Information Security Management System

# ISMS適合性評価制度

JIS Q 27001:2025（ISO/IEC 27001:2022+Amd 1:2024）

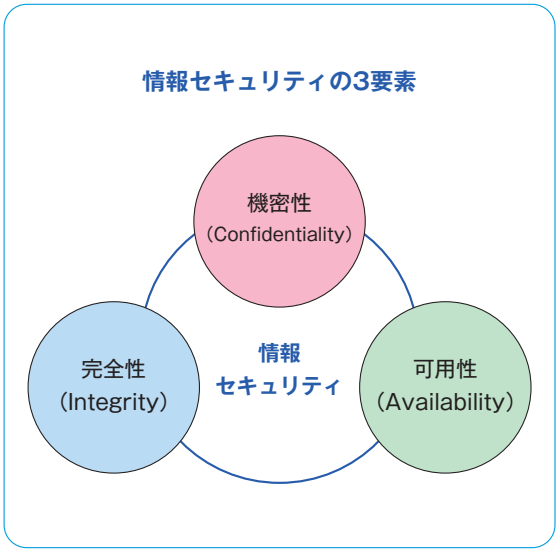
組織の情報セキュリティのための仕組みが
国際規格に適合していることを証明する制度です

一般社団法人
情報マネジメントシステム認定センター
（ISMS-AC）

情報セキュリティマネジメントシステム

## ISMSとは

近年、ITシステムやネットワーク、クラウドサービスは社会インフラとして不可欠なものとなっています。一方で、標的型攻撃やランサムウェア、サプライチェーン攻撃などによる被害・影響も多発しており、さらに生成AIなどの普及に伴い、情報管理の重要性は一層高まっています。こうした中、組織の情報を保護し、信頼を確保する有効な手段の1つがISMSです。ISMSとは、Information Security Management System（情報セキュリティマネジメントシステム）の略で、情報のCIA（「機密性（Confidentiality）」、「完全性（Integrity）」、「可用性（Availability）」）を維持し、情報セキュリティを継続的に管理・改善するための体系的な仕組みです。これは、情報が漏えいしないようにし（機密性）、改ざんや誤りがないようにし（完全性）、そして必要なときに必要な人が利用できるようにする（可用性）ということです。ISMSには、技術的対策だけでなく、従業員の教育・訓練、組織体制の整備なども含まれます。




ISMS構築にあたり必要となる

## ISMSの国際規格「ISO/IEC 27001（JIS Q 27001）※1」

ISMSを構築するにあたって、必要となるのがISO/IEC 27001（JIS Q 27001）というISMSの国際規格です。この規格には、ISMSをどのように構築、実施、維持、改善すべきなのかが記載されています。また、管理策と呼ばれる情報セキュリティの対策集も記載されています。特に管理策については、ISO/IEC 27002（JIS Q 27002）というガイドライン規格があり、管理策を導入する際の参考になります。

ISMSを正しく運用していることを示すための第三者証明

## ISMS認証※2

「ISMS認証」とは、第三者であるISMS認証機関が、組織の構築したISMSがISO/IEC 27001（JIS Q 27001）に基づいて適切に運用管理されているかを、利害関係のない公平な立場から審査し証明することです。

したがって、「ISMS認証」によって、組織は、ISO/IEC 27001という国際規格に沿って、情報セキュリティを確保するための仕組みをもち、その仕組みを維持し継続的に改善していることを、顧客や取引先に対して客観的に示すことができます。この「ISMS認証」を取得するには、ISMS認証機関に申請し、審査を受ける必要があります。

**※1　ISO/IEC 27001とJIS Q 27001**

国際規格「ISO/IEC 27001」は、ISO（International Organization for Standardization：国際標準化機構）が発行する国際規格であり、原文は英語です。これを日本国内での使用のために日本語に翻訳し、国内規格として発行したものが「JIS Q 27001」です。翻訳されたJIS Q 27001は、ISO規格と同じ内容であること（IDT：IDENTICAL）が認められています。規格の正式名称は次の通りです。

- ISO/IEC 27001 Information security, cybersecurity and privacy protection - Information security management systems - Requirements
- JIS Q 27001 情報セキュリティ、サイバーセキュリティ及びプライバシー保護ー情報セキュリティマネジメントシステムー要求事項

ISO/IEC 27001（JIS Q 27001）は、追補が発行されています。詳細はISMS-ACのウェブサイト（https://isms.jp/isms/about.html）を参照してください。

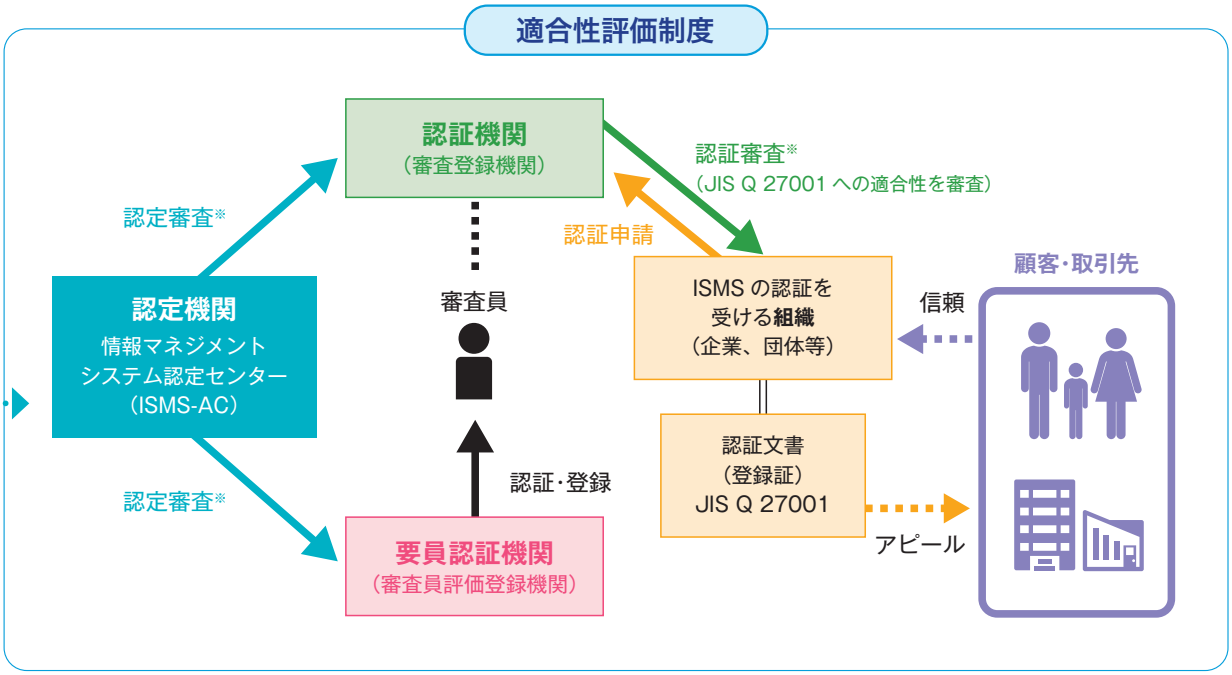
**※2　ISMS認証**

この「ISMS認証」と同義語として使用されるものに「ISO/IEC 27001認証」「JIS Q 27001認証」があります。上記※1の通り、ISO/IEC 27001とJIS Q 27001の内容は同じものですので、「ISO/IEC 27001認証」「JIS Q 27001認証」も同じ意味です。本書では「ISMS認証」に統一して記載しています。

認証の公平な運用のための国際的な枠組み

# ISMS適合性評価制度 ～認定と認証～

認証を公正に運用するために、国際的な枠組みが定められています。これを「適合性評価制度」と呼んでいます。適合性評価制度は「認証機関」「認定機関」「要員認証機関」から構成されます。




## 認定機関

認証機関が適切に認証審査が実施できることを審査し、確認します。これを、「認定審査」といいます。

## 認証機関

第三者機関として組織のISMSを審査します。これを「認証審査」といいます。

## 要員認証機関

認証審査に関する能力をもつ審査員を認証、登録します。

## 認定機関がISMS認証機関を認定する意義

認定機関である情報マネジメントシステム認定センター（ISMS-AC）は、認証機関が適切に審査を実施できる体制・能力をもっているかを、国際規格（ISO/IEC 27006-1）※に照らして審査し、適合していると認められる機関を認定して、「認定シンボル」の使用を許可しています。そのため、認定を受けたISMS認証機関は、適切なISMS認証審査を実施することのできる、信頼のおける認証機関であることを意味します。要員認証機関についても同様です。

### 認定シンボル（右）と認証機関マーク（左）が並んだ表示例

認定シンボルと認証機関のマークが２つ並んでいることは、その認証機関が国際規格に従った適切な審査を実施していることを、認定機関であるISMS-ACが保証していることを示します。

※ISO/IEC 27006-1 情報セキュリティ、サイバーセキュリティ及びプライバシー保護ー情報セキュリティマネジメントシステムの審査及び認証を行う機関に対する要求事項　第1部：一般

ISMS認証を受ける際に知っておきたい

# ISMS認証について

## ■ 認証範囲

組織の必要に応じて定めることができます。必ずしも全社を範囲とする必要はありません。

## ■ 認証を受けるには ～申請から認証取得までの流れ～

### ①認証機関の選択

認定された認証機関の中から、申請先を選びます。

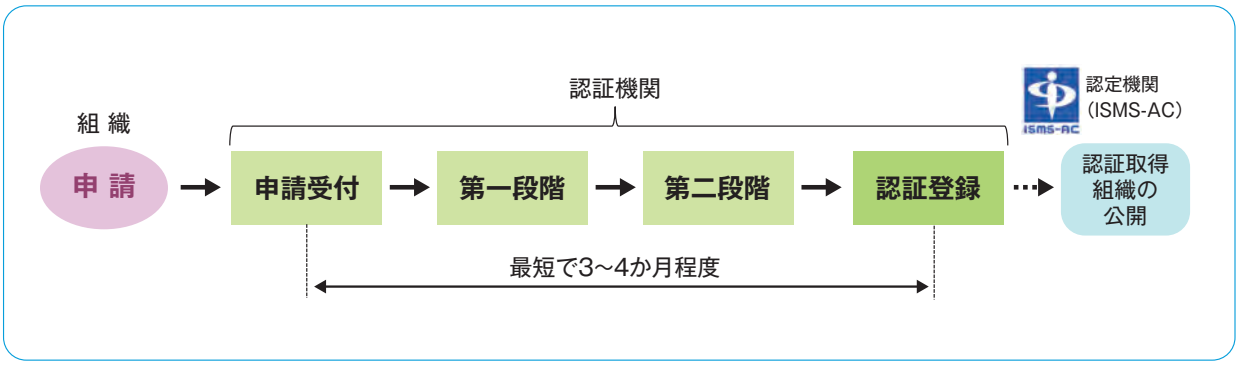
・認証登録に関わる料金は、認証範囲や受審組織の規模等の他、認証機関によって異なります。

・認証機関はISMS認証機関一覧を参照下さい。（参照先：https://isms.jp/lst/isr/）

### ②申請

選んだ認証機関に申請します。

（ISMS-ACではありませんので、ご注意ください。）




### ③初回認証審査

申請が受理され、審査に入れる状態になったら、認証機関によって審査が開始されます。審査は原則として第一段階と第二段階の2段階で行われます。

（審査日数や審査工数は、認証範囲、受審組織の規模等によって異なります。）

### ④認証登録

審査の結果、ISO/IEC 27001（JIS Q 27001）に適合していることが確認されると認証されます。

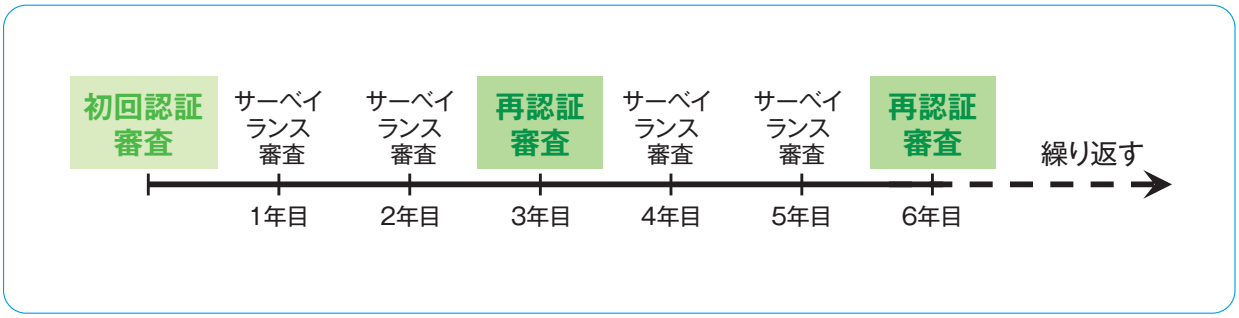
認証の有効期限は3年です。

### ⑤報告・公開

認証された旨が各認証機関からISMS-ACに報告されましたら、ホームページで公開します。

## ■ 認証を維持するには ～認証の信頼性を維持するために～

初回審査の後も年に1回以上の中間的な審査（サーベイランス審査）が、そして3年ごとに認証の有効期限を更新するための全面的な審査（再認証審査）が実施され、組織のISMSが引き続き規格に適合し、有効に維持されていることが確認されます。



認定機関の国際的な協力体制

# 国際的な認定の枠組み ～国際的な相互承認～

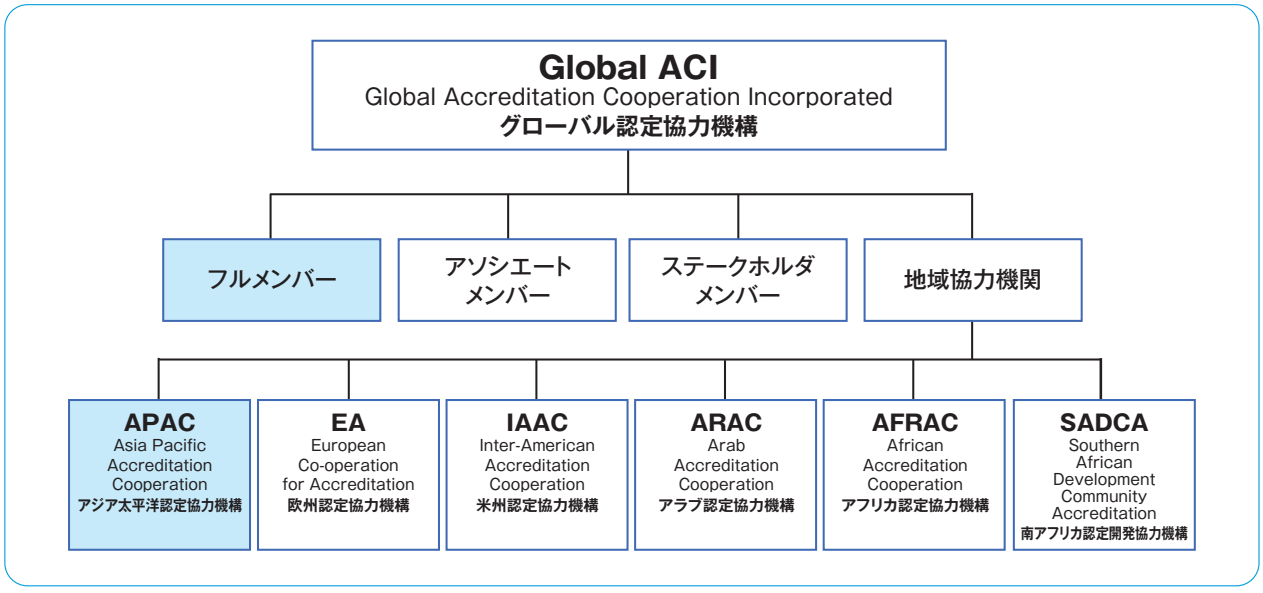
## ■ ISMS-ACはグローバル認定協力機構に加盟し、国際的な認定機関として貢献しています。

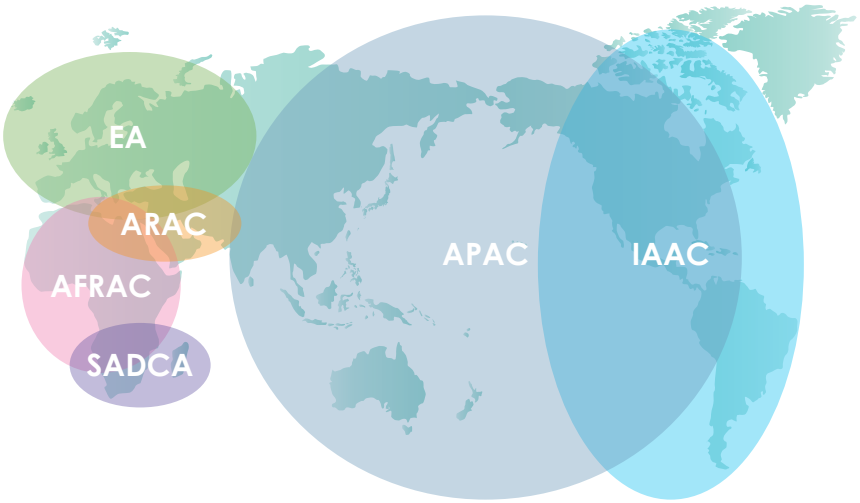
ISMS-ACは、認定機関の国際的枠組みに関する組織であるグローバル認定協力機構（Global ACI※）に加盟しており、ISMS等のマネジメントシステム認証機関の認定機関として、国際的に整合の取れた活動を行っています。

Global ACIの主な目的の一つは、加盟認定機関間の相互評価等に基づいて国際的な相互承認の仕組みを確立することです。Global ACIの多角的承認取決め（MRA）に署名した認定機関によって認定された認証機関による認証は、Global ACIによってその信頼性を保証されます。

ISMS-ACは、2006年にアジア太平洋地域におけるIAFの下部組織であるPAC（現APAC）に、2007年にIAF（現Global ACI）に加盟した後、2018年にISMSのIAF MLA（現Global ACI MRA）に署名しました。ISMSに係る多くの認定・認証数の実績をもつISMS-ACは、今後も認定機関の国際的な協力に貢献していきます。

※Global ACI設立
2026年1月1日に、IAF（国際認定フォーラム）とILAC（国際試験所認定協力機構）が統合され、グローバル認定協力機構（Global ACI：Global Accreditation Cooperation Incorporated）が設立されました。IAF及びILACの機能や各種活動はGlobal ACIに引き継がれ、IAF・ILAC相互承認協定の署名認定機関としての地位は維持されます。また、IAF MLAマークについては、Global ACIでの準備が整い新たなマークに切り替わるまで、引き続き有効です。



ISMS認証取得組織へのアンケートより

# ISMS導入・ISMS認証取得の効果（メリット）

近年のコンピュータ処理への依存度の高まりやインターネットの爆発的な広がりとともに、それに比例して情報資産への脅威も増大し、システムや人的な脆弱性を突いたセキュリティ事故も件数・規模ともに増加しているため、自社のみならず取引先における情報セキュリティ管理のリスクを把握する重要性についての認識が高まりを見せています。

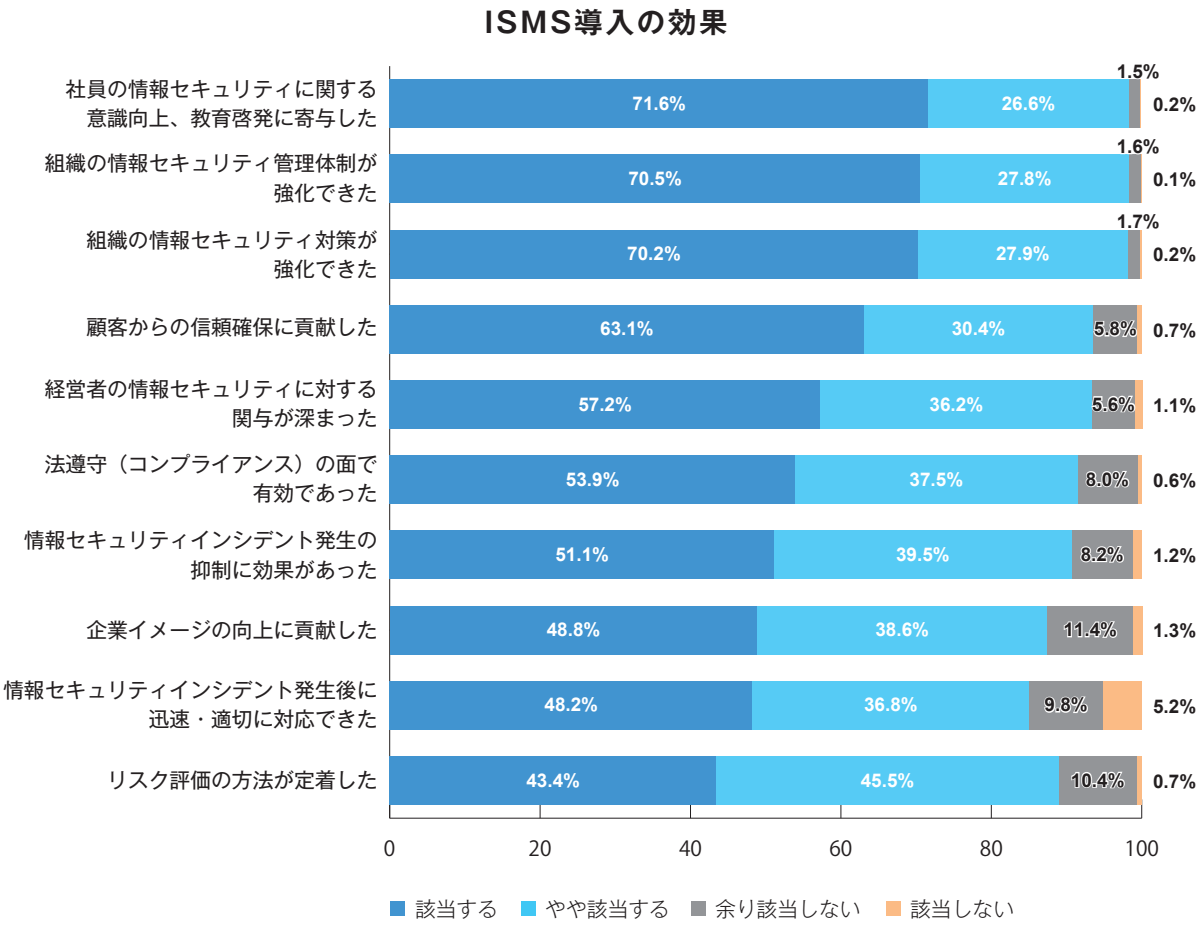
ISMS認証取得組織を対象に「ISMSを導入し、認証を取得された効果」を尋ねたところ、以下のような効果（メリット）が見えてきました。

## ■ 内部的な効果（メリット）：

- 社員の情報セキュリティに関する意識向上につながる。
- 情報セキュリティ対策・コンプライアンスを強化できる。
- 経営者の情報セキュリティに対する関与が深まる。
- 組織の情報セキュリティレベルを向上し、期待レベルを維持できる。 など。

## ■ 対外的な効果（メリット）：

- 顧客からの信頼確保につながる。
- 企業イメージの向上につながる。 など。




【アンケート調査概要】
■ 調 査 期 間：2024年3月
■ 調 査 対 象：2024年2月時点で、ISMS-AC認定のISMS認証機関からISMS認証を取得し、登録情報を公開している6,790組織
■ 調 査 方 法：郵送でアンケートの案内をし、WEB上から質問（選択形式及び記述形式）に回答いただいた。
■ 有効回答数：1,704件
■ 回　収　率：25.1%
公開URL：https://isms.jp/enquete/2023/report2023.pdf

クラウドサービスを取り扱う組織には…

# ISMSクラウドセキュリティ認証

ISMSクラウドセキュリティ認証とは、ISMS認証の認証範囲内に含まれる組織のクラウドサービスの提供及び／又は利用に関して、ISO/IEC 27017※に規定されるクラウドサービス固有の管理策が適切に実施されていることを認証する仕組みです。

## ■ 認証基準

ISMSクラウドセキュリティ認証の認証基準は、「ISO/IEC 27017に基づくISMSクラウドセキュリティ認証に関する要求事項（JIP-ISMS517-2.0）」です。この認証基準のなかで「ISO/IEC 27001」への適合が求められています。

## ■ ISMSクラウドセキュリティ認証のメリット

ISMS認証に加えて、ISMSクラウドセキュリティ認証を取得することにより、組織はクラウドサービス固有のリスクについて網羅的なアセスメントを実施して必要な管理策を導入していることを、認証機関による審査・認証によって対外的に表明することができます。

また、企業や一般ユーザがクラウドサービスプロバイダ、クラウドサービスカスタマに対して情報を預けることができるかどうかを評価する一つの指標となります。

## ■ 認証の対象となる組織

ISMS認証を取得している／取得する組織で、ISO/IEC 27017に従ってクラウドサービスを提供している組織（クラウドサービスプロバイダ）・クラウドサービスを利用している組織（クラウドサービスカスタマ）の両方が対象となります。

**※ISO/IEC 27017とは**

クラウドサービスに関する情報セキュリティ対策を実施するためのガイドライン規格であり、クラウドサービスを提供する組織と利用する組織の両方を対象としています。正式名称は次の通りです。

■ISO/IEC 27017:2026 情報セキュリティ、サイバーセキュリティ及びプライバシー保護ーISO/IEC 27002に基づくクラウドサービスのための情報セキュリティ管理策

**※ISO/IEC 27017に基づくISMSクラウドセキュリティ認証に関する要求事項（JIP-ISMS517）とは**

ISO/IEC 27017は、上述の通りガイドライン規格であり、要求事項を定めた規格ではありません。認証を行うためには、組織が何を行う必要があるかについて定めた要求事項（認証基準）が必要となります。そのため、ISO/IEC 27017を基に策定された認証基準が「ISO/IEC 27017に基づくISMSクラウドセキュリティ認証に関する要求事項（JIP-ISMS517-2.0）」です。JIP-ISMS517-2.0は、ISO/IEC 27017:2026の発行に伴い、従来のJIP-ISMS517-1.0を改訂したものです。

ISMSクラウドセキュリティ認証は、この認証基準JIP-ISMS517に基づき、ISMS-ACの認定を受けた認証機関が審査、認証を行います。

お問い合わせ先

■ ISMS認証取得に関するお問い合わせ

▶▶▶ 各認証機関にお問い合わせください。

**認証機関一覧はこちら https://isms.jp/lst/isr/**

■ ISMS適合性評価制度全般に関するお問い合わせ

▶▶▶ 当センターまでお問い合わせください。

**情報マネジメントシステム認定センター（ISMS-AC）**

**https://isms.jp/contact/index.html**

当センターでは、次の制度における認定も実施しています。

### ■ ITSMS適合性評価制度

ITサービスマネジメントシステム（ITSMS）のための制度です。ITSMS認証取得によって、信頼できるITサービスを提供できることを外部に表明できます。また、認証維持のための継続的な審査によって、サービス品質の向上と維持を図ることができます。
https://isms.jp/itsms.html

### ■ BCMS適合性評価制度

事業継続マネジメントシステム（BCMS）のための制度です。BCMS認証取得によって対外的な信頼性が向上します。また認証審査を受審することによって、より有効なBCMSの構築・運用に向けた改善につなげることができます。
https://isms.jp/bcms.html

### ■ AIMS適合性評価制度

AIマネジメントシステム（AIMS）のための制度です。AIMS認証取得によって、AIシステムを開発・提供・利用するための国際的な仕組みを構築・運用していることを対外的に表明できます。
https://isms.jp/aims.html

### ■ PIMS適合性評価制度

プライバシー情報マネジメントシステム（PIMS）のための制度です。PIMS認証取得によって、PII（Personally Identifiable Information：個人識別可能情報）の収集・利用・保管・加工などの処理に関するリスクを管理し、プライバシー保護を実施するための枠組みを導入、運用していることを対外的に表明できます。
https://isms.jp/pims.html

**一般社団法人 情報マネジメントシステム認定センター（ISMS-AC）**

〒106-0032 東京都港区六本木一丁目9-9 六本木ファーストビル内
URL https://isms.jp/

文書番号：JIP-ISMS120-7.3 October 2026