都市のリスクマネジメント

第180回

自治体の情報セキュリティとは

合同会社KUコンサルティング代表社員、電子自治体エバンジェリスト　髙橋邦夫

今回より6回にわたり「都市のリスクマネジメント」コーナーに「自治体情報セキュリティ」をテーマとした投稿をさせていただく。

市役所にとって危機管理というと防犯対策や防災対策が思い浮かぶであろうが、今日においてはリアルの犯罪に劣らぬほどサイバー攻撃による被害は増大しており、市役所の事業継続を考えた際にはデジタルデータの保全は防災対策の肝となっている。行政運営のデジタル化による効率化・高度化が求められている現代において、サイバー攻撃と自然災害の両者に立ち向かう情報セキュリティは市役所経営にとって重要な施策であることを経営層に知っていただきたい。

情報セキュリティとは

情報セキュリティという言葉は知っていても、人に説明できる職員は少ないのではないだろうか。情報セキュリティを人に説明する際には情報保護との違いを伝えると理解が得やすい。情報保護とは文字通り、適切な方法で集めた情報をしっかりと処理・管理することであるのに対して、情報セキュリティとは集めた情報を利用することを前提に効用を確保するために脅威から守ることをいう。

つまり情報セキュリティとは情報を利用することが大前提であり、入札予定価格や職員の処罰情報など情報保護が優先される情報に対して、市民の情報や測量・調査データなど市役所が保有する多くの情報は活用するために集める情報であって、市民や事業者は利活用を期待して申請や届け出を行い、行政も費用をかけてでも測量や調査を行うのではなかろうか。

一方で利用するためには、鍵のかかる書庫に閉まっておくだけでは済まない。特に複数人が共有する情報においては、それぞれの職員が必要な時に最新の正しい情報を入手できるようでなければいけない。その際に関係のない人が情報を見たり、改ざんしたりすることがないように施すことも必要である。

利用する際に効用を高め、一方でリスクに対処する、これゆえに情報セキュリティは難しいのであって、情報化の進展とともに改善を繰り返さなければならないものである。

自治体にとってのサイバー攻撃とは

情報セキュリティと似た言葉にサイバーセキュリティがある。情報セキュリティがリアルの世界での対策も含めるのに対して、サイバーセキュリティはデジタルデータを対象としている。市役所のデジタル化が進むほどにサイバーセキュリティの比重が重くなるのは当然のことである。

サイバー攻撃とはネットワーク経由で情報を盗んだり、業務を妨げたりする攻撃のことであり、昨今ではサーバに保管されているファイルを暗号化して、復旧と引き換えに金銭を要求する「ランサムウエア攻撃」や、大量のデータを送り付けてサーバに障害を起こす「DDoS攻撃」などがある。

サイバー攻撃の多くは特定の国や企業などを標的にしたもので、日本でも名だたる大企業が被害に遭っている。市役所の関係では市民病院や教育委員会、図書館などが被害に遭っており、業務が滞るだけでなく、手術や

診療ができなくなることで、人の命にまで関わる重大な脅威となっている。

首長部局で大きな被害が出ていないのは、平成27年に日本年金機構や長野県内の自治体がサイバー攻撃に遭い、同年にマイナンバー制度が始まることもあり、全国自治体に強靱化策（三層分離）が徹底されたことが大きい。

今日に至ってもインターネットの脅威から自治体の業務を守るよう総務省ではガイドラインで三層分離を原則としてはいるものの、新型コロナ禍を経て、業務の一部をインターネットと接続するパソコンでできるモデル（βモデル）を提示したり、クラウドサービスでの情報交換を認めたりするなど、インターネット活用は市役所業務に浸透しつつある。

インターネットのサービスを利用する際には、情報セキュリティが担保されているかどうか、経営層から確認することが重要である。

市民の信託を得るために

地震大国であり、ゲリラ豪雨が頻発する日本では、いつどこで大きな被害が起こるのかを予測するのは困難である。以前は自自治体が被災した際の対策で済んでいたものの、デジタル社会においては、データセンターの立地や通信、電力にまで気を配らねばならなくなった。

情報セキュリティでは情報を保全するために不可欠な基本概念を「機密性」「完全性」「可用性」という三つの要素で表す。「機密性」とは許可されたものだけが情報にアクセスできる状態にすること、「完全性」とは情報を正確かつ完全な状態に保つこと、そして「可用性」とは必要な時に情報を利用可能な状態にしておくことである。これらいずれかが欠けてしまうと情報を正しく処理することができなくなってしまう。

自然災害とサイバー攻撃のいずれにおいても「可用性」は脅かされる。自然災害においては通信や電力が途絶えてしまう、サイバー攻撃においては発覚時に被害を大きくしないためネットワークから切り離すためである。職員が利用する情報機器にあっては、BCPに従って復旧を待つしかないのであろうが、昨今では市民や利用者向けのアプリやSNSを活用したサービスが増えている。特に情報発信を主とするサービスにおいては「可用性」が第一と考える。始めたサービスが効用を高められているか、経営層にはその視点からのチェックも求められている。

また、自然災害にしてもサイバー攻撃にしても被害が大きくなれば「可用性」のみならずデータ流失という「機密性」やデータ喪失といった「完全性」も脅かされる。東日本大震災では被災自治体のサーバが水没して、職員が総出でデータを再入力したことや、日本年金機構へのサイバー攻撃では125万件もの年金データが漏えいして、当時のトップが責任を取って辞任したことなど、情報セキュリティをおろそかにすることが自治体経営そのものに影響を与えることは過去の事件・事故から読み取れる。

何よりも市役所が保有する情報の多くが市民や利用者、事業者などが提供したものである。彼らは市役所を信用して情報を提供しているのであるから、その情報をいいかげんに扱うと市民などからの信用を失うこととなる。市民からの信託を受けた経営層には、信用を確保すべく情報セキュリティ対策に関心を示していただきたい。

筆者プロフィール

髙橋邦夫（たかはし くにお）

1963年東京都豊島区生まれ。埼玉大学教育学部卒業。豊島区情報管理課長、税務課長、最高情報セキュリティ統括責任者（CISO）を経て2018年3月退職。合同会社KUコンサルティング設立。総務省地域情報化アドバイザー、総務省テレワークマネージャー、文部科学省学校DX戦略アドバイザー、J-LIS地方支援アドバイザーなど、これまでに全国250を超える地方自治体の支援を行ってきた。文部科学省「教育情報セキュリティポリシーに関するガイドライン」改定検討会座長、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係る検討会」委員などを歴任。2015年「情報化促進貢献個人等表彰」、2022年「情報通信月間記念式典」において総務大臣表彰受賞。2024年情報セキュリティ大学院大学より「情報セキュリティ文化賞」受賞。著書に『DXで変える・変わる自治体の新しい仕事の仕方』『全体最適の視点で効果を上げる自治体DXの進め方』など