内部情報セキュリティ監査チェックリスト 2013 年版

附属書 A （A5 情報セキュリティのための方針群）	インタビュー等サイト（現地）確認	確認の有無	不適合の有無	備考（メモ）
A.5.1 情報セキュリティのための経営陣の方向性 A.5.1.1 情報セキュリティのための方針群 管理策 情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員及び関連する外部関係者に通知しなければならない。 A.5.1.2 情報セキュリティのための方針群のレビュー 管理策 情報セキュリティのための方針群は、あらかじめ定めた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当かつ有効であることを確実にするためにレビューしなければならない	**「情報セキュリティ方針文書を見せてください」** ・経営陣が承認しているか。 **「情報セキュリティ方針文書は職員へどのように公表していますか」** ・従業員、外部関係者のすべてに公表、通知できているか。 **「情報セキュリティ方針はマネジメントレビュー時に行っていますか」** ・マネジメントレビューは適切な間隔で行っているか。 ・緊急のマネジメントレビューを行うことがあるか。			

附属書 A （A.6 情報セキュリティのための組織）	インタビュー等サイト（現地）確認	確認の有無	不適合の有無	備考（メモ）
A.6.1 内部組織 A.6.1.1 情報セキュリティの役割及び責任 管理策 全ての情報セキュリティの責任を定め、割り当てなければならない。 A.6.1.2 職務の分離 管理策 相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離しなければならない。 A.6.1.3 関係当局との連絡 管理策 関係当局との適切な連絡体制を維持しなければならない。 A.6.1.4 専門組織との連絡 管理策 情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持しなければならない。 A.6.1.5 プロジェクトマネジメントにおける情報セキュリティ 管理策 プロジェクトの種類に係わらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組まなければならない。	**「情報セキュリティ管理責任者は誰ですか」** ・経営陣が任命、承認しているか。 ・情報セキュリティ管理責任者が〇〇さんであることを、どのような形で周知、公表を行っているか。 **「セキュリティに関する役割及び責任の明示されている文書を見せてください」** ・どのような文書があるか。 ・セキュリティ順守を監視、違反追求の責任が明確になっているか。 ・雇用前の該当者に伝達する手段はあるか。 **「立場が異なる職務・責任について説明してください」** ・審査や検査は、役割の分離がおこなわれているか。 **「関係官庁との連絡体制はどのようになっていますか」** ・関係官庁、通信業者、サービス提供者が明確になっているか。 ・連絡体制は、維持、更新されているか。 **「専門組織との連絡体制はどのようになっていますか」** ・研究会、専門家の協会・団体が明確になっているか。 ・連絡体制は、維持、更新されているか。 **「新規プロジェクトの情報セキュリティ活動はどのようになっていますか」** ・新規プロジェクトも情報セキュリティ活動の対象になっているか。			

内部監査チェックリスト（情報セキュリティ ISMS／ISO27001:2013 附属書 A）

この度は、**内部情報セキュリティ附属書 A 監査チェックリストサンプル**のご覧頂きまして、ありがとうございます。

この他に、**内部品質監査チェックリストサンプル、内部環境監査チェックリスト、内部個人情報保護監査チェックリスト、内部労働安全衛生監査チェックリスト、内部苦情対応監査チェックリスト**もございます。

http://www.isonavi.net/tools/checklst.html
をご覧ください。