八尾市教育情報セキュリティポリシー

第２版

令和８年２月
八尾市教育委員会

目次

第１章 対象範囲及び用語説明

１．対象範囲

（１）対象機関の範囲

① 本セキュリティポリシーが適用される行政機関等は、八尾市教育委員会及び八尾市立学校（八尾市立小学校、中学校及び義務教育学校をいう。以下同じ。）とする。

（２）情報資産の範囲

本セキュリティポリシーが対象とする情報資産は、次のとおりとする。

① 教育情報ネットワーク、教育情報システム及びこれらに関する設備、電磁的記録媒体

② 教育情報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

２．用語説明

（１）本セキュリティポリシーにおける用語説明

① 校務系情報

児童生徒の成績、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、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

② 校務外部接続系情報

校務系情報のうち、保護者メールや学校ホームページ等インターネット接続を前提とした校務で利用される情報

③ 学習系情報（教育系情報）

児童生徒のワークシート、作品、アンケートなど、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

④ 校務外部接続用端末

校務外部接続系情報にアクセス可能な端末

⑤ 児童生徒用１人１台端末

学習系情報にアクセス可能な端末で、児童生徒が利用する端末

⑥ 教職員用端末

学習系情報、校務外部接続系情報あるいは校務系情報にアクセス可能な端末で、教職員のみが利用可能な端末

⑦ 校務系システム

校務系ネットワーク、校務系サーバ及び教職員用端末から構成される校務系情報を取り扱うシステム及び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

⑧ 校務外部接続系システム
校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ（CMS）及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム

⑨ 学習系システム
学習系ネットワーク、学習系サーバ、児童生徒用１人１台端末及び教職員用端末から構成される学習系情報を取り扱うシステム及び、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

⑩ 教育情報システム
校務系システム、校務外部接続系システム及び学習系システムを合わせた総称

⑪ 校務系サーバ
校務系情報を取り扱うサーバ

⑫ 学習系サーバ
学習系情報を取り扱うサーバ

⑬ 教育情報ネットワーク
八尾市立学校において、授業等で利用する学校教育のネットワーク

⑭アクセス制御
内部・外部からの不正アクセスを防御するために、多要素認証による強固な制御を含む利用者認証、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

⑮ 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

⑯ 可用性
情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性

⑰ 完全性
情報が破壊、改ざん又は消去されていない特性

⑱ 機密性
情報に関して、アクセスを認められた者だけがこれにアクセスできる特性

第２章 組織体制

１．組織体制

（１）統括教育情報セキュリティ責任者

① 教育長を統括教育情報セキュリティ責任者とする。

② 統括教育情報セキュリティ責任者は、教育情報ネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③ 統括教育情報セキュリティ責任者は、教育情報ネットワークにおける情報セキュリテ

ィ対策に関する権限及び責任を有する。

④ 統括教育情報セキュリティ責任者は、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者及び教育情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤ 統括教育情報セキュリティ責任者は、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、必要かつ十分な措置を行う権限及び責任を有する。

⑥ 統括教育情報セキュリティ責任者は、教育情報ネットワーク、教育情報システム及び情報資産に関する共通的な情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

⑦ 統括教育情報セキュリティ責任者は、緊急時には回復のための対策を講じなければならない。

（2）教育情報セキュリティ責任者

① 教育監を教育情報セキュリティ責任者とする。

② 教育情報セキュリティ責任者は、本市の教育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。

③ 教育情報セキュリティ責任者は、本市において所有している教育情報システムにおける開発、設定の変更、運用、見直し等を行う際の情報セキュリティに関する統括的な権限及び責任を有する。

④ 教育情報セキュリティ責任者は、本市において所有している教育情報システムについて、情報セキュリティポリシーの遵守に関する意見の集約及び教職員等（教職員、非常勤教職員及び臨時教職員をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。

（3）教育情報セキュリティ管理者

① 校長を教育情報セキュリティ管理者とする。

② 教育情報セキュリティ管理者は当該学校の情報セキュリティ対策に関する権限及び責任を有する。

③ 教育情報セキュリティ管理者は、当該学校において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、教育情報セキュリティ責任者及び統括教育情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

（4）教育情報システム管理者

① 教育センター所長を教育情報システムに関する教育情報システム管理者とする。

② 教育情報システム管理者は、所管する教育情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③ 教育情報システム管理者は、所管する教育情報システムにおける情報セキュリティに関する権限及び責任を有する。

④ 教育情報システム管理者は、所管する教育情報システムに係る情報セキュリティ実施

手順の維持・管理を行う。

（５）教育情報システム担当者

① 教育センター職員を教育情報システムに関する教育情報システム担当者とする。

② 教育情報システム担当者は、教育情報システム管理者の指示等に従い、教育情報システムの開発、設定の変更、運用、更新等の作業を行う。

（６）兼務の禁止

① 情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

② 監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

第３章 情報資産の分類と管理方法

１．情報資産の分類

（１）重要性分類

① 本市における情報資産は、機密性、完全性及び可用性の３つの観点から影響度を評価し、次のとおり４段階の重要性分類を行い、必要に応じて取扱制限を行うものとする。

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。

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。（Ⅰを除く）

Ⅲ：セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼす。（Ⅱ以上を除く）

Ⅳ：セキュリティ侵害が学校事務及び教育活動の実施に影響をほとんど及ぼさない。（Ⅲ以上を除く）

分類	校務系	学習系	学習系あるいは 校務外部接続系
Ⅰ	○指導要録原本 ○教職員の人事情報		
Ⅱ	○学籍関係 ○成績関係 ○指導関係 ○進路関係 ○児童生徒及び教職員に関する個人情報 ○健康関係 ○教職員に割り当てた機密性の高い情報（システムログイン ID/PW 等） ○名簿等（児童生徒名簿、緊急連絡網、住所録等）	○児童生徒の学習系情報（学習システムログイン ID/PW 管理台帳、学習用端末 ID/PW 管理台帳）	

Ⅲ	○児童生徒の名前（座席表、名列表等） ○学校運営関係	○学校運営関係（授業用教材、教材研究資料等） ○児童生徒の学習系情報（児童生徒の学習記録、学習活動の記録、アンケート回答）	○学校運営関係（欠席連絡等）
Ⅳ			○学校運営関係（学校要覧、学校紹介パンフレット等） ○学校活動の記録 ※保護者の承諾がある場合、以下は公開可能 ・学校行事等の児童生徒写真 ・学習活動の記録

図表１　情報資産の例示

※文部科学省「教育情報セキュリティポリシーに関するガイドライン（令和７年３月）」内の例示を参考

２．情報資産の管理

（１）管理責任

① 統括教育情報セキュリティ責任者は、教育情報セキュリティポリシーに基づき、学校現場での教育情報セキュリティ運用管理に関する実施手順ひな形を作成しなければならない。

② 教育情報セキュリティ管理者は、実施手順ひな形に基づき、自校の実施手順を作成しなければならない。

③ 教育情報セキュリティ管理者は、自校の所管する情報資産について管理責任を有する。

④ 教育情報セキュリティ管理者は、教職員等の情報資産の取扱いに際し、実施手順に基づいた運用管理を指導しなければならない。

⑤ 教職員等は、実施手順に基づき、適切に情報資産を取り扱わなければならない。

（２）情報資産の取扱い

① 情報の作成および入手

㋐ 教職員等は、業務上必要のない情報を作成および入手してはならない。

㋑ 情報を作成する教職員等は、作成途上の情報についても、取扱いを許可されていない者の閲覧や紛失・流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

② 情報資産の利用

㋐ 情報資産を利用する教職員等は、業務以外の目的に情報を利用してはならない。

㋑ 情報資産を利用する教職員等は、情報資産の分類に応じ、適切な取扱いをしなければならない。

（３）情報資産の保管

① 教育情報セキュリティ管理者又は教育情報システム管理者の措置事項

㋐ 教育情報セキュリティ管理者は、情報資産の保管先を定め、教職員等に周知しなければならない。

㋑ 教育情報セキュリティ管理者又は教育情報システム管理者は、情報資産を記録したUSB メモリ等の外部電磁的記録媒体を保管する場合は、外部電磁的記録媒体への書込禁止の措置を講じなければならない。

㋒ 教育情報セキュリティ管理者又は教育情報システム管理者は、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電磁的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地域に保管しなければならない。なお、クラウドサービスを利用する場合はサービスの機能として自然災害対策がなされていることを確認すること。

㋓ 教育情報セキュリティ管理者又は教育情報システム管理者は、重要性分類Ⅲ以上の情報を記録した電磁的記録媒体を保管する場合、耐火、耐震、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

② 教職員等の遵守事項

㋐ 教職員等は、教育情報セキュリティ管理者が指定した保管先にのみ情報資産を保管しなければならない。

㋑ 教職員等は、児童生徒が生成する学習系情報の保管先について児童生徒に指示し、それ以外の場所に保管しないよう指導しなければならない。

（4）情報資産の外部持ち出し

① 分類に応じた情報資産の外部持ち出し制限

教職員等は、重要性分類Ⅱ以上の情報資産を外部持ち出しする場合は、教育情報セキュリティ管理者を通して教育情報セキュリティ責任者に報告し、個別許可を得なければならない。また、限定されたアクセスの措置設定（アクセス制限や暗号化）を行い、持ち出し持ち帰りの記録をつけなければならない。なお、外部持ち出しツールに限定されたアクセスの措置設定（アクセス制限や暗号化）機能を有する場合には、有効にしなければならない。

② 電子メール、外部ストレージサービスによる情報の送信

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、外部ストレージサービスにより重要性分類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（アクセス制限や暗号化）を行わなければならない。

㋑ 利用する電子メール、外部ストレージサービスは教育委員会又は学校から提供される公式サービスのみを利用し、私的に契約したサービスを利用してはならない。

③ 外部電磁的記録媒体を用いた情報の外部持ち出し

USB メモリ等の物理的な媒体による情報の外部持ち出しでは、紛失・盗難リスクを伴うことから以下を遵守しなければならない。

㋐ 管理された機器以外の使用禁止：教育委員会又は学校から支給された公的な機器のみを利用すること。

④ FAX による情報の送信

FAX による情報の送信は、限定されたアクセスの措置（アクセス制限や暗号化）が不可能であること、誤送信のリスクがあることに鑑み、原則として、送信相手が FAX 受信を指定してきた場合等、FAX 利用がやむを得ない場合にのみ利用すること。

（5）情報資産の破棄

① 情報資産を廃棄する教職員は、重要性分類Ⅲ以上の情報が記載された紙媒体の書類を廃棄する場合には、内容が復元できないように細断、熔解またはこれに準ずる方法にて廃棄しなければならない。

② 情報を記録している電磁的記録媒体を利用しなくなった場合、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。

③ 業者に廃棄委託する場合、廃棄する情報資産を業者が引き取る際、教職員等が立ち会わなければならない。

第４章 物理的セキュリティ

１．サーバ等の管理

（1）サーバ等の管理

① 機器の取付け

教育情報システム管理者は、サーバ等の機器の取付けを行う場合、地震、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、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 機器の電源

㋐ 教育情報セキュリティ責任者及び教育情報システム管理者は、施設管理部門と連携し、重要性分類Ⅱ以上の情報資産を格納しているサーバ等の機器の電源について、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。

㋑ 教育情報セキュリティ責任者及び教育情報システム管理者は、施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

③ 通信ケーブル等の配線

㋐ 教育情報セキュリティ責任者及び教育情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの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。

㋑ 教育情報セキュリティ責任者及び教育情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

㋒ 教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク接続口

を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。

㋓ 教育情報セキュリティ責任者及び教育情報システム管理者は、自ら又は教育情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更又は追加できないように必要な措置を施さなければならない。

④ 機器の定期保守及び修理

㋐ 教育情報システム管理者は、重要性分類Ⅲ以上のサーバ等の機器の保守点検を実施しなければならない。

㋑ 教育情報システム管理者は、電磁的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、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とともに秘密保持体制の確認等を行わなければならない。

⑤ 機器の廃棄等

教育情報システム管理者は、機器を廃棄又はリース返却等をする場合、機器内部の記憶装置から、全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。

２．管理区域の管理

（１）管理区域の構造等

① 管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋（以下「サーバ室」という。）や電磁的記録媒体の保管庫をいう。

② 教育情報セキュリティ責任者及び教育情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

③ 教育情報セキュリティ責任者及び教育情報システム管理者は、サーバ室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

（２）管理区域の入退室管理等

① 教育情報システム管理者は、管理区域への入退室を許可された者のみに制限し、入退室管理簿の記載等による入退室管理を行わなければならない。

② 地方公共団体職員等及び外部委託事業者が、管理区域に入室を許可する場合、これらの者に身分証明書等を携帯させ、必要に応じ、その提示を求めなければならない。

③ 教育情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限しなければならない。また、管理区域への入退室を許可されたそれぞれのシステムの管理担当職員が付き添うものとし、外見上当該職員と区別できる措置を講じなければならない。

④ 教育情報システム管理者は、重要性分類Ⅱ以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（３）機器等の搬入出

① 教育情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ搬入する機器の管理担当職員又は委託した業者に確認を行わせなければならない。

② 教育情報システム管理者は、情報システム室の機器等の搬入出について、搬入する機器の管理担当職員を立ち会わせなければならない。

3．通信回線及び通信回線装置の管理

（1）通信回線及び通信回線装置の管理

① 教育情報セキュリティ責任者は、施設内の通信回線及び通信回線装置を、施設管理部門と連携し、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 教育情報セキュリティ責任者は、外部へのネットワーク接続ポイント及び該当ポイントに接続される端末を正確に把握し、適切な管理を行わなければならない。

③ 教育情報セキュリティ責任者は、重要性分類Ⅲ以上の情報資産を取り扱う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、インターネットを通信経路とする回線の場合、通信の暗号化を行わなければならない。

④ 教育情報セキュリティ責任者は、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セキュリティ対策を実施しなければならない。

⑤ 教育情報セキュリティ責任者は、重要性分類Ⅱ以上の情報資産を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。

⑥ 運用開始前にはネットワークの帯域確保などを十分検証し、利用状況に応じて改修計画を行うこと。

⑦ 学校内の無線通信の干渉による影響がないよう留意すること。

⑧ 無線 LAN の接続の際には、クライアント証明書を用いる等、教育委員会が配備したパソコン等以外がアクセスできないよう対策を講じること。

4．教職員等の利用する端末や電磁的記録媒体等の管理

（1）教職員等の利用する端末や電磁的記録媒体等の管理

① 教育情報システム管理者は、不正アクセス防止のため、ログイン時の ID 及びパスワードによる認証、加えて多要素認証の実施等、取り扱う情報の重要度に応じて適切な物理的措置を講じなければならない。電磁的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 教育情報システム管理者は、校務系システム、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 教育情報システム管理者は、端末の電源起動時のパスワード（BIOS パスワード、ハー

ドディスクパスワード等）を設定しなければならない。

④ 教育情報システム管理者は、取り扱う情報の重要度に応じて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。特に校務情報等の重要な情報資産へのアクセスについては、多要素認証を必須とすること。パブリッククラウド上で重要な情報（重要性分類Ⅱ以上）を取り扱う際には、多要素認証を含む強固なアクセス制御による対策を講じなければならない。ただし、児童生徒またはその保護者が重要性分類Ⅱ以上の情報資産にアクセスする場合は、児童生徒本人またはその保護者が、当該児童生徒に関するもののみにアクセスすることを想定していることから、多要素認証を設定することが望ましいものの、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際のロック機能の有効化、パスワードの複雑性の確保等により本人確認を厳格に行う前提で、ID 及びパスワードでの認証を許容する。

⑤ 教育情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末に暗号化機能を持つセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。

⑥ 教育情報システム管理者は、特に強固なアクセス制御による対策を講じたシステム構成の場合、重要性分類Ⅲ以上の情報資産を取り扱う端末に対し、当該データ暗号化等の措置により、不正アクセスや教員の不注意等による情報流出への対策を講じなければならない。

⑦ 教育情報システム管理者は、パソコンやモバイル端末におけるマルウェア感染の脅威に対し、ウイルス対策ソフトの導入等の対策を講じなければならない。なお、OS によっては標準的にウイルス対策ソフトを備えている製品、OS としてウイルス感染のリスクが低い仕組みとなっている製品などもあるため、実際に運用する端末において適切な対策を講じること。強固なアクセス制御による対策を講じたシステム構成の場合、重要性分類Ⅱ以上の校務情報等の重要な情報資産を取り扱う端末に対し、当該端末の状況および通信内容を監視し、異常、あるいは不審な挙動を検知する仕組み（ふるまい検知）等の活用を検討し、適切な対策を講じること。

⑧ 教育情報システム管理者は、インターネットへ接続をする場合、教職員等のパソコン、モバイル端末に対して不適切なウェブページの閲覧を防止する Web フィルタリング等の対策を講じなければならない。

５．児童生徒用１人１台端末のセキュリティ対策

（１）児童生徒用１人１台端末のセキュリティ対策

① 不適切なウェブページの閲覧防止

児童生徒が端末を利用する際には、Web フィルタリング、検索エンジンのセーフサーチ、セーフブラウジングなどを活用し、不適切なウェブページの閲覧を防止するための対策を講じなければならない。

② マルウェア感染対策

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。

③ 端末を不正利用させないための防止策

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。

④ セキュリティ設定の一元管理

児童生徒への端末配付後においても、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環境を整備することが望ましい。

６．教室等における児童生徒用１人１台端末や電磁的記録媒体の管理

（１）教室等における児童生徒用１人１台端末や電磁的記録媒体の管理

① 教育情報システム管理者は、盗難防止のため、教室等で利用する児童生徒用１人１台端末の保管庫による管理等の物理的措置を講じなければならない。

② 教育情報システム管理者は、児童生徒用１人１台端末及び電磁的記録媒体について、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。

③ 教育情報システム管理者は、情報システムへのアクセスにおけるログインパスワードの入力等による認証を設定しなければならない。

第５章 人的セキュリティ

１．教育情報セキュリティ管理者の措置事項

（１）情報資産の管理

① 教育情報セキュリティ管理者は、教職員等による情報資産の外部持ち出しが行われないよう、管理しなければならない。

② 教育情報セキュリティ管理者は、廃棄処理を外部に委託する場合は、学校の外に委託業者が持ち出す行為に教職員等が立ち合うように指示し、誤廃棄を予防しなければならない。

（２）教職員等の情報セキュリティ意識醸成

① 教育情報セキュリティ管理者は、教職員等に対して、日頃から情報セキュリティに関する話題を積極的に提供し、情報セキュリティ研修を受講させるなど、積極的にセキュリティ認識の向上を図らなければならない。

② 教育情報セキュリティ管理者は、校内でセキュリティ事故につながりかねないヒヤリ・ハット事案を抑止するために、教職員等が事案を発見した際に、ただちに対処し、すみやかに報告が上がるよう、セキュリティ意識の醸成に努めなければならない。

③ 教育情報セキュリティ管理者は、教職員等が常に教育情報セキュリティポリシー及び

実施手順を閲覧・確認できるように配慮しなければならない。

④ 教育情報セキュリティ管理者は、新規採用教職員等及び他自治体から本市に新規赴任した教職員等、及び非常勤及び臨時の教職員に対し、教育情報セキュリティポリシー等遵守すべき内容を理解・浸透するように指導を行わなければならない。

（3）端末等の持ち込みの記録

① 教育情報セキュリティ管理者は、端末等の持ち込みについて、「第５章 人的セキュリティ　２．教職員等の遵守事項　（4）貸与以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用」に基づき許可を行った場合は、個人保有情報機器使用許可報告書(第１号様式)を作成し、教育情報セキュリティ責任者に報告しなければならない。

② 教育情報セキュリティ管理者は、前項により使用を許可した情報機器については、教育系情報の事務に使用する範囲内で適用させる。また、学校予算等により購入した情報機器も、教職員保有の情報機器と同様の扱いとする。

（4）新規ソフトウェア及びコンテンツの導入・利用判断

① 教育情報セキュリティ管理者は、教職員等から、導入したソフトウェア・コンテンツの制限解除や、業務上新たなソフトウェア・コンテンツの導入について、事前に相談があった場合は、教育情報システム管理者に報告して、判断を仰がなければならない。

（5）インターネット接続及び電子メール利用の制限

① 教育情報セキュリティ管理者は、教職員等に業務端末による作業を行わせる場合において、業務以外でのインターネット接続及び電子メールの利用をしないよう教職員等に指導しなければならない。なお Web フィルタリングの設定について、教職員等から相談があった場合は、教育情報システム管理者に報告して、判断を仰がなければならない。

２．教職員等の遵守事項

（1）教育情報セキュリティポリシー等の遵守

① 教職員等は、教育情報セキュリティポリシー及び実施手順を遵守しなければならない。

（2）執務上での管理

① 教職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報資産が印刷された文書等について、第三者に使用されること又は教育情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧され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。

（3）貸与端末の取扱い

① 教職員等は、業務以外の目的での端末の使用および情報資産の外部への持ち出し、教育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。

② 教職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を変更してはならない。

（４）貸与以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

① 教職員等は、業務上やむを得ない場合を除いて、教育委員会貸与以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、教育情報セキュリティ管理者の許可を得て利用することができるが、その場合であっても校務系情報を取り扱ってはならない。

（５）モバイル端末や電磁的記録媒体等の持ち出し及び教育委員会・学校が構築・管理している環境（本セキュリティポリシーが適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境）の外部における情報処理作業の制限

① 教職員等は、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、教育情報セキュリティ管理者の許可を得なければならない。

② 教職員等は、外部（主に他の八尾市立学校）で情報処理業務を行う場合には、教育情報セキュリティ管理者の許可を得なければならない。

（６）ID の取扱い

教職員等は、自己の管理する ID に関し、次の事項を遵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。

（７）パスワードの取扱い

教職員等は、自己の管理するパスワードに関し、次の事項を遵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。

③ パスワードを他の人には知られないよう、教職員は児童生徒を指導すること。忘れた場合及び漏洩した場合はすぐに教職員に報告させ、再設定を行うこと。

④ パスワードが流出したおそれがある場合には、教育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。

（８）教職員等の管理する IC カード等の取扱い

① 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。

② 業務上必要のないときは、IC カード等をカードリーダ若しくはパソコン等の端末のスロット等から抜いておかなければならない。

③ IC カード等を紛失した場合には、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に通報し、指示に従わなければならない。

（９）外部電磁的記録媒体の取扱い

① 利用する外部電磁的記録媒体は教育委員会又は学校から貸与された媒体を使用しなければならない。

② 外部電磁的記録媒体は、職員室の書庫等の鍵のかかる場所に施錠保管しなければならない。

(10) 電子メールの利用制限

① 市の電子メール利用制限に準じるものとする。

(11) クラウドサービス、ソーシャルメディアサービス利用制限

① 重要性分類Ⅰの情報資産は、インターネットを通信経路としたパブリッククラウドサービスで取り扱ってはならない。
② 重要性分類Ⅱの情報資産を、インターネットを通信経路としたパブリッククラウドサービスで取り扱う場合、通信を暗号化し第三者による傍受を防ぐなどの対策を講じなければならない。
③ 私的に契約したクラウドサービスや個人アカウントを業務利用してはならない。
④ ソーシャルメディアサービスを利用して、業務上知り得た情報を公開してはならない。

(12) 不正プログラム対策に関する教職員等の遵守事項

① パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。また、自動更新される設定の場合は、自動更新設定を変えてはならない。
② 外部からデータ又はソフトウェ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ェ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 コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、すみやかに教育情報セキュリティ管理者に報告し、指示を仰がなければならない。また、以下の対応を行わなければならない。
㋐ パソコン等の端末の場合、有線 LAN につながる業務端末（教職員用端末等）の場合は、LAN ケーブルの即時取り外しを行わなければならない。
㋑ モバイル端末の場合、無線 LAN につながる業務端末（教職員用端末及び１人１台端末）の場合は、直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。
㋒ 上記の措置を実施後、直ちに当該機器をシャットダウンしなければならない。

(13) 電子署名・暗号化

① 教職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、定められた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

(14) 無許可ソフトウェアの導入等の禁止

① 教職員等は、パソコン等に無断でソフトウェ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、教育情報システム管理者に書面による許可を得て、ソフトウェアを導入することができる。なお、管理者権限が必要なソフトウェア導入作業については、教育情報システム担当者が対応するものとする。
③ 教職員等は、不正にコピーしたソフトウェアを利用してはならない。

(15) 機器構成の変更の制限

① 教職員等は、教育委員会が貸与したパソコンやプリンタ等に対し機器の改造及び増設・交換を行ってはならない。

(16) ネットワーク接続の禁止

① 教職員等は、教育委員会が貸与したパソコンやプリンタ等以外を八尾市地域イントラネットワークに接続してはならない。

(17) 業務以外の目的でのウェブ閲覧の禁止

① 教職員等は、業務以外の目的でウェブを閲覧してはならない。

3．教育委員会事務局職員の遵守事項

（1）教育委員会事務局職員の遵守事項

① 教育委員会事務局職員は、教育情報セキュリティ責任者の指導の下、以下の規定を遵守しなければならない。

㋐ 八尾市教育情報セキュリティポリシー等の遵守

㋑ 業務以外の目的での使用の禁止

㋒ 教職員用端末による外部における情報処理作業の禁止

㋓ 重要性分類Ⅱ以上の情報資産について教職員用端末以外のパソコン、モバイル端末及び電磁的記録媒体等によるアクセスの禁止

㋔ 職務上知りえた情報の秘匿

㋕ 業務を離れる場合の遵守事項

4．児童生徒の遵守事項

（1）児童生徒に児童生徒用１人１台端末等を利用させるにあたり教職員が指導すべき事項

① 貸与された児童生徒用１人１台端末やモバイルルータ及び学習系クラウドサービスは学習目的で利用すること。

② ID及びパスワードなど利用者認証情報は他の人に知られないようにすること。

③ 利用する端末のセキュリティ機能の設定を、許可なく変更してはならないこと。

④ 無断で外部ソフトウェアをインストールしないようにすること。

⑤ 学校から許可されたコミュニケーションツール（SNS、チャット等）のみを利用すること。

⑥ 学習用端末が動作しない、勝手に操作されている、いつもと異なる画面や警告が表示される、ウイルス感染が疑われるなどの症状がでた場合、すぐに担任教員に報告すること。

⑦ 学習用端末は大事に取り扱い、盗難・紛失・破損等に注意すること。また、端末等を破損あるいは紛失した場合には、すぐに教職員に報告すること。

⑧ 私物端末など許可されていない端末を学校に持ち込んで、学校のネットワークにつながないこと。

⑨ メールを送信する必要が生じた場合には、誤った宛先や必要のない宛先に送付しないよう、送付前によく確認すること。また、差出人が不明または不自然に添付されたファイルを受信した場合は、開封する前に教職員に報告すること。

⑩ 学校内外で動画や写真の撮影を行う場合は適切な許可を得てから行うこと。

⑪ 端末で生成した情報の保存先を学習系クラウドに指定できる機能がある場合には、この機能を利用して原則学習系クラウドに保管し、児童生徒用１人１台端末本体への保存は必要最小限とすること。

⑫ 重要性分類Ⅱ以上の情報資産（児童生徒本人の情報に限る）を児童生徒用１人１台端末にダウンロードした場合には、目的を達成した時点で速やかにデータを削除すること。また、該当資産を閲覧する際には、離席時には端末ロックする、周囲に他の児童生徒がいる状態では閲覧しない等の対策を講じること。

５．研修・訓練

（１）情報セキュリティに関する研修・訓練

① 教育情報システム管理者は、教職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行うこと。

（２）研修計画の策定及び実施

① 研修計画において、毎年度最低１回は教職員対象の情報セキュリティ研修を開催しなければならない。

② 新規採用の教職員等を対象とする情報セキュリティの内容を含んだ研修を実施しなければならない。

③ 研修は、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム担当者及びその他教職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

６．情報セキュリティインシデントの連絡体制の整備

（１）学校内からの情報セキュリティインシデントの報告

① 教職員等は、情報セキュリティインシデントを認知した場合、速やかに教育情報セキュリティ管理者に報告しなければならない。

② 報告を受けた教育情報セキュリティ管理者は、速やかに統括教育情報セキュリティ責任者、教育情報システム管理者に報告しなければならない。

③ 教育情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じて統括教育情報セキュリティ責任者及び教育情報セキュリティ責任者に報告しなければならない。

（２）学校内からの情報セキュリティ違反行為の報告

① 教職員等は、教育情報セキュリティポリシーに対する違反行為を発見した場合、直ちに教育情報セキュリティ管理者に報告を行わなければならない。

② 違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると教育情報セキュリティ管理者が判断した場合は、教育情報セキュリティ責任者に報告を行い適切に対処しなければならない。

（3）住民等外部からの情報セキュリティインシデントの報告

① 教職員等は、管理対象のネットワーク及び教育情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、教育情報セキュリティ管理者に報告しなければならない。

② 報告を受けた教育情報セキュリティ管理者は、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に報告しなければならない。

（4）情報セキュリティインシデントの原因の究明・記録等

① 統括教育情報セキュリティ責任者は、情報セキュリティインシデントについて、原因を調査し、記録を保存しなければならない。

第6章 技術的セキュリティ

1．コンピュータ及びネットワークの設定管理

（1）ファイルサーバ及び端末の設定等

① 教育情報システム管理者は、教職員等が使用できるファイルサーバの容量を設定するものとする。

② 教育情報システム管理者は、業務遂行にあたり最低限必要な範囲内においてフォルダ及びファイルを使用できるように設定しなければならない。

③ 教育情報システム管理者は、住民の個人情報、人事記録等、特定の教職員等しか取扱えないデータについて、特に必要がある場合は別途ディレクトリを作成する等の措置を講じ、同一学校等であっても、特定の教職員以外がアクセスできない領域を作成することができるものとする。

（2）バックアップの実施

① 教育情報セキュリティ責任者及び教育情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、校務系情報については、定期的にバックアップを実施しなければならない。また、教育系情報については、必要に応じて教育情報システム管理者がバックアップを実施しなければならない。

（3）ログの取得等

① 教育情報セキュリティ責任者及び教育情報システム管理者は、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 教育情報セキュリティ責任者及び教育情報システム管理者は、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（4）ネットワークの接続制御、経路制御等

① 教育情報セキュリティ責任者は、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、所管するネットワークの内部におけるファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

② 教育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、所管する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。

（5）外部の者が利用できるシステムの分離等

① 教育情報システム管理者は、保護者等の外部の者が利用できるシステム等がある場合、重要性が高い情報、特に情報資産重要性分類Ⅱ以上を扱うシステムとの論理的又は物理的な分離、もしくは各システムにおけるアクセス権管理の徹底を行うこと。

（6）外部ネットワークとの接続制限等

① 教育情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には統括教育情報セキュリティ責任者の許可を得なければならない。

② 教育情報システム管理者は、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。

③ 教育情報システム管理者は、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。

④ 教育情報セキュリティ責任者及び教育情報システム管理者は、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。

⑤ 教育情報システム管理者は、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、統括教育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。

（7）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 教育情報システム管理者は、アクセス制御による対策を講じたシステム構成の場合は、各システムにおけるアクセス権管理を徹底しなければならない。

ネットワーク分離による対策を講じたシステム構成の場合は、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）を論理的又は物理的に分離をしなければならない。

② 教育情報システム管理者は、校務系システムとその他のシステム（校務外部接続系システム、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。

（8）複合機のセキュリティ管理

① 教育情報セキュリティ責任者は、複合機を調達及び運用をする場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

② 教育情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

（9）特定用途機器のセキュリティ管理

① 教育情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施しなければならない。

(10) 無線 LAN 及びネットワークの盗聴対策

① 統括教育情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な通信の暗号化及び認証技術の使用を義務付けなければならない。

② 統括教育情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、通信の暗号化等の措置を講じなければならない。

(11) 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、必要がある場合を除き、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、重要な電子メールを誤送信した場合、教育情報セキュリティ管理者に報告しなければならない。

⑤ 教職員等は、ウェブで利用できるフリーメールサービス等を統括教育情報セキュリティ責任者の許可無しに使用してはならない。

⑥ メールを送信する際には、誤った宛先や必要のない宛先に送付しないよう、送付前によく確認すること。

⑦ 児童生徒が差出人不明または不自然に添付されたファイルを受信した場合は、開封する前に教職員に報告させなければならない。

２．アクセス制御

（1）アクセス制御

① 教育情報セキュリティ責任者又は教育情報システム管理者は、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。特に強固なアクセス制御による対策を講じたシステム構成の場合、重要性分類Ⅱ以上の情報資産へのアクセスについては、当該システムへの認証強度の向上とアクセス権管理を徹底すること。

（2）特権を付与された ID の管理等

① 教育情報システム管理者は、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。

② 教育情報システム管理者の特権を代行する者は、教育情報システム管理者が指名した者でなければならない。

③ 教育情報システム管理者は、特権を付与された ID 及びパスワードの変更について、外部委託事業者に行わせてはならない。

3．システム開発、導入、保守等

（1）情報システムの調達

① 教育情報セキュリティ責任者及び教育情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

② 教育情報セキュリティ責任者及び教育情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（2）情報システムの開発

① 教育情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

（3）情報システムの導入

① 教育情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

② 教育情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

③ 教育情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

④ 教育情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

（4）システム開発・保守に関連する資料等の整備・保管

① 教育情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

4．不正プログラム対策

（1）統括教育情報セキュリティ責任者の措置事項

① 外部ネットワークから受信したファイルは、インターネットのゲートウェイなどにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムの

システムへの侵入を防止しなければならない。

② 外部ネットワークに送信するファイルは、インターネットのゲートウェイなどにおいてコンピュータウイルス等不正プログラムのチェックを行い、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。

③ 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。

④ 所掌するサーバ及びパソコン等の端末に、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ェアを常駐させ、常に安全な状態に保たなければならない。

（2）教育情報システム管理者の措置事項

① 教育情報システム管理者は、その所掌するサーバ及びパソコン等の端末を守るため、コンピュータウイルス等の不正プログラムへの対策を講じなければならない。

② 不正プログラム対策を実施し、常に最新な状態に保たなければならない。

③ インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、市が管理している電磁的記録媒体以外を教職員等に利用させてはならない。

（3）教職員等の遵守事項

① パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

② 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。

③ 端末に対して、不正プログラム対策ソフトウェアによるチェックを定期的に実施しなければならない。

④ 教育情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。

⑤ コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、直ちに利用を中止し、LAN ケーブルの即時取り外しや機内モード等、通信を行わない設定への変更を行った後、当該機器をシャットダウンしなければならない。

5．不正アクセス対策

（1）統括教育情報セキュリティ責任者の措置事項

① 使用されていないポート及び SSID（無線 LAN ネットワーク名）を閉鎖しなければならない。

② 不要なサービスについて、機能を削除又は停止しなければならない。

③ 統括教育情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

（2）攻撃の予告

① 統括教育情報セキュリティ責任者は、サーバ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。

（3）サービス不能攻撃

① 統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じるよう努めなければならない。

（4）標的型攻撃

① 統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じるよう努めなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じるよう努めなければならない。

（5）記録の保存

① 統括教育情報セキュリティ責任者は、サーバ等に攻撃を受け、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。

（6）教職員等による不正アクセス

① 統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等による不正アクセスを発見した場合は、当該教職員等が所属する学校等の教育情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

6．セキュリティ情報の収集

（1）セキュリティホールに関する情報の収集及び共有並びにソフトウェアの更新等

① 教育情報セキュリティ責任者及び教育情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（2）不正プログラム等のセキュリティ情報の収集及び周知

① 教育情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、教職員等に周知しなければならない。

（3）情報セキュリティに関する情報の収集及び共有

① 教育情報セキュリティ責任者及び教育情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

第７章 運用

１．情報システムの監視

（１）情報システムの監視

① 教育情報セキュリティ責任者及び教育情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを監視できる措置を講じなければならない。

② 教育情報セキュリティ責任者及び教育情報システム管理者は、重要なログ等を取得するサーバの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。

２．ドキュメントの管理

（１）情報システム仕様書等の管理

① 教育情報セキュリティ責任者及び教育情報システム管理者は、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による閲覧や紛失等がないよう、適切に管理しなければならない。

（２）障害記録の管理

① 教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

（３）記録の保存

① 教育情報セキュリティ責任者は、サーバ等に攻撃を受け、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、関係部局との緊密な連携に努めなければならない。

３．教職員等の ID 及びパスワードの管理

（１）利用者 ID の取扱い

① 統括教育情報セキュリティ責任者及び教育情報システム管理者は、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、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

② 教育情報セキュリティ責任者及び教育情報システム管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検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 教育情報セキュリティ責任者又は教育情報システム管理者は、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。パスワードファイルを不正利用から保護するため、オペレーティングシステム等で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。

４．IC カード等の取扱い

（１）IC カード等の取扱い

① 統括教育情報セキュリティ責任者及び教育情報システム管理者は、IC カード等の紛失等の通報があり次第、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。

５．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 登録について、ID 登録やパスワードポリシーは教育委員会にて一元管理し、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や、児童生徒の発達段階に応じた複雑性を上げたパスワードポリシーによりセキュリティ強度を上げていくなど適切な措置を講じなければならない。

② 転出/卒業/退学時の ID 削除処理

㋐ 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、八尾市立学校の在学期間を超えて個人を特定する情報を保持しないようにすること。

㋑ 転出や卒業、退学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。

（２）多要素認証等によるなりすまし対策

① 本人確認を厳格に行う必要がある場合においては児童生徒の ID 及びパスワードに加えて多要素認証を設定すること。パブリッククラウド上で重要な情報（重要性分類Ⅱ以上）を取り扱う際には、多要素認証を含む強固なアクセス制御による対策を講じなければならない。ただし、児童生徒またはその保護者が重要性分類Ⅱ以上の情報資産にアクセスする場合は、児童生徒本人またはその保護者が、当該児童生徒に関するもののみにアクセスすることを想定していることから、多要素認証を設定することが望ましいものの、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際のロック機能の有効化、パスワードの複雑性の確保等により本人確認を厳格に行う前提で、ID 及びパスワードでの認証を許容する。

（３）学習用ツールへのシングルサインオン

① 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 及び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。

６．特権を付与された ID の管理等

（１）特権を付与された ID の管理等

① 教育情報セキュリティ責任者及び教育情報システム管理者は、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。

② 教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与された ID 及びパスワードの変更について、外部委託事業者に行わせてはならない。

7．教育情報セキュリティポリシーの遵守状況の確認・管理

（1）遵守状況の確認及び対処

① 教育情報セキュリティ責任者及び教育情報セキュリティ管理者は、教育情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに統括教育情報セキュリティ責任者に報告しなければならない。

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

（2）パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

① 統括教育情報セキュリティ責任者及び統括教育情報セキュリティ責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、教職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（3）業務以外の目的でのウェブ閲覧の禁止

① 教職員等は、業務以外の目的でウェブを閲覧してはならない。

② 統括教育情報セキュリティ責任者は、教職員等のウェブ利用について、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、教育情報セキュリティ管理者に通知し適切な措置を求めなければならない。

（4）教職員等の報告義務

① 教職員等は、教育情報セキュリティポリシーに対する違反行為を発見した場合、直ちに統括教育情報セキュリティ責任者及び教育情報セキュリティ管理者に報告を行わなければならない。

8．侵害時の対応等

（1）緊急時対応計画の策定

① 教育情報セキュリティ責任者は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ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、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

② 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。

㋐ 関係者の連絡先

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

（２）緊急時対応計画の見直し

① 教育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規定を見直さなければならない。

９．例外措置

（１）例外措置の許可

① 教育情報セキュリティ責任者は、情報セキュリティ関係規定を遵守することが困難な状況で、学校事務及び教育活動の適正な遂行を継続するため、遵守事項とは異なる方法を採用し又は遵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、統括教育情報セキュリティ責任者の許可を得て、例外措置を取ることができる。

（２）緊急時の例外措置

① 教育情報セキュリティ責任者は、学校事務及び教育活動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、事後速やかに統括教育情報セキュリティ責任者に報告しなければならない。

（３）例外措置の申請書の管理

① 統括教育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を適切に保管し、定期的に申請状況を確認しなければならない。

第８章　外部委託

１．外部委託

（１）外部委託事業者の選定基準

① 教育情報システム管理者は、外部委託事業者の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

② 第三者機関の認証を受けているなど、適切なセキュリティ対策が施されていることが確認できる事業者（サービス）を利用するよう努めなければならない。

（２）確認・措置等

① 教育情報システム管理者は、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定期的に確認し、必要に応じ是正措置しなければならない。また、その内容を統括教育情報セキュリティ責任者に報告しなければならない。

（３）システム管理記録及び作業の確認

① 教育情報システム管理者は、所管する教育情報システムの運用においてバックアップ等実施した作業について、作業記録を作成しなければならない。

② 教育情報セキュリティ責任者及び教育情報システム管理者は、所管するシステムにお

いて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

③ 教育情報セキュリティ責任者、教育情報システム管理者又は教育情報システム担当者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、２名以上で作業をするなど、複数でその作業内容を確認しなければならない。

第９章　クラウドサービスの利用

１．サービス利用

（１）利用の可否判断における留意点

① 教育情報セキュリティ責任者は、SaaS 型パブリッククラウドサービスなど、利用者の個別要望に沿ったカスタマイズは原則困難であり利用者の要望を反映した個別契約に基づく調達として扱うことは原則難しい特性を持つサービスを利用する際は、以下の観点によりサービスの安全性および事業者のサービス提供ポリシーや体制等を確認しなければならない。

２．利用における情報セキュリティ対策

（１）利用者認証

① クラウド利用者がクラウド事業者における当該クラウドサービスを提供する情報システムの運用もしくは開発に従事する者又は管理者権限を有する者について、適切な利用者確認がなされていることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

② クラウド利用者が当該クラウドサービスのログインに関わる認証機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

③ クラウド利用者側管理者権限を有する者の ID の管理について、第７章「６．特権を付与された ID の管理等」を遵守していること。

（２）アクセス制御

① クラウド利用者が当該クラウドサービスに対して、アクセスする権限のない者がアクセスできないように、システム上制限する機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

② クラウド利用者が、クラウド事業者の提供するアクセス制御機能を用いて、情報資産毎に、許可されたクラウドを利用する教職員等及び児童生徒のみがアクセスできる環境を設定していること。

（３）クラウドに保管するデータの暗号化

① クラウド利用者が当該クラウドサービスへのデータの保管に際し、情報漏えい等に備えて、暗号化等の保護措置を講じられていることを、クラウド事業者にサービス提供定款や契約書面上で確認または合意していること。

（4）マルチテナント環境におけるテナント間の安全な管理

① クラウド利用者が、複数のクラウド利用者がクラウドリソースを共用する環境において、特定のクラウド利用者に対して発生したセキュリティ侵害が、他のクラウド利用者に影響を与えないように対策が講じられていることを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

（5）クラウドサービスを提供する情報システムに対する外部からの悪意のある脅威の侵入を想定した技術的セキュリティ対策

① クラウド利用者が当該クラウドサービスを提供する情報システムを監視し、セキュリティ侵害を検知することを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

② クラウド利用者が当該クラウドサービスを提供する情報システムのインターネット接続境界において、クラウド利用者以外による不正な通信・侵入を防ぐ措置を講じるとともに、外部脅威の侵入を検知し、防御する対策を講ずることを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

（6）情報の通信経路のセキュリティ確保

① クラウド利用者が教育情報システムのインターネット境界から当該クラウドサービスを提供する情報システムまでの情報の通信経路において、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準･手順等の整備、通信の暗号化等）をクラウド事業者に求め、合意のうえ、利用していること。

② クラウド利用者が、クラウド事業者が保守運用等を遠隔で行う場合の保守運用拠点と管理区域間での通信回線及び通信回線装置の管理について、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準･手順等の整備、通信の暗号化等）をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

（7）クラウドサービスを提供する情報システムの物理的セキュリティ対策

① クラウド利用者が当該クラウドサービスのサーバ等の管理条件を第４章「１．サーバ等の管理」に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

② クラウド利用者がクラウド事業者側の管理区域（サーバ等を設置）及び保守運用拠点の管理において、第４章「２．管理区域（情報システム室等）の管理」に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

③ クラウド利用者がクラウドサービス事業者が利用する資源（装置等）の処分（廃棄）にあたり、セキュリティを確保した対応となっているかをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。なお、当該確認に当たっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

（8）クラウドサービスを提供する情報システムの運用管理

① クラウド利用者がクラウド事業者に対して、サービスの一時停止等クラウド利用者に影響があり得る運用手順の有無、有る場合にはクラウド利用者への影響範囲（時間、サービス内容、連絡方法等）について情報提供を求め、クラウド利用者が業務運営に支障がないことを確認し、合意していること。

② クラウド利用者が当該クラウドサービスにおけるデータバックアップ及び復旧手順について、第６章「１．コンピュータ及びネットワークの設定管理（２）バックアップの実施」に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること

③ クラウド利用者が当該クラウドサービスにおける情報セキュリティの確保や監査に必要なログの取得について、第６章「１．コンピュータ及びネットワークの設定管理（３）ログの取得等」に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

（9）クラウドサービスを提供する情報システムのマルウェア対策

① クラウド利用者がクラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等について、マルウェア対策を講じることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

② クラウド利用者が内部システムに侵入した攻撃を検知して対処するために、通信をチェックする等の対策を講じることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

(10) クラウド利用者側のセキュリティ確保

① クラウド利用者がクラウドサービスにアクセスするクラウドを利用する教職員等及び児童生徒側端末について、保管するデータの外部流出、改ざん等から保護するために必要な措置を講じていること。

② クラウド利用者が標的型攻撃による外部からの脅威の侵入を防止するために、クラウドを利用する教職員等及び児童生徒への教育や入口対策を講じていること。

(11) クラウド事業者従業員の人的セキュリティ対策

① クラウド利用者がクラウドサービスに関わるクラウド事業者従業員に対して、クラウド事業者の情報セキュリティポリシー及び保守運用管理規程等を遵守することをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

② クラウド利用者がクラウドサービスに関わるクラウド事業者従業員に対して、業務に用いる ID 及びパスワードその他の個人認証に必要な情報及び媒体について、部外者及び業務に関わらない従業員に漏えいすることがないように、適切に管理することをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

③ クラウド利用者がクラウドサービスに関わらない従業員等がクラウド利用者のデータを知り得る状態にならないよう、業務に関わるクラウド事業者従業員に対して秘匿を義務づけることをクラウド事業者に求め、サービス提供定款や契約書面上で確認ま

たは合意していること。

④ クラウド利用者がクラウド利用者のデータ及びデータを格納した端末機器又は電磁的記録媒体の外部持ち出しについて、クラウド利用者の許可なく外部持ち出しできないこと及び外部持ち出しにおける安全管理手順をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

⑤ クラウド利用者がクラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等に、マルウェアを侵入させないよう、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意していること。

(12) サービス終了時等のデータの廃棄及び利用者アカウント抹消

① クラウド利用者がサービス利用終了時等において、クラウド利用者のデータ及び利用者アカウント情報が不用意に残置されないよう、適切に破棄するための流れについてサービス提供定款や契約書面上で確認または合意していること。

② クラウド利用者がサービス利用終了時等におけるデータの扱いについて、スムーズに回収、次期システムへの移行等を行えるよう、その措置の流れについてサービス提供定款や契約書面上で確認または合意していること。

③ クラウド利用者がクラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理していること。

3．事業者のサービス提供に係るポリシー等に関する事項

（1）守秘義務、目的外利用及び第三者への提供の禁止

① クラウド利用者がクラウドサービス事業者がコンテンツにアクセスできるかどうかを確認し、サービスに係る情報及び受託した情報に関する守秘義務、目的外利用及び第三者への提供の禁止条項について、サービス提供に係る契約に含めていること。

（2）準拠する法令、情報セキュリティポリシー等の確認

① クラウド利用者がクラウド事業者がどのような規範に基づいてサービス提供するか開示を求め、クラウド利用者の準拠する法令、情報セキュリティポリシーを確認し、それらとの整合を確認していること。

（3）クラウド事業者の管理体制

① クラウド利用者がクラウド事業者に対して、情報セキュリティポリシー等の遵守を担保する管理体制が整備されているか、クラウド事業者の組織体制を確認し、合意していること。

（4）クラウド事業者従業員への教育

① クラウド利用者がクラウド事業者に、従業員に対して個人情報保護等の関係法令、守秘義務等、業務遂行に必要な知識、意識向上のための適切な教育及び訓練を実施し、充分な知識とセキュリティ意識を醸成することを求めていること。

② クラウド利用者がクラウド事業者に、従業員への上記育成計画、教育実績等の情報を提示させ、自らデータを管理する場合と同様の教育・訓練を実施しているかを確認し

ていること。

（5）情報セキュリティに関する役割の範囲、責任分界点

① クラウド利用者がクラウド事業者の情報セキュリティに関する役割の範囲と責任分界点について開示するよう求めていること。

② クラウド利用者がクラウド事業者の情報セキュリティに関する役割の範囲と責任分界点がクラウド利用者側で講ずる情報セキュリティ対策の役割の範囲と整合することを確認し、合意していること。

（6）監査

① クラウド利用者がクラウドサービスの監査状況、範囲・条件、内容等についてクラウド事業者に開示するよう求めていること。

② クラウド利用者がクラウド事業者によるクラウドサービスに関する監査レポート等を根拠にして、自らの関係法令、情報セキュリティポリシーと照らし合わせ、安全性が確保されているかについて確認していること。

（7）情報インシデント管理及び対応フローの合意

① クラウド利用者が情報セキュリティインシデント管理に関する責任範囲と及びインシデント対応フローを、サービス仕様の一部として定めることについて、クラウド事業者に対して求めていること。

（8）クラウドサービスの提供水準及び品質保証

① クラウド利用者は、クラウドサービスの提供水準（サービス内容、提供範囲等）と品質保証（サービス稼働率、故障等の復旧時間等）を確認するとともに、それらの水準・品質が、業務遂行に求められる要求水準を満たすことを確認し、合意していること。

（9）その他留意事項

① クラウド利用者がクラウド事業者がサービスを安定して提供可能な企業・団体であるかについて考慮していること。

② クラウド利用者がクラウド事業者を変更する際のデータ移行の方法などについて、クラウド事業者にサービス提供定款や契約書面上で確認または合意していること。

③ クラウド利用者がクラウド事業者に対して、クラウドサービスにおいて扱う情報資産や情報システム等について、日本の法令が適用されること及び係争等における管轄裁判所が日本国内であることを確認していること。

④ クラウド利用者がクラウド事業者において個人情報の適切な管理が行われているか確認するとともに、確認した項目については、調達時においてサービスの過剰な排除にならないよう留意した上で、契約要件等として定めていること。

4．サービス利用における教職員等の留意点

（1）ID及びパスワード等の秘匿

① 教職員等は、ID及びパスワードについて秘匿管理を行わなければならない。

② 教職員等は、多要素認証に必要な要素（知識、生体、物理）についても適切に管理を行わなければならない。もし該当要素が流出等したと考えられる場合には、速やかに

教育情報セキュリティ管理者に報告しなければならない。

（2）重要性分類に基づく情報管理

① パブリッククラウド上で重要な情報（重要性分類Ⅱ以上）を取り扱う際には、多要素認証を含む強固なアクセス制御による対策を講じるよう努めなければならない。ただし、児童生徒またはその保護者が重要性分類Ⅱ以上の情報資産にアクセスする場合は、児童生徒本人またはその保護者が、当該児童生徒に関するもののみにアクセスすることを想定していることから、多要素認証を設定することが望ましいものの、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際のロック機能の有効化、パスワードの複雑性の確保等により本人確認を厳格に行う前提で、ID 及びパスワードでの認証を許容する。

（3）学校外からのパブリッククラウド利用

① 教職員等は、学校外からクラウドサービスを利用する際、情報資産の取扱いをクラウドサービス上のみで行わなければならない。

5．ソーシャルメディアサービスの利用

（1）ソーシャルメディアサービスの利用に関する留意点

① 教育情報システム管理者は、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以下のとおりとする。

㋐ 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。

㋑ 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（IC カード等）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。

② 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。

③ 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。

第 10 章 評価・見直し

1．監査

（1）実施方法

① 統括教育情報セキュリティ責任者は、教育情報セキュリティ監査者を指名し、教育情報ネットワーク及びシステム等の情報資産における情報セキュリティ対策状況について、必要に応じて監査を行わせなければならない。

（2）監査を行う者の要件

① 教育情報セキュリティ監査者は、監査及び情報セキュリティに関する専門知識を有す

る者でなければならない。

（3）監査実施計画の立案及び実施への協力

① 教育情報セキュリティ監査者は、監査を行うに当たって、監査実施計画を立案しなければならない。

② 監査対象となる情報資産を所管する教職員その他の関係者は、監査の実施に協力しなければならない。

（4）委託事業者に対する監査

① 情報セキュリティ監査者は、監査対象となる情報資産に関して外部委託が行われている場合、委託事業者（再委託事業者を含む。）に対して、情報セキュリティポリシーの遵守について監査を必要に応じて行わなければならない。

（5）報告

① 情報セキュリティ監査者は、監査実施後は結果を取りまとめ、統括教育情報セキュリティ責任者に報告するものとする。

（6）保管

① 統括教育情報セキュリティ責任者は、教育情報セキュリティ責任者又は教育情報システム管理者に対して、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管させなければならない。

（7）監査結果への対応

① 統括教育情報セキュリティ責任者は、監査結果を踏まえ、指摘事項を所管する教育情報セキュリティ管理者又は教育情報システム管理者に対し、当該事項への対処をさせなければならない。また、指摘事項を所管していない教育情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

（8）情報セキュリティポリシー及び関係規程等の見直し等への活用

① 監査結果については、情報セキュリティポリシー等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

2．自己点検

（1）実施方法

① 教育情報システム管理者は、所管するネットワーク及び情報システムについて、必要に応じて自己点検を実施し、教育情報セキュリティ責任者に報告しなければならない。

② 教育情報セキュリティ管理者は、所管する学校等における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、必要に応じて自己点検を行い、教育情報セキュリティ責任者に報告しなければならない。

（2）報告

① 教育情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、統括教育情報セキュリティ責任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、自己の権限の範囲内で改善を図らなければならない。
② この点検結果を情報セキュリティポリシー等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

3．教育情報セキュリティポリシー及び関係規程等の見直し

（1）情報セキュリティポリシー等の維持及び運用

① 統括教育情報セキュリティ責任者は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー等に新たに必要な対策が発生した場合には改善を行い、情報セキュリティポリシー等の維持及び運用に努めなければならない。

改訂履歴

版数	発行日	改訂履歴
第１版	令和７年２月	初版発行
第２版	令和８年２月	文部科学省「教育情報セキュリティポリシーに関するガイドライン」の令和７年３月改訂に伴った改訂