# ISO/IEC 27000 ファミリー規格の展開とその活用

2021年12月17日

国立研究開発法人 情報通信研究機構 (NICT)
山下　真
ISO/IEC JTC1 SC27 WG1, WG4

# 目　次

# 国際標準化組織

JTC 1: 情報技術 (Information technology)

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

WG 1: 情報セキュリティマネジメントシステム

WG 4: セキュリティ・コントロール及び
セキュリティ・サービス

# 規格開発の段階

| | |
|---|---|
| PWI | Preliminary Work Item |
| NP | New Work Item Proposal |
| WD | Working Draft |
| CD | Committee Draft |
| DIS | Draft International Standard |
| FDIS | Final Draft International Standard |
| **IS** | **International Standard** |

| | |
|---|---|
| PWI | Preliminary Work Item |
| NP | New Work Item Proposal |
| WD | Working Draft |
| DTS | Draft Technical Specification |
| **TS** | **Technical Specification** |

| | |
|---|---|
| PWI | Preliminary Work Item |
| NP | New Work Item Proposal |
| WD | Working Draft |
| DTR | Draft Technical Report |
| **TR** | **Technical Report** |

# ISO/IEC 27000 ファミリー規格一覧　1/5

| | 文書番号 | 内容 | 備考 |
|---|---|---|---|
| | ISO/IEC 27000:2018 | ISMS – 概要及び用語<br>（JISは用語部分を採用） | |
| ★ | ISO/IEC 27001:2013 | ISMS – 要求事項 | 附属書A更新へ |
| ★ | ISO/IEC 27002:2013 | 情報セキュリティ管理策 | 改定作業中　FDIS |
| ★ | ISO/IEC 27003:2017 | ISMS – 指針 | |
| | ISO/IEC 27004:2016 | 情報セキュリティマネジメント – 監視、測定、分析及び評価 | |

以下 ★ について本講演で特に言及

# ISO/IEC 27000 ファミリー規格一覧　2/5

| 文書番号 | 内容 | 備考 |
|---|---|---|
| ISO/IEC 27005:2018 | 情報セキュリティ・リスクマネジメントの手引 | 改定作業中　DIS |
| ISO/IEC 27006:2015 | ISMSの審査及び認証を行う機関に対する要求事項 | 改定作業中　CD<br>番号変更: ISO/IEC 27006-1 |
| ISO/IEC 27006-2 | ISMSの審査及び認証を行う機関に対する要求事項 – 第2部 プライバシー情報マネジメントシステム | 策定中　CDからDISへ<br>ISO/IEC 27701:2019に基づくPIMS対応 |
| ISO/IEC 27007:2020 | ISMS監査の指針 | |

# ISO/IEC 27000 ファミリー規格一覧　3/5

| 文書番号 | 内容 | 備考 |
|---|---|---|
| ISO/IEC TS 27008:2019 | 情報セキュリティ管理策の評価指針 | |
| ISO/IEC 27009:2020 | 分野別ISMS要求事項を定める規格に対する要求事項（規格開発者向け） | |
| ISO/IEC 27010:2015 | セクター間及び組織間のコミュニケーションにおける情報セキュリティマネジメント | 定期レビューの結果、「改定せず」 |
| ★ ISO/IEC 27011:2016 | ISO/IEC 27002 に基づく通信事業者のための情報セキュリティ管理策の実践の規範 | 改定作業中　CD<br>改定 ISO/IEC 27002 対応など |

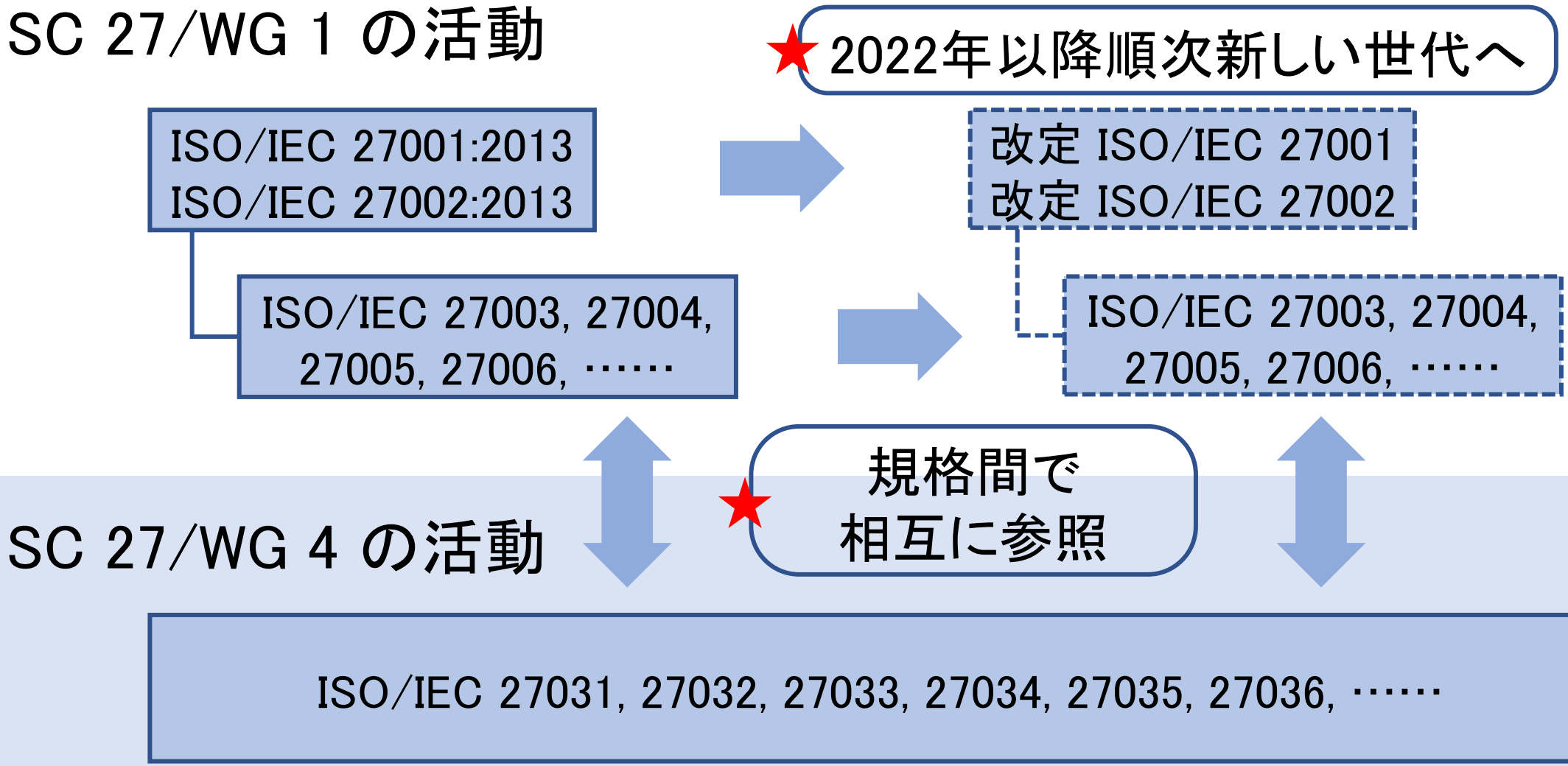
# ISO/IEC 27000 ファミリー規格一覧　4/5

| 文書番号 | 内容 | 備考 |
|---|---|---|
| ISO/IEC 27013:2021 | ISO/IEC 27001 及び ISO 20000-1 の統合実施の手引 | 改定作業を終え出版<br>ISO/IEC 20000-1:2018 対応 |
| ISO/IEC 27014:2020 | 情報セキュリティガバナンス | |
| ISO/IEC TR 27016:2014 | 情報セキュリティマネジメント - 組織活動の経済性 | |
| ★ ISO/IEC 27017:2015 | 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 | 改定作業開始へ<br>改定 ISO/IEC 27002 対応など |

# ISO/IEC 27000 ファミリー規格一覧　5/5

| 文書番号 | 内容 | 備考 |
| --- | --- | --- |
| ISO/IEC 27019:2017 | ISO/IEC 27002 に基づくエネルギー産業における制御システムの情報セキュリティ管理策 | |
| ISO/IEC 27021:2017 | ISMS専門家向け要求事項 | |
| ISO/IEC TS 27022:2021 | ISMSプロセスモデルの指針<br>ISO/IEC 33004 に定めるプロセス参照モデルによるISMSプロセスの記述 | |
| ISO/IEC TR 27023:2015 | ISO/IEC 27001, ISO/IEC 27002管理策の 2005 年版対 2013 年版対応表 | |

# ISO/IEC 27000 ファミリー規格と関連規格の展開



# サイバーセキュリティ関連規格一覧　1/2

| | 文書番号 | 内容 | 備考 |
|---|---|---|---|
| ★ | ISO/IEC TS 27100:2020 | サイバーセキュリティの概要及び概念 | WG 1 |
| | ISO/IEC 27102:2019 | 情報セキュリティリスクマネジメントにおけるサイバー保険の活用 | WG 1 |
| | ISO/IEC TR 27103:2018 | サイバーセキュリティ・フレームワークと ISO/IEC 27001、ISO/IEC 27002 その他の文書との対応関係 | WG 1 |
| | ISO/IEC TR 27109 | サイバーセキュリティの教育・訓練 | 計画中<br>WG 1 |
| | ISO/IEC TS 27110 | サイバーセキュリティ・フレームワーク開発指針 | WG 1 |
| | ISO/IEC 27032:2012 | インターネット・セキュリティ | 改定作業中　CD<br>WG 4 |
| ★ | ISO/IEC TS 5689 | サイバーフィジカルシステムの概念モデルに基づくセキュリティ・フレームワーク | 策定準備中　NPへ<br>WG 4 |

# サイバーセキュリティ関連規格一覧　2/2

| | 文書番号 | 内容 | 備考 |
|---|---|---|---|
| ★ | ISO/IEC 27400 | IoTにおけるセキュリティ及びプライバシーの指針 | 策定中　DIS<br>WG4 |
| ★ | ISO/IEC 27402 | IoT機器のセキュリティ対策基本要求事項 | 策定中　CD<br>WG4 |
| | ISO/IEC 27403 | 居住環境におけるIoTセキュリティ・プライバシーの指針 | 策定中　WD<br>WG4 |

# SC 27/WG 4 の活動

WG 4 のタイトル：　Security controls and services

セキュリティ・コントロール及び
セキュリティ・サービス

- 情報セキュリティ及びサイバーセキュリティの分野ごとに、指針、手引を中心とする文書を提供。

　　・・・以下のスライドに主要文書一覧

- 利用者は、目的に応じて必要な文書を選び、活用することができる。

# SC 27/WG 4 の主な活動分野と文書　1/4

- 情報システム及びネットワーク
  - ISO/IEC 27002 管理策と関係して、技術を中心にさらに詳細な指針を提示

| | 適用分野・場面 | 文書番号 |
|---|---|---|
| ★ | ネットワークセキュリティ | ISO/IEC 27033 Part 1 – Part 7 |
| | インターネットセキュリティ | ISO/IEC 27032 |
| | 侵入検知・防御システム（IDPS） | ISO/IEC 27039 |
| | アプリケーションセキュリティ | ISO/IEC 27034 Part 1 – Part 7 |
| | ストレージ機器のセキュリティ | ISO/IEC 27040 |
| | 事業継続を支えるセキュリティ | ISO/IEC 27031 |
| ★ | インシデントマネジメント | ISO/IEC 27035 Part 1 – Part 4 |

# SC 27/WG 4 の主な活動分野と文書　2/4

- 製品及びサービスの調達・供給
  - 調達する製品及びサービスの
    - セキュリティに関する信頼確保
    - サプライチェーンリスクの考慮
  - 供給する製品及びサービスのセキュリティに関する信頼・品質確保と情報提供

| 適用分野・場面 | 文書番号 |
|---|---|
| ★ 供給者関係及びサプライチェーンにおけるセキュリティ | ISO/IEC 27036 Part 1 – Part 4 |
| ハードウェア、ソフトウェア製品のライフサイクルにおけるセキュリティ | ISO/IEC 6114　策定中 |
| PKI認証局の運用 | ISO/IEC 27099　策定中 |

# SC 27/WG 4 の主な活動分野と文書　3/4

- デジタル証拠
  - 訴訟において証拠として認められるデータの取得・保存の技術要件と運用要件等

| 適用分野・場面 | 文書番号 |
| --- | --- |
| デジタル証拠、<br>インシデント調査のプロセスと技術 | ISO/IEC 27037, ISO/IEC 27041,<br>ISO/IEC 27042, ISO/IEC 27043 |
| eディスカバリー | ISO/IEC 27050 Part 1 – Part 4 |

# SC 27/WG 4 の主な活動分野と文書　4/4

- サイバーセキュリティ
  - SC 41 (IoT)、SC 42 (AI, ビッグデータ) の文書を基礎とするセキュリティの指針等
  - サイバーフィジカルシステムの枠組み

| 適用分野・場面 | 文書番号 |
|---|---|
| ★ IoTのセキュリティ及びプライバシー | ISO/IEC 27400　策定中 DIS<br>ISO/IEC 27402　策定中 CD<br>ISO/IEC 27403　策定中 WD |
| ★ サイバーフィジカルシステムの概念モデルに基づくセキュリティ・フレームワーク | ISO/IEC TS 5689<br>策定準備中(PWI)、NPへ |
| ビッグデータの活用におけるセキュリティ及びプライバシー | ISO/IEC 20547-4<br>ISO/IEC 27045　NPから策定へ<br>ISO/IEC 27046　策定中 WD |

# 目　次

1. ISO/IEC 27000 ファミリー規格と関連規格の展開

2. 情報セキュリティリスクマネジメントとISMSの文書についての工夫

# ISMSにおいて適用する管理策を決めるプロセス

- 情報セキュリティリスクアセスメント

  ISO/IEC 27001:2013, 6.1.2, 8.2

- 情報セキュリティリスク対応

  ISO/IEC 27001:2013, 6.1.3, 8.3

# 情報セキュリティリスクの認識

1. 様々な場面におけるリスク源、事象及び結果の連鎖をリスクシナリオとして記述する。
2. それぞれのリスクシナリオについて目標とする状態（情報セキュリティ目的・目標）を定める。
3. それぞれのリスクシナリオについて現実の状態を知る。
4. 情報セキュリティリスクを、2 と 3 の乖離として認識する。

リスクの定義
目的に対する不確かさの影響
（ISO/IEC 27000:2018, 3.61）

# リスクシナリオの記述例　顧客情報管理システムの一場面から

**場面：　情報システムに顧客情報を持つ。情報システムに不備があるかもしれない。**

**情報セキュリティ目的：　顧客情報を漏洩しない。**

| リスクシナリオ | |
|---|---|
| リスク源 | 1. 顧客情報を情報システムに持つ。<br>2. 顧客情報管理システムをインターネットにつながる内部ネットワークに置く。<br>3. セキュリティ設定について担当者の技術力が足りない。<br>4. 脆弱性情報の収集と脆弱性への対応が不十分である。<br>5. 顧客情報管理システム又はネットワークの設定に不備がある。<br>6. 外部から不正侵入を試みる者が存在する。 |
| 事象 | 1. 組織の内部ネットワークに外部者が侵入する。<br>2. 情報システムに外部者が侵入する。<br>3. 外部者が顧客情報を見たり取得したりする。<br>4. 外部者が顧客情報を悪用する。 |
| 結果 | 1. お客様が不利益を被る。<br>2. 会社の信頼を損なう。<br>3. 会社が経済的損害を被る。 |

山下「ISO/IEC 27000シリーズの現在と今後」
日本ISMSユーザグループ　情報セキュリティマネジメント・セミナー2016 より引用、加筆

# 情報セキュリティリスク対応　管理策の決定

- ISO/IEC 27001:2013, 6.1.3 b), c)

1. 管理策の決定
   特定した情報セキュリティリスクを低減するために必要な管理策を決定する。[6.1.3 b)]

2. 管理策の確認
   決定した管理策を附属書Aの管理策群と比較して、見落しがないことを確認する。[6.1.3 c)]

# 情報セキュリティリスク対応　管理策の決定

- 管理策は、組織が独自に決めてもよく、既存の他の規格や文書にある管理策群を使ってもよい。

- 管理策を決定する根拠は、意図するリスク低減が達成される見込みであること。残留するリスクを受け入れてよいこと。

# 情報セキュリティリスク対応　適用宣言書　1/2

**管理策を ISO/IEC 27001 附属書A 以外から選び、又は独自に決める場合**

- ISO/IEC 27001:2013, 6.1.3 d)
  - 以下の事項を適用宣言書に書く。
    1. 6.1.3 b) で決定した管理策
    2. それぞれの管理策について
       a. **含めた（採用した）理由　！**
       b. 実施しているか否か
    3. 採用した管理策から対応づけられない附属書Aの管理策について、除外した理由　＝　除外してよいことの説明

極めて簡潔なこの要求事項の解釈は、一つでない可能性も。
解釈の例：
理由として以下を説明する。
① この管理策で対応する情報セキュリティリスク
② リスク低減の必要性
③ この管理策の有効性

# 情報セキュリティリスク対応　適用宣言書　2/2

## 管理策を ISO/IEC 27001 附属書A から選ぶ場合

- ISO/IEC 27001:2013, 6.1.3 d)
  - 以下の事項を適用宣言書に書く。
    1. 附属書Aの管理策ごとに、採用、不採用の区別
    2. 採用した管理策と他に追加した管理策について
       a. **採用又は追加した理由　！**
       b. 実施しているか否か
    3. 採用しなかった管理策について、不採用でよい理由

解釈の例：
理由として以下を説明する。
① この管理策で対応する情報セキュリティリスク
② リスク低減の必要性
③ この管理策の有効性

# 管理策を比較すること (6.1.3 c)) の難しさ　1/2

- 決定した管理策群と附属書Aの管理策群の比較（6.1.3 c)）は、必ずしも簡単・自明ではない。
  - 管理策群の適用分野や想定する場面が違えば、背後に想定するリスクや、観点、粒度、用語が違う。

    <u>管理策群の例</u>

    a. ISO/IEC 27002（ISO/IEC 27001, Annex A）

    b. 政府機関等のサイバーセキュリティ対策のための統一基準

    c. NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations

# 管理策を比較すること (6.1.3 c)) の難しさ　2/2

- 決定した一つの管理策が附属書Aの一つの管理策に過不足なく対応付けられるとは限らない。
- 附属書Aの一つの管理策が及ぶ範囲は、読者によって理解が違うかもしれない。

  例　　ログ取得の対象、種類

  （ISO/IEC 27002:2013 12.4 ログ取得及び監視）

  情報セキュリティのレビューの範囲、方法

  （ISO/IEC 27002:2013 18.2 情報セキュリティのレビュー）

- **管理策を採用しているか否かは、「はい」と「いいえ」で表現できるとは限らない。**

# ISO/IEC 27002 新旧管理策の対応例

- 改定 ISO/IEC 27002 では、管理策の単位と表現はより一般的に

| ISO/IEC 27002:2013 | 改定 ISO/IEC 27002 |
|---|---|
| 6.2.1 モバイル機器の方針 | 8.1 利用者端末 |
| 11.2.8 無人状態にある利用者装置 | |
| 9.2.4 利用者の秘密認証情報の管理 | 5.17 認証情報 |
| 9.3.1 秘密認証情報の利用 | |
| 9.4.3 パスワード管理システム | |

- 「6.2.1 モバイル機器の方針」を採用していれば「8.1 利用者端末」も採用しているとは限らない。
  - **採用しているとは　・・・「どの範囲で」「どのように」を説明する。**

# ＜参考＞　改定 ISO/IEC 27002 における記事の量

- 改定 ISO/IEC 27002 では、管理策ごとの手引が一層充実した。

| | ISO/IEC 27002: 2013 | ISO/IEC 27002 改定 |
|---|---|---|
| 管理策数 | 114 | 93 |
| 総記述量 | 77ページ<br>(5章～18章) | 121ページ<br>(5章～8章) |
| 管理策あたりの記述量 | 0.7ページ | 1.3ページ |

# 管理策を採用することの説明について　1/2

- 適用宣言書において管理策を採用している理由の説明とは･･･、
  - **一つの解釈:**
    **情報セキュリティリスクアセスメントと情報セキュリティリスク対応について説明する。**
    - 想定する様々な情報セキュリティリスクシナリオの説明を含む。
  - **加えて前提も説明するか?**
    - 組織で確立した情報セキュリティ方針と情報セキュリティ目的（ISO/IEC 27001:2013，5章, 6.2）
    - 組織の状況の理解とその記述（同 4章）

# 管理策を採用することの説明について　2/2

- ISO/IEC 27001:2013 は、組織におけるISMSのそれぞれの活動について文書化を求めている。
- 適用宣言書とそこにおける管理策を採用することの説明は、ISMSについて組織が整備する文書化の中で他から不可分の一部である。

**ISO/IEC 27002 改定は、ISMS関連文書について再確認する機会**

- 適用宣言書に含める説明の範囲
- 文書や情報を提供・開示・公開する範囲
  - ✓組織内での説明や周知の場合
  - ✓外部者に説明する場合
    - ✓一般的な公表
    - ✓利害関係者への説明

# 目　次

1. ISO/IEC 27000 ファミリー規格と関連規格の展開

2. 情報セキュリティリスクマネジメントとISMSの文書についての工夫