参考資料１－３

教育情報セキュリティポリシーに関するガイドライン

（令和４年３月）

平成 29 年 10 月 18 日　　策　定
令和３年５月　　改　訂
令和４年３月　一部改訂

文 部 科 学 省

重要：本書の位置付けについて

本書は、地方公共団体の各教育委員会が教育情報セキュリティポリシー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基本理念と検討する際の考え方について解説したものである。

平成 29 年 10 月版「教育情報セキュリティポリシーに関するガイドライン」策定以降、確実に教職員の情報セキュリティに関する意識を高める効果をもたらしているが、一方でガイドライン記載の具体的な対策例を一言一句遵守することが目的化してしまったため、昨今の急速な技術的進展（クラウド活用等）に対応できず、その結果、教育情報の活用に硬直性が生じるという弊害が各地で生じている。

本来セキュリティは教育関係者が遵守すべき基本理念をしっかりと共有した上で、各教育委員会がそれぞれの状況（費用、活用状況や環境整備状況）に応じて最新技術を随時取り入れながら適切なセキュリティを独自に確保すべきものである。

各教育委員会において教育情報セキュリティポリシーの策定・改訂を行う際には、本文の理念を踏まえつつ、教育委員会・学校の実態（実現したい学習や校務の環境、費用・運用面のコスト、ネットワークの構築状況等）を踏まえ、参考資料はあくまで参考としつつ、関係者（教育委員会・学校の担当者、有識者等）と十分に議論を行い、柔軟に対応されたい。文部科学省においても、ICT 活用教育アドバイザーによる相談体制を構築しているため、随時活用されたい。

主な改訂箇所（令和 3 年 5 月）

- 「第 1 章 本ガイドラインの目的」に GIGA スクール構想の実現についての内容を追記
- 「第 2 章 本ガイドライン制定の背景・経緯」にクラウド・バイ・デフォルトなど政府の方向性を踏まえた今後の教育環境 ICT 整備の方向性を追記
- 「第 3 章 地方公共団体における教育情報セキュリティの考え方」にローカルブレイクアウト及びクラウド活用を前提とした今後のネットワーク構成を整理
- 「1.3 情報資産の分類と管理方法」にクラウド活用における新たな情報資産などについて情報資産分類及び情報資産の取り扱いを整理
- 「1.9.4 約款による外部サービスの利用」についてソーシャルメディアサービス利用における留意点を追記
- 「1.10 事業者に対して確認すべきプライバシー保護に関する事項」に事業者に対するプライバシー保護に関する確認事項を整理
- 「1.11 クラウドサービス活用における個人情報について」にクラウドサービス利用する際の個人情報保護条例に関する内容を追記
- 「1.12 1 人 1 台端末に対するセキュリティ」に学習者用端末のセキュリティ及び ID 管理ついて追記

主な改訂箇所（令和４年３月）

「1.4.4. 教職員等の利用する端末や電磁的記録媒体等の管理」に振る舞い検知等の記述を追加

・「1.5.1. 教職員等の遵守事項」に校務端末の持ち出しに関する記述を適正化

・「1.6.1. コンピュータ及びネットワークの管理」に校務端末の使い分けについて対策毎に記述を適正化

目次

本文

第１章 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（令和２年 12 月)」（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、文部科学省では平成 29 年 10 月に、主に地方公共団体が設置する学校を対象とした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「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 月版)」を策定した。さらに、令和元年 12 月及び令和３年５月に改訂を行った。

本ガイドラインにおいては参考資料を記載しているが、基礎的な地方公共団体の中でも数が多い公立小学校及び中学校等の設置者である市の教育委員会を想定して記述している。また、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。

技術は日々進歩しており、本ガイドラインではクラウドサービスの活用について全てをカバーできている訳ではないが、各教育委員会・学校のポリシーに沿って、構築時点での最適解を選択するように期待する。

令和元年度に文部科学省が打ち出した GIGA スクール構想の実現に基づいた教育情報ネットワーク及び１人１台端末の環境整備が進み、子供たちの学びを深めるために利活用が益々進んでいくことが期待されている。本ガイドラインを参考にし、地方公共団体や学校の状況

に応じて適切な環境整備を実施頂きたい。

なお、本ガイドラインは、学校において安心してICT（情報通信技術（以下、「ICT」と言う。）を活用できる環境を維持する観点から、クラウドサービスに限らず、地方公共団体における情報セキュリティ対策の動向、技術的な進展等も踏まえつつ、引き続き見直しを行う予定である。

第２章 本ガイドライン制定の背景・経緯

（１）国の方向性・学習指導要領の改訂等

文部科学省においては、第3期教育振興基本計画（平成30年6月15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。

令和2年度からは、新学習指導要領が小学校から順次実施されており、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が必修化されている。

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、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、デジタル教科書が位置付けられ、デジタル教材と組み合わせた積極的な活用の環境が整うこととなる。

このような状況に加え、令和元年6月には、「学校教育の情報化の推進に関する法律」が公布・施行され、地方公共団体など関係者に対し学校教育の情報化が義務付けられることとなった。

（２）学校でのICT利用の特徴

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重要性が高い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。

しかしながら、実際の学校におけるICT活用は国際的にも大きく後塵を拝しており、一般社会からも大きく取り残された危機的状況である。このため、学校関係者は法律に則りICTの積極的な導入、活用を進める義務がある。その際、昨今、学校が保有する重要性が高い情報に対する不正アクセス事案や持ち出した学校情報を記録した媒体の紛失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。

（３）ガイドライン作成の経緯と主な改訂内容

①「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月版）」

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、「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。

②「教育情報セキュリティポリシーに関するガイドライン（令和元年12月版）」

教育現場における多様な学習環境の実現、教員の働き方改革の実現に対応したシステムが必要であり、それらを実現する手段としてのクラウドは有力な解決策としての認識が広がってきた。また、平成29年のガイドラインの策定・普及により、教育現場においては確実に教職員の情報セキュリティに関する意識が高まった一方、関係者においてガイドライン記載の具体的対策例を一言一句遵守することが目的化してしまい、教育情報活用の高コスト化、硬直化をもたらす懸念が新たに生じた。

これらを踏まえ、クラウドを活用した環境構築に関する内容を追記するとともに、教育委員会はじめ関係者が遵守すべき理念と、あくまで知見のない者が参考例とすべき内容を明確にした「教育情報セキュリティポリシーに関するガイドライン（令和元年 12 月版）」のとおり改訂を行った。

また、Society5.0 時代において社会構造や雇用環境が大きく変化することが考えられており、そのような社会で求められる能力や子供たち自身の多様化を踏まえ、児童生徒の学習の多様化（ICT を活用した自宅学習、個別最適化された学び等）や、その実現に向けた教員の働き方改革（テレワーク等）など、教育現場の改善が喫緊の課題である。それらを改善・実現するための手段としてクラウドは有力な解決策であり、前例にとらわれずクラウド化や組織を超えた広域統合を検討すべき時代である。このことを踏まえ、令和元年 12 月版の改訂において、クラウド化に力点を置き、第 5 章を追加し、その視点でのセキュリティ対策について追記を行った。（オンプレミス型の環境構築を否定するものではない。）

③「教育情報セキュリティポリシーに関するガイドライン（令和 3 年 5 月版）」

GIGA スクール構想に基づく 1 人 1 台端末、1 人 1 アカウント、教育用クラウドサービスの本格活用を進めることによって、一人一人の多様なニーズや特性等に対応した個別最適な学びと協働的な学びを充実させることができる。

GIGA スクール構想の推進により、児童生徒の「1 人 1 台端末」及び「高速大容量の通信環境」を一体とした学校の ICT 環境整備が急速に進んだことから、1 人 1 台端末を活用するために必要なセキュリティ対策やクラウドサービスの活用を前提としたネットワーク構成等の課題に対応するとともに、児童生徒端末と教員用端末から得られる各種教育データを効果的に活用して教育の質的改善を図るため「教育情報セキュリティポリシーに関するガイドライン（令和 3 年 5 月版）」の改訂を行った。

④「教育情報セキュリティポリシーに関するガイドライン（令和４年３月)」

今後の推奨ネットワーク構成として示した「アクセス制御による対策を講じたシステム構成」への円滑な移行を図るため、詳細な技術的対策の追記及び従来の「ネットワーク分離による対策を講じたシステム構成」と今後の「アクセス制御による対策を講じたシステム構成」について、明示的に書き分ける等の一部改訂を行った。なお、本改訂においては令和３年９月に発足したデジタル庁の協力も得て実施した。

【今般のガイドライン改訂経緯と今後の方向性について】

○　近年、急速に進化し発展したクラウドサービスは、社会全体で多方面にわたり利用が増加し、政府情報システムの整備においても、「デジタル社会の実現に向けた重点計画」（令和３年 12 月 24 日閣議決定）の方針も踏まえて、クラウドサービスの利用を第一候補として、その検討を行うものとするクラウド・バイ・デフォルト原則に基づくこととしている。各地方公共団体においてもクラウドの活用を念頭に置いてセキュリティを確保していく必要がある。

○　教育においては、社会全体のデジタル化、デジタルトランスフォーメーション(DX)、Society5.0 時代の到来という大きな潮流の中で、学校教育の基盤的なツールとして ICT は必要不可欠なものであり、GIGA スクール構想に基づく１人１台端末の本格運用を進めることによって、一人一人の多様なニーズや特性等に対応した個別最適な学びと協動的な学びを充実させることが重要である。

そのためには、児童生徒の学習履歴（スタディ・ログ)、生活・健康情報（ライフ・ログ)、教職員の支援等に関する情報とその効果・有効性の評価（アシスト・ログ）等を、低コストでありながら、セキュリティも担保して、有機的に結びつけながら活用できる環境構築が必要である。

さらには、新しい教育の提供手段や緊急時における教育提供手段として、同時双方向型の遠隔授業へのニーズも高まっている。そうした新しい教育ニーズに技術的にも経済的にも対応可能な学校 ICT 環境の整備が必要となる。

「令和の時代のスタンダード」として、GIGA スクール構想による学校 ICT 環境の実現を推進してきたところであるが、今般の新型コロナウイルス感染症の影響により、コロナ禍において子供たちの学びを保障する観点から、当初 4 年間で整備する予定であった計画を１年間に前倒し、学校 ICT 環境の整備を進めたところ。

○　そうした社会全体の急速な変化がある中で、児童生徒の 1 人 1 台端末環境が概ね整っているが、教育現場の ICT 環境はクラウドサービスの利用を進める上でまさに過渡期にあると考えられる。本ガイドラインは、従来のオンプレミスを前提とした ICT 環境

整備を否定するものではないが、社会全体のデジタル化が大きく促進している中で、学校教育が遅れをとることのないよう、自らが実現したい環境について、コストや学校規模、利便性、運用性等、情報資産の重要性を鑑みながら、クラウドサービスの利用を念頭に置いた学校 ICT 環境の整備に前向きに取り組んでいただきたい。また、併せて各自治体における教育情報セキュリティポリシーの見直しも進めていただきたい。

第３章 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に関するガイドラインは、以下の①～⑥を基本理念として、「参考資料」にて対策基準の例をまとめている。

各教育委員会・学校においては、本ガイドラインを参考にしつつ、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、児童生徒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児童生徒による重要性が高い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、学校が保有する重要性が高い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重要性が高い情報等にアクセスするリスクを回避することが必要である。

③標的型及び不特定多数を対象とした攻撃等による脅威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、標的型及び不特定多数を対象とした攻撃等による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、平成29年のガイドライン策定時に教員が個人情報を外部に持ち出す際のルールについて、考え方を明確にした。

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重要性が高い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。なお、通信経路の暗号化を必須とし、データへの適切なアクセス制限を行った上で、データそのもの及びデータ格納先の暗号化については運用を考慮して対策を講ずることが必要である。

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重要性が高い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。

（補足）技術的対策に関する考え方

ここに記されている内容は、主な対策の考え方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。対策については、参考資料を参照しつつ、各教育委員会で整理・判断されたい。

（１）学校が保有する重要性が高い情報に対するセキュリティ強化

（主な対策）

①標的型及び不特定多数を対象とした攻撃等による脅威への対応

・ウェブ閲覧やインターネットメールなどのインターネットを介した外部からのリスクの高いシステムと重要性が高い情報、特に重要性分類Ⅱ(セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす情報資産)以上を扱うシステムとの論理的又は物理的な分離、もしくは各システムにおけるアクセス権管理の徹底。

②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、もしくは各システムにおけるアクセス権管理の徹底。

③アクセス権管理の徹底がされていない学習系システムへの重要性分類Ⅱ以上の保管の原則禁止

（２）学校単位で重要性が高い情報を管理するリスクの低減

（主な対策）

①校務系システムについて、クラウドの活用も含めた教育委員会による一元管理

・学習系システムも含め、情報セキュリティ確保の観点からは教育委員会において一元管理することが効果的である。

②学校のインターネット接続環境の一元管理によるセキュリティ対策強化

・教育委員会のデータセンター等でインターネット接続環境を集約することが想定される一方で、局所的にネットワークの負荷が増大し、授業における安定的な稼動に支障をきたす可能性もあることから、学校から直接インターネットへ接続する学校直収型や、センター集約において、一部の通信を直接インターネットへ接続するローカルブレイクアウト（インターネットブレイクアウトともいう。）の構成も想定される。GIGA スクール構想に基づき、児童生徒が 1 人 1 台端末を安定したクラウドサービスが利用可能な高速なネットワーク環境下で利用する、時代に即した学校直収型及びローカルブレイクアウトの構成も積極的に検討されるべきである。なお、どのような構成においてもセキュリティ対策指針は教育委員会で統一であるべきであり、それに基づいて、セキュリティ対策機器を設置することや、インシデント発生時の体制の確立など、各学校で適切なセキュリティ対策を講じる必要があ

る。用途・目的に応じて柔軟に判断されたい。

③校務系システム及び学習系システムへのアクセス権限に関する最小権限の原則の徹底と通信の暗号化等の実装による安全管理措置の実施

④大規模災害に備え、学校設置のシステムからの大規模災害対応済データセンター・自治体システム設置のデータセンターやクラウドサービスの活用への移行の推奨

（３）教職員による人的な重要性が高い情報の漏えいリスクの最小化

（主な対策）

①管理されたUSBメモリ等の電磁的記録媒体以外の使用禁止

※　具体的には、暗号化、パスワード設定等を実施し、教職員専用として管理されたもの

②電磁的記録媒体の暗号化の徹底

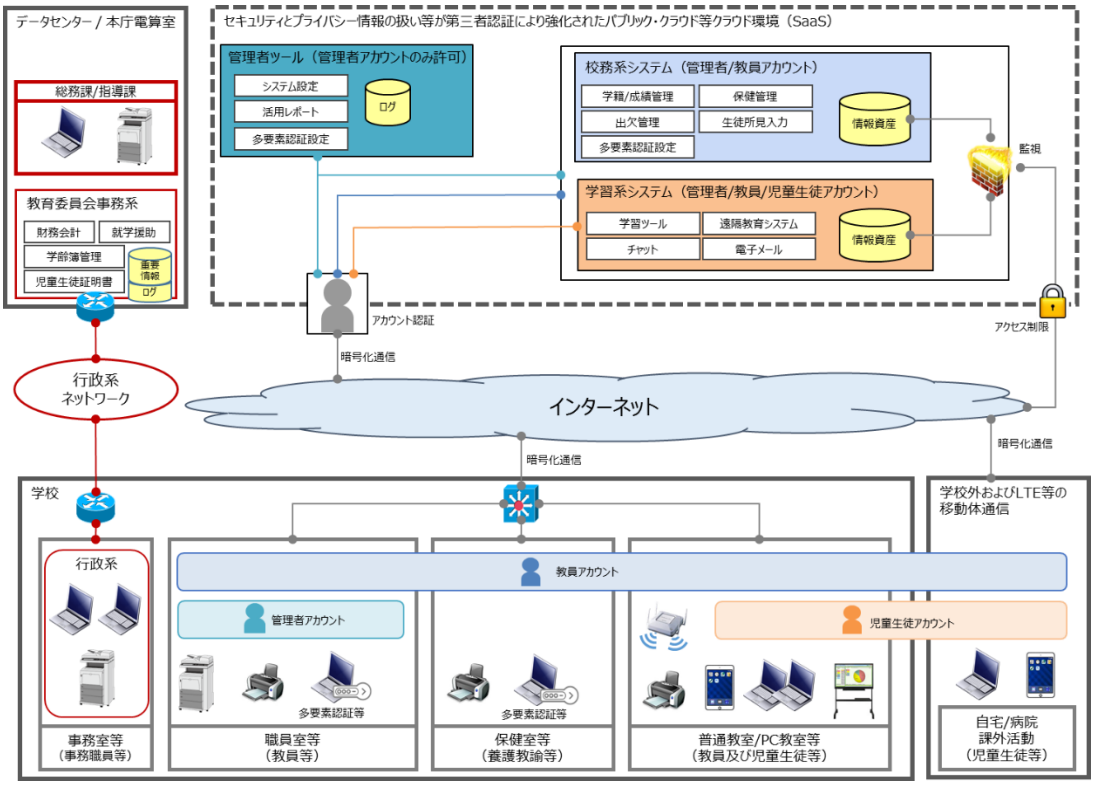
※　暗号化については、コストや実現したい環境を踏まえつつ、ストレージやファイル等に対し、適切なレベルの暗号化を行うことで、一層のセキュリティの向上が見込まれる

（図表：学校におけるネットワーク等の構成のイメージ）

以下の図表は、ネットワーク等の構成のイメージであり、画一的な方策を示しているものではない。教育委員会・学校においては、自らが実現したい環境、コスト等を踏まえながらネットワーク構成を検討すること。

＜1 人 1 台端末を活用するために必要なネットワーク構成イメージ（アクセス制御による対策を講じたシステム構成）＞

GIGA スクール構想の実現に向けたクラウドの活用を前提とした今後の推奨ネットワーク構成である。

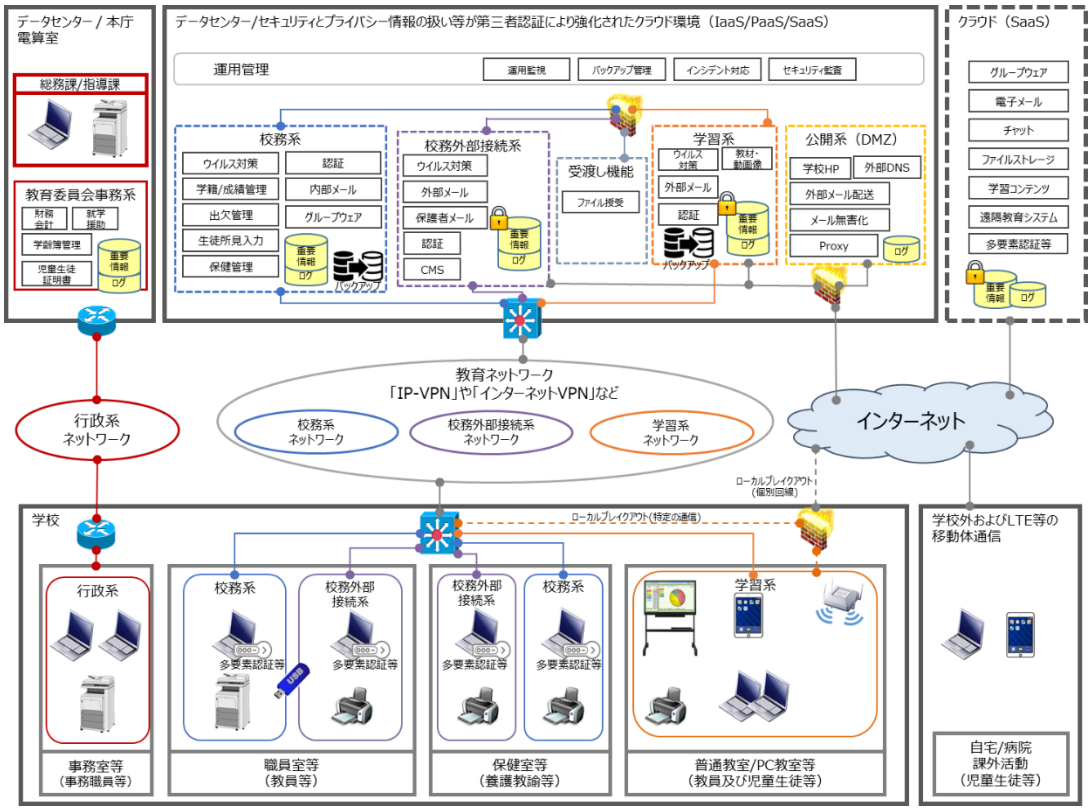


※　学校からのインターネットへの接続形態としては、「センター集約型」、「学校直収型」が想定される。上記の図は学校直収型を想定しているが、十分な帯域が確保されているセンター集約型も想定される。

※　クラウドサービスで管理されるデータは、サービス提供事業者により厳格に管理されていることを前提としており、クラウドサービスへの接続形態を物理的又は論理的に分離する必要がない。（利用するクラウドサービスの選定においては、「1.9 クラウドサービスの利用」を参照）

※　インターネットに接続する校務用端末に重要な情報資産が格納される可能性があるため、不正アクセスやマルウェア対策、さらには教員等の不注意による情報流出への対策を実施すること。

＜データセンターとクラウドを併用し、ネットワーク分離を基本としたネットワーク構成イメージ（ネットワーク分離による対策を講じたシステム構成）＞



※　学校からのインターネットへの接続形態としては、「センター集約型」、「学校直収型」が想定される。上記の図は、データセンターやインターネットへの接続は「センター集約型」で行い、ネットワークを論理分離している場合のイメージである。

※　上記図表におけるクラウド（破線部分）とは、校務系や学習系ごと等に構築される、いわゆるマルチクラウドで運用する場合のイメージである。

※　一部の通信を直接インターネットへ接続するローカルブレイクアウトについては学校から直接インターネットへ接続する構成となるため、ローカルブレイクアウトによるインターネットとの接続ポイントについては、学校直収型と同様のセキュリティ対策を実施すること。

※　ローカルブレイクアウト構成については、「新たなインターネット回線を個別に準備」、「既存機器から特定の通信のみインターネットへ接続」することが想定される。既存機器の性能や回線費用などを考慮し、適切に選択すること。

第４章 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、その「対策基準」を遵守する義務を負う。また、児童生徒においても本ガイドラインに規定した対策について遵守するよう、職員、教員、保護者等が適切に指導を行うこと。

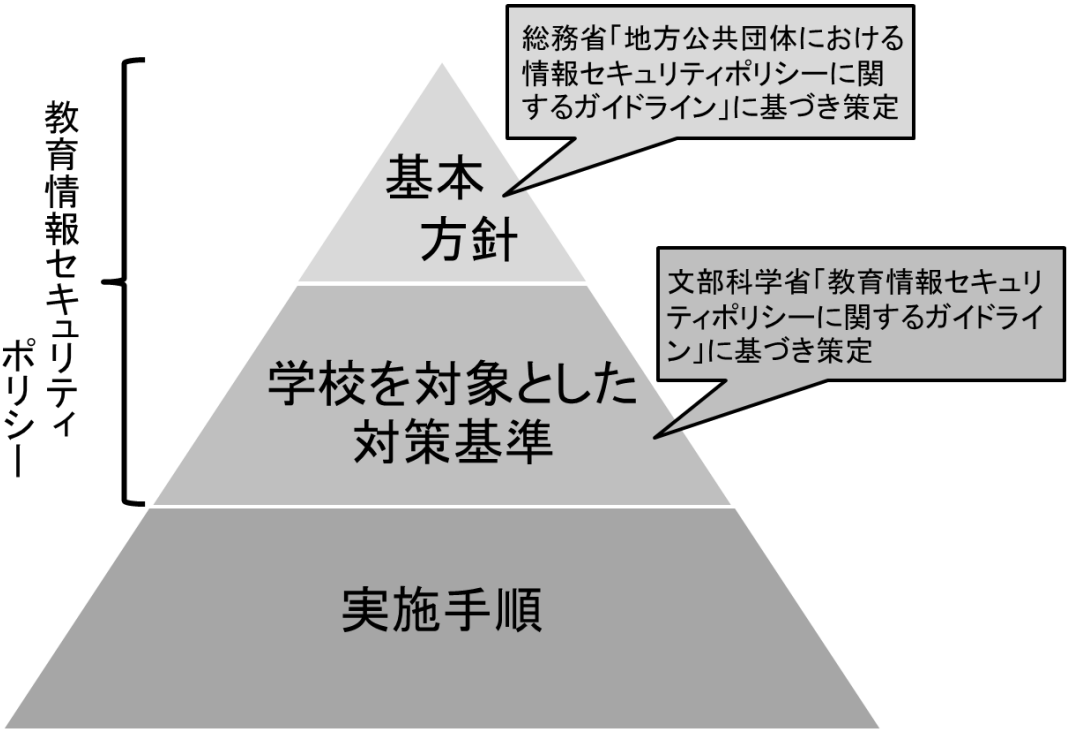
なお、本ガイドラインの対象とする範囲は「教育情報セキュリティポリシー」を構成する「対策基準」の部分であるが、『本文』の基本理念は、「実施手順」の策定においても踏まえるべきものである。特に、令和4年3月改訂版の本ガイドラインにおいては、GIGAスクール構想における児童生徒1人1台端末、1人1アカウント、それらを利用してクラウドへのアクセスを適切に実現するための明確な基準を示している。GIGAスクール構想及び各施策の実現を促進する情報セキュリティポリシーを定めるため、各地方公共団体においては常に最新のガイドラインを参照されたい。

※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」（https://www.soumu.go.jp/main_content/000727474.pdf）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、『参考資料』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

※本ガイドラインの対象範囲は、教育情報システムにおける、「情報資産」、「校務系及び学習系等の端末」、「クラウド利用もしくはオンプレミス利用による校務系・学習系システム」、「端末と校務系・学習系システムと外部情報資産を接続するネットワークとそのインターフェース」とする。

第５章 教育現場におけるクラウドの活用について

クラウドサービスは、正しい選択を行えば、コスト削減に加えて、情報システムの迅速な整備、柔軟なリソースの増減、自動化された運用による高度な信頼性、災害対策、テレワーク環境の実現等に寄与する可能性が大きく、前述のとおり、学習環境の多様化、教員の働き方改革の実現等、クラウドは教育現場の改善の手段としても有力な解決策の一つである。

学校における ICT 環境整備を進めるに当たっては、これらの特徴と、教育現場において活用できる資源（費用・人員等）が限られている現状を踏まえ、校務系・学習系を問わず、システム更改時においてはクラウドサービスの利用も有力な選択肢として、検討を進めていくことが重要である。

クラウドサービスの利用に係る検討は、上記のメリットのほか、運用の負荷に関する効率化が未知数であることや、オンプレミス型と比べて初期費用は大幅に低減される一方で、一定の運用費用の負担が継続することなど、その特性を正しく認識することが重要であり、その上で、その対象となるサービス・業務及び取り扱う情報を明確化し、クラウドサービスの利用メリットを最大化並びに開発の規模及び経費の最小化の観点により、導入に向けた検討を行うことが望ましい。

また、クラウドサービスの活用に向けては、各自治体の教育情報セキュリティポリシーが、クラウドサービスの活用を前提とした内容となるよう確認・見直しを行った上で、利用しようとするクラウドサービスと、自らのセキュリティポリシーが適合しているかどうかを判断することが重要である。

なお、クラウドサービスの安全性の確認については、情報セキュリティの実態をクラウド利用者が個別に詳細に調査することは困難であることから、第三者による認証やクラウドサービス事業者が提供する監査報告書を利用することが重要であり、クラウドサービスの選定に際しては、求める内容に応じた認証規格等を参考にする仕組みとすることが望ましい。

（クラウドサービスの利用においては、「参考資料　1.9 クラウドサービスの利用」を参照すること。）

「教育情報セキュリティポリシーに関するガイドライン」　参考資料

『参考資料』　情報セキュリティ対策基準の例

1.1. 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（公開系情報）	校務系情報のうち、保護者メールや学校ホームページ等インターネット接続を前提とした校務で利用される情報
学習系情報	児童生徒のワークシート、作品など、学校が保有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ当該情報に教員及び児童生徒がアクセスすることが想定されている情報

校務用端末	校務系情報にアクセス可能な端末
校務外部接続用端末	校務外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 及び、校務系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
校務外部接続系システム	校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ(CMS)及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム
学習系システム	学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム 及び、学習系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
教育情報システム	校務系システム、校務外部接続系システム及び学習系システムを合わせた総称
校務系サーバ	校務系情報を取り扱うサーバ
校務外部接続系サーバ	校務外部接続系情報を取り扱うサーバ
学習系サーバ	学習系情報を取り扱うサーバ

(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、クラウドサービス等
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（クラウドサービスを除く）、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、SDカード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、クラウドサービス契約関連文書等

1.2. 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、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及びCISOが別途選任した者から構成される情報セキュリティ委員会を設置し、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。

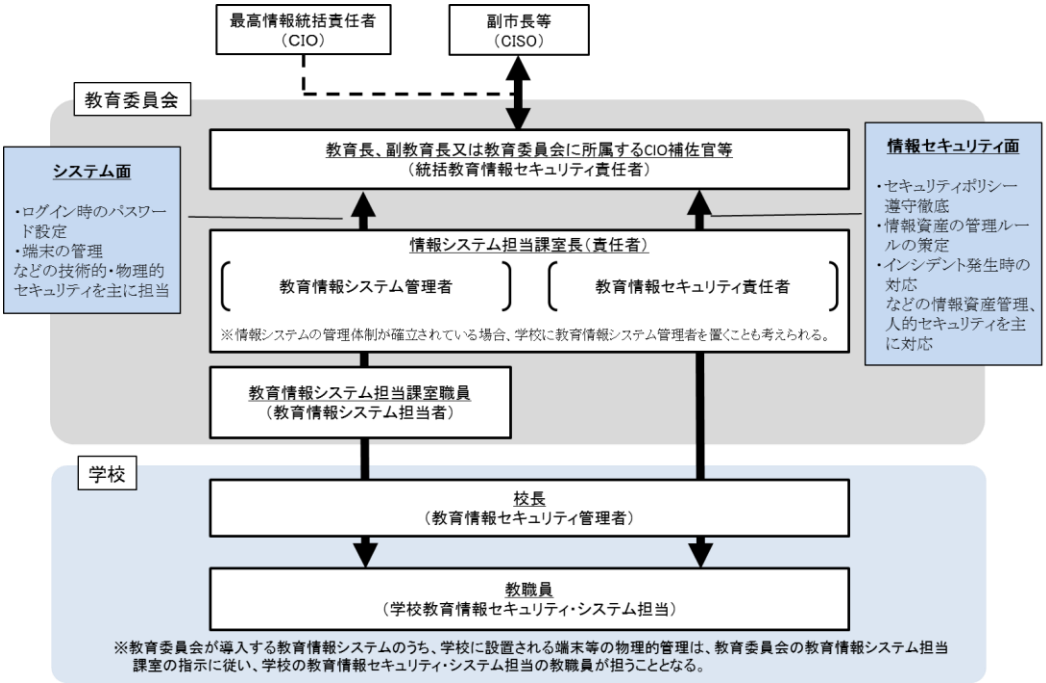
（１）最高情報セキュリティ責任者（CISO：Chief Information Security Officer、以下「CISO」という。）

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、情報セキュリティに精通した外部の有識者等が想定され、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。

1.3. 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、その分類を表示し、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。

※　情報資産の分類の表示先

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

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、電磁的記録媒体または保存されている領域（フォルダやサーバ）に情報資産の分類が異なる情報が複数記録されている場合、最

高度の分類に従って、当該電磁的記録媒体または保存されている領域を取り扱わなければならない。

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USBメモリ等の外部電磁的記録媒体を保管する場合は、外部電磁的記録媒体への書込禁止の措置を講じなければならない。

（ウ）教育情報セキュリティ管理者又は教育情報システム管理者は、情報システムのバックアップで取得したデータを記録する電磁的記録媒体を保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。なお、クラウドサービスを利用する場合はサービスの機能として自然災害対策がなされていることを確認すること。【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、重要性分類Ⅲ以上（機密性2A以上、完全性2A以上又は可用性2A以上）の情報を記録した電磁的記録媒体を保管する場合、耐火、耐震、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦情報の送信

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

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

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

⑧情報資産の運搬

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

⑨情報資産の提供・公表

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

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

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

⑩情報資産の廃棄

（ア）重要性分類Ⅲ以上（機密性2A以上）の情報資産を廃棄する者は、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	校務系	学習系	公開系
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 ・卒業証書授与台帳 ・転退学受付（整理）簿 ・転入学受付（整理）簿 ・就学児童・生徒異動報告書 ・休学・退学願等受付（整理）簿 ・教科用図書給付児童・生徒名簿 ・要・準要保護児童・生徒認定台帳 ・その他校内就学援助関係書類 ○成績関係 ・通知表 ・評定一覧表 ・進級・卒業認定資料 ・定期考査・テスト等の答案用紙 （児童・生徒が記入済のもの） ・定期考査素点表 ・成績に関する個票等 ○指導関係 ・事故報告書・記録簿 ・生徒指導・特別指導等記録簿 ・児童・生徒等の個人写真・集合写真 ・指導記録・指導カード （児童・生徒等理解カード） ・教育相談・面接の記録・カード等 ・個別の教育支援計画 （学校生活支援シート） ・個別指導計画 ・家庭訪問記録・個別面談記録 ・教務手帳 ・週ごの指導計画 （個人情報が含まれるもの） ○進路関係 ・調査書 ・推薦書 ・公立高校入学者選抜に係る成績一覧表 ・入学者選抜に関する表簿（原書等） ・私立高校入試に係る事前相談資料 ・卒業生進路先一覧等 ・進路希望調査 ・進路判定会議資料 ・進路指導記録簿	○児童・生徒に関する個人情報 （生活歴、心身の状況、財産状況等の情報、電話番号、メールアドレス、住所、生年月日、性別等の基本情報を含むもの） ○学校教職員に関する個人情報 （病歴、心身の状況、収入等の情報、電話番号、メールアドレス、住所、生年月日、性別等の基本情報を含むもの） ○健康関係 ・健康診断票 ・歯の検査表 ・心臓管理等医療情報 ・学校生活管理指導票 ・児童・生徒等健康調査票 ・児童・生徒の健康保険等被保険者証の写 ・健康診断に関する表簿 ・就学時健康診断票 ○教職員に割り当てた機密性の高い情報 ・情報システムログインID/PW管理台帳 ・情報端末ログインID/PW管理台帳 ○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 ・PTA会員名簿 ・職員緊急連絡網・職員住所録 ・委員会名簿 ・PTA役員連絡網 ○各種帳票ファイル ・指導要録作成システム等、データの入っていない帳票	○児童生徒の学習系情報 ・学習システムログインID/PW管理台帳 ・学習用端末ID/PW管理台帳	
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	○児童生徒の氏名 ・出席簿 ・名列表 ・座席表 ・児童生徒委員会名簿	○学校運営関係 ・卒業アルバム ・学校行事等の児童・生徒の写真	○学校運営関係 ・授業用教材 ・教材研究資料 ・生徒用配布プリント ○児童生徒の学習系情報 ・児童生徒の学習記録 （確認テスト、ワークシート、レポート、作品等） ・学習活動の記録（動画・写真等）	
Ⅳ	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 ・各種届綴形・校務分掌表 ・ＰＴＡ資料 ・学園・学校・学年・学級だより ・学校・学園ホームページ掲載情報 ・学校行事のしおり ○学校活動の記録 ※　保護者の承諾がある場合、以下は公開可能 ・学校行事等の児童・生徒の写真 ・学習活動の記録（動画・写真・作品等）

※　この表については、情報資産の分類を検討する際のイメージ・参考である。以下の注釈も踏まえつつ、各自治体・学校が実現したい環境と情報セキュリティのバランスを考慮し、柔軟に対応することが必要である。

（注１）児童生徒の氏名、性別、学年等の属性情報を、生活歴、心身の状況、電話番号等といった情報と束ねたリスト等については、上記のとおり重要性分類Ⅱとして扱うことが望ましい一方で、児童生徒が学習活動を通して生み出す学習系情報の中にも、氏名、性別、学年といった属性情報を置くことは自然なことであり、様々な学習系ツールの利用場面も含めて、これらの属性情報について学習系システムの中において扱うことを一義的に禁止するものではない。前述のとおり、活用場面等に応じて、実態に即した形で運用すること。

（注２）児童生徒の学習記録等についても、児童生徒自身が振り返りとして活用することも想定される。その活用が児童生徒にとって有益となる場合であって、自身の情報に対しては当該児童生徒以外からの不要なアクセスを防ぐ環境を構築する等の配慮をした上で、学習系システムにおいて運用することなども考えられる。なお、それらの情報をクラウド事業者が、利用者の同意なく無断使用（目的外利用（無断解析等）、第三者への提供等）しないよう留意すること。

（注３）ログインID/PW自体は情報資産として取り扱うものではないが、ログインID/PWを束ねた管理台帳については重要性分類Ⅱ以上として扱うこと。

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１）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２）情報資産の分類に応じて、利用する情報システム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３）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４）情報資産の共有とは、保護者等に情報を共有すること（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。

（注５）データの消去及び機器の廃棄については、「1.4.1　（７）機器の廃棄等」を参照し、データ消去が確実に行われるよう留意すること。

情報資産の分類					情報資産の取扱例								
重要性分類	定義	機密性	完全性	可用性	複製・配布	組織外部への持ち出し制限*	端末制限	情報の組織外部への送信**	情報資産の運搬***	組織外部での情報処理****	使用する電磁記録媒体	情報資産の保管	情報資産の廃棄
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	本ガイドラインに準拠していることを確認した上で業務遂行上必要な場合には、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	限定されたアクセスの措置がとられていること*****	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（電子データの場合もこれらの対策に準じたサーバに保管） ・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） ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・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	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（電子データの場合もこれらの対策に準じたサーバに保管） ・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） ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁記録媒体の持ち込み禁止	同上
Ⅳ	影響をほとんど及ぼさない。	1	1	1									

*： 組織外部への持ち出しとは、教育委員会・学校が構築・管理している環境(本ガイドラインが適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境)の外に情報資産を持ち出すことを示す。

**：情報の組織外部への送信とは、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。

***：情報資産の運搬とは、USBメモリやハードディスク等の外部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。

****:組織外部での情報処理とは、教育委員会・学校が構築・管理している環境(本ガイドラインが適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境)の外において情報資産を管理・電算処理することを示す。

*****：限定されたアクセスの措置とは、適切かつ限定的な利用を前提とし、外部に送信される際に適切なアクセス制限を講じることを指す。

図表6　情報資産の取扱例

1.4. 物理的セキュリティ

本項においては、特にサーバ及び管理区域に関する部分の取扱いについては、主にオンプレミスの場合を想定している。クラウドサービスを利用する場合には、「1.9　クラウドサービスの利用」を軸に確認・検討すること。

1.4.1. 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、重要性分類Ⅲ以上（可用性2A以上）のサーバ等の機器の定期保守を実施しなければならない。

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

（６）施設外又は学校外への機器の設置

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。日本データセンター協会(2017)データセンター セキュリティ ガイドブックを参照し、物理的機器設置時のデータセンター提供者が必要なセキリュティ仕様を把握することが出来る。また、事業者のISO 27001取得を確認することは、事業者が情報セキュリティマネジメントシステム（ISMS）事業者として最低限必要な要件を満たしているかを確認する際に有効である。

（７）機器の廃棄等

機器が不要になった場合やリース返却等を行う場合には、機器内部の記憶装置からの情報漏えいのリスクを軽減する観点から、情報を復元困難な状態にする措置を徹底する必要がある。この場合、一般的に入手可能な復元ツールの利用によっても復元が困難な状態とすることが重要であり、OS及び記憶装置の初期化(フォー マット等)に

よる方法は、ハードディスク等の記憶演算子にはデータの記憶が残った状態となるため、適当でないことに留意が必要である。

（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。

1.4.2. 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、重要性分類Ⅱ以上（機密性2B以上）の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、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、管理区域への入退室を許可された教職員を立ち会わせなければならない。

(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、フロアスイッチBOX等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、地方公共団体職員及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。

1.4.3. 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ポイント及び該当ポイントに接続される端末を正確に把握し、適切な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は、重要性分類Ⅲ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、通信経路上で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、重要性分類Ⅱ以上の情報資産を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。

（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。

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ほか、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か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構成も考えらえる。ただし、局所的にネットワークの負荷が増大し、授業における安定的な稼動に支障をきたす可能性もあることから、用途・目的に応じて柔軟に判断する必要がある。

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。

（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。

1.4.4. 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】

（教員等の利用する端末について）

① 教育情報システム管理者は、不正アクセス防止のため、ログイン時のIDパスワードによる認証、加えて多要素認証の実施等、使用する目的に応じ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、校務系システム、タブレットやパソコン等教育情報システムへアクセスする端末への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多要素認証を設定しなければならない。特にアクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産へのアクセスについては、多要素認証を必須とすること。

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

⑦ 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】

⑧ 教育情報システム管理者は、パソコンやモバイル端末におけるマルウェア感染の脅威に対し、ウイルス対策ソフトの導入等の対策を講じなければならない。なお、OSによっては標準的にウイルス対策ソフトを備えている製品、OSとしてウイルス感染のリスクが低い仕組みとなっている製品などもあるため、実際に運用する端末において適切な対策を講じること。アクセス制御による対策を講じたシステム構成の場合、校務情報等の重要な情報資産を取り扱う端末に対し、当該端末の状況および通信内容を監視し、異常、あるいは不審な挙動を検知する仕組み（ふるまい検知）等の活用を検討し、適切な対策を講じること。

⑨ 教育情報システム管理者は、インターネットへ接続をする場合、教職員等のパソコン、モバイル端末に対して不適切なウェブページの閲覧を防止する対策を講じなければならない。

（学習者用端末について）

※パソコン教室などに設定されている学習者用端末を対象としている。1人1台端末については後述する「1.12. 1人1台端末におけるセキュリティ」も参照すること

① 教育情報システム管理者は、盗難防止のため、教室等で利用するパソコンの保管庫による管理等の物理的措置を講じなければならない。

② 教育情報システム管理者は、電磁的記録媒体について、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

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

（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。なお、アクセス制御による対策を講じたシステム構成の場合においては、校務・学習等各システム別による端末配備を求めるものではない。適切なアクセス権が設定された指導者用端末は、同じく適切なアクセス権が設定された校務系サーバ及び校務外部接続系サーバ、及び同様のサービスを提供するクラウド環境にアクセスすることができる。

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多要素認証の利用

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多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ファイルの暗号化

端末に保存したファイルを暗号化し、暗号鍵を保持しない利用者は情報の閲覧等ができない仕組み。教職員等の負担を考慮し、ファイル保存時に自動で暗号化される仕組みも有効である。

⑦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。

⑧マルウェア対策

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、既存のパターンファイルから検出する手法に加え、ふるまい検知が有効である。ふるまい検知とは、既存のパターンファイル情報に依存することなく、各端末における通常時の通信傾向を学習し、そこから逸脱する不審な通信について検知する仕組み。隔離された安全な領域（サンドボックス）で不審なプログラムの挙動を検知することにより、未知の攻撃にも有効である。

なお、マルウェアに感染し攻撃を検知した場合には、その根本原因や感染した端末の特定と隔離、影響範囲の関係や時系列での不正なふるまいの状況を一元的に把握することができるEDR（Endpoint Detection and Response）も有効である。運用体制・端末のリソース状況・実現したい機能・コストを鑑みて検討すること。

⑨不適切なウェブページの閲覧防止

アクセス制御による対策を講じたシステム構成の場合、不適切なウェブページへの閲覧を防止する対策として「フィルタリングソフト」、「検索エンジンのセーフサーチ」、「セーフブラウジング」等がある。実現したい機能や実際の運用に応じて適切に整備することが重要である。

（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、認証の都度、異なるパスワードを発行するため

に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の観点から、例文④以降を省略している。

1.5. 人的セキュリティ

クラウドサービスの利用においては、本項及び「1.9　クラウドサービスの利用」を踏まえて確認・検討すること。

1.5.1. 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教育委員会・学校が構築・管理している環境(本ガイドラインが適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境)の外部における情報処理作業の制限

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

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

(ウ)教職員等は、外部で情報処理業務を行う場合には、教育情報セキュリティ管理者の許可を得なければならない。

④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

(ア)教職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、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。なお、アクセス制御による対策を講じたシステム構成の場合は、情報セキュリティ管理者の包括的承認を行う等、運用実態や教職員等の負担も考慮し検討すること。

⑥パソコンやモバイル端末におけるセキュリティ設定変更の禁止

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

⑦机上の端末等の管理

教職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は教育情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適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

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。

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。

なお、1人1台端末におけるセキュリティ対策に関しては後述の「1.12. 1人1台端末におけるセキュリティ」も参照すること。

〔児童生徒への指導事項の例〕

・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

②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

情報の漏えいは、モバイル端末の不正な持ち出しや移動中にモバイル端末が盗難

に遭い、かつ不正アクセスに遭うことが原因で発生する場合が多い。ネットワーク分離による対策を講じたシステム構成の場合、教職員等が端末を持ち出す場合には、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。一方で、アクセス制御による対策を講じたシステム構成等においては、情報セキュリティ管理者の包括的承認を行う等、運用実態や教職員等の負担も考慮し検討する必要がある。また、端末アクセス時のログインパスワードの徹底、多要素認証の利用を行い、不正アクセスを防ぐことが重要である。

（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、認証による本人確認手段の確保と、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5版）」（令和3年5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。

③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
・重要性分類Ⅱ以上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。

④持ち出し及び持ち込みの記録

ネットワーク分離による対策を講じたシステム構成の場合、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。一方で、アクセス制御による対策を講じたシステム構成の場合は、学校外での端末利用に対して「1.4.4.教職員等の利用する端末や電磁的記録媒体等の管理」に示している適切な安全管理措置が講じられている前提においては、情報セキュリティ管理者の包括的承認を行う等、運用実態や教職員等の負担も考慮し検討する必要がある。

（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、「1.8. 外部委託」を参照のこと。

1.5.2. 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。

1.5.3. 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、「1.7.3. 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。

1.5.4. 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。

なお、1人1台端末におけるID及びパスワード等の管理に関しては後述の「1.12. 1人1台端末におけるセキュリティ」も参照すること。

【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複数の教育情報システムを扱う教職員等は、同一のパスワードを複数のシステム間で用いてはならない。　（シングルサインオンを除く）

⑥仮のパスワード（初期パスワードを含む）は、最初のログイン時点で変更しなければならない。

⑦サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。

⑧教職員等間でパスワードを共有してはならない。（ただし、共有IDに対するパスワ

ードは除く）
⑨共有IDに対するパスワードは定期的に又はアクセス回数に基づいて変更しなければならない。
⑩取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の多要素認証を設定しなければならない。

（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(Identification)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。

なお、共有IDを利用することは避けることが望ましい一方で、利用せざるを得ない場合には多要素認証と組み合わせることにより、ログから利用者を特定できることもある。

（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、名前などの個人情報からは推測できないこと、類推しやすい並び方やその安易な組合せにしないこと、パスワードの使い回しの禁止、英数（可能であれば記号も）を混在すること、英字は小文字と大文字を混在すること、12桁以上とすること等）、パスワードの共有禁止などを定める。なお、パスワードの定期的な変更はセキュリティ対策としては効果が薄く、上述のとおり、想像しにくいパスワードを設定した上で流出時に速やかに変更をすることが推奨されるが、共有IDに対するパスワードにおいては、退職者/離職者によるなりすまし対策になり得る。

（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。なお、パスワードの設定については、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も効果的である。

（注２）サービス利用時に都度ID/パスワード等の認証情報を入力する場合、サービス毎のアカウント情報管理が非常に煩雑になるため、一度の認証により一定時間は各種サービスにアクセスが行えるシングルサインオンの導入を行うことにより、運用効率化と運用負荷の最小化、煩雑な運用によるセキュリティリスクを低減することが期待できる。

1.6. 技術的セキュリティ

本項においては、特にサーバに関する部分の取扱いについては、主にオンプレミスの場合を想定している。クラウドサービスを利用する場合には、「1.9　クラウドサービスの利用」を軸に確認・検討すること。また、学習者用端末に関しては「1.12　1人1台端末におけるセキュリティ」を軸に確認・検討すること。

1.6.1. 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。また、アクセス制御による対策を講じたシステム構成の場合は、教職員端末での情報資産の管理がより重要となってくる。対策等については「1.4.4 教職員等の利用する端末や電磁的記録媒体等の管理」を参照すること。

なお、「1.9.1　学校現場におけるクラウドサービスの利用について　②セキュリティ水準の向上」に記載のとおり、多くの情報システムにおいては、クラウドサービスを適切に利用することで、オンプレミスよりも効率的に情報セキュリティレベルを向上させることが可能となる。

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

（2）バックアップの実施

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等について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

（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、所管するネットワークの内部におけるファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

②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、所管するネットワークに適切なアクセス制御を施さなければならない。

（9）外部の者が利用できるシステムの分離等

教育情報システム管理者は、保護者等の外部の者が利用できるシステム等がある場合、重要性が高い情報、特に情報資産重要性分類Ⅱ(セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす情報資産)以上を扱うシステムとの論理的又は物理的な分離、もしくは各システムにおけるアクセス権管理の徹底を行うこと。

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

①教育情報システム管理者は、アクセス制御による対策を講じたシステム構成の場合は、各システムにおけるアクセス権管理の徹底をしなければならない。

ネットワーク分離による対策を講じたシステム構成の場合は、校務系システム及び学習系システム間の通信経路の論理的又は物理的な分離をするとともに、ウェブ閲覧やインターネットメールなどのインターネットを介した外部からのリスクの高いシステムと重要性が高い情報（特に校務系）を論理的又は物理的に分離をしなければならない。

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

（１２）複合機のセキュリティ管理

①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、仕様通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。なお、ログの取得については、セキュリティインシデントに対して即時に対応するためには、リアルタイムでログの取得・分析等を行う手法を採用することも効果的である。

（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。

（9）外部の者が利用できるシステムの分離等

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

（１０）外部ネットワークとの接続制限等

所管するネットワークにおいて、インターネットに接続し、公開し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、所管するネットワーク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）重要性が高い情報に対するインターネットを介した外部からのリスク、児童生徒による重要性が高い情報へのアクセスリスクへの対応

児童生徒の成績情報や生徒指導関連情報等の個人情報などを含む重要性が高い情報を扱う「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インターネットを介した外部からのリスクの高いシステムと重要性が高い情報（特に校務系）との論理的又は物理的な分離、もしくは各システムにおけるアクセス権管理の徹底を行うこと。
・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などの対応、もしくは各システムにおけるアクセス権管理の徹底を行うこと。

また、ネットワーク分離による対策を講じたシステム構成の場合、「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、各システムにおけるアクセス権管理の徹底、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、個人情報などを含む重要性が高い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、上記のネットワーク分離による対策を講じたシステム構成での考え方に従った場合、校務用端末については、以下のような対応が考えられる。

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」の分離によるセキュリティの品質に準ずる対策を行い、1 台の端末で運用する 等

一方、アクセス制御による対策を講じたシステム構成においては、各システムにおけるアクセス権管理の徹底を行うとともに、端末に対して「1.4.4. 教職員等の利用する端末や電磁的記録媒体等の管理」に示している適切な安全管理措置を行うことで、「校務系システム」「校務外部接続系システム」「学習系システム」に接続する端末を 1 台に統合し運用することが可能である。

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、重要性が高い情報の保護に関する方法を判断する必要がある。

（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）及びWPA（WPA（Wi-Fi Protected Access）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WPA2以降の暗号方式を採用しなければならない。暗号化を含めた無線LAN全般に関するセキュリティ対策は「Wi-Fi提供者向け セキュリティ対策の手引き」を参照されたい。
（https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/）

（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。

規約に基づかずに利用されているフリーメールサービス等に対しては、外部への不正な情報の持ち出し等に利用される場合があることから、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。

1.6.2. 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。特にアクセス制御による対策を講じたシステム構成の場合、重要な情報資産へのアクセスについては、当該システムへの認証強度の向上とアクセス権管理を徹底すること。

②利用者IDの取扱い

（ア）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、その利用期間に合わせて特権IDを作成・削除する、もしくは、入力回数制限を設ける等のセキュリティ機能を強化しなければならない。

（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）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、組織外部からのシステムアクセスを認める場合、アクセスする利用者の本人確認、システムアクセスの対象となる児童生徒の本人（保護者）同意を得る等の措置を講じなければならない。

④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、外部から教育ネットワークに接続することを許可する場合は、利用者のID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、利用期間に合わせて、その都度作成し、本人確認の上で払い出しを行うことが望ましい。そのように運用しない場合であっても、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。

なお、各システムへのログインに多要素認証を用いる場合は、シングルサインオンを併用するなど、教職員等の負担を十分考慮した仕組みを導入することが望ましい。

また、各システムへのアクセスに対し、端末のIPアドレスやWebブラウザ、場所や時間などが通常と異なる際のリスクを判定し、追加の認証を行う方式であるリスクベース認証を用いることにより重要な情報資産へのアクセスに関するセキュリティを強化することができる。

（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）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、適切な利用者認証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、検疫システムやモバイルデバイス管理ツール（Mobile Device Management）がある。モバイル端末を学校内に持ち帰った場合等に、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よう、検疫システムによる確認を義務付けたり、MDMによるモバイル端末の状況を確認し、接続の可否を判断することなどにより、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。

1.6.3. 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「1.9 クラウドサービスの利用」の記載も参照しつつ、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ならびに使用したオープンソースのバージョン（リポジトリ）を適切な方法で保管しなければならない。

（５）情報システムにおける入出力データの正確性の確保

①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30年2月28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

1.6.4. 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などにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

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

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

④所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

⑤不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

⑥不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

⑦業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

（２）教育情報システム管理者の措置事項

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

①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を守るため、コンピュータウイルス等の不正プログラムへの対策を講じなければならない。

②不正プログラム対策は、常に最新の状態に保たなければならない。

③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。 なお、不正プログラム対策ソフトウェアに限らず、ハードウェア、オペレーティングシステムによって、システム改変検知や不正プログラムの侵入を防止するケースもある。

（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。なお、今般では個人データを盗取した後にランサムロックを掛けて身代金を要求する二重恐喝被害事例も増えているため、より一層の注意が必要である。

（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、不正な挙動等を検知し、早期

対処する仕組みを構築することに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。なお、端末のリソース状況・実現したい機能・コストを鑑みて検討すること。

（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。

1.6.5. 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及びSSID（無線LANネットワーク名）を閉鎖しなければ

ならない。

②不要なサービスについて、機能を削除又は停止しなければならない。

③不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、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所管するネットワークのサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（5）教職員等による不正アクセス

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

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

（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）

1.6.6. 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。

1.7. 運用

クラウドサービスの利用においては、本項及び「1.9　クラウドサービスの利用」を踏まえて確認・検討すること。

1.7.1. 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、教職員の不正な利用、自らのシステムが他の情報システムに対する攻撃に悪用されること等を防ぐためには、ネットワーク監視等により情報システムの稼働状況について常時監視を行うことが必要である。したがって、情報システムの監視に係る対策について規定する。

【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、重要性分類Ⅱ以上の情報資産を格納する校務系システム及び校務外部接続系システムを常時監視しなければならない。

④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、重要性分類Ⅲ以上の情報資産を格納する学習系システムを常時監視しなければならない。【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教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及びクラウドサービスでの管理が望ましい。

（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。

1.7.2. 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。

1.7.3. 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。

1.7.4. 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。

1.7.5. 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)

③著作権法（昭和45年法律第48号)

④不正アクセス行為の禁止等に関する法律（平成11年法律第128号)

⑤個人情報の保護に関する法律（平成15年5月30日法律第57号)

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

⑦サイバーセキュリティ基本法（平成26年法律第104号)

⑧○○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。

1.7.6. 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、地方公務員法をはじめとするによる懲戒処分の対象とする。

（２）違反時の対応

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

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。

1.8　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。なお、クラウドサービスを利用する場合は、「1.9クラウドサービスの利用」を参照すること。

【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】

（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）外部委託事業者を選定する際に参照できる規格である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）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７）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８）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「1.11.1 監査（４）外部委託事業者に対する監査」を参照されたい。

1.9. クラウドサービスの利用

1.9.1. 学校現場におけるクラウドサービスの利用について

ガイドライン初版（平成 29 年 10 月 18 日策定）においては、オンプレミスやプライベートクラウドの利用を想定した内容であった一方、パブリッククラウドサービスについては、利用を禁止してはいないが、機密性が低い情報資産に限定し、積極的な活用に向けた記述ではなかった。

令和元年 12 月版の改訂では、パブリッククラウドの特性を踏まえ、「1.9　クラウドサービスの利用」として、パブリッククラウドの利用に向けた考え方を追記した。

具体的には、パブリッククラウドサービスの積極的な活用に向けて、パブリッククラウドにおいて重要性の高い情報資産を取り扱うことも想定し、その特性に基づくメリット及び留意点、さらにその留意点を踏まえつつセキュリティ確保に関して検討・確認することが望ましい事項を記載した。

本項においては、学校現場におけるクラウドサービスの利用に関する考え方を示しており、基本的には、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2018年6月7日　各府省情報化統括責任者（CIO）連絡会議決定）の内容を参考にしている。

（1）教育システムにおけるクラウドサービスの定義

※　クラウドサービスの定義に関する詳細については、巻末＜参考＞を参照のこと。

クラウドサービスとは、クラウドコンピューティングを利用したサービスである。

クラウドコンピューティングは、共用の構成可能なコンピューティングリソース(ネットワーク、サーバ、ストレージ、アプリケーション、サービス)の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続きまたはクラウド事業者とのやりとりで速やかに割当てられ提供されるものである。

- 教育システムにおけるクラウド

事業者等によって定義されたインターフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービス。

- 教育システムにおけるパブリッククラウド

学校や教職員や生徒が、必要な時に必要なだけ自由にリソースを特定のハードウェアや通信環境に依存せずに利用できる ICT サービス。

➢ 教育システムにおけるプライベートクラウド

サービス提供元の組織でのみ利用可能なクラウドサービスであり、リソースも自らによって制御する。政府内においては、政府共通プラットフォームや各府省独自の共通基盤、共通プラットフォーム等が該当する。

コミュニティクラウド及びハイブリッドクラウドは、パブリッククラウド又はプライベートクラウドの応用的な利用形態であることから、本項ではパブリッククラウドとプライベートクラウドの 2 形態について記述する。

参考：**コミュニティクラウドとハイブリッドクラウド**

コミュニティクラウドでは、クラウドサービスのインフラストラクチャは複数の組織で共有され、共通の関心事(使命、セキュリティ上の必要、ポリシーまたは法令遵守の観点から)をもつ特定の共同体の専用使用のために使われる。例えば､統合型校務支援システムをクラウドサービス化して、複数自治体の学校が共同利用する場合は、コミュニティクラウドと言える。管理はその共有組織が行う場合も第三者の場合もあり、設置場所は組織の施設内または外部の場所となる。

ハイブリッドクラウドでは、クラウドサービスのインフラストラクチャは二つ以上の異なるクラウドインフラ(プライベート、コミュニティまたはパブリック)の組み合わせである。各クラウドサービスは独立した存在であるが、標準化された、あるいは固有の技術で相互に結合され、データとアプリケーションの移動可能性を実現している。

（2）クラウドサービスのメリット

① 効率性の向上

多くのクラウドサービスでは、共用の物理又は仮想的リソース（サーバ、ストレージ、ネットワーク機器等）を用いて情報処理環境をサービス提供するため、複数の利用者が物理リソースを共有する。さらにパブリッククラウドサービスの場合は、マルチテナント設計による隔離を前提に多くの利用者で共有するため、費用負担の軽減効果は大きい。

また、多くの場合、クラウド事業者が計画的に用意した物理リソースを仮想化設定することでサービス提供可能であること、多様な基本機能があらかじめ提供されていることなどから、導入時間を短縮することが可能となる。

⇒ クラウドサービスを利用することで、教育委員会自らがサーバ等を用意する（オンプレミス）ことがなく、初期費用を大幅に抑えられることから、ICT 環境への投資可能額が比較的乏しい小規模の教育委員会においても、導入促進が期待される。（ただし、クラウドサービスにおいてはシステム稼働に伴う費用（機器設置環境、人件費等）を含めてのサービス価格設定となるため、従来のオンプレミス環境の保守・運用費への影響も踏まえ、長期的な視点でのコスト比較・検討を行うことが必要。）

⇒ 安定したクラウドサービス利用環境を構築することを目的として、複数年契約を考慮した予算措置等の工夫をすることが求められる。

② セキュリティ水準の向上

セキュリティ水準が第三者認証等によって担保されたクラウドサービスは、一定水準の情報セキュリティ機能を基本機能として提供しつつ、より高度な情報セキュリティ機能の追加も可能としている。多くの情報システムにおいては、オンプレミス環境で情報セキュリティ機能を個々に構築するよりも、クラウドサービスを利用する方が、その激しい競争環境下での新しい技術の積極的な採用と規模の経済から、効率的に情報セキュリティレベルを向上させることが期待される。

⇒ サーバ等の管理を教育委員会・学校が行うのではなく、専門的な知識を有し、かつ最新の情報に基づく情報セキュリティ対策を随時実施するクラウド事業者に一定程度委ねることができるため、より効率的・効果的に情報セキュリティを担保することが可能となる。

③　技術革新対応力の向上

多くのクラウドサービスでは、最新技術を活用し、試行することが容易であるため、技術革新対応力が高い。そのため、様々な特長を有する教育系クラウドサービス（例えば、デジタルコンテンツ、協働学習ツール、個別学習向けデジタルドリル等）が次々と登場している。

⇒　学校現場において、現場に適したクラウドサービスを選択し、活用することが可能となってきている。目的に応じて新しい機能や特長を持ったクラウドサービスを使い分けることも可能で、日進月歩で進化する新しいサービスの取り入れが容易である。

④　柔軟性向上

多くのクラウドサービスは、リソースの追加、変更等が容易であり、数ヶ月の試行運用といった短期間のサービス利用にも適している。また、一般に汎用サービス化した機能の組合せを選択する等の対応によって、新たな機能の追加のみならず、業務の見直し等の対応が比較的簡易に可能となるほか、従量制に基づく価格が公表されていることから、値下げ競争が起きている状況にある。

⇒　クラウドサービス利用により、情報システムの導入準備期間が短縮され、途中からのリソース拡張や機能追加が容易であるため、教育委員会・学校では、スモールスタートで利用し、その後の状況に合わせて必要な分の拡張が柔軟に可能である。

⑤　可用性・完全性の効率的確保

クラウドサービスにおいては、仮想化等の技術により、複数の物理サーバのリソースを統合されたリソースとして利用でき、統合されたリソースの中で、利用者が必要なリソース分だけ柔軟に設定することができる。その結果、24 時間 365 日の稼働で、バックアップを前提とした場合でも過剰な投資を行うことなく、個々の物理的なリソースの障害等がもたらす情報システム全体への悪影響を極小化しつつ、大規模災害の発生時にも継続運用が可能となるなど、情報システム全体の可用性を向上させることができる。

⇒　教育委員会自らがシステムを管理するよりも、より強固な環境下での情報資産の管理を行うクラウドサービスを利用することで、災害による情報の破損・消失のリスクを低減するなど、より効率的に、可用性・完全性を確保することができる。なお、クラウドサービスにおける可用性や完全性の担保はサービス契約内容や後述する SLA などにより違いがある、そのため実現したい機能や費用などを総合的に検討した上でどのようなサービスを利用するのかを検討する必要がある。

⑥　保守・運用稼働の削減

クラウドサービス利用では、クラウド側の保守・運用をクラウド事業者に一元的に任せることから、オンプレミスと比較して、教育委員会・学校の稼働を削減することができる。

⇒　クラウドサービスの利用により、情報システムの保守・運用についての教育委員会・学校負担を軽減することができる。

（3）クラウドサービスの特性に起因する留意点

クラウドサービスは、クラウドならではの特性に起因する留意点が存在する。クラウドサービスを利用する際は、国際的な規格であるクラウドセキュリティ認証等の取得・準拠状況を確認することや、後述する対策（1.9.2、1.9.3）を適切に講じることで、それらのリスクを最小限に抑えることが可能である。

特性１　マルチテナント

クラウドサービスは、物理リソースを複数の利用者が共用するため、クラウド利用者は、特定の利用者の振る舞いが他の利用者に影響を与えないよう、第三者の検証による国際標準への準拠状況を確認する等、適切な安全管理措置が行われていることを確認する必要がある。

特性２　サービス提供元のセキュリティ情報を確認

クラウドサービスは、サービス提供元のクラウド事業者内のみでサービス運営が完結しているものだけでなく、インフラ基盤を IaaS 事業者から供給を受けて、アプリケーションを SaaS として提供する事業者も存在する。

このような場合、クラウドサービスのセキュリティレベルは、SaaS 事業者が適切なセキュリティレベルを確保していることを確認する必要がある。(IaaS 事業者が堅牢なセキュリティ対策を実施していたとしても、SaaS 事業者の委託作業の中でセキュリティインシデントが発生すると、データの流出が発生したり、データにアクセスできなくなったりする可能性がある。）なお、セキュリティインシデントだけでなく、クラウドサービスに集約される教育データの取り扱いについても IaaS 事業者及び SaaS 事業者にて利用者の意図しない取り扱いをされることが無いよう留意する必要がある。

また、その確認作業においては、クラウドサービスの情報セキュリティの実態を、クラウド利用者自らが詳細に調査することは困難であることから、第三者による認証や各クラウドサービス事業者が提供している監査報告書を利用することが重要である。

特性３　グローバル展開

クラウドサービスによっては、管理する情報資産やシステムについて、日本の法令が適用されないケースや、係争時における管轄裁判所が日本国外となるケースが存在し、情報資産の保全に影響することがある。クラウドサービスの選択の際には、自らの情報資産の管理に日本の法令が適用されること、係争時における管轄裁判所が日本国内となることを留意する必要がある。

特性４　サービス利用型の外部委託構造

パブリッククラウド事業者の多くは、複数の利用者に対してある程度の定型的なサービスを提供するため、利用者からの過度に詳細なカスタマイズの要求には応えられないことがある。業務内容についてもクラウドサービスの利用を前提とした内容となるよう検討・整理した上で、自システム・業務の一部についてクラウドサービスを利用することが受け入れ可能かを確認する必要がある。

特性５　責任分界点

クラウドサービスは、クラウド事業者が提供するサービスを、クラウド利用者が目的に応じて選択・利用することから、クラウド事業者が管理責任を負う部分と、クラウド利用者が管理責任を負う部分を分けて考えることが重要である。一方で、契約や利用規約で示されるクラウド事業者との責任分界点が曖昧になり、サイバー攻撃などのセキュリティ侵害に対する責任や役割分担が不明確となる可能性があるため、適切にセキュリティ管理を行う観点から、それぞれの役割分担・責任分界点を明確にする必要がある。

特性６　サービスの継続性

クラウド事業者の経営方針などに起因して、一方的にサービスを停止する可能性もあることから、クラウドサービスを利用する場合には、利用停止等に係る契約上の規定を確認しておくことが必要である。

（４）クラウドサービス利用における安全性の担保

教育システムは、必要なサービスに応じて適切なクラウドサービスを選択することが求められる。クラウド利用者とクラウド事業者で、情報セキュリティ確保の役割分担を明確にしつつ、必要な情報セキュリティがクラウド事業者において確保され、かつ業務の信頼性や継続性を確保するための必要な対策がとられていることを確認することが重要である。本ガイドラインでは、下記の２つの観点からクラウドサービス利用における安全性の担保に向けて検討・確認することが望ましい内容を 1.9.2、1.9.3 項に示している。

①　クラウドサービスに求められる情報セキュリティ対策(1.9.2 項)

クラウドサービスを提供する情報システムの情報セキュリティ対策は、システム所有者であるクラウド事業者の権限と責任範囲となるため、クラウド利用者はクラウドサービス側のセキュリティ対策の多くをクラウド事業者に委ねる構造になる。そのため、クラウド事業者が講じる情報セキュリティ対策を、クラウド利用者が確認する形で安全性を担保する形になる。

なお、クラウドサービスに必要な情報セキュリティ対策は、クラウド事業者による対策だけでは完結せず、クラウド利用者自らが実施すべき対策があることに留意願いたい。

② クラウド事業者のサービス提供ポリシー等の確認(1.9.3 項)

クラウドサービス利用における安全性担保のためには、クラウド事業者が実施する情報セキュリティ対策に加えて、サービス提供ポリシーがクラウド利用者のセキュリティポリシーや内部統制に求められる事項に適合するか、クラウド事業者として適切にサービス提供できる管理体制を有しているか等を確認する必要がある。

なお、前述のとおり、クラウド利用者においては、自らの情報セキュリティポリシーを、クラウドサービスの利用を前提とした内容に改めることが大前提である。

（5）クラウドサービスの情報セキュリティを把握するための第三者認証等の活用

クラウドサービスの情報セキュリティの実態を、クラウド利用者自らが詳細に調査することは困難であることから、クラウドの利用に関しては、第三者による認証や各クラウドサービス事業者が提供している監査報告書を利用することが重要である。

クラウド事業者の選定においても、求める内容に応じた認証規格を参考にすることで、1.9.2、1.9.3 項に示したクラウド事業者の責務と対策を履行できる能力を持ち、情報セキュリティの確保等が適切に行われていると判断することが可能である。これらの取得・準拠の状況を踏まえ、クラウドサービスのセキュリティ対策・内容等を確認していくことが、円滑な導入に有効である。

＜認証制度の例＞

- ISO/IEC 27001(情報セキュリティマネジメントシステム)
- ISO/IEC 27002(情報セキュリティマネジメントシステム)
- ISO/IEC 27014(情報セキュリティガバナンス)
- ISO/IEC 27017(クラウドサービスの情報セキュリティ)
  https://isms.jp/isms-cls/lst/ind/index.html
- ISO/IEC 27018（クラウドサービスにおける個人情報の取扱い）
- 米国 FedRAMP
  https://marketplace.fedramp.gov/#/products?status=Compliant
- AICPA SOC2（日本公認会計士協会 IT7 号）
- AICPA SOC3（SysTrust/WebTrsuts）（日本公認会計士協会 IT2 号）
- JASA クラウドセキュリティ推進協議会 CS ゴールドマーク
  http://jcispa.jasa.jp/cs_mark_co/cs_gold_mark_co/
- ASP・SaaS 安全・信頼性に係る情報開示認定

（6） 自組織の内部統制基準や情報セキュリティポリシーとの適合性の確保

現在の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おいては、「データセンターを（目視で）確認すること」など、クラウドサービスの利用にはなじまない内容となって

いるケースがあることから、クラウド利用者は、自らの情報セキュリティポリシーを、クラウドセキュリティに関する認証や、クラウド事業者が提供する監査報告書を利用する等、クラウドサービスの利用を前提とした内容に改める必要がある。その上で、クラウド事業者のサービス提供基準が自組織の内部統制基準や情報セキュリティポリシーを満たしていることを確認する必要がある。

1.9.2　クラウドサービスの利用における情報セキュリティ対策

【趣旨】

校務系システム、学習系システムにおいてクラウドサービスを利用する場合、クラウドの利用者である教育委員会等（以下、「クラウド利用者」と言う。）は、クラウド事業者（以下、「クラウド事業者」と言う。）が、自らの情報資産を預けるに値する安心安全で信頼できるパートナーであることを慎重に確認しなければならない。

※　本項における「クラウド利用者」とは、クラウドサービスの選定・契約の主体となり得る者（主に教育委員会）を想定している。教職員や児童生徒は、別途、「エンドユーザ」として整理する。

クラウドサービスにおいて情報セキュリティを確保するためには、クラウド事業者が協働して情報セキュリティ対策を構築することが必要となる。

そこで、クラウド利用者は、クラウドサービスを提供する全てのクラウド事業者（IaaS/PaaS を運用事業者を介して利用する場合は運用事業者と分担）が役割分担して総合的な情報セキュリティ対策を講じているかを確認する必要がある。

具体的には、SaaS 事業者の多くは IaaS/PaaS 事業者が供給するインフラ基盤やプラットフォーム基盤上でサービスを提供している。一方、本ガイドラインの中にはインフラ基盤やプラットフォーム基盤に関するものも存在する。その場合は、SaaS 事業者が自らのサービスのセキュリティに加え、責任をもって IaaS/PaaS 事業者によるインフラ基盤やプラットフォーム基盤を確認し、クラウド利用者に回答することが望ましい。なお、SaaS 事業者と IaaS/PaaS 事業者間の契約などにおいてはクラウド利用者がその内容を確認することが困難であることも考えられる。そのため SaaS 事業者と IaaS/PaaS 事業者間のセキュリティ対策においても本ガイドラインを準拠していることを求めることで確認することも有効である。

クラウド事業者の選定においては、1.9.1（５）で例示した認証規格を参考にすることで、情報セキュリティの確保等が適切に行われていると判断することが可能である。

なお、本項 1.9.2 及び次項 1.9.3 においては、クラウド事業者を SaaS 事業者、すなわち、自らのサービスのセキュリティに加え、IaaS/PaaS 事業者によるインフラ基盤やプラットフォーム基盤のセキュリティを確認し、クラウドサービスを提供している事業者であると設定し、クラウド利用者がクラウド事業者に求める事項と、クラウド利用者自らが実

施すべき事項との組み合わせで、クラウド利用者が有するべき規定を例示している。

【例文】

（1）利用者認証

① クラウド利用者は、クラウド事業者における当該クラウドサービスを提供する情報システムの運用もしくは開発に従事する者又は管理者権限を有する者について、適切な利用者確認がなされていることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	
② クラウド利用者は、当該クラウドサービスのログインに関わる認証機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	
③ クラウド利用者側管理者権限を有する者の ID の管理について、1.6.2 例文(1)③を遵守しなければならない。	

（2）アクセス制御

① クラウド利用者は、当該クラウドサービスに対して、アクセスする権限のない者がアクセスできないように、システム上制限する機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	
② クラウド利用者は、クラウド事業者の提供するアクセス制御機能を用いて、情報資産毎に、許可されたエンドユーザのみがアクセスできる環境を設定しなければならない。	

（3）クラウドに保管するデータの暗号化

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

（４）マルチテナント環境におけるテナント間の安全な管理

① クラウド利用者は、複数のクラウド利用者がクラウドリソースを共用する環境において、特定のクラウド利用者に対して発生したセキュリティ侵害が、他のクラウド利用者に影響を与えないように対策が講じられていることを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	

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

① クラウド利用者は、当該クラウドサービスを提供する情報システムを監視し、セキュリティ侵害を検知することを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	
② クラウド利用者は、当該クラウドサービスを提供する情報システムのインターネット接続境界において、クラウド利用者以外による不正な通信・侵入を防ぐ措置を講じるとともに、外部脅威の侵入を検知し、防御する対策を講ずることを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	

（６）情報の通信経路のセキュリティ確保

① クラウド利用者は、教育情報システムのインターネット境界から当該クラウドサービスを提供する情報システムまでの情報の通信経路において、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準･手順等の整備、通信の暗号化等）をクラウド事業者に求め、合意のうえ、利用しなければならない。	
② クラウド利用者は、クラウド事業者が保守運用等を遠隔で行う場合の、保守運用拠点と管理区域間での通信回線及び通信回線装置の管理について、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準･手順等の整備、通信の暗号化等）をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	

（７）クラウドサービスを提供する情報システムの物理的セキュリティ対策

① クラウド利用者は、当該クラウドサービスのサーバ等の管理条件を 1.4.1（サーバ等の管理）に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	
② クラウド利用者は、クラウド事業者側の管理区域（サーバ等を設置）及び保守運用拠点の管理において、1.4.2（教育委員会等のサーバ室にサーバを設置している場合）に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	

（８）クラウドサービスを提供する情報システムの運用管理

① クラウド利用者は、クラウド事業者に対して、サービスの一時停止等クラウド利用者に影響があり得る運用手順の有無、有る場合にはクラウド利用者への影響範囲（時間、サービス内容)、連絡方法等について情報提供を求め、クラウド利用者が業務運営に支障がないことを確認し、合意しなければならない。また、クラウド事業者の設定不備等によるインシデント発生時にも同様の確認をしなければならい。【推奨事項】	
② クラウド利用者は、当該クラウドサービスにおけるサーバの冗長化について、1.4.1(2)に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	
③ クラウド利用者は、当該クラウドサービスにおけるデータバックアップについて、1.6.1(2)に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	
④ クラウド利用者は、当該クラウドサービスにおける情報セキュリティの確保や監査に必要なログの取得について、1.6.1(6)に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	

（９）クラウドサービスを提供する情報システムのマルウェア対策

① クラウド利用者は、クラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等について、マルウェア対策を講じることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	
② クラウド利用者は、内部システムに侵入した攻撃を検知して対処するために、通信をチェックする等の対策を講じることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	

（10）クラウド利用者側のセキュリティ確保

① クラウド利用者は、クラウドサービスにアクセスする利用者側端末について、保管するデータの外部流出、改ざん等から保護するために必要な措置を講じなければならない。	
②クラウド利用者は、標的型攻撃による外部からの脅威の侵入を防止するために、エンドユーザへの教育や入口対策を講じなければならない。	

（11）クラウド事業者従業員の人的セキュリティ対策

① クラウド利用者は、クラウドサービスに関わるクラウド事業者従業員に対して、クラウド事業者の情報セキュリティポリシー及び保守運用管理規程等を遵守することをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	

② クラウド利用者は、クラウドサービスに関わるクラウド事業者従業員に対して、業務に用いるID及びパスワードその他の個人認証に必要な情報及び媒体について、部外者及び業務に関わらない従業員に漏えいすることがないように、適切に管理することをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	
③ クラウド利用者は、クラウドサービスに関わらない従業員等がクラウド利用者のデータを知り得る状態にならないよう、業務に関わるクラウド事業者従業員に対して秘匿を義務づけることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	
④ クラウド利用者は、クラウド利用者のデータ及びデータを格納した端末機器又は電磁的記録媒体の外部持ち出しについて、クラウド利用者の許可なく外部持ち出しできないこと及び外部持ち出しにおける安全管理手順をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	
⑤ クラウド利用者は、クラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等に、マルウェアを侵入させないよう、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。	

（12）データの廃棄等について

① クラウド利用者は、サービス利用終了時等において、クラウド利用者のデータが不用意に残置されないよう、適切に破棄するための流れについてサービス提供定款や契約書面上で確認または合意しておかなければならない。	

② クラウド利用者は、サービス利用終了時等におけるデータの扱いについて、スムーズに回収、次期システムへの移行等を行えるよう、その措置の流れについてサービス提供定款や契約書面上で確認または合意しておかなければならない。	

【解説】

（1）利用者認証

①、③　クラウド事業者、利用者に関わらず、クラウドサービスにおいて認証情報が漏えいした場合のセキュリティ侵害の影響度が甚大であることから、適切な本人確認が行われていることが必要。例えば、クラウドサービスへのログイン及び端末へのログイン時における多要素認証や、管理者が操作するエリアへの入退室の厳格な管理等があげられるが、具体的な手法については事業者によって異なることに留意すること。

② クラウドサービスへのログインにおける利用者認証は、権限のない者によるなりすまし及びマルウェア感染した端末からの不正アクセスを防御する上で必要な機能である。特に、インターネット接続前提の端末で重要な情報資産を扱う場合は、ID・パスワード認証に加え、多要素認証による対応など、より強度の高い認証方式を採用しなければならない。

（注１）教職員等のクラウドサービスへのログインにおける個人認証は、なりすましによる不正アクセスに対する防御として必要な機能である。特に重要な情報資産を取り扱う場合は ID・パスワード認証に加え、多要素認証を導入するなど、ネットワークの構築状況を踏まえつつ適切なセキュリティ対策を行うことが重要である。

（２）アクセス制御

アクセス制御は、あらゆるセキュリティ侵害に対して、その被害を最小範囲に留める有効な手段である。そのため、クラウド事業者によるアクセス制御機能の提供とクラウド利用者による適切なアクセス権限の設定は必須な対策である。

なお、適切なアクセス権限設定を行うためには、情報資産を適切に分類し、情報資産毎に最小限のアクセス権限のみを付与することを原則とする必要がある。

（３）クラウドに保管するデータの暗号化

データの暗号化については、特にインターネット接続環境において重要な情報資産を扱う場合における情報漏えいを前提とした出口対策として有効である一方、その手段・方式によっては、高い情報処理能力が求められ、システムの処理能力が低下する等の副作用が生じることや、そのコストを総合的に考慮し、必要に応じてクラウド利用者が選択すること。

対策については、クラウド事業者が機能を提供する場合とクラウド利用者が自ら機能を整備する場合がある。クラウド利用者が整備する場合でシステム的に実施が困難な場合は、組織個別の暗号鍵を設定して暗号化機能を利用したり、セキュリティ強度は低下するが、教職員等（エンドユーザ）が取り扱うファイルやフォルダにパスワード設定する形で、情報漏えいや改ざんリスクに備えることも検討されたい。

（４）マルチテナント環境におけるテナント間の安全な管理

クラウドサービスでは、当該教育委員会以外の複数の利用者がリソースを共用するため、特定の利用者に対して発生したセキュリティ侵害が、他の利用者に対して影響を及ぼすことがないようにクラウド事業者は対策を講じる必要がある。

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

①～②　インターネットを通信経路とするクラウドサービスは、閉域網よりも、悪意を持った外部の脅威からの攻撃リスクが比較的高く、脅威の侵入に備えたセキュリティ対策を講ずる必要がある。

（６）情報の通信経路のセキュリティ確保

①　パブリッククラウドの利用において、情報の通信経路としてインターネットを用いる場合は、通信経路上での暗号化等の保護措置は必須であることから、クラウド事業者が提供する保護措置を確認し、利用しなければならない。

②　保守運用に用いる通信回線についても、送受信される情報の暗号化を行う等、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置が求められる。具体的な手法については、事業者によって異なることに留意すること。

（７）クラウドサービスを提供する情報システムの物理的セキュリティ対策

①～②　クラウドサービスを提供する情報システムの設置場所における物理的セキュリ

ティ対策は、教育委員会等のサーバ室と同等レベルが求められる。保守運用拠点へのセキュリティ侵害は、その被害が広範囲に及ぶことから、保守運用拠点がデータセンターとは別ロケーションの場合には、その物理的セキュリティ対策も①と同等の充分な堅牢性と入退室管理が求められる。

（８）クラウドサービスを提供する情報システムの運用管理

① 利用者増減に伴う仮想環境の設定変更、容量拡張、機能追加等において、サービスの一時停止や機能制限等が起こりうることから、クラウド利用者に影響する運用作業に関しての事前連絡や回復の連絡など運用フローを確認し、クラウド利用者側の業務への支障を最小限に抑える必要がある。なお、IaaS 事業者等からインフラの供給を受けている SaaS 事業者においても、インフラ供給者の保守・運用に伴うクラウド利用者への影響の有無、影響の範囲（内容、時間）等について把握し、クラウド利用者の告知が求められる。また、クラウド事業者による設定不備等によってセキュリティインシデントが発生する事例もあるため、利用しているサービスの正常性の確認やインシデント発生時には対応状況についてクラウド事業者へ情報を求めることも重要である。

②～④ クラウド事業者においても、サーバ冗長化（サービス可用性）、データバックアップ、ログ取得について、1.4 項及び 1.6 項の規定に準じた対策が必要である。詳細は各クラウド事業者が提供するサービス・対応を踏まえて検討すること。

ログ管理については、クラウド利用者の内部統制上、定期的な取得・管理が義務づけられる場合もあることから、監査やインシデント発生時における対応等、クラウドサービスにおけるモニタリング機能やインシデントの自動通知機能等も活用しつつ、必要に応じて、クラウド事業者にログの提出やログ管理レポートの提出を求める。

（９）クラウドサービスを提供する情報システムのマルウェア対策

クラウドサービスが悪意のある脅威に乗っ取られた場合、クラウド内に保管しているデータ全体に深刻なセキュリティ侵害が及ぶことから、その安全管理対策は最上位に位置付けられる。

既知のマルウェア対策に加えて、インターネットからの未知のマルウェア対策が重要になり、ネットワーク機器のログ監視を強化して、情報を外部に持ち出そうとするなどの正常ではないふるま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の対策が必要である。また、万が一、マルウェアが内部システムに侵入した場合の対策も必要である。

（10）クラウド利用者側のセキュリティ確保

ここでは、クラウドサービスを利用する上で、クラウド利用者として特に重要な点につ

いて再掲している。

クラウドサービスにアクセスする利用者側端末は、クラウドサービスを提供する情報システム同様、マルウェア対策及び重要な情報保管における保護措置が求められる。また、クラウド利用者は、一時的であっても、利用者側端末に重要な情報が保管される場合は、悪意のある外部脅威の侵入リスクに備えて、該当情報に暗号化等の安全管理措置を講じる必要がある。

(11) クラウド事業者従業員の人的セキュリティ対策

クラウド事業者は、クラウド利用者のデータを預かる責務として、業務に関わる従業員の過失や不正行為により、データの機密性・完全性・可用性が脅かされる状態を排除しなければならない。そのために従業員に求めるセキュリティ遵守事項として、①クラウド事業者のセキュリティ規定等の遵守、②ID/パスワード等個人認証に必要な情報の適切な管理、③利用者データ取り扱いにおける秘匿、④利用者データの外部持ち出しにおける適切な管理、⑤従業員によるサーバや端末へのマルウェア感染の抑止が必要になる。

(12) データの廃棄等について

① 不完全なデータの廃棄は外部への情報漏洩につながるため、クラウド事業者に預けた個人を特定しうるデータの消去及びデータを格納した機器・媒体等の廃棄について、規約、プライバシーポリシー、契約要件等によってその措置について確認しておかなければならない。また、ストレージ等の物理マシンの保守交換時においても、データを消去しないまま作業が行われないよう、保守作業時におけるデータの消去を確実に行うことも必要である。

（可能であれば、データを格納した機器・媒体等の廃棄を確実にする手順を確認しておくことが望ましい。）

なお、データの特性や重要性に応じて、データの保存期限を決めておき、期限を過ぎたデータを定期的に消去することも重要である。

また、該当クラウドサービスが「NIST SP800-88(メディア廃棄)」に準拠しているかどうか、及び後述の 1.10 における宣言書を宣言しているかどうかを確認することが望ましい。

② クラウドサービスの利用終了後に預けたデータを回収することが必要になるが、その回収方法等についてはあらかじめ手順・方法を確認しておくことが必要である。

1.9.3　パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項

【趣旨】

クラウド利用者は、教育情報システムにパブリッククラウドサービスを利用する場合においては、クラウド事業者及び提供サービスに対する信頼性や内在するリスクを評価し、総合的に情報セキュリティを確保ができるクラウド事業者が提供するサービスを選定する必要がある。この観点からクラウド事業者のサービス提供ポリシーや体制等について確認・検証すべき事項について規定する。

クラウド利用者は、クラウドサービス及びクラウド事業者が保有するセキュリティリスクを踏まえ、自ら実施するセキュリティ対策と総合して関係法令、教育情報セキュリティポリシーが遵守できるかを評価する必要がある。なお、クラウド事業者の選定においては、1.9.1（5）で例示した認証規格を参考にすることで、情報セキュリティの確保等が適切に行われていると判断することが可能である。

【例文】

（1）守秘義務、目的外利用及び第三者への提供の禁止

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

（2）準拠する法令、情報セキュリティポリシー等の確認

クラウド利用者は、クラウド事業者がどのような規範に基づいてサービス提供するか開示を求め、クラウド利用者の準拠する法令、情報セキュリティポリシーを確認し、それらとの整合を確認しなければならない。 （クラウド事業者の準拠する認証制度、個人情報保護指針、プライバシーポリシー、情報セキュリティに関する基本方針及び対策基準、保守運用管理規程　等）	

（3）クラウド事業者の管理体制

① クラウド利用者は、クラウド事業者に対して、情報セキュリティポリシー等の遵守を担保する管理体制が整備されているか、クラウド事業者の組織体制を確認し、合意しなければならない。 確認すべき項目例を下記に示す。 （ア） サービスの提供についての管理責任を有する責任者の設置 （イ） 情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者（システム管理者）の設置 （ウ） サービスの提供に係る情報システムの運用に関する事務を統括する責任者の設置	

（４） クラウド事業者従業員への教育

① クラウド利用者は、クラウド事業者に、従業員に対して個人情報保護等の関係法令、守秘義務等、業務遂行に必要な知識、意識向上のための適切な教育及び訓練を実施し、充分な知識とセキュリティ意識を醸成することをに求めなければならない。	
② クラウド利用者は、クラウド事業者に、従業員への上記育成計画、教育実績等の情報を提示させ、自らデータを管理する場合と同様の教育・訓練を実施しているかを確認しなければならない。	

（５） 情報セキュリティに関する役割の範囲、責任分界点

① クラウド利用者は、クラウド事業者の情報セキュリティに関する役割の範囲と責任分界点について開示するよう求めなければならない。	

② クラウド利用者は、クラウド事業者の情報セキュリティに関する役割の範囲と責任分界点がクラウド利用者側で講ずる情報セキュリティ対策の役割の範囲と整合することを確認し、合意しなければならない。	

（６）監査

① クラウド利用者は、クラウドサービスの監査状況、範囲・条件、内容等についてクラウド事業者に開示するよう求めなければならない。	
② クラウド利用者は、クラウド事業者によるクラウドサービスに関する監査レポート等を根拠にして、自らの関係法令、情報セキュリティポリシーと照らし合わせ、安全性が確保されているかについて確認しなければならない。	

（７）情報インシデント管理及び対応フローの合意

① クラウド利用者は、情報セキュリティインシデント管理に関する責任範囲と及びインシデント対応フローを、サービス仕様の一部として定めることについて、クラウド事業者に対して求めなければならない。	

② クラウド利用者は情報セキュリティインシデント管理に関する責任範囲と及びインシデント対応フローを検証しなければならない。	

（８）クラウドサービスの提供水準及び品質保証

① クラウド利用者は、クラウドサービスの提供水準（サービス内容、提供範囲等）と品質保証（サービス稼働率、故障等の復旧時間等）を確認するとともに、それらの水準・品質が、業務遂行に求められる要求水準を満たすことを確認し、合意しなければならない。	

（9）クラウド事業者の再委託先等との合意事項

① クラウド利用者は、クラウド事業者と合意したサービス履行内容及び情報セキュリティ対策について、クラウド事業者自らが実施する内容と、再委託先等に委託する内容も含めて提示することをクラウド事業者に求めなければならない。また、サプライチェーンリスク対策が適切に講じられていることをクラウド事業者に求めなければならない。	
② クラウド利用者は、①の提示内容が、クラウド事業者と合意したサービス履行内容及び情報セキュリティ対策と整合していることを確認しなければならない。	

(10) その他留意事項

① クラウド利用者は、クラウド事業者がサービスを安定して提供可能な企業・団体であるかについて考慮しなければならない。	

② クラウド利用者は、クラウド事業者間でのデータ形成の互換性が必ずしも保証されている訳ではないことから、事業者を変更する際のデータ移行の方法などについて、クラウド事業者にサービス提供定款や契約書面上で確認または合意しなければならない。	
③ クラウド利用者は、クラウド事業者に対して、クラウドサービスにおいて扱う情報資産や情報システム等について、日本の法令が適用されること及び係争等における管轄裁判所が日本国内であることを確認すること。	

【解説】

（1）守秘義務、目的外利用及び第三者への提供の禁止

クラウド事業者は、クラウド利用者のデータを預かる立場であるため、守秘義務を遵守するとともに、同意のない目的外利用及び第三者への提供は行ってはならない。

また、クラウド事業者は、自社のサービスの提供に従事する要員に対して、就業中に取り扱った情報に関する守秘義務、目的外利用及び第三者への提供の禁止条項を、雇用契約又は派遣契約に含めなければならない。なお、退職時又は契約終了時以降の守秘義務についても同契約に含めなければならない。

（2）準拠する法令、情報セキュリティポリシー等の確認

前述のとおり、現在の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おいては、「データセンターを（目視で）確認すること」など、クラウドサービスの利用にはなじまない内容となっているケースがあることから、クラウド利用者は、自らの情報セキュリティポリシーを、クラウドサービスの利用を前提とした内容に改めた上で、クラウド事業者の規範と照らし合わせなければならない。

なお、法令、セキュリティポリシー等の遵守義務の実効性を担保するため、クラウド事業者に課せられるセキュリティポリシー等の遵守義務を怠った場合の損害賠償規定内容を確認しておくことが必要である。

（注1）クラウドに保管するデータの著作権については注意が必要である。アプリケーションやコンテンツ等で他者の著作物を複製してクラウドに保管する場合は、当該複製行為が契約違反や著作権侵害に相当しないことを確認しておくことが必要である。（オンプレミスのサーバ用に購入したアプリケーションのライセンスを、クラウド上のサーバにインストールすることを認めていないソフトウェアベンダもあるため、注意が必要）

（注2）クラウド利用者のデータの知的財産権について、帰属先をクラウド事業者とする場合があるので、クラウド利用者の不利益にならないよう契約内容等を十分に確認すること。

（3）クラウド事業者の管理体制

クラウド事業者が合意した内容を確実に遂行できるガバナンスを保有していることを確認する上で、適切に従業員、管理者が配置されている等、クラウド事業者の管理体制を確認することが有効である。

また、クラウド利用者とクラウド事業者は情報セキュリティの役割を分担するため、双方で管理体制を確認・共有し、円滑に連絡をとることができ

る体制を整備しておく必要がある。

（4）クラウド事業者従業員への教育

クラウド事業者の従業員は、仮想環境の運用等で高度な専門スキルが求められる。また同時に、サイバー脅威とその防御策等情報セキュリティに関する専門性も求められるため、従業員のスキルやセキュリティ意識の育成はクラウド事業者の業務信頼性に直結するといって過言ではない。セキュリティインシデントの多くは、人的な不正行為や過失により生じることから、クラウド事業者従業員の育成方針や教育計画について確認する必要がある。

（5）情報セキュリティに関する役割の範囲、責任分界点

責任分界点が曖昧なままサービス利用することは、脆弱性を放置し、セキュリティ侵害を誘発する危険性が高いため、事前のすり合わせが重要である。また、クラウド事業者が機能を提供し、クラウド利用者が機能を利用するケース（例：利用者登録、アクセス制御）や運用事業者がクラウド利用者の作業を行うケース等についても、クラウド利用者、クラウド事業者、運用事業者それぞれの役割の範囲を確認することが必要である。

（6）監査

クラウドにおける監査は、第三者の外部検査機関が評価し、安全性が確保されていることをクラウド利用者にレポート報告する形態等が想定される。クラウド利用者は、これらのレポートを自ら実施する監査結果と同等と見なして安全性を確保することが可能かを確認する必要がある。

「1.9.1　（6）自組織の内部統制基準や情報セキュリティポリシーとの適合性の確保」に示したとおり、機密性の観点から、クラウド利用者による直接監査（サーバルームを覗く等）ができない、データ保管場所を秘匿している場合があることから、自らのセキュリティポリシーをクラウドサービスの利用を前提とした内容に改めた上で、検討を行うこと。

（7）情報インシデント管理及び対応フローの合意

クラウド利用者はクラウド事業者によるログの定期的なチェック等の情報インシデント管理手順を合意しておくことが必要である。また、クラウド利用者内部不正によるインシデント発生等、クラウド事業者に対して、ログの提供等、原因究明に向けた調査協力を依頼する必要があるため、協力の範囲を合意しておくことも重要である。

（8）クラウドサービスの提供水準及び品質保証

利用しようとするクラウドサービスについて、利用規約、SLA（service

level agreement)、SLO（service level objective）などで示された水準等を、業務内容やコストと照らし合わせ、運用に支障がないことを確認すること。

（9）クラウド事業者の再委託先等との合意事項

クラウド事業者は、ITサプライチェーンを構成してサービスを提供する場合もあり、その場合にはクラウド事業者と再委託先等との関係において、サービス供給の停止、故意または過失による不正アクセス、セキュリティ管理レベルの低下などのリスクを考慮する必要がある。クラウド利用者は、これらのリスクに対して、クラウド事業者が合意した内容を確実に遂行できるガバナンスを保有していることを確認しておくことが望ましい。

(10) その他留意事項

① クラウド利用者が長期的に存続することを保証されている地方公共団体主体であること対して、クラウド事業者は民間企業であるケースが多く、企業存続リスク、一方的なサービス停止リスクについて、クラウド利用者の業務継続計画との整合性を確保する必要がある。

② サービス解約時のデータ返却方式や費用等、事業者を変更する際のデータ移行に関する条件を確認しておくことが望ましい。

③ クラウドサービスを利用にあたっては、クラウドサービス事業者の事業所の場所に関わらず、データセンターの所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、重要な情報を蓄積する場合には、日本の法令の範囲内で運用でき、係争時の管轄裁判所が日本国内となるクラウドサービスを選択する必要がある。

重要性が相対的に低い情報であっても、パブリッククラウドサービスを利用する場合には、どの国の法令が適用されるかを確認し、リスク等を考慮した上で選択すること。

1.9.4. 約款による外部サービスの利用

【趣旨】

本項でいう約款による外部サービスとは、インターネット上に約款を掲示し、同意した利用者に対して情報処理機能を提供するサービスであり、SaaS 型パブリッククラウドサービスの一種であるが、1.9.2 及び 1.9.3 で想定する個別契約締結型サービスとは別種であり、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除くものである。

原則、約款に提示された提供条件だけで利用を判断することになるため、リスクを十分踏まえて、利用に際して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、機密性の高い情報の取扱いには十分に留意するように規定しなければならない。

（ア）約款によるサービスを利用してよい範囲

（イ）業務により利用する約款による外部サービス

（ウ）利用手続及び運用手順

（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

前述のとおり、有料、無料に関わらず、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除き、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を想定しており、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

・ファイル転送サービス など

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ため、提示された約款の範囲で利用の可否判断が求められることが一般的である。

このようなサービスを利用する場合の主なリスクとして、以下のことが想定される。

① 利用者データの取り扱いについてのセキュリティ遵守事項（知りえた情報の秘匿義務、目的外利用の禁止、無許可での第三者への提供の禁止、安全な廃棄手順等）が約款に示されていない場合がある。

② 利用者データの利用権限がサービス提供者側に帰属することを前提にサービス提供する場合がある。

③ セキュリティインシデント調査等においては、利用者の当該サービスへのアクセス記録が必要になるが、利用者の求めに応じてアクセス記録を提供する等、利用者のインシデント対応に協力することが約款に示されていない場合が多い。

④ 当該サービスについて、物理的・人的・技術的セキュリティ対策等が約款に示されていないため、利用者データ保管における安全管理措置が不明な場合が多い。

⑤ 約款や利用規約が予告なく一方的に変更されたり、サービスが停止する可能性がある。

これらの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。

留意すべき事項としては、具体的には以下の項目が考えられる。

①約款による外部サービスの利用手順を定める

・利用できる情報資産の範囲
・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、機密性の高い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

（注1）「サービス約款」を提示するサービス提供形態は一般的であり、約款を提示する形態のサービス全般が、そのまま本項の「約款による外部サービス」に該当するものではない。本項で規定する「約款による外部サービス」とは、個人向けのWebサービスを想定しており、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除くものである。

便利な反面、セキュリティ面での裏付けを確認できないことが多く、利用リスクが残るため、利用できる範囲を制限し、対策を講じた上で利用することを述べている。

（注2）　教職員等が学校において、個人アカウントにより無断で約款による外部サービスを取り扱うことはセキュリティポリシー違反であり、学校の情報セキュリティ管理をすり抜ける行為である。情報資産の重要性によっては外部漏えい事案に相当するため、教育情報セキュリティ管理者は充分注意が必要である。一概に利用を禁止するものではなく、教職員の私的利用を禁止し、情報セキュリティ管理者が教職員等の利用を把握できる状態にすることが重要である。そのためには、約款内容をふまえて残存するリスクを明らかにして、リスクが許容できる範囲で利用規定を整備し、教育委員会や学校が契約したサービスのみを教職員等に提供することが望ましい。なお、約款による外部サービスの利用については「政府機関・地方公共団体等における業務でのLINE利用状況調査を踏まえた今後のLINEサービス等の利用の際の考え方（ガイドライン）」（令和3年4月30日）を参照されたい。

（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。

・情報が分析され、漏えいすることを防ぐため、利用端末や送信元をインターネット上で匿名化する対策の導入を検討することや、グループメール等では、組織名を名乗らないといった運用面での対策を行うことが望ましい。
・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。

1.9.5. 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。

なお、データの保存を伴う場合には1.9.2及び1.9.3で想定する個別契約締結型サービスの検討を行うこと。

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

③利用するソーシャルメディアサービスごとの責任者を定めなければならない。

(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。

1.10. 事業者に対して確認すべきプライバシー保護に関する事項

【趣旨】

外部委託やクラウドサービスの利用に当たっては、事業者における個人情報の適切な管理が行われていることが必須であることから、個人情報の収集・利用範囲や管理期間、データの統制と所有の在り方等について、事業者に確認を行う必要がある。

これらの項目については、調達時においてサービスの過剰な排除にならないよう留意した上で、契約要件等として定めなければならない。

特に、ISO／IEC 27018 等第三者認証の取得の確認や、下記の「学習者のプライバシーに関する宣言書」等を参考にされたい。

なお、最新の情報については出典に記載したウェブサイトを確認すること。

※本項においては、学習システムに関するクラウドサービスを提供する事業者を「学習サービスプロバイダー」と呼称する

（1） 個人情報の定義

個人情報とは、学習者及びその保護者（以下「学習者等」といいます）に関する情報であって、氏名、性別、住所、生年月日、電話番号、メールアドレス等により、特定の学習者等を識別することができるものをいいます。

（2） 個人情報の取得

個人情報を取得するときは、適正かつ公正な手段により行い、利用目的をあらかじめ公表するか、または取得後速やかに学習者等に通知もしくは公表いたします。

（3） 個人情報の利用

利用目的の達成に必要な範囲内で､適正に学習者等の個人情報を取り扱います。 利用目的のために必要な場合を除き、個人プロファイルを作成しません。

（4） 利用目的

学習サービスプロバイダーが取得した個人情報は、当該学習サービスのためのみに利用するものとする。学習者等への当該学習サービスに関わらないターゲティング広告の目的には利用しません。利用目的の詳細は、学習サービスプロバイダーのプライバシーポリシーに明記します。

（5） 個人情報の第三者への提供

事前に学習者等から同意を頂いている場合、法令等により提供が認められている場合を除き、学習者等の個人情報を第三者に提供しません。たとえば、学習者等への

当該学習サービスに関わらないターゲティング広告の目的で個人情報を第三者へ提供しません。

（6） 不適切なポリシー等の変更禁止

教育機関または学習者等に対する明確な通知、あるいは公表なしに、学習者等のプライバシーポリシーの実質的な変更を行いません。個人情報保護法その他の法令に反するような変更は行いません。

（7） 個人情報の保持期間

学習サービスプロバイダーは、学習サービスの提供期間（利用者と合意した期間）が満了したときは、個人情報を廃棄・削除します。

（8） 個人情報の取扱いについての情報開示

収集する学習者等の個人情報の種類や、個人情報の利用目的、第三者提供、共同利用については、教育機関、学習者等が容易に理解できる表現にて、利用規約または学習者サービスプロバイダーのプライバシーポリシーで明確に示します。

（9） 利用者による個人情報の開示等の請求

個人情報を提供した教育機関または学習者等から、学習者サービスプロバイダーが保有する個人情報の開示・訂正・追加・削除および利用停止の要求があったときは法令に従い、速やかに対応いたします。

（１０）個人情報の適正管理

学習者等の個人情報は、細心の注意のもと、厳重に管理し、不正アクセス又は個人情報の紛失、破壊、改ざん、漏洩、盗難等のリスクに対し、適切な安全対策を講じます。また、個人情報を正確かつ最新の状態で管理します。

（１１）委託

学習サービスの提供について、その業務の全部又は一部を第三者に委託し、委託先に対して必要な範囲で学習者等の個人情報を提供する場合があります。この場合には、当該委託先との間で個人情報保護の契約を締結し、学習サービスプロバイダーと同等の義務を課し、個人情報保護法等を遵守するよう適切な監督を行います。

（１２）合併/事業譲渡

学習サービスプロバイダーの学習サービス事業が、合併、事業譲渡その他の事由により承継されたことに伴って、承継後の事業者が個人情報を取得した場合には、そ

れまでに収集された個人情報については承継後の事業者は同様の義務を負い、あらかじめ学習者等の同意を得ないで、承継前における個人情報の利用目的の達成に必要な範囲を超えて、個人情報を取り扱いません。

（１３）匿名加工情報の取り扱い

学習サービスプロバイダーは、 同意を得ない場合、匿名加工情報とせずに第三者へ提供しません。学習サービスの利用状況の分析等のため、匿名加工情報を作成する場合は、個人情報保護法等の法令に従い、個人情報を特定の個人を識別できないように加工して、「個人に関わる情報項目」「提供方法」を公表します。

※出典

・児童生徒のプライバシー誓約（https://studentprivacypledge.org/privacy-pledge/）
US の「Future of Privacy Forum」（研究機関）及び「Software＆Information Industry Association」（規格標準化推進団体）が運営する「生徒児童のプライバシーを保護するサービスプロバイダーの誓約」

・学習者のプライバシーに関する宣言書（https://giga.ictconnect21.jp/declare/）
一般社団法人 ICT CONNECT 21 が国内の個人情報保護法等に合わせた日本版の「学習者プライバシー宣言書」

1.11. クラウドサービス活用における個人情報について

【趣旨】

今般の法改正により、地方公共団体の個人情報保護制度についても全国的な共通ルールを規定するとともに、個人情報保護に万全を期すため、個人情報保護委員会が、公的部門を含め、個人情報の取扱いを一元的に監視監督する体制を確立することとなった。

改正法においては、現状一定の地方公共団体の条例において規定されているいわゆる「オンライン結合」に特化した形での制限規定は設けず、今後その解釈が示される安全管理措置や利用・提供の制限に係る規定等により、個人情報の安全性を確保することとされている。

また、地方公共団体において個人情報を取り扱う際に個人情報保護審議会への諮問答申を得ることとしている例があるところ、こうした審議会への諮問については、法律による全国的な共通ルールの下で、国のガイドライン等により制度の適正な運用が図られることから、個人情報の適正な取扱いを確保するため「特に必要である」ときに限って認めることとされている。

しかしながら、改正法が施行（※）されるまでの間は、個人情報を取り扱う際に、地方公共団体ごとに定められた個人情報保護条例に準拠する必要がある。

特にクラウドサービスを活用する際には個人情報を取り扱うケースも考えらえるため、自治体ごとに制定された手続きに沿って適切に対応する必要がある。

また、現状多くの地方公共団体では個人情報を取り扱う際に個人情報保護審議会への諮問答申を得ることとしている。そのため、当面、個人情報保護審議会へ諮問する際に整理すべき項目の例を示す。

※法の公布の日（令和3年5月19日）から起算して2年を超えない範囲内において政令で定める日から施行

【個人情報保護審議会に諮る上で整理すべき項目の例】

（1） クラウド活用の目的

主には、「児童生徒に対する学習活動目的」になると考えられるが、自治体として、当該システムの目的を明確にしておくことが重要。また、個人情報を取り扱う理由も明確化すること。

（2） システムの対象範囲

諮問に関わるシステムの対象範囲を明確にすること。新規のシステムでは全てが対象になること考えられるが、既存システムの一部にクラウドサービスを利用し、そこで個人情報を取り扱う場合などは、対象部分がわかるように整理することが求められる。

（3） 本人（保護者）同意の要否

本人（保護者）同意の必要性を確認すること。なお、同意を得ることにより個人情報保護審議会への諮問を不要としている自治体もあるため、自治体ごとに確認を行うこと。

（4） セキュリティリスクに対する技術的対策

想定されるリスクを洗い出し、それらのリスクに対してどのような技術的対策を講じているかを整理すること。

（5） インシデント発生時の責任分界点の明確化（クラウド事業者側の体制含む）

組織体制を明確化し、インシデント発生時の取り決めを整理すること。特に、SaaS 事業者はサービス提供の基盤として IaaS 事業者のサービスを利用しているケースが多いため責任分界点に留意する必要がある。

（6） クラウド事業者の二次利用に対する対策

個人情報提供先のクラウド事業者における二次利用に対する対策を整理する。契約内容で縛ることやクラウド事業者における「個人情報保護方針」及び「プライバシーポリシー」などを確認すること。

（7） クラウド事業者の第三者認証取得の有無

クラウド事業者において、セキュリティやプライバシーに関する第三者認証を取得しているかどうかを確認する。前述の 1.9.1 項に示した認証制度の例や 1.10 項に示した「児童生徒のプライバシー誓約」及び「学習者のプライバシーに関する宣言書」などを参考にすること。

1.12. １人１台端末におけるセキュリティ

1.12.1. 学習者用端末のセキュリティ対策

【趣旨】

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

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

また、学校外では、家庭等での学習継続のため、各家庭の無線LANやLTE等の移動体通信を用いて、Web会議システム等を利用した同時双方向の学習や健康観察の実施、クラウド環境のグループウェアや電子メール機能を活用した児童生徒・家庭等への課題の配信等、整備された端末を児童生徒が家庭等に持ち帰り、学習に活用する機会が多くなることも想定される。

これらを踏まえ、利用するネットワークや場所にとらわれないセキュリティ対策を講じることが必要である。

なお、児童生徒の所有するICT機器を活用するBYOD（Bring Your Own Device）についても、多様なICT端末の活用における有効な選択肢として検討する必要がある。

高等学校等において自治体が整備する端末とBYOD端末が同一の教育活動の中で使用されるケースも考えられるため、BYODを行う際には、本ガイドラインを参考にしつつ自治体が整備する端末の環境と同等のセキュリティ対策を講じる必要がある。

BYODについては今後の実証研究などを通して、引き続き環境整備の在り方を検討していく方針であり、本ガイドラインにも随時反映していく。

【例文】

（１）授業に支障のないネットワーク構成の選択（帯域や同時接続数など）

クラウドサービス提供事業者側のサービス要件基準を満たしたネットワーク構成を設計する。また、運用開始前には十分検証し、利用状況に応じて定期的に改修計画を行うこと。

（２）不適切なウェブページの閲覧防止

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

＜対策例＞

①フィルタリングソフト
②検索エンジンのセーフサーチ
③セーフブラウジング

（３）マルウェア感染対策
学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

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

（５）セキュリティ設定の一元管理
児童生徒への端末配布後においても、端末のセキュリティ設定やOSアップデート、ウェブブラウザのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状態確認などの作業を、離れた場所からでも一元管理できることが望ましい。

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

（７）運用・連絡体制の整備
学校内外での端末の運用ルールを制定し、インシデント時の連絡先対応方法を各学校にて整理しなければならない。

（解説）

（１）授業に支障のないネットワーク構成の選択（帯域や同時接続数など）
クラウドサービスでは、クラウドサービス提供事業者側のセキュリティ基準を満たしたサービスがインターネット上で提供される。その際、従来のネットワーク構成では円滑に授業を進めることに支障が出るケースがあるため、クラウド利用を前提としたネットワーク構成を再度選択する必要がある。なお、これらのクラウドサービス提供者側のセキュリティ基準は公開されていないケースが多いため、余裕を持ったネットワークの設計を行う必要がある。これらの代表例としては例えば次のようなものが

ある。

①グローバルIPアドレス

クラウドサービスに対し、同一のグローバルIPアドレスから短時間に多数の接続が行われた場合、クラウドサービス事業者側でロボット判定の実施や攻撃と認識しアクセスを一定期間停止させるといった措置を行うことがある。セキュリティの観点からクラウドサービス提供者側では基準を明確に提供していないことが多いが、運用を考慮して、本運用開始前に事前にテストをすることが必須となる。

②通信帯域

オンラインでの学習のみならず、学校内で画面共有や動画の配信等を行うことも想定し、利用するクラウドサービスで必要とされる帯域を確保することが重要になる。Web会議システム等で必要な帯域などクラウドサービスに関する要件はクラウドサービス提供者が公開しているが、設計上の理論値のみで判断することなく実運用を踏まえた上で設計を行う必要がある。また、これらに関しては本運用開始前に事前にテストをすることが必須となる。

（２）不適切なウェブページの閲覧防止

不適切なウェブページとは、違法な情報及び青少年有害情報を含むウェブページのことであり、インターネットを利用して公衆の閲覧（視聴を含む）に供されている情報であって青少年の健全な成長を著しく阻害するものをいい、例示すると、次のとおりである。

一　犯罪若しくは刑罰法令に触れる行為を直接的かつ明示的に請け負い、仲介し、若しくは誘引し、又は自殺を直接的かつ明示的に誘引する情報

二　人の性行為又は性器等のわいせつな描写その他の著しく性欲を興奮させ又は刺激する情報

三　殺人、処刑、虐待等の場面の陰惨な描写その他の著しく残虐な内容の情報

前述のとおり学校内外での利用を前提とした時に、利用するネットワークや場所にとらわれないセキュリティ対策を実施することが重要である。

なお、目的は児童生徒による不適切なウェブページの閲覧防止であるため、実現したい機能や実際の運用に応じて適切に整備することが重要である。これらの対策としては例えば次のものがある。

①フィルタリングソフト

端末に標準的に搭載された製品、インターネットサービスプロバイダーが提供する製品、セキュリティ事業者が提供する製品・サービスなどがある。

フィルタリングの方式は特定のURLを指定して閲覧を防ぐブラックリスト方式、特定のURLのみを閲覧許可するホワイトリスト方式、特定の情報が含まれる場合に閲覧を防ぐカテゴリ（コンテンツ）フィルタリング方式などがあるため、実現したい機能やフィルタリングの精度、実際の運用等を考慮して適切に整備すること。なお、フィルタリングは当初の設定だけではなく、利用上での設定変更等が必要となるため運用体制を整備することが望ましい。

また、不適切なウェブページの閲覧防止に加えて、コンテンツフィルタリングではカバーしきれない、日々増大するマルウェアサイトやC&Cサーバ、フィッシングサイト等の悪意あるサイトへの通信をブロックするなどのセキュリティ対策も重要である。

②検索エンジンのセーフサーチ

検索エンジンの検索結果に不適切な情報が含まれる場合に表示させないようにする機能であり、有害情報を閲覧する機会の低減に繋がる。

③セーフブラウジング

ウェブページ閲覧時に不正なサイトであることが疑われる場合、利用者に対して警告を表示する機能である。対象となるウェブサイトは主に2種類あり、1つはマルウェアなどの不正なソフトウェアをインストールさせようするウェブサイトであり、もう1つは正規のウェブサイトになりすまし、IDやパスワードを不正に入力させるフィッシングサイトである。利用者の判断が必要となるが、不正なウェブサイトへの接続対策となる。

（注１）フィッシングとは、実在するサービスやシステム、組織を語って、ログインIDやパスワード、個人情報等を盗み出す犯罪のこと。改ざんされたホームページやフィッシングメール等にリンクがあり、これをクリックすることで偽のホームページ（フィッシングサイト）に誘導し、IDとパスワードを入力させる。

（３）マルウェア感染対策

学校内外で児童生徒がインターネットを利用する際に、不正なウェブサイトによるマルウェア感染などのリスクが発生するため対策を講じる必要がある。主な対策としてはウイルス対策ソフトをインストールする、OSやウェブブラウザを含むソフトウェアを常に最新のバージョンにアップデートを行うことなどがある。

なお、OSによっては標準的にウイルス対策ソフトを備えている製品、OSとしてウイルス感染のリスクが低い仕組みとなっている製品などもあるため、実際に運用する端末において適切な対策を講じること。

（４）端末を不正利用させないための防止策

学習者用端末の利用においては、端末の端末認証やユーザ認証の徹底が求められる。また、学習者用端末の利用においては、端末のセキュリティ状態の監視に加えて、学習に不適切なアプリケーションやコンテンツの利用を制限し、教員の目の届かない環境下でも常に安全で児童生徒が安心して利用できる状態を維持しなければならない。

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

（５）セキュリティ設定の一元管理

児童生徒への端末配布後においても、端末のセキュリティ設定やOSやウェブブラウザを含むソフトウェアのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状態確認などの作業を、離れた場所からでも一元管理できることが望ましいため、MDM等によりセキュリティ制御を行うこと。ただし、実現したい機能・規模・コストを鑑みて柔軟に検討すること。

（６）端末の盗難・紛失時の情報漏洩対策

端末の盗難・紛失などのインシデントが発生した場合においても重要性が高い情報が漏えいすることが無いように対策を講じる必要がある。具体的にはデータの保存はクラウドサービスを利用することにより端末内部に情報を保存しないようにする運用や、MDMなどにより管理者が離れた場所からでも端末をロックする、あるいは必要に応じてデータの削除や端末の初期化を行うリモートワイプ機能などの対策を講じること。また、これらの機能を事前に周知すること自体が盗難、転売対策にもなる。

（７）運用・連絡体制の整備

1人1台端末の利活用において、学校側が規定している各種ガイドラインを児童生徒の保護者も正しく理解し、端末を活用する場所にかかわらず児童生徒の情報リテラシー教育を促すことは、学校として行うべき重要な活動である。特にインシデント発生時の報告に関してはマニュアル等を作成し周知徹底する必要がある。また、児童生徒に関しては定期的に報告手順の確認や報告の訓練を実施することが望ましい。

学校外での利用機会が増加することにより、盗難や紛失など情報セキュリティインシデントが発生件数の増加が危惧される。情報セキュリティインシデントが発生した場合の報告体制に関してマニュアル等を作成の上で対象者に周知徹底する必要がある。

1.12.2. 児童生徒における ID 及びパスワード等の管理

【趣旨】

GIGAスクール構想における1人1台端末の整備と併せて、児童生徒一人一人に個別のIDを付与することで、児童生徒の学びを蓄積し、教員やAIによるフィードバックが行われ、個別最適化された学びを提供することが期待できる。一方で、なりすまし等によるIDの不正使用や不正アクセスによる情報漏洩等のセキュリティリスクも考えられるため、利用する学習用ツールやクラウド上のアプリケーションのID/パスワードに対して安全管理措置を講じなければならない。例えば、パスワードに関しては定期的な更新を求める運用は廃止し、複雑性を満たすパスワードを設定の上、パスワードの流出を検出した際には速やかに新しいパスワードに変更しなければならない。

なお、クラウド上の学習用ツールごとに異なるID/パスワードでのログインが必要になるなど、学習面での利便性の低下が課題となることも考えられる。そこで、シングルサインオンを採用し、ID/パスワードなどによる認証を必要とする複数のシステム(アプリケーション)に対して、最初に1回だけ認証を行うことにより、その後の認証を全てシステムにより自動化する技術もある。

【例文】

（１）ID登録・変更・削除

①入学/転入時のID登録処理

IDについてはシンプル・ユニーク（唯一無二)・パーマネント/パーシスタント（永続的な識別）な構成要素になっていることや、児童生徒の発達段階に応じた複雑性を上げたパスワードポリシーによりセキュリティ強度を上げていくなど適切な措置を講じなければならない。

ID登録やパスワードポリシーにおいては情報セキュリティ対策として重要な要素であるため学校毎に管理するのではなく、同一の教育委員会等の組織にて一元管理することが望ましい。

②進級/進学時のID関連情報の更新

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

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

③転出/卒業/退学時のID削除処理

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

転出や卒業/退学時に学習用ツールのサービス利用期間が終了する場合は、あらかじめ児童生徒本人によるデータ移行をサービス利用期間内に実施し、IDの利用停止後、最終的にはID及び関連するデータの完全削除を行うこと。

ただし、本人同意や個人情報保護条例に従った適切な管理の下、一部のデータを活用することは可能である。

（２）多要素認証によるなりすまし対策

本人確認を厳格に行う必要がある場合においては児童生徒の ID/パスワードに加えて多要素認証を設定することが望ましい。

（３）学習用ツールへのシングルサインオン

学習履歴を活用したり、個人の成果物を保存するアプリケーションが増えてくると、サービス利用時に都度 ID/パスワード等の認証情報を入力したり、サービス毎のアカウント情報管理が非常に煩雑になるため、一度の認証により一定時間は各種サービスにアクセスが行えるシングルサインオンの導入を行うことが望ましい。

(解説)

（１）ID登録・変更・削除

①入学/転入時のID登録処理

入学/転入時や端末配布時にはID登録が完了している必要があり、ID登録においては必要が生じた時にID発行が完了していることが重要である。また、IDの命名規則においてはユニーク（唯一無二)・パーマネント/パーシスタント（永続的な識別）であることに加え、同一組織内における転入/転出時等にID変更を不要とするような命名規則（学校IDを含めないなど）とすることにより、情報管理の効率化及び認証情報の流出や更新漏れなどを防ぐことができる。

②進級/進学時のID関連情報の更新

IDはパーマネント/パーシスタント（永続的な識別）になるように考慮した上での命名規則のもと、ID変更については必要最小限になるような工夫が必要となる。そのため進級/進学時においてはIDそのものを変更するのではなく、IDに付随する属性情報を更新することにより、進級・進学に伴った適切なセキュリティポリシーの適用や、各種サービス利用がシームレスに行うことができるようにすることが重要である。

また属性情報については統合型校務支援システム等に最初に登録がされるものがほとんどであるため、各種児童生徒情報と連動したID管理を行うことで、IDのライフサイクル（IDの登録～停止～削除）を必要が生じた時に正確に行うことでセキュリティ確保を実現できる。なお、ID管理を日常的に運用する上で、必要に応じて事業者へ運用を依頼することも想定して環境整備の段階から運用面を踏まえた計画が必要である。

③転出/卒業/退学時のID削除処理

IDについては数字のみで構成したものや、児童生徒の氏名の一部を使うなど命名規則はさまざまであるが、ユニークなIDについては個人を識別できる可能性があるため、個人情報保護法の観点から個人情報に相当するとも考えられる。そのため個人のIDを集約した管理データは各自治体が制定する個人情報保護条例に照らした適切なID管理が求められている。

学習用ツールのサービス利用期間を超えて利用可能なIDの存在や、当該IDに付随する個人情報の保持や一部の継続利用においては、本人の同意や教育委員会による個人情報保護審議会の承認の下、IDや関連するデータの削除漏れがない適切な管理を実施する必要がある。

（２）多要素認証によるなりすまし対策

特にデータの秘匿性や完全性の確保が相応に求められる場合においては、児童生徒のID/パスワードに加え、多要素認証を設定し、本人確認を厳格に行うことが有効である。なお、多要素認証の設定においては、導入後の運用面（認証装置の配布方法や紛失対策など）について留意すること。

（３）学習用ツールへのシングルサインオン

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

そのため、シングルサインオンと認証情報の一元管理により、運用効率化と運用負荷の最小化、煩雑な運用によるセキュリティリスクを低減することが可能である。また、シングルサインオンに利用するID/パスワードは漏洩した際の影響範囲が大きいため、必要に応じて多要素認証と組み合わせることでよりセキュリティリスクを低減することができる。

1.13. 評価・見直し

1.13.1. 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、外部の専門家を充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、脆弱性の情報等重要性が高い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」（令和2年12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。

1.13.2. 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。

1.13.3. 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

【参考別表】　権限・責任等一覧表

※本一覧表は「参考資料　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参考例である。

※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
1．1 対象範囲及び用語説明				適用される行政機関、情報資産の範囲の定義及び用語説明											
1．2 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)	①		教育情報システム担当者の設置						○					
		②		教育情報システム担当者の担う役割					△	○					
	(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										○	
1．3 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			○				

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
1．4 物理的セキュリティ対策	1．4．1 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					○						
	1．4．2 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					○		△				
	1．4．3 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		○			○						
	1．4．4 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					○						

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
1．5 人的セキュリティ対策	1．5．1 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				○							△
	1．5．2 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									○		
	1．5．3 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	○										
	1．5．4 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							○				

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
1．6 技術的セキュリティ	1．6．1 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		○		△							

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
1．6 技術的セキュリティ	1．6．2 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					○						
	1．6．3 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					○						

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
1．6 技術的セキュリティ	1．6．4 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		○									
	1．6．5 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		○			○						
	1．6．6 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		○			○						

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
1．7 運用	1．7．1 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		○			○						
	1．7．2 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		○									
	1．7．3 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	○								○		
	1．7．4 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	○										
	1．7．5 法令遵守			主要な法令遵守								○			
	1．7．6 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	△	○			△						
1．8 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					○						
		（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	△	△			○						○

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
1．9 クラウドサービスの利用	1．9．1 学校現場におけるクラウドサービスの利用について	（1）		クラウドサービスのメリット											
		（2）		クラウドサービスの特性に起因する留意点											
		（3）		クラウドサービス利用における安全性の担保について											
		（4）		クラウドサービスの情報セキュリティを把握するための第三者認証等の活用											
		（5）		クラウドサービス利用の規定範囲											
		（6）		クラウドサービスの定義・分類											
	1．9．2 パブリッククラウドの利用における情報セキュリティ対策	（1）		個人認証					○						○
		（2）		アクセス制御					○						○
		（3）		クラウドに保管するデータの暗号化					○						○
		（4）		マルチテナント環境におけるテナント間の安全な管理					○						○
		（5）		クラウドサービスを提供する情報システムに対する外部からの悪意のある脅威の侵入を想定した技術的セキュリティ対策					○						○
		（6）		情報の通信経路のセキュリティ確保					○						○
		（7）		クラウドサービスを提供する情報システムの物理的セキュリティ対策					○						○
		（8）		クラウドサービスを提供する情報システムの運用管理					○						○
		（9）		クラウドサービスを提供する情報システムのマルウェア対策					○						○
		（10）		クラウド利用者側のセキュリティ確保					○						○
		（11）		クラウド事業者従業員の人的セキュリティ対策					○						○
		（12）		データの廃棄及びサービス利用終了時のデータ返却					○						○
	1．9．3 パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項	（1）		守秘義務、目的外利用及び第三者への提供の禁止					○						○
		（2）		準拠する法令、情報セキュリティポリシー等の確認					○						○
		（3）		クラウド事業者の管理体制					○						○
		（4）		クラウド事業者従業員への教育					○						○
		（5）		情報セキュリティに関する役割の範囲、責任分界点					○						○
		（6）		監査					○						○
		（7）		情報インシデント管理及び対応フローの合意					○						○
		（8）		クラウドサービスの提供水準及び品質保証					○						○
		（9）		クラウド事業者の再委託先及び供給者との合意事項					○						○
		（10）		その他留意事項					○						○
	1．9．4 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）		約款によるサービスの利用における対策の実施							○				
	1．9．5 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2A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					○						

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
1．10　事業者に対して確認すべきプライバシー保護に関する事項				事業者における個人情報の適切な管理					○						○
1．11 クラウドサービス活用における個人情報について				個人情報保護審議会に諮る上で整理すべき項目の例					○						
1．12　1人1台端末におけるセキュリティ	1．12．1　学習者用端末のセキュリティ対策	（1）		授業に支障の出ない構成の選択（帯域や同時接続数など）					○						
		（2）		不適切なウェブページの閲覧防止					○						
		（3）		マルウェア感染対策					○						
		（4）		端末を不正利用させないための防止策					○						
		（5）		セキュリティ設定の一元管理					○						
		（6）		端末の盗難・紛失時の情報漏洩対策					○						
		（7）		運用・連絡体制の整備					○		○				
	1．12．2　児童生徒におけるID及びパスワード等の管理	（1）	①	入学/転入時のID登録処理					○						
			②	進級/進学時のID関連情報の更新					○						
			③	転出/卒業/退学時のID削除処理					○						
		（2）		多要素認証によるなりすまし対策					○						
		（3）		学習用ツールへのシングルサインオン					○						
1．13　評価・見直し	1．13．1　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									○		
	1．13．2　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									○		
	1．13．3　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			情報セキュリティポリシー及び関係規程等の見直しに関する規定									○		

【参考】クラウドサービスの定義・分類
（「政府機関等の情報セキュリティ対策のための統一基準　平成 30 年度版」を参照）

① クラウドサービスとは

クラウドサービスとは、クラウドコンピューティングを利用したサービスである。

クラウドコンピューティングは、共用の構成可能なコンピューティングリソース(ネットワーク、サーバ、ストレージ、アプリケーション、サービス)の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続きまたはクラウド事業者とのやりとりで速やかに割当てられ提供されるものである。

このクラウドモデルは 3 つのサービスモデル、および 4 つの実装モデルによって構成される。

② クラウドのサービスモデル

一口にクラウドサービスと言っても様々な形態がある。クラウドが提供するサービスは、その構成要素から大きく　SaaS(Software as a Service)、PaaS(Platform as a Service)、IaaS（Infrastructure as a Service）の 3 種類がある。

ア　SaaS

クラウド事業者がアプリケーションプログラムを持つ機能を提供するサービスである。クラウド利用者は、Web ブラウザ、モバイルアプリまたは軽量のクライアントアプリからアクセスする。クラウド利用者はインターネット経由でアプリケーションを利用する立場であり、学習系分野では、タブレット向けのデジタルドリル、協働学習支援、デジタルコンテンツ配信等各種サービスが提供されている。校務系分野では、学校ホームページ作成、緊急連絡網等のサービスが提供されている。

クラウド利用者が独自にシステム構築することなく利用可能であるため、最も普及しているモデルと言える。

イ　PaaS

クラウド事業者が OS やミドルウェアを含めたプラットフォームを提供するサービスである。PaaS の特徴は、クラウド利用者が下位層のサーバ、ネットワークその他のインフラを管理しない点である。

ウ　IaaS

クラウド事業者がサーバやストレージ、ネットワークなどのハードウェアが提供する機能を仮想環境として提供するサービスである。

教育委員会等が、地域ごとの具体的な運用形態、学校数等を踏まえ、IaaS 基盤の上に、OS、ミドルウェア、アプリケーション等を導入して専用システムを構築することが可能である。

実際には、情報システムの設計・開発並びに運用及び保守を併せて担う運用事業者を介してIaaS 基盤を活用していく場合が多い。

③　クラウドの実装モデル

クラウドサービスはその利用形態によって、パブリッククラウド、プライベートクラウド、コミュニティクラウド、ハイブリッドクラウドの 4 つに分けられる。

ア　パブリッククラウド

クラウドサービスのインフラストラクチャはクラウド事業者の所有で、データの存在場所としてはそのクラウド事業者の施設内となり、複数のクラウド利用者が共同で利用する形態である。

イ　プライベートクラウド

クラウドサービスのインフラストラクチャは単一の組織の専用使用のために提供される。管理はその組織が行う場合も第三者の場合もあり、設置場所は組織の施設内または外部の場所となる。

ウ　コミュニティクラウド

クラウドサービスのインフラストラクチャは複数の組織で共有され、共通の関心事(使命、セキュリティ上の必要、ポリシーまたは法令遵守の観点から)をもつ特定の共同体の専用使用のために使われる。例えば､統合型校務支援システムをクラウドサービス化して、複数自治体の学校が共同利用する場合は、コミュニティクラウドと言える。管理はその共有組織が行う場合も第三者の場合もあり、設置場所は組織の施設内または外部の場所となる。

エ　ハイブリッドクラウド

クラウドサービスのインフラストラクチャは二つ以上の異なるクラウドインフラ(プライベート、コミュニティまたはパブリック)の組み合わせである。各クラウドサービスは独立した存在であるが、標準化された、あるいは固有の技術で相互に結合され、データとアプリケーションの移動可能性を実現している。

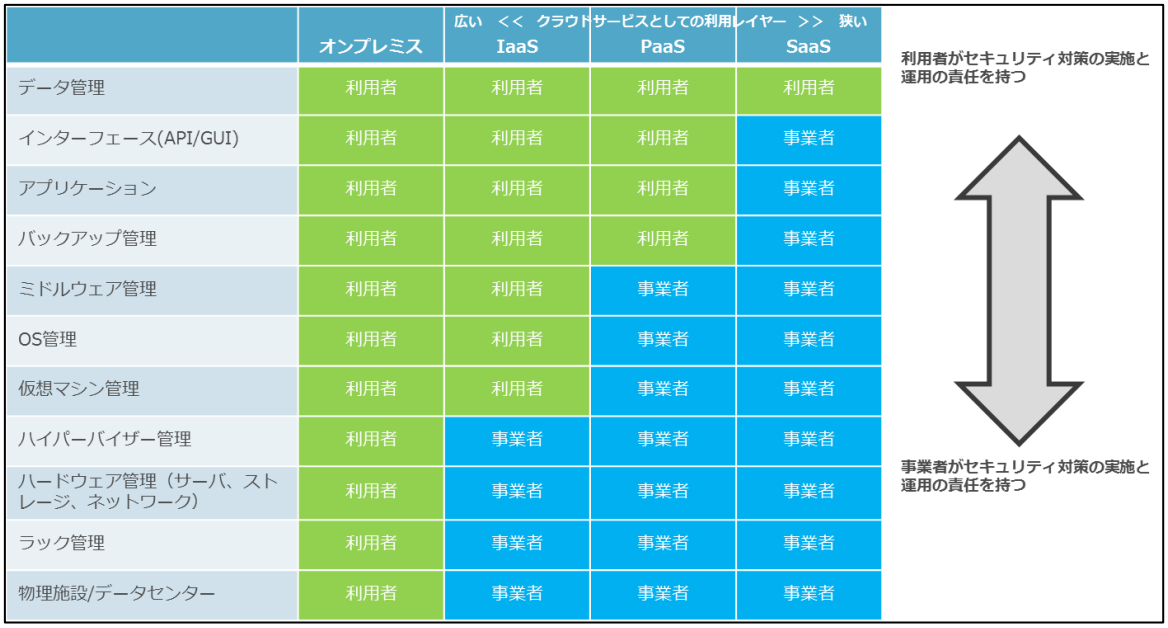
なお、コミュニティクラド及びハイブリッドクラウドは、パブリッククラウド又はプライベートクラウドの応用的な利用形態であることから、本項ではパブリッククラウドとプライベートクラウドの 2 形態について記述する。

④責任分界点（情報セキュリティ確保の役割分担）

クラウド利用者とクラウド事業者の責任分界点は、クラウドサービスモデルで異なる（以下の図表参照)。

全体として、IaaS⇒PaaS⇒SaaS とクラウドサービスとしての利用レイヤが広くなるに従

い、クラウド事業者側の管理に依拠する範囲が広がることに留意する必要がある。これらの特徴をふまえて、責任分界点を識別し、クラウド利用者側（教育委員会。IaaS/PaaS を、運用事業者を介して利用する場合には運用事業者と分担する。具体的には調達仕様書等において運用事業者の業務内容を定義することが多い。以下同じ。）での管理施策について講じる（詳細は 1.9.2.に記載）。



	オンプレミス	広い << クラウドサービスとしての利用レイヤー >> 狭い IaaS	PaaS	SaaS
データ管理	利用者	利用者	利用者	利用者
インターフェース(API/GUI)	利用者	利用者	利用者	事業者
アプリケーション	利用者	利用者	利用者	事業者
バックアップ管理	利用者	利用者	利用者	事業者
ミドルウェア管理	利用者	利用者	事業者	事業者
OS管理	利用者	利用者	事業者	事業者
仮想マシン管理	利用者	利用者	事業者	事業者
ハイパーバイザー管理	利用者	事業者	事業者	事業者
ハードウェア管理（サーバ、ストレージ、ネットワーク）	利用者	事業者	事業者	事業者
ラック管理	利用者	事業者	事業者	事業者
物理施設/データセンター	利用者	事業者	事業者	事業者

図表　　クラウドサービスモデル毎の責任分界点

「教育情報セキュリティポリシーに関するガイドライン」の改訂に係る検討会　委員

岡村　久道	英知法律事務所
○高橋　邦夫	合同会社ＫＵコンサルティング　代表社員
西田　光昭	柏市教育委員会　柏市教育研究所 教育専門アドバイザー
林山　耕寿	シスコシステムズ合同会社
藤村　裕一	国立大学法人鳴門教育大学大学院 遠隔教育プログラム推進室長