平成 27 年度　行政監査　結果報告（概要）

1　監査のテーマ

情報セキュリティについて

2　監査テーマの選定理由

平成27年5月に，日本年金機構における外部からのウィルスメールによる不正アクセスによって，大量の個人情報が流出するという事件が発生した。また同10月に「行政手続における特定の個人を識別するための番号の利用等に関する法律（いわゆるマイナンバー法）」が施行されたことに伴い，平成28年1月から国の行政機関や地方自治体における個人番号の利用が開始され，順次，その利用方法も拡大される計画である。

このような状況のなか，本市の個人情報を処理する業務系システム及び情報系ネットワークシステムについて，神戸市情報セキュリティポリシー等に照らして，情報セキュリティを維持・管理する仕組みが適切に整備・運用されているか，特に業務系システムの個人情報の一部を編集加工して他のシステムで利用する場合の運用が適切であるかを検証し，情報セキュリティ対策の維持・向上を図ることを目的として，監査を実施。

(報)P.41～42

3　監査対象部局等

全ての局室区，個人情報を処理する全 182 システム　(報)P.42

4　監査の期間

平成 27 年 8 月 19 日から平成 28 年 3 月 16 日　(報)P.42

5　監査の結果

(1) 監査結果の大要　　指摘事項　4 件　　意見　9 件

(2) 監査の結果（指摘事項・意見（抜粋））

監査の結果，事務処理はおおむね適正に行われているものと認められた。しかし，事務の一部について改善を要する事例があったので，今後，適正な事務処理に努められたい。

特に，情報セキュリティの確保と情報資産の活用を図るため，情報系ネットワーク上の外部記憶装置（NAS 等）を利用してデータの保存，活用する場合のセキュリティ対策の徹底を図るとともに，情報セキュリティ侵害が発生した場合又は侵害の恐れがある場合の組織全体の適切な初動対応を確保するため，情報セキュリティ責任者（企画調整局情報化推進部長）のリーダーシップの下，迅速に組織全体で対応（連絡，証拠保全，被害拡大の防止，復旧，再発防止等の措置）する仕組みを強化することを検討されたい。

(報)P.45～60

○　指　摘　事　項

（1）情報資産の管理

①情報資産の管理方法

ア)情報系ネットワーク上での NAS 利用による個人情報の保存

NAS 等を利用して個人情報を保存し活用する場合の個人情報の保護対策について，その対策を情報セキュリティポリシーで明記し，その徹底を図るべきである。　(報)P.61

（２）物理的セキュリティ

①サーバの管理

サーバを施錠可能な区画に設置し，容易に取り外せないように固定して取り付けるなど適正な管理を行うべきである。 (報)P.62

○ **意　見**

（１）情報資産の管理

①情報システム台帳

情報システム台帳は，本市の情報資産の管理及び情報システムの全容を把握する上で基本となる台帳である。台帳と実際が異なる事例が散見されたので，次の事項について検討されたい。

ア)台帳の定期的な更新（台帳作成の義務化）

イ)登録すべき情報システムの明確化（台帳に登録すべきシステムの定義の明確化） (報)P.64

②情報資産の保管方法

ア)機密性３のデータの保存方法

情報漏えい対策を強化するため，対策基準等に機密性３のデータの具体的な保存方法を明記し，その方法を徹底することを検討されたい。 (報)P.65

（２）物理的セキュリティ

①コンピュータの設置場所

セキュリティレベルの向上の観点から，サーバの集約化を検討されたい。 (報)P.66

②スタンドアロンシステムのあり方

スタンドアロンシステムについて，情報系ネットワークのイントラで処理することも含めて，よりセキュリティ対策の確実なあり方を検討されたい。 (報)P.66

（３）技術的セキュリティ

①不正アクセス対策の強化

不正アクセス対策をより明確にするため，総務省のガイドラインも参考にして，対策基準を見直し，サービス不能攻撃及び標的型攻撃への対策を明記することを検討されたい。 (報)P.66～67

（４）運用

①情報システムの監視

ア)ログ解析

ログ解析は，不正アクセス・不正利用の早期発見，被害拡大の防止に資することから，特に基幹業務系システムについて，ログ解析の実施水準を標準化することを検討されたい。 (報)P.67

②情報セキュリティインシデントへの対応

ア)CSIRT （Computer Security Incident Response Team）の設置

インシデントに備えた全庁的な各種対応やインシデント発生時に主導的に適時対応を指示する仕組みを明確にし，初動対応力の強化を図るため，情報セキュリティ責任者（企画調整局情報化推進部長）を中心に，情報セキュリティ管理者，情報基盤管理者，基幹業務系ネットワーク管理者，情報系ネットワーク管理者，主要な業務システム管理者並びに情報セキュリティに関する事務局で構成する CSIRT の設置を検討されたい。 (報)P.67～68