JNSA

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

1年で準備する個人情報保護法対策

個人情報保護法施行まで後1年と迫った。また、情報漏えい事件は相変わらず多発し、企業は、保護法への対策が急務となっている。
よって、当セミナーでは、以下を説明いたします

1．個人情報保護法の最新動向、
2．1年間ですべき個人情報保護法への対策

平成　16年　5月　18日

個人情報保護ガイドライン作成ワーキンググループ　リーダー
㈱大塚商会　　佐藤　憲一

JNSA書籍

個人情報保護法対策
セキュリティ実践マニュアル

著者：NPO JNSA 個人情報保護ガイドライン
作成ワーキンググループ
発売：インプレスコミュニケーションズ
定価：¥3,500(税別)
発売日：2003年12月2日
ISBN：4-8443-1858-6

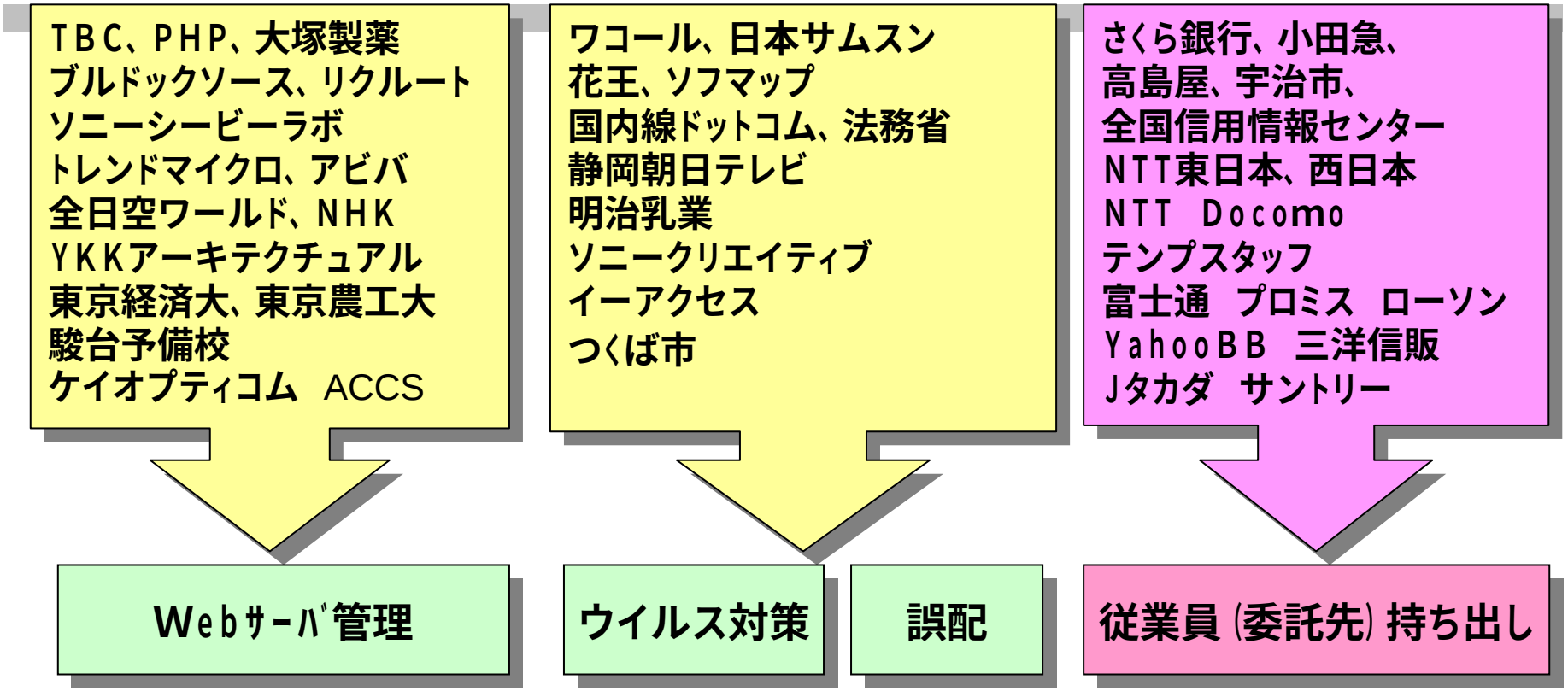
第1章　実態編　情報漏えいが企業を滅ぼす
第2章　入門編　個人情報保護法で何が変わるのか
第3章　導入編　社内の仕組み作りから始めよう
第4章　対策編　個人情報の取り扱いを事例で学ぼう
第5章　応用編　法令・規範の知識を広げよう
付　録　資料編
- 個人情報保護チェックリスト
- 規程・基準・契約書等サンプル
- 個人情報保護法・政令案全文
- JIS Q 15001:1999目次
- JIS X 5080:2002目次

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

個人情報の社会状況


DMがよく届く
電話勧誘が多い
情報主体
(本人)
サービス利用
(個人情報の提供)
事業者
内部からの漏洩
不正アクセス
ウイルス
外部 (インターネット)
からの漏洩
名簿業者など
個人情報の売買、漏洩
個人情報保護
・ 何から行なえば良いか
・ どの程度の対策が妥当か
・ 個人情報保護法に従えばOKか

個人情報流出の事例



① **従業員、元従業員、委託業者、派遣社員、取引先等からの不正持ち出しによる漏洩**
② 個人情報を記載した書類、PCを含む電子媒体等の紛失
③ システムの設定ミス、システム管理者の認識不足による、Webサイトからの個人情報閲覧
④ メール配信時の誤配信、ウイルス付きメールの配信

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

政府の個人情報関連スケジュール

《平成15年》

5月30日　個人情報保護法　公布

12月10日　同　政令　公布

《平成16年》

3月25日　基本方針の策定（内閣府・国民生活審議会）

5月中旬　経産省　同ガイドラインの策定

JIS　Q　15001　の改定

《平成17年》

4月　1日　個人情報保護法　全面施行

内閣府

http://www5.cao.go.jp/seikatsu/kojin/index.html

経産省

http://www.meti.go.jp/policy/it_policy/privacy/privacy.htm

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

講演のゴール

企業の経営者、情報システム室、及び総務部、人事部の方からの質問

① 政府の保護法に対する方針が見えない
② 保護法が企業経営に及ぼす影響がわからない
③ 保護法を遵守するために企業は、何を行えば良いのか　わからない
④ 個人情報漏洩の対策は、どこから何を手をつければ良いのか　わからない
⑤ 個人情報漏洩の対策は、どの範囲まで、強化すれば良いのか　わからない
⑥ 個人情報漏洩の対策を行うための基準がないのか

第一章　個人情報と個人情報保護法

第二章　個人情報保護法への具体的対処法

《 参考資料 》

Copyright (c) 2003-2004　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

第一章　個人情報と個人情報保護法

1．個人情報保護法　施行まで1年である

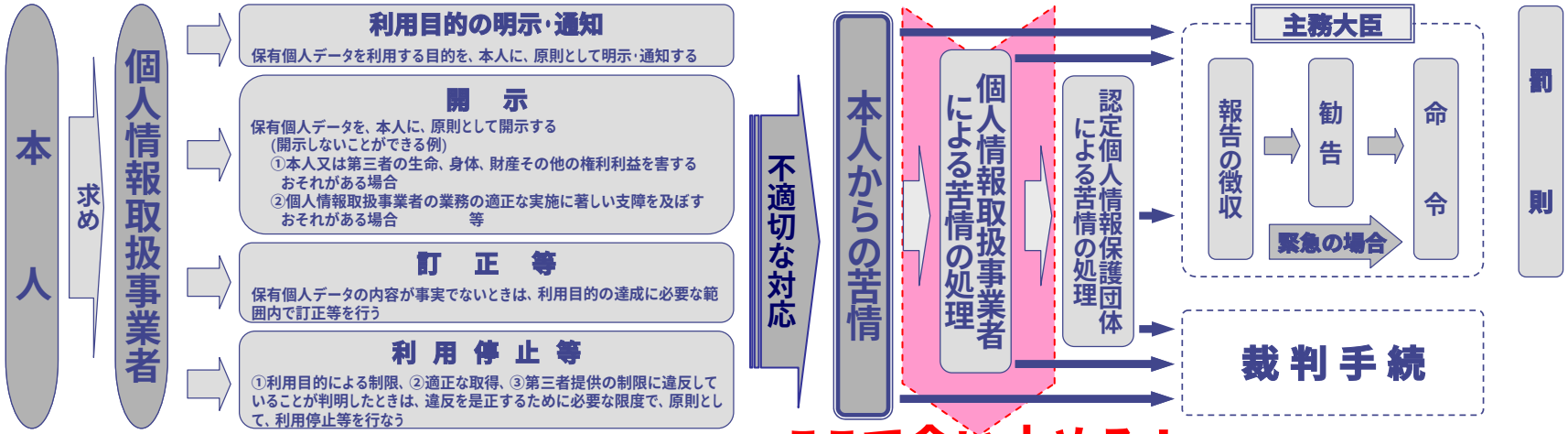
2．対象となる「個人情報」は、「顧客情報」＋「就業者情報」である為、ほとんどの企業は、この法律の対象となる

3．企業が遵守するための基本原則は、「本人の意思の尊重」と「安全性の確保」である

Copyright (c) 2003-2004　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

個人情報取扱事業者

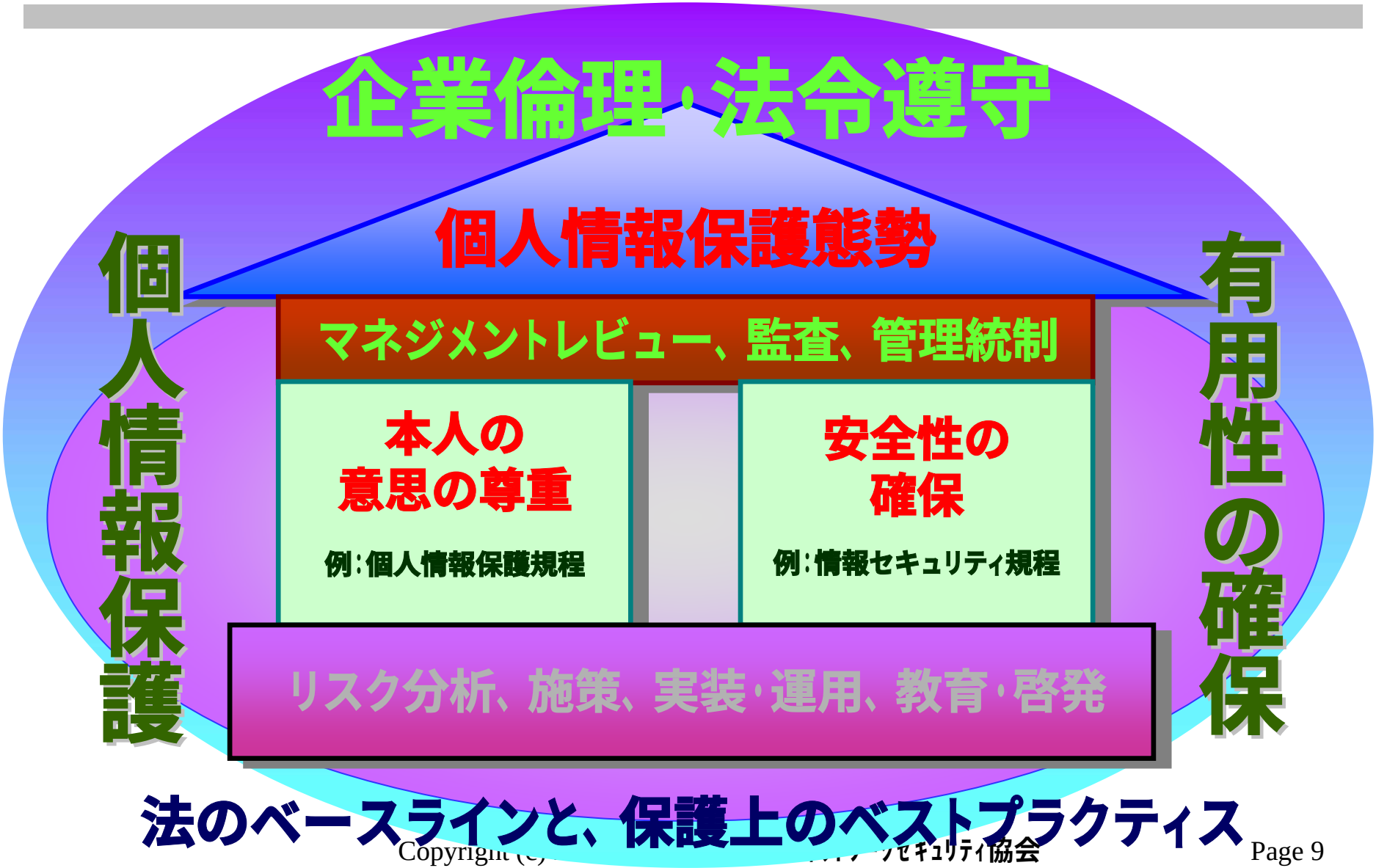
注:『「特定の個人の数」の合計が過去6月以内のいずれの日においても5千を超えない』場合も、**社会的信頼の確保**を考慮する必要がある。



※政府資料を基に作成

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

個人情報保護の２本柱


企業倫理・法令遵守
個人情報保護態勢
マネジメントレビュー、監査、管理統制
本人の
意思の尊重
例：個人情報保護規程
安全性の
確保
例：情報セキュリティ規程
リスク分析、施策、実装・運用、教育・啓発
個人情報保護
有用性の確保
法のベースラインと、保護上のベストプラクティス

個人情報

個人情報とは？

生存する個人に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ，それにより特定の個人を識別することができることとなるものを含む)。

個人情報の種類

基本的事項－ 氏名、住所、本籍・国籍、生年月日・年齢、性別、電話番号
写真、音声

心身の状況－ 保健医療、健康状態、病歴、障害、身体・精神の特徴、性生活
家庭生活　－ 家庭状況、親族関係、婚姻歴
社会生活　－ 職業・職歴、学歴、資格、賞罰、公的扶助、趣味・嗜好等の記録
資産・収入 － 資産/収入/納税/取引状況、銀行等カード情報、所持品
思想・信条 － 信教(思想・信条・宗教)、政治的見解、組合等への加盟

個人情報の取り扱い

JNSA

カテゴリ ＼ 法令・規範		個人情報保護法(第15条～第36条、第56条～第59条、附則第1条～第5条)	プライバシーマーク制度(JIS Q 15001:1999)
全般	レベル	「常識の範囲」のレベルを明確化したもの 企業が遵守すべき最低限のルール	「望ましい取扱い」のレベルを明確化したもの OECD8原則に基づくルール
	強制力	法律であり、適合することが当然	事業の要に応じて判断して申請する
	目標	悪くないようにする	大丈夫な状態にする
対象	管理レベル	Plan-Do(マネジメント)	Plan-Do-Check-Action(マネジメントシステム)
	対象領域	原則として社外の個人情報が対象	社外のみならず就業者の個人情報を含む
	個人の状態	原則として生存者のみ	生死問わず
	情報形態	原則としてデータのみ	形態問わず
	情報件数	大量	件数問わず
	保有期間	長期	期間問わず
	利用理由	事業の要	理由問わず
	取扱いレベル	量と期間に応じて取扱いが変わる	リスクに応じた取扱いをする
個人の権利の尊重	本人関与	オプトアウトを中心に要求	オプトインとオプトアウトの両方を要請
	事前同意	原則として同意は必要ない	同意が必要
	利用目的の開示	利用目的の通知、公表	利用目的の明示
	利用目的の内容	利用目的に特に規制なし	適切な利用目的が必要 範囲(物理・論理・取扱者、情報の機密度、権限　等)
	対情報主体	不安な相手にはならない	安心を与え、信頼を得る
賞罰	賞	適合して当然なのでインセンティブは無い	社会的信頼を得るというインセンティブあり
	罪決定の手順	報告の徴収→勧告→命令	報告書提出→実態調査→改善勧告・要請
	罪の決定	命令に適切に対処しない	申請に虚偽があった　または、 実態を改善・解消しない
	罰の内容	6ヶ月以下の懲役または30万円以下の罰金 社名は公表しない	認定の取消し 社名の公表

就業者情報含む
←2003/12　政令

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

個人情報取扱事業者の義務

JNSA

利用目的による制限：**利用目的の明確化、その達成に必要な範囲内での取扱い**
☆ 利用目的をできる限り特定しなければならない。（第15条）
★ 本人の同意なく利用目的の達成に必要な範囲を超えて取り扱ってはならない。（第16条）
☆ 個人情報の取得に際して利用目的を通知又は公表しなければならない。（第18条）
★ 本人の同意なく個人データを第三者に提供してはならない。（第23条）

適正な取得：**適法かつ適正な方法による取得**
★ 偽りその他不正の手段により取得してはならない。（第17条）

正確性の確保：**利用目的の達成に必要な範囲内で正確性、最新性を確保**
☆ 正確かつ最新の内容に保つよう努めなければならない。（第19条）

安全性の確保：**取扱いに当たり、安全管理のための措置が講じられるよう配慮**
★ 安全管理のために必要な措置を講じなければならない。（第20条）
★ 従業者・委託先に対する必要な監督を行わなければならない。（第21、22条）

透明性の確保：**取扱いに当たり、本人が適切に関与し得るよう配慮**
☆ 利用目的等を本人の知り得る状態に置かなければならない。（第24条）
☆ 本人の求めに応じて保有個人データを開示しなければならない。（第25条）
☆ 本人の求めに応じて訂正等を行わなければならない。（第26条）
☆ 本人の同意なき目的外利用等について、本人の求めに応じて利用停止等を行わなければならない（第27条）

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

個人情報取扱事業者の義務

JNSA

第２０条　(安全管理措置)

　個人情報保護取扱事業者は、その取り扱う個人データの漏えい、滅失又ははき損の防止その他の**個人データの安全管理のために必要かつ適切な措置**を講じなければならない。

第２１条　(従業員の監督)

　個人情報保護取扱事業者は、その従業員に個人データを取り扱わせるに当っては、当該個人データの安全管理が図られるよう、**当該従業員に対する必要かつ適切な監督**を行わなければならない。

第２２条　(委託先の監督)

　個人情報保護取扱事業者は、個人データの取り扱いの全部又は一部を委託する場合は、その取り扱いを委託された個人データの安全管理が図られるよう、**委託を受けた者に対する必要かつ適切な監督**をおこなわなければならない。

★印　→　　6ヶ月以下の懲役又は30万円以下の罰金 (第56条)

Copyright (c) 2003-2004 NPO日本ネットワークセキュリティ協会

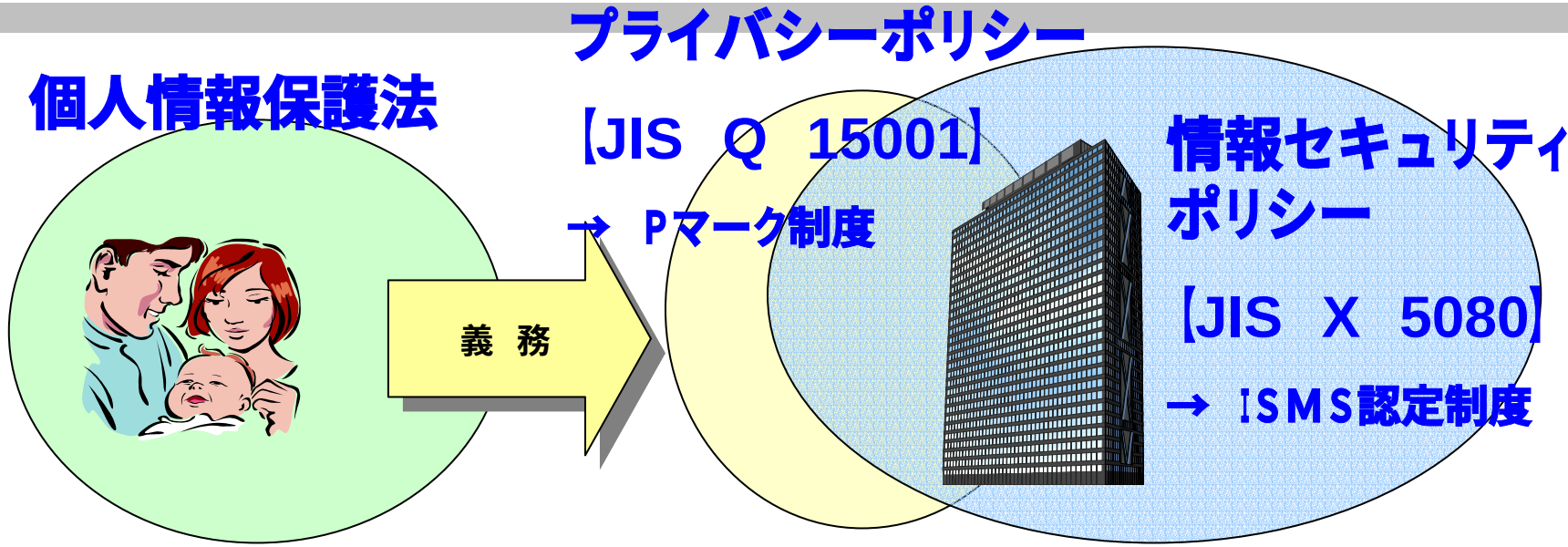
第二章　個人情報保護法への具体的対処法

1．個人情報保護法の対策規準は、
JIS Q 15001とJIS X 5080である

2．企業内の対処は、個人情報を直接取り扱う人（部署）から、全員参加で仕組み作りを行いましょう

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

法律、規格の関係



1. 個人情報保護法は、「顧客」を保護するために、「企業」に課せられた法律
2. 「企業」は、「顧客情報」の取り扱いを適切に実施するためのコンプライアンス（法令遵守）は、JIS Q 15001に基づき作成 ← **本人の意思の尊重**
3. 「企業」にとっての顧客情報は、今や「情報資産」である。この資産を適切に取り扱うためのコンプライアンスは、JIS X 5080に基づき作成 ← **安全性の確保**

Copyright (c) 2003-2004 NPO日本ネットワークセキュリティ協会

個人情報保護に関するコンプライアンス・プログラムの要求事項（JIS Q 15001）

本人の意思の尊重

0 序章
1 適用範囲
2 引用規格
3 定義
4 コンプライアン
4.1 一般要求事項
4.2 個人情報保護方針
4.3 計画
4.3.1 個人情報の特定
4.3.2 法令及びその他の規範
4.3.3 内部規定
4.3.4 計画書
4.4 実施及び運用
4.4.1 体制及び責任
4.4.2 個人情報の収集に関する措置
4.4.2.1 収集の原則
4.4.2.2 収集方法の制限
4.4.2.3 特定の機敏な個人情報の収集の禁止
4.4.2.4 情報主体から直接収集する場合の措置
4.4.2.5 情報主体以外から間接的に収集する場合の措置

個人情報の利用及び提供に関する措置
4.4.3.1 利用及び提供の原則
4.4.3.2 収集目的の範囲外の利用及び提供の場合の措置
4.4.4 個人情報の適正管理義務
4.4.4.1 個人情報の正確性の確保
4.4.4.2 個人情報の利用の安全性の確保
4.4.4.3 個人情報の委託処理に関する措置
4.4.5 個人情報に関する情報主体の権利
4.4.5.1 個人情報に関する権利
4.4.5.2 個人情報の利用又は提供の拒否権
4.4.6 教育
4.4.7 苦情及び相談
4.4.9 文書管理
4.5 監査
4.6 事業者の代表者による見直し

Copyright (c) 2003-2004 NPO日本ネットワークセキュリティ協会

情報セキュリティマネジメントの実践のための規範（JIS X 5080）

1.範囲
2.用語および定義
3.情報セキュリティ基本方針
　3.1情報セキュリティ基本方針文書
4.組織のセキュリティ
　4.1情報セキュリティ基盤
　4.2第三者によるアクセスのセキュリティ
　4.3外部委託
5.資産分類及び管理
　5.1資産に関する責任
　5.2情報の分類
6.人的セキュリティ
　6.1職務定義及び雇用におけるセキュリティ
　6.2利用者の訓練
　6.3セキュリティ事件・事故及び誤作動への対応
7.物理的及び環境的セキュリティ
　7.1セキュリティが保たれた領域
　7.2装置のセキュリティ
　7.3其の他の管理策
8.通信及び運用管理
　8.1操作手順及び責任
　8.2システム計画作成及び受入れ
　8.3悪意のあるソフトウェアからの保護
　8.4システムの維持管理
　8.5ネットワークの管理
　8.6媒体の取扱い及びセキュリティ
　8.7情報及びソフトウェアの交換
9.アクセス制御
　9.1アクセス制御に関する業務上の要求事項
　9.2利用者のアクセス管理
　9.3利用者の責任
　9.4ネットワークのアクセス制御
　9.5オペレーティング・システムのアクセス制御
　9.6業務用ソフトウェアのアクセス制御
　9.7システムアクセス及びシステム使用状況の監視
　9.8移動型計産処理及び遠隔操作
10.システム開発及び保守
　10.1システムのセキュリティ要求事項
　10.2業務用システムのセキュリティ
　10.3暗号による管理策
　10.4システム・ファイルのセキュリティ
　10.5開発及び支援過程におけるキュリティ
11.事業継続管理
　11.1事業継続管理の種々の面
12適合性
　12.1法的要求事項への適合
　12.2情報セキュリティ基本方針及び技術適合のレビュー
　12.3システム監査の考慮事項

安全性の確保

Copyright (c) 2003-2004 NPO日本ネットワークセキュリティ協会

個人情報保護法とJIS Q 15001

Copyright (c) 2003-2004 NPO日本ネットワークセキュリティ協会

対策のポイント

① まずは個人情報を特定しよう
② 個人情報取り扱いのプロセスを知ろう
③ 個人情報保護の管理状況を確認しよう
④ 個人情報のリスクを共通認識しよう
⑤ 利用目的をちゃんと決めよう
⑥ 提供、委託を管理しよう
⑦ 廃棄、削除、消去をきちんとしよう
⑧ 危機管理しよう
⑨ 個人情報保護の組織体制を創ろう
⑩ 態勢を維持向上しよう
⑪ 企業倫理とコンプライアンスに統合しよう
⑫ 計画立ててみんなで目的･目標を持って進めよう

リスク評価
(安全管理策検討)

利用目的、適正取得

委託先の監督
第三者提供

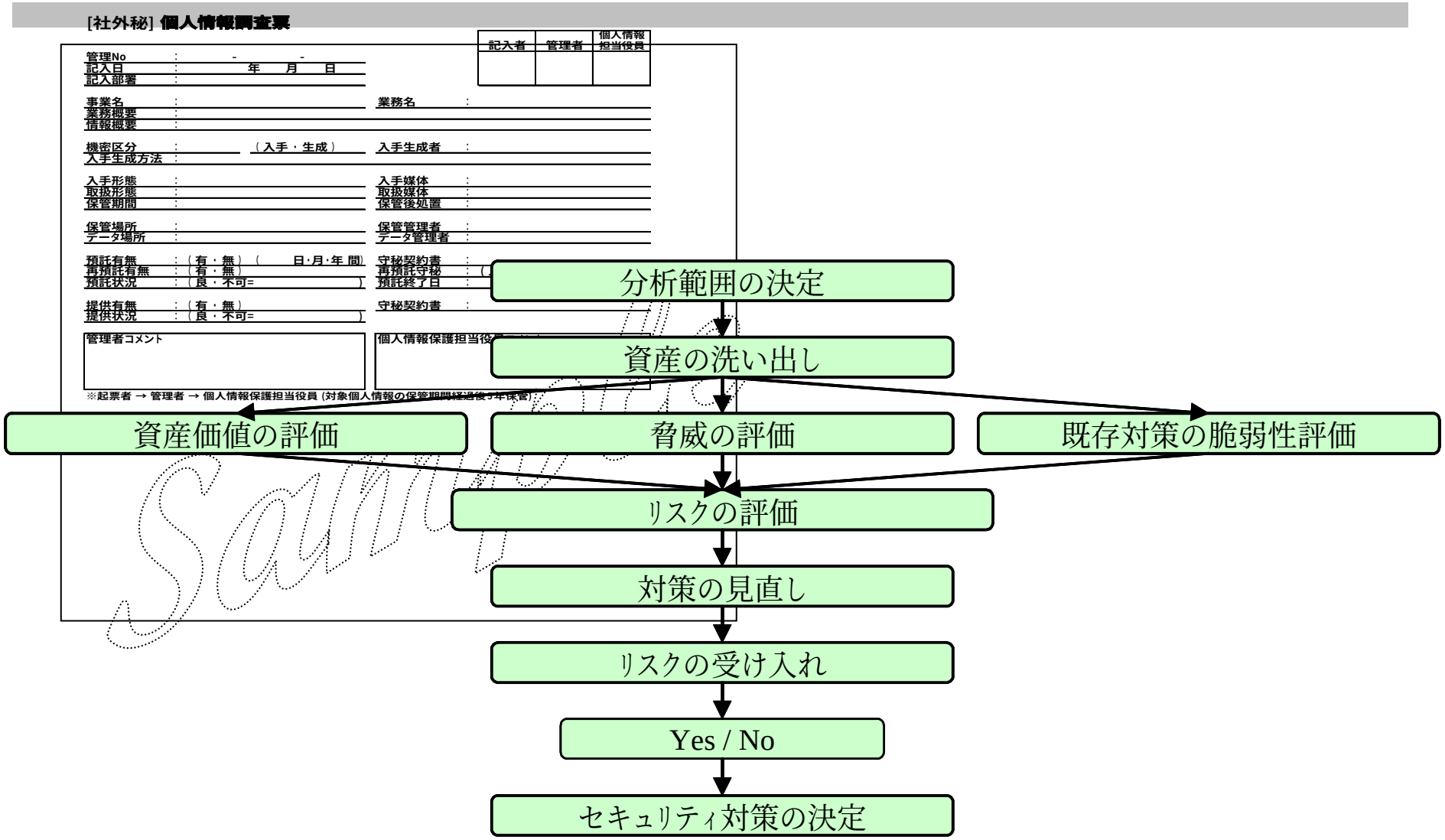
苦情処理、危機管理

従業員の監督

維持向上

Copyright (c) 2003-2004 NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

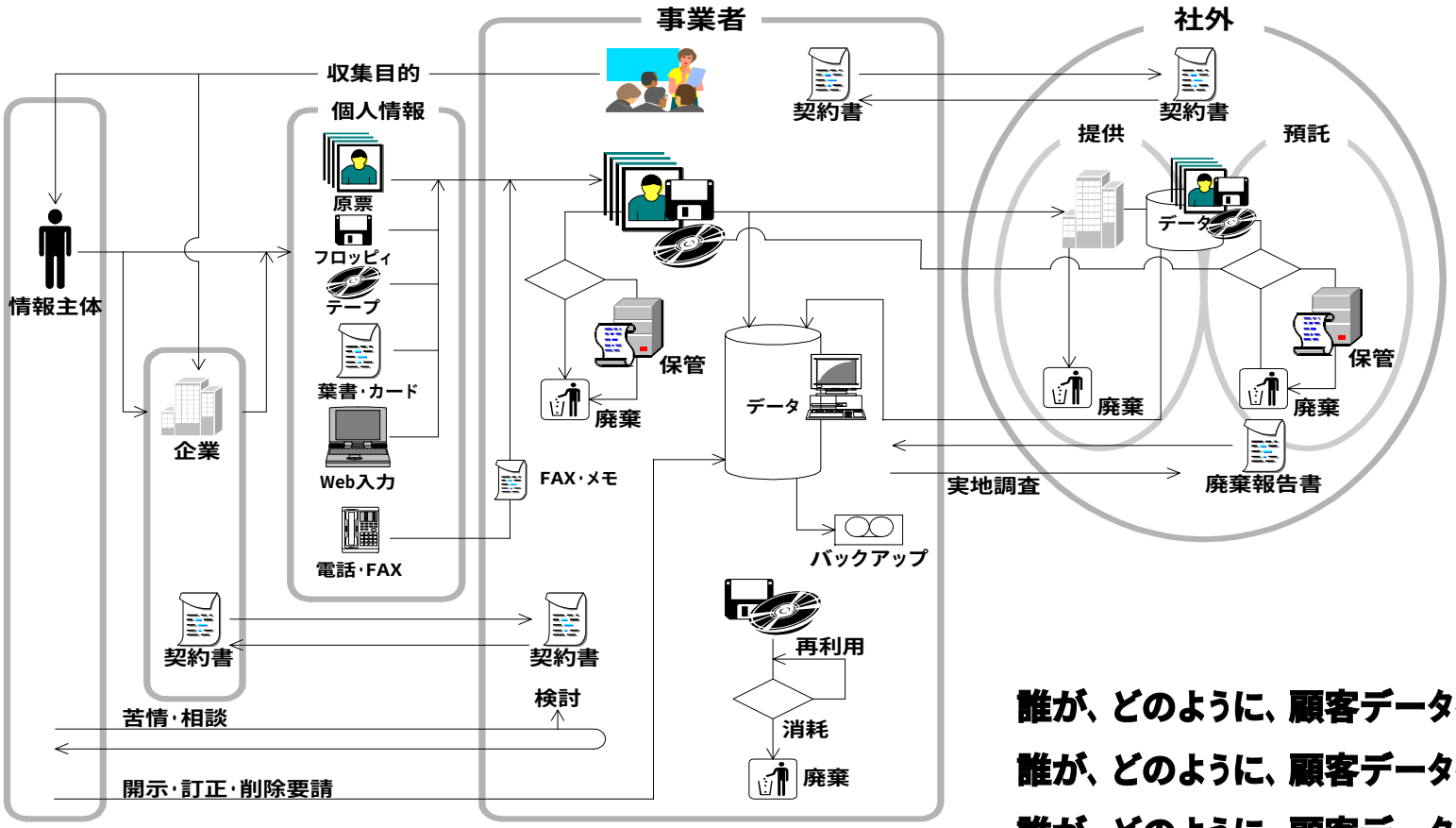
①まずは個人情報を特定しよう



Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

②個人情報取り扱いのプロセスを知ろう

- 業務プロセスと情報フロー



誰が、どのように、顧客データを収集し、
誰が、どのように、顧客データを加工し、
誰が、どのように、顧客データを利用し、
誰が、どのように、破棄するのか？

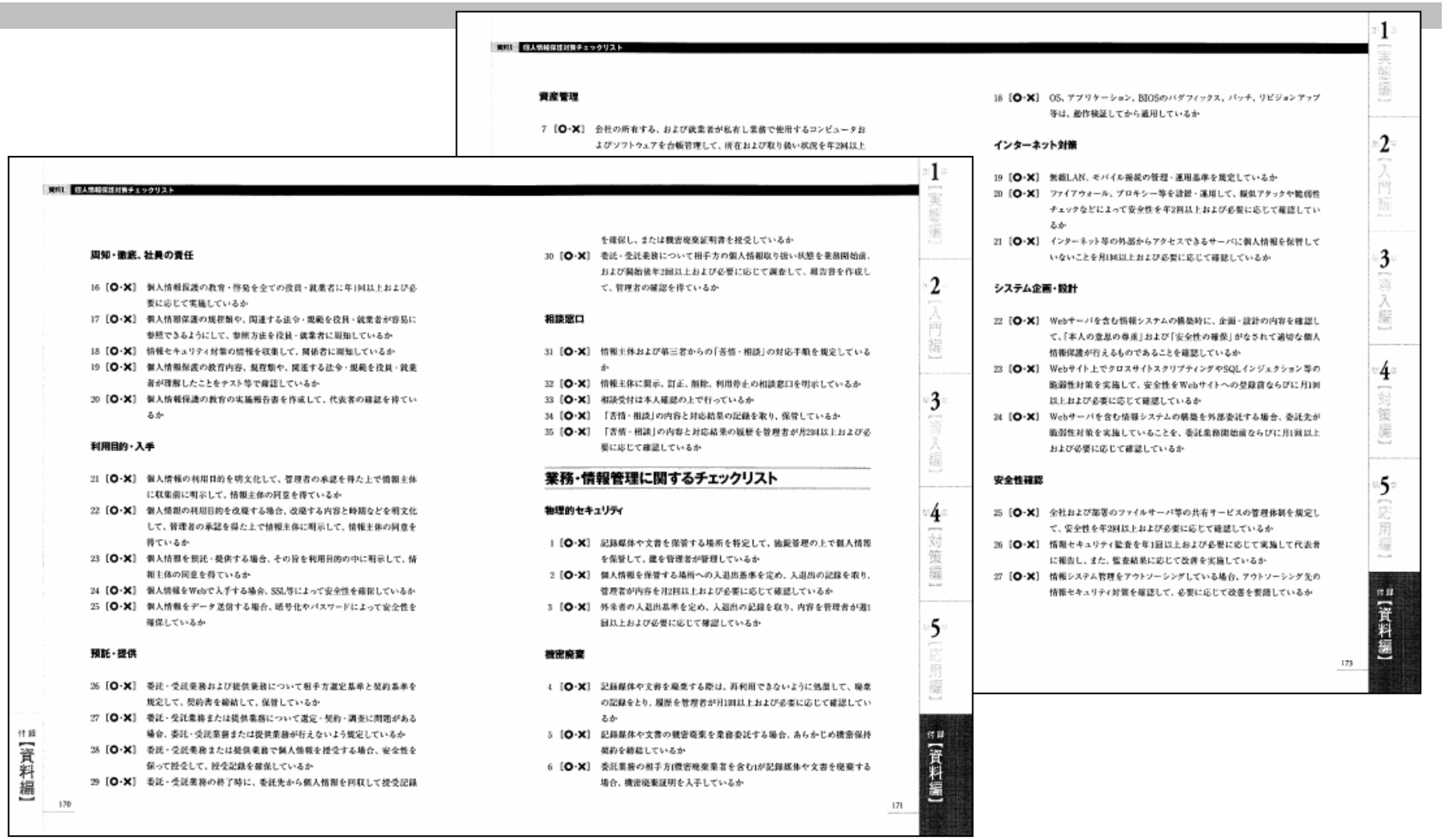
Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

「本人の意思の尊重」のポイント

- 収集
  - 利用目的の明示、本人の理解と(入手手段に応じた)同意の確保
  - 直接収集・間接収集、業務受託
  - 未成年等の個人情報、機微(センシティブ)な個人情報
  - 任意収集事項の影響への同意
  - みなし同意(サイレントマジョリティ)
  - 本人の意思の限界・制限の可能性
  - 公開情報の利用
- 保有
  - 利用目的の誠実な適用
  - 相談窓口、開示・訂正・削除・利用停止、費用、履歴・記録
  - 本人確認
  - プロファイリング
  - インハウス情報
  - 利用目的の変更、経年変化に対する再同意
  - 業務移管・M&A・廃業等の際の処置・同意確保
  - 正確性の確保と限界、同意を得ない利用の可能な条件と範囲
- 廃棄
  - 保有期間後の廃棄・破棄・削除・消去

Copyright (c) 2003-2004 NPO日本ネットワークセキュリティ協会

③個人情報保護の管理状況を確認しよう



資料1 個人情報保護対策チェックリスト

資産管理

7【○・×】 会社の所有する、および就業者が私有し業務で使用するコンピュータおよびソフトウェアを台帳管理して、所在および取り扱い状況を年2回以上

18【○・×】 OS、アプリケーション、BIOSのパッチフィックス、パッチ、リビジョンアップ等は、動作検証してから適用しているか

インターネット対策

19【○・×】 無線LAN、モバイル接続の管理・運用基準を規定しているか
20【○・×】 ファイアウォール、プロキシー等を設置・運用して、擬似アタックや脆弱性チェックなどによって安全性を年2回以上および必要に応じて確認しているか
21【○・×】 インターネット等の外部からアクセスできるサーバに個人情報を保管していないことを月1回以上および必要に応じて確認しているか

システム企画・設計

22【○・×】 Webサーバを含む情報システムの構築時に、企画・設計の内容を確認して、「本人の意思の尊重」および「安全性の確保」がなされて適切な個人情報保護が行えるものであることを確認しているか
23【○・×】 Webサイト上でクロスサイトスクリプティングやSQLインジェクション等の脆弱性対策を実施して、安全性をWebサイトへの登録前ならびに月1回以上および必要に応じて確認しているか
24【○・×】 Webサーバを含む情報システムの構築を外部委託する場合、委託先が脆弱性対策を実施していることを、委託業務開始前ならびに月1回以上および必要に応じて確認しているか

安全性確認

25【○・×】 全社および部署のファイルサーバ等の共有サービスの管理体制を規定して、安全性を年2回以上および必要に応じて確認しているか
26【○・×】 情報セキュリティ監査を年1回以上および必要に応じて実施して代表者に報告し、また、監査結果に応じて改善を実施しているか
27【○・×】 情報システム管理をアウトソーシングしている場合、アウトソーシング先の情報セキュリティ対策を確認して、必要に応じて改善を要請しているか

173

周知・徹底、社員の責任

16【○・×】 個人情報保護の教育・啓発を全ての役員・就業者に年1回以上および必要に応じて実施しているか
17【○・×】 個人情報保護の規程類や、関連する法令・規範を役員・就業者が容易に参照できるようにして、参照方法を役員・就業者に周知しているか
18【○・×】 情報セキュリティ対策の情報を収集して、関係者に周知しているか
19【○・×】 個人情報保護の教育内容、規程類や、関連する法令・規範を役員・就業者が理解したことをテスト等で確認しているか
20【○・×】 個人情報保護の教育の実施報告書を作成して、代表者の確認を得ているか

利用目的・入手

21【○・×】 個人情報の利用目的を明文化して、管理者の承認を得た上で情報主体に収集前に明示して、情報主体の同意を得ているか
22【○・×】 個人情報の利用目的を改廃する場合、改廃する内容と時期などを明文化して、管理者の承認を得た上で情報主体に明示して、情報主体の同意を得ているか
23【○・×】 個人情報を預託・提供する場合、その旨を利用目的の中に明示して、情報主体の同意を得ているか
24【○・×】 個人情報をWebで入手する場合、SSL等によって安全性を確保しているか
25【○・×】 個人情報をデータ送信する場合、暗号化やパスワードによって安全性を確保しているか

預託・提供

26【○・×】 委託・受託業務および提供業務について相手方選定基準と契約基準を規定して、契約書を締結して、保管しているか
27【○・×】 委託・受託業務または提供業務について選定・契約・調査に問題がある場合、委託・受託業務または提供業務が行えないよう規定しているか
28【○・×】 委託・受託業務または提供業務で個人情報を授受する場合、安全性を保って授受して、授受記録を確保しているか
29【○・×】 委託・受託業務の終了時に、委託先から個人情報を回収して授受記録を確保し、または機密廃棄証明書を授受しているか
30【○・×】 委託・受託業務について相手方の個人情報取り扱い状態を業務開始前、および開始後年2回以上および必要に応じて調査して、報告書を作成して、管理者の確認を得ているか

相談窓口

31【○・×】 情報主体および第三者からの「苦情・相談」の対応手順を規定しているか
32【○・×】 情報主体に開示、訂正、削除、利用停止の相談窓口を明示しているか
33【○・×】 相談受付は本人確認の上で行っているか
34【○・×】 「苦情・相談」の内容と対応結果の記録を取り、保管しているか
35【○・×】 「苦情・相談」の内容と対応結果の履歴を管理者が月2回以上および必要に応じて確認しているか

業務・情報管理に関するチェックリスト

物理的セキュリティ

1【○・×】 記録媒体や文書を保管する場所を特定して、施錠管理の上で個人情報を保管して、鍵を管理者が管理しているか
2【○・×】 個人情報を保管する場所への入退出基準を定め、入退出の記録を取り、管理者が内容を月2回以上および必要に応じて確認しているか
3【○・×】 外来者の入退出基準を定め、入退出の記録を取り、内容を管理者が週1回以上および必要に応じて確認しているか

機密廃棄

4【○・×】 記録媒体や文書を廃棄する際は、再利用できないように処置して、廃棄の記録をとり、履歴を管理者が月1回以上および必要に応じて確認しているか
5【○・×】 記録媒体や文書の機密廃棄を業務委託する場合、あらかじめ機密保持契約を締結しているか
6【○・×】 委託業務の相手方(機密廃棄業者を含む)が記録媒体や文書を廃棄する場合、機密廃棄証明を入手しているか

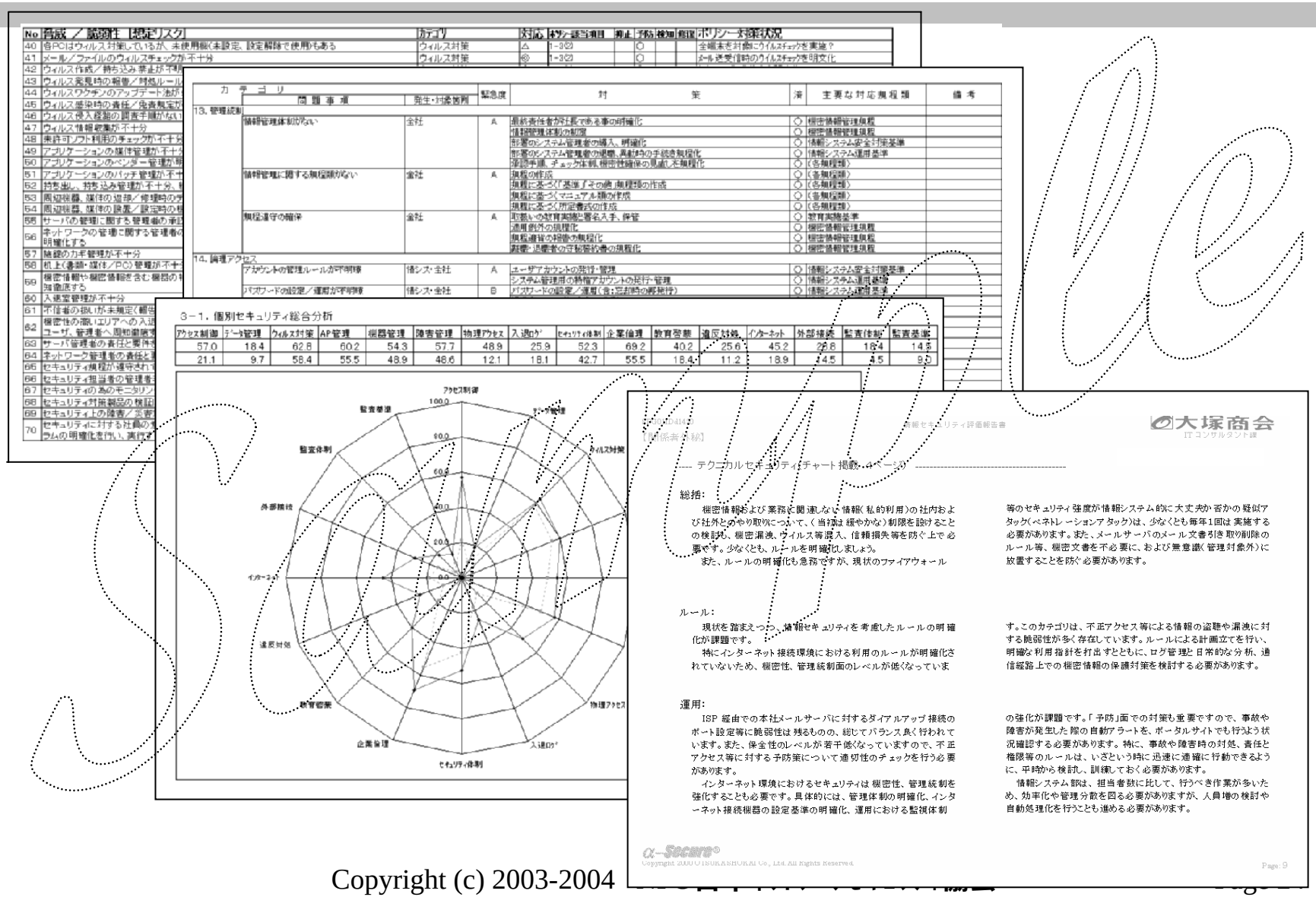
170

1【実態編】 2【入門編】 3【導入編】 4【対策編】 5【応用編】 付録【資料編】

※『個人情報保護法対策セキュリティ実践マニュアル』(JNSA/インプレス)(初校)より抜粋引用

Copyright (c) 2003-2004 NPO日本ネットワークセキュリティ協会

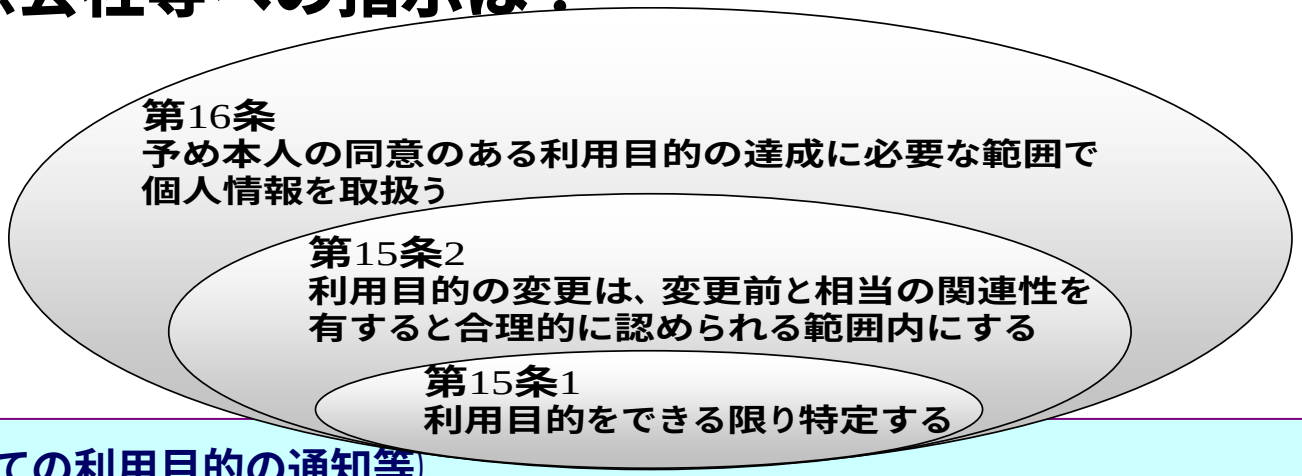
④個人情報のリスクを共通認識しよ



Copyright (c) 2003-2004

⑤利用目的をちゃんと決めよう

- いつ、誰が、どのように入手して、何のためにどのように取扱い、管理し、いつまで保有し、外に出すか出さないか、問合せ窓口はどこか　等
- どのように利用目的を伝えて、同意を得るか
- 関係会社等への指示は？



(取得に際しての利用目的の通知等)
第十八条　個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。
3　個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。

妥当な利用目的とは

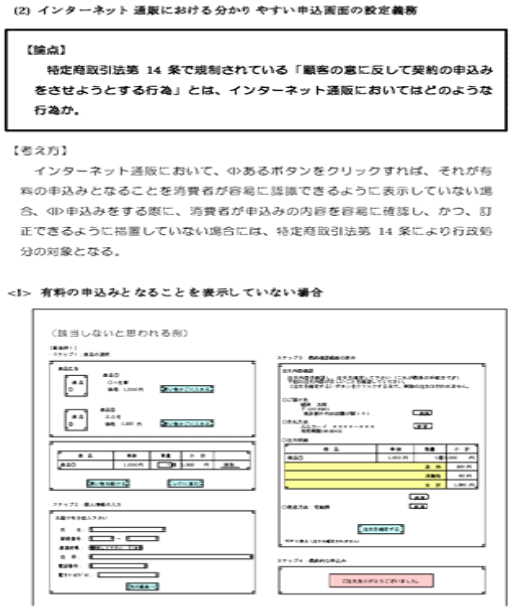
- 法的要請、業務の要請
- 収集項目
- 安全性対策、管理･態勢
- 保有期間
- 収集･利用時の注意
  - 自社の権利と義務
  - 個人の権利と義務
  - 法的要請等への対応
  - 媒体に応じた注意
- 開示･訂正･削除･利用停止
  - 制限･期間
  - 費用
- 再利用、利用者範囲
- 委託･提供
  - 受けるもの、出すもの
  - 相手先管理、安全管理
  - 責任の所在と限界
- 相談、クレーム、苦情
- その他

- 業界基準、ガイドライン
- 必要最低限なものにする
- 業界基準、ガイドライン
- 法や業務の要請
- 保有者は誰か
  - 予め説明責任を確保する
    契約、約款(明示･告知･同意)
  - 制限、告知義務･通知義務、安全管理等要請事項
  - 司法･税務命令、任意要請
  - 明示証拠、同意確保の妥当性
- 本人確認、対応マニュアル･訓練
  - 応じられない内容と根拠、判断者、判断基準、手順
  - 相談等の拒否にならない費用
- 商品DM、関連会社
- 業務委託、関係会社
  - 「第三者提供」の明確化
  - 業者選定基準
  - 委託契約等の守秘約款
- 相談窓口、問合せ方法、業界団体、ADR、オンブズマン
- 利用目的の版管理、改ざん防止
  未成年者、成年被後見人、被保佐人、被補助人

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

本人の同意の確保

- **直接収集、間接収集**
- **収集手段**(参考：電子商取引等に関する準則(平成１５年６月経済産業省))
  http://www.meti.go.jp/kohosys/press/0004141/0/030613denshishotorihiki.pdf


(2) インターネット通販における分かりやすい申込画面の設定義務

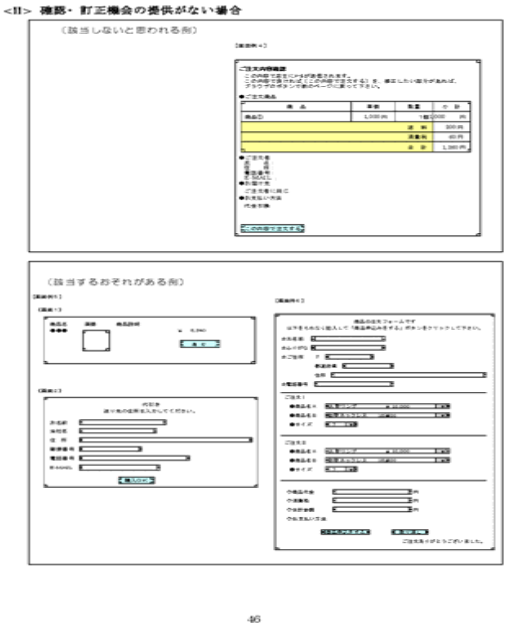
【論点】
特定商取引法第 14 条で規制されている「顧客の意に反して契約の申込みをさせようとする行為」とは、インターネット通販においてはどのような行為か。

【考え方】
インターネット通販において、<I>あるボタンをクリックすれば、それが有料の申込みとなることを消費者が容易に認識できるように表示していない場合、<II>申込みをする際に、消費者が申込みの内容を容易に確認し、かつ、訂正できるように措置していない場合には、特定商取引法第 14 条により行政処分の対象となる。

<I> 有料の申込みとなることを表示していない場合

（該当しないと思われる例）

44


<II> 確認・訂正機会の提供がない場合

（該当しないと思われる例）

（該当するおそれがある例）

46

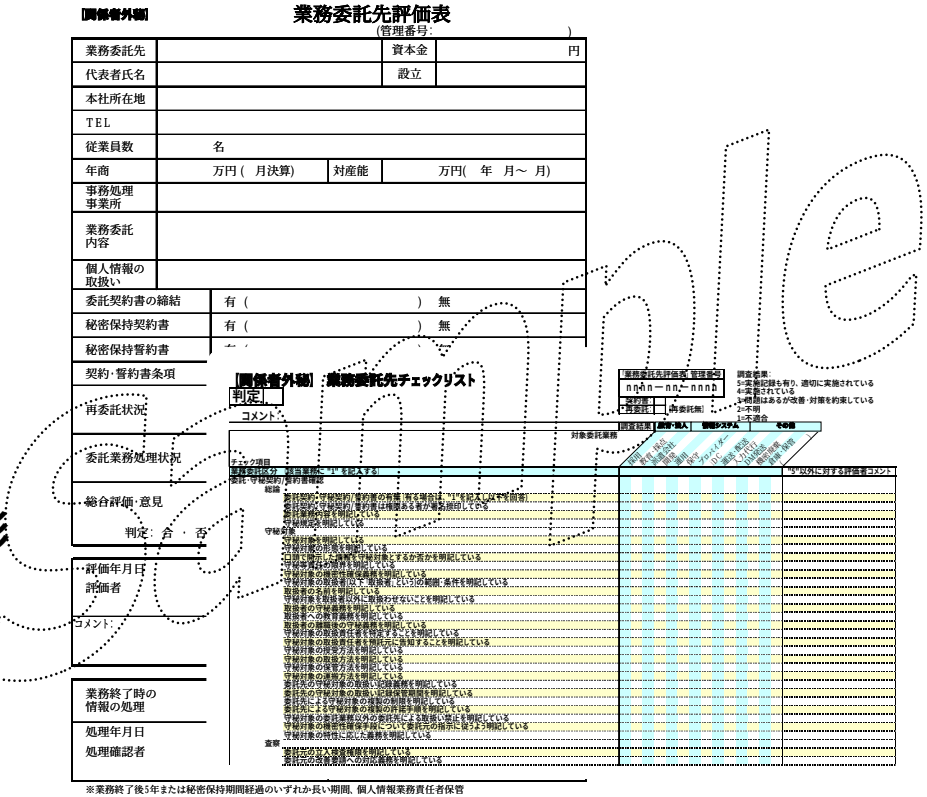
- **その他の参考：特定商取引法(特に第**11、12、14**条)、電子契約法**

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

⑥提供、委託を管理しよう

- 個人情報を社外に出す場合、提供と委託の2つのパターンがある。
  ※ 個人情報保護法　第二十二条（委託先の監督）、第二十三条（第三者提供の制限）

  - **提供**：適切な相手に提供する
    - 情報を会社および本人以外に、有償または無償で渡して、その個人情報の返却を求めない授受の形態。
  - **委託**：契約書、現地視察、授受記録により説明責任を確保
    - 情報処理やシステム開発、ＤＭ発送代行、倉庫等での保管、コールセンター、カスタマセンター、廃棄等の業務委託のために個人情報を預ける形態。
    - 委託先と守秘契約書を締結し、業務委託が終了した際に、その個人情報を委託元が回収、または委託先での機密廃棄を確認。



Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

業務委託管理のポイント

- 利用目的への明記
  - どのような業務について委託するか
  - 委託内容をどのように規定するか
  - 情報交換制度等をどう規定するか
- 業者選定･評価
  - 経営状態の他、個人情報保護･情報セキュリティ状況を確認する
  - 個人情報の取扱い･管理状況を査察する
  - 評価基準を明確化し、委託の可否を適切に判断する
- 業務契約
  - 守秘約款、責任･義務と権限･限界、権利、委託期間、有効期限
  - 再委託の制限、管理責任者の特定、事故等の報告義務　他
- 機密性確保
  - 授受形態(手渡、メール、宅配便、郵送、FAX、Web等)に応じた対策
  - 委託先で棚等への格納および施錠管理、鍵管理、利用履歴
- 授受管理
  - 受領書、控えの確保
- 取扱い状況確認･査察、依頼･指導･要請
- 検収、業務終了後の個人情報の取扱い
  - 返却･機密廃棄、データ消去
- 業務が長期に渡る場合
  - 延長の場合は、業務契約の有効期限を確認
  - 指導等や査察の定期的実施
  - 業務に不要となった情報の有無の確認

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

⑦廃棄、削除、消去をきちんとしよう

- 保管期間･保有期間経過後、すみやかに処理する。

- シュレッダーにかけるか溶解処理する。
  すぐに処理できない場合は、保管し施錠管理する。

- 消去等が可能な記録媒体は、データを消去の上、初期化して廃棄する。
- 消去が不可能な記録媒体は、裁断、破砕して廃棄する。
- 使用済コンピュータ機器は、ハードディスクの内容を消去してリース返却または廃棄する。

- 廃棄処理業者と秘密保持契約し、廃棄物の授受書、廃棄証明を得る。
- 廃棄物、回収物、処理物の量等を確認する。
- 適切に処理しているか確認する。

- 環境管理(ISO14000s)や品質管理(ISO9000s)との整合性、法的保管期間の確保
- 廃棄物に関する法令･規範の遵守

Copyright (c) 2003-2004　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

⑧危機管理しよう

- 個人情報の流出･漏洩等の事故発生またはそのおそれを知った際の対処手順
  - ポイントは個人情報の表す本人の権利の尊重！
  - すみやかな対応(報告･連絡･相談)が重要
  - 相談窓口･苦情対応手順、一元管理
  - 危機管理体制の整備･運用、権限(委譲、回復)
  - 以上の規定化、周知、予行演習、効果測定、規定改善
  - 記録の管理、保管
- 苦情の第三者による解決
  - 国民消費者センター
  - 訴訟、民事調停

※ BCP(事業継続計画)、CP(不測事態対応計画)、DR(障害復旧計画) 等も明確化することが望ましい

BCP : Business Continuous Plan
CP : Contingency Plan
DR : Disaster Recovery Plan

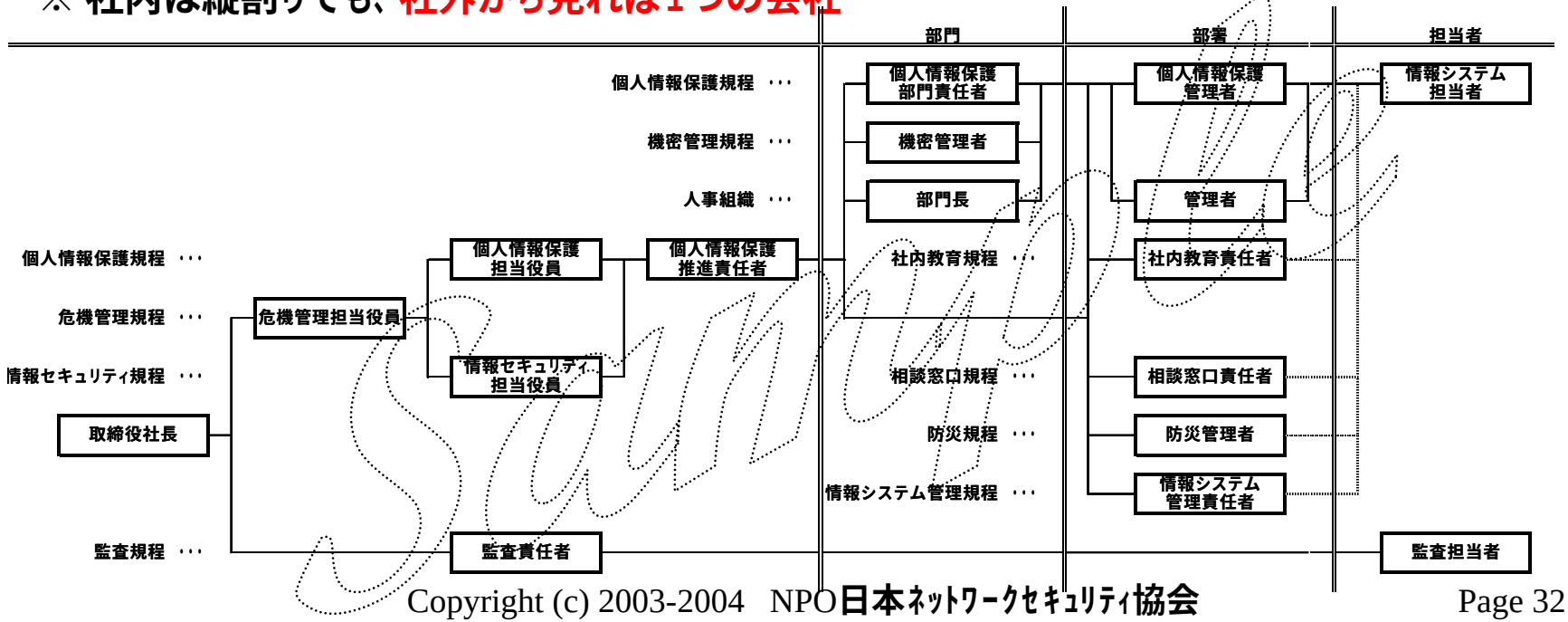
Copyright (c) 2003-2004　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

⑨個人情報保護の組織体制を創る

- トップダウン体制
  - 推進体制
    - 全社単位の推進体制、教育、相談窓口、情報システム
    - 業務単位の推進体制

    「重要な業務執行は取締役会が決定する」(商法260条2項:原文は文語体)
  - 監査体制

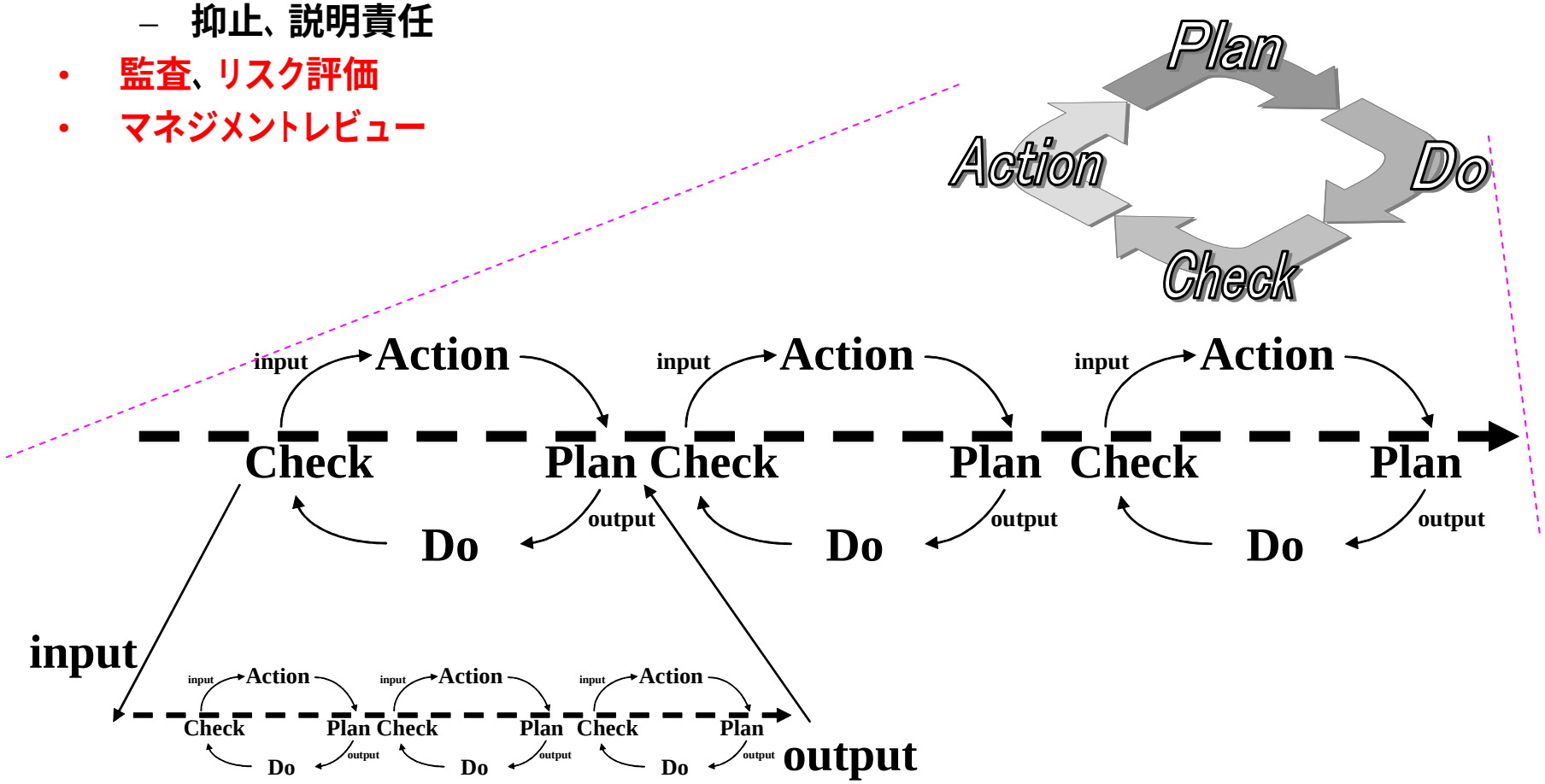
※ 社内は縦割りでも、社外から見れば1つの会社



Copyright (c) 2003-2004 NPO日本ネットワークセキュリティ協会

⑩態勢を維持向上しよう

- ルールの明確化と教育･啓発、訓練、効果測定
  - ソーシャルエンジニアリング･ミス(過失)の防止
  - 抑止、説明責任
- 監査、リスク評価
- マネジメントレビュー



Copyright (c) 2003-2004 NPO日本ネットワークセキュリティ協会

顧客対応／社員しつけ

マナーからルールへ

お客様相談窓口の設置

1．報告･対応ルール化
　①行動基準
　②判断基準
2．社外告示の明確化
　①情報開示
　②各種テンプレート作

顧客対応

1．お詫び文
2．状況説明
3．原因
4．現在の緊急対策
5．今後の方針

社員しつけの実施

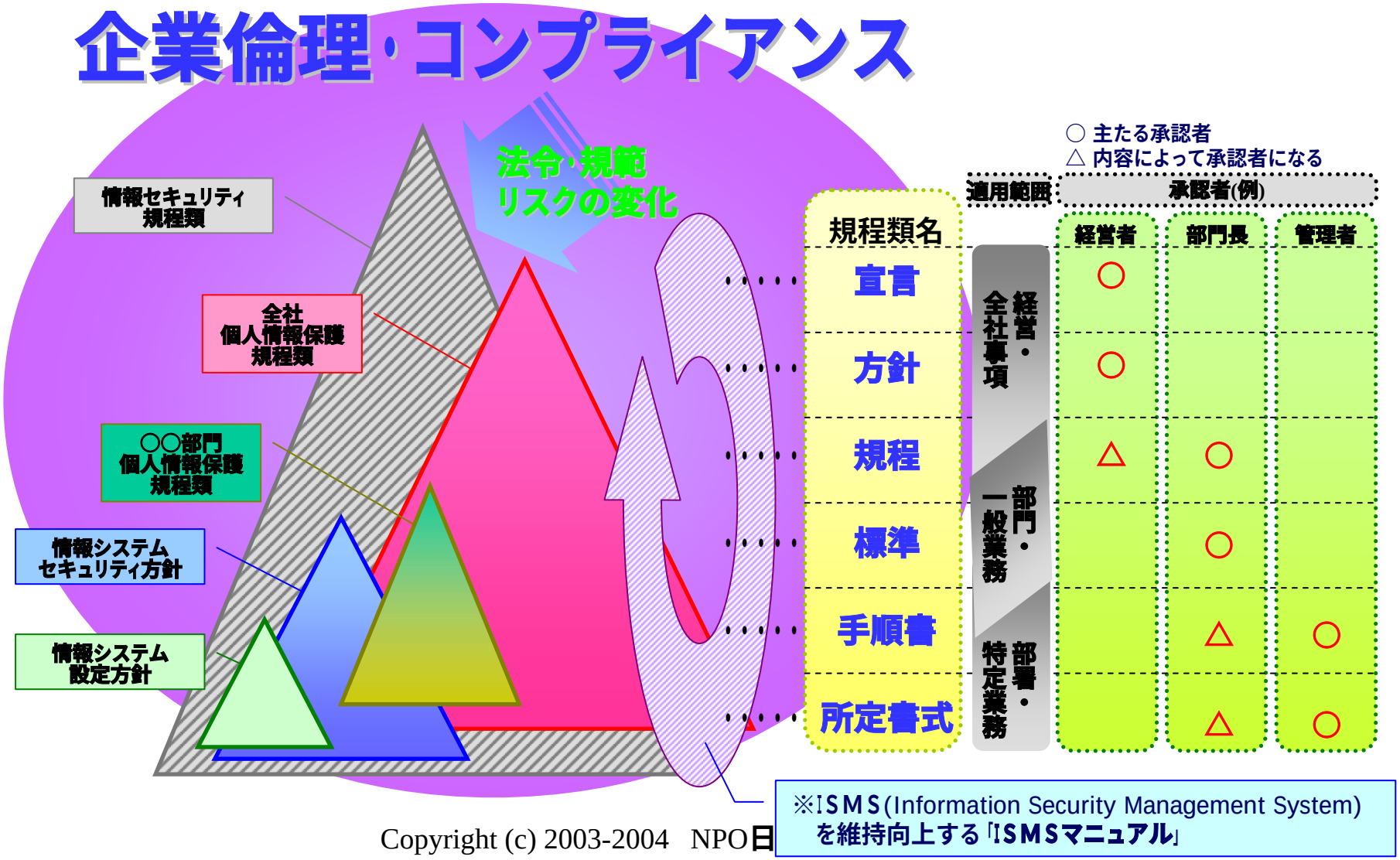
1．報告･対応ルール化
　①行動基準
　②判断基準
2．行動マニュアル
3．教育

サポート10訓

1．顧客からデータは、預からない
2．公共の場で、顧客名は言わない
3．ウイルス対策は怠らない
　：
　：
10．クレームは、待たせない　と

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

⑪企業倫理とコンプライアンスに統合しよう



Copyright (c) 2003-2004　NPO日

個人情報保護　宣言と方針

個人情報保護への取組み宣言書

当社は、お客様の個人情報がお客様にとって重要な守るべきものであるとともに、当社にとっても重要な経営情報であると認識しております。当社は、お客様の個人情報を適切に守り、お客様との信頼関係を損なわないために、次のようにすることをここに宣言します。

1. 個人情報の取扱いに関する規程類を明確化し、就業者に周知徹底します。また、取引先等に対しても適切に個人情報を取扱うように要請します。
2. 個人情報の収集に際しては、予め収集・利用目的を告知し、お客様の同意の上で収集します。また、同意を得た利用目的に従って個人情報を取扱います。
3. 保有するお客様の個人情報について、お客様ご本人からの開示、訂正、削除、利用停止の依頼を次のメールアドレスでお受けして、誠意を持って対応させて頂きます。
4. 保有するお客様の個人情報について、流出等の事故を招かないよう、必要となる対策を講じます。

(中略)

n. 当社は、個人情報の取扱いを適切なものとするよう、外部の第三者による監査を受け、必要となる改善を実施します。

以上

nnnn年 nn月 nn日
株式会社XXXXX
代表取締役　XX　XX

株式会社XXXXX　個人情報保護方針

当社は、お客様個人を識別し得る情報(以下、「個人情報」といいます。)を適切に保護することが重要であると認識し、以下のように会社として取組んでおります。

1. 適正な管理

当社は、お客様の個人情報を取扱う部門ごとに、個人情報の管理責任者を置き、個人情報の適切な管理を行います。また、役員を含む就業者に対する教育・啓発を実施します。さらに、合理的な対策を講じることにより、個人情報の不正または不適切な取扱い、事故等を招かないように尽力いたします。

2. 収集目的等の明示

当社は、お客様から個人情報を収集させていただく場合は、収集目的、当社の問合せ窓口等(以下、「収集目的等」といいます。)を明示したうえで必要な範囲の個人情報を収集させていただきます。

なお、当社のWebサイトはCookieを使用しておりません。

3. 第三者への開示・提供

当社は、お客様の個人情報を適切に管理し、法的な要請等によらない限り、お客様の事前承認なく第三者に開示・提供することはありません。また、お客様の個人情報を業務委託先に提供する場合は、守秘契約等によって業務委託先に個人情報保護を義務付けるとともに、業務委託先が適切に個人情報を取扱うように管理いたします。

なお、当社のWebサイトでリンクしている、および、当社のWebサイトにリンクしている他のWebサイトでの個人情報の取扱いに関して、当社は一切の責任を負いません。

4. 個人情報の利用

当社は、お客様の個人情報を、あらかじめお客様に明示した収集目的等の範囲で利用します。また、当社は、お客様にご利用頂いた当社のサービス、商品等に関連する情報を、電子メールまたは送付物によりご紹介する場合があります。これらのご紹介を不要とされる場合、後述する電子メールアドレスの問合せ窓口にご連絡いただくことによって、以降のご紹介を行わないようにいたします。

5. 個人情報の照会、訂正、削除

当社は、お客様の個人情報を、お客様の照会、訂正、削除要請に従って取扱います。後述する電子メールアドレスの問合せ窓口にご連絡ください。

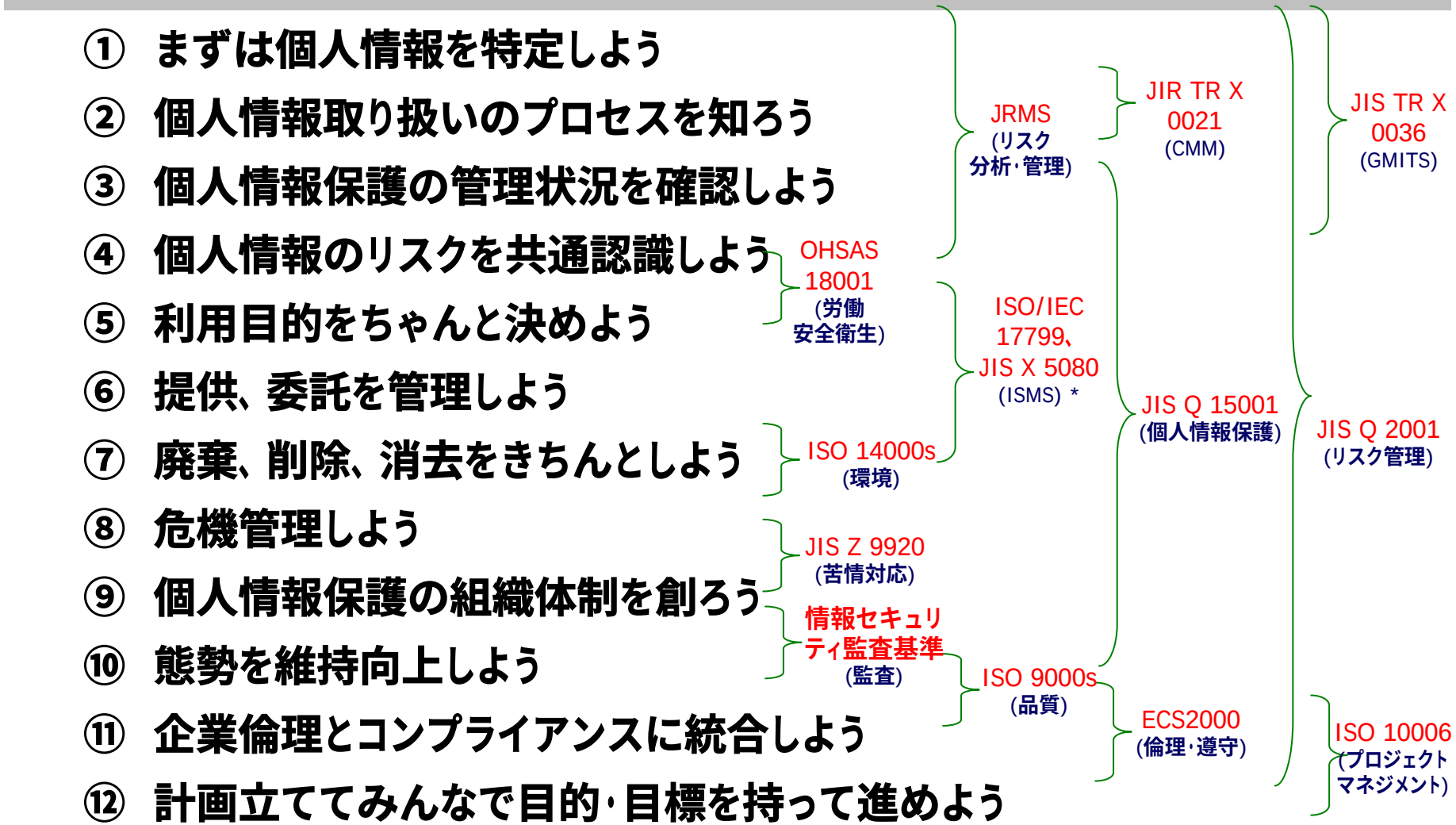
6. 法令・規範の遵守

当社は、お客様の個人情報に関連する日本の法令・規範を遵守するとともに、本方針の内容を継続的に見直し、その改善を図ります。

■ 本方針および当社の個人情報の取扱いに関するお問合せ窓口
電子メール: privacy@xxxxx.co.jp

Copyright (c) 2003-

個人情報保護態勢の構築と規範例



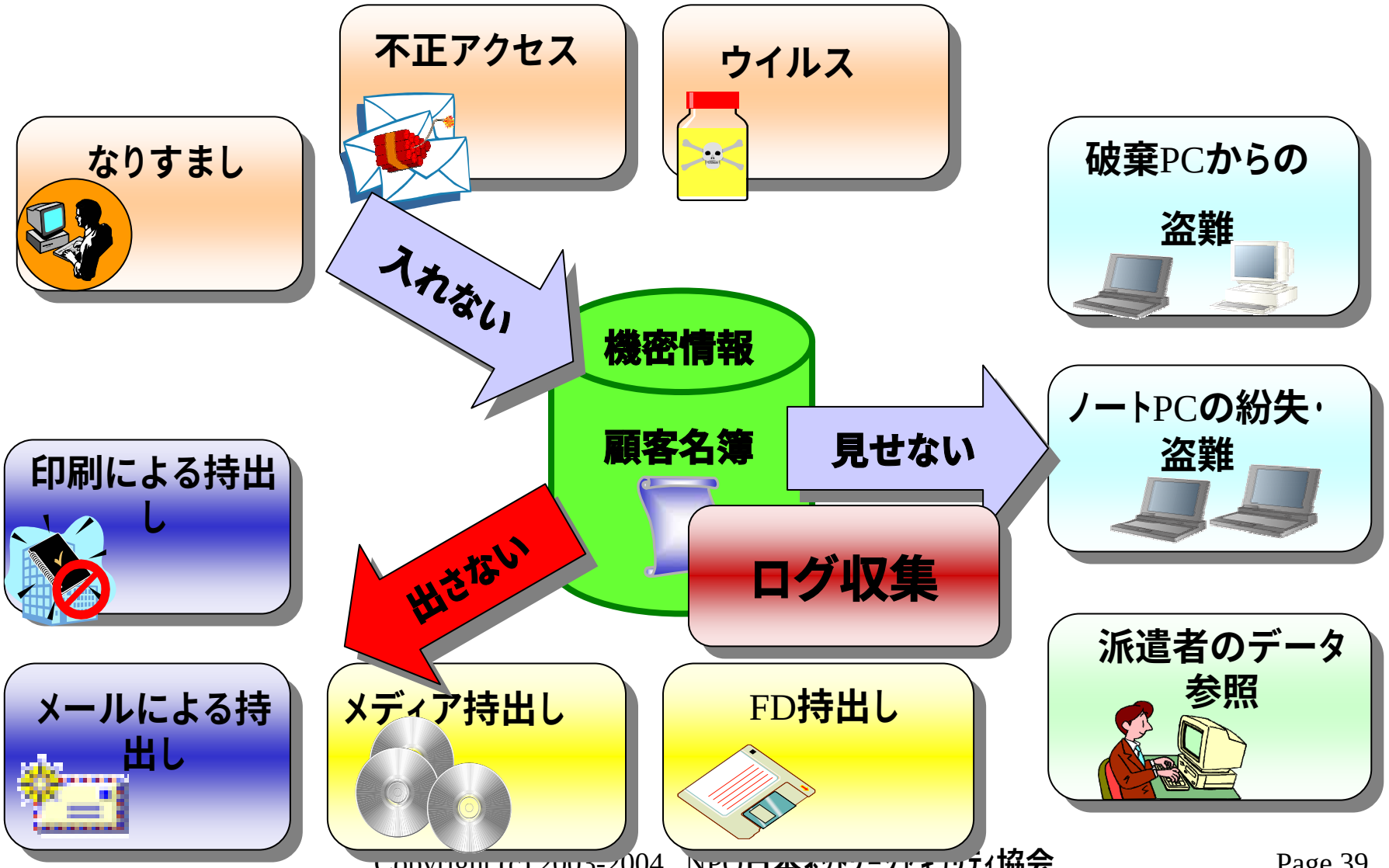
「安全性の確保」ポイント (データ管理)

- リスク管理、プロセス管理
  - 個人情報の特定
  - 業務と情報の流れに基づく脅威と脆弱性の特定
  - 業務改善
  - 経営方針・戦略・ビジネスモデルとの適合性

  ※「JIPDECリスクマネジメントシステム(JRMS)解説書」
  ISBN 4-89078-012-2　¥9,500
- ライフサイクルに沿った管理
  - 収集時の安全性の確保(と責任の限界)
  - 保管、利用、廃棄・破棄・削除・消去
  - 提供・委託
- 持ち出し、搬送・運搬・送信時の機密性確保
  - 電子メールへの添付ファイル、送信経路は安全？
- 運搬・保管、郵送・宅配時の機密性確保
  - 集荷、配送、配達確認、不着、保管、集荷・配送代行、再委託
- 可用性(Availability)の確保
- 利用権限、利用制限
  - 認証、認可、記録性(証拠性)
  - Need to Know、Need to Use

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

出さない、入れない、見せない



Copyright (c) 2003-2004 NPO日本ネットワークセキュリティ協会

「安全性の確保」ポイント(システムセキュリティ)

- 企画・設計・開発、導入
  - ※ 調査(インシデントレスポンス)
    コンピュータフォレンジック、ハニーポット、ハニーネット
  - セキュアなWebサーバーの構築と運用
    http://www.ipa.go.jp/security/awareness/administrator/secure-web/index.html
  - セキュアプログラミング講座
    http://www.ipa.go.jp/security/awareness/vendor/programming/index.html
  - 安全なWebアプリ開発40箇条の鉄則
    http://java-house.jp/~takagi/paper/idg-jwd2003-takagi-dist.pdf
  - Webアプリの欠陥検査 実践編
    http://java-house.jp/~takagi/paper/jnsa-nsf-2003-takagi-dist.pdf
- 運用・維持・保守、スペック、廃棄
  - 管理、運用、利用
- 業務委託(運用、ヘルプデスク、ASP、iDC等)、再委託の管理、委託作業状況の査察、事故・違約時の処置・解決方法
  - アウトソーシング、分社化
- 派遣社員、受入出向社員、アルバイト、パートタイマー
  - 勤務形態
  - 有効なシナジーを得るコアコンピタンス
- 利用者(OS/APアップデート、ウイルスチェック、端末、モバイル・リモート、無線LAN(WEPキー、MACアドレス、ESS-ID)、不正利用、操作ミス、破損・紛失等)
  - リモートアクセス環境におけるセキュリティ
    http://www.ipa.go.jp/security/awareness/administrator/remote/index.html

Copyright (c) 2003-2004 NPO日本ネットワークセキュリティ協会

「安全性の確保」のポイント (その他)

- 物理セキュリティ
  - 入退出管理、物理アクセス管理、外来者・不審者対応
  - 紙・記録媒体・コンピュータの取扱い、管理
- 論理セキュリティ
  - ID管理(発行、停止、更新、削除)
  - パスワード管理(発行、再発行、変更、リマインダ、キーロガー)
  - 論理アクセス管理(職務、職位、職制、職級、承認、見直し)
  - ウイルス・不正アクセス対策(予防、update、発見、対応、再発防止)
  - 記録の確保(ログ改ざん・喪失防止、タイムスタンプ、定期的分析、報告、保管・管理)
  - 新たな脅威・脆弱性(発見、検討、対処、見直し)
- 障害・不測事態対策
  - 危機管理(リスクマネジメント、リスクコミュニケーション)
    - 発見方法、発現時の対処・連絡、対抗手段、再発防止策
    - 暫定処置、代替措置・手段、保有・転嫁
    - 権限委譲と権限復帰
  - 利用規約、SLA (Service Level Agreement)
  - 守秘契約、誓約書

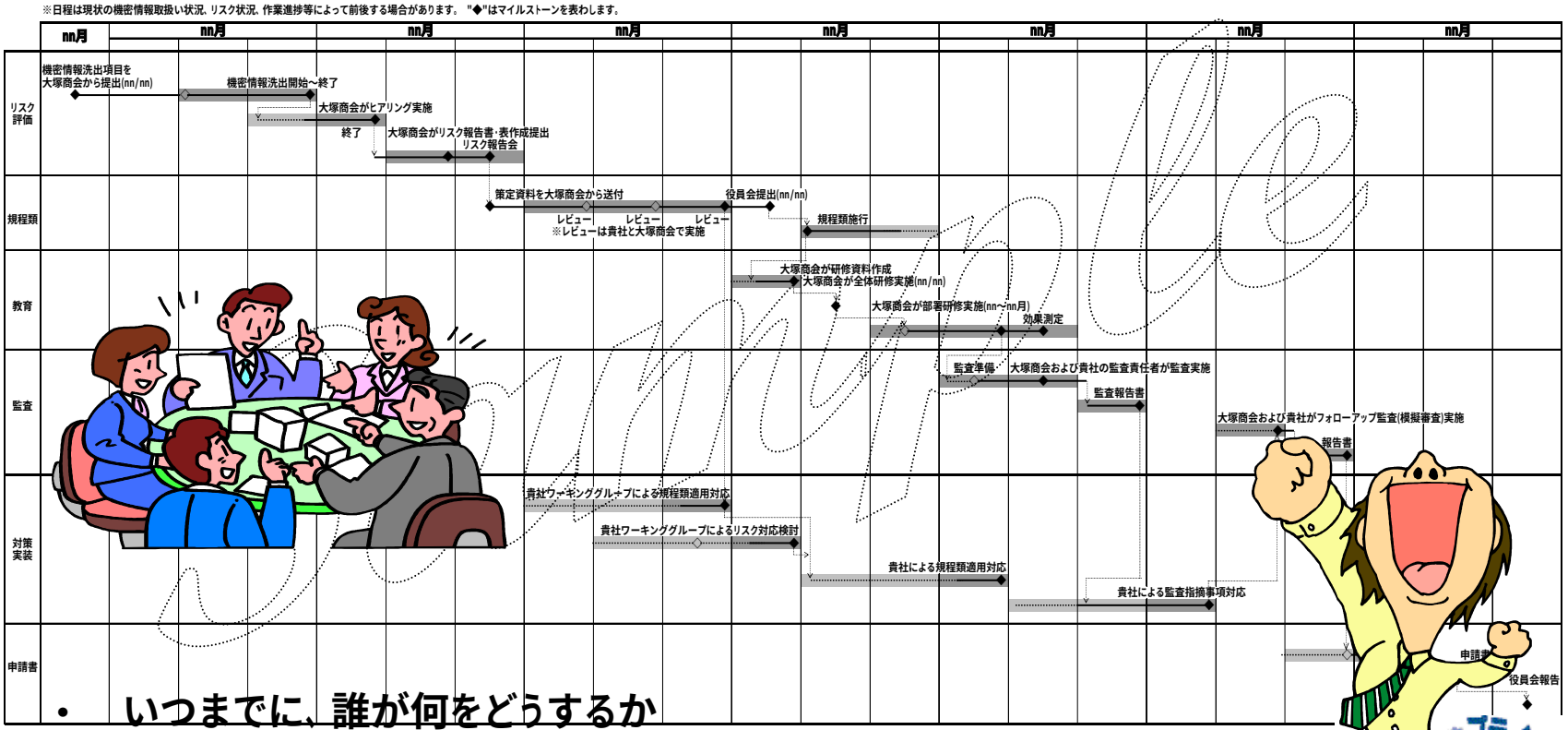
Copyright (c) 2003-2004 NPO日本ネットワークセキュリティ協会

「個人情報保護態勢」のポイント

- トップの統括、経営層・管理層の協力、予算・資源確保
- ルール(社内規程)の明確化
  - 責任と権限、役割分掌、牽制、手続き等
  - 各種規程の相関性・整合性・実行性・遵法性等の確認
- 最新のルールの周知(教育・啓発)
  - 経営層・管理層と就業者層それぞれの教育、キャリアパス
  - 俯瞰事項と具体事項、業務レベルまで落とし込んだ内容
  - 理解・効果測定、予行演習・訓練
- 監査、遵法性確認、リスク分析・評価、自主点検、相互点検、改善確認
- 賞罰のルール
- 記録(証拠)の確保および廃棄
  - 関連法令・施行令、規範(基準・規格、RFC 3227)
- 維持向上(Plan – Do – Check – Action)
- マネジメントシステムの統合
  - 環境(EMS)、品質(QMS)、労働安全衛生(OHSMS)、プロジェクト管理(PM)、倫理・遵法

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

⑫計画立ててみんなで目的･目標を持って進めよう



- いつまでに、誰が何をどうするか
- 法令･規範･リスク評価･監査上、妥当か
- どのような対策をおこなうか
- 全体的に、施策と結果をどう評価するか
- 達成、充足の評価はどうか

たとえば．．．

たいせつにします プライバシー
A123456(01)

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

まとめ

- 企業に要求される基準や態勢の維持向上。
- CSR(**社会的責任**:Corporate Social Responsibility)を果たす上で、「個人情報取扱事業者」でない企業・個人にとっても、個人情報保護法の要求する保護レベルを確保する必要がある。
  - 個人情報保護法のみならず、従来の刑法・民法典下の裁判で負けなければ良いというわけでもない。
    危ない企業と取引して連帯責任を負うのか。(危うきに近寄らず)
  - 保護レベルの目安としてのプライバシーマークは、**入札要件**になってくる。
- 個人情報保護のベースラインは. . .
  - プライバシーマーク(JIS Q 15001)
  - ISMS(JIS X 5080)
- 個人情報保護(**遵法**)は、やってあたりまえ。
  - **他社への差別化**を図らなければ生き残れない。
  - **マネジメントシステム**を確立し、Plan-Do-Check-Actionで維持向上する。
  - 企業倫理への昇華、コンプライアンスの融合

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

《参考資料》保護法関連サービス

- コンサルティングサービス
  - 情報セキュリティポリシー構築支援サービス
  - 情報セキュリティガイドライン策定支援サービス
  - ＢＳ７７９９認証取得支援サービス
  - ＩＳＭＳ認証取得支援サービス
  - プライバシーマーク取得支援サービス
  - 個人情報保護態勢構築支援サービス
  - 情報セキュリティリスク評価支援サービス
  - 情報セキュリティ監査支援サービス
  - 情報セキュリティ教育支援サービス
  - ＩＳＭＳ構築支援サービス
  - 危機管理計画策定支援サービス
  - 統合マネジメントシステム構築支援サービス
- インテグレート運用サービス
  - 情報セキュリティシステム構築サービス
  - セキュリティチェックサービス (擬似アタック)
  - エマージェンシーサービス
  - データ復旧サービス
  - ＩＤＣ・アウトソーシングサービス
  - ITセキュリティ監視サービス

Copyright (c) 2003-2004　NPO日本ネットワークセキュリティ協会

個人情報保護対策支援例 (コンサル)

JNSA

① まずは個人情報を特定しよう
② 個人情報取り扱いのプロセスを知ろう
③ 個人情報保護の管理状況を確認しよう
④ 個人情報のリスクを共通認識しよう
⑤ 利用目的をちゃんと決めよう
⑥ 提供、委託を管理しよう
⑦ 廃棄、削除、消去をきちんとしよう
⑧ 危機管理しよう
⑨ 個人情報保護の組織体制を創ろう
⑩ 態勢を維持向上しよう
⑪ 企業倫理とコンプライアンスに統合しよう
⑫ 計画立ててみんなで目的・目標を持って進めよう

a,c
c
d
b,f
e
g,h

	【カテゴリ】	【サービス】
a	リスク分析・リスク評価	分析・評価、改善コンサル
		システムコンサル
		ペネトレーションアタック
b	教育・啓発、訓練	集合研修、セミナー
		e-ラーニング
c	安全対策	ISMS構築
		ActiveDirectoryコンサル
		システムコンサル
		サイト・ゾーン管理、iDC
		Webセキュリティ
		機密廃棄
d	危機管理	危機管理計画策定
e	企業倫理、コンプライアンス	文書管理コンサル
		ISO取得コンサル
		統合マネジメントシステム構築
f	監査、改善	情報セキュリティ監査
g	ISMS	ISMS認証取得
		ISMS態勢構築
h	個人情報保護	プライバシーマーク取得
		個人情報保護態勢構築

情報セキュリティポリシー構築

Copyright (c) 2003-2004 NP

個人情報保護対策支援例(インテグレート)

① まずは個人情報を特定しよう
② 個人情報取り扱いのプロセスを知ろう
③ 個人情報保護の管理状況を確認しよう
④ 個人情報のリスクを共通認識しよう
⑤ 利用目的をちゃんと決めよう
⑥ 提供、委託を管理しよう
⑦ 廃棄、削除、消去をきちんとしよう
⑧ 危機管理しよう
⑨ 個人情報保護の組織体制を創ろう
⑩ 態勢を維持向上しよう
⑪ 企業倫理とコンプライアンスに統合しよう
⑫ 計画立ててみんなで目的・目標を持って進めよう

	【カテゴリ】	【プロダクツ】
a	データ消去	データ消去ツール
b	安全対策	
	不正アクセス・改ざん	IDS、疑似アタック、改ざん復旧
	不祥事防止	フィルタリング、インベントリ、暗号化
	物理対策	入退出管理、盗難防止
	論理対策	不正プログラム対策、ログ採取
	ウイルス対策	ウイルス対策
	バージョンアップ	パッチ、パターンファイル
	可用性確保	UPS、冗長化、リソース監視
		データバックアップ
	データ管理	コピー防止、文書管理
	認証、暗号化	認証、暗号化、PKI、プリンタ管理
	時間同期	時間同期
	端末・モバイル管理	コンソールロック、認証、OS
		デバイスコントロール、残留情報対策
c	管理統制	ワークフロー管理、電子承認
		グループウェア、社内ポータル
		文書管理
		ライセンス管理
		資産管理

Copyright (c) 2003-2004 NPO日本ネットワークセキュリティ協会

ご清聴を感謝申し上げます

Copyright (c) 2003-2004　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会