

2006年版  
**Pマーク**

ライバシーマーク制度  
[JISQ15001:2006]

**取得・更新の秘訣！10のポイント**  
～読めば分かるPマーク取得・更新のコツ～

株式会社日本ルシーダ



# 2006年版Pマーク [JISQ15001:2006] 取得・更新の秘訣！10のポイント ～読めば分かるPマーク更新のコツ～

JISQ15001:2006では、個人情報保護法との整合性を取り、マネジメントシステム(PDCAサイクル)に即した内容に改定されている。2005年12月15日に案が発表され、2006年5月20日に制定されました。プライバシーマークは、2年ごとの更新が求められていますので、2006年11月20以降に更新する企業は、このJISQ15001:2006に準拠しなければ更新できなくなります。

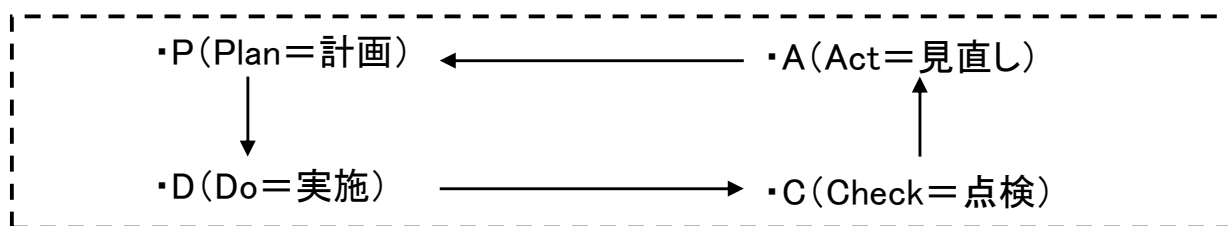
現在、JISQ15001:1999と新しいJISQ15001:2006とでは、**何が違う**のでしょうか？大きな特徴は

- ・用語の統一：個人情報保護法との用語の統一する
- ・個人情報保護法の概念の取り込みを明確にする
- ・マネジメントシステムへより具体的に、厳密に取り組む

の3本ではないでしょうか。

さらに大きな違いは、**通常業務における点検業務が明示される**ようになったことでしょう。また、その規格が、ISO Guide 72(「マネジメントシステム規格の正当性及び作成に関する指針(2001)」)に従って作成されている**“PDCAサイクル”**に即した形になっており、より管理体制を強化、明確する方向に進んでいるものといえましょう。

この“PDCAサイクル”とは、



であり、特に**安全管理措置を物理的、技術的に定義**することが大きな取得のための大きなチェックポイントとなっています。

昨今、個人情報保護の取扱いをめぐり、多くの事件、事故が発生し、また企業側の被害も予期せぬ大きなものとなっています。この対策として保護法が制定されてから、このP-マークの重要性が高まり当然のことながら、その**取得・更新における審査が非常に厳しく**なっています。また企業間取引においても、このP-マークの取得が常識となってきていることも事実です。

新たに文書の作成や分析作業を行わなければならなくなっているから状況も合わせて、旧制度での運用している場合、早急に、かつ新JISQ15001:2006への対応を考えなくてはならないでしょう。



# 「安全管理措置」を いかにクリアするかが大きなポイント！ ～物理的安全管理措置編～

## Point 1 外部記録媒体の使用制限

情報漏えいの典型的な例として、社内情報をUSBメモリに記録、自宅のPCへコピーといったものがあります。会社指定のUSBのみ使用可能にしたり、一切の使用を禁止している会社もあります。それは、安全管理措置の物理的なチェック項目にもあがっているこのポイントによるものです。

### 1.2 盗難等の防止

#### チェック項目⑦

FD、MO、CD、USBフラッシュメモリ等の外部記憶媒体の利用はルールに従っている。



なら、指定ドライブへの情報書き込み、コピーをパソコン単位の禁止設定できます。

## Point 2 モバイルPCのドライブ暗号化

ノート型PCで個人情報を取扱っていた場合、常に第三者によってPC内の情報を見られてしまう可能性が潜んでいます。それは、安全管理措置の物理的なチェック項目にもあがっているこのポイントによるものです。

### 1.3 機器・装置等の物理的な保護

#### チェック項目①

個人情報を取扱う機器・装置等について、安全管理上の脅威(盗難、破壊、破損等)や環境上の脅威(漏水、火災、停電、地震等)からの物理的な保護装置がある。

個人情報を収納したドライブがあれば、当然のことながらパスワードをかけておく必要がありますが、このようなリスクを間接的に回避するために、モバイルPCの取扱い自体の意識を高めること、またモバイルPCをいつ誰が使用したかの状況を監視することも大切なポイントです。



なら、「操作監視」機能により、持ち出しパソコンつまり、社外で使用したパソコンの操作を記録できます。



# 「安全管理措置」を いかにクリアするかが大きなポイント！ ～技術的安全管理措置編～

## Point 3 個人情報へのアクセス権限の設定

昨今、従業員同士の情報共有の為に、社内情報見放題の企業が多く見られますが、個人情報へのアクセスには制限をかけなければいけません。顧客情報、重要ファイルへのアクセスには認証が必要、社内データベース管理ソフトの無制限使用を防止する等の処置が必要です。

## Point 4 個人情報へのアクセス履歴の記録

いつ・誰が・どの個人情報にアクセスしたか等の記録を残しておき、監査の際に見せる必要があります。紙媒体の情報なら閲覧の記録を、電子ファイルならアクセス履歴をコンピュータ上に残し、長期保存できるシステムが必要となります。

## Point 5 個人情報へのアクセス情報を定期的にチェック

個人情報へのアクセスを記録・保存だけでなく、定期的なチェックもする必要があります。毎月1度はセキュリティ管理者によって確認される必要があります、確認の記録を残しておく必要があります。

それは、安全管理措置の技術的なチェック項目にもあがっているこのポイントによるものです。

### 2.4 個人情報へのアクセス記録

#### チェック項目①

個人情報へのアクセスや操作の成功と失敗の記録を取得し、保管している。

#### チェック項目②

取得した記録について、漏洩、滅失及びき損から適切に保護している。



なら、各パソコンで使用したファイルの書き込み、削除等各種操作監視情報、操作禁止違反情報の件数を表示します。  
(日次・週次・月次)

また、指定アドレスにメール通知機能があることでクリアできます。



# 「外的要因」に対する対策は・・・ ～ネットワークを考える～

## Point 6 社内ネットワークアクセスの権限設定

もし社内ネットワークへ外部の端末が侵入できたら、ネットワーク上にある個人情報を丸ごと持っていかれてしまいます。そのようなリスクを回避するためにも社内LANへのアクセス時にID、パスワード認証を行う必要があります。完全に排除するにはさまざまな観点からの環境作りが必要となります。



なら、こんな点がチェックできます。

- ・管理パソコンとして登録されていない未登録パソコンを検出
- ・各パソコンの外部ネットワークとの通信を記録

## Point 7 メール添付ファイルの暗号化

インターネット上での盗聴やメールの誤送信による情報漏えいは年々、増える傾向にあります。メール添付の際もそうですが、日ごろから個人情報、機密情報は暗号化しておくべきでしょう。それは、安全管理措置の技術的なチェック項目にもあがっているこのポイントによるものです。

### 2.6 個人情報の移送・通信時の対策

#### チェック項目③

盗聴される可能性のあるネットワーク(例えばインターネットや無線LAN等)で個人情報を送信(例えば本人及び従業員による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等)する際に、個人情報の暗号化又はパスワードロック等を実施している。



なら、重要な文書を暗号化して保存しておくことができます。



# 「外的要因」に対する対策は・・・ ～ネットワークを考える～

## Point 8 ウィルス対策ソフト、セキュリティパッチの適用

ウィルス対策ソフト、セキュリティパッチの更新が定期的になされているか、管理が必要です。更新切れのままになっている事もあります。それは、安全管理措置の技術的なチェック項目にもあがっているこのポイントによるものです。

2.5 個人情報を取扱う情報システムに関する不正ソフトウェア対策  
チェック項目①  
ウィルス対策ソフトウェアが導入され、常に最新版が適用されている。



なら、アプリケーションインストール状況にて、  
セキュリティパッチの更新確認が可能です。  
※ウィルス対策ソフトは別途購入です。



# 「業務効率」にもつながる・・・ ～その他のチェックポイント～

## Point 9 不正ソフトウェアの管理、使用禁止

ShareやWinny等、社内情報に危険を及ぼすソフトウェアは完全廃止しなければいけません。使用の禁止は勿論のこと、現在使用されているソフトウェアの情報を管理しておく必要があります。それは、安全管理措置の技術的なチェック項目にもあがっているこのポイントによるものです。

2.5 個人情報を取扱う情報システムに関する不正ソフトウェア対策  
チェック項目④  
個人情報にアクセスできる端末にファイル交換ソフトウェア(WinnyやShareなど)をインストールしていない。



なら、各パソコンのアプリケーションのインストール、アンインストール状況を表示  
また、各パソコンにインストールされているアプリケーションのバージョンを含む一覧表示  
また、動作を禁止したいアプリケーションの使用を禁止  
などの対策がとれます。

## Point 10 Webメール・掲示板書き込みの使用禁止

社内でのWebメール・掲示板書き込みは業務の効率を下げるだけでなく、証拠の残らない情報漏えいの発信源となってしまう恐れがあります。使用禁止を促す事に加え、使用状況の証拠をとる事も有効です。



なら、基本的なパソコンの操作履歴を管理します。  
・各パソコンの電源ON/OFF日時  
・アプリケーションの起動/終了日時  
・アプリケーション名  
・ファイル名(操作ウィンドウ名)を記録  
※i-FILTERといった商品にて使用禁止も可能です。

