**監査結果公表第８号**

行政監査結果報告について

地方自治法第１９９条第２項の規定に基づき、一般行政事務の執行について監査をしたので、同条第９項の規定により、その結果に関する報告を公表する。

令和３年　３月１１日

四日市市監査委員　加　藤　　光
同　廣　田　正　文
同　森　川　　慎
同　荒　木　美　幸

## 第１　監査の概要

１　監査の種類

地方自治法第１９９条第２項の規定に基づく行政監査

２　行政監査のテーマ

情報セキュリティの管理について

３　監査の目的

地方公共団体は、住民の個人情報等の重要情報を多数保有し、それを基に多くの行政サービスを提供している。その業務の多くは、情報システムやネットワークを活用して行われていることから、そのトラブルは、組織内部にとどまらず市民に多大で重大な影響を及ぼす。本市の保有する情報資産を守り、行政サービスの提供という業務を継続するため、情報セキュリティ対策を講じることが必要である。本市の情報セキュリティの維持管理に係る仕組みが適切に整備・運用されているかを検証し、情報セキュリティ対策の維持向上を図ることを目的とする。

４　監査の対象

本市全体の情報セキュリティの管理を統括する総務部ＩＣＴ戦略課を対象に、本市の情報セキュリティ管理が適切になされているかについて、監査を実施した。

５　監査の実施場所及び監査期間等

| | |
|---|---|
| 実施場所 | 四日市市役所　監査委員室 |
| 事前調査期間 | 令和３年１月１４日から令和３年２月　９日まで |
| 監査期間 | 令和３年２月１０日 |

６　監査の主な実施内容

四日市市監査基準に基づき、情報セキュリティの管理に係る事務についてその内在するリスクを想定したうえでリスクへの対応策が講じられリスクが発現していないか、当該事務の管理が法令等に適合し、正確で、最小の経費で最大の効果を挙げているか、その組織及び運営の合理化に努めているか等について、監査対象所属に対し、必要に応じて関係書類や資料の提出を求めるとともに、監査資料に基づく関係職員からの説明の徴取、視察等の方法により監査を実施した。なお、この監査に当たっては、情報通信技術（ＩＣＴ）に関する専門的な知見・技術を必要とするため、総務省情報流通行政局が実施する地域情報化アドバイザー派遣制度を活用し、地域情報化アドバイザーの派遣を受け、関係職員からの説明の徴取、視察等の調査に立ち会わせた。

## 第２　監査対象事務の概要

### １　情報セキュリティの概要

#### （１）地方公共団体における情報セキュリティについて

地方公共団体の情報セキュリティ対策については、総務省が「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」（平成１３年３月策定）を定め、これによりその実施方法の概要を示している。このガイドラインによると、地方公共団体における情報セキュリティの考え方は、次のとおりである。

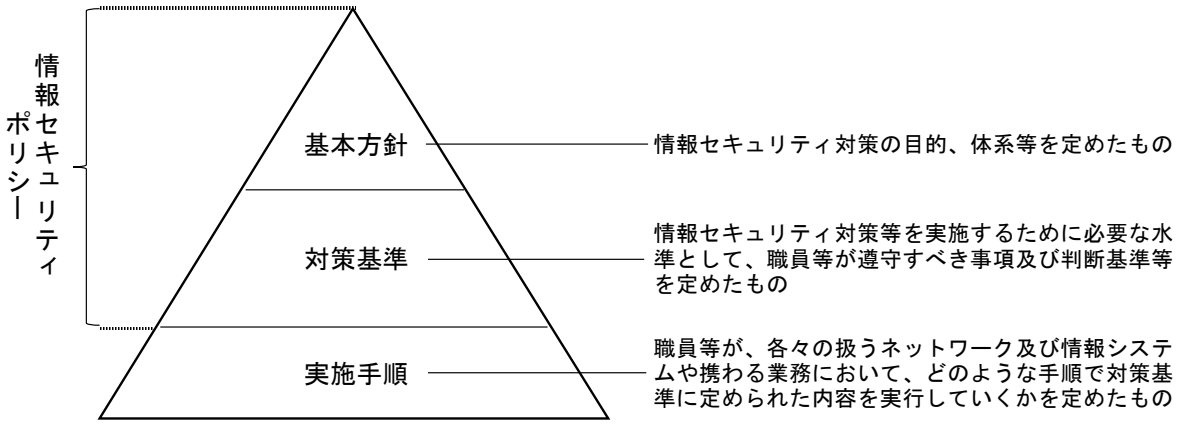
> 地方公共団体は、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、ほかに代替することができない行政サービスを提供している。また、地方公共団体の業務の多くが情報システムやネットワークに依存していることから、住民生活や地域の社会経済活動を保護するため、地方公共団体は、情報セキュリティ対策を講じて、その保有する情報を守り、業務を継続することが必要となっている。
>
> 今後、各種手続のオンライン利用の本格化や情報システムの高度化等、電子自治体が進展することにより、情報システムの停止等が発生した場合、広範囲の業務が継続できなくなり、住民生活や地域の経済社会活動に重大な支障が生じる可能性も高まる。また、地方公共団体はＬＧＷＡＮ等のネットワークにより相互に接続しており、一部の団体で発生したＩＴ障害がネットワークを介して他の団体に連鎖的に拡大する可能性は否定できない。
>
> これらの事情から、全ての地方公共団体において、情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくことが必要となっている。また、情報セキュリティの確保に絶対安全ということはないことから、情報セキュリティに関する障害・事故及びシステム上の欠陥（以下「情報セキュリティインシデント」という。）の未然防止のみならず、情報セキュリティインシデントが発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要である。

#### （２）情報セキュリティポリシーについて

総務省策定の「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」によると、「情報セキュリティ対策を徹底するには、対策を組織的に統一して推進することが必要であり、そのためには組織として意思統一し、明文化された文書」を定める必要があるとされており、これが「情報セキュリティポリシー」である。

情報セキュリティポリシーの体系は、別図１に示すとおり階層構造となっており、情報セキュリティ対策における基本的な考え方を定めた「基本方針」と、この基本方針に基づき、全ての情報システムに共通の情報セキュリティ対策の基準を定めた「対策基準」の２つで構成される。「対策基準」を具体的なシステムや手順、手続に展開して、個別の実施事項を定めるものが「実施手順」である。「基本方針」と「対策基準」を総称したものが「情報セキュリティポリシー」である。

〔別図１〕　情報セキュリティポリシーに関する体系図




情報セキュリティ対策の実施プロセスは、情報セキュリティポリシー・実施手順の策定・周知を行う「策定･導入（Ｐｌａｎ)」、セキュリティ対策の実施やセキュリティ侵害時の対応をする「運用（Ｄｏ)」、監査・点検を行う「評価（Ｃｈｅｃｋ)」、情報セキュリティポリシー・実施手順の更新を行う「見直し（Ａｃｔｉｏｎ)」の４段階に分けることができる。この実施サイクルを定期的に繰り返すことによって、環境の変化に適応しつつ、情報セキュリティ対策の水準の向上を図ることができ、情報セキュリティは確保される。

令和２年１２月に、「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」において、情報セキュリティ対策として、行政手続のオンライン化への対応も踏まえた「三層の対策」の見直しやテレワーク等のリモートアクセスの安全な実施方法の検討・整理などを実施するための改定が行われた。

※「三層の対策」の見直しの概要は、次のとおりである（総務省「自治体情報セキュリティ対策の見直しのポイント」から引用)。

①マイナンバー利用事務系の分離の見直し

住民情報の流出を徹底して防止する観点から他の領域との分離は維持しつつ、国が認めた特定通信に限り、インターネット経由の申請等のデータの電子的移送を可能とし、ユーザビリティの向上及び行政手続のオンライン化に対応。

②ＬＧＷＡＮ接続系とインターネット接続系の分割の見直し

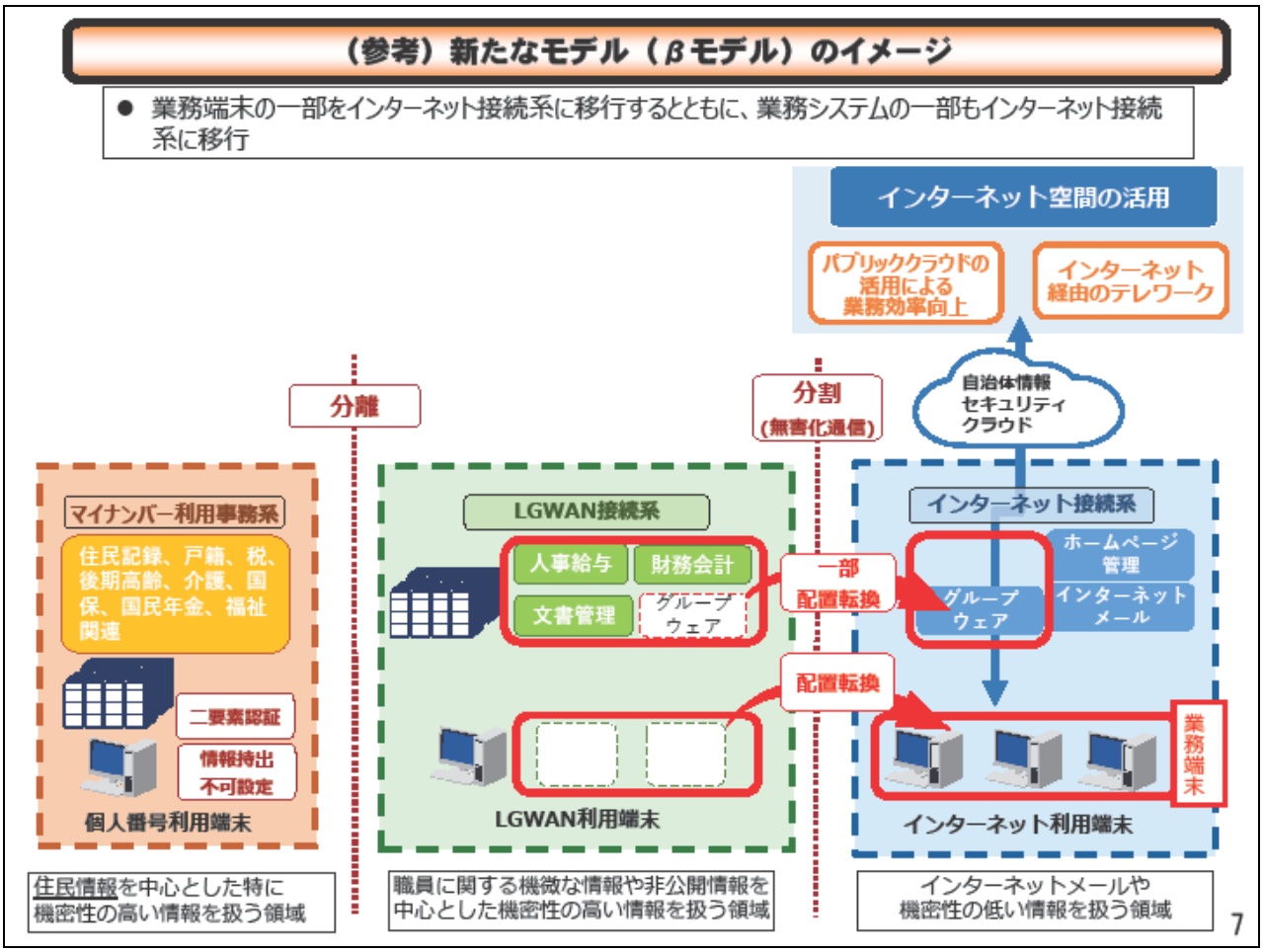
従来の「三層の対策」の基本的な枠組みを維持しつつ、効率性・利便性の高いモデルとして、インターネット接続系に業務端末・システムを配置した「新たなモデル」（別図２）を提示。ただし、「新たなモデル」の採用に当たっては人的セキュリティ対策の実施が条件となる。

「三層の対策」は、セキュリティ強化のため、①マイナンバー利用事務系では端末からの情報持ち出し不可設定等を図り、住民情報流出を徹底して防止すること、②ＬＧＷＡＮ接続系とインター

ネット接続系を分割し、ＬＧＷＡＮ環境のセキュリティを確保すること、③都道府県と市区町村が協力して、自治体情報セキュリティクラウドを構築し、高度な情報セキュリティ対策を実施することである。

ＬＧＷＡＮとは、「総合行政ネットワーク」の略称で、地方公共団体の組織内ネットワーク（庁内ＬＡＮ）を相互に接続し、高度情報流通を可能とする通信ネットワークとして整備し、地方公共団体相互のコミュニケーションの円滑化、情報の共有による情報の高度利用等を図ることにより、各地方公共団体と国の各府省、住民等との間の情報交換手段の確保のための基盤とすることを目的とした、高度なセキュリティを維持した行政専用のネットワーク（インターネットから切り離された閉域ネットワーク）をいう。

〔別図２〕　「三層の対策」の見直し
（総務省「自治体情報セキュリティ対策の見直しのポイント」から抜粋）



## 2　本市の情報セキュリティ管理の概要

### （1）四日市市情報セキュリティポリシーについて

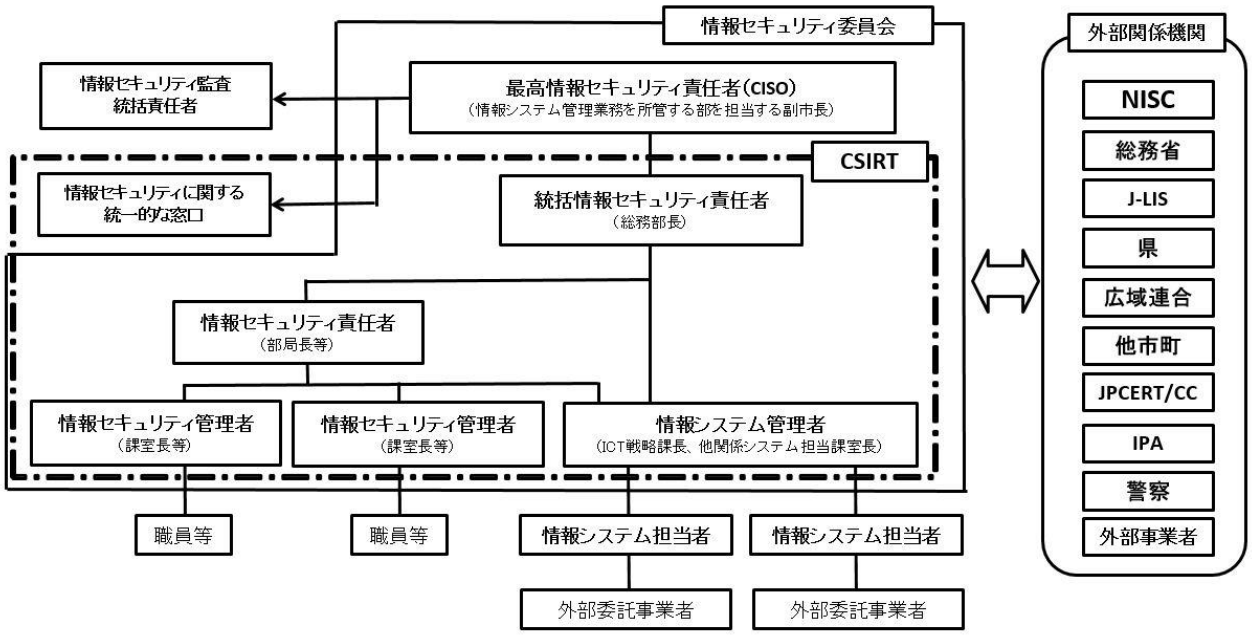
本市においては、総務省が策定した「地方公共団体における情報セキュリティポリシーに関するガイドライン」を参考に、平成１９年度に「四日市市情報セキュリティポリシー」を策定した。そののち、平成２７年３月と平成３０年９月に「地方公共団体における情報セキュリティポリシーに関するガイドライン」が改定されており、これらの改定に合わせて、平成２９年１月と平成３１年２月にそれぞれ所要の改定を行っている。

四日市市情報セキュリティポリシーにおいて規定されている情報セキュリティに関する体制と情報セキュリティ対策の内容は、それぞれ別表１及び別図３並びに別表２のとおりである。

〔別表１〕　情報セキュリティに関する体制

| 役職等名称<br>〔担任者〕 | 主な権限・責任 |
|---|---|
| 最高情報セキュリティ責任者<br>（ＣＩＳＯ）<br>〔総務部担当副市長〕 | 本市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。 |
| 統括情報セキュリティ責任者<br>〔総務部長〕 | ＣＩＳＯを補佐する。ＩＣＴ戦略課長に情報セキュリティ対策に係る実務を補佐させ、必要に応じて権限を委譲することができる。 |
| 情報セキュリティ責任者<br>〔部長、局長等〕 | 当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。 |
| 情報セキュリティ管理者<br>〔課長等〕 | その所管する課室等の情報セキュリティ対策に関する権限及び責任を有する。 |
| 情報システム管理者<br>〔情報システム管理所属の課長等〕 | その所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。 |
| 情報システム担当者<br>〔課等の担当職員〕 | 情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う。 |
| 情報セキュリティ委員会 | 情報セキュリティに関する重要事項等を決定する。 |
| 情報セキュリティに関する統一的な窓口（ＣＳＩＲＴ） | 情報セキュリティインシデントに関するコミュニケーションの核として、情報セキュリティインシデントが発生した際に、発生状況のとりまとめ、ＣＩＳＯへの報告、報道機関等への通知・公表などを行う。 |

〔別図３〕　組織体制図




〔別表２〕　情報セキュリティ対策の内容

| 対策 | 対策内容の概要 |
|---|---|
| 組織体制の確立 | 本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。 |
| 情報資産の分類と管理 | 本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。 |
| 情報システム全体の強靭性の向上 | 主に住民情報などの機密情報を取り扱う「基幹業務系（個人番号利用系）」と、その他の行政情報を取り扱う「情報系（ＬＧＷＡＮ系）」と、インターネットに接続された「インターネット系」の３つのネットワークで構成されている。それぞれに応じた対策を講じる。<br>ア　基幹業務系　　原則として、他の領域との通信をできないようにする。<br>イ　情報系　　インターネット接続系の情報システムとの通信経路を分割する。<br>ウ　インターネット系　　不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。 |
| 物理的セキュリティ | サーバ等、サーバ室等、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じる。 |
| 人的セキュリティ | 情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。 |

| | |
|---|---|
| 技術的セキュリティ | コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。 |
| 運用 | 情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じる。 |
| 外部サービスの利用 | 外部委託する場合には、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。 |
| 評価・見直し | 定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図る。 |

（2）四日市市情報セキュリティ実施手順について

四日市市情報セキュリティポリシーに基づく情報セキュリティ対策及び特定個人情報保護のための安全管理措置を実施するために必要となる事項を、「四日市市情報セキュリティ実施手順」として定めた。その内容は、公開することにより本市の行政運営に重大な支障を及ぼすおそれがあるため非公開とされている。

## 第３　監査の着眼点

１　想定されるリスクからの着眼点

情報セキュリティの管理に係るリスクを、その仕組みが適切に整備・運用されず、重大な情報セキュリティインシデント（情報セキュリティに関する障害・事故及びシステム上の欠陥をいう。以下同じ。）が発生するリスクと想定し、リスク発現を防止するための対応策を確認するため、次のとおり監査の着眼点を設定した。

（1）情報資産を保護するための基本方針等が策定されているか。
（2）全庁的な情報システムに係るセキュリティ管理を統括する体制が整備され、管理状況が適切に把握されているか。
（3）情報システムのサーバ等の管理は適切になされているか。
（4）情報システムの運用、保守等を外部委託する場合、受託事業者における情報セキュリティ確保のための適切な監督は行っているか。
（5）不正アクセスやウイルスなどに対する対策は適切に講じられているか。
（6）情報システムの障害・事故時の対応計画について策定しているか。
（7）情報セキュリティ対策の実施に係るＰＤＣＡサイクルは機能しているか。

２　３Ｅ（経済性、効率性、有効性）、合規性等の視点からの着眼点

情報セキュリティの管理に係る事務について、経済性、効率性、有効性及び合規性等の視点

を監査の着眼点として設定した。

## 第４　監査の結果

上記の着眼点に基づき監査を行った結果、次のとおり、リスクが発現したもの及びリスク発現の可能性のあるもの並びに事務の一部に改善を要するものなどが見受けられた。今後の事務執行に当たっては、これらに十分留意するとともに、その措置を講じるよう要望する。

なお、措置を講じたときは、遅滞なく報告されたい。

### １　想定されるリスクからの着眼点に着目して行った監査の結果

（１）情報資産を保護するための基本方針等が策定されているか。

**リスク発現の可能性（○予防策あり、△可能性あり、×発現）**

○　情報セキュリティ対策を組織的に統一して推進するため、情報セキュリティ対策の基本方針とそれを実行に移すための基準である対策基準（併せて「情報セキュリティポリシー」という。以下同じ。）が策定されている。

（２）全庁的な情報システムに係るセキュリティ管理を統括する体制が整備され、管理状況が適切に把握されているか。

**リスク発現の可能性（○予防策あり、△可能性あり、×発現）**

△　情報セキュリティ対策を確実に行うため、最高情報セキュリティ責任者（ＣＩＳＯ）をトップとする組織体制となっており、決定機関である情報セキュリティ委員会、情報セキュリティインシデントに対処するための窓口（ＣＳＩＲＴ）が設置されている。

情報セキュリティインシデントへの対処については、「情報セキュリティ緊急時対応計画」を定め、これに基づき実施している。

情報資産を機密性・完全性・可用性に基づいて分類し、分類に応じた取扱いを情報セキュリティポリシーに定め、それに基づく管理を行っている。

これらのほかに、以下の指摘及び意見に掲げる事象又は状況が生じており、情報セキュリティの管理の仕組みが適切に整備・運用されず、重大な情報セキュリティインシデントが発生するリスクが発現する可能性がある。

したがって、次のとおり、指摘し、及び、意見する。

**指　摘**

情報セキュリティ責任者等について

情報セキュリティ責任者は各部局長が、情報セキュリティ管理者は各課室長等がそれぞれ担当することが情報セキュリティポリシーに定められているが、このことは十分に周知されていないように思われる。各部局・所属における情報セキュリティ対策を実効あるものとするため、役職を担任する全ての職員に対し、情報セキュリティ対策に関する知識と技術の教育・啓発を行い、それぞれの職務・責任等に関する意識づけを徹底すること。当該職員による積極的な取組みを推進するため、その教育・啓発内

容は、当該知識・技術を取得することの動機づけを確保できるものとし、丁寧に行うこと。

**意　見**

①　情報セキュリティに係る組織体制の強化について

業務が情報システム化され、情報システムへの依存度は大きく、情報システムの数も多くなっている。社会状況の変化や新たな脅威の発生などにより情報セキュリティ上のリスクは常に変化しており、その変化に対応するためには、常に最新の情報セキュリティに関する情報を収集できる体制が必要となる。外部の専門家を職員として任用したり、情報処理に関する資格の取得を奨励したりして（別表３参照）、情報通信技術に関する専門的な知見・技術を持った職員の育成確保を図り、組織体制の強化に努めること。

②　ＣＳＩＲＴの体制強化について

ＣＳＩＲＴは、当課の職員による体制となっているが、情報セキュリティインシデントの発生の際には報道機関等への通知、被害の拡大防止のための応急措置の実施、被害に対する補償等の対応も重要となることから、広報部門、財政部門、法務部門を所管する所属も体制に組み入れることにより、機動的な体制となるよう強化を図ること。

③　ＰｏＣについて

情報セキュリティインシデントの発生に関する情報等を受け付ける統一的な窓口（ＰｏＣ）を当課に設置しているが、外部の者からの情報等も多く収集できるよう、ＰｏＣが当課に設置されていることを、ホームページなどを活用して広く周知すること。

④　情報資産の分類について

情報資産保護のため、情報資産を機密性・完全性・可用性に基づいて分類し、分類に応じた取扱いを情報セキュリティポリシーに定めているが、個別の情報資産がどの分類に該当するのかを示す統一的な物差しがないため、当該分類に該当する情報資産の例を示すなどした運用基準を作成すること。

〔別表３〕　市区町村における情報化についての職員の人材育成等の実施状況
（複数回答。平成３１年４月１日現在。）
（総務省自治行政局地域情報政策室「地方自治情報管理概要（令和元年度）」（令和２年３月）から引用し作成）

| | 情報化のために外部の専門人材を採用 | 情報処理（技術）に関する資格取得を奨励 | 民間企業等へ職員を研修派遣 |
|---|---|---|---|
| 団体数 | １０５ | ９２ | ２４ |
| 全体に占める割合 | ６．０％ | ５．３％ | １．４％ |

※　調査対象となった市区町村は 1,741 団体

（３）情報システムのサーバ等の管理は適切になされているか。

**リスク発現の可能性（〇予防策あり、△可能性あり、×発現）**

△　サーバ等は、空調設備により適切な温度や湿度が保たれている場所に設置されている。設置場所は津波等による浸水の影響がない建物の中層階にある。サーバはラックに固定されて設置されており、設置場所のある建物自体の免震化もなされている。電源供給の停止に備えて予備電源が備え付けられている。

サーバ等の保守管理については、機器等の導入に際しては必ずメーカー等の保守契約を付けるようにしており、保守業者による障害対策がなされている。

サーバの管理区域への出入りについては、入退出できる者を制限するとともに、ＩＤカード等により入退出者の管理を行っている。

端末等の外部への持ち出しは、原則として禁止しており、持ち出す場合には所属長の許可が必要となっている。

これらのほかに、以下の指摘及び意見に掲げる事象又は状況が生じており、情報セキュリティの管理の仕組みが適切に整備・運用されず、重大な情報セキュリティインシデントが発生するリスクが発現する可能性がある。

したがって、次のとおり、指摘し、及び、意見する。

**指　摘**

①　サーバ室内の整理整頓について

サーバ室内には、サーバが設置されているほかに、作業を行うための職員がいたり、印刷機や多数の不用となったパソコン、空きダンボール箱などが置かれていたりして、精密機器と人と物が混在し、雑然とした状況であった。また、サーバラックには、機器の排気熱が他の機器の周辺に滞留するのを防止するため、ダンボール紙による目張りがされていたり、機密情報が載った紙類が「中古のダンボール箱」に入れられて保管されていたりするなど、重要な情報資産を管理する方法としては相応しいとは思えない方法により管理がなされていた。現在のＣＩＳＯはその職に就いてからサーバ室に入室したことがなく、その状況を確認したことがないことも問題であると考える。

不用なものは廃棄し、機器などの設置場所が誰が見ても一目でわかるよう整理整頓を行い、サーバ等の精密機器と人と物とが明確に分離されたレイアウトとするとともに、重要な情報資産に相応しい方法でその管理を行うこと。そして、サーバにとって最適な環境を維持できるよう管理監督していくこと。

加えて、改修工事を伴うほどの抜本的なレイアウト変更を行うことにより、サーバの安全な運用と職員等の効率的な作業の実施を確保した機能的なサーバ室を早急に実現させること。

②　サーバのバックアップデータの管理について

サーバのバックアップデータについて、サーバ室とは別の場所で管理しており、その場所へは鍵付きの保管箱に入れて移動させている。移動準備のため保管箱がサーバ室内の机の上に置かれていたが、その鍵も同じ机の近接したところに置かれていた。保管箱の設置場所やその鍵の管理方法を見直すなど、バックアップデータの管理の厳重

化を図ること。

**意　見**

ＩＤカード管理の厳重化について

サーバ室への入室権限を有するＩＤカードについては、それを保有する職員がそれぞれで施錠できる机の引き出しに入れて管理している。権限を有するＩＤカードを一元的に保管する方法などを検討し、管理の更なる厳重化を図ること。

（４）情報システムの運用、保守等を外部委託する場合、受託事業者における情報セキュリティ確保のための適切な監督は行っているか。

**リスク発現の可能性（〇予防策あり、△可能性あり、×発現）**

〇　契約書には、個人情報の取扱いや秘密の保持について定めた「個人情報取扱注意事項」の遵守に係る規定が設けられており、これに基づき受託事業者に対し必要に応じて必要な指示を行っている。

（５）不正アクセスやウイルスなどに対する対策は適切に講じられているか。

**リスク発現の可能性（〇予防策あり、△可能性あり、×発現）**

×　パソコンにログインするときには、基幹業務系においてはＩＤ、パスワード、生体認証（指紋等）の多要素の認証情報を、それ以外の情報系においてはＩＤ、パスワードの認証情報を用いている。

ＩＤカードのカードリーダ等からの抜取りなど、ＩＤカード及びパスワード等の取扱いに関する遵守事項を守るよう全庁的に指導を行っている。

業務に必要のない情報へのアクセスを禁止するため、共有フォルダへのアクセス権限は所属単位とするなど、必要なアクセス制御を行っている。

コンピュータウイルス等による情報システムの損傷等を防止するため、不正プログラム対策ソフトウェアをシステムに常駐させており、そのソフトウェアは、最新の状態に保たれている。ソフトウェアによる端末に対するチェックは、定期的に実施されている。

これらのほかに、以下の指摘及び意見に掲げる事象又は状況が生じており、人的セキュリティにおいては、情報セキュリティの管理の仕組みが適切に整備・運用されず、重大な情報セキュリティインシデントが発生している。また、技術的セキュリティなどにおいても重大な情報セキュリティインシデントが発生するリスクが発現する可能性がある。

したがって、次のとおり、指摘し、及び、意見する。

**指　摘**

情報セキュリティに係る遵守事項の徹底について

令和元年度に、情報へのアクセス権限を有する職員が業務以外の目的で個人情報を閲覧したことが判明し、当該職員が懲戒処分を受けるという事件が発生した。事件後速

やかに庁内掲示板等を通じて全職員に対し個人情報の適正な取扱いの徹底について通知しているが、このような事件が起きるのは、職員全体の情報セキュリティに対する認識の甘さや情報セキュリティに関する規範意識の低さに原因があるものと思われる。このような事件の再発防止のためには情報セキュリティポリシーや遵守事項を定めた規程等の十分な理解を促進することが必要であることから、実効性のある方法で全ての職員に対し情報セキュリティ教育を実施し、遵守事項の徹底を図ること。

**意　見**

①　認証情報の多要素化について

情報系のネットワークにおいても、個人情報等の機密性の高い情報を扱っているため、情報システムのログインに際し複数の認証情報を入力する必要がある多要素認証とすることを検討すること。

②　特権ＩＤ等の管理について

管理者権限等の特権を付与されたＩＤ及びパスワードについて、ＩＤを利用する者を必要最小限にし、パスワードの漏えい等が発生しないよう厳重に管理しているが、情報システムの一部にはＩＤ及びパスワードの変更がシステム上できないものがあるとのことである。特権を付与されたＩＤによるなりすましが原因で情報セキュリティ被害が生じた事故事例も企業等で発生しており、ＩＤ及びパスワードの厳重な管理のため、ＩＤ及びパスワードが変更できないことによるマイナスを補完できるような対策を講じること。

③　情報システムの適正な稼働の確保について

令和２年７月には、税システムのプログラムミスを原因とする市・県民税の課税誤りが発生し、５０名を超える納税者に税の還付又は追加徴収の必要を生じさせてしまった。このシステムを所管する所属は、事故の再発防止のため、プログラムを変更した際のチェックとシステムから出力されたデータの正確性の検証・確認に努めることとしている。本市全体の情報セキュリティ管理を統括する当課にあっては、次に掲げる事項に取り組むこと。

ア　この事故は、全国標準のシステムを本市独自のプログラムに変更したことも一つの要因であると考える。標準的なシステムに変更を加えることにより、誤りが発生するリスクや経済性を低下させるリスクがあることを全庁的に周知すること。

イ　システム導入時やプログラム変更時における適正な稼働のチェックとそれができる体制の確保（システム化された業務の内容に精通した職員の育成など）について、全庁的に徹底を図ること。

（６）情報システムの障害・事故時の対応計画について策定しているか。

**リスク発現の可能性（〇予防策あり、△可能性あり、×発現）**

〇　情報セキュリティインシデントが発生した場合又は発生するおそれがある場合において被害の最小化又は未然防止を図ることを目的にその対応について定めた「情報セキュリティ緊急時対応計画」が策定されている。

（７）情報セキュリティ対策の実施に係るＰＤＣＡサイクルが機能しているか。

**リスク発現の可能性（〇予防策あり、△可能性あり、×発現）**

×　情報セキュリティ対策に関する監査は、平成３１年２月に実施されていた。

このほかに、以下の指摘及び意見に掲げる事象又は状況が生じており、人的セキュリティにおいて、情報セキュリティの管理の仕組みが適切に整備・運用されず、重大な情報セキュリティインシデントが発生している。

したがって、次のとおり、指摘し、及び、意見する。

**指　摘**

①　情報セキュリティ対策に関する監査等について

情報セキュリティ対策に関する監査について、令和元年度の実施実績はない。平成３１年２月に実施した監査は、「ＩＴ推進課情報基盤整備グループと業務グループ」を対象に、監査人「ＩＴ推進課課長補佐」により行われたものであった。情報セキュリティ対策に係るＰＤＣＡサイクルを実施し、更に高いレベルの情報セキュリティ対策を行うため、次のア及びイに掲げる事項などに取り組み、効果的な監査・自己点検を行うこと。

ア　情報セキュリティポリシー及び情報セキュリティ監査実施要綱に基づき、監査を毎年度実施するとともに、監査対象からの独立性を確保した監査人による監査とすること。独立性の確保のため、外部から専門的な人材を登用することも一つの方法として検討すること。

イ　自己点検について、例えば、全職員を対象とした、自己チェックリストを用いたアンケート方式による点検を行うなど、その方法を工夫すること。

※　自己点検とは、情報セキュリティ対策の実施状況を自ら点検・評価することをいう。

②　情報セキュリティ委員会の実施について

情報セキュリティポリシーでは、情報セキュリティ委員会はその必要に応じて会議を招集するとされているが、会議がこれまで一度も開催されていない。ＩＣＴは日進月歩の分野であり、何か大きな問題や事故などが起きないと開催しないのではなく、情報セキュリティ対策の全庁的（議会、各委員会、公営企業を含む。以下同じ。）な実施状況を確認し、必要な対策を先取りする場として、また、情報システムの運用に関して職員等が守るべき規程を全ての職員が遵守する仕組みを作る場として、会議を定期的に開催すること。

**意　見**

情報セキュリティ意識の向上について

部局によって情報セキュリティに対する意識に違いがあるように思われる。特に、学校の教諭と議会の議員は、専門家からも指摘があるように、情報セキュリティに対する意識が少し低いのではないかと懸念される。情報セキュリティをより強く意識し、それに対するリスクマネジメントを強化できるよう、教育委員会及び議会における情

報セキュリティ対策の実施状況を確認したうえで、その状況に応じた適切な指導助言を行うこと。

## ２　３Ｅ（経済性、効率性、有効性）、合規性等の視点から行った監査の結果

### 意　見

（１）情報セキュリティポリシーの見直しについて【有効性の視点】

令和２年１２月に総務省策定の「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」が改定されており、改定内容を精査したうえで、情報セキュリティポリシーについて、適時に必要に応じた見直しを行うこと。

（２）情報セキュリティ対策実施に係る組織体制の強化について【有効性の視点】

情報セキュリティ対策をこれまで以上に確実に実施し、更なる効果を挙げるため、情報システム管理を統括する当課だけでなく全庁一体（公営企業も含む。）となってその取組みを推進できる組織とし、体制を強化すること。

（３）当課の体制の維持強化について【有効性の視点】

当課は、市民サービスや地域社会の向上を目指すため、情報通信技術を活用した行政事務の効率化を「戦略」的に推進するという役割を担う部署として平成３１年度から現在の課名となった。このような当課の目的を職員全員で共有し、「ＩＣＴ戦略」課としての風土・文化を構築したうえで、情報セキュリティ管理を統括する所属として、その体制の維持強化に努めること。

（４）テレワーク推進のための情報セキュリティ対策について【有効性の視点】

新型コロナウイルスの感染症対応等による業務継続や職員の多様な働き方の実現に向けた働き方改革の要請からテレワークの推進が重要な課題となっている。テレワークについては、業務継続という情報セキュリティの可用性維持の観点から重要であるが、一方で、大量の、又は機密性の高い個人情報等の取扱いに関する安全性をいかに確保するか等の課題がある。このことから、令和２年１２月に改定された「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」の内容などを踏まえ、それに必要な情報セキュリティ対策を講じ、できる限り早く、そして強力に、テレワークの推進を図ること。

（５）情報セキュリティに関する情報の収集について【有効性の視点】

情報セキュリティ対策は適時に講じる必要があることから、連絡窓口と体制について職員への周知を徹底し、情報セキュリティを脅かす事象や脅かすおそれのある事象（ヒヤリ・ハット）に係る情報については、ＩＣＴ推進員を介することなく、気付いた職員から直接、迅速に収集できるようにすること。

（６）インターネットの適正な利用について【有効性の視点】

インターネットの利用について、公務と関係のないＷＥＢサイトの閲覧の禁止を職員に対して義務付けている。当課が実施しているＷＥＢサイトのフィルタリングを公務上、閲覧が必要であることを理由にオーバーライドした件数の統計情報を所属ごとに取得し、その結果を各所属長に通知することにより、この遵守事項の実効性を上げられないか検討すること。

## 3　まとめ

今回、「情報セキュリティの管理について」をテーマに監査を行ったところ、以上のとおり改善を要する事項が認められた。

本市は、法令等に基づき、市民の個人情報や企業の経営情報など重要な情報を多数保有しており、それを基に市民や企業に対し行政サービスを提供している。行政サービスを提供する手段として、その多くが情報システムやネットワークに依存していることから、市民の生活や地域の社会経済活動を支えるため、情報セキュリティ対策を講じて、保有する情報を守る必要がある。また、行政手続のオンライン化、情報システムの高度化などの電子自治体化を進めるため、他の地方公共団体等のネットワークとも相互に接続しており、情報システムの障害、停止等が発生した場合には、本市のみならず他の広範囲の地域の住民や企業等にも重大な影響を与えることになる。このような事情から情報セキュリティ対策の実効性を高め、その対策レベルを一層強化していくことが求められる。

一方で、行政手続のオンライン化やテレワーク（リモートワーク）の実現による現地対応の充実など情報システムを利用した市民生活の効率性と利便性の向上という新たな要請もある。

今回の行政監査が、情報セキュリティの管理に係る事務処理の適切な改善や見直しを推進し、効率性・利便性の向上と情報セキュリティの確保の両立及び全庁的な情報セキュリティ対策レベルの底上げを実現し、今後のより一層の行政サービスの向上につながることを期待する。