前橋市情報セキュリティ監査業務仕様書

令和７年１０月
前橋市　未来創造部 情報政策課

１．件名

前橋市情報セキュリティ監査業務

２．背景

前橋市（以下「本市」という。）では、デジタル化の推進や市民の個人情報保護の観点から、市民の個人情報をはじめ、行政運営上重要な情報や情報システムを様々な脅威から防ぎ、市民へ安全・安定した行政サービス提供を継続するための様々な施策を実施している。

本市では、情報セキュリティポリシーを定めており、情報セキュリティ対策に関する事項を総合的・体系的・具体的に定めている。

本市の情報セキュリティポリシーは、セキュリティに関する統一的かつ基本的な方針である「基本方針」と、情報セキュリティ基本方針を実行に移すための「対策基準」及び「実施手順」の３要素に分類している。

本市では職員の業務生産性の向上とセキュリティ対策コストの最適化を目指し、令和７年度より、各種業務端末環境におけるChromebookを主体としたα´モデルによる強靭化を進めており、強靭化のための様々な対策及び施策を実施している。

総務省が示す、「地方公共団体における情報セキュリティポリシーに関するガイドライン(令和７年３月版)」において、LGWAN接続系とインターネット接続系の分割の在り方として示されている　α´モデルを採用する場合は、高度なセキュリティ対策の確実な実施が必要になることから、その実施について移行前に外部監査を実施し、移行後においても定期的に外部監査を実施し、その監査報告書を地方公共団体情報システム機構に提出することとされている。

以上の背景から、本市の情報セキュリティ監査を確実に実施するため「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」をもとに、本市が主催する監査として入札を実施する。

３．目的

本業務は、総務省が示す「α´モデル採用自治体における外部監査の実施手順」に従い、α´モデルの採用にあたり必須となる、「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」における組織的・人的対策に係る監査項目（23 項目）情報セキュリティ方針が遵守されていることを検証するための、セキュリティ監査を実施するものである。

ガイドラインに準拠して適切にセキュリティ対策が実施されているかを第三者による独立かつ専門的な立場から点検・評価し、問題点を確認するとともに、改善方法等について検討を行うことで、より適切な運用体制の構築やセキュリティ対策の維持向上を図る。

また、情報セキュリティ方針の運用における支援を受け、本市の情報セキュリティ対策の更なる改善に取り組むため、職員のセキュリティ意識向上に向けた啓発及びさらなるセキュリティ強化に関する各種助言を得ることを目的とする。

４．監査対象

本市の行政関連の業務に関するネットワーク及びシステムを対象とする（具体的な範囲は、別に受託者に指示する。）。

５．業務内容

業務内容について以下に示す。

1　助言型監査の実施及び外部監査報告書等作成（α’モデル採用自治体における外部監査）
2　国が例示する最新のセキュリティポリシー案との整合性確認、指摘及び監査により明らかになった脆弱性に対し、実現可能な具体的な対策案の提示
3　監査結果報告会の開催
4　その他本市のセキュリティ対策を含むDX推進関連施策全般に関する各種助言

６.適用基準等

本業務を実施するにあたり用いる適用基準等は、次のとおりとする。

必須とする基準

1　前橋市情報セキュリティポリシー（令和７年４月改定）
　セキュリティポリシーの詳細版は、別に受託者に提示する。

参考とする基準

1　個人情報の保護に関する法律（平成１５年法律第５７号）
2　地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省）
3　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（総務省）
4　前橋市個人情報の保護に関する法律施行条例（令和4年12月13日条例第43号）
5　上記のほか委託期間において情報セキュリティに関し有用な基準等で、本市と協議して採用するもの

参考とする資料

1　前橋市情報セキュリティポリシー（概要版）
2　ネットワーク構成図（概要版）

※ 上記以外の資料は、受託者へ契約締結後に本市との協議の上必要に応じて提供する。業務完了後に返却又は廃棄すること。

７.業務委託期間

(1) 契約期間

契約締結日から令和８年３月３１日まで

(2) 業務実施期間

前項契約期間のうち、監査の実施日は協議の上決定する。また、緊急時における対応については、本市と協議の上、柔軟に対応すること。

８.監査について

(1) 監査人要件

1　受託者はISO/IEC27001(JIS Q 27001:2023)認証を取得していること。

2　受託者はChromebookを端末とした自治体セキュリティ強靭化監査に関する対応実績を有すること。ただし、行政系ネットワークに関するものに限り、教育系ネットワークに関するものを除く。

3　監査責任者、監査人、監査補助者等で構成される監査チームを編成すること。

4　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。

5　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。

ア　システム監査技術者
イ　公認情報システム監査人（CISA）
ウ　公認システム監査人
エ　ISMS 主任審査員
オ　ISMS 審査員
カ　公認情報セキュリティ主任監査人
キ　公認情報セキュリティ監査人

6　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。

ア　情報セキュリティ監査
イ　情報セキュリティに関するコンサルティング
ウ　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。）

7　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.スケジュール

1　業務実施計画書の作成にあたり、業務全体のスケジュールを提示すること。

2　情報セキュリティ監査の結果を監査報告書（任意様式）、国の指定様式の作成を確実に実施するスケジュール案とすること。

3　実際の業務に当たっては、本市と協議の上決定するものとする。

１０.成果物の納入

(1) 成果物

1　監査計画書
2　監査に使用したチェックリスト
3　監査報告書（任意様式）
4　外部監査の実施に係る報告様式（指摘事項に対する改善方針、基本情報）
5　改定後の情報セキュリティポリシー案等
6　監査結果報告会での説明資料
7　業務完了報告書
8　その他必要な書類

(2) 様式及び部数

1　A列４版（必要に応じてA列３版三つ折も可。A列３版三つ折の場合、両面印刷は不可とする。）とし、様式は任意とする。
2　監査報告書は監査対象についての脆弱点を網羅した非公開の「情報セキュリティ監査報告書（詳細版）」と公開を前提とした「情報セキュリティ監査報告書（公開版）」の２種類を作成し、提出すること。

(3) 納期限
1　実施計画書は、契約締結後速やかに提出すること。
2　その他については、本市と協議の上決定する。なお、最終納期限は令和８年３月３１日とする。

(4) 著作権等
1　成果物に関する著作権、著作隣接権、商標権、意匠権及び所有権（以下、「著作権等」という。）は、原則本市に帰属する。
2　成果物に含まれる受託者又は第三者が権利を有する著作物等（以下「既存著作物」という。）の著作権等は、個々の著作者等に帰属するものとする。
3　納入される成果物に既存著作物等が含まれる場合は、受託者が当該既存著作物の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続を行うものとする。

(5) その他
1　成果物等の納入後、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、当該箇所の修正を行うこと。
2　監査報告書の作成にあたっては、(別紙) 外部監査報告書作成　業務内容に従うこと。

１１．留意事項
(1) 秘密保持義務に関する事項
受託者は、本業務の利用により直接又は間接に知り得た情報（以下、「機密情報」という。）について、次の事項を遵守しなければならない。契約期間満了後又は契約解除後も同様とする。
1　機密情報を本業務以外の目的に使用しないこと。
2　機密情報を第三者に漏らさないこと。
3　機密情報が漏洩しないよう管理徹底すること。
4　機密情報を複製又は複写する場合は、本市の許可を事前に得ること。
5　機密情報を市の施設外に持ち出す場合は、本市の許可を事前に得た上で、紛失及び盗難を避けるため厳重に保管し、データは必ず暗号化すること。
6　機密情報を市の施設外に持ち出した場合は、監査終了時に破棄し、「情報資産廃棄報告書」を提出すること

(2) その他
1　「情報セキュリティポリシー（基本方針、対策基準、実施手順）」及び監査に必要と認められる書類で、本市が妥当と判断する情報を受託者にのみ開示する。
2　本業務は、事業を一括して他の事業者に委託してはならない。業務の一部を他の事業者に再委託しようとする場合は、受託者は本市に対し申請を行い、あらかじめ許可を得ること。申請時に、委託業務内容及び再委託の事業者名を明記した書面とともに、再委託事業者の身元を明らかにする資料等の提出を求める。なお、再委託が許可される場合は、受託者に求めるものと実質同水準の情報セキュリティを確保する措置が担保されていると判断できる場合に限る。
3　本市での作業が必要な場合は、原則として平日９時から１７時までを作業可能時間とする。
4　本市が準備しなければならない事項については、十分な期間を設けた上で、内容と期限を明確にすること。

5　本業務に関し発生した事故については、その内容に関わらず速やかに書面をもって報告するとともに、その解決に努めること。

6　業務の進行状況について、本市から問合せがあったときは、その都度報告すること。

7　受託者は、本業務の実施にあたり、規程、要領その他関係法令等を遵守すること。

8　この仕様書に定めのない事項について、必要のあるときは、受託者と本市が都度協議し、決定するものとする。

１２．　発注部署

前橋市 未来創造部 情報政策課
連絡先：〒371-8601 群馬県前橋市大手町二丁目12番1号
電話番号：027-898-5883

（別紙）

外部監査報告書作成 業務内容

（ア）監査計画の策定

監査基本計画書をもとに、情報セキュリティ監査計画を策定すること。計画書には、以下の内容を含めること。

1　監査基準
2　監査対象
3　スケジュール
4　各監査対象向け監査項目（評価項目及び監査基準）
5　監査実施体制

（イ）予備審査

「６．適用基準等」に記載されている「必須とする基準」「参考とする基準」、各監査資料を精査し、ヒアリングに向けた事前監査を実施すること。

「（ウ）ヒアリング」を円滑に実施するため、予備審査をもとに事前ヒアリングシートを作成すること。

（ウ）ヒアリング

α´モデル採用自治体における外部監査の実施手順に規定されている監査実施例に従い、ヒアリング対象者、ヒアリング対象部門を特定し、ヒアリングを実施すること。

1　ヒアリングは現地にて対面で実施すること。
2　被監査者に対し、事前に被監査者が記入したチェックリストに従い、インタビューを行うこと。
3　必要に応じて、作業現場、記録類や情報保管場所等について情報セキュリティ方針の遵守状況等を視察及びレビューすること。
4　ヒアリングの結果、情報セキュリティ方針が十分に遵守されていない場合、現状の運用及び遵守できない理由について確認すること。

（エ）ヒアリング結果分析

1　「α´モデル採用自治体における外部監査の実施手順」に基づき、ヒアリング結果の分析を行うこと。

（オ）監査報告書の作成

1　ヒアリング結果を分析の結果をもとに、「監査報告書」を作成すること。
2　監査報告書の様式及び記載項目は他の自治体の実績から任意に作成すること。
3　監査報告書に指摘事項がある場合は、その具体的な内容について監査報告書に記載すること。
4　監査報告書に指摘事項がある場合は、指摘事項に対する改善方針として、外部監査の実施に係る報告様式にも当該指摘事項への改善方針及び対応完了予定日を記載すること。
5　外部監査の実施に係る報告様式に記載する基本情報として団体名、採用モデル、監査実施に係る情報及び担当者等を記載すること。

（カ）その他関連作業

その他、（ア）～（オ）の過程でより良い監査にするための作業があれば提案し、実施すること。