令和8年第5回加賀市教育委員会定例会の議件を次のとおり提出する。

令和8年5月26日

加賀市教育委員会

教育長　松　本　向　貴

1　審議事項

議案第31号　令和8年度6月補正予算（案）について

議案第32号　学校施設の在り方の検討について

2　報告事項

報告第19号　加賀市における教育情報セキュリティポリシーの改訂について

報告第20号　山中図書館の空調工事に伴う対応について

3　その他

○ 加賀温泉郷ウオークの開催結果について

議案第 31 号　令和 8 年度 6 月補正予算（案）について

議案第 32 号　学校施設の在り方の検討について

市議会令和 8 年 6 月定例会に上程または公表前の内容であり、非公開で審議するものであります。

審議事項、報告案件、その他が終了した後、傍聴者の退席を確認後、審議をお願いいたします。

報告第19号

加賀市における教育情報セキュリティポリシーの改訂について

1　改訂の経緯

令和６年度末に加賀市教育委員会において教育情報セキュリティポリシーを策定したが、その後、令和７年３月に文部科学省の「教育情報セキュリティポリシーに関するガイドライン」が改訂された。同ガイドラインでは、「次世代校務 DX 環境」の構築を見据え、校務系・学習系ネットワークを統合し、情報資産をクラウド環境で管理するとともに、アクセス権限を厳格に管理することを基本的な方向性としている。

加賀市教育委員会としても、サーバ更新等の環境の変化を踏まえ、より安全性の高い情報管理体制を構築するため、教育情報セキュリティポリシーの改訂を行った。あわせて、学校現場の実態に即した内容への見直し、文言整理、文書体系の整理等も実施した。

2　主な改訂内容

（1）文部科学省ガイドライン改訂への対応

令和７年３月の文部科学省ガイドライン改訂に合わせ、「誰がアクセスできるか」というアクセス主体に基づく分類へ変更を行った。

（2）次世代校務 DX 環境の構築を見据えた変更

校務系ネットワークと学習系ネットワークの統合を可能とするとともに、校務データをクラウド環境に保存することを前提とした運用へ見直しを行った。

（3）児童生徒性暴力等防止に係る規定の反映

令和７年９月に教職員へ周知した「児童生徒性暴力等の防止に向けたセキュリティポリシーの運用について」に基づき、スマートフォンの取扱い等に関する規定を反映した。

（緊急時を除き、職員室外でのスマートフォン利用を禁止する等の規定を追加）

（4）学校現場の実態に合わせた見直し

デジタルカメラの管理方法など、現在の学校運用に即した内容へ見直した。

（5）文書体系の見直し

「加賀市立学校情報セキュリティ対策基準」、「同運用マニュアル」、「同実施手順」の３本立てだった文書を「加賀市立学校情報セキュリティ対策基準」への一本化を行った。

（6）文言整理

誤字脱字の修正および表現の整理を行った。

3　改訂時期

本改訂は令和８年５月１日をもって施行する。

加賀市立学校情報セキュリティ対策基準

加賀市教育委員会

【令和８年５月１日　改訂版】

	改訂履歴
初　版	平成 19 年 10 月 1 日
改訂 1	令和 7 年 4 月 1 日
改定 2	令和 8 年 5 月 1 日

目次

１．目的・趣旨

１．１ 目的

本「加賀市立学校情報セキュリティ対策基準」は、加賀市教育委員会（以下「教育委員会」という。）が所管する小中学校及び義務教育学校（以下「学校」という。）において、「加賀市情報セキュリティに関する規程(令和３年４月30日訓令・教育委員会訓令・ 選挙管理委員会訓令・監査委員訓令・ 公平委員会訓令・農業委員会訓令・ 固定資産評価審査委員会訓令・病院事業訓令・消防本部訓令・ 議会訓令第１号、以下「規程」という。）」を実行に移す上で守るべき統一的な基準を示すものとする。

１．２ 趣旨

学校教育の情報化の進展により、児童生徒及びその保護者等の個人情報を含む情報資産は一層の適切な管理・運用が求められている。さらに、学校のＩＣＴ環境は、文部科学省が打ち出したＧＩＧＡスクール構想に基づく一人１台端末の整備やクラウドサービス本格活用等の進展により、大きく変化しつつある。

文部科学省が「教育情報セキュリティポリシーに関するガイドライン」を初めて示したのは平成29年10月であるが、学校のＩＣＴ環境の変化に伴い改訂が続けられており、今後も情報セキュリティ対策の動向や技術的な進展等を踏まえ改訂されることが予想される。

教育委員会においても、規程で定められた基本方針に基づきつつ、安全かつ適切な情報管理を継続するため、個々の対策を具体化した本対策基準を作成するとともに、文部科学省の最新ガイドラインに準拠した情報セキュリティ対策を盛り込むよう今後も随時改訂し、対応していくものとする。

２．教育情報セキュリティポリシーの構成と文書体系

２．１ 構成

文部科学省がガイドラインを示している「教育情報セキュリティポリシー」は、教育委員会や学校等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り、該当する情報資産を取り扱う全教職員等に浸透、定着させるためにも、安定した統一的な規範であることが求められる。

一方、情報処理・通信技術の進歩等による急速な環境の変化に柔軟に対応することも必要となることから、本市の教育情報セキュリティポリシーは、一定の長期にわたり不変的な部分と

して統一的な規範を定めた「基本方針」に当たる規程と、情報資産を取り巻く環境の変化に柔軟に対応する指針となる「対策基準」の２部構成で策定している。

２．２ 文書体系

教育情報セキュリティポリシーの文書体系は次の通りとなる。

文書名	内容
加賀市情報セキュリティに関する規程	セキュリティ対策の目的や基本方針を定めた統一的な規範で、訓令及び教育委員会訓令等により制定されている。学校のみならず、加賀市の機関全体に適用される。
加賀市立学校情報セキュリティ対策基準	学校にある情報を脅威から守るため、具体的な対策の基準を示したもの。

３．用語の定義

本対策基準において用いる用語の定義は、当該各号に定めるところによる。

(1)　情報セキュリティ

情報資産の機密性、完全性及び可用性が維持されていることをいう。

(2)　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ことで、情報の漏洩が防止されている状態をいう。

(3)　完全性

情報の破壊、改ざん、消去等による被害が防止されている状態をいう。

(4)　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いう。

(5)　加賀市における教育情報セキュリティポリシー

「加賀市情報セキュリティに関する規程」と「加賀市立学校情報セキュリティ対策基準」を合わせたものを指す。

(6)　教職員等

臨時的任用教職員、非常勤講師等を含めた教職員全員を、教職員等と称する。教職員等は学校が所管する情報資産を取り扱う立場にあり、校内教育情報セキュリティ責任者の監督、及び校内教育情報セキュリティ管理者の指導の下、情報セキュリティを遵守しなければならない。

(7)　教育委員会事務局職員

教育ネットワークを利用して、学校が所管する情報にアクセスできる教育委員会事務局職員を指す。教育委員会事務局職員は学校の情報資産にアクセスできる立場にあるため、学校情報セキュリティ責任者の監督・指導の下、情報セキュリティを遵守しなければならない。

(8)　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。

(9)　情報システム

コンピュータ（ハードウェア及びソフトウェア）及びネットワーク、並びに電磁的記録媒体から構成され、情報処理を行う仕組みをいう。

(10)　情報資産

当該教育情報セキュリティポリシーにおいて対象とする情報資産は、次のものをいう。

1　学校において使用するすべてのネットワーク及び情報システム並びにこれらに関連する設備

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や動画等を含む。）

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

(11) 学校情報

電磁的に記録された学校事務の執行に関わる情報をいう。

(12) 学習情報

児童生徒のワークシート、作品等、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、生徒指導等に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をいう。

(13) 校務情報

児童生徒の成績、出欠及びその理由、健康診断結果、指導要録、教職員の個人情報等、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、生徒指導等に活用することを想定しており、かつ当該情報に児童生徒がアクセスすることが想定されていない情報をいう。

(14) 学習系ネットワーク

インターネットに接続可能な、授業に用いる各教室等のネットワークと一人１台端末で学習に用いるネットワークをいう。

(15) 校務系ネットワーク

インターネットに接続可能な校務処理に用いるネットワークをいう。

(16) 教育ネットワーク

学習系システム及び校務系システムが利用するネットワークをいう。強固なアクセス制御による対策を採用する場合は、物理的に統合されたネットワークとすることができる。この場合、（１４）及び（１５）の各ネットワークは論理的なセグメントとして取り扱うことが望ましい。

(17) 学習系システム

学習系ネットワーク、学習用サーバー（クラウド含む）、及び学習者用端末から構成される学習情報を取り扱うシステム、並びに学習情報を扱ううえで、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をいう。

(18) 校務系システム

校務系ネットワーク、校務用サーバー（クラウド含む）、及び校務用端末から構成される校務情報を取り扱うシステム、並びに校務情報を主に取り扱ううえで、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をいう。

(19) 教育情報システム

学習系システム及び校務系システムを合わせた総称を指す。

(20) サーバー

ネットワーク上で学校情報を処理し、端末機に提供するコンピュータをいう。

(21) 端末機

ネットワークを通じてサーバーに接続された端末をいう。

(22) 外部記録媒体

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）をいう。ハードディスク、ＵＳＢメモリ等。

(23) ＮＡＳ

ネットワークに直接接続して使用するファイルを保存するサーバー。ネットワークに接続している複数のデバイスから同時にアクセスが可能な外部記録媒体をいう。なお、ＮＡＳの新規設置は原則禁止とし、既存のＮＡＳは段階的に廃止する。複合機のスキャナー保存先として一時的に利用する場合は、学校情報システム責任者の許可を得るものとする。

(24) 一人１台端末

文部科学省が 2019 年に打ち出したＧＩＧＡスクール構想で導入され、教育委員会が児

童生徒に貸与している学習者用端末をいう。

(25) 無線ＬＡＮ

電波等を利用してデータの送受信を行う校内通信網システムをいう。

(26) 情報セキュリティインシデント

コンピュータシステムやネットワークに対する攻撃及び不正アクセス等、情報の機密性や完全性、可用性を脅かす出来事をいう。（マルウェア感染やデータ漏洩、サイバー攻撃等）

(27) ソーシャルネットワークサービス

インターネット上で展開される情報メディアサービスで、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通等といった社会的な要素を含んだプラットホームのことをいう。

(28) 標的型攻撃

明確な意思と目的を持ち、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をいう。

(29) 外部サービス

事業者等の教育委員会外の組織で、情報システムの一部又は全部の機能を提供する者をいう。外部サービスを利用して自組織に向けて独自のサービスを提供する事業者は含まない。

(30) 外部サービス利用者

外部サービスを利用する教職員等又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう。

４．学校情報セキュリティ組織体制

学校情報セキュリティの管理体制は、次に掲げる通りとする。

(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。学校における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関する統括的な権限及び責任を有する。

統括教育情報セキュリティ責任者は、緊急時には最高情報セキュリティ責任者(Chief Information Security Officer。略称で CISO。)に直ちに報告を行うとともに、情報資産等の回復のための対策を講じなければならない。

(2)　学校情報セキュリティ責任者

教育委員会学校指導課長を学校情報セキュリティ責任者とする。学校における情報資産に対する侵害が発生した場合、又は侵害の恐れがある場合には必要かつ十分な措置を行う権限及び責任を有する。

(3)　学校情報システム責任者

教育委員会教育庶務課長を学校情報システム責任者とする。所管する教育情報システムにおける情報セキュリティの保全に努める。また、全校に渡る外部サービスにおける契約、設定の変更、運用、見直し及び情報セキュリティ対策を行う権限及び責任を有する。

(4)　校内教育情報セキュリティ責任者

学校における各校長を各学校の校内教育情報セキュリティ責任者とする。当該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権限及び責任を有する。

また、所属の教職員から校内教育情報セキュリティ管理者を 1 名選任して学校情報セキュリティ責任者に報告する。

(5)　校内教育情報セキュリティ管理者

学校において校内教育情報セキュリティ管理者を各校１名選任し、校内教育情報セキュリティ責任者を補佐するとともに、所属する教職員の情報セキュリティ対策の実施について、管理、指導を行いつつ、教育情報セキュリティポリシーの周知及び啓発に努める。

(6)　校内教育情報システム管理者

学校における各情報システムの管理、運用に携わる担当者として、校内教育情報システム管理者を各校１名選任し、校内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管理者と協力して、校内教育情報セキュリティの保全に努める。

(7)　セキュリティ事案連絡・相談窓口との連携

学校情報セキュリティ責任者は、教育委員会学校指導課内にセキュリティ事案連絡・相談窓口を設置する。各学校等において、情報資産に対する侵害、または侵害の恐れがある事案が発生した場合には、当該事案を正確に把握したうえで、セキュリティ事案連絡・相談窓口に報告させ、学校情報システム責任者、校内教育情報セキュリティ責任者と連携を図る。

(8)　学校の外部サービス管理者

学校情報システム責任者を学校の外部サービス管理者とする。所管する外部サービスにおける契約、設定の変更、運用、見直し及び情報セキュリティ対策を行う権限及び責任を有する。

５．情報資産の分類と管理

５．１ 情報資産の分類

情報資産の保護の必要性及びアクセス主体に基づき、下表の通り、重要性の分類を定める。

重要性分類	定義	アクセス主体
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と想定される情報資産	学校長、教務主任等の特定職務者に限定
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と想定される情報資産	特定の部局・学年団内の教職員に限定
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資産	全教職員がアクセス可能
Ⅳ	ほとんど影響を及ぼさない情報資産。上記のⅠ、Ⅱ、Ⅲ以外	教職員及び児童生徒がアクセス可能

※各重要性分類に対して、アクセス可能な主体を明確にし、クラウドストレージ上でのアクセス権限設定に反映する。
※業務で取り扱う情報資産は、作成、入手、利用、保管、廃棄等の各局面で、上記の重要性分類を踏まえた管理としなければならない。
※情報資産分類及び例示については別表１を参照。情報資産の機密性、完全性、及び可用性確保の重要度に応じ、総合的に判断した上で分類している。

５．２ 情報資産の管理

(1)　管理責任

1　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。

2　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「５．１」の分類に基づき管理しなければならない。

3　校内教育情報セキュリティ責任者は、別表１に示した情報資産分類及び例示に基づき、自校向け情報資産台帳を整備することが望ましい。

(2)　情報資産分類の確認及び表示

教職員等は、情報資産について、その分類を確認し、必要に応じて重要性分類を表示する等適切な管理を行わなければならない。

※情報資産の分類の表示先ファイルの例

ファイル（ファイル名、ファイル属性・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等

(3)　情報資産の作成

1　教職員等は、業務上必要のない情報資産を作成してはならない。

2　情報資産を作成する者は、情報資産の作成後に、「５．１」の分類に基づき管理しなければならない。

3　情報資産を作成する者は、作成途上の情報についても、紛失や流失等を防止しなければならない。また、情報資産の作成途上で不要になった場合は、当該情報資産を消去しなければならない。

(4)　情報資産の入手

1　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「５．１」の分類に基づいた取り扱いをしなければならない。

2　学校外の者が作成した情報資産を入手した者は、「５．１」の分類に基づき、当該情報資産を管理しなければならない。

3　情報資産を入手した者は、その情報資産の分類が不明な場合、校内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

1　情報資産を利用する者は、業務以外の目的で情報資産を利用してはならない。

2　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。

(6)　情報資産の保管

1　校内教育情報セキュリティ責任者は、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。

2　校内教育情報セキュリティ責任者は、情報資産を記録した外部記録媒体を保管する場合、施錠可能な場所に保管しなければならない。

(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ー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際、重要性分類Ⅲ以上の情報を扱う場合は、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。

(8)　情報資産の提供・公表

1　重要性分類Ⅲ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を行わなければならない。

2　校内教育情報セキュリティ責任者は、保護者等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。

(9)　情報資産の廃棄

1　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内蔵及び外部記録媒体が不要になった場合、当該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。

2　情報資産の廃棄を行う者は、情報を記録している内蔵及び外部記録媒体の廃棄を行う場合、情報資産の性質に応じ、学校情報セキュリティ責任者又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。

(10)　情報システムの強靭性向上

学校情報システム責任者は、重要性分類Ⅱ以上の情報資産について、アクセスを許可された教職員が該当情報資産を不正に外部持ち出ししたり、悪意のある関係者がなりすまし行為を行ったりすることを防ぐため、情報システムをインターネットで接続系システムからネットワーク分離する形や、強固なアクセス制御、例えば利用者認証や端末認証等の安全管理措置を講じなければならない。

６．物理的セキュリティ対策

６．１ コンピュータ教室及び準備室の管理

(1)　コンピュータ教室及び準備室の構造等

1　コンピュータ教室及び準備室から外部に通ずるドアは必要最小限にし、施錠設備等によって許可されていない者の立ち入りを防止しなければならない。また、施錠設備に関連する鍵等は適正に管理しなければならない。

2　コンピュータ教室及び準備室内に設置する機器等については、転倒及び落下防止等の耐震対策、防火措置等を講じなければならない。

3　コンピュータ教室及び準備室内には、温度及び湿度を適正に保つための空気調節設備を設置しなければならない。

(2)　コンピュータ教室及び準備室の入退室管理等

1　コンピュータ教室及び準備室への入退室は、教職員等（教育委員会事務局職員を含む）及び許可された児童生徒、保護者、外部委託業者のみに制限しなければならない。

2　外部委託事業者がコンピュータ教室へ入室する場合は、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。また、併せて名札その他の身分証明書等を着用しなければならない。

3　コンピュータ教室内への機器等の搬入時は、教職員等の同行、立ち合いを行い、事故等のないようにしなければならない。

６．２ 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及び学校情報システム責任者は、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、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。また、将来的には、無線化の措置も考慮することが望ましい。

(2)　統括教育情報セキュリティ責任者及び学校情報システム責任者は、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学校情報システム責任者は、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学校情報システム責任者は、自ら又は教育情報システムの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)　統括教育情報セキュリティ責任者及び学校情報システム責任者は、ネットワーク機器間を接続する通信ケーブルに、接続先機器を明示するよう外部委託事業者等に指示しなければならない。

(6)　統括教育情報セキュリティ責任者及び学校情報システム責任者は、外部委託事業者に、ネットワーク機器の設置場所、接続口（ハブのポート等）、機器用ＩＰアドレス、配線経路等を示す資料を作成するよう指示し、作成された資料を保管しなければならない。

(7)　学校情報システム責任者は、剥き出しとなっているケーブルについて、用途調査を行い、利用中のケーブルは配管等に収納するなどの措置を取り、不要なケーブルは撤去しなければならない。

６．３ 外部記録媒体の管理

(1)　USB メモリ、SD カード、外付けハードディスク等の外部記録媒体は、施錠可能

な場所に保管する等の盗難防止対策を講じなければならない。

(2) 重要性分類Ⅱ以上の学校情報等が記録された外部記録媒体は、耐火機能を有する保管庫に保管する等、その内容が確実に復元できる対策を講じなければならない。

(3) 外部記録媒体を外部機関と交換する場合は、適切な盗難防止策を講じるとともに、その履歴を残さなければならない。

６．４ 教職員等が利用する端末の管理

(1) 学校情報システム責任者は、不正アクセス防止のため、ログイン時のＩＤ及びパスワードによる認証等使用する目的に応じた適切な措置を講じなければならない。内蔵及び外部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) 学校情報システム責任者は、教育情報システムへアクセスする端末について、以下のセキュリティ設定を施さなければならない。

1 ログイン時のパスワード入力を必須とすること。

2 一定時間無操作の状態が続いた場合に自動的に画面ロック及びスリープ状態に移行する設定を行うこと。

(3) 学校情報システム責任者は、重要性分類Ⅱ以上の情報資産を取り扱う場合、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。

６．５ その他の機器の管理

(1) 校務用端末は盗難防止のため、原則として、端末を配備された職員室や保健室・図書室等から持ち出さない環境に置くとともに、職員室や保健室・図書室等に教職員が不在の際は部屋の施錠を徹底するものとする。

(2) ネットワーク機器及びその他の機器については、不可抗力による損傷、破損又は意図的な情報の傍受等を防止するため、必要な措置を講じるよう努めなければならない。

7．人的セキュリティ対策

7．1 教職員等の遵守事項

(1)　加賀市における教育情報セキュリティポリシーの遵守

教職員等は、情報セキュリティの重要性を認識し、加賀市における教育情報セキュリティポリシーに従い、情報資産を適正に扱わなければならない。

(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。

また、校内教育情報セキュリティ管理者は、所属する教職員等に対し、業務以外の目的でのインターネットへのアクセスを行わないよう指導し、適切に利用させなければならない。

(3)　情報資産の持ち出しの制限

教職員等は、端末機（一人１台端末を除く）、外部記録媒体、その他の情報資産を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。

(4)　端末機等の持ち込み等の制限

1　教職員等は、持ち込んだ私物端末を業務に使用する場合は、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。

2　教職員等は、私物端末に個人情報を含む業務情報を記録してはならない。

3　教職員等は、いかなる場合においても、私物端末（スマートフォン、タブレット、カメラ等）を使用して児童生徒を撮影（写真・動画を問わず）してはならない。児童生徒の撮影は、公的に配備された端末機を使用するものとする。

4　教職員等は、公的に配備された端末機に記録した児童生徒の画像・動画を学校外に持ち出す場合は、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　教職員等は、私物のスマートフォンを職員室外で使用する場合は、緊急連絡の用途

に限定し、児童生徒に見せてはならない。

(5)　机上の端末機等の管理

教職員等は、端末機や外部記録媒体、印刷された文書について、第三者に使用、閲覧等されることのない場所へ保管する等適切な措置を講じなければならない。

(6)　ソフトウェアの無断導入等について

1　教職員等は、原則として端末機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学校情報システム責任者の許可　　を得た時に限り、ソフトウェアを導入することができる。

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。

(7)　機器構成の変更の制限

教職員等は、端末機等に対し、機器の改造及び増設・交換を行ってはならない。

1　教職員等は、業務上、端末機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、学校情報システム責任者の許可を得なければならない。

2　学校情報システム責任者は、端末機等に対し、機器の改造、増設、交換等を行う場合、想定されるリスクを考え、その対策を講じたうえで構成の変更を行わなければならない。

(8)　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、個人情報の扱い上の必要がある場合においては、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、電子メールの送信等により情報資産を無断で外部に持ち出してはならない。

5　教職員等は、電子メールで送るデータの機密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の方法を使用して、送信しなければならない。

(9)　無許可でのネットワーク接続の禁止

教職員等は、許可されていない端末機を学校情報システム責任者の許可なくネットワークに接続してはならない。

(10)　業務以外の目的でのインターネット閲覧の禁止

1　教職員等は、業務以外の目的でインターネットを閲覧してはならない。

2　出所が不明なファイルや内容に確証の得られていないファイル等は、展開してはならない。

3　校内教育情報セキュリティ責任者は、教職員等が業務以外の目的でインターネットを閲覧していることが疑わしい又は判明した場合、当該教職員等への注意、指導を行わなければならない。

4　校内教育情報セキュリティ責任者は、教職員等のインターネット利用について、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速やかにインターネット利用の停止等必要な措置を講じなければならない。

7．2 研修

(1)　学校情報セキュリティ責任者は、学校の教職員等に対し、情報セキュリティの重要性や加賀市における教育情報セキュリティポリシーに係る研修を定期的に実施しなければならない。

(2)　校内教育情報セキュリティ責任者は、利用する情報資産に関する情報セキュリティの理解を高めるため、所属する教職員等に対し、研修を定期的に実施することが望ましい。

7．3 侵害（事故、欠陥等を含む）の報告

(1)　侵害等の報告

1　教職員等は、情報セキュリティに関する侵害（システム上の欠陥及び誤作動等を含

む）を発見した場合、速やかに校内教育情報セキュリティ責任者を通じて学校情報システム責任者に報告しなければならない。

2　学校情報システム責任者は、当該事故等による情報セキュリティの侵害の程度に応じて速やかに学校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に報告しなければならない。

(2)　侵害等の分析、記録等

侵害等のあった学校においては、学校情報システム責任者が、校内教育情報システム責任者と連携し、侵害等の原因を分析し、原因と再発防止策等の記録を作成し、学校情報セキュリティ責任者に提出しなければならない。

7．4 ＩＤ及びパスワード等の管理

(1)　　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（共通アカウント）は原則として使用を禁止する。すべての教職員等について個別のＩＤを付与するものとする。

(2)　　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　パスワードは秘密にし、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　パスワードが流失した恐れがある場合には、校内教育情報セキュリティ責任者を通じ、学校情報システム責任者に速やかに報告し、パスワードを変更しなければならない。

5　仮のパスワード（初期パスワードを含む）は、最初のログイン時に変更することを

推奨する。ただし、システムにより自動的にパスワード変更が求められる場合はこの限りではない。

6　教職員間であってもパスワードを共有してはならない。

8．技術的セキュリティ対策

8．1 サーバー及びネットワークの管理

(1)　クラウドストレージの設定

1　学校情報システム責任者は、教職員等が使用できるクラウドストレージの容量及び利用範囲を設定し、教職員等に周知しなければならない。

2　学校情報システム責任者は、クラウドストレージのアクセス権限を学校及び組織の単位で構成し、教職員等が権限のない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。

（附則）オンプレミスのファイル共有サーバーについては、学校情報システム責任者が廃止を決定するまでの間、従前の運用を継続することができる。ただし、新規ファイルの保存はクラウドストレージへの移行を優先すること。

(2)　バックアップの実施

学校情報システム責任者は、所管するサーバー等（校内サーバーを除く）に記録された情報について、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。

(3)　情報システム仕様書等の管理

学校情報システム責任者は、所管する情報システムのネットワーク構成図、情報システム仕様書等について、外部記録媒体に関わらず、業務上必要とする者以外が閲覧したり、紛失等がないよう適切に管理しなければならない。

(4)　ログの取得等

1　学校情報システム責任者は、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　学校情報システム責任者は、ログとして取得する項目、保存期間、取り扱い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。

(5)　障害記録

学校情報システム責任者は、教職員等からのシステム障害の連絡、システム障害に対する処置結果及び再発防止策等を障害記録として記録し、一定の期間保存しなければならない。

(6)　ネットワークの接続制御、経路制御等

1　学校情報システム責任者は、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　学校情報システム責任者は、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)　外部ネットワークとの接続制限等

1　学校情報システム責任者は、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、教育委員会内及び市内小中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。

2　学校情報システム責任者は、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。

3　学校情報システム責任者は、ウェブサーバー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、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うえで接続しなければならない。

4　学校情報システム責任者は、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、学校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。

(8)　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　学校情報システム責任者は、インターネットを介した外部からのリスク及び児童生徒による重要性が高い情報へのアクセスリスクに対応するため、統合されたネットワークにおいて、多要素認証を含む強固なアクセス制御を講じたシステム構成を採用しなければならない。また、利用者認証・端末認証・アクセス権管理の徹底により、校務系システム及び学習系システムが取り扱う情報へのアクセスを論理的に分離することが望ましい。

2　学校情報システム責任者は、利用者認証、端末認証、ログ監視、リスクベース認証等により、不正アクセスを防止する措置を講じるものとする。

(9)　電子メールのセキュリティ管理

学校情報システム責任者の設定及び制御によるものとする。

8．2 アクセス制御等

(1)　アクセス制御

1　学校情報システム責任者は、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　強固なアクセス制御による対策を採用する場合、学校情報システム責任者は、重要性分類Ⅱ以上の情報資産を取り扱うシステムに対して、以下の措置を講じなければならない。

(1) 多要素認証（パスワードに加え、生体認証又はワンタイムパスワード、証明書による所持等）の導入

(2) 端末認証（アクセス元端末の登録・認可及びセキュリティ状態の確認）

(3) ロールベースのアクセス権管理（利用者の職務に基づくアクセス権付与）

(4) リスクベース認証（アクセスの時間帯・場所・パターン等に基づく動的な認証強化）

(5) すべてのアクセスの記録及び異常検知

(2) 利用者ＩＤの取り扱い

1 学校情報システム責任者は、利用者の登録、変更、抹消等の情報管理、教職員等の異動、退職等に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

2 利用されていないIDが放置されないように教育委員会教育庶務課等と連携し、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

(1) 学校情報システム責任者は、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) 特権を付与されたIDにて外部委託業者が作業を行う場合、学校情報システム責任者による許可を必要とし、学校システム責任者は、作業内容の確認を行わなければならない。

(3) 学校情報システム責任者は、特権を付与されたID及びパスワードについては、定期的な変更又は入力回数制限等により、特にセキュリティ機能を強化しなければならない。

(3) パスワードに関する情報の管理

1 学校情報システム責任者は、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。各情報システムにおいて、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 学校情報システム責任者は、教職員等に対してパスワードを発行する場合、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。

(4)　特権による接続の制限

学校情報システム責任者は、特権によるネットワーク及び情報システムへの接続を必要最小限にしなければならない。

(5)　クラウド認証基盤の利用

1　学校情報システム責任者は、教職員等及び児童生徒のユーザー認証を、クラウドベースの統合認証基盤により管理しなければならない。

2　オンプレミスの認証基盤（Active Directory 等）は段階的に廃止し、クラウド認証基盤への移行を完了させるものとする。

3　クラウド認証基盤においては、多要素認証を有効化することが望ましい。

８．３ システム開発、導入、保守等

(1)　情報システムの調達

1　学校情報システム責任者は、情報システム開発、導入、保守、運用等の調達に当たって、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　学校情報システム責任者は、機器及びソフトウェアの調達に当たって、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。

3　学校情報システム責任者は、システム開発、導入、保守、運用等のそれぞれの調達に当たって、調達仕様書における要件定義を明確にすることにより、解釈の違いによる情報セキュリティの漏れが発生しないよう努めなければならない。

(2)　情報システムの開発

1　学校情報システム責任者は、システム開発の責任者及び作業者を特定し、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

(1) 学校情報システム責任者は、システム開発の責任者及び作業者が使用するＩ

Ｄ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。

(2) 学校情報システム責任者は、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

(1) 学校情報システム責任者は、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。

(2) 学校情報システム責任者は、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

(1) 学校情報システム責任者は、システム開発、テスト環境とシステム稼働後の環境を分離しなければならない。

(2) 学校情報システム責任者は、システム開発及びテスト環境からシステム稼働後の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するとともに、保守の内容についても明確にしなければならない。

(3) 学校情報システム責任者は、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。

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

2　テスト

(1) 学校情報システム責任者は、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。

(2) 学校情報システム責任者は、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。

(3) 学校情報システム責任者は、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。

(4) 学校情報システム責任者は、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。

(5) 学校情報システム責任者は、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・保守に関する資料等の整備・保管

1　学校情報システム責任者は、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　学校情報システム責任者は、テスト結果を一定期間保管しなければならない。

3　学校情報システム責任者は、情報システムを導入する場合、システムの設計や導入環境を記録した資料を取りまとめた「完成図書」を作成しなければならない。外部に委託する場合は、事業者により作成された「完成図書」の内容を確認した上で管理、保管しなければならない。

4　機器導入においては、明細、納品状況写真、設定情報等、ソフトウェア　の導入においても、バージョン、利用機能の要件、設定情報等の図書の作成が望ましい。

5　学校情報システム責任者は、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　学校情報システム責任者は、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　学校情報システム責任者は、故意又は過失により情報が改ざんされる又は漏洩する恐れがある場合に、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　学校情報システム責任者は、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

学校情報システム責任者は、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

学校情報システム責任者は、開発・保守用のソフトウェア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

学校情報システム責任者は、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。

8．4 不正プログラム対策

(1)　不正プログラム対策

1　学校情報システム責任者は、外部ネットワークからの不正プログラムによるコンピュータウイルス感染等を防止するため、不正プログラム対策ソフトウェアの導入等の措置を講じなければならない。また、内部ネットワークから外部ネットワークへの接続時は同様のチェックを行い、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。

2　学校情報システム責任者は、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。

3　学校情報システム責任者は、不正プログラム対策ソフトウェアを常に最新の状態に保たなければならない。

4　不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、学校情報システム責任者が許可した教職員を除く教職員等に当該権限を付与してはならない。

5　業務で利用するソフトウェアは、プログラム更新やバージョンアップ等の開発元のサポートが終了していないソフトウェアを利用するよう努めなければならない。

(2)　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　端末機等において、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　コンピュータウイルス等の不正プログラムに感染又は検知した場合は、下記の手順で情報セキュリティの確保を行わなければならない。

(1) 速やかに校内教育情報システム管理者に報告する。

(2) 校内教育情報システム管理者は速やかに学校情報システム責任者に連絡し対処方法を仰ぐとともに、校内教育情報セキュリティ責任者に報告する。

(3) 学校情報システム責任者は、ＬＡＮケーブルの即時取り外し等の対策について速やかに決定し、校内教育情報システム管理者に連絡するとともに、学校情報セキュリティ責任者に報告する。

(4) 学校情報システム責任者は、一連のインシデントへの対応について、報告書にまとめ、統括教育情報セキュリティ責任者を含めたセキュリティ関係者に報告する。

(5) 学校情報システム責任者は、インシデントへの対応後、インシデントへの対応方法の検証及び同一のインシデントが極力起きないようにする方策の検討に努める。

８．５ 不正アクセス対策

(1)　不正アクセス対策

1　学校情報システム責任者は、外部ネットワークからの不正アクセスによる侵入等を防止するため、不正アクセス対策ソフトウェアの導入等の措置を講じなければならない。

2　学校情報システム責任者は、不正アクセス対策ソフトウェアのパターンファイルを常に最新の状態に保たなければならない。

3　学校情報システム責任者は、内部ネットワーク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くてならない。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。

4　学校情報システム責任者は、不正アクセスによる攻撃を受けた場合、使用されていないポート及びＳＳＩＤ（無線ＬＡＮネットワーク名）を直ちに閉鎖しなければならない。

5　学校情報システム責任者は、不正アクセスによる攻撃を受けた場合、不要なサービスについて、直ちに機能を削除又は停止しなければならない。

6　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、データの書き換えを検出し、学校情報システム責任者へ通報するよう設定することが望ましい。

7　学校情報システム責任者は、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。

学校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を連携し、監視、通知、外部連絡窓口及び適切な対応等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

統括教育情報セキュリティ責任者は、サーバー等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

(3)　サービス不能攻撃

学校情報システム責任者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、

情報システムの可用性を確保する対策を講じなければならない。

(4)　標的型攻撃

学校情報システム責任者は、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、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、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。

(5)　記録の保存

学校情報システム責任者は、内部ネットワーク等の攻撃を受け、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。

(6)　内部からの攻撃監視

学校情報システム責任者は、教職員等が使用している端末機等からの所管するネットワークのサーバー等に対する攻撃や外部に対する攻撃を監視しなければならない。

８．６ セキュリティ情報の収集

(1) 学校情報システム責任者は、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

学校情報システム責任者は、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、対応方法を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

学校情報システム責任者は、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。

(4)　ＯＳアップデート等の適用管理

1　学校情報システム責任者は、校務用端末及び学習用端末のＯＳアップデート・セキュリティパッチの適用状況をリモートで一元管理し、定期的に適用状況を確認しなければならない。

2　学校情報システム責任者は、ＯＳアップデートが一定期間以上実施されていない端末を検出した場合、当該端末の利用者・所属校の校内教育情報セキュリティ責任者及び校内教育情報システム管理者に対象リストを通知し、アップデートの実施を指導しなければならない。

９．運用

９．１ 情報システムの監視

(1) 学校情報セキュリティ責任者及び学校情報システム責任者は、不正プログラム、不正アクセス等による情報システムへの攻撃、侵入等を防止するため、サーバー監視等により情報システムの稼働状況について監視を行う等の措置を講じるよう努めなければならない。

(2)　学校情報セキュリティ責任者及び学校情報システム責任者は、不正プログラム、不正アクセス等のアクセスログ等を取得するサーバー等について、アクセスログの正確性を担保するため、正確な時刻設定及びサーバー間の時刻同期ができる措置を講じなければならない。

９．２ 個人情報等を取り扱うネットワーク等

教職員等は、別表１の情報資産分類及び例示の通り、個人情報等を適切に取り扱わなければならない。

９．３ 外部記録媒体の使用の制限

(1)　外部記録媒体の使用

外部記録媒体は、原則として公費で購入したものを使用し、私物の外部記録媒体は使用してはならない。

(2)　ＵＳＢメモリの使用の制限

教育内部系（校務用）端末機においては、上記（１）のほかに学校情報セキュリティ責任者と学校情報システム責任者が使用を認めた学校の管理職及び教職員以外はＵＳＢメモリを使用してはならない。

(3)　ＳＤカードの使用の制限

ＳＤカードを端末機に接続した場合は、データ読み取り以外に使用してはならない。

(4)　外付けハードディスクの利用の制限

校務用端末機及び学習用端末機においては、学校情報システム責任者が使用を認めた学校の管理職以外は外付けハードディスクを使用してはならない。

(5)　端末機内蔵のＤＶＤドライブの使用の制限

校務用端末機及び学習用端末機にＤＶＤドライブが内蔵されている場合は、データの読み取り以外に使用してはならない。

９．４ データ保存場所

校務用端末機及び学習用端末機のデータは、教育委員会が指定したクラウドストレージに保存しなければならない。端末機のローカルストレージへの業務データの保存は極力行わない。

９．５ インターネットの閲覧

校務用端末機及び学習用端末においては、学校情報システム責任者が必要と認めた場合以外は閲覧制限を解除してはならない。

９．６ 侵害（事故、欠陥等を含む）時の対応

学校情報セキュリティ責任者は、情報セキュリティに関する事故や障害又は加賀市における教育情報セキュリティポリシーの違反等により情報資産への侵害が発生した場合又は発生する恐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連絡体制を構築しなければならない。

９．７ 例外措置

(1)　例外措置の許可

教職員等は、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、校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する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、学校情報セキュリティ責任者、学校情報システム責任者及び校内教育情報セキュリティ責任者の許可を得て、例外措置をとることができる。

(2)　緊急時の例外措置

教職員等は、校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時は、事後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。

(3)　例外措置の管理

学校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、例外措置の申請書及び審査結果等を適切に保管することに努めなければならない。

９．８ 法令遵守

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 1 号）

4　不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）

5　個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）

6　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）

7　サイバーセキュリティ基本法（平成 26 年法律第 104 号）

９．９ 学習用ネットワークへの端末接続管理

(1)　教育ネットワークに接続可能な端末は、原則として教育委員会が配備した端末に限定する。

(2)　教職員等が私物端末を教育ネットワークに接続する場合は、以下のすべてを満たした上で、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。

1　業務上の必要性が明確であること

2　OS のセキュリティアップデートが最新であること

3　マルウェア対策ソフトウェアが導入されていること

(3)　許可されていない端末のネットワーク接続は禁止する。

１０．外部委託

１０．１ 外部委託

「加賀市外部サービス利用基準」に準拠する。とりわけ、外部委託事業者が担う領域に関して、設計、開発、保守、運用等の各工程における切り分けや範囲を明確にしなければならない。

１０．２ 外部サービスの利用

(1)　外部サービスの選定

1　学校情報システム責任者は、取り扱う情報の格付け及び取り扱い制限を踏まえ、外

部サービス利用基準に従って外部サービスの利用を検討しなければならない。

2　重要性分類Ⅱ以上の情報を取り扱う外部サービスの選定は、原則として、学校情報システム責任者が行わなければならない。

3　学校の外部サービス管理者は、外部サービスで取り扱う情報の格付け及び取り扱い制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定しなければならない。

(2)　外部サービスの利用に係る調達・契約（重要性分類Ⅱ以上の情報を取り扱う場合）

1　学校情報システム責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。

2　学校情報システム責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たしたことを契約までに確認し、調達仕様に内容を契約に含めなければならない。

(3)　外部サービスの利用確認

学校の外部サービス管理者は、外部サービスを利用する場合には、利用申請の許可権者へ外部サービスの利用確認を行わなければならない。

１１．外部サービスの運用

１１．１ ウェブ会議システムの利用時の対策

(1)　学校情報システム責任者は、ウェブ会議を適切に利用するための利用手順を定めることに努めなければならない。

(2)　教職員等は、ウェブ会議を主催する場合、会議に無関係の者が参加できないよう対策を講じなければならない。

１１．２ ウェブサイト・ソーシャルネットワークの利用

学校情報システム責任者は、教育委員会又は学校が管理するアカウントでウェブサイトやソーシャルネットワーク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運用手順を定めることに努めなければならない。

(1)　本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の公式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入欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

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

(3)　重要性分類Ⅱ以上の情報は、ウェブサイトやソーシャルネットワークサービスで発信してはならない。

(4)　利用するウェブサイト・ソーシャルネットワークサービスごとの責任者を定めなければならない。

１２．ＳａａＳ型パブリッククラウドサービスの利用

１２．１ ＳａａＳ型パブリッククラウドサービスの利用における情報セキュリティ対策について

(1)　利用者認証

1　学校情報システム責任者は、クラウド事業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若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、サービス提供約款や契約書面上で確認又は合意しなければならない。

2　学校情報システム責任者は、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　教育委員会側管理者権限を有する者のＩＤの管理については、学校情報システム責任者は、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。

4　特権を付与されたIDにて外部委託業者が作業を行う場合、学校情報システム責任者による許可を必要とし、学校システム責任者は、作業内容の確認を行わなければならない。

5　学校情報システム責任者は、特権を付与されたID及びパスワードについては、定期的な変更又は入力回数制限等により、特にセキュリティ機能を強化しなければならない。

(2)　アクセス制御

1　学校情報システム責任者は、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、サービス提供約款や契約書面上で確認又は合意しなければならない。

2　学校情報システム責任者は、クラウド事業者の提供するアクセス制御機能を用いて、情報資産ごとに許可されたクラウドを利用する教職員等及び児童生徒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

学校情報システム責任者は、当該クラウドサービスへのデータの保管に際し、情報漏洩等に備えて、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約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

学校情報システム責任者は、複数のクラウド利用者がクラウドソースを共有する環境において、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、サービス提供約款や契約書面上で確認又は合意しなければならない。

(5)　技術的セキュリティ対策

学校情報システム責任者は、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、サービス提供約款や契約書面上で確認又は合意しなければならない。

(6)　情報通信経路のセキュリティ確保

1　学校情報システム責任者は、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、合意のうえ、利用しなければならない。

2　学校情報システム責任者は、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、サービス提供約款や契約書面上で確認又は合意しなければならない。

(7)　情報システムの物理的セキュリティ対策

1　学校情報システム責任者は、当該クラウドサービスのサーバー等の管理条件について、保守運用拠点へのセキュリティ侵害による被害は広範囲に及ぶ恐れがあることから、保守運用拠点がデータセンターと別の場所の場合、物理的セキュリティ対策も十分な堅牢性と入退室管理が図られているか、クラウド事業者に説明を求め、サービス提供約款や契約書面上で確認又は合意しなければならない。

2　学校情報システム責任者は、クラウド事業者側の管理区域（サーバー等を設置）及び保守運用拠点の管理において、十分な堅牢性や入退室管理が図られているか、クラウド事業者に説明を求め、サービス提供約款や契約書面上で確認又は合意しなければならない。

3　学校情報システム責任者は、クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）に当たり、セキュリティを確保した対応となっているかをクラウド事業者に説明を求め、サービス提供約款や契約書面上で確認又は合意しなければならない。なお、当該確認に当たっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認

証等を利用できる。

(8)　運用管理

1　学校情報システム責任者は、クラウド事業者に対し、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。また、クラウド事業者の設定不備等によるインシデント発生時にも同様の確認をしなければならない。

2　学校情報システム責任者は、クラウドサービスにおけるサーバー冗長化について、実施されていることをサービス提供約款や契約書面上で確認又は合意しなければならない。

3　学校情報システム責任者は、当該クラウドサービスにおけるデータのバックアップ及び復旧手順についてクラウド事業者に求め、サービス提供約款や契約書面上で確認又は合意しなければならない。

4　学校情報システム責任者は、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の対策をクラウド事業者に求め、サービス提供約款や契約書面上で確認又は合意しなければならない。

(9)　情報システムへのマルウェア対策

1　学校情報システム責任者は、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ー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、サービス提供約款や契約書面上で確認又は合意しなければならない。

2　学校情報システム責任者は、内部システムに侵入した攻撃を検知して対処するため、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、サービス提供約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　学校情報システム責任者は、クラウドサービス利用のため、アクセスする教職員等及び児童生徒側端末について、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　学校情報システム責任者は、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、クラウドを利用する教職員等及び児童生徒への教育や入口対策を講じなければならない。

(11)　クラウド事業者側の人的セキュリティ対策

1　学校情報システム責任者は、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定等を遵守することをクラウド事業者に求め、サービス提供約款や契約書面上で確認又は合意しなければならない。

2　学校情報システム責任者は、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、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洩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、サービス提供約款や契約書面上で確認又は合意しなければならない。

3　学校情報システム責任者は、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、サービス提供約款や契約書面上で確認又は合意しなければならない。

4　学校情報システム責任者は、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が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、サービス提供約款や契約書面上で確認又は合意しなければならない。

5　学校情報システム責任者は、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ー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、サービス提供約款や契約書面上で確認又は合意しなければならない。

(12)　サービス終了時等のデータ廃棄及びアカウント抹消について

1　学校情報システム責任者は、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及び利用者アカウント情報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、サービス提供約款や契約書面上で確認又は合意しなければならな

い。

2　学校情報システム責任者は、サービス利用終了時等におけるデータの扱いについて、スムーズに回収し、次期システムへの移行等を行えるよう、その措置の流れをサービス提供約款や契約書面上で確認又は合意しなければならない。

3　学校情報システム責任者は、クラウドサービスで利用するすべての情報資産について、クラウドサービスの利用終了時期を確認しクラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

(13)　クラウドサービス要件基準を満たすネットワーク設計

学校情報システム責任者は、利用するクラウドサービスの要件基準を確認し、要件基準を満たすネットワークを設計しなければならない。

１２．２ ＳａａＳ型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、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。確認すべき項目は下記の通り。

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、従業員への上記の育成計画や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リ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とインシデント対応フローを、サービスの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とインシデント対応フローを検証し、インシデントに備えた組織体制を整備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等について、クラウド事業者にサービス提供約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。

4　クラウド利用者は、クラウド事業者において個人情報の適切な管理が行われているか確認するとともに、確認した項目については、調達時においてサービスの過剰な排除にならないよう留意したうえで、契約要件等として定めなければならない。

１２．３ ＳａａＳ型パブリッククラウドサービス利用における教職員等の留意点

(1)　ＩＤ・パスワード等の秘匿

1　教職員等は、ID・パスワードについて秘匿管理を行わなければならない。

2　教職員等は、多要素認証に必要な要素（知識、生体、物理）についても適切に管理を行わなければならない。もし該当要素が流失等したと考えられる場合には、速やかに学校情報システム責任者に報告しなければならない。

(2)　モバイル端末持ち歩きリスク

教職員等は、クラウドサービスにアクセスする際に活用するモバイル端末について、紛失・盗難を避けるよう、適切に管理しなければならない。

(3)　重要性分類に基づく情報管理

パブリッククラウド上で重要な情報（重要性分類Ⅱ以上）を取り扱う際には、多要素認証を含む強固なアクセス制御による対策を講じる必要がある。

(4)　学校外からのパブリッククラウド利用

1　教職員等は、学校外からクラウドサービスを利用する際、情報資産の取り扱いをクラウドサービス上のみで行うことを原則とする。

2　クラウドサービスから端末にファイルをダウンロードする際は、情報資産の外部持ち出しに基づく安全管理措置として、端末の安全性を事前に確認するとともに、作業が終わり次第、当該端末から情報資産を速やかに消去しなければならない。

(5)　ＳａａＳ型パブリッククラウドサービスの学習用途、校務用途混在リスクへの対応

1　教職員等は、強固なアクセス制御による対策を講じたシステム構成にてクラウドを利用している場合には、クラウドサービスを学習用途と校務用途で適切に使い分けるよう、共有先やダウンロード方法等の運用ルールについて、あらかじめ確認し、適切に運用しなければならない。

2　教職員等は、ネットワーク分離による対策を講じたシステム構成の下でクラウドサービスをしている場合は、クラウドサービスを学習用途と校務用途で使い分けるよう、適切に運用しなければならない。

１３.一人１台端末におけるセキュリティ対策

１３．１ 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（帯域や同時接続数等）

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しなければならない。

(2)　不適切なウェブページの閲覧防止

学校情報システム責任者は、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くてはならない。

【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

学校情報システム責任者は、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

学校情報システム責任者は、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

学校情報システム責任者は、児童生徒への端末配備後においても、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等の作業を離れた場所からでも一元管理できるようにしなければならない。

(6)　端末の盗難・紛失時の情報漏洩対策

学校情報システム責任者は、児童生徒が端末を紛失した場合、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

学校情報システム責任者は、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や対応方法を各学校にて周知しなければならない。

１３．２ 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が「シンプル」「唯一無二」「永続的な識別」な構成要素となっている等、適切な措置を講じなければならない。ＩＤ登録やパスワードポリシーにおいては、情報セキュリティ対策として重要な要素であるため、学校ごとに管理するのではなく、教育委員会にて一元管理する。

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、中学校進学にも変更不要とする。

3　転出、卒業時のＩＤ削除処理

「唯一無二（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しなければならない。転出や卒業時に学習用ツールのサービス利用期間が終了する場合は、あらかじめ児童生徒本人によるデータ移行を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消去を行うこと。ただし、本人同意や適切な管理の下、一部のデータを活用することは可能である。

(2)　学習用ツールへのシグナルサインオン

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、その都度、ＩＤやパスワード等の認証情報を入力したり、サービスごと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、一定時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。

１４．評価・見直し

１４．１ 監査

(1)　監査の実施

教育委員会は、加賀市立学校情報セキュリティ対策基準が遵守されているか定期的に監査しなければならない。

(2)　加賀市立学校情報セキュリティ対策基準等の見直しへの活用

教育委員会は、監査の結果、加賀市立学校情報セキュリティ対策基準の見直しが必要と判断された場合は速やかに見直しを行わなければならない。

１４．２ 自己点検

(1)　自己点検の実施

校内教育情報セキュリティ責任者は、加賀市立学校情報セキュリティ対策基準が遵守されているか、定期的に又は必要に応じて、自己点検を実施しなければならない。

(2)　報告

自己点検を行った場合は、自己点検結果を学校情報システム責任者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、改善を図らなければならない。この場合、合わせて改善策を学校情報システム責任者に報告すること。

2　自己点検結果の報告等により、情報セキュリティ対策の見直しが必要な場合、教育委員会は速やかに見直しを行わなければならない。

１４．３ 加賀市立学校情報セキュリティ対策基準等の見直し

教育委員会は、社会情勢の変化や新たな教育関係情報への脅威の発生に対し、迅速かつ適切に対応するため、必要に応じて、加賀市立学校情報セキュリティ対策基準の見直しを行わなければならない。

報告第20号

山中図書館の空調工事に伴う対応について

１．現状と背景

山中図書館の館内空調設備が故障したため緊急修繕を行うが、工事完了は7月中旬となる見込みである。

近年、他館において、熱中症発生事例が報告されていることを鑑み、暑さ指数（WBGT）に基づく運用基準を定め、利用者の安全を最優先に確保する。

２．熱中症対策に伴う対応案

館内（閲覧室）の暑さ指数（WBGT）の測定値に基づき、以下のとおりとする。

基準値（WBGT）	対応内容
28℃以上（厳重警戒）	退館勧告：利用者への速やかな退館をお願いする。
31℃以上（危険）	臨時休館：施設の利用を中止し、休館措置を講ずる。
熱中症警戒アラート発表時	午後休館：午後の開館を取りやめる。

※WBGT（湿球黒球温度）とは、気温・湿度・輻射熱の3要素を考慮して算出される熱中症予防指標のこと。

※熱中症警戒アラートは、対象となる日の「前日の17時頃」または「当日の5時頃」の1日2回、都道府県ごとに発表される。

３．判断の根拠

・厚生労働省基準（R7.6.1）：長時間作業によるリスク

・日本気象協会：事務作業29℃以上、軽作業26℃以上でリスク

４．山中図書館内での対応

・事前に館内掲示、図書館HP、加賀市HP等を通じて利用者への周知を行う。

・個別空調が設置されている学習室を閲覧エリアとして解放する。

・通常は持ち込みを制限している閲覧室においても、熱中症対策として、蓋付き容器（水筒・ペットボトル等）による水分補給を認める。