資料１

個人情報流出事案検証委員会　主な委員意見

（第１回　平成２８年１月２９日、第２回　平成２８年２月８日）

【調査結果の妥当性に関する意見】

○　今回の最大の教訓は、「インターネット上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。情報セキュリティは個人情報の漏えいを防ぐ、保護することを最優先にした体制の構築が必要。

○　インターネット上の不審情報の通報は、最初はその内容がよく理解できないものが多くあるが、調査を進めると思いがけない事実が判明することもよくある。今回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。

○　個人情報の流出が疑われる場合に、最初にやるべきは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。通報メールがあった時点で、個人情報の流出を疑いつつ、今回の事案のように既にデータが削除されていることも前提に、まず通報者へのコンタクトを行い、専門家と連携しながらログ、サーバを押さえていくことを考える必要があった。

○　キャッシュ調査で得られた情報をもとに、自作システムの売り込みという一面で２か月間にわたって調査が実施されていたが、インターネットの検索においては、キーワードの文字列の入れ方で結果が変わる。ＩＴの専門家ではない市職員によるキャッシュ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かったのではないか。

○　今回の事案では、当初からＩＴの専門家のアドバイスを得て調査を行っていれば、結論が違っていた可能性がある。今後インターネット上の不審情報への対応は、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、専門家の参画を検討する必要がある。

○　インターネット上の不審情報への対応に関しては、専門家の参画とともに、情報システム部門との庁内連携と役割分担による取組が求められる。

　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いため、早期の連携が必要であった。

　普段からコミュニケーションができるような体制づくりをすることが必要。

○　インターネット上の不審情報に対しては迅速な対応が求められる。まず個人情報の流出を疑い、素早く副市長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（少人数のレスポンスチーム）を構築することが必要である。

○　通報者には２種類あり、善意の通報者と通報を金銭に換えようとする者がいる。
　些細な情報であっても、対応を現場任せにせず、エスカレーションする仕組づくり、対応のマニュアル化が必要。

○　通報者への対応は、通報者の匿名性を担保し、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。

○　今回の通報は、市にとって公益通報であり、公益通報で議論されている通報者保護をどうするか、どのように通報を拾い上げるかなど、コンプライアンス機能についての検証も必要。

○　データが消去されていたため、個人情報流出の発覚以降のファイルの特定の調査としては、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いといえ、時間がかかったが、やるべき調査がなされたものと考えられる。また、それにプラスして現在外部の専門業者の確認もしているところであり、適切ではないか。

○　今後の初動対応に関しては、今回の教訓として次の３点に取り組む必要がある。

・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・流出を疑うこと。

・最初の通報は、よくわからない内容であっても、調査をすると思いがけない事実が判明することもある。現場から些細な情報を吸い上げ、集約して組織として共有すること。

・通報者への対応をないがしろにしないこと。通報者の保護、匿名性を担保しつつ、コンタクトの方法をマニュアル化する必要がある。

【指揮命令体制、個人情報保護の対応に関する意見】

○　個人情報保護と情報セキュリティの指揮命令体制は、いざというときに動きが想定できるような体制にしておく必要がある。

○　個人情報保護と情報セキュリティの指揮命令体制のトップに別々の副市長が就くことは大変良いことであるが、体制図が分かれており、図からは２つの担当課（市政情報課、情報化推進課）の連携が分かりにくい。市長トップのもとに、２つのラインが車の両輪のごとく動くことがイメージできる組織図にしておく必要がある。

○　個人情報保護の対応は、平時と非常時に分けて考える必要がある。

○　平時の対応として、個人情報の持ち出しにおいて、ダブルチェックを実施し、ログを取得するということであるが、取得したログを個人情報の担当課、情報化の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、チェックした課長の判断はよかったか等を検証し、なるべく個人情報の持ち出しを少なくするためのＰＤＣＡを回すことが必要。ＰＤＣＡを回して政策効果が上がるようにしないと市民に対する説明責任を果たせない。

○　また、個人情報担当課に集約される庁内の個人情報取扱情報についても、ダブルチェック、ログを取得する対象として位置付けるとともに、外部持ち出しだけでなく、メールの添付での持ち出しについても、同様のセキュリティをかけるべき。

○　平時においては、折角ダブルチェックして、ログを取るのであれば、それをどこかに集約して、ＰＤＣＡを回して、個人情報持ち出しゼロを目指すのがよいのではないか。

○　非常時の対応としては、最初の通報は些細な内容であることが多いので、広く網をか

けて個人情報の漏えいをまず疑うこと。また、体制図においては、「認知」に至るまでが問題。管理職だけでなく、一般職員からも不審なことがあれば通報を求め、吸い上げる体制にしておく必要がある。

○　インシデントの発生時には、その日の間に必要最小限の人が集まり、どのような対応をするかという発想で組織図を考えておく必要がある。

○　持ち出した後の情報の管理については、紙なら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射程に入れて対応する必要がある。

○　自治体では情報系の職員の採用が少ない。情報の専門家をどう確保するか。外部に委託するか、スペシャリストを養成するかを考えていく必要がある。

○　個人情報保護に関しては、４情報（名前、性別、住所、生年月日）だけでなく、どこまで含めるか気になる。ある人が特定されれば個人情報であるが、線引きが曖昧な部分もある。プライバシー保護の観点からは、メールアドレス、顔写真、会員番号などにも配慮が必要。

【市の対応に関する意見】

○　検索ロボットからのアクセスによる２次流出に関しては、市での判断だけではなく、専門業者にも依頼して調査しているということであるので大丈夫と考えられる。

○　二次流出に関しては、ＪＰＣＥＲＴに対して、二次流出があれば連絡を、という依頼をしているということであるが、それなりの長期間監視を続けていく必要がある。

【再発防止策に関する意見】

○　ｅラーニングを受講するだけで終わっては不十分。理解度チェックを行い、レポートを出させるなどしなければならない。

○　データの外部持ち出し承認の二重化等の措置について、住民情報系システムを優先して実施するということである。今回流出した情報には、住民情報系以外のものもあるが、報告書には住民情報系を優先するという記載がなく、どこまで対策を取るかということが分からない内容となっている。

○　データ外部持ち出し時のデータの暗号化は、今回の事案のように正当な権限がある人がその権限のもとにファイルを持ち出すことに対しては意味がないが、データを持ち出さなければならない時に実施することは非常に有効である。

○　ＣＳＩＲＴの設置に関しては、事後対応をするのか、事前の対応（監査）か、品質管理、ｅラーニング等による意識向上を図るもの等、いろいろなモデルがある。求める機能やどのようなものを目指そうとしているかを明確にする必要がある。

○　業務アプリについては、住民サービスの確保の観点から、職員個人が中途半端な処理をしないように、情報部門が庁内の状況を把握して、マニュアルをつくり、メンテナンスできるように取り組んでいく必要がある。どこかに集約することにより、必要な端末

の台数が減り、コストダウンにつながることも考えられる。

○　システム管理においては、業務アプリにアクセスするＩＤの管理、ログの管理を適正に行い、人事異動でいなくなっ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。

【提言】

○　職員の自作システムについては、要件定義と基本設計をしっかりと行い、適正にメンテナンスできるよう、情報部門が取り組んでいく必要がある。また、担当者変更に対応するため、スキルの伝承及びデータの扱いについて整理しておくことも必要である。

○　シャドーＩＴの利用は、原則禁止されているが、育児休業取得者や長期派遣者については、自宅からメール等を参照できるようになっている。外部からのシステム利用については、特定のコンピュータからログをきちんと取得したうえで、利用させる必要がある。

○　内部犯行や内部アクセス対策は、総務省の強靭化事業の対象とはなっていないので、例えば５年先を目標に、ログを収集して、解析できるような体制をつくる必要がある。