202412版

ISO 27001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～

『ISO 27001』とは…

会社の情報セキュリティを体制化し
自社情報を守るための仕組みです。

情報セキュリティマネジメントに関するISO27001は、
機密性、完全性、および可用性の3つの要素を維持しながら、
機密情報を守り、漏えいを防止することを目的としています。

ISOは、人材と組織（会社）を成長させ、
経営のステージアップ（成功）に導く取組みです。

1. 情報セキュリティ管理体制の必要性

■ 近年の情報セキュリティを巡る社会的状況

警視庁が発表したデータによると、情報漏えい件数は近年増加傾向にあります。
主なサイバー事案の検挙状況の分析によると、
情報漏えいの原因となる媒体としては、「社内システム・サーバー」が71.4%を占め、次いで「パソコン」や「書類・紙媒体」が続いています 。
これらのデータは、企業のセキュリティ対策の重要性と、従業員の教育や内部監査の必要性を強調しています。

警視庁統計資料(R4)

■ 事業者による漏えい時のリスクの軽減

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。そのため、
業種問わずISO27001 認証の取得企業数は増加しています。
取得企業数の推移：2002年には約140社だった取得企業数は
2015年には約4,600社、そして2023年4月現在には
約7,300社と、約20年間で50倍以上となっております。

2. 事業の課題を特定する

■ 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

3. ISO 27001の変遷

■　時代が求める規格

ISO 27001は、情報セキュリティ管理の重要性が高まる中、組織が情報資産を保護するための包括的な管理システムを確立する必要性から生まれました。

1990年代後半、インターネットの普及と情報技術の進展に伴い、情報漏洩やサイバー攻撃のリスクが増大。これに対応して、英国規格BS 7799が制定され、後に国際標準化機構（ISO）によってISO 27001として国際規格化されました。

この規格は、情報セキュリティの管理手法とベストプラクティスを提供し、企業が　リスクを適切に管理し、信頼性を高めることを目的としています。

年	内容	目的	表題
2005	初版発行	情報セキュリティ管理	情報セキュリティ、 サイバーセキュリティおよび プライバシー保護 ▪ 情報セキュリティ管理システム ▪ 要求事項
2013	大幅改訂		
2022	最新改訂		

2025年10月31日までに2022年版への移行が必要

4.『マネジメントシステム』とは

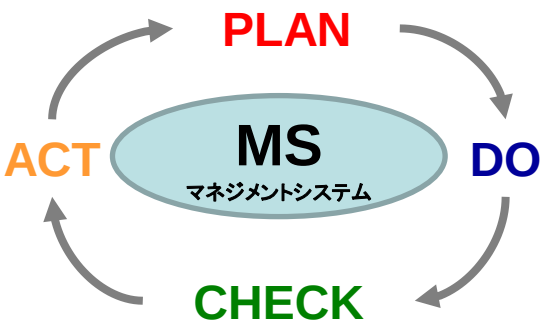
■『マネジメントシステム』

品質管理や環境保護、食品安全等の各分野のISO規格の要求事項に従って会社を運営するためのルールを作り（「規定」、「手順」等）、そのルールを運用するための役割、責任及び権限の体制を整えるものです。各分野のISO規格の目的（目標）を達成するために組織を指揮・管理するための『仕組み』がマネジメントシステムであります。

■『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

5.『ISO 27001』で取組むべきポイント

■**リスクアセスメントの実施**（ISO規格6.1.2）
情報セキュリティリスクを特定し、評価し、適切な対策を講じるプロセスを確立することが重要です。

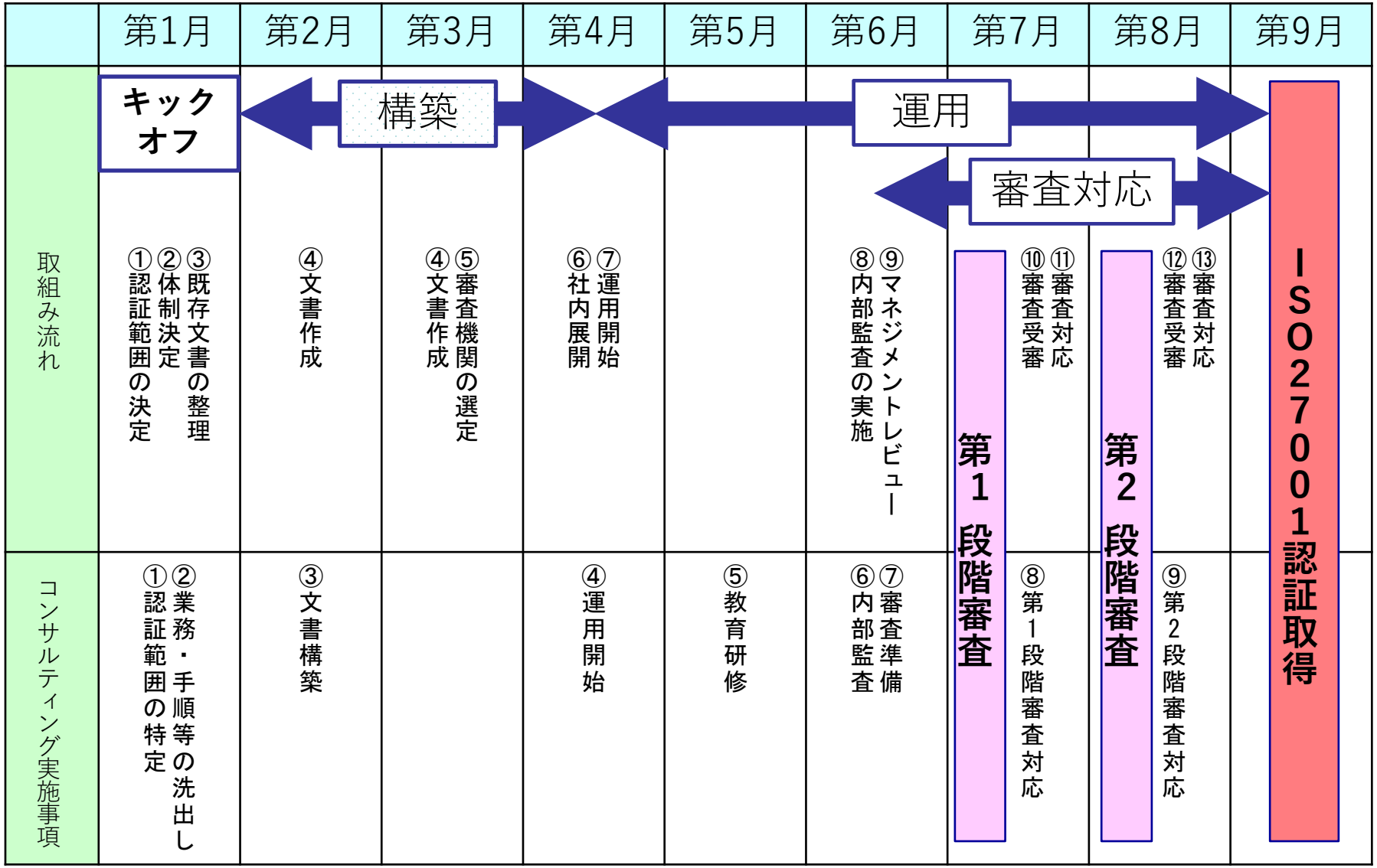
■**ISMS（情報セキュリティ管理システム）の範囲設定**（ISO規格4.3）
ISMSの適用範囲を明確に定義し、管理する情報資産やプロセスを特定することが必要です。

■**情報セキュリティ方針の策定**（ISO規格5.2）
組織の情報セキュリティに関する方針を策定し、全従業員に周知徹底することが求められます。

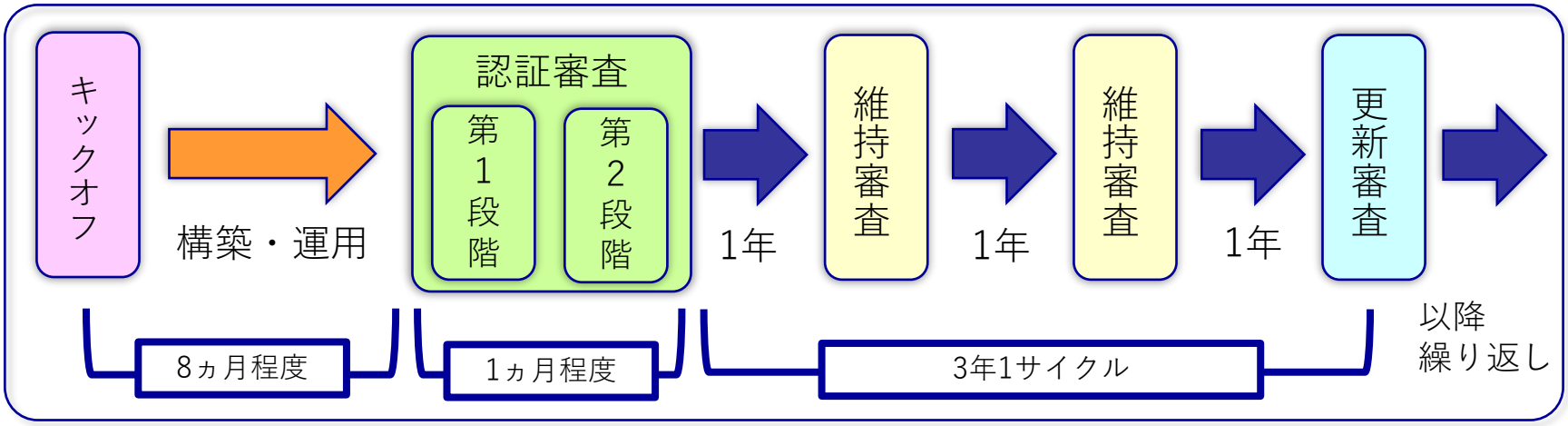
■**セキュリティ対策の実装**
（ISO規格6.1.3）（付属書A管理策）
リスクに応じた適切なセキュリティ対策を実装し、維持することが必要です。

■**内部監査と改善**（ISO規格9.2、10.1）
定期的な内部監査を実施し、ISMSの有効性を評価し、必要に応じて改善を行うことが重要です。

6. 認証取得までの流れと活動



7. 審査



《認証審査》
ISO認証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ISO規格の要求事項に適合していること確認する『第１段階』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『第２段階』で構成されます。（有効期間3年）

《維持審査》
ISO認証を維持するために1年または半年に1回、マネジメントシステムの運用状況を確認する審査です。一般的には1年に1回の維持審査を受けます。

《更新審査》
ISO認証を更新するための審査です。認証審査(第２段階)と同様の審査を行います。