平成 31 年 3 月 22 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、平成 30 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<br>「○」 | レベル４<br>（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<br>「×」 | 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、場当たり的な対策であるため、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 3 年で全ての所属を一巡する内部監査を継続しており、平成 29 年度からは 5 巡目が開始された。今年度はその 2 年目に当たる。

### 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平均は、2.97（昨年度と同じ

値）であった。数値の推移は昨年度と同じ値であったものの、1所属当たりの課題数が増加した。これは、全体の底上げができてきた反面、内部監査時点において精度の高い運用が確認できたことによりレベル３には満たない又はレベル３ではあるが対策の強化が望まれる指摘が増加したためである。

## 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つの観点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

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検出された。

### 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へ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率は約14%（昨年度：9%）であった。昨年度に比べ開封率が上がった要因としては、業務内容を偽装したより巧妙な最新の手口を用いたため、それに係る知識不足が大きいと考えられる。

### 3.4　対策状況確認の結果

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、情報セキュリティポリシーの遵守状況で2.92（昨年度：2.96)、情報システムの管理状況で2.68（昨年度：2.40）であった。特に、情報システムの管理状況で昨年度に検出された課題に対し適切な対応がとられていたことで、全体の対策レベルが向上していた。

## 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93.1%（昨年度：91.4%）となり、昨年度より1.7%向上した。また、設問別では21項目中15項目が昨年度より向上したため、概ね良好な結果であった。

また、設問の内容を昨年度に比べ対策レベルを問う質問としたことで、職員は主観での回答ではなく実態を回答することとなり、回答結果は昨年度よりも低下すると想定していたが、それに反し全体の遵守率は向上した。

以　上