
情報セキュリティ外部監査業務委託仕様書

令和8年4月

佐賀県総務部行政デジタル推進課

目次

| | |
|------------------------------|----|
| 第1章 総論 | 1 |
| 1.1 本業務の背景 | 1 |
| 1.2 本調達の実施の目的 | 1 |
| 第2章 本委託業務の概要 | 2 |
| 2.1 資格条件 | 2 |
| 2.2 本業務の範囲 | 2 |
| 2.3 委託内容 | 2 |
| 2.4 スケジュール | 2 |
| 第3章 委託の詳細要件 | 4 |
| 3.1 サービス要件 | 4 |
| 第4章 委託作業における詳細要件 | 5 |
| 4.1 業務内容 | 5 |
| 第5章 委託業務遂行に関する要件 | 9 |
| 5.1 プロジェクト管理 | 9 |
| 5.2 体制及び要員に関する要件 | 9 |
| 5.3 打合せ・報告に関する要件 | 9 |
| 5.4 本委託業務の納品物 | 10 |
| 第6章 その他 | 11 |
| 6.1 知的財産権の帰属等 | 11 |
| 6.2 機密保持 | 11 |
| 6.3 情報セキュリティに関する受託者の責任 | 11 |
| 6.4 契約不適合責任 | 12 |
| 6.5 法令等の遵守 | 12 |

第1章 総論

1.1 本業務の背景

佐賀県では、県の重要な情報資産を保護するため、セキュリティ対策を行っている。近年、インターネットを経由したサイバーセキュリティの脅威が深刻になっており、システムの脆弱性を突いた不正なアクセスや標的型攻撃メールなどのサイバー攻撃により個人情報流出するリスクが高まってきている。

このような各種サイバー犯罪や刻々と変化する攻撃手段から県の重要な情報資産を守るため、情報システムの運用管理や各所属におけるセキュリティ対策の取組状況等について、第三者による独立かつ専門的な立場からの監査を実施し、問題点を確認するとともに改善方法について検討を行うことで、より適切な情報システムの運用体制の構築やセキュリティ対策の維持向上を図る。

1.2 本調達の目的

情報セキュリティポリシーに基づき実施している本県の情報資産にかかる運用管理について、第三者との共同により客観的かつ専門的な立場から、基準等に準拠して適切に運用されているかを点検・評価し、問題点の確認、改善方法等についての検討・助言・指導を受け、改善を図ることにより、本県の情報セキュリティ対策の向上に資することを目的とする。

第2章 本委託業務の概要

2.1 資格条件

外部監査人は、以下の要件を満たすこと。

- (1) 本業務を実施する監査チーム（2名以上）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（以下「有資格者」という。）が1人以上含まれていること。なお、有資格者については、資格証の写しを提出すること。

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 主任審査員又は ISMS 審査員

オ 公認情報セキュリティ主任監査人又は公認情報セキュリティ監査人（CAIS）

カ 情報処理安全確保支援士

- (2) 本業務を実施する監査チームには、過去3年以内に国又は地方公共団体において、総務省ガイドライン（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及び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）を基に情報セキュリティ監査を実施した実績（実務経験）を有する者が1人以上含まれていること。なお、実績を有する者については、当該実績を確認できる資料（契約書、業務履行完了認定通知及び業務実施人員を示す書類等）の写しを提出すること。

2.2 本業務の範囲

県の情報システムの運用管理における情報セキュリティについて、問題点の抽出及び改善点の提言を求める「助言型監査による運用監査」を実施する。また、第三者の客観的かつ専門的な立場からの助言を確保するため、行政デジタル推進課職員と外部の監査人との共同で監査業務を行う「外部監査」として実施する。なお、当該監査は、助言型監査による運用監査であり、情報システムの脆弱性を検証する技術監査は行わない。

監査対象は、県が指定する4システムとする。1システムの監査において、システム担当所管課（県庁舎内部署）及びシステム利用所属（現地機関）の2所属を対象として監査を実施すること。

2.3 委託内容

本業務における委託内容の詳細は第4章で示す。

2.4 スケジュール

本業務における想定スケジュールは、図1のとおり。

委託期間：契約締結日～令和9年2月26日まで


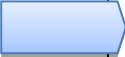

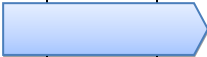

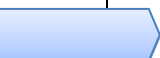

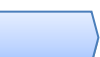
| 作業項目 | 令和8年度 | | | | | | | | |
|--------------------------|---|---|---|----|--|-----|---|---|--|
| | 6月 | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 | 1月 | 2月 |
| 事前打ち合わせ |  | | | | | | | | |
| 監査チェックリスト作成 監査実施計画書作成 | |  | | | | | | | |
| 監査説明会 | | |  | | | | | | |
| 監査事前調査 (監査対応確認シート) | | |  | | | | | | |
| 本調査実施 | | | | |  | | | | |
| 監査報告書の作成 (監査調書の作成を含む) | | | | | | |  | | |
| 監査報告会 | | | | | | | |  | |
| 完成図書（監査報告書等） 提出 | | | | | | | | |  |

図1 委託業務スケジュール

第3章 委託の詳細要件

3.1 サービス要件

3.1.1 体制要件

外部監査人は、以下の体制を構築すること。

- (1) セキュリティ監査の実施にあたって、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。（編成後は、本県に対し体制表を提出し、変更があった場合は、すみやかに届け出ること。）

3.1.2 準拠する基準

- (1) 必須とする基準

- ① 佐賀県情報セキュリティポリシー（情報セキュリティ基本方針及び対策基準）
- ② 情報セキュリティ実施手順（システム担当所管課が作成したもの）

- (2) 参考とする基準

- ① 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
- ② 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
- ③ 情報セキュリティ管理基準（経済産業省）
- ④ 特定個人情報の適正な取扱いに関するガイドライン（個人情報保護委員会）

第4章 委託作業における詳細要件

4.1 業務内容

4.1.1 業務の流れ

監査は概ね次の流れで実施する。

- (1) 監査実施計画書作成、事前打ち合わせ
- (2) 監査チェック項目（情報システム自己点検シート）作成
- (3) 監査説明会
- (4) 監査事前調査（システム担当所管課等が監査対応確認シートを回答。受託者は内容を確認。）
- (5) 本調査実施（インタビュー、関係文書の閲覧、現地視察）
- (6) 監査報告書作成（監査調書作成を含む）
- (7) 監査報告会
- (8) 完成図書（監査報告書等）提出

4.1.2 監査方法及び業務分担

【業務分担について】

| | 業 務 項 目 | 業務分担 | | |
|-----|---------------------------|------|-----|------|
| | | 県 | 受託者 | 原課参加 |
| (1) | 監査実施計画書作成、事前打ち合わせ | ◎ | ◎ | — |
| (2) | 監査チェック項目（情報システム自己点検シート）作成 | — | ◎ | — |
| (3) | 監査説明会 | ○ | ◎ | 有 |
| (4) | 監査事前調査（監査対応確認シート） | — | ◎ | — |
| (5) | 本調査実施 | ○ | ◎ | 有 |
| (6) | 監査報告書作成（監査調書作成を含む） | ○ | ◎ | 有 |
| (7) | 監査報告会 | ○ | ◎ | 有 |
| (8) | 完成図書（監査報告書等）提出 | — | ◎ | — |

※ ◎：主担当 ○：支援（原課との調整等）

4.1.3 業務の詳細

- (1) 監査実施計画書作成、事前打ち合わせ

契約締結後、速やかに次に掲げる事項を含め監査実施に必要な事項について、具体的に記載した監査実施計画書を提出し、県の承認を得ること。

ア 監査目的

イ 監査対象

- ウ 実施体制
- エ 監査基準及び評価基準
- オ 監査実施方法
- カ 役割分担
- キ 実施スケジュール
- ク その他記載すべき事項

なお、実施スケジュールは、「2.4 スケジュール」に基づくものとするが、詳細なスケジュールは県と調整を行うこと。

また、監査実施方法については、県と事前打ち合わせを行い必要な要件を確認すること。

(2) 監査チェック項目作成

監査対象システムごとに、監査基準（「3.1.2 準拠する基準」）に基づき、情報システムの運用・管理等における安全管理措置について、「監査チェック項目（情報システム自己点検シート）」を作成すること。

なお、チェック項目は、30～50項目程度とし、チェック項目ごとに根拠となる監査基準の該当箇所及び項目の説明を明記すること。

(3) 監査説明会（1 監査部門当たり 30 分～1 時間程度を想定）

監査を円滑に進めるため、被監査部門に対し、監査の目的、実施内容、監査の方法等について監査説明会を実施すること。監査説明会は、監査対象の部署ごとに1回ずつ実施することとし、会場は県が準備する。（県が被監査部門及び受託者のスケジュールを調整し、監査説明会の日程を決定する。日程調整により、複数の被監査部門と同時に説明会を開催する場合もある。）

監査において、資料調査又は現地調査等が必要となる場合は、提出を求める資料及び調査内容等について説明するとともに、文書として提示すること。

なお、説明会には、必ず有資格者が1名以上参加すること。

受託者は、説明会に必要な資料を準備し、主体的に説明を行うこと。

(4) 監査事前調査

(2)で作成した監査チェック項目（情報システム自己点検シート）を本調査実施前に、被監査部門へ配布し自己点検を実施する。情報システム自己点検シートを回収した後、本調査で被監査部門にヒアリングする内容を整理すること。

(5) 本調査実施（1 監査部門当たり 2～3 時間程度を想定）

被監査部門ごとに、担当者へのヒアリング、現地調査、資料調査等により、監査チェック項目について調査を実施すること。

受託者は、次に掲げる要件を満たして本調査を行うこと。

ア 本調査には、必ず有資格者が1名以上参加すること。

イ 本調査では、インタビュー、文書記録の閲覧、現地視察を実施し、概ね2～3時間程度を

原則とすること。ただし、監査チームが人員を動員し、本調査に要する時間を縮減する場合はこの限りではない。

ウ 被監査部門の担当者へのインタビューにおいては、監査チェック項目と同時に、セキュリティに対する意識、各種基準の認知度、システムの運用・管理におけるセキュリティ対策の状況等についても確認すること。

エ システムの運用・管理におけるセキュリティ対策上の不備や問題点を明らかにするため、必要な関係書類等を確認すること。

オ 監査実施にあたり、必要があれば各種情報資産の取扱場所など現地訪問し、セキュリティ対策の現状について目視確認を行うこと。

(6) 監査報告書作成（監査調書作成を含む）

監査の実施結果に基づき、監査調書を作成すること。なお、監査調書の作成に当たっては、事実誤認がないか等、被監査部門に十分な確認を行うこと。

監査報告書は、以下の点に留意のうえ作成すること。

ア 監査報告書は、非公開の「監査報告書（詳細版）」と公開を前提とした「監査報告書（概要版）」の2種類を作成すること。

イ 「監査報告書（概要版）」は、本委託業務全体を総括するものとして1つ作成し、「監査報告書（詳細版）」は、監査対象のシステムごとにそれぞれ作成すること。

ウ 「監査報告書（詳細版）」は、評価できる事項、改善すべき事項、改善が望まれる事項という観点から監査結果を記載すること。また、改善すべき事項、改善が望まれる事項については、改善しないことによって発生しうる問題や、具体的な改善策についても記載すること。

その他必要な事項、補足資料等がある場合は記載すること。

エ 監査報告書は、県職員が特段の専門的な知識を有することなく理解ができる内容とすること。なお、専門用語がある場合は、注釈をつけて用語の説明をつけること。

オ 監査報告書は、紙媒体及び電子媒体（CD-R 又は、DVD-R）を一部ずつ提出すること。

カ 提出された内容に不備があると判断した場合は、報告書の修正、補足説明の実施、補足資料の提出等を求める場合がある。

キ 監査報告書について、被監査部門向けの監査報告会を実施する前に、県担当者へのレビューを行うこと。

(7) 監査報告会（1時間程度を想定）

監査対象のシステムごとに、被監査部門向けに監査報告会を実施し、監査の結果、発見された事項（評価できる事項、改善すべき事項、改善が望まれる事項）について、「監査報告書（詳細版）」に基づき報告すること。また、改善すべき事項、改善が望まれる事項については、改善しないことによって発生しうる問題や具体的な改善策についても報告すること。

なお、県は被監査部門及び受託者のスケジュールを調整し、監査報告会の日程を決定する。

受託者は、監査報告会に必要な資料を準備し、監査報告を主体的に開催すること。なお、監査報告会には、必ず有資格者が1名以上参加すること。

(8) 完成図書（監査報告書等）提出

「5.4.1 納品物の内容」に示す納品物を提出期限までに提出すること。

第5章 委託業務遂行に関する要件

5.1 プロジェクト管理

5.1.1 プロジェクト管理方法

PMBOK (Project Management Body of Knowledge) など、世界的にも標準手法として認知されている、プロジェクト管理方法を用いること。

5.1.2 プロジェクト基礎データの収集報告方法

プロジェクトの進捗・品質を担保するために必要な基礎データを明確にし、その取得方法、報告方法について県と合意したうえ収集すること。県に対する報告は収集した基礎データをもとに行うこと。

5.2 体制及び要員に関する要件

5.2.1 プロジェクト体制

本業務に遂行に関するプロジェクト実施体制を敷くこと。

外部組織、協力会社などが存在する場合、その関係、役割、作業分担、責任範囲、指揮系統を明確にすること。

5.2.2 要員計画

本業務を遂行するために、プロジェクトマネージャーを1人割り当てること。

委託業務においては、個別の責任者（各業務責任者）を割り当てること。

プロジェクト要員を計画し、要員の情報（プロフィール情報、スキル情報、参画期間、経験情報）を明確にすること。

5.2.3 組織管理・コミュニケーション管理方法

本業務におけるプロジェクト組織の管理方法、組織間・組織内のコミュニケーション管理方法についてあらかじめ県と合意すること。

5.3 打合せ・報告に関する要件

受託者は、本事業のスケジュール等に十分配慮し、県との打合せ・報告等を主体的に行うこと。

受託者は、本業務の実施にあたり、県と行う打合せ、報告等に関する議事録を作成し、県にその都度提出して内容の確認を得るものとする。

5.4 本委託業務の納品物

5.4.1 納品物の内容

以下に記すものを、県が示す期限までに納品すること。また、提出期限にあたっては、確認や修正に要する日数など十分な余裕をもって作成にあたること。なお、中間成果物に関しては、各フェーズの完了時に提出すること。成果物の内容については県担当者と協議し、県の検収（検査）、承諾を受けること。

(1) 納品物品

- ① 監査実施計画書
- ② 監査チェック項目（情報システム自己点検シート）
- ③ 事前説明会用資料
- ④ 監査調書
- ⑤ 監査報告書（概要版）
- ⑥ 監査報告書（詳細版）
- ⑦ 打合せ議事録・・・一式
- ⑧ 監査で使用了書類等・・・一式

5.4.2 形式等

納品物品は、電子媒体により提出することとし、CD-R 又はDVD-R により1部提出すること（ファイルフォーマットは、Microsoft Office に対応できるデータ形式とする）。

なお、納品物品は日本語表記とする。

5.4.3 納品場所

佐賀県総務部行政デジタル推進課（佐賀県庁新館6階）

第6章 その他

6.1 知的財産権の帰属等

知的財産権等については、委託契約書による。

6.2 機密保持

- (1) 受託者は、本調達に係る作業を実施するに当たり、県から取得した資料（電子媒体、文書、図面等の形態を問わない。）を含めて、契約上知り得た情報を、第三者に開示又は本調達に係る作業以外の目的で利用しないものとする。但し、次のいずれかに該当する情報は、除くものとする。
 - ・取得した時点で、既に公知であるもの
 - ・取得後、受託者の責によらず公知となったもの
 - ・法令等に基づき開示されるもの
 - ・佐賀県から秘密でないと指定されたもの
 - ・第三者への開示又は本調達に係る作業以外の目的で利用することにつき、事前に県と協議の上、承認を得たもの
- (2) 受託者は、県の許可なく、取り扱う情報を指定された場所から持出、又は複製しないものとする。
- (3) 受託者は、本調達に係る検収後、受託者の事業所内部に保有されている本調達に係る佐賀県に関する情報を、裁断等の物理的破壊、消磁その他復元不可能な方法により、速やかに抹消すると共に、県から貸与されたものについては、検収後1週間以内に県に返却するものとする。

6.3 情報セキュリティに関する受託者の責任

6.3.1 情報セキュリティポリシーの遵守

- (1) 受託者は、佐賀県のホームページに公開している「佐賀県情報セキュリティ基本方針」を遵守すること。
- (2) 個人情報の扱いについては「個人情報取扱特記事項」を遵守すること。
- (3) 情報セキュリティに係る取扱いについては「情報セキュリティ特記事項」を遵守すること。

6.3.2 情報セキュリティを確保するための体制の整備

- (1) 受託者は、県の情報セキュリティポリシーに従い、受託者組織全体のセキュリティを確保すると共に、発注者から求められた当該業務の実施において情報セキュリティを確保するための体制を整備すること。
- (2) 個人情報保護のための体制を整備すること。

6.4 契約不適合責任

納入成果物が本仕様書に適合しない旨の県からの通知があった場合には、受託者の責任及び負担において、県が相当と認める期日までに補修を完了するものとする。

6.5 法令等の遵守

- (1) 受託者は、民法（明治29年法律第89号）、刑法（明治40年法律第45号）、著作権法、不正アクセス行為の禁止等に関する法律（平成11年法律第128号）等の関係法規を遵守すること。
- (2) 受託者は、個人情報の保護に関する法律（平成15年法律第57号）及び受託者が定めた個人情報保護に関するガイドライン等を遵守し、個人情報を適正に取り扱うこと。