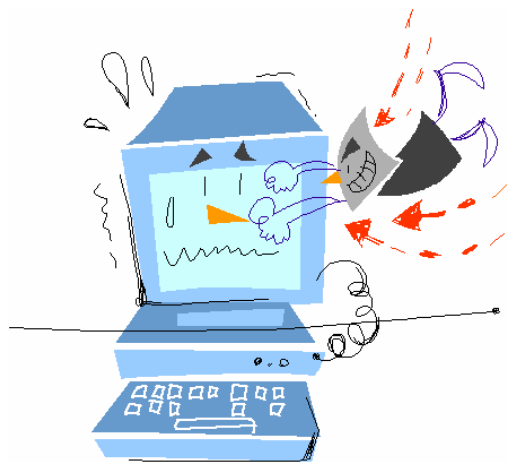


「個人情報保護法 4 月 1 日施行！」

～早急に着手すべき中小企業のリスク管理～



2005.3.8 中小企業家同友会 例会

ファーストコンサルティング 代表
ITコーディネータ 乗山 徹

目 次

- 最近の個人情報漏洩事故
- 事例で見る個人情報の漏洩
- 企業における情報漏洩の犯人は？
- なぜ、事件・事故が起きるのか？
- 2005年個人情報保護法施行のインパクト
- 個人情報保護法で何が変わるのか
- 個人情報保護法への対応策
- プライバシーマークとは
- 参考情報

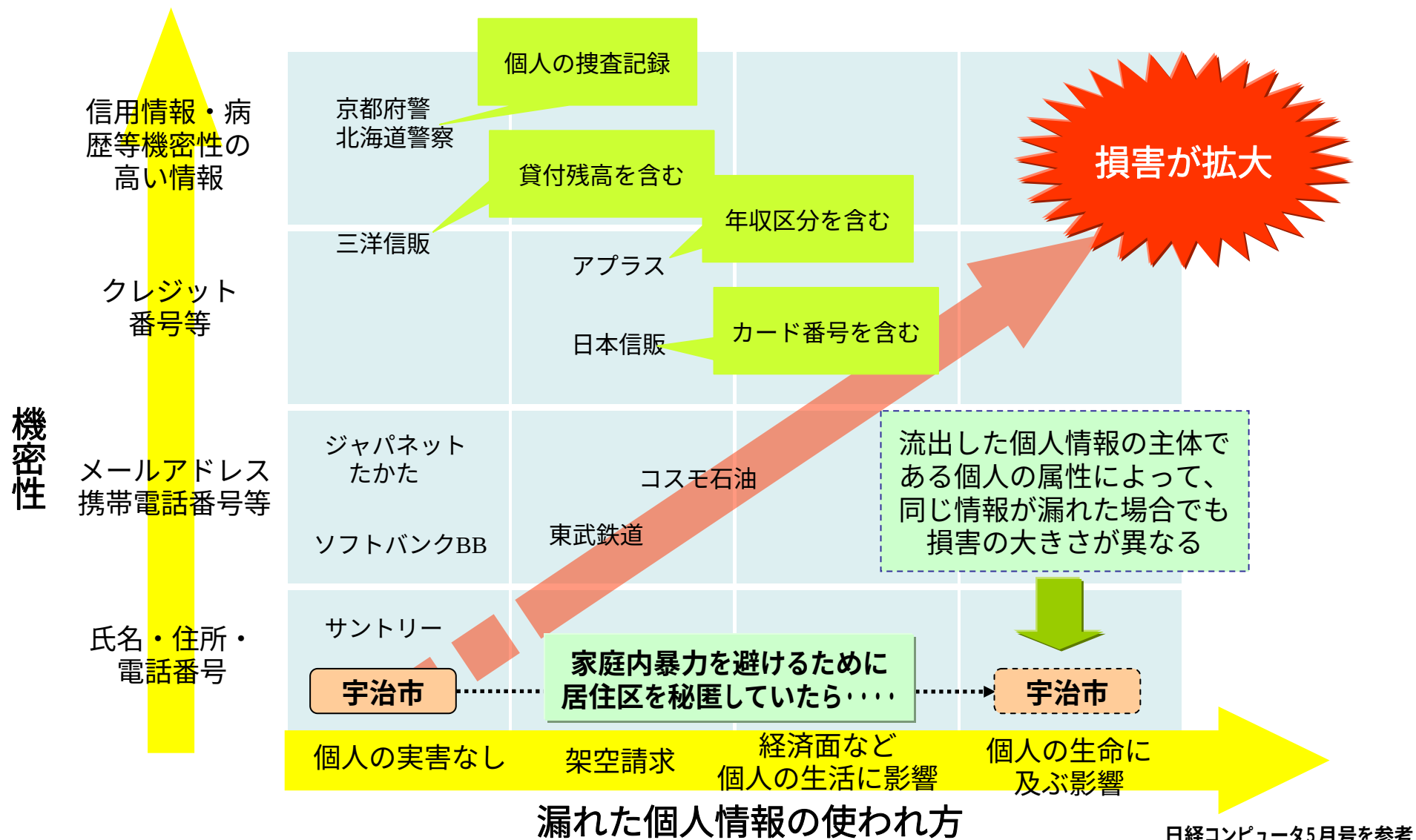
主な情報漏洩事件の概要

企業名	発生時期	件数	内容	流出経路
TBC 東京 ビューティ センター	2003年5月	3万7000件	氏名、住所、電話番号、メールアドレス、職業、スリーサイズ、エステに関する相談ほか	Web上で実施したアンケートなどを集計したCSVファイルを、Web上で閲覧可能な状態で置いていた
ローソン	2003年8月	56万件	氏名、住所、性別、生年月日、電話番号ほか	社外開発委託先のコンピュータから抜き取られた可能性が高い
アプラス	2003年8月	7万9000件	氏名、住所、電話番号、性別、職業、年収ほか	社外開発委託先から流出
ファミリー マート	2003年11月	18万件	氏名、住所、メールアドレスほか	社外メール配信事業委託先から流出
ソフト バンクBB	2004年1月	451万件	氏名、住所、電話番号、メールアドレスほか	内部関係者による持ち出し

道内での個人情報漏洩事件・事故

企業名	発生時期	件数	内 容
リコー	2003年7月	1799件	リコーが紛失したのは、同社がシステム構築を請け負っている帯広市の「除籍・改製原戸籍検索発行システム」が扱うデータの一部。事故はトラブル原因の解明のためにデータを格納した磁気テープをリコーの拠点（横浜市）とやり取りする過程で起こった。磁気テープを宅配便を使ってやり取りしたところ、宅配便業者（ヤマト運輸）が紛失した。 羽田空港内のヤマト運輸の仕分け場で廃棄物にまぎれて粉碎焼却処理された可能性が高いと見られている。
北海道警察 江別警察署	2004年5月	8件	流出した捜査関連書類は、巡査の作成した現行犯人逮捕手続書、捜査報告書、参考報告書、交通事故発生報告書、実況見分調書の5種類6件。氏名や住所など8人分の個人情報が記録されていたとし、巡査宅のインターネット回線からP2Pソフトを経由して流出したものとみられている。 江別市内の男性会社員が6月1日、「個人情報が世界中の不特定多数に閲覧されて精神的苦痛を受けた」として、道に損害賠償200万円の支払いを求める訴訟を札幌地裁に起こした。
丸井今井 釧路店	2004年8月	21件	クレジットカードを使って買い物をした21人の個人情報が流出し、インターネットの通信販売で不正に利用された。29件の不正利用のうち16件約145万円が契約に至り、大部分の商品が都内などに発送されたが、いずれも代金請求前に発覚しており、カードの所有者に経済的被害は発生していない。 同社によると、問題となったカードは釧路店で5月から7月にかけて利用された。カード利用の際、個人情報は保管用伝票に印字し、営業時間終了後に一括して金庫にしまっている。同社では社内から漏れた可能性が高いと見ている。

情報1件当たりの損害は漏れた情報の内容とその使われ方によって変わる



直接被害額の内訳

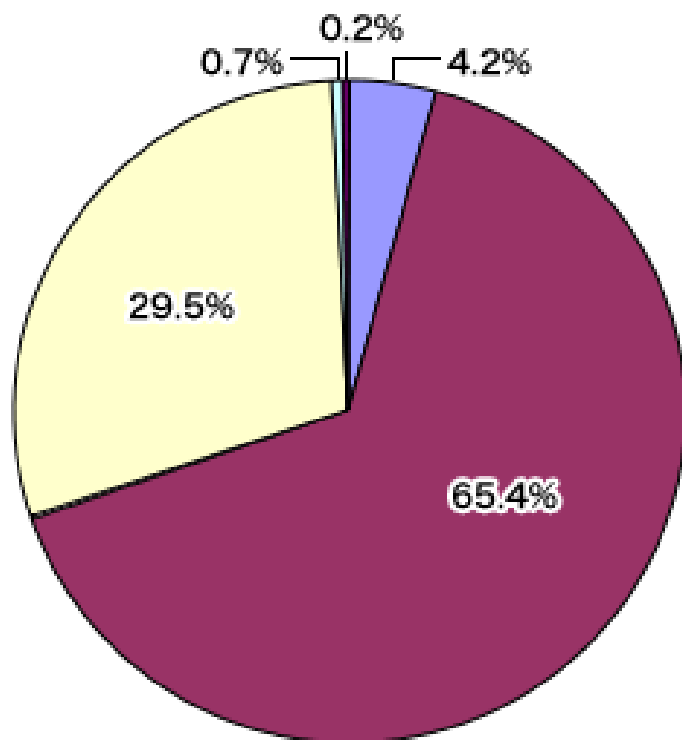
企業名	売上高 (億円)	直接補償額 (億円)	売り上げ比率	備考
TBC 東京 ビューティ センター	411	0.1	0.03%	10人が損害賠償訴訟を起こす (1人当たり115万円)
ローソン	2,500	2.8	0.11%	全員に金券500円
アプラス	1,063	0.8	0.07%	全員に金券1000円
ファミリー マート	9,544	1.8	0.02%	全員にQUOカード1000円
ソフト バンクBB	4,069	23	0.56%	全員に金券500円

間接被害額の内訳

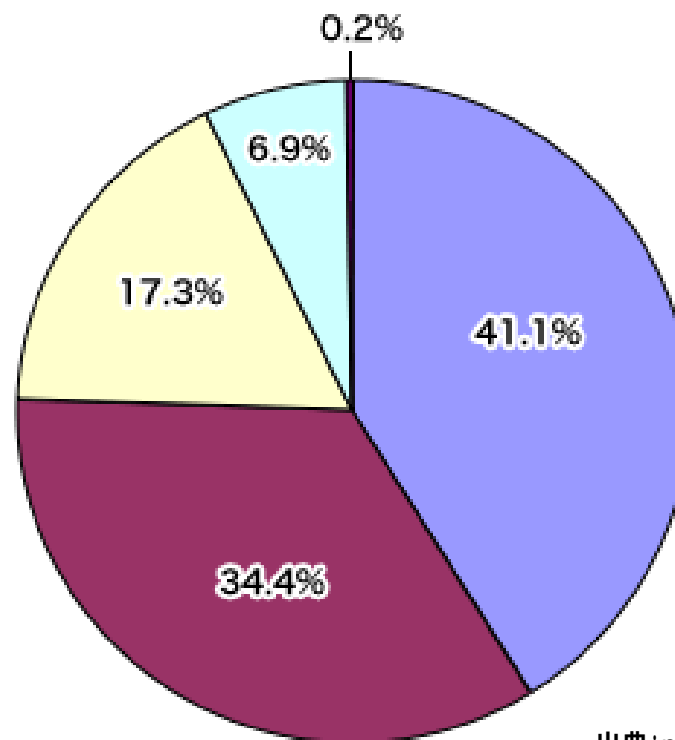
企業名	売上高 (億円)	間接補償額 (億円)	売り上げ比率	備考
TBC 東京 ビューティ センター	411	425.5	103.5%	115万円を全員に適用と仮定
ローソン	2,500	56	2.2%	損害賠償額1万円と仮定して全 員に適用した場合
アプラス	1,063	7.9	0.7%	損害賠償額1万円と仮定して全 員に適用した場合
ファミリー マート	9,544	18.3	0.2%	損害賠償額1万円と仮定して全 員に適用した場合
ソフト バンクBB	4,069	40	1.0%	新聞報道による

個人情報流出時に望まれるのは「金券」より「情報開示」

●大規模な個人情報の流出の起きた企業が、顧客へのお詫びとして500円～1000円程度の金券を配布する、という対応について、どう思われますか。(ひとつだけ)



●ローソンやファミリーマートとは異なり、ジャパネットたかたが取った、営業活動の自粛という対応について、どう思われますか。(ひとつだけ)



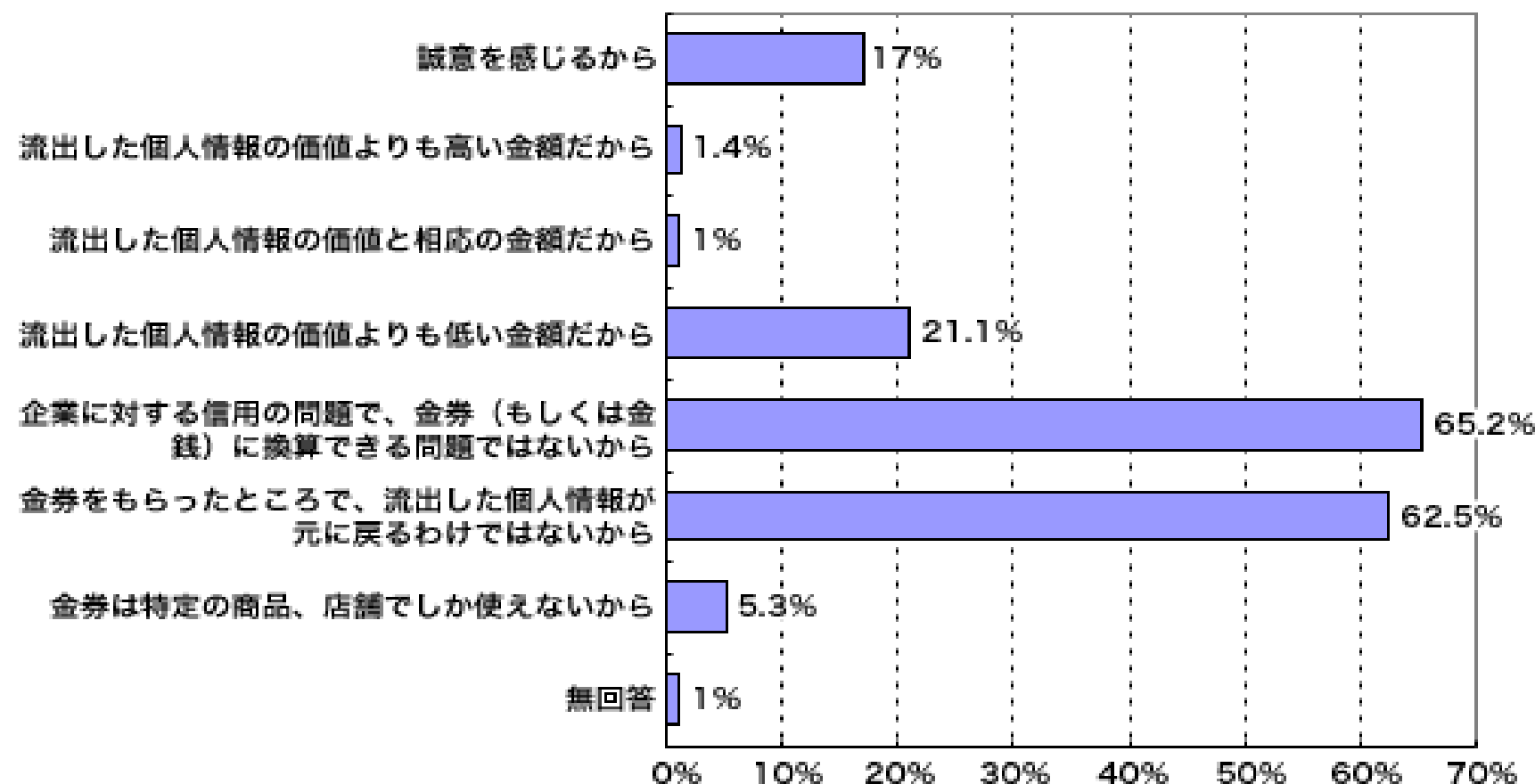
N=4773

出典: nikkeibp.jp アンケートから

■ 評価できる ■ 評価はできないが、何もしないよりはまし ■ 評価できない ■ 分からない ■ 無回答

金額の多寡より信用問題と考える

Q3. Q1 で回答した理由をお答えください。(いくつでも)

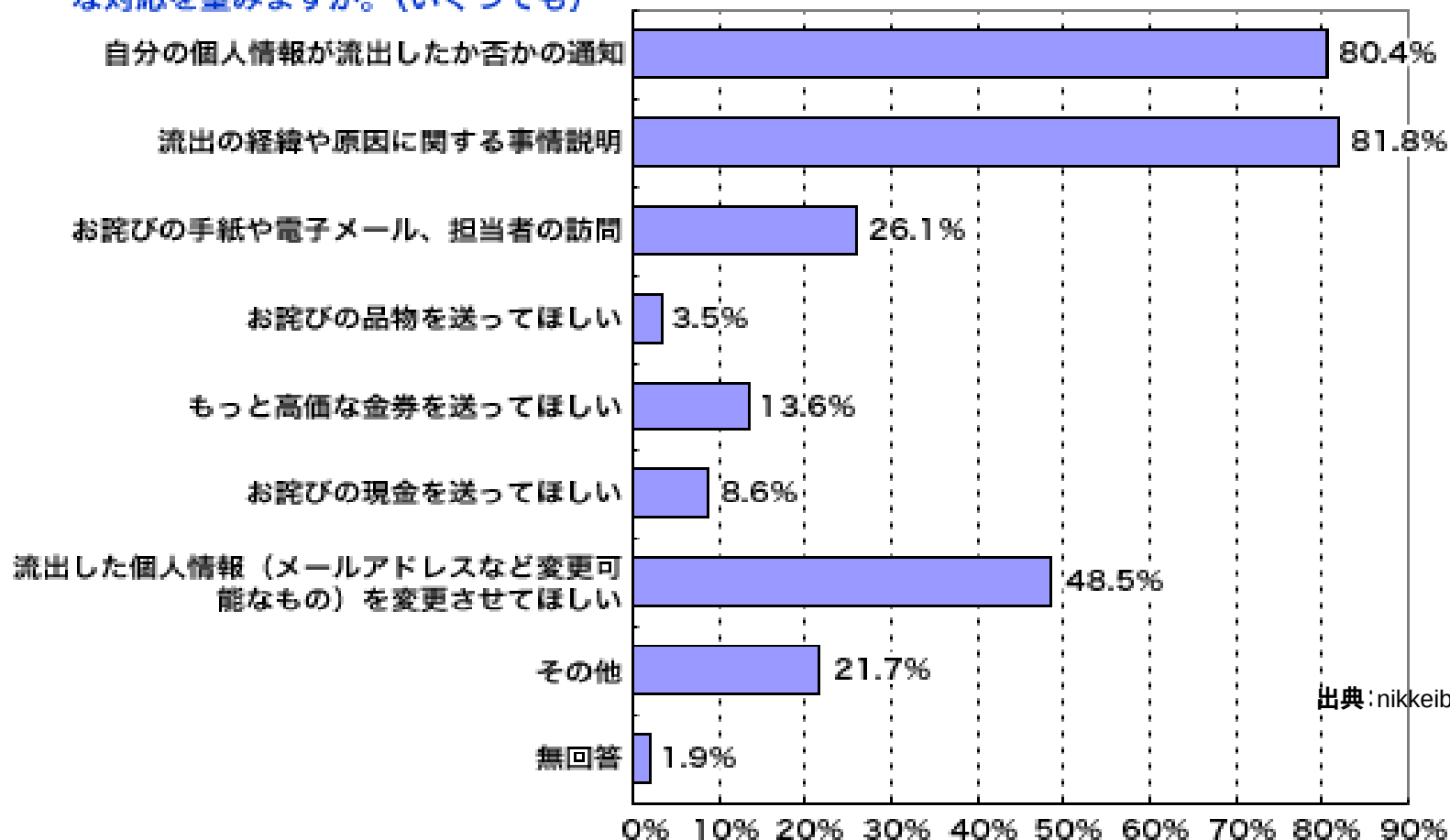


N=4773

出典: nikkeibp.jp アンケートから

流出の有無が知りたい、事情説明をしてほしい

Q4. 個人情報を流出させた企業に対して、「500 円～ 1000 円程度の金券を配布する」以外にどのような対応を望みますか。(いくつでも)



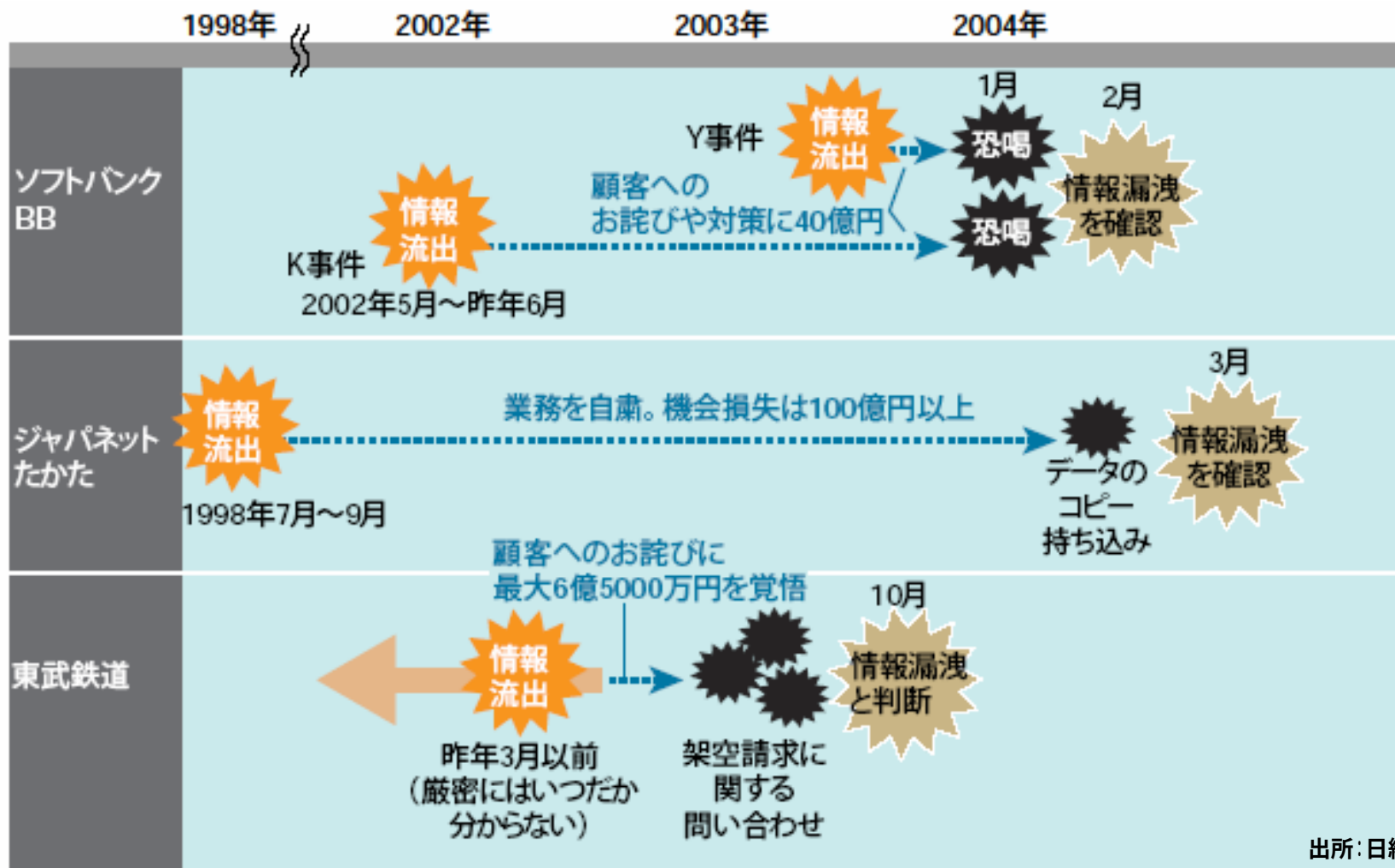
出典: nikkeibp.jp アンケートから

N=4530

(「金券を配布という対応についてどう思うか」の問いに、「何もしないよりまし」「評価できない」を選択した回答者)

情報が漏れた時期と、発覚時期にはタイムラグがある

多くの事件では、かなり前の情報漏洩が、顧客からの問合せなどをきっかけに最近発覚した。この間、どの企業も情報が漏れたことに気づかないまま事業を継続していた。



事例で見る個人情報の漏洩

① 『宇治市21万人の住民基本台帳のデータが流出』

人口約19万人の京都府宇治市で、住民基本台帳のデータが流出し、インターネットで販売されていた。事件は1999年5月22日に発覚した。インターネットで「U市住民票」として売られていた。1998年3月末の住民基本台帳に掲載されていた氏名、住所、生年月日、世帯主名などで、計21万7617件。この件数は市の人口を大幅に超えるが、1998年4月1日時点の『住民記録』（185,800件）『外国人登録』（3,297件）『住民記録外課税者・法人』（28,520件）を足した件数と一致する。

本セキュリティ事故のポイント

●全市民への影響

●損害賠償の裁判判決は、一人当たり1万円

→ 21万人では、21億円になる

■流出経緯

システムの開発に携わった会社のアルバイト大学院生(当時)が、仕事の遅れから、住民票データをサーバーから勤務先のシステム開発会社のMO(光磁気ディスク)にコピーし、システム開発会社に持ち帰り作業をした。そのデータを更に自分のMOにコピーし、それを5月9日頃 リストコンサルタント会社A社という名簿業者に25万8000円で売った。

5月22日に発覚、5月27日には名簿業者からデータを回収、6月3日には販売先の3社すべてからデータを回収した。

■流出した住民データの項目

()内は値のサンプル

ファイルコード(Z)、都市コード(AD)、住民番号(0049180)、CD(2)、世帯番号(0015706)、市内外サイン(空白)、住所コード(A2404)、郵便番号(611)、市内住所(宇治大谷)、番地(6番地の11)、方書(空白)、世帯主名(久保田 勇)、カナ氏名(クボタ イサム)、漢字氏名(久保田 勇)、生年月日(3230512)、性別(1)、続柄1(02)、続柄2(空白)、続柄3(空白)、漢字続柄(世帯主)、住民になった日(3290115)、住民でなくなった日(空白)、住民でなくなった事由(空白)、外国人通称名(空白)、外国人通称名カナ(空白)、国籍コード(空白)、電話番号(空白)、転出住所区分(空白)、転出住所コード(空白)、転出郵便番号(空白)、転出住所(空白)

■持ち出したアルバイトの罪

アルバイトの大学院生が自分で所有していたMOにコピーしたので窃盗罪には当たらない。市の条例に触れるので、条例違反で提訴、書類送検。しかし地方検察庁は、書類送検されていた元大学院生とシステム開発会社を不起訴とした。不起訴の理由は「刑の廃止」で、犯行から書類送検までのあいだに個人情報保護条例が制定され、旧条例が廃止されたにもかかわらず、罰則に関する経過措置の規定が設けられなかったことによる。

元大学院生(3月に卒業)からは、6月24日謝罪文が市に提出された。

■住民からの宇治市に対する損害賠償請求に判決

3人の市民からの損害賠償請求の裁判において、1人1万円の賠償金+裁判費用5000円を支払えという判決が出た。

氏名、住所、生年月日、性別の情報で1万円だった。もっと重要な情報が含まれていたら、より高くなるのではないかと、専門家は見ている。

事例で見る個人情報の漏洩

② 『コンビニ(ローソン)のカード会員 56万人の顧客情報流出』

「ローソン会員カード」の約56万人分の顧客情報が社外に流出した、と発表した。流出したのは会員の「氏名・住所・性別・生年月日・電話番号」などの個人情報。流出したのは2002年8月17日時点の会員分という。同社は同カードの会員約115万人全員に商品券500円分とお詫び状を送った。

本セキュリティ事故のポイント

●多くの顧客(会員115万人)への影響

●お詫びだけで約6億円

■ローソンの対応経緯

- ① 2003年6月9日 会員からの問い合わせ
- ② 6月10日 社内調査開始
- ③ 6月18日 別の会員からの問い合わせ
- ④ 6月19日 顧客情報の流出を確認
- ⑤ 6月23日 調査委員会発足・警察当局への相談
- ⑥ 6月24日 個人情報保護委員会発足
- ⑦ 6月26日 「顧客情報の流出」を発表
- ⑧ 7月9日～12日 カード会員へのお詫び状発送
- ⑨ 7月15日 顧客情報セキュリティ対策(対策A)を発表
- ⑩ 8月6日 調査結果、追加対策(対策B)、社内処分を発表

■ローソン調査委員会の調査結果

- (a) 流出データは信用情報を含まない個人ベース情報のみ
- (b) 社外委託先であるシステム開発運用会社の管理下にある開発用コンピュータから、故意に抜き取られた可能性が高い
- (c) L社および関連会社Lカード社の社員はこのコンピュータのパスワードを持っていない
- (d) このコンピュータにアクセス可能な人物はある程度絞られる
- (e) 情報抜き取り者の特定は捜査機関と相談中

■個人情報保護委員会(委員長：ローソンの社長)で決定した対策

<対策A：会員カード顧客情報セキュリティ対策>

- (A1) 顧客情報操作端末専用ルームに24時間稼働の監視カメラ設置
- (A2) 指紋認証による専用ルームへの入退室管理の強化
- (A3) アクセス端末に指紋認証機器の導入
- (A4) アクセス可能人員の削減
- (A5) 顧客情報運用委託先がL社と同程度のセキュリティ対策を実施

<対策B：店頭を含むあらゆる個人情報への対策>

- (B1) 店舗レベルでの個人情報の取扱い及び廃棄処理の厳格化
- (B2) 懲罰的措置を含む社内規程の制定とその厳格な運用
- (B3) 個人情報保護に関する従業員教育の再徹底
- (B4) 個人情報に関する内部監査の実施
- (B5) 委託先選定基準作成、委託契約内容見直し、定期検査実施

事例で見る個人情報の漏洩

③ 『エステサロンTBCの 3万7000人の個人データ流出』

2002年05月26日、エステサロンTBCの社員が掲示板サイトで「エステサロンTの顧客情報大量流出」を発見。流出元のK社ホームページを停止した。流出したのは、2000年4月から5月にかけて、同社のサイトにアクセスし、資料請求やアンケートに回答した男女3万7810件のデータ。エステ利用顧客のデータは流出していない。K社では、サイトにお詫びを掲載するとともに、専用ホットラインを設けて対応。

本セキュリティ事故のポイント

- ホームページに回答した個人データの保護漏れという、技術的な作業ミス
- 被害弁護団が結成され、集団訴訟原告10名が2002年12月に提訴、更に新たな原告が追加提訴。裁判中。

流失したデータはエステサロンTBCのホームページにアクセスし、資料請求やアンケートに回答したデータ。流出した個人データは、アンケートの内容にもよるが、氏名、住所、年齢などのほか電話番号やメールアドレスも含まれている。

このページについてのご意見・ご感想をお聞かせ下さい。

氏名		
氏名フリガナ		全角で入力してください
性別	☐ 男 ☐ 女	
年齢		
ご職業		
郵便番号		
ご住所		
電話番号		
E-Mail		必ず半角英数字をお願いします
このページについてのご意見・ご感想		
今後、TBCのご案内メール等をお送りしてもよろしいでしょうか？	☐ はい ☐ いいえ	
		送信 キャンセル

これらの回答データは、ホームページの同ディレクトリに保存されており、同ディレクトリのアクセスにはパスワードなどを設定していなかった。

事例で見る個人情報の漏洩

④『大手人材派遣テンプスタッフ社の 9万人の女性登録スタッフの データがインターネット上で売買』

1998年1月、同社の女性登録スタッフ9万人分の個人データが、委託先のシステム開発会社員によって持ち出され、インターネット上の会員制ホームページで容姿ランク付きと宣伝されて 売買された。

流出したデータは女性の氏名、住所、電話番号、生年月日に加えて、プライバシー情報もあったとされている。

本セキュリティ事故のポイント

●外注先の従業員によるデータ持ち出し

●企業の存続の危機

個人情報データの中にプライバシー情報があったとされ問題、派遣者離れの危機

■経緯

2年以上常駐していた外注業者の28歳の男性システムエンジニアは、9万人分の名簿を自分のノートパソコンに記録して持ち出した。それを会員制ホームページ業者に持ち込んだ。業者は、名簿を、下品なホームページで、挑戦的なタイトルのもとで、「容姿ランク付き9万人の個人データ」として5万5000円で売りに出し、数十人が買い取った。名簿が流れた女性の家には無言電話や、不審人物が家の近くをうろついている、という数十件の訴えが相談センターに届けられた。登録スタッフ6名が東京地裁にテンプスタッフ社を訴えて、裁判を起された。

■対策

大事件となり、対外的な信用は失われ、経営の根幹を揺るがしかねない状況に立たされた。

テンプスタッフ社はこの事件を契機に、全社的なセキュリティ対策の構築に乗り出した。監査室を設け、外部の監査法人を利用してシステム監査を実施。そして、セキュリティポリシーを策定し、プライバシーガイドラインを策定。

セキュリティ管理策として、

- 個人認証の強化(ユーザID、パスワード)
- データベースアクセス制限(時間、権限)
- 持ち出し手段の制限(PC、媒体持込禁止)
- アクセスログの管理や監視
- 外部委託会社選定基準(会社評価、再委託制限、派遣者面談)
- ネットワーク出口の規制(メール監視、添付ファイル制限)
- 指紋認証システム導入

などを実施した。

企業における情報漏洩の犯人は？

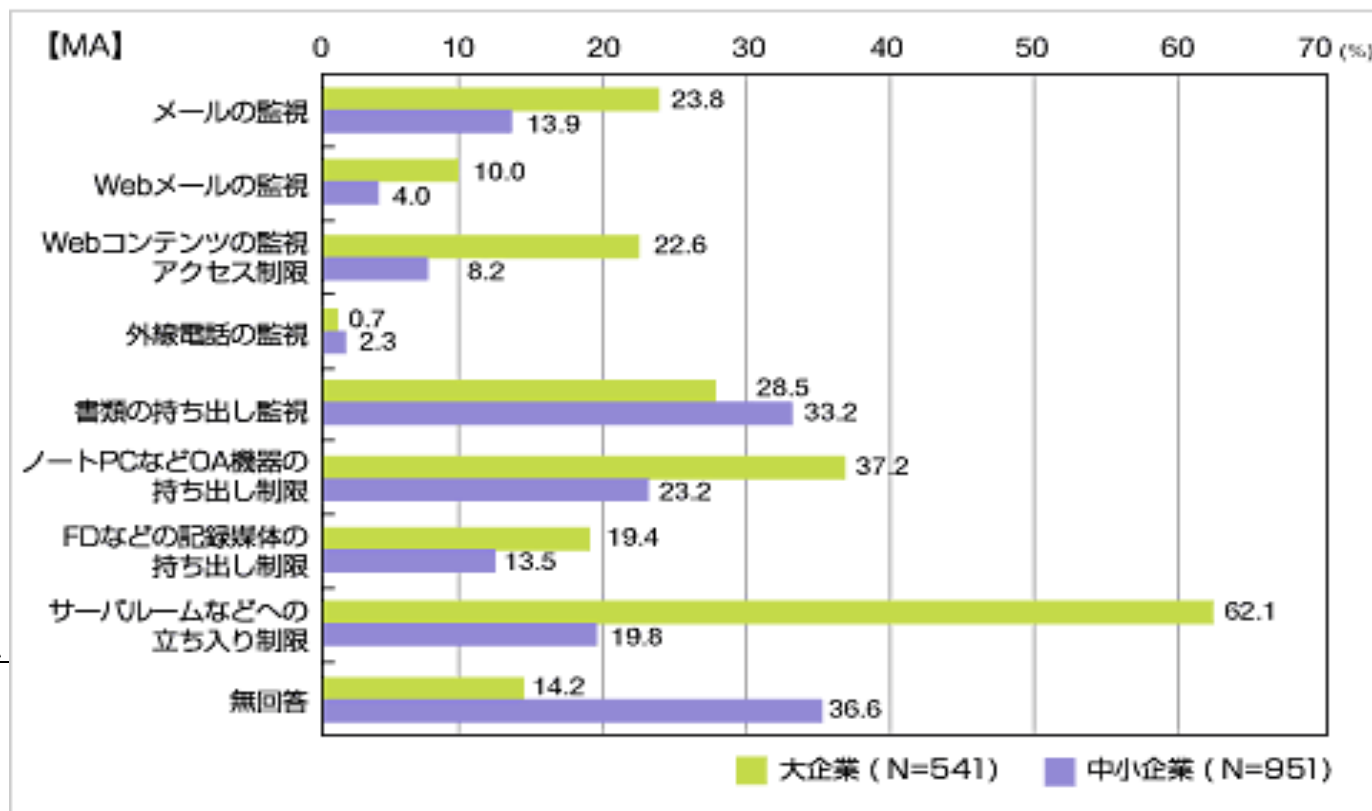
「情報漏洩は社外の悪意ある人間が起こす」という、漠然とした印象があるかもしれない。しかし実際は、社内の人間によって起こるケースが最も多いと考えられている。米国SAIC社の調査では、**実に8割が社内からの漏洩だった**という。

一方、内部からの情報漏洩に対する「守り」は行われているのだろうか。総務省の「情報セキュリティ対策の状況調査」によると、書類やOA機器、記録媒体の持ち出しについては制限を設けていない企業が多いことが伺える。

漏洩被害の背景には、情報の持ち出しに対する社員の無自覚がある。

セキュリティポリシーの策定など、内部からの漏洩を防ぐなんらかの対策が必要である。

■ 内部者による情報漏えい防止対策の実施状況



総務省「情報セキュリティ対策の状況調査」

なぜ、事件・事故が起きるのか？

■個人情報漏洩のリスク

- プライバシー意識の低さ
- 現場中心のボトムアップなマネジメント
- 前提となっている性善説
- 甘いリスク意識
- 個人情報保護やセキュリティに対する教育指導の欠如
- 個人情報保護やセキュリティに対するルールの未確立
- 経営者のリスク認識、危機意識の欠如
- 名簿業者へ持ち込めば大金になるという金銭的な誘惑
- 職場への不満からの嫌がらせ行為、外部からの誘惑

企業活動に欠かせない個人情報



価値ある詳細な個人情報



ルーズな個人情報管理



個人情報漏洩
のリスク



個人情報の保護の重要性

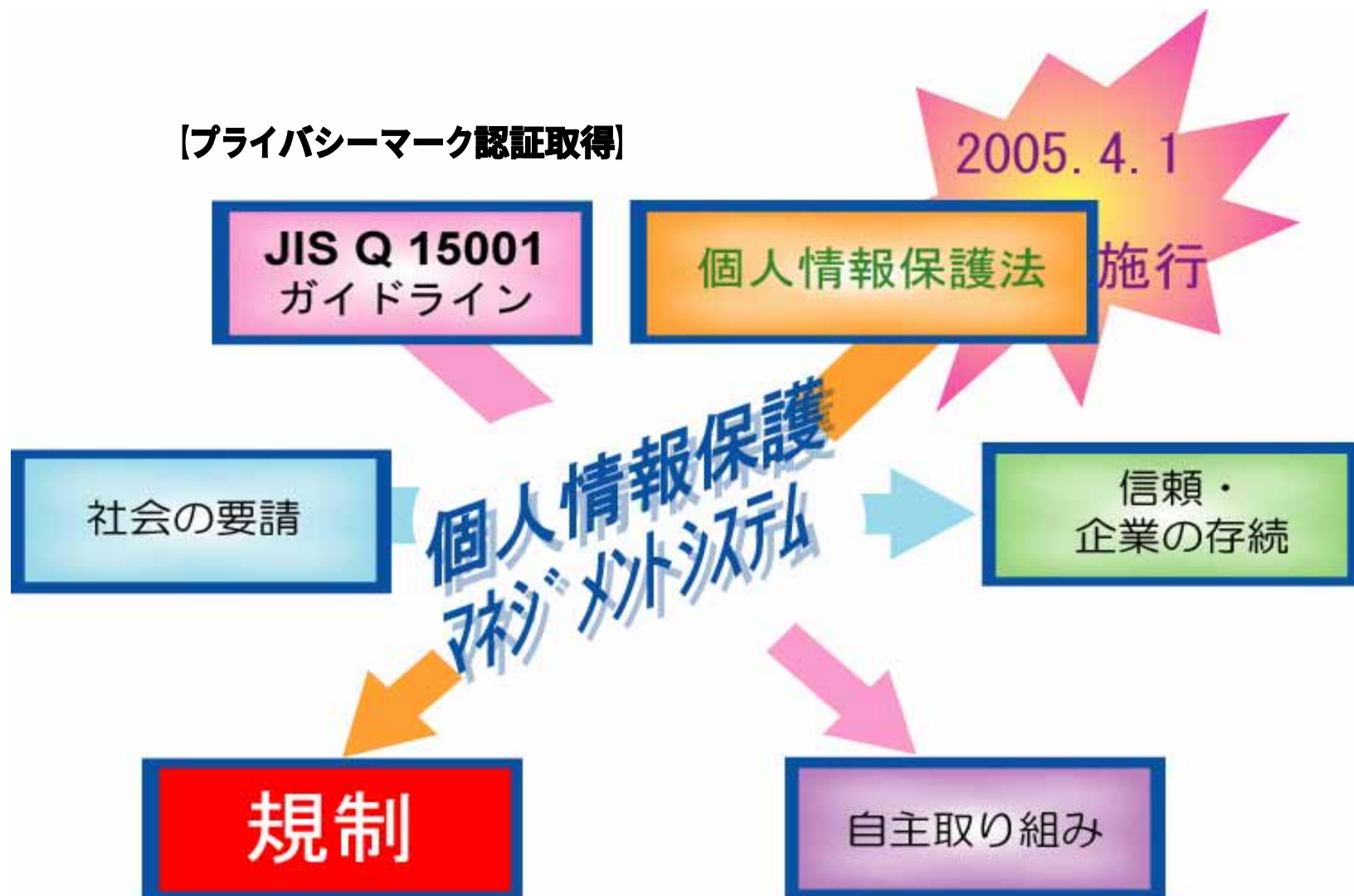
～個人情報漏洩した場合の影響の大きさ～

経営危機を招きかねない --- 個人情報漏洩リスクの重大な影響

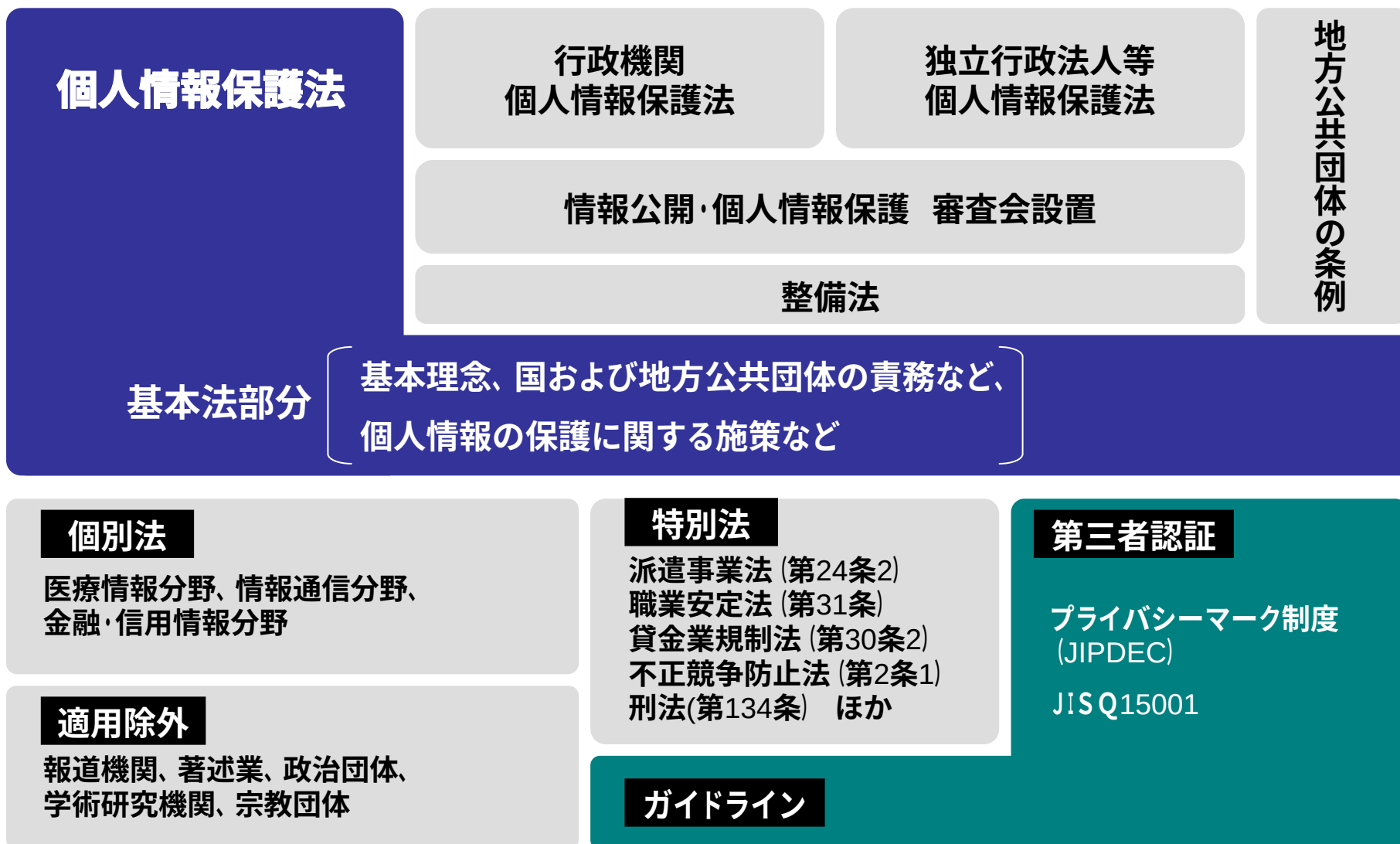
- ★流出の情報量は大量化
- ★多くの顧客への迷惑
- ★流出した情報の回収が困難
- ★顧客への被害防止が難しい
- ★損害賠償費用が膨大化
- ★顧客の信頼の喪失
- ★社会的な信頼が低下
- ★対策の工数・費用の負担
- ★受注の低下、損益の悪化
- ★経営危機
- ★企業存続の危機



個人情報を扱う会社は、委託先を含め個人情報保護への対応が迫られている
～個人情報保護の枠組み～

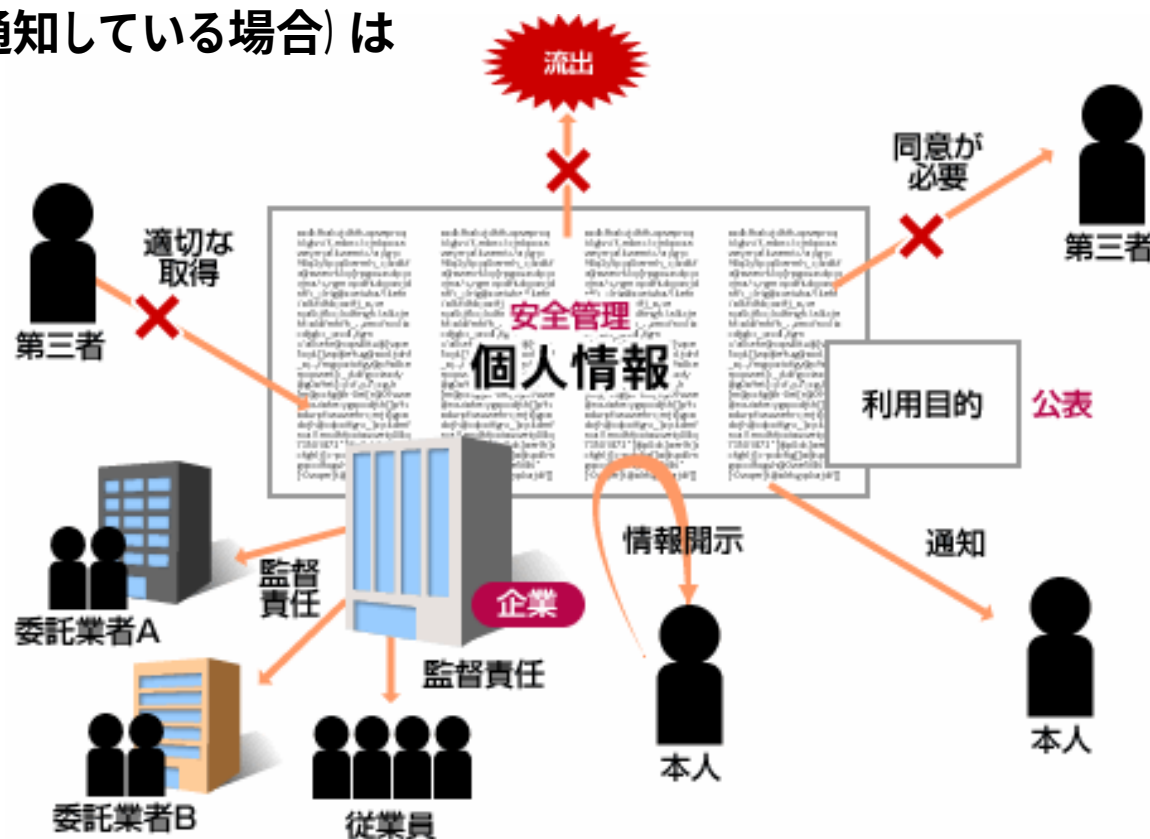


個人情報保護に関する法令と主な規範



個人情報保護法の骨子

- 個人情報の利用目的を**特定**。利用目的を超えた個人情報の取り扱いの原則禁止
- 個人情報の**安全管理**のために必要かつ適切な措置、従業者・委託先に対する**監督**
- 本人の**同意**を得ない個人情報の**第三者提供**の原則禁止、委託、合併等の場合、特定の者との共同利用の場合（共同利用することを通知している場合）は第三者提供とならない
- 本人の求めに応じ、保有する個人情報の開示、訂正、利用停止の義務
- 個人情報の取り扱いに関する苦情の適切かつ迅速な処理・規定に違反すると**6カ月以下の懲役または30万円以下の罰金**など



個人情報保護法 = 個人情報漏洩に対する罰則を与える法律？

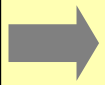
プライバシー侵害の前段階での
予防措置

個人情報保護法

勧告



命令



罰則

※ただし、ミニмумスタンダード
事業者ごとの上乗せを検討すべき

個人情報保護への
取り組み →→→ 顧客満足度の向上へ

プライバシー侵害が実際に
生じた後の権利利益の救済

民法

不法行為責任
債務不履行

刑法

名誉毀損

労働関連法

不正アクセス禁止法

電子署名認証法

憲法13条：生命・自由・幸福追求権

個人情報保護法で何が変わるのか

2005年4月から個人情報の捉え方と対処方法は大きく変化する

	施行前	施行後
企業が集めた顧客情報	「企業の財産」「営業秘密」として保護されている。	「個人情報」という認識がプラスされる。 企業の財産として自由に取扱うことはできない。
個人情報の開示	個人情報の開示請求権は一般的には認められない。	開示の義務がある。
公開情報の利用	本人に対して何もしなくてよい。	利用目的を本人に通知し、または公開しなければならない。
情報漏洩	民事の損害賠償請求	民事での損害賠償請求プラス行政処分

個人情報を扱う会社は、委託先を含め個人情報保護への対応が迫られている ～個人情報の種類～

個人情報の区分

(1) 一般的な個人情報

個人の利益を害するおそれが少ない範囲で
収集される個人情報
(別の言い方をすると、センシティブな個人情報
や機微な個人情報が含まれないもの)

(2) センシティブな個人情報

- a) 個人信用情報(金融、資産)
- b) 趣味・嗜好、身体特性、交友関係
- c) 学歴・結婚歴、性格診断／心理テスト

(3) 特定の機微な個人情報(JIS Q 15001より)

- a) 思想、信条及び宗教に関する事項。
- b) 人種、民族、門地、本籍地(所在都道府県に関する情報を除く。)、身体・精神障害、犯罪歴、その他の社会的差別の原因となる事項。
- c) 勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項。
- d) 集団示威行為への参加、請願権の行使、及びその他の政治的権利の行使に関する事項。
- e) 保健医療及び性生活。

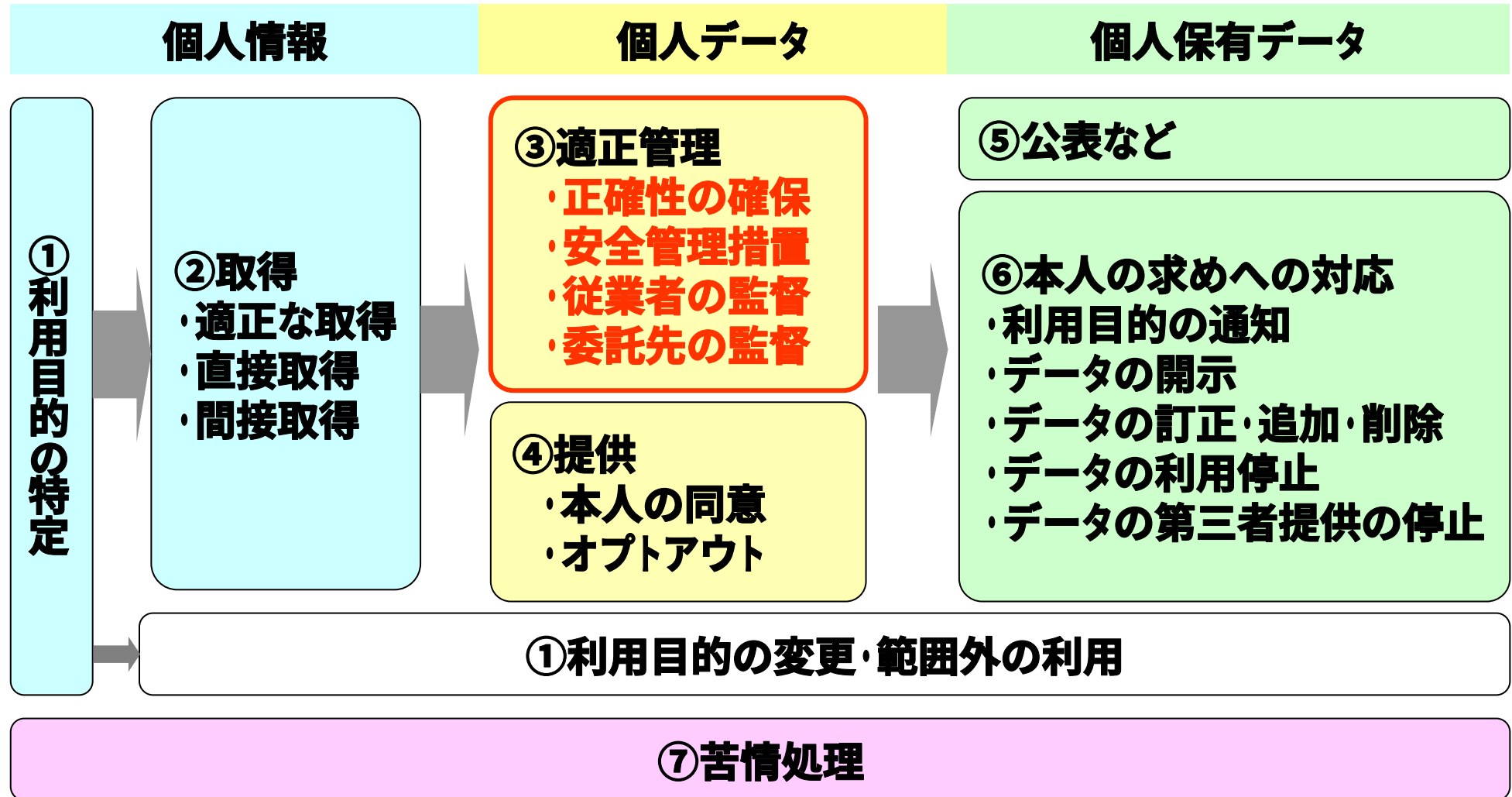
個人情報の例

一般的な個人情報：氏名、性別、住所、電話番号、
出生地(都道府県名)、生年月日、会社名、職業、地位、
社員番号、E-mail、ID番号 など

センシティブな個人情報：結婚、離婚、学歴、成績、
能力、クラブ活動、昇格・降格等、賞罰、容姿、体格、性
格、血液型、収入・資産状況、持家・借家の別、各種団
体加入状況、趣味、交友関係、各種名簿情報(卒業者
名簿、会員名簿等)、口座番号、クレジットカード番号、
保険証番号

特定の機微な個人情報：本籍、国籍、犯罪歴、心
身障害、傷病名、健康状態、思想、宗教、etc.

個人情報保護 = 情報漏洩を起こさないこと？



個人情報を扱う会社は、委託先を含め個人情報保護への対応が迫られている
～個人情報を収集・取扱いする事業者の責任～

□個人情報収集事業者の責任

- 個人情報の保護は**収集した企業に法的責任**がある
- 従業員だけでなく、**委託先の監督責任**もある
- **委託先選択基準、契約での安全確保の担保**
- **委託先の実質的な監督・指導**

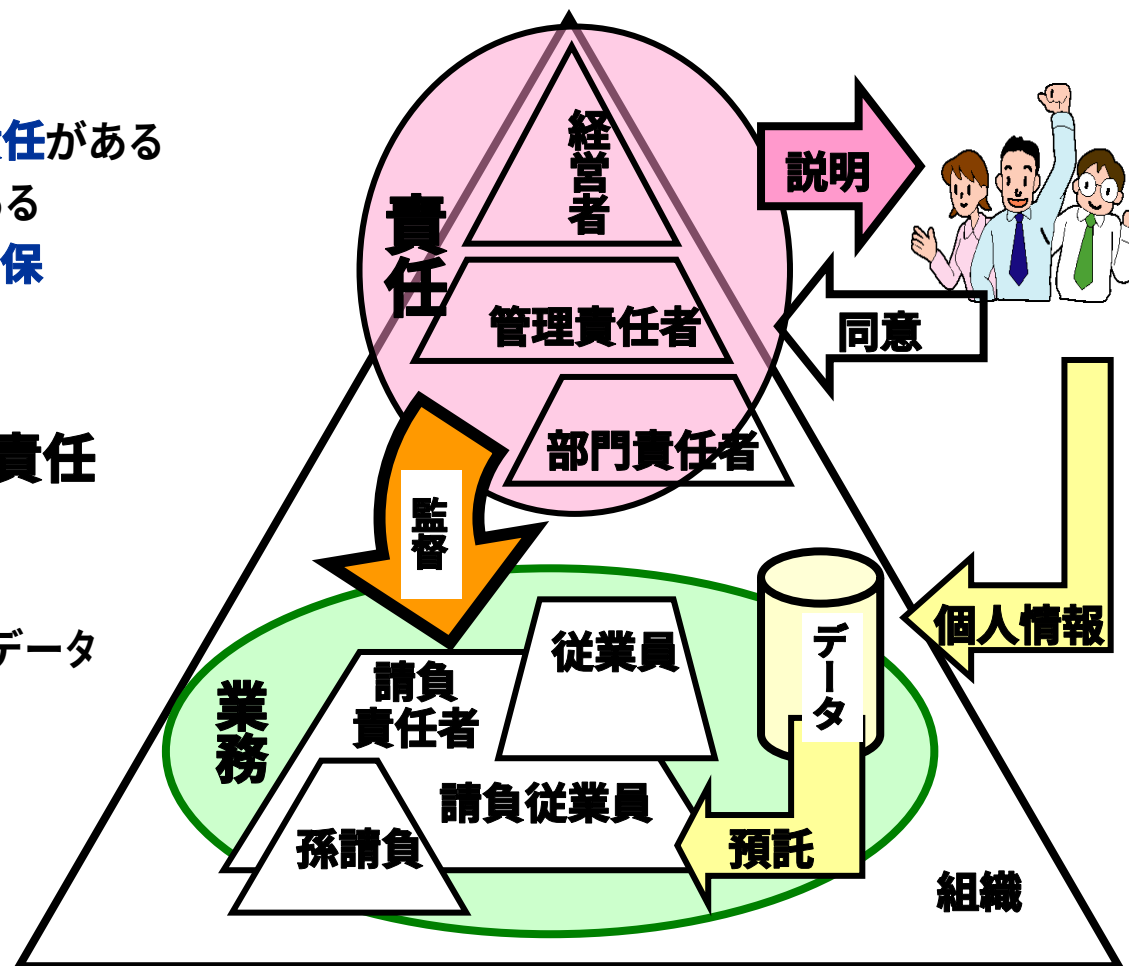
□個人情報の預託を受けた事業者の責任

- 預託元との間に**契約上の責任**がある
- **個人情報を安全保護する法的責任**がある
- 委託を受けた事業者は、個人情報などのデータ
預託と共に**委託元の企業存続の鍵をも
預かっている**
- 従業員に対する**監督責任**がある
- 認められている再委託をするときは、

再委託先を監督・指導

⇒個人情報を直接収集しているフロントエンドの事業者は…Pマークが必須

⇒バックエンドで情報処理業務等を遂行している事業者は…Pマーク、将来的にISMSが必須



委託先を含め個人情報保護への対応が迫られている ～業務委託先の監督も責任範囲になる～

監査権については委託契約に明記しておくほうがよい。
委託先の契約社員、あるいは委託先からの再委託なども考慮しておかなければならない。

宇治市の場合

操作は庁舎内のみできるように改善

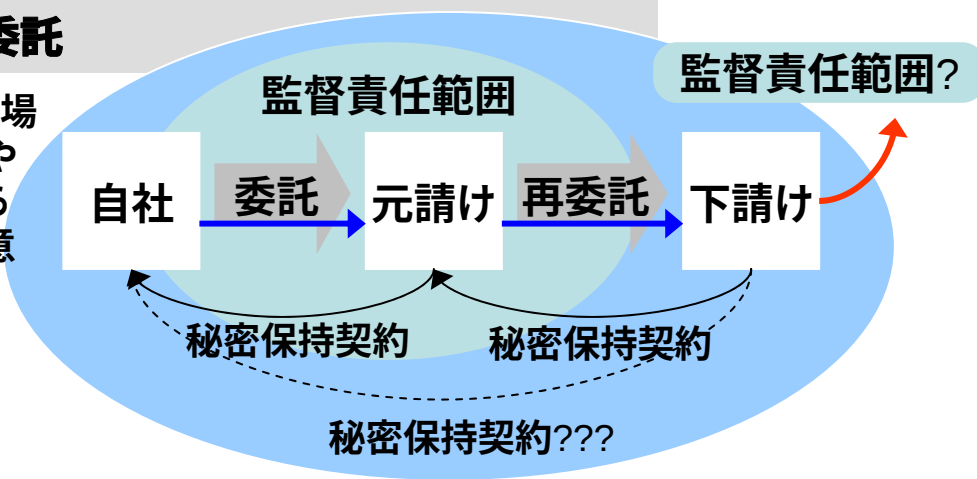


秘密保持契約

→ 個人情報の流れ
→ 情報流出の可能性が残る範囲

一般的な委託

データを渡す場合は委託先や再委託先からの漏洩に注意



個人情報漏洩

委託業者にも罰則規定

審議会答申

札幌市、条例改正へ

札幌市個人情報保護審議会（会長・道幸哲也北大大学院教授）はこのほど、市職員だけでなく、市の委託を受けた業者が業務関連で個人情報を漏らした場合でも、その業者に罰則を与える規定を設けるべきとする提言を提出した。市はこれを市に提出した。市はこの考えに沿って条例を改正し、来年4月に施行する考えだ。

答申は①開示された個人情報の利用・提供停止を本人が請求できる権利を保障②電算処理されて

などを盛り込んだ答申書を市に提出した。市はこの考えに沿って条例を改正し、来年4月に施行する考えだ。

答申は①開示された個人情報の利用・提供停止を本人が請求できる権利を保障②電算処理されて

広く検索できる公文書以外でも個人情報記載された文書の漏洩は罰則（罰金刑）対象③委託業務従事者と委託先の法人も罰則対象④などの内容。

罰則は①電算処理された公文書の場合は2年以下の懲役か100万円以下

下の罰金⑤それ以外の文書情報なら1年以下の懲役または50万円以下の罰金としている。提出後、道幸会長は「業務の外部委託はさらに増えると思われ、厳しい罰則規定を求めた」と述べた。

札幌市は、昨年5月の個人情報保護関連法の成立に加え、現行の市個人情報保護条例が施行後8年を経過したことから、昨年12月、同審議会に個

人情報保護制度のあり方を諮問していた。市は答申をもとに条例改正案作りを進め、9月定例市議会に提出をめざす。

2005年個人情報保護法施行のインパクト

貴社は個人情報保護法に
対応した仕組みがあります
か？



信用力の
低下

受注減

罰則

ビジネスモデルの
転換

個人情報保護法への対応策

人的対策

セキュリティ教育の実施、
契約書や誓約書の再取得

管理的対策

ルールを作る
(組織権限規定、業務規定、
運用管理規定、就業規則改定)

システムの対策

パスワード、暗号化、
ファイアーウォール、
アクセス制御等

物理的対策

建物、設備、PC等

**個人情報保護コンプライアンスプログラムを策定、実行、監査、見直し、
継続的改善を行う経営の仕組み**

今やるべきことは？

- ・守るべきもの(対象)は何か？ → 洗い出す、不要なものは捨てる
- ・何から守るのか？
 - －脅威は何？ → 脅威や脆弱性を認める
 - －どの程度リスクがある？ → 危険の度合いを認識する
- ・どの程度のコストをかけられるか？ → リスク見合いの優先順位付けが必要
- ・順守すべきことの確認 → 法律、条例、ガイドラインの確認・ウォッチ
- ・対応方針の確定、徹底 → 何かあったらどう対応するか知っておく

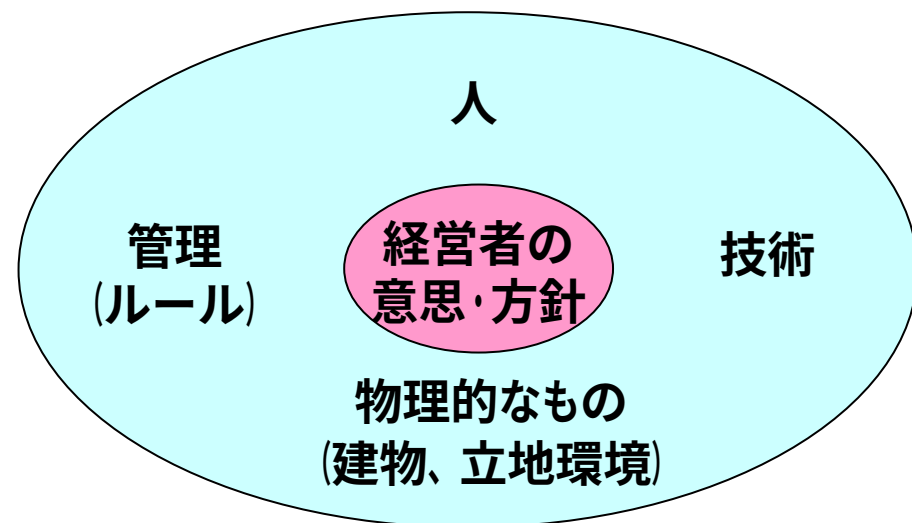
全体を体系的に考える

目的を考えて手段を選んでいく

→ 情報セキュリティマネジメントシステム

確立 → 継続的改善

プライバシーマークはその手段



プライバシーマークとは

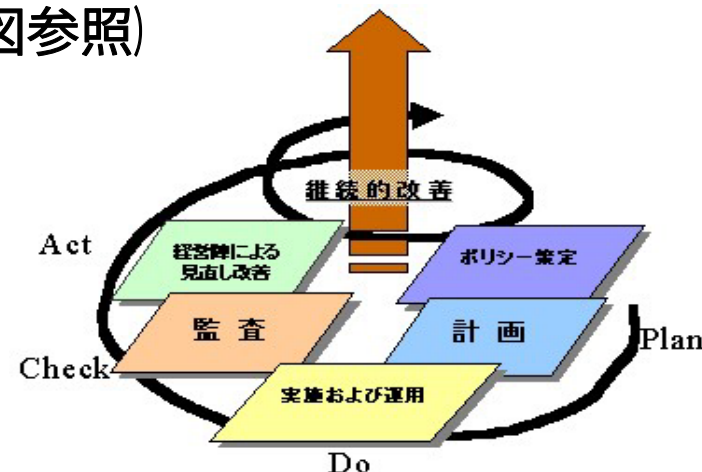


A123456(01)

出展：(財)日本情報処理開発協会 JIPDEC

- (財)日本情報処理開発協会 (JIPDEC) が推進する個人情報保護の認定制度
- JIS Q 15001および関連する法令・規制が要求するコンプライアンス・プログラム (遵守規定) を策定し、実行、監査、見直し改善を実施
- ISO9001, ISO14001と同様のスパイラルアプローチのマネジメントシステムの仕組み (右図参照)
- 個人情報保護についての信頼の証
- 個人情報保護法をクリアする唯一の公式な認証

<http://privacymark.jp/>



出展：(財)日本情報処理開発協会 JIPDEC

JIS Q 15001と個人情報保護法の差異

「個人情報」とは

・・・JIS Q 15001による定義

個人に関する情報であって、当該情報に含まれる氏名、生年月日その他記述、又は個人別に付された番号、記号その他の符号、画像若しくは音声により**当該個人を識別できるもの**（当該情報のみでは識別できないが、他の情報と容易に照合することができ、それによって当該個人を識別できるものを含む。）。

特定の機微な個人情報の収集の禁止

次に示す内容を含む個人情報の収集、利用又は提供を行ってはならない。

- a) 思想、宗教 b) 民族、本籍地、犯罪歴、
- c) 団体権、団体行動の行為 d) 請願権の行使、政治的権利の行使 e) 保健医療及び性生活。

「個人情報」とは

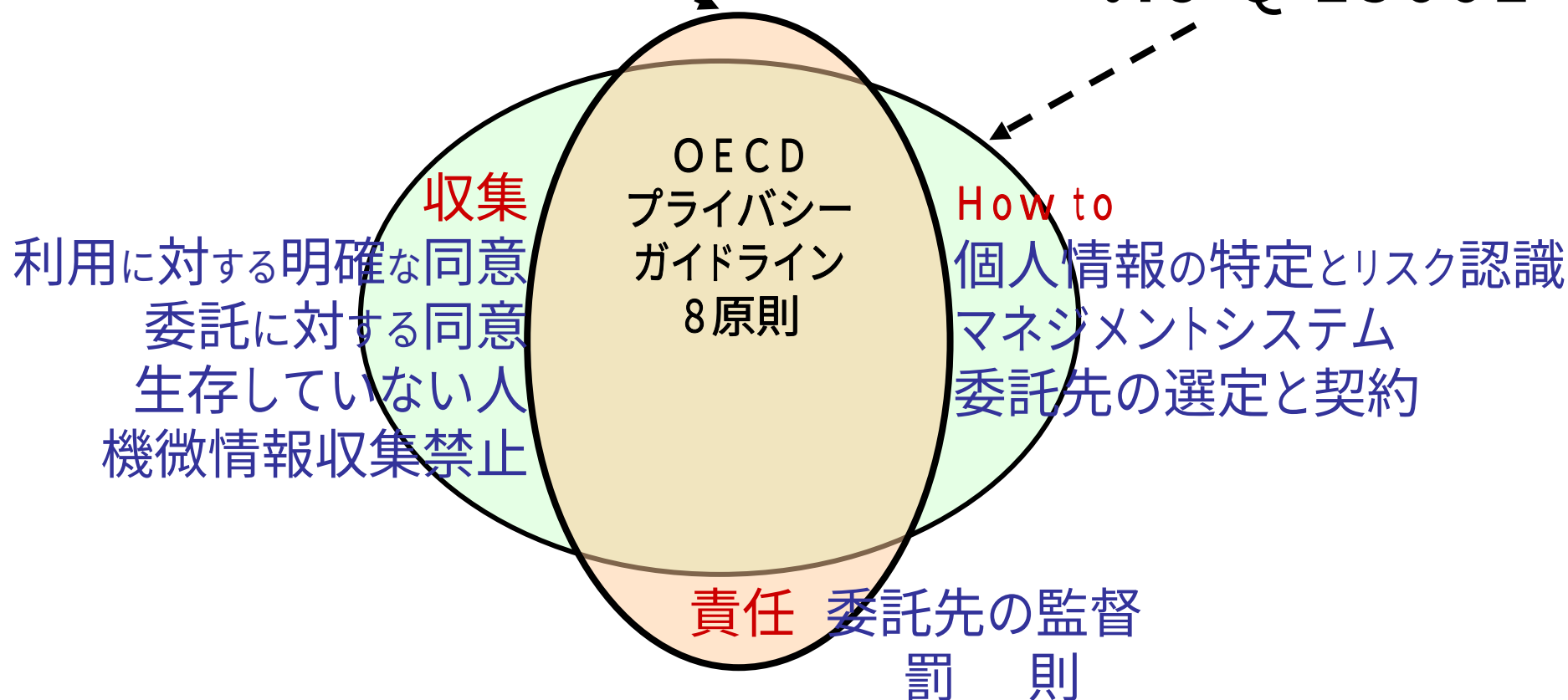
・・・個人情報保護法（平成15年法律第57号）による定義

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。）をいう。

JIS Q 15001と個人情報保護法の差異

個人情報保護法

JIS Q 15001



プライバシーマーク認証取得のメリット

形式的な信頼性

- 取引先・顧客への信用 (マネジメント力がある)
- 技術力のある会社 (障害時の対応等)
- 営業力の強化 (入札等)

実質的な信頼性

- ルールをつくり、実行し、監査、見直し、改善というPDCAサイクルが導入できる
- リスクアセスメント実施。教育の実施。
 - 社員の意識向上、事件・事故の未然防止
- セキュリティに対する緊張感の維持向上

プライバシーポリシーの公開事例



Copyright 2003 - 2004 総務省

総務省

～安心してインターネットを使うために～

国民のための情報セキュリティサイト

[更新履歴](#)
[このサイトの利用方法](#)
[サイトマップ](#)
[リンク集](#)
[教育用資料](#)
[お問い合わせ](#)

知識

情報セキュリティについての知識

はじめに

なぜ、情報セキュリティへの対策が必要なのでしょう。情報セキュリティの重要性と、具体的な内容について説明します。

基礎知識

情報セキュリティの基礎知識です。インターネットや情報セキュリティ、プライバシー、ウイルス、情報セキュリティに関する法律について説明します。

用語辞典

情報セキュリティに関する用語解説です。基礎知識に出てくる用語や、覚えておくと便利な用語について説明します。

事故・被害の事例

正しい情報セキュリティの対策をしていないと、どんな問題が発生するのでしょうか？ここでは実際に起こった事故・被害を紹介します。

対策 & 実践

利用方法に応じた
情報セキュリティ対策と実践

■エンドユーザー

電子メールを送ったり、ホームページを見るとき注意しなくてはならない情報セキュリティ対策と、具体的な実践内容について説明します。

小学生

たいさく
じっせん

一般利用者

対策
実践

■ホームページ開設者

ホームページを作成、公開している人のための情報セキュリティ対策と、具体的な実践内容について説明します。

プロバイダ
利用者

対策
実践

自設サーバー
利用者

対策
実践

■企業・組織

企業や組織の業務で、コンピュータを利用する場合における情報セキュリティ対策と、具体的な実践内容について説明します。

社員
職員全般

対策
実践

情報管理
担当者

対策
実践

組織幹部

対策
実践

[総務省トップページへ戻る](#)
[情報通信行政トップページへ戻る](#)

http://www.soumu.go.jp/joho_tsusin/security/index.htm

個人情報保護ガイドライン（経済産業省）

個人情報保護法の不具合を経済産業省のガイドラインでカバーする運用になっている

原則

個人情報保護法の不具合

個人情報取扱事業者は、電話帳に載っているすべての個人の承諾を得ない限り、譲渡や貸借は不可能

運用

経済産業省のガイドライン

電話帳の譲渡や貸借は問題にしない

資料概要

個人情報の保護に関する法律についての経済産業分野を対象としたガイドラインの策定

本件の概要： 経済産業省では、来年4月1日の個人情報保護法の施行に向けて、当省所管業種における個人情報保護法の適用をまとめたガイドラインを策定した。企業が具体的にどのような対応を行えばよいのか分かるよう、例示を入れるなど、具体的なガイドラインとなっている。

担 当： 商務情報政策局情報経済課

公 表 日： 平成16年6月15日（火）

発表資料名： 1. 個人情報の保護に関する法律についての経済産業分野を対象としたガイドラインの策定
(PDF形式: 724KB) [▶ 詳細](#)



[>> Acrobat Readerをダウンロード\(Adobeサイトへ\)](#)

http://www.meti.go.jp/policy/it_policy/press/0005321/index.html

ISSC（情報セキュリティ・サポートコンソーシアム）

＜サービス・メニュー＞

- ・情報セキュリティポリシー策定の支援
- ・情報セキュリティシステム導入・運用の支援
- ・情報セキュリティ関連セミナーの実施
- ・情報セキュリティ関連社員研修の実施
- ・プライバシーマーク認証取得の支援
- ・ISMS認証取得の支援
- ・各種規定類の作成支援

（問合せ先）

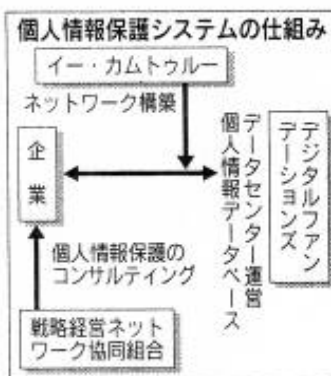
ファーストコンサルティング

〒085-0021 釧路市浪花町9-4-903

Tel 0154-22-0550 Fax 0154-22-0551

E-mail: noriyama@d2.dion.ne.jp

個人情報保護システム



イー・カム
など3社 法規制控え新組織

一括受注へ連携

システム開発のイー・カムツール（札幌市）など道内の情報技術（IT）関連三社は二十一日、

企業の個人情報保護システムを一括受注するため、連携組織を発足する。道内では大量の個人情報を取り扱うコールセンターなどの集積が加速している。来年四月に企業の罰則規定を含む個人情報保護法が完全施行されることもあり、三社が協力して新市場を開拓する。イー・カムツールとデータセンター運営のデジタルファンデーションズ（同市）、戦略経営ネットワーク協同組合（同市）が「情報セキュリティ

イ・サポートコンソーシアム」を設立する。連携組織は、情報管理の仕組みや従業員教育など個人情報の流出防止策を企業に指導し、プライバシーマークなどの取得を支援する。情報保護システムの一括受注は、デジタルファンデーションズが札幌市内で運営するデータセンターで情報を保管・管理することで情報流出の危険を軽減。システム導入に関する助言は、中小企業診断士などで組織する経営戦略ネットワークが担当する。

(振り返り) 個人情報保護法における事業者の義務

平成17年4月1日 完全実施

個人情報の**取扱**

利用目的の**特定**が必要 (15条)

個人情報の**取得**

利用目的の本人への**通知**または**公表**が必要 (18条)

利用目的の**変更**

本人への**通知**または**公表**が必要 (18条3項)

第三者への提供

本人の**同意**が必要 (23条、業務委託などの場合を除く)

まずは、個人情報の洗い出しから始めましょう！

質疑応答

？