	管理策	内容	情報セキュリティ運営管理規程	リスクマネジメント管理規程	適合性管理規程	システム運用管理規程	事業継続管理規程	アクセス管理規程	物理的・環境的管理規程	人的セキュリティ管理規程	内部監査管理規程	外部審査管理規程	是正処置管理規程	セキュリティ事件・事故管理規程
1	5.1	情報セキュリティのための方針群	●											
2	5.2	情報セキュリティの役割及び責任	●											
3	5.3	職務の分離	●											
4	5.4	管理層の責任	●											
5	5.5	関係当局との連絡	●											
6	5.6	専門組織との連絡	●											
7	5.7	脅威インテリジェンス		●										
8	5.8	プロジェクトマネジメントにおける情報セキュリティ	●											
9	5.9	情報及びその他の関連資産の目録		●										
10	5.10	情報及びその他の関連資産の許容される利用		●										
11	5.11	資産の返却								●				
12	5.12	情報の分類		●										
13	5.13	情報のラベル付け		●										
14	5.14	情報の転送		●										
15	5.15	アクセス管理						●						
16	5.16	識別情報の管理						●						
17	5.17	認証情報						●						
18	5.18	アクセス権						●						
19	5.19	供給者関係における情報セキュリティ						●						
20	5.20	供給者との合意における情報セキュリティの取扱い						●						
21	5.21	情報通信技術(ICT)サプライチェーンにおける情報セキュリティの管理	●											
22	5.22	供給者のサービス提供の監視、レビュー及び変更管理						●						
23	5.23	クラウドサービスの利用における情報セキュリティ						●						
24	5.24	情報セキュリティインシデント管理の計画策定及び準備												●
25	5.25	情報セキュリティ事象の評価及び決定												●
26	5.26	情報セキュリティインシデントへの対応												●
27	5.27	情報セキュリティインシデントからの学習												●
28	5.28	証拠の収集												●
29	5.29	事業の中断・阻害時の情報セキュリティ		●			●	●						●
30	5.30	事業継続のためのICTの備え		●			●							●
31	5.31	法令、規制及び契約上の要求事項			●		●							
32	5.32	知的財産権			●		●							
33	5.33	記録の保護			●									
34	5.34	プライバシー及び個人識別可能情報(PII)の保護			●		●							
35	5.35	情報セキュリティの独立したレビュー	●											
36	5.36	情報セキュリティのための方針群、規則及び標準の遵守			●		●							
37	5.37	操作手順書	●											
38	6.1	選考								●				
39	6.2	雇用条件								●				
40	6.3	情報セキュリティの意識向上、教育及び訓練								●				
41	6.4	懲戒手続								●				
42	6.5	雇用の終了又は変更後の責任								●				
43	6.6	秘密保持契約又は守秘義務契約								●				
44	6.7	リモートワーク						●						
45	6.8	情報セキュリティ事象の報告												●
46	7.1	物理的セキュリティ境界							●					
47	7.2	物理的入退							●					
48	7.3	オフィス、部屋及び施設のセキュリティ							●					
49	7.4	物理的セキュリティの監視							●					
50	7.5	物理的及び環境的脅威からの保護							●					
51	7.6	セキュリティを保つべき領域での作業							●					
52	7.7	クリアデスク・クリアスクリーン							●					
53	7.8	装置の設置及び保護							●					
54	7.9	構外にある資産のセキュリティ							●					
55	7.10	記憶媒体								●				
56	7.11	サポートユーティリティ							●					
57	7.12	ケーブル配線のセキュリティ							●					
58	7.13	装置の保守							●					
59	7.14	装置のセキュリティを保った処分又は再利用							●					
60	8.1	利用者エンドポイント機器						●						
61	8.2	特権的アクセス権						●						
62	8.3	情報へのアクセス制限						●						
63	8.4	ソースコードへのアクセス						●						
64	8.5	セキュリティを保った認証						●						
65	8.6	容量・能力の管理							●					
66	8.7	マルウェアに対する保護				●								
67	8.8	技術的脆弱性の管理				●								
68	8.9	構成管理				●								
69	8.10	情報の削除								●				
70	8.11	データマスキング				●								
71	8.12	データ漏洩防止				●								
72	8.13	情報のバックアップ				●								
73	8.14	情報処理施設・設備の冗長性				●								
74	8.15	ログ取得				●								
75	8.16	監視活動				●								
76	8.17	クロックの同期				●								
77	8.18	特権的なユーティリティプログラムの使用						●						
78	8.19	運用システムへのソフトウェアの導入				●								
79	8.20	ネットワークセキュリティ				●								
80	8.21	ネットワークサービスのセキュリティ				●								
81	8.22	ネットワークの分離				●								
82	8.23	ウェブフィルタリング				●								
83	8.24	暗号の利用				●								
84	8.25	セキュリティに配慮した開発のライフサイクル				●								
85	8.26	アプリケーションセキュリティの要求事項				●								
86	8.27	セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則				●								
87	8.28	セキュリティに配慮したコーディング				●								
88	8.29	開発及び受入れにおけるセキュリティテスト				●								
89	8.30	外部委託による開発				●								
90	8.31	開発環境、テスト環境及び本番環境の分離				●								
91	8.32	変更管理	●											
92	8.33	テスト用情報				●								
93	8.34	監査におけるテスト中の情報システムの保護				●	●							

要求事項	-		ISO27001	情報セキュリティ運営管理規程	リスクマネジメント管理規程	適合性管理規程	システム運用管理規程	事業継続管理規程	アクセス管理規程	物理的・環境的管理規程	人的セキュリティ管理規程	内部監査管理規程	外部審査管理規程	是正処置管理規程	セキュリティ事件・事故管理規程
1	-		適用範囲	●											
2	-		引用規格	●											
3	-		用語及び定義	●											
4	-		組織の状況	●											
-		4.1	組織及びその状況の理解	●											
-		4.2	利害関係者のニーズ及び期待の理解	●											
-		4.3	情報セキュリティマネジメントシステムの適用範囲の決定	●											
-		4.4	情報セキュリティマネジメントシステム	●											
5	-		リーダシップ	●											
-		5.1	リーダシップ及びコミットメント	●											
-		5.2	方針	●											
-		5.3	組織の役割、責任及び権限	●											
6	-		計画策定	●											
-		6.1	リスク及び機会に対する活動		●										
-	-		6.1.2 情報セキュリティリスクアセスメント		●										
-	-		6.1.3 情報セキュリティリスク対応		●										●
-		6.2	情報セキュリティ目的及びそれを達成するための計画策定		●										
-		6.3	変更の計画策定		●										
7	-		支援							●					
-		7.1	資源							●	●				
-		7.2	力量							●	●				
-		7.3	認識							●					
-		7.4	コミュニケーション							●					
-		7.5	文書化した情報							●					
8	-		運用		●										
-		8.1	運用の計画策定及び管理		●										
-		8.2	情報セキュリティリスクアセスメント		●										
-		8.3	情報セキュリティリスク対応		●										●
9	-		パフォーマンス評価	●											
-		9.1	監視、測定、分析及び評価	●								●	●		
-		9.2	内部監査	●								●	●		
-		9.3	マネジメントレビュー	●											
10	-		改善	●											
-		10.1	継続的改善	●											
-		10.2	不適合及び是正処置											●	●