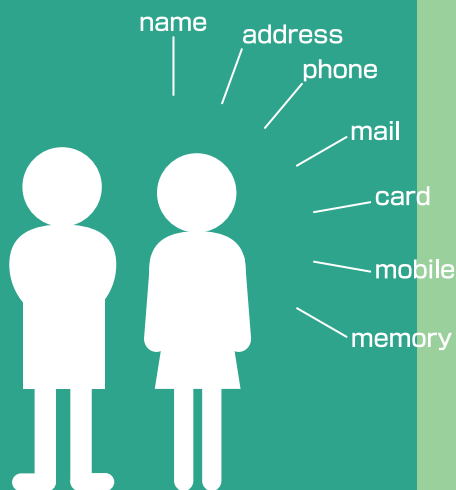


監修

新JISQ15001対応

# 個人情報保護 全体教育編

JISQ15001改正原案作成委員 鈴木靖 (株式会社シーピーデザインコンサルティング)  
JISQ15001改正原案作成委員 高芝利仁 弁護士 (高芝法律事務所)





## はじめに

2005年4月からの個人情報保護法の完全施行後、プライバシーマーク(以下Pマーク)取得事業者も7,000社を越え、個人情報に関する取り扱いの重要度も増えています。このような時代背景の中、Pマーク認証基準であるJISQ15001:1999(旧JIS)がJISQ15001:2006「個人情報保護マネジメントシステム—要求事項」(以下新JIS)と改正され、既にPマークを取得している事業者においても、新JISに対応したマネジメントシステムの構築が要求されています。新JISではPDCA(Plan, Do, Check, Act)サイクルによる継続的な改善を行う仕組みが強化され、要求事項がより具体化されました。

「2007 Pマーク対応 ～新JIS(JISQ15001:2006)2007年度個人情報保護 全体教育編～」は、企業の個人情報保護マネジメントシステムの構築と、Pマークの更新・取得を支援する為の研修ツールとして新JIS改正原案作成委員2名の監修により完成いたしました。個人情報保護能力を高め、企業としてお客様の信頼を得ていくために、取り組まなければならない対策について、具体的に解説します。

本テキストをよく読み、個人情報保護の重要性と会社の取り組みについて十分理解し、業務を行ってください。

2007年3月1日

## 目次

### 序章

- 03 第1節 なぜ個人情報保護が必要なのでしょうか？
- 04 第2節 企業にとって個人情報保護対策は急務！
- 04 第3節 個人情報保護法とプライバシーマーク

### 第1章 なぜプライバシーマークか？

#### 「個人情報保護マネジメントシステム」に適合することの重要性及び利点

- 05 第1節 個人情報に該当するものは何でしょうか？
- 06 第2節 生活者の苦情・不安は何でしょうか？
- 07 第3節 組織として個人情報保護に関する統制が機能していないとどのようなことがおきるのでしょうか。
- 08 第4節 個人情報保護の組織的な統制を確実に機能させるために、有効な手段とは
- 09 第5節 マネジメントシステムを構築するもの
- 10 第6節 旧JISQ15001からの改正ポイント

### 第2章 個人情報保護マネジメントシステム適合のための役割と責任

- 11 第1節 体制と方針及び規程

### 第3章 個人情報保護マネジメントシステムに違反したら？

#### 予想される結果

- 12 第1節 事業者に対する影響は？

### 第4章 個人情報保護マネジメントシステム 基本的なルール

- 13 第1節 個人情報取扱いのシーン
- 14 第2節 取得・利用時のルール
- 16 第3節 利用時のルール
- 17 第4節 本人へのアクセス時のルール
- 18 第5節 提供に関するルール
- 19 第6節 共同利用に関するルール
- 20 第7節 個人情報の取扱いを委託された場合のルール
- 21 第8節 適正管理のルール
- 22 第9節 リスクに応じた対応
- 23 第10節 委託先監督のルール
- 23 第11節 その他のルール
- 24 第12節 見直し・改善
- 25 第13節 緊急対応

### 第5章 安全対策としての日常点検

- 26 第1節 日常の注意事項
- 27 第2節 守るべき事例
- 28 第3節 パソコン利用時の注意
- 28 第4節 個人情報保管場所の注意

#### 29 最後に

- 30 <参考資料> 個人情報保護に関する法律

# 序 章

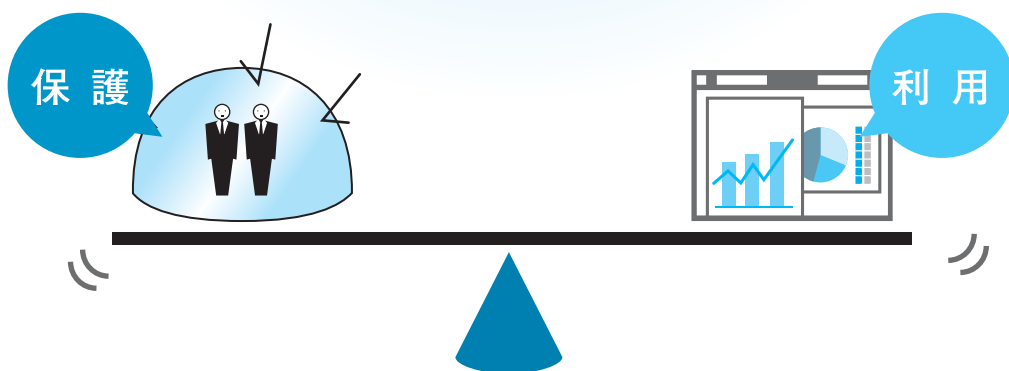
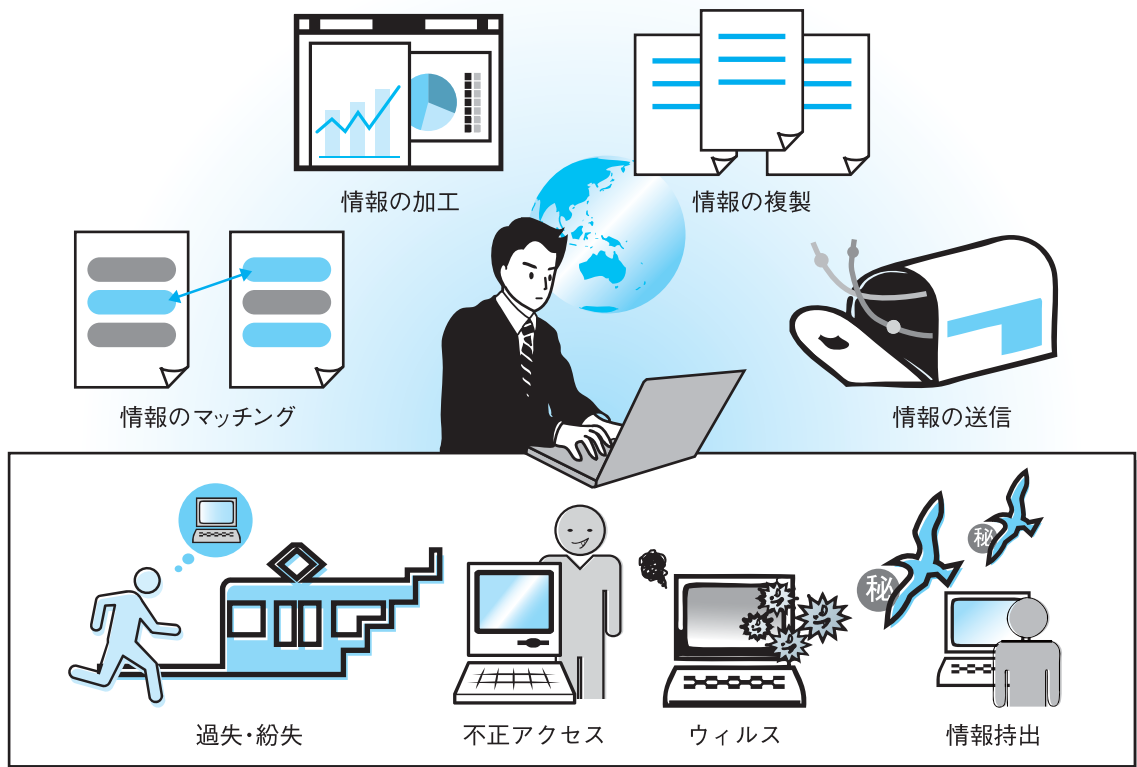
## 第1節

# なぜ個人情報保護が必要なのでしょう？

## 個人情報の不適切な取り扱いの多発によって生活者の不安感、嫌悪感が増大しています。

インターネット普及や、大量なデータ処理が可能になった現在、個人情報を含むありとあらゆる大量な情報が簡単に流通できる環境になりました。さらにIT化が進むにつれ、誰もが簡単に情報のマッチングによる高度な名寄せ、加工や複製、送信するようになっていきます。このような環境の中、個人情報の漏えい事件は後を絶ちません。また、勧誘電話や迷惑メールも巧妙化し、生活者の不安感、嫌悪感も増大しています。

このため、事業者が個人情報を有効に活用し、生活者に満足を得てもらえるサービスを提供するには、「個人情報の保護と利用のバランス」を考える必要に迫られてきたのです。



# 序 章

## 第 2 節

### 企業にとって個人情報保護対策は急務！

2005年4月個人情報保護法の全面施行により  
個人情報保護対策は、すべての事業者にとって必須課題となっています。

そうした背景もあり、2005年4月に個人情報保護法<sup>1)</sup>が全面施行されました。  
どのような事業者でも、個人情報を取り扱う局面があります。つまり、個人情報の取り扱い  
についての見直しと対策は、全ての事業者にとって必須課題といえるのです。

## 第 3 節

### 個人情報保護法とプライバシーマーク

プライバシーマークを取得、更新することによって、  
個人情報保護への取組みを客観的、合理的に对外表明出来ます。

「第三者機関による個人情報保護マネジメントシステムに適合している事業者認定制度」とし  
て、『プライバシーマーク制度<sup>2)</sup>』は1998年より誕生しました。

その1年後に日本工業規格『JISQ15001:1999<sup>3)</sup>』が制定され、『プライバシーマーク制度』は、  
この『JISQ15001』に基づき、個人情報の取扱いの適合性を審査するようになりました。  
その後、罰則を含む法律として、2005年に『個人情報保護法』が登場し、これにより個人情報  
保護という考えが広く知られるようになりました。

この法律の施行を受け、従来のJISQ15001:1999は、JISQ15001:2006に改正され、個人情報保  
護法との不一致をなくし、さらに一歩進んだレベルで個人情報保護を実現するための制度と  
して、認知されてきています。プライバシーマークを取得、更新することは、私達の個人情  
報保護への取組みを客観的、合理的に对外表明出来るのです。

**法の要求** IT社会において個人情報を守る法律として  
**個人情報保護法の登場**

**プライバシーマーク制度**

さらにプラス 審査基準のJISQ15001は  
【個人情報保護マネジメントシステム—要求事項】  
**2006版へ改正へ**

	日本の動き	国際的な動き	
1980		OECD8原則	
1989	通産省ガイドラインの策定		
1995		EU個人情報保護指令	
1998	プライバシーマーク制度の創設		▶ 通産省ガイドラインを認定基準とする
1999	JISQ15001:1999の制定		▶ PDCAサイクルという考え方
2005	個人情報保護法全面施行		▶ 個人情報保護ルール
2006	<b>JISQ15001の改正</b>		▶ 個人情報保護マネジメントシステムという考え方

表 1：『個人情報保護』の動き

1) 個人情報保護法とは  
個人情報保護法は、だれもが安心してIT社会の便益を享受するための制度的基盤として、平成15年5月に成立し、公布され、17年4月に全面施行されました。この法律は、個人情報の有用性に配慮しながら、個人の権利利益を保護することを目的として、民間事業者の皆様が、個人情報を取り扱う上でのルールを定めています。※参考資料参照

2) プライバシーマークとは  
JISQ15001に基づいた適切な個人情報の取り扱いを行っているかどうか審査し、審査に合格した企業に対してプライバシーマークの使用を許諾する制度です。審査は、付与機関である(財)日本情報処理開発協会(JIPDEC)、または付与機関によって指定された指定機関

により実施されます。第三者による認証がなされるため、認定を受けた企業は個人情報を適切に取り扱っていることを疑いなく内外に示すことが可能です。最近では、プライバシーマークの認定を受けていることを入札条件とすることも少なくありません。プライバシーマークの使用許諾を受けた企業は、ウェブサイトやパンフレット、名刺などにプライバシーマークを掲載し、対外的にアピールすることができます。

3) JISQ15001とは  
1998年に制定された、個人情報保護のためマネジメントシステムを構築する際の要求事項を定めたJIS規格です。JISQ15001では、事業者が保有する個人情報を保護するための方針、組織、計画、実施、点検および見直しというマネジメントシステムを構築するための要

## なぜプライバシーマークか？

「個人情報保護マネジメントシステム」に適合することの重要性及び利点

### 第1節

## 個人情報に該当するものは何でしょうか？

### 事業者内で扱う従業員情報や採用情報など、すべてが個人情報となります。

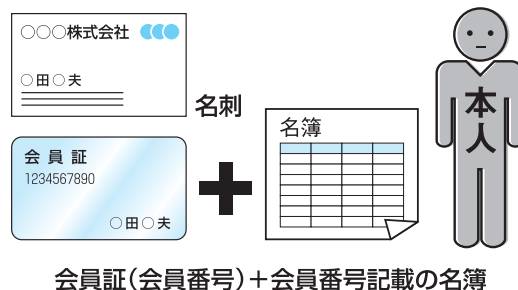
そもそも個人情報とは何でしょうか？ 個人情報とは、特定の個人を識別できる情報のほか、他の情報と容易に照合することができ、それによって特定の個人を識別することができる情報を指します。また、それによって識別される特定の個人を「本人」といいます。

私たちは、日常業務のあらゆるシーンで個人情報を取得していますので、どのようなシーンで個人情報を取得しているか、またこれらの個人情報をどのように運用管理しているかが、大事なポイントとなります。そのためには、まず、何が個人情報にあたるのか十分に理解する必要があります。個人情報は、顧客情報のみではありません。事業者内で扱う従業員情報や採用情報など、すべてが個人情報となります。

### 個人情報の取得例

- ① 情報提供サービス(DM、メルマガ)の申込書
- ② 購入、サービス利用の際の契約書
- ③ 名刺
- ④ 従業員の雇用情報
- ⑤ 採用の際の履歴書

### 特定の個人を識別できる全ての情報



会員証(会員番号) + 会員番号記載の名簿

図1: 個人情報とは？

求事項を記しています。JISQ15001の要求事項は、個人情報保護法よりも厳しいとされており、より高いレベルの仕組みづくりに利用されています。プライバシーマーク制度では1999年4月からJISQ15001に基づき、審査しています。またJISQ15001:1999「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」(以下、「旧JIS」という。)はJISQ15001:2006「個人情報保護マネジメントシステム—要求事項」(以下、「新JIS」という。)として改正され、2006年5月に発表されました。これに伴い、これまでプライバシーマーク制度において付与認定審査基準として適用している旧JISを新JISに移行することになり、旧JISでプライバシーマークを取得した企業は、新JISに対応するために内部規定やルールの変更が必要となりました。当然ながら改正に伴い新JISが求める内部規定の整備や仕組みを満

たしていることが必要です。

# 第1章

## 第2節

# 生活者の苦情・不安は何でしょうか？

## 生活者の苦情・不安は、 半数以上が『不適切な取得』となっています。

では実際に個人情報を取扱われる対象となる生活者にとって、個人情報に関する苦情や、不安としてはどういったものがあるのでしょうか。

2006年6月に国民生活センターが発表した『全国の個人情報相談窓口寄せられた相談の概況』の内訳では、その半数が『不適切な取得』についての苦情や不安でした。そして次が『漏えい・紛失』などといった安全性・正確性に関するもの、さらに『同意のない第三者への提供』、『目的外利用』、といった利用範囲についての不安、さらに『開示等』の透明性に関するものがあげられました。具体的な相談事例として「学習塾からダイレクトメールが送られてくる。子供の学校名まで記載されており、個人情報が不適切に取得されているようで不安だ」、「インターネットで賃貸物件の資料請求をしたら、別の不動産業者から広告がきた。同意していないのに個人情報を提供するのは違法ではないか」、「電話回線契約の申込書類を通信事業者が紛失した。口座番号等の記載があるので悪用が心配だ。事業者の責任を問えるか」などが挙げられます。

私達はお客様からの信頼を失わないためにも、決してこのような不安をお客様や関係者に与えてはいけません。

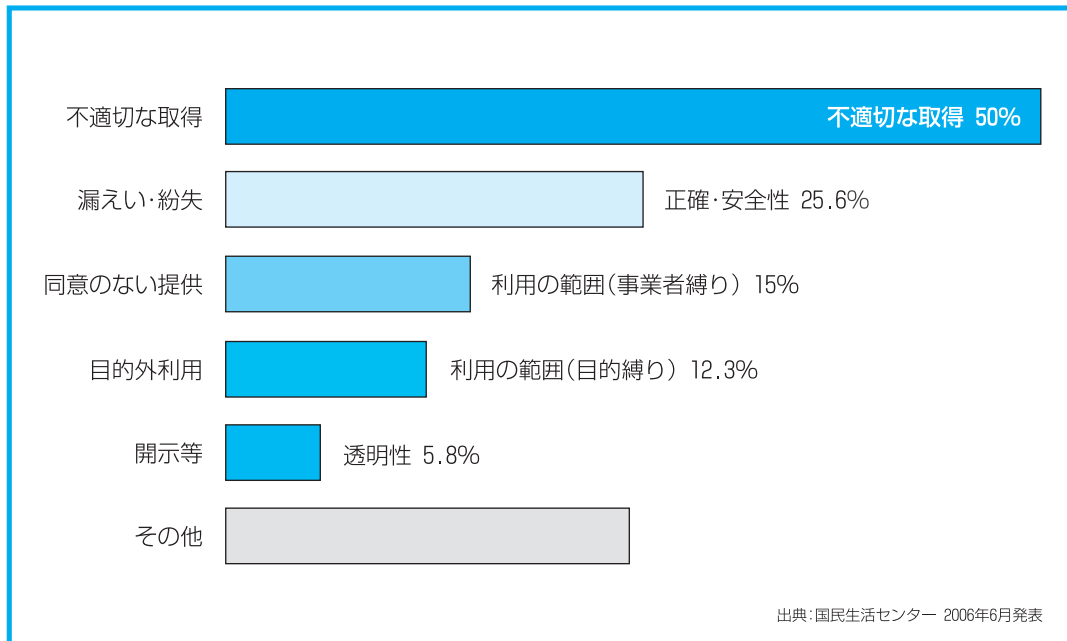


表2：全国の個人情報相談窓口寄せられた相談の概況

# 組織として個人情報保護に関する統制が機能していないとどのようなことがおきるでしょうか。

## 最終的には、 企業存亡の危機ともなりかねません。

個人情報保護のための規程、体制が整備されていない状態では、個人情報の不適切な取得や利用、提供が発生したり、正確性や安全性の不備、本人からの問い合わせなどに対する不適切な対応が発生したりすることが考えられます。これでは、「生活者が感じる個人情報の取扱いに関する不安」を無視した状態とも言えます。お客様及び関係者の信頼を失ってしまう事も当然の結果となりえます。もちろん、お客様の信頼を失墜することは企業にとって大きなダメージであることはいうまでもありません。

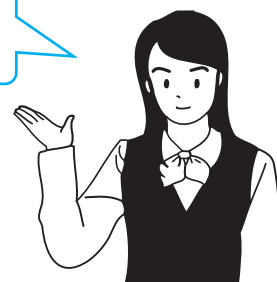
そのほか、個人情報の漏えい事故などのトラブルが発生することにより、

法的処置	罰則規定等による法的処置(行政処分・刑事罰等)
支出激増	高額な経費支出(調査等人件費・裁判費用・損害賠償金 等)
社会的信用失墜	対応の遅れによる二次被害発生に伴う信用失墜
営業機会損失	社会的信用の失墜に伴う営業機会の損失
株価暴落	ダメージの蓄積による株主信用失墜・株価暴落

といった事も考えられます。

個人情報保護の不備は、最終的には企業存亡の危機ともなりかねないのです。このようなことにならないため、個人情報保護に関する統制を機能させることが重要になってきます。

企業にとって  
お客様からの信頼は  
大切な財産です。



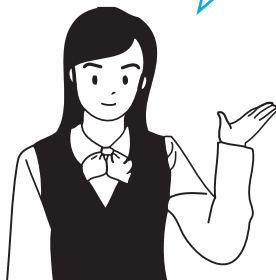
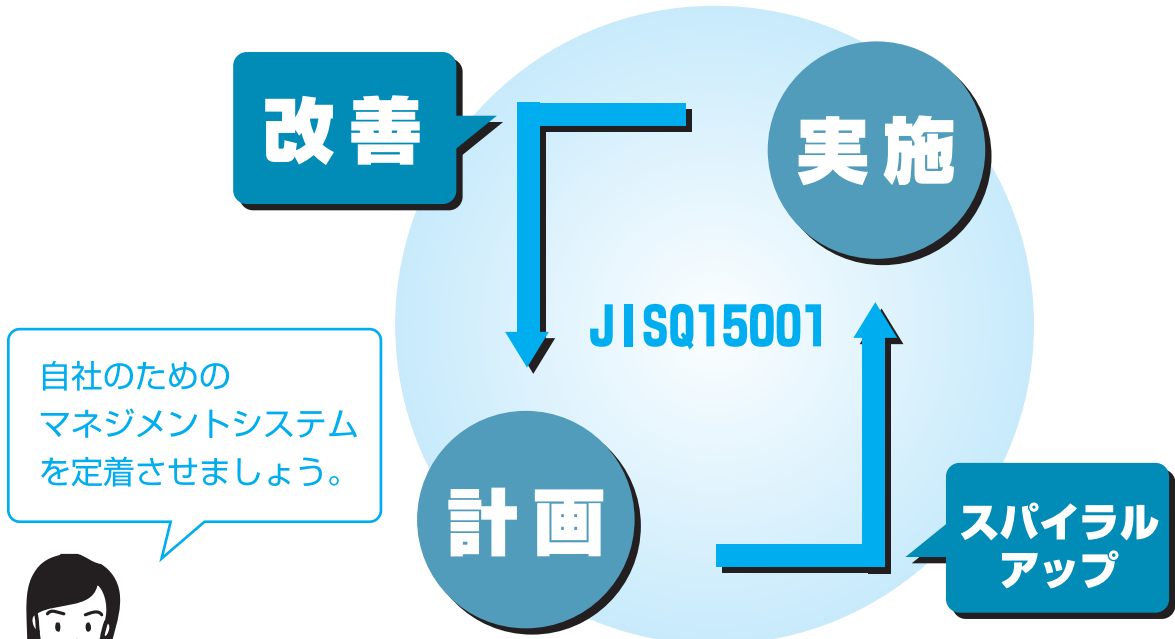
# 個人情報保護の組織的な統制を 確実に機能させるために、有効な手段とは

## JISQ15001

### 「個人情報保護マネジメントシステム—要求事項」への適合

個人情報漏えい事故を起こした企業の多くは、「漏えい防止策は取っていたが」「ルールが守られていなかった」ということが原因となっています。ルールをきちんと守っていくためにも、計画、実施・運用、点検、見直しのサイクル(マネジメントシステム)を定着させることが必要です。個人情報保護の組織的な統制を確実に機能させるために有効な手段となるのが、JISQ15001「個人情報保護マネジメントシステム—要求事項」への適合です。

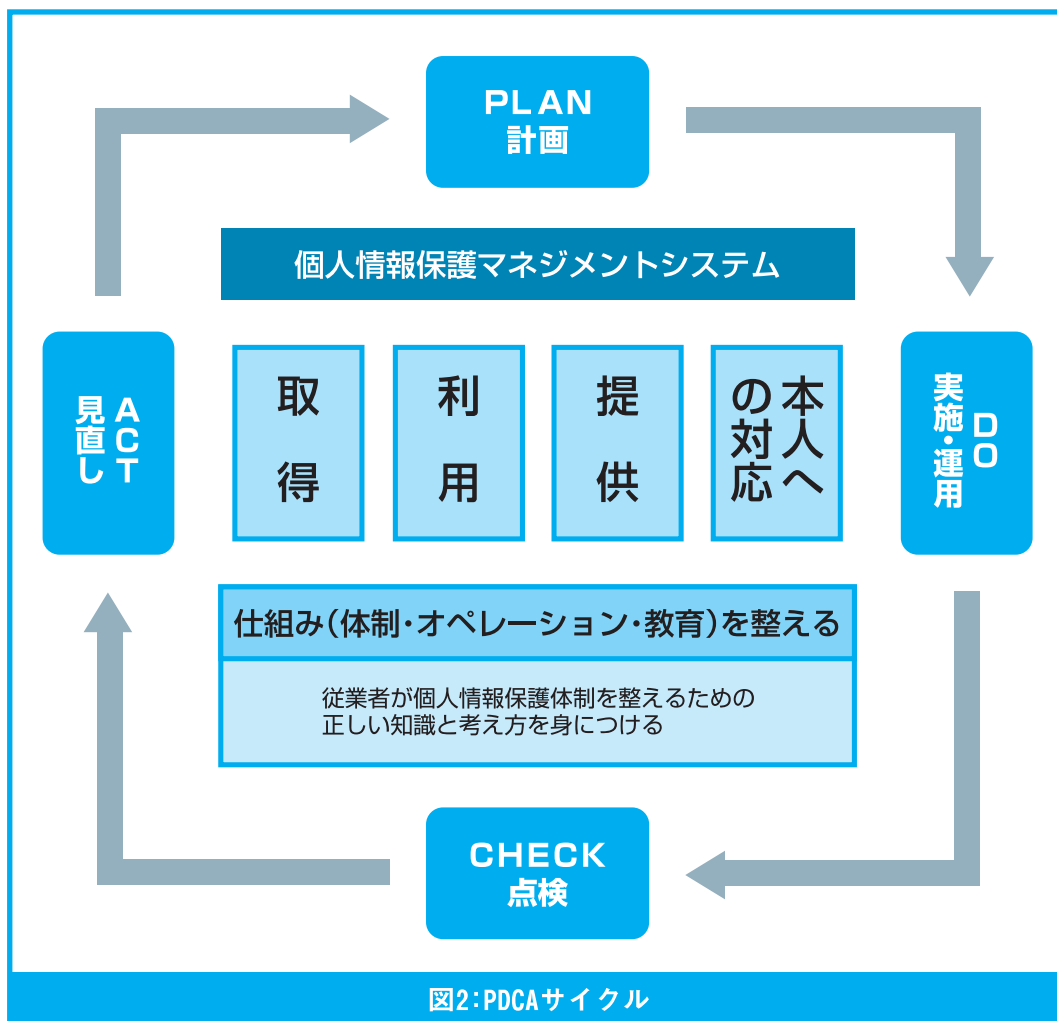
マネジメントシステムは、まず組織としての統制の仕組みをつくり、ルールに従って運用し、その運用の証跡を残し、さらに課題を見つけて改善するというプロセスを繰り返すものです。マネジメントシステムに適合することの重要性は、この「継続性」にあります。個人情報保護への取組みを一過性のものとせず、お客様及び関係者に安心してお付き合いいただけるような取組みを維持していかなければなりません。さらにこの規格により、個人情報保護のためのマネジメントシステムを構築し、その適合性を一定の基準により審査されることにより、プライバシーマークの付与を受ける事が出来るため、第三者機関による客観的、合理的な評価を得られるという利点もあります。



# マネジメントシステムを構築するもの

## 個人情報保護マネジメントシステムは、PDCAサイクルで構成されます。

個人情報保護マネジメントシステムは、PDCAサイクル、つまりPlan(計画)、Do(実施・運用)、Check(点検・監査)、Act(見直し)で構成されます。個人情報保護を実行するための仕組みを整え、ルールに従って運用し、さらに、点検、監査をおこない、問題点の見直しをし、さらに改善していくということ、つまり、PDCAサイクルを回していくことは、企業としての、個人情報保護能力を高めていくことができるのです。



# 旧JISQ15001からの改正ポイント

**個人情報保護のマネジメントシステムとしてPDCAのマネジメントサイクルの重要性が増し、その役割と責任がきちんと定義されることになりました。**

JISQ15001は、2006年5月に改正されました。この改正により、個人情報保護のマネジメントシステムとしてPDCAのマネジメントサイクルの重要性が増し、その役割と責任がきちんと定義されることになりました。

また認定基準としての要求事項も明確化され、より、客観的、合理的な審査が行われるようになりました。

### 名称の改定

個人情報保護マネジメントシステム

### 用語の統一

JISの用語を個人情報保護法の用語に統一

### マネジメントシステム(PDCAサイクル)の明確化

- ▶ ISO Guide 72 に従った規格とし、他のマネジメントシステム規格との構造の整合性を確保

### 認定基準としての要求事項の明確化

- ▶ リスク等の認識・分析及び対策
- ▶ 緊急事態への準備
- ▶ 個人情報保護マネジメントシステム文書(記録管理追加)
- ▶ 点検－運用の確認
- ▶ 是正処置及び予防処置

図3: JISQ15001:2006 改正ポイント