

令和 3 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 2 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

2.1 内部監査の概要

戸田市では、平成 17 年度から 3 年で全ての所属を一巡する内部監査を継続しており、令和 2 年度からは 6 巡目が開始された。今年度はその初年度に当たる。今年度は過去に課題のあった項目に焦点を絞ったうえで、新たなリスク等を想定して監査手続を見直した。また、特定個人情報の取扱いについて確認する項目を追加し監査を行った。

2.2 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は 2.99 であり、昨年度から変動はなく、新たなリスクとなり得る検出はなかった。

3 外部監査

3.1 外部監査の概要

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。）

3.2 サーバ機器等への技術的セキュリティ診断の結果

使用されている暗号化強度の問題やソフトウェアのバージョンが古い問題が確認された。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。

3.3 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、一部の職員による添付ファイルの開封があった。最近では偽装メールを用いた攻撃が流行しており継続的に注意喚起が望まれる。

3.4 対策状況確認の結果

今年度は過去に課題のあった項目に焦点を絞ったうえで、情報セキュリティ監査基準に基づき新たなリスク等を想定して監査手続を見直した。また、特定個人情報の取扱いについて確認する項目を追加し監査を行った。

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や利用における対策状況の確認や、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は、2.77 であり、昨年度より 0.02 低下したが誤差の範囲であった。なお特定個人情報の取扱いに係る対策については、概ね実施できているものの、その対策状況を証明できるまでには至っていない検出があった。

4 自己点検

4.1 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、市職員へ配布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。

4.2 自己点検の結果

全体の遵守率は93.5%（昨年度：93.0%）となり、昨年度より0.5%向上した。今年度と昨年度の遵守率を比較したところ、下位5項目において順位の変動はあったものの同様の項目となっていた。ついては、下位5項目を重点的に改善することにより市全体の底上げが図れると考える。

以 上