ISO/IEC 27000ファミリー規格の最新動向

2019-12-04

ISO/IEC JTC1/SC27 WG1小委員会 主査
（株式会社日立製作所）
相羽 律子

目次

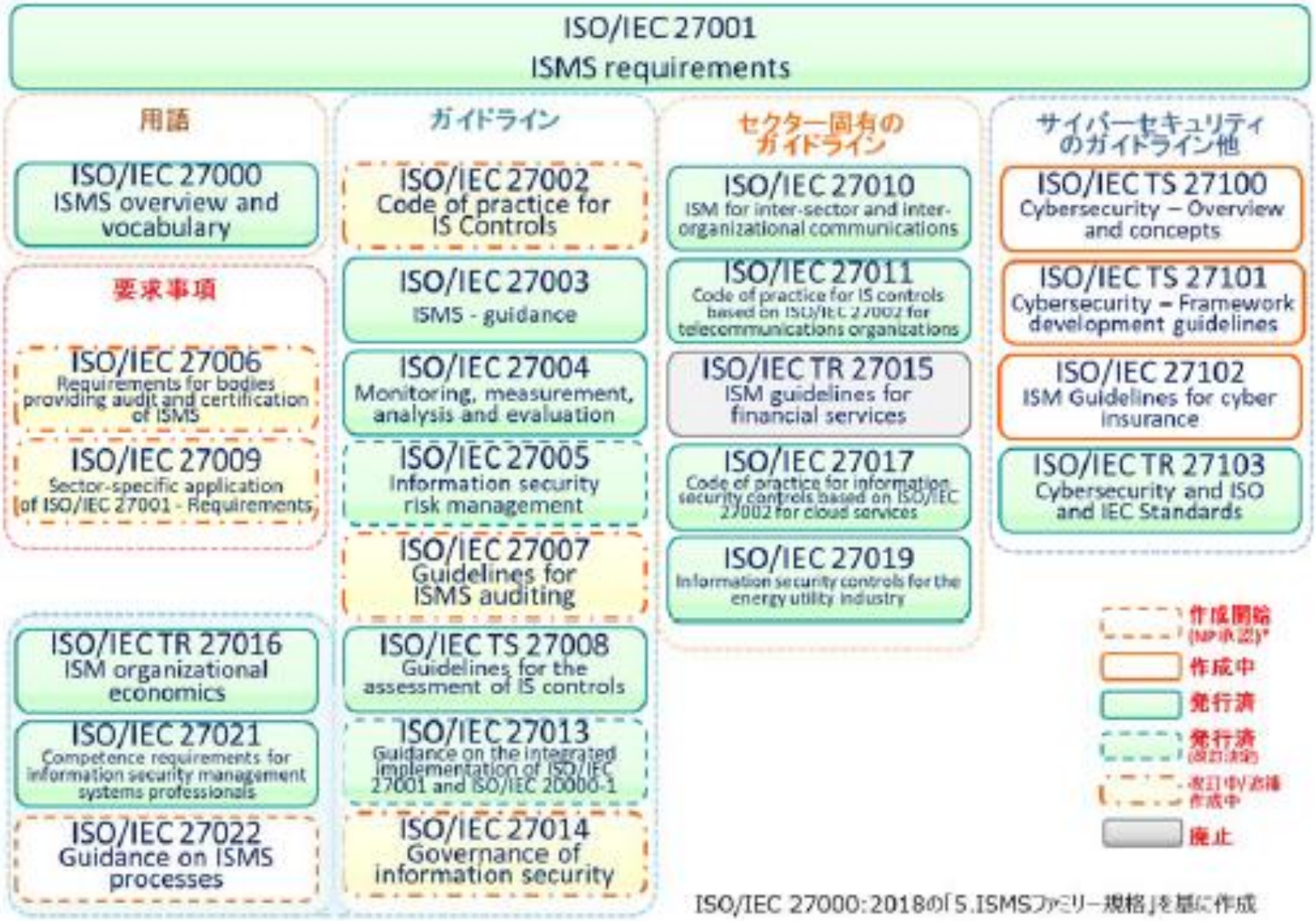
- ISO/IEC 27000ファミリー規格とは
- ISO/IEC JTC1/SC27/WG1における規格化の概況
  - 2019年発行の規格
  - ISO/IEC 27001及びISO/IEC 27002の改訂状況
  - その他の状況

ISO/IEC 27000ファミリー規格とは

ISO/IEC 27000ファミリー規格とは

- **情報セキュリティマネジメントシステム（Information Security Management System: ISMS）に関する国際規格群**
- **ISMS要求事項を規定する規格を軸に、次で構成される**
  - その他の要求事項を規定する規格
  - 用語を規定する規格
  - ISMSの実施を支援する各種ガイドライン規格
  - セクター固有のガイドライン規格
  - サイバーセキュリティに関する規格 他
- **ISO/IEC JTC1/SC27の主にWG1で作成されている一部は、WG4及びWG5でも作成されている**

ISO/IEC 27000ファミリー規格とは



出典：ISO/IEC 27000ファミリーについて（JIPDEC）
https://www.jipdec.or.jp/smpo/u71kba000000jjgv-att/27000family_20190520.pdf

標準化組織（ISO/IEC JTC1/SC27）

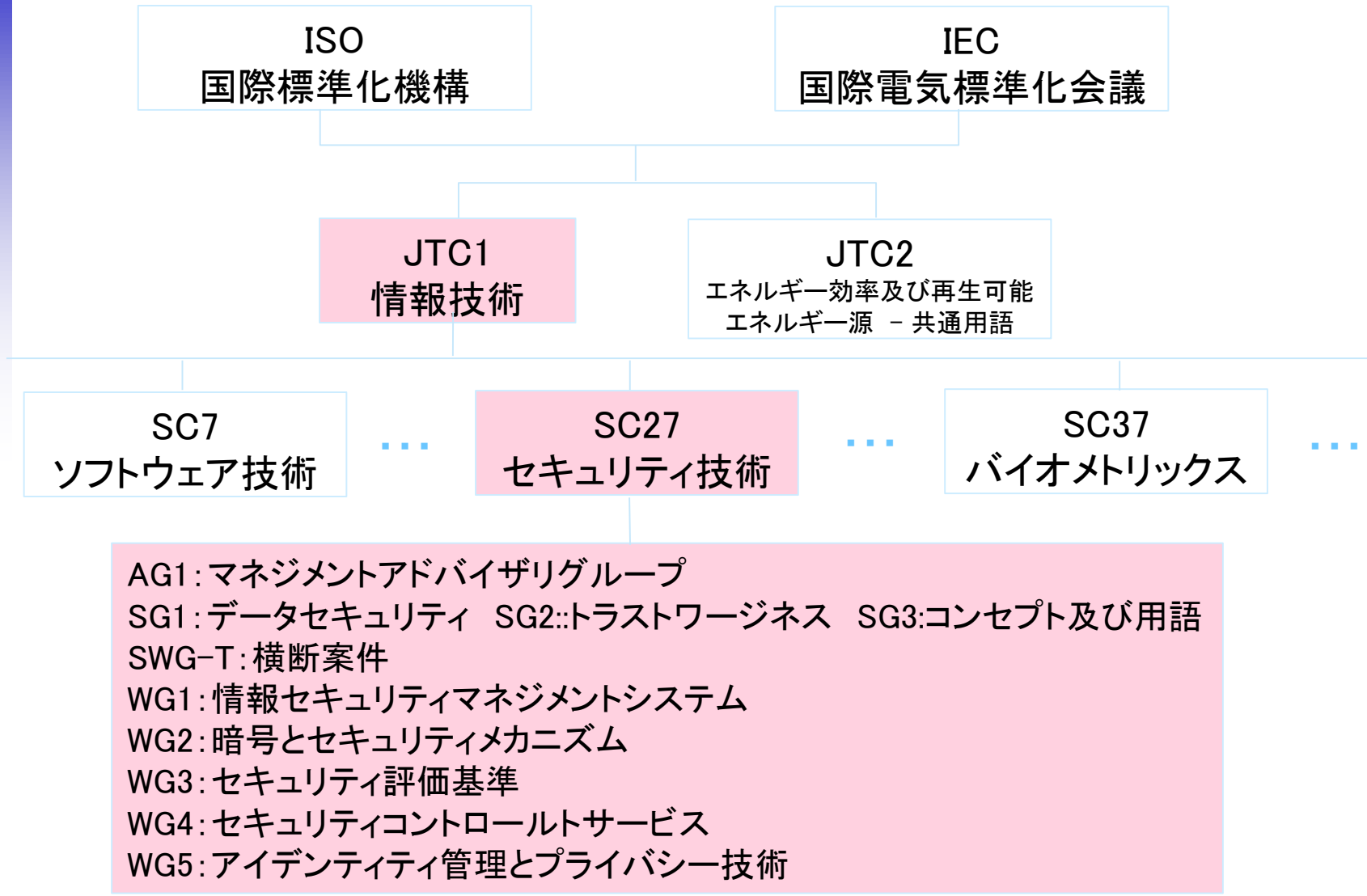


図1　ISO/IEC JTC1/SC27の組織構造

ISO/IEC JTC1/SC27

- **タイトル: IT Security techniques**
  → 変更 Information security, cybersecurity and privacy protection

- **発行済み: 188規格**
- **開発中: 73規格**
- **メンバー国: 48カ国**
- **オブザーバーメンバー国: 30カ国**

（上記数字は全て2019-11-11現在）

- **会合**
  - ISO/IEC JTC1/SC27会合: 年1回（2日間）、春（4～5月）に開催
  - ISO/IEC JTC1/SC27/WGs会合: 年2回（各5日間）、春（4～5月）と秋（10～11月）に開催
  - 2019年は、春は4月にテルアビブ（イスラエル）、秋は10月にパリ（フランス）で開催
  - 開発中規格のドラフト審議、新規格の提案などについて検討

WG1

- **タイトル: Information Security Management System**
- **活動スコープ**
  - 情報セキュリティマネジメントシステム（ISMS）に関する規格の開発
  - マネジメントシステムに関する規格の開発
  - ISO/IEC 27001の要求事項を軸に、この実装に関する規格、又は適合を支援する規格を開発するセキュリティ要求事項を捉えるための手法を示す規格の開発

WG1における規格化：2019-10, パリ会合

第61回 JTC1/SC27/WG1会合

- 開催日時: 10月14日（月）～18日（金）
- 開催場所: Espace Vinci、パリ、フランス
- 出席者
  - コンビナ： Edward Humphreys 英国
  - 副コンビナ： Pablo Corona メキシコ
  - 参加国 29ヶ国：

    アルゼンチン、オーストリア、オーストラリア、ベルギー、カナダ、スイス、中国、ドイツ、デンマーク、スペイン、フィンランド、フランス、英国、アイルランド、インド、イタリア、日本、韓国、ルクセンブルグ、メキシコ、マレーシア、ノルウェー、ニュージーランド、ポーランド、スウェーデン、シンガポール、UAE、米国、南アフリカ
  - 参加リエゾン 4組織：

    Global Platform、ISACA、ISF、ISC2
  - 参加エキスパート　164名（内、日本の出席者10名）

ISO/IEC JTC1/SC27/WG1における規格化の概況

– 2019年に発行の規格

ISO/IEC TS 27008:2019

- Information technology － Security techniques － Guidelines for the assessment of information security controls
  - 2019年1月発行
  - 初版
  - ISMSによって決定された情報セキュリティ管理策の評価に関するガイドライン
  - 情報セキュリティ管理策の実施及び運用状況のレビュー及び評価方法について提供中

ISO/IEC 27102:2019

- Information security management — Guidelines for cyber-insurance

  - 2019年8月発行
  - 初版
  - サイバーインシデントによる影響をマネージするために、組織がリスク対応オプションとしてサイバー保険の購入を検討する際のガイドラインを提供
  - ガイドのユーザーとしては、保険サービス提供者(insurer)、及び被保険者(insured)、すなわち保険サービス導入を検討しているISMS導入組織を対象としている。
  - 日本では、損保協会とタスクフォースを設立し、保険業界におけるサイバー保険の専門家の知見を日本のコメントに反映した

ISO/IEC 27701:2019（WG5で作成）

- Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines
  - 2019年8月発行
  - 初版
  - WG5で作成された規格であるが、ISO/IEC 27009（セクター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）に基づき作成されたセクター規格のひとつ
  - プライバシー情報マネジメントのために、ISO/IEC 27001（要求事項）及びISO/IEC 27002（管理策のガイドライン）を拡張し、1つの規格として示す構成
  - プライバシー情報マネジメントについては、既発行のISO/IEC 29100（JIS X 9250）に基づいた内容

ご参考: ISO/IEC 27701:2019の目次

https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en

ご参考: ISO/IEC 27701:2019の目次（つづき）

7 Additional ISO/IEC 27002 guidance for PII controllers
7.1 General 7.2 Conditions for collection and processing
7.3 Obligations to PII principals 7.4 Privacy by design and privacy by default
7.5 PII sharing, transfer, and disclosure
8 Additional ISO/IEC 27002 guidance for PII processors
8.1 General 8.2 Conditions for collection and processing
8.3 Obligations to PII principals 8.4 Privacy by design and privacy by default
8.5 PII sharing, transfer, and disclosure

Annex A PIMS-specific reference control objectives and controls (PII Controllers)
Annex B PIMS-specific reference control objectives and controls (PII Processors)
Annex C Mapping to ISO/IEC 29100
Annex D Mapping to the General Data Protection Regulation
Annex E Mapping to ISO/IEC 27018 and ISO/IEC 29151
Annex F How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002

https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en

ISO/IEC JTC1/SC27/WG1における規格化の概況

－ ISO/IEC 27001及びISO/IEC 27002の改訂状況

ISO/IEC 27001:2013の改訂

- 昨年の定期レビュー結果は**Confirm**

  → 理由は、マネジメントシステム規格の共通フォーマットの改訂版が2021年に発行見込みのため

- 一方、WG1内に、ISO/IEC 27001の改訂について検討するアドバイザリーグループを設置

  → ISO/IEC 27002の改訂、共通フォーマットの改訂の状況を受け、ISO/IEC 27001を改訂する時期や目的を適切に設定することを目的に議論

  → **ISO/IEC 27001改訂は行わないことを決定**

  - Annex Aのみ入替える検討もしたが、ISO/IEC 27001の改訂は認証の更新などマーケットに大きな影響を与えるため、望ましくないと判断

  - 改訂版では新旧管理策の対応が示される予定のため

ISO/IEC 27001:2013の改訂検討

参考：検討した改訂オプション

Option A: Annex AだけをISO/IEC 27002にあわせて改訂する

Option B: Option Aに加えて、Clause 3に用語及び定義を戻し入れる

Option C: Option Bに加えて、Annex Aの参照について取り決めた6.1.3 の記述の改訂も行う

Option D: 何もしない

→ 現時点では何もしないとの結論となったが、
ISO/IEC 27002や共通フォーマットの改訂の状況は継続的に注視。然るべきタイミングでISO/IEC 27001の改訂の必要性については再議論、投票・決定する

ISO/IEC 27002:2013の改訂検討

- 改訂作業を継続中
  - 2018年4月より改訂作業を開始
  - エキスパートレベルでのドラフト作成段階を終え、ドラフトに対し国単位で賛成/反対/棄権の態度を投票、併せて提出されたコメントを処理するCDステージに進んだ
- 発行は2022年春の予定
- 検討の概況
  - 改訂版の管理策の構成は、ほぼ固まった状況
  - 旧版の管理策と比較して、構成はだいぶ変わったが、対応状況を見ると、大きく追加されたり削除されたりしたものは無い状況。管理策の新旧対応は、Annex Bとして提供される予定
  - 管理策は、organization, people, physical, technicalに分類される
  - 管理策に対し、attributesの概念を追加する

パリ会合結果まとめ

- ISO/IEC 27001は、MS共通フォーマットの改訂（2021年見込み）やISO/IEC 27002の改訂にどう対応するかを検討

  → 改訂しない結論となった

- ISO/IEC 27002改訂作業は、エキスパートレベルでのドラフト作成段階を終え、国単位で投票し、コメント処理するCDステージに進んだ

  → 次回会合（4月のロシア会合）に向けては、国(National body)として意見をまとめて提出する

ISO/IEC JTC1/SC27/WG1における規格化の概況

– その他の状況

ISO/IEC TS 27100の開発

ISO/IEC TS 27100, Information technology – Cybersecurity – Overview and concepts

- サイバーセキュリティの概要及び概念を記述し、用語定義を提供する技術文書
- WG4とのジョイントプロジェクトは解消、WG1単独のプロジェクトとして推進中
- 作業状況
  - WGエキスパートレベルでのドラフト作成を継続
  - 文書の発行は2021年末の見込み。
  - Cyber spaceの定義はISO/IEC 27102の定義を参照する、Digital riskの用語は用いず、cyber riskに統一するなど、いくつか合意事項はあるが、まだ多くは検討段階

ISO/IEC TS 27101の開発

ISO/IEC TS 27101, Information technology – Cybersecurity – Framework development guidelines

- サイバーセキュリティのフレームワーク(CSF)を策定するための指針を示す文書
- 米国NIST文書 Framework for Improving Critical Infrastructure Cybersecurity (以降NIST文書と記す)の構造(Identify, Protect, Detect, Respond, Recover)を用いて構成されている
- 想定利用者:CSFを作る組織。政府機関、業界団体等
- 作業状況:
  - CSFの実装に関する記述を対象外とすることの合意により、文書がシンプル化。プロジェクトが前進した。
  - エキスパートレベルでのドラフト作成段階を終え、国単位で投票し、コメント処理するCDステージに進んだ。2020年中の発行見込み。

ISO/IEC TR 27103の無償配布

ISO/IEC TR 27103:2018 Information technology -- Security techniques -- Cybersecurity and ISO and IEC Standards

- 組織がサイバーセキュリティ・フレームワークを持つことの重要性を示し、既存規格をサイバーセキュリティ・フレームワークにおいて、いかに活用するかについて示した文書
- NIST文書と既存のISO及びIEC規格（ISO/IEC 27002:2013他）との対応を説明している
- 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知る上で有益な文書であるため、（標準化作業における活用を前提に）無償配布

ISO/IEC TR 27103の無償配布

- 内容例

  Identifyファンクションのカテゴリーの説明及び対応する既存規格

Table 1 — Identify categories

Category	Description	References
Business environment	The organization's objectives, stakeholders, and activities are understood and used to inform roles, responsibilities and risk management decisions. Comprehensive security measures are necessary covering the company itself, its group companies, business partners of its supply chain and IT system control outsourcing companies.	ISO/IEC 27001:2013, Clause 4 ISO/IEC 27001: 2013, Clause 5 ISO/IEC 27036 (all parts) ISO/IEC 20243:2015, Clause 4 IEC 62443-2-1:2010, 4.2.1 ISO 31000:2009, 5.3
Risk assessment	The organization understands the risks to the organization's operations and assets. The management are required to drive cybersecurity risk measures considering any possible risk while in proceeding with the utilization of IT.	ISO/IEC 27001:2013, Clause 6 ISO/IEC 27014 ISO/IEC 20243:2015, Clause 4 IEC 62443-2-1:2010, 4.2 ISO 31000 ISO/IEC 38505
Risk management strategy	An organization's approach, the management components and resources to be applied to the	ISO/IEC 27001:2013, 9.3 ISO/IEC 20243:2015, Clause 4

ISO/IEC 27005の改訂

- Information technology -- Security techniques -- Information security risk management
  - 2018年に改訂3版を発行。これは、ISO/IEC 27001:2013に合わせて最低限の編集上の修正を行ったのみで、改訂2版と内容的な差は、ほぼ無い。
  - ISO/IEC 27001:2013に本質的に適合した版作成のための改訂プロジェクトを2019年4月に開始。
  - 作業状況：
    - 現在、エキスパートレベルでコンテンツやコメントを持ち寄り、ドラフトを作成中。
    - 構成もまだ固まっておらず、内容も不確定な状況。

ISO/IEC 27009の改訂

- Information technology － Security techniques － Sector-specific application of ISO/IEC 27001 － Requirements
  - 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、様式などを定めた規格
  - 2006年発行された初版を早期マイナー改訂中
  - 想定利用者は、セクター規格を作成する組織
  - 早期改訂は、付された規格のテンプレートが読みにくいとの、参照組織からの意見に基づいて開始された。読み易さの改善が主たる目的。
  - ISO/IEC 27701、ISO/IEC 27019などが参照している。
  - 作業状況：
    - 規格発行前の編集上の修正を確認する最終段階。2020年度には発行の見込み

その他の状況

- ISO/IEC 27007:2017 Information technology -- Security techniques -- Guidelines for information security management systems auditing

→ 引用規格ISO 19011（マネジメントシステム監査のための指針）の改訂に対応するためのマイナー改訂版が2020年に発行見込み

- ISO/IEC 27006:2015 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems

→ 誤解を生じやすい点に関し追補発行の見込み

- ISO/IEC 27013:2015 Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

→ 引用規格ISO/IEC 20000-1改訂に伴い改訂中。エキスパートで作業文書を作成している段階

その他の状況

- ISO/IEC 27014:2013 Information technology -- Security techniques -- Governance of information security

→ 改訂中。国レベルでの投票において、技術的コメントを提出できる最終段階。2022年には発行見込み

- ISO/IEC 27022 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文書。改訂中。国単位で投票し、コメント処理するCDステージに進んだ。2022年には発行見込み

ISO/IEC 27000ファミリー規格の最新動向

2018-12-07

ISO/IEC JTC1/SC27 WG1小委員会 主査
(株式会社日立製作所)
相羽 律子