堺市個人情報流出事案検証委員会

報告書

平成２８年２月

目　　次

第１章　検証の概要 ･･･ １
１　事案の概要 ･･･ １
２　市の調査の概要 ･･･ １
⑴ 市への通報から個人情報流出の発覚まで（平成２７年６月～９月）
⑵ 全容解明に向けた調査の実施から結果の公表まで（平成２７年９月～１２月）
⑶ 通報者等との接触から接触の結果得た情報の公表まで（平成２７年９月～１２月）
⑷ インターネット動画サイトへの掲載について
３　再発防止策の概要 ･･･ ３
４　堺市個人情報流出事案検証委員会 ･････････････････････････････ ３
⑴ 目的
⑵ 構成
⑶ 開催状況

第２章　検証の結果 ･･･ ４
１　調査結果の妥当性 ･･･ ４
⑴ 初動調査
⑵ 個人情報流出の発覚以降の調査
⑶ 市としての対応
２　再発防止策の妥当性 ･･･ ８

第３章　提　言 ･･･ 12
１　今後あるべきインシデント対応についての観点 ･････････････････ 12
⑴ 初動対応
⑵ 通報への対応
２　情報管理に関する業務のあり方についての観点 ･････････････････ 13
⑴ ログの管理
⑵ 業務アプリ等の管理
⑶ 個人情報データの管理
３　個人情報保護、情報セキュリティに関する職員の認識についての観点 ･･ 14
⑴ 職員の意識の向上
⑵ 職員のＩＴスキルの向上

第１章　検証の概要

堺市個人情報流出事案検証委員会（以下「検証委員会」という。）は、平成２７年９月から１２月にかけて判明した約６８万人の選挙有権者情報等の流出事案（以下「本事案」という。）について、市の調査や再発防止策の妥当性を検証するために開催されたものである。

その報告に当たり、検証の対象とした本事案や市の調査内容、再発防止策並びに検証委員会の開催状況等につき、検証の概要として以下のとおり整理した。

１　事案の概要

堺市職員（平成２７年１２月１４日付け懲戒免職。以下「元市職員」という。）が、無断で自宅に持ち帰っていた選挙データや業務ファイル等を個人で契約していた民間のレンタルサーバー（＊１）（用語説明は、１５～１６頁を参照。以下同じ。）の公開されている部分に保存したことにより、平成２７年４月から６月までの間、インターネット上で閲覧可能な状態となり、約６８万人の有権者データ等の個人情報を含む１５ファイルが外部からアクセスされ、個人情報が流出したもの。

２　市の調査の概要

本事案において、平成２７年６月２４日に市に通報メールが寄せられてから、約６８万人の有権者情報の流出が判明し、１２月にかけて実施した市の調査の概要は以下のとおりである。（詳細は、資料編第１回会議資料・資料３「個人情報流出事案調査報告書」（以下「調査報告書」という。）の１頁～４頁を参照）

⑴　市への通報から個人情報流出の発覚まで（平成２７年６月～９月）

６月２４日に、市ホームページにインターネット上の不審情報についての匿名の通報（メール）が寄せられ、調査を開始した。当初は、インターネットサイトにキャッシュ（＊２）として残されていた情報から、元市職員が自ら開発した選挙システムを他の自治体等に売り込もうとしていた疑いがあることが分かり、元市職員への聞き取りを中心に調査を進めた。キャッシュの中には、個人情報を含むものはなかった。

その後８月２２日に、「選挙に係る個人情報流出があったようである」とのブログ掲載がなされ、個人情報流出の疑いについても調査を開始し、元市職員のパソコン等を押収した。

９月５日、別のインターネットサイトに、「市関係者の個人情報が流出していた」との書き込みがあり、マスキングされた個人情報等の画像が掲載され、元市職員に聞き取りを行った結果、個人契約のレンタルサーバーから個人情報を含む２ファイルが流出していたことが判明した。

９月１２日には、９月５日に書き込みがあったインターネットサイトに、流出したとされる新たな個人情報の一覧の画像がマスキングされて掲載され、改めて調査した結果、新たに４ファイルが流出していたことが判明した。また、元市職員が約６８万人の有権者データを平成１８年度から２３年度までの間、９回にわたり無断で自宅に持ち帰っていたことも新たに判明した。（以上につき、平成２７年９月７日及び９月１３日に公表）

⑵ 全容解明に向けた調査の実施から結果の公表まで（平成２７年９月～１２月）

本事案の全容解明のためには、レンタルサーバーに保存され、外部からアクセスされた個人情報を含むファイルを特定する必要があったが、元市職員は平成２７年６月下旬にレンタルサーバーのファイルを削除していた。また、平成２７年８月上旬に職場や自宅のパソコン、ポータブルハードディスクのファイルも削除し、機器を初期化していた。

レンタルサーバーのファイルの復元は技術的に困難であったが、元市職員を介してレンタルサーバーの操作記録（ログ）（＊３）の提供を受けるとともに、専門業者に依頼して職場や自宅のパソコン等のファイルを復元し、ログとの照合、分析を進めた結果、レンタルサーバーに保存されていた個人情報を含むファイルを特定し、当該ファイルに対して通信事業者（プロバイダー）（＊４）を介したアクセス及び検索ロボット（＊５）からのアクセスがあったことが判明した。

さらに分析の結果、２つのプロバイダーのＩＰアドレス（＊６）を保有する人物から、平成２３年１１月執行の大阪府知事選挙時の約６８万人の有権者データ等の個人情報を含む１５ファイルがアクセスされ、これらの個人情報が外部に流出していたことが判明した。（以上につき、平成２７年１２月１４日に公表）

なお、市としては、随時、ＩＴ分野を専門とする弁護士に相談するなど、専門家の意見を聞きながら対応していた。

⑶ 通報者等との接触から接触の結果得た情報の公表まで（平成２７年９月～１２月）

流出した個人情報を保全し２次被害の発生を防止するため、平成２７年９月から市への通報者や個人情報を含むファイルに外部からアクセスした者に対して、流出した個人情報の消去等を求めるべく、接触の試みを続けた。

その結果、２つのプロバイダーを介してファイルにアクセスした２つのＩＰアドレスのうち１つのＩＰアドレスの保有者と、ＪＰＣＥＲＴ／ＣＣ（＊７）を介して接触（メールによるやり取り）をすることができ、２つのＩＰアドレスの保有者は別人物であること、接触することができた１名は市やＪＰＣＥＲＴ／ＣＣなどへの通報者であること、残る１名は通報者が相談した者であることなどの情報を得た。

その後市は、通報者とのメールによるやり取りの中で、個人情報は削除した旨を確認するとともに、通報者保護や個人情報にアクセスした人数に関する指摘を受けている。（以上につき、平成２７年１２月２５日に公表）

⑷ インターネット動画サイトへの掲載について

元市職員が平成２６年４月から平成２７年１２月までの間、インターネット動画サイトに掲載していた、選挙システムの操作デモンストレーション動画に、実在する市民２名の個人情報が使用されていたことが判明している。（以上につき、平成２７年１２月２５日に公表）

３　再発防止策の概要

市では、本事案を引き起こした大きな原因は、情報セキュリティの面において、「所属長の承認を得ることなく、業務上のデータを外部に持ち出すことができた」点にあると認識している。

また、改めて個人情報の取扱いや情報セキュリティの現状を検証した結果、「職員及び所属長の個人情報及び守秘義務に対する認識が不足し、規定に反して保有個人情報を持ち出すことが可能であったこと」や「承認行為が無くてもシステムからのデータの外部持出しや外部記録媒体の接続が可能であったこと」及び「データの外部持出しの操作記録（ログ）を取得することができないシステムや情報管理が十分できていない個人情報を取り扱う個別システムが存在していたこと」等の課題があったという分析をした。

そのうえで、当該課題を解決するため、情報セキュリティを強化する再発防止策として、「職員の意識向上」、「データの外部持出し制限の強化」、「情報セキュリティ等に関するチェック体制の強化」、「事故発生時の対応の強化」の４つの分野に分け、全職員を対象とした研修やデータのシステム外への持出し承認の二重化、ＣＳＩＲＴ（＊８）や事故対策会議の設置など、２１項目にわたり取り組むこととした。（詳細は、調査報告書の９頁～１４頁を参照）

４　堺市個人情報流出事案検証委員会

(1) 目的

元市職員による有権者等の個人情報流出事案に関して、市の調査や再発防止策の妥当性を検証するに当たり、有識者に専門的な見地から意見を聴取する。

(2) 構成

個人情報の保護、情報セキュリティ等に関し専門的な知識及び経験を有する次の委員で構成する。

氏　　名	主な役職等
中野　秀男（座長）	・帝塚山学院大学情報メディア学科特任教授 兼　ＩＣＴセンター長
赤津　加奈美	・弁護士 ・堺市個人情報保護審議会会長
嶋倉　文裕	・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 西日本支部長

(3) 開催状況

○ 第１回会議

日　　時：平成２８年１月２９日（金）　午前１０時３５分から午後０時１０分

議　　事：個人情報流出事案の概要の説明、市の調査結果の報告、
再発防止策の説明

○ 第２回会議

日　　時：平成２８年２月８日（月）　　午前１０時３０分から午前１１時５９分

議　　事：調査内容の妥当性の検証、再発防止策の妥当性の検証

○ 第３回会議

日　　時：平成２８年２月１５日（月）　午後２時から午後２時５０分

議　　事：個人情報保護、情報セキュリティに関する提言の検討、
審議結果の取りまとめ

○ 市長への報告

日　　時：平成２８年２月２５日（木）　午後３時　中野座長から報告

第２章　検証の結果

１　調査結果の妥当性

調査結果の妥当性の検証においては、市に寄せられた匿名の通報の取扱い、通報者へのコンタクト等、初動調査のあり方に関する意見が多数を占めていたため、初動調査と個人情報流出の発覚以降の調査に分けて整理した。

(1) 初動調査

①　初動調査に関する市の説明

市に対して匿名の通報メールが６月２４日に寄せられてから、８月２２日及び９月５日にインターネットサイトに個人情報の流出に関する書き込みがなされるまでの間は、システムの売込みの疑いで元市職員への聞き取りを中心に調査を進めていた。

また、９月１３日に通報者に協力依頼メールを送付するまでの間、市は通報者にコンタクトを取っていなかった。

その理由については、「通報メールに基づき調査をしたところ、元市職員が作成したと思われるメール文書等がインターネット検索サイトにキャッシュとして残されていることを確認した。メール文書の内容は、元市職員が自作のシステムを民間企業に売り込んでいることを疑わせるものであったことから、元市職員によるシステムの売込みを告発する通報であると認識していた。」、「元市職員は、聞き取りの中で自作システムの売込みの事実を認めており、市として、通報者に対し、それ以上の情報提供を求める必要がなかった。」、「キャッシュとして残されていたファイルには、個人情報を含むものは無かったことから、この時点で個人情報流出の疑いは認識していなかった。」とした。

②　検証委員会の意見

ア　初動対応

本事案の最大の教訓は、「インターネット上などＩＴ系の不審事象が起こった場合は、まず個人情報の漏えいを疑え」ということである。

今回の不審情報に関する通報メールのように、明確に個人情報の流出が指摘されていない場合であっても、インターネット上に不審な事象が発生した場合は、まず個人情報の漏えい・流出を疑って対応していく必要があり、今回も通報メールがあ

った時点で、まず個人情報の流出を疑うべきであった。

また、個人情報の流出が疑われる場合に、最初にやるべきことは事実関係の把握と被害範囲の確認であり、一番事情を知っている通報者に聞くことである。通報メールがあった時点で、まず通報者へのコンタクトを取るべきであった。

本事案においては、こうした点で初動対応が不十分であった。

なお、インターネット上の不審な情報に関する外部からの通報は、最初はその内容が何を指摘しようとしているのか、よく理解できないものも多くあるが、調査を進めると思いがけない事実が判明するということもよくあり、些細な情報であっても、現場の担当職員から吸い上げ、集約して組織として共有する必要がある。

イ　専門家の参画

本事案においては、市として通報メールが寄せられてからまず当該メールの内容に基づいて、市職員による調査を実施し、元市職員が作成したと思われるメール文書等の情報が、インターネットの検索サイトにキャッシュとして残されていることを確認している。

キャッシュから得られた情報は、元市職員が自作のシステムを民間企業に売り込むような内容を疑わせるものであり、キャッシュとして残されていたファイルは個人情報を含むものではなかったということであった。

また、市として、元市職員に聞き取りをしたところ、元市職員もシステム売込みの事実を認めていたことから、キャッシュが残されていた経緯や個人情報の流出にまで考えが至らず、本事案が元市職員による自作システムの売込みの事案ではないかという視点で、約２か月間にわたって、元市職員への聞き取り調査等を実施したということであった。

しかし、インターネットの検索による調査については、キーワードの文字列の入れ方によって結果が変わるものである。

ＩＴの専門家ではない市職員による調査の情報だけで個人情報の流出がなかったと判断するのは難しく、通報メールが寄せられた当初からＩＴの専門家のアドバイスを得て、インターネットの検索やキャッシュが残されていた経緯等の調査を行っていれば、早期に個人情報の流出が判明するなど、結論が違っていた可能性があると言える。

今後インターネット上などＩＴ系の不審情報への対応は、当該情報内容の重要性に関してスクリーニング（選別）を行い、重要と判断したものについては、専門家の参画を得て対応する必要がある。

ウ　データ削除への対応

検証委員会において市に確認したところ、本事案では、通報者が、市に通報する前に、元市職員が個人で契約していたレンタルサーバー内に保存していた個人情報が外部から閲覧できる状態にある旨をＪＰＣＥＲＴ／ＣＣに連絡していた。また、連絡を受けたＪＰＣＥＲＴ／ＣＣが、当該サーバーの運営会社に連絡したことにより、元市職員が、運営会社からの連絡を受けて、市に通報メールが寄せられる前に

データを削除していた。

ＪＰＣＥＲＴ／ＣＣは、情報流出の通報があった場合は、その内容の真偽を判断せず、まずサイトの管理者等に連絡を取るとのことである。

こうしたことを踏まえると、今後の初動対応においては、本事案のように既にデータが削除されていることも念頭に置いて、個人情報の流出を疑いつつ、専門家と連携しながら本人の同意のもとに、データへのアクセスログやサーバーを調査することや、本人がサーバーに保存したデータにアクセスできないようにパスワードを変更することを考える必要があると言える。

エ　関係部局の連携、迅速なレスポンス

インターネット上の不審情報への対応に関しては、イで述べた専門家の参画とともに、情報システム部門や人事部門等関連部門による庁内連携と役割分担による取組が求められる。

本事案に照らすと、当初調査に当たった人事部門は、情報システム、情報セキュリティに関して専門ではなく、情報システム部門との十分な連携が必要であった。

また、情報が数秒で拡散してしまうインターネット社会においては、不審情報に対しても迅速な対応が求められることから、まず個人情報の流出を疑い、素早く上層部まで情報が伝達され、必要なレスポンスが取れるような初動体制を構築することが必要である。

オ　通報者への対応

本事案において、まず通報者にコンタクトを取るべきであったということは、アで述べたとおりである。

通報には公益性のある善意の通報と金銭目的等の悪意の通報の２種類があり、その対応は通報者の意図を見極めながら慎重に行う必要がある。

従って、対応を現場の担当職員任せにせず、現場から情報を吸い上げ、所属長等に報告して判断を仰ぐ仕組みをつくるとともに、その対応をマニュアル化しておく必要がある。

また、通報者への対応は、通報者の匿名性を担保し、通報者に不利益が及ぶことがないようにしつつ、内容の真実性にかかわらず、まず通報に対する謝意を示し、やり取りのなかで情報を得ていくことが必要である。

(2) 個人情報流出の発覚以降の調査

①　外部から閲覧可能なファイルの特定及び外部からのアクセスの確認に関する市の説明

個人情報の流出を確認した時点においては、既に元市職員によって自宅・職場のパソコンや自宅のポータブルハードディスクのデータが消去されていた。そのため、専門業者に依頼して、本事案に関連する可能性のあるファイルを復元し、レンタルサーバーに保存されたファイルのログとの照合、分析によって、外部から閲覧可能な状況にあった個人情報を含むファイルを特定した。

さらに、個人情報を含むファイルへの外部からのアクセスについてもログ分析による調査を行い、海外企業の検索ロボットによるアクセスとプロバイダーを介したアクセスを確認した。プロバイダーを介したアクセスについては、２つのＩＰアドレスからのアクセスであることを確認している。なお、改めて、個人情報にアクセスした全てのアクセスログの解析等を専門機関に依頼して検証している。

②　検証委員会の意見

個人情報の流出を確認した時点において、既に元市職員によって関連するデータが消去されていたということであったため、外部から閲覧可能なファイルを特定し、外部からのアクセスを確認するためには、今回市が実施したファイルの復元、ログとの突合せの作業を実施する以外に他に方法はなく、行うべき調査が全てなされたものであると考える。

さらに、現在、外部の専門機関に依頼して、改めて、個人情報を含むファイルにアクセスした全てのアクセスログの解析等を実施しているということから、対応としては妥当なものである。

⑶　市としての対応

①　個人情報の保全、２次流出の注視、職員の処分等に関する市の説明

⑵①のとおり、個人情報を含むファイルへの外部からのアクセスについて、海外企業の検索ロボットによるアクセスと２つのプロバイダーのＩＰアドレスからのアクセスを確認している。

検索ロボットからのアクセスによる個人情報の２次流出に関しては、ＩＴ分野を専門とする弁護士に相談した結果、当該検索ロボットのＩＰアドレスの発信元が、ホームページ等の被リンク調査を実施するために情報収集をする海外企業であること、また、当該海外企業が利用者のホームページ等がどのようなブログやサイトにリンクされているか等を調査・分析する業務を行っており、そのために必要な情報を収集するためにアクセスしていたと想定されることから、その可能性は低いと考えている。なお、改めて、個人情報にアクセスした全てのアクセスログの解析等を専門機関に依頼して検証している。

また、２つのプロバイダーのＩＰアドレスからのアクセスについては、ＪＰＣＥＲＴ／ＣＣを介して行った１つのＩＰアドレスの所有者とのやり取りの中で、２つのＩＰアドレスの所有者は通報者とその相談者であるとの情報を得ている。また、通報者から直接届いたメールにおいて、「ダウンロードした個人情報を含むファイルを削除した。他に転送はしていない。」「相談者も拡散させることなくデータを削除済み。」との言を得て、通報者と相談者が保有していた流出した個人情報は削除され、そこからの個人情報の２次流出やそれによる被害発生の恐れは少ないものと考えている。

なお、市からＪＰＣＥＲＴ／ＣＣに対して、２次流出や被害発生の通報があれば連絡をしてもらえるように依頼しているが、市として引き続き２次流出やそれによる被害の発生がないか注視していく。

関係職員の処分等については、外部委員（３名）が入った「堺市職員懲戒等審査会」

に諮り、規則で定める処分基準や過去の事例に照らし合わせた中で、適正に決定、判断した。

②　検証委員会の意見

ア　検索ロボットのアクセス

検索ロボットからのアクセスによる個人情報の２次流出については、市のみの判断ではなく、専門家に相談して可能性が低いと判断していること、さらに外部の専門機関にも依頼し、検索ロボットからの情報流出がなかったかということも含めて、改めて全てのアクセスログを解析して調査していることから、対応として妥当なものである。

イ　２つのＩＰアドレスからのアクセス

市として、２つのＩＰアドレスの所有者が通報者とその相談者であるとの情報を得たうえで、通報者からの「ダウンロードした個人情報を含むファイルを削除した。他に転送はしていない。」「相談者も拡散させることなくデータを削除済み。」との言を得て、通報者・相談者からの情報流出の恐れは少ないと考えている。また、市からＪＰＣＥＲＴ／ＣＣに対して、２次流出や被害発生の通報があれば連絡をしてもらえるように依頼するとともに、市としても引き続き２次流出や被害発生がないかを注視していくこととしている。

こうした対応については妥当なものであり、これまでに書き込みのあったインターネットサイトの巡視や関連情報の検索を継続して行うなど、情報の２次流出の監視を続けていく必要がある。

ウ　関係職員の処分等

市として、処分に関する客観的な審査基準を持ち、外部有識者も入れた審査会で慎重にチェックを行っており、適正な処分を基準と手続きに従って行っていると思われる。そうであれば、市が行った処分は妥当であろうと考える。

２　再発防止策の妥当性

①　再発防止の取組に関する市の説明

第１章「３　再発防止策の概要」に記載のとおり、本事案を引き起こした大きな原因は、情報セキュリティの面において「所属長の承認を得ることなく、業務上のデータを外部に持ち出すことができた」点にあると認識し、５つの課題認識のもと、その解決を図るため、２１項目の取組を掲げている。

具体的な再発防止策については、全職員を対象としたｅラーニング研修やＵＳＢの接続口を塞ぐ物理的な措置等、既に緊急対応として実施したものと、データの外部持出し承認の二重化、データ外部持出し時のデータの暗号化等、システム構築が必要なものがあり、後者についてはデータのシステム外への持出し承認の二重化のように次年度に予算を確保して早期に実施していくものと、庁内ＬＡＮ（＊９）へのシンクライアントシステム（＊１０）基盤の導入のように継続検討していくものがある。

②　検証委員会の意見

ア　市の課題認識・再発防止策の妥当性

市として本事案の発生を踏まえ、改めて個人情報の取扱いや情報セキュリティの現状を検証した結果、調査報告書においては課題として５項目が掲げられているが、内部の不正行為に対するＩＴ技術上の課題認識としては妥当であり、再発防止策として緊急に実施したこと、来年度予算を確保して実施しようとしていることについて、必要な対策が示されている。

なお、今後の再発防止策については、以下の各事項に留意して取り組みを進められたい。

イ　職員の意識の向上

再発防止に向けた課題としては、市が示しているＩＴの技術水準に係る課題だけでなく、組織構成員として、職員一人ひとりの意識レベルをどのように変え、個人情報に関するセンシビリティ（感受性・感度）をいかに育てるかということについても課題として認識する必要がある。

ウ　研修効果の確認

全職員を対象とした個人情報保護及び情報セキュリティに関するｅラーニング研修や管理職を対象とした情報の適正管理に関する集合研修を既に実施している。

職員の意識向上のために、必要な取組であると認められるが、研修の受講のみで終わっては不十分であり、受講者が十分に内容を理解しているかチェックを行うとともに、レポートの提出等により意識向上効果の確認をする必要がある。

エ　データのシステム外への持出し制限の強化

ｉ）データのシステム外への持出し承認の二重化

データのシステム外への持出し承認の二重化は、データのシステム外への持出しを行う場合に、本人の認証に加え、所属長によるシステム上の承認がなければ、外部記録媒体へのデータ持出しを不可能にする仕組みである。

調査報告書では、住民情報系システム（＊１１）の端末において導入すると記載しているが、検証委員会における市への質疑で確認したところ、住民情報系システムに限定するのではなく、まずは優先して実施するということであった。

情報資産の分類上最重要である住民情報系システムを優先することについては妥当である。しかし、本事案で流出した情報には、住民情報以外のものもあることから、住民情報の対策に限定することなく取り組んでいく必要がある。

ⅱ）データのシステム外への持出し時のデータの暗号化

システム外への持出し時のデータの暗号化は、システムの端末からデータを外部に持ち出す場合に、強制的にパスワードを付与し、データを暗号化する仕組みである。

データの暗号化は、外部にデータを持ち出さなければならない時に紛失等のリスクに対応するための対策としては非常に有効である。

ⅲ）データのシステム外への持出し時の操作記録（ログ）取得の拡充

現在一部の住民情報系システムの端末で既に実施している入出力操作に係る操作記録（ログ）の取得を拡充し、データのシステム外への持出し時の申請と承認に係る操作記録を取得する仕組みを導入するということである。

ログの取得は内部不正に対する抑止力としての効果が期待できるものである。

しかし、ログを取得するだけでなく、取得したログを個人情報保護担当課及び情報システム担当課にリアルタイムに集約し、定期的に検証することが必要である。

具体的には、可能な限り個人情報の持出しを少なくするために、いつ、誰が何のために持ち出したか、承認した所属長の判断は適切であったか等について、ＰＤＣＡサイクルにより検証することが必要であり、取組の効果を明確にして市民に対する説明責任を果たす必要がある。

まずログを収集することから開始し、分析・解析するということについては、経費的な課題もあることから、例えば５年先を目標とする等、今後の取組を検討されたい。

なお、個人情報保護担当課には庁内の個人情報の取扱い状況が集約されていることから、持出しの二重承認及びログの取得に関しては、集約されている庁内保有の個人情報を対象として実施するとともに、外部への持出しについては、ＵＳＢ等の外部記録媒体の利用によるものに加え、メール添付での持出しについても、その対象とする必要がある。

さらに、持ち出した後の情報の管理についても、紙であれば返却されたかどうか、データであれば完全に削除されコピーがないかということまで視野に入れた対応が必要である。

オ　個人情報保護及び情報セキュリティに関するチェック体制の強化

個人情報の保護と情報セキュリティに関するチェック体制については、それぞれの担任副市長をトップとする系統に分離して構築している。

個人情報の保護とＩＴ化を推進する立場でもある情報セキュリティのチェック体制を分離したことについては、個人情報の保護とＩＴ化の推進の両面でバランスよく業務を推進する仕組みとして評価できるものである。

情報セキュリティに関する統一的な窓口であるＣＳＩＲＴの設置に関しては、求める機能やどのようなものをめざそうとしているかを明確にする必要がある。

なお、通報者からの情報を上位者へ報告し指示を仰ぐ体制、ＣＳＩＲＴの充実等の取組は、実際に事件が起きることを十分に想定したうえで実施していくことが重要である。

カ　事故発生時の対応の強化

個人情報の保護及び情報セキュリティに関する事故発生時の対応については、それぞれの指揮命令体制のもとで２つの担当課（市政情報課、情報化推進課）が連携し、各々の指揮命令体制が車の両輪のように機能するようにしておく必要がある。

また、この指揮命令体制において的確な判断が下せるよう関係部局による事故対策

会議を設置されているが、いざと言う時の動きを想定し、速やかに必要最小限のメンバーにより迅速な対応を取るという発想で体制を考えておく必要がある。

キ　追加すべき再発防止に関する取組

ｉ）業務アプリ等の管理

住民基本台帳や税、福祉、保険年金等の基幹システムの導入に際しては、その調達に係る契約や仕様書の内容のチェックを行うなど、情報化推進課が全体を把握しているとのことであったが、各課における事務処理の効率化のために、エクセルやアクセスを使って職員がシステムを自作している場合がある。

自作システム（業務アプリ）については、事務処理の効率化に資する取組であるが、業務引き継ぎを受けた担当職員の理解不足等により、処理を誤り、業務に支障を生じることがないよう、適切に管理しなければならない。

そのためには、まず情報システム担当課において、どの部署にどのようなシステムがあるかを把握したうえで、集約して管理するのか、各課で管理するのか、また、複雑なシステムについては外部へ業務委託するのか、ということについて、ガイドライン等を定めて仕分けする必要がある。

そのうえで、自作システム（業務アプリ）の運用においては、当該ガイドライン等に沿って要件定義と基本設計を適切に行うとともにデータの適正管理を徹底する必要がある。

また、スキルの伝承やマニュアルの作成にも取り組み、人事異動等による担当者変更に対応できるように管理していく必要がある。

ⅱ）システム管理におけるＩＤ管理等

システム管理においては、アクセスするＩＤ、パスワードの管理を適正に行い、人事異動等により異動した職員にアクセス権が残り続けないように、権限管理を適切に実施する必要がある。

第３章　提　言

個人情報の保護及び情報セキュリティの確保について、次のとおり提言する。

今後二度と同様の事案を発生させないために、計画された再発防止策に着実に取り組まれるとともに、検証委員会の意見、提言に適切に対応されることを期待する。

１　今後あるべきインシデント対応についての観点

(1) 初動対応

①　インターネット上の不審事象への対応

本事案の最大の教訓は、「インターネット上などＩＴ系の不審事象が起こった場合は、まず個人情報の漏えいを疑え」ということである。情報セキュリティの体制の構築に際しては、個人情報の漏えいを防ぐ、個人情報を保護するということを最優先に取り組まれたい。

また、インターネット上の不審事象の場合は、本事案のようにデータが削除されているということを念頭に置いて対応する必要がある。

②　情報の集約と専門家の参画

不審情報への対応に際しては、管理職レベルから注意を払うのではなく、現場の担当職員レベルから些細な情報であっても吸い上げ、集約して組織として共有する必要がある。また、当該情報内容のスクリーニング（選別）を行い、重要と判断したものについては、専門家の参画を得て対応する必要がある。

③　迅速なレスポンスチームの編成

インシデント発生時には、迅速な対応が求められる。

事故発生時の対応の強化策として、関係部局による事故対策会議が設置されているが、インシデント発生後、当該会議の開催に至るまでに、瞬時に必要なレスポンスが取れるよう、少人数の初動体制（レスポンスチーム）が必要である。

また、こうした非常時の体制については、各職員がそれにもとづく活動をイメージできるように、日頃の演習や訓練の実施等により、有事の際の実効性を高めることが必要である。

(2) 通報への対応

①　通報者への対応

個人情報の流出が疑われる場合に、最初に行うべきことは、事実関係の把握と被害範囲の確認であり、事情を一番知っている通報者に聞くことが重要である。

通報者への対応は、通報者の匿名性を担保し、通報者に不利益が及ぶことがないようにしつつ、通報内容の真実性にかかわらず、まず通報に対する謝意を示し、やり取りのなかで情報を得ていくことが必要である。

また、通報者への対応は現場任せにせず、現場から吸い上げた情報を所属長等に報告し判断を仰ぐ仕組みをつくるとともに、対応をマニュアル化しておくことが求められる。

通報者への対応としては、ホイッスルブローイング（内部告発）を考慮し、組織内

の告発者も不利益を被ることがないようにすることが求められる。

② 公益通報対応の見直し

本事案は個人情報の流出の事案であるが、当初の通報メールは市にとって一種の公益通報であったということができる。こうした通報メールへの初動対応は、個人情報保護の問題への対応ではなく、公益通報で議論されている通報者保護をどうするか、どのように通報を受け入れるかという観点から、公益通報対応の問題としてとらえた方が理解しやすいのではないかと考える。

現在、堺市には公益通報者保護法に基づく制度はあるが、職員の職務執行に関する違法又は不適正な行為の通報をどのように受け入れるか、また、通報を受け入れてからどのような体制で、どのような調査を行っていくか等の観点から、公益通報対応の仕組みを見直されたい。

２　情報管理に関する業務のあり方についての観点

(1) ログの管理

インシデントが発生した場合の原因究明のためだけに、ログを取得するのではなく、可能な限り個人情報の持出しを少なくするために、取得したログを個人情報保護担当課及び情報システム担当課にリアルタイムに集約し、半期又は年に一度、いつ、誰が何のために持ち出したか、承認した所属長の判断は適切であったか等について、ＰＤＣＡサイクルによって検証することが必要である。

まずログを収集することから開始し、分析・解析するということについては、経費的な課題もあることから、例えば５年先を目標とする等、今後の取組を検討されたい。

(2) 業務アプリ等の管理

事務処理の効率化のために各課で職員がエクセルやアクセスを使って自作しているシステム（業務アプリ）については、業務引き継ぎを受けた担当職員の理解不足等により、処理を誤り、業務に支障を生じることがないよう、情報システム担当課において、現状を把握したうえで、その運用のガイドライン等を定めることにより適切に管理しなければならない。

なお、データをインターネット上のサーバーに保存しておけるドロップボックスのような、誰もが自由に利用できるクラウドシステムを組織の許可なく組織内の情報システムとして利用する、シャドーＩＴについては、堺市では利用が禁止されている。

例外的に育児休業取得者や他自治体等への長期派遣者については、自宅から庁内ＬＡＮシステム内のメール等を参照できるようになっているが、外部からのシステム利用については、アクセスできるコンピュータを特定し、そのログを適切に取得したうえで、利用させる必要がある。

(3) 個人情報データの管理

庁内の個人情報の取扱状況については、堺市個人情報保護条例に基づき、毎年度個人情報保護担当課に届け出る仕組みとなっている。

個人情報保護担当課において、どのような個人情報データが、どの部署で、どのよう

な事務で、どのような使われ方をしているのか等、適正に管理されているかについて把握する必要がある。

３　個人情報保護、情報セキュリティに関する職員の認識についての観点

(1) 職員の意識の向上

内部不正への再発防止策としては、システム管理上の技術的な対策に加えて、職員の個人情報保護や情報セキュリティに関する意識の向上を図る取組も求められる。

現在職員に対しては、基本的な知識の修得と意識の醸成を図るためにｅラーニング等の研修を実施しているが、十分に理解が深まっているかについて、効果測定を確実に実施していくことが必要である。

また、全職員が個人情報保護や情報セキュリティに関するリテラシー（知識や利用能力）やセンシビリティ（感受性・感度）を向上させていく必要がある。職員は、常にセンサーを働かせてインシデントの発生を意識して業務に取り組むことが求められる。

(2) 職員のＩＴスキルの向上

ＩＴシステムを適正に管理し、情報セキュリティの確保を図る観点からは、職員のＩＴスキルレベルの向上が不可欠である。

職員のＩＴスキルに関しては、今日、情報系の専門職種の採用が困難であると考えられることから、情報システムの専門家をどう確保するかという課題がある。

外部に委託することによりＩＴスキルを確保することや一定のＩＴスキルを職員の採用条件にすること、あるいは職員の採用後に研修等によりＩＴスキルを研鑽させるとともに、情報セキュリティに関する知見も習得させることにより、ＩＴゼネラリストを育成することなどが考えられるが、どのような方策により職員のＩＴスキルを確保することとするのかについて今後検討する必要がある。

≪ 用　語　説　明 ≫

＊１	レンタルサーバー	ウェブサイトやウェブアプリケーションをインターネットで一般公開するために使われる、複数のユーザーが利用するサーバーを提供するサービス
＊２	キャッシュ	インターネットの閲覧時にウェブページの表示速度を上げるために、ウェブページを構成する画像などのファイルを複製して保存されたデータ
＊３	ログ	コンピュータの操作やサーバーへのアクセスに関する記録
＊４	プロバイダー	インターネットに接続するサービスを提供する事業者
＊５	検索ロボット	インターネット上のウェブサイトの情報を取得して検索用データベース･インデックスを作成する自動巡回プログラム
＊６	ＩＰアドレス	インターネットやＬＡＮなどのＩＰネットワークに接続されたコンピュータなどに割り振られる識別番号
＊７	ＪＰＣＥＲＴ／ＣＣ	インターネットを介して発生する侵入やサービス妨害などのコンピュータセキュリティインシデントについて、日本国内のサイトに関する報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行う、特定の政府機関や企業からは独立した中立の組織（一般社団法人）
＊８	ＣＳＩＲＴ	Ｃｏｍｐｕｔｅｒ　Ｓｅｃｕｒｉｔｙ　Ｉｎｃｉｄｅｎｔ　Ｒｅｓｐｏｎｓｅ　Ｔｅａｍの略称。（シーサートと読む。）堺市においては、情報セキュリティに関する障害、事故等の発生に備え、発生した障害、事故等を正確に把握し、及び分析することにより、被害の拡大の防止、情報資産の復旧、再発の防止等の措置を迅速かつ的確に行うことを可能とするため、これらの措置を統一的に行う機能を有する窓口のことを言う。
＊９	庁内ＬＡＮ	主に市役所内部の日常業務に関するシステム（例えば、文書管理や財務会計、人事給与など）を扱う、行政内部のネットワークシステムで、正式名称は「堺市行政情報ネットワークシステム」。インターネット接続や電子メールのほか、部署単位でのファイル共有などを行っている。

＊１０	シンクライアントシステム	利用者が使うコンピュータ（クライアント）に最低限の機能しか持たせず、ソフトウェアの実行やデータの保存などの機能をクライアントから切り離し、サーバーで集中的に管理するシステム シン（thin）は、「薄い・細い」を表す英単語のこと。
＊１１	住民情報系システム	住民基本台帳や税、国保や年金等の住民情報を扱う業務に関する各種システムを扱う、インターネットなどの外部のネットワークに繋がっていない、市役所内部で閉ざされたネットワーク