

内部監査チェックリスト(情報セキュリティ ISMS/ISO27001:2005)

規格要求事項 (4.3 文書化に関する要求事項)	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)
<p>4.3.1 一般</p> <p>文書には、経営陣の決定に関する記録も含めなければならない。文書は、とった処置から、経営陣の決定及び方針へたどれること、並びに記録した結果が再現可能であることを確実にしなければならない。</p> <p>選択した管理策からリスクアセスメント及びリスク対応のプロセスまで、更には ISMS 基本方針及び目的までにつながる関係を説明できることが重要である。</p> <p>ISMS 文書には、次を含めなければならない。</p> <p>a)文書化した ISMS 基本方針[4.2.1b)参照]及び目的</p> <p>b)ISMS の適用範囲[4.2.1a)参照]</p> <p>c)ISMS を支えている手順及び管理策</p> <p>d)リスクアセスメントの方法[4.2.1c)参照]の記述</p> <p>e)リスクアセスメント報告[4.2.1c)～4.2.1g)参照]</p> <p>f)リスク対応計画[4.2.2b)参照]</p> <p>g)情報セキュリティのプロセスを有効に計画、運用及び管理することを確実にするために、組織が必要とする文書化した手順。管理策の有効性をどう測定するか[4.2.2d)参照]を記述するために、組織が必要とした文書化した手順。</p>	<p>「全体を説明した文書を見せて下さい」</p> <p>「文書体系表がありますか」 (この表で相互関係を確認する)</p> <ul style="list-style-type: none"> ・ISMS 基本方針及び目的の文書 ・ISMS 適用範囲 ・ISMS を支えてる手順及び管理策 ・リスクアセスメントの方法 ・リスクアセスメント報告 ・リスク対応計画 ・組織が必要とする文書化した手順 ・この規格が要求する記録 ・適用宣言書 <p>「ISMS基本方針及び目的の文書を見せてください」</p> <p>「選択した管理策の個別方針の文書を見せてください」</p> <ul style="list-style-type: none"> ・以下の項目が、基本方針と整合性がとれているか。 <ul style="list-style-type: none"> －A.11.1.1 アクセス制御方針 －A.11.3.3 クリアデスク・クリアスクリーン方針 －A.11.4.1 ネットワークサービスの利用についての方針 －A.11.7.1 モバイルコンピューティング設備・通信設備のための個別方針 －A.11.7.2 レテワーキングのための個別方針 －A12.3.1 暗号による管理策の利用に関する個別方針 <p>「ISMS適用範囲の文書を見せてください」</p> <p>「ISMSを支えてる手順及び管理策の文書を見せてください」</p> <ul style="list-style-type: none"> ・以下の文書を確認する。 <ul style="list-style-type: none"> －文書管理手順 －記録管理手順 －内部監査手順 －是正処理手順 －予防処置手順 			

内部監査チェックリスト(情報セキュリティISMS／ISO27001:2005)

この度は、内部情報セキュリティ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さいます。

<http://www.isonavi.net/tools/checklst.html>

をご覧ください。