② 詳細管理策の構造化：ＪＩＳ　Ｑ　27002：2024では手引内に下線の付いた小見出しが設けられている（例：「5.9　情報及びその他の関連資産の目録」における「目録」や「管理責任」等）。本管理基準でもこれらを利用し、詳細管理策内で同様の小見出し（【】で括られている事項）を設けている（付番無し）。

「管理策基準」の内容は次のとおりである。

5　組織的管理策
- 5a　組織的管理
  - 5a-5.1　情報セキュリティのための方針群
  - 5a-5.2　情報セキュリティの役割及び責任
  - 5a-5.3　職務の分離
  - 5a-5.4　管理層の責任
  - 5a-5.5　関係当局との連絡
  - 5a-5.6　専門組織との連絡
  - 5a-5.7　脅威インテリジェンス
  - 5a-5.8　プロジェクトマネジメントにおける情報セキュリティ
- 5b　資産管理
  - 5b-5.9　情報及びその他の関連資産の目録
  - 5b-5.10　情報及びその他の関連資産の許容される利用
  - 5b-5.11　資産の返却
  - 5b-5.12　情報の分類
  - 5b-5.13　情報のラベル付け
  - 5b-5.14　情報の転送
- 5c　アクセス権管理
  - 5c-5.15　アクセス制御
  - 5c-5.16　識別情報の管理
  - 5c-5.17　認証情報
  - 5c-5.18　アクセス権
- 5d　供給者管理
  - 5d-5.19　供給者関係における情報セキュリティ
  - 5d-5.20　供給者との合意における情報セキュリティの取扱い
  - 5d-5.21　ＩＣＴサプライチェーンにおける情報セキュリティの管理
  - 5d-5.22　供給者のサービス提供の監視、レビュー及び変更管理
  - 5d-5.23　クラウドサービスの利用における情報セキュリティ
- 5e　インシデント管理
  - 5e-5.24　情報セキュリティインシデント管理の計画策定及び準備
  - 5e-5.25　情報セキュリティ事象の評価及び決定
  - 5e-5.26　情報セキュリティインシデントへの対応
  - 5e-5.27　情報セキュリティインシデントからの学習
  - 5e-5.28　証拠の収集
- 5f　事業継続における情報セキュリティ管理
  - 5f-5.29　事業の中断・阻害時の情報セキュリティ
  - 5f-5.30　事業継続のためのＩＣＴの備え
- 5g　コンプライアンス管理
  - 5g-5.31　法令、規制及び契約上の要求事項
  - 5g-5.32　知的財産権
  - 5g-5.33　記録の保護
  - 5g-5.34　プライバシー及びＰＩＩの保護
  - 5g-5.35　情報セキュリティの独立したレビュー
  - 5g-5.36　情報セキュリティのための方針群、規則及び標準の順守
  - 5g-5.37　操作手順書

6　人的管理策
- 6a　人的管理
  - 6a-6.1　選考
  - 6a-6.2　雇用条件
  - 6a-6.3　情報セキュリティの意識向上、教育及び訓練
  - 6a-6.4　懲戒手続
  - 6a-6.5　雇用の終了又は変更後の責任
  - 6a-6.6　秘密保持契約又は守秘義務契約
  - 6a-6.7　リモートワーク
  - 6a-6.8　情報セキュリティ事象の報告

7　物理的管理策
- 7a　物理的領域の管理
  - 7a-7.1　物理的セキュリティ境界
  - 7a-7.2　物理的入退
  - 7a-7.3　オフィス、部屋及び施設のセキュリティ
  - 7a-7.4　物理的セキュリティの監視
  - 7a-7.5　物理的及び環境的脅威からの保護
  - 7a-7.6　セキュリティを保つべき領域での作業
  - 7a-7.7　クリアデスク・クリアスクリーン
- 7b　装置の管理
  - 7b-7.8　装置の設置及び保護
  - 7b-7.9　構外にある資産のセキュリティ
  - 7b-7.10　記憶媒体
  - 7b-7.11　サポートユーティリティ
  - 7b-7.12　ケーブル配線のセキュリティ
  - 7b-7.13　装置の保守
  - 7b-7.14　装置のセキュリティを保った処分又は再利用

8　技術的管理策
- 8a　情報アクセスの管理
  - 8a-8.1　利用者エンドポイント機器
  - 8a-8.2　特権的アクセス権
  - 8a-8.3　情報へのアクセス制限
  - 8a-8.4　ソースコードへのアクセス
  - 8a-8.5　セキュリティを保った認証
  - 8a-8.6　容量・能力の管理
- 8b　情報資産運用に関する管理
  - 8b-8.7　マルウェアに対する保護
  - 8b-8.8　技術的ぜい弱性の管理
  - 8b-8.9　構成管理