柏市教育情報セキュリティ対策基準

1　対象範囲及び用語説明

(1) 行政機関等の範囲

本対策基準が適用される行政機関等は，内部部局，教育委員会及び学校（柏市立の小学校，中学校及び高等学校を言う。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

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

(3) 用語説明

本対策基準における用語は，以下の通りとする。

用語	定義
個人情報	柏市個人情報保護条例（平成１６年条例第１１号）第２条第２項に規定する定義（個人に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別できるもの（他の情報と照合することができ，

	それにより特定の個人を識別することができることとなるものを含む。）をいう。）によるものとする。
校務系情報	児童生徒の成績，出欠席及びその理由，健康診断結果，指導要録，教員の個人情報など，学校が保有する情報資産のうち，それら情報を学校・学級の管理運営，学習指導，生徒指導，生活指導等に活用することを想定しており，かつ，当該情報に児童生徒がアクセスすることが想定されていない情報
校務外部接続系情報	校務系情報のうち，保護者メールや学校ホームページ等インターネット接続を前提とした校務で利用される情報
学習系情報	児童生徒のワークシート，作品など，学校が保有する情報資産のうち，それら情報を学校における教育活動において活用することを想定しており，かつ当該情報に教員及び児童生徒がアクセスすることが想定されている情報
校務用端末	校務系情報にアクセス可能な端末
校務外部接続用端末	校務外部接続系情報にアクセス可能な端末
学習者用端末	学習系情報にアクセス可能な端末で，児童生徒が利用する端末
指導者用端末	学習系情報にアクセス可能な端末で，教員のみが利用可能な端末
校務系システム	校務系ネットワーク，校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム 及び，校務系情報を扱う上で，適切なアクセス権が設定された領域で利用されるシステム
校務外部接続系システム	校務外部接続系ネットワーク，メールサーバ，ホームページ運用サーバ（CMS）及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム
学習系システム	学習系ネットワーク，学習系サーバ，学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム 及び，学習系情報を扱う上で，適切なアクセス権が設定された領域で利用されるシステム
教育情報システム	校務系システム，校務外部接続系システム及び学習系システムを合わせた総称
校務系サーバ	校務系情報を取り扱うサーバ
校務外部接続系サーバ	校務外部接続系情報を取り扱うサーバ
学習系サーバ	学習系情報を取り扱うサーバ
クラウドサービス	従来は手元のコンピュータに導入して利用していたようなソフトウェアやデータ，あるいはそれらを提供するための技術基盤（サーバなど）を，インターネットなどのネットワークを通じて必要に応じて利用者に提供するサービス。 どのような資源をサービス化するかによって「IaaS（Infrastructure as a Service）」，「PaaS（Platform as a Service）」，「SaaS（Software as a Service）」の 3 つに分類される。

教育システムにおけるクラウドサービス	学校や教職員や児童生徒が，必要な時に必要なだけ自由にリソースを特定のハードウェアや通信環境に依存せずに利用できる ICT サービス
クラウド事業者	クラウドサービスを利用して教育システム用のクラウドサービスを提供する事業者
クラウド利用者	校務系システム，学習系システムにおいてクラウドサービスを利用する場合，クラウドサービスの選定・契約の主体となる教育委員会等をクラウド利用者と言う。一方，教職員や児童生徒は，別途，「エンドユーザ」として整理する

2　組織体制

(1) 最高教育情報セキュリティ責任者（CISO: Chief Information Security Officer，以下「CISO」という。）

ア　副市長を，CISO とする。CISO は，本市における全ての教育ネットワーク，教育情報システム等の情報資産の管理及び教育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，教育情報セキュリティに関する専門的な知識及び経験を有した専門家を最高教育情報セキュリティアドバイザーとして置き，その業務内容を定めるものとする。

(2) 統括教育情報セキュリティ責任者

ア　教育長を，CISO 直属の統括教育情報セキュリティ責任者とする。

イ　統括教育情報セキュリティ責任者は CISO を補佐しなければならない。

(3) 教育情報セキュリティ責任者

ア　指導課長を，教育情報セキュリティ責任者とする。

イ　教育情報セキュリティ責任者は，本市の全ての教育ネットワークにおける開発，設定の変更，運用，見直し等を行う権限及び責任を有する。

ウ　教育情報セキュリティ責任者は，本市の全ての教育ネットワークにおける教育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責任者は，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，教育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，統括教育情報セキュリティ責任者の指示に従うものとする。総括教育情報セキュリティ責任者が不在の場合には，CISO の指示に従い，CISO が不在の場合には自らの判断に基づき，必要かつ十分な措置を行う権限及び責任を有する。

カ　教育情報セキュリティ責任者は，本市の共通的な教育ネットワーク，教育情報システム及び情報資産に関する教育情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

キ　教育情報セキュリティ責任者は，緊急時等の円滑な情報共有を図るため，CISO，統括教育情報セキュリティ責任者，教育情報セキュリティ管理者，教育情報システム管理者，教育情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

ク　統括教育情報セキュリティ責任者は，緊急時にはCISOに早急に報告を行うとともに，回復のための対策を講じなければならない。

(4) 教育情報セキュリティ管理者

ア　学校教育部の各所属長及び各学校の校長を，教育情報セキュリティ管理者とする。

イ　教育情報セキュリティ管理者は，当該所属又は当該学校の教育情報セキュリティ対策に関する権限及び責任を有する。

ウ　教育情報セキュリティ管理者は，当該所属又は当該学校において，情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には，教育情報セキュリティ責任者，統括教育情報セキュリティ責任者及びCISOへ速やかに報告を行い，指示を仰がなければならない。

(5) 教育情報システム管理者

ア　指導課長を，当該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教育情報セキュリティ実施手順の維持・管理を行う。

オ　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対する侵害又は侵害の恐れのある場合には，教育情報セキュリティ責任者へ速やかに報告を行い，指示を仰ぐものとする。

(6) 教育情報システム担当者

ア　指導課担当を，教育情報システムに関する教育情報システム担当者とする。

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

(7) 教育情報セキュリティ委員会

ア　本市の教育情報セキュリティ対策を統一的に行うため，教育情報セキュリティ委員会を設置し，教育情報セキュリティ委員会において，教育情報セキュリティポリシー等，教育情報セキュリティに関する重要な事項を決定する。

イ　教育情報セキュリティ委員会は，毎年度，本市における教育情報セキュリティ対策の改善計画を策定し，その実施状況を確認しなければならない。

ウ　学校教育部長を，教育情報セキュリティ委員会委員長とする。

(8) 兼務の禁止

ア　教育情報セキュリティ対策の実施において，やむを得ない場合を除き，承認又は許可の申請を行う者とその承認者又は許可者は，同じ者が兼務してはならない。

イ　監査を受ける者とその監査を実施する者は，やむを得ない場合を除き，同じ者が兼務してはならない。

(9) 教育情報セキュリティに関する統一的な窓口の設置

ア　CISO は，教育情報セキュリティインシデントの統一的な窓口の機能を有する組織を整備し，教育情報セキュリティインシデントについて部局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する。

イ　CISO による教育情報セキュリティ戦略の意思決定が行われた際には，その内容を関係部局等に提供する。

ウ　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教育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。

3　情報資産の分類と管理方法

(1) 情報資産の分類

教育情報セキュリティにおける情報資産は，その重要性に基づき以下に分類する。

重要性分類
Ⅰ　セキュリティ侵害が教職員又は児童生徒及び保護者の生命，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

重要性分類の例示（下記に限定されないが，例示的に運用に供すること。

また，持ち出しの制限がない分類の例示においても，個人情報が含まれる場合は，持ち出しの制限の分類とみなすものとする。）

重要性分類	情報資産の例示		
	校務系		学習系/公開系
Ⅰ	・指導要録原本 ・教職員の人事方法 ・入学者選抜問題 ・教育情報システム仕様書		
Ⅱ	○学籍関係 ・卒業証書授与台帳 ・転退学受付（整理）簿 ・転入学受付（整理）簿 ・就学児童・生徒異動報告書 ・休学・退学願等受付（整理）簿 ・教科用図書給付児童・生徒名簿 ・要・準要保護児童・生徒認定台帳 ・その他校内就学援助関係書類 ○成績関係 ・通知表 ・評定一覧表 ・進級・卒業認定資料 ・定期考査・テスト等の答案用紙 （児童・生徒が記入したもの） ・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	○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，メールアドレス，住所，生年月日，性別等の基本情報を含むもの） ○健康関係 ・健康診断表 ・歯の検査表 ・心臓管理棟医療情報 ・学校生活管理指導票 ・児童・生徒等健康調査票 ・児童・生徒の健康保険等被保険者証の写 ・健康診断に関する表簿 ・就学時健康診断表 ○教職員に割り当てた機密性の高い情報 ・情報システムログイン ID/PW 管理台帳 ・情報端末ログイン ID/PW 管理台帳 ○その他 ・給食関係書類・寄宿関係書類 ○名簿等	□学習系 ○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 ・学習用端末ログイン ID/PW 管理台帳

	（学校生活支援シート） ・個別指導計画 ・家庭訪問記録・個別面談記録 ・教務手帳 ・週ごとの指導計画 （個人情報が含まれるもの） ○進路関係 ・調査書 ・推薦書 ・公立高校入学者選抜に係る成績一覧表 ・入学者選抜に関する表簿（願書等） ・私立高校入試に係る事前相談資料 ・卒業生進路先一覧等 ・進路希望調査 ・進路判定会議資料 ・進路指導記録簿	・児童生徒名簿 ・保護者緊急連絡網 ・児童生徒の住所録 ・PTA 会員名簿 ・職員緊急連絡網・職員住所録 ・委員会名簿 ・PTA 役員連絡網 ○各種帳票ファイル ・指導要録作成システム等, データの入っていない帳票	
Ⅲ	○児童生徒の氏名 ・出席簿 ・名列表 ・座席表 ・児童生徒役員会名簿	○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	□学習系 ○学校運営関係 ・授業用教材 ・生徒用配布プリント ○児童生徒の学習系情報 ・児童生徒の学習記録（確認テスト，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			□公開系 ○学校運営関係 ・学校・学園要覧

			・学校紹介パンフレット ・使用教科書一覧 ・教育課程編成表 ・学校設定科目の届け出 ・特色紹介冊子原稿 ・学校徴収金会計簿（学年費，教育振興費等） ・学校行事実施計画（避難訓練，体育祭実施計画等） ・保護者への配布文書文例 ・各種届雛形・校務分掌表 ・PTA 資料 ・学園・学校・学年・学級だより ・学校・学園ホームページ掲載情報 ・学校行事のしおり 〇学校活動の記録 ※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）

情報資産の取扱い例	情報資産の重要性分類			
	Ⅰ	Ⅱ	Ⅲ	Ⅳ
複製・配布	必要以上の複製及び配布禁止	同左	同左	

組織外部への持ち出し制限	対策基準に準拠していることを確認した上で業務遂行上必要な場合には，情報セキュリティ管理者の判断で持ち出しを可	同左	情報セキュリティ管理者の包括的承認で可	
端末制限	支給以外の端末での作業の原則禁止	同左	同左	
情報の組織外部への送信	限定されたアクセスの措置がとられていること	同左	同左	
情報資産の運搬	鍵付きケースへの格納	同左	同左	
組織外部での情報処理	禁止	安全管理措置の規定が必要	同左	
使用する磁気媒体記録	施錠可能な場所への保管	同左	同左	
情報資産の保管	・耐火・耐熱・耐水を講じた施錠可能な場所に保管（電子データの場合もこれらの対策に準じたサーバに保管） ・情報資産を格納するサーバのバックアップ ・6か月以上のログ保管 ・サーバの冗長化 ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁記録媒体の持ち込み禁止	同左	・耐火・耐熱・耐水を講じた施錠可能な場所に保管（電子データの場合もこれらの対策に準じたサーバに保管） ・一定期間以上のログ保管 ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁記録媒体の持ち込み禁止	
情報資産の破棄	電磁記録媒体の初期化，復元できないようにして破棄	同左	同左	

(2) 情報資産の管理

ア　管理責任

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

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

イ　情報の作成

(ｱ) 教職員は，業務上必要のない情報を作成してはならない。

(ｲ) 情報を作成する者は，作成途上の情報についても，紛失や流出等を防止しなければならない。また，情報の作成途上で不要になった場合は，当該情報を消去しなければならない。

ウ　情報資産の入手

(ｱ) 学校内の者が作成した情報資産を入手した者は，入手元の情報資産の分類に基づいた取扱いをしなければならない。

(ｲ) 学校外の者が作成した情報資産を入手した者は，(1)の分類に基づき，当該情報の分類と取扱制限を定めなければならない。

(ｳ) 情報資産を入手した者は，その情報資産の分類が不明な場合，教育情報セキュリティ管理者に判断を仰がなければならない。

エ　情報資産の利用

(ｱ) 情報資産を利用する者は，業務以外の目的に情報資産を利用してはならない。

(ｲ) 情報資産を利用する者は，情報資産の分類に応じ，適切な取扱いをしなければならない。

(ｳ) 情報資産を利用する者は，電磁的記録媒体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。

オ　情報資産の保管

(ｱ) 情報資産は，情報資産の分類に従って，適切に保管しなければならない。

(ｲ) 情報資産の保管にクラウドサービスを利用する場合はサービスの機能として自然災害対策がなされていることを確認すること。

カ　情報の送信

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者は，必要に応じ暗号化又はパスワード設定を行わなければならない。

キ　情報資産の廃棄

重要性分類Ⅲ以上の情報資産を廃棄する者は，情報を記録している電磁的記録媒体が不要になった場合，電磁的記録媒体の初期化等，情報を復元できないように処置した上で廃棄しなければならない。

4　物理的セキュリティ

4－1　サーバ等の管理

本項はサーバ等を自己設備として設置運用するものに適用する。クラウ

ドサービスの場合は「9 項　クラウドサービスの利用」で規定する。

(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切に固定する等，必要な措置を講じなければならない。

(2) サーバの冗長化

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について，格納しているデータの重要度に応じて二重化し障害発生時にも業務への支障を最小限にとどめなければならない。

(3) 機器の電源

ア　教育情報システム管理者は，統括教育情報セキュリティ責任者及び施設管理部門と連携し，校務系サーバ等の機器の電源について，停電等による電源供給の停止に備え，当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

イ　教育情報システム管理者は，統括教育情報セキュリティ責任者及び施設管理部門と連携し，落雷等による過電流に対して，サーバ等の機器を保護するための措置を講じなければならない。

(4) 通信ケーブル等の配線

ア　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，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　教育情報システム管理者は，ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

(5) 機器の修理

教育情報システム管理者は，電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合，内容を消去した状態で行わせなければならない。内容を消去できない場合，教育情報システム管理者は，外部の事業者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ほか，秘密保持体制の確認等などを行わなければならない。

(6) 施設外又は学校庁外への機器の設置

教育情報システム管理者は，施設外又は学校外にサーバ等の機器を設置する場合，CISO の承認を得なければならない。なお，教育情報システム管理者は，当該装置に対して適切な管理を行うものとする。

(7) 機器の廃棄等

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

４－２　管理区域(サーバ室等)の管理

(1) 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「サーバ室」という。）や電磁的記録媒体の保管庫をいう。

イ　教育情報システム管理者は，管理区域を外部からの侵入が容易にできないよう措置を講じなければならない。ただし，管理区域への設置が不可能なサーバ類に関しては可能な限りのセキュリティ対策を施すものとする。

ウ　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　教育情報システム管理者は，サーバ室内の機器等に，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。

オ　教育情報システム管理者は，管理区域に配置する消火薬剤や消防用設備等が，機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

(2) 管理区域の入退室管理等

ア　教育情報システム管理者は，管理区域への入退室を許可された者のみに制限し，入退室管理簿の記載による入退室管理を行わなければならない。

イ　地方公共団体職員等及び外部委託事業者が，管理区域に入室を許可する場合，これらの者に身分証明書等を携帯させ，必要に応じ，その提示を求めなければならない。

ウ　教育情報システム管理者は，外部からの訪問者が管理区域に入る場合には，必要に応じて立ち入り区域を制限した上で，管理区域への入退室を許可された職員等が付き添うものとし，外見上職員等と区別できる措置を講じなければならない。

エ　教育情報システム管理者は，重要性分類Ⅲ以上の情報資産を扱うシステムを設置している管理区域について，当該情報システムに関連しないコンピュータ，モバイル端末，通信回線装置，電磁的記録媒体等を接続でき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，あらかじめ職員又は委託した業者に確認を行わせなければならない。

イ　教育情報システム管理者は，サーバ室の機器等の搬入出について，職員を立ち会わせなければならない。

４－３　通信回線及び通信回線装置の管理

ア　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，適切に管理しなければならない。また，通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。及び，最新の管理状況を適宜教育情報セキュリティ責任者にほう報告しなければならない。

イ　教育情報セキュリティ責任者は，外部へのネットワーク接続を必要最低限に限定し，できる限り接続ポイントを減らさなければならない。

ウ　教育情報セキュリティ責任者は，重要性分類Ⅲ以上の情報資産を取り扱う情報システムに通信回線を接続する場合，必要なセキュリティ水準を検討の上，適切な回線を選択しなければならない。また，必要に応じ，送受信される情報の暗号化を行わなければならない。

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

オ　教育情報セキュリティ責任者は，重要性分類Ⅲ以上の情報資産を取り扱う情報システム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。

カ　教育情報セキュリティ責任者は，１人１台端末の運用にあたり児童生徒が同時にインターネットに接続し，クラウドサービスを活用した円滑な授業を行うことができるようインターネット接続環境を整備する。

キ　教育情報セキュリティ責任者は，インターネット接続環境に１人１台の学習系システムが接続されるとともに，校務系システムが接続されることを想定した接続環境の整備を行う。

４－４　教職員の利用する端末や電磁的記録媒体等の管理

（校務用端末，校務外部接続用端末及び指導者用端末について）

ア　教育情報システム管理者は，盗難防止のため，職員室で利用する校務用端末及び校務外部接続用端末に対し施錠管理を行うものとする。ただし，施錠できる場所への保管が不可能な端末等は，情報が漏洩しないよう，適切な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。

イ　教育情報システム管理者は，情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

ウ　教育情報システム管理者は，重要性分類Ⅲ以上のデータを取り扱うシステムについて，教育情報システムへのログインパスワードの入力等による認証を必要とするように設定しなければならない。

エ　教育情報システム管理者は，重要性分類Ⅰ とⅡに関してパスワードの多要素認証を併用するよう努めなければならない。

オ　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しなければならない。

（学習者用端末について）

ア　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。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。

イ　教育情報システム管理者は，情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

５　人的セキュリティ

５－１　教職員の遵守事項

クラウドサービスの利用においては，本項及び「9 項　クラウドサービスの利用」「10 項　1 人 1 台端末におけるセキュリティ」の規定を併せて適用する。

(1) 教職員の遵守事項

ア　教育情報セキュリティポリシー等の遵守

教職員は，教育情報セキュリティポリシー及び実施手順を遵守しなければならない。また，教育情報セキュリティ対策について不明な点，遵守することが困難な点等がある場合は，速やかに教育情報セキュリティ管理者に相談し，指示を仰がなければならない。

イ　業務以外の目的での使用の禁止

教職員は，業務以外の目的で情報資産の外部への持ち出し，教育情報システムへのアクセス，電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

ウ　モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

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

(ｲ) 教職員は，学校のモバイル端末，電磁的記録媒体，情報資産及びソフトウェアを外部に持ち出す場合には，教育情報セキュリティ管理者の許可を得なければならない。

(ｳ) 教職員は，外部で情報処理業務を行う場合には，教育情報セキュリティ管理者の許可を得なければならない。

エ　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) 教職員は，支給以外のパソコン，モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし，業務上必要な場合は，教育情報セキュリティ管理者の許可を得て利用することができる。

(ｲ) 教職員は，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を遵守しなければならない。

オ　持ち出し及び持ち込みの記録

教育情報セキュリティ管理者は，端末等の持ち出し及び持ち込みについて，記録を作成し，保管しなければならない。

カ　パソコンやモバイル端末におけるセキュリティ設定変更の禁止

教職員は，パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を教育情報セキュリティ管理者の許可なく変更してはならない。

キ　机上の端末等の管理

教職員は，パソコン，モバイル端末，電磁的記録媒体及び情報が印刷された文書等について，第三者に使用されること又は教育情報セキュリティ管理者の許可なく情報を閲覧されることがないように，離席

時のパソコン，モバイル端末のロックや電磁的記録媒体，文書等の容易に閲覧されない場所への保管等，適切な措置を講じなければならない。

ク　退職時等の遵守事項

教職員は，異動，退職等により業務を離れる場合には，利用していた情報資産を，返却しなければならない。また，その後も業務上知り得た情報を漏らしてはならない。

(2) 非常勤及び臨時の教職員への対応

ア　教育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，非常勤及び臨時の教職員に対し，採用時に教育情報セキュリティポリシー等のうち，非常勤及び臨時の教職員が守るべき内容を理解させ，また実施及び遵守させなければならない。

イ　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，非常勤及び臨時の教職員にパソコンやモバイル端末による作業を行わせる場合において，インターネットへの接続及び電子メールの使用等が不要の場合，これを利用できないようにしなければならない。

(3) 教育情報セキュリティポリシー等の掲示

教育情報セキュリティ管理者は，教職員等が常に教育情報セキュリティポリシー及び実施手順を閲覧できるように掲示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，教育情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

５－２　研修・訓練

(1) 教育情報セキュリティに関する研修・訓練

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

(2) 研修計画の策定及び実施

ア　CISO は，教職員に対する教育情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い，教育情報セキュリティ委員会の承認を得なければならない。

イ　新規採用の教職員を対象とする教育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。

ウ　研修は，教職員に対して，それぞれの役割，教育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。

エ　CISO は，毎年度１回，教育情報セキュリティ委員会に対して，教職員の教育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。

５－３　教育情報セキュリティインシデントの報告

(1) 学校内からの教育情報セキュリティインシデントの報告

ア　教職員は，教育情報セキュリティインシデントを認知した場合，速やかに教育情報セキュリティ管理者に報告しなければならない。

イ　報告を受けた教育情報セキュリティ管理者は，速やかに統括教育情報セキュリティ責任者，教育情報システム管理者及び教育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。

ウ　教育情報セキュリティ管理者は，報告のあった教育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。

(2) 住民等外部からの教育情報セキュリティインシデントの報告

ア　教職員は，管理対象のネットワーク及び教育情報システム等の情報資産に関する教育情報セキュリティインシデントについて，住民等外部から報告を受けた場合，教育情報セキュリティ管理者に報告しなければならない。

イ　報告を受けた教育情報セキュリティ管理者は，速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に報告しなければならない。

ウ　教育情報セキュリティ管理者は，当該教育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教育情報セキュリティインシデントについて，住民等外部から報告を受けるための窓口を設置し，当該窓口への連絡手段を公表しなければならない。

(3) 教育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　教育情報セキュリティ責任者は，教育情報セキュリティインシデントについて，教育情報セキュリティ管理者，教育情報システム管理者及び教育情報セキュリティに関する統一的な窓口と連携し，これらの教育情報セキュリティインシデント原因を究明し，記録を保存しなければならない。また，教育情報セキュリティインシデントの原因究明の結果から，

再発防止策を検討し，CISO に報告しなければならない。

イ　CISO は，教育情報セキュリティ責任者から，教育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。

5－4　ID 及びパスワード等の管理

(1) ID の取扱い

教職員は，自己の管理する ID に関し，次の事項を遵守しなければならない。

ア　自己が利用している ID は，他人に利用させてはならない。

イ　共用 ID を利用する場合は，共用 ID の利用者以外に利用させてはならない。

(2) パスワードの取扱い

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

ア　パスワードは，他者に知られないように管理しなければならない。

イ　パスワードを秘密にし，パスワードの照会等には一切応じてはならない。

ウ　パスワードは十分な長さとし，文字列は想像しにくいものにしなければならない。

エ　パスワードが流出したおそれがある場合には，教育情報セキュリティ責任者及び教育情報セキュリティ管理者に速やかに報告し，パスワードを速やかに変更しなければならない。

オ　複数の教育情報システムを扱う教職員は，同一のパスワードを複数のシステム間で用いてはならない。

カ　仮のパスワードは，最初のログイン時点で変更しなければならない。

キ　パソコン等の端末にパスワードを記憶させてはならない。

ク　教職員間でパスワードを共有してはならない。

ケ　パスワードのメモを，机上，キーボード，ディスプレイ周辺等，他人が容易に見ることができる場所に置いてはならない。

6　技術的セキュリティ

本項はサーバ等を自己設備として設置運用するものに適用する。クラウドサービスの利用においては，本項及び「9 項　クラウドサービスの利用」の規定を併せて適用する。

また，学習用端末に関しては「10 項　1 人 1 台端末におけるセキュリテ

ィ」で規定する。

６－１　コンピュータ及びネットワークの管理

(1) 文書サーバ及び端末の設定等

ア　教育情報セキュリティ責任者は，教職員が使用できる文書サーバの容量を設定し，教職員に周知しなければならない。

イ　教育情報セキュリティ責任者は，文書サーバを学校の単位で構成し，教職員が他の学校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　教育情報セキュリティ責任者は，住民の個人情報，人事記録等，特定の教職員等しか取扱えないデータについて，別途ディレクトリを作成する等の措置を講じ，同一学校であっても，担当職員以外の教職員が閲覧及び使用できないようにしなければならない。

エ　教育情報セキュリティ責任者は，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，重要性分類Ⅱ以上の機微な個人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

教育情報セキュリティ責任者及び教育情報システム管理者は，ファイルサーバ等に記録された情報について，サーバの冗長化対策に関わらず，次のア及びイに基づきバックアップを実施するものとする。

ア　校務系情報及び校務外部接続系情報については，必要に応じて定期的にバックアップを実施しなければならない。

イ　学習系情報については，必要に応じて定期的にバックアップを実施しなければならない。

(3) 他団体との情報システムに関する情報等の交換

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

(4) 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，互いにその作業結果を確認すること。

(5) 情報システム仕様書等の管理

教育情報セキュリティ責任者は，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，適切に管理しなければならない。

(6) ログの取得等

ア　教育情報システム管理者は，各種ログ及び教育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　教育情報システム管理者は，ログとして取得する項目，保存期間，取扱方法及びログが取得できなくなった場合の対処等について定め，適切にログを管理しなければならない。

ウ　教育情報システム管理者は，取得したログを定期的に点検又は分析する機能を設け，必要に応じて悪意ある第三者等からの不正侵入，不正操作等の有無について点検又は分析を実施しなければならない。

(7) 障害記録

教育情報システム管理者は，教職員からのシステム障害の報告，システム障害に対する処理結果又は問題等を，障害記録として記録し，適切に保存しなければならない。

(8) ネットワークの接続制御，経路制御等

ア　教育情報セキュリティ責任者は，フィルタリング及びルーティングについて，設定の不整合が発生しないように，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責任者は，不正アクセスを防止するため，ネットワークに適切なアクセス制御を施さなければならない。

(9) 外部の者が利用できるシステムの分離等

教育情報システム管理者は，外部の者が利用できるシステムについて，必要に応じ教育ネットワーク及び教育情報システムと物理的に分離する等の措置を講じなければならない。

(10)　外部ネットワークとの接続制限等

ア　教育情報システム管理者は，ウェブサーバ等をインターネットに公開する場合，教育ネットワークへの侵入を防御するために，ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

イ　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責任者の判断に従い，速やかに当該外部ネットワークを物理的に遮断しなければならない。

(11)　ネットワークの分離

ア　教育情報システム管理者は、校務系システム及び学習系システム間の通信経路を論理的に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）を論理的に分離をする，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措置を講じなければならない。

(12)　複合機のセキュリティ管理

ア　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しなければならない。

イ　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教育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なければならない。

(13)　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責任者は，無線 LAN の利用を認める場合，解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

イ　教育情報セキュリティ責任者は，機密性の高い情報を取り扱うネットワークについて，情報の盗聴等を防ぐため，暗号化等の措置を講じなければならない。

(14)　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責任者は，大量のスパムメール等の受信又は送信を検知した場合は，メールサーバの運用を停止しなければならない。

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

エ　教育情報セキュリティ責任者は，教職員が使用できる電子メールボックスの容量の上限を設定し，上限を超えた場合の対応を教職員に周知し

なければならない。

オ　教育情報セキュリティ責任者は，システム開発や運用，保守等のため外部委託事業者の作業員が施設内に常駐する場合は当該作業員の電子メールアドレス利用について，外部委託事業者との間で利用方法を取り決めなければならない。

(15)　電子メールの利用制限

ア　教職員は，自動転送機能を用いて，電子メールを転送してはならない。

イ　教職員は，業務上必要のない送信先に電子メールを送信してはならない。

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

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

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

(16)　電子署名・暗号化

ア　教職員は，情報資産の分類により定めた取扱制限に従い，外部に送るデータの機密性又は完全性を確保することが必要な場合には，CISO が定めた電子署名，暗号化又はパスワード設定等，セキュリティを考慮して，送信しなければならない。

イ　教職員は，暗号化を行う場合に CISO が定める以外の方法を用いてはならない。また，CISO が定めた方法で暗号のための鍵を管理しなければならない。

(17)　無許可ソフトウェアの導入等の禁止

ア　教職員は，原則として事前の申請がない場合はパソコンやモバイル端末にソフトウェアを導入してはならない。ただし，業務上やむを得ない緊急の場合は事後申請を行うものとする。

イ　教職員は，業務上の必要がある場合は，統括教育情報セキュリティ責任者及び教育情報システム管理者の許可を得て，ソフトウェアを導入することができる。なお，導入する際は，教育情報セキュリティ管理者又は教育情報システム管理者は，ソフトウェアのライセンスを管理しなければならない。

ウ　教職員は，不正にコピーしたソフトウェアを利用してはならない。

(18)　機器構成の変更の制限

教職員は，パソコンやモバイル端末に対し機器の改造及び増設・交換

を行ってはならない。

(19)　無許可でのネットワーク接続の禁止

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

(20)　業務以外の目的でのウェブ閲覧の禁止

ア　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。

イ　教育情報セキュリティ責任者は，教職員のウェブ利用について，明らかに業務に関係のないサイトを閲覧していることを発見した場合は，教育情報セキュリティ管理者に通知し適切な措置を求めなければならない。

６－２　アクセス制御

(1) アクセス制御等

ア　アクセス制御

教育情報セキュリティ責任者は，所管するネットワーク，教育情報システム管理者は情報システムごとにアクセスする権限のない教職員がアクセスできないように，システム上制限しなければならない。

イ　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なければならない。

(ｲ) 教職員は，業務上必要がなくなった場合は，利用者登録を抹消するよう，教育情報システム管理者に通知しなければならない。

(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，人事管理部門と連携し，点検しなければならない。

ウ　特権を付与された ID の管理等

(ｱ) 教育情報システム管理者は，管理者権限等の特権を付与された ID を利用する者を必要最小限にし，当該 ID のパスワードの漏えい等が発生しないよう，当該 ID 及びパスワードを厳重に管理しなければならない。

(ｲ)　教育情報システム管理者は，特権を付与された ID に関してパスワードの多要素認証を併用するよう努めなければならない。

(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の特権を代行する者は，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自らが指名しなければならない。

(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てはならない。

(2) 教職員による外部からのアクセス等の制限

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

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

エ　教育情報セキュリティ責任者は，外部からのアクセスを認める場合，通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

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

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

キ　教育情報セキュリティ責任者は，公衆通信回線（公衆無線 LAN 等）を教育ネットワークに接続することは原則として禁止しなければならない。ただし，やむを得ず接続を許可する場合は，利用者の ID 及びパスワード，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，教育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できるよう努めなければならない。

(4) ログイン時の表示等

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

(5) パスワードに関する情報の管理

ア　教育情報システム管理者は，教職員のパスワードに関する情報を厳重

に管理しなければならない。パスワードファイルを不正利用から保護するため，オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は，これを有効に活用しなければならない。

イ　教育情報システム管理者は，教職員に対してパスワードを発行する場合は，仮のパスワードを発行し，ログイン後直ちに仮のパスワードを変更させなければならない。

(6) 特権による接続時間の制限

教育情報システム管理者は，特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

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，教育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・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

教育情報システム管理者は，外部事業者から納入されるシステム開発・保守に関する納入図書等を適切に整備・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，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責任者の措置事項

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

ア　外部ネットワークから受信したファイルは，インターネットのゲートウェイ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，必要に応じ教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。

(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，市が管理している電磁的記録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。

(3) 教職員等の遵守事項

教職員等は，不正プログラム対策に関し，次の事項を遵守しなければならない。

ア　パソコンやモバイル端末において，不正プログラム対策ソフトウェアが導入されている場合は，当該ソフトウェアの設定を変更してはならない。

イ　外部からデータ又はソフトウェアを取り入れる場合には，必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

ウ　差出人が不明又は不自然に添付されたファイルを受信した場合は，速やかに削除しなければならない。

エ　端末に対して，不正プログラム対策ソフトウェアによるフルチェックを定期的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責任者が提供するウイルス情報を，常に確認しなければならない。

キ　コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は，以下の対応を行わなければならない。

(ｱ) パソコン等の端末の場合

LAN ケーブルの即時取り外しを行わなければならない。

(ｲ) モバイル端末の場合

直ちに利用を中止し，通信を行わない設定への変更を行わなければならない。

６－５　不正アクセス対策

(1) 教育情報セキュリティ責任者の措置事項

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

ア　使用されていないポートを閉鎖しなければならない。

イ　不要なサービスについて，機能を削除又は停止しなければならない。

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

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

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

(2) 攻撃の予告

教育情報セキュリティ責任者は，サーバ等に攻撃を受けることが明確になった場合，システムの停止を含む必要な措置を講じなければならない。また，関係機関と連絡を密にして情報の収集に努めなければならない。

(3) 記録の保存

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

(4) 内部からの攻撃

教育情報セキュリティ責任者及び教育情報システム管理者は，教職員及び外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

(5) 教職員による不正アクセス

教育情報セキュリティ責任者及び教育情報システム管理者は，教職員による不正アクセスを発見した場合は，当該教職員が所属する学校の教育情報セキュリティ管理者に通知し，適切な処置を求めなければならない。

(6) サービス不能攻撃

教育情報セキュリティ責任者及び教育情報システム管理者は，外部からアクセスできる情報システムに対して，第三者からサービス不能攻撃を受け，利用者がサービスを利用できなくなることを防止するため，情報システムの可用性を確保する対策を講じなければならない。

(7) 標的型攻撃

教育情報セキュリティ責任者及び教育情報システム管理者は，情報システムにおいて，標的型攻撃による内部への侵入を防止するために，教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また，内部に侵入した攻撃を早期検知して対処するために，通信をチェックする等の内部対策を講じなければならない。

6－6　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

教育情報セキュリティ責任者及び教育情報システム管理者は，セキュリティホールに関する情報を収集し，必要に応じ，関係者間で共有しなければならない。また，当該セキュリティホールの緊急度に応じて，ソフトウェア更新等の対策を実施しなければならない。

(2) 不正プログラム等のセキュリティ情報の収集及び周知

教育情報セキュリティ責任者は，不正プログラム等のセキュリティ情報を収集し，必要に応じ対応方法について，教職員に周知しなければならない。

(3) 教育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責任者及び教育情報システム管理者は，教育情報セキュリティ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，教育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

クラウドサービスの利用においては，本項及び「9 項　クラウドサービスの利用」の規定を併せて適用する。

7－1　情報システムの監視

ア　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。

イ　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。

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，外部と常時接続するシステムを常に監視しなければならない。

７－２　教育情報セキュリティポリシーの遵守状況の確認

(1) 遵守状況の確認及び対処

ア　教育情報セキュリティ責任者及び教育情報セキュリティ管理者は，教育情報セキュリティポリシーの遵守状況について確認を行い，問題を認めた場合には，速やかにCISO及び統括教育情報セキュリティ責任者に報告しなければならない。

イ　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，ネットワーク及びサーバ等のシステム設定等における教育情報セキュリティポリシーの遵守状況について，定期的に確認を行い，問題が発生していた場合には適切かつ速やかに対処しなければならない。

(2) パソコン，モバイル端末及び電磁的記録媒体等の利用状況調査

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，教職員が使用しているパソコン，モバイル端末及び電磁的記録媒体等のログ，電子メールの送受信記録等の利用状況を調査することができる。

(3) 教職員の報告義務

ア　教職員は，教育情報セキュリティポリシーに対する違反行為を発見した場合，直ちに教育情報セキュリティ責任者及び教育情報セキュリティ管理者に報告を行わなければならない。

イ　違反行為が直ちに教育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責任者が判断した場合は，緊急時対応計画に従って適切に対処しなければならない。

７－３　侵害時の対応等

(1) 緊急時対応計画の策定

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

(2) 緊急時対応計画に盛り込むべき内容

緊急時対応計画には，以下の内容を定めなければならない。

ア　関係者の連絡先

イ　発生した事案に係る報告すべき事項
ウ　発生した事案への対応措置
エ　再発防止措置の策定

(3) 業務継続計画との整合性確保

自然災害，大規模又は広範囲に及ぶ疾病等に備えて別途業務継続計画を策定し，教育情報セキュリティ委員会は当該計画と教育情報セキュリティポリシーの整合性を確保しなければならない。

(4) 緊急時対応計画の見直し

CISO は，教育情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ，必要に応じて緊急時対応計画の規定を見直さなければならない。

7－4　例外措置

(1) 例外措置の許可

教育情報セキュリティ管理者及び教育情報システム管理者は，教育情報セキュリティ関係規定を遵守することが困難な状況で，学校事務及び教育活動の適正な遂行を継続するため，遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には，CISO の許可を得て，例外措置を取ることができる。

(2) 緊急時の例外措置

教育情報セキュリティ管理者及び教育情報システム管理者は，学校事務及び教育活動の遂行に緊急を要する等の場合であって，例外措置を実施することが不可避のときは，事後速やかに CISO に報告しなければならない。

(3) 例外措置の申請書の管理

CISO は，例外措置の申請書及び審査結果を適切に保管し，定期的に申請状況を確認しなければならない。

7－5　違反時の対応

(1) 違反時の対応

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

ア　教育情報セキュリティ責任者が違反を確認した場合は，当該教職員が所属する学校の教育情報セキュリティ管理者に通知し，適切な措置を求めなければならない。

イ　教育情報システム管理者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責任者及び当該教職員が所属する学

校の教育情報セキュリティ管理者に通知し，適切な措置を求めなければならない。

ウ　教育情報セキュリティ管理者の指導によっても改善されない場合，教育情報セキュリティ責任者は，当該教職員の教育ネットワーク又は教育情報システムを使用する権利を制限あるいは停止することができる。その後速やかに，教育情報セキュリティ責任者は，教職員の権利を停止あるいは剥奪した旨を 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教育情報セキュリティ管理者に通知しなければならない。

8　外部委託

クラウドサービスの利用においては，本項及び「9 項　クラウドサービスの利用」の規定を併せて適用する。

(1) 外部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，外部委託事業者の選定に当たり，委託内容に応じた教育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，教育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，教育情報セキュリティ監査の実施状況等を参考にして，事業者を選定しなければならない。

ウ　教育情報セキュリティ管理者は，クラウドサービスを利用する場合は，情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

(2) 契約項目

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教育情報セキュリティ要件を明記した契約を締結しなければならない。

・教育情報セキュリティポリシー及び教育情報セキュリティ実施手順の遵守
・外部委託事業者の責任者，委託内容，作業者，作業場所の特定
・提供されるサービスレベルの保証
・外部委託事業者にアクセスを許可する情報の種類と範囲，アクセス方法
・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
・市による教育情報セキュリティインシデント発生時の公表
・教育情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)
・提供された情報の複製禁止
・委託先における情報資産の保管及び破棄
・ポリシー遵守のための体制
・個人情報等の重要性が高い情報について，外部搬送時における盗難及び不正コピーに対する防止措置の実施

(3) 確認・措置等

教育情報セキュリティ管理者は，外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し，必要に応じ，（２）の契約に基づき措置しなければならない。また，その内容を教育情報セキュリティ責任者に報告するとともに，その重要度に応じて CISO に報告しなければならない。

９　クラウドサービスの利用

９－１　クラウド事業者の選定

ア　クラウド利用者は，クラウド事業者を選定するにあたりクラウド事業者が提供するクラウドサービスの情報セキュリティの実態について確認するものとし，確認はクラウド事業者が取得する第三者による認証を利用して確認することができる。

イ　クラウド事業者が取得する第三者による認証制度は以下のものがある。

- ISO/IEC 27017（クラウドサービスの情報セキュリティ）
- ISO/IEC 27018（クラウドサービスにおける個人情報の取扱い）
- または上記に相当する認証

９－２　クラウドサービスの利用における情報セキュリティ対策

(1) 利用者認証

ア　クラウド利用者は，クラウド事業者における当該クラウドサービスを提供する情報システムの運用もしくは開発に従事する者又は管理者権限を有する者について，適切な利用者確認がなされていることをクラウド事業者に求め，サービス提供定款や契約書面上で確認または合意しな

ければならない。

イ　クラウド利用者は，当該クラウドサービスのログインに関わる認証機能の提供をクラウド事業者に求め，サービス提供定款や契約書面上で確認または合意しなければならない。

ウ　クラウド利用者側管理者権限を有する者の ID の管理について，6-2 項(1)ウ（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，許可されたエンドユーザのみがアクセスできる環境を設定しなければならない。

(3) クラウドに保管するデータの暗号化

ア　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。

(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

ア　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，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項（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項（管理区域（サーバ室等）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。

(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，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。また，クラウド事業者の設定不備等によるインシデント発生時にも同様の確認をしなければならい。

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項（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。

ウ　クラウド利用者は，当該クラウドサービスにおけるデータバックアップについて，６－１項（コンピュータ及びネットワークの管理）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。

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項（技術的セキュリティ）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) クラウド利用者のセキュリティ確保

ア　クラウド利用者は，クラウドサービスにアクセスする利用者側端末について，保管するデータの外部流出，改ざん等から保護するために必要な措置を講じなければならない。

イ　クラウド利用者は，標的型攻撃による外部からの脅威の侵入を防止するために，エンドユーザへの教育や入口対策を講じなければならない。

(11) クラウド事業者従業員の人的セキュリティ対策

ア　クラウド利用者は，クラウドサービスに関わるクラウド事業者従業員に対して，クラウド事業者の情報セキュリティポリシー及び保守運用管理規程等を遵守することをクラウド事業者に求め，サービス提供定款や契約書面上で確認または合意しなければならない。

イ　クラウド利用者は，クラウドサービスに関わるクラウド事業者従業員に対して，業務に用いる ID 及びパスワードその他の個人認証に必要な

情報及び媒体について，部外者及び業務に関わらない従業員に漏えいすることがないように，適切に管理することをクラウド事業者に求め，サービス提供定款や契約書面上で確認または合意しなければならない。

ウ　クラウド利用者は，クラウドサービスに関わらない従業員等がクラウド利用者のデータを知り得る状態にならないよう，業務に関わるクラウド事業者従業員に 対して秘匿を義務づけることをクラウド事業者に求め，サービス提供定款や契約書面上で確認または合意しなければならない。

エ　クラウド利用者は，クラウド利用者のデータ及びデータを格納した端末機器又は電磁的記録媒体の外部持ち出しについて，クラウド利用者の許可なく外部持ち出しできないこと及び外部持ち出しにおける安全管理手順をクラウド事業者に求め，サービス提供定款や契約書面上で確認または合意しなければならない。

オ　クラウド利用者は，クラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等にマルウェアを侵入させないようクラウド事業者に求め，サービス提供定款や契約書面上で確認または合意しなければならない。

(12) データの廃棄等について

ア　クラウド利用者は，サービス利用終了時等において，クラウド利用者のデータが不用意に残置されないよう，適切に破棄するための流れを確立する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，その措置の流れを確立する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ておかなければならない。

９－３　パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項

(1) 守秘義務，目的外利用及び第三者への提供の禁止

クラウド利用者は，クラウド事業者と契約時に守秘義務，目的外利用及び第三者への提供の禁止条項を締結しなければならない。クラウド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。

確認すべき項目例を下記に示す。

- 個人情報保護方針
- プライバシーポリシー
- 情報セキュリティに関する基本方針及び対策基準
- 保守運用基準

(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。

- 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
- 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
- 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に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。

９－４　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（機密性 2A 以上）の情報はソーシャルメディアサービスで発信してはならない。

(3) 利用するソーシャルメディアサービスごとの責任者を定めなければならない。

１０　１人１台端末におけるセキュリティ

１０－１ 情報モラル教育等の充実について

学校における１人１台端末の本格的な運用に当たり，教育情報セキュリティ責任者は，情報社会で適正な活動を行うための基となる考え方や態度を育む情報モラル教育の一層の充実を図ること。

１０－２ 学習用端末のセキュリティ対策

(1) 授業に支障のないネットワーク構成の選択（帯域や同時接続数など）

不適切なウェブページの閲覧防止クラウドサービス提供事業者側のサービス要件基準を満たしたネットワーク構成を設計する。また，運用開始前には十分検証し，利用状況に応じて定期的に改修計画を行うこと。

(2) 不適切なウェブページの閲覧防止

児童生徒が端末を利用する際に不適切なウェブページの閲覧を防止する対策を講じなければならない。

＜対策例＞

①フィルタリングシステム

②検索エンジンのセーフサーチ

③セーフブラウジング

(3) マルウェア感染対策

学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

(4) 端末を不正利用させないための防止策

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

(5) セキュリティ設定の一元管理

児童生徒への端末配布後においても，端末のセキュリティ設定や OS アップデート，ウェブブラウザのアップデート，学習用ツールのインストール，端末の利用履歴も含めた状態確認などの作業を，離れた場所からでも一元管理できることが望ましい。

(6) 端末の盗難・紛失時の情報漏洩対策

児童生徒が端末を紛失しても，遠隔操作でロックをかける，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。

(7) 運用・連絡体制の整備

学校内外での端末の運用ルールを制定し，インシデント時の連絡先対応方法を各学校にて整理しなければならない。

１０－３ 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，教育委員会で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。そのため 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内が終了する場合は，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

成績評価につながる CBT（Computer Based Testing）など，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期間は各種サービスにアクセスが行えるシングルサインオンの導入を行うことが望ましい。

１１　評価・見直し

１１－１　監査

(1) 実施方法

CISO は，教育情報セキュリティ監査統括責任者を指名し，教育ネットワーク及び教育情報システム等の情報資産における教育情報セキュリティ対策状況について，毎年度及び必要に応じて監査を行わせなければならない。

(2) 監査を行う者の要件

ア　教育情報セキュリティ監査統括責任者は，監査を実施する場合には，被監査部門から独立した者に対して，監査の実施を依頼しなければならない。

イ　監査を行う者は，監査及び教育情報セキュリティに関する専門知識を有する者でなければならない。

(3) 監査実施計画の立案及び実施への協力

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

イ　被監査部門は，監査の実施に協力しなければならない。

(4) 外部委託事業者に対する監査

外部委託事業者に委託している場合，教育情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて，教育情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

(5) 報告

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

(6) 保管

教育情報セキュリティ監査統括責任者は，監査の実施を通して収集した監査証拠，監査報告書の作成のための監査調書を，紛失等が発生しないように適切に保管しなければならない。

(7) 監査結果への対応

CISO は，監査結果を踏まえ，指摘事項を所管する教育情報セキュリティ管理者に対し，当該事項への対処を指示しなければならない。また，指摘事項を所管していない教育情報セキュリティ管理者に対しても，同種の課題及び問題点がある可能性が高い場合には，当該課題及び問題点の有無を確認させなければならない。

(8) 教育情報セキュリティポリシー及び関係規程等の見直し等への活用

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

１１－２　自己点検

(1) 実施方法

教育情報セキュリティ責任者は，教育情報セキュリティ管理者と連携して，所管する部局における教育情報セキュリティポリシーに沿った教育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責任者は，自己点検結果と自己点検結果に基づく

改善策を取りまとめ，教育情報セキュリティ委員会に報告しなければならない。

(3) 自己点検結果の活用

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

イ　教育情報セキュリティ委員会は，この点検結果を教育情報セキュリティポリシー及び関係規程等の見直し，その他教育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。

１１－３　教育情報セキュリティポリシー及び関係規程等の見直し

教育情報セキュリティ委員会は，教育情報セキュリティ監査及び自己点検の結果並びに教育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，改善を行うものとする。