パネルディスカッション

討議テーマ

JISQ27001:2023への移行について

2023.12.18
JNSA 標準化部会
日本ISMSユーザグループ

パネリストのご紹介

パネリスト			パネリストの立場
ISMS-AC	**星 昌宏 氏**	一般社団法人情報マネジメントシステム認定センター(ISMS-AC)	**ISMSのその信頼性の向上と維持に向けて活動している認定機関としてのアドバイス**
SC27/WG1	**山下　真 氏**	ISO/IEC JTC1/SC27 WG1小委員会、WG4小委員会（国立研究開発法人 情報通信研究機構）	**標準化の観点でのアドバイス**
	土屋 直子 氏	ISO/IEC JTC1/SC27 WG1小委員会（NTTテクノクロス株式会社）	
ISMS-UG	**羽田 卓郎 氏**	日本ISMSユーザグループインプリメンテーション研究会｜ISO/IEC JTC1/SC27 WG1小委員会リエゾン（リコージャパン株式会社）	**規格を具体的に実装する上でのアドバイス**
	尾崎 幸彦 氏	日本ISMSユーザグループインプリメンテーション研究会副主査（株式会社Speee）	

モデレータ：魚脇 雅晴
（標準化部会 日本ISMSユーザグループ WGリーダー
（エヌ・ティ・ティ・コミュニケーションズ株式会社）

テーマ1（全体）

これからJISQ27001:2023への移行を検討する方へのアドバイス

（注意事項や効率化の観点）

マネジメントシステム認証、認定、相互承認

相互承認

認定機関(ISMS-AC) ⇔ 認定機関

ISO/IEC 17011

認定

ISO/IEC 17021-1、
ISO/IEC 27006

認証機関（審査機関）

認証

ISO/IEC 27001

被認証組織（企業等）

IAF（国際認定フォーラム）

ISO/IEC 27001:2022への移行に関する要求事項（IAF MD26）を策定

A-1

JIS Q 27001:2023 への移行(IAF MD26:2023)

■ 移行期間の基準日

ISO/IEC 27001:2022の発行月の月末(2022年10月末日)　※JIS発行日ではない

■ 認証機関の認定の移行（1年間）

2023年10月までに完了した。

■ 組織の認証の移行（3年間）

【移行期限】 2025年10月31日　※認証が決定されること

移行期限後は、JIS Q 27001:2014による認証は無効になる

※2024年5月以降に開始する初回認証、再認証では、必ずJIS Q 27001:2023を用いなければならない。

IAF MD26:2023(和訳)　https://isms.jp/doc/JIP-IMAC226-20.pdf

B-1

ISMS認証の移行について　標準化の観点から

ISO/IEC 27001:2022

- 移行にあたり、本文の要求事項の追加・変更に対応する。
  参考：　2022年12月 情報セキュリティマネジメント・セミナー資料（山下）
- 管理策採用・不採用の理由説明（適用宣言書）にとどまらず、管理策の採用範囲を含む情報セキュリティ対策を示すことが、ISMSの有効性を高めるために役立つ。
  - 適用宣言書のみでなく、仕様書等、他の文書も活用する。

ISO/IEC 27002:2022

- この規格を、素材集として活用する。「望ましい」は横に措いて。

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
NICT　山下 真（ISO/IEC JTC 1/SC 27/WG 1, WG 4）

C-1

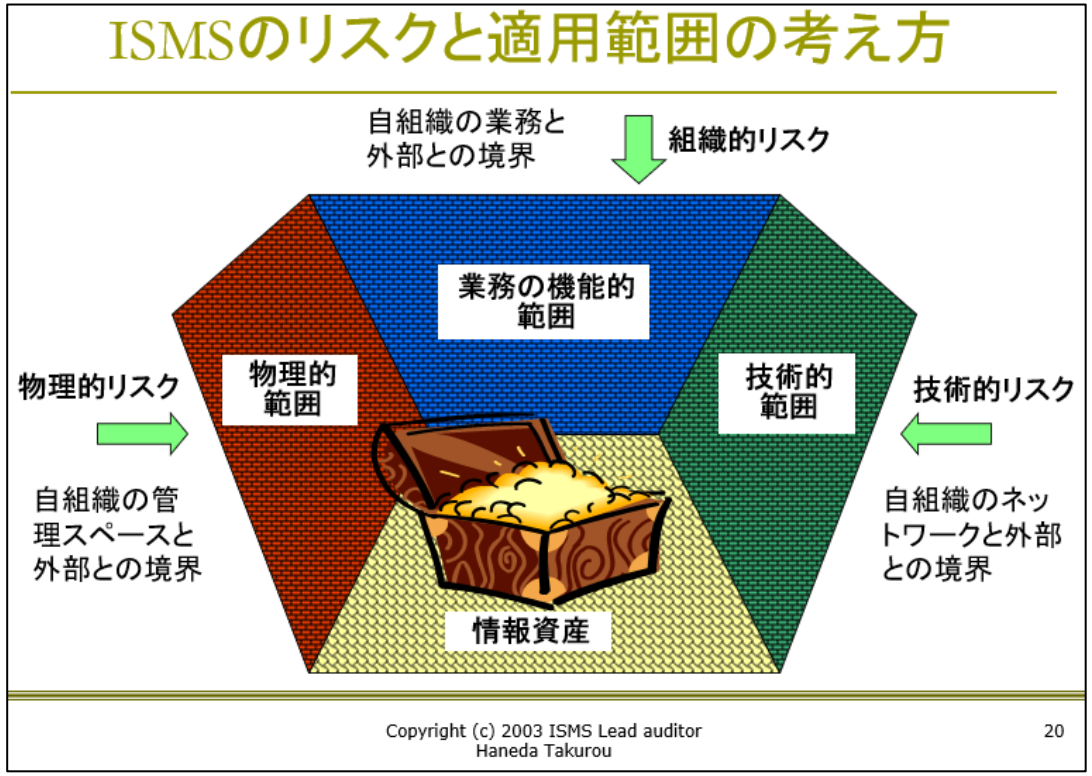
ISO/IEC 27001:2022
新規管理策の理解と対応

　附属書Aの管理策の分類のコンセプトが変更になり、これまでの14分類から4分類になったことで、管理策を一定のまとまりで理解することが難しくなった。そこで、旧分類のコンセプト（リスク対策の手段で分類）による14の属性を追加し、管理策を一定のまとまりで管理しやすくした。

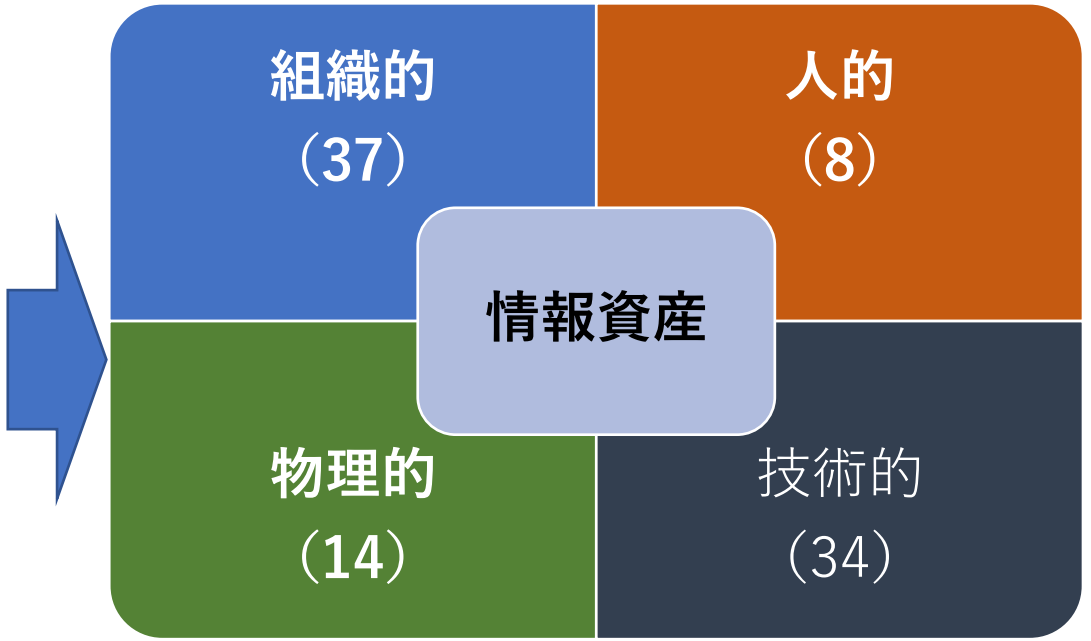
C-1

2022年版の27001附属書Aの分類はリスクベース

- **2003年作成の解説図⇒リスク対策の概念図**



- **2023年作成の附属書Aの解説図⇒リスクベースの分類**



※附属書Aの管理策は「リスク対策」である

C-1

2022年版の27001附属書Aに対策手段ベースの属性を追加

JIS Q 27001:2023(ISO/IEC 27001:2022) 付属書A			旧規格 管理策番号	管理対象 の属性
番号	参照 No	管理策名		
5	5.00	組織的管理策		
5.1	5.01	情報セキュリティのための方針群	A.5.1.1、A.5.1.2	① 組織管理
5.2	5.02	情報セキュリティの役割及び責任	A.6.1.1	
5.3	5.03	職務の分離	A.6.1.2	
5.4	5.04	管理層の責任	A.7.2.1	
5.5	5.05	関係当局の連絡	A.6.1.3	
5.6	5.06	専門組織との連絡	A.6.1.4	
5.7	5.07	脅威インテリジェンス	New	
5.8	5.08	プロジェクトマネジメントにおける情報セキュリティ	A.6.1.5、A.14.1.1	
5.9	5.09	情報及びその他の関連資産の目録	A.8.1.1、A.8.1.2	② 資産管理
5.10	5.10	情報及びその他の関連資産の許容される利用	A.8.1.3、A.8.2.3	
5.11	5.11	資産の返却	A.8.1.4	
5.12	5.12	情報の分類	A.8.2.1	
5.13	5.13	情報のラベル付け	A.8.2.2	
5.14	5.14	情報の転送	A.13.2.1、A.13.2.2、A.13.2.3	
5.15	5.15	アクセス制御	A.9.1.1、A.9.1.2	③ アクセス 権管理
5.16	5.16	識別情報の管理	A.9.2.1	
5.17	5.17	認証情報	A.9.2.4、A.9.3.1 A.9.4.3	
5.18	5.18	アクセス権	A.9.2.2、A.9.2.5、A.9.2.6	
5.19	5.19	供給者関係における情報セキュリティ	A.15.1.1	

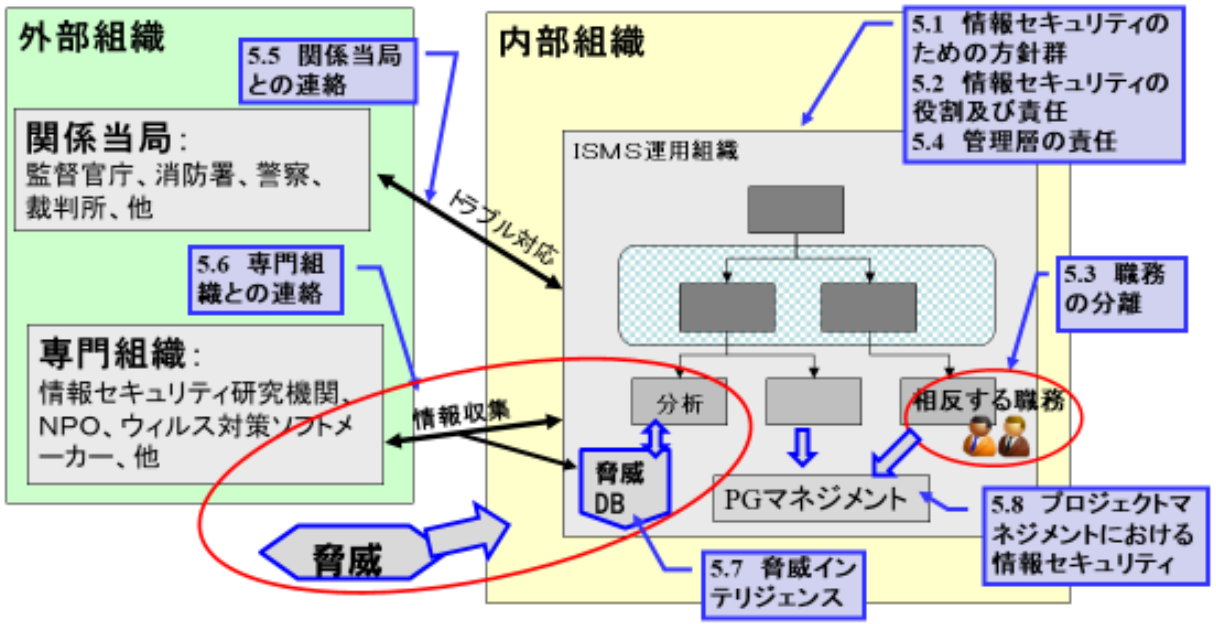
C-1

管理対象ベースのリスク管理モデル：例

第二章　JIS Q 27001:2023　管理策改定概要

II．管理策の改定内容と解説：組織管理

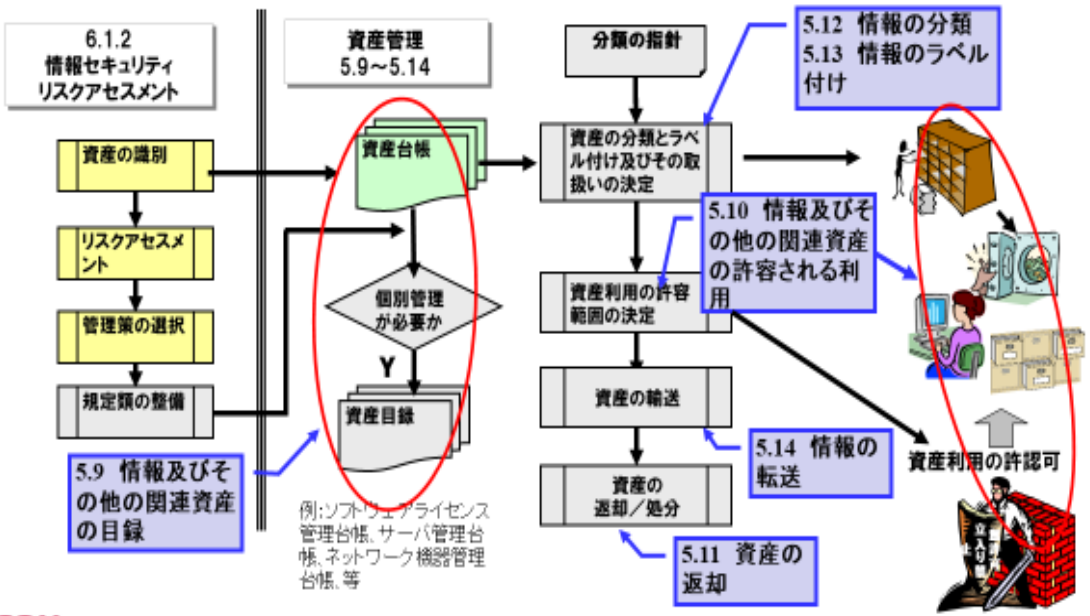
組織管理は、組織がISMSを構築し運用するための方針の確立と組織体制の確立を要求している。組織管理の管理策の実施は、本書第4章「箇条4　組織の状況、箇条 5.2 方針、箇条 5.3 組織の役割、責任及び権限、箇条 7.4 コミュニケーション」の要求事項にしたがってISMSの構築及び運用を行う上で不可欠の対応である。



第二章　JIS Q 27001:2023　管理策改定概要

II．管理策の改定内容と解説：資産管理

資産管理は、組織の資産（情報及び、情報を利用するうえで 不可欠な、情報処理施設とシステムや設備などの保護すべき対象）を特定しその資産の保護の責任を定めることを求めている。そして、資産のライフサイクル全体（取得、作成、利用、保管／保存、転送、売却／譲渡、廃棄）におけるセキュリティを要求している



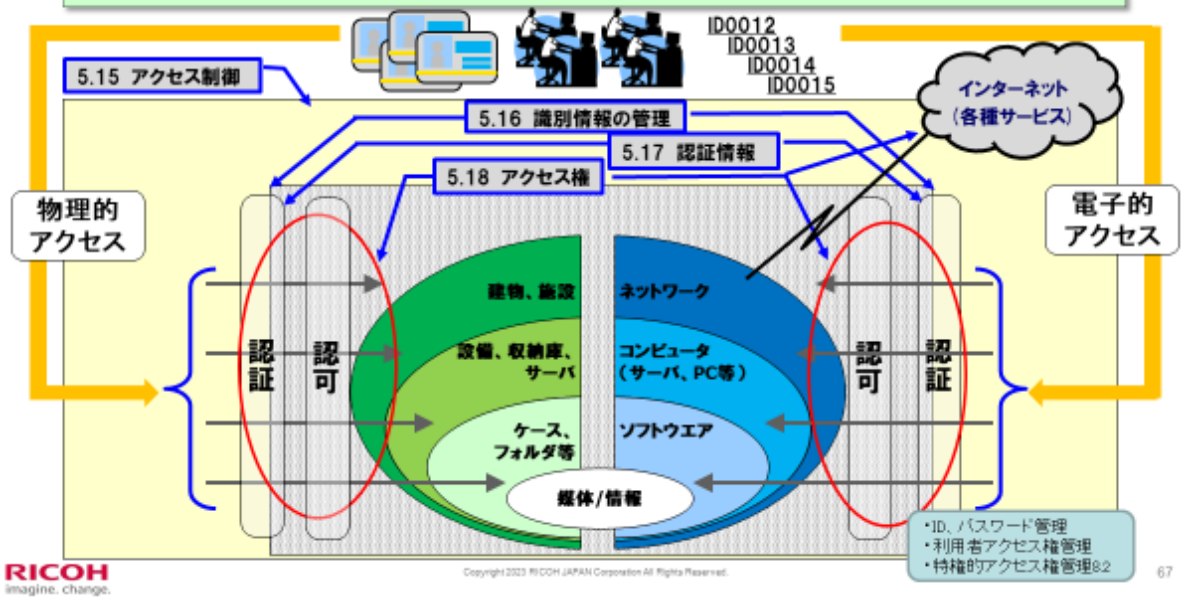
C-1

管理対象ベースのリスク管理モデル：例

第二章　JIS Q 27001:2023　管理策改定概要

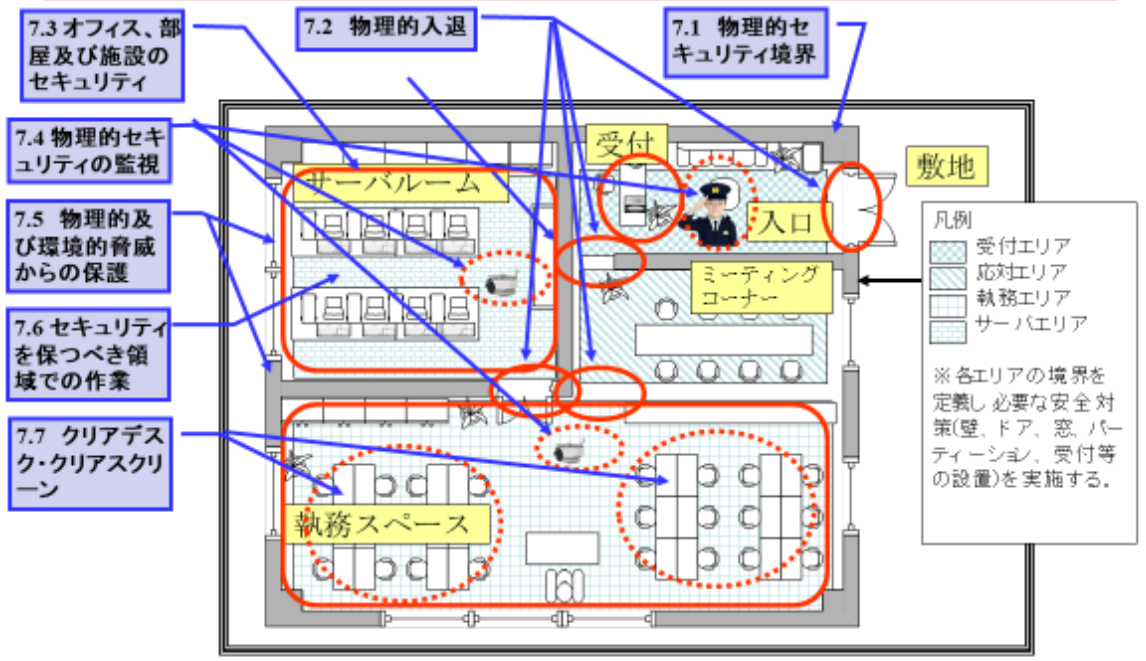
II．管理策の改定内容と解説：アクセス権管理

アクセス権管理は、情報及び情報を扱うための関連資産を保護するために、許可された者が許可された範囲の資産にアクセスできるようにすることを求めている。そのため、「許可された者」を識別するためのID管理、IDを持つ者が本人であることを確認するための認証、認証された者がアクセスできる対象を管理するためのアクセス権を管理する必要がある 。



第二章　JIS Q 27001:2023　管理策改定概要

II．管理策の改定内容と解説：物理的領域の管理



テーマ1（全体）

これからJISQ27001:2023への移行を検討する方へのアドバイス

（注意事項や効率化の観点）

ディスカッションタイム

テーマ1（全体）

これからJISQ27001:2023への移行を検討する方へのアドバイス

（注意事項や効率化の観点）

要約（まとめ）

テーマ2（各論）

新規管理策11個や旧管理策から
の移行についてのTIPSや考え方

認証の移行確認の審査（移行審査）

- **サーベイランス審査、再認証審査と同時に、又は個別の審査**として受けることができる
- **文書審査だけに依存しない。**特に技術的管理策のレビューについてはそれ以外の確認が必要となることがある。
- 移行審査には、**次の事項が含まれる**が、これらに限定されない
  - ISO/IEC 27001：2022のギャップ分析及び被認証組織のISMSの変更の必要性
  - 適用宣言書の更新
  - 該当する場合、リスク対応計画の更新
  - 被認証組織が選択した、新規又は変更された管理策の実施及び有効性
- 認証機関が目的を達成できると判断した場合は、**審査を遠隔で実施する**ことができる

移行審査の工数／認証サイクル

【移行審査の工数】

- **再認証審査と同時**に実施する場合は、**少なくとも0.5人日、追加の審査工数**が必要
- **サーベイランス審査と同時**に実施する場合、又は**単独の審査**として実施する場合は、**少なくとも1人日、追加の審査工数**が必要

※実際にかかる工数は、認証機関にご確認ください。

【認証サイクル】

- 初回登録日を起点として、**認証サイクルに変更はない**
- 移行審査を受けることで、認証の有効期間が伸びることはない

JIS Q 27001:2023への移行について（標準化の観点から）

テーマ２（各論）
新規管理策11個や旧管理策からの移行についてのTIPSや考え方

- 新規管理策は、既存の管理策でも部分的に対象としていたが、昨今のセキュリティ脅威や技術動向を反映し、新規管理策として独立させたものが多い
- 新規管理策以外の管理策も、対象範囲が広がっているものもあるので、改めて、管理策やISO/IEC 27002:2022の手引を見直す
- ISO/IEC 27002:2022の管理策の目的（Purpose）や属性(Attribute）を活用すると、管理策の理解をより深めることができる

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 2023
NTTテクノクロス株式会社 土屋 直子（ISO/IEC JTC 1/SC 27/WG 1）

C-2

新規管理策11個や旧管理策からの移行についてのTIPSや考え方

「新規管理策が出来たのだから、
何か新しい事を始めなければいけない」

と思い込んだり焦ったりする前に。

“新規”管理策であっても各組織で、
それに該当する既存の施策が
全く無いという事態は少ないと思います。

「何となくやっていた(やれているつもり)」
というものも含めれば。

(該当する既存の施策が)以下を満たしていれば、
管理策があると見做して良いんじゃ
ないでしょうか？

- (27002にある)管理策の目的に合致するか。
- 現状の「ルール」「実施状況」から『仕組み』の存在を確認できるか。

そこを起点として、
(二周目からでも良いので)
リスク分析し改善していけば良いのでは。

テーマ2（各論）

**新規管理策11個や旧管理策から
の移行についてのTIPSや考え方**

ディスカッション
タイム

新規管理策11個や旧管理策から
の移行についてのTIPSや考え方

要約（まとめ）

全体総括