教育情報セキュリティポリシーに関するガイドライン

平成２９年１０月１８日　策　定

文 部 科 学 省

目　次

【参考】
教育情報セキュリティ対策基準の例文
権限・責任等一覧表

第 1 章 総則

1.1. 本ガイドラインの目的

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をいう。

地方公共団体における情報セキュリティは、各地方公共団体が保有する情報資産に自ら責任を持って確保すべきものであり、情報セキュリティポリシーも各地方公共団体が組織の実態に応じて自主的に策定するものである。

地方公共団体における情報セキュリティポリシーについては、その策定や見直しを行う際の参考として、総務省において、「地方公共団体における情報セキュリティポリシーに関するガイドライン（平成 27 年 3 月版)」（以下「自治体ガイドライン」と言う。）が既に整備されている。

一方で、地方公共団体が設置する学校（本ガイドラインにおいて「学校」とは、学校教育法第１条に定める小学校、中学校、義務教育学校、高等学校、中等教育学校及び特別支援学校を言う。）においては、コンピュータを活用した学習活動の実施など、教職員はもとより、児童生徒が日常的に情報システムにアクセスする機会がある。このことは、地方公共団体の他の行政事務とは異なる特徴と言える。

このため、本ガイドラインは、地方公共団体が設置する学校を対象とする情報セキュリティポリシー（以下、「教育情報セキュリティポリシー」と言う。）の策定や見直しを行う際の参考として、教育情報セキュリティポリシーの考え方及び内容について解説したものである。

本ガイドラインにおいて記載している例文は、参考としやすくするため公立小学校及び中学校等の設置者である市を想定して記述している。なお、本ガイドラインは、読者として教育情報セキュリティポリシーの策定の担当者、セキュリティ上の職責を担う者などを想定して記述している。

なお、本ガイドラインは、学校において安心して情報通信技術（以下、「ＩＣＴ」という。）を活用できる環境を維持する観点から、地方公共団体における情報セキュリティ対策の同行、技術的な進展等も踏まえつつ、随時見直しを行う予定である。

1.2. 本ガイドライン制定の背景

文部科学省においては、第２期教育振興基本計画（平成25年６月14日閣議決定）等に基づき、学校における計画的なＩＣＴ環境整備の促進を図っている。

学校には、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機微な情報が保管されている。

教職員の校務事務については、効率化の観点から、「統合型校務支援システム」（教務系（成績処理、出欠管理、時数等）・保健系（健康診断表、保健室管理等）、指導要録等の学籍関係、学校事務系などを統合した機能を有しているシステムのことを言う。）の普及が進んできている。

また、学校におけるＩＣＴは、教職員だけでなく、児童生徒により、授業等において積極的に活用することが想定されている。

平成32年度からは、新学習指導要領が小学校から順次実施される予定となっているが、新学習指導要領においては、「情報活用能力の育成を図るため、各学校において、コンピュータや情報通信ネットワークなどの情報手段を活用するために必要な環境を整え、これらを適切に活用した学習活動の充実を図ること」と記載されるなど、各学校における積極的なＩＣＴの活用が求められている。さらに、小学校においては、「プログラミング的思考」などを育むプログラミング教育の必修化も予定されている。

また、教科書制度においても、新学習指導要領の実施に合わせて、紙の教科書に代えて使用することにより、教科書使用義務の一部の履行を認める特別の教材として、デジタル教科書を位置付ける方向で検討が進められている。

このように、学校の教育活動におけるＩＣＴの積極的な活用は、今後、ますます求められているところである。その際、昨今、学校が保有する機微情報に対する不正アクセス事案も発生している中で、児童生徒や外部の者等による不正アクセスの防止等の十分な情報セキュリティ対策を講じることは、教員及び児童生徒が、安心して学校においてＩＣＴを活用できるようにするために不可欠な条件であることは言うまでもない。

しかしながら、現在、学校を対象とした情報セキュリティポリシーを策定している教育委員会は、策定中も含めて64.1％（文部科学省委託調査「教育情報セキュリティポリシー策定及び対策実施状況に関するWEBアンケート調査」（平成29年2月1日NTTラーニングシステムズ株式会社））であり、学校における情報セキュリティ対策の考え方が確立しているとは言い難い状況となっている。

このため、今後の学校における情報セキュリティ対策の考え方を整理することを目的として、平成28年9月に、文部科学省において「教育情報セキュリティ対策推進チーム」を設置し、計５回の審議を経て、今般、「教育情報セキュリティポリシーに関するガイドライン」を取りまとめたものである。

なお、本ガイドラインは、地方公共団体が設置する学校を対象としたものであり、教育

情報セキュリティポリシーは地方公共団体が策定・運用することを想定していることから、検討に当たっては、自治体ガイドラインの考え方を踏まえたものとしている。

1.3. 地方公共団体における教育情報セキュリティの考え方

教育情報セキュリティポリシーガイドラインは、以下の①～⑥の基本的考え方のもと、第2章に具体的な対策基準をまとめている。

各教育委員会・学校においては、対策基準を参考にしつつ、学校における情報セキュリティポリシーの策定と運用ルールの見直しを行うことが期待される。

なお、情報セキュリティの確保に絶対安全ということはないことから、情報セキュリティに関する障害・事故及びシステム上の欠陥（以下、「情報セキュリティインシデント」という。）の未然防止のみならず、情報セキュリティインシデントが発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要である。

また、情報セキュリティ対策は、個人情報の漏えいリスクを軽減する観点からも重要であり、地方公共団体が自ら進んで情報セキュリティに関する意識・リテラシーを高め、主体的にその対策に取り組むことが求められる。加えて、情報セキュリティ対策は、自然災害時等における危機管理対策との連携も重要である。

以上のような考え方を踏まえ、情報セキュリティを対策する部署とこれらを担当する部署は、相互に連携をとって、それぞれの対策に取り組むことが求められる。

①組織体制を確立すること

学校における情報セキュリティ対策の考え方を確立させるためには、情報セキュリティの責任体制を明確にしておく必要がある。

教育情報セキュリティポリシーの実行管理の最終責任を有する最高情報セキュリティ責任者（CISO:Chief information Security Officer）については、本ガイドラインにおいては、情報セキュリティインシデントが発生した際の危機管理等の観点から、自治体ガイドラインと同一の者（副市長等）が担うこととした。教育委員会・学校においては、首長部局の情報政策担当部局と密に連携し、情報セキュリティ対策を講ずる必要がある。

また、学校は、教員を中心に構成され、教員は、児童の教育を司ることがその職務の中心であることから、学校における情報システムの開発、設定の変更、運用、見直し等の権限や情報セキュリティの遵守に関する教育、訓練等については、基本的に教育委員会において責任を持つことを明確にした。

②児童生徒による機微情報へのアクセスリスクへの対応を行うこと

学校においては、コンピュータを活用した学習活動の実施など、児童生徒が日常的に情

報システムにアクセスする機会があることに、その特徴がある。

実際、児童生徒による、学校が保有する機微情報に対する不正アクセス事案も発生している。このため、本来は児童生徒が見ることを想定していない機微情報等にアクセスするリスクを回避することが必要となる。

③インターネット経由による標的型攻撃等のリスクへの対応を行うこと

学校においては、学校ホームページや教職員によるメールの活用、さらには、学習活動におけるインターネットの活用等が行われていることから、地方公共団体のいわゆる行政部局と同様に、標的型攻撃等のインターネット上の脅威に対する対策を講ずることが必要となる。

④教育現場の実態を踏まえた情報セキュリティ対策を確立させること

成績処理等を自宅で行うことを目的として、教員が、個人情報を自宅に持ち帰る場合がある。一方で、個人情報が記載された電子データを紛失することにより懲戒処分等を受けた教員は平成27年度で62名（文部科学省「平成27年度公立学校教職員の人事行政状況調査」）も存在することを踏まえ、教員が個人情報を外部に持ち出す際のルールを明確にした。

また、児童生徒が活用する情報システムにおいては、児童生徒の扱う情報そのものが個人情報となる場合があり、これら情報を完全に匿名化することは困難であることから、児童生徒が活用する情報システムであっても機微な情報を保持する場合、暗号化等の対策を講ずることとした。

⑤教職員の情報セキュリティに関する意識の醸成を図ること

学校は、成績や生徒指導関連等の機微な情報を取り扱うことから、研修等を通じて、教職員の情報セキュリティに関する意識の醸成を図ることが必要である。

⑥教職員の業務負担軽減及びICTを活用した多様な学習の実現を図ること

情報セキュリティ対策を講じることによって校務事務等の安全性が高まるとともに、教員の業務負担軽減へとつながる運用となるよう配慮する必要がある。

また、学校は、児童生徒が学習する場であることに鑑み、授業においてICTを活用した様々な学習活動に支障が生じることのないよう、配慮する必要がある。

（参考）技術的対策を中心とした教育情報システム全体の強靭性向上について

「教育情報セキュリティ対策推進チーム」では、昨今の標的型攻撃等に対応する観点から、総務省「新たな自治体情報セキュリティ対策の抜本的強化に向けて」（平成 27 年 11 月 24 日）及び「教育情報セキュリティのための緊急提言」（「2020 年代に向けた教育の情報化に関する懇談会」第 5 回（平成 28 年 7 月 28 日）取りまとめ）の考え方を踏まえ、技術的対策を中心とした教育情報システム全体の強靭性向上のための大きな方向性を以下のように整理した。

なお、以下に記されている対策は、主な対策を記載したものであり、全ての対策を網羅したものではないため、具体的な対策の詳細については、第２章を参照されたい。

（１）学校が保有する機微情報に対するセキュリティ強化

（主な対策）

①児童生徒によるアクセスリスクからの回避

・校務系システムと学習系システム間の通信経路の論理的又は物理的な分離の徹底

②インターネットリスクからの分断

・校務系システムとウェブ閲覧やインターネットメールなどのシステムとの通信経路の論理的又は物理的な分離の徹底

③学習系システムへの機微情報保管の禁止

（２）学校単位で機微情報を管理するリスクの低減

（主な対策）

①機微情報を保管する校務系サーバの教育委員会による一元管理

・学習系サーバも、ネットワークの負荷・授業における安定的な稼動を前提として、将来的には教育委員会による一元管理が望ましい。

②学校のインターネット接続環境のセンター集約によるセキュリティ対策強化

③校務外部接続系サーバ及び学習系サーバ（機微な個人情報を保管する場合に限る）の暗号化等による安全管理措置の実施

（３）教職員による人的な機微情報漏えいリスクの最小化

（主な対策）

①管理されたＵＳＢ等の電磁的記録媒体以外の使用禁止

②電磁的記録媒体の暗号化の徹底

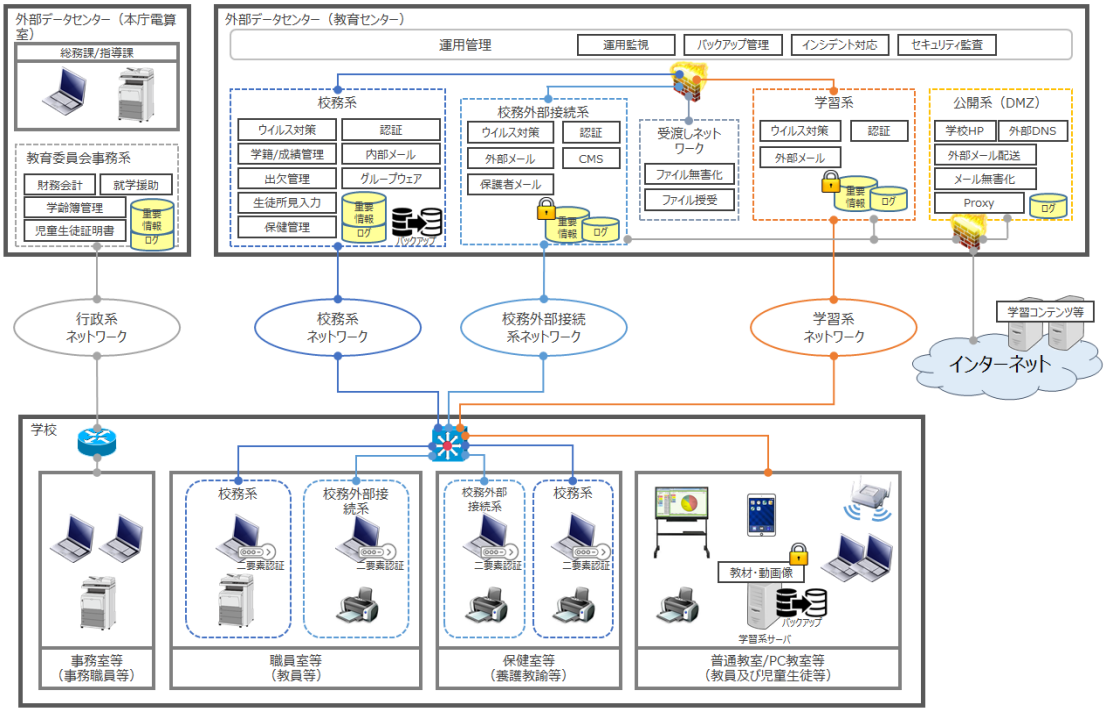
※今後は、学習活動においてインターネットを介したアプリケーションを積極的に活用したり、校務系システムと学習系システムを連携させることを前提として学校が保有する情報を学習指導や生徒指導等の質の向上、学級・学校運営の改善に活用したりす

ることなどが期待されている。

このため、以下の２点については、文部科学省において平成 29～31 年度で実施予定の「次世代学校支援モデル構築事業」において実証し、ガイドラインに反映していく予定である。

①インターネットを介した ASP サービスの利用における留意点

②データを活用した学校・学級の運営改善のための、校務系システムと学習系システムのセキュアな連携の在り方



図表1　学校における情報セキュリティ対策例

1.4.教育情報セキュリティポリシーの構成と学校を対象とした「対策基準」の必要性

地方公共団体において、情報セキュリティ対策を徹底するには、対策を組織的に統一して推進することが必要であり、そのためには組織として意思統一し、明文化された文書として、情報セキュリティポリシーを定めなければならない。

情報セキュリティポリシーの体系は、図表 2 に示す階層構造となっている。

各地方公共団体の情報セキュリティ対策における基本的な考え方を定めるものが、「基本方針」である。この基本方針に基づき、全ての情報システムに共通の情報セキュリティ対策の基準を定めるのが「対策基準」である。この「基本方針」と「対策基準」を総称して「情報セキュリティポリシー」という。さらに「対策基準」を、具体的なシステムや手順、手続に展開して個別の実施事項を定めるものが「実施手順」である。

このように、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、本来は地方公共団体全てを包括するポリシーでなければならない。

しかしながら、学校は、地方公務員法及び教育公務員特例法に定める「服務」に服さない児童生徒が過ごす場所であり、かつ、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、当該児童生徒も想定した情報セキュリティ対策を講ずる必要があり、行政事務を対象とする「対策基準」とは異なる部分がある。

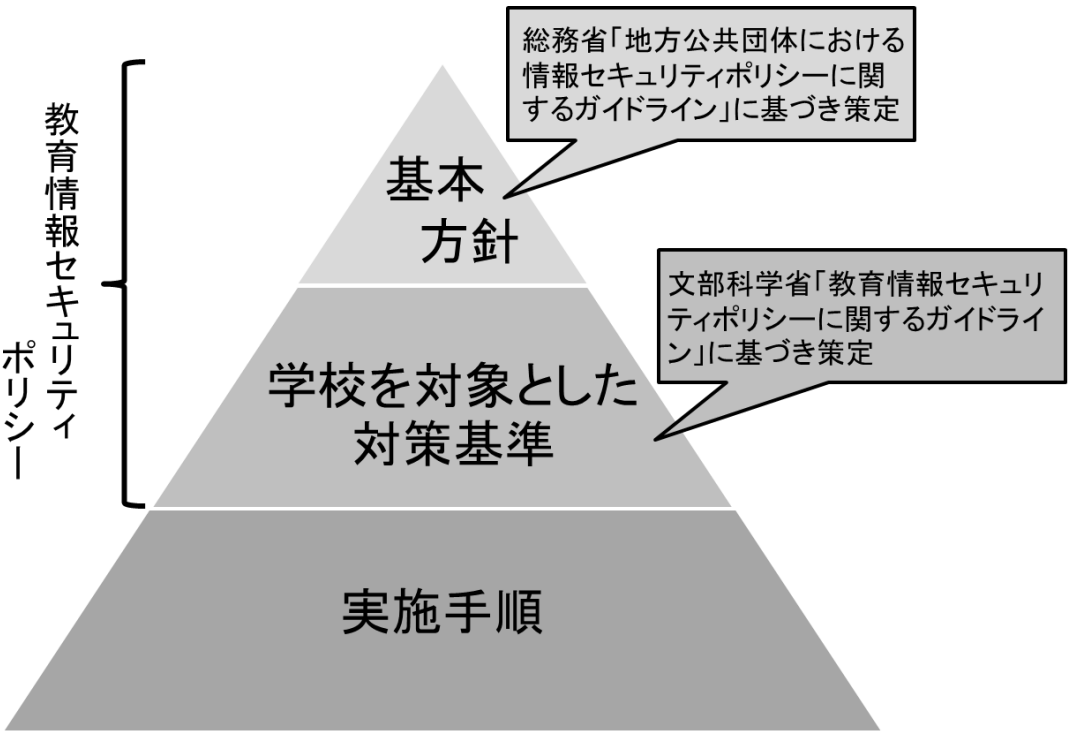
このため、学校の設置者である地方公共団体は、「基本方針」については、地方公共団体が策定したものに従いつつ、「対策基準」については、学校を想定したものを策定することが望ましい。地方公共団体及び教育委員会の長をはじめ、全ての職員、教員、事務職員及び外部委託事業者は、学校関係の業務の遂行に当たっては、当該「対策基準」を遵守する義務を負う。

なお、本ガイドラインの対象とする範囲は「情報セキュリティポリシー」を構成する「対策基準」であり、「基本方針」及び「実施手順」は含まれない。

※リスク分析を含む情報セキュリティ対策の実施サイクルや、「基本方針」については、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（http://www.soumu.go.jp/main_content/000348656.pdf）の第1章及び第2章を参照されたい。

※地方公共団体において扱う情報資産の重要性や取り巻く脅威の大きさによって、必要とされる対策は一様でないことから、本ガイドラインでは、特段の理由がない限り対策することが望まれる事項に加え、各地方公共団体において、その事項の必要性の有無を検討し、必要と認められる時に選択して実施することが望ましいと考えられる対策事項については、「推奨事項」として示している。

各地方公共団体においては、組織の実態に合わせ、必要に応じて「推奨事項」も含めて、教育情報セキュリティポリシーを策定することが期待される。



図表2 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 情報セキュリティ対策基準

2.1. 対象範囲及び用語説明

【趣旨】

情報セキュリティポリシーを適用する行政機関等の範囲、情報資産の範囲及び用語を明確にする。

【例文】

（1）行政機関等の範囲

本対策基準が適用される行政機関等は、内部部局、教育委員会及び学校（小学校、中学校、義務教育学校、高等学校、中等教育学校、特別支援学校を言う。以下同じ。）とする。

（2）情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

①教育ネットワーク、教育情報システム、これらに関する設備、電磁的記録媒体

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

③教育情報システムの仕様書及びネットワーク図等のシステム関連文書

（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	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	校務外部接続系情報にアクセス可能な端末
学習者用端末	学習系情報にアクセス可能な端末で、児童生徒が利用する端末
指導者用端末	学習系情報にアクセス可能な端末で、教員のみが利用可能な端末
校務系システム	校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム
校務外部接続系システム	校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ（CMS)及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム
学習系システム	学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム
教育情報システム	校務系システム、校務外部接続系システム及び学習系システムを合わせた総称
校務系サーバ	校務系情報を取り扱うサーバ
校務外部接続系サーバ	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

(解説)

（1）行政機関等の範囲

地方公共団体が設置する学校の管理運営に係る事務を担う執行機関及び学校を基本に、情報セキュリティポリシーを適用させる範囲を決定する。

（2）情報資産の範囲

情報セキュリティポリシーの対象とする情報資産の範囲と情報資産の例は図表3のとおりであるが、文書で対象としているのは、教育ネットワーク、教育情報システムで取り扱うデータを印刷した文書及びシステム関連文書である。

これら以外の文書は、情報資産に含めていないが、文書管理規程等により適切に管理しなければならない。

文書一般を情報資産に含めなかったのは、従来電子データ等の管理と文書の管理が、一般に異なる部署、制度によって行われてきた経緯、実態を踏まえたものである。しかしながら、情報資産の重要性自体は、電子データ等と文書の場合で異なるものでないことから、情報セキュリティ対策が進んだ段階では、全ての文書を情報セキュリティポリシーの対象範囲に含めることが望ましい。

図表３　情報資産の種類と例

情報資産の種類	情報資産の例
教育ネットワーク	情報資産を扱う通信回線、ルータ等の通信機器
教育情報システム	情報資産を扱うサーバ、パソコン、モバイル端末、汎用機、オペレーティングシステム、ソフトウェア等
これらに関する施設・設備	情報資産を扱うコンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル
電磁的記録媒体	情報資産を扱うサーバ装置、端末、デジタルカメラ、デジタルビデオカメラ、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USBメモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部電磁的記録媒体
教育ネットワーク及び教育情報システムで取り扱う情報	教育ネットワーク、教育情報システムで取り扱うデータ（これらを印刷した文書を含む。）
教育情報システム関連文書	教育情報システム関連のシステム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

2.2. 組織体制

【趣旨】

組織として、情報セキュリティ対策を確実に実施するに当たっては、情報セキュリティ対策に取り組む十分な組織体制を整備し、一元的に情報セキュリティ対策を実施する必要がある。このことから、情報セキュリティ対策のための組織体制、権限及び責任を規定する。

【例文】

（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。

② CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。【推奨事項】

（2）統括教育情報セキュリティ責任者

① 教育長、副教育長又は教育委員会に所属するCIO補佐官等を、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。

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。

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、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISOの指示に従い、CISOが不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

⑥ 統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。

⑦ 統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 教育委員会事務局の情報セキュリティ担当部局（情報システム課等）の課室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統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、見直し等を行う際の情報セキュリティに関する統括的な権限及び責任を有する。

④ 教育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、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には、教育情報セキュリティ責任者、統括教育情報セキュリティ責任者及び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 教育委員会の情報システム担当課の課室長を、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 教育委員会の情報システム担当課の課室職員を、教育情報システムに関する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）情報セキュリティ委員会

① 本市の情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会において、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。

② 情報セキュリティ委員会は、毎年度、本市における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。【推奨事項】

（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。

（9）情報セキュリティに関する統一的な窓口の設置

① CISO は、情報セキュリティインシデントの統一的な窓口の機能を有する組織を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。

② CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供する。

③ 情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

④ 情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。

（解説）

各地方公共団体においては、図表4 のような組織体制を構築して、情報セキュリティ対策に取り組むことを想定している。

（注１）情報セキュリティ対策を確実に実施するに当たっては、組織体制を整備するとともに、必要な予算、人員などの資源を確保することが重要である。

（注２）情報セキュリティポリシーにおいて、誰がどのような権限及び責任を持っているのかを容易に把握できるよう一覧表で整理しておくと便利である。

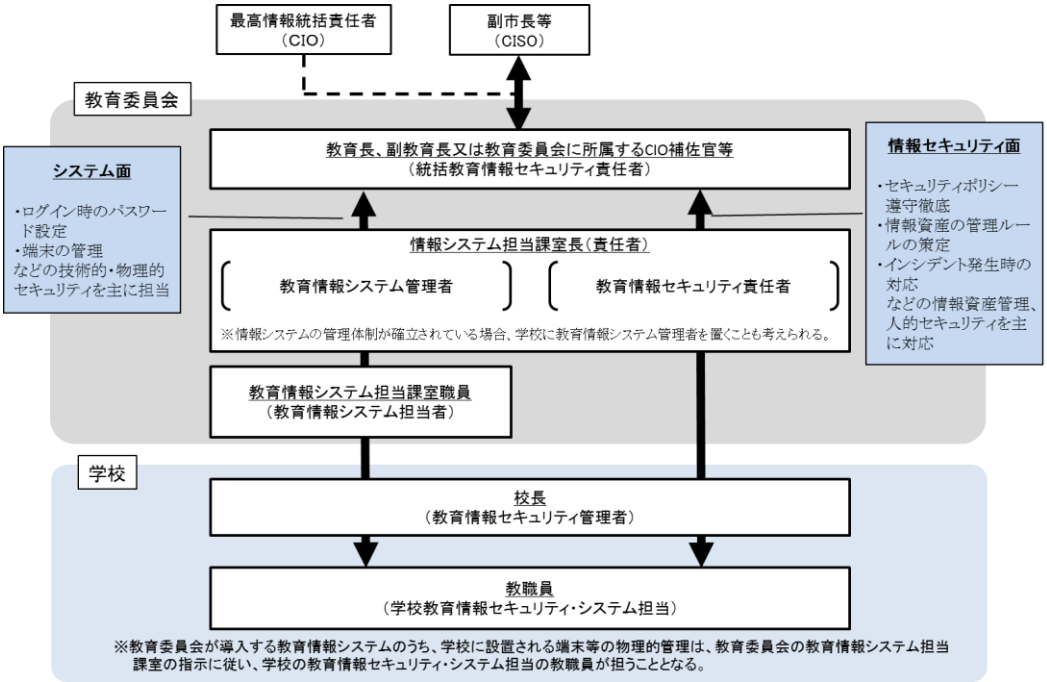
（１）最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）

CISO は、地方公共団体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や情報セキュリティに関する権限及び責任を有する。

例文では、CISO が、情報資産の管理や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こととしているが、小規模の地方公共団体などにおいては、情報通信技術の活用による住民の利便性の向上及び行政運営改善等に関するものを統括する最高情報統括責任者（CIO: Chief Information Officer、以下「CIO」という。）との兼務や情報政策担当部長との兼務など、柔軟な対応が必要となる。

また、適切に情報セキュリティ対策を講じていくに当たっては専門知識を必要とするため、内部の職員のみならず、情報セキュリティに関する外部の専門家を最高情報セキュリティアドバイザー（CISO の補佐）として置くことが望ましい。

（注３）CISO 及びCIO は、副知事、副市長等、庁内を全般的に把握でき、部局間の調整や取りまとめを行うことができる上位の役職者を充てることが望ましい。



図表４　情報セキュリティ推進の組織体制例

（２）統括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は、地方公共団体の教育ネットワークや教育情報システムの開発、設定の変更、運用、見直し等の権限及び責任を有するほか、情報セキュリ

ティ対策に関する権限及び責任を有する。

CISO が不在の場合には、統括教育情報セキュリティ責任者がその権限をCISO に代わって行使できるよう、権限の委譲についても規定しておく。また、情報セキュリティインシデント発生時等の緊急時には、統括教育情報セキュリティ責任者が中心となり被害の拡大防止、事態の回復のための対策実施、再発防止策の検討を行う必要がある。

（注４）統括教育情報セキュリティ責任者には、具体的には教育長、副教育長又は教育委員会に所属するCIO補佐官等が考えられる。

（３）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は、教育情報セキュリティ対策に関する権限及び責任を有する。

（注５）教育情報セキュリティ責任者には、教育委員会事務局の情報セキュリティ担当部局（情報システム課等）の課室長を充てることが想定される。

（４）教育情報セキュリティ管理者

教育情報セキュリティ管理者は、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。

教育情報セキュリティ管理者は、システムの利用現場の担当者であり、学校において、情報資産に対するセキュリティ侵害又はセキュリティ侵害のおそれがある状況に直面する可能性が高い。そのため、このような場合を想定し、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 に対する報告義務を定める。

（注６）教育情報セキュリティ管理者には、校長を充てることが想定される。

（５）教育情報システム管理者

教育情報システム管理者は、個々の教育情報システムに関する権限及び責任を有する。教育情報システム管理者は、個々の教育情報システムの開発、設定の変更、運用、見直し等の権限及び責任を有するほか、所管する教育情報システムに対する情報セキュリティ対策に関する権限及び責任を負う。

個々の教育情報システムに関する情報セキュリティ実施手順の維持・管理は、教育情報システム管理者が行う。

（注７）教育情報システム管理者には、教育委員会の情報システム担当課の課室長等を充てることが想定される。

（注８）教育情報システムの導入・管理・運用は、原則として教育委員会が責任を持って担う。なお、学校が独自に教育情報システムの導入・管理・運用を行う場合は、当該教育情報システムの管理体制が確立している場合に限る。

（６）教育情報システム担当者

教育情報システム担当者とは、教育情報システム管理者の指示等に従う職員等で、開発、設定の変更、運用、見直し等の作業を行う。

（注９）　実際の運用にあたっては、教育委員会の情報システム担当課の指示に従い、学校における教育情報システムの導入・管理・運用等を補助する者が不可欠となる。このため、校長は、校務分掌として、「学校教育情報セキュリティ・システム担当」を置くこととする。

（注１０）教育情報システムの導入・管理・運用等にあたり専門的な知識・技術を有する者が必要になる点や、情報システム担当課の課室職員の業務負担軽減を目的として、外部委託先の運用員やICT支援員等の外部人材に業務を委託する方法もある。

（７）情報セキュリティ委員会

情報セキュリティに関する重要事項を決定する機関として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は、リスク情報の共有、情報セキュリティポリシーの決定等、情報セキュリティに関する重要な事項を決定する。

（注１１）情報セキュリティ委員会の構成員は、CISO、CIO、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等が想定され、定期的及び必要に応じてCISO が構成員を招集し、開催する。

（注１２）小規模の地方公共団体等においては、情報化推進委員会が情報セキュリティ委員会を兼ねるなど、地方公共団体の実情に応じた柔軟な運営が必要である。

（注１３）情報セキュリティに関する意思決定機関として情報セキュリティ委員会以外に庁議や幹部会議等を位置付けることも可能である。

（８）兼務の禁止

情報セキュリティ対策に係る組織において、申請者と承認者が同一であることや監査人と被監査部門の者が同一である場合は、承認や監査の客観性が担保されないため、兼務の禁止を定める。

「やむを得ない場合」とは、例えば、統括教育情報セキュリティ責任者のみに認められた承認について、統括教育情報セキュリティ責任者が申請する場合や小規模団体で代替する者がいない場合などをいう。

（９）情報セキュリティに関する統一的な窓口（「庁内のCSIRT（Computer Security Incident Response Team）」 以下、「庁内のCSIRT」という。）の設置

情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、情報セキュリティインシデントのとりまとめ、CISO・CIO への報告、報道機関等への通知・公表、関係機関との情報共有など、情報セキュリティインシデントに関するコミュニケーションの核となる体制を危機管理等の既存の枠組み等を活用するなどして構築する必要がある。

また、地方公共団体情報システム機構（自治体CEPTOAR）等の関係機関や他の地方公共団体の同様の窓口機能、外部の事業者等と連携して体制を強化することが求められる。

（注１４）一般的に情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生した情報セキュリティインシデントを正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制はCSIRT と呼ばれている。
CSIRT の持つ機能や在り方は組織によって様々であるが、まずは、地方公共団体においては情報セキュリティに関する統一的な窓口の機能を有する体制を整えることが重要である。

（注１５）学校で発生する情報セキュリティインシデントの重要度や影響範囲等を勘案するには、教育委員会の関与が不可欠であり、また、学校からの相談窓口を設け情報共有を行うことが効果的と考えられることから、首長部局のCSIRTと連携することを前提として、教育委員会に学校における情報セキュリティインシデントに関するコミュニケーションの核となる体制を構築していくことが望まれる。

2.3. 情報資産の分類と管理方法

【趣旨】

情報資産を保護するに当たっては、まず情報資産を分類し、分類に応じた管理体制を定める必要がある。情報資産の管理体制が不十分な場合、情報の漏えい、紛失等の被害が生じるおそれがある。そこで、機密性、完全性及び可用性に基づく情報資産の分類と分類に応じた取扱いを定めた上で、情報資産の管理責任を明確にし、情報資産のライフサイクルに応じて取るべき管理方法を規定する。

【例文】

（1）情報資産の分類

本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、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、業務の遂行に支障ある情報
完全性 2A	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学校関係者の権利が侵害される又は学校事務及び教育活動の的確な遂行に軽微な支障を及ぼすおそれがある情報資産	情報が正確・完全な状態である必要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合、業務の遂行に軽微な支障ある情報
完全性 1	完全性 2A 又は完全性 2B の情報資産以外の情報資産	事故があった場合でも業務の遂行に支障がない情報

可用性による情報資産の分類

分類	分類基準	該当する情報のイメージ
可用性 2B	学校で取り扱う情報資産のうち、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

（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）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

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、適切な取扱いをしなければならない。

（ウ）情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

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、情報資産を適切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電磁的記録媒体を保管する場合は、書込禁止の措置を講じなければならない。

（ウ）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、利用頻度が低い電磁的記録媒体や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。【推奨事項】

（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、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

電子メールにより機密性2A以上の情報を外部送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

⑧情報資産の運搬

（ア）車両等により機密性2A以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、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）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）機密性2A以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

（イ）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、住民に公開する情報資産について、完全性を確保しなければならない。

⑩情報資産の廃棄

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

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

（ウ）情報資産の廃棄を行う者は、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。

（解説）

（１）情報資産の分類

情報資産について、機密性、完全性及び可用性を踏まえ、被害を受けた場合に想定される影響の大きさをもとに分類を行い、必要に応じて取扱制限を定める必要がある。

（注１）情報資産の分類は、機密性、完全性及び可用性に基づき、分類することが望ましいが、教職員の理解度等に応じ、以下のような重要性に基づき分類することもあり得る。

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。
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。
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。
Ⅳ 影響をほとんど及ぼさない。

なお、図表5に学校における情報資産の分類について例示するので、参考にされたい。

情報資産の分類					情報資産の例示		
重要性分類	定義	機密性	完全性	可用性	持ち出しの禁止	持ち出しの制限	持ち出しの制限無し
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。	3	2B	2B	・指導要録原本 ・教職員の人事情報 ・入学者選抜問題	・教育情報システム仕様書	
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。	2B	2B	2B	○学籍関係 ・出席簿 ・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 ・評定一覧表 ・進級・卒業認定資料 ・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 ○進路関係 ・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 ・入学者選抜に関する表簿（願書等） ○健康関係 ・健康診断に関する表簿 ・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、氏名、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 （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、氏名、生年月日、性別等の基本情報を含むもの） ○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 ・情報端末ログインID/PW	○成績関係 ・通知表 ・定期考査・テスト等の答案用紙 （児童・生徒が記入済のもの） ○指導関係 ・児童・生徒等の個人写真・集合写真 ・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） ○進路関係 ・調査書 ・推薦書 ・私立高校入試に係る事前相談資料 ・公立高校入学者選抜に係る成績一覧表 ○健康関係 ・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 ○その他 ・給食関係書類・寄宿関係資料 ○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 ・座席表 ・PTA会員名簿 ・職員緊急連絡網・職員住所録 ・委員会名簿 ○児童生徒の学習系情報* （学習後に回収したもの） ・児童生徒の学習記録 （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）	
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。	2A	2A	2A		○児童生徒の学習系情報（学習中） ・児童生徒の学習記録 （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） ○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	
Ⅳ	影響をほとんど及ぼさない。	1	1	1			○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 ・授業用教材 ・教材研究資料 ・生徒用配布プリント （校務分掌名等で出すもの）

※学習後に回収した学習系情報は、児童生徒がアクセスすることを前提とせず、評価根拠等で保存されるため、校務系情報と同等の重要性とする。

図表5　情報資産の例示

（２）情報資産の管理

①　管理責任

情報資産の管理は、その情報資産に係る実務に精通している者が行う必要があり、本ガイドラインでは、情報資産の管理責任者を教育情報セキュリティ管理者（校長等）と想定している。

（注２）管理に当たっては、重要な情報資産について台帳を整備することが望ましい。これにより、情報資産の所在、情報資産の分類、管理責任が明確になる。また、情報資産の管理について、管理不在の状態や二重管理にならないように留意することが重要である。

②　情報資産の分類の表示

（注３）情報システムについて、当該情報システムに記録される情報の分類を規定等により明記し、当該情報システムを利用する全ての者に周知する方法もある。

（注４）機密性2A以上、完全性2A以上、可用性2A以上の情報資産についてのみ表示を行い、表示のない情報資産は、機密性1、完全性1、可用性1とする運用もある。

③　情報の作成～⑩情報資産の廃棄

情報資産の取扱いについて遵守すべき事項は、情報のライフサイクルに着目し定める。情報のライフサイクルには、作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等の局面がある。これらの局面ごとに、情報資産の分類に応じ取扱制限を定める。図表６に情報資産の取扱例を示す。

また、情報のライフサイクルの局面、情報資産の分類及び分類に応じた取扱制限については、定期的又は必要に応じて見直すことが重要である。

なお、教育委員会外の第三者が提供するアプリケーション・コンテンツ（例えば、学校が独自に導入するネットワーク型の視聴覚コンテンツ）に関する情報を告知する場合は、アプリケーション・コンテンツのリンク先のURL やドメイン名の有効性や管理する組織名等の必要情報を明記するなどの対策を講じることが必要である。

（注５）情報の提供、行政手続、意見募集等の行政サービスのためにアプリケーション・コンテンツを提供する場合は、利用者端末の情報セキュリティ水準の低下を招いてしまうことを避けるため、アプリケーション・コンテンツの作成に係る規定の整備やセキュリティ要件の策定等の情報セキュリティ対策を講じておく必要がある。

（注６）情報資産の提供とは、学校外の特定集団（保護者、OB等）に情報を提供すること（保護者メールを使って、学校から関係する保護者に対して、学校から

のお知らせを送付する等）、情報資産の公表とは、学校外の不特定多数の人に情報を提供することを指す。

情報資産の分類					情報資産の管理（取扱い）									
					複製・配布	外部への持ち出し*		端末制限	情報の外部送信**	情報資産の運搬***	外部での情報処理	使用する電磁記録媒体	情報資産の保管	情報資産の廃棄
重要性分類	定義	機密性	完全性	可用性		禁止	制限							
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。	3	2B	2B	必要以上の複製及び配布禁止	児童生徒の転校等に伴う外部への情報移動の特別な理由を除いて禁止	真にやむを得ない場合に限り情報セキュリティ管理者の判断で持ち出しを可	支給以外の端末での作業の原則禁止	暗号化、パスワード設定を行う	鍵付きケースへの格納	禁止	施錠可能な場所への保管	・耐火、耐熱、耐水、耐湿を講じた施錠可能な場所に保管 ・情報資産を格納するサーバのバックアップ ・6か月以上のログ保管 ・サーバの冗長化（推奨事項） ・インターネット接続されるネットワークにサーバーを置く場合は、情報資産にファイル暗号化を実施 ・保管場所への必要以上の電磁記録媒体の持ち込み禁止	電子記録媒体の初期化、復元できないようにして廃棄
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。	2B	2B	2B	同上	同上	同上		同上	同上	安全管理措置の規定が必要	同上	同上	同上
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。	2A	2A	2A	同上		情報セキュリティ管理者の包括的承認で可		同上	同上	同上	同上	・耐火、耐熱、耐水、耐湿を講じた施錠可能な場所に保管 ・情報資産を格納するサーバのバックアップ（推奨事項） ・一定期間以上のログ保管 ・サーバーハードディスクの冗長化（推奨事項） ・保管場所への必要以上の電磁記録媒体の持ち込み禁止	同上
Ⅳ	影響をほとんど及ぼさない。	1	1	1										

＊： 情報資産の持ち出しとは、学校外に情報資産を持ち出すことを示す。
＊＊：外部送信の外部とは、情報システムを構成するネットワーク、端末、サーバの閉じた領域の外側に、情報資産をオンラインで持ち出すことを示す。なお、外部送信の際には、パスワード等は十分信頼できる方法により相手方へ伝える必要がある。
＊＊＊：情報資産の運搬とは、ＵＳＢメモリやハードディスク等の電磁的記録媒体を介して情報資産を運搬する場合を示す。

図表6　情報資産の取扱例

2.4. 物理的セキュリティ

2.4.1. サーバ等の管理

【趣旨】

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。

【例文】

（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切に固定する等、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校務系情報を格納しているサーバを冗長化し、同一データを保持しなければならない。また、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。【推奨事項】

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。【推奨事項】

（3）機器の電源

① 教育情報システム管理者は、統括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、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

② 教育情報システム管理者は、統括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 統括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 統括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 統括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切に管理しなければならない。

④ 統括教育情報セキュリティ責任者、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、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

統括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。

（解説）

（１）機器の取付け

情報システムで利用する機器は、温度、湿度等に敏感であることから、室内環境を整えることが必要である。

（注１）機器の排気熱が、特定の場所に滞留しないよう室内の空気を循環させることにも注意する必要がある。排気熱が機器周辺に滞留すると機器内部が高温に

なり、緊急停止する場合がある。

（２）サーバの冗長化

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することが有効である。

校務系システムは、成績処理等において、教員が毎日の業務において活用するものであり、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、校務系サーバ及び校務外部接続系サーバについては、冗長化を行うことが重要である。

一方で、学習系サーバについては、サーバ冗長化に係るコスト等も勘案し、ハードディスクの冗長化を図ることが適当である。

（注２）サーバの冗長化については、ハードウェアやソフトウェアが二重に必要となるほか、運用面でデータの同期化等が必要となり、これらの費用とサーバ等の緊急停止による損失の可能性を検討した上で、冗長化を行うか否かを判断する必要がある。

（３）機器の電源

何らかの要因で電力供給が途絶し、機器が緊急停止した場合には、情報システムの機能が損なわれるおそれがある。これを避けるために、機器が適正に停止するまでの間電力を供給する予備電源を設ける必要がある。

（注３）予備電源は、パソコン等に接続する小型のUPS（無停電電源装置）、蓄電池設備による給電を行うものや、自家発電機等様々な種類がある。また、これらの予備電源が緊急時に機能した場合に、現状どのくらい給電が行えるかを把握しておくべきである。例えば、1年前には、蓄電池設備により30分程度の電源供給ができていたものが、サーバの増設等により15分程度しか供給できなくなっている場合も考えられる。このために、施設管理部門から予備電源が給電可能な時間等について定期的に確認しておくことが必要である。

（注４）学習系サーバにおいても、情報資産が他にバックアップされていない場合には、予備電源を設けることが適当である。

（４）通信ケーブル等の配線

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。配線収納管等を利用し、通信ケーブル等の損傷を防ぐ必要がある。

（５）機器の定期保守及び修理

情報システムの安定的な運営のためには、定期的に保守を行うことが不可欠である。また、機器を修理に出す場合には、できる限り故障した部品を特定し、情報を消去できる場合は消去を行った上で引き渡すことにより、修理業者から情報が漏えいする可能性を低くしなければならない。内容を消去できないときは、守秘義務契約を締結するとともに、秘密保持に関する体制や運用などが適切であることを確認しなければならない。

（６）施設外又は学校外への機器の設置

施設外又は学校外にサーバ等の機器を設置する場合には、十分なセキュリティ対策がなされているか、定期的に確認する必要がある。

（注５）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。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。地方公共団体職員によるデータセンター内部への立入りがデータセンターのセキュリティポリシーに違反する等、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。

（７）機器の廃棄等

パソコンが不要になった場合やリース返却等を行う場合には、ハードディスクから情報を消去する必要がある。

（注６）情報を消去する場合、オペレーティングシステム（OS）の機能による初期化だけでは、再度復元される可能性がある。データ消去ソフトウェア若しくはデータ消去装置の利用又は物理的な破壊若しくは磁気的な破壊などの方法を用いて、全ての情報を復元が困難な状態にし、情報が漏えいする可能性を低減しなければならない。

2.4.2. 管理区域(情報システム室等)の管理

【趣旨】

情報システム室等は、重要な情報資産が大量に保管又は設置されており、特に厳格に管理する必要がある。情報システム室等が適切に管理されていない場合には、盗難損傷等により重大な被害が発生するおそれがあり、このことから、情報システム室等の備えるべき要件や入退室管理、機器等の搬入出に関する対策を規定する。ただし、対策によっては建物の改修を必要とするなど多額の費用を要するものもある。対策の実施に当たっては、費用対効果を考慮して行う必要がある。

【例文】

（教育委員会等のサーバ室にサーバを設置している場合）

（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、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

② 統括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、管理区域を地階又は1階に設けてはならない。また、外部からの侵入が容易にできないように無窓の外壁にしなければならない。【推奨事項】

③ 統括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、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

④ 統括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 統括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、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。【推奨事項】

⑥ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

（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。

② 地方公共団体職員等及び外部委託事業者が、管理区域に入室を許可する場合、これらの者に身分証明書等を携帯させ、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には、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、機密性2B以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、モバ

イル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（３）機器等の搬入出

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。

(学校にサーバを設置している場合)

（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、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワークの基幹機器及び重要な情報システムについて、サーバラックに固定した上で、サーバラックの施錠管理を行わなければならない。

③ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、サーバラックを、立ち入りを許可されていない不特定多数の者が出入りできる場所に設置してはならない。

④ 統括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、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

⑤ 統括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。

⑥ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

（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すること。

② 教育情報システム管理者は、サーバラックの施錠管理にあたり、管理簿の記載等による管理を行わなければならない。

③ 教職員は、児童生徒が管理区域に入室する場合、必要に応じて立ち入り区域を制限した上で、児童生徒に付き添うものとする。
④ 外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。
⑤ 教育情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立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教職員等が付き添うものとし、外見上教職員等と区別できる措置を講じなければならない。

（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、教職員を立ち会わせなければならない。

（解説）

（１）管理区域の構造等

情報システムの安定的な運営等のために、情報システム室や保管庫（磁気テープ等の保管庫）である管理区域の管理方法について定める。管理区域内には精密機器が多いことから、火災、水害、埃、振動、温度、湿度等の対策を施す必要がある。

また、学校に重要な情報システムを設置する場合においては、学校に専用のサーバ室が整備されていない場合が多いことが考えられることから、それぞれの学校の施設環境に応じた管理区域の管理を行う必要があるが、ネットワークの基幹機器及び重要な情報システムは、サーバラックに固定した上で施錠管理を実施するとともに、サーバラックを、立ち入りの許可がされていない不特定多数の者が出入りできない場所に設置する必要がある。

（注１）ICカード等で扉を自動開閉制御している場合、サーバ室内で発生した火災等により、自動制御の扉が故障し開閉ができず、室内にいる要員が閉じ込められてしまう危険性がある。このような事態を回避するために、手動で扉を開閉できるように、自動扉開閉制御を解除するスイッチの場所を平時から管理区域を管理している教育情報システム管理者が、入室権限のある地方公共団体職員及び教職員等に周知しておくことが必要である。鍵等による立入り防止措置についても、同様である。

（注２）管理区域に配置する消火薬剤は、発泡性のものを避けるべきである。また、スプリンクラーの水がかかる位置に情報システム機器等を設置してはならない。

（注３）情報システム室内では機器等をサーバラックに固定した上で、管理権限の異なる複数のシステムが同一の室内に設置されている場合は、他システムの管理者による不正操作を回避するため、サーバラックの施錠管理を行うことが必要である。

（２）管理区域の入退室管理等

管理区域は情報資産の分類に応じて厳格な管理が行われなければならない。リスク評価を行って許可する範囲を検討し、入室できる者は許可された者のみに制限する。また、外部からの訪問者が管理区域に入室する場合、地方公共団体職員および教職員等が付き添うとともに、訪問者であることを明示したネームプレートを着用させるなど外見上訪問者であることが分かるようにしておくべきである。また、情報漏えい等を回避するため、不要な電子計算機、モバイル端末、電磁的記録媒体等を管理区域に持ち込ませないことが重要である。

（注４）入退室の記録簿は、業者名、訪問者名等を記録する場合が多い。これらの記録簿に個人情報を記述している場合は、紛失等が生じないように保管することが必要である。

（注５）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が望ましい。

（３）機器等の搬入出

搬入出に伴い外部の者が管理区域に立入る場合は、同行、立会いを行い、相手の行動を監視する必要がある。

（注６）同行、立会いについては、原則として非常勤職員や臨時教職員ではなく、地方公共団体職員及び教職員が行う必要がある。

2.4.3. 通信回線及び通信回線装置の管理

【趣旨】

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。

【例文】

①統括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、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

②統括教育情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

③統括教育情報セキュリティ責任者は、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、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

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

⑤統括教育情報セキュリティ責任者は、可用性2B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。

(解説)

学校が使用する通信回線は、施設管理部門が敷設・管理を行っていることが多く、統括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、ネットワークに関する工事を行う場合、施設管理部門と連携して実施する必要がある。学校が使用する通信回線の敷設図、結線図等は、外部への漏えい等がないよう、厳重に管理しなければならない。

また、外部のネットワークへの不必要な接続は情報セキュリティ上の危険性が高まることから、その接続は必要最低限のものに限定するための措置を講ずることが必要である。

特にインターネット回線については、外部からの不正アクセスの侵入経路となり得る他、内部からの情報漏えい経路にもなり得るため、これらの情報セキュリティ上の危険性に対する監視と運用を効率的且つ確実に実施するためにも教育委員会でインターネット接続口を集約する必要がある。

通信回線として利用する回線は、当該システムで取り扱う情報資産の重要性に応じて、適切なセキュリティ機能を備えたものを選択することが必要であり、通信回線の性能低下や異常によるサービス停止を防ぐために、通信回線や通信回線装置を冗長構成にする又は回線の種類を変えて複数の回線を構築しておくことが望ましい。また、庁内から外部に敷設する通信回線の管路についても、例えば異なる通信事業者による複数の経路で構築しておくと、災害発生時の復旧にかかる時間が短縮されるなどの効

果が期待される。

（注１）図面管理を外部委託事業者に依頼する場合でも、当該外部委託事業者で紛失する場合に備えて、各地方公共団体で、控えを保管しておくことが必要である。

2.4.4. 教職員等の利用する端末や電磁的記録媒体等の管理

【趣旨】

教職員等が利用するパソコン、モバイル端末及び電磁的記録媒体等が適切に管理されていない場合は、不正利用、紛失、盗難、情報漏えい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、モバイル端末及び電磁的記録媒体等の盗難及び情報漏えい防止策、持ち出し・持ち込み等に関する対策を規定する。

【例文】

（校務用端末、校務外部接続用端末及び指導者用端末について）

① 教育情報システム管理者は、盗難防止のため、職員室等で利用する校務用端末及び校務外部接続用端末のワイヤーによる固定、教室等で使用する指導者用端末の保管庫による管理等、使用する目的に応じた適切な物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

② 教育情報システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

③ 教育情報システム管理者は、端末の電源起動時のパスワード（BIOSパスワード、ハードディスクパスワード等）を設定しなければならない。【推奨事項】

④ 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二要素認証を設定しなければならない。【推奨事項】

⑤ 教育情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。【推奨事項】

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。【推奨事項】

（学習者用端末について）

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。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。

（解説）

職員室及び教室等からパソコン、モバイル端末及び電磁的記録媒体等が盗難され、情報が漏えいする事例は多く、盗難を防止するための物理的措置が必要である。

また、各学校が保有しているパソコン、モバイル端末及び電磁的記録媒体等が盗難等に遭った場合でも、パスワード等の設定、暗号化により使用できないようにしておくことで、情報が不正使用等される可能性を減らすことができる。特に、パソコン起動時のパスワード機能の利用が情報の漏えいに対する有効な防止対策になる。また、次のパソコンの不正利用を防止するためのパスワード機能及び暗号化機能を活用することが必要である。

①ログインパスワード

OSやソフトウェアにログインする際に使用するパスワードであり、ログインパスワードによって、パソコンの多くの機能の不正利用を防御できる。

②電源起動時のパスワード（BIOSパスワード）

パソコンを起動したときに、OSが起動する前に入力するパスワードであり、このBIOSパスワードの設定をしておくことで、オペレーティングシステムが自動起動しない。

③電源起動時のパスワード（ハードディスクパスワード）

ハードディスクパスワードを設定しておけば、不正利用を防御できる。ただし、ハードディスクパスワードについては、失念すると解除が不可能になる場合があるために留意する必要がある。

④二要素認証の利用

取り扱う情報の重要度等に応じて前述したパスワード等の知識認証、生体認証（指紋、静脈、顔、声紋等）、物理認証（ICカード、USBトークン、トークン型ワンタイムパスワード等）のうち、異なる認証方式2種類を組み合わせた二要素認証を利用することによって、よりセキュリティ機能は強化されることになる。

⑤セキュリティチップの暗号化機能

セキュリティチップを搭載したパソコン、モバイル端末及び電磁的記録媒体の場合は、暗号鍵が当該チップに記録されているために、ハードディスクの暗号化機能を利用することによって、ハードディスク装置を抜き取られても不正利用を

防御できる。

⑥モバイル端末のセキュリティ

モバイル端末を学校外で業務利用する場合は、端末の紛失・盗難対策として、前述のように普段からパスワードによる端末ロックを設定しておくことが必要である。また、紛失・盗難に遭った際は、遠隔消去（リモートワイプ）や自己消去機能により、モバイル端末内のデータを消去する対策も有効である。

（注１）特にセキュリティ機能を強化する必要がある場合には、パスワードの流用等による悪用を防止するため、認証のために一度しか使えないワンタイムパスワードを使用することも考えられる。

（注２）ディスク装置を持たない形態のシンクライアント端末は、端末から情報が漏えいする可能性が非常に低くなることから、情報漏えい防止にも有効である。ただし、シンクライアント端末の場合、サーバ、ネットワークに障害が生じると、業務ができなくなる可能性があることから、その場合の対応、特に災害時等の対応も考慮した上で導入を行う必要がある。

（注３）パソコン、モバイル端末、通信機器、ケーブル等からは、微弱電磁波が流れている。これらから流れる電磁波から、指向性の高いアンテナを利用して、情報を盗聴することが技術的には可能である。このため、機密性の非常に高い情報を取り扱う企業等では、電磁波により重要情報が外部に漏えいすることを防止する対策を行うことがある。この電磁波盗聴対策は、シールドルーム工事等、多額の費用を要するため、盗聴された場合のリスクを考慮した上で、実施の可否を判断する必要がある。

（注４）モバイル端末の遠隔消去（リモートワイプ）機能は、モバイル端末に電源が入っており、かつ通信状態が良好な場合にしか効果が期待できない点に留意する必要がある。このことから、本機能とあわせて、データを暗号化する等、漏えいしても内容が知られることのない仕組みを合わせて導入することが有効である。

（注５）学習者用端末は、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学習者用端末を活用できるよう配慮していくこと観点から、例文③から⑥を省略している。

2.5. 人的セキュリティ

2.5.1. 教職員等の遵守事項

【趣旨】

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、情報漏えい等の被害が発生し得る。このことから、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。

情報漏えい事案の多くが、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。

【例文】

（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外部における情報処理作業の制限

（ア）CISOは、機密性2B以上、可用性2B以上、完全性2B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、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、モバイル端末及び電磁的記録媒体等を用いる場合には、教育情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

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。

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、適切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。

（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等の制限

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）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、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。

（解説）

（１）教職員等の遵守事項

教育情報セキュリティを確保するために、情報セキュリティポリシー及び実施手順に定められている事項等、全ての教職員等が遵守すべき事項について定めたものである。

教育情報セキュリティ管理者は、異動、退職等により業務を離れる場合、教職員等が利用している情報資産を返却させる。またIDについても、速やかに利用停止等の措置を講じる必要がある。

なお、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あたり、以下の事項について指導することが重要である。

〔児童生徒への指導事項〕

・モバイル端末やＵＳＢメモリ等を、学校外に持ち出す場合は、担任の許可を得ること。
・学校では、承認されていない個人のパソコン、モバイル端末等を学校の情報システムに接続してはいけないこと。
・学校では、承認されていない個人のＵＳＢメモリ等をパソコン、モバイル端末等に接続してはいけないこと。
・モバイル端末等のソフトウェアに関する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。
・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が出るといった症状がでた場合、すぐに担任に報告すること。
・自分のＩＤは、他人に利用させてはいけないこと。
※共用でＩＤを利用している場合は、共用ＩＤの利用者以外に利用させてはいけないこと。
・パスワードは他人に知られないようにすること。

・受信したメールについて、送り主やタイトルで不審をいだいたメールは、クリックする前に担任に報告すること

①モバイル端末の持ち出し及び外部における情報処理作業

情報の漏えいは、不正なモバイル端末の持ち出しや移動中にモバイル端末が盗難に遭うなどしたことが原因で発生する場合が多い。重要な情報資産を使って外部で作業する場合には、学校内の安全対策に加え、安全管理に関して追加的な措置を定めた上で、モバイル端末の持ち出しや外部での作業の実施については許可制とするのが適切である。

（注１）モバイル端末の持ち出しを許可した場合にも、モバイル端末は常に携行することを教職員等に周知する必要がある。特に交通機関（電車、バス、自家用車等）による移動時の携行に際しては、紛失、盗難等に留意する必要がある。

（注２）共用しているモバイル端末の持ち出しでは、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必要がある。

（注３）持ち出し専用パソコンによる情報の持ち出しにおいては、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、日常においては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必要がある。

（注４）テレワークを導入する場合は、本人確認手段の確保、通信途上の盗聴を防御するために、安全な通信回線サービスを利用しなければならない。
その際、通信する情報の機密性に応じて、ファイル暗号化、通信経路の暗号化等の必要な措置を取ることが求められる。なお、テレワークセキュリティ対策については、「テレワークセキュリティガイドライン（第3版）」（平成25年3月 総務省）を参照されたい。

（注５）教職員の場合、仕事の持ち帰りが多い実態に鑑み、校務系情報については、その多くが個人情報であることを改めて認識し、各地方公共団体において安全管理措置（安全確保の措置）を徹底すること。

②支給以外のパソコンやモバイル端末等の業務利用

自宅や学校外等での情報処理作業においては支給された端末を使用することとし、支給以外の端末の使用は原則禁止とする。

やむを得ず支給以外の端末を使用する場合は、以下のような対策を実施することが必要である。

・教育情報セキュリティ管理者の許可を得る
・パスワードによる端末ロック機能や遠隔消去機能などの要件を満たしていることを教育情報セキュリティ管理者が確認する

・機密性3の情報資産については支給以外の端末での作業を禁止とする
・支給以外の端末のセキュリティに関する教育を受けた者のみ使用を許可する
・無許可で重要情報等を記録又は持ち出す行為を禁止する
・業務利用する必要がなくなった場合は、支給以外のパソコンやモバイル端末等から業務に関係する情報を削除する

さらに、支給以外の端末から教育ネットワークに接続を行う可能性がある場合は、情報漏えいを防ぐため、以下のような対策を講じる必要がある。

・シンクライアント環境やセキュアブラウザを使用する
・ファイル暗号化機能を持つアプリケーションでの接続のみを許可する

また、支給以外のパソコン、モバイル端末及び電磁的記録媒体を情報システム室に持ち込むことは禁止する。

③持ち出し及び持ち込みの記録

学校内のパソコン、モバイル端末及び電磁的記録媒体の持ち出しや業務利用を許可された支給以外のパソコン、モバイル端末及び電磁的記録媒体の持ち込みについては現状把握や資産管理のためこれを記録する必要がある。

（注６）記録簿に記録を作成する場合は、持ち出しの項目として、所属名、名前、日時、持出物、個数、用途、持出の場所、返却日、管理者の確認印等を設ける。

（注７）持ち込みの項目としては、所属名、名前、日時、持込物、個数、用途、持込の場所、持ち帰り日、管理者の確認印等を設ける。

（２）非常勤及び臨時の教職員への対応

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等の採用時に情報セキュリティポリシー等のうち守るべき内容を理解させ、必要に応じて情報セキュリティポリシーの遵守の同意書への署名を求める。また、パソコンやモバイル端末の機能は、非常勤の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。

（３）情報セキュリティポリシー等の掲示

教職員等が情報セキュリティポリシーを遵守する前提として、イントラネット等に掲示する方法により、教職員等が常に最新の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しなければならない。

（４）外部委託事業者に対する説明

外部委託事業者の内部管理が不十分であることから、情報の漏えい等が発生する事

例は多い。したがって、事業者（外部委託事業者から再委託を受けた事業者を含む）等に情報システムの開発及び運用管理を委託する場合、教育情報システム管理者は、契約の遵守を求め、委託の業務範囲に従って、情報セキュリティポリシー及び実施手順に関する事項を説明する必要がある。

なお、外部委託については、「2.8.1. 外部委託」を参照のこと。

2.5.2. 研修・訓練

【趣旨】

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。

【例文】

（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、教職員等は、毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。【推奨事項】

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。

(解説)

（１）情報セキュリティに関する研修・訓練

情報セキュリティに関する研修・訓練を実施する責任はCISOにあり、研修・訓練を定期的に行わなければならない。

（２）研修計画の立案及び実施

CISOは、全ての教職員等が、情報セキュリティの重要性を認識し、情報セキュリティポリシーを理解し、実践するために、研修及び訓練を定期的かつ計画的に実施する必要がある。

（注１）研修計画には、研修内容や受講対象者のほか、e-ラーニング、集合研修、説明会等の実施方法、時期、日程、講師等を盛り込む。

（注２）部外の研修等に、教職員等を参加させることも有益である。

情報セキュリティポリシーを運用する際、多くの部分は組織の責任者及び利用者の判断や行動に依存している。したがって、全ての教職員等を対象に研修を行う必要がある。情報セキュリティに関する環境変化は早いことから、毎年度最低１回は研修を受講するようにすることが望ましい。

研修内容は、毎回同じ内容ではなく、情報セキュリティ監査の結果や学校内外での情報セキュリティインシデントの発生状況等を踏まえ、継続的に更新することや教職員等が具体的に行動すべき事項を考慮することが望ましい。

新規採用の教職員等に対しては、採用時に情報セキュリティ研修を行うことによって、情報セキュリティの大切さを深く認識させることができる。

また、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研修を実施することが必要である。これは不正アクセスから情報資産を防御することはもとより、不正プログラムの感染、侵入、内部者による情報の漏えい、外部への攻撃等を防

ぐ観点からも重要である。

研修受講を確実にするため、CISOに、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研修の実施状況を報告させる義務を負わせる。

また、CISOは、研修計画を通じて将来の情報セキュリティを担う人材の育成や要員の管理を行うとともに、地方公共団体の長によるメールでの周知等、研修効果を向上させる施策を講じることが望ましい。

なお、外部の専門家や内部の職員を最高情報セキュリティアドバイザー（CISOの補佐）等として登用している場合は、それら専門家等を内部教育に有効活用することも考えられる。

（3）緊急時対応訓練

実際に情報の漏えい等の情報セキュリティインシデントが発生した場合に、即応できる態勢を構築しておくため、緊急時を想定した訓練を定期的に実施しなければならない。

（4）研修・訓練への参加

全ての教職員等に対し、研修・訓練に参加させることが情報セキュリティ確保にとって必要であることから、義務規定を設ける。

（注３）教育・訓練の実施後、理解度試験等を行い、その有効性を評価し、次回の研修・訓練の改善に活用すれば、より効果を上げることができる。

2.5.3. 情報セキュリティインシデントの報告

【趣旨】

情報セキュリティインシデント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、「2.7.3. 侵害時の対応等」による。

【例文】

（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、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及び教育情報セキュリティ責任者に報告しなければならない。

（2）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、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、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に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。

④ CISOは、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るための窓口を設置し、当該窓口への連絡手段を公表しなければならない。【推奨事項】

（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 統括教育情報セキュリティ責任者は、情報セキュリティインシデントについて、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に報告しなければならない。

② CISOは、統括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。

（解説）

（1）学校内からの情報セキュリティインシデントの報告

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に、自らの判断でその情報セキュリティインシデントの解決を図らずに速やかに教育情報セキュリティ管理者に報告し、その指示を仰ぐことが必要である。その情報セキュリティインシデントによる被害を拡大しないためにも、報告ルート及びその方法を事前に定めておく必要がある。

（注１）情報セキュリティインシデント発生時の報告ルートは、学校及び教育委員会の意思決定ルートと整合性を図ることが重要である。

（注２）教職員は、情報セキュリティインシデントかどうか判断に迷う場合も多いと想定されるため、少しでも疑わしいと思った時点で、速やかに教育情報セキュリティ管理者に報告するとともに、教育情報セキュリティ管理者は情報セキュリティに関する統一的な窓口等の専門家による判断を仰ぐことが重要である。

（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

住民からの報告が契機となって、重大な情報セキュリティインシデントの発見につながる場合等も想定されることから、当該報告、連絡を受ける窓口を設置することが望ましい。

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

（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

情報セキュリティインシデント原因を究明し、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管理者は、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。

2.5.4. ID 及びパスワード等の管理

【趣旨】

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えい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えいするリスクを最小限にとどめる必要がある。

【例文】

（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若しくはパソコン等の端末のスロット等から抜いておかなければならない。

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

②統括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統括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）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は一切応じてはならない。
③パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。
④パスワードが流出したおそれがある場合には、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、古いパスワードを再利用してはならない。
⑥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。
⑦仮のパスワードは、最初のログイン時点で変更しなければならない。
⑧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。
⑨教職員等間でパスワードを共有してはならない。

(解説)

（１）ICカード等の取扱い

認証のため、ICカードやUSBトークン等の媒体を利用する場合は、情報のライフサイクルに着目し、利用、保管、返却、廃棄等の各段階における取扱い方法を定めておくことが必要である。

（２）IDの取扱い

ID(Indentification)とは本人確認の情報のことで、情報システムや端末にログイ

ンする際に本人であることを示すものであり、他者にこの情報が渡れば、本人になり代わってログインが可能（なりすましの脅威）となるため、IDは本人だけが分っている必要がある。共用IDの場合は、共用することが許される集団のみが知り得る情報であることから、集団の外に漏らしてはいけない。また、外部からのアクセスの場合には、共用IDの利用は避けることが望ましい。

（３）パスワードの取扱い

パスワードの秘密を担保するため、想像しにくいパスワード設定（例えば、大文字と小文字を組み合わせる、数字とアルファベットと記号を組み合わせる等）、パスワードの共有禁止などを定める。

（注１）複数のシステムを取り扱う等により、複数の異なるパスワードが必要となる場合があるが、全てを覚えることの困難性から、安易なパスワードを数個使い回すといった運用が起こる可能性がある。

パスワードのメモを作成し、机上、キーボード、ディスプレイ周辺等にメモを置くことは禁止する必要はあるが、特定の場所に施錠して保存する等により他人が容易に見ることができないような措置をしていれば、メモの存在がパスワードの効果を削ぐものではないため、パスワードのメモそれ自体の作成を禁止するものではない。

（注２）固定パスワードによるアクセス制限では、時間の経過に伴い、悪意のある第三者による不正侵入、不正操作等のセキュリティリスクが高まるため、 定期的にパスワードを変更することが必要である。

なお、一度限り有効な使い捨てのワンタイムパスワードを利用することで、こうしたリスクを低減する方法もある。

パスワードの定期的変更の是非については専門家の中でも見解が異なっていることから、引き続き、自治体におけるパスワードの運用実態及び技術的動向等も勘案しながら、必要に応じて見直しを行うこととする。

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

【趣旨】

ネットワークや情報システム等の管理が不十分な場合、不正利用による情報システム等へのサイバー攻撃、情報漏えい、損傷、改ざん、重要情報の詐取、内部不正等の被害が生じるおそれがある。このことから、情報システム等の不正利用を防止し、また不正利用に対する証拠の保全をするために、ログの管理やシステム管理記録の作成、バックアップ、無許可ソフトウェアの導入禁止、機器構成の変更禁止等の技術的なセキュリティ対策を規定する。

【例文】

（1）文書サーバ及び端末の設定等

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、機微な個人情報を保管する場合に限る）については、標的型攻撃等によるファイルの外部流出の可能性を考慮し、ファイル暗号化等による安全管理措置を講じなければならない。

（2）バックアップの実施

統括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。【推奨事項】

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

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

統括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、適切に管理しなければならない。

（６）ログの取得等

①統括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統括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統括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

統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

（８）ネットワークの接続制御、経路制御等

①統括教育情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

②統括教育情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

（９）外部の者が利用できるシステムの分離等

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

（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には、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統括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想定される場合には、統括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）ネットワークの分離

①教育情報システム管理者は、校務系システム及び学習系システム間の通信経路の物理的又は論理的な分離をするとともに、校務系システム及び校務外部接続系シ

ステム間の通信経路を物理的又は論理的に分離し、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。

②教育情報システム管理者は、校務系システムと校務外部接続系システム及び学習系システム間で通信する場合には、ウイルス感染のない無害化通信など、適切な措置を図らなければならない。

（１２）複合機のセキュリティ管理

①統括教育情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

②統括教育情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③統括教育情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

（１３）特定用途機器のセキュリティ管理

統括教育情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施しなければならない。

（１４）無線LAN及びネットワークの盗聴対策

①統括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統括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統括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統括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統括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統括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統括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、外部委託事業者との間で利用方法を取り決めなければならない。

⑥統括教育情報セキュリティ責任者は、教職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置しなければならない。【推奨事項】

（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フリーメールサービス等を統括教育情報セキュリティ責任者の許可無しに使用してはならない。

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

（解説）

（1）文書サーバ及び端末の設定等

文書サーバを教育委員会等に設置し、複数の学校等で共用している場合は、教職員等が利用可能な容量を取り決める必要がある。また学校間でのアクセス制御を行う必要がある。

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においては、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ることが重要である。

なお、ファイル暗号化等による安全管理措置を講ずるに当たっては、教職員の業務負担軽減等に考慮して、作成したファイルの自動暗号化及び復号化等の対策を採ることも選択肢の一つとして考えられる。

（2）バックアップの実施

緊急時に備え、ファイルサーバ等に記録される情報について、バックアップを取ることが必要である。

校務系システムは、成績処理等、教員が毎日の業務において活用するものであり、校務系サーバ及び校務外部接続系サーバの情報資産を消失した場合、学校事務の遂行に支障を及ぼすことが予想される。このため、校務系サーバ及び校務外部接続系サーバについては、バックアップを行うことが重要である。

学習系サーバにおいても、児童生徒が作成した情報資産の消失を防ぐためにバックアップを行うことが望ましい。

（注１）バックアップを行う場合には、データの保全を確保するため、バックアップ処理の成否の確認、災害等による同時被災を回避するためバックアップデータの別施設等への保管、システムを正常に再開するためのリストア手順の策定及びリストアテストによる検証が必要である。

（３）他団体との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、紛失又は改ざん等が起こらないようにしなければならない。

（注２）これを担保するため、相手方の団体との間で当該内容を明記した合意文書を取り交わす等の対策を取ることが望ましい。

（４）システム管理記録及び作業の確認

情報システムに対して行った日常の運用作業については、記録を残しておくことが必要である。特に、システム変更等の作業を行った場合は、情報システムの現状を正確に把握するため、当該作業内容を記録し、詐取又は改ざん等のないよう適切に管理しておくことが必要である。

また、システム変更等の作業を行う場合は、2人以上で確認を行い、設定ミス又はプログラムバグ等によるシステム障害のリスクを減らさなければならない。

（５）情報システム仕様書等の管理

情報システム及びネットワークに関する文書は、悪意を持つ者に攻撃材料として使われるおそれがあることから、機密性3相当の文書として扱い、業務上必要のある者以外が閲覧したり、紛失等が生じないように管理する必要がある。

（６）ログの取得等

ログ（アクセスログ、システム稼動ログ、障害時のシステム出力ログ）及び障害対応記録は、悪意の第三者等による不正侵入や不正操作等の情報セキュリティインシデントを検知するための重要な材料となる。また、情報システムに係る情報セキュリティの上の問題が発生した場合には、当該ログ等は、事後の調査の過程で、問題を解明

するための重要な材料となる。したがって、情報システムにおいては、仕様どおりにログ等が取得され、また、改ざんや消失等が起こらないよう、ログ等が適切に保全されなければならない。

なお、校務系システム及び校務外部接続系システムのログについては6か月以上保存することが望ましい。

（注３）保管期限を設定し、期限が切れた場合は、これらの記録を確実に消去する必要がある。

（７）障害記録

システム障害への対応を決める際、過去に起きた類似障害が参考になるので、障害記録を適切に保存しておく必要がある。

（注４）障害記録のデータベース化を図るなど、障害対応を決める場合に活用できるように保管しておくことが重要である。

（８）ネットワークの接続制御、経路制御等

ネットワーク上では、フィルタリング、ルーティング、侵入検知システム等が機能しているが、これらの機能を十分活用するため、ハードウェア及びソフトウェアの設定を適切に行うよう注意する必要がある。また、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

なお、クラウドサービスを利用し、機密性2Ａ以上の情報を外部のデータセンターとやり取りする場合は、VPN接続による通信経路の暗号化や本人認証等の高度なセキュリティ対策を行う必要がある。さらに仮想ネットワークを構築する場合には、仮想ネットワークと物理ネットワークとの対応関係、仮想ネットワークの運用設定方針と設定承認方針及び施設内設備をクラウドサービスに移行する場合の注意事項等について確認し、適切な対策を実施する必要がある。

（９）外部の者が利用できるシステムの分離等

保護者からのメールアドレス登録等を含む電子申請受付システム、施設を訪問した住民等に対する施設案内システムなど、外部の人々が利用できるシステムは、不正アクセス等を防御するため、必要に応じ、他のシステムのネットワークと切り離すなどの措置が必要である。

（１０）外部ネットワークとの接続制限等

インターネットに接続し、公開しているウェブサーバ等が、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ために、庁内及び学校と外部ネットワークの境界にファイアウォールを設置する必要がある。

（注５）このほか、非武装セグメントを設け公開サーバを接続すると有効である。また、非武装セグメントに接続している公開サーバについて、不要なポートの閉鎖、不要なサービスの無効化、エラーメッセージの簡略化(攻撃者に対して、システムの技術情報を過度に表示し、与えない対策)を実施することによって、防御能力を高めることができる。

（１１）ネットワークの分離

児童生徒の成績情報や生徒指導関連情報等の機微な個人情報を扱う「校務系システム」に対するインターネット経由の標的型攻撃や児童生徒による「学習系システム」からの不正アクセスから防止するため、ウェブ閲覧やインターネットメールなどのシステム(「校務外部接続系システム」)や「学習系システム」との通信経路を分離すること。また、「校務系システム」と「校務外部接続系システム」及び「学習系システム」の間で通信する場合には、ウイルスの感染のない無害化通信など、適切な措置を図ること。

あわせて、「校務外部接続系システム」についても、機微な個人情報を扱う可能性があることから、適切な安全管理措置を講ずる必要がある。

なお、上記の考え方に従った場合、校務用端末については、以下のいずれかの対応が必要となる。

①「校務系システム」用と「校務外部接続系システム」用の２台の端末を使い分ける

②「校務系システム」と「校務外部接続系システム」を論理的に分離（仮想化技術等）することにより１台の端末とする

③職員室等に共用のインターネット接続用の端末を配備し、校務用端末についてはインターネット接続を不可とする。

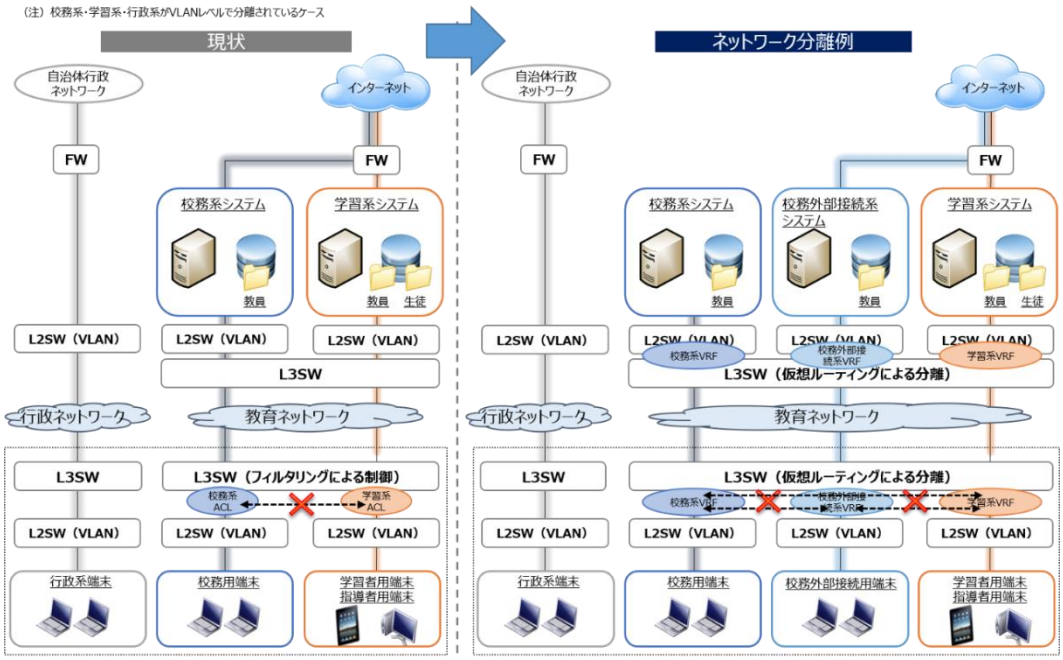
各地方公共団体においては、学校現場における校務事務の実態と対策に係る費用等を勘案して、ネットワークの分離方法を判断する必要がある。

（注６）文部科学省においては、平成29年度から、総務省と連携をし、「校務系情報」と「学習系情報」を有効につなげ、可視化することを通じ、教員による学習指導や生徒指導等の質の向上や学級・学校運営の改善等に資することを目的として、学校におけるデータ活用方策等を整理するための実証研究（「次世代学校支援モデル構築事業」）を実施することとしている。
当該実証研究を通じて「校務系システム」と「学習系システム」とのセキュアな連携の在り方について整理をし、本ガイドラインに反映する予定である。

（注７）無害化通信とは、インターネットメールに添付されたファイルの削除やHTMLメールをテキストデータ化することによってテキスト本文のみを校務系システムで閲覧可能とすること（メール無害化）や、仮想デスクトップ等の画面転送プロトコルを用いた技術によりインターネット接続を前提としたシステ

ムからのウイルス感染がないようにすること（通信の無害化）の総称となる。

なお、ファイルの取り込みにおいては、ファイル無害化機器（ソフトウェア、サービス等も含む）の活用が考えられるが、従来のパターンマッチング型のウイルス対策製品だけでなく、ゼロデイ攻撃を対象にしたウイルス対策製品を利用し無害であることを確認した上でファイルを取り込む方法もある。



図表7　ネットワーク分離例

（１２）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管理の明確化

複合機の管理者を明確にする。あわせて、複合機のネットワーク接続に関して、ルールを定め、内部に周知させる。

②ネットワークによる保護

必要性がない場合には、複合機を外部ネットワーク（インターネット）に接続しない。また、外部ネットワークと複合機を接続する場合には、ファイアウォールやブロードバンドルータを経由させ、許可する通信だけに限定する。

③機器の適切な設定

管理者用 ID、パスワードを工場出荷時に設定されているものから変更する。該当機器の製品ホームページを確認し、ソフトウェアを最新の状態に更新する。

（注８）プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器を「複合機」という。複合機は、施設内ネットワークや公衆電話網等の通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定されることに注意が必要である。

（１３）特定用途機器のセキュリティ管理

サーバやパソコンと同様にネットワーク接続の機能を備えたテレビ会議システム、IP 電話システム、ネットワークカメラシステム等もセキュリティ対策が必要となる。機器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管理の明確化（管理対象の機器を正確に把握）

機器の管理者を明確にする。また、有線 LAN や無線 LAN に接続されている機器を洗い出し、機器がインターネットに直接接続していないか確認する。

②ネットワークによる保護

必要性がない場合には、機器を外部ネットワーク（インターネット）に接続しない。また、外部ネットワークと機器を接続する場合には、ファイアウォールやブロードバンドルータを経由させ、許可する通信だけに限定する。

③機器の適切な設定

管理者用 ID、パスワードを工場出荷時に設定されているものから変更する。機器のアクセス制御機能を有効にし、データアクセス時に ID、パスワード等の認証を求める運用にする。

（注９）テレビ会議システム、IP電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は電磁的記録媒体を内蔵しているものを「特定用途機器」という。これらの機器についても当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により想定される脅威に注意が必要である。

（１４）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。

（注１０）暗号化方式の1つであるWEP（Wired Equivalent Privacy）については、既に脆弱性が公知となっているため、暗号強度が確認されている暗号方式を

採用しなければならない。

（注１１）無線LANの不正利用調査を行い、探査ツール等を用い、無許可のアクセスポイントや使用されていないアクセスポイントが設置されていないことを点検することも有益である。

（１５）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。

中継処理の禁止は、メールサーバが踏み台となり他のサーバに攻撃を行うことを防止するために必要がある。

教職員等が電子メールの送信等により情報の外部への不正な持ち出しをしていないか監視するためには、フィルタリングソフトウェア等を利用する。

（注１２）上司など指定した職員に同報しなければ、送信できないように設定し、外部への持ち出しを牽制する方法等もある。

（注１３）電子メールの送信に使われる通信方式の１つであるSMTP（Simple Mail Transfer Protocol）では、差出人のメールアドレスを誰でも自由に名乗ることができるため、送信者のアドレス詐称（なりすまし）が容易にできる問題がある。このため、電子メールのなりすまし対策として、受信者側は送信ドメイン認証技術（SPF、DKIM)を導入するとともに、正規の送信者に対して受信者側の認証結果を通知する仕組み（DMARC）を導入し、社会インフラとしてのなりすましメール対策を図ることが効果的である。

（１６）電子メールの利用制限

教職員等が電子メールを利用する際の取扱いについて規定したものである。不正な情報の持ち出しを防止する観点から、電子メールの自動転送を禁止する。

プロバイダーが提供するサービスである、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ことから、これらのサービスを利用する場合は、統括教育情報セキュリティ責任者の許可を前提とし、適切なセキュリティ対策を講じる必要がある。

複数の送信先に電子メールを送る場合、他の送信先の電子メールアドレスが分からないようにするには、宛先やCCではなく、BCCに送信先を入力する方法がある。

（注１４）HTML形式の電子メールを使用禁止にする、メールソフトのプレビュー機能を使用しないことによってコンピュータウイルス感染の可能性の低減を図ることができる。

（１７）電子署名・暗号化

暗号方法は、組織として特定の方法を定める。教職員等が自由に暗号方法を利用すると、暗号鍵を紛失した場合に、復号できなくなる可能性が高く、データ自体が完全に破壊されたのと同じ状態になってしまうことがあるためである。

また、署名検証者が電子署名を検証するための電子証明書を信頼できる機関からダウンロードできる環境を整備したり、電子署名の付与を行う教育情報システム管理者から電磁的記録媒体等で入手できる体制を整備する必要がある。

（１８）無許可ソフトウェアの導入等の禁止

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。

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。

（注１５）あらかじめ、一定のソフトウェアを指定して、その範囲では個別の許可を不要とする運用もあり得る。

（１９）機器構成の変更の制限

教職員等が、メモリ増設等の際に静電気を発生させるなど、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り、許可を得ない構成変更は禁止する必要がある。

（２０）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、無許可での接続を禁止する。

（注１６）特に、学校内で無線LANを使用している場合に、教職員等や外部委託事業者がパソコンやモバイル端末等を持込み、無許可でアクセスポイントへ接続する行為を禁止する必要がある。

（２１）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。統括教育情報セキュリティ責任者は、業務外での閲覧を発見した場合は、教育情報セキュリティ管理者に通知

し、対応を求めなければならない。

2.6.2. アクセス制御

【趣旨】

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、情報漏えい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は統括教育情報セキュリティ責任者及び教育情報システム管理者に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。

【例文】

（1）アクセス制御等

①アクセス制御

統括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。

②利用者IDの取扱い

（ア）統括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、統括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）統括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）統括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）統括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、統括教育情報セキュリティ責任者及び教育情報システム管理者が指名し、CISOが認めた者でなければならない。

（ウ）CISOは、代行者を認めた場合、速やかに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及び教育情報システム管理者に通知しなければならない。

（エ）統括教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与されたID及びパスワードの変更について、外部委託事業者に行わせてはならない。

（オ）統括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、その他利用者よりもパスワードの有効期限を短くしたり、入力回数制限を設ける等のセキュリティ機能を強化しなければならない。

（カ）統括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。

（キ）統括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のログ監視を行わなければならない。【推奨事項】

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

④統括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統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部からのアクセスに利用するモバイル端末を教職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

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

⑦統括教育情報セキュリティ責任者は、公衆通信回線（公衆無線LAN等）を教育ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のID及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ICカード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならな

い。

（３）自動識別の設定

統括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、ネットワークで使用される機器について、機器固有情報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。【推奨事項】

（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統括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統括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。

(解説)

（１）アクセス制御

管理者権限（サーバの全ての機能を利用できる権限）等の特権は、全ての機能を利用可能にするので、利用者登録を厳格に行うとともに、特権で利用するID及びパスワードを厳重に管理する必要がある。

（注１）外部委託事業者が利用する場合にも、ID及びパスワードの利用については、全て統括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管理しなければならない。

（注２）管理者権限等の特権の悪用を防ぐために、「セキュアOS」（これまでのOSでは対応できなかったアクセス制御を実施し、セキュリティ強化を図る機能）

を利用することが考えられる。セキュアOSは、「強制アクセス制御」及び「最小特権」の機能に特徴がある。

強制アクセス制御	特権の操作に対しても、情報へのアクセス制御を実施させる機能
最小特権	特権のID を利用できる者でも、強制アクセス制御機能で必要最小限のアクセスしか認めない機能

（注３）児童生徒が扱うIDについては本規定の範囲外となる。

（２）教職員等による外部からのアクセス等の制限

外部から教育ネットワークや情報システムに接続を認める場合は、外部から攻撃を受けるリスクが高くなることから、本人確認手段の確保、通信途上の盗聴を防御するために、原則、安全な通信回線サービスを利用しなければならない。その際、通信する情報の機密性に応じて、ファイル暗号化、通信経路の暗号化、専用回線の利用等の必要な措置を取ることが求められる。また、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。

（注４）持ち込んだモバイル端末を確認するシステムとして、検疫システムがある。検疫システムとは、OSのパッチやコンピュータウイルス対策ソフトウェアのパターンファイルが最新でない、不正プログラムが侵入しているなど、十分なセキュリティ対策が取られていないモバイル端末を教育ネットワークに接続させないシステムである。モバイル端末を学校内に持ち帰った場合等に、検疫システムによる確認を義務付けることにより、様々な脅威の発生を防止することができる。

（注５）学校外から教育ネットワークや情報システムにアクセスする際に公衆無線LAN等の学校外通信回線を利用することは原則禁止であるが、やむを得ず利用する場合は、統括教育情報セキュリティ責任者の許可を得た上で、必要最小限の範囲のみのアクセスとする。さらに、ログを取得し、不正なアクセスがないかを定期的に確認することが求められる。

（３）自動識別の設定

ネットワークに不正な機器の接続を防止するために、電子証明書による端末認証や、接続する機器のIPアドレス、MACアドレス等の認証情報を利用し制限する必要がある。

（４）ログイン時の表示等

ソフトウェアに、ログイン試行回数の制限や、直近に使用された日時が表示される機能等がある場合は、それらを有効に活用し、不正にパソコン等の端末が利用されないようにする必要がある。

（5）パスワードに関する情報の管理

パスワードの機能は、ソフトウェアにより様々な機能があるために、これらの機能を有効に利用することが求められる。

（6）特権による接続時間の制限

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、システムの未使用時には自動的にネットワーク接続を終了するなどの措置を講じる必要がある。

2.6.3. システム開発、導入、保守等

【趣旨】

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又は統合時の十分な検証等も含まれる。

【例文】

（1）情報システムの調達

①統括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統括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ければならならない。

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。【推奨事項】

（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、あらかじめ擬似環境による操作確認を行わなければならない。

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

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

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

（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を適切な方法で保管しなければならない。

（５）情報システムにおける入出力データの正確性の確保
①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を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

（８）システム更新又は統合時の検証等
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。

（解説）

（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。

（注１）情報機器及びソフトウェア等の情報セキュリティ機能の評価に当たっては、第三者機関による客観的な評価である、ISO/IEC15408に基づくITセキュリティ評価及び認証制度による認証の取得の有無を評価項目として活用すること又は構築する情報システムに重要な情報セキュリティ要件があると認められた場合には、第三者機関による当該情報システムのセキュリティ設計仕様書（ST: Security Target）のST評価・ST確認を活用することも考えられる。「ITセキュリティ評価及び認証制度（JISEC）」については、独立行政法人情報処理推進機構のサイトを参照のこと。

（注２）システム調達、開発、導入を行うに当たっては、CISOの許可を得て実施することが望ましい。

（注３）情報システムの利用を満足できるものにするためには、情報システムが当該利用に足りる十分な処理能力と記憶容量を持つことが必要である。また、処理能力と記憶容量の使用状況を監視し、将来的に必要とされる能力・容量を予測して、ハードディスクの増強等適切な措置をとることが望まれる。

（注４）情報システムは可用性の観点から、冗長性を組み入れることを考慮することが望ましい。ただし、冗長性を組み入れることにより、情報システムの完全性、機密性に対するリスクが生じる可能性があるため、この点についても考慮すること。

・機密性を高める対策例

サーバを二重化することにより場合によっては機密性の高い情報が二カ所に保存されることになるため、修正プログラムの適用やソフトウェアの最新化、不要なサービスの停止といったセキュリティの確保を二重化した双方のサーバに同時・同等に実施する。

・完全性を高める対策例

二重化したサーバ内の情報の整合性を確保するために、双方のサーバ内のデータの突合確認や誤り訂正機能の実装などの対策を実施する。

（注５）IT製品の調達において、その製品に他の供給者から供給される構成部品やソフトウェアが含まれる場合には、そのサプライチェーン全体に適切なセキュリティ慣行を伝達し、サプライチェーンの過程において意図せざる変更が加えられないよう、直接の供給者に要求することが必要である。また、提供されたIT製品が機能要件として取り決められたとおりに機能すること、構成部品やソフトウェアについてはその供給元が追跡可能であることを保証させることが望ましい。

（注６）調達する情報システムに応じた要件の詳細については、「非機能要求グレード（地方公共団体版）利用ガイド」（平成26年3月 地方自治情報センター）

「IT製品の調達におけるセキュリティ要件リスト」（平成26年5月19日 経済産業省）を参照されたい。

（注７）オンラインでの申請及び届出等の手続を提供するシステムについては、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」（平成22年8月31日 各府省情報化統括責任者（CIO）連絡会議決定）を参照されたい。

（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

システム開発においては、その責任の所在や実施体制を把握する観点から、責任者と作業者を特定する必要がある。また、システム開発の方針、手順等の規則を決定し、開発に適用する必要がある。

（注８）システム開発において、作業進捗が悪い場合等に、要員の投入が逐次行われるケースがあるが、これらのことが、要員の調整等に不備が生じるケースがある。特に、外部委託でシステム開発を行う場合等は、その理由を明確にして、要員の変更や増減の許可をする必要がある。

② システム開発における管理者及び作業者のIDの管理

システム開発において、開発用のIDは、管理がずさんになりやすい傾向があることから、適切な管理が必要である。

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

外部委託事業者が選定した開発用ソフトウェアについて、一般的に利用が知られていないソフトウェアは、その理由を確認する必要がある。また、利用することとしたソフトウェア以外のソフトウェアは削除することとする。

（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

システム開発において、開発環境と運用環境が同一であると、運用環境で使用しているプログラムやファイルを誤って書き換えてしまうことが発生しやすくなるので、システムの開発環境と運用環境は、できる限り分離し、セキュリティに配慮した設計にすることが必要である。

（注９）情報システムの導入に当たっては、利用する業務の内容や取り扱う情報の重要度に応じて、万一の障害に備えた冗長性や可用性が必要となる場合がある。事前に確認しておく事項としては、例えば次のものがある。

・その箇所が働かないとシステム全体が停止してしまう箇所の有無とその対策内容（冗長化・障害時の円滑な切り替えなど）

・広域災害対策の有無(バックアップ設備を遠隔地に配置しているなど)や対

応方針（サービス継続を優先するかセキュリティ対策の確保を優先するかなど）

② テスト

運用環境への移行は、業務に精通している利用部門の協力を得て、疑似環境における操作について、テストを行い、その結果を確認した後に行う必要がある。

（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。

（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。

（注１０）ウェブシステムの設計においては、ソースコードの記述内容にセキュリティ機能の必要性を調査せずに設計が行われるとセキュリティホールを残してしまうことがある。そこで、セキュリティ上の機能要件を洗い出し、システム開発の計画時に盛り込む必要があるほか、現在、運用しているウェブシステムについても、これらのソースコードの記述内容にセキュリティホールが潜んでいる場合があるため、ソースコードを確認する必要がある。

（注１１）ウェブアプリケーションの開発においては、セキュリティを考慮した実装を行わなければ脆弱性を作り込んでしまうおそれがある。適切なセキュリティを考慮したウェブサイトを構築するための注意点や脆弱性の有無の判定基準については、「安全なウェブサイトの作り方 改訂第７版」及びその別冊資料（2016年1月27日 情報処理推進機構）を参照されたい。

（注１２）外部の者が学校の名前をタイトルに掲げるなどし、学校のウェブサイトと誤解されかねないウェブサイトを構築することがあり、これを完全に防ぐことは困難である。このため、このようなウェブサイトを発見した、又は報告を受けた場合は、速やかに教育情報セキュリティ責任者へ報告し、対処を検討しなければならない。

（注１３）ウェブサイトや電子メール等を利用し、外部の者が提供するウェブアプリケーション又はコンテンツを告知する場合は、以下の対策を講ずること。

・告知するアプリケーション又はコンテンツを管理する組織名を明記する
・告知するアプリケーション又はコンテンツの所在場所の有効性（リンク先のURLのドメイン名の有効期限等）を確認した時期又は有効性を保証する機関について明記する
・電子メールにて告知する場合は、告知内容についての問合せ先を明記する

（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。

（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。

（８）システム更新又は統合時の検証等

システムを更新又は統合する場合は、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。

（注１４）検証等を行う事項としては、例えば次のものがある。

・システム更新又は統合作業時に遭遇する想定外の事象に対応する体制
・システム及びデータ移行手続が失敗した場合や移行直後に障害等が生じた場合における、旧システムへ戻す計画とその手順
・更新又は統合によって影響される業務運営体制
・システム及びデータ移行手続における検証チェックポイントや移行の妥当性基準の明確化

2.6.4. 不正プログラム対策

【趣旨】

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、情報漏えい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。

【例文】

（1）統括教育情報セキュリティ責任者の措置事項

統括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教育情報システム管理者は、その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システムに常駐させなければならない。

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。

（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統括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

統括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。

（解説）

（１）統括教育情報セキュリティ責任者の措置事項

インターネットからの不正プログラム感染、侵入を防御するためには、教育ネットワークとインターネットの境界で不正プログラム対策ソフトウェアを導入する必要がある。

（注１）不正プログラムには、コンピュータシステムの破壊、無差別の電子メールの送信による感染の拡散を行うコンピュータウイルスのほか、暗証番号やパスワード等を盗むことを目的にしているスパイウェアなど、多くの種類が存在している。また、″WannaCrypt″などと呼ばれるランサムウェアに関する被害が数多く発生しているが、ランサムウェアの典型的な拡散方法として、メール等による配布や、ウェブ閲覧を通じた攻撃サイトへの誘導などが知られている。当該マルウェアの感染や、感染後の拡大を防ぐために、ウイルス対策ソフトウェアの定義ファイルを最新版に更新するとともに、メールを開く際には、添付ファイルや本文の内容に十分注意することや、OS やソフトウェアを最新版に更新することが効果的である。あわせて、ランサムウェアに感染しファイルが暗号化された場合、ファイルを復号することが難しいとされているため、バックアップを定期的に実行することが効果的である。

（注２）ソフトウェアの更新は、開発元等から提供されるセキュリティホールのパッチ適用やバージョンアップ等で行うが、これらは開発元がサポートしている期間内でのみ行うことができるため、適宜サポートが終了していないソフトウェアへ切り替え等を行う必要がある。なお、ソフトウェアの更新についてはパソコン等の端末だけでなくサーバやモバイル端末についても同様にOSの更新や修正プログラムを適用する必要がある。

（注３）近年のサイバー攻撃は複雑、巧妙化しており、パターンファイルによる不正プログラム対策ソフトウェアでは検知出来ない攻撃が頻発している状況である。こうしたマルウェアを検知するためには、より迅速にマルウェアを検知することが出来る対策も重要である。

（２）教育情報システム管理者の措置事項

ウイルスチェック等のパターンファイルや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って利用することが不可欠である。

なお、インターネットに接続していないシステムは、不正プログラムの感染、侵入

の可能性は低いが、原則として教職員等が持ち込んだ電磁的記録媒体や古くから保管していた電磁的記録媒体から感染することもあり得るので、電磁的記録媒体の使用は組織内で管理しているものに限るとともに、不正プログラム対策ソフトウェアを開発元等から、定期的に取り寄せ、パターンファイルの更新やパッチの適用を確実に実施することが必要である。

（3）教職員等の遵守事項

教職員等には、不正プログラムに関する情報及び対策を周知して、対策を徹底することが必要であり、特に、不審なメールやファイルの削除、不正プログラム対策ソフトウェアを常に最新の状態に保たせることが重要である。コンピュータウイルスに感染した兆候がある場合には、即座にLANケーブルを取り外す（パソコン等の端末の場合）又は通信を行わない設定への変更（モバイル端末の場合）を行い、被害の拡大を防がなければならない。

（4）専門家の支援体制

不正プログラム対策ソフトウェアの開発元等の専門家と連絡を密にし、不正プログラム感染時等に、支援を受けられるようにしておく必要がある。

2.6.5. 不正アクセス対策

【趣旨】

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、情報漏えい、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又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。

【例文】

（1）統括教育情報セキュリティ責任者の措置事項

統括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、統括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。【推奨事項】

⑤統括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切な対応などを実施できる体制並びに

連絡網を構築しなければならない。

（2）攻撃の予告

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ることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

（3）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。

（4）内部からの攻撃

統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等及び外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（5）教職員等による不正アクセス

統括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、適切な処置を求めなければならない。

（6）サービス不能攻撃

統括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

統括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。

（解説）

（1）統括教育情報セキュリティ責任者の措置事項

使用されていないTCP/UDPポートや不要なサービスは、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。

（注１）重要なファイルの改ざんについては、改ざん検知ソフトウェアの利用によって、不正アクセス、不正プログラムの侵入を検知することが可能である。

（注２）CSIRTを活用してCISOへの報告、各部部局への指示、ベンダとの情報共有及び報道機関への通知・公表などの対応を行うとともに、地方公共団体情報システム機構（自治体CEPTOAR）等の関係機関や他の地方公共団体の同様の窓口機能、外部の事業者等と連携して情報共有を行うことが望ましい。

（２）攻撃の予告

情報システムに対する攻撃予告があり、攻撃を受けることが確実な場合には、システム停止等の措置をとらなければならない。また、関係機関との連絡を密にし、情報収集に努めなければならない。

（注３）攻撃を受けた際の対応として、「緊急時対応計画」に基づき、ログの確保、被害を受けた場合の復旧手順の策定、庁内関係者の役割等を再確認しておく必要がある。

（３）記録の保存

外部から不正アクセスを受けた場合に、その記録としてログ、対応した記録等を保存しておくことは、事実確認、原因追及及び対策検討のため、必要であり、記録の保存について定めておく必要がある。

（注４）不正アクセスについてログ解析を行う場合は、証拠保全用と解析用と分けて保管する必要がある。

（４）内部からの攻撃

教育ネットワークに接続したパソコン、モバイル端末及び不正プログラムに感染した庁内サーバを使って、庁内のサーバや外部のサーバ等に攻撃を仕掛けられる場合があり、これらを監視しなければならない。

（注５）学校内で住民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。

（５）教職員等による不正アクセス

教職員等が学校内にあるパソコンやモバイル端末を利用し、不正アクセスを発見した場合には、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。

（６）サービス不能攻撃

サービス不能攻撃はDoS（Denial of Service）攻撃やDDoS（Distributed Denial of Service）攻撃とも呼ばれている。第三者からサービス不能攻撃を受けた場合でも、情報システムの可用性を維持するために次の例のような対策を行う必要がある。また、これらの対策が適切に実施されているかをモニタリングし、確かめる必要がある。

①情報システムを構成する機器の装備している機能による対策の実施

- サーバ装置、端末及び通信回線装置について、サービス不能攻撃に対抗するための機能が実装されている場合は、これらを有効にする。
- 通信事業者と協議し、サービス不能攻撃が発生時の対処手順や連絡体制を整備する。

②サービス不能攻撃を想定した情報システムの構築

- サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断したり、通信回線の通信量を制限したりするなどの手段を有する情報システムを構築する。
- サービスを提供する情報システムを構築するサーバ装置、端末、通信回線装置及び通信回線を冗長化し、許容される時間内に切り替えられるようにする。
- サービス不能攻撃の影響を排除又は低減するための専用の対策装置を導入する。

③通信事業者の提供するサービスの利用

- 通信事業者が別途提供する、サービス不能攻撃に係る通信の遮断等のサービスがある場合は、これを利用する。

④情報システムの監視及び監視記録の保存

- 学校外からアクセスされるサーバ装置や、そのアクセスに利用される通信回線装置及び通信回線の中から、特に高い可用性が求められるものを優先的に監視する。
- 監視の記録については、監視対象の状態の変動を考慮した上で記録を一定期間保管する。

（７）標的型攻撃

標的型攻撃による外部から教育ネットワーク内への侵入を防ぐため、標的型攻撃メール受信時の人的対策のほか、電磁的記録媒体やネットワークに対する技術的対策についても次の例のような対策を行うこと。また、これらの対策が適切に実施されているかをモニタリングし、確かめる必要がある。なお、対策の検討にあたっては、「高

度サイバー攻撃対処のためのリスク評価等のガイドライン」（平成28年10月7日 情報セキュリティ対策推進会議）及び「高度サイバー攻撃対処のためのリスク評価等のガイドライン 付属書」（平成28年10月 7 日 内閣官房情報セキュリティセンター）も参照されたい。

①人的対策例（標的型攻撃メール対策）

- 差出人に心当たりがないメールは、たとえ興味のある件名でも開封しない。
- 不自然なメールが着信した際は、差出人にメール送信の事実を確認する。
- メールを開いた後で標的型攻撃と気付いた場合、添付ファイルは絶対に開かず、メールの本文に書かれたURLもクリックしない。
- 標的型攻撃と気付いた場合、システム管理者に対して着信の事実を通知し、組織内への注意喚起を依頼した後に、メールを速やかに削除する。
- システム管理者は、メールやログを確認し、不正なメールがなかったかチェックする。（事後対策）

②電磁的記録媒体に対する対策例

- 出所不明の電磁的記録媒体を内部ネットワーク上の端末に接続させない。
- 電磁的記録媒体をパソコン等の端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。
- パソコン等の端末について、自動再生（オートラン）機能を無効化する。
- パソコン等の端末について、電磁的記録媒体内にあるプログラムを媒体内から直接実行することを拒否する。

③ネットワークに対する対策例

- ネットワーク機器のログ監視を強化することにより、情報を外部に持ち出そうとするなどの正常ではない振る舞いや外部との不正な通信を確認し、アラームを発したりその通信を遮断する等、ウェブアクセスによって引き起こされるマルウェア感染を防ぐ。
- 不正な通信がないか、ログをチェックする。（事後対策）

2.6.6. セキュリティ情報の収集

【趣旨】

ソフトウェアにセキュリティホールが存在する場合、システムへの侵入、改ざん、損傷、漏えい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。

【例文】

（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

統括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及び周知

統括教育情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、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

統括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。

(解説)

（1）セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

セキュリティホールは日々発見される性質のものであることから、積極的に情報収集を行う必要がある。

（注１）セキュリティホールの情報収集に関しては、情報収集の体制、分析の手順、情報収集先、情報共有先等を決めておくことが望まれる。

（注２）セキュリティホールの緊急度のレベルに応じて、更新の実施の有無を検討する。深刻なセキュリティホールが発見された場合は、直ちに対応しなければならないが公開された脆弱性の情報がない段階においては、サーバ、端末及び通信回線上で取り得る対策を検討する。また更新計画を定め、他のシステムへの影響、テスト方法、バックアップの実施、パッチの適用後のシステム障害が生じた場合の復旧手順等を盛り込むことが望ましい。

（注３）不正プログラム、セキュリティホールのパッチの適用情報については、必要に応じ、イントラネットを利用して閲覧できるようにし、教職員等に対して速やかに周知することが望ましい。

（2）不正プログラム等のセキュリティ情報の収集・周知

（注４）セキュリティ情報の入手先としては、情報システムの納入業者のほかに、JPCERT/CC（一般社団法人JPCERT コーディネーションセンター）、IPA（独立行政法人 情報処理推進機構）等がある。

（３）情報セキュリティに関する情報の収集及び周知

情報セキュリティに関する技術は、新たな技術の開発や普及状況の変化により、期待した情報セキュリティの有効性が失われることや新技術への移行によって既存技術を利用したサービスを受けることができなくなる等、新たなリスクを発生する可能性もあり、情報システム等の情報セキュリティインシデントやセキュリティ侵害の未然の防止のために情報セキュリティに関する技術の動向や技術環境等の変化に関する情報収集と対策を行う必要がある。

（注５）情報セキュリティに関する技術の変化による新たな脅威として、「重要インフラにおける情報セキュリティ確保に関わる「安全基準等」策定にあたっての指針（第３版）」（平成25年2月22日改定　情報セキュリティ政策会議）では、下記の事項が挙げられている。

・電子計算機の性能向上等により暗号の安全性が低下する「暗号の危殆化」

・インターネットの普及によるIPv4アドレス枯渇化に伴う「IPv6移行」

また、情報収集と対策の検討に当たっては、必要に応じて、外部専門家等の活用も検討する必要がある。

（注６）暗号の危殆化については、「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」（平成20年4月22日情報セキュリティ政策会議決定）、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」（平成25年3月1日総務省及び経済産業省）を参照されたい。

（注７）IPv6への移行については、IPv6通信を導入する場合における他の情報システムへの影響や、IPv6通信を想定していないネットワークに接続される全ての情報システム及びネットワークに対するIPv6通信を抑止するための措置、IPv6通信を想定していないネットワークを監視し、IPv6通信が検知された場合には通信している装置を特定し、IPv6通信を遮断するための措置を考慮する必要がある。

（注８）導入しているソフトウェア（OSを含む。）のサポートが終了した場合、新たな脆弱性が発見されたとしても修正プログラムが製造元から提供されず、情報の流出や第三者を攻撃するための踏み台として利用される等の可能性が高まるため、サポート期間の情報を収集し、適切な対策を実施する必要がある。

2.7. 運用

2.7.1. 情報システムの監視

【趣旨】

情報システムにおいて、不正プログラム又は不正アクセス等による情報システムへの攻撃又は侵入、部内職員の不正な利用、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。

【例文】

①統括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統括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統括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、機密性2B以上、完全性2B以上、可用性2B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統括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、機密性2A、完全性2A、可用性2A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。【推奨事項】

(解説)

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。情報システムの稼働状況について、インターネットからの不正アクセスの状況や部内職員の利用状況も含め、ネットワーク監視等により常時確認を行うことが必要である。また、記録については、証拠としての正確性を確保するために、サーバの時刻設定を正確に行う必要がある。サーバ間で時刻記録に矛盾が生じると、ログ解析等追跡が困難になるとともに、証拠としての正確性が担保できないことになる。

（注１）ネットワーク及び情報システムの稼働中は常時監視し、障害が起きた際にも速やかに対応できる体制である必要がある。このため、リスクに応じて侵入検知システム等の利用、監視体制の整備等の措置を講じる必要がある。ネットワーク監視で侵入検知に利用する、侵入検知システム（IDS: Intrusion Detection System）は、不正プログラム対策ソフトウェアのパターンファイルと同様に、不正アクセスのパターンを検知するためのファイルの更新を行

い、検知能力を維持する必要がある。また、侵入検知だけではなく、侵入を防御する、侵入防御システム（IPS:Intrusion Prevention System）も存在する。

（注２）システム管理者などの特別な権限を持つIDの利用者の記録の確認については、本人以外のシステム管理者又はシステム管理者以外の者が確認するようにし、客観的に確認できる仕組みを構築する必要がある。

（注３）セキュリティ監視の観点からも、重要な情報資産は、教育委員会等によるセンターサーバ保管又はセキュリティ要件を満たしたデータセンターが望ましい。

（注４）首長部局と連携しセキュリティの監視体制（都道府県単位等複数自治体による情報セキュリティの強化を含む）を整備することが望ましい。

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

【趣旨】

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。

【例文】

（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、問題を認めた場合には、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、適切かつ速やかに対処しなければならない。

③統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

（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管理者に報告を行わなければならない。

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切に対処しなければならない。

（解説）

（１）遵守状況の確認及び対処

教育情報セキュリティポリシーを運用する過程において、遵守状況を確認し、違反の有無、教育情報セキュリティポリシーの問題点などを明らかにすることが求められる。確認の結果、問題があった場合には、CISOは速やかに対処する必要がある。

（注１）遵守状況の確認方法としては、自己点検等の実施、情報セキュリティインシデントの報告、日常の業務からの情報セキュリティ対策の問題事項の報告、ログ等からの異常時の発見などがある。

（２）パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

教職員等はパソコン、モバイル端末及び電磁的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CISO及びその指名した者に付与する。

（注２）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や電子メールの送受信記録等の情報を調査することをあらかじめ周知しておくことも重要である。調査が行われるかもしれないということが、不正行為に対する抑止力として効果がある。

（注３）教職員等が利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状況を調査することは、職員等のプライバシーとの関係が問題になるが、基本的には業務利用のパソコン、モバイル端末及び電磁的記録媒体等には、個人のプライバシー侵害になる記録は存在しないと考えられる。したがって、インターネット閲覧記録、電子メールの送受信記録等の調査権を確保しておくことは重要なことになる。ただし、調査は、CISO又はCISOが指名した者が行う必要がある。

（３）教職員等の報告義務

教職員等は、日々の業務で、教育情報セキュリティポリシーに違反した行為を発見した場合、その報告が求められる。統括教育情報セキュリティ責任者は、その報告を受け、情報セキュリティ上重大な影響があると判断した場合に、緊急時対応計画に沿

って適切に対処する。

2.7.3. 侵害時の対応等

【趣旨】

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、緊急時対応計画の策定について規定する。

【例文】

（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、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。

（解説）

（１）緊急時対応計画の策定

情報セキュリティが侵害された場合又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。

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。情報が漏えい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。

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。

（注１）緊急時対応計画を策定する場合は、他の危機管理に関する規程等と整合性を確保し策定する必要がある。また、他の危機管理に関する規程の改定と情報セキュリティポリシーの見直しの時期が異なることにより一時的に不整合が生じないよう、配慮する必要がある。

（注２）庁内のCSIRT が担う役割についても緊急時対応計画を策定する場合に考慮することが望ましい。

（２）緊急時対応計画に盛り込むべき内容

緊急時対応計画に定める事項としては、例えば次のものがある。

①関係者の連絡先

・地方公共団体の長
・CISO
・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
・情報セキュリティに関する統一的な窓口（庁内のCSIRT）
・情報セキュリティに関する統一的な窓口（教育委員会内のCSIRT）
・ネットワーク及び情報システムに係る外部委託事業者
・広報担当課
・都道府県の関係部局
・警察
・関係機関
・被害を受けるおそれのある個人及び法人

②発生した事案に係る報告すべき事項

セキュリティに関する事案を発見した者は、次の項目について速やかに統括教育情報セキュリティ責任者に報告しなければならない。

・事案の状況
・事案が発生した原因として、想定される行為
・確認した被害及び影響範囲（事案の種類、損害規模、復旧に要する額等）
・事案が情報セキュリティインシデントに該当するか否かの判断結果
・記録

また、統括教育情報セキュリティ責任者は、事案の詳細な調査を行うとともに、CISO及び情報セキュリティ委員会へ報告しなければならない。

（注３）統括教育情報セキュリティ責任者が事案の詳細な調査を行うに当たっては、必要に応じて外部専門家のアドバイスを受ける、JPCERT/CC（一般社団法人JPCERT コーディネーションセンター）及び地方公共団体情報システム機構（自治体CEPTOAR）等の関係機関に相談する等、事実確認を見誤らないように努める必要がある。

（注４）庁内のCSIRT に報告を集約し、窓口経由で外部への問合せや相談を行うことが考えられる。

（注５）情報共有や相談については、「地方公共団体における情報セキュリティ対策及び政府の一層の充実・強化について（依頼）」（平成23年10月11日総務省事務連絡）を参照されたい。

③発生した事案への対応措置

（ア）統括教育情報セキュリティ責任者は、次の事案が発生した場合、定められた連絡先へ連絡しなければならない。

・サイバーテロその他の市民に重大な被害が生じるおそれのあるとき
→地方公共団体の長、CISO、都道府県の関係部局、警察、影響が考えられる個人及び法人に連絡
・不正アクセスその他の犯罪と思慮されるとき
→地方公共団体の長、CISO、都道府県の関係部局、警察に連絡
・踏み台となって他者に被害を与えるおそれがあるとき
→地方公共団体の長、CISO、都道府県の関係部局、警察に連絡
・情報システムに関する被害
→教育情報システム管理者、必要と認められる事業者に連絡
・その他情報資産に係る被害
→関係部局等に連絡

（イ）統括教育情報セキュリティ責任者は、次の事案が発生し、情報資産を保護するためにネットワークを切断することがやむを得ない場合、ネットワークを切断する。

・異常なアクセスが継続しているとき又は不正アクセスが判明したとき
・システムの運用に著しい支障をきたす攻撃が継続しているとき

・コンピュータウイルス等、不正プログラムがネットワーク経由で拡がっているとき
・情報資産に係る重大な被害が想定されるとき

（ウ）教育情報システム管理者は、次の事案が発生し、情報資産の防護のために情報システムを停止することがやむを得ない場合、情報システムを停止する。
・コンピュータウイルス等、不正プログラムが情報資産に深刻な被害を及ぼしているとき
・災害等により電源を供給することが危険又は困難なとき
・そのほかの情報資産に係る重大な被害が想定されるとき

（エ）個々のパソコン等の端末のネットワークからの切断については、セキュリティポリシーにおいて特段の定めがあるものを除き、統括教育情報セキュリティ責任者の許可が必要である。

ただし、情報資産の被害の拡大を直ちに停止させる必要がある場合は、事後報告とすることができる。

（オ）事案に係るシステムのログ及び現状を保存する。

（カ）事案に対処した経過を記録する。

（キ）事案に係る証拠保全の実施を完了するとともに、暫定措置を検討する。

（ク）暫定措置を講じた後、復旧する。

（ケ）復旧後、必要と認められる期間、再発の監視を行う。

④再発防止措置の策定

（ア）統括教育情報セキュリティ責任者は、当該事案に係る調査を実施し、情報セキュリティポリシー及び実施手順の改善を含め、再発防止計画を策定し、情報セキュリティ委員会へ報告する。

（イ）情報セキュリティ委員会は、再発防止計画が有効であると認められた場合はこれを承認し、事案の概要とあわせ教職員等に周知する。

（3）業務継続計画との整合性確保

地震及び風水害等の自然災害等や大規模・広範囲にわたる疾病等の事態に備えて、情報セキュリティにとどまらない危機管理規定として業務継続計画（若しくは、ICT部門における業務継続計画）を策定することが重要である。ただし、業務継続計画と情報セキュリティポリシーの間に矛盾があると、職員等は混乱し、適切な対応をとることができなくなるおそれがあるため、各地方公共団体において業務継続計画を策定する際には、情報セキュリティポリシーとの整合性をあらかじめ検討し、必要があれば、情報セキュリティポリシーを改定しなければならない。

（注６）整合性を検討すべき事項は、例えば、施設の耐災害性対策、施設・情報システムの地理的分散、非常用電源の確保、人手による業務処理や郵送・電話の

利用を含む情報システム以外の通信手段の利用、事態発生時の対応体制及び要員計画などがある。

（注７）危機管理には、大規模又は広範囲に及ぶ疾病等によるコンピュータ施設の運用にかかる機能不全等への考慮も望まれる。

（注８）大地震を対象事態としたICT 部門における業務継続計画の策定については、「地方公共団体におけるICT 部門の業務継続計画（BCP）策定に関するガイドライン」（平成20 年8 月 総務省）及び「地方公共団体におけるICT 部門の業務継続計画（ICT-BCP）初動版サンプル」（平成25 年5 月8 日 総務省）を参照されたい。

（４）緊急時対応計画の見直し

緊急時対応計画の実効性を確保するため、新たな脅威の出現等の情報セキュリティに関する環境の変化や組織体制の変化等を盛り込んだ最新の内容となるよう、定期的に見直すことが必要である。また、緊急時対応計画の発動した場合を仮定した訓練や机上試験を定期的に実施しておくことも、緊急時対応計画の実効性を確保する観点から重要である。

2.7.4. 例外措置

【趣旨】

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。

【例文】

（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には、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。

(解説)

例外措置は、教育情報セキュリティポリシーの適用を例外的に排除するものであることから、その承認は、ポリシーの適用が著しく行政事務の遂行を妨げる、緊急を要し通常の手続きを取る時間的な猶予がない、技術的に困難であるなどの合理的な理由が必要である。なお、その場合でも、例外措置は単に適用を排除するだけでなく、リスクに応じて代替措置を定めること及び期限を設けて認めることが望ましい。

CISOは、例外措置についての手続きを定め、明示することによって、ローカルルールの氾濫や、対策の未実施を防止することができる。

(注) 例外措置の内容から判断し、教育情報セキュリティポリシーの遵守自体に無理があると判断される場合には、当該ポリシーの見直しについて検討する必要がある。

2.7.5. 法令等遵守

【趣旨】

教職員等は、全ての法令を遵守することは当然であるが、教職員等が業務を行う際の参考として、情報セキュリティに関する主要な法令を明示し、法令の遵守を確実にする。

【例文】 教職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令等を遵守し、これに従わなければならない。 ①地方公務員法(昭和25年12月13日法律第261号) ②教育公務員特例法(昭和24年1月12日法律第1号) ②著作権法(昭和45年法律第48号) ③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) ④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) ⑤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) ⑥○○市個人情報保護条例(平成○○年条例第○○号)

(解説)

情報セキュリティ対策において関連のある主要な法令について明示し、法令遵守を確実にする。また、法令への適合を確実なものにするためには、必要に応じて有識者による法的な助言を受けることが望ましい。

また、関連する最新の法令に基づき定期的に情報セキュリティポリシーの見直しを行い、最新に保つことが望ましい。

2.7.6. 懲戒処分等

【趣旨】

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。

【例文】

（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

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

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、適切な措置を求めなければならない。

②教育情報システム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は、教職員等の権利を停止あるいは剥奪した旨を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

【趣旨】

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えい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。

なお、個別の地方公共団体が単独で外部委託する場合だけでなく、共同アウトソーシングやクラウドサービス利用の形態等により地方公共団体が共同で外部委託する場合にも対策を行う必要があることに留意する。

【例文】

（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。【推奨事項】

③教育情報システム管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用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には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・教育情報セキュリティポリシー及び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、作業場所の特定
・提供されるサービスレベルの保証
・外部委託事業者にアクセスを許可する情報の種類と範囲、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。

(解説)

（１）外部委託事業者の選定基準

外部委託事業者を選定するに当たっては、情報セキュリティ上、重要な情報資産を取り扱う可能性があることから、技術的能力、信頼性等について考慮して、情報セキュリティ対策が確保されることを確認する必要がある。

また、外部委託事業者の選定にあたり、事業者の情報セキュリティ水準を評価する際には、国際規格の認証取得状況等を参考にして決定することが望ましい。

なお、外部委託事業者の選定条件として仕様等に盛り込む内容としては、例えば次のものがある。

・外部委託事業者に提供する情報の委託事業者における目的外使用の禁止
・外部委託事業者における情報セキュリティ対策の実施内容及び管理体制
・外部委託事業の実施にあたり、外部委託事業者の組織又はその従業員、再委託事業者、若しくはその他の者による意図せざる変更が加えられないための管理体制
・外部委託事業者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）
・実績及び国籍に関する情報提供
・情報セキュリティ要件の適切な実装
・情報セキュリティの観点に基づく試験の実施
・情報セキュリティインシデントへの対処方法
・情報セキュリティ対策その他の契約の履行状況の確認方法
・情報セキュリティ対策の履行が不十分な場合の対処方法

（注１）現在の最新の規格であるISO/IEC27001 については、一般財団法人日本情報経済社会推進協会のホームページ（ISMS 適合性評価制度）又は一般財団法人日本規格協会のホームページを参照されたい。

（注２）ホスティングサービスの利用等においては、サービス提供者側のミスや機器

の故障などの不測の事態によりデータの消失などの事態が発生するおそれがあるため、情報システムや取り扱う情報の重要度に応じたバックアップなどの必要な対策を講じておく必要がある。なお、ホスティング時のデータ消失に関する対策については、「ホスティングサービス等利用時におけるデータ消失事象への対策実施及び契約内容の再確認等について（注意喚起）」（平成24 年7 月6 日 総務省 事務連絡）を参照されたい。

（２）契約項目

外部委託事業者に起因する情報漏えい等の事案を防ぐため、各団体で実施する場合と同様の対策を当該委託事業者に実施させるよう必要な要件を契約等に定める必要がある。以下に示す項目について、委託する業務の内容に応じて明確に要件を規定することが必要である。

①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

外部委託事業者の要員に対して、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について、委託業務に関係する事項を遵守することを定める。

②外部委託事業者の責任者、委託内容、作業者、作業場所の特定

外部委託事業者の責任者や作業者を明確にするとともに、これらの者が変更する場合の手続きを定めておき、担当者の変更を常に把握できるようにする。また、作業場所を特定することにより、情報資産の紛失等を防止する。

③提供されるサービスレベルの保証

通信の速度及び安定性、システムの信頼性の確保等の品質を維持するために、必要に応じて、サービスレベルを保証させる。

④委託事業者に許可する情報の種類とアクセス範囲、アクセス方法

委託に関わる情報の種類を定義し、種類ごとのアクセス許可とアクセス時の情報セキュリティ要求事項、並びにアクセス方法の監視及び管理を行う。

⑤従業員に対する教育の実施

外部委託事業者において、情報セキュリティに対する意識の向上を図るために、従業員に対し教育を行うように規定しておく。

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

外部委託事業者に提供した情報について、不正な利用を防止させるために、業務以外での利用を禁止する。

⑦業務上知り得た情報の守秘義務

業務中及び業務を終了した後も、情報の漏えいを防止するために、業務上知り得た秘密を漏らしてはならない旨を規定する。

⑧再委託に関する制限事項の遵守

一般的に、再委託した場合、再委託事業者のセキュリティレベルは下がることが懸

念されるために、再委託は原則禁止する。例外的に再委託を認める場合には、再委託事業者における情報セキュリティ対策が十分取られており、外部委託事業者と同等の水準であることを確認し、外部委託事業者に担保させた上で許可しなければならない

⑨委託業務終了時の情報資産の返還、廃棄等

委託業務終了時に、不要になった情報資産を返還させるか廃棄させるか等その取扱いについて明確に規定する必要がある。委託終了後の取扱いを明確にすることにより、不要になった情報資産から情報が漏えいする可能性を減らす。

⑩委託業務の定期報告及び緊急時報告義務

定期報告及び緊急時報告の手順を定め、委託業務の状況を適切かつ速やかに確認できるようにすることが必要である。緊急時の職員への連絡先は、外部委託業者に通知しておく必要がある。連絡網には、教職員等の個人情報が記載される場合もあるため、取扱いに注意する。

⑪地方公共団体による監査、検査

外部委託事業者が実施する情報システムの運用、保守、サービス提供（クラウドサービス含む）等の状況を確認するため、当該委託事業者に監査、検査を行うことを明確に規定しておくことが必要である。

なお、地方公共団体において、当該委託事業者に監査、検査を行うことが困難な場合は、地方公共団体による監査、検査に代えて、第三者や第三者監査に類似する客観性が認められる外部委託事業者の内部監査部門による監査、検査又は国際的なセキュリティの第三者認証(ISO/IEC27001 等)の取得等によって確認する。

⑫地方公共団体による情報セキュリティインシデントの公表

委託業務に関し、情報セキュリティインシデントが発生した場合、住民に対し適切な説明責任を果たすため、当該情報キュリティインシデントの公表を必要に応じ行うことについて、外部委託事業者と確認しておく。

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)

外部委託事業者においての情報セキュリティポリシーが遵守されなかったため、被害を受けた場合には、当該委託事業者が損害賠償を行うことを契約書上明記しておく。

（注３）これらの契約項目については、「地方公共団体における業務の外部委託事業者に対する個人情報の管理に関する検討」報告書（平成21年3月 総務省）を参照し、「個人情報の取扱いに関する特記仕様書（雛型）」を活用されたい。

（注４）外部委託事業者に対して、情報セキュリティポリシーの該当部分について、十分に説明しておくことが必要である。

（注５）指定管理者制度に関する考慮事項

指定管理者制度においては、条例により、地方公共団体と指定管理者との間

で協定を締結することになるが、その協定において、委託内容に応じた情報セキュリティ対策が確保されるよう必要な事項を定める必要がある。

（注６）クラウドサービスの利用に関する考慮事項

インターネットを介してサービスを提供するクラウドサービスの利用に当たっては、クラウドサービス事業者の事業所の場所にかかわらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、クラウドサービス事業者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、データセンターの設置されている国の法令により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、個人情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で運用できるデータセンターを選択する必要がある。

なお、クラウドサービスの利用に当たっては、契約の形態が従前の委託や請負と異なることが想定されることから、「地方公共団体におけるASP・SaaS導入活用ガイドライン」（平成22 年4 月 総務省）を参照されたい。

（注７）IT サプライチェーンを構成して提供されるサービスを利用する場合は、外部委託事業者との関係におけるリスク（サービスの供給の停止、故意又は過失による不正アクセス、外部委託事業者のセキュリティ管理レベルの低下など）を考慮しそのリスクを防止するための事項について外部委託事業者と合意し、その内容を文書化しておくことが望ましい。

（注８）外部委託事業者に適用される法令としては、法律のほか、各地方公共団体の制定する個人情報保護条例も適用されることを明記しておく必要がある。

（注９）業務の内容に応じて規定する要件の詳細については、「非機能要求グレード（地方公共団体版）利用ガイド」（平成26 年3 月 地方自治情報センター）を参照されたい。

（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十分なセキュリティ対策がなされているか、定期的に確認し、必要に応じ、改善要求等の措置を取る必要がある。確認した内容は定期的に統括情報セキュリティ責任者に報告する。個人情報の漏えい等の重大なセキュリティ侵害行為が発見された場合には、速やかにCISOに報告を行う。

なお、外部委託事業者に対する監査については、本ガイドラインの「2.9.1 監査（４）外部委託事業者に対する監査」を参照されたい。

2.8.2. 約款による外部サービスの利用

【趣旨】

民間事業者が約款に基づきインターネット上で無料で提供する情報処理サービス等を利用する場合には、リスクを十分踏まえた上で利用を判断し、適切なセキュリティ対策を講じる必要がある。

【例文】

（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2B以上の情報が取扱われないように規定しなければならない。

（ア）約款によるサービスを利用してよい範囲

（イ）業務により利用する約款による外部サービス

（ウ）利用手続及び運用手順

（２）約款による外部サービスの利用における対策の実施

教職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

（解説）

（１） 約款による外部サービスの利用に係る規定の整備

有料、無料に関わらず、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は約款による外部サービスとなる。この代表例としては、以下のものがある。

・電子メール

・ファイルストレージ

・グループウェア等のクラウドサービス など

なお、電気通信サービスや郵便、運送サービス等は約款による外部サービスの適用範囲外である。

また、約款による外部サービスを利用する場合は、約款の範囲内でのサービス利用となり、特約等を個別に締結することが困難であることが多い。このため、リスクを十分踏まえた上で利用を判断し、セキュリティ対策を適切に講ずる必要がある。

具体的には次の事項が考えられる。

①約款による外部サービスの利用手順を定める

・利用申請の許可権限者の決定

・利用申請時の申請内容

－利用する組織名

－利用するサービス
－利用目的（業務内容）
－利用期間
－利用責任者（利用アカウントの責任者） など

②サービス利用中の安全管理に係る運用手順を定める
・サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認
・情報の滅失、破壊等に備えたバックアップの取得
・利用者への定期的な注意喚起
・情報セキュリティインシデント発生時の連絡体制

③当該サービスの利用において、機密性2Aの情報を取り扱う場合に当たっては、以下の規定を確認することが望ましい。
（ア）利用者が登録した情報の目的外利用及びサービス事業者以外の者への提供の禁止
（イ）サービス事業者が業務上知り得た情報の守秘義務

なお、「インターネットを介したASPサービスの利用における留意点」については、平成29年度からの文部科学省実証事業「次世代学校支援モデル構築事業」の中で整理を行い、その結果を、ガイドラインに反映する予定である。

（２）約款による外部サービスの利用における対策の実施

約款による外部サービスの利用を検討する際は、当該サービスの約款、利用規約、その他の利用条件を確認し、利用の必要性を判断した上、セキュリティ対策も適切に講ずる必要がある。具体的には次の事項が考えられる。
・サーバ装置の故障や運用手順誤りに等により、サーバ装置上の情報が滅失し復元不可能となる場合に備えてバックアップを取得する
・サービスの突然の停止に備え、予め代替サービスを確認しておく
・約款や利用規約が予告なく一方的に変更され、セキュリティ設定が変更される場合や一度記録された情報を確実に消去できない場合に備え、サービスで取り扱うことのできる情報をあらかじめ定めておく 等

（注１）グループメールサービスの業務利用においても、その設定によってはメールの内容が外部から閲覧可能な状態となり、必要なセキュリティが確保できない場合があるため利用を禁止する必要がある。やむを得ず利用する場合は、利用の要否を十分に検討の上、必要な対策を講じた上で利用する。なお、グループメールサービス利用時の注意喚起については、「グループメールサービスの利用について（注意喚起）」（平成25 年7 月11 日 総務省 事務連絡）を参照されたい。

2.8.3. ソーシャルメディアサービスの利用

【趣旨】

住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を利用することが多くなるが、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。

【例文】

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。

（ア）本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

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

②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。

(解説)

ソーシャルメディアサービスの利用

インターネット上における、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等のソーシャルメディアサービスは、積極的な広報活動等に利用することができるが、外部サービスを利用せざるを得ず、第三者によるなりすましやアカウントの乗っ取り、予告なしでサービスが停止するといった事態が発生する可能性がある。そのため、利用にあたっては、ソーシャルメディアサービスの運用ポリシーや運用手順を定め、ルールに沿った利用を行うことが求められる。具体的には次の事項が考えられる。

①なりすまし対策

・教育委員会又は学校で管理しているウェブサイト内において、利用するソーシャルメディアサービスのサービス名と当該アカウントページへのハイパーリンクを明記するページを設ける。

・運用しているソーシャルメディアサービスの自由記述欄において、庁内ウェブサイト上のページのURL を記載する。

・ソーシャルメディアサービスの提供事業者が、「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合は、これを利用する。

②アカウント乗っ取り対策

・パスワードを適切に管理する。
・二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用する。
・ソーシャルメディアサービスへのログインに利用する端末が不正アクセスや盗難されないよう、最新のセキュリティパッチや不正プログラム対策ソフトウェアの導入、端末管理等のセキュリティ対策を行う。

③サービスが終了・停止した場合の対応

・あらかじめ発信した情報のバックアップを教育委員会又は学校に保管しておく等、スムーズに別のサービスへの移行が行えるよう適切な準備をしておく。

2.9. 評価・見直し

2.9.1. 監査

【趣旨】

情報セキュリティポリシーの実施状況について、客観的に専門的見地から評価を行う監査が実施されない場合は、情報セキュリティ対策が徹底されない状態や情報セキュリティポリシーが業務に沿わない状態が続くおそれがある。このことから、監査の実施及びその方法について規定する。

監査を行う者は、十分な専門的知識を有するものでなければならない。また、適正な監査の実施の観点から、監査の対象となる情報資産に直接関係しない者であることが望ましい。また、地方公共団体内の情報セキュリティ対策の監査・報告について中立性を保証され、監査に必要な情報へのアクセス等の権限が明確に与えられる必要がある。監査作業に伴う情報の漏えいのリスクを最小限とするため、監査人等が取り扱う監査に係る情報について、漏えい、紛失等が発生しないように保管する必要がある。

【例文】

（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には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

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）外部委託事業者に対する監査

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

（５）報告

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

（６）保管

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

（７）監査結果への対応

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）情報セキュリティポリシー及び関係規程等の見直し等への活用

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

(解説)

（１）実施方法

情報セキュリティ対策状況に対して、定期的な監査だけでなく、様々な状況に対応して監査が行えることを定めておく必要がある。随時監査を行うことを明確にすることにより、情報セキュリティポリシーの違反行為に対する抑止効果も期待できる。

（２）監査を行う者の要件

内部監査、外部監査、いずれの場合も、監査人は、監査対象範囲から独立性を有し、公平な立場で客観的に評価を行うことが求められる。監査人は、監査及び情報セキュリティについて、十分な専門的知識を有する者でなければならない。

（注１）一部又は全部の監査対象範囲に対して、小規模な組織等の理由によって、独立性を維持することができない場合又は組織内に十分な専門的知識を有する者が確保できない場合は、必要な範囲に対して外部の監査人を利用することを検討することが必要である。また、職員等が自らが所属しないその他の部門に対して監査をする相互監査や近隣の自治体との相互監査も有効である。

（注２）監査人は、監査項目が実施できているか否かだけでなく適切な記録が取得

されているかについても確認する必要がある。また、監査項目が実施できていない又は適切な記録が取得されていない場合は、なぜできていないのかその原因にまで踏み込んで分析・報告できることが望ましい。

（３）監査実施計画の立案及び実施への協力

情報セキュリティ監査統括責任者は、情報セキュリティ監査を行うに当たって、監査人の権限、監査実施に関する項目及び内容を定め、これに基づいて監査実施計画を立案する。監査人は、この計画に基づき監査を実施する。なお、システムに対する監査の実施によって業務が中断される可能性があるため、計画の立案に当たっては中断のリスクを最小限に抑えるよう配慮することが必要である。また、システム監査を行うツールにより、監査人は特権的にデータ等へアクセスし得ることから、誤用・悪用を防止するための適切な管理が求められる。

（注３）情報セキュリティ監査統括責任者は、監査計画及びそれに付随するリスクを効果的かつ効率的に管理するのに必要な資質、並びに次の領域における知識及び技能を有することが望ましい。ただし、必要な資質、並びに知識及び技能を有することが困難な場合は、外部の専門家をあてて能力を補完することも考えられる。

・監査の原則、手順及び方法に関する知識
・マネジメントシステム規格及び基準文書に関する知識
・被監査部門の業務、製品及びプロセスに関する知識
・被監査部門の業務及び製品に関し、適用される法的及びその他の要求事項に関する知識
・該当する場合には、被監査部門の利害関係者に関する知識

また、情報セキュリティ監査統括責任者は、監査計画を管理するのに必要な知識及び技能を維持するために適切な専門能力の継続的開発・維持活動に積極的にかかわることが望ましい。

（注４）監査項目の例としては、庁内外において発生した情報セキュリティインシデントから学んだ対策等の遵守状況の確認や、電磁的記録媒体の管理、情報の持ち出し管理、ソフトウェアライセンス管理、FAX 誤送信防止策等の具体的な情報セキュリティ対策の運用状況の確認が挙げられる。

（４）外部委託事業者に対する監査

情報システムの運用、保守等を外部委託している場合は、情報資産の管理が契約に従い適切に実施されているかを点検、評価する必要がある。また、これによって、セキュリティ侵害行為に対する抑止効果も期待できる。

（５）報告

情報セキュリティ監査統括責任者は、監査調書をもとに、被監査部門に対する監査人の指摘事項の正確性や指摘に対する改善提案の実現性を確認し監査報告書を作成し、監査報告書を情報セキュリティ委員会に報告する。

CISOは、監査報告を受けて、被監査部門に改善を指示する。被監査部門は、改善計画を立案し実施する。最後に監査人は、フォローアップ監査により、改善状況や改善計画の完了について確認を行う必要がある。

（６）保管

監査により作成した監査調書には、脆弱性の情報等機微な情報が含まれていることが多いことから、情報セキュリティ監査統括責任者は、紛失等が生じないように保管する必要がある。

（７）監査結果への対応

監査結果を適切にセキュリティ改善に結び付けるため、CISOに関係部局への指示を義務付けた規定である。また、監査の指摘事項と同種の課題が他の部署にも存在する場合があることから、当該可能性の高い部署に対しては、課題や問題点の有無を確認させる必要がある。

（８）情報セキュリティポリシー及び関係規程の見直し等への活用

監査結果は、情報セキュリティポリシー及び関係規程の見直し等の基礎資料として活用しなければならない。

（注５）情報セキュリティ監査の実施方法等については、「地方公共団体における情報セキュリティ監査に関するガイドライン」（平成27年3月 総務省）及び「地方公共団体情報セキュリティ管理基準解説書」（平成17年2 月 総務省）を参考にされたい。

2.9.2. 自己点検

【趣旨】

情報セキュリティポリシーの履行状況等を自ら点検、評価することは、情報セキュリティポリシーの遵守事項を改めて認識できる有効な手段である。自己点検は、情報システム等を運用する者又は利用する者自らが実施するので、監査のような客観性は担保されないが、監査と同様に、点検結果を踏まえ各部門で改善を図ったり、組織全体のセキュリティ対策の改善を図る上での重要な情報になる情報セキュリティ対策の評価を行い、対策の見直しに資するものである。また、教職員等の情報セキュリティに関する意識の向上や知識の習得にも有効である。

このことから、自己点検を定期的に実施する規定を設け、その活用方法とあわせて規定する。

【例文】

（１）実施方法

①統括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

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

(解説)

（１）実施方法

情報セキュリティ対策の実施状況について、定期的な自己点検だけでなく、様々な状況に対応して自己点検を実施する。

（注１）自己点検は自己点検票を用いた、アンケート方式で行う場合が多い。アンケートを行う場合に留意すべき点は、そのセキュリティ対策上担う役割に応じたアンケート項目とすることである。アンケートは、回答者による再認識や新たな発見にもつながり得る。アンケート項目によって、自部門の対策で、何が欠落しているのか鮮明にすることが可能になるために、改善の必要性の認識をさせられる効果もある。

（注２）保有する個人情報の人的な要因による漏えいを踏まえた点検については、「地方公共団体の保有する情報資産の管理状況等の再点検について（周

知）」（平成24 年10 月29 日 総務省 総行情第71 号）及び「地方公共団体における個人情報の漏洩防止対策について（注意喚起）」（平成25 年8 月5 日 総務省 事務連絡）を参照されたい。

（注３）技術的な脆弱性の悪用に対する点検については、「地方公共団体等が管理するウェブサイトに係る脆弱性の確認及び対策の点検・実施等について（依頼）」（平成24 年9 月26 日 総務省 総行情第66 号）を参照されたい。

（２）報告

自己点検結果を情報セキュリティ委員会に報告し、団体全体における対策の状況を把握することが必要である。

（３）自己点検結果の活用

自己点検結果は、教職員等が自らの業務の見直しに活用するとともに、監査結果と同様に、情報セキュリティポリシーの見直し等の情報として活用することができる。

2.9.3. 教育情報セキュリティポリシー及び関係規程等の見直し

【趣旨】

情報セキュリティ対策は、情報セキュリティに関する脅威や技術等の変化に応じて、必要な対策が変化するものであり、教育情報セキュリティポリシー及び関係規程等は、定期的に見直すことが求められる。また監査や自己点検の結果等から、同ポリシー及び関係規程等の見直しの必要性が確認される場合もある。

このことから、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について規定する。

【例文】

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

（解説）

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、監査や自己点検の結果を受けて、情報セキュリティ分野の専門家による評価等を活用しつつ、情報セキュリティポリシー及び関係規程等の見直しを行う。

また、教育情報セキュリティポリシー及び関係規程等は、組織にとっての脅威の変化や組織体制の変更、新たな対策技術の提供等によっても見直すべきものであり、あらか

じめ定めた間隔及び重大な変化が発生した場合等、状況に応じて柔軟に運用していくことが必要である。

（注１）見直しに当たっては、教育情報セキュリティポリシー及び関係規程等と実態との相違を十分考慮することが重要であり、関係部局から意見聴取等を行い、実態把握を行うことが望ましい。また、教育情報セキュリティポリシー及び関係規程等を見直す際には、必要に応じてリスク分析の見直しを行うことが重要である。日頃から新たな攻撃方法や対策技術の情報収集に努め、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に活用することも必要である。

（注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は、地方公共団体の長及びこれに準じる者の決裁により正式に決定される。

（注３）教育情報セキュリティポリシー及び関係規程等を見直した際には、その内容を教職員等や外部委託事業者に十分に周知する必要がある。

（注４）見直しの際は、教育情報セキュリティポリシー及び関係規程等に次の事項によって生じる要求事項が含まれているか確認すること。

・事業計画
・規制、法令及び契約
・現在及び将来予想される情報セキュリティの脅威環境

【参考１】情報セキュリティ対策基準の例文

2.1. 対象範囲及び用語説明

（１）行政機関等の範囲

本対策基準が適用される行政機関等は、内部部局、教育委員会及び学校（小学校、中学校、義務教育学校、高等学校、中等教育学校、特別支援学校を言う。以下同じ。）とする。

（２）情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

①教育ネットワーク、教育情報システム、これらに関する設備、電磁的記録媒体

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

③教育情報システムの仕様書及びネットワーク図等のシステム関連文書

（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	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	校務外部接続系情報にアクセス可能な端末
学習者用端末	学習系情報にアクセス可能な端末で、児童生徒が利用する端末
指導者用端末	学習系情報にアクセス可能な端末で、教員のみが利用可能な端末

校務系システム	校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム
校務外部接続系システム	校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ（CMS)及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム
学習系システム	学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム
教育情報システム	校務系システム、校務外部接続系システム及び学習系システムを合わせた総称
校務系サーバ	校務系情報を取り扱うサーバ
校務外部接続系サーバ	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最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。【推奨事項】

（2）統括教育情報セキュリティ責任者

①教育長、副教育長又は教育委員会に所属するCIO補佐官等を、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。

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。

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、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISOの指示に従い、CISOが不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

⑥統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。

⑦統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教育委員会事務局の情報セキュリティ担当部局（情報システム課等）の課室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統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情報セキュリティに関する開発、設定の変更、運用、見直し等を行う統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、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には、教育情報セキュリティ責任者、統括教育情報セキュリティ責任者及び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教育委員会の情報システム担当課の課室長を、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教育委員会の情報システム担当課の課室職員を、教育情報システムに関する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）情報セキュリティ委員会

①本市の情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会において、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。

②情報セキュリティ委員会は、毎年度、本市における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。【推奨事項】

（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。

（9）情報セキュリティに関する統一的な窓口の設置

①CISO は、情報セキュリティインシデントの統一的な窓口の機能を有する組織を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。

②CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供する。

③情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘

案し、報道機関への通知・公表対応を行わなければならない。

④情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。

2.3. 情報資産の分類と管理方法

（1）情報資産の分類

本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、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、業務の遂行に支障ある情報
完全性 2A	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学校関係者の権利が侵害される又は学校事務及び教育活動の的確な遂行に軽微な支障を及ぼすおそれがある情報資産	情報が正確・完全な状態である必要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合、業務の遂行に軽微な支障ある情報
完全性 1	完全性 2A 又は完全性 2B の情報資産以外の情報資産	事故があった場合でも業務の遂行に支障がない情報

可用性による情報資産の分類

分類	分類基準	該当する情報のイメージ
可用性 2B	学校で取り扱う情報資産のうち、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

（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）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

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、適切な取扱いをしなければならない。

（ウ）情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

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、情報資産を適切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電磁的記録媒体を保管する場合は、書込禁止の措置を講じなければならない。

（ウ）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、利用頻度が低い電磁的記録媒体や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。【推奨事項】

（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、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

電子メールにより機密性2A以上の情報を外部送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

⑧情報資産の運搬

（ア）車両等により機密性2A以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、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）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）機密性2A以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

（イ）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、住民に公開する情報資産について、完全性を確保しなければならない。

⑩情報資産の廃棄

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

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

（ウ）情報資産の廃棄を行う者は、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、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

（２）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校務系情報を格納しているサーバを冗長化し、同一データを保持しなければならない。また、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。【推奨事項】

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。【推奨事項】

（３）機器の電源

①教育情報システム管理者は、統括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、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

②教育情報システム管理者は、統括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統括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統括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統括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切に管理しなければならない。

④統括教育情報セキュリティ責任者、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、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あたり当たり、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ほか、秘密保持体制の確認等などを行わなければならない。

（６）施設外又は学校庁外への機器の設置

統括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

(教育委員会等のサーバ室にサーバを設置している場合)

（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、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

②統括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、管理区域を地階又は1階に設けてはならない。また、外部からの侵入が容易にできないように無窓の外壁にしなければならない。【推奨事項】

③統括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、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

④統括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統括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、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。【推奨事項】

⑥統括教育情報セキュリティ責任者及び教育情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

（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。

②地方公共団体職員等及び外部委託事業者が、管理区域に入室を許可する場合、これらの者に身分証明書等を携帯させ、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には、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、機密性2Ｂ以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（３）機器等の搬入出

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。

（学校にサーバを設置している場合）

（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、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

②統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワークの基幹機器及び重要な情報システムについて、サーバラックに固定した上で、サーバラックの施錠管理を行わなければならない。

③統括教育情報セキュリティ責任者及び教育情報システム管理者は、サーバラックを、立ち入りを許可されていない不特定多数の者が出入りできる場所に設置してはならない。

④統括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、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

⑤統括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。

⑥統括教育情報セキュリティ責任者及び教育情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

（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すること。

②教育情報システム管理者は、サーバラックの施錠管理にあたり、管理簿の記載等による管理を行わなければならない。

③教職員は、児童生徒が管理区域に入室する場合、必要に応じて立ち入り区域を制限した上で、児童生徒に付き添うものとする。

④外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

⑤教育情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立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教職員等が付き添うものとし、外見上教職員等と区別できる措置を講じなければならない。

（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、教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統括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、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

②統括教育情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

③統括教育情報セキュリティ責任者は、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、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

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

⑤統括教育情報セキュリティ責任者は、可用性2Ｂ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端末や電磁的記録媒体等の管理

（校務用端末、校務外部接続用端末及び指導者用端末について）

①教育情報システム管理者は、盗難防止のため、職員室等で利用する校務用端末及び校務外部接続用端末のワイヤーによる固定、教室等で使用する指導者用端末の保管庫による管理等、使用する目的に応じた適切な物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

②教育情報システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

③教育情報システム管理者は、端末の電源起動時のパスワード（BIOSパスワード、ハードディスクパスワード等）を設定しなければならない。【推奨事項】

④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二要素認証を設定しなければならない。【推奨事項】

⑤教育情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。【推奨事項】

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。【推奨事項】

（学習者用端末について）

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。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。

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外部における情報処理作業の制限

(ア) CISO は、機密性 2B 以上、可用性 2B 以上、完全性 2B 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、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、モバイル端末及び電磁的記録媒体等を用いる場合には、教育情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

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。

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、適切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。

（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等の制限

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）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、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、教職員等は、毎年度最低1回は情報セキュリティ研修を受講できるようにしなければならない。【推奨事項】

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、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及び教育情報セキュリティ責任者に報告しなければならない。

（2）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、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、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に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。
④CISOは、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るための窓口を設置し、当該窓口への連絡手段を公表しなければならない。【推奨事項】

（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統括教育情報セキュリティ責任者は、情報セキュリティインシデントについて、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に報告しなければならない。
②CISOは、統括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若しくはパソコン等の端末のスロット等から抜いておかなければならない。
(ウ) IC カード等を紛失した場合には、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に通報し、指示に従わなければならない。
②統括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統括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）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は一切応じてはならない。

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

④パスワードが流出したおそれがある場合には、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、古いパスワードを再利用してはならない。

⑥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。

⑦仮のパスワードは、最初のログイン時点で変更しなければならない。

⑧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。

⑨教職員等間でパスワードを共有してはならない。

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）文書サーバ及び端末の設定等

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、機微な個人情報を保管する場合に限る）については、標的型攻撃等によるファイルの外部流出の可能性を考慮し、ファイル暗号化等による安全管理措置を講じなければならない。

（2）バックアップの実施

統括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。【推奨事項】

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

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

統括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、適切に管理しなければならない。

（6）ログの取得等

①統括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統括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統括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

統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

（８）ネットワークの接続制御、経路制御等

①統括教育情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。
②統括教育情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

（９）外部の者が利用できるシステムの分離等

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

（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には、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統括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想定される場合には、統括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）ネットワークの分離

①教育情報システム管理者は、校務系システム及び学習系システム間の通信経路の物理的又は論理的な分離をするとともに、校務系システム及び校務外部接続系システム間の通信経路を物理的又は論理的に分離し、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。

②教育情報システム管理者は、校務系システムと校務外部接続系システム及び学習系システム間で通信する場合には、ウイルス感染のない無害化通信など、適切な措置を図らなければならない。

（１２）複合機のセキュリティ管理

①統括教育情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

②統括教育情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③統括教育情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

（１３）特定用途機器のセキュリティ管理

統括教育情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施しなければならない。

（１４）無線LAN及びネットワークの盗聴対策

①統括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統括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統括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統括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統括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統括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統括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、外部委託事業者との間で利用方法を取り決めなければならない。

⑥統括教育情報セキュリティ責任者は、教職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置しなければならない。【推奨事項】

（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フリーメールサービス等を統括教育情報セキュリティ責任者の許可無しに使用してはならない。

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

2.6.2. アクセス制御

（1）アクセス制御等

①アクセス制御

統括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。

②利用者IDの取扱い

（ア）統括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、統括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）統括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） 統括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） 統括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、統括教育情報セキュリティ責任者及び教育情報システム管理者が指名し、CISO が認めた者でなければならない。

（ウ） CISOは、代行者を認めた場合、速やかに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及び教育情報システム管理者に通知しなければならない。

（エ） 統括教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与されたID及びパスワードの変更について、外部委託事業者に行わせてはならない。

（オ） 統括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、その他利用者よりもパスワードの有効期限を短くしたり、入力回数制限を設ける等のセキュリティ機能を強化しなければならない。

（カ） 統括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。

（キ） 統括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のログ監視を行わなければならない。【推奨事項】

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

④統括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統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部からのアクセスに利用するモバイル端末を教職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

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

⑦統括教育情報セキュリティ責任者は、公衆通信回線（公衆無線LAN等）を教育ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のID及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ICカード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

（3）自動識別の設定

統括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、ネットワークで使用される機器について、機器固有情報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。【推奨事項】

（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統括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統括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統括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統括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ければならならない。

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。【推奨事項】

（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、あらかじめ擬似環境による操作確認を行わなければならない。

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

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

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

（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を適切な方法で保管しなければならない。

（５）情報システムにおける入出力データの正確性の確保

①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を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

（8）システム更新又は統合時の検証等

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）統括教育情報セキュリティ責任者の措置事項

統括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教育情報システム管理者は、その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システムに常駐させなければなら

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。

（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統括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

統括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）統括教育情報セキュリティ責任者の措置事項

統括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、統括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。【推奨事項】

⑤統括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切な対応などを実施できる体制並びに連絡網を構築しなければならない。

（2）攻撃の予告

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ることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

（3）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。

（4）内部からの攻撃

統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等及び外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（5）教職員等による不正アクセス

統括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、適切な処置を求めなければならない。

（6）サービス不能攻撃

統括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

統括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

統括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及び周知

統括教育情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、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

統括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統括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統括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統括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、機密性2B以上、完全性2B以上、可用性2B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統括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、機密性2A、完全性2A、可用性2A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。【推奨事項】

2.7.2. 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、問題を認めた場合には、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、適切かつ速やかに対処しなければならない。

③統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

（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管理者に報告を行わなければならない。

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切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、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・広範囲に及ぶわたる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には、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。

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12月13日法律第261号)

②教育公務員特例法（昭和24年1月12日法律第1号）
③著作権法（昭和45年法律第48号）
④不正アクセス行為の禁止等に関する法律（平成11年法律第128号）
⑤個人情報の保護に関する法律（平成15年5月30日法律第57号）
⑥行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27 号）
⑦○○市個人情報保護条例（平成○○年条例第○○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、地方公務員法による懲戒処分の対象とする。

（2）違反時の対応

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

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、適切な措置を求めなければならない。

②教育情報システム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は、教職員等の権利を停止あるいは剥奪した旨を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。【推奨事項】

③教育情報システム管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用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には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・教育情報セキュリティポリシー及び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、作業場所の特定
・提供されるサービスレベルの保証
・外部委託事業者にアクセスを許可する情報の種類と範囲、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2B以上の情報が取扱われないように規定しなければならない。

（ア）約款によるサービスを利用してよい範囲
（イ）業務により利用する約款による外部サービス
（ウ）利用手続及び運用手順

（2）約款による外部サービスの利用における対策の実施

教職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

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。

（ア）本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

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

②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。

2.9. 評価・見直し

2.9.1. 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には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

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）外部委託事業者に対する監査

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

（5）報告

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

（6）保管

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

（7）監査結果への対応

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）情報セキュリティポリシー及び関係規程等の見直し等への活用

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

2.9.2. 自己点検

（1）実施方法

①統括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

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及び教育情報セキュリテ

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

2.9.3. 教育情報セキュリティポリシー及び関係規程等の見直し

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

【参考２】　権限・責任等一覧表

※本一覧表は「第３章　情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分（対策基準の例文の規定箇所）				項　目	最高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	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	教職員等	情報セキュリティ監査統括責任者	情報セキュリティ委員会	統一的な窓口	外部委託関係規定
2．1 対象範囲				適用される行政機関の定義											
2．2 組織体制	(1)	①		最高情報セキュリティ責任者の設置	○										
		②		最高情報セキュリティアドバイザーの設置	○										
	(2)	①		統括教育情報セキュリティ責任者の設置	△	○									
		②		教育ネットワークにおける開発等の権限及び責任		○									
		③		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		○									
		④		教育情報セキュリティ責任者等に対する指導及び助言		○	△	△	△	△					
		⑤		情報資産に対するセキュリティ侵害が発生した場合等の権限及び責任	△	○									
		⑥		情報セキュリティ実施手順の維持・管理の権限及び責任		○									
		⑦		最高情報セキュリティ責任者との連絡体制の整備	△	○	△	△	△	△					
		⑧		緊急時の報告と回復のための対策	△	○									
	(3)	①		教育情報セキュリティ責任者の設置			○								
		②		教育情報セキュリティ対策に関する統括的な権限及び責任			○								
		③		教育情報システムにおける開発等を行う統括的な権限及び責任			○								
		④		教育情報システムにおける連絡体制の整備等			○								
	(4)	①		教育情報セキュリティ管理者の設置				○							
		②		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				○							
		③		情報資産に対するセキュリティ侵害が発生した場合の報告等	△	△	△	○							
	(5)	①		教育情報システム管理者の設置					○						
		②		教育情報システムにおける開発等を行う権限及び責任					○						
		③		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					○						
		④		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					○						
	(6)			教育情報システム担当者の設置					△	○					
	(7)	①		情報セキュリティ委員会の設置									○		
		②		情報セキュリティ対策の改善計画を策定、実施状況の確認									○		
	(8)	①		情報セキュリティ対策の実施における承認等の申請者とその承認者等の兼務の禁止											
		②		監査を受ける者と監査を実施する者の兼務の禁止											
	(9)	①		情報セキュリティに関する統一的な窓口の設置	○										
		②		セキュリティ戦略の意思決定が行われた際に、内容を関係部局等に提供	△	△	△	△	△					○	
		③		情報セキュリティインシデントの報道機関への通知・公表等										○	
		④		情報セキュリティに関する他の関係機関や窓口等との情報共有										○	
2．3 情報資産の分類と管理方法	(1)			情報資産の分類											
	(2)	①	(ア)	情報資産の管理責任				○							
			(イ)	複製等された情報資産の管理責任				○							
		②		情報資産の分類の表示							○				
		③	(ア)	業務上必要のない情報の作成の禁止							○				
			(イ)	情報作成時の情報の分類と取扱制限の設定							○				
			(ウ)	作成途上の情報の取扱							○				
		④	(ア)	学校内の者が作成した情報資産の取扱							○				
			(イ)	学校外の者が作成した情報資産の分類と取扱							○				
			(ウ)	分類が不明な情報資産を入手した際の対応				△			○				
		⑤	(ア)	情報資産の業務外目的の利用の禁止							○				
			(イ)	情報資産の分類に応じた適切な取扱							○				
			(ウ)	情報資産の分類が異なる電磁的記録媒体の取扱							○				
		⑥	(ア)	情報資産の分類に応じた適切な保管				○	○						
			(イ)	長期保管する情報資産を記録した電磁的記録媒体の保管				○	○						
			(ウ)	利用頻度の低い電磁的記録媒体等の保管				○	○						
			(エ)	電磁的記録媒体の施錠可能な場所への保管				○	○						
		⑦		電子メール等での送信時の対策											
		⑧	(ア)	車両等での情報資産運搬時の対策							○				
			(イ)	情報資産運搬の許可				許			○				
		⑨	(ア)	情報資産の外部への提供時の対策							○				
			(イ)	情報資産の外部への提供の許可				許			○				
			(ウ)	住民に公開する情報資産の取扱				○	○						
		⑩	(ア)	情報資産廃棄時の対策							○				
			(イ)	情報資産廃棄時の処理の記録							○				
			(ウ)	情報資産廃棄の許可				許			○				

権限・責任等一覧表

※本一覧表は「第３章　情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分（対策基準の例文の規定箇所）				項　目	最高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	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	教職員等	情報セキュリティ監査統括責任者	情報セキュリティ委員会	統一的な窓口	外部委託関係規定
2．4 物理的セキュリティ対策	2．4．1 サーバ等の管理	(1)		サーバ等取付け時の必要な措置					○						
		(2)	①	校務系サーバの冗長化					○						
			②	学習系サーバのハードディスクの冗長化					○						
			③	システム運用停止時間の最小化					○						
		(3)	①	予備電源の設置		△			○						
			②	過電流に対する機器の保護措置		△			○						
		(4)	①	通信ケーブル等の損傷防止措置		○			○						
			②	通信ケーブル等の損傷等時の対応		○			○						
			③	ネットワーク接続口の管理		○			○						
			④	配線の変更・追加の防止措置		○			○	△					
		(5)	①	機器の定期保守の実施					○						
			②	修理時における外部事業者からの情報漏えい防止措置					○						△
		(6)		施設外又は学校外への機器の設置	承	○			○						
		(7)		機器の廃棄等の措置					○						
	2．4．2 管理区域（情報システム室等）の管理	（教育委員会等のサーバ室にサーバを設置している場合）													
		(1)	①	管理区域の定義		○			○						
			②	管理区域の構造		○			○						
			③	管理区域への立入制限等		○			○						
			④	耐震対策等の対策		○			○						
			⑤	外壁等の床下開口部における措置		○			○						
			⑥	消火薬剤等の設置方法		○			○						
		(2)	①	入退室管理方法					○		○				○
			②	入室時の身分証明書等の携帯及び提示							○				○
			③	外部からの訪問者に対する入室管理					○		△				
			④	情報システムに関連しないコンピュータ等の持ち込み禁止					○						
		(3)	①	搬入する機器の既存情報システムへの影響確認					○		△				△
			②	機器等の搬入時の職員の立ち会い					○		△				
		（学校にサーバを設置している場合）													
		(1)	①	管理区域の定義		○			○						
			②	サーバラックの施錠対策		○			○						
			③	管理区域への立入制限等		○			○						
			④	許可されていない者の立ち入り防止対策		○			○						
			⑤	転倒及び落下防止等の措置		○			○						
			⑥	消火薬剤等の設置方法		○			○						
		(2)	①	入退室管理方法					○		○				○
			②	サーバラックの施錠管理							○				○
			③	立ち入り区域の制限等					○		△				
			④	外部委託事業者の管理区域への入室管理					○						
			⑤	外部からの訪問者に対する入室管理					○						
		(3)	①	搬入する機器の既存情報システムへの影響確認					○		△				△
			②	機器等の搬入時の教職員の立ち会い					○		△				
	2．4．3 通信回線及び通信回線装置の管理	①		庁内の通信回線等の適切な管理等		○			○						
		②		外部へのネットワーク接続の限定措置		○			○						
		③		機密性2A以上の情報を扱う通信回線の適切な選択		○			○						
		④		回線の十分なセキュリティ対策の実施		○			○						
		⑤		可用性2B以上の情報を扱う通信回線の可用性の確保		○			○						
	2．4．4 教職員等の利用する端末や電磁的記録媒体等の管理	（校務用端末、校務外部接続系端末及び指導者用端末について）													
		①		パソコン、モバイル端末等の盗難防止措置					○						
		②		情報システムへのログインパスワードの設定					○						
		③		端末の電源起動時のパスワード設定等措置					○						
		④		二要素認証の併用措置					○						
		⑤		パソコン、モバイル端末等におけるデータの暗号化等の利用					○						
		⑥		モバイル端末に対する遠隔消去機能の利用					○						
		（学習者用端末について）													
		①		パソコン、モバイル端末等の盗難防止措置					○						
		②		情報システムへのログインパスワードの設定					○						

権限・責任等一覧表

※本一覧表は「第３章　情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分（対策基準の例文の規定箇所）					項　目	最高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	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	教職員等	情報セキュリティ監査統括責任者	情報セキュリティ委員会	統一的な窓口	外部委託関係規定
2.5 人的セキュリティ対策	2.5.1 教職員等の遵守事項	(1)	①		情報セキュリティポリシー等の遵守				△			○				
			②		情報資産の業務目的以外での使用の禁止							○				
			③	(ア)	情報資産の外部での処理時の安全管理措置	○										
				(イ)	モバイル端末や電磁的記録媒体等の持ち出しの許可				許			○				
				(ウ)	外部での情報処理業務の許可				許			○				
			④	(ア)	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禁止				許			○				
				(イ)	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安全管理措置				許			○				
			⑤		端末等の持出及び持込の記録等				○							
			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				許			○				
			⑦		机上の端末等の管理				許			○				
			⑧		退職時等の遵守事項							○				
		(2)	①		非常勤職員等の教育情報セキュリティポリシー等の遵守				○			△				
			②		非常勤職員等の採用時の同意書への署名				○			△				
			③		インターネット接続等の利用の制限				○			△				
		(3)			情報セキュリティポリシー等の掲示				○			△				
		(4)			外部委託事業者に対する説明				○							△
	2.5.2 研修・訓練	(1)			情報セキュリティに関する研修・訓練の実施	○										
		(2)	①		研修計画の策定等	○								承		
			②		情報セキュリティ研修の受講							○				
			③		新規採用の職員等に対する研修の設定	○						△				
			④		理解度等に応じた研修の実施	○	△	△	△	△	△	△				
			⑤		研修の受講状況の報告	○								△		
		(3)			緊急時対応訓練の実施	○										
		(4)			研修・訓練の参加義務									○		
	2.5.3 情報セキュリティインシデントの報告	(1)	①		情報セキュリティインシデントの報告				△			○				
			②		情報システムに関連する情報セキュリティインシデントの報告		△		○	△					△	
			③		情報セキュリティインシデントの必要に応じた報告	△		△	○							
		(2)	①		住民等外部からの報告時の対応				△			○				
			②		情報システム又はネットワークに関連する情報セキュリティインシデントの報告		△		○	△						
			③		情報セキュリティインシデントの必要に応じた報告	△		△	○							
			④		住民等外部に対する窓口の設置等	○										
		(3)	①		情報セキュリティインシデント原因の究明、再発防止策の報告	△	○		△	△					△	
			②		再発防止策に必要な措置の指示	○										
	2.5.4 ID 及びパスワード等の管理	(1)	①	(ア)	認証に用いるICカード等の職員等間共有の禁止							○				
				(イ)	ICカード等のカードリーダへの常時挿入禁止							○				
				(ウ)	ICカード等紛失時の通報		△			△		○				
			②		ICカード紛失時のアクセス停止措置		○			○						
			③		Cカード切り替え時の旧カードの廃棄方法		○			○						
		(2)	①		自己のIDの他人による利用の禁止							○				
			②		共用ID利用者以外による共用ID利用禁止							○				
		(3)	①		パスワードの管理							○				
			②		パスワードの秘密保持							○				
			③		パスワードの文字の選択							○				
			④		パスワードの流出したおそれのある時の措置				△			○				
			⑤		パスワードの定期的な更新							○				
			⑥		パスワードのシステム間の共有禁止							○				
			⑦		仮パスワードの変更							○				
			⑧		パスワードの記憶機能の利用禁止							○				
			⑨		職員等間でのパスワード共有禁止							○				

権限・責任等一覧表

※本一覧表は「第３章　情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分（対策基準の例文の規定箇所）				項　目	最高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	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	教職員等	情報セキュリティ監査統括責任者	情報セキュリティ委員会	統一的な窓口	外部委託関係規定
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)	①	文書サーバの容量の設定等					○						
			②	文書サーバの学校等単位での設定					○						
			③	特定の情報のためのディレクトリ設定					○						
			④	インターネット接続環境の機微な個人情報のファイル暗号化等					○						
		(2)	①	校務系情報及び校務外部接続系情報のバックアップの実施		○			○						
			②	学習系情報のバックアップの扱い		○			○						
		(3)		他団体との情報システムに関する情報等の交換の許可等		許	許		○						
		(4)	①	情報システムの運用に係る作業記録の作成					○						
			②	システム変更等時の作業内容記録作成等		○			○						
			③	システム変更の作業方法		○			○	○					○
		(5)		ネットワーク構成図等の保管		○			○						
		(6)	①	ログの取得等		○			○						
			②	ログの管理		○			○						
			③	ログの点検・分析		○			○						
		(7)		システム障害等の記録、保存		○			○						
		(8)	①	通信ソフトウェア等の設定情報の管理		○									
			②	ネットワークのアクセス制御		○									
		(9)		外部の者が利用できるシステムの分離等					○						
		(10)	①	ネットワークの外部接続の許可	許	許			○						
			②	外部ネットワークの接続による影響確認					○						
			③	外部ネットワーク管理責任者による損害賠償責任の契約上の担保					○						
			④	ファイアウォール等の設置		○			○						
			⑤	問題発生時の物理的な遮断		△			○						
		(11)	①	校務系システム及び学習系システム間の通信経路の分離等					○						
			②	校務系システムと校務外部接続系システム及び学習系システム間で通信する場合の無害化					○						
		(12)	①	複合機を調達する場合のセキュリティ要件の策定		○									
			②	複合機に対するセキュリティ設定と情報セキュリティインシデント対策の実施		○									
			③	複合機の運用終了時の対策		○									
		(13)	①	特定用途機器に対する対策の実施		○									
		(14)	①	無線LAN利用時の暗号化等の使用義務設定		○									
			②	機密性の高いネットワークへの暗号化等の措置		○									
		(15)	①	電子メールの中継処理禁止の設定		○									
			②	スパムメール等を検知した際のサーバ運用停止		○									
			③	電子メールの送受信容量の上限設定等		○									
			④	電子メールボックスの容量の上限設定等		○									
			⑤	外部委託事業者の電子メールアドレス利用取り決め		○									○
			⑥	添付ファイルの監視等		○									
		(16)	①	自動転送機能の禁止							○				
			②	業務上必要のない送信先への送信禁止							○				
			③	複数人に電子メールを送信する際の方法							○				
			④	重要メールの誤送信時の報告				△			○				
			⑤	ウェブ上のフリーメール等の使用禁止							○				
		(17)	①	電子署名、暗号化等による送信	○						○				
			②	暗号化の方法及び鍵の管理	○						○				
			③	電子署名の正当性を確認する手段の提供	○										
		(18)	①	ソフトウェアの無断導入の禁止							○				
			②	ソフトウェアの導入の許可の取得		許			許		○				
			③	不正コピーしたソフトウェアの利用禁止							○				
		(19)	①	機器の改造及び増設・交換の禁止							○				
			②	機器の改造等の許可		許			許		○				
		(20)		無許可でのネットワーク接続の禁止		許					○				
		(21)	①	業務目的外のウェブ閲覧の禁止							○				
			②	業務目的外のウェブ閲覧発見時の対応		○		△							

権限・責任等一覧表

※本一覧表は「第３章　情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分（対策基準の例文の規定箇所）					項　目	最高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	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	教職員等	情報セキュリティ監査統括責任者	情報セキュリティ委員会	統一的な窓口	外部委託関係規定
2．6 技術的セキュリティ	2．6．2 アクセス制御	(1)	①		アクセス制御		○			○						
			②	(ア)	利用者の情報管理やIDの取扱い等の設定		○			○						
				(イ)	利用者登録抹消の申請		△			△		○				
				(ウ)	利用されるIDの点検		○			○						
			③	(ア)	ID及びパスワードの管理		○			○						
				(イ)	統括情報セキュリティ責任者等の特権を代行する者の要件	○	○			○						
				(ウ)	特権代行者の通知	○	△	△	△	△						
				(エ)	特権付与されたID等の変更の外部事業者への委託禁止		○			○						○
				(オ)	特権付与されたID等のセキュリティ機能強化		○			○						
				(カ)	特権付与されたIDの初期設定以外のものへの変更		○			○						
		(2)	①		外部から内部ネットワーク等へのアクセスの許可		許			許		○				
			②		外部からのアクセス可能人数の制限		○									
			③		外部からのアクセス時の本人確認の機能の確保		○									
			④		外部からのアクセス時の暗号化等の措置		○									
			⑤		外部アクセス用端末等付与時のセキュリティの確保		○			○						
			⑥		外部から持ち込んだ端末等のウイルスの確認等							○				
			⑦		公衆通信回線等の庁内ネットワークへの接続禁止		○									
		(3)			自動識別の設定		○			○						
		(4)			ログイン時のシステム設定					○						
		(5)	①		職員等のパスワード情報の管理等		○			○						
			②		パスワード発行等		○			○						
		(6)			特権によるネットワーク等への接続時間の制限					○						
	2．6．3 システム開発、導入、保守等	(1)	①		調達仕様書への技術的なセキュリティ機能の明記		○			○						
			②		調達時のセキュリティ機能の調査等		○			○						
		(2)	①		システム開発の責任者及び作業者の特定と規則の確立					○						
			②	(ア)	システム開発の責任者等のIDの管理等					○						
				(イ)	システム開発の責任者等のアクセス権限の設定					○						
			③	(ア)	システム開発におけるソフトウェア等の特定					○						
				(イ)	認定外のソフトウェアの削除					○						
		(3)	①	(ア)	システム開発等環境とシステム運用環境の分離					○						
				(イ)	システム開発環境からシステム運用環境への移行の手順の明確化					○						
				(ウ)	移行に伴うシステム停止等の影響の最小化					○						
				(エ)	導入されるシステムやサービスの可用性の確保確認					○						
			②	(ア)	新たなシステム導入前の十分な試験の実施					○						
				(イ)	運用テスト時の擬似環境による操作確認の実施					○						
				(ウ)	テストデータとして個人情報等の使用禁止					○						
				(エ)	受け入れ時の別々の組織でのテストの実施					○						
		(4)	①		システム開発等の資料等の整備・保管					○						
			②		テスト結果の保管					○						
			③		情報システムに係るソースコードの保管					○						
		(5)	①		入力データの正確性を確保できる情報システム設計					○						
			②		情報の改ざん等を検出する情報システム設計					○						
			③		出力データの正確性を確保できる情報システム設計					○						
		(6)			プログラム仕様書等の変更履歴の作成					○						
		(7)			ソフトウェア更新等時の他の情報システムとの整合性確認					○						
		(8)			システム更新又は統合時の検証等の実施					○						

権限・責任等一覧表

※本一覧表は「第３章　情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分（対策基準の例文の規定箇所）					項　目	最高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	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	教職員等	情報セキュリティ監査統括責任者	情報セキュリティ委員会	統一的な窓口	外部委託関係規定
2．6 技術的セキュリティ	2．6．4 不正プログラム対策	(1)	①		不正プログラムのシステムへの侵入防止措置		○									
			②		不正プログラムの外部への拡散防止措置		○									
			③		不正プログラム情報の収集、職員等への注意喚起		○									
			④		不正プログラム対策ソフトウェアの常駐		○									
			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の更新		○									
			⑥		不正プログラム対策ソフトウェアの更新		○									
			⑦		サポート終了ソフトウェアの使用禁止		○									
		(2)	①		不正プログラム対策ソフトウェアの常駐					○						
			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の更新					○						
			③		不正プログラム対策ソフトウェアの更新					○						
			④		インターネットに接続していないシステムにおける電磁的記録媒体の制限及び不正プログラム対策ソフトウェアの導入等					○						
		(3)	①		不正プログラム対策ソフトウェアの設定変更の禁止							○				
			②		外部からのデータ取込時のウイルスチェックの実施							○				
			③		差出人が不明等のファイルの削除							○				
			④		不正プログラム対策ソフトウェアによる定期的なフルチェックの実施							○				
			⑤		添付ファイル送受信時のウイルスチェックの実施							○				
			⑥		ウイルス情報の確認		△					○				
			⑦	(ア)	パソコン等の端末のウイルス感染時の対処方法							○				
				(イ)	モバイル端末のウイルス感染時の対処方法							○				
		(4)			外部の専門家の支援体制の整備		○									
	2．6．5 不正アクセス対策	(1)	①		使用されていないポートの閉鎖		○									
			②		不要なサービス機能の削除、停止		○									
			③		ウェブページの改ざんを防止するための設定		○			△						
			④		定期的なファイルの改ざんの有無の検査		○									
			⑤		監視、通知、外部連絡窓口などの体制及び連絡窓口の構築		○								○	
		(2)			攻撃の予告時の対応	○	○									
		(3)			攻撃を受けた時の対応	○	○									
		(4)			内部からの攻撃等の監視		○			○						
		(5)			職員等による不正アクセス時の対応		○		△	○						
		(6)			サービス不能攻撃対策の実施		○			○						
		(7)			標的型攻撃対策の実施		○			○						
	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・共有及びソフトウェアの更新等		○			○						
		(2)			不正プログラム等のセキュリティ情報の収集・周知		○									
		(3)			情報セキュリティに関する技術情報の収集及び共有		○			○						

権限・責任等一覧表

※本一覧表は「第３章　情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分（対策基準の例文の規定箇所）					項　目	最高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	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	教職員等	情報セキュリティ監査統括責任者	情報セキュリティ委員会	統一的な窓口	外部委託関係規定
2．7 運用	2．7．1 情報システムの監視		①		情報システムの監視		○			○						
			②		サーバの正確な時刻設定等の措置		○			○						
			③		機微な校務系システムの監視		○			○						
			④		学習系システムの監視		○			○						
	2．7．2 情報セキュリティポリシーの遵守状況の確認	(1)	①		情報セキュリティポリシーの遵守状況の確認等	△	△	○	○							
			②		問題発生時の対処	○										
			③		システム設定等における情報セキュリティポリシー遵守状況の確認等		○			○						
		(2)			モバイル端末及び電磁的記録媒体等の利用状況調査	○										
		(3)	①		違反行為の発見時の報告		△			△		○				
			②		緊急時対応計画に従った対応		○									
	2．7．3 侵害時の対応等	(1)			緊急時対応計画の策定	○								○		
		(2)			緊急時対応計画に盛り込むべき内容	○								○		
		(3)			業務継続計画と情報セキュリティポリシーの整合性の確保	○										
		(4)			緊急時対応計画の見直し	○								○		
	2．7．4 例外措置	(1)			例外措置の許可	許			○							
		(2)			緊急時の例外措置	△			○							
		(3)			例外措置の申請書の管理	○										
	2．7．5 法令遵守				主要な法令遵守								○			
	2．7．6 懲戒処分等	(1)			懲戒処分		○	○	○	○	○	○	○			
		(2)	①		違反時の対応（統括情報セキュリティ責任者確認時）		○		△							
			②		違反時の対応（情報システム管理者確認時）		△		△	○						
			③		違反を改善しない職員等のシステム使用の権利の停止等	△	○			△						
2．8 外部サービスの利用	2．8．1 外部委託	(1)	①		外部委託事業者の選定時の確認事項					○						
			②		国際規格の認証取得状況等を参考にした事業者の選定					○						
			③		クラウドサービス利用時の機密性に応じたセキュリティレベルの確認					○						
		(2)			契約項目											○
		(3)			外部委託事業者のセキュリティ確保の確認等	△	△			○						○
	2．8．2 約款による外部サービスの利用	(1)	①	(ア)	約款によるサービスを利用可能な範囲の規定					○						
				(イ)	業務により利用できる約款によるサービスの範囲の規定					○						
				(ウ)	約款によるサービスの利用手続及び運用手順の規定					○						
		(2)	①		約款によるサービスの利用における対策の実施							○				
	2．8．3 ソーシャルメディアサービスの利用	①		(ア)	なりすまし対策の実施					○						
				(イ)	不正アクセス対策の実施					○						
		②			機密性2以上の情報の発信禁止					○						
		③			利用するソーシャルメディアサービスごとの責任者の決定					○						
2．9 評価・見直し	2．9．1 監査	(1)			情報セキュリティ対策状況について監査の実施	○							△			
		(2)	①		被監査部門から独立した者への監査の実施依頼								○			
			②		監査を行う者の要件								○			
		(3)	①		監査実施計画の立案等								○	承		
			②		監査の実施に対する協力				○	○	○					
		(4)			外部委託事業者に対する監査								○			○
		(5)			監査結果の報告								○	△		
		(6)			監査証拠等の保管								○			
		(7)			監査結果への対応	○			△							
		(8)			監査結果の情報セキュリティポリシー及び関係規程等の見直し等への活用									○		
	2．9．2 自己点検	(1)	①		ネットワーク等の自己点検の実施		○			○						
			②		情報セキュリティ対策状況の自己点検			○	○							
		(2)			点検結果と改善策の報告		○	○		○				△		
		(3)	①		自己の権限の範囲内での改善							○				
			②		点検結果の情報セキュリティポリシー及び関係規程等の見直し等への活用									○		
	2．9．3 教育情報セキュリティポリシー及び関係規程等の見直				情報セキュリティポリシー及び関係規程等の見直しに関する規定									○		

教育情報セキュリティ対策推進チーム

平成２８年９月７日
生涯学習政策局長決定

１．趣旨

校務の情報化を進めることは、教職員が学校運営や学級経営に必要な情報や児童生徒の状況等を一元管理・共有することを可能とし、打ち合わせ時間の縮減はもとより、学校運営や学級運営の改善を含め、教育の質を高めることにつながることが期待されている。

このため、今後、統合型校務支援システムの普及をはじめとした校務の情報化を進めていく必要があるが、その際、校務情報には、児童生徒の成績情報や生徒指導関連情報等の多くの個人情報が含まれており、個人情報への不正アクセス被害も生じていることを踏まえると、万全な情報セキュリティ対策を講じておくことが極めて重要である。

現在、校務文書に関する業務等の何らかの情報を電子化している学校数は約８割におよび、そのうち約５割は、統合型校務支援システムを導入しているところであり、情報セキュリティについては、それぞれの教育委員会及び学校において対策が講じられているところであるが、今後、国として学校における情報セキュリティの考え方を整理することにより、各教育委員会・学校が教育の情報化を進めるための基盤的な環境を整えていく必要がある。

このため、「『2020年代に向けた教育の情報化に向けた懇談会』最終まとめ」等も踏まえ、教育版の情報セキュリティポリシーのガイドラインの策定に向けた検討を行うとともに、教育委員会・学校における情報セキュリティ対策について助言等を行うことを目的として、「教育情報セキュリティ対策推進チーム」（以下、「対策推進チーム」という。）を設置する。

２．主な懇談事項

（１）教育版の情報セキュリティポリシーのガイドラインの策定に向けた検討
（２）教育委員会・学校における情報セキュリティに関する助言
（３）教育情報システムに関するインシデントの検証

３．実施方法

（１）対策推進チームの委員は別紙のとおりとする。

（２）生涯学習政策局長が必要と認めるときは、別紙の委員に加えて、他の有識者等の参画を求めることができる。

（３）前各項に定めるもののほか、対策推進チームの運営に関する事項その他必要な事項は、生涯学習政策局長が定める。

（４）会議は、原則として公開とする。ただし、主査が非公開とすることが適当と認める場合には、その一部又は全部を非公開とすることができる。

（５）会議資料は、原則として公開とする。ただし、主査が非公開とすることが適当と認める場合には、その一部又は全部を非公開とすることができる。

（６）本会議の議事要旨を作成し、公開するものとする。

４．その他

（１）対策推進チームの構成員は、職務上知り得た秘密を漏らしてはならない。また、その職を退いた後も同様とする。

（２）対策推進チームの庶務は、初等中等教育局参事官付（学校運営支援担当）その他関係局課の協力を得て生涯学習政策局情報教育課において処理する。また、検討にあたっての技術的な観点その他必要な事項については、大臣官房政策課の協力を得るものとする。

別紙

教育情報セキュリティ対策推進チーム　委員

	岩﨑　進	文部科学省　最高情報セキュリティアドバイザー
	岡村　久道	弁護士/ 京都大学大学院医学研究科講師（非常勤）
	加藤　剛史	静岡県立浜松大平台高等学校教頭
	後藤　厚宏	情報セキュリティ大学院大学学長
	宍戸　常寿	東京大学大学院法学政治学研究科教授
	新保　元康	札幌市立屯田小学校校長
	高倉　弘喜	国立情報学研究所アーキテクチャ科学研究系教授
○	高橋　邦夫	豊島区区民部税務課課長
	田島　康義	三鷹市教育委員会教育部総務課課長補佐
	玉置　崇	岐阜聖徳学園大学教授
	藤村　裕一	鳴門教育大学准教授
◎	山崎　文明	情報安全保障研究所首席研究員

【オブザーバー】

個人情報保護委員会事務局

総務省自治行政局地域情報政策室

（平成 29 年４月１日時点）