杉並区情報セキュリティ基本方針

策　定　日　平成１５年　８月　５日
最終改正日　平成１５年１１月　６日　一部

目　　次

杉並区情報セキュリティ基本方針

１　策定の目的

杉並区（以下「区」という。）は、昭和 61 年に、区が管理する情報を原則として公開する情報公開条例と、個人情報の厳格な取り扱いや自己情報のコントロール権を盛り込んだ個人情報保護条例を同時制定するなど、情報の適正な管理に努めてきた。今日、区にはＩＴを活用し、区民サービスの向上、区民との情報共有の拡充や協働（パートナーシップ）の充実、行政の効率化を図り質の高い行政運営をめざすこと（電子区役所の構築）が求められている。

したがって、区の行政情報はＩＴ（情報技術）によって取り扱われる比重が飛躍的に大きくなってきている。

ネットワークによる高度な情報化は、区の全ての分野に大きな変革をもたらす可能性がある反面、ネットワークを介したシステムに対する不正アクセスや攻撃、情報の漏洩や改ざんといった脅威（リスク）が増大する。原因を問わず、個人情報漏洩や情報システムの障害が発生した場合の影響は甚大であり、区に対する信頼は喪失する。

このため、個人情報はもとより、区が管理する全ての情報を区の情報資産ととらえ、これらをさまざまな脅威から守る効果的で実効性のある情報セキュリティ対策を講ずることが必要である。そこで区は、情報セキュリティを運営していくためのシステム（情報マネジメントシステム）を構築し、情報資産を厳格に保護することを目的に情報セキュリティ基本方針（以下「基本方針」という。）を定める。

２　定義

基本方針における用語の意義は、次に定めるところとする。

(1) 情報セキュリティマネジメントシステム（information security management system）

組織のマネジメントとしてリスクに対する保証すべきレベルを決め、プランを持ち資源を配分して、継続的なマネジメントシステム（ＰＤＣＡモデル）の運用を実現するためのフレームワーク（枠組み）。

(2) 機密性(confidentiality)

アクセスを認可された(authorized)者だけが情報にアクセスできることを確実にすること。

(3) 完全性(integrity)

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。

(4) 可用性(availability)

認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

(5) リスク評価

リスクの重大さを決定するために、算定されたリスクを与えられたリスク基準と比較するプロセス。

(6) リスクマネジメント

リスクに関して組織を指揮し管理する調整された活動。

(7) 情報システム

中央電子計算組織及び小型電子計算組織におけるネットワーク、ハードウェア、ソフトウェア及び記録媒体で構成され、事務処理を行う仕組み。

(8) 情報資産

情報システムで取り扱う全ての情報及び情報システムの開発と運用に係る情報並びに紙等の有体物としての情報をいう。

(9) 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持すること。

３　情報セキュリティ管理体制

基本方針の実効性を高め、情報セキュリティを適正に管理していくために、計画立案・運用・見直し及び改善のマネジメントサイクルに対する経営層の役割と責任を明確にした管理体制（情報セキュリティ運営委員会。以下「委員会」という。）を整備する。委員会はリスク評価の基準を確立するとともに、リスクマネジメントの環境を整備するために、情報セキュリティに関する全般的な方向性かつ目標の設定及び計画的な運営を図る。

４　職員の遵守義務及び違反への対応

区が管理する情報資産について、職員は、情報セキュリティの重要性を認識するとともに、法令等を遵守する。また、基本方針の実効性を確保するために違反者に対しては、必要な処分を行う。

５　外部委託事業者等への対応

脅威から情報資産を保護するため、外部委託事業者等（区の業務を受託する公益法人、民間事業者（ＮＰＯを含む））との間で適切な契約を締結し、その完全な履行を確保する。

６　情報資産の評価等

区が管理する情報資産を機密性、完全性、可用性のそれぞれの視点から評価し、情報資産への脅威の発生度合いや発生した場合の影響を考慮するとともに、適切な情報セキュリティ対策を講ずるものとする。

７　情報資産に対する脅威

特に認識すべき脅威を例示すれば、次のとおりである。

(1) 部外者の侵入による情報資産の破壊・盗難、故意の不正アクセス又は不正操作による情報資産の破壊・盗聴・改ざん・消去等の脅威

(2) 職員又は外部委託事業者等による情報資産の持出、誤操作、パスワード等の不適切管理、故意の不正アクセス又は不正行為による破壊・盗聴・改ざん・消去等、規定外の端末接続による漏洩等の脅威

(3) コンピュータウィルス、地震、落雷、火災等の災害並びに事故、故障等による業務停止の脅威

８　情報セキュリティ対策

脅威から情報資産を保護するために、人的、物理的、技術的及び運用の面から情報セキュリティ対策を講ずるものとする。

(1) 人的セキュリティ

職員の故意又は過失による不正行為から情報資産を適切に保護するため、情報セキュリティに関する権限や責任を定め、基本方針の内容を周知徹底するなど、十分な教育及び啓発が実施できるよう必要な管理策を講じる。また、外部委託事業者等に対しては秘密保持の徹底等、必要な対策を講じる。

(2) 物理的セキュリティ

区の施設への不正な立入り、情報資産の破壊・盗難等を防止するため、入退室管理等、適切な管理策を講ずる。

(3) 情報システムセキュリティ

情報資産を不正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、適切な対策を講ずる。

また、システム開発等委託業務の管理監督、ネットワークの監視、基本方針の遵守状況の確認等、運用面での対策を講ずる。

９　情報セキュリティ実施手順の策定

情報資産に対するリスク分析結果への対応を評価したうえで、各所管で業務内容に応じた具体的な情報セキュリティ実施手順（以下「実施手順」という。）を策定するものとする。

10　情報セキュリティ監査の実施

基本方針及び実施手順が遵守されていることを検証するため、定期的に監査を実施する。

11　評価及び見直し

情報セキュリティ監査の結果等により、基本方針に定める事項及び情報セキュリティ対策の評価を実施し、基本方針の見直しを行う。