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-ISAC100-2.4

2013 年 10 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。	

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、JIS Q 27006:2012「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　この基準及び指針では、JIS Q 27001:2006 の要求事項については ISO/IEC 27001:2013 の該当する記述に読み替えるものとする。更に ISO/IEC 27001:2013 と内容が一致する JIS Q 27001 が制定された時点で、それに読み替えるものとする。

序文

JIS Q 27006:2012の「序文」を参照及び適用する。

１．適用範囲

JIS Q 27006:2012の「1　適用範囲」を適用する。

２．引用規格

JIS Q 27006:2012の「2　引用規格」を適用する。

３．用語及び定義

JIS Q 27006:2012の「3　用語及び定義」を適用する。

４．原則

JIS Q 27006:2012の「4　原則」を適用する。

５．一般要求事項

JIS Q 27006:2012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

JIS Q 27006:2012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

JIS Q 27006:2012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

JIS Q 27006:2012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

JIS Q 27006:2012の「9　プロセス要求事項」を適用する。

ただしJIS Q 27001:2006の要求事項（1.2及び4.3.1）については、ISO/IEC 27001:2013の該当する記述に読み替えるものとする。

１０．認証機関に関するマネジメントシステム要求事項

JIS Q 27006:2012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

JIS Q 27006:2012の「附属書 A」を適用する。

ただし「表 A.1 - ISMS の適用範囲の複雑さの基準」で参照されている管理策の番号は、ISO/IEC 27001:2013 の該当する管理策の番号に読み替えるものとする。

附属書 B

JIS Q 27006:2012 の「附属書 B」を適用する。

附属書 C

JIS Q 27006:2012の「附属書 C」を適用する。

附属書 D

JIS Q 27006:2012 の「附属書 D」を適用する。

ただし「表 D.1 - 管理策の分類」の管理策は、ISO/IEC 27001:2013 の附属書 A の管理策に読み替えるものとする。