令和２年度　行政監査の結果（指摘・意見・リスク発現の可能性があるもの）に基づく措置状況等の報告

１　監査の種類　　行政監査
２　監査のテーマ　　情報セキュリティの管理について
３　監査対象　　総務部　ＩＣＴ戦略課
４　監査実施期間　　令和　３年　２月１０日

指　摘

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

指　摘	措置（具体的内容）・対応状況
（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。 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。	【　措置済　】　　令和　３年　５月３１日 　令和３年５月３１日に動画配信にて令和３年度管理職向け情報セキュリティ研修を実施し、管理職に対して情報セキュリティ対策に関する役割の意識付けや、知識並びに技術の教育・啓発を行った。今後においても引き続き、動画配信等を活用し、情報セキュリティ対策に関する周知・啓発のための研修等を実施していく。

（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。 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。	【　継続努力　】　　令和　３年　９月３０日 　不用なものは廃棄するなど、サーバ室内の整理整頓を行うとともに、ＣＩＳＯ（最高情報セキュリティ責任者）および統括情報セキュリティ責任者による現地確認を行い、サーバ室における現状の課題について情報共有し、課題解決に向けた協議を行った。 　また、サーバ室内で作業するオペレーターとサーバを分離するなど、重要な情報資産に相応しい方法で管理を行うためのレイアウト変更を検討しており、そのレイアウト変更にかかる予算については、令和４年度予算で要求する予定である。
	【　措置済　】　　令和　４年　３月３１日 　サーバ室のセキュリティを高めるため、サーバとオペレーターを分離するサーバ室のレイアウト変更にかかる予算を令和４年度当初予算で要求し、議決された。今後は、令和４年度に業者選定を行い、サーバ室のレイアウト変更を実施していく。
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。	【　措置済　】　　令和　３年　９月３０日 　サーバのバックアップデータを格納した保管箱の鍵の管理方法を見直し、鍵と保管箱が近接しないよう鍵の保管場所の変更を行った。

（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。 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。	【　措置済　】　　令和　３年　６月２４日 　令和３年６月２４日から動画配信にて令和３年度ＩＣＴ推進員会議を実施し、各所属の代表者を対象に業務に関係のない個人情報を閲覧しないように徹底するなど、情報セキュリティ対策に関する周知・啓発を行った。また、抽出した所属を対象に標的型攻撃メールの訓練を実施しており、今後においても引き続き、ＩＣＴ推進員等を通じて全職員に情報セキュリティの教育を実施していく。
（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。 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。	【　措置済　】　　令和　３年　２月２５日 　監査については、令和３年度の監査計画を策定し、監査対象と被監査対象をそれぞれ別所属とすることで、監査対象からの独立性を確保した監査人による監査を実施予定である。 　また、自己点検については、令和３年２月に全職員を対象とした情報セキュリティ自己点検を実施しており、令和３年度も引き続き実施予定である。

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。	【　措置済　】　　令和　３年　４月２７日 　令和３年４月２７日に第１回情報セキュリティ委員会を実施し、役割分担や課題等の意見交換を行った。 　なお、この情報セキュリティ委員会は半年に１回程度定期的に開催することとしたため、令和３年度下期に、第２回の情報セキュリティ委員会を開催する予定である。

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

特になし

意　見

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結果

意　見	措置（具体的内容）・対応状況
（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。 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、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。	【　措置済　】　　令和　３年　９月３０日 　情報通信技術に関する専門的な知見・技術の習得のために積極的な研修派遣を行っており、令和３年度上期においては１０講座を９人の職員が受講した。下期についても研修派遣を予定しており、引き続き、情報セキュリティに関する知識や技術習得等職員の育成を図ることで組織体制の強化に努める。

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。	【　継続努力　】　　令和　３年　９月３０日 　ＣＳＩＲＴの体制については、他の事例等を参考にしながら、情報セキュリティ委員会の役割を見直し、広報部門、財政部門等を所管する所属を組み入れることを検討していく。 【　継続努力　】　　令和　４年　３月３１日 　ＣＳＩＲＴの体制について、他市町の事例等を参考にしながら、次年度以降の情報セキュリティ委員会において、広報部門、財政部門、法務部門を所管する所属を組み入れるよう役割の見直しについて諮っていく。
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。	【　措置済　】　　令和　３年　９月３０日 　市ホームページに統一的な窓口（ＰｏＣ）に関する担当課の情報などを掲載し、広く周知を図った。
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。	【　措置済　】　　令和　３年　９月３０日 　本市の情報資産について、機密性、完全性及び可用性毎に分類し、管理方法をとりまとめた運用基準として「情報資産の分類と管理方法」を作成し、庁内の掲示板に公開し、職員への周知を図った。
（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。 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。	【　継続努力　】　　令和　３年　９月３０日 　どの職員がどのＩＤカードを所有しているかは、ＩＤカード管理担当者が管理台帳により把握しており、各職員で厳格な管理をするように指導している。ＩＤカードを一元的に管理する場合、ＩＤカード使用時の運用の煩雑さや全てのＩＤカードを盗難されるなどのリスクもあることから、引き続き管理方法については検討していく。 【　措置済　】　　令和　４年　３月３１日 　サーバ室のセキュリティを高めるため、令和４年度にサーバ室のレイアウト変更を行う予定であり、レイアウト変更と併せて生体認証装置の導入も行い、ＩＤカードからの切り替えを実施する。

（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。 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。	【　検討中　】　　令和　３年　９月３０日 　情報系のネットワークにおいて、多要素認証を採用する場合は、約３０００台に指紋認証装置の設置を行うなど、認証管理の負担が増大することが見込まれるため、情報系のネットワーク内で取り扱う情報を厳選するとともに、引き続き認証方法についても検討を行っていく。
	【　継続努力　】　　令和　４年　３月３１日 　令和４年３月に総務省が改定した「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」に基づき、情報系のネットワーク内で取り扱う情報を厳選し、情報系ネットワークでは機密性の高い情報を扱わないよう庁内に周知を図るとともに、認証方法についても多要素化について引き続き検討を行っていく。
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。	【　検討中　】　　令和　３年　９月３０日 　システムの構築や運用の制限により、当初設定したＩＤやパスワードを変更できないものもあることから、当該システムにアクセスするまでのところで、新たなアクセス権限を追加するなどの対策の検討を行っていく。
	【　継続努力　】　　令和　４年　３月３１日 　システムの構築や運用の制限により、当初設定したＩＤやパスワードが変更できないものについては、システムを操作する端末にログインする際に、生体認証を含む多要素認証を必須とするなど、特権ＩＤを変更せずにセキュリティの向上に資する対策について引き続き検討する。
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。	【　検討中　】　　令和　３年　９月３０日 関係各課には、標準的なシステムに変更を加えることで、プログラムミスのリスクが増大することや、カスタマイズ経費が別途かかることを周知するとともに、標準システムに業務をあわせていくように運用の見直しについても全庁的に周知していく。
	【　継続努力　】　　令和　４年　３月３１日 関係各課には、標準的なシステムに変更を加えることで、プログラムミスのリスクが増大することや、カスタマイズ経費が別途かかることを周知した。また、標準システムに業務をあわせる運用見直しについては、人事異動に伴い運用知識が形骸化されないように、システム更新の検討段階や人事異動が発生した時に周知していく。
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。	【　継続努力　】　　令和　３年　９月３０日 職員をシステムのプロフェッショナルレベルに育成することは困難であることから、職員と業者でプログラム変更時等にチェックする範囲や項目を明確にし、品質確保の体制を整備していく。
	【　措置済　】　　令和　４年　３月３１日 品質確保の体制については、業者の品質管理担当者を庁舎内に常駐させ、システム導入やプログラム変更時の納品物チェックを強化した。また、職員の育成については、令和４年度に策定予定の本市のデジタル化推進を担う人材を育成する「デジタル人材育成計画」の中で、ＩＴリテラシー（情報化技術、システム検証技術、業務運用設計技術）の向上を図ることとした。

（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。 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。	【　継続努力　】　　令和　３年　９月３０日 　引き続き、全部局には情報セキュリティ対策に関する情報提供等に努めるとともに、特に教育委員会や議会については、関係所属からの情報セキュリティ対策等の実施状況の把握に努め、情報セキュリティの意識を高める手法を検討していく。 【　措置済　】　　令和　４年　３月３１日 　令和４年度に継続して実施するセキュリティ自己点検において、部局毎の回答状況を基に、情報セキュリティ対策の実施状況を把握し、対策が不十分なところについては、適切な助言を行っていく。

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	措置（具体的内容）・対応状況
（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。	【　継続努力　】　　令和　３年　９月３０日 　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」が改定されたことから、本市情報セキュリティポリシーとの差異を確認し、改定内容の中でも必須の項目については見直しを進めているところである。 【　措置済　】　　令和　４年　３月３１日 　令和４年３月の総務省策定「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」の改定を参考に、本市セキュリティポリシーを改定し、令和４年度に改定版を掲示する予定である。
（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。	【　措置済　】　　令和　３年　６月２４日 　全庁的に情報セキュリティ対策の実施を進めていくため、令和３年度の情報セキュリティ委員会の取組として、５月３１日から管理職向け、６月２４日からＩＣＴ推進員向けに動画配信にて情報セキュリティ研修を実施した。引き続き、このような情報セキュリティ研修の実施や、あらゆる機会を捉えて情報セキュリティ対策への各課の意識の向上を図っていく。

（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。	【　継続努力　】　　令和　３年　９月３０日 市総合計画に掲げた「スマート自治体の実現」の主旨に基づき、具体的にいつまでに何をするかを明記した「四日市市情報化実行計画」を令和３年度に策定予定であり、その中に「情報セキュリティ対策」についてもどのように取り組んでいくかを記載する予定である。 【　継続努力　】　　令和　４年　３月３１日 令和４年３月に策定した「四日市市情報化実行計画」に基づき、全職員向けに情報セキュリティに関する動画研修を実施するとともに、ＩＣＴ戦略課職員向けには実践的サイバー防御演習「ＣＹＤＥＲ」等の、より高度な外部研修を取り入れることにより、職員の情報セキュリティに対するさらなる意識・スキル向上を図る。
（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。	【　措置済　】　　令和　３年　９月３０日 令和２年度から、一部の所属を対象に地方公共団体情報システム機構が実施している自治体テレワーク推進実証実験事業の「自治体テレワークシステムｆｏｒＬＧＷＡＮ」を使用した実証実験を行っている。令和３年度については、同システムのライセンスを拡大し、新型コロナウイルス感染症拡大防止の観点から、出勤せずに在宅勤務ができるよう人事課にて「四日市市職員の新型コロナウイルス感染拡大防止にともなう在宅勤務に関する要綱」を制定し、同要綱第１２条の情報セキュリティ対策等において、公文書の取り扱い等について明示している。引き続き、人事課と連携しながらテレワークの実施環境づくりに取り組んでいく。
（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。	【　措置済　】　　令和　３年　９月３０日 令和３年６月２４日からＩＣＴ推進員向けに動画配信にて情報セキュリティ研修を実施し、情報セキュリティを脅かす事象の紹介などを行っており、引き続き職員自ら脅威情報をＩＣＴ戦略課に報告するように掲示板で促していく。

（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。	【　検討中　】　　令和　３年　９月３０日 　現在導入しているフィルタリング製品において取得および作成できる閲覧履歴の統計情報を基に、各所属長に通知する内容の検討や仕組みの構築を進めているところである。 【　継続努力　】　　令和　４年　３月３１日 　各所属長に通知する内容について、フィルタリング製品において取得できる統計情報の分析を進めていく。

リスク発現の可能性があるもの

特になし