都市のリスクマネジメント

第186回

自治体における情報セキュリティ監査

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回目となる本コーナーへの寄稿では、リスクマネジメントの重要ツールである「情報セキュリティ監査」をテーマに、自治体がセキュリティ監査を行うことの効果と課題を明らかにし、経営層の関わりについても述べさせていただきたい。

情報セキュリティ監査の効果

そもそも情報セキュリティ監査とは、組織が保有する情報資産を守るために、適切な対策が講じられているかを第三者の視点で評価するプロセスのことを言う。情報セキュリティ監査にはさまざまな手法が用いられるが、自治体においては総務省が発出する「地方公共団体における情報セキュリティ監査に関するガイドライン」がよりどころとされており、そこでは「準拠性監査（自自治体のルールに沿った運用となっているか）」と「妥当性監査（自自治体のルールが国のガイドラインや取り巻く状況等に照らし妥当かどうか）」が示されているが、私の見立てでは、多くの自治体が「準拠性監査」を行っている。

自治体が情報セキュリティ監査を実施することで得られる最も大きな効果は「行政サービスの継続性を確保する」ことに他ならない。

近年どこで起きても不思議はない自然災害や狙われたなら完全防御は不可能と言われるサイバー攻撃など、予期せぬ事態に直面した際、情報セキュリティ監査を実施している自治体では、迅速な対応を取ることができると言われる。監査の実施によりリスクが事前に把握されていることで、迅速に行動に移すことができ、被害を最小限に抑えることで、公共サービスの継続性（もしくはいち早い復旧）を確保することが可能となる。

さらには「住民からの信頼性の向上」を得ることにつながる効果もある。自治体が定期的に情報セキュリティ監査を行っていることを公表することで、住民の市役所に対する信頼が高まり、安心して行政サービスを利用すること、つまりは行政サービスへの積極的な参加に通じることとなる。特に個人情報保護の観点では、機微情報を取り扱う税務部門や福祉部門などにおいて情報セキュリティ監査を実施することは、住民の権利を守るという観点のみならず、安心して情報を提供してもらえることで、より親身になった住民サービスを創出することへとつながっていく。

さらには「効率的な業務運営とコスト削減」といった効果も考えられる。監査を通じて無駄な情報管理やシステムの改善点を洗い出すことで、業務の効率化を図ることができる。また、セキュリティインシデント（事件・事故）が発生した際の対応コストを考えると、コスト削減という視点で監査の効果を測ることも可能だと考える。

情報セキュリティ監査の課題と解決策

一方で情報セキュリティ監査を実施するに当たっての最も大きな課題として、財政的な制約がある。情報セキュリティ監査には情報システムと行政事務の双方に詳しい専門家を擁する監査法人等との契約が望まれる

だけでなく、監査結果を踏まえた改善措置などに費用を要するからである。財政的に余裕がない自治体では、必要性は理解していても監査が後回しにされる可能性があり、それがセキュリティ上のリスクを増大させることにつながってしまうこととなる。

このような現状を踏まえ、総務省では外部監査と内部監査とを使いこなすようガイドラインに謳っている。外部監査が自治体職員ではない専門家などによる監査であるのに対して、内部監査は自治体職員が自部門でない部門に赴いて監査を行う形態である。機微情報を扱う部門などに外部監査を実施しつつ、そこでノウハウを身に付けた職員が内部監査を行うことで、少ない費用で多くの部門の監査を行えるようになる。

しかしながら、内部監査を組み込む際には、技術的な課題として、監査対象となるシステムやソフトウエアの複雑化が進む中、監査を行う職員に最新技術への対応が求められることが挙げられる。技術的な知識が不足している場合、脆弱性を見落としてしまうリスクが高まることから、継続的な技術アップデートが必要となり、リソースの確保が顕在化してきている。このことへの対策として、大規模な監査を実施して終わりにするのではなく、5年程度で全ての部門に監査が当たるようにすることがポイントとなる。短いサイクルで何度も監査を受けて改善策を取ることで、組織全体での意識改革が進み、結果を基にした継続的な改善プロセスが全体で構築されるようになる。

経営層の関与なしに効果は生まれない

経営層が情報セキュリティ監査に関わる方法としては、経営層が情報セキュリティの重要性を理解し、組織全体にその意識を浸透させる役割を担うことである。具体的には、定期的な監査を通じてその有効性を評価し、市役所が現時点で抱えている情報セキュリティリスクを認識し、必要な対策を講じるためのリソースを確保することである。

先に述べたように、自治体においては財政的制約と人材育成の点から、外部監査と内部監査を使いこなす必要があり、さらには5年程度で全ての部門を対象に監査を実施するには、経営層のリーダーシップによって、内部監査が実施できる人材を早期に育成しなければならない。多くの職員が最新のセキュリティ対策を理解し、他部門に対して指摘できるようになること、一方で他部門の優れた点を自部門に生かせるように持ち帰ること、このような組織が構築されたならば、多大な費用をかけることなく組織全体の情報セキュリティレベルを向上させることが可能となる。

自治体における情報セキュリティ監査は、住民からの信頼を向上させて、行政サービスの継続性を確保するために欠かすことのできない取り組みである。しかし、人的資源や財政的制約、技術的な課題など、さまざまな困難が伴うことから、これらの課題を解決するために、国や地域間での協力体制を構築し、専門人材の育成や監査プロセスの標準化を進めることが求められている。

本コラムをお読みになった経営層には自自治体での情報セキュリティ監査に関心を寄せていただき、どのような監査結果が報告されたのかを知った上で、その指摘を全ての部門が自分ごととするよう、市役所全体へと波及させる指導を行っていただきたい。

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