

令和7年度沖縄県情報セキュリティ外部監査業務に係る質問及び回答について

令和7年8月13日

沖縄県企画部情報基盤整備課

No.	資料名・項目	質問内容	回答
1	仕様書 3 業務内容(2)	仕様書ではセキュリティ診断は、情報セキュリティ外部監査に含まれているように見えますが、計画書をセキュリティ診断個別に作成しても問題ないでしょうか。	セキュリティ診断は、情報セキュリティ外部監査の業務に含まれているため、セキュリティ診断も含めて監査実施計画書の作成をお願いします。
2	仕様書 3 業務内容(3)	情報セキュリティ外部監査は令和8年1月実施でも問題ないでしょうか。 また、セキュリティ診断は令和7年12月実施でも問題ないでしょうか。	監査実施後の監査報告書等の作成、指摘事項改善計画書に関するフォローを行う期間、本県の議会日程等を考慮し、情報セキュリティ外部監査は令和7年10月～11月実施としております。 そのため、要件に変更はありません。 また、セキュリティ診断も令和7年10月～11月実施としております。
3	仕様書 3 業務内容(3)ア	セキュリティ診断の内容はプラットフォーム診断(サーバ診断)、Webアプリケーション診断の2種類で良かったでしょうか。	仕様書のとおりセキュリティ診断は脆弱性調査、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としております。 なお、疑似侵入調査は、プラットフォーム診断による脆弱性診断等を想定しています。
4	仕様書 3 業務内容(4)ア	監査報告書は、監査対象課毎に個別に作成し、監査結果報告書は監査報告書の総括版という認識で間違いなかったでしょうか。	監査報告書は、 <u>監査対象システム毎</u> に個別に作成をお願いします。 また、ご認識のとおり監査結果報告書は監査報告書の総括版となります。
5	仕様書 5 監査対象(1)	セキュリティ診断におけるWebアプリケーション診断の対象画面数をご教示ください。	Webアプリケーション診断は、診断ツールを用いたものを想定しています。よって手動診断による画面遷移等が生じないため、対象画面数の提示をする予定はありません。

No.	資料名・項目	質問内容	回答
6	仕様書 8 成果品と納品方法	監査結果総括報告書とは監査結果報告書のことでしょうか。	ご認識のとおりです。
7	仕様書 8 成果品と納品方法	仕様書ではセキュリティ診断は、情報セキュリティ外部監査に含まれているように見えますが、報告書(詳細版／公開版)、監査結果総括報告書をセキュリティ診断個別に作成しても問題ないでしょうか。	セキュリティ診断に関する報告書(詳細版／公開版)、監査結果総括報告書等の作成方法については、契約締結後に詳細を調整する予定です。
8	仕様書 3 業務内容(7)ウ	Web会議形態での研修でロールプレイ演習は受講者への適切なアドバイスやQAに対応しにくいと思われます。情報基盤整備課様に講師サポートとして動いていただくか弊社講師が貴庁で研修を行う等、受託後に方法をご検討いただくことは可能でしょうか。	内部監査人向け研修については、契約締結後に研修の方法等を調整することは可能です。なお、講師サポートについて、当課はお受けいたしかねるため、必要な場合は貴社にて要員を確保いただきますようお願いいたします。
9	仕様書 3 業務内容(7)ウ	内部監査員研修の時期はいつ頃を想定されていますでしょうか。またこの研修を受講された方は本外部監査にどのように関わられる予定でしょうか。	11月～12月頃の開催を想定しております。また、この研修を受講した者は、内部監査の監査人となる予定ですが、本外部監査に直接関わることはありません。
10	別紙4 入札保証金説明書 3 入札保証金の免除 「過去2年の間に履行期限が到来した2つ以上の契約を全て誠実に履行したことを証明する書類(様式第1号)」	当該業務の契約書の写し(仕様書内容含む)の提出により、証明する書類を満たすとの解釈で良いでしょうか。	ご認識のとおりです。

No.	資料名・項目	質問内容	回答
11	別紙4 入札保証金説明書 5 現金で納付する場合の納付方法	「債権・債務者登録申出書」を提出後、納付書はPDF等の書式を電子メールで弊社へ送付頂けるという認識で良いでしょうか。 また、記載「納付場所」は、沖縄県以外の店舗での入金でも良いでしょうか。	入札参加業者から「債権・債務者登録申出書」が提出された後、当課において「債権・債務者登録申出書」に基づき納入通知書を発行します。 納入通知書を郵送しますので、指定の納付場所において納付をお願いします。 また、沖縄県外では、みずほ銀行で入金が可能となっております。
12	件名:令和7年度沖縄県情報セキュリティ外部監査業務の一般競争入札の公告 4 申請の方法等 (1)申請の方法 イ 法人の登記事項証明書	原本でなくとも、写しの提出で良いでしょうか。	原本の提出をお願いします。
13	件名:令和7年度沖縄県情報セキュリティ外部監査業務の一般競争入札の公告 4 申請の方法等 (1)申請の方法 カ 公告2(3)に関し、過去2カ年間に2件以上の契約履行実績を証する書類	当該自治体様との契約書の写し(仕様書内容を含む)の提出で良いでしょうか。	ご認識のとおりです。
14	04_別紙2_R7仕様書.pdf 3.(3) 情報セキュリティ外部監査の実施(10月～11月) 4.(1)場所	3 業務内容 (3)情報セキュリティ外部監査の実施(10月～11月) においては、「現地調査」という記載があるが、4 業務履行の場所及び期間(1)場所 においては、「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。」とある。現地訪問なしのリモートのみでの監査は可能か。	セキュリティ診断については、リモートでの実施となることを想定しておりますが、ヒアリングを含む現地調査については、リモートでの実施にそぐわない場合も想定されることから、実地(現地訪問)によるものとさせていただきます。
15	04_別紙2_R7仕様書.pdf 3.(4)監査報告書等の作成-イ	監査報告書(公開対応版)について、報告内容として必ず含めるべき点は何かご回答願いたい。	報告内容として以下の項目を含めるようお願いいたします。 ・監査の目的 ・監査対象 ・監査方法 ・監査項目 ・適用基準 ・監査結果(件数、総評)

No.	資料名・項目	質問内容	回答
16	04_別紙2_R7仕様書.pdf 3.(4)監査報告書等の作成-エ	「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」とあるが、インターネットから確認できる範囲で提示可能な対処方法か、または具体的な内部仕様を踏まえた対処方法のどちらを明示する必要があるかご回答願いたい。	インターネットから確認できる範囲で提示可能な対処方法でお願いします。
17	04_別紙2_R7仕様書.pdf 3.(5)指摘事項改善計画に関するフォロー	指摘事項改善計画書の作成については、セキュリティ診断についても作成対象であるとの認識で相違ないか。	ご認識のとおりです。
18	04_別紙2_R7仕様書.pdf 4.業務履行の場所及び期間	セキュリティ診断行為が許容される曜日・時間帯はいつか。 特に、夜間・休日に実施日時が限定される可能性についてご回答願いたい。 またこの回答に当たっては、ツールを利用することによる大量の PACKET 送付と、手作業による一般利用相当の PACKET 送付それぞれを区別して回答いただきたい。	いずれの PACKET 送付を行う場合でも、平日の勤務時間内に実施することを想定しており、休日・勤務時間外の監査実施は予定していません。
19	04_別紙2_R7仕様書.pdf 3.(3) 情報セキュリティ外部監査の実施(10月～11月) 4.業務履行の場所及び期間 5.監査対象	セキュリティ診断について、実施期間10月～11月の範囲内で監査対象に含まれる情報システム全ての診断を完了するもの、という認識で相違ないか。	ご認識のとおりです。
20	04_別紙2_R7仕様書.pdf 3.(3) 情報セキュリティ外部監査の実施(10月～11月)-ア、カ 5.監査対象	セキュリティ診断に疑似侵入調査が含まれているが、これは発見された脆弱性に対して実際に侵入を行うことを意図したものか、もしくは侵入は行わずその可能性があることの調査に留めるものであるか、ご回答願いたい。	疑似侵入調査は、プラットフォーム診断による脆弱性診断等を想定しています。

No.	資料名・項目	質問内容	回答
21	04_別紙2_R7仕様書.pdf 3.(3) 情報セキュリティ外部監査の実施(10月～11月)ーケ 5.監査対象(1)	「セキュリティ診断の対象となるIPアドレス数は合計で5つ程度」とあるが、それぞれどのような用途で用いられるものであるか。	監査対象システムについては、調整中のため、契約締結後に監査対象システムの資料を提供する予定です。
22	04_別紙2_R7仕様書.pdf 3.(3) 情報セキュリティ外部監査の実施(10月～11月)ーケ 5.監査対象(1)	「セキュリティ診断の対象となるIPアドレス数は合計で5つ程度」とある。「程度」とIPアドレス数が増減する可能性を示しているが、これは対象所属との調整結果によって増減する可能性があるとの認識で相違ないか。	ご認識のとおりです。
23	04_別紙2_R7仕様書.pdf 3.(3) 情報セキュリティ外部監査の実施(10月～11月)ーサ	「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。」とあるが、不慮の事態に備えた対象のバックアップ、リカバリを計画として含めることは可能であるか。	不慮の事態に備えて、対象とする情報システムのバックアップ、リカバリ等の実施を計画として含めることは困難なため、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に支障及び損害を与えないようにお願いします。
24	04_別紙2_R7仕様書.pdf 5.監査対象(1)	「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」とある。「最大」とあるが、これは対象所属との調整結果によって3システム未満が対象となる可能性を示しているとの認識で相違ないか。	ご認識のとおりです。
25	04_別紙2_R7仕様書.pdf 5.監査対象(1)	「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」とあるが、対象とする予定であるシステムそれぞれについて以下の点をご回答願いたい。 ・どのような用途で用いられるか。 ・Webアプリケーションである場合、その規模はどの程度か。規模の指標としては、リクエスト数、API本数、画面数等をもとにご回答願いたい。 ・既に対象が決定している場合、WebアプリケーションのURLをご回答願いたい。 ・診断は本番環境に対して行う認識でよいか。	監査対象システムについては、調整中のため、契約締結後に監査対象システムの資料を提供する予定です。 また、ご認識のとおり診断は本番環境に対して行う予定です。

No.	資料名・項目	質問内容	回答
26	04_別紙2_R7仕様書.pdf 5.監査対象(1)	セキュリティ診断の対象となるシステム内にREST APIではなく、GraphQLやgRPC等を使用している通信が含まれているか。	監査対象システムについては、調整中のため、契約締結後に監査対象システムの資料を提供する予定です。
27	04_別紙2_R7仕様書.pdf 5.監査対象(1)	セキュリティ診断の対象となるシステムについて、スマートフォン向けネイティブアプリケーションがその対象範囲に含まれるシステムはあるか。	監査対象システムについては、調整中のため、契約締結後に監査対象システムの資料を提供する予定です。
28	04_別紙2_R7仕様書.pdf 5.監査対象(1)	セキュリティ診断の対象となるWebアプリケーションシステムについて、ログイン機能が存在するか。存在する場合、以下の点についてご回答願いたい。 ・1ユーザー当たりの同時ログイン可能な数に制限はあるか。 ・1ユーザーにつき、単位時間当たりのログイン回数に制限はあるか。(例:1時間に1000回以上のログイン不可) ・多段階、多要素認証の実装を持つシステムは含まれるか。	監査対象システムについては、調整中のため、契約締結後に監査対象システムの資料を提供する予定です。
29	04_別紙2_R7仕様書.pdf 5.監査対象(1)	セキュリティ診断の対象について、IPSやWAF等のセキュリティ装置、ソフトの使用は行っているか。行っている場合は以下の点について可能な範囲でご回答願いたい。 ・具体的にどのような装置、ソフトを利用しているか。 ・攻撃の兆候を含む通信に対する挙動はどのようなものであるか。また、それが著しくセキュリティ診断の妨げとなる場合、部分的に設定を緩和するような措置を取ることが可能であるか。	監査対象システムについては、調整中のため、契約締結後に監査対象システムの資料を提供する予定です。
30	04_別紙2_R7仕様書.pdf 5.監査対象(1)	セキュリティ診断の対象について、その設置場所(オンプレ、ホスティング、IaaS、PaaS等)が貴県の管理する所ではない場合、その設置場所の管理者に診断を行う許諾を既に得ているか、もしくは診断実施までに得られるものと認識して問題ないか。	診断実施までに承諾を得る予定です。

No.	資料名・項目	質問内容	回答
31	04_別紙2_R7仕様書.pdf 5.監査対象(1)	セキュリティ診断の対象について、「ロードバランサ等を利用した冗長化」を行っているか。	監査対象システムについては、調整中のため、契約締結後に監査対象システムの資料を提供する予定です。
32	04_別紙2_R7仕様書.pdf 5.監査対象(1)	セキュリティ診断の対象となるWebアプリケーションシステムについて、ReCAPTCHAのような「自動化されたツールによるアクセスを妨げる実装」を行っているか。行っている場合、診断時にそれらが無効化することが可能かご回答願いたい。	監査対象システムについては、調整中のため、契約締結後に監査対象システムの資料を提供する予定です。
33	04_別紙2_R7仕様書.pdf 5.監査対象(1)	セキュリティ診断の対象となるWebアプリケーションシステムについて、外部組織が提供するWebアプリケーションとの連携機能は存在するか。もし存在する場合、その連携先を診断対象に含める想定であるかご回答願いたい。	監査対象システムについては、調整中のため、契約締結後に監査対象システムの資料を提供する予定です。
34	04_別紙2_R7仕様書.pdf 5.監査対象(1)	セキュリティ診断の対象となるWebアプリケーションシステムについて、データの登録、更新、削除といった処理を実施することに問題はないか。	Webアプリケーションシステムのセキュリティ診断において、データの登録、更新、削除を行うことは想定しておりません。
35	04_別紙2_R7仕様書.pdf	セキュリティ診断実施後の対処が無事完了したことを確認するための「再診断」の実施を希望するか。また希望する場合、「再診断」対象となる基準(危険度等)をご回答願いたい。	再診断は予定しておりません。

No.	資料名・項目	質問内容	回答
36	03_別紙1_契約書案 04_別紙2_R7仕様書	契約不適合責任の期間について、契約書案、仕様書案に該当が見当たらないが、契約不適合責任の期間について落札者業者と検討され追記、修正頂くことは可能か。別途協議となるか。	契約書に契約不適合責任の条項を追記することについては、落札業者と調整することとします。
37	03_別紙1_契約書案	損害賠償に関する上限について、損害賠償)第12条の上限設定について落札者業者と検討され追記、修正頂くことは可能か。別途協議となるか。	契約書に損害賠償に関する上限を追記することについては、落札業者と調整することとします。
38	仕様書 6 適用基準	個人番号利用事務システムの適用基準について	仕様書の「6 適用基準」に「ク 知事部局が保有する特定個人情報等の管理要綱」を追加します。 そのため、添付ファイルの仕様書を差し替えております。