豊島区情報セキュリティ基本方針

令和４年８月

政策経営部情報管理課

改定履歴

制定（改定）年月日	改定内容等
平成 15 年 7 月 1 日	初版制定
平成 21 年 8 月 1 日	一部改定
令和 4 年 8 月 1 日	全部改定

１．目　的

豊島区の情報システムが取り扱う情報には、区民の個人情報のみならず行政運営上重要な情報など、外部への漏えい等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、情報資産、情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、区民のプライバシー、財産その他の権利利益を守るとともに、行政の安定的な運営を確保する上で必要不可欠であり、ひいては、区民の豊島区に対する信頼の維持向上に寄与するものである。

そこで、豊島区の情報セキュリティ対策を整備するために情報セキュリティポリシーを定めることとする。情報セキュリティポリシーは、豊島区が保有する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

２．定　義

この基本方針で使用する用語の定義は、次のとおりである。

(1)　ネットワーク

コンピュータ等（あらゆる物）を相互に接続するための通信網、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

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、業務の処理を行う仕組み又はコンピュータ単体で同様の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（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）、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）及び可用性（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）を維持することをいう。

(4)　情報セキュリティポリシー

豊島区情報セキュリティ基本方針及び豊島区情報セキュリティ対策基準をいう。

(5)　情報セキュリティ対策基準

情報セキュリティ対策を行う上で必要となる基本的な要件を定めた、職員が遵守すべき基準をいう。

(6)　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、地方税若しくは防災に関する事務)又は戸籍事務等に関わる情報システム及びデータをいう。

(7)　LGWAN 接続系

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(マイナンバー利用事務系を除く。)。

(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及びその情報システムで取り扱うデータをいう。

(9)　校務接続系

校務に関わる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。

(10)　通信経路の分割

LGWAN 接続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。

(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) 学校

「豊島区立学校の管理運営に関する規則」で定める豊島区立小学校、中学校及び幼稚園をいう。

(13) 職員

「豊島区職員定数条例」で定める者のうち、「(14) 教職員」を除いた者をいう。

(14) 教職員

市町村立学校職員給与負担法(昭和 23 年法律第 135 号)に規定する職員及び東京都教育委員会に任用され区立学校に勤務する会計年度任用職員並びに「豊島区職員定数条例」で定める者の中で幼稚園教諭のことをいう。

(15) 会計年度任用職員

地方公務員法第 22 条の 2 に規定する会計年度任用職員のことをいう。

(16) 外部委託先

豊島区と契約を締結する法人及び個人をいう。

3．対象とする脅威

情報資産に対する脅威として、主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) 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

4．対象範囲

(1) 行政機関の範囲

この基本方針が適用される行政機関は、区長部局、監査委員事務局、選挙管理委員会事務局、区議会事務局、教育委員会事務局及び学校とする。

(2) 情報資産の範囲

この基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

②ネットワーク及び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

区長をはじめとして豊島区が保有する情報資産に関する業務に携わるすべての職員、教職員、会計年度任用職員は、情報セキュリティの重要性について共通の認識をもつとともに、業務の遂行にあ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。

外部委託先に対しては、情報セキュリティ要件を明らかにした上で遵守させるものとする。

６．情報セキュリティ対策

不正アクセス、データやプログラムの持出し、災害などの脅威から情報資産を保護するために、次の情報セキュリティ対策を講ずるものとする。

(1) 情報セキュリティ管理体制

情報セキュリティ対策を推進・管理するための体制を定め、その権限と責任を明確にするものとする。

(2) 情報資産の分類と管理

豊島区の情報資産をその重要度により分類し、その分類に応じた情報セキュリティ対策を行うものとする。

(3) 情報システム全体の強靭性の向上

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、次の三段階の対策を講ずる。

①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。

②LGWAN 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、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。

③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、都道府県及び市区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対策

情報システムを設置する場所への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

(5) 人的セキュリティ対策

すべての職員に情報セキュリティポリシーの内容を周知徹底する等、職員の教育及び啓発に必要な対策を講ずる。

(6) 技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策を講ずる。

(7) 運用におけるセキュリティ対策

情報セキュリティポリシーの遵守状況の確認、ネットワークの監視等の運用面の対策を講ずる。また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

(8) 業務委託と外部サービスの利用におけるセキュリティ対策

業務委託を行う場合には、外部委託先を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託先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ずる。

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ずる。

ソーシャルメディアサービスを利用する場合には、情報セキュリティ対策を含む運用手順を、ソーシャルメディアサービスごとに定める。

⑼ 評価及び見直しの実施

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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

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が遵守されていることを検証するため、各情報セキュリティ対策基準の定めるところにより、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、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に定める情報セキュリティ対策を講ずるにあたっては、遵守すべき行為及び判断等の基準を統一的に定める必要がある。そのため、情報セキュリティ対策基準を総務省及び文部科学省が示す情報セキュリティポリシーガイドラインに基づき、区長部局及び教育委員会それぞれに策定（以下「各情報セキュリティ対策基準」という。）するものとする。

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を遵守して情報セキュリティ対策を実施するためには、個々の情報資産に係る対応手順等を定めておく必要がある。そのため、各情報セキュリティ対策基準の基本的な要件に基づき、情報資産の情報セキュリティ実施手順を策定するものとする。

１１．情報セキュリティポリシーの開示

基本方針はすべてを開示するものとし、情報セキュリティ対策基準及び情報セキュリティ実施手順の内容は原則として開示しない。

１２．違反者に対する対応

情報セキュリティポリシーに違反する行為をした職員に対しては、適切な措置を講ずることとする。

附　則

この基本方針は、平成１５年７月１日から施行する。

この基本方針は、平成２１年８月１日から施行する。

この基本方針は、令和　４年８月１日から施行する。