

令和5年度新潟市情報セキュリティ外部監査業務委託  
監査報告書  
【概要版】

令和6年2月27日

株式会社カシックス

新潟市情報システム課 一部補記

## I. 監査の概要

### 1. 監査目的

新潟市の情報セキュリティポリシーに準拠した適切な対策が実施されているか、独立かつ専門的な立場から検証し改善することで、情報セキュリティ対策の向上に資することを目的とします。(助言型監査)

### 2. 監査対象

次の所属が所管するシステムを監査対象として実施しました。

| No. | 被監査所属      | 監査対象システム      |
|-----|------------|---------------|
| 1   | 福祉部 障がい福祉課 | 障がい福祉システム     |
| 2   | 福祉部 福祉総務課  | 生活保護システムふれあい  |
| 3   | 福祉部 保険年金課  | 新潟市国民健康保険システム |

### 3. 監査範囲

監査対象システムの運用

### 4. 監査対象期間

監査実施日から過去1年間の記録を監査対象の基本としました。

### 5. 監査手続き

- (1) 文書類・記録類の閲覧
- (2) 職員等へのヒアリング
- (3) 執務室の視察

※技術的検証は含みません。

### 6. 監査場所

監査対象システムの所管所属の執務室等

### 7. 適用する基準

#### (1) 監査の基準

- ① 新潟市情報セキュリティポリシー (基本方針及び対策基準)
- ② 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 (令和5年3月版 (総務省))
- 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 (令和5年3月版 (総務省))
- ④ 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5年7月版 (個人情報保護委員会))
- ⑤ その他情報セキュリティ監査を実施するうえで遵守・参考とする必要がある基準

#### (2) 評価の基準

- ① 地方公共団体の情報セキュリティレベルの評価に係る制度の在り方に関する調査研究報告書 (総務省)
- ② 評価の基準の各項目における評価点は、次の1～5段階の定義に基づいて決定

しました。

| 評価点 | 分類   | 評価点の定義                         |
|-----|------|--------------------------------|
| 5   | 適合   | 現時点における地方公共団体における対応として、推奨できる水準 |
| 4   | 改善事項 | 概ね推奨できる水準に近いが、一部改善の余地がある       |
| 3   | 指摘事項 | 基礎的な取り組みはなされているが、改善の余地がある      |
| 2   |      | 基礎的な取り組みはなされているが、改善すべき点が多い     |
| 1   |      | 基礎的な取り組みがなされていない               |

※総務省「地方公共団体の情報セキュリティレベルの評価に係る制度の在り方に関する調査研究報告書」（平成18年3月）より

## 8. 監査人

株式会社カシックス

## 9. 監査の実施

### (1) 予備調査

- ① 監査ポイントを絞り込み、効率的な監査業務を行うため、監査対象所属から事前にご提示いただいた資料に基づき、業務の概要、システムの概要、システムの運用、情報資産の流れ、手順書等の整備状況を把握しました。
- ② 文書閲覧の結果、不明点を補完し、システム運用やセキュリティ上の目標・懸念事項の把握をするために、文書による事前ヒアリングを実施しました。

### (2) 本監査

- ① 被監査所属の担当者に、監査チェックリストを使用してセキュリティ対策状況についてヒアリングと文書や記録の閲覧を行いました。
- ② 監査項目により、対策実施における監査の証跡として文書や記録を提示または可能な場合、コピーを提出頂きました。
- ③ 被監査所属での対策状況や職員の遵守状況を確認するために執務室等を視察しました。

## 10. 監査項目

- (1) 情報資産の分類と管理
- (2) サーバ等の管理
- (3) 管理区域の管理
- (4) 職員等のパソコン等の管理
- (5) 職員等の遵守事項
- (6) ID及びパスワードの管理
- (7) 不正プログラム対策
- (8) 外部委託

## 11. 監査スケジュール

| イベント            | 日時   | 概要   |
|-----------------|--|--|
| 実施<br>計画<br>説明会 | 令和5年12月5日(火)<br>9時30分～10時00分                     | 監査実施計画の説明会を実施しました。   |
| 予備<br>調査        | 令和5年12月5日(火)<br>〃<br>令和5年12月25日(月)               | ご提示頂いた資料により、業務の概要、システムの概要、システムの運用、情報資産の流れ、手順書等の整備状況を確認しました。<br>-----<br>予備調査ヒアリングシートによる事前調査を行いました。 |
| 本監査             | 【障がい福祉システム】<br>令和6年1月23日(火)<br>10時00分～12時00分     | 監査対象所属に対して、以下のとおり実施しました。<br>①オープニングミーティング<br>(約5分)   |
|                 | 【生活保護システムふれあい】<br>令和6年1月23日(火)<br>13時30分～15時30分  | ②ヒアリング・閲覧<br>(約60分)<br>③現地視察<br>(約30分)<br>④監査人会議(監査人のみ)<br>(約15分)                                  |
|                 | 【新潟市国民健康保険システム】<br>令和6年1月24日(水)<br>10時00分～12時00分 | ⑤中間報告※<br>(約10分)<br>※監査において検出された事実を確認しました。   |
| 監査<br>報告書       | 令和6年2月9日(金)                                      | 監査人より監査報告書(案)を提出しました。  |
|                 | 令和6年2月16日(金)                                     | 監査対象所属が監査報告書(案)を確認しました。  |
|                 | 令和6年2月19日(月)                                     | 監査人より監査報告書を提出しました。   |
| 監査<br>報告会       | 令和6年2月27日(火)                                     | 監査報告書に基づく監査結果、見直し及び改善策についての報告会を実施しました。   |

## II. 監査結果

今回の監査は、貴市（被監査所属）の情報資産の取扱い及び所管する情報システムの運用管理が新潟市情報セキュリティポリシー（基本方針・対策基準）等の監査基準に適合・準拠して行われているかを中心に実施しました。

その結果、業務運用上での情報セキュリティ対策の取り組みにおいて、監査基準に適合・準拠していない指摘事項は検出されませんでした。改善事項が4件検出されました。

### 1. 検出事項

「情報資産管理台帳の作成」、「記憶装置の情報消去」、「情報セキュリティインシデントの報告手順」、「委託事業者の選定基準」に関する改善事項を検出しました。改善事項につきましては、貴市（被監査所属）の事情に合わせて改善措置を検討されることを推奨します。

## III. 改善提言

主な改善提言を以下に示します。

### (1) 情報資産管理台帳の作成

情報資産管理台帳の定期的な更新の確認ができませんでした。

情報資産管理台帳は、少なくとも年1回は見直すよう定められています。情報資産管理台帳は、情報資産を分類し、分類に応じた取扱い（入手、利用、保管、運搬、提供・公表、廃棄等）を定義するために必要な管理台帳です。情報資産の機密性・可用性・完全性を保持するためにも、情報資産管理台帳を定期または随時に更新することを推奨します。

### (2) 記憶装置の情報消去

課で管理している10本のUSBメモリを管理台帳で管理されていますが、所在不明のまま放置されているUSBメモリが2本ありました。

2本とも、定められた場所でないと保管理されていることが確認されました。

「(1) 情報資産管理台帳の作成」とも関連しますが、電磁的記録媒体は毎月1回以上状況把握することが定められています。ある・なしの把握にとどまらず、ない状態を長く続けられないためにも、なぜないのかを追求し、紛失のリスクを回避するようにしてください。

### (3) 情報セキュリティインシデントの報告手順

インシデント発生時に取るべき行動を明確にお答えいただけませんでした。また、マニュアルの整備がされていないとのことでした。

情報セキュリティインシデントはいつ発生するかわかりません。何かが起こってから取るべき行動を確認していると、その間に状況が悪くなる可能性を否定できません。

インシデント発生時に情報システム担当者がいるとは限りません。事前にマニュアルを整備し、課員全員が手順を理解しておくことをお勧めします。

### (4) 委託事業者の選定基準

業務開始に際し必要な書類が、監査の時点で揃っていませんでした。契約書に必要な書類は、契約の中身によって違ってくるのが予想されます。契約時に必要な書類を確認するチェックリストを作成するなどして、業務が始まるまでに必要な書類が揃う手順を整えることを推奨します。

以上