Information Security Management System

情報セキュリティマネジメントシステム

適合性評価制度の概要

JIS Q 27001:2014 (ISO/IEC 27001:2013) 対応版

ISMS

一般財団法人 日本情報経済社会推進協会

1 ISMS適合性評価制度の目的

ISMS(Information Security Management System)適合性評価制度(以下、ISMS制度という)は、国際的に整合性のとれた情報セキュリティマネジメントシステム(ISMS)に対する第三者認証制度である。

ISMS制度は、わが国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られる情報セキュリティを達成し、維持することを目的としている。

2 ISMSの概要

ISMS導入のポイント

ISMSとは、個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用することである。
ISMSが達成すべきことは、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バランス良く維持・改善し、リスクを適切に管理しているという信頼を利害関係者に与えることにある。そのためには、ISMSを、組織のプロセス及びマネジメント構造全体の一部とし、かつ、その中に組み込むことが重要である。

情報セキュリティの3要素(機密性、完全性、可用性)

ISMSでは、情報セキュリティの主な3要素について次のように定義している。

情報セキュリティ	
情報の機密性、完全性及び可用性の維持	
機密性	許可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性
完全性	正確さ及び完全さの特性
可用性	認可されたエンティティが要求したときに、アクセス及び使用が可能である特性

注記:真正性、責任追跡性、否認防止、信頼性などの特性を含めることもある。

※エンティティは、“実体”、“主体”などともいう。情報セキュリティの文脈においては、情報を使用する組織及び人、情報を扱う設備、ソフトウェア及び物理的媒体などを意味する。

(JIS Q 27000:2014より引用)

JIS Q 27001:2014とは

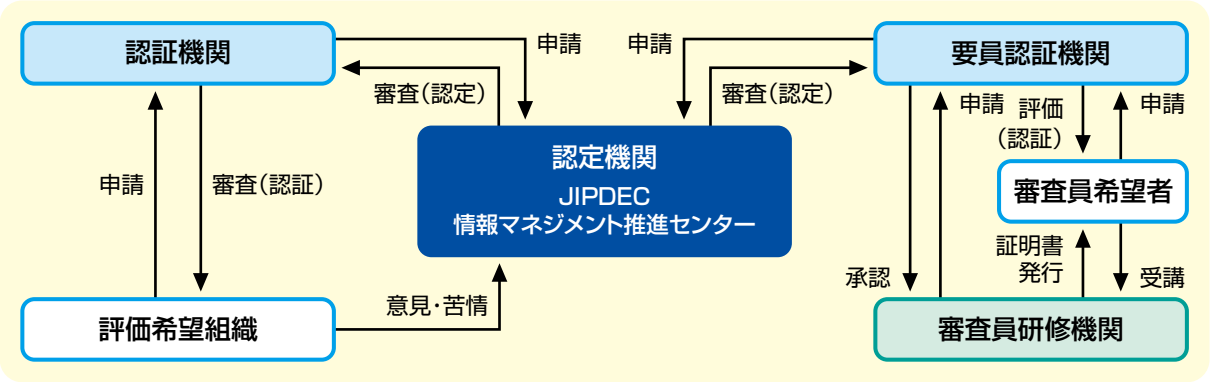
JIS Q 27001(ISO/IEC 27001)は、ISMSの要求事項を定めた規格であり、組織がISMSを確立し、実施し、維持し、継続的に改善するための要求事項を提供することを目的として作成されている。ISMSの確立及び実施について、それをどのように実現するかという方法ではなく、組織が何を行うべきかを主として記述している。この規格は以下のために用いることができる。

- **JIS Q 27001:2014** 情報技術—セキュリティ技術—情報セキュリティマネジメントシステム—要求事項
  (ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements)
- **組織のマネジメント及び業務プロセスを取り巻くリスクの変化への対応**
  JIS Q 27001では、組織は、自らのニーズ及び目的、情報セキュリティ要求事項、組織が用いているプロセス、並びに組織の規模及び構造を考慮して、ISMSの確立及び実施を行う。これは、多くの情報を取り扱うようになっている、現代の組織のマネジメント及び業務プロセスを取り巻くリスクの変化に対応できるように、組織基盤を構築する抜本的な業務改革をする目的に適している。
- **情報セキュリティ要求事項を満たす組織の能力を内外で評価するための基準**
  JIS Q 27001は、情報セキュリティ要求事項を満たす組織の能力を、パフォーマンス評価及び内部監査などにより、組織の内部で評価する基準としても、第二者監査・第三者監査といわれる、外部関係者が評価するための基準としても用いることができる。

3 ISMS適合性評価制度の運用

ISMS制度は、組織が構築したISMSがJIS Q 27001（ISO/IEC 27001）に適合しているか審査し登録する「認証機関」、審査員の資格を付与する「要員認証機関」、及びこれら各機関がその業務を行う能力を備えているかをみる「認定機関」からなる、総合的な仕組みである。なお、審査員になるために必要な研修を実施する「審査員研修機関」は要員認証機関が承認する。

ISMS制度の運用体制



ISMS制度の公平性・透明性・客観性の確保

ISMS制度の運営については、その公平性・透明性及び客観性を確保するために、JIPDEC組織運営機構の中に学識経験者及び業界団体の有識者等から構成される運営委員会及びその下部組織である技術専門部会を設置している。また、認証機関や要員認証機関の認定の可否等を審議する、有識者からなる判定委員会を設置している。これらの詳細は、URL：http://www.isms.jipdec.or.jp/org/を参照のこと。

4 ISMS認証取得の必要性

ISMS制度における認証を取得することは、組織の情報セキュリティ管理体制の整備や社内組織の体質強化につながるだけでなく、対外的にも情報セキュリティの信頼性を向上させることができ、国際的にもアピールすることができる。また、組織が取組むべきリスクマネジメントを維持し、適切な管理策を実施することによって、情報セキュリティインシデントの発生可能性やインシデントが顕在化したときの損害を減らすことができ、企業価値の向上につなげることができる。

ISMSを構築・運用するメリット

●技術面及び人間系の運用・管理面の総合的なセキュリティ対策が実現できる。
—社員のスキル向上、責任の明確化、緊急事態の対処能力の向上など。

●総合的マネジメントの視点から、効率的なセキュリティ対策が実施できる。
—費用対効果を考えた情報資産管理、リスクマネジメントの定着など。

上記の活動を継続することにより、セキュリティ意識の向上などの効果が期待される。

ISMS認証を取得するメリット

●対外的には、情報セキュリティの信頼性を確保できる。
—顧客や取引先からのセキュリティに関する要求事項への対応など。

●内部的には、事業競争力の強化につながる。
—入札条件や電子商取引への参加の条件整備など。

5 ISMS認証基準

ISMS制度の認証基準(JIS Q 27001:2014)

ISMS適合性評価制度における認証基準は、JIS Q 27001:2014(ISO/IEC 27001:2013)である。
JIS Q 27001は、ISO/IEC 27001の制定発行に伴って、日本工業標準調査会(JISC)により日本工業規格(JIS)として制定された国内規格であり、内容は、ISO/IEC 27001を忠実に日本語に翻訳し、国際規格との整合性が厳密に保たれている。2006年3月にJIS Q 27001:2006発行後、ISO/IEC 27001:2005の改訂に伴いJISも改訂が行われ、2014年3月にJIS Q 27001:2014が発行された。

JIS Q 27001:2014の内容

※青字は、MSS共通要素(6頁参照)にないISMS固有の箇条

箇条	概略
4. 組織の状況	
4.1 組織及びその状況の理解 4.2 利害関係者のニーズ及び期待の理解 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 4.4 情報セキュリティマネジメントシステム	組織をとりまく内外の状況や利害関係者のニーズ及び期待を理解、決定し、それらを考慮に入れたうえでISMSの適用範囲を定めることが求められている。
5. リーダーシップ	
5.1 リーダーシップ及びコミットメント 5.2 方針 5.3 組織の役割、責任及び権限	ISMSを推進し、関係者の意識向上を図るためには、トップマネジメントの強力なリーダーシップが不可欠である。ここでは、トップマネジメントの果たすべき役割について規定している。
6. 計画	
6.1 リスク及び機会に対処する活動 6.1.1 一般 6.1.2 情報セキュリティリスクアセスメント 6.1.3 情報セキュリティリスク対応 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	ISMSにおけるリスク及び機会を決定し、情報セキュリティリスクアセスメント、情報セキュリティリスク対応のプロセスを定めて適用することが求められている。 「規定」である「附属書A管理目的及び管理策」は、6.1.3において、附属書Aの管理策と組織が適用した管理策を比較し、除外した場合にはその理由を適用宣言書に記載することが求められている。
7. 支援	
7.1 資源 7.2 力量 7.3 認識 7.4 コミュニケーション 7.5 文書化した情報	7.5では、各箇条で要求される文書類を文書化し、管理し、維持しながら、要員の力量、並びに利害関係者との反復的かつ必要に応じたコミュニケーションを確立することを通じた、ISMSの運用の支援について規定している。
8. 運用	
8.1 運用の計画及び管理 8.2 情報セキュリティリスクアセスメント 8.3 情報セキュリティリスク対応	情報セキュリティの要求事項を実現するために必要なプロセス群の、策定、導入・実施、及び管理について規定している。また、そのために不可欠な情報セキュリティリスクアセスメント、情報セキュリティリスク対応の実施についても規定している。
9. パフォーマンス評価	
9.1 監視、測定、分析及び評価 9.2 内部監査 9.3 マネジメントレビュー	情報セキュリティパフォーマンスの評価(監視、測定、分析及び評価)、内部監査及びマネジメントレビューについて規定している。
10. 改善	
10.1 不適合及び是正処置 10.2 継続的改善	不適合発生時の処置、及びとった処置の文書化と、ISMSの適切性、妥当性及び有効性の継続的改善について規定している。

主な関連規格

●JIS Q 27000:2014　情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―用語
(ISO/IEC 27000:2014　Information technology - Security techniques - Information security management systems – Overview and vocabulary)
―ISMSに関する用語及び定義について規定した規格。ISO/IEC 27000:2014は、ISMSの概要、27000ファミリーの概要、ISMSファミリーで用いられる用語及び定義等についてまとめた規格であり、JIS Q 27000:2014は、その用語及び定義部分について技術的内容を変更することなく国内規格化したものである。

●IS Q 27002:2014　情報技術―セキュリティ技術―情報セキュリティ管理策の実践のための規範
(ISO/IEC 27002:2013　Information technology - Security techniques - Code of practice for information security controls)
―組織の情報セキュリティリスクの環境を考慮に入れた管理策の選定、実施及び管理を含む、組織の情報セキュリティ標準及び情報セキュリティマネジメントを実施するための規範(ベストプラクティス―最良の慣行)をまとめた規格。

6 ISMS制度の基準・規定・手順・ガイド等

ISO/IEC 27001（JIS Q 27001） （ISMS認証基準）	第三者である認証機関が本制度の認証を希望する組織の適合性を評価するためのISMS認証基準である。
ISMSユーザーズガイド	JIS Q 27001の要求事項について一定の範囲でその意味するところを説明しているガイドである。
ISMSユーザーズガイド —リスクマネジメント編—	リスクマネジメント編はISMSユーザーズガイドを補足し、リスクマネジメント、とりわけリスクアセスメント及びその結果に基づくリスク対応についての理解を深めるために必要な事項について、例を挙げて解説している。
医療機関向けISMSユーザーズガイド	ISMSユーザーズガイドの医療機関向け版で、医療機関におけるISMSの理解を深めるためのガイドである。
法規適合性に関する ISMSユーザーズガイド	企業がリスクマネジメントを実施する上で、企業の法的リスクを考慮することは重要であり、とりわけ個人情報保護に対応する手段としてISMSの枠組みは極めて有効である。 本書はISMSの枠組みが法的及び規制要求事項に適合させる仕組みであることを理解するためのガイドである。
クレジット産業向け “PCI DSS”／ISMSユーザーズガイド	ISMSユーザーズガイドのクレジット産業向け版で、クレジット産業におけるISMS構築を主眼として、関連する規範とISMS認証基準とのマッピングを示し、ISMSを構築することがこれらの規範を順守する上で非常に有効な手段であることを示したガイドである。
クレジット加盟店向け “情報セキュリティのためのガイド”	クレジット加盟店向けに、PCI DSS ／ ISMS準拠に関して説明しているガイドである。
地方公共団体と情報セキュリティ ～ISMSへの第1歩～	地方公共団体がISMSに取り組む際に直面するかもしれない特有な問題を洗い出し、それに対処するためのアドバイスやノウ・ハウをわかりやすく記載したハンドブックである。
外部委託における ISMS適合性評価制度の活用方法	組織又は企業において情報処理業務の一部又は全てを外部委託する場合に、情報セキュリティ責任者及び担当者が委託先の選定にISMS適合性評価制度を活用するためのガイドである。
ISMS認証機関認定基準及び指針	認証機関の認定審査及び登録を行う際の認定基準及び指針であり、ISO/IEC 27006（ISO/IEC 17021を含む）に基づいている。
IMS認証機関認定の手順 IMS認証機関認定の手引き	手順は認証機関が認定を受けるための手順と、認定を申請する機関及び認定された機関の権利と義務について規定したもの、手引きは、申請から登録までと登録維持の標準的な流れと条件を示したものである。
IMS認定シンボル使用規定	認定シンボルを使用する場合の、認定シンボルの表示及び適用条件等について規定したものである。

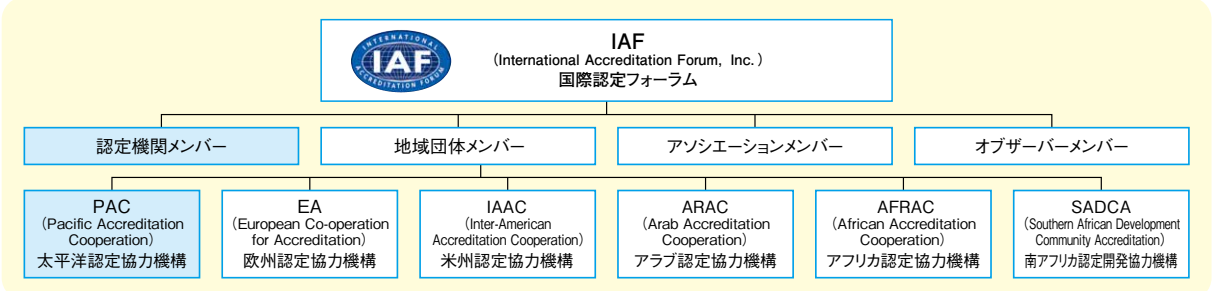
備考：上記の他にも、ISMS制度の普及促進のための各種文書や認定関連文書がある。

7 IAF（国際認定フォーラム）への加盟

IAF（International Accreditation Forum, Inc.）は、マネジメントシステム、製品、要員等の適合性評価プログラムに関わる60余の認定機関メンバーを中心に、地域団体（PAC、EA、IAAC、ARAC、AFRAC、SADCA）、アソシエーション（審査機関の協議会、各国の産業団体等）、オブザーバーを含め総勢90以上の機関が所属している。

IAFの目的の一つは、世界的に整合性のとれた適合性評価プログラムを開発し、国際規格に則して認定機関の能力を確実なものとし、認定された認証の信頼性及び有効性を向上させることによって、組織及びエンドユーザーのリスクを低減することである。また、「Certified once, accepted everywhere」をモットーに国際相互承認を推進し、経済地域間の技術的貿易障壁を除去することにより貿易の促進を目指している。IAFの国際相互承認協定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、IAFによってその信頼性を保証される。JIPDEC情報マネジメント推進センターは、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に、2007年には認定機関メンバーとしてIAFに加盟した。

国際相互承認（MLA）制度については、PACではMLA適用範囲を拡大して、従来の品質/環境マネジメントシステム、製品認証に加え、新規にISMSのMLAが発足した。IAFにおいても、MLA適用範囲にISMSを含めることが決定しており、世界的にも多くの認定・認証数の実績をもつJIPDECは、ISMSのMLA運営に向けて様々な面から貢献していく考えである。



8 ISMS認証基準の移行

2013年10月1日にISO/IEC 27001:2013が発行されたことに伴い、ISO/IEC 27001:2013への移行が開始された。ISO/IEC 27001:2013への移行は、発行と同時に開始し、移行期間は2年間であり、2015年10月1日までに移行を完了させる。この移行計画は、2013年10月の第27回IAF(国際認定フォーラム)年次総会の決議に従っている。

JIS Q 27001:2006(ISO/IEC 27001:2005)からJIS Q 27001:2014(ISO/IEC 27001:2013)への移行時のケースとしては、❶JIS Q 27001:2006(ISO/IEC 27001:2005)により初回審査をする場合、❷JIS Q 27001:2014(ISO/IEC 27001:2013)により初回審査をする場合、❸JIS Q 27001:2006(ISO/IEC 2005)から移行する場合がある。

		2013年			2014年			2015年			2016年		
		1	4	7	10	1	4	7	10	1	4	7	10	1	4	7	10
認証基準	JIS Q 27001:2006 (ISO/IEC 27001:2005) ISO/IEC 27001:2013 JIS Q 27001:2014					12ヶ月				12ヶ月							
					10/1発行												
					JIS化			3/20発行									
❶JIS Q 27001:2006 (ISO/IEC 27001:2005)により初回審査をする場合	JIS Q 27001:2006 (ISO/IEC 27001:2005)による初回審査・登録 JIS Q 27001:2014 (ISO/IEC 27001:2013)への移行					初回審査・登録											
										10/1移行完了							
❷JIS Q 27001:2014 (ISO/IEC 27001:2013)により初回審査をする場合	JIS Q 27001:2014 (ISO/IEC 27001:2013)による初回審査・登録																
					ISO発行日												
								3/20									
								JIS発行日									
❸JIS Q 27001:2006 (ISO/IEC 2005)から移行する場合	維持審査又は更新審査でJIS Q 27001:2006 (ISO/IEC 27001:2005)とJIS Q 27001:2014 (ISO/IEC 27001:2013)との差分を審査																
					10/1												
								24ヶ月									
										10/1移行完了							

JIS Q 27001:2014の主な改訂点

JIS Q 27001:2014の主な改訂点は、以下の通りである。

- ISOのマネジメントシステム規格に共通の構成、用語及び定義、テキストを適用
- JIS Q 31000:2010(ISO/IEC 31000:2009)※との整合

※リスクマネジメントの原則及び指針を定めた規格

- JIS Q 27001:2006の要求事項を継承

既にISMS認証を取得されている組織は、現在の仕組みを大幅に変更することはないが、従前に比べ計画段階における経営的な視点での見直しが必要となる。また、トップマネジメントは、組織の戦略的な方向性を確実にし、リーダーシップとコミットメントを明示する必要があり、その責任に重点が置かれるようになっている。

新規にISMS認証の取得を目指している組織は、従前のマネジメントシステムに比べて経営的要素が加味された仕組みを構築することができる。その結果、組織のガバナンスを強化できるので、組織のマネジメントシステムを見直し、改善する良い機会となる。

なお、JIS Q 27001:2014にはPDCAモデルという表現は明記されていないが、ISO MSS共通要素を定めた附属書SLの「SL5.2 MSS−マネジメントシステム規格」には、「有効なマネジメントシステムには、通常、意図した成果を達成するために、"Plan-Do-Check-Act(PDCA)"のアプローチを用いた組織のプロセス管理を基盤とする」という記述がある。したがって、JIS Q 27001:2014でも、PDCAのアプローチがJIS Q 27001:2006から継続して考慮されている。

9 ISMS認証基準の対比(2014年版 vs 2006年版)

本文の構成

JIS Q 27001:2014は、ISOのマネジメントシステム規格(MSS)の共通要素※を適用して開発されたマネジメントシステム規格となっており、その上で、情報セキュリティに不可欠なISMS固有の要求事項が規定されている。

JIS Q 27001:2014の構成は、前規格であるJIS Q 27001:2006のマネジメントシステムの仕組みを大幅に変更するものではない。計画段階における組織の状況については、情報セキュリティ方針及び情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にしなければならない主旨の要求事項が追加された。

■JIS Q 27001:2014とJIS Q 27001:2006との対比

JIS Q 27001:2014		JIS Q 27001:2006	
0. 序文	7. 支援	0. 序文	6. ISMS内部監査
1. 適用範囲	8. 運用	1. 適用範囲	7. ISMSのマネジメントレビュー
2. 引用規格	9. パフォーマンス評価	2. 引用規格	8. ISMSの改善
3. 用語及び定義	10. 改善	3. 用語及び定義	附属書A(規定)管理目的及び管理策
4. 組織の状況	附属書A(規定)管理目的及び管理策	4. 情報セキュリティマネジメントシステム	附属書B(参考)OECD原則及びこの規格
5. リーダーシップ	参考文献		附属書C(参考)規格の比較
6. 計画		5. 経営陣の責任	参考文献

※2012年5月に発行された「ISO/IEC 専門業務用指針　第1部　統合版ISO補足指針」の「附属書SL(規定)マネジメントシステム規格の提案」に規定されている、「合意形成され、統一された、上位構造、共通の中核となるテキスト、並びに共通用語及び中核となる定義」である。これを示すことによって、マネジメントシステム規格(MSS:Management System Standards)の一貫性及び整合性を向上させることがその狙いである。なお、今後すべてのMSSはこの附属書SLを適用することになった。

「附属書A(規定)管理目的及び管理策」の構成

JIS Q 27001:2014の「附属書A(規定)管理目的及び管理策」ではJIS Q 27001:2006の附属書Aの箇条をほぼ継承している。ただし、2006年版よりも箇条が3つ追加されている。追加された箇条については、新規の内容もあるが、1つの箇条が2つに分けられたものもある。また、箇条と内容の整理が行われたことから、別の箇条へ移動された管理目的・管理策もある。その結果、従来のJIS Q 27001:2006の附属書Aの管理策は133であったが、管理策の追加、削除、変更が行われた結果、JIS Q 27001:2014の附属書Aでは管理策は114となっている。

■JIS Q 27001:2014とJIS Q 27001:2006との対比(附属書A)

JIS Q 27001:2014附属書A	JIS Q 27001:2006 附属書A
A.5 情報セキュリティのための方針群	A.5 情報セキュリティ基本方針
A.6 情報セキュリティのための組織	A.6 情報セキュリティのための組織
A.7 人的資源のセキュリティ	A.8 人的資源のセキュリティ
A.8 資産の管理	A.7 資産の管理
A.9 アクセス制御	A.11 アクセス制御
A.10 暗号	
A.11 物理的及び環境的セキュリティ	A.9 物理的及び環境的セキュリティ
A.12 運用のセキュリティ	A.10 通信及び運用管理
A.13 通信のセキュリティ	
A.14 システムの取得,開発及び保守	A.12 情報システムの取得,開発及び保守
A.15 供給者関係	
A.16 情報セキュリティインシデント管理	A.13 情報セキュリティインシデントの管理
A.17 事業継続マネジメントにおける情報セキュリティの側面	A.14 事業継続管理
A.18 順守	A.15 順守

登録第5662324号

本シンボルは、情報やセキュリティは人によって守られることをイメージしています。

● ISMS制度に関する問合せ先 ●

〒106-0032　東京都港区六本木一丁目9番9号　六本木ファーストビル内
一般財団法人　日本情報経済社会推進協会　情報マネジメント推進センター
TEL　03-5860-7570　FAX　03-5573-0564
URL　http://www.isms.jipdec.or.jp/

文書番号：JIP-ISMS120-5.0

JIPDEC

一般財団法人 日本情報経済社会推進協会

〒106-0032 東京都港区六本木一丁目9番9号 六本木ファーストビル内
TEL 03-5860-7551　FAX 03-5573-0560
URL http://www.jipdec.or.jp/

April 2014