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２年７月14日　改訂】

改　訂　履　歴			
初版	平成２５年１０月　１日	改訂　４	令和　１年１０月　１日
改訂　１	平成２７年　４月　１日	改訂　５	令和　２年　７月１４日
改訂　２	平成２７年　６月 18日	改訂　６	令和　　年　　月　　日
改訂　３	平成３１年　４月　１日	改訂　７	令和　　年　　月　　日

目次

第１章　情報セキュリティ基本方針

１．目的

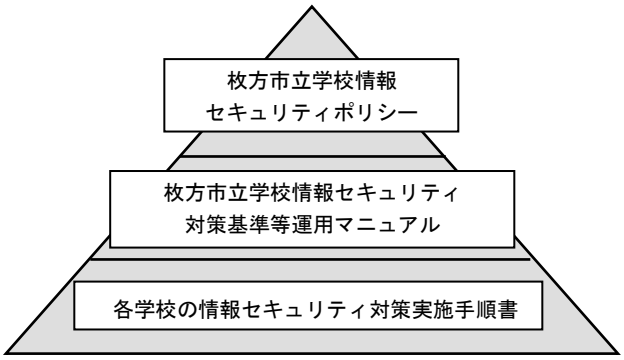
学校教育の情報化を進めるにあたっては、児童・生徒、その保護者、及びその他の関係者の個人情報を情報システムにより取り扱う機会が増大することから、個人情報を含む情報資産の一層適切な管理・運用が求められる。また、日々の授業をはじめとする教育活動や効率化が求められている校務処理における情報システムの活用が進み、システム運営の安定性の確保の観点から、学校における情報セキュリティ対策の強化が必要である。

本市においては、平成 15 年に策定した情報セキュリティポリシーに定めた対策基準の運用を行っているが、学校における情報セキュリティ対策をさらに実効あるものとするために、学校における情報ネットワーク構成の特異性及び学校独自の職制等を考慮した学校情報セキュリティポリシーを定めたものである。

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

枚方市立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］

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原則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．用語の定義

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することをいう。

（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）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（授業用）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」

児童生徒１人１台端末等、授業支援に用いるネットワーク

（７）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。

（８）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。

（９）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。

(10) 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。

(11) スマートデバイス

情報処理端末（デバイス）のうち、スマートフォンやタブレット型端末など、携行可能な多機能端末をいう。

(12) 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扱われる学校情報（これらを印刷した文書も含む。）

(13) 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。

(14) ASP／クラウド

庁外データセンター等でプログラムやデータベースを管理し、ネットワークを介してこれを利用する仕組みや概念。

(15) 移動体通信

電波等を利用してデータの送受信を行う、事業者が提供する広域向けの通信網システム

４．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

５．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ずるものとする。

（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）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ずる。

（３）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、必要な対策を講ずる。

（４）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ずる。

（５）運用

① 情報システムの監視、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、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、緊急時対応計画を整備する。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ずるよう努める。

６．学校情報セキュリティポリシーの適用範囲

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。

７．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。

８．教職員等の責務

（１）校長、教頭、教員、任期付職員、非常勤職員（審議会委員を除く）、会計年度任用職員、臨時職員などの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、情報セキュリティポリシーを順守しなければならない。

９．監査及び自己点検

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。

10．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、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

（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）適用範囲

本対策基準の適用範囲は、枚方市立の全小中学校（以下「市立学校」）、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。

（３）情報資産の分類と管理

①　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	上記Ⅰ、Ⅱ、Ⅲ以外

②　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、①の重要性分類を踏まえた管理体制、手順としなければならない。

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）学校情報統括責任者

教育長を学校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。

（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

学校教育部教育指導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

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名選任して教育指導課に報告するものとする。

（５）校内情報セキュリティ管理者

各学校の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

各学校の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、学校情報セキュリティポリシーの順守及び周知・啓発に努める。

（７）システム統括管理者及びシステム管理者

枚方市情報セキュリティポリシーの定義に準拠する。

（８）CSIRTへの連携

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、CSIRTとの連携を図る。

３．物理的セキュリティ対策

３．１．１　教育委員会サーバ等の機器の管理

（１） 機器の取り付け

① 教育委員会サーバ等の機器の取付けを行う場合は、定められた場所（中央図書館サーバ室）に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

② 教育委員会サーバ等の機器については、ラベルの貼付等、用途、種類等が明確に認識できるよう必要な措置を講じなければならない。

（２） サーバ等の二重化

重要情報を格納しているサーバ等は二重化し、ミラーリング等により同一データを保持する等の措置を講じるよう努めなければならない。

（３） 機器の電源

サーバ等の機器の電源については、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に、十分な電力を供給する容量の予備電源を備え付けなければならない。

（４） 通信ケーブル等の配線

① 通信ケーブル及び電源ケーブルについては、損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

② ネットワーク接続口（ハブのポート等）については、他者が容易に接続できない場所に設置する等適切に管理しなければならない。

（５） 機器の定期保守及び修理

① 情報システムの安定性を保つため、サーバ等については、機器の定期保守を実施する等の措置を講じるよう努めなければならない。

② 記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合は、修理を委託する事業者との間で、守秘義務契約を締結する等、秘密保持体制の確認などを行わなければならない。

（６） 機器の廃棄等

機器の廃棄等の場合は、機器内部の記憶装置から、すべての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

３．１．２ 校内サーバ等の機器の管理

（１） 機器の取付け

① 校内サーバ等の機器の取付けを行う場合は、校内の定められた場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

② 校内サーバ等の機器については、ラベルの貼付等、用途、種類等が明確に認識できるよう必要な措置を講じなければならない。

（２） データ管理

校内情報セキュリティ管理者は、校内サーバの不要なデータ削除、ＤＶＤ等のメディアに保存する等の措置を講じて、適正なデータ管理に努めなければならない。

（３） 機器の電源

学校情報セキュリティ管理者は、校内サーバ等の機器の電源については、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に、十分な電力を供給する容量の予備電源を備え付けなければならない。

（４） 通信ケーブル等の配線

① 通信ケーブル及び電源ケーブルについては、損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

② ネットワーク接続口（ハブのポート等）については、他者が容易に接続できない場所に設置する等適切に管理しなければならない。

（５） 機器の定期保守及び修理

① 情報システムの安定性を保つため、サーバ等については、機器の定期保守を実施する等の措置を講じるよう努めなければならない。

② 記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合は、修理を委託する事業者との間で、守秘義務契約を締結する等、秘密保持体制の確認などを行わなければならない。

（６） 機器の廃棄等

機器の廃棄等の場合は、機器内部の記憶装置から、すべての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

３．２．１　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）」）に準拠する。

３．２．２　コンピュータ教室等の管理

（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（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者は、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。

３．３　通信回線及び通信回線装置の管理

（１） 通信回線の管理

学校情報セキュリティ管理者は、校内の通信回線及び通信回線装置を施設総合教育部門と連携し、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

（２） 外部へのネットワーク接続

学校情報セキュリティ管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

（３） 通信回線の適切な選択と情報の暗号化

学校情報セキュリティ管理者は、情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

（４） 通信回線のセキュリティ対策

学校情報セキュリティ管理者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分な対策を実施しなければならない。

３．４　記録媒体の管理

（１） 記録媒体は、施錠可能な保管庫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） 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。

３．５　その他の機器の管理

（１） 端末機は盗難防止のため、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） スマートデバイスは盗難防止のため、施錠可能な保管庫に保管するなどの物理的措置を講じなければならない。

（３） 端末機及びスマートデバイスは盗難や不正アクセス等に備え、端末認証を必要とするように設定しなければならない。

（４） 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

４．人的セキュリティ対策

４．１ 教職員等の順守事項

（１） 教職員等の順守事項

① 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、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責任者は、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周知、徹底し、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、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

Ⅰ 教職員等は、私物の記録媒体等を校内に持ち込んではならない。

Ⅱ 教職員等は、私物のコンピュータ及びスマートデバイスに個人情報等の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。

４．２ 研修・訓練

（１） 学校情報セキュリティ責任者は、教職員等に対し、情報セキュリティの重要性について啓発に努めるとともに、学校情報セキュリティポリシーに関する研修及び訓練を定期的に実施しなければならない。

（２） システム管理者は、管理する情報システムの情報セキュリティの維持・向上のため、市立学校の教職員等に対し、研修及び訓練を定期的に実施しなければいけない。

（３） 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、研修及び訓練を定期的に実施しなければいけない。

４．３ 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、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 連絡を受けた校内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、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、学校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及び学校情報セキュリティ管理者は、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、保存しなければならない。

４．４ 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。

Ⅰ 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。

Ⅱ　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。

Ⅲ　IC カード等を紛失した場合には、速やかに校内情報セキュリティ責任者に報告し、指示に従わなければならない。

② 学校情報セキュリティ管理者は、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。

③ 学校情報セキュリティ管理者は、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。

② パスワードを記載したメモを作成してはならない。

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 パスワードを他人に知られたおそれがある場合には、パスワードを速やかに変更しなければならない。

⑤ パスワードは定期的に変更し、古いパスワードを再利用してはならない。

⑥ 複数の情報システムを扱う教職員等は、同一のパスワードをシステム間で用いてはならない。

⑦ 端末機のパスワードの記憶機能を利用してはならない。

５．技術的セキュリティ対策

５．１ サーバ及びネットワークの管理

（1） 共有ファイルサーバの設定

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共有ファイル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、共有ファイル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、当該教職員への注意、指導を行わなければならない。

④ 教職員等は、所属する学校の共有ファイル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、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） アクセス記録の取得等

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各種アクセス記録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。

（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 システム統括管理者、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、校内情報セキュリティ責任者は、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

枚方市情報セキュリティポリシーの規定（「６．１サーバ等及びネットワークの管理(10)」）に準拠する。

（８） 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。

（９） 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 児童生徒が扱う電子メールは、学校情報セキュリティ管理者が許可した相手だけに送受信できる設定にしなければならない。

(10) 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。

(11) 無許可でのネットワーク接続の禁止

教職員等は、学校情報セキュリティ管理者の許可なく端末機をネットワークに接続しては

ならない。

(12) 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、実行してはならない。

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、当該教職員への注意、指導を行わなければならない。

④ 学校情報セキュリティ管理者は、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。

(13) 無線LAN及び移動体通信の利用の制限

教職員等は、学校情報セキュリティ責任者が認めた場合に限り、教育外部系（授業用）ネットワーク、新教育外部系ネットワークの無線LAN及び移動体通信を利用することができる。

(14) スマートデバイスに係るセキュリティ管理

① 学校情報セキュリティ管理者及び校内情報セキュリティ責任者は、スマートデバイスが備える機能や使用環境、取り扱う情報、その他業務の特性等に応じ、適正なセキュリティ要件を定め、必要な対策を実施しなければならない。

② 教職員等は、スマートデバイスを使用するにあたり、学校情報セキュリティ管理者等が実施したセキュリティ対策及び、使用手順に従い、適正にスマートデバイスを使用しなければならない。

５．２　アクセス制御

（1） アクセス制御

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

Ⅰ 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。

Ⅱ 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

Ⅰ 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。

Ⅱ 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。

Ⅲ 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。

５．３ 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。

５．４ 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。

（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。

５．５　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内部ネットワーク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。

６．運用

６．１．１　情報システムの監視

（１） 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。

６．１．２　個人情報等を取り扱う端末の制限

（１） 教職員等は、重要性分類Ⅱ以上の情報資産を取り扱う場合は、学校情報セキュリティ管理者が許可する場所に設置した教育内部系（校務用）端末のみで行うものとする。

（２） 教職員等は、学校情報セキュリティ管理者が許可する場所に設置した教育内部系（校務用）端末を校内の他の場所に移動させてはならない。

６．１．３　記録媒体の使用の制限

（１） 記録媒体の使用

記録媒体は必ず公費で購入したものを使用し、私物の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責任者が使用を認めた学校の管理職以外は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および外付けフロッピーディスクの利用の制限

① 教育内部系（校務用）端末機においては、学校情報セキュリティ責任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責任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）端末機および児童生徒が利用するコンピュータ教室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。

６．１．４　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責任者が認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、データは各校に設置されている校内サーバまたは、学校情報セキュリティ責任者が認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責任者が認可したクラウドサーバに保存しなければならない。

６．１．５　インターネットの閲覧制限

（１） 教育内部系（校務用）端末機においては、学校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。

（２） 教育外部系（授業用）および新教育外部系端末機においては、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。

６．２　侵害（事故、欠陥等を含む）時の対応

（１） 緊急時対応計画の策定

校内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、緊急時対応計画を定めておき、侵害時には当該計画に従って、適切に対処するものとする。

（２） 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

① 関係者の連絡先

② 発生した事案に係る報告すべき事項
③ 発生した事案への対応措置
④ 再発防止措置の策定

（3） 事業継続計画との整合性確保

枚方市情報セキュリティポリシーの規定（「７．２侵害（事故、欠陥等を含む）時の対応（３）」）に準拠する。

（4） 緊急時対応計画の見直し

学校情報セキュリティ責任者は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の内容を見直さなければならない。

６．３ 外部委託

枚方市情報セキュリティポリシーの規定（「８．外部委託」）に準拠する。

６．４ 約款による外部サービスの利用

（1） 約款による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、以下を含む約款による外部サービスの利用に関する規定を整備すること。また、当該サービスの利用において機密性の高い情報が取り扱われないよう規定すること。

（ア）約款による外部サービスを利用してよい業務の範囲
（イ）業務に利用できる約款による外部サービス
（ウ）利用手続及び運用手順

（2）約款による外部サービスの利用における対策の実施

教職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクを許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用すること。

６．５ 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し、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。

６．６ 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） 著作権法
（3） 不正アクセス行為の禁止等に関する法律
（4） 個人情報の保護に関する法律
（5） 枚方市個人情報保護条例

7．評価・見直し

7．1　監査

（1） 監査の実施

教育委員会は、学校情報セキュリティポリシー及び学校情報セキュリティ対策実施手順が順守されているか、必要に応じて、別に定める規定に基づき、監査を行うものとする。

（2） 情報セキュリティポリシーの見直しへの活用

監査の結果、学校情報セキュリティポリシー及び学校情報セキュリティ対策実施手順の見直しが必要な場合は速やかに見直しを行うものとする。

7．2　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、学校情報セキュリティポリシー及び学校情報セキュリティ実施手順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、自己点検結果と自己点検に基づく改善策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、自己の業務の範囲内で改善を図らなければならない。

② 自己点検結果の報告等により、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は、速やかに見直しを行うものとする。

7．3　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、必要に応じて学校情報セキュリティポリシーの見直しを行う。