ISO27001：2013
ISMS内部監査員通信講座

ISO27001:2013
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

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

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

監査とは？

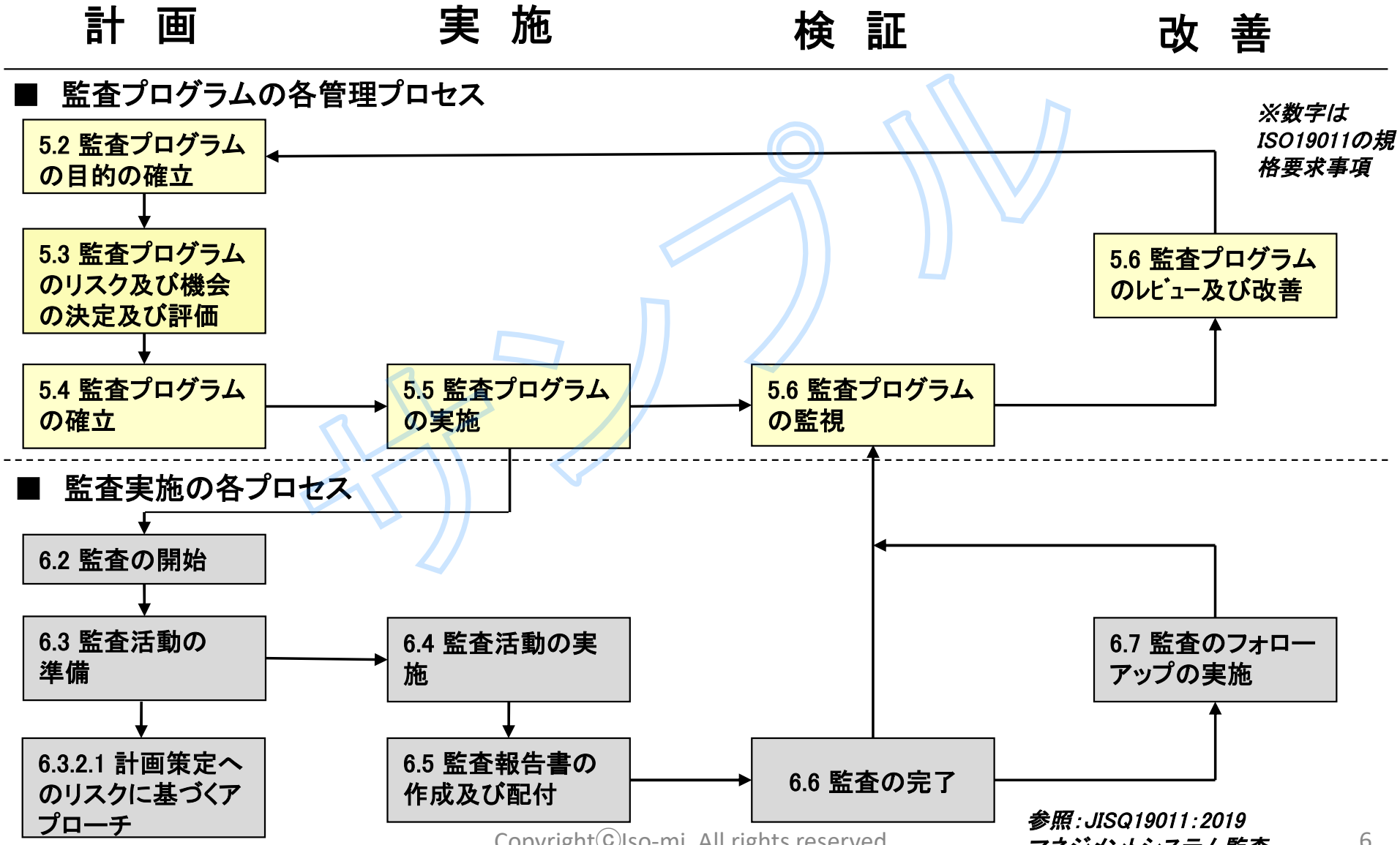
監査とは、**監査基準**が満たされている程度を判定するために、**客観的証拠**を収集し、それを客観的に評価するための体系的で、独立し、文書化されたプロセス。

参照『JISQ19011 :2019 マネジメントシステム監査の指針 3.1』

■ 監査基準：ISO27001の要求事項、顧客要求事項、自社で決めたルール、法令等

■ 客観的証拠：あるものの存在又は真実を裏付けるデータ（後で確認できる情報）

監査プログラムのマネジメント



内部監査とトップの関わり

規格要求事項　9.2　内部監査

f)監査の結果を関連する管理層に報告することを確実にする。

規格要求事項　9.3　マネジメントレビュー

c)、3)監査結果

→ *“内部監査の結果（情報）は、トップに報告される”*

※内部監査での情報は、トップが求めているものなのか？

※トップの関与は、監査計画の形式的な承認だけでは足りない。

内部監査の目的

不適合を見つけるのが目的ではない。

※不適合を指摘するだけに終わらず、その原因を見出すことも内部監査の目的に含まれる。

“業務に役立つための改善情報の提供”

※組織の向上・改善につながるのか？効率を阻害していないか、見過ごしているリスクはないかなどの観点での確認とコメントが大切”

※また、内部監査員は監査員自身の人材育成にもなる。

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）ISO27001:2013の要求事項

②*有効に実施され、維持されている*

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。

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）

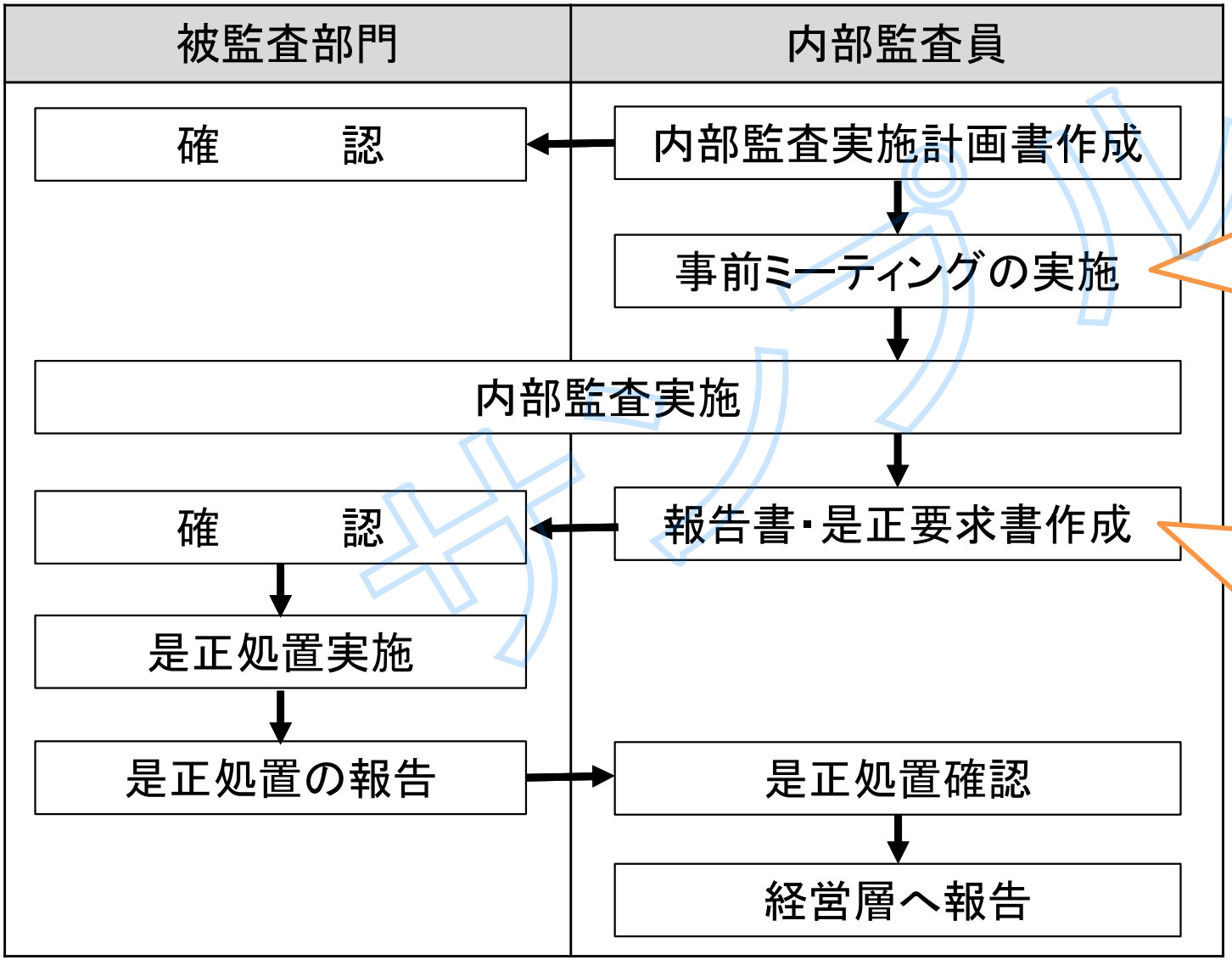
・「内部監査実施計画書」を作成し、被監査部門へ実施通知を行う。内部監査員は、監査メンバーと事前打ち合わせを行い、監査実施に当たっての「内部監査チェックリスト」を準備する。

・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。

内部監査実施のプロセス②



・内部監査チェックリストの作成
・被監査部門の業務の把握
・前回の監査結果の確認

・内部監査報告書は監査実施後、速やかに作成する。
・是正要求書も同時に作成する。

1.計画　内部監査員の選定

属　性	利　　点
営業部門員が行う監査	顧客合意事項を踏まえた監査ができる
関連性のあまりない部門員からの監査	冷静に判断できる
類似活動を行う部門員からの監査	日々の仕事に役立つ情報が得られる
聞き上手な人の監査	日頃の課題や改善のアイデアをより引き出せる
上流部門（上流工程）から下流部門（下流工程）への監査	自分（自部門）の成果（アウトプット）の活用状況がわかる
下流部門（下流工程）から上流部門（上流工程）への監査	自分（自部門）のインプットが適切かどうかがわかる

→ ***監査員自身の利点を意識し、適材適所で割り当てるしかない***

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　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」”

3.報告　監査結果報告の目的

■ 監査結果報告の目的

1.被監査部門への報告
- ・改善情報の提供
- ・正式な監査結果の伝達

2.経営層への報告
- ・マネジメントレビューの資料（インプット情報）

3.組織の知識としての確保
- ・仕組み改善のための情報源
- ・今後の内部監査実施のための資料

3.報告　内部監査報告書②

内部監査報告書の作成ポイント

ポイント	内容
客観的事実の記載	評価に必要な事実が反映されているか。
問題点の特定と事実の正確な把握	何が問題なのかが明確になっているか。
監査基準と評価の妥当性	監査証拠から見て、監査基準及び評価は妥当か。
コメントの意図と納得感	コメントが単なる感覚論ではなく、その意図があるか。納得性があるか。
改善の契機	指摘された事項は、該当部門の問題意識に即した内容であるか。監査を受ける部門の仕事や仕組みの改善の契機となり得るか。

3.報告　是正処置の評価

■ 是正処置の評価

被監査部門から、是正処置の実施報告があったものに関して、内部監査員は、その処置の評価（適合・不適合の判定）を行う。

例）

不適合の内容	ISMS管理策運用規定では、機密情報の漏えいが生じた場合、上長に連絡するとあるが、連絡をしていなかった。

原因の特定
連絡を忘れてしまったため。
是正処置
今後、上長に連絡する。

忘れてしまったのは事象であり、原因ではない。真の原因を特定しているかを見る。

再発防止策が取られているか。単に行っていないことを行うでは不十分。

以　上

ISO27001：2013　ISMS内部監査員研修テキスト①

通信講座用　～監査手順編～

IMI2021-01版

ISOマネジメント研究所

〒279-0026千葉県浦安市弁天1-21-8

E-mail：info@iso-mi.com