大分類	中分類	項番	小分類	マネジメント編 設問№	ユーザー編 設問№
3. 情報セキュリティ基本方針	3. (1) 情報セキュリティ基本方針	3. (1) ①	情報セキュリティ基本方針文書	1	1
		3. (1) ②	見直し及び評価	2	
4. 組織のセキュリティ	4. (1) 情報セキュリティ基盤	4. (1) ①	情報セキュリティ運営委員会	3	
		4. (1) ③	情報セキュリティ責任の割当て	4	2
		4. (1) ④	情報処理設備の認可手続き	5	3
		4. (1) ⑤	専門家による情報セキュリティの助言	6	
		4. (1) ⑥	組織間の協力	7	
	4. (2) 第三者による アクセスのセキュリティ	4. (2) ①	第三者のアクセスから生じるリスクの識別	8	
		4. (2) ②	第三者との契約書に記載するセキュリティ要求事項	9	4
	4. (3) 外部委託	4. (3) ①	外部委託契約におけるセキュリティ要求事項	10	
5. 資産の分類及び管理	5.(1)資産に対する責任	5. (1) ①	資産目録	11	
	5.(2) 情報の分類	5. (2) ①	分類の指針	12	5
		5. (2) ②	情報のラベル付け及び取り扱い		
6. 人的セキュリティ	6. (1) 職務定義 及び雇用におけるセキュリティ	6.(1)①	セキュリティを職責に含めること	13	
		6.(1)③	機密保持契約	14	
	6.(2)利用者の訓練	6.(2)①	情報セキュリティの教育及び訓練	15	
	6.(3)セキュリティ事件・事故 及び誤動作への対処	6.(3)①	セキュリティ事件・事故の報告	16	6
		6.(3)②	セキュリティの弱点の報告	17	7
		6.(3)③	ソフトウェアの誤動作の報告	18	8
		6.(3)④	事件・事故からの学習	19	
		6.(3)⑤	懲戒手続	20	
7. 物理的 及び,環境的セキュリティ	7.(1)物理的セキュリティ境界	7.(1)①	物理的セキュリティ境界	21	9
		7.(1)②	物理的入退管理策	22	10
		7.(1)③	オフィス、部屋及び施設のセキュリティ	23	
		7.(1)④	セキュリティが保たれた領域での作業	24	11
		7.(1)⑤	受渡し場所の隔離	25	12
	7.(2)装置のセキュリティ	7.(2)④	装置の保守	26	
		7.(2)⑥	装置の安全な処分又は再使用	27	13
	7.(3)その他の管理策	7.(3)①	クリアデスク及びクリアスクリーンの個別方針	28	14
					15
		7.(3)②	資産の移動	29	16
8. 通信及び運用管理	8.(1)運用手順及び責任	8.(1)①	操作手順書	30	
		8.(1)②	運用変更管理	31	
		8.(1)③	事件・事故管理手順	32	
	8.(3)悪意のある ソフトウェアからの保護	8.(3)①	悪意のあるソフトウェアに対する管理策	33	17
				34	
	8.(4)システムの維持管理	8.(4)①	情報のバックアップ	35	18
		8.(4)②	運用の記録	36	
		8.(4)③	障害記録		
	8.(5)ネットワークの管理	8.(5)①	ネットワーク管理策	37	
	8.(6)媒体の取扱い及びセキュリティ	8.(6)①	コンピュータの取外し可能な附属媒体の管理	38	19
		8.(6)②	媒体の処分	39	20
		8.(6)③	情報の取扱手順	40	21
		8.(6)④	システムに関する文書のセキュリティ	41	
	8.(7)情報及びソフトウェアの交換	8.(7)①	情報及びソフトウェアの交換契約	42	22
		8.(7)②	配送中の媒体のセキュリティ	43	23
		8.(7)③	電子商取引のセキュリティ	44	24
		8.(7)④	電子メールのセキュリティ	45	25
		8.(7)⑥	公開されているシステム	46	
		8.(7)⑦	情報交換その他の方式	47	26
9. アクセス制御	9.(2)利用者のアクセス管理	9.(2)①	利用者登録	48	
		9.(2)②	特権管理	49	
		9.(2)③	利用者のパスワードの管理	50	27
		9.(2)④	利用者アクセス権の見直し	51	
	9.(3)利用者の責任	9.(3)①	パスワードの使用	52	28
		9.(3)②	利用者領域にある無人運転の装置	53	
	9.(4)ネットワークのアクセス制御	9.(4)①	ネットワークサービスの使用についての個別方針	54	
		9.(4)③	外部から接続する利用者の認証	55	
		9.(4)⑤	遠隔診断用ポートの保護	56	
	9.(5)オペレーティングシステム のアクセス制御	9.(5)①	自動の端末識別	57	
	9.(6)業務用ソフトウェアのアクセス制御	9.(6)①	情報へのアクセス制限	58	
	9.(7)システムアクセス及び システム使用状況の監視	9.(7)①	事象の記録	59	
		9.(7)③	コンピュータ内の時計の同期	60	
	9.(8)移動型計算処理及び遠隔作業	9.(8)①	移動型計算処理	61	29
					30
					31
					32
		9.(8)②	遠隔作業	62	33
					34
10. システムの開発 及び、保守	10.(2)業務用システムのセキュリティ	10.(2)①	入力データの妥当性確認	63	
	10.(3)暗号による管理策	10.(3)①	暗号による管理策の使用に関する個別方針	64	
	10.(4)システムファイルのセキュリティ	10.(4)①	運用ソフトウェアの管理	65	
	10.(5)開発及び支援過程 におけるセキュリティ	10.(5)①	変更管理手順	66	
11. 事業継続管理	11.(1)事業継続管理の種々の面	11.(1)①	事業継続管理手続	67	
12. 適合性	12.(1)法的要求事項への適合	12.(1)①	適用法令の識別	68	
		12.(1)②	知的所有権 (IPR)	69	35
					36
		12.(1)③	組織の記録の保護	70	
		12.(1)④	データの保護及び個人情報の保護	71	
		12.(1)⑦	証拠の収集	72	