東京都北区情報セキュリティ基本方針に関する規程

平成一六年三月二五日
訓令甲第五号

改正　平成一九年一一月二一日訓令甲第三七号　平成二九年　三月二八日訓令甲第六号
平成三一年　三月二九日訓令甲第六号　令和　三年　三月二五日訓令甲第六号
令和　六年　三月二二日訓令甲第四号　令和　七年　三月二六日訓令甲第八号
令和　八年　三月三十日訓令甲第六号

（目的）

第一条　この規程は、東京都北区（以下「北区」という。）が保有する情報及び情報を取り扱う環境の機密性、完全性及び可用性を確保・維持するための統一的かつ基本的な方針を定めることにより、情報セキュリティ対策を組織的に講じ、区民の財産、プライバシー等を守り、もつて安定的かつ継続的に行政サービス及び正確な情報の提供を図ることを目的とする。

（用語の定義）

第二条　この規程において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

一　実施機関　区長、教育委員会（幼稚園、認定こども園、小学校、中学校及び義務教育学校を含む。）、選挙管理委員会、監査委員及び区議会事務局をいう。

二　職員　地方公務員法（昭和二十五年法律第二百六十一号）第三条第二項に規定する一般職の職員及び同条第三項に規定する特別職の職員（区議会議員を除く。）をいう。

三　情報　職員が職務上作成し、又は取得した文書等（文書、図画、写真、フィルム及び電磁的記録（電子的方式、磁気的方式その他人の知覚によつては認識することができない方式で作られた記録をいう。以下同じ。））であつて、当該職員が組織的に用いるものとして、実施機関が現に保有しているもの及び職員が職務上作成し、又は取得した文書であつて当該職員が現に保有しているものをいう。

四　情報資産　次に掲げる情報及び情報を取り扱う環境をいう。

イ　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

ロ　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。）

ハ　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

ニ　業務で使用する情報が記載されている文書（業務遂行上のメモ等を含む。）

五　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及びその構成機器（ハードウェア及びソフトウェアをいう。）をいう。

六　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、情報処理を行う仕組みをいう。

七　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をいう。

八　機密性　情報にアクセスすることを認められた者のみが、情報にアクセスできる状態を確保することをいう。

九　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をいう。

十　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。

十一　マイナンバー利用事務系　個人番号利用事務（社会保障、地方税又は防災に関する事務のうち、個人番号を利用する事務をいう。）、戸籍事務等に係る情報システム及びデータをいう。

十二　ＬＧＷＡＮ接続系　ＬＧＷＡＮに接続された情報システム及び当該情報システムで取り扱うデータ（マイナンバー利用事務系に係るデータを除く。）をいう。

十三　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係るインターネットに接続された情報システム及び当該情報システムで取り扱うデータをいう。

十四　通信経路の分割　ＬＧＷＡＮ接続系及び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のみを許可できるようにすることをいう。

十五　無害化通信　インターネットメール本文のテキスト化、端末への画面転送等により、コンピュータウィルス等の不正なプログラムの付着がないことその他安全が確保された通信をいう。

（対象範囲）
第三条　この規程の対象は、実施機関及び実施機関の職員（以下「職員」という。）並びに情報資産とする。
（対象とする脅威）
第四条　実施機関は、情報資産に対する脅威として、次に定める脅威を想定し、情報セキュリティ対策を実施する。
一　不正アクセス、ウイルス攻撃、サービス不能攻撃その他のサイバー攻撃、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
二　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
三　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
四　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
五　電力供給、通信及び水道供給の途絶等のインフラの障害からの波及等
（職員の遵守義務）
第五条　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持ち、業務の遂行に当たつて東京都北区情報セキュリティポリシー（この規程及び東京都北区情報セキュリティ対策基準（以下「情報セキュリティ対策基準」という。）で構成するものをいう。以下「情報セキュリティポリシー」という。）及び東京都北区情報セキュリティ実施手順（以下「情報セキュリティ実施手順」という。）並びに東京都北区教務用ＩＣＴ環境教務情報セキュリティポリシー（この規程及び東京都北区教務用ＩＣＴ環境情報セキュリティ対策基準（以下「教務対策基準」という。）で構成するものをいう。以下「教務情報セキュリティポリシー」という。）及び東京都北区教務用ＩＣＴ環境情報セキュリティ実施手順（以下「教務実施手順」という。）並びにこれらに関連する法令等を遵守しなければならない。
（情報セキュリティ対策）
第六条　実施機関は、第四条に規定する脅威から情報資産を保護するため、次の各号に掲げる事項について、当該各号に定める情報セキュリティ対策を講じるものとする。
一　組織体制　北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こと。
二　情報資産の分類及び管理　北区の保有する情報資産を機密性、完全性及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こと。
三　紙文書の管理　紙文書を適切に維持管理するために次の対策を実施すること。
イ　紙文書を保管するために施錠できるキャビネット等を設け、施錠管理するとともに、鍵の管理を行うこと。
ロ　キャビネット等は、来訪者及び外部事業者の出入り（納品時を含む。）がある場所からは可能な限り隔離すること。
ハ　紙文書は、必要に応じて書庫で保管すること。
ニ　書庫は、耐火、侵入防止策、他部署との隔離等の対策を必要に応じて講じた上で、収納及び持ち出しの方法を定めて運用すること。
四　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、次の対策を講じること。
イ　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、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こと。
ロ　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こと。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こと。
ハ　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し、原則として高度な情報セキュリティ対策として、都道府県及び区市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こと。

五　物理的セキュリティ　サーバ、サーバ室、通信回線、職員のパソコン等の管理について、物理的な対策を講じること。

六　人的セキュリティ　情報セキュリティに関し、職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じること。

七　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ること。

八　運用　情報システムの監視、情報セキュリティポリシー及び教務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確保その他の情報セキュリティポリシー及び教務情報セキュリティポリシーの運用面の対策を講じ、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正に対応するための緊急時対応計画を策定すること。

九　業務委託及び外部サービス（クラウドサービス）の利用　次に掲げる場合に応じ、それぞれに定める事項を行うこと。

イ　業務委託を行う場合　委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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、必要に応じて契約に基づき措置を講じること。

ロ　外部サービス（クラウドサービス）を利用する場合　当該利用に係る規定を整備し、対策を講じること。

ハ　ソーシャルメディアサービスを利用する場合　ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定めること。

十　評価・見直し　情報セキュリティポリシー及び教務情報セキュリティポリシーの遵守状況を検証するため、定期的に、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ことで、運用改善及び情報セキュリティの向上を図り、情報セキュリティポリシー又は教務情報セキュリティポリシーの見直しが必要な場合は、適宜それらの見直しを行うこと。

（情報セキュリティ監査及び自己点検）

第七条　実施機関は、情報セキュリティポリシー及び教務情報セキュリティポリシーの遵守状況を検証するため、定期的に、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なければならない。

（情報セキュリティポリシー等の見直し）

第八条　実施機関は、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又は教務情報セキュリティポリシーの見直しが必要となつ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つた場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシー又は教務情報セキュリティポリシーの見直しを適宜実施しなければならない。

（情報セキュリティ対策基準等の策定）

第九条　実施機関は、前三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、判断基準等を定める情報セキュリティ対策基準及び教務対策基準を策定する。

（情報セキュリティ実施手順等の策定）

第十条　実施機関は、情報セキュリティ対策基準及び教務対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順及び教務実施手順を策定するものとする。

２　情報セキュリティ実施手順及び教務実施手順は、非公開とする。

（違反に対する対応）

第十一条　情報セキュリティポリシー及び実施手順又は教務情報セキュリティポリシー及び教務実施手順に違反した者に対しては、その違反の程度に応じて地方公務員法の規定による懲戒その他の法令等に基づく厳正な対応を行う。

（委任）

第十二条　この規程の施行に関し必要な事項は、別に定める。

付　則

この訓令は、平成十六年三月二十五日から施行する。

付　則（平成一九年一一月二一日訓令甲第三七号）

この訓令は、平成十九年十二月一日から施行する。

付　則（平成二九年三月二八日訓令甲第六号）

この訓令は、平成二十九年四月一日から施行する。

付　則（平成三一年三月二九日訓令甲第六号）

この訓令は、平成三十一年四月一日から施行する。

付　則（令和三年三月二五日訓令甲第六号）

この訓令は、令和三年四月一日から施行する。

付　則（令和六年三月二二日訓令甲第四号）

この訓令は、令和六年四月一日から施行する。

付　則（令和七年三月二六日訓令甲第八号）

この訓令は、令和七年四月一日から施行する。

付　則（令和八年三月三十日訓令甲第六号）

この訓令は、令和八年四月一日から施行する。