現地審査では概ね以下のようなことを行います。

1. オープニングミーティング
- 審査員の紹介
- 秘密・個人情報保持の誓約
- 審査手順の説明

2. 代表者へのトップインタビュー
- 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
- 個人情報保護の目的について
- 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
- 代表者として認識しているリスク
- マネジメントレビュー

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
- 事業の概要
- 個人情報を取り扱う業務の確認
- 個人情報を特定する手順
- リスクアセスメント及びリスク対策
- 個人情報を取得、利用、本人に連絡又は接触する場合の措置、第三者に提供する場合の措置
- 委託時の措置（委託先選定基準、委託契約）
- 本人からの要求に対する対応
- 認識（教育）
- 運用の確認、内部監査
- 是正
- マネジメントレビュー

4. 文書審査結果の確認
- 文書審査で生じた疑義の確認

5. 現場での実施状況の確認
- 個人情報保護方針の周知状況
- 物理的安全管理措置
  - ○ 建物、室、サーバー室等の入退館（室）管理
  - ○ 盗難等の防止
  - ○ 機器・装置の物理的な保護
- 技術的安全管理措置
  - ○ アクセス時の識別と認証（アクセス認証、デフォルト設定の変更状況、ID、パスワード等の発行・更新・廃棄）
  - ○ アクセス制御、アクセス権限の管理、アクセスの記録
  - ○ 不正ソフトウェア対策（ウィルス対策ソフトウェア、セキュリティパッチ等）
  - ○ 移送・通信時の対策(授受確認、取得時・移送時の暗号化、クロスサイトスクリプティングやSQLインジェクションなどへの対策）
  - ○ 情報システムの動作確認時の対策

6. クロージングミーティング
・ 現地審査での総評
・ 指摘事項の報告
・ 今後の手続きの説明