

# 2002 プライバシーマークセミナー

## プライバシーマーク制度と コンプライアンス・プログラムの留意点

1. 個人情報の保護
2. プライバシーマーク制度の概要
3. コンプライアンス・プログラムの策定
4. コンプライアンス・プログラムの運用
5. プライバシーマーク制度の今後
6. 参 考

財団法人 日本情報処理開発協会  
プライバシーマーク事務局

# 1. 個人情報の保護

## プライバシーと個人情報

### プライバシーの概念

一人にしておかれる権利

1890年代の米国：私的な事柄の報道が背景

自己に関する情報の流れを自身でコントロールする権利  
情報化社会への到来で概念が変化

**個人情報**：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、又は個人別に付けられた番号、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ができ、それによって当該個人を識別できるものを含む。）。

# 1. 個人情報の保護

## 個人情報の取扱の現状認識

個人情報を巡る現象：

- 知らない間に集められる
  - 知らない間に使われ・売買されている
  - 誤ったまま使われている
  - 世間に漏示・漏洩される
- 事業者のリスク**
- 不正な収集・利用  
誤った処理、破壊・改ざん  
紛失・漏えい

個人情報を本人がコントロールできる環境の提供

自己の個人情報を自己がコントロールできていない状況

## 個人情報の保護の促進

事業者としてプライバシーの侵害に至るリスクを防止することが求められる

プライバシーが侵害された状況

# 1. 個人情報の保護

## 個人情報保護の流れを決めたOECDガイドラインとEU指令

### (1) OECDプライバシーガイドラインの採択：1980.9.23

①収集制限の原則	個人データの収集は適法かつ公正な手段によるべきであり、適当な場合にはデータ主体に通知又は同意を得て行うべき。
②データ内容の原則	個人データは、その利用目的に沿ったものであるべきであり、利用目的に必要な範囲内で正確、完全、最新に保たねばならない。
③目的明確化の原則	収集目的は収集時より遅くない時期に明確化されなければならない。その後の利用は収集目的と関連し、かつ明確化されたものに制限するべき。
④利用制限の原則	個人データは明確化された目的以外に使用されるべきではない。
⑤安全保護の原則	個人データは紛失・破壊・修正・開示等の危険に対し、合理的な安全保護措置により保護されなければならない。
⑥公開の原則	個人データに係る開示、実施、政策は一般に公開されなければならない。また、データ管理者を明示する手段を容易に利用できなければならない。
⑦個人参加の原則	自己に関するデータの所在を確認し知らせるべき。また、自己に関するデータについて異議申立ができ、消去、修正、完全化、補正ができればならない。
⑧責任の原則	データ管理者は、以上の原則を実施するための措置に従う責任を有するべき。

### (2) EU指令の採択：1995.10.24、98.10.25日発効

EU域外への個人データの移転禁止（第25条）

EU諸国と同等の「十分なレベルの保護措置」を講じない第三国への個人データ移転禁止

情報・ネットワーク技術の進展／利用の促進・利用範囲の拡大

個人情報保護の議論が各国で活発化

## 1. 個人情報の保護

## 各国の個人情報保護の取り組み

## 【EU諸国】・公的、民間部門をカバーする包括的法律(オムニバス方式)

データ保護監督庁: 業者登録、監視、調査、罰則

## 【米 国】・公的、民間部門を個別の法律(セグメント方式)

1974: プライバシー法(公的部門)

1998.10: 子供のオンラインプライバシー保護法(民間分野)

・業界による自主的な対応の促進 self regulation

1999. 3: BBBOnline Privacy seal Program等のシールプログラム

## 【OECD加盟国】・全ての加盟国で法律が制定

カナダ: 1982プライバシー法(公)、2000(民)

オーストラリア: 1988 プライバシー法(公)、2000(民)

ニュージーランド: 1993プライバシー法(公民)

韓国: 1994個人情報保護法(公)、1995信用情報の利用・保護の法律(民)

## 【OECD非加盟国】・多くの国でデータ保護法制定

イスラエル(1981)、モナコ(1993)、スロベニア(1990)、

リトアニア(1996)、エストニア(1996)、スロバキア(1998)、香港(1995)、台湾(1995)



Copyright © 2002 JIPDEC All rights reserved

5

## 1. 個人情報の保護

## 我が国の個人情報保護の取り組み

## 民間部門: 事業者の自主的な取り組みを推進

1989.6.28 : METI個人情報保護ガイドライン(1997.3.4改訂)

→ 業界ガイドライン登録制度(1989.7.7)

1998.4.1 : JIPDECプライバシーマーク制度

1999.3.20: コンプライアンス・プログラム要求事項の JIS 化

## 自治体: 個人情報保護条例 (1,994団体、60%。H13.4現在)

## 国: 行政機関の保有する電子計算機処理に係る個人情報保護に関する法律

(平成元年成立、平成2年10月施行)

## ⇒ 個人情報保護法制化の動き (2002年臨時国会で成立?)

- 個人情報保護概念の明確化
- 現代社会において必要不可欠な基本ルールの確立
- 国・地方公共団体における、基本法に則った法律上の措置、条例上の措置の促進
- 民間事業者において基本原則の遵守に向けた努力が払われることへの期待

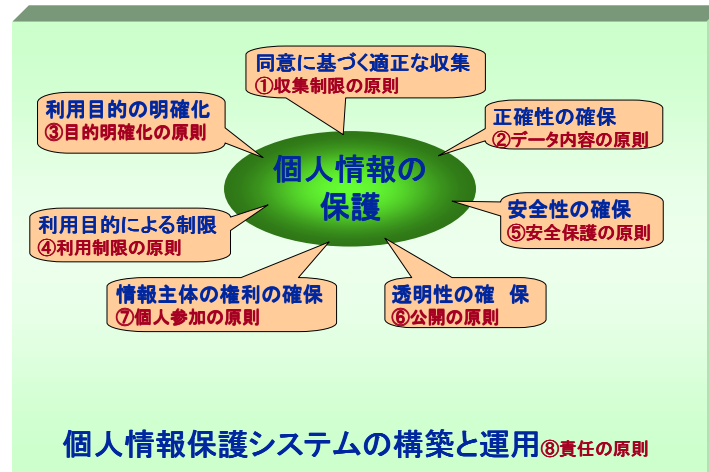


Copyright © 2002 JIPDEC All rights reserved

6

## 1. 個人情報の保護

## 個人情報の保護の概念



Copyright © 2002 JIPDEC All rights reserved

7

## 2. プライバシーマーク制度の概要

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。



Copyright © 2002 JIPDEC All rights reserved

8

## 2. プライバシーマーク制度の概要

### 目的

#### 事業者には:

個人情報の保護に関する信頼獲得へのインセンティブを提供

→ 個人情報保護システムの確立促進  
(JIS Q 15001の普及)

#### 消費者には:

事業者の個人情報の取扱いの適切性を容易に判断できる材料(マーク)を提供

→ 個人情報を自分で守る意識の向上



## 2. プライバシーマーク制度の概要

### 認定を受けることの意義

**直接収集する事業者**: 直接収集の対象者である消費者等からの信頼を得るためには、個人情報の取扱いが適切であることを示す必要があり、そのためにプライバシーマークの認定を受けることに意義。

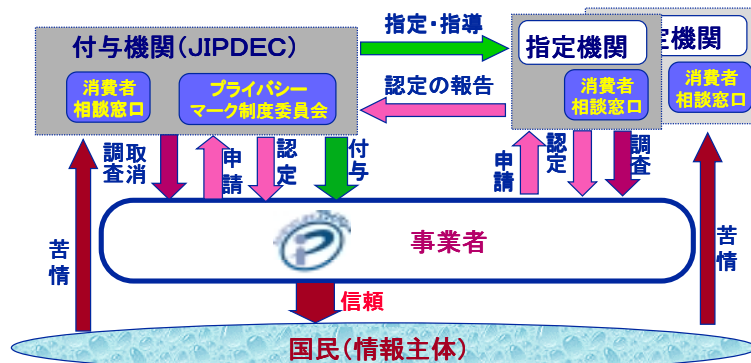
**預託を受ける事業者**: 取引先企業から安心して仕事を任せってもらうためにも、更に、多くの企業と取引を拡大するためにも、認定を受けることが優位。

**第三者から提供を受ける事業者**: ②の場合と同様、認定企業となることによって、個人情報の取扱いが適切な企業として判断され、安心して提供に応じてもらえることができることから、事業の推進に有利。



## 2. プライバシーマーク制度の概要

### 組織



## 2. プライバシーマーク制度の概要

### 付与の対象

- 国内に活動拠点を有する事業者
- JIS準拠のコンプライアンス・プログラム(GP)が策定され、それに基づき個人情報の適切な管理が実施されていること
- 申請の日前2年以内に下記の事項(欠格事項)に該当していないこと

- 認定を取消された事業者
- 個人情報を漏洩した事業者
- その他情報主体の権利を侵害した/恐れのある事業者

実質的に、情報主体から同意を得ることができない事業者

例) 電話帳データ、及びそれを含むソフト等を販売している事業者



## 2. プライバシーマーク制度の概要

### 付与の単位

#### \* 事業者(法人)単位が原則

#### \* マネジメント単位(事業部、工場等)の場合

- ①担当取締役が所掌しているマネジメント単位
- ②企業の代表者による個人情報保護方針(全社的保護方針)を受けてコンプライアンス・プログラムが策定されていること
- ③個人情報の取扱いが他事業部等から独立している  
但し、一部の業務を、他部門の協力を得て行う場合には、下記の内容を示す覚書きを両部門の取締役の名において取り交すこと  
・機密保持、再依頼(委託)、責任分担、返却/消去
- ④代表者名の「欠格事項への該当の有無について」を提出すること
- ⑤会社全体のパンフレットにマークを使用しないこと

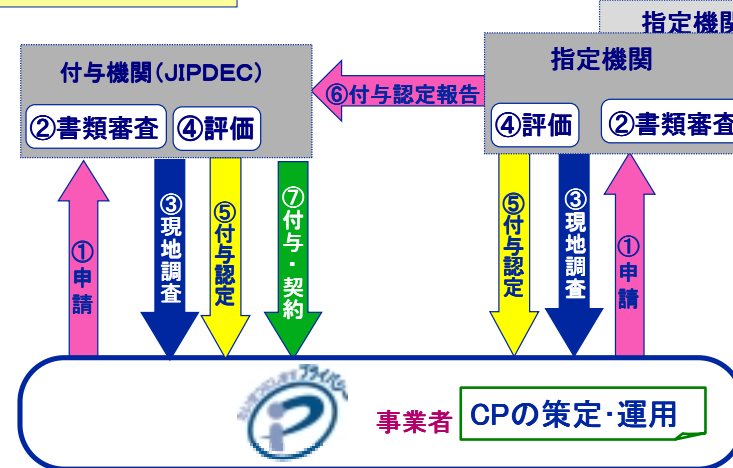
マネジメント単位のリスク: 他のマネジメント単位の違反等についても連帯責任が生じる



## 2. プライバシーマーク制度の概要

### 認定までの手続き

JISA(情報サービス産業協会)  
JMRA(日本マーケティング・リサーチ協会)  
JJA(全国学習塾協会)



## 2. プライバシーマーク制度の概要

### 申請書類

- ①プライバシーマーク付与申請書
- ②別紙:個人情報保護に係る体制の整備を示す書類
- ③登記簿の謄本、抄本等、申請者の実在を証する公的書類
- ④定款、寄付行為その他これらに準ずる規程類
- ⑤役員の名簿
- ⑥コンプライアンス・プログラム文書(JIS Q 15001に準拠)
- ⑦個人情報の適切な保護のためのその他の関係規程等
- ⑧欠格事項への該当の有無について
- ⑨ JIS Q 15001 の各要求事項とCP との対応表
- ⑩教育実施記録(CPを運用するにあたって事前に実施した教育研修記録)
- ⑪監査報告書(CPを導入後に行った点検に関する対応記録)
- ⑫その他、会社概要及び個人情報を取扱う事業を説明する資料

<http://privacymark.jp/appl/process.html#1>



## 2. プライバシーマーク制度の概要

### 申請

- (1) 申請上の注意
  - ①コンプライアンス・プログラムに関する周知徹底する教育が全員になされていること
  - ②コンプライアンス・プログラムに基づく運用実績があること  
Plan、Do、Check、Actionのサイクルを終えていることが望ましい
  - ③運用実績が確認できる記録が確保されていること
- (2) 申請の窓口
  - ①指定機関  
以下の機関に会員となっている事業者は、当該指定機関に申請
    - JISA(社団法人情報サービス産業協会)
    - JMRA(社団法人日本マーケティングリサーチ協会)
    - JJA(社団法人全国学習塾協会)
  - ②上記以外、JIPDEC(財団法人日本情報処理開発協会)に申請



## 2. プライバシーマーク制度

### 審査

#### 1. 書類審査(JISへの適合性)

- ①個人情報保護組織の整備
- ②研修の規定・計画
- ③監査の規定・計画
- ④消費者相談窓口の設置
- ⑤安全管理の措置
- ⑥外部委託の基準、保護に関する契約
- ⑦問題発生時の対応措置

#### 2. 現地調査(半日程度)

- ①経営課題としての認識
- ②全社的取組みの姿勢
- ③運用状況(エビデンスによる確認)



Copyright © 2002 JIPDEC All rights reserved

17

## 2. プライバシーマーク制度の概要

### 認定に係る費用

	規模別料金(消費税別)		
	小規模	中規模	大規模
申請手数料	80,000	150,000	300,000
現地調査料	20,000	50,000	100,000
使用料	50,000	100,000	200,000
合計	150,000	300,000	600,000

この他、現地調査に係る旅費、宿泊費を請求

1. 大規模事業者: 中規模事業を超える事業者
2. 中規模事業者: 資本金、従業員数何れか一方を満たす事業者

	製造業その他	卸売業	小売業	サービス業
資本金	3億円以下	1億円以下	5千万円以下	5千万円以下
従業員	300人以下	100人以下	50人以下	100人以下

3. 小規模事業者: 常時使用する従業員数が20人以下(商業、サービス業は5人以下)



Copyright © 2002 JIPDEC All rights reserved

18

## 2. プライバシーマーク制度の概要

### 認定後の調査等

#### 消費者からのクレーム等を受け実施

- ①報告書の提出を求める
- ②実態調査の実施
- ③改善勧告
- ④改善の要請

↓ (従わない場合)

認定取消し



Copyright © 2002 JIPDEC All rights reserved

19

## 2. プライバシーマーク制度の概要

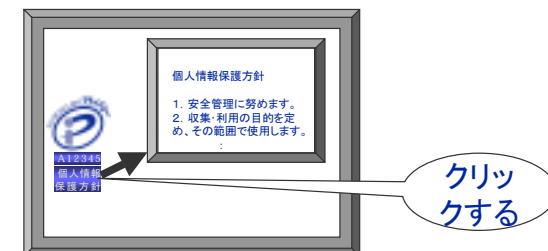
### マークの使用

①有効期限: 使用契約による2年間の使用(更新で継続)

②マークの活用:

- |      |          |         |               |
|------|----------|---------|---------------|
| * 店頭 | * 契約約款   | * マニュアル | * 広告          |
| * 封筒 | * レターヘッド | * 名刺    | * ホームページ etc. |

【ホームページで利用する場合】

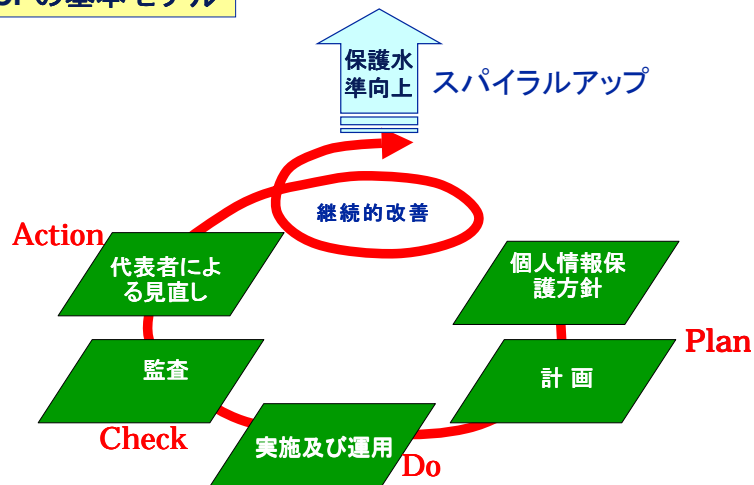


Copyright © 2002 JIPDEC All rights reserved

20

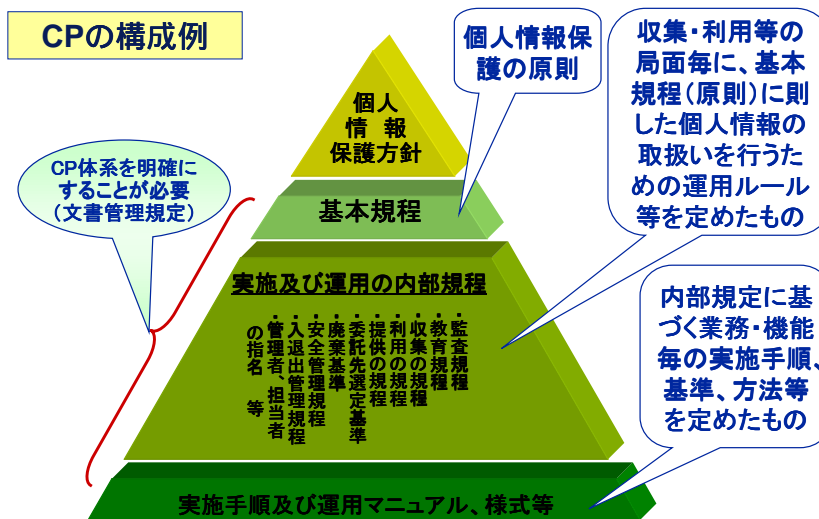
### 3. コンプライアンス・プログラムの策定

#### CPの基本モデル



### 3. コンプライアンス・プログラムの策定

#### CPの構成例



### 3. コンプライアンス・プログラムの策定

#### 【個人情報保護方針の策定】

- ・会社の姿勢を内外に示し、遵守を宣言(約束)する
- ・代表者は、個人情報保護方針を文書化し、従業員に周知。
  - a) 個人情報の収集、利用及び提供に関する方針
  - b) 不正アクセス、個人情報の紛失、破壊、改ざん及び漏えい等の予防、是正に関する方針
  - c) 個人情報に関する法令及びその他の規範を遵守に関する方針
  - d) CPの継続的改善に関する方針

**保護方針は、一般の人が入手可能であること。**

⇒ ホームページへの掲載等

★一般の人が理解できるように具体的な記述にも配慮する

### 3. コンプライアンス・プログラムの策定

#### 【個人情報の特定】

- 保有する個人情報の洗い出し
  - 広く解釈する
  - 公知のもので利用目的が違えば個人情報・電話帳データ
  - 名刺でもDB化、リスト化すれば個人情報
- 入手経路/媒体、保有媒体/形式、その処理経路、保管方法/場所等を洗い出し、それに対するリスクを検討する
  - ⇒ リスクは安全措置を検討する基礎となる
- 特定する手順を確立/維持する
  - ⇒ 事業遂行段階で新たに取扱いが発生する個人情報を見逃さない
  - ⇒ 特定した個人情報の利用目的を将来にわたって引き継ぐ

### 3. コンプライアンス・プログラムの策定

#### 【内部規程(CPの要素)の整備】

- 各部門における個人情報保護のための体制、権限、責任の規程
- 収集、利用、提供の規程
- 情報主体からの開示、訂正、削除の要求に対処する規程
- 適正管理(正確性、安全性、外注管理)のための規程
- 教育の規程
- 監査の規程
- 内部規程の違反に関する罰則の規程
- CP文書を管理する規程

#### 【内部規程の遵守に必要な事項の計画、ドキュメント化】

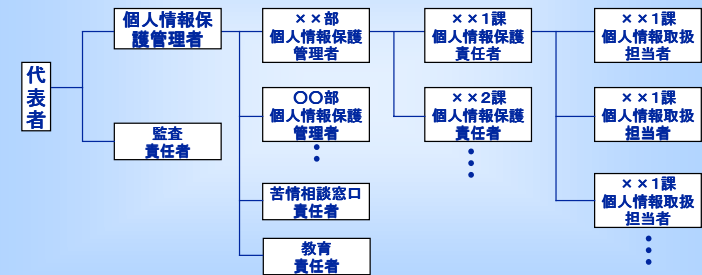
- 教育計画
- 監査計画



### 3. コンプライアンス・プログラムの策定

#### 【各部門における個人情報保護のための体制、権限、責任】

##### ■ 個人情報の保護体制の決定



##### ■ 各担当の役割、権限、責任を規定する(文書化)



### 3. コンプライアンス・プログラムの策定

#### 【収集の規程】個人情報の収集に関する措置(4.4.2)への適合

- 収集の原則(4.4.2.1)
- 収集方法の制限(4.4.2.2)
- 特定の機微な個人情報の収集の禁止(4.4.2.3)
- 情報主体から直接収集する場合の措置(4.4.2.4)
  - ◇ 6つの事項を通知する措置
  - ◇ 同意文言の雛型(個別の取扱い毎に)
  - ◇ Webサイトでは、同意文言を読ませ同意を取る工夫
- 情報主体以外から間接的に収集する場合の措置(4.4.2.5)
  - ◇ 適法かつ公正な手段で収集したものを提供者に確認する
  - ◇ 電話帳(ハローページ)データ、公知データの利用
    - 利用目的が違えば情報主体の同意が必要

上記を実現するため: Webアプリケーション作成要領などが必要

(SSL, Cookie, CSSへの対応等)



### 3. コンプライアンス・プログラムの策定

#### 【利用及び提供の規程】個人情報の利用及び提供に関する措置(4.4.3)への適合

- 利用及び提供の原則(4.4.3.1)
- 収集目的の範囲外の利用及び提供の場合の措置(4.4.3.2)
  - ◇ 改めて同意をとる必要
  - ◇ 収集目的の範囲外であることが確認できる手順の確立

#### 【適正管理の規程】個人情報の適正管理義務(4.4.4)への適合

- 個人情報の正確性の確保(4.4.4.1)
- 個人情報の利用の安全性の確保(4.4.4.2)
- 個人情報の委託処理に関する措置(4.4.4.3)
  - ◇ 委託先選定基準
  - ◇ 委託契約書の雛型



### 3. コンプライアンス・プログラムの策定

#### 【個人情報の開示、訂正、削除の規程】個人情報に関する情報主体の権利(4.4.5)への適合

- 個人情報に関する権利(4.4.5.1)
  - 本人確認の方法・手順の確立(なりすましへの対応)
- 個人情報の利用又は提供の拒否権(4.4.5.2)
  - 対応の方法・手順の確立(誤るとトラブルになる)

#### 【教育・研修規程】(4.4.6)

- 目的、担当、時期、対象、方法、効果の確認、等

#### 【苦情及び相談に関する規程】(4.4.7)

- 目的、担当、手続き・方法、対応

#### 【文書管理に関する規程】(4.4.9)

- 目的、担当、文書体系、改廃管理、配布管理



### 3. コンプライアンス・プログラムの策定

#### 【監査規程】(4.5)

- 目的、担当、対象範囲、時期、責務、報告義務、守秘義務等

#### 【内部規程の違反に関する罰則の規程】

- 機密保持等に関する誓約書を従業員等から取得
- 就業規則等、既存のものを適用することも可

#### 【問題発生時の対応に関する規程】

- 被害の拡大防止
- 早期収束
- 説明責任



### 4. コンプライアンス・プログラムの導入

#### 【代表者による導入の宣言】

- 個人情報取扱い業務に関わる役員及び従業員への意識付け

#### 【実施のための資源を確保する】

- 実施するための役割、責任及び権限の規程を適用
  - CPの実施及び管理に不可欠な資源の確保
    - ◇ リスク評価に基づき総合的な安全措置の構築
  - 規格の内容を理解・実践する能力のある管理者を指名
    - ◇ 役割と権限を自覚させる必要がある
  - 教育体制
    - ◇ 役員及び従業員に対する適切な教育実施
  - 苦情及び相談の体制
    - ◇ 情報主体への対応
  - 監査体制
    - ◇ 客観的な点検・評価ができる体制・責任



### 4. コンプライアンス・プログラムの導入

#### 【CPに基づき運用する】

- 教育の実施(導入教育の徹底)
- 個人情報の収集・利用・提供に関する措置  
Web上の措置: 保護方針の掲示、SSLの対応、Cookie利用の明示
- 個人情報の適正管理義務に関する措置
- 個人情報に関する情報主体の権利に関する措置
- 苦情／情報主体の権利等への対応
- 監査の実施(実効性の確認等のために導入監査が必要)
  - 浸透状況の確認(Q&A方式の調査票)

#### 【事業者の代表者による見直し】

- 監査結果、経営環境などに照らしたCPの見直し
- 監査責任者によるフォローアップ



## 5. プライバシーマークの今後

### 1. 積極的に推進

個人情報保護に関する法律(案)の実行性を担保する手段として、本制度を更に積極的に推進。

### 2. 海外制度(BBBOnline等)との相互承認の推進

日本企業が米国向けに使用

(JIPDECが付与)



米国企業が日本向けに使用

(BBBOnlineが付与)

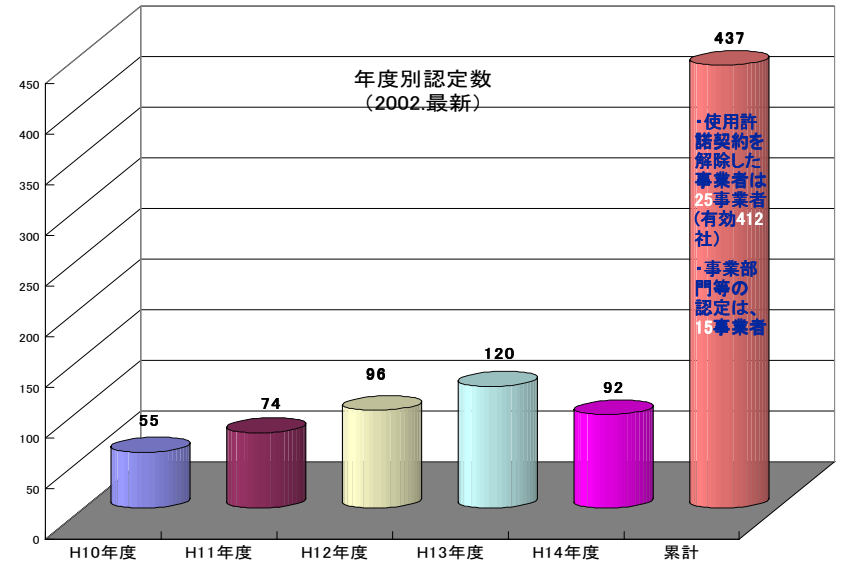


### 3. 韓国(ePRIVACY)、シンガポール、台湾との相互承認の確立



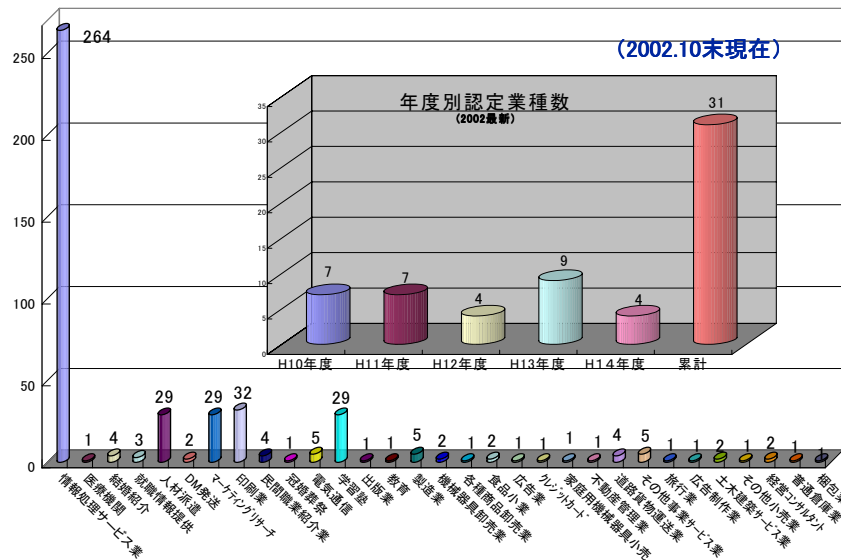
Copyright © 2002 JIPDEC All rights reserved

## 6. 参考



Copyright © 2002 JIPDEC All rights reserved

## 6. 参考



Copyright © 2002 JIPDEC All rights reserved

## 6. 参考

### 事業者の意識

	JISの認知	プライバシーマークの認知	プライバシーマーク企業の保護レベルは高い
監査部門	40.3%	32.2%	58.1%
被監査部門	37.6%	37.4%	57.6%

出展: JIPDEC平成12年11月  
「システム監査実態調査」より



Copyright © 2002 JIPDEC All rights reserved

プライバシーマーク事務局

TEL : 03-3432-9387

FAX : 03-3432-9419

E-mail: info@privacymark.jp

URL: <http://privacymark.jp>

〒105-0011 東京都港区芝公園3丁目5番8号

財団法人 日本情報処理開発協会

