

渋谷区監査委員情報セキュリティ基本方針

令和8年3月26日監査委員決裁

(基本理念)

渋谷区監査委員（以下「監査委員」という。）は、区政運営の適正性および効率性を確保するため、ICTを活用した監査業務の高度化と効率化を図り、信頼性の高い監査活動を推進している。

また、監査に関する情報を適切に管理し、必要に応じて関係者が円滑に情報へアクセスできるよう、情報システムの整備と運用に努めている。

情報システムのサービスの充実を図るに当たり、渋谷区監査委員は、個人情報を適切に保護し、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。

(目的)

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、監査委員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、渋谷区電子計算組織の管理運営に関する規則（令和元年渋谷区規則第43号。以下「規則」という。）に定めるところによるほか、次のとおりとする。

(1) 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。

(2) 情報セキュリティポリシー

本基本方針及び渋谷区情報セキュリティ対策基準をいう。

(3) 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。

(4) 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。

(5) 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。

(6) 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確保することをいう。

- (7) 職員
地方公務員法（昭和25年法律第261号）第3条に規定する地方公務員（ただし、議会の議員を除く。）をいう。
- (8) 非常勤職員
地方公務員法第3条第3項第2号及び第3号並びに第22条の2第1項に規定する者をいう。
- (9) 臨時的任用職員
地方公務員法第22条の3に規定する者をいう。
- (10) 派遣職員
労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律（昭和60年法律第88号）第2条第2号に規定する者をいう。
- (11) 会計年度任用職員
地方公務員法第22条の2に規定する者をいう。
- (12) 職員等
職員、非常勤職員、臨時的任用職員、会計年度任用職員及び派遣職員をいう。
- (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、次に掲げる脅威を想定し、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 基本方針の適用範囲は次のとおりとする。

- (1) 行政機関の範囲 監査委員
- (2) 情報資産の範囲 監査委員の保有する全ての情報資産

（職員等の遵守義務）

第5条 全ての職員等は、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。

(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、次に掲げる情報セキュリティ対策を行うものとする。

(1) 組織体制

監査委員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

監査委員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

サーバー、サーバー室等、通信回線及び職員等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、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。

(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。

2 見直しをした時は、最高情報セキュリティ責任者に報告するものとする。

(準用規定)

第10条 この方針に定めるほか、必要な事項は渋谷区情報セキュリティ対策基準を準用する。

附 則

1 この方針は、令和8年4月1日から施行する。