平成３０年度情報セキュリティ対策強化業務委託仕様書

１　業務名称

情報セキュリティ対策強化業務委託

２　目的

宮崎県庁における情報システムの運用体制、セキュリティの状況等について、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、より適切な運用体制の構築やセキュリティ対策の維持向上を図る。

３　業務内容

次のとおり助言型の情報セキュリティ外部監査に関する支援を実施する。

（１）情報セキュリティ外部監査

①監査実施計画
②監査説明会
③運用系監査
④技術系監査
⑤監査報告書の作成
⑥監査報告会
⑦指摘事項改善計画に関するフォロー

４　業務履行の場所及び期間

（１）場所 宮崎市橘通東２丁目１０番１号 宮崎県庁

（２）期間 契約締結の日から平成３０年１２月２８日（金）まで

５　監査対象

情報セキュリティ監査を実施する対象は、別表（平成３０年度情報セキュリティ外部監査 対象所属及びシステム一覧）のとおりとする。なお、個人番号を扱う２システムについては、技術監査は行わないものとする。

６　適用基準

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。

（１）宮崎県情報セキュリティ基本方針

（２）宮崎県情報セキュリティ対策基準

（３）一般業務用パソコン管理要領
（４）県庁ＬＡＮ－ＷＡＮ運用管理要領
（５）宮崎県外部記録媒体管理要領
（６）宮崎県ソフトウェア資産管理基準
（７）特定個人情報の適正な取扱いに関するガイドライン（個人番号利用事務のみ対象）
（８）宮崎県における特定個人情報等に関する取扱規程（個人番号利用事務のみ対象）

なお、（１）から（８）については、情報提供は可能とする。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次の①に掲げるいずれかの資格又は②に掲げる いずれかの資格を有していること。また、運用系監査を行う監査人のうち半数以上の者は①に掲げるいずれかの資格を有すること。

なお、技術系監査を行う監査人のうち半数以上の者は、②に掲げるいずれかの資格を有すること。

①運用系監査に必要な資格
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

②技術系監査に必要な資格
ア　情報セキュリティアドミニストレータ
イ　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人には、平成２５年度以降に国及び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）本業務を実施する監査人が過去に宮崎県における情報システムの企画、開発、運用、保守作業及び機器の提供に直接又は間接的に携わっている者でないこと。

８　委託業務の実施方法

受託者は、次に記載する業務を実施すること。

（１）情報セキュリティ外部監査

①監査実施計画

契約締結後速やかに、次の事項を含む監査の手順及びその実施時期を具体的に記載した監査実施計画書を提出し、県の実施担当者（以下「実施担当者」という。）の承認を得なければならない。また、監査実施計画書の提出に合わせて、受託業務の価格 内訳書を提出すること。

なお、この内訳書により発注者及び受託者は拘束されないものとする。

ア　業務工程表の作成
イ　予備調査実施方法の要領
ウ　本調査実施方法の要領
エ　監査責任者及び監査人の資格一覧
オ　調査実施場所ごとの調査時期（現地調査は定例議会開会中を避けること）
カ　収集する監査証拠の範囲
キ　特段の評価方法がある場合はその方法
ク　評価日
ケ　監査の協議日時及び内容
コ　監査結果の報告日時及び内容
サ　その他本件監査に必要な事項

なお、受託者は監査の目的を達成するため、監査の進行に伴い、監査実施計画を実施担当者と協議の上、変更することができる。

②監査説明会

監査対象所属を集めた監査説明会において、監査実施内容や手法等について説明を行うこと。

③運用系監査

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、現地調査等は同日に行うこと。
イ　前項の調査等における所要時間は３時間から４時間を見込むこと。なお、調査等の実施においては、システムの実態に合わせて所要時間を検討し、実施担当者と協議の上、決定するものとする。また、調査等の時間配分等は監査人が判断すること。

ウ　業務の実施に当たって、監査調書を作成すること。
エ　監査人は、２名体制とすること。

④技術系監査
ア　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。
イ　疑似侵入検査（オンサイト検査）は、原則として庁内のネットワークに接続した端末から実施すること。庁内ネットワークから接続できない情報システムについては、インターネットを経由した疑似侵入検査を実施すること。なお、対象となるＩＰアドレス数は１０を予定しており、疑似侵入検査にＷｅｂアプリケーション診断は含まない。
ウ　検査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、速報を行うこと。
エ　検査を実施する際には、対象とする情報システム及び庁内ネットワークの運用に対し、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。

⑤監査報告書の作成
ア　監査報告書は、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（紙面サイズ的にはＡ４相当）としても構わない。
イ　報告書の宛先は、情報セキュリティ監査実施責任者とすること。
ウ　監査報告書は、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。
エ　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。
オ　改善指摘事項等については、具体的な改善提案を記載すること。特に、疑似侵 入検査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。
カ　監査結果は、県が用意する様式を用いて総括表としてまとめること。
キ　監査結果の総合的な分析をし、主要な課題の抽出及び改善案をまとめること。
ク　改善計画策定及び改善計画実施等を確認するために利用する指摘事項ごとの指 摘事項改善計画書シートを作成すること。

ケ　今回実施した情報セキュリティ監査の状況及び情報システムを取り巻くリスクの現状について整理し、情報システムの技術的なセキュリティ対策向上につながる追加方策について総括的な改善提案をまとめること。

⑥監査報告会

ア　平成３０年１１月頃に開催予定の監査対象所属等を集めた監査報告会において、運用系監査及び疑似侵入検査それぞれにおける監査結果の概要、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　特に技術系監査の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。

ウ　運用系監査及び技術系監査の両方について報告を行うことができるよう、それぞれについて専門の知識のある要員を派遣すること。

⑦指摘事項改善計画に関するフォロー

ア　受託者は、監査対象所属から監査実施後、随時提出される指摘事項改善計画の案について、内容（改善方法、方針等）を確認し必要な改善がなされるよう支援（主に電話、電子メールを用いたもの）すること。

イ　支援対応する期間は、業務履行期間内とする。

９　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（サイズＡ４、１枚）を提出すること。

また、次の成果品を書面（Ａ４版縦）及び電子媒体（ＣＤ－ＲＯＭ等）で提出すること。

（１）情報セキュリティ外部監査

①監査報告書（書面１部・電子媒体１部）

ア　監査報告書（詳細版）

イ　監査報告書（公開対応版）

ウ　監査結果総括表

１０　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、次の証明書を提出すること。

・データファイル等返却（廃棄）証明書 書面１部

１１　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）情報の取扱については厳重に取り扱い、漏えい等の発生しないように留意すること。

（３）この委託業務を第三者に再委託してはならない。

（４）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実施担当者と協議の上決定するものとする。