豊川市教育情報セキュリティポリシー

（令和７年４月）

豊川市教育委員会

はじめに

情報セキュリティポリシーとは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書のことで、本市においても、豊川市情報セキュリティポリシー（平成 15 年 9 月 22 日策定）を策定し、その後社会の変化等を受けて見直しを行ってきました。

情報セキュリティポリシーは、情報セキュリティ対策の頂点に位置するものであり、本来は豊川市全てを包括するポリシーでなければなりませんが、一方で、市が設置する学校においては、地方公共団体の他の行政事務とは異なる特徴を有しています。

例えば学校は、地方公務員法に定める「服務」に服さない児童生徒が過ごす場所ですが、当該児童生徒がコンピュータを活用した学習活動の実施などにおいて、日常的に情報システムにアクセスする機会があるため、児童生徒においても情報セキュリティポリシーにて規定した対策について遵守するよう、職員や教員、保護者等が適切に指導を行うことが求められています。

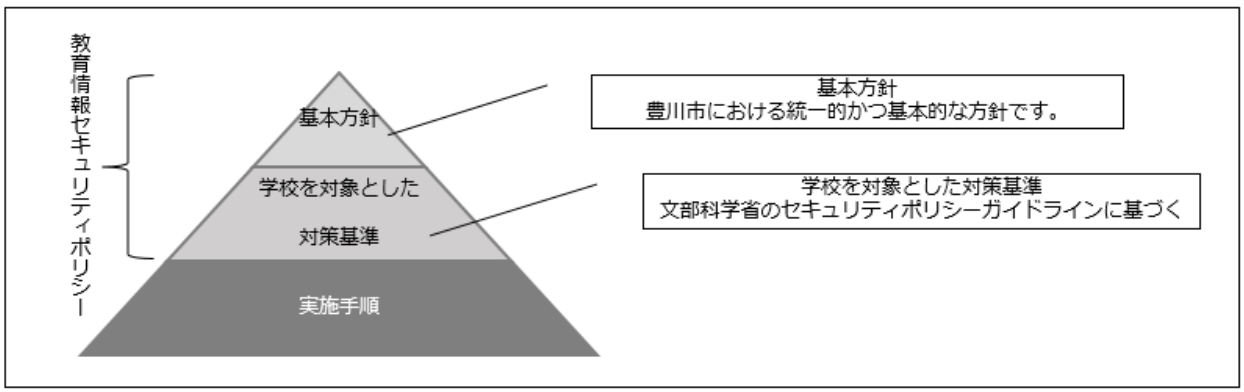
また学校は、指導要録、答案用紙、生徒指導等の記録、進路希望調査票、児童生徒等の住所録等の重要性が高い情報が保管されている場所です。児童生徒の育成においては、 学校教育に直接関わる複数の関係者により、児童生徒に関する情報が多目的で活用されており、さらに学習においても、教職員や他の児童生徒と学習活動を実践する際、児童生徒が生み出す情報は本人の思考の記録であるとともに学習評価の材料となり、必要に応じて他児童生徒に開示する等多目的に活用されることとなります。

そのため、学校教育においては、児童生徒の存在及び取り扱う情報の多様性・多目的性等を考慮した情報セキュリティ対策について講じる必要があります。

そこで、対策の基準について、市のポリシーとは別に策定したものを「教育情報セキュリティポリシー」としてここに定めるものです。

教育情報セキュリティポリシーとは、学校教育に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを総称するもので、「基本方針」及び「学校を対象とした対策基準」の 2 階層で構成されています。

豊川市教育情報セキュリティポリシーに関する体系図



※本ポリシーについては、具体的な遵守事項及び判断基準等を定める対策基準を含んでおり、公にすることにより本市教育行政運営に重大な支障を及ぼすおそれがあることから非公開とします。

目　次

第１編　基本方針	1
豊川市情報セキュリティ基本方針	2
第２編　学校を対象とした対策基準	6
第１ 目的	7
第２ 適用範囲及び用語説明	8
2.1 適用範囲	8
2.2 用語説明	8
2.3 情報資産の範囲	9
第３ 情報セキュリティ管理体制	10
3.1 体制	10
第４ 情報資産の分類と管理	13
4.1 情報資産の分類	13
4.2 情報資産の管理責任	15
第５ 物理的セキュリティ	19
5.1 サーバ等の管理	19
5.2 管理区域（情報システム室等）の管理	20
5.3 ネットワークの管理	21
5.4 教職員等の利用する端末や外部記録媒体等の管理	22
5.5 学習用モバイル端末の管理	23
第６ 人的セキュリティ	26
6.1 教育情報セキュリティ学校管理者（校長）の措置事項	26
6.2 教職員の遵守事項	28
6.3 教育委員会事務局職員の遵守事項	38
6.4 研修・訓練	38
6.5 情報セキュリティインシデントの連絡体制の整備	39

第7 技術的セキュリティ	42
7.1 コンピュータ及びネットワークの設定管理	42
7.2 アクセス制御	45
7.3 システム開発、導入、保守等	46
7.4 不正プログラム対策	49
7.5 不正アクセス対策	49
7.6 セキュリティ情報の収集	50
第8 運用	52
8.1 情報システムの監視	52
8.2 ドキュメントの管理	52
8.3 教職員等の ID 及びパスワードの管理	53
8.4 シンクライアント用 IC カード等の取扱い	54
8.5 児童生徒における ID 及びパスワード等の管理	54
8.6 特権を付与された ID の管理等	56
8.7 教育情報セキュリティポリシーの遵守状況の確認・管理	56
8.8 専門家の支援体制等	57
8.9 侵害時の対応等	58
8.10 例外措置	59
8.11 法令の遵守	60
8.12 懲戒処分	60
第9 外部委託	62
第１０　SaaS 型パブリッククラウドサービスの利用	64
10.1 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	65
10.2 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	68
10.3 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	71
10.4 約款による外部サービスの利用	72
10.5 ソーシャルメディアサービスの利用	72
第11　評価・見直し	73
11.1 学校情報セキュリティ監査及び自己点検	73
11.2 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	73

第１編　基本方針

豊川市教育情報セキュリティポリシーにおける基本方針は、豊川市における統一的かつ基本的な方針である豊川市情報セキュリティポリシー（平成 15 年 9 月 22 日策定）に準ずる。ただし、学校特有の事項については、第２編にて別に規定する。

豊川市情報セキュリティ基本方針

2.1 目的

本市が取り扱う情報資産には、市民の個人情報や行政運営上、重要な情報など、外部への漏洩等が発生した場合には重大な結果を招く情報が多く含まれている。

そのため、情報資産及び情報資産を取り扱うネットワーク、情報システムを様々な脅威から防御することは、市民の財産、プライバシー等の保護、また、行政の安定的な運営のためにも必要不可欠である。ひいては、このことが本市に対する市民からの信頼の維持向上に寄与するものである。本基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2.2 定義

（１）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。

（２）情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（３）情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（４）情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（５）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（６）完全性

情報が破壊、改ざんまたは消去されていない状態を確保することをいう。

（７）可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（８）マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）または戸籍事務等に関わる情報システム及びデータをいう。

（９）ＬGWAN接続系

人事給与、財務会計及び文書管理等ＬＧＷＡＮに接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

（10）インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（11）通信経路の分割

ＬＧＷＡＮ接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

（12）無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

2.3 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（１）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏洩・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏洩・破壊・消去等

（３）地震、落雷、火災等の災害によるサービス及び業務の停止等

（４）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

2.4 適用範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。

（２）対象範囲

本基本方針は、本市の情報資産、職員及び外部委託事業者を対象とする。

（３）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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

2.5 職員等の遵守義務

職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

2.6 情報セキュリティ対策

上記 2.3 の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（１）組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（２）情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（３）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

① マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

② LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③ インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（４）物理的セキュリティ

サーバ、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、該当機器等の管理及び運用を行うための部屋（以下「情報システム室」という。）、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

（５）人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（６）技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（７）運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時

対応計画を策定する。

（８）業務委託と外部サービスの利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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確認し、必要に応じて契約に基づき措置を講じる。

外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、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る。

（９）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的または必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

2.7 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的または必要に応じて情報セキュリティ監査及び自己点検を実施する。

2.8 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

2.9 情報セキュリティ対策基準の策定

上記 2.6、2.7 及び 2.8 に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

2.10 情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

第２編　学校を対象とした対策基準

第１　目的

学校を対象とした対策基準（以下「対策基準」という。）は、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（以下「文科省ガイドライン」という。）に基づき策定するもので、豊川市立小中学校で取り扱う情報資産の管理及び情報セキュリティ対策に関して必要となる事項を定め、学校が保有する情報資産をさまざまな脅威から守り、本市の教育行政サービスを安全に提供し、もって教育市政の円滑な運営及び教育市政に対する信頼を確保することを目的とする。

第 2 適用範囲及び用語説明

2.1　適用範囲

この対策基準が適用される範囲は、豊川市立学校設置条例（昭和 39 年 3 月 31 日条例第 18 号）第２条により設置する学校（以下「学校」という。）とする。

2.2 用語説明

ア　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。

イ　校務外部接続系情報

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。

ウ　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。

エ　校務系端末

校務系情報にアクセス可能な端末。

オ　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。

カ　学習用モバイル端末

学習系情報にアクセス可能なモバイル端末で、児童生徒が利用する端末を学習者用端末、教員のみが利用する端末を指導者用端末という（１人１台端末)。

キ　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扱うシステム。

ク　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扱うシステム。

ケ　学習系システム

学習系ネットワーク、学習系サーバ、学習用モバイル端末から構成される学習系情報を取扱うシステムで無線接続を前提としたもの。

コ　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。

2.3　情報資産の範囲

この対策基準の対象とする情報資産は、以下のとおりとする。

ア　教育ネットワーク、教育情報システム、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

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

第３ 情報セキュリティ管理体制

3.1 体制

学校の情報セキュリティ対策を推進・管理するための組織・体制を次のとおり確立する。

（１）統括教育情報セキュリティ責任者（教育長）

統括教育情報セキュリティ責任者（教育長）は、学校で取り扱う全て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）教育情報セキュリティ責任者（教育部長）

教育情報セキュリティ責任者（教育部長）は、統括教育情報セキュリティ責任者（教育長）を補佐し、学校で取り扱う情報資産の管理及び情報セキュリティ対策に関して必要となる全ての措置を実施する権限及び責任を有する。

（３）教育情報セキュリティ管理者（学校教育課長）

① 教育情報セキュリティ管理者（学校教育課長）は、教育情報セキュリティ責任者（教育部長）を補佐し、学校で取り扱う情報資産の管理及び情報セキュリティ対策に関して学校への指導及び啓発を行う権限及び責任を有する。

② 教育情報セキュリティ管理者（学校教育課長）は、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。）の情報漏洩や不正行為等による情報資産への侵害が発生した場合、教育情報セキュリティ学校管理者（校長）に対して具体的な対策についての指導及び助言を行う。

（４）教育情報システム管理者（庶務課長等）

① 学校における教育情報システムにおいては、庶務課のほか学校教育課等も管理する場合があるため、システム管理者（庶務課長「等」）としている。

② 教育情報システム管理者（庶務課長等）は、教育情報セキュリティ責任者（教育部長）を補佐し、所管するネットワーク及び情報システム等の物理的なセキュリティ対策の企画、立案及び維持管理を行う権限及び責任を有する。

③ 教育情報システム管理者（庶務課長等）は、所管するネットワーク及び情報システム等の物理的な障害が発生した場合、教育情報セキュリティ学校管理者（校長）に対して具体的な対策についての指導及び助言を行う。

（５）教育情報システム担当者（庶務課等）

① 教育情報システムを担当する職員。教育情報システム管理者同様に、庶務課以外のほか学校教育課等も担当する場合があるため、システム担当者（庶務課等）としている。

② 情報システム担当者（庶務課等）は、教育情報システム管理者（庶務課長等）の指示等に従い、教育情報システムの運用、更新等の作業を行う。

（６）教育情報セキュリティ学校管理者（校長）

① 教育情報セキュリティ学校管理者（校長）は、所管する学校で取り扱う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負う。

② 教育情報セキュリティ学校管理者（校長）は、所管する教職員から教育情報セキュリテ

ィ学校主任者（教頭）を１名、教育情報セキュリティ学校担当者（校務主任等）を複数名選任する。

（７）教育情報セキュリティ学校主任者（教頭）

教育情報セキュリティ学校主任者（教頭）は、教育情報セキュリティ学校管理者（校長）を補佐し、所管する学校で取り扱う情報資産の管理及び情報セキュリティ対策について、教育情報セキュリティ学校担当者（校務主任等）に対して具体的な指導及び助言を行う。

（８）教育情報セキュリティ学校担当者（校務主任等）

①　教育情報セキュリティ学校担当者（校務主任等）は、所管する学校で取り扱う情報資産の管理及び情報セキュリティ対策に関して教職員への指導及び啓発を行う。

②　教育情報セキュリティ学校担当者（校務主任等）は、障害時における連絡及び一次対応のほか、教育情報セキュリティ学校主任者（教頭）の指導及び助言に基づく職務を行う。

（９）教育情報セキュリティ委員会

本市の教育情報セキュリティ対策を統一的に行うため、統括教育情報セキュリティ責任者（教育長）、教育情報セキュリティ責任者（教育部長）、教育情報セキュリティ管理者（学校教育課長）、教育情報システム管理者（庶務課長等）及び統括教育情報セキュリティ責任者（教育長）が別途選任した者から構成される教育情報セキュリティ委員会を設置し、教育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。教育情報セキュリティ委員会は、毎年度、学校における情報セキュリティ対策の実施状況を確認し、必要に応じて会議を開催する。

（１０）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、承認または許可の申請を行う者とその承認者または許可者は、同じ者が兼務してはならない。

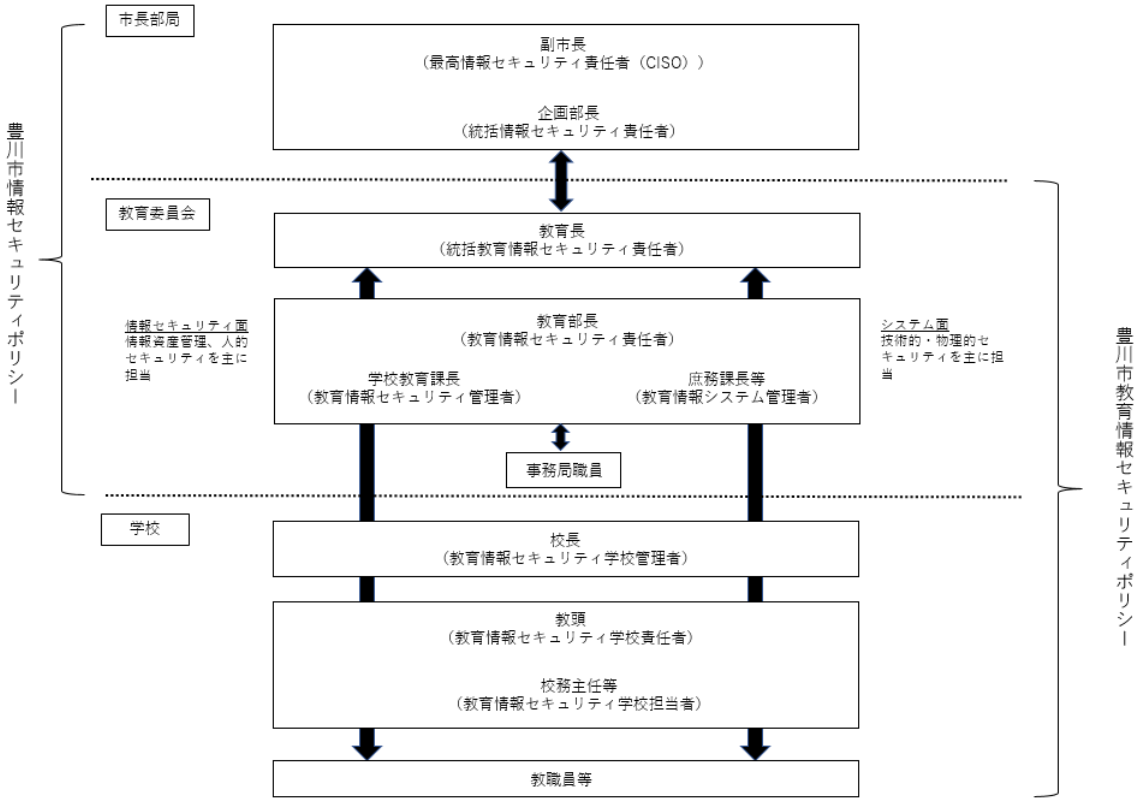
（１１）教職員等

臨時的任用教職員、非常勤講師を含めた教職員全員を、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、教育情報セキュリティ学校管理者（校長）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。

（１２）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り、教育情報セキュリティ責任者（教育部長）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。

（情報セキュリティ管理の組織体制）



第４ 情報資産の分類と管理

4.1 情報資産の分類

情報資産は、外部漏洩の影響（機密性)、情報の改ざんの影響（完全性)、情報にアクセスできなくなる影響（可用性）を踏まえ、被害を受けた場合に想定される影響の大きさをもとに、次のとおり４段階の重要性分類を行い、必要に応じてアクセス制限を行うものとする。

○重要性分類

Ⅰ	セキュリティ侵害が職員または児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす情報資産
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資産（Ⅰを除く）
Ⅲ	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情報資産（Ⅱ以上を除く）
Ⅳ	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情報資産（Ⅲ以外を除く）

（各分類の考え方）

Ⅰ：「セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす」もの、すなわち、情報が侵害された場合に甚大な被害が想定され、学校もしくは特定個人が著しい不利益を被る情報であり、要配慮個人情報を含むもの等を指す。

業務に係る特定の教職員等・教育委員会のみがアクセスする情報であり、児童生徒またはその保護者がアクセスする場合には、児童生徒本人の情報のみにアクセスすることが想定される情報である。要配慮個人情報はすべからく重要性分類Ⅰに該当する。

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。（Ⅰを除く）」もの、すなわち、情報が侵害された場合に大きな被害が想定され、学校もしくは特定個人が大きな不利益を被る情報であり、重要性分類Ⅰには該当しないものの機密性の高いもの（健康、指導、成績、進路に関わる情報等）等を指す。

業務に係る教職員等・教育委員会のみがアクセスする情報であり、児童生徒またはその保護者がアクセスする場合、児童生徒本人の情報のみにアクセスすることが想定される情報である。

※児童生徒の、生活歴・電話番号・メールアドレス・住所・生年月日・性別等の基本情報を含む学校運営に関する情報のうち重要性分類Ⅰに該当しないものと併せて取り扱われる児童生徒の氏名・所属等に関する情報については、重要性分類Ⅱとして取り扱うことが適当である。一方で、学習活動の中で生成される情報（重要性分類Ⅲ相当）の中にも、児童生徒の氏名・所属に関する情報等が含まれることは自然なことである。様々な学習系ツールの利用場面等も想定し、活用場面等に応じて、実態に即した形で運用する必要がある。

※メールアドレスについては、IDとして様々なシステムログインの場面で活用される場合も想定されることから、なりすましによる不正使用や不正アクセス等のセキュリティリスク

も考慮する必要がある。

Ⅲ：「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。（Ⅱ以上を除く）」もの、すなわち、情報が侵害された場合に学校もしくは特定個人が不利益を被る情報であり、Ⅱ以上には該当しないものの侵害の影響を無視できないもの（学校運営・学習活動・学習指導など）を指す。

たとえば、教職員等が学校運営のため日常的に取り扱う情報、児童生徒が学習活動のため日常的に取り扱う情報、保護者とのやりとりのため取り扱う学校運営に関する情報などで、Ⅱ以上を除くものを、重要性分類Ⅲとして取り扱うことが考えられる。

※ワークシートや授業中の確認テストなど、学習活動の中で生成される情報は児童生徒が教室等において相互に閲覧することが想定される情報であり、このような性質の情報資産は重要性分類Ⅲに分類される。ただし、定期考査等の採点結果等、成績に関する情報を含む情報資産は、相互に閲覧することは想定されず、重要性分類Ⅱとして取り扱うことが適当である。

※学習活動の中で生成される情報は重要性分類Ⅲに分類することを想定しているが、教職員等の評価等が加えられ、児童生徒が相互に閲覧すること等が想定されない状態のものについては、重要性分類Ⅱとして取り扱うことが適当な場合もあることに留意すべきである。

Ⅳ：上記以外のセキュリティ侵害が発生しても、学校事務及び教育活動の実施にほとんど影響を及ぼさない情報となる。

○重要性分類に基づく情報資産の例示（文科省ガイドライン）

分類	情報資産の例		
Ⅰ	・指導要録原本 ・教職員の人事情報 ・教育情報システム仕様書		
Ⅱ	○学籍関係 ・卒業証書授与台帳 ・転退学受付（整理）簿 ・転入学受付（整理）簿 ・就学児童・生徒異動報告書 ・休学・退学願等受付（整理）簿 ・教科用図書給付児童・生徒名簿 ・要・準要保護児童・生徒認定台帳 ・その他校内就学援助関係書類 ○成績関係 ・通知表 ・評定一覧表 ・進級・卒業認定資料 ・定期考査・テスト等の答案用紙（記入済のもの）	○進路関係 ・調査書 ・推薦書 ・公立高校入学者選抜に係る成績一覧表 ・私立高校入試に係る事前相談資料 ・卒業生進路先一覧等 ・進路希望調査 ・進路判定会議資料 ・進路指導記録簿 ○児童・生徒に関する個人情報 （生活歴、心身の状況、財産状況等の情報、電話番号、メールアドレス、住所、生年月日、性別等の基本情報を含むもの） ○学校教職員に関する個人情報	○教職員に割り当てた機密性の高い情報 ・情報システムログイン ID/PW 管理台帳 ・情報端末ログイン ID/PW 管理台帳 ○児童生徒の学習系情報 ・学習システムログイン ID/PW 管理台帳 ・学習用モバイル端末 ID/PW 管理台帳 ○名簿等 ・児童生徒名簿 ・保護者緊急連絡網 ・児童生徒の住所録 ・PTA 会員名簿 ・職員緊急連絡網・職員住所録 ・委員会名簿 ・PTA 役員連絡網

Ⅱ	・定期考査素点表 ・成績に関する個票等 ○指導関係 ・事故報告書・記録簿 ・生徒指導・特別指導等記録簿 ・児童・生徒等の個人写真・集合写真 ・指導記録・指導カード（児童・生徒等理解カード） ・教育相談・面接の記録・カード等 ・個別の教育支援計画（学校生活支援シート） ・個別指導計画 ・家庭訪問記録・個別面談記録 ・教務手帳 ・週ごとの指導計画（個人情報が含まれるもの）	（病歴、心身の状況、収入等の情報、電話番号、メールアドレス、住所、生年月日、性別等の基本情報を含むもの） ○健康関係 ・健康診断票 ・歯の検査表 ・心臓管理等医療情報 ・学校生活管理指導票 ・児童・生徒等健康調査票 ・児童・生徒の健康保険等被保険者証の写 ・健康診断に関する表簿 ・就学時健康診断票	○各種帳票ファイル ・指導要録作成システム等、データの入っていない帳票 ○その他 ・給食関係書類・寄宿関係資料
Ⅲ	○児童生徒の氏名 ・出席簿 ・名列表 ・座席表 ・児童生徒委員会名簿	○学校運営関係 ・卒業アルバム ・学校行事等の児童・生徒の写真 ・授業用教材、教材研究資料 ・生徒用配布プリント	○児童生徒の学習系情報 ・児童生徒の学習記録 （確認テスト、ワークシート、レポート、作品等） ・学習活動の記録（動画・写真等）
Ⅳ	○学校運営関係 ・学校・学園要覧 ・学校紹介パンフレット ・使用教科書一覧 ・教育課程編成表 ・学校設定科目の届け出 ・特色紹介冊子原稿 ・学校徴収金会計簿 （学年費、教育振興費等）	・学校行事実施計画 （避難訓練・体育祭実施計画等） ・保護者等への配布文書文例 ・各種届雛形・校務分掌表 ・ＰＴＡ資料 ・学園・学校・学年・学級だより ・学校・学園ホームページ掲載情報 ・学校行事のしおり	○学校活動の記録 ※以下は保護者の承諾がある場合に限る ・学校行事等の児童・生徒の写真 ・学習活動の記録（動画・写真・作品等）

4.2　情報資産の管理

情報資産の管理については、 豊川市個人情報の保護に関する法律施行条例（令和４年 12 月 23 日条例第 39 号)、その他の関連する法令及び規程に基づき、データの漏洩､滅失、き損、改ざん、消去、盗難等の防止を図るため必要な措置を講じなければならない。

（１）管理責任

情報資産の管理責任については以下のとおりとする。

①　管理責任

情報資産は、当該情報資産を所管する学校が適切に管理する責任を有する。

② 利用者の責任

情報資産を業務上利用する職員は、適切に利用する責任を有する。

③ 重要性の効力

データが複製または伝送された場合、当該複製等も分類に基づき管理しなければならない。

（２）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　情報を作成する教職員等は、情報の作成時に重要性分類に基づき、当該情報の分類を定め、分類に準拠した取扱いを行わなければならない。

ウ　情報を作成する教職員等は、作成途上の情報についても、取扱いを許可されていない者の閲覧や紛失・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。

（３）情報資産の入手

ア　ほかの学校等が作成した情報資産を入手した場合、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　外部の者が作成した情報資産を入手した場合、重要性分類に基づき、当該情報の分類を定め、分類に準拠した取扱いを行わなければならない。

ウ　情報資産を入手した教職員等は、その情報資産の分類が不明な場合、教育情報セキュリティ学校管理者（校長）に判断を仰がなければならない。

（４）情報資産の利用

ア　情報資産を利用する教職員等は、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教職員等は、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教職員等は、外部電磁的記録媒体（以下「外部記録媒体」、6.2（11）外部記録媒体の取扱い参照）または保存されている領域（フォルダやサーバ）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外部記録媒体または保存されている領域を取り扱わなければならない。

エ　教職員等が業務時間外に学校以外の場所で学校が保有する電子ファイルを取り扱う必要が生じた場合には、「6.2（6）リモートアクセス機能による外部での情報処理作業」で定めるリモートアクセス機能を使用することとし、外部記録媒体による持ち出しは認めない。

オ　児童・生徒またはその保護者から個人情報を収集した場合，明示した利用目的以外の利用をしてはならない。

カ　情報資産を利用する教職員等は、必要以上の複製及び配布をしてはならない。

（５）情報資産の保管

ア　教育情報セキュリティ学校管理者（校長）は、情報資産の重要性分類に従って、情報資産の保管を適切に行わなければならない。

イ　情報資産が記録された状態のＵＳＢメモリ等の外部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。ただし、記録された内容と重要性分類を照らし合わせて、教育情報セキュリティ学校管理者（校長）が認める場合は、その限りではない。

ウ　教育情報セキュリティ学校管理者（校長）は、持ち運び可能な外部記録媒体（重要性分類Ⅲ以上の情報が記録された状態のもの）を耐火、耐熱、耐水及び耐湿対策を講じたうえ施錠可能な場所（耐火金庫等）への保管等適切な管理を行わなければならない。

エ　学校が保有する電子ファイルは、全てファイルサーバによる集中管理を行い、ファイルサーバ以外へのパソコン等へは保存してはならない。ただし、画像や動画など大容量情報については、各校に配置するワークステーションの共有領域及び「6.2（11）外部記録媒体の取扱い」で定める外部記録媒体（ＵＳＢやＤＶＤ等）に保存することができる。

オ　ファイルサーバに保存する情報は年度ごとに管理し、年度が切り替わる時点で不要な情報を削除するとともに、完結した情報で長期保存が必要なものは「6.2（11）外部記録媒体の取扱い」で定める外部記録媒体に書込禁止措置を講じて保存し、耐火金庫等で保管しなければならない。

カ　本ポリシーにおける情報資産の保管、保存とは、ファイルサーバ上で期間や場所を設定して文書等を集中管理することである。そのため、例えば職員会議用としてファイルサーバ上に作成した資料を学習用モバイル端末に送信して一時的に共有することなどを禁止するものではないが、そのような場合においても重要性分類に従った管理を適切に行わなければならない。

（６）情報資産の持ち出し等

ア　教職員等は、重要性分類Ⅰ・Ⅱの情報資産を、物理的に外部に持ち出す場合、重要学校情報等外部持出申請簿（様式１）により教育情報セキュリティ学校管理者（校長）の個別許可を得なければならない。

イ　車両等により重要性分類Ⅰ・Ⅱの情報資産を物理的に運搬する場合は、必要に応じ暗号化またはパスワードの設定を行う等の安全管理措置を講じ、宛名・差出名を明記して、厳重に封印しなければならない。さらに、施錠可能なカバン等を利用し、持ち出す情報は必要最小限とし、持ち出す情報を外部で情報の複製を作らないこと。併せて、寄り道など、許可した持出先以外の場所に立ち寄らないこと。

ウ　重要性分類Ⅲの情報資産については、教育情報セキュリティ学校管理者（校長）の判断で、教職員等の外部持ち出しについての包括的許可を可とするが、その影響度により重要性分類Ⅰ・Ⅱ相当と位置付ける。

エ　重要性分類Ⅳの情報資産における外部持ち出しについては、特段の制限等を設けないが、

その影響度により重要性分類Ⅲ相当と位置付ける。

オ　外部記録媒体により、外部に電子ファイルを持ち出す場合は、限定されたアクセスの措置設定（パスワード設定によるアクセス制限や暗号化）を行わなければならない。また、外部記録媒体への電子ファイルの複製は、ワークステーションまたは教育委員会が指定するパソコンのみで行う。

カ　外部に持ち出した電子ファイルを学校に持ち帰った際は、速やかにウィルスチェックを行い、保存が必要な電子ファイルをファイルサーバに移すとともに、外部記録媒体から削除する。

キ　教育委員会または学校から利用する電子メール、外部ストレージサービスは教育委員会または学校から提供される公式サービスを利用し、私的に契約したサービスを利用してはならない。

ク　ＦＡＸによる情報の送信は、限定されたアクセスの措置（アクセス制限や暗号化）が不可能であること、誤送信のリスクがあることに鑑み、送信相手がＦＡＸ受信を指定してきた場合にのみ利用することが望ましい。

ケ　外部への持ち出しのほか、教職員等が個人で作成した教材データを教室に持ち込む際に外部記録媒体を使用するような内部利用の場合も含め、外部記録媒体の取扱いについては「6.2（11）外部記録媒体の取扱い」を遵守すること。

コ　電子メールの取扱いについては、「6.2（12）電子メールの利用制限」を遵守すること。

サ　勤務時間外に学校以外の場所で電子ファイルを取り扱う場合については、「4.3(4)エ勤務時間外における情報資産の利用」のとおり外部記録媒体ではなくリモートアクセス機能により行うこと。

（７）情報資産の共有（提供・公表）

情報資産の共有とは、保護者等の関係者に情報（お知らせ含む）を提供することや、学校外の不特定多数の人に情報を公表することを指す。教育情報セキュリティ学校管理者（校長）は、共有する情報が正しい内容であることを事前に確認し、誤共有を防がなければならない。

（８）情報資産の廃棄

教育情報セキュリティ学校管理者（校長）は、データの消去および機器の廃棄については下記を参照し、データ消去が確実に行われるよう留意すること。

ア　情報資産を廃棄する教育委員会事務局職員又は教職員等は、重要性分類Ⅲ以上の情報が記載された紙媒体の書類を廃棄する場合には、内容が復元できないように細断、熔解またはこれに準ずる方法にて廃棄しなければならない。

イ　情報資産を記録している外部記録媒体を利用しなくなった場合、当該媒体の初期化等により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。

ウ　業者に廃棄委託する場合、廃棄する情報資産を業者が引き取る際、教育委員会事務局職員又は教職員等が立ち会わなければならない。

第５ 物理的セキュリティ

5.1 サーバ等の管理

サーバ等のハードウェアは、情報システムの安定的な運用のために適切に管理する必要があり、管理が不十分な場合、情報システム全体に悪影響が及んだり、業務の継続性に支障が生じるおそれがある。このことから、サーバ等の設置や保守・管理、配線や電源等の物理的セキュリティ対策を規定する。

（１）機器の取付け等

教育情報システム管理者（庶務課長等）は、ネットワーク機器及び情報システム機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切な固定を行う等必要な措置を講じなければならない。

ア　学校は、児童生徒が日常的に過ごす場であり、学校のそれぞれの部屋についての入室制限等の管理の徹底が困難である場合も考えられることから、重要な情報資産を格納する校務系サーバ等については、教育委員会が集約して管理することとし、サーバ等は、企画部情報政策課の電算室（本庁北庁舎５階）に設置し、集中管理する（外部クラウドサービスを利用する場合は除く）。

イ　情報政策課の電算室以外にサーバ等を置くことはできず、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。

ウ　落雷による過電流や、停電等による電源供給停止をはじめとした予備電源等の詳細は、情報政策課所管サーバ等の措置に準ずる。

（２）通信ケーブル等の配線

学校の執務室に通信ケーブル等を配線する場合に、ケーブルを剥き出しにしたままにしておくと、踏まれるなどして損傷する可能性が高くなることから必要な措置を講じなければならない。

ア　教育情報システム管理者（庶務課長等）は、教育情報セキュリティ学校管理者（校長）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　教育情報システム管理者（庶務課長等）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教育情報セキュリティ学校管理者（校長）から損傷等の報告があった場合、必要により連携して対応しなければならない。

ウ　教育情報システム管理者（庶務課長等）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　教育情報システム管理者（庶務課長等）は、自らまたは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また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。

（３）サーバの冗長化（バックアップ）

成績処理等、教員が毎日の業務において活用するものについては、サーバが緊急停止した場合、校務の遂行に多大な影響を及ぼすことが考えられることから、冗長化（バックアップ）を行うことが重要である。そこで、教育情報システム管理者（庶務課長等）はサーバ等の機器が緊急停止した場合にも業務を継続できるようにするために、バックアップシステムを設置しなければならない。

（４）機器の定期保守及び修理

ア　教育情報システム管理者（庶務課長等）は、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　外部の事業者に故障を修理させるにあたり、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）外部データセンターへの機器の設置

外部クラウドサービスを利用している場合（外部委託事業者のデータセンターに、システム機器等を設置している場合）は、定期的に物理的なセキュリティ状況を確認する必要がある。

ア　教育情報システム管理者（庶務課長等）は、外部委託事業者を定期的に訪問し、定期報告では把握しきれない設置室内の状況の変化、当該外部委託事業者の要員の変化等を把握する。

イ　教育情報システム管理者（庶務課長等）またはその指名した者によるデータセンター内部への立入りが、当該データセンターのセキュリティポリシーに違反するなどして外部委託事業者を訪問できない場合は、訪問調査に代えて第三者による情報セキュリティ監査報告書、外部委託事業者の内部監査部門による情報セキュリティ監査報告書等によって確認する。

（６）機器の廃棄等

教育情報システム管理者（庶務課長等）は、機器を廃棄またはリース返却等する場合、機器内部の記憶装置から、全ての情報を消去の上、復元できないように処置した上で廃棄等しなければならない。

5.2 管理区域（情報システム室等）の管理

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、当該機器等の管理及び運用を行うための部屋のことであり、本市では企画部情報政策課の電算室のことである。管理区域へ入退室しようとする者は、情報政策課の定める実施手順に従い、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。

5.3 ネットワークの管理

ネットワーク利用における通信回線及び通信回線装置が適切に管理されていない場合は、ネットワークそれ自体のみならず、ネットワークに接続している情報システム等に対しても損傷や不正アクセス等がおよぶおそれがある。このことから、外部ネットワーク接続等の通信回線及び通信回線装置の管理にセキュリティ対策を規定する。

（１）教育ネットワークの定義

学校へ整備する教育ネットワークの定義は以下のとおり。各ネットワーク間の通信経路は物理的または論理的に分離し、それぞれで適切な安全管理措置を講じなければならない。

○教育ネットワーク

分類	定義	ネットワーク名称
地域イントラネット	本庁舎や支所等と学校をつなぐ地域のネットワーク	行政系ネットワーク（LGWAN)、校務系ネットワーク（校務システム等)、校務外部接続系ネットワーク（インターネット）
校内ネットワーク	GIGA 端末の無線接続を前提としたネットワークで、校内で完結するもの	学習系ネットワーク（無線接続系）
市町村立学校ネットワーク	教職員等の人事管理等を扱うネットワーク	県端末用ネットワーク

（２）通信回線及び通信回線装置の管理

統括教育情報セキュリティ責任者（教育長）及び教育情報システム管理者（庶務課長等）は、学校の通信回線及び通信回線装置を、教育情報セキュリティ学校管理者（校長）と連携し、適切に管理し、通信回線及び通信回線装置に関連する文書（通信回線の敷設図等）を適切に保管し、外部への漏洩がないよう厳重に管理しなければならない。

① インターネット経由による標的型攻撃等のリスクへ対応するため、校務系ネットワークはインターネット接続を遮断し、校務外部接続系ネットワークによりＷｅｂ閲覧する。校務外部接続系ネットワークで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、機微な個人情報の取扱いを禁止する。

② 校務外部接続系ネットワークでＷｅｂページ利用をし、そこで得た情報を校務系ネットワークに持ち込む際には、必ずウイルス検索を実施し、問題があれば使用を中止するなどの措置を講じなければならない。

③ 無線ＬＡＮ環境は、教育ネットワークでの使用を原則とする。接続できるコンピュータを決め、一般への開放は原則行わない。

④ 学校は、教育委員会が整備したネットワークを教育委員会の許可なく増設及び設定変更等を行ってはならない。

⑤　学校が独自に整備したパソコン及びプリンタについて、新たに教育ネットワークへ接続する場合は、情報機器等ネットワーク接続申請書（様式２）により教育情報システム管理者（庶務課長等）の許可を得たうえで接続しなければならない。ネットワークへ接続できる端末は信頼性を考慮し、その機種や種類は教育情報システム管理者（庶務課長等）が定めることとする。

（３）外部ネットワークへの接続

統括教育情報セキュリティ責任者（教育長）及び教育情報システム管理者（庶務課長等）は、通信回線による外部ネットワークへの接続を必要最低限のものに限定し、できる限り接続ポイントを減らさなければならない。なお、接続ポイントを減らすこと自体は、セキュリティ対策はもとよりネットワークひっ迫化対策にもなる。

（４）機密を要する情報システムで使用する回線

統括教育情報セキュリティ責任者（教育長）及び教育情報システム管理者（庶務課長等）は、所管する情報システムにおいて重要性Ⅰ～Ⅲの情報資産を取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うえ、適切な回線を選択しなければならない。

（５）ネットワークで使用する回線

ア　ネットワークに使用する回線は送信途上においてデータの破壊、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が実施されたものでなければならない。

イ　統括教育情報セキュリティ責任者(教育長)及び教育情報システム管理者(庶務課長等)は、ネットワークで使用する回線を選択するにあたって、断続的な運用（可用性）を考慮しなければならない。

（６）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）

統括教育情報セキュリティ責任者（教育長）及び教育情報システム管理者（庶務課長等）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。

5.4 教職員等の利用する端末や外部記録媒体等の管理

教職員等が利用するパソコン、モバイル端末及び外部記録媒体等が適切に管理されていない場合、不正利用、紛失、盗難、情報漏洩等の被害を及ぼすおそれがある。このことから、これらの被害を防止するために、教職員等の利用するパソコン、モバイル端末及び外部記録媒体等の盗難及び情報

漏洩防止策、持ち出し・持ち込み等に関する対策を規定する。

（１）教職員等の利用する端末について

ア　教育情報セキュリティ学校管理者（校長）は、学校の執務区域等の端末等について、盗難防止のための措置を講じ、併せて外部記録媒体の使用時以外の施錠管理等の措置を講じなければならない。また、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。

イ　教育情報システム管理者（庶務課長等）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、加えて多要素認証の実施等、使用する目的に応じた適切な物理的措置を講じるほか、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。

ウ　教育情報システム管理者（庶務課長等）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。強固なアクセス制御による対策を講じたシステム構成の場合、重要性分類 II 以上の情報資産を取り扱う端末に対し、当該端末の状況および通信内容を監視し、異常、あるいは不審な挙動を検知する仕組み（ふるまい検知）等の活用を検討し、適切な対策を講じること。

エ　教育情報システム管理者（庶務課長等）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。

5.5 学習用モバイル端末の管理

GIGA スクール構想における１人１台端末の整備に伴い、学校内外で利用する学習用モバイル端末に対してのセキュリティ対策が必要である。

学校内では、校内無線 LAN 等を用いて、クラウド環境にあるデジタル教科書等をはじめとした教育資源の活用のほか、ワープロソフトや表計算ソフト、プレゼンテーションソフトの活用や、グループウェアやファイル共有といった学習用ツールを利用する際のセキュリティ対策が必要である。

学習用モバイル端末は、教室での活用のみならず、学校外における調べ学習や休み時間等における児童生徒による自主的な学習等、様々な学習活動で使用することが期待されている。このため、児童生徒に対する学習用モバイル端末の管理方法等についての指導を前提として、可能な限り、児童生徒が学習活動で自由に端末を活用できるよう、教育委員会事務局と学校が協力の上、配慮していくことが重要である。

（１）不適切なウェブページの閲覧防止

教育情報システム管理者（庶務課長等）及び情報セキュリティ学校管理者（校長）等は、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。

（２）マルウェア感染対策

教育情報システム管理者（庶務課長等）は、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。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。

（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。そのため教育情報システム管理者（庶務課長等）は、児童生徒の利用アカウントに対してアプリケーションのインストール・アンインストールを自由に行う権限を与えないことや、 MDM（モバイル端末管理 Mobile Device Management）等によりセキュリティ制御を行うこと。

（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ため、教育情報システム管理者（庶務課長等）は MDM 等によりセキュリティ制御を行うこと。

（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。具体的には MDM などにより管理者が離れた場所からでも端末をロックする、あるいは必要に応じてデータの削除や端末の初期化を行うリモートワイプ機能などの対策を教育情報システム管理者（庶務課長等）は講じること。また、これらの機能を事前に周知すること自体が盗難、転売対策にもなる。

学校情報セキュリティ学校管理者（校長）は、学習用モバイル端末の盗難防止のため、保管庫の施錠、警備委託対象校舎での保管等、物理的措置を講じなければならない。

（６）端末の持ち出し

学校情報セキュリティ学校管理者（校長）が教育上必要と判断する場合、学習用モバイル端末を学校外へ持ち出す、あるいは家庭へ持ち帰りさせることができる。

（７）学校情報セキュリティ学校管理者（校長）は、学校内外での学習用モバイル端末の運用ルールを作成しなければならない。また、以下について、各学校で対応できるよう整理しておく必要がある。

① 学校外での学習用モバイル端末の取扱い。

② 緊急時の対応方法。

③ 学校外での学習用モバイル端末利用におけるインターネットアクセス及びセキュリティ対策。

（８）学習用モバイル端末にアプリケーション等をインストールする必要があるときは、ソフトウェアインストール申請書（様式３）により学校情報セキュリティ学校管理者（校長）の許可を得なければならない。

（９）原則として、児童生徒に対し、個人で利用するためのメールアカウントは付与しない。

第６ 人的セキュリティ

6.1 教育情報セキュリティ学校管理者（校長）の措置事項

教育情報セキュリティ学校管理者（校長）が、当該学校における情報セキュリティ対策のため実施すべき措置について規定する。なお、具体的な教職員等の遵守事項については「6.２．教職員等の遵守事項」に規定する。

（１）情報資産の管理

①　情報資産の持ち出し及び持ち込みの記録管理

教育情報セキュリティ学校管理者（校長）は、教職員等による情報資産の外部持ち出しについて、記録管理しなければならない。

②　情報資産の廃棄管理

ア　教育情報セキュリティ学校管理者（校長）は、廃棄処理を外部に委託する場合は、学校の外に委託業者が持ち出す行為に教職員等が立ち会うように指示し、誤廃棄を予防しなければならない。

イ　教育情報セキュリティ学校管理者（校長）は、廃棄した情報資産を記録管理しなければならない。

（２）教職員等の情報セキュリティ意識醸成

①　セキュリティ認識の向上

教育情報セキュリティ学校管理者（校長）は、教職員等に対して、日頃から情報セキュリティに関する話題を積極的に提供し、教育情報セキュリティ研修を受講させるなど、積極的にセキュリティ認識の向上を図らなければならない。

②　意識の醸成と風通しのよい関係性維持

教育情報セキュリティ学校管理者（校長）は、校内でセキュリティインシデント（情報漏洩事故や機器等の物理的障害）につながりかねないヒヤリ・ハット事案を抑止するために、教職員等が事案を発見した際に、ただちに対処し、速やかに報告が上がるよう、教職員等に対する情報セキュリティ意識の醸成と風通しのよい関係性維持に努めなければならない。

③　教育情報セキュリティポリシー等の閲覧容易性の確保

教育情報セキュリティ学校管理者（校長）は、教職員等が常に教育情報セキュリティポリシー等を閲覧・確認できるように配慮しなければならない。

（３）端末等の持ち出し及び持ち込みの記録

教育情報セキュリティ学校管理者（校長）は、情報資産のみならず端末そのもの等の持ち出し及び持ち込みについても記録し、保管しなければならない（ただし、学習用モバイル端末については日常的な持ち帰り等が想定されるためこの限りではない）。

（４）教職員等への教育情報セキュリティポリシー等の遵守指導

教育情報セキュリティ学校管理者（校長）は、新規採用教職員等及び他自治体から新規赴任した教職員等、及び非常勤及び臨時の教職員に対し、教育情報セキュリティポリシー等遵守すべき内容を理解・浸透するように指導を行わなければならない。

（５）新規ソフトウェア及びコンテンツの導入・利用判断

教育情報セキュリティ学校管理者（校長）は、教職員等から、導入したソフトウェア・コンテンツの制限解除や、業務上新たなソフトウェア・コンテンツの導入について、事前に相談があった場合は、教育情報システム管理者（庶務課長等）に上申して、判断を仰がなければならない。

① 教育ネットワークで使用するパソコン等の端末に、無断でソフトウェアを導入してはならない。

② シンクライアント環境へのソフトウェアの導入は原則行わない。必要が生じたときには教育情報システム管理者(庶務課長等)に申し出る。特性上、全校一括導入となるため、必要性や安全性を考慮した上で導入を決定する。

③ ただし、シンクライアント以外の環境(ワークステーションや教育用ノートパソコン等)へは、教育上の必要性や安全面、互換性等を考慮した上で、ソフトウェア（原則有償のもの）を導入することができる。事前に教育情報システム管理者（庶務課長等）に上申して判断を仰がせたうえで、教育情報セキュリティ学校管理者（校長）へソフトウェアインストール申請書（様式３）により申請させること。なお、安全面の観点から積極的な導入を促すものではないことに留意すること。

④ パソコンやサーバ等に、不正にコピーしたソフトウェアやファイル共有機能を有したソフトウェアを導入してはならない。

⑤ 学習用モバイル端末へのアプリケーション等インストールについては、「5.5 学習用モバイル端末の管理」を参照のこと。

（６）インターネット接続及び電子メール利用の制限

① 教育情報セキュリティ学校管理者（校長）は、教職員等に業務端末による作業を行わせる場合において、業務以外でのインターネット接続及び電子メールの利用をしないよう教職員等に指導しなければならない。なお、Web フィルタリングの設定について、教職員等から相談があった場合は、教育情報システム管理者（庶務課長等）に上申して、判断を仰がなければならない。

② パソコンやモバイル端末の機能は、教職員等の業務内容に応じて、不必要な機能については制限することが適切である。

（７）校内及び執務室での管理

教育情報セキュリティ学校管理者（校長）は、教職員等と協力して以下を管理しなければな

らない。

① 来校者及びその入退状況を適切に把握・管理しなければならない。

② 名札着用などにより、来校者が第三者であることが識別できるように努めなければならない。

③ 地域住民、保護者などに校内施設を開放する場合、可能な限り執務等開放していない施設へは入場できないよう制限を設けなければならない。

（８）自己点検の実施

① 教育情報セキュリティ学校管理者（校長）は、年１回及び必要に応じて、学校の自己点検を行わなければならない。

② 教育情報セキュリティ学校管理者（校長）は、自己点検の結果を教育情報セキュリティ委員会（事務局：庶務課）に報告しなければならない。

③ 詳細については「11.1 学校情報セキュリティ監査及び自己点検」参照のこと。

6.2 教職員の遵守事項

教職員等が情報資産を不正に利用したり、適正な取扱いを怠った場合、コンピュータウイルス等の感染、情報漏洩等の被害が発生し得る。このことから、豊川市教育情報セキュリティポリシーの遵守や情報資産の業務以外の目的での使用の禁止等、教職員等が情報資産を取り扱う際に遵守すべき事項を明確に規定する。教職員だけでなく、非常勤職員及び臨時職員、外部委託事業者についても、遵守事項を定めなければならない。情報漏洩事案の多くが、教職員等の過失による規定違反から生じており、職場の実態等を踏まえつつ、教職員等の遵守事項を適正に定めるとともに、規程の実効性を高める環境を整備することが重要である。

（１）豊川市教育情報セキュリティポリシー等の遵守

教職員は、豊川市教育情報セキュリティポリシー及びこれに基づく文書に定められている事項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がある場合には、速やかに教育情報セキュリティ学校管理者（校長）等権限のある者に相談し、指示を仰がなければならない。

（２）執務上での管理

① 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。

② 来校者等への対応

来校者等を執務室に入れる場合には、教育情報セキュリティ学校管理者（校長）等の許可を求めなければならない。

③ 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、外部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または教育情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや外部記録媒体、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

① 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。

② 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。

ア 教育ネットワークで使用するパソコン等の端末に、無断でソフトウェアを導入してはならない。

イ シンクライアント環境へのソフトウェアの導入は原則行わない。必要が生じたときには教育情報セキュリティ学校管理者（校長）の許可を得たうえで、教育情報システム管理者（庶務課長等）に申し出る。特性上、全校一括導入となるため、必要性や安全性を考慮した上で導入を決定する。

ウ ただし､シンクライアント以外の環境(ワークステーションや教育用ノートパソコン等)へは、教育上の必要性や安全面、互換性等を考慮した上で、教育情報セキュリティ学校管理者（校長）へソフトウェアインストール申請書（様式３）を申請することによりソフトウェア（原則有償のもの）を導入することができる。申請にあたっては、事前に教育情報セキュリティ学校管理者（校長）の許可を得たうえで、教育情報システム管理者（庶務課長等）に上申して判断を仰ぐこと。なお、安全面の観点から積極的な導入を促すものではないことに留意すること。

エ パソコンやサーバ等に、不正にコピーしたソフトウェアやファイル共有機能を有したソフトウェアを導入してはならない。

オ 学習用モバイル端末へのアプリケーション等インストールについては、「5.5 学習用モバイル端末の管理」を参照のこと。

③ 教職員等は、支給端末の利用において、以下のカスタマイズを無断でしてはならない。業務上機器のカスタマイズ等が必要になったときには､教育情報システム管理者(庶務課長等)に確認するとともに、情報機器カスタマイズ等申請書（様式４）により教育情報セキュリティ学校管理者（校長）の許可を得たうえで行うものとする。

ア セキュリティ機能に関する設定変更

イ メモリ増設等の改造

④ 教職員等は、情報機器等を利用する場合は、盗難・紛失リスクに備えての安全管理をすること（パソコンへのセキュリティワイヤー等)。特に、共用しているモバイル端末の場合、管理者が不明確になりやすく、その結果として所在不明になりやすいので特に注意すること。

⑤ 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。

⑥　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。

⑦　支給端末は、外部へ持ち出してはならない。ただし、業務上必要な場合には、情報機器等外部持出申請簿（様式５）により学校情報セキュリティ学校管理者（校長）の許可を得たうえで持ち出すことができる（ただし、学習用モバイル端末については日常的な持ち出し等が想定されるためこの限りではない）。

（４）私物パソコン等（支給以外のパソコン、モバイル端末及び外部記録媒体等）の業務利用

教職員等は、次の（５）（６）の場合を除き、私物パソコン等（支給以外のパソコン、モバイル端末及び外部記録媒体等）を原則業務に利用してはならない。

（５）校務系システムの障害等で２日以上パソコン等端末を使用できない場合

校務系システムの障害等で２日以上パソコン等端末を使用できない場合、私物パソコン利用申請書（様式６）により教育情報セキュリティ学校管理者（校長）の許可を得て持ち込み、校務事務を行うことができる。学校内で私物パソコンを利用して業務を行う場合は、次の安全管理措置を講じなければならない。

①　市ネットワークへの接続は禁止とする。また、独自環境によるインターネット接続も行わない。

②　ログインパスワードの入力が必要となるように設定する。

③　OS のアップデートを行い、ウイルス対策ソフトをインストールした上で、常時パターンファイルの更新をし、最新の状態にする。

④　不正にコピーしたソフトウェアやファイル共有機能を有したソフトウェアをインストールしない。

⑤　私物パソコンで取り扱う情報は最低限のものとし、重要性分類Ⅰ・Ⅱの情報は原則取り扱わない。使用後は私物パソコンのハードディスク装置から全ての情報を消去したことを教育情報セキュリティ学校管理者（校長）の確認を受けなければならない。

（６）リモートアクセス機能による外部での情報処理作業

教育委員会が整備した、リモートアクセス機能を使って自宅等で校務事務を行う場合は、リモートアクセス利用申請書（様式７）により教育情報セキュリティ学校管理者（校長）の許可を得なければならない。その後、許可内容を教育情報システム管理者（庶務課長等）が確認し、接続設定を行う。リモートアクセス機能を利用する場合は、次の安全管理措置を遵守しなければならない。

①　ウイルス対策ソフトをインストールした上で、常時パターンファイルの更新をし、最新の状態にする。

②　使用するパソコンのＯＳのアップデートを行い、セキュリティを確保する。

③　不正にコピーしたソフトウェアやファイル共有機能を有したソフトウェアをインストールしない。

④　上記対策を施したパソコン以外では操作しない。

⑤　学校以外の場所では情報の印刷、撮影は行わない。
⑥　本機能は衆人環境下での使用を禁止する。
⑦　共有用カードはリモートアクセスを使用できない。

（７）情報機器等や外部記録媒体等の持ち出し及び教育委員会・学校が構築・管理している環境の外部における情報処理作業の制限

①　教職員等は、情報機器等、外部記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、教育情報セキュリティ学校管理者（校長）の許可を得なければならない。外部に持ち出す場合の申請にあたっては、このポリシーにおいて規定された取扱いを遵守すること。
②　教職員等は、外部で情報処理業務を行う場合には、教育情報セキュリティ学校管理者（校長）の許可を得なければならない。
③　学校において余剰台数を活用した持ち出し専用パソコン等を管理する場合は、万一当該パソコンを紛失した場合に、記録されている情報を容易に特定するため、日常において当該パソコンに情報を記録しないようにし、持ち出し時においては持ち出し情報が必要最小限であるかどうか確認を行った上で情報を記録し、返却時においては情報の完全削除をするといった運用を行うこと。

（８）ID の取扱い

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

①　自己が利用している ID は、他人に利用させてはならない。
②　共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。
③　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、教育情報システム管理者（庶務課長等）に申し出なければならない。

（９）パスワードの取扱い

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

①　教職員が業務上使用するパスワードは原則８桁以上の文字数とし、英数字混在の文字列を使うなど、他の者が推測しにくいものでなければならない。
②　パスワードは秘密にし、他人に知られないようにしなければならない。また、他者からの照会等には一切応じてはならない。
③　パスワードを忘れた場合、他の者に知られた場合またはその恐れがある場合には、速やかにパスワードの変更をしなければならない。
④　パスワードが流出した恐れがある場合には、速やかに教育情報システム管理者（庶務課長等）に報告し、パスワードを変更しなければならない。
⑤　端末にパスワードを記憶させてはならない。
⑥　管理者権限は、教育情報セキュリティ学校管理者（校長）が管理し、管理者権限にア

クセスできるパスワードの交付は必要最小限の教職員に制限しなければならない。

⑦　教職員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）。

（１０）シンクライアント用 IC カードの取扱い

教職員等は、シンクライアント用 IC カードに関し、次の事項を遵守しなければならない。

①　認証に用いる IC カードは個人用と共有用の２種類とする。

②　個人用の IC カードを、教職員間で共有してはならない。

③　シンクライアントシステムについては、業務上必要のないときはログオフし、IC カードを端末のスロットから抜いておかなければならない。

④　個人用の IC カードは勤務校だけでなく、他校若しくは市教育委員会事務局へ持ち出して使用することができるが、持ち出しの際には紛失等に注意すること。

⑤　共有用の IC カードは教育情報セキュリティ学校管理者（校長）が適切に管理し、校外への持ち出しは禁止する。

⑥　IC カードを紛失した場合には、速やかに教育情報システム管理者（庶務課長等）に報告し、指示に従わなければならない。

⑦　教育情報システム管理者（庶務課長等）は IC カードの紛失等の通報があり次第、当該アカウントを使用したアクセスを速やかに停止しなければならない。

⑧　IC カードを切り替える場合、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。

⑨　教職員は、業務上必要がなくなった場合は、カード情報を抹消するよう、教育情報システム管理者（庶務課長等）に申し出なければならない。

（１１）外部記録媒体の取扱い

教職員等は、外部記録媒体（ＵＳＢやＤＶＤ等）の取扱いに関し、次の事項を遵守しなければならない。

①　外部記録媒体は、公用購入したものでなければならない。公用購入した外部記録媒体は USB 等外部記録媒体管理簿（様式８）に記載し、教育情報セキュリティ学校管理者（校長）の承認を得なければならない。

②　外部記録媒体は以下の場合に使用することを想定する。

ア　教職員が個人で作成した教材を授業等で使用するなど、学校内でのデータ移動が必要な場合。

イ　学校外で行う研修や会議等で使用する場合

ウ　完結した情報で長期保存する場合

エ　画像や動画を保存する場合

③　教育情報セキュリティ学校管理者（校長）の承認を受けた外部記録媒体は、学校名、番号、使用開始日を表記しなければならない。

④　外部記録媒体は、必要な時にのみ校務用ワークステーション、教室用ノートパソコン及び指導者用端末へ接続して使用する。使用しない時は耐火金庫等で保管しなければならない。

⑤　外部記録媒体を使用する時は、USB 等外部記録媒体使用簿（様式９）に必要事項を記入しなければならない。

⑥　外部記憶媒体をパソコン等の端末と接続して使用する際には、必ずウイルス検索を実施し、「(14) 不正プログラム対策に関する教職員等の遵守事項」に基づきただちに対策を実施すること。

⑦　情報を記録している外部記録媒体が不要になった場合、外部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。また、USB 等外部記録媒体管理簿（様式８）に廃止年月日と処理担当者を記録しなければならない。

⑧　私物の外部記録媒体は、学校内に持ち込んではならない。

（１２）電子メールの利用制限

教職員等は、電子メールの利用に関し、次の事項を遵守しなければならない。

①　電子メールの利用は業務上必要な範囲で適正に行わなければならない。

②　不正な情報の持ち出しを防止するため、自動転送機能を用いた電子メールの転送を禁止する。また、業務上必要のない送信先にメールを送信してはならない。

③　複数人に電子メールを送信する場合は、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らないようにＢＣＣの機能を利用する。

④　重要な電子メールを誤送信した場合、教育情報セキュリティ学校管理者（校長）に報告するとともに、適切な措置を講じなければならない。また、必要に応じて教育情報セキュリティ管理者（学校教育課長）に報告し、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。

⑤　規約に基づかずに利用されているフリーメールサービス等に対しては、外部への不正な情報の持ち出し等に利用される場合がある。そこで、メールアカウントは、県及び市のネットワークで定められたもののみを利用し、フリーメール等の利用をしてはならない。ただし、学習用モバイル端末でコンテンツ利用のためにフリーメール等アカウントを取得する必要がある場合等はこの限りではない。

⑥　重要性分類Ⅰ・Ⅱの情報を電子メールで送信することは原則禁止とする。業務上やむを得ず送信する場合には、4.3（情報資産の取扱い）の規定に準じて取り扱うものとし、送信する情報については、パスワード設定等の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。

⑦　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。また、大容量のファイルを添付して送信してはならない。最大約５ＭＢまでとする。

⑧　差出人、添付ファイルまた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）にアクセスせずに削除する。大量のスパムメール等の受信または送信を検知した場合は、速やかに教育情報システム管理者（庶務課長等）に報告し指示を仰ぐ。

（１３）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

教職員等は、クラウドサービス、ソーシャルメディアサービスの利用に関し、次の事項を遵守しなければならない。

① 強固なアクセス制限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Ⅱ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。

② 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。

③ 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。

（１４）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。

① 情報機器等において、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 外部からデータまたはソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

③ 差出人が不明また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 教育情報システム管理者（庶務課長等）は、端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

⑤ 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。

⑥ ウイルス情報を、常に確認しなければならない。

⑦ コンピュータウイルス等の不正プログラムに感染した場合または感染が疑われる場合は、被害拡大を防ぐため、速やかに以下の対応を行わなければならない。

ア　パソコン端末（校務用端末等）の場合

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

イ　学習用モバイル端末（指導者用端末及び学習者用端末）の場合

無線 LAN につながる業務端末の場合は、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。

その後、速やかに教育情報システム管理者（庶務課長等）に報告し、指示によりコンピュータウイルス感染報告書（様式１０）を提出しなければならない。

（１５）電子署名・暗号化

教職員等は、情報資産の分類により定めた管理体系に従い、外部に送るデータの機密性または完全性を確保することが必要な場合には、電子署名、暗号化また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。

（１６）無許可ソフトウェアの導入等の禁止

① インターネットからソフトウェアをダウンロードし、パソコンやモバイル端末に導入すると、不正プログラムへの感染、侵入の可能性が高まることや、導入済みのソフトウェアに不具合が発生する場合もあり、許可を得ない導入は禁止する必要がある。

② また、不正にコピーしたソフトウェアは、ライセンス違反や著作権法違反となることから、明確に禁止しなければならない。なお、許可を得てインターネットからソフトウェアをダウンロードする場合においても、提供元のサイト等の信頼性が確保できることを確認した上で入手する必要がある。

③ 上記理由により教職員等は、パソコンやモバイル端末へのソフトウェア無断導入を禁止する。業務上必要がある場合等への対応については、「6.2（3）②支給端末への外部ソフトウェア無断インストールの禁止」のとおり。

（１７）機器構成の変更（カスタマイズ）の制限

教職員等が、独自の判断でカスタマイズを行った場合、パソコンを故障させたり、ネットワーク全体にも悪影響を及ぼす可能性がある。

そのため、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。業務上必要がある場合等への対応については、「6.2（3）③支給端末への無断カスタマイズ禁止」のとおり。

（１８）無許可でのネットワーク接続の禁止

セキュリティ上、ネットワークとの接続には適切な管理が必要であることから、教職員等は、教育情報システム管理者（庶務課長等）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。

（１９）業務以外の目的でのウェブ閲覧の禁止

業務外の外部サイトを閲覧している場合、不正プログラムの感染、侵入の可能性が高まるため、業務以外の目的でのウェブ閲覧は禁止しなければならない。また、閲覧先サイトのサーバにドメイン名等の組織を特定できる情報がログとして残ることにより、外部から指摘を受けるようなことがあってはならない。そのため、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。

（２０）外部からのアクセス等の制限

教職員等が外部から内部のネットワークまたは教育情報システムにアクセスすることを制限する。業務上必要がある場合等への対応については、「6.2（6）リモートアクセス機能による外部での情報処理作業」のとおり。

（２１）児童生徒への指導事項

学校における情報の取扱いは、教職員等のみならず、児童生徒も含まれる。 GIGA スクール整備以降、児童生徒による学習活動のデジタルシフトが加速化しており、児童生徒による情報セキュリティの確保は、学校の情報セキュリティ確保のなかで大きな比重を占めるものとなってきた。そこで、教職員等は、児童生徒に学習用モバイル端末等を利用させるにあたり、以下の事項について指導しなければならない。

① 学習用途の利用限定

学習用モバイル端末及び学習系クラウドサービスは、学校での教育活動の目的でのみ利用すること。

② 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。

③ ウイルス対策ソフトウェアの管理

ウイルス対策ソフトウェアは常に最新の状態に保つこと。

④ 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。

⑤ 学習系情報は学習系クラウドに保管

学習用モバイル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、端末本体へのローカル保存は必要最小限とすること。

⑥ ソフトウェアの無断インストール禁止

無断でソフトウェアをインストールしないようにすること。

⑦ 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（チャット等）のみを利用すること。

⑧ ウイルス感染が疑われる場合の報告

学習用モバイル端末が動かない、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、速やかに担任教員等に報告すること。報告を受けた担任教員等は「6.2（14）不正プログラム対策に関する教職員等の遵守事項」のとおり適切に対応すること。

⑨ 端末の安全な取扱い

学習用モバイル端末は大事に取り扱い、盗難・紛失・破損等に注意すること。なお、破損等があった場合、「6.5（6）支給端末の運用・連絡体制の整備」を参照に適切に対応すること。

⑩ 私物端末など許可されていない端末の利用禁止

私物端末など許可されていない端末を学校に持ち込んで、学校のネットワークにつながないこと。

⑪　重要性分類Ⅱ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。

（２２）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。

（２３）ホームページ作成時の遵守事項

各学校のホームページは、豊川市公式ホームページ内コンテンツとしてそれぞれ開設する。そのため、コンテンツ作成ルールは企画部秘書課の指示によるほか、以下の点に留意すること。

①　ホームページ上に情報を発信する場合は、児童生徒、教職員の個人情報の保護に留意するとともに、教育情報セキュリティ学校管理者（校長）の承認を得たうえで配信しなければならない。

②　児童生徒の個人情報は、安全確保のため原則として掲載しない。ただし、教育上特に必要であると認められる個人情報や作品等については、本人及び保護者に対して配信することの意義と問題点について十分説明し、その同意を得たうえで掲載することができる。

③　文章、絵画、写真、音楽等の情報は、その著作権に十分配慮したうえで掲載しなければならない。

④　学校の情報をホームページに公開するにあたっては、情報を定期的に更新し、正確かつ適切な情報を発信する（古い情報や誤った情報が掲載されていないようにすること）。

⑤　ホームページに掲載された情報について、住民等外部から指摘を受けた場合は、教育情報セキュリティ学校管理者（校長）、教育情報セキュリティ学校主任者（教頭）、教育情報セキュリティ学校担当者（校務主任等）で協議し、情報の削除など適切に処理しなければならない。また、当該指摘内容が、情報漏洩などの情報セキュリティインシデントである場合は、「6.5（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」のとおり、教育情報セキュリティ管理者（学校教育課長）に速やかに報告し、迅速かつ適切な措置を講じなければならない。

⑥　ホームページは市公式ホームページを使用し、ソーシャルメディアサービス等の利用は原則禁止とする。

（２３）生成 AI 利用時等の遵守事項

教職員等は、生成 AI（人工的な方法により学習、推論、判断等の知的機能を備え、かつ、質問その他の電子計算機に対する指令に応じて当該知的機能の活用により得られたテキスト、

画像、音声または他のメディア等の結果を自動的に出力するよう作成されたプログラム及び当該プログラムと連携して動作するプログラム）の利用にあたっては、別に定める基準等を遵守し、適切に利用すること。

6.3 教育委員会事務局職員の遵守事項

教育委員会事務局では、学校の管理する一環として、教育情報システムの端末を事務局内に設置して必要に応じて学校の情報資産をモニタリングし、学校とのコミュニケーションに活用することが一般的である。そのため、教育情報システムを利用する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ことを鑑み、教育情報セキュリティ責任者（教育部長）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Ⅰ・Ⅱの情報資産について、校務用端末以外の情報機器等及び外部記録媒体等によるアクセスの禁止
⑤ 知り得た情報の秘匿
⑥ 業務を離れる場合の遵守事項
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する。また、その後も業務上知り得た情報を漏らさない。

6.4 研修・訓練

情報セキュリティを適切に確保するためには、情報セキュリティ対策の必要性と内容を全ての教職員等が十分に理解していることが必要不可欠である。また、情報セキュリティインシデントの多くは、教職員等の規定違反に起因している場合もある。さらに、情報セキュリティの向上は、利便性の向上とは、必ずしも相容れない場合がある。教職員等が業務を優先することが、情報セキュリティ対策の軽視につながることもある。また、情報セキュリティに関する脅威や技術の変化は早いことから、教職員等に対しては、常に最新の状況を周知することが重要である。さらに、実際に情報セキュリティインシデントが発生した場合に的確に対応できるようにするため、緊急時に対応した訓練を実施しておくことが必要である。

これらのことから、教職員等に情報セキュリティに関する研修・訓練を行うことを規定する。

① 統括教育情報セキュリティ責任者（教育長）は、毎年度最低１回は情報セキュリティに関する研修等を実施しなければならない。
② 研修は、教職員に対して、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。
③ 教育情報セキュリティ学校管理者（校長）は、教職員の情報セキュリティ研修の実施状況

について統括教育情報セキュリティ責任者（教育長）に報告しなければならない。

④　対象とされた教職員等は全て、研修・訓練に参加しなければならない。

6.5 情報セキュリティインシデントの連絡体制の整備

情報セキュリティインシデント（情報漏洩事故や機器等の物理的障害）やその発生の予防が重要なことは言うまでもないが、実際に情報セキュリティインシデントを認知した場合に、責任者に報告を速やかに行うことにより、被害の拡大を防ぎ、早期に回復を図れるようにしておく連絡体制を整備することも必要である。このことから、情報セキュリティインシデントを認知した場合の報告義務について規定する。

なお、報告に対する対応については、「8.9　侵害時の対応等」による。

（１）学校内からの情報セキュリティインシデントの報告

①　教職員等は、情報セキュリティインシデント（情報漏洩事故や機器等の物理的障害）を認知した場合、教育情報セキュリティ学校担当者（校務主任等）または教育情報セキュリティ学校主任者（教頭）に報告し、その指示に従って必要な措置を講じなければならない。

②　教育情報セキュリティ学校担当者（校務主任等）または教育情報セキュリティ学校主任者（教頭）は、報告のあった情報セキュリティインシデントが重大であると判断した場合、速やかに教育情報セキュリティ学校管理者（校長）に報告するとともに、情報事故等発生報告書（様式１１）により、情報漏洩等であれば教育情報セキュリティ管理者（学校教育課長）へ、情報システム等の物理的障害であれば教育情報システム管理者（庶務課長等）へ報告し、その指示に従って適切な措置を講じなければならない。

③　報告を受けた教育情報セキュリティ管理者（学校教育課長）または教育情報システム管理者（庶務課長等）は、速やかに統括教育情報セキュリティ責任者（教育長）、教育情報セキュリティ責任者（教育部長）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

①　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、速やかに教育情報セキュリティ学校管理者（校長）に報告するとともに、情報事故等発生報告書（様式１１）により、教育情報セキュリティ管理者（学校教育課長）または教育情報システム管理者（庶務課長等）へ報告しなければならない。

②　報告を受けた教育情報セキュリティ管理者（学校教育課長）または教育情報システム管理者（庶務課長等）は、速やかに統括教育情報セキュリティ責任者（教育長）、教育情報セキュリティ責任者（教育部長）に報告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

①　教職員は、情報漏洩などの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、教育情報セキュリティ学校管理者（校長）を通じ、教育情報セキュリティ管理者（学校教育課長）に情報事故等発生報告書（様式１１）により報告しなければならない。

② 報告を受けた教育情報セキュリティ管理者（学校教育課長）は、速やかに統括教育情報セキュリティ責任者（教育長）及び教育情報セキュリティ責任者（教育部長）に報告しなければならない。

③ 住民からの報告に対しては、適切に処理し、対応した結果については、必要に応じて報告を行った住民等に通知する。

（４）情報セキュリティインシデント報告を受けた教育情報セキュリティ委員会の開催等

① 上記（１）から（３）により報告された情報セキュリティインシデントについては、緊急時対応計画に従って、適切に対処する。当該インシデントが重大な影響を及ぼす可能性がある場合、統括教育情報セキュリティ責任者（教育長）は速やかに教育情報セキュリティ委員会を開催し協議する。

② 情報セキュリティインシデントは、その重要度や影響範囲等を勘案し、重大なものであれば報道機関への通知・公表対応を行わなければならない。その際、必要に応じて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表すること。

（５）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

情報セキュリティインシデントの原因を究明し、効果的な再発防止策を検討するために、情報セキュリティインシデントの発生から対応までの記録を作成し、保存しておく必要がある。

① 統括教育情報セキュリティ責任者（教育長）は、情報セキュリティインシデントの原因を究明し、効果的な再発防止策を検討するために、教育情報セキュリティ責任者（教育部長）及び教育情報セキュリティ管理者（学校教育課長）または教育情報システム管理者（庶務課長等)、情報セキュリティに関する統一的な窓口（企画部情報政策課）等と連携し、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、再発防止策を措置しなければならない。

（６）支給端末の運用・連絡体制の整備

① 学習用モバイル端末の利活用において、学校側が規定している各種ガイドラインを児童生徒の保護者も正しく理解し、端末を活用する場所にかかわらず児童生徒の情報リテラシー教育を促すことは、学校として行うべき重要な活動である。

② 教職員等が利用する学習用モバイル端末を含めて、紛失・盗難等インシデント発生時の報告に関しては周知徹底する必要がある。特に、端末の破損等については、令和４年９月校長会で示された「豊川市小中学校における１人１台端末の持ち帰り方針（学校教育課)」や、令和５年１２月４日付けで通知された「通常使用の範囲外における１人１台端末破損

等の届出様式について（庶務課)」等を参考に適切に対応すること。

③　緊急時の連絡体制

組織・体制	電話番号
統括教育情報セキュリティ責任者（教育長）	0533-88-8032（庶務課）
教育情報セキュリティ責任者（教育部長）	0533-88-8032（庶務課）
教育情報セキュリティ管理者（学校教育課長）	0533-88-8033（学校教育課）
情報システム管理者（教員 PC･生徒 PC 等）	0533-88-8032（庶務課）
情報システム管理者（給食システム）	0533-86-7601（学校給食課）
企画部情報政策課（財務 PC 等）	0533-89-2128（情報政策課）
情報セキュリティ学校管理者（各学校長）	各学校代表番号

第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設定管理

教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、情報セキュリティを確保するため、技術的な対策を講じなければならない。

（１）ファイルサーバ及び端末の設定等

① 教育情報システム管理者（庶務課長等）は、教職員等が使用できるファイルサーバの容量（300GB/校）を設定する。ファイルサーバはネットワークと同様に校務系及び教育系の通信経路を物理的に分離し、それぞれで適切な安全管理措置を講じなければならない。

② 教育情報システム管理者（庶務課長等）は、ファイルサーバを学校等の単位で構成し、教職員等が他の学校等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

③ 教育情報システム管理者（庶務課長等）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、別に専用フォルダ（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、担当教職員以外の教職員等が閲覧及び使用できないようにしなければならない。

④ インターネット接続を前提とするネットワークでは、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、機微な個人情報をファイルサーバ及びパソコン等の端末へ保管することを禁止する。

（２）バックアップの実施

教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、ファイルサーバ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、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）ログの取得等

① 教育情報システム管理者（庶務課長等）は、教育情報システムの各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

② 教育情報システム管理者（庶務課長等）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。

（４）ネットワークの接続制御、経路制御等

① 教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、フィルタリング（有害サイトへのアクセス制限）及びルーティング（通信データの配送経路）について、設定の不整合が発生しないように、所管するネットワークの内部における

ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

② 教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、不正アクセスを防止するため、所管する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

保護者や外部の教育関係者が訪問した際に利用するプリンタなど、外部の人々が利用できるシステムがある場合、不正アクセス等を防御するため、必要に応じ、他のシステムとの論理的または物理的な分離、もしくは各システムにおけるアクセス権管理の徹底を行う。

（６）外部ネットワークとの接続制限等

所管するネットワークにおいて、インターネットに接続し、公開したウェブサーバ等が、外部から攻撃を受けた場合に、教育ネットワークへの侵入を可能な限り阻止する必要がある。

① 校務系ネットワークはインターネット接続を遮断し、校務外部接続系ネットワークによりＷｅｂ閲覧する。具体的な対応について「5.3 (1) ネットワークの定義」のとおり。

② 教育情報システム管理者（庶務課長等）は、所管するネットワークを外部ネットワークと接続しようとする場合には、教育情報セキュリティ責任者（教育部長）及び統括教育情報セキュリティ責任者（教育長）の許可を得なければならない。その際、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調査し、庁内及び学校の全てのネットワーク、教育情報システム等の情報資産に影響が生じないことを確認しなければならない。

③ 教育情報システム管理者（庶務課長等）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、改ざんまたはシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

④ 教育情報システム管理者（庶務課長等）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、統括教育情報セキュリティ責任者（教育長）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）複合機のセキュリティ管理

インターネット接続の機能を備えた複合機も、他の IT 機器と同様の対策が必要となる。複合機の特性や業務上のリスクを勘案し、以下の観点に沿った対策を実施することが重要である。

① 教育情報システム管理者（庶務課長等）は複合機等（電子複写機を含む）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。

② 複合機等は取り扱う情報、利用方法、通信回線の接続形態などから、パソコン等の端末と同様に以下の対策を講じなければならない。

ア 機器の改造、増設及び交換を行ってはならない。

イ 廃棄する場合、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。

ウ 外部記録媒体を使用する時は、6.2（11）（外部記録媒体の取扱い）等の規定を遵守しなければならない。

（８）特定用途機器のセキュリティ管理

特定用途機器（ネットワーク接続の機能を備えたテレビ会議システムや IP 電話等の独立した機器）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。

（９）無線 LAN 及びネットワークの盗聴対策

無線 LAN を利用する場合は、解読が困難な暗号化及び認証技術を使用し、アクセスポイントへの不正な接続を防御する必要がある。

① 教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

② 教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）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、暗号化等の措置を講じなければならない。

（１０）電子メールのセキュリティ管理

メールサーバに対するセキュリティ対策等、電子メールのセキュリティ管理について定める。

① 教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

② 教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、サーバが機能不全に陥るほどの大量のスパムメール等の受信または送信を検知した場合は、メールサーバの運用を停止しなければならない。

③ その他、電子メールの送受信容量の上限（最大約 5MB）等については、「6.2（12）電子メールの利用制限」のとおり。

7.2 アクセス制御

情報システム等をアクセス権限のない者に利用できる状態にしておくと、情報漏洩や情報資産の不正利用等の被害が発生し得る。そこで、アクセス制御を業務内容、権限ごとに明確に規定しておく必要がある。また、不用意なアクセス権限付与による不正アクセスを防ぐために、アクセス権限の管理を集約することが重要である。このことから、利用者登録や特権管理等を用いた情報システムへのアクセス制御、ログイン手順、接続時間の制限等不正なアクセスを防止する手段について規定する。

（１）アクセス制御等

教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、所管するネットワークまた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、システム上制御しなければならない。特に強固なアクセス制御による対策を講じたシステム構成の場合、重要性分類Ⅱ以上の情報資産へのアクセスについては、多要素認証等のアクセスの真正性に関する要素技術を取り入れることで、当該システムへの認証強度の向上とアクセス権管理を徹底すること。

（２）外部からのアクセス等の制限

外部からのアクセスを認める場合として、障害等を理由として自身のモバイル端末を持ち込む場合等が想定される。接続に当たっては許可制とし、許可は必要最小限の者に限定しなければならない。

① 教育情報セキュリティ責任者（教育部長）は、内部のネットワークまたは教育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。

② 外部からのアクセス等について相談があった場合は、教育情報システム管理者（庶務課長等）を通じて教育情報セキュリティ責任者（教育部長）に上申して、判断を仰がなければならない。

③ 教育情報セキュリティ責任者（教育部長）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。

④ 教育情報セキュリティ責任者（教育部長）は、外部からのアクセスに利用する情報機器等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。

（３）ログイン時の表示等

教育情報システム管理者（庶務課長等）は、ログイン時における表示等により、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なシステムがソフトウェアにある場合、それ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

教育委員会事務局職員は、管理者権限等の特権を利用している際に、システムにログインしたままで端末を放置しておくと、他者に不正利用されるおそれがあることから、接続時間を必要最小限にしなければならない。

7.3 システム開発、導入、保守等

システム開発、導入、保守等において、技術的なセキュリティ対策が十分に行われない場合は、プログラム上の欠陥（バグ）によるシステム障害等により業務に重大な支障が生じるおそれがある。このことから、システム開発、導入、保守のそれぞれの段階における対策を規定する。なお、本規定にはシステムの更新または統合時の十分な検証等も含まれる。例えば次世代校務 DX 環境の整備に際し、「ネットワーク分離による対策を講じたシステム構成」等から「強固なアクセス制御による対策を講じたシステム構成」へ移行する際には、その移行期間において、オンプレミス環境とパブリッククラウド環境が共存することが想定される。このような場合についても、本規定を参照し、それぞれの環境に応じた適切なセキュリティ対策を講じること。

（１）情報システムの調達

情報システムを調達する場合は、当該情報システムで取り扱う情報の重要性に応じて、情報システムのライフサイクルで必要となるセキュリティ機能を洗い出し、調達要件に含める必要がある。例えば、アクセス制御の機能、パスワード設定機能、ログ取得機能、データの暗号化等である。

① 教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、情報システム開発、導入、保守等の調達にあたって、一般に公開する調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

② 教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）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

① 教育情報システム管理者（庶務課長等）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。

② 教育情報システム管理者（庶務課長等）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。

③ 教育情報システム管理者（庶務課長等）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）情報システムの導入

① 教育情報システム管理者（庶務課長等）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。

② 教育情報システム管理者（庶務課長等）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。

③ 教育情報システム管理者（庶務課長等）は、導入するシステムやサービスの断続的な運用（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。

④ 教育情報システム管理者（庶務課長等）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。

⑤ 教育情報システム管理者（庶務課長等）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。

⑥ 教育情報システム管理者（庶務課長等）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。

⑦ 教育情報システム管理者（庶務課長等）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・保守に関連する資料等の整備・保管

システム開発や機器等の導入において、開発や機器等の導入に関する資料やシステム関連文書等は、保守や機器更新の際に必要となることから、適切に整備し保管することが必要である。

① 教育情報システム管理者（庶務課長等）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 教育情報システム管理者（庶務課長等）は、テスト結果を一定期間保管しなければならない。

③ 教育情報システム管理者（庶務課長等）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を適切な方法で保管（リポジトリ：変更履歴等を格納する場所）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

情報システムの処理は、入力処理、内部処理、出力処理で構成されている。これらの処理を行うプログラムの設計が正確に行われないと、データが不正確なものになるおそれがある。入力処理の際は、不正確なデータの取り込みが行われないよう、入力データの範囲チェックや不正な文字列等の入力を除去する機能を組み込むことが必要になる。内部処理においても、データの抽出条件の誤りやデータベースの更新処理での計算式のミス等で、データ内容を誤った結果に書き換えてしまうことのないよう、これらを検出するチェック機能を持たせる必要がある。さらには、内部処理が正確に行われていた場合であっても、出力処理で誤った処理がさ

れると、端末画面の表示や印刷物を利用する者に対して、誤ったデータ内容を認識させてしまうおそれがある。このことから、情報システムの処理した結果の正確性が確保されるよう、システムの設計及びプログラムの設計を行う必要がある。

① 教育情報システム管理者(庶務課長等)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 教育情報システム管理者（庶務課長等）は、故意または過失により情報が改ざんされるまたは漏洩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。

③ 教育情報システム管理者（庶務課長等）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

情報システムのプログラムを保守した場合は、必ず変更履歴を作成しておくことが必要になる。変更履歴がないと、プログラム仕様書と実際のソースコードに不整合が生じ、変更時の見落としからシステム障害を招く可能性が高まる。そのため、教育情報システム管理者（庶務課長等）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

数年間のシステム開発等、長期の開発期間を要する場合には、運用環境のシステム保守状況を踏まえて、移行時にシステム障害が生じないように、開発環境のソフトウェアの更新を行っておく必要がある。ソフトウェアのバージョンが違っていたために、運用環境でシステムが緊急停止をすることや、他のシステムに影響を与えることがあり、これを未然に防止することが重要である。そのため、教育情報システム管理者（庶務課長等）は、開発・保守用のソフトウェア等を更新また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)システム更新または統合時の検証等

システムを更新または統合する場合は、システムの長時間の停止や誤動作等による業務への影響が生じないように、事前に慎重な検証等を行っておく必要がある。そのため、教育情報システム管理者（庶務課長等）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

情報システムにコンピュータウイルス等の不正プログラム対策が十分に行われていない場合は、システムの損傷、情報漏洩等の情報セキュリティインシデントが発生するおそれがある。不正プログラム対策としては、不正プログラム対策ソフトウェアを導入するとともに、パターンファイルの更新、ソフトウェアのパッチの適用等を確実に実施することが基本であり、被害の拡大を防止することになる。これらを踏まえ、不正プログラムの感染、侵入を予防し、さらには感染時の対応として取るべき手段を規定する。

（１）教育情報セキュリティ責任者（教育部長）の措置事項

① 外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムの教育情報システムへの侵入を防止しなければならない。

② 外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③ 情報機器等にコンピュータウイルス等の不正プログラム情報を収集し、必要に応じ教職員等に対して注意喚起しなければならない。

④ 情報機器等にコンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

⑤ 不正プログラム対策ソフトウェアは、常に最新の状態に保たなければならない。

（２）教育情報システム管理者（庶務課長等）の措置事項

① 情報機器等を守るため、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。

② 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。

③ 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。

7.5 不正アクセス対策

情報システムに不正アクセス対策が十分に行われていない場合は、システムへの攻撃、情報漏洩、損傷、改ざん等の被害を及ぼすおそれがある。このことから、不正アクセスの防止または被害を最小限にするため、不正アクセス対策として取るべき措置、攻撃を受けた際の対処及び関係機関との連携等について規定する。

（１）教育情報セキュリティ責任者（教育部長）の措置事項

使用されていない TCP/UDP ポート、SSID、不要なサービスは、不正アクセスによる侵入や悪用に利用される可能性が高いため、ポート閉鎖やサービス停止処理を行う

① 使用されていないポート及び SSID（無線 LAN ネットワーク）を閉鎖しなければならない。

② 不要なサービスについて、機能を削除または停止しなければならない。

③ 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、教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）へ通報するよう、設定しなければならない。

④ 情報セキュリティに関する統一的な窓口（企画部情報政策課）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）攻撃予告への対処

教育情報セキュリティ責任者（教育部長）は、サーバ等に攻撃を受けることが明確になった場合、教育情報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

教育情報セキュリティ責任者（教育部長）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，情報システムの断続的な運用（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

教育情報セキュリティ責任者（教育部長）は、教育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。

7.6 セキュリティ情報の収集

ソフトウェアにセキュリティホール（欠陥）が存在する場合、システムへの侵入、改ざん、損傷、漏洩等の被害を及ぼすおそれがある。また、情報セキュリティを取り巻く社会環境や技術環境等は刻々と変化しており、新たな脅威により情報セキュリティインシデントを引き起こすおそれがある。これらのことから、セキュリティホールをはじめとするセキュリティ情報の収集、共有及び対策の実施について規定する。

（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

教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）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

教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、不正プログラム等のセキュリティ情報を収集し、必要に応じて対応方法について、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

教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）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８ 運用

8.1 情報システムの監視

監視に必要な要素は、不正アクセスや不正利用の検知と記録（ログ等）である。情報システムにおいて、不正プログラムまたは不正アクセス等による情報システムへの攻撃または侵入、教職員の不正な利用、自らのシステムが他の情報システムに対する攻撃に悪用されること等を防ぐためには、ネットワーク監視等により情報システムの稼働状況について常時監視を行うことが必要である。したがって、情報システムの監視に係る対策について規定する。

① 教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、セキュリティに関する事案を検知するため、教育情報システムを常時、監視しなければならない。特に強固なアクセス制御による対策を講じたシステム構成の場合、重要性分類Ⅱ以上の情報資産へのアクセスについては、侵入検知システム（IDS）や侵入防御システム（IPS）などの端末・サーバ・通信の監視・制御等によるセキュリティ対策を講じなければならない。

② 教育情報セキュリティ責任者（教育部長）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 教育情報セキュリティ責任者（教育部長）は、重要性分類Ⅰ・Ⅱの情報資産を格納するシステムを常時、監視しなければならない。

④ 内部からの攻撃監視

ア 教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、教職員等及び外部委託事業者が使用している情報機器等の端末から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。

イ 学校内で保護者等に公衆通信回線を提供する場合は、内部の情報システムとネットワークを切り分け、不正アクセスを防止する対策を行わなければならない。

8.2 ドキュメントの管理

情報セキュリティ対策の詳細を記載したドキュメント類（紙媒体、電子媒体ともに）は機密事項に相当し、外部情報漏洩によって攻撃者の手に渡ることを防ぐ必要があることから、その意味で情報システムの仕様書、運用管理記録等情報セキュリティに関するドキュメント管理を厳格に行う必要がある。また、設計変更や障害での対策等の経緯を含めた記録管理により、常にアップデートされた状態を保持することも、故障やセキュリティ侵害時等の対応で必要となる。

（１）システム管理記録及び作業の確認

① 教育情報システム管理者（庶務課長等）は、教育情報システムの運用において実施した作業について、作業記録を作成しなければならない。

② 教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

③ 教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）または教育情報システム担当者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、２名以上で作業させ、互いにその作業を確認させなければならない。

（２）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（教育部長）及び教育情報システム管理者（庶務課長等）は、ネットワーク構成図、教育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。

（３）障害記録の管理

教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、教職員等からのシステム障害の報告（「6.5（1）学校内からの情報セキュリティインシデントの報告」参照)、システム障害に対する処理結果また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

統括教育情報セキュリティ責任者（教育長）及び教育情報セキュリティ責任者（教育部長）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（実際の対応については「8.9 侵害時の対応等」参照)。

8.3 教職員等の ID 及びパスワードの管理

情報システムにおいて正規な利用者がどうかは利用者認証情報に基づき判断されるが、利用者認証情報が外部流出した場合には、簡単に不正アクセスにつながる。利用者認証情報の多くは、知識認証（ID 及びパスワード等）であり、ID 及びパスワードを秘匿管理することが不正アクセス抑止の要である。

（１）利用者 ID の取扱い

① 教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）は、利用者の登録、変更、抹消等の情報管理、教職員等の異動等に伴う利用者 ID の取扱い等の方法を定めなければならない。

② 教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）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（学校教育課）と連携し、点検しなければならない。

③　教職員等の ID 取扱いについては「6.2（8）ID の取扱い」のとおり。

（２）パスワードに関する情報の管理

①　教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）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（パソコンの操作やアプリなどを使うために必要なソフトウェアのこと。いわゆる OS。）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、これを有効に活用しなければならない。

②　教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）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。

③　教職員等のパスワード取扱いについては「6.2（9）パスワードの取扱い」のとおり。

8.4 シンクライアント用 IC カード等の取扱い

情報システムを利用する際の 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）の管理が適切に行われない場合は、情報システム等を不正に利用されるおそれがある。このことから、ID 及びパスワード等の管理に関する遵守事項を規定する。認証情報等は、人的な原因により漏洩しやすい情報である。教育情報システム管理者からの認証情報等の発行から教職員等での管理に至るまで、人的な原因で情報の漏洩するリスクを最小限にとどめる必要がある。

（１）シンクライアント用 IC カード等の取扱い

①　教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）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。

②　教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）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。

③　IC カード等の取扱いについては「6.2（10）シンクライアント用 IC カードの取扱い」のとおり。

8.5 児童生徒における ID 及びパスワード等の管理

GIGA スクール構想における１人１台端末の整備と併せて、児童生徒一人一人に個別の ID を付

与することで、児童生徒の学びを蓄積し、教員や AI によるフィードバックが行われ、個別最適な学びを提供することが期待できる。一方で、なりすまし等による ID の不正使用や、不正アクセスによる情報漏洩等のセキュリティリスクも考えられるため、利用する学習用ツールやクラウド上のアプリケーションの ID 及びパスワードに対して安全管理措置を講じなければならない。

（１）ID 登録・変更・削除

①　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上げたパスワードポリシーによりセキュリティ強度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、教育委員会にて一元管理することが望ましい。なお、ID については数字のみで構成したものや、児童生徒の氏名の一部を使うなど命名規則はさまざまであるが、個人を識別できる可能性があるような ID は、個人情報保護法の観点から個人情報に相当するとも考えられるため留意すること。

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/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。

③　転出/卒業の ID 削除処理

本人の氏名等が推察され、当該個人を特定できるような ID については、個人情報に相当すると考えられる。そのため、そのような個人情報と位置づけ可能な ID を学習用ツール等で用いている場合は、あらかじめ児童生徒本人によるデータ移行を転出/卒業前の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必要がある。

（２）多要素認証等によるなりすまし対策

特にデータの機密性（外部漏洩の影響）や完全性（情報の改ざんの影響）の確保が相応に求められる場合においては、児童生徒の ID 及びパスワードに加え、多要素認証を設定し、本人確認を厳格に行うことが望ましい。

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Ⅱ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。

（３）学習用ツールへのシングルサインオン

① 個別最適な学びの実現が期待される AI ドリル、授業支援システムによる成果物の保存、デジタル教科書などについては、各種サービスの利用にあたり ID 及びパスワードの入力など認証操作が必要になるが、サービスを利用する児童生徒側においては都度の認証情報入力による運用の煩雑化や、児童生徒の認証情報を管理する教育委員会や学校現場からすると管理が複雑化して運用負荷やリスクが高くなる。

② そのため、シングルサインオン（1 回のログインで複数のサービスやアプリケーションにアクセスできるようになる機能。1 つの ID とパスワードで複数のシステムが利用できるようになるため、ユーザー負担軽減はもとより情報漏洩のリスクを抑えることが可能）と認証情報の一元管理により、運用効率化と運用負荷の最小化、煩雑な運用によるセキュリティリスクを低減することが可能である。また、シングルサインオンに利用する ID 及びパスワードは漏洩した際の影響範囲が大きいため、必要に応じて多要素認証と組み合わせることでよりセキュリティリスクを低減することができる。

8.6　特権を付与された ID の管理等

教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）、教育情報セキュリティ管理者（学校教育課長）は、教育情報システムに係る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。

8.7　教育情報セキュリティポリシーの遵守状況の確認・管理

教育情報セキュリティポリシーの遵守を確保するため、教育情報セキュリティポリシーの遵守状況等を確認する体制を整備するとともに、問題があった場合の対応について規定する。

（１）遵守状況の確認及び対処

① 教育情報システム管理者(庶務課長等)及び教育情報セキュリティ管理者(学校教育課長)、教育情報セキュリティ学校管理者（校長）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（教育長）及び教育情報セキュリティ責任者（教育部長）に報告しなければならない。

② 統括教育情報セキュリティ責任者（教育長）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。

③　教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）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教育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）情報機器等及び外部記録媒体等の利用状況調査

①　教職員等はパソコン、学習用モバイル端末及び外部記録媒体等を業務のため使用しているのであって、私的な使用はあってはならない。職員等の業務以外の目的での利用を抑止するため、電子メールの送受信記録等を調査できる権限を統括教育情報セキュリティ責任者（教育長）及びその指名した者に付与する。

②　統括教育情報セキュリティ責任者（教育長）及びその指名した者は、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情報機器等、外部記録媒体のログ、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

①　業務外の外部サイトを閲覧している場合、不正プログラムの感染、侵入の可能性が高まるため、業務以外の目的でのウェブ閲覧は禁止しなければならない。また、閲覧先サイトのサーバにドメイン名等の組織を特定できる情報がログとして残ることにより、外部から指摘を受けるようなことがあってはならない。

②　教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）、教育情報セキュリティ管理者（学校教育課長）は、教職員等のウェブ利用について、明らか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、統括教育情報セキュリティ責任者（教育長）に報告するとともに、教育情報セキュリティ学校管理者（校長）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

教育情報セキュリティ責任者（教育部長）及び教育情報システム管理者（庶務課長等）、教育情報セキュリティ管理者（学校教育課長）は、教職員等による不正アクセスを発見した場合は、統括教育情報セキュリティ責任者（教育長）に報告するとともに、当該教職員等が所属する学校の教育情報セキュリティ学校管理者（校長）に通知し、適切な処置を求めなければならない。

8.8 専門家の支援体制等

コンピュータウイルス等の不正プログラム対策が十分に行われていない場合に備え、不正プログラム感染時等に外部の専門家の支援を受けられるように支援体制を整備する必要がある。このことから、外部との連携や情報等の交換について規定する。

（１）専門家の支援体制

教育情報セキュリティ責任者（教育部長）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）他団体との教育情報システムに関する情報等の交換

他団体との間で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は、その用途等を明確にし、目的外利用や、紛失または改ざん等が起こらないようにしなければならない。教育情報システム管理者（庶務課長等）は、他の団体と教育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（教育部長）の許可を得なければならない。

8.9 侵害時の対応等

情報セキュリティインシデント、システム上の欠陥及び誤動作並びに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事案が発生した場合に、迅速かつ適切に被害の拡大防止、迅速な復旧等の対応を行うため、緊急時対応計画（情報セキュリティインシデント発生時の対応手順書）の策定について規定する。

緊急時対応計画には、情報資産に対するセキュリティ侵害が発生した場合等における連絡、証拠保全、被害拡大の防止、復旧等の迅速かつ円滑な実施と、再発防止策の措置を講じるために必要な事項を定める必要がある。また、自らが所有する情報資産における被害拡大防止のほか、外部への被害拡大のおそれがある場合には、その防止に努めることを定める必要がある。情報が漏洩することなどにより被害を受けるおそれのある関係者に対し早急に連絡することが重要である。さらに、当該事案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、警察・関係機関と緊密な連携に努めることも重要である。

（１）緊急時対応計画（情報セキュリティインシデント発生時の対応手順書）の策定

① 情報セキュリティが侵害された場合または侵害されるおそれがある場合等における具体的な措置について、緊急時対応計画として定める。

② 統括教育情報セキュリティ責任者（教育長）また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、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セキュリティ侵害が発生した場合また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。

（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。

① 警察・関係機関も含めた関係者の連絡先及び連絡順序
② 発生した事案に係る報告すべき事項
③ 発生した事案への対応措置
④ 再発防止措置の策定

（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（教育長）また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。

8.10 例外措置

教育情報セキュリティポリシーの規定をそのまま適用した場合に、学校事務及び教育活動の適正な遂行を著しく妨げるなどの理由により、これに代わる方法によることやポリシーに定められた事項を実施しないことを認めざるを得ない場合がある。このことから、あらかじめ例外措置について規定する。

（１）例外措置の許可

教育情報セキュリティ学校管理者（校長）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または遵守事項を実施しないことについて合理的な理由がある場合には、教育情報セキュリティ管理者（学校教育課長）及び教育情報システム管理者（庶務課長等）の許可を得て、例外措置を取ることができる。

具体的な事例としては、障害を理由とする差別の解消の推進に関する法律（平成 25 年 6 月 26 日号外法律第 65 号）の優先等が想定される。

（２）緊急時の例外措置

教育情報セキュリティ学校管理者（校長）は、災害等緊急を要する場合に例外措置を実施することが不可避のときは、措置事後速やかに教育情報セキュリティ管理者（学校教育課長）に報告しなければならない。

（３）例外措置申請書の管理

① 教育情報セキュリティ学校管理者（校長）は、上記（１）の申請、（２）の報告を行うにあたり、例外措置申請書（様式１２号）により教育情報セキュリティ管理者（学校教育課長）に上申等する。

② 教育情報セキュリティ管理者（学校教育課長）は、例外措置の申請内容等について、教育情報システム管理者（庶務課長等）と共有し、教育情報セキュリティ責任者（教育部長）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（教育長）にも報告する。例外措置の申請書および審査結果については、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。

8.11 法令の遵守

教職員等は、業務の遂行において使用する情報資産を保護するために、地方公務員法（昭和 25 年 12 月 13 日法律第 261 号)、著作権法（昭和 45 年法律第 48 号)、教育公務員特例法（昭和 24 年 1 月 12 日法律第 1 号)、不正アクセス行為の禁止等に関する法律(平成 11 年法律第 128 号)、個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号)、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号)、サイバーセキュリティ基本法（平成 26 年法律第 104 号)、その他関係法令を遵守し、これに従わなければならない。

8.12 懲戒処分

教育情報セキュリティポリシーの遵守事項に対して、教職員等が違反した場合の事項を定めておくことは教育情報セキュリティポリシー違反の未然防止に、一定の効果が期待される。このことから、教育情報セキュリティポリシー違反に対する懲戒処分の規定及び懲戒に係る手続きについて規定する。

（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、地方公務員法による懲戒処分の対象とする。

（２）違反時の対応等

① 教職員は、教育情報セキュリティポリシーを遵守する上で、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、速やかに教育情報セキュリティ学校管理者（校長）に相談し、指示を仰がなければならない。

② 教職員が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、教育情報セキュリティ管理者（学校教育課長）から当該教職員が所属する学校の教育情報セキュリティ学校管理者（校長）に通知し、適切な措置を求めなければならない。

③ 教育情報セキュリティ学校管理者（校長）の指導によっても改善されない場合、統括教育情報セキュリティ責任者（教育長）は、当該教職員の教育ネットワークまた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、統括教育情報セキュリティ責任者（教育長）は、教職員の権利を停止あるいは剥奪した旨を当該教

職員が所属する学校の教育情報セキュリティ管理者（校長）に通知しなければならない。

第９ 外部委託

情報システムの外部委託を行う際は、外部委託事業者からの情報漏洩等の事案を防止するために、情報セキュリティを確保できる外部委託事業者を選定し、契約で遵守事項を定めるとともに、定期的に対策の実施状況を確認する必要がある。このことから、外部委託を行う際に、情報セキュリティ確保上必要な事項について規定する。

（１）外部委託事業者の選定基準

教育情報システム管理者（庶務課長等）、教育情報セキュリティ学校管理者（校長）は、外部委託事業者の選定にあたり、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。

（２）契約項目

教育情報システム管理者（庶務課長等）及び教育情報セキュリティ学校管理者（校長）は、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。

① 教育情報セキュリティポリシーの遵守
② 外部委託事業者の委託先の責任者、委託内容、作業者、作業場所の特定
③ 提供されるサービスレベルの保証
④ 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
⑤ 従業員に対する教育の実施
⑥ 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
⑦ 業務上、知り得た情報の守秘義務
⑧ 再委託に関する制限事項の遵守
⑨ 委託業務終了時の情報資産の返還、廃棄等
⑩ 委託業務の定期報告及び緊急時報告業務
⑪ 市による監査、検査
⑫ 教育委員会による情報セキュリティインシデント発生時の公表
⑬ 教育情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

（３）確認・措置等

教育情報システム管理者（庶務課長等）及び教育情報セキュリティ学校管理者（校長）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。措置することとなった場合、その内容を教育情報セキュリティ責任者（教育部長）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（教育長）にも報告する。

（４）外部委託事業者に対する説明

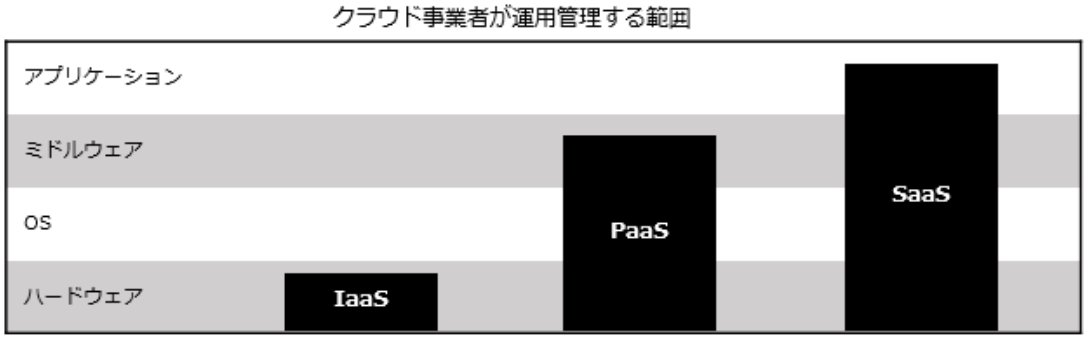
教育情報システム管理者（庶務課長等）は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、教育情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

第１０　SaaS 型パブリッククラウドサービスの利用

（１）SaaS 型パブリッククラウドサービスとは

クラウドサービスとは、自前でサーバ等を持たずに、インターネット経由で外部事業者が提供するサービスを利用する仕組みである（反対に、自前のサーバを核としてシステム構築することをオンプレミス型という）。近年、急速に進化し発展したクラウドサービスは、社会全体で多方面にわたり利用が増加し、国のシステムの整備においても、「デジタル社会の実現に向けた重点計画」（令和３年 12 月 24 日閣議決定）の方針も踏まえて、クラウドサービスの利用を第一候補として、その検討を行うものとするクラウド・バイ・デフォルト原則に基づくこととしている。

クラウドサービスの例としては、IaaS（イアース：Infrastructure as a Service）、 PaaS（パース：Platform as a Service）、SaaS（サース：Software as a Service）等がある。



IaaS はハードウェアの保守管理を中心に行うサービス（システム構築のインフラを提供するサービス）であり、ソフトウェア開発環境の一部が提供されるサービスのこと。PaaS とは異なり、ミドルウェアの導入まで自身で行う必要があるため高い専門知識が必要な一方、カスタマイズの自由度が非常に高いことから企業等の IT 部門が主たる利用層となる。主だったサービスとして、Microsoft 社が提供する「Azure」や Amazon 社が提供する「AWS」がある。

PaaS は開発環境を提供する為のミドルウェアやサーバ OS までを運用管理するサービス（アプリケーション開発のプラットフォームを提供するサービス）であり、ソフトウェア開発環境の全てが提供されるサービスのこと。SaaS のような完成したソフトウェアではなく、ソフトウェアの開発環境が提供され、その提供されたプラットフォーム上でソフトウェア開発を行うため、開発スピードの向上や環境構築の手間を省ける点がメリットとなるが、一方で、プラットフォームに依存するため、カスタマイズの制限があることがデメリットとなる。主たる利用層は開発者となる。

一方で、SaaS はエンドユーザが利用するアプリケーションまで運用管理するサービスとなる。インターネット上で利用の申込みをすれば、無料あるいは少額の初期費用だけですぐに使い始められる。SaaS を利用することで、ユーザーはソフトウェアをインストールすることなく、ブラウザを通じてサービスを利用することができ、いわゆるインターネットを通じて一般ユーザーが利用するサービスは SaaS に分類される。

また、クラウド環境は、プライベートクラウドとパブリッククラウドに分類される。プライベートクラウドは特定の組織専用に構築された環境、パブリッククラウドはインターネットを通じて不特定多数に提供されるサービスであり、SaaS はパブリッククラウドサービスに分類される。

※　以前は、パソコンでメールのやりとりをするためには、メールソフトをインストールする必要があったが、SaaS の代表例である「Gmail」や「Yahoo!メール」が登場し、専用ソフトをインストールすることなくメールのやりとりが可能となっている。また、「Office 365（Microsoft 社の Office アプリを定額で利用できるサブスクリプション型サービス）」や、Dropbox、OneDrive、WEB 会議等用の Microsoft Teams や Zoom、Google カレンダー、業務管理ソフトの kintone 等、SaaS は日常に溢れるクラウドサービスとなっている。

（２）学校現場における SaaS 型パブリッククラウドサービスの利用

すでに学校現場においても、SaaS 型パブリッククラウドサービスが広く普及しており、教職員等及び児童生徒は、インターネット経由でアプリケーションを利用している。SaaS 型パブリッククラウドサービスは、豊川市が独自にシステム構築することなく利用可能であることから、学習系分野では、学習 e ポータル、MEXCBT、デジタル教科書、デジタルドリル、デジタルコンテンツ配信等各種サービスが利用され、校務系分野では、校務支援システム等が利用されている。

（３）SaaS 型パブリッククラウドサービスを利用する教職員等及び児童生徒側の留意点

SaaS 型パブリッククラウドサービスは、インターネット接続環境からのアクセスが前提となるため、常にサイバー脅威（ウイルス感染等）に晒されていることに加えて、ID・パスワードによる利用者認証が多く採用されていることから、ID 及びパスワード等が他者に漏れると、容易に「なりすまし」による不正アクセスが発生する等のリスクが存在することに留意する必要がある。

10.1 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

①　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若しくは開発に従事する者また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しなければならない。

②　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。

③　特権を付与された ID の管理については「8.6 特権を付与された ID の管理等」のとおり。

（２）アクセス制御

① 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。
② 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

① 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。
② 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

① 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、合意の上、利用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措置の管理について、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

① 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「5.1 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。

② 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「5.2 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。

（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

① 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「5.1(3) 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。

② 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及び復旧手順について「7.1（2）バックアップの実施」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。

③ 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、「7.1（3）ログの取得等」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

① 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。

② 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

① 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。

② 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

① 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。
② 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。
③ 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。
④ 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または外部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。
⑤ 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）サービス終了時のデータの廃棄及び利用者アカウント抹消
① 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、適切に廃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。
② 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。
③ 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およ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
① 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。

10.2 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程を含める。

（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、保守運用管理規定 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下記の事項について確認し、合意しなければならない。

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

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、充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

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
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。
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
① 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式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。
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。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。
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上で、契約要件等として定めなければならない。

10.3 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 及びパスワード等の秘匿

① 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。

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。もし該当要素が流出等したと考えられる場合には、速やかに教育情報セキュリティ学校管理者（校長）に報告しなければならない。

（2）モバイル端末の持ち歩きリスク

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（インターネットを通じて不特定多数に提供されるサービス）上で重要な情報（重要性分類Ⅰ・Ⅱ）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Ⅱ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

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

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。

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。

10.4 約款による外部サービスの利用

本項でいう約款による外部サービスとは、有料、無料に関わらず、インターネット上に提示された約款への同意及び簡易なアカウントの登録により当該機能を利用可能なサービスのことであり、代表例としては、電子メールやファイルストレージ、ファイル転送サービスなどがある。このようなサービスでは、利用者データについてのセキュリティ遵守事項が約款に示されていない場合があったり、利用者データの利用権限がサービス提供者側に帰属することを前提にサービス提供される場合がある、セキュリティインシデント調査等への対応協力が約款に示されていない場合が多い、利用者データ保管における安全管理措置が不明な場合がある、約款や利用規約が予告なく一方的に変更されたりサービスが停止する可能性がある、というようなことが主なリスクとして想定される。

① 約款による外部サービスの利用は原則禁止する。

10.5 ソーシャルメディアサービスの利用

市民への情報提供など、ソーシャルメディアサービスを利用する場合は、約款による外部サービス（X（旧 Twitter）や Instagram 等）を利用することが想定されるが、なりすましやサービス停止のおそれがあるため、ソーシャルメディアサービスによる情報発信時の対策を講じる必要がある。なお、データの保存を伴う場合には「10.1 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」及び 「10.2 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 」で想定する個別契約締結型サービスの検討を行うこととなる。

① パブリック型の情報発信については市の公式ホームページを使用することとし、ソーシャルメディアサービスの利用は原則禁止する。

② ホームページについては「6.2（23）ホームページ作成時の遵守事項」のとおり。

第 11　評価・見直し

11.1 学校情報セキュリティ監査及び自己点検

（１）実施方法

① 教育情報セキュリティ学校管理者（校長）は「6.1（８）自己点検の実施」のとおり、年１回及び必要に応じて、学校情報セキュリティの自己点検を行い、問題がある場合には、速やかに是正しなければならない。

② 教育情報セキュリティ学校管理者（校長）は、自己点検の結果を教育情報セキュリティ委員会（事務局：庶務課）に報告しなければならない。

③ 教育情報セキュリティ委員会は、提出された自己点検結果をもとに書面監査を行い、必要に応じて実地監査を行う。監査は、客観性を確保するために、外部の専門的知識・見識を有する者の協力を得て実施することができる。

（２）監査結果への対応

① 統括教育情報セキュリティ責任者（教育長）は、教育情報セキュリティ委員会の監査結果をもとに、指摘事項を所管する教育情報セキュリティ学校管理者（校長）に対し、当該事項への対処を指示しなければならない。

② 統括教育情報セキュリティ責任者（教育長）は、指摘事項を所管していない教育情報セキュリティ学校管理者（校長）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。

11.2　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、教育情報セキュリティ監査及び自己点検の結果並びに教育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及び関係規程等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。

附則

１　この対策基準は、令和７年４月１日から施行する。