

坂戸市教育情報セキュリティポリシー

令和4年11月
坂戸市教育委員会

目次

教育情報セキュリティ基本方針（宣言書）	1
序 坂戸市教育情報セキュリティポリシーの構成	2
第1章 教育情報セキュリティ基本方針	3
1 目的	3
2 定義	3
3 対象とする脅威	4
4 適用範囲	4
5 教職員の遵守義務	4
6 情報セキュリティ対策	5
7 教育情報セキュリティ監査及び自己点検の実施	5
8 教育情報セキュリティポリシーの見直し	5
9 教育情報セキュリティ対策基準の策定	6
10 教育情報セキュリティ実施手順の策定	6
第2章 教育情報セキュリティ対策基準	7
1 対象範囲及び用語説明	7
2 組織体制	8
3 情報資産の分類と管理方法	12
4 物理的セキュリティ	16
5 人的セキュリティ	22
6 技術的セキュリティ	25
7 運用	37
8 外部サービスの利用	39
9 クラウドサービスの利用	40
10 1人1台端末におけるセキュリティ	46
11 評価・見直し	47
【参考】資料編	50
1 策定・改訂記録	50
2 情報資産の分類と例示	51

教育情報セキュリティ基本方針（宣言書）

坂戸市教育委員会の教育情報システムが取り扱う情報には、児童生徒の個人情報のみならず、学校運営上重要な情報が多数含まれています。これらの情報に改ざん、破壊、漏えいなどの事故が生じた場合、児童生徒や学校運営に対して深刻な問題を引き起こすこととなります。

教育情報システムで取り扱う情報資産をさまざまな脅威から保護し、機密性、完全性及び可用性を維持する、いわゆる情報セキュリティ対策の推進は、市民の財産やプライバシーを守ることはもとより、坂戸市教育委員会に対する市民からの信頼の維持や向上に寄与するなど、教育行政を安定的に運営していくために極めて重要な取組です。

そのため、坂戸市教育委員会では、情報資産を故意や偶然という区別に関係なく、改ざん、破壊、漏えいなどの事故から保護することを目的に「教育情報セキュリティポリシー」を策定し、安全対策に努めています。坂戸市教育委員会が保有する情報資産を利用する者には、「教育情報セキュリティポリシー」に基づく行動の遵守を徹底し、強固な情報セキュリティ体制の維持・向上を図ってまいります。

令和4年11月1日

坂戸市教育委員会

教育長 安齊 敏雄

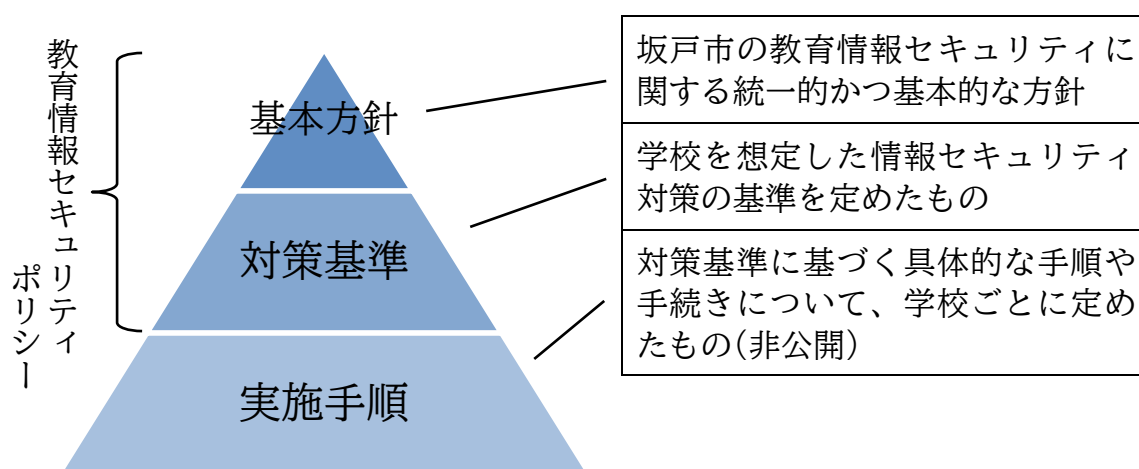
序 坂戸市教育情報セキュリティポリシーの構成

坂戸市教育情報セキュリティポリシー（以下、「本ポリシー」という。）とは、坂戸市立小・中学校（以下、「各学校」という。）が保有する教育の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。

本ポリシーは、本市教育委員会や各学校が保有する情報資産を取り扱うすべての教職員（教育委員会事務局職員、非常勤及び臨時的任用教職員、会計年度任用職員を含む。以下、「教職員」という。）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求められる。一方で、技術の進歩等に伴う教育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、本ポリシーは、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「教育情報セキュリティ対策基準」の2階層から成るものとして策定する。また、本ポリシーに基づき、具体的な情報セキュリティ対策の実施手順として「坂戸市教育情報セキュリティポリシー実施手順」を策定する。

【図】坂戸市教育情報セキュリティポリシーの構成



第1章 教育情報セキュリティ基本方針

1 目的

各学校が取り扱う情報には、児童生徒の個人情報のみならず、保護者、教職員、その他地域住民に関する情報等学校運営に欠かせない重要な情報が数多く含まれ、外部に漏えいした場合に極めて深刻な問題を引き起こすおそれがある。

したがって、本市の教育ネットワークにおいて、個人情報を始めとする各種情報資産をさまざまな脅威から防御することは、信頼ある安心・安全な学校づくりに必要不可欠なことである。

また、平成29～31年に改訂された学習指導要領において、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、各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必須である。

そのため、本基本方針は、各学校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、本市教育委員会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

本基本方針において、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) 教育ネットワーク

本市の学校教育において情報資産を扱う通信回線やルータ等の通信機器で接続し、情報を伝達するための仕組みのことをいう。

(2) 教育情報システム

本市の学校教育において使用されるパソコン、ソフトウェア及び記録媒体等で構成され情報処理を行う仕組みのことをいう。

(3) 情報セキュリティ

情報資産を脅威（自然災害、機器障害、悪意のある行為等の損失を発生させる直接の要因をいう。）から保護し、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が認められた者が、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。

- (1) 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
- (2) 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的要因による情報資産の漏えい・破壊・消去等
- (3) 地震、水害、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) 行政機関等の範囲

本基本方針が適用される機関は、本市教育委員会及び各学校とする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産の範囲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教育ネットワーク図等のシステム関連文書

5 教職員の遵守義務

教職員は、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

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) 組織体制

本市教育委員会及び各学校の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

(2) 情報資産の分類と管理

本市教育委員会及び各学校が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

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

教育ネットワークの監視、本ポリシーの遵守状況の確認等、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、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するための対策を講じる。

(7) 評価・見直し

本ポリシーの順守状況を検証するため、必要に応じて教育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、適宜見直しを行う。

7 教育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、必要に応じて教育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

教育情報セキュリティ監査及び自己点検の結果、本ポリシーの見直しが必要となった

場合及び情報セキュリティに関する状況の変化に対応するために新たに対策が必要となった場合には、適宜本ポリシーを見直す。

9 教育情報セキュリティ対策基準の策定

情報セキュリティ対策、教育情報セキュリティ監査、自己点検及び必要に応じて本ポリシーの見直しを実施するために、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本市教育行政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 教育情報セキュリティ対策基準

1 対象範囲及び用語説明

(1) 行政機関等の範囲

本対策基準が適用される機関は、本市教育委員会及び各学校とする。

(2) 情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

- ① 教育ネットワーク、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教育ネットワーク図等の関連文書

【情報資産の種類と例】

情報資産の種類	情報資産の例
教育ネットワーク	情報資産を扱う通信回線、ルータ等の通信機器
教育情報システム	情報資産を扱うサーバ、パソコン、モバイル端末、オペレーティングシステム、ソフトウェア、クラウドサービス等
これらに関する施設・設備	情報資産を扱うコンピュータ教室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル
電磁的記録媒体	情報資産を扱うサーバ装置（クラウドサービスを除く）、端末、デジタルカメラ、デジタルビデオカメラ、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USBメモリ、外付けハードディスクドライブ、DVD-R、磁気テープ、SDカード等の外部電磁的記録媒体
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	教育ネットワーク、教育情報システムで取り扱うデータ（これらを印刷した文書を含む。）
教育情報システム関連文書	教育情報システム関連のシステム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図、クラウドサービス契約関連文書等

(3) 用語解説

本対策基準における用語は、以下のとおりとする。

用語	定義
校務系情報	児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教員の個人情報など、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
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
学習系情報	児童生徒のワークシート、作品など、学校が保有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ当該情報に教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
校務用端末	校務系情報にアクセス可能な端末
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
学習者用端末	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
指導者用端末	学習系情報にアクセス可能な端末で、教員のみが利用可能な端末
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及び、校務系情報を扱ううえ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
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
学習系システム	学習系ネットワーク、学習系サーバ、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及び、学習系情報を扱ううえで、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
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
校務系サーバ	校務系情報を取り扱うサーバ
校務外部接続系サーバ	校務外部接続系情報を取り扱うサーバ
学習系サーバ	学習系情報を取り扱うサーバ

2 組織体制

(1) 組織体制

- ① 最高情報セキュリティ責任者（CISO：Chief Information Security Officer、以下「CISO」という。）
- ア 教育長を、CISO とする。CISO は、本市における全ての教育ネットワーク、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最終決定権限及び責任を有する。
- イ CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高教育情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。
- ② 統括教育情報セキュリティ責任者
- ア 教育部長を、CISO 直属の統括教育情報セキュリティ責任者とする。
- イ 統括教育情報セキュリティ責任者は、教育部長の中から CISO が任命する。
- ウ 統括教育情報セキュリティ責任者は、CISO を補佐しなければならない。
- エ 統括教育情報セキュリティ責任者は、本市の全ての教育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。
- オ 統括教育情報セキュリティ責任者は、本市の全ての教育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。
- カ 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。
- キ 統括教育情報セキュリティ責任者は、本市の学校教育に関す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、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。
- ク 統括教育情報セキュリティ責任者は、本市の共通的な教育ネットワーク、教育情報システム及び情報資産に関する教育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。
- ケ 統括教育情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、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を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。
- コ 統括教育情報セキュリティ責任者は、緊急時には CISO に早急に報告を行うとともに、回復のための対策を講じなければならない。
- ③ 教育情報セキュリティ責任者
- ア 学校教育課長を教育情報セキュリティ責任者とする。
- イ 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。
- ウ 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。

エ 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、緊急時等における連絡体制の整備、教育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に対する教育、訓練、助言及び指示を行う。

④ 教育情報セキュリティ管理者

ア 教育委員会事務局の各課長及び各学校の校長を、教育情報セキュリティ管理者とする。

イ 教育情報セキュリティ管理者は当該課又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。

ウ 教育情報セキュリティ管理者は、当該課又は学校において、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、統括教育情報セキュリティ責任者及び CIS0 へ速やかに報告を行い、指示を仰がなければならない。

エ 教育情報セキュリティ管理者は、教育情報セキュリティ責任者の指示に従い、学校の情報資産等の管理台帳を作成し、適正な管理を行わなければならない。

⑤ 教育情報システム管理者

ア 学校教育課長を、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。

イ 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。

ウ 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。

エ 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。

⑥ 教育情報システム担当者

ア 学校教育課担当職員を、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。

イ 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。

⑦ 教育情報セキュリティ委員会

ア 本市の教育情報セキュリティ対策を統一的に行うため、CIS0、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及び CIS0 が別途選任した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、教育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。

イ 教育情報セキュリティ委員会は、毎年度、本市における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。

⑧ 兼務の禁止

ア 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。

イ 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。

⑨ 教育情報セキュリティに関する統一的な窓口（CSIRT）の設置

ア CISO は、情報セキュリティインシデントの統一的な窓口の機能を有する組織（CSIRT：Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

イ CSIRT 責任者

（ア）教育部長を CSIRT 責任者とする。

（イ）CSIRT 責任者は、CSIRT の事務を監督し、及び評価し、並びに他の組織等との調整役になるとともに、セキュリティ事故対応に必要な要員、リソース及び技能を確保する。

ウ CSIRT 管理者

（ア）学校教育課長を CSIRT 管理者とする。

（イ）CSIRT 管理者は、セキュリティ事故対応の作業員及び要員を調整するとともに、インシデントに関する最新情報を必要な関係者に提供するとともに、CSIRT の技術的な品質を監督し、及び管理する。また、必要に応じて、インシデントに関する情報提供及び助言等について、市長部局への協力を要請する。

エ 情報セキュリティに関する統一的な窓口（PoC：Point of Contact、以下「PoC」という。）

（ア）学校教育課を PoC とする。

（イ）PoC は、インシデントの発生に関する予兆等の検知及び発見並びに内外からのセキュリティ事故に関する連絡、報告等の受付を行う。

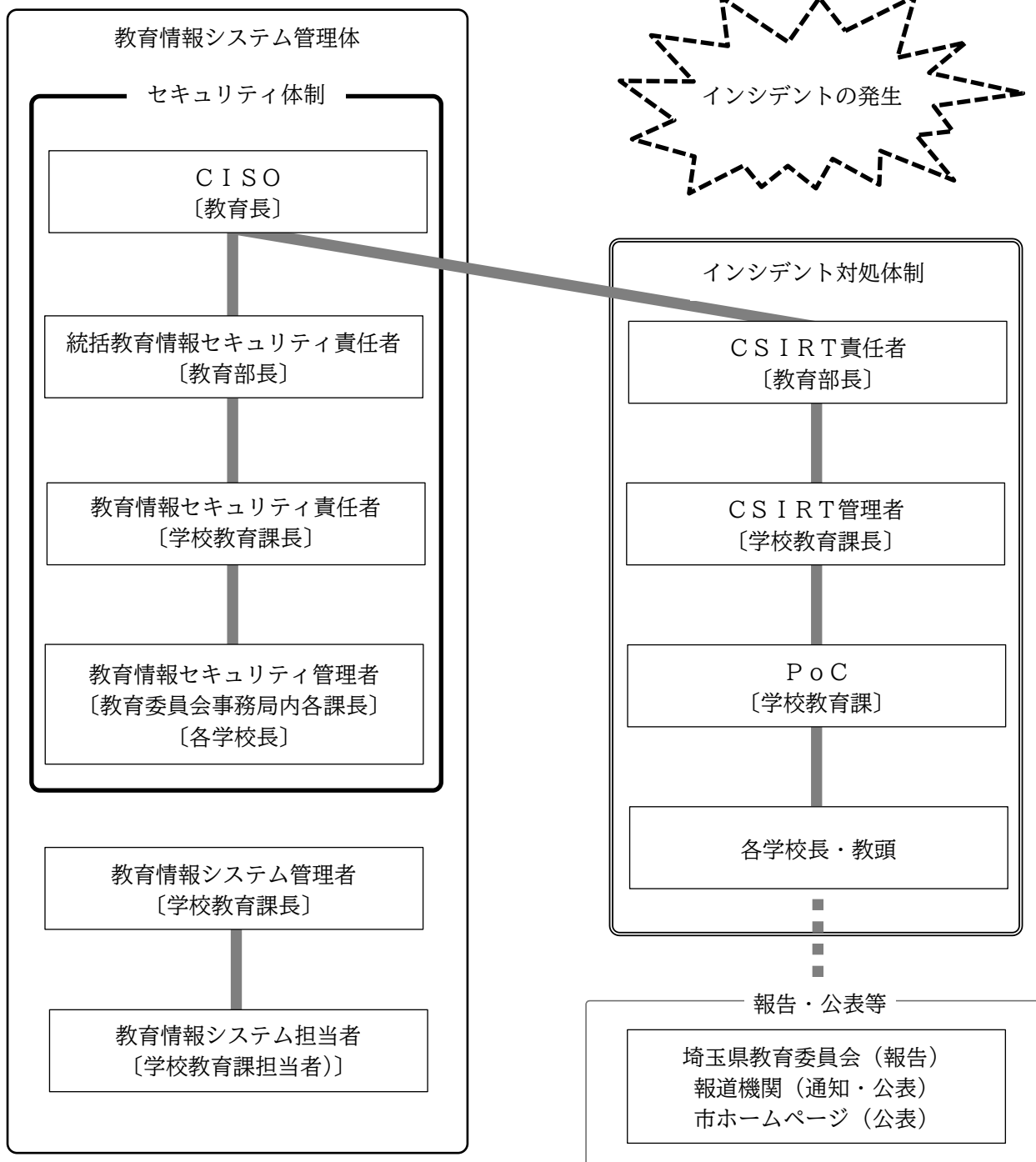
オ CISO による教育情報セキュリティ戦略の意思決定が行われた際には、その内容を各学校等に提供する。

カ 情報セキュリティインシデントを認知した場合には、CISO、埼玉県教育委員会へ報告すること。

キ 情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

ク 情報セキュリティに関して、関係機関等の PoC 機能を有する部署、外部の事業者等との情報共有を行うこと。

(2) 組織体制図



3 情報資産の分類と管理方法

(1) 情報資産の分類

本市の学校教育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、必要に応じて取扱制限を行うものとする。

【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がある情報で秘密文書に相当するもの
機密性 2 B	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 2 A	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 2 A、機密性 2 B 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	該当する情報のイメージ
完全性 2 B	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学校関係者の権利が侵害される又は学校事務及び教育活動の的確な遂行に支障（軽微なものを除く）を及ぼすおそれがある情報資産	情報が正確・完全な状態である必要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合、業務の遂行に支障ある情報
完全性 2 A	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学校関係者の権利が侵害される又は学校事務及び教育活動の的確な遂行に軽微な支障を及ぼすおそれがある情報資産	情報が正確・完全な状態である必要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合、業務の遂行に軽微な支障ある情報
完全性 1	完全性 2 A 又は完全性 2 B 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 2 B	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 2 A	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 2 A又は可用性 2 B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 分 類
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。 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。 IV 影響をほとんど及ぼさない。

(2) 情報資産の管理

① 管理責任

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

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

② 情報資産の分類の表示

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。

※情報資産の分類の表示先

ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅 等

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扱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。

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制限を定めなければならない。
- ウ 情報資産を入手した者は、その情報資産の分類が不明な場合、教育情報セキュリティ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、適切な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、電磁的記録媒体または保存されている領域（フォルダやサーバ）に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体または保存されている領域を取り扱わなければならない。

⑥ 情報資産の保管

- ア 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 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施されていることを確認しなければならない。
- 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、重要性分類Ⅲ以上（機密性2 A以上、完全性2 A以上又は可用性2 A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。

⑦ 情報の送信

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

- ア 電子メール等により重要性分類Ⅲ以上（機密性2 A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 教育情報セキュリティ管理者及び教育情報システム管理者は、電子メール等による外部送信の安全性を高めるため、添付される情報資産を監視する等、出口対策を実施しなければならない。

⑧ 情報資産の運搬

ア 車両等により重要性分類Ⅲ以上（機密性 2 A 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、暗号化又はパスワードの設定を行う等、情報資産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 重要性分類Ⅲ以上（機密性 2 A 以上）の情報資産を運搬する者は、教育情報セキュリティ管理者に許可を得なければならない。

⑨ 情報資産の提供・公表

ア 重要性分類Ⅲ以上（機密性 2 A 以上）の情報資産を外部に提供する者は、限定されたアクセスの措置を行わなければならない。

イ 重要性分類Ⅲ以上（機密性 2 A 以上）の情報資産を外部に提供する者は、教育情報セキュリティ管理者に許可を得なければならない。

ウ 教育情報セキュリティ管理者及び教育情報システム管理者は、保護者等に公開する情報資産について、完全性を確保しなければならない。

⑩ 情報資産の廃棄

ア 重要性分類Ⅲ以上（機密性 2 A 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、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。

4 物理的セキュリティ

(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 サーバの冗長化

ア 教育情報システム管理者は、校務系サーバその他の校務系情報を格納しているサーバを冗長化し、同一データを保持しなければならない。また、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。

イ 教育情報システム管理者は、学習系サーバその他の学習系情報を格納しているサーバのハードディスクを冗長化しなければならない。

③ 機器の電源

ア 教育情報システム管理者は、統括教育情報セキュリティ責任者及び施設管理部門と連携し、校務系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 教育情報システム管理者は、統括教育情報セキュリティ責任者及び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

ア 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、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 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、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 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切に管理しなければならない。

エ 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。

⑤ 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（可用性 2 A 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。

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、教育情報システム管理者は、外部の事業者修理に当たり、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。

⑥ 施設外又は学校外への機器の設置

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、施設外又は学校外にサーバ等の機器を設置する場合、CIS0 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。

⑦ 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、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。

(2) 管理区域（教育情報システム室等）の管理

① 管理区域の構造等

- ア 管理区域とは、教育ネットワークの基幹機器及び重要な教育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「教育情報システム室」という。）や電磁的記録媒体の保管庫をいう。
- イ 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、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。
- ウ 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、教育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。
- エ 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、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

- ア 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による入退室管理を行わなければならない。
- イ 市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。
- ウ 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た上で、管理区域への入退室を許可された市職員等が付き添うものとし、外見上市職員等と区別できる措置を講じなければならない。
- エ 教育情報システム管理者は、重要性分類Ⅱ以上（機密性2 B以上）の情報資産を扱う教育情報システムを設置している管理区域について、当該教育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。また、やむを得ず持ち込む必要がある場合は、事前に教育情報システム管理者の許可を得なければならない。

③ 機器等の搬入出

- ア 教育情報システム管理者は、搬入する機器等が、既存の教育情報システムに与える影響について、あらかじめ市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。
- イ 教育情報システム管理者は、教育情報システム室の機器等の搬入出について、市職員を立ち合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 統括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 統括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街頭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 統括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、必要に応じ、通信経路上での暗号化を行わなければならない。
- ④ 統括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 統括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。

(4) 教職員の利用する端末や電磁的記録媒体等の管理

(教職員の利用する端末について)

- 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 パスワードによる認証、加えて多要素認証の実施等、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 教育情報システム管理者は、校務系システム、パソコン等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するよう努めなければならない。特にアクセス制御による対策を講じたシステム構成の場合、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しなければならない。
- 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、特にアクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産を取り扱う端末に対し、当該ファイルの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、モバイル端末の学校外での業務利用の際は、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。
- ⑧ 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

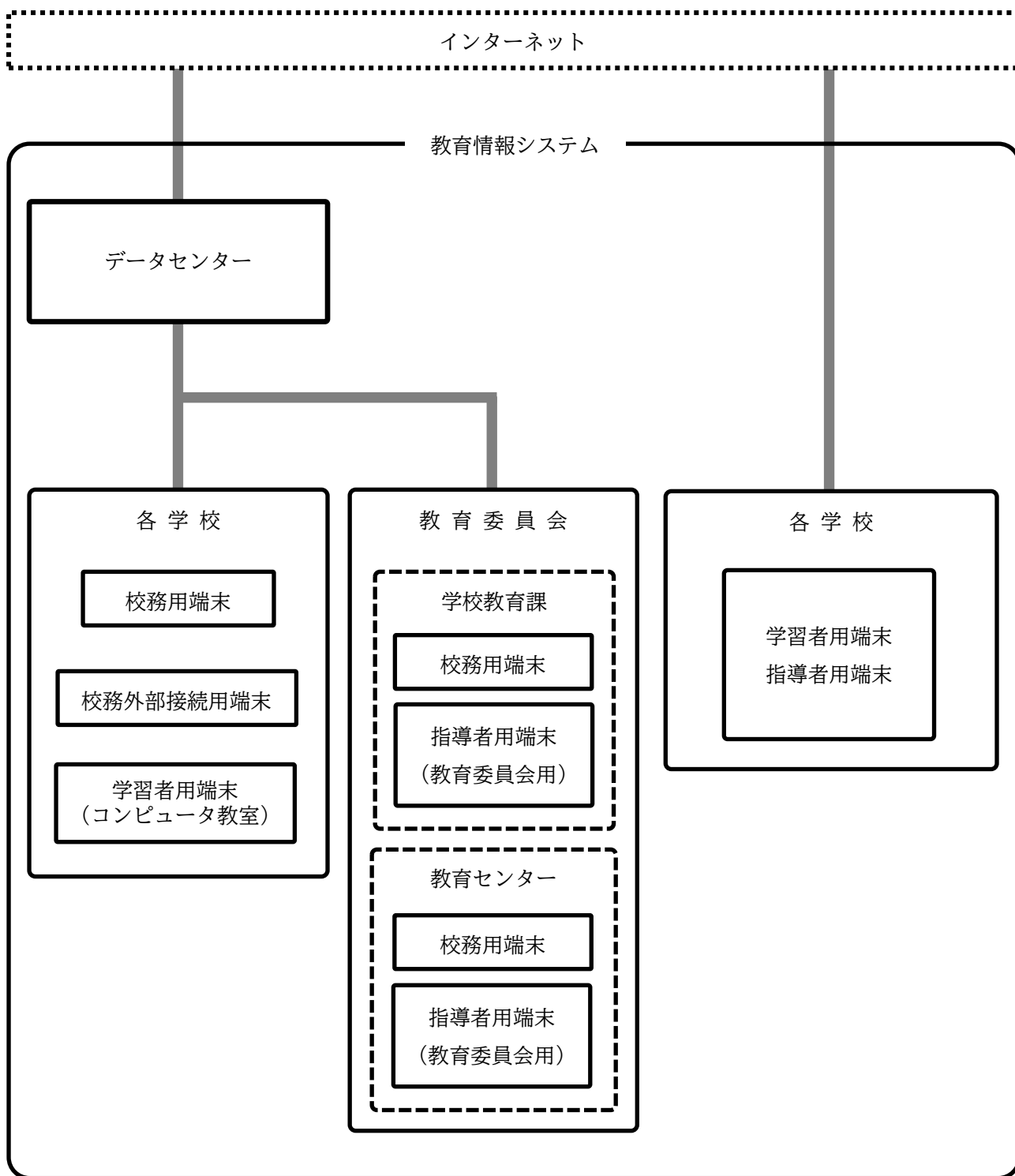
威に対し、ウイルス対策ソフトの導入等の対策を講じなければならない。なお、OSによっては標準的にウイルス対策ソフトを備えている製品、OSとしてウイルス感染のリスクが低い仕組みとなっている製品などもあるため、実際に運用する端末において適切な対策を講じなければならない。アクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産を取り扱う端末に対し、当該端末の状況および通信内容を監視し、異常、あるいは不審な挙動を検知する仕組み（ふるまい検知）等の活用を検討し、適切な対策を講じなければならない。

- ⑨ 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対策を講じなければならない。

（児童生徒の利用する端末について）

- ① 教育情報システム管理者は、盗難防止のため、教室等で利用するパソコン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、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。
- ③ 教育情報システム管理者は、教育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。

(5) 教育情報システム概略図



5 人的セキュリティ

(1) 教職員の遵守事項

① 教職員の遵守事項

ア 教育情報セキュリティポリシー等の遵守

教職員は、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、速やかに教育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。

イ 業務以外の目的での使用の禁止

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。

ウ モバイル端末や電磁的記録媒体等の持ち出し及び本市教育委員会・各学校が構築・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

(ア) CIS0 は、重要性分類Ⅱ以上の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

(イ) 教職員は、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、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。

(ウ) 教職員は、外部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。

エ 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

(ア) 教職員は、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。

(イ) 教職員は、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用いる場合には、教育情報セキュリティ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。

オ 持ち出し及び持ち込みの記録

教育情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。なお、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、情報セキュリティ管理者の包括的承認を行う等、運用実態や教職員の負担も考慮し検討しなければならない。

カ パソコンやモバイル端末におけるセキュリティ設定変更の禁止

教職員は、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教育情報セキュリティ管理者の許可なく変更してはならない。

キ 机上の端末等の管理

教職員は、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。

ク 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 教育情報セキュリティポリシー等の掲示

教育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及び実施手順を閲覧できるように掲示しなければならない。

③ 外部委託事業者に対する説明

教育情報システム管理者は、教育ネットワーク及び教育情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、教育情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

(2) 研修・訓練

① 教育情報セキュリティに関する研修・訓練

CISO は、定期的に教育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

ア CISO は、教職員に対する教育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、教育情報セキュリティ委員会の承認を得なければならない。

イ 研修計画において、教職員は、毎年度最低1回は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。

ウ 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。

③ 緊急時対応訓練

CISO は、緊急時対応を想定した訓練を定期的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

すべての教職員は、定められた研修・訓練に参加しなければならない。

(3) 情報セキュリティインシデントの報告

① 学校内等からの情報セキュリティインシデントの報告

ア 教職員は、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。

イ 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及び PoC に報告しなければならない。

ウ 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 CIS0 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 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

ア 教職員は、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。

イ 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。

ウ 教育情報セキュリティ管理者は、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 CIS0 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。

エ CIS0 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

ア CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

イ CSIRT は、情報セキュリティインシデントであると評価した場合、CIS0 に速やかに報告しなければならない。

ウ CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

エ CSIRT は、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の原因究明の結果から、再発防止策を検討し、CIS0 に報告しなければならない。

オ CIS0 は、CSIRT 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に必要な措置を指示しなければならない。

(4) ID及びパスワード等の管理

① IDの取扱い

教職員は、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。

ア 自己が利用している ID は、他人に利用させてはならない。

イ 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。

② パスワードの取扱い

教職員は、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。

ア 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。

イ 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。

ウ 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。

エ 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。

オ 複数の教育情報システムを扱う教職員は、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）。

カ 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。

キ 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。

ク 教職員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）

ケ 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。

コ 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するよう努めなければならない。

6 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管理

① 文書サーバの及び端末の設定等

ア 教育情報システム管理者は、教職員が使用できる文書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。

イ 教育情報システム管理者は、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。

ウ 教育情報システム管理者は、児童生徒等の個人情報、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、担当職員以外の教職員が閲覧及び使用できないようにしなければならない。

エ 教育情報システム管理者は、インターネット接続を前提とする校務外部接続系サーバ及び学習系サーバに保管する情報（学習系サーバにおいては、個人情報などを含む重要性が高い情報を保管する場合に限る）については、標的型攻撃等によるファイルの外部流出の可能性を考慮し、ファイル暗号化等による安全管理措置を講じなければならない。

② バックアップの実施

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、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、次のア及びイに基づきバックアップを実施するものとする。

ア 校務系情報及び校務外部接続系情報については、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。

イ 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。

③ 他団体との教育情報システムに関する情報等の交換

教育情報システム管理者は、他の団体と教育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、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の許可を得なければならない。

④ 教育情報システム管理記録及び作業の確認

ア 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。

イ 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、所管する教育情報システムにおいて、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。

ウ 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名以上で作業し、互いにその作業を確認しなければならない。

⑤ 教育情報システム仕様書等の管理

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、教育ネットワーク構成図、教育情報システム仕様書等について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失したりすることなどが無いよう、適切に管理しなければならない。

⑥ ログの取得等

ア 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、各種ログ及び学校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。

イ 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、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。

ウ 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、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

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。

⑧ ネットワークの接続制御、経路制御等

ア 統括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。

イ 統括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。

⑨ 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、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ教育ネットワーク及び教育情報システムを分離する等の措置を講じなければならない。

⑩ 外部ネットワークとの接続制限等

ア 教育情報システム管理者は、所管する教育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、CIS0 及び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。

イ 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、庁内及び学校のすべての教育ネットワーク、教育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。

ウ 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。

エ 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、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。

オ 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。

⑪ 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

ア 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

する、もしくはこれらに類する安全管理措置を講じなければならない。

イ 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。

⑫ 複合機のセキュリティ管理

ア 統括教育情報セキュリティ責任者は、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、適切なセキュリティ要件を策定しなければならない。

イ 統括教育情報セキュリティ責任者は、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。

ウ 統括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すべ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。

⑬ 特定用途機器のセキュリティ管理

統括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。

⑭ 無線 LAN 及びネットワークの盗聴対策

ア 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。

イ 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、暗号化等の措置を講じなければならない。

⑮ 電子メールのセキュリティ管理

ア 統括教育情報セキュリティ責任者は、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。

イ 統括教育情報セキュリティ責任者は、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。

ウ 統括教育情報セキュリティ責任者は、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。

エ 統括教育情報セキュリティ責任者は、教職員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に周知しなければならない。

オ 統括教育情報セキュリティ責任者は、システム開発や運用、保守等のため施設内に常駐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、外部委託事業者との間で利用方法を取り決めなければならない。

⑯ 電子メールの利用制限

- ア 教職員は、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。
- イ 教職員は、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。
- ウ 教職員は、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。
- エ 教職員は、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。
- オ 教職員は、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。

⑰ 電子署名・暗号化

- ア 教職員は、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、CISO 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。
- イ 教職員は、暗号化を行う場合に CISO が定める以外の方法を用いてはならない。また、CISO 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。
- ウ CISO は、電子署名の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。

⑱ 無許可ソフトウェアの導入等の禁止

- ア 教職員は、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。
- イ 教職員は、業務上の必要がある場合は、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管理者又は教育情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。
- ウ 教職員は、不正にコピーしたソフトウェアを利用してはならない。

⑲ 機器構成の変更の制限

- ア 教職員は、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。
- イ 教職員は、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、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の許可を得なければならない。

⑳ 無許可でのネットワーク接続の禁止

- ア 教職員は、統括学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。

㉑ 業務以外の目的でのウェブ閲覧の禁止

- ア 教職員は、業務以外の目的でウェブを閲覧してはならない。
- イ 統括教育情報セキュリティ責任者は、教職員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。

(2) アクセス制御

① アクセス制御等

ア アクセス制御

統括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、所管する教育ネットワーク又は教育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。特に、アクセス制御による対策を講じたシステム構成の場合、重要な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。

イ 利用者IDの取扱い

(ア) 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、統括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通知しなければならない。

(ウ) 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。

ウ 特権を付与されたIDの管理等

(ア) 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、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) 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の特権を代行する者は、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が指名し、CISOが認めた者でなければならない。

(ウ) CISOは、代行者を認めた場合、速やかに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及び教育情報システム管理者に通知しなければならない。

(エ) 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、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。

(オ) 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、特権を付与されたID及びパスワードについて、その利用期間に合わせて特権IDを作成・削除する、もしくは、入力回数制限を設ける等のセキュリティ機能を強化しなければならない。

(カ) 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、特権を付与されたIDを初期設定以外のもので変更しなければならない。

(キ) 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、特権を付与

されたIDのログ監視を行わなければならない。

② 外部からのアクセス等の制限

ア 教職員が外部から内部の教育ネットワーク又は教育情報システムにアクセスする場合は、統括教育情報セキュリティ責任者及び当該教育情報システムを管理する教育情報システム管理者の許可を得なければならない。

イ 統括教育情報セキュリティ責任者は、内部の教育ネットワーク又は教育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。

ウ 統括教育情報セキュリティ責任者は、組織外部からのシステムアクセスを認める場合、アクセスする利用者の本人確認、システムアクセスの対象となる児童生徒の本人（保護者）同意を得る等の措置を講じなければならない。

エ 統括教育情報セキュリティ責任者は、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。

オ 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。

カ 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施設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。

キ 統括教育情報セキュリティ責任者は、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及びパスワードによる認証に加えて、生体認証に係る情報等の認証情報及びこれを記録した媒体による認証や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

統括教育情報システム管理者及び教育情報システム管理者は、ネットワークで使われる機器について、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

教育情報システム管理者は、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 パスワードに関する情報の管理

ア 統括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。

イ 統括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、教職員に対し

てパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

⑥ 特権による接続時間の制限

教育情報システム管理者は、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。

(3) システム開発、導入、保守等

① 情報システムの調達

ア 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。

イ 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、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

ア 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。

イ 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い。

ウ 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

ア 開発環境と運用環境の分離及び移行手順の明確化

(ア) 教育情報システム管理者は、教育情報システム開発、保守及びテスト環境と教育情報システム運用環境を分離しなければならない。

(イ) 教育情報システム管理者は、教育情報システム開発・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、教育情報システム開発・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) 教育情報システム管理者は、移行の際、教育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し、移行に伴う教育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) 教育情報システム管理者は、導入する教育情報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。

イ テスト

(ア) 教育情報システム管理者は、新たに教育情報システムを導入する場合、既に稼働している教育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) 教育情報システム管理者は、開発した教育情報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。

(オ) 教育情報システム管理者は、運用環境への移行に先立ち、教育情報システムの脆弱性テストを行い、その結果を確認しなければならない。

④ 教育情報システム開発・保守に関連する資料等の整備・保管

ア 教育情報システム管理者は、教育情報システム開発・保守に関連する資料及び教育情報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。

イ 教育情報システム管理者は、テスト結果を一定期間保管しなければならない。

ウ 教育情報システム管理者は、教育情報システムに係るソースコードならびに使用したオープンソースのバージョン（リポジトリ）を適切な方法で保管しなければならない。

⑤ 教育情報システムにおける入出力データの正確性の確保

ア 教育情報システム管理者は、教育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教育情報システムを設計しなければならない。

イ 教育情報システム管理者は、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教育情報システムを設計しなければならない。

ウ 教育情報システム管理者は、教育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、出力されるように教育情報システムを設計しなければならない。

⑥ 教育情報システムの変更管理

教育情報システム管理者は、教育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、他の教育情報システムとの整合性を確認しなければならない。

⑧ 教育情報システム更新又は統合時の検証等

教育情報システム管理者は、教育情報システム更新・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。

(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

統括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。

ア 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、不正プログラムの教育情報システムへの侵入を防止しなければならない。

イ 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の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。

ウ 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、必要に応じ教職員に対して注意喚起しなければならない。

エ 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。

オ 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。

カ 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。

キ 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。

② 教育情報システム管理者の措置事項

教育情報システム管理者は、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。

ア 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。

イ 不正プログラム対策は、常に最新の状態に保たなければならない。

ウ 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。

③ 教職員の遵守事項

教職員は、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。

ア 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。

イ 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。

ウ 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。

エ 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実施しなければならない。

オ 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。

カ 統括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。

キ 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

統括教育情報セキュリティ責任者は、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かななければならない。

(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

統括教育情報セキュリティ責任者は、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。

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。

ウ 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、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へ通報するよう、設定しなければならない。

エ 重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

オ 統括教育情報セキュリティ責任者は、PoC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

CIS0及び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 記録の保存

CISO 及び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。

④ 内部からの攻撃

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所管するネットワークの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 教職員による不正アクセス

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、教職員による不正アクセスを発見した場合は、当該教職員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 サービス不能攻撃

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なければならない。

⑦ 標的型攻撃

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) 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

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、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

統括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

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。

7 運用

(1) 情報システムの監視

- 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、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 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、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 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、重要性分類Ⅱ以上の情報資産を格納する校務系システム及び校務外部接続系システムを常時監視しなければならない。

(2) 教育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

ア 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 CIS0 及び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。

イ CIS0 は、発生した問題について、適切かつ速やかに対処しなければならない。

ウ 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教育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

CIS0 及び CIS0 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 教職員の報告義務

ア 教職員は、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。

イ 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場合と統括教育情報セキュリティ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。

(3) 侵害時の対応等

① 緊急時対応計画の策定

CIS0 又は教育情報セキュリティ委員会は、情報セキュリティインシデント、教育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。

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

③ 業務継続計画との整合性確保

自然災害、大規模又は広範囲に及ぶ疾病等に備えて別途業務継続計画を策定し、本市教育委員会は当該計画と教育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

CISO 又は教育情報セキュリティ委員会は、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。

(4) 例外措置

① 例外措置の許可

教育情報セキュリティ管理者及び教育情報システム管理者は、教育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、CISO 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

教育情報セキュリティ管理者及び教育情報システム管理者は、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 CISO に報告しなければならない。

③ 例外措置の申請書の管理

CISO 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。

(5) 法令等遵守

教職員は、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等を遵守し、これに従わなければならない。

ア 地方公務員法(昭和25年法律第261号)

イ 教育公務員特例法(昭和24年法律第1号)

ウ 著作権法(昭和45年法律第48号)

エ 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)

- オ 個人情報の保護に関する法律（平成15年法律第57号）
- カ 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）
- キ サイバーセキュリティ基本法（平成26年法律第104号）
- ク 坂戸市個人情報保護条例（平成11年条例第14号）

（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法令による懲戒処分の対象とする。

② 違反時の対応

教職員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。

ア 統括教育情報セキュリティ責任者が違反を確認した場合は、統括教育情報セキュリティ責任者は当該教職員が所属する学校の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。

イ 教育情報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統括教育情報セキュリティ責任者及び当該教職員が所属する学校の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。

ウ 教育情報セキュリティ管理者の指導によっても改善されない場合、統括教育情報セキュリティ責任者は、当該教職員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、統括教育情報セキュリティ責任者は、教職員の権利を停止あるいは剥奪した旨を CIS0 及び当該教職員が所属する学校の教育情報セキュリティ管理者に通知しなければならない。

8 外部サービスの利用

（1）外部委託

① 外部委託事業者の選定基準

ア 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。

イ 教育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。

② 契約項目

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実施手順の遵守

- イ 外部委託事業者の責任者、委託内容、作業員、作業場所の特定
- ウ 提供されるサービスレベルの保証
- エ 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
- オ 外部委託事業者の従業員に対する教育の実施
- カ 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
- キ 業務上知り得た情報の守秘義務
- ク 再委託に関する制限事項の遵守
- ケ 委託業務終了時の情報資産の返還、廃棄等
- コ 委託業務の定期報告及び緊急時報告義務
- サ 市による監査、検査
- シ 市による情報セキュリティインシデント発生時の公表
- ス 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、その内容を統括教育情報セキュリティ責任者に報告するとともに、その重要度に応じて CIS0 に報告しなければならない。

9 クラウドサービスの利用

(1) 学校におけるクラウドサービスの利用

本市教育委員会（以下、クラウド利用者）がクラウドサービスを利用する際は、国際的な規格であるクラウドセキュリティ認証等の取得・準拠状況を確認することや、後述する対策（2）、（3）を適切に講じ、リスクを最小限に抑えることとする。

(2) 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 クラウド利用者は、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なければならない。

ウ クラウド利用者側管理者権限を有する者の ID 等の管理について、「6 技術的セキュリティ」（2）①ウに記載の事項を遵守しなければならない。

② アクセス制御

ア クラウド利用者は、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、サービス提供定款や契約書面上で確認または合意しなければならない。

イ クラウド利用者は、クラウド事業者の提供するアクセス制御機能を用いて、情報資産ごとに、許可されたエンドユーザ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

クラウド利用者は、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、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

クラウド利用者は、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、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 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、サービス提供定款や契約書面上で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 クラウド利用者は、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、合意のうえ、利用しなければならない。

イ クラウド利用者は、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、サービス提供定款や契約書面上で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

ア クラウド利用者は、当該クラウドサービスのサーバ等の管理条件を「4 物理的セキュリティ」（1）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なければならない。

イ クラウド利用者は、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、「4 物理的セキュリティ」（2）に準じた対策をクラウド

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 クラウド利用者は、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を確認し、合意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 クラウド利用者は、当該クラウドサービスにおけるサーバの冗長化について、「4 物理的セキュリティ」(1) ②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なければならない。

ウ クラウド利用者は、当該クラウドサービスにおけるデータバックアップについて、「6 技術的セキュリティ」(1) ②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なければならない。

エ クラウド利用者は、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、「6 技術的セキュリティ」(1) ⑥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対策

ア クラウド利用者は、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なければならない。

イ クラウド利用者は、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、サービス提供定款や契約書面上で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 クラウド利用者は、クラウドサービスにアクセスする利用者側端末について、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 クラウド利用者は、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、エンドユーザ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 クラウド利用者は、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、サービス提供定款や契約書面上で確認または合意しなければならない。

イ クラウド利用者は、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 等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なければならない。

ウ クラウド利用者は、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、サービス提供定款や契約書面上で確認または合意しなければならない。

エ クラウド利用者は、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、サービス提供定款や契約書面上で確認または合意しなければならない。

オ クラウド利用者は、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、サービス提供定款や契約書面上で確認または合意しなければならない。

⑫ データの破棄等について

ア クラウド利用者は、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なければならない。

イ クラウド利用者は、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サービス提供定款や契約書面上で確認または合意しなければならない。

(3) パブリッククラウド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

クラウド利用者は、クラウド事業者と契約時に守秘義務、目的外利用及び第三者への提供の禁止条項を締結しなければならない。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なければならない。契約には、当該条項に違反したクラウドサービス事業者に対する損害賠償規定を含める。

② 準拠する法令、情報セキュリティポリシー等の確認

クラウド利用者は、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なければならない。(クラウド事業者の準拠する認証制度、個人情報保護指針、プライバシーポリシー、情報セキュリティに関する基本方針及び対策基準、保守運用管理規程等)

③ クラウド事業者の管理体制

クラウド利用者は、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

意しなければならない。確認すべき項目例を下記に示す。

ア サービスの提供についての管理責任を有する責任者の設置

イ 情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者（システム管理者）の設置

ウ サービスの提供に係る情報システムの運用に関する事務を統括する責任者

④ クラウド事業者従業員への教育

ア クラウド利用者は、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、十分な知識とセキュリティ意識を醸成することを求めなければならない。

イ クラウド利用者は、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なければならない。

⑤ 情報セキュリティに関する役割の範囲、責任分界点

ア クラウド利用者は、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なければならない。

イ クラウド利用者は、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、合意しなければならない。

⑥ 監査

ア クラウド利用者は、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なければならない。

イ クラウド利用者は、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なければならない。

⑦ 情報インシデント管理及び対応フローの合意

ア クラウド利用者は、情報セキュリティインシデント管理に関する責任範囲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なければならない。

イ クラウド利用者は情報セキュリティインシデント管理に関する責任範囲及びインシデント対応フローを検証しなければならない。

⑧ クラウドサービスの提供水準及び品質保証

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、合意しなければならない。

⑨ クラウド事業者の再委託先等との合意事項

ア クラウド利用者は、クラウド事業者と合意したサービス履行内容及び情報セキュリティ対策について、クラウド事業者自らが実施する内容と、再委託先等に委託

する内容も含めて提示することをクラウド事業者に求めなければならない。また、サプライチェーンリスク対策が適切に講じられていることをクラウド事業者に求めなければならない。

イ クラウド利用者は、アの提示内容が、クラウド事業者と合意したサービス履行内容及び情報セキュリティ対策と整合していることを確認しなければならない。

⑩ その他留意事項

ア クラウド利用者は、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なければならない。

イ クラウド利用者は、クラウド事業者間でのデータ形成の互換性が必ずしも保証されている訳ではないことから、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なければならない。

ウ クラウド利用者は、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なければならない。

(4) 約款による外部サービスの利用

① 約款による外部サービスの利用に係る規定の整備

教育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、機密性の高い情報の取扱いには十分に留意する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続

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。

(5) ソーシャルメディアサービスの利用

① 教育情報システム管理者は、本市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続を定めなければならない。

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（機密性 2A 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。

10 1人1台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（帯域や同時接続数など）

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

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。

<対策例>

- ①フィルタリングソフト
- ②検索エンジンのセーフサーチ
- ③セーフブラウジング

③ マルウェア感染対策

学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

④ 端末を不正利用させないための防止策

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

⑤ セキュリティ設定の一元管理

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 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。

⑥ 端末の盗難・紛失時の情報漏洩対策

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、またはワイプ（データ消去）することで第三者による不正操作や情報漏洩を防ぐ等の安全管理措置を講じなければならない。

⑦ 運用・連絡体制の整備

本市教育委員会で学校内外での端末の統一の運用ルールを制定するとともに、インシデント時の連絡先や対応方法を各学校で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

① ID 登録・変更・削除

ア 入学/転入時の ID 登録処理

ID についてはシンプル・ユニーク（唯一無二）・パーマネント（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。

ID 登録やパスワードポリシーにおいては、情報セキュリティ対策として重要な要素であるため学校毎に管理するのではなく、本市教育委員会で一元的に管理しなければならない。

イ 進級/進学時の ID 関連情報の更新

ID については原則として進級/進学にも変更不要とすることが望ましい。ID を変えることなく ID の属性情報（進級時の組・出席番号、進学先学校名など）の更新を行っておくことで、モバイル端末管理による各種ポリシーや使用アプリケーションの変更を効率的に行うことが可能となる。

さらに、統合型校務支援システム等における児童生徒の氏名と連動した ID 管理を行うことで、校務側で管理している属性情報と一体となった ID を含んだマスター管理の一元化が望ましい。

ウ 転出/卒業/退学時の ID 削除処理

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

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。

ただし、本人同意や個人情報保護条例に従った適切な管理の下、一部のデータを活用することは可能である。

② 多要素認証によるなりすまし対策

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/パスワードに加えて多要素認証を設定することが望ましい。

③ 学習用ツールへのシングルサインオン

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

11 評価・見直し

(1) 監査

① 実施方法

CISO は、教育情報セキュリティ監査統括責任者を指名し、教育ネットワーク及び教育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、毎年度及び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

ア 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。

イ 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

ア 教育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、教育情報セキュリティ委員会の承認を得なければならない。

イ 被監査部門は、監査の実施に協力しなければならない。

④ 外部委託事業者に対する監査

外部委託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委託事業者から下請けとして受託している事業者も含めて、教育情報セキュリティポリシーの遵守について監査を定期的に又は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、教育情報セキュリティ委員会に報告する。

⑥ 保管

教育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切に保管しなければならない。

⑦ 監査結果への対応

CISO 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 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等への活用

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

ア 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、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

イ 教育情報セキュリティ責任者は、教育情報セキュリティ管理者と連携して、所管する部局における教育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、毎年度及び必要に応じて自己点検を行わなければならない。

② 報告

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及び教育情報セキュリ

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

ア 教職員は、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。

イ 教育情報セキュリティ委員会は、この点検結果を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、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

教育情報セキュリティ委員会は、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、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毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

【参考】資料編

1 策定・改訂記録

(1) 教育情報セキュリティ基本方針

決裁日	施行日	備考
令和4年11月1日	令和4年11月1日	策定

(2) 教育情報セキュリティ対策基準

決裁日	施行日	備考
令和4年11月1日	令和4年11月1日	策定

2 情報資産の分類と例示

情報資産の分類					情報資産の例示		
重要性分類	定義	機密性	完全性	可用性	持ち出しの禁止	持ち出しの制限	持ち出しの制限なし
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	<ul style="list-style-type: none"> ・指導要録原本 ・教職員の人事情報 ・入学者選抜問題 	<ul style="list-style-type: none"> ・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。	2 B	2 B	2 B	<ul style="list-style-type: none"> ○学籍関係 <ul style="list-style-type: none"> ・出席簿 ・卒業証書授与台帳 ・転退学受付（整理）簿 ・転入学受付（整理）簿 ・就学児童生徒異動報告書 ・休学・退学願等受付（整理）簿 ・教科用図書給付児童生徒名簿 ・要・準要保護児童生徒認定台帳 ・その他校内就学援助関係書類 ○成績関係 <ul style="list-style-type: none"> ・評定一覧表 ・進級・卒業認定資料 ・定期考査素点表 ・成績に関する個票等 ○指導関係 <ul style="list-style-type: none"> ・事故報告書・記録簿 ・生徒指導・特別指導等記録簿 ○進路関係 <ul style="list-style-type: none"> ・卒業生進路先一覧等 ・進路希望調査 ・進路判定会議資料 ・進路指導記録簿 ・入学者選抜に関する表簿（願書等） ○健康関係 <ul style="list-style-type: none"> ・健康診断に関する表簿 ・健康診断票 ・歯の検査表 ・心臓管理等医療情報 ・学校生活管理指導票 ○児童・生徒に関 	<ul style="list-style-type: none"> ○成績関係 <ul style="list-style-type: none"> ・通知表 ・定期考査・テスト等の答案用紙（児童・生徒が記入済のもの） ○指導関係 <ul style="list-style-type: none"> ・児童生徒等の個人写真・集合写真 ・指導カード（児童生徒等理解カード） ・教育相談・面接の記録・カード等 ・個別の教育支援計画（学校生活支援シート） ・個別指導計画 ・家庭訪問記録・個別面談記録 ・教務手帳 ・週ごとの指導計画（個人情報が含まれるもの） ○進路関係 <ul style="list-style-type: none"> ・調査書 ・推薦書 ・私立高校入試に係る事前相談資料 ・公立高校入学者選抜に係る成績一覧表 ○健康関係 <ul style="list-style-type: none"> ・児童生徒等健康調査票 ・児童生徒の健康保険等被保険者証の写し ○その他 <ul style="list-style-type: none"> ・給食関係書類 ○名簿等 <ul style="list-style-type: none"> ・児童生徒名簿 ・保護者緊急連絡網 ・児童生徒の住所録 ・座席表 ・PTA 会員名簿 	

					<p>する個人状報 (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、生別年月日、性別等の基本情報を含むもの)</p> <p>○学校教職員に関する個人情報 (病歴、心身の状況、収入等の情報、電話番号、メールアドレス、住所、氏名、生別年月日、性別等の基本情報を含むもの)</p> <p>○教職員に割り当てた機密性の高い情報 ・情報システムログインID/PW ・情報端末ログインID/PW</p>	<ul style="list-style-type: none"> ・職員緊急連絡網・職員住所録 ・委員会名簿 	
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		<ul style="list-style-type: none"> ○児童生徒の学習系情報 ・児童生徒の学習記録(ワークシート、レポート、作品等) ・学習活動の記録(動画・写真等) ○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 	
Ⅳ	影響をほとんど及ぼさない	1	1	1		<ul style="list-style-type: none"> ○学校運営関係 ・学校・学園要覧 ・学校紹介パンフレット ・使用教科書一覧 ・教育課程編成表 ・学校設定科目の届け出 ・特色紹介冊子原稿 ・学校徴収金会計簿(学年費、教育振興費等) ・学校行事実施計画(避難訓練・体育祭実施計画等) ・保護者等への配布文書文例 ・各種届雛形・校務分掌表 ・PTA資料 ・学校・学園・学年・学級だより ・学校・学園ホームページ掲載情 	

							報 ・学校行事のしおり ・授業用教材 ・教材研究資料 ・生徒用配布プリント(校務分掌名等で出すもの)
--	--	--	--	--	--	--	--