日進市小中学校情報セキュリティ対策基準

令和７年４月１日制定

情報セキュリティポリシーとは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書をいう。地方公共団体における情報セキュリティポリシーは、各地方公共団体が組織の実態に応じて自主的に策定や見直しを行うものであり、情報セキュリティ対策の頂点に位置するものであり、本来は地方公共団体全てを包括するポリシーでなければならない。

一方で、地方公共団体が設置する学校においては、地方公共団体の他の行政事務とは異なる特徴を有する。 例えば、学校とは地方公務員法及び教育公務員特例法に定める「服務」に服さない児童生徒が過ごす場所であり、当該児童生徒がコンピュータを活用した学習活動の実施などにおいて、日常的に 情報システムにアクセスする機会がある。そのため、児童生徒においても情報セキュリティポリシーにて規定した対策について遵守するよう、職員、教員、保護者等が適切に指導を行うことが求められる。

また、学校には、指導要録、答案用紙、生徒指導等の記録、進路希望調査票、児童生徒等の住所録等の重要性が高い情報が保管されている。児童生徒の育成においては、学校教育に直接関わる複数の関係者により、児童生徒に関する情報が多目的で活用される 。学習においても、教職員や他の児童生徒と協働学習活動を実践する際、児童生徒が生み出す情報は本人の思考の記録であるとともに学習評価の材料となり、必要に応じて他児童生徒に開示する等多目的に活用される。

よって、学校教育においては、児童生徒の存在及び取り扱う情報の多様性・多目的性等を考慮した情報セキュリティ対策を講ずる必要がある。

このような背景を踏まえ、学校における情報セキュリティの考え方を示し、情報セキュリティを確保する上での具体的な遵守事項及び判断基準等を定めるものである。

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、内部部局、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。

ア　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

イ　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。）

ウ　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。

ア　小中学校情報セキュリティポリシー　日進市小中学校情報セキュリティ基本方針及び本対策基準をいう。

イ　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をいう。

ウ　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をいう。

エ　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をいう。

オ　校務用端末

校務系情報にアクセス可能な端末をいう。

カ　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をいう。

キ　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をいう。

ク　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をいう。

ケ　校務系サーバ

校務系情報を取り扱うサーバをいう。

コ　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をいう。

サ　学習系サーバ

学習系情報を取り扱うサーバをいう。

シ　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をいう。

ス　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をいう。

セ　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をいう。

ソ　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をいう。

２　組織体制

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

ア　CISOは「日進市小中学校情報セキュリティ基本方針」で定める。CISOは、本市における全てのネットワーク、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。

ウ　CISO は、情報セキュリティインシデントに対処するための体制（Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

エ　CISO は、CISO を助けて本市における情報セキュリティに関する事務を整理し、CISO の命を受けて本市の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副 CISO」という。）１人を必要に応じて置く。

オ　CISO は、本対策基準に定められた自らの担務を、副 CISO その他の本対策基準に定める責任者に担わせることができる。

（２）教育情報セキュリティ統括責任者

ア　教育情報セキュリティ統括責任者は「日進市小中学校情報セキュリティ基本方針」で定める。教育情報セキュリティ統括責任者は、CISO 及び副 CISO を補佐しなければならない。

イ　教育情報セキュリティ統括責任者は、本市教育委員会の全ての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。

ウ　教育情報セキュリティ統括責任者は、本市教育委員会の全ての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。

エ　教育情報セキュリティ統括責任者は、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。

オ　教育情報セキュリティ統括責任者は、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、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実施する権限及び責任を有する。

カ　教育情報セキュリティ統括責任者は、本市の共通的なネットワーク、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。

キ　教育情報セキュリティ統括責任者は、緊急時等の円滑な情報共有を図るため、CISO、教育情報セキュリティ統括責任者、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、情報システム管理者、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。

ク　教育情報セキュリティ統括責任者は、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。

ケ　教育情報セキュリティ統括責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて CISO にその内容を報告しなければならない。

コ　教育情報セキュリティ統括責任者は、自身の権限に属する事務を学習政策課長に処理させることができる。

（3）教育情報セキュリティ責任者

ア　教育委員会事務局の情報セキュリティ担当部等の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、当該部等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、その所管する部等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、その所管する部等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、小中学校情報セキュリティポリシーの遵守に関する意見の集約並びに教職員、非常勤教職員及び臨時教職員等（以下「教職員等」という。）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　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、その所管する学校等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、その所掌する学校等において、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、教育情報セキュリティ統括責任者及びCISOへ速やかに報告を行い、指示を仰がなければならない。

（5）教育情報システム管理者

ア　教育委員会の情報システム担当課等の長及び校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教育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

教育情報システム管理者の指示等に従い、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者を教育情報システム担当者とする。

（７）教職員等

ア　臨時的任用教職員、非常勤講師を含めた教職員全員を、教職員等と称する。

イ　教職員等は学校が所管する情報資産を取り扱う立場にあり、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しなければならない。

（８）教育委員会事務局職員

ア　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を指す。

イ　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、教育情報セキュリティ責任者の指導の下、情報セキュリティを遵守しなければならない。

（９）情報セキュリティ委員会

ア　本市の情報セキュリティ対策を統一的に実施するため、CISO、CIO、教育情報セキュリティ統括責任者、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、小中学校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　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することが望ましい。

（１０）兼務の禁止

ア　情報セキュリティ対策の実施において、止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　情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

（１１）クラウドサービス利用における組織体制

教育情報セキュリティ統括責任者は、クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

（１２）CSIRT の設置・役割

ア　CISO は、CSIRT を整備し、その役割を明確化しなければならない。

イ　CISO は、CSIRT に所属する職員等を選任し、その中から CSIRT 責任者を置かなければならない。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定

めなければならない。

ウ　CISO は、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

エ　CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部等に提供しなければならない。

オ　情報セキュリティインシデントを認知した場合には、CISO、総務省、都道府県等へ報告しなければならない。

カ　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。

キ　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、委託事業者等との情報共有を行わなければならない。

ク　CSIRT は学校教育課が担うものとする。ただし、日進市情報セキュリティ対策基準に記す CSIRT 担当課と共同で行うものとする。

3　情報資産の分類と管理

3．1　情報資産の分類

本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

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。
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。

情報資産の分類		情報資産の例示			
重要性分類	定義	校務系		学習系	公開系
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。	・指導要録原本 ・教職員の人事情報			
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 ・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 ・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 ・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） ・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 ・個別面談記録 ・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 ・卒業生進路先一覧等 ・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 ・健康診断票 ・歯の検査表 ・学校生活管理指導票 ・児童・生徒等健康調査票 ・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） ○名簿等 ・児童生徒名簿 ・児童生徒の住所録 ・PTA会員名簿 ・職員住所録 ・委員会名簿 ○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	○児童生徒の学習系情報 ・学習システムログインID/PW管理台帳 ・学習用端末ID/PW管理台帳・	
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 ・出席簿 ・名列表 ・座席表 ・児童生徒委員会名簿	○学校運営関係 ・卒業アルバム ・学校行事等の児童・生徒の写真	○学校運営関係 ・教材研究資料 ・授業用教材 ・生徒用配付プリント ○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。				○学校運営関係 ・（学校経営案） ・使用教科書一覧 ・教育課程編成表 ・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）

図表 重要性分類に基づく情報資産の例示

※ 本表は例示であり、個別の事情により本表とは異なる分類となる場合がある。

（注１）児童生徒の氏名、性別、学年等の属性情報を、生活歴、心身の状況、電話番号等といった情報と束ねたリスト等については、上記のとおり重要性分類Ⅱとして扱うことが望ましい一方で、児童生徒が学習活動を通して生み出す学習系情報の中にも、氏名、性別、学年といった属性情報を置くことは自然なことであり、様々な学習系ツールの利用場面も含めて、これらの属性情報について学習系システムの中において扱うことを一義的に禁止するものではない。前述のとおり、活用場面等に応じて、実態に即した形で運用すること。

（注２）児童生徒の学習記録等についても、児童生徒自身が振り返りとして活用することも想定される。その活用が児童生徒にとって有益となる場合であって、自身の情報に対しては当該児童生徒以外からの不要なアクセスを防ぐ環境を構築する等の配慮をした上で、学習系システムにおいて運用することなども考えられる。なお、それらの情報をクラウド事業者が、利用者の同意なく無断使用（目的外利用（無断解析等）、第三者への提供等）しないよう留意すること。

（注３）ログインID/PW自体は情報資産として取り扱うものではないが、ログインID/PWを束ねた管理台帳については重要性分類Ⅱ以上として扱うことが必要である。

３．２　情報資産の管理

（１） 管理責任

ア　CISO または教育情報セキュリティ統括責任者は、教育情報システムとその運用管理を定めた小中学校情報セキュリティ対策基準を策定しなければならない。

イ　教育情報セキュリティ統括責任者は、小中学校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ひな形を作成しなければならない。

ウ　教育情報セキュリティ統括責任者は、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、適宜更新しなければならない。

エ　教育情報セキュリティ管理者は、実施手順ひな形に基づき、自校の実施手順を作成しなければならない。

オ　教育情報セキュリティ管理者は、標準情報資産台帳に基づき、自校で所管する情報資産を確認し、不足内容を補完した自校向け情報資産台帳（以下「台帳」という。）を整備しなければならない。

カ　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。

キ　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しなければならない。

ク　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わなければならない。

（２）情報資産の取り扱い

ア　情報資産の分類の表示

教職員等は、情報資産について、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、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

イ　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、当該情報の分類と取扱制限を定め、分類に準拠した取扱いを行わなければならない。

（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。

ウ　情報資産の入手

（ア）本市教職員等が作成した情報資産を入手した教職員等は、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）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わなければならない。

（ウ）情報資産を入手した教職員等は、入手した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。

エ　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てはならない。

（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、適正な取扱いをしなければならない。

（ウ）情報資産を利用する教職員等は、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を取り扱わなければならない。

（３）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の措置事項

（ア）教育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、教職員等に周知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、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

（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、利用頻度が低い電磁的記録媒体や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長期保管する場合は、自然災害を被る可能性が低い地域に保管することが望ましい。

（エ）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、耐火、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。

イ　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しなければならない。

（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しなければならない。

（４）情報資産の外部持ち出し

ア　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個別許可を得なければならない。また、持ち出し持ち帰りの記録をつけなければならない。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、有効にしなければならない。

（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、有効にしなければならない。

イ　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しなければならない。

（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）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てはならない。

ウ　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しなければならない。

（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こと。

（イ）外部電磁的記録媒体の暗号化

暗号化機能つきの媒体を利用し、暗号化機能を活かすことが望ましい。

エ　FAX 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ことが望ましい。

オ　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教職員は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、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以上の情報資産を運搬する教職員は、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。

カ　情報資産の提供・公表

（ア）重要性分類Ⅲ以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

（イ）重要性分類Ⅲ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、誤公開を防がなければならない

（エ）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しなければならない。

キ　情報資産の廃棄等

（ア）情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の重要性分類に応じ、情報を復元できないように処置しなければならない。

（イ）情報資産の廃棄やリース返却等を行う者は、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）情報資産の廃棄やリース返却等を行う者は、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。

（エ）クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

（オ）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、熔解またはこれに準ずる方法にて廃棄しなければならない。

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、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

（2）サーバの冗長化

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、同一データを保持することが望ましい。

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することが望ましい。

（３）機器の電源

ア　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及び施設管理部門[1]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、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

イ　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　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　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　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正に管理しなければならない。

エ　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、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委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

（５）機器の定期保守及び修理

ア　教育情報システム管理者は、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事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、教育情報システム管理者は、事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

[1] 総務部財産運営課とする。

（6）施設外又は学校外への機器の設置

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、学校の敷地外にサーバ等の機器を設置する場合、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しなければならない。

（7）機器の廃棄等

ア　教育情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

イ　クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

４．２　管理区域（情報システム室等）の管理

（1）管理区域の構造等（教育委員会等のサーバ室にサーバを設置している場合）

ア　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、当該機器等の管理及び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。

イ　教育情報セキュリティ統括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 階に設けてはならない。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にすることが望ましい。

ウ　教育情報セキュリティ統括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。

エ　教育情報セキュリティ統括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、防火措置を講じなければならない。

オ　教育情報セキュリティ統括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、管理区域を囲む外壁等の床下開口部を全て塞ぐことが望ましい。

カ　教育情報セキュリティ統括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、機器及び電磁的記録媒体等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、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わなければならない。ただし、教職員が日常業務を行う職員室等に管理区域を設けている場合は、当該室内への立ち入りの規定に従うものとする。

イ　地方公共団体職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

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なければならない。

エ　情報システム管理者は、原則として、重要性分類Ⅱ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、事前に持ち込み申請を受けていないものに関して、当該情報システムに関連しないもの、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（３）機器等の搬入出

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、あらかじめ地方公共団体職員又は委託事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、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なければならない。

（４）学校にサーバを設置している場合

ア　管理区域の構造等

（ア）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。

（イ）教育情報セキュリティ統括責任者及び 教育情報システム管理者は、ネットワークの基幹機器及び重要な情報システムについて、サーバラックに固定した上で、サーバラックの施錠管理を行わなければならない。

（ウ）教育情報セキュリティ統括責任者及び教育情報システム管理者は、サーバラックを、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る場所に設置してはならない。

（エ）教育情報セキュリティ統括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。

（オ）教育情報セキュリティ統括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、防水措置等を講じなければならない。

（カ）教育情報セキュリティ統括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。

イ　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すること。

（イ）教育情報システム管理者は、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わなければならない。

（ウ）教職員は、児童生徒が管理区域に入室する場合、必要に応じて立ち入り区域を制限した上で、児童生徒に付き添うものとする。

（エ）委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

（オ）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教職員等が付き添うものとし、外見上教職員等と区別できる措置を講じなければならない。

ウ　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わせなければならない。

（イ）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、管理区域への入退室を許可された教職員を立ち会わせなければならない。

４．３　通信回線及び通信回線装置の管理

（１）教育情報セキュリティ統括責任者は、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、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

（２）教育情報セキュリティ統括責任者は、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、適切な管理を行わなければならない。

（３）教育情報セキュリティ統括責任者は、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、適正な回線を

選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

（4）教育情報セキュリティ統括責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

（5）教育情報セキュリティ統括責任者は、重要性分類Ⅱ以上の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

（6）教育情報セキュリティ統括責任者は、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じなければならない。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し、利用状況に応じて定期的に改修計画を行うこと。

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、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）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）を併用することが望ましい。

（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しなければならない。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へのアクセスについては、多要素認証を必須とすること。

（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。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ことが望ましい。

（6）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ることが望ましい。

（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ること。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こと。

（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 Web フィルタリング等の対策を講じなければならない。

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

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。

（2）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。

（3）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。

（4）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ることが望ましい。

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

4．6　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じなければならない。

（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しなければならない。

（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しなければならない。

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

ア　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、記録管理しなければならない。

イ　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、誤廃棄を予防しなければならない。

（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しなければならない。

（2）教職員等の情報セキュリティ意識醸成

ア　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らなければならない。

イ　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なければならない。

ウ　教育情報セキュリティ管理者は、教職員等が常に小中学校情報セキュリティポリシー及び実施手順を閲覧・確認できるように配慮しなければならない。

（3）端末等の持ち出し及び持ち込みの記録

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。

（4）教職員等への小中学校情報セキュリティポリシー等の遵守指導

ア　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、小中学校情報セキュリティポリシー等遵守すべき内容を理解・浸透するように指導を行わなければならない。

イ　教育情報セキュリティ管理者は、教職員等に対して、必要に応じて小中学校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、判断を仰がなければならない。

（6）インターネット接続及び電子メール利用の制限

ア　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しなければならない。

なおWebフィルタリングの設定について、教職員等から相談があった場合は、教育情報システム管理者に上申して、判断を仰がなければならない。

イ　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適切である。

（７）校内及び執務室での管理

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

ア　来校者の氏名及び入退時刻を記録しなければならない。

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

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

（８）自己点検の実施

ア　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わなければならない。

イ　教育情報セキュリティ管理者は、自己点検の結果を教育情報セキュリティ委員会に報告しなければならない。

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、以下の規定を遵守しなければならない。

（１）小中学校情報セキュリティポリシー等の遵守

教職員等は、小中学校情報セキュリティポリシー及びこれに基づく文書に定められている事項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。

（２）執務上での管理

ア　執務室の施錠管理

執務室にて教職員等が不在となる場合には、執務室を施錠しなければならない。

イ　来校者等への対応

来校者等を執務室に入れる場合には、教育情報セキュリティ管理者等の許可を求めなければならない。

ウ　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、適切な措置を講じなければならない。

（３）支給端末の取り扱い

ア　教職員等は、業務目的以外で支給端末を利用してはならない。

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

ウ　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、メモリ増設等の改造等のカスタマイズを無断でしてはならない。

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

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

カ　業務終了後と外出時には、電源を落とさなければならない。

キ　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、適正な措置を講じなければならない。

（４）支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

ア　教職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断を CISO が行った後に、業務上必要な場合は、教育情報セキュリティ統括責任者の定める実施手順に従い、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　教職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、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に関する規定を遵守しなければならない。

（５）モバイル端末や電磁的記録媒体等の持ち出し及び教育委員会・学校が構築・管理している環境の外部における情報処理作業の制限

ア　教職員等は、学校のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、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。

イ　教職員等は、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。

ウ　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。

（６）ID の取扱い

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

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。

ウ　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、教育情報セキュリティ統括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。

（７）パスワードの取扱い

教職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

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等は、同一のパスワードを複数のシステム間で用いてはならない。（シングルサインオンを除く）

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　教職員等間でパスワードを共有してはならない。（ただし、共有 ID に対するパスワードは除く）

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。

（８）IC カード等の取扱い

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

ア　認証に用いる IC カード等を、教職員等間で共有してはならない。

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いておかなければならない。

ウ　IC カード等を紛失した場合には、速やかに教育情報セキュリティ統括責任者及び教育情報システム管理者に通報し、指示に従わなければならない。

（９）外部電磁的記録媒体の取り扱い

ア　利用する外部電磁的記録媒体は教育委員会又は学校から支給された公式の媒体を使用しなければならない。その他の媒体の使用は禁止。

イ　外部電磁的記録媒体は、職員室の書庫等の鍵のかかる場所に施錠保管しなければならない。

（１０）電子メールの利用制限

ア　教職員等は、自動転送機能を用いて、電子メールを転送してはならない。

イ　教職員等は、業務上必要のない送信先に電子メールを送信してはならない。

ウ　教職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

エ　教職員等は、重要な電子メールを誤送信した場合、教育情報セキュリティ管理者に報告しなければならない。

オ　教職員等は、ウェブで利用できるフリーメールサービス等を教育情報セキュリティ統括責任者の許可無しに使用してはならない。

カ　情報ファイルを添付する場合には、パスワード設定等の対策を講じなければならない。その際、パスワードを同一メールに記載しないこと。

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

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

（１１）クラウドサービス、ソーシャルメディアサービス利用制限

ア　重要性分類Ⅱ以上の情報資産を、インターネットを通信経路としたパブリッククラウドサービスで取り扱ってはならない。なお、強固なアクセス制御による対策を講じたシステム構成の場合は、その限りではない。

イ　私的に契約したクラウドサービスを業務利用してはならない 。

ウ　ソーシャルメディアサービスを利用して、業務上知り得た情報を公開してはならない。

（１２）不正プログラム対策に関する教職員等の遵守事項

教職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

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

自動更新される設定の場合は、自動更新設定を変えてはならない。

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に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　教育情報セキュリティ統括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、すみやかに教育情報セキュリティ管理者に報告し、指示を仰がなければならない。また、以下の対応を行わなければならない。

（ア）パソコン等の端末の場合

有線 LAN につながる業務端末（校務用端末等）の場合は、LAN ケーブルの即時取り外しを行わなければならない。

（イ）モバイル端末の場合

無線 LAN につながる業務端末（指導者用端末及び学習者用端末）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わなければならない。

（ウ）指示があるまでは、端末の電源は切らずに保持しなければならない。

（１３）電子署名・暗号化

ア　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、送信しなければならない

イ　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。

（１４）無許可ソフトウェアの導入等の禁止

ア　教職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

イ　教職員等は、業務上の必要がある場合は、教育情報セキュリティ統括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　教職員等は、不正にコピーしたソフトウェアを利用してはならない。

（１５）機器構成の変更の制限

ア　教職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

イ　　教職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、教育情報セキュリティ統括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。

（１６）無許可でのネットワーク接続の禁止

教職員等は、教育情報セキュリティ統括責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

（１７）業務以外の目的でのウェブ閲覧の禁止

教職員等は、業務以外の目的でウェブを閲覧してはならない

（１８）外部からのアクセス等の制限

ア　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、教育情報セキュリティ統括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なければならない。

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

（１９）児童生徒への指導事項

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

ア　学習用途の利用限定

学習者用端末及び学習系クラウドサービスは学習目的で利用すること。

イ　利用者認証情報の秘匿管理

ID 及びパスワードは他の人に知られないようにすること。

ウ　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こと。

エ　端末のソフトウェアに関するセキュリティ機能の設定変更禁止

利用する端末のセキュリティ機能の設定を、許可なく変更してはならないこと。

オ　学習系情報は学習系クラウドに保管

端末で生成した情報の保存先を学習系クラウドに指定できる機能がある場合には、この機能を利用して原則学習系クラウドに保管し、学習者用端末にローカル保存は必要最小限とすること。

カ　無断で外部ソフトウェアのインストール禁止

無断で外部ソフトウェアをインストールしないようにすること。

キ　コミュニケーションツールの利用制限

学校から許可されたコミュニケーションツール（SNS，チャット等）のみを利用すること。

ク　ウイルス感染が疑われる場合の報告

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

ケ　端末の安全な取り扱い

学習用端末は大事に取り扱い、盗難・紛失・破損等に注意すること。

コ　私物端末利用禁止

私物端末など承認されていない端末を学校に持ち込んで、学校のネットワークにつながないこと。

（２０）異動・退職時等の遵守事項

教職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産（紙情報、データの格納された端末、外部記録媒体等）を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

（２１）非常勤及び臨時職員等への対応

ア　小中学校情報セキュリティポリシー等の遵守

教育情報セキュリティ管理者は、非常勤及び臨時職員等に対し、採用時に小中学校情報セキュリティポリシー等のうち、非常勤及び臨時職員等が守るべき内容を理解させ、また実施及び遵守させなければならない。

イ　小中学校情報セキュリティポリシー等の遵守に対する同意

教育情報セキュリティ管理者は、非常勤及び臨時職員等の採用の際、必要に応じ、小中学校情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

ウ　インターネット接続及び電子メール使用等の制限

教育情報セキュリティ管理者は、非常勤及び臨時職員等にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの

使用等が不要の場合、これを利用できないようにしなければならない。

（２２）小中学校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、教職員等が常に小中学校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。

（２３）委託事業者に対する説明

教育情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を事業者に発注する場合、再委託事業者も含めて、小中学校情報セキュリティポリシー等のうち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。

５．３　教育委員会事務局職員の遵守事項

（１）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、以下の規定を遵守しなければならない。

ア　小中学校情報セキュリティポリシー等の遵守

イ　業務以外の目的での使用の禁止

ウ　校務用端末による外部における情報処理作業の禁止

エ　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

オ　知りえた情報の秘匿

カ　業務を離れる場合の遵守事項

（２）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らさない。

５．４　研修・訓練

（１）情報セキュリティに関する研修・訓練

ア　CISO は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

イ　CISO は、定期的にクラウドサービスを利用する教職員等及び委託先を含む関係者の情報セキュリティに関する意識向上、教育及び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う。

イ　研修計画において、教職員等は、年１回を目安に情報セキュリティ研修を受講でき

るようにすることが望ましい。

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

エ　研修は、教育情報セキュリティ統括責任者、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、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。

オ　教育情報セキュリティ管理者は、所管する学校等の研修の実施状況を記録し、教育情報セキュリティ統括責任者及び教育情報セキュリティ責任者に対して、報告しなければならない。

カ　教育情報セキュリティ統括責任者は、研修の実施状況を分析、評価し、CISO に情報セキュリティ対策に関する研修の実施状況について報告しなければならない。

キ　CISO は、毎年度１回、教育情報セキュリティ委員会に対して、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に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

（４）研修・訓練への参加

全ての教職員等は、定められた研修・訓練に参加しなければならない。

５．５　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

ア　教職員等は、情報セキュリティインシデントを認知した場合、速やかに教育情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口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、速やかに教育情報セキュリティ統括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、報告のあった情報セキュリティインシデントについて、日進市等の関係機関に必要な連絡を行うとともに、CISO 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　教育情報セキュリティ責任者は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象者に報告しなければならない。

（２）教職員等の報告義務

ア　教職員等は、小中学校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統括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と教育情報セキュリティ統括責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

（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

ア　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、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、速やかに教育情報セキュリティ統括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CISO 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　CISO 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することが望ましい。

オ　教育情報セキュリティ統括責任者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を検討しなければならない。

（４）　情報セキュリティインシデントの報告内容

ア　教職員等から教育情報セキュリティ管理者への報告は、以下の内容を含むものとする。

(1)　件名
(2)　判明した日時
(3)　発生した日時
(4)　通報者
(5)　事件事故等の内容
(6)　漏えいした情報
(7)　想定される原因
(8)　事件事故等への対応
(9)　復旧方針

イ　教育情報セキュリティ統括責任者は、クラウドサービス事業者からの報告につい

ては、情報セキュリティインシデント発生時の報告手順を定め、クラウドサービス事業者の状況を適正かつ速やかに確認できるよう、インシデント発生時の報告に必要な要件を契約やSLA に定めるか、クラウドサービスの利用前に利用規約等を確認すること

（5）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、CISO 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教育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、CISO に報告しなければならない。

オ　CISO 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。

（6）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、実施手順に反映しなければならない。

6　技術的セキュリティ

6．1　コンピュータ及びネットワークの設定管理

（1）文書サーバの設定等

ア　教育情報システム管理者は、教職員等が使用できる文書サーバの容量を設定し、教職員等に周知しなければならない。

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、教職員等が他の学校等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

ウ　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

ア　教育情報セキュリティ統括責任者及び教育情報システム管理者は、システムのデータベースやファイルサーバ等に記録された情報について、校務系情報及び校務外部接続系情報については、サーバの冗長化対策に関わらず、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。また、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ことが望ましい。

イ　教育情報セキュリティ統括責任者及び教育情報システム管理者は、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その機能の仕様が本市の求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

（3）ログの取得等

ア　教育情報セキュリティ統括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、一定の期間保存しなければならない。

イ　教育情報セキュリティ統括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、適正にログを管理しなければならない。

ウ　教育情報セキュリティ統括責任者及び教育情報システム管理者は、取得したログを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。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

エ　教育情報セキュリティ統括責任者及び教育情報システム管理者は、監査及びデジ

タルフォレンジック[2]に必要となるクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

（4）ネットワークの接続制御、経路制御等

ア　教育情報セキュリティ統括責任者は、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　教育情報セキュリティ統括責任者は、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正なアクセス制御を施さなければならない。

（5）外部の者が利用できるシステムの分離等

教育情報システム管理者は、保護者等の外部の者が利用できるシステム等がある場合、重要性が高い情報、特に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こと。

（6）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 及び教育情報セキュリティ統括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　教育情報セキュリティ統括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、庁内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。

[2] 電子データを調査分析することで事実解明及び証拠保存を行うための技術のこと。

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、教育情報セキュリティ統括責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（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

ア　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しなければならない。

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。

（8）複合機のセキュリティ管理

ア　教育情報セキュリティ統括責任者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

イ　教育情報セキュリティ統括責任者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

ウ　教育情報セキュリティ統括責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消する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。

（9）IoT 機器を含む特定用途機器のセキュリティ管理

教育情報セキュリティ統括責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

（１０）無線 LAN 及びネットワークの盗聴対策

ア　教育情報セキュリティ統括責任者は、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なければならない。

イ　教育情報セキュリティ統括責任者は、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じなければならない。

（１１）電子メールのセキュリティ管理

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

イ　教育情報セキュリティ統括責任者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

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

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

オ　教育情報セキュリティ統括責任者は、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委託事業者の作業員による電子メールアドレス利用について、委託事業者との間で利用方法を取り決めなければならない。

カ　教育情報セキュリティ統括責任者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置を講ずることが望ましい。

（１２）ウェブ会議サービスの利用時の対策

ア　教育情報セキュリティ統括責任者は、ウェブ会議を適切に利用するための利用手順を定めなければならない。

イ　教職員等は、学校の定める利用手順に従い、ウェブ会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

ウ　教職員等は、ウェブ会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

エ　教職員等は、外部からウェブ会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

６．２　アクセス制御

（１）アクセス制御等

教育情報セキュリティ統括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、システム上制限しなければならない。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こと。

（２）教職員等による外部からのアクセス等の制限

ア　教育情報セキュリティ統括責任者は、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しなければならない。

イ　教育情報セキュリティ統括責任者は、民間事業者等の外部組織からの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。

ウ　教育情報セキュリティ統括責任者は、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じなければならない。

エ　教育情報セキュリティ統括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じなければならない。

オ　教育情報セキュリティ統括責任者は、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、パスワード及び生体認証に係る情報等の認証情報並びに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なければならない。

（３）自動識別の設定

教育情報セキュリティ統括責任者及び教育情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定することが望ましい。

（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しなければならない。

（５）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。

６．３　システム開発、導入、保守等

（１）情報システムの調達

ア　教育情報セキュリティ統括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　教育情報セキュリティ統括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、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は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

（ウ）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、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

（イ）教育情報システム管理者は、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、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

（４）システム開発・保守に関連する資料等の整備・保管

ア　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正に整備・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、情報システムに係るソースコードを適正な方法で保管しなければならない。

（５）情報システムにおける入出力データの正確性の確保

ア　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、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（６）情報システムの変更管理

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

（7）開発・保守用のソフトウェアの更新等

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

（8）システム更新又は統合時の検証等

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

6．4　不正プログラム対策

（1）教育情報セキュリティ統括責任者の措置事項

教育情報セキュリティ統括責任者は、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においてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

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においてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

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、必要に応じ職員等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。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

ク　仮想マシン[3]を設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければな

[3] ソフトウェアにより疑似的に再現されたコンピュータのこと。

らない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのかクラウドサービス事業者に報告を求めなければならない。

（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　教育情報システム管理者は、その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。

イ　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。

ウ　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。

エ　インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、学校が管理している媒体以外を教職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

オ　不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、教育情報システム管理者が許可した教職員を除く教職員等に当該権限を付与してはならない。

６．５　不正アクセス対策

（1）教育情報セキュリティ統括責任者の措置事項

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

ア　使用されていないポート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、情報セキュリティ統括責任者及び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することが望ましい。

オ　教育情報セキュリティ統括責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

カ　本市が定めたクラウドサービスの利用に関するポリシー（小中学校情報セキュリ

ティポリシー）におけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認しなければならない。

キ　クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証等、強固な認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。

ク　パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、本市が定めたクラウドサービスの利用に関するポリシー（小中学校情報セキュリティポリシー）を満たすことを確認しなければならない。

（2）攻撃への対処

CISO 及び教育情報セキュリティ統括責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。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）サービス不能攻撃

教育情報セキュリティ統括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。

（4）標的型攻撃

教育情報セキュリティ統括責任者及び教育情報システム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

６．６　セキュリティ情報の収集

（1）セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

ア　教育情報セキュリティ統括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。

イ　教育情報セキュリティ統括責任者及び教育情報システム管理者は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理

内容について情報を求め、学校の業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認しなければならない。

（2）不正プログラム等のセキュリティ情報の収集・周知

教育情報セキュリティ統括責任者は、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、教職員等に周知しなければならない。

（3）情報セキュリティに関する情報の収集及び共有

教育情報セキュリティ統括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

7．1　情報システムの監視

（1）教育情報セキュリティ統括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。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）などの対策を講じなければならない。

（2）教育情報セキュリティ統括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。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならない。

（3）教育情報セキュリティ統括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。

（4）教育情報セキュリティ統括責任者及び教育情報システム管理者は、重要性分類Ⅲ以上の情報資産を格納する学習系システムを常時監視することが望ましい。

（5）暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入することが望ましい。

（6）教育情報セキュリティ統括責任者及び教育情報システム管理者は、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

（7）教育情報セキュリティ統括責任者及び教育情報システム管理者は、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

（8）教育情報セキュリティ統括責任者及び教育情報システム管理者は、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。

ア　サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

イ　クラウドサービス利用の終了手順

ウ　バックアップ及び復旧

（9）内部からの攻撃監視

教育情報セキュリティ統括責任者及び教育情報システム管理者は、教職員等及び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。

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

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　教育情報セキュリティ統括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しなければならない。

ウ　教育情報セキュリティ統括責任者、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。

（2）情報システム仕様書等の管理

教育情報セキュリティ統括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者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

（3）障害記録の管理

教育情報セキュリティ統括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、適切に保存しなければならない。

（4）記録の保存

CISO 及び教育情報セキュリティ統括責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

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

ア　教育情報セキュリティ統括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 の取扱い等の方法を定めなければならない。

イ 教育情報セキュリティ統括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。

（2）パスワードに関する情報の管理

ア　教育情報セキュリティ統括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　教育情報セキュリティ統括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なければならない。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。

７．４　IC カード等の取扱い

（１）IC カード等の取扱い

ア　教育情報セキュリティ統括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しなければならない。

イ　教育情報セキュリティ統括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、破砕するなど復元不可能な処理を行った上で廃棄しなければならない

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

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/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、同一の教育委員会等の組織にて一元管理することが望ましい。

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、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。

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行うことが望ましい。

７．６　特権を付与された ID の管理等

（1）教育情報セキュリティ統括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。

（2）教育情報セキュリティ統括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、教育情報セキュリティ統括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。

（3）CISO は、代行者を認めた場合、速やかに教育情報セキュリティ統括責任者、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。

（4）教育情報セキュリティ統括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。

（5）教育情報セキュリティ統括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。

（6）教育情報セキュリティ統括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しなければならない

（7）教育情報セキュリティ統括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 のログ監視を行うことが望ましい。

７．７　小中学校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、小中学校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 及び教育情報セキュリティ統括責任者に報告しなければならない。

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

ウ　教育情報セキュリティ統括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小中学校情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

（２）パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

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

教育情報セキュリティ統括責任者は、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なければならない。

（４）教職員等による不正アクセスの管理

教育情報セキュリティ統括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、適切な処置を求めなければならない。

７．８　専門家の支援体制等

（１）専門家の支援体制

教育情報セキュリティ統括責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

（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、教育情報セキュリティ統括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。

７．９　侵害時の対応等

（１）緊急時対応計画の策定

ア　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、小中学校情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

イ　CISO 又は情報セキュリティ委員会は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

（２）緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

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・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と小中学校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。

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、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用する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、例外措置を講じることができる。

（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、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに 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正に保管し、定期的に申請状況を確認しなければならない。

７．１１　法令遵守

（１）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　日進市個人情報の保護に関する法律施行条例（令和 4 年日進市条例第 27 号）

ケ　日進市文書管理規程（平成 18 年日進市訓令第 5 号）

（２）教育情報セキュリティ統括責任者及び教育情報システム管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

７．１２　懲戒処分等

（１）懲戒処分

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

（２）違反時の対応

教職員等の小中学校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　教育情報セキュリティ統括責任者が違反を確認した場合は、教育情報セキュリティ統括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、適正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教育情報セキュリティ統括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、適正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、教育情報セキュリティ統括責任者は、当該教職員等の教育ネットワーク又は教育情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、教育情報セキュリティ統括責任者は、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しなければならない。

8　業務委託と外部サービス[4]の利用

8．1　業務委託

（1）委託事業者の選定基準

ア　教育情報セキュリティ管理者は、委託事業者の選定にあたり、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　教育情報セキュリティ管理者は、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、委託事業者を選定することが望ましい。

（2）契約項目

重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

ア　小中学校情報セキュリティポリシー及び小中学校情報セキュリティ実施手順の遵守

イ　委託事業者の責任者、委託内容、作業者の所属、作業場所の特定

ウ　提供されるサービスレベルの保証

エ　委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法

[4] 一般の業者等の学校外の組織が情報システムの一部又は全部の機能を提供するクラウドサービス、ホスティングサービス、ハウジングサービス、ソーシャルメディアサービス等をいう。

オ　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委託事業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　小中学校情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

（3）確認・措置等

教育情報セキュリティ管理者は、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を実施しなければならない。また、その内容を情報セキュリティ統括責任者に報告するとともに、その重要度に応じて CISO に報告しなければならない。

（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、小中学校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。

9　SaaS 型パブリッククラウドサービスの利用

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

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 の管理について、「7．6特権を付与された ID の管理等」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、情報資産毎に、許可された クラウドを利用する教職員等及び児童生徒 のみがアクセスできる環境を設定しなければならない。

（3）クラウドに保管するデータの暗号化

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 「４．１　サーバ等の管理 」 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、「４．２　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)」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、クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）にあたり、セキュリティを確保した対応となっているか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。なお、当該確認に当たっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

（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することが望ましい。

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 、「 ４．１　サーバ等の管理（２）サーバの冗長化 」 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 及び復旧手順 について、 「６．１　コンピュータ及びネットワークの設定管理（２)）バックアップの実施」 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、「６．１　コンピュータ及びネットワークの設定管理（３）ログの取得等」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クラウドを利用する教職員等及び児童生徒側端末について、保管するデータの外部流出、改ざん等から保護するために必要な措置を講じなければならない。

イ　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、クラウドを利用する教職員等及び児童生徒への教育や入口対策を講じなければならない。

（１１）クラウド事業者従業員の人的セキュリティ対策

ア　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 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）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

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及び利用者アカウント情報が不用意に残置されないよう、適切に破棄するための流れについてサービス提供定款や契約書面上で確認または合意しておかなければならない。

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ておかなければならない。

ウ　クラウド利用者は、クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

（１３）クラウドサービス要件基準を満たす配慮を含めたネットワーク設計

クラウド利用者は、利用するクラウドサービスの要件規準を確認し、要件規準を満たすネットワークを設計しなければならない。

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

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。

（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の設置

（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、充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と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と及びインシデント対応フローを検証し、インシデントに備えた組織体制を整備しなければ

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すること。

エ　クラウド利用者は、クラウド事業者において個人情報の適切な管理が行われているか確認するとともに、確認した項目については、調達時においてサービスの過剰な排除にならないよう留意した上で、契約要件等として定めなければならない。

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

ア　教職員等は、ID・パスワードについて秘匿管理を行わなければならない。

イ　教職員等は、多要素認証に必要な要素（知識、生体、物理）についても適切に管理を行わなければならない。もし該当要素が流出等したと考えられる場合には、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。

（2）モバイル端末持ち歩きリスク

教職員等は、クラウドサービスにアクセスする際に活用するモバイル端末について、紛失・盗難を避けるよう、適切に管理しなければならない。

（3）重要性分類に基づく情報管理

パブリッククラウド上で重要な情報（重要性分類 II 以上）を取り扱う際には、多要素認証を含む強固なアクセス制御による対策を講じる必要がある。

（4） 学校外からのパブリッククラウド利用

ア　教職員等は、学校外からクラウドサービスを利用する際、情報資産の取扱いをクラウドサービス上のみで行うことを原則とする。

イ　クラウドサービスから端末にファイルをダウンロードする際は、情報資産の外部持ち出しに基づく安全管理措置として、端末の安全性を事前に確認するとともに、作業が終わり次第当該端末から情報資産をすみやかに消去しなければならない。

（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

ア　教職員等は、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てクラウドサービスを利用している場合には、クラウドサービスを学習用途と校務用途で適切に使い分けるよう、共有先やダウンロード方法等の運用ルールについてあらかじめ確認し、適切に運用しなければならない。

イ　教職員等は、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にてクラウドサービスを利用している場合には、クラウドサービスを学習用途と校務用途で使い分けるよう、適切に運用しなければならない。

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

ア　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順

（2）約款による外部サービスの利用における対策の実施

教職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で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。

９．５　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、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　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、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　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　情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

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）委託事業者に対する監査

ア　事業者に業務委託を行っている場合、情報セキュリティ監査統括責任者は委託事業者（再委託事業者を含む。）に対して、小中学校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。

イ　クラウドサービスを利用している場合は、クラウドサービス事業者における小中学校情報セキュリティポリシーの遵守について、必要に応じて定期的に監査を行わなければならない。クラウドサービス事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書をこの証拠とすることもできる。

（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正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。なお、横断的に改善が必要な事項については、教育情報セキュリティ統括責任者に対し、当該事項への対処を指示しなければならない。

（8）小中学校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、監査結果を小中学校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。

１０．２　自己点検

（1）実施方法

ア　教育情報セキュリティ統括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、所管する部における小中学校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

教育情報セキュリティ統括責任者、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しなければならない。

（3）自己点検結果の活用

ア　教職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

イ　情報セキュリティ委員会は、この点検結果を小中学校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。

１０．３　小中学校情報セキュリティポリシー及び関係規程等の見直し

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、小中学校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。