弟子屈町教育情報セキュリティポリシー

弟子屈町教育委員会

【令和２年１０月１５日施行】

【令和３年　７月１５日改訂】

《目　次》

序　弟子屈町教育情報セキュリティポリシーの構成

本町が設置する学校においては、指導要録、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機微な情報が保管され、また、コンピュータを活用した学習活動の実施など、教職員はもとより、児童生徒が日常的に情報システムにアクセスする機会があり、他の行政事務とは異なる特徴を有している。

学校における情報の漏えいや不正アクセスの防止等の情報セキュリティ対策は、教職員及び児童生徒が安心して ICT を活用できるようにするために不可欠な条件であり、情報セキュリティに関する意識・リテラシーを高め、その対策に取り組まなければならない。

以上のことから、弟子屈町立小中学校における教育情報セキュリティ対策を定める「弟子屈町教育情報セキュリティポリシー」を策定するものとする。

情報セキュリティポリシーは、「基本方針」と「対策基準」から構成されるが、「基本方針」は本町が所掌する情報資産全般に関する情報セキュリティ対策について総合的、体系的かつ具体的に取りまとめた共通のものであることから、この「弟子屈町教育情報セキュリティポリシー」においても「弟子屈町情報セキュリティポリシー（令和２年９月施行。第 2.0 版）」の基本方針に従うものとする。

「対策基準」は、学校の特徴を踏まえる必要があることから、文部科学省が策定する「教育情報セキュリティポリシーに関するガイドライン」を参考に、弟子屈町立小中学校を対象として構成したものである。

また、弟子屈町教育情報セキュリティポリシーに基づくセキュリティ対策の実施手順については、各学校の教育システムに応じ定めるものとし、その際の標準例として「弟子屈町教育情報セキュリティ実施手順」を示す。

第１章　弟子屈町情報セキュリティ基本方針

1. 目的

弟子屈町の各情報システムが取り扱う情報には、町民の個人情報のみならず行政運営上重要な情報など、外部に漏洩等した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報及び情報を取り扱う情報システムをさまざまな脅威から防御することは、町民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。

また、人口減少時代を迎えた我が国において、AI などによる業務の自動化など ICT の進化が期待されているところがある。弟子屈町がこれらに積極的に対応するためには、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、弟子屈町の情報資産の機密性、完全性及び可用性を維持するための対策（情報セキュリティ対策）を整備するために弟子屈町情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については弟子屈町の情報セキュリティ対策の基本的な方針として、情報セキュリティの対象位置付けを定めるものとする。

2. 定義

⑴　情報資産

本基本方針が対象とする情報資産は、次のとおりとする。

①　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

②　ネットワーク及び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　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

⑵　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。

⑶　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。

⑷　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。

⑸　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

⑹　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。

⑺　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。

⑻　可用性

情報にアクセスすることを認められた者が、必要な時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。

⑼ マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障及び地方税等に関する事務）に関わる情報システム及びデータをいう。

⑽ LGWAN 接続系

財務会計及び人事給与等LGWANに接続された情報システム及びその情報システムで取り扱うデータをいう。

⑾ インターネット接続系

インターネットメール、Web 閲覧等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

⑿ 通信経路の分割

マイナンバー利用事務系、LGWAN 接続系及びインターネット接続系の環境間の通信環境を分離した上で安全が確保された通信だけを許可できるようにすることをいう。

⒀ 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウィルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

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。

⑴ 不正アクセス、ウィルス攻撃、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

⑵ 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、外部委託管理の不備、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

⑶ 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

⑷ 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

⑸ 電力供給の途絶、通信の途絶、水道供給の途絶等インフラの障害からの波及等

4. 行政機関の適用範囲

本基本方針が適用される行政機関は、すべての執行機関（町長部局、教育委員会、町議会事務局、監査委員事務局、選挙管理委員会事務局、農業委員会事務局、及び公営企業）とする。

5. 職員等の遵守義務

職員、再任用職員及び会計年度職員（以下「職員等」という。）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。

6. 情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

⑴ 組織体制

本町の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

⑵ 情報資産の分類と管理

本町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し、当該分類に基づき情報セキュリティ対策を実施する。

⑶ 情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じる。

① マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

② LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③ インターネット接続系においては、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、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

⑷ 物理的セキュリティ

サーバ、情報システム室、通信回線及びパソコン等のハードウェアの管理について、物理的な対策を講じる。

⑸ 人的セキュリティ

情報セキュリティに関し、職員等が順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。

⑹ 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。

⑺ 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、外部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、緊急時対応計画を策定する。

⑻ 外部サービスの利用

外部委託や約款による外部サービス、ソーシャルメディアサービスを利用する場合は、外部事業者等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確認し、必要に応じて契約に基づき措置を講じる。

⑼ 評価・見直し

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し、運用改善を行い情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

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、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

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた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町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　弟子屈町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

この対策基準が適用される範囲は、以下のとおりとする。

（１）行政機関等

弟子屈町立小学校及び中学校

（２）情報資産

① 教育ネットワーク、教育情報システム及びこれらに関する設備、電磁的記録媒体

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

③ 教育情報システムの仕様書及びネットワーク図等のシステム関連文書

（３）用語説明

この対策基準における用語は、以下のとおりとする。

用語	定義
校務系情報	児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教員の個人情報など、学校が保有する情報資産のうち、それら情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報
校務外部接続系情報	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することが可能な端末
校務外部接続用端末	校務外部接続系情報にアクセス可能な端末
学習者用端末	学習系情報にアクセス可能な端末で、児童生徒が利用する端末
指導者用端末	学習系情報にアクセス可能な端末で、教員のみが利用可能な端末
校務系システム	校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム及び、校務系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
校務外部接続系システム	校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ（ＣＭＳ）及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム
学習系システム	学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム及び、学習系情報を扱う上

	で、適切なアクセス権が設定された領域で利用されるシステム
教育情報システム	校務系システム、校務外部接続系システム及び学習系システムを合わせた総称
校務系サーバ	校務系情報を取り扱うサーバ
校務外部接続系サーバ	校務外部接続系情報を取り扱うサーバ
学習系サーバ	学習系情報を取り扱うサーバ

2. 組織体制

弟子屈町教育情報セキュリティ管理については、以下の組織体制とする。

（1） 最高情報セキュリティ責任者（CISO）

弟子屈町副町長を、弟子屈町における最高情報セキュリティ責任者（CISO：Chief Information Security Officer 以下「CISO」という）とする。CISO は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おけ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 教育長を CISO 直属の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、弟子屈町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、弟子屈町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、弟子屈町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、弟子屈町の共通的な教育ネットワーク、教育情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

⑦ 統括教育情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

⑧ 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。

（3） 教育情報セキュリティ責任者

① 教育委員会管理課長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、弟子屈町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。

③　教育情報セキュリティ責任者は、弟子屈町において所有している教育情報システムにおける開発、設定の変更、運用、見直し等を行う際の情報セキュリティに関する統括的な権限及び責任を有する。

④　教育情報セキュリティ責任者は、弟子屈町において所有している教育情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び教職員等に対する教育、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

①　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する。

③　教育情報セキュリティ管理者は、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

①　教育委員会管理課担当係長を、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。

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、所管する教育情報システムにおける情報セキュリティに関する権限及び責任を有する。

④　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関す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

①　教育委員会管理課担当係の職員を、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。

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

（7）情報化推進委員会

本町の情報セキュリティ対策を統一的に行うため、情報化推進委員会において、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。

（8）兼務の禁止

①　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

②　監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

（9）情報セキュリティに関する統一的な窓口の設置

①　CISO は、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、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、自らへ報告が行われる体制を整備する。

②　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、その内容を関係部局等に提供

する。

③　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。

④　情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。

3. 情報資産の分類と管理方法

（１）　情報資産の分類

弟子屈町における情報資産は、機密性、完全性及び可用性により、次の通り分類し、必要に応じて取扱制限を行うものとする。

①　機密性による情報資産の分類

分類	分類基準	該当する情報資産のイメージ
機密性３	学校で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	特定の教職員のみが知り得る状態を確保する必要のある情報で秘密文書に相当するもの
機密性２B	学校で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	教職員のみが知り得る状態を確保する必要がある情報資産（教職員のうち特定の教職員のみが知り得る状態を確保する必要があるものを含む）
機密性２A	学校で取り扱う情報資産のうち、直ちに一般に公表することを前提としていないが、児童生徒がアクセスすることを想定している情報資産	教職員及び児童生徒同士のみが知り得る状態を確保する必要がある情報資産（教職員及び児童生徒のうち特定の教職員及び児童生徒のみが知り得る状態を確保する必要があるものを含む）
機密性１	機密性２A、機密性２B 又は機密性３の情報資産以外の情報資産	公表されている情報資産又は公表することを前提として作成された情報資産（教職員及び児童生徒以外の者が知り得ても支障がないと認められるものを含む）

②　完全性による情報資産の分類

分類	分類基準	該当する情報のイメージ
完全性２B	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学区関係者の権利が侵害される又は学校事務及び教育活動の的確な遂行に支障（軽微なものを除く）を及ぼすおそれがある情報資産	情報が正確・完全な状態である必要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合、業務の遂行に支障ある情報

完全性２A	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学校関係者の権利が侵害される又は学校事務及び教育活動の的確な遂行に軽微な支障を及ぼすおそれがある情報資産	情報が正確・完全な状態である必要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合、軽微な支障ある情報
完全性１	完全性２A 又は完全性２B の情報資産以外の情報資産	事故があった場合でも業務の遂行に支障がない情報

③ 可用性による情報資産の分類

分類	分類基準	該当する情報のイメージ
可用性２B	学校で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に支障（軽微なものを除く）を及ぼすおそれがある情報資産	必要な時にいつでも利用できる必要があり、情報システムの障害等による滅失紛失や、情報システムの停止等があった場合、業務の安定的な遂行に支障がある情報
可用性２A	学校で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に軽微な支障を及ぼすおそれがある情報資産	必要な時にいつでも利用できる必要があり、情報システムの障害等による滅失紛失や、情報システムの停止等があった場合、業務の安定的な遂行に軽微な支障がある情報
可用性１	可用性２A 又は可用性２B の情報資産以外の情報資産	滅失、紛失や情報システムの停止等があっても業務の遂行に支障がない情報

（２） 情報資産の管理

① 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。

② 情報資産の分類の表示

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

③ 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） 情報を作成する者は、情報の作成時に（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。

④ 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り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。

⑤ 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、適切な取り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。

⑥ 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は、情報資産の分類に従って、情報資産を適切に保管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、機密性２A 以上、完全性２A 以上又は可用性２A 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、耐震、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。

⑦ 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）電子メールにより機密性２A 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及び教育情報システム管理者は、電子メール等による外部送信の安全性を高めるため、添付される情報資産を監視する等、出口対策を実施しなければならない。

⑧ 情報資産の運搬

（ア） 車両等により機密性２A 以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、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） 機密性２A 以上の情報資産を運搬する者は、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。

⑨ 情報資産の提供・公表

（ア） 機密性２A 以上の情報資産を外部に提供する者は、限定されたアクセスの措置設定（アクセ

ス制限や暗号化、パスワード設定等）を行わなければならない。

（イ） 機密性２A 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及び教育情報システム管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

⑩ 情報資産の廃棄

（ア） 機密性２A 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うえで廃棄しなければならない。

（イ） 情報資産の廃棄を行う者は、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。

4. 物理的セキュリティ

4.1 サーバ等の管理

（１）機器の取り付け

教育情報システム管理者は、サーバ等の機器の取り付けを行う場合、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）サーバの冗長化

① 教育情報システム管理者は、校務系サーバその他の校務系情報を格納しているサーバを冗長化し、同一データを保持しなければならない。また、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

② 教育情報システム管理者は、学習系サーバその他の学習系情報を格納しているサーバのハードディスクを冗長化しなければならない。

（３）機器の電源

① 教育情報システム管理者は、統括教育情報セキュリティ責任者及び施設管理部門と連携し、校務系サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

② 教育情報システム管理者は、統括教育情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

（４）通信ケーブル等の配線

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

（５）機器の定期保守及び修理

①　教育情報システム管理者は、可用性２A 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。

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。

（６）施設外又は学校外への機器の設置

統括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、定期的に当該危機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

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、すべ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、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。

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、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。

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、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ち入りを防止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。

⑥　統括教育情報セキュリティ責任者及び教育情報システム管理者は、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すること。

② 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。

③ 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。

④ 外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

⑤ 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、外見上教職員と区別できる措置を講じなければならない。

（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、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 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、機密性 2A 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。

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、可用性 2B 以上の情報資産を取り扱う情報システムに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。

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）校務用端末、校務外部接続用端末及び指導者用端末の管理

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、校務用サーバ、タブレットやパソコン等教育情報システムへアクセスする端末へのログインパスワードの入力を必要とするように設定しなければならない。

③ 教育情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の多要素認証を設定しなければならない。

（2）学習者用端末の管理

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。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、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 教職員等の遵守事項

（1）教職員等の遵守事項

① 教育情報セキュリティポリシー等の遵守

教職員等は、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、順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 業務以外の目的での使用の禁止

教職員等は、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。

③ 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、機密性２B 以上、可用性 2B 以上、完全性 2B 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。

（ウ）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。

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、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を遵守しなければならない。

⑤ 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　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

教職員等は、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。

⑦　机上の端末等の管理

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。

⑧　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

①　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。

②　教育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、非常勤及び臨時の教職員の採用の際、必要に応じ、教育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。

③　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）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、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）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い、情報化推進委員会の承認を得なければならない。

②　新規採用の教職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

③　研修は、統括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、教育上システム管理者、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。

④　CISO は、毎年度１回、情報化推進委員会に対して、教職員等の情報セキュリティ研修の実施状況について報告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、又、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

すべての教職員等は、定められた研修・訓練に参加しなければならない。

5.3　情報セキュリティインシデントの報告

（１）学校内からの情報セキュリティインシデントの報告

①　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に報告しなければならない。

②　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。

③　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、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）住民等外部からの情報セキュリティインシデントの報告

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

③　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。

（３）情報セキュリティインシデント原因の究明・記録・再発防止等

①　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。

5.4 ID 及びパスワード等の管理

（１）IC カード等の取り扱い

① 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管理者に通報し、指示に従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。

③ 統括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、切り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うえで廃棄しなければならない。

（２）ID の取り扱い

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 を利用している場合は、共用 ID の利用者以外に利用させてはならない、

（３）パスワードの取り扱い

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 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。

⑧ 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）

⑨ 共有 ID に対するパスワードは、定期的に又はアクセス回数に基づいて変更しなければならない。

⑩ 取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の多要素認証を設定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。

④ 教育情報システム管理者は、インターネット接続を前提とする校務外部接続系サーバ及び学習系サーバに保管する情報（学習系サーバにおいては、機微な個人情報を補完する場合に限る）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

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）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、その取り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

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、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。

（5）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

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。

（7）障害記録

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。

（8）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、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、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、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２B 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。

（10）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。

（11）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、校務系システム及び学習系システム間の通信経路の論理的又は物理的な分離をするとともに、ウェブ閲覧やインターネットメールなどのインターネットを介した外部からのリスクの高いシステムと重要性が高い情報（特に校務系）を論理的又は物理的に分離を

する、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。

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、ウィ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。

（12）複合機のセキュリティ管理

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

（13）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。

（14）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、解読が困難な暗号化及び認証技術の利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、暗号化等の措置を講じなければならない。

（15）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。

（16）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、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。

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統括教育情報セキュリティ責任者の許可なしに使用してはならない。

（17）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の設定等、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化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。

（18）無許可ソフトウェアの導入等の禁止

①　教職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

②　教職員等は、業務上の必要がある場合は、統括教育情報セキュリティ責任者及び教育情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、教育情報セキュリティ管理者又は教育情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

③　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。

（19）機器構成の変更の制限

①　教職員等は、パソコンやモバイル端末に対し、機器の改造及び増設・交換を行ってはならない。

②　教職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、統括教育情報セキュリティ責任者及び教育情報システム管理者の許可を得なければならない。

（20）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。

（21）業務以外の目的でのウェブ閲覧の禁止

①　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。

②　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。

6.2　アクセス制御

（1）アクセス制御等

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、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。

②　利用者 ID の取り扱い

（ア）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 の取り扱い等の方法を定めなければならない。

（イ）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、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に通知しなければならない。

（ウ）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。

③　特権を付与された ID の管理等

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

（イ）統括教育情報セキュリティ責任者及び教育情報システム管理者の特権を代行する者は、統括教育情報セキュリティ責任者及び教育情報システム管理者が指名し、CISO が認めたものでなければならない。

（ウ）CISO は、代行者を認めた場合、速やかに統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者及び教育情報システム管理者に通知しなければならない。

（エ）統括教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与された ID 及びパスワードの変更について、外部委託事業者に行わせてはならない。

（オ）統括教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与された ID 及びパスワードについて、その利用期間に合わせて特権 ID を作成・削除する、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。

（カ）統括教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

（２）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、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　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。

③　統括教育情報セキュリティ責任者は、外部からのシステムアクセスを認める場合、アクセスする利用者の本人確認、システムアクセスの対象となる児童生徒の本人（保護者）同意を得る等の措置を講じなければならない。

④　統括教育情報セキュリティ責任者は、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。

⑤　統括教育情報セキュリティ責任者及び教育情報システム管理者は、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、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。

⑥　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、コンピュータウィ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。

⑦　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）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。

（4）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、ログイン後ただちに仮のパスワードを変更させなければならない。

（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

（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うえで導入しなければならない。

②　テスト

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

（オ）教育情報システム管理者は、運用環境への移行に先立ち、システムの脆弱性テストを行い、その結果を確認しなければならない。

（４）システム開発・保守に関連する資料等の整備・保管

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並びに使用したオープンソースのバージョン（リポジトリ）を適切な方法で保管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ィ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ィ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 コンピュータウィ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、コンピュータウィ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。

（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

ータウィ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、コンピュータウィルス等の感染を防止するために、町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。

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 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。

③ 差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

④ 端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

⑤ 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。

⑥ 統括教育情報セキュリティ責任者が提供するウィルス情報を、常に確認しなければならない。

⑦ コンピュータウィ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。

（４）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。

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

統括情教育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 使用されていないポート及び SSID(無線 LAN ネットワーク名)を閉鎖しなければならない。

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 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、データの書き換えを検出し、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。

④　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。

⑤　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）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。

（4）内部からの攻撃

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、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）教職員等による不正アクセス

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。

（6）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。

（7）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。

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、機密性 2B 以上、完全性 2B 以上、可用性 2B 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。

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

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）教職員等の報告義務

① 教職員等は、教育情報セキュリティポリシーに対する違反行為を発見した場合、直ちに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管理者に報告しなければならない。

② 違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括教育情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適切に対処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 又は情報化推進委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当初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。

①　関係者の連絡先

②　発生した事案に係る報告すべき事項

③　発生した事案への対応措置

④　再発防止措置の策定

（３）業務継続計画との整合性確保

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

（４）緊急時対応計画の見直し

CISO 又は情報化推進委員会は、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。

7.4　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、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時は、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　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 行政手続き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 弟子屈町個人情報保護条例（平成 13 年条例第 24 号）

7.6 懲戒処分等

（1）懲戒処分

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

（2）違反時の対応

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

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 教育情報システム管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定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
・町による監査、検査
・町による情報セキュリティインシデント発生時の公表
・教育情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

（３）確認・措置等

教育情報システム管理者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ（２）の契約に基づき措置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。

９．クラウドサービスの利用

9.1　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

① 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又は合意しなければならない。

② 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又は合意しなければならない。

③ 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（1）③を遵守しなければならない。

（２）アクセス制御

① 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又は合意しなければならない。

② 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、情報資源ごとに、許可されたエンドユーザー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

又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又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

① 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上で確認又は合意しなければならない。

② 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又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

① 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、合意の上、利用しなければならない。

② 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又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

① 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又は合意しなければならない。

② 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又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

① 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、あ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。

② 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（2）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又は合意しなければならな

い。

③　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（2）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又は合意しなければならない。

④　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（6）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又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

①　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又は合意しなければならない。

②　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又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

①　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。

②　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、エンドユーザー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

①　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又は合意しなければならない。

②　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又は合意しなければならない。

③　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付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又は合意しなければならない。

④　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又は合意しなければならない。

⑤　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又は合意しなければならない。

（12）データの廃棄等について

① 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についてサービス提供定款や契約書面上で確認又は合意しておかなければならない。

② 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又は合意しておかなければならない。

9.2 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を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。（クラウド事業者の準拠する認証制度、個人情報保護指針、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、保守運用管理規程等）

（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、下記事項について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。

① 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

② 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

③ サービス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

① 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、十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。

② クラウド利用者は、クラウド事業者に、従業員への育成計画、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

① 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に求めなければならない。

② 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

① 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。

② 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

① 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。

② 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

① 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。

② クラウド利用者は、①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

① 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。

② 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わけではないことから、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又は合意しなければならない。

③ 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。

9.3 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

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り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。

・約款によるサービスを利用してよい範囲

・業務により利用する約款による外部サービス

・利用手続き及び運用手順

（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。

9.4 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。

・本町のアカウントによる情報発信が、実際の本町のものであることを明らかにするために、本町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。

・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 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. 事業者に対して確認すべきプライバシー保護に関する事項

（1）個人情報の利用範囲

教育・学校の目的に必要な情報、又は児童生徒・保護者の許可した情報を超えて個人情報の収集、維持、使用、共有をしないこと。

（2）個人情報の無断提供

クラウドサービスの導入によって知り得た個人情報について、売買も含め、無断提供をしないこと。

（3）個人情報を利用した利用者に対する広告活動等の無断使用の禁止

教育・学校の目的を達成すること以外に、個人情報について児童生徒・保護者に対する行動ターゲッティング広告をはじめとする、広告活動その他無断使用をしないこと。

（4）不必要な個人プロファイル作成禁止

教育・学校の目的を達成するため、又は児童生徒・保護者によって許可された場合を除き、不必要な個人プロファイルを作成しないこと。

（5）不適切なポリシー等の変更の禁止

クラウドサービスの運用等において、利用者に対する明確な通知・相談等の対応もなく、利用者のプライバシーポリシーに重大な影響を与えるような変更を行わないこと。

（6）個人情報の保持期間定義

サービス提供期間（利用者と合意した期間）を超えて個人を特定する情報を保持しないこと。

（7）個人情報の利用目的

個人情報を収集、使用、共有、及び保持するのは、教育機関、教師、又は利用者によって承認された目的に限ること。

（8）個人情報の取り扱いについての情報開示

個人情報の取り扱いについて、契約又はプライバシーポリシーで明確に示すこと。

（9）利用者による個人情報管理

個人情報の登録、変更、削除に関するサービスを利用者に提供すること。

（10）個人情報の適正管理

個人情報に対する不正アクセス又は個人情報の紛失、破壊、改ざん、漏えい、盗難等のリスクに対し、適切な安全対策を講じること。また、個人情報を正確かつ最新の状態で管理すること。

（11）再委託

サービス提供の全部又は一部を第三者に再委託又は代行実施させる場合には、個人情報保護法制を遵守し、当該再委託先又は代行実施先について、同等の義務を課し、管理するものとする。

（12）合併・買収

合併又は他社による買収を行う場合、後継企業が以前に収集した個人情報について同様の義務を負うことを条件に、個人情報を継続して管理するものとすること。

11．1 人 1 台端末におけるセキュリティ

11.1　学習者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）

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討し、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 フィルタリングソフト

② 検索エンジンのセーフサーチ

③ セーフブラウジング

（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付後においても、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。

11.2 児童生徒における ID 及びパスワード等の管理

（1）ID 登録・変更・削除

① 入学／転入時の ID 登録処理

ID についてはシンプル・ユニーク（唯一無二）・パーマネント／パーシスタント（永続的な識別）な構成要素になっていることや、児童生徒の発達段階に応じた複雑性を上げたパスワードポリシーによりセキュリティ強度を上げていくなど適切な措置を講じなければならない。

② 進級／進学時の ID 関連情報の更新

ID については原則として進級／進学にも変更不要とすることが望ましい。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）の変更を行っておくことで、MDM による各種ポリシーや使用アプリケーションの変更を効率的に行うことが可能となる。

さらに、統合型校務支援システム等における児童生徒の氏名と連動した ID 管理を行うことで、校務側で管理している属性情報と一体となった ID を含んだマスター管理の一元化が望ましい。

③ 転出／卒業／退学時の ID 削除処理

ユニークな ID は、個人を識別できる可能性があるため、個人情報保護の観点から、サービス提供期間を超えて個人を特定する情報を保持しないようにする必要がある。

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：試験における工程を全てコンピュータ上で行うこと）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。

12. 評価・見直し

12.1 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

① 情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼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 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、情報化推進委員会の承認を得なければならない。

② 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、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

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、情報化推進委員会に報告する。

（６）保管

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

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

12.2 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、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報化推進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

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 情報化推進委員会は、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。

12.3 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

情報化推進委員会は、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、情報セキュリティポリシー及び関係規定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。

第３章　弟子屈町教育情報セキュリティ実施手順

この実施手順は、弟子屈町教育情報セキュリティポリシー（以下「ポリシー」という。）に基づいて、教職員等が教育情報セキュリティ対策を行うための具体的な手順を定めたものである。

1. 情報資産の管理

弟子屈町が保有する情報資産については、弟子屈町教育情報セキュリティポリシー対策基準（以下「対策基準」という。）によって定められた分類により重要度を分類し、適正に管理を行うこと。

⑴　情報資産の管理方法

①　機密性３（秘情報）

職務上必要な限定された関係者のみにアクセスを制限し、それ以外の者にアクセスさせないために、以下のことを必ず実施するとともに、次のとおり必要な対策を取ること。

・外部ネットワークから分離したファイルサーバに保存し、職務上必要な者のみにアクセス権限を設定する。
・データもしくはフォルダにセキュリティ対策を設定するか、ファイルを暗号化する。
・その存在の有無についても、職務上必要な最低限の者以外に漏れないよう、厳格に扱う。

②　機密性２Ａ及び２Ｂ（関係者外秘情報）

関係者のみにアクセスを制限し、それ以外の者にアクセスさせないために、以下のことを必要に応じて実施するとともに、次のとおり必要な対策を取ること。

・外部ネットワークから分離したファイルサーバに保存し、関係者のみにアクセス権限を設定する。
・ファイル自身に適切なパスワードを設定するか、ファイルを暗号化する。

③　機密性１（その他情報）

教職員等がアクセス可能であるため、情報の改ざんや偽情報の流布の防止のために、必要な対策を取ること。

⑵　情報資産の複製、持ち出し及びメール送信

情報資産を複製、持ち出し及びメール送信する場合も、情報資産の分類に応じて、必要な対策を取ること。

①　機密性３（秘情報）

・職務上必要な限定された関係者のみにアクセス制限したフォルダに保存し、原則として、保管場所からの複製、持ち出し、及びメール送信はしない。
・やむを得ず保管場所以外に複製、持ち出し及びメール送信する場合は、教育情報セキュリティ管理者の承認を事前に得るとともに、記録媒体のアクセスを制限するための適切なパスワードの設定や、データ自体を暗号化するなどの措置を行う。
・情報資産の持ち出し時には、肌身離さず所持し、盗難、紛失等に十分注意する。
・複製、持ち出し及びメール送信した情報資産は、不要になり次第速やかに削除し、情報の漏えいを防ぐ。

②　機密性２Ａ及び２Ｂ（関係者外秘情報）

・関係者のみにアクセスできるファイルサーバに保管し、原則として、保管場所からの複製及び持ち出しはしない。
・やむを得ず保管場所以外に複製、持ち出す場合は、教育情報セキュリティ管理者の承認を事前に得るとともに、記録媒体のアクセスを制限するための適切なパスワードの設定や、データ自体を暗号化するなどの措置を行う。
・情報資産の持ち出し時には、盗難、紛失等に十分注意する。

③　機密性１（その他情報）

・外部ネットワークから分離したファイルサーバに保存し、原則として、保管場所からの複製及び持ち出しはしない。
・保管場所以外に複製及び持ち出す場合は、記録媒体のアクセスを制限するための適切なパスワードの設定や、データ自体を暗号化するなどの措置を行う。
・情報資産の持ち出し時には、盗難、紛失等に十分注意する。

⑶　情報処理機器の廃棄について

情報処理機器の廃棄をする際には、情報資産の分類に関係なく、データの消去等を確実に行い、情報の漏えい防止のために、次のとおり必要な対策を取ること。

・データの消去には、破砕処理や、磁気によるデータの消去等を施し、データの復元ができないようにする。
・情報機器の記憶媒体を保守契約により交換する場合又はリース機器の撤去を行う場合は、撤去後の記憶媒体の処理方法についても保守業者に確認を取り、データ消去を確実にする。
・データの消去を外部に委託する際には、データ消去証明書等の提出を義務付ける。

2.　セキュリティの確保

教職員等は、本町が保有する情報資産を守るため、当該情報資産を管理している教育情報セキュリティ管理者の指示の下、対策基準によって定められたセキュリティ対策を実施する。

⑴　物理的セキュリティ

①　情報システムのセキュリティ対策

パソコン等の情報システムについては、次のとおり必要な対策を取ること。

・機器に適切なパスワードを設定し、不要なアクセスを防ぐ。
・パソコンを離れる際には、ロック画面（スクリーンセーバー）にするなど、他人にパソコンを閲覧されないようにする。
・外部記憶装置は、セキュリティ機能付きのものを使用する。
・私物の外部記憶装置を接続しない。

②　入室の制限

サーバ室のように重要な情報機器が設置してある部屋の管理については、次のとおり必要な対策を取ること。

・施錠管理し、不正な入室を防ぎ、入退室については入退室記録簿を備え管理を行う。
・入室できる者を制限する。また、入室を予定していない者が入室を行う際には、入室権限を持つ者が同行する又は部屋の管理者に事前に許可を得る。

・不正な入室が行われないように厳重に管理する。

③　盗難の防止

情報システム及び情報資産（以下「情報資産等」という。）の盗難を防ぐために、次のとおり必要な対策を取ること。

・情報処理機器は、施錠管理できる部屋等に管理し、盗難防止の対策を取る。

・情報資産を管理するキャビネット等は、施錠管理を行う。

④　災害対策

サーバ機器のような重要な情報処理機器のシステム停止を可能な限り防ぐために、次のとおり必要な対策を取ること。

・情報処理機器の備え付けにあたっては、耐震対策を十分に考慮する。

・災害により情報システムが停止しないように、構築時に冗長化を行う。

・災害等によりデータが消失することがないように、サーバ機器は定期的にバックアップを取る。

・停電等による不測のシステム停止によりハードウェア障害が起きないように、無停電電源装置等を用いて、電源断時に自動で終了処理を行う。

⑵　人的セキュリティ

①　情報資産の管理

各部局は、教育情報セキュリティ管理者の指示の下、情報資産の重要度を適切に分類し、情報資産の管理を行うこと。

・情報資産の重要度を適切に設定する。

・機密性３及び機密性２Ａ及び２Ｂの権限範囲が適切であるか定期的に確認する。

・情報資産台帳等を作成し、守るべき情報資産を整理する。

②　情報セキュリティポリシーの徹底

教職員等は、ポリシーを遵守しなければならない。

・定期的にポリシーが遵守されているか確認する。

・情報セキュリティに関する研修に参加する。

・教育情報システム担当者から通知されるセキュリティ情報を確認し、セキュリティ対策を実施する。

③　パスワードの設定管理

教職員等は、パスワードの設定を行う際には、次のとおり設定すること。

・推測しにくいパスワードを設定する。

・８文字以上のパスワードにする。

・英字、数字、記号を組み合わせる。

・初期に設定されているパスワードは使用せず、必ず変更する。

・定期的にパスワードを変更する。

・パスワードをメモしたものを人目に付くところに置かない。

・パスワードを他人に教えない。

・複数のシステムに同じパスワードを設定しない。

④　電子メールのセキュリティ対策

電子メールの利用の際には、次のとおり必要な対策を取ること。

・電子メール内に記載されているURL は、不用意にリンク先にアクセスすると、ウィルス感染、フィッシング詐欺等の危険があることから、URL に間違いがないか、信頼のおけるURL であるかなど、十分に注意する。

・添付ファイルがある場合、コンピュータウィルス感染しているファイルの可能性があるため、不用意に開封しない。開封する場合は、ウィルスチェックを行ってから開封する。

・電子メールの送信者のアドレスが正しいことを確認する。

・身に覚えのない送信主からのメール、明らかに不自然な内容のメール等は不用意に応答せず、必要に応じて情報システム担当者に相談する。

・送り先のメールアドレス入力の際には、間違いの無いように再チェックし送信する。

・添付ファイルを送信するときには、添付ファイルにパスワードを設定する。

⑶　技術的セキュリティ

①　情報システムのセキュリティ対策

パソコン等の情報システムについては、次のとおり必要な対策を取ること。

・導入しているウィルス対策ソフトをインストールし、リアルタイム検索を有効化すること。また、定期的（最低でも月に１回）にウィルス感染チェックを行うこと。

・OS 又はインストールされているソフトウェア等で、セキュリティの脆弱性が発覚した場合には、速やかにセキュリティアップデートを行う。

・不正なアクセスや攻撃を防ぐために、不要な常駐プログラム等を停止する。

・アカウントの管理者は、アカウントの整理を定期的に実施し、不要なアカウントは削除する。

・機器の利用は IP アドレス等で、利用可能な範囲を制限する。

・管理用途で遠隔から機器にアクセスする際は、IP アドレス制限やパスワード等でアクセスを制限し、不特定多数のアクセスを禁止する。

・不正なアクセスを防ぐため、不要なサービスは停止する。

・パスワード等の設定を行い、アクセスできる者を制限する。

・IP アドレスでの利用制限の設定を行い、不要なアクセスを防ぐ。

・登録された MAC アドレスやサブネット、IP アドレス以外から接続できないように設定する。

・校舎内ネットワーク接続パソコンからインターネット接続のため無線 LAN への接続は原則禁止とする。

・SNMP の設定をする場合は、IP アドレスによる接続制限やコミュニティ名を標準設定から変更するなど、不特定多数の読み書きができないようにする。

②　ネットワークへの不正接続対策

ネットワークの接続口が不特定の者によって接続されないよう、次のとおり必要な対策をとること。

・不特定多数が出入りする部屋では、ケーブルを接続するだけで校舎内ネットワーク及びインターネットが利用できるようになる DHCP サーバの設置は行わない。

・ルータモードを持つ機器は校舎内ネットワークに設置しない。

3. 禁止事項

本町の情報資産等を利用するにあたり、以下の行為はしてはならない。

⑴ 法令に違反する行為

- 閲覧権限及び利用権限のない情報資産等へ不正にアクセスする。
- 情報資産等を破壊及び改ざんする。
- コンピュータウィルスを配布する。
- 他人の写真や音声を当人に無断でホームページ等に公開する。
- 他人の作成した文書、写真等を無断でホームページ等に公開する。
- 有償ソフトウェアを無断でコピーして使用する。
- ファイル共有ソフト等を用いて、著作権のあるソフトウェア、音楽ファイル、動画ファイル等を入手したり、入手した情報を公開して提供したりする。
- その他、法令に違反するとみなされる行為。

⑵ 公序良俗に反する行為

- 他人になりすまして、ネットワーク上で発言する。
- 事実と異なる情報を意図的に流す。
- 猥褻とみなされる文章や画像をホームページ等で公開する。
- 人権、性別、思想信条などに基づく差別的な文章等をホームページ等で公開する。
- メーリングリスト等に他人を無断で登録する。
- 他人のファイル等を当人に無断で参照する。
- その他、公序良俗に違反するとみなされる行為。

⑶ 本町の行政運営及び学校運営等に反する行為

- ネットワークを意図的に混雑させる。
- 教育情報セキュリティ管理者や教育情報システム担当者の指示に従わない。
- データ量の多いファイル等をメールで大量に送る。
- アカウントの貸し借りを行う。
- 業務上必要のないソフトウェアをダウンロードして利用する。
- その他、本町の行政運営及び学校運営に反するとみなされる行為。

4. インシデントに対する対応と報告

インシデントが発生した場合には、その被害を最小限に抑えるため、以下のとおり対応しなければならない。

⑴ 重要度の区分

インシデントが発生した場合には、その事象から、以下のように重要度を区分する。

区分	事象
重要度高	・本町（学校）の信用や利益を大きく損なうもの ・本町（学校）の業務・運営に支障があるもの ・違反行為の内容が法律等に違反するもの

	・事象が重大で解決に時間を要するもの ・その他、重要度が高いと認められるもの
重要度低	・本町（学校）の信用や利益を損なう可能性がないもの ・本町（学校）の業務・運営に支障が少ないもの ・事象が軽微ですぐに対応が可能なもの

⑵ インシデントに対する対応

① 教職員等は、インシデントを発見した場合には、速やかに教育情報セキュリティ管理者に連絡をしなければならない。また、教育情報システム担当者にも同様に連絡をすること。

② 教育情報セキュリティ管理者は、インシデントが発生した場合には、速やかに事実関係の確認、問題の解決に努めるとともに、再発防止策の検討及び実施をしなければならない。

③ 教育情報セキュリティ管理者は、発生したインシデントの重要度に関わらず、統括教育情報セキュリティ責任者にインシデントの内容や対応状況、再発防止策等について報告しなければならない。この場合、統括教育情報セキュリティ責任者は、当該事象の重要度区分について判断する。

⑶ 「重要度高」と判断されたインシデントへの対応

① 報告

（ア）当該事象が発生した場合、教育情報セキュリティ管理者は、「インシデント報告書」を作成し、統括教育情報セキュリティ責任者へ提出しなければならない。

（イ）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管理者からインシデントの報告を受けた後、最高情報セキュリティ責任者へ報告しなければならない。

（ウ）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管理者からインシデントの報告を受けた後、情報化推進委員会を開催し、報告を行わなければならない。

② 調査等

（ア）情報化推進委員会は、インシデントが発生した場合、ポリシーの遵守等に問題がなかったか調査を行う。

（イ）統括教育情報セキュリティ責任者は、情報化推進委員会の調査結果に基づき、対応を行う。

・原因が、当該事象が発生した部署（学校）にある場合
　当該教育情報セキュリティ管理者に対して、ポリシーの遵守を徹底させる。

・原因が、対策基準及び実施手順の不備にある場合
　最高情報セキュリティ責任者に対して、対策基準及び実施手順の見直しを進言する。

5. 見直し

最高情報セキュリティ責任者は、対策基準及び実施手順に課題及び問題点が認められる場合又は統括教育情報セキュリティ責任者からポリシー見直しの進言があった場合は、見直しを行うものとする。

別紙１

教育情報セキュリティポリシー緊急時対応計画

教育情報資産への侵害が発生した場合における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるために、緊急時対応計画を次のとおり定める。

① 関係者の連絡先

職　責　等	担当部署	氏　名	連絡先
最高情報セキュリティ責任者	副町長		
統括教育情報セキュリティ責任者	教育長		
教育情報セキュリティ責任者	管理課長		
教育情報セキュリティ管理者	校長		
教育情報システム管理者	管理課担当係長		
教育情報システム担当者	管理課担当係員		
情報システムに係る外部委託事業者			
北海道教育委員会	釧路教育局		
北海道警察	弟子屈警察署警備係		
関係機関			
その他影響が考えられる個人・法人			

② 発生した事案に係る報告事項

セキュリティに関する事案を認めた者は、別紙により速やかに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。

③ 発生した事案への対応措置

ア．統括教育情報セキュリティ責任者実施事項

事　　象	連絡担当部署		
サイバーテロその他住民に重大な被害が生じる恐れがあるとき	最高情報セキュリティ責任者	弟子屈警察署	影響が考えられる個人・法人
不正アクセスその他犯罪と思慮されるとき	最高情報セキュリティ責任者	弟子屈警察署	
踏み台となって他者に被害を与える恐れがあるとき	最高情報セキュリティ責任者	弟子屈警察署	
教育情報システムに関する被害	教育情報システム管理者	必要と認められる事業等	
その他教育情報資産に係る被害	関係部局等		

ネットワーク切断措置対象事例	作業チェック
異常なアクセスが継続しているとき、又は不正アクセスが判明したとき	
コンピュータウィルス等不正プログラムがネットワーク経由で広がっているとき	
教育情報資産に係る重大な被害が想定されるとき	

イ．教育情報システム担当者実施事項

1 次作業・教育情報システム停止対象事例	作業チェック
コンピュータウィルス等不正プログラムが教育情報資産に深刻な被害を及ぼしている場合	
災害等により電源を供給することが危険又は困難なとき	
その他の教育情報資産に係る重大な被害が想定されるとき（統括教育情報セキュリティ責任者へは事後報告）	
2 次作業・処理項目	
事案に係るシステムのアクセス記録及び現状を保存する	
事案に対処した経過の記録	
事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を検討する	
再発防止の暫定措置を講じた後、復旧する	

④　再発防止措置の策定

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実施事項

処理項目	作業チェック
当該事案に係るリスク分析	
情報セキュリティポリシー及び実施手順の修正（CISO への報告）	

別紙２

インシデント報告書

年　　月　　日

報 告 者　　所 属	
職　名　・　氏　名	
教育情報セキュリティ管 理 者 氏 名	

◎インシデントの概要

発生日時	年　　月　　日　　時　　分
事案内容	
原　　因	
被害状況	
応急措置	

◎対処

技術的対処	
事務的対処	

◎再発防止策

技術的対応	
その他対応	