Project Charter

リニューアルプロジェクト

PMO：一般社団法人マネジメントシステム品質協会

MSQA
Management System Quality Association

はじめに

近年、情報セキュリティを取り巻く脅威の高度化・多様化や事業環境の変化に伴い、従来のISMS運用では実効性や効率性の確保が困難になりつつある。また、規程類や様式類の増加による運用負荷の増大、審査対応を目的とした形式的作業の常態化、リスク評価の形骸化などが、組織本来のセキュリティ強化活動を阻害する要因となっている。これらの課題を解消し、経営に資するISMSへと進化させるため、本プロジェクトではISMSの再構築（リニューアル）を実施する。具体的には、規程類・様式類の整理統合によるスリム化、リスクマネジメントプロセスの改善と事象ベースアプローチの導入により実効性を高めるとともに、審査対応のためだけの作業を排除する。さらに、マネジメントシステムおよび管理策のパフォーマンスを定量的に評価し、数値に基づく目標設定と計画策定を行うことで、客観的かつ継続的な改善サイクルを確立する。加えて、内部監査のアウトソーシング活用を含め監査品質を向上させ、組織全体の情報セキュリティ水準と経営品質の持続的向上を図る。

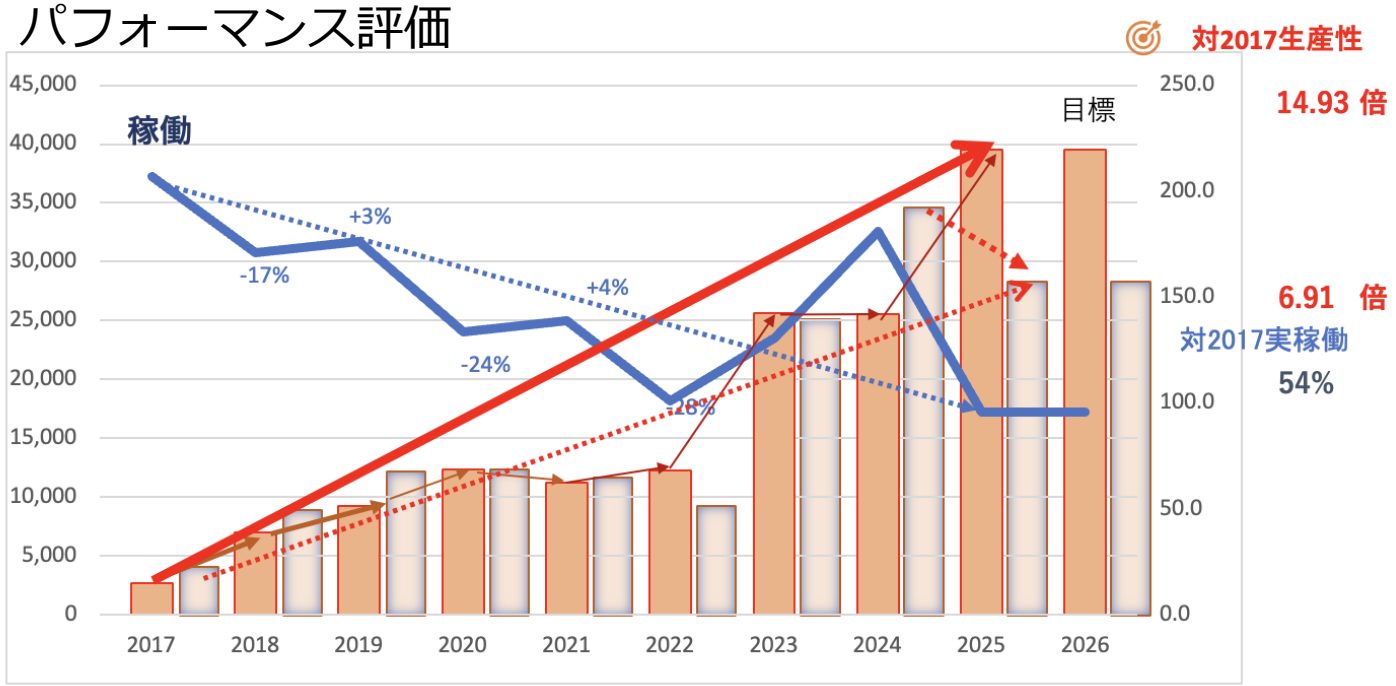
目的：ビジネスを支えるISMSにリニューアルする

- 収益の源泉としてリスクを捉え、リスクのマイナスの影響を抑えつつ、リターンの最大化を追求する
- リスクを全社的視点で合理的かつ最適な方法で管理しリターンを最大化することで、企業価値を高める

出典：（経産省）先進企業から学ぶ事業リスクマネジメント実践

マネジメントシステムの有効性

パフォーマンス評価



リスクを適切に管理して無理・無駄を削減する。情報の機密性・完全性・可用性をバランスよく維持し生産性向上（リターンを最大化）する

$$\text{生産性} = \frac{\text{売上}}{\text{稼働時間}}$$

生産性革命
働き方改革
イノベーション
ニューノーマル

マネジメントとは、成果を上げるために経営資源（ヒト・モノ・カネ）を効率的に活用し、リスク管理のもとに、「目標」や「ミッション」の達成を目指すことである。

変更の計画概要（ISMS 要求事項6.3）

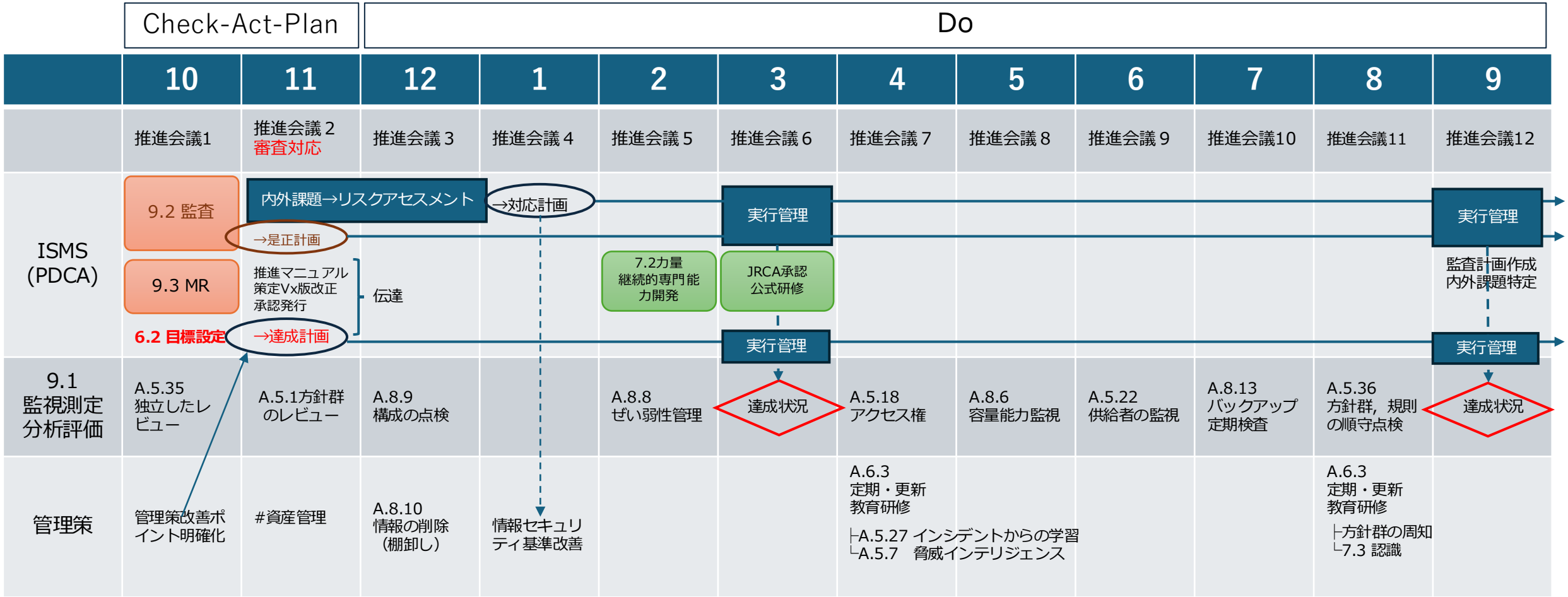
リニューアルプロジェクト期間：2026年1月から12月

6.3 変更の計画策定	ISMS の変更の必要があると決定したとき，その変更は，計画的な方法で行わなければならない。
変更理由及び目的	全社的視点で合理的かつ最適な方法で運用管理し、リターンを最大化することで、企業価値を高めるために、運用することを目的にISMSのマネジメント基準及び管理策基準を再構築するため 。

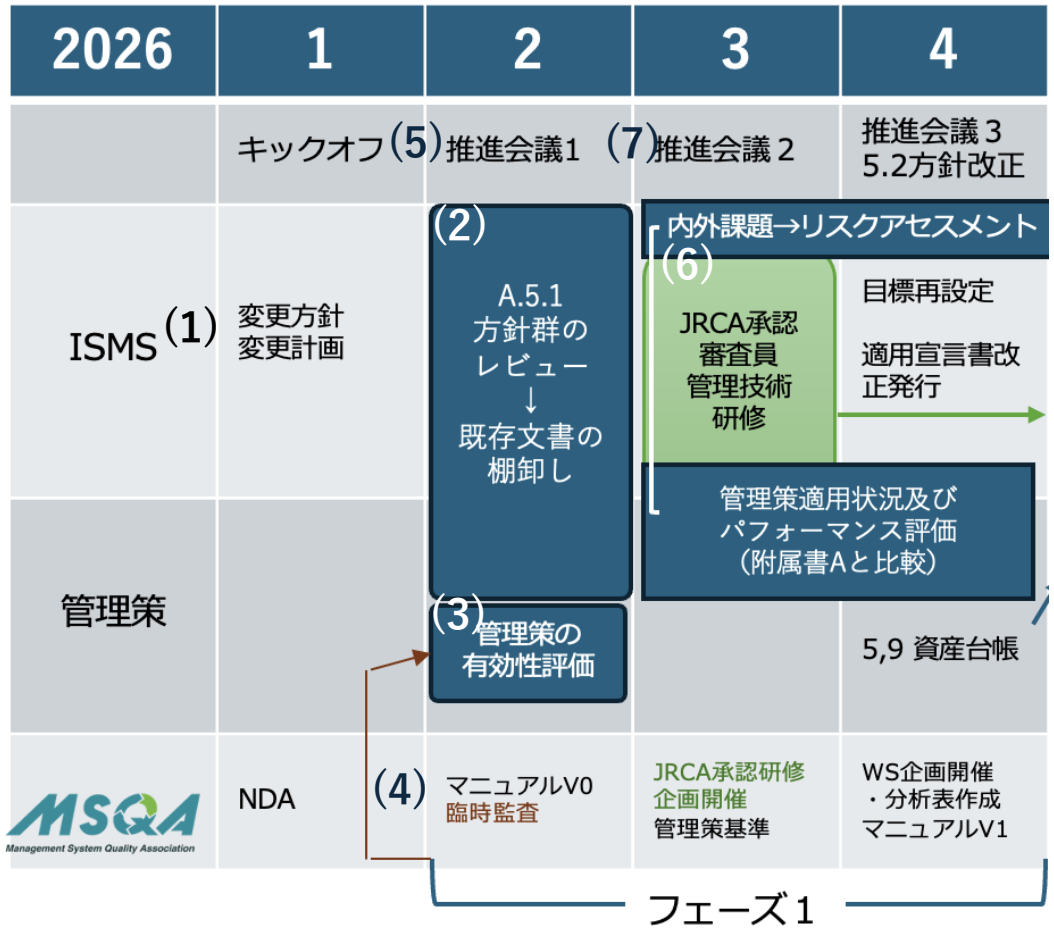
ー	1	2	3	4	5	6	7	8	9	10	11	12
	キックオフ	推進会議1	推進会議２	推進会議３ 5.2方針改正	推進会議４	推進会議５	推進会議６	推進会議７	推進会議８ 目標期限→	推進会議９	審査対応 （分割審査）	推進会議10
ISMS	変更方針 変更計画	A.5.1 方針群の レビュー ↓ 既存文書の 棚卸し	内外課題→リスクアセスメント JRCA承認 審査員 管理技術 研修 管理策適用状況及び パフォーマンス評価 （附属書Aと比較）	目標再設定 適用宣言書改正発行 5,9 資産台帳	→対応計画 →達成計画 推進マニュアル策定V1版 改正承認発行 JRCA登録 管理対象決定 ↓ 情報セキュリティ基準発行	実行管理 9.1 実行計画 ・個別管要要領発行 ・ユーザーマニュアル発行		A.6.3研修 ├A.5.27 └A.5.7 ・管理者マニュアル発行	監査計画作成 A.5.36 方針群，規則の順守点検 内外課題変化	9.2 監査 是正計画 9.3 MR 管理策改善ポイント明確化 対応計画更新	目標設定 ↓ 達成計画 9.1実行計画	A5.方針群のレビュー
管理策		管理策の 有効性評価										
MSQA Management System Quality Association	NDA	マニュアルV0 臨時監査	JRCA承認研修 企画開催 管理策基準	WS企画開催 ・分析表作成 マニュアルV1	対応計画支援 管理基準作成	個別管理要領作成支援	ユーザマニュアル作成支援	定期研修開催 管理者マニュアル作成支援	監査の準備	監査支援 MR支援	審査立会 審査フォロー 運用計画作成	
		フェーズ１			フェーズ2					フェーズ3		

運用管理プロセス案（標準）

期間：10月から翌年９月



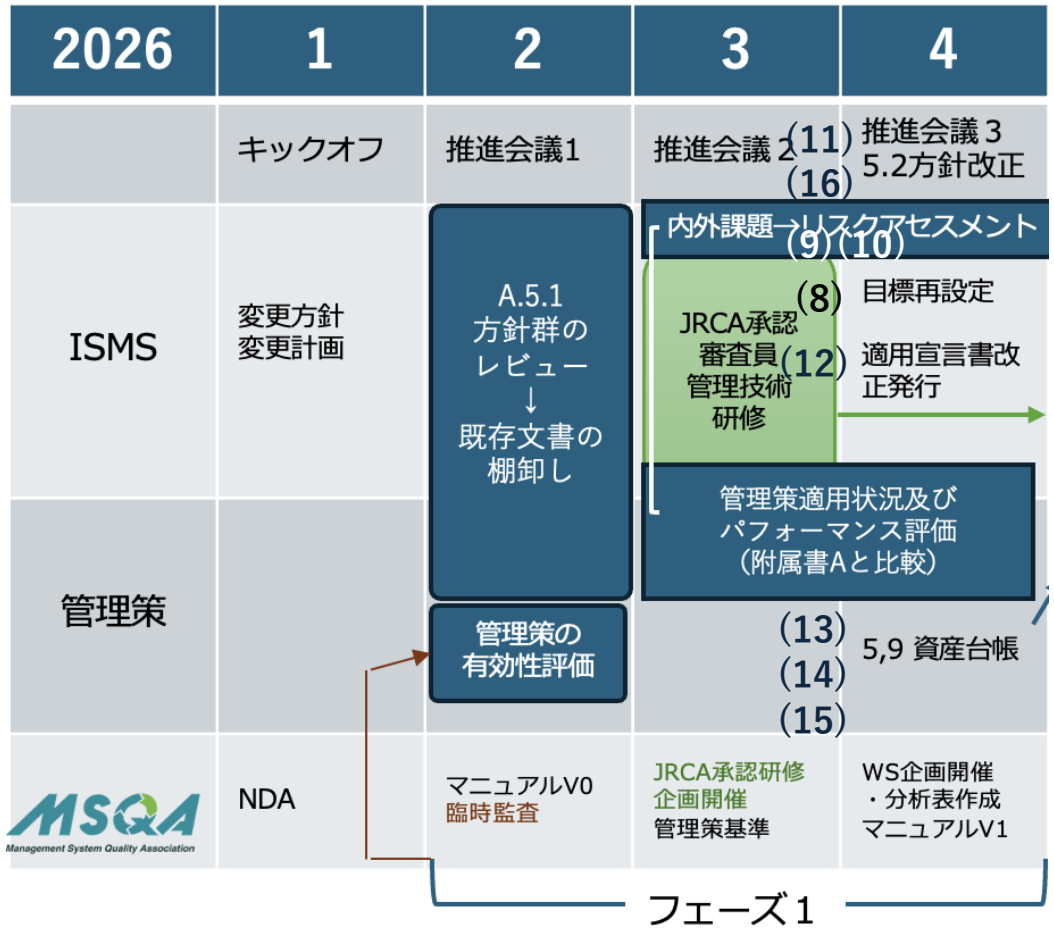
フェーズ１アクションプラン



	アクション	御社	MSQA
(1)	Project Charter ├ 変更方針 └ 変更計画	キックオフ開催 ・リニューアルの目的 ・ISMS運用のあるべき姿 ・変更の計画	Project Charter作成 ー提案 キックオフ参加
(2)	既存文書の棚卸し	1.文書一覧より有効な文書抽出 2.管理策に有効に機能する文書抽出	1.文書体系の理解 2.管理策と文書の整合性確認 3.※臨時監査の実施 4.※管理策管理表作成支援
(3)	管理策の有効性評価	1.管理策の運用状態点検 2.1.から管理策管理表作成	1.※臨時監査の実施 2.※管理策管理表作成支援 3.管理策管理表より有効性評価
(4)	ISMS推進マニュアル 初版の承認発行		ISMS推進マニュアル初版作成
(5)	推進会議１	ISMS推進マニュアル初版の理解	推進会議参加
(6)	JRCA承認研修開催 （企業内開催） 前半：3月　4日-　6日 後半：3月11日-13日	規格要求事項の理解と実践 監査プロセスの理解と実践 （下記ワークショップ開催） ・内外課題の決定 ・リスクアセスメント ・管理策の理解と適用状況把握 ・監査計画・定量的評価技法 ・不適合・改善の機会の記述	JRCAへ企業内開催申請 演習教材の変更 講師派遣 実技・行動評価 JRCA筆記試験の実施
(7)	推進会議２	・内外課題/利害関係者の要求 ・2章 管理策基準（管理表）再確認 ・リスク管理プロセス運用について	推進会議参加

MSQA
Management System Quality Association

フェーズ１アクションプラン



	アクション	御社	MSQA
(8)	6.2 目標の再設定		(2)(3)(6)結果に基づいてマネジメントシステム及び管理策のパフォーマンスを定量的（５段階）評価し数値目標を設定し文書化
(9)	リスク アセスメント①	リスク分析票（アンケート法）作成	様式提供 ワークショップ開催 ※分析票の取りまとめレビュー
(10)	リスク アセスメント②	リスク分析表への取りまとめ	様式提供 ワークショップ開催 ※分析表の取りまとめレビュー
(11)	推進会議３	リスク分析表ーリスク所有者承認 リスクコミュニケーション ISMS推進マニュアル1版 レビュー	推進会議参加
(12)	適用宣言書改正	適用宣言書をレビューし、必要に応じて改正発行	2章 管理策基準→適用宣言書確認
(13)	資産台帳作成① ー主要資産	資産台帳作成 主要資産の特定ー管理責任の明確化	様式提供 ワークショップ開催（#資産管理）
(14)	資産台帳作成② ー資産の格付け	格付け基準に従って分類 処理・保管場所の特定	ワークショップ開催（格付け基準）
(15)	資産台帳作成③ ー支援資産	処理・保管場所等支援資産の特定 情報資産の利用許容範囲等の特定	ワークショップ開催（構成管理）
(16)	基本方針の改正	基本方針改正ー承認発行	改正案の提供 ISMS推進マニュアル1版作成

重要なアクション解説

①JRCA承認ISMSフォーマル研修（管理技術者育成）について

②ISMS運用管理基準文書のリニューアル

③ISMS推進マニュアル 1章マネジメント基準

④リスクマネジメントプロセス

⑤事象ベースのアプローチ法

⑥セキュリティ目標管理プロセス

⑦パフォーマンス（定量的）評価の導入

⑧ISMS推進マニュアル　2章 管理策基準

　管理策見直し方針ーサイバー攻撃・内部不正『早期検知し即応』

⑨5.9 情報及びその他の関連資産の目録　作成・レビュープロセス改善

⑩重要な情報の識別管理： A.5.12 分類（格付け）不正競争防止法の適用

①JRCA承認ISMSフォーマル研修について

競争力を備え、風格のある人格を育成し、気概と向上心に裏付けられた風格と高度な専門性を兼ね備えたスペシャリスト集団を目指す。

ISO/IEC 27001:2022対応『JRCA承認ISMS審査員研修コース』

情報セキュリティスペシャリスト（セキュリティ人材育成）

－　管理技術者・監査リーダー育成　のために　－

目的

1. **自社のマネジメントシステム事務局員や担当者のレベルアップ**
2. **第一者監査、第二者監査への対応（監査品質の向上）**
3. **ISMS関連事業推進者としての技法・ノウハウ修得**

2026年03月開講：前半：04日（水）～ 06日（金）　後半：11日（水）～ 12日（木）13日（金）実技評価及び筆記試験

審査員資格は、組織が構築したマネジメントステムの審査を実施する方のための資格です。マネジメントシステム審査員資格は、第三者審査を行う方のベースラインとなる力量を有していることを示しますが、第三者審査時にしか役に立たないのでしょうか？そんなことはありません。資格を活用できる場面は、他にもあります。
監査と審査は同義です。審査員の目線で自組織のマネジメントシステムを客観的に評価し、効率的で効果的なマネジメントシステム運用技術（力量）の証拠としても有効です。

1	ISMS 適合性評価制度について 情報セキュリティマネジメントシステムについて 情報セキュリティマネジメントシステムの構造 ISO/IEC 27001:2022 箇条の理解	4	ふりかえり 監査（審査）活動の準備 監査（審査）活動の実施 監査の実務考察
2	リスクマネジメントプロセス リスクマネジメント用語及び定義 リスクアセスメント/リスク対応 リスク特定と管理策演習	5	監査（審査）中のコミュニケーション 所見の記述 不適合及び改善の機会抽出（記述演習） 実技評価（不適合の記述）
3	情報セキュリティ管理策とは 管理策の選択 ISO/IEC 27001 附属書 A 管理策解説 ISO/IEC 19011 監査（審査）の指針 解説	6	最終会議の実施 実技評価（不適合の記述）内容の提示（発表） サーベイランス審査/再認証審査について JRCA 筆記試験実施

MSQA
Management System Quality Association

②ISMS運用管理基準文書のリニューアル

目的：全社的視点で合理的かつ最適な方法で管理しリターンを最大化することで、企業価値を高めるため
方針：運用管理のための文書（マニュアル・規定・基準・手順書等）は運用できていることで適合とする

Before

After


初回認証/移行用サンプル

JIS Q 27001:2023 準拠

ISMS 推進マニュアル

ISO 27001

INFORMATION SECURITY MANAGEMENT SYSTEM

制定・改訂履歴

制定、改訂年月日	版番号	レビュー及び改訂の概要（主な改訂箇所・改訂内容等）	レビュアー及び承認
2024 年 3 月 15 日	00.1	レビュー用初版制定	MSQA 中西
2024 年 10 月 5 日	00.2	管理策基準様式を一部改訂	MSQA 中西
2025 年 2 月 3 日	0.40	JIS Q 27002:2024 発行に伴う一部改訂	MSQA 中西
2025 年 2 月 10 日	00.4	管理策基準様式を改訂、JIS Q 27002:2024 に整合	MSQA 中西
2025 年 2 月 21 日	00.5	管理策基準関連文書などの見直し	MSQA 中西
2024 年 月 日	V1.0		

本文書のレビュー及び改訂について

事業、法令、規制及び契約上の要求事項に従って、経営陣の方向性の継続的な適合性、有効性、及び情報セキュリティのサポートを確実にするため、情報セキュリティ基本方針及び ISMS 推進マニュアル（以降「本書」という）は、これを定期し、管理策が承認し、発行し、関連する部長及び関連する利害関係者に伝達し、認識させ、年間計画に従い及び重大な変化が発生した場合にレビューする。

本書は、マネジメント基準 7.5 文書化した情報及び 管理策 A.1 対象文書とする。

レビューの時期　：年間計画に従い実施する

承認発行　：情報セキュリティ管理責任の承認の上、発行する

伝達方法　：情報会議及び定期（更新）教育において伝達する

本マニュアルの構成

第1章　マネジメント基準　－ JIS Q 27001:2023 要求事項への適用

第2章　管理策基準　－ JIS Q 27001:2023 附属書 A（適用宣言した管理策）への適用

- 1 -

情報セキュリティ基本方針 → 6.2 目的（目標）と達成計画

第1章 マネジメント基準

運用計画（マスター）
リスクマネジメント基準ー事象ベース → 運用管理様式
監査基準・是正管理基準

第2章 管理策基準（管理策管理表）

5.組織的管理策
6.人的管理策
7.物理的管理策
8.技術的管理策

→ 情報セキュリティ基準 Security Policies → ユーザーマニュアル / 管理者マニュアル

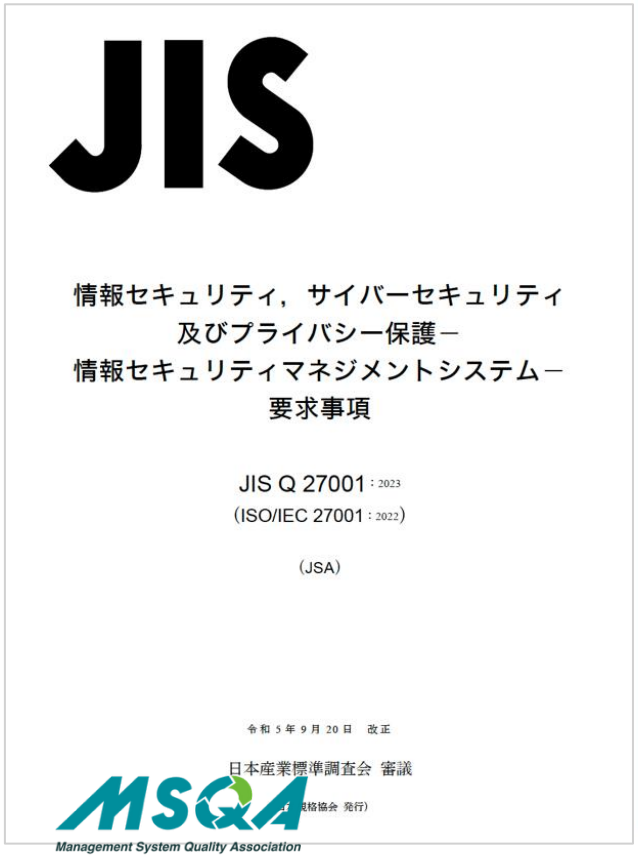
→ トピック固有の管理要領

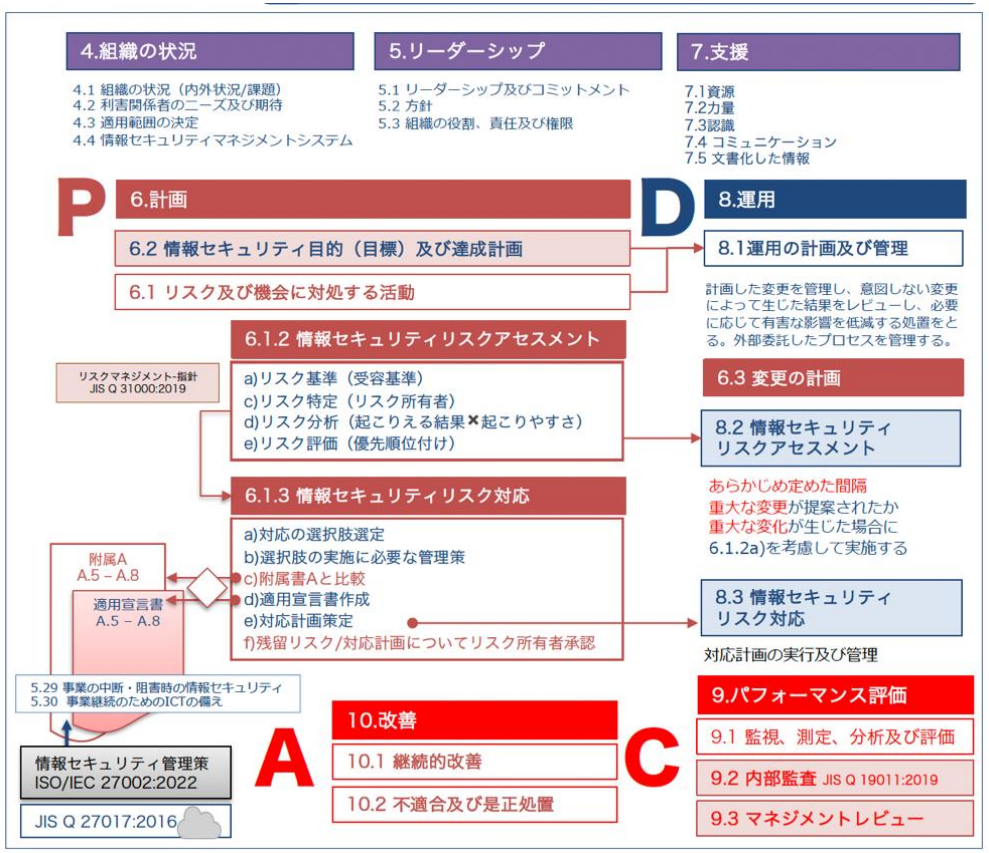
A.5.1 情報セキュリティの方針群ートピック固有の方針

ISMS用語「トピック固有の方針」：運用管理のための文書（マニュアル・規定・基準・手順書等）

③ISMS推進マニュアル 1章マネジメント基準

目的：リスクを全社的視点で合理的かつ最適な方法で管理するリスクマネジメントプロセスを適用することによって、情報の機密性、完全性及び可用性を維持し、かつ、リスクを適切に管理しているという信頼を利害関係に与えリターンを最大化するため。



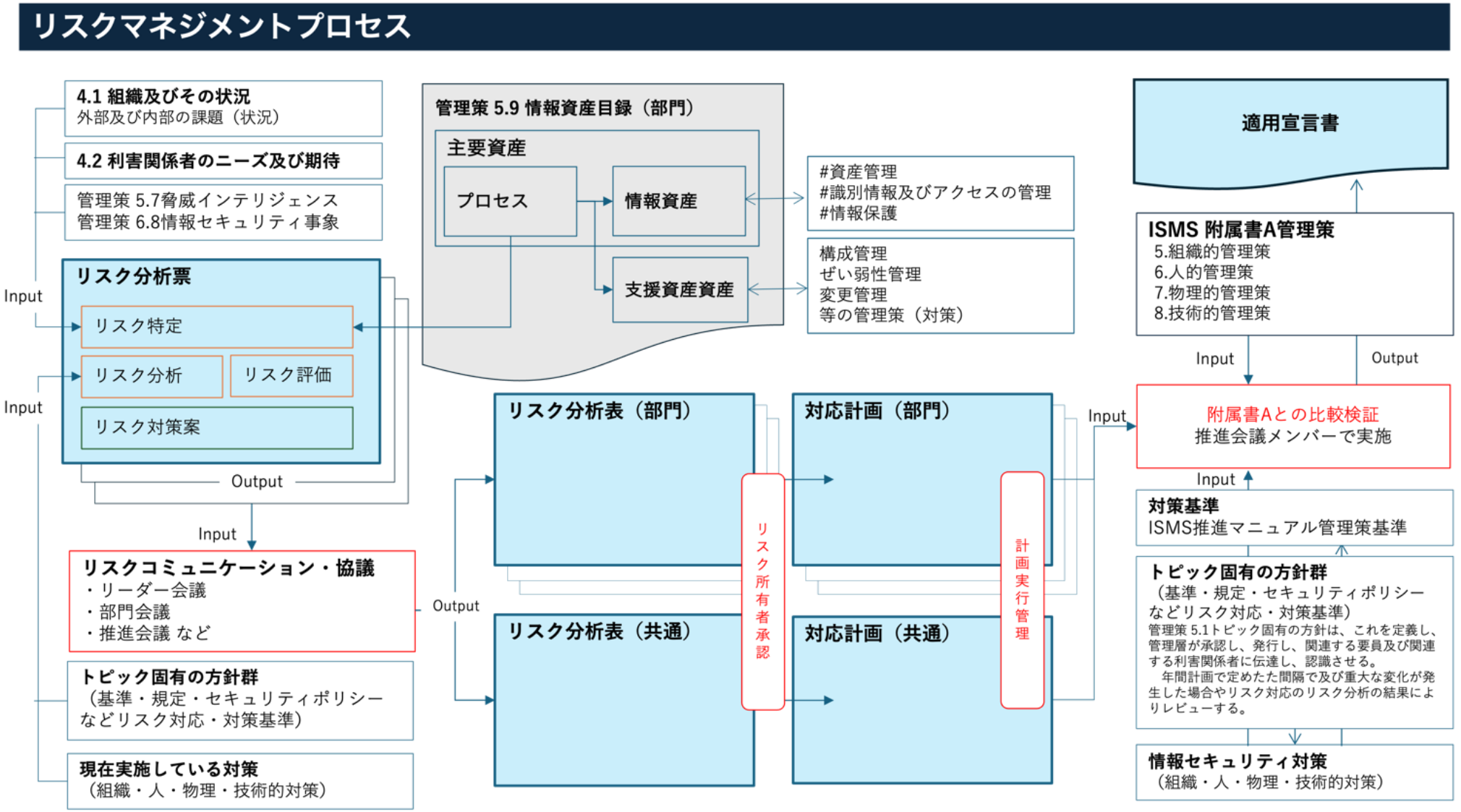


MSQA© ISMS_MAP 2023.07.06 V10.0：https://msqa.jp

④リスクマネジメントプロセス

事業プロセス及び活動

事象ベースのアプローチ法



⑤事象ベースのアプローチ法

出典：ISO/IEC 27005:2022
情報セキュリティリスクの管理に関する手引

事象及び結果の評価を通じてリスクを特定し分析できる。

事象ベースのアプローチは、詳細なレベルで資産を特定することに多大な時間を費やすことなく、高いレベルの、又は戦略的なシナリオを確立することができる。これにより、リスク対応の取組みを重大なリスクに集中させることができる。

このアプローチを使用した事象の評価は、リスクが長期間にわたって変化しない履歴データを利用することができる。

情報資産管理とリスク管理の分離により効率的で効果的なリスクマネジメントプロセスを構築し運用する。

⑥セキュリティ目標管理プロセス

Check

9.2 内部監査

A.5.35情報セキュリティの独立したレビュー
A.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

マネジメントシステム・管理策及びサーバーセキュリティレジリエンスを定量的（５段階）で評価し視覚化する。

Do

計画の実行

Plan

目標を伝達

部門・階層毎に達成のための推進計画を策定する

9.3 マネジメントレビュー

監査結果を報告し次期目標を提案、承認を得る

ISMS 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ー測定可能な５段階評価で目標設定

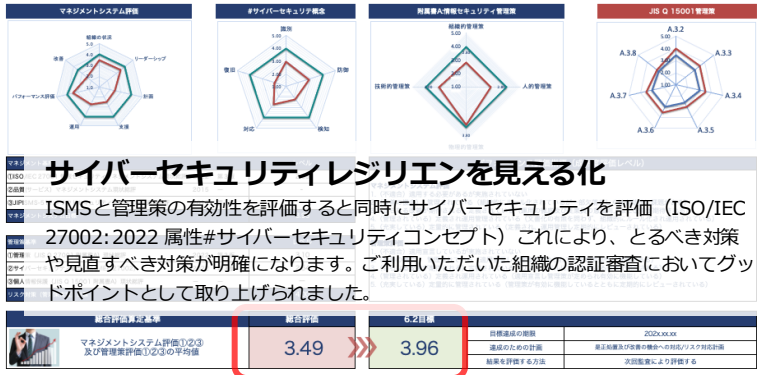
上記達成に必要な項目を洗い出し達成のための計画を策定する

例）A.5.23 評価 2 → 3にするための計画

マネジメントシステムと管理策（リスク対策）を５段階で評価

組織の状況及びそのリスクによって格付けすることが可能である。 この格付けは、**定量的なもの（例えば、1 から5）**も定性的なものもあり得る。（出典：JIS Q 19011:2019 所見の作成）

どこが不足・冗長化しているのか？何を見直す必要があるのか？を明確にしてマネジメントシステムのパフォーマンスを評価します。現状調査・内部監査や監視測定によって、**結果を分析して可視化（見える化）することで、是正改善のポイントが明確になり、評価結果をKPIとして定量的な管理目標としてご活用いただいています。**



ISMS 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

組織は、関連する部門及び階層において、情報セキュリティ目的を確立しなければならない。

情報セキュリティ目的は、次の事項を満たさなければならない。

a) 情報セキュリティ方針と整合している。

b) （実行可能な場合）**測定可能である。**

例）測定可能な目標3.49 → 3.96

Act

10.2 是正処置/改善の機会への対応

MSQA Management System Quality Association

⑦パフォーマンス（定量的）評価の導入

充実点としての審査所見

内部監査では、目標管理の一環として、マネジメントシステム及び管理策の実施（適用）状況について５段階の定量的な評価を実施していました。今年度の監査結果としてマネジメントシステム及び管理策の総合評価は2.95となっていました。管理策の成熟度評価がカテゴリー毎（運用属性毎）にも評価されておりレーダーチャートにより見える化されていました。さらに管理策の評価指標としてサイバーセキュリティレリエンス(属性値 #識別、#防御、#検知、#対応、#復旧が５段階で評価されており、同じくレーダーチャートにより見える化されていました。これを活用することにより、管理策レベルでの実施状況について不十分なところが明確になり、効果的な改善活動につながる有効な方法と評価できます。（主任審査員）

MSQAでは内部監査支援において、定量的な評価を実施しており、監査員の育成（ISMS審査員研修）ではその評価方法と評価ツールを提供しています。

MSQA
Management System Quality Association

⑧ISMS推進マニュアル　2章 管理策基準

目的：管理策の実施理由（目的）を明確にし、リスクレベルに応じたセキュリティ対策を講じるため。

第1章 マネジメント基準

リスクマネジメント基準
ー事象ベースのアプローチ法 → リスク分析表


初回認証/移行用サンプル

JIS Q 27001:2023 準拠

ISMS 推進マニュアル

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

制定・改訂履歴

制定、改訂年月日	版番号	レビュー及び改訂の概要（主な改訂箇所・改訂内容等）	レビュアー及び承認
2024年8月15日	00.1	レビュー用初版制定	MSQA 中西
2024年10月3日	00.2	管理策基準様式を一部改訂	MSQA 中西
2025年2月3日	0.00	JIS Q 27002:2024 発行に伴う一部改訂	MSQA 中西
2025年2月10日	00.4	管理策基準様式を改訂し、JIS Q 27002:2024 に整合	MSQA 中西
2025年2月21日	00.5	管理策基準関連文書などの見直し	MSQA 中西
2024年　月　日	V1.0		

本文書のレビュー及び改訂について

事業、法令、規制及び契約上の要求事項に従って、経営陣の方向性の継続的な適合性、有効性、及び情報セキュリティのサポートを確実にするため、情報セキュリティ基本方針及び ISMS 推進マニュアル（以降「本書」という）は、これを定義し、管理層が承認し、発行し、関連する要員及び関連する利害関係者に伝達し、認識させ、年間計画に従い及び重大な変化が発生した場合にレビューする。

本書は、マネジメントレビュー 7.5 文書化した情報及び 管理策 8.1 対象文書とする。

レビューの時期　：年間計画に従い実施する

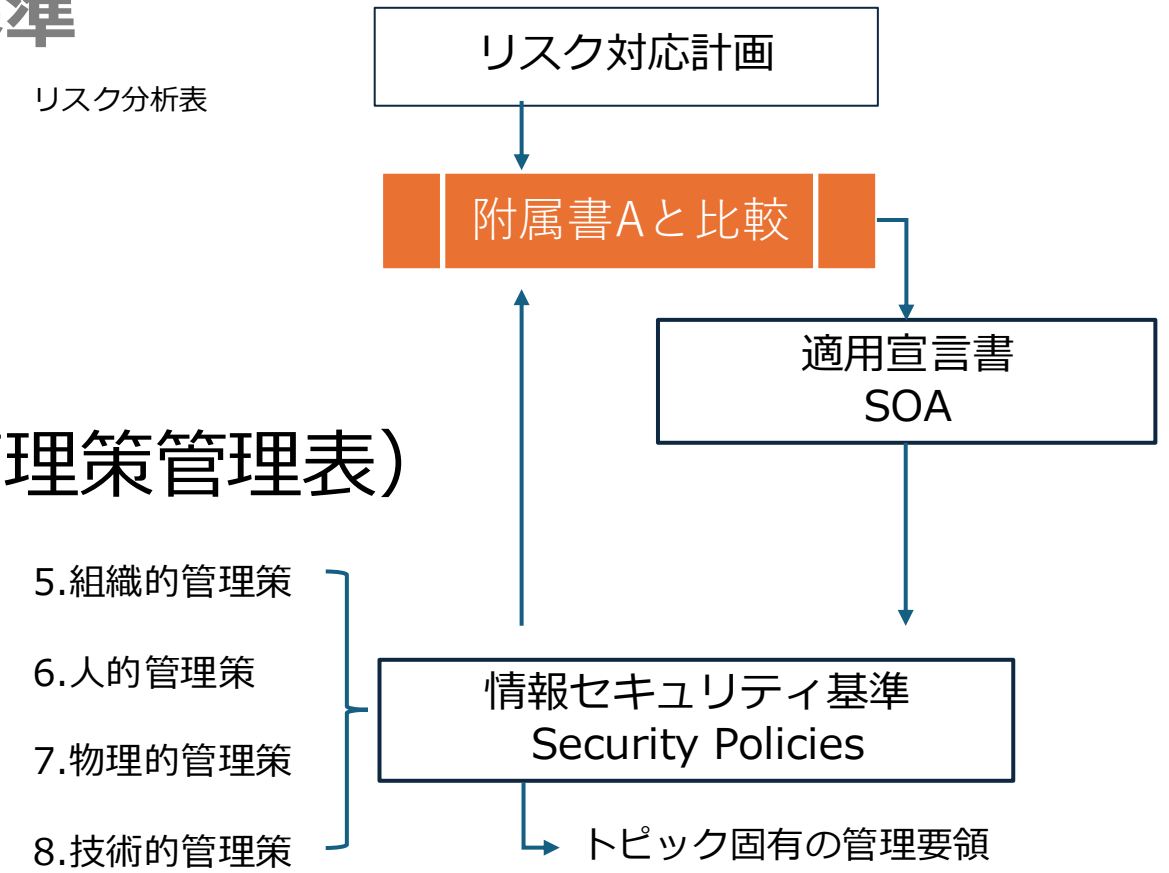
承認発行　：情報セキュリティ管理責任者の承認の上、発行する

伝達方法　：推進会議及び定期（更新）教育において伝達する

第2章 管理策基準

- 1 -

第2章 管理策基準（管理策管理表）



MSQA
Management System Quality Association

⑨5.9 情報及びその他の関連資産の目録　作成・レビュープロセス改善

目的：資産の管理責任を明確にし管理策の適用対象を明確にするため。

資産の定義 組織にとって価値のある全てのもの。情報セキュリティにおいては，次の2 種類の資産を区別することが可能である。

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ー適用部門（部署）

主要資産

① 事業プロセス及び活動　　特定

②情報　特定

A.5.12 分類（格付け）→ A.8.10 削除 / 8.13 バックアップ
→ #アクセス制御
ー 保管場所（支援資産）の特定 」

③（主要資産が依存する）全ての種類のサポート資産 = 支援資産 特定

④全社共通の資産を特定
部門別から共通へ
主要資産
支援資産

⑤ ②③④に対してA.5.10 情報及びその他の関連資産の許容される利用

– ハードウェア	→ エンドポイント・媒体・その他設備・機器	→ #装置
– ソフトウェア	→ アプリケーション・ユーテリティ・OSS他	→ #システム取得・開発・保守 / A.8.1 / A.8.18 / A.8.13
– ネットワーク	→ 社内ネットワーク・Wi-Fi・LTE・ネットワーク機器	→ #ネットワーク
– サービス	→ クラウドサービス・配送サービス・廃棄/清掃・警備	→ A.5.23 クラウド利用 / #供給者関係
– 要員	→ 派遣/契約社員・委託先（請負・委任等）	→ #供給者関係 / #人的セキュリティ
– サイト	→ 主たる執務場所以外の仕事場所・自宅（在宅勤務）	→ A.7.1 / A.6.7 / #物理的セキュリティ
– 組織の構造	→ プロジェクトワーク有無　→A.5.8	

A.8.9 構成管理
A.8.8 ぜい弱性管理
A.8.6 容量能力の管理
A.8.32 変更管理

要員：（組織の指示の下で仕事をしている人々 [経営陣，トップマネジメント，従業員，臨時スタッフ，契約社員，ボランティアなどの組織のメンバを含む]）

⑩重要な情報の識別管理： A.5.12 分類（格付け）不正競争防止法の適用

出典：経産省「知っておきたい営業秘密」

企業・研究機関などにとって重要な、秘密としたい情報が「営業秘密」

企業や研究機関などが、**営業活動や研究・開発から生み出した様々な情報**

営業情報

顧客名簿・情報、
接客マニュアル

技術情報

製造方法、
設計図面、金型

1 非公知性

2 有用性

一般には知られていない情報。

3 秘密管理性

従業員、取引先関係者等の**情報に接する人が、秘密情報と認識できるように管理されている情報。**

特定された主要資産「情報」を格付けし、格付け基準（分類）基準に従って、**「営業秘密」**であることを認識できるようにし管理責任を明確にする。

MSQA
Management System Quality Association

管理策見直し方針
サイバー攻撃・内部不正『早期検知し即応』

管理策 6.8 事象の報告
要員が発見した又は疑いをもった情報セキュリティ事象を，適切な連絡経路を通して時機を失せずに報告する（仕組みを設ける）

管理策 8.16 監視活動
ネットワーク，システム及びアプリケーションについて異常な挙動がないか監視し，適切な処置を講じる。

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監視し，レビューしなければならない。

管理策 5.25 情報セキュリティ事象の評価及び決定
組織は，情報セキュリティ事象を評価し，それらを情報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。

管理策 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。

業務と連動効率的かつ効果的に運用するため、＃識別、＃防御、＃検知、＃対応、＃復旧のために必要な管理策をリスクレベルに応じ見直し、有効に機能させるために、レジリエンス評価結果から対応を計画する。

MSQA
Management System Quality Association

ISO 27001 リニューアルプロジェクト憲章
（Project Charter）

初版：2026年1月30日発行

一般社団法人マネジメントシステム品質協会（MSQA）
〒110-0016 東京都台東区台東1-11-10 大木ビル
公式サイト2026年1月更新：https://msqa.jp
担当理事：中西 孝治　nakanishi@msqa.jp
登録番号：T1010505003082