平成 27 年度　行政監査（監査対象：全ての局室区）

監査結果の概要	措置内容	措置状況
○　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 事務処理用 PC で作成したデータの保存及び所属での情報共有を図るため，情報系ネットワーク上に外部記憶装置 NAS(Network Attached Storage)を設置し，各種の名簿や刊行物の送付先などの個人情報を含むファイルが保存されている事例が散見された。また，事務処理用 PC を職員が共用で使用している所属では，作成したデータを USB で個人ごとに保存管理するために，共用の事務処理用 PC のデバイス制御を解除した上で，各担当者に USB を配付している事例があった。 情報化推進部においては, NAS にデータを保存する場合の職員のアクセス制限やファイルへのパスワード設定を呼びかけているものの，情報セキュリティポリシー上では, NAS 等による個人情報の保存方法について規定されていない。 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。 （企画調整局情報化推進部）	平成 28 年 3 月に, 情報セキュリティポリシーを改正し, 個人情報など，機密性３のデータは，権限のある者だけがアクセスできる環境で保存・利用をしなければならず，NAS 等を利用して，複数の権限ある者でデータを共有したり，所属外にデータを送付・送信したりするときは，パスワード等による情報漏えい対策を施さなければならない旨を明記し，改正趣旨を通知して徹底した。 （企画調整局情報化推進部）	措置済
（イ）生活保護業務における査察指導台帳の作成保存 各区の生活保護業務では，担当係長が，被保護世帯に対するケースワークの査察指導の進行管理を行うため，生活保護システムから被保護世帯に関する必要な情報を事務処理用 PC に取り込み，データを編集加工して「査察指導台帳」を作成保存しているが,「査察指導台帳」ファイルにパスワード設定が行われていない事例があった。また，	指摘事項のうち，ファイルにパスワードが設定されていない事例については，操作職員において，セキュリティ対策への意識低下が招いたために起こったことと考える。 パスワード設定の徹底と共に情報セキュリティの遵守について，継続的に周知徹底を図るべく，各所属内	措置方針

平成 27 年度　行政監査（監査対象：全ての局室区）

監査結果の概要	措置内容	措置状況
「査察指導台帳」の事務処理用 PC による作成保管は，審議会に諮問されていなかった。 「査察指導台帳」のデータには個人情報保護条例第 7 条第 3 項に規定するセンシティブ情報が含まれる場合があることから，適正な情報セキュリティ対策を講じるべきである。 （保健福祉局総務部保護課）	において相互確認していくよう，3 月 24 日の各区保護係長会会議において改めて周知徹底を行った。 査察指導台帳の情報セキュリティ対策については，基幹系ネットワーク内の生活保護システム端末機での運用を徹底すると共に，端末機の増設を含めた対応の検討を行っていく。 （保健福祉局総務部保護課）	
（ウ）同和奨学金・地域改善対策奨学金システムの個人情報の情報系ネットワーク上での保存 同和奨学金システム（ホストシステム）及び地域改善対策奨学金システム（スタンドアロンシステム）では，国庫返還事務や滞納整理事務を行うため，同システムから抽出した個人情報データを事務処理用 PC で編集加工して状況別の奨学生一覧等を作成し，NAS に保存して課内の関係職員で奨学生や返還金の情報を共有化していた。 同和奨学金に関する情報はセンシティブ情報にあたることから，適正な情報セキュリティ対策を講じるべきである。 （教育委員会事務局指導部人権教育課）	同和奨学金システムの端末については，端末の所管課に返還届を提出し，システムの廃止手続きをしている。 また，ＮＡＳに保存されていた奨学生一覧等の個人情報データについては，すでに地域改善対策奨学金専用システム端末に移し変え，課内で個人データを共有するという扱いは取り止めている。 なお，今後，個人情報データの処理等を行う場合は，地域改善対策奨学金システム内で行うこととする。 （教育委員会事務局指導部人権教育課）	措置済

平成 27 年度　行政監査（監査対象：全ての局室区）

監査結果の概要	措置内容	措置状況
（２）物理的セキュリティ ①サーバの管理 　福祉情報システム及び生活保護システムの区役所に設置するセグメントサーバ，精神障害者保健福祉手帳システム及びこども家庭センター(児童虐待対応ナビ)システムのサーバの管理について，施錠可能な区画を設置せずに執務室内にサーバを設置し，また，ラック等に収納して容易に取り外せないよう固定が行われていない事例があった。 　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。 （保健福祉局総務部計画調整課，保護課，障害福祉部こころの健康センター，こども家庭局こども家庭センター）	福祉情報システム及び生活保護システムの，区役所等に設置しているセグメントサーバについては，すべてセキュリティチェーンでラック等へ繋ぎ，容易に持ち出しができないように対策を講じた。 ◇福祉情報システム 平成 28 年 3 月 28～30 日実施 15 拠点すべて完了 ◇生活保護システム 平成 28 年 3 月 16～24 日実施 11 拠点すべて完了 （保健福祉局総務部計画調整課，保護課）	措置済
	精神障害者保健福祉手帳システムのサーバをラックに収納し，チェーンキーにてラックに固定し，容易に取り外せないようにした。 　施錠可能な区画への設置については，今年度末事務所の移転を予定しており，移転後の事務所レイアウトの検討の中で適正な設置場所となるようにしていく。 （保健福祉局障害福祉部こころの健康センター）	措置済
	こども家庭センター(児童虐待対応ナビ)システムのサーバについては，３月３０日に施錠可能な事務什器を購入し，収納した。 （こども家庭局こども家庭センター）	措置済

平成 27 年度　行政監査（監査対象：全ての局室区）

監査結果の概要	措置内容	措置状況
○　意　見　事　項 （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。今回の監査もこの台帳情報をもとに実施したが，台帳記載内容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。 （企画調整局情報化推進部）		
（ア）台帳の定期的な更新 　情報システム台帳については，情報化推進部が本市の情報システムを把握するため任意で作成したものである。情報資産の管理の観点から，この台帳の作成を情報セキュリティポリシー等で義務化し，定期的に情報を更新する仕組みを検討されたい。	平成 28 年 3 月に，情報セキュリティポリシーを改正し，情報システム台帳の作成義務にかかる規定を新設した。今後も，台帳の登載情報が最新の状態に維持されるよう，必要な照会事務等を進めていく。	措置済
（イ）登録すべき情報システムの明確化 　登録されているシステムの中には，インターネットと接続していない PC や他の事業所でも同様に使用されているのではないかと推測されるシステム，国等の他機関が管理運営するシステムのネットワーク機器等があった。 　本市の管理するシステムの全容を正確に把握するため，この台帳に登録すべきシステムの定義の明確化を検討されたい。	情報システムの定義については，情報セキュリティポリシーに，「コンピュータ及びネットワークで構成され，情報処理を行うものを指す」と定義されている。 　一方，情報システム台帳は，本市における ICT 環境全体について，システムの概要を把握するという観点から，単独のパソコンのみの場合はもちろん，国等の他機関が運営するシステムやネットワーク機器であっても，状況の把握が必要なことに変わりはないことから，台帳への登載対象に含めている。 　しかしながら，情報システム台帳の登載内容について，より分かりやすくなるよう，平成 28 年 2 月に実施	措置済

平成 27 年度　行政監査（監査対象：全ての局室区）

監査結果の概要	措置内容	措置状況
	している調査から，調査方法を改めた。 　具体的には，調査票において，「情報システム」と「専用パソコン」を区別したり，神戸市のシステムと，国等の他機関が管理運営するシステムを区別したりする欄を設けており，これにより，台帳上，いわゆる「神戸市の情報システム」の全容を正確に把握することが可能になっている。 （企画調整局情報化推進部）	
②情報資産の保管方法 （ア）機密性３のデータの保存方法 　対策基準では，機密性３のデータ（個人情報など）について，電子メールによる送信を行う場合及び外部に提供する場合には，パスワード等による情報漏えい対策を行わなければならないとされているが（対策基準 4.2.3 エ(3)及びカ(1)），データの保存については，「情報資産管理責任者は，情報資産の重要性分類に従って，情報資産の保管を適切に行わなければならない。」（対策基準 4.2.3 オ(1)）と規定するのみで，具体的な保存方法は規定されていない。 　抽出した事務処理用 PC の個人情報を含むファイルについて，そのデータの保存方法を確認したところ，多くの所属では全てのファイルにパスワード設定又は暗号化のいずれかが行われていたものの，全てのファイルに両方とも行われていなかった事例や一部のファイルに両方とも行われていなかった事例があった。 　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。 （企画調整局情報化推進部）	平成 28 年 3 月に，対策基準を改正し，機密性３のデータは，権限のある者だけがアクセスできる環境で保存・利用をしなければならず，複数の権限ある者でデータを共有したり，所属外にデータを送付・送信したりするときは，パスワード等による情報漏えい対策を施さなければならない旨を明記し，改正趣旨を通知して徹底した。 （企画調整局情報化推進部）	措置済

平成 27 年度　行政監査（監査対象：全ての局室区）

監査結果の概要	措置内容	措置状況
（イ）家庭内暴力（DV）・ストーカー等の被害者の証明書発行制限に関する情報共有 各区市民課では，DV・ストーカー行為等の被害者について，証明書の発行を制限する支援を行っており，住民記録システムでも，発行制限等の処理ができるようになっている。しかし実務上の必要から，各区市民課で，担当係長又は担当者が情報系ネットワーク上の事務処理用 PC を使用して独自に DV・ストーカー行為等の被害者の氏名，生年月日，住所，証明書の発行制限に関する情報等を記録した対象者リストを作成するとともに NAS を利用して係長と担当者が情報を共有している事例があった。 これらの情報は機密性の高い情報であるが，事務処理の効率化の観点から，セキュリティに十分注意した上で，事務処理用 PC を利用した情報共有のあり方について検討されたい。 （市民参画推進局参画推進部区政振興課）	各区市民課には，個人情報保護審議会で認められた範囲で事務処理用 PC を用いた情報処理を行い，NAS を利用した個人情報の情報共有をしないよう周知徹底した。 事務処理用 PC を利用した情報共有のあり方については，現在，企画調整局情報化推進部が導入を検討している全庁共用ファイルサーバを活用した情報共有を考えていきたい。 （市民参画推進局参画推進部区政振興課）	措置済
（2）物理的セキュリティ ①コンピュータの設置場所 ホストコンピュータ及び住民記録，福祉情報等の基幹業務系システムのサーバは，セキュリティカードにより一般職員が入退室不能なマシンルームに設置されているが，市税のサブシステム等のサーバが民間ビルの事務室スペースを改修して設置されていた。 いずれのシステムもセキュリティポリシー上問題はないものの，セキュリティレベルの向上の観点から，ホストコンピュータのクライアント・サーバ・システムへの移行後に，ホストコンピュータの設置場所，ホストデータ入力室等を活用して，サーバの集約化を検討されたい。 （企画調整局情報化推進部）	サーバ等の機器は，市の重要な情報資産として，高いセキュリティレベルと業務継続性を備えた形で管理されるべきと考えており，外部データセンターを活用し，情報化推進部が集約して管理していく予定で，平成 28 年度中の活用開始を目指して，既に調達に向けた作業を開始した。 （企画調整局情報化推進部）	措置済

平成 27 年度　行政監査（監査対象：全ての局室区）

監査結果の概要	措置内容	措置状況
②スタンドアロンシステムのあり方 システム台帳では，個人情報を取り扱っているスタンドアロンシステム（PC 単体で稼働しているシステム）が 54 システムあった。 いずれもアクセス制限のための ID とパスワードの設定は行われていたものの，その多くが，ネットワークに接続していないことを理由にウイルス対策ソフトの常駐がないか，ウイルス対策ソフトを導入していても定義ファイルを更新していなかった。また，審議会の諮問を経ずにシステムを構築したり，施錠可能な管理区域に PC を設置していないシステムも多数あった。さらに，情報の共有化及び業務の効率化を図るため，スタンドアロンのシステムの情報を情報系ネットワーク上で課内共有し，データを編集加工している事例もあった。 インターネット接続がなく，USB 等による外部接続が完全に行われず，当該 PC 内だけで情報の閲覧・処理が行われるのであれば，ウイルス対策ソフトの常駐までは必要ないといえなくはないが，当該 PC に個人情報が保存されている以上，端末本体の盗難等による情報流出に備え，不利用時に施錠できる書庫等へ保管することや業務担当者以外のアクセス制御の徹底などのセキュリティ対策の確実な実施が必要である。 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。 （企画調整局情報化推進部）	スタンドアロンシステムについては，インターネット接続をしないなど，外部とのデータのやりとりがほとんどないか，全くないといった事情が個別にあることが考えられるが，そのような状況でも，セキュリティリスクが相対的に低いだけで，リスクがゼロではない以上，セキュリティ対策が全く不要になることはない。 端末のセキュリティ対策に必要な措置としては，ウイルス対策や認証の管理，操作ログの保存等が考えられる。情報系ネットワークで使用する，いわゆる事務処理用 PC においては，情報化推進部が一括して，これらのセキュリティ対策を施した状態で端末を提供できる。したがって，基幹系の業務や，センシティブ情報を扱う業務など，特別な事情がある場合を除けば，新たにシステムを構築するときは，情報系ネットワーク内で，事務処理用パソコンを使用する形でシステムを構築する方が，セキュリティリスクがより小さいと考えており，所管課から相談があったときも，従来から，事務処理用パソコンの活用を検討するよう，対応してきた。 現場において，左記のような状況があることについては，スタンドアロンのシステムといえども，セキュリティ上問題があると考えており，システムの規模や扱う情報の内容などに応じて，必要なセキュリティ対	措置方針

平成 27 年度　行政監査（監査対象：全ての局室区）

監査結果の概要	措置内容	措置状況
	策を個別に実施するか，事務処理用パソコンを利用する方法に変えるか，適切な対応を早急に求めていく。 （企画調整局情報化推進部）	
（３）技術的セキュリティ ①不正アクセス対策の強化 第三者からのサービス不能攻撃や標的型攻撃の発生事例が，国及び他地方自治体，企業で多数報告されている。本市においても同様の攻撃を受けることが懸念されるが，第三者からのサービス不能攻撃を受けた場合でも情報システムの可用性を維持し，標的型攻撃による外部からの本市システムへの侵入を防ぐ必要がある。 不正アクセス対策について，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」（平成 27 年 3 月一部改訂）では，サービス不能攻撃及び標的型攻撃の項目が追加され，その対策が明記されている。 不正アクセス対策をより明確にするため，本市でも，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。 （企画調整局情報化推進部）	平成 28 年 3 月に，情報セキュリティポリシーを改正し，サービス不能攻撃と標的型攻撃への対応を明記した。 （参考：情報セキュリティ対策基準） 7.5.6 サービス不能攻撃 情報基盤管理者及び業務システム管理者は，外部からアクセスできる情報システムに対して，第三者からサービス不能攻撃を受け，利用者がサービスを利用できなくなることを防止するため，情報システムの可用性を確保する対策に努めなければならない。 7.5.7 標的型攻撃 情報基盤管理者及び業務システム管理者は，情報システムにおいて，標的型攻撃による内部への侵入を防止するために，研修・啓発や自動再生無効化等の人的対策・入口対策を講じたり，内部に侵入した攻撃を早期検知して対処するために，通信をチェックするなどの内部対策を講じたりするなど，必要な対策に努めなければならない。 （企画調整局情報化推進部）	措置済

平成 27 年度　行政監査（監査対象：全ての局室区）

監査結果の概要	措置内容	措置状況
（４）運　用 ①情報システムの監視 （ア）ログ解析 　ログは，OS，アプリケーション，通信機器などが，稼働状態，処理の実行状況，障害・異常の発生状況などについて出力した記録であり，ログの解析結果に基づいて問題箇所を修正することで発生中のトラブルを解決したり，未然に防止したりすることができる。また外部からの不正アクセスや内部の不正利用を検知することができるため，ネットワークを構成する各システム管理者は，ファイアウォールなどネットワーク機器や端末のログの収集を行っている。 　しかし，収集したログの解析については，各システム管理者によって，その頻度，対象機器等が大きく異なっていた。 　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，システムの重要性に鑑み，特に基幹業務系システムについては，ログ解析の実施水準を標準化することを検討されたい。 （企画調整局情報化推進部）	基幹系ネットワークのファイアウォールは，既に月に１回ログ解析を行っている。さらに，更新を検討している次期ネットワークでは，共用ファイアウォールを設置する方向で検討しており，順次，共用ファイアウォールに集約していくことで，全庁的なセキュリティレベルの維持・向上を図っていく。 　情報系ネットワークにおいては，ネットワークログ分析を，平成 28 年 3 月から開始している。 （企画調整局情報化推進部）	措置済
②情報セキュリティインシデントへの対応 （ア）ＣＳＩＲＴの設置 　近年，相次ぐサイバー攻撃による重大な情報セキュリティインシデントの発生や，それに伴うサイバーセキュリティへの関心の高まりを背景として，CSIRT（シーサート：Computer Security Incident Response Team）を設置する企業や組織が増加している。 　CSIRT は，初動対応，原因究明，対応策等のインシデント発生時の対応を主導し，現場組織等に適時対応を指示するとともに，日常的な活動としてインシデントの検知，個別の対応手順の策定などインシデント発生に備えた各種対応を行う。 　本市の対策基準等では，情報資産に対する情報	以前から，情報セキュリティポリシーにおいて，情報セキュリティ管理体制を定めており，副市長がその任につく CISO（情報セキュリティ最高責任者）をトップとして，企画調整局長を情報セキュリティ統括責任者，情報化推進部長を情報セキュリティ責任者，ICT 計画推進担当課長を情報セキュリティ管理者とするなどの体制を置き，情報セキュリティに関する権限と責任を整理していた。	措置済

監査結果の概要	措置内容	措置状況
セキュリティ侵害が発生した場合又は侵害のおそれがある場合に備え，情報セキュリティ総括責任者（企画調整局長）は，緊急時の円滑な情報提供を図るため関係者の連絡体制を整備し，情報基盤管理者及び業務システム管理者は，緊急時対応計画（緊急時の対応手順，緊急連絡網）を策定する，とされている。しかし，複数の業務システム又は全庁的に影響を及ぼすインシデントに対する対応手順は明らかでない。また主要な業務システム以外では，必ずしも情報通信技術に詳しい職員が運用しているわけでないため緊急時対応計画を策定することが困難なシステムもある。 一方で，ホストコンピュータからクライアント・サーバ・システムへの移行により業務所管課がそれぞれ情報システムを管理・運用するようになること，マイナンバー法の施行と個人番号の利用拡大といった情勢を踏まえれば，個別システムのインシデントを全体の被害に拡大させないためにも，緊急時により実践的な初動対応が要求されるようになっている。 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（連絡，証拠保全，被害拡大の防止，復旧，再発防止等の措置）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。 （企画調整局情報化推進部）	さらに，日本年金機構の情報流出事案を受け，総務大臣によるセキュリティ対策の徹底強化を求める通知が出されるなど，CSIRT の設置が全自治体に求められている状況を受け，平成 28 年 3 月に，情報セキュリティポリシーを改正し，セキュリティ対策に第一義的に責任をもつ組織・窓口として，CSIRT の設置を明示する規定新設した。 （参考：情報セキュリティ対策基準抜粋） 3.3.1 CSIRT の設置 情報セキュリティ最高責任者は，情報セキュリティに関する事件・事故,システム上の欠陥及び誤動作(以下，「情報セキュリティに関する事件・事故等」という。）に対処する組織として CSIRT を設置し，企画調整局情報化推進部が,その役割を担う。 3.3.2 CSIRT の役割 CSIRT は，情報セキュリティに関する事件・事故等に対処し，被害拡大防止，復旧，再発防止等に向けた対応を，迅速かつ的確に実施する。 3.3.3 CSIRT の連絡体制 CSIRT の統一窓口は，情報セキュリティ管理者とする。情報セキュリティ管理者は，情報セキュリティに関する事件・事故等が発生したときは，その内容に応じて，基幹系ネットワーク管理者，情報系ネットワーク管理者，業務システム管理者等と適宜連絡し，国や県等の関係機関との情報共有を行う。 （企画調整局情報化推進部）	