プライバシーマークのご提案

～今だからこそ、社員と本気で取り組む情報セキュリティ対策～

『プライバシーマーク』とは…

個人情報を適切に管理していることを証明する第三者認証制度

JIS Q 15001規格に基づく個人情報保護に関する認証制度であり、JIS規格とJIPDECの示す審査基準により審査が行われます。

ISO国際規格によるマネジメントシステム認証制度とは異なり、個人情報保護のための具体的な管理策の実施に特化した取り組みが求められるのが特徴です。

1. 個人情報保護体制の必要性

■ 個人情報漏えいの被害件数は、年々増加傾向にあります

2023年には147社(2022年は120社）の上場企業及びその子会社での個人情報の漏えい事件や紛失事故が発生しました。
これらの事件・事故で漏えいした個人情報の数は前年の約7倍の4,090万人8,718人分で、2023年は紛失事故件数と情報漏えい人数が過去最多を更新しています。
かと言って、個人情報漏えい対策として何から実施したらいいのかわからない場合、認証マーク取得を利用する形で体制を整えていきましょう。

■ ユーザーへの影響

適切な情報セキュリティ管理体制を構築し、運用していることは、信頼性の向上、情報漏えいリスクの軽減、従業員の意識向上などに
寄与します。企業が情報漏えいを引き起こしてしまった場合、
信用問題に関わってくることがほとんどです。

近年は人命に係わる詐欺被害の情報元となる個人情報の
名寄せは巧妙化しており、一層企業における個人情報保護に
関する従業員教育の重要性が叫ばれています。

2. プライバシーマークの変遷

■　個人情報保護を示すシンボル

1980年　「OECDの8原則」プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告

1998年4月1日　通商産業省（現在の経済産業省）の指導により「プライバシーマーク制度」開始

1999年　「JIS Q 15001:個人情報保護に関するコンプライアンス・プログラムの要求事項」制定

2003年5月　個人情報保護法 公布

2005年4月　個人情報保護法 全面施行

2006年4月　「JIS Q 15001:2006」改訂

2017年　「JIS Q 15001:2017」改訂

構築・運用指針（改定版）に基づいた申請の受付は、2024年10月1日より開始。

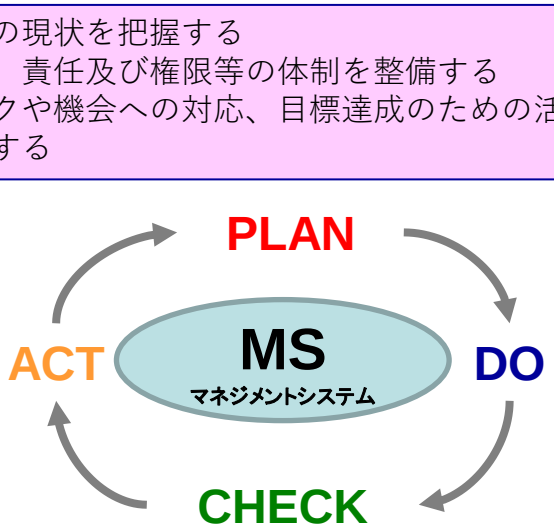
3.『マネジメントシステム』とは

■『マネジメントシステム』

日本情報経済社会推進協会（JIPDEC)が付与するプライバシーマークを取得するために必要な要件を満たす必要があります。個人情報保護方針の策定、個人情報の適切な管理、リスク評価と対策、教育と訓練、監査と見直し問い合わせ・苦情対応、事故対応、これらの要素を含むPDCAサイクルに基づいて構築され、継続的な改善が求められます。

■『マネジメントシステム』の運用

マネジメントシステムの『仕組み』は、下図の構造を採用しています。決めた活動計画を運用し、見直し、改善していく『PDCA』に基づく運用を行い、
レベルアップを行うことが求められています。



- 会社の現状を把握する
- 役割、責任及び権限等の体制を整備する
- リスクや機会への対応、目標達成のための活動を計画する

- 人、物、情報等の資源を管理する
- 教育・訓練の実施、意識向上によって人のレベルアップを行う
- ルールの明確化、活動の確実化のための文書・記録を管理する
- 日常業務において決めた活動計画を実践する

- 実践した活動を監視・測定（点検）する

- 監視・測定（点検）によって得られた情報をもとに現状・体制・活動計画の見直し、改善を行う

4.『プライバシーマーク』で取組むべきポイント

■個人情報保護管理体制の構築
個人情報の管理責任者を明確にし、組織全体での責任体制を確立させること。
個人情報保護方針を策定し、全従業員に周知させる必要があります。

■リスク評価と対策
個人情報に関連するリスクを評価し、それに対する適切な管理策を講じます。
定期的なリスク評価と見直しも行います。

■個人情報の安全管理措置
組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置の徹底させます。

■従業員の教育と啓発
従業員を対象に定期的な個人情報保護に関する教育・訓練を実施します。
意識向上を図り、適切な取扱いを徹底します。

■内部監査と改善
定期的な内部監査を実施し、PDCAを回し評価し、必要に応じて改善を行うことが重要です。

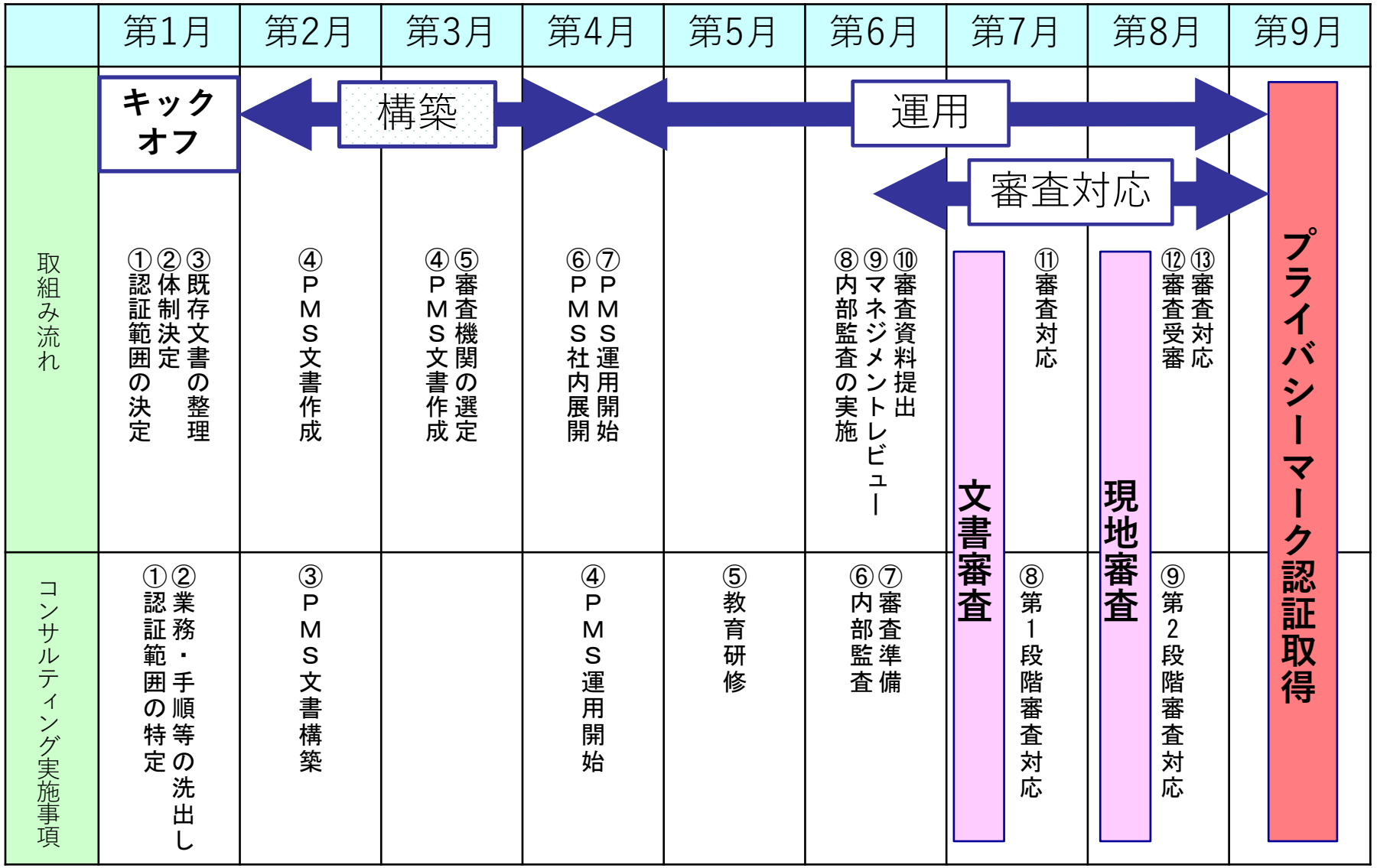
5. 内部監査員の役割

■ リスク及び機会

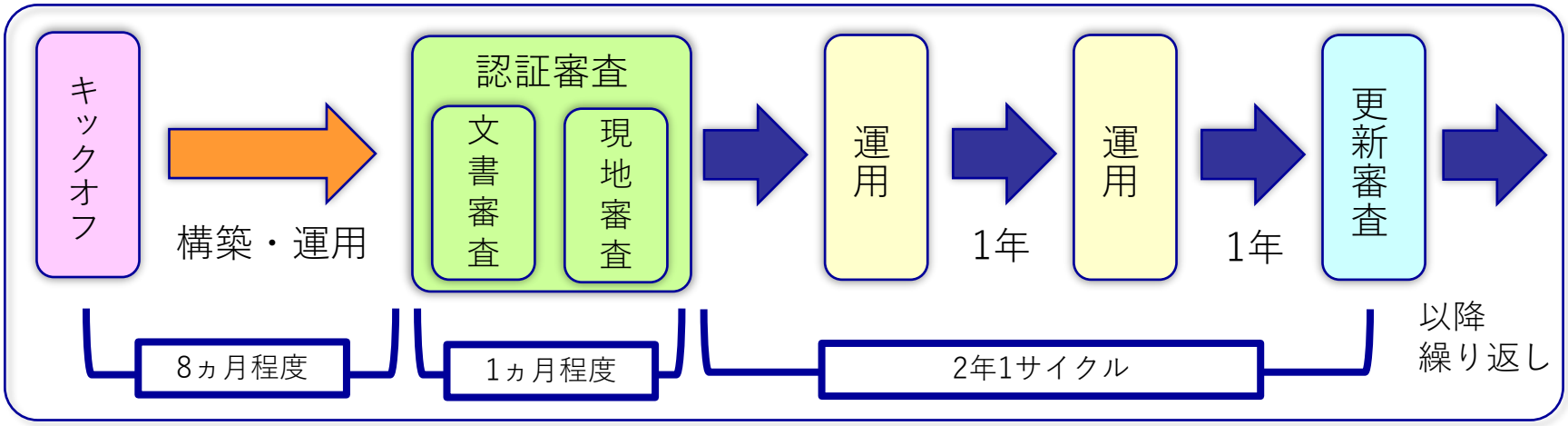
【建設業におけるリスク及び機会の例】

外部の課題 内部の課題	利害関係者 ニーズ及び期待	リスク及び機会	取組みの計画	ISMSへの展開 有効性評価の方法
サイバー攻撃の高度化と多様化への対策（外部の課題）	従業員・顧客・取引先・規制当局（利害関係者）	ランサムウェアやフィッシング攻撃によってシステムが停止したり、データが暗号化される。（リスク）	工程の進捗管理を徹底する。 バックアップ体制を整える。	インシデントの分析と対応を強化する
法規制やコンプライアンスの変化への対応（外部の課題）	データ保護とプライベートの保護（ニーズ）	従業員や契約社員による故意または過失による情報漏えい。（リスク）	定期的な教育の実施と教育内容のクオリティの更新をする。	セキュリティ教育と訓練の実施
従業員の意識と教育（内部の課題）	業務の継続性の信頼性の向上（期待）	AIや機械学習を活用した新しいセキュリティ技術の導入により、脅威の早期検知、早期対応能力が向上する（機会）	クラウドサービス、ソフトの活用を積極的に整える。	脆弱性評価と ペネトレーションテストの実施
リソースと予算の確保（内部の課題）	コスト削減と効率化（期待）	定期的なセキュリティ教育を実施することで、従業員の意識やスキルが向上し、内部からの脅威を減少させる（機会）	—	認証取得 継続的な「改善プロセスの導入

6. 認証取得までの流れと活動



7. 審査



《**認証審査**》
プライバシーマークを取得するための審査です。構築したマネジメントシステムがプライバシーマークの要求事項に適合していること確認する『文書審査』と構築したマネジメントシステムと実態が適合していることを確認する『現地審査』で構成されます。（有効期間2年）

《**運用**》
マネジメントシステムを運用維持するため1年ごと自社にて記録の更新確認、是正改善を繰り返します。

《**更新審査**》
認証審査と同様の審査を行います。