内部監査チェックリスト–有効性（管理策）　（記入例）

帳票の目的

効果的で効率的な監査活動をサポートするために、内部監査時の確認事項を準備し、
要求事項が満たされているか、環境マネジメントシステムが有効に運用されているのかを確認します。

※注釈

本テンプレートでは「適合性」と「有効性」に内容を分けています。
「適合性」：ISO/IEC27001:2022+amd.1:2024の規格要求事項どおりにルールが策定されていることを確認
主に管理責任者や事務局などISOマニュアルなどを策定/改訂する部門を対象とする
「有効性」：ISO/IEC27001:2022+amd.1:2024の要求事項に対する運用に関する確認

実施日：yyyy/mm/dd
内部監査員：〇〇　■■
被監査部門：管理責任者、システム管理、●●部

STEP 1
監査の基本情報を記入します。
※ 当『内部監査チェックリスト』は、被監査部門ごとに確認する項目が異なることを想定し、被監査部門それぞれのチェックリストを作成することを前提としたつくりになっています。

STEP 2
監査で適合性/有効性を確認する ISO規格要求事項を記載します。
※ 当『内部監査チェックリスト』は、ISO/IEC27001:2022+amd.1:2024(JIS Q 27001:2025)用です。

STEP 3
規格要求事項について、被監査部門に対して確認する項目を記入します。
どのような情報が必要なのか、どのような質問をするのかを記入しましょう。

STEP 4
下記の監査評価基準に照らし、確認した結果を評価します。

STEP 5
評価のために確認した文書や記録、インタビューした対象者等を記入します。

STEP 6
備考がある場合は記入します。

STEP 7
部門ごとに、監査対象となる項目を設定します。

◎：重点監査項目
〇：監査対象項目
〇：適合　△：観察事項　×：不適合　－：対象外

表A.1－管理策			チェック事項	検証結果	確認結果　または　文書類(日付)	備考	管理責任者	システム管理	●●部
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方針群とトピック固有の方針は ①定義し管理層が承認しているか ②従業員は入手可能か ③利害関係者に通知・認知させているか ④定期的に見直しているか ⑤重大な変化が発生した場合に見直しているか	〇	・管理策規程(yyyy/mm/dd) ・ISMSマニュアル-5.2 (yyy/mm/dd)		◎		
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。	情報セキュリティの役割と責任を ①定めているか ②適切に割り当てているか	〇	・管理策規程(yyyy/mm/dd) ・ISMSマニュアル-5.3 (yyy/mm/dd)		◎		
5.3	職務の分離	相反する職務及び責任範囲は、分離しなければならない。	重要な業務については、1人で完結しない様にしているか ①実施と検証の担当を分けているか ②作成と承認は別の者か	×	・管理策規程(yyyy/mm/dd) ・経費精算書(yyyy/mm/dd) ●●部において、経費の申請者と承認者が同一であった。	管理策規程の要求事項を満たしていない。	〇	◎	◎
5.4	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。	管理層は、自社の従業者が守らなければならないセキュリティ要求事項を明確にし、通知しているか	△	・管理策規程(yyyy/mm/dd) ・ISMSマニュアル-5.1 (yyyy/mm/dd) ・管理責任者へのインタビュー 年1回管理層が通知をしていた。	今後、期中の人事異動が発生することも考慮して通知するタイミングに改善の余地がある。	◎		
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。	インシデントやシステム障害が発生した場合 ①連絡が必要な関係当局は明確か ②連絡手順は定められているか ③維持しているか				◎		
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。	情報セキュリティに関する ①情報取得先は明確か ②適切な連絡体制を維持しているか				◎		
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・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。	情報セキュリティの脅威に関する情報を ①収集・分析しているか ②脅威インテリジェンスを作成しているか				◎	◎	
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。	・各プロジェクトについて ①取組むセキュリティは明確か ②取組んでいるか ・新しいシステムを導入する際や、既存のシステムを改善する際、セキュリティ要求事項を明確にしているか				〇	◎	〇
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。	・資産目録について ①主要な情報資産を特定し、目録を作成しているか ②維持されているか ・各資産管理責任者は明確か					◎	◎
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。	・資産目録には、許容範囲が明確に記載されているか ・資産の取扱いに関する ①手順は情報分類体系に従い策定されているか ②手順は実施されているか				◎	◎	◎
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。	雇用・契約の変更または終了時に ①返却させなければならない情報資産は明確か ②返却をさせているか				◎		
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。	情報は ①機密性、完全性、可用性に基づいて分類されているか ②取扱いに慎重を要する度合いからの分類か				◎		◎
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。	情報のラベリングに関する ①手順は情報分類体系に従って策定されているか ②手順は実施されているか				◎		◎
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。	①通信設備を利用する情報転送の方針、手順は明確に規定されているか ②方針、手順は実施されているか 例） 極秘：メール不可 関係者外秘／社外秘：メール添付はパスワード ③外部組織との情報転送（運送業者を含む）に関して ・情報転送ルールを定めているか ・セキュリティを保った転送について、合意を取り交わしているか ④電子的メッセージ通信に含まれた情報は，適切に保護されているか 例） 添付メールのパスワード 通信の暗号化　等				◎	◎	◎
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 ①物理的及び論理的アクセス制御は策定し実施しているか ②アクセス制御方針は文書化されているか ③アクセス制御方針はレビューされているか ④利用者に提供するネットワークサービスは、認可したネットワークのみか				〇	◎	
5.16	アイデンティティ(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。	利用者の登録／削除、アイデンティティはライフサイクルを通して管理しているか ①正式なプロセスはあるか ②プロセスは実施されているか					◎	
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り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。	・秘密認証情報（ID／パスワード、生体認証等）の割当ては関係者に通知を含んだ管理プロセスにより管理されているか ①正式な管理のプロセスはあるか ②管理されているか ・秘密認証情報の利用のルールを ①利用者に周知しているか ②利用者は実行しているか ・パスワードについては ①パスワードの入力は対話式か ②パスワード入力時には＊＊＊表示等になるか ③ポリシー違反（必要桁数以下や間違い）の場合メッセージが表示されるか				〇	◎	◎
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。	・情報資産へのアクセス権はアクセス制御ルールに基づき ①提供と削除をしているか ②見直しと修正はしているか ・全てのシステム及びサービスについて利用者のアクセスの割当て／無効化に ①正式なプロセスはあるか ②プロセスは実施されているか ・資産の管理責任者は利用者のアクセス権を定期的に見直しているか ・雇用終了時に ①各システムへのアクセス権を削除しているか ②各入室の権利は抹消されているか				◎	◎	
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。	供給者から供給された製品やサービスに関して、セキュリティリスクを管理するためのプロセスまたは手順は ①定めているか ②実施しているか 情報セキュリティ要求事項について供給者と合意し，文書化しているか					◎	
5.20	供給者との合意における情報セキュリティの取扱い	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。	①関連する全ての情報セキュリティ要求事項を確立しているか ②供給者と要求事項について合意しているか					◎	〇
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要求事項を含めているか ICT製品やサービスに関して、セキュリティリスクを管理するためのプロセスまたは手順は ①定めているか ②実施しているか					〇	
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。	供給者の情報セキュリティの実践とサービス提供の変更を ①定常的／定期的監視しているか ②レビューしているか ③見直し、評価しているか ④供給者によるサービス提供の変更を管理しているか 例） 問題が発生しないことを確認 再契約　等				◎	◎	◎
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取得、利用、管理、終了のプロセスは情報セキュリティ要求事項に基づき策定しているか				◎	◎	◎
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する ①管理のプロセスは定義されているか ②管理層の役割・責任は明確か ③手順は明確か				◎		
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。	情報セキュリティ事象は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ているか				◎		
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の対応について ①文書化した手順があるか ②手順に従って対応しているか				〇	◎	◎
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。	①情報セキュリティインシデントは分析しているか ②分析及び解決から将来起こる可能性又はその影響を低減するために用いているか ③分析結果を組織内で学習しているか				◎		
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。	①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ているか ②手順は実施されているか				◎	◎	〇

表A.1－管理策			チェック事項	検証結果	確認結果　または　文書類(日付)	備考	管理責任者	システム管理	●●部
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。	①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ているか ②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、計画、手順及び管理策を確立し、文書化しているか ③定期的に、これらをの管理策が有効である事を検証しているか				○	◎	
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。	事業継続の目的とICT継続の要求事項に基づいてICTの備えを ①計画しているか ②実施しているか ③維持及びテストしているか				○	◎	
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。	①全ての関連する法令、規制及び契約上の要求事項は文書化されているか ②要求事項を満たすための組織の取組みをは文書化されているか ③文書は最新に保もたれているか ④暗号化に関する規制を順守しているか				◎	◎	◎
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	①知的財産権に関する要求事項の順守の手順を確立しているか ②ソフトウェアライセンスを管理する手順を確認しているか ③手順は実施されているか				◎	◎	◎
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	法令・規則・契約等で必要な記録は、消失、破壊、改ざん、不正アクセス、漏洩から保護、管理されているか				◎	◎	◎
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の保護は、関連する法令、規制及び契約上の要求事項に従って ①識別しているか ②遵守しているか				○	◎	◎
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。	①定期的にISMSの内部監査及び、マネジメントレビューが実施されているか ②重大な変化が生じた場合に、ISMSの内部監査及び、マネジメントレビューが実施されているか				◎		
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。	情報セキュリティ方針、セキュリティ手順について ①正しく実行されているか ②定期的に点検しているか ③技術的順守が実施されているかを点検しているか					◎	◎
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。	①重要な装置や業務に関する手順書は整備されているか ②必要な利用者に利用可能になっているか					◎	
6 人的管理策									
6.1	選考(スクリーニング)	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。	対象の従業者を雇用（選考）する場合 ①確認事項は明確か ②確認事項を実施しているか				◎		◎
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。	対象の従業者を雇用する場合 ①セキュリティ要求事項を明記した雇用契約書等を取り交わしているか				◎		◎
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。	情報セキュリティに関する教育は ①全てに従業員に実施しているか ②意識向上のための教育か ③教育は更新を行っているか				◎		
.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者に対する懲戒処分に関する事項が ①文書化されているか ②周知されているか				◎		◎
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。	雇用終了時に、情報セキュリティ要求事項を一定期間順守させるための、手段を講じているか 例）誓約書の取得				◎		◎
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。	委託先・取引先との契約書の内容は、セキュリティ要求事項が明確になった秘密保持契約を取り交わし署名させているか				◎	○	○
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。	テレワーキングについて ①セキュリティに関する方針は明確か ②セキュリティ対策は明確か ③対策は実施されているか ④認められていない所で実施していないか					◎	○
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は、報告されているか ・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 ①どのようなものでも記録し、報告することを要求しているか ②記録・報告されているか ・従業員に対して、情報セキュリティインシデント発生時に即座に対応できる手順は提供しているか				○	◎	◎
7 物理的管理策									
7.1	物理的セキュリティ境界	物理的セキュリティ境界	①物理的セキュリティ境界を定めているか ②物理的セキュリティ境界を周知しているか				◎		
.7.2	物理的入退	物理的入退	①物理的セキュリティの境界において、入退管理を実施しているか ②対象の従業者以外が立ち入る場所は明確か ③この場所には情報や情報処理施設は無いか ④この場所からの入室の制限はされているか				◎		
.7.3	オフィス、部屋及び施設のセキュリティ	オフィス、部屋及び施設のセキュリティ	施設内におけるセキュリティレベルが明確で、レベルに従った対策が実施されているか				◎		
.7.4	物理的セキュリティの監視	物理的なセキュリティ監視	物理的セキュリティを設けている重要区画について、継続的に監視する対策もしくは設備はあるか				◎		
.7.5	物理的及び環境の脅威からの保護	物理的及び環境的脅威からの保護	資産は自然災害、人的災害から守るべき手段が実施されているか 例） ・PCはどの様に保護しているか ・サーバはどの様に保護しているか ・その他重要な機器は何か、その保護はどうしているか				◎	○	
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	①セキュリティを保つべき領域は明確か ②作業手順は明確か ③作業手順は実施されているか				◎		
7.7	クリアデスク・クリアスクリーン	クリアデスク・クリアスクリーン	①離席時に机上に資産の放置をしない、PCをスリープ状態にする等のルールは定めているか ②使用後の資産は直ちに所定の場所へ格納しているか ③①、②を従業員に周知し確実に遂行させているか ④モニターへ、パスワード等を貼りつけていないか					◎	◎
7.8	装置の設置及び保護	装置の設置及び保護	装置は入退管理を実施している部屋に設置するか盗難防止の処置を施しているか					◎	
7.9	構外にある資産のセキュリティ	構外にある資産のセキュリティ	構外にある装置（例：PC、携帯電話、サーバ等）について セキュリティ対策は実施されているか					○	
7.10	記憶媒体(Storagemedia)	記憶媒体	取り外し可能な記憶媒体の ①分類体系の規定はあるか ②取扱いの要求事項を定めた規定はあるか ③それらの規定に従って、取得、使用、移動及び廃棄のライフサイクルは実施、管理されているか ・分類体系に従って ①取外し可能な媒体の管理手順はあるか ②手順は実施されているか ・媒体が不要になった場合の ①正式な手順はあるか ②手順を用いて処分しているか ③セキュリティを保って処分しているか ・輸送中の媒体は保護されているか ・装置、情報又はソフトウェアの持出しは、事前の認可を得ているか ・持ち運びの規定はあるか				○	◎	◎
7.11	サポートユーティリティ	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から保護されているか 例） ・UPSの設置 ・電源容量の確認 ・適切な空調					◎	
7.12	ケーブル配線のセキュリティ	ケーブル配線のセキュリティ	ケーブル等は保護されているか 例） ・切断・外れが無いように対策を実施 ・電源ケーブルと信号ケーブルが並行ではない ・ケーブルのラベリング					◎	
7.13	装置の保守	装置の保守	・装置は機密性、完全性、可用性の維持を目的に正しく保守されているか 例） ・重要な装置は保守契約を締結 ・メーカー推奨通りに保守を行う ・力量のある者が保守を行う					◎	
7.14	装置のセキュリティを保った処分又は再利用	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、入出力媒体等に蓄積されたデータは処分や再利用の前に ・媒体の破壊 ・専用ソフトウェアによる消去 ・消磁気装置による磁気的消去 等の方法により完全消去しているか					◎	
8 技術的管理策									
8.1	利用者エンドポイント機器（ユーザーエンドポイントデバイス）	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。	・エンドポイントに保存されている情報は保護されているか ・各モバイル機器について ①セキュリティに関する方針は明確か ②セキュリティ対策は明確か ③対策は実施されているか ・複合機等管理者が不明確な装置に関するルールが設定され、実施されているか ・スクリーンセーバは定められた手順に従い、動作するようにセッティングされているか					◎	◎
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。	特権的アクセス権の割当て及び利用は ①制限されているか ②管理されているか					◎	

表A.1－管理策			チェック事項	検証結果	確認結果　または　文書類(日付)	備考	管理責任者	システム管理	●●部
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へのアクセスは、制限されているか 例） 権限外のアクセスが行なわた場合にワーニングメッセージ					○	
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。	①プログラムソースコードへのアクセスは制限されているか ②ソースコードへの書き込み、読み込み、開発ツールやソフトウェアライブラリへのアクセスは制御されているか ③運用環境は実行可能なコードのみか					○	
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。	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か 例） ID／パスワードを設定					○	
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	①資源（ディスク容量、ネットワーク性能等）の利用を監視・調整しているか ②将来必要とする容量・能力を予測しているか					◎	
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	マルウェアから保護するために ①利用者に適切に認識させているか ②検出、予防及び回復のための管理策がなされているか 例） ・マルウェア対策ソフトの導入／パターンの更新／フルスキャン ・ブラウザの設定 ・不正メールの対応　等					◎	◎
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。	・定期的なセキュリティパッチ等を確実に実施しているか ・技術的順守が実施されているかの点検をしているか					◎	◎
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、ネットワークのセキュリティ設定は ①確立されているか ②文書化しているか ③実施しているか ④監視し評価しているか					◎	
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。	不必要になった情報は即座に削除しているか					◎	
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。	データマスキングは適用される法律を考慮して ①アクセス制御に関する組織の規定、トピック固有の個別方針、関連手順は定められているか ②それらはビジネス要求事項に従って運用されているか				○	◎	○
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。	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、デバイスに対してデータ漏洩防止対策をしているか					◎	
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。	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について ①方針は明確か ②定期的に取得しているか ③検査しているか					◎	○
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のに十分な冗長性をもって導入されているか				○	◎	
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たイベントログを ①取得しているか ②適切に保持しているか ③定期的にレビュー、分析しているか 例） アクセスログ、障害ログ、入退出ログ　等 ・ログ機能及びログ情報は保護されているか 例） 限定されたアクセス ログのバックアップ　等 ・システムの実務管理者及び運用担当者の作業は ①記録しているか ②そのログを保護しているか ③定期的にレビューしているか					◎	
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。	ネットワーク、システム、アプリケーションの異常な挙動を ①監視しているか ②分析し評価しているか ③適切な処置を講じているか					◎	
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。	ログを取得しているシステムの時間は ①正しいか ②修正は行っているか					◎	
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。	ユーティリティプログラムの使用は制限し、厳しく管理されているか					○	○
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。	・運用システムに関わるソフトウェアの導入を、セキュリティを保った状態で管理するための ①対策はあるか ②手順はあるか ③手順を実施しているか ・利用者によるソフトウェアのインストールについて ①管理する規則を確立しているか ②規則は実施されているか					◎	◎
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。	ネットワークとネットワークデバイスは適切な管理策が実施されているか 例） ・無線LANは十分な安全対策をとられているか （ファームウェアアップデート、適切な暗号化方式を使用している無線LANの利用） ・MACアドレス等で機器を識別 ・ファイアーウォールの設置、設定 ・決められた機器のみ社内LANに接続できる ・業務以外でメールを利用していないか　等					◎	
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について特定・実施し、監視しているか ①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ているか ②ネットワークサービス合意書にもこれらが盛り込まれているか					◎	
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。	ネットワークは分離されているか 例） ・外部／内部の分離 ・セグメント別　等					◎	
8.23	ウェブフィルタリング	悪意のあるコンテンツへ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。	組織のポリシーから逸脱したウェブサイトへのアクセスを制限しているか					◎	
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。	・暗号による管理策の利用に関する方針は ①策定されているか ②実施されているか ・暗号鍵の利用、保護及び有効期限（lifetime）に関する方針を ①策定しているか ②ライフサイクル全体にわたって実施しているか					○	
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。	①開発のための規則は確立しているか ②規則は適用されているか					◎	○
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。	①アプリケーションの開発・取得時には情報セキュリティ要求事項を特定し対処しているか ②インターネットを利用したアプリケーションサービスは保護されているか ③ホームページ等、一般に公開している情報がある場合、改ざん等からの保護対策を実施しているか ④アプリケーションサービスのトランザクションは保護されているか					◎	
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。	システムの構築に関して ①セキュリティに関する原則を文書化しているか ②全ての情報システムの実装に対して適用しているか					◎	○
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。	ソフトウェア開発時は、セキュリティを考慮した設計（コーディング）をしているか					◎	○
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。	セキュリティ機能の試験は、開発期間中に実施しているか ①受入れ試験のプログラム及び関連する基準は確立しているか ②実施されているか					◎	○
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。	外部にシステム開発を委託した場合、監督／管理しているか					◎	○
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。	・開発環境、試験環境、運用環境は分離しているか ・セキュリティに配慮した開発環境を確立しているか					◎	○
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は、管理しているか 例） 認可の上、変更を行っている 変更の記録、履歴を残す ・システムの変更は ①正式な変更管理手続があるか ②手続きに基づき管理されているか ・OS等の変更では、 ①重要なアプリケーションへの影響をレビューしているか ②試験を行っているか ・パッケージソフトウェアの変更は ①抑止されているか ②必要な変更だけに限られているか ③厳重に管理されているか					◎	○
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。	試験データは ①注意深く選定しているか 例）重要な個人情報が含まれていないか ②保護されているか					○	◎
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。	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（メンテナンスも含む） ①業務プロセスの中断を最小限に抑える計画をしているか ②計画は利用者／部門と合意しているか					○	

前回内部監査									

表A.1－管理策			チェック事項	検証結果	確認結果　または　文書類(日付)	備考	管理責任者	システム管理	●●部
部監査不適合及び観察事項の処置状況									

内部監査チェックリスト−有効性(箇条4.−10.)

実施日:＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
内部監査員:＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
被監査部門:＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

凡例: ○:適合 △:観察事項 ×:不適合 −:対象外

◎:重点監査項目
○:監査対象項目

監査項目	チェック事項	検証結果	確認結果 または 文書類(日付)	備考	管理責任者	システム管理	●●部
4. 組織の状況							
4. 1 組織及びその状況の理解	ISMSに関する外部課題および内部課題を決定/見直しましたか。						
4. 2 利害関係者のニーズ及び期待の理解	ISMSに関する利害関係者は、明確になっていますか。 また、その利害関係者の要求事項は、決定/見直しましたか。						
4. 3 情報セキュリティマネジメントシステムの適用範囲の決定	ISMSの適用範囲を明確化していますか。						
	ISMSの適用範囲は、従業者に周知していますか。						
	ISMSの適用範囲は、現状と合った範囲になっていますか。						
4. 4 情報セキュリティマネジメントシステム	ISMSを確立し、実施し、維持し、継続的改善を行っていますか。						
5. リーダーシップ							
5. 1 リーダーシップ及びコミットメント	情報セキュリティ基本方針は、トップマネジメントによる承認を得ましたか。						
	ISMSは、業務と整合性していますか。						
	トップマネジメントは、ISMSの推進を指示していますか。						
	トップマネジメントは、ISMSの重要性を伝えていますか。						
	ISMSは、セキュリティ目的と事業は整合性がありますか。						
	トップマネジメントは、ISMSの推進を支援していますか。						
	トップマネジメントは、ISMSの改善を支援していますか。						
	トップマネジメントは、ISMSの運営について、管理者を支援していますか。						
5. 2 方針	情報セキュリティ方針は、以下を考慮しているか。 ・事業、業務 ・セキュリティ目的 ・要求事項(規格要求事項、顧客要求事項、法令等) ・継続的な改善						
	情報セキュリティ方針は、作成されていますか。						
	情報セキュリティ方針は、従業者に周知していますか。						
	情報セキュリティ方針は、外部の関係者が入手できますか。						
5. 3 組織の役割、責任及び権限	ISMSの推進体制は、トップマネジメントによる承認を得ましたか。						
	ISMSの推進体制図は、作成されていますか。						
6. 計画							
6. 1 リスク及び機会に対処する活動							
6. 1. 1 一般	「外部及び内部の課題」の検討では、リスク及び機会も検討しましたか。						
	ISMSを確実に推進する方法を検討しましたか。						
	ISMSの計画には、ISMSの有効性の確認も含まれていますか。						

凡例： ○：適合　△：観察事項　×：不適合　－：対象外　　○：監査対象項目

監査項目	チェック事項	検証結果	確認結果　または　文書類(日付)	備考	管理責任者	システム管理	●●部
6．1．2　情報セキュリティリスクアセスメント	リスク受容基準を提示してください。						
	リスクアセスメントを実施する時期と実施する際の評価方法（情報セキュリティリスクアセスメントを実施するための基準）を提示してください。						
	リスクアセスメントの結果は、数値化されていますか。						
	リスクアセスメントは、情報の機密性、完全性及び可用性の喪失を考慮していますか。						
	リスク所有者は、明確になっていますか。						
	リスクアセスメントは、以下を考慮していますか。 ・リスクが顕在化した場合の結果 ・リスクの発生頻度（起こりやすさ）						
	リスクアセスメントでは、数値化した結果とリスク受容基準を比較していますか。						
	リスクアセスメントの手順を提示してください。						
6．1．3　情報セキュリティリスク対応	リスクアセスメントの結果は、リスクに対する対応（保有、低減、移転、回避等）が含まれていますか。						
	リスクアセスメントの結果は、リスクに対応する対策が含まれていますか。						
	リスクに対する対策の漏れはありませんか。						
	「適用宣言書」は作成/更新しましたか。						
	リスク対応計画は作成しましたか。						
	リスク対応計画は、リスク所有者の承認を得ていますか。						
	リスク対応の手順を提示してください。						
6．2　情報セキュリティ目的及びそれを達成するための計画策定	情報セキィリティに関する目標を設定しましたか。						
	設定した目標は、情報セキュリティ方針と矛盾はありませんか。						
	設定した目標は、達成状況を確認できる内容ですか。						
	設定した目標は、リスクアセスメントの結果を考慮していますか。						
	設定した目標は、達成度合の進捗状況を確認していますか。						
	設定した目標は、従業者に周知していますか。						
	情報セキィリティに関する目標の見直しを行いましたか。						
	情報セキィリティに関する目標を提示してください。						
	設定した目標を達成するための計画は作成しましたか。						
6．3 変更の計画	ISMSの変更を、計画的に行いましたか。						
7．支援							
7．1 資源	ISMSの推進に必要な資源は明確になっていますか。						
7．2 力量	ISMSの推進に必要な要員の力量は明確になっていますか。						
	ISMSの推進に必要な要員は、教育等で力量を獲得していますか。						
	ISMSの推進に必要な要員が、力量を備えている事を確認していますか。						
	力量の確認結果を提示してください。						
7．3 認識	ISMS教育は実施していますか。また、ISMS教育では、以下を考慮していますか。 a) 情報セキュリティ方針 b) 情報セキュリティパフォーマンスの向上によって得られる便益を含む、ISMSの有効性に対する自らの貢献 c) ISMS要求事項に適合しないことの意味						
7．4　コミュニケーション	ISMSに関する内部・外部の関係者との連絡内容・方法は明確になっていますか。						

凡例：　○:適合　△:観察事項　×:不適合　−:対象外　　○:監査対象項目

監査項目	チェック事項	検証結果	確認結果　または　文書類(日付)	備考	管理責任者	システム管理	●●部
7．5　文書化した情報							
7．5．1　一般	ISMSの運用に必要な文書は明確になっていますか。						
7．5．2　作成及び更新	各文書には、”タイトル””日付””作成””文書番号”が記載されていますか。						
	各文書の作成・修正では、判り易い表現を考慮していますか。						
	各文書の作成・修正では、レビュー及び承認を行っていますか。						
7．5．3　文書化した情報の管理	各文書は、必要な者が参照できる様になっていますか。						
	各文書は、紛失、情報漏えい、改竄などから保護されていますか。						
	各文書は、必要な者以外に閲覧や配布をしていませんか。						
	各文書は、決められた場所に保管していますか。						
	各文書は、変更管理(版管理、承認等)は行っていますか。						
	不要になった文書は、廃棄または、旧文書である事が判る様に管理していますか。						
	外部文書（他の組織が作成したISMSの運用に必要な文書）は明確になっていますか。						
8．　運用							
8．1 運用の計画策定及び管理	ISMSの運用は行われていますか。						
	情報セキュリティについて、設定した目標を達成するための計画は実行していますか。						
	「マネジメント年次計画書」等で計画している文書（記録）は見直し・作成しましたか。						
	不適合や文書の誤りは是正していますか。						
	委託先を管理していますか。						
8．2 情報セキュリティリスクアセスメント	定期的(年に1回)にリスクアセスメントの結果を見直していますか。						
	ISMSに大きな影響のある変化があった場合は、リスクアセスメントの結果を見直していますか。 【ISMSに影響を及ぼす重大な変化の例】 1）事業の追加／削除／変更、業務手順の大きな変更、住所変更 2）ISMSの主たる担当を変更した場合等 3）関係する法令又は規制の大きな変化 4）契約に関する大きな変更等						
	リスクアセスメントの結果を提示してください。						
8．3 情報セキュリティリスク対応	リスク対応計画の実施事項は実行していますか。						
	リスク対応計画の実行結果を提示してください。						
9．　パフォーマンス評価							
9．1　監視、測定、分析及び評価	ISMSの有効性を評価していますか。						
	パフォーマンス評価の対象は明確になっていますか。						
	評価の対象には、情報セキュリティプロセス及び管理策が含まれていますか。						
	確認方法は決まっていますか。						
	確認の時期と実施者は決まっていますか。						
	確認結果の評価の時期と評価者は決まっていますか。						
	評価結果を提示してくだい。						
9．2　内部監査							

凡例：　○：適合　△：観察事項　×：不適合　－：対象外　　○：監査対象項目

監査項目	チェック事項	検証結果	確認結果　または　文書類(日付)	備考	管理責任者	システム管理	●●部
9．2．1　一般	定期的(年に1回)に内部監査を実施していますか。						
	内部監査では、以下を確認していますか。 ・ISO27001の要求事項に適合している ・当社のルールに適合している。実行している。						
9．2．2　内部監査プログラム	内部監査計画では、以下を考慮していますか。 ・当社の業務 ・前回までの内部監査の指摘、前回の審査の指摘						
	内部監査の監査基準、監査の範囲を明確にしていますか。						
	内部監査員は、自部門の監査を実施していませんか。						
	内部監査結果は、関係者に報告していますか。						
	「内部監査計画書」「内部監査報告書」を提示してください。						
9．3　マネジメントレビュー							
9．3．1　一般	定期的(年に1回)にマネジメントレビューを実施していますか。						
9．3．2　マネジメントレビューへのインプット	「マネジメントレビュー議事録」の項目に「 前回までのマネジメントレビューの結果とった処置の状況」が含まれていますか。						
	「マネジメントレビュー議事録」の項目に「ISMSに関連する外部及び内部の課題の変化」が含まれていますか。						
	「マネジメントレビュー議事録」の項目に「ISMSに関連する利害関係者のニーズ及び期待の変化」が含まれていますか。						
	「マネジメントレビュー議事録」の項目に「情報セキュリティパフォーマンスに関するフィードバック」が含まれていますか。						
	「マネジメントレビュー議事録」の項目に「利害関係者からのフィードバック」が含まれていますか。						
	「マネジメントレビュー議事録」の項目に「リスクアセスメントの結果及びリスク対応計画の状況」が含まれていますか。						
	「マネジメントレビュー議事録」の項目に「継続的改善の機会」が含まれていますか。						
9．3．3　マネジメントレビューの結果	「マネジメントレビュー議事録」の指示項目に「ISMSのあらゆる変更の必要性」が含まれていますか。						
	「マネジメントレビュー議事録」を提示してください。						
10．　改善							
10．1　継続的改善	ISMSを継続的に改善していますか。						
10．2　不適合及び是正処置	「是正処置報告書」に、以下を含めていますか。 1）不適合の修正 2）不適合の結果						
	「是正処置報告書」に、以下を含めていますか。 1）不適合をレビュー 2）不適合の原因 3）類似の不適合の有無						
	「是正処置報告書」に、以下を含めていますか。 ・必要な処置						
	「是正処置報告書」に、以下を含めていますか。 ・是正処置の有効性						
	「是正処置報告書」に、以下を含めていますか。 ・必要に応じ、ISMSの変更						
	不適合は是正されていますか。						
	「是正処置報告書」を提示してください。						

旋回内部監査時の不適合及び観察事項の確認				

内部監査チェックリスト−有効性（管理策）

実施日：＿＿＿＿＿＿＿＿＿＿
内部監査員：＿＿＿＿＿＿＿＿＿＿
被監査部門：＿＿＿＿＿＿＿＿＿＿

◎：重点監査項目
○：監査対象項目

○：適合　△：観察事項　×：不適合　−：対象外

表A.1ー管理策			チェック事項	検証結果	確認結果　または　文書類(日付)	備考	管理責任者	システム管理	●●部
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方針群とトピック固有の方針は ①定義し管理層が承認しているか ②従業員は入手可能か ③利害関係者に通知・認知させているか ④定期的に見直しているか ⑤重大な変化が発生した場合に見直しているか						
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。	情報セキュリティの役割と責任を ①定めているか ②適切に割り当てているか						
5.3	職務の分離	相反する職務及び責任範囲は、分離しなければならない。	重要な業務については、1人で完結しない様にしているか ①実施と検証の担当を分けているか ②作成と承認は別の者か						
5.4	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。	管理層は、自社の従業者が守らなければならないセキュリティ要求事項を明確にし、通知しているか						
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。	インシデントやシステム障害が発生した場合 ①連絡が必要な関係当局は明確か ②連絡手順は定められているか ③維持しているか						
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。	情報セキュリティに関する ①情報取得先は明確か ②適切な連絡体制を維持しているか						
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・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。	情報セキュリティの脅威に関する情報を ①収集・分析しているか ②脅威インテリジェンスを作成しているか						
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。	・各プロジェクトについて ①取組むセキュリティは明確か ②取組んでいるか ・新しいシステムを導入する際や、既存のシステムを改善する際、セキュリティ要求事項を明確にしているか						
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。	・資産目録について ①主要な情報資産を特定し、目録を作成しているか ②維持されているか ・各資産管理責任者は明確か						
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。	・資産目録には、許容範囲が明確に記載されているか ・資産の取扱いに関する ①手順は情報分類体系に従い策定されているか ②手順は実施されているか						
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。	雇用・契約の変更または終了時に ①返却させなければならない情報資産は明確か ②返却をさせているか						
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。	情報は ①機密性、完全性、可用性に基づいて分類されているか ②取扱いに慎重を要する度合いからの分類か						
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。	情報のラベリングに関する ①手順は情報分類体系に従って策定されているか ②手順は実施されているか						
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。	①通信設備を利用する情報転送の方針、手順は明確に規定されているか ②方針、手順は実施されているか 例） 極秘：メール不可 関係者外秘／社外秘：メール添付はパスワード ③外部組織との情報転送（運送業者を含む）に関して ・情報転送ルールを定めているか ・セキュリティを保った転送について、合意を取り交わしているか ④電子的メッセージ通信に含まれた情報は，適切に保護されているか 例） 添付メールのパスワード 通信の暗号化　等						
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 ①物理的及び論理的アクセス制御は策定し実施しているか ②アクセス制御方針は文書化されているか ③アクセス制御方針はレビューされているか ④利用者に提供するネットワークサービスは、認可したネットワークのみか						
5.16	アイデンティティ(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。	利用者の登録／削除、アイデンティティはライフサイクルを通して管理しているか ①正式なプロセスはあるか ②プロセスは実施されているか						
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り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。	・秘密認証情報（ID／パスワード、生体認証等）の割当ては関係者に通知を含んだ管理プロセスにより管理されているか ①正式な管理のプロセスはあるか ②管理されているか ・秘密認証情報の利用のルールを ①利用者に周知しているか ②利用者は実行しているか ・パスワードについては ①パスワードの入力は対話式か ②パスワード入力時には＊＊＊表示等になるか ③ポリシー違反（必要桁数以下や間違い）の場合メッセージが表示されるか						
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。	・情報資産へのアクセス権はアクセス制御ルールに基づき ①提供と削除をしているか ②見直しと修正はしているか ・全てのシステム及びサービスについて利用者のアクセスの割当て／無効化に ①正式なプロセスはあるか ②プロセスは実施されているか ・資産の管理責任者は利用者のアクセス権を定期的に見直しているか ・雇用終了時に ①各システムへのアクセス権を削除しているか ②各入室の権利は抹消されているか						
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。	供給者から供給された製品やサービスに関して、セキュリティリスクを管理するためのプロセスまたは手順は ①定めているか ②実施しているか 情報セキュリティ要求事項について供給者と合意し，文書化しているか						
5.20	供給者との合意における情報セキュリティの取扱い	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。	①関連する全ての情報セキュリティ要求事項を確立しているか ②供給者と要求事項について合意しているか						
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要求事項を含めているか ICT製品やサービスに関して、セキュリティリスクを管理するためのプロセスまたは手順は ①定めているか ②実施しているか						
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。	供給者の情報セキュリティの実践とサービス提供の変更を ①定常的／定期的監視しているか ②レビューしているか ③見直し、評価しているか ④供給者によるサービス提供の変更を管理しているか 例） 問題が発生しないことを確認 再契約　等						
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取得、利用、管理、終了のプロセスは情報セキュリティ要求事項に基づき策定しているか						
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する ①管理のプロセスは定義されているか ②管理層の役割・責任は明確か ③手順は明確か						
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。	情報セキュリティ事象は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ているか						
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の対応について ①文書化した手順があるか ②手順に従って対応しているか						
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。	①情報セキュリティインシデントは分析しているか ②分析及び解決から将来起こる可能性又はその影響を低減するために用いているか ③分析結果を組織内で学習しているか						
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。	①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ているか ②手順は実施されているか						
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。	①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ているか ②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、計画、手順及び管理策を確立し、文書化しているか ③定期的に、これらをの管理策が有効である事を検証しているか						
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。	事業継続の目的とICT継続の要求事項に基づいてICTの備えを ①計画しているか ②実施しているか ③維持及びテストしているか						
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。	①全ての関連する法令、規制及び契約上の要求事項は文書化されているか ②要求事項を満たすための組織の取組みをは文書化されているか ③文書は最新に保もたれているか ④暗号化に関する規制を順守しているか						

表A.1－管理策			チェック事項	検証結果	確認結果 または 文書類(日付)	備考	管理責任者	システム管理	●●部
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	①知的財産権に関する要求事項の順守の手順を確立しているか ②ソフトウェアライセンスを管理する手順を確認しているか ③手順は実施されているか						
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	法令・規則・契約等で必要な記録は、消失、破壊、改ざん、不正アクセス、漏洩から保護、管理されているか						
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の保護は、関連する法令、規制及び契約上の要求事項に従って ①識別しているか ②遵守しているか						
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。	①定期的にISMSの内部監査及び、マネジメントレビューが実施されているか ②重大な変化が生じた場合に、ISMSの内部監査及び、マネジメントレビューが実施されているか						
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。	情報セキュリティ方針、セキュリティ手順について ①正しく実行されているか ②定期的に点検しているか ③技術的順守が実施されているかを点検しているか						
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。	①重要な装置や業務に関する手順書は整備されているか ②必要な利用者に利用可能になっているか						
6 人的管理策									
6.1	選考(スクリーニング)	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。	対象の従業者を雇用(選考)する場合 ①確認事項は明確か ②確認事項を実施しているか						
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。	対象の従業者を雇用する場合 ①セキュリティ要求事項を明記した雇用契約書等を取り交わしているか						
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。	情報セキュリティに関する教育は ①全てに従業員に実施しているか ②意識向上のための教育か ③教育は更新を行っているか						
.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者に対する懲戒処分に関する事項が ①文書化されているか ②周知されているか						
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。	雇用終了時に、情報セキュリティ要求事項を一定期間順守させるための、手段を講じているか 例)誓約書の取得						
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。	委託先・取引先との契約書の内容は、セキュリティ要求事項が明確になった秘密保持契約を取り交わし署名させているか						
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。	テレワーキングについて ①セキュリティに関する方針は明確か ②セキュリティ対策は明確か ③対策は実施されているか ④認められていない所で実施していないか						
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は、報告されているか ・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 ①どのようなものでも記録し、報告することを要求しているか ②記録・報告されているか ・従業員に対して、情報セキュリティインシデント発生時に即座に対応できる手順は提供しているか						
7 物理的管理策									
7.1	物理的セキュリティ境界	物理的セキュリティ境界	①物理的セキュリティ境界を定めているか ②物理的セキュリティ境界を周知しているか						
.7.2	物理的入退	物理的入退	①物理的セキュリティの境界において、入退管理を実施しているか ②対象の従業者以外が立ち入る場所は明確か ③この場所には情報や情報処理施設は無いか ④この場所からの入室の制限はされているか						
.7.3	オフィス、部屋及び施設のセキュリティ	オフィス、部屋及び施設のセキュリティ	施設内におけるセキュリティレベルが明確で、レベルに従った対策が実施されているか						
.7.4	物理的セキュリティの監視	物理的なセキュリティ監視	物理的セキュリティを設けている重要区画について、継続的に監視する対策もしくは設備はあるか						
.7.5	物理的及び環境の脅威からの保護	物理的及び環境的脅威からの保護	資産は自然災害、人的災害から守るべき手段が実施されているか 例) ・PCはどの様に保護しているか ・サーバはどの様に保護しているか ・その他重要な機器は何か、その保護はどうしているか						
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	①セキュリティを保つべき領域は明確か ②作業手順は明確か ③作業手順は実施されているか						
7.7	クリアデスク・クリアスクリーン	クリアデスク・クリアスクリーン	①離席時に机上に資産の放置をしない、PCをスリープ状態にする等のルールは定めているか ②使用後の資産は直ちに所定の場所へ格納しているか ③①、②を従業員に周知し確実に遂行させているか ④モニターへ、パスワード等を貼りつけていないか						
7.8	装置の設置及び保護	装置の設置及び保護	装置は入退管理を実施している部屋に設置するか盗難防止の処置を施しているか						
7.9	構外にある資産のセキュリティ	構外にある資産のセキュリティ	構外にある装置(例:PC、携帯電話、サーバ等)について セキュリティ対策は実施されているか						
7.10	記憶媒体(Storagemedia)	記憶媒体	取り外し可能な記憶媒体の ①分類体系の規定はあるか ②取扱いの要求事項を定めた規定はあるか ③それらの規定に従って、取得、使用、移動及び廃棄のライフサイクルは実施、管理されているか ・分類体系に従って ①取外し可能な媒体の管理手順はあるか ②手順は実施されているか ・媒体が不要になった場合の ①正式な手順はあるか ②手順を用いて処分しているか ③セキュリティを保って処分しているか ・輸送中の媒体は保護されているか ・装置、情報又はソフトウェアの持出しは、事前の認可を得ているか ・持ち運びの規定はあるか						
7.11	サポートユーティリティ	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から保護されているか 例) ・UPSの設置 ・電源容量の確認 ・適切な空調						
7.12	ケーブル配線のセキュリティ	ケーブル配線のセキュリティ	ケーブル等は保護されているか 例) ・切断・外れが無いように対策を実施 ・電源ケーブルと信号ケーブルが並行ではない ・ケーブルのラベリング						
7.13	装置の保守	装置の保守	・装置は機密性、完全性、可用性の維持を目的に正しく保守されているか 例) ・重要な装置は保守契約を締結 ・メーカー推奨通りに保守を行う ・力量のある者が保守を行う						
7.14	装置のセキュリティを保った処分又は再利用	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、入出力媒体等に蓄積されたデータは処分や再利用の前に ・媒体の破壊 ・専用ソフトウェアによる消去 ・消磁気装置による磁気的消去 等の方法により完全消去しているか						
8 技術的管理策									
8.1	利用者エンドポイント機器(ユーザーエンドポイントデバイス)	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。	・エンドポイントに保存されている情報は保護されているか ・各モバイル機器について ①セキュリティに関する方針は明確か ②セキュリティ対策は明確か ③対策は実施されているか ・複合機等管理者が不明確な装置に関するルールが設定され、実施されているか ・スクリーンセーバは定められた手順に従い、動作するようにセッティングされているか						
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。	特権的アクセス権の割当て及び利用は ①制限されているか ②管理されているか						
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へのアクセスは、制限されているか 例) 権限外のアクセスが行なわた場合にワーニングメッセージ						
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。	①プログラムソースコードへのアクセスは制限されているか ②ソースコードへの書き込み、読み込み、開発ツールやソフトウェアライブラリへのアクセスは制御されているか ③運用環境は実行可能なコードのみか						

表A.1－管理策			チェック事項	検証結果	確認結果 または 文書類(日付)	備考	管理責任者	システム管理	●●部
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。	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か 例） ID／パスワードを設定						
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	①資源（ディスク容量、ネットワーク性能等）の利用を監視・調整しているか ②将来必要とする容量・能力を予測しているか						
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	マルウェアから保護するために ①利用者に適切に認識させているか ②検出、予防及び回復のための管理策がなされているか 例） ・マルウェア対策ソフトの導入／パターンの更新／フルスキャン ・ブラウザの設定 ・不正メールの対応　等						
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。	・定期的なセキュリティパッチ等を確実に実施しているか ・技術的順守が実施されているかの点検をしているか						
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、ネットワークのセキュリティ設定は ①確立されているか ②文書化しているか ③実施しているか ④監視し評価しているか						
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。	不必要になった情報は即座に削除しているか						
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。	データマスキングは適用される法律を考慮して ①アクセス制御に関する組織の規定、トピック固有の個別方針、関連手順は定められているか ②それらはビジネス要求事項に従って運用されているか						
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。	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、デバイスに対してデータ漏洩防止対策をしているか						
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。	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について ①方針は明確か ②定期的に取得しているか ③検査しているか						
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のに十分な冗長性をもって導入されているか						
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たイベントログを ①取得しているか ②適切に保持しているか ③定期的にレビュー、分析しているか 例） アクセスログ、障害ログ、入退出ログ　等 ・ログ機能及びログ情報は保護されているか 例） 限定されたアクセス ログのバックアップ　等 ・システムの実務管理者及び運用担当者の作業は ①記録しているか ②そのログを保護しているか ③定期的にレビューしているか						
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。	ネットワーク、システム、アプリケーションの異常な挙動を ①監視しているか ②分析し評価しているか ③適切な処置を講じているか						
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。	ログを取得しているシステムの時間は ①正しいか ②修正は行っているか						
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。	ユーティリティプログラムの使用は制限し、厳しく管理されているか						
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。	・運用システムに関わるソフトウェアの導入を、セキュリティを保った状態で管理するための ①対策はあるか ②手順はあるか ③手順を実施しているか ・利用者によるソフトウェアのインストールについて ①管理する規則を確立しているか ②規則は実施されているか						
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。	ネットワークとネットワークデバイスは適切な管理策が実施されているか 例） ・無線LANは十分な安全対策をとられているか （ファームウェアアップデート、適切な暗号化方式を使用している無線LANの利用） ・MACアドレス等で機器を識別 ・ファイアーウォールの設置、設定 ・決められた機器のみ社内LANに接続できる ・業務以外でメールを利用していないか　等						
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について特定・実施し、監視しているか ①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ているか ②ネットワークサービス合意書にもこれらが盛り込まれているか						
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。	ネットワークは分離されているか 例） ・外部／内部の分離 ・セグメント別　等						
8.23	ウェブフィルタリング	悪意のあるコンテンツへ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。	組織のポリシーから逸脱したウェブサイトへのアクセスを制限しているか						
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。	・暗号による管理策の利用に関する方針は ①策定されているか ②実施されているか ・暗号鍵の利用、保護及び有効期限（lifetime）に関する方針を ①策定しているか ②ライフサイクル全体にわたって実施しているか						
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。	①開発のための規則は確立しているか ②規則は適用されているか						
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。	①アプリケーションの開発・取得時には情報セキュリティ要求事項を特定し対処しているか ②インターネットを利用したアプリケーションサービスは保護されているか ③ホームページ等、一般に公開している情報がある場合、改ざん等からの保護対策を実施しているか ④アプリケーションサービスのトランザクションは保護されているか						
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。	システムの構築に関して ①セキュリティに関する原則を文書化しているか ②全ての情報システムの実装に対して適用しているか						
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。	ソフトウェア開発時は、セキュリティを考慮した設計（コーディング）をしているか						
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。	セキュリティ機能の試験は、開発期間中に実施しているか ①受入れ試験のプログラム及び関連する基準は確立しているか ②実施されているか						
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。	外部にシステム開発を委託した場合、監督／管理しているか						
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。	・開発環境、試験環境、運用環境は分離しているか ・セキュリティに配慮した開発環境を確立しているか						
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は、管理しているか 例） 認可の上、変更を行っている 変更の記録、履歴を残す ・システムの変更は ①正式な変更管理手続があるか ②手続きに基づき管理されているか ・OS等の変更では、 ①重要なアプリケーションへの影響をレビューしているか ②試験を行っているか ・パッケージソフトウェアの変更は ①抑止されているか ②必要な変更だけに限られているか ③厳重に管理されているか						
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。	試験データは ①注意深く選定しているか 例）重要な個人情報が含まれていないか ②保護されているか						
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。	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（メンテナンスも含む） ①業務プロセスの中断を最小限に抑える計画をしているか ②計画は利用者／部門と合意しているか						

前回内部監査不適合及び観察事項の処置状況									

内部監査チェックリスト-適合性(箇条4.-10.及び管理策)

実施日：＿＿＿＿＿＿＿＿＿＿
内部監査員：＿＿＿＿＿＿＿＿＿＿
被監査部門：＿＿＿＿＿＿＿＿＿＿

凡例：　○：適合　△：観察事項　×：不適合　－：対象外

監査項目	要求事項	検証結果	確認した文書類（日付）	備考
4．組織の状況				
4．1 組織及びその状況の理解	組織は，組織の目的に関連し，かつ，そのISMS の意図した成果を達成する組織の能力に影響を与える，外部及び内部の課題を決定しなければならない。			
4．2 利害関係者のニーズ及び期待の理解	組織は，次の事項を決定しなければならない。 a) ISMS に関連する利害関係者			
	b) それらの利害関係者の，関連する要求事項			
	c) それらの要求事項のうち，ISMS を通して取り組むもの			
4．3 情報セキュリティマネジメントシステムの適用範囲の決定	組織は，ISMS の適用範囲を定めるために，その境界及び適用可能性を決定しなければならない。 この適用範囲を決定するとき，組織は，次の事項を考慮しなければならない。 a) 4.1 に規定する外部及び内部の課題			
	b) 4.2 に規定する要求事項			
	c) 組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係			
	ISMS の適用範囲は，文書化した情報として利用可能な状態にしなければならない。			
4．4 情報セキュリティマネジメントシステム	組織は，この規格の要求事項に従って，必要なプロセス及びそれらの相互作用を含む，ISMS を確立し，実施し，維持し，かつ，継続的に改善しなければならない。			
5．リーダーシップ				
5．1 リーダーシップ及びコミットメント	トップマネジメントは，次に示す事項によって，ISMS に関するリーダーシップ及びコミットメントを実証しなければならない。 a) 情報セキュリティ方針及び情報セキュリティ目的を確立し，それらが組織の戦略的な方向性と両立することを確実にする。			
	b) 組織のプロセスへのISMS 要求事項の統合を確実にする。			
	c) ISMS に必要な資源が利用可能であることを確実にする。			
	d) 有効な情報セキュリティマネジメント及びISMS 要求事項への適合の重要性を伝達する。			
	e) ISMS がその意図した成果を達成することを確実にする。			
	f) ISMS の有効性に寄与するよう人々を指揮し，支援する。			
	g) 継続的改善を促進する。			
	h) その他の関連する管理層がその責任の領域においてリーダーシップを実証するよう，管理層の役割を支援する。			
5．2 方針	5.2 方針 トップマネジメントは，次の事項を満たす情報セキュリティ方針を確立しなければならない。 a) 組織の目的に対して適切である。			
	b) 情報セキュリティ目的（6．2 参照）を含むか，又は情報セキュリティ目的の設定のための枠組みを示す。			
	c) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む。			
	d) ISMS の継続的改善へのコミットメントを含む。			
	情報セキュリティ方針は，次に示す事項を満たさなければならない。 e) 文書化した情報として利用可能である。			
	f) 組織内に伝達する。			
	g) 必要に応じて，利害関係者が入手可能である。			
5．3 組織の役割、責任及び権限	トップマネジメントは，情報セキュリティに関連する役割に対して，責任及び権限が割り当てられ，組織内に伝達されることを確実にしなければならない。			
	トップマネジメントは，次の事項に対して，責任及び権限を割り当てなければならない。 a) ISMS が，この規格の要求事項に適合することを確実にする。			
	b) ISMS のパフォーマンスをトップマネジメントに報告する。			
6．計画				
6．1 リスク及び機会に対処する活動				
6．1．1 一般	ISMS の計画を策定するとき，組織は，4.1 に規定する課題及び4.2 に規定する要求事項を考慮し，次の事項のために対処する必要があるリスク及び機会を決定しなければならない。 a) ISMS が，その意図した成果を達成できることを確実にする。			
	b) 望ましくない影響を防止又は低減する。			
	c) 継続的改善を達成する。			
	組織は，次の事項を計画しなければならない。 d) 上記によって決定したリスク及び機会に対処する活動			
	e) 次を行う方法 1) その活動のISMS プロセスへの統合及び実施 2) その活動の有効性の評価			

凡例：　○：適合　△：観察事項　×：不適合　－：対象外

監査項目	要求事項	検証結果	確認した文書類（日付）	備考
6．1．2　情報セキュリティリスクアセスメント	組織は，次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め，適用しなければならない。 a) 次を含む情報セキュリティのリスク基準を確立し，維持する。 1) リスク受容基準 2) 情報セキュリティリスクアセスメントを実施するための基準			
	b) 繰り返し実施した情報セキュリティリスクアセスメントが，一貫性及び妥当性があり，かつ，比較可能な結果を生み出すことを確実にする。			
	c) 次によって情報セキュリティリスクを特定する。 1) ISMS の適用範囲内における情報の機密性，完全性及び可用性の喪失に伴うリスクを特定するために，情報セキュリティリスクアセスメントのプロセスを適用する。 2) これらのリスク所有者を特定する。			
	d) 次によって情報セキュリティリスクを分析する。 1) 6.1.2 c) 1) で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う。 2) 6.1.2 c) 1) で特定されたリスクの現実的な起こりやすさについてアセスメントを行う。 3) リスクレベルを決定する。			
	e) 次によって情報セキュリティリスクを評価する。 1) リスク分析の結果と6.1.2 a) で確立したリスク基準とを比較する。 2) リスク対応のために，分析したリスクの優先順位付けを行う。			
	組織は，情報セキュリティリスクアセスメントのプロセスについての文書化した情報を保持しなければならない。			
6．1．3　情報セキュリティリスク対応	組織は，次の事項を行うために，情報セキュリティリスク対応のプロセスを定め，適用しなければならない。 a) リスクアセスメントの結果を考慮して，適切な情報セキュリティリスク対応の選択肢を選定する。			
	b) 選定した情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定する。			
	c) 6.1.3 b) で決定した管理策を附属書A に示す管理策と比較し，必要な管理策が見落とされていないことを検証する。			
	d) 次を含む適用宣言書を作成する。 － 必要な管理策[6.1.3 のb) 及びc) 参照] － それらの管理策を含めた理由 － それらの必要な管理策を実施しているか否か － 附属書A に規定する管理策を除外した理由			
	e) 情報セキュリティリスク対応計画を策定する。			
	f) 情報セキュリティリスク対応計画及び残留している情報セキュリティリスクの受容について，リスク所有者の承認を得る。			
	組織は，情報セキュリティリスク対応のプロセスについての文書化した情報を保持しなければならない。			
6．2　情報セキュリティ目的及びそれを達成するための計画策定	組織は，関連する機能及び階層において，情報セキュリティ目的を確立しなければならない。			
	情報セキュリティ目的は，次の事項を満たさなければならない。 a) 情報セキュリティ方針と整合している			
	b) （実行可能な場合）測定可能である。			
	c) 適用される情報セキュリティ要求事項，並びにリスクアセスメント及びリスク対応の結果を考慮に入れる。			
	d) これを監視する。			
	e) これを伝達する。			
	f) 必要に応じて，更新する。			
	g) 文書化した情報として利用可能な状態にする。			
	組織は，情報セキュリティ目的に関する文書化した情報を保持しなければならない。			
	組織は，情報セキュリティ目的をどのように達成するかについて計画するとき，次の事項を決定しなければならない。 h) 実施事項			
	i) 必要な資源			
	j) 責任者			
	k) 達成期限			
	l) 結果の評価方法			
6．3 変更の計画	組織がISMS の変更の必要があると決定したとき，その変更は，計画的な方法で行わなければならない。			
7．支援				
7．1 資源	組織は，ISMS の確立，実施，維持及び継続的改善に必要な資源を決定し，提供しなければならない。			
7．2 力量	組織は，次の事項を行わなければならない。 a) 組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。			

凡例：　○：適合　△：観察事項　×：不適合　－：対象外

監査項目	要求事項	検証結果	確認した文書類（日付）	備考
	b) 適切な教育，訓練又は経験に基づいて，それらの人々が力量を備えていることを確実にする。			
	c) 該当する場合には，必ず，必要な力量を身に付けるための処置を講じ，講じた処置の有効性を評価する。			
	d) 力量の証拠として，適切な文書化した情報を保持する。			
7．3 認識	組織の管理下で働く人々は，次の事項に関して認識をもたなければならない。 a) 情報セキュリティ方針			
	b) 情報セキュリティパフォーマンスの向上によって得られる便益を含む，ISMS の有効性に対する自らの貢献			
	c) ISMS 要求事項に適合しないことの意味			
7．4 コミュニケーション	組織は，次の事項を含む，ISMS に関連する内部及び外部のコミュニケーションを実施する必要性を決定しなければならない。 a) コミュニケーションの内容			
	b) コミュニケーションの実施時期			
	c) コミュニケーションの対象者			
	d) コミュニケーションの方法			
7．5 文書化した情報				
7．5．1 一般	組織のISMS は，次の事項を含まなければならない。 a) この規格が要求する文書化した情報			
	b) ISMS の有効性のために必要であると組織が決定した，文書化した情報			
7．5．2 作成及び更新	文書化した情報を作成及び更新する際，組織は，次の事項を確実にしなければならない。 a) 適切な識別及び記述（例えば，タイトル，日付，作成者，参照番号）			
	b) 適切な形式（例えば，言語，ソフトウェアの版，図表）及び媒体（例えば，紙，電子媒体）			
	c) 適切性及び妥当性に関する，適切なレビュー及び承認			
7．5．3 文書化した情報の管理	ISMS 及びこの規格で要求されている文書化した情報は，次の事項を確実にするために，管理しなければならない。 a) 文書化した情報が，必要なときに，必要なところで，入手可能かつ利用に適した状態である。			
	b) 文書化した情報が十分に保護されている（例えば，機密性の喪失，不適切な使用又は完全性の喪失からの保護）。			
	文書化した情報の管理に当たって，組織は，該当する場合には，必ず，次の行動に取り組まなければならない。 c) 配付，アクセス，検索及び利用			
	d) 読みやすさが保たれることを含む，保管及び保存			
	e) 変更の管理（例えば，版の管理）			
	f) 保持及び廃棄			
	ISMS の計画策定及び運用のために組織が必要と決定した外部からの文書化した情報は，必要に応じて 識別し，管理しなければならない。			
8．運用				
8．1 運用の計画策定及び管理	組織は，次に示す事項の実施によって，要求事項を満たすため，及び箇条6 で決定した活動を実施するために必要なプロセスを計画し，実施し，かつ，管理しなければならない。 ― プロセスに関する基準の設定 ― その基準に従った，プロセスの管理の実施			
	組織は，プロセスが計画どおりに実施されたという確信をもつために必要とされる，文書化した情報を利用可能な状態にしなければならない。			
	組織は，計画した変更を管理し，意図しない変更によって生じた結果をレビューし，必要に応じて，有 害な影響を軽減する処置を講じなければならない。			
	組織は，ISMS に関連する，外部から提供されるプロセス，製品又はサービスが管理されていることを確実にしなければならない。			
8．2 情報セキュリティリスクアセスメント	組織は，あらかじめ定めた間隔で，又は重大な変更が提案されたか若しくは重大な変化が生じた場合に，6.1.2 a） で確立した基準を考慮して，情報セキュリティリスクアセスメントを実施しなければならない			
	組織は，情報セキュリティリスクアセスメント結果の文書化した情報を保持しなければならない。			
8．3 情報セキュリティリスク対応	組織は，情報セキュリティリスク対応計画を実施しなければならない。			
	組織は，情報セキュリティリスク対応結果の文書化した情報を保持しなければならない。			
9．　パフォーマンス評価				
9．1 監視、測定、分析及び評価	組織は，次の事項を決定しなければならない。 a) 監視及び測定が必要な対象。これには，情報セキュリティプロセス及び管理策を含む。			
	b) 該当する場合には，必ず，妥当な結果を確実にするための，監視，測定，分析及び評価の方法。選定した方法は，妥当と考えられる，比較可能で再現可能な結果を生み出すことが望ましい			
	c) 監視及び測定の実施時期			
	d) 監視及び測定の実施者			

凡例：　○：適合　△：観察事項　×：不適合　－：対象外

監査項目	要求事項	検証結果	確認した文書類（日付）	備考
	e) 監視及び測定の結果の，分析及び評価の時期			
	f) 監視及び測定の結果の，分析及び評価の実施者			
	組織は，この結果の証拠として，文書化した情報を利用可能な状態にしなければならない。			
	組織は，情報セキュリティパフォーマンス及びISMS の有効性を評価しなければならない。			
9．2　内部監査				
9．2．1　一般	組織は，ISMS が次の状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施しなければならない。 a) 次の事項に適合している。 1) ISMS に関して，組織自体が規定した要求事項 2) この規格の要求事項			
	b) 有効に実施され，維持されている。			
9．2．2　内部監査プログラム	組織は，監査プログラムを計画し，確立し，実施し，維持しなければならない。これには，その頻度，方法，責任，計画策定の要求事項及び報告を含める。			
	それ（れら）の内部監査プログラムを確立するとき，組織は，関連するプロセスの重要性及び前回までの監査の結果を考慮しなければならない。			
	組織は，次に示す事項を行わなければならない。 a) 各監査について，監査基準及び監査範囲を明確にする			
	b) 監査プロセスの客観性及び公平性を確保するために，監査員を選定し，監査を実施する。			
	c) 監査の結果を関連する管理層に報告することを確実にする。			
	組織は，監査プログラムの実施及び監査結果の証拠として，文書化した情報を利用可能な状態にしなければならない。			
9．3　マネジメントレビュー				
9．3．1　一般	トップマネジメントは，組織のISMS 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，あらかじめ定めた間隔で，ISMS をレビューしなければならない。			
9．3．2　マネジメントレビューへのインプット	マネジメントレビューは，次の事項を考慮しなければならない。 a) 前回までのマネジメントレビューの結果講じた処置の状況			
	b) ISMS に関連する外部及び内部の課題の変化			
	c) ISMS に関連する利害関係者のニーズ及び期待の変化			
	d) 次に示す傾向を含めた，情報セキュリティパフォーマンスに関するフィードバック 1) 不適合及び是正処置 2) 監視及び測定の結果 3) 監査結果 4) 情報セキュリティ目的の達成			
	e) 利害関係者からのフィードバック			
	f) リスクアセスメントの結果及びリスク対応計画の状況			
	g) 継続的改善の機会			
9．3．3　マネジメントレビューの結果	マネジメントレビューの結果には，継続的改善の機会，及びISMS のあらゆる変更の必要性に関する決定を含めなければならない。			
	組織は，マネジメントレビューの結果の証拠として，文書化した情報を利用可能な状態にしなければならない。			
10．　改善				
10．1　継続的改善	組織は，ISMS の適切性，妥当性及び有効性を継続的に改善しなければならない。			
10．2　不適合及び是正処置	不適合が発生した場合，組織は，次の事項を行わなければならない。 a) その不適合に対処し，該当する場合には，必ず，次の事項を行う。 1) その不適合を管理し，修正するための処置を講じる。 2) その不適合によって起こった結果に対処する。			
	b) その不適合が再発又は他のところで発生しないようにするため，次の事項によって，その不適合の原因を除去するための処置を講じる必要性を評価する。 1) その不適合をレビューする。 2) その不適合の原因を明確にする。 3) 類似の不適合の有無，又はそれが発生する可能性を明確にする。			
	c) 必要な処置を実施する。			
	d) 講じた全ての是正処置の有効性をレビューする。			
	e) 必要な場合には，ISMS の変更を行う。			
	是正処置は，検出された不適合のもつ影響に応じたものでなければならない。			
	組織は，次に示す事項の証拠として，文書化した情報を利用可能な状態にしなければならない。 f) 不適合の性質及びそれに対して講じたあらゆる処置			
	g) 是正処置の結果			

監査項目	要求事項	検証結果	確認した文書類（日付）	備考
5　組織的管理策				
5.1　情報セキュリティのための方針群	管理策 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。			
5.2　情報セキュリティの役割及び責任	管理策 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。			
5.3　職務の分離	管理策 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。			
5.4　管理層の責任	管理策 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。			
5.5　関係当局との連絡	管理策 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。			
5.6　専門組織との連絡	管理策 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。			
5.7　脅威インテリジェンス	管理策 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。			
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	管理策 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。			
5.9　情報及びその他の関連資産の目録	管理策 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。			
5.10 情報及びその他の関連資産の許容される利用	管理策 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。			
5.11 資産の返却	管理策 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。			
5.12 情報の分類	管理策 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。			
5.13　情報のラベル付け	管理策 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。			
5.14　情報の転送	管理策 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。			
5.15　アクセス制御	管理策 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。			
5.16　識別情報の管理	管理策 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。			
5.17　認証情報	管理策 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。			
5.18　アクセス権	管理策 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。			
5.19　供給者関係における情報セキュリティ	管理策 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。			
5.20　供給者との合意における情報セキュリティの取扱い	管理策 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。			
5.21 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	管理策 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。			
5.22 供給者のサービス提供の監視，レビュー及び変更管理	管理策 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。			
5.23 クラウドサービスの利用における情報セキュリティ	管理策 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。			
5.24 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	管理策 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。			
5.25 情報セキュリティ事象の評価及び決定	管理策 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。			
5.26 情報セキュリティインシデントへの対応	管理策 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。			

凡例：　○:適合　△:観察事項　×:不適合　−:対象外

監査項目	要求事項	検証結果	確認した文書類(日付)	備考
5.27 情報セキュリティインシデントからの学習	管理策 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。			
5.28 証拠の収集	管理策 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。			
5.29 事業の中断・阻害時の情報セキュリティ	管理策 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。			
5.30 事業継続のためのICTの備え	管理策 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。			
5.31 法令，規制及び契約上の要求事項	管理策 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。			
5.32 知的財産権	管理策 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。			
5.33　記録の保護	管理策 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。			
5.34 プライバシー及び個人識別可能情報(PII)の保護	管理策 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。			
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。			
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	管理策 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。			
5.37 操作手順書	管理策 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				
6.1　選考	管理策 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。			
6.2 雇用条件	管理策 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。			
6.3 情報セキュリティの意識向上，教育及び訓練	管理策 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。			
6.4 懲戒手続	管理策 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。			
6.5 雇用の終了又は変更後の責任	管理策 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。			
6.6 秘密保持契約又は守秘義務契約	管理策 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。			
6.7 リモートワーク	管理策 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。			
6.8 情報セキュリティ事象の報告	管理策 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。			
7　組織的管理策				
7.1 物理的セキュリティ境界	管理策 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。			
7.2 物理的入退	管理策 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。			
7.3　オフィス，部屋及び施設のセキュリティ	管理策 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。			
7.4 物理的セキュリティの監視	管理策 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。			
7.5 物理的及び環境的脅威からの保護	管理策 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。			
7.6 セキュリティを保つべき領域での作業	管理策 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。			
7.7 クリアデスク・クリアスクリーン	管理策 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。			
7.8 装置の設置及び保護	管理策 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。			
7.9 構外にある資産のセキュリティ	管理策 構外にある資産を保護しなければならない。			
7.10 記憶媒体	管理策 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。			
7.11 サポートユーティリティ	管理策 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。			
7.12 ケーブル配線のセキュリティ	管理策 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。			
7.13 装置の保守	管理策 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。			
7.14 装置のセキュリティを保った処分又は再利用	管理策 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				
8.1 利用者エンドポイント機器	管理策 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。			
8.2 特権的アクセス権	管理策 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。			
8.3 情報へのアクセス制限	管理策 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。			
8.4 ソースコードへのアクセス	管理策 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。			
8.5 セキュリティを保った認証	管理策 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。			
8.6 容量・能力の管理	管理策 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。			
8.7 マルウェアに対する保護	管理策 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。			
8.8 技術的ぜい弱性の管理	管理策 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。			
8.9 構成管理	管理策 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。			
8.10 情報の削除	管理策 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。			
8.11 データマスキング	管理策 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。			
8.12 データ漏えい防止	管理策 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。			
8.13 情報のバックアップ	管理策 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。			
8.14 情報処理施設・設備の冗長性	管理策 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。			
8.15 ログ取得	管理策 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。			
8.16 監視活動	管理策 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。			
8.17 クロックの同期	管理策 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。			
8.18 特権的なユーティリティプログラムの使用	管理策 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。			
8.19 運用システムへのソフトウェアの導入	管理策 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。			

凡例：　〇:適合　△:観察事項　×:不適合　−:対象外

監査項目	要求事項	検証結果	確認した文書類（日付）	備考
8.20 ネットワークセキュリティ	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。			
8.21 ネットワークサービスのセキュリティ	管理策 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。			
8.22 ネットワークの分離	管理策 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。			
8.23 ウェブフィルタリング	管理策 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。			
8.24 暗号の利用	管理策 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。			
8.25 セキュリティに配慮した開発のライフサイクル	管理策 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。			
8.26 アプリケーションセキュリティの要求事項	管理策 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。			
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	管理策 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。			
8.28 セキュリティに配慮したコーディング	管理策 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。			
8.29 開発及び受入れにおけるセキュリティテスト	管理策 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。			
8.30 外部委託による開発	管理策 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。			
8.31 開発環境，テスト環境及び本番環境の分離	管理策 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。			
8.32 変更管理	管理策 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。			
8.33 テスト用情報	管理策 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			
8.34 監査におけるテスト中の情報システムの保護	管理策 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。			