

ギャップ分析対策表

セキュリティ管理策	要求項目	要求事項	確認	現 状			脆弱性 ランク	詳細対策	関連する規程	項番	対策後 脆弱性 ランク
				関連する 社内規程	該当箇所	分析 結果					
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	情報セキュリティのための経営陣の方向性及び支持を、業務上の要求事項、関連する法令及び規則に従って規定するため。									
A.5.1.1	情報セキュリティ基本方針文書	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。	情報セキュリティ推進委員会が情報セキュリティ基本方針書を策定し、経営者に承認を得、従業員、外部関係者に公表し、通知することを定めているか？	-----	---	N	情報セキュリティ基本方針が明確でない。	ISMS推進委員会が情報セキュリティ基本方針書を策定し、経営者に承認を得ていない。	情報セキュリティ基本方針書	全般 10	1
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。	情報セキュリティ基本方針書を環境変化に合わせて定期的に見直すことを定めているか？	-----	---	N	情報セキュリティ基本方針が明確でない。	情報セキュリティ基本方針書を環境変化に合わせて定期的に見直すことを定めていない。	情報セキュリティ基本方針書	全般 10	1
A.6	情報セキュリティのための組織										
A.6.1	情報セキュリティ基盤	組織内の情報セキュリティを管理するため。									
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らかな方向付け、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。	ISMSの運用・維持にあつての責任・割り当て及び承認を通して、セキュリティを積極的に支持することを定めているか？	-----	---	N	情報セキュリティ推進体制が不明確。	ISMSを推進するにあたり、明瞭な指導と経営陣指示の情報セキュリティの推進体制を確立するよう定められている。	情報セキュリティ運営管理規程	3	1
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、組織のなかの、関連する役割及び職務機能をもつさまざまな部署の代表者が、調整すること。	情報セキュリティを推進する体制が確立され組織を横断的に調整できるようなメンバーが参加しているか？	-----	---	N	情報セキュリティ推進体制が不明確。	情報セキュリティ推進体制が確立されていない。	情報セキュリティ運営管理規程	3	1
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。	情報セキュリティを推進する責任と権限を定めているか？	-----	---	N	不明確な責任	情報セキュリティを推進するための責任と権限を定めていない。	情報セキュリティ運営管理規程	3	1
A.6.1.4	情報処理設備の認可プロセス	新しいハードウェア・ソフトウェアの導入に際して、情報セキュリティの観点から、ハードウェア・ソフトウェアの導入に際しての認可プロセスを定めること。	ハードウェア・ソフトウェアの導入に際しての認可プロセスを定めているか？	-----	---	N	情報処理設備の認可プロセスが不明確。	ハードウェア・ソフトウェアを導入する際の手続きを定めていない。	情報セキュリティ運営管理規程	4	1
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機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、定期的にレビューすること。	機密保持契約又は守秘義務契約の要求事項を特定し、契約者との内容確認を行っているか？	-----	---	N	契約での要求事項が不明確	機密保持契約又は守秘義務契約での要求事項が定められていない。	人的セキュリティ管理規程	4	1
A.6.1.6	関係当局との連絡	関係当局との適切な連絡体制を維持すること。	情報セキュリティインシデントに早急に対応するため行政・情報サービス業者との連絡体制を定めているか？	-----	---	N	行政・情報サービス業者との連絡体制が不明確	情報セキュリティインシデントに早急に対応するため行政・情報サービス業者との連絡体制を定めていない。	情報セキュリティ運営管理規程	5	1

Y・・・対策済み
P・・・一部対策済み
N・・・対策なし
N/A・・・対象外