情報セキュリティマネジメントシステム

ＩＳＭＳ認証機関認定基準及び指針

JIP-ISAC100-3.1

2016 年 8 月 1 日

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.03-5860-7570　　Fax.03-5573-0564
URL　http://www.isms.jipdec.or.jp/

改 版 履 歴

版数	制定／改訂日	改定箇所、改訂理由	備考
0.8	2001.5.1	パイロット事業用として 0.8 版制定	
1.0	2002.3.13	本格事業用として 1.0 版に改版	
2.0	2007.4.1	ISO/IEC Guide62 から ISO/IEC 17021 への移行に伴う変更。及び、指針 EA-7/03 から ISO/IEC 27006 への移行に伴う変更。 上記及び、審査登録⇒認証に伴う文書名の変更。	
2.0a	2007.4.20	誤記訂正：まえがき ISO/IEC 27001:2006⇒:2005 9. ISO/IEC 127006:2007⇒27006:2007 参考文献 ISO/IEC 17021:2007⇒：2006	
2.1	2008.11.12	規格名称等の変更	
2.2	2011.2.1	ISO/IEC 17021:2011 発行に伴う変更。 JIS Q 17021:2007 を ISO/IEC 17021:2011 に読み替える。	
2.2a	2011.4.1	協会名称の変更。	
2.2b	2011.12.26	協会住所、電話・FAX 番号の変更	
2.3	2012.3.22	ISO/IEC 27006:2011 発行に伴う変更。 JIS Q 27006:2008 を ISO/IEC 27006:2011 に置き換える。 ISO/IEC 27006:2011 に対応した JIS Q 27006 制定時の扱いを備考に記述。	
2.4	2013.10.1	ISO/IEC 27006:2011 を JIS Q 27006:2012 に置き換える。 適用する認証基準を ISO/IEC 27001:2013 とする。 - JIS Q 27001:2006 から ISO/IEC 27001:2013 への読み替え、及び ISO/IEC 27001:2013 に対応した JIS Q 27001 発行時の扱いを備考に記述。 - JIS Q 27001:2006 の要求事項を ISO/IEC 27001:2013 の対応した要求事項に読み替えることを追加。	

3.0	2015.10.1	ISO/IEC 27006:2015 発行に伴う変更。 JIS Q 27006:2012 を ISO/IEC 27006:2015 に置き換える。	
3.1	2016.8.1	ISMS クラウドセキュリティ認証の認定開始に伴う変更。 附属書 E（規定）ISMS クラウドセキュリティ認証を行う認証機関に対する追加の要求事項及び指針を追加。 附属書 F（参考）ISMS クラウドセキュリティ認証の審査工数の計算方法を追加。	

まえがき

この基準及び指針は、情報セキュリティマネジメントシステム（以下、ISMSという）認証業務を行っている第三者機関（以下、認証機関という）が、その業務遂行に関して適格であり信頼できると承認されるために遵守すべき一般要求事項及び指針を定めている。

この基準及び指針は、以下の本文で特段の定めのない限り、ISO/IEC 27006:2015「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の審査及び認証を行う機関に対する要求事項」をそのまま適用する。

備考 1　この基準及び指針では、ISO/IEC 27006:2015 邦訳版（一般財団法人 日本規格協会発行）で用いられている用語を使用する。ISO/IEC 27006:2015 と内容が一致する JIS Q 27006 が制定された場合は、その発行時点で、ISO/IEC 27006:2015 をそれに読み替えるものとする。

備考 2　この基準及び指針では、ISO/IEC 17021-1、ISO/IEC 27000、ISO/IEC 27001 及び ISO/IEC 27002 は、それぞれ JIS Q 17021-1、JIS Q 27000、JIS Q 27001 及び JIS Q 27002 と読み替えるものとする。

序文

ISO/IEC 27006:2015の「序文」を参照及び適用する。

１．適用範囲

ISO/IEC 27006:2015の「1　適用範囲」を適用する。

２．引用規格

ISO/IEC 27006:2015の「2　引用規格」を適用する。

３．用語及び定義

ISO/IEC 27006:2015の「3　用語及び定義」を適用する。

４．原則

ISO/IEC 27006:2015の「4　原則」を適用する。

５．一般要求事項

ISO/IEC 27006:2015の「5　一般要求事項」を適用する。

６．組織運営機構に関する要求事項

ISO/IEC 27006:2015の「6　組織運営機構に関する要求事項」を適用する。

７．資源に関する要求事項

ISO/IEC 27006:2015の「7　資源に関する要求事項」を適用する。

８．情報に関する要求事項

ISO/IEC 27006:2015の「8　情報に関する要求事項」を適用する。

９．プロセス要求事項

ISO/IEC 27006:2015の「9　プロセス要求事項」を適用する。

１０．認証機関に関するマネジメントシステム要求事項

ISO/IEC 27006:2015の「10　認証機関に関するマネジメントシステム要求事項」を適用する。

附属書 A

ISO/IEC 27006:2015の「附属書 A」を適用する。

附属書 B

ISO/IEC 27006:2015 の「附属書 B」を適用する。

附属書 C

ISO/IEC 27006:2015の「附属書 C」を適用する。

附属書 D

ISO/IEC 27006:2015 の「附属書 D」を適用する。

附属書 E（規定）
ISMS クラウドセキュリティ認証を行う認証機関に対する追加の要求事項及び指針

E.1　要員の力量

ISO/IEC 27006の箇条7.1の事項に加えて，以下のクラウドセキュリティの知識をもたなければならない。

a)クラウド基盤・要素技術（仮想化など）

b)ISO/IEC 27017:2015及び「ISO/IEC 27017:2015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-ISMS517-1.0）

c)関連する法令及び規制要求事項

d)クラウド固有の情報セキュリティリスク

E.2　ISMSクラウドセキュリティ認証審査チームの選定条件

ISO/IEC 27006の箇条7.2.1 IS 7.2の事項に加えて，クラウドセキュリティの知識及び技能に関する継続的専門的能力開発（CPD）により実証しなければならない。

E.3　認証文書

E.3.1　認証文書

認証文書に関する要求事項は，JIS Q 17021-1の箇条8.2.2によるほか，次による。

E.3.1.1　適用範囲

JIS Q 17021-1　8.2.2 f)「該当する場合，各事業所における活動の種類，製品及びサービスの種類に関する認証の範囲。誤解を招いたり不明瞭にならないように明示する。」について、ISMSクラウドセキュリティ認証の認証文書では、JIS Q 17021-1　8.2.2 f)について、認証文書の適用範囲の記述のなかでクラウドサービスが特定でき、誤解を招かない表現で明確に記載しなければならない。

注記1：クラウドサービス名の記載が無いことにより、例えば、組織の提供する複数のサービスのうちの一部しか適用範囲に含まれていなくても、全てのサービスで認証を取得しているかのように誤解されることを防ぐために、ISMSクラウドセキュリティ認証においては、クラウドサービス名を明確に記載する。

注記2：ISMSクラウドセキュリティ認証は組織に対するマネジメントシステム認証であり、製品又はサービスそのものに対する認証ではない。

E.3.1.2　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

ISMSクラウドセキュリティ認証は、クラウドサービスプロバイダとクラウドサービスカスタマとの2つの立場での認証があるため、どちらの立場で認証を取得したのか、あるいは両方の立場で認証を取得したの

かをJIS Q 17021-1　8.2.2の認証文書のなかで記載しなければならない。

E.3.1.3　認証に用いた規格及び／又はその他の規準文書によって要求されるその他の情報

ISMSクラウドセキュリティ認証における適用規格は、JIS Q 27001とJIP-ISMS517であるため、JIS Q 17021-1 8.2.2の認証文書の中で、JIP-ISMS517-1.0に適合している旨を記載しなければならない。また、同認証文書の中で、当該ISMSクラウドセキュリティ認証の基となるJIS Q 27001認証が識別できることを確実にしなければならない。

E.3.1.4　ISMSクラウドセキュリティ認証の有効期限

ISMSクラウドセキュリティ認証の有効期限は、基となるJIS Q 27001認証の有効期限を越えてはならない。

ISO/IEC 27017を認証文書に記載する場合には、ISO/IEC 27017はガイドラインである旨を明確に記述しなければならない。

記載例（クラウドサービスプロバイダとクラウドサービスカスタマとの両方の立場での認証の場合の例）
ISO/IEC 27017:2015のガイドラインに沿ったクラウドサービスプロバイダ及びクラウドサービスカスタマとして、JIP-ISMS517-1.0に適合していることを証する。

E.4　審査工数

審査工数に関する要求事項は，ISO/IEC 27006の箇条9.1.4.1 IS 9.1.4によるほか，ISMSクラウドセキュリティ認証の追加の審査工数を算出しなければならない。

注記1：ISMSクラウドセキュリティ認証の追加の審査工数は、ISMSクラウドセキュリティ認証の適用範囲を対象としたJIS Q 27001の審査工数を基礎とする。

注記2：審査工数の計算式を導き出すための付加的指針を附属書F（参考）に示す。

E.5　認証の一時停止，取消し又は範囲の縮小

ISMSクラウドセキュリティ認証の基となるJIS Q 27001認証が一時停止，取消し又は範囲の縮小となった場合は、当該ISMSクラウドセキュリティ認証も一時停止，取消し又は範囲の縮小としなければならない。

附属書 F（参考）
ISMS クラウドセキュリティ認証の審査工数の計算方法

F.1　一般

ISMSクラウドセキュリティ認証の追加の審査工数は、ISMSクラウドセキュリティ認証に関する要求事項（JIP-ISMS517）、ISMSクラウドセキュリティ認証の立場（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、両方）、クラウドサービス種別、システム構成、サービス利用者数等を加味して算出する。

この附属書は、JIS Q 27001の審査工数に追加するISMSクラウドセキュリティ認証の審査工数の計算式を導き出すための付加的指針を提供する。JIS Q 27001のサーベイランス審査もしくは再認証審査と併せて拡張する場合における審査工数の計算の基礎として使用できる要因の分類の例を表F.1に示す。

ISMSクラウドセキュリティ認証を拡張する場合の追加の審査工数（表F.1参照）は、JIS Q 27001の初回審査の審査工数を基準としている。

また、ISMSクラウドセキュリティ認証審査のみを単独で追加実施する場合は、表F.1に加えて、1審査人・日程度を追加することが望まれる。

ISMSクラウドセキュリティ認証の拡張後においては、ISMSクラウドセキュリティ認証の適用範囲を対象としたJIS Q 27001のサーベイランス工数もしくは再認証審査工数に表F.1の審査工数を追加する。

表F.1 - 審査工数の計算のための要因の分類の例示
（JIS Q 27001のサーベイランス審査もしくは再認証審査と併せて実施する場合の例）

ISMSクラウドセキュリティ認証の立場	ISO/IEC 27017の管理策による増加要因	クラウドサービス種別等の増加要因	追加の審査工数*
クラウドサービスプロバイダ	40/114=40%	+α	40%+α
クラウドサービスカスタマ	40/114=40%	+α	40%+α
クラウドサービスプロバイダ及びクラウドサービスカスタマ	80/114=70%	+α	70%+α

*ここでいう「追加の審査工数」とは、JIS Q 27001の審査工数に追加するISMSクラウドセキュリティ認証の審査工数のことである。

なお、ISMSクラウドセキュリティ認証審査をJIS Q 27001のサーベイランス審査時、もしくは再認証審査時に併せて拡張する場合の審査方法は、ISMSクラウドセキュリティ認証がJIS Q 27001認証の拡張の認証であるため、初回審査相当（第1段階・第2段階）の審査を行う必要はない。