藤　枝　市

教育情報セキュリティポリシー

藤枝市教育委員会

令和8年4月

初版

第１章

教育情報セキュリティ基本方針

（目次）

第1章 教育情報セキュリティ基本方針

1. 目的

本基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、教育委員会事務局及び学校が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2. 定義

本基本方針における用語の定義は、次の各号に掲げるところによる。

(1) ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

(2) 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(3) 記録媒体

情報が記録され、又は記載される有体物をいう。記録媒体において、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物を「書面」といい、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるものを「電磁的記録」といい、電磁的記録に係る記録媒体を「電磁的記録媒体」という。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R 等の外部電磁的記録媒体がある。

(4) 端末

情報システムの構成要素である機器のうち、職員等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、教育委員会が調達又は開発するもの（政府共通利用型システムが提供するものを含む。）をいう。

(5) モバイル端末

端末のうち、業務上の必要に応じて場所を移動させて使用することを目的としたものをいい、端末の形態は問わない。

(6) 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(7) 教育情報セキュリティポリシー

本基本方針及び教育情報セキュリティ対策基準をいう。

(8) 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(9) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(10) 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(11) 校務系情報

学校が保有する情報資産のうち、それらの情報を学校・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指す。

(12) 校務外部接続系情報

ネットワーク分離による対策を講じたシステム構成において、インターネット接続を前提として、校務で利用される情報を指す。

(13) 学習系情報

学校が保有する情報資産のうち、それらの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指す。

(14) 校務用端末

校務系情報にアクセス可能な端末を指す。

(15) 校務外部接続用端末

ネットワーク分離による対策を講じたシステム構成において、校務外部接続系情報にアクセス可能な端末を指す。

(16) 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指す。

(17) 校務系システム

校務系ネットワーク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

(18) 校務外部接続系システム

ネットワーク分離による対策を講じたシステム構成において、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

(19)　学習系システム

学習系ネットワーク及び学習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

(20)　強固なアクセス制御

内部・外部からの不正アクセスを防御するため、多要素認証、端末認証、アクセス経路の監視等を組み合わせた対策を指す。

(21)　通信の暗号化

通信又は通信経路を暗号化し保護すること。

(22)　常時監視

セキュリティ機器等により情報システム等の状態を継続的に観測及び記録することをいう。なお、24 時間の有人監視を義務付けるものではなく、自動検知と管理者への通知体制の整備をもってこれに代えることができる。

3. 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

(1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

(3) 地震、落雷、火災等の災害によるサービス及び業務の停止等

(4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

(5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4. 適用範囲

(1) 行政機関の範囲

本基本方針が適用される行政機関等は、教育委員会事務局及び藤枝市立学校設置条例（昭和 39 年藤枝市条例第 11 号）に規定する学校（以下「学校」という。）とする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。ただし、市情報セキュリティポリシーの対象となる情報資産については、対象としない。

① 教育ネットワーク、教育情報システム、これらに関する設備、電磁的記録媒体
② 教育ネットワークおよび教育情報システムで取り扱う情報（これらを印刷した文書を含む）
③ 教育情報システムの仕様書およびネットワーク図等のシステム関連文書

5. 職員等の順守義務

全ての職員（職員、会計年度任用職員、非常勤講師、事務職員等）および外部委託事業者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

また、児童生徒が教育課程に基づき、本市の情報資産を利用する際は、情報セキュリティを確保するよう、教職員等が適切に指導を行わなければならない。

6. 情報セキュリティ対策

(1) 組織体制

本市の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

(2) 情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性に応じて分類を行い、当該分類に基づき情報セキュリティ対策を実施する。

(3) 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

① 校務系システムにおいては、原則として、学習系システム等の他の領域とは物理的及び論理的に通信経路を分離した上で、端末への多要素認証の導入やアクセス制御の徹底等により、児童生徒の成績や指導要録等の機微な個人情報の流出を防ぐ。
② 学習系システムにおいては、機微な情報を扱う校務系システムと物理的及び論理的に分離し、児童生徒による不正アクセスやウイルス感染の拡大を防止する。なお、クラウドサービスを活用する場合には、フィルタリングや端末管理機能（MDM）等により、安全な学習環境を確保する。
③ 校務外部接続系システムにおいては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、適切なアクセス制御等により校務系情報を取り扱う環境との独立性を確保した上で、振る舞い検知機能を有する不正プログラム対策ソフトウェア及び端末の操作ログ等の活用により、常時監視を実施する。

(4) 物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、十分な物理的な対策を講じる。

(5) 人的セキュリティ

情報セキュリティに関し、教職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(6) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(7) 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応体制を設定する。

(8) 業務委託と外部サービス（クラウドサービス）の利用

外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、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る。

7. 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8. 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

9. 情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める教育情報セキュリティ対策基準を策定する。

10. 情報セキュリティ実施手順の策定

教育情報セキュリティ対策基準に基づき、教育情報セキュリティ対策を実施するための具体的な手順を定めた教育情報セキュリティ実施手順を策定するものとする。なお、情報

セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

第２章

教育情報セキュリティ対策基準

（目次）

第2章 教育情報セキュリティ対策基準

本対策基準は、情報セキュリティ基本方針を実行に移すための、本市における情報資産に関する情報セキュリティ対策の基準を定めたものである。

1. 対象範囲

(1) 行政機関等の範囲

本対策基準が適用される行政機関等は、教育委員会事務局及び藤枝市立学校設置条例（昭和 39 年藤枝市条例第 11 号）に規定する学校（以下「学校」という。）とする。

(2) 情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

① 教育ネットワーク、教育情報システム、これらに関する設備、電磁的記録媒体

② 教育ネットワークおよび教育情報システムで取り扱う情報（これらを印刷した文書を含む）

③ 教育情報システムの仕様書およびネットワーク図等のシステム関連文書

※ 上記の情報資産に含まれない公文書（情報システムを介さない一般的な紙文書等）については、文書管理規程等の別の定めにより適切に管理しなければならない。
また、教育ネットワークと論理的または物理的に分離されている「行政系ネットワーク」およびその端末機については、市長部局が策定する情報セキュリティポリシーを遵守するものとする。

2. 組織体制

教育情報セキュリティについては、以下の組織、体制で管理を行う。

(1) 最高情報セキュリティ責任者（CISO）

① 教育長を、最高情報セキュリティ責任者とする。

② CISO は、本市における全ての教育ネットワーク、教育情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

(2) 統括教育情報セキュリティ責任者

① 教育部長を、統括教育情報セキュリティ責任者とする。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。

② 統括教育情報セキュリティ責任者は、本市の全ての教育ネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③ 統括教育情報セキュリティ責任者は、本市の全ての教育ネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

④ 統括教育情報セキュリティ責任者は、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者及び教育情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤ 統括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、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

⑥ 統括教育情報セキュリティ責任者は、本市の共通的な教育ネットワーク、教育情報システム及び情報資産に関する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。

(3) 教育情報セキュリティ責任者

① 学校教育監を、教育情報セキュリティ責任者とする。

② 教育情報セキュリティ責任者は、各学校の教育情報セキュリティ管理者を指揮し、情報セキュリティ運用ルールが学校現場において適切に実行されるよう、現場の運用と指導を統括する。

③ 教育情報セキュリティ責任者は、その職務を遂行するため、主席指導主事及び指導主事に、各学校に対する情報セキュリティに関する指導、助言及び連絡調整の実務を行わせることができる。

(4) 教育情報システム管理者

① 教育政策課長を、教育情報システム管理者とする。

② 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。

③ 教育情報システム管理者は、教育情報システムの導入、設定変更、運用及び保守にあたり、市長部局の情報政策担当部局と密に連携し、技術的な指導及び助言を受けるものとする。

④ 教育情報システム管理者は、システムの設計及びネットワーク構築において、市長部局が定める情報セキュリティ水準との整合性を図るため、必要に応じて市長部局の情報政策部門の協力を仰ぐものとする。

(5) 教育情報セキュリティ管理者

① 各学校長を、教育情報セキュリティ管理者とする。

② 教育情報セキュリティ管理者は、当該学校の情報セキュリティ対策に関する権限及び責任を有し、所属する教職員等を監督しなければならない。

(6) 教育情報システム担当者

① 教育政策課等の職員を、教育情報システム担当者とする。

② 教育情報システム担当者は、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) 兼務の禁止

① 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。

② 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。

(8) 教職員等及び事務局職員

① 臨時的任用教職員、非常勤講師を含めた教職員等は、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。

② 教育委員会事務局職員は、統括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) 教育情報セキュリティインシデント対応チーム：教育 CSIRT

① CISO は、教育委員会における情報セキュリティの統一的な窓口及び緊急対応体制として、教育 CSIRT を設置する。CISO は、職員の中から教育 CSIRT の構成員を選任し、その中から業務を統括する CSIRT 責任者を指名しなければならない。

② 教育 CSIRT は、次の各号に掲げる業務を担うものとする。

（ア）インシデント情報の集約及び状況確認を行い、速やかに CISO への報告を行うこと。

（イ）重要度や影響範囲等を勘案し、市長部局と連携して、総務省、都道府県、警察等の関係機関への報告及び報道機関への公表対応を行うこと。

（ウ）地方公共団体情報システム機構(J-LIS)、情報処理推進機構(IPA)、国家サイバー統括室(NCO)及び他の地方公共団体等との情報共有を行うこと。

③ 教育 CSIRT は、CISO によるセキュリティ戦略やインシデント対応に関する決定事項を、速やかに各学校及び関係部局へ周知しなければならない。

(10)　ポリシーの策定及び見直し体制

① 教育情報セキュリティ責任者は、情報セキュリティ対策の実効性を確保するため、既存の会議体を通じて、学校現場における運用実態や改善に関する意見を適時に把握しなければならない。

② 統括教育情報セキュリティ責任者は、前項で集約された意見及び技術的な課題を踏まえ、本ポリシー及び関連する実施手順の策定又は改定案を決定する。

③ 統括教育情報セキュリティ責任者は、決定した策定又は改定案について、CISO 及び教育委員会に報告しなければならない。

3. 情報資産の分類と管理方法

3.1. 情報資産の分類

本市が保有する情報資産は、機密性、完全性及び可用性の３つの要素に基づき、その侵害（漏えい、改ざん、滅失等）がもたらす影響を総合的に評価し、次の４段階で重要性分類を行う。

重要性分類	セキュリティ侵害が発生した場合の影響	各情報資産にアクセスする主体
I	教職員､児童生徒又は保護者の生命､財産､プライバシー等へ甚大な被害を及ぼすもの。	情報の取扱いが真に必要な特定の教職員等及び事務局職員に限定。 児童生徒･保護者は本人の情報のみにアクセス可能。
II	学校事務や教育活動の遂行に重大な支障を及ぼすもの。	業務に係る教職員等及び事務局職員に限定。 児童生徒･保護者は本人の情報のみにアクセス可能。
III	学校事務や教育活動の遂行に影響を及ぼし、その影響を無視できないもの（業務が滞る、社会的信頼を損なう等）。	教職員等及び事務局職員全員。 児童生徒、保護者のうち、利用目的や活動の範囲に照らし､アクセス主体として想定される者。
IV	学校事務や教育活動の遂行にほとんど影響を及ぼさないもの(速やかに再作成や修正が可能なもの)。	特段の利用制限なし｡不特定多数に公開することが想定される。

図１　重要性分類の定義

各情報資産の重要性分類は、３要素のうち最も高い影響度を示す区分を適用するものとする。

不特定多数に公開することを前提とした情報（機密性が低い情報）であっても、改ざんされた場合の影響を無視できないもの、又は必要な時に利用できないと業務に支障が出るものについては、その影響の大きさに応じ、重要性分類Ⅲ以上に位置付けるものとする。

3.2. 情報資産の管理

(1) 管理責任

① 統括教育情報セキュリティ責任者は、教育情報セキュリティ対策基準に基づき、学校現場での情報セキュリティ運用管理に関する実施手順を作成しなければならない。

② 統括教育情報セキュリティ責任者は、学校で標準的に所管する情報資産について、分類を定義した情報資産台帳を作成し、適宜更新しなければならない。

③ 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。

④ 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。

⑤ 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) 情報資産の分類の表示

教職員等は、重要性分類Ⅱ以上の情報資産について、以下の方法等により重要性分類を判別できる表示を付すとともに、適正な管理を行わなければならない。

① 電子データ

ファイル名への特定の識別記号の付記、または重要性分類ごとに区分された保管場所（フォルダ等）への格納および当該保管場所への表示。

② 電磁的記録媒体

ラベル等への重要性分類および取扱制限の表示。

③ 紙媒体

文書の隅や表紙等への重要性分類を示す記号または文言の明示。

(3) 情報の作成

① 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。

② 情報を作成する教職員等は、情報の作成時に 3.1.の分類に基づき、当該情報の分類を定め、分類に準拠した取扱いを行わなければならない。

③ 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。

(4) 情報資産の入手

① 教職員等及び事務局職員が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

② 教職員等及び事務局職員以外の者が作成した情報資産を入手した者は、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。

③ 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、以下のとおり対応することとする。

（ア）教職員等にあっては、所属する学校の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。

（イ）事務局職員にあっては、教育情報システム管理者に判断を仰がなければならない。

(5) 情報資産の利用

① 情報資産を利用する教職員等及び事務局職員は、業務以外の目的に情報資産を利用してはならない。

② 情報資産を利用する教職員等及び事務局職員は、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。

③ 情報資産を利用する教職員等及び事務局職員は、電磁的記録媒体または保存されている領域（フォルダやサーバ）に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体または保存されている領域を取り扱わなければならない。

④ 情報資産を利用する教職員等及び事務局職員は、必要以上の複製及び配布をしてはならない。

(6) 情報資産の保管

① 教育情報セキュリティ管理者又は教育情報システム管理者の措置事項

（ア）教育情報セキュリティ管理者は、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、重要性分類Ⅱ以上の情報を教育委員会が管理するサーバ又は指定されたクラウドストレージへ保存させることを原則とする。

（ウ）前項の規定にかかわらず、業務遂行上やむを得ず承認された端末のローカルディスクに保存させる場合には、当該端末に対しディスク全体の暗号化等の保護措置を講じた上で、一時的な保存に留め、業務終了後又はサーバ等への格納後は速やかに消去させなければならない。

（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、未許可の電磁的記録媒体（私物のＵＳＢメモリ等）への保存を禁止しなければならない。

（オ）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外部電磁的記録媒体を保管する場合は、外部電磁的記録媒体への書込禁止の措置を講じなければならない。

（カ）教育情報セキュリティ管理者又は教育情報システム管理者は、情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、より自然災害を被る可能性が低い地域又は安全が確保された施設に保管しなければならない。なお、クラウドサービスを利用する場合はサービスの機能として自然災害対策がなされていることを確認すること。

（キ）教育情報セキュリティ管理者又は教育情報システム管理者は、重要性分類Ⅲ以上の情報を記録した電磁的記録媒体を保管する場合、施錠可能な場所に保管しなければならない。

② 教職員等の遵守事項

（ア）教職員等及び事務局職員は、重要性分類Ⅱ以上の情報を、教育委員会が管理・承認したサーバまたは適切に管理された領域（暗号化等の措置が講じられた校務用端末のローカルディスク等）以外に保存してはならない。

なお、個人のクラウドストレージや許可のない電磁的記録媒体等への保存は、いかなる場合も禁止とする。

（イ）前項の規定にかかわらず、教育情報システム管理者が利用を承認した外部システム（国、地方公共団体または民間事業者が提供するものを含む）については、当該システム上に情報を保存することができる。

（ウ）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。

(7) 情報資産の外部持ち出し

① 分類に応じた情報資産の外部持ち出し制限

（ア）教職員等は、重要性分類Ⅱ以上の情報資産を外部持ち出しする場合は、限定されたアクセスの措置設定（アクセス制限や暗号化）を行い、教育情報セキュリティ管理者の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。

② 電子メール、外部ストレージサービスによる情報の送信

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

③ 外部電磁的記録媒体を用いた情報の外部持ち出し

外部電磁的記録媒体（USB メモリ、外付け HDD 等）を用いた情報資産の持ち出しは、紛失・盗難リスクを伴うことから原則として禁止とする。

ただし、業務遂行上、外部電磁的記録媒体を使用することが真にやむを得ない場合に限り、以下の条件をすべて満たすことで例外的に持ち出しを許可することができる。

（ア）持ち出すことができる情報は、重要性分類Ⅲ又はⅣの情報資産に限定されるものとし、重要性分類Ⅱ以上の情報資産を含めてはならない。

（イ）教職員等は、持ち出しの前に教育情報セキュリティ管理者の個別の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、（イ）の許可を与える際、当該媒体に重要性分類Ⅱ以上の情報資産が混在していないことを自ら点検・確認しなければならない。

（エ）使用後の媒体は、速やかに情報を消去し、教育情報セキュリティ管理者の確認を受けた上で、所定の保管場所に返却しなければならない。

④ 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。

⑤ 車両等により重要性分類Ⅲ以上の情報資産を運搬する場合は、電子データにあってはパスワード等による暗号化、紙媒体にあっては内容の視認防止措置を講じるとともに、車両等への放置禁止等、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。

⑥ 情報資産の公表

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

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

(8) 情報資産の廃棄等

① 情報資産を廃棄する教職員等及び事務局職員は、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。

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

③ 情報資産の廃棄・リース返却を行う教育委員会事務局職員は教育情報システム管理者の、教職員等は教育情報セキュリティ管理者の承認をそれぞれ得て、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。

④ 業者に廃棄委託する場合、廃棄する情報資産を業者が引き取る際、教育委員会事務局職員又は教職員等が立ち会わなければならない。

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

(2) 通信ケーブル等の配線

① 統括教育情報セキュリティ責任者及び教育情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、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。

③ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

④ 統括教育情報セキュリティ責任者、教育情報システム管理者は、自ら又は教育情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更又は追加できないように必要な措置を施さなければならない。

(3) 機器の定期保守及び修理

① 教育情報システム管理者は、重要性分類Ⅲ以上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。定期保守を実施できない場合、教育情報システム管理者は、情報システムが機能停止した際に、情報システムごとに定められた期間内に復旧が可能となるよう、必要な措置を講じなければならない。

② 教育情報システム管理者は、電磁的記録媒体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秘密保持体制の確認等を行わなければならない。

(4) 施設外又は学校外への機器の設置

統括教育情報セキュリティ責任者及び教育情報システム管理者は、施設外又は学校外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。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。

(5) 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（情報システム室等）の管理

(1) 管理区域の構造等

① 管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、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。

③ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、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。

④ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、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

① 教育情報システム管理者は、管理区域への入退室を許可された者のみに制限し、入退室管理簿の記載等による入退室管理を行わなければならない。

② 地方公共団体職員等及び外部委託事業者が、管理区域に入室を許可する場合、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。

③ 教育情報システム管理者は、外部からの訪問者が管理区域に入る場合には、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の際に職員による入室許可（社員証等の本人確認書類の提示）及び所持品の確認をするものとし、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。

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

(3) 機器等の搬入出

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

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

4.3. 通信回線及び通信回線装置の管理

(1) 統括教育情報セキュリティ責任者は、施設内の通信回線及び通信回線装置を、施設管理部門と連携し、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

(2) 統括教育情報セキュリティ責任者は、外部へのネットワーク接続ポイント及び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) 統括教育情報セキュリティ責任者は、重要性分類Ⅲ以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、インターネットを通信経路とする回線の場合、通信の暗号化を行わなければならない。

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

(5) 統括教育情報セキュリティ責任者は、重要性分類Ⅱ以上の情報資産を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。

(6) 統括教育情報セキュリティ責任者は、学校運営上必要なネットワーク帯域を確保するとともに、遅延等に対する適切な対策を講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。

4.4. 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 及び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) 教育情報システム管理者は、重要性分類Ⅱ以上の情報資産を取り扱う場合、多要素認証（生体認証、物理認証等）を設定しなければならない。特にパブリッククラウドの利用にあたっては、これを必須とする。

(4) 教育情報システム管理者は、前項の規定にかかわらず、児童生徒又は保護者が自らの情報に限定してアクセスする場合に限り、厳格な本人確認措置（パスワードの複雑性確保、ロック機能の有効化等）を講ずることを条件として、ID 及びパスワードによる認証を許容することができる。

(5) 教育情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末に暗号化機能を持つセキュリティチップが搭載されている場合、その機能を有効に活用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よう努めなければならない。

(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、重要性分類Ⅲ以上の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、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、重要性分類Ⅱ以上の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。

(8) 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、MDM（モバイル端末管理）等を用いて離れた場所から一元管理しなければならない。

(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。

5. 人的セキュリティ

5.1. 教育情報セキュリティ管理者の措置事項

(1) 情報資産の管理

① 情報資産の持ち出し及び持ち込みの記録管理

教育情報セキュリティ管理者は、教職員等による情報資産の外部持ち出しについて、記録管理しなければならない。

② 情報資産の廃棄管理

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

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

② 教育情報セキュリティ管理者は、校内でセキュリティ事故につながりかねないヒヤリ・ハット事案を抑止するために、教職員等が事案を発見した際に、ただちに対処し、すみやかに報告が上がるよう、教職員等に対する情報セキュリティ意識の醸成と風通しのよい関係性維持に努めなければならない。

③ 教育情報セキュリティ管理者は、教職員等が常に教育情報セキュリティポリシー及び実施手順を閲覧・確認できるように配慮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) 教職員等への情報セキュリティポリシー等の遵守指導

教育情報セキュリティ管理者は、新規採用教職員等及び他自治体から本市に新規赴任した教職員等、及び非常勤及び臨時の教職員に対し、教育情報セキュリティポリシー等遵守すべき内容を理解・浸透するように指導を行わなければならない。

(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、ソフトウェア等（クラウドサービス等を含む）の導入又は利用に際し、教職員等から要望があった場合は、申請書を作成させ、その教育上の必要性及び費用対効果を確認した上で、教育情報システム管理者に申請し、その承認を得るものとする。

(6) インターネット接続及び電子メール利用の制限

教育情報セキュリティ管理者は、教職員等に対し、業務端末によるインターネット接続及び電子メールの利用を業務目的に限定するよう指導・監督しなければならない。

(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。

① 来校者の氏名及び入退時刻を記録しなければならない。

② 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。

③ 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

① 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。

② 教育情報セキュリティ管理者は、自己点検の結果を CISO に報告しなければならない。

5.2. 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) 教育情報セキュリティポリシー等の遵守

教職員等は、教育情報セキュリティポリシー及び実施手順を遵守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

① 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。

② 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または学校教育情報セキュリティ・システム担当の許可を求めなければならない。

③ 机上の書類・端末等の管理

教職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は教育情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

(3) 支給端末の取扱い

① 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。

② 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及びメモリ増設等の改造を無断でしてはならない。

③ 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、安全管理措置を講じなければならない

④ 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。

⑤ 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。

(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

① 教職員等は、原則として、支給以外のパソコン、モバイル端末、電磁的記録媒体等を業務に利用してはならない。ただし、教育情報システム管理者が、利用目的及び安全性を確認した上で許可した場合は、この限りではない。

② 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、必要な安全管理措置を講じなければならない。

(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

① 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。

② 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、必要な安全管理措置を講じなければならない。

(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。

① 自己が利用している ID は、他人に利用させてはならない。

② 共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

③ 教職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、教育情報セキュリティ責任者又は教育情報システム管理者に通知しなければならない。

(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。

① 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。

② パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

③ パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

④ パスワードが流出したおそれがある場合には、教育情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

⑤ 複数の教育情報システムを扱う教職員等は、同一のパスワードを複数のシステム間で用いてはならない。（シングルサインオンを除く）

⑥ 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。

⑦ 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）

(8) 外部電磁的記録媒体の取扱い

① 利用する外部電磁的記録媒体は教育委員会事務局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する。

② 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。

(9) 電子メールの利用制限

① 教職員等は、自動転送機能を用いて、本市が管理するメールアドレス、又は教育情報システム管理者が公認するドメインのメールアドレス以外へ電子メールを転送してはならない。

② 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。

③ 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。

④ 教職員等は、重要性分類Ⅲ以上の情報を含む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。

⑤ 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使用してはならない。

⑥ 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。

⑦ 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。

(10) 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

① 強固なアクセス制御による対策を講じたシステム構成でない場合、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。

② 私的に契約したクラウドサービスや個人アカウントを業務利用してはならない。

③ ソーシャルメディアサービスを利用して、業務上知り得た情報を公開してはならない。

(11) 不正プログラム対策

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。

① パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

② 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つよう努めなければならない。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。

③ 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。

④ 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。

⑤ 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。

⑥ 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。

⑦ コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、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）有線 LAN につながる業務端末の場合は、LAN ケーブルの即時取り外しを行わなければならない。

（イ）無線 LAN につながる業務端末の場合は、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。

(12)　電子署名・暗号化

① 教職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、CISO が定めた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

② 教職員等は、暗号化を行う場合に CISO が定める以外の方法を用いてはならない。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。

③ 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。

(13)　新規のソフトウェア、サービス及び機器の導入・利用制限

① 教職員等は、支給された端末等の情報システムに対し、以下の行為を無断で行ってはならない。

（ア）ソフトウェアのインストール（フリーソフト、ブラウザ拡張機能等を含む）。

（イ）約款への同意のみで利用可能となるクラウドサービスの業務利用（生成 AI、ファイル転送、SNS、フリーメール等を含む）。

（ウ）機器の接続、増設、交換および改造（私物端末、Wi-Fi ルータ、USB メモリ、メモリ増設等）。

② 教職員等は、業務上、前項に掲げる資産の導入又は利用が必要な場合は、教育情報セキュリティ管理者の指示に従い、教育上の必要性、費用対効果及び管理方法等を記載した申請書を作成しなければならない。

(14)　無許可でのネットワーク接続の禁止

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

(15)　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。

(16)　外部からのアクセス等の制限

① 教職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、教育情報セキュリティ管理者を介して、統括教育情報セキュリティ責任者及び当該情報システムを管理する教育情報システム管理者の許可を得なければならない。

② 教職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を施設内のネットワークに接続する前に、アンチウイルス等を通じて、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

(17)　異動・退職時等の遵守事項

① 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。

② 前項の規定にかかわらず、教育活動の継続性を図るため、教職員等が自ら作成した教材・教具等の著作物（個人情報及び機密情報を含まないものに限る）については、教育情報セキュリティ管理者の許可を得て、複製し持ち出すことができる。

(18)　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当たり、以下の事項について指導を行わなければならない。

① 学習用途の利用限定

学習者用端末及び学習系クラウドサービスは学習目的で利用すること。

② 利用者認証情報の秘匿管理

ID 及びパスワードは他の人に知られないようにすること。また、他人の ID 及びパスワードを使ってなりすましをしないこと。

③ 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。

④ 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。

⑤ 無断で外部ソフトウェアをインストール禁止

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。

⑥ 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のみを利用すること。

⑦ 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。

⑧ 端末の安全な取扱い

学習者用端末は自分専用のものとして大事に取り扱い、他人に貸し借りしないこと。また、盗難・紛失・破損等に注意すること。

⑨ 私物端末など許可されていない端末の利用禁止

私物端末など許可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。

⑩ 重要性分類Ⅱ以上の情報資産（児童生徒本人の情報に限る）の管理

該当資産を端末にダウンロードした場合には、目的を達成し次第すみやかに消去を行う等の対策を講じること。また、該当資産を閲覧する際には、離席時に端末ロックし、周囲に他の児童生徒がいる状態では閲覧しない等の対策を講じること。

5.3. 教育委員会事務局職員の遵守事項

教育委員会事務局職員は、教育情報セキュリティ責任者の指導の下、以下の規定を遵守しなければならない。

(1) 教育情報セキュリティポリシー等の遵守
(2) 業務以外の目的での使用の禁止
(3) 校務用端末による外部における情報処理作業の禁止
(4) 重要性分類Ⅱ以上の情報資産について校務用端末以外のパソコン、モバイル端末及び電磁的記録媒体等によるアクセスの禁止
(5) 知りえた情報の秘匿
(6) 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

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。

(2) 研修計画の策定及び実施

① 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。

② 研修計画において、教職員等は、毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。

③ 研修は、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム担当者及びその他教職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにするよう努めなければならない。

(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) 庁内での情報セキュリティインシデントの報告

① 教育情報セキュリティ責任者（CISO）は、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として、本市（市長部局）が設置する窓口を準用するものとする。

② CISO は、前項の窓口への連絡手段を、市の公式ウェブサイト等を通じて住民等が容易に知ることができるよう、市長部局と連携して適切な措置を講じなければならない。

③ CISO は、準用する窓口を通じて教育委員会の情報資産に関する報告を受けた場合、市長部局の担当部署より速やかに情報の提供を受ける体制を整えなければならない。

(2) 情報セキュリティインシデント原因の究明・記録、再発防止等

① 統括教育情報セキュリティ責任者は、情報セキュリティインシデントについて、教育情報セキュリティ管理者、教育情報システム管理者及び情報セキュリティに関する統一的な窓口と連携し、これらの情報セキュリティインシデント原因を究明し、記録を

保存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。

② CISO は、統括教育情報セキュリティ責任者から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

(3) 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管理

(1) 文書サーバ及び端末の設定等

① 教育情報システム管理者は、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。

② 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。

③ 教育情報システム管理者は、住民の個人情報、人事記録等、特定の教職員等しか取扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一学校等であっても、担当職員以外の教職員等が閲覧及び使用できないようにしなければならない。

④ 教育情報システム管理者は、校務系サーバ、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データの外部流出の可能性を考慮し、情報の重要性に応じた適切な安全管理措置を講じなければならない。

(2) バックアップの実施

統括教育情報セキュリティ責任者及び教育情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、次の①及び②に基づきバックアップを実施するものとする。

① 校務系情報及び校務外部接続系情報については、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。

② 学習系情報については、必要に応じて定期的にバックアップを実施しなければならない。

(3) ログの取得等

① 統括教育情報セキュリティ責任者及び教育情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、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。

③ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施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

① 統括教育情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、所管するネットワークの内部におけるファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

② 統括教育情報セキュリティ責任者は、不正アクセスを防止するため、所管するネットワークに適切なアクセス制御を施さなければならない。

(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

① 教育情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO 及び統括教育情報セキュリティ責任者の許可を得なければならない。

② 教育情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内及び学校の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

③ 教育情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

④ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、教育ネットワークへの侵入を防御するために、ファ

イアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

⑤ 教育情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括教育情報セキュリティ責任者の判断に従い、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

① 教育情報システム管理者は、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、及び児童生徒による当該情報への不正アクセスを防止するため、情報の重要性及びシステム構成に応じ、次の各号に掲げる措置を講じなければならない。

（ア）校務系システム及び学習系システム間については、通信回線を物理的に分離し、インターネット側からの脅威から重要情報を隔離すること。

（イ）同一のネットワーク経路又は同一のアカウント体系を利用する構成にあっては、異なるアカウント体系の採用、又は適切なアクセス権限の設定等のアクセス制御を徹底し、情報の重要性に応じた機密性を確保すること。

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

(8) 複合機のセキュリティ管理

① 統括教育情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を定めなければならない。

② 統括教育情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③ 統括教育情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

(9) 特定用途機器のセキュリティ管理

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

(10)　無線 LAN 及びネットワークの盗聴対策

① 統括教育情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な通信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。

② 統括教育情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、通信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

① 統括教育情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送(電子メールの中継処理)が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

② 統括教育情報セキュリティ責任者は、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。

③ 統括教育情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④ 統括教育情報セキュリティ責任者は、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。

⑤ 統括教育情報セキュリティ責任者は、システム開発や運用、保守等のため施設内に常駐している外部委託事業者の作業員による電子メールアドレス利用について、外部委託事業者との間で利用方法を取り決めなければならない。

6.2. アクセス制御

(1) アクセス制御等

統括教育情報セキュリティ責任者又は教育情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員等がアクセスできないように、システム上制限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、重要性分類Ⅱ以上の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) 外部からのアクセス等の制限

① 統括教育情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

② 統括教育情報セキュリティ責任者は、民間事業者等の外部組織からのシステムアクセスを認める場合、アクセスする利用者の本人確認、システムアクセスの対象となる児童生徒の本人（保護者）同意を得る等の措置を講じなければならない。

③ 統括教育情報セキュリティ責任者は、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の暗号化等の措置を講じなければならない。

④ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部からのアクセスに利用するモバイル端末を教職員等に貸与する場合、モバイル端末管理（MDM）の導入等を通じて、セキュリティ確保のために必要な措置を講じなければならない。

⑤ 統括教育情報セキュリティ責任者は、外部から教育ネットワークに接続することを許可する場合は、利用者の ID 及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

(3) 端末とネットワークの接続可否の自動識別（端末認証）の設定

統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク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

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

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、機器及びソフトウェアの調達に当たっては、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

① システム開発における責任者及び作業者の特定

教育情報システム管理者は、システム開発の責任者及び作業者を特定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。

② システム開発における責任者、作業者の ID の管理

統括教育情報セキュリティ責任者及び教育情報システム管理者は、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。

（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。

③ システム開発に用いるハードウェア及びソフトウェアの管理

（ア）教育情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定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

① 開発環境と運用環境の分離及び移行手順の明確化

（ア）教育情報システム管理者は、システム開発、保守及びテストを行う場合、原則として運用環境から分離された環境で行うよう努めなければならない。

（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。

② テストの実施基準

（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、既存システムへの影響を確認するため、必要に応じた範囲で動作試験を行わなければならない。

（イ）運用テストは、原則として擬似環境（テスト用アカウントやサンドボックス等）で行うものとする。ただし、クラウドサービス等の特性上、擬似環境の準備が困難な場合は、本番環境への影響を最小限にする計画をもってこれに代えることができる。

（ウ）テストデータには、原則として個人情報及び機密性の高い生データを使用してはならない。やむを得ず使用する場合は、特定の個人を識別できないよう加工（マスキング）を施した上で、必要最小限の範囲で利用するものとする。

（エ）教育情報システム管理者は、導入に先立ち受入テストを行い、その結果を確認しなければならない。また、脆弱性の確認については、システムの特性に応じ、開発ベンダーが提供する試験結果報告書や、外部認証（ISMAP、SOC2 等）の確認をもって脆弱性テストに代えることができる。

(4) システム開発・保守に関連する資料等の整備・保管

① 教育情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

② 教育情報システム管理者は、テスト結果を一定期間保管しなければならない。

③ 教育情報システム管理者は、情報システムに係るソースコードならびに使用したオープンソースのバージョン（リポジトリ）を適切な方法で保管しなければならない。

(5) 情報システムにおける入出力データの正確性の確保

① 教育情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

② 教育情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計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) 統括教育情報セキュリティ責任者の措置事項

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

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

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

③ コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ教職員等に対して注意喚起しなければならない。

④ 所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

⑤ 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

⑥ 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

⑦ 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。

(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。

① 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を守るため、コンピュータウイルス等の不正プログラムへの対策を講じなければならない。
② 不正プログラム対策は、常に最新の状態に保たなければならない。
③ 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。

6.5. 不正アクセス対策

(1) 統括教育情報セキュリティ責任者の措置事項

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

① 教育情報システム管理者は、不要な SSID（無線 LAN ネットワーク名）を無効化するものとするとともに、重要なネットワーク機器の未使用ポートの閉鎖その他の無断接続を防止するための必要な措置を講じなければならない。
② 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。
③ 教育情報システム管理者は、ウェブページの改ざんによる被害を防ぐため、データの書き換え検知や速やかな異常確認に努めるものとする。
④ 統括教育情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

(2) 攻撃の予告

CISO 及び統括教育情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講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

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

(4) 標的型攻撃

統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、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

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

(2) 不正プログラム等のセキュリティ情報の収集及び周知

統括教育情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、教職員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

統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

7. 運用

7.1. 情報システムの監視

(1) 統括教育情報セキュリティ責任者及び教育情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視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、重要性分類Ⅱ以上の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）などの端末・サーバ・通信の監視・制御等によるセキュリティ対策を講じなければならない。

(2) 統括教育情報セキュリティ責任者及び教育情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

(3) 統括教育情報セキュリティ責任者及び教育情報システム管理者は、重要性分類Ⅱ以上の情報資産を格納するシステムを常時監視しなければならない。

(4) 統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等及び外部委託事業者が使用しているパソコン等の端末からの所管するネットワークのサーバ等に対する攻撃や外部のサイトに対する攻撃を監視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

① 教育情報システム管理者は、所管する教育情報システムの運用において実施した作業について、作業記録を作成しなければならない。

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、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。

③ 統括教育情報セキュリティ責任者、教育情報システム管理者又は教育情報システム担当者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、あらかじめ定められた手順に基づき実施するとともに、作業内容及び結果の確認を確実に行わなければならない。

(2) 情報システム仕様書等の管理

統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク構成図、情報システム仕様書等について、記録媒体に関わらず、業務上必要とする者以外の者による閲覧や紛失等がないよう、適切に管理しなければならない。

(3) 障害記録の管理

統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

(4) 記録の保存

CISO 及び統括教育情報セキュリティ責任者は、サーバ等に攻撃を受け、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

① 統括教育情報セキュリティ責任者及び教育情報システム管理者は、利用者の登録、変更、抹消等の情報管理、教職員等の異動、出向、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、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

① 統括教育情報セキュリティ責任者又は教育情報システム管理者は、教職員等のパスワードに関する情報を厳重に管理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。

② 統括教育情報セキュリティ責任者又は教育情報システム管理者は、教職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

7.4. IC カード等の取扱い

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

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、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

① 教育情報システム管理者は、児童生徒の ID について、シンプルかつユニーク（唯一無二）であり、卒業まで永続的に識別可能な構成となるよう適切な措置を講じなければならない。また、ID 登録やパスワードポリシーについては、教育委員会等の組織にて一元管理するよう努めるものとする。

② 教育情報システム管理者は、進級・進学時において、原則として ID そのものを変更せず、ID に付随する属性情報（組・出席番号、学校名など）を更新することで対応しなければならない。

③ 教育情報システム管理者は、転出・卒業・退学等により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期間を設けた上で、ID の利用停止および関連するデータの完全削除を行わなければならない。

(2) 多要素認証等によるなりすまし対策

① パブリッククラウド上で重要性分類Ⅱ以上の情報資産（成績、個別の指導記録等）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なければならない。

② ただし、児童生徒またはその保護者が当該情報資産にアクセスする場合については、パスワードの秘匿管理の徹底、ロック機能（誤入力時のアカウントロック）の有効化、パスワードの複雑性の確保等により本人確認を厳格に行うことを前提に、ID 及びパスワードでの認証を許容する。

(3) シングルサインオンの活用

教育情報システム管理者は、学習用ツールごとの認証情報の管理負担を軽減し、セキュリティリスクを低減するため、一度の認証により複数のサービスにアクセスできるシングルサインオン（SSO）の導入に努めるものとする。

7.6. 特権を付与された ID の管理等

(1) 利用者の限定と厳重管理

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（以下「特権 ID」という）を利用する者を業務上必要な最小限の者に限定し、当該 ID およびパスワードの漏洩等が発生しないよう、厳重に管理しなければならない。

(2) ID 登録・変更・削除

教育情報システム管理者の特権を代行する者は、教育情報システム管理者が指名し、CISO または統括教育情報セキュリティ責任者が認めた者でなければならない。

(3) 外部委託業者への委任禁止

教育情報システム管理者は、特権 ID およびパスワードの変更・更新作業について、外部委託事業者に行わせてはならない。

(4) セキュリティ機能の強化

① 教育情報システム管理者は、特権 ID について、多要素認証の実装を原則とする。

② 多要素認証の実装が困難なシステムにおいては、次の各号に掲げる対策を組み合わせて実施し、安全性を確保しなければならない。

（ア）パスワードの長正化（原則 10 桁以上、最低 8 桁以上）及び複雑性の強化

（イ）特権操作ログの常時監視及び異常なアクセスパターンの検知

③ 教育情報システム管理者は、システム上の制限により前項の措置の一部が実施できない場合であっても、有効期間の短縮設定や入力回数制限の厳格化など、当該システムで利用可能なセキュリティ機能を最大限に活用し、特権 ID の保護に努めるものとする。

(5) 初期 ID の変更

教育情報システム管理者は、特権 ID を初期設定（デフォルト）のまま使用せず、推測困難なものに変更しなければならない。

(6) ログの監視

教育情報システム管理者は、不正利用を早期に発見するため、特権 ID による操作ログの監視を行わなければならない。

7.7. 教育情報セキュリティポリシーの遵守状況の確認・管理

(1) 遵守状況の確認及び対処

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

② CISO 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。

③ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処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及び対処

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

(4) 教職員等による不正アクセスの管理

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

7.8. 専門家の支援体制等

(1) 専門家の支援体制

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

(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、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。

7.9. 侵害時の対応等

(1) 緊急時対応計画の策定

CISOは、情報セキュリティインシデント（事故・障害・違反等）が発生した場合、またはそのおそれがある場合に、迅速かつ適切に被害拡大の防止、復旧、証拠保全等を行うため、緊急時対応計画を策定しなければならない。

(2) 緊急時対応計画には、少なくとも以下の事項を定めなければならない

① 関係者の連絡先（緊急連絡網）
② 発生した事案に係る報告すべき事項
③ 発生した事案への対応措置（初動対応、被害拡大防止措置）
④ 再発防止措置の策定手順

(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、CISOは当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

(4) 緊急時対応計画の見直し

CISOは、組織体制の変更や新たな脅威の出現等に応じ、必要に応じて緊急時対応計画を見直さなければならない。

7.10. 緊急時における連絡体制

(1) インシデントの分類

インシデント対応の迅速化及び適切な指揮命令を行うため、事案の重要度を以下の３段階（レベル）に分類する。

① レベル１（軽微な事案）

記録媒体等の紛失（所在不明)、不審なメールの開封、不正アクセスの痕跡等、セキュリティ侵害が疑われる事象の発見。

② レベル２（重大な事案）

ウイルス感染等のセキュリティ被害の確認、校務に支障が出るシステムトラブル、限定的な範囲での情報の流出等、組織的な対応が必要な事案。

③ レベル３（緊急事態）

教育活動の停止を伴うシステム障害、多数の個人情報漏洩、報道機関への公表が予想される事案等、全庁的な対応を要すると統括教育情報セキュリティ責任者が認める事案。

(2) インシデントの発見および第一報

インシデントの発見者は、発見の経緯に応じ、速やかに以下の手順で報告を行わなければならない。

① 教職員等及び事務局職員による発見

教職員等及び事務局職員は、業務遂行中にインシデントまたはその兆候（レベル１以上）を発見した場合、直ちに実施手順で定める被害拡大防止措置を行った後、速やかに以下の区分に従い報告しなければならない。

（ア）教職員等にあっては、所属する学校の教育情報セキュリティ管理者へ報告する。

（イ）事務局職員にあっては、教育情報システム管理者へ報告する。

② 外部委託事業者からの報告

教育情報システムの保守・運用を行う外部委託事業者が、監視アラート等により異常を検知した場合は、契約およびSLA（サービスレベル合意書）に基づき、直ちに教育情報システム担当者または教育情報システム管理者へ通報を行うものとする。通報を受けた職員は、速やかに内容を確認し、レベル判定のプロセスへ移行しなければならない。

③ 外部（児童生徒、保護者、市民等）からの通報

児童生徒、保護者、市民等から、情報セキュリティに関する通報（Web サイトの不具合、情報の流出等）を受けた教職員または事務局職員は、通報内容を正確に記録し、速やかに以下の区分に従い報告しなければならない。

（ア）教職員等にあっては、所属する学校の教育情報セキュリティ管理者へ報告する。

（イ）事務局職員にあっては、教育情報セキュリティ責任者へ報告する。

④ 市長部局等からの連絡

市長部局の CSIRT から､庁内ネットワークにおける攻撃の検知等の連絡を受けた場合、連絡を受けた職員は直ちに教育情報システム管理者へ報告し、連携して対応に当たるものとする。

(3) 教育情報セキュリティ管理者からの報告

教職員等から報告を受けた教育情報セキュリティ管理者は、事案の内容に応じ、直ちに教育委員会事務局の以下の窓口へ報告し、指示を仰がなければならない。

① 技術的な事案（ウイルス、端末・ネットワーク障害等）については、教育情報システム管理者に連絡を行うものとする。

② 人的な事案（情報の紛失、メールの誤送信、不正アクセス等）については、教育情報セキュリティ責任者に連絡を行うものとする。

③ 判断に迷う場合、または両方に関連する場合は、双方へ連絡を行うものとする。

(4) 初期対応と教育 CSIRT の招集

報告を受けた教育情報システム管理者または教育情報セキュリティ責任者は、情報政策担当部局と連携し、直ちに初期調査を行い、事案のレベルを判定する。

レベル 2 以上と判定した場合、直ちに教育 CSIRT 構成員への緊急連絡を行い、迅速な情報共有のもと組織的な対応を開始しなければならない。

組織的な対応が開始された後は、各学校への指示、事業者への命令、及び関係機関への広報対応は、原則として教育 CSIRT が一元的に行うものとする。

(5) レベル２における市長部局等との連携

教育 CSIRT は、レベル２以上と判定した段階で、速やかに市長部局の CSIRT へ事案の概要を共有し、技術的な連携及び支援を要請しなければならない。

被害が行政系ネットワークへ波及するおそれがある場合は、市長部局と協議の上、ネットワークの遮断等の措置を講ずるものとする。

(6) レベル３の判定及び全庁的な意思決定

統括教育情報セキュリティ責任者は、報告された事案が以下のいずれかに該当する場合、またはそのおそれが高いと認める場合、レベル３と判定する。

① 教育情報システムの停止等により、学校の教育活動の継続が困難となる場合
② 紛失、漏洩等した情報資産の件数や内容から、重大な被害が想定される場合
③ 報道機関による報道や SNS 等による拡散など、社会的影響が拡大している場合
④ 市長部局のネットワークへ被害が波及する可能性がある場合

(7) 市長部局への報告及び全庁的な対応

CISO は、前項の規定によりレベル３と判定した場合、速やかに市長部局の CISO へ事案の概要を共有し、全庁的な対応体制について協議しなければならない。

ただし、CISO が不在の場合、または事態が切迫しており CISO の判定を待つ時間的猶予がない場合は、統括教育情報セキュリティ責任者が CISO の職務を代理し、レベル３の判定及び市長部局への連絡を行うことができる。

教育 CSIRT は、前項の規定による判定前であっても、被害拡大防止のために必要と認める場合は、暫定的にレベル３相当とみなして、ネットワークの遮断等の緊急措置を講ずることができる。

(8) 関係機関への報告

統括教育情報セキュリティ責任者は、個人情報の漏洩等の重大なインシデントが発生した場合、法令等の定めに従い、個人情報保護委員会、文部科学省、警察等の関係機関へ速やかに報告を行わなければならない。

7.11. 例外措置

(1) 例外措置の許可

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

(2) 緊急時の例外措置

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

7.12. 法令等遵守

教職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令等を遵守し、これに従わなければならない。

① 地方公務員法（昭和25年12月13日法律第261号）
② 教育公務員特例法（昭和24年1月12日法律第1号）
③ 著作権法（昭和45年法律第48号）
④ 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）
⑤ 個人情報の保護に関する法律（平成15年5月30日法律第57号）
⑥ 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）
⑦ サイバーセキュリティ基本法（平成26年法律第104号）
⑧ 藤枝市個人情報保護法施行条例（令和4年条例第30号）

7.13. 懲戒処分等

(1) 懲戒処分

教育情報セキュリティポリシーに違反した教職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、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。

① 統括教育情報セキュリティ責任者が違反を確認した場合は、統括教育情報セキュリティ責任者は当該教職員等が所属する学校の教育情報セキュリティ管理者に通知し、適切な措置を求めなければならない。
② 教育情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括教育情報セキュリティ責任者及び当該教職員等が所属する学校の教育情報セキュリティ管理者に通知し、適切な措置を求めなければならない。
③ 教育情報セキュリティ管理者の指導によっても改善されない場合、統括教育情報セキュリティ責任者は、当該教職員等の教育ネットワーク又は教育情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括教育情報セ

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

8. 外部委託

(1) 外部委託事業者の選定基準

① 教育情報システム管理者は、外部委託事業者の選定に当たり、委託内容に応じた十分な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。

② 選定に当たっては、ISMAP（政府情報システムのためのセキュリティ評価制度）や ISMS（情報セキュリティマネジメントシステム）、プライバシーマーク等の第三者認証の取得状況や、過去の実績等を評価材料としなければならない。

(2) 契約項目

外部委託契約（仕様書を含む）を締結する場合には、必要に応じて以下の情報セキュリティ要件を明記しなければならない。

① 教育情報セキュリティポリシー及び実施手順の遵守
② 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
③ 提供されるサービスレベルの保証（SLA）
④ 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
⑤ 外部委託事業者の従業員に対する教育の実施
⑥ 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
⑦ 業務上知り得た情報の守秘義務
⑧ 再委託に関する制限事項の遵守（原則禁止または事前の書面承諾）
⑨ 委託業務終了時の情報資産の返還、廃棄等
⑩ 委託業務の定期報告及び緊急時報告義務
⑪ 本市（学校設置者）による監査、検査の受け入れ
⑫ 本市（学校設置者）による情報セキュリティインシデント発生時の公表権限
⑬ 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、契約解除等）

(3) 確認・措置等

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

教育情報システム管理者は、SaaS 型パブリッククラウドサービス（以下「クラウドサービス」という）を選定・利用するにあたり、当該サービスが以下の技術的要件を満たしていることを、サービス仕様書や約款等において確認しなければならない。

(1) 利用者認証

ログインに関わる認証機能が提供されており、管理者権限を持つ者や開発者に対しても適切な本人確認が行われていること。

(2) アクセス制御

アクセス権限のない者がデータにアクセスできないようシステム上で制限する機能が提供されていること。

(3) 暗号化

クラウドサービス上に保管されるデータ、および学校等のネットワーク境界からクラウドサービスまでの通信経路において、暗号化等の保護措置が講じられていること。

(4) マルチテナント保護

複数の利用者がリソースを共用する環境において、他の利用者の影響を受けないよう論理的な分離等の対策が講じられていること。

(5) 脅威対策

外部からの不正な通信・侵入を防ぐ措置、検知・防御する対策、およびサーバ等へのマルウェア感染対策が講じられていること。

(6) 物理的セキュリティ

データセンター等の物理的セキュリティ対策が、本ポリシーに定める管理区域の基準に準じて講じられていること。

(7) 運用管理

データのバックアップ体制、復旧手順、およびセキュリティ監査に必要なログの取得が可能であること。

(8) 廃棄

サービス利用終了時において、データおよびアカウント情報が確実に消去される手順が確立されていること。

9.2. クラウド事業者との契約および確認事項

教育情報システム管理者は、クラウドサービスを利用する場合、クラウド事業者との間で、以下の事項について約款または契約書面上で確認または合意しなければならない。

(1) 守秘義務等

提供した情報の守秘義務、目的外利用の禁止、および第三者への提供の禁止（契約違反時の損害賠償規定を含む）。

(2) 準拠法・管轄

サービスに適用される法令および管轄裁判所（原則として日本国内法および日本国内の裁判所であること）

(3) 管理体制・教育

クラウド事業者の責任者が明確であり、従業員に対して適切なセキュリティ教育が実施されていること。

(4) 責任分界点

情報セキュリティに関する役割の範囲と責任分界点が明確であること。

(5) サービスレベル

稼働率や復旧時間等のサービスレベル（SLA）が業務遂行に求められる水準を満たしていること。

(6) サプライチェーン

再委託先に対しても同等のセキュリティ対策が義務付けられていること。

(7) 運用管理

データのバックアップ体制、復旧手順、およびセキュリティ監査に必要なログの取得が可能であること。

(8) 廃棄

サービス利用終了時において、データおよびアカウント情報が確実に消去される手順が確立されていること。

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 及びパスワード等の秘匿

① 教職員等は、ID 及びパスワードについて秘匿管理を行わなければならない。

② 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

① パブリッククラウドにおけるアクセス制御

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なければならない。

② 児童生徒及び保護者によるアクセスの特例

前項の規定にかかわらず、児童生徒またはその保護者が、当該児童生徒本人に関する情報資産（重要性分類Ⅱ以上）にアクセスする場合は、ID 及びパスワードによる認証を許容することができる。

③ 特例利用時の安全確保措置

前項の特例を適用する場合は、多要素認証の利用に努めるとともに、これに代わる安全確保措置として、次の各号に掲げる措置により本人確認を厳格に行わなければならない。

（ア）パスワードの秘匿管理の徹底

（イ）当該システムにおいて利用可能な、複数回誤入力時のロック機能（アカウントロック）又は入力制限機能の有効化

（ウ）パスワードの複雑性の確保

(4) 学校外からのパブリッククラウド利用

① 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。

② 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。

(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

① 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。

② 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

① 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 教育情報システム管理者は、約款による外部サービスの利用に当たっては、約款において以下の点が規定されていることを確認しなければならない。

（ア）利用者が登録した情報が、利用者の同意なく無断使用（目的外利用、第三者への提供等）されないこと

（イ）サービス事業者が業務上知り得た情報の守秘義務が守られること

(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。

① 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。

② 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。ただし、あらかじめ定められた運用手順に基づき、本人等の同意を得た広報目的の情報については、この限りではない。

(3) 利用するソーシャルメディアサービスごとに運用責任者を定め、当該アカウントの適切な管理及び発信内容の確認を行わせなければならない。

10. 評価・見直し

10.1. 監査

(1) 実施方法

CISO は、教育情報システム管理者にネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

(2) 監査を行う者の要件

① 教育情報システム管理者は、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。

② 監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者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

① 教育情報システム管理者は、監査を行うに当たって、監査の対象、時期、方法等を定めた監査実施計画を立案し、CISOの承認を得なければならない。

② 被監査部門（教育委員会事務局及び学校）は、監査責任者及び監査員から資料の提出や聞き取り等を求められた場合には、業務に支障のない範囲で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

① 教育情報システム管理者は、業務を外部委託している場合（クラウドサービスの利用を含む）、委託事業者（再委託事業者を含む。）に対して、本ポリシー及び契約に基づく情報セキュリティ対策の遵守状況について、定期的又は必要に応じて監査を行わなければならない。

② 前号の監査において、委託事業者への実地監査が困難な場合、又はSaaS型パブリッククラウドサービスを利用する場合は、委託事業者が提出する監査報告書（第三者監査の結果や、ISMAP等の認証取得状況を示す書類）の確認をもって、監査に代えることができる。

(5) 報告

教育情報システム管理者は、監査結果を取りまとめ、CISOに報告する。

(6) 保管

① 教育情報システム管理者は、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) 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

CISOは、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

10.2. 自己点検

(1) 実施方法

① 統括教育情報セキュリティ責任者及び教育情報システム管理者は、所管するネットワーク及び情報システムについて、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。

② 教育情報セキュリティ責任者は、教育情報セキュリティ管理者と連携して、所管する部局における教育情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

(2) 報告

統括教育情報セキュリティ責任者、教育情報システム管理者及び教育情報セキュリティ責任者は、自己点検結果及びそれに基づく改善策を取りまとめ、CISOに報告しなければならない。

(3) 自己点検結果の活用

① 教職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

② CISO は、この点検結果を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。