

令和 7 年度
岡山県情報セキュリティ監査業務
委託仕様書

令和 8 年 1 月 9 日

岡山県総務部デジタル推進課

1 業務名

令和7年度岡山県情報セキュリティ監査業務

2 発注部署（連絡窓口）

岡山県総務部デジタル推進課

所在地：〒700-8570 岡山市北区内山下二丁目4番6号

電話：086-226-7266（直通） FAX：086-235-9737

電子メール：sec@pref.okayama.lg.jp

3 業務の趣旨

外部委託による情報セキュリティ監査を行うことにより、岡山県（以下「県」という。）が岡山県情報セキュリティポリシーに基づき実施している情報資産の管理及び各種業務システムの運用・保守管理状況について現状のセキュリティ水準を把握し、問題点の明確化及び改善策の検討・提示を行い、もって県の情報セキュリティ対策の向上に資することを目的とする。

4 業務の概要

情報システムに係る情報セキュリティの技術的検証等（以下「本業務」という。）を行う。

準拠する基準は次のとおりとする。

（1）必須基準

- ① 岡山県情報セキュリティ基本方針（平成16年3月29日策定）
- ② 岡山県情報セキュリティ対策基準（非公開）（平成16年3月29日策定）
- ③ 岡山県情報セキュリティ個別管理基準（第2版）（非公開）（平成20年3月10日制定）
- ④ 運用監査対象所属が所管するシステムに係る実施手順書及び運用手順書

（2）参考基準

- ① 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（令和7年3月版）（総務省）
- ② 情報セキュリティ管理基準（平成28年改正版）（経済産業省）
- ③ 電気通信回線を通じた送信又は磁気ディスクの送付方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準（住民基本台帳ネットワークシステムセキュリティ基準）（平成14年総務省告示第334号）

5 業務の実施時期

本業務の実施時期は、別紙1「令和7年度岡山県情報セキュリティ監査業務スケジュール」による。なお、詳細な実施日程については、下記6において作成する実施計画書により決定することとする。

6 業務の種類及び内容

本業務の種類及び内容は次のとおりとする。ネットワークセキュリティ診断対象機器については別紙5「ネットワークセキュリティ診断対象機器一覧表」のとおりとする。

(1) 技術的検証

- ① ネットワークセキュリティ診断
- ② Webアプリケーション診断
- ③ データベース診断

詳細は、別紙2「技術的検証の業務内容」のとおりとする。

(2) 特定個人情報の取扱いに関する監査

詳細は、別紙3「特定個人情報の取扱いに関する監査の業務内容」のとおりとする。

(3) 住民基本台帳ネットワークシステム監査

- ① 運用監査
- ② ネットワークセキュリティ診断

詳細は、別紙4「住民基本台帳ネットワークシステム監査の業務内容」のとおりとする。

7 成果物

(1) 種類及び納品時期等

受託者が作成し納品すべき成果物は、別紙6「成果物一覧表」のとおりとする。

(2) 作成様式

紙媒体によるものは、A4版縦（必要に応じてA3版三つ折りも可。ただし、A3版三つ折りの場合、両面印刷は不可）とする。

電子媒体によるものは、紙媒体の成果物と同じ内容のものをCD-R等に記録する。ファイル形式は、Microsoft Word、Excel、又はPowerPointの各ドキュメント形式（office 2016以降）、又はPDF形式とする。

(3) 成果物の内容

成果物に記載すべき内容については、別紙7「成果物の項目」を基準にすることとし、目次体系等を変更又は追加する必要があるときは、県と協議の上、変更又は追加すること。

(4) 帰属

成果物及びこれに付随する資料に係る諸権利は、すべて県に帰属するものとし、書面による県の承諾を得ずに他に公表、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に属するもの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。また、受託者は県に対し著作者人格権を行使しないものとする。

8 監査結果報告会

受託者は、上記6の各業務が終了したときは、速やかに監査対象課所の職員を対象に、次の監査結果報告会を開催しなければならない。

- (1) 技術的検証結果報告会
- (2) 特定個人情報の取扱いに関する監査報告会
- (3) 住民基本台帳ネットワークシステム監査結果報告会

9 監査人の要件

受託者は、以下のすべての条件を満たす者とする。

- (1) 受託者はISO/IEC27001(JIS Q 27001)認証又はプライバシーマーク認証を取得していること。
- (2) 受託者は情報セキュリティサービス基準適合サービスリスト（独立行政法人情報処理推進機構）の情報セキュリティ監査サービス分野及び脆弱性診断サービスに登録されていること。
- (3) 受託者は令和6年度に国の省庁、都道府県および市町村に対する10件以上の情報セキュリティ監査を実施した実績を有すること。
- (4) 各診断又は監査単位で、監査責任者、監査担当者、監査補助者、アドバイザー等で構成される監査チームを編成すること。
- (5) 監査の品質の保持のため監査品質管理責任者、監査品質管理者等の監査品質管理体制をつくること。
- (6) 監査チームには、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人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

- (7) 監査責任者は、確実なプロジェクト運営を行う必要があるため、次に掲げるいずれかの資格を有すること。

ア プロジェクトマネージャ

イ PMP PMI

- (8) 監査担当者のうち1人以上の者は、次に掲げるいずれかの資格を有し、診断には必ず、有資格者が1人以上参加すること。

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 公認情報システムセキュリティプロフェッショナル（CISSP）

- (9) 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1人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。）

- (10) 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、保守等の担当をしていないこと。
- (11) 情報システムの診断及び監査には、現地作業も含め、検証対象の機器に精通し（8）に掲げる資格を有する者が1人以上従事すること。
- (12) 上記各号に定めるほか、入札説明書の「2 入札に参加する者に必要な資格」各号に定める要件を満たすこと。

10 業務における留意事項

本業務の実施に当たっては、以下の事項に留意すること。

- (1) 受託者は、県が本業務の進捗状況について説明を求めた場合、速やかに報告すること。
- (2) 受託者は、県と本業務の実施に関する協議を行った後、速やかに議事録を作成し提出しなければならない。
- (3) 受託者は、本業務の実施に当たり知り得た情報（監査対象となった所属等から収集した監査証拠や参考資料を含む。）を正当な理由なく他に開示し、又は自らの利益のために利用してはならない。これは、契約終了後又は解除後においても同様とする。
- (4) 県は、受託者から本業務の実施上必要となる資料の提供を求められた場合、妥当と判断する範囲内でこれらの資料を無償で提供する。
受託者は、県が提供した資料を善良なる管理者の注意をもって保管し、本業務以外の用途に使用してはならない。
- 受託者は、県があらかじめ承認した場合にのみ、県が提供した資料を本業務の実施上必要な範囲内で複製し、又は改変することができるものとする。
- 受託者は、県が提供した資料を使用した後は、遅滞なく県にこれを返還し、又は県の指示する処置を行うものとする。
- (5) 原則として、受託者が本業務の主要な部分を他の業者に再委託することを禁止する。再委託が必要な場合は、事前に書面により県の承諾を得なければならない。
- (6) 受託者は、関係法令等を遵守し、本業務を円滑に進めなければならない。
- (7) 成果物は、岡山県行政情報公開条例（平成8年岡山県条例第3号）により取り扱うこととし、セキュリティ上明らかになつても差し支えのない部分は、公開の対象とする。
- (8) 受託者は、本業務を主体的に遂行するとともに、全体の進行管理及び事務処理を行うこととする。ただし、監査対象課所との連絡・調整に関する事務処理については、岡山県総務部デジタル推進課が行う。
- (9) 本業務に使用する機器類等の調達に要する費用、本業務に係る交通費及び通信費等は、受託者の負担とする。

11 その他

本業務の実施に当たり、この業務仕様書に記載のない事項については、県と受託者双方の協議の上、決定する。

令和7年度岡山県情報セキュリティ監査業務スケジュール

			技術的検証	特定個人情報の取扱いに関する監査	住民基本台帳ネットワークシステム監査
令和8年	1月	下旬	事前打合せ 実施計画書作成		
			本調査		
	2月	上			
		中			
		下			
	3月	上	報告書作成		
		中			
		下	報告会開催		

技術的検証の業務内容

1 目的

県が管理するサーバやアプリケーションに対して、診断ツール等を用いて擬似的な攻撃を行うことにより、県のネットワーク資源の脆弱性や機器の設定上の不備等を検証し、県が管理するサーバやアプリケーションの技術的なセキュリティレベルの向上を図る。

2 業務の種類

技術的検証では、次の業務を行うこととする。

- (1) ネットワークセキュリティ診断
- (2) Web アプリケーション診断
- (3) データベース診断

3 検証対象

- (1) ネットワークセキュリティ診断

本県の LAN/WAN 上で稼働するサーバ等を対象とし、詳細は別紙5「ネットワークセキュリティ診断対象機器一覧表」のとおりとする。

- (2) Web アプリケーション診断

Web アプリケーション 3 システムを対象とし、各 5 画面 10 アクションを上限とする。

- (3) データベース診断

「PostgreSQL」、「MySQL」等を使用しているデータベースサーバ 2 システム (IP 数) を対象とする。

※ (2) 及び (3) について、具体的な対象システムは県から別途指示する。

4 検証方法

リモート診断又はオンサイト診断により、商用又はフリーウェアによる診断ツールのほか、キオペレーションやブラウザを適宜使用して検証する。

なお、診断ツールは、最初の診断日の 1 週間前までにリリースされている最新バージョン及びパターンのものを使用することとする。

5 準拠する基準

- (1) 必須基準

- ① 岡山県情報セキュリティ基本方針（平成 16 年 3 月 29 日策定）
- ② 岡山県情報セキュリティ対策基準（非公開）（平成 16 年 3 月 29 日策定）
- ③ 岡山県情報セキュリティ個別管理基準（第 2 版）（非公開）（平成 20 年 3 月 10 日制定）

- (2) 参考基準

- ① 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（令和 7 年 3 月版）（総務省）
- ② 情報セキュリティ管理基準（平成 28 年改正版）（経済産業省）

6 検証実施手順

(1) 事前打合せの実施

- ① 検証実施体制（責任者、担当者）及び検証対象機器を決定する。
- ② その他、検証の実施に当たり必要な事項を決定する。

打合せを行った後は、速やかに協議議事録を作成する。

なお、以後も必要に応じて適宜打合せを行うこととする。

(2) 予備調査の実施

検証の実施に当たって、事前に確認が必要な情報について調査を行う。

(例) ① ネットワークセキュリティ診断

- ア 診断対象サーバ、ネットワーク機器の構成
- イ 診断対象機器のIPアドレス（グローバル、プライベート）
- ウ 診断ツールを設置する際に必要なネットワーク構成 等

② データベース診断

- ア 対象機器の管理者アカウント、パスワード、IPアドレス
- イ 対象機器への外部メディアの利用可否 等

(3) 実施計画書の作成

- ① 予備調査の結果及び準拠する基準に基づき、県と協議の上、診断項目、診断手順及び診断実施スケジュールを決定する。

なお、Webアプリケーション診断の診断項目は、次の点に留意して決定することとする。

- ア 他人になりすましてシステムにログインすることが可能か。
- イ 個人情報等の重要なデータにアクセスが可能か。
- ウ 管理者権限を奪うことが可能か。
- エ データベースへ不正にアクセスすることが可能か。
- オ アクセス制御されているリソースへ不正にアクセスすることが可能か。

- ② 技術的検証の詳細な実施内容について、「令和7年度岡山県情報セキュリティ技術的検証実施計画書」を作成し納品する。

(4) 本調査の実施

実施計画書に基づき、次の方法により本調査を実施する。なお、本調査には、県の職員が立ち会うこととする。

① ネットワークセキュリティ診断

リモート診断とオンサイト診断を併用して検証する。詳細は、別紙5「ネットワークセキュリティ診断対象機器一覧表」に示す診断方法のとおりとする。

また、商用又はフリーウェアの診断ツールを使用して、ネットワーク資源の脆弱性の有無及び設定の不備等について診断する。

なお、商用の診断ツールは、Tenable社製「Nessus」、Nmap.org「nmap」等と同程度の診断項目数及び性能を有するものを使用することとする。

② Webアプリケーション診断

リモート診断により検証する。

インターネット経由で診断対象のWebサーバの該当URLにアクセスし、診断を行う。ま

(別紙2) 技術的検証の業務内容

た、商用又はフリーウェアの診断ツールを使用して、ネットワーク資源の脆弱性の有無及び設定の不備等について診断する。

なお、商用の診断ツールは、PortSwigger 社製「Burp Suite Professional」等と同程度の診断項目数及び性能を有するものを使用することとする。

③ データベース診断

オンサイト診断により検証する。

データベースに関わる設定全般が適切か否かについて、データベースサーバが稼働している機器にログインし、診断を行う。また、商用又はフリーウェアの診断ツールを使用して、ネットワーク資源の脆弱性の有無及び設定の不備等について診断する。

なお、商用の診断ツールは、Tenable 社製「Nessus」、Nmap.org 「nmap」等と同程度の診断項目数及び性能を有するものを使用することとする。

7 結果報告

(1) 成果物

当該業務が終了した後、速やかに「令和7年度岡山県情報セキュリティ技術的検証結果報告書」を作成し納品する。

(2) 監査結果報告会

検証対象機器を所管する課所の職員に対して、技術的検証の結果について報告会を開催する。

なお、日程調整・会場確保は、岡山県総務部デジタル推進課が行う。

8 その他

各診断を実施する際は、ハードウェア、ソフトウェア及びネットワークを損傷し、又はこれらの正常な運用を阻害することがないよう留意すること。

特定個人情報の取扱いに関する監査の業務内容

1 目的

行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）において求められている安全管理措置に係る情報資産の管理及び運用・保守管理の状況等について監査を行うことにより現状のセキュリティレベルを把握し、情報セキュリティ対策の改善を図る。

2 監査対象

本庁舎内に所在する3所属（職員数：各所属10～40名程度）を監査対象とする。

岡山市内に所在する1拠点：1所属（職員数：各所属90～110名程度）を監査対象とする。

3 監査方法

監査人が監査対象課所を訪問し、職員へのインタビュー、関係書類のレビュー及び観察を行う。これにより、監査対象課所における個人番号利用事務取扱いの各プロセス（入手・使用・委託・提供・移転・保管・消去）におけるリスク対策の実施状況について評価するとともに、評価の結果明らかになった問題点について改善策の提案を行う。

4 準拠する基準

（1）必須基準

- ① 岡山県情報セキュリティ基本方針（平成16年3月29日策定）
- ② 岡山県情報セキュリティ対策基準（非公開）（平成16年3月29日策定）
- ③ 岡山県情報セキュリティ個別管理基準（第2版）（非公開）（平成20年3月10日制定）
- ④ 特定個人情報保護評価指針（特定個人情報保護委員会）
- ⑤ 特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）
- ⑥ 岡山県特定個人情報等の管理に関する規程
- ⑦ 監査対象所属が所管する特定個人情報取扱規程

（2）参考基準

- ① 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（令和7年3月版）（総務省）
- ② 情報セキュリティ管理基準（平成28年改正版）（経済産業省）

5 監査実施手順

（1）事前打合せの実施

- ① 監査実施体制（監査責任者、監査人等）及び監査対象課所を決定する。
- ② その他、運用監査の実施に当たり必要な事項を決定する。

打合せを行った後は、速やかに協議議事録を作成する。

(別紙3) 特定個人情報の取扱いに関する監査の業務内容

なお、以後も必要に応じて適宜打合せを行うこととする。

(2) 予備調査の実施

監査対象課所の概況（業務内容、所管する情報資産等）について事前に把握するため、アンケートを実施する。

(3) 実施計画書の作成

① 予備調査の結果及び準拠する基準に基づき、県と協議の上、監査実施スケジュール及び監査項目チェックリストを決定する。

なお、監査項目は50項目程度とし、次のとおり区分するものとする。

ア 組織体制に関する事項

イ 情報資産の分類と管理方法

ウ 物理的セキュリティ

エ 人的セキュリティ

オ 技術的セキュリティ

カ 運用、評価・見直し

② 監査の詳細な実施内容について、「令和7年度岡山県特定個人情報の取扱いに関する監査実施計画書」を作成し納品する。

(4) 本調査の実施

実施計画書に基づき、次の方法により本調査を実施する。本調査に要する時間は、原則として1回（1課所）2時間程度とする。なお、本調査には、県の職員が立ち会うこととする。

① インタビュー

情報セキュリティに対する意識、各種基準の認知度、システムの運用・管理状況等について、監査対象課所の職員に聞き取り調査を行う。

② レビュー

各種関係書類のレビューを行う。

③ 視察

重要な情報資産の管理状況等を目視により確認する。

④ 講評

監査対象課所の職員に対し、口頭により監査結果の講評を行う。

6 結果報告

(1) 成果物

当該業務が終了した後、速やかに「令和7年度岡山県特定個人情報の取扱いに関する監査報告書」及び「令和7年度岡山県特定個人情報の取扱いに関する監査個別報告書」（監査対象課所ごとに編集したもの）を作成し納品する。

(2) 監査結果報告会

監査対象課所の職員に対して、運用監査の結果について報告会を開催する。

なお、日程調整・会場確保は、岡山県総務部デジタル推進課が行う。

住民基本台帳ネットワークシステム監査の業務内容

1 目的

住民基本台帳ネットワークシステム（以下「本システム」という。）に係る情報資産の管理及び運用・保守管理の状況等について監査を行うことにより現状のセキュリティレベルを把握し、情報セキュリティ対策の改善を図る。

また、本システムのサーバ機器等に対して、診断ツール等を用いて擬似的な攻撃を行うことにより、ネットワーク資源の脆弱性や機器の設定上の不備等を検証し、本システムの技術的なセキュリティレベルの向上を図る。

2 業務の種類

- (1) 運用監査
- (2) ネットワークセキュリティ診断

3 監査対象

(1) 運用監査

本システムを運用する次の11課所を監査対象とする。

- ① 総務部税務課（本庁舎内）
- ② 県民生活部市町村課（本庁舎内）
- ③ 総務部デジタル推進課（本庁舎内）
- ④ 土木部都市局建築指導課（本庁舎内）
- ⑤ 県警分庁舎（岡山市内）
- ⑥ 備前県民局（岡山市内）
- ⑦ 備中県民局（倉敷市内）
- ⑧ 美作県民局（津山市内）
- ⑨ 国際課海外渡航班（岡山市内）
- ⑩ 精神保健福祉センター（岡山市内）
- ⑪ 岡山県データセンター（岡山市内）

(2) ネットワークセキュリティ診断

別紙5「ネットワークセキュリティ診断対象機器一覧表」のとおりとする。

4 監査方法

(1) 運用監査

監査人が監査対象課所を訪問し、職員へのインタビュー、関係書類のレビュー及び視察を行うことにより、本システムに係る情報資産の管理及び運用・保守管理の状況等について評価するとともに、評価の結果明らかになった問題点について改善策の提案を行う。

(2) ネットワークセキュリティ診断

オンライン診断により、商用又はフリーウェアによる診断ツールの他、キーオペレーションやブラウザを適宜使用して検証する。

なお、商用の診断ツールは、Tenable 社製「Nessus」、Nmap.org「nmap」等と同程度の診断

(別紙4) 住民基本台帳ネットワークシステム監査の業務内容

項目数及び性能を有するものを使用することとする。

5 準拠する基準

(1) 必須基準

- ① 岡山県情報セキュリティ基本方針（平成16年3月29日策定）
- ② 岡山県情報セキュリティ対策基準（非公開）（平成16年3月29日策定）
- ③ 岡山県情報セキュリティ個別管理基準（第2版）（非公開）（平成20年3月10日制定）
- ④ 住民基本台帳ネットワークシステム運用計画
- ⑤ 住民基本台帳ネットワークシステム運営管理要綱
- ⑥ 岡山県住民基本台帳ネットワークシステム運用手順
- ⑦ 住民基本台帳ネットワークシステム緊急時対応計画
- ⑧ 住民基本台帳ネットワークシステム研修計画

(2) 参考基準

- ① 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（令和7年3月版）（総務省）
- ② 情報セキュリティ管理基準（平成28年改正版）（経済産業省）
- ③ 住民基本台帳ネットワークシステム等及びそれに接続している既設ネットワークに関する調査表 都道府県版（総務省）

6 監査実施手順

(1) 運用監査

① 事前打合せの実施

ア 監査実施体制（監査責任者、監査人等）及び監査対象課所を決定する。

イ その他、運用監査の実施に当たり必要な事項を決定する。

打合せを行った後は、速やかに協議議事録を作成する。

なお、以後も必要に応じて適宜打合せを行うこととする。

② 予備調査の実施

監査対象課所の概況（業務内容、所管する情報資産等）について事前に把握するため、アンケートを実施する。

③ 実施計画書の作成

ア 予備調査の結果及び準拠する基準に基づき、県と協議の上、監査実施スケジュール及び監査項目チェックリストを決定する。

なお、監査項目は50項目程度とし、次のとおり区分するものとする。

(ア) 組織体制に関する事項

(イ) 情報資産の分類と管理方法

(ウ) 物理的セキュリティ

(エ) 人的セキュリティ

(オ) 技術的セキュリティ

(カ) 運用、評価・見直し

イ 運用監査の詳細な内容について、「令和7年度岡山県住民基本台帳ネットワークシステム監査実施計画書【運用監査】」を作成し納品する。

(別紙4) 住民基本台帳ネットワークシステム監査の業務内容

④ 本調査の実施

実施計画書に基づき、次の方法により本調査を行う。本調査に要する時間は、原則として1回（1課所）2時間程度をする。なお、本調査には、県の職員が立ち会う場合がある。

ア インタビュー

情報セキュリティに対する意識、各種基準の認知度、本システムの運用・管理状況等について、職員に聞き取り調査を行う。

イ レビュー

各種関係書類のレビューを行う。

ウ 視察

重要な情報資産の管理状況等を目視により確認する。

エ 講評

監査対象課所の職員に対し、口頭により監査結果の講評を行う。

(2) ネットワークセキュリティ診断

① 事前打合せの実施

ア 診断実施体制（責任者、担当者）及び診断対象機器を決定する。

イ その他、診断の実施に当たり必要な事項を決定する。

打合せを行った後は、速やかに協議議事録を作成する。

なお、以後も必要に応じて適宜打合せを行うこととする。

② 予備調査の実施

診断の実施に当たって、事前に確認が必要な情報について調査を行う。

(例)

ア 診断対象サーバ、ネットワーク機器の構成

イ 診断対象機器のIPアドレス（グローバル、プライベート）

ウ 診断ツールを設置する際に必要なネットワーク構成 等

③ 実施計画書の作成

ア 予備調査の結果及び準拠する基準に基づき、県と協議の上、診断項目、診断手順及び診断実施スケジュールを決定する。

イ ネットワークセキュリティ診断の詳細な実施内容について、「令和6年度岡山県住民基本台帳ネットワークシステム監査実施計画書【ネットワークセキュリティ診断】」を作成し納品する。

④ 本調査の実施

上記4（1）により、本調査を実施する。

7 結果報告

(1) 成果物

当該業務が終了した後、速やかに「令和7年度岡山県住民基本台帳ネットワークシステム監査報告書【運用監査】～概要版（公開版）～」、「令和7年度岡山県住民基本台帳ネットワークシステム監査報告書【運用監査】～詳細版（非公開版）～」及び「令和7年度岡山県住民基本台帳ネットワークシステム監査報告書【ネットワークセキュリティ診断】」を作成し納品する。

(2) 監査結果報告会

(別紙4) 住民基本台帳ネットワークシステム監査の業務内容

監査対象課所の職員に対して、監査の結果について報告会を開催する。

なお、日程調整・会場確保は、岡山県県民生活部市町村課が行う。

8 その他

ネットワークセキュリティ診断を実施する際は、ハードウエア、ソフトウエア及びネットワークを損傷し、又はこれらの正常な運用を阻害することがないよう留意すること。

なお、業務端末を対象とする診断は、業務時間内に実施するが、診断に要する時間を除き、業務利用に支障がないよう留意すること。

ネットワークセキュリティ診断対象機器一覧表

別紙5

1 対象機器

ネットワーク	設置場所	サーバ名	台数 (IP数)	診断方法		診断実施 時間帯
				リモート	オンサイト	
県庁LAN/WAN ①行政系ネットワーク	県庁NOC (岡山市内)	wwwサーバ	1	○	○	時間内
		外部DNS	1	○	○	時間内
		Mailサーバ	1	○	○	時間内
		大容量ファイル転送システム	1	○	○	時間内
		ファイアウォール	3		○	時間内
		CMSサーバ	1		○	時間内
		メール無害化外部サーバ	1		○	時間内
		グループウェアサーバ	1		○	時間内
		内部DNSサーバ	1		○	時間内
		庁内Webサーバ	1		○	時間内
		ウィルスチェックサーバ	1		○	時間内
		内部メールサーバ	1		○	時間内
		LGWANメールサーバ	1		○	時間内
		メール無害化内部サーバ	1		○	時間内
		L3スイッチ	1		○	時間内
		庁内チャットシステムサーバ	1		○	時間内
		(小計)	18			
②公開系ネットワーク	NOC (岡山市内)	DNS/Mailサーバ	1	○	○	時間内
		WWWサーバ	1	○	○	時間内
		ファイアウォール	1	○	○	時間内
		(小計)	3			
③データセンター	データセンター (岡山市内)	ファイアウォール	1	○	○	時間内
		DNS/Mailサーバ1号機	1	○	○	時間内
		NTPサーバ	1	○	○	時間内
		(小計)	3			
④学校系ネットワーク	データセンター (岡山市内)	プロキシサーバ2号機	1	○	○	時間内
		WWWサーバ2号機	1	○	○	時間内
		RADIUSサーバ(学習系)	1	○	○	時間内
		ファイアウォール	1	○	○	時間内
		(小計)	4			
県庁LAN/WAN 計		計	28			
住民基本台帳ネットワークシステム	(岡山市内)	代表端末(サーバ)	1		○	閉庁日
		ネットワーク監視装置(サーバ)	1		○	閉庁日
		ファイアウォール	2		○	閉庁日
		ルータ	2		○	閉庁日
		業務端末	11		○	時間内
		(小計)	17			

2 診断方法

(1)「リモート」に○印がある場合

インターネットを経由して、インターネットに公開されている対象機器を診断する。

(2)「オンサイト」に○印がある場合

診断対象機器と同一のセグメントから、対象機器を直接診断する。

3 診断実施時間帯

(1) 時間内 平日の業務時間内(8:30～17:15) のうち、県が事前に許可した時間帯

(2) 時間外 平日の業務時間外(17:30～翌8:00) のうち、県が事前に許可した時間帯

(別紙4)ネットワークセキュリティ診断対象機器一覧表

ネットワークセキュリティ診断対象機器一覧表

別紙5

1 対象機器

ネットワーク	設置場所	サーバ名	台数 (IP数)	診断方法		診断実施 時間帯
				リモート	オンサイト	

(3) 閉序日　　土・日・祝日の9:00～17:00のうち、県が事前に許可した時間帯

成 果 物 一 覧 表

種別	業務区分	題 名	あて名	媒体及び部数	
				紙	電子
実施計画書	技術的検証	1 令和7年度岡山県情報セキュリティ技術的検証実施計画書	岡山県情報セキュリティ委員会	1	1
	特定個人情報の取扱いに関する監査	2 令和7年度岡山県特定個人情報の取扱いに関する監査実施計画書		1	1
	住民基本台帳ネットワーク	3 令和7年度岡山県住民基本台帳ネットワークシステム監査実施計画書【運用監査】		1	1
		4 令和7年度岡山県住民基本台帳ネットワークシステム監査実施計画書【ネットワークセキュリティ診断】		1	1
報告書	技術的検証	5 令和7年度岡山県情報セキュリティ技術的検証結果報告書【ネットワークセキュリティ診断(行政系ネットワーク)】	岡山県情報セキュリティ委員会	1	1
		6 令和7年度岡山県情報セキュリティ技術的検証結果報告書【ネットワークセキュリティ診断(公開系ネットワーク)】		1	1
		7 令和7年度岡山県情報セキュリティ技術的検証結果報告書【ネットワークセキュリティ診断(データセンター)】		1	1
		8 令和7年度岡山県情報セキュリティ技術的検証結果報告書【ネットワークセキュリティ診断(学校系ネットワーク)】		1	1
		9 令和7年度岡山県情報セキュリティ技術的検証結果報告書【Webアプリケーション診断】		1	1
		10 令和7年度岡山県情報セキュリティ技術的検証結果報告書【データベース診断】		1	1
	特定個人情報の取扱いに関する監査	11 令和7年度岡山県特定個人情報の取扱いに関する監査報告書		1	1
		12 令和7年度岡山県特定個人情報の取扱いに関する監査個別報告書		1	1
	住民基本台帳ネットワーク	13 令和7年度岡山県住民基本台帳ネットワークシステム監査報告書【運用監査】～概要版(公開版)～		1	1
		14 令和7年度岡山県住民基本台帳ネットワークシステム監査報告書【運用監査】～詳細版(非公開版)～		1	1
		15 令和7年度岡山県住民基本台帳ネットワークシステム監査報告書【ネットワークセキュリティ診断】		1	1
	全体	16 令和7年度岡山県情報セキュリティ監査全体報告書～概要版(公開版)～		1	1
		17 令和7年度岡山県情報セキュリティ監査全体報告書～詳細版(非公開版)～		1	1
議事録	全体	第××回○○業務協議議事録		1	1

成果物に記載する項目

1 令和7年度岡山県情報セキュリティ技術的検証実施計画書

- (1) 目的 技術的検証を実施する目的について記載する。
- (2) テーマ 重点的に検証するテーマ等について記載する。
- (3) 検証対象 検証の対象とする機器等について記載する。
- (4) 検証方法 検証で適用する監査技法（使用ツール、検証作業の手順等）について記載する。
- (5) 実施日程 事前打合せから結果報告までのスケジュールについて記載する。
- (6) 実施体制 責任者、担当者について記載する。
- (7) 検証項目 検証で確認する項目について記載する。
- (8) 適用基準 検証で準拠する基準について記載する。

2 令和7年度岡山県特定個人情報の取扱いに関する監査実施計画書

- (1) 目的 監査を実施する目的について記載する。
- (2) テーマ 監査の具体的なテーマや重点的に監査を行う事項について記載する。
- (3) 監査範囲 監査対象の業務及び情報システムの範囲並びに監査でレビューする書類等について記載する。
- (4) 監査対象 監査の対象とする課所について記載する。
- (5) 監査方法 監査で適用する監査技法（アンケート、インタビュー、レビュー、視察の手順等）について記載する。
- (6) 実施日程 事前打合せから結果報告までのスケジュールについて記載する。
- (7) 実施体制 監査責任者、担当者について記載する。
- (8) 監査項目 監査で確認する項目について記載する。
- (9) 適用基準 監査で準拠する基準について記載する。

3 令和7年度岡山県住民基本台帳ネットワークシステム監査実施計画書【運用監査】

上記2に準じる。

4 令和7年度岡山県住民基本台帳ネットワークシステム監査実施計画書【ネットワークセキュリティ診断】

上記1に準じる。

5 令和7年度岡山県情報セキュリティ技術的検証結果報告書【ネットワークセキュリティ診断(行政系ネットワーク)】

- (1) 目的 技術的検証を実施した目的について記載する。
- (2) テーマ 重点的に検証したテーマ等について記載する。
- (3) 検証対象 検証の対象とした機器等について記載する。
- (4) 検証方法 検証で適用した監査技法（使用ツール、検証作業の手順等）について記載する。
- (5) 実施日程 検証を実施した日時について記載する。
- (6) 実施体制 責任者、担当者について記載する。
- (7) 検証項目 検証で確認した項目について記載する。
- (8) 適用基準 検証で準拠した基準について記載する。

(別紙7) 成果物に記載する項目

- (9) 検証総評 検証結果の概要（総括・評価）について記載する。
- (10) 指摘事項 検証で確認した事実（危険度等）に基づき、問題点として指摘する事項について記載する。
- (11) 改善勧告 指摘事項に対する改善策の提案について記載する。
- (12) 特記事項 その他特記すべき事項があれば記載する。
- (13) 添付資料 添付すべき資料がある場合に添付する。

6 令和7年度岡山県情報セキュリティ技術的検証結果報告書【ネットワークセキュリティ診断(公開系ネットワーク)】

上記5に準じる。

7 令和7年度岡山県情報セキュリティ技術的検証結果報告書【ネットワークセキュリティ診断(データセンター)】

上記5に準じる。

8 令和7年度岡山県情報セキュリティ技術的検証結果報告書【ネットワークセキュリティ診断(学校系ネットワーク)】

上記5に準じる。

9 令和7年度岡山県情報セキュリティ技術的検証結果報告書【Webアプリケーション診断】

上記5に準じる。

10 令和7年度岡山県情報セキュリティ技術的検証結果報告書【データベース診断】

上記5に準じる。

11 令和7年度岡山県特定個人情報の取扱いに関する監査報告書

- (1) 目的 監査を実施した目的について記載する。
- (2) テーマ 監査の具体的なテーマや重点的に監査を行った事項について記載する。
- (3) 監査範囲 監査対象の業務及び情報システムの範囲並びに監査でレビューした書類等について記載する。
- (4) 監査対象 監査を実施した課所について記載する。
- (5) 監査方法 監査で適用した監査技法（アンケート、インタビュー、レビュー、観察の手順等）について記載する。
- (6) 実施日程 監査を実施した日時について記載する。
- (7) 実施体制 監査人、監査対象課所の担当者について記載する。
- (8) 監査項目 監査で確認した項目について記載する。
- (9) 適用基準 監査で準拠した項目について記載する。
- (10) 監査総評 監査結果の概要（総括・評価）について記載する。
- (11) 指摘事項 監査で確認した事実に基づき、問題点として指摘する事項について記載する。
- (12) 改善勧告 指摘事項に対する改善策の提案について記載する。
- (13) 特記事項 その他特記すべき事項があれば記載する。
- (14) 添付資料 添付すべき資料がある場合に添付する。

(別紙 7) 成果物に記載する項目

- 12 令和5年度岡山県特定個人情報の取扱いに関する監査個別報告書
上記 11 に準じる。
- 13 令和7年度岡山県住民基本台帳ネットワークシステム監査報告書【運用監査】～概要版（公開版）～
上記 11 に準じる。
セキュリティ上公開して差し支えない事柄のみ記載すること。
- 14 令和7年度岡山県住民基本台帳ネットワークシステム監査報告書【運用監査】～詳細版（非公開版）～
上記 11 に準じる。
- 15 令和7年度岡山県住民基本台帳ネットワークシステム監査報告書【ネットワークセキュリティ診断】
上記 5 に準じる。
- 16 令和7年度岡山県情報セキュリティ監査全体報告書～概要版（公開版）～
上記 5、13 に準じる。
住民基本台帳ネットワークシステム監査を除く全ての監査結果について記載すること。ただし、
セキュリティ上公開して差し支えない事柄のみ記載すること。
- 17 令和7年度岡山県情報セキュリティ監査全体報告書～詳細版（非公開版）～
上記 5、14 に準じる。
住民基本台帳ネットワークシステム監査を除く全ての監査結果について記載すること。