

立川市立学校情報セキュリティ基本方針（案）

平成29年●月●日

立川市教育長決定

（目的）

第1条 この基本方針は、立川市立学校設置条例（昭和38年立川市条例第66号）別表に定める立川市立学校（以下「学校」という。）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、立川市教育委員会（以下「教育委員会」という。）及び学校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。

（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な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機関は、学校とする。

- 2 この基本方針の適用を受ける者は、学校に所属する教職員（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。）とする。

(教職員の義務)

第5条 教職員は、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、業務において学校が保有する情報資産を教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、業務において学校が保有する情報資産を利用する教職員以外の者は、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 学校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ための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 学校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) 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。
- (4) 人的セキュリティ 情報セキュリティに関し、教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。
- (5) 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。
- (6) 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

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学校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学校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。

情報セキュリティポリシーの体系図（第2条第5号関係）

