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2024

ISO/IEC 27001:2022 における気候変動への対応について

2024年12月

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

はじめに

2024年2月に、ISOのそれぞれのマネジメントシステム規格に追補（Amendment）が発行され、気候変動に関係する規定が追加されました。

本講演では、ISO/IEC 27001 を題材に、

- 追補発行の経緯
- 追補の内容
- その解釈と適用における留意点

について解説します。

追補への対応を今一度確認するための材料になれば幸いです。

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。

講演の要点

1. ISO/IEC 27001 追補の背景：
   i. 気候変動への国連の取り組み
   ii. これに呼応するISOの活動
2. ISO/IEC 27001:2022「4.1 組織及びその状況の理解」と追補の解釈と適用
3. 気候変動の原因への働きかけと結果への対応を区別すること
4. 気候変動に対する組織の取組みと、ISMSの活動を区別すること

＜参考＞ 関連文書

[1] ISO/IEC Directives, Part 1:2024

Procedures for the technical work — Consolidated ISO Supplement — Procedures specific to ISO

Annex SL Appendix 2 (normative)
Harmonized structure for MSS with guidance for use

https://www.iso.org/directives-and-policies.html

読者： マネジメントシステム規格開発者

[2] ISO Guide 84:2020

Guidelines for addressing climate change in standards

読者： ISO規格開発者

[3] ISO 9001 Auditing Practices Group Guidance on:
Auditing Climate Change issues in ISO 9001

読者： ISO 9001 認証機関、審査員向け

これらは本講演の準備にあたって参考にした文書です。本講演を理解する上では必須ではありません。

気候変動とは

気候変動とは

- 気温および気象パターンの長期的な変化
  1. 自然現象
  2. 人間活動によるもの
     原因：　化石燃料（石炭、石油など）の燃焼によるCO_2排出、その他の温室効果ガスの生成・排出など

参考：国連広報センターウェブページ

https://www.unic.or.jp/
https://www.unic.or.jp/activities/economic_social_development/sustainable_development/climate_change_un/what_is_climate_change/

国連における気候変動への主な取り組み

- 国連気候変動枠組条約締約国会議（COP）
  - COP21においてパリ協定を採択、2015年12月
    - 産業革命前に比べた地球平均気温上昇限度の目標等。
      https://unfccc.int/process-and-meetings/the-paris-agreement
- 国連開発計画
  - 気候変動への適応及びレジリエンスに関する行動の呼びかけ
    https://www.adaptation-undp.org/about
- 持続可能な開発目標（SDGs）
    https://sdgs.un.org/goals
  - 2015年9月
  - 17の目標の中で、「目標13 気候変動に具体的な対策を」

ISOにおける気候変動への対応

国連における気候変動への対応を背景に、
2021年9月、ISOは気候変動への取組み方針を
ロンドン宣言として表明した。

https://www.iso.org/ClimateAction/LondonDeclaration.html

ロンドン宣言の主旨：

ISOは、国際規格及び出版物を通して、以下の達成を促進する。

- パリ協定
- 持続可能な開発目標（SDGs）
- 気候変動への適応及びレジリエンスに関する行動の呼びかけ

マネジメントシステム規格における気候変動への対応

ロンドン宣言を実践する活動の一つとして、2024年2月に、ISOのマネジメントシステム規格に気候変動への対応を追加

1. マネジメントシステム規格に適用する共通の構造（共通の箇条構成、用語及び定義、テキストを含む）の規定（＊）に、気候変動への対応に関する規定を追加した。

   ＊ ISO/IEC Directives, Part 1, Annex SL

2. 2024年2月に、上述の規定を、ISO 9001、ISO 14001、ISO/IEC 27001 を含むそれぞれのマネジメントシステム規格に追補（Amendment）として反映した。

本講演では、本追補の解釈と適用について解説する。

規格：ISO/IEC 27001:2022, 4.1（既存） (1/3)

「4.1 組織及びその**状況**の理解」
Understanding the organization and its **context**

要求事項の主旨

組織の外部及び内部の**課題（issues）**を決定する。課題は、ISMSの目的の達成に関係するもの。

注記の主旨

「**課題（issues）**の決定」とは、ISO 31000:2018, 5.4.1における「**状況（context）**の確定」のこと。

※　規定は標準文書を参照のこと。

規格：ISO/IEC 27001:2022, 4.1（既存） (2/3)

「課題」には、組織自身で解決できるもの、又は解決すべきものとの語感がある。翻訳において避けられない違和感があるが、・・・

この要求事項において、

- 課題（issues）は、状況（context）に近い意味を持ち、「ISMSの活動において前提や与件となる状況」

要求事項の意味：

ISMSの活動において前提や与件となる、かつ、ISMSの目的の達成に関係する、組織の内部及び外部の状況を特定する。

規格：ISO/IEC 27001:2022, 4.1（既存） (3/3)

この要求事項は抽象度が高く、解釈の自由度が高い中で、

外部の状況（課題）の例

- 自然環境、地域の立地
- 法令：　輸出規制、消費者保護、等々
- 国の経済活動・産業政策
- 業界の状況、事業の競争環境

内部の状況（課題）の例

- 組織の方針・目標、業績、内部組織、人員、能力

※ ISO 31000:2018 (JIS Q 31000:2019)「5.4.1 組織及び組織の状況の理解」における例示も参考になる。

規格：ISO/IEC 27001:2022, 4.1 追補　(1/2)

「4.1 組織及びその状況の理解」

追補の主旨：
気候変動が関連する（relevant =直前の要求事項における）課題（issue）であるか否かを決定する。

- 組織にとって新しい要求事項である。求められることは：
  1. 4.1の文脈における課題であるか否かを決定すること。決定したことを示すこと。
  2. 課題であるとすると決定した場合、その内容と対応を明らかにすること。
- 気候変動は外部の状況の一つであり、追補がなくても、気候変動を課題とすることができた。この点では、追補は既存の要求事項に含まれている。
- 組織にとって新しい種類の要求事項である。「課題であるか否かを決定する」ことが明示的に要求事項とされているのは、気候変動だけ。
- 追補は、ISMSに関連して、気候変動への対応を再確認する契機になる。

規格：ISO/IEC 27001:2022, 4.1 追補　(2/2)

「4.1 組織及びその状況の理解」

本文にあわせて「課題」を「前提や与件」に置き換え、追補において直前の要求事項の言葉を使うと、

既存の要求事項と追補の意味：

ISMSの活動において前提や与件となる、かつ、ISMSの目的の達成に関係する、組織の内部及び外部の状況を特定する。（スライド10より）

気候変動が、ISMSの活動において前提や与件となる、かつ、ISMSの目的の達成に関係する、組織の外部の状況であるか否かを決定する。（追補）

規格：ISO/IEC 27001:2022, 4.2 及び追補

「4.2 利害関係者のニーズ及び期待の理解」

- 利害関係者の要求事項の中で、ISMSで取り組むものを決定する。　　※　規定は標準文書を参照のこと。

追補により、ここに注記を追加

> 追補（注記）の主旨：
> 利害関係者の要求事項は、気候変動に関係するものを含んでいる場合がある。

- 注記はISMSの要求事項ではないが、審査において、決定した利害関係者の要求事項があればそれが何であるかについて問われることも考えられる。

気候変動への二つの取り組み：　一般　(1/2)

1. 気候変動を人類の課題と認識し、国、社会、組織、人々がこれに取り組む。
   a. 気候変動を抑制するために、原因に働きかける。
      ・・・ COP21：温室効果ガス排出の管理　等
   b. 気候変動の結果に国、社会、組織、人々が適応する。
      気温上昇、海面上昇、激甚災害増加等に対処する。
      ・・・ SDGs 目標13「気候変動に具体的な対策を」 等

2. 気候変動の結果が組織にもたらす影響に組織が対処する。

   注　組織にもたらす影響を低減するために、組織が気候変動の原因に働きかける（温室効果ガス排出を削減する）ことは、現実にはない。「2. a.」

気候変動への二つの取り組み：　一般　(2/2)

「1. 気候変動を人類の課題と認識し、これに取り組む。」という課題が喫緊のものであることは言うまでもない。

ただし、「1.b. 気候変動の結果に国、社会、組織、人々が適応する。」という活動は、組織がこれに貢献する場合でも、ISMSの活動に係る役割・責任において行うものではないことに留意する。

> 気温上昇、海面上昇、激甚災害増加等の地球規模の課題への対処に組織が貢献をする場合、この貢献は、ISMSの目的や情報セキュリティ目的はとは繋がりがなく、ISMSの活動において行うものではない。

次のスライドでは、ISMSに関係する「1. a.」及び「2.」についてさらに整理する。

気候変動への二つの取り組み： ISMS

	1. a. 人類の課題と認識し、原因に働きかける。	2. 結果が組織にもたらす影響に対処する。
ISOにおける活動	ロンドン宣言、マネジメントシステム規格の追補	---
ISMSにおける活動	気候変動を抑制するために原因に働きかける。	気候変動の結果がもたらす情報セキュリティリスクを特定し、対処する。
リスクマネジメントのプロセス（ISO 31000:2018）	特に、 「組織及びその状況の理解」	主にリスクアセスメント／リスク対応
ISO/IEC 27001:2022 で関係する事項	特に、 4.1 組織及びその状況の理解、 **同 追補（2024）**	主に　6.1.2 情報セキュリティリスクアセスメント 6.1.3 情報セキュリティリスク対応 8.2 情報セキュリティリスクアセスメント 8.3 情報セキュリティリスク対応
ISMSにおける 施策の例	温室効果ガス排出の少ない手段を選ぶ。	気候変動の結果に応じて、情報及び施設・設備・装置・機器の可用性を確保する管理策を実施する。
追補との関係	追補で「課題（前提や与件）とするか否かの決定」を求めている活動	ISOのロンドン宣言を背景とする追補とは別の、組織自身のための活動

組織の活動とISMSの関係

ISMSにおいて、気候変動を人類の課題と認識し、原因に働きかける取組み[1.a.]は、組織全体の取組みと整合性を持つこと。

- 組織全体の取組みをISMSにも適用する。ISMSに固有の取組みは、例が少ないかもしれない。
  - 例1　情報システム関係設備は、電力消費の少ないものを選ぶ。
  - 例2　製品・サービスの選定は、供給者の気候変動への取組みを考慮した組織全体の調達基準・手続きに従う。
- 追補適用についての説明例：
  - 「温室効果ガス排出抑制についての組織全体の方針、規則及び手続きが、ISMSの活動にも適用される。該当する方針、規則及び手続きに、組織の『製品・サービス調達方針及び規則』がある。」

まとめ (1/2)

1. ISO/IEC 27001:2022 追補の発行

   2024年2月に、ISO/IEC 27001:2022 追補が発行された。背景に、国連における気候変動対応の活動と、これに沿うISOの『ロンドン宣言』がある。

2. 追補で加えた要求事項

   気候変動に関する事項が、箇条4に本文と注記として追加された。気候変動がISMSにおける組織の課題であるか否かを決定することが、追加の要求事項である。

まとめ (2/2)

3. 気候変動の原因に働きかける活動　「1. a.」

国連における気候変動対応、ISOのロンドン宣言を背景とする活動。

例えば、ISMSの活動における製品やサービスの調達に際して、環境負荷を考慮する。この考慮は、多くの場合、組織全体の気候変動への取組みの一部に位置づけられるのではないか。

4. 気候変動の結果への対応　「2.」

気候変動の結果が組織自身にもたらす影響への対応は、ISO/IEC 27001箇条6及び箇条8に規定する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要求事項に基づき決定し、実施する。

対応の内容は、「情報及び施設・設備・装置・機器の可用性の確保」である。

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2024

ISO/IEC 27001:2022 における気候変動への対応について

2024年12月

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