R8.3改訂版

知多市教育情報セキュリティポリシー

令和３年３月

知多市教育委員会

目　次

第１　対象範囲及び用語説明

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、内部部局、教育委員会及び学校(小学校、中学校を言う。以下同じ。)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、次の図表１のとおりとする。

（1）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

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

（3）教育情報システムの仕様書及びネットワーク図等のシステム関連文書

（4）個人情報を含むすべての媒体

図表１　情報資産の種類と例

情報資産の種類	情報資産の例
教育ネットワーク	情報資産を扱う通信回線、FW、ルータ等の通信機器の設定情報や管理情報
教育情報システム	情報資産を扱うサーバ、パソコン、モバイル端末、汎用機、オペレーティングシステム、ソフトウェア等の設定情報や管理情報
教育ネットワーク及び教育情報システムに関する施設・設備	情報資産を扱うコンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブルの設定情報や管理情報
電磁的記録媒体	情報資産を扱うサーバ装置（クラウドを含む)、端末、デジタルカメラ、デジタルビデオカメラ、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部電磁的記録媒体に記録された情報

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	教育ネットワーク、教育情報システムで取り扱うデータ（これらを印刷した文書を含む。）
教育情報システム関連文書	教育情報システム関連のシステム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

３　用語説明

本対策基準における用語は、以下のとおりとする。

用語	定義
校務系情報	学校が保有する情報資産のうち、それらの情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報。機微情報を含む。
校務外部接続系情報	校務系情報のうち、ネットワーク分離による対策を講じたシステム構成において、インターネット接続を前提として校務で利用される情報
学習系情報	学校が保有する情報資産のうち、それらの情報を学校における教育活動において活用することを想定しており、かつ、当該情報に教員及び児童生徒がアクセスすることが想定されている情報
校務用端末	校務系情報にアクセス可能な端末
校務外部接続用端末	ネットワーク分離による対策を講じたシステム構成において、校務外部接続系情報にアクセス可能な端末
学習者用端末	学習系情報にアクセス可能な端末で、児童生徒が利用する端末
指導者用端末	学習系情報にアクセス可能な端末で、教員のみが利用可能な端末

校務系システム	校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム
校務外部接続系システム	ネットワーク分離による対策を講じたシステム構成において、校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ(CMS)及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム
学習系システム	学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム
教育情報システム	校務系システム、校務外部接続系システム及び学習系システムを合わせた総称
校務系サーバ	校務系情報を取り扱うサーバ
校務外部接続系サーバ	ネットワーク分離による対策を講じたシステム構成において、校務外部接続系情報を取り扱うサーバ
学習系サーバ	学習系情報を取り扱うサーバ
暗号化	電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)に準拠した暗号技術方法を指す。 本規定において、暗号化とはパスワードに限らず解除キーによる復号化が必要なファイル秘匿の技術をいう。
パスワード管理	暗号を復号化する際にパスワードが用いられることもあるが、単にアクセスを許可するゲートだけにパスワードを使用するケースを指す場合もある。
暗号化及びパスワード	本規定においてはパスワードで復号化可能な暗号化技術を指す。

第２　組織体制

１　最高教育情報セキュリティ責任者

（教育 CISO：Chief Information Security Officer、以下「教育 CISO」という。）

(1) 教育長を、教育 CISO とする。教育 CISO は、本市における全ての教育ネットワーク、教育情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決

定権限及び責任を有する。

(2) 教育 CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めることができる。

2　統括教育情報セキュリティ責任者

（教育 ISGM:Information Security General Maneger、以下「教育 ISGM」という。）

(1) 教育部長を、教育 CISO 直属の教育 ISGM とする。教育 ISGM は教育 CISO を補佐しなければならない。

(2) 教育 ISGM は、本市の全ての教育ネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

(3) 教育 ISGM は、本市の全ての教育ネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

(4) 教育 ISGM は、教育 ISM、教育情報セキュリティ管理者、教育情報システム管理者及び教育情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

(5) 教育 ISGM は、本市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、教育 CISO の指示に従い、教育 CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

(6) 教育 ISGM は、本市の共通的な教育ネットワーク、教育情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

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

(8) 教育 ISGM は、緊急時には教育 CISO に早急に報告を行うとともに、回復のための対策を講じなければならない。

(9) 教育 ISGM は必要に応じ、情報セキュリティやシステム運用に関する知識及び経験を有した専門家を教育情報化コーディネータ（ITCE）として設置し、その業務内容を定めることができる。

3　教育情報セキュリティ責任者

（教育 ISM:Information Security Manager、以下「教育 ISM」という。）

(1) 学校教育課長を教育 ISM とする。

(2) 教育 ISM は、本市の教育情報セキュリティ対策に関する統括的な権限及び責任を有する。

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

(4) 教育 ISM は、本市において所有している教育情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び教職員等(臨時的任用教職員、非常勤講師を含めた教職員全員をいう。以下同じ。)に対する教育、訓練、助言及び指示を行う。

4　教育情報システム管理者（以下「教育シスアド」という。）

(1) 学校教育課長を、教育シスアドとする。

(2) 教育シスアドは、所管する教育情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

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

(4) 教育シスアドは、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の維持・管理を行う。

(5) 教育シスアドは教育 ISM と兼務することができるものとする。

5　教育情報システム担当者（以下「教育シス担」という。）

(1) 学校教育課施設チーム担当者を、教育シス担とする。

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

6　教育情報システムオペレーター（以下「教育シスオペ」という。）

(1) 教育シス担の業務の内、教育情報システムの開発、設定の変更、運用、更新等の作業を、外部人材または委託業者に代行させることができる。

(2) 教育シスオペは、教育シス担の指示等に従い、教育情報システムの開発、設定の変更、運用、更新等の実際の作業の一部を行う。

(3) 外部人材または委託業者の選定は、別途定める。

7　教育情報セキュリティ管理者

（学校 Informaion Security Manager、以下「学校 ISM」という。）

(1) 校長を、学校 ISM とする。

(2) 学校 ISM は当該学校の情報セキュリティ対策に関する権限及び責任を有する。

(3) 学校 ISM は、当該学校において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、教育 ISM、教育 ISGM 及び教育 CISO へ速やかに報告を行い、指示を仰がなければならない。

8　学校情報システム担当者（以下「学校シス担」という。）

(1) 校務主任を、学校シス担とする。

(2) 学校シス担は、学校 ISM の管理下で、教育シス担の指示等に従い、教育情報システムの設定の変更、運用、更新等の作業を行う。

(3) 学校シス担の業務の一部を、ICT 支援員やサポーターといった外部人材もしくは保守委託業者に担当させることができる。

(4) ICT 支援員やサポーターといった外部人材もしくは保守委託業者の選定は、その役割に応じ適切に行うこと。

9　教育情報セキュリティ委員会

(1) 本市の教育情報セキュリティ対策を統一的に行うため、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する委員会を設置することができる。

(2) 委員会の構成員は教育 ISGM が選定し、教育 CISO の承認で定めることとする。

(3) 教育情報セキュリティ委員会では、教育委員会における情報セキュリティ対策の改

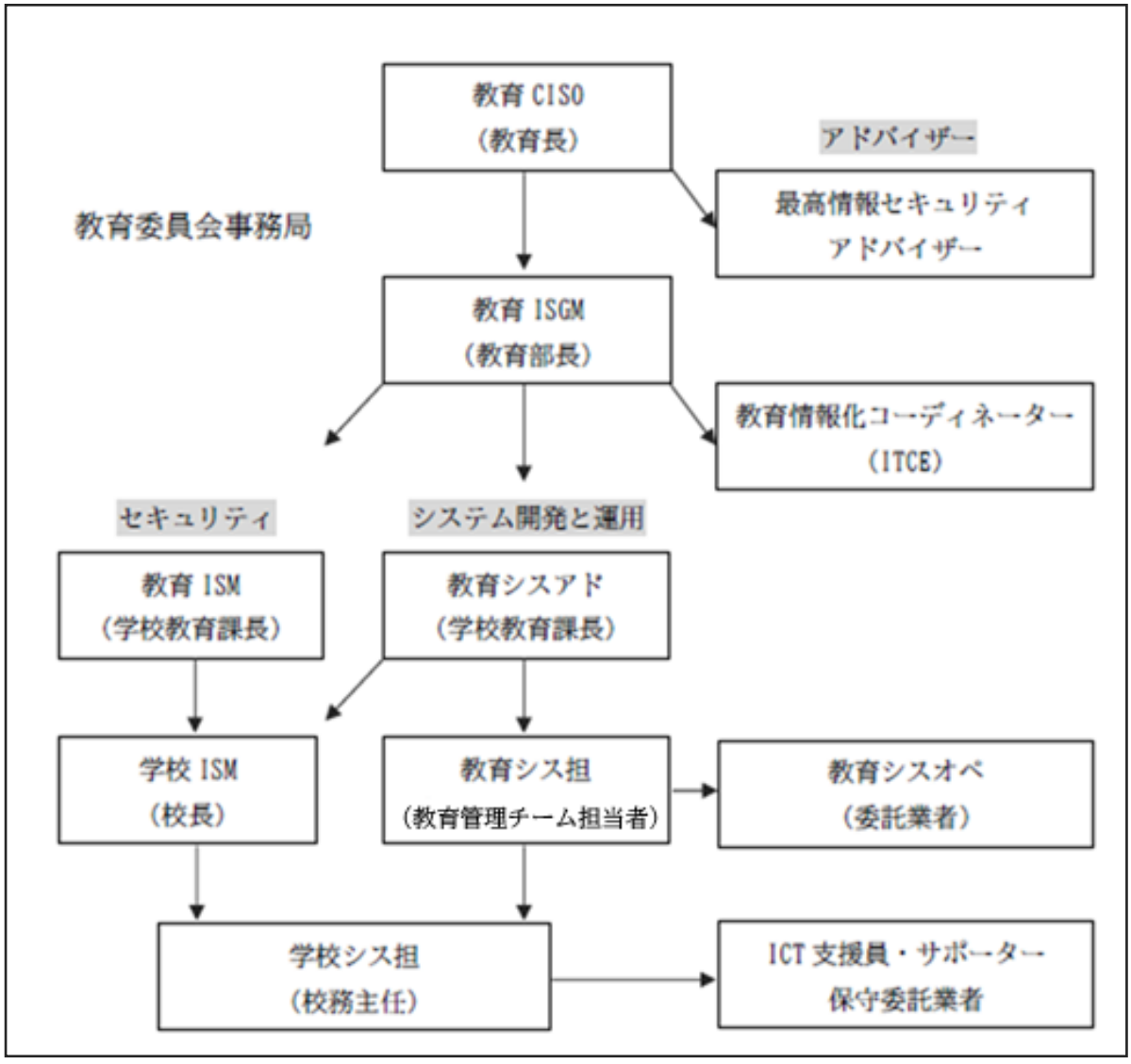
善計画を策定し、その実施状況を定期的に確認することとする。

10　兼務の禁止

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

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

組織図



第３　情報資産の分類と管理方法

１　情報資産の分類

本市における情報資産は、機密性、完全性及び可用性の３つの観点から影響度を評価し、次のとおり４段階の重要性分類を行い、必要に応じて取扱制限を行うものとし、詳細については別に定める知多市教育情報セキュリティ運用要領、（以下「運用要領」という。)」によるものとする。

重要性分類
Ａ 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。
Ｂ 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。（Ａを除く）
Ｃ セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼす。（Ａ,Ｂを除く）
Ｄ セキュリティ侵害が学校事務及び教育活動の実施に影響をほとんど及ぼさない。（Ａ，Ｂ，Ｃを除く）

機密性による情報資産の分類

分類	分類基準	該当する情報資産のイメージ
機密性 3	学校で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	特定の教職員のみが知り得る状態を確保する必要のある情報で秘密文書に相当するもの
機密性 2B	学校で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	教職員のみが知り得る状態を確保する必要がある情報資産(教職員のうち特定の教職員のみが知り得る状態を確保する必要があるものを含む)
機密性 2A	学校で取り扱う情報資産のうち、直ちに一般に公表することを前提としていないが、児童生徒がアク	教職員及び児童生徒同士のみが知り得る状態を確保する必要がある情報資産(教職員及び児童生徒のうち特定の教

	セスすることを想定している情報資産	職員及び児童生徒のみが知り得る状態を確保する必要があるものを含む）
機密性 1	機密性 2A、機密性 2B 又は機密性 3 の情報資産以外の情報資産	公表されている情報資産又は公表することを前提として作成された情報資産（教職員及び児童生徒以外の者が知り得ても支障がないと認められるものを含む）

完全性による情報資産の分類

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

可用性による情報資産の分類

分類	分類基準	該当する情報のイメージ
可用性 2B	学校で取り扱う情報資産のうち、	必要な時にいつでも利用できる必要が

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

２　情報資産の管理

情報資産の管理については、別途定める運用要領によるものとする。

第４　物理的セキュリティ

１　サーバ等の管理

(1) 物理的な機器の取付け

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

(2) 物理サーバの冗長化

ア　教育シスアドは、重要性分類Ｂ以上の情報資産を格納しているサーバを冗長化する等、同一データを保持する対策を講じなければならない。また、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停

止時間を最小限にしなければならない。

イ　教育システアドは、重要性分類Ｃ以上の情報資産を格納しているサーバのハードディスクを原則として冗長化しなければならない。

(3) 物理サーバ機器の電源

ア　教育システアドは、教育 ISGM 及び施設管理部門と連携し、重要性分類Ｂ以上の情報資産を格納している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　教育システアドは、教育 ISGM 及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

(4) 通信ケーブル等の配線

ア　教育 ISGM 及び教育システアドは、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

イ　教育 ISGM 及び教育システアドは、主要な箇所の通信ケーブル及び電源ケーブルについて、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。

ウ　教育 ISGM 及び教育システアドは、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 ISGM、教育システアドは、自ら又は教育シス担及び契約により操作を認められた外部委託事業者以外の者が配線を変更又は追加できないように必要な措置を施さなければならない。

(5) 機器の定期保守及び修理

ア　教育システアドは、重要性分類Ｃ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　教育システアドは、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。内容の消去は外部の事業者に委託できるがその場合、教育システアドは、外部の事業者に故障を修理させるに当たり、修理を委託する事業者との間で、守秘義務契約を締結するとともに秘密保持

体制の確認等を行わなければならない。

(6) 施設外又は学校外への機器の設置

教育 ISGM 及び教育シスアドは、外部データセンターやクラウドなど施設外又は学校外にサーバ等の機器を設置する場合、教育 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。ただし、独立した第三者機関が定める、セキュリティやクラウドサービスに関する国際規格を取得しているクラウドサービス利用については、それを以て代えることができるものとする。

(7) 機器の廃棄等

教育シスアドは、機器を廃棄又はリース返却等をする場合、機器内部の記憶装置から、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。

クラウドサービス利用の場合は、使用開始からデータや通信の暗号化機能を使用し、使用を停止した場合は復号化できないような停止手順を定め、それを実施することで廃棄証明に代えられるものとする。

2　管理区域（情報システム室等）の管理

(1) 管理区域の構造等

ア　管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋またはサーバラック、もしくは電磁的記録媒体の保管庫をいう。（以下「情報システム室」という。）

イ　教育 ISGM 及び教育シスアドは、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うことを原則とする。

ウ　教育 ISGM 及び教育シスアドは、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

エ　教育 ISGM 及び教育シスアドは、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。

オ　学校外に管理区域を設ける場合については、教育 ISGM 及び教育シスアドは、施設管理部門と連携して、管理区域から外部に通ずるドアは最小限とし、鍵、監視

機能、警報装置等によって許可されていない立入を防止しなければならない。

(2) 管理区域の入退室管理等

ア　学校 ISM 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、必要に応じて立ち入り区域を制限した上で、教職員が児童生徒に付き添うものとする。

ウ　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。

エ　学校 ISM は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限しなければならない。また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。

オ　学校外に管理区域を設ける場合については、教育シスアドは、管理区域への入退室を許可された者のみに制限し、IC カード、指紋認証等の生体認証や入退室管理簿の記録による入退室管理を行わなければならない。

カ　学校外に管理区域を設ける場合については、教育シスアドは、重要性分類Ｂ以上（機密性 2B 以上）の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

(3) 機器等の搬入出

ア　教育シスアドは、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　教育シスアドまたは学校 ISM 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者のみに制限し、入退室管理を行わなければならない。また、管理区域への入退室を許可された教職員を立ち会わせなければならない。

３　通信回線及び通信回線装置の管理

(1) 教育 ISGM は、施設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。

(2) 教育 ISGM 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。

(3) 教育 ISGM は、重要性分類Ｃ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、インターネットを通信経路とする回線の場合、通信される情報の暗号化を行わなければならない。

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

(5) 教育 ISGM は、重要性分類Ｂ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。

(6) 教育 ISGM は、学校運営上必要なネットワーク帯域を確保するとともに、遅延等に対する適切な対策を講じなければならない。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す配慮を含めてネットワーク構成を設計する。また、運用開始前には十分検証し、利用状況に応じて定期的に改修計画を行うこと。

４　教職員等の利用する端末や電磁的記録媒体等の管理

(1) 教育シスアドは、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や、校務用端末及び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) 教育シスアドは、教育情報システムへアクセスする端末へのログインパスワードの入力を必要とするように設定しなければならない。

(3) 教育シスアドは、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。端末に暗号化機能を持つセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。

(4) 教育シスアドは、パソコンやモバイル端末におけるマルウェア感染の脅威に対し、ウイルス対策ソフトの導入等の対策を講じなければならない。なお、OSによっては標準的にウイルス対策ソフトを備えている製品、OSとしてウイルス感染のリスクが低い仕組みとなっている製品などもあるため、実際に運用する端末において適切な対策を講じること。

(5) 教育シスアドは、インターネットへ接続をする場合、教職員等のパソコン、モバイル端末に対して不適切なウェブページの閲覧を防止するWebフィルタリング等の対策を講じなければならない。

5　学習者用端末のセキュリティ対策

(1) 不適切なウェブページの閲覧防止

児童生徒が端末を利用する際に不適切なウェブページの閲覧を防止する対策を講じなければならない。

(2) マルウェア感染対策

学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

(3) 端末を不正利用させないための防止策

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

(4) セキュリティ設定の一元管理

児童生徒への端末配付後においても、端末のセキュリティ設定やOSアップデート、ウェブブラウザのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状態確認などの作業を、離れた場所からでも一元管理できることが望ましい。

(5) 端末の盗難・紛失時の情報漏洩対策

児童生徒が端末を紛失しても、遠隔操作でロックをかける、あるいはワイプ（データ消去）することで第三者による不正操作や情報漏洩を防ぐ等の安全管理措置を講じなければならない。

６　学習者用端末や電磁的記録媒体の管理

(1) 教育シスアドは、盗難防止のため、教室等で利用するパソコンの保管庫による管理等の物理的措置を講じなければならない。

(2) 教育シスアドは、パソコン及び電磁的記録媒体について、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。

(3) 教育シスアドは、情報システムへのアクセスにおけるログインパスワードの入力等による認証を設定しなければならない。

第５　人的セキュリティ

１　学校 ISM の措置事項

学校 ISM の措置事項については、別途定める運用要領によるものとする。

２　教職員等の遵守事項

(1) 教育情報セキュリティポリシー等の遵守

学校 ISM を含む教職員等（以下　教職員等と言う）は、教育情報セキュリティポリシー及び運用要領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、速やかに教育 ISM に相談し、指示を仰がなければならない。

(2) 執務上での管理

ア　執務室の施錠管理

執務室にて教職員等が不在となる場合には、執務室を施錠しなければならない。

イ　来校者等への対応

来校者等を執務室に入れる場合には、学校ISMまたは学校シス担の許可を求めなければならない。

ウ　机上の書類・端末等の管理

教職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は学校ISM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。

(3) 支給端末の取扱い

ア　教職員等は、業務目的以外で支給端末を利用してはならない。

イ　教職員等は、外部のソフトウェアを無断で支給端末にインストールしてはならない。 業務上必要な場合には、事前に学校ISMの許可を得ること

ウ　教職員等は、支給端末の利用において、セキュリティ機能に関する設定変更メモリ増設等の改造等を無断でしてはならない。

エ　教職員等は、モバイル端末を利用する場合は、盗難・紛失リスクに備えての安全管理をすること。

オ　業務端末から離れる時は、端末をロックするなど、他者が閲覧できないようにしなければならない。

カ　業務終了後と外出時には、電源を落とさなければならない。

(4) 支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

ア　教職員等は、業務上やむを得ない場合を除いて、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。

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、学校ISMの許可を得た上で、必要な安全管理措置を講じなければならない。

(5) モバイル端末や電磁的記録媒体等の持ち出し及び教育委員会が構築・管理している環境（校務系リモート環境を含む）の外部における情報処理作業の制限

ア　教職員等は、学校のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には学校 ISM の許可を得なければならない。

イ　教職員等は、外部で情報処理業務を行う場合には、学校 ISM の許可を得なければならない。

(6) IDの取扱い

教職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

ア　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。

ウ　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、教育シスアドに通知しなければならない。

(7) 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、他者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、学校 ISM 及び教育 ISM 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。(シングルサインオンを除く)

カ　仮のパスワード(初期パスワードを含む)は、最初のログイン時点で変更しなければならない。

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。

(8) IC カード等の取扱い

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ISGM及び教育シスアドに通報し、指示に従わなければならない。

(9) 電子メールの利用制限

ア　教職員等は、学校 ISM の許可なく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、学校ISMに報告しなければならない。

オ　教職員等は、公務において公用メールアドレス以外のウェブで利用できるフリーメールサービス等を使用してはならない。

カ　情報ファイルを添付する場合には、運用要領に定める対策を講じなければならない。その際、パスワードを同一メールに記載しないこと。

キ　送信時には誤送信を予防するため、送信先のメールアドレス、添付ファイルの内容を確認しなければならない。

ク　差出人、添付ファイル又は本文中のリンク先等が不審なメールを受信した場合には、添付ファイルの閲覧やリンク先（URL）にアクセスせずに、学校ISMに指示を仰ぎなければならない。

(10) クラウドサービス、ソーシャルメディアサービス利用制限

ア　強固なアクセス制御による対策を講じたシステム構成でない場合、重要性分類Ｂ以上の情報資産を、インターネットを通信経路としたパブリッククラウドサービスで取り扱ってはならない。

イ　私的に契約したクラウドサービスや個人アカウントを業務利用してはならない。

ウ　ソーシャルメディアサービスを利用して、業務上知り得た情報を公開してはならない。

(11) 不正プログラム対策

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。OS及びコンピュータウイルス対策ソフトウェアが常に最新の状態に保てるようにしなければなら

ない。自動更新される設定の場合は、自動更新設定を変えてはならない。

イ　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

ウ　差出人、添付ファイル又は本文中のリンク先等が不審なメールを受信した場合は、添付ファイルの閲覧やリンク先（ＵＲＬ等）にアクセスせず、学校ISMに報告し速やかに削除しなければならない。

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

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

カ　教育ISGM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。

キ　コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、すみやかに学校ISMに報告し、指示を仰がなければならない。また、以下の対応を行わなければならない。

(ｱ) パソコン等の端末の場合

有線LANにつながる業務端末（校務用端末等）の場合は、LANケーブルの即時取り外しを行わなければならない。

(ｲ) モバイル端末の場合

無線LANにつながる業務端末（指導者用端末及び学習者用端末）の場合は、直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

(ｳ) 指示があるまでは、端末の電源は切らずに保持しなければならない。

(12) 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、原則として教育 CISO 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、原則として暗号化を行う場合に教育 CISO が定める以外の方法を原則として用いてはならない。

ウ　教育 CISO は、電子署名の正当性を検証するための情報又は手段を、署名検証者

へ安全に提供しなければならない。

(13) 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新規ソフトウェアを導入してはならない。

イ　教職員等は、業務上の必要がある場合は、教育 ISGM 及び教育シスアドの許可を得て、ソフトウェアを導入することができる。なお、導入する際は、教育 ISM 又は教育シスアドは、ソフトウェアのライセンスを管理しなければならない。

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。

エ　すでに市内で導入実績があり安全が確認されており、かつ正しくライセンスが許諾されているソフトウェアに関しては、導入手続きの簡素化を認める。

(14) 機器構成等の変更の制限

ア　教職員等は、パソコンやモバイル端末に対し、ストレージ及びファイル入出力に関する、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、前項の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 ISM 及び教育シスアドの許可を得なければならない。

ウ　マウス、キーボード、マイク、カメラなどデータ保存にかかわらない機器の増設は学校 ISM の許可があれば実施可能とする。

エ　セキュリティ機能に関する設定変更を行ってはならない。

(15) 無許可でのネットワーク接続の禁止

教職員等は、教育 ISM の許可なく校務系、または校務外部接続系ネットワークに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。教育系ネットワークに関しては運用要領に定める。

(16) 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　学校 ISM は、教職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、教育 ISM に通知し適切な措置を求めなければならない。

(17) 外部からのアクセス等の制限

ア　教職員等が外部から校務外部接続系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、教育委員会が構築・管理している環境（校務系リモート環境を含む）においては学校 ISM、それ以外については教育 ISGM 及び当該情報システムを管理する教育システアドの許可を得なければならない。

イ　教育 ISGM 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 ISGM 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 ISGM 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 ISGM 及び教育システアドは、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、アンチウイルス等を通じて、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

(18) 児童生徒への指導事項

教職員等は、児童生徒に学習者用端末等を利用させるにあたり、以下の事項について指導を行わなければならない。

ア　学習用途の利用限定

学習者用端末及び学習系クラウドサービスは学習目的で利用すること。

イ　利用者認証情報の秘匿管理

ID 及びパスワードは他の人に知られないようにすること。

ウ　端末のソフトウェアに関するセキュリティ機能の設定変更禁止

利用する端末のセキュリティ機能の設定を、許可なく変更してはならないこと。

エ　学習系情報は学習系クラウドに保管

端末で生成した情報の保存先を学習系クラウドに指定できる機能がある場合には、この機能を利用して原則学習系クラウドに保管し、学習者用端末へのローカル

保存は必要最小限とすること。

オ　無断で外部ソフトウェアをインストール禁止

無断で外部ソフトウェアをインストールしないようにすること。

カ　コミュニケーションツールの利用制限

学校から許可されたコミュニケーションツール（SNS，チャット等）のみを利用すること。

キ　ウイルス感染が疑われる場合の報告

学習者用端末が動かない、勝手に操作されている、いつもと異なる画面や警告が表示されるなどの症状がでた場合、すぐに担任教員に報告すること。

ク　端末の安全な取り扱い

学習者用端末は大事に取り扱い、盗難・紛失・破損等に注意すること。

ケ　私物端末など許可されていない端末利用禁止

私物端末など承認されていない端末を学校に持ちこまないこと。また、その端末を学校のネットワークに接続しないこと。

コ　重要性分類Ｂ以上の情報資産（児童生徒本人の情報に限る）の管理

該当資産を端末にダウンロードした場合には、目的を達成し次第すみやかに消去を行う等の対策を講じること。また、該当資産を閲覧する際には、離席時に端末ロックし、周囲に他の児童生徒がいる状態では閲覧しない等の対策を講じること。

(19) 異動・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。

3　教育委員会事務局職員の遵守事項

教育委員会事務局職員は、教育 ISM の指導の下、以下の規定を遵守しなければならない。

(1) 教育情報セキュリティポリシー等の遵守

(2) 業務以外の目的での使用の禁止

(3) 校務用端末による外部における情報処理作業の禁止

(4) 重要性分類Ｂ以上の情報資産について校務用端末以外のパソコン、モバイル端末及び電磁的記録媒体等によるアクセスの禁止

(5) 知りえた情報の秘匿

(6) 業務を離れる場合の遵守事項

(7) 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すべて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。

４　研修・訓練

(1) 情報セキュリティに関する研修・訓練

教育 CISO は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

(2) 研修計画の策定及び実施

ア　教育 CISO は、教職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、教育 CISO 及び教育情報セキュリティ委員会の承認を得なければならない。

イ　研修計画において、教職員等は、毎年度最低 1 回は情報セキュリティ研修を受講できるようにしなければならない。

ウ　新規採用の教職員等（他団体から新規に赴任した職員含む）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。

エ　研修は、教育 ISGM、教育 ISM、教育シスアド、学校 ISM、学校シス担及びその他教職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにすることが望ましい。

オ　教育 CISO は、毎年度 1 回、教育情報セキュリティ委員会に対して、教職員等の情報セキュリティ研修の実施状況について報告しなければならない。

(3) 緊急時対応訓練

教育 CISO は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練

計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

(4) 研修・訓練への参加

全ての教職員等は、定められた研修・訓練に参加しなければならない。

5　情報セキュリティインシデントの連絡体制の整備

(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、速やかに学校 ISM に報告しなければならない。

イ　報告を受けた学校 ISM は、速やかに教育 ISM、教育シスアド及び情報セキュリティに関する統一的な窓口に報告しなければならない。

ウ　教育 ISM 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 CISO 及び教育 ISGM に報告しなければならない。

(2) 学校内からの情報セキュリティ違反行為の報告

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、速やかに学校ISMに報告しなければならない。

イ　報告を受けた学校ISMは、速やかに教育ISM、教育ISGM及び情報セキュリティに関する統一的な窓口に報告しなければならない。

ウ　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 ISGM 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。

(3) 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、学校 ISM に報告しなければならない。

イ　報告を受けた学校 ISM は、速やかに教育 ISM 及び教育シスアドに報告しなければならない。情報セキュリティインシデントの報告は、所定の報告書を用いる。

ウ　教育 ISM は、当該情報セキュリティインシデントについて、必要に応じて教育 CISO 及び教育 ISGM に報告しなければならない。

(4) 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

ア　教育 ISGM は、情報セキュリティインシデントについて、教育 ISM、教育シスアド及び情報セキュリティに関する統一的な窓口と連携し、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、教育 CISO に報告しなければならない。

イ　教育 CISO は、教育 ISGM から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

(5) 支給端末の運用・連絡体制の整備

学校内外での支給端末の運用ルールを制定し、インシデント時の連絡先対応方法を各学校にて整理し、実施手順に反映しなければならない。

第６　技術的セキュリティ

１　コンピュータ及びネットワークの設定管理

(1) 文書サーバ及び端末の設定等

ア　教育シスアドは、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　教育シスアドは、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　教育シスアドは、住民の個人情報、人事記録等、特定の教職員等しか取扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一学校等であっても、担当職員以外の教職員等が閲覧及び使用できないようにしなければならない。

エ　教育シスアドは、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データの外部流出の可能性を考慮し、データ暗号化等による安全管理措置を講じなければならない。

(2) バックアップの実施

教育 ISGM 及び教育シスアドは、ファイルサーバ等に記録された情報について、サ

ーバの冗長化対策に関わらず、次のア及びイに基づきバックアップを実施するものとする。

ア　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。

イ　学習系情報については、必要に応じて定期的にバックアップを実施しなければならない。ただし、クラウドサービス利用の場合は原則実施不要とする。

(3) ログの取得等

ア　教育 ISM 及び教育シスアドは、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 ISM 及び教育シスアドは、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

ウ　教育 ISM 及び教育シスアドは、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。

(4) ネットワークの接続制御、経路制御等

ア　教育 ISGM 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 ISGM 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。

(5) 外部の者が利用できるシステムの分離等

教育シスアドは、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。

(6) 外部ネットワークとの接続制限等

ア　教育シスアドは、所管するネットワークを外部ネットワークと接続しようとする場合には、教育 CISO 及び教育 ISGM の許可を得なければならない。

イ　教育シスアドは、接続しようとする外部ネットワークに係るネットワーク構成、

機器構成、セキュリティ技術等を詳細に調査し、庁内及び学校の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

ウ　教育シスアドは、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

エ　教育 ISGM 及び教育シスアドは、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　教育シスアドは、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 ISGM 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) 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　教育シスアドは、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をする、もしくはこれら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　教育シスアドは、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。

(8) 複合機のセキュリティ管理

ア　教育 ISGM 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 ISGM 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 ISGM 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。

(9) 特定用途機器のセキュリティ管理

教育 ISGM 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。

(10) 無線 LAN 及びネットワークの盗聴対策

ア　教育 ISGM は、無線 LAN の利用を認める場合、解読が困難な通信の暗号化及び認証技術の使用を義務付けなければならない。

イ　教育 ISGM は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、通信の暗号化等の措置を講じなければならない。

(11) 電子メールのセキュリティ管理

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

イ　教育 ISGM は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

ウ　教育 ISGM は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

エ　教育 ISGM は、教職員等が使用できる電子メールボックスの容量の上限を設定することができる。設定した場合は上限を超えた場合の対応を教職員等に周知しなければならない。

オ　教育 ISGM は、システム開発や運用、保守等のため施設内に常駐している外部委託事業者の作業員による電子メールアドレス利用について、外部委託事業者との間で利用方法を取り決めなければならない。

カ　教育 ISGM は、教職員等が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すことが不可能となるように添付ファイルの監視等によりシステム上措置することを検討する必要がある。

2　アクセス制御

(1) アクセス制御等

教育 ISGM 又は教育システアドは、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) 外部からのアクセス等の制限

ア　教育 ISGM 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。

イ　教育 ISGM は、民間事業者等の外部組織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。

ウ　教育 ISGM 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通信の暗号化等の措置を講じなければならない。

エ　教育 ISGM 及び教育システアドは、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、モバイル端末管理（MDM）の導入等を通じて、セキュリティ確保のために必要な措置を講じなければならない。

オ　教育 ISGM は、外部ネットワーク(モバイルネットワーク,公衆無線 LAN 等)から校務系、校務外部接続系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。

(3) ログイン時の表示等

教育システアドは、校務系、校務外部接続系ネットワークにおいて、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ教職員等がログインしたことを確認することができるようシステムを設定しなければならない。

(4) 特権による接続時間の制限

教育シスアドは、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。

3　システム開発、導入、保守等

(1) 情報システムの調達

ア　教育 ISGM 及び教育シスアドは、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 ISGM 及び教育シスアドは、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

(2) 情報システムの開発

ア　システム開発における責任者及び作業者の特定

教育シスアドは、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) 教育シスアドは、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) 教育シスアドは、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) 教育シスアドは、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) 教育シスアドは、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

本市の情報セキュリティポリシーに準ずる

(4) 情報システムの変更管理

教育シスアドは、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。

(5) 開発・保守用のソフトウェアの更新等

教育シスアドは、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。

(6) システム更新又は統合時の検証等

教育シスアドは、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。

4　不正プログラム対策

(1) 教育 ISGM の措置事項

教育 ISGM は、校務系、校務外部接続系の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、常に最新の状態に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。

(2) 教育シスアドの措置事項

教育システアドは、校務系、校務外部接続系の不正プログラム対策に関し、次の事項を措置しなければならない。

ア　教育システアドは、その所掌するサーバ及びパソコン等の端末を守るため、コンピュータウイルス等の不正プログラムへの対策を講じなければならない。

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、コンピュータウイルス等の感染を防止するために、市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。

5　不正アクセス対策

(1) 教育 ISGM の措置事項

教育 ISGM 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及び SSID 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、データの書換えを検出し、教育 ISGM 及び教育システアドへ通報するよう、設定しなければならない。

エ　教育 ISGM は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

(2) 攻撃の予告

教育 CISO 及び教育 ISGM は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

(3) サービス不能攻撃

教育 ISGM 及び教育システアドは、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

教育 ISGM 及び教育シスアドは、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

6　セキュリティ情報の収集

(1) セキュリティホールに関する情報の収集及び共有並びにソフトウェアの更新等

教育 ISGM 及び教育シスアドは、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

(2) 不正プログラム等のセキュリティ情報の収集及び周知

教育 ISGM は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、教職員等に周知しなければならない。

(3) 情報セキュリティに関する情報の収集及び共有

教育 ISGM 及び教育シスアドは、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。

第７　運用

1　情報システムの監視

(1) 教育 ISGM 及び教育シスアドは、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

(2) 教育 ISGM 及び教育シスアドは、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

(3) 教育 ISGM 及び教育シスアドは、重要性分類Ｂ以上の情報資産を格納するシステムを監視する責めを負う。

(4) 内部からの攻撃監視

教育ISGM及び教育シスアドは、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所管するネットワーク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。

2　ドキュメントの管理

(1) システム管理記録及び作業の確認

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

(2) 情報システム仕様書等の管理

教育 ISM 及び教育シスアドは、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、紛失したりしないよう、適切に管理しなければならない。

(3) 障害記録の管理

教育 ISM 及び教育シスアドは、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。

(4) 記録の保存

教育 CISO 及び教育 ISGM は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

3　教職員等の ID 及びパスワードの管理

(1) 利用者 ID の取扱い

ア　教育 ISGM 及び教育システアドは、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　教育 ISGM 及び教育システアドは、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

(2) パスワードに関する情報の管理

ア　教育ISGM及び教育システアドは、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。

イ　教育ISGM及び教育システアドは、教職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

4　IC カード等の取扱い

(1) IC カード等の取扱い

ア　教育ISGM及び教育システアドは、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。

イ　教育ISGM及び教育システアドは、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。

5　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

ア　入学/転入時のID登録処理

IDについてはシンプル・ユニーク（唯一無二）・パーマネント/パーシスタント（永続的な識別）な構成要素になっていることや、児童生徒の発達段階に応じた

複雑性をあげたパスワードポリシーによりセキュリティ強化を上げていくなど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毎に管理するのではなく、同一の教育委員会等の組織にて一元管理することが望ましい。

イ　進級/進学時のID関連情報の更新

IDについては原則として進級/進学にも変更不要とすることが望ましい。IDを変えることなくIDの属性情報（進級時の組・出席番号、進学先学校名など）の更新を行っておくことで、MDMによる各種ポリシーや使用アプリケーションの変更を効率的に行うことが可能となる。

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

ウ　転出/卒業/退学時のID削除処理

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

転出や卒業/退学時に学習用ツールのサービス利用期間が終了する場合は、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削除を行うこと。

(2) 学習用ツールへのシングルサインオン

学習履歴を活用したり、個人の成果物を保存するアプリケーションが増えてくると、サービス利用時に都度ID及びパスワード等の認証情報を入力したり、サービス毎のアカウント情報管理が非常に煩雑になるため、一度の認証により一定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。

(3) 多要素認証等によるなりすまし対策

本人確認を厳格に行う必要がある場合においては児童生徒のID及びパスワードに加えて多要素認証を設定することが望ましい。パブリッククラウド上で重要な情報（重要性分類Ｂ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

る対策を講じなければならない。ただし、児童生徒またはその保護者が重要性分類Ｂ以上の情報資産にアクセスする場合は、児童生徒本人またはその保護者が、当該児童生徒に関するもののみにアクセスすることを想定していることから、多要素認証を設定することが望ましいものの、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際のロック機能の有効化、パスワードの複雑性の確保等により本人確認を厳格に行う前提で、ID及びパスワードでの認証を許容する。

6　特権を付与されたIDの管理等

(1) 教育ISGM及び教育シスアドは、管理者権限等の特権を付与されたIDを利用する者を必要最小限にし、当該IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを厳重に管理しなければならない。

(2) 教育ISGM及び教育シスアドの特権を代行する者は、教育ISGM及び教育シスアドが指名し、教育CISOが認めた者でなければならない。

(3) 教育CISOは、代行者を認めた場合、速やかに教育ISGM、教育ISM、学校ISM及び教育シスアドに通知しなければならない。

(4) 教育ISGM及び教育シスアドは、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。

(5) 教育ISGM及び教育シスアドは、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。

(6) 教育ISGM及び教育シスアドは、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　教育情報セキュリティポリシーの遵守状況の確認・管理

(1) 遵守状況の確認及び対処

ア　教育ISM及び学校ISM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、速やかに教育CISO及び教育ISGMに報告しなければならない。

イ　教育CISOは、発生した問題について、適切かつ速やかに対処しなければならな

い。

ウ　教育 ISGM 及び教育シスアドは、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

(2) パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

教育 CISO 及び教育 CISO が指名した者は、不正アクセス、不正プログラム等の調査のために、教職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

(3) 業務以外の目的でのウェブ閲覧の禁止

統括教育情報セキュリティ責任者は、教職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、教育情報セキュリティ管理者に通知し適切な措置を求めなければならない。

(4) 教職員等による不正アクセスの管理

教育ISGM及び教育シスアドは、教職員等による不正アクセスを発見した場合は、学校ISMに通知し、適切な処置を求めなければならない。

8　専門家の支援体制等

(1) 専門家の支援体制

教育ISGM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。

(2) 他団体との情報システムに関する情報等の交換

学校 ISM 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 ISGM 及び教育 ISM の許可を得なければならない。

9　侵害時の対応等

(1) 緊急時対応計画の策定

教育 CISO 又は教育情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発

生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定め、セキュリティ侵害時には当該計画に従って適切に対処することが望ましい。

(2) 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めるべきである。

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

(3) 業務継続計画との整合性確保

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

(4) 緊急時対応計画の見直し

教育 CISO 又は教育情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

10　例外措置

(1) 例外措置の許可

教育 ISM 及び教育シスアドは、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、教育 CISO の許可を得て、例外措置を取ることができる。

(2) 緊急時の例外措置

教育 ISM 及び教育シスアドは、学校事務及び教育活動の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに教育 CISO に報告しなければならない。

(3) 例外措置の申請書の管理

教育 CISO は、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

11　法令等遵守

教職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令等を遵守し、これに従わなければならない。

(1) 地方公務員法(昭和 25 年 12 月 13 日法律第 261 号)

(2) 教育公務員特例法(昭和 24 年 1 月 12 日法律第 1 号)

(3) 著作権法(昭和 45 年法律第 48 号)

(4) 不正アクセス行為の禁止等に関する法律(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)

12　懲戒処分等

(1) 懲戒処分

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

(2)違反時の対応

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

ア　教育 ISM が違反を確認した場合は、教育 ISM は当該教職員等が所属する学校の学校 ISM に通知し、適切な措置を求めなければならない。

イ　教育シスアド等が違反を確認した場合は、違反を確認した者は速やかに教育 ISGM 及び当該教職員等が所属する学校の学校 ISM に通知し、適切な措置を求めなければならない。

ウ　学校 ISM の指導によっても改善されない場合、教育 ISGM 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 ISGM は、教職員等の権利を停止あるいは剥奪した旨を教育 CISO 及び当該教職員等が所属する学校の学校 ISM に通知しなければならない。

第８　外部委託

(1) 外部委託事業者の選定基準

ア　教育シスアドは、外部委託事業者の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

イ　教育シスアドは、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定することが望ましい。

(2) 契約項目

情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

ア　教育情報セキュリティポリシー及び教育情報セキュリティ実施手順の遵守

イ　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

ウ　提供されるサービスレベルの保証

エ　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

オ　外部委託事業者の従業員に対する教育の実施

カ　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

キ　業務上知り得た情報の守秘義務

ク　再委託に関する制限事項の遵守

ケ　託業務終了時の情報資産の返還、廃棄等

コ　委託業務の定期報告及び緊急時報告義務

サ　市による監査、検査

シ　市による情報セキュリティインシデント発生時の公表

ス　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

教育シスアドは、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、(2)の契約に基づき措置しなければならない。また、その内容を教育 ISGM に報告するとともに、その重要度に応じて教育 CISO に報告しなければならない。

(4) 外部委託事業者に対する説明

教育シスアドは、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。

第９　SaaS 型パブリッククラウドサービスの利用

独立した第三者機関が定める、セキュリティやクラウドサービスに関する国内や国際規格を取得しているデータセンターやクラウドサービス利用については、認証内容を精査し、情報セキュリティ対策において適切と見なすことができる。教育 ISGM 及び教育シスアドが検討を行い教育 CISO が承認する。

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

(1) 利用者認証

ア　クラウド利用者は、クラウド事業者における当該クラウドサービスを提供する情報システムの運用もしくは開発に従事する者又は管理者権限を有する者について、適切な利用者確認がなされていることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意サービス提供定款や契約書面上で確認または合意しなければならない。

イ　クラウド利用者は、当該クラウドサービスのログインに関わる認証機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

ウ　クラウド利用者側管理者権限を有する者の ID の管理について、「第７．６　特権を付与された ID の管理等」を遵守しなければならない。

(2) アクセス制御

ア　クラウド利用者は、当該クラウドサービスに対して、アクセスする権限のない者がアクセスできないように、システム上制限する機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

イ　クラウド利用者は、クラウド事業者の提供するアクセス制御機能を用いて、情報資産毎に、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

クラウド利用者は、当該クラウドサービスへのデータの保管に際し、情報漏えい等に備えて、暗号化等の保護措置を講じられていることを、クラウド事業者にサービス提供定款や契約書面上で確認または合意しなければならない。

(4) マルチテナント環境におけるテナント間の安全な管理

クラウド利用者は、複数のクラウド利用者がクラウドリソースを共用する環境において、特定のクラウド利用者に対して発生したセキュリティ侵害が、他のクラウド利用者に影響を与えないように対策が講じられていることを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

(5) クラウドサービスを提供する情報システムに対する外部からの悪意のある脅威の侵入を想定した技術的セキュリティ対策

ア　クラウド利用者は、当該クラウドサービスを提供する情報システムを監視し、セキュリティ侵害を検知することを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

イ　クラウド利用者は、当該クラウドサービスを提供する情報システムのインターネット接続境界において、クラウド利用者以外による不正な通信・侵入を防ぐ措置を講じるとともに、外部脅威の侵入を検知し、防御する対策を講ずることを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

(6) 情報の通信経路のセキュリティ確保

ア　クラウド利用者は、教育情報システムのインターネット境界から当該クラウドサービスを提供する情報システムまでの情報の通信経路において、情報の盗聴、改

ざん、誤った経路での通信、破壊等から保護するために必要な措置(情報交換の実施基準・手順等の整備、通信の暗号化等)をクラウド事業者に求め、合意のうえ、利用しなければならない。

イ　クラウド利用者は、クラウド事業者が保守運用等を遠隔で行う場合の、保守運用拠点と管理区域間での通信回線及び通信回線装置の管理について、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置(情報交換の実施基準・手順等の整備、通信の暗号化等)をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

(7) クラウドサービスを提供する情報システムの物理的セキュリティ対策

ア　クラウド利用者は、当該クラウドサービスのサーバ等の管理条件を「第４．１　サーバ等の管理」に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

イ　クラウド利用者は、クラウド事業者側の管理区域(サーバ等を設置)及び保守運用拠点の管理において、「第４．２　管理区域(情報システム室等)の管理」に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

ウ　クラウド利用者は、クラウド事業者が利用する資源（装置等）の処分（廃棄）にあたり、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求め、サービス提供定款や契約書面上で確認また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) クラウドサービスを提供する情報システムの運用管理

ア　クラウド利用者は、当該クラウドサービスにおけるサーバの冗長化について、「４．１　サーバ等の管理　(2)サーバの冗長化」に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

イ　クラウド利用者は、当該クラウドサービスにおけるデータバックアップについて、適切な対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認ま

たは合意しなければならない。

ウ　クラウド利用者は、当該クラウドサービスにおける情報セキュリティの確保や監査に必要なログの取得について、「第６．１　コンピュータ及びネットワークの設定管理　(3)ログの管理」に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

(9) クラウドサービスを提供する情報システムのマルウェア感染対策

ア　クラウド利用者は、クラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等について、マルウェア感染対策を講じることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

イ　クラウド利用者は、内部システムに侵入した攻撃を検知して対処するために、通信をチェックする等の対策を講じることをクラウド事業者に求め、サービス提供定款や契約書面上で確認また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

ア　クラウド利用者は、クラウドサービスにアクセスするクラウドを利用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。

イ　クラウド利用者は、標的型攻撃による外部からの脅威の侵入を防止するために、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) クラウド事業者従業員の人的セキュリティ対策

ア　クラウド利用者は、クラウドサービスに関わるクラウド事業者従業員に対して、クラウド事業者の情報セキュリティポリシー及び保守運用管理規程等を遵守することをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

イ　クラウド利用者は、クラウドサービスに関わるクラウド事業者従業員に対して、業務に用いる ID 及びパスワードその他の個人認証に必要な情報及び媒体について、部外者及び業務に関わらない従業員に漏えいすることがないように、適切に管理することをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

ウ　クラウド利用者は、クラウドサービスに関わらない従業員等がクラウド利用者のデータを知り得る状態にならないよう、業務に関わるクラウド事業者従業員に対して秘匿を義務づけることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

エ　クラウド利用者は、クラウド利用者のデータ及びデータを格納した端末機器又は電磁的記録媒体の外部持ち出しについて、クラウド利用者の許可なく外部持ち出しできないこと及び外部持ち出しにおける安全管理手順をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

オ　クラウド利用者は、クラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等に、マルウェアを侵入させないよう、クラウド事業者に求め、サービス提供定款や契約書面上で確認また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の廃棄及び利用者アカウント抹消について

ア　クラウド利用者は、サービス利用終了時等において、クラウド利用者のデータ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定款や契約書面上で確認または合意しておかなければならない。

イ　クラウド利用者は、サービス利用終了時等におけるデータの扱いについて、スムーズに回収、次期システムへの移行等を行えるよう、その措置の流れについてサービス提供定款や契約書面上で確認または合意しておかなければならない。

ウ　クラウド利用者は、クラウドサービスで利用する全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配慮を含めたネットワーク設計

ア　クラウド利用者は、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。

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の禁止

クラウド利用者は、クラウド事業者と契約時に守秘義務、目的外利用及び第三者へ

の提供の禁止条項を締結しなければならない。クラウドサービス事業者がコンテンツにアクセスできるかどうかを確認し、サービスに係る情報及び受託した情報に関する守秘義務、目的外利用及び第三者への提供の禁止条項について、サービス提供に係る契約に含めなければならない。契約には、当該条項に違反したクラウドサービス事業者に対する損害賠償規定を含める。

(2) 準拠する法令、情報セキュリティポリシー等の確認

クラウド利用者は、クラウド事業者がどのような規範に基づいてサービス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

ア　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。確認すべき項目例を下記に示す。

(ｱ) 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

(ｲ) 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

(ｳ) サービスの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

ア　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、充分な知識とセキュリティ意識を醸成することをに求めなければならない。

イ　クラウド利用者は、クラウド事業者に、従業員への上記育成計画、教育実績等の情報を提示させ、自らデータを管理する場合と同様の教育・訓練を実施しているかを確認しなければならない。

(5) 情報セキュリティに関する役割の範囲、責任分界点

ア　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。

イ　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

ア　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。

イ　クラウド利用者は、クラウド事業者によるクラウドサービスに関する監査レポート等を根拠にして、自らの関係法令、情報セキュリティポリシーと照らし合わせ、安全性が確保されているかについて確認しなければならない。

(7) 情報インシデント管理及び対応フローの合意

ア　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及びインシデント対応フローを、サービス仕様の一部として定めることについて、クラウド事業者に対して求めなければならない。

イ　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及び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

ア　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

ア　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。

イ　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

ア　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。

イ　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訳ではないことから、事業者を変更する際のデータ移行の方法などについて、クラウド事業者にサービス提供定款や契約書面上で確認または合意しなければならない。

ウ　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。また、国内法以外の法令及び規制が適用される場合にはそのリスクを評価した上でクラウド事業者を選定しなければならない。

エ　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上で、契約要件等として定めなければならない。

3　SaaS型パブリッククラウドサービスの利用における教職員等の留意点

(1) ID及びパスワード等の秘匿

ア　教職員等は、ID及びパスワードについて秘匿管理を行わなければならない。

イ　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。もし該当要素が流出等したと考えられる場合には、速やかに学校ISM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Ｂ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なければならない。ただし、児童生徒またはその保護者が重要性分類Ｂ以上の情報資産にアクセスする場合は、児童生徒本人またはその保護者が、当該児童生徒に関するもののみにアクセスすることを想定していることから、多要素認証を設定することが望ましいものの、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際のロック機能の有効化、パスワードの複雑性の確保等により本人確認を厳格に行う前提で、ID及びパスワードでの認証を許容する。

(4) 学校外からのパブリッククラウド利用

ア　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。

イ　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すみ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

ア　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サービス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。

イ　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場合にてクラウドサービス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使い分けるよう、適切に運用しなければならない。

4　約款による外部サービスの利用

(1) 約款による外部サービスの利用に係る規定の整備

ア　教育シスアドは、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

イ　教育情報システム管理者は、約款による外部サービスの利用に当たっては、約款において以下の点が規定されていることを確認しなければならない。

（ｱ）利用者が登録した情報が、利用者の同意なく無断使用（目的外利用、第三者への提供等）されないこと。

（ｲ）サービス事業者が業務上知り得た情報の守秘義務が守られること。

(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。

5　ソーシャルメディアサービスの利用

(1) 教育シスアドは、教育委員会又は学校が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

ア　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

(2) 重要性分類Ｃ以上（機密性 2A 以上）の情報はソーシャルメディアサービスで発信してはならない。

(3) 利用するソーシャルメディアサービスごとの責任者を定めなければならない。

第１０　評価・見直し

1　監査

(1) 実施方法

教育CISOは、情報セキュリティ監査統括責任者を指名し、教育ネットワーク及び教育情報システム等の情報資産における情報セキュリティ対策状況について、定期的に又は必要に応じて監査を行わせるようにしなければならない。

(2) 監査を行う者の要件

ア　情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

イ　監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

(3) 監査実施計画の立案及び実施への協力

ア　情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、教育情報セキュリティ委員会の承認を得なければならない。

イ　被監査部門は、監査の実施に協力しなければならない。

(4) 外部委託事業者に対する監査

外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、教育情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

(5) 報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、教育情報セキュリティ委員会に報告する。

(6) 保管

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

(7) 監査結果への対応

教育CISOは、監査結果を踏まえ、指摘事項を所管する学校ISM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学校ISMに対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

(8) 情報セキュリティポリシー及び関係規程等の見直し等への活用

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

2　自己点検

(1) 実施方法

ア　教育 ISGM 及び教育シスアドは、所管するネットワーク及び情報システムについて、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 ISM は、学校 ISM と連携して、所管する部局における教育情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

(2) 報告

教育 ISGM、教育シスアド及び教育 ISM 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、教育情報セキュリティ委員会に報告しなければならない。

(3) 自己点検結果の活用

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　教育情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

3　教育情報セキュリティポリシー及び関係規程等の見直し

教育情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

梅香る わたしたちの緑園都市

知多市教育情報セキュリティポリシー

令和３年３月策定

令和４年３月一部改訂

令和５年３月一部改訂

令和６年４月一部改訂

令和７年３月一部改訂

令和８年３月一部改訂

知多市教育委員会

〒478-8601　知多市緑町１番地

電　話　0562-36-2682（直通）　ＦＡＸ　0562-33-7287

ＵＲＬ　https://www.city.chita.lg.jp