真狩村教育情報セキュリティポリシー

真狩村教育委員会

令和３年　４月　１日

＜　目　次　＞

序　真狩村教育情報セキュリティポリシーの目的及び構成

１．目的

真狩村立学校（以下「学校」という。）が取り扱う情報には、児童生徒・保護者の個人情報のみならず、学校運営上重要な情報など、外部に漏えいした場合に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小中学校情報ネットワークの情報を様々な脅威から防御することは、個人の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、学習指導要領にも、情報活用能力育成やプログラミング教育等の導入、感染症等によるオンライン授業での学習の保障など、様々な場面で教育の情報化が求められており、学校がこれに積極的に対応するためには、すべてのネットワーク及び教育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となる。

そのため、学校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、真狩村教育情報セキュリティポリシー（以下「教育情報セキュリティポリシー」という。）を定めることとする。

（※）国際基準化機構（ISO）が定めるもの（ISO7498-2：1989）

・機密性：情報にアクセスすることが認可されたものだけがアクセスできることを確実にすること。

・完全性：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

・可用性：許可された利用者が必要なときに情報アクセスできることを確実にすること。

２．構成

教育情報セキュリティポリシーは、学校が保有する情報資産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ものである。

教育情報セキュリティポリシーは、学校が保有する情報資産を取り扱うすべての職員に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかし一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化に対し柔軟に対応することも必要である。

このようなことから、教育情報セキュリティポリシーは、一定の普遍性を備えた部分としての「教育情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に対応する部分としての「教育情報セキュリティ対策基準」から構成する。

教育情報セキュリティポリシーの構成

文　　書　　名		内　　容
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	情報セキュリティ対策に関する統一的且つ基本的な方針
	教育情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全ての情報システムに共通の情報セキュリティ対策の基準

第１章　真狩村教育情報セキュリティ基本方針

１．趣旨

この教育情報セキュリティ基本方針は、学校の教育情報セキュリティ対策の基本的な方針を定めるものとする。

２．定義

教育情報セキュリティポリシーにおいて、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

（１）ネットワーク

真狩村の内外部局を相互に接続するための通信網、その構成機器（ハードウエア及びソフトウエア）及び記録媒体で構成され、処理を行う仕組みをいう。

（２）教育情報システム

ネットワーク、ハードウェア、ソフトウェア及びアプリケーション及び記録媒体で構成され、処理を行う。

（３）情報資産

ネットワーク及び教育情報システムの開発と運用に係る全てのデータならびにネットワーク及び教育情報システムで取り扱う全てのデータをいう。

（４）情報セキュリティ

情報資産の機密性、完全性及び可用性の維持することをいう。

３．対象範囲

教育情報セキュリティポリシーは、学校の情報資産に関する業務に携わる全ての職員等及び外部委託者を対象とする。

４．教育情報セキュリティ管理体制

教育情報セキュリティ対策を推進、管理するための体制及び役割を定めるものとする。

５．情報資産の分類及び管理

情報資産は、その重要性に応じて分類し、適正な管理を行うこととする。

６．教育情報セキュリティ対策

教育情報セキュリティを確保するため、次の各号に掲げる教育情報セキュリティ対策を講ずるものとする。

（１）物理的セキュリティ対策

教育情報システムを設置する施設への不正な立ち入り、情報資産への損傷、妨害等から保護するために講ずる物理的な対策をいう。

（２）人的セキュリティ対策

教育情報セキュリティに関する職員の責務を定め、職員等に教育情報セキュリティ対策を

周知徹底する等、十分な教育及び啓発を行うために講じる人的な対策をいう。

（3）技術及び運用におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するために講じる、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策及び教育情報システム開発等の外部委託、ネットワークの監視、教育情報セキュリティ対策の実施状況を確認する等の運用面における対策をいう。

（4）障害時におけるセキュリティ対策

情報セキュリティに係る障害が発生した場合に迅速な対応を可能とするために講じる緊急時の対策をいう。

7．教育情報セキュリティ対策基準

教育情報セキュリティ対策を講ずるにあたり、遵守すべき行為及び判断等の基準を明らかにするため、「教育情報セキュリティ対策基準」を定めるものとする。

8．教育情報セキュリティ関係規定

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あたり、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定を定めるものとする。

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

9．法令等の遵守

学校の情報資産に関する業務に携わる全ての職員等及び外部委託者については、教育情報セキュリティポリシーの重要性について共通の認識を持つとともに業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

１０．点検・監査

教育情報セキュリティポリシーの遵守状況について、必要に応じて点検又は監査を実施する。

１１．評価及び見直しの実施

点検又は監査の結果に基づき、教育情報セキュリティ対策の評価を行うとともに、情報セキュリティを取り巻く状況の変化に対応するために、適宜教育情報セキュリティポリシーの見直しを実施する。

第２章　真狩村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おいて規定する教育情報セキュリティ対策を実行に移すための、真狩村の教育情報セキュリティ対策の基準を定めるものとする。

2. 組織体制

学校の教育情報セキュリティ管理体制については、以下のとおりとする。

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

①副村長を、CISO とする。

②CISO は、学校におけるすべての情報資産及び教育情報システムの情報セキュリティを統括権限を有する。

（２）　統括教育情報セキュリティ責任者（CIO : Chief Information Officer、以下「教育 CIO」という。）

①教育長を、教育 CIO とする。

②教育 CIO は、CISO を補佐しなければならない。また、CISO が不在の場合は、その職務を代行する。

③教育 CIO は、学校の情報ネットワーク、教育情報システム等の開発、運用、見直し等の統括権限や責任を有する。

④教育 CIO は、教育情報セキュリティポリシーについて、外部委託事業者または指定管理者に遵守させること。

（３）教育情報セキュリティ責任者

①教育次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、学校の情報セキュリティ対策に対する権限及び責任を有する。

③教育情報システム等の開発、運用、見直し等の統括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、学校において所有している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、教育情報セキュリティポリシーの遵守に関する教職員等への教育、訓練、助言及び指示を行う。

⑤教育情報セキュリティ責任者は、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 CIO 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。

（４）教育情報システム管理者

①教育次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、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（5）教育情報システム担当者

①教育委員会学校教育係を、教育情報システム担当者とする。

②教育情報システム管理者の指示のもと、教育情報システムの開発、設定の変更、運用、見直しを行う。

③セキュリティインシデント発生時には、教育情報セキュリティ責任者を補佐する。

（6）学校教育情報セキュリティ管理者（以下「学校 CIO」という。）

①学校長を、学校 CIO とする。

②学校 CIO は、所管の学校内の情報資産の管理責任を有する。

③学校 CIO は、災害、過失等による障害、ウイルス感染、不正アクセス等に備えて、教育情報システムの適正な管理を行うこと。

④学校 CIO は、学校情報セキュリティ担当者を定め、その資質の向上に努めること。

⑤教育情報セキュリティポリシーについて所管する学校職員に遵守させること。

⑥教育セキュリティ関係規定、障害記録、教育情報システム仕様書等の整備及び管理を行うこと。

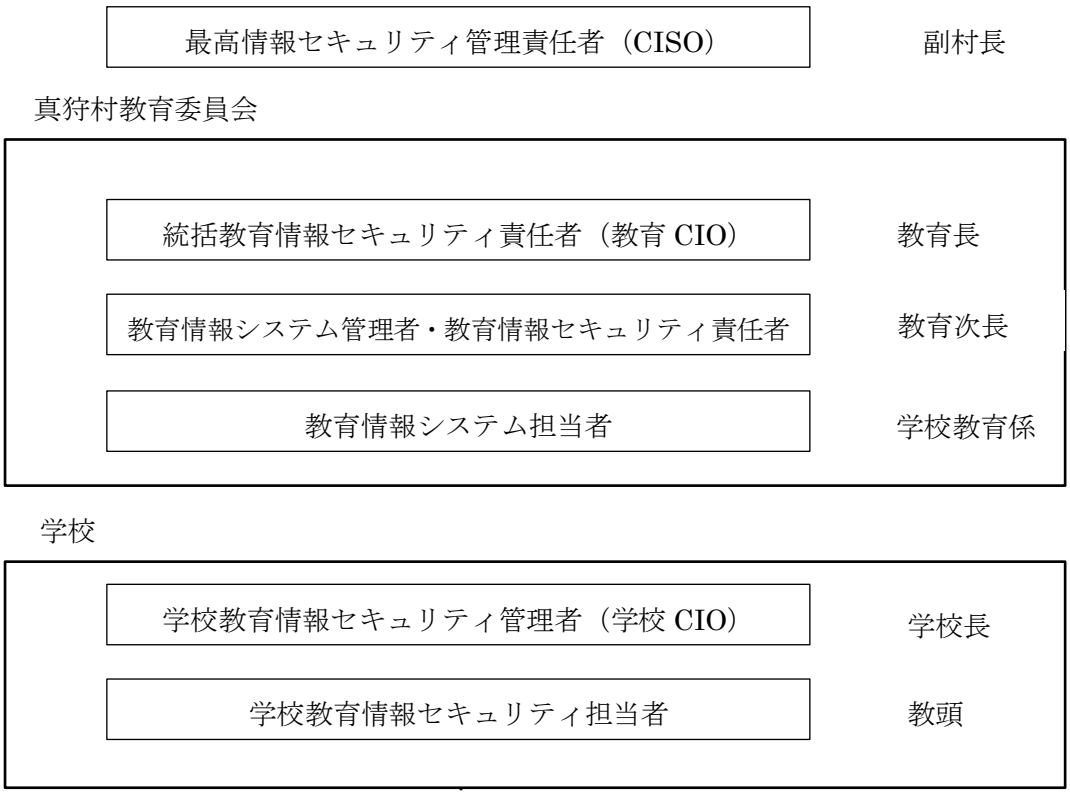
（7）学校教育情報セキュリティ担当者

①教頭を学校教育情報セキュリティ担当者とする。

②学校 CIO を補佐しなければならない。

③学校 CIO に情報セキュリティに必要な情報を提供し、その指示によって学校内の教育情報セキュリティ対策を推進する。

【体制図】



3. 対象範囲及び用語説明

（1）行政機関の範囲

本対策基準が適用される範囲行政機関等は、村内学校とする。

（2）情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりである。

①学校情報ネットワーク、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学校情報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

用語	定義
校務系情報	学校が保有する情報資産のうち、それら情報を学校・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、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（クラウド接続系）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。 小中学校においては学習クラウドとして、Google LLC の「G Suite for Education」を利用する。
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	校務外部接続系情報及び学習系情報にアクセス可能な端末。
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。
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、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。
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。
学校情報ネットワーク	村立学校の隔離された情報ネットワーク。真狩村情報ネットワークとは分かれて独立している。
真狩村情報ネットワーク	真狩村の情報ネットワークの総称。インターネット接続系と LGWAN 系、利用事務系ネットワークに分かれている。真狩村役場電算担当者が管理する。
サーバ	学校情報ネットワーク内のサーバ。データセンターや役場にある。
教職員	教育委員会所管の学校に勤務する教職員や事務職員等。
端末機	パソコンやモバイル端末（タブレット等）機器。
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捉えられる事象（障害、事件、事故、欠陥、攻撃、侵害等）
標的型攻撃	明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種。
役場庁舎サーバ室	機器等を安全に設置するため、庁舎内に高度な電源・空調を備え、セキュリティ・災害体制が整備されたサーバ室。真狩村役場電算担当者が管理する。
特定個人情報	個人番号（マイナンバー）を内容に含む個人情報

４．情報資産の分類と管理

（１）情報資産の分類

学校の情報資産の機密性、完全性及び可用性の度合により別表１に分類する。

（２）情報資産の管理

①管理責任

（ア）学校 CIO 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利用者の責任

情報資産を利用するものは、情報資産の分類に従い利用する責任を負う。

③情報の作成

（ア）教職員は、業務上必要のない情報を作成してはならない。

（イ）情報を作成する者は、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。

（エ）教職員が業務上作成した情報の著作権はすべて真狩村教育委員会に帰属する。

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、入手した情報資産の分類が不明な場合、学校 CIO 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、適切な取扱いをしなければならない。

（ウ）情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥情報資産の保管

（ア）学校 CIO 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。

情報資産の保管場所は、次のとおりとする。

保管場所	説明	保管できる情報資産分類
校務系共有フォルダ X ドライブ	役場内にある校務系ネットワーク用サーバ	写真や動画等大容量データ
校務系共有フォルダ Y ドライブ	データセンターにある校務系ネットワーク用サーバ	全ての情報資産（写真や動画は除く）

校務外部接続系共有フォルダ X ドライブ	役場内にある校務外部接続系ネットワーク用サーバ	写真や動画等大容量データ、機密性２A 以下のもの
校務外部接続系共有フォルダ Y ドライブ	データセンターにある校務外部接続系ネットワーク用サーバ	機密性２A 以下のもの（個人が特定される情報は除くこと）
学習用 Google クラウド	Google LLC の G Suite for Education という教育機関として認証を受けた学校用の学習系クラウド。	機密性２A 以下のもの（個人が特定される情報は除くこと）
持ち出しのできない電磁的記録媒体	情報処理に用いられる記憶媒体のうち、持ち出しのできない媒体（端末に内臓されている HDD 等）	校務外部接続系端末（ノート PC・共有 PC のみ）原則として機密性２A 以下のもの（ただし個人が特定される情報は除く）
持ち出しのできる電磁的記録媒体	情報処理に用いられる記憶媒体のうち、持ち出しのできる媒体（USB・DVD－R 等）	原則として機密性２A 以下のもの（ただし個人が特定される情報は除く）

（イ）学校 CIO は、情報資産を記録した持ち出しのできる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る等の情報保護対策をして保管しなければならない。

（ウ）学校 CIO は、機密性２A 以上、完全性２A 以上または可用性２A 以上の情報を記録した持ち出し可能な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。

（エ）学校 CIO は、情報資産を記録した持ち出し可能な電磁的記録媒体等の授受について台帳を整備し、次の事項を記録しておくこと。

・情報資産等の名称

・搬入者及び受領者の氏名並びに所属等の名称

・授受年月日

・その他学校 CIO が必要と認める事項

（オ）不要となったデータについては、速やかに消去すること。

（カ）長期的に保存する機密性２A 以下の写真や動画の大容量データについては、持ち出し可能な電磁的記録媒体での保管とすること。

⑦情報の送信

電子メール等により機密性２以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

⑧情報資産の運搬

（ア）やむを得ず、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、情報資産等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、学校 CIO 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、必要に応じ暗号化又はパスワードの設定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、学校 CIO に許可を得なければならない。

（ウ）学校 CIO 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・破壊等、情報を復元できないように処置した上で廃棄しなければならない。

（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、学校 CIO の許可を得なければならない。

５．特定個人情報の取扱い

特定個人情報を取り扱う場合は、学校情報ネットワーク内に構築された閉鎖的な環境で取り扱うものとし、ファイルやデータの暗号化や利用者認証パスワード等の漏えい防止のための措置を講じなければならない。

ただし、学校 CIO 及び教育情報セキュリティ責任者の許可を得て、学校情報ネットワーク外で取り扱う場合は、常に最新のウイルスセキュリティ対策を講じた環境で行うこととする。

６． 物理的セキュリティ

（１）サーバ等の管理

①　装置の取付け等

（ア）サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

（イ）教育情報セキュリティ責任者、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容易に操作できないように、利用者の ID・パスワードの設定等の措置を施さなければならない。

（ウ）無線 LAN の導入は、経路の暗号化等、十分な漏えい防止策を講じなければ実施してはならない。

（エ）重要なサーバ等の機器については、冗長化を図り、メインサーバに障害が生じた場合は速やかにセカンダリーサーバで対応を行えるようにするなど、システム運用が停止しない措置を講じなければならない。

（オ）学校情報ネットワークの基幹サーバはデータセンターに置き、データセンターの管理は外部委託者によるものとする。

②　機器の電源

（ア）サーバ等の電源については、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

（イ）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施さなければならない。

③　配線

（ア）配線は傍受または損害を受けることがないよう、可能な限り必要な措置を施さなければ

ならない。

（イ）主要な箇所の配線については、損傷等についての定期的な点検を行わなければならない。

（ウ）教育 CIO から許可を得た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、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。

④　機器の定期保守及び修理

（ア）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。

（イ）教育情報システム管理者は、電磁的記録媒体を内蔵する機器を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、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行わなければならない。

⑤　施設外又は学校校舎外への機器の設置

教育 CIO 及び教育情報システム管理者は、施設外又は学校校舎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。

⑥　機器の廃棄等

教育情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。ただし、守秘義務契約を締結している事業者の場合は、この限りではない。

（２）ネットワークにおける措置

①ネットワーク構築上の措置

（ア）学校情報ネットワークについては、安全対策に万全な措置を講じなければならない。

（イ）学校情報ネットワークは、校務を取り扱う校務系、校務において外部との接続をする校務外部接続系、児童生徒の学習で利用する環境の学習系に切り分けて構築しなければならない。

（ウ）事業の目的により無線通信とする場合は、次の事項を遵守すること。

・学校 CIO は、利用者の端末機を管理すること。

・セキュリティ機能を有する暗号化手法や端末機等のアクセス制御を行うこと。

②ネットワーク機器等

（ア）基幹機器（管理用及び認証サーバ、交換機等）について

学校情報ネットワークの基幹機器（管理用及び認証用サーバ、交換機等については、データセンターに設置しなければならない。また、ネットワークの運用上重要な機能を有する機器については、障害発生時にネットワークの運用が停止しないように冗長化を図る等必要な措置を講じなければならない。

・主要なネットワーク機器（ハブ、ルータ等）及び配線については、管理者以外の者が容易に操作できないような場所に格納する等の必要な措置を講じなければならない。

・ネットワーク機器等の構成管理を適切に行わなければならない。

・主要なネットワーク機器については、落雷等による異常電波及び停電等の電気的障害に対し、必要な防護措置を講じなければならない。

（イ）ネットワーク機器の設置

学校情報ネットワーク機器は、教育委員会が指定した場所に設置する。業務上必要があり、設置した場所を移動する場合は、学校 CIO が教育情報セキュリティ責任者に許可を得なければならない。

③通信回線

各学校間とデータセンター間を結ぶ通信回線については、専用回線または高いセキュリティ機能を有する回線により構成し、外部からの情報の盗聴及び情報の漏えい等を防止しなければならない。

（3）教職員等の利用する端末や電磁的記録媒体等の管理

（校務用端末及び指導者用端末について）

① 教育情報システム管理者は、盗難防止のため、職員室等で利用する校務用端末のワイヤー等による固定、教室等で使用する指導者用端末の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 教育情報システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

③ 教育情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体か、認証パスワード付与機能付きの媒体を使用しなければならない。

（学習者用端末について）

① 教育情報システム管理者は、盗難防止のため、教室等で利用する場合は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、タブレット端末等のモバイル端末の場合は、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。

（端末の持ち出しについて）

① 児童生徒及び教職員については、教育 CIO が認める場合、端末の持ち出しを可能とする。

② 持ち出し可能と認める端末は、アプリやソフトウェアによるウイルス対策、フィルタリングが適用されているもののみとする。

③ 学校情報ネットワークに再接続する際、必要に応じてリフレッシュを行う。

7． 人的セキュリティ

（1）教職員における情報セキュリティの徹底

①教育情報セキュリティポリシーの遵守

すべての教職員は、教育情報セキュリティポリシー及び関係規定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、速やかに学校 CIO に相談し、指示を仰がなければならない。

②ID 又はアカウント及びパスワードの管理

すべての教職員は、アクセス権限にかかる情報を適切に管理し、次の事項を遵守しなければならない。

・ID 又はアカウント及びパスワードは他者に知られないように管理にしなければならない。

・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すること。

・仮のパスワードは、最初のログイン時点で変更すること。

・必要でない限り、システム間及び教職員間でのパスワードの共有は行わないこと。

・端末機のパスワードの記憶機能を利用してはならないこと。

・パスワードが流出した可能性がある場合は、速やかに教育情報セキュリティ責任者に報告し、パスワードを変更しなければならない。

③業務以外の目的での使用の禁止

すべての教職員は、業務以外の目的で情報資産の外部への持ち出し、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。

④学校情報ネットワークに接続できる端末

学校情報ネットワークに接続できる端末は、以下のとおりである。

（ア）真狩村教育委員会が設置した端末

（イ）その他教育 CIO が必要と認めた端末

⑤④における指導者用端末の使用について

教職員は、④の端末機のうち、指導者用端末について以下のとおり使用しなければならない。

（ア）教職員は、各学校で取得した管理対象アカウントでのみログインを行い、私的なアカウントでのログインは認めない。

（イ）教職員は、指導者用端末にインストールしたいアプリケーション（以下、「アプリ」という。）がある場合は、教育システム管理者の許可を得ること。

（ウ）学校 CIO は、使用しているアプリを把握しておかなければならない。

（エ）指導者用端末等を校外から持ち出すことを原則禁止とする。ただし、教育 CIO が必要と認める場合は、この限りではない。

（オ）撮影した写真や動画のデータは、学習系情報の場合は学習用 Google クラウド、校務系の場合は校務系・校務外部系 X フォルダに保存すること。保存する必要がなくなった場合は、速やかに削除すること。

（カ）教職員は、タブレットの保管について学校 CIO の指示に従い、盗難防止に努めなければならない。

⑥学習用 Google クラウドの管理

教育委員会が認めた外部クラウドは、Google LLC から認証を受けた「G Suite for Education」のサービスであり、学校ごとに児童生徒及び教職員へ付与する専用アカウントを利用すること。

プライベートアカウントによるGoogleのクラウドサービスの使用を禁ずる。

学校CIOは、学校でのGoogleクラウド管理者を定め、教職員の転出入等のアカウント管理や、クラウド内の情報資産の使用方法等が、真狩村教育情報セキュリティポリシーを遵守しているか定期的に確認しなければならない。

児童生徒及び教職員の転出入があった場合は、教育システム管理者に速やかに報告すること。

⑦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

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。

⑧端末や電磁的記録媒体等の情報の持ち出しにおける情報処理作業の制限

（ア）教職員は、端末のソフトウェア及びアプリ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責任者の許可なく変更してはならない。

（イ）教職員は、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CIOの許可なく情報が閲覧されることがないように、離席時の端末ロックや電磁的記録媒体、文書等が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。

（ウ）教職員は、異動、退職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。

（エ）教職員は、端末機のソフトウェア及びアプリのインストール及びアンインストール、若しくは機器の改造、設定変更、増設、交換は、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

⑨個人所有の端末の業務利用

教職員は、④以外で個人が所有している端末を、原則持ち込んではいけない。

やむを得ず業務上で必要する場合は、以下のことを厳守すること。

（ア）ネットワーク接続の有無に関わらず、教育CIOの許可を得ること。

（イ）教育CIOの許可を得て使用し、業務で使用する必要がなくなった場合は、速やかに教育CIOに報告し使用を終了すること。

⑩退職時等の遵守事項

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

（２）会計年度任用職員等への対応

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責任者は、会計年度任用職員等に対し、採用時に教育情報セキュリティポリシー等のうち、会計年度任用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責任者は、会計年度任用職員等の採用の際、必要に応じ、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、会計年度任用職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

（3）教育情報セキュリティポリシー等の掲示

教育情報セキュリティ管理者は、教職員等が常に教育情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

（4）外部委託事業者に対する説明

教育情報セキュリティ責任者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、教育情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

（5）研修・訓練

学校 CIO は、定期的に教職員を対象とする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。

（6）情報セキュリティインシデントに対する報告

①教職員は、ネットワークの利用に際して情報セキュリティインシデントを発見した場合、速やかに学校 CIO 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教職員は、学校 CIO の指示に従い、情報セキュリティインシデントに対し適切に対処しなければならない。

③教職員は、情報セキュリティに対する事故、システム上の欠陥及び誤操作を発見した場合または村民等外部から通報を受けた場合、速やかに学校 CIO に報告しなければならない。

④学校 CIO 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 CIO 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。

（7）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 CIO は、情報セキュリティインシデントについて、学校 CIO、教育情報システム責任者及び小中学校ネットワーク管理を委託している業者と連携し、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。

②CISO は、教育 CIO に、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。

（8）法令等の遵守

教職員は、取り扱う情報資産及び教育情報システムについて、特に次の法令等に従わなければならない。

①地方公務員法第 33 条（秘密を守る義務）

②著作権法（昭和 45 年法律第 48 号）

③真狩村個人情報保護条例（平成 17 年条例第 11 号）

④真狩村情報公開条例（平成 17 年条例第 10 号）

８．技術的セキュリティ

（１）外部系ネットワークとの接続にかかる措置

①外部ネットワークを利用し、教委以外の者と通信（メールやホームページ編集作業を行う場合を除く）を行うときは、原則として機密性２A 以上のデータは取り扱ってはならない。

②外部クラウドの利用は、教育情報セキュリティ責任者が使用を認めた学習用 Google クラウドのみとし、授業等で使用する場合は機密性２A までは保存できるものとする。ただし個人が特定できないよう、個人情報（出席番号、氏名、住所、電話番号、メールアドレス等）を削除すること。

③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）ホームページを利用した情報提供の措置

原則として個人情報を取り扱ってはならない。ただし、学校教育上個人情報を取り扱う必要があるときは、あらかじめ個人情報保護条例に基づく必要な対処を行い、適正に適用しなければならない。

（３）バックアップの実施

教育 CIO 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、以下のとおりバックアップを実施する。

①校務系情報及び校務外部接続系情報についてじゃ、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、必要に応じてバックアップを実施しなければならない。

（４）コンピュータウイルス対策

①ウイルス対策の実施

（ア）教育情報システム管理者は、外部のネットワークから受信したファイルについてウイルスチェックを行うなど、ネットワークへの感染を防止しなければならない。

（イ）教育情報システム管理者は、ウイルスの感染、侵入が生じる可能性が著しく低い場合を除き、ウイルスチェック用のソフトウェア及びアプリを導入しなければならない。

（ウ）教育情報システム管理者は、サーバ及び端末機に、ウイルスチェック用のソフトウェア及びアプリを導入しなければならない。

（エ）教育情報システム管理者は、端末機に対して、ウイルスチェック用のソフトウェア及びアプリによるフルチェックを定期的に実施しなければならない。

（オ）教育情報システム管理者は、ウイルスチェック用のソフトウェア及びアプリ及びパターンファイルを常に最新のものに保たなくてはならない。

（カ）教育情報システム管理者は、システムがインターネットに接続していない場合、定期的にウイルスチェック用のソフトウェア及びアプリ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。また、電磁的記憶媒体を使う場合、コンピュータウイルス等の感染を防止するために、支給以外の電磁的記憶媒体を教職員に利用してはならない。

（キ）業務で利用するソフトウェア及びアプリは、パッチやバージョンアップなど開発元の

サポートが終了したソフトウェア及びアプリは利用してはならない。

②ウイルス対策の周知・徹底

教職員は、次の事項を遵守しなければならない。

（ア）外部からデータまたはソフトウェア及びアプリを取り入れる場合には、必ずウイルスチェックを行うこと。

（イ）添付ファイルのあるメールを送受信するときは、添付ファイルにウイルスが感染していないかどうか確認を行うこと。

（ウ）差出人が不明または不自然に添付されたファイル、URL などは開かずに速やかに削除すること。

（エ）教育 CIO または教育情報セキュリティ責任者が許可した電磁的記憶媒体以外は使用しないこと。

③ウイルス感染時の対応

（ア）教育情報システム管理者は、ウイルスチェックの結果、ウイルス感染を発見したときは、影響範囲及び感染経路等を調査し、ウイルスの削除等必要な対策を速やかに行うこと。

（イ）教育情報システム管理者は、ウイルスによりネットワーク及びシステム等情報資産に影響が生じたときは、侵害等の対応に基づき、必要な措置を講じなければならない。

（ウ）教職員は、ウイルスに感染した場合また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。

・パソコン等の LAN ケーブルの即時取り外しを行うこと。無線の場合は、直ちに通信を切断すること。

・むやみにシャットダウンをせず、そのままの画面で置いておき、教育システム管理者に報告し、指示を仰ぐこと。

（5）システムの開発、導入、保守における措置

①システムの調達

（ア）教育情報システム管理者は、システムの調達に当たって、調達仕様書が情報セキュリティの確保の上で問題の無いようにしなければならない。

（イ）教育情報システム管理者は、機器及びソフトウェア及びアプリを調達する場合は、製品が情報セキュリティ上問題にならないかどうか、確認しなければならない。

②システムの開発

（ア）教育情報システム管理者は、小中学校情報ネットワークを利用し、システムの開発を行うときは、CISO に協議しなければならない。

（イ）教育情報システム管理者は、システムの開発に当たって、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、若しくは最小限に抑えるため、次の事項に留意し、必要な対策を講じなければならない。

・システムの運転状況を監視する機能を備えるとともにシステムの障害箇所の検知機能を備えること。

・障害箇所を特定するため、ロギング情報（処理及び操作の記録情報）が取得できること。

・必要に応じて故障個所を閉塞し縮退運転ができるようにすること。
・必要に応じてサーバ、ディスク装置等主要機器の代替機器を備え、障害時に代替機器への切替が容易に行えること。
・本番の運用環境と開発、保守環境とは別に分けること。
・本番のシステムデータ及びプログラムとテスト用のデータ及びプログラムは別に管理すること。
・データ及びシステムのバックアップが容易に行えるようにすること。
・データ入力時のエラーチェックが行えるようにすること。
・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 を削除すること。
・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すること。
・教育情報システム管理者は、システムの維持管理に必要な各種ドキュメントを整備し、保管場所を定め厳重に保管しなければならない。

③システムの導入

（ア）教育情報システム管理者は、システムを導入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。

（イ）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、当該ネットワークの教育情報システム管理者に協議し、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。

④システムの保守

（ア）教育情報システム管理者は、システムの保守を行うときは、不具合の確認を行い、既存のシステムの運用に影響が出ないようにしなければならない。

（イ）教育情報システム管理者は、システムの追加、変更、廃棄等をしたときは、その際の履歴を記録するとともに、ドキュメントの変更整備を行わなければならない。

⑤機器の保守等

（ア）機器の保守点検を定期的に実施するとともに、その記録を適切に保存しなければならない。

（イ）記録媒体の含まれる機器について、外部の業者に修理させる場合は、当該機器に記録されている内容が消去された状態で行わなければならない。ただし、情報を消去することが難しい場合は、修理を委託する事業者に対し秘密を守ることを契約に定めなければならない。

（ウ）記録媒体の含まれる機器を廃棄、リース返却等をする場合は、当該機器に記録されている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。

（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修正

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最新の情報を収集し、必要に応じてネットワーク、システムの端末機及びサーバ等のソフトウェア及びアプリに最新

のプログラム修正を行うことにより、セキュリティホールを防ぐ等、必要な措置を講じなければならない。

②セキュリティ侵害の対策

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最新の情報を収集し、必要に応じて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。

③ウイルス対策の周知・徹底

教育情報セキュリティ管理者は、常時ウイルスに関する情報収集に努めるとともに、必要に応じてウイルス対策について教職員に対する啓発を行わなければならない。

9．運用

（1）システム等の適正運用

①関係規程の作成

学校 CIO は、教育情報セキュリティポリシーに基づき、当該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 CIO の承認を得なければならない。

②運用管理手法、運用計画の明確化

（ア）教育情報システム管理者は、システムの運用を開始する前に、運用管理の手法及び体制等について明らかにしなければならない。

（イ）教育情報システム管理者は、システムの運用に当たり、運用計画を策定し、年間・月間・週間等における運用スケジュール、システムの運用時間、運用形態等運用管理に必要な事項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、ネットワークの運用に当たり、運用管理の手法及び体制、運用計画を明らかにしなければならない。

③機器操作の適正化

（ア）システムにおける措置

システムのサーバ等の機器については教育情報システム管理者、また端末機については教育情報セキュリティ責任者が、それぞれ指示若しくは承認したものが行わなければならない。

教育情報システム管理者は、操作マニュアル等を作成する、または利用方法の周知を行う等、ネットワークの利用の適正化に努めなければならない。また、ネットワークの追加、変更、廃棄等したときは、その履歴を記録するとともに常に変更を反映し、操作マニュアル等を最新の状態にしなければならない。

教育情報システム管理者は、ネットワークのオペレーション作業の実施について適切に管理しなければならない。

・スケジュール管理

・出力及び廃棄帳票の管理

・磁気テープ等の記録媒体の管理
・オペレータの電子計算機室への入退室管理
・オペレータの作業内容の把握、管理
・電子計算機機器及びネットワーク機器の障害時の対応
・その他必要な事項

（イ）ネットワークにおける措置

ネットワーク機器の操作については、教育情報システム管理者が指示若しくは承認した者が行わなければならない。

教育情報システム管理者は、操作マニュアル等を作成する、または利用方法の周知を行う等、ネットワークの利用の適正化に努めなければならない。また、ネットワークの追加、変更、廃棄等をしたときは、その履歴を記録するとともに常に変更を反映し、操作マニュアル等を最新の状態にしなければならない。

教育情報システム管理者は、ネットワークのオペレーション作業の実施について適切に管理しなければならない。

④データ等のバックアップ運用

教育情報システム管理者は、万一の事故、障害等の発生に備え、データ・プログラムのバックアップを適切に行わなければならない。

データ・プログラムのバックアップに当たっては、次の事項に留意しなければならない。

（ア）教育情報システム管理者は、バックアップコピーを取得するデータ、取得の方法及びサイクルを定め、それに基づいてデータのバックアップを適切に実施しなければならない。

（イ）教育情報システム管理者は、プログラムの変更の都度、プログラムのバックアップコピーを取得しなければならない。

（ウ）教育情報システム管理者は、データのバックアップ取得後、次のデータのバックアップ取得までの間、必要に応じて、データベースの更新記録情報を取得しなければならない。

（２）システム等の監視及び予防措置

①システム等の監視

（ア）重要システムの運用に当たっては、情報セキュリティに関する事案を検知するため、教育 CIO 及び教育情報セキュリティ責任者は、常にシステムの稼働監視を行わなければならない。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、不正な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）ネットワークに係る情報セキュリティに関する事案を検知するため、教育 CIO は、ネットワークの稼働監視を行わなければならない。特に、外部と接続するネットワークについては、ファイアウォール、侵入監視装置等を用い、不正な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。

（ウ）監視により得られた結果については、消去や改ざんされないために、必要な措置を講じ、定期的に安全な場所に保管しなければならない。

（エ）重要なログ等を取得するサーバについては、正確な時刻設定およ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。

②予防措置

（ア）教育 CIO 及び教育情報セキュリティ責任者は、システム及びネットワークに障害または侵害が発生し、システムが利用できない場合に備え、業務への影響を最小限に抑えるため、代替処理方法を定めなければならない。

（イ）システムに被害が生じる恐れがある事案を発見した場合、教育情報セキュリティ責任者は予防措置を講じなければならない。また、教育情報セキュリティ責任者は、直ちに教育 CIO に報告しなければならない。

（ウ）教育 CIO は、直ちに当該事案を CISO に報告しなければならない。

（エ）ネットワークに被害が生じる恐れがある事案を発見した場合、教育情報セキュリティ責任者は、予防措置を講じなければならない。また、教育情報セキュリティ責任者は、直ちに教育 CIO に報告しなければならない。

（オ）教育 CIO は、直ちに当該事案を CISO に報告し、改善について指示を受け、速やかに対策に向け、適切な措置を講じなければならない。

（３）システム及びネットワークの障害時、侵害時の対応

①障害時の対応

（ア）システムにおける措置

(A)責任体制

教育 CIO 及び教育情報セキュリティ責任者は、システムの障害時における連絡及び対処の責任者となり、関係者との連携によりシステムを速やかに回復しなければならない。

(B)障害時における対応方法の周知

教育 CIO 及び教育情報セキュリティ責任者は、障害時における対応方法について、関係者に周知しなければならない。

(C)障害時の連絡及び対処

a.ネットワークの利用者が障害を発見した時は、直ちに、学校 CIO または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。

b.学校 CIO は、障害を発見し、または障害の連絡を受けたときは、直ちに、障害状況及び影響範囲を調査するとともに、教育情報セキュリティ責任者に当該障害状況等を連絡しなければならない。

c.学校 CIO は、障害に関係する教育情報セキュリティ責任者と連携し、障害の回復に向け適切な措置を講じなければならない。

d.教育 CIO は、障害発生の原因及び処理の報告を求めるとともに、ネットワーク上の障害、故障の原因及び処理結果について記録しなければならない。

e.学校 CIO または教育情報セキュリティ責任者は、ネットワークに重大障害が発生している場合は、直ちに教育 CIO に報告を行わなければならない。

f.報告を受けた教育 CIO は、直ちに CISO に報告を行わなければならない。

(D)再発防止措置

教育 CIO 及び教育情報セキュリティ責任者は、障害原因等を分析し、再発防止に向け必要な改善措置を講じなければならない。

(E)事後検証

CISO は、報告のあった障害事案について、再発防止に向け必要な改善措置を講じなければならない。

②侵害時の対応

(A)責任体制

教育 CIO 及び学校 CIO は、所管する情報資産及びネットワークにおいて、不正行為等による情報の漏えい、滅失、改ざん等の侵害事案が発生した場合、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に実施するとともに、再発防止の措置を講じなければならない。また、CISO は、侵害時の対応が円滑に実施されるよう、監督、指導を行わなければならない。

(B)侵害時の対応方法の周知

教育 CIO は、所管する情報資産に対し、作成される関係規程において、侵害時の対応方法を明記させるとともに、関係する管理者、教職員に対し当該対応方法について周知を行わなければならない。

(C)侵害時の連絡

a システムの利用者が侵害事案の発生を発見したときは、直ちに学校 CIO に報告する。

b.学校 CIO は、侵害事案の発生を発見し、または侵害の報告を受けたときは、直ちに、教育情報セキュリティ責任者及び教育 CIO に報告を行わなければならない。

c.報告を受けた教育 CIO は、直ちに CISO に報告しなければならない。

d.教育 CIO 及び学校 CIO は、侵害事案が法令等に違反するものと見込まれた場合、CISO と協議し、警察等関係機関に通報しなければならない。

e.CISO は、侵害事案がサイバー攻撃等による緊急時の場合においては、緊急連絡体制を設置し、情報セキュリティ対策が適切に実施されるよう、監督、指導を行わなければならない。

f.侵害を発見した者または侵害の報告を受けた者は、当該侵害事案を報告すべき者が不在の場合その他の場合において、急に要するときは、上記の規定にかかわらず、直ちに当該侵害事案を報告すべき者の上位の者に報告しなければならない。

(D)事案への対処

a.学校 CIO 及び教育情報セキュリティ責任者は、侵害事案が発生したときは、次の事項について調査を実施しなければならない。

・事案の内容

・事案が発生した原因

・確認した被害・影響範囲

b.学校 CIO は、次の事案が発生し情報資産保護のためにシステムの停止がやむを得ない場合は、教育情報セキュリティ責任者に協議の上、システムを停止しなければならない。ただし、情報資産を保護するため急を要する場合には、学校 CIO は当該協議をしないでシステムを停止することができる。

・システムの運用に著しい支障をきたす攻撃が継続しているとき
・コンピュータウイルス等不正プログラムが情報に深刻な被害を及ぼしているとき
・その他情報資産に係る重大な被害が想定されるとき

c.学校 CIO 及び教育情報セキュリティ責任者は、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とともに、事案に対処した経過を記録しなければならない。

d.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講じた後、システムの復旧を行う。

e.教育 CIO は、上記の対処に当たり、学校 CIO から随時報告を求め、作業の実施を管理しなければならない。

(E)再発防止措置

学校 CIO 及び教育情報セキュリティ責任者は、当該事案に係る原因及びリスク等を分析し、再発防止に向け必要な改善措置を講じなければならない。また、教育 CIO は、改善措置の実施について確認を行うとともに、再発防止に向け、関係する管理責任者、教職員に対し対応方法について周知を行わなければならない。

(F)事後検証

CISO は、報告のあった侵害事案について、再発防止に向け必要な改善措置が講じられているか教育 CIO に報告を求めることができる。

（４）例外措置

①例外措置の許可

学校 CIO 及び教育情報セキュリティ責任者は、ポリシー等を遵守することが困難な状況で、事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、また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 に承認を受けて、例外措置を取ることができる。

②緊急時の例外措置

学校 CIO 及び教育情報セキュリティ責任者は、事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避の場合は、事後直ちに CISO に報告しなければならない。

（５）ポリシー等の遵守状況の確認

①ポリシー等の遵守状況の確認

教育情報セキュリティ責任者は、学校等において、ポリシー及び所管する情報資産に係る関係規程が遵守されているかどうか、また、侵害等の問題が発生していないかについて確認し、問題が発生した場合には、直ちに教育 CIO に報告しなければならない。

教育 CIO は、学校において、ポリシー及び所管する情報資産に係る関係規程が遵守されているかどうか、また、侵害等の問題が発生していないかについて確認し、問題が発生した場合には、直ちに CISO に報告しなければならない。

CISO は、ポリシー等の遵守状況及び問題発生の状況について確認を行うため、学校 CIO に報告を求めることができる。

教育 CIO は、所管する情報資産について関係規程の作成または見直しが行われた場合、当該学校 CIO から報告を受けなければならない。また、学校 CIO は、関係規程を見直し、

変更（役職名や連絡先の変更等軽微なものを除く。）が行われた場合、CISO に報告を行わなければならない。

②ポリシー違反に関する対応

故意または重大な過失により、ポリシーに違反し、教委が保有する情報資産に危害が加えられるなど、校務の運用に支障を生じさせた教職員は、懲戒処分に関する指針に基づく処分を受けることがある。

１０．外部サービスの利用

（１）外部委託

教育情報システムの外部委託を行う際は、以下の点に留意する。これは共同アウトソーシングやクラウドサービス利用の形態等による場合も同様である。

①選定基準

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、外部委託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。

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、情報セキュリティマネジメントシステムの国際規格認証取得状況、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。

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

②契約項目

教育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関係規程の遵守。
・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補償
・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業務
・村による監査、検査
・村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、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 CIO に報告するとともに、その重要度に応じて CISO にしなければならない。

（２）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 2B 以上の情報が取り扱われない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

教職員は、利用するサービスの約款、その他提供条件から、利用にあ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。

（３）ソーシャルメディアサービスの利用

教育情報システム管理者は、教育委員会また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教育委員会または学校のアカウントによる情報発信が、教育委員会または学校のものであることを明らかにするために、プロフィール画面等に掲載し、参照可能とするとともに、アカウントの自由記述欄等に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等を適切に管理し、不正アクセス対策を行うこと。

③機密性２A 以上の個人が特定される情報は、ソーシャルメディアサービスで発信してはならない。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。

１１．点検・評価及び見直し

（１）点検・評価

①学校 CIO は、所管するシステム及びネットワークに係る関係規程に基づき、必要な情報セキュリティ対策が実際になされているかどうか、また、関係規程に記載された情報セキュリティ対策に不足がないかどうかについて、定期的に点検を行わなければならない。外部委託事業者に委託している場合も、教育情報セキュリティポリシーの遵守について定期的に点検を行わなければならない。

②学校 CIO 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、教育情報セキュリティポリシーの記載に疑義が生じたときは、直ちに教育 CIO 及び CISO に報告しなければならない。

③CISO は、教育 CIO 及び学校 CIO に対し、情報セキュリティ対策の監査、点検実施の要請、点検結果の報告を求めることができる。

④CISO または教育 CIO は、関係規程に基づき必要な情報セキュリティ対策が実際に実施さ

れているかどうか、また、関係規程に記載された情報セキュリティ対策に不足がないかどうかについて、定期的に点検を行うとともに、点検結果に基づき、必要な改善を行わなければならない。

（2）セキュリティ対策の見直し、変更

①CISO または教育 CIO は、新たに必要な対策が発生した場合または点検の結果、教育情報セキュリティポリシーの内容に疑義が生じた場合等において、教育情報セキュリティポリシーの実効性を評価し、必要な部分の見直し、変更を行わなければならない。

②CISO または教育 CIO は、対策基準の変更を行ったときは、速やかに学校 CIO その他関係者に周知を行わなければならない。

③学校 CIO は、所管するシステム及びネットワークについて、教育情報セキュリティポリシーの変更並びに情報セキュリティをめぐる情勢の変化等に伴い、適宜情報セキュリティ対策の見直しを行い、必要があると認めるときは、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。

④CISO は、ネットワークについて、教育情報セキュリティポリシーの変更に伴う情報セキュリティ対策の見直しを行わなければならない。

別表１　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	持ち出しの禁止	持ち出しの制限	持ち出しの制限なし
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 ・転退学記録簿 ・転入学記録簿 ・就学児童生徒異動報告書 ・休学・退学願受付簿 ・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 ・評定一覧表 ・進級・卒業認定資料 ・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 ○進路関係 ・卒業生進路先一覧等 ・進路希望調査 ・進路判定会議資料 ・進路指導記録簿 ・入学者選抜に関する表簿（願書等） ○健康関係 ・健康診断に関する表簿 ・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） ○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） ○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	○成績関係 ・通知票 ・定期考査・テスト等の答案用紙（児童生徒が記入済みのもの） ○指導関係 ・児童生徒等の個人写真・集合写真 ・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 ・個別指導計画 ・家庭訪問記録・個別面談記録 ・教務手帳 ・週ごとの指導計画（個人情報が含まれるもの） ○進路関係 ・調査書 ・推薦書 ・私立高校入試に係る事前相談資料 ・公立高校入学者選抜に係る成績一覧表 ○健康関係 ・児童生徒健康調査票 ・児童生徒の健康保険等被保険者証の写 ○その他 ・給食関係書類・寄宿関係資料 ○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 ・座席表 ・PTA 会長名簿 ・職員緊急連絡網・職員住所録 ・委員会名簿	
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**		○児童生徒の学習系情報 ・児童生徒の学習記録 （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） ○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	
Ⅳ	影響をほとんど及ぼさない。	**1**	**1**	**1**			○学校運営関係 ・学校要覧 ・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 ・保護者等への配布文書例 ・各種届出雛形・校務分掌票 ・PTA 資料 ・学校・学級だより ・学校 HP 掲載情報 ・学校行事のしおり ・授業用教材 ・教材研究資料 ・生徒用配布プリント

（参考資料）【教育情報セキュリティ管理体制】

名称	職名	職務	情報セキュリティインシデント対策
最高情報セキュリティ責任者（CISO）	副村長	学校における全ての情報資産及び教育情報システムの情報セキュリティを統括する最高責任者	統一的な窓口の機能を有する組織を整備し、インシデント報告を受けた場合、状況を確認し、報告体制（関係部局へ情報提供し、重要度影響度合いを勘案して報道機関へ通知・公表等）を整備する。
統括教育情報セキュリティ責任者 （教育 CIO）	教育長	CISO を補佐し、教育ネットワーク、教育情報システム等の開発、運用、見直し等の統括権限や責任を有し、CISO が不在の場合は、その職務を代行する。	障害時、必要な場合 CISO に報告。 侵害時、必要な措置、再発防止の措置実施。必要な場合 CISO に報告
教育情報システム管理者	次長	個々の教育情報システムに関する権限及び責任を有する。個々の教育情報システムの開発、設定の変更、運用、見直し等の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関する情報セキュリティ対策の権限及び責任を負う。	
教育情報セキュリティ責任者	次長	個々の教育情報システムに関する権限及び責任を有する。個々の教育情報システムの開発、設定の変更、運用、見直し等の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関する情報セキュリティ対策の権限及び責任を負う	障害時、連絡及び対処の責任者
教育情報システム担当者	学校教育係	個々の教育情報システムの開発、設定の変更、運用、見直しを行う。 セキュリティインシデント発生時には、教育情報セキュリティ責任者を補佐する。	障害時侵害時ともに教育情報システム管理者を補佐する。
学校教育情報セキュリティ責任者 （学校 CIO）	学校長	学校における情報セキュリティに関する適正な運用及び管理を行う。 教育情報セキュリティ管理者は、所管する情報資産及び教育情報システムに関して次の職務を行う。 １情報資産の管理に関すること。 ２災害、過失等による障害、ウイルス感染、不正アクセス等に備えて、教育情報システムの適正な管理を行うこと。 ３情報セキュリティ担当者を定め、その資質の向上に努めること。 ４教育情報セキュリティポリシーについて職員に遵守させること。 ５教育情報セキュリティポリシーについて外部委託事業者または指定管理者に遵守させること。 ６教育情報セキュリティ実施手順、障害記録、教育情報システム仕様書等の整備及び管理を行うこと。	障害時、連絡及び対処の責任者 侵害時　必要な措置を迅速に実施するとともに、再発防止の措置
学校教育情報セキュリティ担当者	教頭等	教育情報セキュリティ管理者（校長）の情報セキュリティに関する適正な運用及び管理を補佐する。 教育情報セキュリティ管理者（校長）に情報セキュリティに必要な情報を提供し、その指示によって学校内の教育情報セキュリティ対策を推進する。	