

情報セキュリティ監査業務委託仕様書

1 業務名

情報セキュリティ監査業務委託

2 目的

本業務は、最新のセキュリティ情報及び専門的知識を有する第三者により、県の情報システムについて情報セキュリティ監査を実施するものである。

また、その結果を踏まえ、監査対象課所等に対しては、問題点の確認、改善方法等についての検討、助言を行う。

これにより、庁内の情報セキュリティ対策の向上を図る。

3 期間

契約日から令和6年3月22日（金）まで

4 履行場所

埼玉県企画財政部情報システム戦略課が指定する場所

5 委託内容

- (1) 発注者が提示する情報システムを対象として、各情報システムの運用形態に応じた情報セキュリティ対策の妥当性に関する検証・評価及び改善に向けた助言型監査を実施する。
- (2) 情報セキュリティ監査終了後、対象となったシステムの管理者に対し、監査内容や監査結果等について説明、助言等を行う監査結果報告会を実施する。
- (3) 明らかになった脆弱性に対して、実現可能な具体的な対策案を提示し、次年度以降に対応できるよう業務を補佐する。

6 実施方法

別紙「情報セキュリティ監査実施方法」のとおり。

7 適用基準

(1) 必須とする基準等

- ア 埼玉県情報セキュリティポリシー
- イ 情報セキュリティ共通実施手順
- ウ 監査対象システムに関する基本情報（設計書・運用手順書等）

(2) 参考とする基準

- ア 個人情報の保護に関する法律（平成15年法律第57号）
- イ 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3月版、総務省）
- ウ 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5年

3月版、総務省)

エ 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、発注者と協議して採用するもの

8 要件

- (1) 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。
- (2) 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。
- (3) 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。
 - ア システム監査技術者
 - イ ISMS主任審査員
 - ウ ISMS審査員
 - エ 公認システム監査人
 - オ 公認情報システム監査人（CISA）
 - 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
- (4) 監査チームには、監査の効率と品質の保持のため次の実績（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 情報システム又はサーバの運用管理経験
 - 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）

9 成果物

以下の成果物について、それぞれの提出期限までに提出し、発注者の確認を得ること。

最終納品期限は、令和6年3月22日（金）とし、印刷物2部及び電子データ（DVD-R）1枚を納品すること。

なお、電子データについては、Microsoft Office 2019で閲覧できる形式とする。

また、事前調査、ヒアリング及び現地調査で作成した資料についても、必要に応じて添付する。

納品物	提出期限
打合せ議事録（ヒアリング及び報告会含む）	打合せ終了後1週間以内

情報セキュリティ監査実施計画書	キックオフ会議開催前日
監査対象システムに対する事前調査表	キックオフ会議において協議した日程
情報セキュリティ監査結果報告書	キックオフ会議において協議した日程

10 成果物の納入場所

埼玉県企画財政部情報システム戦略課

(埼玉県さいたま市浦和区高砂三丁目15-1)

11 成果物の帰属

成果物及びこれに付随する資料は、全て発注者に帰属するものとし、書面による発注者の承諾を受けずに他に公表、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、発注者は、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 委託業務における留意事項

業務の実施にあたっては、以下の事項に留意する。

(1) 業務実施計画書の提出

契約締結後、受注者は発注者と協議し、委託業務内容及び各業務の実施時期に係る業務実施計画書を提出するものとする。

(2) 資料の提供等

本業務の実施に当たり、発注者が妥当と判断する範囲内資料及び情報を提供する。

なお、受注者は、発注者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、契約終了後は本業務に当たり受注者が収集又は作成した一切の資料を破棄し、「廃棄破棄証明書」(様式任意)を提出すること。

(3) 技術的検証

技術的検証については、監査対象システム及び県庁LAN/WANの運用に対し、支障及び損害を与えないように実施するものとする。

(4) 再委託

受託者は、本業務の実施にあたり他の業者に再委託することを原則、禁止する。

再委託が必要な場合は、発注者と協議の上、事前に書面により発注者の承認を得ること。

(5) 関係法令の遵守

受託者は、業務の実施にあたり、知り得た情報及び成果品の内容を正当な理由なく他に開示し又は自らの利益のために利用してはならない。これは、契約終了後又は契約解除後においても同様とする。

(6) 報告等

受注者は作業スケジュールに十分配慮し、発注者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。遅延している場合は、遅延の回復対策を内容とした文書を作成し、報告すること。

13 その他

本業務の実施にあたり、本仕様書に記載のない事項については発注者と協議の上決定するものとする。