改正2.0 2026年2月4日発行

ISMAP構築支援プロジェクト概要

政府情報システムのためのセキュリティ評価制度への対応

一般社団法人マネジメントシステム品質協会 編
私たちは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

はじめに

- 近年、行政機関におけるクラウドサービスの利用は急速に拡大しており、その安全性・信頼性を客観的に担保する仕組みとして「政府情報システムのためのセキュリティ評価制度（ISMAP）」の重要性が高まっています。ISMAPは、政府が求める高いセキュリティ水準を満たしたクラウドサービスのみを事前に評価・登録する制度であり、単なる技術的対策の有無だけでなく、組織体制、運用管理、証跡管理、委託先統制、インシデント対応など、多面的かつ継続的な管理能力が求められます。そのため、ISMAP対応は一時的な対応プロジェクトではなく、経営層の関与のもとで全社的に取り組むマネジメント活動として位置付けることが不可欠です。

- 一方で、ISMAPの管理基準は広範かつ詳細であり、既存のISMSやクラウドセキュリティ認証を取得している場合であっても、責任共有モデルの整理、ログ・変更管理の実証、契約・規程類の整合など、追加的な整備や高度化が必要となるケースが少なくありません。また、実際の監査においては、文書整備のみならず「実際に運用され、証明できること」が強く求められるため、証跡の体系化や部門横断の連携体制の構築が成功の鍵となります。

- 本提案書では、こうしたISMAP制度の特性を踏まえ、対象組織の成熟度や既存統制の状況に応じた最適な支援アプローチを提示するとともに、ギャップ分析から統制整備、証跡構築、監査対応、登録後の維持運用に至るまで、一貫した支援サービスの提供方針を示します。単なる基準適合を目的とするのではなく、クラウドサービスの信頼性向上と事業競争力強化を両立させる持続可能なセキュリティ基盤の確立を最終的な目標とします。

ISMAP管理基準が改正されます 令和７年12月25日時点

ISMAP管理基準について、改正された国際規格(JIS Q 27001:2023、 JIS Q 27002:2024、ISO/IEC 27014:2020)の反映、管理策の数を減らす見直し等が実施されます。

※本管理基準の改定日・施行日については検討中で、適宜更新される可能性があります。

さらに、改正が予定されている国際規格（JIS Q 27017）を反映するための改正が想定されます。

ISO/IEC 27017は2026年1月14日FDIS（ファイナルドラフト）が発行され、８週間で最終投票ののちISOとして正式に発行されます。

ISMAP 管理基準

ISMAP 管理基準の目的 ISMAP 管理基準は、クラウドサービス事業者がISMAPクラウドサービスリスト (以下「ISMAP 等クラウドサービスリスト」という。)への登録申請を行う上で実施すべきセキュリティ対策の一覧及びその活用方法を示すことを目的としており、ISMAPの情報セキュリティ監査基準等に従って監査を行う場合、原則として監査人が監査の前提として用いる基準となる。

ISMAP基準の特質

本制度においては、情報セキュリティ監査の仕組みを活用した枠組みを活用することとしている。
これは、民間において実施されている情報システムに関するセキュリティ監査により、既に一定程度の知見が集積していること、一定の評価水準を確保することが可能なこと、運用後の継続的な確認が可能であることといった観点による。

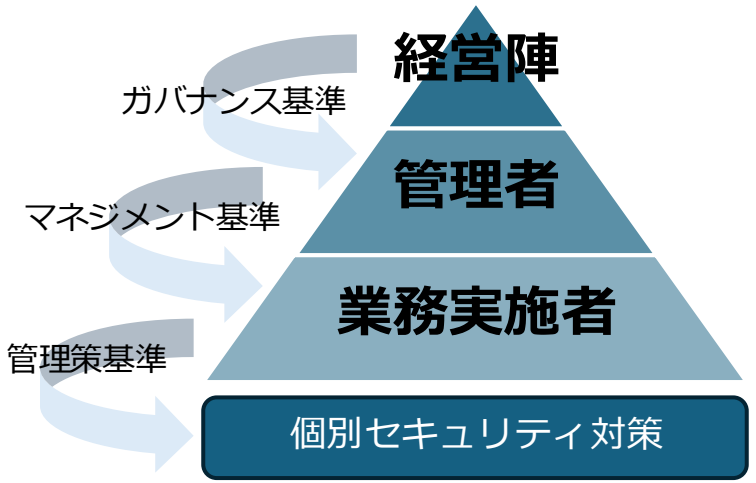
本管理基準は、以下の規格に準拠及び文書を参照し作成されている。

情報セキュリティ管理基準(令和７年改正版)	JIS Q 27001:2023 JIS Q 27002:2024 ISO/IEC 27014:2020
クラウド情報セキュリティ管理基準(平成28年3月版)	JIS Q 27001:2014 JIS Q 27002:2014 JIS Q 27017:2016
政府機関等のサイバーセキュリティ対策のための統一基準群（令和７年度版）	統一基準群は、国の行政機関及び独立行政法人等（以下「政府機関等」という。）の情報セキュリティ水準を向上させるための統一的な枠組みであり、政府機関等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定しています。
NIST Special Publication 800-53 Revision 5	組織と情報システムのための セキュリティおよびプライバシー管理策

JIS Q 27002:2024発行に伴い改正されます

ISMAP 管理基準の構成

管理基準は、「ガバナンス基準」、「 マネジメント基準」及び「管理策基準」から構成される。それぞれの基準は、統制目標と詳細管理策で構成される。それぞれの基準が対象として想定する主体や各項目の粒度の関係を示した概念図が右記のものとなる。



ガバナンス基準	組織体のガバナンスのうち、情報セキュリティガバナンスを確立するための目的及びプロセスを定めている。
マネジメント基準	管理者が実施すべき事項として、情報セキュリティマネジメントの確立、運用、レビュー、維持及び改善、文書化した情報の管理並びに情報セキュリティリスクコミュニケーションに必要な事項を定めている。
管理策基準	組織における情報セキュリティマネジメントの確立段階において、リスク対応方針に従って管理策を実施する際の選択肢を与えるものである。

「管理策基準」における詳細管理策を実施するための参考情報（例示）として、手引きを定めている。

基本言明要件

クラウドサービス事業者は、言明の対象となる管理策として、以下の内容を実施し、書面にて言明を行わなければならない。また、特に変更の言明が行われていない限りにおいて、その言明はクラウドサービス事業者が責任を負うものとして有効であると見なされる。なお、言明の対象となるクラウドサービスの基盤に言明の対象外となるサービスを利用している場合において、当該対象外のサービスがISMAPクラウドサービスリストに登録されている場合には、当該対象外のサービスが実施している統制を引き継ぐことで当該統制に係る監査の手続を省略することができる。

⑴ ガバナンス基準 ： 全て実施しなければならない。
⑵ マネジメント基準 ： 全て実施しなければならない。
⑶ 管理策基準 全ての統制目標としての管理策について、原則として実施しなければならない。また、詳細管理策（X.X.X）も原則として実施すべきものとする。 他方、クラウドサービス事業者は自身の提供するサービスと照らし、合理的な適用が不可能又はリスク分析の結果、実施不要と適切に判断した統制目標としての管理策及び詳細管理策については、その理由を示すことで対象外とすることができる。

ガバナンス基準

情報セキュリティガバナンスの概要

情報セキュリティガバナンスでは、組織体における複数のガバナンスの領域のうち、組織体の情報セキュリティ確保の達成に関するガバナンスを扱う。情報セキュリティに関するガバナンスモデルの策定にあたっては、情報技術等の他のガバナンスの領域とのモデルの対象範囲の重複の可能性があり、コーポレートガバナンスの観点からそれぞれの整合についての考慮が求められる。 ガバナンス主体は、組織体内に情報セキュリティマネジメントシステムを構築する。情報セキュリティマネジメントシステムの目的は、組織のサイズ、スケール及び構造により異なる可能性があり、それらを整合させるようにする。 なお、本管理基準の「第４章 マネジメント基準」に示す管理策にも、情報セキュリティマネジメントシステムにおけるガバナンスに対応する内容が含まれている。

情報セキュリティガバナンスの目的

ガバナンス主体は、以下に示す目的に照らして適切な、組織体における情報セキュリティガバナンスの目的を設定する。

目的１：組織体全体の統合された包括的情報セキュリティを確立する

目的２：リスクに基づく取組を採用して意思決定を行う

目的３：投資の方向性を決定する

目的４：内部及び外部の要求事項との適合性を確実にする

目的５：セキュリティに積極的な文化を醸成する

目的６：セキュリティのパフォーマンスが現在及び将来の組織体の要求事項を満たすことを確実にする

マネジメント基準

マネジメント基準は、JIS Q 27001:2023を基に、情報セキュリティについて組織を指揮統制するために調整された活動である、情報セキュリティマネジメントの確立、運用、レビュー、維持及び改善、文書化した情報の管理並びに情報セキュリティリスクコミュニケーションを行うための基準を定める。 クラウドサービスにおいては、クラウドサービス利用者の環境等を考慮して、クラウドサービス提供者の管理策等を検討し、実施する必要がある。そのため、クラウドサービス利用者及びクラウドサービス事業者間において、クラウドサービスにおける情報セキュリティリスクとその対応について、情報交換することが非常で重要である。リスクコミュニケーションについては、クラウドサービスにおいて特に考慮するべき事項として規定する。

情報セキュリティマネジメントの確立

情報セキュリティマネジメントを確立するために、その基盤となる適用範囲を決定し、方針を確立する。これらをもとに、情報セキュリティリスクアセスメントを実施し、その対応を計画し実施する。それにより、必要なプロセス及びそれらの相互作用を含む、組織が有効な情報セキュリティマネジメントを実施するための基盤作りを行う。 情報セキュリティリスクコミュニケーションは、意思決定者とその他の利害関係者との間で情報セキュリティリスクに関する情報を交換、共有し、リスクを管理する方法に関する合意を得る。 マネジメント基準における統制目標及び詳細管理策は、別表2に定められている。

管理策基準

管理策基準は、情報セキュリティ管理基準における管理策の整理体系を踏襲している。

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

並びにクラウド情報セキュリティ管理基準の一部の管理策を基礎とした「9 クラウドサービス固有の管理策」で構成される。

管理策基準における統制目標及び詳細管理策は、別表3に示されている。

ISMAP評価基準の全体構成と項目数の例

ISMAP管理基準は次の3つの主要カテゴリーに分かれています。

分野	項目数（概数）	内容概要
① **ガバナンス基準**	約 **18項目**	情報セキュリティガバナンスの仕組み（戦略・方針・責任・評価など）
② **マネジメント基準**	約 **85項目**	ISMS的な管理プロセス（リスク評価・計画・実行・点検・改善など）
③ **管理策基準**	約 **1,095項目超**	技術・運用管理レベルのコントロール（詳細管理策）
合計	約 **1,198項目以上**	ISMAP全体の管理策総数（概数）

① ガバナンス基準（18項目）
対象者： 経営層・組織トップ
主な内容：
- 情報セキュリティ戦略と目的の定義・承認
- ガバナンス体制・指揮統制の確立
- リスクマネジメント方針の策定
- 法令・契約遵守の統一基準整備

※クラウド事業者全体の方針や仕組み、継続的な監視・評価といったトップ視点の統制が求められます。

② マネジメント基準（85項目）
対象者： 管理者・セキュリティ責任者
主な内容：
- 情報セキュリティポリシー整備
- リスクアセスメント実施方法
- 計画・実装・点検・改善のサイクル化
- 役割と責任の明確化・教育・訓練管理
- 外部委託先とのセキュリティ統制管理

※ISMSでいうPDCA（計画・実行・点検・改善）の体系化リスク管理とそれを運用する体制が該当します。

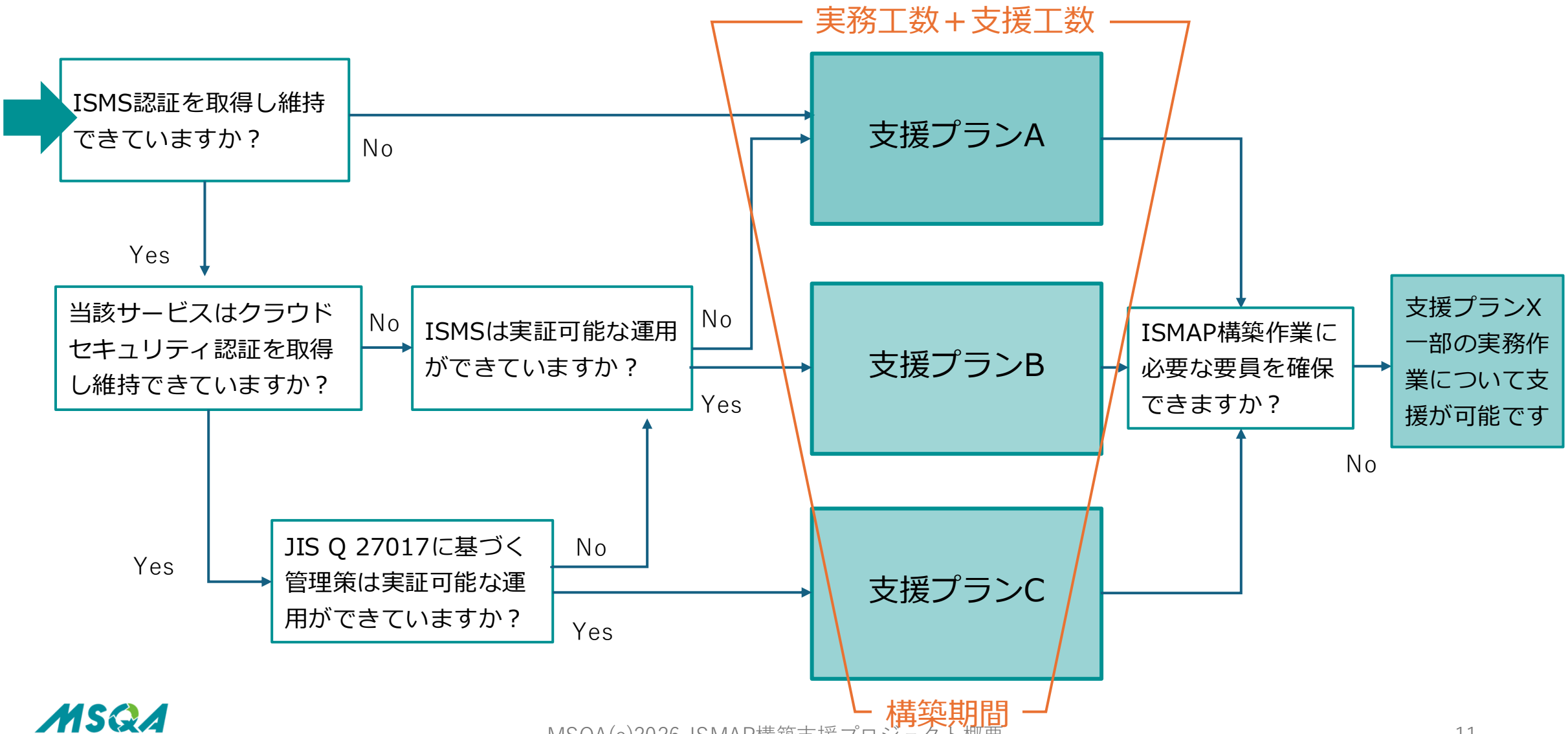
③ 管理策基準（約1,095項目超）
対象者： 実務担当者・運用部門
主なカテゴリ例（代表的なもの）：
1. 情報セキュリティ方針と組織管理
2. 人的資源のセキュリティ
3. 資産管理
4. アクセス制御・認証管理
5. 暗号・鍵管理
6. 物理的環境・環境セキュリティ
7. 操作・運用のセキュリティ
8. 通信の安全性
9. システム開発・保守管理
10. 供給者／外部委託管理
11. インシデント対応管理
12. 事業継続と可用性管理
13. 順守（法令／契約）管理

※これらは、ISO/IEC 27001/27002/27017に加え NIST SP800-53 等を参考に非常に詳細な管理策として整理されており1,000項目超が要求されています。

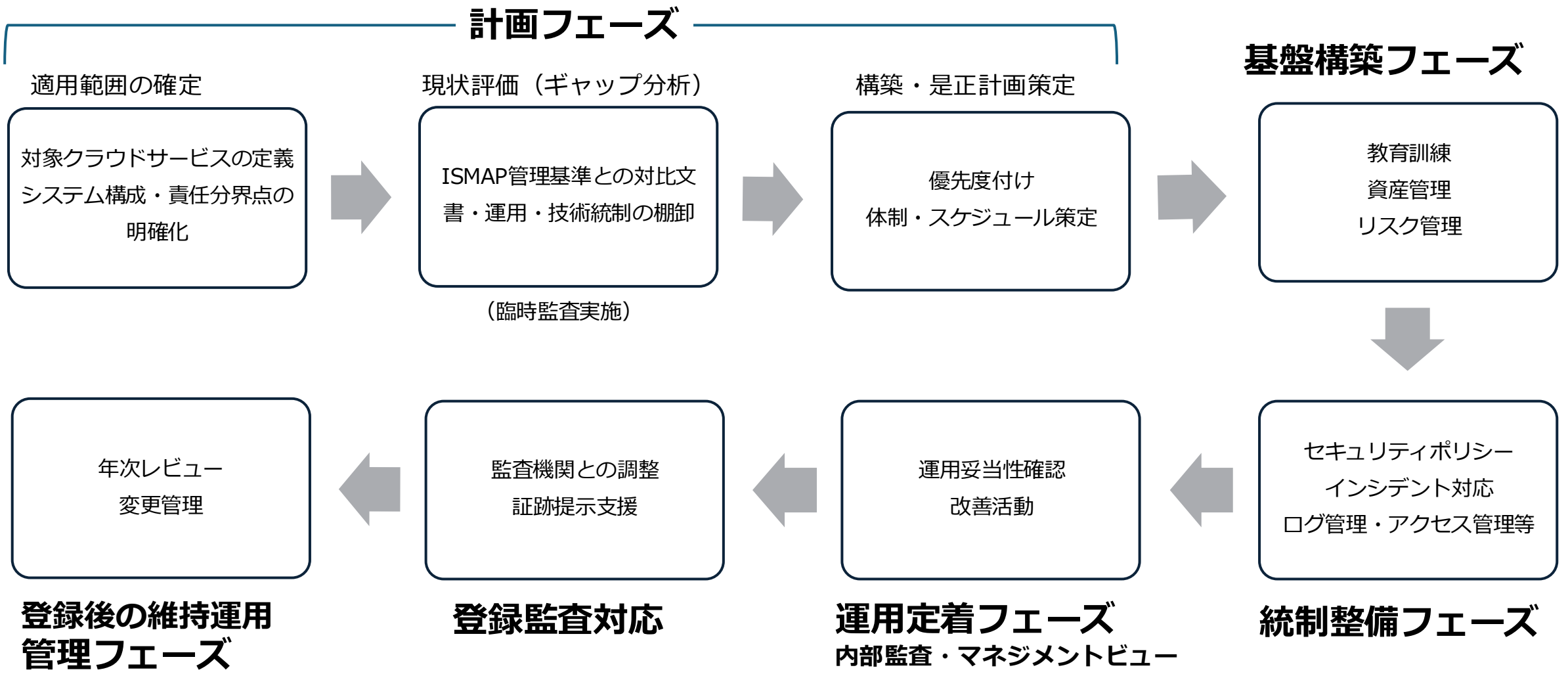
ISMAP評価項目の選択・適用について

- **ガバナンス基準とマネジメント基準は原則すべて必須適用** となります。
- **管理策基準は「統制目標」が原則必須**、詳細管理策はサービスの特性に応じて選択適用可能な項目もありますが、多くの重要管理策は必須です。

1.支援プランの選択肢


実務工数＋支援工数
ISMS認証を取得し維持できていますか？
No
Yes
当該サービスはクラウドセキュリティ認証を取得し維持できていますか？
No
ISMSは実証可能な運用ができていますか？
No
Yes
Yes
JIS Q 27017に基づく管理策は実証可能な運用ができていますか？
No
Yes
支援プランA
支援プランB
支援プランC
ISMAP構築作業に必要な要員を確保できますか？
No
支援プランX
一部の実務作業について支援が可能です
構築期間

2. ISMAP認証取得の一般プロセス



3.ISMAP構築支援における想定工数と具体的作業内容の例

実際の規模（クラウドサービス数、システム複雑性、組織規模）により±30～50%程度の変動が想定されます。

工数は目安として

現場担当者（依頼側）　＝内部工数

支援事業者（コンサル／監査支援）　＝外部工数

を分けて記載しています。

単位： **人日（1人×1日＝8時間想定）**

3.1 プラン別全体想定工数

支援プランA：ISMS未取得事業者

ISMS認証を取得しているが実証可能な運用ができていない場合は支援プランAを推奨します。
調査結果でプランAを推奨する場合があります。

区分	人日目安	プランX適用
現場担当者工数	120～180人日	90 ～ 120人日
MSQA支援工数	110～160人日	140 ～ 220人日

支援プランB：ISMS取得事業者

クラウドセキュリティ認証を取得しているが実証可能な運用ができてきていない場合は支援プランBを推奨。
調査結果によりプランAを推奨する場合があります。

区分	人日目安	プランX適用
現場担当者工数	70～110人日	50 ～90人日
MSQA支援工数	60～100人日	80 ～120人日

支援プランC：クラウドセキュリティ認証取得事業者

クラウドセキュリティ認証を取得しているが実証可能な運用ができてきていない場合は支援プランBを推奨

区分	人日目安	プランX適用
現場担当者工数	40～60人日	30 ～ 70人日
MSQA支援工数	50～80人日	60 ～100人日

注記：支援プランXで一部の実務作業について支援が可能です。実際の規模（クラウドサービス数、システム複雑性、組織規模）により±30～50%程度の変動が想定されます。

3.2 支援プランA：ISMS未取得事業者例

計画フェーズ

作業内容	現場	支援
適用範囲の確定	2	2
現状評価（分析）	5	8
構築・是正計画策定	3	3
導入研修	1	1

基盤構築フェーズ

作業内容	現場	支援
キックオフ・体制構築	3	2
情報資産洗い出し	15	8
リスクアセスメント	20	15
基本方針・規程作成	10	20
教育・意識向上研修	5	3

統制整備フェーズ

作業内容	現場	支援
アクセス権棚卸	12	6
ログ管理設計	10	8
委託先管理整備	8	6
インシデント管理整備	10	8
技術統制設定確認	20	12

運用定着フェーズ
内部監査・マネジメントビュー

作業内容	現場	支援
管理者・実務管理研修	2	2
内部監査	10	10
是正対応	5	8
証跡整理	10	6
マネジメントレビュー	2	2

登録監査対応

作業内容	現場	支援
証跡一覧作成	10	6
想定問答集作成	5	6
模擬監査	6	8
監査対応	10	10
是正対応	15	8

登録後の維持運用管理フェーズ

作業内容	現場	支援
セキュリティ目標確立	1	1
維持管理計画作成	2	2
改善サイクル確立	1	2
方針群のレビュー	5	3

注記：支援プランXで一部の実務作業について支援が可能です。実際の規模（クラウドサービス数、システム複雑性、組織規模）により±30～50%程度の変動が想定されます。

3.3 支援プランB：ISMS取得事業者例

差分分析フェーズ

作業内容	現場	支援
現状評価（分析）	5	8
管理策マッピング	8	12
証跡レビュー	10	10
責任分界整理	6	6

基盤構築フェーズ

作業内容	現場	支援
キックオフ・体制構築	1	2
情報資産洗い出し	3	4
リスクアセスメント	5	8
基本方針・規程作成	5	10
教育・意識向上研修	5	3

拡張整備フェーズ

作業内容	現場	支援
クラウドログ強化	12	8
暗号鍵管理見直し	6	6
脆弱性管理高度化	8	6
委託先条項見直し	6	4
技術統制設定確認	10	6

運用定着フェーズ
内部監査・マネジメントビュー

作業内容	現場	支援
管理者・実務管理研修	2	2
内部監査	10	10
是正対応	3	5
証跡整理	10	6
マネジメントレビュー	2	2

登録監査対応

作業内容	現場	支援
証跡一覧作成	10	6
想定問答集作成	5	6
模擬監査	6	8
監査対応	10	10
是正対応	5	6

登録後の維持運用管理フェーズ

作業内容	現場	支援
セキュリティ目標確立	1	1
維持管理計画作成	2	2
改善サイクル確立	1	2
方針群のレビュー	5	3

注記：支援プランXで一部の実務作業について支援が可能です。実際の規模（クラウドサービス数、システム複雑性、組織規模）により±30～50%程度の変動が想定されます。

3.4 支援プランC：クラウドセキュリティ認証取得事業者例

差分分析フェーズ

作業内容	現場	支援
現状評価（分析）	5	8
管理策マッピング	8	12
証跡レビュー	10	10
責任分界整理	6	6

基盤構築フェーズ

作業内容	現場	支援
キックオフ・体制構築	1	2
情報資産洗い出し	3	4
リスクアセスメント	5	8
基本方針・規程作成	5	10
教育・意識向上研修	5	3

統合整理フェーズ

作業内容	現場	支援
既存文書整理	6	6
クロスマッピング	5	10
証跡体系整理	6	6

最適化フェーズ
内部監査・マネジメントビュー

作業内容	現場	支援
不足統制追加	6	8
過剰統制削減	4	4
内部監査	10	10
証跡整理	10	6
マネジメントレビュー	2	2

登録監査対応

作業内容	現場	支援
証跡一覧作成	10	6
想定問答集作成	5	6
模擬監査	6	8
監査対応	10	10
是正対応	5	6

登録後の維持運用管理フェーズ

作業内容	現場	支援
セキュリティ目標確立	1	1
維持管理計画作成	2	2
改善サイクル確立	1	2
方針群のレビュー	5	3

注記：支援プランXで一部の実務作業について支援が可能です。実際の規模（クラウドサービス数、システム複雑性、組織規模）により±30～50%程度の変動が想定されます。

工数が増減しやすい要因

要因	影響度
クラウド構成の複雑性	非常に大
外部委託数	大
ログ取得状況	大
文書整備度	中
組織規模	中
自動化ツール利用	減少要因

実務上の重要ポイント

- **証跡収集が最大工数源**
- **責任共有モデルの整理が監査通過率を左右**
- **ログ・時刻同期・権限管理は技術＋文書の両輪**
- **未取得企業は「教育工数」が想像以上に大きい**
- **既取得企業は“整理”が中心で“構築”は少ない**

4.組織として意識すべきこと（経営・全社視点）

① 政府調達水準のセキュリティであるという理解

- 一般企業向けセキュリティより高水準
- 「十分」ではなく「政府利用に耐えるか」が基準
- 社外への信頼証明としての意味が大きい

② クラウド事業の競争力に直結

- 入札参加資格・選定条件に影響
- ブランド価値・市場信頼性の向上
- 海外基準（FedRAMP等）との整合も意識

③ 技術部門だけの活動ではない

- 契約管理、法務、営業、サポート部門も対象
- SLA、責任共有、利用規約の整備が必須
- 「組織統制＋技術統制」の両立

④ 維持運用コストを前提にした判断

- 年次レビュー・変更管理が継続的に発生
- システム変更＝統制見直し
- 人的リソース確保が重要

⑤ 透明性と説明責任

- 障害・事故・変更の記録
- 利用者への情報開示姿勢
- 「隠さない文化」が評価される

5. 組織担当者が持つべき認識（実務視点）

① **監査は“文書確認”ではなく“実証確認”**
ISMS以上に以下が重視される
- 実ログ/設定画面/構成図
- アラート履歴/チケット履歴 等

② **責任共有モデルの理解が必須**
- クラウド事業者の責任範囲
- 利用者責任範囲
- 再委託先責任範囲

③ **証跡の体系化が成功の鍵**（必要となる証跡例）

分類	例
技術	アクセスログ、設定値、暗号鍵管理記録
運用	障害記録、変更申請、作業承認
管理	教育記録、委託先評価、リスク評価
契約	SLA、利用規約、NDA

「設定しています」ではなく
「この画面・このログです」が必要

これが曖昧だと監査評価が大きく下がる

④ **不適合は“改善機会”**
- 技術的不備より「説明不足」が指摘されやすい
- 是正計画の具体性が重要
- 迅速な対応体制が評価対象

⑤ **担当者は“調整役”**
- 技術部門、法務、営業の橋渡し
- 証跡収集のハブ
- 単独で完結しない

6.監査で特に重視される観点

観点	見られる内容
構成管理	ネットワーク図・責任分界
ログ管理	保存期間・改ざん防止
アクセス管理	権限棚卸・特権管理
暗号管理	鍵管理方法・保管
変更管理	承認プロセス・影響評価
委託先	再委託契約・評価記録
インシデント	報告・再発防止
SLA	可用性・障害時対応

7.よくある誤解

誤解	実際
ISMSがあれば十分	不十分 （クラウド特有統制が必要）
文書で説明すればよい	技術実証が必須
エンジニアだけの仕事	法務・営業も対象
登録後は楽になる	維持工数が継続
完璧でないと登録不可	改善計画があれば可

8.成功する組織の共通点

- 全ての要員が正しく理解・認識している
- 構成図・設定値・ログを常時更新
- チケット管理が日常業務に組込済み
- リスクマネジメントプロセスの定着
- 全ての要員がリスク感性を持って業務に取り組む
- 委託先との契約条項が明確
- 変更管理が形式でなく実運用
- 技術と文書が一致している
- 監査を「品質確認イベント」と捉える文化

9.ISMAP監査における不適合（指摘事項）

「技術設定の不足」よりも「証明できないこと」 に起因するケースが多いのが特徴です。
以下は、実務で発生しやすい代表的な指摘事例の整理です。

1. アクセス管理に関する不適合

事例

- 管理者権限の棚卸が年1回のみで、記録も未保存
- 退職者アカウントが残存
- 特権IDの利用履歴が確認できない

指摘内容例

- 権限管理手順は存在するが、実施証跡が確認できない
- 特権ID利用の事後レビューが未実施

改善例

- 四半期棚卸＋承認ログ保存
- 特権IDは申請制・利用ログ自動取得

2. ログ管理に関する不適合

事例

- ログ取得設定はあるが保存期間が短い
- 改ざん防止策が不十分
- ログレビューが実施されていない

指摘内容例

- ログの完全性が保証されていない
- 監視体制の実効性が確認できない

改善例

- 保存期間の明確化（例：1年以上）
- WORMストレージやSIEM活用
- 定期レビュー記録の残存

3. 変更管理に関する不適合

事例

- 緊急変更の承認記録が未保存
- 本番反映前の影響評価が未実施
- チケット管理と実作業が一致しない

指摘内容例

- 変更管理手順と運用実態に乖離がある
- 緊急変更の統制が確認できない

改善例

- 緊急変更テンプレート導入
- 承認履歴の自動保存
- チケットとログの紐付け

4. 構成管理に関する不適合

事例

- ネットワーク構成図が最新でない
- 責任分界点の記載不足
- 再委託先範囲が不明確

指摘内容例

- 構成管理情報の最新性が担保されていない
- 責任共有モデルの明確性に欠ける

改善例

- 月次更新ルール
- 構成変更時の図更新必須化

5. 委託先管理に関する不適合

事例

- NDA未締結
- セキュリティ条項が曖昧
- 再委託先評価未実施

指摘内容例

- 委託先のセキュリティ確保が証明できない
- 契約条項に管理責任の記載が不足

改善例

- 契約テンプレ統一
- 年次評価チェックリスト導入

6. インシデント管理に関する不適合

事例

- 軽微障害を記録していない
- 再発防止策の文書化不足
- 報告経路が曖昧

指摘内容例

- インシデント定義が不明確
- 再発防止プロセスが確認できない

改善例

- 重大度分類の明文化
- チケット化の徹底

7. 暗号・鍵管理に関する不適合

事例

•鍵のローテーション未実施
•鍵保管場所が共有フォルダ
•アクセス制御不足

指摘内容例

•「鍵管理の適切性が確認できない」

改善例

•HSM／KMS利用
•鍵更新スケジュール定義

8. SLA・可用性に関する不適合

事例

- SLA定義はあるが測定記録なし
- 稼働率算出根拠が不明
- 障害時の通知基準不明確

指摘内容例

- 「可用性指標の客観的証明が不足」

不適合の傾向まとめ

分類	多い原因
技術	設定不足より証跡不足
運用	実施しているが記録していない
文書	最新化不足
組織	責任範囲不明確
契約	委託先条項不足

監査でよくある評価コメント（軽微指摘レベル）

- 「運用は適切だが記録が不足」
- 「証跡の体系化が望ましい」
- 「更新頻度の明確化が必要」
- 「手順と実運用の一致確認が望まれる」

重要な理解

ISMAP監査では**“未実施”より“未証明”の方が重大評価になりやすい。**

そのため多くの不適合は、以下の構図で発生します。

技術不足 ＜ 記録不足

設定ミス ＜ 説明不能

10.ISMAP構築支援体制

支援要員の力量

1.日本規格協会グループ要員認証協会登録ISMS/クラウドセキュリティ主任審査員
2.日本規格協会グループ要員認証協会登録ISMS/クラウドセキュリティ審査員
3.日本規格協会グループ要員認証協会（JRCA）承認研修コース主任講師
4.公認情報セキュリティ監査人（CAIS-Auditor）
5.情報処理安全確保支援士（セキュリティスペシャリスト）

私たちMSQAは上記いずれかの力量を有する要員がチームとなってISMAP構築・運用を支援します。

プランX（実務作業支援）をご活用の場合も、有資格者をアサインし支援することにより生産性と品質を維持します。

おわりに

本プロジェクトは、ISMAP登録の達成のみを目的とするものではなく、クラウドサービスの信頼性向上と持続的なセキュリティ運用基盤の確立を実現するための取り組みです。制度要求への適合を通じて、組織の統制力・説明責任・事業競争力を総合的に高め、将来のサービス拡張や制度改定にも柔軟に対応できる体制づくりを支援してまいります。

代表理事・主任講師　中西　孝治

ISMAP（政府情報システムのためのセキュリティ評価制度）構築支援プロジェクト概要

一般社団法人マネジメントシステム品質協会は、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。
http://msqa.jp

初版（1.0版）発行：2024.04.01
改訂（2.0版）発行：2026.02.04 ISMAP基準/ISMS改正に対応