柏原市情報セキュリティに関する基準

情報セキュリティ基本方針

1.1 目的

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。
柏原市においても市民の個人情報や自治体としての運営上重要な情報などを多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。このため、これらの情報資産を様々な脅威から防御することは、市民の権利、利益を守るため、行政の安定的、継続的な運営のためにも必要不可欠である。また、本市には、地域全体の情報セキュリティ基盤を強化していく役割も期待されている。これらの状況を鑑み、本市における情報資産に対する安全対策を推進し、市民からの信頼を確保し、さらに地域に貢献するため、柏原市情報セキュリティに関する基準（以下「情報セキュリティポリシー」という。）のうち基本方針は、地方自治法（昭和２２年法律第６７号）第２４４条の６第１項に規定するサイバーセキュリティを確保するための方針として、本市が保有するコンピュータ、情報システム、ネットワーク及びこれらで取り扱うデータ等（以下「情報資産」という。）の機密性、完全性、可用性を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

1.2 構成

情報セキュリティポリシーは、情報セキュリティを確保するための対策について総合的、体系的かつ具体的に取りまとめたものとして、柏原市の全職員（会計年度任用職員及び臨時的任用職員を含む。）に浸透、普及及び定着させるものであり、一定の普遍性をもった部分（情報セキュリティ基本方針）と、技術水準等情報セキュリティに関する社会状況の変化を的確に反映させるべき部分（情報セキュリティ対策基準）の２章で構成するものとする。

1.3 定義

情報セキュリティポリシーの用語の意義は、当該各号に定めるところによる。

① ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

② 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、これら全体で業務処理を行うものをいう。

③ 情報通信機器

コンピュータ、ネットワーク及びこれらの運用に必要な機器をいう。

④ 電磁的記録媒体

情報システムでデータ等を電子的方式、磁気的方式及びそれ以外の人の知覚によって認識できない方式で記録するための媒体であって、ハードディスク、フロッピーディスク、ＣＤ、ＤＶＤ、ＵＳＢメモリー、磁気テープ等をいう。

⑤ 情報セキュリティ

情報資産の機密性、完全性、可用性を維持することをいう。

⑥ 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

⑦ 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

⑧ 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

⑨ 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

⑩ マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）に関わる情報システム及びその情報システムで取り扱うデータをいう。

⑪ LGWAN 接続系

庁内情報及び財務会計等の LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう。（マイナンバー利用事務系を除く。）

⑫ インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

⑬ 通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

⑭ 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウィルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

⑮ 職員等

職員(任期付職員及び再任用職員を含む)、会計年度任用職員及び臨時的任用職員等をいう。

1.4 情報セキュリティの確保

情報セキュリティを確保するための対策は、対象となる情報資産の重要度に応じ、的確かつ

効率的に行われるようにしなければならない。

1.5 情報資産への脅威

情報資産に対する脅威の発生度合や発生した場合の影響に照らし、情報セキュリティポリシーで想定する脅威は、次の各号のとおりとする。

①不正アクセス、ウィルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい、破壊、改ざん、消去、重要情報の詐取、機器及び媒体の盗難、内部不正等。

②職員等、委託者又は第３者による情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等。

③地震、落雷、火災等の災害及び事故、故障等によるサービス及び業務の停止。

④電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等。

⑤大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等。

1.6 対象範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局及び地方公営企業とする。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

① ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

② ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

1.7 情報セキュリティ対策

前記 1.5 の脅威から情報資産を保護するために、次の各項に掲げる対策を講ずるものとする。

（１）組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（２）情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（３）マイナンバー利用事務系、LGWAN 接続系及びインターネット接続系の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

① マイナンバー利用事務系においては、原則として、他の領域との通信をできないように

した上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

② LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③ インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（4）物理的セキュリティ対策

情報通信機器を設置する施設への不正な立入り、損傷、盗難等から情報通信機器を保護するために、入退出管理等の物理的な対策を講ずる。

（5）人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、又職員等が遵守すべき事項を定めるとともに教育及び啓発を行う等の人的な対策を講じる。

（6）技術的セキュリティ対策

コンピュータ等の管理、アクセス制御、ウィルス対策ソフト等の不正プログラム対策、不正アクセス対策、ログ確認等の技術面の対策を講ずる。

（7）運用におけるセキュリティ対策

情報通信機器の定期的な保守・監視、情報セキュリティポリシーの遵守状況の確認、緊急事態に備えた連絡体制の構築等の制度運用面の対策を講じ、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（8）業務委託と外部サービス（クラウドサービス）の利用

業務委託する場合には、業務委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、業務委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス）を利用する場合には、利用にかかる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（9）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

1.8 情報資産所管課等の長の責務

（1）情報資産所管課等の長は、当該情報資産の管理責任を有する。

（2）情報資産所管課等の長は、「情報セキュリティ対策基準」に定める留意事項を具体的に実行に移すための手順（以下「実施手順」という。）を定めるものとする。

（3）情報資産所管課等の長は、情報セキュリティポリシー及び前項の実施手順の遵守状況を適宜点検するものとする。

1.9 利用課等の長の責務

利用課等の長は、職員等に情報セキュリティポリシー及び実施手順を理解及び遵守させ、情報セキュリティの確保上問題が生じないよう管理、指導するものとする。

1.10 職員等の責務

情報資産を利用する職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティ対策基準に従い、利用する責任を有し又、各情報資産所管課等の長が定める情報セキュリティ実施手順を遵守し情報セキュリティの確保上問題が生じないようにしなければならない。

1.11 情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。