兵庫県情報システム外部監査業務委託仕様書

令和５年７月

兵庫県企画部デジタル改革課

兵庫県情報システム外部監査業務委託仕様書

１　概要

兵庫県（以下「県」という。）では情報システムのセキュリティ確保のため、外部からのサイバー攻撃に備えるための技術的セキュリティ監査を外部事業者に委託し、その他の監査項目については県内部で対応してきた。

しかし、県における事前承認手続きを経ていない情報システム開発業務の再委託事案や、県内自治体における業務受託業者による個人情報の大量紛失事案の発生を受け、運用管理体制や個人情報の管理方法のチェック等、物理的・人的セキュリティ等に着目した監査をさらに徹底する必要が生じ、令和４年度に外部専門家による外部監査を実施した。定期的な監査による情報セキュリティ向上のため、本年度も監査を実施する。

本仕様書は、県情報システムのセキュリティが適正に確保されているか否かを物理的・人的セキュリティを中心に点検・評価し、問題点の確認、改善方法等についての検討・助言・指導を行うことを目的とする情報システム外部監査業務委託契約（以下「本契約」という。）にあたり、発注者である県と受託者の間において、詳細な仕様を定めるものである。

２　委託期間

契約締結日から令和６年３月 29 日まで

３　履行場所

県庁第３号館 12・13 階（兵庫県企画部デジタル改革課）、
監査対象システム設置場所他

４　受託者の要件

（１）資格要件

監査責任者、監査人等で構成される監査チームを編成すること。また同チームには、情報セキュリティ監査に必要な知識及び経験（地方公共団体における情報セキュリティ監査の実績）を持ち、次に掲げるいずれかの資格を有する者が１名以上含まれていること。

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
オ　ISMS 審査員
カ　公認情報セキュリティ主任監査人

キ　公認情報セキュリティ監査人
ク　情報処理安全確保支援士

（２）実績要件
監査チームには、監査の効率と品質の保持のため、次のいずれかの実績（実務経験）を有する専門家が、上記（１）とは別に１名以上含まれていること。

ア　情報セキュリティ監査
イ　情報セキュリティに関するコンサルティング
ウ　情報セキュリティポリシーの作成に関するコンサルティング（支援を含む）

（３）入札参加要件
受託者（企業グループの構成員を含む）及び再委託先事業者（県の承認がある場合。詳細は後述）は、監査対象の情報システムの開発・運用・機器等の調達等（ただし、企画・コンサルティング・調達支援のみの場合は除く）には参加していないこと。

５　監査対象
別紙１「監査対象システム一覧」のとおり。
ただし契約締結後、セキュリティインシデントの発生等、監査対象を別システムに変更すべき事由が生じた場合は、県と受託者双方協議のうえ、監査対象を変更することがある。

６　監査基準
（１）必須とする基準
ア　県情報セキュリティ対策指針（以下、「県指針」という。）
イ　県行政情報ネットワーク運用管理要綱

（２）参考とする基準
ア　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
イ　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
ウ　各監査対象システムの運用管理要綱
エ　その他情報セキュリティに関し有用な基準等は、県と協議のうえ採用すること。

７　業務内容
（１）監査計画の策定
受託者は、契約締結後２週間以内に、県に次の事項を含む監査手順及びその実施時期を記載した「監査実施計画書」を提出し、承認を得ること。

ア　監査対象及び範囲
イ　実施方法
ウ　実施スケジュール
エ　監査の実施体制
オ　進捗管理及び報告方法
カ　監査結果の報告の日時・内容
キ　その他、監査実施時に必要な事項

（２）書面監査の実施

ア　調査票（チェックシート）の作成

（ア）書面監査のため、監査対象システムの業務主管課に配布し、情報システムの状況を照会する、調査票（チェックシート）を作成すること。なお、調査票の監査項目は、前年度監査結果との比較を想定し、原則として令和４年度調査票（別紙２）と同じ項目を含むこととし、監査対象システムの性質上、固有の項目が追加となる場合は別紙として作成すること。

（イ）調査票は、県指針等への対応を中心に項目を設定すること。ただし、単に県指針等の各項目を列挙するのではなく、同指針等で求められている内容を、必ずしも情報システムに習熟しているとは限らない業務主管課の担当職員にも分かりやすい表現に落とし込みながら、監査に必要な情報を得られる内容とすること。

（ウ）調査票の内容については、配布前に県に提出し、承認を得ること。

（エ）業務主管課への調査票の配布は県が行うが、業務主管課からの質問受付とその回答、調査票の回収、追加資料の依頼等は、原則として受託者が業務主管課と直接行うこととし、県に適宜状況を共有すること。ただし、業務主管課との応対で疑問等が生じた場合は、業務主管課への連絡前に県に相談することとする。

（オ）書面監査にあたり、監査対象システムの運用管理要綱、仕様書や完成図書等の資料収集が必要な場合は、調査票に必要となる資料を明記し、業務主管課に提出を求めること。

イ　調査票の分析・評価

調査票の回答内容を基に監査を行うこと。

（３）実地監査の実施

ア　書面監査の結果、または県と受託者との協議の結果、より詳細な監査の必要性が認められたシステムについて、業務主管課へのヒアリング、当該システムの運用管理に係る各種帳簿等の追加チェックや現地調査（必要な場合）等を行う、実地監査を実施すること。

イ　実地監査の対象システム数は 10 を上限とする。

ウ　業務主管課との調整（日程や場所等）は県が中心となって実施するが、受託者もこれに協力すること。また、ヒアリング項目の作成や監査対象となる帳票等の指定については受託者で対応すること。

エ　実地監査に際し、直接システムの設置場所を確認する必要がある場合は、これに対応すること。なお、業務主管課へのヒアリングについては原則対面での実施とするが、やむを得ない理由がある場合はWeb会議等による実施も可とする。

（４）技術監査の実施

ア　下記の脆弱性検査ツール（ネットワークスキャナ）から最低１つを選択して使用し、ハードウェア・ソフトウェア等の脆弱性、修正プログラムの適用の有無等を確認するとともに、発見された脆弱性について具体的な解決方法を提示すること。

・Nessus
・Penetrator Vulnerability Scanner
・QualysGuard
・Rapid7 nexpose

イ　技術監査の対象となるサーバは、監査対象システムのサーバのうち代表的なものとする。ただし、インターネット上に公開されているサーバは別途監査を実施するため対象外とする。

ウ　技術監査の際には、以下の点に留意すること。

（ア）使用するツールは事前に書面で県に報告し、承諾を得ること。

（イ）ファイアウォールやフィルタリングシステムで隔てられた場所からではなく、県の指定する、対象サーバと同セグメントから監査を実施すること。

（ウ）対象サーバに障害を生じさせないよう、細心の注意をもって業務を行うこと。もし障害が発生した場合は、県に速やかに報告するとともに、障害の解消のため、県及び県庁WANや各情報システムの維持管理業者に協力して対応にあたること。

（エ）技術監査の実施中に、情報漏えい等につながる危険性が高い脆弱性等が検出された場合には、その内容及び改善策について速やかに県に報告すること。

（オ）技術監査においては、使用したツールのログや通信のログを取得するなど検査の内容を確実に記録し、県にログを提供すること。

（カ）県が必要と判断した場合、対象機器のログを確認すること。

（キ）県が必要と判断した場合、サーバ等の設定ファイル等を確認し、問題点を指摘するとともに改善策について助言を行うこと。

（５）監査結果の報告

ア　県への報告

書面監査、実地監査及び技術監査の結果を「情報セキュリティ監査報告書」としてまとめ、県に書面で報告すること。

同報告書は、各監査により検出された問題点や脆弱性等を指摘事項として示すとともに、指摘事項に対し、具体的な改善指導内容を記載すること。

改善指導内容については以下に例示するが、その他必要な内容があれば記載すること。

（ア）　運用管理要綱等の作成・修正の指導

監査の結果、監査対象システムの運用管理要綱等に作成・修正の必要がある場合は、その内容を具体的に示すこと。

（イ）　物理的・人的な脆弱性改善の指導

監査の結果、監査対象システムの物理的・人的な脆弱性が判明し、改善する必要がある場合は、改善案を具体的に示すこと。

（ウ）　システム上の脆弱性改善の指導

監査の結果、監査対象システム上の脆弱性が判明し、改善する必要がある場合は、改善案を具体的に示すこと。

また、同報告書は庁内で公開するため、全庁公開にそぐわない内容（セキュリティホールの詳細情報等）を省略した、庁内公開版の報告書を別途用意すること。

イ　業務主管課への説明

（ア）全ての監査対象システム毎にレポートを作成すること。

（イ）指摘事項が多数確認されたシステム等について、前号（ア）から（ウ）の内容を業務主管課に対面で説明すること。ただし、やむを得ない理由がある場合はWeb会議等による実施も可とする。

（ウ）（イ）の対象システムは県と受託者協議の上決定し、数は10を上限とする。

（エ）業務主管課との調整（日程や場所等）は県が中心となって実施するが受託者もこれに協力すること。

８　作業時間

（１）実地監査等、県の施設内で行う、又は県職員を直接対象とする作業については、原則として県の勤務時間内（休日を除く日の８時45分～17時45分）に行うこと。ただし、技術的監査については、対象サーバの利用用途や稼働時間等を考慮し、県と協議のうえ、作業時間を決定すること。

（２）その他、具体的な作業日時等については、県との協議のうえ決定すること。

９　再委託

（１）受託者は、委託業務の全部又は主体的部分（委託業務における総合的な企画及び判断並びに業務遂行管理部分）を一括して第三者に委任し、又は請け負わせてはならない。

（２）受託者は委託業務の一部を第三者に委任し、又は請け負わせ（以下「再委託等」という。）てはならない。ただし、あらかじめ再委託等の相手方の住所、氏名及び再委託等を行う業務の範囲等を記載した、再委託の必要性がわかる書面を県に提出し、県の書面による承認を得た場合は、受託者は、県が承認した範囲の業務を第三者に再委託等することができるものとする。

10　納品物

（１）成果物

以下の成果物を製本版、電子媒体それぞれ正副各１部納品すること。
ただし、エについては電子媒体のみとする。

ア　監査実施計画書
イ　情報セキュリティ監査報告書
ウ　情報セキュリティ監査報告書（庁内公開版）
エ　監査の過程で収集した各種ログ

（２）納品方法

ア　納入に必要な資材は、受託者において用意すること。
イ　製本版は原則としてA4判の用紙を使用し、種類別にチューブファイル等に収め、背表紙等には内容を簡記すること。ただし必要に応じてA3判で作成してもよい。
ウ　電子媒体はCD-ROM、DVD-ROM又はUSBメモリとすること。
エ　電子媒体に収録内容を簡記すること。
オ　電子データは、Microsoft Office 2016以降で編集できること。

11　留意事項

（１）契約不適合責任

引き渡された目的物が種類、品質又は数量に関して契約の内容に適合しない場合、県は受託者に対し、履行の追完を請求することができる。

履行の追完は、民法第562条第１項本文にかかわらず、代替物の引渡し又は不足分の引渡しの方法によること。

（２）機密保持

本業務遂行上知り得た情報を第三者に漏らしてはならない。また、本契約が終

了し、又は解除された後においても同様とすること。
なお、受託者が、個人情報など流出した場合に重大な損害が発生しうる情報を保持した場合は、完了報告までに、電子データの消去及び書類の廃棄又は返却を行い、書面で県に報告すること。

（３）法令等の順守
県指針等を順守すること。また、個人情報保護法等の法令及び契約書の別記「個人情報取扱特記事項」を遵守すること。

（４）知的財産の取扱い
ア　成果物及びこれに付随する資料は、全て県に帰属するものとし、書面による県の承諾を受けないで他に公表、譲渡、貸与又は使用してはならない。ただし、成果物及びこれに付随する資料に関し、受託者が従前から保有する著作権は受託者に留保されるものとし、県は、本業務の目的の範囲内で自由に利用できるものとする。
イ　本委託業務で得られた成果物の著作権（著作権法（昭和 45 年法律第 48 号）第 27 条、第 28 条の権利を含む。）を無償で県に譲渡すること。
ウ　本委託業務で得られた成果物に著作者人格権を行使しないこと。また、本委託業務で得られた成果物に第三者の著作者がある場合は、当該著作者に著作者人格権を行使しないように必要な措置をとること。
エ　本委託業務によって得られた成果物について、県が使用する権利及び県が第三者に使用を許諾する権利を無償で許諾すること。
オ　特許権、著作権等の知的財産権の対象となっている第三者の技術等を使用するときは、その使用に関する一切の責任を負う。また、それに関わる費用については受託者の負担とする。

（５）疑義の解釈
本仕様書に定めのない事項及び疑義の生じた場合には、県と受託者の協議により定めるものとする。

12　本契約担当課
県企画部デジタル改革課

連絡先：〒650-8567
兵庫県神戸市中央区下山手通５-10-１（県庁第３号館 12 階）
TEL　：078-341-7711（内線 2283）
FAX　：078-362-9027
Mail　：sysad@pref.hyogo.lg.jp

（別紙1）監査対象システム一覧

No.	システム名	部局名	所属名
1	議会LAN	県議会	総務課
2	公文書ファイル管理簿システム	総務部	法務文書課
3	名簿管理システム	総務部	秘書課
4	兵庫県職員福利厚生システム	総務部	職員課
5	兵庫情報ハイウェイ	企画部	デジタル改革課
6	庁内データ検索システム	企画部	デジタル改革課
7	兵庫県情報セキュリティクラウド（県庁WAN）	企画部	デジタル改革課
8	災害対応総合情報ネットワークシステム	危機管理部	災害対策課
9	高圧ガス製造事業所等管理システム	危機管理部	消防保安課
10	介護保険指定機関等管理システム	福祉部	高齢政策課
11	支援費制度指定事業所管理システム	福祉部	障害福祉課
12	国保事業費納付金等算定標準システム	福祉部	国保医療課
13	レセプト管理システム	福祉部	地域福祉課
14	兵庫県広域災害・医療救急情報システム	保健医療部	薬務課
15	肝がん入院医療費助成システム	保健医療部	疾病対策課
16	森林地理情報システム	農林水産部	林務課
17	農政環境部工事台帳システム	農林水産部	農林水産部　総務課
18	兵庫県流域下水道公営企業会計システム	土木部	下水道課
19	気象・海象観測情報システム	土木部	港湾課
20	兵庫県ＣＧハザードマップホームページ	土木部	技術企画課
21	高潮危険度予測システム	土木部	港湾課
22	適用業務システム 県民住宅ローン	まちづくり部	住宅政策課
23	企業庁財務会計システム	企業庁	企業庁：総務課
24	はりま姫路総合医療センター(旧姫路循環器病センター)電子カルテシステム	病院局	県立はりま姫路総合医療センター
25	加古川医療センター電子カルテシステム	病院局	県立加古川医療センター
26	病院事業財務会計システム	病院局	病院局：経営課
27	特別支援教育就学奨励費システム	教育委員会	財務課
28	校務支援システム	教育委員会	教育企画課
29	ひょうご図書館情報ネットワークシステム	教育委員会	社会教育課
30	兵庫県立美術館美術情報システム	教育委員会	社会教育課

＜備考＞

監査対象を別システムに変更すべき事由が生じた場合は、県と受託者双方協議のうえ、監査対象を変更することがある。

（別紙２）令和４年度 情報システム外部監査 調査票　記載例

システム名	○○システム
課室名	○×課
担当者名	○○　××
内線	内線○○○○

No	大区分	中区分	小区分	設問	回答	備考欄	提出物
1	情報資産の分類		情報資産の分類	情報資産をその内容に応じて分類し、その重要度に応じて分類していますか？	1.している		・情報資産管理台帳
2			実施手順	情報システムの適正な運用を図るために必要な情報セキュリティ対策の実施手順（システム運用管理要綱）を策定していますか？	2.概ねしている		・システム運用管理要綱
3			要綱	指針及び運営管理要綱の遵守状況を定期的に点検し、支障を認めた場合には迅速かつ適切な措置を講じていますか？	3.どちらとも言えない		
4	物理的セキュリティ対策	機器の設置	火災・水害、ほこり、振動等の排除	通信機器やサーバ等は、火災、水害、温度等の影響を可能な限り排除した場所に設置し、固定用ベルト、アンカーで固定する等の措置を講じていますか？	4.あまりしていない		
5			耐震、免震化	重要な通信機器やサーバ等を設置する場合に、機器の固定等の耐震対策だけでなく、免震ラックに設置する等の措置を講じていますか？	5.していない		
6			配線の保護	機器等の配線が損傷を受けないよう、カバー・収納管に収納するなどしていますか？	1.している		
7			接続口の隔離	ネットワークのスイッチやハブのネットワーク接続口は、第三者が容易に接続できないように、隠ぺい、閉鎖等の措置がされていますか？	2.概ねしている		
8		設置場所	設置場所	システム機器の設置場所はどこですか？【複数選択可】 1.○号館△階、2.○号館◇階、3.防災棟、4.庁内別サーバ室、5.執務室内、6.Nデータセンター、7.Fデータセンター、8.Cデータセンター、9.クラウド利用(AWS,Google,Azure等）、 10.LGWAN-ASP、 11.その他（具体的に）	☐ 1.○号館△階 ☑ 2.○号館◇階 ☐ 3. 防災棟 ☐ 4. 庁内別サーバ室 ☐ 5. 執務室内 ☑ 6.Nデータセンター ☐ 7.Fデータセンター ☐ 8.Cデータセンター ☐ 9. クラウド利用(AWS,Google,Azure等) ☑ 10. LGWAN-ASP ☐ 11. その他（具体的に備考欄へ記入）		
9			耐震、防火、防犯対策	情報システム室には、耐震対策、防火対策、防犯対策等の措置を講じていますか？	1.している		
10			入退室の管理	情報システム室の入退出はあらかじめ許可した者のみとし、入退室管理簿の記載等を行っていますか？	1.している		
11			入退室管理、名札・身分証明書の携帯	情報システム室に入室する者は、身分証明書等を携帯し、運用管理者の指定する担当職員の求めに従い提示していますか？	1.している		
12		情報資産の管理	データのバックアップの作成	重要な情報資産について、データのき損、滅失等に備えるため、保管するデータのバックアップを定期的に作成していますか？	2.概ねしている		
13			データの暗号化	機密性の高い情報を外部へ送信、提供する場合、必要に応じ暗号化又はパスワード設定を行っていますか？	2.概ねしている		
14		記録媒体の管理等	データの媒体又は電子メール等による持出し	個人情報、機密情報等が記録されたUSBメモリ、DVD、ハードディスク等の電子媒体を持ち出す場合は、データの暗号化、パスワードによる保護を行っていますか？	1.している		
15			記録媒体の廃棄	USBメモリ、DVD、ハードディスク等の電子媒体が不要となった場合は、データを復元できないように消去を行ったうえで廃棄していますか？	1.している		
16		IDおよびパスワードの管理	パスワード安全性１	パスワードの桁数は最低何桁以上ですか？	4. 7桁		
17			パスワード安全性２	パスワードは英数記号等を混在させていますか？	1.している		
18	人的セキュリティ対策	教育・訓練	情報セキュリティ対策に関する研修・普及啓発	システム利用者に情報セキュリティ研修、標的型攻撃訓練等を年1回以上受講させていますか？	3.どちらとも言えない		
19			不測事態に備えた訓練の計画的な実施	情報システム管理者、情報システム担当者がセキュリティインシデントが発生した場合の訓練を年1回以上受講していますか？	4.あまりしていない		
20		事故等の報告	過去の報告	過去に情報の漏えいやシステムに重大な障害が生じた場合、速やかに統括者に報告しましたか？ ※障害等が発生したことがない場合、1を選択して備考にその旨記載	1.している	過去に重大な障害なし	
21			報告手順の確認	情報の漏えいやシステムに重大な障害が生じた場合の報告先と報告手順を知っていますか？	2.概ね把握している		
22			契約	システムの開発・運用等を事業者等に委託しようとする場合は、関連法令、県情報セキュリティ対策指針、その他遵守すべき事項を明記した契約を締結していますか？	1.している		・委託契約書（仕様書、個人情報取扱特記事項を含む） ・賃貸借契約書（委託部分を含む場合）

No	大区分	中区分	小区分	設問	回答	備考欄	提出物
23		外部委託に関する管理	個人情報取扱特記事項	個人情報を取り扱う事務を委託する場合は、契約書に個人情報取扱特記事項（「個人情報を取り扱う事務の委託に伴う措置について（平成9年11月2日1付け文第294号知事公室長通知）」）を規定していますか？	1.している		
24			損害賠償	委託事業者との契約書には、この契約仕様、要綱等が遵守されなかったことにより損害が発生した場合の賠償等の規定を定めていますか？	1.している		
25			再委託の承認	再委託、再々委託等を行う場合には、相手方の氏名、業務の範囲、その必要性、体制等を記載した書面の提出を受け、再委託事業者等の安全管理措置を確認のうえ書面で承認していますか？	1.している		・再委託申請書 ・再委託承認書
26			データ受け渡し	委託事業者とのデータの受け渡しに係る内容、日付等を記録していますか？	2.概ねしている		
27			名簿作成	委託事業者の責任者や業務に従事する者の氏名、作業場所等を記載した名簿を作成していますか？	2.概ねしている		
28			身分証明の確認	委託事業者に身分証明書を携帯させ、必要に応じて提示を求めていますか？	1.している		
29			従事者に対する教育	委託事業者の従業員に対する教育が実施されているかを確認していますか？	2.概ねしている		
30		アクセス記録の取得等	各種アクセス記録の保存	各種アクセス記録等情報セキュリティ対策に必要な記録を取得し、1年間以上（個人番号利用事務は７年以上）、保存していますか？	3.どちらとも言えない		
31			アクセス記録等の分析、監視	定期的にアクセス記録等を分析、監視していますか？	2.概ねしている		
32		情報システムにおけるアクセス制御	利用者管理	利用者IDの登録、変更、退職した利用者の抹消等の取扱いに関わる手続を定め、利用者を適正に管理していますか？	2.概ねしている		
33			アクセス制御	情報通信機器にセキュリティ上の問題が認められ、情報資産に脅威が生じるおそれがある場合には、速やかに当該情報通信機器を内部ネットワークから遮断できますか？	1.している		
34		外部ネットワークとの接続	外部ネットワークの有無	県以外の機関が管理する情報システム（以下「外部ネットワーク」という。）との接続口を持っていますか？ ※「持っていない」と回答した場合、No.38へ。（No.35～37は回答不要）	1.持っている		
35			外部ネットワークの回線種別	外部との物理的接続回線は何ですか？【複数選択可】 専用線、IP-VPN、広域イーサネット、インターネットVPN、エントリーVPN、その他（具体的に）	☐ 1.専用線 ☑ 2.IP-VPN ☐ 3.広域イーサネット ☐ 4.インターネットVPN ☐ 5.エントリーVPN ☐ 6.その他（備考欄に具体的に記載）		
36			ファイアウォールの設置	外部ネットワークと接続する場合、ファイアウォールの設置、論理的なネットワークの分割等、適切なネットワーク経路制御を講じている。	1.している		
37			ユーザ認証、ファイアウォールの設置	外部からの接続時の認証方法をお答えください。 パスワードのみ、ユーザ名・パスワード、多要素認証、その他(具体的に)	3.多要素認証		
38	技術的セキュリティ対策	コンピュータウイルス対策	ウイルスチェック	外部のネットワークからデータを取り入れる際には、利用者端末等においてウイルスチェックを行い、システムへの侵入を防止していますか？	2.概ねしている		
39			コンピュータウイルス情報	EMOTET、ランサムウェア等のコンピュータウイルスが流行した場合、その情報について利用者に対する注意喚起を行っていますか？	2.概ねしている		
40			ウイルスチェック用のパターンファイル更新	システムで独自に利用するパソコンやサーバのウイルスチェック用のパターンファイルは常に最新のものに更新していますか？	1.している		
41			コンピュータウイルスに対する修正プログラムの入手	コンピュータウイルス等のセキュリティ修正プログラムの入手に努め、端末、情報通信機器、サーバ等に速やかに適用していますか？	1.している		
42		不正アクセス対策	ポート管理（ネットワーク上のサーバがサービスを区別	通信機器、サーバ等のftp、telnet、smtp等の不要なポートは、ファイアウォールや機器設定で閉じていますか？	1.している		
43			不要なユーザＩＤの削除	不正アクセスを防止するため、端末、サーバ、通信機器及び端末上の不要な利用者IDは速やかに削除していますか？	3.どちらとも言えない		
44			セキュリティホール対策	不正アクセスを防止するため、サーバや通信機器のセキュリティホールに対しては、速やかに修正プログラムを適用していますか？	1.している		
45			Webサーバ保護	Webサーバについては、WAF、Webページ改ざんの検出する措置等を実施していますか？	4.あまりしていない		
46			不正アクセス	不正アクセスを受けるおそれが認められる場合には、勤務時間外でもシステムの停止を含む必要な措置は可能にしていますか？	2.概ねしている		

No	大区分	中区分	小区分	設問	回答	備考欄	提出物
47	運用面の対策	クラウドサービス利用の対策	クラウド利用の有無	クラウドサービス（インターネット、専用回線等により接続された情報システムが提供するサービス）を利用していますか？ ※「していない」と回答した場合、No.52へ。（No.48～51は回答不要）	1.している		
48			クラウド利用形態	クラウドサービスの利用形態をお答えください【複数選択可】 1. ホームページのホスティング、2. ファイル保管・データ共有、3. サーバ利用、4. データバックアップ、5. 情報共有・ポータル、6. スケジュール共有、7. LGWAN-ASP、 8. その他（具体的に）	☑ 1. ホームページのホスティング ☐ 2. ファイル保管・データ共有 ☐ 3. サーバ利用 ☐ 4. データバックアップ ☐ 5. 情報共有・ポータル ☐ 6. スケジュール共有 ☐ 7. LGWAN-ASP ☐ 8. その他（備考欄に具体的に記載）		
49			クラウド利用のセキュリティ	クラウドサービスを利用するに当たり、データセンター、通信回線等の情報の流通経路全般にわたるセキュリティ対策の状況を確認していますか？	2.概ねしている		
50			クラウドのバックアップ	クラウド環境のデータについて、バックアップを取得していますか。	3.どちらとも言えない		
51			クラウドの停止	クラウドサービスが中断・停止した場合の対策を検討し、委託先を選定する際の要件としていますか？	5.していない		
52		緊急時対応計画等	緊急時対応計画の策定	システムの情報資産への侵害が発生した場合に備えて、あらかじめ関係機関との連絡体制や復旧対策等を定めた緊急時対応計画を策定していますか？	2.概ねしている		・緊急時対応計画
53			災害時等、緊急時の連絡体制	災害時等、緊急時の連絡体制について、連絡手順などを外部委託事業者等も含めて作成し、情報交換を円滑に行えるよう連絡体制を明確にしていますか？	1.している		・連絡体制表
54			緊急時対応計画の見直し	情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、緊急時対応計画の規定を見直していますか？	3.どちらとも言えない		