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2022

抜 粋

ISO/IEC 27001 改定内容と関連規格の動向

2022年12月16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

1. ISO/IEC 27001 改定

1.1 ISO/IEC 27001 前版及び改定版

1.2 改定の背景

1.3 ISO/IEC 27001 本文の改定概要

1.4 附属書A と ISO/IEC 27002 の関係

1.5 ISO/IEC 27001 本文の改定内容

1.1 ISO/IEC 27001 前版及び改定版

前版：　**ISO/IEC 27001:2013**,
Information technology — Security techniques — Information security management systems — Requirements

2013年10月1日

JIS Q 27001:2014

改定版：　**ISO/IEC 27001:2022**,
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

2022年10月25日

1.2 改定の背景 （1）

a. ISO/IEC 27001:2013
   - マネジメントシステム規格として安定して活用されてきた。
   - 2013年版から、マネジメントシステム規格（MSS）共通の構造・テキスト・用語定義を規格の基礎にしている。

b. MSS共通の構造・テキスト・用語定義
   - それぞれのマネジメントシステム規格における適用経験をもとに、ISO/IEC 27001:2013 で採用した版以後、改定されている。

     ISO/IEC Directives, Part 1 — Consolidated ISO Supplement — Procedure for the technical work — Procedures specific to ISO: 2022, Annex SL

1.2 改定の背景（2）

c. ISO/IEC 27001:2013 の改定

- 文書出版後3年目となる2016年に国際委員会 SC 27 において改定要否を検討した。その結果、以下を決定した。
  - ISO/IEC 27001:2013 の本文は改定の必要がない。
  - 先行して ISO/IEC 27002:2013 を改定することによって、附属書Aの差し替えが必要になる。差し替えの時期や方法については、後に検討する。
- 2022年に ISO/IEC 27002:2022 が出版され、その管理策を ISO/IEC 27001 附属書A に反映して ISO/IEC 27001:2013 を改定することとした。

1.3 ISO/IEC 27001 本文の改定概要 （1）

a. ISO/IEC 27001:2013 からの高い連続性

- ISO/IEC 27001:2022 への改定において、本文の追加・変更は少ない。要求事項の追加・変更も少ない。
- 追加・変更の内容
  - ✓最新のMSS共通テキストの反映（後出b）
  - ✓ISO/IEC 27001 に固有の変更（後出c）
- 用語定義は変わらない。ISO/IEC 27000 を引用する。

1.3 ISO/IEC 27001 本文の改定概要（2）

b. 最新のMSS共通テキストの反映

ISO/IEC 27001:2013 から ISO/IEC 27001:2022 への改定において、最新のMSS共通の構造とテキスト(#)を反映した。

今回の ISO/IEC 27001 改定は、附属書Aに ISO/IEC 27002 改定を反映するために進められた。ただし、最終ドラフト（FDIS）の段階で、最新のMSS共通の構造とテキストも反映することを決定した。

ISO/IEC Directives, Part 1 — Consolidated ISO Supplement — Procedure for the technical work — Procedures specific to ISO: 2022, Annex SL

c. ISO/IEC 27001 に固有の変更

上記とは別に、ISO/IEC 27001 に固有の、形式的な変更がある。

- 管理目的への言及の削除（ISO/IEC 27002:2022 に対応）
- 参照する ISO 31000 細分箇条の更新（ISO 31000 の改定に対応）

1.4 附属書A と ISO/IEC 27002 の関係

附属書A と ISO/IEC 27002 の関係は、2013年版における関係を維持している。

a. ISO/IEC 27002:2022 の管理策を、附属書Aで一覧にして示す。

b. ISO/IEC 27002:2022 の管理策における推奨（recommendation、～することが望ましい）を、ISO/IEC 27001 附属書Aでは要求事項（requirement、～しなければならない）に変える。

c. ISO/IEC 27001:2022, 6.1.3 において、組織が決定した管理策群を検証するために附属書Aと照合する。

管理策については、次の講演「ISO/IEC 27002改定の解説」で取り上げる。

1.5 ISO/IEC 27001 本文の改定内容

この節では、ISO/IEC 27001 本文の19の変更ごとに説明:

a. 変更内容
b. 変更の主旨
c. MSS共通テキストに基づく変更か、
   ISO/IEC 27001 に固有の変更か
d. 要求事項の追加・変更の有無

ISO/IEC 27001 のテキストは記載しない。必要に応じ原文書を参照されたい。

また、細部については異なる解釈もあり得ることにご留意ください。

1.5.1「4.1 組織及びその状況の理解」

変更箇所	注記
変更内容	ISO 31000 の中の参照先箇条番号: ISO 31000:2018, Risk management — Guidelines, 5.4.1 ← ISO 31000:2009, Risk management — Principles and Guidelines, 5.3
変更の主旨	ISO 31000 が改定されたため、改定後の構成にあわせる。 組織の外部状況及び内部状況について ISO 31000 で説明している箇所を参照する点では変わらない。
MSS共通か	ISO/IEC 27001 に固有。
要求事項の追加・変更	なし。 変更前後の記述はいずれも参考情報であり、要求事項ではない。 一般に、注記には要求事項も指針・手引もない。

1.5.2「4.2 利害関係者のニーズ及び期待の理解」

変更箇所	b), c)
変更内容	b) 「情報セキュリティに関連する要求事項」から「情報セキュリティ」を削除した。組織が決定する利害関係者の要求事項の範囲を情報セキュリティに限定しないことになる。 c) 改定で追加。b) で決定した利害関係者の要求事項の中で、組織がISMSにおいて取り組むものを特定する。
変更の主旨	利害関係者の要求事項を決定するとき、はじめから情報セキュリティに関するものか否かを区別するとは限らない。
MSS共通か	共通。MSS共通テキストの変更を反映するもの。
要求事項の追加・変更	なし。要求する手順の追加を要求事項の追加・変更と見ることもできる。ただし、結果として決定（特定）する利害関係者の要求事項は情報セキュリティ/ISMSに関するものであって変わらない。

1.5.3「4.4 情報セキュリティマネジメントシステム」

変更箇所	4.4
変更内容	ISMSの確立、実施、維持及び継続的な改善の要求事項である。ISMSに、必要なプロセス及びプロセス間の相互作用（interactions）を含むことを追加した。
変更の主旨	前版においても、要求事項への対応は、多くはプロセスとして実施される。ISMSは、プロセス及びプロセスの間の相互作用を含んでいる。改定における追加は、このことを明示したものである。
MSS共通か	共通。MSS共通テキストの変更を反映するもの。
要求事項の追加・変更	なし。 組織がISMSにおけるプロセスを一層明確に意識する契機になり得る。

1.5.4「5.1 リーダーシップ及びコミットメント」

変更箇所	注記
変更内容	この規格における「事業」(“business”) の意味を説明する注記を追加した。
変更の主旨	MSS共通テキストにおける注記の追加を反映する変更である。ただし、以下の問題がある。MSS共通テキストでは、5.1 b) に “the organization’s business processes” という記述がある。しかし、ISO/IEC 27001:2013 及び ISO/IEC 27001:2022 では、この箇所を “the organization’s processes” としている。このため、注記で説明している語 business がこの文書にはない。
MSS共通か	共通。MSS共通テキストへの追加を反映するもの。
要求事項の追加・変更	なし。

1.5.5「5.3 組織の役割、責任及び権限」

変更箇所	5.3 第1文
変更内容	情報セキュリティに関連する責任及び権限の割当てと伝達に関する、トップマネジメントに対する要求事項である。伝達について「組織内で」(within the organization) を追加した。
変更の主旨	ISO/IEC 27001:2013 において、MSS共通テキストにおける「組織内で」を含めなかった。改定にあたってMSS共通テキストにあわせた。
MSS共通か	この変更によりMSS共通テキストに一致する。
要求事項の追加・変更	組織外への伝達を除外するという、要求事項の縮小である。したがって、ISMSの活動を継承しながら ISO/IEC 27001 の改定によってこの点で不適合になることはない。

1.5.6「6.1.3 情報セキュリティリスク対応」c)

変更箇所	6.1.3 c), 注記1, 注記2　（改定版における注記2, 注記3）
変更内容	この二つの注記では、情報セキュリティリスク対応に関連付けて附属書A とその使い方を説明している。この説明記事から管理目的の記述を削除した。
変更の主旨	ISO/IEC 27002:2013 では、管理策の上位に管理目的 (Control objective) があった。ISO/IEC 27002:2022 では、管理策ごとに、管理策に関する説明の1項目として目的 (Purpose) を設けた。これによって、附属書Aから管理目的の記述が無くなった。この変更を受けた注記の変更である。
MSS共通か	ISO/IEC 27001 に固有。
要求事項の追加・変更	なし。

1.5.7「6.1.3 情報セキュリティリスク対応」d)

変更箇所	6.1.3, d)
変更内容	ここでは、適用宣言書に含める事項を列挙している。その表現を整備した。 発行済の Corrigendum (正誤表) を吸収する変更である。
変更の主旨	ISO/IEC 27001:2013, Corrigendum 2 (正誤表 2) を反映した。
MSS共通か	ISO/IEC 27001 に固有。
要求事項の追加・変更	なし。

1.5.8「6.2 情報セキュリティ目的及び それを達成するための計画策定」d)

変更箇所	6.2, d)
変更内容	情報セキュリティ目的に関する要求事項を列挙する中に、「d) (情報セキュリティ目的を)監視する」を追加した。
変更の主旨	MSS共通テキストの改定を反映した。
MSS共通か	共通。
要求事項の追加・変更	追加。

1.5.9「6.2 情報セキュリティ目的及び それを達成するための計画策定」g)

変更箇所	6.2, g)
変更内容	情報セキュリティ目的に関する要求事項を列挙する中に、「g) 文書化した情報として利用可能な状態にする」を追加した。
変更の主旨	MSS共通テキストの改定を反映した。
MSS共通か	共通。
要求事項の追加・変更	追加。 ISOIEC 27001:2013 でも、この直後の文で、情報セキュリティ目的に関する文書化した情報を保持することを求めている。要求事項の追加は、「利用可能な状態にする」ことである。

1.5.10「6.3 変更の計画策定」

変更箇所	6.3
変更内容	細分箇条 6.3 を追加した。
変更の主旨	MSS共通テキストの改定を反映して、ISMSの変更を行う場合に、計画的に行うべきことを追加した。
MSS共通か	共通。
要求事項の追加・変更	追加。

1.5.11「7.4 コミュニケーション」

変更箇所	7.4, d), e)　（改定版における 7.4, d) ）
変更内容	コミュニケーションの必要性の決定を求める要求事項においてその a) 内容、b) 実施時期、c) 対象者 等を列挙する中で、 d) コミュニケーションの実施者 e) コミュニケーションの実施プロセス の2項目をまとめて、 d) コミュニケーションの方法　にした。
変更の主旨	ISO/IEC 27001:2013 では、MSS共通テキストと異なるテキストとしていた。これを、MSS共通テキストにあわせる変更である。
MSS共通か	共通。
要求事項の追加・変更	形式的には要求事項の変更に見える。「実施者」と「実施プロセス」は「方法」と同等であり実質的な変更はないと見られる。

1.5.12「8.1 運用の計画策定及び管理」第1段落

変更箇所	8.1 第1段落
変更内容	第1文の変更： ・「箇条6で決定した活動を実施するために」 ←「箇条6.1で決定した活動を実施するために」 ・計画策定及び管理の方法を追加：「ー プロセスに関する基準の設定」、「ー その基準に従った、プロセスの管理の実施」 前版の第2文（「6.2で決定した情報セキュリティ目的・・」）を削除
変更の主旨	箇条6（計画）を受けて箇条8でその実施を求めることを、6.1.2 と 8.2、6.1.3 と 8.3 の対応も含めて、包括的に表現した。
MSS共通か	共通。ISO/IEC 27001:2013 における固有の記述を解消した。
要求事項の追加・変更	MSS共通テキストで一般的な表現を採っている部分である。 前版との対応も、一般的な要求事項として同等と見られる。 追加された2項目は、実施方法を定めている点で要求事項を追加しているとも見られる。また、8.2及び8.3は、MSS共通テキストに沿って8.1に追加された2項目をISO/IEC 27001 において具体化しているという側面もある。

1.5.13「8.1 運用の計画策定及び管理」第4段落

変更箇所	8.1, 第4段落
変更内容	・管理対象について: 「外部から提供されるプロセス、製品又はサービスが」←「外部委託したプロセスが決定され、かつ、」 ・管理する範囲がISMSに関連するものであることを明示した。
変更の主旨	MSS共通テキストの変更を反映した。本来、外部から提供される製品及びサービスも管理すべきである。
MSS共通か	共通。
要求事項の追加・変更	外部から提供される製品及びサービスの管理を要求事項として追加した。 ISO/IEC 27002:2013, 同2022における供給者関係についての管理策（ISO/IEC 27002:2022, 5.19 他）で製品及びサービスの調達を扱っていることと整合する ISO/IEC 27001 の変更である。

1.5.14「9.1 監視、測定、分析及び評価」第1段落

変更箇所	9.1 第1段落 b)
変更内容	監視，測定，分析及び評価の方法に関する注記を本文に移した。
変更の主旨	MSS共通テキストの変更を反映した。 注記には推奨事項（recommendation,「～することが望ましい」として表現）を書くことができない。これを解消するための修正である。
MSS共通か	共通。
要求事項の追加・変更	なし。

1.5.15「9.1 監視、測定、分析及び評価」第3段落

変更箇所	9.1 第3段落、前版の9.1第1文
変更内容	情報セキュリティパフォーマンス及びISMSの有効性の評価を要求する文を、9.1 の冒頭から最後に移した。
変更の主旨	MSS共通テキストの変更を反映した。 監視・測定・分析・評価というサイクルの最後にある、評価に関する要求事項である。また、評価の対象がマネジメントの指標の中でも上位にある、情報セキュリティパフォーマンス及びISMSの有効性であり、総括する要求事項として 9.1 の最後にあることが自然である。
MSS共通か	共通。
要求事項の追加・変更	なし。

1.5.16「9.2 内部監査」

変更箇所	9.2
変更内容	9.2 の内容を維持しつつ、二つの細分箇条「9.2.1 一般」及び「9.2.2 内部監査プログラム」に分けて構成を明確にした。 9.2.2 の記述をMSS共通テキストにあわせた。その内容は ISO/IEC 27001:2013, 9.2 に合致しており、改定において内容をすべて継承している。
変更の主旨	MSS共通テキストの変更を反映した。
MSS共通か	共通。
要求事項の追加・変更	なし。構成の明示のみ。

1.5.17「9.3 マネジメントレビュー」

変更箇所	9.3
変更内容	9.3 の内容を維持しつつ、三つの細分箇条「9.3.1 一般」、「9.3.2 マネジメントレビューへのインプット」及び「9.3.3 マネジメントレビューの結果」に分けて構成を明確にした。 マネジメントレビューのインプット（9.3.2）に、利害関係者のニーズ及び期待の変化を追加した。
変更の主旨	MSS共通テキストの変更を反映した。
MSS共通か	共通。
要求事項の追加・変更	追加。 マネジメントレビューのインプットに、利害関係者のニーズ及び期待の変化を追加した。

1.5.18「10 改善」

変更箇所	細分箇条の順序
変更内容	前版における「10.1 継続的改善」と「10.2 不適合及び是正処置」の順序を入れ替えた。
変更の主旨	MSS共通テキストの変更を反映した。
MSS共通か	共通。
要求事項の追加・変更	なし。

1.5.19 全般

変更箇所	「文書化した情報を保持する」
変更内容	各所で、上記要求事項を「文書化した情報を利用可能な状態にする」に変えた。 文書化した情報を保持しているが利用可能でない、という状態を避けるための変更である。 なお、ISO/IEC 27001:2022 に固有のテキストには、「文書化した情報を保持する」という表現もある。
変更の主旨	MSS共通テキストの変更を反映した。
MSS共通か	共通。
要求事項の追加・変更	拡大。文書化した情報が存在するだけでなく、利用可能な状態にあることも求める。但し、前版から、7.5.3 a) においてすべての文書化した情報について「入手可能（利用可能）かつ利用に適した状態」であることを求めていたため、要求事項の追加はないとも読める。

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2022

抜 粋

ISO/IEC 27001 改定内容と関連規格の動向

2022年12月16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