

**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

<b>収集制限の原則</b>	個人データの収集は正当かつ公正な手段によるべきであり、適宜な場合にはデータ主体に通知又は同意を得て行うべき。
<b>データ内容の原則</b>	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。
<b>目的明確化の原則</b>	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一致し、かつ明確化されたものに制限するべき。
<b>利用制限の原則</b>	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。
<b>安全保護の原則</b>	個人データは紛失・破壊・修正・漏示等の危険に対し、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。
<b>公開の原則</b>	個人データに係る開示、変更、削除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。
<b>個人参加の原則</b>	自己に関するデータの所在を通知し知らされるべき。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、復元ができなければならない。
<b>責任の原則</b>	データ管理者は、以上の原則を履行するための措置に努む責任を有するべき。

(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、民間部門を個別的法律(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)



## 1. 個人情報の保護

## 我が国の個人情報保護の取組み

## 民間部門: 事業者の自主的な取組みを推進

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)

行政機関の保有する個人情報の保護に関する法律(03.5.23成立H15年法律第58号)

## 個人情報保護に関する法律 (2003.5.23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個人情報保護ルールの確立

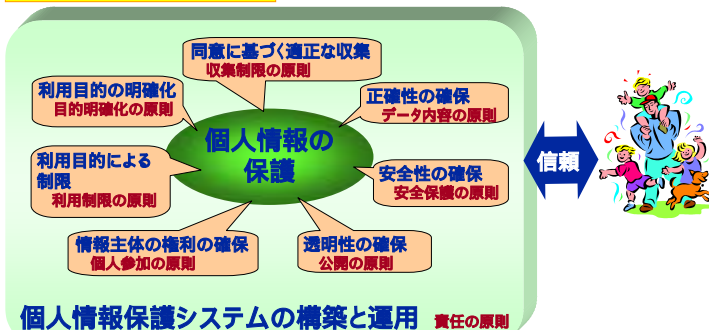
国・地方公共団体における、法律上の措置、条例上の措置の促進

民間事業者の法律遵守に向けた努力が払われることへの期待



## 1. 個人情報の保護

## 個人情報の保護の概念



## 個人情報保護の本質

消費者と企業との信頼関係構築  
 企業活動に個人情報を有効に活用(情報流通促進)  
 適切で質の高いサービスの提供



## 2. プライバシーマーク制度の概要

個人情報保護JIS(JIS Q 15001:1999)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。



事業者には: 個人情報の取扱いに関するリスクヘッジと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

## 消費者の不安解消と信頼獲得: (直接収集する事業者)

直接収集の対象者である消費者等の個人情報の取扱いに関する不安解消と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

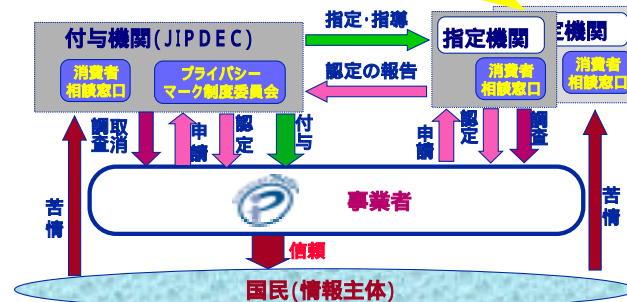
## 取引先企業の信頼獲得: (第三者から提供、預託を受ける事業者)

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事業推進上優位に立つ

## 2. プライバシーマーク制度の概要

## 組織

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)  
MEDIS-DC (医療情報システム開発センター)



## 2. プライバシーマーク制度の概要

## 付与の対象

- 国内に活動拠点を持つ事業者
- JIS準拠のコンプライアンス・プログラム (CP) 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

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

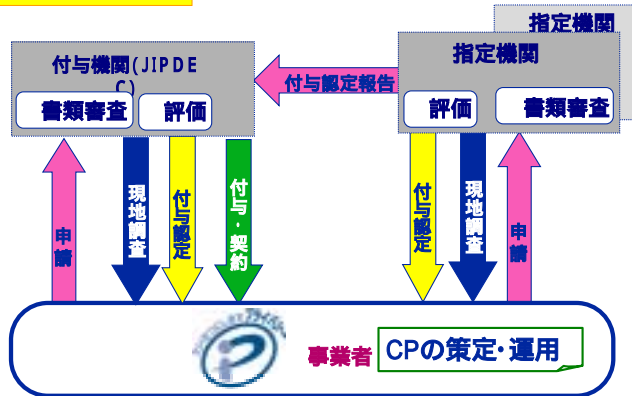
## \* マネジメント単位 (事業部等) の場合の要件

担当取締役が所掌しているマネジメント単位  
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  
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  
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  
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



## 2. プライバシーマーク制度の概要

## 申請書類

## プライバシーマーク付与申請書

別紙: 個人情報保護に係る体制の整備を示す書類  
 登記簿の謄本、抄本等、申請者の実在を証する公的書類  
 定款、寄付行為その他これらに準ずる規程類  
 役員の名簿  
 コンプライアンス・プログラム文書 (JIS Q 15001に準拠)  
 個人情報の適切な保護のためのその他の関係規程等  
 欠格事項への該当の有無について  
 JIS Q 15001 の各要求事項とCP との対応表  
 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)  
 監査報告書 (CPを導入後に行った点検に関する対応記録)  
 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

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従業員全員になされていること (申請時に**教育報告書**必要)  
 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, Actのサイクルを終えていることが望ましい  
 (現地調査時に、運用記録をチェックする)  
 導入後の監査を実施し、必要な改善を加えコンプライアンス・プログラムの実効性を確保していること  
 申請時に**監査報告書**の提出を求める

## (2) 申請の窓口

## 指定機関

指定機関の会員となっている事業者は、当該指定機関に申請  
 その他は、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の概要

## 審査

## 1. 書類審査 (規程、マニュアル、基準等のJISへの適合性)

個人情報保護組織に関する規程  
 個人情報の取扱に関する規程  
 教育研修規程と教育研修計画  
 監査規程と監査計画  
 消費者相談窓口の設置に関する規程  
 安全管理の措置に関する規程  
 外部委託の基準、契約に関する規程  
 問題発生時の対応措置に関する規程

## 2. 現地調査 (半日から1日程度)

経営課題としての認識 (経営層)  
 全社的取組み姿勢の確認 (経営層、個人情報保護管理者)  
 運用状況 (運用実績記録による) 確認  
 取現場の確認



## 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)



## 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

報告書の提出を求める  
実態調査の実施  
改善勧告  
改善の要請

従わない場合

認定取消し



## 2. プライバシーマーク制度の概要

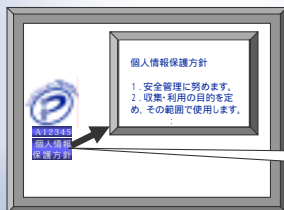
## マークの使用

有効期限: 使用契約 による2年間の使用(更新で継続)

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]

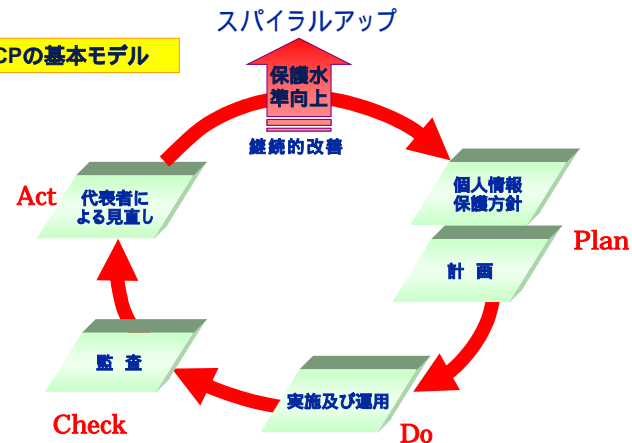


クリックする



## 3. コンプライアンス・プログラムの策定

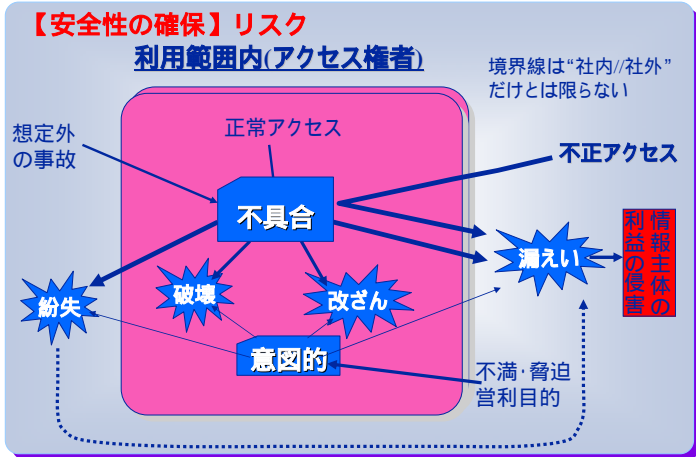
## CPの基本モデル







### 3. コンプライアンス・プログラムの策定



### 3. コンプライアンス・プログラムの策定

**【リスクへの対応の視点】**

これらの事情は事業者毎に異なるから、事業者自身が実情に合わせて対処しなければならない

「個人情報への不正アクセス」の防止

➢ 物理的と論理的アクセス対策

「個人情報の破壊・改ざん」の防止

➢ 使用不可の防止(正確性の確保)

「個人情報の紛失・漏えい」の防止

➢ 第三者へ渡ること(目的外利用)の防止

◆ 技術的対処

悪さをしようと思ってもできない仕組み  
 ヒューマンエラー防止

◆ 人の管理

ルール化と行動の制約  
 エビデンス(証跡)の確保

◆ フェイルセーフ

バックアップ  
 記録、ログ、...

### 3. コンプライアンス・プログラムの策定

**【リスクへの対応手順】**

1. 自社のリスクを把握する



2. リスクに合った対策を検討

(自分の身の丈を知る)



(自分に合った服を着る)

3. リスク対策を実施



(残存リスクを理解する)

4. リスクと対策を評価する



### 3. コンプライアンス・プログラムの策定

**【リスクと対応の管理】** 部署・業務・サービス・個人情報毎に

プロセス	対処すべきリスク	選択した対処法	関連する規程	エビデンス (確認できるもの)
収集				
保管				
利用				
委託・預託				
破棄				
訂正・削除				

・「特定表」と合わせて整理してもよい

## 3. コンプライアンス・プログラムの策定

1. 個人情報の安全管理に関する組織的対応の実施	(1)個人情報に関する安全管理体制の整備 (2)個人情報を取り扱う従業員以外の者によるアクセスの安全管理 (3)委託の安全管理に関する規程(選定基準、契約書)
2. 個人情報に対する責任者の明確化	個人データを適切に保護するために、個人データの安全管理に関する責任者を定めること
3. 人的な安全管理対策の実施	(1)雇用及び契約時における安全管理対策の実施 (2)従業員の役割・責任の明確化 (3)従業員に対する教育・訓練の実施 (4)事故又は違反等への対処
4. 物理的な安全管理対策の実施	(1)安全管理区画の設置 (2)装置のセキュリティ (3)盗難等に対する対策



## 3. コンプライアンス・プログラムの策定

5. 技術的な安全管理対策の実施	(1)情報システム等の管理 1)情報システム等の管理・運用の責任を明確にし、手順を確立 2)コンピュータウイルス等の侵入防止、検出の予防措置 3)バックアップ実施の手順確立 4)ネットワークの管理 5)記録媒体の物理的保護 6)個人情報情報の授受に伴う漏えい等を予防する措置
	(2)アクセス制御 1)個人情報へのアクセス手続きの整備(業務上及び安全管理上の要求への適合) 2)アクセス権限を管理手続きの整備 3)アクセス制御の有効性を維持する責任を従業員に認識させる措置 4)内部及び外部のネットワークへのアクセス制御措置 5)オペレーティングシステム(OS)によるアクセス制御措置 6)アプリケーションシステムによるアクセス制御措置 7)情報システムへのアクセス、使用状況の監視措置 8)モバイル機器の利用、在宅勤務、リモート保守作業等の遠隔作業のリスクに応じた保護対策



## 3. コンプライアンス・プログラムの策定

6. 安全管理措置の法令等の遵守措置	事業者は、個人データの安全管理を図るために必要な措置を講じる場合、法令、条例等に違反しないようにしなければならない。
7. 安全管理状況の評価・見直し	(1)個人データの安全管理を図るための基本方針、内部規程等の遵守を確実にするために、適切な監視活動、監査を実施することが望ましい。 (2)また、監視活動、監査の過程で発見された重要な問題点は、組織の代表者に報告することが望ましい。 (3)組織の代表者は、報告された問題点についての改善を指示することが望ましい。
8. ウェブ特有の問題	Cookieなどのウェブバグの利用の通知(と同意) Cookie、セッションIDなど代理認証の注意点 <ul style="list-style-type: none"> <li>▶タイムアウトの設定など</li> <li>▶クロスサイトスクリプティング(CSS/XSS)など</li> <li>▶同一サーバ上でのSSL採用ページと不採用ページの混在時の問題</li> </ul>



## 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

#### 【実施のための資源の確保】

- 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に基づく運用】

- 教育の実施(導入教育の徹底)
  - 全従業員に対する教育の実施
  - 未実施者への対応
  - 教育カリキュラムの充実
    - コンプライアンス・プログラムの理解度
    - コンプライアンス・プログラムに違反したときの影響 など
  - 日常的教育の必要性
    - 繰り返し実施することが重要
    - 最後は、人の問題に帰することを十分認識する必要がある
- 理解度の把握
  - 理解度の把握とカリキュラム・教授方法の改善
    - 理解度の把握方法
    - 受講後のテスト、感想
    - 日常の自己点検リストの実施と把握



### 4. コンプライアンス・プログラムの導入

#### 【CPに基づく運用】

- 個人情報の収集・利用・提供に関する措置の実行
  - 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の実行
- 個人情報に関する情報主体の権利に関する措置の実行
- 苦情/情報主体の権利等への対応
- 定着状況の把握
  - 日常的な現状把握(特に、導入初期段階は重要)
  - 現場担当者とのミーティング
- 不具合個所の発見
  - 現場担当者とのミーティングを通じた不具合
  - 自己点検リストの活用による浸透状況把握
- 不具合個所の早期是正
  - 是正指示と確認の励行



## 4. コンプライアンス・プログラムの導入

## 【CP運用の監査】

- 監査の重要性の認識
  - コンプライアンス・プログラムの改善に結びつく重要な役割の認識
  - 監査結果の信頼性確保が重要
- 監査の公平性、独立性
  - 内部監査 独立性の確保、厳正・中立な立場の堅持
- 監査の実施
  - CPの実効性の確認等のための導入時監査
  - 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】

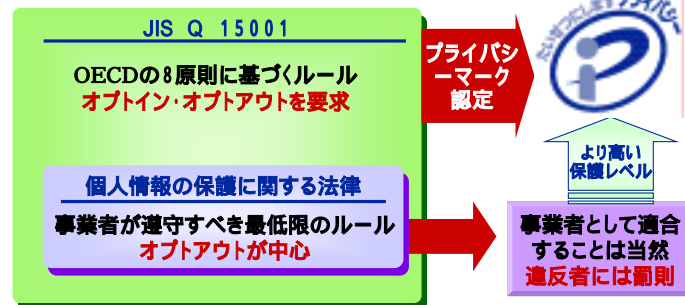
- 監査結果、経営環境などに照らしたCPの見直し決定と指示
- 監査責任者によるフォローアップ
  - 現場の改善計画と改善計画に基づく実施状況の確認



## 5. プライバシーマークの今後

個人情報保護に関する法律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。

高い信頼性を獲得



## 5. プライバシーマークの今後

海外制度 (BBBOnline、韓国(ePRIVACY)等) との相互承認の推進  
 プライバシーマークの認定事業者は、簡単な手続きで相互承認マークを使用することができる。

プライバシーマークの認定を受けている日本企業が米国向けに使用

(JIPDECが付与)

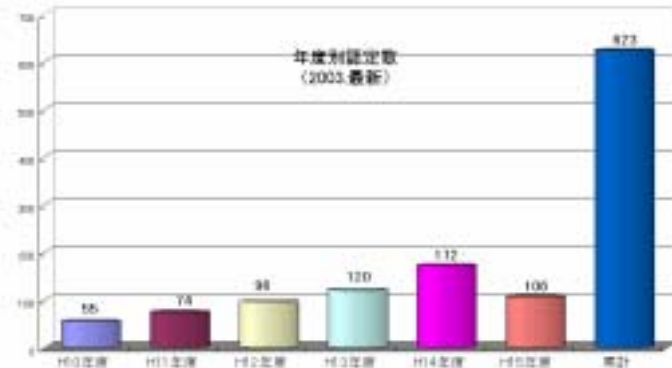


BBBOnlineシールの認定を受けている米国企業が日本向けに使用

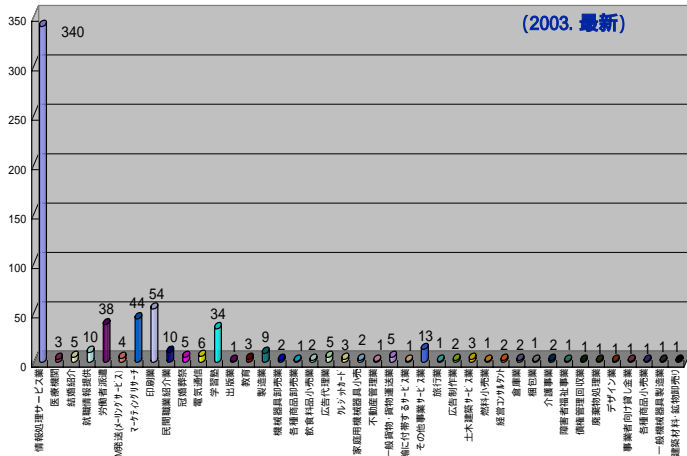
(BBBOnlineが付与)



## 6. 参考



## 6. 参考



## 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