

# ISO/IEC 27000 ファミリー規格について

～ ISO/IEC JTC 1/SC 27/WG 1 に

おける検討状況 ～



## Contents

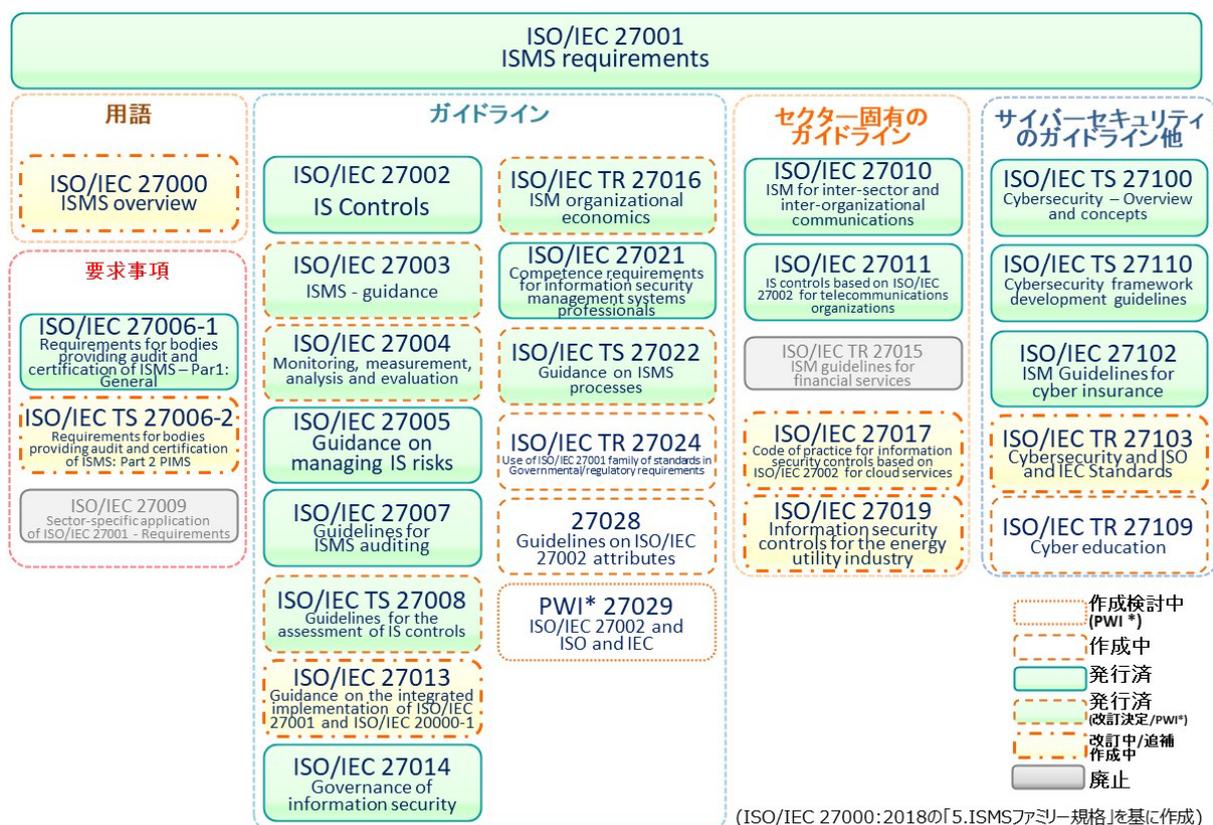
1. ISO/IEC 27000 ファミリー規格とは .....	2
2. ISO/IEC JTC 1/ SC 27/WG 1 会議の結果概要 .....	4
2-1 WG1 における ISO/IEC 27000 ファミリー規格の検討状況 .....	4
2-2 主なプロジェクトの進捗状況 .....	5
【個々の規格の概要】 .....	6
■ ISO/IEC 27000～ISO/IEC 27010 .....	6
■ ISO/IEC 27011～ISO/IEC 27019 .....	13
■ ISO/IEC 27021～ISO/IEC 27029 .....	16
■ ISO/IEC TS 27100～ISO/IEC TS 27110 .....	18
参考：ISO/IEC JTC 1 における規格作成の段階 .....	20

# 1. ISO/IEC 27000 ファミリー規格とは

ISO/IEC 27000 ファミリー規格は、情報セキュリティマネジメントシステム（ISMS）に関する国際規格であり、ISO（国際標準化機構）及びIEC（国際電気標準会議）の合同専門委員会 ISO/IEC JTC 1（情報技術）の分科委員会 SC 27（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）において標準化作業が進められています。

ISO/IEC 27000 ファミリー規格は、要求事項を規定した規格（ISMS 要求事項を規定した ISO/IEC 27001、ISMS 認証機関のための要求事項を規定した ISO/IEC 27006 及びセクター固有の ISMS 実施のための追加の要求事項の枠組みを規定した ISO/IEC 27009）と、ISMS 実施の様々な側面に関する手引を規定した規格（一般的なプロセス、管理策に関する指針及びセクター固有の手引）から構成されています。規格の番号は、現時点では 27000～27040 番台及び 27100～27110 番台の一部が中心となっています。

ISO/IEC 27000 ファミリー規格は、主に SC 27/WG 1（情報セキュリティマネジメントシステム）において作成されています。以下の図は、WG 1 における規格の作成/改訂状況を示しています。



\*PWI : ISO 規格作成/改訂手続(NP)前に設置される予備段階で、主に規格の作成/改訂の方針等について検討しています（「作成中」は手続済で作成段階にある規格です。）規格作成の段階については、「2-1 WG1 における ISO/IEC 27000 ファミリー規格の検討状況」をご参照下さい。

※ ISO/IEC TS 27006-2 は、SC 27/WG 5 のプロジェクトとして登録されていますが、SC 27/WG 1 と合同で策定され、ISO/IEC 27006 の第 2 部（Part 2）であるため記載しています。

また、SC 27/WG 1 の他、SC 27/WG 4（セキュリティコントロールとサービス）、SC 27/WG 5（アイデンティティ管理とプライバシー技術）においても関連する規格が策定されています。以下は、現在、作成・発行されている規格

の一例です。

**ISO/IEC 27018:2019**

Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

**ISO/IEC 27031:2011**

Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity

**ISO/IEC 27032:2023**

Cybersecurity — Guidelines for Internet security

**ISO/IEC 27701:2019**

Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

詳細については、ISO の Web サイトをご参照ください。

ISO/IEC JTC 1/SC 27 で作成された規格一覧：

<https://www.iso.org/committee/45306/x/catalogue/>

## 2. ISO/IEC JTC 1/ SC 27/WG 1 会議の結果概要

WG 1 会議は、2024 年 3 月 25～27 日に Web 会議で開催されました（多くのプロジェクトは、この会期外に Web 会議で審議を実施）。以下に ISO/IEC 27000 ファミリー規格の検討状況を一覧表として示すとともに、主なプロジェクトの進捗状況等を記載します。

### 2-1 WG1 における ISO/IEC 27000 ファミリー規格の検討状況

\*各会議で審議される規格の段階を示しています。既に IS 発行済で現在改訂中のものについては、（）で改訂段階を示しています。

例：（DIS） – IS 発行済だが、現在改訂中で DIS 審議

※下表の色分け：緑色は発行済規格[斜字は改訂決定]、薄黄色は改訂中/追補作成中規格、灰色は中止プロジェクトです（白は作成中）。

ISO/IEC 番号	規格内容	規格作成の段階*	
		2024 年 3 月 会議	2024 年 10 月 会議（予定）
<a href="#">27000</a>	ISMS 概要	(WD)	(CD)
<a href="#">27001</a>	ISMS 要求事項	IS	IS
<a href="#">27002</a>	情報セキュリティ管理策	IS	IS
<a href="#">27003</a>	ISMS の手引	(PWI)	(WD)
<a href="#">27004</a>	ISM – 監視、測定、分析及び評価	(PWI)	(PWI)
<a href="#">27005</a>	情報セキュリティリスクマネジメントに関する指針	IS	IS
<a href="#">27006-1</a>	ISMS 認証機関に対する要求事項	IS	(PWI)
<a href="#">TS 27006-2</a>	ISO/IEC 27701 認証機関に対する要求事項	(DIS)	(DIS)
<a href="#">27007</a>	ISMS 監査の指針	IS	IS
<a href="#">TS 27008</a>	IS 管理策の評価(assessment)のための指針	(PWI)	(CD)
<a href="#">27009</a>	セクターへ規格の 27001 適用 – 要求事項	(廃止)	(廃止)
<a href="#">27010</a>	セクター間及び組織間コミュニケーションのための情報セキュリティマネジメント	IS	IS
<a href="#">27011</a>	ISO/IEC 27002 に基づく電気通信組織のための情報セキュリティ管理策	FDIS	IS
<a href="#">27013</a>	ISO/IEC 27001 と ISO/IEC 20000-1 との統合導入についての手引	(DAM)	(IS<追補 1>)
<a href="#">27014</a>	情報セキュリティのガバナンス	IS	IS
<a href="#">TR 27015</a>	金融サービスに対する情報セキュリティマネジメントの指針	(廃止)	(廃止)
<a href="#">TR 27016</a>	ISM – 組織の経済的側面(Organizational economics)	TR	(PWI)
<a href="#">27017</a>	ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範	(CD)	(CD)
<a href="#">27019</a>	エネルギー業界のための情報セキュリティ管理策	(DIS)	(FDIS)
<a href="#">27021</a>	ISMS 専門家の力量に関する要求事項	IS	IS
<a href="#">TS 27022</a>	ISMS プロセスに関する手引	(PWI)	(PWI)
<a href="#">TR 27023</a>	ISO/IEC 27001 及び ISO/IEC 27002 改訂版のマッピング	(廃止)	(廃止)
<a href="#">TR 27024</a>	各国の規制要求事項等における ISO/IEC 27001 ファミリー規格の使用	WD	DTR
<a href="#">27028</a>	ISO/IEC 27002:2022 の属性の利用及び作成に関する手引	CD	CD
<a href="#">27029</a>	ISO/IEC 27002 の管理策及び手引を参照している規格一覧	PWI	SD
<a href="#">TS 27100</a>	サイバーセキュリティの概要及びコンセプト	TS	TS
<a href="#">27102</a>	ISM – サイバー保険のためのガイドライン	IS	IS
<a href="#">TR 27103</a>	サイバーセキュリティと ISO 及び IEC 規格	(CD)	(CD)
<a href="#">TR 27109</a>	サイバーセキュリティに関する教育・訓練	WD	DTR
<a href="#">TS 27110</a>	サイバーセキュリティフレームワーク策定の指針	TS	TS

## 2-2 主なプロジェクトの進捗状況

### 27000 (Information security management systems – Overview)

2023年8～10月に実施したWDに対するコメント募集の結果、約30件のコメントが寄せられた。2024年1月8日にコメント審議のためのオンライン会議を実施し、全てのコメント審議を終了した。審議の結果、次回は2nd WDを発行することになった。

その後、2ndWDに対して1月～3月の間でコメント募集が実施され、約80件のコメントが寄せられた。5月21日に2ndWDに対するコメント審議のためのオンライン会議を実施した。ISO事務局より、「ISO/IEC 27000 family of standards」という用語と、箇条「5 ISO/IEC 27001 and other ISMS related standards」の構成について指摘があった。これを受けて、ISO/IEC Directivesに合わせて「family」を使用しないこと（「series」は使用可）、及び箇条5の構成はType A MSS、Type B MSS、その他というようにISO/IEC DirectivesのAnnex SLの用語・分類に合わせて変更することになった。審議の結果、次回はCDを発行することになった。

※本文書の表題「ISO/IEC 27000 ファミリー規格について」は、今後の改訂審議における更なる変更を考慮して現時点では変更せずに、ISO/IEC 27000 改訂版の発行に合わせて変更予定です。

### 27006-1 (Requirements for bodies providing audit and certification of information security management systems - Part1 General)

2023年12月28日にFDIS投票終了後、2024年3月1日に発行された。

今回の会議にて、改訂時に解決に至らなかった事項（力量に関する要求事項等）について審議するためのPWI（予備段階）が設置された。

■ ISO/IEC 27006の規格群として、WG 5会議において次の規格の改訂について審議された。

### TS 27006-2 (Requirements for bodies providing audit and certification of information security management systems - Part 2: Privacy information management systems)

ISO/IEC 27701がISO/IEC 27001から独立したマネジメントシステムとなる\*ことを受けて、ISO/IEC 27006-2もISO/IEC 27006-1からISO/IEC 17021-1（マネジメントシステム認証機関に対する要求事項）に基づく構成に変更され、それに伴い、標題、規格番号、適用範囲も変更するようことになった。そのため、現在、DISを基にドラフトを大幅に修正して改訂作業中。

なお、現時点では、ISO/IEC 27701、ISO/IEC 27706（27006-2から番号変更）ともに2024年内発行を目標に改訂作業が進められている。※今後の状況によっては、発行が遅れる可能性がある

\*FDIS 27701申請時にISO事務局からの強い指示によって、ISO規格のマネジメントシステム共通の構成・テキストを適用して文書全体を変更しなければならなくなった（その結果、「ISO/IEC 27001の拡張」という表現を使用せずに、ISMSとは独立したマネジメントシステム規格としなければならなくなった）。

(2024年1月のオンライン国際会議での審議結果を含む)

## 【個々の規格の概要】

### ■ ISO/IEC 27000～ISO/IEC 27010

#### ISO/IEC 27000:2018

Information technology – Security techniques – Information security management systems – Overview and vocabulary

2018年2月発行 [第5版] (改訂中)

ISMSファミリー規格の概要、ISMSファミリー規格において使用される用語等について規定した規格。

- **国内規格の発行** : 2019年3月に JIS Q 27000:2019 として制定された。

#### **JIS Q 27000:2019**

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 27000:2018 の用語及び定義の技術的内容を変更することなく作成した国内規格 (ISMS の概要等を示した ISO/IEC 27000:2018 の箇条 4 以降は含まれていない) 。

#### ■ **改訂について** :

- 2009年：第1版発行。2012年12月：第2版発行。2014年1月：第3版発行（その際に27001:2013、27002:2013対応）。2016年2月：第4版発行。2018年2月：第5版発行。
- 2021年4月 Web 会議にて合意された、ISO/IEC 27002 改訂の影響を受ける27000ファミリー規格全体の段階的改訂スケジュールに従って、第2段階の改訂として、27000、27008、27019、27103 の改訂検討を開始することが合意された。これを受けて、2021年10月 Web 会議にて、27000 の改訂方針 (DS : Design Specification) を検討するためにPWIが設置された。
- 2023年4月 Web 会議にて、改訂方針も合意されプロジェクト開始の準備が整ったことから、改訂プロジェクト (36か月間) を開始することがWG1 Convenor (議長) から提案された。特に反対はなく、承認された。なお、PWIにおいて、タイトル及び内容を以下の通り変更することになった。
  - タイトル : Information security, cybersecurity and privacy protection – Information security management systems – Overview
  - 内容 : ① ISO/IEC 27000 ファミリーの規格で使用される用語の定義を削除 (理由 : ISO/IEC 27000 は、各規格で審議された用語の定義を記載した単なる用語集という位置付けにも関わらず、「用語の定義は ISO/IEC 27000 改訂で審議すべし、各規格の作成/改訂で審議すべしではない」という誤解があり、用語の定義の更新に問題が生じたため) 。
  - ② 新たに附属書を追加し、ISO/IEC 27000 ファミリーで共通に使用される定義を記載する。
  - ③ 情報セキュリティのコンセプト及び概念を追加する。

※ 27000 ファミリー規格の策定・改訂に対応する必要があるため、比較的短期間でマイナーな改訂が実施されていた。

[\(2.1に戻る\)](#)

#### ISO/IEC 27001:2022

Information security, cybersecurity and privacy protection — Information security management systems – Requirements

2022年10月発行 [第3版]

組織の事業リスク全般を考慮して、文書化した ISMS を確立、実施、維持及び継続的に改善するための要求事項を

規定した規格。

- **国内規格の発行**：2023年9月に JIS Q 27001:2023（JIS Q 27001:2014 の改正版）として制定された。

### JIS Q 27001:2023

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情報—情報セキュリティマネジメントシステム—要求事項

- **正誤票の発行**：なし（第2版に対して発行された正誤票は、第3版発行時に統合された。）

### ■ 改訂について：

- 2005年に第1版発行後、2008年10月に規格発行から3年目の定期レビュー（Pre-review）審議を行い、改訂開始が決定された。これを受けた改訂作業を経て、2013年10月に第2版が発行された。
- 2016年4月タンパ会議にて規格発行から3年目の定期レビュー（Pre-review）審議を行った。その結果、現時点では改訂は行わず現行版を維持することになった。
- 2019年4月テルアビブ会議にて規格発行から5年目の定期レビュー（Systematic review）審議を行った結果、「ISO/IEC Directives, Part 1 —Consolidated ISO Supplement —Procedure for the technical work — Procedures specific to ISO —（ISO/IEC 専門業務用指針第1部—統合版 ISO 補足指針—ISO 専用手順—）」の Annex SL（マネジメントシステム規格の共通要素を定めた附属書）の改訂を考慮して、現時点では維持（confirm）とする方向となった。一方で、この Annex SL 改訂版の発行時期、ISO/IEC 27002 の改訂等を考慮した 27001 次期改訂への対応案がいくつか提示され、次回会議にて審議することになった。
- 2019年10月パリ会議にて上記に関して審議した結果、現時点では改訂を開始しないが、今後 Annex L\*や ISO/IEC 27002 の改訂状況をみながら必要に応じて再度検討することになった。  
\*2019年版では Annex SL から Annex L（（規定）マネジメントシステム規格の提案）に附属書番号が変更されたが、2020年版にて再び Annex SL となった。
- 2021年4月 Web 会議にて、ISO/IEC 27002 の改訂審議が DIS 段階となったことを受けて、27002 改訂の影響を受ける 27000 ファミリー規格全体の改訂スケジュールについて検討した。その結果、第1段階の改訂として 27001、27009、27017 を改訂することになった。  
27001 については、附属書 A を ISO/IEC 27002 改訂版に整合させるために限定的な改訂を実施し、Amendment（追補）を作成することになった。なお、すでに正誤票が2件発行されていることから、これらの正誤票と Amendment を ISO/IEC 27001:2013 に統合して、ISO/IEC 27001 第3版として発行される見込み。並行して PWI を設置し、27001 全面改訂を検討することになった。
- 2022年10月に、第3版が発行された。この第3版では、当初の予定通り、附属書 A を ISO/JIS 27002:2022 に沿って更新したことに加えて、ISO 中央事務局の指示により ISO/IEC Directives, Part 1 の Annex SL\*最新版に沿って本文を更新した。

[\(2.1に戻る\)](#)

## ISO/IEC 27002:2022

Information security, cybersecurity and privacy protection—information security controls

2022年2月発行 [第3版]

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ベストプラクティスをまとめた規格。ISO/IEC 27001 の「附属書 A 管理目的及び管理策」と整合がとられている。

※ 当初、ISO/IEC 17799 として発行されたが、2007年7月に規格番号が 27002 へ改番された。

- **国内規格の発行** : 2014 年 3 月に JIS Q 27002:2014 (JIS Q 27002:2006 の改正版) として制定された。

### JIS 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

- **正誤票の発行** : なし

#### ■ **改訂について** :

- 2005 年に第 1 版発行後、2008 年 10 月に規格発行から 3 年目の定期レビュー (Pre-review) 審議を行い、改訂開始が決定された。これを受けた改訂作業を経て、2013 年 10 月に第 2 版が発行された。
- 2016 年 4 月タンパ会議にて規格発行から 3 年目の定期レビュー (Pre-review) 審議を行った。その結果、改訂する方向となり、SP (Study Period) <sup>1</sup>を設置して、design specification (改訂の方針等) について検討することになった。
- 2017 年 11 月ベルリン会議にて SP を終了し正式に改訂プロジェクトを開始するための NP 投票を実施した結果、2018 年 4 月武漢会議より改訂プロジェクトが開始された。

なお、design specification 審議において規格名称を以下に変更することになった。

Information technology — Security techniques — Information security controls

- 2022 年 2 月に、数年にわたる審議の後、改訂版が発行された (その後、2022 年 3 月に修正版 [Corrected version] が発行された)。
  - ✓ 関連する改訂 : 2021 年 4 月 Web 会議にて、27002 の改訂審議が DIS 段階となったことを受けて、27002 改訂の影響を受ける 27000 ファミリー規格全体の改訂スケジュールについて、前回の会議にて検討した結果、3 段階に分けて関連規格を改訂することになった。第 1 段階として、27001、27009、27017 の PWI を設置し、改訂検討を開始した。
  - ✓ 関連する改訂 : 2021 年 10 月 Web 会議にて、第 2 段階として、27000、27008、27019、27103 の PWI を設置し、改訂検討を開始した。
  - ✓ 関連する改訂 : 2022 年 10 月 Web 会議にて、第 3 段階として、27003、27004 の改訂の必要性を審議した。その結果、改訂することで合意されたことから、PWI を設置し、改訂検討を開始した。
  - ✓ 関連する改訂 : 2023 年 10 月 Web 会議にて、第 4 段階として、27022 の改訂の必要性を審議した。その結果、改訂することで合意されたことから、PWI を設置し、改訂検討を開始した。また、27016 改訂の必要性を検討する必要性についてコメントを募集することになった。Web 会議後、27016 改訂のために PWI 設置をするか否かについてコメントを募集した結果、特に反対はなかったため 2024 年 1 月に PWI 設置が設置された。

[\(2.1 に戻る\)](#)

## ISO/IEC 27003:2017

Information technology – Security techniques – Information security management system – Guidance

2017 年 4 月発行 [第 2 版] (改訂検討中)

ISO/IEC 27001 : 2013 に規定する ISMS の要求事項に対するガイダンス規格。箇条 4 から 10 は、ISO/IEC 27001 の構成に沿っており、各箇条では、要求される活動 (Required activity) 、説明 (Explanation) 、ガイダ

<sup>1</sup>SP (Study Period) : 期間を設定して設置される検討プロジェクト。ISO 策定・改訂以外の事項 (例 : 27009 事例集の検討) や、規格の策定・改訂の開始前に必要な方針 (design specification) について検討される。なお、2019 年 10 月のパリ会議から、ISO/IEC Directives (ISO/IEC 専門業務用指針) に沿って SP に代わり PWI を設置することになった。

ンス（Guidance）、関連情報（Other Information）について記載されている。

■ 改訂について：

- 2010年に第1版発行後、2013年5月にISO/IEC 27001:2013に対応するための早期改訂開始が決定された。これを受けた改訂作業を経て、2017年4月に第2版が発行された。
- 2020年4月Web会議にて規格発行から3年目の定期レビュー（Periodical pre-review）審議を行った結果、現時点では改訂は行わず現行版を維持することになった。
- 2022年10月Web会議にて、（2021年4月Web会議にて合意された、ISO/IEC 27002改訂の影響を受ける27000ファミリー規格全体の段階的改訂スケジュールの第3段階として改訂の必要性を審議した結果）ISO/IEC 27001第3版で本文が変更されることになったことから、PWIを設置し、改訂を検討することになった。
- 2024年3月ロンドン会議にて、プロジェクト開始の準備が整ったことから、改訂プロジェクト（36か月間）を開始することが合意された。

[\(2.1に戻る\)](#)

## [ISO/IEC 27004:2016](#)

Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation

2016年12月発行 [第2版] **(改訂検討中)**

ISO/IEC 27001:2013に規定する「9.1 監視、測定、分析及び評価」の要求事項を満たすために情報セキュリティのパフォーマンス及びISMSの有効性の評価を支援することを目的としたガイダンス規格。

■ 改訂について：

- 2009年に第1版発行後、2012年5月に規格発行から3年目の定期レビュー（Periodical pre-review）審議の結果により改訂開始が決定された。これを受けた改訂作業を経て、2016年12月に第2版が発行された。
- 2019年4月にテルアビブ会議にて規格発行から3年目の定期レビュー（Periodical pre-review）審議を行った。その結果、現時点では改訂は行わず現行版を維持することになった。一方で、英国から編集上の不備による適用への影響が報告され、不備を修正するための正誤票（Corrigendum）を発行する方向となった。
- 2022年4月にWeb会議にて5年目の定期レビュー（Systematic review）を行った結果、ISO/IEC 27001:2013からの参照をISO/IEC 27001:2022に更新するための正誤票（Corrigendum）を発行する方向となった。
- 2022年10月Web会議にて、（2021年4月Web会議にて合意された、ISO/IEC 27002改訂の影響を受ける27000ファミリー規格全体の段階的改訂スケジュールの第3段階として改訂の必要性を審議した結果）ISO/IEC 27001第3版で本文が変更されること、及び用語の再検討が必要というコメント等を受けて、PWIを設置することになった。

[\(2.1に戻る\)](#)

## [ISO/IEC 27005:2022](#)

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

2022年10月発行 [第4版]

情報セキュリティのリスクマネジメントに関するガイドライン規格。

#### ■ 改訂について：

- 2008年6月に第1版発行後、2010年4月にISO 31000:2009及びISO Guide 73:2009との整合に限定した改訂を行うことが決定され、2011年に第2版が発行された。
- 2013年10月にISO/IEC 27001:2013に対応するための早期改訂開始が決定されたが、ISO規定の期間内に発行に至らなかったため2016年4月にいったん改訂プロジェクトはキャンセルとなった。そのため、改めてSP (Study Period) を設置して、design specification (今後の改訂の方針、方向性等) を検討することになった。
- 2017年4月ハミルトン会議にて、ISO/IEC 27005:2011に対して提出された Defect Report (ISO/IEC 27001:2005 対応であり廃止すべきという英国提案) を審議した結果、SPと並行してISO/IEC 27001:2013に合わせるための編集上の修正を示した正誤票を発行する手続を実施することになった。
- 2017年10-11月ベルリン会議にて、ISOの手続上の関係から正誤票ではなく改訂版を発行することになった。そのため、正誤票案の内容を反映した版を迅速化手続によって準備し、2018年7月に第3版として発行された (なお、上記の通りISO/IEC 27001:2013に合わせるための技術的な修正は行われていない)。  
ISO/IEC 27001:2013 対応のための改訂については、2013年10月に開始したSPにて検討した結果、2019年4月テルアビブ会議にて本SPを終了し、正式に改訂プロジェクトを開始するためのNP投票を実施することになった。2019年10月パリ会議にて、NP投票結果を受けて改訂プロジェクトを開始することになった。
- 2020年4月Web会議にて、規格名称について、2017年に合意されたDesign Specification (改訂方針) に従って変更すべきとの提案を受けて、以下に変更することになった。  
Guidance on managing information security risks
- 2022年10月に、第4版が発行された。

[\(2.1に戻る\)](#)

## ISO/IEC 27006-1:2024

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

2024年3月発行 [第1版]

ISMS認証を希望する組織の審査・認証を行う認証機関に対する要求事項を規定した規格。

マネジメントシステム認証機関に対する要求事項としてはISO/IEC 17021-1が規定されているが、ISMS認証機関に対しては併せてISO/IEC 27006が要求される。

- **国内規格の発行**：2018年3月にJIS Q 27006:2018 (JIS Q 27006:2012の改正版) として制定された。

### JIS Q 27006:2018

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

#### ■ 改訂について：

- 2007年に第1版発行後、ISO/IEC 17021の改訂版ISO/IEC 17021:2011が発行されたことを受けて、2011年4月にISO/IEC 27006もISO/IEC 17021:2011との整合に限定した早期改訂を行うことが決定され、2011年に第2版が発行された。
- その後、2012年5月にISO/IEC 17021:2011 整合以外の内容も含む改訂開始が決定された。これを受けた改訂作業を経て、2015年に第3版が発行された。
- 2018年4月武漢会議にて規格発行から3年目の定期レビュー (Pre-review) 審議を行った。その結果、6か月

間の SP (Study Period) を設置し、追補の発行が必要か検討することになった。

- 2018年9-10月イビク会議において、追補発行の可能性について検討した結果、追補を発行することになり、2020年3月に追補1が発行された。
- 2020年9月Web会議にて、ISO/IEC TS 27006-2 発行に伴い、ISO/IEC 27006-1 への番号変更が必要になったこと、及び今後の ISMS セクター規格認証（例：ISO/IEC 27701）の認定への共通的な対応を検討する必要が生じたことから、27006 改訂について検討するために PWI を設置することになった。
- PWI27006 審議のために実施された 2021年2月Web会議にて、ISMS セクター規格認証対応のため、及びニューノーマルに関連する事項を検討するための改訂開始が決定された。なお、規格番号は 27006-1 へ、これに伴いタイトルを以下に変更するための手続きを進めることになった。

Requirements for bodies providing audit and certification of information security management systems – Part1: General

- 2024年3月に、数年にわたる審議の後、改訂版が発行された。
- 2024年3月ロンドン会議にて、改訂時に保留となった事項（審査員の力量他）を検討するために、PWIを設置することになった。

※27006 から 27006-1 への変更に伴い、2024年版が（ISO/IEC 27006-1 としての）第1版となった。

#### ■ ISO/IEC 27006 の規格群

##### ISO/IEC TS 27006-2:2021

Requirements for bodies providing audit and certification of information security management systems - Part 2: Privacy information management systems

2021年2月発行（改訂中）

ISO/IEC 27701 の認証を希望する組織の審査・認証を行う認証機関に対する要求事項を規定した規格。

ISO/IEC 27701 の認証機関に対しては、ISO/IEC 27006 と併せて ISO/IEC TS 27006-2 への適合が要求される。

#### ■ 改訂について：

- 2021年4月Web会議にて、TS から IS へ変更するための改訂について審議された。その結果、改訂を開始（ISO/CASCO の承認要）することになった。本改訂は、ISO/IEC JTC 1/SC 27/WG 5 にて審議される。

[\(2.1 に戻る\)](#)

#### ISO/IEC 27007:2020

Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing

2020年1月発行 [第3版]

ISMS 監査の実施に関するガイドライン規格。ISO 19011:2018（マネジメントシステム監査のための指針－2018年07月発行）に加えて、ISMS 固有のガイダンスを提供する。

#### ■ 改訂について：

- 2011年に第1版発行後、2014年4月に規格発行から3年目の定期レビュー（Periodical pre-review）を実施した結果、改訂開始が決定され、2017年10月に第2版が発行された。
- 2018年9-10月イビク会議にて、ドイツ提案による ISO 19011:2018 対応のための早期改訂について審議した結

果、ISO 19011:2018 対応に限定したマイナーな早期改訂開始が決定され、2020 年 1 月に第 3 版が発行された。

[\(2.1に戻る\)](#)

## [ISO/IEC TS 27008:2019](#)

Information technology – Security techniques – Guidelines for the assessment of information security controls

2019 年 1 月発行 (改訂検討中)

情報セキュリティの管理策のレビューに関する技術仕様。

### ■ 改訂について :

- 2011 年に第 1 版発行後、2014 年 4 月に規格発行から 3 年目の定期レビュー (Periodical pre-review) を実施した結果、改訂開始が決定され、2019 年 1 月に第 2 版が発行された。改訂審議の中で、TR (Technical Report : 標準報告書) から TS (Technical Specification : 標準仕様書) となり、さらに適用範囲の変更とともに標題も変更された。
- 2021 年 4 月 Web 会議にて合意された、ISO/IEC 27002 改訂の影響を受ける 27000 ファミリー規格全体の段階的改訂スケジュールに従って、第 2 段階の改訂として、27000、27008、27019、27103 の改訂検討を開始することが合意された。これを受けて、27008 の改訂方針を検討するために PWI が設置された。
- 2024 年 3 月ロンドン会議にて、プロジェクト開始の準備が整ったことから、改訂プロジェクト (36 か月間) を CD から開始することが WG1 Convenor (議長) から提案された。特に反対はなく、承認された。

※TS への変更に伴い、2019 年が (ISO/IEC TS 27008 としての) 第 1 版となった。

[\(2.1に戻る\)](#)

## [ISO/IEC 27009:2020](#)

Information security, cybersecurity and privacy protection – Sector-specific application of ISO/IEC 27001 - requirements

2020 年 4 月発行

ISO/IEC 27001 を各セクターに適用した規格を作成する際の、規格の記述方法、様式等を定めた規格であり、セクター規格を作成する組織を対象としている。

### ■ 改訂について :

- 2017 年 4 月ハミルトン会議にて早期改訂を開始することが決定され、2020 年 4 月に第 2 版が発行された。
- 2021 年 4 月 Web 会議にて、ISO/IEC 27002 の改訂審議が DIS 段階となったことを受けて、27002 改訂の影響を受ける 27000 ファミリー規格全体の段階的改訂スケジュールについて検討した。その結果、第 1 段階の改訂として 27001、27009、27017 を改訂することになり、27009 改訂検討のための PWI を設置することになった。
- 2023 年 4 月 Zoom 会議の WG 1 Plenary (全体会議) で、WG 1 Convenor より、この規格の利用が他の ISO 規格作成において必須ではないこと、ISO/CASCO により“sector-specific”の定義についての懸念が示されていること等から廃止とする提案があった。これに対して、特に反対はなかったため、廃止することになった。
- その後、2023 年 5 月 3 日に廃止された。

[\(2.1に戻る\)](#)

## [ISO/IEC 27010:2015](#)

Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications

2015年11月発行 [第2版]

セクター間及び組織間コミュニケーションのための情報セキュリティマネジメントに関する規格。情報共有コミュニティの中で情報セキュリティマネジメントを実施するためのガイダンスや、セクター間及び組織間コミュニケーションにおける情報セキュリティに関する管理策及び手引を提供する。

### ■ 改訂について：

- 2012年に第1版発行後、2014年10月にISO/IEC 27001:2013対応のための早期改訂が決定され、2015年に第2版が発行された。
- 2018年4月武漢会議にて規格発行から3年目の定期レビュー（Periodical pre-review）審議を行った。その結果、現時点では改訂は行わず現行版を維持することになった。

[\(2.1に戻る\)](#)

## ■ ISO/IEC 27011～ISO/IEC 27019

### [ISO/IEC 27011:2024](#)

Information security, cybersecurity and privacy protection Information security controls based on ISO/IEC 27002 for telecommunications organization

2024年3月発行 [第3版]

電気通信業界内の組織における、ISO/IEC 27002に基づいた情報セキュリティマネジメント導入を支援するガイドライン規格であり、SC 27とITU-Tが共同で作成したものである。

### ■ 改訂について：

- 2008年に第1版発行後、2013年10月に（ISO/IEC 27001:2013対応のための）改訂開始が決定され、2016年に第2版が発行された。
- 2019年4月テルアビブ会議にて規格発行から3年目の定期レビュー（Pre-review）審議を行った。その結果、改訂プロジェクトを開始するためのNP投票を実施することになった。なお、規格の標題を変更することになった。
- 2019年10月パリ会議にてNP投票結果を受けて改訂プロジェクトを開始することになった。
- 2024年3月に第3版が発行された。

[\(2.1に戻る\)](#)

### [ISO/IEC 27013:2021](#)

Information security, cybersecurity and privacy protection – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

2021年11月発行 [第3版] **(追補作成中)**

ISO/IEC 20000-1及びISO/IEC 27001の統合実践に関するガイダンス規格。

ISO/IEC 20000-1担当のSC 7/WG 25（IT Service management）\*と連携して作成された。

\*現在のSC 40/WG 2 Service management - Information technology

### ■ 改訂について：

- 2012年に第1版発行後、2013年10月に（ISO/IEC 27001:2013対応のための）改訂開始が決定され、2015年に第2版が発行された。

- 2018年4月武漢会議にて規格発行から3年目の定期レビュー（Pre-review）審議を行った。その結果、現時点では改訂は行わず現行版を維持することになった。一方で、ISO/IEC 20000-1の改訂版が2018年に発行される見込みのため、12カ月間のSP（Study Period）を設置し、今後改訂が必要か検討するためにISO/IEC 20000-1との違いを検証することになった。
- 2018年9-10月イビク会議にてISO/IEC 20000-1:2018が2018年9月に発行されたことに伴い、SPを終了して正式に改訂プロジェクトを開始するためのNP投票を実施することになった。
- 2019年4月テルアビブ会議にてNP投票結果を受けて改訂プロジェクトが開始され、2021年11月に第3版が発行された。
- 2022年10月Web会議にてISO/IEC 27001:2022及びISO/IEC 27002:2022との整合を図るために追補（Amendment）を作成する方向となった。

[\(2.1に戻る\)](#)

### [ISO/IEC 27014:2020](#)

Information security, cybersecurity and privacy protection –Governance of Information security  
2020年12月発行 [第2版]

情報セキュリティのガバナンスに関する規格であり、情報セキュリティガバナンスの原則及びプロセスの手引を提供する。

- 国内規格の発行：2015年7月にJIS Q 27014:2015として制定された。

#### **JIS Q 27014:2015**

情報技術—セキュリティ技術—情報セキュリティガバナンス

#### ■ 改訂について：

- 2016年4月タンパ会議にて規格発行から3年目の定期レビュー（Pre-review）審議を行った結果、改訂する方向となり、SP（Study Period）を設置して、design specification（改訂の方針等）について検討することになった。
- 2017年4月ハミルトン会議にてSPを終了し正式に改訂プロジェクトを開始するためのNP投票を実施した結果、2017年10月ベルリン会議より改訂プロジェクトが開始され、2020年に第2版が発行された（その後、2022年4月に修正版 [Corrected version] が発行された）。

[\(2.1に戻る\)](#)

### [ISO/IEC TR 27015:2012](#)

Information technology – Security techniques – Information security management guidelines for financial services

2012年11月発行（2017年7月廃止）

金融サービスのための情報セキュリティマネジメントに関する技術報告書

2016年10月アブダビ会議にて改訂について審議された結果、TC 68/SC 2（Financial Services, security）等からも改訂の支持が得られず廃止を求める国が多かったため、廃止の手続きを進め、2017年7月に廃止された。

[\(2.1に戻る\)](#)

### [ISO/IEC TR 27016:2014](#)

Information technology – Security techniques – Information security management – Organizational economics

### 2014年2月発行 (改訂検討中)

組織の情報資産の保護に対して経済学的な視点を適用し、モデル及び例示の使用を通して情報セキュリティに関する組織の経済性を適用する方法の手引を提供する技術報告書。

#### ■ 改訂について：

- 2019年4月テルアビブ会議にて規格発行から5年目の定期レビュー (Systematic-review) 審議を行った。その結果、現時点では改訂は行わず現行版を維持することになった。
- 2023年10月Web会議にて、27001改訂版の発行に伴って27016を改訂する必要性についてコメントを募集することになった。Web会議後、27016改訂のためにPWI設置をするか否かについてコメントを募集した結果、特に反対はなかったため2024年1月にPWI設置が設置された。

[\(2.1に戻る\)](#)

## ISO/IEC 27017:2015

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

### 2015年12月発行 (改訂中)

ISO/IEC 27002に基づいてクラウドサービスのための情報セキュリティ管理策の実践の規範を提供する規格。

#### ■ 国内規格の発行：2016年12月にJIS Q 27017:2016として制定された。

JIS Q 27017:2016

情報技術—セキュリティ技術—JIS Q 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範

#### ■ 改訂について：

- 2018年4月武漢会議にて規格発行から3年目の定期レビュー (Pre-review) 審議を行った。その結果、現時点では改訂は行わず現行版を維持することになった。
- 2021年4月Web会議にて、ISO/IEC 27002の改訂審議がDIS段階となったことを受けて、27002改訂の影響を受ける27000ファミリー規格全体の改訂スケジュールについて検討した。その結果、第1段階の改訂として27001、27009、27017を改訂することになり、27017改訂検討のためのPWIを設置することになった。
- 2022年10月Web会議にて、改訂方針も合意されプロジェクト開始の準備が整ったことから、改訂プロジェクトを開始することがWG1 Convenorから提案された。特に反対はなく、改訂プロジェクト開始 (36か月間) が承認された。

[\(2.1に戻る\)](#)

## ISO/IEC 27019:2017

Information technology – Security techniques – Information security controls for the energy utility industry

### 2017年10月発行 (改訂中)

エネルギー業界のための情報セキュリティ管理策。

#### ■ 改訂について：

- 2013年7月にTRとして発行後、2014年10月メキシコ会議にて1年間のSP (Study Period) での審議結果を経て、早期改訂の開始が決定された。この改訂中に、TRからISに変更し、名称も変更された。その後、2017年にISとして発行された。
- 2018年9-10月イビク会議にて附属書A (表Aの11.7) 内の表記 (should -> shall) の指摘があり、正誤表を発行することになったが、ISOの手続き上、正誤票は発行されず、2019年7月に規格本体にこの修正が加えられ

た。

- 2021年4月Web会議にて合意された、ISO/IEC 27002改訂の影響を受ける27000ファミリー規格全体の改訂スケジュールに従って、第2段階の改訂として、27000、27008、27019、27103の改訂検討を開始することが合意された。これを受けて、27019の改訂方針を検討するためにPWIが設置された。
- 2022年10月Web会議にて、改訂方針も合意されプロジェクト開始の準備が整ったことから、改訂プロジェクトを開始することがWG1 Convenorから提案された。特に反対はなく、改訂プロジェクト開始（36か月間）が承認された。

※TRからISへの変更に伴い、2017年が（ISO/IEC 27019としての）第1版となった。

[\(2.1に戻る\)](#)

## ■ ISO/IEC 27021～ISO/IEC 27029

### [ISO/IEC 27021:2017 \[追補 1\]](#)

Information technology – Security techniques – Competence requirements for information security management systems professionals

2017年10月発行 [第3版]

2021年12月追補1発行

ISMS 専門家の力量に関する要求事項について規定した規格。

#### ■ 改訂について：

- 2019年4月テルアビブ会議にて韓国から修正提案があり、追補を発行する方向となった。
- 2020年4月Web会議にて規格発行から3年目の定期レビュー（Periodical pre-review）審議を行った結果、規格の改訂は行わず現行版を維持することになった。
- 2021年11月にISO/IEC 27021:2017に対する追補1が発行された。
- 2022年10月～2023年3月間に規格発行から5年目の定期レビュー（systematic review）が実施された（レビュー結果は、現行版を維持すべき：15か国、改訂すべき：6か国、棄権：4か国）。

[\(2.1に戻る\)](#)

### [ISO/IEC TS 27022:2021](#)

Information technology – Guidance on ISMS processes

2021年3月発行 **(改訂検討中)**

ISMSのプロセスについてのガイダンスを提供する規格。

（策定中に、規格のタイプがIS（International Standard）からTS（Technical Specification）へ変更された。）

#### ■ 改訂について：

- 関連する改訂：2023年10月Web会議にて、ISO/IEC 27001・27002改訂を受けた27000ファミリー規格全体の段階的改訂スケジュールの第4段階として、27022のPWIを設置し、改訂検討を開始した。

[\(2.1に戻る\)](#)

### [ISO/IEC TR 27023:2015](#)

Information technology – Security techniques – Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

2015年7月発行

ISO/IEC 27001 及び ISO/IEC 27002 新旧対応表をまとめた技術報告書。

2013 年 10 月に発行された ISO/IEC JTC 1/SC 27 N13143「JTC 1/SC 27/SD3 – Mapping Old-New Editions of ISO/IEC 27001 and ISO/IEC 27002」の内容をそのまま取り込んだものである。SD3 (Standing Document 3) は ISO の内部文書であるため、より正式な ISO 文書である TR として発行された。

■ 改訂について：

- 2014 年 7 月～10 月に早期発行のための DTR 投票が行われ、可決された。これを受けた手続を経て、2015 年に発行された。
- 2020 年 4 月 Web 会議にて規格発行から 5 年目の定期レビュー (Systematic review) 審議を行った結果、現時点では改訂は行わず現行版を維持することになった (ISO/IEC 27001、ISO/IEC 27002 の改訂後に改訂予定)。
- 2022 年 10 月 Web 会議にて廃止する方向で手続を進めることになった。その後、2022 年 10 月 26 日に廃止された。

[\(2.1に戻る\)](#)

## [ISO/IEC TR 27024](#)

ISO/IEC 27001 family of standards references list – Use of ISO/IEC 27001 family of standards in Governmental/Regulatory requirements

(作成中)

各国の政府及び規制上の要求事項における ISO/IEC 27001 ファミリー規格の使用に関する事例をまとめた技術報告書 (英国、ドイツ、オーストラリアなどの事例を掲載している)。

- 2024 年 3 月ロンドン会議にて、標題を以下に変更することになった。  
Reference list of the use of ISO/IEC 27000 series of standards in Government /Regulatory requirements

[\(2.1に戻る\)](#)

## [ISO/IEC 27028](#)

Information security, cyber security and privacy protection – Guidance on ISO/IEC 27002 attributes

(作成中)

ISO/IEC 27002:2022 で新たに採り入れられた属性 (Attribute) の利用及び作成に関する手引

[\(2.1に戻る\)](#)

## [ISO/IEC 27029](#)

Information security, cyber security and privacy protection – ISO/IEC 27002 relationship with ISO and IEC standards

(作成検討中)

ISO/IEC 27002 の管理策及び手引を参照している ISO/IEC (及び ISO) 規格の一覧を提供する規格

■ 発行について：

- 2023 年 4 月 Zoom 会議の WG 1 Plenary (全体会議) にて、WG 1 Convenor (議長) より、ISO 事務局の介入によって (無料公開とするために) 27029 案をもとに次の WG 1 SD (Standing Document : WG1 に関連する様々な情報を提供する文書) \*を作成し、本プロジェクトをキャンセルするという報告があった。特に反対はなく、承認

された。以下のタイトルで発行予定

WG1/SD 10 ISO/IEC 27001 and ISO/IEC 27002 relationships with other ISO and IEC standards

\*次の Web サイトで公開予定：

<https://committee.iso.org/sites/jtc1sc27/home/wg2.html>

[\(2.1に戻る\)](#)

## ■ ISO/IEC TS 27100～ISO/IEC TS 27110

### [ISO/IEC TS 27100:2020](#)

Information technology – Cybersecurity – Overview and Concepts

2020 年 12 月発行

サイバーセキュリティの概要（用語の定義を含む）を提供する規格。

[\(2.1に戻る\)](#)

### [ISO/IEC 27102:2019](#)

Information security management — Guidelines for cyber-insurance

2019 年 8 月発行

組織の情報セキュリティリスクマネジメントの中で、サイバーインシデントの影響を管理するためのリスク対応の選択肢の 1 つとしてサイバー保険を採用する場合のガイドラインを提供する規格。

[\(2.1に戻る\)](#)

### [ISO/IEC TR 27103:2018](#)

Information technology – Security techniques – Cybersecurity and ISO and IEC Standards

2018 年 2 月発行 **(改訂中)**

サイバーセキュリティフレームワークにおいて、既存の ISO 及び IEC 規格を活用する方法についての手引を提供する規格。

サイバーセキュリティのためのフレームワークの背景と概要について説明し、ISO/IEC 27000 ファミリーをはじめとする既存の ISO 及び IEC 規格とのマッピングを提供している。

#### ■ 改訂について：

- 2021 年 4 月 Web 会議にて合意された、ISO/IEC 27002 改訂の影響を受ける 27000 ファミリー規格全体の改訂スケジュールに従って、第 2 段階の改訂として、27000、27008、27019、27103 の改訂検討を開始することが合意された。これを受けて、27103 の改訂方針を検討するために PWI が設置された。
- 2023 年 4 月 Web 会議にて、改訂方針も合意されプロジェクト開始の準備が整ったことから、改訂プロジェクトを開始することが WG1 Convenor から提案された。特に反対はなく、改訂プロジェクト開始（18 か月間）が承認された。

[\(2.1に戻る\)](#)

### [ISO/IEC TR 27109](#)

Information technology, cybersecurity and privacy protection – cybersecurity education and training

**(作成中)**

サイバーセキュリティに関する教育・訓練等の情報を提供する規格

[\(2.1に戻る\)](#)

### **ISO/IEC TS 27110:2021**

Information technology, cybersecurity and privacy protection – Cybersecurity framework development guidelines

2021年2月発行

サイバーセキュリティの枠組みを構築するためのガイドラインを提供する規格。

(発行準備段階で、規格番号が 27101 から 27110 へ変更された。)

[\(2.1に戻る\)](#)

以上

参考：ISO/IEC JTC 1 における規格作成の段階

\*()は、省略可能な場合がある。

国際規格(IS)	(PWI)* → NP → WD → CD → DIS → FDIS → IS		
追補 (Amendment)	(PWI)* → (NP)* → WD → CDAM → DAM → FDAM → Amendment		
技術仕様書(TS)	(PWI)* → NP → WD → DTS → TS		
技術報告書(TR)	(PWI)* → DTR → TR		
<b>PWI</b>	Preliminary Work Item	<b>CDAM</b>	Committee Draft Amendment
<b>NP</b>	New work item Proposal	<b>DAM</b>	Draft Amendment
<b>AWI</b>	Approved work Item	<b>FDAM</b>	Final Draft Amendment
<b>WD</b>	Working Draft	<b>DTS</b>	Draft Technical Specification
<b>CD</b>	Committee Draft	<b>TS</b>	Technical Specification
<b>DIS</b>	Draft International Standard	<b>DTR</b>	Proposed Draft Technical Report
<b>FDIS</b>	Final Draft for International standard	<b>TR</b>	Technical Report
<b>IS</b>	International Standard		

※PWI は、ISO 規格作成/改訂手続前に設置される予備段階で、通常、NPに進めるには時期尚早な事項等を審議するために設置される。WG1 では、特に規格の作成/改訂に先立って、その方針(design specification)等を審議するために設置されている。

#### 追補 (Amendment)

既存の IS に対して、変更及び/又は追加を行うものであり、部分的な改訂とみなされる。

#### 技術仕様書 (TS : Technical Specification)

まだ開発の途上にある等の理由から、将来的に国際規格として合意が得られる可能性があるが現時点では直ちに是得られない場合に発行することができる文書。発行後 3 年以内に見直しが行われる。

#### 技術報告書 (TR : Technical Report)

IS 又は TS として通常発行されるものとは異なる種類の収集データを含む文書。規定を示すような内容は含まない。

ISO/IEC における規格作成に関しては、ISO/IEC Directives で規定されている。詳細は、以下を参照。

- **ISO/IEC Directives, Part 1** —Consolidated ISO Supplement —Procedure for the technical work — Procedures specific to ISO — (ISO/IEC 専門業務用指針第 1 部—統合版 ISO 補足指針—ISO 専用手順—)
- **ISO/IEC Directives, Part 2** —Principles and rules for the structure and drafting of ISO and IEC documents (ISO/IEC 専門業務用指針第 2 部 ISO 及び IEC 文書の構成及び作成に関する原則と規則)
- **JTC 1 Supplement** (JTC 1 補足指針)

<https://www.iso.org/directives-and-policies.html>

[\(2.1 に戻る\)](#)