プライバシーマーク現地審査
質問例と回答例

～マイナンバー法対応済

株式会社ハピネックス

目　次

＜3.4.3.2 安全管理措置＞

＜3.4.3.3 従業者の監督＞

＜3.4.3.4 委託先の監督＞

プライバシーマーク現地審査の概要

文書による審査が終了すると、現地審査が実施されます。

＜現地審査の目的＞

1. 個人情報保護マネジメントシステム（PMS）の通りに体制が整備され、運用しているか
2. 文書上の審査において生じた疑義の確認

＜現地審査の流れ＞

1. 審査員からの挨拶
   - リーダー審査員とサブの審査員、2 名体制

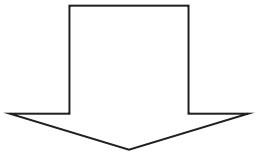
2. 代表者へのインタビュー
   - 個人情報に関する事故の有無確認
   - 事業内容/経営方針
   - プライバシーマーク申請のきっかけ
   - 個人情報保護方針とその周知方法
   - 個人情報保護管理者・監査責任者の任命
   - マネジメントレビュー、など

3. 運用状況の確認
   - 申請担当者、個人情報保護管理者、監査責任者等へのヒアリング
   - 個人情報を取り扱う業務の確認
   - 個人情報特定の手順
   - リスクの認識と処理
   - 教育・訓練
   - 監査
   - 委託契約・選定基準
   - 輸送／オンサイト委託／ネットワーク
   - 不正アプリケーション／ウィルス／リモートアクセス
   - 電話帳データ等本人の同意を取れてないものの利用・提供の有無
   - 本人からの要求に対する対応

4. 現場での実施状況の確認
   - 個人情報保護方針の周知状況
   - 物理的アクセス制御
   - 入口・マシン室・倉庫・書庫・金庫・引出し
   - 鍵管理
   - 論理的アクセス制御
   - クライアント／サーバ
   - 暗号化
   - 暗号鍵管理
   - バックアップ
   - 記録媒体の管理
   - 記録
   - 授受、破棄等の確認書類
   - 入退室、アクセスログ
   - 管理台帳
   - オンライン特有の処置
   - 個人情報保護方針の掲載
   - 収集時の SSL の使用
   - サービス、業務毎の“同意文言”
   - Cookie などのウェブバグの利用の有無
   - クロスサイトスクリプティング（CSS）などのセキュリティ対策

5. 文書上の審査において生じた疑義の確認

6. 総括
   - 口頭で講評、指摘事項等が説明される。
   - 後日、正式に「指摘事項報告書」が郵送される



現地審査で指摘された事項に対して改善を行い、「改善報告書」を提出。
「改善報告書」の内容が妥当と判断されれば、プライバシーマークが付与される。

＜プライバシーマーク申請の動機、課題＞

3.　プライバシーマークを取得しようと考えた動機は何ですか。	社長	
＜例＞ 当社は技術者のスキル情報を保有しており、当社の財産であると同時に、技術者本人にとっても非常に重要な情報です。この観点からも個人情報保護の仕組みを構築したいと考えていました。 また、得意先からも派遣従業員に対する個人情報保護の徹底した教育を要請されています。 こうした環境下、個人情報保護の仕組みを構築することは、企業の責任であり義務であると考えていました。 そこで、第三者認証であるプライバシーマークの取得を検討しました。プライバシーマークの取得は、安全な個人情報取扱の判断基準になります。 当社にとって、プライバシーマーク取得は、安全性を技術者や得意先に示すことができるこので大変意義があります。		
＜回答のポイント＞ ● 個人情報保護に対する企業責任 ● プライバシーマークの取得が安全な個人情報取扱の判断基準となっていること		
＜貴社の場合＞		

4.　プライバシーマークを取得するメリットについて、どうお考えですか。	社長	
＜例＞ プライバシーマークは、個人情報を適切に取り扱う事業者に与えられる第三者認証です。プライバシーマークの取得は、得意先や技術者などの利害関係者に安心感を与えます。得意先からも評価されるでしょう。そして、個人情報に関する社員の意識が向上することも大きなメリットです。		
＜回答のポイント＞ ● 利害関係者からの信頼の獲得 ● 個人情報に関する社員の意識向上		
＜貴社の場合＞		

5.　プライバシーマークを今後運用していくに当たり、どんな課題があるとお考えですか。	社長	
＜例＞ プライバシーマークの仕組みを構築し、運用を開始して、まだ数ヶ月です。全社員に 100%定着しているとは言いがたいのも事実です。今後も運用を継続し、必要な部分は改善し、より有効なマネジメントシステムにしたいと考えています。 そのためには、「人材の育成」が最も重要だと考えています。プライバシーマークのマネジメントシステムについて理解している人材を今後も育成したいと思います。		
＜回答のポイント＞ ● 継続的な改善 ● 人材育成		
＜貴社の場合＞		

3.2 個人情報保護方針

事業者の代表者は、個人情報保護の理念を明確にした上で、次の事項を含む個人情報保護方針を定めるとともに、これを実行し、かつ、維持しなければならない。

a）事業の内容および規模を考慮した適切な個人情報の取得、利用および提供に関すること（特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い（以下、“目的外利用”という。）を行わないこと及びそのための措置を講じることを含む。）。

b）個人情報の取扱いに関する法令、国が定める指針その他の規模を遵守すること。

c）個人情報の漏えい、滅失又はき損の防止及び是正に関すること。

d）苦情及び相談への対応に関すること。

e）個人情報保護マネジメントシステムの継続的改善に関すること。

f）代表者の氏名

事業者の代表者は、この方針を文書（電子的方式、磁気的方式など人の知覚によっては認識できない方式で作られる記録を含む。以下、同じ。）化し、従業者に周知させるとともに、一般の人が入手可能な措置を講じなければならない。

＜審査のポイント＞

- ■ 個人情報だけでなく、特定個人情報を含んだ保護方針となっていること。
- ■ 代表権を持つ者を代表者として表示していること。
- ■ 従業者及び一般の人が入手できるための具体的な手段を整えていること。
- ■ 分かりやすく目に付きやすい場所にリンクを表示していること。
- ■ 問合せ先を明示していること。
- ■ 公開している個人情報保護方針と規定文書としての個人情報保護方針が同一であること。

＜エビデンス＞

- ■ 公開している個人情報保護方針
- ■ 従業者が入手可能な措置
- ■ 登記事項証明書等
- ■ ウェブサイトのトップページ
- ■ 一般の人が入手可能な措置
- ■ 規定文書としての個人情報保護方針

12.　個人情報保護方針について、説明してください。	社長	
＜例＞ 当社の個人情報保護に関する公式文書であり、個人情報保護の理念と経営責任を明確にするため、別紙のように定めています。 社員に対しては、文書化した個人情報保護方針を総務部から各部門へ配布し、周知徹底しています。 社外の人には、ホームページで公開しています。そして、トップページから 1 クリックで個人情報保護方針のページに移動できるようにしています。また、問い合わせ窓口も明記しています。		
＜回答のポイント＞ ● 理念と経営責任 ● 従業員への周知徹底 ● 一般の人が入手可能な措置 ● トップページからのリンク		
＜貴社の場合＞		

13.　従業員に個人情報保護方針を周知したことを、どのように確認していますか。	社長	
＜例＞ 教育計画書に基づき、従業員に対し、教育を行っています。教育終了後、理解度テストを実施し、理解度を確認しています。		
＜回答のポイント＞ ● 従業員教育と理解度確認		
＜貴社の場合＞		

3.3.3 リスクなどの認識、分析及び対策

事業者は、3.3.1 によって特定した個人情報について、目的外利用を行わないため、必要な対策を講じる手順を確立し、かつ、維持しなければならない。事業者は、3.3.1 によって特定した個人情報について、その取扱いの各局面におけるリスク（個人情報の漏えい、滅失またはき損、関連する法令、国が定める指針その他の規範に対する違反、想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれ）を認識し、分析し、必要な対策を講じる手順を確立し、かつ、維持しなければならない。

＜審査のポイント＞

- リスクの認識・分析・対策を定めた手順に従い実施していること。
- 特定個人情報もリスクの認識・分析・対策の対象としていること。
- 個人情報を取り扱う業務の流れが明らかになっており、取扱いの局面におけるリスクを具体的に認識していること。
- 立案した安全対策や把握した残存リスクをリスク分析表等に反映させ、かつ運用面で確認できること。
- 認識したリスクと対策との関連付けが明確であること。明確でなければ見直しができない。
- 個人情報は、取得及び利用面での適正な取扱いも求められる。単に情報資産を守るという観点からのみのリスクの認識、分析及び対策となっていないこと。
- 個人情報の漏えい、滅失、毀損のほかに法令・国が定める指針等に対する違反なども必要に応じてリスクとして認識していること。
- 講じることとした対策は規定化していること。
- リスクの見直しを定期的及び随時実施していること。

＜エビデンス＞

- リスク分析表等、リスクの認識、分析及び対策を実施した記録
- リスクの認識、分析及び対策を実施した記録
- リスク分析表等、リスクの認識、分析及び対策を実施した記録と規定との対応
- リスク分析表等、リスクの認識、分析及び対策を実施した記録及びその更新履歴

19.　目的外利用が行われないよう、どのような対策をしていますか。		管理者
＜例＞ 部門長が個人情報の目的外利用が行われていないことを確認し、個人情報の適切な管理を実施しています。 また、個人情報の目的外利用を行われないよう、内部監査などを通じて個人情報の取り扱いが手順書通り行われているかを確認しています。		
＜回答のポイント＞ ● 日常の対策 ● 定期的な対策		
＜貴社の場合＞		

20.　リスク分析のやり方を説明してください。		管理者
＜例＞ 事務局が、「リスク分析表」を用いてリスク分析を行っています。 具体的には、ライフサイクルの各局面（取得・入力、移送・送信、利用・加工、委託、保管・バックアップ、消去・廃棄）におけるリスクを抽出し、それぞれの評価と対策を決定しました。リスク分析の結果は、社長の承認を得ています。 ＜手許に「リスク分析表」を用意しておく＞		
＜回答のポイント＞ ● 「リスク分析表」 ● ライフサイクル毎のリスク分析 ● リスク分析結果の承認		
＜貴社の場合＞		

21.　残存リスクをどのように管理していますか。		管理者
＜例＞ 安全対策や管理状態に問題があり、リスクの可能性が残る項目については、残存リスクとしました。残存リスクについては、社長の承認を得ることとし、どのような残存リスクが存在するかを、「社内教育」を通じて社員に認識させています。		
＜回答のポイント＞ ● 残存リスクの社長の承認		
＜貴社の場合＞		

22.　リスクへの対策を規程に反映していますか。		管理者
＜例＞ 実施した安全対策は、リスク分析表の関連規程欄に、実施した安全対策を、どの手順書に規定しているかを明確にしています。		
＜回答のポイント＞ ● リスク分析表の関連規程欄		
＜貴社の場合＞		

23.　リスクの見直しをしていますか。		管理者
＜例＞ 定期的な見直しは、年 1 回（4 月）に行っています。また、個人情報管理台帳が新たに作成された時及び見直しが行われたときは、リスクの分析を随時実施しています。		
＜回答のポイント＞ ● 定期的見直しと随時見直し		
＜貴社の場合＞		