第198回

自治体における情報漏えいのリスク（その1）

立命館大学情報理工学部教授　上原哲太郎



個人情報保護と行政への信頼

自治体情報システムにおけるリスクの中でも、個人情報の漏えいは市民の関心が高く、一度でも事故が起きれば行政への信頼を大きく損なう。平成14年の住民基本台帳ネットワーク（住基ネット）稼働、平成15年の個人情報保護法制定を巡る議論を機に、多くの市民が個人情報の扱われ方を意識し、特に行政による情報管理に厳しい目を向けるようになった。

その後も、行政手続きのデジタル化が進むにつれ、個人情報が適切に保護されるかという関心は続いている。自治体は、市民から法に基づいて多くの情報を預かる立場である。そこには氏名や住所だけでなく、所得、健康、福祉サービスの利用状況など、機微性の高い情報も含まれる。自治体には預かった情報を確実に守る責務があり、それを脅かすリスクを継続的に把握し、事故の可能性を低減し続けることが求められている。

前回は情報滅失への備えを述べたが、情報を失わず保管することと、その情報を権限のない者に渡さないことは、いずれも重要なリスクマネジメントである。今回から数回にわたり、実際の事故の教訓から情報漏えいを防ぐためのマネジメントの在り方について考えたい。まず今回は、職員や委託先による情報の持ち出しに関わる三つの事例を取り上げる。

U市の住民基本台帳データ漏えい事件

自治体の大規模な個人情報漏えい事件として早くから知られているのが、U市の事件である。平成10年、乳幼児健診システムの開発業務の再々委託先に勤務するアルバイト従業員が、住民基本台帳などのデータを不正に複製し、名簿販売業者に売却した。その業者が実際に販売したことにより約21万件のデータの流出が翌平成11年に発覚し、市の管理責任が問われた。

この事件では、被害を受けた住民が市に損害賠償を求め、市の責任が認められた。裁判では、市が再委託を承認していたことや、市の担当者と再々委託先の従業員が直接打ち合わせを行い、開発業務も市庁舎内で行われていたことなどから、実質的な指揮監督関係が認められている。

情報システムの開発や運用には専門性が必要であり、自治体が外部事業者を活用することは避け難い。しかし、業務を委託しても、住民情報を保護する自治体の責任がなくなるわけではない。本件では開発や試験のため住民の実データが再々委託先の従業員に渡されていたにもかかわらず、開発作業の監督責任が十分に果たされず、結果的にデータの持ち出しを許した。そもそも開発に実データが必要であったのか、必要であるとしても全データを渡す必要があったのか、事前に十分検討されるべきであった。実務的にはテスト用のデータの作成と提供、および実データを用いたテストを自治体側で行うことによりリスクが低減できた事案である。

S市の職員による個人情報流出

残念ながら自治体職員自身による情報の持ち出し事件も時折発生する。平成27年に発覚

したS市の事件では、市職員が自ら開発した選挙事務システムのデモのため、無断で自宅に持ち帰っていた選挙データなどを、個人で契約したレンタルサーバーの公開領域に保存していた。その結果、約68万人分の有権者情報などがインターネット上で閲覧可能となり、外部からアクセスされた。

市の検証では、市の情報システムから承認がなくてもデータを持ち出せたことや、持ち出しの操作記録を取得できないシステムがあったことなどが課題とされた。また、外部から通報が寄せられた際、当初は職員による自作システムの売り込みに関する問題として調査が進められ、個人情報流出への初動対応が不十分であったことも指摘されている。

この事例からは、情報セキュリティポリシーによって持ち出しを禁止するだけでは事故防止には不十分と分かる。情報システム上、職員が閲覧可能なデータは制限できるべきであるし、データ閲覧の権限と複製して外部に持ち出す権限は分けて考える必要がある。業務上必要なデータ持ち出しに際しても、承認と記録を伴う仕組みにしておかなければならない。

さらに、大きな事故の兆候を迅速に捉える体制も重要である。外部からの通報は、必ずしも原因や被害範囲を明確に示すものとは限らない。内容が分かりにくいからと現場の判断にとどめず、情報システム部門や専門家につなぎ、組織として調査する必要があるだろう。

A市のUSBメモリー紛失

令和4年6月には、A市の委託業務に関わる作業者が、全市民約46万人分の個人情報を記録したUSBメモリーを紛失した。データ移管作業後の帰宅途上で生じたもので、USBメモリーは後日発見された。

調査では、市の承諾を得ない再委託・再々委託が行われており、仕様書で定めた運搬方法が守られておらず、市側のチェック機能も十分ではなかったとされた。本件は個人情報の漏えいは確認されなかったが、市には多数の問い合わせが寄せられ、給付金関係業務が一時停止するなど、通常業務に大きな支障が生じた。

この事案は、媒体を紛失した作業者の不注意に目が向きやすいが、長年委託先に業務を依存してきたことによる委託先管理の甘さがもたらした事件というべきである。自治体のリスクマネジメントとしては、長年の委託関係によって業務遂行の細部を点検する目が曇ったことが問題であり、大量の情報を庁外に運ぶ必要性や、移送後の媒体の保管・返却・消去まで含めて、自治体側で作業手順を管理すべき事案であったと言える。現在、総務省の「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」はUSBメモリーなどを用いないデータ連携を促すべく改定の検討が進められており、本年度末ごろに改定される見込みである。

情報の持ち出しを管理する

今回取り上げた事例に共通するのは、職員や委託先が扱える情報が、自治体の管理下にある情報システムの外へ無断または不適切に持ち出されたことに起因する点である。職員による作業はもちろん、委託先であっても、データ管理の責任は自治体側にあることを常に意識すべきであろう。

職員による直接作業であっても委託作業であっても、各データのアクセス権はシステム上、作業者別に厳密に設定されるべきである。やむを得ずシステム外にデータを持ち出す場合も、その必要性を審査・記録し、作業後の取り扱いまで確認する体制が求められる。作業実態の点検や監査を通じて、規程と現場作業の隔たりを見付け、改善することが、事故リスクの低減につながるのである。

筆者プロフィール

上原哲太郎（うえはら てつたろう）

京都大学博士（工学）。1995年京都大学大学院工学研究科博士後期課程研究指導認定退学。京都大学大学院工学研究科助手、和歌山大学システム工学部講師、京都大学大学院工学研究科助教授、京都大学学術情報メディアセンター准教授を経て、2011年総務省技官。通信規格と情報セキュリティ施策に従事。2013年より現職。総務省やデジタル庁でセキュリティ確保に関わる委員会の委員を務める。内閣府公文書管理委員会委員。暗号技術検討会（CRYPTREC）委員。NPO情報セキュリティ研究所代表理事、NPOデジタル・フォレンジック研究会会長、（一財）情報法制研究所理事、京都府警察サイバーセキュリティ戦略アドバイザー、和歌山県警察サイバー犯罪対策アドバイザー、滋賀県警察サイバーセキュリティ対策委員会アドバイザー、芦屋市CIO補佐官。