

令和2年度情報セキュリティ外部監査
監査報告書

令和3年3月24日

株式会社 I T スクエア

目 次

第1章 実施概要	1
第2章 監査結果	3

第1章 実施概要

1 監査目的

情報セキュリティポリシーは、「Plan」（文書化したポリシーの確立）、「Do」（対策の導入・運用）、「Check」（対策の評価・見直し）、「Act」（対策の有効性の維持・改善）のPDCAサイクルに基づき運用していく必要があります。

このPDCAサイクルの「Check」に相当するものとして、第三者の客観的な視点で、運用状況についての『助言型監査』を実施し、情報セキュリティレベルの維持・向上を図ることを目的に実施しました。

2 監査対象

以下の5システムを監査対象としました。

No.	システム名	所管所属（被監査所属）
1	新潟市住民記録システム	市民生活部 市民生活課
2	国民健康保険収納支援システム	福祉部 保険年金課
3	固定資産税補完システム	財務部 資産評価課
4	家屋評価システム	財務部 資産評価課
5	税収納支援システム	財務部 市税事務所 納税課

3 監査対象期間

令和2年4月1日から本調査の実施日までを対象期間としました。

ただし、情報システムの開発・運用・保守については、開発・更新を実施した時期から本調査の実施日までを対象期間としました。

4 実施内容

新潟市情報セキュリティポリシー（基本方針・対策基準）等への準拠性監査

5 監査の重点項目

以下の三点を監査の重点項目としました。

- ①個人情報（個人番号及び特定個人情報を含む）の取扱い
- ②情報システムの利用者管理（ID・パスワードの取扱い）
- ③コンピュータウイルス対策

6 適用基準等

【適用基準（新潟市）】

- ①新潟市情報セキュリティ基本方針
- ②新潟市情報セキュリティ対策基準
- ③その他、新潟市職員が遵守すべき情報セキュリティに関する手引き、手順書等

【参考基準】

- ①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（平成30年9月版 総務省）
- ②情報セキュリティ管理基準（平成28年改訂版 経済産業省）

- ③特定個人情報の適正な取り扱いに関するガイドライン
(令和2年5月版 個人情報保護委員会)
- ④情報セキュリティ監査基準 (平成15年経済産業省告示第114号)
- ⑤情報セキュリティ監査基準 実施基準ガイドライン (平成15年 経済産業省)
- ⑥情報セキュリティ監査基準 報告基準ガイドライン (平成15年 経済産業省)
- ⑦個別管理基準 (監査項目) 策定ガイドライン (平成15年 経済産業省)

7 監査実施体制

(1) 新潟市様監査担当部署

総務部ICT政策課

(2) 監査人

株式会社 I T スクエア

8 監査実施方法

(1) 監査実施説明会

被監査所属を対象に、監査の目的、実施方法、日程及び予備調査の実施方法等の説明を行いました。

開催日：令和2年12月24日、25日

会 場：新潟市役所分館

(2) 予備調査

監査項目の抽出、監査チェックリストの作成及び判定の尺度を決定するため、以下の①、②を実施しました。

- ①新潟市情報セキュリティポリシー、被監査所属及び情報システムに関する文書・記録の閲覧

実施期間：令和2年12月25日～令和3年1月22日

- ②被監査所属及び情報システムを対象としたアンケートの実施

実施期間：令和2年12月25日～令和3年1月14日

(3) 本調査

監査チェックリストに基づきヒアリング、資料閲覧、視察（現場確認）を行いました。

実施期間：令和3年1月25日～1月26日

(4) 監査報告会

総務部ICT推進課様及び被監査所属へ監査実施概要及び結果概要を報告し、改善提言を行いました。

開催日：令和3年3月15日、17日

会 場：新潟市役所本館、ふるまち庁舎

第2章 監査結果

1 監査結果

ほとんどの項目で情報セキュリティに関して良好であると評価することができました。しかし、監査基準に適合・準拠した状況が確保されていない事項（指摘事項）も検出されました。以下に監査結果の概要を記します。

(1) 指摘事項

「情報資産管理」「情報システムの使用者管理」「電磁的記録媒体の管理」「情報システムの使用状況把握」「情報資産の施錠管理」「情報システムのID、パスワード管理」「情報システムのウイルス対策」に関する指摘事項を検出しました。これらについては、貴市（被監査所属）の事情に合わせて是正措置を実施されることを推奨します。

2 全体的な改善提言

(1) 情報資産台帳の維持・管理

一部の情報資産が情報資産台帳に登録されていない状況が見られました。漏えい等に直接つながる問題ではありませんが、情報資産台帳に登録して管理することを推奨します。

(2) 情報システムの利用者管理（ID・パスワードの取扱い）

情報システムのIDの管理方法やパスワードに関して不備が検出されました。ID、パスワードの管理を徹底することを推奨します。

(3) コンピュータウイルス対策

情報システムの脆弱性対策（セキュリティパッチの適用）に関して不明瞭な部分がありました。パッチマネジメントの仕組みを確立することを推奨します。

以上

令和2年度情報セキュリティ外部監査

監査報告書

令和3年3月24日

株式会社ITスクエア
