都市のリスクマネジメント

第182回

自治体が情報セキュリティポリシーを策定する意義

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

4月号に引き続き本コーナーに「自治体情報セキュリティ」をテーマとした寄稿をさせていただく。前回は一般論として、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記したが、今号以降は情報セキュリティ対策を効果的に行うための組織の在り方と経営層の関与について書いていきたい。

情報セキュリティポリシーとは

情報セキュリティを高めるためには「多層防御」「多重防御」といった複数の対策を組み合わせることが有効である。対策を大別すると「物理的対策」「技術的対策」「人的対策（組織的対策）」という三つないし四つに分けることが知られているが、どんなに強固な部屋や高価なセキュリティ製品を調達しても、職員がルールを知らずにドアを開け放したり、管理者用パスワードを単純なものにしてしまったりしては効果がないどころかリスクとなってしまう。この点から私は人的対策が最も重要だと考えている。ただし職員各自の情報リテラシーを高めたとしても、それぞれがバラバラに対策を講じるのは非効率である。また、対策を組み合わせれば組み合わすほど、ルールをしっかり作成しないと職員は途方に暮れてしまう。

そこで情報セキュリティのルールブックである情報セキュリティポリシーを策定し、組織の誰もがポリシーに書かれたルールに従うことで、導入した対策の効果を高めるのである。「情報セキュリティポリシーは情報システム担当者の読み物」だと勘違いしている職員を多数見かけるが、全ての職員が一読して頭に入れておくことが重要であり、人的対策の最たるものは情報セキュリティポリシーを組織の全職員に理解させることだと考える。

総務省のガイドライン

パソコンが普及し、パソコンを使っての仕事と成果物をサーバに保管するスタイルが確立してきた平成12年、国は政府機関職員向けの情報セキュリティポリシーを策定した。これを受けて総務省では、地方自治体が情報セキュリティポリシーを策定する際に参考となる「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」（以下、ガイドライン）を翌年に発行する。

総務省の働きかけにより、現在ではほぼ全て（99％）の自治体が情報セキュリティポリシーを策定している。このことは大変喜ばしいことではあるが、デジタル社会の進展は目まぐるしく、総務省もここ数年は毎年度ガイドラインの改定を公表している。一方の自治体では毎年改定する余裕はなく、中には10年以上変わっていない自治体もあると聞く。個人的には毎年変える必要はないと思ってはいるものの、大規模なパソコンの置き換えやネットワーク機器の更新を行った際には、新たな機器が有効に使われるよう情報セキュリティポリシーを見直すべきだと考える。

なお、情報セキュリティポリシーは「基本方針」「対策基準」「実施手順」という3段構成で成り立つものである。前者二つは組織単位（市役所の場合は首長部局用、学校現場用、市民病院用など）で、「実施手順」は職場ごと、システムごとに作ることが望ましい。総務省のガイドラインは前者二つを対象としており、「実施手順」においては情報システム部門がひな形を作り、各職場で管理職員を中心に定期的に改定することとなっているが、徹底されている自治体は少ないと見ている。

閉ざされた空間で働く職場、カウンターに面した職場、外部の団体と共に働く職場など働く環境はさまざまなので、それぞれに適したセキュリティ対策を考え、決めたルールを「実施手順」に落とし込んでいただきたい。

経営層の関与なしに効果は生まれない

そもそも総務省が策定したガイドライン通りに情報セキュリティポリシーを策定すべきなのかというと、私はそうは思っていない。情報セキュリティポリシーの肝となる組織体制にあっても、自治体ごとに適任者を充てるべきであって、CISO（最高情報セキュリティ責任者）に相応しい人物がいるのであれば、必ずしも副市長を充てる必要はないし、機器を外部に持ち出す際に情報担当部長の許可を得ていてはスピード感に欠けるのであれば、課長の許可に変えればよい。ガイドラインの第1編に書かれている概念を理解し、第3編の解説を読みつつ、第2編の例文を自組織に合わせて変更するかどうかを判断すればよいのである。

何よりも大切なことは、情報セキュリティポリシーが市役所の目指す行政サービスと足並みが揃っているかどうかを確認することである。例えば、アウトリーチ型の住民サービスを目指している自治体の情報セキュリティポリシーが「情報機器の持ち出しは禁止」を原則として、職員の庁舎外での活動に制限を掛けるルールとなっていたらどうであろうか。担当職員は該当者の情報を紙で持ち歩くリスクを抱えざるを得ず、紙に書かれていること以外の相談を受けた場合は追って回答しなければならない。これで市役所の目指す行政サービスが実現できるのであろうか。

また本テーマであるリスクマネジメントにおいても、市役所ごとに抱えているリスクはまちまちであり、時にはガイドラインに書かれていない対策が必要となる場合もある。東日本大震災では津波による情報の流失が、胆振東部地震ではブラックアウトによる丸2日に及ぶ広域大規模停電が発生した。これらを経験したわれわれは市役所が保有している情報資産を洗い出し、それらが抱えるリスクを考えたうえで、そのリスクに備えた対策を練ることが求められている。

このように情報セキュリティ対策は市役所の行政運営をつかさどる重要な施策の一つであり、情報セキュリティ対策が網羅されている情報セキュリティポリシーは情報システムの担当者だけで策定するものではなく、経営層の関与を経て策定され、全ての職員に周知しなければならないものである。

本コラムをお読みになった経営層には市役所が目指す行政サービスと情報セキュリティポリシーとの足並みが揃っているかどうか、これを機に再確認していただきたい。

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