JIS

# 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

JIS Q 27006：2018

（ISO/IEC 27006：2015）

（JIPDEC/JSA）

平成 30 年 3 月 20 日　改正

日本工業標準調査会 審議

（日本規格協会 発行）

日本工業標準調査会標準第二部会 情報技術専門委員会 構成表

| | 氏名 | 所属 |
|---|---|---|
| （委員会長） | 伊　藤　　智 | 国立研究開発法人新エネルギー・産業技術総合開発機構 |
| （委員） | 青　木　裕佳子 | 公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会 |
| | 小　高　久　義 | 総務省行政管理局 |
| | 岩　田　秀　行 | 日本電信電話株式会社 |
| | 榎　本　義　彦 | 日本アイ・ビー・エム株式会社 |
| | 山　田　美佐子 | 一般財団法人日本消費者協会 |
| | 小　野　文　孝 | 東京大学 |
| | 橋　本　　崇 | 日本銀行金融研究所 |
| | 神　保　光　子 | 日本電気株式会社 |
| | 菅　野　育　子 | 愛知淑徳大学 |
| | 鈴　木　正　敏 | 一般社団法人ビジネス機械・情報システム産業協会 |
| | 足　立　朋　子 | 株式会社東芝 |
| | 西　山　　茂 | 新潟国際情報大学 |
| | 中　溝　和　孝 | 総務省国際戦略局 |
| | 三　宅　　滋 | 株式会社日立製作所 |
| | 福　田　泰　和 | 一般財団法人日本規格協会 |

主　務　大　臣：経済産業大臣　　制定：平成 20.9.20　　改正：平成 30.3.20
官　報　公　示：平成 30.3.20
原 案 作 成 者：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 1-9-9　六本木ファーストビル内　TEL 03-5860-7551）
一般財団法人日本規格協会
（〒108-0073　東京都港区三田 3-13-12　三田 MT ビル　TEL 03-4231-8530）
審　議　部　会：日本工業標準調査会　標準第二部会（部会長　大崎　博之）
審議専門委員会：情報技術専門委員会（委員会長　伊藤　智）

この規格についての意見又は質問は，上記原案作成者又は経済産業省産業技術環境局 国際電気標準課（〒100-8901 東京都千代田区霞が関 1-3-1）にご連絡ください。

なお，日本工業規格は，工業標準化法第 15 条の規定によって，少なくとも 5 年を経過する日までに日本工業標準調査会の審議に付され，速やかに，確認，改正又は廃止されます。

# 目　次

ページ

# まえがき

この規格は，工業標準化法第 14 条によって準用する第 12 条第 1 項の規定に基づき，一般財団法人日本情報経済社会推進協会（JIPDEC）及び一般財団法人日本規格協会（JSA）から，工業標準原案を具して日本工業規格を改正すべきとの申出があり，日本工業標準調査会の審議を経て，経済産業大臣が改正した日本工業規格である。

これによって，**JIS Q 27006**:2012 は改正され，この規格に置き換えられた。

この規格は，著作権法で保護対象となっている著作物である。

この規格の一部が，特許権，出願公開後の特許出願又は実用新案権に抵触する可能性があることに注意を喚起する。経済産業大臣及び日本工業標準調査会は，このような特許権，出願公開後の特許出願及び実用新案権に関わる確認について，責任はもたない。

白　　紙

日本工業規格　　JIS

Q 27006：2018

(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

Information technology—Security techniques—
Requirements for bodies providing audit and certification of information security management systems

## 序文

この規格は，2015 年に第 3 版として発行された **ISO/IEC 27006** を基に，技術的内容及び構成を変更することなく作成した日本工業規格である。

なお，この規格で点線の下線を施してある参考事項は，対応国際規格にはない事項である。

マネジメントシステムを審査及び認証する機関に対する基準を規定する規格として，**JIS Q 17021-1**:2015 がある。

このような審査及び認証する機関を，**JIS Q 27001**:2014 に沿って情報セキュリティマネジメントシステム（以下，ISMS という。）の審査及び認証を実施する目的で，**JIS Q 17021-1**:2015 に適合しているとして認定するためには，**JIS Q 17021-1**:2015 に対して追加の要求事項及び手引が必要である。この規格は，このような追加の要求事項及び手引を提供する。

この規格は，**JIS Q 17021-1**:2015 の構成に沿っている。また，**JIS Q 17021-1**:2015 を ISMS 認証に適用するための ISMS 固有の追加の要求事項及び手引は，“IS”という表記によって識別されている。

この規格において，“～なければならない”という表現は，**JIS Q 17021-1**:2015 及び **JIS Q 27001**:2014 の要求事項を反映する必須要件の規定を示すために用いられている。“～ことが望ましい”という表現は，推奨事項を示すために用いられている。

この規格の主な目的は，認定機関が認証機関を評価しようとする場合に用いる規格の適用を，より有効に整合できるようにすることである。

この規格において，“マネジメントシステム”及び“システム”という用語は，区別なく用いられている。マネジメントシステムの定義は，**JIS Q 9000**:2005 に規定されている。この規格で用いられているマネジメントシステムを，他の種類のシステム，例えば，IT システムと混同しないほうがよい。

## 1　適用範囲

この規格は，**JIS Q 17021-1**:2015 及び **JIS Q 27001**:2014 に規定する要求事項に加えて，ISMS の審査及び認証を行う機関に対する要求事項を規定し，かつ，手引を提供する。この規格は，ISMS 認証を行う認証機関の認定を支援することを主として意図している。

この規格に含まれる要求事項は，ISMS 認証を行う機関によって，力量及び信頼性の観点から実証され