令和6年度
中小企業サイバーセキュリティ
社内体制整備事業

第4回

第7編：ISMSの構築と対策基準の策定と実施手順【レベル3】

セミナー内容

編	テーマ
第1編	サイバーセキュリティを取り巻く背景
第2編	中小企業に求められるデジタル化の推進とサイバーセキュリティ対策
第3編	これからの企業経営に必要なIT活用とサイバーセキュリティ対策
第4編	セキュリティ事象に対応して組織として対策すべき対策基準と具体的な実施
第5編	各種ガイドラインを参考にした対策の実施

セミナー内容

編	テーマ
第6編	ISMSなどのフレームワークの種類と活用法の紹介
第7編	ISMSの構築と対策基準の策定と実施手順
第8編	具体的な構築・運用の実践
第9編	中小企業が組織として実践するためのスキル・知識と人材育成
第10編	全体総括

セミナー内容

第13章. ISMSの要求事項と構築（LV.3 網羅的アプローチ）

第14章. ISMSの管理策

第15章. 組織的対策

第13章. ISMSの要求事項と構築（LV.3 網羅的アプローチ）

【LV.3 網羅的アプローチ】の概要
【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順
ISMS文書体系（ISMS構築・導入に必要な文書と記録）
ISO/IEC27001の審査準備と審査内容

【LV.3 網羅的アプローチ】の概要

【参照：テキスト13-1.】
P3

概要

特徴

アプローチ手法	特徴	想定される適用ケース
Lv.3 網羅的アプローチ	• 脅威や攻撃手法に対して、網羅的な対策を講じることを目指すアプローチ手法。 • ISMSなどの認証が可能なレベルを目指して、対策基準を策定。	• ISMSのフレームワークに沿った対策基準を策定する場合。

メリット・デメリット

アプローチ手法	メリット	デメリット
Lv.3 網羅的アプローチ	• 可能な限り多くの脅威や攻撃手法に対して対策を講じる。 • 予測できない脅威や新たな攻撃手法に対しても準備ができる状態を維持できる。	• 全体的な実施には時間がかかる。

【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順

ISO/IEC27001 各要求事項の概要

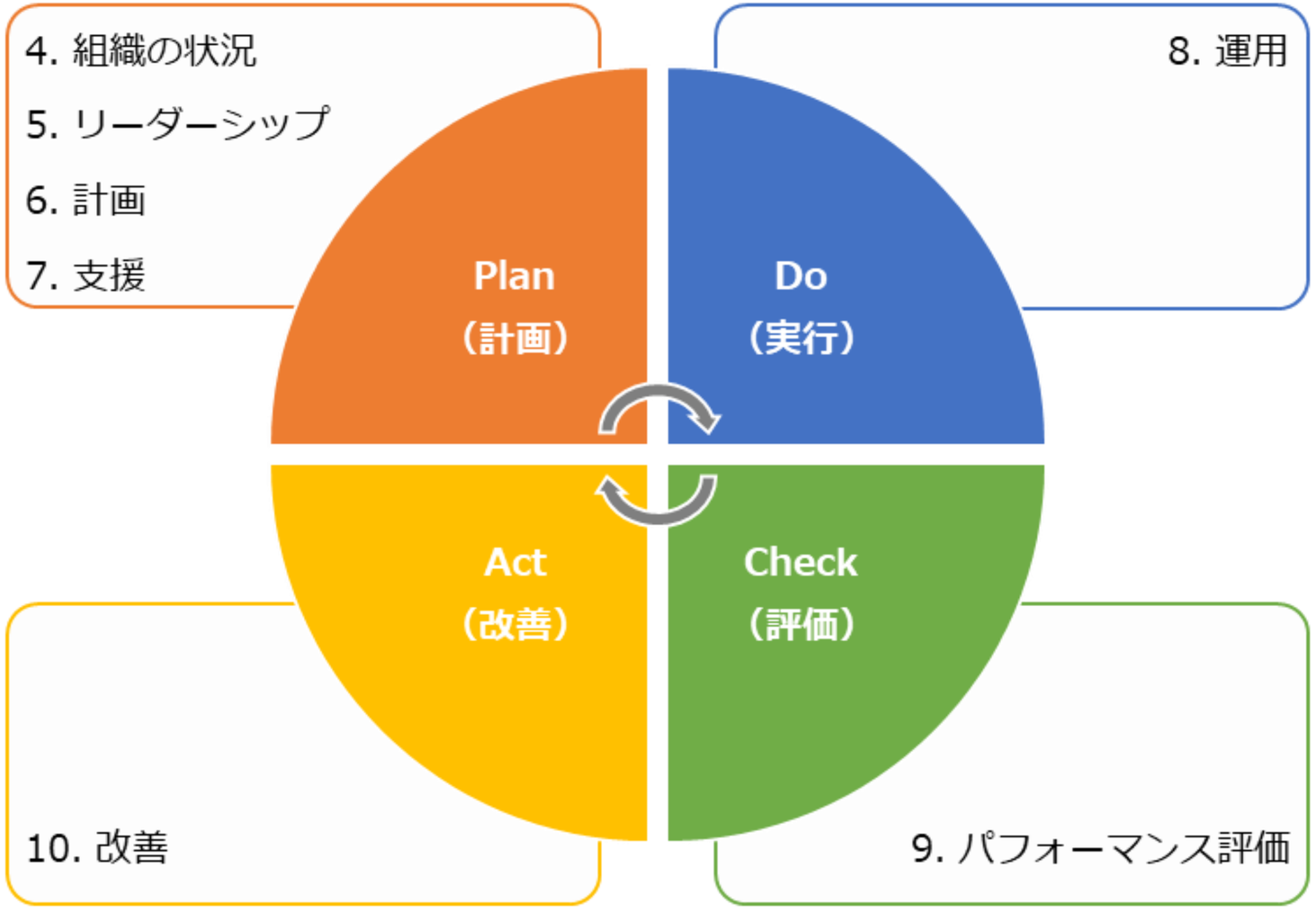
【参照：テキスト13-2-1.】
P4

構成	概要
1. 適用範囲	ISMS運用のための要求事項の規程
2. 引用規格	ISO/IEC 27000（ISMSの概要と用語）を引用する
3. 用語および定義	用語および定義は、ISO/IEC 27000に定めている
4. 組織の状況	組織の内情などを把握した上で、適用範囲の決定を要求する
5. リーダーシップ	トップマネジメントが実施するべきことのまとめ
6. 計画	ISMSの計画を立てる（PDCAのP）
7. 支援	構成員の教育など、組織が行うべきサポートの要求
8. 運用	ISMSを実行する際の要求（PDCAのD）
9. パフォーマンス評価	適切に構築・運用できているかを評価する（PDCAのC）
10. 改善	是正処置や不適格があった場合の対処法（PDCAのA）

【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順

ISMSの確立、運用、監視

【参照：テキスト13-2-1.】
P5



【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順

ISMS：4. 組織の状況

【参照：テキスト13-2-2.】
P5

4. 組織の状況	作成文書（例）	テキスト
4.1 組織及びその状況の理解 （組織の目的に関連する内部・外部課題）	• 外部及び内部の課題	P6, P7
4.2 利害関係者のニーズ及び期待の理解 （利害関係者から要求される情報セキュリティ）	• 利害関係者のニーズ及び期待	P7, P8
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 （物理的配置、論理的構成を含め、適用範囲を決定）	• ISMS適用範囲 • レイアウト図 • ネットワーク図	P8, P9, P10
4.4 情報セキュリティマネジメントシステム （PDCAに基づく運用）	―	―

【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順

ISMS：5. リーダーシップ

【参照：テキスト13-2-3.】
P11

5. リーダーシップ	作成文書（例）	テキスト
5.1 リーダーシップ及びコミットメント （トップが責任を持って実行すること）	―	P11, P12
5.2 方針 （情報セキュリティ方針の作成）	• 情報セキュリティ方針	P13
5.3 組織の役割、責任及び権限 （役割と権限の割り当てと、それの文書化）	• ISMSの運用組織図 • 責任者または部門の名称と役割を明記した文書	P14, P15

【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順

ISMS：6. 計画

【参照：テキスト13-2-4.】
P15

6. 計画	作成文書（例）	テキスト
6.1 リスク及び機会に対する活動 （情報資産に対するリスクの決定と対応手順の確立）	• 資産目録（情報資産管理台帳） • リスクアセスメント結果報告書 • 適用宣言書 • リスク対応計画	P16, P17, P18, P19, P20, P21, P22
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 （目的の確立と、達成のための計画策定）	• ISMS有効性評価表	P22, P23, P24
6.3 変更の計画策定 （変更が必要な時は計画的に）	―	―

【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順

ISMS：7. 支援

【参照：テキスト13-2-5.】
P24

7. 支援	作成文書（例）	テキスト
7.1 資源 （必要資源【人、物、金、情報】の決定）	―	P25, P26
7.2 力量 （要員の力量を定義し、評価する。結果に応じて教育を計画と実施）	• 力量確認表 • 教育計画書 • 理解度確認テスト • 教育実施記録	P26, P27, P28, P29, P30
7.3 認識 （適用範囲のすべての要員が認識しなければならい内容）	―	P30
7.4 コミュニケーション （意思疎通に必要なプロセスの確立）	―	P30, P31
7.5 文書化した情報 （文書化した情報の作成、更新、管理）	―	P31, P32

【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順

ISMS：8. 運用

【参照：テキスト13-2-6.】
P33

8. 運用	作成文書（例）	テキスト
8.1 運用の計画及び管理 （計画した活動の一覧表作成）	• ISMS年間計画表	P33, P34, P35
8.2 情報セキュリティリスクアセスメント （実施したリスクアセスメントプロセス結果の文書化）	• リスクアセスメント結果報告書	P35
8.3 情報セキュリティリスク対応 （実施したリスク対応計画結果の文書化）	• リスク対応計画	P35, P36

【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順

ISMS：9. パフォーマンス評価

【参照：テキスト13-2-7.】
P36

9. パフォーマンス評価	作成文書（例）	テキスト
9.1 監視、測定、分析及び評価 （情報セキュリティのパフォーマンスとISMSの有効性の評価）	• ISMS有効性評価表	P36, P37
9.2 内部監査 （ISMSの適合性、有効性についての監査）	• 内部監査チェックリスト • 内部監査計画書 • 内部監査結果報告書	P37, P38, P39, P40
9.3 マネジメントレビュー （トップマネジメントが、ISMSの有効性を評価する）	• マネジメントレビュー報告書	P40, P41, P42

【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順

ISMS：10. 改善

【参照：テキスト13-2-8.】
P42

10. 改善	作成文書（例）	テキスト
10.1 継続的改善 （ISMSのPDCAサイクルを継続して実施し、情報セキュリティパフォーマンスを向上させるために必要な改善を継続していく）	―	―
10.2 不適合及び是正処置 （不適合が発生した際の是正処置の実施）	• 是正要求書兼回答書	P43, P44, P45

ISMS文書体系（ISMS構築・導入に必要な文書と記録）

ISMS文書としての策定内容とポイント

【参照：テキスト13-3-1.】
P46

ISO/IEC 27001:2022附属書Aの管理策

カテゴリ	項目数	管理策
組織的管理策	37	組織として取り組む必要のある管理策。 組織としてのルールを定めるもの。
人的管理策	8	従業員に関して取り組む必要のある管理策。 情報セキュリティの意識向上や教育など。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。 オフィス、部屋および施設の物理的セキュリティや監視、装置の保守など。
技術的管理策	34	技術面での管理策。 ネットワーク、システム全般のセキュリティ、データの暗号化、バックアップ、脆弱性管理、ログ管理、マルウェア対策など。

ISMS文書体系（ISMS構築・導入に必要な文書と記録）

【参照：テキスト13-3-2.】
P47

ISMSの要求事項

- ISO/IEC 27001の要求事項

要求事項	内容
ISMSの構築	組織は、ISMSを計画し、導入する。
リスクアセスメント	組織内の情報セキュリティリスクを識別し、そのリスクを評価する。
リスク対応策の実施	評価されたリスクに対して、適切な対応策を実施する必要がある。
ISMSの維持と改善	ISMSは、PDCAサイクルに従って運用し、継続的に監視・評価され、必要に応じて改善していく。
認証取得のための要件遵守	ISO/IEC 27001の認証を取得するには、これらの要求事項をすべて満たす必要がある。

ISMS文書体系（ISMS構築・導入に必要な文書と記録）

ISMSの管理策

【参照：テキスト13-3-2.】
P48

- 情報セキュリティマネジメントの具体的な管理策を示す規格がISO/IEC 27002。
- ISO/IEC 27002の管理策を取り入れ、リスク低減のための目的と管理策で構成されているもの（リスト）が「ISO/IEC 27001附属書Ａ」
- この「ISO/IEC 27001附属書Ａ」は、要求事項を補完するガイドラインとして位置づけされている。
- 全ての管理策を採用する必要はないが、採用しない理由を明確にしなければならない。

ISMS文書体系（ISMS構築・導入に必要な文書と記録）

ISMSの管理策における属性

【参照：テキスト13-3-2.】
P51

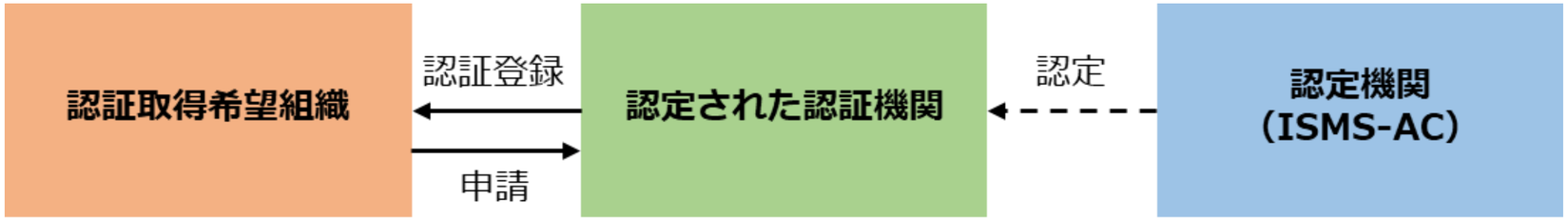
カテゴリ	属性数	属性
管理策タイプ	3	＃予防、＃検知、＃是正
情報セキュリティ特性	3	＃機密性、＃完全性、＃可用性
サイバーセキュリティ概念	5	＃識別、＃防御、＃検知、＃対応、＃復旧
運用機能	15	＃ガバナンス、＃資産管理、＃情報保護、＃人的資源のセキュリティ、＃物理的セキュリティ、＃システムおよびネットワークのセキュリティ、＃アプリケーションのセキュリティ、＃セキュリティを保った構成、＃識別情報およびアクセス管理、＃脅威およびぜい弱性の管理、＃継続、＃供給者関係のセキュリティ、＃法および順守、＃情報セキュリティ事象管理、＃情報セキュリティ保証
セキュリティドメイン	4	＃ガバナンスおよびエコシステム、＃保護、＃防御、＃対応力

ISO/IEC27001の審査準備と審査内容

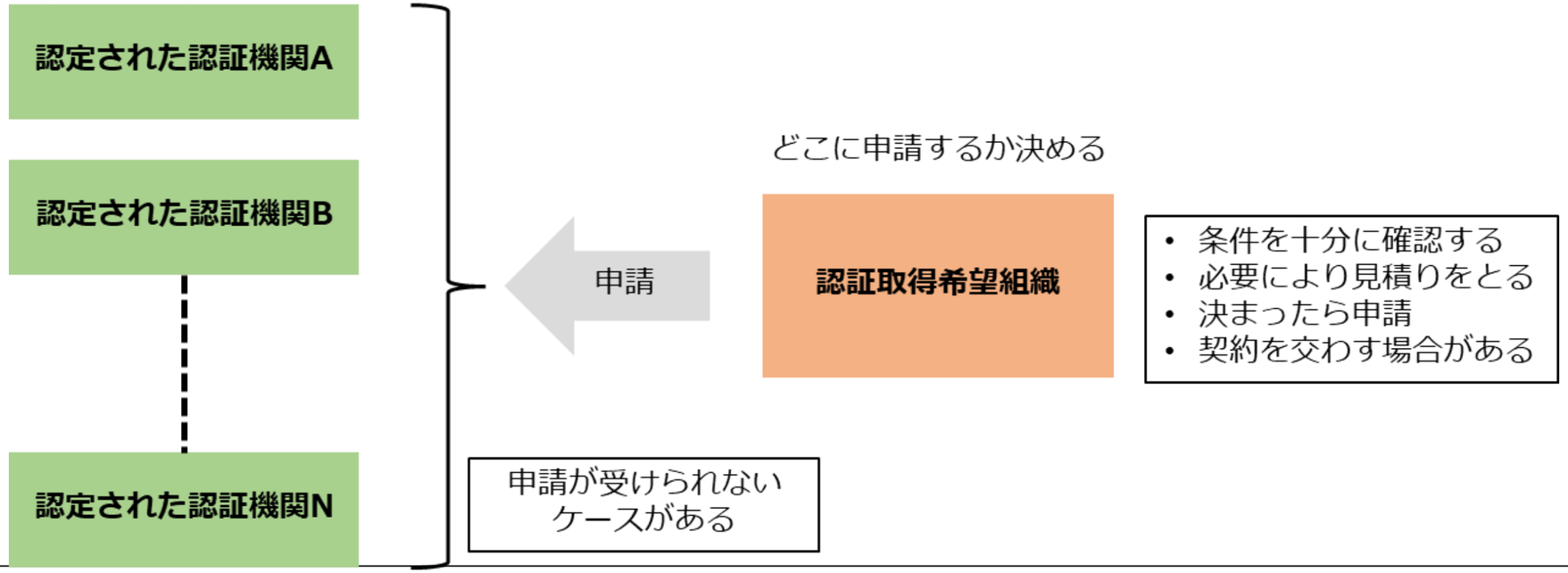
ISO/IEC27001の認証機関の選定と申し込み

【参照：テキスト13-4-1.】
P53

認証取得の申請先



認証機関の選択



ISO/IEC27001の審査準備と審査内容

ISO/IEC27001の審査事前準備

【参照：テキスト13-4-2.】
P54

ISMSの構築ステップ

1. 適用範囲の決定
2. 情報セキュリティ方針の策定
3. 体制の確立
4. ISMS文書化
5. リスクアセスメントの実施
6. 従業員の教育
7. 内部監査
8. マネジメントレビュー

ISO/IEC27001の審査準備と審査内容

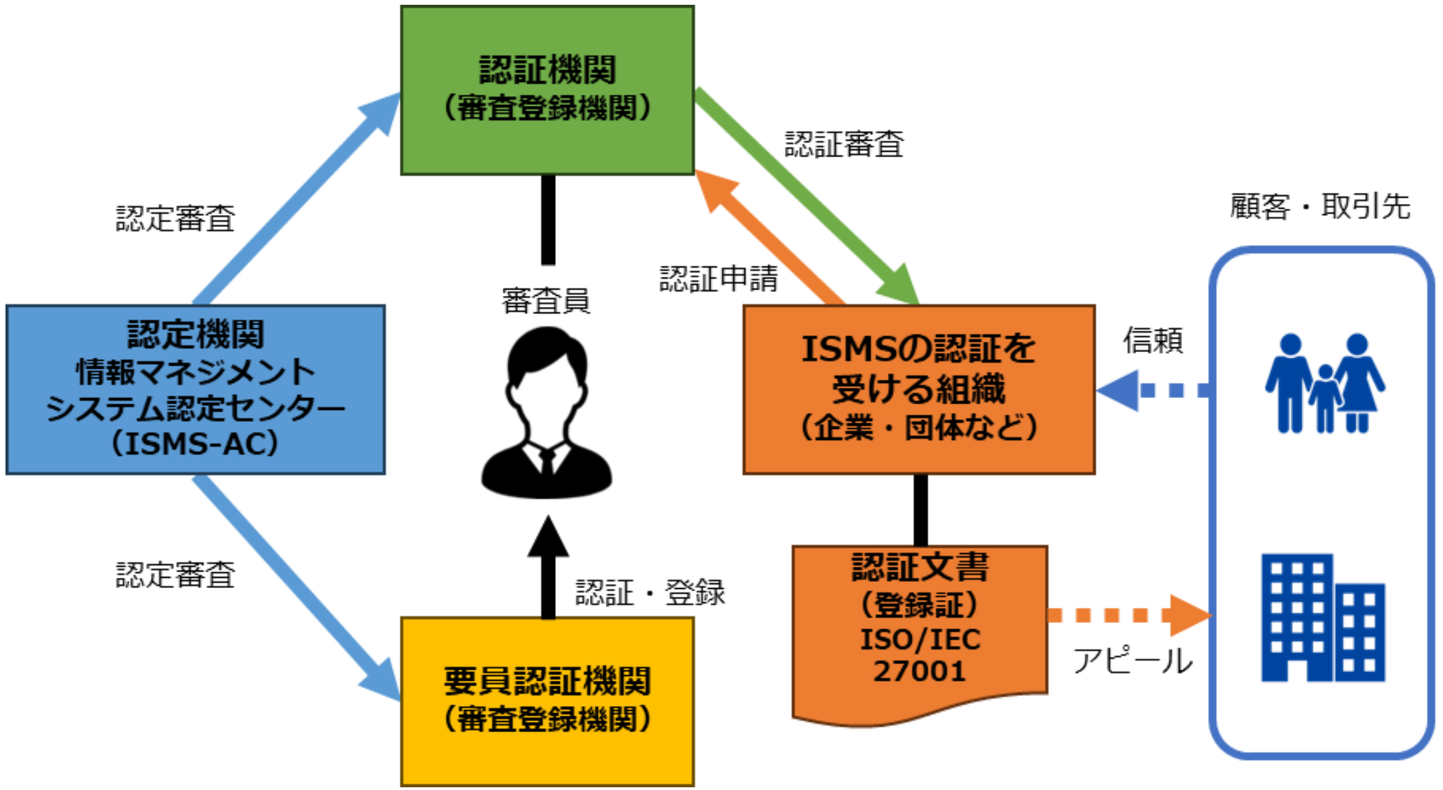
ISO/IEC27001の審査（第一段・第二段）

【参照：テキスト13-4-3.】
P55

「ISMS認証」は、組織のISMSがISO/IEC 27001に準拠しているかを第三者認証機関が審査する制度。この評価は国際的な「ISMS適合性評価制度」のもとで行われる。

認定と認証

認定	認定機関が認証機関を審査し、認証を遂行する能力のあることを公式に承認する行為を認定と言う。
認証	第三者が文書で保証する手続きを認証と言う。



ISO/IEC27001の審査準備と審査内容

ISO/IEC27001の審査（第一段・第二段）

【参照：テキスト13-4-3.】
P56

ISMS認証審査プロセス

ステップ	申請	審査日程の確認	初回認証審査	認証登録	報告・公開
概要	新規取得する際、今までと異なる認証機関で受診する場合は、申請が必要です。	組織と認証機関との間で、審査日程の確認を行います。	新規の場合は原則として1次審査と2次審査の2回で実施されます。	審査の結果、適合していることが確認されると認証書が発行され、登録完了となります。	認証された旨が認証機関からISMS-ACに報告され次第、ISMS-ACホームページで公開されます。

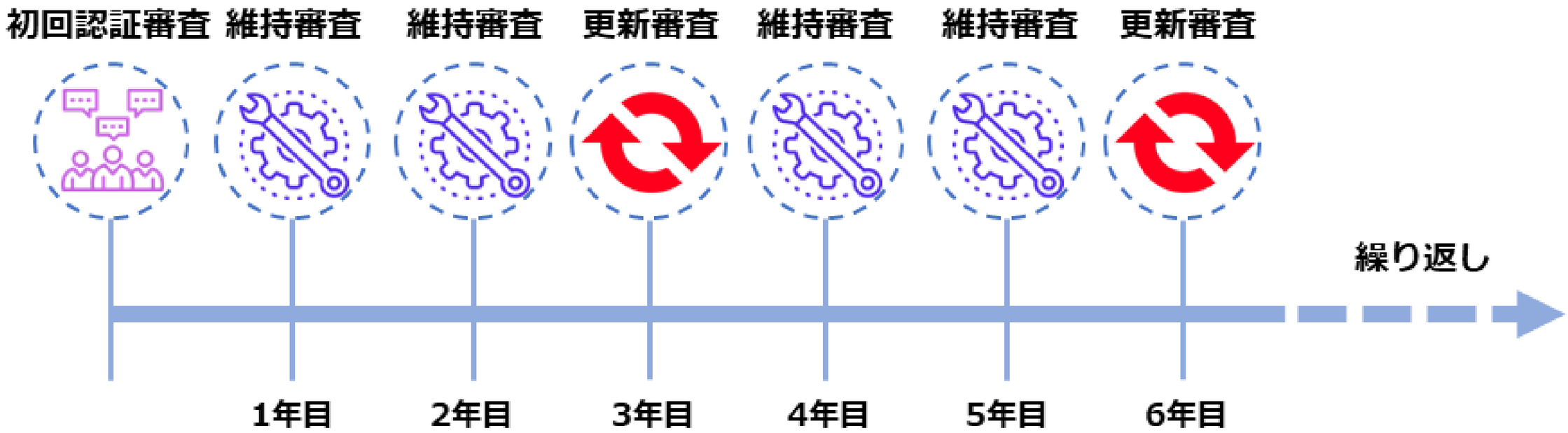
ISO/IEC27001の審査準備と審査内容

ISO/IEC27001の維持審査・再認証審査

【参照：テキスト13-4-4.】
P57

ISMS認証の維持および更新審査プロセス

- 年に1回以上の維持審査（サーベイランス審査）
- 3年ごとに認証の有効期限を更新するための更新審査



第14章. ISMSの管理策

管理策の分類と構成

管理策の分類と構成

管理策：ISO/IEC 27002

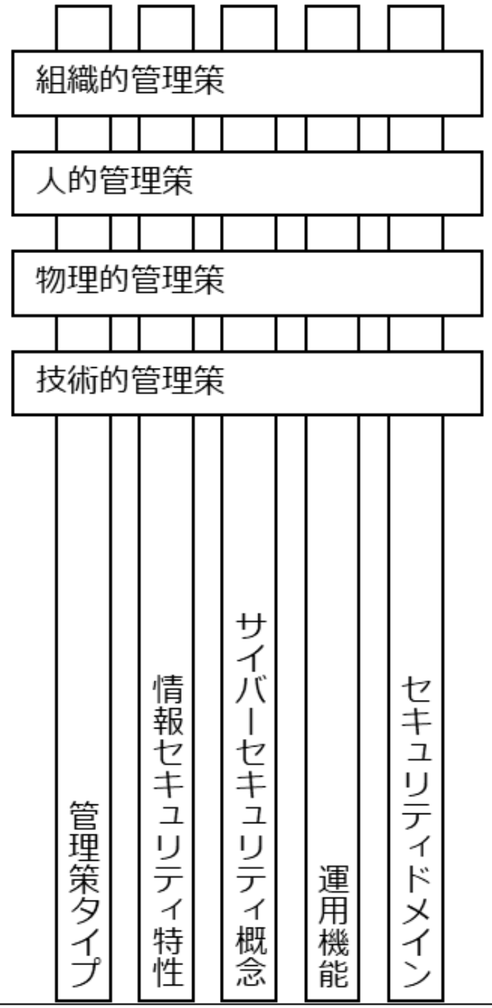
【参照：テキスト14-1-1.】
P60

ISO/IEC 27002:2013

- 情報セキュリティのための方針群
- 情報セキュリティのための組織
- 人的資源のセキュリティ
- 資産の管理
- アクセス制御
- 暗号
- 物理的及び環境的セキュリティ
- 運用のセキュリティ
- 通信のセキュリティ
- システムの取得、開発及び保守
- 供給者関係
- 情報セキュリティインシデント管理
- 事業継続マネジメントにおける情報セキュリティの側面
- 遵守

改訂

ISO/IEC 27002:2022



管理策の分類と構成

管理策のテーマと属性

【参照：テキスト14-1-2.】
P61, P62

カテゴリ	属性数	関連するガイドラインなど
管理策タイプ	3	ー
情報セキュリティ特性	3	ISO/IEC 27001
サイバーセキュリティ概念	5	サイバーセキュリティフレームワーク
運用機能	15	ISO/IEC 27002:2022
セキュリティドメイン	4	ー

各テーマより管理策の例示

- ISO/IEC 27002 附属書Aに記載
- 使い方は別紙、ISMS管理策の属性説明資料を参照

管理策の分類と構成

対策基準と実施手順の作成方法

【参照：テキスト14-1-3.】
P63

1. 管理策の決定
   a. リスクアセスメント結果を考慮し、適切なリスク対応を選択する。
   b. 実施に必要なすべての管理策を決定する。
2. 管理策の検証
   a. 必要な管理策の見落としがないか検証する。
3. 適用宣言書の作成
   a. 必要な管理策と実施する理由を記載する。
   b. 管理策をすでに実施しているかを記載する。
   c. 管理策を除外した理由を記載する。
4. 実施手順の作成
   a. 具体的な実施手順を作成する。

第15章. 組織的対策

作成する候補となる実施手順書類について

組織的対策として重要となる実施項目

作成する候補となる実施手順書類について

【参照：テキスト15-1.】
P67

5.1 情報セキュリティのための方針群

情報セキュリティ方針およびトピック固有の個別方針は、これを定義し、経営陣によって承認され、発行し、関連する要員および関連する利害関係者へ伝達し認識され、計画した間隔でおよび重要な変化が発生した場合にレビューしなければならない。

【実施手順：テキストP72】

5.2 情報セキュリティの役割および責任

情報セキュリティの役割および責任を、組織の要求に従って定め、割り当てなければならない。

【実施手順：テキストP73】

5.3 職務の分離

相反する職務および責任範囲は、分離しなければならない。

【実施手順：テキストP74】

作成する候補となる実施手順書類について

【参照：テキスト15-1.】
P67, P68

5.4 経営陣の責任

経営陣は、組織の確立された情報セキュリティ方針、トピック固有の個別方針および手順に従った情報セキュリティの適用を、すべての要員に要求しなければならない。

【実施手順：テキストP74】

5.5 関係当局との連絡

組織は、関係当局との連絡体制を確立および維持しなければならない。

【実施手順：テキストP74】

5.6 専門組織との連絡

組織は、情報セキュリティに関する研究会または会議、および情報セキュリティの専門家からの協会・団体との連絡体制を確立し維持しなければならない。

【実施手順：テキストP75】

作成する候補となる実施手順書類について

【参照：テキスト15-1.】
P68

5.7 脅威インテリジェンス

情報セキュリティの脅威に関連する情報を収集および分析し、脅威インテリジェンスを構築しなければならない。

【実施手順：テキストP81】

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

情報セキュリティをプロジェクトマネジメントに組み入れなければならない。

【実施手順：テキストP76】

5.9 情報及びその他の関連資産の目録

管理責任者を含む情報およびその他の関連資産の目録を作成し、維持しなければならない。

【実施手順：テキストP81】

作成する候補となる実施手順書類について

【参照：テキスト15-1.】
P68

5.10 情報及びその他の関連資産の利用の許容範囲

情報およびその他の関連資産の利用並びに取扱い手順の許容範囲に関する規則は、明確にし、文書化し、実施しなければならない。

【実施手順：テキストP82】

5.11 資産の返却

要員および必要に応じてその他の利害関係者は、雇用、契約または合意の変更または終了時に、自らが所持する組織の資産のすべてを返却しなければならない。

【実施手順：テキストP83】

5.12 資産の分類

情報は、機密性、完全性、可用性および関連する利害関係者の要求事項に基づく組織の情報セキュリティの要求に従って分類しなければならない。

【実施手順：テキストP77】

作成する候補となる実施手順書類について

【参照：テキスト15-1.】
P68, P69

5.13 情報のラベル付け

情報のラベル付けに関する適切な一連の手順は、「5.12 情報の分類」で確立した分類体系に従って策定し、実施しなければならない。
【実施手順：テキストP77】

5.14 情報転送

情報転送の規則、手順または合意を、組織内および組織と他の関係者との間のすべての種類の転送設備に関して備えなければならない。
【実施手順：テキストP77】

5.15 アクセス制御

情報およびその他の関連資産への物理的および論理的アクセスを制御するための規則を、業務および情報セキュリティの要求事項に基づいて確立し、実施しなければならない。
【実施手順：テキストP79】

作成する候補となる実施手順書類について

【参照：テキスト15-1.】
P69

5.16 識別情報の管理

組織の情報およびその他の関連資産にアクセスする個人およびシステムを一意に特定できるようにし、アクセス権を適切に割り当てなければならない。

【実施手順：テキストP79】

5.17 認証情報

認証情報の割り当ておよび管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理しなければならない。

【実施手順：テキストP79】

5.18 アクセス権

情報およびその他の関連資産へのアクセス権は、アクセス制御に関する組織のトピック固有の個別方針および規則に従って、提供、レビュー、変更および削除しなければならない。

【実施手順：テキストP80】

作成する候補となる実施手順書類について

【参照：テキスト15-1.】
P69

5.19 供給者関係における情報セキュリティ

供給者の製品またはサービスの使用に関連する情報セキュリティリスクを管理するためのプロセスおよび手順を定義し実施しなければならない。

【実施手順：テキストP89】

5.20 供給者と合意における情報セキュリティの取扱い

供給者関係の種類に応じて、各供給者と、関連する情報セキュリティ要求事項を確立し合意をとらなければならない。

【実施手順：テキストP89】

5.21 ICTサプライチェーンにおける情報セキュリティの管理

ICT 製品およびサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセスおよび手順を定め、実施しなければならない。

【実施手順：テキストP90】

作成する候補となる実施手順書類について

【参照：テキスト15-1.】
P69, P70

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

サービスの供給者の情報セキュリティの実践およびサービス提供の変更を定常的に監視し、レビューし、評価し、管理しなければならない。

【実施手順：テキストP93】

5.23 クラウドサービスの利用における情報セキュリティ

クラウドサービスの取得、利用、管理および終了のプロセスを、組織の情報セキュリティ要求事項に従って定めなければならない。

【実施手順：テキストP83】

5.24 情報セキュリティインシデント管理の計画及び準備

セキュリティインシデント管理のプロセス、役割および責任を定義、確立および伝達し、セキュリティインシデント管理の計画を定めなければならない。

【実施手順：テキストP84】

作成する候補となる実施手順書類について

【参照：テキスト15-1.】
P70

5.25 情報セキュリティ事象の評価及び決定

情報セキュリティ事象に対して、セキュリティインシデントに分類するか否かを決定するための評価を実施しなければならない。

【実施手順：テキストP85】

5.26 情報セキュリティインシデントへの対応

セキュリティインシデントに対し、文書化した手順に従って対応しなければならない。

【実施手順：テキストP85】

5.27 情報セキュリティインシデントからの学習

セキュリティインシデントから得られた知識を、情報セキュリティ管理策を強化し、改善するために用いなければならない。

【実施手順：テキストP86】

作成する候補となる実施手順書類について

【参照：テキスト15-1.】
P70

5.28 証拠の収集

情報セキュリティ事象に関連する証拠の特定、収集、取得および保存のための手順を定め、実施しなければならない。

【実施手順：テキストP87】

5.29 事業の中断・阻害時の情報セキュリティ

事業の中断・阻害時に情報セキュリティを適切なレベルに維持するための方法を定めなければならない。

【実施手順：テキストP87】

5.30 事業継続のためのICTの備え

事業継続の目的およびICT 継続の要求事項に基づいて、ICT の備えを計画、実施、維持および試験しなければならない。

【実施手順：テキストP88】

作成する候補となる実施手順書類について

【参照：テキスト15-1.】
P70, P71

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する法令や契約事項を特定・文書化し、遵守しなければならない。

【実施手順：テキストP90】

5.32 知的財産権

知的財産権を保護するための適切な手順を実施しなければならない。

【実施手順：テキストP91】

5.33 記録の保護

記録を、消失、破壊、改ざん、認可されていないアクセスおよび不正な流出から保護しなければならない。

【実施手順：テキストP91】

作成する候補となる実施手順書類について

【参照：テキスト15-1.】
P71

5.34 プライバシー及びPIIの保護

適用される法令、規制および契約上の要求事項に従って、プライバシーの維持およびPII の保護に関する要求事項を特定し、満たさなければならない。

【実施手順：テキストP93】

5.35 情報セキュリティの独立したレビュー

情報セキュリティおよびその実施の管理に対する組織の取組について、あらかじめ定めた間隔で、または重大な変化が生じた場合に、独立したレビューを実施しなければならない。

【実施手順：テキストP93】

作成する候補となる実施手順書類について

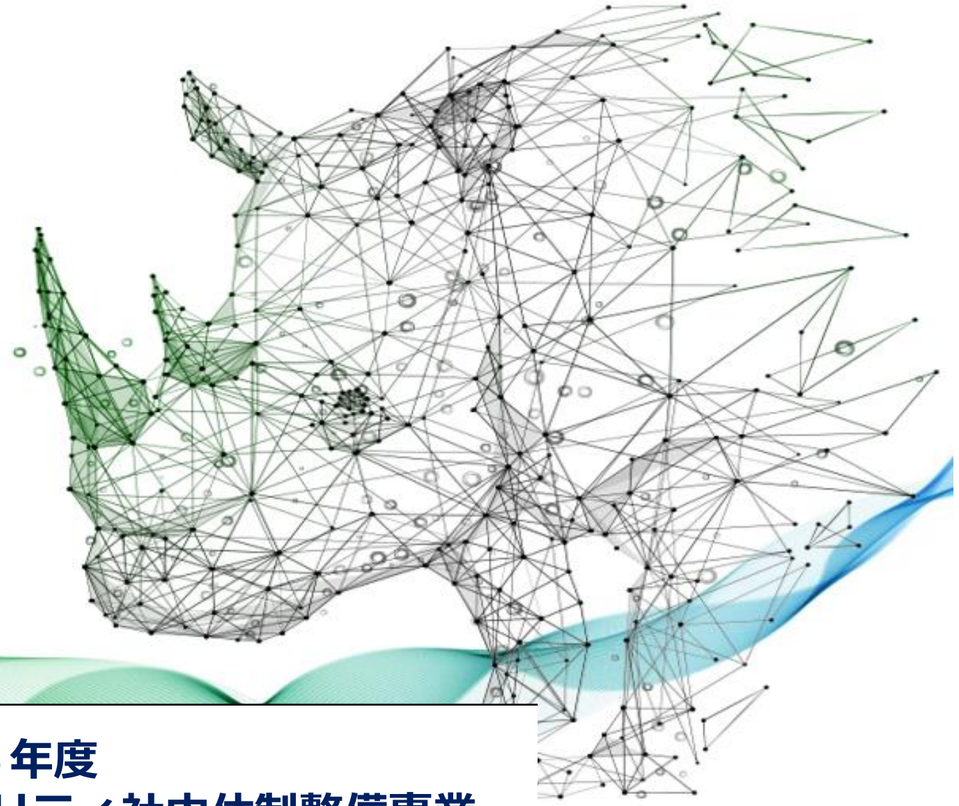
【参照：テキスト15-1.】
P71

5.36 情報セキュリティのための方針群、規則及び標準の順守

組織の情報セキュリティ方針、トピック固有の個別方針、規則および標準を順守していることを定期的にレビューしなければならない。
【実施手順：テキストP94】

5.37 操作手順書

情報処理設備の操作手順を文書化し、必要な要員に対して利用可能な状態としなければならない。
【実施手順：テキストP94】



令和６年度
中小企業サイバーセキュリティ社内体制整備事業