配 付 番 号 ：

管　理　区　分
管　理　文　書

文書番号	ISMS-A-04
制 定 日	2023.10.01
改 訂 日	
改訂番号	1

※購入希望の場合は、https://www.iso-mi.com/
ISO27001:2022 の取得及び更新に必須となる管理策に対応した文書のサンプルです。
修正可能なワードファイルで提供しています。

ISMS管理策運用規定（抜粋版）

ＪＩＳ Ｑ ２７００１：２０２３ 適用

（ ＩＳＯ/ＩＥＣ ２７００１：２０２２ ）

承　認	作　成

株式会社　サンプル

ISMS 管理策運用規定	制定日 2023.10.01	文書番号 ISMS-A-04
	改訂日	改訂番号 1

目　　次

Ⅰ．組織的管理策 …… P5
5.1　情報セキュリティのための方針群 …… P5
5.2　情報セキュリティの役割及び責任 …… P5
5.3　職務の分離 …… P5
5.4　管理層の責任 …… P5
5.5　関係当局との連絡 …… P5
5.6　専門組織との連絡 …… P6
5.7　脅威インテリジェンス …… P6
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 …… P6
5.9　情報及びその他の関連資産の目録 …… P6
5.10 情報及びその他の関連資産の許容される利用 …… P6
5.11 資産の返却 …… P7
5.12 情報の分類 …… P7
5.13 情報のラベル付け …… P8
5.14 情報の転送 …… P8
5.15 アクセス制御 …… P9
5.16 識別情報の管理 …… P10
5.17 認証情報 …… P10
5.18 アクセス権 …… P11
5.19 供給者関係における情報セキュリティ …… P11
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 …… P12
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 …… P13
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 …… P13
5.23 クラウドサービス利用における情報セキュリティ …… P14
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 …… P15
5.25 情報セキュリティ事象の評価及び決定 …… P17
5.26 情報セキュリティインシデントへの対応 …… P17
5.27 情報セキュリティインシデントからの学習 …… P17
5.28 証拠の収集 …… P18
5.29 事業の中断・阻害時の情報セキュリティ …… P18
5.30 事業継続のための ICT の備え …… P21
5.31 法令、規制及び契約上の要求事項 …… P21
5.32 知的財産権 …… P22
5.33 記録の保護 …… P22

5.34 プライバシー及び個人識別可能情報（PII）の保護 ····· P22
5.35 情報セキュリティの独立したレビュー ····· P22
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 ····· P23
5.37 操作手順書 ····· P23

Ⅱ．人的管理策 ····· P24
6.1 選考 ····· P24
6.2 雇用条件 ····· P24
6.3 情報セキュリティの意識向上、教育及び訓練 ····· P24
6.4 懲戒手続 ····· P24
6.5 雇用の終了又は変更後の責任 ····· P24
6.6 秘密保持契約又は守秘義務契約 ····· P24
6.7 リモートワーク ····· P25
6.8 情報セキュリティ事象の報告 ····· P25

Ⅲ．物理的管理策 ····· P26
7.1 物理的セキュリティ境界 ····· P26
7.2 物理的入退 ····· P26
7.3 オフィス、部屋及び施設のセキュリティ ····· P26
7.4 物理的セキュリティの監視 ····· P26
7.5 物理的及び環境的脅威からの保護 ····· P27
7.6 セキュリティを保つべき領域での作業 ····· P27
7.7 クリアデスク・クリアスクリーン ····· P27
7.8 装置の設置及び保護 ····· P28
7.9 構外にある資産のセキュリティ ····· P28
7.10 記録媒体 ····· P28
7.11 サポートユーティリティ ····· P28
7.12 ケーブル配線のセキュリティ ····· P28
7.13 装置の保守 ····· P29
7.14 装置のセキュリティを保った処分又は再利用 ····· P29

Ⅳ．技術的管理策 ····· P30
8.1 利用者エンドポイント機器 ····· P30
8.2 特権的アクセス権 ····· P30
8.3 情報へのアクセス制限 ····· P30
8.4 ソースコードへのアクセス ····· P30
8.5 セキュリティを保った認証 ····· P30
8.6 容量・能力の管理 ····· P31

8.7　マルウェアに対する保護 …… P31
8.8　技術的ぜい弱性の管理 …… P31
8.9　構成管理 …… P31
8.10 情報の削除 …… P31
8.11 データマスキング …… P32
8.12 データ漏えいの防止 …… P32
8.13 情報のバックアップ …… P32
8.14 情報処理施設・設備の冗長性 …… P32
8.15 ログ取得 …… P32
8.16 監視活動 …… P33
8.17 クロックの同期 …… P33
8.18 特権的なユーティリティプログラムの使用 …… P33
8.19 運用システムへのソフトウェアの導入 …… P33
8.20 ネットワークセキュリティ …… P33
8.21 ネットワークサービスのセキュリティ …… P33
8.22 ネットワークの分離 …… P33
8.23 ウェブ・フィルタリング …… P34
8.24 暗号の使用 …… P34
8.25 セキュリティに配慮した開発のライフサイクル …… P34
8.26 アプリケーションセキュリティの要求事項 …… P35
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 …… P35
8.28 セキュリティに配慮したコーディング …… P36
8.29 開発及び受入れにおけるセキュリティテスト …… P36
8.30 外部委託による開発 …… P36
8.31 開発環境、テスト環境及び本番環境の分離 …… P36
8.32 変更管理 …… P37
8.33 テスト用情報 …… P38
8.34 監査におけるテスト中の情報システムの保護 …… P38

改訂歴表

ISMS 管理策運用規定	制定日 2023.10.01	文書番号 ISMS-A-04
	改訂日	改訂番号 1

Ⅰ　組織的管理策

1　情報セキュリティのための方針群（5.1）

1.1　情報セキュリティ方針群

ISMS 事務局は、**「情報セキュリティ基本方針」**を始めとする情報セキュリティに関わる固有の方針群は社長の承認を得て、発行し、全従業員及び関連する外部関係者に公表し、通知する。

1.2　情報セキュリティ方針群のためのレビュー

ISMS 事務局は、年に一度（マネジメントレビュー時）、または事業上の重大な変化が発生したときに、**「情報セキュリティ基本方針」**を始めとする固有の方針群が、適切、妥当及び有効であるかレビューし、社長の承認を得る。

2　情報セキュリティの役割及び責任（5.2）

「ISMS マニュアル」にて、情報セキュリティの役割と責任を明確にする。具体的な従業員に関しての役割及び責任は、**「就業規則」**および**「誓約書」**によって、文書化することを確実にする。

3　職務の分離（5.3）

通信及び運用管理（情報システムの操作とその操作ログの取得等の管理）において、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るようにする。実施が難しい場合には、上長による監督等を実施する。

4　管理層の責任（5.4）

管理層は、組織の方針及び手順に従った情報セキュリティの適用を、すべての従業員及び契約相手に要求する。

5　関係当局との連絡（5.5）

ISMS 事務局は、当社 ISMS の円滑な運用、緊急時の対応を図るため、下記の機関との連絡体制を確立する。　→　*具体的な連絡先は、一覧表にしておく*

(1) 社内他組織（適用範囲外）
(2) 関連会社
(3) 行政（自治体）
(4) 業界団体事務局
(5) 警察
(6) 消防署
(7) 通信会社（NTT など）
(8) プロバイダー

6　専門組織との連絡（5.6）

システム管理責任者は、組織のシステム、ネットワークを安全な状態に保つため、下記の専門組織から情報収集を行い、適切な処置を講じる。　*→具体的な連絡先は、一覧表にしておく*

(1) JIPDEC（日本情報経済社会推進協会）
(2) IPA（情報処理推進機構）
(3) 主要ソフト（OS など）ベンダー
(3) マルウェアソフトベンダー
(4) その他（JPCERT、JVN 等）

7　脅威インテリジェンス（5.7）

当社は、適切なリスクの低減処置を講じることが出来るように、IPA（情報処理推進機構）、JPCERT コーディネーションセンター、JVN（脆弱性対策情報ポータルサイト）等の外部の脅威インテリジェンス（知見）を活用して、脅威インテリジェンスを構築する。

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（5.8）

ISMS 事務局は、社内の活動（開始日と終了日がある特定の活動）においても、情報セキュリティの取り込みを確実にするために、各プロジェクト責任者に、機密文書漏えい防止などの適切な情報セキュリティ対策の実施を命じる。

9　情報及びその他の関連資産の許容される利用（5.9）

9.1　資産目録

適用範囲内における情報資産は、**「情報資産台帳」**において特定する。**「情報資産台帳」**に登録されていない情報資産を新たに入手･作成した場合、あるいは登録されている情報資産に変動があった場合は、該当担当者もしくは該当部門長は、その内容を**「情報資産整理表」（非管理文書）**に記入し、ISMS 事務局に提出し、ISMS 管理責任者の承認を得る。

9.2　資産の管理責任者

情報資産の管理責任者は、**「情報資産台帳」**にて明示し、変更が生じた場合には、該当担当者もしくは該当部門長が、**「情報資産整理表」（非管理文書）**に記入し、ISMS 事務局に提出し、ISMS 管理責任者の承認を得る。

１０　情報及びその他の関連資産利用の許容範囲（5.10）

10.1　資産利用の許容範囲

情報資産利用の許容範囲は、**「情報資産台帳」**にて明示し、変更が生じた場合には、該当担当者もしくは該当部門長が、**「情報資産整理表」（非管理文書）**に記入し、ISMS 事務局に提出し、ISMS 管理責任者の承認を得る。

10.2　資産の取扱い

該当部門は、**「情報資産台帳」**及び下記に従って適切に、取扱うこととする。

【帳票類】

区分	極秘（資産価値 4）	部外秘（資産価値 3）	社外秘（資産価値 2）
保管	鍵付き収容場所（キャビネット等）に常時施錠。	鍵付き収容場所（キャビネット等）所属長不在時は施錠。	保管される室内が施錠される場合を除き、鍵付き収容場所。
持ち出し（移送）	原則持ち出し不可	所属長の許可を得ること。第三者に公開・譲渡することは禁止	所属長の許可を得ること
利用（アクセス）権限	限定された担当者かつ所属部門長が許可した者	部門長以上の役職者および所属部門員	従業員のみ
コピー	業務手続きを除き不可	所属長の許可を得ること	従業員の判断で可能
ＦＡＸ	行わない	行わない	行わない
廃棄	シュレッダー、または契約業者による廃棄処理。	シュレッダー、または契約業者による廃棄処理。	シュレッダーで廃棄処理

【電子データ】

区分	極秘（資産価値 4）	部外秘（資産価値 3）	社外秘（資産価値 2）
保管	アクセス制限のあるフォルダ	アクセス制限のあるフォルダ	指定のフォルダ
持ち出し（移送）	原則持ち出し不可	所属長の許可を得ること。第三者に公開・譲渡することは禁止	所属長の許可を得ること
利用（アクセス）権限	限定された担当者かつ所属部門長が許可した者	部門長以上の役職者および所属部門員	従業員のみ
コピー（複製）	業務手続きを除き不可	所属長の許可を得ること	従業員の判断で可能
メール	添付は行わない	添付は行わない	所属長の許可を得ること
削除	契約業者による廃棄処理。専用ソフトによる消去	契約業者による廃棄処理。専用ソフトによる消去	契約業者による廃棄処理。専用ソフトによる消去

１１　資産の返却（5.11）

人事担当者又は該当担当者は、雇用、契約の終了・変更時に、該当する従業員又は外部利用者から、従業員証、社用名刺、施設入退室カード、貸与 PC、スマートフォンをはじめ、貸与した情報資産の返却を確実に行う。

１２　情報の分類（5.12）

当社は、情報の分類において、下記に基づき、機密性、完全性、可用性及び関連する利害関係者からの要求事項を考慮する。

(1) 情報の共有や制限、情報の完全性の保護、利用可能性の確保といった業務上のニーズ

(2) 情報の機密性、完全性、利用可能性に関する法的要求事項

(3) 情報のライフサイクルを通じた価値、取り扱いに慎重を要する度合い及び重要性の変化

１３　情報のラベル付け（5.13）

情報のラベリングは、5.12 で確立された分類体系を反映し、下記に基づき実施する。

(1) 物理的なラベル付け

(2) ヘッダやフッタに付ける

(3) メタデータ（データを表す属性や関連する情報の記述）

(4) 電子透かし

(5) ゴムスタンプ

１４　情報の転送（5.14）

14.1　情報転送の方針及び手順

情報の転送については、下記の項目を確実に行う。

(1) 外部組織から機密情報を預かった場合は、情報名、当社の責任者、利用期限、返却/廃棄方法を明示し、記録する。

(2) 電子メールの取り扱いに関しては、利用方法を明示する。*(参照:14.3)*

(3) 公共の場（不特定の人がいる電車内や飲食店等）や狭い空間内（エレベーター内等）では、権限のない人に聞かれてしまう可能性があるため、顧客情報等の機密性のある情報の会話をしてはならない。

14.2　情報転送に関する合意

該当担当者は、当社の業務を委託する場合はもとより、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、合意する。

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（5.24）

情報セキュリティインシデントが発生した場合、下記に従った対応を行う。

(1) コンピュータマルウェア感染時の対応

	対応内容
１．感染発覚時の対応	・発見者は、感染等が認められたら、直ちに端末をネットワークから遮断し、直ちにシステム担当者に連絡をとる。システム担当者は、下記を行う。 ①被害拡大阻止の対応（当座の処置） ②システム管理責任者及び ISMS 管理責任者へ連絡
２．確認と対応	１．システム管理責任者は、対応の指示をシステム担当者に行い、ISMS 管理責任者に状況報告を行う。マルウェアが急速に広く伝播する恐れがある場合には、必要な対応を迅速に関係者へ通知（周知）を行う。 ２．利用者は、感染等の有無に関わらず、怪しいメールは決して開かない。感染の恐れがある端末では、メールや Web の閲覧を行わない。
	３．感染したメールが外部に送信された場合、送信した先方に、送信者は電話などにより連絡し、感染の拡大を防止する。
	４．システム管理責任者は、感染端末のメール利用について、利用者アカウントの停止、および、端末登録の停止を行う。
	５．システム管理責任者は、当該端末の復旧対策などは、応急処置対応を終えてから着手する。
３．再発防止対策	・ISMS 管理責任者は、ISMS 推進委員会において協議を行い、再発防止対策を決定し、関係者に指示する。
４．報告書の作成	・システム管理責任者は、**「セキュリティインシデント報告書」**を作成し、ISMS 管理責任者に提出する。

(2) 不正アクセス時の対応

	対応内容
１.不正アクセス発覚時の対応	・発見者は、不正アクセスが認められたら、直ちにシステム管理責任者に連絡をとる。
２．確認と対応	・連絡を受けたシステム管理責任者は、対応に着手すると共に、ISMS 管理責任者に連絡を行い、下記を考慮して、必要な対応を迅速に関係者へ通知を行う。 ①不正アクセスの有無　②情報の保存 ③調査の実施　④復旧対策
３．再発防止対策	・ISMS 管理責任者は、ISMS 推進委員会において協議を行い、再発防止対策を決定し、関係者に指示する。
４．報告書の作成	・システム管理責任者は、**「セキュリティインシデント報告書」**を作成し、ISMS 管理責任者に提出する。

(3) サービス停止時（システム障害時）の対応

	対応内容
１．サービス停止時の対応	・発見者は、サービス停止が認められたら、直ちにシステム管理責任者に連絡をとる。
２．確認と対応	・連絡を受けたシステム管理責任者は、対応に着手すると共に、ISMS 管理責任者に連絡を行い、下記を考慮して、必要な対応を迅速に関係者へ通知を行う。 ①委託業者等への連絡 ②調査の実施 ③復旧対策
３．再発防止対策	・ISMS 管理責任者は、ISMS 推進委員会において協議を行い、再発防止対策を決定し、関係者に指示する。
４．報告書の作成	・システム管理責任者は、**「セキュリティインシデント報告書」**を作成し、ISMS 管理責任者に提出する。

(4) 機密情報の漏えい・流出・盗難発覚時の対応

	対応内容
１．発覚時の対応	・通報を受けた者及び発見した者は、下記の事項を実施する。 ①被害拡大阻止の対応（当座の処置） ②ISMS 管理責任者に連絡
２．確認と対応	１．連絡を受けた ISMS 管理責任者は、社長に連絡する。 ２．ISMS 管理責任者は、社長及び関係責任者と対応を協議し、関係者に指示を行う。
	３．指示を受けた関係者は、下記の事項を実施する。 ①状況の確認 →漏洩した情報資産の保管場所、使用者を特定する。 ②原因の追究 →システム管理責任者へサーバーの該当フォルダに対するアクセス権限設定の再確認を依頼し、不審点があれば究明する。 →疑わしいハードウェア、ソフトウェアがあれば、その設定を確認し、原因を追及、除去する。 ③被害拡大阻止の完了 →スマートフォンの紛失、ノート PC の紛失、資料ファイルの紛失、それらの盗難などにより機密漏洩が危惧される場合は、その持出し先、保管状況を調査し、可能な限り回収に努める。 ④ISMS 管理責任者に報告（進捗状況を随時報告）
３．外部への対応	社長又は ISMS 管理責任者は、必要に応じて、下記の事項への対応を行う。 ①顧客等（利害関係者）への対応 ②行政（経済産業省等）への対応 ③マスコミへの対応　　→ プレスリリースを作成し、HP に掲載
	社長又は ISMS 管理責任者は、必要に応じて、経過報告を HP 等にて行う。
４．再発防止対策	・ISMS 管理責任者は、ISMS 推進委員会において協議を行い、再発防止対策を決定し、関係者に指示する。
５．報告書の作成	・ISMS 管理責任者は、**「セキュリティインシデント報告書」**を作成し、社長に提出する。

Ⅱ　人的管理策

1　選考（6.1）

人事採用担当者は、個人情報保護法、各種ガイドライン、倫理に反しないことを確実にする。また、人事採用担当者は、採用予定者が情報セキュリティに関するその役割を果たすために、必要な力量を備えていることの確認を行う。また、雇用中にも適格かつ適切でありつづけることを確実にする。

2　雇用条件（6.2）

人事採用担当者は、採用予定者に対して、情報セキュリティに関する各自の責任を自覚させるために、当社の**「服務規程」**を説明し、**「機密保持誓約書」**に署名、提出させる。

3　情報セキュリティの意識向上、教育及び訓練（6.3）

ISMS管理責任者は、すべての従業員及び、関係する場合には、契約相手に、**「ISMSマニュアル7.2.2」**に規定する自覚教育、手順書教育を実施する。

4　懲戒手続（6.4）

情報セキュリティ違反を犯した従業員に対して、当社の**「服務規程」**に定める懲戒規定に則り処罰する。また、情報セキュリティに関する優れた行動をとった従業員に対しては、ISMS 推進委員会の審議の上、報償を行う。

5　雇用の終了又は変更後の責任（6.5）

管理部門は、すべての従業員に対して、雇用の終了又は変更の実施に対する責任及び義務を明確に定め、社長の承認を得て、その対応を確実に行う。

6　秘密保持契約又は守秘義務契約（6.6）

ISMS 推進委員会は、他部門の協力を得て、秘密保持契約又は守秘義務契約の特定を行い、レビューし、必要に応じて、見直す。具体的には、下記の項目に留意して行う。

(1) 保護される秘密情報の定義
(2) 秘密保持契約の有効期間
(3) 契約終了時に要求する処置
(4) 認可されていない情報開示を避けるための、署名者の責任及び行為
(5) 企業秘密及び知的財産権の所有権、並びにこれらの秘密情報の保護との関連
(6) 秘密情報の許可された利用範囲、及び情報を利用する署名者の権利
(7) 秘密情報に関する行為の監査及び監視の権利
(8) 認可されていない開示又は秘密情報漏えいの、通知及び報告のプロセス

Ⅲ　物理的管理策

1　物理的セキュリティ境界（7.1）

セキュリティエリアを下記の 3 段階に設定し、**「セキュリティエリア図」**で示す。

エリア	領域の内容
セキュリティエリア 1	来訪者が従業員の同行なしに出入りできる領域
セキュリティエリア 2	当社従業員及び従業員が同行した来訪者のみ出入りできる領域
セキュリティエリア 3	当社従業員の中で認可された者だけが出入りできる領域

2　物理的入退（7.2）

2.1　物理的入退管理策

セキュリティ対策が必要な施設への入退館は、下記の項目を確実にする。

(1) 建物入り口は、セキュリティキーと暗証番号により施錠する。

(2) セキュリティキーは管理部門責任者が認可した従業員にのみ貸与する。セキュリティ管理責任者はセキュリティキーを貸与した従業員を記録する。

(3) セキュリティキーを貸与された者は、セキュリティキーの紛失、盗難に注意を払い責任を持って保管しなければならない。また他人に貸与してはならない。

2.2　受渡場所

来訪者との打ち合わせ、及び宅配便、事務用品の納品など、外部業者との貨物の受取りは、原則として、前項 7.1 で設定したセキュリティエリア 1 で実施する。

また、資料、媒体などの送信物、受信物は前項 7.1 に示すセキュリティエリア 1 内に放置しないこととする。

3　オフィス、部屋及び施設のセキュリティ（7.3）

ISMS 事務局は、目的・用途に照らし合わせて、当該建物・部屋に具備するべき物理的セキュリティ条件を明確にし、ISMS 推進委員会での検討を経て、ISMS 管理責任者の承認を得る。

4　物理的セキュリティの監視（7.4）

4.1　一般

認可されていない物理的アクセスを検知し、抑止するために、監視カメラなどのビデオ監視システムや侵入者アラームを設置し、物理的なアクセスの監視を行う。

Ⅳ　技術的管理策

1　利用者エンドポイント機器（8.1）

従業員は、ノート PC 等のモバイル機器の利用を行う場合は、下記の項目を確実に行う。

(1) 社外へ持ち出し可能なモバイル機器は、会社が認めたモバイル機器に限定する。

(2) 盗み見の危険を避けるため、喫茶店や電車内等での公共の場所での使用を禁止する。

(3) 部外秘以上の情報を PC に格納して持ち出す場合は、暗号化する。

(4) 社外に持ち出し時及び持ち出し期間中は、マルウェア定義パターンファイルが最新になっていることを確認する。

(5) 社外で使用したモバイル機器を社内ネットワークに接続する場合は、接続前にマルウェアチェックを実施する。

2　特権的アクセス権（8.2）

管理部門責任者は、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るようにする。

3　情報へのアクセス制限（8.3）

システム管理責任者は、認可された者だけがアクセスできるように管理を行う。また、取扱いに慎重を要するシステムは、利用者がアクセスできるデータを制御し、物理的又は論理的なアクセス制御を行う。

4　ソースコードへのアクセス（8.4）

システム管理責任者は、プログラムソースコード（情報資産としてある場合）へのアクセス管理を行い、セキュリティが保たれた環境で保持する。

5　セキュリティを保った認証（8.5）

セキュリティに配慮したログオンにおいて、下記の事項を行う。

(1) 非認可利用者の助けとなる表示はしない。

(2) 許容失敗回数を制限する。(3 回まで)

(3) 入力したパスワードは、記号でパスワードの文字を隠す。

(4) 業務用システムへのログオン状態で、ログオン PC から一定時間何のアクセスもない場合、利用者が離席したと見なし、サーバー側から自動的にログオフさせる。

(5) 機密性の高い業務用システムには、必要に応じ、運用時間を定める。

３２　変更管理（8.32）

32.1　一般

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、ISMS 推進委員会での審議を経て、社長の承認を得て実施する。

32.2　システムの変更管理手順

システム管理責任者は、開発の全ての段階からその後の全ての保守業務において、システム、アプリケーション及び製品の完全性及び可用性を確実にするために、情報システムの変更に際しては下記の事項を順守する。

(1) 情報システムを変更する前に、変更の妥当性の検証を行い、システム管理責任者の承認を得る。またシステムの利用者に対し変更を周知する。

(2) 情報システムの変更に関する記録を残すこと。

32.3　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

システム管理責任者は、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する。

32.4　パッケージソフトウェアの変更に対する制限

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、行わない。また、ベンダーが提供する修正ソフトをインストールする場合は、システム管理責任者は、業務用ソフトウェアへの影響を検証する。

３３　テスト用情報（8.33）

システム管理責任者は、下記の事項を考慮し、テストデータを保護し、管理を行う。

(1) テストに使用するデータは、認識できるようにその名前にテストデータであることを表示する。

(2) 実際の運用データを試験に使用することは避ける。やむをえず使用する場合には、その内容に含まれる個人情報及び顧客情報を削除、修正し使用する。

(3) やむをえず実際の運用データを試験に使用する際には、使用前に ISMS 管理責任者の承認を得る。また、テスト終了後に、削除の旨を通知する。

(4) テストデータは、テスト完了後直ちに削除する。

３４　監査におけるテスト中の情報システムの保護（8.34）

運用システムの点検を伴う監査要求事項及び活動は、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、テストを実施する側と管理者との間で合意して、実行する。

ISMS 管理策運用規定	制定日 2023.10.01	文書番号 ISMS-A-04
	改訂日	改訂番号 1

改 訂 歴 表

改訂番号	改 訂 日 付	内　　容	作成	承認
1	2023.10.01	制定	○○	●●