経営者層編

ガイドラインの目次		対策	現状の評価	1年後の評価	備考（実施目標日、進捗状況等）
事前準備	1.1.1	組織的 人的 技術的 物理的 ① 組織方針とサイバーセキュリティ 組織方針にあたる文書にサイバーセキュリティ確保に関する事項も組み入れている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.1.1	組織的 人的 技術的 物理的 ② 維持するサービス範囲・水準 任務保障を果すために維持するサービスの範囲・水準を示している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.1.2	組織的 人的 技術的 物理的 ③ サイバーセキュリティ方針 セキュリティ対策に取り組むことをサイバーセキュリティ方針等に含め、組織の内外に対して宣言しているる。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.2	組織的 人的 技術的 物理的 ④ 経営リスクとしてのサイバーセキュリティリスクの管理 サイバーセキュリティに関する責任及び権限を明確にした上で、リスク管理体制を構築しているる。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	

経営者層編

ガイドラインの目次		対策	現状の評価	1年後の評価	備考（実施目標日、進捗状況等）
平時対策	2.1	組織的 人的 技術的 物理的 ① 組織内外のコミュニケーション 組織内外のコミュニケーションにおいて、サイバーセキュリティリスク、インシデント等の情報を取扱っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.2.1	組織的 人的 技術的 物理的 ② 情報セキュリティ責任者の指名 情報セキュリティ対策の推進の責任者として最高情報セキュリティ責任者（CISO）を指定している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.2.2	組織的 人的 技術的 物理的 ③ 責任者・組織などの役割 情報セキュリティ担当者を指定し、役割及び権限を割り当てている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.2.3	組織的 人的 技術的 物理的 ④ 役割の分離 サイバーセキュリティに係る職務については分離に関する規程を設けている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	

経営者層編

ガイドラインの目次		対策	現状の評価	1年後の評価	備考（実施目標日、進捗状況等）
インシデント発生時及び事後対応	3.1	組織的 人的 技術的 物理的 ① 情報開示 平時におけるサイバーセキュリティ確保の取組に対する姿勢や、インシデント発生の対応に関する情報の開示に取り組んでいる。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	3.2	組織的 人的 技術的 物理的 ② インシデント対応及び事業継続対応 インシデント発生時には、情報セキュリティ責任者（CISO等）に、事業継続計画等に沿ったインシデント対応、事業継続対応を指示している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	