坂戸市議会情報セキュリティ基本方針

1　目的

坂戸市議会（以下「議会」という。）が実施する情報セキュリティ対策に関する基本的な事項を定め、議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ことを目的に坂戸市議会情報セキュリティ基本方針を定める。

また、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する。

2　定義

（1）情報セキュリティ

情報資産を脅威（自然災害、機器障害、悪意のある行為等の損失を発生させる直接の要因をいう。）から保護し、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。

（2）情報資産

情報システム及びネットワークで取り扱う個人情報、行政文書、図面などの情報、OS、ソフトウェア等に関する情報並びに情報システム及びネットワークに関する設備又はその関連文書のことをいう。

（3）情報システム

コンピュータ、ソフトウェア及び電磁的記録媒体で構成された情報処理を行う仕組みのことをいう。

（4）ネットワーク

コンピュータ等を通信回線、ルーター等の周辺装置を用い人やものをつないで情報資産を伝達する仕組みのことを言う。

（5）電磁的記録媒体

電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるものに係る記録媒体のことをいう。

（6）機密性

情報に接続することを認められた者だけが、情報に接続できる状態を確保することをいう。

（7）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。

（８）可用性

情報に接続することが認められた者が、必要なときに中断されることなく、情報に接続できる状態を確保することをいう。

（９）基幹系ＬＡＮ（個人番号利用事務系ＬＡＮ）

個人番号利用事務（社会保障、地方税及び防災に関する事務）又は戸籍事務等に係る情報システム及びその情報システム等で取り扱うデータが使用するネットワークのことをいう。

（10）ＬＧＷＡＮ（総合行政ネットワーク）系ＬＡＮ

ＬＧＷＡＮに接続された情報システム及びその情報システム等で取り扱うデータが使用するネットワークのことをいう。（マイナンバー利用事務系を除く）

（11）インターネット系ＬＡＮ

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等で取り扱うデータが使用するネットワークのことをいう。

（12）議会用インターネット

議会用インターネットメール、議会用文書共有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等で取り扱うデータが使用するネットワークのことをいう。

（13）通信経路の分割

基幹系ＬＡＮ、ＬＧＷＡＮ系ＬＡＮ、インターネット系ＬＡＮ及び議会用インターネットのそれぞれのネットワークを分離したうえで、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コンピュータ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を防止するなどの安全が確保された通信をいう。

（15）職員等

議会が所管する情報資産に関する業務に携わる正規職員、再任用職員、会計年度任用職員、委託事業者等及び労働者派遣契約に基づき議会の業務の処理に従事する派遣労働者等をいう。

（16）外部サービス

議会及び坂戸市行政機関以外の者が一般向けに情報システム（通信回線、配送等を含む）の一部又は全部の機能を提供するものをいう。

（17）クラウドサービス

外部サービスの中で、事業者によって定義されたインターフェイスを用いた、拡張性、柔軟性を持つ物理的又は仮想的なリソースによりネットワーク経由でアクセスできる情報システム等をサービスとして提供するものをいう。

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、外部委託管理の不備、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

4　適用範囲

（1）適用機関の範囲

本基本方針が適用される機関は、議会とする。

（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　情報システム及びネットワーク並びにこれらに関する設備及び電磁的記録媒体

②　情報システム及びネットワークで取り扱う情報（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

④　その他 ISMS に定義される情報資産

5　議員及び職員等の遵守義務

議員及び職員等は、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ポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6　情報セキュリティ対策

対象とする脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（1）組織体制

議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

議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、次の四段階の対策を講じる。

① 基幹系ＬＡＮ（個人番号利用事務系ＬＡＮ）

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止する。

② ＬGWAN（総合行政ネットワーク）系ＬＡＮ

ＬGWANと接続する業務用システムと、インターネット系ＬＡＮ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 インターネット系ＬＡＮ

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 議会用インターネット

MDM（モバイルデバイス管理）の運用等の高度な情報セキュリティ対策を実施する。

（4）物理的セキュリティ

サーバ、情報システム室、通信回線並びに議員及び職員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、議員及び職員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、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの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

議会の業務を受託する事業者（当該事業者から派遣されている者を含む。）及び公的施設の管理を行う指定管理者等（以下併せて「委託事業者等」という。）に当該業務を行わせる場合には、議会が定める情報セキュリティ要件等、セキュリティ対策上、遵守させるべき事項を、委託事業者等の選定要件として提示する。さらに、契約や協定等（以下「契約等」という。）の締結時等に、議会が定める情報セキュリティ要件を契約等事項に明記し、委託事業者等において要件を満たすセキュリティ対策が確保されていることを確認、又は、別途、書面による提出を求める等の措置を講じる。

なお、クラウドサービスの利用に当たっては、利用に関する手順等を定めるとともに、必要に応じて、当該利用の対象とする情報について定める等、規定を整備し、対策を講じる。

（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、適宜情報セキュリティポリシーの見直しを行う。

7　情報セキュリティ監査及び自己点検の実施

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する。

8　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシー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、情報セキュリティポリシーを見直す。

9　情報セキュリティ対策基準の策定

情報セキュリティ対策、情報セキュリティ監査、自己点検及び必要に応じて情報セキュリティポリシーの見直しを実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

なお、当該対策基準は、情報セキュリティ対策の基準を定めるものであり、公にすることにより、議会の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。

10　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、当該実施手順は、関連する情報システム等のセキュリティ対策を具体的かつ詳細に定めるものであり、公にすることにより、関連する業務の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。