【抜粋版】ISO/IEC27001:2022　内部監査チェックリスト（附属書A管理策）

確認（承認）	記入者
2023.00.00	2023.00.00
○○	○○

監査該当部門は、●で示しています。総合評価結果は適合、不適合、観察事項とします。－は非該当もしくは今回の監査では確認しなかった事項です。
なお、有効性評価については、管理策の目的を満たしているか、結果は出ているかを評価し、○、△、×で評価します。

規格項目等	チェック内容	ISMS管理責任者（ISMS事務局）	営業部門	○○部門	総務部門	システム課	コメント	有効性評価	総合評価結果	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 目的：事業上、法令、規制、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、適切性、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										
	「情報セキュリティ基本方針」を始めとする方針群を社長の承認を得て、発行し、全従業員及び関連する外部関係者に公表し、通知しているか	●					各方針群確認	○	適合	
	レビュー実施のための手順は確立されているか	●					「ISMS管理策運用規定」にて明確化	○	適合	
5.2　情報セキュリティの役割及び責任 目的：組織内における情報セキュリティの実施、運用及び管理のために、定義され、承認され、理解される仕組みを確立するため										
	情報セキュリティの責任を文書化して、具体的に明確にしてるか	●					「ISMSマニュアル」にて明確化	○	適合	
5.3　職務の分離 目的：不正行為、業務ミス、情報セキュリティ管理策の回避のリスクを軽減するため										
	不正使用の危険性を低減するために、職務を分離させるか、一つの職務権限に一人ではなく、複数の者を割り当てているか	●					「ISMS管理策運用規定」にて明確化	○	適合	
5.4　管理層の責任 目的：管理層が、情報セキュリティにおける自らの役割を理解し、全ての要員が自らの情報セキュリティの責任を認識し、果たすことを確実にすることを目的として行動することを確実にするため										
	すべての従業員及び契約相手に、当社の方針及び手順に従ったセキュリティの適用を要求しているか	●					「ISMS管理策運用規定」にて明確化	○	適合	
5.5　関係当局との連絡 目的：自社と、関連する法規制及び監督的な関係当局との間で情報セキュリティに関して適切なコミュニケーションが行われることを確実にするため										
	具体的な連絡体制を確立し、適切なコミュニケーションが行われているか	●					「ISMS管理策運用規定」にて明確化	○	適合	
5.6　専門組織との連絡 目的：自社と、専門組織との間で情報セキュリティに関する、適切なコミュニケーションが行われることを確実にするため										
	具体的な連絡体制を確立し、適切なコミュニケーションが行われているか					●	XXベンダーから情報提供を受けていた	○	適合	
5.7　脅威インテリジェンス 目的：自社の脅威環境を認識し、適切な低減処置を講じることができるようにするため										
	どのようにして、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ているか	●					「ISMS管理策運用規定」にて明確化	○	適合	
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 目的：プロジェクトと成果物に関連する情報セキュリティリスクが、プロジェクトのライフサイクルを全体を通じてプロジェクトマネジメントで効果的に対処されることを確実にするため										
	プロジェクトマネジメントにおいても情報セキュリティの取り組みを行っており、情報セキュリティが保たれているか	●					「ISMS管理策運用規定」にて明確化	○	適合	
5.9　情報及びその他の関連資産の目録 目的：自社の情報及びその他の関連資産を特定し、そ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										
	適用範囲内における情報資産は、「情報資産台帳」において特定しているか		●	●	●	●	「情報資産台帳」は更新されていたが、クラウドサービスが一部漏れてい	△	観察	
	資産の管理責任者は、「情報資産台帳」にて明示しているか		●	●	●	●	「情報資産台帳」にて明確化	○	適合	
5.10　情報及びその他の関連資産利用の許容範囲 目的：情報及びその他の関連資産が適切に保護、利用、取り扱いされることを確実にするため										
	資産利用の許容範囲は、「情報資産台帳」にて明示しているか		●	●	●	●	「情報資産台帳」にて明確化	○	適合	
	資産の取扱いは、分類に従って適切に行っているか （資産の紛失がないように整理・整頓されているか）		●	●	●	●	営業部において、紙袋に入った顧客資料が識別不明（管理不明）の状態で、机の下に置かれていた。	△	不適合	
5.11　資産の返却 目的：雇用、契約または合意を変更または終了するプロセスの一環として、組織の資産を保護するため										
	雇用、契約の終了時に、該当する従業員又は外部利用者から、社員証、社用名刺、施設入退室カード、貸与PC、携帯電話をはじめ、貸与した情報資産の返却を確実に行っているか				●		退職者の対応確認 （A氏確認）	○	適合	
5.12　情報の分類 目的：自社における情報の重要度に従って、情報の保護の要件を特定及び理解することを確実にするため										
	情報の分類は、基準に基づき、分類しているか		●	●	●	●	「情報資産台帳」にて明確化	○	適合	
5.13　情報のラベル付け 目的：情報の分類の伝達を容易にし、情報処理及び管理の自動化を支援するため										
	情報のラベル付けは、実施しているか		●	●	●	●	「情報資産台帳」にて明確化	○	適合	
5.14　情報の転送 目的：自社内及び外部の利害関係者との間で転送される情報のセキュリティを維持するため										
	情報転送の方針及び手順は周知され、適切に実施されているか	●				●	「ISMS管理策運用規定」にて明確化。Aに再確認	○	適合	
	他組織と機密情報を転送する場合は、秘密保持契約等を締結し、合意しているか		●	●	●	●	秘密保持契約書確認	○	適合	
	電子メールはウィルス感染対策を施しているか、また、その利用手順は周知され、適切に実施されているか		●	●	●	●	ウィルス対策ソフト導入確認	○	適合	
5.15　アクセス制御 目的：情報及び関連するその他の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										

規格項目等	チェック内容	ISMS管理責任者（ISMS事務局）	営業部門	○○部門	総務部門	システム課	コメント	有効性評価	総合評価結果	備考
	アクセス制御方針を定め、周知しているか	●					「ISMS管理策運用規定」にて明確化	○	適合	
	社内のネットワーク及びネットワークサービスへのアクセスは、セキュリティが保たれているか					●	アクセス制御実施	○	適合	
	過去のアクセス履歴等を考慮するなどの動的要素も考慮して、アクセス制御を行っているか					●	アクセス制御実施	○	適合	
5.16 識別情報の管理 目的：自社の情報及び関連するその他の資産にアクセスする個人及びシステムを一意に特定できるようにし、アクセス権の適切な割り当てを可能にするため										
	社内システムへの利用者登録及び登録削除、登録変更は適切に行っているか					●	退職者削除確認 (A氏確認)	○	適合	
5.17 認証情報 目的：本人（相手）認証を確実にし、認証プロセスの失敗を防止するため										
	パスワードの新規発行をする場合、事前に、利用者の確認を行っているか					●	利用者確認実施	○	適合	
	パスワードは、10文字以上でアルファベットと数字を混在させるなどしているか		●	●	●	●	利用者のPCデモ確認	○	適合	
	利用者がパスワードを再設定する場合、文字数が10桁未満は受け付けないなど、設定ルールは機能しているか					●	利用者確認実施	○	適合	
5.18 アクセス権 目的：情報及び関連するその他の資産へのアクセスが、事業上の要求事項に従って定義され、認可されていることを確実にするため										
	情報システム責任者は、すべてのシステムにおいて、責任者の承認を得て、個人ごとにIDとパスワードを発行しているか					●	利用者確認実施	○	適合	
	アカウントリストの見直しを行い、適切であるか、抹消漏れがないかを確認しているか					●	上長の確認実施	○	適合	
	雇用、契約の終了時に、情報システム責任者に依頼して、該当する従業員の社内システムへのアクセス権限をすべて抹消しているか					●	退職者削除確認 (A氏確認)	○	適合	
5.19 供給者関係における情報セキュリティ 目的：供給者から供給された製品もしくはサービスの利用に関連した情報セキュリティリスクを管理するため										
	供給者の製品またはサービスの使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策定している					●	「ISMS管理策運用規定」にて明確化	○	適合	
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 目的：供給者関係において、合意されたレベルの情報セキュリティを維持するため										
	供給者（外部の業者）に委託する場合に、守秘義務等を含む契約書、または覚書を取り交わしているか					●	契約書確認 (A社契約書)	○	適合	
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 目的：情報通信技術（ICT）製品及び情報通信技術（ICT）サービスのサプライチェーンに関連したものにおいても、情報セキュリティリスクを管理するため										
	ICTサービス及び製品に関して、情報セキュリティが確保できるように、供給者に要求しているか					●	契約書確認 (B社契約書)	○	適合	
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 目的：供給者との合意に沿って、合意されたレベルの情報セキュリティ及びサービス提供を維持するため										
	供給者（外部）のサービスの監査を年一回、もしくは必要に応じて行い、その結果を情報セキュリティ委員会にて報告を行って		●	●	●	●	営業部において、登録漏れ	△	観察	
	供給者（外部）が提供するサービスに変更があった際は、リスクを再評価し、必要に応じて手順等を見直し、その結果を情報セキュリティ委員会にて報告を行っているか	●					変更はなかった	○	適合	
5.23 クラウドサービス利用における情報セキュリティ 目的：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										
	どのようにして、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ているか		●	●	●	●	クラウドサービスの利用方針確認	○	適合	
	どのようにして、クラウドサービス利用におけるリスクは把握しているか		●	●	●	●	「リスクアセスメント結果表」にて明確化	○	適合	
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 目的：情報セキュリティ事象に関する伝達を含む、情報セキュリティインシデントへの迅速で、効果的で、一貫性があり、かつ秩序のある対応を確実にするため										
	情報セキュリティインシデントが発生した場合の手順と責任は明確か	●					「ISMS管理策運用規定」にて明確化	○	適合	
5.25 情報セキュリティ事象の評価及び決定 目的：情報セキュリティ事象の効果的な分類及び優先順位付けを確実にするため										
	ISMS管理責任者は、情報セキュリティ事象の評価及び決定を行い、その結果および指示事項を社内に伝達しているか	●					メール等で伝達 （2023.00.00伝達）	○	適合	
5.26 情報セキュリティインシデントへの対応 目的：情報セキュリティインシデントへの効率的かつ効果的な対応を確実にするため										
	情報セキュリティインシデントへの対応手順は明確か	●					「ISMS管理策運用規定」にて明確化	○	適合	
5.27 情報セキュリティインシデントからの学習 目的：将来のインシデントの起こりやすさ又はその影響を減らすため										
	情報セキュリティインシデントから得られた情報は、再発防止のための社員教育に役立てているか	●					セキュリティ教育実施 （2023.00.00実施）	○	適合	
5.28 証拠の収集 目的：懲戒処分及び法的処置の目的で、情報セキュリティインシデントに関連する証拠の一貫した効果的な管理を確実にするため										
	セキュリティインシデントの結果、法的処置がとられる可能性があると判断した場合は、記録、証拠を保全する手順があるか	●					「ISMS管理策運用規定」にて明確化	○	適合	
5.29 事業の中断・阻害時の情報セキュリティ 目的：事業の中断・阻害時に情報及び関連するその他の資産を保護するため										
	困難な状況（災害もしくは大事故時など）においても、情報セキュリティ及び情報セキュリティマネジメントを適切に維持管理できるように、組織で行うべきことは明確か	●					「事業継続計画書」にて明確化していた。	○	適合	
	「事業継続計画書」を作成し、社長の承認を得ているか	●					「事業継続計画書」にて明確化していた。	○	適合	
	「事業継続計画書」を検証し、評価しているか		●	●	●	●	法定停電の点検を計画していたが、必要な事前準備や事後対応等の確認は、一部、不明確であった。	△	観察	
8 技術的管理策 8.1 利用者エンドポイント機器 目的：ユーザーエンドポイントデバイスを使用することでもたらされるリスクから情報を保護するため										
	モバイル機器の利用を行う場合の方針は制定され、運用・実行されているか		●	●	●	●	「ISMS管理策運用規定」にて明確化	○	適合	
	盗み見やのぞき見防止のための対策はされているか		●	●	●	●	利用者確認実施	○	適合	
8.2 特権的アクセス権 目的：認可されたユーザー、ソフトウェアコンポーネント、サービスだけに特権アクセス権が与えられることを確実にするため										

規格項目等	チェック内容	ISMS管理責任者（ISMS事務局）	営業部門	○○部門	総務部門	システム課	コメント	有効性評価	総合評価結果	備考
	管理者権限の割当ては最小限とし、割当て者には責任を認識させ、厳重な管理を誓約させているか					●	利用者確認実施	○	適合	
8.3 情報へのアクセス制限 目的：情報及び関連するその他の資産への認可されたアクセスのみを確実にし、認可されていないアクセスを防止するため										
	認可された者だけがアクセスできるようなシステム及び業務用ソフトウェアは、適切に管理を行っているか					●	利用者確認実施	○	適合	
8.4 ソースコードへのアクセス 目的：認可されていない機能が入り込むことを防止し、意図しないまたは悪意のある変更を回避し、価値の高い知的財産の機密性を維持するため										
	プログラムソースコード（情報資産としてある場合）や開発ツール等へのアクセス管理は行っているか					●	アクセスはできないことを確認	○	適合	
8.5 セキュリティを保った認証 目的：ユーザー等の認証はセキュリティを保って認証することを確実にするため										
	許容失敗回数の制限や入力したパスワードは、マスキングして隠すなどセキュリティに配慮したログオン手順になっているか					●	利用者確認実施	○	適合	
8.6 容量・能力の管理 目的：情報処理施設、人的資源、オフィス及びその他の施設で必要とされる容量・能力の確保を確実にするため										
	システムの容量・能力の管理及びその予測を行っているか					●	管理記録確認 (2023.00.00管理記録)	○	適合	
8.7 マルウェアに対する保護 目的：情報及びその他の関連資産をマルウェアに対して保護することを確実にするため										
	個人貸与PCのウィルス対策機能が有効となっているか、パターン定義ファイルが最新のものになっているか		●	●	●	●	利用者確認実施	○	適合	
8.8 技術的ぜい弱性の管理 目的：技術的ぜい弱性の悪用を防止するため										
	常に業務用ソフトウェアのベンダーや、外部の専門機関が発する情報を、時機を失せずに取得し、自らが管理するシステムのぜい弱性の改善を行っているか					●	管理記録確認 (2023.00.00管理記録)	○	適合	
	情報システムが、当社の定めたセキュリティ基準に従って順守					●	システム課が日常業務の	○	適合	
8.9 構成管理 目的：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または誤った変更によって構成が変えられないことを確実にするため										
	どのようにして、ハードウェア（スマートフォン等含む）、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、レビューしているか					●	「ISMS管理策運用規定」にて明確化	○	適合	
	設定管理は適切か（変更・更新管理の手順はあるか、ネットワーク機器は初期設定のまま使用していないかなど）					●	「ISMS管理策運用規定」にて明確化	○	適合	
8.10 情報の削除 目的：取扱いに慎重を要する情報の不必要な漏洩を防止し、情報の削除に関する法律、規制及び契約上の要求事項を順守するため										
	どのようにして、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ているか					●	「ISMS管理策運用規定」にて明確化	○	適合	
8.24 暗号の使用 目的：事業上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、真正性または完全性を保護するための暗号の適切かつ効果的な使用を確実										
	暗号の利用方針を定め、周知しているか					●	「ISMS管理策運用規定」にて明確化	○	適合	
	暗号に使用する鍵は、適切に管理を行っているか					●	システム課で適切に管理	○	適合	
8.25 セキュリティに配慮した開発のライフサイクル 目的：情報セキュリティを、ソフトウェアやシステムのセキュリティに配慮した開発ライフサイクルにおいて設計し、実装することを確実にするため										
	セキュリティに配慮した開発のための方針は策定し、関係者に周知されているか					●	「ISMS管理策運用規定」にて明確化	○	適合	
8.26 アプリケーションセキュリティの要求事項 目的：アプリケーションを開発または取得する場合、すべての情報セキュリティ要求事項が特定され、対応することを確実にするため										
	アプリケーションを開発または取得する場合、情報セキュリティ要求事項の分析及び必要な要求事項の明確化を行っているか					●	「ISMS管理策運用規定」にて明確化	○	適合	
	不特定多数の人が利用するネットワーク（公衆ネットワーク）を利用する場合には、セキュリティ確保を確実にして利用を行っ					●	リスク周知実施	○	適合	
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 目的：情報システムが開発ライフサイクルにおいてセキュリティに配慮して設計・実装・運用されることを確実にするため										
	情報システム構築は、情報セキュリティの必要性とアクセスの必要性の均衡を保ちながら、全てのアーキテクチャ層（業務、データ、アプリケーション及び技術）において、設計・開発することを原則としているか					●	議事録確認 (2023.00.00)	○	適合	
8.28 セキュリティに配慮したコーディング 目的：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情報セキュリティのぜい弱性の数を減らすことを確実にするため										
	どのようにして、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ているか					●	「ISMS管理策運用規定」にて明確化	○	適合	
8.29 開発及び受入れにおけるセキュリティテスト 目的：アプリケーション等を運用環境に導入するときに、情報セキュリティ要求事項が満たされているか、妥当性を確認するため										
	セキュリティ機能の試験を、確実に、開発期間中に実施できるように、適切な監督、監視を行っているか					●	該当なし	－	－	
	業務用システムの新規導入及び改訂・更新する際、適切な受入試験を行っているか					●	該当なし	－	－	
8.30 外部委託による開発 目的：自社が要求する情報セキュリティ対策が、外部委託したシステム開発で実施されることを確実にする										
	外部委託によるソフトウェア開発を行う場合、セキュリティ要求事項を明確にし、外部委託業者の適切な監督、監視及びレビューは行っているか					●	該当なし	－	－	
8.31 開発環境、テスト環境及び本番環境の分離 目的：開発及びテスト環境による影響から運用環境とデータを保護するため										
	開発環境は、分離しているか					●	該当なし	－	－	
	セキュリティに配慮した開発環境は確立されているか					●	該当なし	－	－	
8.32 変更管理 目的：変更を実行するときに情報セキュリティを維持するため										
	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、情報セキュリティ委員会での審議を経て、経営陣の承認を得て実施しているか	●				●	マネジメントレビューで実施 (2023.00.00、MR議事録)	○	適合	
	情報システムの変更に際しては、変更の妥当性の検証を行い、変更に関する記録を残しているか					●	作業日報確認 (2023.00.00日報)	○	適合	
	オペレーティングシステムを含むプラットフォーム（情報システムの基盤）の変更に際しては、情報の機密性、完全性、可用性を考慮し、その上で動作する業務ソフトウェアへの影響やシステム全体を検証した上で実施しているか					●	作業日報確認 (2023.00.00日報)	○	適合	
	市販のソフトウェアの変更は、ベンダーが提供する修正プログラムによるものを除き、行っていないか					●	作業日報確認 (2023.00.00日報)	○	適合	

規格項目等	チェック内容	ISMS管理責任者（ISMS事務局）	営業部門	○○部門	総務部門	システム課	コメント	有効性評価	総合評価結果	備考
8.33 テスト用情報 目的：テストの適切な実施、及びテストに使用された運用情報の保護を確実にするため										
	テストデータは保護し、管理を行っているか					●	該当なし	ー	ー	
8.34 監査におけるテスト中の情報システムの保護 目的：監査やその他の保証活動が運用システムや業務プロセスに与える影響を最小限に抑えるため										
	運用システムの点検を伴う監査要求事項及び活動は、運用システムや業務プロセスの中断のリスクを最小限に抑えるために、慎重に計画し、実行しているか					●	法定点検の事例検証 (2023.00.00日報)	○	適合	