情報セキュリティ基本方針

制定　令和元年５月 27 日　区長決定　要綱第 227 号
改正　令和５年３月 24 日　区長決定　要綱第 86 号

（目的）
第１条　この基本方針は、品川区（以下「区」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、区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)　情報セキュリティポリシー　この基本方針および区長が別に定める情報セキュリティ対策基準をいう。
(5)　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。
(6)　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。
(7)　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。
(8)　マイナンバー利用事務系（個人番号利用事務系）　個人番号利用事務（社会保障、地方税に関する事務）または戸籍事務等に関わる情報システムおよびデータをいう。
(9)　ＬＧＷＡＮ接続系　ＬＧＷＡＮ（マイナンバー利用事務系および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。
(10)　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。
(11)　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。
(12)　職員等　常勤職員、暫定再任用職員、定年前再任用短時間職員、会計年度任用職員、派遣職員、委託業者、指定管理者および協定によりネットワークを利用する者のことをいう。

（対象とする脅威）
第３条　区は、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、品川区組織規則（平成２７年品川区規則第３号）第２条に定める部の課および品川区教育委員会事務局処務規則（平成１３年品川区教育委員会規則第５号）第２条に定める事務局の課ならびに品川区保健所処務規程（昭和５０年品川区訓令甲第８号）、品川区清掃事務所処務規程（平成１２年品川区訓令第２号）、品川区会計管理室規則（昭和４０年品川区規則第１０号）、品川区議会事務局処務規程（昭和５１年品川区議会議長訓令甲第２号）、品川区監査委員事務局規程（昭和５５年品川区監査委員訓令甲第１号）および品川区選挙管理委員会事務局規程（昭和５７年品川区選挙管理委員会訓令甲第１号）に定める機関とする。

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情報セキュリティポリシーおよ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。

（情報セキュリティ対策）

第６条　区は、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)　区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)　区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。

(3)　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、情報システムに対し、次の３段階の対策を講じる。

ア　マイナンバー利用事務系においては、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ぐとともに、利用するシステム自体にも２要素以上の認証の仕組みを備える。

イ　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。

ウ　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。

(4)　管理系ネットワーク（統括情報セキュリティ責任者が定める管理者のもと、庁内ネットワークに接続し安全に利用するために必要な情報システムを設置する領域をいう。）のセキュリティは、インターネット接続系、マイナンバー利用事務系およびＬＧＷＡＮ接続系とは論理的に分離する。

(5)　サーバ機器、サーバ室、通信回線およ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。

(6)　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、十分な教育および啓発を行う等の人的な対策を講じる。

(7)　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。

(8)　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の確保等、情報セキュリティポリシーの運用面の対策を講じるとともに、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切に対応するため、緊急時対応計画を策定する。

(9)　業務委託を行う場合には、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た上、情報セキュリティ要件を明記した契約を委託事業者と締結し、当該契約に基づき必要な措置を講じる。

(10)　外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

(11)　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。

(12)　情報セキュリティポリシーの遵守状況を検証するため、定期的または必要に応じて情報セキュリティ監査およ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とともに、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。

（情報セキュリティ対策基準の策定）

第７条　前条に規定する対策等を実施するために、具体的な遵守事項およ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。

（共通事項実施手順の策定）

第８条　前条の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について、共通事項実施手順により定めるものとする。なお、共通事項実施手順は、公にすることにより区の行政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。

付　則

この要綱は、令和元年６月１日から適用する。

付　則

この要綱は、令和５年４月１日から適用する。