個人情報保護法と
Pマーク制度について

Business Uphill by the Infomation & Large Desire
Office BUILD
オフィス・ビルド

オフィス・ビルド

目　次

1．世界の動き

EU諸国の動き

年	状　況
1970年代	スウェーデン、ドイツ、デンマークなどで個人情報保護法の法制化が進む
1980年代	OECDで「プライバシー保護と個人データの国際交流についてのガイドラインに関する理事会勧告」を採択（OECD8原則）
1995年	「EU指令（個人データ処理に係る個人の保護及びその自由な流通に関する欧州会議及びEU理事会指令」を採択
1996年以降	EU各国で法制改革・法制化が進む（イタリアなど15ヶ国）

他の国々の動き

国	年	状　況
アメリカ	1974年	プライバシー法施行、「公正信用取引」、「ケーブル通信政策法」、「ビデオプライバシー法」などに盛り込まれる
	1999年	商務省ガイドライン「セーフハーバー法」で対応
カナダ	1977年	カナダ人権法制定
	1982年	連邦プライバシー法制定
オーストラリア	1988年	プライバシー法施行
韓国	1994年	公共機関により管理された個人情報の保護に関する法律施行

OECD8原則とは

原　　則	内　　容
1. 目的明確化の原則	収集目的を明確にし、利用は収集目的に合致
2. 利用制限の原則	データ主体の同意がある場合、法律の規定による場合以外は目的以外に利用使用ない
3. 収集制限の原則	適法・公正な手段により、かつ情報主体に通知または同意を得て収集
4. データ内容の原則	利用目的に沿ったもので、正確・完全・最新
5. 安全保護の原則	合理的安全保護処置により、紛失・破壊・使用・修正・開示等から保護
6. 公開の原則	データ収集の実施方針を公開し、データの存在・利用目的・管理者を明示
7. 個人参加の原則	自己に関するデータの所在および内容を確認させ、又は異議申し立てを保障
8. 責任の原則	管理者は諸原則の実施の責任を有する

2. 個人情報保護法とは

個人情報保護関連5法

民間部門はこの法律のみ適用

- **個人情報の保護に関する法律（基本法）**
- 行政機関の保有する個人情報の保護に関する法律
- 独立行政法人等の保有する個人情報の保護に関する法律
- 情報公開・個人情報保護審査会設置法
- 行政機関の保有する個人情報の保護に関する法律の施行に伴う関係法律の整備に関する法律

目　的

- 個人の利益権利を保護すること
- **個人情報**の適正な取り扱いについて、国・地方公共団体の責務等や**個人情報を取り扱う事業者**の遵守すべき義務を定めること

個人情報の定義

- **個人情報保護法の定義**

第二条　この法律において「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。）をいう。

- **JISQ15001での定義**

個人に関する情報であって、当該情報に含まれる**氏名、生年月日その他の記述、又は個人に付けられた番号、記号その他の符号、画像若しくは音声**によって当該個人を識別できるもの
（当該情報だけでは識別できないが、他の情報と容易に照合することにより当該個人を識別できるものを含む）

個人情報取扱事業者の定義

- 個人情報データベース**等**を事業の用に供している者（データベース等とは、名詞ホルダーまで含む）

- 過去**6ヶ月間**において**5千**を越えた者

個人情報保護法の概要－１

項　目	内　　容
正式名	個人情報の保護に関する法律
公布日	平成１５年５月３０日
構　成	６章５９条＋附則７条
施行日	第１章～３章　公布日から施行 第４章以降（個人情報取扱事業者の義務と罰則 （平成１７年４月１日施行）
概　要	・個人情報の定義（第２条１項） ・個人情報取扱事業者の定義（第２条３項） ・個人情報取扱事業者の義務（第１５条～３６条） ・罰則（第５６条～５９条）

個人情報保護法の概要－２

内　　容

- 個人情報の利用目的を特定すること（第１５条）
- 個人情報の利用目的による制限（第１６条）
- 個人情報を適正に取得すること（不正取得の禁止）（第１７条）
- 利用目的を本人に通知または公表（第１８条）
- 個人情報の正確性の確保および安全管理措置をすること（第１９、２０条）
- 従業員および委託先社員の監督をすること（第２１、２２条）
- 本人の承認が無ければ第三者への提供は禁止（第２３条）
- 保有個人データに関する事項を公表すること（第２４条）
- 本人から開示・訂正・利用停止を求められたら応じること（第２５～２７条）
- 応じない場合はその理由を説明すること（第２８条）

罰　則

- 違反した条項により異なるが
  - 6ヶ月以下の懲役または
  - 30万円以下の罰金

罰金の額ではなく
企業にとっては新聞報道など社会的制裁が致命的

3．個人情報をめぐるトラブル事例

事例1（内部流失）

- 2001年8月、A百貨店の男性社員（38）が、同社の顧客カード会員のデータ約38 万人分を持ち出し、東京都内の民間信用調査会社に売却していたことが分かった。同社は男性社員を9日付で懲戒解雇し、窃盗と背任の罪にあたるとして警視庁新宿署に告訴した。
- データには顧客の氏名、住所、生年月日、年齢、郵便番号、電話番号が記録されていたという。（日本経済新聞8月16日）
- 38万2182人分の顧客データ流出、
- 複写したフロッピーディスク40枚と MO3 枚
- **情報の安全対策の不備から発生**

事例2（安全対策）

・P化粧品は、同社HPへの不正アクセスおよび営業所の業務用PC盗難によって、顧客情報が流出した可能性があると発表した。同社によれば、何者かがHPに不正アクセスし、顧客情報の　一部を閲覧した形跡が見つかったという。その後の詳細な調査により、不正アクセスを受けたのは5万1千件の個人情報で、氏名、生年月日、メールアドレス、住所、電話番号、職業などが含まれる。

・盗難被害に遭ったパソコンには氏名、住所、電話番号、メールアドレスなどを含む838名分の顧客情報が保存されていたという。同社では被害に遭った顧客全員にお詫びと報告を行った。

・原因対策として、HPの脆弱性の解消や、営業所の業務用管理パソコンに盗難防止用のセキュリティワイヤーを設置など、それぞれの事件に対応した防止策を実施するとしている。

事例3（委託先の管理責任）

・99年5月、京都府宇治市の乳幼児検診システム用住民データ約22万人分が名簿業者に流出し、「宇治市住民票」という名で、ネット上で販売されていることが発覚した。市民全員の個人データと外国人登録者のデータなどが流出した。

・流出したデータには、住所、氏名、生年月日、一部には電話番号などが記載されていた。**市はシステムの開発に関わった20代の大学院生を、市の「個人情報保護条例」違反（秘密漏えい）の罪で告発している。**

・管理責任を問われ、市が損害賠償

・個人情報保護に取り組む必要性と個人情報保護は経営上の重要な課題

その他の事例

- Yahoo-bb
  - 660万件の情報流失→500円の金券を配布
- 三洋信販→116万件
- シティバンク日本支店→12万件
- 阪急交通社→62万件
- ローソン→56万件
- 東京ディズニーランド→12万件
- 企業の損害賠償に要する費用は1件当たり平均、2億4千万円超のデータもある

適用除外企業でも情報流失は命取り

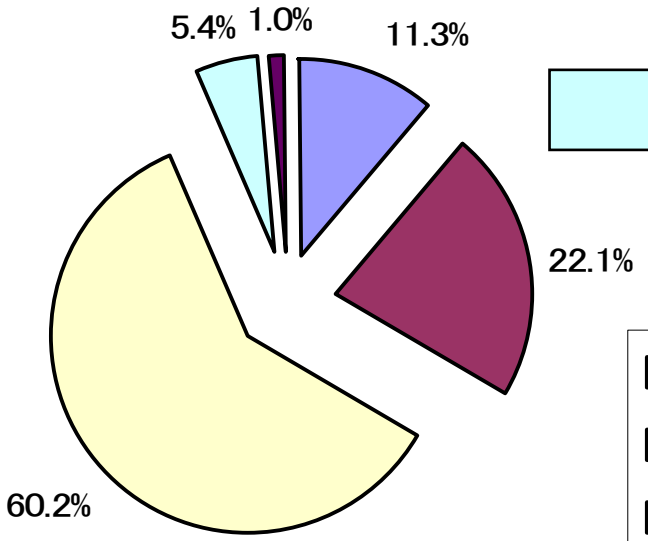
- 税理士事務所、FP
- 医者、美容整形、結婚相談所
- 塾、学校
- 測量会社、土地家屋調査士事務所、不動産
- DMを使用する業種

など、個人情報を扱う企業は山ほどある

流失事故から恐喝やオレオレ詐欺に発展するケースも

4月のJR福地山線脱線事故→死亡者が匿名となったり、JR側が名簿を出さないという事態があった→以前では考えられない

情報流失した場合の顧客の対応

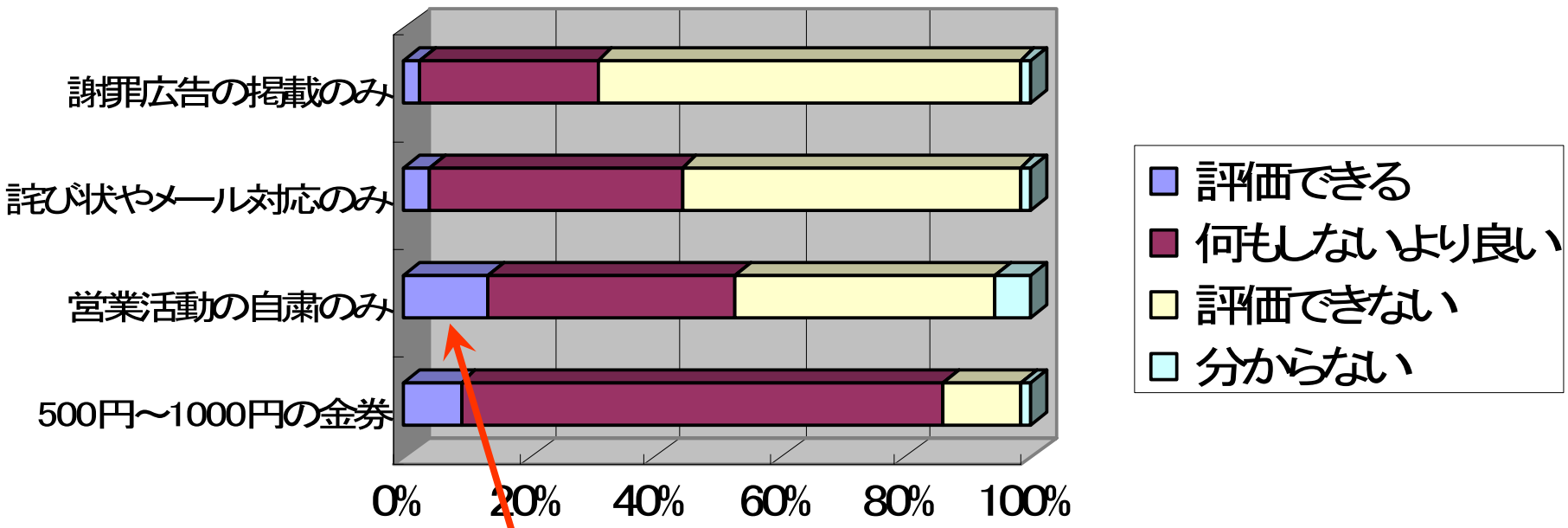


取引中止が33%

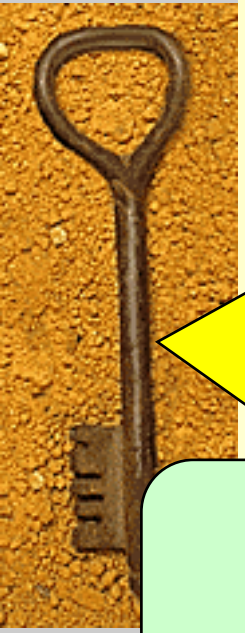
企業の対応によっては、取引中止となるグループが60%

日本能率協会総合研究所によるアンケート調査結果　有効回答7634

対応に対する顧客の評価



営業活動の自粛が最も多い意見



リスクマネジメントの一環として

個人情報管理

が不可欠な時代になった!!

4. 個人情報保護法への対応とPマーク制度

法律の遵守に関し行うこと

内　　容
・個人情報の利用目的を特定すること（第１５条）
・個人情報の利用目的による制限（第１６条）
・個人情報を適正に取得すること（不正取得の禁止）（第１７条）
・利用目的を本人に通知または公表（第１８条）
・個人情報の正確性の確保および安全管理措置をすること（第１９、２０条）
・従業員および委託先社員の監督をすること（第２１、２２条）
・本人の承認が無ければ第三者への提供は禁止（第２３条）
・保有個人データに関する事項を公表すること（第２４条）
・本人から開示・訂正・利用停止を求められたら応じること（第２５～２７条）
・応じない場合はその理由を説明すること（第２８条）

企業の取り組みと評価

- **社員が法律を遵守するには**

→法律を遵守するためには文書化（マニュアルや規定）が不可欠

→教育や監視も必要

- **顧客に安心してもらうには**

→会社の広告やキャンペーンよりも、法律が遵守されていることを第三者に証明してもらうのが一番分かりやすい

ファイル参照→順守の担保性

誰からも分かること

- 個人情報保護法を包括的に網羅しているシステム

  JISQ15001（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）

- 第三者評価制度

  プライバシーマーク制度

制度の骨子－１

概要	個人情報の取扱いについて適切な保護措置を講ずる体制を整備している民間事業者等に対し、その旨を示すマークとしてプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認容する制度
目的	1.個人情報の保護に関する個人の意識の向上を図ること 2.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 3.民間事業者に対して CP へのインセンティブを与えることを目的とする

制度の骨子－２

基　準	通商産業省の個人情報保護ガイドライン に準拠した C/P を策定し、 実際に個人情報の保護を推進している民間事業者 平成11年4月よりJISQ15001に読み替えて運用
取得単位	企業単位（事業部、工場単位も可）
使用範囲	店頭、契約約款、説明書、宣伝・広告用資料 封筒、便箋、名刺、ホームページ　等

制度の骨子－３

期間	マーク付与の有効期限は２年間、以降は２年毎の更新
公表	JIPDEC（日本情報処理開発協会）のHP
取り消し	個人情報の不適切な取扱いを行った民間事業者については、プライバシーマーク制度委員会における審議に基づいて、改善の勧告及びプライバシーマークの取消を行う

JISQ15001の仕組み

- **規格構成**

  4．1～4．6まで

  マネジメントシステムを意図して作成

- **要求事項**

  ISO14001：1996（旧版）と酷似

  ISOを構築した経験がある企業は取り組みやすい

作成する文書量は少ない

個人情報保護方針の策定

JISQ15001の概念

計画（P）
- 個人情報の特定
- 法令の特定
- 文書化
- 教育および監査計画の策定

実施（Do）
- 体制の確立
- 個人情報の収集、利用、安全管理
- 苦情受付
- 教育の実施

検証（C）
- 監査

見直し（A）
- 経営者の見直し

コンプライ
プログラム

取得までの流れ

6ヶ月～10ヶ月

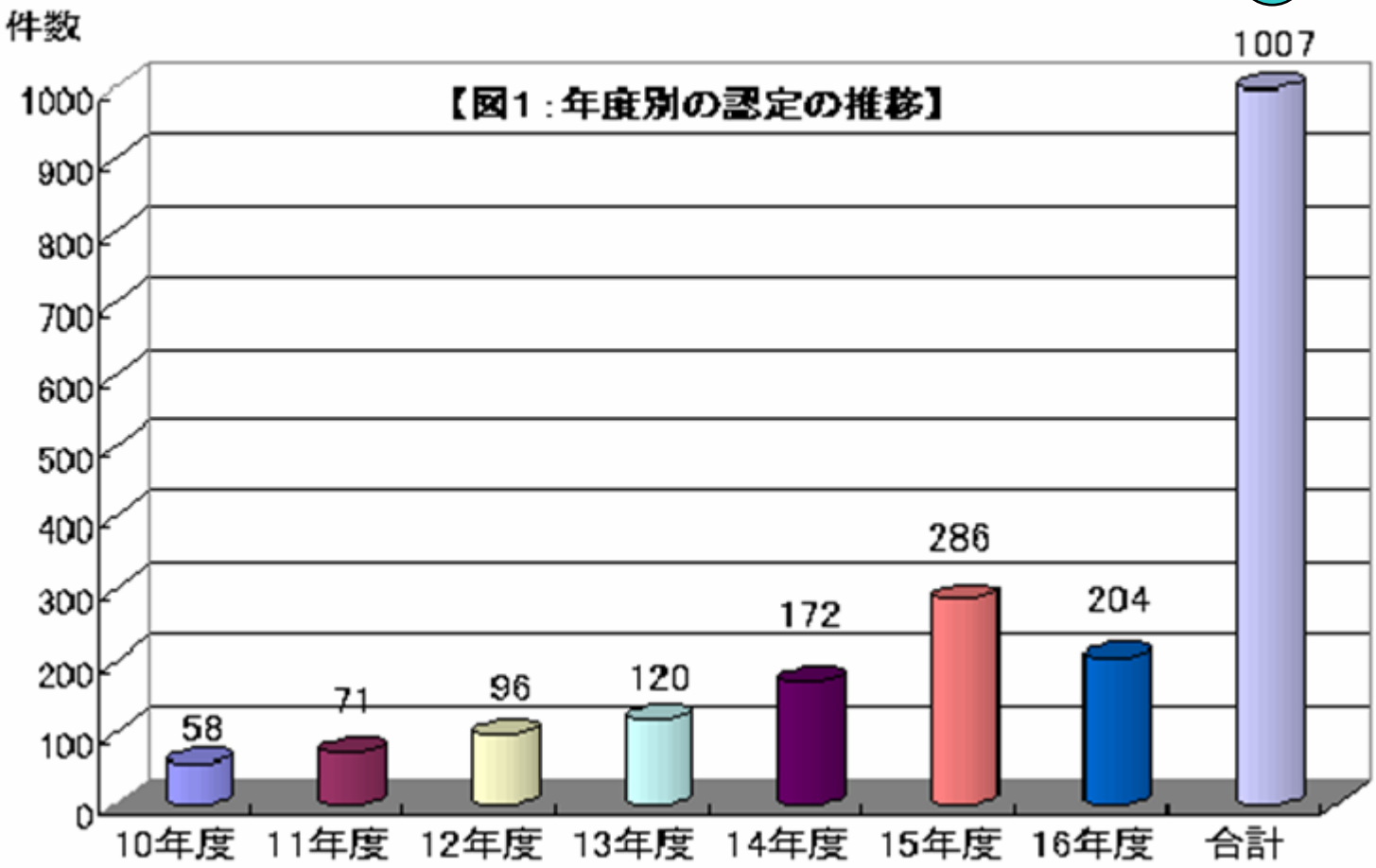
システム構築 → 運　用 → 見直し → 審　査

個人情報の洗い出し
法律の特定
文書化

運用・見直しの実績がないと審査申し込みが出来ない（現在、待ち時間6ヶ月以上）

取得状況

H.17.5. 2現在
1，361件



取得費用

- コンサルティング料金

＋

- 審査費用
  - 審査機関は4団体
  - 企業規模によって登録審査、30万～120万
  - 更新審査、22万～90万（2年毎）

参考情報

単位は万円

審査料金

種　別	新規のとき			更新のとき		
事業者規模	小	中	大	小	中	大
申請料	5	5	5	5	5	5
審査料	20	45	95	12	30	65
マーク使用料	5	10	20	5	10	20
合　計	30	60	120	22	45	90

中規模事業者の定義

	製造業	卸売業	小売業	サービス業
資本金	3億以下	1億以下	5千万以下	5千万以下
従業員	300人以下	100人以下	50人以下	100人以下

小規模事業者の定義

常時使用する従業員の数が二十人（卸売業、小売業[含、飲食店]又はサービス業に属する事業を主たる事業として営む者については、五人）以下の事業者

最後に・・・

- ２１世紀はコンプライアンスの時代
- 法律を守れない企業は市場から退場
  - ISO14001：2004の改訂では遵法性がより強化
  - CSR（企業の社会的責任）がより鮮明に
- 大企業では包括的なC/Pを策定してHPで公開する企業もある

おわり

- 問合せ先

Business Uphill by the Infomation & Large Desire
Office BUILD
オフィス・ビルド

オフィス・ビルド　野々村　剛

0586-26-1009

build.iso@anet.ne.jp

- 資料・出典
  - JICCA（日本ISOコンサルティング協会）

    http://www.jicca.com/
  - JIPDEC（日本情報処理開発協会）

    http://www.jipdec.jp/
  - 日本能率協会総合研究所

    http://www.jmar.co.jp/MDB/index.html
  - 総務省（関連ページ）

    http://www.soumu.go.jp/gyoukan/kanri/kenkyu.htm