日本 ISMS ユーザグループ／日本ネットワークセキュリティ協会 主催
情報セキュリティマネジメント・セミナー2024

ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説

2024年12月6日
NTTテクノクロス株式会社
土屋 直子
ISO/IEC JTC1 SC27 WG1国内委員会委員

目次

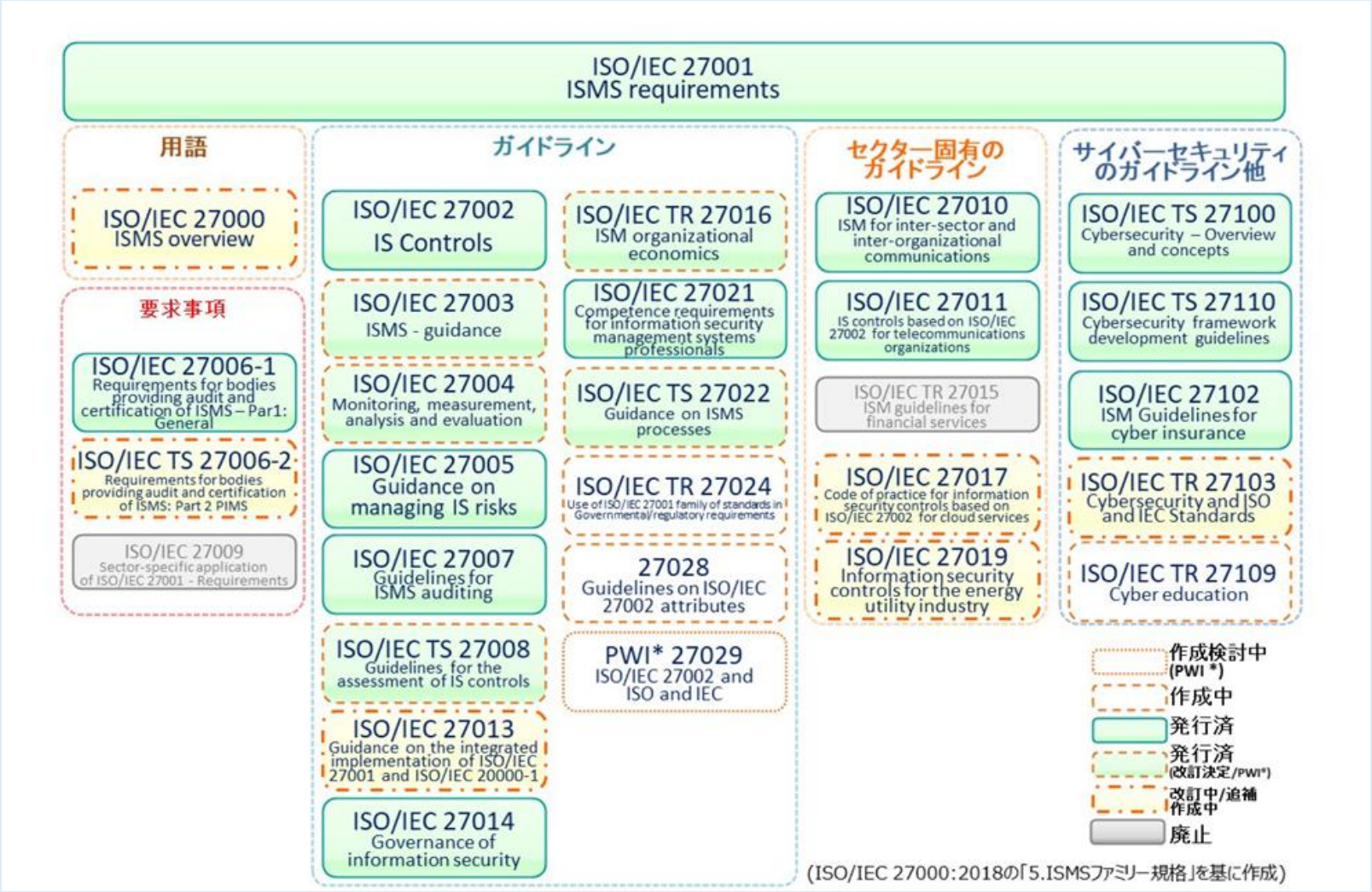
目次

ISO規格が発行されるまで

国際標準化組織
JTC 1: 情報技術
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

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

ISO/IEC 27000 関連規格とは



出典：JIPDEC「ISO/IEC 27000 ファミリー規格について」（2024年6月14日）
https://www.jipdec.or.jp/project/smpo/u71kba000000jjgv-att/27000family_20240614.pdf

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

ISO/IEC 27000 関連規格の改訂

ISO/IEC 27002:2022とISO/IEC 27001:2022改訂を受けて、
その他のISO/IEC 27000 関連規格が順次、改訂中

ISO/IEC 27002:2022（情報セキュリティ管理策）
ISO/IEC 27001:2022（ISMS-要求事項）
ISO/IEC 27005:2022（情報セキュリティリスクマネジメント指針）

ISO/IEC 27006-1:2024（ISMSの審査及び認証を行う機関向け要求事項）
ISO/IEC 27011:2024（通信事業者向け情報セキュリティ管理策）
ISO/IEC 27019:2024（エネルギー業界向け情報セキュリティ管理策）

ISO/IEC 27017（クラウドサービス向け情報セキュリティ管理策）**【DIS】**
ISO/IEC 27103（サイバーセキュリティとISO/IEC規格）**【DIS】**
ISO/IEC 27000（ISMS-概要及び用語）**【CD】**
ISO/IEC 27008（情報セキュリティ管理策の評価ガイドライン）**【CD】**
ISO/IEC 27003（ISMS-指針）**【WD】**
・・・

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

ISO/IEC 27000 関連規格 改訂状況

規格番号	発行年	規格内容	改訂段階
27000	2018年	ISMS-概要及び用語	CD
27001	2022年	ISMS-要求事項	**Amd1:2024**
27002	2022年	情報セキュリティ管理策	
27003	2017年	ISMS-指針	WD
27004	2016年	情報セキュリティマネジメント - 監視、測定、分析及び評価	WD
27005	2022年	情報セキュリティリスクマネジメント指針	
27006-1	**2024年**	ISMSの審査及び認証を行う機関向け要求事項	
27006-2 （WG5）	2021年	ISMSの審査及び認証を行う機関向け要求事項 - 第2部 プライバシー情報マネジメントシステム （ISO/IEC 27701認証対応）	
27007	2020年	ISMS監査ガイドライン	PWI
TS 27008	2019年	情報セキュリティ管理策の評価ガイドライン	CD
27009	2020年	ISO/IEC 27001の分野固有の適用の要求事項	廃止
27010	2015年	セクター間及び組織間のコミュニケーションのための 情報セキュリティマネジメント	

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

ISO/IEC 27000 関連規格 改訂状況

規格番号	発行年	規格内容	改訂段階
27011	**2024年**	通信事業者向け情報セキュリティ管理策	
27013	2021年	ISO/IEC 27001とISO/IEC 20000-1の統合実装のための指針	**Amd1:2024**
27014	2020年	情報セキュリティガバナンス	
TR 27016	2014年	情報セキュリティマネジメントの組織活動の経済性	
27017	2015年	クラウドサービス向け情報セキュリティ管理策	DIS
27018 （WG5）	2019年	PIIプロセッサとして作動するパブリッククラウドにおける 個人識別可能情報(PII)の保護のための実践の規範	DIS
27019	**2024年**	エネルギー業界向け情報セキュリティ管理策	
27021	2017年	ISMS専門家のための力量の要求事項	Amd1:2021
TS 27022	2021年	ISMSプロセスの指針	
TR 27024	（開発中）	政府及び規制上の、ISO/IEC 27001、ISO/IEC 27002、 及びその他の情報セキュリティ規格の利用	CD
27028	（開発中）	ISO/IEC 27002の属性の指針	DIS
27029	（開発中）	ISO/IEC 27002とISO/IEC規格	Committee Document
27701 （WG5）	2019年	プライバシー情報マネジメントのためのISO/IEC 27001及びISO/IEC 27002への拡張―要求事項及びガイドライン	DIS

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

ISO/IEC 27000 関連規格 改訂状況

規格番号	発行年	規格内容	改訂段階
TS 27100	2020年	サイバーセキュリティー概要及び概念	
27102	2019年	情報セキュリティマネジメントーサイバー保険のためのガイドライン	
TR 27103	2018年	サイバーセキュリティとISO/IEC規格	DIS
TR 27109	(開発中)	サイバーセキュリティの教育・訓練	AWI
TS 27110	2021年	サイバーセキュリティフレームワーク開発のためのガイドライン	

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

ISO/IEC 27000 関連規格 改訂トピックス

- **ISO/IEC 27001:2022/Amd 1:2024**
  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
  －情報セキュリティマネジメントシステム－要求事項
  追補1－気候変動対応

【概要】

2021年9月に、国連における気候変動対策の活動を背景として
ISOが『ロンドン宣言』を表明。
それを具体化する施策の一つとして、
2024年2月にISOのマネジメントシステム規格に追補が発行され、
気候変動への対応に関する規定が追加された。

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

ISO/IEC 27000 関連規格 改訂トピックス

- **ISO/IEC 27017　【DIS】**
  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
  – 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

【概要】

ISO/IEC 27017のベースである
ISO/IEC 27002が2022年に改訂されたの受け、
ISO/IEC 27017をISO/IEC 27002:2022にそろえるために改訂中。
クラウドサービスを取り巻く脅威や技術動向を
改訂版ISO/IEC 27017に反映する方向。

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

ISO/IEC 27000 関連規格 改訂トピックス

- **ISO/IEC 27028　【DIS】**
  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
  ーISO/IEC 27002の属性の指針

【概要】

ISO/IEC 27002:2022で採用された
「属性（Attribute）」に関するガイドライン規格を開発中。
属性の使い方や属性の例に関するガイダンスを含める方向で開発中。

まとめ（ 1. ISO/IEC 27000 関連規格の動向）

- ISO/IEC 27002:2022とISO/IEC 27001:2022改訂の改訂を受けて、ISO/IEC 27000 関連規格が順次、改訂されている
- ISO/IEC 27017（クラウドセキュリティ）改訂は現在DIS
- ISO/IEC 27028（ISO/IEC 27002の属性の指針）など
  いくつかの規格が新規に開発中

1. ISO/IEC 27000 関連規格の動向

2. ISO/IEC 27002 ポイント解説

2-(1) 2013年版からの留意すべき変更点

2-(2) 管理策をより深く理解するための視点

2-(1) 2013年版からの留意すべき変更点

本講演の2-(1)では、2013年版からの留意すべき変更点として、
用語を取り上げて解説します。

2-(1) 2013年版からの留意すべき変更点
A.　英用語の留意点
B.　JIS訳語の留意点

※ISO/IEC 27001:2022、ISO/IEC 27002:2022改訂についての参考資料
情報セキュリティマネジメント・セミナー
https://www.jnsa.org/seminar/std/isms/2023/index.html
https://www.jnsa.org/seminar/2022/isms2022/index.html
https://www.jnsa.org/seminar/2021/isms2021/index.html

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

A.英用語の留意点

英用語の留意すべき変更例

No.	ISO/IEC 27002:2013		ISO/IEC 27002:2022	
1	employee	従業員	personnel	要員
2	information, other assets associated with information and information processing facilities	情報，情報に関連するその他の資産及び情報処理施設	information and other associated assets	情報及びその他の関連資産
3	information security continuity	情報セキュリティ継続	information security during disruption	事業の中断・阻害時の情報セキュリティ
4	secret authentication information	秘密認証情報	- authentication information - secret authentication information	・認証情報 ・秘密認証情報 ※上記2用語の使い分け
5	teleworking	テレワーキング	remote working	リモートワーク
6	mobile device	モバイル機器	- user end point device - mobile device	・利用者エンドポイント機器 ・モバイル機器 ※上記2用語の使い分け

上記No.1～３について、次頁以降で解説します。

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

A.英用語の留意点（例-No.1）

No.	ISO/IEC 27002:2013	ISO/IEC 27002:2022
1	employee　従業員	personnel　要員

2013年版では、「従業員（employee）」という表現が使われていた。

2022年版では、「従業員」には含まれていなかった、経営陣、トップマネジメント、派遣社員、ボランティアなども含む表現として、「要員（personnel）」という表現が使われている。

例）
6.3 情報セキュリティの意識向上、教育及び訓練
　（要員に対する教育・訓練）
6.8 情報セキュリティ事象の報告
　（要員による情報セキュリティ事象の報告）

A.英用語の留意点（例-No.2）

No.	ISO/IEC 27002:2013		ISO/IEC 27002:2022	
2	information, other assets associated with information and information processing facilities	情報，情報に関連するその他の資産及び情報処理施設	information and other associated assets	情報及びその他の関連資産

2013年版では、情報及び関連資産を網羅的に指す表現として、
「情報，情報に関連するその他の資産及び情報処理施設」
という表現が使われていた。

2022年版では、「情報及びその他の関連資産」と表現を簡明にした。
対象とする資産の範囲や意味に変更はない。

例）
5.9 情報及びその他の関連資産の目録
（旧8.1.1 資産目録）
5.10 情報及びその他の関連資産の許容される利用
（旧8.1.3 資産利用の許容範囲）

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

A.英用語の留意点（例-No.3）

No.	ISO/IEC 27002:2013		ISO/IEC 27002:2022	
3	information security continuity	情報セキュリティ継続	information security during disruption	事業の中断・阻害時の情報セキュリティ

2013年版では、「情報セキュリティ継続」という表現が使われていた。
一般的に広く使われている「事業継続」という用語と比べ、
「情報セキュリティ継続」という用語は、
ISO/IEC 27002:2013でしか使われておらず、わかりづらいとして、
2022年版では、「事業の中断・阻害時の情報セキュリティ」という一般的な表現を採用した。

例）
5.29 事業の中断・阻害時の情報セキュリティ
（旧17.1 情報セキュリティ継続）

B.JIS訳語の留意点

JIS訳語の留意すべき変更例

No.	ISO/IEC 27002:2022	JIS Q 27002:2014	JIS Q 27002:2024
1	management	・経営陣（主に）	・経営陣 ・管理層 ※上記2訳語の使い分け。以下、同様。
2	information processing facility	・情報処理施設（主に）	・情報処理施設 ・情報処理設備 ・情報処理施設・設備
3	- device - equipment	・機器 ・装置	・装置 ・機器 ・装置・機器
4	disruption	・故障 ・中断	・事業の中断・阻害 ・中断・阻害 ・中断
5	personally identifiable information	・個人を特定できる情報	・個人識別可能情報
6	identity	・識別情報 ・本人 ・ID	・識別情報 ・本人 ・アイデンティティ

上記No.1～３について、次頁以降で解説します。

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

B.JIS訳語の留意点（例-No.1）

No.	ISO/IEC 27002:2022	JIS Q 27002:2014	JIS Q 27002:2024
1	management	・経営陣（主に）	・経営陣 ・管理層

“management”のJISにおける和訳を、
一部、「経営陣」から「管理層」に変更した。

トピック固有の方針の承認や、要員に対するトピック固有の方針を含む方針群の情報セキュリティの適用の責任は、
経営陣だけではなく管理層も含むため。

例）
5.1 情報セキュリティのための方針群
（管理層によるトピック固有の方針の承認）
5.4 管理層の責任（旧7.2.1 経営陣の責任）(Management responsibilities)
（要員に対するトピック固有の方針を含む方針群の
情報セキュリティの要求）

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

B.JIS訳語の留意点（例-No.2）

No.	ISO/IEC 27002:2022	JIS Q 27002:2014	JIS Q 27002:2024
2	information processing facility	・情報処理施設（主に）	・情報処理施設 ・情報処理設備 ・情報処理施設・設備

“information processing facility”は、
建屋だけでなく、情報システム、ネットワーク及びその構成要素を含む。

したがって、以下のように訳し分けた。

「情報処理施設」：建屋の場合

「情報処理設備」：情報システムやネットワークなどの設備の場合

「情報処理施設・設備」：上記、両方を含む場合

例）
8.14 情報処理施設・設備の冗長性
（旧17.2.1情報処理施設の可用性）
（建屋だけでなく、ネットワークやその他の設備の冗長性）

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

B.JIS訳語の留意点（例-No.3）

No.	ISO/IEC 27002:2022	JIS Q 27002:2014	JIS Q 27002:2024
3	- device - equipment	・機器 ・装置	・装置 ・機器 ・装置・機器

“device”、”equipment”は、意味の範囲に重なりがあるため、
いずれの英用語でも、以下のように訳し分けた。

「機器」：小型で持ち運ぶものの場合（ノートPC、タブレット、スマートフォン、など）

「装置」：固定の場所に備え付けるものの場合（アンテナ、ATM、サーバ、など）

「装置・機器」：上記、両方を含む場合

例）
7.9 構外にある資産のセキュリティ
（構外にある装置・機器のセキュリティ）

1. ISO/IEC 27000 関連規格の動向

2. ISO/IEC 27002 ポイント解説

2-(1) 2013年版からの留意すべき変更点

2-(2) 管理策をより深く理解するための視点

2-(2) 管理策をより深く理解するための視点

組織において、ISMSだけではなく、複数のフレームワークを活用したセキュリティ体制を構築する組織が増えています。

本講演の2-(2)では、改めて、ISMSの管理策を深く理解することで、他のフレームワークと対比させ、ISMSだけでなく他のフレームワークもより深く理解し、組織により合ったセキュリティ体制を構築するためのトピックを提供します。

※2-(2)は、2013年版からの変更点ではなく、
ISMSそのものの考え方の解説です。

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

ISMSにおける情報セキュリティ管理策の決定について

ISO/IEC 27001:2022
6.1.3 情報セキュリティリスク対応

組織は、

- **必要な全ての管理策**を決定する。
- 組織で設計、又は任意の情報源から管理策を特定することができる。
- 附属書A の管理策は、全てを網羅していない。
  必要な場合は、追加の管理策を含めることが可能。

「管理策」とは？

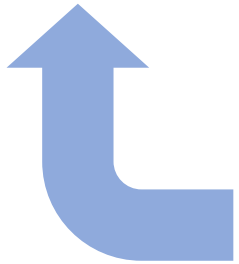
「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

ISO/IEC 27002:2022 における「管理策」の定義

ISO/IEC 27002:2022では、「管理策（control）」の定義を、ISO 31000:2018から引用している。

管理策（control）
リスクを維持及び／又は修正する対策

注釈1 管理策は，リスクを維持及び／又は修正するプロセス，方針，方策，実務
　　又はその他の条件及び／若しくは活動を含む。ただし，これらに限定されない。
注釈2 管理策が，常に意図又は想定した修正効果を発揮するとは限らない。
（出典：JIS Q 31000:2019 ）



管理策（control）
リスクを修正する対策

注釈1 管理策には，リスクを修正するためのあらゆるプロセス，方針，
　　仕掛け，実務及びその他の処置を含む。
注釈2 管理策が，常に意図又は想定した修正効果を発揮するとは限らない。
（出典：JIS Q 31000:2010 ）

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

管理策について

ISO/IEC 27002:2022

例）
5.14 情報の転送
5.18 アクセス権
7.2　物理的入退
8.10 情報の削除
8.24 暗号の利用
8.28 セキュリティに配慮した
　　コーディング
・・・

⇒リスクを修正する？

例）
5.1　情報セキュリティのため
　　の方針群
5.12 情報の分類
5.13 情報のラベル付け
8.17 クロックの同期
・・・

**⇒リスクを修正しないかも
しれないが、維持する？**

**様々な管理策が、組織の状況によって、
リスクを修正することも、リスクを維持することもありえる？**

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

「管理策」の語の用法

5.1 情報セキュリティのための方針群

管理策

属性

管理策タイプ	情報セキュリティ特性	サイバーセキュリティ概念	運用機能	セキュリティドメイン
#予防	#機密性 #完全性 #可用性	#識別	#ガバナンス	#ガバナンス及びエコシステム #レジリエンス

管理策（Control）

情報セキュリティ方針…は、これを定義し……　管理策

目的（Purpose）

…情報セキュリティに対する管理層の指示及び支援……するため。

手引（Guidance）

…方針群のより低いレベルでは…トピック固有の方針によって……　管理策

情報セキュリティ方針及びトピック固有の方針のレビューでは……　管理策

その他の情報（Other information）

……

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

ISMSにおける「管理策」の特徴

- ISMSに必須の管理策はある？ → **No**
- 重要なシステムの場合に必須の管理策はある？ → **No**
- 情報の重要度に応じた高中低等のレベル分けに分類された管理策はある？ → **No**

ISMSでは、**管理策は、組織のリスクアセスメントの結果により、組織が全て決定**する。

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

まとめ（2-(2) 管理策をより深く理解するための視点）

- 「管理策」はISO/IEC 27001:2022の附属書Aだけではない。
- ISO/IEC 27002:2022の手引の内容も「管理策」。

附属書Aだけでなく ISO/IEC 27002:2022の手引なども参考にしながら、組織にとって最適な情報セキュリティ対策（管理策）を決定するとよい。

「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」 NTTテクノクロス 土屋直子

全体まとめ

1. ISO/IEC 27000 関連規格の動向

2. ISO/IEC 27002 ポイント解説

2-(1) 2013年版からの留意すべき変更点

2-(2) 管理策をより深く理解するための視点

ご清聴ありがとうございました。