

令和 6 年度沖縄県情報セキュリティ外部監査業務仕様書

1 業務名称

令和 6 年度沖縄県情報セキュリティ外部監査業務

2 目的

沖縄県における情報システムの運用体制、及びそのセキュリティの現状等について、第三者による専門的・客観的な立場から外部監査を実施し、情報セキュリティ上の問題点を明確にするとともに、問題点に対する改善策の助言を受けることで、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ことを目的とする。

3 業務内容

受託者は、次に記載する業務を実施すること。

(1) 監査実施に当たっての打ち合わせ

ア 当該委託業務に関する打ち合わせは、契約締結後から行う。なお、打ち合わせは 4 回程度とし、双方協議の上、必要な時に随時、Web 会議等により行う。その他の調整事項については、随時メール又は電話で行う。

イ 打ち合わせ後、速やかに打合せ記録簿を提出すること。

(2) 情報セキュリティ外部監査説明会の実施及び監査実施計画書の作成

ア 監査対象所属等を集めた監査説明会を Web 会議等により実施し、監査実施内容や手法等について説明を行うこと。

イ 契約後速やかに、以下の内容が記載された監査実施計画書を提出すること。なお、本件監査の目的を達するため、同計画書を、監査の進行に伴い、情報基盤整備課と協議して変更することができる。

(ア) 本監査実施方法の要領

(イ) 監査実施内容毎の監査従事者

(ウ) 収集する監査証拠の範囲

(エ) 監査証拠の収集方法

(オ) 特段の評価方法があるときはその旨

(カ) その他本件監査に必要な事項

(3) 情報セキュリティ外部監査の実施（10 月～11 月）

ア 対象となる情報システムの運用状況及び対象所属における適用基準への適合性に関す

るヒアリング、現地調査及び書面調査並びにセキュリティ診断（脆弱性調査、疑似侵入調査、web アプリケーション診断等）を実施すること。

イ 監査人は2名以上とし、7に示す監査人要件を満たすこと。

ウ 監査の実施にあたり、事前調査及び事前提出資料が必要となる場合は、あらかじめ内容及び実施時期等を情報基盤整備課と協議すること。

エ セキュリティ診断は対象所属と調整の上、実施すること。

オ ヒアリングはWeb 会議等により実施し、所要時間は3時間程度を見込むこと。なお、システムの実態に合わせて所要時間及びヒアリング回数を検討し、協議の上、決定するものとする。時間配分等は監査人が判断すること。

カ セキュリティ診断は、対象となる情報システムを構成するサーバの技術的な脆弱性を調査すること。

キ セキュリティ診断は、インターネット側に公開されている情報システムに対し、インターネットを経由した調査を実施すること。

ク インターネット経由のセキュリティ診断を実施するにあたっては、インターネットへ接続するための端末及びインターネット回線を別途用意すること。

ケ セキュリティ診断の対象となるIPアドレス数は5つ程度とする。

コ セキュリティ診断により判明した脆弱性のうち、危険度が高く早急な対応を必要とするものについては、情報基盤整備課長に対し速報を行うこと。

サ セキュリティ診断を実施する際には、対象とする情報システムの運用に対し、支障及び損害を与えないようにすること。また、そのための実施条件等があれば、あらかじめ監査実施計画書に盛り込むこと。診断当日の状況によっては調査が延期される場合があるので、予備日を見込むこと。

シ 監査実施後は監査調書を作成し、情報基盤整備課へ提出すること。

（4）監査報告書等の作成

ア 監査報告書及び監査結果報告書（以下、「監査報告書等」という。）は、A4版（縦）で作成し、様式は任意とする。ただし、表示の都合上、必要のある場合には、A3版二つ折り横の形式（紙面サイズのA4相当）としても構わない。

イ 監査報告書は、監査対象ごとに監査対象の脆弱点を網羅した非公開の監査報告書（詳細版）と、外部公開を前提にした監査報告書（公開対応版）の2種類を作成すること。

ウ 監査報告書には、実施した監査の対象、監査の内容、証拠に裏付けられた合理的な根拠に基づく意見、制約又は除外事項及びその他当該監査の目的に照らして必要と判断した事項を明瞭に記載すること。

エ 監査報告書は、監査の状況及び情報システムを取り巻くリスクの現状を踏まえ、情報システムのセキュリティ対策向上につながる追加方策について具体的な改善提案をまとめること。なお、セキュリティ診断により検出された技術的な脆弱性については、対処方法を明示すること。

オ 監査結果報告書は、監査報告書の内容について総合的な分析をし、主要な課題の抽出及び改善案等をまとめた総括版とすること。

(5) 監査結果報告会の実施

ア 監査報告書提出後、監査対象所属等を集めた監査報告会を Web 会議等により実施し、監査結果の概要、分析等について全体説明を行うとともに、対象所属へ個別に改善指摘事項等の内容、問題点の説明及び改善提案を行うこと。

イ 特に技術的な改善計画提案については、専門的な知識の少ない職員を対象として、分かりやすい資料を用いた説明に努めること。

(6) 指摘事項改善計画に関するフォロー

ア 監査対象所属が、改善指摘事項等に対する改善計画を策定し実施するための「指摘事項改善計画書」（様式）を作成すること。

イ 監査対象所属から提出される指摘事項改善計画書について、内容（改善方法、方針等）を評価し、必要な改善がなされるよう助言（主に電話、電子メールを用いたもの）すること。なお、支援期間は業務履行期間内とする。

(7) 内部監査人（情報基盤整備課職員）向けの研修会

ア 内部監査人となる職員に対し、情報基盤整備課が策定した内部監査マニュアル等を参考に、リモート監査を前提とした運用状況の確認方法、検証及び評価方法、助言等の方法等を含む情報セキュリティ監査の実施に関する研修会を行うこと。

イ 研修会は午前・午後の 2 回に分けて Web 会議等により行い、対象人数の総数は 20 人程度を見込むこと。（この人数にはオブザーバーとして参加する市町村職員を含むものとする）

ウ 研修内容については、ロールプレイ演習等を含めた座学のみでない実践的な研修とすること。

4 業務履行の場所及び期間

(1) 場所

ヒアリングを含む運用監査、セキュリティ診断ともに実地またはリモートで実施する。

(2) 期間

契約締結の日から令和 7 年 1 月 31 日まで

5 監査対象

(1) 情報セキュリティ外部監査を実施する情報システムは最大 10 システム（うち個人番号利用事務システム 3 システム）とし、セキュリティ診断を実施する情報システム数は最大 3 システムとする。

(2) 外部監査対象情報システムは、情報基盤整備課が別途指定する。

6 適用基準

(1) 情報セキュリティ監査を実施するに当たり用いる適用基準は、次のとおりとする。

- ア 沖縄県情報セキュリティ基本方針
- イ 沖縄県情報セキュリティ対策基準
- ウ 沖縄県情報システム基本方針
- エ 沖縄県情報システムガイドライン
- オ CORAL 21 ネットワーク運用管理要綱及び要領
- カ CORAL 21 基幹システムが提供するインターネットサービスの利用要領
- キ 沖縄県一括導入パソコン等及び管理システム運用管理要領
- ク その他、各システム管理運用要綱等

(2) 上記ア、イ、オ～クについては、契約締結後に情報を提供する。ただし、業務完了時には返却もしくは破棄すること。

7 監査人要件

本業務の内、情報セキュリティ外部監査を実施する監査人の要件については、次のとおりとする。

(1) 監査人は、情報セキュリティ監査に必要な知識及び経験を持つ者とする。

(2) 情報セキュリティ監査の監査責任者はアに掲げるいずれかの資格又はイに掲げるいずれかの資格を有していること。なお、運用に関する監査を行う監査人のうち1人以上の者は、アに掲げるいずれかの資格を有すること。また、技術に関する監査を行う監査人のうち1人以上の者は、イに掲げるいずれかの資格を有すること。

ア 運用に関する監査に必要な資格

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

イ 技術に関する監査に必要な資格

- (ア) 情報処理安全確保支援士
- (イ) 情報セキュリティスペシャリスト
- (ウ) 情報セキュリティアドミニストレータ
- (エ) 公認情報システムセキュリティプロフェッショナル (CISSP)

(3) 情報セキュリティ監査を実施する監査チームには、過去2年の間に国・地方公共団体に対し行われた情報セキュリティ監査業務の実務経験を有する者が1人以上含まれてい

ること。

- (4) 運用に関する監査を行う監査人のうち1人以上の者は、リモート監査の実務経験を有する者又はリモート監査に関する研修等を受講している者であること。
- (5) 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。

8 成果品と納品方法

業務完了時には県の示す様式の業務完了報告書（A4版縦、1枚）と、業務調整議事録（任意様式、A4版縦、1部）を提出すること。また、次の成果品を書面（任意様式、A4版縦、正副各1部）及び電子媒体（CD-R等）で提出すること。

- (1) 監査報告書（詳細版）
- (2) 監査報告書（公開対応版）
- (3) 監査結果総括報告書
- (4) 監査調書

9 データファイル等の返却及び破棄

- (1) 業務完了時には、監査及びその他の業務の実施に際して収集した一切の物及び電磁的記録（以下「データファイル等」という。）を実施担当者に引き渡し、それらに対する所有権、著作権及びその他一切の権利を放棄すること。
- (2) 受託業者が電子的に複製等を行い保有するデータファイル等については、業務完了時には返却もしくは廃棄し、データファイル等返却（廃棄）証明書を書面により提出すること。

10 再委託の制限

- (1) 契約の全部の履行を一括又は分割して第三者に委任し、又は請負わせることはできない。また、以下の業務（以下「契約の主たる部分」という）については、その履行を第三者に委任し、又は請負わせることはできない。ただし、これにより難い特別な事情があるものとして県が書面で認める場合は、これと異なる取扱いをすることがある。

○ 留意事項

「契約の主たる部分」とは、契約金額の50%を超える業務、企画判断、管理運営、指導監督、確認審査などの統括的かつ根幹的な業務のことをいう。

- (2) 再委託の相手方の制限

本契約の競争入札参加者であった者に契約の履行を委任し、又は請負わせることはできない。また、指名停止措置を受けている者、暴力団員又は暴力団と密接な関係を有する者に契約の履行を委任し、又は請負わせることはできない。

(3) 再委託の承認

契約の一部を第三者に委任し、又は請負わせようとするときは、あらかじめ書面による県の承認を得なければならない。

1 1 著作権

- (1) この契約に基づいて制作された成果物の所有権・著作権等は、沖縄県に属するものとする。
- (2) 成果物に第三者が権利を有する著作権が含まれている場合は、受託者は当該著作権の使用に関する負担金の一切の手続きを行い、第三者の著作権その他の権利を侵害してはならない。

1 2 注意事項

- (1) 本業務によって県の業務に支障がでないように留意すること。
- (2) 業務上必要となる情報については厳重に取り扱い、漏えい等が発生しないように留意すること。
- (3) 委託業務の実施にあたり、本仕様書に記載のない事項及び内容を変更する必要がある場合は、双方協議の上、決定し変更するものとする。