JIS_Q_27001:2023 附属書A				JIS_Q_27001:2014 附属書A				
	管理策			管理目的		管理策		
5 組織的管理策	1	情報セキュリティのための方針群	情報セキュリティ方針及びトピック固有の方針は、これを定義し、管理層が承認し、発行し、関連する要員及び関連する利害関係者に伝達し、認識させ、あらかじめ定めた間隔で、及び重大な変化が発生した場合に、レビューしなければならない。	群 5 情報セキュリティのための方針	性 1 情報セキュリティのための経営陣の方向	1	情報セキュリティのための方針群	情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員及び関連する外部関係者に通知しなければならない。
5 組織的管理策	2	情報セキュリティの役割及び責任	情報セキュリティの役割及び責任は、組織のニーズに従って定め、割り当てなければならない。			2	情報セキュリティのための方針群のレビュー	情報セキュリティのための方針群は、あらかじめ定めた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当かつ有効であることを確実にするためにレビューしなければならない。
5 組織的管理策	3	職務の分離	相反する職務及び相反する責任範囲は、分離しなければならない。	6 情報セキュリティのための組織	1 内部組織	1	情報セキュリティの役割及び責任	全ての情報セキュリティの責任を定め、割り当てなければならない。
5 組織的管理策	4	管理層の責任	管理層は、組織の確立された情報セキュリティ方針、トピック固有の方針及び手順に従った情報セキュリティの適用を、全ての要員に要求しなければならない。			2	職務の分離	相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離しなければならない。
5 組織的管理策	5	関係当局との連絡	組織は、関係当局との適切な連絡体制を確立し、維持しなければならない。			3	関係当局との連絡	関係当局との適切な連絡体制を維持しなければならない。
5 組織的管理策	6	専門組織との連絡	組織は、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確立し、維持しなければならない。			4	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しなければならない。
5 組織的管理策	7	脅威インテリジェンス	情報セキュリティの脅威に関する情報を収集及び分析し、脅威インテリジェンスを構築しなければならない。			5	プロジェクトマネジメントにおける情報セキュリティ	プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組まなければならない。
5 組織的管理策	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	情報セキュリティをプロジェクトマネジメントに組み入れなければならない。		2 モバイル機器及びテレワーキング	1	モバイル機器の方針	モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用しなければならない。
5 組織的管理策	9	情報及びその他の関連資産の目録	情報及びその他の関連資産の目録を、それぞれの管理責任者を含めて作成し、維持しなければならない。			2	テレワーキング	テレワーキングの場所でアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施しなければならない。
5 組織的管理策	10	情報及びその他の関連資産の許容される利用	情報及びその他の関連資産の許容される利用に関する規則及び取扱手順は、明確にし、文書化し、実施しなければならない。	7 人的資源のセキュリティ	1 雇用前	1	選考	全ての従業員候補者についての経歴などの確認は、関連する法令、規制及び倫理に従って行わなければならない。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行わなければならない。
5 組織的管理策	11	資産の返却	要員及び必要に応じてその他の利害関係者は、雇用、契約又は合意の変更又は終了時に、自らが所持する組織の資産の全てを返却しなければならない。			2	雇用条件	従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任及び組織の責任を記載しなければならない。
5 組織的管理策	12	情報の分類	情報は、機密性、完全性、可用性及び関連する利害関係者の要求事項に基づく組織の情報セキュリティのニーズに従って、分類しなければならない。		2 雇用期間中	1	経営陣の責任	経営陣は、組織の確立された方針及び手順に従った情報セキュリティの適用を、全ての従業員及び契約相手に要求しなければならない。

5 組織的管理策	13	情報のラベル付け	情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施しなければならない。
5 組織的管理策	14	情報の転送	情報の転送の規則、手順又は合意を組織内及び組織と他の関係者との間の全ての種類の転送手段に関して備えなければならない。
5 組織的管理策	15	アクセス制御	情報及びその他の関連資産への物理的及び論理的アクセスを制御するための規則を、事業上及び情報セキュリティの要求事項に基づいて確立し、実施しなければならない。
5 組織的管理策	16	識別情報の管理	識別情報のライフサイクル全体を管理しなければならない。
5 組織的管理策	17	認証情報	認証情報の割当て及び管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理しなければならない。
5 組織的管理策	18	アクセス権	情報及びその他の関連資産へのアクセス権は、組織のアクセス制御に関するトピック固有の方針及び規則に従って、提供、レビュー、変更及び削除しなければならない。
5 組織的管理策	19	供給者関係における情報セキュリティ	供給者の製品又はサービスの利用に関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め、実施しなければならない。
5 組織的管理策	20	供給者との合意における情報セキュリティの取扱い	供給者関係の種類に応じて、関連する情報セキュリティ要求事項を確立し、各供給者と合意しなければならない。
5 組織的管理策	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	ICT製品及びサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め、実施しなければならない。
5 組織的管理策	22	供給者のサービス提供の監視、レビュー及び変更管理	組織は、供給者の情報セキュリティの活動及びサービス提供を定常的に監視し、レビューし、評価し、変更を管理しなければならない。
5 組織的管理策	23	クラウドサービスの利用における情報セキュリティ	クラウドサービスの調達、利用、管理及び利用終了のプロセスを、組織の情報セキュリティ要求事項に従って確立しなければならない。
5 組織的管理策	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	組織は、情報セキュリティインシデント管理のプロセス、役割及び責任を定め、確立し、伝達することによって、情報セキュリティインシデント管理を計画し、準備しなければならない。
5 組織的管理策	25	情報セキュリティ事象の評価及び決定	組織は、情報セキュリティ事象を評価し、それらを情報セキュリティインシデントに分類するか否かを決定しなければならない。

	中	2	情報セキュリティの意識向上、教育及び訓練	組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受けなければならず、また、定めに従ってその更新を受けなければならない。
		3	懲戒手続	情報セキュリティ違反を犯した従業員に対して処置をとるための、正式かつ周知された懲戒手続を備えなければならない。
	変更 3 雇用の終了及び	1	雇用の終了又は変更に関する責任	雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、その従業員又は契約相手に伝達し、かつ、遂行させなければならない。
8 資産の管理	1 資産に対する責任	1	資産目録	情報及び情報処理施設に関連する資産を特定しなければならない。また、これらの資産の目録を、作成し、維持しなければならない。
		2	資産の管理責任	目録の中で維持される資産は、管理されなければならない。
		3	資産利用の許容範囲	情報の利用の許容範囲、並びに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は、明確にし、文書化し、実施しなければならない。
		4	資産の返却	全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却しなければならない。
	2 情報分類	1	情報の分類	情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類しなければならない。
		2	情報のラベル付け	情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施しなければならない。
		3	資産の取扱い	資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施しなければならない。
	3 媒体の取扱い	1	取外し可能な媒体の管理	組織が採用した分類体系に従って、取外し可能な媒体の管理のための手順を実施しなければならない。
		2	媒体の処分	媒体が不要になった場合は、正式な手順を用いて、セキュリティを保って処分しなければならない。
		3	物理的媒体の輸送	情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護しなければならない。

5 組織的管理策	26	情報セキュリティインシデントへの対応	情報セキュリティインシデントは、文書化した手順に従って対応しなければならない。
5 組織的管理策	27	情報セキュリティインシデントからの学習	情報セキュリティインシデントから得られた知識は、情報セキュリティ管理策を強化し、改善するために用いらなければならない。
5 組織的管理策	28	証拠の収集	組織は、情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための手順を確立し、実施しなければならない。
5 組織的管理策	29	事業の中断・阻害時の情報セキュリティ	組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画しなければならない。
5 組織的管理策	30	事業継続のためのICTの備え	事業継続の目的及びICT継続の要求事項に基づいて、ICTの備えを計画し、実施し、維持し、試験しなければならない。
5 組織的管理策	31	法令、規則及び契約上の要求事項	情報セキュリティに関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組を特定し、文書化し、また、最新に保たなければならない。
5 組織的管理策	32	知的財産権	組織は、知的財産権を保護するための適切な手順を実施しなければならない。
5 組織的管理策	33	記録の保護	記録は、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護しなければならない。
5 組織的管理策	34	プライバシー及び個人識別可能情報（PII）の保護	組織は、適用される法令、規則及び契約上の要求事項に従って、プライバシーの維持及びPIIの保護に関する要求事項を特定し、満たさなければならない。
5 組織的管理策	35	情報セキュリティの独立したレビュー	人、プロセス及び技術を含む、情報セキュリティ及びその実施の管理に対する組織の取組みについて、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施しなければならない。
5 組織的管理策	36	情報セキュリティのための方針群、規則及び標準の順守	組織の情報セキュリティ方針、トピック固有の方針、規則及び標準を順守してるいることを定期的にレビューしなければならない。
5 組織的管理策	37	操作手順書	情報処理設備の操作手順は、文書化し、必要とする要員に対して利用可能にしなければならない。
6 人的管理策	1	選考	要員になる全て候補者についての経歴などの確認は、適用される法令、規制及び倫理を考慮に入れて組織に加わる前に、及びその後継続的に行わなければならない。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行わなければならない。

9 アクセス制御	1 アクセス制御に対する業務上の要求事項	1	アクセス制御方針	アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューしなければならない。
		2	ネットワーク及びネットワークサービスへのアクセス	利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを、利用者に提供しなければならない。
	2 利用者アクセスの管理	1	利用者登録及び登録削除	アクセス権の割当てを可能にするために、利用者の登録及び登録削除についての正式なプロセスを実施しなければならない。
		2	利用者アクセスの提供（provisioning）	全ての種類の利用者について、全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために、利用者アクセスの提供についての正式なプロセスを実施しなければならない。
		3	特権的アクセス権の管理	特権的アクセス権の割当て及び利用は、制限し、管理しなければならない。
		4	利用者の秘密認証情報の管理	秘密認証情報の割当ては、正式な管理プロセスによって管理しなければならない。
		5	利用者アクセス権のレビュー	資産の管理責任者は、利用者のアクセス権を定められた間隔でレビューしなければならない。
		6	アクセス権の削除又は修正	全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除しなければならず、また、変更に合わせて修正しなければならない。
	3 利用者の責任	1	秘密認証情報の利用	秘密認証情報の利用時に、組織の慣行に従うことを、利用者に要求しなければならない。
	4 システム及びアプリケーションのアクセス制御	1	情報へのアクセス制限	情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制限しなければならない。
		2	セキュリティに配慮したログオン手順	アクセス制御方針で求められている場合には、システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順によって制御しなければならない。
		3	パスワード管理システム	パスワード管理システムは、対話式でなければならず、また、良質なパスワードを確実とするものでなければならない。
		4	特権的なユーティリティプログラムの使用	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。

6 人的管理策	2	雇用条件	雇用契約書には、情報セキュリティに関する要員及び組織の責任を記載しなければならない。
6 人的管理策	3	情報セキュリティの意識向上、教育及び訓練	組織の要員及び関連する利害関係者は、職務に関連する組織の情報セキュリティ方針、トピック固有の方針及び手順についての、適切な、情報セキュリティに関する意識向上プログラム、教育及び訓練を受けなければならず、また、定常的な更新を受けなければならない。
6 人的管理策	4	懲戒手続	情報セキュリティ方針違反を犯した要員及びその他の関連する利害関係者に対して処置をとるために、懲戒手続きを正式に定め、伝達しなければならない。
6 人的管理策	5	雇用の終了又は変更後の責任	雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、施行し、関連する要員及びその他の利害関係者に伝達しなければならない。
6 人的管理策	6	秘密保持契約又は守秘義務契約	情報保護に対する組織の要求事項を反映する秘密保持契約又は守秘義務契約は、特定し、文書化し、定常的にレビューし、要員及びその他の関連する利害関係者が署名しなければならない。
6 人的管理策	7	リモートワーク	組織の構外でアクセス、処理又は保存される情報を保護するために、要員が遠隔で作業をする場合のセキュリティ対策を実施しなければならない。
6 人的管理策	8	情報セキュリティ事象の報告	組織は、要員が発見した又は疑いを持った情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告するための仕組みを設けなければならない。
第 7 物理的管理	1	物理的セキュリティ境界	情報及びその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いなければならない。
第 7 物理的管理	2	物理的入退	セキュリティを保つべき領域は、適切な入退管理策及びアクセス場所(受付など)によって保護しなければならない。
第 7 物理的管理	3	オフィス、部屋及び施設のセキュリティ	オフィス、部屋及び施設に対する物理的セキュリティを設計し、実装しなければならない。
第 7 物理的管理	4	物理的セキュリティの監視	施設は、許可していない物理的アクセスについて継続的に監視しなければならない。
第 7 物理的管理	5	物理的及び環境的脅威からの保護	自然災害及びその他の意図的又は意図的でない、インフラストラクチャに対する物理的脅威などの物理的及び環境的脅威に対する保護を設計し、実装しなければならない。
第 7 物理的管理	6	セキュリティを保つべき領域での作業	セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し、実装しなければならない。
	5	プログラムソースコードへのアクセス制御	プログラムソースコードへのアクセスは、制限しなければならない。
10 暗号	1 暗号による管理策	1 暗号による管理策の利用方針	情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施しなければならない。
		2 鍵管理	暗号鍵の使用、保護及び有効期間(lifetime)に関する方針を策定し、そのライフサイクル全体にわたって実施しなければならない。
11 物理的及び環境的セキュリティ	1 セキュリティを保つべき領域	1 物理的セキュリティ境界	取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いなければならない。
		2 物理的入退管理策	セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護しなければならない。
		3 オフィス、部屋及び施設のセキュリティ	オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用しなければならない。
		4 外部及び環境の脅威からの保護	自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用しなければならない。
		5 セキュリティを保つべき領域での作業	セキュリティを保つべき領域での作業に関する手順を設計し、適用しなければならない。
		6 受渡場所	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理しなければならない。また、可能な場合には、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離さなければならない。
	2 装置	1 装置の設置及び保護	装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、又は保護しなければならない。
		2 サポートユーティリティ	装置は、サポートユーティリティの不具合による、停電、その他の故障から保護しなければならない。
		3 ケーブル配線のセキュリティ	データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護しなければならない。
		4 装置の保守	装置は、可用性及び安全性を継続的に維持することを確実にするために、正しく保守しなければならない。

策 7 物理的管理	7	クリアデスク・クリアスクリーン	書類及び取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定義し、適切に実施させなければならない。
策 7 物理的管理	8	装置の設置及び保護	装置は、セキュリティを保って設置し、保護しなければならない。
策 7 物理的管理	9	構外にある資産のセキュリティ	構外にある資産を保護しなければならない。
策 7 物理的管理	10	記憶媒体	記憶媒体は、組織における分類体系及び取扱いの要求事項に従って、その取得、使用、移送及び廃棄のライフサイクルを通して管理しなければならない。
策 7 物理的管理	11	サポートユーティリティ	情報処理施設・設備は、サポートユーティリティの不具合による、停電、その他の中断から保護しなければならない。
策 7 物理的管理	12	ケーブル配線のセキュリティ	電源ケーブル、データ伝送ケーブル又は情報サービスを支援するケーブルの配線は、傍受、妨害又は損傷から保護しなければならない。
策 7 物理的管理	13	装置の保守	装置は、情報の可用性、完全性及び機密性を維持することを確実にするために、正しく保守しなければならない。
策 7 物理的管理	14	装置のセキュリティを保った処分又は再利用	記憶媒体を内蔵した装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保てるよう上書きしていることを確実にするために、検証しなければならない。
8 技術的管理策	1	利用者エンドポイント機器	利用者エンドポイント機器に保存されている情報、処理される情報、又は利用者エンドポイント機器を介してアクセス可能な情報を保護しなければならない。
8 技術的管理策	2	特権的アクセス権	特権的アクセス権の割当て及び利用は、制限し、管理しなければならない。
8 技術的管理策	3	情報へのアクセス制限	情報及びその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の個別方針に従って、制限しなければならない。
8 技術的管理策	4	ソースコードへのアクセス	ソースコード、開発ツール、及びソフトウェアライブラリへの読取り及び書込みアクセスを適切に管理しなければならない。
8 技術的管理策	5	セキュリティを保った認証	セキュリティを保った認証技術及び手順を、情報へのアクセス制限、及びアクセス制御に関するトピック固有の方針に基づいて備えなければならない。

		5 資産の移動	装置、情報又はソフトウェアは、事前の許可なしでは、構外に持ち出してはならない。
		6 構外にある装置及び資産のセキュリティ	構外にある資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、セキュリティを適用しなければならない。
		7 装置のセキュリティを保った処分又は再利用	記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保って上書きしていることを確実にするために、検証しなければならない。
		8 無人状態にある利用者装置	利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にしなければならない。
		9 クリアデスク・クリアスクリーン方針	書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用しなければならない。
12 運用のセキュリティ	1 運用の手順及び責任	1 操作手順書	操作手順は、文書化し、必要とする全ての利用者に対して利用可能にしなければならない。
		2 変更管理	情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更は、管理しなければならない。
		3 容量・能力の管理	要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測しなければならない。
		4 開発環境、試験環境及び運用環境の分離	開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために、分離しなければならない。
	2 マルウェアからの保護	1 マルウェアに対する管理策	マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施しなければならない。
	3 バックアップ	1 情報のバックアップ	情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査しなければならない。
	4 ログ取得及び監視	1 イベントログ取得	利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューしなければならない。
		2 ログ情報の保護	ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護しなければならない。

8 技術的管理策	6	容量･能力の管理	現在及び予測される容量･能力の要求事項に合わせて、資源の利用を監視し、調整しなければならない。
8 技術的管理策	7	マルウェアに対する保護	マルウェアに対する保護を実施し、利用者の適切な認識によって支援しなければならない。
8 技術的管理策	8	技術的ぜい弱性の管理	利用中の情報システムの技術的ぜい弱性に関する情報を獲得しなければならない。また、そのようなぜい弱性に組織がさらされている状況を評価し、適切な手段をとらなければならない。
8 技術的管理策	9	構成管理	ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティ構成を含む構成を確立し、文書化し、実装し、監視し、レビューしなければならない。
8 技術的管理策	10	情報の削除	情報システム、装置又はその他の記憶媒体に保存している情報は、必要でなくなった時点で削除しなければならない。
8 技術的管理策	11	データマスキング	データマスキングは、適用される法令を考慮して、組織のアクセス制御に関するトピック固有の方針及びその他の関連するトピック固有の方針並びに事業上の要求事項に従って利用しなければならない。
8 技術的管理策	12	データ漏えい防止	データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存又は送信するシステム、ネットワーク及びその他の装置に適用しなければならない。
8 技術的管理策	13	情報のバックアップ	合意されたバックアップに関するトピック固有の方針に従って、情報、ソフトウェア及びシステムのバックアップコピーは、維持し、定期的に検査しなければならない。
8 技術的管理策	14	情報処理施設･設備の冗長性	情報処理施設･設備は、可用性の要求事項を満たすのに十分な冗長性をもって、導入しなければならない。
8 技術的管理策	15	ログ取得	活動、例外処理、過失及びその他の関連する事象を記録したログを取得し、保存し、保護し、分析しなければならない。
8 技術的管理策	16	監視活動	情報セキュリティインシデントの可能性を評価するために、ネットワーク、システム及びアプリケーションについて異常な挙動がないか監視し、適切な処置を講じなければならない。
8 技術的管理策	17	クロックの同期	組織が使用する情報処理システムのクロックは、組織が採用した時刻源と同期させなければならない。
8 技術的管理策	18	特権的なユーティリティプログラムの使用	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。
		3	実務管理者及び運用担当者の作業ログ	システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューしなければならない。
		4	クロックの同期	組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、単一の参照時刻源と同期させなければならない。
	5 運用ソフトウェアの管理	1	運用システムに関わるソフトウェアの導入	運用システムに関わるソフトウェアの導入を管理するための手順を実施しなければならない。
	6 技術的ぜい弱性管理	1	技術的ぜい弱性の管理	利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得しなければならない。また、そのようなぜい弱性に組織がさらされている状況を評価しなければならない。さらに、それらと関連するリスクに対処するために、適切な手段をとらなければならない。
		2	ソフトウェアのインストールの制限	利用者によるソフトウェアのインストールを管理する規則を確立し、実施しなければならない。
	7 情報システムの監査に対する考慮事項	1	情報システムの監査に対する管理策	運用システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意しなければならない。
13 通信のセキュリティ	1 ネットワークセキュリティ管理	1	ネットワーク管理策	システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御しなければならない。
		2	ネットワークサービスのセキュリティ	組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定しなければならず、また、ネットワークサービス合意書にもこれらを盛り込まなければならない。
		3	ネットワークの分離	情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離しなければならない。
	2 情報の転送	1	情報転送の方針及び手順	あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び管理策を備えなければならない。
		2	情報転送に関する合意	合意では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱わなければならない。
		3	電子的メッセージ通信	電子的メッセージ通信に含まれた情報は、適切に保護しなければならない。
		4	秘密保持契約又は守秘義務契約	情報保護に対する組織の要件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し、文書化しなければならない。

8 技術的管理策	19	運用システムへのソフトウェアの導入	運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順及び対策を実施しなければならない。
8 技術的管理策	20	ネットワークセキュリティ	システム及びアプリケーション内の情報を保護するために、ネットワーク及びネットワーク装置のセキュリティを保ち、管理し、制御しなければならない。
8 技術的管理策	21	ネットワークサービスのセキュリティ	ネットワークサービスのセキュリティ機能、サービスレベル及びサービス要求事項を特定し、実装し、監視しなければならない。
8 技術的管理策	22	ネットワークの分離	情報サービス、利用者及び情報システムは、組織のネットワーク上で、グループごとに分離しなければならない。
8 技術的管理策	23	ウェブ・フィルタリング	悪意のあるコンテンツにさらされることを減らすために、外部のウェブサイトへのアクセスを管理しなければならない。
8 技術的管理策	24	暗号の利用	暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施しなければならない。
8 技術的管理策	25	セキュリティに配慮した開発のライフサイクル	ソフトウェア及びシステムのセキュリティに配慮した開発のための規則を確立し、適用しなければならない。
8 技術的管理策	26	アプリケーションセキュリティの要求事項	アプリケーションを開発または取得する場合、情報セキュリティ要求事項を特定し、規定し、承認しなければならない。
8 技術的管理策	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	セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの開発活動に対して適用しなければならない。
8 技術的管理策	28	セキュリティに配慮したコーディング	セキュリティに配慮したコーディングの原則をソフトウェア開発に適用しなければならない。
8 技術的管理策	29	開発及び受入におけるセキュリティテスト	セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施しなければならない。
8 技術的管理策	30	外部委託による開発	組織は、外部委託したシステム開発に関する活動を指揮し、監視し、レビューしなければならない。
8 技術的管理策	31	開発環境、テスト環境及び本番環境の分離	開発環境、試験環境及び本番環境は、分離してセキュリティを保たなければならない。

14 システムの取得、開発及び保守	項1 情報システムのセキュリティ要求事	1	情報セキュリティ要求事項の分析及び仕様化	情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含めなければならない。
		2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護しなければならない。
		3	アプリケーションサービスのトランザクションの保護	アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護しなければならない。 - 不完全な通信 - 誤った通信経路設定 - 認可されてないメッセージの変更 - 認可されていない開示 - 認可されてないメッセージの複製又は再生
	2 開発及びサポートプロセスにおけるセキュリティ	1	セキュリティに配慮した開発のための方針	ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用しなければならない。
		2	システムの変更管理手順	開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理しなければならない。
		3	オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	オペレーティングプラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験しなければならない。
		4	パッケージソフトウェアの変更に対する制限	パッケージソフトウェアの変更は、抑止しなければならず、必要な変更だけに限らなければならない。また、全ての変更は、厳重に管理しなければならない。
		5	セキュリティに配慮したシステム構築の原則	セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用しなければならない。
		6	セキュリティに配慮した開発環境	組織は、全てのシステム開発ライフサイクルを含む、システム開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護しなければならない。
		7	外部委託による開発	組織は、外部委託したシステム開発活動を監督し、監視しなければならない。
		8	システムセキュリティの試験	セキュリティ機能(functionality)の試験は、開発期間中に実施しなければならない。
		9	システムの受入れ試験	新しい情報システム、及びその改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立しなければならない。
	タ 3 試験デー	1	試験データの保護	試験データは、注意深く選定し、保護し、管理しなければならない。

8 技術的管理策	32	変更管理	情報処理施設と情報システムへの変更は、変更管理手順に従わなければならない。
8 技術的管理策	33	テスト用情報	テスト用情報は、適切に選定し、保護し、管理しなければならない。
8 技術的管理策	34	監査におけるテスト中の情報システムの保護	運用システムのアセスメントを伴う監査におけるテスト及びその他の保証活動を計画し、テスト実施者と適切な管理者との間で合意しなければならない。

15 供給者関係	1 供給者関係における情報セキュリティ	1	供給者関係のための情報セキュリティ方針	組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化しなければならない。
		2	供給者との合意におけるセキュリティの取扱い	関連する全ての情報セキュリティ要求事項を確立しなければならず、また、組織の情報に対して、アクセス、処理、保存若しくは通信を行う、又は組織の情報のためのIT基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意しなければならない。
		3	ICTサプライチェーン	供給者との合意には、情報通信技術(ICT)サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めなければならない。
	2 供給者のサービス提供の管理	1	供給者のサービス提供の監視及びレビュー	組織は、供給者のサービス提供を定常的に監視し、レビューし、監査しなければならない。
		2	供給者のサービス提供の変更に対する管理	関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、供給者によるサービス提供の変更(現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む。)を管理しなければならない。
16 情報セキュリティインシデント管理	1 情報セキュリティインシデントの管理及びその改善	1	責任及び手順	情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立しなければならない。
		2	情報セキュリティ事象の報告	情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告しなければならない。
		3	情報セキュリティ弱点の報告	組織の情報システム及びサービスを利用する従業員及び契約相手に、システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は、どのようなものでも記録し、報告するように要求しなければならない。
		4	情報セキュリティ事象の評価及び決定	情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定しなければならない。
		5	情報セキュリティインシデントへの対応	情報セキュリティインシデントは、文書化した手順に従って対応しなければならない。
		6	情報セキュリティインシデントからの学習	情報セキュリティインシデントの分析及び解決から得られた知識は、インシデントが将来起こる可能性又はその影響を低減するために用いらなければならない。
		7	証拠の収集	組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用しなければならない。
17 事業継続の側面	1 情報セキ	1	情報セキュリティ継続の計画	組織は、困難な状況(adverse situation)(例えば、危機又は災害)における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定しなければならない。

	続マネジメントにおける情報セキュリ	ユリティ継続	2	情報セキュリティ継続の実施	組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立し、文書化し、実施し、維持しなければならない。
			3	情報セキュリティ継続の検証、レビュー及び評価	確立及び実施した情報セキュリティ継続のための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために、組織は、定められた間隔でこれらの管理策を検証しなければならない。
		2 冗長性	1	情報処理施設の可用性	情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入しなければならない。
	1 8 順守	1 法的及び契約上の要求事項の順守	1	適用法令及び契約上の要求事項の特定	各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保たなければならない。
			2	知的財産権	知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施しなければならない。
			3	記録の保護	記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護しなければならない。
			4	プライバシー及び個人を特定できる情報(PII)の保護	プライバシー及びPIIの保護は、関連する法令及び規制が適用される場合には、その要求に従って確実にしなければならない。
			5	暗号化機能に対する規制	暗号化機能は、関連する全ての協定、法令及び規制を順守して用いなければならない。
		2 情報セキュリティのレビュー	1	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管理(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)に対する組織の取組みについて、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施しなければならない。
			2	情報セキュリティのための方針群及び標準の順守	管理者は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類、及び他の全てのセキュリティ要求事項を順守してるいることを定期的にレビューしなければならない。
			3	技術的順守のレビュー	情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューしなければならない。

適用宣言書

趣旨・目的

「適用宣言書」（以下、本宣言書）は、株式会社三重県農協情報センター（以下、当社）でISMS構築に伴い、JIS_Q_27001:2023内に書かれている管理策の基準項目を使い、当社が実施する基準項目及びその理由等を記載したものである。

適用対象者

本宣言書は、株式会社三重県農協情報センターにて業務を遂行する全従業員に適用される。

その他

本書の規格条項番号は、JIS_Q_27001:2023の項番を参照しています。

代表取締役社長　藤井　義裕

改定履歴

Ver.	改訂日	変更内容	作成者
1.0	2005年6月21日	新規	情報セキュリティ委員会
2.0	2005年11月1日	詳細管理策9.(8)①	情報セキュリティ委員会
3.0	2006年11月1日	ISO／IEC27001(JIS_Q_27001)への移行に伴う見直し	情報セキュリティ委員会
4.0	2008年10月30日	社長交代	情報セキュリティ委員会
5.0	2010年8月31日	役員執行体制の変更および規程名称変更に伴う見直し等	情報セキュリティ委員会
6.0	2012年4月1日	Pマークに関する記述を削除	情報セキュリティ委員会
7.0	2012年10月1日	情報セキュリティ対策規程の改正に伴う見直し	情報セキュリティ委員会
8.0	2014年10月24日	ISO／IEC27001:2013(JIS_Q_27001:2014)への移行に伴う見直し	情報セキュリティ委員会
9.0	2016年9月1日	情報資産管理台帳の改善にともなう見直し	情報セキュリティ委員会
10.0	2020年9月1日	在宅勤務開始および規程名称変更に伴う見直し	情報セキュリティ委員会
11.0	2021年12月1日	パスワードポリシー変更に伴う見直し 14.1.2「公衆ネットワーク上のアプリケーションサービスのセキュリティ考慮」	情報セキュリティ委員会
11.1	2022年9月30日	規程制定に伴う、名称の変更 個人情報保護基本規程 → 個人情報取扱規程 個人情報管理規程 → 個人情報取扱細則	情報セキュリティ委員会
11.2	2023年10月1日	要領名称修正(リモート勤務実施要領)、記録様式名称修正	情報セキュリティ委員会
12.0	2024年10月8日	ISO／IEC27001:2022(JIS_Q_27001:2023)への移行に伴う見直し	情報セキュリティ委員会

ISO 27001:2023 附属書A				ISO 27002:2024		適用						管理策			情報セキュリティ特性			サイバーセキュリティ概念					運用機能											セキュリティドメイン			
		管理策		目的		採否	主な対策・選択および除外の理由等	規程等文書	記録	備考	区分	予防	検知	是正	機密性	完全性	可用性	識別	防御	検知	対応	復旧	ガバナンス	資産管理	情報保護	人的資源のセキュリティ	物理的セキュリティ	システムおよびネットワークのセキュリティ	アプリケーションセキュリティ	セキュリティを保った構成	識別情報およびアクセスの管理	脅威および脆弱性の管理	継続	供給者関係のセキュリティ	法令および順守	情報セキュリティ事象管理	情報セキュリティ保証	ガバナンスおよびエコシステム	保護	防御	レジリエンス
第5章 組織的管理策	1	情報セキュリティのための方針群	情報セキュリティ方針およびトピック固有の方針は、これを定義し、管理層が承認し、発行し、関連する要員および関連する利害関係者に伝達し、認識させ、あらかじめ定めた間隔で、および重大な変化が発生した場合に、レビューしなければならない。	事業、法令、規制、契約上の要求事項に従って、情報セキュリティに対する管理層の指示および支援の継続的な適合性、適切性、有効性を確実にするため。		採	情報セキュリティ委員会指揮のもとリスクアセスメント等を実施し、レビューしている。	・リスクアセスメントマネジメント報告書		旧「A.5.1.1 」「A.5.1.2」	統合																							ガバナンスおよびエコシステム			
						採		・情報セキュリティ基本方針 第14条 評価および見直し ・情報セキュリティ対策規程 第36条 情報セキュリティポリシーの評価および見直し			予防			機密性	完全性	可用性	識別					ガバナンス																レジリエンス
第5章 組織的管理策	2	情報セキュリティの役割および責任	情報セキュリティの役割および責任は、組織のニーズに従って定め、割り当てなければならない。	組織内における情報セキュリティの実施、運用および管理のために、定義され、承認され、理解される構造を確立するため。		採	情報セキュリティ管理組織および体制を構築し、役割および責任を定めている。	・セキュリティ組織図		旧「A.6.1.1」																								ガバナンスおよびエコシステム			
						採		・情報セキュリティ対策規程 第3条 情報セキュリティ管理組織体制の役割			予防			機密性	完全性	可用性	識別					ガバナンス																レジリエンス
第5章 組織的管理策	3	職務の分離	相反する職務および相反する責任範囲は、分離しなければならない。	情報セキュリティ管理策の不正、誤りおよび回避のリスクを軽減するため。		採	情報セキュリティ対策規程等に記載されているルールに従い分離している。			旧「A.6.1.2」																								ガバナンスおよびエコシステム			
						採		・情報セキュリティ対策規程 第19条 情報処理設備管理 （4）職務の分離 ・システム開発規程 ・システム運用管理規程 ・ネットワーク管理規程			予防			機密性	完全性	可用性		防御				ガバナンス					識別情報およびアクセスの管理										
第5章 組織的管理策	4	管理層の責任	管理層は、組織の確立された情報セキュリティ方針、トピック固有の方針および手順に従った情報セキュリティの適用を、全ての要員に要求しなければならない。	管理層が、情報セキュリティにおける自らの役割を理解し、全ての要員が自らの情報セキュリティの責任を認識し、果たすことを確実にすることを目的として行動することを確実にするため。		採	情報セキュリティ基本方針等で要求している。			旧「A.7.2.1」																								ガバナンスおよびエコシステム			
						採		・情報セキュリティ基本方針 ・情報セキュリティ対策規程 ・各種規程			予防			機密性	完全性	可用性	識別					ガバナンス																
第5章 組織的管理策	5	関係当局との連絡	組織は、関係当局との適切な連絡体制を確立し、維持しなければならない。	組織と、関係する法務、規制および監督当局との間で、情報セキュリティに関して適切な情報の流通が行われることを確実にするため。		採	情報セキュリティ対策規程の組織体制の役割に従い対応している。また、各部門においても各々関係組織との適切な関係を維持している。	・情報セキュリティ対策規程 第3条 情報セキュリティ管理組織体制の役割 ・緊急時対応計画書	・法令・ガイドライン管理台帳	旧「A.6.1.3」																											
						採					予防			是正	機密性	完全性	可用性	識別	防御		対応	復旧	ガバナンス																	防御	レジリエンス
第5章 組織的管理策	6	専門組織との連絡	組織は、情報セキュリティに関する研究会または会議、およ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確立し、維持しなければならない。	情報セキュリティに関して適切な情報流通が行われることを確実にするため。		採	セキュリティ情報は、保守契約ベンダー等から入手している。日本規格協会、社団法人中部産業連盟、BSIジャパン等の研修会、説明会に参加している。			旧「A.6.1.4」																											
						採					予防			是正	機密性	完全性	可用性		防御		対応	復旧	ガバナンス																	防御	
第5章 組織的管理策	7	脅威インテリジェンス	情報セキュリティの脅威に関する情報を収集および分析し、脅威インテリジェンスを構築しなければならない。	適切なリスク低減処置を講じることが可能となるように、組織の脅威環境についての認識をもつため。		採	・組織の情報セキュリティリスクマネジメントプロセスの改善 ・技術的な予防および検知の管理策への追加 ・情報セキュリティ訓練のプロセスおよび手法 上記を踏まえて構築している。	・情報セキュリティ対策規程 第34条 緊急事態への対応	・LanScope Cat、m- FILTER関連資料/ログ ・疑似アタック試験関連資料	新規 IPAによる10大脅威(2024) ①ランサムウェアによる被害 ②サプライチェーンの弱点を悪用した攻撃 ③内部不正による情報漏えい等の被害 ④標的型攻撃による機密情報の窃取 ⑤修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃) ⑥不注意による情報漏えい等の被害 ⑦脆弱性対策情報の公開に伴う悪用増加 ⑧ビジネスメール詐欺による金銭被害 ⑨テレワーク等のニューノーマルな働き方を狙った攻撃 ⑩犯罪のビジネス化(アンダーグラウンドサービス) 規格書に、一般的には他の情報源が構築した脅威インテリジェンスを受取り、それを利用する、と記載されていることから、緊急時対応計画書に脅威インテリジェンスと入手源は必要ない判断と	新規																													
						採					予防	検知	是正		機密性	完全性	可用性	識別		検知	対応		ガバナンス	資産管理	情報保護						脅威および脆弱性の管理							防御	レジリエンス
第5章 組織的管理策	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	情報セキュリティをプロジェクトマネジメントに組み入れなければならない。	プロジェクトのライフサイクル全体を通して、プロジェクトマネジメントにおいて、プロジェクトおよび成果物に関する情報セキュリティに効果的に対処することを確実にするため。		採	経営会総にかかる企画・方策等を検討する企画会議、業務遂行の進捗を確認する統括会議、センター運営課題などを検討する情報センター運営対策会議、リスク管理に関する意思決定を行う内部管理委員会、情報セキュリティ全般を管理する情報セキュリティ委員会など部門横断的な会議体において取り組んでいる。	・情報セキュリティ対策規程 第7条 情報の管理方針 （4）プロジェクトにおける情報管理 第30条 情報システムに対するセキュリティ要件の明確化 第32条 情報システムの開発管理 ・システム運用管理規程 第13条 セキュリティ要件 ・システム開発規程 第5条 プロセス （1）要件定義 （3）セキュリティ要件の明確化	・会議録	新規 旧「A.6.1.5 」「A.14.1.1 」	（新規）																											
						採					予防				機密性	完全性	可用性	識別	防御	検知	対応	復旧	ガバナンス	資産管理	情報保護	人的資源のセキュリティ	物理的セキュリティ	システムおよびネットワークのセキュリティ	アプリケーションセキュリティ	セキュリティを保った構成	識別情報およびアクセスの管理	脅威および脆弱性の管理	継続	供給者関係のセキュリティ	法令および順守	情報セキュリティ事象管理	情報セキュリティ保証	ガバナンスおよびエコシステム	保護	防御	レジリエンス
第5章 組織的管理策	9	情報および その他の関連資産の目録	情報およびその他の関連資産の目録を、それぞれの管理責任者を含めて作成し、維持しなければならない。	組織の情報およびその他の関連資産を特定し、それらの情報セキュリティを維持し、適切な管理責任を割り当てるため。		採	情報資産管理台帳を作成し、管理責任者（部署）を明記し、管理を行い且つ定期的に資産の見直しを行っている。	・情報セキュリティ対策規程 第7条 情報の管理方針 （3）情報の管理簿 ・情報資産洗出し要領	・情報資産管理台帳 「緊急時対応計画書_別表4（業務別度旧判断基準） ・機器管理台帳（システム） ・ソフトウェア管理台帳（システム） ・LanScope ・文書管理システム ・書類管理システム ・設備管理システム ・各システムの管理書類 （分掌表・分担表・社内システム管理表）	旧「A.8.1.1 」「A.8.1.2」 大意は変化なし	統合																											
						採					予防				機密性	完全性	可用性	識別	防御					資産管理															ガバナンスおよびエコシステム	保護		
第5章 組織的管理策	10	情報およびその他の関連資産の許容される利用に関する規則および取扱手順は、明確にし、文書化し、実施しなければならない。	情報およびその他の関連資産の許容される利用に関する規則および取扱手順は、明確にし、文書化し、実施しなければならない。	情報およびその他の関連資産を適切に保護し、利用し、取り扱うことを確実にするため。		採	・資産管理台帳に、利用者の範囲（部署）を明記している。 システムで管理する情報資産やシステムの利用は ユーザID／パスワードでアクセス制御を実施している。 ・情報資産の取扱に関する手続きを定めている。 ・情報セキュリティ対策規程等に記載されているルールに従い実施している。	・情報資産洗出し要領 ・ネットワーク管理規程 ・アクセス制御管理規程 ・情報資産取扱規程 ・情報セキュリティ対策規程 第7条 情報の管理方針 （2）情報の取扱基準 ・個人情報取扱規程 ・個人情報取扱細則	・情報資産管理台帳 ・ユーザ／グループ登録依頼書 ・情報取扱申請書兼報告書（総秘／社外秘） ・厳秘情報利用許可申請書	新規 旧「A.8.1.3 」「A.8.2.3」 意味合いとしては大きな変更はない	（新規）																											
						採					予防				機密性	完全性	可用性		防御					資産管理	情報保護														ガバナンスおよびエコシステム	保護		
第5章 組織的管理策	11	資産の返却	要員および必要に応じてその他の利害関係者は、雇用、契約または合意の変更または終了時に、自らが所持する組織の資産の全てを返却しなければならない。	雇用、契約、または合意を変更または終了するプロセスの一環として、組織の資産を保護するため。		採	情報セキュリティ対策規程等でルール化している。	・情報セキュリティ対策規程 第11条 利用権限の承認 第12条 退職時の情報資産の返還	・誓約書	旧「A.8.1.4」																											
						採					予防				機密性	完全性	可用性		防御					資産管理																保護		
第5章 組織的管理策	12	情報の分類	情報は、機密性、完全性、可用性および関連する利害関係者の要求事項に基づく組織の情報セキュリティのニーズに従って、分類しなければならない。	組織における情報の重要度に従って、情報の保護のニーズを特定し、理解することを確実にするため。		採	情報セキュリティ対策規程等に記載されているルールに従い分類している。	・情報セキュリティ対策規程 第6条 情報の分類 ・情報資産取扱規程 ・情報リスクアセスメントマネジメント要領_別表2(分類基準表) ・情報資産洗出し要領		旧「A.8.2.1」																											
						採					予防				機密性	完全性	可用性	識別	防御							情報保護														保護	防御	
第5章 組織的管理策	13	情報のラベル付け	情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施しなければならない。	情報の分類の伝達を容易にし、情報の処理および管理の自動化を支援するため。		採	情報セキュリティ対策規程等に記載されているルールに従い実施している。	・情報セキュリティ対策規程 第7条 情報の管理方針 ・情報資産取扱規程 第4条 情報の表示 ・情報リスクアセスメントマネジメント要領_別表2(分類基準表) ・情報資産洗出し要領		旧「A.8.2.2」 変化なし																											
						採					予防				機密性	完全性	可用性		防御							情報保護														保護	防御	
第5章 組織的管理策	14	情報の転送	情報の転送の規則、手順または合意を組織内および組織と他の関係者との間の全ての種類の転送手段に関して備えなければならない。	組織内および外部の利害関係者との間で転送される情報のセキュリティを維持するため。		採	情報セキュリティ対策規程等に記載されているルールに従い備えている。	・情報セキュリティ対策規程 第22条 情報およびソフトウェアの交換に関する管理 （1）情報およびソフトウェアの交換 （2）電子メールの管理 （4）電話、ファクシミリ等の情報交換時の管理 ・電子メール利用規程 第7条 電子メール利用ルール ・情報セキュリティインシデント対策管理規程 ・ネットワーク管理規程 ・FAX送受信取扱要領	・FAXログ ・FAX送受信管理簿 ・e-FILTERログ ・ウィルスゲートウェイログ（Fortigate）	旧「A.13.2.1」「A.13.2.2」「A.13.2.3」	統合																											
						採					予防				機密性	完全性	可用性		防御					資産管理	情報保護															保護		
第5章 組織的管理策	15	アクセス制御	情報およびその他の関連資産への物理的および論理的アクセスを制御するための規則を、事業および情報セキュリティの要求事項に基づいて確立し、実施しなければならない。	情報およびその他の関連資産への認可されたアクセスを行わせ、認可されていないアクセスを防ぐことを確実にするため。		採	情報セキュリティ対策規程等に記載されているルールに従い実施している。	・情報セキュリティ対策規程 第23条 アクセス制御に関する業務上の要求事項 第27条 ネットワークのアクセス制御 （1）ネットワークサービス使用時の個別方針 ・アクセス制御管理規程 第3条 方針および業務上の要求事項 ・ネットワーク管理規程 第21条 資源へのアクセス権		旧「A.9.1.2」																											
						採					予防				機密性	完全性	可用性		防御													識別情報およびアクセスの管理							保護		
第5章 組織的管理策	16	識別情報の管理	識別情報のライフサイクル全体を管理しなければならない。	組織の情報およびその他の関連資産にアクセスする個人およびシステムを一意に特定できるようにし、アクセス権を適切に割り当てることができるようにするため。		採	情報セキュリティ対策規程等に記載されているルールに従い管理している。	・情報セキュリティ対策規程 第24条 情報利用者のアクセス管理 ・アクセス制御管理規程 第4条 システム利用者登録 ・ネットワーク管理規程 第13条 利用者ID申請 第14条 利用者ID登録・変更・削除	・ユーザ／グループ登録依頼書 ・システムライフサイクル一覧	旧「A.9.2.1」																											
						採					予防				機密性	完全性	可用性		防御													識別情報およびアクセスの管理							保護		
第5章 組織的管理策	17	認証情報	認証情報の割当ておよび管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理しなければならない。	適切なエンティティ認証を確実にし、認証プロセスの失敗を防ぐため。		採	情報セキュリティ対策規程等に記載されているルールに従い管理している。 パスワードは、規程どおりの基準文字で構成されていないと登録できないシステムで制限している。	・情報セキュリティ対策規程 第25条 パスワード使用における注意事項 第26条 システムへのアクセス制御 ・アクセス制御管理規程 第7条 パスワードの使用 ・ネットワーク管理規程 第18条 パスワードの有効期限 第20条 初期パスワードの設定 ・クライアントPC管理規程 第2条 クライアントPCの管理	ユーザID一覧表	旧「A.9.2.4」「A.9.3.1」「A.9.4.3」	統合																											
						採					予防				機密性	完全性	可用性		防御													識別情報およびアクセスの管理							保護		

5組織的管理策	18	アクセス権	情報およびその他の関連資産へのアクセス権は、組織のアクセス制御に関するトピック固有の方針および規則に従って、提供、レビュー、変更および削除しなければならない。	情報およびその他の関連資産へのアクセスを、事業上の要求事項に従って定義し、認可することを確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い実施している。	・情報セキュリティ対策規程 第24条 情報利用者のアクセス管理 第25条 パスワード使用における注意事項 第28条 システムへのアクセス制御 ・アクセス制御管理規程 第4条 システム利用者登録 第6条 システム利用者のパスワード管理 ・クライアントPC管理規程 第2条 クライアントPCの管理 ・ネットワーク管理規程 第11条 利用者ID管理運用 第13条 利用者ID申請 ・入退カード管理規程 第10条 返却	ユーザID一覧表 ユーザID見直し報告書 ・誓約書 ・入退カード申請書 ・ユーザ／グループ登録依頼書	旧「A.9.2.2」「A.9.2.5」「A.9.2.4」 大意としての変更はなし	統合	予防			機密性	完全性	可用性		防御												識別情報およびアクセスの管理								保護		
策5組織的管理	19	供給者関係における情報セキュリティ	供給者の製品またはサービスの利用に関連する情報セキュリティリスクを管理するためのプロセスおよび手順を定め、実施しなければならない。	供給者関係において合意したレベルの情報セキュリティを維持するため。	採	情報セキュリティ対策規程等に記載されているルールに従い実施している。	・情報セキュリティ対策規程 第5条 情報利用者 第15条 外部委託 ・外部委託管理規程	・業務委託契約	旧「A.15.1.1」		予防			機密性	完全性	可用性	識別																供給者関係のセキュリティ				ガバナンスおよびエコシステム	保護		
策5組織的管理	20	供給者との合意における情報セキュリティの取扱い	供給者関係の種類に応じて、関連する情報セキュリティ要求事項を確立し、各供給者と合意しなければならない。	供給者関係において合意したレベルの情報セキュリティを維持するため。	採	情報セキュリティ対策規程等に記載されているルールに従っている。	・情報セキュリティ対策規程 第5条 情報利用者 第15条 外部委託 ・外部委託管理規程	・業務委託契約	旧「A.15.1.2」		予防			機密性	完全性	可用性	識別																供給者関係のセキュリティ				ガバナンスおよびエコシステム	保護		レジリエンス
5組織的管理策	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	ICT製品およびサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセスおよび手順を定め、実施しなければならない。	供給者関係において合意したレベルの情報セキュリティを維持するため。	採	情報セキュリティ対策規程等に記載されているルールに従い実施している。	・情報セキュリティ対策規程 第15条 外部委託 ・外部委託管理規程 第7条 委託先の管理・監督 第8条 検収 ・外部クラウドの利用方針	・業務委託契約	新規 旧「A.15.1.3」 ※外部クラウドの利用もサプライチェーンに含まれる。	(新規)	予防			機密性	完全性	可用性	識別																供給者関係のセキュリティ				ガバナンスおよびエコシステム	保護		
策5組織的管理	22	供給者のサービス提供の監視、レビューおよび変更管理	組織は、供給者の情報セキュリティの活動およびサービス提供を定常的に監視し、レビューし、評価し、変更を管理しなければならない。	供給者との合意に沿って、合意したレベルの情報セキュリティおよびサービス提供を維持するため。	採	情報セキュリティ対策規程等に記載されているルールに従い管理している。	・情報セキュリティ対策規程 第15条 外部委託 ・外部委託管理規程 第7条 委託先の管理・監督 第8条 検収	ベンダー定例会議議事録 ベンダー報告書等	旧「A.15.2.1」「A.15.2.2」	統合	予防			機密性	完全性	可用性	識別																供給者関係のセキュリティ			情報セキュリティ保証	ガバナンスおよびエコシステム	保護	防御	
5組織的管理策	23	クラウドサービスの利用における情報セキュリティ	クラウドサービスの調達、利用、管理および利用終了のプロセスを、組織の情報セキュリティ要求事項に従って確立しなければならない。	クラウドサービスの利用における情報セキュリティを規定し、管理するため。	採	・クラウドサービスの利用に関するトピック固有の個別方針の確立 ・クラウドサービスの選定基準、利用の範囲、役割および責任 ・クラウドサービスプロバイダが提供する情報セキュリティ機能が自らのセキュリティ要求事項を満たすことの確認 ・クラウドサービス利用時の情報のバックアップ手法 ・クラウドサービス利用終了時のデータ削除	・外部クラウドの利用方針 ・外部クラウド利用チェックリスト運用ガイドライン	・SaaS利用時のチェックポイント ・外部クラウド利用チェックリスト	新規	新規	予防			機密性	完全性	可用性		防御															供給者関係のセキュリティ				ガバナンスおよびエコシステム	保護		
5組織的管理策	24	情報セキュリティインシデント管理の計画策定および準備	組織は、情報セキュリティインシデント管理のプロセス、役割および責任を定め、確立し、伝達することによって、情報セキュリティインシデント管理を計画し、準備しなければならない。	情報セキュリティ事象に関する伝達を含む、情報セキュリティインシデントへの迅速で、効果的で、一貫性があり、かつ、秩序のある対応を確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い準備している。	・情報セキュリティ対策規程 第19条 情報処理設備管理 (3)セキュリティ事件・事故管理手順 ・システム運用管理規程 第6条 オペレーション管理 ・ネットワーク管理規程 ・情報セキュリティインシデント対策管理規程 ・電子メール利用規程 ・情報セキュリティ事件・事故報告規程	・システムログ ・障害報告書 ・情報セキュリティインシデント対応報告書	「A.16.1.1」				是正	機密性	完全性	可用性				対応	復旧	ガバナンス													情報セキュリティ事象管理				防御	
策5組織的管理	25	情報セキュリティ事象の評価および決定	組織は、情報セキュリティ事象を評価し、それらを情報セキュリティインシデントに分類するか否かを決定しなければならない。	情報セキュリティ事象の効果的な分類および優先順位付けを確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い、情報セキュリティ委員会にて検討し、決定している。	・情報セキュリティ対策規程 第14条 セキュリティ事件、事故等の対応 ・情報セキュリティ事件・事故報告規程 ・情報セキュリティインシデント対策管理規程	・障害報告書 ・情報セキュリティインシデント対応報告書	新規 旧「A.16.1.4」	(新規)		検知		機密性	完全性	可用性			検知	対応															情報セキュリティ事象管理				防御	
策5組織的管理	26	情報セキュリティインシデントへの対応	情報セキュリティインシデントは、文書化した手順に従って対応しなければならない。	情報セキュリティインシデントへの効率的かつ効果的な対応を確実にするため。	採	情報セキュリティ対策規程に従い、情報セキュリティ委員会にて検討し、対応している。	・情報セキュリティ対策規程 第14条 セキュリティ事件・事故等の対応 ・情報セキュリティ事件・事故報告規程 ・情報セキュリティインシデント対策管理規程	・障害報告書 ・情報セキュリティインシデント対応報告書	旧「A.16.1.5」 記述としては変化はなし				是正	機密性	完全性	可用性				対応	復旧														情報セキュリティ事象管理				防御	
策5組織的管理	27	情報セキュリティインシデントからの学習	情報セキュリティインシデントから得られた知識は、情報セキュリティ管理策を強化し、改善するために用いられなければならない。	将来のインシデントの起こりやすさ又は影響を減らすため。	採	情報セキュリティ対策規程に従い、情報セキュリティ委員会にて検討し、再発防止等に努めている。	・情報セキュリティ対策規程 第14条 セキュリティ事件・事故等の対応 ・情報セキュリティ事件・事故報告規程 ・情報セキュリテイインシデント対策管理規程	・障害報告書 ・情報セキュリテイインシデント対応報告書	旧「A.16.1.6」		予防			機密性	完全性	可用性	識別	防御																	情報セキュリティ事象管理				防御	
策5組織的管理	28	証拠の収集	組織は、情報セキュリティ事象に関連する証拠の特定、収集、取得および保存のための手順を確立し、実施しなければならない。	懲戒処置および法的処置の目的で、情報セキュリティインシデントに関連する証拠の一貫した効果的な管理を確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い実施している。 各種ログの保存、契約書管理、事故等の報告書管理	・情報セキュリティ対策規程 第35条 関連する法令の遵守 (3)証拠の収集		旧「A.16.1.7」				是正	機密性	完全性	可用性			検知	対応															情報セキュリティ事象管理				防御	
5組織的管理策	29	事業の中断・阻害時の情報セキュリティ	組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画しなければならない。	事業の中断・阻害時に情報およびその他の関連資産を保護するため。	採	情報セキュリティ対策規程等に記載されているルールに従い計画している。	・情報セキュリティ対策規程 第34条 緊急事態への対応 ・緊急時対応計画書		旧「A.17.1.1」「A.17.1.2」「A.17.1.3」	統合	予防		是正	機密性	完全性	可用性		防御		対応												継続						保護		レジリエンス
5組織的管理策	30	事業継続のためのICTの備え	事業継続の目的およびICT継続の要求事項に基づいて、ICTの備えを計画し、実施し、維持し、試験しなければならない。	事業の中断・阻害時に組織の情報およびその他の関連資産の可用性を確実にするため。	採	・事業影響度分析(BIA)の実施 事業活動の中断・阻害から生じる影響を経時的に評価し、優先的に復旧すべきICTサービス等を特定する。 ・復旧時間目標(RecoveryTimeObject)の設定 ICTサービス等をいつまでに復旧させるのかを目標として定める。 ・復旧ポイント目標((RecoveryPointObject)の設定 ICTサービス等をどの程度どのレベル、どのポイントまで復旧させるのかを目標として定める。 ・ICT継続計画の作成実施および試験 上記を考慮し、ICTサービスを求められる時間内までに必要なポイントまで復旧させるための計画を作成し、その試験／訓練などを行っている。	・緊急時対応計画書 目的	・緊急対策本部指揮訓練シナリオ	新規	新規			是正			可用性				対応												継続								レジリエンス
策5組織的管理	31	法令、規則および契約上の要求事項	情報セキュリティに関連する法令、規制および契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組を特定し、文書化し、また、最新に保たなければならない。	情報セキュリティに関連する法令、規制および契約上の要求事項の順守を確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い実施している。	・情報セキュリティ対策規程 第35条 関連する法令の遵守 (1)関連する法令の明確化	・法令・ガイドライン管理台帳	旧「A.18.1.1」「A.18.1.5」	統合	予防			機密性	完全性	可用性	識別																	法令および順守			ガバナンスおよびエコシステム	保護		
策5組織的管理	32	知的財産権	組織は、知的財産権を保護するための適切な手順を実施しなければならない。	知的財産権および権利関係のある製品の利用に関連する、法令、規制および契約上の要求事項の順守を確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い実施している。	・情報セキュリティ対策規程 第35条 関連する法令の遵守 (2)遵守策の策定と適用 ・ソフトウェア管理規程 第4条 ソフトウェア利用者の遵守事項	・ソフトウェア管理台帳	旧「A.18.1.2」		予防			機密性	完全性	可用性	識別																	法令および順守			ガバナンスおよびエコシステム			
5組織的管理策	33	記録の保護	記録は、消失、破壊、改ざん、認可されていないアクセスおよび不正な流出から保護しなければならない。	記録の保護および可用性に関連する、法令、規制および契約上の要求事項の順守、並びにコミュニティまたは社会の期待に応えることを確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い保護している。	・情報セキュリティ対策規程 第7条 情報の管理方針 第19条 情報処理設備管理 (9)情報のバックアップ (10)運用の記録 ・情報資産取扱規程 第5条 情報の保管		旧「A.18.1.3」		予防			機密性	完全性	可用性	識別	防御					資産管理	情報保護										法令および順守					防御	
策5組織的管理	34	プライバシーおよび個人識別可能情報(PII)の保護	組織は、適用される法令、規則および契約上の要求事項に従って、プライバシーの維持およびPIIの保護に関する要求事項を特定し、満たさなければならない。	PIIの保護の情報セキュリティの側面に関連する法令、規制および契約上の要求事項の順守を確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い実施している。	・情報セキュリティ対策規程 第8条 個人情報の保護 ・個人情報保護基本方針 ・個人情報取扱規程 ・個人情報取扱細則		旧「A.18.1.4」		予防			機密性	完全性	可用性	識別	防御						情報保護										法令および順守				保護		
5組織的管理策	35	情報セキュリティの独立したレビュー	人、プロセスおよび技術を含む、情報セキュリティおよびその実施の管理に対する組織の取組みについて、あらかじめ定めた間隔で、または重大な変化が生じた場合に、独立したレビューを実施しなければならない。	組織における情報セキュリティ管理の取組の、継続的な適切性、十分性および有効性を確実にするため。	採	内部監査実施計画に基づき監査を実施している。	・情報セキュリティ基本方針 第13条 監査 ・情報セキュリティ対策規程 第3条 情報セキュリティ管理組織体制の役割 (5) 監査室 第36条 情報セキュリティポリシーの評価および見直し ・内部監査規程 ・内部監査実施細則 ・内部監査実施要領	内部監査実施計画書 監査報告書	旧「A.18.2.1」		予防		是正	機密性	完全性	可用性	識別	防御																		情報セキュリティ保証	ガバナンスおよびエコシステム			
策5組織的管理	36	情報セキュリティのための方針群、規則および標準の順守	組織の情報セキュリティ方針、トピック固有の方針、規則および標準を順守していることを定期的にレビューしなければならない。	情報セキュリティを、組織の情報セキュリティ方針、トピック固有の方針、規則および標準に従って実施し、運用することを確実にするため。	採	情報セキュリティ基本方針等に記載されているルールに従い実施している。	・情報セキュリティ基本方針 第14条 評価および見直し ・情報セキュリティ対策規程 第36条 情報セキュリティポリシーの評価および見直し		旧「A.18.2.2」「A.18.2.3」	統合	予防			機密性	完全性	可用性	識別	防御																法令および順守		情報セキュリティ保証	ガバナンスおよびエコシステム			
策5組織的管理	37	操作手順書	情報処理設備の操作手順は、文書化し、必要とする要員に対して利用可能にしなければならない。	情報処理設備の正確で、かつ、セキュリティに配慮した操作を確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い実施している。	・情報セキュリティ対策規程 第19条 情報処理設備管理 (1)操作手順整備		旧「A.12.1.1」		予防		是正	機密性	完全性	可用性		防御			復旧		資産管理			物理的セキュリティ	システムおよびネットワークのセキュリティ	アプリケーションセキュリティ	セキュリティを保った構成	識別情報およびアクセスの管理	脅威およびぜい弱性の管理	継続			情報セキュリティ事象管理		ガバナンスおよびエコシステム	保護	防御	
6人的管理策	1	選考	要員になる全て候補者についての経歴などの確認は、適用される法令、規制および倫理を考慮に入れて組織に加わる前に、およびその後継続的に行わなければならない。また、この確認は、事業上の要求事項、アクセスされる情報の分類および認識されたリスクに応じて行わなければならない。	全ての要員が、予定する役割に対して適格かつ適切であり、雇用中に適格かつ適切であり続けることを確実にするため。	採	情報セキュリティ対策規程等のルールに従い実施している。	・情報セキュリティ対策規程 第9条 雇用における機密保持契約	・誓約書	旧「A.7.1.1」		予防			機密性	完全性	可用性		防御							人的資源のセキュリティ												ガバナンスおよびエコシステム			
6人的管理策	2	雇用条件	雇用契約書には、情報セキュリティに関する要員および組織の責任を記載しなければならない。	要員が、予定する役割における自らの情報セキュリティの責任を理解することを確実にするため。	採	情報セキュリティ対策規程等のルールに基づき記載している。	・情報セキュリティ対策規程 第9条 雇用における機密保持契約 第10条 情報利用者の権利と義務 第11条 利用権限の承認 第12条 退職時の情報資産の返還	・誓約書	旧「A.7.1.2」 ※誓約書は雇用契約書に準じたもの		予防			機密性	完全性	可用性		防御							人的資源のセキュリティ												ガバナンスおよびエコシステム			
6人的管理策	3	情報セキュリティの意識向上、教育および訓練	組織の要員および関連する利害関係者は、職務に関連する組織の情報セキュリティ方針、トピック固有の方針および手順についての、適切な、情報セキュリティに関する意識向上プログラム、教育および訓練を受けなければならず、また、定常的な更新を受けなければならない。	要員および関連する利害関係者が自らの情報セキュリティの責任を意識し、それを果たすことを確実にするため。	採	情報セキュリティポリシーや諸規程および年間計画書に基づき定期的に全従業員等に実施している。	・情報セキュリティ基本方針 第10条 教育・研修 ・情報セキュリティ対策規程 第13条 情報利用者への教育 ・セキュリティ教育実施規程	・セキュリティ教育計画 ・教育予定表兼実施結果報告書 ・出席者名簿	旧「A.7.2.2」		予防			機密性	完全性	可用性		防御							人的資源のセキュリティ												ガバナンスおよびエコシステム			

6人的管理策	4	懲戒手続	情報セキュリティ方針違反を犯した要員およびその他の関連する利害関係者に対して処置をとるために、懲戒手続きを正式に定め、伝達しなければならない。	要員およびその他の関連する利害関係者が情報セキュリティ方針違反の結果を理解すること、違反を抑止すること、およびそれを犯した要員およびその他の関連する利害関係者を適切に扱うことを確実にするため。	採	情報セキュリティポリシーおよび規程等に対する違反は、就業規則および情報セキュリティ基本方針等で規定している。	・情報セキュリティ基本方針 第11条 情報セキュリティに関する違反への対応 ・情報セキュリティ対策規程 第38条 違反に対する措置 ・就業規則		旧「A.7.2.3」		予防		是正	機密性	完全性	可用性		防御		対応					人的資源のセキュリティ												ガバナンスおよびエコシステム			
策6人的管理	5	雇用の終了または変更後の責任	雇用の終了または変更の後もなお有効な情報セキュリティに関する責任および義務を定め、施行し、関連する要員およびその他の利害関係者に伝達しなければならない。	雇用または契約を変更または終了する手続きの一部として、組織の利益を保護するため。	採	情報セキュリティ対策規程等でルール化している。	・情報セキュリティ対策規程 第11条 利用権限の承認 第12条 退職時の情報資産の返還	・誓約書	旧「A.7.3.1」		予防			機密性	完全性	可用性		防御					資産管理		人的資源のセキュリティ												ガバナンスおよびエコシステム			
6人的管理策	6	秘密保持契約または守秘義務契約	情報保護に対する組織の要求事項を反映する秘密保持契約または守秘義務契約は、特定し、文書化し、定常的にレビューし、要員およびその他の関連する利害関係者が署名しなければならない。	要員または外部の関係者がアクセスできる情報の秘密保持のため。	採	情報セキュリティ対策規程等でルール化している。	・情報セキュリティ対策規程 第9条 雇用における機密保持契約 第10条 情報利用者の権利と義務 第11条 利用権限の承認 第12条 退職時の情報資産の返還	・誓約書	旧「A.13.2.4」		予防			機密性				防御						情報保護	人的資源のセキュリティ								供給者関係のセキュリティ				ガバナンスおよびエコシステム			
策6人的管理	7	リモートワーク	組織の構外でアクセス、処理または保存される情報を保護するために、要員が遠隔で作業をする場合のセキュリティ対策を実施しなければならない。	要員が遠隔で作業をする場合の情報セキュリティを確実にするため。	採	リモート勤務実施要領、就業規則等に記載されているルールに従い実施している。	・リモート勤務実施要領 ・クライアントPC管理規程 第6条 クライアントPCの持ち出しおよび、貸し出し	・PC持ち出し申請書 兼返却報告書	旧「A.6.2.2」		予防			機密性	完全性	可用性		防御					資産管理	情報保護		物理的セキュリティ	システムおよびネットワークのセキュリティ											保護		
策6人的管理	8	情報セキュリティ事象の報告	組織は、要員が発見したまたは疑いを持った情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告するための仕組みを設けなければならない。	要員が、特定する可能性がある情報セキュリティ事象を、時機を失せず、一貫性をもって効果的に報告することを支援するため。	採	情報セキュリティ基本方針、情報セキュリティ対策規程、情報セキュリティ事件・事故報告規程等に基づきルール化している。	・情報セキュリティ対策規程 第14条 セキュリティ事件・事故等の対応 第32条 情報システムの開発管理 ・情報セキュリティ事件・事故報告規程	・障害報告書 ・是正予防対策計画書 ・是正予防対策計画管理台帳	旧「A.16.1.2」「A.16.1.3」	統合		検知		機密性	完全性	可用性			検知																情報セキュリティ事象管理				防御	
7物理的管理策	1	物理的セキュリティ境界	情報およびその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いなければならない。	組織の情報およびその他の関連資産への認可されていない物理的アクセス、損傷および干渉を防ぐため。	採	情報セキュリティ対策規程等に従いルール化している。また、入退室カードを使用して、境界ごと(部屋ごと)に入室許可を付与し管理している。	・情報セキュリティ対策規程 第16条 情報資産の保管や設置場所のセキュリティ ・施設管理規程 第20条 従業員等の入退館 ・入退カード管理規程 ・コンピュータ室等の入退管理要領	・入退管理システムのログ ・監視カメラ録画データ(約4ヵ月)	旧「A.11.1.1」		予防			機密性	完全性	可用性		防御								物理的セキュリティ												保護		
7物理的管理策	2	物理的入退	セキュリティを保つべき領域は、適切な入退管理策およびアクセス場所(受付など)によって保護しなければならない。	組織の情報およびその他の関連資産に、認可された物理的アクセスだけがなされることを確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い保護している。 入退室カードを使用して、境界ごと(部屋ごと)に入室許可を付与し管理している。 メール車との受け渡しは専用の部屋にて行い、個々の受発送についても発送室前で管理している。	・情報セキュリティ対策規程 第16条 情報資産の保管や設置場所のセキュリティ (4)受渡し場所の設置 ・施設管理規程 第3章 入退館管理 ・入退カード管理規程 ・コンピュータ室等の入退管理要領	・入退管理システムのログ ・監視カメラ録画データ(約4ヵ月)	旧「A.11.1.2」「A.11.1.6」	統合	予防			機密性	完全性	可用性		防御								物理的セキュリティ				識別情報およびアクセスの管理								保護		
策7物理的管理	3	オフィス、部屋および施設のセキュリティ	オフィス、部屋および施設に対する物理的セキュリティを設計し、実装しなければならない。	オフィス、部屋および施設内の組織の情報およびその他の関連資産への認可されていない物理的アクセス、損傷、および干渉を防ぐため。	採	情報セキュリティ対策規程等に記載されているルールに従い実装している。 入退室カードを使用して、境界ごと(部屋ごと)に入室許可を付与し管理している。	・情報セキュリティ対策規程 第16条 情報資産の保管や設置場所のセキュリティ ・施設管理規程 第20条 従業員等の入退館 ・コンピュータ室等の入退管理要領	・入退管理システムのログ ・監視カメラ録画データ(約4ヵ月)	旧「A.11.1.3」		予防			機密性	完全性	可用性		防御					資産管理			物理的セキュリティ												保護		
理策7物理的管	4	物理的セキュリティの監視	施設は、許可していない物理的アクセスについて継続的に監視しなければならない。	認可されていない物理的アクセスを検知し、抑止するため。	採	・入退管理システムの設置 ・警備員(守衛)の配置 ・侵入者警報を起動する接触式検知器の設置 ・個人情報に配慮した監視データの適正期間の保護 上記により継続的に監視している。	・情報セキュリテイ対策規程 第16条 情報資産の保管や設置場所のセキュリティ ・セコム・セキュリティサービス契約書 ・施設管理規程 第20条 従業員等の入退館	監視カメラ録画データ(約4ヵ月)	新規	新規	予防	検知		機密性	完全性	可用性		防御	検知							物理的セキュリティ												保護	防御	
理策7物理的管	5	物理的および環境的脅威からの保護	自然災害およびその他の意図的または意図的でない、インフラストラクチャに対する物理的脅威などの物理的および環境的脅威に対する保護を設計し、実装しなければならない。	物理的および環境的脅威に起因する事象の結果を防止または低減するため。	採	情報セキュリティ対策規程等に記載されているルールに従い実装している。 (建物はコンピュータ施設としての設計、ハロンガス、スプリンクラーおよび消火器等の設置、マシン室の耐震対策)	・情報セキュリティ対策規程 第16条 情報資産の保管や設置場所のセキュリティ ・施設管理規程 ・入退カード管理規程		旧「A.11.1.4」		予防			機密性	完全性	可用性		防御								物理的セキュリティ												保護		
7物理的管理策	6	セキュリティを保つべき領域での作業	セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し、実装しなければならない。	セキュリティを保つべき領域にある情報およびその他の関連資産を、この領域で作業する要員による損傷および認可されていない干渉から保護するため。	採	情報セキュリティ対策規程等に記載されているルールに従い実装している。 入退室カードを使用して、境界ごと(部屋ごと)に入室許可を付与し管理している。	・情報セキュリティ対策規程 第16条 情報資産の保管や設置場所のセキュリティ ・施設管理規程 第3章 入退館管理 ・入退カード管理規程 ・コンピュータ室等の入退管理要領	・入退管理システムのログ ・監視カメラ録画データ(約4ヵ月) ・コンピュータ室等入室許可申請書	旧「A.11.1.5」		予防			機密性	完全性	可用性		防御								物理的セキュリティ												保護		
策7物理的管理	7	クリアデスク・クリアスクリーン	書類および取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定義し、適切に実施させなければならない。	通常の勤務時間内および時間外の、机、スクリーンおよびその他アクセス可能な場所にある情報への認可されていないアクセス、情報の消失および損傷のリスクを低減するため。	採	情報セキュリティ対策規程等に記載されているルールに従い実施している。	・情報セキュリティ対策規程 第16条 情報資産の保管や設置場所のセキュリティ (5)クリアデスク、クリアスクリーン ・クライアントPC管理規程 第3条 クリアスクリーンの実施		旧「A.11.2.9」		予防			機密性				防御								物理的セキュリティ												保護		
理策7物理的管	8	装置の設置および保護	装置は、セキュリティを保って設置し、保護しなければならない。	物理的および環境的脅威、並びに認可されていないアクセスおよび損傷によるリスクを低減するため。	採	情報セキュリティ対策規程等に記載されているルールに従い保護している。	・情報セキュリティ対策規程 第17条 コンピュータ機器のセキュリティ		旧「A.11.2.1」		予防			機密性	完全性	可用性		防御					資産管理			物理的セキュリティ												保護		
7物理的管理策	9	構外にある資産のセキュリティ	構外にある資産を保護しなければならない。	構外にある装置・機器の紛失、損傷、盗難または侵害、および組織の業務の中断を防止するため。	採	情報セキュリティ対策規程等に記載されているルールに従い保護している。 (リモートワーク、受託システムの納品・保守等でのPC等持ち出し)	・情報セキュリティ対策規程 第7条 情報の管理方針 第8条 個人情報の保護 第9条 雇用における機密保持契約 ・情報資産取扱規程 第12条 承認手続き ・クライアントPC管理規程 第6条 クライアントPCの持ち出しおよび、貸し出し ・リモート勤務実施要領	・情報取扱申請書兼報告書(厳秘／社外秘) ・PC持ち出し申請書兼返却報告書	旧「A.11.2.6」		予防			機密性	完全性	可用性		防御					資産管理			物理的セキュリティ												保護		
7物理的管理策	10	記憶媒体	記憶媒体は、組織における分類体系および取扱いの要求事項に従って、その取得、使用、移送および廃棄のライフサイクルを通して管理しなければならない。	記憶媒体上の情報に対して認可された開示、変更、移動または破棄だけがなされることを確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い管理している。	・情報セキュリティ対策規程 第16条 情報資産の保管や設置場所のセキュリティ (6)資産の移動 第17条 コンピュータ機器のセキュリティ (4)機器管理・廃棄 第21条 媒体の取扱に関する管理 第22条 情報およびソフトウェアの交換に関する管理 (1)情報およびソフトウェアの交換 ・情報資産取扱規程 ・クライアントPC管理規程		旧「A.8.3.1」「A.8.3.2」「A.8.3.3」「A.11.2.5」	統合	予防			機密性	完全性	可用性		防御					資産管理			物理的セキュリティ												保護		
理策7物理的管	11	サポートユーティリティ	情報処理施設・設備は、サポートユーティリティの不具合による、停電、その他の中断から保護しなければならない。	サポートユーティリティの故障および中断・阻害による情報およびその他の関連資産の消失、損傷若しくは侵害、または組織の運用の中断を防止するため。	採	情報セキュリティ対策規程等に記載されているルールに従い保護している。	・情報セキュリティ対策規程 第17条 コンピュータ機器のセキュリティ (2)電源の確保		旧「A.11.2.2」		予防	検知			完全性	可用性		防御	検知							物理的セキュリティ												保護		
理策7物理的管	12	ケーブル配線のセキュリティ	電源ケーブル、データ伝送ケーブルまたは情報サービスを支援するケーブルの配線は、傍受、妨害または損傷から保護しなければならない。	電源ケーブおよび通信ケーブルの配線に関連した、情報およびその他の関連資産の消失、損傷、盗難または侵害、並びに組織の運用の中断を防止するため。	採	情報セキュリティ対策規程等に記載されているルールに従い保護している。	・情報セキュリティ対策規程 第17条 コンピュータ機器のセキュリティ (3)ケーブルのセキュリティ		旧「A.11.2.3」 大きな変更は無し		予防			機密性		可用性		防御								物理的セキュリティ												保護		
理策7物理的管	13	装置の保守	装置は、情報の可用性、完全性および機密性を維持することを確実にするために、正しく保守しなければならない。	不十分な保守による、情報およびその他の関連資産の消失、損傷、盗難または侵害、並びに組織の運用の中断を防止するため。	採	情報セキュリティ対策規程等に記載されているルールに従い保守している。	・情報セキュリティ対策規程 第17条 コンピュータ機器のセキュリティ (1)装置の設置および保護 ②予備機器・保守・保全	・保守契約書	旧「A.11.2.4」 大意として変更は無し		予防			機密性	完全性	可用性		防御					資産管理			物理的セキュリティ												保護		レジリエンス
7物理的管理策	14	装置のセキュリティを保った処分または再利用	記憶媒体を内蔵した装置は、処分または再利用する前に、全ての取扱いに慎重を要するデータおよびライセンス供与されたソフトウェアを消去していること、またはセキュリティを保てるよう上書きしていることを確実にするために、検証しなければならない。	処分または再利用する装置からの情報漏えいを防止するため。	採	情報セキュリティ対策規程等規程に記載されているルールに従い検証している。	・情報セキュリティ対策規程 第17条 コンピュータ機器のセキュリティ (4)機器管理・廃棄 第21条 媒体の取扱に関する管理 ・情報資産取扱規程 第14条 情報の廃棄		旧「A.11.2.7」		予防			機密性				防御					資産管理			物理的セキュリティ												保護		
8技術的管理策	1	利用者エンドポイント機器	利用者エンドポイント機器に保存されている情報、処理される情報、または利用者エンドポイント機器を介してアクセス可能な情報を保護しなければならない。	利用者エンドポイント機器を使用することによってもたらされるリスクから情報を保護するため。	採	情報セキュリティ対策規程等に記載されているルールに従い保護している。	・情報セキュリティ対策規程 第7条 情報の管理方針 第17条 コンピュータ機器のセキュリティ 第26条 無人運転装置に対するセキュリティ確保 ・情報資産取扱規程 ・クライアントPC管理規程 第2条 クライアントPCの管理 第6条 クライアントPCの持ち出しおよび、貸し出し ・アクセス制御管理規程	・情報取扱申請書兼報告書(厳秘／社外秘) ・厳秘情報利用許可申請書 ・PC持ち出し申請書 兼返却報告書	旧「A.6.2.1」「A.11.2.8」	統合	予防			機密性	完全性	可用性		防御					資産管理	情報保護														保護		
策8技術的管理	2	特権的アクセス権	特権的アクセス権の割当ておよび利用は、制限し、管理しなければならない。	認可された利用者、ソフトウェア構成要素およびサービスだけに特権的アクセス権が与えられることを確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い管理している。	・情報セキュリティ対策規程 第24条 情報利用者のアクセス管理 ・アクセス制御管理規程 第5条 特権管理 ・ネットワーク管理規程 第26条 特権ID		旧「A.9.2.3」 大意では変更はない		予防			機密性	完全性	可用性		防御												識別情報およびアクセスの管理								保護		
8技術的管理策	3	情報へのアクセス制限	情報およびその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の個別方針に従って、制限しなければならない。	情報およびその他の関連資産への認可されたアクセスだけを確実にし、認可されていないアクセスを防止するため。	採	情報セキュリティ対策規程等に記載されているルールに従い制限している。	・情報セキュリティ対策規程 第23条 アクセス制御に関する業務上の要求事項 ・アクセス制御管理規程 第3条 方針および業務上の要求事項 ・ネットワーク管理規程 第21条 資源へのアクセス権		旧「A.9.4.1」 大意としては変更なし		予防			機密性	完全性	可用性		防御												識別情報およびアクセスの管理								保護		
8技術的管理策	4	ソースコードへのアクセス	ソースコード、開発ツール、およびソフトウェアライブラリへの読取りおよび書込みアクセスを適切に管理しなければならない。	認可されていない機能が入り込むことを防止し、意図しないまたは悪意のある変更を回避し、価値の高い知的財産の機密性を維持するため。	採	情報セキュリティ対策規程等に記載されているルールに従い管理している。	・情報セキュリティ対策規程 第32条 情報システムの開発管理 (4)ソースライブラリへのアクセス制御 ・システム運用管理規程 第13条 セキュリティ要件 ・システム開発規程 第5章 ソースコード管理		旧「A.9.4.5」		予防			機密性	完全性	可用性		防御										アプリケーションセキュリティ	セキュリティを保った構成	識別情報およびアクセスの管理								保護		

8 技術的管理策	5	セキュリティを保った認証	セキュリティを保った認証技術および手順を、情報へのアクセス制限、およびアクセス制御に関するトピック固有の方針に基づいて備えなければならない。	システム、アプリケーションおよびサービスへのアクセスを許可するときに、利用者またはエンティティをセキュリティを保って認証することを確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い備えている。	・情報セキュリティ対策規程 第25条 パスワード使用における注意事項 第28条 システムへのアクセス制御 ・アクセス制御管理規程 第4条 システム利用者登録 ・クライアントPC管理規程 第2条 クライアントPCの管理		旧「A.9.4.2」		予防			機密性	完全性	可用性		防御												識別情報およびアクセスの管理								保護		
策 8 技術的管理	6	容量・能力の管理	現在および予測される容量・能力の要求事項に合わせて、資源の利用を監視し、調整しなければならない。	情報処理施設、人的資源、オフィスおよびその他の施設で必要とされる容量・能力の確保を確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い調整している。	・情報セキュリティ対策規程 第19条 情報処理設備管理 (6)システムの受け入れ ・システム運用管理規程 第10条 リソース管理		旧「A.12.1.3」		予防	検知			完全性	可用性	識別	防御	検知													継続					ガバナンスおよびエコシステム	保護		
8 技術的管理策	7	マルウェアに対する保護	マルウェアに対する保護を実施し、利用者の適切な認識によって支援しなければならない。	情報およびその他の関連資産をマルウェアに対して保護することを確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い実施および支援している。 (ウイルス対策ソフトの導入、ウイルス定義ファイルの最新化)	・情報セキュリティ対策規程 第19条 情報処理設備管理 (6)システムの受け入れ (7)コンピュータウイルス対策 (8)購入ソフトウェアの保守 ・システム運用管理規程 第17条 不具合およびセキュリティホール情報の収集 第18条 パッチの適用 ・情報セキュリティインシデント対策管理規程		旧「A.12.2.1」 大意では大きな変更はない		予防	検知	是正	機密性	完全性	可用性		防御	検知					情報保護			システムおよびネットワークのセキュリティ	アプリケーションセキュリティ	セキュリティを保った構成	識別情報およびアクセスの管理	脅威およびぜい弱性の管理	継続	供給者関係のセキュリティ	法令および順守	情報セキュリティ事象管理	情報セキュリティ保証	ガバナンスおよびエコシステム	保護	防御	レジリエンス
策 8 技術的管理	8	技術的ぜい弱性の管理	利用中の情報システムの技術的ぜい弱性に関する情報を獲得しなければならない。また、そのようなぜい弱性に組織がさらされている状況を評価し、適切な手段をとらなければならない。	技術的ぜい弱性の悪用を防止するため。	採	保守契約ベンダー等から情報を入手しており、保守ベンダーとは製品の保守契約以外に技術支援の契約もしている。 また、DMZセグメントについては、擬似アタックテストを専門ベンダーに依頼しており、発見された脆弱性については対策を講じている。	・システム運用管理規程 第17条 不具合およびセキュリティホール情報の収集 第18条 パッチの適用 ・情報セキュリティ対策規程 第19条 情報処理設備管理 (12)新技術への対応		旧「A.12.6.1」「A.18.2.3」	統合	予防			機密性	完全性	可用性	識別	防御													脅威およびぜい弱性の管理						ガバナンスおよびエコシステム	保護	防御	
策 8 技術的管理	9	構成管理	ハードウェア、ソフトウェア、サービスおよびネットワークのセキュリティ構成を含む構成を確立し、文書化し、実装し、監視し、レビューしなければならない。	ハードウェア、ソフトウェア、サービスおよびネットワークが、必要とされるセキュリティ設定で正しく機能し、認可されていない変更または誤った変更によって構成が変えられないことを確実にするため。	採	・役割、責任および手順を定める。 ・構成を文書化し、構成および変更の記録を取得する。 ・標準テンプレート等を利用し、適切な構成を可能とする。 ・構成の妥当性を検証し、定期的なレビューを行う。 上記により実施している。	・システム運用管理規程 第12条 新システムの導入 ・システム受入要領	運用設計書兼導入計画書	新規	新規	予防			機密性	完全性	可用性		防御											セキュリティを保った構成									保護		
8 技術的管理策	10	情報の削除	情報システム、装置またはその他の記憶媒体に保存している情報は、必要でなくなった時点で削除しなければならない。	取扱いに慎重を要する情報の不用意な漏えいを防止し、情報の削除に関する法令、規制および契約上の要求事項を順守するため。	採	・関連する法律および規制、契約上の要求事項を考慮した適切な削除手法の選択 ・削除結果を証拠として記録する。 ・情報削除を行うサービス提供者を利用する場合、認定された安全な廃棄サービス提供者を利用する。また、サービス提供者から情報削除の証拠を得る。 ・古い版や、複製および一時ファイル等も削除する。 ・特殊な復旧ツールを利用しても情報を復旧することができないようにセキュリティを保った削除ソフトウエアを利用する。 ・物理的媒体の場合には、処分する記憶媒体の種類に適した処分の仕組みを使用する。 上記により削除している。	・情報資産取扱規程 第14条 情報の廃棄 第21条 保存期間 第22条 廃棄時期および廃棄方法		新規	新規	予防			機密性				防御						情報保護										法令および順守				保護		
策 8 技術的管理	11	データマスキング	データマスキングは、適用される法令を考慮して、組織のアクセス制御に関するトピック固有の方針およびその他の関連するトピック固有の方針並びに事業上の要求事項に従って利用しなければならない。	PIIを含む、取扱いに慎重を要するデータの開示を制限し、法令、規制および契約上の要求事項を順守するため。	採	マスキング(仮名化または匿名化は未使用) ・処理するデータの使用法に応じたデータマスキングの強度のレベル ・処理するデータへのアクセス制御 ・処理するデータの使用法に関する合意または制限 ・処理するデータの提供および受領の追跡 上記により利用している。	・個人情報を含むテストデータ取扱管理要領 ・アクセス制御管理規程 第3条 方針および業務上の要求事項		新規	新規	予防			機密性				防御						情報保護														保護		
策 8 技術的管理	12	データ漏えい防止	データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存または送信するシステム、ネットワークおよびその他の装置に適用しなければならない。	個人またはシステムによる情報の認可されていない開示および抽出を検出し、防止するため。	採	・漏洩から保護すべき情報の特定 ・データが漏洩する可能性のある経路の監視 ・データ漏洩を防止するための処置 ・データ漏洩を起こす可能性のある要員への教育および訓練 上記を踏まえ適用している。	・情報セキュリティ対策規程 第13条 情報利用者への教育 第36条 情報セキュリティポリシーの評価および見直し ・情報セキュリティインシデント対策管理規程 第6条 インシデント予防	・LanScope Cat、m-FILTER関連資料／ログ	新規	新規	予防	検知		機密性				防御	検知					情報保護														保護	防御	
8 技術的管理策	13	情報のバックアップ	合意されたバックアップに関するトピック固有の方針に従って、情報、ソフトウェアおよびシステムのバックアップコピーは、維持し、定期的に検査しなければならない。	データまたはシステムの損失からの回復を可能にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い定期的に検査している。	・情報セキュリティ対策規程 第19条 情報処理設備管理 (9)情報のバックアップ (11)障害対策 ・システム運用管理規程 第7条 ファイル管理 第11条 障害管理		旧「A.12.3.1」				是正		完全性	可用性					復旧											継続						保護		
策 8 技術的管理	14	情報処理施設・設備の冗長性	情報処理施設・設備は、可用性の要求事項を満たすのに十分な冗長性をもって、導入しなければならない。	情報処理施設・設備の継続的な運用を確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い導入している。 統合ネットワークなど重要機器については冗長化構成としている。	・情報セキュリティ対策規程 第17条 コンピュータ機器のセキュリティ 第34条 緊急事態への対応 ・緊急時対応計画書		新規 旧「A.17.2.1」 記述内容としては変更なし	(新規)	予防					可用性		防御					資産管理									継続						保護		レジリエンス
8 技術的管理策	15	ログ取得	活動、例外処理、過失およびその他の関連する事象を記録したログを取得し、保存し、保護し、分析しなければならない。	事象を記録し、証拠を生成し、ログ情報の完全性を確実にし、認可されていないアクセスを防止し、情報セキュリティインシデントにつながる可能性のある情報セキュリティ事象を特定し、調査を支援するため。	採	情報セキュリティ対策規程等に記載されているルールに従い分析している。	・情報セキュリティ対策規程 第19条 情報処理設備管理 (10)運用の記録 第20条 ネットワークの管理 第24条 情報利用者のアクセス管理 第29条 システム使用状況の監視 ・システム運用管理規程 第6条 オペレーション管理 ・アクセス制御管理規程 第8条 アクセス状況の監視	・アクセスログほか各サーバログ ・LanScope Catログ ・m-FILTERログ ・PROXYログ ・障害報告書 ・是正処置結果報告表 ・JP1監視メッセージ ・統合NW監視メッセージ ・作業報告書 ・クローズ指示書(管理簿) ・本番作業実施伺 ・システム保守管理表	旧「A.12.4.1」「A.12.4.2」「A.12.4.3」	統合		検知		機密性	完全性	可用性			検知																情報セキュリティ事象管理			保護	防御	
8 技術的管理策	16	監視活動	情報セキュリティインシデントの可能性を評価するために、ネットワーク、システムおよびアプリケーションについて異常な挙動がないか監視し、適切な処置を講じなければならない。	異常な挙動および情報セキュリティインシデントの可能性を検出するため。	採	・アウトバウンド／インバウンドのトラフィックを監視する。 ・重要なシステムやデータへのアクセス ・セキュリティツールのログ ・イベントログ ・システムリソースの使用および動作状況 ・アラートを発生させるための適切なしきい値の設定 ・アラートによる関係者への伝達 ・アラートに対して適切な対応を実施するための要員の教育、訓練 上記を踏まえ適切な処置を講じている。	・情報セキュリティ対策規程 第19条 情報処理設備管理 (10)運用の記録 第20条 ネットワークの管理 第24条 情報利用者のアクセス管理 第29条 システム使用状況の監視 ・システム運用管理規程 第6条 オペレーション管理 ・アクセス制御管理規程 第8条 アクセス状況の監視 ・情報セキュリティインシデント対策管理規程 第3 条役割・責任(4)システム担当部門／運用担当部門②システムのアクセス権やログ等を監視する。	・アクセスログほか各サーバログ ・LanScope Catログ ・m-FILTERログ ・PROXYログ ・JP1監視メッセージ ・統合NW監視メッセージ	新規	新規		検知	是正	機密性	完全性	可用性			検知	対応															情報セキュリティ事象管理				防御	
策 8 技術的管理	17	クロックの同期	組織が使用する情報処理システムのクロックは、組織が採用した時刻源と同期させなければならない。	セキュリティ関連の事象およびその他の記録されたデータの関係付けおよび分析を可能にし、情報セキュリティインシデントの調査を支援するため。	採	情報セキュリティ対策規程等に記載されているルールに従い同期させている。	・情報セキュリティ対策規程 第29条 システム使用状況の監視		旧「A.12.4.4」			検知			完全性			防御	検知																情報セキュリティ事象管理			保護	防御	
8 技術的管理策	18	特権的なユーティリティプログラムの使用	システムおよびアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。	ユーティリティプログラムの使用が、システムおよびアプリケーションについての情報セキュリティ管理策に害を与えないことを確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い厳しく管理している。	・情報セキュリティ対策規程 第28条 システムへのアクセス制御 (2)システムユーティリティプログラムの使用 ・アクセス制御管理規程 第5条 特権管理		旧「A.9.4.4」 大意は影響なし		予防			機密性	完全性	可用性		防御									システムおよびネットワークのセキュリティ	アプリケーションセキュリティ	セキュリティを保った構成									保護		
8 技術的管理策	19	運用システムへのソフトウェアの導入	運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順および対策を実施しなければならない。	運用システムの完全性の維持を確実にし、技術的ぜい弱性の悪用を防止するため。	採	情報セキュリティ対策規程、ソフトウェア管理規程等に記載されているルールに従い実施している。	・情報セキュリティ対策規程 第32条 情報システムの開発管理 (2)運用ソフトウェアの管理 ・システム運用管理規程 ・システム開発規程 第5章 ソースコード管理 ・ソフトウェア管理規程 第2章 ソフトウェア管理	・システム導入等伺(導入計画書) ・本番作業実施伺	新規 旧「A.12.5.1」「A.12.6.2」	(新規)	予防			機密性	完全性	可用性		防御										アプリケーションセキュリティ	セキュリティを保った構成									保護		
8 技術的管理策	20	ネットワークセキュリティ	システムおよびアプリケーション内の情報を保護するために、ネットワークおよびネットワーク装置のセキュリティを保ち、管理し、制御しなければならない。	ネットワークおよびそれを支援する情報処理設備において、情報をネットワークを通じた侵害から保護するため。	採	情報セキュリティ対策規程等に記載されているルールに従い制御している。	・情報セキュリティ対策規程 第20条 ネットワークの管理 ・ネットワーク管理規程		旧「A.13.1.1」		予防	検知		機密性	完全性	可用性		防御	検知								システムおよびネットワークのセキュリティ											保護		
策 8 技術的管理	21	ネットワークサービスのセキュリティ	ネットワークサービスのセキュリティ機能、サービスレベルおよびサービス要求事項を特定し、実装し、監視しなければならない。	ネットワークサービスの利用におけるセキュリティを確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い監視している。	・情報セキュリティ対策規程 第27条 ネットワークのアクセス制御 (8)ネットワークサービス使用のセキュリティ ・ネットワーク管理規程		旧「A.13.1.2」		予防			機密性	完全性	可用性		防御									システムおよびネットワークのセキュリティ											保護		
策 8 技術的管理	22	ネットワークの分離	情報サービス、利用者および情報システムは、組織のネットワーク上で、グループごとに分離しなければならない。	業務のニーズに基づいて、ネットワークをセキュリティ境界で分割し、それらの間のトラフィックを管理するため。	採	情報セキュリティ対策規程等に記載されているルールに従い分離している。	・情報セキュリティ対策規程 第27条 ネットワークのアクセス制御 (6)ネットワーク領域分割 ・ネットワーク管理規程 第7条 領域分割		旧「A.13.1.3」		予防			機密性	完全性	可用性		防御									システムおよびネットワークのセキュリティ											保護		
策 8 技術的管理	23	ウェブ・フィルタリング	悪意のあるコンテンツにさらされることを減らすために、外部のウェブサイトへのアクセスを管理しなければならない。	システムがマルウェアによって危険にさらされることを防ぎ、認可されていないウェブ資源へのアクセスを防止するため。	採	・情報アップロード機能を持つウェブサイト ・既知のまたは疑わしい悪意のあるウェブサイト ・違法なコンテンツを供給しているウェブサイト ・業務上不適切なウェブサイトおよびウェブアプリケーション 上記へのアクセスを管理している。	・情報セキュリテイ対策規程 第20条 ネットワークの管理 ※OA系とインターネット系は物理分離	・N/W関連図他 ・ESET Endpoint関連資料	新規	新規	予防			機密性	完全性	可用性		防御									システムおよびネットワークのセキュリティ											保護		
8 技術的管理策	24	暗号の利用	暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施しなければならない。	事業上および情報セキュリティの要求事項に従い、暗号に関連する法令、規制および契約上の要求事項を考慮して、情報の機密性、真正性または完全性を保護するための暗号の適切かつ効果的な利用を確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い実施している。	・情報セキュリティ対策規程 第31条 暗号化の管理 ・電子メール利用規程 第7条 電子メール利用ルール		旧「A.10.1.1」「A.10.1.2」	統合	予防			機密性	完全性	可用性		防御											セキュリティを保った構成									保護		
管理策 8 技術的	25	セキュリティに配慮した開発のライフサイクル	ソフトウェアおよびシステムのセキュリティに配慮した開発のための規則を確立し、適用しなければならない。	情報セキュリティを、ソフトウェアおよびシステムのセキュリティに配慮した開発ライフサイクルにおいて設計し、実装することを確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い適用している。	・情報セキュリティ対策規程 第32条 情報システムの開発管理 ・システム開発規程		新規 旧「A.14.2.1」 大意としては変更は無し	(新規)	予防			機密性	完全性	可用性		防御									システムおよびネットワークのセキュリティ	アプリケーションセキュリティ										保護		

策 8 技術的管理	26	アプリケーションセキュリティの要求事項	アプリケーションを開発または取得する場合、情報セキュリティ要求事項を特定し、規定し、承認しなければならない。	アプリケーションを開発または取得する場合、全ての情報セキュリティ要求事項を特定し、対応することを確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い承認している。	・情報セキュリティ対策規程 第20条 ネットワークの管理 第27条 ネットワークのアクセス制御	・統合NW設計書	旧「A.14.1.2」「A.14.1.3」	統合	予防			機密性	完全性	可用性		防御									システムおよびネットワークのセキュリティ	アプリケーションセキュリティ										保護	防御	
8 技術的管理策	27	セキュリティに配慮したシステムアーキテクチャおよびシステム構築の原則	セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの開発活動に対して適用しなければならない。	情報システムを、開発のライフサイクルにおいてセキュリティに配慮して設計し、実装し、運用することを確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い適用している。	・情報セキュリティ対策規程 第32条 情報システムの開発管理 第33条 開発および支援プロセスにおけるセキュリティ ・システム開発規程 第5条 プロセス ・システム運用管理規程 第13条 セキュリティ要件		新規 旧「A.14.2.5」	（新規）	予防			機密性	完全性	可用性		防御									システムおよびネットワークのセキュリティ	アプリケーションセキュリティ										保護		
8 技術的管理策	28	セキュリティに配慮したコーディング	セキュリティに配慮したコーディングの原則をソフトウェア開発に適用しなければならない。	ソフトウェアをセキュリティに配慮して作成し、それによってソフトウェアの潜在的な情報セキュリティのぜい弱性の数を減らすことを確実にするため。	採	・IDEの利用 ・フレームワーク適用による重大なセキュリティ対策の自動化 ・パッケージマネージャによる外部パッケージの管理と定期的な更新 ・コーディング基準の遵守	・システム開発規程 第5条③セキュリティ要件の明確化 ・システム運用管理規程 第13条 セキュリティ要件 ・コーディング基準		新規	新規	予防			機密性	完全性	可用性		防御									システムおよびネットワークのセキュリティ	アプリケーションセキュリティ										保護		
8 技術的管理策	29	開発および受入におけるセキュリティテスト	セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施しなければならない。	アプリケーションまたはコードを本番環境に導入するときに、情報セキュリティ要求事項が満たされているかどうかの、妥当性確認をするため。	採	情報セキュリティ対策規程等に記載されているルールに従い実施している。	・情報セキュリティ対策規程 第19条 情報処理設備管理 （6）システムの受け入れ 第32条 情報システムの開発管理 ・システム開発規程 第5条 プロセス ・システム運用管理規程 第3章 システムの受入 第4章 システムの変更・保守		新規 旧「A.14.2.8」「A.14.2.9」	（新規）	予防			機密性	完全性	可用性	識別										システムおよびネットワークのセキュリティ	アプリケーションセキュリティ								情報セキュリティ保証		保護		
策 8 技術的管理	30	外部委託による開発	組織は、外部委託したシステム開発に関する活動を指揮し、監視し、レビューしなければならない。	組織が要求する情報セキュリティ対策が、外部委託したシステム開発で実施されることを確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従いレビューしている。	・情報セキュリティ対策規程 第15条 外部委託 第32条 情報システムの開発管理 ・システム開発規程 ・外部委託管理規程	・業務委託契約 ・機密保持契約	旧「A.14.2.7」		予防	検知		機密性	完全性	可用性	識別	防御	検知								システムおよびネットワークのセキュリティ	アプリケーションセキュリティ					供給者関係のセキュリティ				ガバナンスおよびエコシステム	保護		
8 技術的管理策	31	開発環境、テスト環境および本番環境の分離	開発環境、試験環境および本番環境は、分離してセキュリティを保たなければならない。	開発活動およびテスト活動による危険から本番環境およびそのデータを保護するため。	採	情報セキュリティ対策規程等に記載されているルールに従いセキュリティを保っている。	・情報セキュリティ対策規程 第19条 情報処理設備管理 （5）情報システムの開発環境の整備 第32条 情報システムの開発管理 第33条 開発および支援プロセスにおけるセキュリティ ・システム開発規程 第3章 テスト環境整備 第4章 システム試験データの保護		新規 旧「A.12.1.4」「A.14.2.6」	（新規）	予防			機密性	完全性	可用性		防御									システムおよびネットワークのセキュリティ	アプリケーションセキュリティ										保護		
8 技術的管理策	32	変更管理	情報処理施設と情報システムへの変更は、変更管理手順に従わなければならない。	変更を実行するときに情報セキュリティを維持するため。	採	情報セキュリティ対策規程等に記載されているルールに従い変更管理している。	・情報セキュリティ対策規程 第19条 情報処理設備管理 （2）運用変更管理 第33条 開発および支援プロセスにおけるセキュリティ ・システム運用管理規程 第4章 システムの変更・保守 ・システム開発規程 第5章 ソースコード管理	・システム導入等伺 （導入計画書） ・本番作業実施伺	旧「A.12.1.2」「A.14.2.2」「A.14.2.3」「A.14.2.4」	統合	予防			機密性	完全性	可用性		防御									システムおよびネットワークのセキュリティ	アプリケーションセキュリティ										保護		
8 技術的管理策	33	テスト用情報	テスト用情報は、適切に選定し、保護し、管理しなければならない。	テストの適切な実施、およびテストに使用する運用情報の保護を確実にするため。	採	情報セキュリティ対策規程等に記載されているルールに従い管理している。	・情報セキュリティ対策規程 第32条 情報システムの開発管理 （3）システム試験データの保護 ・システム開発規程 第4章 システム試験データの保護 ・個人情報を含むテストデータ取扱管理要領	・個人情報を含むテストデータ取扱申請・報告書	旧「A.14.3.1」		予防			機密性	完全性			防御						情報保護														保護		
策 8 技術的管理	34	監査におけるテスト中の情報システムの保護	運用システムのアセスメントを伴う監査におけるテストおよびその他の保証活動を計画し、テスト実施者と適切な管理者との間で合意しなければならない。	監査およびその他の保証活動が運用システムおよび業務プロセスに与える影響を最小限に抑えるため。	採	情報セキュリティ対策規程等に記載されているルールおよび契約等に基づき合意している。	・情報セキュリティ対策規程 第36条 情報セキュリティポリシーの評価および見直し ・内部監査規程	・内部監査年度計画書 ・内部監査実施計画書 ・電算データの授受に関する契約書 （みのり監査法人） ・システムにかかる内部統制評価への協力のお願	旧「A.12.7.1」 大意としては変更ない		予防			機密性	完全性	可用性		防御						情報保護			システムおよびネットワークのセキュリティ										ガバナンスおよびエコシステム	保護		