自治体情報システムα´モデル採用に係る外部監査業務仕様書

1. 委託業務名

自治体情報システムα´モデル採用に係る外部監査業務

2. 業務の目的

本業務は、本市情報システムのα´モデル導入前に外部監査を行うものである。

3. 履行場所

主な履行場所は五島市役所本庁舎（五島市市福江町1番1号）とする。

なお、来庁又は本市職員の立会を要しない作業については、この限りではない。

4. 業務委託期間

(1) 契約期間

契約締結日翌日から令和8年2月28日まで

(2) 監査スケジュール

前項契約期間のうち、監査の実施日は協議の上決定する。ただし、5(3)で示すα´モデルの「監査報告書」「外部監査の実施に係る報告様式」の提出期限は令和8 年1 月中旬とする。

5. 業務委託内容

本市情報システムのα´モデル採用に関する監査。

(1) 監査計画の作成

監査に係る具体的な実施内容、実施体制、実施工程等を明記した監査実施計画書を本市と協議・調整の上策定すること。

(2) 外部監査の実施

監査項目には、別紙 1「α´モデル採用自治体における監査項目一覧」で指定する以下の項目を含むこととし、監査資料のレビュー及び監査対象課へのヒアリング等により実施する。

- α´/β/β´モデル共通の監査項目

α´/β/β´モデルの採用にあたり必須となる、総務省「地方公共団体における情報セキュリティ監査に関するガイドライン（令和 6 年 10 月版)」(以下、「監査ガイドライン」という。）における組織的・人的対策に係る監査項目（23 項目）

- α´モデル固有の監査項目

監査ガイドライン「3.11.　α´モデルを採用する場合の追加監査項目」(17 項目)

(3) 監査報告書の作成
報告書の構成には以下の項目を含めるものとする。また、別紙 2「外部監査の実施に係る報告様式」についても作成する。

- (2)の監査項目すべてについての監査結果
- 指摘事項がある場合は、その具体的な内容
- 指摘事項に対する改善方針案

6. 対象範囲
五島市の情報通信ネットワーク基盤
(システム利用部門及び個別ネットワークについては、監査対象に含まない。具体的な範囲は、別に受託者に指示する。)

7. 作業時間
原則として土、日、祝日を除く 8:45～17:15 とする。ただし、来庁又は本市職員の立会を要しない作業については、この限りではない。

8. 監査実施体制及び要件
(1) 受託者は ISO/IEC27001(JIS Q 27001)認証又はプライバシーマーク認証を取得していること。
(2) 監査責任者、監査人、監査補助者、アドバイザー等で構成される監査チームを編成すること。
(3) 監査の品質の保持のため監査品質管理責任者、監査品質管理者等の監査品質管理体制をつくること。
(4) 監査チームには、情報セキュリティ監査に必要な知識及び経験（地方公共団体における情報セキュリティ監査の実績）を持ち、次に掲げるいずれかの資格を有する者が１人以上含まれていること。
- システム監査技術者
- 公認情報システム監査人（CISA）
- 公認システム監査人
- ISMS 主任審査員
- ISMS 審査員
- 公認情報セキュリティ主任監査人
- 公認情報セキュリティ監査人

・　情報処理安全確保支援士

(5) 監査チームには、監査の効率と品質の保持のため次のいずれかの実績（実務経験）を有する専門家が１人以上含まれていること。

・　情報セキュリティ監査
・　情報セキュリティに関するコンサルティング
・　情報セキュリティポリシーの作成に関するコンサルティング（支援を含む）

(6) 監査チームの構成員が、監査対象となる情報資産の管理及び当該情報資産に関する情報システムの企画、開発、運用、保守等に関わっていないこと。

9. 提出書類

本業務に係る提出書類は、次に掲げるとおりとする。

提出書類	部数	提出時期	備考
①業務責任者指定通知書	１部	業務着手時	「8 監査人の要件」を満たすことが確認できる書類の写しを添付すること。また、業務期間中に業務責任者を変更するときは、速やかに届け出ること。
②履行管理体制表			業務期間中に履行管理体制を変更するときは、速やかに届け出ること。
③監査報告書	１部	業務完了時	J-LIS 報告用の監査報告書は 1 月中旬までに提出すること。
④本件業務で使用した資料、書類、議事録等			
⑤その他、本市が別に必要と定めるもの	必要数		
⑥ “①～⑤”の電子データ（CD-R または DVD-R）	１部		電子データは、Microsoft Word、Microsoft Excel 、Microsoft PowerPoint 及び PDF を基本とする。

10. 提出書類

成果物及びこれに付随する資料は、全て本市に帰属するものとし、書面による本市の承諾を受けないで他に公表、譲渡、貸与又は使用してはならない。ただし、成果物及びこれに付

随する資料に関し、受託者が従前から保有する著作権は受託者に留保されるものとし、本市は、本業務の目的の範囲内で自由に利用できるものとする。

11. 委託業務の留意事項

業務の実施にあたっては、以下の事項に留意する。

(1) 監査実施計画書の提出

契約締結後、受託者は監査実施計画書を提出し、本市と協議により委託業務の詳細内容及び各作業の実施時期を決定するものとする。

(2) 資料の提供等

本業務の実施にあたり、必要な資料及びデータの提供は本市が妥当と判断する範囲内で提供する。なお、受託者は、本市から提供された資料は適切に保管し、特に個人情報に係るもの及び情報システムのセキュリティに係るものの保管は厳格に行うものとする。また、契約終了後は本件監査にあたり収集した一切の資料については、速やかに本市に返還、又は破棄するものとし、同じく電子データについては、復元困難な形で消去するものとする。

(3) 再委託

原則として、本業務の全部又は一部を第三者に委託（以下「再委託」という。）してはならない。止むを得ず再委託を行う場合は理由及び範囲を明確にし、事前に本市の承認を得ること。

(4) 秘密保持義務

本業務で知り得た情報及び入手したデータは、本契約の履行期間及び履行後において第三者に漏らしてはならず、本業務に関わる従業員その他関係者にも周知徹底しなければならない。

データを取り扱うときは、これを流出させないように留意しなければならない。特に、次に掲げる各号を遵守すること。

- 本市の情報を目的外に使用しないこと。
- 本市の情報を複写、複製する場合には本市の許可を事前に得ること。
- 本市の情報を外部記憶媒体等で持ち出す場合は、紛失及び盗難を避けるため厳重に保管すること。また、データは必ず暗号化をすること。
- 本市の情報を取り扱う際は、のぞき見等への対策を行い、関係者以外に情報が知れ渡らないようにすること。

(5) 議事録の作成

受託者は、本業務の実施にあたり本市と行う会議、打ち合わせ等に関する議事録を作成し、本市にその都度提出して内容の確認を得るものとする。

(6) 関係法令の遵守

受託者は業務の実施にあたり、関係法令等を遵守し業務を円滑に進めなければならない。

(7) 報告等

受託者は作業スケジュールに十分配慮し、本市と密接に連絡を取り業務の進捗状況を報告するものとする。

12. その他特記事項

(1) 交通費その他いっさいの諸経費は本業務による費用に含まれており、別途支給することはないので注意すること。

(2) ISMS、関連情報の最新動向、コンサルティングのノウハウを活用し、企画・提案を行うこと。

(3) 成果物の納入後、その内容が要求品質を満たしていないものについては、受託者の責任において関連する項目を再検査し、当該個所の修正を行うこと。

(4) 契約書類に定めのない事項及び疑義が生じた場合は、業務担当者と協議をするものとし、その内容を記載した議事録を提出すること。

【別紙1】α'モデルを採用する場合の追加監査項目

項目		No.	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
3. 情報システム全体の強靭性の向上	技術的対策	1	**ⅰ）接続先のクラウドサービスの証明書による認証** 統括情報セキュリティ責任者及び情報システム管理者により、以下の対策が実施されている。 ・接続先のクラウドサービスが本物であるか否か、正当性を確認する。	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、LGWAN接続系からパブリッククラウドサービスに接続するさい、接続先が本物であるか否か、正当性を確認する対策が実施されているか確かめる。	―	―	
		2	**ⅱ）マルウェア対策ソフト** 統括情報セキュリティ責任者及び情報システム管理者により、パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策が実施されている。	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策が実施されているか確かめる。	―	―	
		3	**ⅲ）パッチ適用** 統括情報セキュリティ責任者及び情報システム管理者により、脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する対策が実施されている。	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する対策が実施されているか確かめる。	―	―	
		4	**ⅳ）接続先制限** 統括情報セキュリティ責任者及び情報システム管理者により、LGWAN接続系から外部へのアクセス先をLGWAN-ASP及び利用が許可されたクラウドサービスのみに限定する対策が実施されている。	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、LGWAN接続系から外部へのアクセス先をLGWAN-ASP及び利用が許可されたクラウドサービスのみに限定する対策が実施されているか確かめる。	―	―	
		5	**ⅴ）ローカルブレイクアウトテナントアクセス制御** 統括情報セキュリティ責任者又は情報システム管理者によって、団体専用テナントを利用時は、利用するクラウドサービスへのアクセスを自らの団体が利用するテナントのみに制限する対策が実施されている。	□システム構成図 □アクセス制御方針 □アクセス管理基準 □システム設計書 □機器等の設定指示書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、団体専用テナントを利用時は、利用するクラウドサービスへのアクセスを自らの団体が利用するテナントのみに制限していることを確かめる。	―	―	

項目	No.	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
	6	**vi）メール無害化/ファイル無害化** CISO又は統括情報セキュリティ責任者によって、LGWAN接続系にインターネットからファイルを取り込む際に、以下の対策が実施されている。 ・ファイルからテキストのみを抽出 ・ファイルを画像PDFに変換 ・サニタイズ処理 ・未知の不正プログラム検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューとCISO又は統括情報セキュリティ責任者へのインタビューにより、LGWAN接続系にインターネットからファイルを取り込む際に、ファイルからテキストのみを抽出、ファイルを画像PDFに変換、サニタイズ処理、未知の不正プログラム検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認するなどの対策が実施されているかを確かめる。	―	―	
	7	**vii）権限管理** 統括情報セキュリティ責任者又は情報システム管理者によって、不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限関連する属性に応じて適切に管理する対策が実施されている。	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限関連する属性に応じて適切に管理していることを確かめる。	―	―	
	8	**viii）アクセス制御** 統括情報セキュリティ責任者又は情報システム管理者によって、不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認可に基づき、アクセスの許可または拒否を行う対策が実施されている。	□アクセス制御方針 □アクセス管理基準 □システム設計書 □機器等の設定指示書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認可に基づき、アクセスの許可または拒否が実施されていることを確かめる。	―	―	・アクセス制御についてはNo.221～247も関連する項目であることから参考にすること。
	9	**ix）IDS/IPS** 統括情報セキュリティ責任者又は情報システム管理者によって、ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断する対策が実施されている。	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断する対策が実施されていることを確かめる。	―	―	

項目		No.	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
		10	**ｘ）DDoS対策** 統括情報セキュリティ責任者又は情報システム管理者によって、サービス不能攻撃の一つであるDDoS（Distributed Denial of Service）攻撃による被害を最小化するために、以下の対策が実施されている。 ・DDoS対策機器の導入 ・DDoS対策サービスの利用によって、高負荷攻撃への耐性を向上 ・負荷分散装置（ロードバランサ）による耐性向上	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、DDoS対策として、DDoS対策機器の導入、DDoS対策サービスの利用による高負荷攻撃への耐性の向上、負荷分散装置（ロードバランサ）による耐性の向上などの対策が実施されているかを確かめる。	―	―	※1
		11	**xi）通信路暗号化** 統括情報セキュリティ責任者又は情報システム管理者によって、通信路上の盗聴・改ざんによる被害を最小化するために、以下の対策が実施されている。 ・暗号技術を用いて通信路上のデータを暗号化する ・通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、通信路上の盗聴・改ざんによる被害を最小化するため、暗号技術を用いて通信路上のデータを暗号化する、通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする対策が実施されているかを確かめる。	―	―	
		12	**xii）クラウドサービスからファイルダウンロード制限** 統括情報セキュリティ責任者又は情報システム管理者によって、必要性に応じクラウドサービス上から業務端末へのファイルダウンロードを制限する**する対策が実施されている。**	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、必要性に応じ、クラウドサービス上から業務端末へのファイルダウンロードを制限するする対策が実施されているかを確かめる。	―	―	※2
	組織的・人的対策	13	**ｉ）手続・規定** クラウドサービスを利用開始する場合の申請、承認等に係る規定を整備するとともに、運用を徹底している。	□クラウドサービス事業者選定基準 □実施手順書	監査資料のレビューと情報セキュリティ管理者へのインタビューにより、クラウドサービス事業者選定の際、利用するクラウドサービスのアプリケーションや、格納する情報資産などに応じた情報セキュリティ対策が確保されていることを確認しているか確かめる。	―	―	
		14	**ⅱ）情報セキュリティ研修計画** 職員等が毎年度最低1回は情報セキュリティ研修を受講できるように計画されている。	□研修・訓練実施基準 □研修・訓練実施計画	監査資料のレビュー又は統括情報セキュリティ責任者へのインタビューにより、研修計画において、職員等が毎年度最低1回は情報セキュリティ研修を受講できるように計画されているか確かめる。	5.2.(2)	6.3	・αモデルにおいては推奨事項だが、β・β’モデルにおいては必須事項となる。

項目		No.	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
		15	**ⅲ）実践的サイバー防御演習（CYDER）の確実な受講** CISOによって、実践的サイバー防御演習（CYDER）を受講しなければならないことが定められ、受講計画が策定されており、また、受講計画に従い、職員等が受講している。	□研修・訓練実施計画 □研修・訓練受講記録 □研修・訓練結果報告書	監査資料のレビュー又は統括情報セキュリティ責任者へのインタビューにより、実践的サイバー防御演習（CYDER）の受講計画について文書化され、正式に承認されているか確かめる。 また、職員等が適切に受講しており、その受講記録が取られていることを確かめる。	―	―	
		16	**ⅳ）演習等を通じたサイバー攻撃情報やインシデント等への対策情報共有** 職員等が以下の演習やそれに準ずる演習を受講している。 ・インシデント対応訓練（基礎/高度） ・分野横断的演習	□研修・訓練実施計画 □研修・訓練受講記録 □研修・訓練結果報告書	監査資料のレビュー又は統括情報セキュリティ責任者へのインタビューにより、職員等がインシデント対応訓練（基礎/高度）、分野横断的演習又はそれに準ずる演習を受講しているか確かめる。	5.2.(2)	―	
		17	**ⅴ）自治体情報セキュリティポリシーガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し** 自治体情報セキュリティポリシーガイドライン等の見直し踏まえて、適時適切に情報セキュリティポリシーの見直しがされている。	□情報セキュリティポリシー	監査資料のレビュー又は統括情報セキュリティ責任者へのインタビューにより、情報セキュリティポリシーが自治体情報セキュリティポリシーガイドライン等の見直しを踏まえて、適時適切に見直しがされていることを確かめる。	9.3	―	・情報セキュリティポリシーの策定・遵守については、No.334～342、No.403～413、No.420～421も関連する項目であることから参考にすること。

※J-LIS追記
1：推奨事項
2：α’モデル(ア)・α’モデル(ウ)においては推奨事項、α’モデル(イ)においては必須事項

【別紙1】α'・β・β'共通の監査項目

項目			No.	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
1. 組織体制		(3)CSIRTの設置・役割	4	**ⅲ）CSIRTの設置・役割の明確化** CSIRTが設置され、部局の情報セキュリティインシデントについてCISOへの報告がされている。また、CISOによって、CSIRT及び構成する要員の役割が明確化されている。	□情報セキュリティポリシー □CSIRT設置要綱	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、CSIRTが設置されており、規定された役割に応じて情報セキュリティインシデントのとりまとめやCISOへの報告、報道機関等への通知、関係機関との情報共有等を行う統一的な窓口が設置されているか確かめる。また、監査資料のレビューとCISO又は構成要員へのインタビューにより、CSIRTの要員構成、役割などが明確化されており、要員はそれぞれの役割を理解しているか確かめる。	1.(9)	5.5 5.6 5.24 5.25 5.26 6.8	
5. 人的セキュリティ	5.1. 職員等の遵守事項	(1) 職員等の遵守事項 ① 情報セキュリティポリシー等の遵守	85	**ⅰ）情報セキュリティポリシー等遵守の明記** 統括情報セキュリティ責任者又は情報セキュリティ責任者によって、職員等が情報セキュリティポリシー及び実施手順を遵守しなければならないことが定められ、文書化されている。	□情報セキュリティポリシー □職員等への周知記録	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、職員等の情報セキュリティポリシー及び実施手順の遵守や、情報セキュリティ対策について不明な点及び遵守が困難な点等がある場合に職員等がとるべき手順について文書化され、正式に承認されているか確かめる。また、承認された文書が職員等に周知されているか確かめる。	5.1.(1)①	5.1	
			86	**ⅱ）情報セキュリティポリシー等の遵守** 職員等は、情報セキュリティポリシー及び実施手順を遵守するとともに、情報セキュリティ対策について不明な点や遵守が困難な点等がある場合、速やかに情報セキュリティ管理者に相談し、指示を仰げる体制になっている。	□情報セキュリティポリシー □実施手順書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、情報セキュリティポリシー及び実施手順の遵守状況を確かめる。また、情報セキュリティ対策について不明な点及び遵守が困難な点等がある場合、職員等が速やかに情報セキュリティ管理者に相談し、指示を仰げる体制が整備されているか確かめる。必要に応じて、職員等へのアンケート調査を実施し、周知状況を確かめる。	5.1.(1)①	5.1	・職員等の情報セキュリティポリシーの遵守状況の確認及び対処については、No.334～342も関連する項目であることから参考にすること。
		(1) 職員等の遵守事項 ② 業務以外の目的での使用の禁止	88	**ⅱ）情報資産等の業務以外の目的での使用禁止** 職員等による業務以外の目的での情報資産の持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスは行われていない。	□端末ログ □電子メール送受信ログ □ファイアウォールログ	監査資料のレビューと情報システム管理者及び職員等へのインタビューにより、業務以外の目的での情報資産の持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスが行われていないか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)②	－	
		(1) 職員等の遵守事項 ③ モバイル端末や電磁的記録媒体の持ち出し及び外部における情報処理作業の制限	90	**ⅱ）情報資産等の外部持出制限** 職員等がモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合、情報セキュリティ管理者により許可を得ている。	□端末等持出・持込基準/手続 □庁外での情報処理作業基準/手続 □端末等持出・持込申請書/承認書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等がモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合、情報セキュリティ管理者から許可を得ているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)③ (イ)	8.1 6.7 7.9	・紛失、盗難による情報漏えいを防止するため、暗号化等の適切な処置をして持出すことが望ましい。
			91	**ⅲ）外部での情報処理業務の制限** 職員等が外部で情報処理作業を行う場合は、情報セキュリティ管理者による許可を得ている。	□庁外での情報処理作業基準/手続 □庁外作業申請書/承認書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等が外部で情報処理作業を行う場合、情報セキュリティ管理者から許可を得ているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)③ (ウ)	8.1 6.7 7.9	・情報漏えい事故を防止するため、業務終了後は速やかに勤務地に情報資産を返却することが望ましい。

項目			No.	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
		(1) 職員等の遵守事項 ④ 支給以外のパソコン、モバイル端末及び電磁的記録媒体の業務利用	92	**ⅰ)支給以外のパソコン、モバイル端末及び電磁的記録媒体の業務利用基準及び手続** 統括情報セキュリティ責任者又は情報セキュリティ責任者によって、職員等が業務上支給以外のパソコン、モバイル端末及び電磁的記録媒体を利用する場合の基準及び手続について定められ、文書化されている。	□端末等持出・持込基準/手続 □支給以外のパソコン等使用申請書/承認書	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、支給以外のパソコン、モバイル端末及び電磁的記録媒体利用手順が文書化され、正式に承認されているか確かめる。	5.1.(1)④	5.10 7.8	
			93	**ⅱ)支給以外のパソコン、モバイル端末及び電磁的記録媒体の利用制限** 職員等が情報処理作業を行う際に支給以外のパソコン、モバイル端末及び電磁的記録媒体を用いる場合、当該端末の業務利用の可否判断をCISOが行った後に、業務上必要な場合は、統括情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ管理者による許可を得ている。また、機密性の高い情報資産の支給以外のパソコン、モバイル端末及び電磁的記録媒体による情報処理作業は行われていない。	□支給以外のパソコン等使用申請書/承認書 □支給以外のパソコン等使用基準/実施手順書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等が情報処理作業を行う際に支給以外のパソコン、モバイル端末及び電磁的記録媒体を用いる場合、情報セキュリティ管理者の許可を得ているか確かめる。また、端末のウイルスチェックが行われていることや、端末ロック機能及び遠隔消去機能が利用できること、機密性3の情報資産の情報処理作業を行っていないこと、支給以外の端末のセキュリティに関する教育を受けた者のみが利用しているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。また、手順書に基づいて許可や利用がされているか確かめる。	5.1.(1)④	8.1 6.7 7.8 7.9	
			94	**ⅲ)支給以外のパソコン、モバイル端末及び電磁的記録媒体の庁内ネットワーク接続** 職員等が支給以外のパソコン、モバイル端末及び電磁的記録媒体を庁内ネットワークに接続することを許可する場合、統括情報セキュリティ責任者又は情報セキュリティ責任者によって、情報漏えい対策が講じられている。	□庁外での情報処理作業基準/手続 □支給以外のパソコン等使用申請書/承認書 □支給以外のパソコン等使用基準/実施手順書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、支給以外のパソコン、モバイル端末及び電磁的記録媒体を庁内ネットワークに接続することを許可する場合は、シンクライアント環境やセキュアブラウザの使用、ファイル暗号化機能を持つアプリケーションでの接続のみを許可する等の情報漏えい対策が講じられているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)④	8.20 8.21	
		(1) 職員等の遵守事項 ⑤ 持ち出し及び持ち込みの記録	96	**ⅱ)端末等の持出・持込記録の作成** 情報セキュリティ管理者によって、端末等の持ち出し及び持ち込みの記録が作成され、保管されている。	□端末等持出・持込基準/手続 □端末等持出・持込申請書/承認書	監査資料のレビューと情報セキュリティ管理者へのインタビューにより、端末等の持ち出し及び持ち込みの記録が作成され、保管されているか確かめる。	5.1.(1)⑤	7.1	・記録を定期的に点検し、紛失、盗難が発生していないか確認することが望ましい。
		(1) 職員等の遵守事項 ⑦ 机上の端末等の管理	100	**ⅱ)机上の端末等の取扱** 離席時には、パソコン、モバイル端末、電磁的記録媒体、文書等の第三者使用又は情報セキュリティ管理者の許可なく情報が閲覧されることを防止するための適切な措置が講じられている。	□クリアデスク・クリアスクリーン基準	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビュー、執務室の視察により、パソコン、モバイル端末の画面ロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管といった、情報資産の第三者使用又は情報セキュリティ管理者の許可なく情報が閲覧されることを防止するための適切な措置が講じられているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)⑦	7.7	

項目		No.	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
	(3) 情報セキュリティポリシー等の掲示	108	**ⅱ）情報セキュリティポリシー等の掲示** 情報セキュリティ管理者によって、職員等が常に最新の情報セキュリティポリシー及び実施手順を閲覧できるように掲示されている。	□職員等への周知記録	監査資料のレビューと情報セキュリティ管理者へのインタビュー及び執務室の視察により、職員等が常に最新の情報セキュリティポリシー及び実施手順を閲覧できるよう、イントラネット等に掲示されているか確かめる。	5.1.(3)	5.1	
	(4) 外部委託事業者に対する説明	110	**ⅱ）委託事業者に対する情報セキュリティポリシー等遵守の説明** ネットワーク及び情報システムの開発・保守等を委託事業者に発注する場合、情報セキュリティ管理者によって、情報セキュリティポリシー等のうち、委託事業者及び再委託事業者が守るべき内容の遵守及びその機密事項が説明されている。	□業務委託契約書 □委託管理基準	監査資料のレビューと情報セキュリティ管理者へのインタビューにより、ネットワーク及び情報システムの開発・保守等を発注する委託事業者及び再委託事業者に対して、情報セキュリティポリシー等のうち委託事業者等が守るべき内容の遵守及びその機密事項が説明されているか確かめる。	5.1.(4)	5.19 5.20	・再委託は原則禁止であるが、例外的に再委託を認める場合には、再委託事業者における情報セキュリティ対策が十分取られており、委託事業者と同等の水準であることを確認した上で許可しなければならない。 ・委託事業者に対して、契約の遵守等について必要に応じ立ち入り検査を実施すること。 ・委託に関する事項ついては、No.337～366も関連する項目であることから参考にすること。
5.2. 研修・訓練	(1) 情報セキュリティに関する研修・訓練	112	**ⅱ） 情報セキュリティ研修・訓練の実施** CISOによって、定期的にセキュリティに関する研修・訓練が実施されている。	□研修・訓練実施基準 □研修実施報告書 □訓練実施報告書	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、定期的に情報セキュリティに関する研修・訓練が実施されているか確かめる。	5.2.(1)	6.3	
5.3. 情報セキュリティインシデントの報告		123	**ⅰ）情報セキュリティインシデントの報告手順** 統括情報セキュリティ責任者によって、情報セキュリティインシデントを認知した場合の報告手順が定められ、文書化されている。	□情報セキュリティインシデント報告手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、職員等が情報セキュリティインシデントを認知した場合、又は住民等外部から情報セキュリティインシデントの報告を受けた場合の報告ルート及びその方法が文書化され、正式に承認されているか確かめる。	5.3.(1)～(3)	6.8	・報告ルートは、団体の意思決定ルートと整合していることが重要である。
	(1) 庁内での情報セキュリティインシデントの報告	124	**ⅰ）庁内での情報セキュリティインシデントの報告** 庁内で情報セキュリティインシデントが認知された場合、報告手順に従って関係者に報告されている。	□情報セキュリティインシデント報告手順書 □情報セキュリティインシデント報告書	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、職員等へのインタビューにより、報告手順に従って遅滞なく報告されているか確かめる。また、個人情報・特定個人情報の漏えい等が発生していた場合、必要に応じて個人情報保護委員会へ報告されていることを確かめる。	5.3.(1)	6.8	

項目			No.	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
	5.4. ID及びパスワード等の管理	(1) ICカード等の取扱い	130	**ⅲ）認証用ICカード等の放置禁止** 認証用ICカード等を業務上必要としないときは、カードリーダーやパソコン等の端末のスロット等から抜かれている。	□ICカード等取扱基準	監査資料のレビューと情報システム管理者及び職員等へのインタビュー並びに執務室の視察により、業務上不要な場合にカードリーダーやパソコン等の端末のスロット等から認証用のICカードやUSBトークンが抜かれているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.4.(1)① (イ)	5.16 5.18	
			131	**ⅳ）認証用ICカード等の紛失時手続** 認証用ICカード等が紛失した場合は、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報され、指示に従わせている。	□ICカード等取扱基準 □ICカード紛失届書	監査資料のレビューと統括情報セキュリティ責任者及び情報システム管理者へのインタビューにより、認証用のICカードやUSBトークンが紛失した場合は、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報され、指示に従わせているか確かめる。	5.4.(1)① (ウ)	5.16 5.18	
			132	**ⅴ）認証用ICカード等の紛失時対応** 認証用ICカード等の紛失連絡があった場合、統括情報セキュリティ責任者及び情報システム管理者によって、当該ICカード等の不正使用を防止する対応がとられている。	□ICカード等取扱基準 □ICカード等管理台帳	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、紛失した認証用のICカードやUSBトークンを使用したアクセス等が速やかに停止されているか確かめる。	5.4.(1)②	5.16 5.18	
			133	**ⅵ）認証用ICカード等の回収及び廃棄** ICカード等を切り替える場合、統括情報セキュリティ責任者及び情報システム管理者によって、切替え前のカードが回収され、不正使用されないような措置が講じられている。	□ICカード等取扱基準 □ICカード等管理台帳	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、認証用のICカードやUSBトークンを切り替える場合に切替え前のICカードやUSBトークンが回収され、破砕するなど復元不可能な処理を行った上で廃棄されているか確かめる。	5.4.(1)③	5.16 5.18	・回収時の個数を確認し、紛失・盗難が発生していないか確実に確認することが望ましい。
		(3) パスワードの取扱い	138	**ⅱ）パスワードの取扱い** 職員等のパスワードは当該本人以外に知られないように取扱われている。	□パスワード管理基準	監査資料のレビューと情報システム管理者及び職員等へのインタビューにより、職員等のパスワードについて照会等に応じたり、他人が容易に想像できるような文字列に設定したりしないように取り扱われているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.4.(3)①～③	5.17	内閣サイバーセキュリティセンター(NISC)のハンドブックでは、「ログイン用パスワード」は、英大文字(26種類)小文字(26種類)＋数字(10種類)＋記号(26種類)の計88種類の文字をランダムに使って、10桁以上を安全圏として推奨している。
			139	**ⅲ）パスワードの不正使用防止** パスワードが流出したおそれがある場合、不正使用されない措置が講じられている。	□パスワード管理基準	監査資料のレビューと情報システム管理者及び職員等へのインタビューにより、パスワードが流出したおそれがある場合、速やかに情報セキュリティ管理者に報告され、パスワードが変更されているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.4.(3)④	5.17	
			142	**ⅵ）パスワード記憶機能の利用禁止** サーバ、ネットワーク機器及びパソコン等の端末にパスワードが記憶されていない。	□パスワード管理基準	監査資料のレビューと情報システム管理者及び職員等へのインタビュー、執務室の視察により、サーバ、ネットワーク機器及びパソコン等の端末にパスワードが記憶されていないか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.4.(3)⑦	5.17	

【別紙２】指摘事項に対する改善方針

#N/A

No.	監査項目種別	項目番号	監査項目	指摘事項	改善方針	対応完了予定日
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						

【別紙２】指摘事項に対する改善方針

記入例

No.	監査項目種別	項目番号	監査項目	指摘事項	改善方針	対応完了予定日
1		4	iii）CSIRTの設置・役割の明確化	CSIRT設置要綱が未策定であり、構成要員へのインタビューを行ったところ、CSIRTにおける自身の役割を理解していない職員が散見された。	速やかにCSIRT設置要綱を策定するとともに、構成要員への説明会を実施する。	2025/12/31
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						