柏市固定資産評価審査委員会情報セキュリティ基本方針

令和８年３月３１日策定

１　目的

本方針は，柏市固定資産評価審査委員会が保有する情報資産の機密性，完全性及び可用性を維持するため，本委員会が柏市情報セキュリティポリシーに準じて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。

２　定義

(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，情報処理を行う仕組みをいう。

(3) 情報セキュリティ

情報資産の機密性，完全性及び可用性を維持することをいう。

(4) 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。

(5) 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。

(6) 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。

(7) ＬＧＷＡＮ接続系

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。

(8) 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。

(9) 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。

(10) 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，コンピュータウイ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。

3 対象とする脅威

情報資産に対する脅威として，以下の脅威を想定し，情報セキュリティ対策を実施する。

(1) 不正アクセス，ウイルス攻撃，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，内部不正等

(2) 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，火災等の災害によるサービス及び業務の停止等

(4) 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

(5) 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

(6) その他柏市情報セキュリティポリシーに規定するもの

4 適用範囲

(1) 行政機関の範囲

本方針が適用される範囲は，次項で定義する本委員会に係る情報資産を有する全ての行政機関とする。

(2) 情報資産の範囲

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

5　書記等の義務

書記及び委員等（以下「書記等」という。）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，本方針に基づき業務の遂行にあたらなければならない。

6　情報セキュリティ対策

上記３の脅威から情報資産を保護するため，柏市情報セキュリティポリシーに準じた以下の情報セキュリティ対策を講じる。

(1) 組織体制

本委員会の情報資産について，情報セキュリティ対策を推進する組織体制を確立する。

(2) 情報資産の分類と管理

本委員会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) 情報システム全体の強靭性の向上

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，柏市情報セキュリティポリシーに準じた次の対策を講じる。

①ＬＧＷＡＮ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。

②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，都道府県及び市区町村のインターネットとの通信を集約した上で，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

サーバ，情報システム室，通信回線及び書記等のパソコン等の管理について，物理的な対策を講じる。

(5) 人的セキュリティ

情報セキュリティに関し，書記等が遵守すべき事項を定めるとともに，十分な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

コンピュータ等の管理，アクセス制御，不正プログラム対策，不正アクセス対策等の技術的対策を講じる。

(7) 運用

情報システムの監視，業務委託を行う際のセキュリティ確保等，運用面の対策を講じるものとする。また，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は柏市情報セキュリティポリシーにおける緊急時対応計画に準じて対応する。

(8) 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には，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，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，利用に係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。

7　自己点検の実施及び方針の見直し

必要に応じて自己点検を実施し，その結果，本方針の見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には，保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し，リスクを検討したうえで，本方針を見直すものとする。