6.パフォーマンス評価と継続的改善

（初級者編）

個人情報保護・情報セキュリティをマネジメントする
―ISO19011:2011による内部監査―

株式会社エム・ピー・オー
代表取締役 森口修逸

「パフォーマンス評価」の目的

1. マネジメントシステム規格の「第9章　パフォーマンス評価」の構成
   「運用確認」、「監視、測定、分析及び評価」、「内部監査」、
   「マネジメントレビュー」、「是正処置」、「継続的改善」
2. パフォーマンス:計画した活動の**実施** ➡ 達成した程度の**評価**
   - 初級編の内容:「内部監査とは何か？」の理解
     - 「内部監査」、「マネジメントレビュー」、「是正処置」、「継続的改善」
   - 上級編の内容:内部監査の特定分野での具体的な実施例
     A）保健医療等「特定の分野」での法令等の要求事項と留意点
     B）初級編で未解説項目の説明:「運用確認」、「監視、測定、分析及び評価」
     C）継続的改善につなげるためのHowTo
       ✓ 不適合の指摘手法例と是正処置の改善事項の回答手法例

注:ISO/IEC27000より
2.59 パフォーマンス(performance):　測定可能な結果。
注記 1　パフォーマンスは，定量的又は定性的な所見のいずれにも関連し得る。
注記 2　パフォーマンスは，活動，プロセス(2.61)，製品(サービスを含む。)，システム，又は組織(2.57)の運営管理に関連し得る。

6項　「パフォーマンス評価と継続的改善」の全体

A)　パフォーマンス評価とは何か？（初級編）

- 9.2 内部監査
- 9.3 マネジメントレビュー
- 10.1 是正処置
- 10.2 継続的改善

B)　パフォーマンスを向上させるには（上級編）

- 1．医療・健診分野における監査とは
- 8.1 現場管理者による運用確認の実務
- 9.1 監視、測定、分析及び評価の実務
- 9.2 内部監査の指摘のHowTo
- 10.1 是正処置の改善力向上のHowTo
- 10.2 継続的改善のHowTo

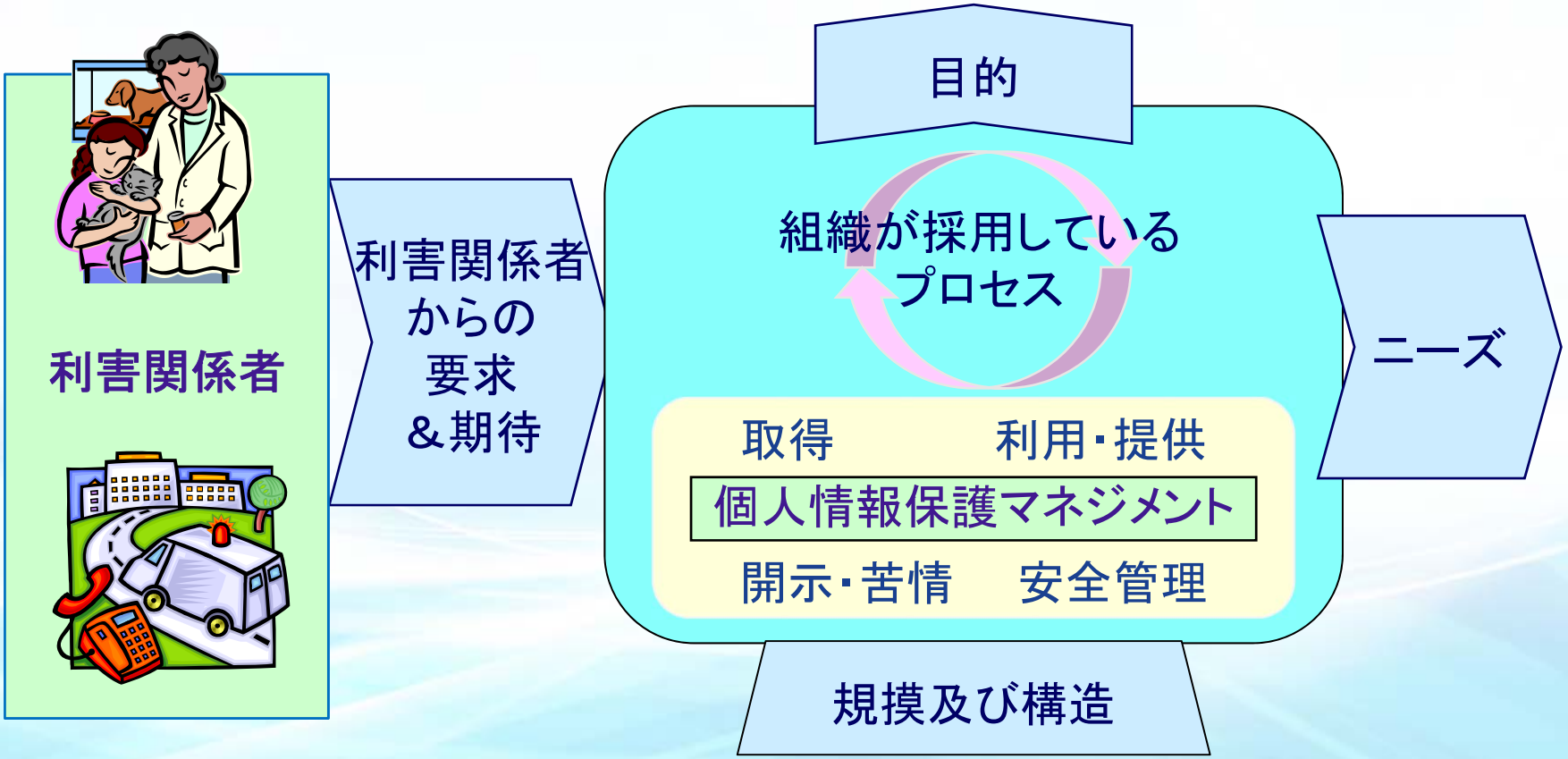
A） パフォーマンス評価とは何か？（初級編）

- 9.2 内部監査
- 9.3 マネジメントレビュー
- 10.1 是正処置
- 10.2 継続的改善

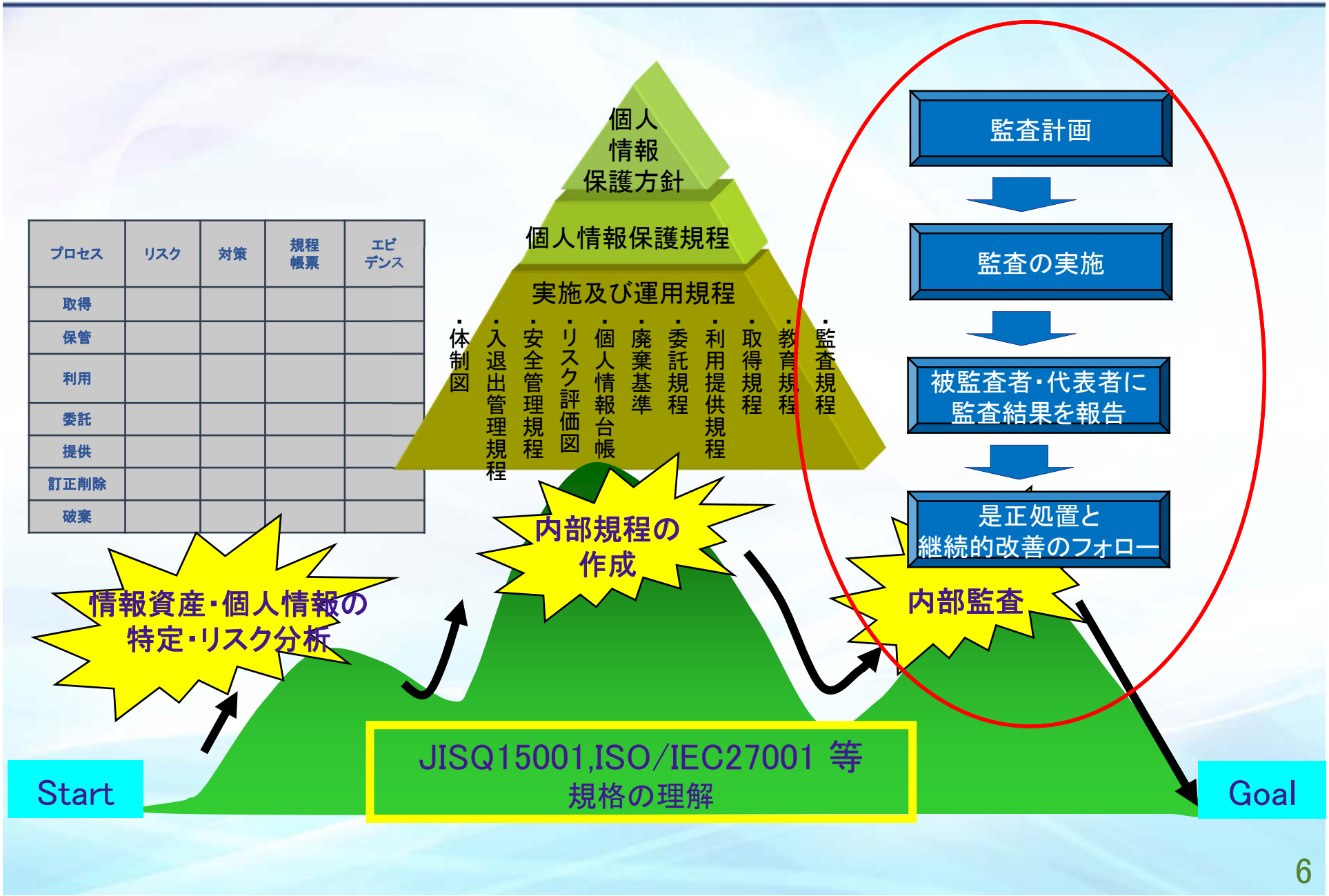
マネジメントとは何か？

組織内外の環境変化に対応して組織を維持発展させること

1.「利害関係者からの」 **個人情報保護・情報セキュリテイに関する要求/期待、**
2.「組織自身の」 **規摸及び構造、ニーズ、目的，採用している業務プロセス**
は、時間とともに変化してゆき、マネジメントに影響を与える



マネジメントシステム確立に至る経緯と作業量



coffee　break　①

さて、これは何に見えますか？

さて、これは何に見えますか？

マネジメントシステムにおける監査の定義

9.2　内部監査[ISMS :ISO/IEC27001 : 2013、PMS :JISQ15001 : 2017 共通]

組織は，ISMS/PMSが次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**しなければならない:

a) 次の事項に適合している
　1) ISMS/PMSに関して，組織自体が規定した要求事項
　2) この規格の要求事項

b) 有効に実施され，維持されている。
　組織は，次に示す事項を行わなければならない:

c) 頻度，方法，責任及び計画に関する要求事項及び報告を含む，**監査プログラムの計画**，確立，実施及び維持。監査プログラムは，関連するプロセスの重要性及び前回までの監査の結果を考慮に入れなければならない;

d) 各監査について，監査基準及び監査範囲を明確にする;

e) 監査プロセスの客観性及び公平性を確保する監査員を選定し，監査を実施する;

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;

g) 監査プログラム及び**監査結果の証拠として，文書化した情報を保持**する。

3.1 監査（audit） ISO 19011:2011 : マネジメントシステム監査の為の指針

「監査基準が満たされている程度を判定するために、監査証拠を収集し、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」

監査の種類

◆内部監査----------第一者による監査

自社のISMS/PMSが旨く機能していることの確認

◆外部監査----------第二者による監査

組織のISMS/PMSを購入者等が確認

供給者に対する業者監査も該当

---------第三者による監査

審査機関による組織のISMS/PMSの確認

ISMS：情報セキュリテイマネジメントシステム：ISO/IEC27001:2013

PMS：個人情報保護マネジメントシステム　：JISQ15001：2017

ISO19011による監査のためのガイドライン

1. ISO19011 の制定及び改訂の経緯とそのポイント
2. ISO19011:2011

   「マネジメントシステム監査のためのガイドライン」概説

   A)　(P)内部監査の確立までとHowto

   B)　(D)監査員の監査現場での振舞い

   C)　(C)是正処置要求・報告と監査報告書

   D)　(A)マネジメントレビューと継続的改善

ISO19011の制定・改訂の経緯とそのポイント

1. ISO19011は、品質・環境のマネジメントシステムの監査のためのガイドラインとして制定
2. ISO19011:2002の定期見直し（2007年）に際して改訂が決定
3. 2011年11月末にISO化、日本語訳語、2012年にJIS化
4. 第一者（内部監査）・第二者監査のみに適用

   第三者認証監査のためには、ISO17021 が制定済
5. マネジメントシステム全般に対応

   品質（ISO9001）・環境（ISO14001）の規格と同様に、

   ISMS（ISO/IEC27001:2013）等に対しても参照規格化

   Pマーク（JISQ15001：2017）の改版に際して参照規格と　された
6. 監査のための様々な参考資料が附属書に追加された

内部監査の重要性

P

◆内部監査：第一者監査
- 自社のマネジメントシステムが旨く機能していることの確認。

1.内部監査が役に立っている

＝ 組織にマネジメントシステムが定着

2.内部監査の運用の仕方によっては、

a.マネジメントにとって重要で意味のある活動に出来る、反面、

b.ほとんど何の意味も持たない活動となる可能性も

3.マネジメントシステムを継続的に改善してゆく仕掛けとして

内部監査が最も重要

ポジティブな監査であること！

P

監査側と被監査側が利害対決

被監査側：不適合が出ると恥

監 査 側 ：意地でも指摘　件数 xx件

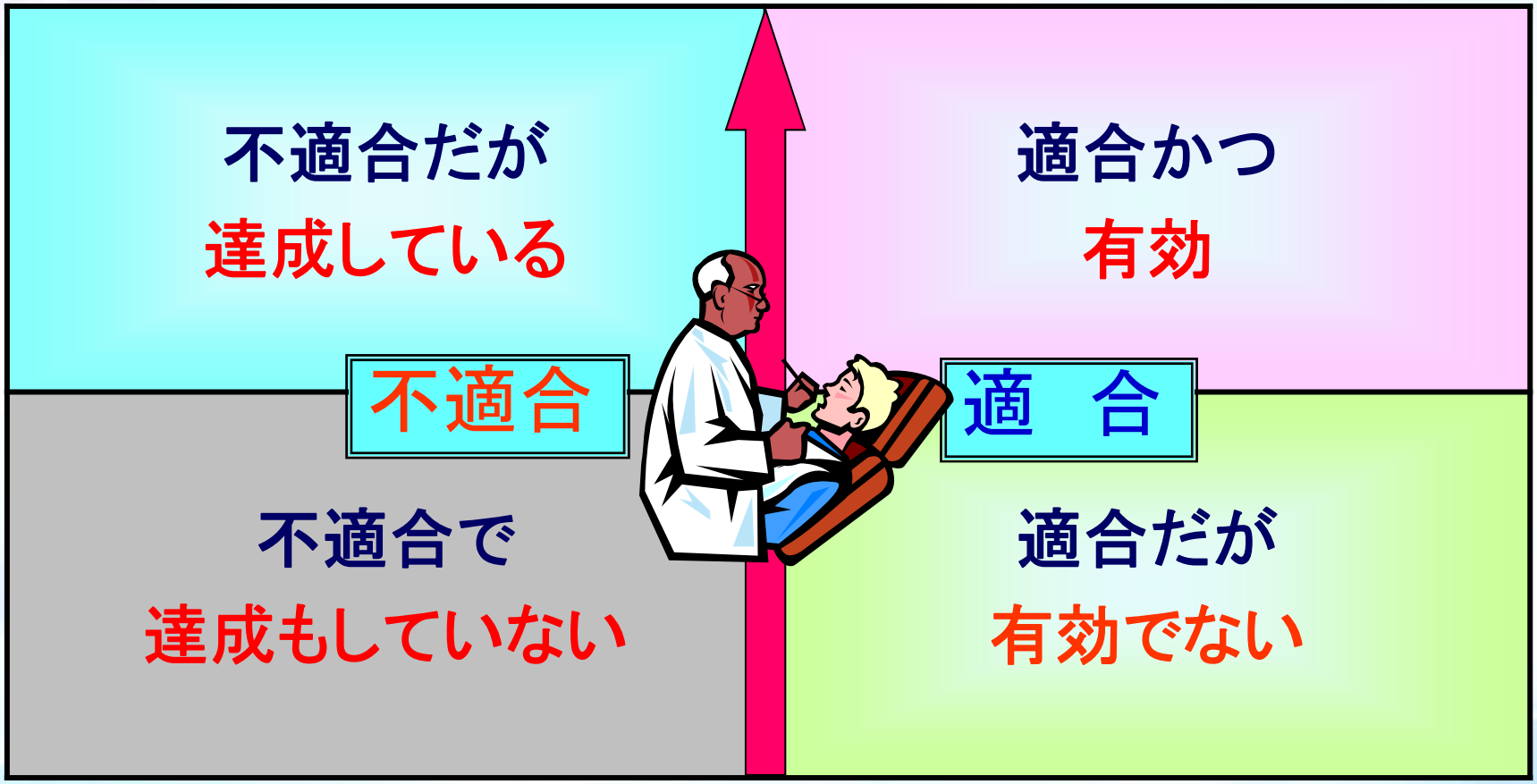
監査に対する互いの、期待と信頼と協力が必要

「不適合の抽出でなく、予防である」

不適合は、宝の山：被監査側もプラス思考

監査結果の適合と有効性

P



適合性判定から有効性判定へ

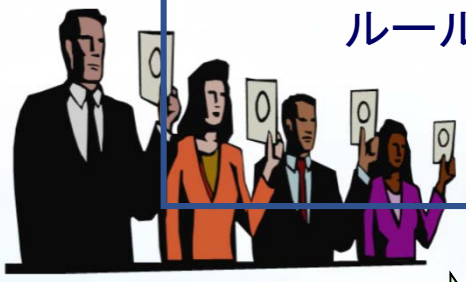
P

マネジメントシステムの成熟度に対応した判定方法

こちらへ
向かいましょう

構築直後

・適合性の監査：
　適合／不適合
・皆が設定された
　ルールを守っている



成熟期

・有効性重視の監査：
　有効／有効でない
・計画した結果
　何をしたい、何を期待するのか
・達成度合い
　役に立っているのか、いないのか

実行することよりも、
実行した後が重要

「適合」とは　：　要求事項を満たしていること
　→ 皆が設定したルールを守っている

「有効」とは　：　計画した活動を実行し、
　計画した結果を達成した程度
→ 計画するルールの良さ

基本及び用語の定義（ISO/IEC27000）

監査プログラムもPDCAから

P

トップ

5.2 監査目的の設定

監査管理者

5.3 監査プログラムの策定

・監査責任者の役割及び責任

・監査責任者の力量

・監査プログラムに

適用する範囲の決定

関わるリスクの特定・評価

手順の確立

資源の特定

5.4 監査プログラムの実施

・一般（事務局的役割）

D

・個々の監査目的、適用範囲及び基準の明確化

・監査方法の選定

・監査チームメンバーの選定

・監査チームリーダーに対する個々の監査の責任の割当

・成果の管理

・記録の管理及び維持

7 監査員の力量及び評価

6 監査の実施

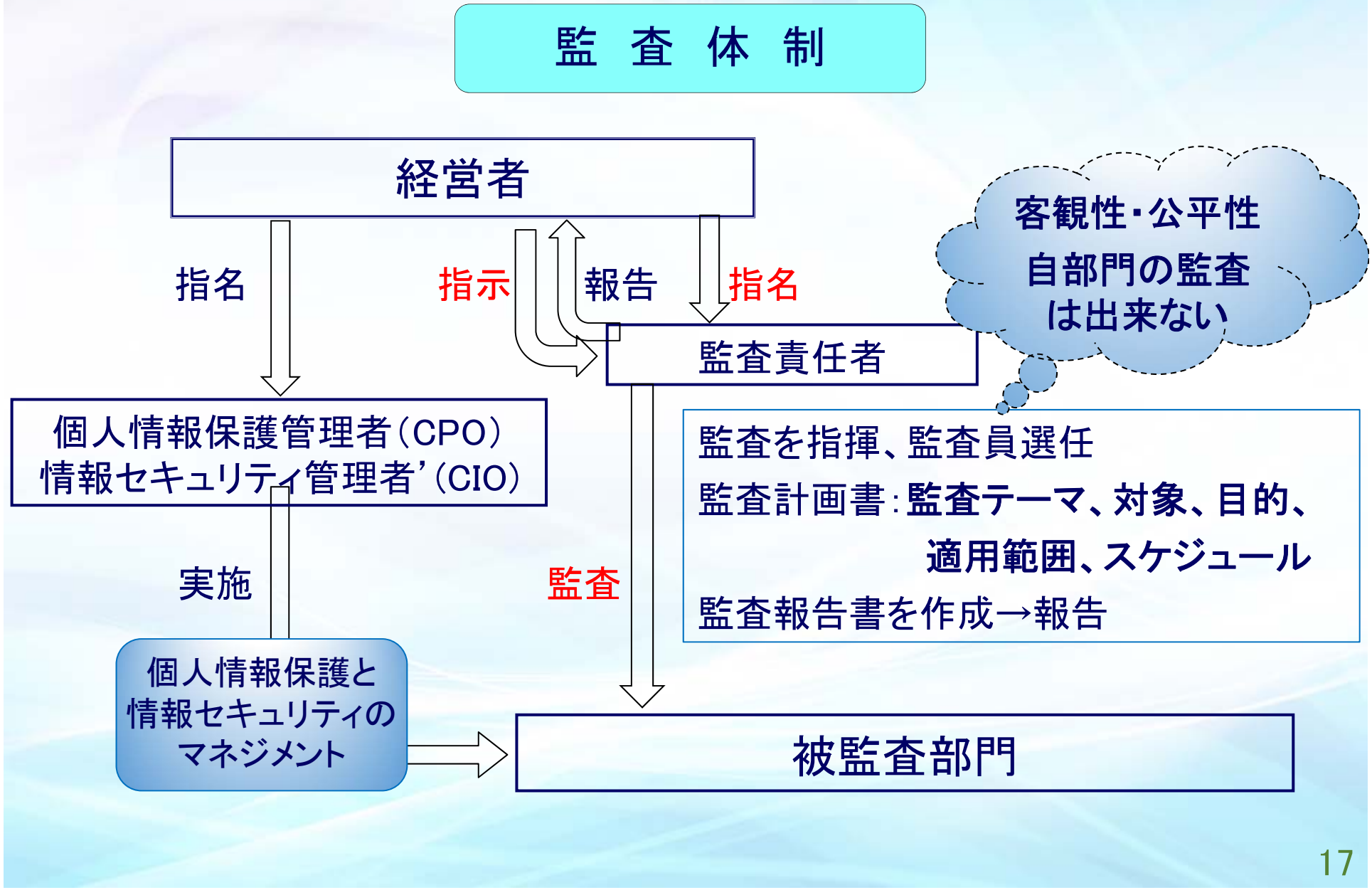
5.5 監査プログラムの監視 C

5.6 監査プログラムのレビュー 及び改善 A

ISO 19011:2011 に記載の内部監査のフローより

監査責任者の指名と監査の指揮

P



「力量：competence」の評価について

P

力量：意図した結果を達成するために知識及び技能を適用する能力
⇒　監査プロセスにおける個人の行動の適切な適用ができること

必要な力量（知識・技能）の設定
⇒　それに基づく評価を実施
⇒　監査員候補者に必要な力量があるかどうか判断

- 監査責任者による監査員の選定・評価を支援する手引き
  - 監査員の共通の知識及び技能
  - 付属書A ：「マネジメントシステムの各分野固有の知識及び技能の例示」
  - 「×」の事例；
    業務経験の年数、教育・訓練回数、監査経験日数等の設定により、
    満足していれば（自動的に）監査員の資格を与える　など**質を考慮しない**場合

ISO19011　7項、附属書A

D

さて、これは何に見えますか？

監査プログラムの実施 D

1.被監査組織にとり、次期の判断に資する監査結果の獲得のために

a. マネジメントシステムが**有効に機能**しているか

b. 重要事項及び**監査に係るリスクに着目**しているか

2.経営者の役割と監査責任者の役割

a. 経営者の役割:「5.2:監査プログラムの目的の設定」

① マネジメントシステムの**パフォーマンス改善、有効性の判定**

② 外部要求事項を満たす(**認証の取得等**)

③ **契約上の要求事項の検証**

④ **供給者としての信頼獲得・維持**

⑤ 組織の**目的と機関全体の方針との両立・整合の確認**

b. 監査プログラムに関して

5.2項 目的の設定:組織の目的と機関全体の方針との両立・整合

5.3項 策定 :監査の目的、適用範囲、審査基準の設定等

5.4項 実施 : [詳しくは次ページ]

監査実施の連絡･調整･報告の作業

D

1. 監査プログラムの進行状況の把握と連絡･連携
2. 監査の目的･適用範囲の明確化
3. 監査活動の調整･スケジュール作成

   5.3 監査プログラムの策定から

   5.6 監査プログラムのレビュー及び改善まで、

   通常、3カ月以上を要する
4. 必要な力量の監査チームの構成
5. 監査プログラムに従った合意された時間内での監査の実施を確実に
6. 監査活動が記録され、その記録が適切に管理･維持されていること

ISO 19011 5.4項

監査の実施(Do)の詳細

D

6.2		監査の開始
	6.2.1	一般
	6.2.2	被監査者との最初の連絡
	6.2.3	監査の実施可能性の判定

6.3		監査活動の準備
	6.3.1	監査に備えた文書レビュー
	6.3.2	**監査計画の作成**
	6.3.3	監査チームへの作業の割当て
	6.3.4	**作業文書の作成(チェックリスト等)**

6.4		**監査活動の実施**
	6.4.1	一般
	6.4.2	初回会議
	6.4.3	監査の実施中の文書レビュー
	6.4.4	監査中の連絡
	6.4.5	案内役及びオブザーバーの役割及び責任
	6.4.6	情報の収集及び検証
	6.4.7	**監査所見の作成**
	6.4.8	**監査結論の作成**
	6.4.9	最終会議の実施

6.5		監査報告書の準備、承認及び配付
	6.5.1	監査報告書の作成
	6.5.2	監査報告書の配付

6.7		**監査フォローアップの実施**

監査に係るリスク

D

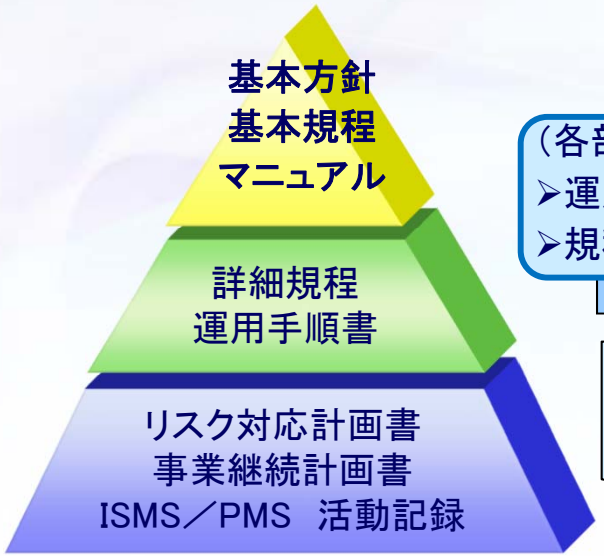
- 監査プログラムの管理者は、監査プログラムを策定する際に、「監査プログラムの目的の達成」に影響を及ぼすリスクを考慮する必要がある。

項目	リスクの事例
計画の不適切な策定	監査目的の設定監査プログラムを適用する範囲の決定が適切でない。
監査資源不足	監査プログラムの策定又は監査の実施に十分な時間が割けない。
監査チームの構成ミス	チームとして監査を効果的に実施するための力量を備えていない。
監査実施の際のコミュニケーション不足	監査プログラムに関するコミュニケーションが効果的でない。
監査記録及びその管理不適切	監査プログラムの有効性を実証するための監査記録の保護が十分でない。
監査プログラムの監視・レビュー及び改善不足	監査プログラムの成果が効果的に監視されていない

ISO19011 5.3.4項

チェックリストの作成手法

D



（各部門）
- 運用手順書の抜け確認
- 規程整備状況確認

前回
監査報告書

当該被監査部門の
関連プロセス認識

問題点をレビュー

チェックリスト作成

◆時間的制約：監査はサンプリング方式

例1　⇒監査ポイントをチェックリストにまとめる。

◆○×式の消し込み帳票

例2　⇒記述式チェックリスト

◆手順書中の客観的証拠に繋がるキーワードをチェック対象にする。

例3　⇒手順書利用型チェックリスト

手順書利用型チェックリスト作成例

D

規程

「入退室管理手順書」　･･･抜粋･･･

4　職員入退室管理

(2) 最初入室･最終退室の管理

各室ごとに、**朝一番に入室した者及び夜最後に退出した者**は、「最初入室者･最終退室者管理表」に**入室時間または最終退室時間を記入**する。

各施設ごとに**総務部長又は各部門の長**は、毎月「最初入室者･最終退室者管理表」の**内容を確認し、入退室に関し問題があれば調査し、**

情報セキュリティ責任者又は各部門の情報セキュリティ管理者へ報告する。･･･････

チェックリスト

	実施者	チェックポイント	YorN
「最初入室者･最終退室者管理表」に関して	部員	入室時間または最終退室時間が記入　されているか？	
	部門管理者	内容は確認されているか？	
		退室に関し問題があれば調査されているか？	
		情報セキュリティ責任者又は各部門の情報セキュリティ管理者へ報告されているか？	
	･････	･････	

監査チェックリスト例

D

①監査場所･部署
②監査対象項目
③確認文書名称･番号
④応対者
⑤観察事項（不適合状況）

内部監査チェックリスト

被監査部署 ： ①　　監査日 ：

出　席　者 ： ④　　監査チーム ：

②

判　定：○：適合、X：重大な不適合、△：軽微な不適合、□：観察

規格要求事項	チェック項目（質問事項）	制定	実施	維持	客観的証拠	判定
3.1 一般要求事項	ＰＭＳを確立し，実施し，維持し，かつ，改善しているか。	○	○	○	③ ⑤	
3.2 個人情報保護方針	個人情報保護の理念は明確か	○				
	個人情報保護方針には、a)～ｆ）が含まれているか	○		○		
	方針を文書化し，従業者に周知させるとともに，一般の人が入手可能な措置は適切か（法令の改訂等による変更への対応が、確実におこなわれているか）	○	○	○		
3.3 計画						
3.3.1 個人情報の特定	事業の用に供するすべての個人情報を特定するための手順を確立，維持されているか。（改訂が適切におこなわれているか）	○		○		
3.3.2 法令，国が定める指針その他の規範	個人情報の取扱いに関する法令，国が定める指針その他の規範を特定し参照できる手順を確立	○	○	○		

監査現場でのHowTo

D

1. 通常の監査手順、監査員の力量・資質・実務経験等、
2. 監査現場での具体的進め方の例、監査のテクニック、
3. 確認すべき項目、監査員の態度・心構え
4. 結論に記載すべき事項
5. 適合・不適合・是正処置の定義、是正処置の流れ
6. 監査所見（用語の定義）、所見を決定する際に考慮すべき事項
7. 是正処置要求書・報告書及び監査報告書　例
8. 是正処置の流れ、不適合及び是正処置と他部門への展開、
9. 是正処置への対応（Pマークのみの対応）、

通常の監査手順

D

1. 監査実施場所
   - ·監査員は会議室で待機
   - ·被監査部門の担当者は、監査員から設定された時間に入室
2. 被監査部門の担当者：各部門の管理者及びその実務代理
3. 監査側はチェックリストを順に確認
   - ·「前回比較で、向上が見られたと思われるか？それはどの点か？」などについて説明を受けつつ、管理者としての理解度を監査
4. 業務のフローチャートと台帳の記載内容は、毎年確実に見直してあることは確認するが、中身の評価はしない
5. 現場の状況視察：机上での確認後に、必要に応じて実施

監査員の力量・資質・実務経験等

D

1. 監査員の力量

   監査に必要とされるノウハウ・スキルは、

   実地の監査、日常業務を通じた訓練も重要

2. 監査員に必要な資質：ISO19011:　7.2.2項
   個人的特質、監査テクニック、態度・心構え

3. 監査員には以下の側面も必要

   ① 実務経験

   ② マネジメントセンス

監査現場での具体的進め方の例

D

✓監査場所　　：（総務部、システム開発部等）
✓監査対象　　：（文書管理、物理的入退室管理策等）
✓文書名称･番号　：　確認文書（規程、標準、手順書等）
✓応対者　　：被監査側で監査に立合った人
✓観察事項　　：要求事項に抵触する事実

（**不適合事項**）　**10月分の**「最初入室者･最終退室者管理表」において**10月10日、11日の両日**に退室時間･退出者が未記入の状態で“総務部長確認済み”の押印がなされている。

エビデンスとなる
具体的日時･事柄を記載

（**内部規定**）　「**入退室管理規程**」においては、「入退室に関し問題があれば、その原因を調査し、情報セキュリティ責任者へ報告する。」と規定されていてる。

不適合の原因とした
具体的規程･条項を記載

監査のテクニック

D

- Open Question (5W1H)
- 回答の内容を確認する
- 相手を変えて質問を繰り返す
- 事実を客観的に観察し把握する

確認すべき項目

D

① 管理対象が特定されているか

② 手順/文書化ができているか

③ 手順/文書化の内容は十分か

④ 作業が手順通り実施されているか

⑤ 必要な記録が保管・活用されているか

⑥ システムが有効に機能しているか

脅威、脆弱性、情報及びリスク対策のモデル D

脅威：
システム又は組織に損害を与える可能性があるインシデントの潜在的な原因

セーフガード（リスク対策）：
リスク対応のための慣行，手順又は仕組み。
注記 “セーフガード”は，“管理策”と同義語とすることがある

ぜい（脆）弱性：
一つ以上の脅威がつけ込むことのできる，資産又は資産グループがもつ弱点

監査員の態度・心構え

D

- 正確・明瞭に話し、質問を繰り返す
- 相手の話に耳を傾け、冷静に理解・判断
- 質問による作業の邪魔は最小限に
- 不適合を探し回らず問題なければ評価

C

さて、これは何に見えますか？

監査結論に記載すべき事項

C

1. 監査基準（規程等）への適合の程度
   a. マネジメントシステムの頑健さ、強みの認識
   b. 目的に見合うマネジメントシステムの有効性を含む。
2. マネジメントシステムの効果的実施、維持及び改善
   a. マネジメントシステムが引き続き適切、妥当、有効で、かつ、
   b. 改善が継続することを確実にするためのマネジメントプロセスの能力
3. 監査目的の達成、監査範囲の網羅性、監査基準の達成
4. 所見に関する根本原因

ISO19011：6.4.8

適合・不適合・是正処置の定義と記録

C

◆適合、不適合、是正処置の定義

1. 適合（ISO/IEC27000）　要求事項を満たしていること
2. 不適合（ISO/IEC27000）　要求事項を満たしていないこと
3. 是正処置（ ISO/IEC27000）
   不適合の原因を除去し、再発を防止するための処置
4. （参考）不適合の除去　→　修正適合

◆記載内容（メモ → 是正処置要求書）

- 監査実施日　・監査メンバー
- 部署、応対者　・監査場所
- 監査の基準　（規格、規程、標準、手順、要求事項）
- 不適合状況　・不適合レベル
- 確認した文書　・確認した記録
- 勧告事項　・是正処置期限

監査所見(用語の定義)

C

◆定義：収集された監査証拠を、監査基準に対して評価した結果

- 注記1）監査所見：適合又は不適合
- 注記2）監査所見を適切に行うことにより、改善の機会の特定又は優れた実践事例の記録を導き得る。
- 注記3）監査基準が法的及びその他の要求事項から選択される場合、監査所見は順守又は不順守と呼ばれる。

◆注

◆監査基準　：　監査証拠と比較する基準として用いる一連の方針、手順または要求事項

◆監査証拠　：　監査基準に関連し、かつ、検証できる、記録、時日の記述又はその他の情報

ISO19011：3.4

監査所見を決定する際に考慮すべき事項

C

B.8.1　監査所見の決定

①前回までの監査記録及び結論のフォローアップ状況記録

②監査依頼者の要求事項

③通常の慣行を超える所見又は改善の機会となる

④サンプルサイズ

⑤監査所見の分類(存在する場合)

B.8.2　適合の記録

① 適合を示す監査基準の識別

② 適合を支持する監査証拠

③ 適合の明示(あれば)

B.8.3　不適合の記録

① 監査基準の記述又は監査基準への参照

② 不適合の明示

③ 監査証拠

④ 関連する監査所見(あれば)

ISO19011：B. 8

是正処置要求書/報告書及び監査報告書　例　C

内部監査　是正処置要求書・報告書

		No.	
被監査所属		監査日	

1 不適合の内容

□重大な不適合　□軽微な不適合　□改善要望

被監査所属長	監査ﾁｰﾑﾘｰﾀﾞ

上記不適合について、是正処置を求めます。提出期限：年　月　日

2 修正・是正処置計画

不適合処置(修正処置)：

不適合の原因：

是正処置：

監　査　報　告　書

作成日：　年　月　日

代表者(承認)	監査責任者	監査ﾘｰﾀﾞ

監査チームリーダ作成　→監査責任者が最終確認　→事業団の代表者の承認

被監査所属(対応者)		
監査メンバー	リーダ：	メンバー：
監査種別	定期　臨時　フォローアップ	
監査日時		
監査目的		

1.　監査の結果概要・監査全体での講評

2.　監査結果

不適合事項	是正処置要求書 No.　～ No.　を参照	

改善要求事項：

発見された不適合の数	
重大な不適合	件
軽微な不適合	件
改 善 事 項	件

是正処置の流れ

C

1. 事故発生から：緊急事態対応手順書

・JISQ15001 付属書A　3.3.7　緊急事態への準備
・ISO/IEC27001　　9.1　監視、測定、分析及び評価
　ISO/IEC27002　　A.16　情報セキュリテイインシデント管理

日常業務 → 従業者・顧客が不適合発見 → 是正処置 事故報告

①当該部署の是正処置
②当該部署・他部署のリスク評価
③フォローアップ

リスク対応計画書

2. 内部監査・外部監査から：内部監査規程

JISQ15001　　9.2　内部監査
ISO/IEC27001　9.2　内部監査

監査の実施 → 内部監査員が不適合を発見 → 是正処置 監査結果報告

ISO/IEC27001:2013　10.1
JISQ15001:2017　　10.1

不適合及び是正処置と他部門への展開

C

不適合!

1. 是正の実施
   a) 必要な処置の実施
   b) 是正処置の有効性をレビュー

■不適合を管理・是正のための処置
■不適合がもたらした結果への対処

3. 不適合の再発又は他所での発生を防止する処置の必要性を評価
1) 不適合のレビュー
2) 不適合の原因の明確化
3) 類似の不適合の有無，又は発生可能性の明確化

2. 規程等の変更（必要な場合）

■検出された不適合のもつ影響に応じた是正処置を実施

4. 処置内容の記録 ■ エビデンスとして，下記の文書化情報を保持:
・不適合の性質及びとった処置（が適正だったか？）、・是正処置の結果（は良好か？）

ISO/IEC27001: 10.1
JISQ15001: 10.1

是正処置への対応（Pマークのみの対応）

C

不適合を指摘の際の対応
- 監査チーム側：**是正処置要求書**を発行、
- 被監査側　　：**是正報告書**で対策案を回答

注：旧規格より、「予防処置」の記述が廃止

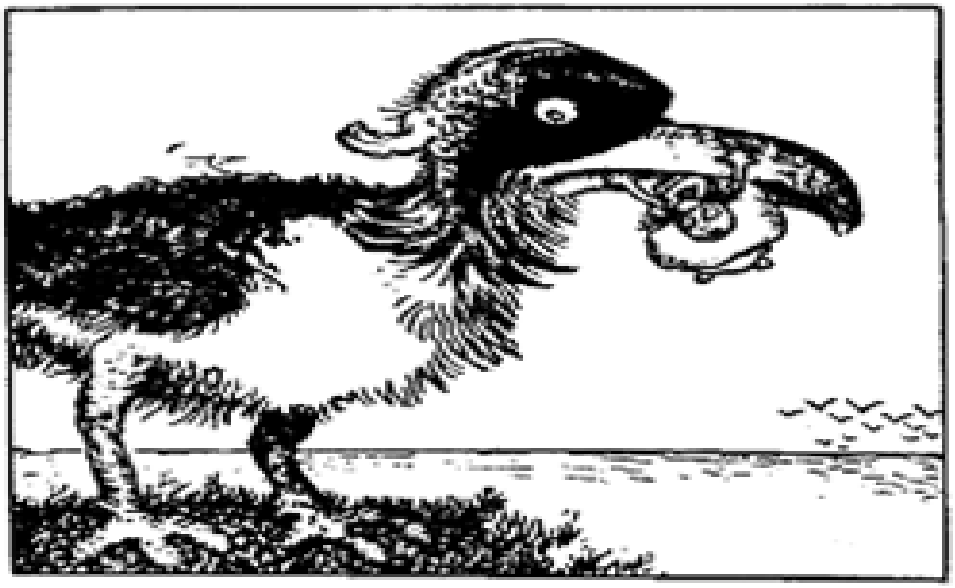
JISQ15001：2017　附属書A.3.8　是正処置

1. 事業者は，不適合に対する是正処置を確実に実施するための責任及び権限を定める手順を確立し，実施し，かつ，維持しなければならない。
2. その手順には，次の事項を含めなければならない。
   a. 不適合の内容を確認する。
   b. 不適合の原因を特定し，是正処置を立案する。
   c. 期限を定め，立案された処置を実施する。
   d. 実施された是正処置の結果を記録する。
   e. 実施された是正処置の有効性をレビューする

参考：規格書本文の定義「10.1　不適合及び是正処置」

coffee break ④

A



監査結果の活用

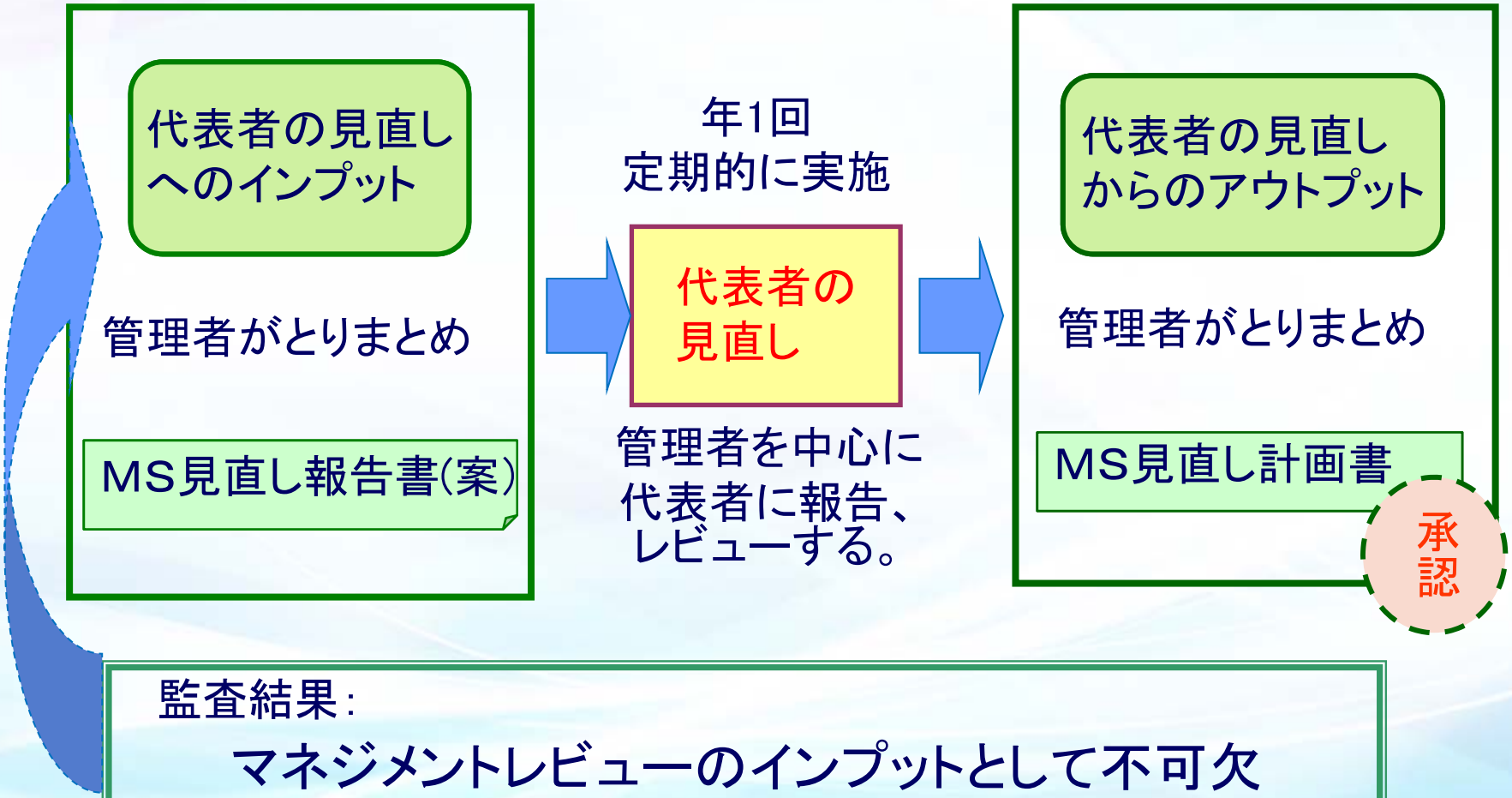
A

1. 経営者へのフィードバック
   - ① 監査責任者には、経営者への報告の義務あり
   - ② PDCAをまわし、Aへつなげていく
2. 被監査部門へのフィードバック
   - ✓ 速やかに適切な処置をする
     - → 是正処置（再発防止）
     - → 他部署での同種・同根の不適合の発生防止
3. マネジメントレビューのインプットとして不可欠
4. 継続的改善に繋げる
   - ① 是正処置とは、現状マネジメントシステムの不具合の是正
   - ② 改善とは、現状マネジメントシステムに不具合は無くとも、経営全体を見渡して、その改善を目指すこと。

代表者による見直し（マネジメントレビュー）

A

・ 組織のマネジメントシステムが引き続き，**適切，妥当かつ有効であること**を確実に
・ **あらかじめ定めた間隔**で，マネジメントシステムをレビュー



監査結果：

マネジメントレビューのインプットとして不可欠

マネジメントレビューのインプット・アウトプット A

インプット

a) 前回までのレビュー結果と採った処置

b) 外部及び内部の課題の変化

例 ・外部：法令規範の改正、意識の変化・技術の変化

・内部：組織の事業領域の変化

c) 監査によるパフォーマンス評価のフイードバック

1) 不適合及び是正処置、
2) 監視及び測定の結果、
3) 監査結果、
4) マネジメントシステム目的の達成

d) 利害関係者からのフィードパック

e) リスクアセスメントの結果及びリスク対応計画

f) 継続的改善の機会

マネジメント レビュー

アウトプット

●マネジメントシステムのあらゆる変更の必要性に関する決定

●マネジメントレビューの結果の証拠として文書化した情報を保持

ISO/IEC27001:及びJISQ15001:
9.3 マネジメントレビュー

継続的改善の定義

A

- ISO/IEC27001：2013, JISQ15001:2017

10.2 継続的改善

組織は，ISMS（もしくは、PMS）の適切性，妥当性及び有効性を継続的に改善しなければならない。

- ISO/IEC27000：2013

2.15 継続的改善

パフォーマンスを向上するために繰り返し行われる活動

- 是正処置と継続的改善の相違

是正処置：対象部門における是正処置完了時点で
不適合が是正されたことの検証を実施する。

継続的改善：現状維持にとどまらず、経営者に対し「マネジメントシステムの見直し」（改善）の提言を含む。

継続的改善についての監査員の姿勢

A

1. マネジメントシステムの**有効性の改善**を監査で測定
   - ✓計画したことが計画したとおりに達成されたか？
   - ✓その結果がハッピーであったか（期待通りであったか）？
2. 大幅な改善でなくても、前より少しでも改善が見られればOK
3. 最高を狙っていると、すぐに天井が見え、改善がすすまなくなる
4. じっくりと腰をすえ、長い目で見守るべき

最後に！：監査員自身の通常の業務スキル向上へのメリット

- ✓ 監査現場でのテクニック・態度・心構えに関わる技量は、内部監査にとどまらず今後の顧客との対応や戦略の提案等にも応用できる。
- ✓ 当該部門の是正処置からリスク評価による他部門への展開は、機関の改善に重要なポイント。
- ✓ 被監査者の立場になった場合でも、内部監査員の指摘に感謝し敬意を表し、よりよい組織になるような努力が望まれる。

監査はなぜ必要か、監査の狙い

A

監査は、組織の(定期)**健康診断**
積極的に、自己の病巣を早期発見

→(自己ﾁｪｯｸ)するための攻撃的機能

PDCAの“C”をまわして、
如何に“A”に結びつけるか
うまくいかなかった場合
→　取り返しのつかない事態
（不祥事、機密事項の漏洩・・・・）

ご清聴ありがとうございました。

（初級編END）

株式会社エム・ピ・オー
代表取締役　森口修逸

URL:　www.m-p-o.co.jp
Email:　info@m-p-o.co.jp

パフォーマンス評価　初級編　資料　（ JISQ19011:2017等）

1. 監査員の個人の資質・行動
2. 監査員の共通の知識及び技能　a)　監査の原則、手順及び方法
3. 監査員の共通の知識及び技能　b)マネジメントシステム及び基準文書
4. 監査員の共通の知識及び技能
   c)組織の概要、
   d)適用される法的及び契約上の要求事項，並びに被監査者に適用されるその他の要求事項
5. 監査に係るリスクについて（その他）
6. 附属書A（分野に固有の監査員の知識及び技能に関する手引き及び例）
   A.5 組織の災害対応力（resilience）、セキュリティ、緊急時対応準備及び
   事業継続マネジメント分野に固有の監査員の知識及び技能の例
   A.7 情報セキュリティマネジメント分野に固有の監査員の知識及び技能の例
7. 附属書B（監査を計画及び実施する監査員に対する追加の手引き）
8. 内部監査の概略フロー
9. 内部監査フロー例
10. マネジメントシステムとは何か？
11. (参考)ISOマネジメントシステムにおける「予防処置」の用語の削除

監査員の個人の資質・行動

1. **倫理的**（公正である、信用できる、誠実である、正直である、分別がある）
2. **広い心**（別な考え方又は視点を進んで考慮する）
3. **外交的**（目的を達成するように人と上手に接する）
4. **観察力**（物理的な周囲の状況、活動を積極的に観察する）
5. **鋭い知覚**（状況を認知し、理解できる）
6. **適応性**（異なる状況に容易に適合）
7. **粘り強い**（根気があり、目的の達成に集中）
8. **決断力**（論理的な理由づけ及び分析に基づき、時宜を得た結論に到達）
9. **自律的**（他人と効果的なやりとりをしながらも独立して行動し、役割を果たす）
10. **不屈の精神**（ときには受け入れられなくても望んで責任を持ち倫理的に行動する）
11. **良い体制づくり**（効果的な時間管理、優先度付け、計画性、及び効率性を発揮する）
12. **改善に前向き**（組織の置かれている状況から学び、よりよい監査結果を目指す）
13. **文化面に敏感**（被監査者の文化を注意深く観察し、敬意を払う）
14. **協働的**（監査チームメンバーと被監査者要員とともに効果的に活動）

赤字新19011の追加分

ISO19011　7.2.2項

監査員の共通の知識及び技能　a)

a)監査の原則、手順及び方法

① 監査の原則，手順・及び方法を適用
② 効果的に作業を計画し・必要な手配を実施
③ 合意した日程内で監査を実施
④ 効果的な面談，聞き取り，観察，並びに文書，記録及びデータの調査によって，情報を収集
⑤ 専門家の意見を理解し，検討
⑥ 監査のためにサンプリング技法を使用することの適切性及びそれによる結果を理解
⑦ 収集した情報の関連性及び正確さを検証
⑧ 監査所見及び監査結論の板拠とするために，監査証拠が十分かつ適切であることを確認
⑨ 監査前見及び監査結諦の信頼性に影響する可能性がある要因を評価
⑩ 監査活動を記録するために作業文書（ワークシート）を適用
⑪　監査所見を文書化し適切な監査報告書を作成
⑫　情報・データ，文書及び記録の機密及びセキュリティを維持
⑬　口頭又は書面で効果的に意思を疎通(自身で，又は通訳及び翻訳の利用を通じて)
⑭　監査に付随するリスクの種類を理解

ISO19011:7.2.3.2　a)

監査員の共通の知識及び技能　b）

b)マネジメントシステム及び基準文書

監査員が監査範囲を理解し、監査基準を適用することが可能になる

① 監査基準として用いるMS規格または他の文書

② 被監査者及び他の組織によるマネジメントシステム規格の適用（該当する場合）

③ マネジメントシステムの構成要素間の相互作用

④ 基準文書間の階層の認識

⑤ 様々な監査状況への基準文書の適用

ISO19011:7.2.3.2　b）

監査員の共通の知識及び技能　c),d)

c)組織の概要:

① 組織の形態・統治・規模・構造，機能及び相互関係。

② 計画，予算化及び人事管理を含む・全般的な事業及びその管理の概念，プロセス及び関連用語。

③ 被監査者の文化的及び社会的側面

d)適用される法的及び契約上の要求事項，並びに被監査者に適用されるその他の要求事項

① 法律及び規制並びにその所管官庁

② 基本的な法律用語

③ 契約及び法的責任

ISO19011:7.2.3.2　c) d)

附属書A（分野に固有の監査員の知識及び技能に関する手引き及び例）

A.1　一般

A.2　情輸送安全マネジメント分野に固有の監査員の知識及び技能の例

A.3　環境マネジメント分野に・・・・・・・・・・・・の例

A.4　品質マネジメント分野に・・・・・・・・・・・・の例

A.5　記録マネジメント分野に・・・・・・・・・・・・の例

A.6　組織の災害対応力（resilience）、セキュリティ、緊急時対応準備及び事業継続マネジメント分野に固有の監査員の知識及び技能の例

A.7　情報セキュリティマネジメント分野に固有の監査員の知識及び技能の例

A.8　労働安全衛生マネジメント分野に・・・・・・・・・・・・の例

ISO19011:付属書A　目次

A.6 組織の災害対応力(resilience)、セキュリティ、緊急時対応準備及び事業継続マネジメント分野に固有の監査員の知識及び技能の例

1. プロセス，科学及び技術の知識⇒　事業継続及び復旧マネジメントの基となる災害への対応力，セキュリティ，緊急時対応準備，緊急時対応
2. 機密情報の収集及び監視の方法
3. 停止・中断事象のリスクの管理
   停止・中断事象の予期，回避，予防，保護，軽減，対応及び停止・中断事象からの復旧
4. a、リスクアセスメント、b.影響度分析、c. リスク対応
   a. 資産の洗出し及び価値評価，リスクの特定，分析，評価
   b. 人的，物理的及び無形の資屋並びに環境関連
   c. 採用可能な・事前及び事後の対応策
5. 要員・現場の実務的な方法及び慣行
   a. 情報の完全性及び影響の受けやすさへの対応方法及び慣行
   b. 情報セキュリティ及び個人情報の保護の関連
   c. 資産保護及び物理的セキュリティ
   d. 予防，抑止及びセキュリティマネジメント
   e. 事態の軽減，対応及び危機管理
   f. 事業継続，緊急事態及び復旧マネジメント
   g. (演習及び試験の手法を含む)パフォーマンスの監視，測定及び報告

A.7 情報セキュリティマネジメント分野に固有の監査員の知識及び技能の例

1. 規格の指針　ISO/IEC 27000, **27001, 27002**, 27003,27004 及び27005 のような、顧客及び利害関係者の要求事項の特定及び評価
2. 情報セキュリティに係る法律及び規制
   例えば，知的財産，組織の記録の内容，保護及び保管，データ保護及び個人情報の保護，暗号による管理策に関する規則規制，対テロ対策，電子商取引，電子署名及びデジタル者名・職場での監督・職場における人間工学・電気通信の傍受及びデータの監視　(例えば，電子メール)，コンピュータの不正利用・電子的な証拠の収集，侵入試験
3. マネジメントシステムの基礎となるプロセス，科学及び技術
4. リスクの特定，分析及び評価及び、技術動向，脅威及びぜい(脆)弱性
5. リスクマネジメントの方法及び慣行
   a. 電子的及び物理的管理策
   b. 情報の完全性及び影響の受けやすさの
   c. 管理策の有効性の測定及び評価
   d. (試験，監査及びレビューを含む)パフォーマンスの測定，監視及び記録

附属書B（監査を計画及び実施する監査員に対する追加の手引き）

（参考）
ISOマネジメントシステムにおける「予防処置」の用語の削除

1．「予防処置」の用語は、ISO/IEC27001：2013やJISQ15001:2017の前規格まで、「是正処置及び予防処置」として掲げられていた。しかし、今回の改正で、「マネジメントシステムそのものが予防措置である」との理由で、従来用いられていた予防処置の用語は削除された。

2．用語は廃止されたが、概念としては、

（1）「組織の状況　箇条4における外部及び内部の課題」及び

（2）「計画段階　箇条6におけるリスク及び機会に関す対処する活動」

に含まれている。

参照　JISQ27001（ISO/IEC27001のJIS版）の巻末の「解説」の「3.1.　**対応国際規格の審議中に特に問題となった事情のb）予防処置(preventive action)の用語の削除**」に説明されている。

JISQ27001（ISO/IEC27001のJIS版）の巻末の「解説」

内部監査の概略フロー

内部監査のプロセス

1. Plan（計画・準備段階）
   - ・監査日程、分担の確定
   - ・チェックリストの作成

2. Do（実施段階）
   - ・客観的証拠の把握
   - ・是正処置要求書の作成・発行

3. Check、Action（フォローアップ段階）
   - ・是正処置完了時点でフォローアップ

内部監査員の資格，監査チームの編成

4. 内部規定に基づき資格付け・認定

5. 監査員（監査メンバー）
   - ・主管業務における実務経験
   - ・個人情報保護ISMS教育の受講実績
   - ・内部監査参加経験

6. チームリーダー
   - ・監査チームの総指揮
   - ・監査対象部門との窓口

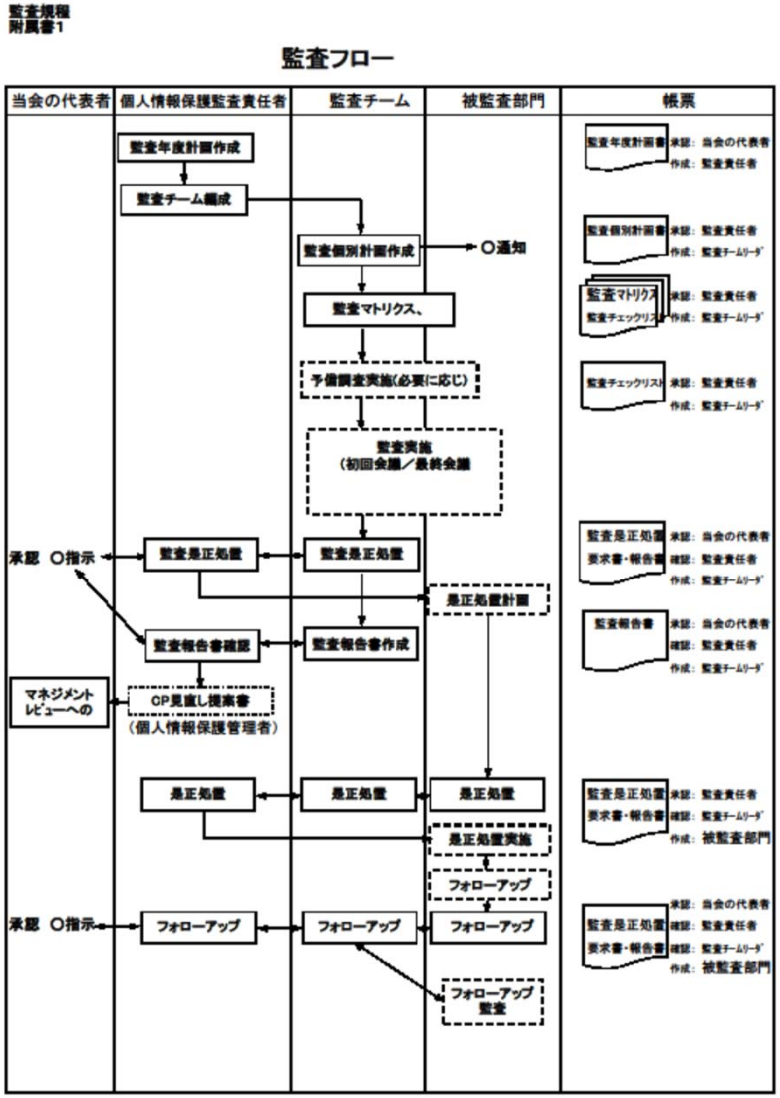
ISO19011

是正処置の責任及び権限一覧例

	緊急事態	運用確認	内部監査	外部監査
原因の特定	個人情報 取扱責任者	所属長	被監査部門 所属長	個人情報保護管理者 （被監査部門所属長）
処置の決定	個人情報 取扱責任者	所属長	被監査部門 所属長	個人情報保護管理者 （被監査部門所属長）
処置の実施	個人情報 取扱責任者	所属長	被監査部門 所属長	個人情報保護管理者 （被監査部門所属長）
処置の確認 効果の確認	個人情報 保護管理者	所属長	監査責任者 監査員	個人情報保護管理者

個人情報保護
マネジメントシステムの場合

内部監査フロー例


監査規程
附属書1
監査フロー
当会の代表者
個人情報保護監査責任者
監査チーム
被監査部門
帳票
監査年度計画作成
監査チーム編成
監査個別計画作成
○通知
監査マトリクス、
予備調査実施(必要に応じ)
監査実施
(初回会議／最終会議
承認 ○指示
監査是正処置
監査是正処置
是正処置計画
監査報告書確認
監査報告書作成
マネジメント
レビューへの
CP見直し提案書
(個人情報保護管理者)
是正処置
是正処置
是正処置
是正処置実施
フォローアップ
承認 ○指示
フォローアップ
フォローアップ
フォローアップ
フォローアップ
監査
監査年度計画書
監査個別計画書
監査マトリクス
監査チェックリスト
監査チェックリスト
監査是正処置
要求書・報告書
監査報告書
監査是正処置
要求書・報告書
監査是正処置
要求書・報告書

監査に係るリスクについて(その他)

1. 監査計画の作成(6.3.2.1項)
   - 監査に起因するリスクを認識する。
     - 例:安全衛生、環境及び品質に影響
       被監査者の製品、サービス、要員又は事業所環境に対し、
       監査チームメンバーの存在が、脅威を引き起こす場合がある
2. 初回会議の実施(6.4.2項)
   - 監査チームメンバーの存在に起因するかもしれない組織に対する
     リスクを管理する方法の紹介
3. 情報の収集および検証(6.4.6項)
   - 証拠の収集中に監査チームが新しいまたは変更された状況及びリスク
     を認識した場合、チームがしかるべく対応することが望ましい。

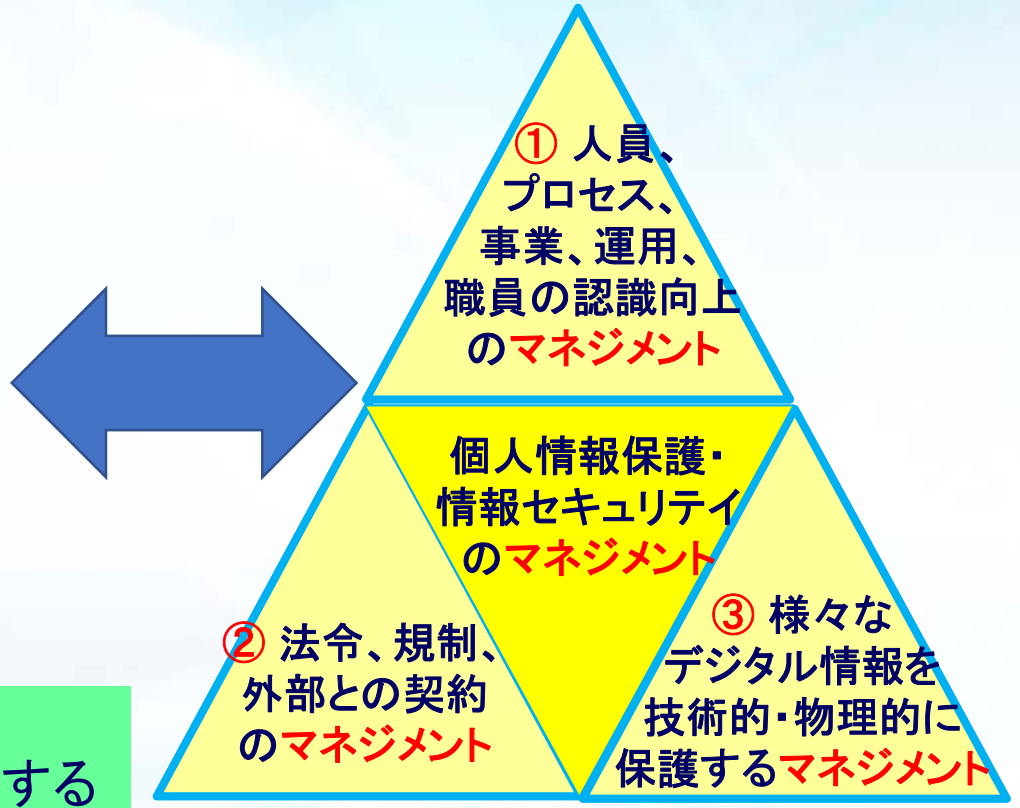
マネジメントシステムとは何か？

マネジメントとは：当該組織にとって文化である対象物を一定の方向に向かせること

組織の方針

- ○組織のニーズ
- ○組織の目的
- ○組織の個人情報保護要求事項
- ○組織が採用しているプロセス
- ○組織の規模及び構造

これらは、
時間とともに組織に対する影響が変化する



マネジメントすべき対象物

・マネジメントシステム実践のキモ

- 範囲（Scope）の明確化
- 職員への定期及び臨時の教育：経営者・管理者や内部監査の各担当者、及び利用者全員
- リスクマネジメントと管理策の有効性測定
- 定期的な監査、特に、内部監査を活用した継続的改善

及び、優秀な経営陣！

図：「ISO/IEC27001実践ガイド」よりMPO作成