立川市情報セキュリティ基本方針

令和７年10月17日
立 川 市 長 決 定

（目的）

第１条　この基本方針は、市が保有する情報資産の機密性、完全性及び可用性を維持するため、市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及び構成機器（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、情報処理を行う仕組みをいう。

(3)　情報資産　次に定めるとおりとする。

ア　ネットワーク、情報システム及びこれらに関する設備並びに電磁的記録媒体（以下「情報システム等」という。）

イ　紙文書

ウ　情報システム等及び紙文書で取り扱う情報

(4)　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。

(5)　情報セキュリティポリシー　この基本方針及び別に定める情報セキュリティ対策基準をいう。

(6)　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。

(7)　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。

(8)　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。

(9)　個人番号利用事務系　個人番号利用事務（福祉、保健若しくは医療その他の社会保障、地方税（地方税法（昭和 25 年法律第 226 号）第１条第１項第４号に規定する地方税をいう。）又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。

(10)　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をいう。

(11)　インターネット接続系　インターネットメール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。

(12)　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うえで、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。

(13)　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、コンピュータウィ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。

（対象とする脅威）

第３条　情報資産に対する情報セキュリティ対策の実施に当たり、対象とする脅威は、次の各号に掲げるとおりとする。

(1)　サイバー攻撃（不正アクセス、ウイルス攻撃、サービス不能攻撃等をいう。）、部外者の侵入その他の意図的な要因による情報資産の漏えい、破壊、改ざん、消去等

(2)　情報資産の管理不備、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、保守・管理の不備、機器故障その他の非意図的要因による情報資産の漏えい、破壊、改ざん、消去等

(3)　地震、落雷、火災その他の災害によるサービス及び業務の停止、情報資産の消失等

(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、水道供給及び通信の途絶等のインフラの障害からの波及

(6)　その他情報セキュリティを脅かす事案

（適用範囲）

第４条　この基本方針の適用を受ける市の機関は、立川市組織条例（昭和42年立川市条例第１号）第１条に規定する部等、会計課、教育委員会事務局、図書館、選挙管理委員会事務局、監査委員事務局、農業委員会事務局、固定資産評価審査委員会事務局及び議会事務局をいう。

２　この基本方針の適用を受ける者は、市長、副市長、教育長及び会計管理者並びに前項に規定する市の機関に所属する職員（地方公務員法（昭和25年法律第261号）第３条第２項に規定する一般職の職員及び同条第３項に規定する特別職の職員をいう。以下同じ。）、教育公務員特例法第２条に規定する教育公務員及び立川市非常勤職員給与等支給条例別表に掲げる職員（以下「職員」という。）とする。

（職員の義務）

第５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、業務の遂行に当たって情報セキュリティポリシー及び別に定める情報セキュリティ実施手順を遵守しなければならない。

（委託等に伴う措置）

第６条　委託等により、業務において市が保有する情報資産を職員以外の者に利用させる場合は、情報セキュリティポリシーと同等以上の水準での情報セキュリティを確保できるよう、契約等において必要な措置を講じるものとする。

２　委託等により、業務において市が保有する情報資産を利用する職員以外の者は、当該業務の範囲において情報セキュリティポリシーを遵守するものとする。

（情報セキュリティ対策）

第７条　第３条に規定する脅威から情報資産を保護するために講じる情報セキュリティ対策は、次の各号に掲げる区分に応じ、当該各号に定めるとおりとする。

(1)　組織体制　市の保有する情報資産について、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ものとする。

(2)　情報資産の分類及び管理　市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　情報システム全体に対し、次の三段階の対策を講じる。

①個人番号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うえで、端末からの情報持ち出し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、都道府県と市区町村のインターネット接続口を集約したうえで、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　サーバ、情報システム室、通信回線、パソコン等の管理について、物理的な対策を講じるものとする。

(5)　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別に定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じるものとする。

(6)　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ものとする。

(7)　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るものとする。この場合において、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ものとする。

（情報セキュリティ監査及び自己点検の実施）

第８条　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するものとする。

（情報セキュリティポリシーの見直し）

第９条　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は、情報セキュリティポリシーを見直すものとする。

（情報セキュリティ対策基準の策定）

第１０条　この基本方針に基づいた情報セキュリティ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を策定するものとする。この場合において、情報セキュリティ対策基準は、公にすることにより市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、外部に周知すべき事項を除いて原則非公開とする。

（情報セキュリティ実施手順の策定）

第１１条　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を定めた情報セキュリティ実施手順を策定するものとする。この場合において、情報セキュリティ実施手順は、公にすることにより市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、原則非公開とする。

附　則

この基本方針は、平成 29 年４月１日から施行する。

附　則

この基本方針は、令和元年７月 10 日から施行する。

附　則

この基本方針は、令和７年 10 月 17 日から施行する。

情報セキュリティポリシーの体系図（第２条第５号関係）