# 枚方市立学校情報セキュリティポリシー

枚方市教育委員会

【令和6年4月1日 改訂版】

| | 改訂履歴 |
|---|---|
| 初　版 | 平成25年10月 1日 |
| 改訂 1 | 平成27年 4月 1日 |
| 改訂 2 | 平成27年 6月 18 日 |
| 改訂 3 | 平成31年 4月 1日 |
| 改訂 4 | 令和 1年10月 1日 |
| 改訂 5 | 令和 2年 7月14日 |
| 改訂 6 | 令和 3年 4月 1日 |
| 改訂 7 | 令和 4年 4月 1日 |
| 改訂 8 | 令和 6年 4月 1日 |
| | |
| | |

# 第1章 情報セキュリティ基本方針

## 1.目的

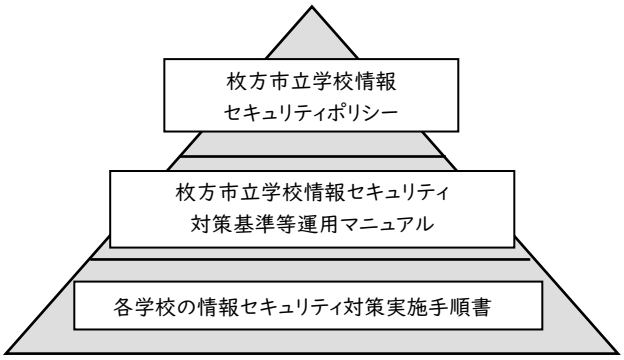
学校教育の情報化の進展により、児童・生徒、その保護者等の個人情報を含む情報資産の一層適切な管理・運用が求められる。そのため、本市においては学校における情報セキュリティ強化の観点から平成25年10月に枚方市立学校情報セキュリティポリシー（以降、学校情報セキュリティポリシーという。）を策定した。文部科学省からは平成29年10月に「学校情報セキュリティポリシーに関するガイドライン」が示された。その後、GIGAスクール構想の実現に基づく1人1台端末の整備やクラウドサービスの本格活用など学校のICT環境の変化に伴ってガイドラインが改訂され、今後も情報セキュリティ対策の動向や技術的な進展等を踏まえ改訂される。本市においても安全かつ適切な情報管理を行っていくには最新のガイドラインに準拠した情報セキュリティ対策が必要であり、学校情報セキュリティポリシーを都度見直し、これに基づき適正に対応していく。

## 2.枚方市立学校情報セキュリティポリシーの構成と文書体系

学校情報セキュリティポリシーは、学校が保有する情報資産に対する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。

このポリシーは、学校が保有する情報資産を取り扱う全職員に浸透、定着させるものであり、安定した統一的な規範であることが求められる。一方、情報処理・通信技術の進歩による急速な環境の変化に柔軟に対応することも必要となることから、不変的な部分として統一的な規範を定めた『情報セキュリティ基本方針』と情報資産を取り巻く環境の変化に柔軟に対応する部分となる『情報セキュリティ対策基準』の2部構成として策定する。

【文書体系のイメージと説明】




| 文書名 | | 内容 |
|---|---|---|
| 枚方市立学校情報セキュリティポリシー | 情報セキュリティ基本方針 | 学校のセキュリティ対策の目的や方針を定めた統一的な規範 |
| | 情報セキュリティ対策基準 | 学校にある情報を脅威から守るための具体的な対策を示したもの |
| 枚方市立学校情報セキュリティ対策基準等運用マニュアル | | 情報セキュリティ対策基準を適正かつ円滑に管理・運用するために各項に対する解説を示したもの |
| 各学校の情報セキュリティ対策実施手順書 | | 学校において情報セキュリティ対策を実行するために各教職員が行動する手順を示したもの |

3.学校教育における個人情報

（1）個人情報

個人情報保護法において「個人情報」とは、生存する個人に関する情報で、氏名、生年月日、住所、顔写真などにより特定の個人を識別できる情報をいう。

これには、他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものも含まれる。例えば、生年月日や電話番号などは、それ単体では特定の個人を識別できないような情報ですが、氏名などと組み合わせることで特定の個人を識別できるため、個人情報に該当する場合がある。また、メールアドレスについてもユーザー名やドメイン名から特定の個人を識別することができる場合は、それ自体が単体で、個人情報に該当する。

（2）学校教育で取り扱う主な個人情報

①個人に関するもの（児童・生徒、保護者、教職員等学校教育にかかわる者）

・個人に関する情報

名前、生年月日、性別、住所、電話番号 、メールアドレス、ID、入学日や卒業日、学年、学級、出席番号、部活動、学習成績や評価、出席状況、入学、編入学、卒業、転学、財産・収入、卒業証書授与台帳等。

・保健情報

（ア）体重、身長、視力、聴力などの基本的な体格・体調データ。

（イ）血圧、心拍数などの生理測定データ。

（ウ）医療履歴、過去の病歴、アレルギー情報、手術歴、現在および過去に処方された薬物の記録、ワクチン接種記録、生活歴、心身の状況等。

（エ）生活習慣に関する情報。

・指導・支援記録

（ア）指導に関する情報。

（イ）支援に関する情報。

・学習に関する情報

ワークシート、振り返りシート、レポート等の成果物、作品、写真、動画等。

・その他

教育相談、家庭訪問記録、座席表等。

4.個人情報の利用目的

（1）個人情報の利用目的

個人情報の取り扱いには、教育の質の向上、児童・生徒の安全確保、そしてより良い学校生活の提供が目的にある。

①教育活動への利用や学習状況の把握と支援

学習記録や成績等を分析し、個別最適な支援に生かす。

②健康管理と支援

体調や健康、出欠等に関する情報をもとに、教職員同士での情報共有による適切な支援、関係機関との円滑な連携を図る。

③安全確保への利用

万が一の事態や災害時において、迅速に保護者へ連絡を取るなどの緊急対応、児童・生徒の安全を確保するために利用する。

他にも、学校長が真に必要と認める際には、緊急的に上記以外の目的で個人情報を利用する場合がある。

（2）個人情報の取り扱いに関する取組

児童・生徒の個人情報は、関連する法令や規定に従い、厳重に管理する。また、不要になった情報は適切に破棄する。

5.用語の定義

枚方市立学校情報セキュリティポリシーにおける用語の定義は、次に定めるところによる。

(1) 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し、情報を安全・安心に使用するためのルールや技術のことをいう。

(2) 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。

(3) 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。

(4) 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。

(5) 学校情報

電磁的に記録された学校事務の執行に関わる情報をいう。

(6) 校務情報

児童・生徒の成績、出欠及びその理由、健康診断結果、指導要録、教職員の個人情報など、学校が保有する情報資産のうち、それら情報を学校・学級の管理運営、学習指導、生徒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をいう。

(7) 学習情報

児童・生徒のワークシート、作品など、学校が保有する情報資産のうち、それら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、かつ当該情報に教職員及び児童・生徒がアクセスすることが想定されている情報をおいう。

(8) 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（ハードウエア及びソフトウエア）をいい、校内においては以下のとおり分類する。

①「教育外部系（学習用）ネットワーク」

インターネットに接続可能な授業に用いるコンピュータ教室及び各教室等のネットワーク

②「教育内部系（校務用）ネットワーク」

インターネットに接続可能な校務処理に用いるネットワーク

③「新教育外部系ネットワーク」

１人１台端末で学習に用いるネットワーク

(9) 教育ネットワーク

情報資産を扱う通信回線、ルータ等の通信機器

(10) サーバ等

ネットワーク上で学校情報を処理し、端末機に提供するコンピュータをいう。

(11) 端末機

ネットワークを通じてサーバに接続されたパソコンをいう。

(12) 情報システム

学校情報を処理するためのハードウエア及びソフトウエアをいう。

(13) 校務系システム

教育内部系（校務用）ネットワーク、校務用サーバ及び校務用端末から構成される校務情報を取り扱うシステム及び、校務情報を主に取り扱う上で、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いう。外部接続時には論理分離される仕組みを有する。

(14) 学習系システム

教育外部系（学習用）ネットワーク及び新教育外部系ネットワーク、学習用サーバ（クラウド含む）、学習者用端末及び指導者用端末から構成される学習情報を取り扱うシステム及び、学習情報を扱う上で、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いう。

(15) 教育情報システム

校務系システム及び学習系システムを合わせた総称

(16) 外部記録媒体

情報システムでデータ等を記録するための媒体（メディア）をいう。

ハードディスク、フロッピーディスク、USBメモリ等。

(17) 1人1台端末

GIGA スクール構想で児童・生徒及び教職員等に配備された端末をいう。

(18) 情報資産

情報システム及びネットワーク並びにこれらで取り扱われる学校情報（紙の文書も含む。）

(19) 無線 LAN

電波等を利用してデータの送受信を行う構内通信網システムをいう。

(20) 情報セキュリティインシデント

コンピュータシステムやネットワークに対する攻撃や不正アクセスなど、情報の機密性や完全性、可用性を脅かす出来事のことをいう。（ウイルス感染、データ漏えい、サイバー攻撃など）

(21) ソーシャルメディアサービス

インターネット上で展開される情報メディアのサービスで、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだプラットフォームのことをいう。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持った Web サイトやネットサービスなどを総称する用語。

(22) 標的型攻撃

明確な意思と目的を持ち、特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種をいう。

(23) 外部サービス

「外部サービス」とは、事業者等の庁外の組織が情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において自組織の情報が取り扱われる場合に限る。

(24)「外部サービス提供者」

「外部サービス提供者」とは、外部サービスを提供する事業者をいう。外部サービスを利用して自組織に向けて独自のサービスを提供する事業者は含まれない。

(25)「外部サービス利用者」

「外部サービス利用者」とは、外部サービスを利用する自組織の職員等又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう。

(26) スマートデバイス

スマートフォン及びタブレット型コンピュータの総称をいう。

6.情報資産への脅威

情報資産に対して想定される脅威は、その発生度合や発生した場合の影響を考慮するものとし、次のとおりとする。

(1) 部外者による意図的な不正アクセス、又は不正操作によるデータやプログラムの漏えい・持出・盗聴・改ざん・消去、機器及び外部記録媒体の盗難等

(2) 教職員等及び外部委託業者による非意図的な操作、又は意図的な不正アクセス又は不正操作によるデータやプログラムの漏えい・持出・盗聴・改ざん・消去、機器及び外部記録媒体の盗難、規定外の情報システム接続や操作によるデータ漏えい等

(3) 地震、落雷、火災、水害等の災害並びに事故、故障等による業務の停止

(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) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

7.情報セキュリティ対策

情報資産を脅威から保護するため、次に定める情報セキュリティ対策を講じるものとする。

(1) 管理体制

情報資産を管理し、機密性、完全性および可用性を維持するための体制を確立する。

(2) 情報資産の分類と管理

本市教育委員会及び市立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セキュリティ対策を実施する。

(3) ネットワーク分離によるセキュリティ対策

情報セキュリティの強化を目的とし、情報ネットワークに対し、以下の対策を講じる。

① 教育内部系（校務用）と教育外部系（学習用）及び新教育外部系ネットワークは、原則として、ほかの領域との通信をできないよう物理分離する。

② 教育内部系（校務用）においては、外部接続との通信経路を論理分離する。

(4) 物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・盗難等から保護するために施設整備等の物理的な対策を講じる。

(5) 人的セキュリティ対策

情報セキュリティに関する権限や責任を定めるとともに、全ての教職員等に枚方市立学校情報セキュリティポリシーを周知徹底するための教育を実施する等、必要な対策を講じる。

(6) 技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、コンピュータウイルス対策ソフト導入等の技術面における対策を講じる。

(7) 運用

① 情報システムの監視、枚方市立学校情報セキュリティポリシーの順守状況の確認、外部委託を行う際のセキュリティ確保等、枚方市立学校情報セキュリティポリシーの運用面の対策を講ずる。

② 情報セキュリティが侵害される事態が発生した場合に被害の拡大防止、復旧等を迅速かつ的確に実施するため、連絡体制マニュアルを整備する。また、侵害に備えた対応訓練の定期的な実施等の対策を講じるよう努める。

(8) 外部委託

外部に業務委託を行う場合には、外部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、外部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。外部サービスを利用する場合には、利用にかかる規定を確認し対策を講じる。

ソーシャルメディアサービスを利用する場合には、教育委員会が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。

## 8.枚方市立学校情報セキュリティポリシーの適用範囲

枚方市立学校情報セキュリティポリシーの適用範囲は、枚方市立の全小中学校、教育委員会、教育文化センターの教育工学室及び中央図書館のサーバ室に設置した学校用のシステム、サーバ等とする。

ただし、枚方市立の小中学校の図書室に設置する「学校図書館システム」は、情報ネットワーク構成の特異性を考慮し、「枚方市情報セキュリティポリシー」に基づいて管理・運用しており、「枚方市立学校情報セキュリティポリシー」の適用範囲外とする。

## 9.情報セキュリティ委員会

枚方市情報セキュリティポリシーの規定（「7 情報セキュリティ委員会」）に準拠する。

## 10.教職員等の責務

(1) 校長、教頭、教員、学校事務職員、任期付職員、非常勤職員（附属機関等委員を除く）、会計年度任用職員、臨時職員、その他学校に所属する職員（以下「教職員等」という。）は、情報資産の利用にあたっては、関連法令を順守しなければならない。

(2) 教職員等は、情報セキュリティの重要性を認識し、枚方市立学校情報セキュリティポリシーを順守しなければならない。

## 11.監査及び自己点検

枚方市立学校情報セキュリティポリシーの順守状況を検証するため、必要に応じて情報セキュリティ監査を受ける。また、定期的に自己点検を実施する。

## 12.枚方市立学校情報セキュリティポリシーの評価・見直し

情報セキュリティ監査の結果等により、枚方市立学校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、情報システムの変更や新たな脅威の発生等、状況の変化に迅速かつ的確に対応するため、必要に応じて枚方市立学校情報セキュリティポリシーの見直しを実施する。

# 第2章 情報セキュリティ対策基準

## 1.趣旨及び情報資産の範囲

(1) 趣旨

情報セキュリティ対策基準は、情報セキュリティ基本方針に沿って個々の対策を具体化したものであり、学校における情報セキュリティ対策の基準とする。

(2) 情報資産の範囲

本対策基準が対象とする情報資産は,次のとおりとする。

① 教育ネットワーク、教育情報システム、及びこれらに関する設備及び記録媒体

② 教育ネットワーク及び教育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)

③ 教育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

情報セキュリティ対策基準は、情報セキュリティ基本方針に沿って個々の対策を具体化した ものであり、学校における情報セキュリティ対策の基準とする。

## 2.管理体制

情報セキュリティの管理体制は、次に掲げるとおりとする。

(1) 教育情報統括責任者

教育長を教育情報統括責任者とし、市立学校における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する統括的な権限及び責任を有する。

教育情報統括責任者は、緊急時には情報セキュリティ責任者(CISO)に早急に報告を行うとともに、回復のための対策を講じなければならない。

(2) 学校情報セキュリティ責任者

学校教育部長を学校情報セキュリティ責任者とし、市立学校における情報資産に対する侵害が発生した場合、又は侵害の恐れがある場合に必要かつ十分な措置を行う権限及び責任を有する。

(3) 学校情報セキュリティ管理者

学校教育部教育研修課長を学校情報セキュリティ管理者とし、市立学校における情報資産の管理及び情報セキュリティ対策に関する統括的な権限及び責任を有する。

(4) 校内情報セキュリティ責任者

市立学校における各学校長を校内情報セキュリティ責任者とし、当該学校における情報セキュリティ実施手順書を策定し、情報資産の管理及び情報セキュリティ対策に関する権限及び責任を有する。また所属の教職員から校内情報セキュリティ担当者を1名選任して教育研修課長に報告するものとする。

(5) 校内情報セキュリティ管理者

市立学校における各教頭を校内情報セキュリティ管理者とし、校内情報セキュリティ責任者を補佐するとともに所属する教職員の情報セキュリティ対策の実施について管理、指導を行う。

(6) 校内情報セキュリティ担当者

市立学校における各情報システムの管理、運用に携わる担当者を校内情報セキュリティ担当者とし、校内情報セキュリティ責任者及び校内情報セキュリティ管理者と協力して、枚方市立学校情報セキュリティポリシーの周知及び啓発に努める。

(7) セキュリティ事案連絡・相談窓口(CSIRT)との連携

学校情報セキュリティ管理者は、発生した事案を正確に把握した上で、セキュリティ事案連絡・相談窓口に報告し、連携を図る。

(8) 学校の外部サービス統括管理者

学校教育部教育研修課長を学校の外部サービス統括管理者とする。学校の外部サービス統括管理者は、学校の外部サービスを統括し、外部サービス管理者に対し、指導、助言を行う権限及び責任を有する。

(9) 学校の外部サービス管理者

市が利用している外部サービスを所管している担当課の長を学校の外部サービス管理者とする。学校の外部サービス管理者は、所管する外部サービスにおける契約、設定の変更、運用、見直し及び情報セキュリティ対策を行う権限及び責任を有する。

3. 情報資産の分類と管理方法

(1) 情報資産の分類

情報資産が漏洩、利用不能、改ざん等のセキュリティ侵害を受けた際の影響の深刻度に応じ、下表のとおり重要性の分類を定める。

| | 重要性分類 |
|---|---|
| Ⅰ | 侵害により、教職員又は児童・生徒の生命、財産、プライバシー等へ重大な影響を及ぼすと想定される情報資産 |
| Ⅱ | 侵害により、学校事務及び教育活動の実施に重大な影響を及ぼすと想定される情報資産 |
| Ⅲ | 侵害により、学校事務及び教育活動の実施に軽微な影響を及ぼす情報資産 |
| Ⅳ | ほとんど影響を及ぼさないもの。上記Ⅰ、Ⅱ、Ⅲ以外 |

※業務で取扱う情報資産は、作成、入手、利用、保管、廃棄等の各局面で、上記の重要性分類を踏まえた管理としなければならない。

※情報資産分類については、別表1及び2を参照

(2) 情報資産の管理

① 管理責任

(ア) 校内情報セキュリティ責任者は、その所管する情報資産について管理責任を有する。

(イ) 情報資産が複製又は伝送された場合には、複製等された情報資産も(1)の分類に基づき管理しなければならない。

② 情報資産分類の確認及び表示

教職員等は、情報資産について、その分類を確認し、必要に応じて重要性分類を表示するなど適切な管理を行わなければならない。

※情報資産の分類の表示先の例

ファイル(ファイル名、ファイル属性(プロパティ)、ヘッダー・フッター等)、格納するドライブのラベル等

③ 情報資産の作成

(ア) 教職員等は、業務上必要のない情報資産を作成してはならない。

(イ) 情報資産を作成する者は、情報資産の作成時に(1)の分類に基づき、当該情報資産の分類と取扱制限を定めなければならない。

(ウ) 情報資産を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。

また、情報資産の作成途上で不要になった場合は、当該情報資産を消去しなければならない。

④ 情報資産の入手

(ア) 学校内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

(イ) 学校外の者が作成した情報資産を入手した者は、(1)の分類に基づき、当該情報資産の分類と取扱制限を定めなければならない。

(ウ) 情報資産を入手した者は、その情報資産の分類が不明な場合、校内情報セキュリティ責任者に判断を仰がなければならない。

⑤ 情報資産の利用

(ア) 情報資産を利用する者は、業務以外の目的で情報資産を利用してはならない。

(イ) 情報資産を利用する者は、情報資産の分類に応じ、適切な取り扱いをしなければならない。情報資産を利用する者は、ドライブまたは保存されている領域(フォルダやサーバ)に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該ドライブまたは保存されている領域を取り扱わなければならない。

⑥ 情報資産の保管

(ア) 校内情報セキュリティ責任者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

(イ) 校内情報セキュリティ責任者は、情報資産を記録した外部記録媒体を保管する場合は、施錠可能な場所で保管しなければならない。

(ウ) 校内情報セキュリティ責任者は、情報システムのバックアップで取得したデータを記録する外部記録媒体を保管する場合は、自然災害を被る可能性が低い場所に保管しなければならない。

⑦ 情報の送信

情報資産が組織内部(組織が利用するサーバやクラウドサービス等)から組織外部(家庭や地域、事業者等)に電子メール等により外部送信される場合は、情報資産分類に応じ以下を実施しなければならない。

(ア) 電子メール等により重要性分類Ⅲ以上の情報を外部送信する者は、限定されたアクセスの措置設定を行わなければならない。

(イ) 学校情報セキュリティ管理者は、電子メール等による外部送信の安全性を高めるため、添付される情報資産を監視する等、出口対策を実施しなければならない。

⑧ 情報資産の提供・公表

(ア) 重要性分類Ⅲ以上の情報資産を外部に提供する者は、限定されたアクセスの措置設定を行わなければならない。

(イ) 重要性分類Ⅲ以上の情報資産を外部に提供する者は、校内情報セキュリティ責任者に許可を得なければならない。

(ウ) 校内情報セキュリティ責任者は、保護者等に公開する情報資産について、完全性を確保しなければならない。

⑨ 情報資産の廃棄

(ア) 重要性分類Ⅲ以上の情報資産を廃棄する者は、情報を記録している内蔵及び外部記録媒体が不要になった場合、当該記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。

(イ) 情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

(ウ) 情報資産の廃棄を行う者は、校内情報セキュリティ責任者の許可を得なければならない。

4.物理的セキュリティ対策

4.1 教育委員会サーバ等の機器の管理

枚方市情報セキュリティポリシーの対策基準(「4.1 サーバの管理」)に準拠する。

4.2 中央図書館内のサーバ室の管理

枚方市情報セキュリティポリシーの対策基準(「4.2管理区域(サーバ室等)の管理」)に準拠する。

4.3 コンピュータ教室及び準備室の管理

(1) コンピュータ教室及び準備室の構造等

① コンピュータ教室及び準備室から外部に通ずるドアは必要最小限にし、施錠設備等によって許可されていない者の立ち入りを防止しなければならない。また、施錠設備に関連する鍵等は適正に管理しなければならない。

② コンピュータ教室及び準備室内に設置する機器等については、転倒及び落下防止等の耐震対策、防火措置等を講じなければならない。

③ コンピュータ教室及び準備室内には温度及び湿度を適正に保つための空気調節設備を設置しなければならない。

(2) コンピュータ教室及び準備室の入退室管理等

① コンピュータ教室及び準備室への入退室は教職員等(教育委員会職員を含む)及び許可された児童・生徒、保護者・外部委託事業者のみに制限しなければならない。

② 外部委託事業者がコンピュータ教室への入室を行う場合は、身分証明書等を携帯し、求めにより提示しなければならない。また、名札その他の身分証明書等を着用しなければならない。

③ コンピュータ教室内への機器等の搬入時は、教職員等の同行、立会いを行い、事故等のないようにしなければならない。

4.4 通信回線及び通信回線装置の管理

枚方市情報セキュリティポリシーの対策基準(「4.3 通信回線及び通信回線装置の管理」)に準拠する。

4.5 外部記録媒体の管理

(1) 外部記録媒体は、施錠可能な場所に保管するなどの盗難防止対策を講じなければならない。

(2) 重要度の高い学校情報等が記録された外部記録媒体は、耐火機能を有する保管庫に保管するなど、その内容が確実に復元できる対策を講じなければならない。

(3) 外部記録媒体を外部機関と交換する場合は、適切な盗難防止策を講じるとともに、その履歴を残さなければならない。

4.6　教職員等が利用する端末の管理

(1) 学校情報セキュリティ管理者は、不正アクセス防止のため、ログイン時の ID パスワードによる認証など使用する目的に応じた適切な措置を講じなければならない。内蔵及び外部記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

(2) 学校情報セキュリティ管理者は教育情報システムへアクセスする端末へのログインパスワードの入力を必要とするように設定しなければならない。

(3) 学校情報セキュリティ管理者は、重要性分類Ⅱ以上の情報資産を取り扱う場合、パスワード以外に生体認証や物理認証等の多要素認証を設定しなければならない。

(4) 学校情報セキュリティ管理者は、1 人 1 台端末の学校内外での業務利用の際は、上記対策（多要素認証を除く）に加え、遠隔消去機能を利用する等の措置を講じなければならない。

4.7　その他の機器の管理

(1) 校務用端末は盗難防止のため、ワイヤーによる固定等の物理的措置を講じなければならない。

(2) 端末機は盗難や不正アクセス等に備え、ログインパスワードの入力を必要とするように設定しなければならない。

(3) ネットワーク機器及びその他の機器については、不可抗力による損傷、破損、または意図的な情報の傍受等を防止するため、必要な措置を講じるよう努めなければならない。

5. 人的セキュリティ対策

5.1 教職員等の順守事項

(1) 枚方市立学校情報セキュリティポリシーの順守

教職員等は、情報セキュリティの重要性を認識し、枚方市立学校情報セキュリティポリシー並びに校内情報セキュリティ責任者が定める学校情報セキュリティ対策実施手順書に従い、情報資産を適正に扱わなければならない。

(2) 業務以外の目的での使用の禁止

教職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

また、校内情報セキュリティ管理者は、所属する教職員等に対し業務以外の目的でのインターネットへのアクセスを行わないよう常に指導し、適切に利用させなければならない。

(3) 情報資産の持ち出しの制限

教職員等は、端末機（1人1台端末を除く）、外部記録媒体、その他の情報資産を外部に持ち出す場合には、校内情報セキュリティ責任者の許可を得なければならない。

(4) 端末機等の持ち込み等の制限

① 教職員等は、私物のコンピュータ及び外部記録媒体等を校内に持ち込んではならない。

② 教職員等は、私物のスマートデバイスに個人情報を含む業務情報を記録してはならない。

(5) 机上の端末機等の管理

教職員等は、端末機や外部記録媒体、印刷された文書については、第三者に使用、閲覧等されることのない場所への保管等、適切な措置を講じなければならない。

(6) 無許可ソフトウエアの導入等の禁止

① 教職員等は、端末機に無断でソフトウエアを導入してはならない。

② 教職員等は、業務上の必要がある場合は、学校情報セキュリティ管理者の許可を得た場合に限り、ソフトウエアを導入することができる。

③ 教職員等は、不正にコピーしたソフトウエアを利用してはならない。

(7) 機器構成の変更の制限

① 教職員等は、端末機等に対し機器の改造及び増設・交換を行ってはならない。

② 教職員等は、業務上、端末機に対し機器の改造及び増設・交換を行う必要がある場合には、学校情報セキュリティ管理者の許可を得なければならない。

③ 学校情報セキュリティ管理者は、端末機等に対し、機器の改造、増設、交換等を行う場合は、想定されるリスクを考え、その対策を講じた上で構成の変更を行わなければならない。

(8) 電子メールの利用制限

① 教職員等は、自動転送機能を用いて、電子メールを転送してはならない。

② 教職員等は、業務上必要のない送信先に電子メールを送信してはならない。

③ 教職員等は、複数人に電子メールを送信する場合、必要があるときを除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

④ 教職員等は、電子メールの送信等により情報資産を無断で外部に持ち出してはならない。

⑤ 教職員等は、電子メールで送るデータの機密性を確保することが必要な場合には、暗号化又はパスワード設定の方法を使用して、送信しなければならない。

⑥ 児童・生徒が電子メールを使用する場合は、校内情報セキュリティ責任者が許可した相手に限定して送受信するようにしなければならない。

(9) 無許可でのネットワーク接続の禁止

教職員等は、許可されていない端末機を学校情報セキュリティ管理者の許可なくネットワークに接続してはならない。

(10) 業務以外の目的でのインターネット閲覧の禁止

① 教職員等は、業務以外の目的でインターネットを閲覧してはならない。

② 出所が不明なファイルや、内容に確証の得られていないファイル等は、展開してはならない。

③ 校内情報セキュリティ責任者は、教職員等が業務以外の目的でインターネットを閲覧していることが疑わしい又は判明した場合、当該教職員等への注意、指導を行わなければならない。

④ 校内情報セキュリティ責任者は、教職員等のインターネット利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、速やかにインターネット利用の停止等必要な措置を講じなければならない。

5.2 研修・訓練

(1) 学校情報セキュリティ管理者は、市立学校の教職員等に対し、情報セキュリティの重要性や枚方市立学校情報セキュリティポリシーにかかる研修及び訓練を定期的に実施しなければならない。

(2) 校内情報セキュリティ責任者は、利用する情報資産に関する情報セキュリティの理解を高めるため、所属する教職員等に対し、研修または訓練を定期的に実施しなければいけない。

5.3 侵害（事故、欠陥等を含む）の報告

(1) 侵害等の報告

① 教職員等は、情報セキュリティに関する侵害（システム上の欠陥及び誤動作等を含む）を発見した場

合、速やかに校内情報セキュリティ責任者を通じ学校情報セキュリティ管理者に報告しなければならない。

② 学校情報セキュリティ管理者は、当該事故等による情報セキュリティの侵害の程度に応じて、速やかに学校情報セキュリティ責任者、教育情報統括責任者に報告しなければならない。

(2) 侵害等の分析、記録等

侵害等のあった学校の校内情報セキュリティ責任者は、侵害等の原因を分析し、原因と再発防止策等の記録を作成し、学校情報セキュリティ管理者に提出しなければならない。

5.4 ID及びパスワード等の管理

(1) IC カードの取り扱い

① 教職員等は、自己の管理するICカード等に関し、次の事項を順守しなければならない。

(ア) 認証に用いる IC カード等を、教職員等間で共有してはならない。

(イ) 退席時又は業務上必要のない場合等は、IC カード等をカードリーダ等から取り外しておかなければならない。

(ウ) IC カード等を紛失した場合には、速やかに人事総合教育部門（教職員課）に報告し、指示に従わなければならない。

(エ) 人事総合教育部門（教職員課）は、ICカード等の紛失等の報告があった場合は、当該ICカード等を使用したアクセス等を速やかに停止しなければならない。

(オ) 人事総合教育部門（教職員課）は、ICカード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で、廃棄しなければならない。

(2) IDの取り扱い

教職員等は、自己の管理するIDに関し、次の事項を順守しなければならない。

① 自己が利用しているIDは、他人に利用させてはならない。

② 共用IDを利用する場合は、共用ID の利用者以外に利用させてはならない。

(3) パスワードの取り扱い

教職員等は、自己の管理するパスワードに関し、次の事項を順守しなければならない。

① パスワードは、他者に知られないように管理しなければならない。

② パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

③ パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

④ パスワードが流出したおそれがある場合には、校内情報セキュリティ責任者を通じ、学校情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

⑤ 複数の教育情報システムを扱う教職員等は、同一のパスワードを複数のシステム間で用いてはならない。（シングルサインオンを除く）

⑥ 仮のパスワード（初期パスワードを含む）は、最初のログイン時点で変更しなければならない。

⑦ サーバ、ネットワーク機器及び端末機（1人1台端末を除く）にパスワードを記憶させてはならない。

⑧ 教職員等間でパスワードを共有してはならない。（ただし、共有 ID に対するパスワードは除く）

6.技術的セキュリティ対策

6.1 サーバ及びネットワークの管理

(1) ファイル共有サーバの設定

① 学校情報セキュリティ管理者は、教職員等が使用できるファイル共有サーバの容量を設定し、教職員等に周知しなければならない。

② 学校情報セキュリティ管理者は、ファイル共有サーバを学校の単位で構成し、教職員等が他校のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

③ 校内情報セキュリティ責任者は、教職員等が業務以外の目的でインターネットを閲覧していることが疑わしい又は判明した場合、当該教職員等への注意、指導を行わなければならない。

④ 校内情報セキュリティ責任者は、所属する学校のファイル共有サーバの容量の増設を依頼する場合は、保存された既存のファイル等を整理してもなお増設が必要な場合に限り、学校情報セキュリティ管理者に増設の依頼をしなければならない。

(2) バックアップの実施

学校情報セキュリティ管理者は、所管するサーバ等（校内サーバを除く）に記録された情報について、必要に応じて定期的にバックアップを実施しなければならない。

(3) 情報システム仕様書等の管理

学校情報セキュリティ管理者は、所管する情報システムのネットワーク構成図、情報システム仕様書等について、外部記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

(4) ログの取得等

① 学校情報セキュリティ管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

② 学校情報セキュリティ管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

(5) 障害記録

学校情報セキュリティ管理者は、教職員等からのシステム障害の連絡、システム障害に対する処理結果及び再発防止策等を障害記録として記録し、一定の期間保存しなければならない。

(6) ネットワークの接続制御、経路制御等

① 学校情報セキュリティ管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウエア等を設定しなければならない。

② 学校情報セキュリティ管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

(7) 外部ネットワークとの接続制限等

① 学校情報セキュリティ管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内及び学校の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

② 学校情報セキュリティ管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

③ 学校情報セキュリティ管理者は、ウェブサーバ等をインターネットに公開する場合、教育ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

④ 学校情報セキュリティ管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産

に脅威が生じることが想定される場合には、学校情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

(8) 重要性が高い情報に対するインターネットを介した外部からのリスク、児童・生徒による 重要性が高い情報へのアクセスリスクへの対応

① 学校情報セキュリティ管理者は、校務系システム及び学習系システム間の通信経路の論理的又は物理的な分離をするとともに、ウェブ閲覧やインターネットメールなどのインターネットを介した外部からのリスクの高いシステムと重要性が高い情報（特に校務系システム）を論理的又は物理的に分離をしなければならない。

② 学校情報セキュリティ管理者は、校務系システム及び学習系システムとの間で通信する場合には、各システムにおけるアクセス権管理の徹底を行う等の適切な措置を図らなければならない。また、ネットワーク分離による対策を講じたシステム構成ではウイルス感染のない無害化通信など、適切な措置を図らなければならない。

(9) 電子メールのセキュリティ管理

学校情報セキュリティ管理者の設定及び制御によるものとする。

## 6.2 アクセス制御

(1) アクセス制御等

① アクセス制御

学校情報セキュリティ管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員等がアクセスできないように、システム上制限しなければならない。

② 利用者IDの取扱い

(ア) 学校情報セキュリティ管理者は、利用者の登録、変更、抹消等の情報管理、教職員等の異動、出向、退職に伴う利用者IDの取扱い等の方法を定めなければならない。

(イ) 利用されていないIDが放置されないように人事総合教育部門（教職員課）等と連携し、点検しなければならない。

③ 特権を付与されたIDの管理等

(ア) 学校情報セキュリティ管理者は、管理者権限等の特権を付与されたIDを利用する者を必要最小限にし、当該IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを厳重に管理しなければならない。

(イ) 学校情報セキュリティ管理者は、特権を付与されたIDにて外部委託事業者が作業 を行う場合は、教職員等の立会いにより、作業内容の確認を行わなければならない。

(ウ) 学校情報セキュリティ管理者は、特権を付与されたID及びパスワードについて は、定期的な変更または入力回数制限等により、特にセキュリティ機能を強化しなければならない。

(2) パスワードに関する情報の管理

① 学校情報セキュリティ管理者は、教職員等のパスワードに関する情報を厳重に管理しなければならない。各情報システムにおいて、パスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

② 学校情報セキュリティ管理者は、教職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

(3) 特権による接続の制限

学校情報セキュリティ管理者は、特権によるネットワーク及び情報システムへの接続を必要最小限にしなければならない。

6.3 システム開発、導入、保守等

枚方市情報セキュリティポリシーの規定（「6.3システム開発、導入、保守等」）に準拠する。

6.4 不正プログラム対策

(1) 不正プログラム対策

① 学校情報セキュリティ管理者は、外部ネットワークからの不正プログラムによるコンピュータウイルス感染等を防止するため、内部ネットワークと外部ネットワークの境界に、不正プログラム対策ソフトウエアの導入等の措置を講じなければならない。また、内部ネットワークから外部ネットワークへの接続時は、同様のチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

② 学校情報セキュリティ管理者は、コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ教職員等に対して注意喚起しなければならない。

③ 学校情報セキュリティ管理者は、所管するサーバ等及び端末機等に、コンピュータウイルス等の不正プログラム対策ソフトウエアを常駐させなければならない。

④ 学校情報セキュリティ管理者は、不正プログラム対策ソフトウエアを常に最新の状態に保たなければならない。

⑤ 不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、学校情報セキュリティ管理者が許可した教職員を除く教職員等に当該権限を付与してはならない。

⑥ 業務で利用するソフトウェアは、プログラム更新やバージョンアップなどの開発元のサポートが終了していないソフトウェアを利用するよう努めなければならない。

(2) 教職員等の順守事項

教職員等は、不正プログラム対策に関し、次の事項を順守しなければならない。

① 端末機等において、不正プログラム対策ソフトウエアが導入されている場合は、当該ソフトウエアの設定を変更してはならない。

② 外部からデータ又はソフトウエアを取り入れる場合には、必ず不正プログラム対策ソフトウエアによるチェックを行わなければならない。

③ 差出人が不明、又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

④ 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウエアでチェックを行わなければならない。

⑤ コンピュータウイルス等の不正プログラムに感染または検知した場合は、LAN ケーブルの即時取り外しを行い、速やかに学校情報セキュリティ管理者に報告しなければならない。

6.5 不正アクセス対策

(1) 不正アクセス対策

① 学校情報セキュリティ管理者は、外部ネットワークからの不正アクセスによる侵入等を防止するため、内部ネットワークと外部ネットワークの境界に、不正アクセス対策ソフトウエアの導入等の措置を講じなければならない。

② 学校情報セキュリティ管理者は、不正アクセス対策ソフトウエアのパターンファイルを常に最新の状態に保たなければならない。

③ 学校情報セキュリティ管理者は、内部ネットワーク等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

(2) 記録の保存

学校情報セキュリティ管理者は、内部ネットワーク等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

(3) 内部からの攻撃

学校情報セキュリティ管理者は、教職員等が使用している端末機等からの所管するネットワークのサーバ等に対する攻撃や外部に対する攻撃を監視しなければならない。

## 7.運用

### 7.1 情報システムの監視

(1) 学校情報セキュリティ責任者及び学校情報セキュリティ管理者は、不正プログラム、不正アクセス等による情報システムへの攻撃、侵入等を防止するため、サーバ監視等により情報システムの稼働状況について監視を行う等の措置を講じるよう努めなければならない。

(2) 学校情報セキュリティ責任者及び学校情報セキュリティ管理者は、不正プログラム、不正アクセス等のアクセスログ等を取得するサーバ等については、アクセスログの正確性を担保するため、正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

### 7.2 個人情報等を取り扱うネットワーク等

教職員等は、別表1及び2情報資産分類のとおり、個人情報等を適切に取り扱う。

### 7.3 外部記録媒体の使用の制限

(1) 外部記録媒体の使用

外部記録媒体は必ず公費で購入したものを使用し、私物の外部記録媒体は使用してはならない。

(2) USBメモリの使用の制限

① USBメモリは、シリアルナンバーを資産管理ソフトに登録したもの以外は使用してはならない。

② 教育内部系（校務用）端末機においては、上記の制限の他に学校情報セキュリティ管理者が使用を認めた学校の管理職及び教職員以外はUSBメモリを使用してはならない。

(3) SDカードの使用の制限

SDカードを端末機に接続した場合は、データ読み取り以外に使用してはならない。

(4) 外付けハードディスクの利用の制限

① 教育内部系（校務用）端末機及び教育外部系（授業用）端末機においては、学校情報セキュリティ管理者が使用を認めた学校の管理職以外は使用してはならない。

② 教育外部系（授業用）端末機においては、校内情報セキュリティ管理者が認めた音楽授業用途のフロッピーディスク以外は使用してはならない。

(5) 端末機内蔵のDVDドライブの使用の制限

教育内部系（校務用）端末機及び教育外部系（授業用）端末機に内蔵されているDVDドライブは、データの読み取り以外に使用してはならない。

7.4 データ保存場所

(1) 教育内部系（校務用）端末機においては、データは中央図書館のファイルサーバ（各学校のPドライブ等）または、学校情報セキュリティ管理者が許可したクラウドサーバに保存しなければならない。

(2) 教育外部系（授業用）端末機およびコンピュータ教室用端末機においては、データは各校のPドライブから中央図書館のファイルサーバまたは、学校情報セキュリティ管理者が許可したクラウドサーバに保存しなければならない。

(3) 新教育外部系端末機においては、データは学校情報セキュリティ管理者が許可したクラウドサーバに保存しなければならない。

7.5 インターネットの閲覧制限

(1) 教育内部系（校務用）端末機及び1人1台端末においては、学校情報セキュリティ管理者が必要と認めた場合以外は閲覧制限を解除してはならない。

(2) 教育外部系（授業用）においては、校内情報セキュリティ責任者が必要と認めた場合以外は閲覧制限を解除してはならない。

7.6 侵害（事故、欠陥等を含む）時の対応

(1) 連絡体制マニュアルの策定

学校情報セキュリティ責任者は、情報セキュリティに関する事故や障害、又は枚方市立学校情報セキュリティポリシーの違反等により情報資産への侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、連絡体制マニュアルを定めておく。

7.7 例外措置

(1) 例外措置の許可

教職員等は、情報セキュリティ関係規定を順守することが困難な状況で、校務の適正な遂行を継続するため、順守事項とは異なる方法を採用する又は順守事項を実施しないことについて合理的な理由がある場合には、学校情報セキュリティ責任者および校内情報セキュリティ責任者の両名の許可を得て、例外措置をとることができる。

(2) 緊急時の例外措置

教職員等は、校務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに校内情報セキュリティ責任者に報告しなければならない。

(3) 例外措置の管理

学校情報セキュリティ責任者および校内情報セキュリティ責任者は、例外措置の申請書及び審査結果等を適切に保管しなければならない。

7.8 法令順守

教職員等は、職務の遂行において使用する情報資産を保護するために、次の法令の他、関係法令を順守し、これに従わなければならない。

(1) 地方公務員法
(2) 教育公務員特例法
(3) 著作権法
(4) 不正アクセス行為の禁止等に関する法律
(5) 個人情報の保護に関する法律
(6) 行政手続における特定の個人を識別するための番号の利用等に関する法律

8.外部委託

8.1 外部委託

枚方市情報セキュリティポリシーの規定(「8.1 外部委託」)に準拠する。

8.2 外部サービスの利用(重要性分類Ⅱ以上の情報を取り扱う場合)

(1) 外部サービスの利用に係る規定の整備

学校情報セキュリティ管理者は、枚方市立学校の外部サービスの利用に関する規定を整備すること。

(2) 外部サービスの選定

① 学校の外部サービス管理者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。

② 学校の外部サービス管理者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。

(3) 外部サービスの利用に係る調達・契約

① 学校の外部サービス管理者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

② 学校の外部サービス管理者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たしたことを契約までに確認し、調達仕様の内容を契約に含めること。

(4) 外部サービスの利用確認

① 学校の外部サービス管理者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用確認を行うこと。

8.3 外部サービスの利用(重要性分類Ⅱ以上の情報を取り扱わない場合)

(1) 外部サービスの利用に係る規定の整備

学校情報セキュリティ管理者は、枚方市立学校の外部サービス(重要性分類Ⅱ以上の情報を取り扱わない場合)の利用に関する規定を整備すること。

(2) 外部サービスの利用確認

学校の外部サービス管理者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用確認を行うこと。

9.外部サービスの運用

9.1 Web会議システムの利用時の対策

(1)学校情報セキュリティ管理者は、Web 会議を適切に利用するための利用手順を定めなければならな

い。

（2）教職員等は、本市の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

（3）教職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

9.2 ソーシャルメディアの利用

学校情報セキュリティ管理者は、教育委員会又は学校が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(1) 本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

(2) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

(3) 重要性分類Ⅲ以上の情報は、ソーシャルメディアサービスで発信してはならない。ただし、児童・生徒の学習記録については、評価や成績情報とその個人が特定されない状態であれば利用可能とする。また、本市主催の教職員研修や教育イベント等で視聴対象者を限定する場合、教職員の授業力向上や学び続ける教職員の育成の観点から、児童・生徒の学習活動の記録を発信することができる。

(4) 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なければならない。

10.1人1台端末におけるセキュリティ対策

10.1 セキュリティ対策

(1) 授業に支障のないネットワーク構成の選択（帯域や同時接続数など）

クラウドサービス提供事業者側のサービス要件基準を満たしたネットワーク構成を設計すること。

(2) 不適切なウェブページの閲覧防止

学校情報セキュリティ管理者は、児童・生徒が端末を利用する際に不適切なウェブページの閲覧を防止する対策を講じなければならない。

【対策例】

① フィルタリングソフト

② 検索エンジンのセーフサーチ

③ セーフブラウジング

(3) マルウェア感染対策

学校情報セキュリティ管理者は、学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

(4) 端末を不正利用させないための防止策

学校情報セキュリティ管理者は、端末のセキュリティ状態の監視に加えて、不適切なアプリケーションやコンテンツの利用を制限し、常に安全で児童・生徒が安心して利用できる状態を維持しなければならない。

(5) セキュリティ設定の一元管理

学校情報セキュリティ管理者は、児童・生徒への端末配備後においても、端末のセキュリティ設定や

OSアップデート、ウェブブラウザのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状態確認などの作業を、離れた場所からでも一元管理できるようにしなければならない。

(6) 端末の盗難・紛失時の情報漏洩対策

学校情報セキュリティ管理者は、児童・生徒が端末を紛失した場合、遠隔操作でロックをかける、あるいはワイプ（データ消去）することで第三者による不正操作や情報漏洩を防ぐ等の安全管理措置を講じなければならない。

(7) 運用・連絡体制の整備

学校情報セキュリティ管理者は、学校内外での端末の運用ルールを制定し、インシデント時の連絡先対応方法を各学校にて周知しなければならない。

10.2 児童・生徒における ID 及びパスワード等の管理

(1) ID登録、変更、削除

① 入学、転入時のID登録処理

IDについてはシンプル・ユニーク（唯一無二）・パーマネント/パーシスタント（永続的な識別）な構成要素になっていることなど適切な措置を講じなければならない。

ID登録やパスワードポリシーにおいては情報セキュリティ対策として重要な要素であるため学校毎に管理するのではなく、教育委員会にて一元管理する。

② 進級、進学時のID関連情報の更新

IDについては原則として進級、進学にも変更不要とする。

③ 転出、卒業時のID削除処理

ユニークなIDは個人を識別できる可能性があるため、個人情報保護の観点から、サービス提供期間を超えて個人を特定する情報を保持しないようにしなければならない。

転出や卒業時に学習用ツールのサービス利用期間が終了する場合は、あらかじめ児童・生徒本人によるデータ移行をサービス利用期間内に実施し、IDの利用停止後、最終的にはID及び関連するデータの完全削除を行うこと。

ただし、本人同意や適切な管理の下、一部のデータを活用することは可能である。

(2) 学習用ツールへのシングルサインオン

学習履歴を活用したり、個人の成果物を保存するアプリケーションが増えてくると、サービス利用時に都度ID/パスワード等の認証情報を入力したり、サービス毎のアカウント情報管理が非常に煩雑になるため、一度の認証により一定時間は各種サービスにアクセスが行えるシングルサインオンの導入を行うことが望ましい。

11.評価・見直し

11.1 監査

(1) 監査の実施

教育委員会は、枚方市立学校情報セキュリティポリシー及び枚方市立学校情報セキュリティ対策実施手順書が順守されているか監査を行うものとする。

(2) 枚方市立学校情報セキュリティポリシーの見直しへの活用

教育委員会は、監査の結果、枚方市立学校情報セキュリティポリシー及び枚方市立学校情報セキュリティ対策実施手順書等の見直しが必要な場合、速やかに見直しを行うものとする。

11.2 自己点検

(1) 自己点検の実施

校内情報セキュリティ責任者は、枚方市立学校情報セキュリティポリシー及び枚方市立学校情報セキュリティ実施手順書が順守されているか、定期的に又は必要に応じて自己点検を実施しなければならない。

(2) 報告

自己点検を行った場合は、自己点検結果を学校情報セキュリティ管理者に報告しなければならない。

(3) 自己点検結果の活用

① 教職員等は、自己点検の結果に基づき、改善を図らなければならない。この場合、合わせて改善策を学校情報セキュリティ管理者に報告すること。

② 自己点検結果の報告等により、枚方市立学校情報セキュリティポリシー、その他情報セキュリティ対策の見直しが必要な場合、教育委員会は速やかに見直しを行うものとする。

11.3 枚方市立学校情報セキュリティポリシーの見直し

教育委員会は、社会情勢の変化や新たな脅威の発生に対し迅速かつ適切に対応するため、必要に応じて枚方市立学校情報セキュリティポリシーの見直しを行う。

## 巻末 [別表1] 情報資産分類

機密性による情報資産の分類

| 分類 | 分類基準 | 該当する情報資産のイメージ |
|---|---|---|
| 機密性 3 | 学校で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産 | 特定の教職員のみが知り得る状態を確保する必要のある情報で秘密文書に相当するもの |
| 機密性 2B | 学校で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産 | 教職員のみが知り得る状態を確保する必要がある情報資産（教職員のうち特定の教職員のみが知り得る状態を確保する必要があるものを含む） |
| 機密性 2A | 学校で取り扱う情報資産のうち、直ちに一般に公表することを前提としていないが、児童生徒がアクセスすることを想定している情報資産 | 教職員及び児童生徒同士のみが知り得る状態を確保する必要がある情報資産（教職員及び児童生徒のうち特定の教職員及び児童生徒のみが知り得る状態を確保する必要があるものを含む） |
| 機密性 1 | 機密性 2A、機密性 2B 又は機密性 3の情報資産以外の情報資産 | 公表されている情報資産又は公表することを前提として作成された情報資産（教職員及び児童生徒以外の者が知り得ても支障がないと認められるものを含む） |

完全性による情報資産の分類

| 分類 | 分類基準 | 該当する情報資産のイメージ |
|---|---|---|
| 完全性 2B | 学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学校関係者の権利が侵害される又は学校事務及び教育活動の的確な業務の遂行に支障（軽微なものを除く）を及ぼすおそれがある情報資産 | 情報が正確・完全な状態である必要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合、業務の遂行に支障ある情報 |
| 完全性 2A | 学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学校関係者の権利が侵害される又は学校事務及び教育活動の的確な業務の遂行に軽微な支障を及ぼすおそれがある情報資産 | 情報が正確・完全な状態である必要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合、業務の遂行に軽微な支障ある情報 |
| 完全性 1 | 完全性 2A 又は完全性 2B の情報資産以外の情報資産 | 事故があった場合でも業務の遂行に支障がない情報 |

可用性による情報資産の分類

| 分類 | 分類基準 | 該当する情報資産のイメージ |
|---|---|---|
| 可用性 2B | 学校で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産情報 | 情報が正確・完全な状態である必要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合、業務の遂行に支障ある情報 |
| 可用性 2A | 学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学校関係者の権利が侵害される又は学校事務及び教育活動の的確な業務の遂行に軽微な支障を及ぼすおそれがある情報資産 | 必要なときにいつでも利用できる必要があり、情報システムの障害等による滅失紛失や、情報システムの停止等があった場合、業務の安定的な遂行に支障がある情報 |
| 可用性 1 | 滅失、紛失や情報システムの停止等があっても業務の遂行に支障がない情報 | 滅失、紛失や情報システムの停止等があっても業務の遂行に支障がない情報 |

別表２

［情報資産の分類及び例示］

| 情報資産の分類 | | | | | 情報資産の例示 | | |
|---|---|---|---|---|---|---|---|
| 重要性分類 | 定義 | 機密性 | 完全性 | 可用性 | 教育内部系（校務用）ネットワーク<br>校外への持ち出し禁止 | クラウド（※１）または教育外部系（授業用）ネットワークも可<br>アカウントによるアクセス制限 | <br>公開 |
| Ⅰ | セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。 | ３ | ２Ｂ | ２Ｂ | ・指導要録原本<br>・教職員の人事情報 | | |
| Ⅱ | セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす。 | ２Ｂ | ２Ｂ | ２Ｂ | ○学籍関係<br>・卒業証書授与台帳<br>○成績関係<br>・評定一覧表・定期考査素点表<br>・定期考査の答案用紙・総合的な成績に関する個票や一覧<br>○指導関係<br>・事故報告書・記録簿・生徒指導・特別指導等記録簿<br>・教育相談・面接の記録､カード等<br>・個別の教育支援計画（学校生活支援シート）・個別指導計画<br>・家庭訪問記録・個別面談記録<br>○進路関係<br>・卒業生進路先一覧表・進路希望調査・調査書<br>・推薦書・私立高校入試に係る事前相談資料<br>○健康関係<br>・健康診断に関する表簿・健康診断票・歯牙検査簿<br>・心臓管理等医療情報・学校生活管理指導票<br>○児童・生徒に関する個人情報<br>（生活歴、心身の状況、財産状況等の情報、電話番号、個人メールアドレス、住所、生年月日、性別等の基本情報を含むもの）<br>○学校教職員に関する個人情報<br>（病歴、心身の状況、収入等の情報、電話番号、個人メールアドレス、住所、生年月日、性別等の基本情報を含むもの）<br>○教職員に割り当てた機密性の高い情報一覧<br>・情報システムログインID/PW・情報端末ログイン ID/PW<br>○児童生徒の学習系情報一覧<br>・情報システムログインID/PW・情報端末ログイン ID/PW | ○学籍関係<br>・出席簿<br>○指導関係<br>・教育相談、家庭訪問等の記録メモ<br>○成績関係<br>・小テスト、単元テスト、確認テストの成績一覧<br>○会議関係<br>・職員会議や学年会議等の資料（※３）<br>・教育委員会内における会議等の資料（※４） | |
| Ⅲ | セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす。 | ２Ａ | ２Ａ | ２Ａ | | ○成績関係<br>・小テスト・単元テスト・確認テストの問題、答案及び成績・評価<br>○名簿等<br>・児童生徒名簿・座席表・委員会名簿<br>○児童･生徒の学習情報<br>・児童･生徒の学習記録（ワークシート、レポート、作品等）<br>・学習活動の記録（動画・写真等）<br>○学校運営関係<br>・卒業アルバム<br>・学校教育活動（※２）の児童・生徒の写真<br>（他者と共有する場合は、共有する目的を明確にし、承諾を得ることが重要） | |
| Ⅳ | 影響をほとんど及ぼさない | Ⅰ | Ⅰ | Ⅰ | | | ○学校運営関係<br>・学校・学園要覧・学校紹介パンフレット・教育課程編成表<br>・学校行事実施計画（避難訓練・体育祭実施計画等）・保護者等への配布文書<br>・ＰＴＡ資料・学校､学年､学級だより・学校行事のしおり<br>○学校関係の記録<br>※保護者の承諾がある場合、以下は公開可能<br>・学校教育活動（※２）の児童・生徒の写真<br>・学習活動の記録（動画・写真・作品等） |

（※１）教育委員会が使用を認めているアプリケーションや学習支援ソフトを提供している企業等が利用しているクラウドサービス。
（※２）学校教育活動とは、授業、校外学習、部活動、委員会活動、学校行事、学級活動など、児童･生徒が学校で行う活動全般を言います。
（※３）校外への持ち出しが禁止されている情報が含まれる場合は、教育内部系（校務用）ネットワークを利用します。
（※４）課及び部署ごとで様々な情報を扱うことから、担当課でクラウドを活用するかを決定する。