松伏町教育情報セキュリティポリシー

令和５年３月策定
令和７年８月改訂

松伏町教育委員会
教育総務課

目次

第１章　松伏町教育情報セキュリティポリシーの目的及び構成

１　目的

松伏町立小・中学校（以下「学校」という。）が取り扱う情報には、児童、生徒及び保護者の個人情報のみならず、学校運営上重要な情報など、外部に流出した場合に極めて重大な結果を招く情報が多数含まれている。したがって、これらの情報及び情報を取り扱う教育情報システムの情報を様々な脅威から防御することは、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。また、学習指導要領にも、情報活用能力育成やプログラミング教育等、より一層の教育の情報化が求められており、学校がこれに積極的に対応するためには、教育情報システムが高度な安全性を有することが不可欠な前提条件となる。そのため、学校の情報資産の機密性、完全性及び可用性を維持するための対策（情報セキュリティ対策）を整備するために、松伏町教育情報セキュリティポリシー（以下「教育情報セキュリティポリシー」という。）を定めることとする。

２　構成

教育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関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。

教育情報セキュリティポリシーは、学校が保有する情報資産を取り扱うすべての教職員に浸透、普及及び定着させるものであり、安定的な規範であることが要請される。しかし一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化に対し柔軟に対応することも必要である。

このようなことから、教育情報セキュリティポリシーは、一定の普遍性を備えた部分としての「教育情報セキュリティポリシー基本方針」と、情報資産を取り巻く状況の変化に対応する部分としての「教育情報セキュリティポリシー対策基準」から構成する。

【教育情報セキュリティポリシーの構成】

文書名	内容	
教育情報セキュリティポリシー	教育情報セキュリティポリシー基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	教育情報セキュリティポリシー対策基準	教育情報セキュリティポリシー基本方針を実行に移すためのすべての教育情報システムに共通の教育情報セキュリティ対策の基準

第２章　教育情報セキュリティポリシー基本方針

１　目的

この基本方針は、松伏町教育委員会（以下「教育委員会」という。）及び学校が管理する情報資産の機密性、完全性及び可用性を確保するため、様々な脅威に対する抑止、予防、検知及び回復について、組織的かつ体系的に取り組むための統一的な方針並びに情報セキュリティ対策を実施するに当たっての基本的な考え方及び方策を定めることを目的とする。

２　定義

教育情報セキュリティポリシーにおいて、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

（１）情報資産

教育情報システムの開発と運用に係るすべてのデータ及び教育情報システムで取り扱うすべてのデータをいう。

（２）教育情報システム

ネットワーク、ハードウェア、ソフトウェア、アプリケーション及び記録媒体で構成され、処理を行う仕組みをいう。

（３）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。

（４）機密性

情報に接続することを認められた者だけが、情報に接続できる状態を確保することをいう。

（５）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。

（６）可用性

情報に接続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、情報に接続できる状態を確保することをいう。

３　対象範囲

教育情報セキュリティポリシーが適用される行政機関等は、教育委員会及び学校とする。

４　情報セキュリティ管理体制

情報セキュリティ対策を推進、管理するための体制及び役割を定めるものとする。

５　情報資産の分類及び管理

情報資産は、その重要性に応じて分類し、適正な管理を行うこととする。

６　情報セキュリティ対策

情報セキュリティを確保するため、次の各号に掲げる情報セキュリティ対策を講ずるものとす

る。

（１）物理的セキュリティ対策

教育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、妨害等から保護するために講ずる物理的な対策をいう。

（２）人的セキュリティ対策

教育情報セキュリティに関する教職員の責務を定め、教職員等に情報セキュリティ対策を周知徹底する等、十分な教育及び啓発を行うために講じる人的な対策をいう。

（３）技術的セキュリティ対策

情報資産を外部からの不正な接続等から適切に保護するために講じる、情報資産への接続制御、ネットワーク管理等の技術的な対策をいう。

（４）障害時におけるセキュリティ対策

情報セキュリティに係る障害が発生した場合に迅速な対応を可能とするために講じる緊急時の対策をいう。

７　教育情報セキュリティポリシー対策基準

教育情報セキュリティポリシー基本方針を実行に移すためのすべての教育情報システムに共通の情報セキュリティ対策の基準、「教育情報セキュリティポリシー対策基準」を定めるものとする。

８　教育情報セキュリティポリシー関係規程

教育情報セキュリティポリシー対策基準を遵守して、情報セキュリティ対策を実施するに当たり、その具体的な手順等を明らかにするため、教育委員会及び学校で関連規程を定めるものとする。

なお、この規程の中で、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のある情報については、非公開とする。

９　法令等の遵守

教職員は、取り扱う情報資産及び教育情報システムについて、関係法令等に従うものとする。

１０　点検及び監査

教育情報セキュリティポリシーの遵守状況について、必要に応じて点検及び監査を実施する。

１１　評価及び見直しの実施

点検又は監査の結果に基づき、情報セキュリティ対策の評価を行うとともに、情報セキュリティを取り巻く状況の変化に対応するために、適宜、教育情報セキュリティポリシーの見直しを実施する。

第３章　教育情報セキュリティポリシー対策基準

１　趣旨

この教育情報セキュリティポリシー対策基準は、教育情報セキュリティポリシー基本方針において規定する情報セキュリティ対策を実行に移すための、情報セキュリティ対策の基準を定めるものとする。

２　組織体制

教育情報セキュリティ管理体制については、以下のとおりとする。

（１）最高情報統括責任者（CIO: Chief Information Officer、以下「CIO」という。）

①教育長を、CIO とする。

②CIO は、情報資産、教育情報システム及び情報セキュリティに関する最終決定権限及び責任を有する。

（２）情報システム管理者

①教育総務課長を、情報システム管理者とする。

②情報システム管理者は、CIO を補佐し、情報資産、教育情報システム及び情報セキュリティに関する権限や責任を有し、CIO が不在の場合は、その職務を代行する。

③情報システム管理者は、情報セキュリティインシデント発生時には CIO 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。

④情報システム管理者は、情報セキュリティ管理者及び情報システム部門に対して、情報資産、教育情報システム及び情報セキュリティに関する指導及び助言を行う。

⑤情報システム管理者は、教育情報セキュリティポリシーに対する意見の集約、教職員等の教育、訓練及び助言を行う。

（３）情報システム部門

①情報システム部門は、教育総務課とする。

②情報システム部門は、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。

（４）情報セキュリティ管理者

①校長を、その所管する学校の情報セキュリティ管理者とする。

②情報セキュリティ管理者は、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情報セキュリティ管理者は、情報セキュリティインシデント発生時には情報システム管理者に速やかに報告を行い、指示を仰がなければならない。

④情報セキュリティ管理者は、教職員の中から情報担当者を任命し、教育情報システムの導入、管理及び運用等を補佐させることができる。また、必要に応じて ICT 支援員等の外部人材に支援を求めることができる。

（５）兼務の禁止

情報セキュリティ対策の実施において、自ら承認すると規定されている場合及びやむを得ない場合を除き、承認を申請する者と承認者は、同じ者が兼務してはならない。

3　対象範囲及び用語説明

（1）行政機関の範囲

本対策基準が適用される行政機関等は、教育委員会及び学校とする。

（2）情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりである。

①教育情報システム、これらに関する設備、電磁的記録媒体

②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

（3）用語説明

用語	定義
校務系情報	学校が保有する情報資産のうち、それら情報を学校及び学級の管理運営、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接続することが想定されていない情報。
公開系情報	校務系情報のうち、保護者メールや学校ホームページ等の、外部と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。
学習系情報	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接続することが想定されている情報。
校務用端末	校務系情報に接続可能な端末。
学習者用端末	学習系情報に接続可能な端末で、児童生徒が利用する端末。
指導者用端末	学習系情報に接続可能な端末で、教職員が利用する端末。
校務系システム	校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム。
公開系システム	公開系ネットワーク及び公開系サーバから構成される公開系情報を取り扱うシステム。
学習系システム	学習系ネットワーク、持込系ネットワーク、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム。
教育情報システム	校務系システム、公開系システム及び学習系システムを合わせた総称。
サーバ	教育情報システムのサーバ。
教職員	教育委員会所管の学校に勤務する又は学校事務に従事する教職員等。
端末	パソコンやモバイル端末（タブレット等）機器。
情報セキュリティインシデント	情報セキュリティに関する問題として捉えられる事象（障害、事件、事故、欠陥、攻撃、侵害等）。

標的型攻撃	明確な意思と目的を持った人間が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。
役場庁舎電算室	松伏町情報システム部門が管理する電算室。
特定個人情報	個人番号（マイナンバー）を内容に含む個人情報。

4　情報資産の分類と管理

（1）情報資産の分類

学校の情報資産の機密性、完全性及び可用性の３つの観点から影響度を評価し、別表のとおり重要性分類を行い、必要に応じて取扱制限を行う。

（2）情報資産の管理

①管理責任

（ア）情報セキュリティ管理者は、その所管する学校の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。

（ウ）教職員は、情報資産について、その分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

②利用責任

情報資産を利用する者は、情報資産の分類に従い利用する責任を負う。

③情報の作成

（ア）教職員は、業務上必要のない情報を作成してはならない。

（イ）情報を作成する者は、情報の作成時に（1）の分類に基づき、当該情報の分類と取り扱い制限を定めなければならない。

（ウ）情報を作成する者は、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、情報の作成途中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。

（エ）教職員が業務上作成した情報の著作権は、全て教育委員会に帰属する。

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、当該情報の分類と取扱い制限を定めなければならない。

（ウ）情報資産を入手した場合は、その情報資産の分類が不明な場合、情報システム管理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、業務以外の目的に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た取扱いをしなければならない。

（ウ）情報資産を利用する者は、情報資産の分類が異なる情報が同一の記録媒体に複数記録されている場合、最高度の分類に従って、当該記録媒体を取り扱わなければならない。

（エ）情報資産を利用する者は、必要以上の複製及び配布をしてはならない。

⑥情報資産の保管

（ア）情報セキュリティ管理者は、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）情報セキュリティ管理者は、情報資産を記録した持ち出しのできる電磁的記録媒体を保管する場合は、書き込み禁止の措置を講じる等の情報保護対策をして保管しなければならない。

（ウ）情報セキュリティ管理者は、重要性３以上の情報を記録した持ち出し可能な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。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）情報セキュリティ管理者は、情報資産を記録した持ち出し可能な電磁的記録媒体等の授受について台帳を整備し、次の事項を記録しておくこと。

・情報資産等の名称
・搬入者及び受領者の氏名並びに所属等の名称
・承認日
・授受年月日
・その他情報セキュリティ管理者が必要と認める事項

⑦情報の送信

電子メール、外部ストレージサービス等により重要性３以上の情報を外部送信する者は、必要に応じ暗号化の設定をしなければならない。なお、利用する電子メール、外部ストレージサービス等は教育委員会又は学校が管理する ID でのみ使用することができる。

⑧情報資産の運搬

（ア）やむを得ず、車両等により重要性３以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化の設定を行う等、情報資産等の不正利用を防止するための措置を講じなければならない。

（イ）重要性３以上の情報資産を運搬する者は、情報セキュリティ管理者に承認を得なければならない。

⑨情報資産の提供及び公表

（ア）重要性３以上の情報資産を外部に提供する者は、必要に応じ暗号化の設定を行わなければならない。

（イ）重要性３以上の情報資産を外部に提供する者は、情報セキュリティ管理者に承認を得なければならない。

（ウ）管理者及び情報セキュリティ管理者は、住民に公開する情報資産について、誤公開を防ぎ、かつ完全性の確保のため、定期的な確認を行わなければならない。

⑩情報資産の廃棄

（ア）重要性３以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化、破壊等、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、情報システム管理者及び情報セキュリティ管理者に承認を得なければならない。

5　特定個人情報の取扱い

特定個人情報を取り扱う場合は、校務系システム内で取り扱うものとし、ファイルやデータの暗号化の設定等、流出を防ぐための措置を講じなければならない。

6　物理的セキュリティ

（1）サーバ等の管理

①装置の取付け等

（ア）サーバ等を取り付ける場合は、火災、水害、埃（ほこり）、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な固定等必要な措置を施さなければならない。

（イ）情報システム管理者及び情報セキュリティ管理者により操作を認められた者以外の者が容易に操作できないよう、パスワードの設定等の措置を施さなければならない。

（ウ）無線 LAN の導入は、経路の暗号化等、十分な流出防止策を講じなければ実施してはならない。

②電源

（ア）サーバ等の電源については、当該機器を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）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施さなければならない。

③配線

（ア）配線は傍受又は損傷を受けることがないよう、可能な限り必要な措置を施さなければならない。

（イ）主要な箇所の配線については、損傷等についての定期的な点検を行わなければならない。

（ウ）情報システム管理者及び情報セキュリティ管理者から認められた者以外の者が配線を変更、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）情報システム管理者は、サーバ等の機器の定期保守を実施しなければならない。

（イ）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、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し、秘密保持体制や運用等が適切であることを確認しなければならない。

⑤施設外又は学校外への機器の設置

（ア）情報システム管理者は、施設外又は学校外にサーバ等の機器を設置する場合、CIOの承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（イ）情報システム管理者は、外部の事業者のデータセンタに機器を設置している場合には、定期的にセキュリティ対策状況を確認するか、第三者による監査報告書等によって確認しなければならない。

⑥機器の廃棄等

機器を廃棄する場合やリース返却等をする場合、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。ただし、守秘義務契約を締結している事業者の場合は、この限りではない。

（２）教育情報システムにおける措置

①ネットワーク構築上の措置

（ア）教育情報システムについては、安全対策に万全な措置を講じなければならない。

（イ）教育情報システムは、校務を取り扱う校務系、児童生徒が利用する学習系及び必要に応じ個人所有の端末を接続する持込系に切り分けて構築しなければならない。

（ウ）学校事務職員が利用する業務系ネットワークは、松伏町情報ネットワークであり、松伏町の情報システム部門により管理され、教育情報システムと接続してはならない。

（エ）業務上必要があり無線通信とする場合は、次の事項を遵守すること。

・情報セキュリティ管理者は利用者の端末を管理すること。

・経路の暗号化及び端末等の接続制御を行うこと。暗号化の方式は、WPA2以降の方式を使用しなければならない。

（オ）情報システム管理者は、教育情報システムの構築にあたっては、インターネットを通信経路とする前提で、内部及び外部両面からの不正なアクセスから防御するため、多要素認証による利用者認証、端末認証、通信の監視、制御等を組み合わせたセキュリティ対策の構築に努めなければならない。

②ネットワーク機器等

（ア）基幹機器（サーバ等）について

・教育情報システムの基幹機器（サーバ等）については、役場庁舎電算室、学校内又は情報システム管理者の指定する事業者のデータセンタ内に設置しなければならない。また、ネットワークの運用上重要な機能を有する機器については、障害発生時にネットワークの運用が停止しないように冗長化を図る等必要な措置を講じなければならない。

・主要なネットワーク機器（スイッチ、ルータ等）及び配線については、情報システム管理者以外の者が容易に操作できないような場所に格納する等の措置を講じなければならない。

・ネットワーク機器等の構成管理を適切に行わなければならない。

・主要なネットワーク機器については、落雷等による異常電波及び停電等の電気的障害

に対し必要な防護措置を講じなければならない。

（イ）ネットワーク機器の設置

ネットワーク機器は、情報システム管理者が指定した場所に設置する。業務上必要があり設置した場所を移動する場合は、情報システム管理者の承認を得なければならない。また、業務上の必要があり新設及び増設を行う場合には、ネットワーク機器使用承認及び接続申請及び設定作業依頼書（様式第１号）により情報システム管理者の承認を得なければならない。情報システム管理者は、承認したネットワーク機器が学習系システムに利用されるものであったときは、承認日、設置場所、機器の型番及び設定に必要な ID 等を記録した台帳を整備し、また承認した事実を示すラベルシールを作成し、機器の見える位置に貼付しておかなければならない。

（ウ）学校外における学習系ネットワークの整備

情報システム管理者は、学習系システムを利用するためネットワーク機器を自ら承認して学校外に整備することができるが、承認した機器の取扱いは（イ）の規定を適用する。

③通信回線

（ア）学校と役場庁舎電算室を結ぶ通信回線については、専用回線又は高いセキュリティ機能を有する回線により構成し、外部からの情報の盗聴及び情報の流出等を防止しなければならない。インターネット回線を利用した VPN（Virtual Private Network）は、これを利用してはならない。

（イ）情報システム管理者は、重要性３以上の情報資産を取り扱う教育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。

（ウ）情報システム管理者は、学校運営上必要なネットワーク帯域を確保するとともに、遅延等に対する適切な対策を講じなければならない。また、運用開始前には十分検証し、利用状況に応じて定期的に改修計画を行わなければならない。

（３）教職員の利用する端末や電磁的記録媒体等の管理

①校務用端末及び指導者用端末について

（ア）情報セキュリティ管理者は、盗難防止の為、職員室等で利用する校務用端末のワイヤー等による固定、教室等で利用する指導者用端末の保管庫による管理等、利用する目的に応じた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。

（イ）情報システム管理者は、教育情報システムへのパスワードの入力その他認証を必要とするように設定しなければならない。

（ウ）情報セキュリティ管理者は、端末等におけるデータ暗号化機能等を有効に利用しなければならない。また、端末に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。同様に、電磁的記録媒体についてもデータ暗号化機能を備え、かつパスワードの入力その他認証を必要とする媒体を利用しなければならない。

（エ）情報システム管理者は、パブリッククラウド上において重要性３以上の情報を取り扱う際には、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。

（オ）情報システム管理者は、マルウェア感染の脅威に対し、ウィルス対策ソフトの導入や、異常及び不審な挙動を検知する仕組み（ふるまい検知）等の活用に努めなければならない。

（カ）情報システム管理者は、校務用端末及び指導者用端末において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。

（キ）情報システム管理者は、端末の学校外での利用の際は、上記対策に加え、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。

②学習者用端末について

（ア）情報セキュリティ管理者は、盗難防止の為、学校内で保管する場合は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。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。

（イ）情報システム管理者は、端末の教育情報システムへのパスワードの入力その他認証を必要とするように設定しなければならない。

（ウ）情報システム管理者は、マルウェア感染の脅威に対し、ウィルス対策ソフトの導入や、異常及び不審な挙動を検知する仕組み（ふるまい検知）等の活用に努めなければならない。

（エ）情報システム管理者は、学習者用端末において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。

（オ）情報システム管理者は、端末の学校外での利用の際は、上記対策に加え、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。

（カ）情報システム管理者は、児童生徒への端末配布後においても、端末のセキュリティ設定や 0S アップデート、ウェブブラウザのアップデート、学習者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、システムの設計及び構築に努めなければならない。

③保管庫について

（ア）情報セキュリティ管理者は、指導者用端末及び学習者用端末の保管庫について、情報システム管理者の指定する場所に固着し、移設してはならない。ただし、業務上必要があり保管庫移設承認申請書（様式第２号）により情報システム管理者の承認を得た場合には、この限りでない。

（イ）情報システム管理者は、指導者用端末及び学習者用端末の保管庫について、適切に管理されているか、定期的に確認しなければならない。

7　人的セキュリティ

（１）教職員における情報セキュリティの徹底

①教育情報セキュリティポリシーの遵守

教職員は、教育情報セキュリティポリシー及び関係規程を遵守しなければならない。また、

情報セキュリティ対策に対し不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

②ID 及びパスワードの管理

教職員は、ログインにかかる情報を適切に管理し、次の事項を遵守しなければならない。

（ア）ID 及びパスワードは他者に知られないよう管理しなければならない。

（イ）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すること。

（ウ）仮のパスワードは、最初のログイン時に変更すること。

（エ）必要でない限り、システム間及び教職員間でのパスワードの共有は行わないこと。

（オ）パスワードが流出した可能性がある場合は、速やかに情報セキュリティ管理者に報告し、指示を仰がねばならない。

（カ）利用する情報資産の重要度に応じて、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するよう努めなければならない。

③業務以外の情報資産の持ち出し等の禁止

教職員は、業務以外の目的で情報資産の外部への持ち出し、教育情報システムへの接続、電子メールアドレスの利用及びインターネットへの接続を行ってはならない。

④教育情報システムに接続できる端末

教育情報システムに接続できる端末は、以下のとおりである。

（ア）教育委員会が支給した端末

（イ）学校が購入し、情報システム管理者が学校用端末として承認した端末

（ウ）情報セキュリティ管理者が承認した個人所有の端末

⑤④における教育委員会が支給する端末の利用について

教職員は、教育委員会が支給する端末の利用について次の事項を遵守しなければならない。

（ア）教育委員会から支給された ID でのみログインを行うこと。

（イ）情報セキュリティ管理者は、利用しているソフトウェア及びアプリケーションを把握しておかなければならない。また、業務上必要がありソフトウェア及びアプリケーションを追加する場合には、ソフトウェア及びアプリケーション使用承認申請書（様式第３号）により情報システム管理者の承認を得なければならない。情報システム管理者は、承認したソフトウェア及びアプリケーションについて、承認に至る審査の過程を記録しておかなければならない。

⑥外部クラウドの利用

（ア）強固なアクセス制御による対策を講じたシステム構成でない場合、重要性３以上の情報資産を、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ってはならない。

（イ）付与された専用 ID 以外の外部クラウドサービスは利用することができない。

（ウ）情報セキュリティ管理者は、クラウド内の情報資産の利用方法等が、教育情報セキュリティポリシーに遵守しているか定期的に確認をしなければならない。

（エ）教職員の異動があった場合は、情報システム管理者は速やかに ID の追加、編集、削除等の対応を行わなければならない。

⑦端末におけるセキュリティ設定変更の禁止

教職員は、端末のソフトウェア及びアプリケーションに関するセキュリティ機能の設定を情報セキュリティ管理者の承認なく変更してはならない。

⑧端末や電磁的記録媒体等の情報の持ち出し及び外部における情報処理作業の制限

（ア）情報セキュリティ管理者は、端末や電磁的記録媒体等の持ち出し及び持込みについて、記録を作成し、保管しなければならない。

（イ）教職員は、端末のソフトウェア及びアプリケーションに関するセキュリティ機能の設定を、情報セキュリティ管理者の承認なく変更してはならない。

（ウ）教職員は、端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に利用されること又は情報セキュリティ管理者の承認なく情報を閲覧されることがないように、離席時の端末のロックや電磁的記録媒体、文書等が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。

（エ）教職員は、異動、退職により業務を離れる場合には、利用していた端末及び情報資産を返却しなければならない。またその後も業務上知り得た情報を漏らしてはならない。

（オ）教職員は、端末のソフトウェア及びアプリケーションのインストール及びアンインストール、若しくは機器の改造、設定変更、増設、交換を行う場合は、情報システム管理者の承認を得なければならない。

（カ）教職員は、著作権法や利用許諾契約等に違反するソフトウェア及びアプリケーションの利用又は複製を行ってはならない。

⑨④における情報セキュリティ管理者が承認した個人所有の端末の利用について

教職員は、個人所有の端末を、原則業務に利用してはならない。業務上必要があり利用する場合は、以下のことを遵守すること。

（ア）利用前に情報セキュリティ管理者の承認を得ること。

（イ）教育情報システムには、原則接続してはならない。業務上必要がある場合には、情報セキュリティ管理者の承認を得て、持込系ネットワークに接続することができる。

（ウ）重要性３以上の情報資産を取り扱ってはならない。

（エ）情報セキュリティ管理者の承認を得て利用し、業務で利用する必要がなくなった場合は、速やかに情報セキュリティ管理者に報告し利用を終了すること。

⑩退職時等の遵守事項

教職員は、異動、退職等により業務を離れる場合には、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

（２）非常勤及び臨時の教職員への対応

情報セキュリティ管理者は、非常勤及び臨時の教職員に対し、採用時に教育情報セキュリティポリシーのうち、守るべき内容を理解させ、実施及び遵守させなければならない。

（３）教育情報セキュリティポリシーの掲示

情報セキュリティ管理者は、教職員が常に教育情報セキュリティポリシーを閲覧できるように掲示しなければならない。

（４）研修及び訓練

情報セキュリティ管理者は、必要に応じて教職員を対象とする情報セキュリティに関する研修及び訓練を実施、又は受講させなければならない。

（５）情報セキュリティインシデントに対する報告

①教職員は、教育情報システムの利用に際して情報セキュリティインシデントを発見した場合、速やかに情報セキュリティ管理者に報告しなければならない。

②教職員は、情報セキュリティ管理者の指示に従い、情報セキュリティインシデントに対し適切に対処しなければならない。

③教職員は、情報セキュリティに対する事故、教育情報システムの欠陥及び誤動作を発見した場合又は外部から通報を受けた場合は、速やかに情報セキュリティ管理者に報告しなければならない。

④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、情報システム管理者及びCIOに報告しなければならない。

（６）情報セキュリティインシデント原因の究明、記録及び再発防止等

①情報システム管理者は、情報セキュリティインシデントについて、情報セキュリティ管理者及び教育情報システムの管理を委託している業者と連携し、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデント原因究明の結果から、再発防止策を検討し、CIO に報告しなければならない。

②CIOは、情報システム管理者に、再発防止策の実施を指示しなければならない。

（７）法令等の遵守

教職員は、取り扱う情報資産を保護し教育情報システムを適切に利用するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

①地方公務員法（昭和 25 年法律第 261 号）

②教育公務員特例法（昭和 24 年法律第 1 号）

③著作権法（昭和 45 年法律第 48 号）

④不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）

⑤個人情報の保護に関する法律（平成 15 年法律第 57 号）

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（平成 25 年法律第 27 号）

⑦サイバーセキュリティ基本法（平成 26 年法律第 104 号）

⑧個人情報の保護に関する法律施行条例（令和 4 年条例第 20 号）

⑨松伏町情報公開条例（平成 16 年条例第 25 号）

８　技術的セキュリティ

（１）校務系サーバ及び端末の設定等

①情報システム管理者は、教職員等が使用できる校務系サーバの容量を設定し、教職員に周知しなければならない。

②情報システム管理者は、校務系サーバを学校等の単位で構成し、教職員が他の学校等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、特定の教職員しか取扱えないデータについて、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、担当教職員以外の教職員が閲覧および使用できないようにしなければならない。

（２）外部系ネットワークとの接続にかかる措置

インターネット接続を利用し、外部の者と通信（メールやホームページ編集作業を行う場合を除く。）を行うときは、原則として重要性３以上のデータは取り扱ってはならない。

（３）ログの取得等

①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情報システム管理者は、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。

③情報セキュリティ管理者は、取得したログを定期的に点検又は分析する機能等を導入するなど、必要に応じて悪意ある第三者等からの不正な侵入又は操作の有無について把握できる体制の構築に努めなければならない。

（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ねばならない。

（５）外部の者が利用できるシステムの分離等

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、特に重要性３以上を扱うシステムとの倫理的または物理的な分離、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）ホームページを利用した情報提供の措置

原則として個人情報は取り扱ってはならない。業務上必要があるときは、個人情報の保護に関する法律施行条例に基づき適正に運用しなければならない。

（７）バックアップの実施

情報セキュリティ管理者及び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、以下のとおりバックアップを実施する。

①校務系情報及び公開系情報については、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。特に校務系情報については、１日１回以上のバックアップを実施するよう努めなければならない。

②学習系情報については、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。

（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情報システム管理者は、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は、各システムにおけるアクセス権管理の徹底を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倫理的また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）を倫理的又は物理的に分離をしなければならない。

②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（持込系、学習系、情報系、基幹系及び図書システム系等）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、ウィルス感染のない無害化通信など、適切なシステムの構築に努めなければならない。

（９）複合機のセキュリティ管理

①情報システム管理者は、複合機を調達する場合、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、適切なセキュリティ要件を策定しなければならない。

②情報システム管理者は、複合機が備える機能について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。

③情報システム管理者は、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。

（１０）コンピュータウィルス等の不正プログラム対策

①コンピュータウィルス等不正プログラム対策の実施

（ア）情報システム管理者は、インターネットから受信したファイルについてコンピュータウィルス等の不正プログラムのチェックを行うなど、ネットワークへの感染を防止しなければならない。

（イ）情報システム管理者は、コンピュータウィルス等の不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、ウィルス対策用ソフトウェアを導入しなければならない。

（ウ）情報システム管理者は、サーバ及び端末に、ウィルス対策用ソフトウェアを導入し、常駐させなければならない。導入するソフトウェアについては、異常及び不審な挙動を検知する仕組み（ふるまい検知）、エンドポイント検出応答（EDR）等の機能を有したものとするよう努めなければならない。

（エ）情報システム管理者は、端末に対して、ウィルス対策用ソフトウェアによるフルチェックを定期的に実施しなければならない。

（オ）情報システム管理者は、ウィルス対策用ソフトウェアのプログラム及びパターンファイルを常に最新のものに保たなくてはならない。

（カ）情報システム管理者は、システムがインターネットに接続していない場合、定期的にウィルス対策用ソフトウェアのプログラム及びパターンファイルの更新を実施しなければならない。また、電磁的記憶媒体を使う場合、ウィルスの感染等を防止するために、支給以外の電磁的記憶媒体を教職員に利用させてはならない。

（キ）業務で利用するソフトウェア及びアプリケーションは、開発元のサポートが終了した

ソフトウェア及びアプリケーションを利用してはならない。

②コンピュータウィルス等の不正プログラム対策の周知及び徹底

教職員は、次の事項を遵守しなければならない。

（ア）外部からデータ、ソフトウェア及びアプリケーションを取り入れる場合には、必ずコンピュータウィルス等の不正プログラムチェックを行うこと。

（イ）添付ファイルのあるメールを送受信するときは、必ず添付ファイルのコンピュータウィルス等の不正プログラムチェックを行うこと。

（ウ）差出人が不明又は不自然な添付ファイルのあるメールは直ちに削除すること。

（エ）情報システム管理者及び情報セキュリティ管理者が承認した電磁的記憶媒体以外は利用しないこと。

③コンピュータウィルス等の不正プログラム感染時の対応

（ア）情報システム管理者は、コンピュータウィルス等の不正プログラムチェックの結果、コンピュータウィルス等の不正プログラム感染を発見したときは、影響範囲及び感染経路等を調査し、駆除等必要な対策を速やかに行うこと。

（イ）情報システム管理者は、コンピュータウィルス等の不正プログラムにより情報資産に影響が生じたときは、侵害等の対応に基づき、必要な措置を講じなければならない。

（ウ）教職員は、コンピュータウィ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、以下の対応を行わなければならない。

・端末の利用を直ちに中止し、電源を切ること。

・端末にＬＡＮケーブルが接続されている場合には、抜くこと。

（１１）不正アクセス対策

①情報システム管理者の措置事項

（ア）使用されていないポート及びSSIDを閉鎖しなければならない。

（イ）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。

②攻撃の予告

CIO及び情報システム管理者は、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、関係機関に必要な通報を速やかに行うとともに、関係機関と連絡を密にして情報の収集及び対応に努めなければならない。

③サービス不能攻撃

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なければならない。

④標的型攻撃

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、自動再生無効化等の人的対策や入口対策の実施に努めるとともに、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体制の構築に努めなければならない。

（１２）システムの開発、導入、保守における措置

①システムの調達

（ア）情報システム管理者は、システムの調達に当たって、調達仕様書が情報セキュリティ上問題のないようにしなければならない。

（イ）情報システム管理者は、機器、ソフトウェア及びアプリケーションを調達する場合は、製品が情報セキュリティ上問題にならないかどうか、確認しなければならない。

②システムの開発

（ア）情報システム管理者は、教育情報システムを利用し、システムの開発を行うときは、CIO の承認を得なければならない。

（イ）情報システム管理者は、システムの開発に当たって、リスク分析を行うとともに、事故、障害等による被害の発生を防止する、若しくは最小限に抑えるため、次の事項に留意し、必要な対策を講じなければならない。

・システムの運転状況を監視する機能を備えるとともにシステムの障害箇所の検知機能を備えること。

・障害箇所を特定するため、ロギング情報（処理及び操作の記録情報）が取得できること。

・必要に応じて故障箇所を閉塞し縮退運転ができるようにすること

・必要に応じてサーバ、ディスク装置等主要機器の代替機器を備え、障害時に代替機器への切替えが容易に行えること

・本番の運用環境と開発、保守環境とは別に分けること

・本番のシステムデータ及びプログラムとテスト用のデータ及びプログラムは別に管理すること。

・データ及びシステムのバックアップが容易に行えるようにすること

・データ入力時のエラーチェックを行えるようにすること

・システム開発の責任者及び作業者が利用する ID を管理し、開発完了後、開発用 ID を削除すること

・システム開発の責任者及び作業者の接続権限を設定すること

・情報システム管理者は、システムの維持管理に必要な各種ドキュメントを整備し、保管場所を定め厳重に保管しなければならない。

③システムの導入

（ア）情報システム管理者は、システムを導入する前に十分なテストを行い、不具合の発見及び解消に努めなければならない。

（イ）情報システム管理者は、既存のネットワークを利用したシステムを導入しようとするときは、当該ネットワークのシステム管理者と協議し、ネットワークへの接続テストを行うとともに、接続権限を明確にし、接続の管理等に関する事項を定めなければならない。

④システムの保守

（ア）情報システム管理者は、システムの保守を行うときは、不具合の確認を行い、既存の

システムの運用に影響が出ないようにしなければならない。

（イ）情報システム管理者は、システムの追加、変更、廃棄等をしたときは、その際の履歴を記録するとともに、ドキュメントの変更整備を行わなければならない。

⑤機器の保守等

（ア）機器の保守点検を定期的に実施するとともに、その記録を適切に保存しなければならない。

（イ）記録媒体の含まれる機器について、外部の業者に修理させる場合は、当該機器に記録されている内容が消去された状態で行わなければならない。ただし、情報を消去することが難しい場合は、修理を委託する事業者に対し秘密を守ることを契約に定めなければならない。

（ウ）記録媒体の含まれる機器を廃棄、リース返却等をする場合は、当該機器に記録されている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。

（１３）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修正

情報システム管理者は、情報セキュリティに関する最新の情報を収集し、必要に応じてネットワーク、システムの端末機及びサーバ等のソフトウェア及びアプリケーションに最新のプログラム修正を行うことにより、セキュリティホールを防ぐ等、必要な措置を講じなければならない。

②セキュリティ侵害の対策

情報システム管理者は、情報セキュリティに関する最新の情報を収集し、必要に応じて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。

③コンピュータウィルス等の不正プログラム対策の周知及び徹底

情報セキュリティ管理者は、常時コンピュータウィルス等の不正プログラムに関する情報収集に努めるとともに、必要に応じてウィルス対策について教職員に対する啓発を行わなければならない。

9　運用

（1）システム等の適正運用

①関係規程の作成

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に基づき、教育情報システムにおける情報セキュリティ対策の実施に関し必要となる事項を定めた関係規程を作成し、適切に運用しなければならない。

②運用管理手法、運用計画の明確化

（ア）情報システム管理者は、システムの運用を開始する前に、運用管理の手法及び体制等について明らかにしなければならない。

（イ）情報システム管理者は、システムの運用に当たり、運用計画を策定し、年間、月間及

び週間等における運用スケジュール、システムの運用時間、運用形態等運用管理に必要な事項を明確にしなければならない。

（ウ）情報システム管理者は、ネットワークの運用に当たり、運用管理の手法及び体制、運用計画を明らかにしなければならない。

③機器操作の適正化

（ア）システムにおける措置

サーバ等の機器については情報システム管理者、また端末については情報セキュリティ管理者が、それぞれ指示若しくは承認した者が操作を行わなければならない。

情報システム管理者は、操作マニュアル等を作成し、研修を実施する等、機器操作の適正化に努めなければならない。また、システムの追加、変更、廃棄等をしたときは、その履歴を記録するとともに常に変更を反映し、操作マニュアル等を最新の状態にしなければならない。

情報システム管理者は、システムのオペレーション作業の実施に当たり、次の事項について管理方法を明確に定め、適切に運用管理を行わなければならない。

・スケジュール管理
・出力及び廃棄帳票の管理
・磁気テープ等の記録媒体の管理
・オペレータの電子計算機室への入退室管理
・オペレータの作業内容の把握、管理
・電子計算機機器及びネットワーク機器の障害時の対応
・その他必要な事項

（イ）ネットワークにおける措置

ネットワーク機器の操作については、情報システム管理者が指示若しくは承認した者が行わなければならない。

情報システム管理者は、操作マニュアル等を作成する、又は利用方法の周知を行う等、ネットワークの利用の適正化に努めなければならない。また、ネットワークの追加、変更、廃棄等をしたときは、その履歴を記録するとともに常に変更を反映し、操作マニュアル等を最新の状態にしなければならない。

情報システム管理者は、ネットワークのオペレーション作業の実施について適切に管理しなければならない。

④データ等のバックアップ運用

情報システム管理者は、万一の事故、障害等の発生に備え、データ・プログラムのバックアップを適切に行わなければならない。

データ・プログラムのバックアップに当たっては、次の事項に留意しなければならない。

（ア）情報システム管理者は、バックアップコピーを取得するデータ、取得の方法及びサイクルを定め、それに基づいてデータのバックアップを適切に実施しなければならない。

（イ）情報システム管理者は、プログラムの変更の都度、プログラムのバックアップコピーを取得しなければならない。

（ウ）情報システム管理者は、データのバックアップ取得後、次のデータのバックアップ取得までの間、必要に応じて、データベースの更新記録情報を取得しなければならない。

（２）システム等の監視及び予防措置

①システム等の監視

（ア）重要システムの運用に当たっては、情報セキュリティに関する事案を検知するため、情報システム管理者は、常にシステムの稼働監視を行わなければならない。特に、外部と接続するシステムについては、ファイアウォール等を用い、不正な接続による攻撃を受けていないかどうか監視、分析を行わなければならない。

（イ）ネットワークに係る情報セキュリティに関する事案を検知するため、情報システム管理者は、ネットワークの稼働監視を行わなければならない。特に、外部と接続するネットワークについては、ファイアウォール、侵入監視装置等を用い、不正な接続による攻撃を受けていないかどうか監視、分析を行わなければならない。

（ウ）監視により得られた結果については、消去や改ざんされないために必要な措置を講じ、定期的に安全な場所に保管しなければならない。

（エ）重要なログ等を取得するサーバについては、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予防措置

（ア）情報セキュリティ管理者は、教育情報システムに障害又は侵害が発生し、教育情報システムが利用できない場合に備え、業務への影響を最小限に抑えるため、代替処理方法を定めなければならない。

（イ）教育情報システムに被害が生じるおそれがある事案を発見した場合、情報セキュリティ管理者は予防措置を講じなければならない。また、情報セキュリティ管理者は、直ちに情報システム管理者に報告しなければならない。

（ウ）情報システム管理者は、直ちに、当該事案を CIO に報告し、適切な措置を講じなければならない。

（３）システム及びネットワークの障害時、侵害時の対応

①障害時の対応

（ア）責任体制

情報システム管理者及び情報セキュリティ管理者は、教育情報システムの障害時における連絡及び対処の責任者となり、関係者との連携により教育情報システムを速やかに回復しなければならない。

（イ）障害時における対応方法の周知

情報システム管理者及び情報セキュリティ管理者は、システムの運用を開始する前に、障害時における対応マニュアルを関係者に周知しなければならない。

（ウ）障害時の連絡及び対処

・教育情報システムの利用者が障害を発見したときは、直ちに情報セキュリティ管理者に報告しなければならない。

・情報セキュリティ管理者は、システムの回復に向け適切な措置を講じなければならな

い。

・情報セキュリティ管理者は、障害の被害が重大な場合又はシステムの運用に著しい支障が発生している場合は、直ちに、情報システム管理者に報告を行わなければならない。

・情報システム管理者は、障害及び故障の発生の原因及び処理の報告を求めるとともに、当該障害及び故障の原因及び処理結果について記録しなければならない。

・報告を受けた情報システム管理者は、直ちに、CIO に報告を行わなければならない。

（エ）再発防止措置

情報システム管理者及び情報セキュリティ管理者は、障害原因等を分析し、再発防止に向け必要な改善措置を講じなければならない。

（オ）事後検証

CIO は、報告のあった障害事案について、再発防止に向け必要な改善措置が講じられているか情報システム管理者に報告を求めることができる。

②侵害時の対応

（ア）責任体制

情報システム管理者及び情報セキュリティ管理者は、所管する情報資産及び教育情報システムにおいて、不正行為等による情報の流出、滅失、改ざん等の侵害事案が発生した場合、連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速に実施するとともに、再発防止の措置を講じなければならない。また、CIO は、侵害時の対応が円滑に実施されるよう、監督、指導を行わなければならない。

（イ）侵害時の対応方法の周知

情報システム管理者は、所管する情報資産に対し作成される関係規程において、侵害時の対応方法を明記させるとともに、関係する管理者、教職員に対し当該対応方法について周知を行わなければならない。

（ウ）侵害時の連絡

・教育情報システムの利用者が侵害事案の発生を発見したときは、直ちに、情報セキュリティ管理者に報告する。

・情報セキュリティ管理者は、侵害事案の発生を発見し、又は侵害の報告を受けたときは、直ちに、情報システム管理者に報告を行わなければならない。

・報告を受けた情報システム管理者は、直ちに、CIO に報告しなければならない。

・情報システム管理者及び情報セキュリティ管理者は、侵害事案が法令等に違反するものと見込まれる場合、CIO と協議し、警察等関係機関に通報しなければならない。

・CIO は、侵害事案がサイバー攻撃等による緊急時の場合においては、緊急連絡体制を設置し、情報セキュリティ対策が適切に実施されるよう、監督、指導を行わなければならない。

（エ）侵害時の対処

・情報システム管理者及び情報セキュリティ管理者は、侵害事案が発生したときは、事案の内容、原因、被害及び影響範囲等について調査を実施しなければならない。

・情報セキュリティ管理者は、次の事案が発生し情報資産保護のためにシステムの停止がやむを得ない場合は、情報システム管理者と協議の上、システムを停止しなければならない。ただし、教育情報システムの運用に著しい支障を来す攻撃が継続しているとき、コンピュータウィルス等不正プログラムが情報資産に深刻な被害を及ぼしているとき、及びその他の情報資産に係る重大な被害が想定されるとき等、情報資産を保護するため急を要する場合には、情報セキュリティ管理者は当該協議をしないでシステムを停止することができる。

・情報システム管理者及び情報セキュリティ管理者は、事案に係るシステムの接続記録及び現状を保存するとともに、事案に対処した経過を記録しなければならない。

・事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を講じた後、システムの復旧を行う。

・情報システム管理者は、上記の対処に当たり、情報セキュリティ管理者から随時報告を求め、作業の実施を管理しなければならない。

（オ）再発防止措置

情報システム管理者及び教育情報セキュリティ管理者は、当該事案に係る原因及びリスク等を分析し、再発防止に向け必要な改善措置を講じなければならない。また、情報システム管理者は、改善措置の実施について確認を行うとともに、再発防止に向け、関係する教職員に対し対応方法について周知を行わなければならない。

（エ）事後検証

CIO は、報告のあった侵害事案について、再発防止に向け必要な改善措置が講じられているか情報システム管理者に報告を求めることができる。

（４）例外措置

①例外措置の承認

情報システム管理者及び情報セキュリティ管理者は、ポリシー等を遵守することが困難な状況で、事務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、CIO に承認を受けて、例外措置を取ることができる。

②緊急時の例外措置

情報システム管理者及び情報セキュリティ管理者は、事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、事後直ちに CIO に報告しなければならない。

（５）ポリシー等の遵守状況の確認

①ポリシー等の遵守状況の確認

情報セキュリティ管理者は、学校において、ポリシー及び所管する情報資産に係る関係規程が遵守されているかどうか、また、侵害等の問題が発生していないかについて確認し、問題が発生した場合には、直ちに、情報システム管理者に報告しなければならない。

情報システム管理者は、学校において、教育情報セキュリティポリシー及び所管する情報資産に係る関係規程が遵守されているかどうか、また、侵害等の問題が発生していないか

について確認し、問題が発生した場合には、直ちに、CIO に報告しなければならない。

CIO は、教育情報セキュリティポリシー等の遵守状況及び問題発生の状況について確認を行うため、情報システム管理者に報告を求めることができる。

情報システム管理者は、所管する情報資産について関係規程の作成又は見直しが行われた場合、当該情報セキュリティ管理者から報告を受けなければならない。また、情報システム管理者は、関係規程を見直し、変更（役職名や連絡先の変更等の軽微なものを除く。）が行われた場合、CIO に報告を行わなければならない。

②ポリシー違反に関する対応

故意又は重大な過失により、ポリシーに違反し、委員会が保有する情報資産に危害を加えるなど、公務の運営に支障を生じさせた教職員は、懲戒処分に関する指針に基づく処分を受けることがある。

１０ 外部サービスの利用

（１）外部委託

教育情報システムの外部委託を行う際は、以下の点に留意する。これは共同アウトソーシングやクラウドサービス利用の形態等による場合も同様である。

①選定基準

情報セキュリティ管理者及び情報システム管理者は、外部委託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。

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティマネジメントシステムの国際規格認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定しなければならない。

情報セキュリティ管理者及び情報システム管理者は、クラウドサービスを利用する場合は、情報の重要性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

②契約項目

教育情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

（ア）教育情報セキュリティポリシー及び教育情報セキュリティ関係規程の遵守
（イ）外部委託事業者の責任者、委託内容、作業者、作業場所の特定
（ウ）提供されるサービスレベルの補償
（エ）外部委託事業者に接続を承認する情報の種類と範囲、接続方法
（オ）外部委託事業者の従業員に対する教育の実施
（エ）提供された情報の目的外利用及び受託者以外の者への提供の禁止
（カ）業務上知り得た情報の守秘義務
（キ）再委託に関する制限事項の遵守
（ク）委託業務終了時の情報資産の返還、廃棄等
（ケ）委託業務の定期報告及び緊急時報告義務

（コ）町による監査、検査

（サ）町による情報セキュリティインシデント発生時の公表

（シ）教育情報セキュリティポリシーが遵守されなかった場合の規程（損害賠償等）

③確認及び措置等

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、契約に基づき措置しなければならない。またその内容を重要度に応じてCIOに報告しなければならない。

（２）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利用に係る規程の整備

情報システム管理者は、以下を含む約款による外部サービスの利用に関する規程を整備しなければならない。また、当該サービスの利用において、承認なく重要性３以上の情報が取り扱われないように規定しなければならない。

（ア）約款によるサービスを利用してよい範囲

（イ）業務により利用す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

教職員は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが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しなければならない。

（３）ソーシャルメディアサービスの利用

情報システム管理者は、教育委員会又は学校が管理するID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教育委員会又は学校のIDによる情報発信が、教育委員会又は学校のものであることを明らかにするために、プロフィール画面等に掲載し、参照可能とするとともに、IDの自由記述欄等に運用組織を明示する等の方法で成りすまし対策を行うこと。

②パスワードや認証の為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し、不正接続対策を行うこと。

③重要性３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。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。

１１　点検、評価及び見直し

（１）点検、評価

①情報セキュリティ管理者は、所管する教育情報システムに係る関係規程に基づき必要な情報セキュリティ対策が実際に実施されているかどうか、また、関係規程に記載された情報セキュリティ対策に不足がないかどうかについて、定期的に点検を行わなければならない。外部委託事業者に委託している場合も、教育情報セキュリティポリシーの遵守について定期的に点検を行わなければならない。

②情報セキュリティ管理者は、点検結果に基づき、必要な改善を行わなければならない。また、点検結果において、教育情報セキュリティポリシーの記載に疑義が生じたときは、直ちに、情報システム管理者及びCIOに報告しなければならない。

③CIOは、情報システム管理者及び情報セキュリティ管理者に対し、情報セキュリティ対策の監査、点検実施の要請、点検結果の報告を求めることができる。

④CIO又は情報システム管理者は、関係規程に基づき必要な情報セキュリティ対策が実際に実施されているかどうか、また、関係規程に記載された情報セキュリティ対策に不足がないかどうかについて、定期的に点検を行うとともに、点検結果に基づき、必要な改善を行わなければならない。

（２）セキュリティ対策の見直し、変更

①CIO又は情報システム管理者は、新たに必要な対策が発生した場合又は点検の結果、教育情報セキュリティポリシーの内容に疑義が生じた場合等において、教育情報セキュリティポリシーの実効性を評価し、必要な部分の見直し、変更を行わなければならない。

②CIO又は情報システム管理者は、対策基準の変更を行ったときは、速やかに情報セキュリティ管理者その他関係者に周知を行わなければならない。

③情報セキュリティ管理者は、所管する教育情報システムについて、教育情報セキュリティポリシーの変更並びに情報セキュリティをめぐる情勢の変化等に伴い、適宜情報セキュリティ対策の見直しを行い、必要があると認めるときは、関係規程の変更を行わなければならない。

１２　学習者用端末におけるセキュリティ

（１）学習者用端末のセキュリティ対策

①授業に支障のないネットワーク構成の選択

情報システム管理者は、教職員及び児童生徒全員が端末を同時に利用しても授業に支障のないシステムの構築に努めなければならない。また、運用開始前には十分検証し、利用状況に応じて改修を行わなければならない。

②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、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。

（ア）教育委員会が認めたフィルタリングサービスは、株式会社LoiLoの提供する「ロイロWebフィルタ」であり、情報システム管理者は端末において有効に利用されるよう設定しなければならない。また、情報セキュリティ管理者はフィルタリングされる個々のウェブページについて、適切に設定されているか、定期的に確認をしなければならない。

（イ）情報システム管理者は、端末に検索エンジンのセーフサーチ、セーフブラウジング等、不適切なコンテンツへの接続を未然に防止する措置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

情報システム管理者は、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。

④セキュリティ設定の一元管理

情報システム管理者は、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なければならない。

⑤端末の盗難及び紛失時の情報漏洩対策

情報システム管理者は、児童生徒が端末を紛失しても、遠隔操作でロックをかける、又はワイプ（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。

⑥運用及び連絡体制の整備

情報セキュリティ管理者は、学校での端末の統一の運用ルールを制定するとともに、情報セキュリティインシデント時の連絡先や対応方法を整備しなければならない。

（２）児童生徒における ID 及びパスワード等の管理

①ID の登録、変更及び削除

（ア）入学及び転入時の ID 登録処理

情報システム管理者は、ID についてはシンプル、ユニーク（唯一無二）及びパーマネント（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。また、ID は教育委員会において一括して発行及び管理しなければならない。パスワードは、これを保存してはならない。

（イ）進級及び進学時の ID 関連情報の更新

情報システム管理者は、ID については原則として進級及び進学に変更されることがないよう努めなければならない。

（ウ）転出、卒業及び退学時の ID 削除処理

情報システム管理者は、転出、卒業及び退学時には、あらかじめ児童生徒本人によるデータ移行を実施し、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わなければならない。

②シングルサインオンの利用

情報システム管理者及び情報セキュリティ管理者は、新規にサービスを導入する場合には、可能な限り既存の ID を利用したシングルサインオンを利用しなければならない。

１３　SaaS 型パブリッククラウドサービスの利用

（１）SaaS 型パブリッククラウドサービスの利用における情報セキュリティ対策

①利用者認証

（ア）情報システム管理者は、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若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確認または合意しなければならない。

（イ）情報システム管理者は、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、確認または合意しなければならない。

②アクセス認証

（ア）情報システム管理者は、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、確認または合意しなければならない。

（イ）情報システム管理者は、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及び児童生徒のみがアクセスできる環境を設定しなければならない。

③クラウドに保管するデータの暗号化

情報システム管理者は、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確認または合意しなければならない。

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

情報システム管理者は、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確認または合意しなければならない。

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

（ア）情報システム管理者は、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、確認しなければならない。

（イ）クラウド利用者は、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、確認または合意しなければならない。

⑥情報の通信経路のセキュリティ確保

（ア）情報システム管理者は、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る等、セキュリティの確保に努めなければならない。

（イ）情報システム管理者は、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、確認または合意しなければならない。

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

情報システム管理者は、当該クラウドサービスのサーバ等の管理、運用及び廃棄等の条件について、外部委託の場合と同等以上の対策をクラウド事業者に求め、確認または合意し

なければならない。

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

（ア）情報システム管理者は、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の確認をしなければならない。また、クラウド事業者の設定不備等によるインシデント発生時にも同様の確認をしなければならない。

（イ）情報システム管理者は、当該クラウドサービスにおけるサーバの冗長化をクラウド事業者に求め、確認または合意しなければならない。

（ウ）情報システム管理者は、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、確認または合意しなければならない。

（エ）情報システム管理者は、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、確認または合意しなければならない。

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感染対策

（ア）情報システム管理者は、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、マルウェア感染対策を講じることをクラウド事業者に求め、確認または合意しなければならない。

（イ）情報システム管理者は、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、確認または合意しなければならない。

⑩クラウド利用者側のセキュリティ確保

（ア）情報システム管理者は、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なければならない。

（イ）情報システム管理者は、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なければならない。

⑪クラウド事業者従業員の人的セキュリティ対策

（ア）情報システム管理者は、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、確認または合意しなければならない。

（イ）情報システム管理者は、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、確認または合意しなければならない。

（ウ）情報システム管理者は、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、確認または合意しなければならない。

（エ）情報システム管理者は、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、確認または合意しなければならない。

（オ）情報システム管理者は、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、確認または合意しなければならない。

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

（ア）情報システム管理者は、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確認または合意しておかなければならない。

（イ）情報システム管理者は、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確認または合意しておかなければならない。

（ウ）情報セキュリティ管理者は、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なければならない。

⑬クラウドサービス要件基準を満たす配慮を含めたネットワーク設計

情報システム管理者は、利用するクラウドサービスの要件基準を確認し、要件基準を満たすネットワークを設計しなければならない。

別表　情報資産の分類

【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、誤謬又は破損により、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	情報が正確及び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、誤謬又は破損により、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	情報が正確及び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	必要な時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２Ａ	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軽微な支障を及ぼすおそれがある情報資産	必要な時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軽微な支障がある情報
可用性１	可用性２Ａ又は可用性２Ｂの情報資産以外の情報資産	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

【重要性による情報資産の分類】

分類	分類基準	該当する情報の具体例
重要性１	学校で取り扱う情報資産のうち、情報が侵害された場合に甚大な被害が想定され、学校もしくは特定個人が著しい不利益を被る情報であり、要配慮個人情報を含む情報資産	指導要録、教職員の人事記録、健康診断票、医師等による指導・診療・調剤の事実等の要配慮個人情報、犯罪経歴・犯罪による被害事実・少年法に関する事項
重要性２	学校で取り扱う情報資産のうち、情報が侵害された場合に大きな被害が想定され、学校もしくは特定個人が大きな不利益を被る情報であり、重要性１には該当しないものの機密性の高い情報資産	通知表、定期考査・テスト等の採点結果、調査書、進路希望調査票、養護教諭・スクールカウンセラー等による記録、転入学情報、連絡網、住所録
重要性３	学校で取り扱う情報資産のうち、情報が侵害された場合に学校もしくは特定個人が不利益を被る情報であり、重要性２以上には該当しないものの侵害の影響を無視できない情報資産	出席簿、座席表、授業用教材、児童生徒の学習記録（確認テスト、ワークシート、レポート、作品、日常的な簡易な健康観察等）、学習活動の記録（動画、写真等）、卒業アルバム
重要性４	学校で取り扱う情報資産のうち、上記以外の、セキュリティ侵害が発生しても学校事務及び教育活動の実施にはほとんど影響を及ぼさない情報資産	学校要覧、学校紹介パンフレット、学校ホームページ掲載情報、保護者の同意を得て広報等に活用するもの

附則　策定及び改訂記録

１　教育情報セキュリティポリシー基本方針

決裁日	施行日	備考
令和 ５ 年 ２ 月２０日	令和 ５ 年 ３ 月１３日	策定
令和 ７ 年 ８ 月１９日	令和 ７ 年 ８ 月２１日	改訂

２　教育情報セキュリティポリシー対策基準

決裁日	施行日	備考
令和 ５ 年 ２ 月２０日	令和 ５ 年 ３ 月１３日	策定
令和 ７ 年 ８ 月１９日	令和 ７ 年 ８ 月２１日	改訂

付録　様式

目次

様式第１号（松伏町教育情報セキュリティポリシー第３章６（２）関係）

令和　　年　　月　　日

情報システム管理者（教育総務課長）　様

学校名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

校　長＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

ネットワーク機器使用承認及び接続申請及び設定作業依頼書

下記の機器を使用したいので、使用及び（ 校務系 ・ 学習系 ・ 情報系 ）ネットワークへの接続する承認の申請及び設定作業の依頼をします。

記

使用する機器

メーカ名	機器名	使用方法及び理由

以上

- - - -教育総務課処理欄- - - -

課　長	主　幹	担　当	承認印

設定作業実施日　　設定作業者

校務系　・　学習系　接続承認番号

様式第２号（松伏町教育情報セキュリティポリシー第３章６（３）関係）

令和　　年　　月　　日

情報システム管理者（教育総務課長）　様

学校名＿＿＿＿＿＿＿＿＿＿＿＿＿＿

校　長＿＿＿＿＿＿＿＿＿＿＿＿＿＿

保管庫移設承認申請書

下記のとおり保管庫を移設したいので、承認を申請します。

記

移設する保管庫

移設をする保管庫の設置場所、経緯及び理由

以上

- - - -教育総務課処理欄- - - -

課　長	主　幹	担　当	承認印
移設作業実施日			

様式第３号（松伏町教育情報セキュリティポリシー第３章７（１）関係）

令和　　年　　月　　日

情報システム管理者（教育総務課長）　様

学校名＿＿＿＿＿＿＿＿＿＿＿＿＿＿

校　長＿＿＿＿＿＿＿＿＿＿＿＿＿＿

ソフトウェア及びアプリケーション使用承認申請書

下記のとおりソフトウェア又はアプリケーションを使用したいので、承認を申請します。

記

使用するソフトウェア及びアプリケーション

名称 （ライセンスの有無）	導入先	使用方法及び理由
（　　）	校務系 ・ 学習系	

以上

- - - -- - - - - - - - - - - - - - -教育総務課処理欄- - - -- - - - - - - - - - - - - -

課　長	主　幹	担　当	承認印
事前審査完了日		設定作業者	

※審査票を添付すること