中 野 区 情 報 安 全 対 策 基 本 方 針

策定日
2002 年 3 月 29 日
最新改定日
2021 年 4 月 1 日

＜基本理念＞

中野区が真に豊かで持続可能な地域社会をつくりあげていくためには、区民の個人情報や行政運営上重要な情報資産を様々な脅威から守り、区民の財産やプライバシー等の保護及び事務の安定的な運営を確保することが重要であることから、情報セキュリティ対策について基本方針を定め、これに基づき情報セキュリティマネジメントシステム（ISMS）体制を構築・運用し、積極的に取り組みます。

1　基本方針

（1）体制

中野区は、区長のリーダーシップの下、最高情報安全責任者（CISO）を中心とした情報セキュリティ体制を確立し、情報セキュリティに対する責任を明確にします。

（2）対象となるリスク

中野区は、以下のリスクを想定し、情報セキュリティ対策を実施します。

ア　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・持出・盗聴・改ざん・消去等

イ　職員又は外部委託事業者による情報資産の持出、誤操作、アクセスのための認証情報又はパスワードの不適切管理、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、搬送中の事故による情報資産の盗難、規定外の端末接続による漏洩等

ウ　地震、落雷、火災等の災害、不正プログラム及び事故、故障等によるサービス及び業務の停止等

（3）講ずる対策

中野区は、情報資産の機密性、完全性及び可用性を確保するため、以下の対策を講じます。

ア　物理的セキュリティ

施設への不正な立入り、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じます。

イ　人的セキュリティ

情報セキュリティに関する権限や責任を定め、職員及び外部委託事業者に情報セキュリティ対策の内容を周知徹底する等十分な教育が行われるように必要な対策を講じます。

ウ　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ます。

エ　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、外部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ます。

(4)情報セキュリティインシデント等への対応

ア　情報資産に対する侵害が発生した場合等に迅速かつ適切に対応するため、事業継続計画(ICT-BCP)を策定します。

イ　中野区は、情報セキュリティインシデントに備えた体制を整備し、情報セキュリティインシデントが発生した場合、その原因を迅速に究明し、その影響を最小限に止めるとともに再発防止に努めます。

(5)リスクマネジメント

中野区は、情報資産の様々なリスクに適切に対処するため、リスクアセスメントを実施した上で、対応策を定め、リスクマネジメントを行います。

(6)監査

中野区は、情報セキュリティポリシー等が遵守されていること検証するため、定期的に監査を実施します。

(7)違反等への処分

中野区は、情報セキュリティに関連する違反行為に対して、法令及び区の規定に従い厳正に処分を行います。

(8)環境の整備

中野区は、本基本方針に従い遵守すべき行為及び判断等の基準をさだめた情報安全対策基準や情報システムにおける情報セキュリティ対策を実施するための具体的な手順を定めた情報安全対策実施手順など区のルールを整備し、その周知と共に確実に実行できる環境を整備します。

(9)評価及び見直しの実施

中野区は、監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシー等の見直しを実施します。

2　職員遵守事項

(1)職員は、情報セキュリティに関するルールを遵守します。

(2)職員は、業務以外の目的で文書の作成や閲覧、情報システムへのアクセス、メールの使用及びインターネットへのアクセス等を行いません。

(3)職員は、情報の紛失や漏えい等がないように、文書等を適正に保管し、パソコン等情報機器の使用にあたってはルールを厳守します。

(4)職員は、情報セキュリティに関する理解促進とスキルの向上を図るため、継続

的に研修を受講し、情報セキュリティに対する自覚をもって日々の業務を遂行します。

3 その他

(1)範囲

情報セキュリティポリシーが対象とする行政機関の範囲は、区長部局、会計室、区議会事務局及び各行政委員会事務局及び各教育機関(事務室及び職員室のみ)とする。なお、区民が自由に利用するために設置した情報システム、及び各教育機関における教育のために用いる情報システム等は、情報セキュリティポリシーの対象外とします。

(2)言葉の定義

ア 情報セキュリティ

情報の機密性、完全性及び可用性を維持すること。

(ｱ)機密性

認可されていないもの、プロセスに対して、情報を使用不可又は非公開にする特性。

(ｲ)完全性

情報の正確さ及び完全さを保護する特性。

(ｳ)可用性

認可されたもの、プロセスから要求されたときにアクセス可能かつ利用可能にする特性。

イ 情報セキュリティポリシー

本基本方針及び情報安全対策基準。

ウ 情報資産

職員が職務上作成し又は入手する情報で、文書、図画、写真、フィルム、電磁的記録、その他の記録媒体により保管しているもの及びそれらを取り扱うネットワーク及び情報システム。

エ 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、その構成機器(ハードウェア及びソフトウェア)。

オ 情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組み。

カ 情報セキュリティ事象

情報資産における、情報セキュリティの方針・基準等への違反若しくは対応・処置の不具合等の可能性又はセキュリティに関連し得る未知の状態。

キ　情報セキュリティインシデント

　　情報セキュリティ事象のうち、行政運営を危うくするリスク及び情報セキュリティを脅かすリスクが高い特定の状況が発生した状態。

ク　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。

ケ　LGWAN 接続系

　　人事給与、財務会計及び文書管理等 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。

コ　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。

サ　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。