

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、平成 29 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業務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、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、標準的な対策が実践されている。
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、属人的な対策であるため、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、場当たりの対策であるため、改善必要である。
	レベル 0	情報セキュリティポリシー等の基準が適用されていない。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 年度から内部監査を開始し今年度で 13 年目を迎える。情報セキュリティ対策の取り組みを全庁的に浸透させるため、3 年で全ての所属を一巡させており、今年度から 5 巡目が開始された。

2.2 内部監査の結果

全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、2.97（昨年度より0.02ポイント向上）であった。

昨年度に比べ今年度の数値が向上した要因として、1所属当たりの課題数が減少し、良い取り組みである評価事項が増加している点が挙げられる。

3 自己点検

3.1 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。

3.2 自己点検の結果

その結果、約6割の項目で遵守率が90%以上となり、概ね良好な結果だった。また、遵守率が低く課題として検出された事項と内部監査で検出された課題とが合致し、比較的精度の高い点検結果となった。

4 外部監査

4.1.1 外部監査の概要

外部監査では、監査中期計画に基づき、サーバ機器等への技術的セキュリティ診断、市職員への標的型攻撃を想定したメール訓練及び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。）を実施した。

4.2.1 サーバ機器等への技術的セキュリティ診断の結果

不正プログラムに対する防御は問題なく実施されているが、一部のサーバや利用端末の設定不備や制御方法の見直しに関する課題が確認された。

4.2.2 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へ訓練用ファイルを添付し送付した結果、添付ファイルの開封率が約9%であった。

4.2.3 対策状況確認の結果

全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、情報セキュリティポリシーの遵守状況で2.96、情報システムの管理状況で2.40であった。

5 今後の取り組みについて

内部監査及び外部監査で課題が発見された項目については、市から改善計画が立案され順次対応が進められている。本報告書の提出時点においては技術的な課題を除き、概ね改善対応が完了していることから、課題を早期解決する仕組みが機能しているといえる。

今後の対策として、技術的な課題は適切な時期にフォローアップを徹底することで、より確実な運用管理が期待できる。

以 上