渋谷区議会情報セキュリティ基本方針

令和８年３月２３日議長決裁

（基本理念）

渋谷区議会（以下、「議会」という。）は、ＩＣＴを活用した議会活動の効率化及び透明性並びに公平な情報提供の実現に努め、開かれた議会運営を推進している。

さらに、情報システムサービスの充実を図るに当たり、議会は、個人情報の保護と情報セキュリティの確保に向けて、以下の方針で取り組むこととする。

（趣旨）

第１条　この基本方針は、地方自治法第２４４条の６第１項の規定に基づき、議会の保有する情報資産を適切かつ安全に管理するために、情報セキュリティに関する基本的事項を定めるものとする。

（定義）

第２条　この基本方針における用語の意義は、次のとおりとする。

（１）ネットワーク　電子計算機、周辺機器及び端末装置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含む。)をいう。

（２）電子計算機　ハードウェア及びソフトウェアで構成するコンピュータ及び周辺機器をいう。

（３）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た記録が格納されている媒体をいう。

（４）入出力帳票　情報処理に必要な帳票類をいう。

（５）データ　入出力帳票又は記録媒体に記録されている情報をいう。

（６）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。

（７）情報セキュリティ　情報資産を正確かつ完全に保持し、許可された者が必要なときに利用可能な状態に維持し、許可されていない者がアクセスできないことを確実にすることをいう。

（８）情報セキュリティポリシー　情報資産を情報セキュリティの脅威から守るために議会が定める基本方針等をいう。

（９）情報資産 ハードウェア、ソフトウェア及びネットワークで構成される情報システム、情報システムに記録されているデータ、入出力帳票、設計書、手順書等のドキュメント等の総称をいう。

（１０）機密性　アクセスを許可された者だけが情報にアクセスできることを確実にすることをいう。

（１１）完全性　情報及び処理方法が、正確であること及び完全であることを保護することをいう。

（１２）可用性　許可された利用者が、必要なときに、情報及び資産にアクセスできることを確実にすることをいう。

（１３）業務委託 業務を外部へ委託することをいう。
（１４）委託事業者 業務を受託する事業者をいう。

（情報資産に対する脅威）
第３条　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

（適用範囲）
第４条
（１）対象者
本基本方針が適用されるのは、議会が保有する情報資産を取り扱う議員及び渋谷区議会事務局職員（会計年度任用職員等を含む。以下「事務局職員」という。）とする。
（２）情報資産の範囲
本基本方針は、議会の保有する全ての情報資産を対象とする。

（議員及び事務局職員の遵守義務）
第５条　全ての議員及び事務局職員は、情報セキュリティの重要性を認識し、関連する法令及び情報セキュリティポリシーを遵守しなければならない。

（情報セキュリティ対策）
第６条　第３条に規定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行うものとする。
（１）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）物理的セキュリティ　通信回線及び議員並びに事務局職員の端末等の管理について、物理的な対策を講じる。
（４）人的セキュリティ 情報セキュリティに関し、議員及び事務局職員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。
（５）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。

（６）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。
（７）業務委託　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。

（個人情報保護）
第７条　収集し、蓄積した個人情報の保護は、情報セキュリティの上で、最も優先して対策を行う。

（情報セキュリティ監査）
第８条　情報セキュリティポリシーが遵守されていることを確認するために、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行う。

（評価・見直し）
第９条　情報セキュリティポリシーは、その有効性を適時評価し、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見直しを行う。

(情報セキュリティ対策基準及び実施手順)
第１０条　議会は、この方針に基づき、必要に応じて情報セキュリティ対策基準及び具体的な実施手順を定めるものとする。

附 則
この方針は、令和８年４月１日から施行する。