令和４年７月　定例教育委員会

第３別館２階会議室

議事日程（令和４年７月８日　10時）

日程番号	議事			
1	６月教育委員会会議録の承認			
2	会議録署名委員の指名			
3	教育長報告			
4	議題			
	（1）	議案第29号	今治市教育情報セキュリティポリシーの策定について	
		議案第30号	今治市公民館運営審議会委員の委嘱について	
		議案第31号	今治市青少年センター運営協議会委員の委嘱について	
		議案第32号	今治市視聴覚ライブラリー運営審議会委員の委嘱について	
		議案第33号	今治市図書館運営審議会委員の委嘱について	
		議案第34号	今治市図書館指定管理者選定審議会委員の委嘱について	

資料１

第９回教育委員会議案第29号

今治市教育情報セキュリティポリシーの策定について

今治市教育情報セキュリティポリシーを別紙のとおり定める。

令和４年７月８日提出

今治市教育委員会
教育長　田坂　敏

今治市教育情報セキュリティポリシー

今治市教育委員会

令和４年　月策定

目　次

第１章　はじめに

当市における「情報セキュリティポリシー」については、当市全体（市長（水道事業管理者の職務を行う市長を含む。）、各行政委員会及び委員、消防長及び議会）を対象とし、基本方針及び対策基準から構成された「今治市情報セキュリティポリシー」（平成17年１月16日策定、直近改訂令和４年６月13日）が策定されています。

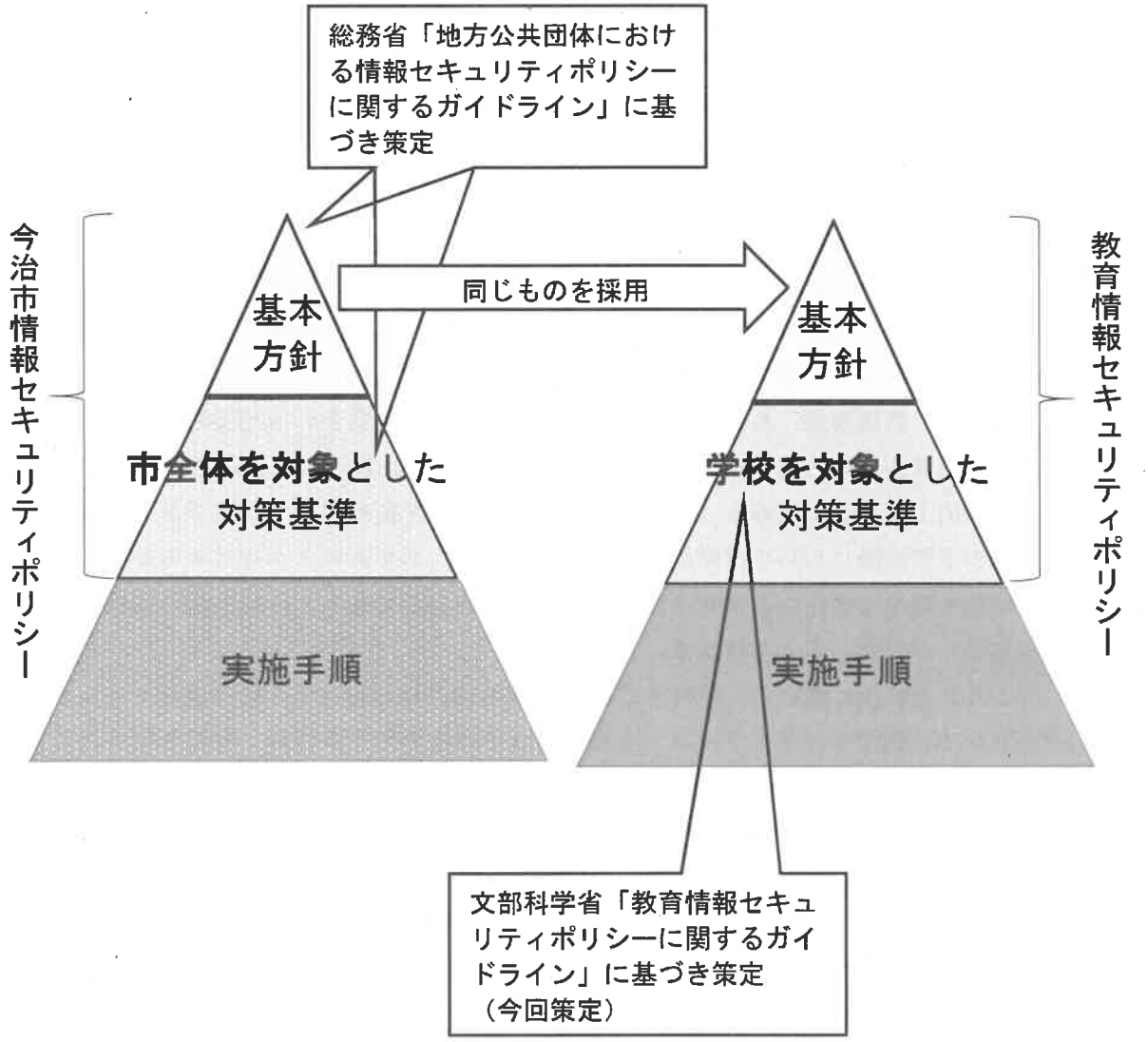
一方では、これまでの学校又は教育に関する情報セキュリティポリシーは、「教育の情報化に関する手引」（文部科学省平成22年10月改訂）に則り、基本方針、実施基準及び実施手順の全てが当市内の学校ごとに制定運用されており、学校現場では複数の情報セキュリティポリシーの網がかかった状態となっています。

学校は、指導要録、生徒指導等の記録、進路希望調査票といった機微な情報が保管されているほか、地方公務員法（昭和25年法律第261号）及び教育公務員特例法（昭和24年法律第１号）等に定める「服務」に服さない児童生徒が過ごす場所であり、当該児童生徒が学習活動において日常的に学校にある情報システムにアクセスすることから、当該児童生徒をも想定した情報セキュリティ対策が必要であり、行政事務とは異なる「対策基準」が必要と考えられます。

こうした状況に鑑み、文部科学省は平成29年10月18日付けで「教育情報セキュリティポリシーに関するガイドライン」を制定し（その後令和元年12月、令和３年５月及び令和４年３月に改訂）、学校の設置者である地方公共団体は、学校における情報セキュリティポリシーの「基本方針」は、市全体に共通するものに従いつつも、「対策基準」については学校を想定したものを教育委員会が統一して策定することが望ましいとしました。

そこで、当市教育情報セキュリティポリシー（対策基準）を上記ガイドラインに則り策定することとしました。したがって、「基本方針」は、「今治市情報セキュリティポリシー」中の「第２章　基本方針」をそのまま採用します（次ページの図参照）。ここに再掲はしませんが、諸兄においては別途参照していただきたい。「基本方針」とともに情報セキュリティポリシーの構成要素である「対策基準」について、学校にフォーカスしたものを次章以降に述べます。

なお、教育委員会には学校教育以外の所管事項もあり、学校においても行政一般に共通の事務等同様の事項があることから、「今治市情報セキュリティポリシー」の対策基準が依然そのまま適用される担当部署及び業務があることに留意する必要があります。したがって、教育委員会においては、学校を対象とした対策基準と市全体を対象とした対策基準が並立するものであることを付言します。



地方公共団体における教育情報セキュリティポリシーに関する体系図

第２章　学校における教育情報セキュリティ対策基準

２．１．　対象範囲及び用語説明

（１）行政機関の範囲

本対策基準が適用される行政機関は、市長、教育委員会及び学校（小学校及び中学校をいう。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、次のとおりとする。

①教育ネットワーク、教育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

（３）用語説明

本対策基準における用語は、以下の通りとする。

用語	定義
校務系情報	児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教員の個人情報など、学校が保有する情報資産のうち、それら情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報
校務外部接続系情報（公開系情報）	校務系情報のうち、保護者メールや学校ホームページ等インターネット接続を前提とした校務で利用される情報
学習系情報	児童生徒のワークシート、作品など、学校が保有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ、当該情報に教員及び児童生徒がアクセスすることが想定されている情報
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	校務外務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、並びに校務系情報を扱う上

	で、適切なアクセス権が設定された領域で利用されるシステム
校務外部接続系システム	校務外部接続系ネットワーク、メールサーバ、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、並びに学習系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
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	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

２．２．　組織体制

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

①副市長を、CISOとする。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。

②CISO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アドバイザーとして置くものとする。

（２）統括教育情報セキュリティ責任者

①教育長を、CISO直属の統括教育情報セキュリティ責任者とする。統括教育情報セキュリティ責任者はCISOを補佐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。（本市の共通的なネットワークに係るものを除く。）

③統括教育情報セキュリティ責任者は、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。（本市の共通的なネットワークに係るものを除く。）

④統括教育情報セキュリティ責任者は、教育情報セキュリティ責任者、教育情報セキュリティ管理者、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統括教育情報セキュリティ責任者は、本対策基準が対象とする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、CISOの指示に従い、CISOが不在の場合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総括教育情報セキュリティ責任者は、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。(本市の共通的なネットワーク、情報システム及び情報資産に係るものを除く。)

⑦総括教育情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、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統括教育情報セキュリティ責任者は、緊急時には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。

（3）教育情報セキュリティ責任者

①副教育長を教育情報セキュリティ責任者とする。

②教育情報セキュリティ責任者は、本市の教育情報セキュリティ対策に関する総括的な権限及び責任を有する。

③教育情報セキュリティ責任者は、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、見直し等を行う総括的な権限及び責任を有する。

④教育情報セキュリティ責任者は、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、教育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（教職員、非常勤教職員及び臨時教職員をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。

（4）教育情報セキュリティ管理者

①校長を、教育情報セキュリティ管理者とする。

②教育情報セキュリティ管理者は、当該学校の情報セキュリティ対策に関する権限及び責任を有する。

③教育情報セキュリティ管理者は、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は、情報セキュリティに関する統一的な窓口（後述（9））、教育情報セキュリティ責任者、統括教育情報セキュリティ責任者及びCISOへ速やかに報告を行い、指示を仰がなければならない。

（5）教育情報システム管理者

①各教育情報システムの担当課長を、当該教育情報システムに関する教育情報システム管理者とする。

②教育情報システム管理者は、所管する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教育情報システム管理者は、所管する教育情報システムにおける情報セキュリティに関する権限及び責任を有する。

④教育情報システム管理者は、所管する教育情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（6）教育情報システム担当者

①各教育情報システムの担当課の職員を、教育情報システム担当者とする。

②教育情報システム担当者は、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。

（7）情報セキュリティに関する統一的な窓口、統括情報セキュリティ責任者及び情報セキュリティ委員会

本市の情報セキュリティ対策を統一的に取り扱う「情報セキュリティに関する統一的な窓口」、「統括情報セキュリティ責任者」及び「情報セキュリティ委員会」は、「今治市情報セキュリティポリシー」の定めるところによる。本市の教育ネットワークは、教育委員会独自の構築管理でなく、市行政ネットワークの一部として一体運用されている。情報セキュリティ対策についても、市として統一的に実施することがほとんどである。このため、本対策基準にあっても、「今治市情報セキュリティポリシー」中の組織との連携は必至であり、教育委員会の組織で完結しないことに留意する必要がある。

（8）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。

2．3．　情報資産の分類と管理方法

（1）情報資産の分類

本対策基準が対象とする情報資産は、機密性、完全性及び可用性により、次により分類し、必要に応じて取扱制限を行うものとする。

【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ていないが、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、児童生徒がアクセスすることを想定している情報資産	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、業務の遂行に支障がある情報
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	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がある情報

	ある情報資産	
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、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	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

【機密性、完全性及び可用性を踏まえた重要性分類】

重要性分類
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
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もの
Ⅲ　セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼすもの
Ⅳ　影響をほとんど及ぼさないもの

（２）情報資産の管理

①管理責任

（ア）教育情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

（イ）情報資産が複製又は伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。

②情報資産の分類の表示

教職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的媒体（ＣＤ－Ｒのラベル等）、文書の隅等に情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わねばならない。

③情報の作成

（ア）教職員等は、業務上必要のない情報を作成してはならない。

（イ）情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

（ウ）情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

④情報資産の入手

（ア）学校内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

（イ）学校外の者が作成した情報資産を入手した者は、（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

（ウ）情報資産を入手した者は、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管理者に判断を仰がなければならない。

⑤情報資産の利用

（ア）情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

（イ）情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。

（ウ）情報資産を利用する者は、電磁的記録媒体又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、当該電磁的記録媒体を取り扱わなければならない。

⑥情報資産の保管

（ア）教育情報セキュリティ管理者又は教育情報システム管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

（イ）教育情報セキュリティ管理者又は教育情報システム管理者は、情報資産を記録したUSBメモリ等の外部電磁的記録媒体を保管する場合は、外部電磁的記録媒体への書込禁止の措置を講じなければならない。

（ウ）教育情報セキュリティ管理者又は教育情報システム管理者は、情報システムのバックアップで取得したデータを記録する電磁的記録媒体を保管する場合は、

自然災害を被る可能性が低い地域に保管しなければならない。なお、クラウドサービスを利用する場合は、サービスの機能として自然災害対策がなされていることを確認すること。

（エ）教育情報セキュリティ管理者又は教育情報システム管理者は、重要性分類Ⅲ以上（機密性２Ａ以上、完全性２Ａ以上又は可用性２Ａ以上）の情報を記録した電磁的記録媒体を保管する場合、耐火、耐震、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦情報の送信

情報資産が組織内部（組織が利用するサーバやクラウドサービス等）から組織外部（家庭や地域、事業者等）に電子メール等により外部送信される場合は、情報資産分類に応じ、以下を実施しなければならない。

（ア）電子メール等により重要性分類Ⅲ以上（機密性２Ａ以上）の情報を外部送信する者は、限定されたアクセスの措置設定（アクセス制限や暗号化）を行わなければならない。

（イ）教育情報セキュリティ管理者及び教育情報システム管理者は、電子メール等による外部送信の安全性を高めるため、添付される情報資産を監視する等、出口対策を実施しなければならない。

⑧情報資産の運搬

（ア）車両等により重要性分類Ⅲ以上（機密性２Ａ以上）の情報資産を運搬する者は、必要に応じ施錠できるケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

（イ）重要性分類Ⅲ以上（機密性２Ａ以上）の情報資産を運搬する者は、教育情報セキュリティ管理者に許可を得なければならない。

⑨情報資産の提供・公表

（ア）重要性分類Ⅲ以上（機密性２Ａ以上）の情報資産を外部に提供する者は、限定されたアクセスの措置設定を行わなければならない。

（イ）重要性分類Ⅲ以上（機密性２Ａ以上）の情報資産を外部に提供する者は、教育情報セキュリティ管理者に許可を得なければならない。

（ウ）教育情報セキュリティ管理者及び教育情報システム管理者は、保護者等に公開する情報資産について、完全性を確保しなければならない。

⑩情報資産の廃棄

（ア）重要性分類Ⅲ以上（機密性２Ａ以上）の情報資産を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。

（イ）情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

（ウ）情報資産の廃棄を行う者は、教育情報セキュリティ管理者の許可を得なければならない。

2．4．　物理的セキュリティ

2.4.1．　サーバ等の管理

（1）機器の取付け

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

（2）サーバの冗長化

①教育情報システム管理者は、校務系サーバその他の重要情報を格納しているサーバ、セキュリティサーバ及びその他の基幹サーバについて障害が発生した場合を想定し、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。

②教育情報システム管理者は、学習系サーバその他の学習系情報を格納しているサーバのハードディスクを冗長化しなければならない。

（3）機器の電源

①教育情報システム管理者は、教育情報セキュリティ責任者及び施設管理部門と連携し、校務系サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正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。

②教育情報システム管理者は、教育情報セキュリティ責任者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

①教育情報セキュリティ責任者及び教育情報システム管理者は、施設管理部門と連携し、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。

②教育情報セキュリティ責任者及び教育情報システム管理者は、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。

③教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク接続口（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正に管理しなければならない。

④教育情報セキュリティ責任者及び教育情報システム管理者は、自ら又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

①教育情報システム管理者は、重要性分類Ⅲ以上（可用性２Ａ以上）のサーバ等の機器の定期保守を実施しなければならない。

②教育情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、教育情報システム管理者は、外部の事業者に故障を修理させるに当たり、修理を委託する事業者との間で、守秘義務契約を締結するとともに秘密保持体制の確認等を行わなければならない。

（６）施設外又は学校外への機器の設置

教育情報セキュリティ責任者及び教育情報システム管理者は、施設外又は学校外にサーバ等の機器を設置する場合、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。

（７）機器の廃棄等

教育情報システム管理者は、機器を廃棄又はリース返却等をする場合、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。

２.４.２. 管理区域（情報システム室等）の管理

（１）管理区域の構造等

①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（以下「情報システム室」という。）又は電磁的記録媒体の保管庫をいう。

②教育情報セキュリティ責任者及び教育情報システム管理者は、管理区域に外部からの侵入が容易にできないように必要な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及び教育情報システム管理者は、施設管理部門と連携して、許可されていない立入りを防止するよう対策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及び教育情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

⑤教育情報セキュリティ責任者及び教育情報システム管理者は、管理区域に配置する

消火薬剤や消防用設備等が、機器等及び電磁的記録媒体等に影響を与えないようにしなければならない。

（２）管理区域の入退室管理等

①教育情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ＩＣカード、指紋認証等の生体認証又は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。

②地方公共団体職員等及び外部委託事業者が管理区域に入室することを許可する場合、これらの者に身分証明書等の携帯を義務付け、必要に応じ、その提示を求めなければならない。

③教育情報システム管理者は、外部からの訪問者が管理区域に入る場合は、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された地方公共団体職員等が付き添うものとし、外見上地方公共団体職員等と区別できる措置を講じなければならない。

④教育情報システム管理者は、重要性分類Ⅱ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又は個人所有であるコンピュータ、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

①教育情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ地方公共団体職員又は委託した業者に確認を行わせなければならない。

②教育情報システム管理者は、情報システム室の機器等の搬入出について、地方公共団体職員を立ち会わせなければならない。

2.4.3. 通信回線及び通信回線装置の管理

①教育情報セキュリティ責任者は、施設内の通信回線及び通信回線装置を、施設管理部門と連携し、適正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し、構成図、仕様書等、記録媒体の形態に関わりなく適切に保管しなければならない。

②教育情報セキュリティ責任者及び教育情報システム管理者は、外部へのネットワーク接続ポイント及び該当ポイントに接続される端末を正確に把握し、適正な管理を行わなければならない。

③教育情報セキュリティ責任者は、重要性分類Ⅲ以上（機密性２Ａ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、適正な回線を選択しなければならない。また、必要に応じ、通信経路上での暗号化を行わなければならない。

④教育情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報の破壊、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を実施しなければならない。

⑤教育情報セキュリティ責任者は、重要性分類Ⅱ以上の情報資産を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。

2.4.4. 教職員等の利用する校務用端末、校務外部接続用端末及び指導者用端末並びに電磁的記録媒体等の管理

（1）教育情報システム管理者は、不正アクセス防止のため、ログイン時のＩＤ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適正な物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

（2）教育情報システム管理者は、校務系システム、タブレット端末やパソコン等教育情報システムへアクセスする端末へのＩＤやログインパスワードの入力を必要とするように設定しなければならない。

（3）教育情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の多要素認証を設定しなければならない。アクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産のアクセスについては、多要素認証を必須とすること。

（4）教育情報システム管理者は、必要に応じて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。

（5）教育情報システム管理者は、アクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産を取り扱う端末に対し、当該ファイルの暗号化等の措置により、不正アクセスや教員の不注意等による情報流出への対策を講じなければならない。

（6）教育情報システム管理者は、モバイル端末の学校外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。

（7）教育情報システム管理者は、パソコンやモバイル端末におけるマルウェア観戦の脅威に対し、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。アクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産を取り扱う端末に対し、当該端末の状況及び通信内容を監視

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。

（8）教育情報システム管理者は、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対策を講じなければならない。

2.4.5. コンピュータ教室等の学習者用端末の管理

①教育情報システム管理者は、盗難防止のため、教室等で利用する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教育情報システム管理者は、電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

②教育情報システム管理者は、情報システムへの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。

2.5. 人的セキュリティ

2.5.1. 教職員等の遵守事項

（1）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

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

②業務以外の目的での使用の禁止

教職員等は、業務以外の目的で情報資産の外部への持ち出し、教育情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

③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・学校が構築・管理している環境（本対策基準が適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境）の外部における情報処理作業の制限

（ア）CISOは、重要性分類Ⅱ以上の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

（イ）教職員等は、学校のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、教育情報セキュリティ管理者の許可を得なければならない。

（ウ）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管理者の許可を得なければならない。

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、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断をCISOが行った後に、業務上必要な場合は、教育情報セキュリティ管理者の許可を得て利用することができる。

（イ）教職員等は、支給以外のパソコン、モバイル端末を利用した外部での情報処理作業を行う場合は、教育情報セキュリティ管理者の許可を得たうえで、安全管理措置に関する規定を遵守しなければならない。

⑤持ち出し及び持ち込みの記録

教育情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。なお、アクセス制御による対策を講じたシステム構成の場合は、教育情報セキュリティ管理者の包括的承認を行う等、運用実態や教職員等の負担も考慮し検討すること。

⑥パソコンやモバイル端末におけるセキュリティ設定変更の禁止

教職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を教育情報セキュリティ管理者の許可なく変更してはならない。

⑦机上の端末等の管理

教職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は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、適正な措置を講じなければならない。

⑧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。

⑨児童生徒への指導

児童生徒は、教職員等でないことから、教育情報セキュリティポリシーを遵守する義務を負うものではないが、学校の学習系システムを利用することから、教職員等は児童生徒に対し、学習者用端末等を活用させるに当たり留意すべき事項を指導しなければならない。

（２）非常勤及び臨時の教職員への対応

①教育情報セキュリティポリシー等の遵守

教育情報セキュリティ管理者は、非常勤及び臨時の教職員に対し、採用時に教育情報セキュリティポリシー等のうち、非常勤及び臨時の教職員が守るべき内容を理

解させ、また実施及び遵守させなければならない。

②教育情報セキュリティポリシー等の遵守に対する同意

教育情報セキュリティ管理者は、非常勤及び臨時の教職員の採用の際、必要に応じ、教育情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

③インターネット接続及び電子メール使用時の制限

教育情報セキュリティ管理者は、非常勤及び臨時の教職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

（3）教育情報セキュリティポリシー等の掲示

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

（4）外部委託事業者に対する説明

教育情報システム管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、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。

2.5.2. 研修・訓練

（1）情報セキュリティに関する研修・訓練

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

①CISO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、情報セキュリティ委員会の承認を得なければならない。

②研修計画において、教職員等が毎年度最低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。

③新規採用の教職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

④研修は、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム担当者及びその他の教職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

⑤CISOは、毎年度1回、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

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。

2.5.3. 情報セキュリティインシデントの報告

（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を認知した場合、速やかに教育情報セキュリティ管理者に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は、速やかに教育情報システム管理者に報告しなければならない。

③教育情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じてCISO及び統括教育情報セキュリティ責任者、教育情報セキュリティ責任者及び情報セキュリティに関する統一的窓口に報告しなければならない。

（2）住民等外部からの情報セキュリティインシデントの報告

①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、速やかに教育情報セキュリティ管理者に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は、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報システム管理者及び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。

③教育情報セキュリティ管理者は、当該情報セキュリティインシデントについて、必要に応じてCISO及び教育情報セキュリティ責任者に報告しなければならない。

（3）情報セキュリティインシデント原因の究明・記録、再発防止等

①教育情報セキュリティ責任者は、情報セキュリティインシデントについて、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の原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO及び統括教育情報セキュリティ責任者に報告

しなければならない。

②CISOは、教育情報セキュリティ責任者から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

2.5.4. ＩD及びパスワード等の管理

（1）ＩＣカード等の取扱い

①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又はパソコン等の端末のスロット等から抜いておかなければならない。

（ウ）ＩＣカード等を紛失した場合には、速やかに教育情報セキュリティ管理者、教育情報システム管理者及び教育情報セキュリティ責任者に通報し、指示に従わなければならない。

②教育情報セキュリティ責任者、及び教育情報システム管理者は、ＩＣカード等の紛失等の通報があり次第、当該ＩＣカード等を使用したアクセス等を速やかに停止しなければならない。

③教育情報セキュリティ責任者、及び教育情報システム管理者は、ＩＣカード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

（2）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を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）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パスワードは、他者に知られないように管理しなければならない。

②パスワードを秘密にし、パスワードの照会等に一切応じてはならない。

③パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

④パスワードが流出したおそれがある場合は、教育情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

⑤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。）

⑥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。

⑦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。

⑧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。）

⑨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。

⑩取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の多要素認証を設定しなければならない。

2．6．　技術的セキュリティ

2.6.1．　コンピュータ及びネットワークの管理

（1）文書サーバの設定等

①教育情報システム管理者は、教職員等が使用できる文書サーバの容量を設定し、教職員等に周知しなければならない。

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

③教育情報システム管理者は、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教育情報システム管理者は、インターネット接続を前提とする校務外部接続系サーバ及び学習系サーバに保管する情報（学習系サーバにおいては、個人情報などを含む重要性が高い情報を保管する場合に限る。）については、標的型攻撃等によるファイルの外部流出の可能性を考慮し、ファイル暗号化等による安全管理措置を講じなければならない。

（2）バックアップの実施

教育情報セキュリティ責任者及び教育情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、次の①及び②に基づきバックアップを実施するものとする。

①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。

②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。

（3）他団体との情報システムに関する情報等の交換

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

（4）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。

②教育情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

③統括教育情報セキュリティ責任者、教育情報システム管理者又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名以上で作業し、互いにその作業を確認しなければならない。

（5）情報システム仕様書等の管理

教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク構成図、情報システム仕様書について、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、適正に管理しなければならない。

（6）ログの取得等

①教育情報セキュリティ責任者及び教育情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

②教育情報セキュリティ責任者及び教育情報システム管理者は、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。

③教育情報セキュリティ責任者及び教育情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（7）障害記録

教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録

し、適正に保存しなければならない。

（8）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、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正なアクセス制御を施さなければならない。

（9）外部の者が利用できるシステムの分離等

教育情報システム管理者は、保護者等の外部の者が利用できるシステム等がある場合、重要性が高い情報、特に情報資産重要性分類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）以上を扱うシステムとの論理的若しくは物理的な分離、又はシステムにおけるアクセス権管理の徹底を行わなければならない。

（10）外部ネットワークとの接続制限等

①教育情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合は、CISO及び統括教育情報セキュリティ責任者の許可を得なければならない。

②教育情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内及び学校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。

③教育情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業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の損害賠償責任を契約上担保しなければならない。

④教育情報セキュリティ責任者及び教育情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、教育ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

⑤教育情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが予想される場合は、教育情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

(11) 重要性が高い情報に対するインターネットを介した外部からのリスク、児童生徒による重要性の高い情報へのアクセスリスクへの対応

①教育情報システム管理者は、アクセス制御による対策を講じたシステム構成の場合は、各システムにおけるアクセス権管理の徹底をしなければならない。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は、校務系システム及び学習系システム間の通信経路の物理的又は論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を介した外部からのリスクの高いシステムと重要性が高い情報(特に校務系)を論理的又は物理的に分離をしなければならない。

②教育情報システム管理者は、校務系システムとその他のシステム（校務外部接続系システム、学習系システム）との間で通信する場合は、各システムにおけるアクセス権管理の徹底を行う等の適切な措置を図らなければならない。また、ネットワーク分離による対策を講じたシステム構成で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。

(12) 複合機のセキュリティ管理

①教育情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能及び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、適正なセキュリティ要件を策定しなければならない。

②教育情報セキュリティ責任者は、複合機が備える機能について適正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。

③教育情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消する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。

(13) IoT機器を含む特定用途機器のセキュリティ管理

教育情報システム管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

(14) 無線ＬＡＮ及びネットワークの盗聴対策

①教育情報セキュリティ責任者は、無線ＬＡＮの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

②教育情報セキュリティ責任者は、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。

(15) 電子メールのセキュリティ管理

①教育情報セキュリティ責任者は、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。

③教育情報セキュリティ責任者は、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。

④教育情報セキュリティ責任者は、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し、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。

⑤教育情報セキュリティ責任者は、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は、作業上必要と認められる場合に限り、外部委託事業者との間で利用方法を取り決め利用できるものとする。

(16) 電子メールの利用制限

①教職員等は、自動転送機能を用いて、電子メールを転送してはならない。

②教職員等は、業務上必要のない送信先に電子メールを送信してはならない。

③教職員等は、複数人に電子メールを送信する場合、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。

④教職員等は、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管理者に報告しなければならない。

⑤教職員等は、ウェブで利用できる電子メール、ネットワークストレージサービス等を使用してはならない。ただし、ネットワーク上のセキュリティに問題がないことが確認でき、職務上必要と認められる場合に限り、教育情報セキュリティ責任者の許可を得て使用することができる。

(17) 電子署名・暗号化

①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は、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。

②教職員等は、暗号化を行う場合にCISOが定める以外の方法を用いてはならない。また、CISOが定めた方法で暗号のための鍵を管理しなければならない。

③CISO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。

(18) 無許可ソフトウェアの導入等の禁止

①教職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

②教職員等は、業務上の必要がある場合は、教育情報セキュリティ責任者及び教育情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、教育情報セキュリティ管理者又は教育情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

③教職員等は、不正にコピーしたソフトウェアを利用してはならない。

(19) 機器構成の変更の制限

①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。

②教職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合は、教育情報セキュリティ責任者及び教育情報システム管理者の許可を得なければならない。

(20) 無許可でのネットワーク接続の禁止

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

(21) 業務以外の目的でのウェブ閲覧の禁止

①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。

②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。

2.6.2. アクセス制御

(1) アクセス制御等

①アクセス制御

教育情報セキュリティ責任者又は教育情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員等がアクセスできないように、システム上制限しなければならない。アクセス制御による対策を講じたシステム構成の場合、重要な情報資産へのアクセスについては、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利用者ＩＤの取扱い

(ア) 教育情報セキュリティ責任者及び教育情報システム管理者は、利用者の登録、

変更、抹消等の情報管理、教職員等の異動、出向、退職者に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

（イ）教職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、教育情報セキュリティ責任者又は教育情報システム管理者に通知しなければならない。

（ウ）教育情報セキュリティ責任者及び教育情報システム管理者は、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。

③特権を付与されたＩＤの管理等

（ア）教育情報セキュリティ責任者及び教育情報システム管理者は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワード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。

（イ）教育情報セキュリティ責任者及び教育情報システム管理者の特権を代行する者は、教育情報セキュリティ責任者及び教育情報システム管理者が指名することができる。

（ウ）教育情報セキュリティ責任者及び教育情報システム管理者は、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。

（エ）教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与されたＩＤ及びパスワードについて、その利用期間に合わせて特権ＩＤを作成・削除する、若しくは、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。

（オ）教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与されたＩＤを初期設定以外のものに変更しなければならない。

（２）外部からのアクセス等の制限

①教職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、教育情報セキュリティ責任者及び当該情報システムを管理する教育情報システム管理者の許可を得なければならない。

②教育情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③教育情報セキュリティ責任者は、組織外部からのアクセスを認める場合、アクセスする利用者の本人確認、システムアクセスの対象となる児童生徒の本人（保護者）同意を得る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。

⑤教育情報セキュリティ責任者及び教育情報システム管理者は、外部からのアクセスに利用するモバイル等の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。

⑥教職員等は、持ち込んだ又は持ち帰ったモバイル等の端末を施設内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

⑦教育情報セキュリティ責任者は、外部から教育ネットワークに接続することを許可する場合は、利用者のＩＤ、パスワード及び生体認証に係る情報等の認証情報並びに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）自動識別の設定

教育情報セキュリティ責任者及び教育情報システム管理者は、児童生徒が学校のネットワークで使用する機器について、機器固有情報又はデバイス証明書によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

（４）ログイン時の表示等

教育情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ教職員等がログインしたことを確認することができるようシステムを設定しなければならない。

（５）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又は教育情報システム管理者は、教職員等のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

②教育情報セキュリティ責任者又は教育情報システム管理者は、教職員等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。

（６）特権による接続時間の制限

教育情報セキュリティ責任者又は教育情報システム管理者は、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。

2.6.3. システム開発、導入、保守等

（1）情報システムの調達

①教育情報セキュリティ責任者及び教育情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

②教育情報セキュリティ責任者及び教育情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（2）情報システムの開発

①システム開発における責任者及び作業者の特定

教育情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

②システム開発における責任者、作業者のＩＤの管理

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

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

③システム開発に用いるハードウェア及びソフトウェアの管理

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

（イ）教育情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

（3）情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

（ア）教育情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

（イ）教育情報システム管理者は、システム開発・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。

（ウ）教育情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

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

②テスト

（ア）教育情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

（イ）教育情報システム管理者は、運用テストを行う場合、あらかじめ疑似環境による操作確認を行わなければならない。

（ウ）情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

（エ）教育情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織に、それぞれ独立したテストを行わせなければならない。

（オ）教育情報システム管理者は、運用環境への移行に先立ち、システムの脆弱性テストを行い、その結果を確認しなければならない。

（4）システム開発・保守に関連する資料等の整備・保管

①教育情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

②教育情報システム管理者は、テスト結果を一定期間保管しなければならない。

③教育情報システム管理者は、情報システムに係るソースコード及び使用したオープンソースのバージョン（リポジトリ）を適正な方法で保管しなければならない。

（5）情報システムにおける入出力データの正確性の確保

①教育情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

②教育情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③教育情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（6）情報システムの変更管理

教育情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（7）開発・保守用のソフトウェアの更新等

教育情報システム管理者は、開発・保守用のソフトウェア等の更新又はパッチの適

用をする場合、他の情報システムとの整合性を確認しなければならない。

（8）システム更新又は統合時の検証等

教育情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

2.6.4. 不正プログラム対策

（1）教育情報セキュリティ責任者の措置事項

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

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などにおいて、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。

③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。

⑤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。

⑥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。

⑦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）教育情報システム管理者の措置事項

教育情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

①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。

②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。

③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。

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

（3）教職員等の遵守事項

教職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

①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。

②外部からデータ又はソフトウェアを取り入れる場合は、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差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

④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教育情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。

⑦コンピュータウイルス等の端末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、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

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

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。

（4）専門家の支援体制

教育情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

2.6.5. 不正アクセス対策

（1）教育情報セキュリティ責任者の措置事項

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

①使用されていないポート及びSSID（無線ＬＡＮネットワーク名）を閉鎖しなければならない。
②不要なサービスについて、機能を削除又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及び教育情報システム管理者へ通報するよう、設定しなければならない。
④重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。
⑤教育情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正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）攻撃への対処

CISO及び統括教育情報セキュリティ責任者は、サーバ等に攻撃を受け又は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収集に努めなければならない。

（3）記録の保存

CISO及び統括教育情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合は、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。

（4）内部からの攻撃

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

（5）教職員等による不正アクセス

教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等による不正アクセスを発見した場合は、当該教職員等が所属する学校等の教育情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

（6）サービス不能攻撃

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

じなければならない。

（7）標的型攻撃

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

2.6.6. 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

教育情報セキュリティ責任者及び教育情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（2）不正プログラム等のセキュリティ情報の収集・周知

教育情報セキュリティ責任者及び教育情報システム管理者は、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

教育情報セキュリティ責任者及び教育情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術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。

2.7. 運用

2.7.1. 情報システムの監視

①教育情報セキュリティ責任者及び教育情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

②教育情報セキュリティ責任者及び教育情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

③教育情報セキュリティ責任者及び教育情報システム管理者は、重要性分類Ⅱ以上の情報資産を格納する校務系システム及び校務外部接続系システムを常時監視しなければ

ならない。

④教育情報セキュリティ責任者及び教育情報システム管理者は、重要性分類Ⅲ以上の情報資産を格納する学習系システムを常時監視しなければならない。

2.7.2. 教育情報セキュリティポリシーの遵守状況の確認

（1）遵守状況の確認及び対処

①教育情報セキュリティ責任者及び教育情報セキュリティ管理者は、教育情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合は、速やかにCISO及び統括教育情報セキュリティ責任者に報告しなければならない。

②CISOは、発生した問題について、適正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及び教育情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における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、問題が発生していた場合は適正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

CISO及び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）教職員等の報告義務

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、直ちに教育情報セキュリティ責任者及び教育情報セキュリティ管理者に報告しなければならない。

②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統括教育情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適正に対処しなければならない。

2.7.3. 侵害時の対応等

（1）緊急時対応計画の策定

CISO又は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に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において、連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

（2）緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

①関係者の連絡先

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）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、情報セキュリティ委員会は当該計画と教育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

CISO又は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。

2.7.4. 例外措置

（1）例外措置の許可

教育情報セキュリティ管理者及び教育情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、学校事務及び教育活動の適正な遂行を継続するため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合は、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

教育情報セキュリティ管理者及び教育情報システム管理者は、学校事務及び教育活動の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに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

CISOは、例外措置の申請書及び審査結果を適正に保管しなければならない。

2.7.5. 法令等遵守

教職員等は、職務の遂行において使用する情報資産を保護するために、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年法律第261号）

②教育公務員特例法（昭和24年法律第１号）
③地方教育行政の組織及び運営に関する法律（昭和31年法律第162号）
④著作権法（昭和45年法律第48号）
⑤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）
⑥個人情報の保護に関する法律（平成15年法律第57号）
⑦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）
⑧サイバーセキュリティ基本法（平成28年法律第31号）
⑨今治市個人情報保護条例（平成17年条例第21号）
⑩今治市教育委員会が取り扱う個人情報の保護に関する規則（平成17年教育委員会規則第69号）
⑪今治市情報資産の管理運用に関する規則（平成18年規則第２号）

2.7.6. 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法令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は、速やかに次の措置を講じなければならない。

①統括教育情報セキュリティ責任者が違反を確認した場合は、統括教育情報セキュリティ責任者は当該教職員等が所属する学校の教育情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

②教育情報セキュリティ管理者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統括教育情報セキュリティ責任者及び当該教職員等が所属する学校の教育情報セキュリティ管理者に通知し、適正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管理者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又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は、教職員等の権利を停止又は剥奪した旨をCISO及び当該教職員等が所属する学校の教育情報セキュリティ管理者に通知しなければならない。

2．8．　外部サービスの利用

2.8.1．外部委託

（1）外部委託事業者の選定基準

①教育情報システム管理者は、外部委託事業者の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

②教育情報システム管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定しなければならない。

（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は、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・教育情報セキュリティポリシー及び教育情報セキュリティ実施手順の遵守
・外部委託事業者の責任者、委託内容、作業者及び作業場所の特定
・提供されるサービスレベルの保証
・外部委託事業者にアクセスを許可する情報の種類及び範囲並びにアクセス方法
・外部委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び受託者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・市による監査、検査
・市による情報セキュリティインシデント発生時の公表
・教育情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

（3）確認・措置等

教育情報システム管理者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、（2）の契約に基づき措置しなければならない。また、その内容を統括教育情報セキュリティ責任者に報告するとともに、その重要度に応じてCISOに報告しなければならない。

2.8.2．約款による外部サービスの利用

（1）約款による外部サービスの利用に係る規定の整備

教育情報システム管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、機密性の高い情

報の取扱いには十分留意するよう規定しなければならない。
①約款によるサービスを利用してよい範囲
②業務により利用する約款による外部サービス
③利用手続及び運用手順

（２）約款による外部サービスの利用における対策の実施
教職員等は、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、適正な措置を講じた上で利用しなければならない。

2.8.3. ソーシャルメディアサービスの利用

（１）教育情報システム管理者は、教育委員会又は学校が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。
①本市のアカウントによる情報発信が、実際に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実施すること。
②パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ＩＣカード等）を適正に管理するなどの方法で、不正アクセス対策を実施すること。

（２）重要性分類Ⅲ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。

（４）アカウント乗っ取りを確認した場合は、被害を最小限にするための措置を講じなければならない。

2.8.4. クラウドサービスの利用

①教育情報システム管理者は、クラウドサービス（民間事業者が提供するものに限らず、本市が自ら提供するもの等を含む。以下同じ。）を利用するに当たり、取り扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断しなければならない。
②教育情報システム管理者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して事業者を選定し、必要に応じて事業の実施場

所及び契約に定める準拠法・裁判管轄を指定しなければならない。

③教育情報システム管理者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、事業者を選定する際の要件としなければならない。

④教育情報システム管理者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めなければならない。

⑤教育情報システム管理者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービス提供事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

⑥教育情報システム管理者は、前５号に定める事項を踏まえ、統括教育情報セキュリティ責任者及び教育情報セキュリティ責任者にクラウドサービス利用の可否を問わなければならない。

２．９．　１人１台端末におけるセキュリティ

２.９.１．　学習者用端末のセキュリティ対策

教育情報セキュリティ管理者をはじめ、１人１台端末の設置運用管理に携わる者は、連携して以下の事項に留意しなければならない。

（１）授業に支障のないネットワーク構成の選択（帯域や同時接続数など）

クラウドサービス提供事業者側のサービス要件基準を満たしたネットワーク構成を設計する。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立てること。

（２）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。

＜対策例＞

①フィルタリングソフト又はサービス

②検索エンジンのセーフサーチ

③セーフブラウジング

（３）マルウェア感染対策

学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

（４）端末を不正利用させないための防止策

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

（5）セキュリティ設定の一元管理

児童生徒への端末配布後においても、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。

（6）端末の盗難、紛失時の情報漏えい対策

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えいを防ぐ等の安全管理措置を講じなければならない。

（7）運用・連絡体制の整備

学校内外での端末の運用ルールを制定し、インシデント発生時の連絡先及び対応方法を各学校にて整理しなければならない。

2.9.2　児童生徒におけるＩＤ及びパスワード等の管理

（1）ＩＤ登録・変更・削除

①入学／転入時のＩＤ登録処理

ＩＤ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。

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／進学時にも変更不要とする。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（Mobile Device Management：モバイル機器管理システム）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とする。

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を行うものとする。

③転出／卒業時の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のデータ移行をサービス利用期間内に実施可能とし、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とする。　ただし、本人同意、保護者同意及び個人情報保護条例に従った適切な管理の下、一部のデータを活用することは可能とする。

（２）多要素認証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、システムが許容できるときは、児童生徒のＩＤ／パスワードに加えて多要素認証を設定することとする。

（３）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、サービス利用時に都度ＩＤ／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となるときは、システムが許容する限りにおいて、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とする。

2.10.　評価・見直し

2.10.1．監査

（１）実施方法

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、毎年度及び必要に応じて監査を行わせなければならない。

（２）監査を行う者の要件

①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。

②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

①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、情報セキュリティ委員会の承認を得なければならない。

②被監査部門は、監査の実施に協力しなければならない。

（4）外務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、監査結果をとりまとめ、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正に保管しなければならない。

（7）監査結果への対応

CISOは、監査結果を踏まえ、指摘事項を所管する教育情報セキュリティ責任者及び教育情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない教育情報セキュリティ責任者及び教育情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

（8）教育情報セキュリティポリシー及び関係規定等の見直し等への活用

情報セキュリティ委員会は、監査結果を教育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。

2.10.2. 自己点検

（1）実施方法

①教育情報セキュリティ責任者及び教育情報システム管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

②教育情報セキュリティ責任者は、教育情報セキュリティ管理者と連携して、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

教育情報セキュリティ責任者及び教育情報システム管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、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

①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。

②情報セキュリティ委員会は、この点検結果を教育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。

2.10.3. 教育情報セキュリティポリシー及び関係規定等の見直し

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、教育情報セキュリティポリシー及び関係規定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。

資料２

第９回教育委員会議案第 30 号

今治市公民館運営審議会委員の委嘱について

標記のことについて、社会教育法第 30 条第 1 項の規定により別紙の者に委嘱する。

令和４年７月８日提出

今治市教育委員会
教育長　田坂　敏

「理　　由」
欠員補充による

今治市公民館運営審議会委員候補者名簿

館名　　今治市中央公民館

	氏　　名	区　　分	備　　考
候補者	大澤　誠二	学校教育の関係者	今治市小中学校長会長
	越智　千英子	社会教育の関係者	今治市連合婦人会
	八木　正史	社会教育の関係者	今治市ＰＴＡ連合会長
	清水　正惠	家庭教育の向上に資する活動を行う者	今治市母子寡婦福祉連合会長
任　　期		令和４年７月８日　～　令和５年７月８日	

退　任　委　員

	氏　　名	区　　分	備　　考
前任者	高井　　剛	学校教育の関係者	今治市小中学校長会長
	阿部　ツヤ子	学校教育の関係者	今治市連合婦人会副会長
	中川　豊和	社会教育の関係者	今治市ＰＴＡ連合会長
	志尾　順子	学識経験のある者	今治市民生児童委員協議会副会長

今治市公民館運営審議会委員候補者名簿

館名　今治市城東公民館

	氏　名	区　分	備　考
候補者	門岡　達也	学校教育の関係者	日吉中学校長
	片上　泰彦	学校教育の関係者	立花中学教頭
任　期	令和４年７月８日　～　令和５年５月１３日		

退　任　委　員

	氏　名	区　分	備　考
前任者	髙井　剛	学校教育の関係者	日吉中学校長
	佐藤 寿一	学校教育の関係者	立花中学教頭

今治市公民館運営審議会委員候補者名簿

館名　今治市富田公民館

	氏　名	区　分	備　考
候補者	藤原　勝彦	学校教育の関係者	富田小学校長
	馬越　吉章	学校教育の関係者	南中学校長
	秋山　正信	学識経験のある者	富田地区部落総代会長
任　期		令和４年７月８日　～　令和５年６月３日	

退任委員

	氏　名	区　分	備　考
前任者	馬越　吉章	学校教育の関係者	富田小学校長
	矢野　弘之	学校教育の関係者	南中学校長
	曽我部　通	学識経験のある者	富田地区部落総代会長

今治市公民館運営審議会委員候補者名簿

館名　今治市波止浜公民館

	氏　名	区　分	備　考
候補者	宇髙　淑文	学校教育の関係者	波止浜小学校長
	羽田　基美	社会教育の関係者	波止浜小学校ＰＴＡ教養研修部長
	山口　知奈	社会教育の関係者	北郷中学校ＰＴＡ副会長
	三宅　昇	学識経験のある者	波止浜校区自治会副会長
任　期		令和４年７月８日　～　令和５年２月２５日	

退　任　委　員

	氏　名	区　分	備　考
前任者	三好　春彦	学校教育の関係者	波止浜小学校長
	鳥生　有希	社会教育の関係者	波止浜小学校ＰＴＡ婦人部長
	山田　明美	社会教育の関係者	北郷中学校ＰＴＡ副会長

今治市公民館運営審議会委員候補者名簿

館名　今治市朝倉公民館

	氏　名	区　分	備　考
候補者	眞鍋　奈津美	社会教育の関係者	朝倉小学校ＰＴＡ代表
	池田　貴子	社会教育の関係者	朝倉中学校ＰＴＡ代表
任　期	令和４年７月８日　～　令和５年２月２５日		

退　任　委　員

	氏　名	区　分	備　考
前任者	高瀬　美希	社会教育の関係者	朝倉小学校ＰＴＡ代表
	酒井　英理	社会教育の関係者	朝倉中学校ＰＴＡ代表

今治市公民館運営審議会委員候補者名簿

館名　　今治市大三島公民館

	氏　　名	区　　分	備　　考
候補者	髙杉　秀夫	学校教育の関係者	大三島小学校長
	近藤　勲	学校教育の関係者	大三島中学校長
	永井　真奈美	社会教育の関係者	大三島認定こども園保護者会会長
	大亀　智子	社会教育の関係者	大三島町愛護班連絡協議会会長
任　　期	令和４年７月８日　～　令和５年６月３日		

退　任　委　員

	氏　　名	区　　分	備　　考
前任者	渡辺　務	学校教育の関係者	大三島小学校校長
	松岡　洋介	学校教育の関係者	大三島中学校校長
	杉野　浩代	社会教育の関係者	大三島認定こども園保護者会会長
	菅　一博	社会教育の関係者	大三島町愛護班連絡協議会会長

「参　照」

社会教育法（抜すい）

（公民館運営審議会）

第29条　公民館に公民館運営審議会を置くことができる。

2　公民館運営審議会は、館長の諮問に応じ、公民館における各種の事業の企画実施につき調査審議するものとする。

第30条　市町村の設置する公民館にあっては、公民館運営審議会の委員は、当該市町村の教育委員会が委嘱する。

2　前項の公民館運営審議会の委員の委嘱の基準、定数及び任期その他当該公民館運営審議会に関し必要な事項は、当該市町村の条例で定める。この場合において、委員の委嘱の基準については、文部科学省令で定める基準を参酌するものとする。

公民館運営審議会の委員の委嘱の基準を条例で
定めるに当たって参酌すべき基準を定める省令

社会教育法第30条第2項の文部科学省令で定める基準は、学校教育及び社会教育の関係者、家庭教育の向上に資する活動を行う者並びに学識経験のある者の中から委嘱することとする。

今治市公民館条例（抜すい）

（審議会）

第11条　法第29条第1項の規定により、公民館ごとに公民館運営審議会（以下「審議会」という。）を置く。

2　審議会は、公民館ごとに委員12人以内をもって組織し、その委員は、次に掲げる者のうちから教育委員会が委嘱する。

（1）学校教育及び社会教育の関係者

（2）家庭教育の向上に資する活動を行う者

（3）学識経験のある者

3　委員の任期は、2年とする。ただし、補欠の委員の任期は、前任者の残任期間とする。

4　特定の地位又は職により委嘱された委員の任期は、当該地位又は職にある期間とする。

資料　3

第９回教育委員会議案第 31 号

今治市青少年センター運営協議会委員の委嘱について

標記のことについて、今治市青少年センター条例第５条の規定により別紙の者に委嘱する。

令和４年７月８日　提出

今治市教育委員会
教育長　田坂　　敏

「理　　由」
欠員補充による

今治市青少年センター運営協議会委員 候補者名簿

	氏　名	区　分	備　考
候補者	野澤　道生	教育の機関の代表	今治地区高等学校等生徒指導連絡協議会会長 今治東中等教育学校長
	門岡　達也	教育の機関の代表	今治市小中学校長会代表 日吉中学校長
	脇田　康一	教育の機関の代表	今治市小中学校生徒指導主事会代表 近見中学校教諭
任　期		令和４年7月８日～令和５年７月３１日	

退　任　委　員

	氏　名	区　分	備　考
前任者	向井　誠二	教育の機関の代表	今治地区高等学校等生徒指導連絡協議会会長 今治南高等学校長
	高須　昌寿	教育の機関の代表	今治市小中学校長会代表 近見中学校長
	武田　洋輔	教育の機関の代表	今治市小中学校生徒指導主事会代表 日吉中学校教諭

「参　照」

今治市青少年センター条例（抜すい）

（運営協議会）

第5条　センターの適正な運営を図るため、今治市青少年センター運営協議会を置く。

2　今治市青少年センター運営協議会の委員(以下この条において「委員」という。)は、20人以内をもって組織し、今治市教育委員会(以下「教育委員会」という。)が委嘱する。

3　委員の任期は、2年とする。ただし、再任を妨げない。

4　補欠の委員の任期は、前任者の残任期間とする。

今治市青少年センター条例施行規則（抜すい）

（運営協議会委員）

第5条　条例第5条第2項に規定する今治市青少年センター運営協議会(以下「運営協議会」という。)の委員は、警察、教育、児童福祉、労働等の機関及び民間有志者の代表等のうちから今治市教育委員会(以下「教育委員会」という。)が委嘱する。

資料　4

第９回　教育委員会議案第 32 号

今治市視聴覚ライブラリー運営委員会委員の委嘱について

標記のことについて、今治市立視聴覚ライブラリー条例第１２条の規定により別紙の者に委嘱する。

令和４年７月８日　提出

今治市教育委員会
教育長　田坂　敏

「理　　由」
欠員補充による

今治市視聴覚ライブラリー運営委員会委員　候補者名簿

候補者	氏　　名	区　　分	役　職　名
	塩崎　規子	学校教育関係者	視聴覚教育部会　副委員長 別宮小学校　教諭
任　　期		令和４年７月８日　～　令和５年７月８日	

退任委員

前任者	氏　　名	区　　分	役　職　名
	石丸　大樹	学校教育関係者	視聴覚教育部会　委員長 吉海小学校　教諭

「参　照」

今治市立視聴覚ライブラリー条例（抜すい）

（委員）

第12条　運営委員会の委員（以下「委員」という。）の定数は、10人以内とする。

2　委員は、学校教育及び社会教育に関する教育関係者及び行政担当者並びに視聴覚教育に関する学識経験者のうちから選任するものとする。

3　委員の任期は、２年とする。ただし、補欠の委員の任期は、前任者の残任期間とする。

4　前項の規定にかかわらず、特定の地位又は職により任命された委員の任期は、当該地位又は職にある期間とする。

今治市立視聴覚ライブラリー条例施行規則（抜すい）

（運営委員会）

第６条　今治市視聴覚ライブラリー運営委員会（以下「運営委員会」という。）の委員は、次に掲げる者のうちから、教育委員会が任命し、又は委嘱する。

（１）　小中学校の代表者

（２）　社会教育関係団体及び施設の代表者

（３）　学校教育及び社会教育行政の担当者

（４）　学識経験者

資料５

第９回教育委員会議案第 33 号

今治市図書館運営審議会委員の委嘱について

標記のことについて、今治市執行機関の附属機関設置条例第４条の規定により別紙の者に委嘱する。

令和４年７月８日提出

今治市教育委員会
教育長　田坂　敏

「理　　由」
任期満了による

今治市図書館運営審議会委員　候補者名簿

	氏　　名	区　　分	役　職　名
候補者	菅　征永	学校教育及び社会教育の関係者	今治市立宮窪小学校長
	高橋　靖	学校教育及び社会教育の関係者	今治市立伯方中学校長
	森田　悦子	学校教育及び社会教育の関係者	今治市連合婦人会　副会長
	長尾　正人	家庭教育の向上に資する活動を行う者	今治市ＰＴＡ連合会　副会長
	松木　博	学識経験のある者	今治史談会委員
	濱田　栄子	学識経験のある者	今治明徳短期大学 幼児教育学科　講師
	日野　郁子	学識経験のある者	朗読奉仕グループ「みちくさ」代表
	八木　純子	学識経験のある者	朗読奉仕グループ「なみかた ざんぶらこ」メンバー
	阿部　由美子	学識経験のある者	お話グループ「やより」　会員
	金本　ひろみ	学識経験のある者	「ひよこの会」　代表
	木下　誠	学識経験のある者	利用者代表（中央図書館）
	菊川　世紀	学識経験のある者	利用者代表（波方図書館）
	竹内　信子	学識経験のある者	利用者代表（大西図書館）
任　　期		令和４年７月８日　～　令和６年７月７日	

「参　照」

今治市執行機関の附属機関設置条例（抜すい）

（構成）

第３条　附属機関は、それぞれ別表に掲げる定限以内の数の委員をもって組織する。

第４条　附属機関の委員は、当該機関の属する執行機関が、それぞれの定めるところにより、当該機関の担任する事項に関し、学識経験を有する者その他最も適当と認められる関係者のうちから選任する。

今治市図書館運営審議会規則（抜すい）

（委員の構成）

第3条　審議会の委員の定数は、15人以内をもって組織し、その委員は、次に掲げる者のうちから教育委員会が委嘱し、又は任命する。

(1)　学校教育及び社会教育の関係者

(2)　家庭教育の向上に資する活動を行う者

(3)　学識経験のある者

2　特定の地位又は職により委嘱又は任命された委員の任期は、当該地位又は職にある期間とする。

別表（第２条、第３条、第５条関係）

附属機関の属する執行機関	附属機関	担任する事項	構成の数の定限	任期
市長	今治市総合計画審議会	総合計画に関する重要事項についての調査、審議及び市長に対する意見の答申に関する事項	２０人	
	今治市国土利用計画審議会	国土利用計画(今治市計画)に関する重要事項についての調査、審議及び市長に対する意見の答申に関する事項	２０人	２年
	今治市住居表示審議会	住居表示についての調査、審議及び市長に対する意見の答申に関する事項	１５人	
	今治市行政改革推進審議会	行政改革の推進についての調査、審議及び市長に対する意見の答申に関する事項	１２人	２年
	今治市健康づくり施策推進審議会	健康づくりに関する施策の総合的かつ計画的な推進についての調査、審議及び市長に対する意見の答申に関する事項	１５人	２年
	今治市老人ホーム入所判定委員会	老人ホームの入所措置に関する事項についての要否判定の審議及び市長に対する意見の答申に関する事項	７人	２年
	今治市地域包括支援センター運営協議会	地域包括支援センターの運営に関する事項についての調査、審議及び市長に対する意見の答申に関する事項	１５人	２年
	今治市地域密着型サービス拠点等整備事業者選定審議会	地域密着型サービス拠点等整備事業者の選定に関する事項についての調査、審議及び市長に対する意見の答申に関する事項	５人	２年
	今治市次世代育成支援対策地域協議会	次世代育成支援対策の推進についての調査、審議及び市長に対する意見の答申に関する事項	１８人	２年
	今治市廃棄物減量等推進審議会	一般廃棄物の減量化、資源化及び適正処理に関する計画等についての調査、審議及び市長に対する意見の答申に関する事項	２０人	２年
	今治環境パートナーシップ会議	環境基本計画に関する重要事項についての調査、審議及び市長に対する意見の答申に関する事項	１６人	２年
	今治市野間馬保存管理審議会	野間馬の保存育成及び活用に関する事項についての調査、審議及び市長に対する意見の答申に関する事項	１０人	２年
	今治市景観まちづくり会議	市の良好な景観形成に関する事項についての調査、審議及び市長に対する意見の答申に関する事項	２０人	２年

	今治市水道施設整備事業評価審議会	水道施設整備事業の事業評価についての調査、審議及び市長に対する意見の答申に関する事項	５人	
	今治市ごみ処理施設整備検討審議会	ごみ処理施設整備に関する専門的な事項等についての調査、審議及び市長に対する意見の答申に関する事項	１０人	
	今治市中心市街地再生基本計画策定審議会	中心市街地再生基本計画に関する重要事項についての調査、審議及び市長に対する意見の答申に関する事項	１５人	
教育委員会	今治市学校給食運営審議会	学校給食に関する事項についての調査、審議及び意見の答申に関する事項	２０人	２年
	今治市通学区域調整審議会	市立小学校及び中学校の通学区域の調整に関する事項についての調査、審議及び意見の答申に関する事項	２０人	２年
	今治市立花カルチャーセンター運営審議会	カルチャーセンターの各種事業の企画、実施についての調査、審議及び意見の答申に関する事項	１２人	２年
	今治市美須賀コミュニティプラザ運営審議会	美須賀コミュニティプラザの各種事業の企画、実施についての調査、審議及び意見の答申に関する事項	１２人	２年
	今治市開発総合センター運営審議会	開発総合センターの各種事業の企画、実施についての調査、審議及び意見の答申に関する事項	１２人	２年
	今治市図書館運営審議会	今治市立図書館の運営に関する事項についての調査、審議及び意見の答申に関する事項	１５人	２年

資料６

第９回教育委員会議案第 34 号

今治市図書館指定管理者選定審議会委員の委嘱について

標記のことについて、今治市公の施設に係る指定管理者の指定の手続等に関する条例第 15 条の規定により別紙の者に委嘱する。

令和４年７月８日提出

今治市教育委員会
教育長　田坂　敏

「理　　由」
今治市立図書館指定管理者の選定のため

今治市図書館指定管理者選定審議会委員　候補者名簿

	氏　名	区　分	役　職　名
候補者	吉良　佳世	学識経験者	医療法人勤有会きら病院　副院長
	相原　正樹	学識経験者	今治市行政改革推進審議会　委員
	濱田　栄子	学識経験者	今治明徳短期大学 幼児教育学科　講師
	森　聖二	市　職　員	総合政策部長
	秋山　直人	市　職　員	教育委員会事務局副教育長
任　期		令和４年７月８日から指定管理者が指定されるまで又は指定管理者を選定しないことの決定をするまで	

「参　照」

今治市公の施設に係る指定管理者の指定の手続等に関する条例（抜すい）

（審議会）

第15条　市長等の諮問に応じ、指定管理者の選定について審議するため、別表のとおり指定管理者選定審議会（以下「審議会」という。）を置く。

2　審議会の委員の定数は、審議会ごとに5人以内とし、次に掲げる者のうちから市長等が委嘱又は任命する。

（1）　学識経験者

（2）　市職員

3　審議会の委員の任期は、指定管理者が指定されるまで又は指定管理者を選定しないことの決定をするまでの間とする。

別表（第15条関係）

審議会の名称	指定施設の名称
今治市図書館指定管理者選定審議会	今治市立中央図書館、今治市立波方図書館、今治市立大西図書館及び今治市立大三島図書館