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

個人情報保護のガイドライン

NPO JNSA
個人情報保護ガイドライン作成WG

㈱大塚商会 佐藤 憲一

2002 年 11 月15日

第一章 個人情報保護法

【 ゴール 】

１．個人情報保護法の概要を理解する
２．個人情報保護法による企業の義務を理解する

個人情報保護法

平成13年3月 閣議決定
平成14年6月 通常国会に提出も再検討

第1章 総則
　目的(第1条)
　定義(第2条)
　　個人情報、個人情報データベース等、個人情報取扱事業者、個人データ、保有個人データ
第2章 基本原則(第1条～第8条)
第3章 国及び地方公共団体の責務等
　国及び地方公共団体の責務(第9条、第10条)
　法制上の措置等(第11条)
第4章 個人情報の保護に関する施策等
　第1節 個人情報の保護に関する基本方針(第12条)
　第2節 国の施策(第13条～第15条)
　第3節 地方公共団体の施策(第16条～第18条)
　第4節 国及び地方公共団体の協力(第19条)
第5章 個人情報取扱事業者の義務等
　第1節 個人情報取扱事業者の義務
　第2節 民間団体による個人情報の保護の推進
第6章 雑則
第7章 罰則
附則

POINT

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)。 （第二条 1.）

e－Mailアドレス

あらゆる「人」に関する全情報が対象

- 顧客情報
- 私的情報
- 名刺情報
- 社員情報

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、学業・学歴、資格、賞罰、成績、公的扶助、趣味・嗜好等の記録
資産・収入 －－ 資産状況、収入状況、納税状況、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

個人情報取扱事業者

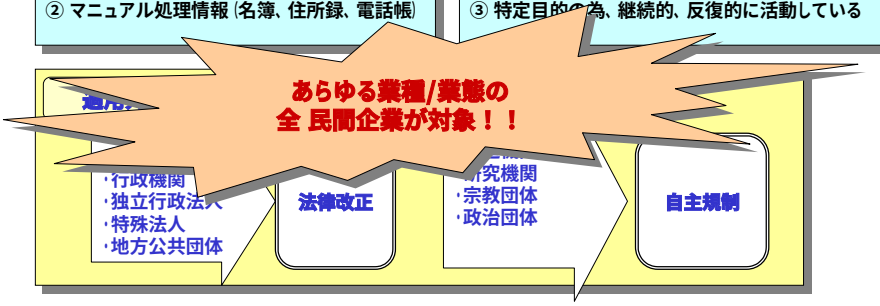
1. 個人情報データベース等を事業の用に供している者 （第二条 3.）

「個人情報データベース等」を保有

① 個人情報をコンピュータを利用して検索できる体系に構成されたもの
② マニュアル処理情報（名簿、住所録、電話帳）

「事業」

① 法人、個人を問わない
② 公益活動、営利活動等を問わない
③ 特定目的の為、継続的、反復的に活動している



2. 個人情報データベースに5000人（1000～10000人の範囲）以上を保有

個人情報取扱事業者の義務

第4条 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20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21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23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28条）

第5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22条）

第6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24条）

第7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25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26、27条）

第8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29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30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31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32条）

苦情の適切かつ迅速な処理に努めなければならない。（第36条）

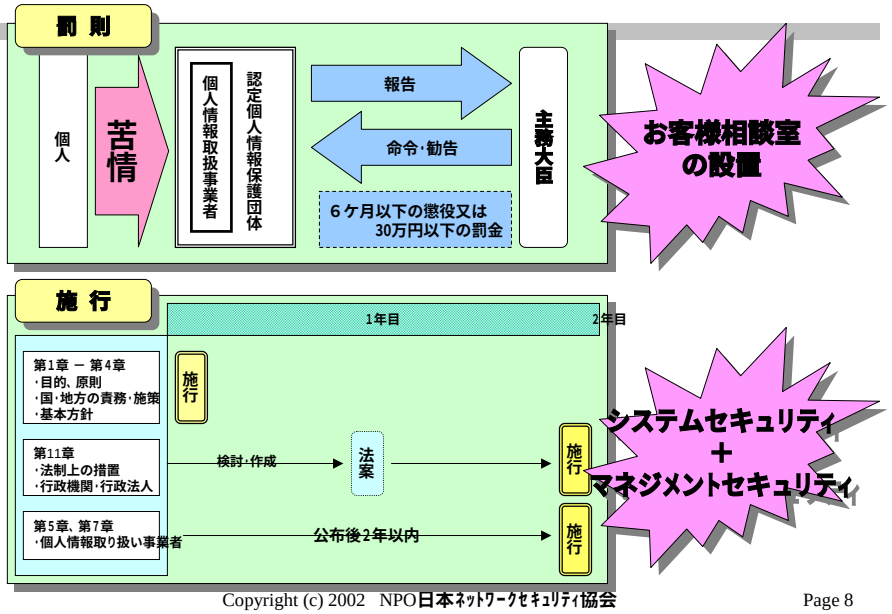
第7条　安全性の確保

第25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26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27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。

個人情報保護法の罰則と施行



第二章　ＪＮＳＡ　個人情報保護ガイドライン作成ＷＧ

【　ゴール　】

１．個人情報保護ガイドライン作成ＷＧの活動方針並びに進捗を説明いたします

活動方針

１．背景

国会で審議されている『個人情報保護法』が成立された場合、ＪＮＳＡ会員企業のみならず民間企業のほとんどが、「個人情報取扱事業者」となり、この法律の対象企業となる。
しかしながら、この法律は、曖昧さ、不明確さが非常に多く、企業が遵守する為の標準的ガイドラインの作成、公開が不可欠であると認識した。この為、政策部会は、平成１４年度、「個人情報保護ガイドライン作成ワーキンググループ」を発足させることにした。

２．活動目的

① 個人情報取扱事業者となる民間企業が、個人情報保護法を遵守し、健全な経営活動を行なう為に必要なガイドラインを作成する。

民間企業：情報サービス業、製造業、流通業、建設業、サービス業 等々の一般業種
除外1：保護法上の適用除外→政治団体、宗教団体、学術研究期間、報道機関
除外2：所轄省庁から別途指導が出ている業界→金融業、医療機関 等々

② 作成したガイドラインは、ＪＮＳＡ参加企業は勿論の事、広く民間企業へ公開、流布し、ＪＮＳＡの知名度を向上させる

具体的活動方法

第一ステップ　：　保護法の全体的理解を深める
→　モデル企業を想定し、その企業が個人データを入手、保管、加工・修正・利用、破棄するまでのワークフロー上、個人データと保護法との関与を大雑把に整理する

第二ステップ　：　個人データと保護法の関係を整理整頓する
→　ワークフロー毎に、脅威、システム、運用、組織の項目を作成し、整理する

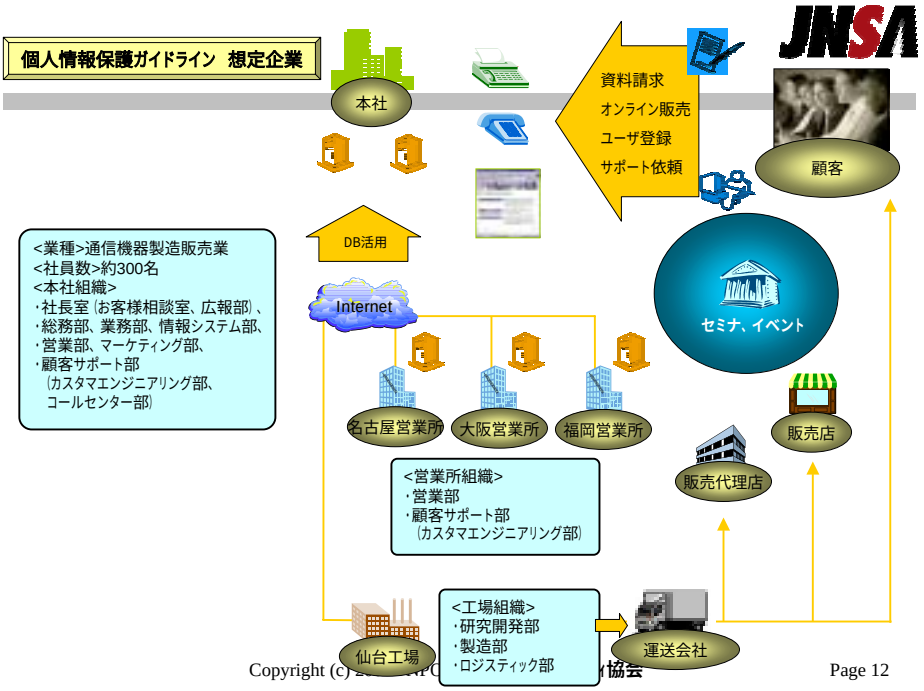
第三ステップ　：　具体的対策、テンプレートの作成
→　ワークフロー上、企業が対処すべき具体的対策、または標準的テンプレートを作成する
また、この作業により、ガイドラインの基本が完成する（Ｖｅｒ０．６？）

第四ステップ　：　見識者とのレビュー
→　作成したガイドラインについて、見識者、主務大臣による指針　等より、レビューを実施し、精度を向上させる

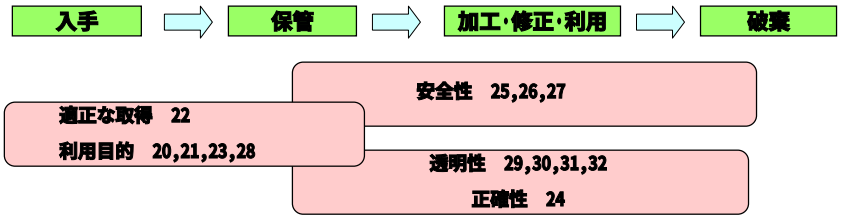
第五ステップ　：　ガイドライン　Ｖｅｒ０．８
→　民間企業が、理解しやすい、読みやすい校正、内容とする

来春

第六ステップ　：　ガイドラインの公開
→　ガイドラインは、「出版物」or「ドキュメント」として、広く公開させる為のしくみを構築する



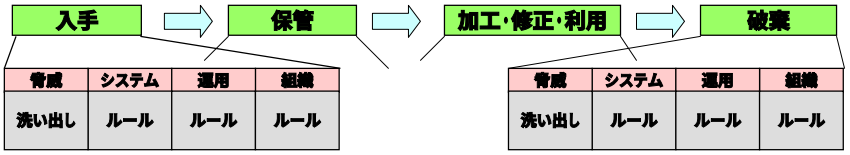
データフローと5つの原則



	責任の原則（OECD8原則）（第3条）	個人情報が個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ、個人情報を取り扱う者は、以下の基本原則にのっとり、個人情報の適性な取扱いに努めなければならない。
5原則	利用目的による制限（第4条）	個人情報は、その利用の目的が明確にされるとともに、当該目的の達成に必要な範囲内で取り扱われなければならない。
5原則	適正な取得（第5条）	個人情報は、適法かつ適正な方法で取得されなければならない。
5原則	正確性の確保（第6条）	個人情報は、その利用の目的の達成に必要な範囲内で正確かつ最新の内容に保たれなければならない。
5原則	安全性の確保（第7条）	個人情報の取扱いにあたっては、漏えい、滅失又はき損の防止その他の安全管理のために必要かつ適切な措置が講じられるよう配慮されなければならない。
5原則	透明性の確保（第8条）	個人情報の取扱いに当たっては、本人が適切に関与し得るように配慮されなければならない。

JNSA個人情報WG

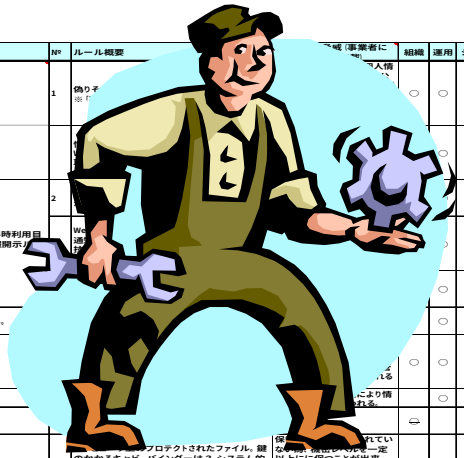
ルール化へのアプローチ



5項目	入手	保管	加工・修正・利用	破棄
安全性 25,26,27		アクセス管理 保管責任明確化 安全な保管方法 保管・取出しの手続き 保管・取出しのログ	アクセス管理 バックアップ 利用ルール 入退室管理 アクセスログ 機密保持契約	廃棄のルール 廃棄業者選定 廃棄証明のルール
適正な取得 22	取得時遵守事項			
利用目的 20,21,23,28	取得時利用目的通知・公表のルール プライバシーポリシの公表	合併・分社時の利用ルール	個人情報利用時の遵守事項と承認ルール	
透明性 29,30,31,32		個人情報管理方法 個人情報開示・訂正手続き		
正確性 24		個人情報更新ルール	個人情報更新ルール	削除ルール
基本精神 3	※5つの原則について、共通事項として、 ルールを定め運用すること。 教育・啓蒙、罰則			

JNSA個人情報WG

ルールとJIS対応表



フェーズ	ルール	№	ルール概要	組織	運用	システム	JIS X 5080	JIS Q 15001	個情保法
入手	取得時遵守事項	1	偽りそ	○	○	⇔	3.1.1, 4.1, 6.1, 8.7, 9.4, 10.3	4.2,4.3,4.4.1, 4.4.2	5.22
					○	○	3.1,	4.4.2	5.22
		2					3.1	4.4.3	5.20
	個人情報の種別ごとに、取得時利用目的通知・公表のルール（情報開示ルールの提示）		We		○	○	6.1.1, 6.1.3 6.2 8.6.3	4.4.3	5.23
					○		3.1, 8.6.3	4.4.3	5.20,5.23,5.28
保管	アクセス管理ルールを定める。				○	○	3.1, 9全般	-	5.25
	ＤＢ（個人情報）管理			○	○	○	4.3, 6全般, 8全般	4.4.4	5.24,5.25,5.28
	第３者からの取得情報管理				○	○	8全般	4.4.4	5.24
	保管責任を明確にする。			⇔					
	保管の方法を定める。（安全保管ルール	9	プロテクトされたファイル、鍵のかかるキャビ、バインダーは？ システム的対応、及びnetwork対応、許可されたユーザのみアクセスでき、開示要求に即応できる方法で保管する。	○	○	○	7全般、9全般	4.4.4	5.24,5.25,5.29,5.33,5.34

標準テンプレート・例

標準テンプレート･例

第三章　個人情報保護への緊急対策法

【　ゴール　】

１．企業内にて、個人情報を保護する為に、
即実現可能な対策について説明します

個人情報の流出 (1)

●1995年5月、消費者金融「プロミス」の顧客データ約20万人分が元社員が落ちだして逮捕。
●1996年8月、全国信用情報センター連合会から80万件以上の情報流出し、3人が逮捕。
●1998年1月、派遣プログラマらが、さくら銀行の顧客データ約2万人分を持ち出して逮捕。
●1998年1月、高島屋の顧客データ約50万人分が名簿業者に流出した。
●1998年1月、大手人材派遣会社「テンプスタッフ」の派遣社員9万人分の情報が流出した。
●1998年4月17日、宇治市乳幼児検診システムの開発を受注した会社の元大学院生のアルバイト男性が21万人分の住民情報が入ったMOを不正にコピーして持ち出した。
●1999年7月、社員ら88人が関係して、NTT東・西日本とNTTドコモの顧客情報を持ち出して、解雇された。

●2000年2月22日、千葉県警は、電話利用者の個人データ計1600件を外部に漏らしていたNTT東日本神奈川支店の男性元社員(56)と、120万円を受け取っていたNTT東日本千葉支店の男性社員(52)を懲戒解雇後に、NTT法違反容疑で逮捕。
●2000年2月21日、民間のシンクタンク「PHP研究所」、1万6000人以上の個人情報が無防備な状態のまま放置されていたことが判明した。
●2000年3月1日、「プレイステーション2」予約で、PlayStation.com Japanの運営を担当している日本アイ・ビー・エムのサーバーに対して不正アクセスがあり、顧客情報が流出していたことが判明した。
●2000年3月2日、警視庁公安津は1997年10月にオウム真理教(アレフに改称)関連のコンピュータ・ソフト会社に発注した本田技研の人事管理システムで、約3000人分の管理職名簿が流出していたことを発表した。

 参考：CAMBER WEB

個人情報の流出 (2)

●2000年3月12日、「大塚製薬」が公開している「カロリーメイトバランスチェック」に登録した人の住所、氏名、年齢、電話番号をはじめ、身長、体重、食事内容、運動量、妊娠の有無などの個人情報約9900人分が、約2カ月間にわたって閲覧できるようになっていたことが、分かった。登録者全員にメールでおわびするというが、約9900人分のメールはトラフィックの邪魔であり、スパムといえる。
●2000年10月25日/キャラクターグッズの販売ビジネスなどを手掛けているソニー系のソニー・クリエイティブプロダクツは、ユーザー3000人に新製品を告知する電子メールを送信しようとしたところ、誤って送信先の3000人分全員のメールアドレスが掲載された一覧表を送信してしまった。
●2000年10月30日/ハウステンボスジェイアール全日空ホテルが顧客1500人に新サービスを告知する電子メールを送信したところ、誤って顧客の氏名と電子メールアドレスが本人を含めて全顧客にも見える状態のまま送信した。
●2001年1月23日/イー・アクセスが、電子メールで情報の配信を申し込んでいたユーザーのメールアドレス約2万6000件を、自動配信システムのプログラムミスが原因で、誤って外部の約1000人に送信していた。
●2001年2月15日/リクルート社が運営する情報サービス「キーマンズネット」で会員情報が一部サービスを停止し、第3者に閲覧可能になっていたことが判明した。
●2001年7月17日/ソニー系列の化粧品会社ソニーCPラボラトリーズで顧客約1万人の氏名、住所、メールアドレスがインターネット上で閲覧可能な状態になっていたことが分かった。
●2001年10月23日/豊能税務署で、納税者約60人分の個人データが入力されているパソコンを紛失した。

 参考：CAMBER WEB

個人情報の流出（3）

●2001年10月25日/国内線航空券をインターネットで予約するサービスを提供している「国内線ドットコム」が、会員約4000人分のメールアドレスが表示した広告メールを誤って配信した。
●2001年10月29日/NTTドコモ埼玉支店、明治乳業、レナウンでも登録者のメールアドレスの流出事故を起こした。
●2001年11月7日/法の番人である法務省が、メールアドレスを登録していた約5000人のあて先欄に1メールに付き、それぞれ約20人づつアドレスを書いて誤送信し、アドレスが漏れた。

●2002年1月31日/静岡朝日テレビは、番組への意見などをメールで寄せた視聴者約1900人に対し、担当者が会員制サイトの案内メールを送ったとき、ほかの視聴者のアドレスも誤って送信した。
●2002年5月26日/エステティックサロンTBCのサイトから、資料を請求した人など約3万人の住所、名前、電話番号、メールアドレスなどの個人データが漏洩した。
●2002年6月16日/CATV業者であるメディアッティ・コミュニケーションズ(シティケーブルネット)で加入申込書個人情報の漏洩があった。
●2002年7月2日/パソコン学院「アビバ」のWebサイトから約1200人分の個人情報が流出した。

 参考：CAMBER WEB

個人情報の流出（4）

●2002年7月6日/電子自治体推進パイロットを推進している北海道の深川市のマルチメディア・センターが提供しているインターネット接続サービスの登録者1551人のメール・アドレス、388人分のイントラネット利用者のデータなど、1900件の個人情報が入ったパソコン1台が盗まれた。
●2002年7月31日/関西電力とブロードバンド事業子会社ケイ・オプティコムが運営しているインターネット・カフェ「opti c@fe」の会員リスト1万7,324人分がインターネットで閲覧できる状態になっていた。
●2002年8月20日/NHKのホームページで、クレジットカード番号などの個人情報を盗んだり、偽の報道を掲載したり、偽の受信料申し込みページを作って、別の講座に振り込ませるようにできる欠陥が指摘された。
●2002年9月3日/アンチウイルスで知られるトレンドマイクロの製品「ウイルスバスター」のユーザー向け会員契約更新サイトで、ユーザー10人の氏名、メールアドレス、製品番号などが誤って表示されていた。
●2002年9月13日/NTTドコモの関連会社「ドコモ・システムズ」社員(26)が携帯電話の顧客の通話記録を持ち出し、創価大学生課副課長と、同大嘱託職員に渡した疑いで、警視庁保安課が逮捕した。
●2002年9月27日/アップルコンピュータのホームページで、利用者がアンケートに回答すると、他人の名前、住所、年齢、電話番号の他、使用しているパソコン、基本ソフト、購入時期、今後の購入計画などの個人情報が見られるプログラムミスが見つかった。
●2002年10月2日/筑波大学の学内専用の「新学務システム」に登録されていた全学生の顔写真が認証なしで、自由に閲覧できるようになっていた。

 参考：CAMBER WEB

UFJつばさ証券の顧客リスト流出、旧東和の1万人超分

参照：朝日新聞社

UFJつばさ証券（東京都千代田区）の顧客データが大量に流出し、東京都内の名簿業者に持ち込まれていたことが11日、わかった。同社の前身の一つ、旧東和証券の新宿新都心、赤坂、新橋の都内3支店の名簿とみられ、住所、氏名から口座の残高までが細かく記入されている。最大で1万1000人分にのぼるとみられ、UFJつばさ証券は7日、警視庁丸の内署に窃盗の疑いで被害届を出した。

旧東和証券は00年4月、ユニバーサル証券など3社と合併してつばさ証券となり、02年6月にはさらにUFJキャピタルマーケッツ証券と合併してUFJつばさ証券になっている。UFJつばさ証券によると01年10月、顧客から「つばさ証券の名簿を基に他社が勧誘に来た」などのクレームがあり、流出が発覚した。

今月になって流出名簿のうち2冊、約3200人分を入手して調べたところ、3支店のうち旧東和新宿新都心支店の00年2月末現在の顧客名簿であることが分かった。顧客の氏名、住所、生年月日や職場の連絡先のほか株式、債券など商品別の預かり資産額などが記入されていた。名簿は計7冊あり、全部で約1万1000人分になるとみられる。同社によると、データは合併直前の00年3月に旧東和のコンピューター端末機から引き出されたらしい。しかし、アクセス記録は00年3月以前分は消去されており、だれが引き出したか確認できないという。

旧東和で支店のすべての顧客データを見ることができるのは、支店長と経理担当課長だけとされていたが、「支店のパスワードと営業担当のID番号がわかれば、だれでもデータを入手することは可能だった」（UFJつばさ証券広報部）という。

名簿業者は「名簿は昨年の夏ごろに入手した。持ち込んだ人はだれだか分からない。何人に売ったかについては言えないが、うち以外にも出回っている可能性は高いと思う」と話している。

金融機関からの個人情報流出では98年1月、さくら銀行（当時）の約2万人分の顧客情報が名簿業者に持ち込まれたことが発覚した。このほかでは、昨年8月に小田急百貨店の社員が約38万人分の顧客情報を信用調査会社に売却したことが判明、自治体でも京都府宇治市で約21万人分の住民票データが流出（99年5月）するなど、被害は後を絶たない。

UFJつばさ証券の広報部長は「お客様に多大なご迷惑をかけ深くおわびします。今後は情報セキュリティー対策を重要な経営課題として、法令順守などの教育研修を重ねていくので、ご理解をいただきたい」とのコメントを出した。

昨今の情報漏洩→危機管理

TBC
ブルドックソース
ソニーシービーラボ
トレンドマイクロ
全日空ワールド
YKKアーキテクチュアル

ワコール、日本サムスン
花王、ソフマップ
国内線ドットコム、法務省
静岡朝日テレビ
明治乳業

さくら銀行、小田急、
高島屋、宇治市、
全国信用情報センター
NTT東日本、西日本
NTT Docomo
テンプスタッフ
富士通　防衛庁事件

Webサーバ管理 | ウイルス対策

システムセキュリティ対策

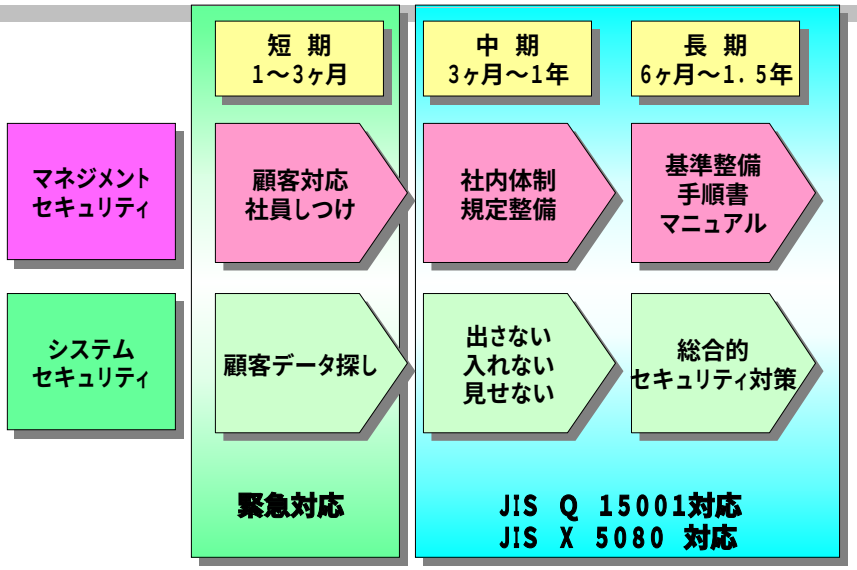
誤配 | 従業員（委託先）持ち出し

マネジメントセキュリティ対策

1. 企業の信用失墜
2. イメージダウン
3. 株価の下落
4. 損害賠償保証
5. 株主代表訴訟、社長交代

1. 売上低迷
2. 減給
3. リストラ
4. 倒産

マネジメント／システム　セキュリティ対策



顧客対応／社員しつけ

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

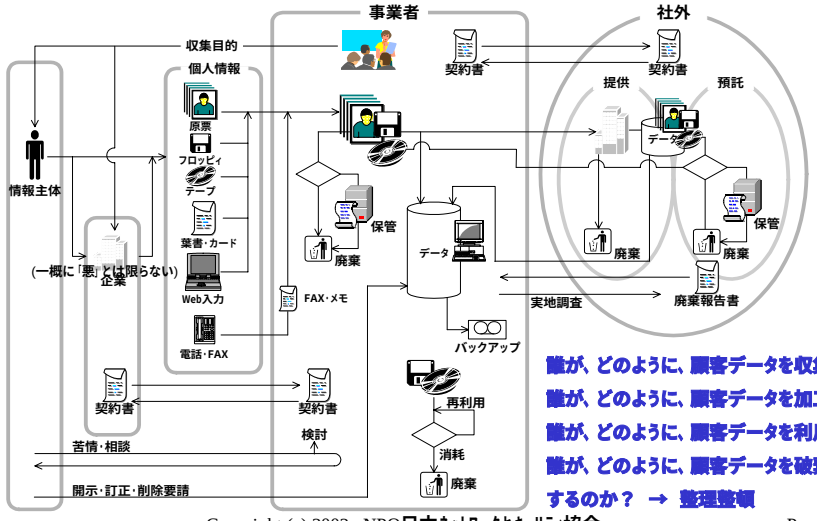
社員しつけの実施

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

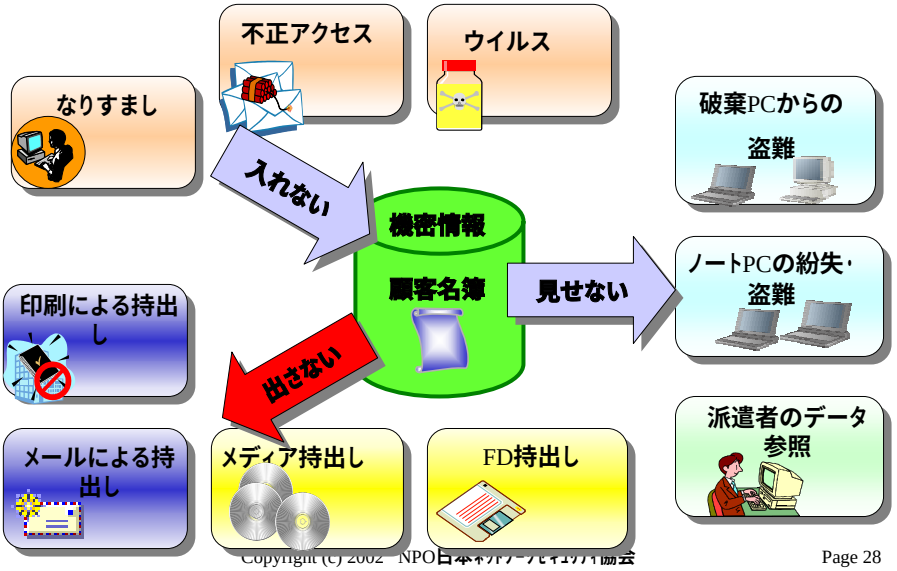
1．顧客からデータは、預からない
2．公共の場で、顧客名は言わない
3．ウイルス対策は怠らない
　：
　：
10．クレームは、待たせない　と

顧客データフロー分析



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、顧客データを破棄
するのか？ → 整理整頓

出さない、入れない、見せない



第四章　個人情報に関する規格／制度

【　ゴール　】

１．JIS　Q　15001を説明します

２．Ｐマーク制度を説明します

個人情報保護に関する制度･ガイドライン

個人情報保護制度

1) 国 －－ 行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律
2) 地方自治体 －－ 個人情報の保護に関する条例（1529団体）、個人情報の保護に関する規則、規定（865団体）
3) その他 －－ 民法（名誉毀損）、刑法（不正アクセス禁止法）、知的財産法（著作権法、特許法）

個人情報保護ガイドライン

1．国
　① 通産省1999年3月　「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）」
　　JIPDEC　→ http://www.jipdec.or.jp/security/privacy/JISQ15001.html
　② 郵政省1998年12月 「電気通信事業における個人情報保護に関するガイドライン」
　　http://www.tca.or.jp/japan/privacy
2．業界団体ガイドライン
　① JIS Q 15001に基いた業界ガイドライン
　　(社) 情報サービス産業協会、(社) 全国学習塾協会、(社) 全国信販協会 、電気事業連合会、
　　電子商取引実証推進協議会、電子ネットワーク協議会、(社) 日本クレジット産業協会、
　　日本コンパクトディスクレンタル商業組合、(社) 日本ダイレクト･メール協会、日本チェーンストア協会、
　　(社) 日本通信販売協会、 (社) 日本熱供給事業協会、日本百貨店協会、(社) 日本ガス協会、
　　結婚情報サービス協議会、 (社) 日本マーケティングリサーチ協会
　② その他代表的なもの
　　･「金融機関等における個人データの保護の為の取り扱い指針」（ (財) 金融情報システムセンター）
　　･「信用情報機関における個人信用情報の保護に関する指針」(全国銀行協会連合会、全国銀行信用
　　情報センター、全国信用情報センター連合会、 (社) 日本クレジット産業協会)

個人情報保護に関するガイドライン

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）

0 序章
1 適用範囲
2 引用規格
3 定義
4 コンプライアンス・プログラム要求事項
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
4.4.3 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

プライバシーマーク制度

1．制度概要　個人情報保護JISに適合したコンプライアンス・プログラムを整備し、個人情報の取り扱いを適切に行っている事業者を、第三者機関であるJIPDEC（及びその指定機関）が、評価・認定し、その証として「**プライバシーマーク**」と称するロゴの使用を許諾する制度

2．交付機関　（社）情報サービス産業協会、（社）日本マーケティング・リサーチ協会
（社）全国学習塾協会

3．交付数　392社　（平成14年10月2日）

4．国際化　米国・カナダBBBonlineと相互認定（2001.06.01）

プライバシーマーク制度（確認事項）

1．申請要件
次の欠格事項に適合しない民間事業者であること
① 3ヶ月以内にプライバシーマーク付与を否とする旨の決定を受けた事業者
② 2年以内にプライバシーマーク使用契約の解除を受けた事業者
③ 2年以内に個人情報の取扱いにおいて個人情報の外部への漏洩その他情報主体の利益の侵害を行った事業者

2．審査内容
方式審査→予備審査（→本審査）の順に行なわれる。

3．方式審査
申請書が申請基準の通りに揃っている事を確認し、受理するか否かを決定。受理によって、プライバシーマークの審査契約が成立し、審査料金の入金を確認することによって、予備審査に移行する。

4．予備審査
書類審査と現地調査があり、申請書類の内容が審査基準等に適合している場合に、現地調査を行なう。予備審査は、**JIS Q 15001および審査機関のガイドライン**に基づいて行なわれる。

5．更新手続き
プライバシーマーク使用許諾は、**2年間ごとに更新手続き**が必要。

プライバシーマーク審査最重要項目

1．規程類の整備
代表者が個人情報保護を宣言し、規程･細則･その他を整備していること

2．体制の整備
代表者によって個人情報の管理者が指名され、個人情報を適切に取扱う体制が整備されていること

3．周知徹底
年1回以上、個人情報の収集、利用及び提供に従事する者に対し、個人情報保護に係る周知徹底の措置（教育、研修等）を講じていること

4．システム監査
年1回以上、企業内の個人情報保護の状況を監査し、必要な改善および規程類の見直しを代表者が指示していること

5．常設の相談窓口の開設
個人情報保護に関する相談窓口が常設され、かつ明示･公開されていること

6．セキュリティ措置の実施
物理的･論理的に外部からの侵入又は内部からの漏えいが発生しないよう適正な安全措置を講じ、記録しチェック･報告後、保管管理していること

7．関連企業等との契約
個人情報の提供、業務委託は個人の同意を得て行ない、提供･委託先と守秘契約を締結する等、適切な個人情報保護が講じられるようにしていること

Pマーク取得企業の事例紹介

1.会社概要

1) 設立･売上高 －－ 1984年7月設立 (資本金 3億円)、2000年度売上 29億円
2) 従業員数 －－－ 150名 (内SE 140名)
3) 主な業務内容 － ①パッケージソフトウェア開発、②受託ソフトウェア開発、③先端技術調査

2. 取得の動機

設立以来15年間、業務用パッケージ販売、システムソリューション販売を行なってきた。
2000年度は、新たにASP、XML、セキュリティを基礎技術としたWebソリューション事業を展開することにした。また、日本政府は、IT基本法に基く各種政策、法案が整備する方向を示した。
この背景より、「個人情報保護」が21世紀の経営戦略上、大変重要な企業基盤になると判断し、その基本となる「プライバシーマーク」を取得することとした。

3. 取得の目的

① 企業の社会的信用度･信頼度を向上させる
② 社員および関連会社の個人情報、セキュリティに関するモラル向上を図る

Pマーク取得企業の事例紹介

4.具体的個人情報

① パッケージソフトウェアを購入された顧客情報
② お客様のシステム開発･テスト等を実施する上で、お客様から貸与された個人情報
③ Webサイト、セミナー、展示会 等々で収集した個人情報
④ 社員の個人情報

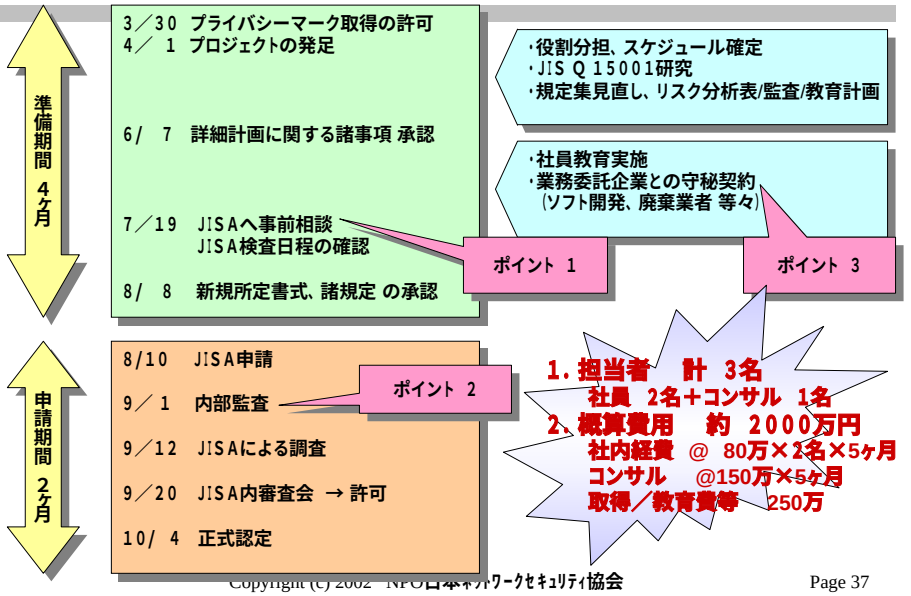
5.取得の効果

① 顧客からの信頼が向上した → 受注の増加、無茶な価格値引きの減少
② 業界･同業他社からの企業評価が向上した → 協業依頼の増加、セミナー等の増加
③ システム開発上、セキュリティを加味した設計をするようになった→データベースアクセス制御
④ 社員のネチケット、セキュリティ意識が向上した

6.今後の課題

1) 社内 ： ① さらに個人情報を維持管理するための設備投資
② システムに最新セキュリティ機能を加えるための技術力
③ 社員のモラル維持
2) 顧客 ： ① 顧客が得られるプロフィットの明確化

プライバシーマーク取得過程



自己紹介

佐藤 憲一

昭和57年 (株)大塚商会入社。現在、マーケティング本部テクニカルソリューションセンター 部長代理。
平成12年 (株)オーエスケイ取締役兼務。
平成9年 セキュリティビジネス推進部 責任者となり、企業の立場に立った情報セキュリティに関する幅広いソリューション＆サービス体系を企画、構築、提供している。情報セキュリティポリシー 個人情報保護、セキュリティ教育に関して研究している。
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) 日本パーソナルコンピュータソフトウエア協会 情報セキュリティ研究会 主査
(社) 情報サービス産業協会 セキュリティ評価基準部会 委員

連絡先 ： Kenichi.Satoh@otsuka-shokai.co.jp

(株)大塚商会

本社所在地	〒101-8373 東京都 千代田区 三崎町2-12-1
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
上 場	2000年7月14日に東証一部上場 業種：サービス業 コード：4768
資 本 金	103億7485万円
企業理念	「顧客満足の追求」
社員数	6272人 （営業系40%、SE系24%、CE系21%、事務系15%）
拠点数	国内220拠点