適用宣言書

文書番号	A-07	版数	1.2版
作成者/更新者	飯田晃紀	作成日/更新日	2024/7/1
承認者	西村孝徳	承認日	2024/7/1

○:適用、×:適用除外
○:実施、未:未実施、－:適用除外

表A.1－管理目的及び管理策			適用	27001:2022実施	27017:2015実施 クラウドカスタマ AWS	27017:2015実施 クラウドカスタマ Heroku	27701:2019実施 PII管理者	27701:2019実施 PII処理者	管理策を含めた理由 または 管理策を除外した理由	規定・手順書	相当するJISQ27001:2014附属書Aの要求事項
ISO/IEC 27001:2022 付属書A											
A.5. 組織的管理策											
A.5.1	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。	○	○	○	○	○	○	情報セキュリティのための経営層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 方針に、変化が生じた場合に適切性、妥当性、有効性を維持するため	A-02 情報セキュリティ方針 B-01 ISMSマニュアル5.2 C-01 情報セキュリティ手順書5.1	5.1.1情報セキュリティのための方針群 5.1.2情報セキュリティのための方針群のレビュー
A.5.2	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。	○	○	○	○	○	○	ISMSの構築・運用を円滑に行うため	B-01 ISMSマニュアル8.1 C-01 情報セキュリティ手順書5.2	6.1.1情報セキュリティの役割及び責任
A.5.3	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。	○	○	○	○	○	○	許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	C-01 情報セキュリティ手順書5.3	6.1.2職務の分離
A.5.4	経営陣の責任	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。	○	○	○	○	○	○	ISMSの取り組みが、経営陣の経営戦略の一部であることを確実にするため	B-01 ISMSマニュアル5 C-01 情報セキュリティ手順書5.4	7.2.1経営陣の責任
A.5.5	関係当局との連絡	組織は，関係当局との連絡体制を確立し，維持しなければならない。	○	○	○	○	○	○	情報セキュリティインシデントを時機を失せずに報告するため	A-08 連絡先一覧表 C-01 情報セキュリティ手順書5.5	6.1.3関係当局との連絡
A.5.6	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・団体との連絡体制を確立し，維持しなければならない。	○	○	○	○	○	○	社内からの通知だけではなく、関係するセキュリティ情報を最新に保つため	A-08 連絡先一覧表 C-01 情報セキュリティ手順書5.6	6.1.4専門組織との連絡
A.5.7	脅威インテリジェンス	情報セキュリティの脅威に関連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。	○	○	－	－	－	－	脅威環境を認識し、適切に対応できる体制を整えるため 27017/27701には追加実施の手引なし	C-01 情報セキュリティ手順書5.7	新規
A.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	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。	○	○	○	○	○	○	情報セキュリティリスクがプロジェクトの中で特定及び対処されることを確実にし、セキュリティの不具合又はセキュリティが確保されていない場合に起こると思われる業務上の損傷の可能性を低減するため	C-01 情報セキュリティ手順書5.8	6.1.5プロジェクトマネジメントにおける情報セキュリティ 14.1.1セキュリティに配慮した開発のための方針
A.5.9	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。	○	○	○	○	○	○	全ての資産を明確に認識し、管理責任者を明確にし、維持管理するため	D-02-01 資産目録 C-01 情報セキュリティ手順書5.9	8.1.1資産目録 8.1.2資産の管理責任
A.5.10	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。	○	○	○	○	○	○	資産利用の許容範囲を明確にし、認可されていない開示又は不正使用から保護するため	D-02-01 資産目録 C-01 情報セキュリティ手順書5.10	8.1.3資産利用の許容範囲 8.2.3資産の取扱い
A.5.11	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。	○	○	○	○	○	○	退職者が、不正に当社の資産を使用するのを防ぐため	C-01 情報セキュリティ手順書5.11	8.1.4資産の返却
A.5.12	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。	○	○	○	○	○	○	価値、取扱い等、重要性を明確にするため	C-01 情報セキュリティ手順書5.12	8.2.1情報の分類
A.5.13	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。	○	○	○	○	○	○	従業員に分類に対応した識別方法とその取扱い方法を明確にするため	C-01 情報セキュリティ手順書5.13	8.2.2情報のラベル付け
A.5.14	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。	○	○	○	○	○	○	あらゆる形式の通信設備を利用した情報転送を保護し、取引先や外部組織と自社のセキュリティーレベルの相違による情報交換のトラブルを防ぐため	C-01 情報セキュリティ手順書5.14	13.2.1情報転送の方針及び手順 13.2.2情報転送に関する合意 13.2.3電子的メッセージ通信
A.5.15	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。	○	○	○	○	○	○	情報資産への認可されていないアクセスを防止し、認可されたアクセスを確実にするため	C-01 情報セキュリティ手順書5.15	9.1.1アクセス制御方針 9.1.2ネットワーク及びネットワークサービスへのアクセス
A.5.16	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。	○	○	○	○	○	○	アクセス権の適切な割当て、変更、削除を可能にするため	C-01 情報セキュリティ手順書5.16	9.2.1利用者登録及び登録削除
A.5.17	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。	○	○	○	○	○	○	利用者の認可によって情報システム又はサービスへのアクセスを確実にするため	C-01 情報セキュリティ手順書5.17	9.2.4利用者秘密認証 9.3.1情報の管理秘密認証情報の利用 9.4.3パスワード管理システム
A.5.18	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。	○	○	○	○	○	○	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に対する有効な管理を維持するため	C-01 情報セキュリティ手順書5.18	9.2.2利用者アクセスの提供 9.2.5利用者アクセス権のレビュー 9.2.6アクセス権の削除又は修正
A.5.19	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。	○	○	○	○	○	○	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	C-01 情報セキュリティ手順書5.19	15.1.1供給者関係のための情報セキュリティの方針
A.5.20	供給者との合意における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。	○	○	○	○	○	○	関連する情報セキュリティ要求事項を満たすという義務に関し、供給業者との間に誤解が生じないことを確実にするため	C-01 情報セキュリティ手順書5.20	15.1.2供給者との合意におけるセキュリティの取扱い
A.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	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。	○	○	○	○	○	○	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	C-01 情報セキュリティ手順書5.21	15.1.3ICTサプライチェーン
A.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	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。	○	○	○	○	○	○	供給者が提供するサービスの合意における情報セキュリティの条件の順守を確実にするため	C-01 情報セキュリティ手順書5.22	15.2.1供給者のサービス提供の監視及びレビュー 15.2.2供給者のサービス提供の変更に対する管理
A.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	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。	○	○	－	－	－	－	クラウドサービスの利用における情報セキュリティの維持を確実にするため 27017/27701には追加実施の手引なし	C-01 情報セキュリティ手順書5.23	新規
A.5.24	情報セキュリティインシデント管理の計画及び準備	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。	○	○	○	○	○	○	情報セキュリティインシデントに対する迅速，効果的で整然とした対応を確実にするため	C-01 情報セキュリティ手順書5.24	16.1.1(情報セキュリティインシデントの管理及びその改善)責任及び手順
A.5.25	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。	○	○	○	○	○	○	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するため	C-01 情報セキュリティ手順書5.25	16.1.4情報セキュリティ事象の評価及び決定
A.5.26	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に対して、予め準備した手順通りの対応を確実にするため	C-01 情報セキュリティ手順書5.26	16.1.5情報セキュリティインシデントへの対応
A.5.27	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なければならない。	○	○	○	○	○	○	再発する又は影響の大きいインシデントを特定するため	C-01 情報セキュリティ手順書5.27	16.1.6情報セキュリティインシデントからの学習
A.5.28	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。	○	○	○	○	○	○	必要な証拠の特定、収集、取得及び保存のため。また、インシデントの重大さに気が付く前に、必要な証拠を破壊してしまわないため	C-01 情報セキュリティ手順書5.28	16.1.7証拠の収集
A.5.29	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・阻害時における，情報及び関連する資産を保護するため	C-01 情報セキュリティ手順書5.29	17.1.1情報セキュリティ継続の計画 17.1.2情報セキュリティ継続の実施 17.1.3情報セキュリティ継続の検証、レビュー及び評価
A.5.30	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。	○	○	－	－	－	－	事業の中断・阻害時における，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 27017/27701には追加実施の手引なし	C-01 情報セキュリティ手順書5.30	新規
A.5.31	法令，規制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。	○	○	○	○	○	○	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するため	C-01 情報セキュリティ手順書5.31	18.1.1適用法令及び契約上の要求事項の特定 18.1.5暗号化機能に対する規制
A.5.32	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。	○	○	○	○	○	○	著作権を侵害しないことを確実にするため	C-01 情報セキュリティ手順書5.32	18.1.2知的財産権
A.5.33	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。	○	○	○	○	○	○	記録及び情報を消失，破壊及び改ざんから保護するため	C-01 情報セキュリティ手順書5.33	18.1.3記録の保護
A.5.34	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，規制及び契約上の要求事項に従って，プライバシー及び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。	○	○	○	○	○	○	プライバシー及びPIIの保護の関係する法令、規制、契約事項の要求に従うため	C-01 情報セキュリティ手順書5.34	18.1.4プライバシー及び個人を特定できる情報の保護
A.5.35	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。	○	○	○	○	○	○	取組が引き続き適切、妥当及び有効であることを確実にするため	C-01 情報セキュリティ手順書5.35	18.2.1情報セキュリティの独立したレビュー
A.5.36	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いることを定期的にレビューしなければならない。	○	○	○	○	○	○	すべてのセキュリティ手順が正しく実行されることを確実にするため	C-01 情報セキュリティ手順書5.36	18.2.2情報セキュリティのための方針群及び標準の順守
A.5.37	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。	○	○	○	○	○	○	不注意又は故意によるシステムの不正使用のリスクを低減するため	C-01 情報セキュリティ手順書5.37	12.1.1操作手順書
A.6. 人的管理策											
A.6.1	選考	要員になる全ての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。	○	○	○	○	○	○	従業員候補者について可能な範囲においてセキュリティ上の危険性がないということを確認するため	C-01 情報セキュリティ手順書6.1	7.1.1選考
A.6.2	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。	○	○	○	○	○	○	雇用する従業員、契約相手との間で情報セキュリティに関する責任の内容を互いの了解を得るため	C-01 情報セキュリティ手順書6.2	7.1.2雇用条件
A.6.3	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。	○	○	○	○	○	○	方針群，セキュリティ要求事項，法的責任及び実務管理や手順の浸透を図るため	B-01 ISMSマニュアル5.1 B-01 ISMSマニュアル7.3 C-01 情報セキュリティ手順書6.3	7.2.2情報セキュリティの意識向上，教育及び訓練
A.6.4	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，懲戒手続を正式に定め，伝達しなければならない。	○	○	○	○	○	○	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	C-01 情報セキュリティ手順書6.4	7.2.3懲戒手続
A.6.5	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。	○	○	○	○	○	○	従業員の職務変更、退職時における雇用者・従業員の責任を明確にするため	C-01 情報セキュリティ手順書6.5	7.3.1雇用の終了又は変更に関する責任
A.6.6	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ニーズ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。	○	○	○	○	○	○	情報漏えいの抑止を法的に強制できるようにするため	C-01 情報セキュリティ手順書6.6	13.2.4秘密保持契約又は守秘義務契約
A.6.7	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。	○	○	○	○	○	○	組織の構外でアクセス，処理及び保存される情報を保護するため	C-01 情報セキュリティ手順書6.7	6.2.2テレワーキング
A.6.8	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も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。	○	○	○	○	○	○	情報セキュリティ事象の報告手順及びその連絡先を明確にするため	C-01 情報セキュリティ手順書6.8	16.1.2情報セキュリティ事象の報告 16.1.3情報セキュリティ弱点の報告
A.7 物理的管理策											
A.7.1	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。	○	○	○	○	○	○	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	A-04 レイアウト図 C-01 情報セキュリティ手順書7.1	11.1.1物理的セキュリティ境界
A.7.2	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。	○	○	○	○	○	○	セキュリティを保つべき領域について，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	A-04 レイアウト図 C-01 情報セキュリティ手順書7.2	11.1.2物理的入退管理策 11.1.6受渡場所
A.7.3	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。	○	○	○	○	○	○	壁や窓などの破壊により、建物内部への不正な侵入を防ぐため	A-04 レイアウト図 C-01 情報セキュリティ手順書7.3	11.1.3物理的入退管理策
A.7.4	物理的セキュリティの監視	施設は，認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、抑制するため 27017/27701には追加実施の手引なし	A-04 レイアウト図 C-01 情報セキュリティ手順書7.4	新規

表A.1－管理目的及び管理策			適用	27001:2022実施	27017:2015実施 クラウドカスタマ AWS	27017:2015実施 クラウドカスタマ Heroku	27701:2019実施 PII管理者	27701:2019実施 PII処理者	管理策を含めた理由 または 管理策を除外した理由	規定・手順書	相当するJISQ27001:2014附属書Aの要求事項
A.7.5	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。	○	○	○	○	○	○	自然災害又は人的災害からの損傷を回避するため	C-01 情報セキュリティ手順書7.5	11.1.4外部及び環境の脅威からの保護
A.7.6	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，実施しなければならない。	○	○	○	○	○	○	セキュリティを保つべき領域での監督されていない作業を回避するため	C-01 情報セキュリティ手順書7.6	11.1.5セキュリティを保つべき領域での作業
A.7.7	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め，適切に実施させなければならない。	○	○	○	○	○	○	取扱いに慎重を要する又は重要な業務情報を保護するため 27017には追加実施の手引なし	C-01 情報セキュリティ手順書7.7	11.2.9クリアデスク・クリアスクリーン方針
A.7.8	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。	○	○	○	○	○	○	物理的、環境的脅威から装置を保護するため	C-01 情報セキュリティ手順書7.8	11.2.1装置の設置及び保護
A.7.9	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。	○	○	○	○	○	○	構外にある装置の保護、セキュリティを確保するため	C-01 情報セキュリティ手順書7.9	11.2.6構外にある装置及び資産のセキュリティ
A.7.10	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。	○	○	○	○	○	○	媒体の不適切な取扱いによる情報の漏洩を防ぐため	C-01 情報セキュリティ手順書7.10	8.3.1取外し可能な媒体の管理 8.3.2媒体の処分 8.3.3物理的媒体の輸送 11.2.5資産の移動
A.7.11	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。	○	○	○	○	○	○	物理的、環境的脅威から装置を保護するため	C-01 情報セキュリティ手順書7.11	11.2.2サポートユーティリティ
A.7.12	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。	○	○	○	○	○	○	物理的、環境的脅威から装置を保護するため	C-01 情報セキュリティ手順書7.12	11.2.3ケーブル配線のセキュリティ
A.7.13	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。	○	○	○	○	○	○	装置の可用性・完全性を維持するため	C-01 情報セキュリティ手順書7.13	11.2.4装置の保守
A.7.14	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。	○	○	○	○	○	○	処分又は再利用する装置からの情報漏洩を防止するため	C-01 情報セキュリティ手順書7.14	11.2.7装置のセキュリティを保った処分又は再利用
A.8 技術的管理策											
A.8.1	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。	○	○	○	○	○	○	エンドポイント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	C-01 情報セキュリティ手順書8.1	6.2.1モバイル機器の方針 11.2.8無人状態にある利用者装置
A.8.2	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。	○	○	○	○	○	○	特権が割り当てられた利用者を制御するため	C-01 情報セキュリティ手順書8.2	9.2.3特権的アクセス権の管理
A.8.3	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方針に従って，制限しなければならない。	○	○	○	○	○	○	情報及びアプリケーションシステム機能のアクセス権を制御するため	C-01 情報セキュリティ手順書8.3	9.4.1情報へのアクセス制限
A.8.4	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。	○	○	○	○	○	○	ソースコードの意図しない変更を回避するため	C-01 情報セキュリティ手順書8.4	9.4.5プログラムソースコードへのアクセス制御
A.8.5	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。	○	○	○	○	○	○	認可されていないアクセスの危険性を最小限に抑えるため	C-01 情報セキュリティ手順書8.5	9.4.2セキュリティに配慮したログオン手順
A.8.6	容量・能力の管理	現在の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。	○	○	○	○	○	○	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	C-01 情報セキュリティ手順書8.6	12.1.3容量・能力の管理
A.8.7	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。	○	○	○	○	○	○	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	C-01 情報セキュリティ手順書8.7	12.2.1マルウェアに対する管理策
A.8.8	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。	○	○	○	○	○	○	技術的ぜい弱性に対する効果的な管理プロセスを確立するため	C-01 情報セキュリティ手順書8.8	12.6.1技術的ぜい弱性の管理 18.2.3情報セキュリティのための方針群及び標準の順守
A.8.9	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。	○	○	-	-	-	-	ハードウェア，ソフトウェア，サービス及びネットワークが、必要とされるセキュリティ設定で正しく機能し、不適切に構成が変更されていないことを確実にするため 27017/27701には追加実施の手引なし	C-01 情報セキュリティ手順書8.9	新規
A.8.10	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。	○	○	-	-	-	-	取扱いに慎重を要する情報の不必要な漏洩を防止し、情報の削 27017/27701には追加実施の手引なし	C-01 情報セキュリティ手順書8.10	新規
A.8.11	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。	○	○	-	-	-	-	個人を特定できる情報(PII)を含む取り扱いに慎重を要するデータの開示を制限し、法律、規制及び契約上の要求事項を順守するため 27017/27701には追加実施の手引なし	C-01 情報セキュリティ手順書8.11	新規
A.8.12	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。	○	○	-	-	-	-	個人やシステムによる情報の認可されていない開示及び抽出を検出し、防止するため 27017/27701には追加実施の手引なし	C-01 情報セキュリティ手順書8.12	新規
A.8.13	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を維持し，定期的に検査しなければならない。	○	○	○	○	○	○	重要な情報及び、ソフトウェア及びシステムイメージの回復を確実にするため	C-01 情報セキュリティ手順書8.13	12.3.1情報のバックアップ
A.8.14	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。	○	○	○	○	○	○	情報処理施設について、可用性の要求事項を満たすのに十分な冗長性をも	C-01 情報セキュリティ手順書8.14	17.2.1情報処理施設の可用性
A.8.15	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。	○	○	○	○	○	○	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，状況を把握するため	C-01 情報セキュリティ手順書8.15	12.4.1イベントログ取得 12.4.2ログ情報の保護 12.4.3実務管理者及び運用担当者の作業ログ
A.8.16	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。	○	○	-	-	-	-	異常な行動・動作及び潜在する情報セキュリティインシデントを検出するため 27017/27701には追加実施の手引なし	C-01 情報セキュリティ手順書8.16	新規
A.8.17	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。	○	○	○	○	○	○	イベントログの正確さを確実にするため	C-01 情報セキュリティ手順書8.17	12.4.4クロックの同期
A.8.18	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。	○	○	○	○	○	○	システムユーティリティの使用による情報セキュリティ管理策への害を防止するため	C-01 情報セキュリティ手順書8.18	9.4.4特権的なユーティリティプログラムの使用
A.8.19	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。	○	○	○	○	○	○	運用システムの完全性の維持を確実にするため	C-01 情報セキュリティ手順書8.19	12.5.1運用システムに関わるソフトウェアの導入 12.6.2ソフトウェアのインストールの制限
A.8.20	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。	○	○	○	○	○	○	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 27017には追加実施の手引なし	C-01 情報セキュリティ手順書8.20	13.1.1ネットワーク管理策
A.8.21	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の要求事項を特定し，実装し，監視しなければならない。	○	○	○	○	○	○	ネットワークサービス提供者が合意したサービスを，セキュリティを保って管理するため 27017には追加実施の手引なし	C-01 情報セキュリティ手順書8.21	13.1.2ネットワークサービスのセキュリティ
A.8.22	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。	○	○	○	○	○	○	ネットワーク内に保管又は処理される情報を保護するため	C-01 情報セキュリティ手順書8.22	13.1.3ネットワークの分離
A.8.23	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リソースへのアクセスを防止するため 27017/27701には追加実施の手引なし	C-01 情報セキュリティ手順書8.23	新規
A.8.24	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。	○	○	○	○	○	○	情報の機密性，真正性及び／又は完全性を保護するため	C-01 情報セキュリティ手順書8.24	10.1.1暗号による管理策の利用方針 10.1.2鍵(かぎ)管理
A.8.25	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。	○	○	○	○	○	○	セキュリティを考慮した開発のため	C-01 情報セキュリティ手順書8.25	14.2.1セキュリティに配慮した開発のための方針
A.8.26	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又は取得する場合，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。	○	○	○	○	○	○	公衆ネットワークを介してアクセス可能なアプリケーションについて、ネットワークに関連した脅威から情報を保護するため 27017には追加実施の手引なし	C-01 情報セキュリティ手順書8.26	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の考慮 14.1.3アプリケーションサービスのトランザクションの保護
A.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	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。	○	○	○	○	○	○	セキュリティに配慮したシステムを構築するため	C-01 情報セキュリティ手順書8.27	14.2.5セキュリティに配慮したシステム構築の原則
A.8.28	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。	○	○	-	-	-	-	ソフトウェアがセキュリティに配慮して記述され、それによりソフトウェアの潜在的な脆弱性の数を減らすため 27017/27701には追加実施の手引なし	C-01 情報セキュリティ手順書8.28	新規
A.8.29	開発及び受入れ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。	○	○	○	○	○	○	セキュリティ要求事項に適切に対処していることを検証するため	C-01 情報セキュリティ手順書8.29	14.2.8システムセキュリティの試験 14.2.9システムの受入れ試験
A.8.30	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。	○	○	○	○	○	○	実施される作業の質及び正確さを管理するため	C-01 情報セキュリティ手順書8.30	14.2.7外部委託による開発
A.8.31	開発環境，テスト環境及び本番環境の分離	開発環境，テスト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	○	○	○	○	○	○	開発・試験活動による影響から運用環境とデータを保護するため	C-01 情報セキュリティ手順書8.31	12.1.4開発環境，試験環境及び運用環境の分離 14.2.6セキュリティに配慮した開発環境
A.8.32	変更管理	情報処理設備及び情報システムの変更は，変更管理手順に従わなければならない。	○	○	○	○	○	○	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の管理を確実にするため	C-01 情報セキュリティ手順書8.32	12.1.2変更管理 14.2.2システムの変更管理手順 14.2.3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
A.8.33	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。	○	○	○	○	○	○	試験データの不正利用を管理するため	C-01 情報セキュリティ手順書8.33	14.3.1試験データの保護
A.8.34	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層との間で合意しなければならない。	○	○	○	○	○	○	業務プロセスの中断のリスクを最小限に抑えるため	C-01 情報セキュリティ手順書8.34	12.7.1情報システムの監査に対する管理策
ISO/IEC 27017 クラウドセキュリティに関連する管理策											
ISO/IEC 27017:2015 付属書A											
CLD.6.3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係 目的:情報セキュリティマネジメントに関してクラウドサービスカスタマとクラウドサービスプロバイダとの間で共有し分担する役割及び責任について、両社間の関係を明確にするため											
CLD.6.3.1	クラウドコンピューティング環境における役割及び責任の共有及び分担	クラウドサービスの利用に関して共有し分担する情報セキュリティの役割を遂行する責任は、クラウドサービスカスタマ及びクラウドサービスプロバイダのそれぞれにおいて特定の関係者に割り当て、文書化し、伝達し、実施することが望ましい。	○	-	○	○	-	-	クラウドサービスプロバイダとの責任分界点を明確にすることで、カスタマとしての義務と責任を明らかにするため	C-01 情報セキュリティ手順書9.1	N/A
A.8.1 資産に対する責任 目的:組織の資産を特定し，適切な保護の責任を定めるため。											
CLD8.1.5	クラウドサービスカスタマの資産の除去	クラウドサービスプロバイダの施設にあるクラウドサービスカスタマの資産は、クラウドサービスの合意の終了時に、時機を失せずに除去されるかまたは必要な場合には返却されることが望ましい。	○	-	○	○	-	-	クラウドサービスプロバイダの管理下にある、不要になった資産を確実に消去するため	C-01 情報セキュリティ手順書9.2	N/A
CLD 9.5 共有する仮想環境におけるクラウドサービスカスタマデータのアクセス制御 目的:クラウドコンピューティングにおける共有する仮想環境利用時の情報セキュリティリスクを低減するため											
CLD.9.5.1	仮想コンピューティング環境における分離	クラウドサービス上で稼働するクラウドサービスカスタマの仮想環境は、他のクラウドサービスカスタマ及び認可されていないものから保護することが望ましい。	X	-	-	-	-	-	クラウドサービスカスタマとしての実施の手引きなし	N/A	N/A
CLD.9.5.2	仮想マシンの要塞化	クラウドコンピューティング環境の仮想マシンは、事業場のニーズを満たすために要塞化することが望ましい。	○	-	○	○	-	-	クラウド上に配置する資産への不正アクセスを防御するため	C-01 情報セキュリティ手順書9.3	N/A
A.12.1 運用の手順及び責任 目的:情報処理設備の正確かつセキュリティを保った運用を確実にするため。											
CLD.12.1.5	実務管理者の運用のセキュリティ	クラウドコンピューティング環境の管理操作のための手順は、これを定義し、文書化し、監視することが望ましい。	○	-	○	○	-	-	不注意又は故意によるクラウドサービスの停止やデータの喪失といったリスクを低減するため	C-01 情報セキュリティ手順書9.4	N/A
A.12.4 ログ取得及び監視 目的:イベントを記録し，証拠を作成するため。											

表A.1－管理目的及び管理策			適用	27001:2022実施	27017:2015実施 クラウドカスタマ AWS	27017:2015実施 クラウドカスタマ Heroku	27701:2019実施 PII管理者	27701:2019実施 PII処理者	管理策を含めた理由 または 管理策を除外した理由	規定・手順書	相当するJISQ27001:2014附属書Aの要求事項
CLD.12.4.5	クラウドサービスの監視	クラウドサービスカスタマは、クラウドサービスカスタマが利用するクラウドサービスの操作の特定の側面を監視する能力を持つことが望ましい。	○	-	○	○	-	-	クラウドサービスの運用が適切であり、乗っ取りなどの不正な利用が行われていないことを確実にするため	C-01 情報セキュリティ手順書9.5	N/A
A.13.1 ネットワークセキュリティ管理 目的:ネットワークにおける情報の保護，及びネットワークを支える情報処理施設の保護を確実にするため。											
CLD13.1.4	仮想及び物理ネットワークのセキュリティ管理の整合	仮想ネットワークを設定する際には、クラウドサービスプロバイダのネットワークセキュリティ方針に基づいて、仮想ネットワークと物理ネットワークとの間の整合性を検証することが望ましい。	X	-	-	-	-	-	クラウドサービスカスタマとしての実施の手引きなし	N/A	N/A
ISO/IEC 27701 PIMSに関連する管理策											
ISO/IEC 27701:2019 付属書A PIMS固有の管理目的及び管理策(PII管理者)											
A.7.2 収集および処理の条件 目的:処理が，適用される各法域の法的根拠及び明確に定義された適法な目的をもち，適法であることを判断し，文書化するため。											
A.7.2.1	目的の特定及び文書化	組織は、PIIを処理する具体的な目的を特定し、文書化しなければならない。	○	-	-	-	○	-	PII管理者として、個人情報保護法に定める利用目的を明確にするため	C-01 情報セキュリティ手順書10.1.1	N/A
A.7.2.2	適法な根拠の特定	組織は、特定された目的のために、PIIの処理に関連する適法な根拠を判断し、文書化し、順守しなければならない。	○	-	-	-	○	-	個人情報保護法において定義されるPIIの範囲を明確にするため	C-01 情報セキュリティ手順書10.1.2	N/A
A.7.2.3	いつどのように同意を得るかの決定	組織は、PII主体からPII処理について同意が得られたかどうか、いつ、また、どのように得られたかを組織が実証できるプロセスを決定し、文書化しなければならない。	○	-	-	-	○	-	個人情報保護法においてPII主体の同意を得る対象と手段を明確にするため	C-01 情報セキュリティ手順書10.1.3	N/A
A.7.2.4	同意の取得及び記録	組織は、文書化したプロセスに従って PII 主体から同意を得て記録しなければならない。	○	-	-	-	○	-	同意を得るための要件を明確にするため	C-01 情報セキュリティ手順書10.1.4	N/A
A.7.2.5	プライバシー影響評価	組織は、新しいPII処理又は既存のPII処理の変更が計画されている場合は常に、プライバシー影響評価の必要性を評価し、適切な場合には、それを実施しなければならない。	○	-	-	-	○	-	PII処理の追加や変更を円滑に行うため	C-01 情報セキュリティ手順書10.1.5	N/A
A.7.2.6	PII処理者との契約	組織は、組織が利用するPII処理者と書面で契約しなければならず、PII処理者との自らの契約が附属書 B の適切な管理策の実施に確実に対処しなければならない。	○	-	-	-	○	-	適切なPII処理の委託を可能とするため	C-01 情報セキュリティ手順書10.1.6	N/A
A.7.2.7	共同PII管理者	組織は、共同PII管理者と共に、PIIの処理(PII保護及びセキュリティ要求事項を含む)に対する、それぞれの役割及び責任を決定しなければならない。	○	-	-	-	○	-	個人情報保護法に定める「共同利用」に対応するため	C-01 情報セキュリティ手順書10.1.7	N/A
A.7.2.8	PIIの処理に関連する記録	組織は、PIIの処理に関する自らの義務履行の助けとなる必要な記録を決定し、安全に維持しなければならない。	○	-	-	-	○	-	法令や契約などで必要となる記録を確実に実施するため	C-01 情報セキュリティ手順書10.1.8	N/A
A.7.3 PII主体に対する義務 目的:PII 主体に彼らのPII の処理に関する適切な情報が提供されることを確実にし，かつ，PII の処理に関連してその他の適用されるPII 主体に対する義務を果たすため。											
A.7.3.1	PII主体に対する義務の決定及び履行	組織は，PII 主体に対する彼らのPII の処理に関連した法律上，規制上及びビジネス上の組織の義務を決定及び文書化し，これらの義務を果たす手段を提供しなければならない。	○	-	-	-	○	-	個人情報保護法に定められたPII主体への義務に対応するため	C-01 情報セキュリティ手順書10.2.1	N/A
A.7.3.2	PII主体のための情報の決定	組織は、処理に関してPII主体に提供する情報及びそうした情報提供の タイミングに関して決定し、文書化しなければならない。	○	-	-	-	○	-	個人情報保護法に定められたPII主体に提供する情報を決定するため	C-01 情報セキュリティ手順書10.2.2	N/A
A.7.3.3	PII主体への情報提供	組織は，PII 管理者を特定する情報，及びPII の処理について説明する情報を，PII 主体に明確かつ容易にアクセス可能な方法で提供しなければならない。	○	-	-	-	○	-	個人情報保護法に定められたPII主体への情報提供に対応するため	C-01 情報セキュリティ手順書10.2.3	N/A
A.7.3.4	同意を変更又は撤回するための仕組みの提供	組織は、PII主体が同意を変更又は撤回するための仕組みを提供しなければならない。	○	-	-	-	○	-	個人情報保護法における「利用停止」に相当する項目として対応するため	C-01 情報セキュリティ手順書10.2.4	N/A
A.7.3.5	PIIの処理に対する異議申し立ての仕組みの提供	組織は、PII主体が自らのPIIの処理に対して異議を申し立てる仕組みを提供しなければならない。	○	-	-	-	○	-	個人情報保護法における「苦情の処理」に相当する項目として対応するため	C-01 情報セキュリティ手順書10.2.5	N/A
A.7.3.6	アクセス，訂正及び／又は消去	組織は，PII 主体が自らのPII にアクセスし，それを訂正及び／又は消去することに対する組織の義務を果たすための方針，手順及び／又は仕組みを実施しなければならない。	○	-	-	-	○	-	個人情報保護法において、PIIの訂正、追加、削除への対応が求められているため	C-01 情報セキュリティ手順書10.2.6	N/A
A.7.3.7	第三者に通知するPII管理者の義務	組織は、共有しているPIIに関する同意の変更、撤回又はPIIの処理に 対する異議について、PIIを共有している第三者に通知すると共に、適切な方針、手順及び/又はそれを行うための仕組みを実施しなければならない。	○	-	-	-	○	-	個人情報保護法に定める「共同利用」に対応するため	C-01 情報セキュリティ手順書10.2.7	N/A
A.7.3.8	処理されるPIIの複製の提供	組織は，PII 主体から要請された場合，処理されるPII の複製を提供可能としなければならない。	○	-	-	-	○	-	保有する個人情報の複製を提供する必要が発生した場合に対応するため	C-01 情報セキュリティ手順書10.2.8	N/A
A.7.3.9	要請の処理	組織は、PII主体からの正当な要請を取扱い、対応するための方針及び手順を定め文書化しなければならない。	○	-	-	-	○	-	個人情報保護法において定められた開示請求に対応するため	C-01 情報セキュリティ手順書10.2.9	N/A
A.7.3.10	自動化された意思決定	組織は，PII の自動化された処理だけに基づいてなされた組織の意思決定から生じる，PII 主体に対する法的義務を含む義務を特定し，対処しなければならない。	○	-	-	-	○	-	自動化された意思決定に係る規制がある法域からの個人情報取得に対応するため	C-01 情報セキュリティ手順書10.2.10	N/A
A.7.4 プライバシー・バイ・デザイン及びプライバシー・バイ・デフォルト 目的:プロセス及びシステムが，収集及び処理(使用，開示，保持，送信及び処分を含む。)が特定された目的に必要なものに限られるように設計されていることを確実にするため。											
A.7.4.1	収集制限	組組織は，PII の収集を，特定した目的との関連性，比例制，必要性において，最小限に制限しなければならない。	○	-	-	-	○	-	システムや業務プロセス検討時に、収集するPIIを最小限にする手法を選択するため	C-01 情報セキュリティ手順書10.3.1	N/A
A.7.4.2	処理制限	組織は、PIIの処理を、特定された目的に対して適切で、関連性があり、必要なものに制限しなければならない。	○	-	-	-	○	-	システムや業務プロセス検討時に、処理するPIIを最小限にする手法を選択するため	C-01 情報セキュリティ手順書10.3.2	N/A
A.7.4.3	正確性及び品質	組織は、PIIのライフサイクル全体を通じて、PIIの処理目的に必要とされる範囲で、正確、完全かつ最新であることを確実にし、文書化しなければならない。	○	-	-	-	○	-	対象のPIIが正確、完全であることを担保するため	C-01 情報セキュリティ手順書10.3.3	N/A
A.7.4.4	PII最小化目標	組織は、データ最小化目標、及びそれらの目標を達成するために使用する(非識別化などの)仕組みを定め文書化しなければならない。	○	-	-	-	○	-	非識別化などを利用して、管理対象PIIを最小化するため	C-01 情報セキュリティ手順書10.3.4	N/A
A.7.4.5	処理終了時のPIIの非識別化及び消去	組織は，元のPII がもはや特定した目的のために必要でなくなった場合は，速やかにPII を消去するか，又はPII 主体の識別若しくは再識別が可能でない形態にしなければならない。	○	-	-	-	○	-	不要になったPIIから情報漏洩が発生しないようにするため	C-01 情報セキュリティ手順書10.3.5	N/A
A.7.4.6	一時ファイル	組織は，PII の処理の結果で生成された一時ファイルを，文書化した規定の期間内に，文書化した手順に従って処分(例えば，消去又は破壊)することを確実にしなければならない。	○	-	-	-	○	-	一時ファイルから情報漏洩が発生しないようにするため	C-01 情報セキュリティ手順書10.3.6	N/A
A.7.4.7	保持	組織は、PIIを処理する目的のために必要とされる期間を超えて、PIIを 保持してはならない。	○	-	-	-	○	-	長期保管に起因する情報漏洩を防止するため	C-01 情報セキュリティ手順書10.3.7	N/A
A.7.4.8	処分	組織は、PIIの処分に関する文書化した方針、手順及び/又は仕組みをもたなければならない。	○	-	-	-	○	-	利用しなくなったPIIを確実に消去・識別不可とするため	C-01 情報セキュリティ手順書10.3.8	N/A
A.7.4.9	PIIの送信の管理策	組織は、データ送信ネットワーク上で送信される(例えば、別の組織に送られる)PIIに対して、データがその意図する宛先に到達することを確実 にするように設計した、適切な管理策に従わなければならない。	○	-	-	-	○	-	送信担当者を限定することで操作記録を保持し、正しい送信が行われたことを確認するため	C-01 情報セキュリティ手順書10.3.9	N/A
A.7.5 PIIの共有、移転及び開示 適用される義務に従って，PII を共有するかどうか，他の法域又は第三者に移転するかどうか，及び／又は開示するかどうかを決定し，もしするのであれば，それらはどういう場合かを文書化するため。											
A.7.5.1	法域間でのPII移転の根拠の特定	組織は、法域間でのPIIの移転に関連する根拠を特定し、文書化しなければならない。	○	-	-	-	○	-	JIS Q 15001:2023における「A.15 外国にある第三者への提供の制限」に対応するため	C-01 情報セキュリティ手順書10.4.1	N/A
A.7.5.2	PIIの移転が可能な国及び国際的な組織	組織は、PIIの移転が可能な国及び国際的な組織を規定し、文書化しなければならない。	○	-	-	-	○	-	JIS Q 15001:2023における「A.15 外国にある第三者への提供の制限」に対応するため	C-01 情報セキュリティ手順書10.4.2	N/A
A.7.5.3	PIIの移転の記録	組織は、PIIの第三者への移転又は第三者からの移転を記録し、PII主体に対する義務に関連する将来の要請に対応するために、それら関係者との協力を確実にしなければならない。	○	-	-	-	○	-	JIS Q 15001:2023における「A.15 外国にある第三者への提供の制限」に対応するため	C-01 情報セキュリティ手順書10.4.3	N/A
A.7.5.4	第三者へのPII開示の記録	組織は，どのPII を，誰に，いつ開示したかを含め，PII の第三者への開示を記録しなければならない。	○	-	-	-	○	-	JIS Q 15001:2023における「A.15 外国にある第三者への提供の制限」に対応するため	C-01 情報セキュリティ手順書10.4.4	N/A
ISO/IEC 27701:2019 付属書B PIMS固有の管理目的及び管理策(PII処理者)											
B.8.2 収集および処理の条件 目的:処理が適用される各法域の法的根拠に基づいて適法であり、明確に定義された適法な目的をもつことを判断し、文書化すること。											
B.8.2.1	取引先の合意	組織は，適切な場合には，PII を処理するための契約が，取引先の義務を支援する組織の役割を果たすことを確実にしなければならない(処理の性質及び組織が利用可能な情報を考慮に入れて)。	○	-	-	-	-	○	適切な取引先支援を実施するため	C-01 情報セキュリティ手順書11.1.1	N/A
B.8.2.2	組織の目的	組織は，取引先に代わって処理するPII を，取引先の文書化した指示に示されている目的のためだけに処理することを確実にしなければならない。	○	-	-	-	-	○	取引先から提供された情報を保護するため	C-01 情報セキュリティ手順書11.1.2	N/A
B.8.2.3	マーケティング及び広告のための使用	組織は，適切なPII 主体から事前の同意を確実に得ることなく，契約の下で処理されるPII をマーケティング及び広告の目的で使用してはならない。組織は，マーケティング及び広告目的のPII 使用に同意することを，PII 主体がサービスを受ける際の条件にしてはならない。	○	-	-	-	-	○	PII処理が適法であることを確実にするため	C-01 情報セキュリティ手順書11.1.3	N/A
B.8.2.4	侵害的指示	組織は，取引先の処理の指示が適用される法令を侵害するという見解がある場合，取引先に通知しなければならない。	○	-	-	-	-	○	取引先の不法行為を防止するため	C-01 情報セキュリティ手順書11.1.4	N/A
B.8.2.5	取引先の義務	組織は，取引先が自らの義務の順守を実証可能となるように，適切な情報を取引先に提供しなければならない。	○	-	-	-	-	○	取引先の義務に対応できるようにするため	C-01 情報セキュリティ手順書11.1.5	N/A
B.8.2.6	PIIの処理に関連する 記録	組織は，取引先に代わって実施するPII の処理に関する(適用される契約で規定されている)自らの義務の順守の実証に役立てるため，必要な記録を決定し，維持しなければならない。	○	-	-	-	-	○	契約を順守していることを確実にするため	C-01 情報セキュリティ手順書11.1.6	N/A
B.8.3 PII主体に対する義務 目的:PII 主体に彼らのPII の処理に関する適切な情報が提供されることを確実にし，かつ，PII の処理に関連してその他の適用されるPII 主体に対する義務を履行するため。											
B.8.3.1	PII主体に対する義務	組織は，PII 主体に対する義務を順守する手段を取引先に提供しなければならない。	○	-	-	-	-	○	取引先が持つ本人に対する義務に対応するため	C-01 情報セキュリティ手順書11.2.1	N/A
B.8.4 プライバシー・バイ・デザイン及びプライバシー・バイ・デフォルト 目的:プロセス及びシステムが，PII の収集及び処理(使用，開示，保持，送信及び処分を含む。)が特定された目的に必要なものに限られるように設計されることを確実にするため。											
B.8.4.1	一時ファイル	組織は，PII の処理の結果生成された一時ファイルを，文書化した規定の期間内に，文書化した手順に従って処分(例えば，消去又は破壊)することを確実にしなければならない。	○	-	-	-	-	○	一時ファイルから取引先情報の漏洩が発生しないようにするため	C-01 情報セキュリティ手順書11.3.1	N/A
B.8.4.2	PIIの返却、移転又は処分	組織は，安全なやり方でPII を返却，移転及び／又は処分する能力を提供しなければならない。また，組織の方針を取引先が確認可能であるようにしなければならない。	○	-	-	-	-	○	取引先情報の不必要な残留による事故を防止するため	C-01 情報セキュリティ手順書11.3.2	N/A
B.8.4.3	PIIの送信の管理策	組織は，データ送信ネットワーク上で送信するPII に対して，データがその意図する宛先に到達することを確実にするように設計した，適切な管理策に従わなければならない。	○	-	-	-	-	○	操作記録を保持し、正しい送信が行われたことを取引先に提示できるようにするため	C-01 情報セキュリティ手順書11.3.3	N/A
B.8.5 PIIの共有、移転及び開示 目的:PII が他の法域若しくは第三者に共有，移転，及び／又は適用される義務に基づいて開示されるかどうかを決定し，もしするのであれば，それはどのような場合かを文書化するため。											
B.8.5.1	法域間でのPII移転の根拠	組織は，法域間でのPII の移転の根拠及びこれに関する何らかの意図する変更を，取引先がそうした変更に異議を申し立てるか，又は契約を終了可能であるように，取引先にタイムリーに通知しなければならない。	○	-	-	-	-	○	取引先の要求に迅速に対応できるようにするため	C-01 情報セキュリティ手順書11.4.1	N/A

表A.1－管理目的及び管理策			適用	27001:2022実施	27017:2015実施 クラウドカスタマ AWS	27017:2015実施 クラウドカスタマ Heroku	27701:2019実施 PII管理者	27701:2019実施 PII処理者	管理策を含めた理由 または 管理策を除外した理由	規定･手順書	相当するJISQ27001:2014附属書Aの要求事項
B.8.5.2	PIIの移転が可能な国及び国際的な組織	組織は、PIIの移転が可能な国及び国際的な組織を規定し、文書化しなければならない。	○	-	-	-	-	○	情報の取り扱いが適法であることを示すため	C-01 情報セキュリティ手順書11.4.2	N/A
B.8.5.3	第三者へのPII開示の記録	組織は，どのPII を，誰に，いつ開示したかを含め，PII の第三者への開示を記録しなければならない。	○	-	-	-	-	○	情報の取り扱いが適法であることを示すため	C-01 情報セキュリティ手順書11.4.3	N/A
B.8.5.4	PII開示要請の通知	組織は，PII の開示に関する何らかの法的拘束力のある要請について，取引先に通知しなければならない。	○	-	-	-	-	○	取引先の要求に迅速に対応できるようにするため	C-01 情報セキュリティ手順書11.4.4	N/A
B.8.5.5	法的拘束力のあるPII開示	組織は，法的拘束力のないPII 開示の要請を拒否し，いかなる開示に対しても，PII を開示する前に該当する取引先に相談し，当該取引先によって承認されたPII 開示に関する契約で合意された要件を受け入れなければならない。	○	-	-	-	-	○	取引先情報を適切に取り扱うため	C-01 情報セキュリティ手順書11.4.5	N/A
B.8.5.6	PII の処理に使用する委託先などの開示	組組織は，PII を処理するために委託先などを使用することを，使用前に取引先に開示しなければならない。	○	-	-	-	-	○	適正な下請負者を選定するため	C-01 情報セキュリティ手順書11.4.6	N/A
B.8.5.7	PII を処理する委託先などの関与	組織は，取引先との契約に従ってPII を処理することに限定して，委託先などを従事させなければならない。	○	-	-	-	-	○	下請負者のPII情報保護を確実にするため	C-01 情報セキュリティ手順書11.4.7	N/A
B.8.5.8	PII を処理する委託先などの変更	組織は，書面による包括的な権限付与がなされている場合は，PII を処理する委託先などの追加又は交代に関して変更する意図があれば取引先に通知し，それによって，そうした変更に異議を申し立てる機会を取引先に与えなければならない。	○	-	-	-	-	○	適切な下請負社の変更を行うため	C-01 情報セキュリティ手順書11.4.8	N/A