別冊2

生駒市教育情報セキュリティ対策基準

令和７年４月１日

生駒市教育委員会

目　次

この基準（以下「対策基準」という。）は、生駒市教育情報セキュリティ基本方針（令和７年４月１日施行。以下「基本方針」という。）９．教育情報セキュリティ対策基準の策定に基づき、生駒市教育委員会（以下「教育委員会」という。）における情報資産の取扱いについて遵守すべき事項及び情報セキュリティ対策の実施に関する統一的な基準を定めることにより、教育委員会が保有する情報資産を様々な脅威から守り、機密性、完全性、可用性を維持することを目的とする。

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行政機関等は、教育委員会及び学校（小学校、中学校を言う。以下同じ。）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、教育情報システム並びにこれらに関する設備及び電磁的記録媒体

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

（３）用語説明

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（公開系情報）	校務系情報のうち、保護者メールや学校ホームページ等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、校務系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
校務外部接続系システム	校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ（CMS）及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム
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、学習系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
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

教育長	最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。） ①CISO 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。 ②CISO 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。

教育部長	CISO 直属の統括教育情報セキュリティ責任者 ①統括教育情報セキュリティ責任者は CISO を補佐する。 ②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。 ③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。 ④教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者及び教育情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。 ⑤本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、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。 ⑥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情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。 ⑦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する。 ⑧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る。
教育総務課長	教育情報セキュリティ責任者 ①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。 ②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。 ③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、情報セキュリティポリシーの遵守に関する意見の集約及び教職員等（教職員、非常勤教職員及び臨時教職員をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。

校長	教育情報セキュリティ管理者 ①当該学校の情報セキュリティ対策に関する権限及び責任を有する。 ②当該学校において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、教育情報セキュリティ責任者、統括教育情報セキュリティ責任者及びCISO へ速やかに報告を行い、指示を仰ぐ。
教育指導課長	教育情報システム管理者 ①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。 ②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。 ③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。
教育委員会の情報システム担当課の課室職員	教育情報システム担当者 ①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。
情報セキュリティ委員会	本市の情報セキュリティ対策を統一的に行うため、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及びCISO が別途選任した者から構成される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。
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、同じ者が兼務しない。
情報セキュリティに関する統一的な窓口の設置	情報セキュリティに関して、生駒市CSIRT と協調して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。
教職員等	臨時的任用教職員、非常勤講師を含めた教職員全員 ①学校が所管する情報資産を取り扱う立場にあり、教育情報セキュリティ管理者の指導の下、情報セキュリティを遵守する。

教育委員会事務局職員	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 ①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責任者の指導の下、情報セキュリティを遵守する。

３．情報資産の分類と管理方法

３．１．情報資産の分類

（１）情報資産の分類

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

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）機密性による情報資産の分類

分類	分類基準	【該当する情報のイメージ】 ・分類に応じた取扱い
機密性 3	学校で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	【特定の教職員のみが知り得る状態を確保する必要のある情報で秘密文書に相当するもの】 ・機密性 3 の情報資産に対しては、支給以外の端末での作業の原則禁止とする。 ・業務以外の目的での利用を禁止する。 ・必要以上の複製及び配付を禁止する。 ・必要に応じ、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する。 ・保管場所への必要以上の電磁的記録媒体等の持ち込みを禁止する。 ・必要に応じ、情報の送信又は情報資産の運搬若しくは提供時に暗号化又はパスワード設定等する。 ・復元不可能な処理を施して廃棄する。

		・業務上必要な場合を除き、外部に持ち出さない。
機密性2B	学校で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	【教職員のみが知り得る状態を確保する必要がある情報資産（教職員のうち特定の教職員のみが知り得る状態を確保する必要があるものを含む）】 ・業務以外の目的での利用を禁止する。 ・必要以上の複製及び配付を禁止する。 ・必要に応じ、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する。 ・保管場所への必要以上の電磁的記録媒体等の持ち込みを禁止する。 ・必要に応じ、情報の送信又は情報資産の運搬若しくは提供時に暗号化又はパスワード設定等する。 ・復元不可能な処理を施して廃棄する。 ・業務上必要な場合を除き、外部に持ち出さない。
機密性2A	学校で取り扱う情報資産のうち、直ちに一般に公表することを前提としていないが、児童生徒がアクセスすることを想定している情報資産	【教職員及び児童生徒同士のみが知り得る状態を確保する必要がある情報資産（教職員及び児童生徒のうち特定の教職員及び児童生徒のみが知り得る状態を確保する必要があるものを含む）】 ・業務以外の目的での利用を禁止する。 ・必要以上の複製及び配付を禁止する。
機密性1	機密性2A、機密性2B又は機密性3の情報資産以外の情報資産	【公表されている情報資産又は公表することを前提として作成された情報資産（教職員及び児童生徒以外の者が知り得ても支障がないと認められるものを含む）】

（3） 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】 ・分類に応じた取扱い

完全性 2B	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適確な遂行に支障（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、業務の遂行に軽微な支障ある情報】 ・バックアップする。 ・業務上必要な場合を除き、外部に持ち出さない。 ・必要に応じ、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する。
完全性 2A	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	
完全性 1	完全性 2 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】

（４）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】 ・分類に応じた取扱い
可用性 2B	学校で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	【必要な時にいつでも利用できる必要があり、情報システムの障害等による滅失紛失や、情報システムの停止等があった場合、業務の安定的な遂行に支障がある情報】 ・バックアップする。 ・必要に応じ、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する。
可用性 2A	学校で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に支障を及ぼすおそれがある情報資産	
可用性 1	可用性 2 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】

※　重要性分類に基づく情報資産の例示は、別表のとおり

３．２．情報資産の管理

（１）管理責任

①CISO 又は統括教育情報セキュリティ責任者は、教育情報システムとその運用管理を定めた生駒市教育情報セキュリティ対策基準を策定する。

②統括教育情報セキュリティ責任者は、生駒市教育情報セキュリティ対策基準に基づき、学校現場での情報セキュリティ運用管理に関する実施手順を作成する。

③統括教育情報セキュリティ責任者は、学校で標準的に所管する情報資産について、分類を定義した標準情報資産台帳（以下「標準台帳」という。）を作成し、適宜更新する。

④教育情報セキュリティ管理者は、自校の所管する情報資産について管理責任を有する。

⑤教育情報セキュリティ管理者は、教職員等の情報資産の取扱いに際し、台帳及び実施手順に基づいた運用管理を指導する。

⑥教職員等は、台帳及び実施手順に基づき、適切に情報資産を取り扱う。

（２）情報資産の取扱い

①情報資産の分類の表示

教職員等は、情報資産について、必要に応じファイル（ファイル名、ヘッダー、フッター等)、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、取扱制限についても明示する等適正な管理を行う。

②情報の作成

(ア)教職員等は、業務上必要のない情報を作成してはならない。

(イ)情報を作成する教職員等は、情報の作成時に３．１の分類に基づき、当該情報の分類を定め、分類に準拠した取扱いを行う。

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

③情報資産の入手

(ア)本市教職員等以外の者が作成した情報資産を入手した教職員等は、３．１の分類に基づき、当該情報の分類を定め、分類に準拠した取扱いを行う。

(イ)情報資産を入手した教職員等は、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ぐ。

④情報資産の利用

(ア)情報資産を利用する教職員等は、業務以外の目的に情報資産を利用しな

い。

（イ）情報資産を利用する教職員等は、情報資産の分類に応じ、適切に取扱う。

（ウ）情報資産を利用する教職員等は、電磁的記録媒体又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又は保存されている領域を取り扱う。

（３）情報資産の保管

①教育情報セキュリティ管理者又は教育情報システム管理者の措置事項

（ア）教育情報セキュリティ管理者は、重要性分類に従って情報資産の保管先を定めるなど適正に保管し、教職員等に周知する。

（イ）教育情報セキュリティ管理者又は教育情報システム管理者は、情報資産を記録した USB メモリ等の外部電磁的記録媒体を保管する場合は、必要に応じて外部電磁的記録媒体への書込禁止の措置を講ずる。

（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以上の情報を記録した電磁的記録媒体を保管する場合、施錠可能な場所に保管する。

②教職員等の遵守事項

（ア）教職員等は、教育情報セキュリティ管理者が指定した保管先にのみ情報資産を保管する。

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

（４）情報資産の外部持ち出し

①分類に応じた情報資産の外部持ち出し制限

（ア）教職員等は、重要性分類Ⅱ以上の情報資産を外部持ち出しする場合は、限定されたアクセスの措置設定（アクセス制限や暗号化）を行い、教育情報セキュリティ管理者の許可を得る。また、必要に応じて持ち出し持ち帰りの記録をつける。なお、外部持ち出しツールに限定されたアクセスの措置設定（アクセス制限や暗号化）機能を有する場合には、有効にする。

（イ）重要性分類Ⅲの情報資産については、教職員等の外部持ち出しについて、教育情報セキュリティ管理者の判断で包括的許可を可とする。なお、外部持ち出しツールに限定されたアクセスの措置設定（アクセス制限や暗号化）機能を有する場合には、有効にする。

②電子メール、外部ストレージサービスによる情報の送信

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

（ア）電子メール、外部ストレージサービスにより重要性分類Ⅲ以上の情報を外部送信する者は、限定されたアクセスの措置設定（アクセス制限や暗号化）を行う。

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

③外部電磁的記録媒体を用いた情報の外部持ち出し

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

（ア）管理された外部電磁的記録媒体以外の使用禁止

教育委員会又は学校から支給された公的な媒体のみを利用する。

（イ）外部電磁的記録媒体の暗号化の徹底

暗号化機能つきの媒体を利用し、暗号化機能を活かす。

④FAX による情報の送信

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

⑤情報資産の運搬

（ア）車両等により重要性分類Ⅲ以上の情報資産を運搬する場合は、必要に応じ暗号化又はパスワードの設定を行う等の安全管理措置を講じ、宛名・差出名を明記して、厳重に封印する。

（イ）重要性分類Ⅲ以上の情報資産を運搬する教職員等は、教育情報セキュリティ管理者に許可を得る。

⑥情報資産の公表

（ア）教育情報セキュリティ管理者は、公開する情報が正しい内容であることを事前に確認し、誤公開を防ぐ。

（イ）教育情報セキュリティ管理者は、住民に公開する情報資産について、改ざんや消去されないように定期的に確認する。

（５）情報資産の廃棄

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

②情報を記録している電磁的記録媒体を利用しなくなった場合、情報を復元できないように処置した上で廃棄する。

③情報資産の廃棄・リース返却を行う教職員等は、教育情報セキュリティ管理者の許可を得たのち、行った処理について、日時、担当者及び処理内容を記録する。

④業者に廃棄委託する場合、廃棄する情報資産を業者が引き取る際、教職員等が立ち会う。

４．物理的セキュリティ

４．１．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、必要な措置を講ずる。

（２）サーバの冗長化

①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、同一データを保持する。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する。

②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する。

（３）機器の電源

①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る。

②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ずる。

（４）通信ケーブル等の配線

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、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ずる。

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、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、連携して対応する。

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、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する。

④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す。

（５）機器の定期保守及び修理

①教育情報システム管理者は、重要性分類Ⅲ以上（可用性 2A 以上）のサーバ等の機器の定期保守を実施する。

②教育情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせる。

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とともに秘密保持体制の確認等を行う。

（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、CISO の承認を得る。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する。

（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、全ての情報を消去の上、復元不可能な状態にする措置を講ずる。

４．２．管理区域（情報システム室等）の管理

（教育委員会等のサーバ室にサーバを設置している場合）

（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」という。）や電磁的記録媒体の保管庫をいう。

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、管理区域を地階又は 1 階に設けない。

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、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する。

④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、防水措置等を講じる。

⑤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

与えないようにする。

（２）管理区域の入退室管理等

①教育情報システム管理者は、管理区域への入退室を許可された者のみに制限し、IC カード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行う。

②地方公共団体職員等及び外部委託事業者が管理区域に入室する場合、これらの者に身分証明書等を携帯させ、必要に応じてその提示を求める。

③教育情報システム管理者は、外部からの訪問者が管理区域に入室する場合には、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地方公共団体職員等が付き添うものとし、外見上地方公共団体職員等と区別できる措置を講じる。

④教育情報システム管理者は、重要性分類Ⅱ以上（機密性 2B 以上）の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませない。

（３）機器等の搬入出

①教育情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ地方公共団体職員又は委託した業者に確認を行わせる。

②教育情報システム管理者は、情報システム室の機器等の搬入出について、地方公共団体職員を立ち会わせる。

４．３．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、適切に管理する。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する。

（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該当ポイントに接続される端末を正確に把握し、適切な管理を行う。

（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、適切な回線を選択する。また、必要に応じて通信経路上での暗号化を行う。

（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する。

（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する。

（６）統括教育情報セキュリティ責任者は、学校運営上必要なネットワーク帯域を確保するとともに、遅延等に対する適切な対策を講ずる。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す配慮を含めて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に改修計画を行う。

４．４．教職員等の利用する端末や電磁的記録媒体等の管理

（１）教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ずる。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する。

（２）教育情報システム管理者は、校務系システム、教育情報システムへアクセスする端末へのログインパスワード等の認証情報の入力を必要とするように設定する。

（３）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利用する。端末に暗号化機能を持つセキュリティチップが搭載されている場合、その機能を有効に活用する。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する。

（４）教育情報システム管理者は、特に強固なアクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産を取り扱う端末に対し、当該データ暗号化等の措置により、不正アクセスや教員の不注意等による情報流出への対策を講ずる。

（５）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ずる。

（６）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ずる。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ずる。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、校務情報等の重要な情報資産を取り扱う端末に対し、当該端末の状況及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、適切な対策を講ずる。

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

４．５．学習者用端末のセキュリティ対策

（１）不適切なウェブページの閲覧防止

教育情報システム管理者は、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ため、フィルタリングソフトや検索エンジンのセーフサーチ、セーフブラウジング等の対策を講ずる。

（２）マルウェア感染対策

教育情報システム管理者は、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ずる。

（３）端末を不正利用させないための防止策

教育情報システム管理者は、端末のセキュリティ状態の監視に加えて、不適切なアプリケーションやコンテンツの利用を制限し、常に安全で児童生徒が安心して利用できる状態を維持する。

（４）セキュリティ設定の一元管理

教育情報システム管理者は、端末のセキュリティ設定や OS アップデート、ウェブブラウザのアップデート、学習用ツールのインストール等の一元管理を行い、端末の利用履歴等の状態を確認する。

（５）端末の盗難・紛失時の情報漏洩対策

教育情報システム管理者は、端末の盗難・紛失時の第三者による不正操作や情報漏洩に備え、遠隔制御や遠隔消去等の安全管理措置を講ずる。

４．６．パソコン教室等における学習者用端末や電磁的記録媒体の管理

（１）教育情報システム管理者は、盗難防止のため、教室等で利用するパソコンの保管庫による管理等の物理的措置を講ずる。

（２）教育情報システム管理者は、パソコン及び電磁的記録媒体について、情報が保存される必要がなくなった時点で速やかに記録した情報を消去する。

（３）教育情報システム管理者は、情報システムへのアクセスにおけるログインパスワードの入力等による認証を設定する。

５．人的セキュリティ

５．１．教育情報セキュリティ管理者の措置事項

（１）情報資産の管理

①情報資産の持ち出し及び持ち込みの記録管理

教育情報セキュリティ管理者は、教職員等による情報資産の外部持ち出しについて、記録管理する。

②情報資産の廃棄管理

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

(イ)教育情報セキュリティ管理者は、廃棄した情報資産を記録管理する。

（２）教職員等の情報セキュリティ意識醸成

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

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

③情報セキュリティポリシー等の閲覧容易性確保

教育情報セキュリティ管理者は、教職員等が常に教育情報セキュリティポリシー及び実施手順を閲覧・確認できるように配慮する。

（３）端末等の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、保管する。

（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教育情報セキュリティ管理者は、新規採用教職員等及び他自治体から本市に新規赴任した教職員等、及び非常勤及び臨時の教職員に対し、教育情報セキュ

リティポリシー等遵守すべき内容を理解・浸透するように指導を行う。
②教育情報セキュリティ管理者は、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。

（５）新規ソフトウェア及びコンテンツの導入・利用判断

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

（６）インターネット接続及び電子メール利用の制限

①教育情報セキュリティ管理者は、教職員等に業務端末による作業を行わせる場合において、業務以外でのインターネット接続及び電子メールの利用をしないよう教職員等に指導する。なお、ウェブフィルタリングの設定について、教職員等から相談があった場合は、教育情報システム管理者に上申して、判断を仰ぐ。
②教育情報セキュリティ管理者は、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できる。

（７）情報資産を取り扱う執務室の管理

教育情報セキュリティ管理者は、教職員等と協力して管理する。
①来校者の氏名等を記録する。
②来校者には名札の着用等により、第三者であることが識別できるようにする。
③地域住民、保護者などに校内施設を開放する場合、情報資産を取り扱う執務室へは入室できないよう制限を設ける。

（８）自己点検の実施

教育情報セキュリティ管理者は、年１回、学校の自己点検を行い、その結果を必要に応じて情報セキュリティ委員会に報告する。

５．２．教職員等の遵守事項

教職員等は、教育情報セキュリティ管理者の指導の下、次の事項を遵守する。

（１）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する。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、指示を仰ぐ。

（２）執務上での管理

教職員等は、執務に際しては、次の事項を遵守する。

①執務室の施錠管理

情報資産を取り扱う執務室にて教職員等が不在となる場合には、執務室を施錠する。

②来校者への対応

来校者を情報資産を取り扱う執務室に入室させる場合には、教育情報セキュリティ管理者又は教育情報セキュリティ担当者の許可を求める。

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、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、適切な措置を講ずる。

（３）支給端末の取扱い

教職員等は、支給端末の取扱いについては、次の事項を遵守する。

①教職員等は、業務目的以外で支給端末を利用しない。

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せず、業務上必要な場合は、事前に教育情報セキュリティ管理者の許可を得る。

③教職員等は、支給端末の利用において、セキュリティ機能に関する設定変更やメモリ増設等の改造をしない。

④教職員等は、支給端末の盗難・紛失等に注意する。

⑤教職員等は、支給端末から離席する時は、端末をロックするなど、他者が閲覧できないようにする。

（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

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業務に利用しない。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た上で安全に配慮して利用する。

（５）支給端末や電磁的記録媒体等の持ち出し及び教育委員会・学校が構築・管理している環境の外部で情報処理業務を行う場合の取扱い

教職員等が、支給端末、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や、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る。

（６）ID の取扱い

教職員等は、自己の管理する ID に関し、次の事項を遵守する。

①自己が利用しているIDは、他人に利用させない。
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、教育情報システム管理者に通知する。

（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、次の事項を遵守する。
①パスワードは、他者に知られないように管理する。
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する。
④パスワードが流出したおそれがある場合には、教育情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更する。
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ない。
⑥初期パスワードは、最初のログイン時点で変更する。
⑦教職員等間でパスワードを共有しない。ただし、共有IDに対するパスワードは除く。
⑧共有IDに対するパスワードは、必要に応じて定期的に又はアクセス回数に基づいて変更する。

（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、次の事項を遵守する。
①認証に用いるICカード等を、教職員等間で共有しない。
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く。
③ICカード等を紛失した場合には、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に通報し、指示に従う。

（９）外部電磁的記録媒体の取扱い

教職員等は、外部電磁的記録媒体の取扱いに関し、次の事項を遵守する。
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ものを使用する。
②外部電磁的記録媒体は、職員室の書庫等に施錠保管する。

（１０）電子メールの取扱い

教職員等は、電子メールの取扱いに関し、次の事項を遵守する。
①自動転送機能を用いて、電子メールを転送しない。
②業務上必要のない送信先に電子メールを送信しない。

③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する。
④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する。
⑤ウェブで利用できるフリーメールサービス等を教育情報システム管理者の許可なく使用しない。
⑥情報ファイルを添付する場合には、必要に応じてパスワード設定等の対策を講ずる。
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する。
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にアクセスしない。

（１１）クラウドサービス、ソーシャルメディアサービスの取扱い

教職員等は、クラウドサービス、ソーシャルメディアサービスの取扱いに関し、次の事項を遵守する。
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わない。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ない。ただし、業務上必要な場合は教育情報システム管理者の許可を得て利用する。
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、次の事項を遵守する。
①支給端末において、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ない。また、OS 及び不正プログラム対策ソフトウェアが常に最新の状態に保てるようにする。
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う。
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、速やかに削除する。
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する。
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う。
⑥教育情報システム管理者が提供するウイルス情報を、常に確認する。
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、直ちに教育情報セキュリティ管理者に報告し、指示を仰ぎ、以下の

対応を行う。

（ア）有線 LAN につながる端末の場合は、LAN ケーブルの即時取り外しを行い、指示があるまでは、端末の電源は切らずに保持する。

（イ）無線 LAN につながる端末の場合は、直ちに利用を中止し、通信を行わない設定への変更を行い、指示があるまでは、端末の電源は切らずに保持する。

（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、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、送信する。

②教職員等は、暗号化を行う場合に CISO が定める以外の方法を用いない。また、CISO が定めた方法で暗号のための鍵を管理する。

③CISO 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する。

（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ない。

②教職員等は、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する。

③教職員等は、不正にコピーしたソフトウェアを利用しない。

（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・交換を行わない。

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、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る。

（１６）無許可でのネットワーク接続の禁止

教職員等は、統括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、教育情報セキュリティ管理者を介して、統括教育情報セキュリティ責任者及び当該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る。
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する。

（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う。

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。

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。

③ウイルス対策ソフトウェアの管理
ウイルス対策ソフトウェアは常に最新の状態に保つ。

④セキュリティ機能の設定
利用する端末のセキュリティ機能の設定を、学校の許可なく変更しない。

⑤学習系情報の保管
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する。

⑥外部ソフトウェアのインストール
無断で外部ソフトウェアをインストールしない。

⑦コミュニケーションツールの利用
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。

⑧ウイルス感染が疑われる場合の報告
学習者用端末が動かない、勝手に操作されている、いつもと異なる画面や警告が表示されるなどの症状が発生した場合、直ちに教職員等に報告する。

⑨端末の取り扱い
学習者用端末は取り扱いに注意し、盗難・紛失・破損等が発生した場合は直ちに教職員等に報告する。

⑩私物端末の利用
私物端末など、承認されていない端末を学校のネットワークに接続しない。

（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、返却する。また、

その後も業務上知り得た情報を漏洩しない。

５．３．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責任者の指導の下、以下の規定を遵守する。

（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）知り得た情報の秘匿

（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すべて返却する。また、その後も業務上知り得た情報を漏洩しない。

５．４．研修・訓練

（１）情報セキュリティに関する研修・訓練

CISOは、定期的に情報セキュリティに関する研修及び訓練を実施する。

（２）研修計画の策定及び実施

①CISO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、情報セキュリティ委員会の承認を得る。

②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する。

③研修は、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム担当者及びその他教職員等に対して、それぞれの役割に応じた内容にする。

④CISOは、必要に応じて、情報セキュリティ委員会に対して、教職員等の情報セキュリティ研修の実施状況について報告する。

（３）緊急時対応訓練

CISOは、緊急時対応を想定した訓練を必要に応じて実施する。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する。

（４）研修・訓練への参加

教職員等は、定められた研修及び訓練に参加する。

５．５．情報セキュリティインシデントの連絡体制の整備

（１）学校内からの情報セキュリティインシデントの報告

①教職員等は、情報セキュリティインシデントを認知した場合、直ちに教育情報セキュリティ管理者に報告する。

②報告を受けた教育情報セキュリティ管理者は、直ちに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する。

③教育情報セキュリティ責任者は、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CISO及び統括教育情報セキュリティ責任者に報告する。

（２）教育情報セキュリティポリシーに対する違反行為の報告

①教職員等は、教育情報セキュリティポリシーに対する違反行為を発見した場合、直ちに教育情報セキュリティ責任者に報告を行う。

②教育情報セキュリティ責任者は、報告のあった違反行為について、必要に応じて統括教育情報セキュリティ責任者に報告する。

③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する。

（３）住民等外部からの情報セキュリティインシデントの報告

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

②報告を受けた教育情報セキュリティ管理者は、直ちに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する。

③教育情報セキュリティ責任者は、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CISO及び統括教育情報セキュリティ責任者に報告する。

（４）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統括教育情報セキュリティ責任者は、情報セキュリティインシデントについて、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、記録を保存する。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、CISOに報告する。

②CISOは、統括教育情報セキュリティ責任者から、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に必要な措置を指示する。

（５）支給端末の運用・連絡体制の整備

学校内外での支給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、実施手順に反映する。

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設定管理

（１）ファイルサーバ及び端末の設定等

①教育情報システム管理者は、教職員等が使用できるファイルサーバの容量を設定し、教職員等に周知する。

②教育情報システム管理者は、ファイル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する。

③教育情報システム管理者は、住民の個人情報、人事記録等、特定の教職員等しか取扱えないデータについて、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等が閲覧及び使用できないようにする。

④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ずる。

（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、必要に応じて定期的にバックアップを実施する。

（３）ログの取得等

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、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、一定の期間保存する。

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、ログとして取得する項目、保存期間及び取扱方法等について定め、適切にログを管理する。

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、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する。

（４）ネットワークの接続制御、経路制御等

①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する。
②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す。

（５）外部の者が利用できるシステムの分離等

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

（６）外部ネットワークとの接続制限等

①教育情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO 及び統括教育情報セキュリティ責任者の許可を得る。
②教育情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内及び学校の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認する。
③教育情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理事業者との契約において、契約上その事業者が負う損害賠償責任の内容と範囲を担保する。
④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する。
⑤教育情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括教育情報セキュリティ責任者の判断に従い、直ちに当該外部ネットワークを物理的に遮断する。

（７）重要性が高い情報に対するインターネットを介した外部からのリスク、児童生徒による重要性が高い情報へのアクセスリスクへの対応

①教育情報システム管理者は、強固なアクセス制御による対策を講じたシステム構成については、各システムにおけるアクセス権管理の徹底をする。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については、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。

②教育情報システム管理者は、校務系システムとその他のシステム（校務外部接続系システム、学習系システム）との間で通信する場合には、各システムにおけるアクセス権管理の徹底を行う等の適切な措置を図る。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、適切な措置を図る。

（８）複合機のセキュリティ管理

①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する。

②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ずる。

③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ずる。

（９）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する。

（１０）無線 LAN 及びネットワークの盗聴対策

①統括教育情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な通信経路の暗号化及び認証技術の使用を義務付ける。

②統括教育情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、通信経路の暗号化等の措置を講ずる。

（１１）電子メールのセキュリティ管理

①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う。

②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する。
③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する。
④統括教育情報セキュリティ責任者は、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する。
⑤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る。

６．２．アクセス制御

（１）アクセス制御等

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、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員等がアクセスできないように、システム上制限する。特に強固なアクセス制御による対策を講じたシステム構成の場合、重要な情報資産へのアクセスについては、多要素認証等のアクセスの真正性に関する要素技術を取り入れることで、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。

（２）外部からのアクセス等の制限

①統括教育情報セキュリティ責任者は、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する。
②統括教育情報セキュリティ責任者は、民間事業者等の外部組織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ずる。
③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通信経路の暗号化等の措置を講ずる。
④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等に貸与する場合、モバイル端末管理（MDM）の導入等を通じて、セキュリティ確保のために必要な措置を講ずる。
⑤統括教育情報セキュリティ責任者は、外部から教育ネットワークに接続することを許可する場合は、利用者の ID 及びパスワード、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（IC カード等）による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ずる。

（３）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等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する。

（４）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する。

６．３．システム開発、導入、保守等

（１）情報システムの調達

①統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システム開発、導入、保守等の調達に際しては、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する。

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、機器及びソフトウェアの調達に際しては、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する。

（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する。また、必要に応じてシステム開発のための方針や手順等を確立する。

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 を削除する。

(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する。

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する。

(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する。

（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)教育情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離する。

(イ)教育情報システム管理者は、システム開発・保守及びテスト環境からシ

ステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にする。

(ウ)教育情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮する。

(エ)教育情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入する。

②テスト

(ア)教育情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行う。

(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う。

(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ない。

(エ)教育情報システム管理者は、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う。

(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、システムの脆弱性テストを行い、その結果を確認する。

（４）システム開発・保守に関連する資料等の整備・保管

①教育情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適切に整備・保管する。

②教育情報システム管理者は、テスト結果を一定期間保管する。

③教育情報システム管理者は、情報システムに係るソースコード並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する。

（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する。

②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情報システムを設計する。

③教育情報システム管理者は、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する。

（６）情報システムの変更管理

教育情報システム管理者は、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する。

（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、他の情報システムとの整合性を確認する。

（８）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、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う。

６．４．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、次の事項を措置する。

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

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

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する。

④所管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る。

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、常に最新の状態を維持する。

⑥不正プログラム対策のソフトウェアは、常に最新の状態を維持する。

⑦開発元のサポートが終了したソフトウェアは、業務で利用しない。

（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、次の事項を措置する。

①教育情報システム管理者は、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ずる。

②不正プログラム対策は、常に最新の状態を維持する。

③市が管理している電磁的記録媒体以外の利用を禁止する。

６．５．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、以下の事項を措置する。

①使用されていないポート及びSSID（無線LANネットワーク名）を閉鎖する。

②不要なサービスについて、機能を削除又は停止する。

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の対策を講ずる。

④統括教育情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築する。

（２）攻撃の予告

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ずる。また、関係機関と連絡を密にして情報の収集に努める。

（３）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ずる。

（４）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、研修等の人的対策や入口対策を講ずる。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ずる。

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、必要に応じて関係者間で共有する。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する。

（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、必要に応じて、教職員等に対応方法等を周知する。

（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、必要に応じて関係者間で共有する。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る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ずる。

７．運用

７．１．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する。特に強固なアクセス制御による対策を講じたシステム構成の場合、重要な情報資産へのアクセスについては、侵入検知システム（IDS）や侵入防御システム（IPS）等の対策を講ずる。

（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ずる。

（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する。

（４）内部からの攻撃監視

統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等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する。

７．２．ドキュメントの管理

（１）システム管理記録及び作業の確認

①教育情報システム管理者は、所管する教育情報システムの運用において実施した作業について、作業記録を作成する。

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、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理する。

③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、必要に応じて 2 名以上で作業し、互いにその作業を確認する。

（２）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、ネットワーク構成図、情報システム仕様書等について、記録媒体に関わらず、業務上必要とする者以外の閲覧や紛失等がないよう適切に管理する。

（３）障害記録の管理

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、教職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存する。

（４）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た場合には攻撃の記録を保存し、さらに被害が疑われる場合は警察及び関係機関との緊密な連携に努める。

７．３．教職員等の ID 及びパスワードの管理

（１）利用者 ID の取扱い

①統括教育情報セキュリティ責任者及び教育情報システム管理者は、利用者の登録、変更、抹消等の情報管理、教職員等の異動、出向、退職者に伴う利用者 ID を適切に取り扱う。

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、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、点検する。

（２）パスワードに関する情報の管理

①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、教職員等のパスワードに関する情報を厳重に管理する。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、これを有効に活用する。

②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、教職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させる。

７．４．IC カード等の取扱い

（１）IC カード等の取扱い

①統括教育情報セキュリティ責任者及び教育情報システム管理者は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止する。

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、IC カード等を切り替える場合、切替え前のカードを回収し、IC カードを所管する部門に返却する。

７．５．児童生徒における ID 及びパスワード等の管理

（１）ID 登録・変更・削除

①入学・転入時の ID 登録処理

ID については唯一無二性や、永続的な識別などの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ずる。ID 登録は教育情報システム管理者が一元管理する。

②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。

③転出・卒業・退学時の ID 削除処理

転出・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、必要に応じて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を完全削除する。

（２）多要素認証によるなりすまし対策

児童生徒の ID 及びパスワードに加えて、必要に応じて多要素認証を設定する。

（３）学習用ツールへのシングルサインオン

一度の認証により各種サービスにアクセスが行えるシングルサインオンを必要に応じて導入する。

７．６．特権を付与された ID の管理等

（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、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する。

（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 が認めた者とする。

（３）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する。

（４）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、許可なく外部委託事業者に行わせない。

（５）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・削除し、又は、入力回数制限を設ける等のセキュリティ機能を強化する。

（６）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に変更する。

（７）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 を必要に応じてログ監視する。

７．７．教育情報セキュリティポリシーの遵守状況の確認・管理

（１）遵守状況の確認及び対処

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

②CISO は、発生した問題について、適切かつ速やかに対処する。

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、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切かつ速やかに対処する。

（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

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

（３）業務以外の目的でのウェブ閲覧の禁止

統括教育情報セキュリティ責任者は、教職員等のウェブ利用について、明ら

かに業務に関係のないサイトを閲覧していることを発見した場合は、教育情報セキュリティ管理者に通知し適切な措置を求める。

（４）教職員等による不正アクセスの管理

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、教職員等による不正アクセスを発見した場合は、当該教職員等が所属する学校等の教育情報セキュリティ管理者に通知し、適切な処置を求める。

７．８．専門家の支援体制等

（１）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く。

（２）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、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る。

７．９．侵害時の対応等

（１）緊急時対応計画の策定

CISO 又は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、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する。

（２）緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定める。

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、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

合性を確保する。

（４）緊急時対応計画の見直し

CISO 又は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す。

７．１０．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、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 に報告する。

（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する。

７．１１．法令等遵守

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等を遵守し、これに従う。

７．１２．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、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る。

①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等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、適切な措置を求める。

②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等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、適切な措置を求める。

③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、統括教育情報セキュリティ責任者は、教職員等の権利を停止あるいは剥奪した旨を CISO 及び当該教職員等が所属する学校の教育情報セキュリティ管理者に通知する。

８．外部委託

（１）外部委託事業者の選定基準

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

②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、事業者を選定する

（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する。

・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
・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

づき措置する。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CISOに報告する。

（４）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、ネットワーク及び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、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する。

９．SaaS型パブリッククラウドサービスの利用

この章内容はすべて「SaaS型パブリッククラウドサービス利用実施手順書」とした。

以下、目次のみ記載する。

９．１．SaaS型パブリッククラウドサービスの利用における情報セキュリティ対策

（１）利用者認証
（２）アクセス制御
（３）クラウドに保管するデータの暗号化
（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
（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
（６）情報の通信経路のセキュリティ確保
（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
（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
（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
（１０）クラウド利用者側のセキュリティ確保
（１１）クラウド事業者従業員の人的セキュリティ対策
（１２）サービス終了時等のデータの廃棄及び利用者アカウント抹消について
（１３）クラウドサービス要件基準を満たす配慮を含めたネットワーク設計

９．２．SaaS型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
（２）準拠する法令、情報セキュリティポリシー等の確認
（３）クラウド事業者の管理体制
（４）クラウド事業者従業員への教育
（５）情報セキュリティに関する役割の範囲、責任分界点
（６）監査
（７）情報インシデント管理及び対応フローの合意

（８）クラウドサービスの提供水準及び品質保証
（９）クラウド事業者の再委託先等との合意事項
（１０）その他留意事項

９．３．SaaS 型パブリッククラウドサービス利用における教職員等の留意点
（１）ID・パスワード等の秘匿
（２）モバイル端末持ち歩きリスク
（３）重要性分類に基づく情報管理
（４）学校外からのパブリッククラウド利用
（５）SaaS 型パブリッククラウドサービスの学習用途、校務用途混在リスクへの対応

９．４．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
（２）約款による外部サービスの利用における対策の実施

９．５．ソーシャルメディアサービスの利用

１０．評価・見直し
１０．１．監査
（１）実施方法
CISO は、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、必要に応じて監査を行う。

（２）監査を行う者の要件
①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、監査の実施を依頼する。
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とする。

（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る。
②被監査部門は、監査の実施に協力する。

（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、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必要に応じて行う。

（５）報告

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切に保管する。

（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する。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る。

（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

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する。

１０．２．自己点検

（１）実施方法

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、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する。

②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、必要に応じて自己点検を行う。

（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、情報セキュリティ委員会に報告する。

（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る。

②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する。

１０．３．教育情報セキュリティポリシー及び関係規程等の見直し

（１）情報セキュリティ委員会は、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ふまえ、情報セキュリティポリシー及び関係規程等について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。

（別紙）

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	校務系	学習系	公開系
Ⅰ	セキュリテイ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	2B	2B	・指導要録原本 ・教職員の人事情報 ・入学者選抜問題 ・教育情報システム仕様書		
Ⅱ	セキュリテイ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（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 ・通知表 ・評定一覧表 ・進級・卒業認定資料 ・定期監査・テスト等の答案用紙 （児童・生徒が記入済のもの） ・定期考査素点表 ・成績に関する個票等 ○指導関係 ・事故報告書・記録簿 ・生徒指導・特別指導等記録簿 ・児童・生徒等の個人写真・集合写真 ・指導記録・指導カード （児童・生徒等理解カード等） ・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 ・調査書 ・推薦書 ・公立高校入学者選抜に係る成績一覧表 ・入学者選抜に関する表簿（願書等） ・私立高校入試に係る事前相談資料 ・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、生年月日、性別等の基本情報を含むもの） ○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、生年月日、性別等の基本情報を含むもの） ○健康関係 ・健康診断表 ・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・生徒等健康調査票 ・児童・生徒の健康保険等被保険者証の写 ・健康診断に関する表簿 ・就学時健康診断票 ○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管理台帳 ・情報端末ログインID／PW管理台帳 ○その他 ・給食関係書類・寄宿関係資料 ○名簿等 ・児童生徒名簿 ・保護者緊急連絡網 ・児童生徒の住所録 ・PTA会員名簿 ・職員緊急連絡網・職員住所録 ・委員会名簿 ・PTA役員連絡網 ○各種帳票ファイル ・指導要録作成システム等、データの入っていない帳票		
Ⅲ	セキュリテイ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 ・座席表 ・児童生徒委員会名簿	○学校運営関係 ・授業用教材 ・教材研究資料 ・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、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）	
Ⅳ	影響をほとんど及ぼさない。	1	1	1			○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 ・学園・学校・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 ○学校活動の記録 ※保護者の承諾がある場合、以下は公開可能 ・学校行事等の児童・生徒の写真 ・学習活動の記録 （動画・写真・作品等）