東大阪市立学校園情報セキュリティ基本方針

1　目的

この方針は、東大阪市立学校園の取り扱う情報資産の機密性、完全性、可用性を維持し、東大阪市立学校園の情報セキュリティを確保するための対策について基本的事項を定めたものである。東大阪市立学校園の情報資産を扱う者は本方針をよく理解し、これに沿った行動を取ることで、情報セキュリティの脅威を軽減することを目的としている。

2　用語の定義

この方針において、次に掲げる用語の意義は、次に定めるところによる。

（１）東大阪市立学校園情報セキュリティポリシー

東大阪市立学校園情報セキュリティ基本方針及び東大阪市立学校園情報セキュリティ対策基準をいう。

（２）端末

情報システムの構成要素である機器のうち、職員等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいう。端末には、モバイル端末も含まれる。

（３）利用者 ID

情報システムやネットワークを利用するときに、個人や学校園を識別するためにあらかじめ登録された文字列をいう。

（４）ネットワーク

端末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）をいう。

（５）通信回線

複数の情報システム又は機器等（教育委員会が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、教育委員会や学校園の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、モバイルルータなど教育委員会が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。

（６）通信回線装置

通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。また、物理的なハードウェアを有する通信回線装置を「物理的な通信回線装置」という。

（７）無線LAN

IEEE802.11a、802.11b、802.11g、802.11n、802.11ac、802.11ax、802.11ad等の規格により、無線通信で情報を送受信する通信回線をいう。

（８）電磁的記録媒体

電磁的記録（電子的もしくは磁気的方式による記録）のための媒体をいう。

（９）電子メール等

端末を使用し、ネットワークを通じて行う電子通信をいう。文字以外の画像や音声などのデータを含むものとする。

(10) 電子署名

情報の正当性を保証するための電子的な署名情報をいう。

(11) アクセス

端末、ネットワーク及び情報システムを通じて、データの参照、変更等を行うことをいう。

(12) 情報システム

端末、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をいう。

(13) 校務系情報

学校が保有する情報資産のうち、それらの情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報

(14) 学習系情報

学校が保有する情報資産のうち、それらの情報を学校における教育活動において活用することを想定しており、かつ、当該情報に教員及び児童生徒がアクセスすることが想定されている情報

(15) 教育情報システム

校務系システム（校務系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム）及び学習系システム（学習系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム）を合わせた総称

(16) ソフトウェア

サーバ装置、端末、通信回線装置等を動作させる手順及び命令を、当該サーバ装置等が理解できる形式で記述したものをいう。OS や OS 上で動作するアプリケーションを含む広義の意味である。

(17) アプリケーション

OS 上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。

(18) ソーシャルメディア

インターネット上において、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成していくものをいう。

(19) 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。

(20) 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。

(21) 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。

(22) 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。

(23) 情報セキュリティインシデント

望ましくない又は予期しない情報セキュリティ事象であって、業務の遂行及び情報セキュリティを脅かすものをいう。

(24) 不正プログラム

コンピュータウイルス(自己増殖し、被害を与える悪意のあるプログラム)、ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム）、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。

(25) 強固なアクセス制御

インターネットを通信経路とする前提で、内部・外部からの不正アクセスを防御するために、多要素認証による利用者認証、端末認証、端末・サーバ・通信の監視・制御等を組み合わせたセキュリティ対策を指す。利用者毎に情報へのアクセス権限を適切に設定するとともに、①アクセスの真正性、②端末・サーバ・通信の安全性の観点から、端末とクラウドサービスを提供するサーバ間の通信を暗号化し、認証により利用者のアクセスの適正さを常に確認しなければならない。

(26) 通信の暗号化

通信又は通信経路を暗号化し保護すること

(27) クラウドサービス

クラウドコンピューティングを利用したサービスをいう。クラウドコンピューティングとは、共用の構成可能なコンピューティングリソース(ネットワーク、サーバ、ストレージ、アプリケーション、サービス)の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続き又はクラウド事業者とのやりとりで速やかに割当てられ提供されるものをいう。

コンピューティングリソースの実装の在り方で、パブリッククラウドとプライベートクラウドに大別できる。

【パブリッククラウド】

複数の利用者で端末リソースを共有してサービス提供される形態で、資源利用の最適化（コスト低減、サービス開始までの期間短縮）が図れる。

【プライベートクラウド】

１つの利用者に対し端末リソースを占有してサービス提供される形態で、利用者運用の個別化（機能改変、運用の自由度向上）が図れる。

また、クラウドサービス事業者が提供するコンピューティングリソースの範囲によって、以下の呼び方が用いられる。

（ア）SaaS（サース、サーズ）

「Software as a Service」の略称。クラウドサービス事業者がソフトウェアを稼働しインターネット経由でユーザーがアクセスすることによって利用できる仕組み。

（イ）PaaS（パース）

「Platform as a Service」の略称。ソフトウェアを動作させるための環境を提供するサービス。動作させるソフトウェアの開発、設定、運用は、利用者側で行う。

（ウ）IaaS（イアース、アイアース）

「Infrastructure as a Service」の略称。システムの稼働に不可欠なサーバやネットワークなどのインフラをインターネット経由で提供するサービス。基本ソフト(OS)、データベース、動作させるソフトウェアは利用者が用意する。

(28) オンプレミス

コンピューティングリソースを自前で自組織内運用する形態。クラウド型との対比で使われることが多い。

(29) シングルサインオン（SSO：Single Sign On）

一度のID・パスワードによるユーザー認証（ログイン）を行うだけで、複数のアプリケーション、クラウドサービスなどにログインすることができる仕組み。利用者の利便性が向上するが、SSOのための専用システムが必要になる。

3　対象とする脅威

学校園が作成または取得した情報の電子化への脅威や取り扱う情報に対する脅威を想定し、機密性、完全性及び可用性を確保するために必要な基本事項を定める。

（１）電子化された情報の所定外の場所への保管による情報の漏洩等

（２）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏洩、破壊、改ざん及び消去等

（３）情報資産の無断持ち出し（自校園内での持ち運びを含む。）、目的外使用、無許可ソフトウェアの使用等の規定違反、プログラム上の欠陥、操作ミス、故障等の非意図的要因による情報資産の漏洩、破壊及び消去等

4　適用範囲

（１）学校園の範囲

本基本方針が適用される学校園は、東大阪市立学校園とする。

（２）教職員等の範囲

本基本方針が適用される者は、学校園の情報を取り扱う教職員、会計年度任用職員及びその他学校園の情報を取り扱う者（以下「教職員等」という。）とする。

（３）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①　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

②　ネットワーク及び情報システムで取り扱う情報（印刷した文書を含む。）

③　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

（４）個人情報

学校園における個人情報とは、教職員、児童・生徒、保護者に関する情報で、その情報に含まれる氏名、生年月日その他の記述等により、特定の個人を識別できるものをいう。

5　教職員等の遵守義務

教職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたって「東大阪市立学校園情報セキュリティポリシー」（以下「市立学校園情報セキュリティポリシー」という。）を遵守しなければならない。

6　情報セキュリティ対策

対象とする脅威から情報資産を保護するために、学校園が保有する個人情報を取り扱うことができるのは、次の情報セキュリティ対策が講じられている場合とする。

（１）組織体制

学校園の情報資産について、情報セキュリティ対策を推進する組織体制が教育委員会及び学校園において確立されていること。

（２）情報資産の分類と管理

学校園が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が講じられていること。

（３）物理的セキュリティ

サーバ等の管理、情報システムの設置場所、通信回線及び教職員等の端末並びに電磁的記録媒体等の管理について、物理的対策が講じられていること。

（４）人的セキュリティ

情報セキュリティに関し、教職員等が遵守すべき事項が定められていると共に、十分な教育及び啓発を行う等の人的な対策が講じられていること。

（５）技術的セキュリティ

端末等の管理、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が講じられていること。

（６）運用

情報システムの監視、市立学校園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、市立学校園情報セキュリティポリシーの運用面の対策が講じられていること。

（７）情報資産に対するセキュリティ侵害

情報資産等に対するセキュリティ侵害が発生した場合、迅速かつ適切に対応できること。

７　情報セキュリティ自己点検の実施

市立学校園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自己点検を実施する。

８　市立学校園情報セキュリティポリシーの見直し等

（１）市立学校園情報セキュリティポリシーの見直し

「７　情報セキュリティ自己点検の実施」の結果、市立学校園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処するため新たに対策が必要となった場合には、市立学校園情報セキュリティポリシーを見直す。

（２）東大阪市立学校園情報セキュリティ委員会の設置

市立学校園情報セキュリティポリシーの決定、変更等、リスク情報の共有及び情報セキュリティに関する重要な事項を決定するため、東大阪市立学校園情報セキュリティ委員会（以下「学校園情報セキュリティ委員会」という。）を置く。なお、学校園情報セキュリティ委員会に関する必要な事項は別に定める。

９　東大阪市立学校園情報セキュリティ対策基準

「６　情報セキュリティ対策」の条件の具体化や「７ 情報セキュリティ自己点検の実施」、「８　市立学校園情報セキュリティポリシーの見直し等」に規定する対策等を実施するための具体的な遵守事項及び判断基準等については、別に定める東大阪市立学校園情報セキュリティ対策基準によるものとする。

附則（施行期日）

本基本方針は平成 21 年 10 月１日から施行する。

本基本方針は令和３年４月１日から施行する。

本基本方針は令和８年４月１日から施行する。