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

目次

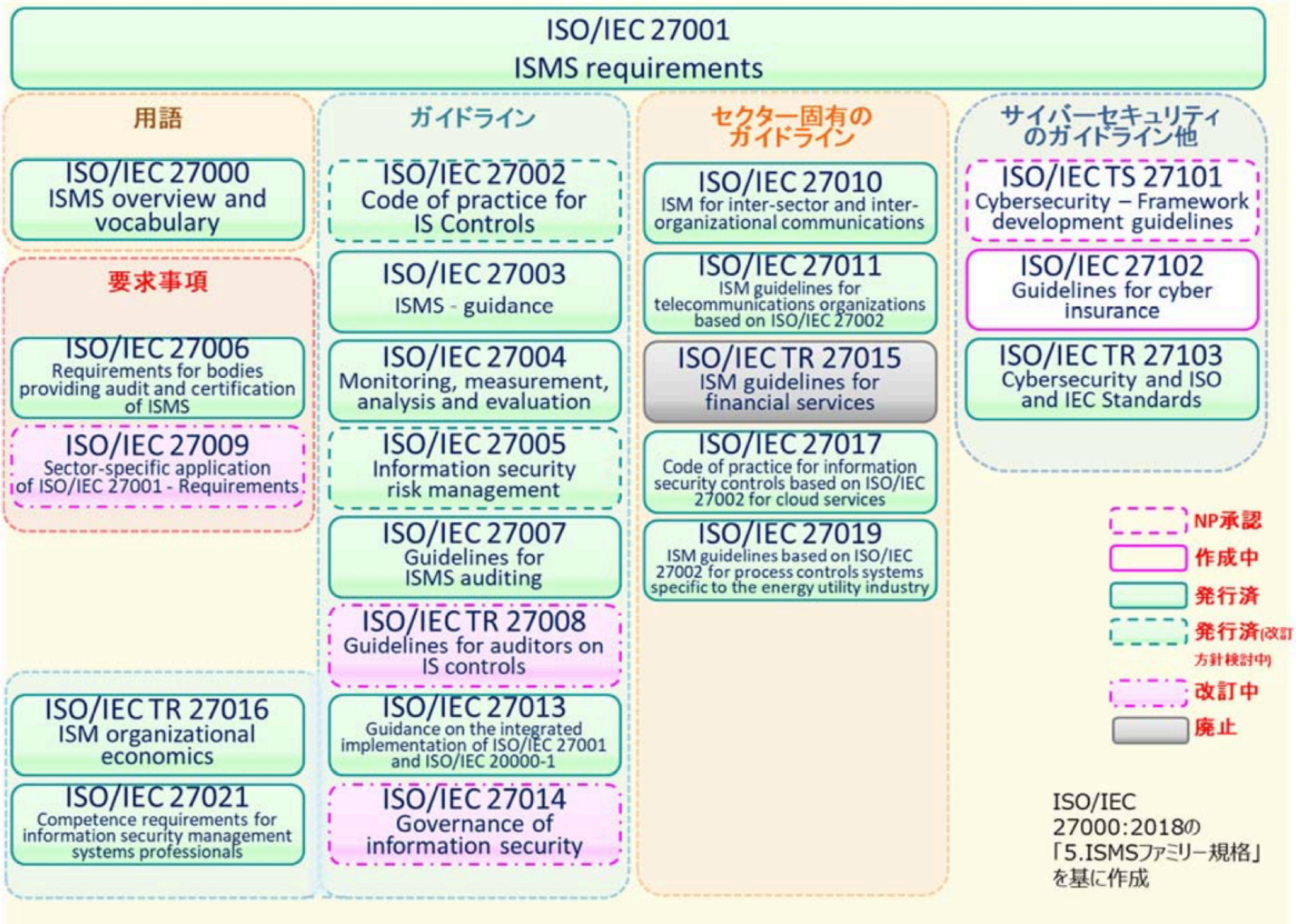
- ISO/IEC 27000ファミリー規格とは
- ISO/IEC JTC1/SC27/WG1における規格化の概況
  - ISO/IEC 27001及びISO/IEC 27002の改訂状況
  - サイバーセキュリティに関する規格開発の本格化
  - その他の状況

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
- **規格の番号は、現時点では 27000～27040 番台及び 2710X 番台となっている**
- **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/u71kba000000jigv-att/27000family_20180620.pdf

標準化組織（ISO/IEC JTC1/SC27）

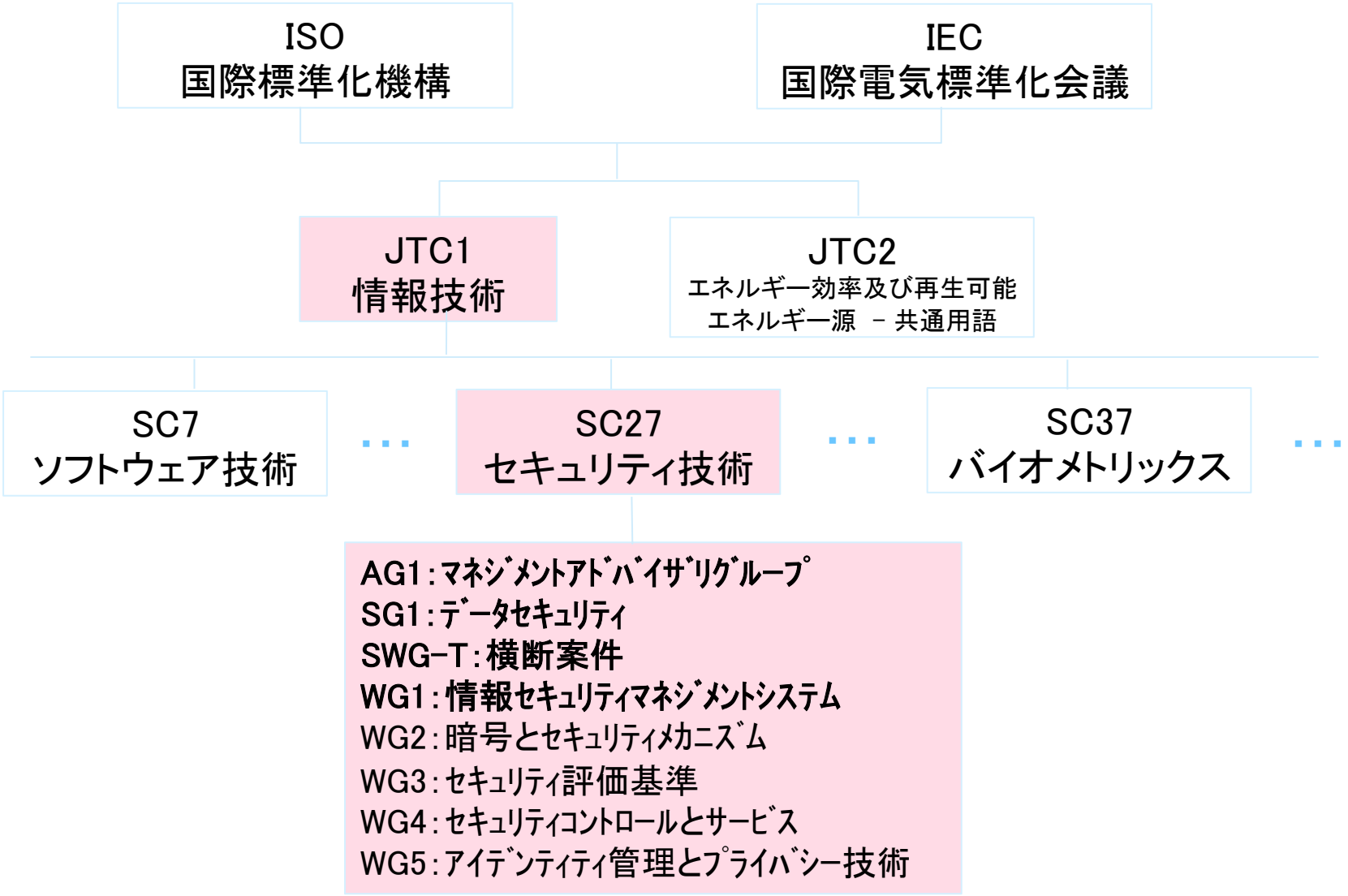


図1　ISO/IEC JTC1/SC27の組織構造

ISO/IEC JTC1/SC27

- タイトル: IT Security techniques　←変更について審議中

- 発行済み: 183規格
- 開発中: 61規格
- メンバー国: 51カ国
- オブザーバーメンバー国: 27カ国

（上記数字は全て2018-11-29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
  - 2018年は、春は4月に武漢（中国）、秋は9～10月にイエビク（ノルウェー）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

2018年発行の規格

- ISO/IEC 27000:2018 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
  - 改訂5版
  - ISO/IEC 27003, ISO/IEC 27004の改訂などに伴い、掲載する用語に変更が生じたことに伴う改訂
  - ISO/IEC 27001及びISO/IEC 27002に関する用語については変更なし
  - JIS化について:
    - ISO/IEC 27000:2018(改訂3版)は、JIS Q 27000:2014として用語部分のみJIS化
    - 改訂4版は、用語に変更がなかったためJIS改訂は行われず
    - 改訂5版のJIS化は現在作業中。来年発行予定

2018年発行の規格

- ISO/IEC 27005:2018 Information technology -- Security techniques -- Information security risk management
  - 改訂3版
  - 内容的には、ISO/IEC 27001:2013に合わせて編集上の修正を行ったのみ
  - 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は、改訂を検討中
    - 改訂プロジェクトは未開始
    - 改訂に向けた作業期間を設け、コンテンツを収集中

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の改訂状況

- **現在、定期レビューの投票期間**　←年内に投票結果

- 一方で、WG1内に、次期改訂における選択肢を検討するアドバイザリーグループを設置
  - 次期改訂について検討する必要性とは？

    → マネジメントシステム規格の共通フォーマット改訂との時期調整

＜想定されるスケジュール＞

ISO/IEC 27001	2019年春改訂開始	→	2022年春発行（36ヶ月の場合）
	2019年春改訂開始	→	2023年春発行（48ヶ月の場合）

※共通フォーマット改訂版発行は2022年見込み

ISO/IEC 27001:2013の改訂状況

- 前回改訂時に平行線をたどった（次の改訂でも対立が想定される）課題について、改訂に先立ち、検討作業を実施
  - 期間：2017年10月～2018年10月
  - トピックス：
    - Annex Aの必要性（特定の一つの管理策群との比較は必要か etc.）
    - 適用宣言書の必要性（固有名詞である必要はあるか etc.）
  - 結果：
    - 25名のWGエキスパートの意見を収集
    - 特定の結論は出さずに収集した意見をまとめて本検討は終了。まとめた内容はWG1内文書として発行
    - Annex A、適用宣言書とも必要との回答が優勢も、根強い反対もあり
    - 議論は、改訂開始後に持ち越し

ISO/IEC 27002:2013の改訂

- **2018年4月より改訂作業を開始済み**
- 改訂作業開始前に、1年間の準備期間を置き、デザインスペックを決定している
- **現在はWGエキスパートレベルで作業文書(WD)を作成中**
- 発行は2021年以降の見込み
- ISO/IEC 27001との改訂版同時発行については、する・しない含めて今後の検討課題
- 改訂プロジェクトの進め方：
  - 先行して規格本文の構成、及び管理策を確定する
  - 各管理策の内容詳細の議論はその後に

ISO/IEC 27002:2013の改訂

- これまでに議論した内容　← 注：決定事項ではありません
  - タイトル:
    Information technology – Security techniques – Information security controls
  - 規格の構成:
    - 管理策の最上位カテゴリ:
      organization, people, physical, technical
    - 各管理策の記述構成:
      control, purpose, implementation guidance, and other information
    - その他: 管理策にattributesを付属する
      ex. Control type (preventive, detective, corrective), CIA

ISO/IEC 27001及びISO/IEC 27002の改訂の状況

＜まとめ＞

- ISO/IEC 27001は、5年毎の定期見直しスキームに基づき、改訂を開始するか判断のタイミング
  Annex SL改訂とのタイミングで改訂開始が遅れる可能性も
- ISO/IEC 27001は改訂作業に伴い想定される課題を先出しで個別に検討中
- ISO/IEC 27002は改訂作業を既に開始済み
  まだ、WGエキスパートレベルで作業文書（WD）を作成中の段階

ISO/IEC JTC1/SC27/WG1における規格化の概況

– サイバーセキュリティに関する規格開発の本格化

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
- 今後の作業及び課題:
  - WGエキスパートレベルで作業文書を作成している状況
    文書の発行は2020年以降の見込み
  - 保有課題:次についてコンセンサスを得ること
    - サイバーセキュリティとは何か
    - 情報セキュリティとの違い
    - ISMSとの関係　他

プロジェクトは、まだ始まったばかり…

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：サイバーセキュリティ・フレームワークを作る組織。政府機関、業界団体等
- 現在は、WGエキスパートレベルで作業文書を作成している状況。文書の発行は2019年以降の見込み。

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）無償配布を決定。現在準備中

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 27102の開発

ISO/IEC 27102 Information technology -- Security techniques -- Information security management guidelines for cyber insurance

- 組織のリスクマネジメントの枠組みの中で、サイバー保険をリスク低減の対策に用いる際のガイドラインを提供する
- タイトル変更を提案中。今後、投票を経て決定見込み

  ISO/IEC 27102 Information technology – Information Security Management – Guidelines for cyber insurance

- 想定利用者：保険利用者と保険事業者
- 今後の予定：
  - SC27メンバーだけでなく、全メンバー国に投票のため回付するレベルでのドラフト検討（技術面の検討の最終段階）
  - 進捗によっては、2019年の発行もあり得る

サイバーセキュリティに関する規格開発の本格化

＜まとめ＞

- ISO/IEC 27100（Overview and concepts）及びISO/IEC 27101（Framework development guidelines）はいずれもWGエキスパートレベルで作業文書を推敲する初期段階。
- ISO/IEC 27102（Cyber insurance)は、技術面の検討の最終段階。早ければ2019年に発行も
- ISO/IEC 27103（Cybersecurity and ISO and IEC Standards）は、無償での提供へ

ISO/IEC JTC1/SC27/WG1における規格化の概況

– その他の状況

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、早期のマイナー改訂に進む見込み

- ISO/IEC 27009:2016 Information technology -- Security techniques -- Sector-specific application of ISO/IEC 27001 - Requirements

→ 改訂中。SC27メンバー内においてドラフトを検討する段階

- 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

その他の状況

- 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改訂に伴い改訂に進む見込み

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

→ 改訂作業中。WGエキスパートで作業文書を作成している段階

- ISO/IEC 27019:2017 Information technology -- Security techniques -- Information security controls for the energy utility industry

→ 正誤表を発行予定

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