令和５年３月31日

情報セキュリティ監査実施報告書

この情報セキュリティ監査実施報告書は令和４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内部監査（以下「内部監査」という。）、情報セキュリティ自己点検（以下「自己点検」という。）及び情報セキュリティ外部監査（以下「外部監査」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、場当たり的で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４年度）はその３年目に当たる。今年度は、内部監査員の理解度向上を目的に、事前学習時間を設け、さらに判定の精度を向上させるため、

具体的な検出内容の事例紹介を含めた内部監査員養成研修を行った。また、委託業者が全ての内部監査に立会いサポートを行った。

（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 2.98（前年度 3.08）と昨年度より低下した。これは内部監査の立会い及び作成された報告書の内容から昨年度よりも検出の精度が高まった結果であると言え、監査対象の対策状況が悪化したわけではないと考える。

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

外部ネットワークに接続できないエリアのサーバで使用されているソフトウェア等のセキュリティ更新プログラムが未適用である問題が検出された。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、対応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、多くの訓練参加者は添付ファイルを開封することなく訓練を終了する結果となり、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も、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が実施されているか否かの視点で確認を行った。評価は成熟度モデルを採用し 3.00 を標準としている。

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、2.84 であり、昨年度よりも 0.02 向上した。特に特定個人情報の取り扱いについて改善が見られた。一方、幾つかの記録の残し方について対策が不十分な点が確認され、インシデントが発生した際に説明責任を果たせなくなる懸念があった。

今年度の課題及び改善方法を庁内に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、市の全職員を対象に情報セキュリティ自己点検を実施し、集計した結果から情報セキュリティ対策の浸透状況を継続的に確認している。

（２）自己点検の結果

市全体の遵守率は 95.0%（昨年度：93.5%）となり、昨年度より 1.5%向上した。この要因として半数以上の項目が向上しており、このうち 3 項目では 5%以上向上している。一方、昨年度より下げた項目は 6 つあったが全て 1 %以下で誤差の範囲であった。

以 上