令和２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

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する。また、訓練用の標的型メールを用いた擬似訓練を実施する。

実施後、問題点の抽出、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及び職員のサイバー攻撃への意識向上を図る。

３　業務内容

実施する業務は、次のとおりとする。詳細は「７　業務の実施方法」を確認すること。

（１）情報セキュリティ外部監査

別表（令和２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）に掲げる１７システムの技術系監査（脆弱性診断）を行う。

（２）システム管理者の自己チェックリスト作成

システム管理者に配布し、システムの運用・管理に関する自己チェックを行うためのチェックリストを作成、提供する。（配布、とりまとめ等は不要。）

（３）標的型メール擬似訓練

約６，０００アドレス（全職員＋代表アドレス）に対し、１１月と２月に擬似メールを送信する。

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 契約締結の日から令和３年３月１２日（金）まで

５　適用基準

本業務の内、情報セキュリティ外部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又は破棄すること。

６　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からケいずれかの資格を有していること。また、技術系監査を行う監査人のうち半数以上の者は、カからケいずれかの資格を有すること。
・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
カ　ネットワークスペシャリスト
キ　情報セキュリティスペシャリスト
ク　情報処理安全確保支援士
ケ　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２７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。

7　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１４日以内に、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　調査実施システムごとの調査時期（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

宮崎県庁で開催予定の監査対象所属等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　擬似侵入検査（オンサイト検査）は、インターネットを経由して実施すること。（Ｗｅｂアプリケーション診断を含む。）なお、対象となるＩＰアドレス数は１７を予定している。 必ずしも宮崎県庁において実施する必要はない。

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の担当者及び保守業者と連絡を密に行い、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。

④監査報告書の作成

ア　監査報告書の宛先は、実施担当者とすること。

イ　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。

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　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、擬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。

オ　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。

カ　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。

キ　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。

ク　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。

⑤監査報告会

ア　令和２年１月頃にリモートで開催予定の監査報告会において、技術監査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　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　監査報告会については、専門知識のある要員が説明を行うこと。

⑥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。

（２）システム管理者のチェックリスト作成

ア　監査対象システムの管理者が自らシステムの運用・管理に関する事項を点検できるよう、適用基準をもとに汎用的なチェックリストを作成すること。

イ　各チェック項目の評価及び説明等をまとめた資料を作成すること。チェックリスト及び説明資料の配布は、実施担当者が行う。

ウ　チェックリスト及び説明資料については概ね１００項目程度とし、専門的な知識の少ない職員を対象として、分かりやすい資料の作成に努めること。

（３）標的型メール擬似訓練

①訓練実施計画（契約締結後１４日以内）

ア　計画策定協議（１回）をリモートで実施し、以降はメール、電話、リモートで協議を行うこと。

イ　訓練実施計画書を作成し、実施担当者の承認を得ること。

また、訓練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。ただし、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。なお、受託者は訓練の目的を達成するため、訓練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事前準備

ア　訓練用標的型メールの作成

添付ファイルのパターンとインターネットサイトへのリンクを組み込んだパターンの２種類を作成すること。また、第２回擬似訓練では、添付ファイル、インターネットサイトへのリンクを開くと画面表示が変わる（ウイルスに感染した画面を表示する。）よう、設定を追加すること。

訓練用メールのパターン毎に、５種類程度のメール本文案を作成すること。

イ　教育用コンコンテンツの作成（Microsoft 社 Powerpoint ５頁程度）

開封者及び職員全員に配布する標的型メールのセキュリティ対策教育コンテンツを作成すること。

開封者へのコンテンツ配信は、訓練用標的型メール（以下「擬似訓練メール」という。）開封時に配布すること。職員全体へのコンテンツ配信は訓練終了後、実施担当者が行う予定。

ウ　メールサーバ等の整備

擬似訓練メールを送信するドメインの設定を行い、メールサーバを用意すること。また、送信用プログラムを作成し、送信スケジュールに基づいてメール送信ができるようにすること。

なお、メールサーバにおいては、「SMTP Authentication」、「SMTP over SSL」、「第三者中継の禁止」、「ウイルス対策ソフト導入」等のセキュリティ対策を実施すること。

エ　送信スケジュール

送信スケジュールは、職員の情報（職員番号、所属）を基に個別に設定できること。

オ　ＷＥＢサーバの準備

開封者に対する教育コンテンツを表示するＷＥＢサーバを用意し、期間中のコンテンツ掲示と問合せ対応（１次対応のみ）を実施すること。

また、開封者の情報（職員番号、所属）についてＷＥＢサーバ上に記録できるプログラムを作成すること。

ＷＥＢサーバは、宮崎県庁からのみアクセスができるようにアクセス制御を実施すること。

ＷＥＢサーバにおいて「ウイルス対策ソフト導入」等のセキュリティ対策を実施すること。

カ　アンケートの作成

課題および対策を抽出するために必要な職員へのアンケート案を作成すること。なお、職員へのアンケートについては、実施担当者が訓練後に実施する。

③訓練の実施

ア　委託業務の期間中に全職員に対して、訓練用標的型メールを２回送信すること。なお、各回の送信については日時とメール本文を変え、最大５グループに分けて送信を行うこと。

イ　動作確認テストの実施

擬似訓練メールを用いた一連の動作について確認テストを実施し問題が無いことを確認すること。

ウ　擬似訓練メールの送信

受信側のメールサーバ負荷を考慮しながら擬似訓練メールを送信すること。送信側のメールサーバは対象者に一斉送付する能力を持たせること。

エ　情報収集と分析の実施

訓練で収集した開封者の情報と、訓練後に実施する職員アンケートについて、開封者の情報（職員番号、所属）とその取った行動などについての分析を行うこと。なお、未開封者に対する分析についても行うこと。

④結果報告

ア　訓練の目的、訓練対象者、実施手順、実施結果（集計）、アンケート結果、総括、今後の課題および対策案等について実施担当者と協議した上で、報告書としてまとめること。

イ　実施担当者に対して訓練結果報告（宮崎県庁において２時間程度１回）を行うこと。

8　成果品と納品方法

業務完了時には、県の示す洋式の業務完了報告書（Ａ４縦）を１部提出すること。また、次の成果品を、書面（Ａ４縦）及び電子媒体（ＣＤ－ＲＯＭ等）で各１部提出すること。

（１）情報セキュリティ外部監査

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

（２）標的型メール擬似訓練

ア　実施計画書

イ　訓練用標的型メール

ウ　教育用コンテンツ

エ　実施報告書

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、業務完了時に返却または廃棄し、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

１０　注意事項

（１）本業務によって県の業務に支障が出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。

（５）本業務の内、標的型メール擬似訓練について、擬似訓練メールは送付先の個人を第三者が特定できないように留意すること。

（６）本業務の内、標的型メール擬似訓練について、擬似訓練メールの添付ファイルに関して、実行しても対象者の端末に影響を与えないこと。