１　目的

久御山町立学校情報セキュリティ対策基準（以下「対策基準」という。）は、久御山町情報セキュリティ基本方針（以下「基本方針」という。）に基づき、久御山町立学校の情報システムを活用して収受した学校運営上必要な情報や、児童生徒及び教職員等に関する個人情報等の様々な情報の取扱いに関するセキュリティ対策を実施する上で必要な基準を定めることを目的とする。

２　対象範囲及び用語説明

2.1　行政機関等の範囲

本対策基準が適用される行政機関等は、教育委員会及び町立学校とする。

2.2　情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

ア　教育ネットワーク、教育情報システム、これらに関する設備、電磁的記録媒体

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

ウ　教育情報システムの仕様書及びネットワーク図等のシステム関連文書

2.3　用語説明

ア　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

イ　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

ウ　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

エ　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

オ　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

３　情報セキュリティ管理体制

3.1　体制

適切に情報セキュリティ対策を推進・管理するための体制として、次の者をおく。

3.1.1　統括教育情報セキュリティ責任者

教育長を統括教育情報セキュリティ責任者とする。

3.1.2　教育情報セキュリティ責任者

教育次長を教育情報セキュリティ責任者とする。

3.1.3　校内教育情報セキュリティ責任者

校長を校内教育情報セキュリティ責任者とする。

3.1.4　教育情報システム管理者

学校教育課長を教育情報システム管理者とする。

3.2　権限と責任

前項で定めた情報セキュリティ管理体制における権限と責任については次のとおりとする。

3.2.1　統括教育情報セキュリティ責任者

ア　統括教育情報セキュリティ責任者は、本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。

イ　統括教育情報セキュリティ責任者は、本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。

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責任者、教育情報セキュリティ管理者に対して、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。

エ　統括教育情報セキュリティ責任者は、本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、必要かつ十分な措置を行う権限及び責任を有する。

オ　統括教育情報セキュリティ責任者は、本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。

3.2.2　教育情報セキュリティ責任者

ア　教育情報セキュリティ責任者は、本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。

イ　教育情報セキュリティ責任者は、本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。

ウ　教育情報セキュリティ責任者は、本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。

3.2.3　校内教育情報セキュリティ責任者

ア　校内教育情報セキュリティ責任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。

イ　校内教育情報セキュリティ責任者は、町立学校において、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へ速やかに報告を行い、指示を仰がなければならない。

3.2.4　教育情報システム管理者

ア　教育情報システム管理者は、所管する教育情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

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

ウ　教育情報システム管理者は、所管する教育情報システムに係る情報セキュリティ実施手順を策定し、その維持・管理を行う。

3.2.5　兼務の禁止

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。

4　情報資産の分類と管理

4.1　情報資産の分類と管理方法

対象となる情報資産は、機密性、完全性及び可用性を踏まえ、次の各号に掲げるとおり分類し、必要に応じて取扱制限を行うものとする。

	重要性分類
Ⅰ	セキュリティの侵害が児童生徒又は教職員等の生命、財産、プライバシー等へ重大な影響を及ぼす情報を含むもの
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情報を含むもの
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情報を含むもの
Ⅳ	セキュリティ侵害が影響をほとんど及ぼさないもの

4.2　情報資産の管理

4.2.1　管理責任

ア　校内教育情報セキュリティ責任者は、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、複製された情報資産も 4.1 の分類に基づき管理しなければならない。

4.2.2　情報資産の分類の表示

教職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、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。

4.2.3　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 4.1 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。

4.2.4　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、重要性分類に基づき、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、校内教育情報セキュリティ責任者に判断を仰がなければならない。

4.2.5　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。

4.2.6　情報資産の保管

ア　校内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、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　校内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、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　校内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、重要性分類Ⅲ以上の情報を記録した電磁的記録媒を保管する場合、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。

4.2.7　情報の送信

電子メールにより重要性分類Ⅲ以上の情報を外部送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

4.2.8　情報資産の運搬

ア　車両等により重要性Ⅲ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こうじなければならない。

イ　重要性分類Ⅲ以上の情報資産を運搬する者は、校内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。

4.2.9　情報資産の提供・公表

ア　重要性分類Ⅲ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　重要性分類Ⅲ以上の情報資産を外部に提供する者は、校内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。

ウ　校内教育情報セキュリティ責任者は、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。

4.2.10　情報資産の廃棄

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

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、校内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。

5　物理的セキュリティ

5.1　サーバ等の管理

5.1.1　機器の取付

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

5.1.2　機器の電源

ア　教育情報システム管理者は、校務系サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

イ　教育情報システム管理者は、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。

5.1.3　通信ケーブル等の配線

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

イ　教育情報セキュリティ責任者と教育情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、損傷等の報告があった場合、連携して対応しなければならない。

ウ　教育情報セキュリティ責任者と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。

エ　教育情報セキュリティ責任者と教育情報システム管理者は、自ら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講じなければならない。

5.1.4　機器の定期保守及び修理

ア　教育情報システム管理者は、重要性分類Ⅲ以上のサーバ等の機器の定期保守を実施しなければならない。

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、

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。

5.1.5　施設外又は学校外への機器の設置

教育情報セキュリティ責任者及び教育情報システム管理者は、施設外又は学校外にサーバ等の機器を設置する場合、統括教育情報セキュリティ責任者の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

5.1.6　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。

5.2　管理区域の管理

5.2.1　管理区域の構造等

ア　管理区域とは、ネットワークの機関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。

イ　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。

ウ　教育情報セキュリティ責任者及び教育情報システム管理者は、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。

エ　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、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

オ　教育情報セキュリティ責任者及び教育情報システム管理者は、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、防火装置、防水装置等を講じなければならない。

カ　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。

5.2.2　管理区域の入退室管理等

ア　教育情報システム管理者は、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。

イ　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。

ウ　教職員等は、児童生徒が管理区域に入室する場合、必要に応じて立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。

エ　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。

オ　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、外見上教職員等と区別できる措置を講じなければならない。

5.2.3　機器等の搬入出

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

イ　教育情報システム管理者は、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等を立ち会わせなければならない。

5.3　ネットワークの管理

5.3.1　通信回線及び通信回線装置の管理

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

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

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

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

5.4　教職員等の利用する端末や電子記録媒体等の管理

5.4.1　校務用端末、校務外部接続用端末及び指導者用端末について

ア　教育情報システム管理者は、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、盗難防止のための措置を講じなければならない。また、電子記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

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

5.4.2　学習者用端末について

ア　教育情報システム管理者は、盗難防止のため、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。

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

6　人的セキュリティ

6.1　教職員等の遵守事項

6.1.1　教職員等の遵守事項

ア　教育情報セキュリティポリシーの遵守事項

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

イ　業務以外の目的での使用の禁止

教職員等は、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外部における情報処理作業の制限

（ア）統括教育情報セキュリティ責任者は、重要性分類Ⅲ以上の情報資産を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やむを得ない事情により外部に持ち出す場合には、校内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。

（ウ）教職員等は、やむを得ない事情により外部で情報処理業務を行う場合には、校内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。

エ　支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

（ア）教職員等は、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、校内教育情報セキュリティ責任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、校内教育情報セキュリティ責任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

校内教育情報セキュリティ責任者は、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校内教育情報セキュリティ責任者の許可無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校内教育情報セキュリティ責任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。

6.1.2　非常勤及び臨時の教職員等への対応

ア　教育情報セキュリティポリシー等の遵守

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

イ　教育情報セキュリティポリシー等の遵守に対する同意

校内教育情報セキュリティ責任者は、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。

ウ　インターネット接続及び電子メール使用等の制限

校内教育情報セキュリティ責任者は、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。

6.1.3　情報セキュリティーポリシー等の掲示等

校内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等しなければならない。

6.1.4　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。

6.2　研修・訓練

6.2.1　統括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。

6.2.2　研修計画の策定及び実施

ア　統括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う。

イ　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。

ウ　研修は、教育情報セキュリティ責任者、校内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その他の教職員等に対して、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。

6.2.3　緊急時対応訓練

統括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。

6.2.4　研修・訓練への参加

全ての教職員等は、情報セキュリティに関する意識を深め情報セキュリティ上の問題が生

じないようにするため、定められた研修・訓練に参加しなければならない。

6.3　情報セキュリティインシデントの報告

6.3.1　学校内からの情報セキュリティインシデントの報告

ア　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、速やかに校内教育情報セキュリティ責任者に報告しなければならない。

イ　報告を受けた校内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責任者、教育情報システム管理者に報告しなければならない。

ウ　校内教育情報セキュリティ責任者は、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。

6.3.2　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

ア　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、校内教育情報セキュリティ責任者に報告しなければならない。

イ　報告を受けた校内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責任者に報告しなければならない。

ウ　校内教育情報セキュリティ責任者は、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。

6.3.3　情報セキュリティインシデントの原因の究明・記録、再発防止等

ア　教育情報セキュリティ責任者は、情報セキュリティインシデントについて、校内教育情報セキュリティ責任者、教育情報システム管理者と連携し、これらの情報セキュリティインシデントの原因を究明し、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、統括教育情報セキュリティ責任者に報告しなければならない。

イ　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。

6.4　ＩＤ及びパスワード等の管理

6.4.1　ＩＣカード等の取扱い

ア　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通報し、指示に従わなければならない。

イ　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。

ウ　教育情報セキュリティ責任者及び教育情報システム管理者は、ＩＣカード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃

棄しなければならない。

6.4.2　ＩＤ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。

ア　教職員等は、自己が利用しているＩＤは、他人に利用させてはならない。

イ　共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

6.4.3　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。

ア　パスワードは、他人に知られないように管理しなければならない。

イ　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

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

エ　パスワードが流出したおそれがある場合には、校内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。

オ　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。

カ　仮のパスワードは、最初のログイン時点で変更しなければならない。

キ　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。

ク　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）

ケ　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。

7　技術的セキュリティ

7.1　コンピュータ及びネットワークの管理

7.1.1　文書サーバ及び端末の設定等

ア　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。

イ　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。

ウ　特定の教職員等のみが取り扱う権限を持つ情報については、権限のない者が閲覧及び使用できないよう設定しなければならない。

エ　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。

7.1.2　バックアップの実施

教育情報セキュリティ責任者及び教育情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策にかかわらず、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。

7.1.3　他団体との情報システムに関する情報等の交換

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

7.1.4　システム管理記録及び作業の確認

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

イ　教育情報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。

ウ　外部委託事業者がシステム変更等の作業を行う場合は、できる限り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。

7.1.5　情報システム仕様書等の管理

教育情報セキュリティ責任者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。

7.1.6　ログの取得等

ア　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。

イ　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、適切にログを管理しなければならない。

ウ　教育情報セキュリティ責任者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。

7.1.7　障害記録

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。

7.1.8　ネットワークの接続制御、経路制御等

ア　教育情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

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

7.1.9　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、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ教育ネットワーク及び教育情報システム分離する等の措置を講じなければならない。

7.1.10　外部ネットワークとの接続制限等

ア　教育情報システム管理者は、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、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。

イ　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。

ウ　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者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。

エ　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。

オ　教育情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、教育情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

7.1.11　機微情報に対するインターネットリスク、児童生徒による機微情報へのアクセスリスクへの対応

ア　教育情報システム管理者は、校務系システム及び学習系システム間の通信経路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リスクの高いシステムと機微情報（特に校務系）を論理的又は物理的に分離する、もしくはこれに類する安全管理措置を講じなければならない。特にクラウドについても、通信経路の論理的又は物理的な分離によるセキュリティの品質に準じた安全管理措置を講じること。

イ　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、ウイ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。

7.1.12　複合機のセキュリティ管理

ア　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。

イ　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。

ウ　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。

7.1.13　特定用途機器のセキュリティ管理

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。

7.1.14　無線ＬＡＮ及びネットワークの盗聴対策

ア　教育情報セキュリティ責任者は、無線ＬＡＮの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務づけなければならない。

イ　教育情報セキュリティ責任者は、重要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。

7.1.15　電子メールの利用制限

ア　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。

イ　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。

ウ　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。

エ　教職員等は、重要な電子メールを誤送信した場合、校内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。

オ　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セキュリティ責任者の許可無しに使用してはならない。

7.1.16　電子署名・暗号化

ア　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、統括教育情報セキュリティ責任者が定めた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

イ　教職員等は、暗号化を行う場合に統括教育情報セキュリティ責任者が定める以外の方法を用いてはならない。

ウ　統括教育情報セキュリティ責任者は、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。

7.1.17　無許可ソフトウェアの導入等の禁止

ア　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。

イ　教職員等は、業務上必要がある場合は、教育情報セキュリティ責任者及び教育情報システム管理者の許可を得て、ソフトウェアを導入することができる。

ウ　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。

7.1.18　機器構成の変更の制限

ア　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。

イ　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。

7.1.19　無許可でのネットワーク接続の禁止

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

7.1.20　業務以外の目的でのウェブ閲覧の禁止

ア　教職員等は、業務以外の目的でウェブを閲覧してはならない。

イ　教育情報セキュリティ責任者は、教職員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、校内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。

7.2　アクセス制御等

7.2.1　アクセス制御

ア　アクセス制御等

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。

イ　利用者ＩＤの取扱い

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

（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、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。

（イ）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点検しなければならない。

ウ　特権を付与されたＩＤの管理等

（ア）教育情報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のパスワード漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

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

（ウ）統括教育情報セキュリティ責任者は、代行者を認めた場合、速やかに教育情報セキュリティ責任者、校内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通知しなければならない。

（エ）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）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）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。

7.2.2　教職員等による外部からのアクセス等の制限

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

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

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

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

オ　教育情報セキュリティ責任者及び教育情報システム管理者は、外部からのアクセスに利用するモバイル端末を教職員等に貸与する場合、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。

カ　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、パッチの適用状況を確認しなければならない。

キ　教育情報セキュリティ責任者は、公衆通信回線（公衆無線ＬＡＮ等）を教育ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のＩＤ及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ＩＣカード等）による認証に加えて通信内容の暗号化等、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。

7.2.3　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。

7.2.4　パスワードに関する情報の管理

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。

7.2.5　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。

7.3　システム開発、導入、保守等

7.3.1　情報システムの調達

ア　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。

イ　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。

7.3.2　情報システムの開発

ア　システム開発における責任者及び作業者の特定

教育情報システム管理者は、システム開発の責任者及び作業者を特定しなければなら

ない。また、システム開発のための規則を確立しなければならない。

イ　システム開発における責任者、作業者のＩＤの管理

（ア）教育情報システム管理者は、システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

（イ）教育情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

ウ　システム開発に用いるハードウェア及びソフトウェアの管理

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

（イ）教育情報システム管理者は、利用を認めたソフトウェアをシステムから削除しなければならない。

7.3.3　情報システムの導入

ア　開発環境から運用環境への移行手順の明確化

（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。

（イ）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。

（ウ）教育情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

イ　テスト

（ア）教育情報システム管理者は、特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。

7.3.4　システム開発・保守に関連する資料等の整備・保管

ア　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。

イ　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。

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

7.3.5　情報システムにおける入出力データの正確性の確保

ア　教育情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当

性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

イ　教育情報システム管理者は、故意又は過失により情報が改ざんされ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。

ウ　教育情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

7.3.6　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。

7.3.7　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。

7.3.8　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。

7.4　不正プログラム対策

7.4.1　教育情報セキュリティ責任者の措置事項

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

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

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

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

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

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

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

キ　業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

7.4.2　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として、次の事項を措置しなければならない。

ア　教育情報システム管理者は、その所掌するサーバ又はパソコン等の端末を守るため、コンピュータウイルス等の不正プログラム対策を講じなければならない。

イ　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。

ウ　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、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。

7.4.3　教職員等の遵守事項

教職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

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

イ　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。

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

エ　コンピュータウイルス等に感染したおそれがある場合は、ＬＡＮケーブルの即時取り外し又は端末の通信機能の停止等、他への感染を防止する措置を講じるとともに、速やかに校内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。

7.4.4　専門家の支援体制

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。

7.5　不正アクセス対策

7.5.1　教育情報セキュリティ責任者の措置事項

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

ア　使用されていないポートを閉鎖しなければならない。

イ　不要なサービスについて、機能を削除又は停止しなければならない。

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

エ　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

7.5.2　攻撃の予告

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、関係機関との連絡を密にして情報の収集に努めなければならない。

7.5.3　記録の保存

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は、サーバ等に攻撃を受け、当該攻撃が犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

7.5.4　内部からの攻撃

教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等及び外部委託事業者が使用しているパソコン等の端末からの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。

7.5.5　教職員等による不正アクセス

教育情報セキュリティ責任者及び教育情報システム管理者は、教職員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の校内教育情報セキュリティ責任者に通知し、適切な処置を求めなければならない。

7.5.6　サービス不能攻撃

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

7.5.7　標的型攻撃

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

7.6　セキュリティ情報の収集

7.6.1　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

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。

7.6.2　不正プログラム等のセキュリティ情報の収集及び周知

教育情報セキュリティ責任者が、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。

7.6.3　情報セキュリティに関する情報の収集及び共有

教育情報セキュリティ責任者及び教育情報システム管理者は、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館教頭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。

8　運用

8.1　情報システムの監視

ア　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。

イ　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。

ウ　教育情報セキュリティ責任者及び教育情報システム管理者は、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。

8.2　教育情報セキュリティポリシーの遵守状況の確認

8.2.1　遵守状況の確認及び対処

ア　教育情報セキュリティ責任者及び校内教育情報セキュリティ責任者は、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、速やかに統括教育情報セキュリティ責任者に報告しなければならない。

イ　統括教育情報セキュリティ責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

ウ　教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における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。

8.2.2　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

教育情報セキュリティ責任者は、不正アクセス、不正プログラム等の調査のために、教職員が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

8.2.3　教職員等の報告義務

ア　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、直ちに校内教育情報セキュリティ責任者に報告を行わなければならない。

イ　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。

8.3　侵害時の対応等

8.3.1　緊急時対応計画の策定

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、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。

8.3.2　緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

ア　関係者の連絡先

イ　発生した事案に係る報告すべき事項

ウ　発生した事案への対応措置

エ　再発防止措置の策定

8.3.3　緊急時対応計画の見直し

統括教育情報セキュリティ責任者は、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。

8.4　例外措置

8.4.1　例外措置の許可

校内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、統括教育情報セキュリティ責任者の許可を得て、例外措置を取ることができる。

8.4.2　緊急時の例外措置

校内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、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。

8.4.3　例外措置の申請書の監理

統括教育情報セキュリティ責任者は、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。

8.5　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、以下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。

ア　教育公務員特例法（昭和 24 年法律第 1 号）
イ　地方公務員法（昭和 25 年法律第 261 号）
ウ　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）
エ　著作権法（昭和 45 年法律第 48 号）
オ　個人情報の保護に関する法律（平成 15 年法律第 57 号）
カ　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）
キ　久御山町個人情報保護条例（平成 13 年 7 月条例第 12 号）

8.6　懲戒処分等

8.6.1　懲戒処分

情報セキュリティポリシー及びこれに基づく文書に違反した教職員等及びその監督責任者は、その重大性、発生した事象の状況等に応じて、地方公務員法による懲戒処分の対象となる。

8.6.2　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。

ア　教育情報セキュリティ責任者は違反を確認した場合は、当該教職員等が所属する学校の校内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。
イ　教育情報システム管理者が違反を確認した場合は、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校内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。
ウ　校内教育情報セキュリティ責任者の指導によっても改善されない場合、教育情報セキュリティ責任者は、当該教職員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、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校内教育情報セキュリティ責任者に通知しなければならない。

9　外部委託

9.1　外部委託

9.1.1　外部委託事業者の選定基準

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。

9.1.2　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、作業者の所属、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及びアクセス方法
・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）

9.1.3　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、安全を確保しなければならない。またその内容を教育情報セキュリティ責任者に報告するとともに、その重要度に応じて、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。

10　クラウドサービスの利用

10.1　クラウドサービスの利用におけるセキュリティ対策

教育情報システム管理者は、利用しようとするクラウドサービスについて、安全性を確認しなければならない。また、重要性分類Ⅱ以上の情報資産については、クラウドサービスを利用しない。

10.2　約款による外部サービスの利用

10.2.1　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扱いには十分に留意するように規定しなければならない。

ア　約款によるサービスを利用してよい範囲
イ　業務により利用する約款による外部サービス

ウ　利用手続及び運用手順

10.2.2　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。

10.3　ソーシャルメディアサービスの利用

10.3.1　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、次の対策を行わなければならない。

（ア）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。

（イ）パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ＩＣカード等）等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

イ　重要性分類Ⅲ以上の情報はソーシャルメディアサービスで発信してはならない。

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。

11　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

11.1　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っては、事業者における個人情報の適切な管理が行われていることが必須であることから、次のプライバシー保護に関する事項について、事業者に確認を行わなければならない。

11.1.1　個人情報の利用範囲

教育・学校の目的に必要な情報、または児童生徒・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。

11.1.2　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。

11.1.3　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。

11.1.4　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、または児童生徒・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。

11.1.5　不適切なポリシー等の変更等の禁止

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。

11.1.6　個人情報の保持期間定義

サービス提供機関（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。

11.1.7　個人情報の利用目的

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

11.1.8　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、契約またはプライバシーポリシーで明確に示すこと。

11.1.9　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。

11.1.10　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。

11.1.11　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、管理するものとすること。

11.1.12　合併/買収

合併また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。

12　評価・見直し

12.1　監査

12.1.1　実施方法

統括教育情報セキュリティ責任者は、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内部監査を行わなければならない。

12.1.2　監査結果への対応

統括教育情報セキュリティ責任者は、内部監査をした場合、その結果を踏まえ、指摘事項を所管する校内教育情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない校内教育情報セキュリティ責任者に対しても、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。

12.1.3　教育情報セキュリティポリシーの見直し等への活用

統括教育情報セキュリティ責任者は、監査結果を教育情報セキュリティポリシーの見直し時に活用しなければならない。

12.2 自己点検

12.2.1　実施方法

ア　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。

イ　教育情報セキュリティ責任者は、校内教育情報セキュリティ責任者と連携して、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。

12.2.2　報告

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、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。

12.2.3　自己点検結果の活用

ア　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。

イ　統括教育情報セキュリティ責任者は、この点検結果を教育情報セキュリティポリシー等の見直し時に活用しなければならない。

12.2.4　教育情報セキュリティポリシーの見直し

統括教育情報セキュリティ責任者は、内部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ふまえ、教育情報セキュリティポリシーについて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。