都市のリスクマネジメント

第192回

自治体情報システムとリスクマネジメント

立命館大学情報理工学部教授　上原哲太郎

情報システムのリスクとは

わが国の自治体で初めてコンピュータを導入したのは大阪市であり、それは昭和35年にまでさかのぼられる。平成初期までには多くの自治体が、少なくともバックオフィスの業務の多くを情報システムに依存するようになった。その後住民基本台帳ネットワーク（住基ネット）や総合行政ネットワーク（LGWAN）、マイナンバー制度など、行政事務の効率化を加速させる基盤が整備された。このように60年以上にわたり自治体情報システムは発展を続け、行政サービスの高度化と効率化に貢献してきた。

このように自治体情報システムは現在の行政サービスの基盤であるが、そこにトラブルが起きれば行政サービスの停止や個人情報漏えいなどの事故、ひいては行政に対する信頼の毀損といった重大な問題を引き起こす。しかしこのような情報システムの重要性に比して、リスクを俯瞰（ふかん）的にまとめたものはまだ少ないように思われる。そこで今回から、情報システムにおけるリスクへの理解を深め、適切なマネジメントに資するよう稿を進めていきたい。初回となる本稿では、自治体情報システムのリスク全体を俯瞰できるよう、情報システムにまつわるトラブルを原因から四つに分類し、それぞれ解説する。

システム障害によるトラブル

自治体情報システムにおけるリスクで最も発生頻度の高いのはシステム障害である。障害というと機器の故障などが思い浮かぶが、情報システムにおいてはそのような物理的要因に加えて、急激な需要増加に対する性能不足、ソフトウェア設定の人為的誤り、ソフトウェアの瑕疵（かし）（いわゆるバグ）に起因する障害にも備える必要がある。近年は、住基ネットやLGWANといった相互連携の仕組みや、データセンターやクラウドなどといった、それを土台として情報システムを構築するプラットフォームが増加し、これらとの関係に起因した外部的要因によるシステム障害の発生も増加傾向にある。

システム障害による業務への影響を抑え、障害発生時にも業務を継続するためには、システムの多重化・冗長化と呼ばれる対策や、情報システムの堅牢性の定期的な検査を含めた保守・点検、障害発生時の迅速な対応手順の整備などが必要となる。また、障害の原因が通信事業者やクラウドなど外部要因である場合には、責任分界、障害への対応責任、稼働率をはじめとした品質の保証範囲と障害時の保障および免責の範囲などを明確にしたSLA（サービス・レベル・アグリーメント）の締結も重要である。

サイバー攻撃など外部からの攻撃によるトラブル

情報システムからのデータ窃取や人為的なシステム障害・破壊をたくらむ外部からの攻撃は、自治体も標的となっている。平成27年の日本年金機構に対する不正アクセス事案は、公的機関を狙うサイバー攻撃の深刻さを浮き彫りにしたが、この攻撃者は日本の多数の組織からの情報窃取を同時に行っており、

その中には自治体も含まれていたことが分かっている。そこで同年開始されたのが自治体に対するセキュリティ強化策、いわゆる三層分離対策である。これが功を奏して首長部局におけるサイバー攻撃被害はその後散発的に発生しているものの比較的軽微なものに限られているが、学校や病院など、情報システム管理者を配置しにくい部局では大量の個人情報漏えいなど深刻な被害がいまだに後を絶たない。

サイバー攻撃への対策としては、システムのバグを速やかに修正する脆弱性管理、迷惑メール対策やウイルス対策ソフトの導入・更新、そしてパスワードなどの重要情報を攻撃から守るための職員向けセキュリティ教育などが基本となる。また、セキュリティ事故に対応するための組織としてCSIRT（シーサート）を設置し、副市長など最高情報セキュリティ責任者（CISO）をトップとした事故即応体制をつくって常時情報収集などの活動を行うことも必要である。

職員・委託先によるポリシー違反に起因する事故

情報システムのセキュリティ維持には情報セキュリティポリシーの策定と職員に遵守徹底が必要であるが、実際の自治体情報システムの運用においては、職員や委託先職員によるポリシー違反がしばしば発生し、ミスによる情報漏えい等のリスク要因といえる。例えば、許可されていないUSBメモリへのデータ移送と持ち出し、業務で許されていないクラウドサービスの利用などが事故を起こすリスクが高く、情報漏えいやマルウェア感染などの事故につながることがある。

これらのリスクを低減するには、情報セキュリティポリシーの周知徹底はもちろん、定期的な研修・教育そして監査の実施が不可欠である。また、技術面でもポリシー違反がそもそも行えない仕組みや、そういった行為を早期発見できる仕組みが必要である。

職員・委託先によるデータ持ち出しなどの内部犯行

自治体においても内部関係者が業務上知り得た住民情報を無断で持ち出し、外部に漏えいさせる事件が散発的に発生している。特に委託先による事件は大規模な事故になりやすい。平成10年に発生し大きな事件として扱われたU市住民基本台帳データ持ち出し事件は再々委託先のアルバイトの犯行だった。情報システムに関しては専門性が高いため、業務の細部が委託先任せになることが多いが、それこそがリスク管理の大きな問題として認識されるべきであろう。

内部犯行を防ぐには、業務権限に応じた情報管理の徹底、システムにおけるアクセス権限の最小化、重要データへのアクセスログの監視が不可欠である。さらに、内部通報制度の整備なども有効な手段となる。また委託先管理において契約の精査、委託先における作業の監督や監査体制の構築なども有効であろう。

まとめ

このように自治体の情報システムにおけるリスクは多岐にわたるため、リスクマネジメント体制を構築するとなると、これら全てのリスクへの目配りが必要になってくる。しかし自治体情報システムは多くが委託に頼った形で構築運営されてきたため、自治体側の担当者から責任者に至るまで、システムへの深い理解を持つ人材が育ちにくく、リスクの所在を把握し適切に対策を講じることが難しくなっているのではないだろうか。本稿から続く連載が、リスクという観点から自治体情報システムを見直し、事故を未然に防ぎ起きた場合にも被害を最小に抑えるための知見としてお役に立てることを願っている。

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。