監査公表第721号

地方自治法第199条第２項の規定による監査を実施し，同条第９項に規定する監査の結果に関する報告及び同条第10項に規定する意見を決定しましたので，次のとおり公表します。

平成28年５月12日

京都市監査委員　中　村　三之助
同　　鈴　木　正　穂
同　　西　村　京　三
同　　光　田　周　史

平成 27 年度

行政監査結果報告

平成 28 年 5 月

京 都 市 監 査 委 員

目　　次

表記に関する注意事項

注　　文中及び表中に用いる比率は，小数点以下第２位を四捨五入した。そのため，構成比については，総計と内訳の計とが一致しない場合がある。

第１　監査の概要

１　監査のテーマ及び選定理由

⑴　テーマ

個人情報の取扱いについて

⑵　選定理由

行政サービスの多様化に伴い，地方公共団体が市民等の個人情報を取り扱う機会も多種多様に及んでいる。

また，近年，行政の場においても，情報通信技術（ＩＣＴ）の利活用の機会は飛躍的に増大しており，個人情報の漏えいに係る新たなリスクが増加している。

技術的な対策も必要とされる一方で，個人情報の漏えいの多くは人的な要因によって生じており，職員が正しくリスクを認識し，適切な取扱いを行うことが一層重要となっている。

そこで，各所属における個人情報の漏えいに係るリスク対策の実施状況を検証するため，テーマとして選定した。

２　監査の目的及び着眼点

⑴　目的

職員の個人情報保護及び情報セキュリティの確保に係る適切な認識に基づく情報活用能力（情報リテラシー），特に情報管理能力の向上に資することを目的とする。

⑵　着眼点

都市監査基準準則第 22 条の別項第４　行政監査の着眼点を参考に，主として次に掲げる着眼点について監査を実施した。

ア　個人情報取扱事務の届出が適正に行われ，個人情報の取扱いの制限が職員に周知されているか。

イ　個人情報の適正な管理のために必要な措置が講じられているか。

ウ　研修や自己点検の機会が有効に利用されているか。

３　監査の対象

⑴　監査対象局等

環境政策局，行財政局，総合企画局，文化市民局，産業観光局，保健福祉局，都市計画局，建設局，会計室並びに各区役所及び区役所支所

⑵　監査対象の個人情報

平成27年４月１日時点で上記⑴の監査対象局等が取り扱う個人情報。ただし，京都市個人情報保護条例（以下「個人情報保護条例」という。）第40条第１項及び同条第３項に掲げる個人情報を除く。

⑶　監査の対象年度

平成26年度及び平成27年度（必要に応じて他の期間も対象とした。）

⑷　監査の実施期間

平成27年７月から平成28年４月まで

４　監査の実施方法

監査は，次の⑴及び⑵の方法により実施した。

⑴　全庁調査

上記の監査対象局の課等（360 課等）の課長等に対し，調査票により，所属における個人情報の取扱いに係るリスク認識及び周知等の状況に関する調査を行い，必要なものについて文書及び口頭による質問調査を実施した。

⑵　実地調査

ア　上記⑴の全庁調査の結果及び各所属における個人情報を取り扱う情報システムの運用管理状況に係る予備調査の結果等を参考に，①所属内で個人情報を取り扱う情報システムを運用管理している事業所及び②情報システムの端末が設置されている課等から，次の表に掲げる課等を対象として，実地調査を行い，関係帳簿，証書類等の審査並びに文書及び口頭による質問調査を実施した。

行財政局	市税事務所	納税室納税推進担当 東山税務センター 下京税務センター
保健福祉局	長寿社会部 保健衛生推進室	長寿福祉課（注） 桃陽病院
東山区役所	福祉部	支援保護課
下京区役所	福祉部	支援課 保護課

注　京都市下京東部地域包括支援センターに設置された情報システムを対象とした。

イ　総合企画局情報化推進室（以下「情報化推進室」という。）に対し，個人情報保護及び情報セキュリティに関する取組の状況等を確認した。

第２　個人情報の取扱いの概要

１　本市における規程及び体制等

⑴　規程等

ア　個人情報保護

(ｱ)　制度の沿革等

地方公共団体及び本市における個人情報保護制度に係る主な沿革は，次のとおりである。

本市における個人情報保護条例に係る事務は，情報化推進室情報管理担当が統轄している。平成27年度の担当は，情報管理課長，個人情報保護係長（情報管理課長事務取扱）及び補佐職員２名である。

年月	主な沿革等
昭和62年12月	京都市電子計算機処理に係る個人情報の保護に関する条例の制定
平成６年４月	個人情報保護条例の施行
平成17年４月	個人情報の保護に関する法律（以下「個人情報保護法」という。）の施行 ・　地方公共団体は，この法律の趣旨にのっとり，その地方公共団体の区域の特性に応じて，個人情報の適正な取扱いを確保するために必要な施策（具体的には，個人情報保護条例）を策定し，実施する責務を有するとされている（第５条）。 個人情報保護条例の全面改正
平成25年５月	行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「番号法」という。）の成立
平成27年９月	個人情報保護法の一部改正
平成27年10月	番号法の施行 個人情報保護条例の一部改正

総務省「地方自治情報管理概要」（平成26年４月１日現在）によれば，個人情報保護対策等に係る条例の制定率は，市区町村においては平成18年度以降，100％となっている。

(ｲ)　個人情報の定義等

個人情報保護条例における個人情報の定義及び適用の範囲は，次のとおりである。

ａ　個人情報とは，個人に関する情報で，個人が識別され，又は識別され得るものをいう。ただし，法人等の役員に関する情報を除く（同条例第２条第１号）。

b　統計法に係る個人情報については，個人情報保護条例の規定は適用しない（同条例第 40 条第１項）。

c　本市の職員並びに本市が設立した地方独立行政法人の役員及び職員の人事，給与，服務，福利厚生等に関する個人情報については，京都市情報公開・個人情報保護審議会（以下「個人情報保護審議会」という。）への報告，市長への個人情報取扱事務の届出，個人情報保護審議会の意見聴取等の規定は適用しない（同条例第 40 条第３項）。

イ　情報セキュリティ

(ｱ)　制度の沿革等

地方公共団体及び本市における情報セキュリティ対策に係る主な沿革は，次のとおりである。

本市の市長部局（監査対象局等）における情報セキュリティ対策に係る規程等は，情報化推進室情報政策担当が所管している。情報セキュリティ対策は，平成 27 年度は，情報政策課長，ＩＴガバナンス推進係長及び補佐職員２名の担当事務の一つに位置付けられている。

年月	主な沿革等
平成 13 年３月	総務省「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」の策定 ・　地方公共団体における情報セキュリティポリシーの策定を推進するため，策定や見直しを行う際の参考として，考え方及び内容について解説したもの。 ・　情報セキュリティ対策は，個人情報保護対策と内容的に重なる部分も多く，担当部署が相互に連携をとってそれぞれの対策に取り組むことが求められるとされている。
平成 14 年１月	京都市情報セキュリティポリシー（情報セキュリティ基本方針及び情報セキュリティ対策基準）の策定
平成 19 年 10 月	京都市情報セキュリティ対策基準（以下「情報セキュリティ対策基準」という。）の策定
平成 22 年４月	京都市高度情報化推進のための情報システムの適正な利用等に関する規程（以下「情報システムの適正な利用等に関する規程」という。）の策定 ・　情報システムの適正な利用及び情報セキュリティの確保に関し必要な事項を定めたもの。
平成 25 年５月	番号法の成立

平成26年11月	サイバーセキュリティ基本法の成立 ・　地方公共団体は，サイバーセキュリティ[1]に関する自主的な施策（具体的には，情報セキュリティポリシー）を策定し，実施する責務を有するとされている（第５条）。
平成27年３月	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一部改定 ・　新たな対策技術の動向や，新たに成立した法令等を踏まえたもの。

総務省「地方自治情報管理概要」（平成26年４月１日現在）によれば，情報セキュリティポリシーについては，市区町村では1,704団体（97.8%）とほとんどの団体で策定されており，主要な情報資産についてのセキュリティ対策実施手順は，本市を含む893団体（51.3%）で策定されている。

なお，情報セキュリティ対策基準については，総務省「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」の改定等に伴い，改定検討作業に着手しているところである。

(ｲ)　個人情報の取扱い等

ａ　個人情報の取扱い

電子情報及び入出力帳票は重要性Ⅰ及びⅡに分類するものとされており（情報セキュリティ対策基準　１　電子情報等の保護に関する管理基準第４条），プライバシーに関する情報（個人に関して，通常他人に知られたくないと認められる情報）は，重要性Ⅰに分類されている。

ｂ　情報セキュリティの定義

情報セキュリティとは，情報資産[2]が次のいずれにも該当する状態をいうものとされている(情報システムの適正な利用等に関する規程第２条第５号)。

(a)　機密が保持されている状態

(b)　破壊，改ざん，不正な消去その他の事故のない状態

(c)　必要があるときに利用することができる状態

(2)　体制

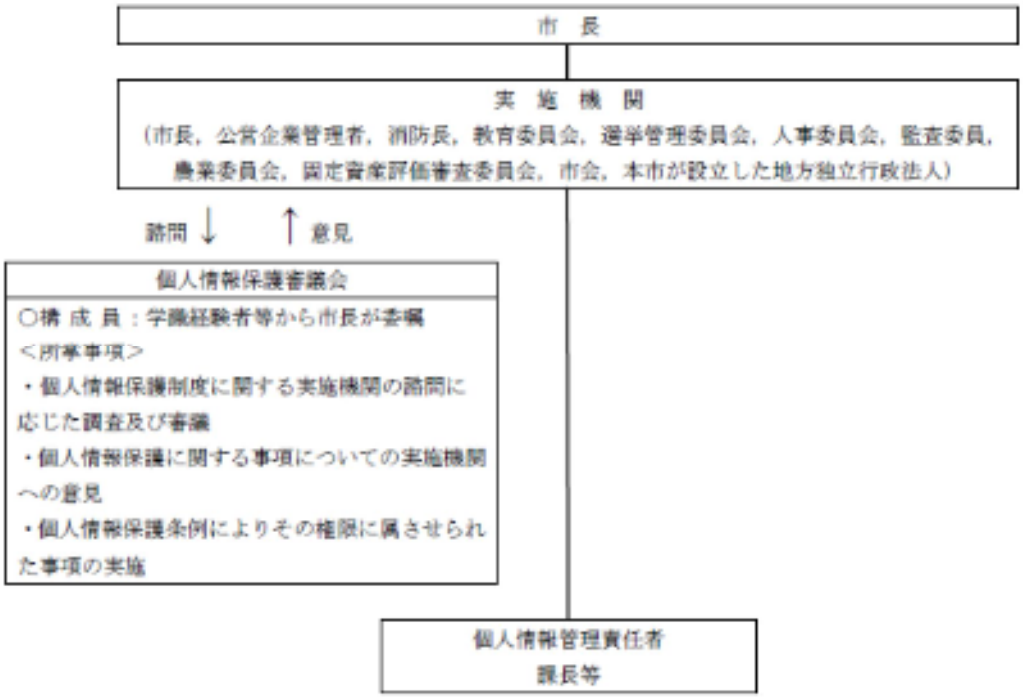
次のとおり，課長等が所属職員の指揮監督や指導等を行うものとされている。

---

[1] 電磁的方式により記録，発信，伝送，受信される情報の漏えい等の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ，その状態が適切に維持管理されていること。

[2] ①情報システム，②電子情報，③入出力帳票並びに④情報システムに係る設計書，仕様書その他情報システムの企画，調達，開発，運用，管理及び評価を行うために必要な書類をいう（情報システムの適正な利用等に関する規程第２条）。

ア　個人情報保護



(ｱ)　実施機関（市長）

個人情報保護条例上の個人情報保護制度を実施する機関は，市長部局（監査対象局等）にあっては市長とされている（個人情報保護条例第２条第３号）。

実施機関は，個人情報の保護に関し必要な措置（条例の遵守，職員の意識啓発，事務処理上の改善や整備等）を講じなければならない（個人情報保護条例第３条第１項，個人情報保護事務の手引　３　京都市個人情報保護条例の趣旨及び運用（以下「個人情報保護条例の趣旨及び運用」という。））。

また，実施機関は，個人情報を適正に管理させるため，個人情報管理責任者を置かなければならない（個人情報保護条例第 12 条第２項）。

(ｲ)　個人情報管理責任者（課長等）

所属における個人情報の適正な管理について責任を負うとともに，個人情報の保護に関し，所属職員を指揮監督する（京都市個人情報の保護に関する事務取扱要綱（以下「個人情報保護事務取扱要綱」という。）第３　２）。

個人情報管理責任者は，実施機関が市長にあっては京都市公文書取扱規程（以下「公文書取扱規程」という。）に定める文書管理責任者（文書管理所属（課等）の長）をもって充てる（個人情報保護事務取扱要綱第３　１）。

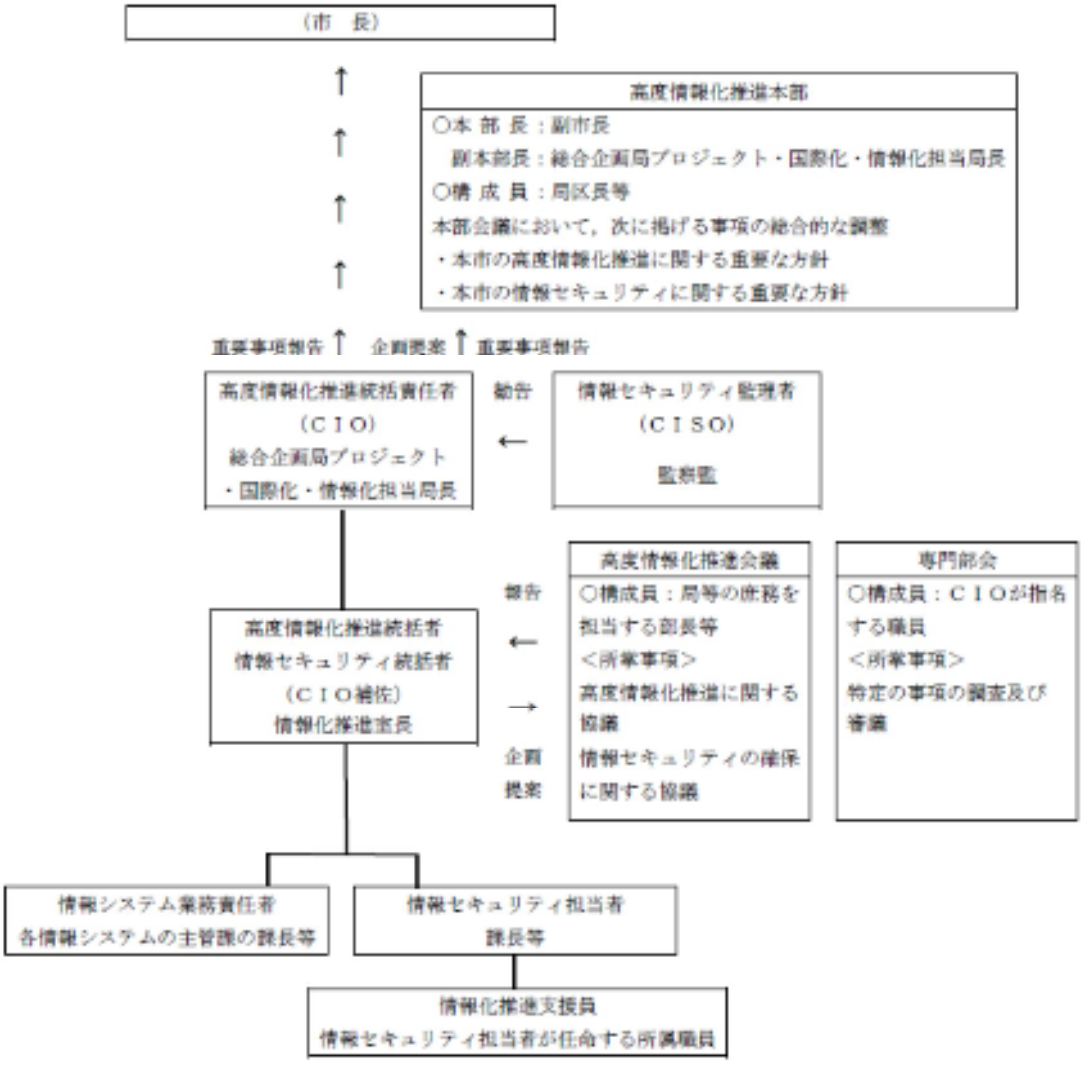
(ｳ)　個人情報保護審議会

京都市情報公開・個人情報保護審議会条例により設置されており，①個人情報保護制度に関する実施機関の諮問に応じた調査及び審議，②個人情報保護に関する事項についての実施機関への意見並びに③個人情報保護条例によりその権限に属させられた事項を行う（同条例第１条）。

委員は，学識経験者等から市長が委嘱する（同条例第２条第２項）。

イ　情報セキュリティ

情報セキュリティの確保を含む高度情報化推進のための体制は，情報システムの適正な利用等に関する規程において定められている。



主なものは次のとおりである。

(ｱ)　高度情報化推進統括責任者（総合企画局プロジェクト・国際化・情報化担当局長）

本市の事務の高度情報化推進に係る事務の責任者として，当該事務を統括す

る（同規程第５条第３項）。

(ｲ)　情報セキュリティ統括者（情報化推進室長）

高度情報化推進統括責任者（以下「統括責任者」という。）の命を受け，情報セキュリティ対策に関する事務を掌理する（同規程第７条第４項）。

(ｳ)　情報システム業務責任者（情報システムの主管課の課長等）

情報システムの構築及び運用に係る業務を主管する課等（以下「情報システムの主管課」という。）において，主管する情報システムの安定的な運用及び管理に努め，情報セキュリティを確保するために必要な措置を採る（同規程第８条第３項）。

(ｴ)　情報セキュリティ担当者（課長等[1]）

情報セキュリティを確保するために必要な措置を講じるとともに，所属職員を指導する（同規程第９条第３項）。

(ｵ)　情報化推進支援員（情報セキュリティ担当者が任命する所属職員）

課等における情報セキュリティ対策に関する事務について，情報セキュリティ担当者を補佐する（同規程第10条第２項及び第３項）。

活動内容は，次のとおりとされている（情報化推進支援員設置要綱）。

ａ　情報セキュリティ担当者の補佐

ｂ　情報システムの導入及び運用に係る諸制度の職員への周知及び運用

ｃ　情報化及び情報セキュリティ対策の推進及び情報化推進室との連絡調整

(ｶ)　京都市高度情報化推進本部

本市の高度情報化を全庁的に推進し，電子情報及び情報システムの情報セキュリティの確保に必要な対策を実施するため，市長部局以外を含めた局区長等[2]で構成されており，本市の情報セキュリティに関する重要な方針について総合的な調整を行う（京都市における高度情報化推進に関する体制を整備するための要綱）。

---

1 ①情報化推進室情報管理課長が公文書の管理の単位を別に定めたとき（公文書取扱規程第３条第４項ただし書）及び②庶務を担当する課長及び担当課長が情報セキュリティ担当者を指名したときを除き，各所属の個人情報管理責任者と情報セキュリティ担当者は同一の課長等となる。

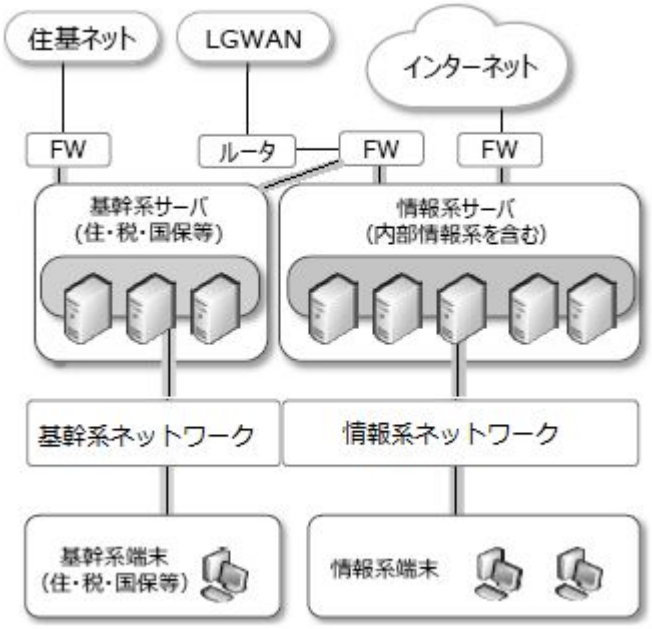
2 公営企業管理者（交通局長，上下水道局長），教育長，会計管理者，監察監，市長部局の各局の長，行財政局財政担当局長，区長会当番区区長，消防局長，市会・選挙管理委員会・監査・人事委員会の各事務局長。京都市における高度情報化推進に関する体制を整備するための要綱別表第１に掲げられている。

⑶　管理状況

本市における個人情報の管理状況等は，主に次のとおりである。

ア　情報化推進室における情報システム等（全庁共通の情報システム）の管理状況

地方公共団体における平成27年４月１日時点の一般的な情報システムの構成は，次のとおりである。



注１　「住基ネット」は，住民基本台帳ネットワークシステムの通称で，全国共通に本人確認を行うための地方公共団体共同の情報システムのこと。

２　「ＬGWAN（エルジーワン。Local Government Wide Area Network)」は，総合行政ネットワークの略称で，国と各自治体間を繋いでいる行政専用のネットワークのこと。

３　「FW」は，ファイアウォールの略で，外部との通信を監視し，外部からの攻撃から内部のネットワーク等を保護するためのもの。

４　「ルータ」は，通信機器の一種であり，ＬGWANに接続するためにはＬGWAN接続ルータが必要とされる。

（総務省　自治体情報セキュリティ対策検討チーム報告より一部変更）

本市の市長部局等における「基幹系」及び「情報系」の情報システムは，それぞれ次のとおりである。

⑺　基幹業務システム

住民記録，税，福祉等の基幹業務については，情報化推進室，各業務の所管課，各区役所及び区役所支所等間の共通のネットワークを用いて情報システムを運用している。

また，基幹業務のうち主なものについては，大型汎用コンピュータを用いて情報システムを運用している。

各情報システムの主管課は，それぞれの業務の所管課であるが，基盤となる大型汎用コンピュータ及びネットワークは情報化推進室が管理している。

なお，大型汎用コンピュータについては，オープンシステム（一般的な技術の機器等により構築された情報システム）への刷新が進められている。

(ｲ) イントラネット

インターネット接続（電子メールの利用及びホームページの閲覧等），行政業務情報システム（文書管理，財務会計，庶務事務等の内部事務を処理する情報システム），ファイル共有システム（ドックサーブ[1]）を含む庁内のネットワークシステムである。

行政業務情報システム内の各情報システム等の主管課は，それぞれの業務の所管課であるが，基盤となる情報システム等は情報化推進室が管理している。

イントラネットに接続できるパソコンをイントラネットパソコンといい，①情報化推進室が各所属に配備したパソコン及び②情報化推進室が指定した機種を各所属が調達し，情報化推進室への接続申請を経たパソコンに限られる。

なお，平成13年度末の時点では，情報化推進室が管理するイントラネットパソコン（上下水道局及び教育委員会を除く。）の配備台数は1,560台，利用者数は1,560人であったが，平成14年度以降利用者数が増加し，平成27年度末の時点では，イントラネットパソコンの配備台数は8,677台，利用者数は10,167人となっている。

イ　情報システム業務責任者（情報システムの主管課の課長等）が管理する情報システム

各所属における個人情報保護対策の実施状況を検証する観点から，上記アの状況を基に，管理に係る情報化推進室の関与の程度により区分すると，主に次のとおりとなる。

(ｱ) 基幹業務システム

a　大型汎用コンピュータで運用している情報システム

---

[1] 庁内のネットワーク上の共有フォルダにファイルの保存を行えるもの。他の職員が閲覧できない個人フォルダと，所属ごとの共有のフリースペースフォルダとがあり，用途に応じて，各自が作成したデータを保存及び共有することができる。

情報化推進室が管理している大型汎用コンピュータ及びネットワークを用いて運用している情報システムである。

b　それ以外（上記 a の各情報システムと連携する情報システムなど）

サーバ[1]等は独自で構築し，ネットワークは情報化推進室が管理しているものを共通で利用している情報システムなどがある。

(ｲ)　イントラネットに接続している情報システム

イントラネットに接続している情報システムについては，イントラネットを管理する情報システム業務責任者（情報化推進室情報政策課長）が許可をしたうえで，イントラネットの適切な維持管理に必要な設定を実施させることとされている(情報セキュリティ対策基準　５　ネットワーク管理基準第 17 条及び第 18 条)。

(ｳ)　その他，独自でネットワークの構築等を行っている情報システム

なお，第１　４(1)に掲げる全庁調査のうち，情報システムの管理に係る各所属におけるリスク認識及び周知等の状況については，上記(ｱ) b 及び(ｳ)の情報システムを「各所属で管理する情報システム」として，回答があった 78 システムを対象としている。

ウ　各所属の課長等が管理するもの

(ｱ)　特定の情報システムに属さない情報機器

特定の情報システムに属さない電子計算機(以下「スタンドアロンパソコン」という。)，ソフトウェア，周辺機器及び記録媒体については，情報セキュリティ担当者（課長等）が，盗難，不正操作，盗み見等による被害を防止するため，必要な措置を講じなければならないとされている（情報セキュリティ対策基準　２　情報システム運用管理基準第５条第３項)。

(ｲ)　公文書（電子情報及び紙文書）

公文書については，公文書取扱規程に則り，未処理の公文書については職員が常に適切に管理し（第 40 条第１項)，完結文書については文書管理責任者（個人情報管理責任者に同じ。課長等）が適切に保管しなければならない（第 43 条第５項等）とされている。

---

[1] 情報システムにおいて，他の電子計算機に対し機能や情報を提供する役割の電子計算機のこと。

なお，公文書とは，実施機関の職員等が職務上作成し，又は取得した文書，図画及び電磁的記録であって，当該実施機関の職員等が組織的に用いるものとして，当該実施機関が保有しているものとされており（京都市情報公開条例第２条第２号），情報セキュリティ対策基準における電子情報及び入出力帳票には，公文書に該当するものも含まれる。

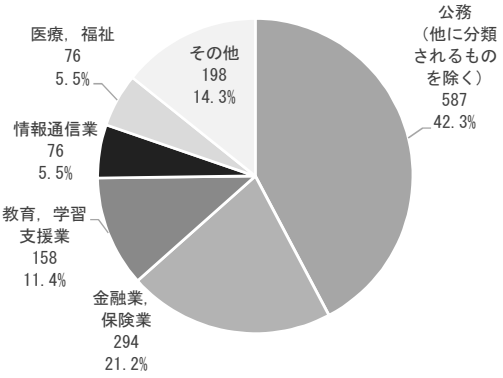
2　全国の個人情報漏えい事案の動向

⑴　個人情報漏えい事案の集計結果

日本ネットワークセキュリティ協会[1]「2013 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」によれば，平成 25 年に報道等で公表された個人情報漏えい事件・事故の集計結果は，次のとおりである。

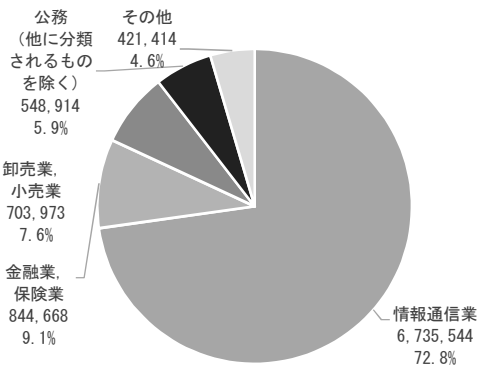
ア　業種別比率

(ｱ)　漏えい件数（単位：件）



「公務」の占める割合が 42.3%と高いのは，個人情報を取り扱う機会の多さに加え，小規模事案でも公表することが多いためと考えられるとされている。

(ｲ)　漏えい人数（単位：人）



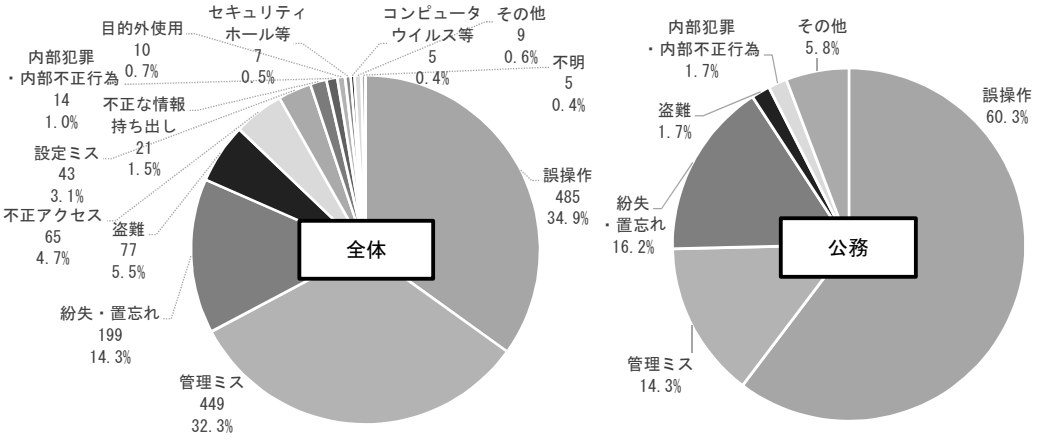
「公務」の占める割合が 5.9%と漏えい件数に比べて低いのは，取り扱う個人情報が住民票の交付など１人単位であり，１回で漏えいする人数が少ない(件数の約７割が紙媒体の誤送付等による 10 人未満の漏えいである)ためと考えられるとされている。

---

[1] ネットワークセキュリティシステムに携わる企業等により設立され，ネットワークセキュリティに関する啓発，教育，調査研究及び情報提供に関する事業を実施する特定非営利活動法人。以下，本項においては特定非営利活動法人日本ネットワークセキュリティ協会「2013 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」を参考としている。
なお，同報告書の内容は，後述する本市の情報化推進支援員研修等にも利用されている。

イ　漏えい原因別比率

(ｱ)　漏えい件数（単位：件）

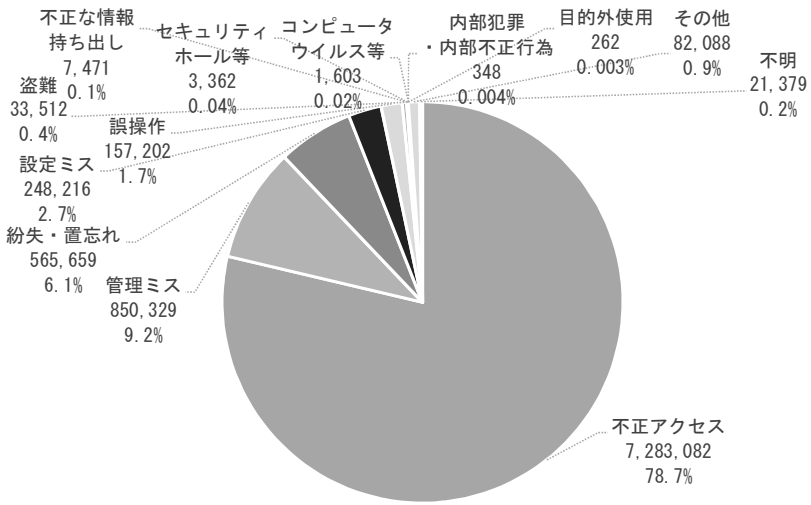


「誤操作（郵送，ＦＡＸ，電子メールの宛先誤り等)」「管理ミス（社内での紛失等)」「紛失・置忘れ（持出し先での紛失等)」といったヒューマンエラーが 81.6%を占めており，平成 19 年以降，この３原因が上位を占める傾向が続いているとされている。

「公務」では「誤操作」の占める割合が 60.3%と高く，１年間に公表された「誤操作」の件数の約７割を「公務」（誤送付等）が占めるとされている。

また，「内部犯罪・内部不正行為」については，全体では減少傾向にあるとされているが，14 件中 10 件を「公務」が占める。

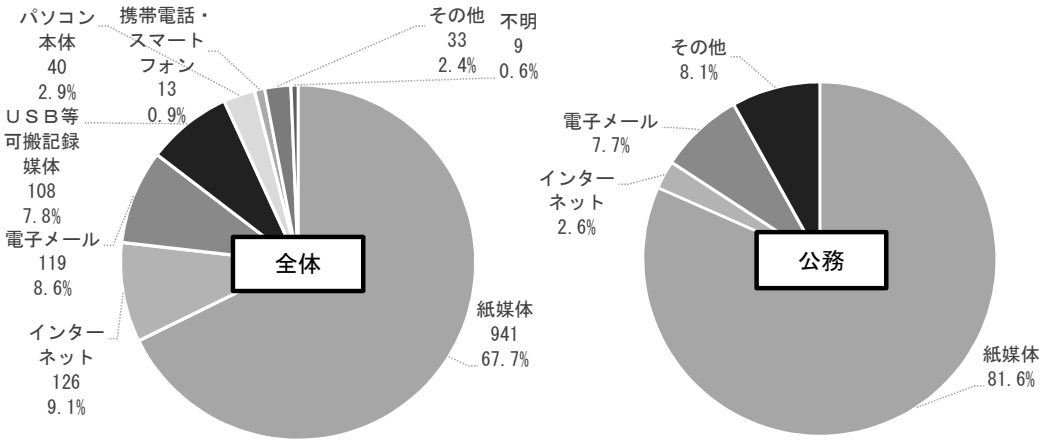
(ｲ)　漏えい人数（単位：人）



１件当たりの被害（漏えい人数）が拡大傾向にある「不正アクセス」が 78.7%と突出しているほか，悪意がない原因である「管理ミス」で漏えい人数の多い事案が生じているとされている。

ウ　漏えい媒体・経路別比率

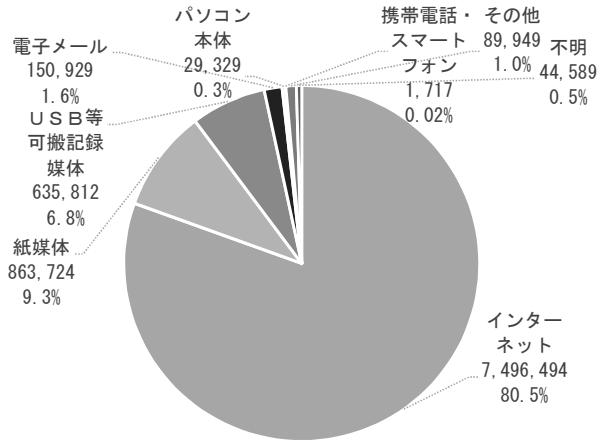
(ｱ)　漏えい件数（単位：件）



「紙媒体」による漏えい件数が 67.7%と最も多く，平成 21 年以降，減少傾向にあったが，平成 25 年は増加したとされている。「インターネット」経由の漏えい原因については，「不正アクセス」が約５割と最も多く，平成 24 年と比較し約 1.7 倍に増加したとされている。

また，「公務」では，特に紙媒体の比率が 81.6%と高いとされている。

(ｲ)　漏えい人数（単位：人）



「インターネット」が 80.5%を占めており，大規模な漏えいの比率が高いとされている。平成 25 年に公表された事案のうち，漏えい人数が多い上位 10 件中８件が「インターネット」によるものであり，うち７件が「不正アクセス」によるものであったとされている。

⑵　平成 27 年度に生じた個人情報漏えい事案の事例

上記⑴の動向に加え，平成 27 年度には，日本年金機構において，標的型攻撃による不正アクセスが生じ約 125 万件の個人情報が流出した事案や，堺市において，職員が業務データを無断で持ち帰り約 68 万人の個人情報が流出した事案が発生したところである。

以上のような状況から，後述の「第３　２　個人情報の適正な管理のために必要な措置」では，①誤送付，紛失などの誤りを防止する対策，②漏えい目的の情報持出しなどの内部不正を防止する対策及び③標的型攻撃などの外部からの攻撃に対する対策の状況を確認している。

第３　調査の結果

第１　２⑵に掲げる着眼点に沿って，次の各項目について述べる。

規程等の状況	本市における個人情報保護条例及び情報セキュリティ対策基準等の状況を確認する。
運用の状況	全庁的な運用の状況（全庁共通の情報システムにおける技術的対策等）を記載する。
全庁調査の結果等	運用の状況を踏まえたうえで，各所属において必要とされている主な対策を挙げる。 また，第１　４⑴に掲げた全庁調査の集計結果から，各所属におけるリスク認識の状況等の傾向を確認する。
実地調査の結果等	主として実地調査で確認された問題等を記載する。 本市の規定に違反する取扱いをしていたものに限らず，本市の現状の規定に明確に違反しているとまではいえないが，検討を要すると考えられるものや，良好事例についても記載している。 なお，監査の目的を達成する観点から，実地調査の時点で既に改善がされていた問題等も，他の所属において同様の問題が生じている可能性等を鑑み，事例として記載している。

1　個人情報取扱事務の届出及び個人情報の取扱いの制限に係る職員への周知

⑴　規程等の状況

ア　個人情報保護条例

⑺　個人情報の収集等の制限（同条例第６条，第８条，第８条の２，第 10 条，第 11 条）

個人情報の収集，利用及び提供並びに電子計算機処理等の制限は，次のとおりであり，次に掲げる事項を行う場合は，あらかじめ個人情報保護審議会の意見を聴かなければならない。

ａ　本人外収集（同条例第６条第２項）

個人情報は，法令に定めがあるときや，本人の同意があるときなどを除き，原則として本人から収集しなければならない。

ｂ　センシティブ情報の収集（同条例第６条第３項）

①思想，信条及び宗教に関する個人情報，②人種，民族その他社会的差別の原因となるおそれがあると認められる社会的身分に関する個人情報並びに③病歴，遺伝子に関する情報その他身体的特質に関する個人情報で個人の権利利益を侵害するおそれがあると認められるもの（以下「センシティブ情報」という。）は，法令に定めがあるときを除き，原則として収集してはならない。

ｃ　目的外利用及び提供（同条例第８条第１項，第８条の２）

個人情報は，法令に定めがあるときや，本人の同意があるときなどを除き，原則として個人情報の目的外の利用，提供をしてはならない[1]。

ｄ　センシティブ情報等の電子計算機処理（同条例第 10 条第１項）

センシティブ情報や犯罪に関する個人情報は，法令に定めがあるときを除き，原則として電子計算機処理[2]をしてはならない。

ｅ　新たな電子計算機処理（同条例第 10 条第２項）

新たに個人情報の電子計算機処理をしようとするときは，あらかじめ個人

---

[1] 番号法第２条第８項に規定する特定個人情報の利用の制限については，個人情報保護条例第８条の２において別に定められており，あらかじめ個人情報保護審議会の意見を聴いて目的外利用等を行うことはできない。

[2] 電子計算機を使用して行われる情報の入出力等をいう。ただし，文書作成ソフトの利用，イメージ情報としての保存，製版等の印刷物製作，ＦＡＸ，電子メール等を除く（個人情報保護条例第２条第４項，個人情報保護条例の趣旨及び運用）。

情報保護審議会の意見を聴かなければならない。

ｆ　**電子計算機の結合**（同条例第 11 条）

法令に定めがあるときを除き，個人情報の提供等を行うために，実施機関以外のものとの間において，電子計算機を結合してはならない。

(ｲ)　個人情報取扱事務の届出（同条例第７条）

ａ　個人情報取扱事務を開始しようとするときは，あらかじめ，事務の名称及び目的等を市長に届け出なければならない。

ｂ　個人情報取扱事務の届出により，保有する個人情報の把握や，収集の必要性や範囲を再確認し，慎重かつ責任を持って個人情報を取り扱うことが期待できるとされている（個人情報保護条例の趣旨及び運用）。

ｃ　なお，個人情報を収集しようとするときは，個人情報取扱事務の目的を明確にしなければならないとされており（同条例第６条第１項），その趣旨は，「内部規制として，事務を所管する部署において事務の目的を確認すること」とされている（個人情報保護条例の趣旨及び運用）。

(ｳ)　個人情報取扱事務目録の作成（同条例第７条第４項）

ａ　市長は，個人情報の取扱いの状況を市民に周知するため，届出に係る事項を記載した目録を作成し，市民が閲覧できるようにしなければならない（個人情報保護条例の趣旨及び運用）。

ｂ　実務上は，情報化推進室情報管理担当から各局等へ定期的に個人情報取扱事務目録データを送付し，確認を求めている。

⑵　運用の状況

ア　平成 26 年度の個人情報保護制度の運用状況（実施機関が市長であるもの）は，開始届 50 件，変更届 45 件，廃止届 18 件，個人情報取扱事務数 1,469 件とされており，全実施機関の個人情報取扱事務数 2,143 件の 68.5％を占めていた。

実施機関	開始届	変更届	廃止届	取扱事務数
市長（市長部局分）	50 件	45 件	18 件	1,469 件
合計（公営企業等を含む全実施機関合計）	70 件	57 件	25 件	2,143 件

また，平成 26 年度に開催された個人情報保護審議会で承認を得た案件は 20 件であり，うち 18 件は電子計算機処理に係る案件であった。

⑶　全庁調査の結果等

ア　各所属において必要とされている主な対策

本市の研修においては，課長級職員の留意点は，特に次の２点とされている。

(ｱ)　所属で取り扱っている個人情報の種類及び管理状況を確認すること。

個人情報取扱事務においては，作業マニュアルがあることが望ましい。

(ｲ)　所属の職員が何をすべきか具体的にイメージできるよう，個別具体的な業務内容に沿って，個人情報の管理についての意識の徹底を図ること。

イ　全庁調査の結果

(ｱ)　所管する個人情報取扱事務ごとの個人情報の取扱いの制限に係る周知の状況（複数回答）

回答した所属のうち，所管する個人情報取扱事務（個人情報取扱事務目録に記載されている個人情報取扱事務）ごとの個人情報の取扱いの制限について，業務マニュアル等への記載などがされているものがあると回答したのは，25.6％であった。

個人情報取扱事務目録の周知（確認の依頼等）をしたものがあるとの回答が最も多く，35.8％であった。

（単位：所属，％）

①業務マニュアル等への記載などがされているものがある	73	25.6%
②上記①はしていないが，個人情報取扱目録の周知をしたものがある	102	35.8%
③上記②はしていないが，個人情報保護条例の内容自体を周知しているものがある	99	34.7%
④周知されていないものがある	16	5.6%
⑤それ以外のものがある（把握していないなど）	38	13.3%

注　所管する個人情報取扱事務がないと回答した所属等を除く 285 所属に占める割合

⑷　実地調査の結果等

ア　個人情報取扱事務の届出がされていなかったものがあった。

２　個人情報の適正な管理のために必要な措置

実施機関は，個人情報の漏えい，改ざん，滅失及びき損の防止その他の個人情報の適正な管理のために必要な措置を講じるとともに，個人情報を適正に管理させるため，個人情報管理責任者（課長等）を置かなければならないとされている（個人情報保護条例第12条第２項）。

個人情報を含むデータ等の保護については，情報セキュリティ対策に関する基準を遵守するとともに，それぞれの所属において，個人情報の内容，取扱いの目的に応じ，適切な措置を講じるものとされている（個人情報保護条例の趣旨及び運用）。

⑴　帳票による管理

ア　規程等の状況

(ｱ)　文書管理

個人情報の有無や，電子情報と紙文書の別にかかわらず，公文書については文書管理システムに登録して管理することとされている。

ａ　公文書取扱規程

⒜　常時執務の用に供するものや帳簿類は，当該公文書をとじる簿冊等を文書管理システムに登録しなければならない（同規程第40条第２項）。

⒝　完結した文書については，当該公文書をとじる簿冊等を文書管理システムに登録し（同規程第40条第３項，第４項），紙文書をとじた簿冊又は電磁的記録の保管場所を文書管理システムに登録しなければならない（同規程第41条第５項）。

(ｲ)　情報セキュリティ対策基準等

ａ　情報システム運用管理基準

情報セキュリティ担当者（課長等）は，課等において利用する電子計算機，ソフトウェア，周辺機器及び記録媒体を管理するため，情報資産管理簿を整備しなければならない（同管理基準第７条第４項）。

ｂ　情報資産管理簿の様式及び記載要領

「情報資産管理簿の提出について」（平成25年５月27日付け総合企画局情報化推進室情報政策課長依頼）において示されており，個人情報の有無を区別することとされている。

⒜　情報システムの主管課において作成するもの

・　基幹業務システムに係る機器等

・　情報システム全体がネットワークで接続され，情報システムの主管課が管理や保守の全てを行っているもの

⑹　各課等において作成するもの

・　機器を設置している課等で管理や保守の一部を行っているもの

・　イントラネットパソコン及び周辺機器

イ　全庁調査の結果等

(ｱ)　全庁調査の結果

a　情報資産管理簿の更新の状況

更新されていない，又は，最新の状態かどうか不明であると回答した所属が23.1%，備え付けられていないと回答した所属が10.6%あった。

（単位：所属，%）

①更新されている	223	61.9%
②更新されていない，又は，最新の状態かどうか不明である	83	23.1%
③備え付けられていない	38	10.6%
無回答	16	4.4%
合計	360	100.0%

注　回答（無回答を含む。）には，庶務を担当する課等で一括して事務を行うこととされている場合等を含む。以下同じ。

b　情報資産管理簿の保管状況

平成25年度に，情報資産管理簿の整備状況等を確認するために提出が依頼された後，更新が必要であることは引き継がれていなかったと回答した所属が13.1%，過年度の照会回答として保管されていたと回答した所属が17.8%あった。

（単位：所属，%）

①更新が必要なことが分かるような状態で保管されていた	198	55.0%
②常用のものとして保管されているが，更新が必要であることは引き継がれていなかった	47	13.1%
③過年度の照会回答として保管されていた	64	17.8%
④保管されていなかった	32	8.9%
無回答	19	5.3%
合計	360	100.0%

ウ　実地調査の結果等

(ｱ)　個人情報取扱事務で組織的に用いている個人情報を含む文書について，文書

管理システムへの登録がされていないものがあった。

また，各区等に共通する文書の登録状況が区等によって異なっていた。

(ｲ) 情報資産管理簿が最新の状態に更新されていないものがあった。

(ｳ) 情報システムの主管課において，ネットワークの物理的な配線状況に係る文書が保管されていないものがあった。

⑵ 機器等の管理

ア 規程等の状況

(ｱ) 情報セキュリティ対策基準

a 情報システム室管理基準

情報システムの基幹的なサーバ等（大型汎用コンピュータ等）については，外部から容易に進入できない場所に設置し，必要な保安措置を講じなければならないとされているほか，入退室の管理及び監視，電子機器の持込み制限等について規定されている。

b 情報システム運用管理基準

情報システム業務責任者等は，盗難，不正操作，盗み見等による被害を防止するため，それぞれ次のことを行わなければならないとされている。

⒜ 情報システム業務責任者（情報システムの主管課の課長等）の責務

- 主管する情報システムのサーバについて，施錠可能な区画内に設置し（同管理基準第３条第１項），物理的対策を講じる（同管理基準第４条第１号）。
- 主管する情報システムの構成要素である電子計算機等について，①必要な措置を講じるとともに，②運用手順を定め，③職員に周知する（同管理基準第５条第１項)。

⒝ 情報セキュリティ担当者（課長等）の責務

- 上記の運用手順が遵守されるよう，職員を指導及び監督する（同管理基準第５条第２項)。
- 特定の情報システムに属さない電子計算機等について，①必要な措置を講じるとともに，②職員に周知する（同条第３項)。

⒞ 職員の責務

- 情報システム業務責任者及び情報セキュリティ担当者の指示に従い，電子計算機等を適切に取り扱う（同管理基準第 12 条)。
- 私物機器（個人が所有する電子計算機等）を使用しない（同管理基準第 11 条)。

c 電子情報等の保護に関する管理基準

情報システム業務責任者等は，情報の漏えいを防止するため，それぞれ次

のことを行わなければならないとされている。

⑷ 情報システム業務責任者（情報システムの主管課の課長等）の責務

・ 所管する情報システムに係る電子情報の保護に関し，適切な方法を定め，適切な運用を図る（同管理基準第 11 条第１項)。

・ 所管する情報システムに係る重要性Ⅰに該当する電子情報及び入出力帳票（個人情報等）について，安全な保管設備を備える等の必要な対策を講じる（同管理基準第 12 条)。

・ 復元が困難な電子情報等の複製は，耐火性の保管庫に保管し，又は物理的に隔離された施設に保管する等の必要な措置を講じる（同管理基準第 13 条)。

⑸ 情報セキュリティ担当者（課長等）の責務

・ 課等における電子情報等の保護に関する事務を掌理する（同管理基準第３条第３項)。

⑹ 職員の責務

・ 重要性Ⅰに該当する電子情報及び入出力帳票（個人情報等）について，施錠可能な場所に保管する等の適切な措置を講じる（同管理基準第６条第２項）。

・ 入出力帳票の廃棄に当たっては，適切に処分する（同管理基準第９条)。

・ 電子情報が記録されている記録媒体の廃棄に当たっては，記録されている電子情報を復元することができないよう，確実に電子情報の消去又は記録媒体の破壊をするなど，適切な措置を講じる（同管理基準第 10 条）。

イ 運用の状況

⑺ 情報化推進室によるサーバの管理等

ａ 情報化推進室サーバ室

大型汎用コンピュータ等については，情報化推進室がサーバ室を設置し，情報システム室管理基準に則った取扱いを行っている。

ｂ 京都市データセンターの整備

各所属で開発した情報システムのサーバ等については，各情報システムの主管課の執務室等に分散して設置していたが，平成 23 年度から民間施設内に

京都市専用のデータセンターを整備し，順次サーバ等の移設を行い，集約して管理している。

c　共用サーバ等の構築

これまでは，情報システムを開発する際，各情報システムの主管課で基盤となるサーバ等の調達及び運用管理を実施していたが，情報セキュリティの向上等のため，平成 26 年度に京都市データセンター内に大規模な共用サーバ機器等を構築し，今後は原則として当該サーバ等を利用するよう庁内に依頼している。

京都市クラウド活用の手引（平成 27 年６月策定）では，個人情報等の機密を要する情報を取り扱う情報システムにおいてクラウド[1]を活用する場合は，情報化推進室の許可を得たもの以外は当該サーバ等を利用することとされている。

d　情報システムの最適化

情報システムの導入時及び更新時の最適化の方針に基づき，各情報システムの主管課において，各区役所及び区役所支所に配置されていたサーバの集約化等が行われている。

(ｲ)　イントラネットパソコンの廃棄等の際の取扱い

イントラネットパソコンについては，イントラネットへの接続停止や，リース終了後の返却を行う場合は，情報化推進室が事業者に委託するなどしてデータの消去を行っている。

ウ　全庁調査の結果等

(ｱ)　各所属において必要とされている主な対策

機器等の管理に関して，各所属において必要とされている主な個人情報保護対策は，次のとおりである。

a　文書や情報機器等については，施錠管理等を行う。

b　機器等の廃棄を行う場合は，物理的な破壊又はデータの消去を行う。

c　情報システムの更新等を行う場合は，共用サーバ等の利用を検討する。

(ｲ)　全庁調査等の結果

[1] インターネット等のネットワークを通じて情報システムを利用する形態のこと。

a　個人情報を取り扱う情報システムの設置及びサーバ等の管理状況

現在，個人情報を取り扱う情報システムの設置状況の現況を全庁的に管理している帳票類はないため，情報システムに係る予算計上の状況等を基に確認したところ，57 所属 117 システムが設置されているとの回答があった。

⑷　サーバ等の設置場所等

個人情報を取り扱う情報システムのサーバ等の設置場所等については，次のとおり回答があった。

（単位：システム，％）

情報化推進室サーバ室又は京都市データセンター	41	35.0%
所属	44	37.6%
事業者	14	12.0%
他団体	10	8.5%
その他	8	6.8%
合計	117	100.0%

⑸　サーバ等を所属に設置している情報システムのネットワークの状況

上記のうち，サーバ等を所属に設置していると回答があった情報システムのネットワークの状況については，所属内のネットワークとの回答が 43.2%，スタンドアロンとの回答が 36.4%と多くを占めていた。

（単位：システム，％）

他の庁舎等とのネットワーク	7	15.9%
所属内のネットワーク	19	43.2%
スタンドアロン（ネットワーク構築・接続していない）	16	36.4%
その他	2	4.5%
合計	44	100.0%

⑹　所属内でのサーバ等の設置状況

上記のうち，他の庁舎等とのネットワークと回答があったものについては，概ねサーバ室を設けていると回答があったが，所属内のネットワークと回答があったものについては，小型のサーバ等を使用しているものや，サーバ専用の機器を置かずパソコン同士を接続しているものなどであり，概ね執務室内に設置していると回答があった。

（単位：システム，％）

他の庁舎等とのネットワーク	サーバ室	6	85.7%
	執務室	1	14.3%
	合計	7	100.0%
所属内のネットワーク	サーバ室	0	0.0%
	執務室	18	94.7%
	その他	1	5.3%
	合計	19	100.0%

b　個人情報が保存された記録媒体やスタンドアロンパソコンの管理状況

70.6%と多くの所属が，個人情報が保存された記録媒体やスタンドアロンパソコンがあると回答した。

（単位:所属，％）

①ある	254	70.6%
②ない	93	25.8%
無回答	13	3.6%
合計	360	100.0%

c　記録媒体の保存期間やデータ廃棄方法

情報システムのバックアップや個人情報の読み込みに用いる記録媒体について，保存期間やデータ廃棄方法が決まっていないものがあると回答があった情報システムが，41.0%あった。

（単位:システム，％）

①全て決まっている	26	33.3%
②決まっていないものがある	32	41.0%
③該当する記録媒体はない	20	25.6%
合計	78	100.0%

エ　実地調査の結果等

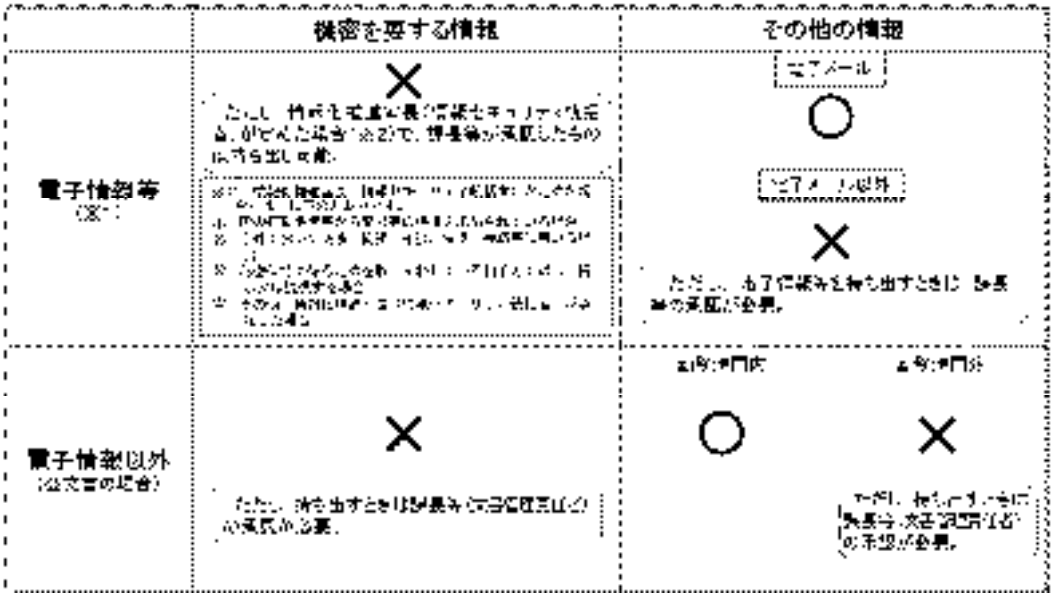
(ｱ)　記録媒体やスタンドアロンパソコン等について,施錠管理等はされていたが,廃棄可能なものや，廃棄の可否が不明なものが保管されていたものがあった。

⑶ 誤り（誤送付，紛失等）を防止するための対策

ア 持出し

(ｱ) 規程等の状況

平成26年８月に，文書等の庁外への持出しや電子メールでの送信について，厳格に取り扱うことを目的として，公文書取扱規程（第48条）及び情報セキュリティ対策基準（１　電子情報等の保護に関する管理基準第７条及び第８条）が改正され，取扱いが次のとおり改められた（文書等の持出し等に関する事務の変更について（平成26年８月８日付け情報化推進室情報政策課長，情報管理課長通知））。



※1　電子情報等とは，電子情報と入出力帳票のことを指し，公文書に該当する電子情報等も含まれます。

（「情報セキュリティに関する解説書」から抜粋）

(ｲ) 運用の状況

a　イントラネット（電子メールの送信）

添付ファイルへのパスワード設定を忘れると，誤送信等による情報漏えいの恐れがあるため，平成27年６月から，添付ファイルへのパスワード設定や，情報セキュリティ担当者（課長等）への同時送信がされていない場合は，送信をブロック（禁止）している。

(ｳ) 全庁調査の結果等

a　各所属において必要とされている主な対策

(a) 電子メールでの送信については，一定の技術的対策がされている（機密

を要する情報が含まれる添付ファイルのパスワードを電子メールの本文に記載しないといった，運用上のルールを所属内で徹底する必要がある。）。

⑹ 記録媒体や紙文書での持出しについては，課長等が適切に承認し，記録媒体内の電子情報については必要に応じて暗号化する必要がある。

b 全庁調査の結果

⑹ 個人情報を含む文書や電子情報等の執務室外への持出しを行う事務

59.2%の所属が，個人情報の執務室外への持出し（庁外への持出しに該当しないものを含む。）があると回答した。

（単位：所属，%）

①ある	213	59.2%
②ない	143	39.7%
③把握できていない	1	0.3%
無回答	3	0.8%
合計	360	100.0%

⑹ 執務室外への持出しを行う媒体（複数回答）

個人情報の執務室外への持出しがあると回答した所属のうち，電子情報（記録媒体）の持出しがあると回答した所属は17.8%であり，主に紙文書が持出しに用いられている傾向にあった。

（単位：所属，%）

①紙	205	96.2%
②電子情報（記録媒体）	38	17.8%

⑹ 個人情報を持ち出す目的（複数回答）

交渉，協議等に使用すると回答した所属の割合が，77.0%であった。

交渉，協議等に使用する場合，相手方への提供や受渡しに比べて，持ち帰り時の紛失の可能性や，すぐに紛失に気づかない可能性があり，より適切な取扱いが求められると考えられる。

（単位：所属，%）

①文書や電子情報等の提供や受渡し	81	38.0%
②交渉，協議，相談，催促，会議等に使用	164	77.0%
③その他（保管場所の変更など）	26	12.2%

⑹ 庁外への持出しに係る課長等の承認の状況

承認ができていると回答した所属は，課長等の承認が必要な持出しがあると回答した所属等のうち，72.2%であった。

できていないことがあると回答した所属から抽出して状況を聞き取った

ところ，職員が無断で持出しを行った場合は確認する手段がないため，全てできているとまではいいきれないなどの回答であった。

また，できていると回答した所属から抽出して状況を聞き取ったところ，持ち出す文書等を毎回目視確認しているわけではないが，外勤の状況は把握しているため，外勤の目的に応じて持ち出す文書等も了承しているなどの回答であった。

なお，返却の確認ができていないものがあると回答した所属も，11.7%あった。

（単位：所属，%）

できている	148	72.2%
できていないことがある	54	26.3%
全くできていない	3	1.5%
その他（執務室外への持出しはあるが庁外への持出しはないなど）	8	-
合計	213	100.0%

イ　送付

(ｱ)　全庁調査の結果等

ａ　全庁調査の結果

⒜　個人情報を含む情報等を送付する機会がある所属（複数回答）

郵送，電子メールの一斉送信，ＦＡＸとも，半数以上の所属が送付する機会があると回答した。

（単位：所属，％）

①郵送	235	65.3%
②電子メールの一斉送信	214	59.4%
③FAX	223	61.9%

⒝　住民記録，税，福祉関係の業務を所管する課等における誤送付防止対策（複数回答）

住民記録，税，福祉関係の業務を所管していると回答があった15課等における一斉発送の手順については，次のとおり回答があった。

（単位：所属，％）

①マニュアルなどの文書で定め，共有されているものがある	9	60.0%
②文書はないが運用として職員間で共有されているものがある	7	46.7%
③具体的な手順はないが，一般的な対応として複数名で確認するよう周知しているものがある	7	46.7%
④特に決まっていないものがある	1	6.7%

⒞　区役所及び市税事務所等の住民記録，税，福祉関係の業務を行う課等における誤送付防止対策

所属でプリンターから１件ずつ出力して送付する郵便物があると回答した所属のうち，88.2％の所属は何らかの誤送付防止対策（ダブルチェック等）がとられていると回答した一方で，11.8％の所属は，対策がとられていないと回答した。

（単位：所属，％）

①誤送付防止対策がとられている	97	88.2%
②誤送付防止対策がとられていない	13	11.8%
合計	110	100.0%

(ｲ)　実地調査の結果等

ａ　個別に送付する少量の郵便物については，封かんせずに所定の場所へ集約することとし，発送前にまとめて内容の照合を行ってから封かんすることで，

複数名によるチェックが必ず実施されるようにしているものがあった（良好事例）。

b　同一業務を行う課等間の会議等において，他の課等で生じた誤送付等の具体的な原因や再発防止対策等の情報共有がされていたものがあった（良好事例）。

⑷ 内部不正（漏えい目的の持出し等）に関する対策

ア 規程等の状況

(ｱ) 情報セキュリティ対策基準

a 情報システム利用者管理基準

⒜ 情報システム業務責任者（情報システムの主管課の課長等）は，故意又は過失による情報資産の漏えい等の事故を防止するため（同管理基準第１条），次のことを行わなければならない。

① 利用者認証及び利用者権限の制御

・ 利用者認証機能[1]及び利用者権限[2]制御機能[3]を設けることにより，許可された以外の者の利用及び権限を越えた利用を防止する（同管理基準第３条）。

・ 利用者認証機能は，識別コード[4]及びパスワード又は生体認証を利用する方法によることとし（同管理基準第４条），識別コードは利用者個人ごとに異なるものを付与する（同管理基準第６条）。

・ パスワードの文字数，使用する文字種及び管理方法について定めるとともに，利用者に周知し（同管理基準第７条第２項），利用者に初期パスワードの変更（同管理基準第８条第１項）及びパスワードの定期的な変更（同管理基準第９条）をさせる。

② 利用者権限の管理（同管理基準第 10 条）

・ 利用者の職責及び必要性を勘案し，取扱い可能な情報及び利用可能な機能の範囲を必要最小限に設定するなど，適切な利用者権限の制御を行う。

・ 管理者権限を持つ識別コードは，担当職務又は職責に即して必要最低限の者に付与する。

・ 異動等により情報システムを利用する必要がなくなった者の識別コード等を直ちに無効にするとともに，識別コードを登録したカード

---

[1] 情報システムの利用者を識別コードにより識別し，その有効性を判別する機能のこと（同管理基準第２条）。

[2] 情報システムの機能，情報等を取り扱うことができる権利のこと（同管理基準第２条）。

[3] 情報システムの利用者に対し，利用者権限の一部又は全部を制限する機能のこと（同管理基準第２条）。

[4] 利用者を識別するために情報システムが認識する記号のこと（同管理基準第２条）。

を交付している場合は返納させる。

③ ログの管理

・ 情報の漏えい等の事故発生時の原因調査等の目的で利用するため，操作履歴，通信履歴等のログ[1]を取得する機能を設け（同管理基準第11 条），適切に定めた保存期間が満了するまで保存する（同管理基準第12 条）。

・ 定期的に又は適宜ログの点検及び分析をする（同管理基準第13 条第１項）。

・ 情報システムの利用者に対し，ログの取得，保存，点検及び分析を行うことをあらかじめ周知する（同管理基準第14 条）。

④ 例外措置

基準を遵守することが困難な場合は，情報セキュリティ統括者（情報化推進室長）の許可を得て，例外措置を採る（同管理基準第18 条）。

(b) 情報セキュリティ担当者（課長等）は，所管するスタンドアロンパソコンについて，機能上及び運用上必要な範囲において，上記に準じて利用者認証等を行わなければならない（同管理基準第17 条）。

(c) 情報システムの利用者は，他の職員との識別コード又はパスワードの共有や，複数の情報システム間でのパスワードの共有をしてはならない（同管理基準第15 条，第16 条）。

イ 運用の状況

次のとおり，全庁共通の情報システムについては，情報セキュリティ対策基準に則った機能が設けられている。

(ｱ) 住民記録，税，福祉等の基幹業務に係る情報システムのうち，大型汎用コンピュータで運用しているもの

a 利用者認証及び利用者権限の制御

(a) 利用者個人ごとに異なる識別コードが付与されている。

(b) パスワードを定期的に変更しなければ利用ができない機能が設けられており，パスワードに一定以上の文字数や文字種を使用しなければならない

[1] 情報システムの利用状況や通信の記録のこと（同管理基準第２条）。

とする制限も設けられている。

b　利用者権限の管理

⑷　各情報システムの主管課及び区役所等の権限や端末では，電子データで情報を出力できないよう，制限がされている。

c　ログの管理

⑷　情報化推進室の端末からの情報の出力については，ログの取得，確認等により不正行為の監視を行っている。

⑹　個人情報の閲覧等についてもログの取得を行っており，通知文に記載するなどの方法により職員に周知している。また，適宜ログの確認等が行われており，平成 26 年度には，情報システムの主管課及び区役所等において業務以外の目的での閲覧がされていないか，確認が行われた。

⑹　平成 27 年度からは，区役所等でログインや画面の表示をしたまま長時間操作がされないなど，不適切な運用が見られる場合は，情報化推進室から各情報システムの主管課に連絡がされることとなった。

(ｲ)　イントラネット

a　利用者認証及び利用者権限の制御

⑷　利用者個人ごとに異なる識別コードが付与されている。

⑹　行政業務情報システムについては，パスワードを定期的に変更しなければ利用ができない機能が設けられており，パスワードに一定以上の文字数や文字種を使用しなければならないとする制限も設けられている。

b　利用者権限の管理

⑷　イントラネットパソコンの管理者権限は制限されており，許可されたソフトウェア[1]の導入を行う際など，必要に応じて情報化推進室から臨時的に管理者権限が付与される。

⑹　行政業務情報システムの担当者の権限については，各所属では，所属長の権限でのみ付与できる。

c　ログの管理

[1] 電子計算機を構成する回路や装置などの物理的実体をハードウェアと呼ぶのに対し，それ自体は形を持たないプログラム（電子計算機を動作させる命令や処理手順のまとまり）や，プログラムの扱うデータなどをソフトウェアという。

⑷　ログの取得を行っており，イントラネットホームページ[1]等を通じて職員に周知している。

⑸　データの持出し等を防止するため，後述するコンプライアンス推進月間及び情報セキュリティ対策強化月間の取組として，スマートフォンやＵＳＢメモリ等，許可を得ていない機器の接続状況の確認を行っている。

⑹　平成26年度には，電子メールの送信履歴についての確認が行われた。

ｄ　内部不正に関するその他の主な対策

⑷　インターネット経由での持出し

・　電子メールでの自宅への送信等を防止するため，情報セキュリティ担当者（課長等）への同時送信がされていない場合は，添付ファイルの送信をブロック（禁止）している。

・　オンラインストレージ[2]へのアップロードやＷＥＢメール[3]の使用，他の電子メールのソフトウェアの導入については，制限されている。

⑸　外部記録媒体の接続等による持出し

・　自動的にデータの暗号化がされるため，イントラネットパソコン以外で開けるような形式で外部記録媒体にデータを保存するには，情報セキュリティ担当者（課長等）が管理する機器による認証が必要となる。

・　パソコンをイントラネットに接続するには，情報化推進室での接続手続が必要とされており，私物のパソコンをイントラネットに接続することはできない。

⑹　パソコン本体の持出し

・　自動的にデータの暗号化がされるため，イントラネットに接続していない状態では，パソコン本体に保存したデータを開くことが制限される。

・　なお，非公開情報が含まれたファイルは，必ずドックサーブ又はフロッピーディスクなどの記録媒体に保存することとされている。

ウ　全庁調査の結果等

---

[1] インターネットの技術を利用した職員向けネットワーク上のホームページのこと。

[2] インターネット上でファイル管理用のディスクスペースを貸し出すサービスのこと。

[3] インターネットを通じて無料で自分のメールアドレスが開設できるものなど，インターネット上等で利用することができる電子メールのシステムのこと。

(ｱ) 各所属において必要とされている主な対策

a　住民記録，税，福祉等の基幹業務に係る情報システムのうち，大型汎用コンピュータで運用しているもの

(a)　ＩＤカード[1]及びパスワードの適切な管理

(b)　情報化推進室の端末から出力して受領したデータの適切な管理

b　イントラネット

(a)　課長等による機器等の適切な管理

c　その他の情報システム等

情報セキュリティ対策基準に則り，利用者個人ごとの権限の管理により，利用者権限がない者の不正利用を防止する必要がある。

また，情報システムの正当な利用者権限を持つ者が不正を行う場合もあるため[2]，操作履歴等のログの管理により，利用者権限がある者の不正利用を防止する必要がある。

ログは「監視カメラ」にも例えられるものであり，情報セキュリティ対策基準上は，定期的に又は適宜点検及び分析することも求められているが，最低限，ログを取得したうえでその旨を利用者に周知することにより「防犯カメラ」として機能させる必要がある。

さらに，情報システムを利用する職員に対して，①ログ管理は職員を疑う目的で行われるものではなく，情報の流出が生じた場合に，不正を行っていない職員が疑われないようにするためのものでもあること，②そのためにも識別コード及びパスワードは適切に管理する必要があることを認識させる必要がある。

(ｲ) 全庁調査の結果

各所属で管理する情報システムについての回答は，次のとおりであった。

なお，本調査の実施後，個人情報の流出事案の発生を受けて，市長部局において，情報システムの管理状況に係るチェックシートに基づく点検が実施され

---

[1] 識別コード（利用者を識別するために情報システムが認識する記号）を登録したカードのこと。

[2] 独立行政法人情報処理推進機構が，2015 年に発生し，社会的に影響が大きかったと考えられる情報セキュリティの脅威に関する事案から選出，発表した「情報セキュリティ 10 大脅威 2016」においても，組織における脅威のうち「内部不正による情報漏えい」は，「標的型攻撃による情報流出」に次いで２位とされている。

た。

a　個人情報の不正な持出しを防止する対策

⑻　サーバ等からの不正な持出しを防止する対策

情報システムのサーバ等（スタンドアロンの場合は，当該パソコン等）に記録媒体等の機器を接続して，個人情報データを外部に持ち出すことについて，スタンドアロンと回答があった情報システム以外については，概ね何らかの対策が取られている（①，②）と回答があったが，スタンドアロンと回答があった情報システムについては，可能な状態であると回答があったものが，86.7%あった。

・　スタンドアロン以外

（単位:システム，%）

①不可能な状態にしている(機器の接続ができない状態にしている，暗号化等)	29	46.0%
②可能な状態であるが，対策を講じている(サーバ室への機器の持込み制限等)	15	23.8%
③可能な状態である	11	17.5%
④不明	8	12.7%
合計	63	100.0%

・　スタンドアロン

（単位:システム，%）

①不可能な状態にしている(機器の接続ができない状態にしている，暗号化等)	1	6.7%
②可能な状態であるが，対策を講じている(サーバ室への機器の持込み制限等)	1	6.7%
③可能な状態である	13	86.7%
④不明	0	0.0%
合計	15	100.0%

⑼　端末からの不正な持出しを防止する対策

スタンドアロンと回答があった情報システム以外のうち，可能な状態であると回答があったものが，41.3%あった。

・　スタンドアロン以外

（単位:システム，%）

①不可能な状態にしている(機器の接続や情報出力ができない状態にしている，暗号化等)	15	23.8%
②可能な状態であるが，対策を講じている(ログの定期点検等)	20	31.7%
③可能な状態である	26	41.3%
④不明	2	3.2%
合計	63	100.0%

b　ＩＤ（識別コード）及びパスワードの管理等

⑷　利用者個人ごとの利用者認証機能の設定

情報セキュリティ対策基準に従い，利用者個人ごとにＩＤ等を設けていると回答があったものは41.0%であり，共用のＩＤ等を設けていると回答があったものが51.3%，ＩＤ等による管理を行っていないと回答があったものが7.7%あった。

なお，利用者個人ごとのＩＤ等を設けていない（②，③）と回答があったシステムのうち，業務上必要な者以外の利用を防止するための何らかの対策（端末の施錠管理等）がされていると回答があったものは，73.9%であった。

（単位：システム，%）

①利用者個人ごとにIDやパスワードを設けている	32	41.0%
②共用のIDやパスワードを設けている	40	51.3%
③IDやパスワードによる管理を行っていない	6	7.7%
合計	78	100.0%

⑸　パスワードの定期的な変更等

パスワードの変更や，パスワードに一定以上の文字数や文字種を使用することについて，情報システム上の制限や利用者への周知を行っていないとの回答が，52.6%あった。

（単位：システム，%）

①情報システム上，定期的な変更や，一定以上の文字数や文字種の使用をしないといけない制限を加えている	22	28.2%
②情報システム上の制限はないが，利用者に変更などを行うよう周知している	15	19.2%
③特に行っていない（パスワードを設けていない場合を含む。）	41	52.6%
合計	78	100.0%

c　管理者権限の管理

情報セキュリティ対策基準においては，管理者権限を持つ識別コードは，担当職務又は職責に即して必要最低限の者に付与することとされており，管理者権限に係る回答は次のとおりであった。

なお，利用者本人のみが管理者権限を付与されており，その登録・変更・抹消等も行える（下記⑷，⑸とも③のみ）と回答があったものが 3.8%，委託事業者のみが行える（下記⑷，⑸とも④のみ）と回答があったものが12.8%あった。

⑷ 管理者権限が付与されている者（複数回答）

（単位：システム，％）

①課長等	10	12.8%
②利用者としての権限のない係長や主管課職員等	14	17.9%
③利用者本人	13	16.7%
④委託事業者	19	24.4%
⑤その他	7	9.0%

注　管理者権限の設定がないなどの 30 システムを含むため，合計 100％未満となる。

⑸ 管理者権限を付与する（登録・変更・抹消等を行う）ことができる者（複数回答）

（単位：システム，％）

①課長等	10	12.8%
②利用者としての権限のない係長や主管課職員等	14	17.9%
③利用者本人	8	10.3%
④委託事業者	19	24.4%
⑤その他	10	12.8%

注　管理者権限の設定がないなどの 29 システムを含むため，合計 100％未満となる。

d　ログの管理

⑷ ログの取得や保存の状況

ログの取得や保存は，情報の漏えい等が発生した場合の原因を調査，特定するために有効であるが，行っていないと回答があったものが，47.4％あった。

（単位：システム，％）

①行っている	41	52.6%
②行っていない	37	47.4%
合計	78	100.0%

⑸ 情報の漏えい等が発生した場合の原因を調査，特定する方法

ログの取得や保存を行っていないと回答があったシステムのうち，情報の漏えい等が発生した場合の原因を調査，特定する方法がないと回答があったものが，78.4％あった。

（単位：システム，％）

①ある	8	21.6%
②ない	29	78.4%
合計	37	100.0%

⑹ 情報システムの利用者への周知の状況

ログの取得等については，情報の漏えい等が発生した場合の原因の調査

等に利用できるだけでなく，ログの取得等を行っていることを情報システムの利用者に周知することにより，不正利用の抑止効果も期待できるものである[1]が，ログの取得や保存を行っていると回答があったシステムのうち，周知を行っていないと回答があったものが，41.5%あった。

（単位:システム，%）

①行っている	24	58.5%
②行っていない	17	41.5%
合計	41	100.0%

(d) ログの点検や分析の状況

ログの取得や保存を行っていると回答があったシステムのうち，取得したログの点検や分析を行っていると回答があったものは，36.6%にとどまった。

（単位:システム，%）

①行っている	15	36.6%
②行っていない	26	63.4%
合計	41	100.0%

なお，ログの取得や保存を行っていると回答があったシステムの，ログの点検や分析の状況及び周知の状況をまとめると，以下のとおりである。

（単位:システム，%）

点検や分析，周知を行っている	12	29.3%
点検や分析を行っているが，周知を行っていない	3	7.3%
点検や分析を行っていないが，周知を行っている	12	29.3%
点検や分析，周知を行っていない	14	34.1%
合計	41	100.0%

エ　実地調査の結果等

(ア) サーバ等の施錠管理等はされていたが，サーバ等に保存されている情報を端末から出力して持ち出すことについては，十分な対策が取られていなかったもの（ログを取得する機能はあったが使用していなかったものや，一部の操作についてログを取得する機能が設けられていないものなど）があった。

(イ) 閲覧や操作の権限が，担当業務ごとに設定されていなかったものがあった。

(ウ) 複数の情報システム間で同一のパスワードを使用していたものや，初期パス

[1] 独立行政法人情報処理推進機構「組織内部者の不正行為によるインシデント調査」（平成24年7月）によれば，一般企業の社員3,000人にアンケート調査を実施した結果，「内部不正防止効果が期待できる対策」として最も多かった回答は「社内システムの操作の証拠が残る（54.2%）」であったとされている。

ワードを変更していなかったものがあった。

⑸ 外部からの攻撃（標的型攻撃等）に対する対策

ア 規程等の状況

(ｱ) 情報セキュリティ対策基準

a ネットワーク管理基準

情報システム業務責任者（情報システムの主管課の課長等）は，次のことを行わなければならない。

⒜ ネットワークの構築や構成の変更を行うときは，あらかじめ情報セキュリティ統括者（情報化推進室長）の承認を得たうえで（同管理基準第３条第２項），不正アクセス行為[1]等の事故を防止するために必要な措置を講じる（同管理基準第４条）。

⒝ 所管する情報システムを外部ネットワーク[2]に接続するときは，情報セキュリティ統括者（情報化推進室長）が許可した場合を除き，イントラネットを経由させる（同管理基準第９条第１項）。

⒞ 所管する情報システムの態様に応じ，不正侵入等に関する監視を行う（同管理基準第12条第１項）。

⒟ 不正アクセス行為を防止するため，ハードウェア及びソフトウェアに係る修正プログラムを速やかに適用する（同管理基準第13条第１項）。

b ネットワーク利用基準

⒜ 職員は，インターネットを利用するに当たり，情報セキュリティ統括者（情報化推進室長）が許可した情報システムを利用する場合を除き，イントラネットを経由して接続しなければならない（同利用基準第６条）。

⒝ 職員は，情報セキュリティ統括者（情報化推進室長）が許可した場合を除き，個人情報等を，インターネットを介して送信し，又は，送信可能な状態にし，若しくは受信するよう仕向けてはならない（同利用基準第７条第１項）。

c コンピュータウイルス等の脅威に関する対策基準

⒜ 情報システム業務責任者は，所管する情報システムの機能上及び運用上

---

[1] 不正アクセス行為の禁止等に関する法律第２条第４項に規定する不正アクセス行為（通信回線を通じて，本来自分が利用する権限を持っていない情報システムを利用する行為など）のこと（同管理基準第４条）。

[2] インターネット等の本市が管理していないネットワークのこと（同管理基準第２条）。

必要となる脅威[1]に関する対策（コンピュータウイルス[2]の感染防止等）を実施しなければならない（同対策基準第５条）。

⑹ コンピュータウイルス対策ソフト[3]が導入されている情報システムを利用する職員は，常時監視機能[4]及び定期検索機能[5]を用いて，コンピュータウイルスの検索を実施しなければならない（同対策基準第７条第１項）。

⑹ 情報システム又は電子計算機を利用する職員は，外部記録媒体の持込み及び持出しに際し，コンピュータウイルスの検索を実施しなければならない（同対策基準第７条第４項，第９条）。

⑹ 職員は，脅威による被害を防止するため，次のことを実施しなければならない（同対策基準第 11 条）。

- 不審な電子メールは，添付ファイルを開かず速やかに削除する。
- 情報システム業務責任者（情報システムの主管課の課長等）及び情報セキュリティ担当者（課長等）の許可なく，電子計算機等にソフトウェアを導入しない。
- 情報システム業務責任者（情報システムの主管課の課長等）及び情報セキュリティ担当者（課長等）が提供する情報を常に確認し，指示される対策を実施する。

⑷ イントラネット利用の手引

個人情報等の非公開情報が含まれたファイルを保存する場合は，必要に応じて暗号化（パスワードの設定等）をする。

なお，日本年金機構において個人情報の流出事案が発生したことを受け，平成 27 年６月には，電子メールの開封に関する注意事項と共に，暗号化の実施について改めて通知がされている。

---

[1] コンピュータウイルス（次の脚注参照）や不正アクセスなどの，情報システムの正常な運用を妨げる要因のこと（同対策基準第２条第２号）。

[2] 電子計算機に保存した電子情報の流出等の被害を起こす目的で作成された悪質なプログラムのこと（同対策基準第２条第２号）。

[3] コンピュータウイルスの感染を防止するため及び感染したコンピュータウイルスを除去するためのソフトウェアのこと（同対策基準第２条第５号）。

[4] 電子計算機内を常時監視し，コンピュータウイルスを検出する機能のこと（同対策基準第２条第７号）。

[5] あらかじめ登録された日時に自動的に電子計算機内を検索し，コンピュータウイルスを検出する機能のこと（同対策基準第２条第８号）。

イ　運用の状況

次のとおり，全庁共通の情報システムについては，情報セキュリティ対策基準に則った機能等が設けられている。

(ｱ)　住民記録，税，福祉等の基幹業務に係る情報システムのうち，大型汎用コンピュータで運用しているもの

a　ネットワークをインターネットと論理的に分離している。

b　コンピュータウイルス対策ソフトの導入及び定期的なウイルス定義ファイル[1]の更新を行い，コンピュータウイルスの感染を防止している。

c　上記ア(ｲ)の通知に基づき，情報化推進室で出力する電子データの受渡しに当たっては，原則として全てのファイルにパスワードを設定し暗号化を行うことを関係課等に通知している。

(ｲ)　イントラネット

a　予防的対策

(a)　コンピュータウイルス対策

コンピュータウイルス対策ソフトの導入及び定期的なウイルス定義ファイルの更新を行い，コンピュータウイルスの感染を防止している。

(b)　電子メールの利用に係る対策

イントラネットパソコンのコンピュータウイルス対策ソフトとは別に，自動的にコンピュータウイルス等を検知し，イントラネットに到達する前に電子メールを削除するシステムを導入している。

(c)　セキュリティホール対策等

・　イントラネットパソコンで使用されているソフトウェアのプログラム上の欠陥（セキュリティホール）を利用した攻撃に対応するため，随時，各パソコンに対して，修正プログラムを自動的に配布している。

・　修正プログラムの提供等のサポートが終了したソフトウェアを導入しているパソコンについては，イントラネットへの接続を停止している。

(d)　インターネット上のホームページの利用に係る対策

インターネット上のホームページの閲覧を制限するシステムを導入して

[1] コンピュータウイルスに感染したファイルの特徴等を収録したファイルをいい，コンピュータウイルス対策ソフトがコンピュータウイルス等を検出するのに用いる。パターンファイルともいう。

おり，閲覧することでコンピュータウイルスに感染するおそれがあるホームページ等については閲覧が制限されるほか，上記(b)以外の電子メール（ＷＥＢメール）の使用や，許可されていないソフトウェアのダウンロードなども制限される。

b　コンピュータウイルスに感染した場合等の対策

(a)　コンピュータウイルスの感染の有無等の監視に加え，定期的に，パソコン本体のコンピュータウイルスの検索が自動的に行われている。

(b)　外部からの不審な通信等を検知，遮断するシステムを導入したうえで，外部事業者による常時監視を行っている。

(c)　平成28年度には，情報セキュリティ対策の更なる強化を図るため，年々巧妙化する標的型攻撃への対策として，外部への情報漏えいを防止するため，イントラネットから外部に通信する際のログの常時監視の導入等が予定されている。

ウ　全庁調査の結果等

(ｱ)　各所属において必要とされている主な対策

a　イントラネット

(a)　予防的対策

・　不審な電子メールの開封等はしないことを職員に周知する。

(b)　コンピュータウイルスに感染した場合の対策

・　感染が疑われる場合はＬＡＮケーブルを抜き，課長等及び情報化推進室に連絡するよう，あらかじめ職員に周知する。

・　機密を要する情報には必要に応じてパスワードを設定することを徹底する。

・　パスワードの文字数，使用する文字種及び管理方法について，外部からの攻撃を考慮したものとする。

b　その他の情報システム等

外部ネットワークに接続するときは，原則として，上記イ(ｲ)の対策がなされているイントラネットを経由させることとなる。

・　所管する情報システムについて，ネットワークの構築や構成の変更，外部ネットワークへの接続を行うときは，あらかじめ情報セキュリティ統括

者（情報化推進室長）の承認又は許可を得る。

・　所管する情報システムの態様等に応じて，必要な対策を行う。

(ｲ)　全庁調査の結果

a　イントラネット

(a)　電子メールの使用（受信した電子メールの確認を含む。）

各所属における電子メールの使用状況は，以下のとおりであり，89.2%の所属が，電子メール（所属用又は個人用メールアドレス）を使用する機会があると回答した。

所属用メールアドレス（課の代表アドレス）　（単位：所属，%）

①使用することがある	177	49.2%
②使用することがない	61	16.9%
③所属用メールアドレスがない	119	33.1%
無回答	3	0.8%
合計	360	100.0%

個人用メールアドレス　（単位：所属，%）

①使用することがある	320	88.9%
②使用することがない	36	10.0%
③把握していない	1	0.3%
無回答	3	0.8%
合計	360	100.0%

(b)　電子メールの開封に関する注意喚起

96.1%の所属が，今年度に入ってから何らかの周知を行った（①，②）と回答したが，口頭による質問調査では，電子メールを使用する職員が，具体的な攻撃の手法（関係団体からの連絡に偽装するなど）や，コンピュータウイルスの感染が疑われる場合の対応を十分に認識していない事例も見られた。

（単位：所属，%）

①情報化推進室等からの通知等をイントラネットパソコンを利用する全職員に転送や回覧，周知を行った	234	65.0%
②（①に加え）課内会議等を通じて周知，指導した	112	31.1%
③していない	3	0.8%
④分からない	1	0.3%
無回答	10	2.8%
合計	360	100.0%

(c)　必要に応じた暗号化の実施（パスワードの設定等）

・　個人情報を含むファイルの暗号化の実施状況

イントラネット（パソコン本体又はファイル共有システム（ドックサーブ））に保存している個人情報を含むファイルについて，一部を含

め暗号化を行っている（①，②）と回答した所属の割合は，68.6%であったが，全てのファイルについて暗号化を行っていると回答した所属の割合は，9.6%にとどまった。

（単位：所属，%）

①行っている	28	7.8%	9.6%
②行っていないものがある	173	48.1%	59.0%
③全く行っていない	92	25.6%	31.4%
④個人情報を保存していない	60	16.7%	－
不明又は無回答	7	1.9%	－
合計	360	100.0%	100.0%

・　暗号化についての所属のルールの有無

どのような情報を暗号化するかについての所属のルールがあると回答した所属の割合も，9.2%であった。

（単位：所属，%）

①ある	27	7.5%	9.2%
②ない（各担当者の判断による）	265	73.6%	90.8%
③個人情報を保存していない	60	16.7%	－
不明又は無回答	8	2.2%	－
合計	360	100.0%	100.0%

・　暗号化の方法の認知度

61.3%の所属において，個人情報が含まれたファイルを取り扱う職員の一部又は全員が，ファイルの暗号化の方法を知らなかった（②，③）と回答があった。実地調査においては，使用のつど，パスワードが設定された圧縮ファイルを別に作成している事例も見られた。

（単位：所属，%）

①全員知っていた	113	31.4%	38.7%
②一部知っていた	169	46.9%	57.9%
③全員知らなかった	10	2.8%	3.4%
④個人情報を保存していない	60	16.7%	－
不明又は無回答	8	2.2%	－
合計	360	100.0%	100.0%

b　その他の情報システム等

(a)　コンピュータウイルス対策及びセキュリティホール対策

コンピュータウイルス対策ソフト及びウイルス定義ファイルの更新並びに修正プログラムの適用がされていると回答があった情報システムは，50.0%にとどまった。

また，分からないとの回答も9.0%あった。

（単位：システム，％）

①されている	39	50.0%
②されていない	32	41.0%
③分からない	7	9.0%
合計	78	100.0%

エ　実地調査の結果等

(ｱ)　非公開情報が含まれたファイルは，必要に応じて暗号化（パスワードの設定等）をすることとされているが，個人情報を含むファイルの保存や暗号化（パスワードの設定等）等について，業務を所管する課等から統一的な取扱いが示されておらず，暗号化がされていなかったものがあった。

(ｲ)　外部記録媒体の持込み及び持出しに際し，コンピュータウイルスの検索を実施していなかったものがあった。

⑹ 個人情報取扱事務の委託

ア 規程等の状況

(ｱ) 個人情報保護条例等

ａ 個人情報取扱事務の委託に伴う措置（個人情報保護条例第 13 条）

個人情報取扱事務を委託しようとするときは，当該個人情報を保護するために必要な措置(委託事業者選定時の調査,委託契約書への必要事項の明記,履行中の監督等）を講じなければならない（同条第１項，個人情報保護条例の趣旨及び運用)。

ｂ 個人情報取扱事務の委託契約書における規定事項（ひな型）

個人情報取扱事務を委託する場合の委託契約書に掲げる事項については,情報化推進室作成の「電子計算機による事務処理等の委託契約に係る共通仕様書」及び行財政局財政部契約課作成の「財務会計基礎研修「契約事務」テキスト」を参照するほか，当該規定事項の必要性についても十分検討することとされている。

(ｲ) 情報セキュリティ対策基準等

ａ 情報システムの委託に関する管理基準

①情報システムに関する開発，保守等及び②電子計算機による情報の入出力処理等に係る委託について，契約書又は仕様書の記載事項等が定められている。

ｂ 電子計算機による事務処理等の契約に係るガイドライン

契約に際しての留意事項及び手続が示されており，委託契約書には，情報セキュリティ対策基準等の規定を受けて定められた「電子計算機による事務処理等の委託契約に係る共通仕様書」を添付することとされている。

イ 全庁調査の結果等

(ｱ) 全庁調査の結果

ａ 個人情報取扱事務の委託の状況

委託事務の中に個人情報が含まれるものがある（個人情報取扱事務の委託を行っている）と回答した所属の割合は，23.9％であった。

（単位：所属，％）

①ある	86	23.9%
②ない	268	74.4%
無回答	6	1.7%
合計	360	100.0%

b　個人情報取扱事務に係る委託の内容（複数回答）

個人情報取扱事務の委託を行っていると回答した所属の委託事務の内容については，次のとおり回答があった。

（単位：所属，％）

①システムや機器等の開発，保守等	34	39.5%
②データ入力等	42	48.8%
③通知等の封入，封かん	26	30.2%
④印刷（名簿など個人情報を含む内容）	25	29.1%
⑤配送（宛先リストの貸出しや提供）	22	25.6%
⑥調査やイベントその他の委託	34	39.5%
⑦その他	21	24.4%

注　委託事務の中に個人情報が含まれるものがあると回答した86所属に占める割合

c　委託事業者の個人情報の取扱状況についての確認

個人情報取扱事務の委託を行っていると回答した所属のうち，委託事業者の個人情報の取扱状況を確認していないものがある，又は確認していない（②，③）と回答した所属の割合が，合計で19.8％であった。

（単位：所属，％）

①している	69	80.2%
②していないものがある	10	11.6%
③していない	7	8.1%
合計	86	100.0%

ウ　実地調査の結果等

(ｱ)　委託契約書に「電子計算機による事務処理等の委託契約に係る共通仕様書」が添付されていないものがあった。

なお，行財政局財政部契約課は，年間契約依頼についての各局等への通知文に，該当する契約には当該仕様書を添付するよう記載している。

3　研修や自己点検の機会の有効利用

⑴　規程等の状況

ア　文書管理

㋐　公文書取扱規程

ａ　情報化推進室情報管理課長は，随時，文書管理所属（課等）の文書処理状況を調査することができる（同規程第56条第１項)。

ｂ　文書管理統括者（局及び区にあっては庶務を担当する課長，会計室にあっては次長）は，随時，局区等における文書処理状況を調査することができる。調査を行った場合は，その結果を情報化推進室情報管理課長に報告しなければならない（同規程第56条第２項)。

イ　情報セキュリティ対策基準等

㋐　情報セキュリティ教育実施基準

ａ　情報セキュリティ統括者（情報化推進室長）の責務

次の研修等を実施しなければならない(同実施基準第２条第１項，第３条)。

⒜　新規採用職員を対象とする研修

⒝　職員に対する定期的な研修及び啓発

⒞　情報システム業務責任者（情報システムの主管課の課長等）に対する研修（情報システムの管理方法，職員の指導監督の方法等）

⒟　情報セキュリティ担当者（課長等）に対する研修（情報システムの管理方法，職員の指導監督の方法等）

ｂ　情報システム業務責任者（情報システムの主管課の課長等）の責務

⒜　情報システムを安全に運用するための具体的な手順書を策定し，利用者に周知するとともに，情報セキュリティ統括者（情報化推進室長）に内容を報告する（同実施基準第６条第１項）。

⒝　必要な知識を維持するために，情報セキュリティ統括者（情報化推進室長）が実施する研修を受講する（同実施基準第５条第１項）。

⒞　職員に対して，必要に応じて情報提供，研修等を実施する(同条第２項)。

ｃ　情報セキュリティ担当者（課長等）の責務

⒜　必要な知識を維持するために，情報セキュリティ統括者（情報化推進室長）が実施する研修を受講する（同実施基準第５条第１項）。

⑹ 職員に対して，必要に応じて情報提供，研修等を実施する（同条第２項）。

(ｲ) 情報セキュリティに関する点検及び監査実施基準

a 自主点検

⑻ 情報システム業務責任者（情報システムの主管課の課長等）による点検

所管する情報システムの取扱いについて，情報セキュリティ対策基準等の遵守状況を点検し（同実施基準第２条第１項），その結果を情報セキュリティ統括者（情報化推進室長）に報告しなければならない（同条第４項）。

⑹ 情報セキュリティ担当者（課長等）による点検

課等で利用する情報システムやスタンドアロンパソコンの取扱いについて，情報セキュリティ対策基準等の遵守状況を点検し（同実施基準第２条第２項），その結果を情報セキュリティ統括者（情報化推進室長）に報告しなければならない（同条第４項）。

b 内部監査

情報セキュリティ統括者（情報化推進室長）は，情報セキュリティ対策基準等の遵守状況及び情報システムの安全性を確認するため，定期的に監査を実施しなければならない（同実施基準第３条第１項）。

c 外部監査

次の事項は，職員による監査とは別に，定期的に専門的な知識及び技術を有する外部団体に委託して実施する（同実施基準第５条）。

⑻ 情報システムの安全性に関する技術的検証

⑹ 第３条（内部監査）に掲げる事項

d 監査結果の報告

情報セキュリティ統括者（情報化推進室長）は，監査の結果を定期的に統括責任者（総合企画局プロジェクト・国際化・情報化担当局長）に報告しなければならない（同実施基準第６条）。

(ｳ) 情報システムの適正な利用等に関する規程

a 情報セキュリティ対策基準の見直し

統括責任者（総合企画局プロジェクト・国際化・情報化担当局長）は，情報セキュリティ対策の実施状況等を踏まえ，必要があると認めるときは，情報セキュリティ対策基準の見直しを行わなければならない（同規程第 19 条）。

⑵ 運用の状況

ア 研修の実施状況

平成26年度に実施された,個人情報保護制度又は情報セキュリティに係る内容が含まれる研修は次のとおりである。

研修名	対象者	研修科目	参加人数
新規採用職員研修	新規採用職員	個人情報保護制度 情報セキュリティ	(指名制)
基本理念研修	①採用後２年目職員 ②希望又は推薦する主任級以下の職員	個人情報保護制度 情報セキュリティ	(①は指名制)
新任課長級職員研修	新任課長級職員	情報セキュリティ	(指名制)
情報化推進支援員研修	各所属で選任された情報化推進支援員	個人情報保護制度 情報セキュリティ	(指名制)
コンプライアンス推進月間及び情報セキュリティ対策強化月間に係る研修	①局区等の服務を担当する課長（原則受講） ②課長級職員（希望制） ③各局区等において推薦する職員	個人情報保護 情報セキュリティ	79名 (注)
ｅラーニングによる情報セキュリティ研修	希望者	個人情報保護 情報セキュリティ	各コース 11～62名 (注)

注　監査対象外の局等の受講人数を含む。

なお，平成27年度は上記に加え，社会保障・税番号（マイナンバー）制度に係る所属長研修が実施された。

(ｱ) 新規採用職員研修

行財政局人材育成推進室[1]（以下「人材育成推進室」という。）が主体となり，新規採用職員を対象に実施している。公務員としての基本理念と職員としての基礎的な知識を習得することを目的としている。平成26年度は４月１日から21日にかけて実施されている。

(ｲ) 基本理念研修

人材育成推進室が主体となり，採用後２年目職員は指名制，その他の主任級以下の職員は希望・推薦制により実施している。平成26年度は平成27年１月に実施されている。

[1] 平成28年４月１日付けで人事部に統合した。

(ｳ) 新任課長級職員研修

人材育成推進室が主体となり，新任課長級職員を対象に実施している。課等の運営の責任者として，必要な知識を習得することを目的としている。平成 26 年度は４月下旬から６月初旬にかけて３日間にわたり実施されている。

(ｴ) 情報化推進支援員研修

情報化推進室が主体となり，各所属において，情報セキュリティ担当者を補佐するために選任された情報化推進支援員を対象に実施している。平成 26 年度は６月 25 日に実施されている。

(ｵ) コンプライアンス推進月間及び情報セキュリティ対策強化月間に係る研修

後述するコンプライアンス推進月間及び情報セキュリティ対策強化月間の取組の一環として，行財政局コンプライアンス推進室（以下「コンプライアンス推進室」という。）及び情報化推進室が，課長級職員のうち受講を希望する者等を対象に実施している。平成 26 年度は 11 月７日に実施されている。

(ｶ) ｅラーニング[1]による情報セキュリティ研修

地方公共団体情報システム機構[2]が地方公務員を対象に実施しており，受講を希望する職員は受講可能となっている。情報セキュリティ担当者（課長等）をはじめ，情報化推進支援員や個人情報を取り扱う事務に従事する職員は，可能な限り受講するよう，情報化推進室から各局等に依頼している。

イ コンプライアンス推進月間及び情報セキュリティ対策強化月間の取組

情報セキュリティ対策の重要性や，電子情報を含む個人情報の適切な取扱いを再確認するため，「情報セキュリティ対策強化月間」が実施されており，効果的かつ効率的な取組とするため，平成 23 年度から「コンプライアンス推進月間[3]」と同時期に実施されている。８月から９月までを実施期間とし，平成 26 年度は８月１日付けで取組の依頼を行っている。

主な取組内容は，次のとおりである。

---

[1] インターネットを利用した研修システムのこと。
なお，同研修はイントラネットパソコンでの受講ができる。

[2] 平成 26 年４月１日設立。根拠法は地方公共団体情報システム機構法。地方公共団体が運営する組織として，住民基本台帳法，公的個人認証法（電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律）及び番号法の規定による事務，地方公共団体の情報システムに関する支援等を行う。

[3] 職員一人一人がコンプライアンスに関する理解を深め，不祥事の根絶に向け構築してきた仕組みや制度の運用状況を再点検することにより，コンプライアンスの一層の定着を図るために実施している。

(ｱ) チェックシートに基づく点検

a 所属長による点検

所属における不適切な事務処理や不祥事の発生につながるリスクを回避するため，業務管理等に係る基本的な制度やルール，日常業務における必須の確認事項について，チェックシートにより，所属長自らが点検する。

b 所属職員による点検

自らの日常業務に関する基本的事項及び情報セキュリティに関する事項等について改めて点検するため,チェックシートにより,職員自らが点検し,点検した結果を所属長に提出する。

(ｲ) 職場ミーティングの実施

a 職場ミーティングテーマを題材とした意見交換

所属長は，テーマに基づく職場ミーティングを実施し，意見交換を行う。平成26年度は,複数のテーマから１つ以上のテーマを選択して実施することとされ，誤送付等の事務処理誤りの防止をテーマとして選択した所属は,76.8%であったとされている。

b 所属職員のチェックシートによる点検結果等に対する検討

所属長は，所属職員のチェックシートによる点検結果を踏まえ，所属職員ができていなかった事項等の改善に向けて，意見交換を行う。

(ｳ) 点検等の結果の報告

所属長によるチェックシートに基づく点検等の結果，改善を要する項目については，コンプライアンス推進室に改善措置を報告する。平成26年度は，全ての項目に問題なしとした所属長等の割合が，31.6%であった。

また，職場ミーティングの実施結果をコンプライアンス推進室に報告する。

(ｴ) イントラネットパソコンに接続された外部機器の確認

情報漏えい等を防止するため，スマートフォンやＵＳＢメモリ等，許可を得ていない周辺機器の使用を情報化推進室において確認し，使用していた職員の所属長に注意喚起を行った。

ウ 自己点検の状況の確認等

(ｱ) コンプライアンス推進室において，業務監察として，チェックシートから抜粋した項目を含む所属長ヒアリング及び点検が実施されている。

(ｲ)　情報化推進室を中心として，特定個人情報に係る点検及び内部監査の実施が予定されている。

エ　その他の主な自己点検等の取組

平成 27 年度には，個人情報の流出事案の発生を受けて，12 月から１月にかけて，情報システムの管理状況に係るチェックシートに基づく点検が実施された。

なお，平成 23 年度までは，所属長によるチェックシートに基づく点検等に加え，ＷＥＢ及び情報システムに係るチェックシートに基づく点検が行われていた。

オ　その他の主な啓発等の取組

(ｱ)　イントラネットパソコンを利用して，情報漏えいやウイルス感染などの情報セキュリティ上の注意事項等をポップアップ画面で配信した。

(ｲ)　地方公共団体情報システム機構や総務省等からの注意喚起に係る情報提供等について，庁内メールで周知した。

(ｳ)　京都府が実施している標的型メールテスト[1]に参加し，総合企画局職員を対象として実施した。

⑶　全庁調査の結果等

ア　各所属において必要とされている主な対策

(ｱ)　個人情報管理責任者及び情報セキュリティ担当者等（各所属の課長等）

ａ　所属の職員が定期的に受講する必要がある研修は，各所属で選任された情報化推進支援員を対象とした研修のみであるため，当該研修の内容を所属内で有効活用する必要がある。

また，課長等自身を含む所属の職員が必要な知識を維持するためにも，希望制の研修の受講をはじめとした自主学習の機会を活用する必要がある。

ｂ　自己点検の機会については，全庁的に設けられているため，依頼文に沿って実施，報告する必要がある。

(ｲ)　情報システム業務責任者（情報システムの主管課の課長等）

ａ　運用手順書の策定等により，各情報システムの運用に係る具体的な事項を周知する必要がある。

ｂ　情報システムの主管課における運用管理等については，全庁的な研修及び点

[1] 特定の組織内の情報を狙った攻撃の一種である標的型メールを模擬的に職員に送付し，適切な対応を取れるようにするための訓練のこと。

検の機会はないため，課長等自身を含む情報システム担当職員が必要な知識を習得，維持するための手段を設け，点検の機会を確保する必要がある。

イ　全庁調査の結果

(ｱ)　個人情報管理責任者及び情報セキュリティ担当者等（各所属の課長等）

a　研修内容の所属内での伝達状況

毎年度，各所属から職員が受講することとされている情報化推進支援員研修の内容について，所属内での伝達をしていないとの回答も18.9%あったが，77.2%の所属は，何らかの方法で伝達を行った（①，②，③）と回答した。

なお，平成27年度情報化推進支援員研修では，日本年金機構の個人情報流出事案や，特定個人情報の取扱いなどの新たな内容も盛り込まれている。

（単位：所属，%）

①研修資料の配布や回覧を行った	242	67.2%
②（①に加え）伝達研修を実施した	19	5.3%
③他の方法で周知や対応を行った	17	4.7%
④していない	68	18.9%
無回答	14	3.9%
合計	360	100.0%

b　個人情報の取扱いや情報セキュリティに関する知識を得る方法（複数回答）

主に通知等により得ていると回答した所属の割合が，94.2%であった。

庁内メールによる照会回答という形式で行われるチェックシートによる点検が，一定の知識を得る機会としての機能も果たしているともいえるが，基本的には，不適切な事案の発生に伴う通知等によりその都度知識を得ており，研修や自主学習で改めてまとまった知識を得る機会がない者がいるといえる。

（単位：所属，%）

①庁内向け研修	223	61.9%
②庁内メール等による通知や周知	339	94.2%
③自主学習（希望制のeラーニング研修，イントラネットホームページの資料，一般書籍など）	57	15.8%

c　所属内での指導の状況（複数回答）

所属内での指導について，主にコンプライアンス推進月間及び情報セキュリティ対策強化月間におけるチェックシートによる点検の取組を通じて行っていると回答があった割合が，83.3%であった。

（単位：所属，％）

①チェックシート（所属職員向け）を配布することで指導している	300	83.3%
②別の機会や方法で適切な取扱いについて指導（周知）している	91	25.3%
③実際の取扱いについて目視点検等を行っている	77	21.4%

(ｲ) 情報システム業務責任者（情報システムの主管課の課長等）

所管する情報システムに係る研修及び点検等の実施状況についての回答は，次のとおりであり，各情報システムの取扱いについて，個別の管理基準やマニュアル等により必要な情報を伝達する手段や，定期的な点検の機会を設けていないと回答したものがあった。

a 情報システムの管理に係る周知の方法

情報システムの管理に係る情報セキュリティ対策基準の周知（所属内での情報共有や担当者間での引継ぎ）の方法について，何らかの方法で周知している（①，②）と回答があった割合は，65.4％であった。

（単位：システム，％）

①情報セキュリティ対策基準自体を周知している	43	55.1%
②情報システム個別の管理基準や管理マニュアルが情報セキュリティ対策基準を満たしている	8	10.3%
③特に周知していない	27	34.6%
合計	78	100.0%

b 端末の利用者に対する情報セキュリティに関する研修の実施状況

情報セキュリティに関して，端末の利用者に対する研修を行っておらず，操作マニュアル等にも記載していないとの回答が，35.9％あった。

（単位：システム，％）

①行っている	28	35.9%
②行っていないが操作マニュアル等に記載している	22	28.2%
③行っていない	28	35.9%
合計	78	100.0%

c 情報システムの取扱いについての点検の実施状況

情報システムの取扱いに関して，個人情報保護や情報セキュリティの観点からの点検を行っていないと回答したものが，34.6％あった。

（単位：システム，％）

①定期的に行っている	15	19.2%
②定期的にではないが行っている	36	46.2%
③行っていない	27	34.6%
合計	78	100.0%

第４　意見

個人情報を取り扱う全庁共通の情報システムについては，「第３　調査の結果」に掲げたように，情報セキュリティ上の高い技術的対策がされていた。

さらに，平成 27 年度２月補正予算においては，新たな自治体情報セキュリティ対策の抜本的強化として，国と各自治体間を繋いでいる行政専用のネットワークに接続している本市の情報システムのセキュリティをより一層向上させることにより，マイナンバーに係る情報セキュリティ対策にも万全を期すこととされている。

一方，各所属における対策については，情報セキュリティ対策基準等のルールは概ね整備されていたが，各所属の運用に問題があったものが一部に見受けられた。

個人情報保護，情報セキュリティ等のそれぞれのルールの徹底にとどまらず，個人情報に係る情報セキュリティの確保という観点からのルール等の整備が望まれる。

このため，今回の監査で発見された事項の是正にとどまることなく，全庁的な取組を求める。

１　個人情報の取扱いの開始時や情報システム等の導入時の対策

⑴　事務のＩＣＴ化等を踏まえた個人情報保護条例の運用の明確化及び周知等

個人情報保護条例上，個人情報取扱事務を開始する場合は，あらかじめ市長に届け出ることとされており，また，新たな電子計算機処理（処理の大幅な変更を含む。）や，法令に定めがない電子計算機の結合を行う場合は，あらかじめ個人情報保護審議会の意見を聴くこととされているが，解釈の誤り等により必要な手続が漏れ，不適切な取扱いが生じることがないよう，各所属においてどのような場合に手続が必要かが理解され，適切な取扱いがなされるよう，運用の明確化及び周知について検討されたい。

なお，各所属において，個人情報の処理方法や情報出力方法に応じた必要な個人情報保護対策がとられるよう，個人情報保護審議会の意見を聴くに当たり提出される審議票の記載事項についても，事務のＩＣＴ化等を踏まえた見直しが検討されることが望ましい。

⑵　個人情報を取り扱う情報システムに係る事前審査等の検討

現在，個人情報の取扱いの開始時のチェックと情報システムの導入時のチェック等はあるが，連動はしていないなど，個人情報を取り扱う情報システムの導入という観点からの事前審査等は行われていない状況にあるため，既にある仕組みも活用

し，個人情報を取り扱う情報システムの導入や改修に当たり，情報セキュリティ対策基準の遵守をはじめとした必要な対策がされる仕組みを検討されたい。

また，個人情報を取り扱う情報システムの設置状況について，全庁的な把握がされるよう検討されたい。

（参考１）個人情報保護，情報セキュリティ等に関する事前審査等の状況

１　個人情報保護条例等

・　電子計算機の結合（法令に定めがある場合を除く。）

実施機関（市長等）が，①個人情報保護審議会の意見を聴いたうえで，②公益上必要があり，かつ，③個人情報の保護に関し必要な措置が講じられていると認めるときに行えるものとされている。［実施機関内部において，必要な措置が講じられていると認めるための情報セキュリティ上の具体的な基準や手続は定められていない。］

・　電子計算機処理

新たに実施する場合は個人情報保護審議会の意見を聴くこととされている。［情報セキュリティ対策等についての審議を求めることはしていない。］

・　個人情報の電算処理等に係る審議票

個人情報保護審議会の運営要領で様式が定められており，電算処理面と運用面の個人情報保護対策の記入欄が設けられている。

事務手続マニュアルで審議票の作成ポイントが示されている。

［個人情報保護対策については，情報セキュリティ対策基準等を遵守することとして，各個人情報取扱事務を所管する課等や，情報セキュリティの所管部局に委ねている。］

２　情報セキュリティ対策基準

ネットワークの構築や構成の変更を行うときは，あらかじめ，必要な情報セキュリティ対策が講じられていることについて，情報セキュリティ統括者（情報化推進室長）の承認を得ることとされている。［上記１及び下記３とは異なり，定期的な提出依頼等は行われていない。］

３　情報システムの適正な利用等に関する規程

情報システムの開発等をするときは，情報システムを効果的かつ効率的に利用するため，高度情報化推進統括者（情報化推進室長）の審査を受けることとされている。［軽易な情報システムの開発は審査の対象外とされており，具体的には，原則として 500 万円以上の情報システムが対象とされている。］

（参考２）個人情報を取り扱う情報システムの設置状況の把握の状況

１　情報システム台帳

ＩＴガバナンスの強化の取組の一環として，各所属で所管している情報システムの概要，経費等を把握するために，個人情報の有無についても記入欄が設けられている台帳を作成している。［予算に経費が計上されている情報システム（情報システムの大部分を占める。）を対象としている。］

２　情報資産管理簿

電算処理業務の状況を記載することとされており，個人情報処理の有無についても記入欄が設けられている。［下記２⑵のとおり，更新が徹底されていないほか，全庁の最新の状況の把握はされていない。］

３　個人情報保護審議会承認案件に係る書類，個人情報取扱事務目録

情報システムの導入とそれ以外の電子計算機処理，情報システムの導入と改修等を区別せず，案件や事務等ごとに作成されている。

※　情報システムの適正な利用等に関する規程上の「情報システム」には該当するが，個人情報保護条例上の「電子計算機処理」には該当しないとされているものもある（ホームページ開発等）。

2　個人情報の取扱いに係る管理帳票の整備

⑴　個人情報を含むファイル等の管理方法の検討

台帳や名簿などの常用の公文書については，文書管理システムに簿冊の情報等を登録して管理することとされているが，徹底がされておらず，特定の情報システム以外のパソコン等に保存されている個人情報を含むデータや，個人情報を含む紙文書の一部が，組織的に管理されていない状況にある。

少なくとも個人情報を含むデータについては，その保存場所も含めて組織的に適正な管理がされるよう，各所属における事務効率も勘案して検討されたい。

⑵　情報資産管理簿の整備等

情報資産管理簿については，過年度の照会回答として取り扱われているなど，作成及び更新が徹底されていない状況にあった。

パソコンの管理については任意の帳票等で行われていた事例もあり，情報資産管理簿の整備が必要であることが十分に認識されていないことと同時に，所属で実務上管理したい内容（用途や情報システム別の管理，使用者，保管場所等）に対応していないことも考えられる。

情報資産の管理を徹底するとともに，必要な情報の更新が容易にでき，有効活用が図られるものとなるよう，様式の抜本的な見直しも含めて検討されたい。

また，庁舎等内の通信回線の敷設図，結線図等の文書についても，確実に整備及び保管がされるよう検討されたい。

⑶　個人情報保護審議会で承認を受けた対策の継続

個人情報取扱事務については作業マニュアルがあることが望ましいとされているほか，情報システムについては運用手順を定めて周知する必要があるが，具体的なマニュアル等を定めていない所属もあり，個人情報保護審議会で承認された内容が引き継がれるルールになっていない状況にある。

各所属において承認を受けた内容が把握され，個人情報保護に係る対策が継続されるよう，仕組みを検討されたい。

3　イントラネットパソコンの取扱い

⑴　暗号化の徹底等

平成 27 年度に，日本年金機構において，不正アクセスによる約 125 万件の個人情報流出事案が発生したことを受け，本市においてこのような事案を発生させること

のないよう，電子メールの取扱いに留意するほか，非公開情報が含まれたファイルを保存する場合は，必要に応じてパスワードを設定するなど，暗号化を実施するよう，改めて通知がされているが，個人情報が含まれたファイルにパスワードが設定されていないものが見受けられた。

「不正アクセスによる情報流出事案に関する調査結果報告」（平成 27 年８月 20 日日本年金機構不正アクセスによる情報流出事案に関する調査委員会）においても，情報流出につながったことの要因として，個人情報等の重要情報は共有ファイルサーバに保管しないことを原則とし，例外的に保管する場合にはパスワードを設定するなどの運用ルールはあったが，共有ファイルサーバがインターネット接続環境下に設置されているというリスク認識や，サイバーセキュリティの危機意識に欠けており，運用ルールが本当に実行されているかなどの点検・確認が行われていなかったことなどが構造的な問題として挙げられている。

本市のイントラネットは高い技術的対策がされているが，パスワードは「金庫の鍵」にも例えられるものであり，多層防御[1]の観点から暗号化は実施する必要がある。

不審な電子メールの開封等をしないことについて，外部からの攻撃の具体例や，開封等をした場合の対応も含めて周知徹底するとともに，非公開情報のうち少なくとも個人情報については暗号化が徹底されるよう，パスワード設定に係るルールの見直しも含めて，改めて早急に対策を講じられたい。

⑵ イントラネットパソコンでの取扱いを禁止する事項の見直し

現在，情報セキュリティ上の観点から，個人情報保護審議会に諮る必要がある個人情報の電子計算機処理をイントラネットパソコンで行うことは原則禁止されている[2]が，禁止する事項については，データの形式だけでなく，データの質（センシティブ情報であるかどうかなどの内容，漏えい時の影響等）に応じて判断されるべきである。

また，イントラネットパソコンでのデータの保存を禁止することで，日本年金機構の事案のような外部からの攻撃による流出のおそれは低下したとしても，技術的

---

[1] コンピュータウイルスへの感染予防だけでなく，感染することを想定して，感染後の被害の回避や低減のために，複数の対策を行うこと。

[2] なお，個人番号利用事務で用いる特定個人情報については，イントラネットパソコンで取り扱うことが禁止されている。

対策が不十分なスタンドアロンパソコン等を利用することになれば，堺市の事案のような職員の持出しによる流出のおそれは相対的に高まる。イントラネットパソコンでの取扱いを禁止する事項についての検討に当たっては，スタンドアロンパソコンや記録媒体に保存する場合のリスク（長所及び短所）や，ルールの実効性についても留意する必要がある。

以上のことを踏まえ，各所属での取扱状況を把握したうえで，実状に応じた新たなルール作りを検討されたい。

⑶ ファイル共有システムの適切な運用管理の促進

利用者権限の制御の観点から見た本市のファイル共有システム（ドックサーブ）の各フォルダの特性等は，次のとおりである。

個人フォルダ
イントラネット利用の手引：本人のみが中身を閲覧，保存，削除，編集することができる。
メリット：他の職員が閲覧できない。
デメリット：人事異動等により自動的にデータが他所属に持ち出される可能性がある。
データの管理状況を組織的に確認できない。
フリースペースフォルダ（所属ごとの共有フォルダ）
イントラネット利用の手引：同一の課等に所属する全ての職員がファイルの作成，更新，削除等を行うことができる。
課等において複数の職員が使用するデータ等を保存する。
メリット：人事異動等により自動的に当該所属の職員以外は閲覧できなくなる。
データの管理状況を組織的に確認できる。
デメリット：所属内の業務上必要がない職員も閲覧できる可能性がある。
（パスワード等の適正な管理が必要）

これらの特性等を踏まえ，情報システムの利用者権限の制御に準じて，所属ごとに一定の利用ルール（パスワード管理方法，異動時の整理，フォルダ階層の管理等）があることが望ましいと考えられる。

各所属におけるファイル共有システム（ドックサーブ）での適正な情報管理が促進されるよう，対策を講じられたい。

4 スタンドアロンパソコンの取扱い

スタンドアロンパソコンについては，情報セキュリティ担当者（課長等）が，必要な範囲において情報システムに係る規定に準じて利用者権限の管理等を行わなければならないとされており，ログ管理をはじめとした情報セキュリティ対策を講じるかどうかの判断が各所属に委ねられている。

情報システムと比べて，データの不正な持出しが比較的容易に行われるおそれがあ

るため，個人情報の管理に利用する所属において，対策の必要性が認識され，業務やデータの質等に応じて必要な対策がとられるような方策を検討されたい。

５　情報システム等に係る教育及び点検の充実

現在，全庁に共通する基幹業務システムの端末やイントラネットパソコンの取扱い，紛失や誤送付の防止等については，研修や通知等により繰り返し周知され，チェックシートによる定期的な自己点検も実施されているが，情報システムの主管課等を対象とした周知や教育は行われていない状況にある。

⑴　情報システムの運用管理に係る自己点検の継続

平成 27 年度には，個人情報の流出事案の発生を受けて，情報システムの管理状況について，チェックシートによる自己点検が実施された。

コンプライアンス推進月間及び情報セキュリティ対策強化月間に併せて今後も定期的に実施するなど，情報システムの運用管理に係る定期的な自己点検の機会の付与について検討されたい。

また，所属以外の者による自己点検の状況の確認についても検討されたい。

⑵　情報システムの取扱い等に係る教育

ア　情報システムの主管課等に対する教育

自己点検の実施をはじめとした情報システムの適正な取扱いの確保には，いわゆる意識啓発だけでなく，本市の情報セキュリティ対策基準を理解し，実践するために必要な知識の習得が不可欠である。

情報システムの管理運用を行う所属のほか，情報システムを導入する可能性のある所属や，スタンドアロンパソコンで個人情報を取り扱っている所属等に対する教育の実施について，ｅラーニングによる情報セキュリティ研修を業務研修と位置付けて受講させることや，マイナンバー制度に係る研修資料を活用することなど，既存の研修等の有効活用も含めて検討されたい。

なお，情報セキュリティ人材の不足は全国的な課題であり，平成 27 年 10 月には，組織の各部署内で情報セキュリティポリシーの運用等を行う人材の育成・確保のための新たな国家試験（情報セキュリティマネジメント試験）が創設されたところである。

資格制度等の活用に関して，行財政局総務部法制課においては，職員の政策法務能力の向上を図り，組織的な法務体制の構築に資することを目的として，研修

として自治体法務検定に係るテキストの配布及び受検の機会の提供を行っているほか，行財政局人事部人事課においては，資格取得支援制度を運用している。

本市におけるそれらの取組も参考として検討することが望ましい。

イ　情報セキュリティ担当者（課長等）等に対する教育

意識の向上には，日常業務に即したイメージを持ちやすくし，当事者意識を育むことが有効であると考えられる。

過去には「情報セキュリティニュース」の発行等，平易かつ具体的な表現による啓発の取組がされていた。同様の内容を繰り返し周知するなど，具体的なリスクや対策がより理解されやすいよう，庁内メールや情報化推進支援員研修を通じた意識啓発の有効性の向上について，引き続き検討されたい。

また，誤送付等の事務処理ミスに関しても，より具体的な事例やその再発防止策について，同一の業務を行う区等間での情報共有等が促進されるよう検討されたい。

なお，平成 26 年度の行政監査結果報告でも述べているように，イントラネットホームページの構成が複雑化しており，イントラネットホームページに掲載しているだけでは，各所属の職員が，手引や委託契約時に必要な情報等の存在に気が付かない場合も多いため，個人情報保護及び情報セキュリティに係る既存の情報についても積極的な周知を行われたい。

６　局が所管する情報に係るリスクを踏まえた取扱い

監査の実施期間中に，保健福祉局子育て支援部児童福祉センターにおいて，個人情報の流出事案が判明し，同センターで管理する情報システムが長期間にわたって規定違反の状態にあり，個人情報の漏えいを防止するために必要な措置が講じられていなかった（情報システムのうち共有フォルダについては，必要な閲覧制限等がされておらず，また，ログの取得機能も備えていなかった）ことが明らかとなった。

保健福祉局は，他の局等に比べ，個人情報を取り扱う情報システムの件数や，センシティブ情報の取扱件数が多いことから，所管するそれらの情報に係るリスクを踏まえた取扱いが求められる。

上記１から５までの意見の趣旨を踏まえ，保健福祉局において，総合企画局情報化推進室等とも連携し，次のとおり取り組まれたい。

⑴　情報システム

各情報システムにおいて，具体的にどのような情報出力・保存や閲覧の機能があり，それぞれの操作等に対して情報セキュリティ対策（ログの取得等）がされているか等について，設計書や運用手順書等により組織的に引き継がれ，専門的な知識や経験がない職員でも理解できるようになっているか，再確認をされたい。

また，必要に応じて局内の情報システムの実地点検も実施されたい。

⑵ 情報システム以外

次のとおり，局内の個人情報データの取扱いに係るリスク評価を実施されたい。

ア　イントラネットパソコンやスタンドアロンパソコンでの個人情報の取扱状況及び個人情報保護対策・情報セキュリティ対策の状況の洗い出しを行われたい。

イ　上記アの個人情報について，現状の本市のルール上許容されるかどうかにかかわらず，どのように取り扱うのが適当か（スタンドアロンパソコンのセキュリティの向上の必要性など）について，検討し，実行されたい。

なお，一定の個人情報保護対策がとられている状態が継続することが重要であるため，対策の実効性についても十分留意して検討されたい。

ウ　上記イの検討に当たり，現状の本市のルール上許容されるかどうかにかかわらず，イントラネットに常時保存することが適当でないと判断される情報については，リスクを勘案したうえで必要な当面の対策を講じたうえで検討を実施されたい。

⑶ 区役所及び区役所支所の福祉部及び保健部

いわゆる大区役所制の推進により，福祉事務所及び保健所（保健センター）が区に統合されるとともに，区等にもイントラネットパソコンが概ね一人一台配備され，また，各業務の情報システムの端末も業務ごとに複数台配備されているなど，事務の状況は大きく変わっている。

自己点検の結果の集約及び改善の取組等は，区等を単位として行われる体制となっているが，業務を統括する保健福祉局の各課等においても，各区等の事務の状況をヨコ並びで確認し，必要に応じて統一的な取扱いを示すなどの取組が必要である。

業務を統括する課等において，区等における事務の実状を踏まえたうえで，ファイル共有システム（ドックサーブ）等の統一的な取扱いルールを示す，情報システム導入前に使用していた記録媒体等の要否や適切な廃棄方法を指示するなどの取組

を行われたい。

特に，支援課，保護課及び支援保護課は，児童福祉センターと同様にいわゆるケース記録を取り扱う点で共通しているほか，支援課及び支援保護課は，業務を統括する課等が複数にわたっている。できるだけ所属内での管理がしやすいよう，紙台帳の元データの取扱いをはじめとして，一定の福祉事務所共通ルールを示すことについても検討されたい。

⑷　局としての管理体制

上記⑴から⑶までの状況を踏まえたうえで，児童福祉センターにおける情報流出事案の再発防止対策にとどまらず，局全体における取組として，継続的に情報システムにおける個人情報の取扱状況を把握し，情報セキュリティの確保がなされるよう，管理体制を整備されたい。

その際，局内の人材や既存のチェック制度，各所属を巡回する制度などを活用することを含めて検討されたい。

7　取組の全庁的な展開

上記６で述べた事項については，他の局等にも共通するものであることから，保健福祉局をはじめ各局等の改善に向けた今後の取組や，既に実施している取組のうち，共有可能なものについては，総合企画局において全庁的な展開を図り，各局等の責任で実施すべき対策を明確化するなど，個人情報に係る情報セキュリティの確保に向けた取組の促進に努められたい。

第５　結び

１　全庁的な運用管理体制及び人材育成

⑴　情報通信技術（ＩＣＴ）が社会基盤として必要不可欠のものとなると同時に，情報セキュリティの確保も不可欠となっている。ＩＣＴの発展を踏まえた情報セキュリティの確保のためには，制度を所管する課等や各局，各執行機関内における取組にとどまらず，全庁的な取組が必要である。

本市の情報セキュリティの確保及び推進のための体制としては，局区長等で構成される京都市高度情報化推進本部，局等の庶務を担当する部長等で構成される高度情報化推進会議，各所属の情報セキュリティ担当者及びそれを補佐する情報化推進支援員等が，既に設置されており，それらも有効に機能させる必要がある。

しかしながら，現状では，「第４　意見」においても述べたように，個人情報の取扱いの開始時のチェックと情報システムの導入時のチェック等が連動していない，個人情報を取り扱う情報システムの設置状況の全庁的な把握がされていないなど，情報セキュリティ上の制度や体制と，個人情報保護制度との連携がされていない状況も見受けられた。

また，昨今，スマートフォン等の小型情報機器の普及や，インターネットを利用した攻撃の増加など，個人情報に係る新たな脅威も生じている。

そのため，個人情報をはじめとした情報資産に係る情報セキュリティの確保のための体制の充実，強化が求められる。

⑵　「高度情報化推進のための京都市行動計画～情報通信技術（ＩＣＴ）京都（2012版）～」においては，「職員の情報活用能力（情報リテラシー）の向上」に関して，今後はＩＣＴを効果的に活用した施策や事業の立案，事務の見直しなどを行うことができる能力や，セキュリティを常に意識して情報を取り扱う能力を身につけた職員を増やしていくことが重要であるとして，ＩＣＴ人材の育成及び研修等の実施に取り組むとされている。

各所属の職員の情報リテラシーの向上と併せて，専門部署の職員による関与（指導・監督等）の程度も向上させる必要があるが，情報セキュリティに関しては，全国的に見ても，組織の各部署の人材だけでなく，組織内の専門人材も不足している

状況にあるとされている[1]。

個人情報取扱事務を所管する課等や，情報システムの主管課等も含め，それぞれにどのような役割を担わせるのが適当かを改めて検討したうえで，それに応じた人材育成を行っていく必要があり，既存の計画に盛り込むなどの計画的な取組が求められる。

２　個人情報に係る情報セキュリティ対策の更なる強化

⑴　総務省は，マイナンバー制度の施行を控えた中での日本年金機構における個人情報流出事案を受け，標的型攻撃等の新たな脅威に対応するため，地方公共団体の情報セキュリティに係る抜本的な対策を検討するチームを設置した。同チームの報告[2]では，情報システムのセキュリティ向上のための対策（マイナンバー利用事務において，端末からの情報持出し不可設定等により，個人情報流出を徹底して防止すること等）を講じることにより，各地方公共団体の情報セキュリティ対策の抜本的強化を図ることが必要であるとされ，本市においても対策が進められている。

マイナンバー以外の個人情報の取扱いについても，こうした動向を踏まえ，情報セキュリティ対策の強化について，抜本的な対策の必要性を含め，改めて検討すべき時機にある。

本市におけるファイル共有システムや基幹業務システムのセキュリティ対策の一層の強化について，安全性，実効性，経済性等の観点から，国や他都市等の動向も注視しながら，引き続き長期的な視点で検討していくことが求められる。

⑵　現在は，紙文書であってもパソコン等で原稿の作成及び保存を行っている場合が大半であり，個人情報の適正な取扱いに当たっては，収集，利用，提供を必要な範囲に留めるだけでなく，データの処理及び保存形態に応じた情報セキュリティ対策が重要となっている。

特定個人情報（マイナンバーをその内容に含む個人情報）の取扱いについては，各地方公共団体共通のガイドラインにおいて，利用，提供の制限等と共に，安全管理措置の具体的な内容が示されている。

マイナンバー制度の導入を契機として，個人情報の適正な管理のために必要な措

---

[1] 「サイバーセキュリティ戦略」（平成 27 年９月４日閣議決定）等。

[2] 平成 27 年 11 月 24 日「新たな自治体情報セキュリティ対策の抜本的強化に向けて～自治体情報セキュリティ対策検討チーム報告～」。

置としての情報セキュリティ対策の指針等，時代に即した個人情報保護制度の在り方を改めて検討していくことが求められる。

⑶　第 31 次地方制度調査会において，「人口減少社会に的確に対応する地方行政体制及びガバナンスのあり方に関する答申」が取りまとめられた。

答申においては，地方公共団体のガバナンスに関して，長自らが，行政サービスの提供等の事務上のリスクを評価及びコントロールし，事務の適正な執行を確保する体制（内部統制体制）を整備及び運用することが求められるとされ，内部統制の対象とするリスクについては，地方公共団体が最低限評価すべき重要なリスクであり，取組の発展のきっかけとなるものをまず設定すべきであるとされている。

情報の管理，とりわけ個人情報の管理は行政サービスの基礎となる重要な事務であり，答申においても，財務に関する事務の執行におけるリスクを最低限評価するリスクとしたうえで，情報の管理に関するリスク等についても地方公共団体の判断により内部統制の対象とすることが考えられるとされている。

答申を受け，今後，地方自治法の改正等が検討されていくこととなるが，本市における取組に当たっては，個人情報の管理に関するリスクを内部統制の対象とすることについて検討されることが望ましい。

また，民間企業等の動向として，各種マネジメントシステムの統合運用のための環境整備が図られており，品質，環境，労働安全衛生，情報セキュリティなどの複数の側面から内部監査を同時に実施し，組織全体のリスク等を一元管理することなどによる効率性と有効性の向上が期待されている。

本市全体におけるマネジメントとして，ＩＳＯマネジメント規格を準用した独自の環境マネジメントシステム（ＫＹＯＭＳ）のほか，業務監察や各局等における職場巡察等の仕組みは既に存在している。

今後，取り組まれる内部統制の制度化を契機として，個人情報の管理体制の在り方も含めた本市全体のマネジメント体制を改めて整理していくことが求められる。

（監査事務局）