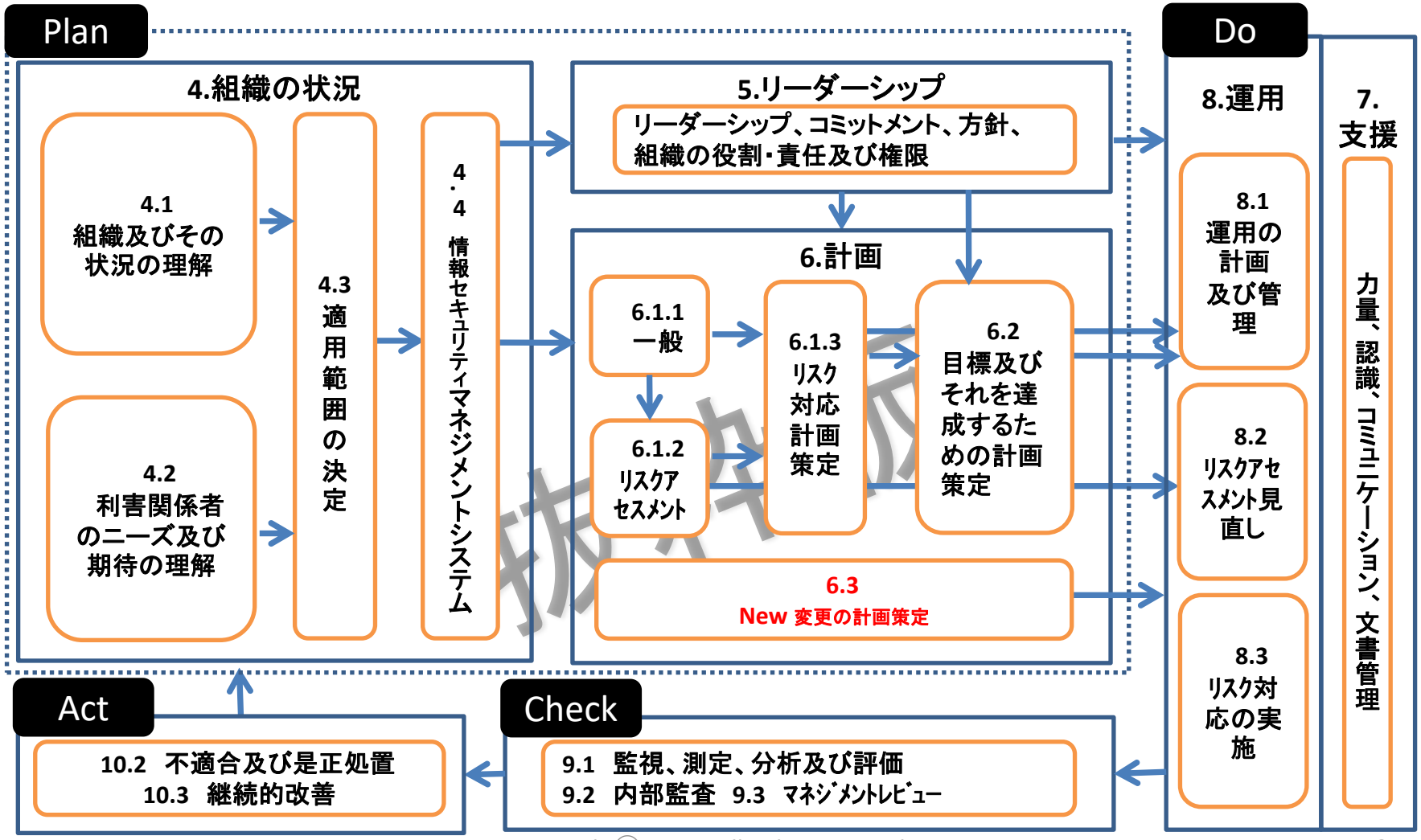
ISO27001：2022
ISMS内部監査員通信講座

ISO/IEC27001:2022
ISMS内部監査員研修テキスト②
～規格要求事項の理解編～

ISOマネジメント研究所
established in 2001

ISO/IEC27001:2022の全体像



ISO/IEC27001：2022の規格要求事項

本文

1.適用範囲　2.引用規格　3.用語及び定義
4.組織の状況　5.ﾘｰﾀﾞｰｼｯﾌﾟ　6.計画　7.支援　8.運用
9.ﾊﾟﾌｫｰﾏﾝｽ評価　10.改善

附属書A管理策：　分類4、管理策93

5.組織的管理策（37）　6.人的管理策（8）
7.物理的管理策（14）　8.技術的管理策（34）

ISO/IEC27001：2022での改訂箇所①

No	改訂箇所
1	4.2 利害関係者のニーズ及び期待の理解　C)
2	4.4 情報セキュリティマネジメントシステム
3	5.3 組織の役割、責任及び権限
4	6.2 情報セキュリティ目的及びそれを達成するための計画策定　d)
5	6.3 変更の計画策定　新規要求事項
6	7.4 コミュニケーション　d)
7	8.1 運用の計画策定及び管理
8	9.2.1 内部監査（一般）
9	9.2.2 内部監査プログラム

4.1　組織及びその状況の理解

- 組織の目的に関連し、かつ、そのISMSの意図した成果を達成する組織の能力に影響を与える、外部及び内部の課題を決定すること

※ 課題とは、組織において解決すべき（議論すべき）問題のこと。課せられた題・問題。

【内部監査での着眼点】

・ISMSの意図した成果は明確か。

・外部及び内部の課題は明確になっているか。

4.2　利害関係者のニーズ及び期待

次の事項を決定すること

① ISMSに関係する利害関係者

② それらの利害関係者の、情報セキュリティに関連する要求事項

③ それらの要求事項のうち、ISMSを通して取り組むもの

※ 利害関係者の要求事項には、法的及び規制要求事項並びに契約上の義務を含めてもよい。

【内部監査での着眼点】

・利害関係者の要求事項は明確か。

・利害関係者の要求事項を明確にするプロセスは確立されているか。

・利害関係者に漏れはないか。

5.2　方針

・経営層（社長）は、次の事項を満たす情報セキュリティ方針を確立すること。また、方針は、**文書化して、**組織内に伝達すること。必要に応じて、利害関係者が入手可能であること

① 組織の目的に対して適切である
② 情報セキュリティ目的を含むか又は情報セキュリティ目的の設定のための枠組みを示す
③ 情報セキュリティに関連して適用される要求事項を満たすことへのコミットメントを含む
④ 情報セキュリティマネジメントシステム（ISMS）の継続的改善へのコミットメントを含む

【内部監査での着眼点】
・作成した情報セキュリティ方針は、現在の置かれた状況にあっているか。
・作成した方針は、従業員に理解されているか

5.3　組織の役割、責任及び権限

・経営層（社長）は、情報セキュリティに関連する役割に対して、責任及び権限を割り当て、組織内に伝達することを確実にしなければいけない

・次の事項に対して、責任及び権限を割り当てなければならない
① ISMSが、この規格の要求事項に適合することを確実にする
② ISMSのパフォーマンスを経営層（社長）に報告する

【内部監査での着眼点】
・割り当てられた責任及び権限は組織内に周知しているか。
・割り当てられた責任及び権限は有効に機能しているか。

8.1　運用の計画及び管理①

・組織は、次の事項の実施によって、情報セキュリティ要求事項を満たすため、及び6で決定した活動を実施するために必要なプロセスを計画し、実施し、かつ管理すること。

①プロセスに関する基準の設定

②その基準に従った、プロセスの管理の実施

・プロセスが計画通りに実施されたという確信をもつために必要な程度の、文書化した情報を利用可能な状態にすること

・計画した変更を管理し、意図しない変更によって、生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置をとること

9.3　マネジメントレビュー（インプット①）

・マネジメントレビュー（インプット）は、次の事項を実施すること

①前回までのマネジメントレビューの結果とった処置の状況
②ISMSに関連する外部及び内部の課題の変化
③ISMSに関連する利害関係者のニーズ及び期待の変化
④次に示す傾向を含めた、情報セキュリティパフォーマンスに関するフィードバック
　1）不適合及び是正処置
　2）監視及び測定の結果
　3）監査の結果
　4）情報セキュリティ目的の達成

ISO/IEC27001:2013年版との違い

	ISO/IEC27002:2013	ISO/IEC27002:2022
管理策の分類	14分類	4分類 （組織的管理策、人的管理策、物理的管理策、技術的管理策）
管理策の数	114	93
管理策の構成	管理目的 管理策名 管理策（内容） 実施の手引き 関連情報	管理策名 管理策の属性 管理策（内容） 管理目的（それぞれに） 実施の手引き 関連情報

ISO/IEC27001:2013年版との対比表①

■組織的管理策

管理策No	管理策タイトル	ISO27001:2013管理策
5.1	情報セキュリティのための方針群	5.1.1　情報セキュリティのための方針群 5.1.2　情報セキュリティのための方針群のレビュー
5.2	情報セキュリティの役割と責任	6.1.1　情報セキュリティの役割及び責任
5.3	職務の分離	6.1.2　職務の分離
5.4	経営陣の責任	7.2.1　経営陣の責任
5.5	関係当局との連絡	6.1.3　関係当局との連絡
5.6	専門組織との連絡	6.1.4　専門組織との連絡

ISO/IEC27001:2013年版との対比表②

■組織的管理策

管理策No	管理策タイトル	ISO27001:2013管理策
5.7	脅威インテリジェンス	―
5.8	プロジェクトマネジメントにおける情報セキュリティ	6.1.5　プロジェクトマネジメントにおける情報セキュリティ 14.1.1　情報セキュリティ要求事項の分析及び仕様化
5.9	情報及びその他の関連資産の目録	8.1.1　資産目録 8.1.2　資産の管理責任
5.10	情報およびその他の関連資産利用の許容範囲	8.1.3　資産利用の許容範囲 8.2.3　資産の取扱い
5.11	資産の返却	8.1.4　資産の返却
5.12	情報の分類	8.2.1　情報の分類

ISO/IEC27001:2013年版との対比表⑤

■組織的管理策

管理策No	管理策タイトル	ISO27001:2013管理策
5.20	供給者との合意における情報セキュリティの取扱い	15.1.2　供給者との合意におけるセキュリティの取扱い
5.21	ICTサプライチェーンの情報セキュリティ管理	15.1.3　ICTサプライチェーン
5.22	供給者のサービス提供の監視、レビュー及び変更管理	15.2.1　供給者のサービス提供の監視及びレビュー 15.2.2　供給者のサービス提供の変更に対する管理
5.23	クラウドサービス利用のための情報セキュリティ	ー
5.24	情報セキュリティインシデント管理の計画策定及び準備	16.1.1　責任及び手順

ISO/IEC27001:2013年版との対比表⑦

■組織的管理策

管理策No	管理策タイトル	ISO27001:2013管理策
5.30	事業継続のためのICTの備え	―
5.31	法令、規制及び契約上の要求事項	18.1.1　適用法令及び契約上の要求事項の特定 18.1.5　暗号化機能に対する規制
5.32	知的財産権	18.1.2　知的財産権
5.33	記録の保護	18.1.3　記録の保護
5.34	プライバシー及び個人を特定できる情報（PII）の保護	18.1.4　プライバシー及び個人を特定できる情報(PII)の保護
5.35	情報セキュリティの独立したレビュー	18.2.1　情報セキュリティの独立したレビュー

5.23　クラウドサービス利用のための情報セキュリティ

5.23　クラウドサービス利用のための情報セキュリティ
目的：クラウドサービスの利用における情報セキュリティを規定及び管理するため

□要求事項

クラウドサービスの調達、利用、管理及び利用終了のプロセスを、組織の情報セキュリティ要求事項に従って確立しなければならない。

□実施の手引き（概要）

クラウドサービスの利用に関する個別方針を確立し、全ての関連する利害関係者に伝達すること。クラウドサービスの利用には、クラウドサービスを提供する事業者との間で、情報セキュリティに関する責任の共有及び分担、並びに共同作業を伴う可能性があるので、お互いの責任を適切に定義し、実践することが必要。クラウドサービスの利用におけるリスクを特定するために、リスクアセスメントを実施することも必要。

■理解のﾎﾟｲﾝﾄ

クラウドサービス利用方針を策定し、これに基づき、クラウドサービスの調達（契約）、利用、管理及び利用終了のプロセスを管理することが必要。クラウドサービスの調達（契約）時には、リスクアセスメントを実施すること。

5.30　事業継続のためのICTの備え

5.30　事業継続のためのICTの備え 目的：事業の中断・阻害時に組織の情報及びその他の関連資産の可用性を確実にするため
□要求事項 事業継続の目的及びICT継続の要求事項に基づいて、ICTの備えを計画、実施、維持及び試験しなければならない。
□実施の手引き（概要） 事業活動の中断・阻害時によって生じる影響を評価（ビジネスインパクト分析（BIA））すること。評価の結果、特定した優先順位の高い事業においては、復旧時間目標（RTO）及び復旧ポイント目標（RPO）を設定すること。これらを踏まえたICT 継続戦略（計画）を立案し、実施し、維持し、試験すること。
■理解のﾎﾟｲﾝﾄ 主に災害時において、情報の可用性を図っておくこと。まずは、復旧事業の優先順位を決め、具体的に対応するための復旧時間目標や復旧ポイント目標を考えておくこと。また、計画のテストも実施して、検証する必要がある。

8.16　監視活動

8.16　監視活動
目的：異常な行動・動作及び潜在する情報セキュリティインシデントを検出するため

□要求事項

情報セキュリティインシデントの可能性を評価するために、ネットワーク、システム及びアプリケーションについての異常な挙動がないか監視し、適切な処置を講じなければならない。

□実施の手引き（概要）

主に監視ツールを用いた継続的な監視を行うことを意図している。例えば、プロセスまたはアプリケーションの予期せぬ終了、マルウェアに関連する活動、不審なIPアドレスやネットワークドメインから発信されるトラフィック、システムの異常な挙動などの監視を行うこと。

■理解のﾎﾟｲﾝﾄ

ファイヤーウォール、ログ情報、セキュリティソフト（ウイルス対策ソフト）、等を活用して監視し、適切な処置を講じることが必要である。5.7 脅威インテリジェンスとも関係してくる。

8.23　ウェブ・フィルタリング

8.23　ウェブ・フィルタリング

目的：システムがマルウェアによって危険にさらされることを防ぎ、認可されていないウェブリソースへのアクセスを防止するため

□要求事項

悪意のあるコンテンツにさらされることを減らすために、外部ウェブサイトへのアクセスを管理しなければならない。

□実施の手引き（概要）

違法な情報が掲載されていたり、ウイルスやフィッシングの材料が含まれていることが知られているウェブサイトにアクセスするリスクを低減することが必要。

5.7脅威インテリジェンスから得られた、アクセスすべきでないウェブサイトの種類を特定し、ウェブサイトへのアクセスをブロックすること。

■理解のポイント

ウェブへのアクセスを含むオンラインリソースの安全かつ適切な使用について、周知等が必要となる。技術的な対策としては、セキュリティソフト（ウイルス対策ソフト）等を活用して、外部のウェブサイトへのアクセスを管理することになる。