JNSA 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2023

ISO/IEC 27001 及び ISO/IEC 27002 の活用

― 情報セキュリティ管理策を軸に ―

2023年12月18日

国立研究開発法人 情報通信研究機構 (NICT)
山下　真
ISO/IEC JTC 1/SC 27/WG 1, WG 4

目　次

はじめに （1/2）

　ISO/IEC 27001 及び ISO/IE 27002 の改定（2022年版）は、情報セキュリティ管理策群を新しい体系に基づき整理した点に特徴がある。この機会に管理策群の活用に関係する二つの話題をとり上げる。

1. 情報セキュリティリスク対応（ISO/IEC 27001:2022, 6.1.3）において作成する適用宣言書では、管理策を採用した理由（＝管理策が必要であると決定した理由、＝管理策を含めた理由）の説明が求められる。一体何を説明すべきか。
2. ISO/IEC 27002 の管理策と手引は、素材集である。形式は推奨事項（「～望ましい。」）であるが。

はじめに （2/2）

本講演に関係する主な用語

情報セキュリティ管理策
情報セキュリティリスク
情報セキュリティリスクアセスメント
情報セキュリティリスク対応
適用宣言書
要求事項、推奨事項（推奨）

本講演資料とあわせて、必要に応じ、国際標準文書又は
日本産業標準（JIS）文書をご覧ください。

1. 管理策を採用しているとは

この話題の文脈: ISO/IEC 27001 の構成より

6 計画策定

6.1.2 情報セキュリティリスクアセスメント

プロセスを定め適用する
- リスク特定
- リスク分析
- リスク評価

6.1.3 情報セキュリティリスク対応

プロセスを定め適用する
- 管理策の決定
- 管理策の検証
- 適用宣言書の作成
- 情報セキュリティリスク対応計画の作成

8 運用

8.2 情報セキュリティリスクアセスメント

- 情報セキュリティリスクアセスメントを実施する

8.3 情報セキュリティリスク対応

- 情報セキュリティリスク対応計画を実施する

管理策を採用しているとは

ISO/IEC 27001,「6.1.3 情報セキュリティリスク対応」では、必要であると決定した管理策[6.1.3 b)] について、**含めた理由**を適用宣言書に書くことを求めている。

- この要求事項の意図は何か、疑問に思ったことはありませんか？「含める」という表明以上に何を示す？
- 管理策の意味に広がりがある中で、含めているか否かという二分法で表現できますか？

補足：「管理策が必要であると決定する (determine, 6.1.3 b))」
「管理策を含める (include, 6.1.3 d))」
「管理策を採用する (本資料独自の表現)」
・・・ 文脈に応じて使い分けるが、同義

適用宣言書に関する要求事項

適用宣言書に含めること:　ISO/IEC 27001:2022, 6.1.3 d)

① 必要であると決定した管理策

② 必要であると決定した（含めた）理由 (justification)

③ 必要であると決定した管理策を実施しているか否か

④ 必要であると決定した管理策に対応していない附属書Aの管理策について、必要でない理由（除外した理由）

補足1:　①では附属書Aに関係なく管理策を決定することが基本形。

補足2:　必要であるが実施していない管理策については、それに伴う残留リスクを保有することについてリスク所有者の承認を得る (6.1.3 f))。

適用宣言書に関する要求事項の一つの解釈

附属書Aの管理策から選ぶ場合の要求事項の解釈

適用宣言書に含めること:　ISO/IEC 27001:2022, 6.1.3 d)

① 必要であると決定した附属書Aの管理策
② 必要であると決定したその他の管理策
③ 必要であると決定した（含めた）理由 (justification)
④ 必要であると決定した管理策を実施しているか否か
⑤ ①で選ばなかった附属書Aの管理策が必要でない理由（除外した理由）

管理策の内容に広がりがあること

- 情報セキュリティ対策を一般的な表現で示すそれぞれの管理策は、その内容に広がりがある。

- ISO/IEC 27001 及び ISO/IEC 27002 の改定において、この傾向が一歩進んだ面もある。
  - 複数の管理策を統合し、一層広い意味を持つようになった例
  - 手引を拡充したことによって管理策の内容がより広く見えるようになった例

管理策の再編 （1/2）

- 旧管理策と新管理策の対応において、変更の少ない例と、複数の管理策を統合し変更も多い例がある。

<u>変更の少ない例</u>

一つの旧管理策を一つの新管理策に継承し、かつ、管理策と手引に追加変更も少ないもの

ISO/IEC 27002:2022	ISO/IEC 27002:2013
5.5　関係当局との連絡	6.1.3　関係当局との連絡
7.8　装置の設置及び保護	11.2.1　装置の設置及び保護
8.22　ネットワークの分離	13.1.3　ネットワークの分離

管理策の再編 （2/2）

変更の多い例

複数の旧管理策を一つの新管理策にまとめ、手引の内容も充実させたもの

ISO/IEC 27002:2022	ISO/IEC 27002:2013
5.14　情報の転送	13.2.1　情報転送の方針及び手順
	13.2.2　情報転送に関する合意
	13.2.3　電子的メッセージ通信
8.15　ログ取得	12.4.1　イベントログ取得
	12.4.2　ログ情報の保護
	12.4.3　実務管理者及び運用担当者の作業ログ

管理策の例：「5.14 情報の転送」

主題：　情報の転送

主旨：　その規則，手順又は合意を備えること。

ISO/IEC 27002:2022, 5.14 手引より

1. トピック固有の方針を持つこと。
2. 情報の媒体と転送手法に応じた手引の記述
   - 電子的転送／物理的記憶媒体の輸送／口頭での伝達(追加)
3. 組織内転送と外部との転送を対象とすること。
4. 組織の規則、手順、合意を持つ。

この管理策について、「必要である」か「必要ではない」のどちらかに決定する基準は何か？「必要である」の意味は?

適用宣言書に関する要求事項 ［再掲］

適用宣言書に含めること:　ISO/IEC 27001:2022, 6.1.3 d)

① 必要であると決定した管理策

② 必要であると決定した（含めた）理由 (justification)

③ 必要であると決定した管理策を実施しているか否か

④ 必要であると決定した管理策に対応していない附属書Aの管理策について、必要でない理由（除外した理由）

必要であるとした理由の説明について （1/2）

疑問に思うこと

必要であると決定した管理策について、その理由の説明を求めているのはなぜか？

- 除外した管理策について理由の説明を求めるのは理解できるが。
- 以下は理由の説明になっているか？ この説明で適合といえるか？

情報セキュリティリスクアセスメント及び情報セキュリティリスク対応のプロセスをとおして、この管理策が必要であると決定した。

必要であるとした理由の説明について （2/2）

情報セキュリティリスクアセスメント及び情報セキュリティリスク対応のプロセスをとおして、この管理策が必要であると決定した。（再掲）

- 要求事項 (ISO/IEC 27001:2022, 6.1.3 d)) の記述は簡潔であり、上記の説明では不適合であると判定する根拠はない。
- 他方、意味のある説明をすることは、組織自身がそのISMSの内容を認識し、組織内で共有し、ISMSの有効性を高めることに役立つのではないか。

役に立つ説明に向けて考えること（1/2）

- 「必要である理由／含める理由」、「除外した理由」を意味のあるものにするには、決定した情報セキュリティ対策が、情報セキュリティリスクの低減と情報セキュリティ目的の達成にどのようにつながるかを説明する。
- 要求事項では「必要である」と「除外している」に二分して問うが、二分法では情報セキュリティ対策は十分には表現できない。
- 管理策の内容・意味の広がりの中で、必要であると考える範囲を説明する。要求事項を超えて。

役に立つ説明に向けて考えること（2/2）

- 説明は、適用宣言書だけで完結する必要はない。
  適用宣言書に書くことができる記事の量は限られている。

- 組織で備える文書、仕様書等の全体を見ると、説明があるはず。

管理策と手引の活用

ISO/IEC 27002 の管理策及び手引の背後には、一般的に想定している情報セキュリティリスクがある。

- 「5.14 情報の転送」の裏に、場面や方法に応じた情報セキュリティリスクの想定がある。
  - 電子的転送／物理的記憶媒体の輸送／口頭での伝達

1. 管理策及び手引を理解する。
2. 管理策及び手引から、組織のISMSにとって関係する情報セキュリティリスクに気付く。規格の改定も契機に。
3. 気付きがあれば、遡って情報セキュリティリスクアセスメント及び情報セキュリティリスク対応のプロセスを実施し、補正する。

「目的」の活用　管理策を理解する助けとして

	ISO/IEC 27002:2022 目的（purpose）	ISO/IEC 27002:2013 管理目的（control objective）
記載場所	管理策の下	管理策に対して上位
ISO/IEC 27001 附属書Aに記載	なし	あり
範囲	管理策ごと	カテゴリごと（複数の 管理策をまとめて）

- 「目的」は、関係する情報セキュリティリスクの裏返し。
- ISO/IEC 27001 附属書A 管理策で想定する場面の例を知るために、ISO/IEC 27002:2022 を参照して「目的」を読む。

2. ISO/IEC 27002 は素材集であること

ISO の国際標準における要求事項と推奨事項

1. 要求事項
   「～しなければならない。」 “shall”
   ISO/IEC 27001 は、要求事項を多く含む国際標準の例

2. 推奨事項
   「～が望ましい。」 “should”
   ISO/IEC 27002 は、推奨事項を多く含む国際標準の例

ISO の国際標準における要求事項

1. 要求事項とは
   求める状態・行動を示す文であって、これ合致しているか否かを客観的に検証できるもの。（正確な定義は ISO/IEC Directives, Part 2を参照。）
2. 要求事項の表現は
   助動詞 shall を使う例が多い。JIS では「しなければならない」。
3. 要求事項には適合の概念がある。
4. 要求事項を示す文書に適合しているとは
   当該文書にあるすべての要求事項に適合していること。
5. 適合の確認方法・説明方法： 第一者（自己適合宣言）、
   第二者（供給者に対する調達者）、第三者

ISO の国際標準における推奨事項

1. 推奨事項とは
   薦める状態・行動を示す記述。
   （正確な定義は ISO/IEC Directives, Part 2 を参照。）
2. 推奨事項の表現は
   助動詞 should を使う例が多い。JISでは「～望ましい」。
3. 推奨事項には適合の概念はない。
4. 推奨事項の意味をより明確にするためには、前提、評価基準等、何等かの条件を加える必要があることが多い。
5. 日常語における「望ましい」という意味は持たない例もある。

ISO/IEC 27001 と ISO/IEC 27002 における 要求事項と推奨事項

ISO/IEC 27001:2022

本文：**要求事項**
「～しなければならない。」

附属書A　管理策
「～しなければならない。」
要求事項の形式を持つが、
直接の要求事項ではない。
関連：　本文 6.1.3 c) d)

ISO/IEC 27002:2022
5.1 ～ 8.34

‘属性’：該当する属性値

‘管理策’：**推奨事項**
「～することが望ましい。」

‘目的’

‘手引’：**推奨事項**と説明
「～することが望ましい。」
及び平叙文

‘その他の情報’：説明
平叙文

管理策の採否はどのように決めているか

1. 管理策

   管理策の採否を決定するとき、2段階の判断をしている。

   ① 場面や状況に合致しなければ採用しない。

   例 「6.7 リモートワーク」が適用できない職種・職場

   ② 情報セキュリティリスクアセスメント及び情報セキュリティリスク対応のプロセスを通して採用するか否かを決定する。

2. 手引

   手引についても同じ。

「望ましい」の効果

- 管理策及び手引は、「～望ましい」という推奨事項の形式を採っている。
- しかし、このことは、管理策及び手引の採用・不採用には関係しない。

- 情報セキュリティリスクアセスメント及び情報セキュリティリスク対応の文脈において、ISO/IEC 27002 は、中立的な記述の集まりである。

ISO/IEC 27002 は、素材集である。

ISO/IEC 27002 の標題 （1/2）

ISO/IEC 27002:2013

Information technology – Security techniques –

Code of practice for information security controls （注）

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

ISO/IEC 27002:2022

Information security, cybersecurity and privacy protection –

Information security controls

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 –

情報セキュリティ管理策

注　母体である英国 BS 7799 の標題 Code of best practice ～ が関係している。

ISO/IEC 27002 の標題 （2/2）

- 標題を「情報セキュリティ管理策」にした背景
  - この文書が素材集であることを明確にする。
  - 「規範」（code）から受けるイメージとは違う。

講演のまとめ

1. ISO/IEC 27001 に基づく情報セキュリティリスク対応において、「管理策を含めている、除外している」という区別だけでなく、一つの管理策の広がりの中で採用している範囲を説明できることは、組織自身がそのISMSの内容を認識し、組織内で共有し、ISMSの有効性を高めることに役立つ。要求事項の範囲を超えて。

2. ISO/IEC 27002 は、情報セキュリティ管理策の素材集であると割り切って活用する。「望ましい。」という推奨事項の表現にとらわれずに。

JNSA 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2023

ISO/IEC 27001 及び ISO/IEC 27002 の活用

― 情報セキュリティ管理策を軸に ―

2023年12月18日

国立研究開発法人 情報通信研究機構 (NICT)
山下　真
ISO/IEC JTC 1/SC 27/WG 1, WG 4