議第 43 号
令和 6 年 6 月 27 日

熊本市立学校情報セキュリティ対策基準の改定について

熊本市立学校情報セキュリティ対策基準を別紙のとおり改定したいので議決を求める。

熊本市教育長　遠藤　洋路

（提出理由）

現在、GIGA スクール構想のもと、本市でも児童生徒の 1 人 1 台端末、1 人 1 アカウント、教育用クラウドの環境が整備され、各学校で活用が進んでいる。教職員や児童生徒が安心して ICT を活用するために、熊本市立学校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講じているところである。

しかし、学校での ICT 利用が本格化し、児童生徒の学び方や教職員の働き方を取り巻く環境が急速に変化しており、変化に合わせた熊本市立学校情報セキュリティ対策基準の改定が困難な状況にある。

この変化に柔軟に対応するため、熊本市立学校情報セキュリティ対策基準を改定するまでの間の暫定的な取扱いについて、教育 CISO に権限と責任を与える必要がある。

よって、熊本市教育委員会教育長事務委任等規則（昭和２７年教育委員会規則第 6 号）第 2 条の規定に基づき、教育委員会の議決を求めるものである。

これが、この議案を提出する理由である。

1 改定の趣旨

現在、本市立学校においては、児童生徒の 1 人 1 台端末、1 人 1 アカウント、教育用クラウドアプリ環境が整備され、学校での ICT 利用が本格化するにあたって、教職員及び児童生徒が安心して ICT を活用するために、不正アクセスや盗難・紛失の防止等、情報資産の保護に向けた情報セキュリティ対策を講じている。

一方、児童生徒の学び方や、教職員の働き方を取り巻く環境が急速に変化しており、情報セキュリティ対策基準に適合させつつ、常に変化している環境に合わせた運用をすることが困難となっている。

この変化に柔軟に対応するため、熊本市立学校情報セキュリティ対策基準を改定するまでの間の暫定的な取扱いについて、教育 CISO に権限と責任を与える必要があり、熊本市立学校情報セキュリティ対策基準を改定する次第である。

2 改定内容について

【熊本市立学校情報セキュリティ対策基準 第 10 章】

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

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、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。教育 CISO は、見直しまでの間の暫定的な運用を行う権限及び責任を有する。ただし、教育CISOは、次の教育委員会会議において、これを報告しなければならない。

【熊本市立学校情報セキュリティ対策基準 制定日、施行日、附則の追加】

令和 5 年 12 月 28 日 制定（令和 6 年 6 月28日 施行）

附則

令和 5 年 12 月 28 日 制定

令和 6 年 4 月 1 日 施行

令和 6 年 6 月28日 施行

熊本市立学校情報セキュリティ対策基準

令和　5 年 12 月 28 日　制定

（令和　6 年　6 月 28 日　施行）

熊本市教育委員会

目次

第１章　総則

１－１　目的

本市立学校においては、児童生徒の 1 人 1 台端末、1 人 1 アカウント、教育用クラウドアプリ環境が整備され、教職員及び児童生徒が日常的にクラウドサービスを利用している。

そのため、熊本市情報セキュリティ基本方針（以「基本方針」という。）にもとづき、熊本市立学校情報セキュリティ対策基準（以下「対策基準」という。）を策定し、教育情報セキュリティを確保し、適切に運用管理することを目的とする。

１－２　対象

対策基準の対象は、次の範囲とする。なお、それ以外の情報システム等および情報資産は、熊本市情報セキュリティ対策基準に則るものとする。

（１）行政機関の範囲

市立小学校、市立中学校、市立高等学校、市立総合ビジネス専門学校、市立特別支援学校、市立幼稚園（「以下「学校」という。）及び教育委員会事務局とする。

（２）対象とする情報システム

① 行政機関に所属する職員が利用する校務系システム

② 行政機関に所属する職員及び児童生徒が利用する学習系システム

（３）対象とする情報資産

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ネットワーク図等のシステム関連文書

本基準で用いる用語の定義は以下のとおり

第１表　用語の定義

用語	定義
教育情報セキュリティポリシー	熊本市情報セキュリティ基本方針及び本対策基準をいう。
教職員	臨時的任用職員、会計年度任用職員を含めた学校に勤務するすべての者をいう。
執務室	校長室、職員室、事務室、保健室など教職員が校務事務する部屋をいう。
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、教職員の個人情報など、学校が保有する情報資産のうち、それら情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報。
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、作品等、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、かつ当該情報に教職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。なお、教育活動を目的に、児童生徒のワークシート、作品などに教職員が指導コメント等を付記した場合も学習系情報と見なす。
端末	パソコン、タブレット端末、モバイル端末等のコンピュータ及びそれに付随する装置をいう。
校務用端末	校務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、教職員が利用可能な端末。
業務端末	教職員が利用する校務用端末及び指導者用端末の総称。
教育ネットワーク	熊本市教育委員会事務局及び熊本市立学校を相互に接続するための通信網とその構成機器（ハードウェア及びソフトウェア）、学習者用端末及び指導者用端末がインターネットに接続するためのモバイル通信サービスをいう。
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。校務系システムでは、インターネットから遮断された校務支援システムとインターネットに接続可能な校務外部接続システムの 2 種に分類される。校務外部接続システムのサーバは、校内サーバとクラウドサービス利用の 2 種に分類される。
学習系システム	学習系ネットワーク、学習系サーバ、学習系クラウド、学習者用端末及び指導者用端末等から構成される学習系情報を取り扱うシステム。
教育情報システム	校務系システムと学習系システムの総称。
教育情報システム基盤	校務系システムでは、校務用端末、校内のネットワークで構成され、学習系システムでは、指導者用端末及び学習者用端末、モバイルネットワークで構成される。
個別サービス	教育情報システム基盤上に、個別サービス提供を目的にサーバ導入やクラウドサービスを利用する形態を指す。個別サービスの提供主管は、教育情報システム基盤を提供する主管（教育情報システム管理者の所属組織）とは異なる部局になる。
クラウド（クラウドサービス）	利用者が自前でサーバを構築する形ではなく、同等の機能・性能をインターネット上のサービスとして利用する形態。ネットワークを経由してデータやアプリケーションを提供するサービス全般をいう。
校務系クラウド	校務目的でコンテンツ、アプリケーションを提供するパブリッククラウドサービス。
学習系クラウド	学習目的でコンテンツ、アプリケーションを提供するパブリッククラウドサービス。
SaaS	・Software as a Service の略で、ソフトウェア（アプリケーション、コンテンツ）をインターネットを通じて遠隔から利用者に提供する方式をいう。
マルウェア	不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアや悪質なコードの総称。コンピュータウイルスなどが含まれる。
電磁的記録媒体	情報を記録可能な電磁的記録媒体を指す。サーバ等の固定式なものと、USB メモリ等の外部記録媒体に大別される。

外部記録媒体	持ち出し可能な磁的記録媒体。USB メモリ、SD カード、外付けハードディスクドライブ、DVD-R、磁気テープ等をいう。
約款による外部サービス	インターネット上に約款を掲示し、同意した利用者に対して簡易なアカウントの登録により情報処理機能を提供するサービス。SaaS 型パブリッククラウドサービスの一種であるが、個別契約締結型クラウドサービスとは別種。利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものは含まない。代表例は、電子メール、ファイルストレージ、ファイル転送サービスなど。

１－３　組織体制

学校情報セキュリティ対策実現のため、以下の体制と所掌事項を定める（第１図および第２図参照）。

（１）教育最高情報セキュリティ責任者（以下「教育 CISO」という。）

① 教育長を、教育 CISO とする。教育 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。

② 教育 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。

③ 教育 CISO 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、教育情報システム管理者、教育情報システム担当者及び学校情報セキュリティ管理者、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。

④ 教育 CISO は、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、必要かつ十分な措置を行う権限及び責任を有する。

⑤ 教育 CISO は、本市の教育ネットワーク、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。

（２）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、教育委員会事務局教育次長が担う。

② 統括教育情報セキュリティ責任者は、熊本市立学校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し、教育 CISO を補佐する。

③ 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教育 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、教育情報システム管理者、教育情報システム担当者、学校情報セキュリティ管理者を網羅する連絡体制を含めた緊急連絡網を整備する。

④ 統括教育情報セキュリティ責任者は、緊急時には教育 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。

（３）教育情報セキュリティ責任者

① 教育情報セキュリティ責任者は、教育委員会事務局教育センター所長が担う。

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ポリシーの遵守について監督し、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）教育情報システム管理者

① 教育情報システム管理者は、教育情報システムを所管する組織の長*が担う。

② 教育情報システム管理者は、教育情報システムにおける情報セキュリティ管理に関する権限及び責任を有する。

③ 教育情報システム管理者は、教育情報システムに関する情報セキュリティの維持・管理を行う。

④ 教育情報システム管理者は、教育情報セキュリティ責任者と連携して、情報セキュリティの確保に努める。

（＊教育センターが所管する教育情報システム（校務系及び学習系システム）については、教育センター所長が担う。これ以外に、独立した別システムを導入している場合は、導入元の組織の長が担う）

（５）教育情報システム担当者

① 教育情報システム担当者は、教育センター教育情報班職員及び教育情報システムを所管する組織の担当者が担う。

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

③ 教育情報システム担当者は、情報セキュリティ事故の疑い等について学校からの報告受付を担い、すみやかに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に報告する。（教育センターが所掌する教育情報システム以外についても学校からの窓口機能を担う。）

（６）学校情報セキュリティ管理者

① 学校情報セキュリティ管理者は、各学校の校長が担う。

② 学校情報セキュリティ管理者は当該学校の情報セキュリティ全般に関する権限及び責任を有する。

③ 学校情報セキュリティ管理者の所掌業務は、次に掲げる事項とする。

ア 学校における情報セキュリティ対策の整備、運用及び管理等

イ 教育情報セキュリティポリシーの遵守に関し、基本方針、対策基準及び同実施手順についての校内周知を行い、情報セキュリティの維持・向上に努める。

ウ 情報セキュリティ事故発生時の情報収集、教育情報システム管理者への報告及び対応。

（７）学校情報セキュリティ担当者

学校情報セキュリティ担当者は、学校情報セキュリティ管理者及び教育情報システム管理者の指示に従い、学校における教育情報システムの作業を担当する者である。校長が校務分掌する教職員及び教頭の2名が担う。

（８）教育情報セキュリティ監査統括責任者

① 本市の代表監査委員を教育情報セキュリティ監査統括責任者とする。

② 教育情報セキュリティ監査統括責任者は、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う。

（９）教職員

① 臨時的任用職員、会計年度任用職員を含めた学校に勤務するすべての者をいう。

② 教職員は学校の情報資産を取り扱う立場にあり、学校情報セキュリティ管理者の指導の下、教育情報セキュリティポリシーを順守する義務を負う。

③ 教職員のうち、児童生徒の指導を行う者は、児童生徒に対して情報モラル（セキュリティを含む）教育を行う。

（10）個別サービス導入責任者

① 個別サービス導入責任者は、教育センターが所管する教育情報システム基盤上に、独自にサーバを構築・運用（クラウドサービス利用を含む）して個別サービスを提供する者である。

② 個別サービスを提供するために、サーバ又はクラウドサービスを教育センターが所管する教育情報システム基盤に接続する場合には、教育 CISO の許可が必要になる。

（11）教育委員会事務局職員

① 教育ネットワークを利用して、学校で取り扱う情報資産にアクセスできる教育委員会事務局職員を指す。

② 教育委員会事務局職員は学校の情報資産にアクセスできる立場にあり、学校情報セキュリティ責任者の指導の下、教育情報セキュリティポリシーを順守する義務を負う。

（12）教育情報セキュリティ委員会

① 本市の教育情報セキュリティ対策を統一的に行うため、教育情報セキュリティ委員会（以下「委員会」という。）において、教育情報セキュリティに関する重要な事項を検討する。なお、委員会で検討した内容は教育委員会会議で決定するものとする。

② 委員会において、次に掲げる事項を検討する。

ア 教育情報セキュリティに関する教育及び訓練に関すること

イ 対策基準に関すること

ウ 学校のICT利用状況及び情報セキュリティ対策状況の確認に関すること

エ 教育情報セキュリティに関する重要な事項

③ 委員会の構成員は、教育 CISO、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、教育情報システム担当者及び必要に応じて情報セキュリティに精通した外部の有識者を加える。

④ 定期的及び必要に応じて、教育 CISO が構成員を招集し、開催する。

（13）教育情報セキュリティに関する統一的な窓口の設置（教育 CSIRT）

① 教育情報セキュリティインシデントに関する統一的な窓口として、教育情報セキュリティ責任者に「教育 CSIRT」を設置する。

② 教育情報セキュリティインシデントが発覚した際には、関連部門と協力して、教育情報セキュリティインシデントを正確に把握・分析し、被害の最小化、原因究明、再発防止策実施の指揮を担う。

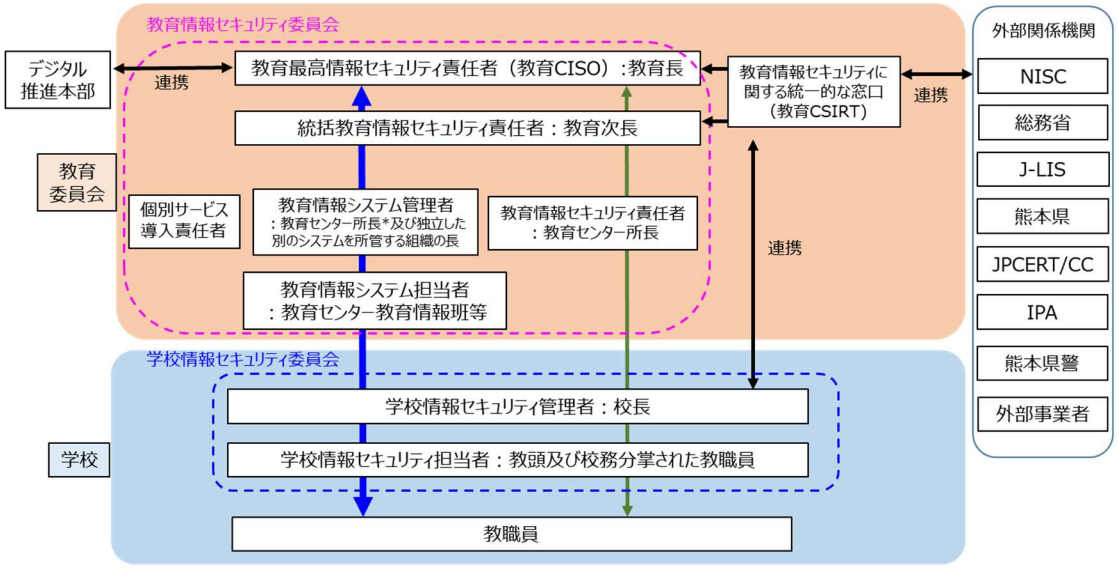
③ 教育情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行う。

④ 教育情報セキュリティに関して、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。

（14）学校情報セキュリティ委員会

学校情報セキュリティ委員会は、校内の情報セキュリティレベルの維持、意識向上、情報セキュリティポリシーの周知徹底を目的に組織する。

本委員会は、学校情報セキュリティ管理者を委員長とし、学校情報セキュリティ担当者等が委員となり、原則として前期1回、後期1回（年2回）開催する。



＊教育センターが所管する校務系システム及び学習系システム以外の情報システムについては、該当システムを所管する組織の長が情報システム管理者を担う

第１図　熊本市教育情報セキュリティ管理体制

第２章　情報資産

２－１　情報資産の分類

（１）分類の基準

下記の重要性分類に従って、学校で取り扱うすべての情報を分類する。

・ 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。

（機密性３、完全性２B、可用性２B に相当する）

・ 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。

（機密性２B、完全性２B、可用性２B に相当する）

・ 重要性分類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。

（機密性２A、完全性２A、可用性２A に相当する）

・ 重要性分類Ⅳ：影響をほとんど及ぼさない。

（機密性１、完全性１、可用性１に相当する）

ただし、「重要性分類Ⅱ以下」とは、重要性分類Ⅱ、Ⅲ、Ⅳを指す。また、「重要性分類Ⅱ以上」とは、重要性分類Ⅱ、Ⅰを指す。

（２）標準資産台帳の作成

教育委員会事務局は、熊本市立学校で取り扱う標準的な情報資産を分類整理し、熊本市立学校標準情報資産台帳（以下「標準資産台帳」という）を作成し、必要に応じて更新する。

（３）学校毎の資産台帳の作成

学校情報セキュリティ管理者は、標準資産台帳に基づき、学校で取り扱う情報を網羅した資産台帳（以下「資産台帳」という）を作成し、適宜更新する。

２－２　情報資産の管理

（１）管理責任

① 学校情報セキュリティ管理者は、所管する学校の情報資産について管理責任を有する。

② 学校情報セキュリティ管理者は、教育委員会事務局が提示する実施手順ひな形に基づき、各校の学校情報セキュリティ対策手順を作成する。

③ 学校情報セキュリティ管理者は、教職員の情報の取扱いに際し、各校で制定した資産台帳及び実施手順に基づいた管理を行う。

④ 教職員は、各校で制定した資産台帳及び実施手順に基づき、適切に情報資産を取り扱う。なお、取扱いで許可制のものについては、学校情報セキュリティ管理者の許可を必要とする。

（２）情報資産の分類表示

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など適切な管理を行う。

※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

① 教職員は、業務上必要のない情報を作成しない。

② 情報を作成する者は、各校で制定した資産台帳及び実施手順に基づいて取り扱う。

③ 情報を作成する者は、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・流失等を防止する必要がある。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。

（４）情報資産の入手

① 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。

② 教職員以外の者が作成した情報資産を入手した者は、２－１（１）の分類に基づき取り扱う。

③ 情報資産を入手した者は、入手した情報資産の分類が不明な場合、学校情報セキュリティ管理者に判断を仰ぐ。

（５）情報資産の取扱い

① 情報資産を取り扱う者は、業務以外の目的で情報資産を利用してはならない。

② 教職員は、情報資産の漏えいを防ぐために、各校で制定した資産台帳及び実施手順に基づいて取り扱う。

③ 情報資産を取り扱う者は、情報資産の分類が異なる情報が取り扱う書類や電磁的記録媒体に複数記録されている場合、より上位の分類に従って、当該書類や電磁的記録媒体を取り扱う。

④ 児童生徒の機微情報を取り扱う者は、情報の入手・取扱い・当該児童生徒への情報伝達において、他者への漏えいが発生しないよう行動する。

（６）情報資産の記録・複製

① 資産台帳において校務系システムでの保管が規定されている情報を、校務系システム以外の情報システムに記録・保管しない。

② 資産台帳において複製が禁じられている情報資産について、複製が必要な場合は、事前に学校情報セキュリティ管理者の許可を得る。また複製枚数は必要な部数のみとする。

（７）情報資産の保管

① 学校情報セキュリティ管理者は、資産台帳に従って、情報資産の保管先を定め、教職員に周知する。

② 学校情報セキュリティ管理者は、情報資産を記録したUSBメモリ等の外部記録媒体を保管する場合は、書き込み禁止の措置を講じる。

③ 教職員は、学校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。

④ 教職員は、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。

⑤ クラウドサービスに保管する情報は、重要性分類Ⅲ以下とする。

（８）情報資産の外部持ち出し

① 教職員が、持ち出しを禁止するものを除く重要性分類Ⅱ以上の情報資産を外部持ち出しする場合は、暗号化またはパスワード設定を行い、学校情報セキュリティ管理者の個別許可を得る。また、持ち出し持ち帰りの記録をつける。

② 重要性分類Ⅲの情報資産については、教職員の外部持ち出しについて、学校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。外部持ち出しツールに暗号化やパスワード設定機能を有する場合には有効にする。

（９）情報の送信

① 電子メールにより重要性分類Ⅲ以上の情報を外部送信する場合は、暗号化又はパスワード設定を行う。

② 情報をFAXにて送信する場合は、相手がFAX受信を指定してきた場合にのみ送信する。

（10）情報資産の搬送

① 車両等により重要性分類Ⅲ以上の情報資産を搬送する場合は、宛名・差出名を明記して、破損が生じない梱包を施す。

② 重要性分類Ⅲ以上の情報資産を運搬する場合は、学校情報セキュリティ管理者に許可を得て、記録する。

（11）情報資産の公表

① 学校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、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。

② 情報資産を外部に公開する者は、公開する情報（重要性分類Ⅲ以上）が正しい内容であることを確認し、誤公開を防ぐ。

（12）情報資産の廃棄

① 情報資産の廃棄を行う者は、学校情報セキュリティ管理者の許可を得る。

② 紙媒体の廃棄

情報資産を廃棄する者は、重要性分類Ⅲ以上の情報が記載された書類を廃棄する場合に細断、熔解またはこれに準ずる方法にて廃棄する。

③ 電磁的記録媒体の廃棄

ア 学校で実施する場合

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、情報を復元できないように破壊処置を行う。確実な履行を確認し、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。

イ 業務委託する場合

（ア）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、電磁的記録媒体の設置場所において、情報を復元できないようにデータ消去を行い、確実な履行を確認する。

（イ）情報資産を破棄する者は、電磁的記録媒体の破壊処理を行う委託事業者に完了証明書（写真添付）を提出させる。

（ウ）情報資産を廃棄する者は、完了証明書（提出期限を指定）により、確実な履行を確認し、記録を残す。

第２表 情報資産の例示

情報資産の分類		情報資産の例示
重要性分類	定義	
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。	<学籍関係> ○指導要録原本　○教職員の人事情報　○卒業証書授与台帳　○要・準要保護児童生徒認定台帳 ○校内就学援助関係書類 <成績関係> ○評定一覧表　○進級・卒業認定資料 <指導関係> ○生徒指導記録簿　○教育相談・面接の記録等　○個別の教育支援計画　○個別指導計画　○人権レポート ○きずなアンケート（児童生徒が記入済のもの）　○心のアンケート（児童生徒が記入済のもの） <進路関係> ○調査書　○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） <児童生徒に関する個人情報> ○生活歴、心身の状況、電話番号、メールアドレス、住所等の基本情報を含むもの <学校教職員に関する個人情報> ○生活歴、心身の状況、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> ○健康診断票　○歯の検査表　○学校生活管理指導表　○就学時健康診断票 <名簿等> ○出席簿　○児童生徒の住所録　○職員緊急連絡網　○職員住所録
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。	<学籍関係 > ○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・退学願等受付簿　○教科用図書給付児童生徒名簿 <成績関係> ○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） ○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　○家庭訪問記録　○教務手帳 <進路関係> ○卒業生進路先一覧等　○進路希望調査 <教職員に割り当てた情報> ○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> ○出勤簿　○体温チェック表　○給食関係書類　○入学者選抜問題　○教育情報システム仕様書
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	<児童生徒の氏名> ○名列表　○座席表　○委員会・係名簿　○部活動名簿　○出席簿補助簿 <児童生徒に関する個人情報> ○生年月日、性別 <学校運営関係> ○学校経営案　○職員会議の資料　○授業用教材　○教材研究資料 ○過去のテスト問題　○確認テスト　○卒業アルバム <児童生徒の活動の記録等> ○学習記録（ワークシート・レポート・作品等） ○授業や学校行事等の活動記録（動画・写真）
Ⅳ	影響をほとんど及ぼさない	<学校運営関係> ○学校要覧　○学校紹介パンフレット　○使用教科書一覧　○教育課程編成表　○記入前のアンケート ○学校設定科目の届け出　○学校徴収金会計簿（学年費等） ○学校行事実施計画（体育大会実施計画等）　○保護者等への配布文書　○各種届雛形 ○校務分掌表　○学校・学年・学級だより　○学校行事のしおり <児童生徒の活動の記録等>（公開に対して、保護者の承諾がある場合） ○学習記録（ワークシート・レポート・作品等） ○授業や学校行事等の活動記録（動画・写真）

第３表　情報資産の管理一覧

<table>
<tr><td colspan="2" rowspan="2">情報資産の管理</td><td colspan="3">重要性分類</td></tr>
<tr><td>Ⅰ・Ⅱ</td><td>Ⅲ</td><td>Ⅳ</td></tr>
<tr><td rowspan="5">取扱い（情報資産の作成・利用）</td><td>取扱い者制限</td><td>・業務上必要な教職員のみが取り扱える（児童生徒の閲覧禁止）</td><td>学習系情報：児童生徒と教職員が取り扱える
校務系情報：教職員のみが取り扱える（児童生徒の閲覧禁止）</td><td>－</td></tr>
<tr><td>取扱い場所の制限</td><td>原則、執務室</td><td>校務系情報は原則、学校内</td><td>－</td></tr>
<tr><td>取扱い管理</td><td>本人以外に見られない・盗まれない・他人に伝えない</td><td>関係者以外に見られない・盗まれない・他人に伝えない</td><td>－</td></tr>
<tr><td>児童生徒の機微情報（テスト結果、通知表等）</td><td>情報入手・取扱い・当該児童生徒への伝達において、他者に漏えいしないようにする</td><td>－</td><td>－</td></tr>
<tr><td>机上への置き去り</td><td colspan="2">禁止</td><td>－</td></tr>
<tr><td colspan="2">複製・配布</td><td>個別許可が必要</td><td colspan="2">－</td></tr>
<tr><td rowspan="8">外部持ち出し</td><td>外部持ち出しの許可</td><td colspan="2">個別許可が必要</td><td>－</td></tr>
<tr><td>外部電子メール</td><td colspan="2">パスワード設定を行う</td><td>－</td></tr>
<tr><td>郵送・宅配による輸送（外部記録媒体）</td><td colspan="2">パスワード設定を行う</td><td>－</td></tr>
<tr><td>郵送・宅配による輸送（紙媒体）</td><td colspan="2">宛名、差出名を明記し、破損が生じない梱包を施す。</td><td>－</td></tr>
<tr><td>FAX</td><td colspan="2">禁止（送信先が FAX 受信を指定した場合を除く）</td><td>－</td></tr>
<tr><td>非公式ストレージサービス・メールサービス（個人契約したサービスの業務利用）</td><td colspan="3">禁止</td></tr>
<tr><td>外部への情報提供</td><td colspan="2">パスワード設定を行う</td><td>－</td></tr>
<tr><td>教職員の自宅持ち帰り</td><td>禁止</td><td colspan="2">自宅からのクラウドサービス利用は可（端末に情報をダウンロードしない）</td></tr>
<tr><td>電磁記録媒体の利用制限</td><td colspan="3">原則禁止（事情がある場合には、学校情報セキュリティ管理者に相談要）</td></tr>
<tr><td rowspan="3">保管</td><td>パスワード等によるアクセス権の設定（データ保管先）</td><td colspan="2">実施</td><td>－</td></tr>
<tr><td>施錠保管（外部記録媒体又は紙媒体）</td><td colspan="2">実施</td><td>－</td></tr>
<tr><td>クラウドサービス（校務系・学習系ともに）</td><td>禁止</td><td colspan="2">許可</td></tr>
<tr><td>廃棄</td><td>物理的破壊</td><td colspan="2">実施</td><td>－</td></tr>
</table>

	（電磁式記録媒体等）		
	裁断・溶解（紙媒体）	実施	－
	教職員の立会い	実施	－
	廃棄記録の作成及び保存	実施	－
外部での情報処理		禁止	自宅からのクラウドサービス利用は可 （端末に情報をダウンロードしない）
使用する端末制限		校務用端末のみ	指導者用端末*は可 私物端末で学校外からクラウド利用する場合は 申請・許可が必要

*指導者用デジタル教科書を利用する場合のみ校務用端末の利用を許可

第３章　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

教育情報システム管理者及び個別サービス導入責任者は、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、必要な措置を講じる。

（２）サーバの冗長化

教育情報システム管理者及び個別サービス導入責任者は、データセンタ等の管理区域に設置される校務系サーバを冗長化し、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。

（３）機器の電源

① 教育情報システム管理者及び個別サービス導入責任者は、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及び個別サービス導入責任者は、施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じる。

（４）機器の定期保守及び修理

① 教育情報システム管理者及び個別サービス導入責任者は、重要性分類Ⅲ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及び個別サービス導入責任者は、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う。内容を消去できない場合、教育情報システム管理者及び個別サービス導入責任者は、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。

（５）施設外又は学校外への機器の設置

教育情報システム管理者及び個別サービス導入責任者は、施設外又は学校外にサーバ等の機器を設置する場合、教育

CISO 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する。

（６）機器の廃棄等

教育情報システム管理者及び個別サービス導入責任者は、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（２－２（12）③ に記載）を講じる。

（７）個別サービス提供におけるサーバ設置

① 個別サービスを教育センターが所管する教育情報システム基盤に接続する場合には、教育 CISO の許可を必要とする。

② 教育 CISO は、個別サービス導入責任者のサーバ設置に関する安全措置について、対策基準を満たす場合に許可する。

３－２ 管理区域の管理

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。重要性分類Ⅱ以上の情報資産を扱う場合の管理区域は、市の情報システム室やデータセンタといった専用の施設が望ましい。移行過程については学校で情報を保管する場合も残るので学校での管理区域についても規定する。

（１）管理区域がデータセンタ等専用の施設である場合

① 管理区域の構造等

教育情報システム管理者は、下記条件を満たすデータセンタ等専用の施設を選択する。

ア 管理区域は、地階又は1階に設けていない。また、外部からの侵入が容易にできないように無窓の外壁であること。

イ 管理区域から外部に通ずるドアは必要最小限で、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できること。

ウ 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、防水措置等が講じられていること。

エ 管理区域を囲む外壁等の床下開口部を全て塞がれていること。

オ 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構造であること。

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、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。

イ 教育情報システム管理者は、外部委託事業者等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、その提示を求める。

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る。

エ 教育情報システム管理者は当該情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにする。

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、既存の情報システムに与える影響について、あらかじめ市職員等又は委託した業者に確認を行わせる。

イ 教育情報システム管理者及び個別サービス導入責任者は、管理区域の機器等の搬入出について、市職員等を立ち会わせなければならない。

（２）管理区域が学校の場合

① 校内管理区域の構造等

ア 学校情報セキュリティ管理者は、ネットワークの基幹機器及びサーバ設置に関して、施錠管理を行う。

イ 学校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、サーバ及びネットワーク基幹機器を、立ち入りを許可されていない不特定多数の者が出入りできない場所に設置する。

ウ 学校情報セキュリティ管理者は、学校情報セキュリティ担当者と連携して、鍵等によって許可されていない立入りを防止する。

エ 教育情報システム管理者は、機器等に、転倒及び落下防止等の耐震対策、防火措置等を講じることが望ましい。

② 校内管理区域の入退室管理等

ア 学校情報セキュリティ管理者は、管理区域への入退室を許可された者のみに制限すること。

イ 学校情報セキュリティ管理者は、サーバラックの施錠管理にあたり、管理簿の記載等による管理を行う。

ウ 教職員は、児童生徒が管理区域に入室する場合、児童生徒に付き添う。

エ 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、求めにより提示する。

オ 学校情報セキュリティ管理者は、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教職員が付き添う。

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、既存の情報システムに与える影響について、あらかじめ委託した業者に確認を行う。

イ 教育情報システム管理者及び学校情報セキュリティ管理者は、情報システム室の機器等の搬入出について、管理区域への入退室を許可された教職員を立ち会わせる。

３－３ 執務室等の管理

① 教職員は、執務室に教職員が不在になる場合には、施錠する。

② 教職員は、学校情報セキュリティ管理者の許可なく来校者などを執務室へ入室させない。

③ 学校情報セキュリティ管理者は、重要性分類Ⅲ以上の情報資産、コンピュータ、電磁式記録媒体等を盗難や破壊から保護するために、必要により施錠可能な保管庫を用意する。

④ 学校情報セキュリティ管理者又は学校情報セキュリティ担当者は、第三者が校内に立ち入る場合、氏名及び入退時刻を記録する。

⑤ 学校情報セキュリティ管理者又は学校情報セキュリティ担当者は、第三者が校舎内に立ち入る場合、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する。

⑥ 施設開放時の制限

学校情報セキュリティ管理者又は学校情報セキュリティ担当者は、地域住民、保護者、児童生徒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る。

３－４ 通信回線及び通信回線装置の管理

① 教育情報システム管理者は、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 教育情報システム管理者は、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 教育情報システム管理者は、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、通信経路上での暗号化を行う。

④ 教育情報システム管理者は、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 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。

3－5 教職員が利用する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、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、多要素認証の実施や使用する目的に応じた適切な物理的措置を講じる。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、タブレットや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する。

③ 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。

④ アクセス制御による対策を講じたシステムを構成する場合は、校務系情報等の重要な情報資産へのアクセスについて、多要素認証を設定する。

⑤ 教育情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用する。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の使用が望ましい。

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、校務系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、不正アクセスや教職員の不注意等による情報流出への対策を講じる。

⑦ 教育情報システム管理者は、指導者用端末の学校外での業務利用の際は、上記対策に加え、遠隔での端末ロック機能を利用する等の措置を講じる。

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じる。アクセス制御による対策を講じたシステム構成の場合、機微な校務系情報等の重要な情報資産を取り扱う端末に対し、当該端末の状況および通信内容を監視し、異常、あるいは不審な挙動を検知する仕組み（ふるまい検知）等の活用を検討し、適切な対策を講じる。

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る。

⑩ 校務用端末の持ち出し制限

教職員は、許可なく校務用端末を校外へ持ち出さない。事情により校外に持ち出す場合には、事前に学校情報セキュリティ

管理者の許可を得る。

⑪ 私物外部記録媒体の業務端末への接続禁止

教職員は、校外から持ち込んだ外部記録媒体（私物または出所不明な媒体等）を業務端末（校務用端末等）に接続しない。

⑫ 私物情報端末の校内ネットワーク接続禁止

教職員は、パソコン等の私物情報端末を学校に持ち込んで、校内ネットワークに接続してはならない。なお、本市が提供するクラウドサービスに学校外から私物情報端末でアクセスする場合を除く。

３－６　児童生徒が利用する学習者用端末の管理

① 端末ログインパスワード設定

教育情報システム管理者は、端末起動時のログインパスワードの入力を必要とするように設定する。

② 盗難防止対策

教育情報システム管理者は、学校で保管管理する学習者用端末については、盗難防止のため、鍵のかかる部屋等で管理する。また、年に３回、学習者用端末の所在確認を行う。

第４章　人的セキュリティ対策

４－１　教職員の遵守事項

（１）教職員の遵守事項

① 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自校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、速やかに学校情報セキュリティ管理者に相談し、指示を仰ぐ。

② 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わない。

③ 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事務局・学校が構築・管理している環境（本市が提供す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 教職員は、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、学校情報セキュリティ管理者の許可を得る。

イ 教職員は、外部で情報処理業務を行う場合には、安全管理措置を遵守する。

ウ 学校情報セキュリティ管理者は、教職員が、本市が提供するクラウドサービスを利用して外部で情報処理を行う際に使用する端末が支給端末以外である場合、OS、WEBブラウザ、搭載されたウイルス対策ソフトの有無、ファイル共有ソフトを搭載していないこと、家族とアカウント共有していないことを申告させ、サポート期限が切れていないなど、外部情報処理環境の安全性を確認した上で利用を許可する。

エ 教職員は、本市が提供するクラウドサービスを利用する場合、情報処理はクラウドサービス内で実施し、端末にデータをダウンロードしない。

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

教職員は、校内において、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、学校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。

⑤ 持ち出し及び持ち込みの記録

学校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。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など、運用実態や教職員の負担も考慮し検討する。

⑥ 机上の管理

教職員は、校務用端末、指導者用端末、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、離席時は、校務用・指導者用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、適切な措置を講じる。

⑦ 端末の覗き見対策

教職員は、校務用パソコンについて以下の覗き見対策を実施すること。

・ 長時間の離席時にはパソコンのシャットダウンまたはログオフを実施する。

・ 短時間の離席時には端末表示画面をロックする。

⑧ 共用端末の画面クリア

複数の教職員が共用する端末において、各教職員にログオンアカウントが付与されている場合には、離席時には表示画面をロックする。

⑨ 知りえた情報の秘匿

教職員は、不特定多数の人がいる場所において、情報資産の内容や職務上知り得た情報を話さない。

⑩ 退職時等の遵守事項

教職員は、異動、退職等により業務を離れる場合には、利用していた情報資産を、返却する。また、その後も業務上知り得た情報を漏らさない。

（２）学習者用端末及び学習系クラウド利用についての児童生徒への指導事項

① ID の管理

教職員は、児童生徒の ID について、秘匿管理することや他人に利用させてはいけないことを指導する。

② パスワードの管理

教職員は、児童生徒のパスワードを他人に知られないように指導する。ただし、保護者や教職員から指示があった場合は、パスワードを伝えるよう指導する。

③ 学習系情報は学習系クラウドに保管

教職員は、学習者用端末で生成した学習系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は、不正アクセスに備えて、この機能を利用するよう指導する。

④ マルウェア感染が疑われる場合の報告

教職員は、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が出るといった症状が発覚した場合は、すぐに報告するよう指導する。

⑤ 不適切な使用の禁止

教職員は、児童生徒が端末及び学習系クラウドを利用するにあたり、不適切な使用をしないことを指導する。

⑥ 端末の安全な取扱い管理

教職員は、児童生徒が学習用端末を取り扱うにあたり、盗難・紛失・破損等に対する安全管理を指導する。

（３）新規赴任教職員への遵守指導

学校情報セキュリティ管理者は、新規採用教職員及び他自治体から本市に新規赴任した教職員に対し、教育情報セキュリティポリシー、自校実施手順に基づき遵守すべき内容を理解させ、遵守するように指導する。

（４）インターネット接続及び電子メール使用等の制限

学校情報セキュリティ管理者は、教職員にパソコンや業務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は、業務上必要最小限にするように指導する。

（５）教職員の離任

① 退職や異動により教職員が離任した場合、学校情報セキュリティ管理者は、校務システムの教職員名簿リストに離任日を入力し、速やかに当該者の校務システムの操作権を無効にする手続きを講じる。

② 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する。また、その後も業務上知り得た情報を公開することはできない。

（６）外部委託事業者に対する説明

教育情報システム管理者及び個別サービス導入責任者は、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。

４－２　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、以下の規定を順守する。

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返却する。また、その後も業務上知り得た情報を漏らさない。

４－３　研修

（１）情報セキュリティに関する研修

教育CISOは、定期的に情報セキュリティに関する研修を実施する。

（２）研修計画の策定及び実施

① 教育 CISO は、教職員に対する情報セキュリティに関する研修計画を立案し、実施する。

② 教育 CISO は、研修計画において、毎年度１回は教職員が情報セキュリティ研修を受講できるようにする。

③ 教育 CISO は、新規採用の教職員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。

④ 学校情報セキュリティ管理者は、必要に応じて教育 CISO に、教職員の情報セキュリティ研修の実施状況について報告する。

⑤ 教育 CISO は、デジタル推進本部に、情報セキュリティ研修の実施状況について報告する。

（３）情報セキュリティに関する校内施策の実施

学校情報セキュリティ管理者は、学校情報セキュリティ委員会等を通して、校内の教職員を対象とした情報セキュリティに関する事故事例を共有するなど、教職員に対して注意喚起及び情報セキュリティ意識を向上させる施策を、定期的または必要に応じて実施する。

（４）研修への参加

① 全ての教職員は、定められた研修に参加する。

② 教育委員会事務局職員は、教職員向け研修に参加することが望ましい。

４－４ 情報セキュリティインシデントの報告

（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 情報セキュリティに関する連絡フローの整備

学校情報セキュリティ管理者は、実施手順に情報セキュリティに関する連絡フローを記して、教職員に周知する。

② 教職員は、情報セキュリティインシデントが疑われる事象を認知した場合、速やかに学校情報セキュリティ管理者に報告する。

以下に、情報セキュリティインシデントが疑われる事象が想定される事例を示す。

ア 他教職員の教育情報セキュリティポリシーに関する違反行為発見

イ 復元可能な廃棄物の発見

ウ 学校で取り扱う情報の改ざん、消去

エ 部外者の職員室等への無断侵入

オ コンピュータやネットワークの不具合

カ 学校ホームページ上での情報誤公開・改ざん

③ 報告を受けた学校情報セキュリティ管理者は、速やかに教育情報システム担当者に連絡する。人的要因に関連する場合には、あわせて教育情報セキュリティ責任者に連絡する。また情報セキュリティに関する統一的な窓口（教育 CSIRT）の指示に従い、調査に協力する。

（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、学校情報セキュリティ管理者に報告する。

② 報告を受けた学校情報セキュリティ管理者は、速やかに教育情報システム担当者に連絡する。人的要因に関連する場合には、教育情報セキュリティ責任者にも連絡する。また情報セキュリティに関する統一的な窓口（教育 CSIRT）の指示に従い、調査に協力する。

（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 CISO は、情報セキュリティインシデントについて、統括教育情報セキュリティ責任者、学校情報セキュリティ管理者、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情報セキュリティに関する統一的な窓口（教育 CSIRT）と連携し、

これらの情報セキュリティインシデントの原因を究明し、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、再発防止策を検討する。

② 教育 CISO は、情報セキュリティインシデントについて、再発防止策を実施するために必要に応じて関係部局等との連携を図る。

４－５　ID 及びパスワード等の管理

（１）IC カード等の取扱い

① 教職員は、自己の管理する IC カード等に関し、次の事項を遵守する。

ア 認証に用いるICカード等を、教職員間で共有しない。

イ 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く。

ウ ICカード等を紛失した場合には、速やかに教育情報システム管理者に通報し、指示に従う。

② 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。

③ 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、切替え前のカード等を回収し、破砕するなど復元不可能な処理を行った上で廃棄する。

（２）ID の取扱い

教職員は、自己の管理するIDに関し、次の事項を遵守する。

① 自己が利用している ID は、他人に開示及び利用させない。

② 共用 ID を利用する場合は、共用 ID の利用者以外に開示及び利用させない。

（３）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、学校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は、同一のパスワードを複数のシステム間で用いない。（シングルサインオンを除く）

⑥ 仮のパスワードは、最初のログイン時点で変更する。

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ない。

⑧ 教職員間でパスワードを共有しない。

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する。

⑩ 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。

第５章　技術的セキュリティ

５－１　コンピュータ及びネットワークの管理

（１）文書サーバ及び端末の設定等

① 教育情報システム管理者及び個別サービス導入責任者は、教職員が使用できる文書サーバの容量を設定し、教職員に周知する。

② 教育情報システム管理者及び個別サービス導入責任者は、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する。

③ 教育情報システム管理者及び個別サービス導入責任者は、住民の個人情報、人事記録等、特定の教職員しか取り扱えないデータについて、別途ディレクトリを作成するなどの措置を講じ、同一学校等であっても、業務上アクセスが必要な教職員のみが閲覧及び使用できるようにする。

④ 教育情報システム管理者及び個別サービス導入責任者は、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、個人情報など重要性が高い情報を保管する場合に限る）については、サイバー攻撃リスクを考慮し、ファイル暗号化等による安全管理措置を講じる。

（２）バックアップの実施

教育情報システム管理者及び個別サービス導入責任者は、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① 及び② に基づきバックアップを実施するものとする。

① 校務系情報及び校務外部接続系情報については、定期的にバックアップを実施する。

② 学習系情報については、必要に応じて定期的にバックアップを実施する。

（３）システム管理記録及び作業の確認

① 教育情報システム管理者及び個別サービス導入責任者は、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 教育情報システム管理者及び個別サービス導入責任者は、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 教育情報システム管理者、個別サービス導入責任者、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する。

（４）情報システム仕様書等の管理

教育情報システム管理者及び個別サービス導入責任者は、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したり、紛失等がないよう、適切に管理する。

（５）ログの取得等

① 教育情報システム管理者及び個別サービス導入責任者は、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 教育情報システム管理者及び個別サービス導入責任者は、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、適切にログを管理する。

③ 教育情報システム管理者及び個別サービス導入責任者は、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。

（６）障害記録

教育情報システム管理者及び個別サービス導入責任者は、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、適切に保存する。

（７）ネットワークの接続制御、経路制御等

① 教育情報システム管理者は、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、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 教育情報システム管理者は、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実施する。

ア 物理的接続制限

校務系ネットワークには、不正接続防止システムを設置し、登録されていない機器の接続ができない構造とする。

イ 無線LAN

校内に敷設される無線 LAN は、RADIUS 認証、VLAN 認証、MAC アドレス認証などによる接続機限定を施す。

（８）外部の者が利用できるシステムの分離等

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

（９）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、教育 CISO 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、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責任者による損害賠償責任を契約上担保する。

④ 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サイバー脅威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、教育 CISO 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する。

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

① 教育情報システム管理者は、アクセス制御による対策を講じたシステム構成の場合は、各システムにおけるアクセス権管理を徹底する。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など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。

（11）複合機のセキュリティ管理

① 教育情報システム管理者は、複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定する。

② 教育情報システム管理者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティ事故への対策を講じる。

③ 教育情報システム管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じる。

（12）無線 LAN 及びネットワークの盗聴対策

① 教育情報システム管理者は、無線 LAN の利用を認める場合、解読が困難な記号化及び認証技術の使用を義務付ける。

② 教育情報システム管理者は、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る。

（13）電子メールのセキュリティ管理

① 教育情報システム管理者は、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 教育情報システム管理者は、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 教育情報システム管理者は、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 教育情報システム管理者は、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する。

⑤ 教育情報システム管理者は、システム開発や運用、保守等のため庁舎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。

（14）電子メールの利用制限

① 教職員は、自動転送機能を用いて、電子メールを転送しない。

② 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ない。

③ 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する。

④ 教職員は、電子メールを誤送信した場合、学校情報セキュリティ管理者に報告する。

⑤ 教職員は、個人で契約したウェブで利用できるフリーメールサービス、ファイルストレージサービス等を使用しない。

（15）無許可ソフトウェアの導入等の禁止

① 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ない。

② 教職員は、業務上の必要がある場合は、学校情報セキュリティ管理者に申告し、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。

③ 教職員は、不正にコピーしたソフトウェアを利用しない。

（16）機器構成の変更の制限

① 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・交換を行わない。

② 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、教育情報システム管理者の許可を得る。

（17）無許可でのネットワーク接続の禁止

教職員は、教育 CISO 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。

（18）業務以外の目的でのウェブ閲覧の禁止

① 教職員は、業務以外の目的でウェブを閲覧しない。

② 学校情報セキュリティ管理者は、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、適切な是正措置を求める。

5－2 アクセス制御

（1）アクセス制御

① アクセス制御

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がアクセスできないように、システム上制限する。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。

② 利用者 ID の取扱い

ア 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る。

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、学校情報セキュリティ管理者又は教育情報システム管理者に通知する。

ウ 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努める。

③ 特権を付与された ID の管理等

ア 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。

イ 教育情報システム管理者の特権を代行する者は、教育情報システム管理者が指名し、教育CISOが認めた者とする。

ウ 教育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、教育情報システム管理者、学校情報セキュリティ管理者に通知する。

エ 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る場合は、外部委託契約の中で安全管理を義務付ける。

オ 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などのセキュリティ機能を強化する。

カ 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。

（2）外部からのアクセス等の制限

① 教職員が校務用端末を用いて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、当該情報システムを管理する学校情報セキュリティ管理者の許可を得る。

② 学校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、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。

③ 学校情報セキュリティ管理者は、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る。

④ 教育情報システム管理者は、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

る。

⑤ 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る。

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する。

⑦ 教育情報システム管理者は、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じる。

（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）パスワードに関する情報の管理

① 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、これを有効に活用する。

② 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するよう指導する。

５－３ システム開発、導入、保守等

（１）情報システムの調達

① 教育 CISO、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個別サービス導入責任者は、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する。

② 教育 CISO、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個別サービス導入責任者は、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及び個別サービス導入責任者は、システム開発の責任者及び作業者を特定する。また、システム開発のための規則を確立する。

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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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ことが望ましい。

イ 教育情報システム管理者及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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。

５－４　不正プログラム対策

（１）教育情報システム管理者及び個別サービス導入責任者の措置事項

教育情報システム管理者及び個別サービス導入責任者は、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、必要に応じ学校に対して注意喚起する。

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る。

⑤ 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させない。

（２）教育情報システム担当者及び個別サービス導入責任者の措置事項

教育情報システム担当者及び個別サービス導入責任者は、不正プログラム対策に関し、次の事項を措置する。

① 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つ。

② 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つ。

③ 学校セキュリティ管理者及び教育情報システム担当者は、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、公式な電磁的記録媒体以外を教職員に利用させない。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する。

（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、次の事項を遵守する。

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 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、以下の対応を行う。

ア 端末のネットワークからの切り離し

（ア）校務用端末の場合は、有線LANケーブルを即時取り外す。

（イ）指導者用端末又は学習者用端末の場合は、直ちに利用を中止し、モバイル通信を行わない設定へと変更する。

イ 速やかに教育情報システム担当者に連絡し、指示に従う。

ウ 教育情報システム担当者の指示があるまでは、端末の電源を切らない。

（４）専門家の支援体制

教育情報システム管理者は、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。

５－５ 不正アクセス対策

（１）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及び個別サービス導入責任者は、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。

（２）教職員による不正アクセス

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学校情報セキュリティ管理者に通知し、適切な処置を求める。

（３）サービス不能攻撃

教育情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じる。

（４）標的型攻撃

教育情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じる。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じる。

５－６ 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

教育情報システム管理者及び教育情報システム担当者は、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

教育情報システム管理者及び教育情報システム担当者は、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、教職員に周知する。

（３）情報セキュリティに関する情報の収集及び共有

① 教育情報システム管理者及び教育情報システム担当者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有する。

② 外部委託業者から情報収集できるよう、情報セキュリティに関する提供を契約内容に盛り込む。

③ 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る。

第６章　運用

６－１　情報システムの監視

① 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、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。

② 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る。

６－２　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 学校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責任者は、発生した問題について、適切かつ速やかに対処する。

③ 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

教育 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

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、直ちに学校情報セキュリティ管理者に報告を行う。

６－３　例外措置

（１）例外措置の許可

学校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、教育 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

学校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などの場合であって、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 CISO に報告する。

（３）例外措置の記録管理

教育 CISO は、例外措置の記録を適切に管理する。

６－４　法令遵守

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を遵守し、これに従う。

・ 地方公務員法（昭和 25 年 12 月 13 日法律第 261 号）

・ 教育公務員特例法（昭和 24 年 1 月 12 日法律第 1 号）

・ 著作権法（昭和 45 年法律第 48 号）

・ 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）
・ 個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）
・ 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）
・ サイバーセキュリティ基本法（平成 26 年法律第 104 号）

６－５　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、地方公務員法による懲戒処分の対象とする。

（２）違反時の対応

① 学校情報セキュリティ管理者は、教育情報セキュリティポリシーに対する教職員の違反を確認した場合は、速やかに教育情報セキュリティ責任者に通知し、適切な措置を講じる。その後速やかに教育情報セキュリティ責任者は、教育 CISO、統括教育情報セキュリティ責任者に通知する。

② 教育情報システム管理者等が違反を確認した場合は、速やかに教育 CISO、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学校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 CISO 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することができる。その後速やかに、教育 CISO は、教職員の権利を停止した旨を当該教職員が所属する学校の学校情報セキュリティ管理者に通知する。

第７章　外部委託

７－１　外部委託事業者の選定基準

① 教育情報システム管理者及び個別サービス導入責任者は、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及び個別サービス導入責任者は、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。

７－２　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事故発生時の公表
・ 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）
・ セキュリティ情報（脆弱性情報等）の収集と情報提供

７－３　確認・措置等

教育情報システム管理者及び個別サービス導入責任者は、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、7－２の契約に基づき措置する。また、その内容を教育CISOに報告する。

第８章　外部サービス利用

８－１　クラウドサービスの利用

（１）クラウドサービスの情報セキュリティを把握するための第三者認証等の活用

クラウドサービスの情報セキュリティの実態を、クラウド利用者自らが詳細に調査することは困難である場合も多いため、クラウドの利用に関しては、第三者による認証や各クラウドサービス事業者が提供している監査報告書を利用する。

クラウド事業者の選定においても、求める内容に応じた認証規格を参考にすることで、（２）（３）項に示したクラウド事業者の責務と対策を履行できる能力を持ち、情報セキュリティの確保等が適切に行われていると間接的に判断することが可能である。

多くの SaaS 事業者は、クラウドサービス基盤を大手クラウド事業者から仕入れており、大手クラウド事業者は第三者認証制度を取得している場合が多い。その場合は、SaaS 事業者が自ら提供するアプリケーション領域に特化して（２）（３）項を確認することが有効である。

＜認証制度の例＞

・ ISO/IEC27001（情報セキュリティマネジメントシステム）
・ ISO/IEC27002（情報セキュリティマネジメントシステム）
・ ISO/IEC27014（情報セキュリティガバナンス）
・ ISO/IEC27017（クラウドサービスの情報セキュリティ）
　https://isms.jp/isms-cls/lst/ind/index.html
・ ISO/IEC27018（クラウドサービスにおける個人情報の取扱い）
・ 米国 FedRAMP
　https://marketplace.fedramp.gov/#/products?status=Compliant
・ AICPASOC2（日本公認会計士協会 IT7 号）
・ AICPASOC3（SysTrust/WebTrsuts）（日本公認会計士協会 IT2 号）
・ JASA クラウドセキュリティ推進協議会 CS ゴールドマーク
　http://jcispa.jasa.jp/cs_mark_co/cs_gold_mark_co/

・ ASP・SaaS 安全・信頼性に係る情報開示認定

（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

教育情報システム管理者及び個別サービス導入責任者は、当該クラウドサービスのログインに関わる認証機能（ID,パスワード等）の提供をクラウド事業者に確認する。

② アクセス制御

ア 教育情報システム管理者及び個別サービス導入責任者は、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確認する。

イ 教育情報システム管理者及び個別サービス導入責任者は、クラウド事業者の提供するアクセス制御機能を用いて、情報資産毎に、許可されたエンドユーザのみがアクセスできる環境を設定する。

③ クラウドに保管するデータの暗号化

教育情報システム管理者及び個別サービス導入責任者は、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、必要に応じて、クラウド事業者に確認する。

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

教育情報システム管理者及び個別サービス導入責任者は、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、一部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、必要に応じて、クラウド事業者に確認する。

⑤ 情報の通信経路のセキュリティ確保

教育情報システム管理者及び個別サービス導入責任者は、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が講じられていることを、クラウド事業者に確認する。

⑥ クラウドサービスを提供する情報システムの運用管理

教育情報システム管理者及び個別サービス導入責任者は、クラウド利用者としての業務運営に支障がないことを確認するために、必要に応じてクラウド事業者に対して、サーバの冗長化及びデータバックアップの有無、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る。

⑦ データの廃棄等について

ア 教育情報システム管理者及び個別サービス導入責任者は、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、必要に応じて廃棄証明書の発行を求める。

イ 教育情報システム管理者及び個別サービス導入責任者は、サービス利用終了時等におけるデータの扱いについて、回収及び次期システムへの移行等を行えるよう、必要に応じてその措置の流れについてクラウド事業者に確認する。

⑧ 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

教育情報システム管理者及び個別サービス導入責任者は、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確認する。

⑨ クラウド事業者従業員の人的セキュリティ対策

教育情報システム管理者及び個別サービス導入責任者は、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、下記の

遵守をクラウド事業者に確認する。

ア 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

イ クラウド利用者のデータの秘匿

ウ 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無断での外部持ち出し禁止

（３）パブリッククラウド事業者のサービス提供ポリシー等に関する確認事項

① 守秘義務、目的外利用及び第三者への提供の禁止

教育情報システム管理者及び個別サービス導入責任者は、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する。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る。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

教育情報システム管理者及び個別サービス導入責任者は、必要に応じて、クラウド事業者がどのような規範に基づいてサービスを提供するか開示を求め、準拠する法令、情報セキュリティポリシー等を確認する。

③ 情報セキュリティに関する役割の範囲、責任分界点

教育情報システム管理者及び個別サービス導入責任者は、必要に応じて、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、クラウド利用者で支障が出ないかを確認する。

④ 監査

教育情報システム管理者及び個別サービス導入責任者は、必要に応じて、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レポート開示するよう求め、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する。

⑤ 情報セキュリティインシデント管理及び対応フローの合意

教育情報システム管理者及び個別サービス導入責任者は、必要に応じて、情報セキュリティインシデント管理に関する責任範囲と事故対応フローを、クラウド事業者に対して求め、内容の妥当性を検証する。

⑥ クラウドサービスの提供水準及び品質保証

教育情報システム管理者及び個別サービス導入責任者は、必要に応じて、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）を確認し、それらの水準・品質が、業務遂行に支障がないことを確認する。

⑦ クラウド事業者の再委託先等との合意事項

教育情報システム管理者及び個別サービス導入責任者は、第三者認証を取得していないクラウド事業者を利用する場合、必要に応じて、クラウド事業者自らが実施するセキュリティ対策内容について、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、業務遂行に支障がないことを確認する。

⑧ 日本の法令が適用されることの確認

教育情報システム管理者及び個別サービス導入責任者は、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する。

（４）クラウドサービス利用者の留意事項

教職員は、学習系クラウドサービスを利用する場合、利用対象となる児童生徒と教職員のみがアクセス可能な環境を設定する。

８－２　約款による外部サービスの利用

（１）約款による外部サービスの利用の可否判断ポイント

① 知りえた情報の秘密保持義務、目的外利用の禁止、無許可での第三者への提供の禁止、安全な廃棄手順が約款に存在しているか

② 利用者データの知的財産権が利用者に帰属しているか（サービス提供者側に帰属することはないか）

③ 技術的対策、人的対策等の安全管理措置が記載されているか

④ 情報セキュリティ事故発覚時に調査協力が得られるか

⑤ 一方的な利用規約の変更、サービス停止のリスクに対して、どこまでの範囲でなら利用可能か

（２）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する。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する。

① 約款によるサービスを利用してよい範囲

② 業務により利用する約款による外部サービス

③ 利用手続及び運用手順

（３）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する。

８－３　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、教育委員会又は学校が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を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に当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等でなりすまし対策を行うこと。

イ パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ICカード等）等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

② 重要性分類Ⅲ以上の情報はソーシャルメディアサービスで発信してはならない。

③ 利用するソーシャルメディアサービスごとの責任者を定めなければならない。

第９章　１人１台端末におけるセキュリティ

９－１　学習者用端末のセキュリティ対策

（１）授業・学習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）

教育情報システム管理者は、学校での ICT 活用に支障が出ないネットワーク構成及びインターネット接続帯域を確保する。また、利用状況に応じて定期的に見直す。

（２）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対策を講じる。

＜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（マルウェアに感染した Web サイトや不正な Web サイトにアクセスした時に、ブラウザに警告を表示させる仕組み）

（３）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じる。

（４）端末を不正利用させないための防止策

① 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。

② 教職員は、児童生徒が端末で外部コミュニケーション（メール、SNS 等）や情報の交換を行う場合に、学校から許可されたコミュニケーションツールのみを利用するように指導する。

（５）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、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ることが望ましい。

（６）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、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などの安全管理措置を講じる。

（７）運用・連絡体制の整備

学校情報セキュリティ管理者は、学校内外での端末の運用ルールを制定し、事故時の連絡先対応方法を各学校にて整理する。

９－２　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

① 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/パーシスタント（永続的な識別）な構成要素になっていることや、児童生徒の発達段階に応じた複雑性を上げたパスワードポリシーによりセキュリティ強度を上げていくなど適切な措置を講じる。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、市内共通で利用するクラウドサービスについては、教育委員会事務局にて一元管理する。

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、MDM 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。

③ 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。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。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）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、サービス毎のアカウント情報管理が非常に煩雑になるため、一度の認証により一定時間は各種サービスにアクセスが行えるシングルサインオンの導入を必要に応じて講じる。

（３）児童生徒のパスワードに関する情報の管理

① 教職員は、児童生徒に対して、端末ログインパスワード及びサービス利用パスワードを設定するよう指導する。また、児童生徒に対してサービス利用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するよう指導する。

② 児童生徒が端末ログインパスワードを失念した場合等、教職員は学校情報セキュリティ管理者の指示の下、教育情報システム管理者へ端末ログインパスワードのリセットを依頼する。

③ 児童生徒がサービス利用パスワードを失念した場合等、学校情報セキュリティ担当者が当該児童生徒のサービス利用パスワードをリセットする。

（４）児童生徒の端末本体及び学習系クラウドの保存領域へのアクセス

① 教職員は、学校情報セキュリティ管理者の指示の下、位置情報や児童生徒の端末本体及び教育委員会が所管する学習系クラウドの保存領域にアクセスし、保存されている情報をパスワードをリセットするなどし、確認することができる。

② 保護者は、児童生徒の端末本体及び教育委員会が所管する学習系クラウドの保存領域にアクセスし、保存されている情報をパスワードをリセットするなどし、確認することができる。なお、保護者による子どもの ID 及びパスワード管理については、「熊本市学習用タブレット端末の利用についての同意書」の規定により、保護者と児童生徒本人は秘匿管理に留意する。

第１０章 評価・見直し

１０－１ 監査

（１）実施方法

教育 CISO 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、毎年度及び必要に応じて監査を行う。

（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 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、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、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う。

（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、委員会並びにデジタル推進本部に報告する。

（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する。

（７）監査結果への対応

教育 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定等の見直し等への活用

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

学校情報セキュリティ管理者は、教育情報セキュリティポリシーに基づいた自校の実施手順に沿った自校の情報セキュリティ対策状況について、年１回、自己点検を実施する。

（２）報告

学校情報セキュリティ管理者は、自己点検結果を教育情報セキュリティ責任者に報告する。

（３）改善策の取りまとめ

教育情報セキュリティ責任者は、各校の自己点検結果に基づき改善策を取りまとめ、委員会に報告する。

（４）自己点検結果の活用

① 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る。

② 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

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、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。教育 CISO は、見直しまでの間の暫定的な運用を行う権限及び責任を有する。ただし、教育ＣＩＳＯは、次の教育委員会会議において、これを報告しなければならない。

附　則

令和　５年１２月２８日　制定

令和　６年　４月　１日　施行

令和　６年　６月２８日　施行