QUANTITATIVE AUDIT EVALUATION

監査結果を「数値」で評価し、目標と改善につなげる

MSQA
Management System Quality Association

MSQAの内部監査における5段階の定量的評価と、
マネジメントレビュー・目標・対応計画までの運用サイクル

5段階
成熟度評価レベル

5属性
サイバーセキュリティ概念

15属性
運用機能（運用属性）

一般社団法人マネジメントシステム品質協会（MSQA）

https://msqa.jp/

ABOUT THIS MATERIAL

本資料のねらい

MSQAが5年以上実践してきた「監査結果の定量的評価」を、これから取り組む皆様に向けて公開します。

この資料を解説する対象

企業・組織のご担当者の皆様

ISMSなどマネジメントシステムの構築・再構築を、検討している、または進めている企業・組織のご担当者

コンサルタント・講師の皆様

マネジメントシステムの健全な普及促進を目的として、支援や教育に携わるコンサルタント・講師

情報公開を始めた理由

5年以上

MSQAで実践してきた実績

効果と有効性

目標設定と継続的改善で確認

Good Point

審査で評価されたこと

これらに基づき、情報公開を開始しました。

WHY QUANTITATIVE

定量的評価がもたらす6つの効果

「適合／不適合」だけでなく、成熟度を数値で示すことで、目標・計画・予算の判断材料になります。

01

目標設定に活用

マネジメントシステムと管理策（附属書A・クラウドセキュリティ・AIMS・SCS評価）の評価を数値化し、6.2の目標設定に使えます。

02

達成計画を具体化

測定可能な数値目標に対して、何を・いつまでに・誰がやるかのアクションプランを作成できます。

03

継続的改善の可視化

評価結果を時系列で管理し、年度ごとの改善の推移を一目で示せます。

04

レジリエンス可視化

#識別・#防御・#検知・#対応・#復旧で評価し、自組織のサイバーセキュリティ対策の姿が見えます。

05

MRのインプット

評価結果をレーダーチャートで示し、マネジメントレビューのインプット情報として使えます。

06

予算の重点配分

レーダーチャートで弱点が見えるため、予算や工数を重点的に配分できます。

WHY OBJECTIVES

明確な目標設定が、継続的改善の要

毎年設定する目標と達成計画を、効率的かつ効果的に決められるかどうかが、マネジメントシステムの成果を左右します。

これまでの課題

- 特にISMSでは、測定可能な目標の設定が困難でした
- 6.2 b) は「（実行可能な場合）測定可能である」ことを求めています
- JIS版では objectives が「情報セキュリティ目的」と訳され、測れる目標として扱われにくい面がありました
- 達成度が測れないと、計画・監視・評価がつながりません

「目的」と「目標」

ISMS原文

Information security objectives and planning to achieve them

→ JIS Q 27001：情報セキュリティ目的

QMS原文

Quality objectives and planning to achieve them

→ JIS Q 9001:2015：品質目標

Objectives【名】目的、目標（出典：英辞郎 on the WEB）

目的と目標は同じ意味と考えられます。ISMSの「目的」も、測定可能な「目標」として設定することが大切です。

MSQAの解決策

5段階評価を採用

内部監査の評価結果を、そのまま測定可能な数値目標にします。毎年必要な目標と達成計画を効率的かつ効果的に設定でき、継続的改善の要となる仕組みとして、この課題の解決に成功しました。

EVALUATION SCALE

5段階の成熟度評価レベル

内部監査様式「総評_総合」シートの評価指標です。所見の種類がそのまま評価点になります。

評価	所見	マネジメントシステム（箇条4～10）	管理策（附属書A等）
1	不適合	規格要求事項を満たしていない	適用宣言されているが管理策もしくは社内要求事項を満たしていない
2	改善の機会（−）	要求事項を満たしているが有効性に課題がある	適用宣言されている管理策及び社内要求を満たしているが有効性に課題がある
3	適合	規格要求事項を満たしている	適用宣言されている管理策及び社内要求がリスクレベルに応じ実施されている
3	改善の機会（＋）	より効率的・効果的な運用のために改善の余地がある	より有効に機能させるために改善の余地がある
4	充実点（Good Point）	優れた運用及び管理が実施されている	リスクレベルに応じ優れた運用及び管理が実施されている
5	充実点（Strong Point）	極めて優れた運用管理が実施されている	リスクの変化に対応しリスクレベルに応じ極めて優れた運用管理が実施されている

根拠：JIS Q 19011 6.4.8

監査所見の格付けは、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。

MSQAはこれを受けて、ISMS推進マニュアル 6.2.3「評価指標」で5段階評価を定め、9.2 内部監査の「所見の格付け」に適用しています。

注記：不適合は是正計画を作成し、監査リーダーのフォローアップ後に実行、結果は次回監査で評価します。改善の機会は被監査部署及び委員会等で検討し適用します。

SELECT STANDARDS

まず、評価する基準を選ぶ

監査様式 V9.3 の1シート目「評価対象選択」で、組織が評価する基準を「対象／対象外」から選びます。

評価対象基準の選択と総合評価

【使い方】本監査で評価する基準の「評価対象」欄（黄色）をプルダウンで「対象」または「対象外」に設定します。「対象」とした基準のチェックシートにのみ所見を記述・評価してください（対象外の基準はチェックシートがグレー表示になり、総評_総合の集計・チャートからも除外されます）。総合評価は「対象」とした基準の現状評価の平均値です。

No.	評価基準	評価シート	評価対象	現状評価	目標	差異	評価範囲・備考
1	ISMS 要求事項（JIS Q 27001 箇条4〜10）	27001	対象	2.96	3.50	(0.54)	箇条4〜10
2	ISMS 附属書A 管理策（JIS Q 27001 附属書A）	附属書A	対象	3.00	3.50	(0.50)	5〜8 管理策（#サイバーセキュリティ概念・#運用属性を含む）
3	クラウド ISO/IEC 27017 CSC管理策	ISO27017_CSC	対象外				クラウドサービスカスタマ
4	クラウド ISO/IEC 27017 CSP管理策	ISO27017_CSP	対象外				クラウドサービスプロバイダ
5	SCS評価制度（サプライチェーン）	SCS評価制度	対象外				★4
6	AIMS 要求事項（ISO/IEC 42001 箇条4〜10）	AIMS_42001	対象外				箇条4〜10
7	AIMS 附属書A 管理策（ISO/IEC 42001）	AIMS_42001	対象外				A.2〜A.10
	総合評価（「対象」とした基準の平均値）			2.98	3.50	(0.52)	SCS評価制度は H 列で評価段階（★3：基礎項目のみ／★4：全項目）を選択
評価対象とした基準の数				2	※レーダーチャートは3基準以上で有効な形になります		

選べる基準は7つ：ISMS要求事項、ISMS附属書A管理策、ISO/IEC 27017（CSC／CSP）、SCS評価制度（★3／★4）、AIMS要求事項、AIMS附属書A管理策。既定ではISMS要求事項と附属書Aの2つが対象です。

※ 様式は「9.2監査様式_ISMS2026V9.3」（V9.3以上）をご使用ください。
MSQA会員の方にはLMS専用コースで最新版を提供していますので、ダウンロードしてご利用ください。

プルダウンで選ぶ

評価対象欄で「対象／対象外」を選択

対象外は集計しない

チェックシートはグレー表示になり、集計・チャートから外れます

総合評価は対象の平均

対象とした基準の現状評価を平均し、総合評価チャートを自動作成

HOW THE FORM WORKS

監査様式での評価の流れ

対象とした基準のチェックシートで所見を選ぶだけで、評価点と属性別の集計が自動で計算されます。

① 評価対象を選択

1シート目で評価する基準を「対象」に設定

② チェックシートで監査

対象とした基準のシートにのみ所見を記述

③ 所見をプルダウン選択

不適合／改善の機会（－・＋）／適合／充実点

④ 評価（1〜5）を自動算出

所見と評価点の対応表から関数で変換

⑤ 属性ごとに自動集計

属性フラグで、サイバー概念・運用属性別に平均

附属書Aシートの記入イメージ（抜粋）

箇条	管理策標題	所見（選択）	評価（自動）	識別	防御	検知	対応	復旧	運用属性
5.1	情報セキュリティのための方針群	適合	3	●					#ガバナンス
5.7	脅威インテリジェンス	改善の機会（－）	2	●		●	●		#脅威及びぜい弱性の管理
5.24	インシデント管理の計画策定及び準備	充実点（GoodPoint）	4				●	●	#情報セキュリティ事象管理

※ 表の所見・評価は説明用の記入例です。属性（●）はJIS Q 27002:2024 4.2の属性に基づき様式に設定済みで、評価点が属性ごとの列に展開され「総評_総合」シートで平均されます。

「総評_総合」シートで全体を見える化

対象とした基準の評価が自動で集計され、レーダーチャートと総合評価が1枚にまとまります。



1. **マネジメントシステム評価**
   箇条4〜10（ISMS／AIMS）
2. **#サイバーセキュリティ概念**
   識別・防御・検知・対応・復旧
3. **附属書A 管理策**
   組織的・人的・物理的・技術的
4. **管理策 #運用属性**
   ガバナンス〜情報セキュリティ保証
5. **SCS評価制度・AIMS・27017**
   対象外の基準は「対象外」と表示
6. **総合評価 → 6.2目標**
   対象とした基準の平均値と目標

シート下部には、対象とした基準だけを軸にした総合評価チャート（レーダー／横棒）も自動で作成されます。

※ 画面は様式V9.3.1の記入例（サンプル値）です。

SCORING

総合評価の算定と目標値

「対象」とした基準の現状評価の平均を総合評価とし、そのまま6.2の数値目標として設定します。

ISMS 要求事項

2.96

JIS Q 27001 箇条4〜10の平均

ISMS 附属書A 管理策

3.00

JIS Q 27001 附属書A（93管理策）の平均

総合評価

2.98

対象とした基準の平均
（2.96＋3.00）÷ 2

6.2 目標

3.50

対象とした基準の目標の平均
期限・計画・評価方法とセットで設定

※ 数値は様式V9.3.1の記入例（既定の2基準を対象）です。

ISO/IEC 27017（CSC／CSP）、SCS評価制度（★3／★4）、AIMS（ISO/IEC 42001 要求事項・附属書A）を「対象」にすると、その基準も平均に加わり、総合評価チャート（レーダー／横棒）の軸になります（レーダーは3基準以上で有効な形になります）。

INTEGRATED

SCS評価制度・AIMS・クラウドも、同じ物差しで統合管理

多くの企業が採用を検討している制度や規格への適用状況も、ISMSと同じ5段階で定量的に評価できます。

SCS評価制度

サプライチェーン強化に向けたセキュリティ対策評価制度（経済産業省）

取引先からの対策要求に応えるため、★3（基礎）・★4（標準）の要求への適合状況を評価します。

AIMS（ISO/IEC 42001）

AIマネジメントシステム

AIを利用・提供する組織の責任あるAIガバナンスとして、要求事項と附属書A管理策を評価します。

JIS Q 27017

クラウドサービスの情報セキュリティ管理策

クラウドを利用（CSC）・提供（CSP）する組織向けに、クラウド固有の管理策の適用状況を評価します。

統合管理のメリット

規格・制度ごとに別々の評価を行わず、1つの監査様式で同じ5段階の物差しを使うため、比較・優先順位付け・目標設定・対応計画を一元的に進められます。

今後の対応予定

SOC2・SOC3

ISMAP（政府情報システムのためのセキュリティ評価制度）

CASE STUDY

実際の事例：現状調査の結果を目標につなげる

ある支援先のフェーズ1臨時監査（現状調査）の結果です。組織名は伏せています。

マネジメントシステム評価

1.72　箇条4〜10の平均

管理策評価

2.71　附属書Aの平均

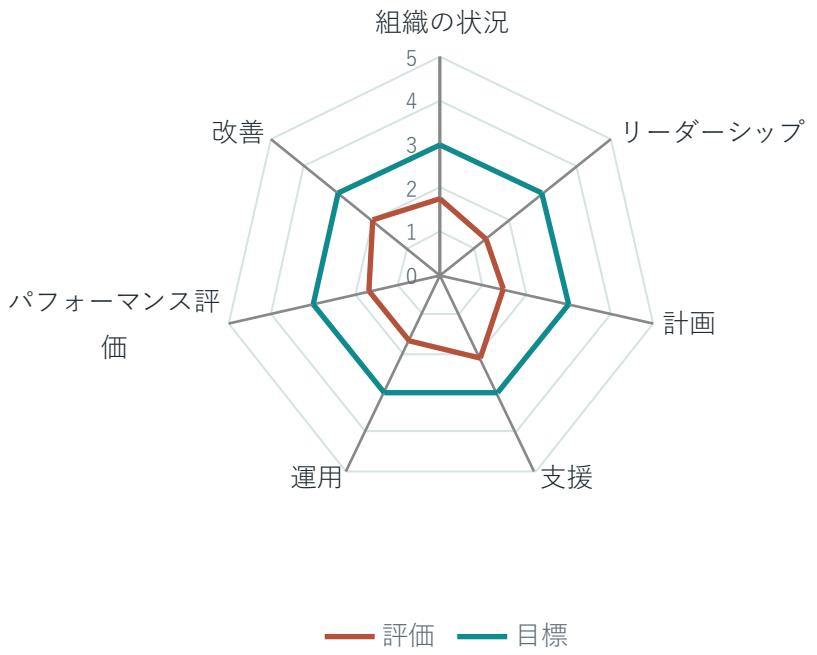
総合評価

2.22　（1.72＋2.71）÷ 2

6.2 目標

3.00　期限を定めて設定

マネジメントシステム評価（箇条4〜10・実例）



弱点がはっきり

リーダーシップ 1.33、計画 1.50 が特に低く、体制と目標・計画の整備が最優先と分かります。

計画に落とし込む

評価1・2の項目を3に引き上げる対応計画を作り、期限を決めて進捗を管理します。

次の監査で測る

同じ様式で再評価し、総合評価 2.22 → 3.00 の達成度を数値で確認します。

※ 実際の現状調査（臨時監査）結果。目標3.00は当該組織が設定した値です。

HOW TO USE

活用法：構築・再構築は「調査（臨時監査）」から

新規構築や再構築のフェーズ1として調査（臨時監査）を行い、課題を数値で明確にしてからフェーズ2以降に進みます。

PHASE 1

調査（臨時監査）

同じ監査様式で、要求事項と管理策の現状を5段階で評価します。

課題の明確化

どこが不足しているか

評価1・2の項目と、レーダーチャートで弱い属性を洗い出します。

PHASE 2 以降

構築・再構築

課題を対応計画書に落とし込み、優先順位をつけて進めます。

内部監査

効果を数値で確認

同じ様式で再評価し、フェーズ1からの改善を確認します。

新規構築の場合

今の仕事のやり方を要求事項・管理策に当てはめて評価し、すでにできていること（評価3）と足りないこと（評価1・2）を分けます。足りない部分から構築するので、ムダな文書や手順を作りません。

再構築の場合

既存のISMSを評価し、形骸化・冗長化している部分を見える化します。評価の低い箇条や属性に絞って見直すので、全体を作り直さずに効果的な再構築ができます。

CYCLE

評価結果から継続的改善を回すサイクル

内部監査の定量評価を起点に、マネジメントレビュー・目標・対応計画をつなぎ、次の監査で結果を測ります。

STEP 1

内部監査（9.2）

マネジメントシステムと管理策を5段階で定量評価

STEP 2

マネジメントレビュー（9.3）

総合評価とレーダーチャートをインプットとして報告

STEP 3

次期目標の設定（6.2）

総合評価・属性別評価を数値目標として設定

STEP 4

対応計画の作成

評価1→3・2→3・3→4を目指す具体的な計画

STEP 5

実行と進捗管理

ISMS推進会議で対応計画の進捗を監視・レビュー

次回の内部監査で結果を定量的に評価し、次のサイクルへ

規格要求事項：6.2 情報セキュリティ目的及び計画策定

JIS Q 27001:2023（ISO/IEC 27001:2022）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」の要求事項です。

組織は，関連する機能及び階層において，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。

c)　適用される情報セキュリティ要求事項，並びにリスクアセスメント及びリスク対応の結果を考慮に入れる。

d)　これを監視する。

e)　これを伝達する。

f)　必要に応じて，更新する。

g)　文書化した情報として利用可能な状態にする。

組織は，情報セキュリティ目的に関する文書化した情報を保持しなければならない。

組織は，情報セキュリティ目的をどのように達成するかについて計画するとき，次の事項を決定しなければならない。

h)　実施事項

i)　必要な資源

j)　責任者

k)　達成期限

l)　結果の評価方法

b) の「測定可能」を、5段階評価で満たします。

5段階評価で、6.2の要求事項をこう満たします

内部監査の定量的評価を起点にすることで、目的（a〜g）と計画（h〜l）の要求事項を、一つの仕組みで満たせます。

目的の要求事項	5段階評価での対応
a) 方針と整合	方針に基づくISMS全体の実施状況を、総合評価で測ります
b) 測定可能	**総合評価・属性別評価（例：2.22 → 3.00）を数値目標にします**
c) 要求事項・リスク対応の結果を考慮	要求事項（箇条4〜10）と、リスク対応で選んだ管理策（附属書A）を評価します
d) 監視	ISMS推進会議で対応計画の進捗を監視します
e) 伝達	マネジメントレビューでレーダーチャートを使って報告・共有します
f) 更新	毎年の内部監査結果をもとに、次期目標に更新します
g) 文書化	マニュアル6.2.4と「総評_総合」の6.2目標欄に記録します

計画の要求事項	対応
h) 実施事項	対応計画書（評価1・2 → 3、3 → 4）
i) 必要な資源	弱点の属性に予算・工数を重点配分
j) 責任者	6.2.4と対応計画書に明記
k) 達成期限	「総評_総合」の目標達成の期限
l) 評価方法	次回の内部監査で定量的に評価

ISMS推進マニュアル「6.2」で定めています

定量的評価は、ISMS推進マニュアル 6.2（目標及び達成計画の策定）に組み込まれています。

6.2.1

関連する部門及び階層において、情報セキュリティ目的（目標）を確立する。

6.2.2 目標設定基準

マネジメント編（JIS Q 27001要求事項）と管理策編のパフォーマンスを 5 段階で評価する。総合評価はマネジメントシステム評価及び管理策評価より算定する。定量的なパフォーマンス評価によって、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、を明確にする。現状調査・内部監査や監視測定によって、結果を分析し、可視化（見える化）することで、是正改善のポイントを明確にし、評価結果をKPIとして定量的な管理目標とする。

6.2.3 評価指標

マネジメントシステム評価・管理策評価

1（不適合）～ 5（極めた運用）の5段階で評価

サイバーセキュリティレジリエンス評価

管理策評価をJIS Q 27002:2024 4.2 c) サイバーセキュリティ概念（識別・防御・検知・対応・復旧）の属性毎に分析

運用機能別評価

管理策評価を4.2 d) 運用機能（ガバナンス、資産管理 … 情報セキュリティ保証）の属性毎に分析

6.2.4 に目標と達成計画を記載します（次ページ）。

評価結果を「測れる目標」と「計画」に変える

評価1・2の項目は3へ、3の項目はより効率的・効果的に改善して4を目指します。

1 → 3　**不適合を是正し要求事項を満たす**

2 → 3　**有効性の課題を解消する**

3 → 4　**効率的・効果的な運用で優れた水準へ**

ISMS推進マニュアル 6.2.4 の記載例

目標	総合評価目標 3.00（前回評価結果 2.86）
達成計画	要求事項 5.2・6.2/8.1・7.2 と、管理策 5.9・5.12・5.16・5.25 を改善（2→3 など）し、「対応計画」に基づいて実施・記録
監視	ISMS推進会議で進捗を監視・レビュー
責任者	情報セキュリティ責任者
達成期限	2027年9月30日
評価方法	内部監査でパフォーマンスを定量的に測定

計画は「対応計画書」で一元管理

MSQAでは「リスク対応計画書」ではなく「対応計画書」という名称で、組織のあらゆる計画をひとつにまとめて進捗を管理します。

リスクアセスメントの結果
6.1.3 リスク対応

組織の課題
4.1 外部・内部の課題

目標達成のための計画
6.2 定量評価に基づく目標

監査・審査の所見への対応
是正処置・改善の機会

対応計画書

- リスク対応だけでなく、課題・目標・所見への対応を1つの計画に集約
- 誰が・何を・いつまでに・どの評価点を目指すかを明記
- ISMS推進会議で進捗を一元的に監視・レビュー
- 結果は次回の内部監査で定量的に評価

改正で採用された「属性」で、管理策を別の切り口から見る

JIS Q 27002:2024（ISO/IEC 27002:2022）では、管理策が4つのテーマに再編され、各管理策に5つの属性が付けられました。

4つのテーマ（93管理策）

37 組織的管理策	8 人的管理策
14 物理的管理策	34 技術的管理策

大きな分類になったため、テーマだけでは弱点の場所が見えにくくなりました。

5つの属性

管理策タイプ	予防・検知・是正	
情報セキュリティ特性	機密性・完全性・可用性	
サイバーセキュリティ概念	識別・防御・検知・対応・復旧	MSQAが評価に活用
運用機能（運用属性）	ガバナンス、資産管理など15の属性値	MSQAが評価に活用
セキュリティドメイン	ガバナンス及びエコシステム・保護・防御・レジリエンス	

出典：JIS Q 27002:2024 4.2 テーマ及び属性

サイバーセキュリティ概念は、NIST CSFに準拠

管理策を「識別・防御・検知・対応・復旧」で見ることで、サイバーセキュリティ対策の強さと弱さが分かります。

NIST CSFとは

米国国立標準技術研究所（NIST）のサイバーセキュリティフレームワーク（Cybersecurity Framework）。組織がサイバーセキュリティリスクを管理するための枠組みとして、世界中で使われています。

JIS Q 27002:2024のサイバーセキュリティ概念は、ISO/IEC TS 27110のフレームワークに基づき、CSFと同じ5つの機能を属性値としています。

識別
Identify

資産・リスクを把握する

防御
Protect

被害を防ぐ対策を実施する

検知
Detect

異常や攻撃を見つける

対応
Respond

インシデントに対処する

復旧
Recover

事業を元に戻す

見える化すると、予算と対応計画を集中できる

5つの機能ごとの評価をレーダーチャートで示すと、「検知が弱い」「復旧が弱い」といった偏りが分かります。セキュリティ対策を講じるときに、予算と対応計画を、識別・防御・検知・対応・復旧のカテゴリー別に集中できます。

※ NIST CSF 2.0（2024年）では「統治（Govern）」が加わり6機能になっています。

OPERATIONAL CAPABILITIES

運用属性（運用機能）で、実務の弱点を見つける

運用機能は、情報セキュリティ機能についての実践者の観点で管理策を見る属性です。15の属性値があります。

#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	#システム及びネットワークのセキュリティ
#アプリケーションセキュリティ	#セキュリティを保った構成	#識別情報及びアクセスの管理
#脅威及びぜい弱性の管理	#継続	#供給者関係のセキュリティ
#法令及び順守	#情報セキュリティ事象管理	#情報セキュリティ保証

MSQAの具体的な活用方法

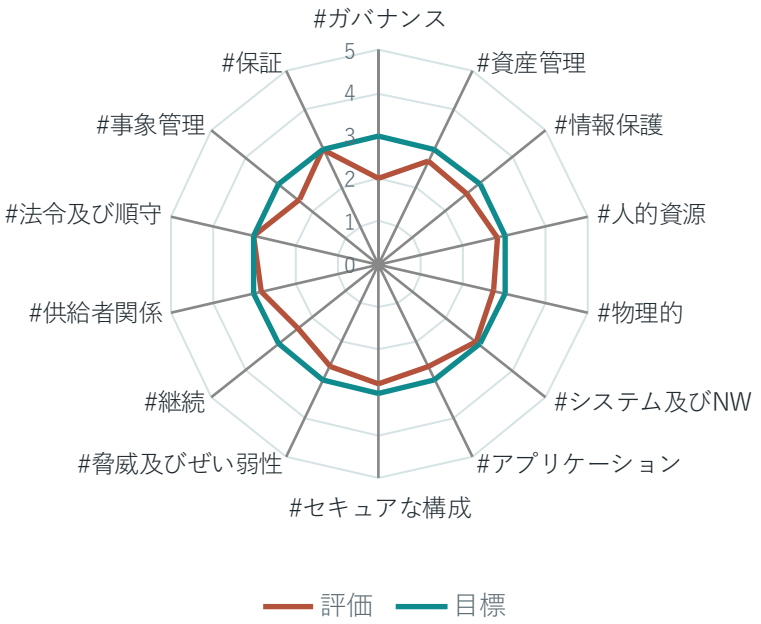
- 改正で採用された属性を、MSQAは評価の切り口として採用しました
- 監査様式の附属書Aシートで、管理策ごとに属性を設定済み
- 所見を選ぶだけで、運用属性ごとの評価を自動で集計
- 4テーマでは見えない弱点（例：#ガバナンス、#継続）をレーダーチャートで特定し、対応計画を属性別に立てる

VISUALIZE

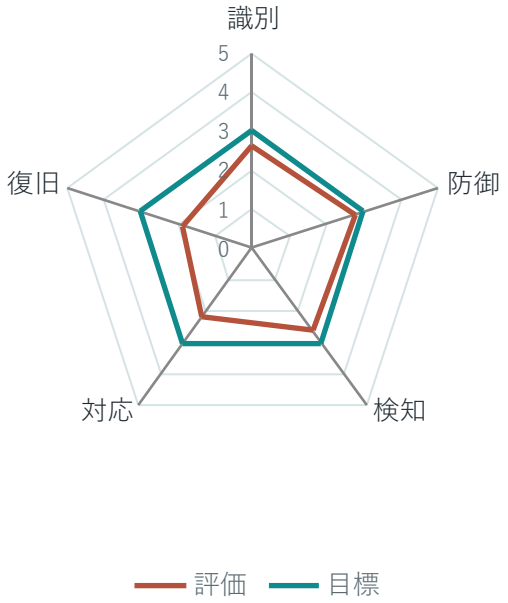
レーダーチャートで弱点とレジリエンスを見える化

運用属性やサイバーセキュリティ概念の切り口で、重点的に改善すべき点がはっきりします。

管理策 #運用属性（実例）



#サイバー概念（実例）



弱点が明確に

#ガバナンス 2.0、#事象管理 2.4、#継続 2.4 など目標との差が大きい属性が一目で分かる

レジリエンスを把握

対応 2.2・復旧 1.9 が低く、インシデント対応と復旧に偏りがあると分かる

予算を重点配分

差の大きい属性（事象管理・継続など）に予算・工数を集中できる

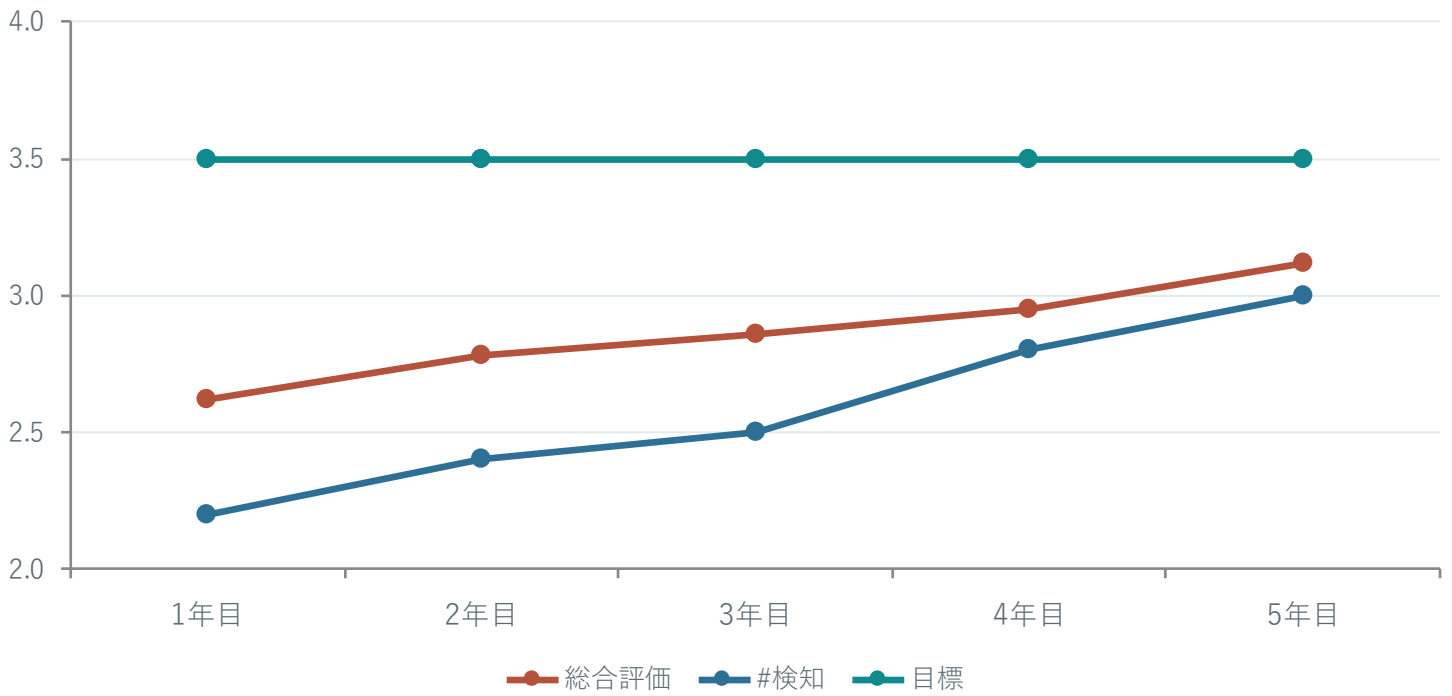
※「実際の事例」と同じ支援先の現状調査結果（実例、組織名は伏せています）。様式では附属書Aの評価から自動で作成されます。

TREND

時系列で追うと、継続的改善が見えてくる

数年分の評価結果を並べると、改善活動の成果を経営層や審査員にそのまま示せます。

総合評価と属性別評価の推移（イメージ）



※ グラフは説明用のイメージ（例示データ）です。

改善の推移を証明

毎年の内部監査結果を同じ物差しで比較できます。

MRで傾向を議論

伸びた属性・停滞した属性を把握し、次期目標に反映します。

審査でも説明しやすい

継続的改善（10.1）の証拠として、数値で示せます。

GOOD POINT

審査においても評価されています

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ジリエンス（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。

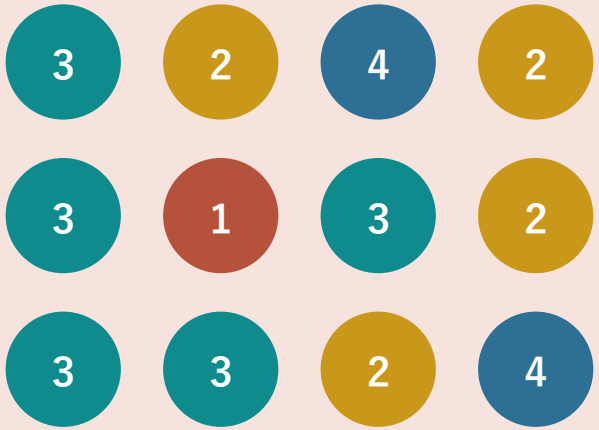
2025年 支援企業の再認証審査において、Good Pointとして評価いただいた審査員による所見

留意点：サンプリングによる評価のぶれ

監査はサンプリングで行うため、サンプルの取り方によって評価が上下するリスクがあります。

ばらつきがある状態

サンプルの選び方で評価が変わる



選ぶ行・列によって 2.0〜3.0 と上下

目指す状態

どこをどうサンプルしても「3」



どのサンプルでも 3 ＝ 仕組みが定着

押さえておきたい点

- サンプリング方法を変えると評価は上下する
- 重要なのは、どこをどのようにサンプルしても総合評価が「3」になること
- 内部監査で3に近づいても、審査で改善の機会などの指摘があれば評価が下がることも想定しておく

※ 図は説明用のイメージです。

SUMMARY

測る・決める・改善する

測る

監査様式で、所見を選ぶだけで5段階の評価と属性別集計が自動で作成されます。

決める

総合評価とレーダーチャートをMRに報告し、測定可能な目標と対応計画を決めます。

改善する

対応計画書で進捗を一元管理し、次回監査で効果を測って時系列で追跡します。

MSQAでは定量的評価と現状の見える化を目的とした内部監査を支援しています。主任審査員資格を有し、多くの企業の定量的評価を支援してきた監査チームを派遣しています。お気軽にお問い合わせください。

※ 様式は「9.2監査様式_ISMS2026V9.3」（V9.3以上）をご使用ください。
MSQA会員の方にはLMS専用コースで最新版を提供していますので、ダウンロードしてご利用ください。

一般社団法人マネジメントシステム品質協会（MSQA）

https://msqa.jp/

MSQA
Management System Quality Association