



ISMS

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-ISAC100-5.0

2024 年 5 月 31 日

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 番 9 号

六本木ファーストビル内

Tel.03-5860-7570 Fax.03-5573-0564

URL <https://isms.jp/>

ISMS-AC の許可なく転載することを禁じます

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。	
3.1a	2018.4.2	一般社団法人化に伴う変更	
4.0	2020.8.26	・ISO/IEC 27006:2015/Amd 1:2020 発行に伴う変更。 ・ISMS クラウドセキュリティ認証を行う認証機関に対する要求事項を別冊化することに伴う変更。	
4.1	2022.10.25	・ISO/IEC 27001:2022 発行に伴う変更。 適用する認証基準を ISO/IEC 27001:2022 とする。 - JIS Q 27001:2014 から ISO/IEC 27001:2022 への読み替え、及び ISO/IEC 27001:2022 に対応した JIS Q 27001 発行時の扱いを備考に記述。 - JIS Q 27001:2014 の要求事項を ISO/IEC 27001:2022 の対応した要求事項に読み替えることを 7 に追加。	
5.0	2024.5.31	・ISO/IEC 27006-1:2024 発行に伴う変更	

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 27006-1:2024「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 – 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」をそのまま適用する。

備考 この基準及び指針では、参照している ISO/IEC 文書について、例えば“ISO/IEC 27001:2022”は“JIS Q 27001:2023”というように、対応する JIS 規格がある場合は、それに読み替えるものとする。更に ISO/IEC 27006-1:2024 と内容が一致する JIS Q 27006-1 が制定された時点で、それに読み替えるものとする。

序文

ISO/IEC 27006-1:2024の「序文」を参照及び適用する。

1. 適用範囲

ISO/IEC 27006-1:2024の「1 適用範囲」を適用する。

2. 引用規格

ISO/IEC 27006-1:2024の「2 引用規格」を適用する。

3. 用語及び定義

ISO/IEC 27006-1:2024の「3 用語及び定義」を適用する。

4. 原則

ISO/IEC 27006-1:2024の「4 原則」を適用する。

5. 一般要求事項

ISO/IEC 27006-1:2024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 27006-1:2024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 27006-1:2024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 27006-1:2024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 27006-1:2024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 27006-1:2024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 27006-1:2024の「附属書 A」を適用する。

附属書 B

ISO/IEC 27006-1:2024 の「附属書 B」を適用する。

附属書 C

ISO/IEC 27006-1:2024の「附属書 C」を適用する。

附属書 D

ISO/IEC 27006-1:2024 の「附属書 D」を適用する。

附属書 E

ISO/IEC 27006-1:2024 の「附属書 E」を適用する。