NetworkSecurityForrum2004

ISMS認定/Pマークを 早く安く取得するポイント

平成16年 10月 28日
NPO 日本ネットワークセキュリティ協会　幹事
㈱大塚商会　テクニカルソリューションセンター
佐藤 憲一
Kenichi.Satoh@otsuka-shokai.co.jp

1

自己紹介

NPO JNSA

正式名称　特定非営利活動法人 日本ネットワークセキュリティ協会
事務所　東京都江東区、大阪市北区
目　的　一般の人々に対し、ネットワークセキュリティに関する啓発、教育、調査研究及び情報提供に関する事業を実施することによって、ネットワークセキュリティに関する標準化の推進と技術水準の向上に寄与し、もって公益の増進に寄与することを目的とする。
参加企業　176社（平成16年8月）

㈱大塚商会

本社所在地　東京都 千代田区 三崎町
主業務内容　ｺﾝﾋﾟｭｰﾀ、複写機、通信機器、ｿﾌﾄｳｪｱの販売および受託ｿﾌﾄの開発等を行うｼｽﾃﾑｲﾝﾃｸﾞﾚｰｼｮﾝとｻﾌﾟﾗｲ供給、保守、教育支援等のｻｰﾋﾞｽ&ｻﾎﾟｰﾄを主な事業としている。
創　業　1961年（S36年）7月17日
資 本 金　103億7485万円
社員数　6272人　（営業系40%、SE系45%、事務系15%）
拠点数　国内220拠点

佐藤 憲一

株式会社 大塚商会 S&S本部 テクニカルソリューションセンター 部長代理
(株)オーエスケイ取締役兼務。
NPO 日本ネットワークセキュリティ協会 幹事。 個人情報保護ガイドライン作成WGリーダー
(社) 情報サービス産業協会 情報セキュリティマネジメント部会 委員
2002,2003,2004 RSA Conference実行委員

2

個人情報保護に関する執筆書籍

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

3

講演のまとめ

1. まずは、個人情報保護法対応後、ISMS、Pマーク取得を検討しましょう

2. 個人情報保護法対応、ISMS、Pマーク取得には、経験豊富なコンサルタントに一部委託すると早く安く実現できます

3. 社内特定部署（例えば情報システム室、法務部）にて、今自分達でできることから準備しましょう
準備が早ければ早いほど、さらに早く安く実現できます

【追加要件】
4. 取得には、経営者及び社内各部署との理解と協力が不可欠です
5. 取得には、最低3ヶ月(通常6ヶ月) の準備期間が必要です
6. 取得には、2名以上の社内専任化(又はプロジェクト)が必要です
（社員200名まで2名、300名増える毎に1名）
7. 取得時は、取得要件を網羅的に満足することが必要です
（各々の項目の強化は、取得後次の更新までの中期計画にて行います）

4

講演内容

第一章　ISMS、Pマーク　取得分析

O社の経験、実績に基づき、標準的取得企業モデルより、
工数、人件費の分析と考察をする

第二章　取得前企業分析

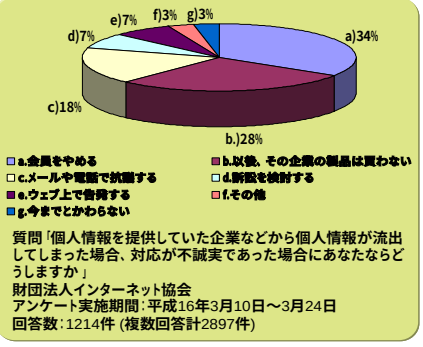
O社のコンサル実績約100社の実態調査分析より、
①最重要項目の明確化、②個人情報保護法への対応
を分析する

第三章　個人情報保護法対策の推進法

個人情報保護法　対策の進め方を説明する

5

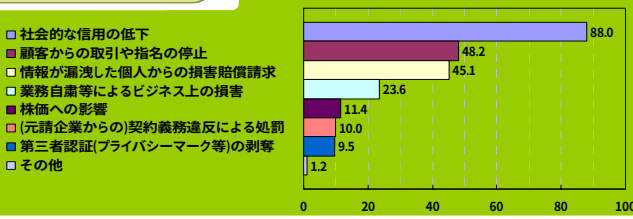
個人情報漏洩がもたらす企業への影響



質問「個人情報を提供していた企業などから個人情報が流出してしまった場合、対応が不誠実であった場合にあなたならどうしますか」
財団法人インターネット協会
アンケート実施期間：平成16年3月10日～3月24日
回答数：1214件 (複数回答計2897件)

←94%（a～e）の人が、何らかの行動にでると回答している。

質問「個人情報漏洩により深刻な被害を及ぼす事項（3つまで回答）」
三菱総合研究所gooリサーチ結果
調査期間：平成16年5月14日(金)～5月16日(日)
回答数：508名



特損も企業イメージの失墜も、大きな痛手になる。→

6

個人情報保護法の基準

平成17年4月　施行

個人情報保護法

義 務

プライバシーポリシー　【 JIS Q 15001 】
→ Pマーク制度

情報セキュリティポリシー　【 JIS X 5080 】
→ ISMS認定制度

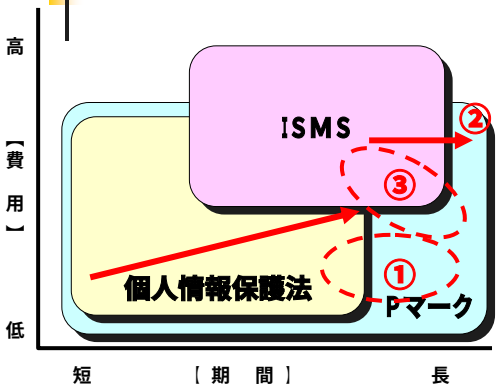
経産省　個人情報保護法ガイドライン

1. 個人情報保護法は、顧客/社員情報を適切に保護/管理するための法律
2. 「企業」は、個人情報の「取り扱い」を適切に実施するため、「JIS Q 15001」に基づき
   コンプライアンスを確立する
3. 「企業」は、個人情報を「安全」に維持管理するため、「JIS X 5080」に基づき
   コンプライアンスを確立する

個人情報保護法対応は、ISMS、Pマーク取得の近道である

7

保護法、ISMS、Pマーク　対応方法



【 主な特徴 】

1. Pマークは、保護法対応に加え、
   監査、審査機関対応が不可欠
2. ISMSは、より高度な安全管理が
   必要となるため、対策費が高くなる

【 最近の傾向 】

パターン① ： 保護法対策　Pマーク と捕らえ、Pマーク取得する企業
パターン② ： ISMS取得後、Pマーク（ 保護法対策）取得する企業
パターン③ ： ISMS、Pマークの同時取得する企業

8

個人情報取扱事業者の義務(罰則)

個人情報の取扱に関する苦情の適切かつ迅速な処理に努める(第32条)

勧　告

☆ 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)
☆ **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は、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)

命令／緊急命令

6カ月以下懲役
or
30万円以下の罰金

★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)
★ 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)
★ **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**に対する必要な監督を行わなければならない。(第21条)
★ **委託先**に対する必要な監督を行わなければならない。(第22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)

個人情報保護法対策　10ヶ条

	経営者	情宣	総務法務	営業サポート
1．個人情報保護規程を作る			●	
2．社員教育を実施する			●	
3．個人情報用APの運用管理(入力/訂正/削除)を実施する		●	●	●
4．個人情報DBサーバのアクセス管理(ログ)をする		●		
5．個人情報の取扱(利用目的/同意)を明確にする				●
6．委託契約書の再整備をする		●	●	
7．苦情窓口を明確化する	●			
8．プライバシーポリシーを公表する	●			
9．社内運営体制、責任を明確化する	●			
10．法令、規範を遵守する	●	●	●	

第一章　ISMS、Pマーク　取得分析

1．取得の作業フローは、個人情報保護法対策、ISMS、Pマークとも、ほぼ同一フローである

2．一般的に経験豊富なコンサルに一部委託した方が、短期間、低コストで取得が可能である

11

ISMS、Pマーク　比較

		Pマーク	ISMS
所　管	認定機関	財団法人　日本情報処理開発協会	
	名　　称	プライバシーマーク制度	ISMS適合性評価制度
	目　的	個人情報の保護に関する個人の意識の向上を図ること、民間事業者の個人情報の取扱いに関する適切性の判断の指標を個人に与えること、民間事業者に対して個人情報保護措置へのインセンティブを与えることを	わが国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られる情報セキュリティレベルを達成すること
	審査団体	指定期間　4社	審査登録機関　14社
	基　準	JIS　Q　15001:1999	JIS　X　5080:2002
実　績	開始年月	1998.04	2002.04
	認定社数	902　社　(2004.10.6)	522　事業所　(2004.10.5)
	審査期間	6～8ヶ月	1～1.5ヶ月
	対　象	全社	事業部

12

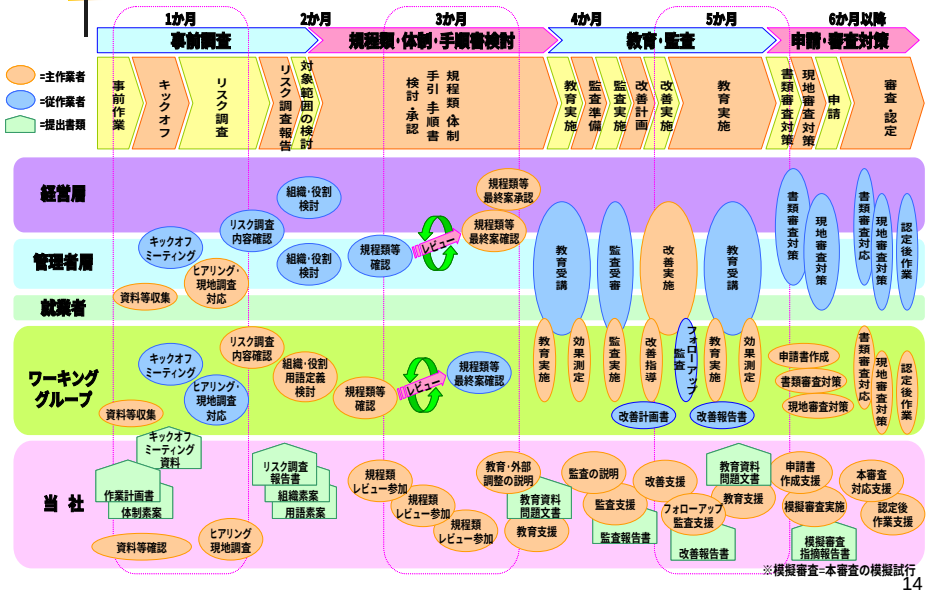
ISMS/Pマーク　取得作業フロー

1．キックオフ
2．事前調査・現状把握
3．情報資産調査
4．リスク分析・評価
5．リスク管理
6．規程類の策定・改訂
7．基準、実施手順書の策定・改訂
8．（システム再構築）
9．教育・訓練
１０．（運用の実施）
１１．内部監査の実施
１２．審査準備
１３．受審
１４．認証取得

一般的な
作業フロー

13

取得準備作業例



14

工数と人件費

モデル企業 ： 従業員２００名以下の情報処理部門がある企業 （人日単価：内作４万円／日、ｺﾝｻﾙ１２万円／日）

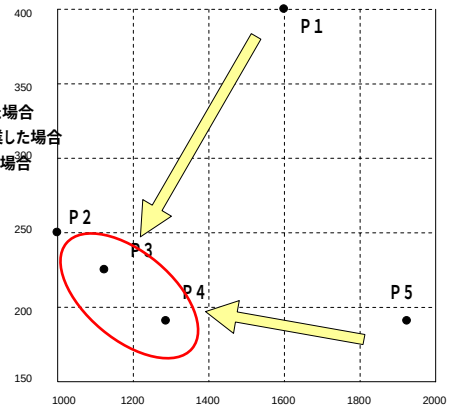
		P1	P2	P3		P4		P5	
		内作	内作	内作	ｺﾝｻﾙ	内作	ｺﾝｻﾙ	内作	ｺﾝｻﾙ
事前調査	全体計画、体制	15	10	8	2	6	4	4	8
現状把握	組織・業容、規程類調査	25	20	14	2	10	6	4	10
情報資産調査	資産洗い出し、資産台帳作成	40	30	28	3	15	6	4	20
リスク分析	リスク分析・評価	40	20	18	3	10	6	4	12
リスク管理	管理策検討、管理台帳、対応計画	40	20	18	3	12	6	4	12
規程類作成	規程類、基準、手順書の作成	80	50	40	4	20	10	6	25
社員教育	計画、コンテンツ開発、実施	50	30	25	2	15	12	4	20
運用	規程、基準、手順書に基づく運用、修正	50	25	24	2	20	6	12	10
内部監査	計画、実施	30	25	20	2	14	4	4	16
審査準備	全体見直し	30	20	12	2	4	4	4	10
	工数 小計 （人日）	400	250	207	25	126	64	50	143
	工数 合計 （人日）	**400**	**250**	**232**		**190**		**193**	
	費用 小計 （万円）	1600	1000	828	300	504	768	200	1716
	総費用 （万円）	**1600**	**1000**	**1128**		**1272**		**1916**	

P1 → セキュリティマネジメントをよく知らない一般的企業
P2 → 企業でマネジメントに精通している人がいる 又は、ISO9000/14000を取得している企業
P3 → Ｐ２企業が、セキュリティコンサルをアドバイザとして活用した場合
P4 → Ｐ２企業が、社員を主体にセキュリティコンサルと一緒に作業した場合
P5 → Ｐ２企業が、セキュリティコンサルに、実作業を全面委託する場合

15

最適化への検討（1）

P1 → セキュリティマネジメントをよく知らない一般的企業
P2 → 企業でマネジメントに精通している人がいる
又は、ISO9000/14000を取得している企業
P3 → Ｐ２企業が、セキュリティコンサルをアドバイザとして活用した場合
P4 → Ｐ２企業が、社員を主体にセキュリティコンサルと一緒に作業した場合
P5 → Ｐ２企業が、セキュリティコンサルに、実作業を全面委託する場合



1．コンサルに、一部委託したほうが、
短期間で低コストで、取得ができる。

2．コンサルに全面委託するより、社内工数を掛けた
ほうが、低コストでほぼ同工数で取得できる。

【最適取得のための考察】

① 社内工数＋コンサルタント の共同作業が望ましい
② 総工数は、１９０～２３０人日程度 かかる
③ 総人件費は、１１００万円～１３００万円程度 かかる

16

最適化への検討（2）

		P2	P3			P4		
		内作	内作	ｺﾝｻﾙ	効率	内作	ｺﾝｻﾙ	効率
事前調査	全体計画、体制	10	8	2	100%	6	4	100%
現状把握	組織・業容、規程類調査	20	14	2	80%	10	6	80%
情報資産調査	資産洗い出し、資産台帳作成	30	28	3	103%	15	6	70%
リスク分析	リスク分析・評価	20	18	3	105%	10	6	80%
リスク管理	管理策検討、管理台帳、対応計画	20	18	3	105%	12	6	90%
規程類作成	規程類、基準、手順書の作成	50	40	4	88%	20	10	60%
社員教育	計画、コンテンツ開発、実施	30	25	2	90%	15	12	90%
運用	規程、基準、手順書に基づく運用、修正	25	24	2	104%	20	6	104%
内部監査	計画、実施	25	20	2	88%	14	4	72%
審査準備	全体見直し	20	12	2	70%	4	4	40%
	工数　小計　（人日）	250	207	25	93%	126	64	76%
	コンサル比率				**11%**			**34%**
	工数　合計　（人日）	**250**	**232**		**93%**	**190**		**76%**

[最適取得のための考察]

① コンサルは、全工数の約10% (P2) ~30% (P1) 程度が望ましい
② コンサル投入による効果は、プロジェクト推進、技術的項目、課題早期発見と解消　である
　特に、大きい効果は、現状把握、規程類作成、内部監査　である。
③ 社内担当者の精神的拠所、プロジェクトの品質向上　等の間接的効果がある。

17

第二章　取得前企業分析

1．取得前企業分析では、規程類、契約書、社員教育、アクセス制御　に、課題がある

2．個人情報保護法への対策では、苦情処理、個人情報の社内取扱　に、課題がある

1．課題は、コンサルの参加より、飛躍的に改善される　←　前章

2．課題は、各担当部署より普段より作成、実施できる項目が多い

18

リスク評価と監査での指摘事項

［大塚商会セキュリティコンサル実施企業分析］

◆JIS Q 15001の項目(( )内および網掛け部分はJIS X 5080の項目)
※「4.4.4.2」はJIS X 5080の該当事項に細分化している。

Point	件数 緊急	通常	指摘		
21			21	4.2	個人情報保護方針（3 セキュリティ基本方針）
109	3	38	24	4.3.1	個人情報の特定（5 資産の分類及び管理）
33	1	8	14	4.3.2	法令及びその他の規範（12 適合性）
125	5	40	30	4.3.3	内部規程（3.1.1 情報セキュリティ基本方針文書）
32	1	13	3	4.3.4	計画書
50		20	10	4.4.1	体制及び責任（4 組織のセキュリティ）
138	17	21	45	4.4.2.1	収集の原則
82	4	15	40	4.4.2.2	収集方法の制限
43	2	15	7	4.4.2.3	特定の機微な個人情報の収集の禁止
30	4	2	14	4.4.2.4	情報主体から直接収集する場合の措置
77	7	18	20	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
107	3	22	54	4.4.3.1	利用及び提供の原則
113	6	37	21	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
36	2	6	18	4.4.4.1	個人情報の正確性の確保
98	2	34	24	6	*人的セキュリティ*
124	4	50	12	6.3	*セキュリティ事件・事故及び誤動作への対処*
81	3	31	10	7	*物理的及び環境的セキュリティ*
102	2	36	24	8	*通信及び運用管理*
111	28	12	3	9	*アクセス制御*
104	1	50	1	10	*システムの開発及び保守*
92	2	41	4	11	*事業継続管理*
168	7	61	25	4.4.4.3	個人情報の委託処理に関する措置（4.3 外部委託）
108	3	40	19	4.4.5.1	個人情報に関する権利
119	2	54	5	4.4.5.2	個人情報の利用又は提供の拒否権
151	9	46	32	4.4.6	教育（6 情報セキュリティの教育及び訓練）
132	2	62	2	4.4.7	苦情及び相談
108	2	37	28	4.4.8	コンプライアンス・プログラム文書
76	2	34	2	4.4.9	文書管理（12.1.3 組織の記録の保護）
108	3	47	5	4.5	監査（12.3 システム監査の考慮事項）
110	1	45	17	4.6	事業者の代表者による見直し（3.1.2 見直し及び評価）

◆緊急改善を3、通常改善を2、指摘事項を1で加算

19

指摘事項の傾向 (1)

- **「個人情報の特定」関連**
  - 部署/個人で勝手に集めて使用。
  - 安全管理、情報の精度の確保に問題がある。
- **「内部規程」関連**
  - 個人情報の定義、機密区分、取扱いルールがない。
  - 属人的対処、対症療法的施策のみ。全体最適化を図っていない。
  - 規程を就業者に公開していない。規程から業務で何を直したら良いかが見えてこない。
  - ルールを実施する体制、リソース、ツールがない。
- **「教育」関連**
  - 業務に即した教育を行っていない。
  - 4月の新採用時等の定型的、一時的な教育しか行っていない。
- **「収集、利用目的、個人の権利」関連**
  - 個人情報保護の意識が十分でなく、何をしたら良いかわかっていない。
  - 利用目的の範囲が不明瞭。利用目的外利用に関する規定もない。
  - Web上のプライバシーポリシーが、自社の権利やシステムセキュリティに終始して、不十分。
  - 保管期間の意識がない(放置によるリスクの高まり)。

20

指摘事項の傾向 (2)

- 「委託」関連
  - 形式上の守秘約款しかなく、守秘対象物の明確化、授受管理、監督・監理、業務終了時の守秘対象物の取扱い管理(返却/機密廃棄)等を行っていない。
- 「提供」関連
  - 事前の本人同意を得ずに提供し、または提供を受けている。
- 「情報システム対策」関連
  - リスクの変化に対応していない。気づいたことしかやっていない。
  - 手間のかかることは重要そうでも後回しにする(リスクの放置)。
  - システム内容、対策、運用等について見直しを行っていない。
  - 情報システム管理部署・担当者のみで対策を終始し、抱え込む。
- 「監査」関連
  - 「個人情報保護監査」の視点がない。
  - 監査組織がシステム監査までやれない、やりたがらない。
  - 個人情報保護について監査できるほどの管理統制を行っていない。

21

指摘事項の傾向 (3)

- 「苦情対応」関連
  - 責任不在。苦情対応は放棄し逃げることができない業務。
    - 大変すぎて手を付けることができない。「予防」だけで手いっぱい。
    - 「最後の砦」である苦情対応の重要さを認識していない。
    - 個人情報保護法完全施行後に多発すると思われる苦情集団を認識していない。
  - 問い合せ、相談といった「苦情の芽」のすべてを集中管理するマンパワーを確保していない。
    - 「苦情の芽」と気づくためのセンスとセンサーを育んでいない。
  - 現場レベルで対処し、隠蔽している。苦情の集中管理・対応が必要
- 「代表者による推進、見直し」関連
  - 対症療法しか行っていないので、マネジメントシステムもPDCAサイクルもない。
  - 目的、目標、ビジョンがないので何をどうしたら良いか思いつかない。
  - 「それどころじゃない」
    - 収益の数字に直接結び付かない事項は二の次
    - 経営・事業継続への影響を認識していない。
  - 担当者、担当部署に任せて十分と考えている(管理体制・機能、管理能力、知識、情報がない)。

22

第三章　個人情報保護法対策の推進法

1．今から自部署内で、できることから始める事が肝心である

2．保護法への対策ができれば、ISMS認定、Pマーク取得は、容易に取得可能である

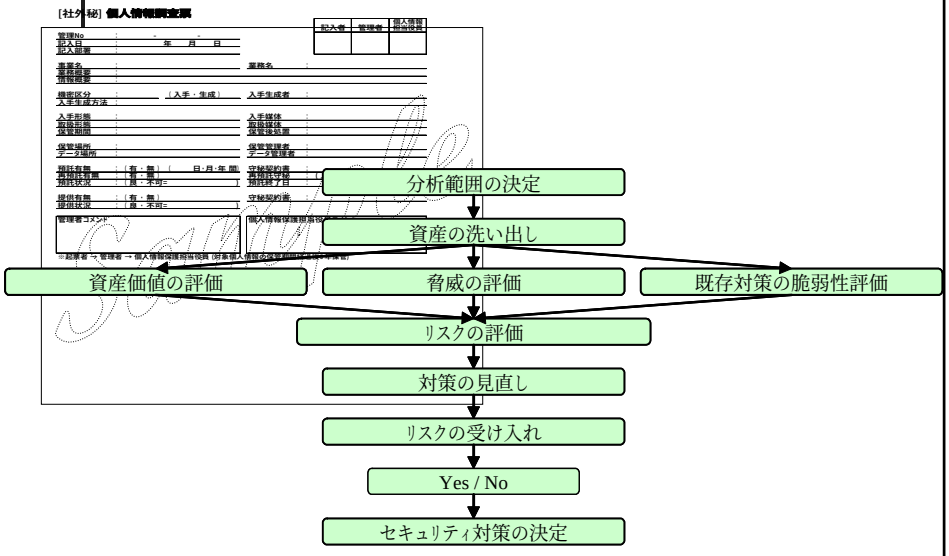
23

個人情報保護法対策のポイント

部署内	① まずは個人情報を特定しよう	リスク評価 (安全管理策検討)
	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	
コンサル	⑤ 利用目的をちゃんと決めよう	利用目的、適正取得
	⑥ 提供、委託を管理しよう	規程類、基準見直し
	⑦ 廃棄、削除、消去をきちんとしよう	委託先の監督
	⑧ 危機管理しよう	苦情処理、危機管理
全　社	⑨ 個人情報保護の組織体制を創ろう	全社統制
	⑩ 態勢を維持向上しよう	従業員の監督
	⑪ 企業倫理とコンプライアンスに統合しよう	維持向上
	⑫ 計画立ててみんなで目的･目標を持って進めよう	

24

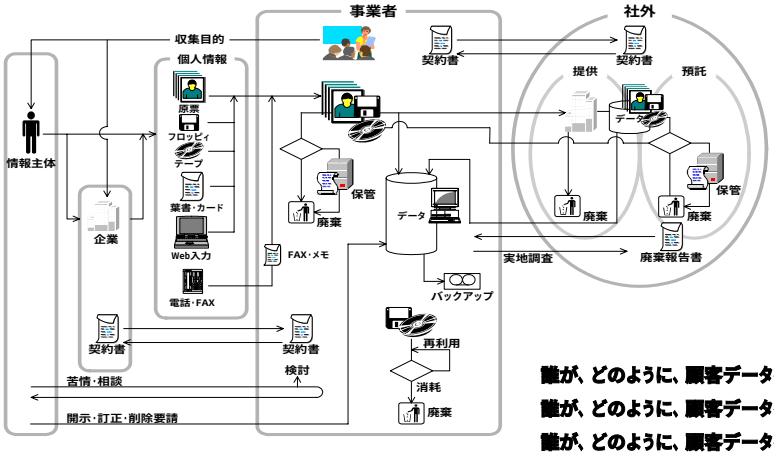
①まずは個人情報を特定しよう



25

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？

26

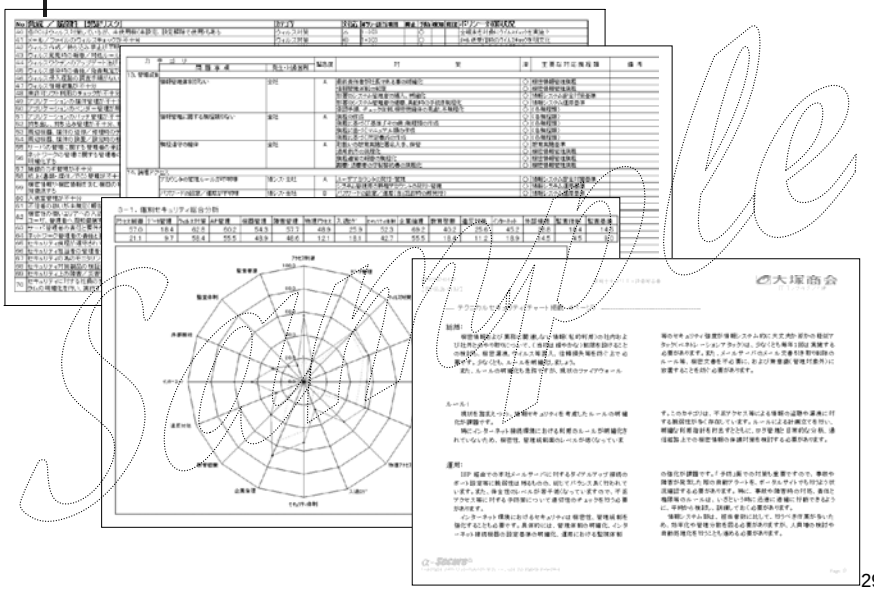
「本人の意思の尊重」のポイント

- 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

③個人情報保護の管理状況を確認しよう

※『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

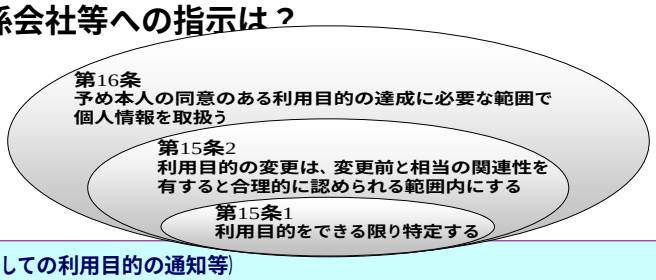
④個人情報のリスクを共通認識しよう



29

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。

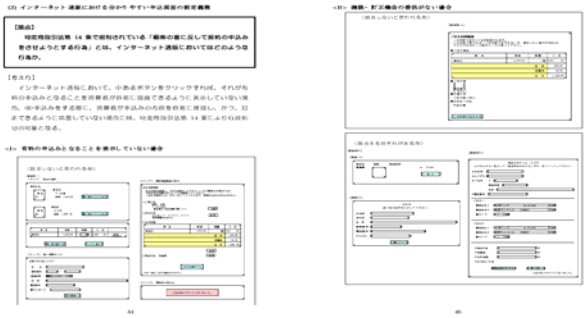
妥当な利用目的とは

- 法的要請、業務の要請 → 業界基準、ガイドライン
- 収集項目 → 必要最低限なものにする
- 安全性対策、管理・態勢 → 業界基準、ガイドライン
- 保有期間 → 法や業務の要請
- 収集・利用時の注意 → 保有者は誰か
  - 自社の権利と義務 → 予め説明責任を確保する
契約、約款(明示・告知・同意)
  - 個人の権利と義務 → 制限、告知義務・通知義務、安全管理等要請事項
  - 法的要請等への対応 → 司法・税務命令、任意要請
  - 媒体に応じた注意 → 明示証拠、同意確保の妥当性
- 開示・訂正・削除・利用停止 → 本人確認、対応マニュアル・訓練
  - 制限・期間 → 応じられない内容と根拠、判断者、判断基準、手順
  - 費用 → 相談等の拒否にならない費用
- 再利用、利用者範囲 → 商品DM、関連会社
- 委託・提供 → 業務委託、関係会社
  - 受けるもの、出すもの → 「第三者提供」の明確化
  - 相手先管理、安全管理 → 業者選定基準
  - 責任の所在と限界 → 委託契約等の守秘約款
- 相談、クレーム、苦情 → 相談窓口、問合せ方法、業界団体、ADR、オンブズマン
- その他 → 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

31

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

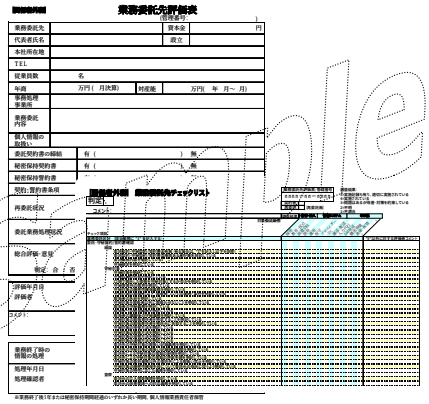


- その他の参考：特定商取引法(特に第11、12、14条)、電子契約法

32

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。



33

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

34

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

35

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

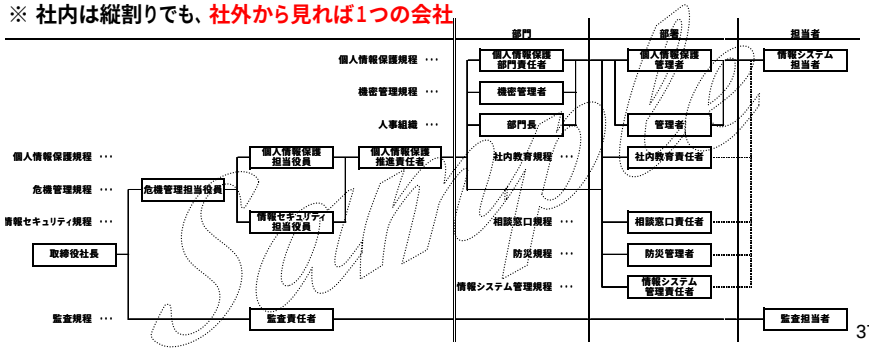
36

⑨個人情報保護の組織体制を創ろう

- **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**

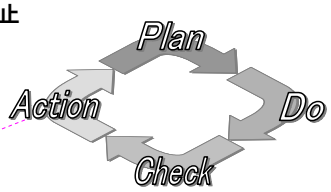
※ 社内は縦割りでも、**社外から見れば1つの会社**

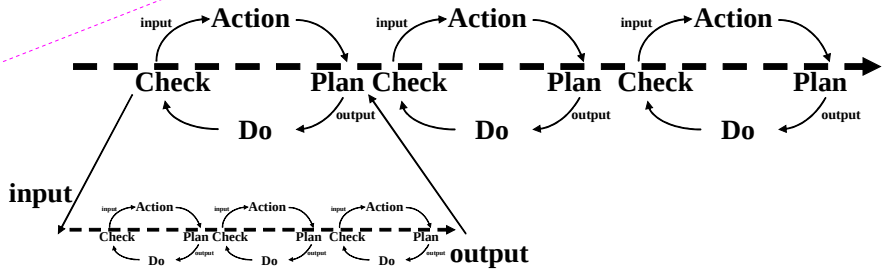


37

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**





38

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

39

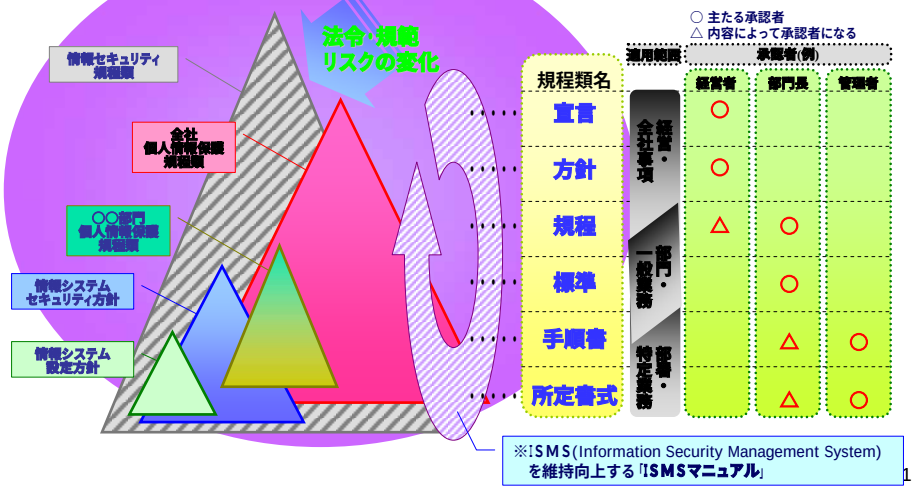
「個人情報保護態勢」のポイント

- 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

40

⑪企業倫理とコンプライアンスに統合しよう

企業倫理・コンプライアンス



※ISMS(Information Security Management System)を維持向上する「ISMSマニュアル」

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(例)

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

「安全性の確保」のポイント(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

43

「安全性の確保」のポイント(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

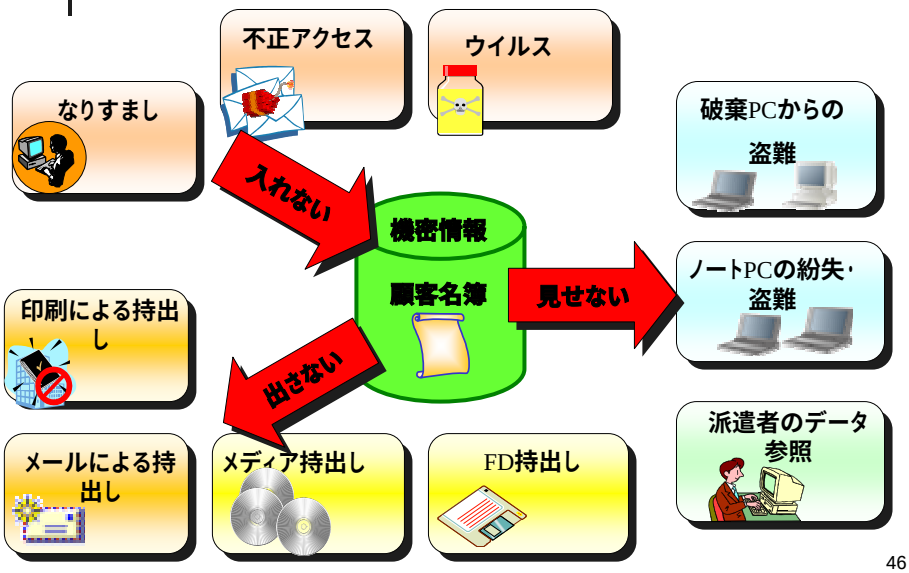
44

「安全性の確保」のポイント(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

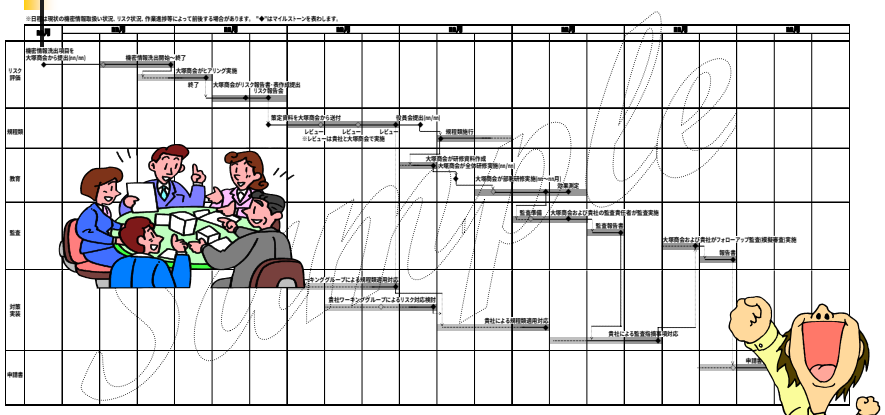
45

出さない、入れない、見せない



46

⑫計画立ててみんなで目的･目標を持って進めよう



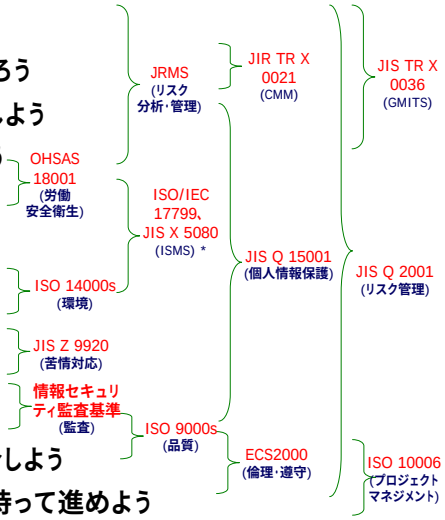
- いつまでに、誰が何をどうするか
- 法令･規範･リスク評価･監査上、妥当か
- どのような対策をおこなうか
- 全体的に、施策と結果をどう評価するか
- 達成、充足の評価はどうか

たとえば．．．

ISMS

個人情報保護態勢の構築と規範例

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



* **ISMS**: Information Security Management System

講演のまとめ

1．まずは、個人情報保護法対応後、ISMS、Pマーク取得を検討しましょう

2．個人情報保護法対応、ISMS、Pマーク取得には、経験豊富なコンサルタントに一部委託すると早く安く実現できます

3．社内特定部署（例えば情報システム室、法務部）にて、今自分達でできることから準備しましょう
準備が早ければ早いほど、さらに早く安く実現できます

〔追加要件〕
4．取得には、経営者及び社内各部署との理解と協力が不可欠です
5．取得には、最低3ヶ月(通常6ヶ月) の準備期間が必要です
6．取得には、2名以上の社内専任化(又はプロジェクト)が必要です
（社員200名まで2名、300名増える毎に1名）
7．取得時は、取得要件を網羅的に満足することが必要です
（各々の項目の強化は、取得後次の更新までの中期計画にて行います）

49

「個人情報保護法」施行まで半年
今、我々が対処すべきことは！

全員参加のＣＰ作成と意識アップ

ご静聴ありがとうございました

50