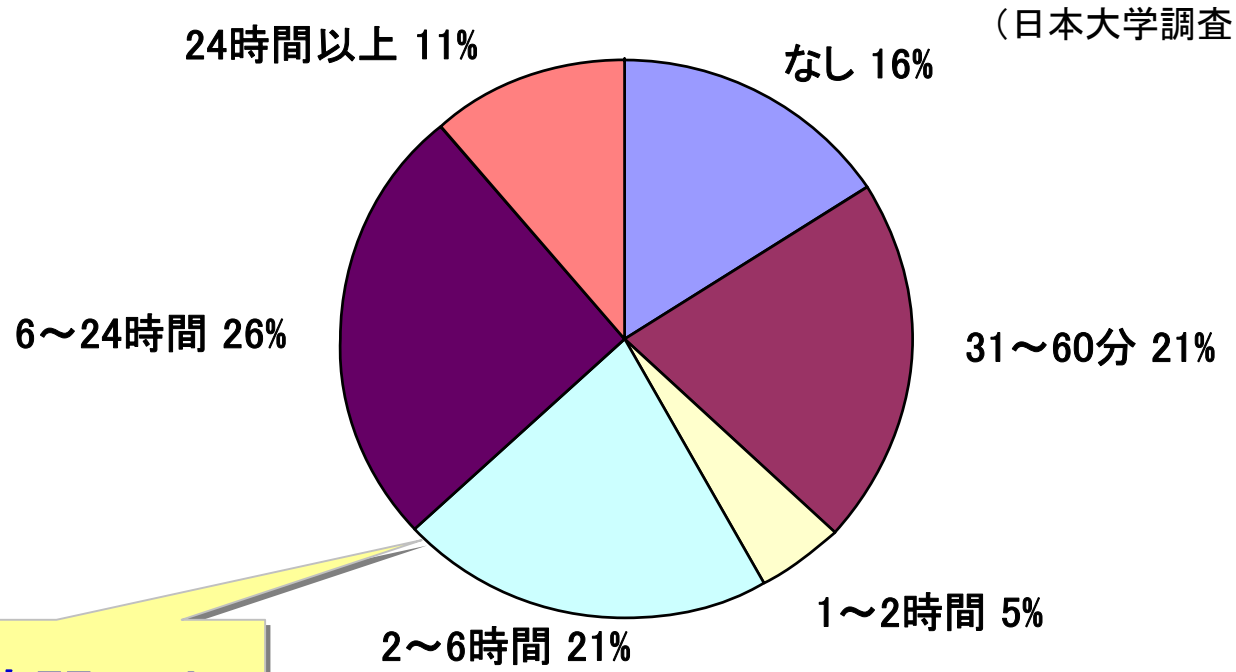


被害額のイメージ を持つ

【アンケート調査結果】企業利用ネットワークの信頼性実態

過去1年間の最大ダウン時間

（日本大学調査）



平均2時間以上

被害額のイメージ を持つ

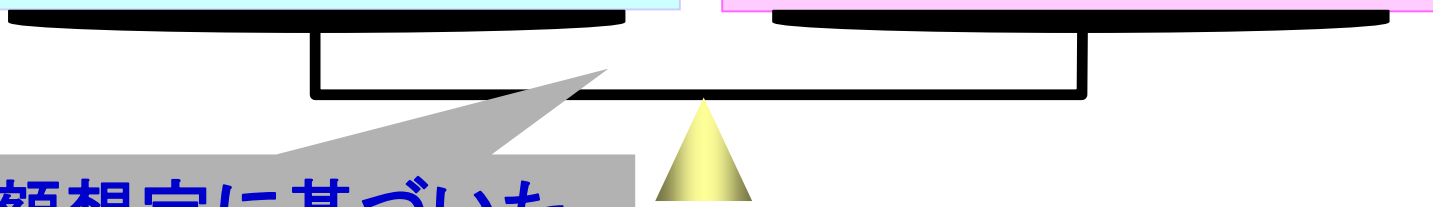
被害額

＝ ダウン時間 2 時間以上
＝ 1年間の業務時間の 0.1%
＋
その他の被害

適切な投資額

(経済産業省調査)
(KPMG調査)

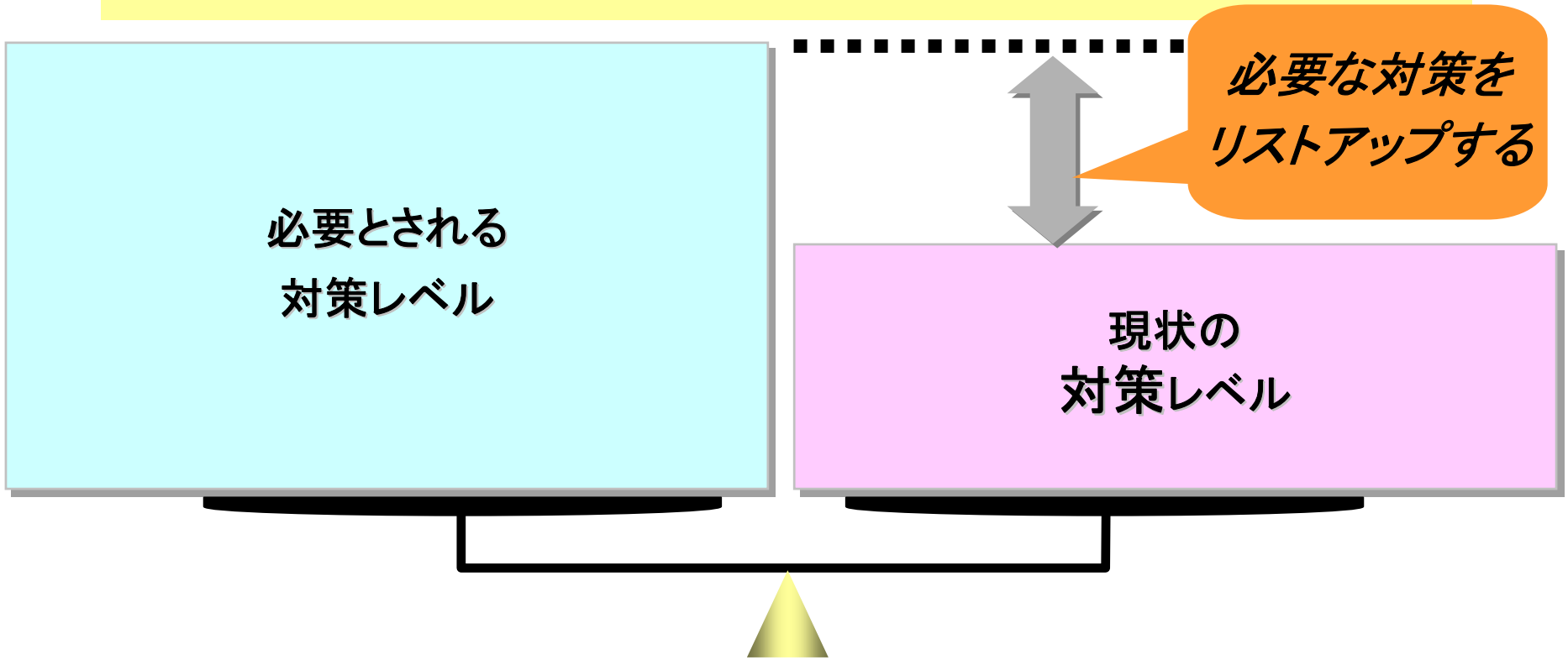
IT予算：売上高の1%
情報セキュリティ対策予算：
IT予算の10%
→ 売上高の0.1%



被害額想定に基づいた決定

リスク評価の目的

情報セキュリティ対策の実施状況



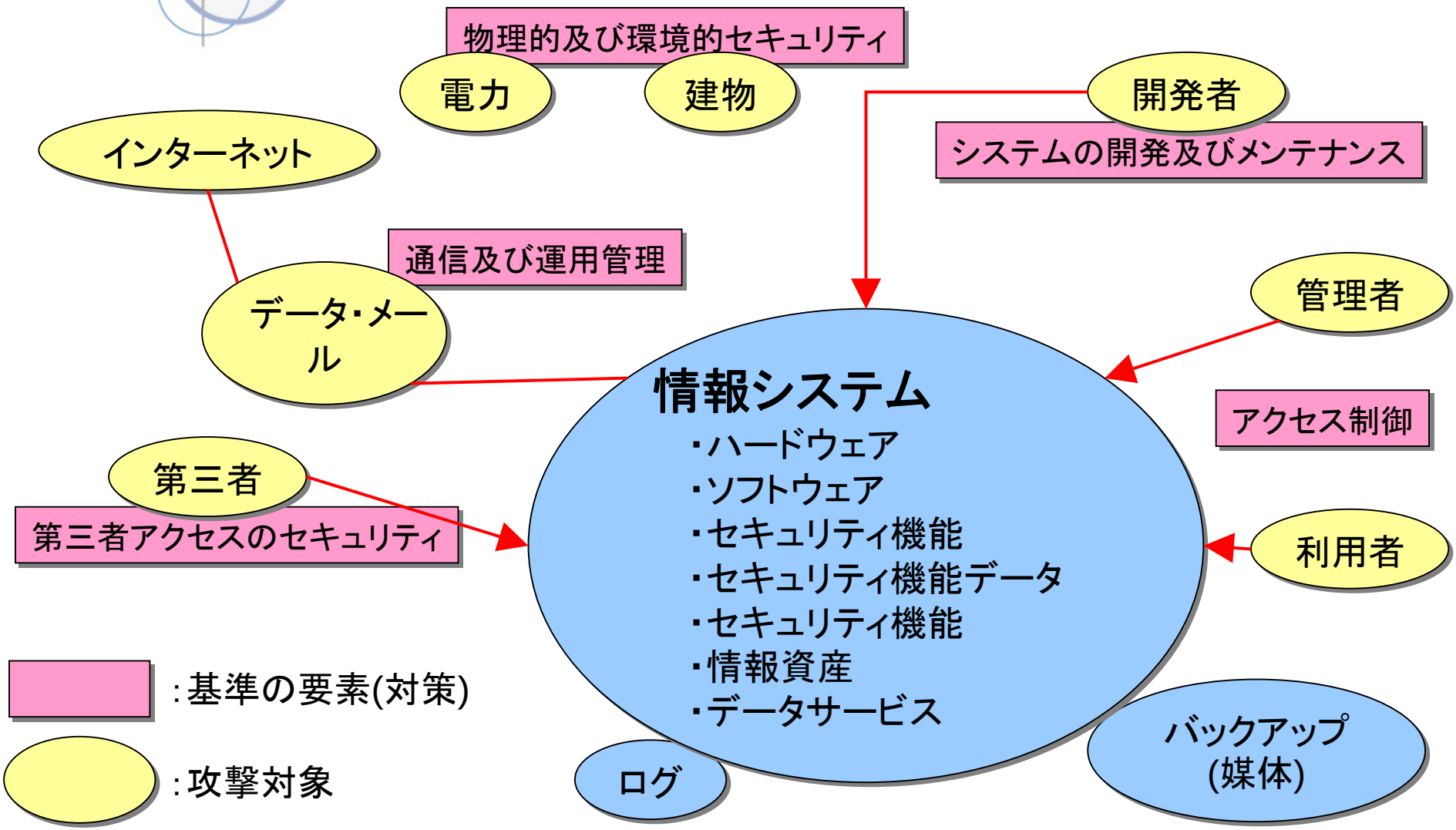
リスク評価の手順

1. セキュリティの現状の調査
2. 業務プロセスの分析
3. 情報資産のリストアップ
4. 情報資産の被害額評価
5. 情報資産に対する脅威のリストアップ
6. 脅威に対する情報セキュリティ対策立案

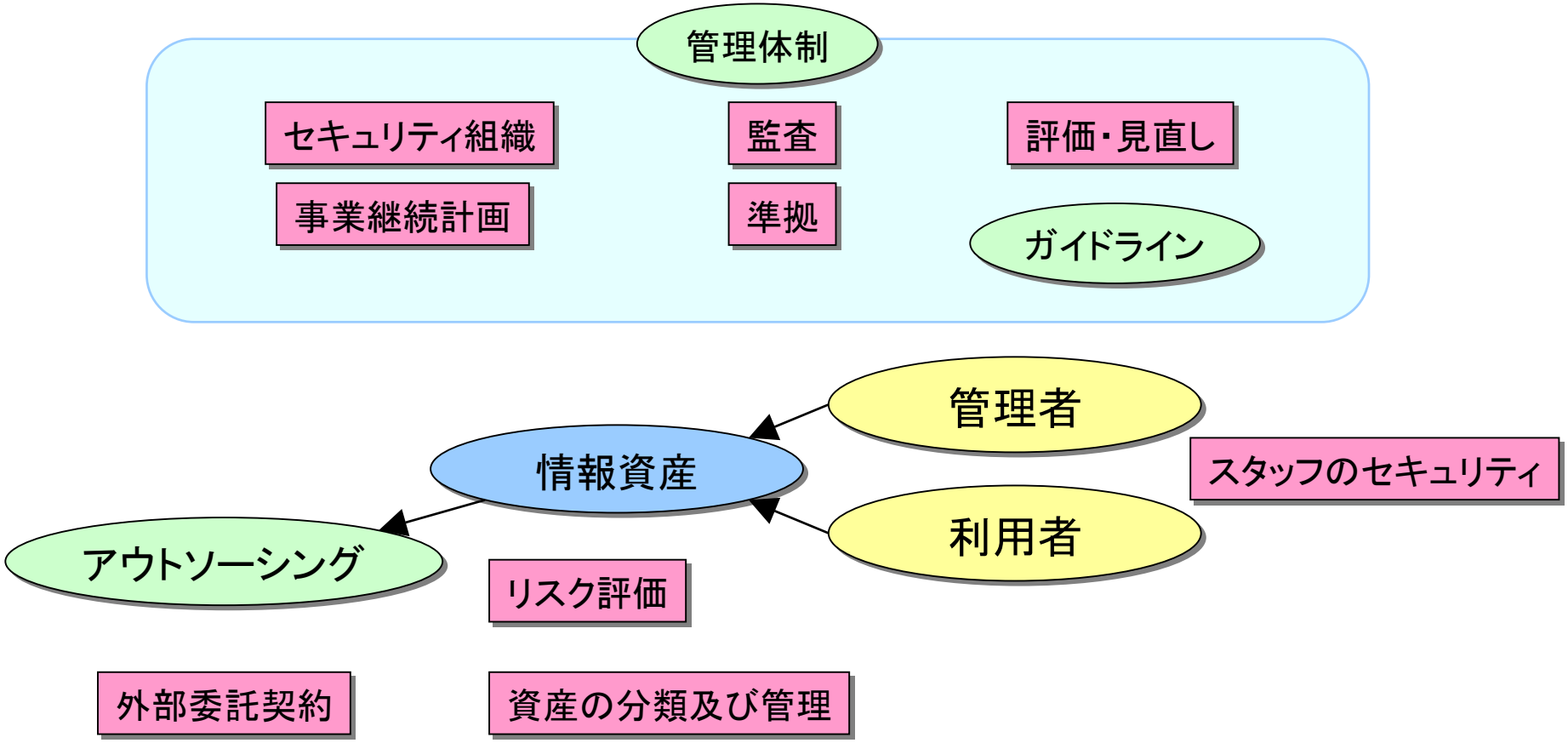
リスク管理

1. 情報セキュリティ対策の選択
2. セキュリティ基準の作成

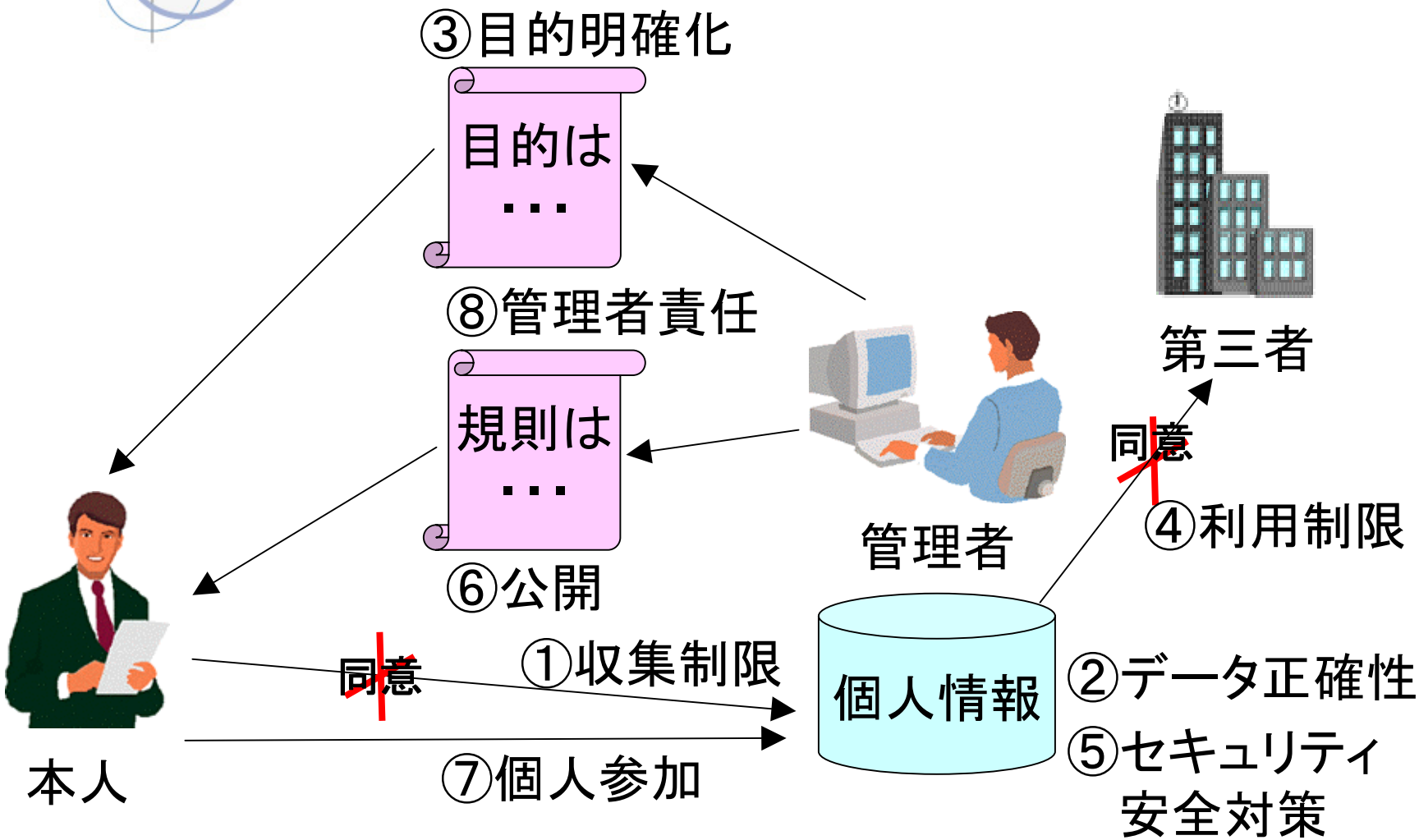
セキュリティ対策



セキュリティ対策（マネジメント）



個人情報に関するOECD8原則



個人情報の保護に関する法律　第四章　個人情報取扱事業者の義務等

個人情報の流れ

情報主体（本人）

直接収集

事業者

提供

他組織
（個人情報利用）

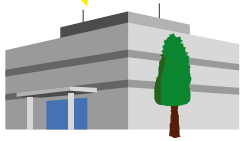
個人情報

預託

処理結果

直接収集

間接収集



他組織

預託

他組織
（情報処理）

預託の連鎖

他組織
（情報処理）

5. 導入事例(ミツエーリンクス殿)

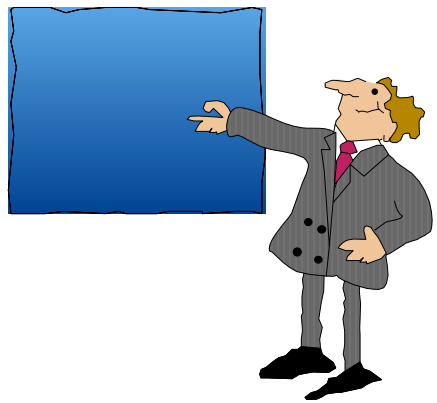
BS7799認証取得

認証取得の範囲・登録日

認証取得の目的

認証取得の難しさ

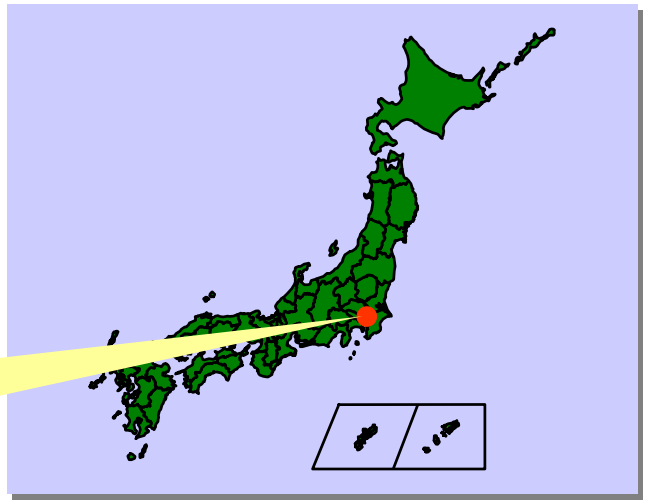
認証取得後に感じたメリット



BS7799認証取得

ミツエーリンクス殿

- 業種
  - Webサイト構築・マルチメディアコンテンツ制作のサービス提供
  - URL：http://www.mitsue.co.jp/
- 従業員数
  - 約100名



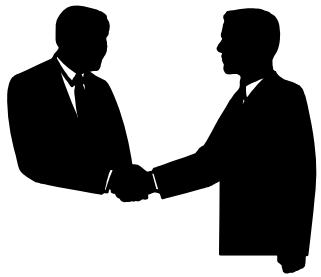
認証取得の範囲･登録日

- 適用範囲
  - デジタルコンテンツの制作及びサーバー管理事業の運営における情報セキュリティ管理
  - 全社レベルで取得
- 登録日
  - 2001年9月5日（ISMSは2002年8月15日）
  - 国内で初取得の3社のうちの一つ

日立ソフトがコンサルティング

認証取得の目的

1. プロセス管理の導入
2. 組織内での価値観の共有
   - 共通言語・共通尺度に
3. 継続的なセキュリティの改善
4. 顧客との信頼関係の強化
   - 対外的な実力のアピール
   - よりよいサービス・製品の提供



企業の差別化戦略

認証取得時の難しさ

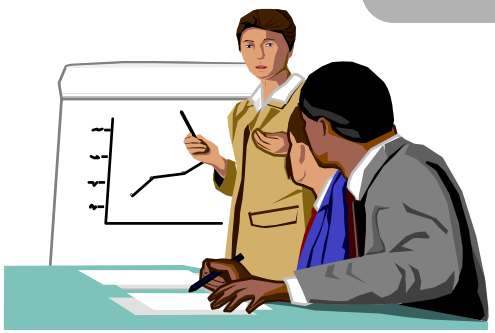
- 目標設定の自由度の高さ
  - 必要な対策レベルの把握の難しさ
- 取組の習慣化
  - 3ヶ月毎の情報資産の棚おろし
- 組織メンバの管理体制導入に関する疑問の解消
  - 100件以上の質問に対応

認証取得
成功の秘訣

認証取得後に感じたメリット

- 強制力を持った外部審査による継続的改善の維持
- 外部審査員の客観的な視点によるチェック

•半年/1年毎にサーベイランス
•3年毎に更新審査



システム規格社「月刊アイソス」2001年12月号参照

6. どうしたら導入できるか

ISMS策定のポイント

認証取得スケジュール案

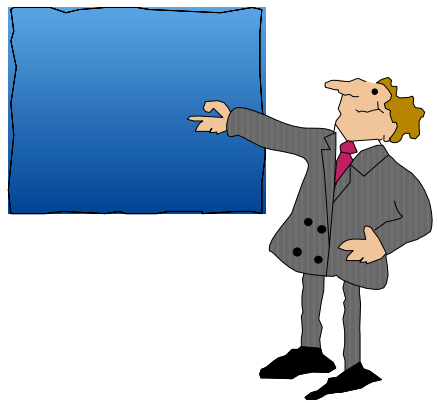
コンサルティングの必要性

コンサルへ頼む分野

コンサルティングの効果

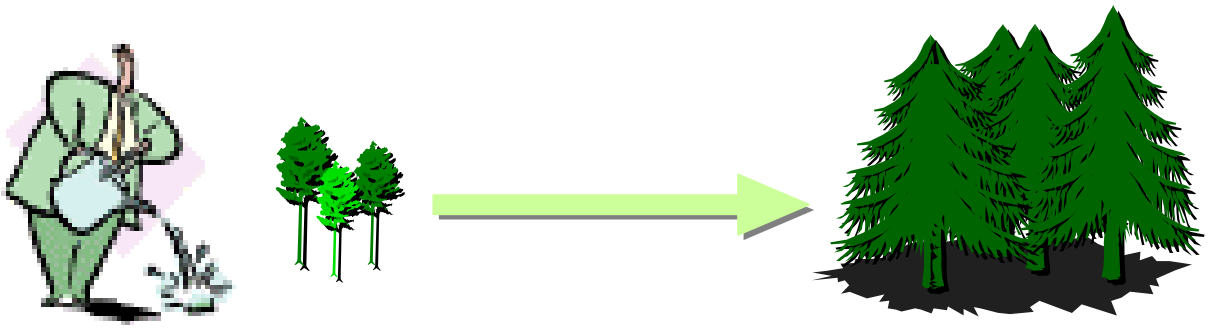
コンサルテーションの上手な利用法

よくある質問



ISMS導入のポイント

- 形式的な認証取得にこだわらない
  - 導入の機会に業務改善に役立てる
  - 従業員の意識向上を図る
- 文書化・対策の程度を正しく選ぶ
  - 業務・組織の文化に合わせる
- 継続的に改善していく
  - 小さく始めて大きく育てる



認証取得スケジュール案

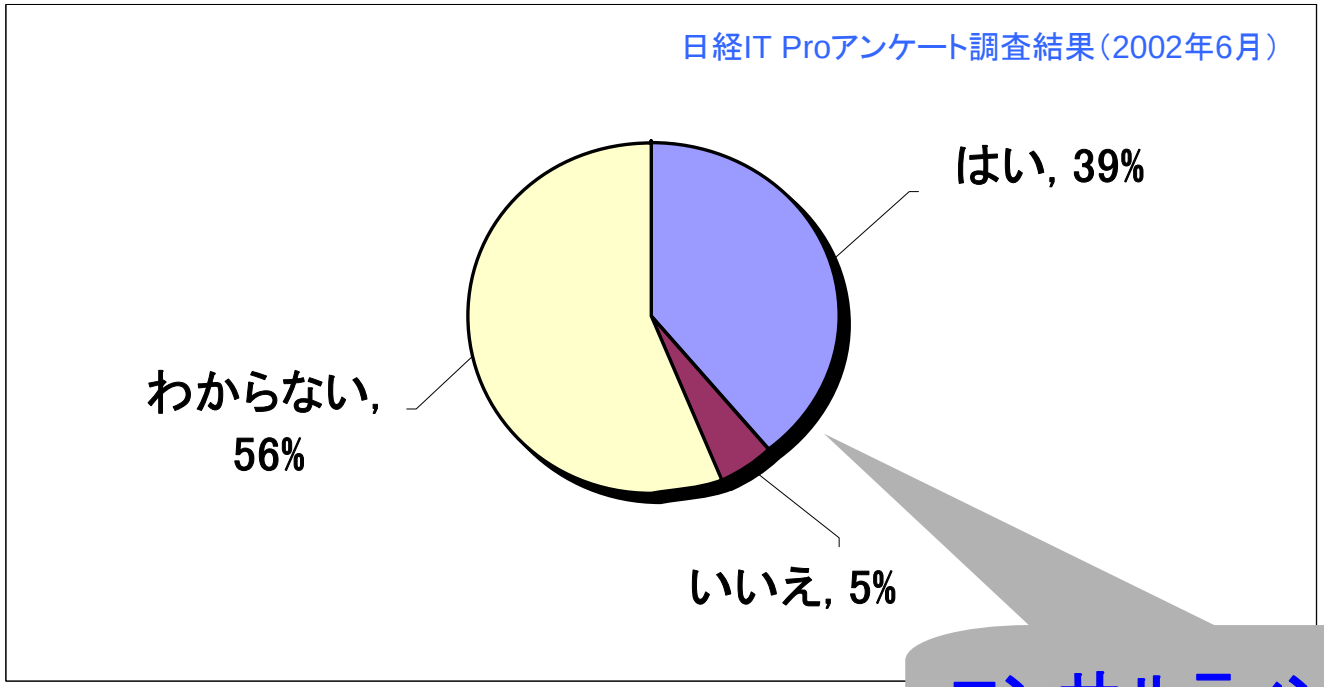
ISMS認証取得スケジュール案

フェーズ	作業	1	2	3	4	5	6	7	8	9	10	11	12
													（ヶ月）
フェーズ 1	管理体制確立												
	基本方針策定												
フェーズ 2	リスク評価												
フェーズ 3	対策基準策定												
フェーズ 4	手順書作成												
フェーズ 5	システム運用												
審査										▲予備審査		▲書類審査	▲本審査

ISMS構築に必要な期間	
ミツエーリンクス殿	5ヶ月
H13年度37社平均	7ヶ月
一般	12ヶ月

コンサルティングの必要性

- ISMS認証取得にはコンサルティングが必要ですか？



コンサルティングが必要と考える企業が多い

コンサルティングを頼む分野

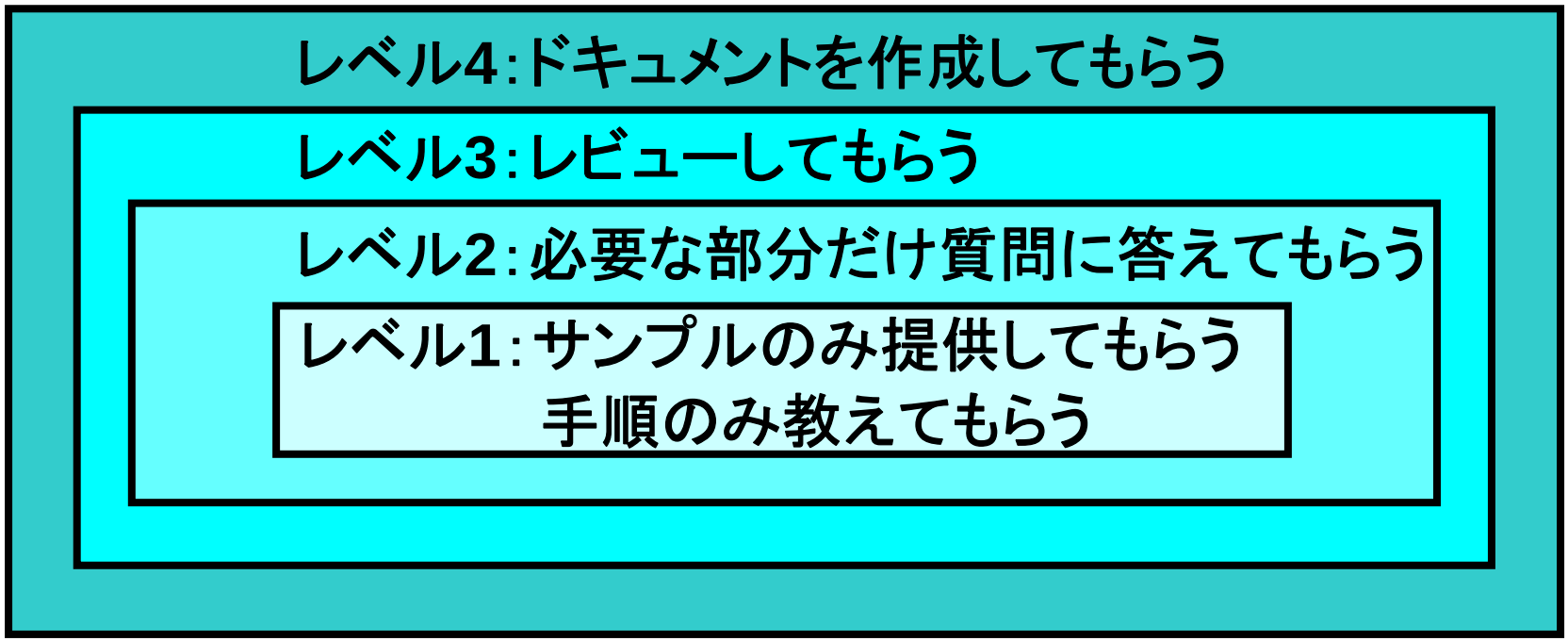
- ポリシー作成
- リスク評価
- 技術的対策立案
- 教育
- 監査

コンサルティングの効果

- 他社の導入事例について情報
- 管理者の負荷軽減(コスト減)
- セキュリティ対策の推進
- よりレベルの高い知識
- 外部の目から見た(客観的な)リスク評価

コンサルティングの上手な利用法

- 各フェーズ毎に利用レベルを選択する
- 自立して運用することを第一に考える



よくある質問

- Q1：ISMS適合性評価制度とBS7799の違いは？
- A1：ほぼ同じ。

  審査登録機関によっては、1度の審査で両方の認証を取得することが可能。
- Q2：認証審査に必要な費用は？
- A2：審査登録機関によって異なる。

  初回審査は200万円前後

  （対象範囲の従業員の人数、業務内容、情報資産の数 等で見積り）

  参考：http://www.isms.jipdec.jp/lst/isr/ (ISMS審査登録機関一覧)

7. まとめ

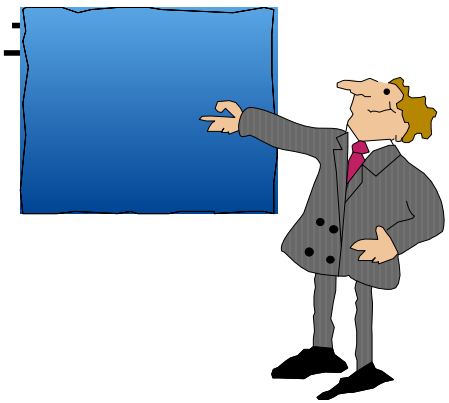
企業風土

まずどうする？システム監査

システム監査

情報システムのセキュリティ設計レビュ

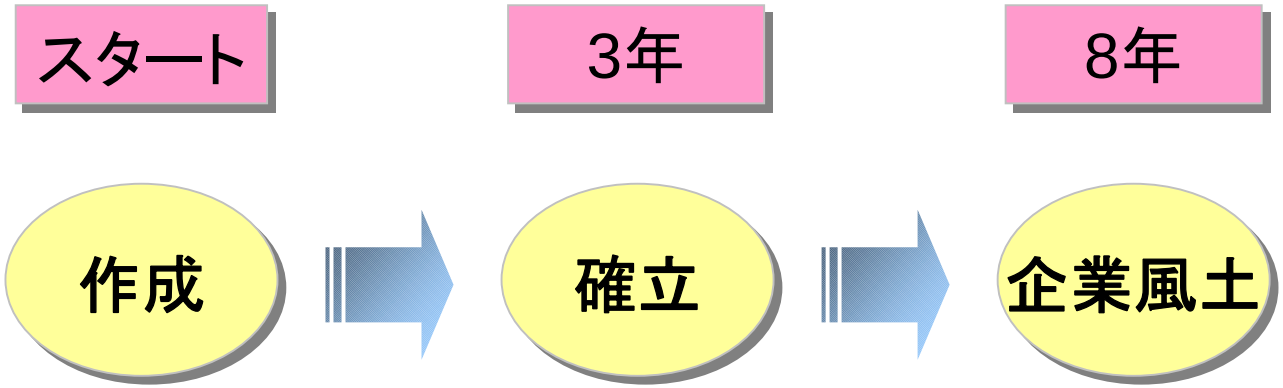
まとめ



企業風土

- システムより風土が大事

「なぜかお客が集まるサービス逃げるサービス」山崎宣次 より



マネジメントシステムの成長

まずどうする？ システム監査

BS7799／ISMS 認証制度

http://www.xisec.com/
(BS7799)

プライバシーマーク

http://www.isms.jipdec.jp/
(ISMS)

http://privacymark.jp/
(プライバシーマーク)

システム監査

情報セキュリティ監査

システム監査
企業台帳

情報セキュリティ
監査企業台帳

経済産業省

リスク評価
現状調査

「システム監査のすすめ」

システム監査

- 人による監査
- ツールによる脆弱性診断
- 情報システムのセキュリティ設計レビュー
  - 1. ISO15408 ITセキュリティ評価基準
    - 開発プロセス
    - セキュリティ機能
  - 2. セキュアプログラミング(実装の確実性)

まとめ

- 情報セキュリティ対策は製品ではない
- 一連のプロセスである
  - マネジメントシステム(ISMS):継続的改善
  - リスク評価
- ISMS認証取得
  - コンサルティングが推進力
- システム監査のすすめ

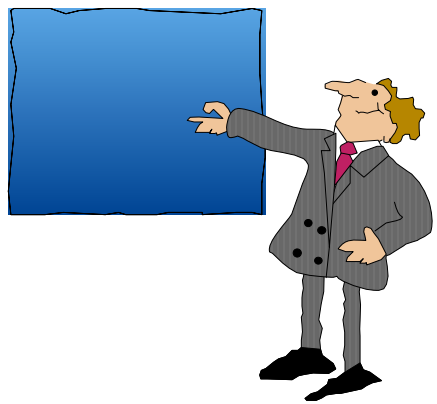
付録

情報セキュリティ 関連図書

日立ソフトのクロスインダストリーソリューション

日立ソフトのコンサルテーションサービス

日立ソフトのコンサルテーション実績

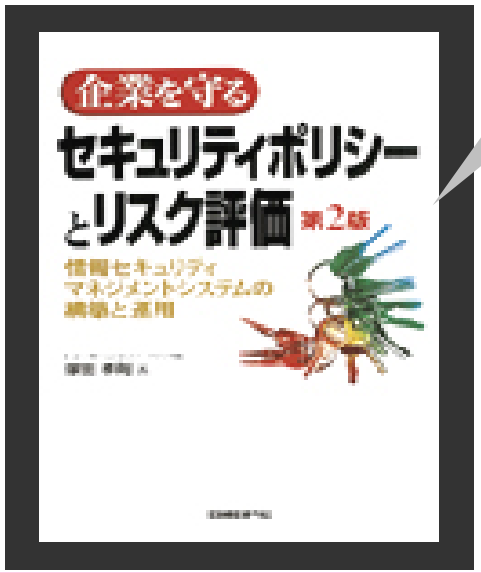


情報セキュリティ 関連図書

日経BP社 にて紹介中

企業を守る セキュリティポリシーと リスク評価

情報セキュリティマネジメントシステムの構築と運用
2003年5月



第2版

塚田孝則 著

目次

情報セキュリティ 関連図書

日経BP社 にて紹介中

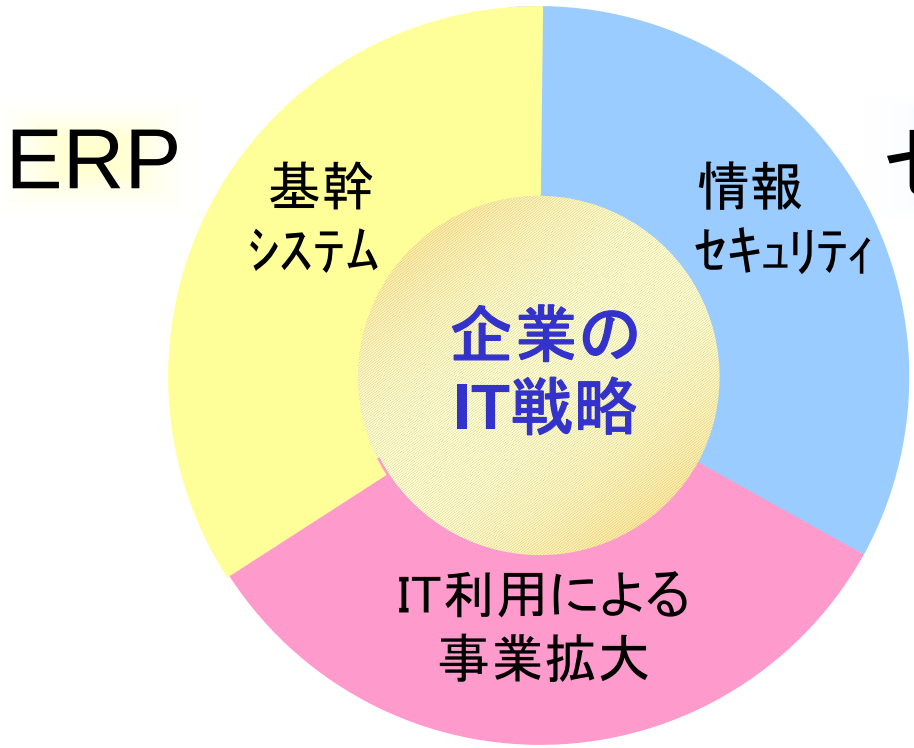
企業システムのためのPKI

公開鍵インフラストラクチャの構築・導入・運用
2001年12月

塚田孝則 著

目次

日立ソフトのクロスインダストリーソリューション



日立ソフトのセキュリティコンサルテーション

分野	コンサルテーション内容	主な実績
セキュリティポリシー	企業としての情報セキュリティリスク分析・セキュリティポリシー策定支援、BS7799、ISMS、プライバシーマーク認証取得支援	BS7799認証取得支援コンサルテーション（日本初取得3社のうちの1社：ミツエーリンクス殿） ●http://www.mitsue.co.jp/
		雑誌特集記事での紹介 ●月刊「ITセレクト」2002年12月号での紹介 ●月刊「ITセレクト」2002年8月号
		IPA殿平成14年度「情報セキュリティ監査支援技術の調査」、「エンタープライズネットワークのセキュリティ」、「インターネットサーバーの安全性向上策に関する調査」の3件採択 ●http://www.ipa.go.jp/security/index.html
セキュリティ設計	情報システムの開発でのセキュリティ上の脅威分析と対策策定、「ISO15408」に基づくセキュリティ設計	IPA殿平成13年度電子政府向け「電子申請業務における X.509 属性証明書を用いた資格確認技術の開発」採択 ●http://www.ipa.go.jp/security/fy13/detail.html
PKI	PKIの整備、認証局構築、ディレクトリ構築、暗号メール、アクセスコントロールなどの、PKIを用いたアプリケーションの開発・構築	IPA殿平成13年度電子政府向けプロテクションプロファイル「属性証明書管理・利用ツール（上記）」「PKIスマートカード」2件の作成 ●http://www.ipa.go.jp/security/ccj/dnldhome.htm

日立ソフトのコンサルテーションサービス

サービス名		サービスコンポーネント
リスク分析 セキュリティポリシー策定支援		リスク分析支援
		セキュリティポリシー策定支援
		BS7799・ISMS認証取得支援
		プライバシーマーク認証取得支援
		情報セキュリティ実施手順書作成支援
		情報システム調達及び委託におけるセキュリティ確保ガイドライン作成支援
		情報セキュリティ監査支援
		システム監査支援
セキュリティ設計書作成支援 セキュアシステム構築支援		システム設計におけるセキュリティ分析支援
		プロテクションプロファイル作成支援
		セキュリティターゲット作成支援
		ISO15408認証取得支援
コンテンツフィルタリングシステム構築		メールフィルタリング設計支援
PKIシステム構築	ディレクトリ設計支援	ディレクトリ設計支援
	PKIシステム設計支援	PKIアプリケーション設計支援
		認証局運用設計支援
アクセスコントロールシステム構築		アクセスコントロール設計支援

DIGITAL&GLOBAL 日立ソフト

日立ソフトのコンサルテーション実績

DIGITAL & GLOBAL

項番	サービス名	顧客	履行期間	技術的特徴
1	BS7799認証取得支援 コンサルテーション	ミツエーリンクス殿 （情報サービス業）	2001年3月 ～2001年5月	組織の全業務に関する詳細なリスク評価、対策策定 **（日本初のBS7799認証取得）**
2	セキュリティポリシー作成支援コンサルテーション	日東電工（製造業）	2001年8月 ～2001年9月	セキュリティ基本方針策定、リスク評価、セキュリティ基準作成、運用手順書体系見直し、教育計画策定に関するアドバイス
3	情報セキュリティ対策 レベル評価	コンピュータソフトウェア 開発A（金融）	2001年10月 ～2001年11月	情報セキュリティに関するIT投資方針の提案、外部委託での問題点分析と対策策定
4	インシデントレスポンス （事故処理手順）	中央官庁B	2001年10月 ～2001年11月	インシデントレスポンス体制の現状とウィルスについての調査
5	ISMS認証取得支援 コンサルテーション	サービス業C （公共料金徴収代行）	2002年7月 ～2003年3月	体制・ISMS策定、対象業務に関する詳細なリスク評価、対策策定、手順書整備、運用での教育・監査実施に関するアドバイス
6	プライバシーマーク取得 支援	データセンタD （金融・公共）	2002年9月 ～2003年3月	組織の全業務に関する詳細な個人情報のリストアップ、リスク評価、対策策定、個人情報保護規則類一式策定
7	BS7799・ISMS認証取得 支援コンサルテーション	中央官庁外郭団体E	2002年10月 ～2003年3月	体制・ISMS策定、対象業務に関する詳細なリスク評価、対策策定、手順書整備、運用での教育・監査実施に関するアドバイス
8	インターネットサーバーの安全性 向上策調査報告書作成	情報処理振興事業協会（IPA）	2003年1月 ～2003年3月	インターネットサーバーへのDoS攻撃等に関する対策を網羅的に記述
9	システム監査	中央官庁J	2003年3月	システム監査の実施監査計画の作成
10	セキュリティポリシー作成支援コンサルテーション	県庁F（地方自治体）	2003年6月 ～2004年3月	セキュリティ基本方針策定、リスク評価、セキュリティ基準作成、運用手順書体系見直し、教育・監査の実施

他多数

お問合せ先

DIGITAL&GLOBAL
日立ソフト
HitachiSoft

お問合せ先（情報セキュリティコンサルテーションサービス）

TEL: 03-5780-3681　9:00 - 12:00, 13:00 - 17:30（土日祝日および弊社休業日を除く）
E-Mail: sec-info@ari.hitachi-sk.co.jp （24時間）
URL：http://www.hitachi-sk.co.jp/Products/sec/
住所: 〒140-0002　東京都品川区東品川4丁目12番6号　日立ソフトタワー　セキュリティビジネス部