

詳細管理策チェックシート

A.5 セキュリティ基本方針				
A.5.1 情報セキュリティ基本方針				
管理目的: 情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項、関連する法令及び規則に従って規定するため				
	管理策	チェック項目	ギャップ	現状
A.5.1.1	情報セキュリティ基本方針及び文書	情報セキュリティ基本方針文書は、経営陣によって承認され、全従業員及び関連する外部関係者に公表し、通知すること。		
A.5.1.2	情報セキュリティ基本方針のレビュー	情報セキュリティ基本方針は、あらかじめ定められた間隔で、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、及び有効であることを確実にするためにレビューすること。		

A.6 情報セキュリティのための組織				
A.6.1 内部組織				
管理目的: 組織内の情報セキュリティを管理するため				
	管理策	チェック項目	ギャップ	現状
A.6.1.1	情報セキュリティに対する経営陣の責任	経営陣は、情報セキュリティの責任に関する明瞭な方向付け、自らの関与の明示、責任の明確な割当て及び承認を通して、組織内におけるセキュリティを積極的に支持すること。		
A.6.1.2	情報セキュリティの調整	情報セキュリティ活動は、組織の中の、関連する役割及び職務機能を持つさまざまな部署の代表が、調整すること。		
A.6.1.3	情報セキュリティ責任の割当て	すべての情報セキュリティ責任を、明確に定めること。		
A.6.1.4	情報処理設備の許可プロセス	新しい情報処理設備に対する経営陣による認可プロセスを定め、実施すること。		
A.6.1.5	機密保持契約	情報保護に対する組織の必要を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューすること。		
A.6.1.6	関係者の協力	関係当局との適切な連絡体制を維持すること		
A.6.1.7	専門組織との連絡	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すること。		
A.6.1.8	情報セキュリティの独立したレビュー	情報セキュリティ及びその実施のマネジメントに対する組織の取組み(例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順)は、あらかじめ定められた間隔で、又はセキュリティの実施に重大な変化が生じた場合に、独立したレビューを実施すること		

A.6.2 外部組織				
管理目的: 外部組織によってアクセス、処理、通信、又は管理される組織の情報処理施設のセキュリティを維持するため。				
	管理策	チェック項目	ギャップ	現状
A.6.2.1	外部組織に関係したリスクの識別	外部組織が関する業務プロセスからの、組織の情報及び情報処理施設に対するリスクを識別し、外部組織にアクセスを許可する前に適切な管理策を実施すること。		
A.6.2.2	顧客対応におけるセキュリティ	顧客が組織の情報及び資産にアクセスする前に、明確にしたすべてのセキュリティ要求事項に対処すること。		
A.6.2.3	第三者との契約書におけるセキュリティ要求事項	組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理に関わる第三者との契約、又は情報処理施設に製品・サービスを追加する第三者との契約は、関連するすべてのセキュリティ要求事項を取り上げること。		

A.7 資産の管理				
A.7.1 資産に対する責任				
管理目的: 組織の資産の適切な保護を達成し、維持するため。				
	管理策	チェック項目	ギャップ	現状
A.7.1.1	資産目録	すべての資産を明確に識別し、また、重要な資産すべての目録を作成し維持すること。		
A.7.1.2	資産の保有者	情報及び情報処理施設と関連する資産のすべてについて、組織のなかに、その保有者を指定すること。		
A.7.1.3	資産利用の許容範囲	情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則を明確にし、文書化し、実施すること。		

A.7.2 情報の分類				
管理目的: 情報の適切なレベルでの保護を確実にするため。				
	管理策	チェック項目	ギャップ	現状
A.7.2.1	分類の指針	情報は、組織に対しての価値、法的要求事項、取扱に慎重を要する度合い及び重要性の観点から分類すること。		
A.7.2.2	情報のラベル付け及び取り扱い	情報に対するラベル付け及び取扱に関する適切な一連の手順は、組織が採用した分類体系に従って策定し、実施すること。		