こうすれば

Pマークが取得出来ます

ジャグラは印刷業界のプライバシーマーク付与認定指定機関（審査機関）です

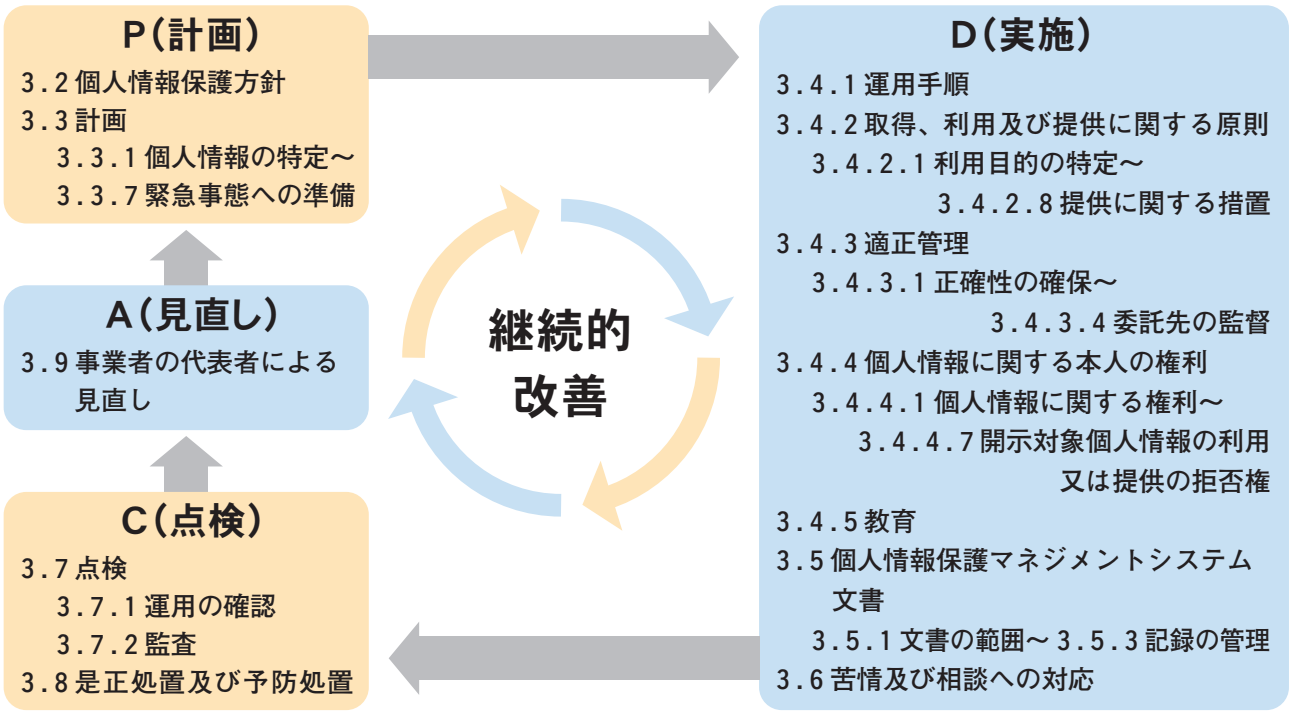
プライバシーマークを取得するには、「個人情報保護マネジメントシステム－要求事項」JIS　Q　15001-2006に準じた個人情報保護マネジメントシステム（略称：PMS）を構築し、運用し、維持した上で、審査機関の審査を受けなければなりません。

個人情報保護マネジメントシステムは、計画（PLAN）、実施・運用（DO）、点検・内部監査（CHECK）、見直し（ACT）を継続的にするPDCAサイクルを機能させる必要があります。

以下に、個人情報保護マネジメントシステムの構築について解説します。

プライバシーマークでは、JIS Q 15001-2006が個人情報保護マネジメントシステムとあるように、マネジメントシステムとして機能させることを要求しています。すなわち、PDCAサイクルを機能させなければなりません。JIS Q 15001-2006におけるPDCAを個々に見ていきましょう。

JIS Q 15001-2006におけるPDCAサイクル



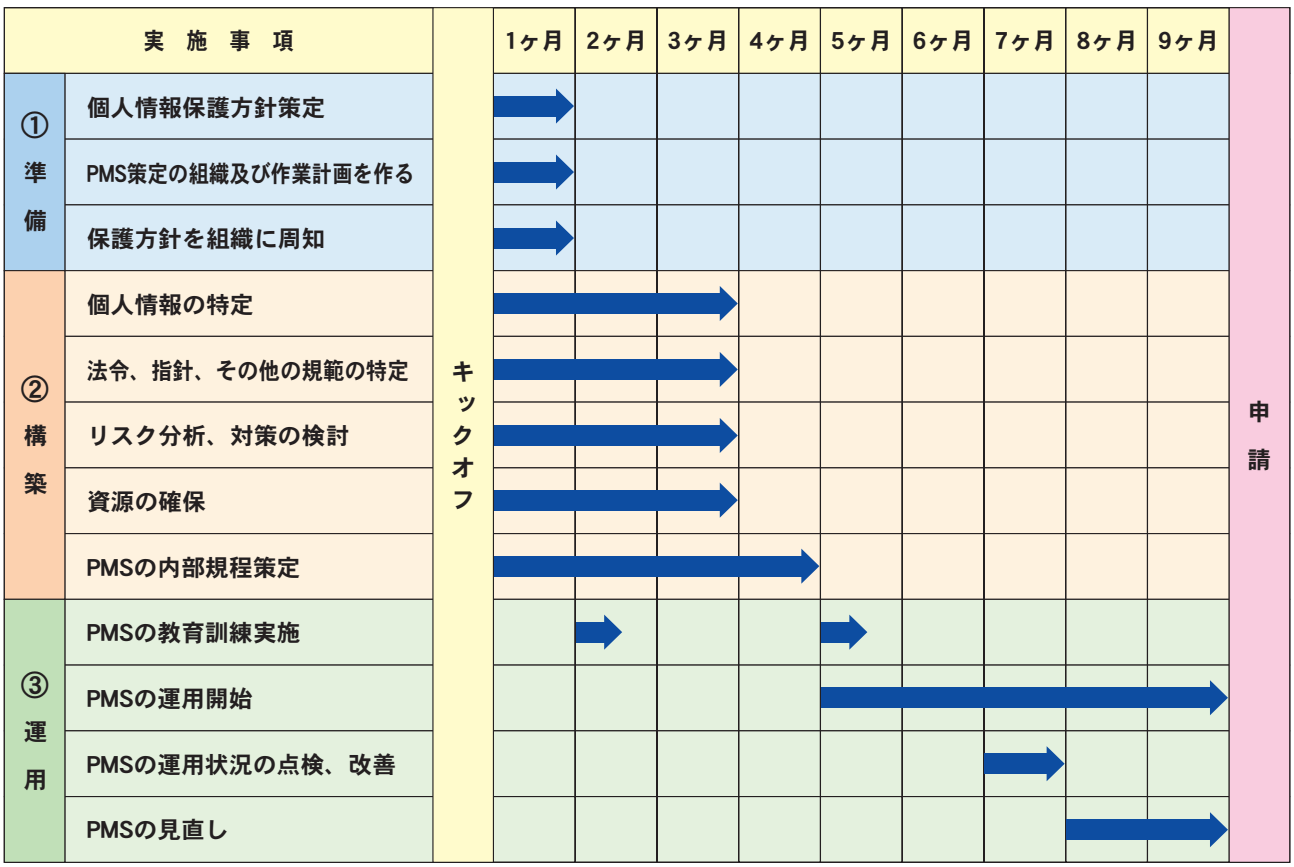
※財団法人日本情報処理開発協会の資料をもとに作成

P（計画）	・3.2 個人情報保護方針を策定し、実行します。 ・3.3.1 個人情報の特定では、自社で取り扱う個人情報を特定します。 ・3.3.2 法令、国、地方自治体が定める指針その他の規範など、自社として参照すべき規範などを特定します。 ・3.3.3 リスク分析では、3.3.1で特定した個人情報のリスク分析をします。 ・3.3.4 資源、役割、責任及び権限では、代表者はPMSを運用するための資源を用意し、その中での役割、責任、権限を明確にします。 ・3.3.5 内部規程は、個人情報保護マネジメントシステムを運用するための内部規程を準備します。社内に規定がある場合は、それらの規定の準用もできます。 ・3.3.6 教育や監査について計画を立案して実施します。この際、代表者の承認を得て、実施されたあとは報告書を作成し、代表者に報告します。 プライバシーマーク活動についての年間計画もあると便利です。 ・3.3.7 緊急事態への準備では、事故等が発生した場合の手順を明確にしておきます。
D（実施）	・3.4.1 実施及び運用する手順を決めて下さい。 ・3.4.2.1 利用目的を特定する際は、できるだけ具体的に利用目的を特定し、利用の際はその範囲内で利用します。 ・3.4.2.2 個人情報は適正な方法により取得します。 ・3.4.2.3 機微情報は原則として取得、利用、提供しません。 ・3.4.2.4 本人より直接書面にて個人情報を取得する場合は、書面にて8項目を通知して同意を得て取得します。 ・3.4.2.5「本人より直接書面」以外の方法で取得する場合は、利用目的をウェブなどで公表します。 ・3.4.2.6 利用目的外の利用は原則不可。利用目的外の利用をすることがある場合は、その具体的な手順を決めておき、その手順に基づいてします。 ・3.4.2.7 除外規定以外で、本人にアクセスすることがある場合は、その具体的な手順を決めておき、その手順に基づいてします。 ・3.4.2.8 除外規定以外で、第三者に個人情報を提供することがある場合は、その具体的な手順を決めておき、その手順に基づいてします。

D（実施）	・3.4.3.1	取り扱う個人情報は正確性を確保します。
	・3.4.3.2	取り扱う個人情報に応じた安全管理措置を講じます。リスク分析の結果を反映すると良いでしょう。
	・3.4.3.3	個人情報を取り扱う従業者の監督をします。誓約書の取得は一つの対策です。
	・3.4.3.4	個人情報を取り扱う委託先の監督をします。委託先を評価して契約を締結するほか、個人情報の取扱状況を報告してもらう等の方策があります。
	・3.4.4	本人の権利を保護するため、開示請求（訂正・追加・削除、拒否、利用目的の通知を含む）に対応する窓口を設置し、請求があったら対応します。
	・3.4.5	最低限、年１回、全従業者に教育をします。個人情報の取扱状況に応じて教育のレベルを変えることは可能です。
	・3.5	文書の範囲、記録の範囲を明確にして管理します。
	・3.6	本人からの苦情、相談を受け付ける窓口を設置し、対応します。
C（点検）	・3.7.1	各部門などで、日常点検（月次点検など）をして、チェックします。
	・3.7.2	内部監査で、運用できているかどうかチェックします。
	・3.8	不適合があった場合は、是正の手順で改善します
A（見直し）	・3.9	事業者の代表者による見直しで、全体的な見直しを含めて検討します。

PMS策定・運用のスケジュール

PMS策定の作業計画の例 （注）実施事項の期間はあくまでも例です



※財団法人日本情報処理開発協会の資料をもとに作成

① 準　備

「個人情報保護方針を策定する」「PMS策定の組織及び作業計画を作る」「保護方針を組織に周知する」

・個人情報保護方針＝個人情報保護方針は定めるだけでなく、それを組織内外に周知します。周知する方法は、原本と同じものを、ウェブに掲載する、社内に掲示する等の方法があります。

② 構　築

「個人情報の特定」「法令、指針、その他の規範」「リスク分析、対策の検討」「資源の確保」「PMSの内部規程策定」

・個人情報の特定では、自社で取り扱う個人情報を特定します。主に（印刷や発送、データ処理等で）受託して預かる個人情報と従業員より預かる個人情報のほか、PMSを運用する中で発生する個人情報も特定します。

・法令、国が定める指針その他の規範では、個人情報保護法、事業分野のガイドライン（印刷の場合は経済産業省）、雇用管理の場合のガイドライン（厚生労働省）のほか、印刷業界のガイドライン等を特定し、参照します。官公庁より個人情報を含む物件を受注している場合は条例も特定します。ウェブで受注している場合は特定商取引法、メルマガ等を発行している場合は特定電子メール法も必須です。

・リスク分析では、「個人情報ごとに（グルーピング可）」「取り扱う局面ごとに」「具体的なリスクを洗い出し」てリスク分析をする必要があります。洗い出されたリスクに応じた対応策を検討し、講じることにした安全対策は成文化し（どの規定に反映したか）、それでも残るリスクは残存リスクとして管理する必要があります。（次頁参照）

・PMSを実行するための資源を用意し、役割、責任及び権限を明確にします。

・個人情報保護マネジメントシステムを運用するための内部規程を準備します。社内に規定がある場合は、それらの規定の準用もできます。

③ 運　用

「PMSの教育訓練の実施」「PMSの運用開始」「PMSの運用状況の点検、改善」「PMSの見直し」

・PMSを運用する際には、最初に自社で規定した個人情報の取扱ルールを教育し、それから運用します。

・教育はそのほかに、最低限、年１回、全従業者に教育をします。個人情報の取扱状況に応じて教育のレベルを変えることは可能です。

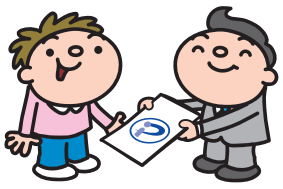
・運用を開始したら、運用状況がどうか自主点検、内部監査します。不適合があった場合は、是正をします。

・その他、PMSを全体的に見直すことを含めた代表者による見直しを実施します。

以上、ひととおり、PMSを運用してから、ジャグラに申請をして下さい。

申請

ジャグラあて、プライバシーマークの新規申請します。



申請以後

申請後、おおむね1ヶ月後に現地審査をします。

現地審査後、不適合があれば3ヶ月以内に是正（改善）を実施します。

プライバシーマーク認定取得

その後、是正が完了するとジャグラ審査会でPマークを認定（通常現地審査後、3ヶ月～6ヶ月）

→ジャグラよりJIPDECあて連絡

JIPDEC手続（Pマーク使用料＋契約書）終了後、プライバシーマーク交付

印刷業のリスクの洗い出しの例

以下に印刷会社における具体的なリスクを例示します。（これがリスクの全てではありませんので、各社でもリスクの洗い出しが必要です）

局　面	ケース	リスク	対　策（規程）	残存リスク
取得	手渡し	原稿紛失	授受記録（○○規程第○条） 営業カバンにしまう（○○規程第○条）	ひったくり
	メール	漏えい	ファイルの暗号化、またはPW設定を依頼する	
	宅配便	受領後の放置	管理ゾーンでの保管（○○規程第○条）	
	FAX	放置	受信後、担当者に渡す（○○規程第○条）	
	ウェブでの取得(ある場合)	漏えい	暗号化（SSL）する（○○規程第○条）	
移送	社用車で 顧客→自社	車上荒らし	不要な立ち寄り禁止（○○規程第○条） やむを得ない立ち寄りの際は、カバンに入れて携行する。車内放置禁止（○○規程第○条）	
	委託先への移送	原稿(媒体)紛失	授受記録（○○規程第○条）	盗難
	委託先からの移送	原稿、成果物紛失	授受記録（○○規程第○条） 原稿またはデータ、中間生成物の処理の報告を受ける。(○○規程第○条）	
	校正のやりとり	原稿紛失	不要な立ち寄り禁止（○○規程第○条） やむを得ない立ち寄りの際は、カバンに入れて携行する。車内放置禁止（○○規程第○条） 授受記録（○○規程第○条）	
	社用車で納品	車上荒らし 成果物の紛失	不要な立ち寄り禁止（○○規程第○条） やむを得ない立ち寄りの際は、カバンに入れて携行する。車内放置禁止（○○規程第○条） 授受記録（○○規程第○条）	トラックの荷くずれ
利用	各種印刷	不正アクセス (直接関係のない者のアクセス アクセス権限のない者のアクセス)	PCやサーバーへのアクセス制限をする。 （○○規程第○条） アクセスログをチェックする。 （○○規程第○条）	
加工	各種印刷	入力間違い 加工間違い	入力者の制限（○○規程第○条） 内校をする（○○規程第○条） チェックをする（○○規程第○条）	
保管	データ、外部媒体、成果物	盗難	施錠保管（○○規程第○条）	
	データ保管	不正アクセス (直接関係のない者のアクセス アクセス権限のない者のアクセス)	PCやサーバーへのアクセス制限をする。 （○○規程第○条） アクセスログをチェックする。 （○○規程第○条）	

保管	外部媒体、成果物保管	保管されていた個人情報がなくなっていることに気づかない	個別管理（○○規程第○条）	
	成果物保管	見本として、発注者の同意を得ずに、他の発注者に見せる	目的外利用の禁止（○○規程第○条）	
委託	委託先からの漏えいなどの事故		評価し、合格した委託先のみに発注する。（○○規程第○条） 契約を締結する。（○○規程第○条） 個人情報の取扱状況の報告を受ける（○○規程第○条）	
廃棄	廃棄物からの漏えい	紙	シュレッダー処理（○○規程第○条）	
		外部媒体	物理的破壊（○○規程第○条）	
		HDD	物理的破壊（○○規程第○条）	
		ヤレ紙、廃版	契約回収業者で廃棄（○○規程第○条）	
返却	社用車で納品	車上荒らし原稿の紛失	不要な立ち寄り禁止（○○規程第○条） やむを得ない立ち寄りの際は、カバンに入れて携行する。社内放置禁止（○○規程第○条） 授受記録（○○規程第○条）	
発送	宅配便	DMの紛失	授受記録（○○規程第○条）	
	郵送	DMの紛失	DMの紛失（○○規程第○条）	
その他	携帯電話	紛失	携帯電話の利用ルール	

リスク分析をする際には、以下のリスクについても考慮しながら進めるとよいでしょう。

※不正アクセス：第３者＝天変地異、部外者（ハッカー）、第２者＝提携会社、グループ企業、外注先（製本、発送、データ入力業者）、情報主体へのなりすまし、第１者＝社員、パート、派遣（いわゆる内部犯）
※コンピュータのリスク：盗難（ノート型）、容量オーバー、誤操作、システム（バージョンアップ）、ID／PW、クッキー、スクリーンセーバー、作業データのバックアップ・消し忘れ、通信経路上の盗聴、サーバー管理
※紙・媒体リスク：盗難、紛失、劣化、裏面使用（14001との兼ね合い）、磁気、FD等のフォーマット、FDの再利用、シュレッダーの利用
※Web（LAN）サーバのリスク：不特定多数のアクセス、24時間・365日稼働、バックアップ、ファイアウォールでは防げない事項、認証情報（ID／PW）の不正利用、単純なアクセスミス、アクセス権限、クロスサイトスクリプティング
※鍵の管理：建物、部屋、金庫、書庫、マシンルーム、ラック等の施錠→合鍵管理、入退管理（最初と最後）、その記録の確認
※データの管理：データベースの管理、暗号化（SSL）、記録（ログ）、を取る。管理者用PW（サーバ、ルータ、ファイアウォール…）、社員のID／PWの180日以内の強制変更、暗号キー管理、無線LANの暗号化
※輸送・受け渡し、委託時：授受の記録、受領の確認、委託先の評価、チェック、委託先の業務フローの確認

また、携帯電話の管理ルールの成文化やウェブで受注をしている場合などのSQLインジェクション攻撃への対応、また決済をしている場合などのクロスサイトスクリプティングの対応なども必要となっています。

そのほかにも、PCやサーバーなどの情報システムのリスク分析、建物などのリスク分析も実施すると自社で必要な安全対策が見えてきます。

JaGra
社団法人
日本グラフィックサービス工業会
the Japan Graphic services industry association JaGra
【TEL】03-3667-2271　【FAX】03-3661-9006
〒103-0001　東京都中央区日本橋小伝馬町7-16ニッケイビル