品川区監査委員情報セキュリティ基本方針

制定　令和７年 11 月 28 日　監査委員協議決定　要綱第１号

（目的）

第１条　この基本方針は、品川区監査委員および品川区監査委員事務局（以下「監査委員等」という。）が保有する情報資産の機密性、完全性および可用性を維持するため、監査委員等が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。

（定義）

第２条　この基本方針において、次の各号に掲げる用語の意義は、当該各号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ならびに当該コンピュータ等のハードウェアおよびソフトウェアをいう。

(2)　情報システム　コンピュータ、ネットワークおよ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、完全性およ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、改ざんまた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（インターネット接続系以外）に接続された情報システムおよ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およびその情報システムで取り扱うデータをいう。

(9)　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。

(10)　職員等　地方公務員法（昭和 25 年法律第 261 号）第３条に規定する一般職および特別職の職員をいう。

（対象とする脅威）

第３条　監査委員等は、情報資産に対する脅威として、次の各号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および業務の停止等
(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　この基本方針が適用される行政機関は、地方自治法（昭和 22 年法律第 67 号）第 195 条第１項に基づき設置する品川区監査委員および品川区監査委員条例（昭和 39 年４月８日条例第４号）に基づき設置する品川区監査委員事務局とする。
２　この基本方針が適用される情報資産は、次のとおりとする。
(1)　ネットワークおよび情報システムならびにこれらに関する設備および電磁的記録媒体
(2)　ネットワークおよび情報システムで取り扱う情報
(3)　情報システムの仕様書およびネットワーク図等のシステム関連文書
(4)　第１号から第３号までに関する印刷物および紙文書

（職員等の遵守義務）
第５条　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この基本方針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　監査委員等は、第３条の脅威から情報資産を保護するために、次のとおり情報セキュリティ対策を講じる。
(1)　監査委員等が保有する情報資産の重要性を機密性、完全性およ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。
(2)　情報システムに対し、次の対策を講じる。
ア　ＬＧＷＡＮ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、インターネット接続系からＬＧＷＡＮ接続系に対して通信する場合には、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とともに高度な情報セキュリティ対策として、東京都および区のインターネットとの通信を集約した上で、東京都セキュリティクラウドの導入等を実施する。
(3)　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。
(4)　情報セキュリティに関し、十分な教育および啓発を行う等の人的な対策を講じる。
(5)　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)　情報システムの監視、情報セキュリティ対策の遵守状況の確認、業務委託を行う際のセキュリティの確保等、この基本方針の運用面の対策を講じる。
(7)　ソーシャルメディアサービスを利用する場合には、発信することができる情報、利用するソーシャルメディアサービスごとの責任者等について、運用手順を定める。
(8)　情報セキュリティ対策の遵守状況を検証するため、必要に応じて情報セキュリティ自己点検を実施し、運用改善を行い、情報セキュリティの向上を図るとともに、必要に応じてこの基本方針の見直しを実施する。

付　則
この要綱は、令和８年４月１日から適用する。