ISMS文書とISMSマニュアル　ISO/IEC 27001:2022（JIS Q 27001:2023）にて必要な「文書化する情報」

7.5 文書化した情報

7.5.1 一般

組織のISMSは，次の事項を含まなければならない。

a) この規格が要求する**文書化した情報**

b) ISMSの有効性のために必要であると組織が決定した，**文書化した情報**

JIS Q 27000：2019　情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語

3.19　**文書化した情報**（documented information）

組織（3.50）が管理し，維持するよう要求されている情報，及びそれが含まれている媒体。

注記1　文書化した情報は，あらゆる形式及び媒体の形をとることができ，あらゆる情報源から得ることができる。

注記2　文書化した情報には，次に示すものがあり得る。

- 関連するプロセス（3.54）を含むマネジメントシステム（3.41）
- 組織（3.50）の運用のために作成された情報（文書類）
- 達成された結果の証拠（記録）

※ISMSマニュアルの役割

- **要求事項の網羅と体系化**
  ISO/IEC 27001の各章や附属書Aの管理策を、組織の実情に合わせて整理・文書化する必要があります。これを一元的にまとめるのがマニュアルの役割です。
- **審査対応の基盤資料**
  認証審査では、ISMSの運用状況や管理策の実施状況を説明する必要があります。マニュアルがないと、審査員に体系的に説明できず、認証取得が困難になります。
- **社内教育・運用の指針**
  従業員が情報セキュリティのルールや手順を理解し、実行するための教材としても機能します。マニュアルがあることで、教育や運用が標準化されます。
- **PDCAサイクルの起点**
  ISMSは継続的改善が求められるため、マニュアルは「Plan」の基準となり、改善活動の出発点になります。

4.3 情報セキュリティマネジメントシステムの適用範囲の決定
ISMSの適用範囲は，文書化した情報として利用可能な状態にすること。

5.2 方針
情報セキュリティ方針を確立し，文書化した情報（e項）として利用可能であること。

6.1.2 情報セキュリティリスクアセスメント
リスクアセスメントのプロセスについての文書化した情報を保持すること。

6.1.3 情報セキュリティリスク対応
適用宣言書を作成すること。
リスク対応のプロセスについての文書化した情報を保持すること。

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
目的を確立し，文書化した情報（g項）として利用可能な状態にすること。
目的に関する文書化した情報を保持すること。

7.2 力量
力量の証拠として，適切な文書化した情報（d項）を保持すること。

8.1 運用の計画策定及び管理
プロセスが計画どおりに実施されたという確信をもつために必要とされる，文書化した情報を利用可能な状態にすること。

8.2 情報セキュリティリスクアセスメント
リスクアセスメント結果の文書化した情報を保持すること。

8.3 情報セキュリティリスク対応
リスク対応結果の文書化した情報を保持すること。

9.1 監視測定，分析及び評価
監視測定，分析及び評価の結果の証拠として，文書化した情報を利用可能な状態にすること。

9.2.2 内部監査プログラム
監査プログラムの実施及び監査結果の証拠として，文書化した情報を利用可能な状態にすること。

9.3.3 マネジメントレビューの結果
マネジメントレビューの結果の証拠として，文書化した情報を利用可能な状態にすること。

10.2 不適合及び是正処置
不適合の性質及びそれに対して講じたあらゆる処置（n項）及び是正処置の結果（g項）の証拠として，文書化した情報を利用可能な状態にすること。

A.5.9 情報及びその他の関連
資産の目録情報及びその他の関連資産の目録を，それぞれの管理責任者を含めて作成し，維持すること。

A.5.10 情報及びその他の関連資産の許容される利用
情報及びその他の関連資産の許容される利用に関する規則及び取扱手順は，明確にし，文書化し，実施すること。

A.5.26 情報セキュリティインシデントへの対応
情報セキュリティインシデントは，文書化した手順に従って対応すること。

A.5.31 法令，規制及び契約上の要求事項
情報セキュリティに関連する法令，規制及び契約上の要求事項，並びにこれらの要求事項を満たすための組織の取組を特定し，文書化し，また，最新に保つこと。
情報処理設備の操作手順は，文書化し，必要とする要員に対して利用可能にすること。

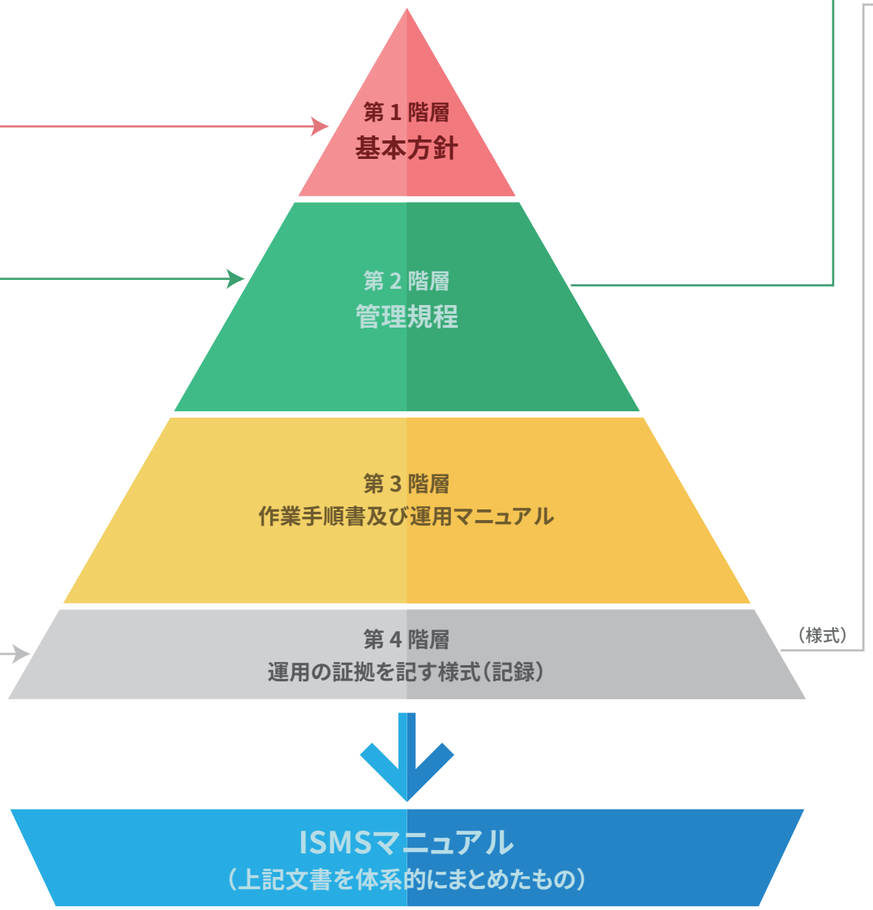
5.37 操作手順書
情報処理設備の操作手順は，文書化し，必要とする要員に対して利用可能にしなければならない。

A.6.6 秘密保持契約又は守秘義務契約
情報保護に対する組織のニーズを反映する秘密保持契約又は守秘義務契約は，特定し，文書化し，定常的にレビューし，要員及びその他の関連する利害関係者が署名すること。

A.8.9 構成管理
ハードウェア，ソフトウェア，サービス及びネットワークのセキュリティ構成を含む構成を確立し，文書化し，実装し，監視し，レビューすること。

A.8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則
セキュリティに配慮したシステムを構築するための原則を確立し，文書化し，維持し，全ての情報システムの開発活動に対して適用すること。

※「A.」は附属書Aを示す



※作り方によっては、第1階層と第2階層の間の文書となる場合もある。

※ 記述内容

ISMSマニュアルは、ISO/IEC27001で要求されている事項を、体系的にまとめたものになります。
（「要求事項の網羅と体系化」）
よって、ISO/IEC27001の規格要求事項に沿った形式で、記述されることが一般的です。
目次としては、一般的にISO/IEC27001の要求事項と同じ項目になります。
記述内容としては、各要求事項に対して、組織がどのような対応をするのか（規定）を記述することになります。
なお、先のように別の規程書にて規定している場合は、その旨を記述することになります。

管理規程の例

ISMSの基本運営に関する規程（ISMS全体の運用に関する基本事項）
例えば、以下の要求事項が該当します。
- 4.3 情報セキュリティマネジメントシステムの適用範囲の決定
- 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
- 8.1 運用の計画策定及び管理
- 9.1 監視測定，分析及び評価
- A.5.31 法令，規制及び契約上の要求事項

リスクマネジメントに関する規程（リスクアセスメントおよびリスク対応に関する事項）
例えば、以下の要求事項が該当します。
- A.5.9 情報及びその他の関連（アクセス制御に関する規程でも可）
- A.5.10 情報及びその他の関連資産の許容される利用（アクセス制御に関する規程でも可）
- 6.1.2 情報セキュリティリスクアセスメント
- 6.1.3 情報セキュリティリスク対応
- 8.2 情報セキュリティリスクアセスメント
- 8.3 情報セキュリティリスク対応

アクセス制御に関する規程（情報システムや情報へのアクセスに関するルール）

物理的なセキュリティに関する規程（施設や区域への入退管理及び設備や機器などに関するルール）
例えば、以下の要求事項が該当します。
- A.5.37 操作手順書
- A.8.9 構成管理

人的なセキュリティに関する規程（従業員の採用から退職まで、教育訓練や懲戒などに関するルール）
例えば、以下の要求事項が該当します。
- 7.2 力量
- A.6.6 秘密保持契約又は守秘義務契約

システムの開発及び保守に関する規程（情報システムの開発や導入、保守に関するルール）
例えば、以下の要求事項が該当します。
- A.6.6 8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則

委託先に関する規程（委託先との契約、評価、管理に関するルール）
例えば、以下の要求事項が該当します。
- A.6.6 秘密保持契約又は守秘義務契約

情報セキュリティインシデントに関する規程（情報セキュリティの事件および事故に関するルール）
例えば、以下の要求事項が該当します。
- A.5.26 情報セキュリティインシデントへの対応

事業継続管理に関する規程
（災害や事故が発生した場合の事業継続計画および情報セキュリティ維持に関するルール）

内部監査に関する規程（ISMSの適合性や有効性を評価する内部監査に関するルール）
例えば、以下の要求事項が該当します。
- 9.2.2 内部監査プログラム

マネジメントレビューに関する規程（トップマネジメントによるISMS見直しに関する手順など）
例えば、以下の要求事項が該当します。
- 9.3.3 マネジメントレビューの結果

是正処置に関する規程（ISMSにおける不適合が発生した場合に関するルール）
例えば、以下の要求事項が該当します。
- 10.2 不適合及び是正処置

文書管理に関する規程（ISMS関連文書の作成や承認、改訂、保管、廃棄に関するルール）

2025.07.18