適用宣言書

関連文書 ： COM-B10 リスクマネジメント管理規定

2025.03.25作成

※適用性：採：適用する　否：適用しない

管理策			採否	採否理由	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、関連する要員関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。	採	マネジメントシステムの要求事項	TMS基本方針 個人情報保護方針 TMS運用規定 7.1
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・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。	採	マネジメントシステムの要求事項	TMS運用規定 2.2
5.3	職務の分離	相反する職務及び相反する責任範囲は、分離なければならない。	採	マネジメントシステムの要求事項	システム管理規定 2.3
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、全ての要因に要求しなければならない。	採	マネジメントシステムの要求事項	教育及び人的管理規定 4.1
5.5	関係当局との連絡	組織は、関係当局との適切な連絡体制を確立し、維持しなければならない。	採	マネジメントシステムの要求事項	TMS運用規定 4.1
5.6	専門組織との連絡	情報セキュリティを推進するための責任と権限を定める。	採	マネジメントシステムの要求事項	TMS運用規定 4.1
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。	採	リスク対応	システム利用・運用規定 1.2 リスクマネジメント管理規定 5.1① IPA情報セキュリティ10大脅威
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。	採	マネジメントシステムの要求事項	TMS運用規定 4.2
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。	採	リスク対応	リスクマネジメント管理規定 3.1
5.10	情報及び関連する資産の許容範囲	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。	採	リスク対応	ISMS運用マニュアル 4.2
5.11	資産の取扱い	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。	採	リスク対応	ISMS運用マニュアル 5.2
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に従って、分類しなければならない。	採	リスク対応	ISMS運用マニュアル 5.1
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。	採	リスク対応	ISMS運用マニュアル 5.1
5.14	情報転送	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。	採	リスク対応	システム利用・運用規定 6.2
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およ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。	採	リスク対応	アクセス管理規定 2.1
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。	採	リスク対応	アクセス管理規定 3
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。	採	リスク対応	アクセス管理規定 3
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。	採	リスク対応	アクセス管理規定 3.2 ／ 7.1
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。	採	マネジメントシステムの要求事項	ISMS運用マニュアル 3.1
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。	採	マネジメントシステムの要求事項	ISMS運用マニュアル 3.1
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。	採	マネジメントシステムの要求事項	ISMS運用マニュアル 3.1(5)
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。	採	マネジメントシステムの要求事項	購買及び外部提供者管理規定 5.2 ／ 5.3 ／ 5.4
5.23	クラウドサービス利用時の情報セキュリティ	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。	採	マネジメントシステムの要求事項	ISMS運用マニュアル 3.1(5)
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。	採	リスク対応	不適合及び緊急事態管理規定 3
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。	採	リスク対応	不適合及び緊急事態管理規定 3.3
5.26	情報セキュリティインシデントの対応	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。	採	リスク対応	不適合及び緊急事態管理規定 3.4

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。	採	リスク対応	不適合及び緊急事態管理規定 6.1
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。	採	リスク対応	不適合及び緊急事態管理規定 3.10
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。	採	リスク対応	事業継続管理規定 3.1
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。	採	リスク対応	事業継続管理規定 5
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。	採	マネジメントシステムの要求事項	適合性管理規定 2.6
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。	採	法的要求事項	適合性管理規定 2.2
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。	採	マネジメントシステムの要求事項	適合性管理規定 2.3
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、適応される法令、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。	採	法的要求事項	適合性管理規定 2.4
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。	採	マネジメントシステムの要求事項	TMS運用規定 7.5
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。	採	マネジメントシステムの要求事項	適合性管理規定 3.1
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。	採	リスク対応	システム管理規定 2.1
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、適応される法令、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。	採	リスク対応	教育及び人的管理規定 2
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。	採	リスク対応	教育及び人的管理規定 3
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、定常な更新を受けなければならない。	採	マネジメントシステムの要求事項	教育及び人的管理規定 4.2
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。	採	リスク対応	教育及び人的管理規定 5 就業規則 第6章
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。	採	リスク対応	教育及び人的管理規定 6
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、要員及びその他の利害関係者が署名しなければならない。	採	リスク対応	TMS運用規定 6.2 機密保持契約書
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。	採	リスク対応	アクセス管理規定 8.1 テレワーク勤務規定
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。	採	リスク対応	不適合及び緊急事態管理規定 3.7/3.8
7. 物理的管理策					
7.1	物理的セキュリティ境界線	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。	採	リスク対応	物理的・環境的管理規定 2.1
7.2	物理的入退	セキュリティを保つべき領域は、適切な入退管理及びアクセス場所によって保護しなければならない。	採	リスク対応	物理的・環境的管理規定 2.2
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、実施しなければならない。	採	リスク対応	物理的・環境的管理規定 2.3
7.4	物理的なセキュリティ監視	施設は、許可していない物理的アクセスについて継続的に監視しなければならない。	採	リスク対応	物理的・環境的管理規定 2.2
7.5	物理的及び環境的な脅威からの保護	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な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。	採	リスク対応	物理的・環境的管理規定 2.4
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。	採	リスク対応	物理的・環境的管理規定 2.5
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。	採	リスク対応	物理的・環境的管理規定 3.8

7.8	機器の設置及び保護	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。	採	リスク対応	物理的・環境的管理規定 3.1
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。	採	リスク対応	物理的・環境的管理規定 3.5
7.10	記憶媒体	記録媒体は、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。	採	リスク対応	システム利用・運用規定 5.1
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。	採	リスク対応	物理的・環境的管理規定 3.2
7.12	ケーブル配線のセキュリティ	電源ケーブル、データ転送ケーブ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。	採	リスク対応	物理的・環境的管理規定 3.3
7.13	装置の保守	装置は、情報の可用性及び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。	採	リスク対応	物理的・環境的管理規定 3.4
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。	採	リスク対応	物理的・環境的管理規定 3.6
8. 技術的管理策					
8.1	ユーザー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、処理されている情報、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。	採	リスク対応	システム利用・運用規定 5.1 アクセス管理規定 5
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。	採	リスク対応	アクセス管理規定 3.2
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。	採	リスク対応	アクセス管理規定 7.1
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。	採	リスク対応	システムの開発および保守管理規定 4.3
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。	採	リスク対応	アクセス管理規定 7 / 7.1 システム管理規定 8 / 8.1
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。	採	リスク対応	システム管理規定 5.1
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。	採	リスク対応	システム管理規定 6 システム利用・運用規定 2
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。	採	リスク対応	システムの開発および保守管理規定 6.1
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。	採	リスク対応	システム利用・運用規定 1.2
8.10	情報の削除	情報システム、装置又はその他の記録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。	採	リスク対応	システム利用・運用規定 5.2 個人情報保護マニュアル A.3.4.4.6
8.11	データマスキング	データマスキングは、適応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、並びに事業の要求事項に従って利用しなければならない。	採	リスク対応	システム利用・運用規定 6.1(10) 個人情報保護マニュアル A.3.4.3.2
8.12	データ漏洩防止	データ漏洩防止策を，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せない。	採	リスク対応	システム利用・運用規定 6.1
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。	採	リスク対応	システム管理規定 7.1
8.14	情報処理施設の冗長性	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。	採	リスク対応	事業継続管理規定 6
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情報を取得し、保持し、保護し、分析しなければならない。	採	リスク対応	システム管理規定 10.1
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。	採	リスク対応	システム管理規定 10
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。	採	リスク対応	システム管理規定 11
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。	採	リスク対応	アクセス管理規定 6.3
8.19	運用システムに関わるソフトウエアの導入	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。	採	リスク対応	システムの開発および保守管理規定 4.1
8.20	ネットワークのセキュリティ	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。	採	リスク対応	システム管理規定 8
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。	採	リスク対応	システム管理規定 8.3
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。	採	リスク対応	アクセス管理規定 5.2
8.23	ウエブフィルタリング	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、外部ウエブサイトへのアクセスを管理しなければならない。	採	リスク対応	アクセス管理規定 5.3

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。	採	リスク対応	システム管理規定 3.2
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を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。	採	リスク対応	システムの開発および保守管理規定 5.1
8.26	アプリケーションのセキュリティ要求事項	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。	採	リスク対応	システム利用・運用規定 7.1
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。	採	リスク対応	システムの開発および保守管理規定 5.5
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。	採	リスク対応	システムの開発および保守管理規定 5.9
8.29	開発及び受入れ時の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。	採	リスク対応	システム管理規定 5.2
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、レビューしなければならない。	採	マネジメントシステムの要求事項	システムの開発および保守管理規定 5.7
8.31	開発環境、試験環境及び運用環境の分離	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。	採	リスク対応	システムの開発および保守管理規定 3
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。	採	リスク対応	システムの開発および保守管理規定 5.2
8.33	試験情報	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。	採	リスク対応	システムの開発および保守管理規定 4.2
8.34	監査試験時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。	採	マネジメントシステムの要求事項	システムの開発および保守管理規定

【2024.03.01】