令和6年度

札幌市情報セキュリティ内部監査支援業務

仕様書

1. 業務名称

令和6年度 札幌市情報セキュリティ内部監査支援業務

2. 業務期間

契約締結日から令和7年3月21日（金）まで

3. 語句定義

No.	語句	説明
1	本市担当者	本市における情報セキュリティ内部監査業務を担当する本市情報システム部の職員。
2	職員	本市の情報資産に接するすべての職員。
3	業務責任者	受託者側で配置する本市担当者の指示に従い本業務に関して一切の事項を処理する者。
4	CISO 承認	札幌市情報セキュリティポリシーに基づく最高情報セキュリティ責任者の承認が必要な案件のことを指す。

4. 業務の概要

本業務は、本市担当者が監査基準に準拠した適切な情報セキュリティ内部監査を実施できるよう支援を行うものである。

※監査基準については、「8.監査基準」参照

5. 発注部署

札幌市デジタル戦略推進局情報システム部システム調整課

連絡先：〒003-0801 北海道札幌市白石区菊水 1 条 3 丁目 1-5 菊水分庁舎

電話番号：011-826-6479　FAX：011-813-2185

6. 履行場所

現地ヒアリングの支援については本市が別に定めた場所（札幌市内）で行うものとする。

※現地ヒアリングについては、「7.業務内容」参照

7. 業務内容

業務全体像は別紙1「情報セキュリティ内部監査全体像」のとおり。

(1)昨年度の課題の洗い出し

本市が令和5年度に実施した情報セキュリティ内部監査の結果より、本市担当者と課題点等を洗い出す。

(2)内部監査実施手順書及び調査票の案の作成

ア　本市における令和 6 年度情報セキュリティ内部監査の実施にあたって、別紙 2「情報セキュリティ内部監査実施要領」（以下、「要領」という。）の 2.実施項目に掲げる①自己点検（以下、「自己点検」という。）、②現地ヒアリング（以下、「現地ヒアリング」という。）について、具体的な手順を記した内部監査実施手順書及び調査票の案を作成すること。

※調査票は、本市と協議のうえ、入力フォーム等のツールを用いても構わない。なお、集計については受託者が行うこと。

イ　内部監査実施手順書及び調査票、並びにそれに付随する資料等は、情報セキュリティに明るくない職員が使用することを想定し、平易かつ詳細に記載すること。

また、本市と協議のうえ、必要に応じて専門用語を解説した用語集等を作成すること。

(3)現地ヒアリングの支援

ア　現地ヒアリングについて、本市が選定する所属、システム及びCISO承認に対し、本市担当者とともに現地を訪問して実施すること。

※対象数は要領の対象範囲を参照

イ　現地ヒアリングにおける現地への訪問については、「9. 監査人の要件」に掲げる条件を満たす監査人を1名以上配置すること。

(4)情報セキュリティ内部監査の結果の集計

自己点検の結果を所属、職員、システム及びCISO承認の項目ごとに集計すること。

また、現地ヒアリングの結果を所属、システム、CISO承認の項目ごとに集計すること。

(5)情報セキュリティ内部監査の結果の分析

(4)で集計した結果について、自己点検の結果を所属、職員、システム及びCISO承認の項目ごとに要領1.実施方針に基づき分析すること。また、同様に現地ヒアリング

の結果を所属、システム、CISO 承認の項目ごとに分析すること。

(6)監査報告書の作成及び説明会の実施

(4)の集計を取りまとめるとともに、(5)の分析結果を基に情報セキュリティに対する改善提案等も含めた報告書を作成し、本市担当者に対し説明会を実施すること。

8. 監査基準

(1)札幌市情報セキュリティポリシー（基本方針及び対策基準）

(2)情報セキュリティ技術対策基準

(3)情報セキュリティ実施手順

(4)札幌市情報セキュリティ監査実施要領

(5)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）

(6)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）

(7)上記のほか内閣サイバーセキュリティセンター（NISC）や独立行政法人情報処理推進機構（IPA）等が発信している情報セキュリティに関する有用な基準等で、本市と協議して採用するもの

9. 監査人の要件

(1)受託者は、独立行政法人情報処理推進機構（IPA）が公開している情報セキュリティサービス基準適合サービスリストのうち情報セキュリティ監査サービスに係る部分に掲載されていること。

(2)業務責任者には、情報セキュリティ監査に必要な経験（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を選任すること。

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

10. 提出書類

受託者は、下表に定めるドキュメント（電子データ）を本市に提出すること。

また、そのほか本市で必要とするものについては、その都度提出すること。

提出ドキュメント	提出時期	備考
① 業務責任者指定通知書	業務着手時	「9. 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 履行管理体制図		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 監査実施計画書		
④ 情報セキュリティ内部監査の集計結果及び実施報告書	業務完了時	
⑤ 実施報告書のダイジェスト版		
⑥ 本件業務で使用した資料、書類、議事録等		
⑦ その他、本市が別に必要と定めるもの		

※電子データは、Microsoft Word、Microsoft Excel、Microsoft PowerPoint 及び PDF を基本とする。

11. 成果物の帰属

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。

12. 環境に対する配備

(1)受託者は、本市の環境マネジメントシステムに準じ、環境負荷低減に努めること。

(2)電気、水道、油、ガス等の使用にあたっては、極力節約に努めること。

(3)ごみ減量及びリサイクルに努めること。

(4)両面コピーの徹底やミスコピーを減らすことで、紙の使用量を減らすよう努めるこ

と。

(5)自動車等を使用する場合は、できるだけ環境負荷の少ない車両を使用し、アイドリングストップの実施など環境に配慮した運転を心がけること。

(6)業務に係る用品等は、札幌市グリーン購入ガイドラインに従い、極力ガイドライン指定品を使用すること。

13. 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。

ア　本市の情報を目的外に使用しないこと。

イ　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。

ウ　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。

エ　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)議事録等の作成

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。

14. その他特記事項

(1)交通費その他一切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)契約図書に定めのない事項及び疑義が生じた場合は、本市と協議するものとし、その内容を記載した議事録を提出すること。

業務責任者指定通知書

令和　　年　　月　　日

（あて先）札幌市長

受託者（住所）
（氏名）　　㊞

件　　名　＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

上記業務に係る業務責任者等について、次のとおり定めたので通知します。

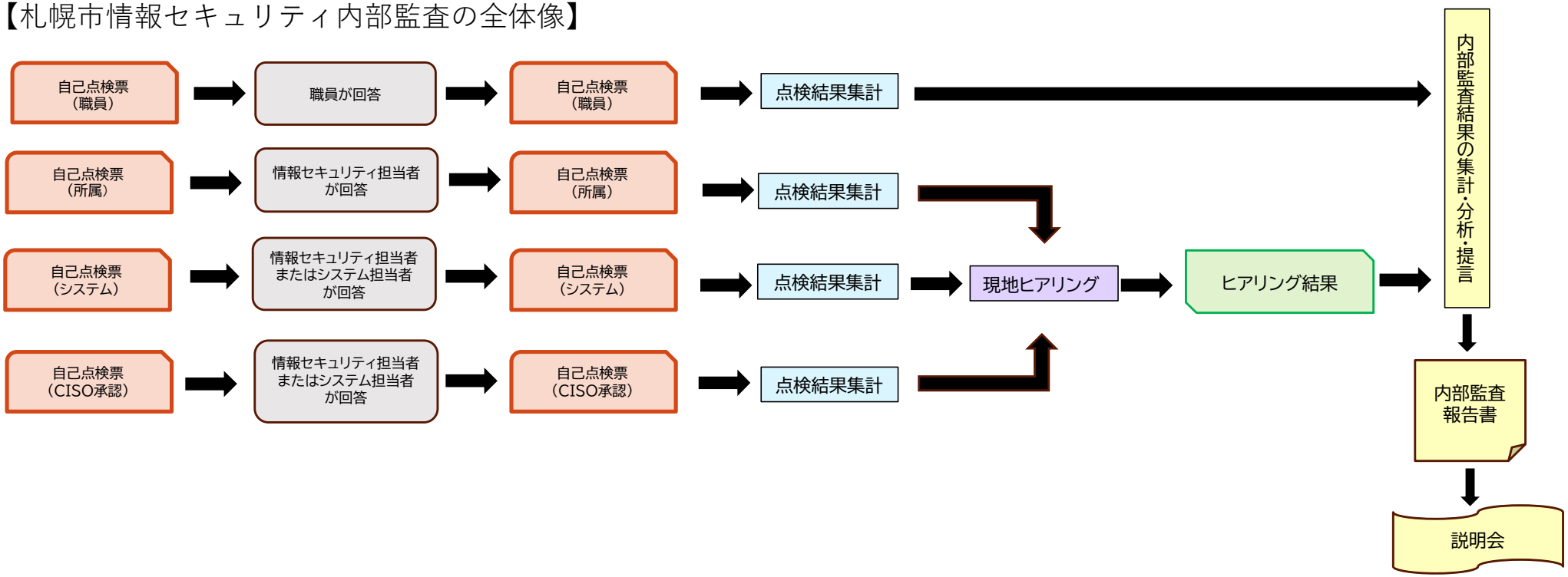
区分	氏名	備考（資格等）
業務責任者		

別紙1

＜情報セキュリティ内部監査全体像＞

本市では、「札幌市情報セキュリティポリシー」に基づき、定期的に、ポリシーの遵守状況や組織のセキュリティ対策に不足がないか等を確認するために、情報セキュリティ内部監査を毎年実施している。
全体像は以下のとおり。

【札幌市情報セキュリティ内部監査の全体像】



別紙1

○想定スケジュール

	8月			9月			10月			11月			12月			1月			2月			3月		
契約																								
キックオフ																								
課題洗い出し																								
実施手順書及び調査票作成																								
内部監査実施通知																								
自己点検																								
現地ヒアリング																								
結果分析																								
報告書の作成																								
説明会の実施																								

別紙２

情報セキュリティ内部監査実施要領

1. 実施方針

内部監査の実施方針は以下の 3 点とし、助言型監査とする。

(1) ポリシーに基づく対策の実施状況の確認

ポリシーに規定される各項目が遵守されているかをチェックし、必要に応じて改善提案を行う。

(2) 情報資産の取扱状況の確認

情報資産（個人情報、機密情報等）の取扱状況の実態（一覧の作成状況等）をチェックし、必要に応じて改善提案を行う。

(3) 緊急時の連絡・報告体制の整備状況の確認

情報システムを利用する業務において、緊急時の連絡・報告体制等の必要資料が整備されているかをチェックし、必要に応じて改善提案を行う。

2. 実施項目

内部監査の実施項目は以下の 2 点とする。

実施項目	備考
① 自己点検	「1. 実施方針」に掲げる(1)～(3)の状況について、各所属等は、調査票を基に自身で確認を行い、その結果を記入する。 自己点検は、所属、職員、システム及び CISO 承認（※）の各単位で行う。
② 現地ヒアリング	「1. 実施方針」に掲げる(1)～(3)の状況を客観的に評価するため、情報システム部は、各所属等へ自己点検の内容を基にした詳細の聞き取り及び必要に応じた改善提案を行う。 現地ヒアリングは、所属、システム及び CISO 承認の各単位で行う。

※ 札幌市情報セキュリティポリシーに基づく最高情報セキュリティ責任者の承認が必要な案件のことを指す。

3. 対象範囲

自己点検は、本市における全ての所属、職員、システム及び CISO 承認を対象に実施する。

現地ヒアリングは、所属、システム及び CISO 承認について実施する。CISO 承認は、本市が一部を抽出したもの（約 15 件）について検査を行う。

各数量は概ね次に掲げるとおりである。

(1) 所属数　約 500

(2) 職員数　約 15,000

(3) システム数　約 300

(4) 現地ヒアリングの実施数　約 50