島本町立学校教育情報セキュリティポリシー

令和5年4月

島本町教育委員会

目　次

第1章　教育情報セキュリティ基本方針

第2章　教育情報セキュリティ対策基準

第1章　教育情報セキュリティ基本方針

１　目的

現在、島本町立小学校及び中学校（以下「学校」という。）においては、文部科学省提唱の「ＧＩＧＡスクール構想」に基づき、１人１台の端末及び教育用クラウドサービスの活用を進め、個別に最適化された教育環境において、協働的な学びの充実を推進している。学校が取り扱う情報には、児童生徒（以下「児童生徒等」という。）、保護者、教職員等の個人情報及び学校運営上重要な情報が多数含まれ、外部への漏洩等が発生した場合、極めて重大な結果を招くおそれがある。そのため、学校のＩＣＴ環境整備が進むに当たり、不正アクセスや盗難・紛失等、情報資産の保護に向けた十分な情報セキュリティ対策を講じることは、教職員及び児童生徒等が安心してＩＣＴを活用するために必要不可欠である。

また、ＧＩＧＡスクール構想の推進により、クラウドサービスの活用を前提としたネットワーク構成等の課題に対応するとともに、児童生徒等の端末と教職員の端末から得られる各種教育情報を効果的に活用して教育の質的改善を図るため、文部科学省の「教育情報セキュリティポリシーに関するガイドライン(令和４年３月版)」を参考に、島本町教育委員会において「島本町立学校教育情報セキュリティポリシー」（以下「このポリシー」という。）を策定するものとする。

２　構成

このポリシーは、学校が保有する情報資産に対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ものである。このポリシーは、学校が保有する情報資産を取り扱う全教職員に浸透、定着させるものであり、安定した統一的規範であることが求められる。一方、情報処理や通信技術の進歩による急速な環境の変化に柔軟に対応することも必要であることから、不変的な部分として統一的な規範を定めた「教育情報セキュリティ基本方針」と、情報資産を取り巻く環境の変化に柔軟に対応する部分となる「教育情報セキュリティ対策基準」の２部構成として策定する。

[教育情報セキュリティポリシーの構成]

文　書	内　　容	
島本町立学校教育情報セキュリティポリシー	教育情報セキュリティ基本方針	教育情報セキュリティ対策に関する統一的かつ基本的な方針
	教育情報セキュリティ対策基準	教育情報セキュリティ基本方針を実行に移すためのすべての教育情報システムに共通の教育情報セキュリティ対策の基準

3　用語の定義

このポリシーにおける用語の定義は、次に定めるところによる。

用　語	定　　義
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。
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。
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。
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。
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。
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の、外部と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	学校が保有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ当該情報に教職員及び児童生徒がアクセスすることが想定されている情報。
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。インターネットへの接続は問わない。
サーバ	ネットワーク上で学校情報を処理し、端末に提供するコンピュータ。
端末機	ネットワークを通じてサーバに接続されたパソコンやモバイル端末（タブレット等）機器。
校務用端末	校務系情報全てにアクセス可能な端末。
学習者用端末	学習系情報にアクセス可能な端末で、児童生徒が利用する端末。
指導者用端末	学習系情報にアクセス可能な端末で、教職員のみが利用可能な端末。
教育情報システム	情報資産を扱うハードウェア、ソフトウェア、クラウドサービス等。
情報セキュリティインシデント	情報セキュリティに関する問題としてとらえられる事象（障害、事件、事故、欠陥、攻撃、侵害等）。
記録媒体	情報システムでデータ等を記録するための媒体（メディア）。サーバ、端末機、デジタルカメラ、デジタルビデオカメラ、通信回線装置等に内蔵される内蔵電磁的記録媒体と、外付けハードディスク、CD-ROM、DVD-R、USB メモリ、SDカード等の外部電磁的記録媒体。
スマートデバイス	情報処理端末（デバイス）のうち、スマートフォンやタブレット等、携行可能な多機能端末。
情報資産	情報システム及びネットワーク並びにこれらで取り扱われる学校情報（これらを印刷した文書も含む）。
無線LAN	電波等を利用してデータの送受信を行う構内通信網システム。
クラウド	学校外、庁舎外でプログラムやデータベースを管理し、ネットワークを介してこれを利用する仕組みや概念。
ソーシャルメディアサービス	インターネット上における、ホームページ、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等。
教職員	教育委員会所管の学校に勤務する教職員等。会計年度任用職員を含む。

4　情報資産の分類と管理

学校の情報資産の機密性、完全性及び可用性により、次のとおり分類し、必要に応じて取扱制限を定め、適正な管理を行う。

分類	分 類 基 準
Ⅰ	セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼすもの。
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もの。
Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼすもの。
Ⅳ	影響をほとんど及ぼさないもの。

[情報資産の分類]

情報資産の分類					情報資産の例示		
重要性分類	定義	機密性	完全性	可用性	校務系	学習系	公開系
Ⅰ	セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。	3	2B	2B	・指導要録原本 ・教職員の人事情報 ・入学者選抜問題 ・教育情報システム仕様書		
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。	2B	2B	2B	○学籍関係 ・出席簿 ・卒業証書授与台帳 ・転退学受付(整理)簿 ・転入学受付(整理)簿 ・就学児童・生徒移動報告書 ・休学・退学願等受付(整理)簿 ・教科用図書給付児童・生徒名簿 ・要・準要保護児童・生徒認定台帳 ・その他校内就学援助関係書類 ○成績関係 ・通知表 ・評定一覧表 ・進級・卒業認定資料 ・定期考査・テスト等の答案用紙 （児童・生徒が記入済のもの） ・定期考査素点表 ・成績に関する個票等 ○指導関係 ・事故報告書・記録簿 ・生徒指導・特別指導等記録簿 ・児童生徒等の個人写真・集合写真 ・指導記録・指導カード （児童・生徒等理解カード） ・教育相談・面接の記録・カード等 ・個別の教育支援計画 （学校生活支援シート） ・個別指導計画 ・家庭訪問記録・個別面談記録 ・教務手帳 ・週ごとの指導計画	○児童生徒の学習系情報 ・学習システムログインID/PW 管理台帳 ・学習者用端末ID/PW 台帳	

Ⅱ					（個人情報が含まれるもの） 〇進路関係 ・調査書 ・推薦書 ・公立高校入学者選抜に係る成績一覧表 ・入学者選抜に関する表簿（願書等） ・私立高校入試に係る事前相談資料 ・卒業生進路先一覧表 ・進路希望調査 ・進路判定会議資料 ・進路指導記録簿 〇児童・生徒に関する個人情報 （生活歴、心身の状況、財産状況等の情報、電話番号、メールアドレス、住所、氏名、生年月日、性別等の基本情報を含むもの） 〇学校教職員に関する個人情報 （病歴、心身の状況、収入等の情報、電話番号、メールアドレス、住所、氏名、生年月日、性別等の基本情報を含むもの） 〇健康関係 ・健康診断票 ・歯の検査表 ・心臓管理等医療情報 ・学校生活管理指導票 ・児童・生徒等健康調査票 ・児童・生徒の健康保険等被保険者証の写 ・健康診断に関する表簿 ・就学時健康診断票 〇教職員に割り当てた機密性の高い情報 ・情報システムログインID/PW ・情報端末ログインID/PW 〇その他 ・給食関係書類・寄宿関係資料 〇名簿等 ・児童生徒名簿 ・保護者緊急連絡網 ・児童生徒の住所録 ・PTA会員名簿 ・職員緊急連絡網・職員住所録 ・委員会名簿 ・PTA役員連絡網 〇各種帳票ファイル ・指導要録作成システム等、データの入っていない帳票		
Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす。	2A	2A	2A	〇児童生徒の氏名 ・出席簿 ・名列表 ・座席表 ・児童生徒委員会名簿 〇学校運営関係 ・卒業アルバム ・学校行事等の児童・生徒の写真	〇学校運営関係 ・授業用教材 ・教材研究資料 ・生徒用配布プリント 〇児童生徒の学習系情報 ・児童生徒の学習記録（確認テスト、ワークシート、レポート、作品等） ・学習活動の記録（動画・写真等）	

Ⅳ	影響をほとんど及ぼさない。	1	1	1			○学校運営関係 ・学校・学園要覧 ・学校紹介パンフレット ・使用教科書一覧 ・教育課程編成表 ・学校設定科目の届け出 ・特色紹介冊子原稿 ・学校徴収金会計簿 （学年費、教育振興費等） ・学校行事実施計画 （避難訓練・体育祭実施計画等） ・保護者等への配布文書文例 ・各種届雛形・校務分掌表 ・PTA資料 ・学園・学校・学年・学級だより ・学校・学園ホームページ掲載情報 ・学校行事のしおり ○学校活動の記録 ※保護者の承諾がある場合、以下は公開可能 ・学校行事等の児童・生徒の写真 ・学習活動の記録（動画・写真・作品等）
重要性分類	定義	機密性	完全性	可用性	校務系	学習系	公開系
情報資産の分類					情報資産の例示		

※機密性による情報資産の分類

分類	分類基準
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
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
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、児童生徒等がアクセスすることを想定している情報資産
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

※完全性による情報資産の分類

分類	分類基準
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支障(軽微なものを除く)を及ぼすおそれがある情報資産
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
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

※可用性による情報資産の分類

分類	分類基準
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
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
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

[情報資産の取扱例]

情報資産の分類					情報資産の取扱例								
重要性分類	定　義	機密性	完全性	可用性	複製・配布	組織外部への持ち出し制限 ※1	端末制限	組織外部への送信 ※2	情報資産の運搬 ※3	組織外部での情報処理 ※4	使用する電磁記録媒体	情報資産の保管	情報資産の廃棄
Ⅰ	セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。	3	2B	2B	必要以上の複製及び配布禁止	本ガイドラインに遵守していることを確認した上で業務遂行上必要な場合には、情報セキュリティ管理者の判断で持ち出しを可	支給以外の端末での作業の原則禁止	限定されたアクセスの措置が取られていること ※5	鍵付きケースへの格納	禁止	施錠可能な場所への保管	・耐火、耐熱、耐水、耐湿を講じた施錠可能な場所に保管(電子データの場合もこれらの対策に準じたサーバに保管) ・情報資産を格納するサーバのバックアップ ・6か月以上のログ保管 ・サーバの冗長化(推奨事項) ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁記録媒体の持ち込み禁止	電子記録媒体の初期化、復元できないようにして廃棄
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。	2B	2B	2B	同上	同上		同上	同上	安全管理措置の規定が必要	同上	同上	同上
Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす。	2A	2A	2A	同上	情報セキュリティ管理者の包括的承認で可		同上	同上	同上	同上	・耐火、耐熱、耐水、耐湿を講じた施錠可能な場所に保管(電子データの場合もこれらの対策に準じたサーバに保管) ・情報資産を格納するサーバのバックアップ(推奨事項) ・一定期間以上のログ保管 ・サーバ・ハードディスクの冗長化(推奨事項) ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁記録媒体の持ち込み禁止	同上
Ⅳ	影響をほとんど及ぼさない。	1	1	1									
情報資産の分類					情報資産の例示								

※1 組織外部への持ち出しとは、教育委員会・学校が構築している環境（本ポリシーが適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境）の外に情報資産を持ち出すことを示す。
※2 情報の組織外部への送信とは、情報システムを構築するネットワーク、端末、サーバの閉じた領域の外側に、情報資産をオンラインで持ち出すことを示す。
※3 情報資産の運搬とは、USBメモリやハードディスク等の外部電磁的記録媒体を介して情報資産を運搬する場合を示す。
※4 組織外部での情報処理とは、教育委員会・学校が構築・管理している環境（本ポリシーが適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境）の外において情報資産を管理・電算処理することを示す。
※5 限定されたアクセスの措置とは、適切かつ限定的な利用を前提とし、外部に送信される際に適切なアクセス制限を講じることを示す。

5 教育情報セキュリティ対策

情報資産を脅威から保護するため、次に定める教育情報セキュリティ対策を講ずるものとする。

⑴ 管理体制

情報資産を管理し、機密性、完全性及び可用性を維持するための体制を確立する。

⑵ 物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・盗難等から保護するために施設整備等の物理的な対策を講ずる。

⑶ 人的セキュリティ対策

教育情報セキュリティに関する権限や責任を定めるとともに、全教職員等にこのポリシーを周知徹底するための教育及び啓発を行う等、必要な対策を講ずる。

⑷ 技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、不正プログラム対策ソフトウェアの導入等の技術面における対策を講ずる。

⑸ 運用

① 情報システムの監視、この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、このポリシーの運用面の対策を講ずる。

② 情報セキュリティが侵害される事態が発生した場合に、被害の拡大防止、復旧等を迅速かつ的確に実施するため、緊急時対応計画を整備する。また、侵害に備えた対応訓練の定期的な実施等の対策を講ずるよう努める。

6 適応範囲

このポリシーの適用範囲は、学校、教育委員会、教育センターにおける学校用のシステム、サーバ、クラウドサービス等とする。

7 関係規程

教育情報セキュリティ対策基準を遵守して、教育情報セキュリティ対策を実施するに当たり、その具体的な手順等を明らかにするため、教育委員会及び各学校内で関連規程を定めるものとする。

なお、この規程の中で、公にすることにより学校運営に重大な支障を及ぼすおそれのある情報については、非公開とする。

８　教職員等の責務

学校長、教頭、教職員、会計年度任用職員やその他学校に所属する職員（以下「教職員等」という。）は、情報資産の利用に当たっては、関連法令を遵守しなければならない。また、教職員等は、教育情報セキュリティの重要性を認識し、このポリシーを遵守しなければならない。

９　監査及び点検

このポリシーの遵守状況を検証するため、必要に応じて監査を受け、定期的に点検を実施する。

１０　評価及び見直しの実施

監査又は点検の結果等により、このポリシーに定める事項、及び教育情報セキュリティ対策の評価を行うとともに、情報システムの変更や新たな脅威の発生等、状況の変化に迅速かつ的確に対応するため、必要に応じてこのポリシーの見直しを実施する。

第2章　教育情報セキュリティ対策基準

１　趣旨

この教育情報セキュリティ対策基準は、教育情報セキュリティ基本方針に沿って個々の対策を具体化したものであり、学校における教育情報セキュリティ対策の基準とする。

２　管理体制

教育情報セキュリティの管理体制は以下のとおりとする。

⑴　教育情報統括管理責任者

教育長を教育情報統括管理責任者とし、学校における全てのネットワークや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統括的な権限及び責任を有する。

⑵　教育情報統括責任者

教育こども部長を教育情報統括責任者とし、学校における情報資産に対するセキュリティ侵害が発生した場合、又はセキュリティ侵害のおそれがある場合に必要かつ十分な措置を行う権限及び責任を有する。

⑶　教育情報セキュリティ管理者

教育推進課長を教育情報セキュリティ管理者とし、学校における情報資産の管理及び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。

⑷　教育情報セキュリティ担当者

教育推進課参事を教育情報セキュリティ担当者とし、教育情報セキュリティ管理者の指示に従い、学校における情報資産の管理、運用ルールの策定及び情報セキュリティ対策に関する教職員等の教育研修、助言を行う。

⑸　教育情報システム管理者

教育総務課長を教育情報システム管理者とし、学校における教育情報システムの導入、管理、運用、見直し等に関する統括的な権限及び責任を有するほか、所管する教育情報システムに対する情報セキュリティ対策に関する権限及び責任を負う。

⑹　教育情報システム担当者

教育総務課職員を教育情報システム担当者とし、教育情報システム管理者の指示に従い、学校における教育情報システムの導入、管理、運用、見直し等の作業を行う。また、学校における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管理者を補佐する。

⑺　学校教育情報セキュリティ責任者

各学校長を学校教育情報セキュリティ責任者とし、所属校における教育情報セキュリティ実施手順書を策定し、情報資産の管理及び情報セキュリティ対策に関する権限及び責任を有する。また、学校における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、教育情報セキュリティ管理者、教育情報統括責任者、教育情報統括管理責任者に対する報告義務を定める。

⑻　学校教育情報セキュリティシステム管理者

各学校の教頭を学校教育情報セキュリティシステム管理者とし、学校教育情報セキュリティ責任者を補佐するとともに、所属する教職員等の教育情報セキュリティ対策の実施について、管理、指導を行う。また、個々の教育情報システムの管理、運用、見直し等の権限及び責任を有する。

⑼　学校教育情報セキュリティシステム担当者

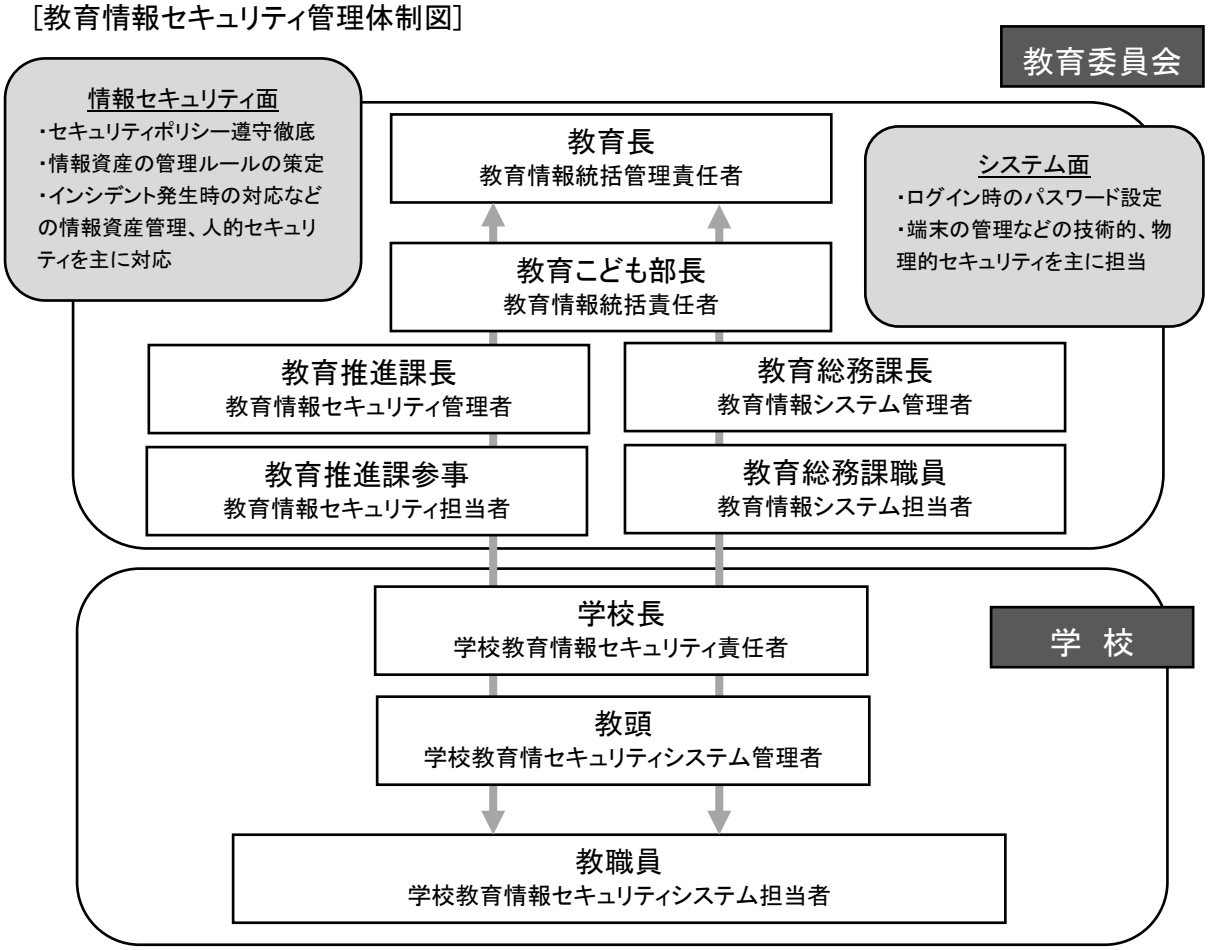
各学校の情報システムの管理、運用に携わる教職員等を学校教育情報セキュリテ

ィシステム担当者とし、管理、運用、見直し等の作業を行う。また、学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者と協力して、全教職員に対しこのポリシーの遵守及び周知・啓発に努める。

⑽　情報セキュリティ委員会への連携

教育情報統括責任者は、情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生した事案を正確に把握した上で、総合政策部長に報告し、連携を図る。

[教育情報セキュリティ管理体制図]



3　物理的セキュリティ対策

サーバ等や機器の保守・管理、配線や電源等の物理的セキュリティ対策は以下のとおりとする。

⑴　サーバ等の管理

ア　機器の取付け等

①　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 サーバ等の機器については、ラベルの貼付等、用途、種類等が明確に認識できるよう必要な措置を講じなければならない。

イ サーバの冗長化

重要なサーバ等の機器については、冗長化を図り、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生じた場合には、速やかにセカンダリサーバで対応できるように措置を講じ、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。

ウ 機器の電源

① サーバ等の電源については、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なければならない。

② 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。

エ 通信ケーブル等の配線

① 通信ケーブル及び電源ケーブルについては、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 主要な箇所の通信ケーブル及び電源ケーブルについては、定期的な点検を行い、損傷等が報告された場合は、連携して対応しなければならない。

③ 教育委員会及び学校長から許可を得た者、又は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。

オ 機器の定期保守及び修理

① 情報システムの安定的な運用のために、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 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は、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。

カ 機器の廃棄等

機器を廃棄又はリース返却をする場合、機器内部の記録装置から、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。

⑵ 通信回線及び通信回線装置の管理

ア 通信回線の管理

学校教育情報セキュリティ責任者は、学校内の通信回線及び通信回線装置を教

育委員会と連携し、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。

イ　外部へのネットワーク接続

学校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。

ウ　通信回線の適切な選択と情報の暗号化

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

エ　通信回線の暗号化

学校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。

⑶　教職員等の利用する端末や電磁的記録媒体等の管理

ア　校務用端末、校務外部接続用端末及び指導者用端末について

①　学校教育情報セキュリティシステム管理者は、盗難防止のため、端末のワイヤーによる固定や保管庫による管理等、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　学校教育情報セキュリティシステム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

③　学校教育情報セキュリティシステム管理者は、端末の電源起動時のパスワード(BIOS パスワード、ハードディスクパスワード等）を設定しなければならない。

④　学校教育情報セキュリティシステム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についても、データ暗号化機能を備える媒体を使用しなければならない。

イ　学習者用端末について

①　学校教育情報セキュリティシステム管理者は、盗難防止のため、教室等で利用するパソコンやモバイル端末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 学校教育情報セキュリティシステム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

③ 学校教育情報セキュリティシステム管理者は、授業に支障のないネットワーク構成の選択（帯域や同時接続数等）を行うこと。

④ 学校教育情報セキュリティシステム管理者は、児童生徒等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）フィルタリングソフト、検索エンジンのセーフサーチ、セーフブラウジングなど。

⑤ 学校教育情報セキュリティシステム管理者は、学校内外での端末におけるマルチウェア感染対策を講じなければならない。

⑥ 学校教育情報セキュリティシステム管理者は、端末のセキュリティ状態の監視に加えて、不適切なアプリケーションやコンテンツの利用を制限し、常に安全で児童生徒等が安心して利用できる状態を維持しなければならない。

⑦ 学校教育情報セキュリティシステム管理者は、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。

4 人的セキュリティ

教職員等が情報資産を取扱う際に遵守すべき人的セキュリティ対策は、以下のとおりとする。

⑴ 教職員等の遵守事項

ア 教育情報セキュリティポリシー等の遵守

教職員等は、この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、不明な点や遵守することが困難な点等がある場合は、速やかに学校教育情報セキュリティシステム管理者に相談し、指示を仰がなければならない。

イ 業務以外の目的での使用禁止

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。

ウ 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（本ポリシーが適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境）の外部における情報処理作業の制限

① 学校教育情報セキュリティ責任者は、重要分類Ⅱ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。

② 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、学校教育情報セキュリティシステム管理者の

許可を得なければならない。

③　教職員等は、外部で情報処理業務を行う場合には、学校教育情報セキュリティシステム管理者の許可を得なければならない。

エ　支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

①　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、業務上必要な場合には、学校教育情報セキュリティシステム管理者の許可を得て利用することができる。

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、学校教育情報セキュリティシステム管理者の許可を得た上で、外部で情報処理作業を行う際に、安全管理措置を遵守しなければならない。

オ　持ち出し及び持ち込みの記録

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

カ　パソコンやモバイル端末におけるセキュリティ設定変更の禁止

教職員等は、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、学校教育情報セキュリティシステム管理者の許可なく変更してはならない。

キ　机上の端末等の管理

教職員等は、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、又は学校教育情報セキュリティシステム管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

ク　退職時等の遵守事項

教職員等は、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。

ケ　情報セキュリティポリシー等の掲示

学校教育情報セキュリティ責任者は、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。

コ　外部委託事業者に対する説明

学校教育情報セキュリティシステム管理者は、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。

⑵　研修・訓練

ア　学校教育情報セキュリティ責任者は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

イ　学校教育情報セキュリティ責任者は、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、教育委員会の承認を得なければならない。

ウ　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。

エ　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。

オ　緊急時対応訓練

学校教育情報セキュリティ責任者は、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。

カ　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。

⑶　情報セキュリティインシデントの報告

ア　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、速やかに学校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　報告を受けた学校教育情報セキュリティ責任者は、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。

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、必要に応じて教育情報統括責任者及び教育情報統括管理責任者に報告しなければならない。

イ　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、学校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　報告を受けた学校教育情報セキュリティ責任者は、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。

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、速やかに教育情報統括責任者及び教育情報統括管理責任者に報告しなければならない。

④　教育情報統括責任者は、教育情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置

し、当該窓口への連絡手段を公表しなければならない。

ウ　情報セキュリティインシデント原因の究明・記録、再発防止等

①　教育情報統括責任者は、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、教育情報統括管理責任者に報告しなければならない。

②　教育情報統括管理責任者は、教育情報統括責任者から、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。

⑷　ＩＤ及びパスワード等の管理

ア　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。

イ　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、学校教育情報セキュリティ責任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。

5　技術的セキュリティ

情報システム等の不正利用を防止し、不正利用に対する証拠の保全をするための技術的セキュリティ対策は以下のとおりとする。

⑴　コンピュータ及びネットワークの管理

ア　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、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、機微な個人情報を保管する場合に限る。）については、標的型攻撃等によるファイルの外部流出の可能性を考慮し、ファイル暗号化等による安全管理措置を講じなければならない。

イ　バックアップの実施

教育情報統括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、校務系情報及び校務外部接続系情報、学習系情報について、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。

ウ　他団体との情報システムに関する情報等の交換

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

エ　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、所属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　教育情報統括責任者及び教育情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

③　教育情報統括責任者、教育情報システム管理者又は教育情報システム担当者

及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない。

オ　情報システム仕様書等の管理

教育情報統括責任者及び教育情報システム管理者は、ネットワーク構成図、情報システム仕様書等について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

カ　ログの取得等

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

②　教育情報統括責任者及び教育情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

③　教育情報統括責任者及び教育情報システム管理者は、取得したログを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。

キ　障害記録

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

ク　ネットワークの接続制御、経路制御等

①　教育情報統括責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、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　教育情報統括責任者は、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。

ケ　外部ネットワークとの接続制限等

①　教育情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、教育情報統括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、庁舎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洩、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　教育情報統括責任者及び教育情報システム管理者は、ウェブサーバ等をイン

ターネットに公開する場合、教育ネットワークへの侵入を防御するために、フェ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、教育情報統括責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

コ　無線ＬＡＮ及びネットワークの盗聴対策

①　教育情報統括責任者は、無線ＬＡＮの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

②　教育情報統括責任者は、機密性の高い情報を取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。

サ　電子メールのセキュリティ管理

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

②　教育情報統括責任者は、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　教育情報統括責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④　教育情報統括責任者は、教職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を教職員等に周知しなければならない。

シ　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教育情報統括責任者の許可なしに使用してはならない。

⑥　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、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。

⑦　児童生徒等が扱う電子メールは、学校教育情報セキュリティ責任者が許可し

た相手だけに送受信できる設定にしなければならない。

ス　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、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。

セ　機器構成の変更制限

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、教育情報統括責任者及び教育情報システム管理者の許可を得なければならない。

ソ　無許可でのネットワーク接続の禁止

教職員等は、学校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。

タ　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　学校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。

チ　無線ＬＡＮ及び移動体通信の利用制限

教職員等は、学校教育情報セキュリティ責任者が認めた場合に限り、教育外部系（授業用）ネットワーク、新教育外部系ネットワークの無線ＬＡＮ及び移動体通信を利用することができる。

ツ　スマートデバイスに係るセキュリティ管理

①　学校教育情報セキュリティシステム管理者は、スマートデバイスが備える機能や使用環境、取扱う情報、その他業務の特性等に応じ、適正なセキュリティ要件を定め、必要な対策を実施しなければならない。

②　教職員等は、スマートデバイスを使用するにあたり、学校教育情報セキュリティシステム管理者等が実施したセキュリティ対策及び、使用手順に従い適正にスマートデバイスを使用しなければならない。

⑵　アクセス制御等

ア　アクセス制御等

学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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。

イ　利用者ＩＤの取扱い

①　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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　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、学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者に通知しなければならない。

③　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、利用されていないＩＤが放置されないよう、人事管理部門と連携し、点検しなければならない。

ウ　特権を付与されたＩＤの管理等

①　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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のパスワードの漏洩等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

②　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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。

③　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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。

④　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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。

エ　教職員等による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、学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者の許可を得なければならない。

②　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管

理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

⑤　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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。

⑦　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、公衆通信回線（公衆無線ＬＡＮ等）を教育ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のＩＤ及びパスワード、生体認証に係る情報等の認証情報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。

オ　パスワードに関する情報の管理

①　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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　学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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。

カ　特権による接続時間の制限

学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者は、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。

⑶　システム開発、導入、保守等

ア　情報システムの調達

①　教育情報統括責任者及び教育情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

②　教育情報統括責任者及び教育情報システム管理者は、機器及びソフトウェア

の調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

イ　情報システムの開発

①　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、開発を行う場合には、教育情報統括責任者に協議しなければならない。

②　教育情報システム管理者は、システム開発に当たって、リスク分析を行うとともに、事故、障害等による被害の発生を防止する、もしくは最小限に抑えるため、必要な対策を講じなければならない。

ウ　情報システムの導入

①　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、十分なテストを行い、不具合の発見及び解消に努めなければならない。

②　教育情報システム管理者は、個人情報及び機密性の高いデータを、テストデータに使用してはならない。

③　教育情報システム管理者は、既存のネットワークを利用したシステムを導入しようとするときは、ネットワークへの接続テストを行うとともに、アクセス権限を明確にし、アクセスの管理等に関する事項を定めなければならない。

エ　システム開発、保守に関連する資料等の整備、保管

教育情報システム管理者は、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。

オ　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。

カ　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。

⑷　不正プログラム対策

ア　学校教育情報セキュリティ責任者の措置事項

学校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及び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　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。

イ　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　不正プログラム対策ソフトウェア開発者が提供するウイルス情報を、常に確認しなければならない。

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、以下の対応を行い、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。

・パソコン等の端末の場合は、ＬＡＮケーブルの即時取り外しを行わなければならない。

・モバイル端末の場合は、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　専門家の支援体制

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

⑸　不正アクセス対策

ア　学校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　使用されていないポートや不要なサービスについて、ポート閉鎖や機能を削除又は停止しなければならない。

②　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。

③　教育委員会及び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。

イ　学校教育情報セキュリティ責任者は、情報システムに対する攻撃予告があり、攻撃を受けることが明確になった場合には、システムの停止を含む必要な措置を講じなければならない。また、教育委員会との連絡を密にし、情報の取集に努めなければならない。

ウ　学校教育情報セキュリティ責任者は、外部から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、警察及び教育委員会との緊密な連携に努めなければならない。

エ　教育情報統括責任者及び教育情報システム管理者は、教職員等及び外部委託事業者が使用しているパソコンやモバイル端末からのネットワークや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。

オ　教育情報統括責任者は、教職員等が学校内にあるパソコンやモバイル端末を利用した不正アクセスを発見した場合には、当該教職員等が所属する学校教育情報セキュリティ責任者に通知し、適切な措置を求めなければならない。

カ　学校教育情報セキュリティ責任者は、標的型攻撃による内部への侵入を防止するために、以下のような対策を講じなければならない。

①　人的対策（標的型攻撃メール対策）

・差出人に心当たりのないメールは開封しない。

・不自然なメールが着信した際は、差出人にメール送信の事実を確認する。

・メールを開封した後で標的型攻撃と気付いた場合、添付ファイルは絶対開封せず、メールの本文に書かれたＵＲＬもクリックしない。

・標的型攻撃と気付いた場合、学校教育情報セキュリティ責任者に対して着信の事実を報告し、組織への注意喚起を依頼した後に、メールを速やかに削除する。

・学校教育情報セキュリティシステム管理者は、メールやログを確認し、不正なメールがなかったかチェックする。（事後対策）

②　電磁的記録媒体に対する対策

・出所不明の電磁的記録媒体を内部ネットワーク上の端末に接続させない。

・電磁的記録媒体をパソコン等の端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。
・パソコン等の端末について、自動再生（オートラン）機能を無効化する。
・パソコン等の端末について、電磁的記録媒体内にあるプログラムを媒体内から直接実行することを拒否する。

⑹　セキュリティ情報の収集

ア　教育情報統括責任者及び教育情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、学校と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、ソフトウェアの更新等の対策を実施しなければならない。

イ　教育情報統括責任者及び教育情報システム管理者は、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、対処方法について教職員等に周知しなければならない。

ウ　教育情報統括責任者及び教育情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、学校と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。

6　運用

⑴　情報システムの監視

ア　教育情報統括責任者及び教育情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。特に外部と接続するシステムについては、ファイアウォール等を用い、不正アクセスによる攻撃を受けていないかどうか、監視、分析を行わなければならない。

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

ウ　教育情報統括責任者及び教育情報システム管理者が指名した者は、重要性分類Ⅱ以上の情報資産を格納する校務系システム及び校務外部接続系システムを常時監視しなければならない。

エ　教育情報統括責任者及び教育情報システム管理者が指名した者は、重要性分類Ⅲ以上の情報資産を格納する学習系システムを常時監視しなければならない。

⑵　教育情報セキュリティポリシーの遵守状況の確認

ア　教育情報統括責任者及び教育情報セキュリティ管理者は、このポリシーに基づ

き、情報システム及びネットワークにおける情報セキュリティ対策の実施に関し、必要となる事項を定めた関係規程を作成し、教育情報統括管理責任者の承認を得なければならない。

イ　教育情報統括責任者及び教育情報セキュリティ管理者は、このポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに教育情報統括管理責任者に報告し、適切に対処しなければならない。

ウ　教育情報統括責任者及び教育情報セキュリティ管理者は、ネットワーク及びサーバ等のシステム設定時におけるこの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。

⑶　パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

教育情報統括責任者及び教育情報システム管理者が指名した者は、不正アクセス、不正プログラム等の調査のために、教職員等が業務で利用しているパソコン、モバイル端末及び電磁記録媒体等のログ、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。

⑷　教職員等の報告義務

ア　教職員等は、このポリシーに対する違反行為を発見した場合、直ちに学校教育情報セキュリティ責任者及び学校教育情報セキュリティシステム管理者に報告を行わなければならない。

イ　アの違反行為が、直ちに情報セキュリティ上重大な影響を及ぼす可能性があると教育情報統括責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

⑸　侵害時の対応等

ア　緊急時対応計画の策定

教育情報統括責任者は、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該計画に従って、適切に対処しなければならない。

イ　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

ウ　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、当該計画とこのポリシーの整合性を確保しなければならない。

エ　緊急時対応計画の見直し

教育情報統括責任者は、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。

⑹　例外措置

ア　例外措置の許可

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

イ　緊急時の例外措置

教育情報統括責任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、事後速やかに教育情報統括管理責任者に報告しなければならない。

ウ　例外措置の申請書の管理

教育情報統括責任者及び教育情報システム管理者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

⑺　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。

・地方公務員法（昭和２５年法律第２６１号）
・教育公務員特例法（昭和２４年法律第１号）
・著作権法（昭和４５年法律第４８号）
・不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）
・個人情報の保護に関する法律（平成１５年法律第５７号）
・行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号）
・島本町情報公開条例（昭和５８年島本町条例第２４号）
・島本町個人番号の利用及び特定個人情報の提供に関する条例（平成２７年島本町条例第２２号）

・島本町個人情報の保護に関する法律施行条例（令和４年島本町条例第２４号）

⑻　懲戒処分等

ア　教育情報統括責任者は、教職員等がこのポリシーに規定する事項及び指示に違反した場合には、当該教職員等が所属する学校教育情報セキュリティ責任者に通知し、ネットワーク及び情報機器等の利用を停止し、その権利を剥奪することができる。

イ　当該教職員等は、違反の重大性、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関係法令による懲戒処分の対象とする。

7　外部委託

⑴　外部委託事業者の選定基準

ア　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。

イ　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。

⑵　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)

⑶　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、前項の契約に基づき措置しなければならない。また、その内容を教育情報統括責任者に報告するとともに、その重要度に応じて教育情報統括管理責任者に報告しなければならない。

⑷　約款による外部サービスの利用

ア　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、機密性の高い情報が取扱われない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
・利用手続及び運用手順

イ　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。

⑸　ソーシャルメディアサービスの利用

ア　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　教育委員会又は学校のアカウントによる情報発信が、実際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やプロフィール画面等に当該情報を掲載して参照可能とするとともに、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。

イ　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。

ウ　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。

８　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

外部委託やクラウドサービスの利用に当たり、個人情報の収集・利用範囲や管理期間、データの統制と所有の在り方等について、以下の事項について事業者に確認しなければならない。

⑴　個人情報の利用範囲

教育、学校の目的に必要な情報、又は児童生徒等及び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。

⑵　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。

⑶　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等及び保護者に対する行動ターゲ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。

⑷　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、又は児童生徒等及び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。

⑸　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。

⑹　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。

⑺　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、教職員、又は利用者によって承認された目的に限ること。

⑻　個人情報の取扱いについての情報開示

個人情報の取扱いについて、契約又はプライバシーポリシーで明確に示すこと。

⑼　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。

⑽　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、漏洩、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。

⑾　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、個人情報保護法制等を遵守し、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、管理すること。

⑿　合併・買収

合併又は他社による買収を伴う場合、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。

9　点検・評価・見直し

⑴　実施方法

教育情報統括責任者及び学校教育情報セキュリティ責任者は、所管する教育情報システム及び教育ネットワーク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、定期的又は必要に応じて、点検を行わなければならない。また、外部委託事業者に委託している場合、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、このポリシーの遵守について、定期的に又は必要に応じて、点検を行わなければならない。

⑵　報告

教育情報統括責任者及び学校教育情報セキュリティ責任者は、情報セキュリティ対策状況についての点検結果を教育情報統括管理責任者に報告する。

⑶　保管

教育情報統括責任者及び学校教育情報セキュリティ責任者は、点検の実施を通して収集した点検結果、点検報告書作成のための調書等を、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。

⑷　点検結果への対応

教育情報統括責任者及び学校教育情報セキュリティ責任者は、点検結果に基づき、必要な改善を行わなければならない。また、点検結果において、このポリシーの記載事項に疑義が生じた場合には、速やかに教育情報統括管理責任者に報告し、対処しなければならない。

⑸　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・変更

ア　教育情報統括管理責任者及び教育情報統括責任者は、新たに必要な対策が発生した場合又は点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、このポリシー及び関係規程等について、定期的に又は必要に応じて評価を行い、必要があると認めた場合、見直し、変更等を行わなければならない。

イ　教育情報統括管理責任者及び教育情報統括責任者は、教育情報セキュリティ対策基準の変更を行った場合には、速やかに学校教育情報セキュリティ責任者及びその他関係者に周知を行わなければならない。

ウ　教育情報統括責任者は、所管する教育情報システム及び教育ネットワーク等について、このポリシーの変更並びに情報セキュリティに関する状況の変化等に応じて、適宜情報セキュリティ対策の見直しを行い、必要があると認めた場合、当該システム及びネットワークの関係規程の変更を行わなければならない。