

情報セキュリティポリシー運用及びセキュリティ監査業務委託仕様書

1 業務名

情報セキュリティポリシー運用及びセキュリティ監査業務

2 目的

国において急速に行政のデジタル化が進展する中で、市役所のDX推進にあたっては、デジタル化の進展と足並みを揃えながら、情報セキュリティ対策の徹底や個人情報保護制度の適切な運用により、安全・安心を確保しつつ、スピード感を持って進めていくことが不可欠である。

国におけるデジタル庁の設置をはじめとする急速な行政のデジタル化の進展及び令和5年度に実施した北九州市情報セキュリティポリシーの改正に伴い、専門的な知識を持つ業者による、他都市の状況なども加味した幅広い知見を活用した、セキュリティポリシーの運用・改善を図る。

また、情報システムやマイナンバー等の管理・運用について、本市が定める「北九州市情報セキュリティポリシー」等に準拠して適切に実施されているかを、第三者による独立的かつ専門的な立場から、点検・評価し、問題点の確認、改善方法等についての検討、助言、指導を行うことによって、本市の情報セキュリティの維持・向上を図る。

3 委託期間

契約締結日から令和7年3月31日

4 委託内容

(1) セキュリティに関する個別案件相談対応

各課からデジタル市役所推進室に相談のあった案件について、来庁、電話、メール、WEB会議等を利用し相談対応を行うもの。本市セキュリティポリシー及び総務省のガイドラインに対応した最適な運用となるよう、専門的な立場から国や業界等の最新情報を収集し、運用方法・解釈等の提案をするもの。

(2) セキュリティポリシー改定補助

「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5年度末改定予定分）を踏まえ、本市のセキュリティポリシーを見直すに当たり、修正の必要な規定や項目の選定、具体案などについて助言等（本市への影響有無や追加・修正・削除などの修正パターンに応じた具体的な修正文案を提案、改定箇所、改定の背景の解説、他都市での修正文案に関する情報提供）を行う。

また、改正後のポリシーにおいて、より実用的かつ現実的な運用方法を提案するもの。

(3) 自己点検結果を活用したセキュリティ対策の提案等

本市のセキュリティ対策基準では、「各行政機関は、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない」ことになっており、自己点検の結果をセキュリティポリシーやセキュリティ対策の見直し時に活用することになっている。令和5年度に改定したセキュリティチェックシートを活用し、全職員向けに自己点検を実施する予定であるが、その実施方法の提案、点検結果の集計及び回答の傾向の分析を行うとともに、その結果を踏まえ、必要なセキュリティ対策を提案してもらうもの。

(4) β モデル採用自治体における外部監査（助言型）の実施

令和5年8月15日付け総務省通知「 β/β' モデル採用自治体における外部監査の実施及び監査報告書の提出について」に沿って、市に対し外部監査を実施する。（幹部職員向けにipadを配布し、インターネット接続系に該当端末を置きつつ、LGWAN接続系のグループウェアや共有ファイルを操作できるようになることから、局所的にいわゆる三層の対策における β モデルの状態となるため。）

通常のセキュリティ監査のように特定のシステムを利用する部署に対する監査ではなく、特定の職に就くものが利用するシステムとなるため、効率的かつ監査手法を提案すること。

(5) 情報セキュリティ監査

ア 業務内容

対象システムについて、適用基準に基づき本市の実情に沿った監査項目（基本的には、項目数50～60程度、うち10項目程度はマイナンバーに関するもの、3項目程度は委託業者の情報セキュリティ対策に関するもの、3項目程度は電磁的記録媒体の利用時における情報セキュリティ対策に関するものを想定。なお、事前調査においてシステム所管課に聞き取りを行う等、監査対象システムにとって実効性のある監査項目になるよう必要に応じて質問項目の加除修正を行うこと。）を設定し、「管理体制に関する事項」、「情報資産の分類と管理方法」、「物理的セキュリティ」、「人的セキュリティ」、「技術的セキュリティ」、「運用、評価・見直し」の各分野を遍く確認し、助言型の情報セキュリティ監査を実施する。

【共通事項】

- ・市長事務部局の各業務システムはシステム基盤上で稼働しており、システム基盤はデジタル市役所推進課が所管しているが、平成30年度に監査実施済

みであるため、システム基盤に該当する監査項目は割愛する。

- ・現地視察対象は、市長事務部局は、検診管理システムは2課（システム所管課及びシステムを利用する区役所等の担当課1課）、残り2システムは1課（システム所管課）とする。教育委員会は、1システムごとに、2課（システム所管課及びシステムを利用する学校等）とする。
- ・現地視察時間は、1課当たり3時間以内とする。
- ・システムベンダーへのヒアリングは、Web 会議システムを利用したオンラインでのヒアリングも可能とする。

- (ア) 監査実施計画書の提出
- (イ) 事前調査の実施
- (ウ) 監査チェックリストの作成
- (エ) ヒアリング及び視察
- (オ) 監査結果の意見交換
- (カ) 監査報告書の作成
- (キ) 監査報告会の実施
- (ク) フォローアップ支援の実施

イ 対象

- 市長部局 3システム
- 教育委員会 2システム

| システム所管課 | | 対象システム名 | システムベンダー |
|------------|--------------------|---------------------|--------------------|
| 市長 事務部局 | 保健福祉局 健康推進課 | 検診管理システム | 日本コンピューター株式会社 |
| | 市民文化スポーツ局 戸籍住民課 | 戸籍コンビニ交付システム | 富士フィルムシステムサービス株式会社 |
| | | 証明書コンビニ交付システム（住民票等） | 株式会社TKC |
| 教育 委員会 | 学校教育課 | 報酬等支払いシステム | 西日本電信電話株式会社 |
| | 教職員課 | 服務管理システム | 西日本電信電話株式会社 |

ウ 監査基準

| | 監査基準 | |
|----|---|-------|
| 1 | 北九州市情報セキュリティ基本方針 | 必須 |
| 2 | 北九州市情報セキュリティ対策基準 | 必須 |
| 3 | 北九州市個人情報保護事務取扱要領 | 必須 |
| 4 | 北九州市情報資産の管理及び運用に関する要領 | 市長事務局 |
| 5 | 北九州市教育委員会情報セキュリティに関する規程 | 教育委員会 |
| 6 | 北九州市立学校情報資産の管理及び運用に関する要領 | 教育委員会 |
| 7 | 北九州市情報セキュリティ監査実施要綱 | 以下参考 |
| 8 | 個人情報保護法 | |
| 9 | 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） | |
| 10 | 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） | |
| 11 | 特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編） | |
| 12 | 教育情報セキュリティポリシーに関するガイドライン（文部科学省） | |
| 13 | その他有用な基準で、本市と協議して採用されるもの | |

※1及び2を合わせて「北九州市情報セキュリティポリシー」とする。

5 スケジュール

(1) 概要

本委託業務のスケジュールの詳細については、本市と調整し、決定することとする。なお、現時点で想定している概ねのスケジュールは以下のとおり。

| 4月 | 5月 | 6月 | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 | 1月 | 2月 | 3月 |
|---------------------------|----|----|----|----|----|-----|-----|-----|----|----|----|
| セキュリティに関する個別案件相談対応 | | | | | | | | | | | |
| セキュリティポリシー改定補助 | | | | | | | | | | | |
| 自己点検結果を活用したセキュリティ対策の提案等 | | | | | | | | | | | |
| βモデル採用自治体における外部監査（助言型）の実施 | | | | | | | | | | | |
| 情報セキュリティ監査 | | | | | | | | | | | |

(2) 定例会の開催等

ア キックオフ会議

業務計画書等を作成し、市に提出してその承認を受けること。

イ 定例報告会

(ア) 月1回を目途に開催すること。

(イ) 業務を実施するに当たって、有益となる国や自治体における事例や技術動向等、情報セキュリティ関連の情報提供を行うこと。

※開催手法について、本市と受託者の協議の上、Web 会議等に代えても差し支えない。その場合、Web 会議の実施に当たって必要となる設備等は、原則として受託者が用意すること。

6 実施体制

(1) 本業務を確実に履行できる体制を設けること。

(2) 本業務に従事する者の中から、本市との情報共有、連絡を行う担当者を1名選任し、本市へ書面等により連絡すること。

(3) 本業務に従事する者については、以下の要件を満たす者を含めること。

過去5年間の間に、セキュリティ監査及び相談業務の政令指定都市での実務経験を2年以上有していること並びに情報システムの管理運用、情報セキュリティ対策、情報セキュリティポリシーの策定（改定を含む。）及び情報セキュリティ監査に係る専門的な知見を有していること。

上記に加えて、監査を実施する体制は以下のとおりとすること。

ア 監査を行うに当たり、監査責任者、監査人、監査補助者等、複数の要員で構成される監査チームを編成すること。

イ 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名以上含まれていること。

(ア) 公認情報セキュリティ主任監査人

(イ) 公認情報セキュリティ監査人

(ウ) 情報セキュリティ監査人補

(エ) 情報セキュリティ監査アソシエイト

(オ) 情報処理安全確保支援士

(カ) システム監査技術者

(キ) ISMS 主任審査員

(ク) ISMS 審査員

(ケ) 公認システム監査人（CSA）

(コ) 公認情報システム監査人（CISA）

- (サ) CISSP (Certified Information Systems Security Professional)
- (シ) CISM (Certified Information Security Manager)

ウ 監査チームの構成員が、監査対象とな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。

7 成果物

本業務で想定している成果物は以下のとおりである。

| 成果品 | 内容 | 納入期限 |
|----------------|-----------------------|-----------|
| 監査報告書 (概要版) | | 令和7年1月31日 |
| 監査報告書 (詳細版) | システムごとに作成すること | 令和7年1月31日 |
| 業務完了報告書 | 各業務の実施結果をまとめたもの。 | 業務終了後 |
| その他 | 本業務の遂行過程で取得し、又は作成した資料 | 随時 |

※ 成果物は指定のない限り電子データとし、日本語表記とすること。また、電子データの作成は、特に指定がない限り、本市職員が、Word、Excel、Powerpoint で編集できるソフトを使用すること。それ以外のソフトを使用する際には本市に相談すること。

8 業務実施に当たっての留意事項

(1) 業務の遂行

ア 本業務の実施に当たっては、本仕様書に定めるものの他、本市の指示に従うこと。

イ 本業務の円滑な遂行を図るため、受託者は本市職員との連絡・連携を密にして業務を実施すること。

ウ 本業務の実施に先立ち、業務を行う受託者の体制を書面にまとめ、本市に通知し、承認を得ること。

業務を遂行するための体制及び配置予定の要員について、その名簿及び各要員が有する資格・業務経験・役割を具体的に示すこと。また、作業スケジュールに対応して要員の配置に変動を生じさせる場合には、配置計画についても理由を付して明示すること。

エ 本業務の実施に関し、業務の進行管理を可能とする業務計画書を書面により本市に提出し、本市の承認を得ること。

オ 本業務の実施に関し、Web 会議等の対面によらない方式を活用することがで

きる。その際は、予め本市の承認を得ること。

カ 本業務に必要なとなるパソコン、周辺機器、消耗品等は、受託者が用意すること。

キ 本業務に必要なとなる作業場所等の環境は、受託者の負担で用意すること。ただし、ヒアリングや打合せ、進捗状況報告等、本市及び受託者が会議等を行う場所については、事前に日程調整を行った上で、本市が用意する。

ク 本業務の進捗状況については常に把握して円滑な執行管理を図ることとし、業務計画書に変更が生じることが判明した場合は、事前に本市と協議を行うこと。また、変更となった場合は速やかに変更した業務計画書を提出すること。

(2) 情報の提供

発注者は、受注者の業務遂行に当たり必要な情報を提供する。ただし、必要とされる範囲は、受注者の申出に基づき発注者と受注者との間で協議する。

(3) 資料の貸与

ア 受注者は、本業務遂行上必要がある場合は、発注者の所有する資料の貸与を要請することができるものとする。

イ 発注者は、受注者から前項の要請があり、その必要性を認める場合は、要請された資料を貸与するものとする。

ウ 受注者は、前項により資料の提供を受けた場合は、適正に提供資料の維持管理に当たらなければならない。また、発注者からの返還要求があったとき及び本委託業務が終了したときは、当該資料を速やかに発注者に返還しなければならない。

(4) 法令等の遵守

本業務の履行に当たっては、関係の法令、本市条例・規則・要綱等を十分理解し、遵守すること。

9 情報セキュリティに関する事項

受託者及び業務従事者は、業務の実施に当たって関係の法令、本市条例・規則・要綱等を遵守し、常に情報セキュリティが確保されるよう努めなければならない。

10 その他

本業務の履行に際して疑義が生じた場合には、双方で協議を行い必要な措置を講じるものとする。