ISO/IEC 27002 改定について

2019年12月4日

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

目　次

ISO/IEC 27002 改定の目標と原則

1. **現行版の価値と役割を継承する。**
2. 新たな要件に対応する。
3. 管理策体系について利用組織ごとの見方があることに配慮する。
4. 利用時の負担軽減を図る。

ISO/IEC 27002 と関連規格の展望

5. ISO/IEC 27002 の管理策を説明する規格
6. ISO/IEC 27002 に管理策を追加する規格
7. ISO/IEC 27002 のサイバーセキュリティへの適用

改定でめざすこと

1. ISO/IEC 27002の価値と役割を継承する。

- ISO/IEC 27001とあわせて使用
- 情報セキュリティ管理策の汎用の手引・参考書

⇒「適用範囲」に反映

2. 情報セキュリティ管理策を活用するさまざまな場面や視点に配慮する。

- 情報セキュリティ管理策群の体系を緩やかに規定
- 組織ごとの視点に基づく管理策体系も可能に

⇒「テーマ」及び「属性」によるアプローチ

改定の経緯

年月	活動等
2013-10	ISO/IEC 27002:2013出版
2016-01	改定要否について出版後3年目の投票
2016-04	改定実施を決定 1回目の検討期間（study period）を開始 [米国・タンパ]
2016-10	2回目の検討期間を開始 [UAE, アブダビ]
2017-04	3回目の検討期間を開始 [ニュージーランド・ハミルトン]
2017-10~11	検討期間を終了 成果として設計書（design specification）を完成 [ドイツ・ベルリン]
2018-04	改定プロジェクト開始を決定 [中国・武漢]
2018-06~	改定ドラフトを半年ごとに検討
2019-10	3rd Working Draft に対する意見書を審議 [フランス・パリ]
2020-04	1st CDに対する意見書を審議（予定） [ロシア・サンクトペテルブルグ]

ISO/IEC 27001 改定について

- ISO/IEC 27001, Annex A を通して ISO/IEC 27001 と ISO/IEC 27002 は連動するが、
- ISO/IEC 27001 の改定時期は、以下を考慮して今後判断する。
  1. 改定する場合の利用組織への影響
  2. ISOマネジメントシステム共通テキスト・共通用語定義改定の状況
  3. ISO/IEC 27002 改定の状況

改定 ISO/IEC 27002 の標題　－設計書より－

- 改定版
  “Information security controls”
  「情報セキュリティ管理策」
  - 管理策の集合、素材集

- 現行版（2013年版）
  “Code of practice for information security controls”
  「情報セキュリティ管理策の
  実践のための規範」

改定 ISO/IEC 27002 の適用範囲 －設計書より－

- 一般的な情報セキュリティ管理策群とその実施の手引を参照情報として提供する。
- 組織における次の用途向けに：
  a. ISO/IEC 27001に基づくISMSに関連して
  b. 情報セキュリティ管理策の適用に
  c. 独自に情報セキュリティマネジメントの指針を策定するために

規格の適用範囲は、現行版のものと同等

目　次

ISO/IEC 27002 改定の目標と原則

1. 現行版の価値と役割を継承する。
2. **新たな要件に対応する。**
3. 管理策体系について利用組織ごとの見方があることに配慮する。
4. 利用時の負担軽減を図る。

ISO/IEC 27002 と関連規格の展望

5. ISO/IEC 27002 の管理策を説明する規格
6. ISO/IEC 27002 に管理策を追加する規格
7. ISO/IEC 27002 のサイバーセキュリティへの適用

追加する管理策の例（候補、検討中）

5 組織の管理策

- クラウドサービスの利用における情報セキュリティ
  - ✓新規
  - ✓クラウドサービスを利用する組織向け
- 事業継続のためのICTの備え
  - ✓ISO/IEC 27002:2005, 14 Business continuity management に近い内容を一つの管理策に集約
- デジタル権利マネジメント
  - ✓新規

追加する管理策の例（候補、検討中）

7 物理的管理策

- 施設の物理的セキュリティ監視
  - ✓新規
  - ✓施設境界の監視

追加する管理策の例（候補、検討中）

8 技術的管理策

- データマスキング
  - ✓新規
- 通信トラフィックの監視
  - ✓新規
- 脆弱性情報の開示及び取扱い
  - ✓新規
- ウェブ・フィルタリング
  - ✓新規
- セキュアコーディングの原則
  - ✓新規（ISO/IEC 27002:2005 に一部存在）

目　次

ISO/IEC 27002 改定の目標と原則

1. 現行版の価値と役割を継承する。
2. 新たな要件に対応する。
3. **管理策体系について利用組織ごとの見方があることに配慮する。**
4. 利用時の負担軽減を図る。

ISO/IEC 27002 と関連規格の展望

5. ISO/IEC 27002 の管理策を説明する規格
6. ISO/IEC 27002 に管理策を追加する規格
7. ISO/IEC 27002 のサイバーセキュリティへの適用

管理策群の構成　－現行版 (2013年版) －

5　情報セキュリティのための方針群
6　情報セキュリティのための組織
7　人的資源のセキュリティ
8　資産の管理
9　アクセス制御
10 暗号
11 物理的及び環境的セキュリティ
12 運用のセキュリティ
13 通信のセキュリティ
14 システムの取得、開発及び保守
15 供給者関係
16 情報セキュリティインシデント管理
17 事業継続マネジメントにおける情報セキュリティの側面
18 順守

管理策群の構成　－設計書より－

- 管理策群を4分類

5 組織の管理策　Organizational controls

例「情報セキュリティの役割及び責任」「情報の分類」

6 人の管理策　People controls

例「情報セキュリティの意識向上、教育及び訓練」

7 物理的管理策　Physical controls

例「オフィス、部屋及び施設のセキュリティ」「装置の保守」

8 技術的管理策　Technological controls

例「情報のバックアップ」「ネットワークの分離」

管理策群の構成　－設計書より－

4分類にした理由は？

- 管理策群の分類については様々な見方があることを認識し、多くの組織に共通であると考えられる最低限の分類を示す。

分類基準は？

- 管理策の機能を発揮させる仕組みや役割が「組織」「人」「物理的なもの」「技術」のいずれであるかによって分類する。

一つの管理策が複数の分類に関係するときは？

- 主に関係する章に割り当てる。

管理策配下の構成　　－設計書より－

5.x　標題

属　性

管理策（Control）

xxxxxxxxxxxxxxxxxxxxxxx

目的（Purpose）

xxxxxxxxxxxxxxxxxxxxxxx

手引（Guidance）

xxxxxxxxxxxxxxxxxxxxxxx

関連情報（Other information）

xxxxxxxxxxxxxxxxxxxxxxx

管理策の属性　－設計書より－

- 4分類とは別の観点からの分類を属性と属性値で表す。

属性	属性値
Control type	Preventive, Detective, Corrective
Information security properties	Confidentiality, Integrity, Availability
Cybersecurity concepts	Identify, Protect, Detect, Respond, Recover

記述例
5.1　情報セキュリティポリシー

Control type	**Information security properties**	**Cybersecurity concepts**
Preventive	Confidentiality, Integrity, Availability	Identify

管理策の属性　　－設計書より－

- 管理策の体系は、組織で独自に再構成することも想定している。
  - 組織で属性及び属性値を決定する。

補足

改定 ISO/IEC 27002 の付属書に新旧管理策対応表を含める予定

目　次

管理策の数は少なく

- 3rd Working Draft では　（今後も増減）

章	数
5　組織の管理策 Organizational controls	39
6　人の管理策 People controls	7
7　物理的管理策 Physical controls	14
8　技術的管理策 Technological controls	37
全体	97

参考　ISO/IEC 27002:2013　114

管理策の数は少なく

- 組織の負担軽減のため管理策数削減
  - 他方、改定版は現行版の内容を包含する方針
    - ISO/IEC 27001:2013の要求事項は弱めない。
      （ある管理策を採用しない場合に説明を求める要求事項 [6.1.3 c), d)] を改定によって弱めない。）

- 複数の管理策を統合する例（検討中）
  - 「5.1.1 情報セキュリティのための方針群」＋
    「5.1.2 情報セキュリティのための方針群のレビュー」
  - 「12.1.2 変更管理」＋
    「14.2.2 システムの変更管理手順」＋…

管理策の数は少なく

- 課題
  - 「管理策を実施している（採用している）」ことの分解能が劣化
  - 管理策の一部を実施している場合、その管理策を実施していると言えるか？
- 本来の解決
  - 管理策統合の有無によらず、組織が管理策の実施範囲や実施内容を開示し、説明すること。
    - 例：　ITサービスの調達・供給関係において、供給者が管理策の実施について適切な具体性を持って説明すること。

目　次

場面ごとの手引　（1／3）

- 組織の情報セキュリティ対策を、場面ごとに、ISO/IEC 27002 よりも詳しく説明

規格	適用場面
ISO/IEC 27031	事業継続へのICTの備え
ISO/IEC 27032	インターネットセキュリティ （現行版：サイバーセキュリティ）
ISO/IEC 27033	ネットワークセキュリティ
ISO/IEC 27034	アプリケーションセキュリティ
ISO/IEC 27035	情報セキュリティインシデントマネジメント
ISO/IEC 27036	供給者関係における情報セキュリティ

場面ごとの手引　（2／3）

- 組織の情報セキュリティ対策を、場面ごとに、ISO/IEC 27002 よりも詳しく説明

規格	適用場面
ISO/IEC 27037	デジタル証拠の特定・収集・取得及び保持
ISO/IEC 27038	デジタル・リダクション
ISO/IEC 27039	IDPSの選択・導入及び運用
ISO/IEC 27040	ストレージ・セキュリティ
ISO/IEC 27041	情報セキュリティインシデント調査
ISO/IEC 27042	デジタル証拠の分析及び解釈
ISO/IEC 27043	インシデント調査の原則及びプロセス
ISO/IEC 27050	エレクトロニック・ディスカバリー

場面ごとの手引　（３／３）

- SC27/WG4が規格開発を担当
  - ISO/IEC 27002 の管理策・実施の手引との対比で、より詳しい内容、特に技術的内容を多く含む。
- 多くは ISO/IEC 27002 の管理策が起点

目　次

ISO/IEC 27002 改定の目標と原則

1. 現行版の価値と役割を継承する。
2. 新たな要件に対応する。
3. 管理策体系について利用組織ごとの見方があることに配慮する。
4. 利用時の負担軽減を図る。

ISO/IEC 27002 と関連規格の展望

5. ISO/IEC 27002 の管理策を説明する規格
6. **ISO/IEC 27002 に管理策を追加する規格**
7. ISO/IEC 27002 のサイバーセキュリティへの適用

管理策を追加する関連規格の位置づけ

- ISO/IEC 27002 が示す組織の情報セキュリティマネジメントとは異なる側面の管理策を定める。

例

- ISO/IEC 27017
  クラウドサービスプロバイダが実施する管理策によって、クラウドサービスカスタマの情報の CIA を維持する。
- ISO/IEC 27019
  エネルギー供給事業者が実施する管理策によって、社会資源である重要インフラの稼働を維持する。

管理策を追加する関連規格の二つの形式

A) 分野別規格 (sector-specific standards)

- ISO/IEC 27001 及び ISO/IEC 27002 に基づく
- ISO/IEC 27009 準拠
  - ISO/IEC 27009 は、
    - ✓規格開発者向け規格
    - ✓ISO/IEC 27001, ISO/IEC 27002 を拡張する方法を要求事項として規定

B) その他の関連規格

- 形式規定は緩やか

A）分野別規格

- ISO/IEC 27001 及び ISO/IEC 27002 を包含
  - ISO/IEC 27009 の要求事項に沿って開発
- 分野対応ISMSの認証基準になり得る
  「ISO/IEC 27017 を考慮したISMS認証」
  - ただし、認定基準の整備を待つ

標準	分野
ISO/IEC 27011:2016	通信事業
ISO/IEC 27017:2015	クラウドサービス利用者、事業者
ISO/IEC 27018:2014	PIIを扱うクラウドサービス事業者
ISO/IEC 27019:2017	エネルギー産業の制御システム
ISO/IEC 27701:2019	プライバシー情報マネジメント

B) その他の関連規格

- ISO/IEC 27002 に加える管理策及び手引を規定
  - 規格開発の規定は特になく、それぞれに適した内容と形式を採る。
  - 認証基準にはならない。

標準	分野
ISO/IEC 27030 （開発中）	IoTのセキュリティ及びプライバシー

管理策群の全体像

- 様々な適用に対応する管理策群の全体を ISO/IEC 27002 と関連規格が分担して記述
- SC27/WG1に加えて、WG4 及び WG5 の活動も貢献

目　次

サイバーセキュリティへの適用の現状

- ISO/IEC 27002 は、サイバーセキュリティに広く使われている。
  - 組織の情報セキュリティにとって、サイバー空間は深刻なリスク源
  - リスク特定においてサイバー空間に存在するサイバーリスクを認識し、対応している。

サイバーセキュリティの管理策

- ISO/IEC 27002 の管理策は、サイバーセキュリティの管理策でもある。
  - 管理策は、サイバーセキュリティの体系に自然に対応づけることができる。
    - ISO/IEC TR 27103 において、NIST CSF* に ISO/IEC 27002 管理策を対応づけ

      * Framework for Improving Critical Infrastructure Cybersecurity
  - 改定 ISO/IEC 27002 において、管理策にサイバーセキュリティの属性が与えられる。
    - Identify, Detect, Protect, Respond, Recover

サイバーセキュリティの規格

- ISO/IEC 27002 は、サイバーセキュリティの規格でもある。
  - サイバーセキュリティの分野別規格が ISO/IEC 27002 を含む。
    例：ISO/IEC 27019:2017
    Information security controls for the energy utility industry
  - サイバーセキュリティの規格が ISO/IEC 27002 を前提とする。
    例：ISO/IEC 27030
    Guidelines for security and privacy in Internet of Things (IoT)　[開発中]

サイバーセキュリティの規格としての課題

- 情報セキュリティとサイバーセキュリティを通して整合性のある概念と用語を整備すること

1. 両者の関係の説明と使い分け
   - ISO/IEC TS 27100 開発においても検討
2. 両者をあわせて表現する用語の可能性
3. 両者に適用できる共通規格における用語
   例：情報セキュリティインシデント／
   サイバーインシデント

サイバーセキュリティの規格としての課題

- 概念と用語に慣性があり、収斂には時間が必要

参考：

SC27のタイトル

Information security, cybersecurity and privacy protection

information security の定義 (ISO/IEC 27000)

preservation of confidentiality, integrity and availability of information

cybersecurity の定義 (ISO/IEC 27100, 暫定)

safeguarding of society, people, organizations and nations from cyber risks

下線を付けた語に対してさらに定義があるが、ここでは省略

ISO/IEC 27002 改定について

2019年12月4日

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