

情報セキュリティ及び特定個人情報の安全管理措置に係る監査実施報告書

この情報セキュリティ監査実施報告書は令和3年度に実施した戸田市情報セキュリティ監査支援業務委託のうち情報セキュリティ及び特定個人情報の安全管理措置に係る内部監査（以下「内部監査」という。）、情報セキュリティ及び特定個人情報の安全管理措置に係る外部監査（以下「外部監査」という。）及び情報セキュリティ自己点検（以下「自己点検」という。）の実施結果を報告するものである。それぞれの結果は下記のとおりである。

記

1 内部監査及び外部監査における判定基準

内部監査及び外部監査では、監査項目ごとに下表で示す判定基準を基に監査対象の対策状況を判定した。

「監査の判定基準」

評価	成熟度判定	分類基準
適合 「○」	レベル4 (評価事項)	レベル3の状態が継続的に続けられており、さらに積極的な改善活動がなされている。
	レベル3	情報セキュリティポリシー等の基準を満たしており、標準的で適切な状態である。
不適合 「×」	レベル2	情報セキュリティポリシー等の基準に対し、対策漏れがあり改善の余地がある。
	レベル1	情報セキュリティポリシー等の基準に対し、場当たりの対策不足のため改善が必要である。
	レベル0	情報セキュリティポリシー等の基準が、実施されていない。又は認識されていない。

2 内部監査

(1) 内部監査の概要

戸田市の内部監査は、平成17年度より概ね3年で全ての所属を一巡する計画が継続されており、令和2年度からは6巡目が開始され、今年度（令和3年度）はその2年目に当たる。

(2) 内部監査の結果

前頁に示す監査判定基準に基づく市全体の対策レベル平均は 3.08（前年度 2.99）と昨年度より向上した。これは昨年度の課題に対する改善活動が水平展開され、市全体で積極的な改善活動が進んだためであると考えられる。

3 外部監査

監査中期計画に基づき、次の 3 つの手法で外部監査を行った。

- ① サーバ機器等への技術的セキュリティ診断
- ② 市職員への標的型攻撃を想定したメール訓練
- ③ 監査対象所属への情報セキュリティ対策状況確認（以下「対策状況確認」という。）

（1）サーバ機器等への技術的セキュリティ診断の結果

サーバで使用されているソフトウェア等のバージョンが古い問題が検出された。検出された課題については、可能な限り対応することが望まれるが、そうすることで生じる動作不具合及び改善にかかる費用を鑑みた適切な対応を検討されたい。

（2）市職員への標的型攻撃を想定したメール訓練の結果

業務内容を偽装するメールに訓練用ファイルを添付し送信した結果、添付ファイルの開封はなく概ね良好な結果であった。より巧妙な偽装メールを用いた攻撃が流行していることから、今後も継続した注意喚起が望まれる。

（3）対策状況確認の結果

今年度も最新のサイバー攻撃や番号法改正の動向を視点に加えた監査を継続して行った。外部監査と内部監査との違いは、監査対象の範囲と監査時に求める対策の水準である。外部監査では内部監査項目に加え、情報システムの管理及び利用における対策状況を範囲とした確認や、特定個人情報の取扱い全般に係る安全管理措置が、個人情報保護委員会が求める水準で実施されているか否かの視点で確認を行った。

その結果、前頁に示す監査の判定基準に基づく市全体の対策レベル平均は、2.82 であり、昨年度よりも 0.05 向上した。特定個人情報を含めた情報資産の保護は概ね実施できているが、取扱手順の記載内容と実態とに相違があるなど、より運用精度を上げるために必要な課題の検出があった。

今年度の課題点を庁内でも共有し、水平展開することで事故を未然に防ぐための予防対策を期待したい。

4 自己点検

（1）自己点検の概要

内部監査を補填する取り組みとして情報セキュリティ自己点検票を作成し、市職員へ配付及び回収した結果を情報セキュリティ対策の見直しへ活用した。

（2）自己点検の結果

全体の遵守率は93.5%（昨年度：93.5%）となり、昨年度と同率であった。
その他、ヒヤリハットを含めた自由意見では、現状の対策に対する具体的な問題提起などが多く見られ、職員の情報セキュリティリスク対策に対する意識が向上していると感じる意見が目立った。

以 上