(5a-5.1.5参考)　トピック固有の方針は、一般に、組織内で対象とする特定のグループのニーズに対応するように、又は特定のセキュリティ領域を対象とするように構成される。

5a-5.1.6　トピック固有の方針は、組織の情報セキュリティ方針に沿い、それを補完する。

(5a-5.1.6参考)　このようなトピックの例を、次に示す。

ａ）アクセス制御
ｂ）物理的及び環境的セキュリティ
ｃ）資産管理
ｄ）情報の転送
ｅ）利用者エンドポイント機器のセキュリティを保った構成及び取扱い
ｆ）ネットワークセキュリティ
ｇ）情報セキュリティインシデント管理
ｈ）バックアップ
ｉ）暗号及び鍵管理
ｊ）情報の分類及び取扱い
ｋ）技術的ぜい弱性の管理
ｌ）セキュリティに配慮した開発

5a-5.1.7　トピック固有の方針の作成、レビュー及び承認に関する責任は、関連する要員に、権限及び技術的力量のレベルに基づいて割り当てる。

5a-5.1.8　レビューには、次のものの変化に応じた、組織の情報セキュリティ方針及びトピック固有の方針並びに情報セキュリティの管理に関する、改善の機会の評価を含める。

ａ）組織の事業戦略
ｂ）組織の技術環境
ｃ）規制、法令及び契約
ｄ）情報セキュリティリスク
ｅ）現在の及び予想される情報セキュリティの脅威の環境
ｆ）情報セキュリティ事象及びインシデントから学んだ教訓

5a-5.1.9　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、マネジメントレビュー及び監査の結果を考慮する。

5a-5.1.10　一貫性を維持するため、一つの方針を変更する場合は、他の関連する方針のレビュー及び更新を検討する。

5a-5.1.11　情報セキュリティ方針及びトピック固有の方針は、意図する読者にとって適切で、アクセスでき、かつ、理解しやすい形で、関連する要員及び利害関係者に伝達する。

5a-5.1.12　必要な場合には、方針の受領者に、方針を理解したこと及びその順守に同意することの確認を求める。

(5a-5.1参考１)　組織は、これらの方針文書について、組織のニーズを満たす形式及び名称を決定することが可能である。

(5a-5.1参考２)　組織によって、情報セキュリティ方針及びトピック固有の方針を単一の文書にすることがある。

(5a-5.1参考３)　組織は、トピック固有の方針に、標準、指令、方針、その他の名称を付けることがある。

5a-5.1.13　情報セキュリティ方針又はトピック固有の方針を組織外に配布する場合には、秘密情報を不適切に開示しないように注意する。

(5a-5.1.13参考)　表１に、情報セキュリティ方針とトピック固有の方針との違いを示す。

表１　情報セキュリティ方針とトピック固有の方針との違い

	情報セキュリティ方針	トピック固有の方針
詳細さのレベル	一般的又は高いレベル	固有及び詳細
文書化し、正式に承認する人	トップマネジメント	適切なマネジメントレベル

5a-5.2　情報セキュリティの役割及び責任

管理策：情報セキュリティの役割及び責任は、組織のニーズに従って定め、割り当てる。

目的：　組織内における情報セキュリティの実施、運用及び管理のために、定義され、承認され、理解される構造を確立するため。

詳細管理策

5a-5.2.1　情報セキュリティの役割及び責任の割当ては、情報セキュリティ方針及びトピック固有の方針に従って行う。

5a-5.2.2　組織は、次の事項に関する責任を定義し、管理する。

ａ）情報及びその他の関連資産の保護
ｂ）特定の情報セキュリティプロセスの実施
ｃ）情報セキュリティのリスクマネジメント活動、特に残留リスクの受容
ｄ）組織の情報及びその他の関連資産を使用する全ての要員

5a-5.2.3　必要な場合には、この責任を、個別のサイト及び情報処理施設に対する、より詳細な手引で補完する。

5a-5.2.4　情報セキュリティの責任を割り当てられた個人は、情報セキュリティに関する職務を他者に委任してもよい。しかし、アカウンタビリティは依然としてその個人にあり、委任した職務がいずれも正しく実施されていることを、その個人が確認する。

5a-5.2.5　個人が責任をもつ各セキュリティ領域を定義し、文書化し、伝達する。

5a-5.2.6　承認のレベルを定義し、文書化する。

5a-5.2.7　特定の情報セキュリティの役割をもつ個人は、その役割に必要な知識及び技能において力量をもつ。

5a-5.2.8　その役割に関連し、その役割の責任を果たす上で必要な最新の動向に追随し続けるように支援される。

5a-5.3　職務の分離

管理策：相反する職務及び相反する責任範囲は、分離する。

目的：　情報セキュリティ管理策の不正、誤り及び回避のリスクを軽減するため。

詳細管理策

5a-5.3.1　組織は、どの職務及び責任範囲を分離する必要があるかを決定する。

(5a-5.3.1参考)　職務及び責任範囲の分離は、相反する可能性がある職務を一人の個人が自ら実行することを防ぐために、相反する職務を異なる個人に分離することを目的としている。次の事項は、分離が必要になる可能性のある活動の例である。

ａ）変更の提案、承認及び実行
ｂ）アクセス権の要求、承認及び付与
ｃ）コードの設計、実装及びレビュー