連載（31）

使いこなして何ぼ!!のISO

…ＩＳＯコンサルティングの現場から…

第31回　今回もPマークコンサルの現場から…②

～安全管理措置についてPマーク審査ではこんなことが聞かれる～

平松　徹

1．あるPマーク審査の指摘

今、私のPマークのコンサル先A社がPマークの審査を受けています。そこで気がついたことなど含め、今回はPマーク審査について書いていきます。なんといっても認証取得コンサルティングは取って初めて意味あるものです。だから、審査に合格してもらうことがとても大事になります。

今Pマークの取得を考えていらっしゃる会社さんなんかも審査員がどのような審査をするか、けっこう気になるところですね。そこで今回は、現地審査で最もポイントになる「安全管理措置」のところをまず取り上げます。

A社について次のような指摘がありました。

- 「営業社員がノートパソコンを企業から持ち出し使っている」。
- しかし「①暗号化などの対策が講じられていない。②ノートパソコンの紛失、盗難などの対策がとられていない」。
- ということで「③持ち出しノートパソコンについてのリスクを認識し、安全対策を規定し、実施すること」。

安全管理措置の審査は、現地審査の中でも独立して実施されます。この指摘では「情報漏えい」ということがないような仕組みと実行を求めています。

安全管理措置については手順書を作って、仕組みを整備し、着実に実行する。A社も安全管理措置については手順書を作っているのですが、持ち出しノートパソコンのこの部分の規定が確かに抜けていました。さっそく具体的な措置について検討し、手順書を整備することになりました。

2．安全管理措置の分類

安全管理措置については、上記の指摘に限らず、大事なところですので、その審査について網羅的にふれます。参考にしてください。

以下は、Pマーク審査員をしている知人の話や日本規格協会から出版されている「個人情報保護マネジメントシステム実施のためのガイドライン」をもとにまとめました。

安全管理措置については、次のように分類されて考えられています。

1．物理的安全管理措置
①建物、室、マシン室、個人情報の取扱い場所などへの入退館(室)管理
②個人情報、個人情報を記録した媒体の盗難などの防止
③機器・装置の物理的な保護
2．技術的安全管理措置
①個人情報へのアクセス権限の管理
②不正ソフトウェア対策
③個人情報の移送・通信時の対策

経済産業省のガイドライン(個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン)では、他に「人的安全管理措置」と「組織的安全管理措置」がありますが、そちらはプライバシーマネジメントシステムの運用状況

表1　建物、室、マシン室、個人情報の取扱い場所などへの入退館(室)管理

	項目	審査質問の例	実施の具体例
1	入退館、入退室などの制限	・建物、室、マシン室、個人情報の取扱い場所などへの入退をどのように制限しているか	・従業員はセキュリティカードによる入退館、外部者は受付から内線電話による呼出し ・立ち入り可能エリアの分離 ・フロアー別入退室管理 ・社員証などによる識別管理
2	記録とその保管	・建物、室、マシン室、個人情報の取扱い場所への入退の記録はどうなっているか ・どのように保管され、またそれは定期的にチェックされているか	・最初の入室者と最終退室者チェックリスト ・入退館名簿 ・個人情報保護管理者が毎週末に確認

表2　個人情報を記録した媒体の盗難などの防止

	項目	審査質問の例	実施の具体例
1	施錠での管理	・個人情報を記録した媒体はどのように施錠保管され、管理されているか ・保管場所の鍵は特定者が管理しているか	・社屋の鍵、部屋の鍵、保管庫・キャビネット・ロッカーなどの鍵の配付管理 ・施錠管理者の規定類整備
2	個人情報媒体の廃棄の管理	・個人情報を記録した媒体(文書、記録類、USBメモリーなど)の廃棄は、再利用できない措置を講じているか	・シュレッダーによる裁断 ・組織指定の業者への依頼による廃棄 ・廃棄責任者を明確にする
3	携帯可能PCの管理(特に盗難防止)	・どのように管理されているか ・盗難防止措置が施されているか	・使用についての申請書管理 ・使用しないときに机の上などに放置しない ・鍵のあるキャビネットなどに保管 ・チェーンロックの使用 ・教育による周知徹底
4	CD、USBフラッシュメモリ等の外部記憶媒体の管理(盗難防止、紛失防止など)	・CD、USBフラッシュメモリなどの利用のルールはあるか ・どのように運用されているか	・机上、その他の場所に放置しない ・使用についての申請書管理 ・台帳管理 ・教育による周知徹底
5	PC操作上の情報漏えい防止	・個人情報を取扱うPCの操作で、情報漏えいがないように仕組みが整備されているか	・離席時のパスワード付きスクリーンセーバーの起動 ・個人情報閲覧についての操作マニュアルの取り扱いを注意する(机上に放置しないなど)

の審査で確認します。

3・物理的安全管理措置の入退館管理の審査で聞かれるのは

まず安全管理措置についてです。建物の入退館などの管理を**表1**にまとめました。

建物や各フロアー、各部屋への入退の管理は、セキュリティの入り口の部分ですから確実に管理できていないといけません。誰がどこに入ることができるかを明確にすることが基本です。それが誰にも分かるように識別管理することになります。

社員証を首から掛けることがよく行われています。中小企業の場合、社員証がなくても誰が社員か一目瞭然ですから必要ではないのではとも思われますが、外から見ると確実な管理ができている会社、しっかりとした会社との印象を与えますので、けっこう良いかもしれません。

4・盗難防止の措置については次のようなことが審査される

次は個人情報を記録した媒体の盗難など防止についてです。個人情報の入った文書や記録類、パソコン、USBフラッシュメモリーやCDなどが対象になります(**表2**参照)。

携帯用のパソコンが盗まれて騒ぎになることがよく新聞などで報道されます。もし盗難や紛失し

表3　機器・装置の物理的な保護

	項目	審査質問の例	実施の具体例
1	安全管理上の脅威	・盗難、破壊、破損などからの物理的な保護装置があるか	・金属の網の入った窓ガラスの設置 ・監視カメラの設置 ・記録媒体、文書類などは収納の仕方を工夫する（飛散、落下、移動など）
2	環境上の脅威	・漏水、火災、停電、地震などからの物理的な保護装置があるか	・免震、浸水、落下物などに対する対策 ・高温多湿、強い時期のある場所でのネットワーク機器の設置の禁止 ・転倒防止の措置 ・大事な書類などは防火金庫に保管
3	バックアップ	・個人情報のバックアップが実施されているか	・外付けハードディスクなどにバックアップ ・バックアップについての手順の整備 ・重要書類は耐火金庫に保管

たら大変なことになるということです。

説明責任ということが今盛んに言われます。何かあればそれをきちんと説明する責任があるということです。きちんと仕組みを作っていて確実に運用しているのにも関わらず事故が起きることもあります。状況をしっかりと説明すれば、罪は軽い。仕組みもなく、管理もされていないのであれば説明できず、ひたすら謝るばかりになります。これですと罪は重いですね。説明責任もまずは仕組みを作りしっかりと実行することが大切ということです。

企業の状況に応じて、盗まれたり、紛失したりしない仕組みを整備し、確実に運用することですね。教育による周知徹底も大事です。携帯パソコンやUSBメモリーなどは使用するについて申請書による管理も必要かもしれません。盗難や紛失を防ぐこと、よその企業に行って使用するときの留意点など明確にしておく必要もあります。うるさい会社などでは外部からのUSBメモリーなどは使用を禁止しているところもあります。そのあたりは従業員への教育も必要です。

Pマーク審査では電子データに関するものはかなり細かく聞かれます。「そこまでしないといけないの？」と感じることも多いと思います。もしものことがあったら企業の評判が下がるわけですから、手数が少しくらい余計にかかっても実行することが必要です。

5．地震など自然災害に対して機器類の保護もしっかりと実行しなければなりません

そして物理的安全措置の最後は機器類の保護の話です。ポイントをまとめると次のようになります。

> 個人情報取り扱い機器・装置について物理的に保護しているかどうかが審査される。
> ●安全管理上の脅威　→　盗難、破壊、破損などに対してどのように対処しているか
> ●環境上の脅威に　→　漏水、火災、停電、地震などに対してどのように対処しているか

これも**表3**にまとめました。

このあたりの仕組みができることはPマークを取得することで得することの一つです。防災について深く取り組んでいない会社が特に中小企業では多い。あらためて災害などが発生したらどうするかを検討し、仕組みを整備することが大切です。

バックアップが物理的措置に入ることは少し違和感があるかもしれません。ただ、災害や紛失、盗難などに備えて、個人情報をバックアップしておくことも個人情報システムの「可用性の確保」ということで重要です。可用性とはいつでも使うことができるということ。情報システムの脆弱性を取り除くことにつながります。

6．次は技術的安全管理措置のアクセス制限

次に技術的安全管理措置に行きます。まずアクセス制限です（**表4**参照）。

技術的安全管理措置については、Pマーク審査員はかなり細かく要求してきます。これは覚悟しておく必要があります。もともとPマークの基盤である「個人情報保護法」についての政府の基本

表4　個人情報へのアクセス権限の管理

	項目	審査質問の例	実施の具体例
1	アクセス制御の管理	・アクセス制限の仕組みがあるか ・確実に運用されているか	・職務分掌管理規定の整備 ・アクセス制限についての方針と手順の明確化、文書化など仕組みの整備 ・アクセス制御機構は、デフォルトの設定を残さない ・従業者に付与するアクセス権限は必要最小限 ・個人情報を保管している情報システムには、許可範囲を超えたアクセスができない ・生体認証
2	認証と識別情報（ID、パスワードなど）の管理	・認証と識別情報（ID、パスワードなど）の発行・更新・廃棄の、ルールはどうなっているか。実行されているか	・パスワードについての管理の仕組みの文書化 ・認証と識別情報（ID、パスワードなど）は、平文（ひらぶん）で記録しない ・識別情報（ID、パスワードなど）を、複数人で共用しない
3	アクセス記録	アクセス記録について管理されているか	・記録についての仕組みの整備 ・個人情報を保管している情報システムへのアクセスログが取得され、保管されている ・取得した記録が漏えい、滅失、毀損から適切に保護されている

方針を明確にした「個人情報の保護に関する基本方針」に次のようにあります。

個人情報の保護に関する基本方針

> **(1)個人情報保護法設定の背景**
>
> 近年、経済・社会の情報化の進展に伴い、官民を通じて、コンピュータやネットワークを利用して大量の個人情報が処理されている。こうした個人情報の取り扱いは、今後ますます拡大していくものと予想されるが、個人情報はその性質上いったん誤った取り扱いをされると、個人に取り返しのつかない被害を及ぼすおそれがある。
>
> 実際、事業者からの顧客情報等の大規模な流出や、個人情報の売買事件が多発し、社会問題化している。(平成16年4月2日　閣議決定)

実際に、マンションの売り込みや相場商品の勧誘で見ず知らずの会社から電話がかかってきて迷惑することが多いですね。電話を切りたいのですが、しつこく電話の向こうから迫ってきます。それも忙しいときに限ってかかってきます。前に「もう結構ですから」と何度か言ったら「けっこう、けっこうと俺は鶏じゃないぞ、ふざけるな……」との捨てぜりふを残してガチャンと電話を切られました。あんまりなので思わず笑っちゃいましたが……。

迷惑メールも本当に迷惑ですね。何とかして欲しい人も大勢いらっしゃると思います。そのような被害が増えているし、どのようなルートで個人情報が漏れたのかも分からないことが多い。手数やお金がかかってもそれぞれの会社が個人情報についてしっかりと管理しないといけません。

だから電子データの取り扱いは特に力を入れる必要があります。

特にパスワード管理をはじめとしたアクセス制限が重要です。「パスワードは平文で記録していないか、複数人で共用していないか」「アクセス制限機構はデフォルトの設定を残していないか」などはPマーク審査員の使う「チェックリスト」に実際に載っていますので、必ず聞かれる質問と心得てください。皆さんの会社はできていますか。

7．不正ソフトウェア対策

次に不正ソフトウェア対策です(**表5**参照)。

これらの不正ソフトウェアについての対策も確実に実行できていないといけません。ウィルスに感染すると、自社のみでなくインターネットを通じて周りに大きな迷惑がかかります。これも心して万全の対策を打っておく必要があります。

ほんの数日前なのですが、こんなことがありました。私の主催している中小企業診断士の研究会

表5　不正ソフトウェア対策

	項目	審査質問の例	実施の具体例
1	最新版管理	・ウィルス対策の管理はどのようにしているか	・個人情報を取扱う情報システムにはウィルス対策ソフトウェアが導入され、常に最新のパターンファイルが適用されている
2	セキュリティパッチの適用	・セキュリティ対策用修正ソフトウェアについてはどのようにしているか	・個人情報を取扱う情報システムのOS、アプリケーションなどにセキュリティ対策用修正ソフトウェア（セキュリティパッチ）を適用している
3	ファイル交換ソフトウェアの不使用	・ファイル交換ソフトウェアなどについてはどのように対処しているか	・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、Shareなど）をインストールしていない

表6　個人情報の移送・通信時の対策

	項目	審査質問の例	実施の具体例
1	移送･通信時の授受の記録	・個人情報を記録した媒体（記録媒体、紙）は、移送･通信時の授受の記録がとられているか	・電子媒体、紙媒体での記録管理の仕組みができている ・台帳で管理している
2	移送･通信時における紛失･盗難への対策	・移送時における紛失・盗難への対策が実施されているか	・媒体に保管されている個人情報の暗号化やパスワードロックなどが実行されている
3	ネットワークの管理	・盗聴される可能性のあるネットワークの管理はどうなっているか	・盗聴される可能性のあるネットワーク（インターネットや無線LANなど）で個人情報を送信する場合、個人情報の暗号化やパスワードロックなどを実施している

のメーリングリストにウィルス付きと思われるメールが送信されてきました。夜中の10時頃です。顧問先の環境ISOの最終審査が終って打ち合わせが済んで一杯やってほろ酔い気分の電車の中で、その事実が分かりました。びっくりして途中の上野駅で降りて、駅の中の喫茶店に入り、急いでそのメーリングリストに送信しました。「今ウィルス付きのメールが送られてきましたが、決して開かないようにお願いします」「もし開いてウィルスに感染しても平松は責任をおいません」との内容です。もちろん私もウィルス付きのメールは開かないでその場で削除しました。感染したときのことを考えるとこれはもう緊急事態！！。疲れていたので帰ってすぐにでも寝たかったのですが……。メーリングリストは便利ですが、セキュリティを確実にしないと本当に怖いですね。

8．最後が個人情報の移送･通信時の対策

最後が、個人情報の移送・通信時の対策です（**表6**参照）。

クレジット情報などは暗号化しての送信が当然と思いますが、一般の個人情報もそこまでする必要なのかと思うかもしれません。しかし、大量の個人情報のデータが簡単に送信受信できることを考えると、個人情報に関する重要なプロセスは暗号化を取り入れる必要があると思います。会社の事業内容や規模にもよりますが、履歴書情報など採用に関わるデータの送信であれば無理してでも暗号化の必要があります。漏れたら個人のプライバシーに関わりますし、漏れたことが分かると世間的にも大きな問題になりますので。

以上今回は、安全管理措置、それも物理的と技術的のところのみに限定して取り上げました。次回はその他の審査のところについてご紹介いたします。

筆　者
平松 徹（ひらまつ とおる）
(株)ソフィア　代表取締役
JRCA　ISO9001主任審査員
CEAR　ISO14001主任審査員
社会保険労務士、中小企業診断士、行政書士
TEL：047-308-2256　FAX：047-308-2257
E-mail：to@iso-hiramatsu.jp