ISO27001：2022
ISMS内部監査員通信講座

ISO/IEC27001:2022
ISMS内部監査員研修テキスト①
～監査手順編～

ISOマネジメント研究所
established in 2001

よくある内部監査の課題

課題１	毎年、同じチェックリスト（同じ質問）
課題２	内部監査への積極的関与が乏しい
課題３	形式的で、実用的でない（審査のためのもの）
課題４	あら探しになっている
課題５	質問が抽象的でわかりにくい
課題６	文書と記録ばかり求める
課題７	不適合が出ず、結果はいつも同じ
課題８	適切なやり方がわからない
課題９	役に立っていない

監査員に必要な知識及び技量

項　目	内　　容
監査の原則、プロセス及び方法	重要事項を優先し、重点的に取り組む。有効にコミュケーションを取る。プロセスを最初から最後まで監査できる。監査活動及び監査所見を文書化し、報告書を作成する。
ISO規格要求事項及び基準文書	ISO規格要求事項及び関連文書を理解している。それらの重要性や優先順位を理解している。
組織及び組織の状況	マネジメントシステムに影響を及ぼす、関連する外部・内部の課題、関連する利害関係者のニーズ及び期待を理解している。
適用される法令・規制要求	適用される法令・規制要求事項を理解している。

参照：JIS Q19011：2019　マネジメントシステム監査のための指針

役に立つ内部監査とは？

■技術部門：セキュリティリテラシーの向上

■営業部門：情報活用の効率化

■経営層：情報漏えいの未然防止

■運用面：形式的にならずに、機能する

“役に立つとは、目的実現に対する貢献度が高いこと”

内部監査は、〇〇の役に立つ？！

内部監査成功の条件

× 審査のための内部監査

○ 会社のための内部監査

そもそも内部監査では何をみる？

・ISMSが、以下の状況にあるか否かに関する情報を提供するために、あらかじめ定めた間隔で内部監査を実施すること

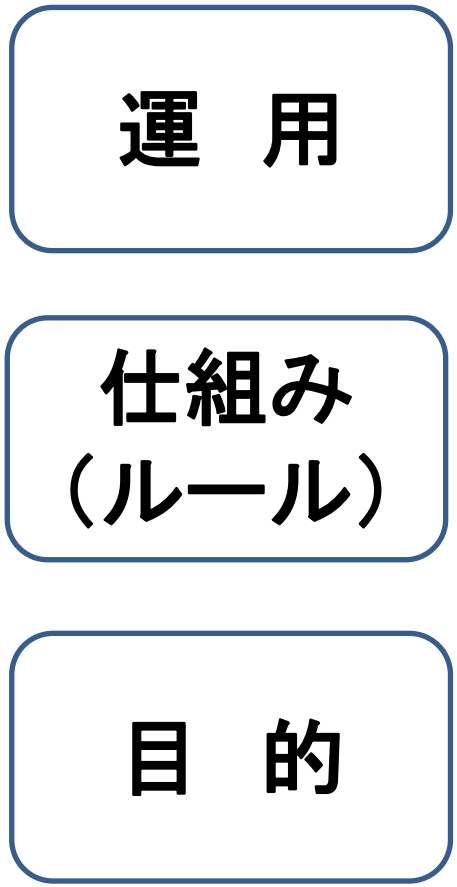
①以下の事項に*適合している*

1）ISMSに関して、組織自体が規定した要求事項

2）ISO27001:2022の要求事項

②*有効に実施され、維持されている*

内部監査の目線



STEP1

仕組み通りの運用をしているか？（適合性）

STEP2

運用結果は目的を達成できているか？（有効性）

適合性と有効性の内部監査の例

他人によるのぞき見を防止するために、PCの操作がなかった場合、20分間以内にスクリーンセーバーを起動させていた。

■ 適合性の監査

マニュアルに「20分間以内にスクリーンセーバーを起動させること」が記載されていることを確認して、その通りに運用しているかどうかを確認して、「適合」「不適合」を判断した。

■ 有効性の監査

マニュアルで定められた「20分間以内」という基準が適切なのか、リスクはないのか、状況についての聞き取りや、基準の有効性や根拠について質問した。

適合性監査と有効性監査の違い

	適合性の内部監査	有効性の内部監査
スタイル	守りの内部監査	攻めの内部監査
見込める成果	・顧客、自社及び利害関係者に安心が得られる ・現状維持ができる	・プロセス改善に役立つ ・経営目的を実現 ・現状を超えた成果が見込める
実施のしやすさ	やさしい （ルール通り行っているかどうかは判定がしやすい）	難しい （監査基準が難しい。程度による判定が難しい）

<u>有効性の内部監査のためには</u>

・課題の認識（外部及び内部課題の認識、事故・事件事例）
・他者の視点（顧客・社会など）
・あるべき姿（課題・問題・目的思考・リスク要因の把握）

内部監査実施のプロセス①

1.計　画
（通知、準備）

2.実　施
（初回会議、監査、最終会議）

3.報　告
（監査結果報告）

4.フォローアップ
（是正処置の評価）

・「内部監査実施計画書」を作成し、被監査部門へ実施通知を行う。内部監査員は、監査メンバーと事前打ち合わせを行い、監査実施に当たっての「内部監査チェックリスト」を準備する。

・初回会議にて、監査リーダーが、監査の段取りを説明。監査実施にあたっては、「内部監査チェックリスト」を活用して行う。最終会議では、「内部監査報告書」へ盛込む内容の確認と理解（合意）を被監査側より得る。

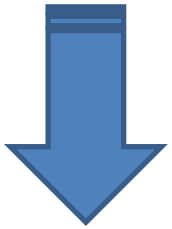
・監査リーダーが、「内部監査報告書」を作成し、被監査部門に通知する。不適合がある場合は、「是正処置に関する報告書」を発行し、回答期限を示す。

・監査リーダーは、不適合の該当部門に対して、実施した是正処置の評価を行う。問題があると評価した場合は、再度、「是正処置に関する報告書」を発行する。

内部監査チェックリスト③

■ 具体的な質問文作成の例

ISMSマニュアル
4.1　組織及びその状況の理解
当社は、外部及び内部の課題を、ISMS推進委員会の中で、議論して明確にする。
また、これらの外部及び内部の課題に関する情報をISMS推進委員会で監視し、レビューを行う。



ISMS マニュアルで規定したことから読み取り、どのように行っているのか、どんなアウトプットがあるのか、など、具体的な回答が相手から得られるように、質問を考える。

想定できる質問
会社における外部及び内部の課題は、どのようにして決定し、明確化していますか。

2.実施　初回会議

■ 初回会議で行うこと

1.今回実施する監査目的、監査範囲、監査基準、「内部監査実施計画書」に記載した事項の確認
2.監査基準となる文書の確認
3.スケジュール調整が必要な場合は、その対応

“外部審査と違って、初回会議は形式的に行う必要はない”

2.実施　監査の進め方①

■ 監査での注意点

1.「内部監査実施チェックリスト」に基づき質問する。ただし、これにとらわれ過ぎずに、必要に応じて、相手の理解しやすい言葉に置き換えたり、質問を掘り下げたりすること。
2.相手とお互いにコミュニケーションが適切にとれること。
3.相手（監査部門）の現状や課題を理解しようという姿勢で臨む。

“指摘を出すことが目的ではなく、改善のための情報収集が目的”

2.実施　監査の進め方②

■ 内部監査員としての態度

1.自分がしゃべり過ぎずに、相手の話に耳を傾ける。
2.相手の立場を考え、相手のミスを問いただすのではなく、
　支援する。
3.良い点があれば、評価し、相手を褒める。
4.コミュニケーションが取りやすい雰囲気を作る。

“不適合事項を見つけに来たのだという態度ではなく、仕組みが効果的だということを皆さんと確認するためにチェックしているのだ、という態度で臨むのがよい。”

2.実施　質問の仕方

■ 3つの質問の仕方

情報の問い	さらなる情報を引き出す質問。いつ、どこで、誰が、どのように。
意味の問い	相手の言ったことの意味がよくわからないときにそれを尋ねる質問。それは、どういう意味か。具体的にいうとそれは何か。
論証の問い	相手の言ったことの根拠がよくわからないときにそれを尋ねる質問。それはなぜか、それはどうしてわかるのか。

“質問のよしあしは、質問の目的による。話題を広げるための質問は「情報の問い」、理解するための質問は「意味の問い」、納得するための質問は「論証の問い」”

2.実施　監査所見②（監査結果の評価区分）

評価区分	内容
適合	監査基準に監査証拠が適合しており問題がない状態。
不適合 （重大）	監査基準に監査証拠が適合していない状態で、仕組み又は手順に完全な欠如がある、あるいは、それらが全く機能していない状態。 ここに該当する場合には、あらためて内部監査の実施も考えられる。 *例）手順が現場と全く整合していない、同じミスが再発している*
不適合 （軽微）	監査基準に監査証拠が適合していない状態で、仕組み又は手順に一部欠如がある、あるいは、それらが一部機能していない状態。 *例）ルールはあるが一部整合していない、是正処置が一部不徹底*
観察事項 *※改善の機会、推奨事項ともいう*	監査基準に監査証拠が適合しているが、このままの状態だと不適合になり得る状態。 ※内部監査員が気づいた改善を指摘してもよい。リスクの観点から見るとよい。

2.実施　監査の結論

■ 監査の結論

監査チームは、監査報告（最終会議）の前に、監査チーム内で、合意を得るために、以下の事項について、打ち合わせをすること。

1.監査中に収集した情報や監査所見（個人ごとの評価）を、レビュー（見直し）する。
2.不適合および観察事項の内容を検討する。
3.不適合の是正処置のフォローについて確認する。