適用宣言書

ISO27001:2022

A株式会社

適用欄（適用＝○、適用除外＝×、管理策を実施していない＝△）

ISO27001附属書A 管理目的及び管理策	適用欄	実施	管理策を含めた理由	関連文書
5 組織的管理策				
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個別方針は、これを定義し、経営陣によって承認され、発行し、関連する要員及び関連する利害関係者へ伝達し認識され、計画した間隔で及び重要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、規制及び契約上の要求事項に従って、経営陣の方向性の継続的な適合性、有効性、及び情報セキュリティのサポートを確実にするため。	情報セキュリティ管理規程
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の着実な運用には各人の役割を定義して意識してもらうことが必要となるため。	情報セキュリティ管理規程
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。	○	○	不適切な変更や誤用の可能性を少なくし、責任領域を分離する必要があるため。	情報セキュリティ管理規程
5.4 経営陣の責任				
経営陣は,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。	○	○	当社が定めたISMSに従うことを全ての関係者に要求し、ISMSを維持・管理していく際に、経営陣の率先随伴がモラルとして必要なため(今後、採用の際には管理	情報セキュリティ管理規程
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。	○	○	緊急時に関係機関と協力して速やかな処置がとれるように、これらの組織との連絡体制を明確にしておく必要があるため。	情報セキュリティ管理規程
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。	○	○	有効な情報セキュリティ対策を確立するために適宜専門家の知識と経験を活用する必要があるため。	情報セキュリティ管理規程
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。	-	-	セキュリティ脅威に対する教育を行っていないため	情報セキュリティ管理規程
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。	○	○	ルーチン業務以外でのプロジェクト業務においても、セキュリティに取組み、会社全体としてのセキュリティレベルの底上げを図るため。	情報セキュリティ管理規程
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。	○	○	組織の情報及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。	情報セキュリティ管理規程
5.10 情報及びその他の関連資産の利用の許容範囲				
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。	○	○	情報及びその他の関連資産が適切に保護、利用及び取扱いされることを確実にするため。	情報セキュリティ管理規程
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。	○	○	従業員などは、誓約書、雇用契約書などに従い、退職時、異動時、契約終了時には、自らが所持する当社の資産を確実に返却させるため。	情報セキュリティ管理規程
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。	○	○	情報資産の重要度に応じた適切な管理策を実施するために分類の指針を定める必要があるため。	情報セキュリティ管理規程
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。	○	○	情報資産をリスクに応じて分類し、区分に応じた取り扱いを行うため。	情報セキュリティ管理規程
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。	○	○	組織内及び外部の利害関係者との間で転送される情報セキュリティを維持するため。	情報セキュリティ管理規程
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。	○	○	情報及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。	情報セキュリティ管理規程
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。	○	○	認可されていないアクセスを防止するために、正規の利用者登録及び登録削除手順を明確にし、実施する必要があるため。	情報セキュリティ管理規程
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。	○	○	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。	情報セキュリティ管理規程

適用宣言書

ISO27001:2022

A株式会社

適用欄（適用＝○、適用除外＝×、管理策を実施していない＝△）

ISO27001附属書A 管理目的及び管理策	適用欄	実施	管理策を含めた理由	関連文書
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。	○	○	情報及びその他の関連資産へのアクセスが、業務上の要求事項に従って定義及び認可されることを確実にするため。	情報セキュリティ管理規程
5.19 供給者関係のための情報セキュリティ				
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。	情報セキュリティ管理規程
5.20　供給者との合意におけるセキュリティの取り扱い				
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。	○	○	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。	情報セキュリティ管理規程
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				
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。	○	○	供給者の情報セキュリティ上の責務を明確にし、一定の品質を担保するため。	情報セキュリティ管理規程
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の変更を定常的に監視し,レビューし,評価し,管理しなければならな	○	○	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及びサービスの提供を維持するため。	情報セキュリティ管理規程
5.23 クラウドサービス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	○	○	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及び管理するため。	情報セキュリティ管理規程
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				
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して、迅速、効果的、かつ、整然とした対処を確実に行うことが組織のダメージを低減することにつながるため。	情報セキュリティ管理規程
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	○	○	情報セキュリティ事象は、これを評価、分類して、後のISMSの改善に反映するため。	情報セキュリティ管理規程
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発生時には、混乱が無いように手続きを明示しておく必要があるため。	情報セキュリティ管理規程
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。	○	○	セキュリティ事故の再発防止のために、情報セキュリティインシデントから学習し、活用する仕組みを備える必要があるため。	情報セキュリティ管理規程
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。	○	○	懲戒や法的手続きのためには、客観的な証拠を残すことが必要となるため。	情報セキュリティ管理規程
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・阻害時に情報及びその他の関連資産を保護するため。	情報セキュリティ管理規程 事業継続計画マニュアル
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,実施,維持及び試験しなければならない。	○	○	事業の中断・阻害時に情報及びその他の関連資産の可用性を確実にするため。	情報セキュリティ管理規程 事業継続計画マニュアル
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。	○	○	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の順守を確実にするため。	情報セキュリティ管理規程 関連法規制一覧表
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。	○	○	法令や規制に関する文書化した情報がないため。	情報セキュリティ管理規程
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。	○	○	組織の重要な記録は、法令、規則、契約及び事業上の要求事項に従って、消失、破壊及び改ざんから保護する必要があるため。	情報セキュリティ管理規程
5.34プライバシー及び個人を特定できる情報(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,プライバシーの保護(preservation)及びPIIの保護(protection)に関する要求事項を特定し,満たさなければならない。	○	○	関連する法令、規則（個人情報保護マネジメントシステム)、契約条項の中の要求事項に従って個人情報を保護するため。	情報セキュリティ管理規程
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	○	○	利害関係の薄い第三者によるレビューを実施することで、情報セキュリティの漏れを無くし、高度化する必要があるため。	情報セキュリティ管理規程
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。	○	○	情報セキュリティが組織の情報セキュリティ方針、トピック固有の個別方針、規則及び標準に従って実施及び運用されるとこを確実にするため。	情報セキュリティ管理規程
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。	○	○	情報セキュリティの維持において、誤用による悪影響を防ぐため。	情報セキュリティ管理規程

適用宣言書

ISO27001:2022

A株式会社

適用欄（適用＝○、適用除外＝×、管理策を実施していない＝△）

ISO27001附属書A 管理目的及び管理策	適用欄	実施	管理策を含めた理由	関連文書
6　人的管理策				
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。	○	○	社員としての適性を採用時に判断することで、不正行為やセキュリティ上のリスクを軽減するため	情報セキュリティ管理規程
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。	○	○	従業者、契約相手、第三者の利用者に対して、社内の責務を文書化して自覚を促すため	情報セキュリティ管理規程 雇用契約書
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れ	○	○	情報セキュリティ確保には社員などの意識が重要であるので、組織に継続して浸透させていく必要があるため。	情報セキュリティ管理規程
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講じるために,懲戒手続を正式に定め,伝達しなければならない。	○	○	適用対象者による情報セキュリティ基本方針及び情報セキュリティ基本規程、情報セキュリティ実施手順をはじめとするISMS文書への違反は、罰則の対象であることを明示し、正式な懲戒手続きによって処罰される必要があるため。	就業規則 情報セキュリティ管理規程
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。	○	○	従業員などの退職や、異動の変更・停止・解除、及びこのような取り決めの変更・終了などに関する具体的な責任を明確にする必要があるため。	情報セキュリティ管理規程 機密保持誓約書
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。	○	○	内部組織として従業員の責務を明示し、秘密保持の誓約書に署名することで意識を促すため。	情報セキュリティ管理規程 機密保持誓約書
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。	○	○	外部で作業を実施する事があるため	情報セキュリティ管理規程
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。	○	○	要員が、特定可能な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。	情報セキュリティ管理規程
7 物理的管理策				
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。	○	○	セキュリティを確保するために当社領域の物理的境界を明確にし、且つ第三者の立ち入りを制限する領域の物理的境界を明確にする必要があるため。	情報セキュリティ管理規程
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【訳注:受付など】によって保護しなければならない。	○	○	組織の情報及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。	情報セキュリティ管理規程
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。	○	○	無許可の者が無断で立ち入ることができないようにするため。	情報セキュリティ管理規程
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、抑止するため。	情報セキュリティ管理規程
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。	○	○	セキュリティ領域を自然災害や人的災害から保護する必要があるため。	情報セキュリティ管理規程

適用宣言書

ISO27001:2022

A株式会社

適用欄（適用＝○、適用除外＝×、管理策を実施していない＝△）

ISO27001附属書A 管理目的及び管理策	適用欄	実施	管理策を含めた理由	関連文書
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。	○	○	管理区域でのセキュリティを担保するため、定められた者が認可された作業を行うことを確実にするため。	情報セキュリティ管理規程
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。	○	○	認可されていないアクセスを防止するために、クリアデスク及びクリアスクリーンを従業者各自の日常の行動として定める必要があるため。	情報セキュリティ管理規程
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。	○	○	環境上のリスク及び認可されていないアクセスから装置を保護するため。	情報セキュリティ管理規程
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。	○	○	構外作業中の不正アクセスや改ざん、破損から保護するため 。	情報セキュリティ管理規程
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。	○	○	記憶媒体上の情報に対して認可された開示、変更、移動又は廃棄だけがなされていることを確実にするため。	情報セキュリティ管理規程
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。	○	○	停電や電気的異常から装置を保護するため。	情報セキュリティ管理規程
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	○	○	電源ケーブル及ぶ通信ケーブルを損傷から保護する必要があるため。	情報セキュリティ管理規程
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。	○	○	継続性が求められる装置（機器）は、保守を実施し可用性、完全性を確保する必要があるため。	情報セキュリティ管理規程
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。	○	○	装置を廃棄又は再使用する場合の情報漏洩を防ぐため。	情報セキュリティ管理規程
8 技術的管理策				
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。	○	○	利用者終端装置を利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。	情報セキュリティ管理規程
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。	○	○	権限のない者による特権の使用により、不正アクセスや障害の発生が起こらないように管理する必要がある	情報セキュリティ管理規程
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	○	○	開示範囲の異なる情報に対して適切にアクセス権を制御するため。	情報セキュリティ管理規程
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。	×	×	開発に関する業務が無いため。	ー
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。	○	○	情報システムへの安全なアクセスを実現するために、重要度に応じた適切な手続きを定める必要があるため。	情報セキュリティ管理規程
8.6 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。	○	○	情報機器の障害を未然に防止し、安定稼動を可能にするため。	情報セキュリティ管理規程
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。	○	○	マルウェアからの脅威（破壊、漏えい）から情報資産を保護するため。	情報セキュリティ管理規程
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。	○	○	情報システム全般のリスクに対処して、そのリスクを低減するため。	情報セキュリティ管理規程

適用宣言書

ISO27001:2022

A株式会社

適用欄（適用＝○、適用除外＝×、管理策を実施していない＝△）

ISO27001附属書A 管理目的及び管理策	適用欄	実施	管理策を含めた理由	関連文書
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、認可されていない変更又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。	情報セキュリティ管理規程
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えいを防止し、情報の削除に関する法令、規制及び契約上の要求事項を遵守するため。	情報セキュリティ管理規程
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。	○	○	PIIを含む、取扱い慎重を要するデータの開示を制限し、法令、規制及び契約上の要求事項を順守するため。	情報セキュリティ管理規程
8.12 データ漏えいの防止				
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。	○	○	個人又は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。	情報セキュリティ管理規程
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。	○	○	重要な情報資産の破壊、焼失、紛失などのリスクに備えて、事業継続を図るため	情報セキュリティ管理規程
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。	○	○	情報処理施設は、可用性の要求事項を満たすことで、データの破壊や業務への影響を最小限に抑える必要があるため。	情報セキュリティ管理規程
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。	○	○	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。	情報セキュリティ管理規程
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。	情報セキュリティ管理規程
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。	○	○	正確な記録のため。	情報セキュリティ管理規程
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。	○	○	許可のない者がユーティリティを使用して不正行為を行わないようにするため。	情報セキュリティ管理規程
8.19 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、技術的ぜい弱性の悪用を防止するため。	情報セキュリティ管理規程
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。	○	○	設備間を移動する情報資産に対して、データの不正アクセスや改ざんから保護する必要があるため。	情報セキュリティ管理規程
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	○	○	取扱う情報資産が求めるセキュリティレベルに応じたネットワークサービスを利用するため。	情報セキュリティ管理規程
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。	○	○	適切なアクセス権を担保するために、関係者以外からのアクセスをネットワークレベルで分離することは効果が高いため。	情報セキュリティ管理規程
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ていることを防ぎ、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。	情報セキュリティ管理規程
8.24 暗号の使用				
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。	○	○	業務及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、規制及び契約上の要求事項を考慮して、情報の機密性、真正性又は完全性を保護するための暗号の適切かつ効果的な使用を確実にするため。	情報セキュリティ管理規程
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。	×	×	開発に関する業務が無いため。	ー

適用宣言書

ISO27001:2022

A株式会社

適用欄（適用＝○、適用除外＝×、管理策を実施していない＝△）

ISO27001附属書A 管理目的及び管理策	適用欄	実施	管理策を含めた理由	関連文書
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。	×	×	開発に関する業務が無いため。	ー
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開発活動に対して適用しなければならない。	×	×	開発に関する業務が無いため。	ー
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。	×	×	開発に関する業務が無いため。	ー
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。	×	×	開発に関する業務が無いため。	ー
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。	×	×	開発に関する業務が無いため。	ー
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。	×	×	開発に関する業務が無いため。	ー
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。	×	×	開発に関する業務が無いため。	ー
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	×	×	開発に関する業務が無いため。	ー
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。	×	×	開発に関する業務が無いため。	ー

版番号	発行 年月日	改定内容	作成者	承認者
1	○○○○/○/○	初版制定	佐藤	田中