市川市における電子自治体への取り組み

第7回 情報セキュリティマネジメントへの取り組み

井堀幹夫 市川市CIO（情報政策監）
text by Ihori Mikio

情報化の進展で問われる情報セキュリティマネジメント

今日、情報化が進展し、行政が利用する情報システムは、以前のように業務単位の個別システムで構成されるクローズドな形態から、業務や組織に関係なく多くの関係者が連鎖するオープンなネットワーク型の形態に変化してきている。インターネットが普及したことで、市民も、地域や行政の情報に直接アクセスすることができ、行政手続などの電子サービスを受けることができるようになった。このように、誰もが利用できるネットワーク型の情報システムが普及してきたことで、情報の管理、情報の伝達、情報の公開に関しては、これまで以上に高度化した情報セキュリティマネジメントが問われるようになってきたと言える。

市川市においては、これまで、「電子計算組織に係るデータ保護に関する規程」、「個人情報保護条例」、「情報資産に係る情報セキュリティに関する規程」などにより個人情報保護と情報セキュリティに対応してきた。

しかし、情報化の進展に伴い、さらに情報セキュリティマネジメントの精度を高めるために、全国の地方自治体で初めて情報セキュリティマネジメント（ISMS適合性評価制度）の認証を取得し、「個人情報保護条例」を改正し、「住民基本台帳の一部の写しの閲覧に係る事務の適正な運用に関する条例」を制定するなど、情報管理に関する対策の強化を図ってきた。

情報セキュリティに関する基本的な考えと戦略

紙媒体や電子化された情報など、すべての情報の取り扱いについて、技術面での取り組みだけではなく、職員一人ひとりの心構えや、普段の行動の中でセキュリティに対する取り組みを強化しなければならない。それは、情報セキュリティ対策は、「技術面の対策」と「運用面の対策」が車の両輪であり、この両面の対策が整ってこそ、セキュリティの確保が実現できるからである。

情報セキュリティを維持するためには「PDCAサイクル」が大切だと言われている。プラン（Plan）すなわちセキュリティ対策の計画を立て、実行（Do）し、定期的に見直し（Check）を図り、改善を実施（Action）する、という一連のサイクルを続けていくことであるが、これを続けることによって「スパイラルアップ」、すなわち、らせん階段を上っていくようにどんどん情報セキュリティマネジメントの取り組みを向上させていくことができる。

情報セキュリティマネジメントに関して、首長がリーダーシップを発揮しやすい環境を整備し、外部のセキュリティ審査機関からのチェックを通じて、常に緊張感を維持できるようにしている。このことは、市民からの信頼性も高まり、情報セキュリティマネジメントを向上させる戦略としても効果的である。

情報セキュリティ対策の進め方

①適用範囲の決定と情報資産の洗い出し

情報セキュリティマネジメントは、その適用範囲を明確にしなければならない。適用範囲が決定したら、そこにはどのような情報資産があるのかを洗い出しする。情報資産とは、業務で使用する申請書、台帳、その他の帳票などに記録されている情報だけでなく、情報機器などハードウエアに関するもの、ソフトウエアに関するもの、サービスに関するものが含まれる。

そして、情報は、個人情報に限定したものではなく、業務で利用される全ての情報資産が対象となる。洗い出された情報資産は、適切に管理するために管理台帳を作成し、情報資産台帳として、情報資産名、関連業務、保存場所、保存期間、管理責任者、記録媒体などを記録しておく。

どこに、どのような情報が、どれだけあるのか。その情報資産を誰がどのように管理しているかを把握するのが、ここでのポイントである。市川市では、現時点において14,904種類の情報資産が管理されており、その適用業務は、税や福祉、保健、戸籍、教育、救急消防など基幹業務の大半が含まれている。

②情報セキュリティリスクの把握

洗い出された情報資産は、資産としての価値や脅威、脆弱性について、そのリスクを分析し把握する必要がある。これをリスク分析評価というが、一定の基準を設けて評価結果を数値化することで、判断基準がぶれないように分かりやすく表現することが大切である。

市川市では、情報資産の価値を判断するに当たって、情報資産の重要性を3段階に分類しランク付けを行うこととした。3段階に区分された情報資産は、「機密性」、「完全性」、「可用性」のそれぞれの観点から評価を行う。機密性とは、情報へのアクセスが許されない者には、絶対にアクセスできないようにすること。完全性とは、正確な情報や正確な処理方法を確保すること。可用性とは、情報へのアクセスを許可された者が、必要なときに確実にその情報を利用できるようにすることである。

また、情報資産には、どのような脅威があるかを把握する。脅威は意図的（故意）によるもの、偶発的（故障・過失）によるもの、環境的（自然）によるもの、この3タイプに区別できる。市川市では、すべての情報資産

に対して、地震や火災、盗難、紛失など51種類の脅威を想定して、その可能性を検証した。脅威のランク付けの基準についても3段階として、意図的に発生する脅威に関しては、発生要因が安易であるか、困難であるかで1から3にランク付けし、偶発的な脅威や環境的な脅威に関しては、発生頻度の高い場合にランク3を設定するなど1から3段階にランク付けした。

こうして、情報資産の脅威が明らかにされると、次に、脆弱性について把握する。脆弱性は、施錠設備や電源など物理的なもの、暗号化や設定など論理的なもの、研修や契約など管理的なものなど3つの観点で3段階評価をする。3つに分類された脆弱性については、対策を実施しているのか、手順書はあるのかといった評価指針に関して1から3までのランク付けを行う。

> リスク値 ＝ 情報資産の価値のランク値×
> 脅威の総合ランク値×脆弱性総合ランク値

リスク値の計算式はこのように表されるが、それぞれのランク値が1～3であるため、リスクの最高値は27となる。ここで重要なことは、情報資産が認識できること、それに内在するリスクが可視化されることである。ここで算出されたリスク値はリスク管理シートに記録する。

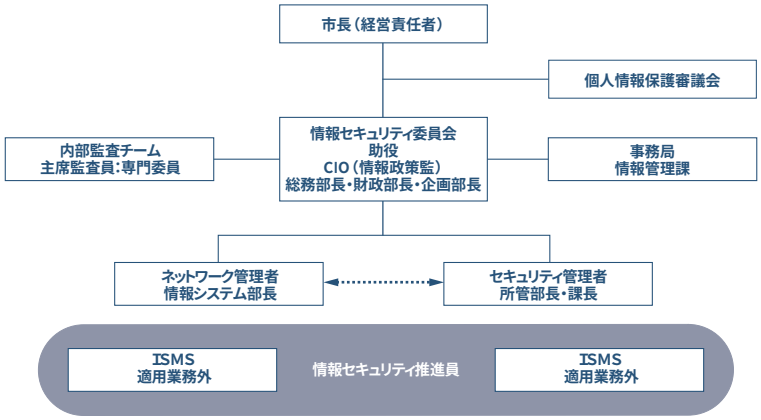
③リスクの特定と低減化

すべての情報資産に対して、リスク値が算出されると、次は、リスク値が高い情報資産を特定して、今後どのような計画で、その高いリスク値の情報資産のリスクを下げていくかに目を向けなければならない。

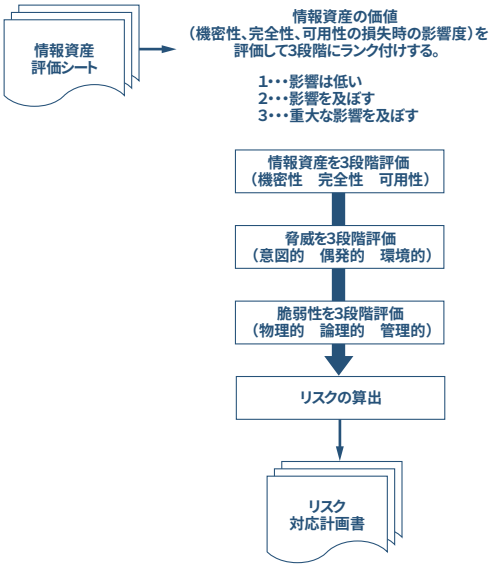
リスク対応計画は、情報セキュリティ委員会で計画内容を精査し、経営責任者である首長の承認を得て計画を実行することになる。計画された情報セキュリティ対策は、市川市の総合5カ年計画とも整合を図り、予算や人員確保などに関して計画達成に支障がないよう対応されることが重要である。

資料　市川市の情報セキュリティマネジメント

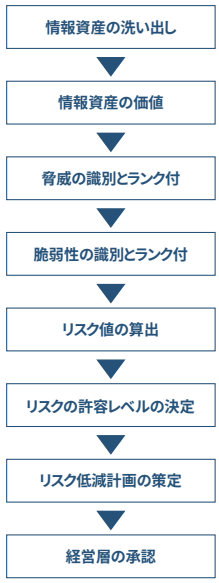
■ 情報セキュリティマネジメント体制



■ 情報資産のリスク分析評価



■ 情報セキュリティマネジメントの進め方



市川市役所作成

人材を組織内で効果的に活かせるような組織づくりをすることが大切である。

それには、自治体CIOによるマネジメントの役割が問われる。自治体CIOは、行政能力とIT能力に関するスキルと経験を持ち、行政経営改革に関するプロジェクトの編成と発足、軌道修正などに関与し、しかも、総合的な危機管理にも関与するスペシャルスタッフでもあるべきである。

今や、自治体の仕事の多くは、人々の考えを実行するために、何らかの情報システムと関わっている。情報システムは仕事のインフラストラクチュアであるとも言えるが、その情報システムのガバナンスは、自治体CIOが関与することで、より安心・安全な行政システムにつながなければならないのではないか。

今後、地方自治体は、分権時代を見据えて、ますます、情報セキュリティマネジメントの精度を高めていく必要がある。これからは、住民をはじめ地域の団体等との深い信頼関係にもとづいた都市経営の設計と構築が求められることを認識の上に取り組まなければならない。

課題と今後の展望

適切な情報セキュリティマネジメントのためには、情報ガバナンスへの対応が大切である。組織の目標を明確にして戦略的に計画性をもって取り組まなければならないが、そのためには、目標達成のために従事する

1948年大阪府生まれ。1972年市川市役所入庁。1992年同企画部企画課主幹・課長補佐。総合計画の策定、CATV会社・コミュニティFM会社の設立、HP開設、庁内LAN構築等を担当。1999年同企画部情報システム課長。360システム構築、イントラネットシステム構築、いちかわ情報プラザ開設等を担当。2003年同情報システム部長。2005年同CIO（情報政策監／現職）。2004年度に財団法人地方自治情報センターより情報化職員個人特別表彰。