情報化安全対策事業

1. 人的な対策

(1) 情報セキュリティポリシーの周知

サイバー攻撃や情報漏洩事件の増加に対し、庁内における情報セキュリティ体制の強化と遵守の徹底を図るため、本市情報セキュリティポリシー※の改定や情報セキュリティ実施手順※の作成を行うとともに、全庁的に周知を図った。

また、情報セキュリティについての全庁的な研修やeラーニング※を実施した。

◆情報セキュリティ研修 … 実施日：平成27年8月26日、受講人数：255人

◆eラーニング … 実施時期：平成27年7月～12月、受講人数：延べ19人

※ eラーニング … 主にインターネットを利用して、パソコン等で行う学習形態のこと。

※ 情報セキュリティポリシー … 河内長野市が所掌する情報資産に関する情報危機管理として、情報セキュリティ対策を総合的、体系的かつ具体的に取りまとめたもの。

※ 情報セキュリティ実施手順 … 情報セキュリティポリシーに基づき情報セキュリティ対策として遵守すべき事項の具体的な実施手順を定めたもの。

(2) 情報セキュリティポリシーの遵守確認

情報セキュリティポリシーを遵守できているかを確認するために、情報セキュリティ自己チェック及び情報セキュリティ内部監査等を実施し、情報セキュリティポリシー遵守の徹底に努めた。

◆情報セキュリティ自己チェック … 実施時期：平成27年8月、実施人数：966人

◆情報セキュリティ内部監査 … 実施時期：平成27年11月、実施対象部署数：2課

(3) 職員への注意喚起・啓発

人事異動の際や年末年始におけるパソコンなどの取扱いや不審なメールを受信した場合の取扱いについての注意喚起など、庁内ネット等を通じて、職員へ情報セキュリティ対策の啓発を行った。

2. 技術的な対策

(1) ウイルス対策

ウイルス感染の脅威からパソコン等を守るため、ウイルス対策ソフトの適用や安全な設定更新を行った。

(2) セキュリティ関連機器の管理

ファイアウォール※やメール、インターネット接続関連機器の運用を行い、庁内ネットワークの安全性を保った。また、サーバ室の出入りに認証機器を設置し、特定の者だけが入退室可能とするとともに、入退室の記録を取得し、厳格な入退室管理を行った。

〔 ※ ファイアウォール … 組織内のコンピュータネットワークへ外部から侵入されるのを防ぐ装置。 〕

3. データ保管及び廃棄

データの消滅防止を図るとともに、事故や災害発生時の被害を最小限に抑えるため、住民情報システム、財務会計システム、文書管理システム、ファイルサーバなど主要なシステムについて日々データのバックアップを実施したほか、それらを定期的に遠隔地へ保管するなどの対策を行った。

また、不要となったCD-ROM、ハードディスクなど、記録媒体の廃棄物からの情報漏えいを防ぐため、専門の事業者への委託により、適正に廃棄処分した。