

第5章

情報セキュリティ対策の推進

5.1 情報セキュリティ対策の強化

サイバー攻撃が急速に複雑・巧妙化している中、情報セキュリティの強化は継続した課題であり、上田市においても、資産管理システムの導入やウイルス対策など、情報漏えいを未然に防ぐための各種セキュリティ対策を実施してきました。

市が取り扱う情報には、市民の個人情報をはじめ行政運営において重要な情報など、外部への漏えいが発生した場合には極めて重大な被害を招く情報が多数含まれており、市民の個人情報などを守り、また、行政事務の安定的な運営のためにも情報セキュリティ対策の強化は必要不可欠です。

今後も、サイバー攻撃などのさまざまな脅威や情報漏えいに対応するため、システム及びネットワークの障害監視など、技術的・物理的なセキュリティ対策を強化していきます。

また、人為的なミスによる情報セキュリティ事故を防止するため、情報セキュリティに関する内部監査などを毎年実施するとともに、研修などを通じて、職員の情報セキュリティ意識の向上や情報リテラシー*の向上に取り組んでいきます。

5.2 情報セキュリティポリシーの運用

上田市が保有する個人情報や行政運営において重要な情報などの情報資産を守るため、情報セキュリティ対策について基本的な事項を定めた「上田市情報セキュリティポリシー*」に基づき、庁内の情報セキュリティの確保に努めてきました。

また、国において、社会情勢の変化、新たな情報機器、サービス及び脅威などに対応して、情報セキュリティポリシーのガイドラインを策定しており、上田市においても、これに合わせ情報セキュリティポリシーの改定を行ってきました。

今後も、国のガイドラインの改定に伴い、情報セキュリティポリシーも見直しを図るとともに、情報漏えいなどの危険を防止し、安全・安心な運用を行うため、計画(Plan)、実行(Do)、評価(Check)、改善(Action)のPDCAサイクルに基づき運用を進めていきます。

5.3 個人情報保護の徹底

これまでも、個人情報については、「上田市個人情報保護条例」に基づき適切に取り扱っていますが、引き続き、適正な利用や安全管理措置の徹底を図る必要があります。

今後、各施策の推進に当たっては、個人情報の取扱いについて、法律、条例、情報セキュリティポリシーを遵守するとともに、個人情報保護の徹底を図ります。

更に、マイナンバーカード*の利活用を促進していくことから、「行政手続における特定の個人を識別するための番号の利用等に関する法律」など関係法令に基づき、特定個人情報*の取扱いについても、引き続き、適切な安全管理措置を講じるとともに、マイナンバー*を利用する職員に対しては、特定個人情報の取扱いに関する研修を実施し、特定個

個人情報ファイルを取扱う部署においては、特定個人情報保護評価を実施し記載事項の見直しを行います。

また、個人情報を取り扱う際に外部委託が生じる場合にも、委託を受けた者に対し市と同等のセキュリティ管理対策に関する項目を盛り込んだ契約を締結することにより、個人情報の適正な取扱いを確保します。

