

松阪市長様

平成 27 年 03 月実施

平成 26 年度情報セキュリティ監査業務委託報告書

平成 27 年 03 月 16 日



T I S 株式会社

1. 実施根拠
2. 監査の目的
3. 監査の対象
 - (1) システム
 - (2) 組織
4. 監査の実施
 - (1) 監査の実施者
 - (2) 体制
 - (3) 作業記録
5. 監査表
 - (1) 参考資料
 - (2) 作成方法
 - (3) 監査表名称 (ファイル名)
6. 参考資料
7. 添付書類
8. 監査の結果
 - (1) 監査の手法
 - (2) 総合評価
9. 松阪市情報セキュリティ対策基準に対する改善提案
 - (1) 評価基準
 - (2) 監査前評価
 - (3) 監査後評価

1. 実施根拠

「平成26年度情報セキュリティ監査業務委託仕様書」に従い作業を実施。

以下、主な作業。

- ・情報セキュリティ監査業務（以下「監査」という。）
- ・松阪市情報セキュリティポリシーの見直し案

2. 監査の目的

本業務は、

「松阪市における情報システムの運用体制、セキュリティの状況等について、第三者による独立かつ専門的な立場からの監査を実施し、問題点を確認するとともに改善方法の検討を行うことで、より適切な運用体制の構築やセキュリティ対策の維持向上を図ること」

を目的とする。

3. 監査の対象

(1) システム

- ・基幹系情報システム
- ・庁内情報ネットワークシステム

(2) 組織

松阪市経営企画部情報企画課

4. 監査の実施

(1) 監査の実施者（以下「実施者」という。）

名称：T I S株式会社

部署：コーポレート本部 セキュアワンセンター

住所：東京都新宿区西新宿 8-17-1

住友不動産新宿グランドタワー

電話番号：03-5337-4242

(2) 体制

実施者の責務のもと、以下の体制で実施。

役割	氏名	所属
総責任者	早矢仕 善弘	T I S株式会社 コーポレート本部 セキュアワンセンター センター長
実施責任者	同上	同上
実施監督者	鳥田 芳春	T I S株式会社 コーポレート本部 総務部 セキュリティ監査室
実施監督者	石橋 弘	T I S株式会社 コーポレート本部 総務部 セキュリティ監査室
実施者①	早矢仕 善弘	前記と同じ
実施者②	中西 大介	T I S株式会社 コーポレート本部 セキュアワンセンター シニアコンサルタント

(3) 作業記録

以下の日時にて監査を実施（日時順に記載）

日時	場所	作業内容
2015年02月14日	T I S株式会社	情報セキュリティポリシー見直し作業、監査表作成等
2015年03月06日	貴市庁内	監査
2015年03月07日	T I S株式会社	監査結果まとめ①
2015年03月08日	T I S株式会社	監査結果まとめ②
2015年03月08日	T I S株式会社	改善内容検討
2015年03月08日	T I S株式会社	最終納品物作成

5. 監査表

(1) 参考資料

松阪市提供

- ・松阪市情報セキュリティ基本方針
- ・松阪市情報セキュリティ対策基準
- ・松阪市個人情報保護条例（平成17年1月1日条例第7号）

総務省提供

- ・地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省）平成22年11月版
- ・地方公共団体における情報セキュリティ監査に関するガイドライン（総務省）平成22年11月一部改定版

(2) 作成方法

上記資料をもとに実施者が作成した草案を貴市経営企画部情報企画課と打ち合わせを行い作成。

(3) 監査表名称（ファイル名）

平成26年度情報セキュリティ監査詳細結果（平成26年度情報セキュリティ監査詳細結果.xls）

6. 参考資料

実施者が本業務を実施するにあたり参考にした書類。

NO	書類名称
1	松阪市情報セキュリティ基本方針
2	松阪市情報セキュリティ対策基準
3	地方公共団体における情報セキュリティポリシーに関するガイドライン(総務省)平成22年11月版
4	地方公共団体における情報セキュリティ監査に関するガイドライン(総務省)平成22年11月一部改定版
5	松阪市個人情報保護条例（平成17年1月1日条例第7号）
6	平成26年度情報セキュリティ監査業務委託仕様書

7. 添付書類

本報告書の添付資料は以下のとおりである。

- ・平成26年度情報セキュリティ監査詳細結果
- ・平成26年度情報セキュリティ対策基準 改善提案

8. 監査の結果

(1) 監査の手法

監査は、主に以下の手法を用いて実施した。

手法	概要と効果
ヒアリング	聞き取り調査。 実施者が監査項目に対して、その該当項目の業務内容を実施している担当者などに質問することで調査する。
エビデンス確認	目視での調査。 実施者が監査項目に対して、その該当項目の実施状況を知るために、該当項目を実施した際に残る紙または電子媒体での記録を調査する。

(2) 総合評価

概ね松阪市情報セキュリティ対策基準に定められた事項の実施確認または実施しているであろうと推察できる。なお、セキュリティ監査は大きく分類すると、

- ・プロセスに対しての監査
- ・結果に対しての監査

の2つに分類できる。

まず、「プロセスに対しての監査」では、松阪市情報セキュリティ対策基準に定められた内容に沿って実施されているかを監査した。その結果、実行すべき項目やそれに対する承認行為が体系的に構築されており、それは松阪市情報セキュリティ対策基準を十分に満たすものであると評価できる。また、職員またはシステム関係者が特別に意識せずとも日常執務の流れで無理なく実施できるように構築されていることを確認した。

次に、「結果に対しての監査」では、プロセスの実施によって得られる結果の正しさを監査した。その結果、実施結果に大きな瑕疵はなく、正確に実施されていることを確認した。

監査詳細項目は別紙（平成26年度情報セキュリティ監査詳細結果）のとおりであるが、200を超える監査項目のうち十分な実施を確認できなかった項目は以下の2つである。

- ① 実施をしているが改善を推奨する（△） 2項目
定期的な資産の棚卸し行為の未実施
フォーマット（定型文書雛型）の整備
- ② 未実施のため実施を推奨する（×） 1項目
脆弱性情報の組織的な収集行為の未実施

9. 松阪市情報セキュリティ対策基準に対する改善提案

(1) 評価基準

以下、実施者が監査を行うにあたり、基準とした評価項目である。

- ・修正すべきであると考ええる項目
 - ①記載されるべき項目が著しく欠損または不記載な場合
 - ②記載項目が著しく不合理な場合
 - ③別団体が作成する資料の内容と比較して著しく劣っている場合
など根本的に発想を変えるべきであると考えられる場合
- ・修正したほうがよいと考ええる項目
 - ①項目は記載されているが、その内容が不明瞭な場合
 - ②使用者（職員など）の実業務で混乱を招くような記載がある場合
など、より具体的な記載が必要だと考えられる場合
- ・修正することを推奨する項目（実施者の主観的評価）
 - ①実施者が主観的な観点から修正したほうがよいと考ええる場合
など、修正した方がよりよくなると考える場合

(2) 監査前評価

①評価方法

実施者は、貴市の監査を実施する前に、貴市から提供された情報セキュリティに関する資料を別団体の資料（総務省ガイドライン及び他地方自治体が作成した情報セキュリティに係る資料など）とその記載内容を比較検討し、また実施者が過去に実施した地方自治体の情報セキュリティ監査での経験などを踏まえ改善提案業務を実施する。

②対象

貴市から提供された情報セキュリティに関する書類

③結果詳細

平成 26 年度情報セキュリティ対策基準 改善提案を参照

④総合評価（まとめ）

修正することを推奨する項目 10 項目

(3) 監査後評価

①評価方法

実施者が貴市の監査を行った後に、その監査結果と貴市から提供された情報セキュリティに関する資料を比較検討し、改善提案業務を実施。

②対象

貴市から提供された情報セキュリティに関する書類及び実施者が行った監査結果。

③結果詳細

松阪市情報セキュリティ対策基準改善提案を参照

④総合評価

なし

以上