別紙

情報セキュリティ監査実施方法

１　監査対象システム

以下の情報システムを対象として、各情報システムの運用形態に応じた情報セキュリティ対策の実効性を検証し、改善点の指摘を行う。

項番	システム名称
1	県庁LANシステム

２　実施体制

情報セキュリティ監査における監査結果報告会については、監査責任者を含む２名以上で実施しなければならない。

ヒアリング、報告会その他の打合せ（キックオフ会議を除く。）は、原則として県が指定するWeb会議システムにて行うこととする。

なお、キックオフ会議についても、協議によりWeb会議システムにて開催する場合がある。

３　監査項目

⑴　情報システム運用監査

「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」及び「α’／β／β’モデル採用地方公共団体における外部監査の実施及び監査報告書の提出について（通知）」に基づき、監査対象システムの運用状況及び最新のセキュリティ情報を踏まえ、あらかじめ県と協議の上、監査項目（別紙付表を参照）を決定する。

⑵　情報システムの技術的検証

監査項目のうち技術的な項目については、設定の状況がシステムの保有情報や運用形態に照らして必要十分なものとなっているかどうかについても検証を行う。

(例)アクセスログ確認時の閾値の妥当性

ファイアウォール設定の妥当性の確認　等

⑶　侵入検査

脆弱性スキャナ等による検査又は検査者による手動の検査を行う。ただし、対象システムの運用について支障及び損害を与えないように十分配慮して実施する。

４　実施の手順

⑴　初回打合せ

契約締結後速やかに発注者と打合せを行い、監査項目及び監査の進め方等について協議・確認を行う。

⑵　監査実施計画書の作成

情報セキュリティ監査実施計画書（以下、「監査実施計画書」という。）を作成する。

なお、監査実施計画書は、以下の項目を含めるものとし、キックオフ会議開催前日までに提出することとする。

ア　監査目的
イ　監査対象システム
ウ　被監査部門
エ　監査方法
オ　実施体制
カ　監査項目
キ　適用基準
ク　スケジュール

⑶　事前調査

決定した監査項目に基づき調査書を作成し、監査対象システムの管理者に対し書面による事前調査を実施する。調査書の送付及び回収については、発注者が行う

⑷　監査の実施

ヒアリング及び侵入検査により情報セキュリティ監査（以下、「監査」という。）を実施する。

監査日程については、発注者が監査対象システム管理者と調整を行う。

⑸　監査結果報告書の作成

監査時の検出事項について重要度等の位置付けを決定し、情報セキュリティ監査実施日から２週間以内に監査結果報告書を作成する。

監査結果報告書には、以下の項目を含めるものとする。

ア　監査目的
イ　監査テーマ
ウ　監査対象システム
エ　実施体制
オ　監査方法
カ　監査実施日時
キ　監査項目
ク　検出事項の評価根拠
ケ　適用基準
コ　監査結果概要（総括）
サ　監査結果（指摘事項、改善勧告、特記事項）

⑹　監査対象システム管理者に対する監査結果報告会

監査結果報告書の内容及び監査で検出された事項に対する対応策について、説明を行うための報告会を以下のとおり実施する。

なお、会場は発注者が用意する。

ア　対 象 者　監査対象システム管理者
イ　時　　間　１～３時間程度
ウ　実施時期　監査実施終了日から令和８年３月１１日（水）の間で、発注者が受注者及び監査対象システム管理者と調整した日

エ　内　　容

㈠　監査の概要

㈡　監査結果

㈢　監査結果で判明したシステム管理運営上の課題

㈣　課題に対する解決策

5　実施における留意点

⑴　監査実施時の検出事項は、監査終了時に書面で提示し確認をとること。

⑵　監査実施時に検出された事項の重要度等の位置付けについては、推奨する事項を除き、監査結果報告書の作成時に発注者と協議の上決定すること。

6　資料の提供等

本業務の実施に当たり、発注者は以下の資料を提供する。

資料の取扱いは、仕様書12⑵によること

⑴　埼玉県情報セキュリティポリシー

⑵　情報セキュリティ共通実施手順

⑶　監査対象システムに関する基本情報（設計書・運用手順書等）

⑷　上記以外の提供資料及びデータ