MSQA
Management System Quality Association

JRCA

JRCA承認研修機関

MANAGEMENT SYSTEM QUALITY ASSOCIATION

マネジメントシステムの構築・運用・人材育成を、ひとつのパートナーで。

ISMSをコアに、認証取得から運用改善、内部監査、
教育研修・力量認定まで一貫して伴走します。



JRCA承認研修機関（ISMS審査員研修／ISMS-CLS審査員研修）

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 MSQA

MSQAについて

ISMS（ISO/IEC 27001）をコアに据え、専門家が
連携するネットワーク型組織として発足しました。

> **マネジメントシステムの健全な普及促進で、
> 経済社会の進歩発展に貢献します**

私たちの特徴

ネットワーク型の専門家集団

審査員・コンサルタント・講師が連携し、
課題に合ったチームで支援します。

認証取得後の「運用・改善」に強い

形だけのISMSにしない、現場で回る
仕組みづくりを重視しています。

人材育成まで一貫支援

JRCA承認研修と独自の力量認定制度で、
組織の人材を育てます。

法人概要

名称	一般社団法人 マネジメントシステム 品質協会（MSQA）
創業	2013年2月14日
設立	2019年11月29日
所在地	東京都台東区台東1-11-10 大木ビル
認定	JRCA承認研修機関 ISMS-CLS TC-07

沿革

2013.02	2019.11	2022.10	2023.01	2024.10	2025	2026.02	2026
創業 ISMS認証・運用支援、LMS運用開始	一般社団法人として設立	情報セキュリティ管理策実践ガイドリリース	ISMS推進マニュアル活用ガイドリリース	内部監査チームを増強	JRCA承認	ISMAP構築（認証）支援をリニューアル	経済産業省マナビDX登録

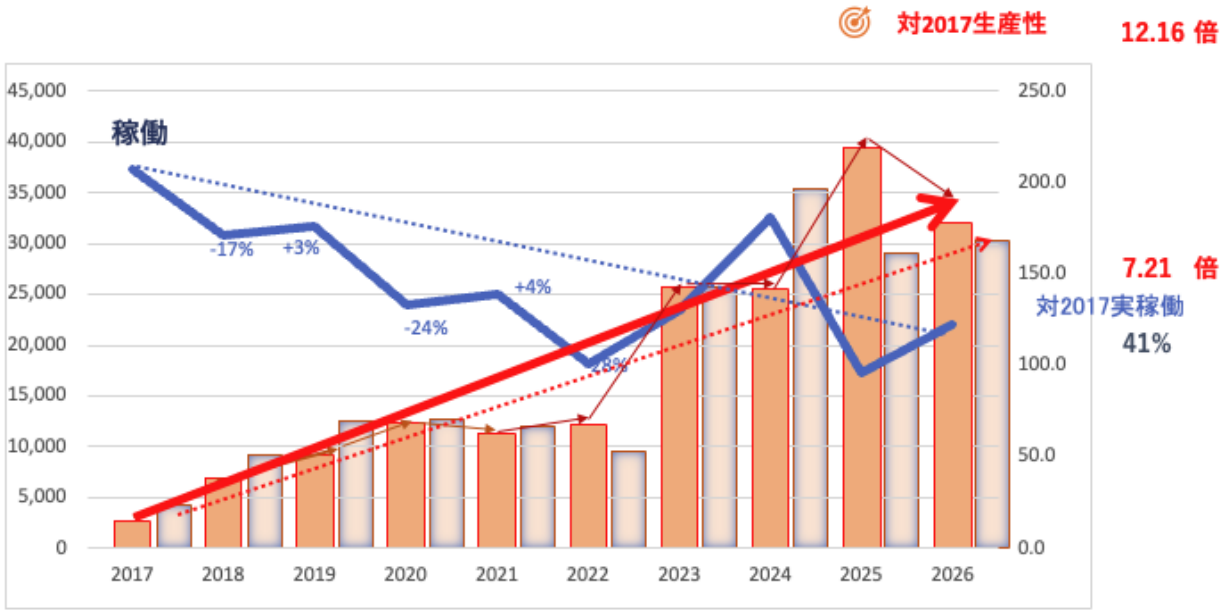
PROVEN IN PRACTICE

MSQA自らが実践し、成果を実証

自らマネジメントシステムを運用・実践し、意図した成果として生産性向上を実証しています。

12.16 倍
生産性（2017年比・生産性協会指標）

41 %減
要員の実稼働時間（2017年比）



売上・支援件数が増える一方で、要員の実稼働時間は減少。一人ひとりの生産性が向上しています。
棒グラフ：生産性（生産性協会指標）　折れ線：メンバーの実稼働時間

事象ベースのリスクマネジメント

2017年から実践。リスクを収益の源泉として捉え、マイナスの影響を抑えつつリターンの最大化を追求しています。2024年はISO/IEC 27017改正対応の需要で稼働が増えましたが、生産性の向上により多くの組織の支援を実現しました。

> 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。

出典：ISO/IEC 27005:2022

MSQA IN NUMBERS

数字で見るMSQA

全国の組織から選ばれ、受注額は2019年から大きく伸びています。

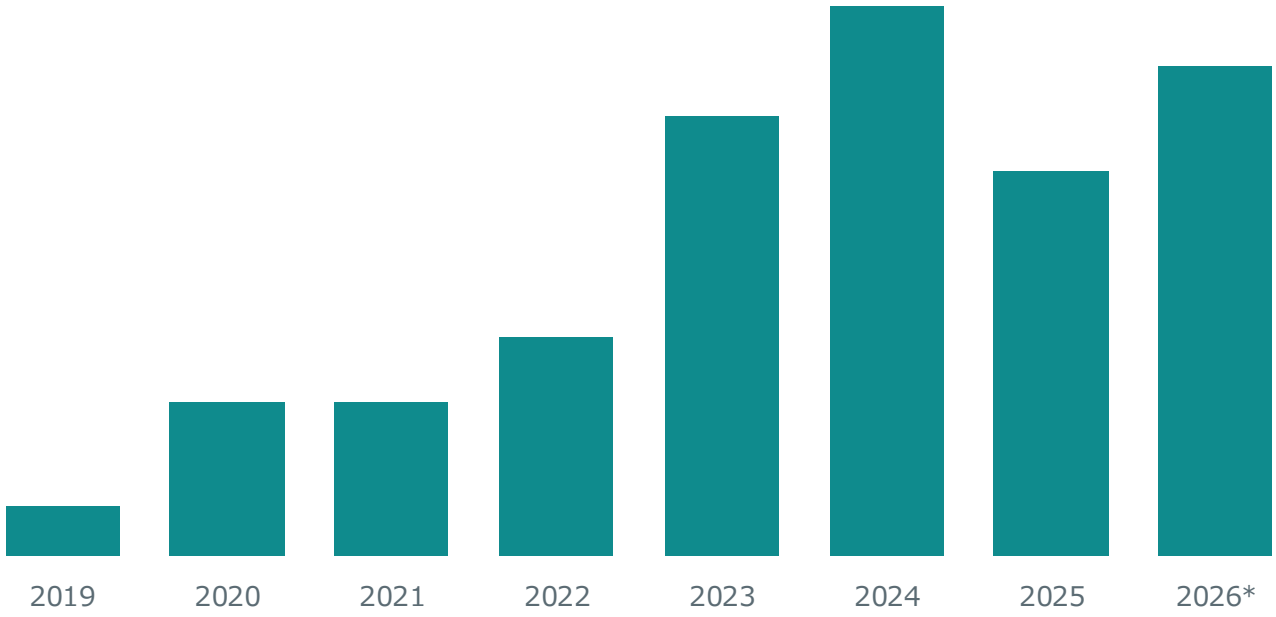
302件
延べ支援先組織・企業数

32都道府県
支援先の所在地

216件
研修受講者のレビュー

10倍超
受注額の伸び（2019年→2024年）

年間受注額の推移



2024年はISO/IEC 27001:2022改正対応の特需により突出しました。
法人会員（支援先企業）数も上場企業を加え、年々増加傾向にあります。

※セミナー及び書籍販売を除く受注額の推移。*2026年は10月中旬時点。

SERVICES

4つの支援で、認証から運用まで伴走

構築・認証取得だけでなく、その後の運用・監査・人材育成まで一貫して支援します。

認証支援

主任審査員が加わる現状調査から始め、
ISMS新規認証、
クラウドセキュリティ認証、ISMAP、
ISMS-PIMS、AIMSの導入を
伴走支援します。

運用支援

認証取得後の運用・改善、
リスクマネジメント改善、ISO 9001との
統合運用、ISMS再構築（規程・様式の
スリム化）を支援します。

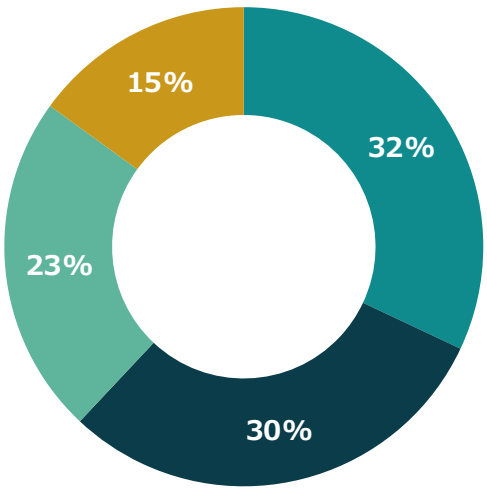
教育支援

JRCA承認研修・MSQA公認研修、
企業内研修に加え、LMSで
教材・様式を提供します。

監査支援

内部監査チームの派遣、監査プログラムの
作成・運用、チェックリスト等の
ツール提供、内部監査員の育成を
行います。

支援内容別の受注構成（2019～2026年累計）



運用支援	32%
認証支援	30%
教育支援	23%
監査支援	15%

最も大きいのは運用支援。認証取得後も継続して改善を支えるパートナーとして選ばれています。（その他支援は1%未満のため省略）

OUR APPROACH

現状調査から始める構築・再構築支援

ISMSの新規認証・構築・再構築において、主任審査員が
加わる現状調査（臨時監査）から始めます。

STEP 1

主任審査員を含むチームで支援

審査の視点を持つ主任審査員が構成メンバーとして参加します。

STEP 2

現状調査（臨時監査）

組織全体、各部門、適用範囲の業務プロセスを複数回に分けて調査し、記録を分析します。

STEP 3

現状を定量的に評価

マネジメントシステムと管理策の現状を5段階で定量評価し、見える化します。

STEP 4

フィットアンドギャップ分析

要求事項・管理策と現状を照らし合わせ、活かせる仕組みと不足を明確にします。

STEP 5

構築（再構築）・運用計画を作成し支援

分析結果に基づく計画で、構築から運用、認証審査まで伴走します。

**再構築では、ISO/IEC 27001 箇条6.3「変更の計画」に
基づいて変更の計画を作成し、認証審査まで伴走します。**

POLICY

『3つのやすい』　わかりやすい・すすめやすい・はじめやすい

目指すのは「維持審査を意識しない運用」。審査直前の作業をなくし、業務と連携したスリムで
スマートな運用を重視して、必要な文書・記録に限定した構築と運用をご提案します。

WHY START WITH A SURVEY

なぜ現状調査から始めるのか

ISMS・クラウドセキュリティ認証・SCS評価制度対応・ISMAP対応など、
新規認証・構築・再構築において現状調査から始めます。

現状調査から始める理由

すでに実施されているマネジメントプロセス及びセキュリティ対策の実施状況を正確に把握し、
フィットアンドギャップ分析により、要求を満たしていない点や不足を抽出することが目的です。
創業時の組織でない限り、すでに規則や規定・技術対策が取られているのが実情です。現状調査を
しっかり実施することで、効率的で効果的な構築・再構築が可能となります。

実施状況を正確に把握 › フィットアンドギャップ分析 › 課題を整理し対応計画を作成 › 作業量・工数が明確に

お見積りの考え方

構築・再構築をご検討の企業・組織からは、総額見積を求められることが多くあります。

フェーズ1の見積を優先

フェーズ1の見積を優先して着手し、
必要な作業量や工数が算定され次第、
フェーズ2以降の見積を提示します。

予算化に総額見積が必要な場合

フェーズ1を実施する前のヒアリングで
現状を把握し、これまでの支援実績をもとに
概算を提示します。最大値で算定し、予算を
超えることのないよう配慮します。

組織の現状に合わせた構築・再構築

現状調査から始めることで、組織の現状に合わせた構築・再構築が可能となり、
現状のマネジメントプロセスやセキュリティ対策との整合を図ります。

審査・監査のための直前作業を不要にします

審査・監査直前の準備作業を実施せず、普段の業務の中に組み込んで運用を進め、
審査・監査がいつ実施されても良い状態にすることを方針に支援します。

ISO/IEC 27001:2022 序文の「ISMSを，組織のプロセス及びマネジメント構造（management structure）全体の一部とし，かつ，その中に組み込むこと，並びにプロセス，情報システム及び管理策を設計する上で情報セキュリティを考慮することは，重要である」という一節を重視しています。

PROJECT MODEL

新規認証プロジェクトの進め方

約8〜12か月で認証取得を目指すモデルスケジュールです。推進会議（全12回）で進捗を共有します。現状調査の結果により、PHASE 3の期間は短縮・延長されます。

PHASE 1

現状調査・計画

1〜2か月目｜Plan

- キックオフ、事前チェックリストの作成
- 現状調査（6回）と記録分析
- 調査結果の分析評価、目標と達成計画の策定
- ISMS推進マニュアル初版の作成

PHASE 2

資産管理・人材育成

3か月目｜Plan

- 資産管理ワークショップ（情報資産の格付け・管理策決定）
- LMSによる事前学習
- JRCA承認フォーマル研修（40時間以上）の講師派遣

PHASE 3

リスク管理・実装
運用管理・定期研修

4〜5か月目｜Do・Check

- リスク管理ワークショップ、リスク対応計画の策定
- 附属書A管理策の実装、適用宣言書・推進マニュアル1版
- 定期研修（意識向上）

PHASE 4

内部監査
マネジメントレビュー
認証審査対応

6〜9か月目｜Check・Act

- 内部監査の実施と結果報告
- マネジメントレビュー＞次期目標と計画の策定支援
- 審査前研修、第一段階・第二段階審査の立会い
- 審査所見への対応（是正）支援

8〜12か月目　認証決定

認証後は運用支援・内部監査支援で
継続的な改善を支えます。

EVENT-BASED RISK MANAGEMENT

事象ベースで、効率的・効果的なリスク管理

資産の洗い出しに多大な時間をかけず、影響の大きいリスクに集中する。
ISO/IEC 27005:2022に準拠した事象ベースのアプローチでISMSを構築します。

従来の資産ベース

- 情報資産を詳細に洗い出し、資産・脅威・ぜい弱性の組み合わせで評価
- 台帳の作成と維持に多くの工数がかかる
- リスクが細分化され、重大なリスクが埋もれやすい

MSQAの事象ベース

- **起こり得る事象とその結果からリスクを特定**
- **高いレベル・戦略的なシナリオで重大なリスクに集中**
- **ワークショップで現場の知見を活かし、短期間で実施**

> ISO/IEC 27001は、資産、脅威及びぜい弱性の特定によるリスクの特定を要求していない。事象及び結果を考慮することによるリスクの特定など、他のリスク特定の方法を用いてもよい。
>
> **出典：ISO/IEC 27007:2020 情報セキュリティ監査の指針**

> 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、組織は自らの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。
>
> **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**

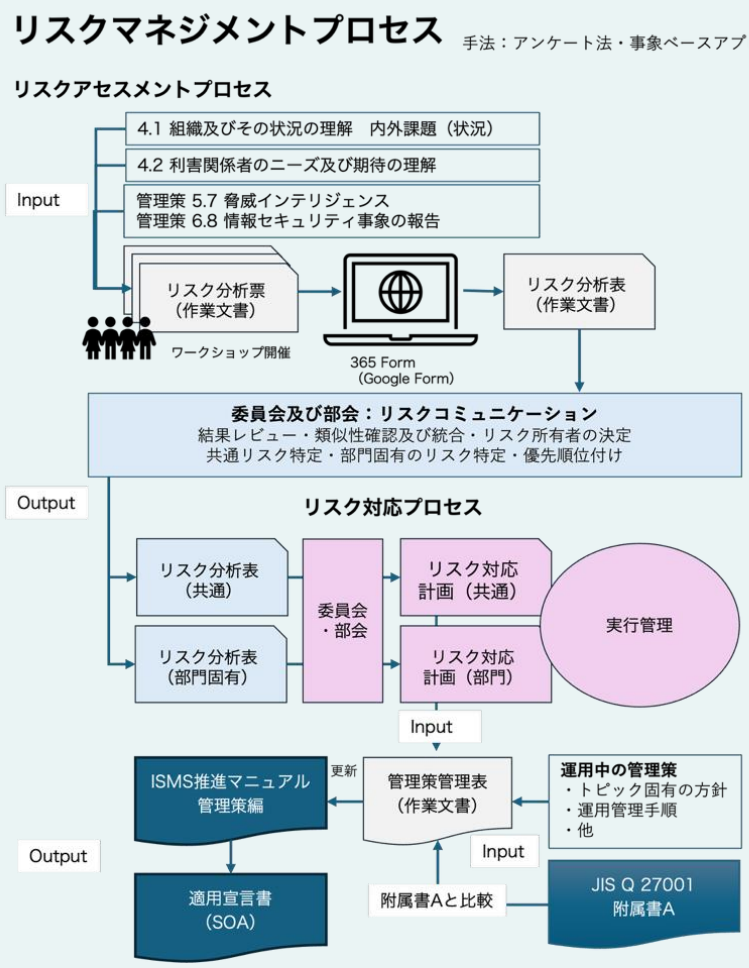
上場企業を含む多くの企業で導入、効果は実証済み

ISMS新規認証及びISMS再構築支援において、事象ベースのリスクマネジメントを多くの企業に導入いただいています。
MSQA自身も2017年から実践しています。

RISK MANAGEMENT PROCESS

リスクマネジメントプロセス（導入例）

ワークショップで事象を特定し、委員会・部会のリスクコミュニケーションを
経て、リスク対応と適用宣言書までを一つの流れで管理します。



1. 事象を特定

内外の課題、利害関係者の要求、
脅威インテリジェンスを入力に、ワークショップで
事象と結果からリスクを特定します。

2. シンプルに分析・評価

「起こり得る結果」と「現実的な
起こりやすさ」を各3段階で評価し、
掛け合わせてリスクレベルを決めます。

3. リスクコミュニケーション

委員会・部会で結果をレビューし、
類似リスクの統合、リスク所有者の
決定、優先順位付けを行います。

4. 対応計画から適用宣言書へ

リスク対応計画と管理策管理表を附属書Aと比較し、
推進マニュアルと適用宣言書に反映します。

PERFORMANCE VISUALIZATION

パフォーマンスを定量評価し、見える化

現状調査・内部監査・監視測定の結果を5段階で評価し、改善点と目標（KPI）を明確にします。

5段階の定量評価

マネジメントシステムと管理策を5段階で格付け。
不足や冗長を明らかにし、評価結果をKPIとして
活用できます（JIS Q 19011:2019の考え方に準拠）。

サイバーレジリエンスの見える化

ISO/IEC 27002:2022の属性
（#識別 #防御 #検知 #対応 #復旧）で評価し、
サイバー攻撃への強みと弱点を明確にします。

マネジメントレビューへ

見える化した現状をトップマネジメントへの
インプットとし、経営層と
パフォーマンスを共有します。



総合パフォーマンス評価シート（例）

認証審査でグッドポイントとして評価されました

内部監査では、マネジメントシステム及び管理策の実施状況について5段階の定量的な評価を実施していました。管理策の成熟度評価やサイバーセキュリティレジリエンスが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。

ご支援先の審査所見より抜粋

2026年

AIMS・クラウドセキュリティ・
サイバーセキュリティに加え、
SCS評価制度にも対応した
見える化を開始

監査支援

内部監査支援で定量評価を実施。
監査員育成では評価方法と評価ツールを提供

STANDARDS

幅広いマネジメントシステムに対応

情報セキュリティを中心に、クラウド・プライバシー・AI・
政府調達・サプライチェーンまでカバーします。

ISMS

ISO/IEC 27001

情報セキュリティマネジメントシステムの
構築・認証・運用

クラウドセキュリティ

ISO/IEC 27017（ISMS-CLS）

クラウドサービス固有の
リスクに対応した管理策

ISMS-PIMS

ISO/IEC 27701

プライバシー情報マネジメントの構築

AIMS

ISO/IEC 42001・JIS Q 42001

AIマネジメントシステムの
導入と活用ガイドブック

ISMAP

**政府情報システムのための
セキュリティ評価制度**

クラウドサービスの構築・登録支援

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**

★3確認・★4評価への対応支援

統合支援

複合支援・ISO 9001等との統合

本ページの全てを複合して支援でき、
ISO 9001など他のマネジメントシステムとの
統合も可能。ビジネスを支える効率的で効果的な
マネジメントシステム等の統合運用を
支援します。

SOC2 / SOC3

報告書取得に向けた対応

既存ISMSを基盤に、ギャップ分析から
統制設計、Type1・Type2評価まで支援

WHY COMPETENCE MATTERS

教育研修を重視する理由

認証取得後の維持活動を支えるのは、管理者や担当者の力量です。

認証取得後も力量を維持する

MSQAでは、認証取得後の維持活動のため、管理者や担当者が力量を有し、
維持できていることを重視しています。セキュリティ対策は技術的な対策も
さることながら、要員が正しい知識と能力（力量）を備えることが大切です。

ISO/IEC 27001「7.2 力量」の要求

ISO/IEC 27001などマネジメントシステム規格の「7.2 力量」では、以下のように要求しています。

組織は，次の事項を行わなければならない。

a)	組織の情報セキュリティパフォーマンスに影響を与える業務を その管理下で行う人（又は人々）に必要な力量を決定する。
b)	適切な教育，訓練又は経験に基づいて，それらの人々が力量を備えていることを確実にする。
c)	該当する場合には，必ず，必要な力量を身に付けるための処置を講じ，講じた処置の有効性を評価する。
d)	力量の証拠として，適切な文書化した情報を保持する。

MSQAの取り組み

MSQAでは必要な力量を定義し、適切な教育訓練を提供するとともに、講じた処置の有効性を
評価し、第三者機関として力量を認定し、力量の証拠として修了証やバッジを発行しています。

a) **必要な力量を定義** › b) **適切な教育訓練を提供** › c) **処置の有効性を評価** › d) **力量を認定し修了証・バッジを発行**

WHY MSQA TRAINING

MSQAの教育研修が選ばれる理由

教育研修の品質は、どの研修機関にも負けないと自負しています。

JRCA承認研修機関

JRCA承認フォーマル研修
ー ISMS管理技術者 Lv3認定
ー ISMS審査員（監査員）資格取得
クラウドセキュリティ審査員研修（ISMS-CLS TC-07）

01

オリジナルガイドを教本に

MSQAが執筆・発行する実践ガイドを教本として使用します。
研修後も現場の手引きとして使い続けられます。

02

運用実績から生まれた実践ツール

MSQA自らの運用実績と、支援の現場で得た
知見をもとにした実践ツールを使って学びます。

03

実践的なワークショップが豊富

演習とワークショップを豊富に取り入れ、
受講後すぐに現場で使える力を養います。

40 時間以上
JRCA承認フォーマル研修
ー ISMS管理技術者 Lv3認定
ー ISMS審査員（監査員）資格取得
ー 演習50％以上

12 時間以上
JRCA承認ISMS-CLS研修
ー クラウドセキュリティ管理技術 Lv3認定
ー ISMS-CLS審査員（監査員）資格取得

216 件
継続的専門能力開発コースなど
受講者の声

TRAINING

実務で使える力を育てる教育研修

JRCA承認研修とMSQA公認研修の2本柱。オンライン・集合・企業内のいずれにも対応します。

JRCA承認研修コース

審査員登録に必要なフォーマル研修

ISMS審査員研修

JRCA承認フォーマル研修（コード ISMS6A）。計40時間以上・演習50%以上。
2026年度は10回開催（予定含む）。

クラウドセキュリティ審査員研修

ISMS-CLS承認研修機関（登録番号 ISMS-CLS TC-07）。
ISMS審査員の力量をクラウドへ拡張するアドオン研修（計12時間以上）。

ISMS継続的専門能力開発（CPD）

各5時間。クラウドセキュリティ管理技術／最新情報と
脅威インテリジェンス／ISMS運用技術／監査（審査）技術。

MSQA公認研修コース

- Lv1 ISMS基礎研修
- Lv2 リスクマネジメントプロセス管理基礎研修
- Lv3 ISMSリスクアセスメント研修
- Lv2 ISMS内部監査員養成研修
- Lv4 ISMSフォーマル研修講師 育成研修
- Lv5 SCSセキュリティ専門家研修

オンライン
ZOOMで全国から受講

集合研修
対面で演習中心に学ぶ

企業内研修
オンサイト・リモートで実施

ORIGINAL GUIDES

現場で選ばれる実践ガイド・教材

JRCA承認研修の教本（教材）として使用しているほか、マネジメントシステムの構築・再構築では担当者用ガイドとしてご提供しています。



ISMS推進マニュアル活用ガイドブック

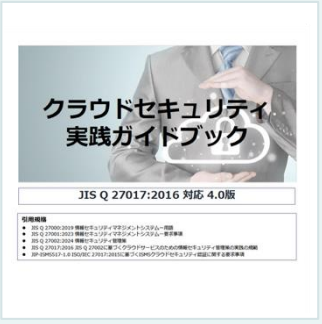
JRCA承認研修 教本

ISMS｜冊子



AIマネジメントシステム推進マニュアル活用ガイド

AIMS



クラウドセキュリティ実践ガイド

JRCA承認研修 教本

クラウド｜冊子



ISMS及び改正管理策一覧 12.1版

JRCA承認研修 教本

ISMS｜電子版



ISO/IEC 27017:2026 クラウドセキュリティ管理策 新旧対比一覧

クラウド



ISO/IEC 27002:2022 対応 情報セキュリティ管理策実践ガイド

JRCA承認研修 教本

ISMS｜冊子



マネジメントシステム監査（審査）実践ガイド

JRCA承認研修 教本

監査｜冊子

オンラインストアで販売中

isms-society.stores.jp

冊子・電子版をご用意しています。

ストアはこちら

COMPETENCE CERTIFICATION

力量を「見える化」する認定バッジ

研修修了と認定試験で力量を段階的に認定。次に目指すレベルが明確になります。

例：ISMS管理技術者のレベル（Lv1〜Lv7）



認定区分



ISMS管理技術者

Lv1〜Lv7

自組織のISMS推進を担う基幹人材



ISMSフォーマル研修講師

Lv2〜Lv7

各コースを担当できる講師人材



ISMS内部監査員

Lv2〜Lv6

内部監査を計画・実施できる人材



ISMSコンサルタント

Lv3〜Lv7

構築・運用を指導できる専門家



ISMS審査員

Lv3〜Lv7

JRCA承認研修と連動した審査員



SCSセキュリティ専門家

Lv5

SCS評価制度の★3確認・★4評価



クラウドセキュリティ管理技術者

Lv3〜Lv7

クラウド固有リスクへの対応力

認定バッジは名刺・署名・SNSなどで提示でき、組織の人材力を対外的に示せます。

VOICES

受講者の声

研修予約サイトに寄せられたレビューから抜粋してご紹介します。

216件

受講後のレビュー件数
（研修予約サイト掲載、
2026年10月時点）

右のQRコードから、すべての
レビューをご覧いただけます。

レビューはこちら

> 今回でCPD研修は3回目の参加となります。毎回、実際の現場の運用に則した説明なので、非常に分かりやすく、提供される資料も沢山ありますので、業務においても重宝しています。

> 情報セキュリティに関する最新の動向と、リアルな背景を踏まえて、規格や制度の変化についてご説明いただけるので腹落ちしながら理解を深める事ができます。

> 規格の説明のみならず、改正ポイントや管理策適用ノウハウについても、分かりやすく解説くださいました。オリジナルのテキストについても、今後も使わせていただきます。

> 講師の方の豊富な経験と知識で盛りだくさんのテキストで大変役に立ちます。解説もわかりやすいです。また以前受講した際の資料のアップデート版もいただくことができて大変助かります。

VOICES

受講者の声（実践・リスクマネジメント）

現場の運用に結びつく実践的な内容と、事象ベースのリスクマネジメントが評価されています。

> 規格の内容や解釈を淡々と述べるのではなく、その解釈と
> マネジメントシステムの本来の目的を基に「効率的・効果的な運用」の実現を
> 目指して工夫された実践例を聞くことができるので、非常に有用な時間に
> なっております。

> 「規格がこうなっているからリスク対応しなくてはいけない」という一辺倒の
> お話ではなく、「（活動に）リスクが潜在するから、リスク対応のために
> 規格を利用してリスク対応しましょう」という現場側、規格側の意図を
> 踏まえたお話であり、大変勉強になりました。

> 事象及び結果の評価を通じてリスクを特定しアセスメントを
> 行うことで、高いレベルの改善シナリオを確立することができる
> ことを具体的な手順により示され理解しやすい内容でした。

> 『ISMSリスクアセスメント（事象ベースのアプローチ）
> 実践セミナー』では、リスク分析票の実例が参考になった。

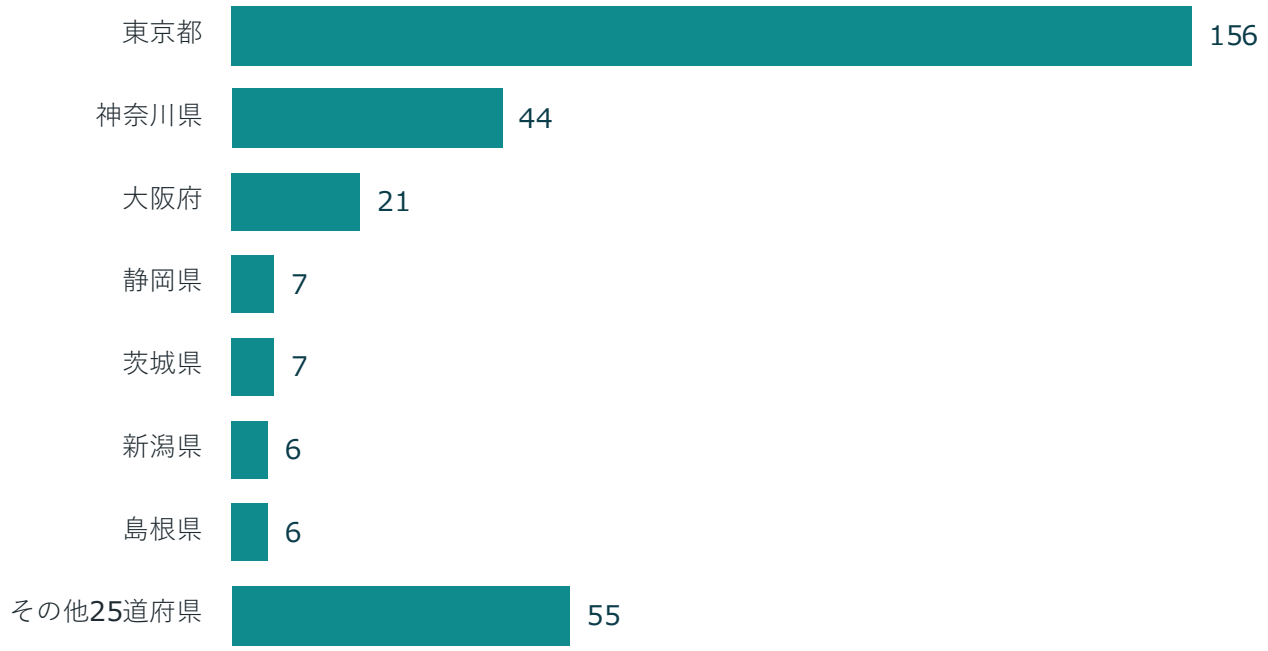
> クラウドセキュリティの実践を伴ったCPDでした。
> 毎回、経験された内容をお話し頂いていますので、自分の
> 事のような想像ができますので、大変参考になっています。

TRACK RECORD

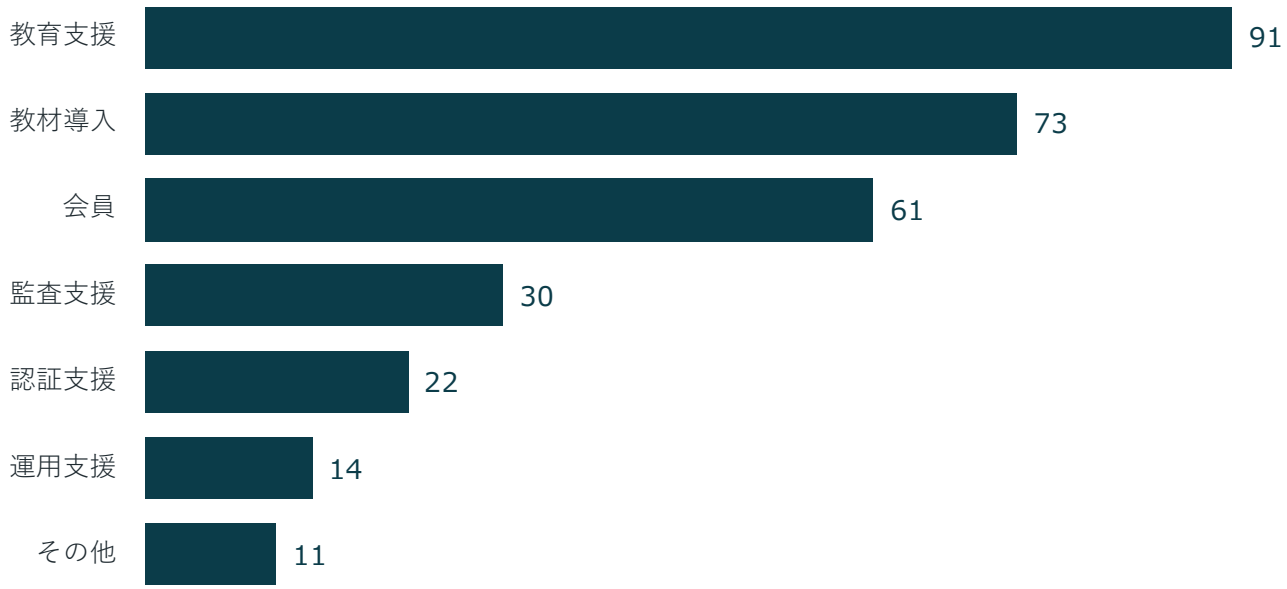
全国32都道府県・延べ302件の支援実績

首都圏を中心に、北海道から九州まで全国の組織を支援しています。

都道府県別の支援件数（延べ）



支援内容別の件数（延べ）



※2026年10月時点の社内集計。1組織が複数の支援内容に該当する場合はそれぞれ計上。

MEMBERSHIP

会員制度で、継続的な相談相手に

MSQAは、組織の形態よりも「関係性」を重視する会員制の
非営利法人です。関わり方に合わせて3つの会員区分をご用意しています。

協会の運営に寄与する会員

正会員

- 総会への参加と議決権、理事の互選
- ワーキンググループ・技術委員会・運営委員会の主催・参加
- 法人会員・パートナー会員としての権利
- 入会は正会員の紹介と理事会の承認が必要です

各種支援をご利用いただく会員

法人会員 **一般会員**

- 会員価格の適用、Cloud for LMSの利活用、技術委員会への参加（法人会員）
- 法人会員はマネジメントシステム支援の専用コースを利用可能
- 従業員の教育研修（力量管理）や運用管理コンテンツとサービスを提供
- 力量を身につけるための教育研修プログラムの提供及び教材作成提供
- 法人会員へはJRCA承認フォーマル研修など企業内研修に講師を派遣
- 運用管理に関する相談など多角的なサポートを受けることが可能です

ビジネスパートナーとして活動いただく会員

パートナー会員 **賛助会員**

- ビジネスパートナーとしての活動
- コンサルティング業務や人材育成事業の支援
- 自社のコンテンツ・サービスをMSQA支援先企業に情報発信
- 賛助会員は協会の事業を賛助

会員制度の詳細・入会申請

入会金・年会費、入会申請フォームは会員制度のページで
ご案内しています。右のQRコードからご覧ください。

https://msqa.jp/members.html

NEXT STAGE

次期の活動目標

教育研修事業の公的な位置づけを強化し、より多くの方が学べる環境を整えます。

承認されました

経済産業省「マナビDX」への講座登録

デジタル人材育成のポータルサイトに講座を掲載し、学び直しを考える方に広く届けます。
承認された研修コース：JRCA承認ISMSフォーマル（管理技術者・審査員資格取得）研修
力量認定：ISMS管理技術者Lv３

申請完了

SCS評価制度における研修事業者登録

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の
専門人材を育成する研修事業者を目指します。

申請完了

「第四次産業革命スキル習得講座／専門実践教育訓練講座」の申請

認定・指定を受けた講座として、受講者が公的な支援制度を活用しやすい研修を提供します。

目指す姿

**JRCA承認研修とMSQA力量認定制度に、公的な講座認定を加え、
実務で使えるマネジメントシステム人材を全国へ。**

※2026年10月時点で、マナビDXは承認済み、その他の制度は申請が完了した段階です。

CONTACT

まずはお気軽にご相談ください

認証取得の準備、運用の見直し、内部監査、人材育成など、
どの段階からでもご相談いただけます。

1
お問い合わせ

2
現状と課題のヒアリング

3
最適な支援メニューのご提案

所在地
〒110-0016 東京都台東区台東1-11-10 大木ビル

Webサイト
https://msqa.jp/（お問い合わせフォーム）

研修情報・LMS
https://msqa-lms.jp/

研修予約・受講者の声
https://isms-society.stores.jp/reserve/msqa

お問い合わせ
msqa.jp/contact.html

公式サイト
msqa.jp

一般社団法人マネジメントシステム品質協会（MSQA）