第５章　情報セキュリティとその対策

１　情報セキュリティの考え方

本市は、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、ほかに代替することができない行政サービスを提供しています。また、業務の多くが情報システムやネットワークに依存していることから、住民生活や地域の社会経済活動を保護するため、情報セキュリティ対策を講じて、その保有する情報を守り、業務を継続することが必要となっています。

今後、各種手続のオンライン利用の本格化や情報システムの高度化等、電子自治体が進展することにより、情報システムの停止等が発生した場合、広範囲の業務が継続できなくなり、住民生活や地域の経済社会活動に重大な支障が生じる可能性も高まります。また、LGWAN 等のネットワークにより他の自治体と相互に接続しており、一部の団体で発生した IT 障害がネットワークを介して他の団体に連鎖的に拡大する可能性は否定できません。

これらの事情から、情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくことが必要となっています。また、情報セキュリティの確保に絶対安全ということはないことから、情報セキュリティに関する障害・事故及びシステム上の欠陥（以下「情報セキュリティインシデント」という。）の未然防止のみならず、情報セキュリティインシデントが発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要です。

２　情報セキュリティの維持

情報セキュリティ対策を徹底するには、対策を組織的に統一して推進することが必要であり、今後も引き続き、組織として意思統一し明文化された文書である本市の情報セキュリティポリシーにより対策を実行していきます。

なお、情報通信技術を活用した行政の推進等に関する法律（平成 14 年法律第 151 号）第 13 条第１項は、「地方公共団体は、情報通信技術を活用した行政の推進を図るため、条例又は規則に基づく手続について、手続等に準じて電子情報処理組織を使用する方法その他の情報通信技術を利用する方法により行うことができるようにするため、必要な施策を講ずるよう努めなければならない。」と規定しています。また、「サイバーセキュリティ基本法」第５条では、地方公共団体においてサイバーセキュリティに関する自主的な施策の策定と実施が責務規定として法定化されています。

このことから、本市においても、職員研修を継続して実施するとともに、情報セキュリティポリシーの遵守及び適時適正な見直しを行い、情報セキュリティレベルの維持に努めます。