

杉並区議会情報セキュリティ基本方針

(令和8年3月19日杉議会第1208号)

目次

- 1 目的
- 2 定義
 - (1) ネットワーク
 - (2) 情報システム
 - (3) 情報資産
 - (4) 機密性
 - (5) 完全性
 - (6) 可用性
 - (7) 情報セキュリティ
 - (8) 情報セキュリティポリシー
 - (9) 内部情報系
 - (10) インターネット接続系
 - (11) 通信経路の分割
 - (12) 無害化通信
- 3 対象とする脅威
- 4 適用範囲
 - (1) 対象機関の範囲
 - (2) 情報資産の範囲
- 5 職員の遵守義務及び違反への対応
- 6 情報セキュリティ対策
 - (1) 組織体制
 - (2) 情報資産の分類と管理
 - (3) 情報システム全体の強靱性の向上
 - (4) 物理的セキュリティ
 - (5) 人的セキュリティ
 - (6) 技術的セキュリティ
 - (7) 運用
 - (8) 業務委託と外部サービス（クラウドサービス）等の利用
- 7 情報セキュリティ監査及び自己点検の実施
- 8 情報セキュリティポリシーの見直し
- 9 情報セキュリティ対策基準の策定
- 10 情報セキュリティ実施手順の策定

1 目的

杉並区議会（以下「議会」という。）が実施する情報セキュリティ対策についての基本的な事項を定めるための基本方針として、また、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、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杉並区議会情報セキュリティ基本方針を定める。

2 定義

この方針において、次に掲げる用語の意義は、それぞれ次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及びその構成機器（ハードウェア

及びソフトウェア)をいう。

(2) 情報システム

議会の組織運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。

(3) 情報資産

情報システムで取り扱う全ての情報及び情報システムの開発と運用に係る情報並びに紙等の有体物としての情報をいう。

(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) 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。

(8) 情報セキュリティポリシー

この方針及び情報セキュリティ対策基準をいう。

(9) 内部情報系

総合行政ネットワーク(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。

(10) インターネット接続系

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。

(11) 通信経路の分割

内部情報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。

(12) 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ない等、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、以下のものを想定し、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、通信の断絶、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) 対象機関の範囲

基本方針が適用される範囲は、議会事務局及び議員とする。

(2) 情報資産の範囲

この方針が対象とする情報資産は、次のとおりとする。ただし、議会事務局の職員が職務上作成し、又は取得したものに限る。

- ① 情報システム
- ② 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 職員の遵守義務及び違反への対応

議会事務局の職員は、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。また、この方針の実効性を確保するために違反者に対しては、議長が必要な処分等を行う。

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に、以下の情報セキュリティ対策を講じる。

(1) 議会事務局に係る情報セキュリティ対策

① 組織体制

議会が保有する情報資産について、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

議会が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靱性の向上

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、次の二段階の対策を講じる。

ア 内部情報系においては、L G W A N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の分割を行う。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。

イ 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、都道府県及び区市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、情報システム室を有する場合には、それらの管理について、また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、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

情報システムへのアクセス制御、不正プログラム対策、不正アクセス対策等の技術的な対策を講じる。

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、業務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）等の利用

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。

(2) 議員に係る情報セキュリティ対策

① 物理的セキュリティ

議長は、杉並区役所内において、議員が使用するネットワーク及び情報システムを構築するときは、区のネットワーク及び情報システムとは物理的に独立したものとして構築し、管理する。

② 技術的セキュリティ

議長は、議員が使用するパソコン端末（区がリース契約を締結しているものをいう。以下「議員パソコン」という。）に対し、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。

③ 運用

議員パソコンの使用に当たっては、別に定める使用基準により適切な管理を行うものとする。

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、リスクを検討した上で、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

上記6(1)、7及び8に規定する対策等を実施するために、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。

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、情報セキュリティ実施手順は、公にすることにより議会の組織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。

附 則

この方針は、令和8年4月1日から施行する。