

# ISO/IEC 27000 ファミリーについて

## ～ISO/IEC JTC 1/SC 27/WG 1 における検討状況～

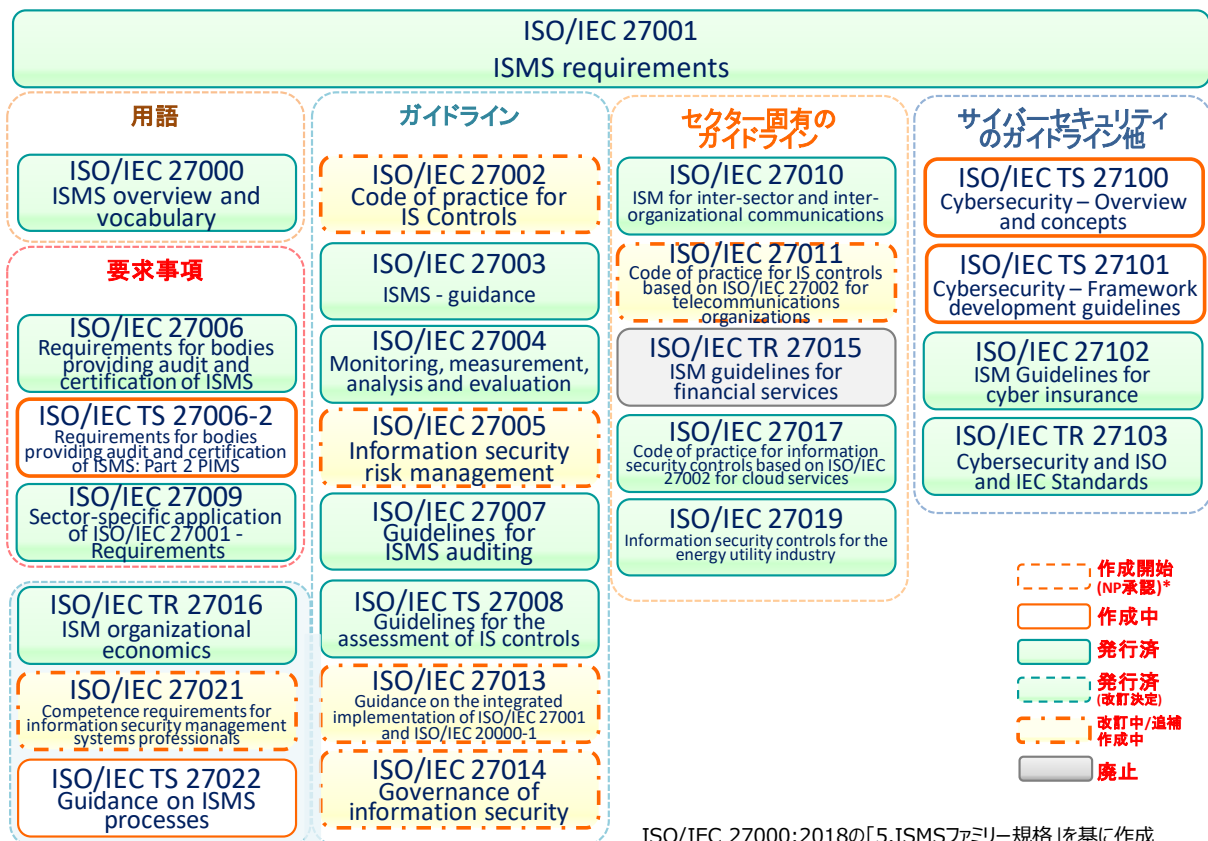
2020 年 11 月 10 日

### 1. ISO/IEC 27000 ファミリーとは

ISO/IEC 27000 ファミリーは、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）の設置する合同専門委員会 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。



\*作成開始（NP 承認）： ISO 規格の作成可否について実施される NP（New work item Proposal）投票の結果、新規作成が決定された規格です。

（「作成中」は NP 承認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、12 ページをご参照下さい。

※ ISO/IEC TS 27006-2（27558 から番号変更）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 と合同で策定することになっており、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 27032:2012**

Information technology – Security techniques – Guidelines for cybersecurity

**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. 個々の規格の概要

### **ISO/IEC 27000:2018**

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

2018年2月発行 [第5版]

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 27000:2019 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。

※ 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る。

### **ISO/IEC 27001:2013**

Information technology – Security techniques – Information security management systems – Requirements

2013年10月発行 [第2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：2014年3月に JIS Q 27001:2014 (JIS Q 27001:2006 の改正版) として制定された。

#### **JIS Q 27001:2014**

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—要求事項

■ 正誤票の発行：2014年9月に ISO より正誤票が発行された (JIS 正誤票は 2014年11月に発行)。その後、2015年11月にも ISO より正誤票が発行された (JIS 正誤票は 2015年12月に発行)。

■ 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 専門業務用指針 第1部 統合版 ISO 補足指針」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。

### **ISO/IEC 27002:2013**

Information technology – Security techniques – Code of practice for information security controls

2013 年 10 月発行 [第 2 版] (改訂中)

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：2014 年 9 月に ISO より正誤票が発行された (JIS 正誤票は 2014 年 11 月に発行)。  
その後、2015 年 11 月にも正誤票が発行された (JIS Q 27002:2014 では対応済みのため、対応する JIS 規格の正誤票はない)。

■ 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) \*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

\*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 専門業務用指針 (ISO/IEC Directives) に沿って SP に代わり PWI\*\*という呼称を使用することになった。

\*\*PWI (Preliminary Work Item)

ISO における規格作成の段階のうち、提案段階 (NP 審議) の 1 つ前の段階である予備段階で検討するために登録される審議案件。NP に進めるには時期尚早な事項や、規格の追補・改訂プロジェクト開始前の予備的な審議事項 (例：PWI 27006 改訂審議) などが、PWI として登録される。

### **ISO/IEC 27003:2017**

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

2017 年 4 月発行 [第 2 版]

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。

**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]

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。

**ISO/IEC 27005:2018**

Information technology – Security techniques – Information security risk management

2018年7月発行 [第3版] **(改訂中)**

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 and opportunities

### **ISO/IEC 27006:2015 [追補 1]**

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

2015 年 10 月発行 [第 3 版]

2020 年 3 月追補 1 発行

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 月イェピク会議において、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性が生じたことから、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。

- ISO/IEC 27006 の規格群

#### **ISO/IEC TS 27006-2（作成中）**

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

ISO/IEC 27701 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。

2020 年 4 月 Web 会議にて開催された WG 1・WG 5 合同会議において新規プロジェクトとして承認され、規格を作成することになった。その際に、規格のタイプを 3 年間かけて作成する IS（International



Standard) から比較的早期に発行可能な TS (Technical Specification)\*へと変更し、2020 年中の発行を目指すことになった。また、規格番号については、ISO/CASCO の承認を経て 27558 から 27006-2 へ変更することになった。

2020 年 9 月 Web 会議にて開催された WG 1・WG 5 合同会議において、27006-2 への規格番号の変更に伴い、ISO/IEC 専門業務用指針 (ISO/IEC Directives) に従って規格名称が ISO/IEC 27006 に沿って変更された。

\* TS (Technical Specification) : 技術仕様書

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は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 ([ISO/IEC Directives Part 1 and Consolidated ISO Supplement](#) [ISO/IEC 専門業務用指針第 1 部及び統合版 ISO 補足指針] 参照)。

### **ISO/IEC 27007:2020**

Information technology – Security techniques – 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 月イェビク会議にて、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。

### **ISO/IEC TS 27008:2019**

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

2019 年 1 月発行

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。

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

### **ISO/IEC 27009:2020**

Information technology – Security techniques – 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。

### **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。

### **ISO/IEC 27011:2016**

Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

2016年12月発行 [第2版] **(改訂中)**

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。

### **ISO/IEC 27013:2015**

Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

2015年11月発行 [第2版] **(改訂中)**

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 Maintenance and development of ISO/IEC 20000 - Information technology - Service management

■ 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月イエビク会議にて 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を開始することになった。

### **ISO/IEC 27014:2013**

Information technology – Security techniques –Governance of Information security

2013年4月発行 (改訂中)

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た。

### **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。

### **ISO/IEC TR 27016:2014**

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

2014年2月発行

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。

### **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

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。

### **ISO/IEC 27019:2017**

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

2017年10月発行

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月イェ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。

※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。

### **ISO/IEC 27021:2017**

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

2017年10月発行（追補作成中）

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。

### **ISO/IEC TS 27022**（作成中）

Information technology – Security techniques – Guidance on ISMS processes

ISMS のプロセスについてのガイダンスを提供する規格。

2019年4月テルアビブ会議にて新規プロジェクトとして承認され、規格を作成することになった。

2020年4月 Web 会議にて、規格のタイプを IS(International Standard)から TS(Technical Specification)に変更することになった。

### **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)。

### **ISO/IEC TS 27100 (作成中)**

Information technology – Cybersecurity – Overview and Concepts

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。

2018年9-10月イエビク会議にて新規プロジェクトとして承認され、規格を作成することになった。

### **ISO/IEC TS 27101\* (作成中)**

Information technology – Cybersecurity – Framework development guidelines

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。

2018年4月武漢会議にて新規プロジェクトとして承認され、規格を作成することになった。

\*規格番号を 27110 へ変更予定。

### **ISO/IEC 27102:2019**

Information technology – Security techniques – 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。

### **ISO/IEC TR 27103:2018**

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

2018年2月発行

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。

2018年9-10月イエビク会議にて、サイバーセキュリティフレームワークと既存規格の関係を示す有益な文書であり (標準化作業での活用を前提とした) 無償配布のための手続を進めることが決定された。

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

WG 1 会議は、2020 年 9 月 12 日～16 日に Web 会議で開催されました。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。

#### 3-1 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：IS (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	規格策定の段階*	
		2020 年 9 月会議 (今回)	2021 年 4 月会議 (次回予定)
ISO/IEC 27000	ISMS 概要及び用語	IS[第 5 版]	IS[第 5 版]
ISO/IEC 27001	ISMS 要求事項	IS[第 2 版]	IS[第 2 版]
ISO/IEC 27002	情報セキュリティ管理策の実践のための規範	IS[第 2 版] (2nd CD)	IS[第 2 版] (DIS)
ISO/IEC 27003	ISMS の手引	IS[第 2 版]	IS[第 2 版]
ISO/IEC 27004	ISM – 監視、測定、分析及び評価の手引	IS[第 2 版] (正誤票発行)	IS[第 2 版] (正誤票発行)
ISO/IEC 27005	情報セキュリティリスクマネジメントに関する指針	IS[第 3 版] (CD)	IS[第 3 版] (2nd CD)
ISO/IEC 27006	ISMS 認証機関に対する要求事項	IS[第 3 版]<追補 1>	IS[第 3 版]<追補 1> (PWI)
ISO/IEC TS 27006-2	ISO/IEC 27701 認証機関に対する要求事項	DTS	TS
ISO/IEC 27007	ISMS 監査の指針	IS[第 3 版] (IS)	IS[第 3 版] (IS)
ISO/IEC TS 27008	IS 管理策の評価(assessment)のための指針	TS	TS
ISO/IEC 27009	セクター規格への 27001 適用に関する要求事項	IS[第 2 版]	IS[第 2 版]
ISO/IEC 27010	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[第 2 版]	IS[第 2 版]
ISO/IEC 27011	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の実践の規範	IS[第 2 版] (2nd WD)	IS[第 2 版] (3rd WD)
ISO/IEC 27013	ISO/IEC 27001 と ISO/IEC 20000-1 との統合導入についての手引	IS[第 2 版] (CD)	IS[第 2 版] (DIS)
ISO/IEC 27014	情報セキュリティのガバナンス	IS (FDIS)	IS (IS[第 2 版])
ISO/IEC TR 27015	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)
ISO/IEC TR 27016	ISM – 組織の経済的側面(Organizational economics)	TR	TR
ISO/IEC 27017	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	IS	IS
ISO/IEC 27019	エネルギー業界のための情報セキュリティ管理策	IS	IS
ISO/IEC 27021	ISMS 専門家の力量に関する要求事項	IS	IS (DAM)
ISO/IEC TS 27022	ISMS プロセスに関する手引	2nd CD(TS に変更)	TS
ISO/IEC TR 27023	ISO/IEC 27001 及び ISO/IEC 27002 改訂版のマッピング	TR	TR
ISO/IEC TS 27100	サイバーセキュリティの概要及びコンセプト	DTS	TS
ISO/IEC TS 27101	サイバーセキュリティフレームワーク策定の指針	TS 発行準備中 (規格番号を 27110 へ変更予定)	TS
ISO/IEC 27102	サイバー保険のための ISM 指針	IS	IS
ISO/IEC TR 27103	サイバーセキュリティと ISO 及び IEC 規格	TR	TR

ISO 規格作成の段階は、次のとおり

NP → WD → CD → DIS → FDIS → IS (発行済)

TR/TS 規格作成の段階は、次のとおり。

TR: DTR → TR TS: NP → WD → DTS → TS

NP: New work item Proposal (NWIP)

WD: Working Draft

CD: Committee Draft

DIS: Draft International Standard

FDIS: Final Draft for International standard

IS: International Standard

TR: Technical Report (技術報告書)

TS: Technical Specification (技術仕様)

DTR/DTS: Proposed Draft Technical Report/ Specification

※PWI: Preliminary Work Item のことであり、上記表内の PWI では改訂等について予備的な審議が実施されます。

### 3-2 主なプロジェクトの進捗状況

#### 27002 (Information security controls)

今回の会議に先立って 2nd CD が発行されており、この 2nd CD に対して約 1800 件のコメントが寄せられた。会議では、事前に配付した文書で議論が必要と示されたコメントについて、9 月 12 日～14 日の 4 日間にわたって審議したがコメント処理が終了しなかったため、追加の会議を 10 月 12 日～14 日に実施し、残りのコメントの審議を行い、全てのコメント処理を終了した。今回の審議の結果、DIS を発行することになった。

#### 27005 (Information security risk management)

今回の会議に先立って CD が発行されており、これらのコメントについて審議した結果、採用されたコメントのなかで具体的な修正までの議論に至らなかったものや、内容の変更につながるものが多かったことから、参加者の多くから次回は 2nd CD とすることが提案された。今回の審議の結果、2nd CD を発行することになった。

#### 27006 (Requirements for bodies providing audit and certification of ISMS)

■ISO/IEC 27006 の規格群として、WG 1・WG 5 合同会議において次の規格の作成について審議された。

#### TS 27006-2 (Requirements for bodies providing audit and certification of PIMS according to ISO/IEC 27701 in combination with ISO/IEC 27001)

今回の会議に先立って発行された DTS 投票結果は、賛成 24 か国、棄権 21 か国、反対 2 か国（イタリア、日本）で、コメントは約 120 件だった。会議では、特にコメントの多かった要員の力量要求事項等について審議された。また、最小審査工数は重要なことから、会議に先立って DTS 投票とは別にコメント募集（CfC：Call for Contribution）を実施した。会議では、この CfC に寄せられた各国コメントを基に議論され、最終的に多数意見に基づいて合意した。

なお、規格番号が 27558 から 27006-2 へ変更されたことに伴い、ISO/IEC 専門業務用指針（ISO/IEC Directives）に従って規格名称を以下に変更することになった。

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

今回の審議の結果、TS を発行することになった。

また、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 を新たに設置することになった。

### 3-3 その他

昨今のサイバーセキュリティに関する動向を踏まえて各国から様々な提案がなされたことを受けて、現在、以下の規格の策定が進められています。

- ・サイバーセキュリティ – 概要及びコンセプト(TS:技術仕様書)  
名称: ISO/IEC TS 27100 Cybersecurity – Overview and concepts  
今回の Zoom 会議において DTS が審議された結果、TS を発行することになった。  
サイバーセキュリティの概要や関連する定義等を規定する規格。
- ・サイバーセキュリティフレームワークを策定するためのガイドライン(TS:技術仕様書)  
名称: ISO/IEC TS 27101\* Cybersecurity – Framework development guidelines  
2019 年 10 月開催のバリ会議において PDTS が審議された結果、TS を発行することになった。  
米国から提案された文書をもとにしている。  
\*規格番号を 27110 へ変更予定。

発行された規格:

- ・サイバーセキュリティフレームワークと ISO・IEC 規格の関連を示す技術報告書  
名称: ISO/IEC TR 27103 Cybersecurity and ISO and IEC Standards  
2018 年 2 月発行。
- ・サイバー保険に関するガイドライン規格  
名称: ISO/IEC 27102 Information security management guidelines for cyber insurance  
2019 年 8 月発行。

以上