議案第２２号

大野市教育情報セキュリティポリシーの策定について

令和８年３月２６日提出

大野教育委員会

教育長　久保俊岳

提案理由

国のガイドラインに基づき、統一的な情報セキュリティポリシーを整備することで、情報漏えい防止と教育活動の継続性を確保できるため、大野市教育情報セキュリティポリシーの策定を行う

大野市教育情報セキュリティポリシー

令和8年●月●日　策定

大野市教育委員会

〈 目　次 〉

序　教育情報セキュリティポリシーの構成

教育情報セキュリティポリシーとは、大野市教育委員会（以下「教育委員会」という。）、大野市立小学校及び中学校（以下「学校」という。）、大野市青少年教育センター（以下「教育センター」という。）が所掌する情報資産に関する教育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を総称する。教育情報セキュリティポリシーは、教育委員会や学校、教育センター（以下「学校等」という。）が所掌する情報資産に関する業務に携わる市職員や教職員、会計年度任用職員等（以下「教職員等」という。）及び外部委託事業者に浸透、普及、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。しかしながら一方では、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へ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を一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）に分けて策定することとした。

具体的には、教育情報セキュリティポリシーを、

教育情報セキュリティ基本方針
教育情報セキュリティ対策基準

の２階層に分け、それぞれを策定することとする。また、教育情報セキュリティ対策基準を、具体的なシステムや手順、手続きに展開して個別の実施事項を定めるものが教育情報セキュリティ実施手順である（下表参照）。

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基本方針	教育情報セキュリティ対策における基本的な考え方
	教育情報セキュリティ対策基準	教育情報セキュリティ基本方針を実行に移すための全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１章　情報セキュリティ基本方針

１　目的

情報セキュリティ基本方針（以下「基本方針」という。）は、学校等が保有する情報資産の機密性、完全性及び可用性を維持するため、学校等が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２　定義

⑴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（ハードウェア及びソフトウェア）をいう。

⑵情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

⑶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。

⑷情報セキュリティポリシー

基本方針及び教育情報セキュリティ対策基準をいう。

⑸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。

⑹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。

⑺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。

３　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

⑴不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

⑵情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監

査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

(3)地震、落雷、火災等の災害によるサービス及び業務の停止等

(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

4　適用範囲

(1)行政機関の範囲

基本方針が適用される行政機関は、学校等とする。

(2)情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①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、電磁的記録媒体

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

5　職員（市職員、教職員等）の遵守義務

職員は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって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実施手順を遵守しなければならない。

6　情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の教育情報セキュリティ対策を講じる。

(1)組織体制

学校等の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

(2)情報資産の分類と管理

学校等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、当該分類に基づき情報セキュリティ対策を実施する。

(3)物理的セキュリティ

サーバ類、サーバ室等、通信回線等及び教職員等のパソコン等の管理について、物理的な対策を講じる。

(4)人的セキュリティ

情報セキュリティに関し、教職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(5)技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(6)運用

教育情報システムの監視、教育情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、教育情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産への侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

(7)外部サービスの利用

外部委託する場合には、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（クラウドサービス）を利用する場合には、利用にかかる規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、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)評価・見直し

教育情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。教育情報セキュリティポリシーの見直しが必要な場合は、教育情報セキュリティポリシーの見直しを行う。

7　情報セキュリティ監査及び自己点検の実施

教育情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8　教育情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、教育情報セキュリティポリシーの見直しが必要となった場合及び情報セキリティに関する状況の変化に対応するため新たに対策が必要になった場合には、教育情報セキュリティポリシーを見直す。

9　教育情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める教育情報セキュリティ対策基準を策定する。

１０　教育情報セキュリティ実施手順の策定

教育情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた教育情報セキュリティ実施手順を策定するものとする。

なお、教育情報セキュリティ実施手順は、公にすることにより学校の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

第２章　情報セキュリティ対策基準

１　管理体制

教育情報セキュリティの管理体制は以下のとおりとする。

(1)教育情報統括管理責任者

教育長を教育情報統括管理責任者とする。教育情報統括管理責任者は、教育委員会や学校、青少年教育センター（以下「学校等」という。）における全てのネットワークや教育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権限及び責任を有する。

(2)教育情報統括責任者

教育委員会事務局長を教育情報統括責任者とする。教育情報統括責任者は、学校等における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。

(3)教育情報セキュリティシステム管理者

教育総務課長を教育情報セキュリティシステム管理者とする。教育情報セキュリティ・システム管理者は、学校等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。また、学校等における教育情報システムの導入、管理、運用、見直し等に関する統括的な権限及び責任を有するほか、所管する教育情報システムに対する情報セキュリティ対策に関する権限及び責任を負う。

(4)教育情報セキュリティ担当者

教育情報セキュリティシステム管理者の指示に従い、学校等における情報資産の管理、運用ルールの策定及び情報セキュリティ対策に関する教職員等の教育研修、助言を行う者を教育情報セキュリティ担当者とする。

(5)教育情報システム担当者

教育情報セキュリティシステム管理者の指示に従い、学校等における教育情報システムの導入、管理、運用、見直し等の作業を行う。また、学校等における情報資産

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、教育情報セキュリティシステム管理者を補佐する者を教育情報システム担当者とする。

(6)学校教育情報セキュリティ責任者

各学校長を学校教育情報セキュリティ責任者とする。学校教育情報セキュリティ責任者は、所属校における教育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、学校における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システム管理者、教育情報統括責任者及び教育情報統括管理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。

(7)学校教育情報セキュリティシステム管理者

各学校の教頭を学校教育情報セキュリティシステム管理者とする。学校教育情報セキュリティシステム管理者は、学校教育情報セキュリティ責任者を補佐するとともに、所属する教職員等の教育情報セキュリティ対策の実施について、管理、指導を行う。また、個々の教育情報システムの管理、運用、見直し等の権限及び責任を有する。

(8)学校教育情報セキュリティシステム担当者

各学校の情報システムの管理、運用に携わる教職員を学校情報セキュリティシステム担当者とする。学校教育情報セキュリティシステム担当者は、学校教育情報セキュリティシステム管理者の指示に従い、情報システムの管理、運用、見直し等の作業を行う。また、学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者と協力して、全教職員に対してこのポリシーの遵守及び周知・啓発に努める。

(9)教育情報セキュリティ委員会への連携

①市の情報セキュリティ対策を統一的に行うため、教育情報統括管理責任者、教育情報統括責任者、教育情報セキュリティシステム管理者から構成される教育情報セキュリティ委員会を設置し、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

②教育情報セキュリティ委員会は、必要に応じて、市における教育情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。

(10)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。

(11)教職員等

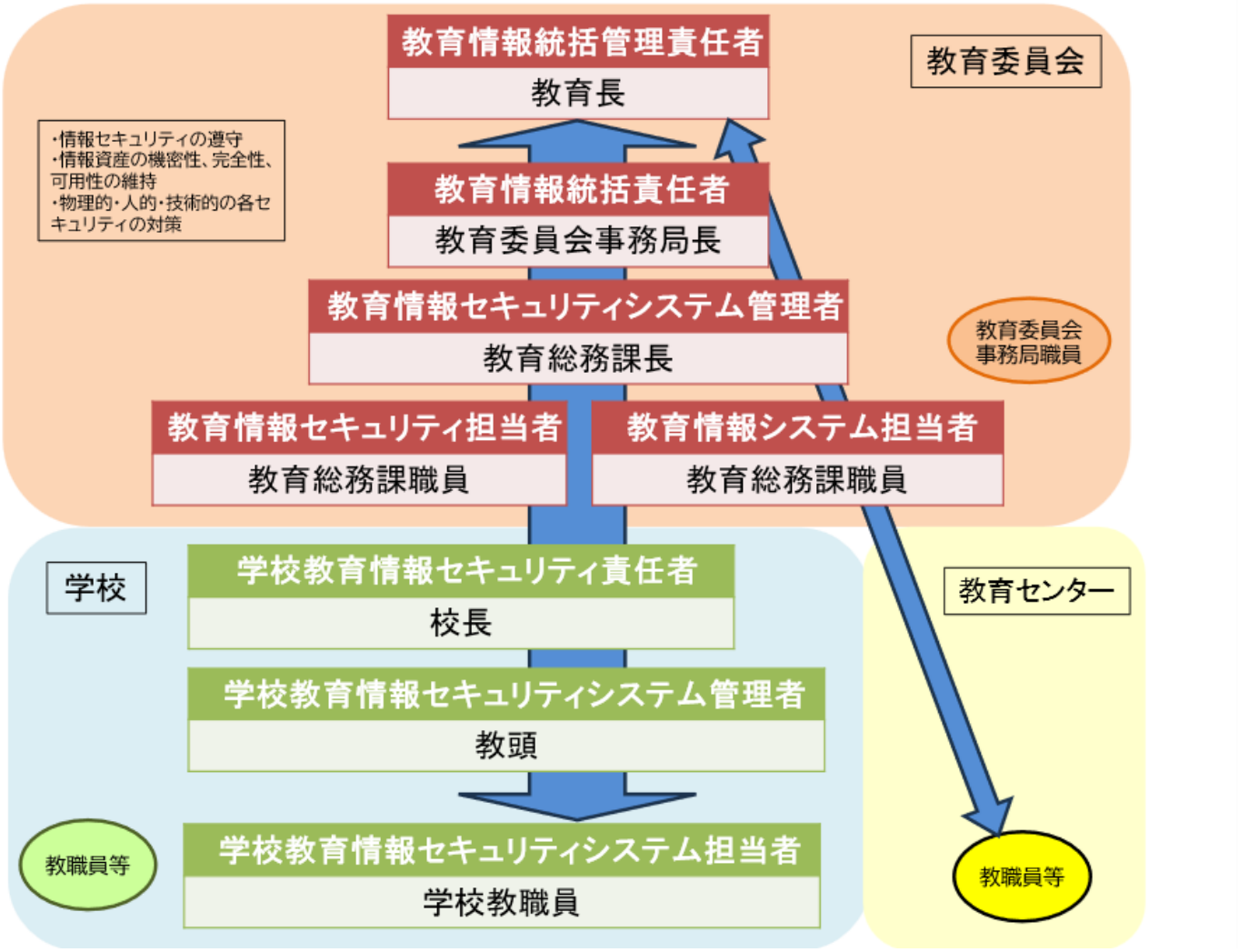
①臨時的任用教職員、非常勤講師を含めた教職員全員を、教職員等と称する。

②教職員等は学校が所管する情報資産を取り扱う立場にあり、学校教育情報セキュリティ責任者の指導の下、情報セキュリティを遵守しなければならない。

(12)教育委員会事務局職員

①教育ネットワークを利用して、学校が所管する情報にアクセスできる教育委員会事務局職員（以下「市職員」という。）を指す。

②市職員は学校の情報資産にアクセスできる立場にあり、教育情報セキュリティシステム責任者の指導の下、情報セキュリティを遵守しなければならない。



２ 情報資産の分類と管理

学校等における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を定め、適正な管理を行う。

分類	分類基準
Ⅰ	セキュリティ侵害が教職員等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もの
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もの
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もの
Ⅳ	影響をほとんど及ぼさないもの

【機密性による情報資産の分類】

機密性	分類基準	該当する情報資産のイメージ
機密性３	学校等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	特定の教職員等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	学校等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	特定の教職員等のみが知り得る状態を確保する必要がある情報資産（教職員等のうち特定の教職員等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	学校等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、児童生徒等がアクセスすることを想定している情報資産	教職員等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（教職員等及び児童生徒のうち特定の教職員等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）
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で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	学校等で取り扱う情報資産のうち、改ざん、誤びゅう又は破壊により、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・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、業務の遂行に支障がある情報
完全性２Ａ	学校等で取り扱う情報資産のうち、改ざん、誤びゅう又は破壊により、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がある情報
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	学校等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（軽微なものは除く）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	学校等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１Ａ	可用性２Ｂ又は可用性２Ａの情報資産以外の情報資産	停止等があった場合でも業務の遂行に支障がない情報

【情報資産の分類】

情報資産の分類					情報資産の例示		
重要性	定　義	機密性	完全性	可用性	校務系	学習系	公関係
Ⅰ	セキュリティ侵害が教職員等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 ・教職員の人事情報 ・教育情報システム仕様書		
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 ・卒業証書授与台帳 ・転退学受付簿 ・転入学受付簿 ・就学児童・生徒移動報告書 ・教科用図書給付児童・生徒名簿 ・要・準要保護児童・生徒台帳 ・その他校内就学援助関係書類 ○成績関係 ・通知表 ・定期考査・テスト等の答案用紙（記入済のもの） ・定期考査素点表 ・成績に関する個票等 ○指導関係 ・児童生徒等の個人写真・集合写真 ・教育相談・面接の記録 ・個別の教育支援計画 ・個別指導計画 ・教務手帳 ○進路関係 ・調査書 ・推薦書 ・公立学校入学者選抜に係る成績一覧表 ・入学者選抜に係る表簿（願書等）	○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 ・学習者用端末 ID/PW 台帳	

					・私立学校入試に係る事前相談一覧表 ・卒業生進路先一覧表 ・進路希望調査 ・進路判定会議資料 ・進路指導記録簿 ○児童生徒に関する個人情報（生活歴、心身の状況、財産状況等の情報、電話番号、メールアドレス、住所、氏名、生年月日、性別等の基本情報を含むもの）		
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	○児童生徒の氏名 ・出席簿 ・名列表 ・児童生徒委員会名簿 ○学校運営関係 ・卒業アルバム ・学校行事等の児童生徒の写真	○学校運営関係 ・授業用教材 ・生徒用配布プリント ○児童生徒の学習系情報 ・児童生徒の学習記録（確認テスト・レポート・作品等） ・学習活動の記録（動画・写真等）	
Ⅳ	影響をほとんど及ぼさない	1	1	1			○学校運営関係 ・学校要覧 ・使用教科書一覧 ・教育課程編成表 ・学校設定費目の届出 ・学校徴収金会計簿 ・学校行事実施計画 ・保護者等への配布文書 ・各種ひな形・校務分掌表 ・ＰＴＡ資料 ・学校・学年・学級だより ・学校ホームページ掲載情報 ・学校行事のしおり

							○学校活動の記録 ＊保護者の承諾がある場合、公開可能 ・学校行事等の児童生徒の写真 ・学習活動の記録（動画・写真・作品等）

【情報資産の管理】

情報資産の管理は、以下のとおりとする。

情報資産の分類					情報資産の管理方法								
重要性	定義	機密性	完全性	可用性	複製・配布	組織外部への持ち出し＊1	端末制限	組織外部への送信＊2	情報資産の運搬＊3	組織外部での情報処理＊4	使用する電磁的記録媒体	情報資産の保管	情報資産の廃棄
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	2 B	2 B	必要以上の複製及び配布禁止	本ガイドラインに遵守していることを確認した上で業務遂行上必要な場合には、教育情報セキュリティ管理者の判断で持ち出しを可	支給以外の端末での作業の原則禁止	限定されたアクセスの措置が取られていること＊5	鍵付きケースへの格納	禁止	施錠可能な場所への保管	・耐火、耐熱、耐水、耐湿を講じた施錠可能な場所に保管（電子データの場合もこれらの対策に準じたサーバに保管） ・情報資産を格納するサーバのバックアップ ・６か月以上のログ保管 ・サーバの冗長化（推奨事項） ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁的記録媒体の持ち込み禁止	電子的記録媒体の初期化、復元できないようにして廃棄

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。	2 B	2 B	2 B	同上	同上		同上	同上	安全管理措置の規定が必要	同上	同上	同上
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。	2 A	2 A	2 A	同上	教育情報セキュリティ管理者の包括的承認で可		同上	同上	同上	同上	・耐火、耐熱、耐水、耐湿を講じた施錠可能な場所に保管（電子データの場合もこれらの対策に準じたサーバに保管） ・情報資産を格納するサーバのバックアップ（推奨事項） ・一定期間以上のログ保管 ・サーバ・ハードディスクの冗　長化（推奨事項） ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁的記録媒体の持ち込み禁止	同上
Ⅳ	影響をほとんど及ぼさない	1	1	1									

＊1 組織外部への持ち出しとは、教育委員会・学校・教育センターが構築している環境（この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）の外に情報資産を持ち出すことを示す。

＊2 情報の組織外部への送信とは、情報システムを構築するネットワーク、端末、サーバの閉じた領域の外側に情報資産をオンラインで持ち出すことを示す。

＊3 情報資産の運搬とは、ＵＳＢメモリやハードディスク等の外部電磁的記録媒体を介して情報資産を運搬する場合を示す。

＊4 組織外部での情報処理とは、教育委員会・学校・教育センターが管理している環境（この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）の外において情報資産を管理・電算処理することを示す。

＊5 限定されたアクセスの措置とは、適切かつ限定的な利用を前提とし、外部に送信される際に適切なアクセス制限を講じることを示す。

3　物理的セキュリティ

3．1　サーバ等の管理

(1)機器の取付け

教育情報セキュリティシステム管理者は、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正に固定する等、必要な措置を講じなければならない。

(2)サーバの冗長化

①教育情報セキュリティシステム管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

(3)機器の電源

①教育情報セキュリティシステム管理者は、教育情報システム担当者及び市の施設管理担当部門と連携し、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、当該機器が適正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。

②教育情報セキュリティシステム管理者は、教育情報システム担当者及び市の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。

(4)通信ケーブル等の配線

①教育情報セキュリティシステム管理者及び教育情報システム担当者は、市の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。

②教育情報セキュリティシステム管理者及び教育情報システム担当者は、主要な箇所の通信ケーブル及び電源ケーブルについて、学校等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。

③教育情報セキュリティシステム管理者及び教育情報システム担当者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

④教育委員会及び学校長から許可を得た者又は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、追加できないように必要な措置を講じなければならない。

(5)機器の定期保守及び修理

①教育情報セキュリティシステム管理者は、可用性２Ａ以上のサーバ等の機器の定期保守を実施しなければならない。

②教育情報セキュリティシステム管理者は、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、教育情報セキュリティシステム管理者は、外部の業者に故障を修理させるに当たり、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ほか、秘密保持体制の確認等を行わなければならない。

(6)施設外又は学校等の外への機器の設置

教育情報セキュリティシステム管理者は、施設外又は学校等の外にサーバ等の機器を設置する場合、教育情報統括管理責任者の承認を得なければならない。また、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。

(7)機器の廃棄等

教育情報セキュリティシステム管理者は、機器を廃棄、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。

３．２ 管理区域（サーバ室等）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「情報システム室」いう。）や電磁的記録媒体の保管庫をいう。

②教育情報統括責任者及び教育情報セキュリティシステム管理者は、管理区域を地階又は１階に設けてはならない。

③教育情報統括責任者及び教育情報セキュリティシステム管理者は、市の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。

④教育情報統括責任者及び教育情報セキュリティシステム管理者は、情報システム室内の機器等に、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。

⑤教育情報統括責任者及び教育情報セキュリティシステム管理者は、市の施設管理部門と連携して、管理区域を囲む外壁等の床下開口部をすべて塞がなければならない。

⑥教育情報統括責任者及び教育情報セキュリティシステム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

(2)管理区域の入退室管理等

①教育情報セキュリティシステム管理者は、管理区域への入退室を許可された者のみに制限し、IC カード、指紋認証等の生体認証又は入退室管理簿の記載による入退室管理を行わなければならない。

②市職員及び外部委託事業者は、管理区域に入室する場合、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。

③教育情報セキュリティシステム管理者は、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た上で、管理区域への入退室を許可された市職員が付き添うものとし、外見上職員と区別できる措置を講じなければならない。

④教育情報セキュリティシステム管理者は、機密性２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、又は個人所有であるコンピュータ、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教育情報セキュリティシステム管理者は、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教育情報セキュリティシステム管理者は、情報システム室の機器等の搬入出について、職員を立ち会わせなければならない。

３．３ 通信回線及び通信回線装置の管理

①教育情報セキュリティシステム管理者及び学校教育情報セキュリティ責任者は、学校等内の通信回線及び通信回線装置を、適正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正に保管しなければならない。

②教育情報セキュリティシステム管理者及び学校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教育情報セキュリティシステム管理者及び学校教育情報セキュリティ責任者は、重要分類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、適正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教育情報セキュリティシステム管理者及び学校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システム管理者及び学校教育情報セキュリティ責任者は、可用性２の情報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。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

３．４ 教職員等の利用する端末や電磁的記録媒体等の管理

⑴校務用端末、校務外部接続用端末及び指導者用端末について

①学校教育情報セキュリティシステム管理者は、盗難防止のため、端末のワイヤーによる固定や保管庫等による管理等、使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。

②学校教育情報セキュリティシステム管理者は、情報システム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学校教育情報セキュリティシステム管理者は、端末の電源起動時のパスワード（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学校教育情報セキュリティシステム管理者は、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。端末にセキュリティー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る媒体を使用しなければならない。

⑵学習用端末について

①学校教育情報セキュリティシステム管理者は、盗難防止のため、端末のワイヤーによる固定や保管庫等による管理等、使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。

②学校教育情報セキュリティシステム管理者は、情報システム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学校教育情報セキュリティシステム管理者は、授業に支障のないネットワーク構成の選択（帯域や同時接続数等）を行うこと。

④学校教育情報セキュリティシステム管理者は、児童生徒等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（フィルタリング設定、検索エンジンのセーフサーチ、セーフブラウジング等）を講じなければならない。

⑤学校教育情報セキュリティシステム管理者は、学校内外での端末におけるマルチウェア感染対策を講じなければならない。

⑥学校教育情報セキュリティシステム管理者は、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等が安心して利用できる状態を維持しなければならない。

⑦学校教育情報セキュリティシステム管理者は、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整理しなければならない。

⑧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、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。

4　人的セキュリティ

4.1 学校教育情報セキュリティ責任者の措置事項

(1)情報資産の管理

①情報資産の持ち出し及び持込みの記録管理

学校教育情報セキュリティ責任者は、教職員等による情報資産の外部持ち出しについて、記録管理しなければならない。

②情報資産の廃棄管理

（ア）学校教育情報セキュリティ責任者は、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。

（イ）学校教育情報セキュリティ責任者は、廃棄した情報資産を記録管理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学校教育情報セキュリティ責任者は、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学校教育情報セキュリティ責任者は、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、直ちに対処し、すみやかに報告が上がるよう、教職員等に対する情報セキュリティ意識の醸成と風通しのよい関係性維持に努めなければならない。

③情報セキュリティポリシー等の閲覧容易性確保

学校教育情報セキュリティ責任者は、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。

(3)端末等の持ち出し及び持込みの記録

学校教育情報セキュリティ責任者は、端末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。

(4)教職員等への情報セキュリティポリシー等の遵守指導

①学校教育情報セキュリティ責任者は、新規採用教職員等及び他自治体から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。

②学校教育情報セキュリティ責任者は、教職員等に対して、必要に応じて情報セキュリティポリシーの遵守の同意書への署名を求める。

⑸新規ソフトウェア及びコンテンツの導入・利用判断

学校教育情報セキュリティ責任者は、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、教育情報セキュリティ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。

⑹インターネット接続及び電子メール利用の制限

①学校教育情報セキュリティ責任者は、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、教育情報セキュリティ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学校教育情報セキュリティ責任者は、パソコンやモバイル端末の機能は、教職員等の業務内容に応じて、不必要な機能については制限することが適切である。

⑺校内及び執務室での管理

学校教育情報セキュリティ責任者は、教職員等と協力して下記を管理しなければならない。

①来校者の氏名及び入退時刻を記録しなければならない。

②来校者には名札などを着用させ、第三者であることが識別できるようにしなければならない。

③地域住民、保護者などに校内施設を開放する場合、執務室等開放していない施設へは入場できないよう制限を設けなければならない。

⑻自己点検の実施

①学校教育情報セキュリティ責任者は、年１回、学校の自己点検を行わなければならない。

②学校教育情報セキュリティ責任者は、自己点検の結果を教育情報セキュリティ委員会に報告しなければならない。

４.２ 教職員等の遵守事項

教職員等は、学校教育情報セキュリティシステム管理者の指導の下、以下の規定を遵守しなければならない。

⑴教育情報セキュリティポリシー等の遵守

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。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに学校教育情報セキュリティシステム管理者に相談し、指示を仰がなければならない。

⑵執務上での管理

①執務室の施錠管理

執務室にて教職員等が不在となる場合には、執務室を施錠しなければならない。

②来校者等への対応

来校者等を執務室に入れる場合には、学校教育情報セキュリティシステム管理者又は学校情報セキュリティシステム担当者の許可を求めなければならない。

③机上の書類・端末等の管理

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学校教育情報セキュリティシステム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) 支給端末の取扱い

①教職員等は、業務目的以外で支給端末を利用してはならない。

②教職員等は、外部のソフトウェアを無断で支給端末にインストールしてはならない。業務上必要な場合には、事前に学校教育情報セキュリティシステム管理者の許可を得ること。

③教職員等は、支給端末の利用において、下記のカスタマイズを無断でしてはならない。

(ア) セキュリティ機能に関する設定変更

(イ) メモリ増設等の改造

④教職員等は、モバイル端末を利用する場合は、盗難・紛失リスクに備えての安全管理をすること。

⑤業務端末から離れる時は、端末をロックするなど、他者が閲覧できないようにしなければならない。

⑥業務終了後と外出時には、電源を落とさなければならない

(4) 支給以外のパソコン、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、支給以外のパソコン、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、学校教育情報セキュリティシステム管理者の許可を得て利用することができる。

②教職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、学校教育情報セキュリティシステム管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

(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・教育センターが構築・管理している環境（本ガイドライン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、学校のモバイル端末、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、学校教育情報セキュリティシステム管理者の許可を得なければならない。

②教職員等は、外部で情報処理業務を行う場合には、学校教育情報セキュリティシステム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。

③教職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、学校教育情報セキュリティシステム管理者又は教育情報セキュリティシステム管理者に通知しなければならない。

(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、学校教育情報セキュリティシステム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パソコン等の端末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）

⑨共有ＩＤに対するパスワードは定期的に又はアクセス回数に基づいて変更しなければならない。

(8) ＩＣカード等の取扱い

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

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。

③ＩＣカード等を紛失した場合には、速やかに学校教育情報セキュリティシステム管理者及び教育情報セキュリティ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支給された公式の媒体を使用しなければならない。その他の媒体の使用は禁止する。

②外部電磁的記録媒体は、学校教育情報セキュリティシステム管理者が管理し、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、学校教育情報セキュリティシステム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情報ファイルを添付する場合には、パスワード設定等の対策を講じなければならない。その際、パスワードを同一メールに記載しないこと。

⑦送信時には誤送信を予防するため、送信先のメールアドレス、添付ファイルの内容を確認しなければならない。

⑧差出人、添付ファイル又は本文中のリンク先等が不審なメールを受信した場合には、添付ファイルの閲覧やリンク先（ＵＲＬ）にアクセスせずに、学校教育情報セキュリティシステム管理者に指示を仰ぎなければならない。

(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Ⅱ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。なお、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、その限りではない。

②私的に契約したクラウドサービスを業務利用してはならない。

③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

教職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

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。

②ＯＳ及びコンピュータウイルス対策ソフトウェアは、常に最新の状態に保てるようにしなければならない。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。

③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。

④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。

⑤端末に対して、不正プログラム対策ソフトウェアによるフルチェックを必要に応じて実施しなければならない。

⑥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ェアでチェックを行わなければならない。

⑦教育情報統括管理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。

⑧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、すみやかに学校教育情報セキュリティシステム管理者に報告し、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により接続する端末（校務用端末等）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により接続する端末（指導者用端末及び学習者用端末等）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）指示があるまでは、端末の電源は切らずに保持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、教育情報統括管理責任者が定めた電子署名、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。

②教職員等は、暗号化を行う場合に教育情報統括管理責任者が定める以外の方法を用いてはならない。また、教育情報統括管理責任者が定めた方法で暗号のための鍵を管理しなければならない。

③教育情報統括管理責任者は、電子署名を使用する場合には、正当性を検証するための情報又は手段を、署名検証者へ安全に提供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、パソコンやモバイル端末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、教育情報統括管理責任者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、学校教育情報セキュリティシステム管理者又は教育情報セキュリティシステム管理者は、ソフトウェアのライセンスを管理しなければならない。

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、パソコンやモバイル端末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、パソコンやモバイル端末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、教育情報統括管理責任者の許可を得なければならない。

(16)無許可でのネットワーク接続の禁止

教職員等は、教育情報統括管理責任者の許可なくパソコンやモバイル端末を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

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。

(18)外部からのアクセス等の制限

①教職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、学校教育情報セキュリティ責任者を介して、教育情報統括管理責任者及び当該情報システムを管理する教育情報セキュリティシステム管理者の許可を得なければならない。

②教職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を施設内のネットワークに接続する前に、アンチウイルス等を通じて、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

(19)児童生徒への指導事項

教職員等は、児童生徒に学習者用端末等を利用させるにあたり、以下の事項について指導を行わなければならない。

①学習用途の利用限定

学習者用端末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利用者認証情報の秘匿管理

ＩＤ及びパスワードは他の人に知られないようにすること。

③ＯＳ及びウイルス対策ソフトウェアの管理

ＯＳ及びウイルス対策ソフトウェアは常に最新の状態に保つこと。

④端末のソフトウェアに関するセキュリティ機能の設定変更禁止

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。

⑤学習系情報は学習系クラウドに保管

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、学習者用端末にローカル保存は必要最小限とすること。

⑥無断で外部ソフトウェアをインストール禁止

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

⑦コミュニケーションツールの利用制限

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

⑧ウイルス感染が疑われる場合の報告

学習用端末が動かない、勝手に操作されている、いつもと異なる画面や警告が示されるなどの症状がでた場合、すぐに担任教員又は教職員に報告すること

⑨端末の安全な取扱い

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。

⑩私物端末の利用禁止

私物端末など承認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接続しないこと

(20) 異動・退職時等の遵守事項

教職員等は、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（紙情報、データの格納された端末、外部記録媒体等）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。

４.３ 教育委員会事務局職員の遵守事項

教育委員会事務局職員は、教育情報セキュリティシステム管理者の指導の下、以下の規定を遵守しなければならない。

(1) 教育情報セキュリティポリシー等の遵守

(2) 業務以外の目的での使用の禁止

(3) 校務用端末による外部における情報処理作業の禁止

(4) 重要性分類Ⅱ以上の情報資産について校務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

(5) 知りえた情報の秘匿

(6) 業務を離れる場合の遵守事項

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全て返却する。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。

４．４ 非常勤及び会計年度任用職員への対応

(1) 情報セキュリティポリシー等の遵守

教育情報セキュリティシステム管理者は、非常勤及び会計年度任用職員に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び会計年度任用職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

(2) 情報セキュリティポリシー等の遵守に対する同意

教育情報セキュリティシステム管理者は、非常勤及び会計年度任用職員の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

(3) インターネット接続及び電子メール使用等の制限

教育情報セキュリティシステム管理者は、非常勤及び会計年度任用職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

5　情報セキュリティ

5.1 研修・訓練

(1)情報セキュリティに関する研修・訓練

学校教育情報セキュリティ責任者は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

(2)研修計画の策定及び実施

①学校教育情報セキュリティ責任者は、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い、教育委員会の承認を得なければならない。

②研修計画において、教職員等は毎年度最低１回の情報セキュリティ研修を受講できるようにしなければならない。

③新規採用の教職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

(3)緊急時対応訓練

学校教育情報セキュリティ責任者は、緊急対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

(4)研修・訓練への参加

すべての教職員等は、定められた研修・訓練に参加しなければならない。

5．2 情報セキュリティインシデントの報告

(1)学校内で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、速やかに学校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報告を受けた学校教育情報セキュリティ責任者は、速やかに教育情報セキュリティ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システム管理者は、報告を受けた情報セキュリティインシデントについて、必要に応じて教育情報統括管理責任者及び教育情報統括責任者に報告しなければならない。

(2)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、学校が管理する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、学校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報告を受けた学校教育情報セキュリティ責任者は、速やかに教育情報セキュリティ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システム管理者は、当該情報セキュリティインシデントについて、必要に応じて教育情報統括管理責任者及び教育情報統括責任者に報告しなければならない。

④教育情報統括責任者は、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るための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

(3)情報セキュリティインシデント原因の究明・記録、再発防止等

①教育情報統括責任者は、情報セキュリティインシデントについて、教育情報セキュリティシステム管理者は、情報セキュリティに関する統一的な窓口と連携し、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、教育情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、教育情報統括管理責任者に報告しなければならない。

②教育情報統括管理責任者は、教育情報統括責任者から情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するための必要な措置を支持しなければならない。

6　技術的セキュリティ

6．1　コンピュータ及びネットワークの管理

(1)文書サーバの設定等

①教育情報セキュリティシステム管理者は、教職員等が使用できる文書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教育情報セキュリティシステム管理者は、文書サーバを学校等の単位で構成し、教職員等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教育情報セキュリティシステム管理者は、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、別途ディレクトリを作成する等の措置を講じ、同一学校であっても、担当教職員等以外の教職員等が閲覧及び使用できないようにしなければならない。

(2)バックアップの実施

教育情報統括責任者及び教育情報セキュリティシステム管理者は、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、校務系情報及び

校務外部接続系情報、学習系情報について、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)他団体との情報システムに関する情報等の交換

教育情報セキュリティシステム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、教育情報統括管理責任者及び教育情報統括責任者の許可を得なければならない。

(4)システム管理記録及び作業の確認

①教育情報セキュリティシステム管理者は、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正に管理しなければならない。

③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名以上で作業し、互いにその作業を確認しなければならない。

(5)情報システム仕様書等の管理

教育情報セキュリティシステム管理者は、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することや、紛失等がないよう、適正に管理しなければならない。

(6)ログの取得等

①教育情報セキュリティシステム管理者は、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、適正にログを管理しなければならない。

③教育情報セキュリティシステム管理者は、取得したログを定期的に点検又は分析する機能を設け、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。

(7)障害記録

教育情報セキュリティシステム管理者は、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、適正に保存しなければならない。

(8)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システム管理者は、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システム管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

(9)外部ネットワークとの接続制限等

①教育情報セキュリティシステム管理者は、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、教育情報統括責任者の許可を得なければならない。

②教育情報セキュリティシステム管理者は、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、庁内及び学校のすべてのネットワーク、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教育情報セキュリティシステム管理者は、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うえで接続しなければならない。

⑤教育情報セキュリティシステム管理者は、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、教育情報統括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。

(10)複合機のセキュリティ管理

①教育情報統括責任者は、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、適正なセキュリティ要件を策定しなければならない。

②教育情報統括責任者は、複合機が備える機能について適正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教育情報統括責任者は、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。

(11)特定用途機器のセキュリティ管理

教育情報統括責任者は、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講じなければならない。

(12)無線 LAN 及びネットワークの盗聴対策

①教育情報統括責任者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務づけなければならない。

②教育情報統括責任者は、機密性の高い情報を扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

(13)電子メールのセキュリティ管理

①教育情報統括責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

②教育情報統括責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

③教育情報統括責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④教育情報統括責任者は、教職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を教職員等に周知しなければならない。

⑤教育情報統括責任者は、システム開発や運用、保守等のため学校等に駐在している外部委託事業者の作業員による電子メールアドレス利用について、委託先との間で利用方法を取り決めなければならない。

⑥教育情報統括責任者は、教職員等が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すことが不可能となるように、添付ファイルの監視等によりシステム上措置を講じなければならない。

(14)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。

(15)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、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。

(16)無許可ソフトウェアの導入等の禁止

①教職員等は、パソコンやモバイル端末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、教育情報セキュリティシステム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、教

育情報セキュリティシステム管理者は、ソフトウェアのライセンスを管理しなければならない。

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。

(17)機器構成の変更の制限

①教職員等は、パソコンやモバイル端末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、パソコンやモバイル端末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、教育情報セキュリティシステム管理者の許可を得なければならない。

(18)無許可でのネットワーク接続の禁止

教職員等は、教育情報セキュリティシステム管理者及び学校教育情報セキュリティ責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

(19)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教育情報セキュリティシステム管理者及び学校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、教育情報統括責任者に通知し適正な措置を求めなければならない。

６．２ アクセス制御

(1)アクセス制御

①アクセス制御

学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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）学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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。

（イ）教職員は、業務上必要がなくなった場合は、利用者登録を抹消するよう、学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者に通知しなければならない。

（ウ）学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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。

③特権を付与されたIDの管理等

（ア）学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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。

（イ）学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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。

（ウ）学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、特権を付与されたID及びパスワードについて、教職員の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

（エ）学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者、特権を付与されたIDを初期設定以外のものに変更しなければならない。

(2)教職員による外部からのアクセス等の制限

①教職員が外部から内部のネットワーク又は情報システムにアクセスする場合は、学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者の許可を得なければならない。

②学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

⑤学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、外部からのアクセスに利用するモバイル端末を教職員に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

⑥教職員は、持ち込んだ又は外部から持ち帰ったモバイル端末を校内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

⑦学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、公衆通信回線（公衆無線LAN等）を教育ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、

利用者のID、パスワード及び生体認証に係る情報等の認証情報認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

(3) 自動識別の設定

学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

(4) ログイン時の表示等

学校教育情報セキュリティシステム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ教職員がログインしたことを確認することができるようシステムを設定しなければならない。

(5) 認証情報の管理

①学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、教職員の認証情報を厳重に管理しなければならない。認証情報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認証情報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学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、教職員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、初回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学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、認証情報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。

(6) 特権による接続時間の制限

学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

６．３ 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システム開発における責任者及び作業者の特定

教育情報セキュリティシステム管理者は、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。

②システム開発における責任者、作業者のＩＤの管理

（ア）教育情報セキュリティシステム管理者は、システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

（イ）教育情報セキュリティシステム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

③システム開発に用いるハードウェア及びソフトウェアの管理

（ア）教育情報セキュリティシステム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

（イ）教育情報セキュリティシステム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

(3) 情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

（ア）学校教育情報セキュリティシステム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

（イ）学校教育情報セキュリティシステム管理者は、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。

（ウ）学校教育情報セキュリティシステム管理者は、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。

（エ）教育情報セキュリティシステム管理者は、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。

②テスト

（ア）教育情報セキュリティシステム管理者は、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。

（イ）教育情報セキュリティシステム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

（ウ）教育情報セキュリティシステム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

（エ）教育情報セキュリティシステム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテスト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教育情報セキュリティシステム管理者は、システム開発・保守に関連する資料及び文書を適正に整備・保管しなければならない。

②教育情報セキュリティシステム管理者は、テスト結果を一定期間保管しなければならない。

③教育情報セキュリティシステム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

(5) 情報システムにおける入出力データの正確性の確保

①教育情報セキュリティシステム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

②教育情報セキュリティシステム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③教育情報セキュリティシステム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

(6) 情報システムの変更管理

教育情報セキュリティシステム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

(7) 開発・保守用のソフトウェアの更新等

教育情報セキュリティシステム管理者は、開発・保守用のソフトウェア等を更新、又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

(8) システム更新又は統合時の検証等

教育情報セキュリティシステム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

６．４ 不正プログラム対策

(1) 学校教育情報セキュリティ責任者の措置事項

学校教育情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

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なければならない。

⑤不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

⑥不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

⑦業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

(2) 学校教育情報セキュリティシステム管理者の措置事項

学校教育情報セキュリティシステム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

①教育情報セキュリティシステム管理者は、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システムに常駐させなければならない。

②不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

③不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

④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、学校等が管理している媒体以外を教職員等に利用させてはならない。また、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、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア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。

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、教育情報セキュリティシステム管理者が許可した教職員等を除く教職員等に当該権限を付与してはならない。

(3) 教職員等の遵守事項

教職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

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端末に対して、不正プログラム対策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。

⑤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ェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを LGWAN 接続系に取込む場合は無害化しなければならない。

⑥不正プログラム対策ソフトウェア開発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。

⑦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、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

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

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。

(4) 専門家の支援体制

教育情報統括責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておくことができる。

６．５ 不正アクセス対策

(1) 教育情報統括責任者の措置事項

教育情報統括責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

①使用されていないポート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ばらない。

③不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、教育情報統括責任者及び教育情報セキュリティシステム管理者へ通報するよう、設定しなければならない。

④教育情報統括責任者は、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正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) 攻撃への対処

教育情報統括責任者はサーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、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。

(3) 記録の保存

教育情報統括責任者は、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。

(4) 内部からの攻撃

教育情報統括責任者及び教育情報セキュリティシステム管理者は、教職員等及び外部委託事業者が使用しているパソコン等の端末からのネットワークやサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

(5) サービス不能攻撃

教育情報統括責任者及び教育情報セキュリティシステム管理者は、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。

(6) 標的型攻撃

教育情報統括責任者及び教育情報セキュリティシステム管理者は、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なければならない。

６．６ 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・共有及びソフトウェアの更新等

教育情報統括責任者及び教育情報セキュリティシステム管理者は、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・周知

教育情報統括責任者及び教育情報セキュリティシステム管理者は、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

教育情報統括責任者及び教育情報セキュリティシステム管理者は、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、セキュリティ侵害等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。

7　運用

7．1 情報システムの監視

①教育情報統括責任者及び教育情報セキュリティシステム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

②教育情報統括責任者及び教育情報セキュリティシステム管理者は、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。

③教育情報統括責任者及び教育情報セキュリティシステム管理者は、外部と常時接続するシステムを常時監視しなければならない。

7．2 情報セキュリティポリシーの遵守状況の確認

(1) 遵守状況の確認及び対処

①教育情報統括責任者及び教育情報セキュリティシステム管理者は、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、速やかに教育情報統括管理責任者に報告し、適正かつ速やかに対処しなければならない。

②教育情報統括責任者及び教育情報セキュリティシステム管理者は、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、定期的に確認を行い、問題が発生していた場合には適正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

教育情報統括責任者及び教育情報セキュリティシステム管理者が指名した者は、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) 教職員等の報告義務

①教職員等は、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システム管理者及び学校教育情報セキュリティ責任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統括責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

7．3 侵害時の対応

(1) 緊急時対応計画の策定

教育情報統括管理責任者は、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正に実施するために、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正に対処しなければならない。

(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) 業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

(4) 緊急時対応計画の見直し

教育情報統括管理責任者は、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。

7．4 例外措置

(1) 例外措置の許可

教育情報統括責任者及び教育情報セキュリティシステム管理者は、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、行政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、教育情報統括管理責任者の許可を得て、例外措置を講じることができる。

(2) 緊急時の例外措置

教育情報統括責任者及び教育情報セキュリティシステム管理者は、行政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、事後速やかに教育情報統括管理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

教育情報統括責任者及び教育情報セキュリティシステム管理者は、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

７．５ 法令遵守

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著作権法（昭和４５年法律第４８号）
③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）
④個人情報の保護に関する法律（平成１５年法律第５７号）
⑤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)
⑥サイバーセキュリティ基本法（平成２８年法律第３１号）
⑦大野市個人情報の保護に関する法律施行条例（令和５年条例第１号）
⑧大野市特定個人情報の取扱いに関する管理規程

７．６ 懲戒処分等

(1)懲戒処分

教育情報セキュリティポリシーに違反した教職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法をはじめとする懲戒処分の対象とする。

(2)違反時の対応

教職員等の教育情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

①教育情報統括管理責任者が違反を確認した場合は、当該教職員等が所属する学校の学校教育情報セキュリティ責任者に通知し、適切な措置を求めなければならない。
②教育情報セキュリティシステム管理者等が違反を確認した場合は、違反を確認した者は速やかに教育情報統括管理責任者及び当該教職員等が所属する学校の学校教育情報セキュリティ責任者に通知し、適切な措置を求めなければならない。

③学校教育情報セキュリティ責任者の指導によっても改善されない場合、教育情報統括管理責任者は、当該教職員等の教育ネットワーク又は教育情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、教職員等の権利を停止あるいは剥奪した旨を当該教職員等が所属する学校の学校教育情報セキュリティ責任者に通知しなければならない。

8　外部サービスの利用

8．1 外部委託

(1) 外部委託先の選定基準

①教育情報セキュリティシステム管理者は、外部委託先の選定に当たり、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教育情報セキュリティシステム管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、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。

③教育情報セキュリティシステム管理者は、クラウドサービスを利用する場合は、情報の機密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

重要な情報資産を取扱う業務を委託する場合には、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。

・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実施手順の遵守
・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
・提供されるサービスレベルの保証
・外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
・外部委託事業者の従業員に対する教育の実施
・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
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・市による監査、検査
・市による情報セキュリティインシデント発生時の公表
・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定（損害賠償等）

(3) 確認・措置等

教育情報セキュリティシステム管理者は、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、(2)の契約に基づき措置しなければならない。また、その内容を教育情報統括責任者に報告するとともに、その重要度に応じて教育情報統括管理責任者に報告しなければならない。

8．2 外部サービスの利用

(1) 外部サービスの利用に係る規定の整備

教育情報セキュリティシステム管理者は、以下を含む外部サービスの利用に関する規定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、機密性の高い情報が取り扱われないように規定しなければならない。

①外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準

②外部サービス提供者の選定基準

③外部サービスの利用申請の許可権限者と利用手続

(2) 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外部サービスの利用を申請し、適正な措置を講じた上で利用しなければならない。

8．3 ソーシャルメディアサービスの利用

①教育情報セキュリティシステム管理者は、学校等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。

（ア）学校等のアカウントによる情報発信が、実際の学校等のものであることを明らかにするために、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己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実施すること。

（イ）パスワードや認証のためのコード等の認証情報を適正に管理するなどの方法で、不正アクセス対策を実施すること。

②機密性２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。

9　評価・見直し

9．1 監査

(1)実施方法

教育情報統括管理責任者は、教育情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報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統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

②監査を行う者は、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情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

②被監査部門は、監査の実施に協力しなければならない。

(4)外部事業者に対する監査

外部事業者に委託している場合、教育情報セキュリティ監査統括責任者は外部事業者から下請けとして受託している事業者も含めて、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

教育情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告する。

(6)保管

情報セキュリティ監査統括責任者は、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しなければならない。

(7)監査結果への対応

教育情報統括管理責任者は、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システム管理者及び学校教育情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない学校教育情報セキュリティ責任者に対しても、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

教育情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規程等の見直し、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。

９．２ 自己点検

(1)実施方法

①教育情報統括管理責任者は、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なければならない。

②教育情報統括責任者は、教育情報セキュリティシステム管理者及び学校教育情報セキュリティ責任者と連携して、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わなければならない。

(2) 報告

教育情報統括責任者、教育情報セキュリティシステム管理者及び学校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、教育情報セキュリティ委員会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教育情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、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。

９．３ 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

教育情報セキュリティ委員会は、教育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、教育情報セキュリティポリシー及び関係規程等について、必要があると認めた場合、改善を行うものとする。

情報セキュリティポリシー概要（案）

令和8年3月策定

本ポリシーは、教育機関が扱う情報を守るために、**①組織体制の整備、②情報資産の適切管理、③物理・人的・技術的セキュリティの徹底、④事故対応と継続的改善**を体系的に規定し、学校・教育委員会が保有する情報資産の機密性・完全性・可用性を守るための基本的な考え方と対策を示す総合的な指針として策定しました。

◆ポリシーの構成

1. **教育情報セキュリティ基本方針**
   → 情報セキュリティ対策の基本的な考え方を示す普遍的部分
2. **教育情報セキュリティ対策基準**
   → 基本方針を実行するための具体的な基準

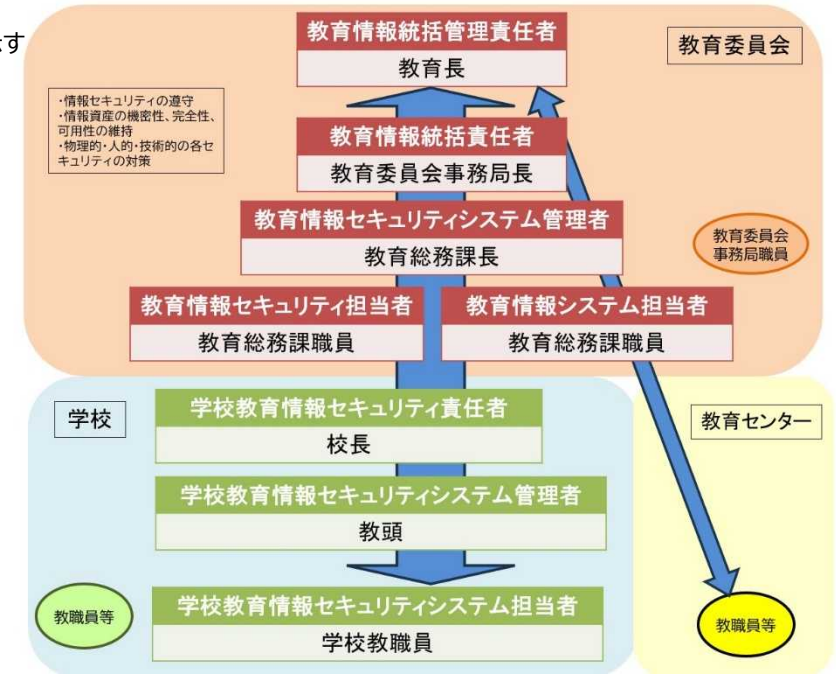
◆対象範囲と情報資産

1. **適用される組織**
   教育委員会、小中学校、青少年教育センター
2. **情報資産の範囲**
   ①教育ネットワーク、情報システム、サーバ等
   ②上記で扱うすべてのデータ・文書
   ③システム仕様書・ネットワーク図等も含む

◆想定する脅威

1. 不正アクセス、ウイルスなどのサイバー攻撃
2. 機器故障・設定ミス・規定違反などの人為的要因
3. 地震・火災など災害
4. 大規模感染症による業務停滞
5. 電力・通信障害などインフラ停止

◆管理体制（イメージ図）



◆教職員が特に遵守すべき主な事項

1.端末・記録媒体の取り扱い
・支給端末の私的利用禁止
・無断ソフトウェアインストール禁止離席時のロック
・モバイル端末紛失時の速やかな報告
2.パスワード・ID管理
・他者と共有禁止　・定期変更
・初期パスワードの速やかな変更
・システム間の使い回し禁止
3.電子メール
・自動転送禁止
・不必要な宛先送信禁止
・添付ファイルはパスワード設定
・不審メールは開かず管理者へ報告
4.インターネット・クラウド
・業務外の閲覧禁止
・私的クラウドサービスの業務利用禁止
・機密性の高い情報のクラウド保存禁止
5.児童生徒への指導
・ID・パスワード管理
・外部ソフトの無断インストール禁止
・不適切サイト対策（フィルタリング）
・学習用端末の適切な取り扱い

◆基本的なセキュリティ対策の柱

1.組織体制
役割・権限を明確化し、管理責任者、システム管理者、学校責任者など多層的な体制を構築
2.情報資産の分類と管理
情報の機密性・完全性・可用性に応じて分類し、保管・持ち出し・廃棄方法を規定
3.物理的セキュリティ
サーバ室の管理、機器の盗難防止、配線管理、電源対策など。
4.人的セキュリティ
職員の遵守事項、研修、意識啓発、来校者管理、事故時の報告義務など
5.技術的セキュリティ
アクセス制御、不正プログラム対策（ウイルス対策）、不正アクセス防止、ログ管理、システム開発・導入・保守の規律、ネットワーク管理
6.運用管理
監視、遵守状況チェック、緊急時対応計画、業務継続計画との整合、例外措置のルール化
7.外部サービス利用
外部委託先の選定基準、クラウド利用ルール、ソーシャルメディアの運用基準
8.評価・見直し
監査と自己点検、結果に基づく改善

◆事故発生時の対応フロー

1. 教職員が発見　→　速やかに学校責任者へ報告
2.学校責任者　→　教育情報セキュリティ管理者へ報告
3.必要に応じ 教育情報統括責任者・管理責任者へ報告
4.原因究明・記録・再発防止策の検討
5.必要に応じ外部公表・警察等との連携

◆違反時の措置

1. 地方公務員法等に基づく懲戒処分の対象
2.システム利用の停止・剥奪
3.外部事業者の違反は契約に基づく措置

大野市教育情報セキュリティポリシー説明日程