# 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７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
令和６年１月　　改　訂
令和７年３月　　改　訂

文 部 科 学 省

**重要：はじめに**

本ガイドラインは、主に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。

児童生徒の学び方、教職員等の働き方の変化に合わせて、学校現場にて必要とされる教育情報システム及び情報セキュリティは日々変遷を遂げており、本ガイドラインも時代の要請に沿って改訂を行ってきた。

令和元年度以降、GIGA スクール構想に基づく１人１台端末の整備、クラウドサービスの本格活用が進み、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ようになった。

また、令和５年３月には「GIGA スクール構想の下での校務 DX について～教職員の働きやすさと教育活動の一層の高度化を目指して～」を取りまとめ、クラウド上での校務実施を前提とした次世代校務 DX の姿を示すとともに、パブリッククラウド上で学習系・校務系情報を取り扱うに当たってこれまでの境界防御型セキュリティに代わって、強固なアクセス制御による対策を前提とするセキュリティの考え方が導入された。

さらに、生成 AI の登場など、教育現場を取り巻く環境は日々変化している。

このように教育 DX が進展する中で、教育委員会及び学校に必要とされるセキュリティ対策は高度化し、ますます重要度を増している。詳細は後述する「第１編 総則」「第１章 本ガイドラインの目的等」に譲るが、学校教育の現場においては、地方公共団体の他の行政事務とは異なり、教職員や児童生徒が守るべき情報資産に触れることから、自治体の情報セキュリティポリシーとは別に「教育情報セキュリティポリシー」を定めることを求めている。しかしながら、令和６年度時点で教育委員会独自の教育情報セキュリティポリシーを定めている割合は約５割に留まっており、大変憂慮すべき事態である。

各教育委員会には本ガイドライン「第１編 総則」の理念を踏まえつつ、「第２編 教育情報セキュリティ対策基準（例文・解説）」や、「第３編 付録」を参考にしながら、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、関係者（教育委員会・学校の担当者、有識者等）と迅速かつ十分に議論を行い、教育情報セキュリティポリシーの策定・見直しを実施いただきたい。

※　「第１編 総則」の基本理念は、「対策基準」だけではなく「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月改訂版以降、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。

※　「第２編 教育情報セキュリティ対策基準（例文・解説）」では、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に関する対策基準を扱っている。特に、校務系システム及び校務外部接続系システムについては地方公共団体で構成が異なるため、必要となる対策は一様ではない。各地方公共団体においては、組織が目指すべき教育情報セキュリティの姿に合わせた対策を選択して、対策基準を策定いただきたい。
また、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、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、組織が目指すべき教育情報セキュリティの姿に合わせ、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。

本改訂の主な改訂箇所（令和７年３月）

- 「第１編 総則」の「第３章 教育現場におけるクラウドの活用について（３）学校現場におけるクラウドサービスの利用」及び「第２編 教育情報セキュリティ対策基準（例文・解説）」の「３.１. 情報資産の分類」「３.２. 情報資産の管理」「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」「７.５. 児童生徒における ID 及びパスワード等の管理」「９.３. SaaS 型パブリッククラウドサービス利用における教職員等の留意点」等について、情報資産の分類・仕分け・管理方法を見直し
- 「第３編 付録」の「（１）本ガイドラインにおける用語定義」「（３）技術的対策に関する考え方」について、強固なアクセス制御による対策に関する記載を見直し

目次

# 第１編 総則

## 第１章 本ガイドラインの目的等

（１）本ガイドラインの目的

情報セキュリティポリシーとは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書をいう。地方公共団体における情報セキュリティポリシーは、各地方公共団体が組織の実態に応じて自主的に策定や見直しを行うものであり、その参考として「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６年10月）」（以下「自治体ガイドライン」と言う。）が総務省において整備されている。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。

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、地方公共団体の他の行政事務とは異なる特徴を有する。例えば、学校と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、当該児童生徒がコンピュータを活用した学習活動の実施などにおいて、日常的に情報システムにアクセスする機会がある。そのため、児童生徒においても情報セキュリティポリシーにて規定した対策について遵守するよう、職員、教員、保護者等が適切に指導を行うことが求められる。

また、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。児童生徒の育成においては、学校教育に直接関わる複数の関係者により、児童生徒に関する情報が多目的で活用される。学習においても、教職員や他の児童生徒と協働学習活動を実践する際、児童生徒が生み出す情報は本人の思考の記録であるとともに学習評価の材料となり、必要に応じて他児童生徒に開示する等多目的に活用される。

よって、学校教育においては、児童生徒の存在及び取り扱う情報の多様性・多目的性等を考慮した情報セキュリティ対策を講ずる必要がある。

このような背景を踏まえ、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、その後も改訂を行ってきた。

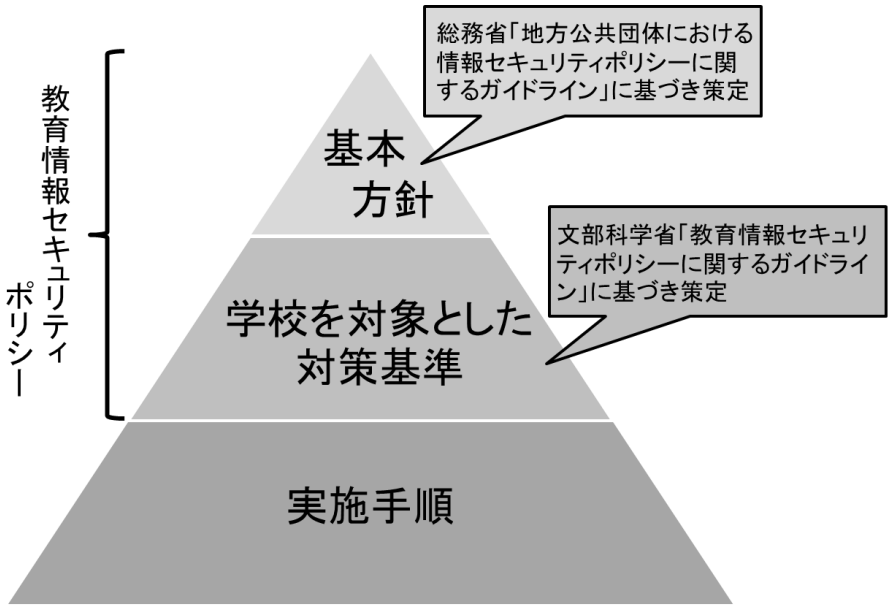
（２）本ガイドラインの位置付け

情報セキュリティポリシーの体系は、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「基本方針」、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「対策基準」、対策基準に基づき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「実施手順」の階層構造となっている。このうち「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。

学校教育においては、「第１編第１章（１）本ガイドラインの目的」で述べたとおり、地方公共団体の他の行政事務とは異なる特徴を有するため、そちらを考慮した情報セキュリティ対策を講ずる必要がある。

このため、学校の設置者である地方公共団体は、「基本方針」については総務省の定める自治体ガイドラインに基づき策定し、「対策基準」については学校を想定したものを策定するとともに、「実施手順」のひな形についても策定することが求められる。各学校はこのひな形を基に「実施手順」を策定することが求められる。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、学校を対象とした「対策基準」及び「実施手順」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が求められる。

本ガイドラインに基づき策定いただきたいのは「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。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、自治体ガイドライン
（https://www.soumu.go.jp/main_content/000970701.pdf）を参照されたい。




**図表１　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**

（３）本ガイドラインの読み方

①対象範囲

本ガイドラインでは、情報セキュリティの観点から守る対象として、学校で扱う情報資産（校務系情報、学習系情報）を想定している。情報資産のセキュリティを確保するためには、学校が保有するデータそのもの及びそのデータを生成・保管・流通する媒体（紙、ネットワーク、サーバ、端末等）の両方をセキュリティ侵害から守り、情報漏洩を防止することが必要であり、これら全てが本ガイドラインの対象範囲となる。

なお、学校には本ガイドラインが適用される「教育ネットワーク」とは別に、「行政系ネットワーク」が敷設され、行政系端末により自治体共通業務（出張処理等）が実施されている場合もあるが、この取扱いについては首長部局が自治体ガイドライン（https://www.soumu.go.jp/main_content/000970701.pdf）を基に策定した自治体の情報セキュリティポリシーに準拠すること。また、「教育ネットワーク」が「行政系ネットワーク」と論理的または物理的に分離されていない場合は、自治体ガイドラインが適用されるので注意が必要である。

②想定される読者

本ガイドラインの読者は、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いる。本ガイドラインは主に地方公共団体が設置する学校を対象としているが、それ以外の学校における情報セキュリティ対策の実施においても参考になるため、学校法人、附属学校を置く国立大学法人、小中高等学校を設置する各学校設置会社や、それぞれが設置する学校においても参照いただきたい。（ただし、設置者等によって準拠する法令が異なる場合があることに留意する必要がある。例えば、「個人情報保護法」（令和３年改正）においては、公立学校に対しては法第５章（公的規律）が適用される一方、私立学校（株立含む）に対しては法第４章（民間規律）が適用される。また、国立学校（国立大学法人が設置する学校）及び地方公共団体・地方独立行政法人が設置する大学の附属学校に対しては規律内容によって法第４章又は法第５章が適用されるなど、学校の設置者等によって異なるため、個人情報保護に係る規定について参照する際には、個人情報保護法におけるこれらの規律の違いに留意する必要がある。）

なお、本ガイドラインでは第２編 教育情報セキュリティ対策基準（例文・解説）にて対策基準の例をまとめており、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。

③本ガイドラインの構成

「第１編 総則」においては、教育情報セキュリティの基本的な考え方を示している。

「第２編 教育情報セキュリティ対策基準（例文・解説）」においては、教育情報セキュリティ対策基準の例文と解説を示している。対策基準の策定に当たっては、各例文を参照しつつ、各自治体の実情に応じた対策基準を教育委員会にて策定いただきたい。

なお本ガイドラインに基づき策定いただきたいのは「対策基準」の部分ではあるが、実施手順の策定においても、主に第２編「２．組織体制」「３．情報資産の分類と管理方法」「５．人的セキュリティ」が参考となる。本内容を参考としつつ、各自治体の実情に応じた実施手順のひな形についても教育委員会にて策定いただき、各学校にはそのひな形を基に各学校の実情に応じた実施手順を策定いただきたい。

「第３編 付録」においては、用語の解説や、次世代の校務 DX に関する内容等を示している。

（４）本ガイドラインの経緯

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、学習者用端末と指導者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月版）」

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。

※　「アクセス制御による対策を講じたシステム構成」については、令和５年３月に公開した「GIGA スクール構想の下での校務 DX について～教職員の働きやすさと教育活動の一層の高度化を目指して～」を踏まえつつ、冒頭に「強固な」と追記する文言修正を、後述する令和６年１月改訂にて行っている。本修正においては、新たな要素技術の追加は行っていない。

⑤「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６年１月版）」

令和５年３月に公開した「GIGA スクール構想の下での校務 DX について～教職員の働きやすさと教育活動の一層の高度化を目指して～」（以下、「提言」という。）では、次世代の校務 DX の在り方について示した。次世代の校務 DX とは、「校務系・学習系ネットワークの統合」「校務系システムのクラウド化」「データ連携基盤（ダッシュボード）の創出」により、ロケーションフリーを含む「働き方改革」、「データ連携」、「レジリエンス」の観点から、学校教育環境における課題を解決するものである。

この次世代の校務 DX を実現するに際し、校務系・学習系システムをパブリッククラウド上で運用しつつ情報セキュリティを確保することがこれまで以上に重要であり、コストとベネフィットを総合的に勘案し検討することが必要である。

そこで令和６年１月版では、上記提言及び「GIGA スクール構想」「教師を取り巻く環境整備について緊急的に取り組むべき施策（提言）」にて示されている、教職員の働き方改革や児童生徒の主体的な学びの実現の重要性を踏まえつつ、次世代の校務 DX を踏まえた教育情報セキュリティの考え方について、強固なアクセス制御による対策の考え方に基づくネットワーク統合を前提としたパブリッククラウド活用において適切なセキュリティ対策を講じる重要性について、追記を行った。また、自治体ガイドライン、「政府機関等のサイバーセキュリティ対策のための統一基準群」（令和５年改定）、「個人情報保護法」（令和３年改正）等、現行の関連法令・指針に即するように加筆修正を行うとともに、本ガイドラインの読みやすさ向上に向け、書きぶり等について修正を行った。

⑥「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７年３月版）」

教育現場におけるクラウド活用が進んでいること等を踏まえ、情報資産の分類・仕分け・管理方法について見直しを行うとともに、強固なアクセス制御による対策に関する記載の見直し等を行った。

## 第２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

本ガイドラインは、以下の①～⑦を基本理念として、「第２編 教育情報セキュリティ対策基準（例文・解説）」にて対策基準の例文・解説をまとめている。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。

**⑦児童生徒の情報セキュリティ・情報モラルに関する意識の醸成を図ること**

児童生徒が１人１台の学習者用端末を活用し学習活動を行うことから、教職員等からの指導を通じて、児童生徒の情報セキュリティ・情報モラルに関する意識の醸成を図ることが必要である。インターネット等の安全な利用や、コミュニケーションツールにおけるモラル習得など、児童生徒を被害者にも加害者にもしないための指導が必要である。

## 第３章 教育現場におけるクラウドの活用について

（１）クラウドサービスの活用

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。

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。

クラウドサービスは、正しく選択することにより、教育委員会に対して次のようなメリットをもたらす効果が見込める。

| | |
|---|---|
| ①効率性の向上 | 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。<br>※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。<br>※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 | 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 | 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 | 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 | 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。<br>※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。 |

**図表 2　クラウドサービスのメリット**

このように、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、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。

（2）クラウドサービスの定義・分類

①クラウドサービスとは

クラウドサービスとは、事業者によって定義されたインタフェースを用いた、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であって、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いう（出典：「政府機関等の対策基準策定のためのガイドライン」（令和５年度版）13.「統一基準における用語定義」）。

クラウドサービスの利用は、サーバを核とした情報処理機能を自前で構築して使うことから、外部の情報処理能力をサービスとして利用することへの手法の転換と言える。所有から利用への転換により、自前で行う行為がクラウド事業者に委ねる行為に変わる。

②クラウドのサービスモデル

クラウドサービスの例としては、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）、SaaS（Software as a Service）等がある（出典：「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」）。

- IaaS（Infrastructure as a Service）
  利用者に、CPU機能、ストレージ、ネットワークその他の基礎的な情報システムの構築に係るリソースが提供されるもの。利用者は、そのリソース上にOSや任意機能（情報セキュリティ機能を含む。）を構築することが可能である。

- PaaS（Platform as a Service）
  IaaSのサービスに加えて、OS、基本的機能、開発環境や運用管理環境等もサービスとして提供されるもの。利用者は、基本機能等を組み合わせることにより情報システムを構築する。

- SaaS（Software as a Service）
  利用者に、特定の業務系のアプリケーション、コミュニケーション等の機能、運用管理系の機能、開発系の機能、セキュリティ系の機能等がサービスとして提供されるもの。

IaaSを採用した場合、教育委員会等は、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。

PaaSを採用した場合、教育委員会等は、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くてすむという特徴がある。

SaaSを採用した場合、教職員等及び児童生徒は、インターネット経由でアプリケーションを利用することとなる。教育委員会等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。学習系分野では、学習eポータル、MEXCBT、デジタル教科書、デジタルドリル、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、校務支援システム、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。

③クラウドの実装モデル

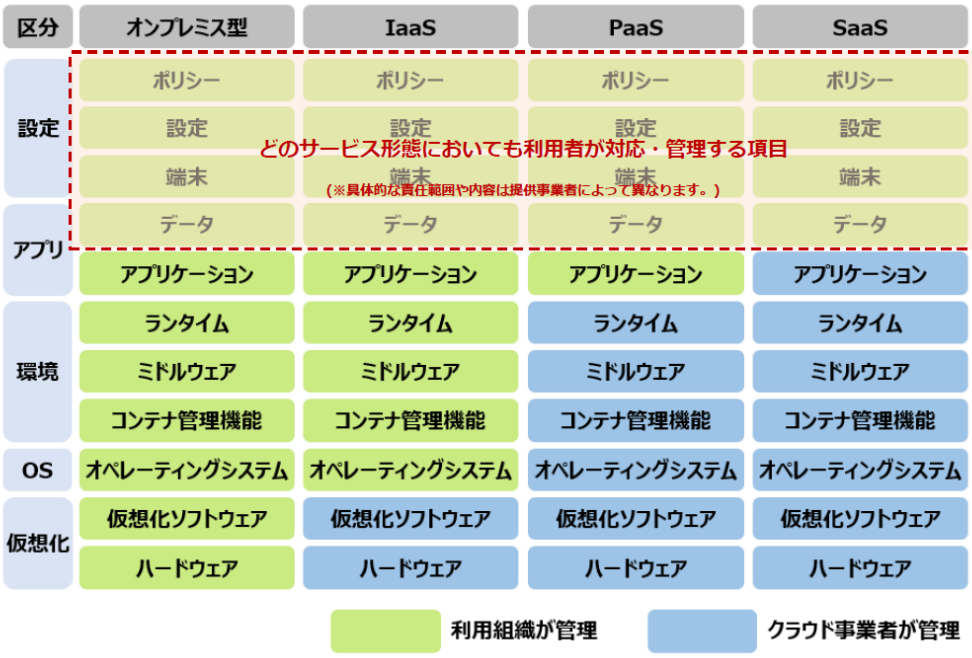
クラウドサービスはその実装の在り方によって、主にパブリッククラウドとプライベートクラウドの２つに分けられる。（出典：内閣サイバーセキュリティセンター「クラウドを利用したシステム運用に関するガイダンス」（詳細版））。

- パブリッククラウド
  クラウドサービスの提供方式のひとつ。CPU、ストレージ、メモリ等のコンピュータリソースの利用率を最適化するために、一般ユーザーや複数の利用者でリソースを共用して実装されるクラウドコンピューティング方式。

- プライベートクラウド
  クラウドサービスの提供方式のひとつ。クラウド事業者が１つの組織に対してクラウドサービスを提供するものであり、当該組織外のユーザーは利用することができない、その組織専用に実装されるクラウドコンピューティング方式。

④責任分界点（情報セキュリティ確保の役割分担）

クラウドサービスの選定・契約の主体である教育委員会等（以下、「クラウド利用者」という。）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。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（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「第２編９．２．SaaS型パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項」に記載）。




図表 3　クラウドサービスモデル毎の責任分界点

（出典）内閣サイバーセキュリティセンター「クラウドを利用したシステム運用に関するガイダンス」

（３）学校現場におけるクラウドサービスの利用

学校現場におけるクラウドサービスの利用形態としては、主に以下の２パターンが想定される。

①IaaS・PaaS型プライベートクラウドサービスの利用

校務系システムをインターネット接続する校務外部接続系システムや学習系システムとネットワーク分離して、インターネットからのサイバー脅威の侵入を遮断する場合、IaaS・PaaSを利用する構成が考えられる。

具体的には、校務支援システムやファイルサーバを構築するうえで、自前でサーバを導入（オンプレミス）ではなく、IaaS・PaaSを利用してサーバ基盤（コンピューティング能力）の提供を受け、その基盤上にSI事業者がアプリケーションを乗せて校務系システムを構築する形態である。当該モデルは、システム自体がインターネットから遮断される構成とするため、通信回線としてプライベート回線を用いる構成（注）となる。

（注）校務系システム、校務外部接続系システム、学習系システムにおいてインターネットアクセスを許容しつつも、アクセス管理や不正アクセス検知を行うことでインターネットからのサイバー脅威の侵入を遮断し、IaaS・PaaSを利用する構成も実装し得る。

この形態でIaaS・PaaSを利用する場合、クラウド事業者と契約するのはSI事業者となり、自治体はSI事業者に外部委託する形態となる。このサービス提供形態である場合は、教育委員会はSI事業者とSaaS事業者として契約し、SI事業者はSaaS事業者として情報管理責任を負う形態が望ましい。この形態について情報セキュリティ対策基準を検討する場合は、「第２編８．外部委託」を参照すること。

②SaaS型パブリッククラウドサービスの利用

（ア）SaaS型パブリッククラウドの特性を踏まえた安全なクラウドサービスの選定の必要性

GIGAスクール構想の推進によって学校現場で活用の進むクラウドサービスは主にSaaS型パブリッククラウドサービスに分類される。SaaS型パブリッククラウドサービスの利用に当たっては、利用者の個別要望に沿ったカスタマイズは原則困難であり、外部委託のように、利用者の要望を反映した個別契約に基づく調達として扱うことは原則難しい特性を持つ。

このようなSaaS型パブリッククラウドサービスの特性を踏まえた安全なクラウドサービスの選定に当たっては、該当クラウドサービスの安全性及びクラウド事業者の信頼性等の確認が必要になるが、原則クラウド事業者の提示するサービス要件、監査報告書等からクラウド利用者がサービス利用の可否を判断することが求められる。なお、前述のとおりSaaS型パブリッククラウドサービスはアプリケーション及び下位層のサーバ、ネットワーク、その

他のインフラを合わせて提供するサービス形態であるため、サービス利用可否の判断に当たっては、アプリケーションのみならず、クラウドサービス事業者が契約しているクラウド基盤のデータ管理や信頼性等の確認も必要であることに留意すべきである。

詳しくは、「第２編９．１． SaaS型パブリッククラウドサービスの利用における情報セキュリティ対策」及び「第２編９．２．SaaS型パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項」を参照すること。

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

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

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

重要性分類については、「第２編３．情報資産の分類と管理方法」を参照すること。
強固なアクセス制御による情報セキュリティ対策については、「第３編（３）技術的対策に関する考え方」を参照すること。

（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

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場合も多いため、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は、求める内容に応じた認証規格を参考にすることで、「第２編　９．１．SaaS 型パブリッククラウドサービスの利用における情報セキュリティ対策/９．２．SaaS 型パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項」に示す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間接的に判断することが可能である。そのため、第三者認証取得の有無、監査報告書等からクラウド事業者と提供するクラウドサービスの安全性、信頼性を優先的に確認することを推奨する。

＜認証制度の例＞

- ISO/IEC27001（情報セキュリティマネジメントシステム）
- ISO/IEC27002（情報セキュリティマネジメントシステム）
- ISO/IEC27014（情報セキュリティガバナンス）
- ISO/IEC27017（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/IEC27018（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/WebTrust）（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
  https://jcispa.jasa.jp/cloud_security/cs_mark/
- ASP・SaaS安全・信頼性に係る情報開示認定
- 政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program:通称、ISMAP）

## 第２編 教育情報セキュリティ対策基準（例文・解説）

### 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、以下のとおりとする。

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

| | |
|---|---|
| 校務外部接続用端末 | ネットワーク分離による対策を講じたシステム構成において、校務外部接続系情報にアクセス可能な端末 |
| 学習者用端末 | 学習系情報にアクセス可能な端末で、児童生徒が利用する端末 |
| 指導者用端末 | 学習系情報にアクセス可能な端末で、教員のみが利用可能な端末 |
| 校務系システム | 校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム<br>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 | ネットワーク分離による対策を講じたシステム構成において、校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ（CMS）及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム |
| 学習系システム | 学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム<br>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 | ネットワーク分離による対策を講じたシステム構成において、校務外部接続系情報を取り扱うサーバ |
| 学習系サーバ | 学習系情報を取り扱うサーバ |

**図表 4　用語説明**

（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5　情報資産の種類と例のとおりであるが、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。

| 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 |
| 教育ネットワーク及び教育情報システムに関する施設・設備 | 情報資産を扱うコンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル |
| 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 |

**図表 5　情報資産の種類と例**

## 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（臨時的任用教職員、非常勤講師を含めた教職員全員をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。

（４）教育情報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。

（10）教職員等

① 臨時的任用教職員、非常勤講師を含めた教職員全員を、教職員等と称する。

② 教職員等は学校が所管する情報資産を取り扱う立場にあり、教育情報セキュリティ管理者の指導の下、情報セキュリティを遵守しなければならない。

（11）教育委員会事務局職員

① 教育ネットワークを利用して、学校が所管する情報にアクセスできる教育委員会事務局職員を指す。

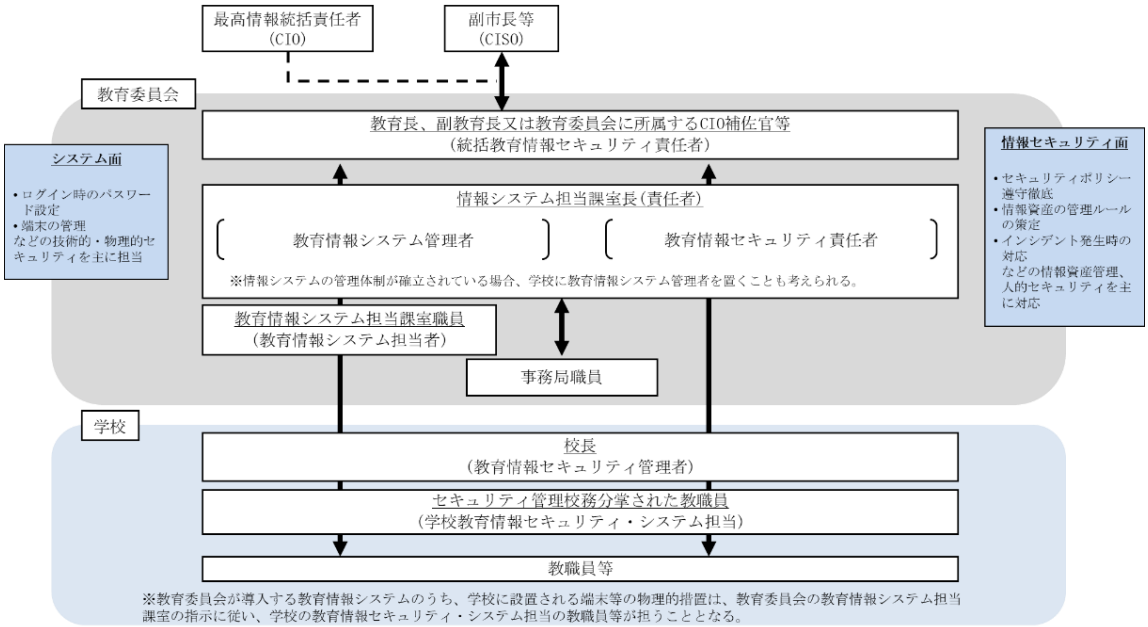
② 教育委員会事務局職員は学校の情報資産にアクセスできる立場にあり、教育情報セキュリティ責任者の指導の下、情報セキュリティを遵守しなければならない。

（解説）

各地方公共団体においては、図表6　情報セキュリティ対策推進のための組織体制例のような体制を構築して、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。




**図表６　情報セキュリティ対策推進のための組織体制例**

（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。

（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）実際の運用に当たっては、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・運用等に当たり専門的な知識・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。

（10）教職員等

教職員等とは、臨時的任用教職員、非常勤講師を含めた教職員全員を指す。

教職員等は、教育情報セキュリティ管理者の指導の下、情報セキュリティを遵守しなければならない。

（11）教育委員会事務局職員

教育委員会事務局職員は、教職員等のように学校で取り扱う情報について直接取り扱う立場にはないが、情報にアクセスできることから、教育情報セキュリティ責任者の指導の下、情報セキュリティを遵守しなければならない。

## ３．情報資産の分類と管理方法

### ３．１．情報資産の分類

【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系を定める必要がある。そのためには、学校に存在する文書やデータファイルなどの情報資産を、その重要性に応じて分類・仕分けすることが前提となる。情報資産を分類できていない場合は、情報資産の管理方法が曖昧になり、情報の漏えい、紛失、改ざん、情報にアクセスできなくなる等の被害が生じるおそれがある。

【例文】

（１）情報資産の分類

本市における情報資産は、機密性、完全性及び可用性の３つの観点から影響度を評価し、次のとおり４段階の重要性分類を行い、必要に応じて取扱制限を行うものとする。

| 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。（Ⅰを除く） |
| Ⅲ セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼす。（Ⅱ以上を除く） |
| Ⅳ セキュリティ侵害が学校事務及び教育活動の実施に影響をほとんど及ぼさない。（Ⅲ以上を除く） |

| 情報資産の分類 | | 情報資産の例示<br>各情報資産にアクセスする主体 | | |
|---|---|---|---|---|
| 重要性分類 | 定義 | 教職員等※・教育委員会 | 教職員等・教育委員会・児童生徒・保護者 | 不特定多数 |
| 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。 | **業務に係る特定の教職員等・教育委員会のみがアクセスすることが想定される情報**<br><br>○情報システムの設計に関する情報<br>・教育情報システム設計書・設定書<br><br>○学校運営に関する情報<br>・入学者選抜問題<br>・指導要録原本<br>・教職員の人事記録<br><br>○健康に関する情報（医師等による指導・診療・調剤の事実等要配慮個人情報を含むもの）<br><br>○指導に関する情報（犯罪の経歴、犯罪により害を被った事実、少年法に関する事項等要配慮個人情報を含むもの）<br><br>○その他要配慮個人情報を含む情報　　等 | **業務に係る特定の教職員等・教育委員会に加えて、児童生徒またはその保護者がアクセスする場合、児童生徒本人の情報のみにアクセスすることが想定される、要配慮個人情報等を含む情報**<br><br>○健康に関する情報（医師等による指導・診療・調剤の事実等要配慮個人情報を含むもの）<br>・健康診断票<br><br>○その他要配慮個人情報を含む情報　　等 | |
| Ⅱ | セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす。（Ⅰを除く） | **業務に係る教職員等・教育委員会のみがアクセスすることが想定される情報**<br>○情報システムの運用に関する情報<br>・システムログインID管理台帳<br>・端末ログインID管理台帳<br><br>○学校運営に関する情報（Ⅰを除くもの）<br>・教職員および児童生徒の、生活歴、電話番号、メールアドレス、住所、生年月日、性別等の基本情報を含むもの<br><br>○健康に関する情報（医師等による指導・診療・調剤の事実等要配慮個人情報を含まないもの）<br>・養護教諭・スクールカウンセラー等による記録<br><br>○指導に関する情報（Ⅰを除くもの）<br>・個別指導計画<br>・生徒指導に関する記録<br>・家庭訪問や個別面談に関する記録<br><br>○成績に関する情報<br>・進級・卒業認定資料<br><br>○進路に関する情報<br>・進路希望調査<br>・入学者選抜に関する表簿（願書等）<br>・調査書<br>・推薦書<br>・卒業生進路先情報<br><br>○学籍に関する情報<br>・転退学・転入学・就学・休学等に関する情報<br>・教科用図書の給付に関する情報<br><br>○児童生徒の氏名・所属等に関する情報<br>・児童生徒名簿、児童生徒住所録<br>・保護者緊急連絡網<br>・職員緊急連絡網、職員住所録　　等 | **業務に係る教職員等・教育委員会に加えて、児童生徒またはその保護者がアクセスする場合、児童生徒本人の情報のみにアクセスすることが想定される、要配慮個人情報等を含まない情報**<br><br>○成績に関する情報<br>・通知表<br>・定期考査・テスト等の採点結果<br><br>○健康に関する情報（医師等による指導・診療・調剤の事実等要配慮個人情報を含まないもの）　　等 | |
| Ⅲ | セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼす。（Ⅱ以上を除く） | **教職員等全員・教育委員会がアクセスすることが想定される情報**<br><br>○学校運営に関する情報（職員室等で日常的に運用するもので、Ⅱ以上を除くもの）<br>・職員会議資料<br><br>○児童生徒の氏名・所属等に関する情報（教室等で日常的に運用するもので、Ⅱ以上を除くもの）<br>・出席簿　　等 | **教職員等全員・教育委員会に加えて、児童生徒及び保護者がアクセスすることが想定される情報**<br><br>○児童生徒の氏名・所属等に関する情報<br>・座席表<br>・児童生徒委員会名簿<br><br>○学校運営に関する情報<br>・卒業アルバム<br>・児童生徒の個人写真・集合写真、学校行事等の児童生徒の写真<br><br>○学習活動の中で生成される情報<br>・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、日常的な簡易な健康観察等）<br>・学習活動の記録（動画・写真等）<br><br>○学習指導に関する情報<br>・授業用教材、児童生徒用配布プリント　　等 | |
| Ⅳ | セキュリティ侵害が学校事務及び教育活動の実施に影響をほとんど及ぼさない。（Ⅲ以上を除く） | **教職員等全員・教育委員会がアクセスすることが想定される、Ⅲ以上を除く情報** | **教職員等全員・教育委員会に加えて、児童生徒及び保護者がアクセスすることが想定される、Ⅲ以上を除く情報** | **不特定多数に公開することが想定される情報**<br><br>○学校運営に関する情報（広報等のため活用するもの）<br>・学校・学園要覧<br>・学校紹介パンフレット<br>・学校・学園ホームページ掲載情報<br><br>○学習活動で生成される情報（保護者の同意等を得て広報等のため活用するもの）　　等 |

※「教職員等」とは、臨時的任用教職員、非常勤講師を含めた教職員全員を指す。

図表 7　重要性分類に基づく情報資産の例示

（解説）

（１）情報資産の分類

本来情報資産は、外部漏えいの影響（機密性）、情報の改ざんの影響（完全性）、情報が使えなくなる影響（可用性）の３つの観点から、セキュリティ侵害による被害を受けた場合に想定される影響を考慮して、その影響度合いに応じて分類・仕分けを行うべきである。

一方で、学校教育においては、膨大な量の情報が存在し、一つひとつの文書やデータファイルなどの情報資産について３次元の影響を加味した分類・仕分けを行うことは現実的ではない。そのため、３次元を１次元に単純化した重要性分類によって、分類・仕分けをすることを推奨したい。

重要性分類とは、当該情報資産のセキュリティ侵害による影響（被害）の大きさによって分類する考え方である。重要な情報とは、万が一セキュリティ侵害が発生した場合により大きな影響（被害）を受けることを意味し、４段階で定義している。分類・仕分けにおいては、各分類の定義に留意しつつ実施されたい。

図表７重要性分類に基づく情報資産の例示は、各情報資産にアクセスする主体に基づき代表的な情報資産を分類している。これらはあくまでも教育委員会等が情報資産の分類を検討する際に参考となるように例示しているものであり、情報資産に含まれる情報や運用場面、アクセスする主体等の運用実態を教育委員会等が十分に把握した上で適切な分類を行うことが重要である。

以下に、各分類の考え方について解説する。

- 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」もの、すなわち、情報が侵害された場合に甚大な被害が想定され、学校もしくは特定個人が著しい不利益を被る情報であり、要配慮個人情報を含むもの等を指す。

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

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

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

※児童生徒の、生活歴・電話番号・メールアドレス・住所・生年月日・性別等の基本情報を含む学校運営に関する情報のうち重要性分類Iに該当しないものと併せて取り扱われる児童生徒の氏名・所属等に関する情報については、重要性分類Ⅱとして取り扱うことが適当である。一方で、学習活動の中で生成される情報（重要性分類Ⅲ相当）の中にも、児童生徒の氏名・所属に関する情報等が含まれることは自然なことである。様々な学習系ツールの利用場面等も想定し、活用場面等に応じて、実態に即した形で運用する必要がある。
※メールアドレスについては、IDとして様々なシステムログインの場面で活用される場合も想定されることから、なりすましによる不正使用や不正アクセス等のセキュリティリスクも考慮する必要がある。

- 重要性分類Ⅲ：
「セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼす。（Ⅱ以上を除く）」もの、すなわち、情報が侵害された場合に学校もしくは特定個人が不利益を被る情報であり、Ⅱ以上には該当しないものの侵害の影響を無視できないもの（学校運営・学習活動・学習指導など）を指す。
たとえば、教職員等が学校運営のため日常的に取り扱う情報、児童生徒が学習活動のため日常的に取り扱う情報、保護者とのやりとりのため取り扱う学校運営に関する情報などで、Ⅱ以上を除くものを、重要性分類Ⅲとして取り扱うことが考えられる。

※ワークシートや授業中の確認テストなど、学習活動の中で生成される情報は児童生徒が教室等において相互に閲覧することが想定される情報であり、このような性質の情報資産は重要性分類Ⅲに分類される。ただし、定期考査等の採点結果等、成績に関する情報を含む情報資産は、相互に閲覧することは想定されず、重要性分類Ⅱとして取り扱うことが適当である。
※学習活動の中で生成される情報は重要性分類Ⅲに分類することを想定しているが、教職員等の評価等が加えられ、児童生徒が相互に閲覧すること等が想定されない状態のものについては、重要性分類Ⅱとして取り扱うことが適当な場合もあることに留意すべきである。

- 重要性分類Ⅳ：
上記以外の、セキュリティ侵害が発生しても学校事務及び教育活動の実施にほとんど影響を及ぼさない情報である。

なお、機密性、完全性及び可用性に基づく分類基準及び該当する情報資産のイメージは以下のとおりである。情報資産の分類の際には、重要性分類が機密性・完全性・可用性の３次元の要素を単純化したものであることを念頭に置いて、機密性の観点だけではなく、完全性・可用性への観点も想定する必要がある。例えば、図表７は「不特定多数がアクセスする情報」は機密性を有さないために重要性分類Ⅳに分類することを想定した図としているが、実際に教育現場で扱われる不特定多数がアクセスする情報のうち、改ざんされた場合に影響の大きいもの（完全性の侵害への影響を無視できないもの）や、使えなくなった場合に影響の大きいもの（可用性の侵害への影響を無視できないもの）については、その影響の大きさにより重要性分類Ⅲと位置付けることも想定される。

| 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） |

**図表８　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 |

**図表 9　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 |
|---|---|---|
| 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 |

**図表 10　可用性による情報資産の分類**

３．２．情報資産の管理

【趣旨】

情報資産の管理責任を明確にし、「第２編３．１．情報資産の分類」で定めた情報資産の分類に応じた管理方法を規定する。

【例文】

（１）管理責任

① CISOまたは統括教育情報セキュリティ責任者は、教育情報システムとその運用管理を定めた学校教育情報セキュリティ対策基準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、学校教育情報セキュリティ対策基準に基づき、学校現場での情報セキュリティ運用管理に関する実施手順ひな形を作成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、学校で標準的に所管する情報資産について、分類を定義した標準情報資産台帳（以下「標準台帳」という。）を作成し、適宜更新しなければならない。

④ 教育情報セキュリティ管理者は、実施手順ひな形に基づき、自校の実施手順を作成しなければならない。

⑤ 教育情報セキュリティ管理者は、標準情報資産台帳に基づき、自校で所管する情報資産を確認し、不足内容を補完した自校向け情報資産台帳（以下「台帳」という。）を整備しなければならない。

⑥ 教育情報セキュリティ管理者は、自校の所管する情報資産について管理責任を有する。

⑦ 教育情報セキュリティ管理者は、教職員等の情報資産の取扱いに際し、台帳及び実施手順に基づいた運用管理を指導しなければならない。

⑧ 教職員等は、台帳及び実施手順に基づき、適切に情報資産を取り扱わなければならない。

（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

① 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。

② 情報を作成する教職員等は、情報の作成時に３．１の分類に基づき、当該情報の分類を定め、分類に準拠した取扱いを行わなければならない。

③ 情報を作成する教職員等は、作成途上の情報についても、取扱いを許可されていない者の閲覧や紛失・流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

（４）情報資産の入手

① 本市教職員等が作成した情報資産を入手した教職員等は、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。

② 本市教職員等以外の者が作成した情報資産を入手した教職員等は、３．１の分類に基づき、当該情報の分類を定め、分類に準拠した取扱いを行わなければならない。

③ 情報資産を入手した教職員等は、その情報資産の分類が不明な場合、教育情報セキュリティ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

① 情報資産を利用する教職員等は、業務以外の目的に情報資産を利用してはならない。

② 情報資産を利用する教職員等は、情報資産の分類に応じ、適切な取扱いをしなければならない。

③ 情報資産を利用する教職員等は、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。

④ 情報資産を利用する教職員等は、必要以上の複製及び配布をしてはならない。

（６）情報資産の保管

① 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の措置事項

（ア）教育情報セキュリティ管理者は、資産台帳に従って、情報資産の保管先を定め、教職員等に周知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。

② 教職員等の遵守事項

（ア）教職員等は、教育情報セキュリティ管理者が指定した保管先にのみ情報資産を保管しなければならない。

（イ）教職員等は、児童生徒が生成する学習系情報の保管先について児童生徒に指示し、それ以外の場所に保管しないよう指導しなければならない。

（７）情報資産の外部持ち出し

① 分類に応じた情報資産の外部持ち出し制限

（ア）教職員等は、重要性分類Ⅱ以上の情報資産を外部持ち出しする場合は、限定されたアクセスの措置設定（アクセス制限や暗号化）を行い、教育情報セキュリティ管理者の個別許可を得なければならない。また、持ち出し持ち帰りの記録をつけなければならない。なお、外部持ち出しツールに限定されたアクセスの措置設定（アクセス制限や暗号化）機能を有する場合には、有効にしなければならない。

（イ）重要性分類Ⅲの情報資産については、教職員等の外部持ち出しについて、教育情報セキュリティ管理者の判断で包括的許可を可とする。なお、外部持ち出しツールに限定されたアクセスの措置設定（アクセス制限や暗号化）機能を有する場合には、有効にしなければならない。

② 電子メール、外部ストレージサービスによる情報の送信

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、外部ストレージサービスにより重要性分類Ⅲ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）利用する電子メール、外部ストレージサービスは教育委員会又は学校から提供される公式サービスのみを利用し、私的に契約したサービスを利用してはならない。

③ 外部電磁的記録媒体を用いた情報の外部持ち出し

USBメモリ等の物理的な媒体による情報の外部持ち出しでは、紛失・盗難リスクを伴うことから以下を遵守しなければならない。

（ア）管理された外部電磁的記録媒体以外の使用禁止

教育委員会又は学校から支給された公的な媒体のみを利用すること。

（イ）外部電磁的記録媒体の暗号化の徹底

暗号化機能つきの媒体を利用し、暗号化機能を活かすこと。【推奨事項】

④ FAXによる情報の送信

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

⑤ 情報資産の運搬

（ア）車両等により重要性分類Ⅲ以上の情報資産を運搬する場合は、必要に応じ暗号化又はパスワードの設定を行う等の安全管理措置を講じ、宛名・差出名を明記して、厳重に封印しなければならない。

（イ）重要性分類Ⅲ以上の情報資産を運搬する教職員等は、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。

⑥ 情報資産の公表

（ア）教育情報セキュリティ管理者は、公開する情報が正しい内容であることを事前に確認し、誤公開を防がなければならない。

（イ）教育情報セキュリティ管理者は、住民に公開する情報資産について、改ざんや消去されないように定期的に確認しなければならない。

（８）情報資産の廃棄

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

（イ）情報を記録している電磁的記録媒体を利用しなくなった場合、情報を復元できないように処置した上で廃棄しなければならない。

（ウ）情報資産の廃棄・リース返却を行う教育委員会事務局職員は教育情報システム管理者の、教職員等は教育情報セキュリティ管理者の許可をそれぞれ得て、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。

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

（解説）

情報資産は分類毎に管理体系が規定される。重要性の高い情報は、より厳重に管理されるべきであることは言うまでもない。

以下に広義の管理体系について記載するが、広義の管理体系とは、教職員の情報の取扱管理を超えて、物理的・技術的セキュリティ等の個別対策に広がるものである。

本項では、教職員等による情報資産の作成、入手、利用、保管、外部持ち出し（送信、運搬、公表)、廃棄等の一連のライフサイクルに着目した管理について規定している。

情報資産の管理に当たっては、前項にて示した分類の考え方や、本項にて示す管理体系の考え方と合わせて、運用及び個別対策についても関連の深い章を各解説にて示すため適宜参照すること。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管理体系については、定期的又は必要に応じて見直すことが重要である。

行政機関等の保有する個人情報については、個人情報保護法第６６条第１項に基づき、安全管理措置を講じることが義務付けられており、当該安全管理措置の具体的な内容等については個人情報保護委員会が策定する各種ガイドライン等を参照されたい。なお、行政機関等が個人情報を含む情報を保有する場合には、本ガイドラインにおける重要性分類にかかわらず、個人情報保護法上の安全管理措置と同等ないしそれ以上の安全管理措置を行うことが求められる点に留意が必要である。

（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。

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。

（５）情報資産の利用

情報資産を利用する教職員等は、情報資産の分類に応じ、適切な取扱いをしなければならない。「第２編３.１. 情報資産の分類」を踏まえ、各情報資産にアクセスする主体に応じた適切な取扱いが実現できるよう、アクセスを想定していない第三者からの不要なアクセスを防ぐ環境（適切なアクセス制御を講じること等による他者への秘匿が確保された環境）で取り扱うことが重要である。

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

アクセス制御については「第２編６.２. アクセス制御」に、強固なアクセス制御による情報セキュリティ対策については「第３編（３）技術的対策に関する考え方」に詳細を示しているため、参照すること。

以下に、重要性分類を踏まえた、情報資産の他者への秘匿及び取扱制限に関する考え方を示す。

- 重要性分類Ⅰ：
  情報を取り扱うことが真に必要な者、すなわち、業務に係る特定の教職員等・教育委員会・児童生徒本人とその保護者のみがアクセスできるような取扱制限が必要である。取扱制限を行うに当たっては、特に必要な場合に限って必要な権限のみ（編集・閲覧・複製・ダウンロード等）を付与することが重要である。
  例えば、児童生徒の要配慮個人情報を含む健康情報については、その情報を業務上取り扱わなければならない担任教員と養護教諭のみがアクセスできるよう設定するなど、職務上特に必要な場合に限って適切に取扱制限を定めることが考えられる。

- 重要性分類Ⅱ：
  業務に係る教職員等・教育委員会・児童生徒本人とその保護者のみがアクセスできるような取扱制限が必要である。
  例えば、児童生徒の成績に関する情報については、その児童生徒の指導に関わる教職員等のみがアクセスできるよう設定をするなど、職務上必要な場合に限って適切に取扱制限を定めることが考えられる。

- 重要性分類Ⅲ：
  教職員等・教育委員会・児童生徒・保護者のうち、アクセスする主体として想定される者のみがアクセスできるような取扱制限が必要である。
- 重要性分類Ⅳ：
  特段の利用制限等はないため、業務上管理し易い場所で取り扱うことで差し支えない。

重要性分類Ⅱ以上の情報資産を強固なアクセス制御による対策を講じたシステム構成において取り扱う際の、多要素認証の設定のあり方については「第２編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（４）」を参照すること。

重要性分類Ⅱ以上の情報資産（児童生徒本人の情報に限る）を児童生徒が取り扱う際の、教職員等から児童生徒への指導事項については、「第２編５.２. 教職員等の遵守事項1 (19) 児童生徒への指導事項⑪」を参照すること。

また、アクセスを想定していない第三者からの不要なアクセスを防ぐ（適切なアクセス制御を講じること等による他者への秘匿を行う）ためには、利用者認証情報の秘匿が重要である点に留意されたい。特に知識認証（ID及びパスワード等）の秘匿管理については、「第２編７.３. 教職員等のID及びパスワードの管理（19）児童生徒への指導事項②」「第２編７.３. 教職員等のID及びパスワードの管理」「第２編７.５. 児童生徒におけるID及びパスワード等の管理」にて示しているため、参照すること。

なお、情報資産をSaaS型パブリッククラウドサービス上で取り扱う場合には、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。クラウドサービスの利用に関する各規定については「第２編９.SaaS型パブリッククラウドサービスの利用」にて示しているため、参照すること。

（７）情報資産の外部持ち出し

外部持ち出しとは、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。また、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や暗号化を講じることを指す。

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。

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。

（８）情報資産の廃棄

データの消去及び機器の廃棄については、「第２編４．１．サーバ等の管理（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。

## 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、オンプレミスの場合と民間事業者のデータセンターを利用する外部委託の両方を想定している。なお、IaaS, PaaS型クラウドを利用してコンピューティングリソースを調達して、教育情報システムを構築・運用する場合は「第２編８．外部委託」を、SaaS型パブリッククラウドサービスを利用する場合は「第２編９．SaaS型パブリッククラウドサービスの利用」を軸に検討すること。

### 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、重要性分類Ⅱ以上の情報資産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、重要性分類Ⅲの情報資産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、重要性分類Ⅱ以上の情報資産を格納しているサーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

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。

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については、サーバが緊急停止した場合、校務の遂行に多大な影響を及ぼすことが考えられることから、重要性分類Ⅱ以上の情報資産を格納しているサーバについては、冗長化を行うことが重要である。

一方で、重要性分類Ⅲの情報資産を格納しているサーバについては、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）重要性分類Ⅲの情報資産を格納している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ISO27001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。

また、原則として、以下の表に記載されている方法により、記録されている情報資産の重要性分類に応じて、機器の廃棄等を行わなければならない。

| 分類 | 機器の廃棄等の方法 | 確実な履行を担保する方法 |
|---|---|---|
| （１）重要性分類Ⅰ・Ⅱ | 一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当である。<br>具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③OS等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。 | 校内等において（２）で後述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。 |
| （２）重要性分類Ⅲ | 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に消去することが適当である。<br>具体的には、（１）で先述した方法①～⑤のほか、OS等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。<br>OS及び記憶装置の初期化（フォーマット等）による方法は、HDD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、適当ではない。 | 校内等において消去を実施し、教職員等が作業完了を確認する方法など適切な方法により確認を行う。 |

**図表 11　重要性分類に応じた機器の廃棄等の方法**

（注６）情報を消去する場合、オペレーティングシステム（OS）及び記憶装置の初期化だけでは、再度復元できてしまう。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。

（注７）サーバ装置や端末等の電磁的記録媒体については、②～⑤の対策を講じることが望ましい。特に、端末の機能により、既に暗号化の処置がなされているものについては「⑤暗号化消去」が有効である。「①物理的な方法による破壊」については、主に紙媒体について、内容が復元できないように細断、熔解またはこれに準ずる方法を講じることを想定している。ただし、電磁的記録媒体に電源が入らない場合等には、粉砕等の適切な方法により「①物理的な方法による破壊」を実施することも想定される。

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当たり、管理簿の記載等による管理を行わなければならない。

③ 教職員等は、児童生徒が管理区域に入室する場合、必要に応じて立ち入り区域を制限した上で、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なければならない。また、管理区域への入退室を許可された教職員等が付き添うものとし、外見上教職員等と区別できる措置を講じなければならない。

（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（電磁的記録媒体等の保管庫）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、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、重要性分類Ⅱ以上の情報資産を格納する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。

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、インターネットを通信経路とする回線の場合、通信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。

（６）統括教育情報セキュリティ責任者は、学校運営上必要なネットワーク帯域を確保するとともに、遅延等に対する適切な対策を講じなければならない。クラウドサービス提供事業者側のサービス要件基準を満たす配慮を含めてネットワーク構成を設計する。また、運用開始前には十分検証し、利用状況に応じて定期的に改修計画を行うこと。

（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。また、通信回線装置については定期的及び必要に応じてバージョンアップを行うことが望ましい。

（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。

（６）授業に支障のないネットワーク構成の選択（帯域や同時接続数など）

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。

- 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。

- 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。

## 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】

（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及びパスワードによる認証、加えて多要素認証の実施等、使用する目的に応じた適切な物理的措置を講じなければならない。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、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、パブリッククラウド上で重要な情報（重要性分類Ⅱ以上）を取り扱う際には、多要素認証を含む強固なアクセス制御による対策を講じなければならない。ただし、児童生徒またはその保護者が重要性分類Ⅱ以上の情報資産にアクセスする場合は、児童生徒本人またはその保護者が、当該児童生徒に関するもののみにアクセスすることを想定していることから、多要素認証を設定することが望ましいものの、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際のロック機能の有効化、パスワードの複雑性の確保等により本人確認を厳格に行う前提で、ID及びパスワードでの認証を許容する。

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

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

（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Webフィルタリング等の対策を講じなければならない。

（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、強固なアクセス制御による対策を講じたシステム構成の場合においては、校務・学習等各システムの通信経路をインターネットに統合でき、教員の利用する端末を用途別に分けずに１台に統合できるメリットがある。

ただし、学習指導において、校務系情報を児童生徒に誤表示する新たなリスクがあるため、利用においてはこのリスクを念頭に置いて使用されたい。

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。

（２）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。

（３）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。

・　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ID及び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要素以上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。

なお知識認証（ID及びパスワード等）の管理については、「第２編７.３. 教職員等のID及びパスワードの管理」「第２編７.５. 児童生徒におけるID及びパスワード等の管理」を参照されたい。

（５）暗号化機能を持つセキュリティチップの利用

暗号化機能を持つ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）データ暗号化

端末に保存したデータを暗号化し、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、データ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）マルウェア感染対策

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

不適切なウェブページへの閲覧を防止する対策として「Webフィルタリング」、「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。

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。

（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。

## ４．５．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。

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も重要である。

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）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＞

①Webフィルタリング

②検索エンジンのセーフサーチ

③セーフブラウジング

（２）マルウェア感染対策

学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

（３）端末を不正利用させないための防止策

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

（４）セキュリティ設定の一元管理

児童生徒への端末配布後においても、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。

（５）端末の盗難・紛失時の情報漏洩対策

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

（解説）

（１）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 Webフィルタリング

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。

Web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、Web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。

（２）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。

（３）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。

（４）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。

（５）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。

## ４．６．パソコン教室等における学習者用端末や電磁的記録媒体の管理

【趣旨】

パソコン教室等に設定されている児童生徒が共用利用する学習者用端末や電磁的記録媒体の管理については、児童生徒が共用で利用し、学校内で保管管理されることを前提とした管理が求められる。

【例文】

（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、パソコン及び電磁的記録媒体について、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

（３）教育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）

（１）共用端末の場合は、運用管理責任が曖昧になる危険性があるため、モバイル端末の場合は、保管庫からの取り出しから返却までの運用管理手順を規定する必要がある。

（２）端末及び電磁的記録媒体が共用であるため、学習活動で生成した情報は、学習活動終了後には、共用の端末及び電磁的記録媒体から消去することが必要である。なお、情報の保存が必要な場合には、個人管理フォルダに移設することが望ましい。

（３）共用端末であっても利用に当たっては、ログインパスワードを設定し、正規な学習者のみがアクセスできる環境を整備しなければならない。

## ５．人的セキュリティ

人による安全管理措置については、先に「第２編３．２．情報資産の管理」として、情報の生成から廃棄までのライフサイクルにおける基本的な安全管理措置を規定している。本項では、「第２編３．２．情報資産の管理」に加えて、セキュリティ侵害を予防するために必要となる人的な安全管理措置事項を記載している。

なお、クラウドサービスの利用においては、本節及び「第２編９．SaaS 型パブリッククラウドサービスの利用」を踏まえて確認・検討すること。

### ５．１．教育情報セキュリティ管理者の措置事項

【趣旨】

教育情報セキュリティ管理者が、当該学校における情報セキュリティ対策のため実施すべき措置について規定する。なお教職員等の遵守事項については「第２編５．２．教職員等の遵守事項」に規定する。

【例文】

（１）情報資産の管理

① 情報資産の持ち出し及び持ち込みの記録管理

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

② 情報資産の廃棄管理

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

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

（２）教職員等の情報セキュリティ意識醸成

① 教育情報セキュリティ管理者は、教職員等に対して、日頃から情報セキュリティに関する話題を積極的に提供し、情報セキュリティ研修を受講させるなど、積極的にセキュリティ認識の向上を図らなければならない。

② 教育情報セキュリティ管理者は、校内でセキュリティ事故につながりかねないヒヤリ・ハット事案を抑止するために、教職員等が事案を発見した際に、ただちに対処し、すみやかに報告が上がるよう、教職員等に対する情報セキュリティ意識の醸成と風通しのよい関係性維持に努めなければならない。

③　情報セキュリティポリシー等の閲覧容易性確保

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・確認できるように配慮しなければならない。

（3）端末等の持ち出し及び持ち込みの記録

教育情報セキュリティ管理者は、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。

（4）教職員等への情報セキュリティポリシー等の遵守指導

①　教育情報セキュリティ管理者は、新規採用教職員等及び他自治体から本市に新規赴任した教職員等、及び非常勤及び臨時の教職員に対し、教育情報セキュリティポリシー等遵守すべき内容を理解・浸透するように指導を行わなければならない。

②　教育情報セキュリティ管理者は、教職員等に対して、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。

（5）新規ソフトウェア及びコンテンツの導入・利用判断

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

（6）インターネット接続及び電子メール利用の制限

①　教育情報セキュリティ管理者は、教職員等に業務端末による作業を行わせる場合において、業務以外でのインターネット接続及び電子メールの利用をしないよう教職員等に指導しなければならない。

なおWebフィルタリングの設定について、教職員等から相談があった場合は、教育情報システム管理者に上申して、判断を仰がなければならない。

②　教育情報セキュリティ管理者は、パソコンやモバイル端末の機能は、教職員等の業務内容に応じて、不必要な機能については制限することが適切である。

（7）校内及び執務室での管理

教育情報セキュリティ管理者は、教職員等と協力して下記を管理しなければならない。

①　来校者の氏名及び入退時刻を記録しなければならない。

② 来校者には名札などを着用させ、第三者であることが識別できるようにしなければならない。
③ 地域住民、保護者などに校内施設を開放する場合、執務室等開放していない施設へは入場できないよう制限を設けなければならない。

（8）自己点検の実施
① 教育情報セキュリティ管理者は、年1回、学校の自己点検を行わなければならない。
② 教育情報セキュリティ管理者は、自己点検の結果を情報セキュリティ委員会に報告しなければならない。

（解説）

（1）情報資産の管理

教育情報セキュリティ管理者は、教職員等による情報資産の外部持ち出し及び外部委託による廃棄処理について、記録管理の運用を行わなければならない。

① 情報資産の持ち出し及び持ち込みの記録管理

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、管理者の確認欄等を設ける。
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、管理者の確認欄等を設ける。

（2）教職員等の情報セキュリティ意識醸成

教育情報セキュリティ管理者は、教職員等に対する情報セキュリティ意識の醸成及び風通しのよい関係性維持を行わなければならない。また、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。

（3）端末等の持ち出し及び持ち込みの記録

教育情報セキュリティ管理者は、（1）にて規定した情報資産の持ち出し及び持ち込みだけではなく、端末そのもの等の持ち出し及び持ち込みについても、記録し保管しなければならない

（4）教職員等への情報セキュリティポリシー等の遵守指導

教育情報セキュリティ管理者は、新規採用教職員等及び他自治体から本市に新規赴任した教職員等に、及び非常勤及び臨時の教職員に対し、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。

（5）新規ソフトウェア及びコンテンツの導入・利用判断

教育情報セキュリティ管理者は、ソフトウェア・コンテンツの利用制限解除や新規導入について、教職員等から相談を受けた際、教育情報システム管理者に上申し判断を仰がなければならない。

（7）校内及び執務室での管理

教育情報セキュリティ管理者は教職員等と協力し、来校者の記録管理を行うとともに、来校者の識別や執務室等の開放していない施設への入場制限を行わなければならない。

（8）自己点検の実施

教育情報セキュリティ管理者は、当該学校の自己点検を行い、その結果を情報セキュリティ委員会に報告しなければならない。

5．2．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。

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】

教職員等は、教育情報セキュリティ管理者の指導の下、以下の規定を遵守しなければならない。

（1）教育情報セキュリティポリシー等の遵守

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）執務上での管理

① 執務室の施錠管理

執務室にて教職員等が不在となる場合には、執務室を施錠しなければならない。

② 来校者等への対応

来校者等を執務室に入れる場合には、教育情報セキュリティ管理者または学校教育情報セキュリティ・システム担当の許可を求めなければならない。

③ 机上の書類・端末等の管理

教職員等は、パソコン、モバイル端末、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。

（3）支給端末の取扱い

① 教職員等は、業務目的以外で支給端末を利用してはならない。

② 教職員等は、外部のソフトウェアを無断で支給端末にインストールしてはならない。業務上必要な場合には、事前に教育情報セキュリティ管理者の許可を得ること。

③ 教職員等は、支給端末の利用において、下記のカスタマイズを無断でしてはならない。

(ア)セキュリティ機能に関する設定変更

(イ)メモリ増設等の改造

④ 教職員等は、モバイル端末を利用する場合は、盗難・紛失リスクに備えての安全管理をすること。

⑤ 業務端末から離れる時は、端末をロックするなど、他者が閲覧できないようにしなければならない。

⑥ 業務終了後と外出時には、電源を落とさなければならない。

（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

① 教職員等は、業務上やむを得ない場合を除いて、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。

② 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、必要な安全管理措置を講じなければならない。

（５）モバイル端末や電磁的記録媒体等の持ち出し及び教育委員会・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

① 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。

② 教職員等は、外部で情報処理業務を行う場合には、教育情報セキュリティ管理者の許可を得なければならない。

（６）IDの取扱い

教職員等は、自己の管理するIDに関し、次の事項を遵守しなければならない。

① 自己が利用しているIDは、他人に利用させてはならない。

② 共用IDを利用する場合は、共用IDの利用者以外に利用させてはならない。

③ 教職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、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。

（７）パスワードの取扱い

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

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。

（８）ICカード等の取扱い

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

① 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。

② 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。

③ 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。

（９）外部電磁的記録媒体の取扱い

① 利用する外部電磁的記録媒体は教育委員会又は学校から支給された公式の媒体を使用しなければならない。その他の媒体の使用は禁止する。

② 外部電磁的記録媒体は、職員室の書庫等の鍵のかかる場所に施錠保管しなければならない。

(10) 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。

⑥ 情報ファイルを添付する場合には、パスワード設定等の対策を講じなければならない。その際、パスワードを同一メールに記載しないこと。

⑦ 送信時には誤送信を予防するため、送信先のメールアドレス、添付ファイルの内容を確認しなければならない。

⑧ 差出人、添付ファイル又は本文中のリンク先等が不審なメールを受信した場合には、添付ファイルの閲覧やリンク先（URL）にアクセスせずに、教育情報セキュリティ管理者に指示を仰ぎなければならない。

(11) クラウドサービス、ソーシャルメディアサービス利用制限

① 強固なアクセス制御による対策を講じたシステム構成でない場合、重要性分類Ⅱ以上の情報資産を、インターネットを通信経路としたパブリッククラウドサービスで取り扱ってはならない。

② 私的に契約したクラウドサービスや個人アカウントを業務利用してはならない。

③ ソーシャルメディアサービスを利用して、業務上知り得た情報を公開してはならない。

(12) 不正プログラム対策

教職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

① パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
OS及びコンピュータウイルス対策ソフトウェアが常に最新の状態に保てるようにしなければならない。自動更新される設定の場合は、自動更新設定を変えてはならない。

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、すみやかに教育情報セキュリティ管理者に報告し、指示を仰がなければならない。また、以下の対応を行わなければならない。

(ア)パソコン等の端末の場合

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

(イ)モバイル端末の場合

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

(ウ)指示があるまでは、端末の電源は切らずに保持しなければならない。

(13) 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。

③ CISOは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

(14) 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。

(15) 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。

(16) 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。

(17) 業務以外の目的でのウェブ閲覧の禁止

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。

(18) 外部からのアクセス等の制限

① 教職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、教育情報セキュリティ管理者を介して、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 教職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を施設内のネットワークに接続する前に、アンチウイルス等を通じて、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

(19) 児童生徒への指導事項

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

① 学習用途の利用限定
学習者用端末及び学習系クラウドサービスは学習目的で利用すること。

② 利用者認証情報の秘匿管理
ID及びパスワードは他の人に知られないようにすること。

③ ウイルス対策ソフトウェアの管理
ウイルス対策ソフトウェアは常に最新の状態に保つこと。

④ 端末のソフトウェアに関するセキュリティ機能の設定変更禁止
利用する端末のセキュリティ機能の設定を、許可なく変更してはならないこと。

⑤ 学習系情報は学習系クラウドに保管
端末で生成した情報の保存先を学習系クラウドに指定できる機能がある場合には、この機能を利用して原則学習系クラウドに保管し、学習者用端末にローカル保存は必要最小限とすること。

⑥ 無断で外部ソフトウェアをインストール禁止
無断で外部ソフトウェアをインストールしないようにすること。

⑦ コミュニケーションツールの利用制限
学校から許可されたコミュニケーションツール(SNS,チャット等)のみを利用すること。

⑧ ウイルス感染が疑われる場合の報告
学習用端末が動かない、勝手に操作されている、いつもと異なる画面や警告が表示されるなどの症状がでた場合、すぐに担任教員に報告すること。

⑨ 端末の安全な取扱い
学習用端末は大事に取り扱い、盗難・紛失・破損等に注意すること。

⑩　私物端末など許可されていない端末の利用禁止
私物端末など許可されていない端末を学校に持ち込んで、学校のネットワークにつながないこと。

⑪　重要性分類Ⅱ以上の情報資産（児童生徒本人の情報に限る）の管理
該当資産を端末にダウンロードした場合には、目的を達成し次第すみやかに消去を行う等の対策を講じること。また、該当資産を閲覧する際には、離席時に端末ロックし、周囲に他の児童生徒がいる状態では閲覧しない等の対策を講じること。

（20）異動・退職時等の遵守事項

教職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産（紙情報、データの格納された端末、外部記録媒体等）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。

（解説）

（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。

（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

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
・　データ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。

（５）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

外部における情報処理作業とは、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。

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、強固な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、教育情報セキュリティ管理者の包括的承認を行う等、運用実態や教職員等の負担も考慮し検討する必要がある。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、データ暗号化、通信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）教職員等の場合、仕事の持ち帰りが多い実態に鑑み、特に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を徹底すること。

（６）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は本人だけが知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。

（７）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６）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７）サービス利用時に都度ID及びパスワード等の認証情報を入力する場合、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。

（８）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。

（10）電子メールの利用制限及び留意事項

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８）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。

（11）クラウドサービス、ソーシャルメディアサービス利用制限

例えば私的に契約したWEBメール・ストレージ等のクラウドサービスや個人アカウントを用いて学校の情報資産を外部に持ち出してしまうと、教育情報セキュリティ管理者が管理できなくなるため、利用を禁止する必要がある。また、私的に契約した教育アプリケーションやコンテンツを利用する場合も、ウイルス感染等の不正アクセスリスクが存在するため、利用を禁止する必要がある。教職員等に対しては、安全性が確認されている利用が認められたサービスのみの利用を徹底する必要がある。

（12）不正プログラム対策

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。

（13）電子署名・暗号化

暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で暗号方法は、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。

（14）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９）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。

（15）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。

（16）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10）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。

（17）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。

（19）児童生徒への指導事項

学校における情報の取扱いは、教職員等のみならず、児童生徒も含まれる。GIGAスクール整備以降、児童生徒による学習活動のデジタルシフトが加速化しており、児童生徒による情報セキュリティの確保は、学校の情報セキュリティ確保のなかで大きな比重を占めるものとなってきた。その意味で児童生徒に情報モラル・セキュリティ指導を通して情報セキュリティ意識を醸成させる教員の役割は大きい。本項では、児童生徒に指導いただきたい内容について記載している。

## ５．３．教育委員会事務局職員の遵守事項

【趣旨】

教育委員会事務局では、学校の管理する一環として、教育情報システムの端末を事務局内に設置して必要に応じて学校の情報資産をモニタリングし、学校とのコミュニケーションに活用することが一般的である。そのため、教育情報システムを利用する教育委員会事務局職員は、学校の情報資産にアクセスできる立場にあることを鑑み、遵守規定を示す。

【例文】

教育委員会事務局職員は、教育情報セキュリティ責任者の指導の下、以下の規定を遵守しなければならない。

（１）教育情報セキュリティポリシー等の遵守
（２）業務以外の目的での使用の禁止
（３）校務用端末による外部における情報処理作業の禁止
（４）重要性分類Ⅱ以上の情報資産について校務用端末以外のパソコン、モバイル端末及び電磁的記録媒体等によるアクセスの禁止
（５）知りえた情報の秘匿
（６）業務を離れる場合の遵守事項

異動、退職等により業務を離れる場合には、利用していた情報資産をすべて返却する。また、その後も業務上知り得た情報を漏らさない。

（解説）

教育委員会事務局職員は、学校の情報資産にアクセスできる立場にあることから、無断での情報外部持ち出しや改ざんが可能である点で、内部脅威であり、情報セキュリティの順守義務を負う。学校では、教育情報セキュリティ管理者が教職員等を管理・指導する立場であるが、教育委員会事務局職員の情報セキュリティ順守については、教育情報セキュリティ責任者が担うこととする。

## ５．４．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

① CISOは、教職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、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。

⑤ CISO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。

５．５．情報セキュリティインシデントの連絡体制の整備

【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連絡体制を整備することも必要である。このことから、情報セキュリティインシデントを認知した場合の報告義務について規定する。

なお、報告に対する対応については、「第２編７．９．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）学校内からの情報セキュリティ違反行為の報告

① 教職員等は、教育情報セキュリティポリシーに対する違反行為を発見した場合、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。

（３）住民等外部からの情報セキュリティインシデントの報告

① 教職員等は、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】

（４）情報セキュリティインシデント原因の究明・記録、再発防止等

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。

（５）支給端末の運用・連絡体制の整備

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

（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）教職員等は、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）学校内からの情報セキュリティ違反行為の報告

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。

（３）住民等外部からの情報セキュリティインシデントの報告

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。

（４）情報セキュリティインシデント原因の究明・記録、再発防止等

情報セキュリティインシデントの原因を究明し、効果的な再発防止策を検討するために、教育情報セキュリティ管理者は、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。

（５）支給端末の運用・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。

教職員等が利用する端末を含めて、特に紛失・盗難等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。

## 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、オンプレミスの場合と民間事業者のデータセンターを利用する外部委託の両方を想定している。なお、IaaS・PaaS 型クラウドサービスを利用してコンピューティングリソースを調達して、教育情報システムを構築・運用する場合は「第２編８． 外部委託」を、SaaS 型パブリッククラウドを利用する場合は「第２編９．SaaS 型パブリッククラウドサービスの利用」を軸に検討すること。

### ６．１．コンピュータ及びネットワークの設定管理

【趣旨】

ネットワークや情報システム等の設定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、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。

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

（２）バックアップの実施

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）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。

（4）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。

（5）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。

（6）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。

（7）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、強固なアクセス制御による対策を講じたシステム構成の場合は、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。

（8）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。

（9）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。

(10) 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、解読が困難な通信の暗号化及び認証技術の使用を義務付けなければならない。

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、通信の暗号化等の措置を講じなければならない。

(11) 電子メールのセキュリティ管理

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】

（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データの外部流出の可能性を考慮し、データ暗号化等による安全管理措置を講じることが重要である。

なお、データ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）ログの取得等

ログ（アクセスログ、システム稼動ログ、障害時のシステム出力ログ）及び障害対応記録は、悪意の第三者等による不正侵入や不正操作等の情報セキュリティインシデントを検知するための重要な材料となる。また、情報システムに係る情報セキュリティの上の問題が発生した場合には、当該ログ等は、事後の調査の過程で、問題を解明するための重要な材料となる。したがって、情報システムにおいては、仕様どおりにログ等が取得され、また、改ざんや消失等が起こらないよう、ログ等が適切に保全されなければならない。

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

（注２）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。

（４）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。

（５）外部の者が利用できるシステムの分離等

保護者や外部の教育関係者が訪問した際に利用するプリンタなど、外部の人々が利用できるシステムは、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。

（６）外部ネットワークとの接続制限等

所管するネットワークにおいて、インターネットに接続し、公開し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３）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。

（７）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、強固なアクセス制御による対策を講じたシステム構成においては、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「第２編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。

各教育委員会においては、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。

（８）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 及び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４）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。

（９）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及び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及びパスワード等の認証を求める運用にする。

（注５）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。

（10）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６）暗号化方式の１つであるWEP（Wired Equivalent Privacy）及び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７）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。

（11）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である。

（注８）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９）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。

## 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

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。特に強固なアクセス制御による対策を講じたシステム構成の場合、重要性分類Ⅱ以上の情報資産へのアクセスについては、多要素認証等のアクセスの真正性に関する要素技術を取り入れることで、当該システムへの認証強度の向上とアクセス権管理を徹底すること。

（２）外部からのアクセス等の制限

① 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。

② 統括教育情報セキュリティ責任者は、民間事業者等の外部組織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。

③ 統括教育情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために通信の暗号化等の措置を講じなければならない。

④ 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、モバイル端末管理（MDM）の導入等を通じて、セキュリティ確保のために必要な措置を講じなければならない。

⑤ 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）端末とネットワークの接続可否の自動識別（端末認証）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）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

各情報資産の分類に応じてアクセス制御を適切に講じることが重要である。例えば重要性分類Ⅱ以上の情報資産については、教職員等が職務上必要な場合に限って情報資産にアクセスできるよう設定することや、児童生徒およびその保護者が児童生徒本人の情報のみに限ってアクセスできるよう設定することが、情報セキュリティの確保において非常に重要である。権限を付与する際は、必要な権限のみ（編集・閲覧・複製・ダウンロード等）を付与することにも留意されたい。また、そのアクセス権限が運用実態に沿った適切なものかどうか、定期的に確認することが必要である。重要性分類に応じた管理の在り方については、「第２編３.２. 情報資産の管理」を参照すること。

多要素認証等のアクセスの真正性に関する要素技術を取り入れることで、認証強度の向上とアクセス権管理を徹底すること。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。

（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、データ暗号化、通信の暗号化、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１）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２）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）端末とネットワークの接続可否の自動識別（端末認証）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）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。

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「第２編９．SaaS型パブリック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。例えば次世代校務DX環境の整備に際し、「ネットワーク分離による対策を講じたシステム構成」等から「強固なアクセス制御による対策を講じたシステム構成」へ移行する際には、その移行期間において、オンプレミス環境とパブリッククラウド環境が共存することが想定される。このような場合についても、本規定を参照し、それぞれの環境に応じた適切なセキュリティ対策を講じること。

【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

## 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。

（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。

（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化、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。そのため、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を講じることが重要である。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。

（注４）昨今特に大きな脅威となっているものとして「Emotet（エモテット）」が挙げられる。悪意のある者により、不正なメールに添付されるなどして、感染の拡大が試みられている。Emotetの感染を狙う不正なメールの中には「正規メールへの返信を装う」手口が使用される場合があり、受信者が違和感を抱かないよう工夫されているのが特徴である。その他、添付ファイルを暗号化することでウイルス対策ソフトの検知を逃れるケースも報告されている。Emotetへの感染を予防し、被害を最小限にとどめるための対策として「組織内への注意喚起の実施」、「信頼できないWord文書やExcelファイルにおいてマクロの実行禁止」、「メールの監査ログの取得やSOCによる常時監視」のほか、Emotet対策だけに限らないが、「ダウンローダーがC&Cサーバと通信できないネットワーク環境とすること」、「暗号化されたファイルが添付されたメールのゲートウェイでの着信拒否」などが挙げられる。

その他、Emotetの最新情報や対策の具体的な内容については、独立行政法人情報処理推進機構やJPCERTコーディネーションセンター（JPCERT/CC）のウェブサイトで確認できるため、参照することが望ましい。

参考：独立行政法人情報処理推進機構「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて

（https://www.ipa.go.jp/security/announce/20191202.html）

参考：JPCERT/CC「マルウエア Emotetへの対応 FAQ」

（https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html#7）

（注５）Emotetと並んで大きな被害を生んでいるウイルスの種類としてランサムウェアが挙げられる。ランサムウェアとは、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語である。従来は感染した端末等に特定の制限をかけ、その解除と引き換えに金銭を要求していたが、令和元年頃からパソコン内のファイルの暗号化に加え、身代金を支払わなければそのファイルの内容を公開するといった被害者に対して情報漏洩を迫る脅迫手法も確認されるようになった。身代金を払ったとしても攻撃元が情報を正常な状態に戻す、又は外部に公表しないといった行為をとる確証は全くない。

ランサムウェアの感染経路としては、VPN機器等のネットワーク機器の脆弱性を利用した侵入、リモートデスクトップからの侵入、不審メールやその添付フ

ァイルが多い。（警察庁「令和４年上半期におけるサイバー空間をめぐる脅威の情報等について」）また、USBメモリ等の電磁的記録媒体を介して感染する場合も想定される。

ランサムウェアの対策を実施するための具体的な方法については、以下のドキュメントやウェブサイトが参考となるため、参照することが望ましい。

参考：NISCサイバーセキュリティ・ポータル（ストップ！ランサムウェアランサムウェア特設ページ）

（https://www.nisc.go.jp/tokusetsu/stopransomware/index.html）

参考：JPCERT/CC「ランサムウェア対策特設サイト」

（https://www.jpcert.or.jp/magazine/security/nomore-ransom.html）

参考：独立行政法人情報処理推進機構「ランサムウェアの脅威と対策～ランサムウェアによる被害を低減するために～」（2017年１月27日）

（https://www.ipa.go.jp/files/000057314.pdf）

（注６）フィッシングとは、公的機関や金融機関など、実在する組織や個人になりすました攻撃者がメールやSMSを送信し、正規のウェブサイトを模倣した偽サイトに誘導させることで、認証情報、ATMの認証番号、クレジットカード番号といった重要な機密情報を詐取する手口である。昨今は、より一層利用者が気づきにくい手口で重要な機密情報の取得を試みるケースもあり、さらなる注意が必要になる。対策として、「メールやSMSに添付されているURLは安易にクリックせず、ウェブサイトにアクセスする際は、あらかじめ登録しているURLからアクセスする」、「Webサービスにログインする場合に、多要素認証等の設定が可能な場合、有効化する」などが挙げられる。フィッシングメールに対する対策、対応の詳細は以下のドキュメントに記載されているため、参照することが望ましい。

参考：独立行政法人情報処理推進機構「情報セキュリティ10大脅威2024」解説書、フィッシングによる個人情報等の詐取（24頁から25頁）（2024年２月）

（https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.pdf）

（注７）昨今特に大きな脅威となっているものとして「詐欺サイト」が挙げられる。インターネットで調べごとをしているとき、突然画面に「セキュリティの警告」が広がり、サポートに連絡してください、画面上のボタンを押してくださいなどの指示が行われる。Webフィルタリングで多くのサイトへのアクセスは防げるが、完全な削除は技術的に困難であり、画面の中のボタンを押さない、画面に書いてある番号に電話しない、画面の指示につられて個人情報の入力や、料金の支払いを行わない、という基本対策の徹底が有効な対策である。

（２）教育情報システム管理者の措置事項

ウイルスチェック等のパターンファイルや不正プログラム対策ソフトウェアは常に最新の状態に保って利用することが不可欠である。

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

## 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）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。

（４）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、ベンダー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）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

（４）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、対策の検討に当たっては、「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）

## 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」策定に当たっての指針（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。

## ７．運用

クラウドサービスの利用においては、本項及び「第２編９．SaaS型パブリッククラウドサービスの利用」を踏まえて確認・検討すること。

### 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。特に強固なアクセス制御による対策を講じたシステム構成の場合、重要性分類Ⅱ以上の情報資産へのアクセスについては、侵入検知システム（IDS）や侵入防御システム（IPS）などの端末・サーバ・通信の監視・制御等によるセキュリティ対策を講じなければならない。

（２）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の情報資産を格納するシステムを常時監視しなければならない。【推奨事項】

（５）内部からの攻撃監視

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。

（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。また、インターネットと繋がっているサーバ(Webサーバ)への外部からの攻撃を検知し、防御する機能であるWAF（Web Application Firewall）も存在する。このようなネットワーク監視・制御等によるセキュリティ対策は年々重要性を増しており、近年ではネットワークとセキュリティを統合してクラウドサービスとして提供するSASE（Secure Access Service Edge）というサービスモデルも出現している。

（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。

（５）内部からの攻撃監視

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。

７．２．ドキュメントの管理

【趣旨】

情報セキュリティ対策の詳細を記載したドキュメント類は機密事項に相当し、外部情報漏えいによって攻撃者の手に渡ることを防ぐ必要があることから、その意味で情報システムの仕様書、運用管理記録等情報セキュリティに関するドキュメント管理を厳格に行う必要がある。また、設計変更や障害での対策等の経緯を含めた記録管理により、常にアップデートされた状態を保持することも、故障やセキュリティ侵害時等の対応で必要になるものであり、情報セキュリティ確保における必須事項である点に留意いただきたい。

【例文】

（１）システム管理記録及び作業の確認

① 教育情報システム管理者は、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。

（２）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。

（３）障害記録の管理

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、教職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

（４）記録の保存

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。

（解説）

（１）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。

（２）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。

（３）障害記録の管理

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１）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。

（４）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２）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。

## ７．３．教職員等の ID 及びパスワードの管理

【趣旨】

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

【例文】

（１）利用者 ID の取扱い

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、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。

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、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

（２）パスワードに関する情報の管理

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。

（解説）

実際に不正アクセスの多くは、利用者認証情報の外部流出に起因して発生している。情報セキュリティ強化において、利用者認証の強化が最優先で求められており、多要素認証導入が進む一方で、知識認証（ID及びパスワード等）に頼るだけの情報システムも数多く存在する。教職員等のID及びパスワードの管理は不正アクセスを起こさないための要であり、管理の重要性は計り知れないことを念頭に置くべきである。

なお、パスワードの取扱いについては、「第２編５.２．教職員等の遵守事項（７）パスワードの取扱い」にパスワード設定等の具体的な内容が示されているため、参照されたい。

## ７．４．ICカード等の取扱い

【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「第２編７．５．児童生徒におけるID及びパスワード等の管理」も参照すること。

【例文】

（１）ICカード等の取扱い

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、ICカード等の紛失等の通報があり次第、当該ICカード等を使用したアクセス等を速やかに停止しなければならない。

② 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。

（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。

## ７．５．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及びパスワードに対して安全管理措置を講じなければならない。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及び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及び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、一度の認証を行うことで、複数のシステムへのアクセスを可能とする技術もある。

【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。

（２）多要素認証等によるなりすまし対策

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

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

（３）学習用ツールへのシングルサインオン

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

(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、個人情報に該当するものである。そのため個人のIDを集約した管理データは、個人情報保護法に基づく適切なID管理が求められている。

（2）多要素認証等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及びパスワードに加え、多要素認証を設定し、本人確認を厳格に行うことが有効である。

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

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。

また、パスワードの取扱いについては、「第２編５.２. 教職員等の遵守事項（７）パスワードの取扱い」にパスワード設定等の具体的な内容が示されているため、参照されたい。

（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当たりID及びパスワードの入力など認証操作が必要になるが、サービスを利用する児童生徒側においては都度の認証情報入力による運用の煩雑化や、児童生徒の認証情報を管理する教育委員会や学校現場からすると管理が複雑化して運用負荷やリスクが高くなる。

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及びパスワードは漏洩した際の影響範囲が大きいため、必要に応じて多要素認証と組み合わせることでよりセキュリティリスクを低減することができる。

## ７．６．特権を付与されたIDの管理等

【趣旨】

管理者権限（クラウドサービス・サーバの全ての機能を利用できる権限）等の特権を付与されたIDは、全ての機能が利用可能であることから、限られた利用者のみが運用する等の厳格な管理が求められる。

このことから、特権を付与されたIDの管理に係る手続きについて規定する。

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

（２）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。

（３）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。

（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、特権を付与されたID及びパスワードの変更について、外部委託事業者に行わせてはならない。

（５）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。

（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、特権を付与されたIDを初期設定以外のものに変更しなければならない。

（７）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】

（解説）

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。

（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。

## ７．７．教育情報セキュリティポリシーの遵守状況の確認・管理

【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。

② CISOは、発生した問題について、適切かつ速やかに対処しなければならない。

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）業務以外の目的でのウェブ閲覧の禁止

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

（４）教職員等による不正アクセスの管理

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。

（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）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。

（４）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。

## ７．８．専門家の支援体制等

【趣旨】

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

【例文】

（１）専門家の支援体制

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

（２）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。

（解説）

（１）専門家の支援体制

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

（２）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１）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。

７．９．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。

## ７.10. 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１）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。

## ７.11. 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】

（１）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）

（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。

## ７.12. 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。

## 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、SaaS型パブリッククラウドサービスを利用する場合は、「第２編９．SaaS型パブリック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。

（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）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当たり、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当たり、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）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、再委託先も含め、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。

また、契約を行う際に「外部委託先に関するセキュリティ要件のチェックシート」（後述）に基づいて、委託事業者のセキュリティ要件の遵守状況を確認する必要があるほか、定期的に（１年に１回程度）確認することが有効である。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。また、教育情報システム管理者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、速やかに報告させる必要がある。

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「第２編10．１．監査（４）外部委託事業者に対する監査」を参照されたい。

| 項目 | 確認事項 | チェック欄 |
|---|---|---|
| １.基本事項 | 契約に係るデータ及び知り得た秘密等の取扱いについて、その重要性を認識し、適切に取扱う。 | ☑ |
| ２.法令等遵守 | 個人情報の保護に関する法令等を遵守する。 | ☑ |
| ３.秘密の保持 | 契約の履行に際して知り得た秘密を他に漏らさない。 | ☑ |
| | 契約の終了後、解除後及び職を退いた場合においても同様とする。 | ☑ |
| ４.目的外使用及び第三者への提供禁止 | 契約に係るデータを委託者が指示する目的以外に使用し、第三者に提供しない。 | ☑ |
| ５.データの受領 | 委託者からデータ等の提供を受けた場合は、データ等の受領証を作成し、委託者に提出する。 | ☑ |
| ６.データの持ち出し | 委託者の環境からデータを持出す場合は、書面で持出す目的、データの内容及び暗号化等の対策を記し、委託者から承認を受ける。 | ☑ |
| | 委託者の環境から業務システムで利用している本番データ（住民情報が含まれるデータ）を持出すことを禁止する。業務委託契約において本番データの持出しが認められている場合は、都度書面で申請し、委託者から承認を受ける。 | ☑ |
| ７.複写及び複製の禁止 | 本契約に係るデータを委託者の承認なく、用紙、記録媒体等に複写し、又は複製しない。 | ☑ |
| ８.パソコン及びデータの持込み | 委託者の環境にパソコン及びデータを持込み、作業を行う場合は、書面で委託者からパソコン及びデータ持込みにかかる承認を受ける。 | ☑ |
| ９.安全管理義務 | 契約に係るデータの管理責任者を定め、業務の従事者を限定する。 | ☑ |
| | 契約に係るデータを取扱う場所を特定する。 | ☑ |
| | データの無断持出し禁止を周知徹底し、やむを得ず、持ち出す場合は、委託者の承認を得たうえで、管理簿等の書面に記録する。 | ☑ |
| | 紛失、損傷、焼失等の事故が生じないよう安全かつ適切な管理体制を整備する。 | ☑ |
| | パソコンやデータを持ち込む場合、最新のウイルス対策ソフト等の使用していることや不正なプログラムが書かれていないことを確認する。 | ☑ |
| 10.データの返却・消去 | 委託者から借用したデータは、速やかに返却する。借用したデータを複製・保存した場合は消去し、消去したことが分かる書類を委託者に提出する。 | ☑ |
| 11.記録媒体の廃棄 | 契約の履行上、委託者から廃棄指示がある場合の記録媒体等は、確実に物理的に破壊し、又はすべての記録を復元不可能な状態に消去した後に廃棄し、廃棄したことが分かる書類を委託者に提出する。 | ☑ |
| 12.監督及び監査 | 委託者が、契約の履行に関し必要があるときは、受託者及び再委託先に対して報告を求め、監査を行い、又は監査に立会うことができるように、体制等を整備する。 | ☑ |
| 13.教育 | 従業者に対して、データの保護及び秘密の保持等データの取扱いに関し履行すべき責務について充分な教育を行う。 | ☑ |
| | 教育の実施状況を記録する | ☑ |
| 14.事故発生の報告義務 | 安全管理措置等が履行できない場合及び情報漏えい等の事故が発生した場合等に備え、直ちに委託者へ通知、報告できる体制を整備する。 | ☑ |
| 15.再委託の禁止 | 委託者の承諾なしに、業務を第三者に委託し又は請け負わせない。 | ☑ |
| | 委託者の承諾を受けて再委託した場合は、再委託者に本契約の規定を遵守させる。 | ☑ |

**図表12　外部委託先に関するセキュリティ要件のチェックシート（サンプル）**

（出典：総務省「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」改定のポイントについて②（情報セキュリティインシデント関係）
https://www.soumu.go.jp/main_content/000857160.pdf）

（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。

## ９．SaaS型パブリッククラウドサービスの利用

本項では、クラウドサービス利用のうち、SaaS型パブリッククラウドサービスを教職員等及び児童生徒が直接利用する場合について、クラウドサービスの安全性及びクラウド事業者の信頼性等を確認するプロセスについて記載する。尚、本ガイドラインは、IT事業者が、クラウドサービスの一類型であるIaaSの上に自社や他社のサーバを運用し、クラウド利用者にサービス提供するモデルでは、クラウド利用者は、当該事業者に対してSaaSと同等の契約を満たすことを求めることを推奨する。本項の「クラウド利用者」とは、クラウドサービスの選定・契約の主体である教育委員会等を指す。

※クラウドサービスの特徴や教育情報システムでの活用意義等については、「第１編第３章 教育現場におけるクラウドの活用について」を参照すること。

SaaS型パブリッククラウドサービス利用が安全であり、クラウド事業者が信頼できるパートナーであることについては「クラウド事業者が提供するクラウドサービスが必要充分な情報セキュリティ対策を講じられていること」、「クラウド事業者のサービス提供ポリシー等から信頼できるパートナーであることを確認すること」の２つの観点で確認が必要である。各観点について、「第２編９．１．SaaS型パブリッククラウドサービスの利用における情報セキュリティ対策」及び「第２編９．２．SaaS型パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項」にそれぞれ記載しているため、参照すること。

なお、SaaS型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場合も多いため、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。

まずは第三者認証取得の有無、監査報告書等からクラウド事業者と提供するクラウドサービスの安全性、信頼性を優先的に確認することを推奨する。

また第三者認証を有していない場合でも、インフラ基盤供給を受けるIaaS・PaaS事業者が第三者認証を有する場合もあるため、その場合は、SaaS型パブリッククラウド事業者がSaaS提供する範囲を優先して、「第２編９．１． SaaS型パブリッククラウドサービスの利用における情報セキュリティ対策」及び「第２編９．２．SaaS型パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項」に示した規定を確認することが求められる。

## ９．１．SaaS型パブリッククラウドサービスの利用における情報セキュリティ対策

【趣旨】

本項では、SaaS型パブリッククラウドサービス（学習eポータル、デジタル教科書、デジタルドリル、協働学習支援サービス、デジタルコンテンツ配信サービス、校務支援システム、学校ホームページ作成サービス、緊急連絡網サービス等）の情報セキュリティ対策が適切に講じられているかを確認する内容について記載する。尚、本ガイドラインは、IT事業者が、クラウドサービスの一類型であるIaaSの上に自社や他社のサーバを運用し、クラウド利用者にサービス提供するモデルでは、クラウド利用者は、当該事業者に対してSaaSと同等の契約を満たすことを求めることを推奨する。第三者認証取得の確認等から、クラウド事業者と提供するクラウドサービスの安全性、信頼性を間接的に確認できた場合についても、各規定についてひととおり報告を求めて内容を確認し、契約内容に反映することが望ましい。

【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、「７．６．特権を付与されたIDの管理等」を遵守しなければならない。 |  |

（２）アクセス制御

| | |
|---|---|
| ① クラウド利用者は、当該クラウドサービスに対して、アクセスする権限のない者がアクセスできないように、システム上制限する機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。 |  |

| | |
|---|---|
| ② クラウド利用者は、クラウド事業者の提供するアクセス制御機能を用いて、情報資産毎に、許可されたクラウドを利用する教職員等及び児童生徒のみがアクセスできる環境を設定しなければならない。 |  |

（３）クラウドに保管するデータの暗号化

| | |
|---|---|
| ① 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「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、「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）」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、クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）に当たり、セキュリティを確保した対応となっているかをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。<br>なお、当該確認に当たっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。 |  |

（８）クラウドサービスを提供する情報システムの運用管理

| | |
|---|---|
| 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、「４．１．サーバ等の管理（２）サーバの冗長化」に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。 |  |

| | |
|---|---|
| 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及び復旧手順について、「６．１．コンピュータ及びネットワークの設定管理（２）バックアップの実施」に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。 |  |
| 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、「６．１．コンピュータ及びネットワークの設定管理（３）ログの取得等」に準じた対策をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。 |  |

（９）クラウドサービスを提供する情報システムのマルウェア感染対策

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

（10）クラウド利用者側のセキュリティ確保

| | |
|---|---|
| ①　クラウド利用者は、クラウドサービスにアクセスするクラウドを利用する教職員等及び児童生徒側端末について、保管するデータの外部流出、改ざん等から保護するために必要な措置を講じなければならない。 |  |

| | |
|---|---|
| ② クラウド利用者は、標的型攻撃による外部からの脅威の侵入を防止するために、クラウドを利用する教職員等及び児童生徒への教育や入口対策を講じなければならない。 |  |

(11) クラウド事業者従業員の人的セキュリティ対策

| | |
|---|---|
| ① クラウド利用者は、クラウドサービスに関わるクラウド事業者従業員に対して、クラウド事業者の情報セキュリティポリシー及び保守運用管理規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）サービス終了時等のデータの廃棄及び利用者アカウント抹消

| | |
|---|---|
| ① クラウド利用者は、サービス利用終了時等において、クラウド利用者のデータ及び利用者アカウント情報が不用意に残置されないよう、適切に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。 |  |
| ③ クラウド利用者は、クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。 |  |

（13）クラウドサービス要件基準を満たす配慮を含めたネットワーク設計

| | |
|---|---|
| ① クラウド利用者は、利用するクラウドサービスの要件基準を確認し、要件基準を満たすネットワークを設計しなければならない。 |  |

【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、知識認証（ID及びパスワード等）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知識認証（ID及びパスワード等）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

ここでのアクセス制御の意味は、クラウドサービスでのデータ保管において、アクセス権限に応じてアクセスできるフォルダを制限する機能（狭義のアクセス制御の機能）を指す。

学校には、学校管理者、一般教職員、児童生徒が存在し、各々の立場・役割に応じてアクセスできる情報が異なる。また、学習系情報と校務系情報については、各情報資産にアクセスする主体がそれぞれ異なるため分類して管理する必要があることから、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、クラウドを利用する教職員等及び児童生徒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、通信の暗号化を行う等、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。

③機器内部の記憶装置から全ての情報を消去のうえ復元不可能な状態にするなどの処置は、情報資産が許可なく第三者に漏えいすることを防ぐためであり、装置等の資源が適切に処分されることをクラウドサービス事業者の方針及び手順が組織やシステムが求める基準を満たしているか確認することが重要である。

ただし、クラウド利用者側が直接装置等の資源に対して情報の抹消や破壊を行うことが暗号化消去以外には難しいクラウドサービスにおいては、監査報告書や媒体・装置の「廃棄証明書」等を入手して確認することが考えられる。特に重要性分類Ⅲ以上の情報資産の記録された資源の処分においては、記憶装置や記憶媒体の破壊など復元不可能な処理が行われていることを確認する必要がある。

（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、４． 物理的セキュリティ及び６． 技術的セキュリティ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感染対策

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。

既知のマルウェア感染対策に加えて、インターネットからの未知のマルウェア感染対策が重要になり、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検知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クラウド利用者側端末は、クラウドサービスを提供する情報システム同様、マルウェア感染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、クラウド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及び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

① 不完全なデータの廃棄及び利用者アカウント情報の抹消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を確認することが望ましい。

② SaaS型パブリック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。

③ SaaS型パブリッククラウドサービスで扱う情報資産の移行及び削除に当たっては、クラウドサービスモデルにより異なり、情報資産が保管されているハードウェアはクラウドサービス事業者が所有していること及びそのハードウェアがクラウドサービス利用者間で共有されることを、利用するサービスモデルに応じて考慮する必要がある。情報資産のクラウドサービスでの利用を終了する場合、利用終了時までには、そのデータがクラウドサービス事業者及び他のクラウドサービス利用者に参照されないような処理 (暗号化等) を施す必要がある。これらのセキュリティ対策は、クラウドサービス選定や契約時における対策だけでなく、契約後の情報システムの導入・構築、その後の運用・保守、更には契約終了時に至るまで情報システムのライフサイクル全般において行う必要があり、セキュリティ対策の実施状況やその可否は、①②に記載したとおり契約前に確認しておく必要がある。

(13) クラウドサービス要件基準を満たす配慮を含めたネットワーク設計

クラウドサービスが所定の機能・性能を発揮する条件として、クラウドサービスが求める要件基準を満足する利用が求められるため、要件基準がクラウド利用者として受け入れられるかを確認する必要がある。特にネットワーク帯域・遅延特性により、クラウド利用者の体感するクラウドサービスの機能・性能が変わり、可用性を満たさないリスクがあるため、クラウドサービスが求める要件基準を満足するネットワークを設計することが必要である。

## ９．２．SaaS型パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項

【趣旨】

クラウド利用者は、教育情報システムにSaaS型パブリッククラウドサービス（学習eポータル、デジタル教科書、デジタルドリル、協働学習支援サービス、デジタルコンテンツ配信サービス、校務支援システム、学校ホームページ作成サービス、緊急連絡網サービス等）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。

第三者認証取得の確認等から、クラウド事業者と提供するクラウドサービスの安全性、信頼性を間接的に確認できた場合についても、外部サービス利用として契約により情報セキュリティを確保する観点から、各規定について報告を求めて内容を確認し、契約内容に反映することが必要である。

【例文】

（１）守秘義務、目的外利用及び第三者への提供の禁止

| | |
|---|---|
| ① 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

| | |
|---|---|
| ① 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。<br>（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。<br>確認すべき項目例を下記に示す。<br>（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<br>（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<br>（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、インシデントに備えた組織体制を整備しなければならない。 |  |

（８）クラウドサービスの提供水準及び品質保証

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

（9）クラウド事業者の再委託先等との合意事項

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

（10）その他留意事項

| | |
|---|---|
| ① クラウド利用者は、クラウド事業者がサービスを安定して提供可能な企業・団体であるかについて考慮しなければならない。 |  |
| ② クラウド利用者は、クラウド事業者間でのデータ形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。また、国内法以外の法令及び規制が適用される場合にはそのリスクを評価した上でクラウド事業者を選定しなければならない。 |  |
| ④ クラウド利用者は、クラウド事業者において個人情報の適切な管理が行われているか確認するとともに、確認した項目については、調達時においてサービスの過剰な排除にならないよう留意した上で、契約要件等として定めなければならない。 |  |

（解説）

（1）守秘義務、目的外利用及び第三者への提供の禁止

SaaS型パブリッククラウドサービス事業者は、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、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

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ーもあるため、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

クラウドサービスにおける監査は、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。

「第２編９．１．SaaS型パブリッククラウドサービスの利用における情報セキュリティ対策」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。

インシデント発生時の即応体制として、クラウド事業者に対して調査協力、情報提供等を速やかに指示できるクラウド利用者側での体制（教育CSIRT）とクラウド利用者及び事業者との連絡体制を確立しておく必要がある。

（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 インターネットを介して提供されるクラウドサービスの利用に当たっては、クラウドサービス事業者の事業所の場所にかかわらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。

具体的には、クラウドサービス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るデータセンターを選択する必要がある。管轄裁判所に関しては、国外の裁判所で裁判を行うこととならないよう、契約において日本国内の裁判所（必要に応じて地方公共団体の所在地を管轄する裁判所）を合意管轄裁判所として規定する必要がある。また、外国に本社を置く企業が提供するサービスを地方公共団体が利用する場合の紛争を当該企業の本社の所在地を管轄する裁判所が管轄することも考えられる一方、その場合は日本の国内法と同等の個人情報の保護などが確立されないおそれがあることについて、クラウド利用者は契約締結の際に十分に留意する必要がある。

重要性が相対的に低い情報であっても、クラウド事業者が海外のデータセンター等にサーバ装置を設置してサービスを提供している場合は、当該サーバ装置に保存されている情報に対し、現地の法令等が適用され、現地の政府等による検閲や接収を受ける可能性があるというリスクが許容できること確認した上で選択すること。

④　SaaS型パブリッククラウド利用者は、ISO/IEC27018等第三者認証の取得の確認など、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の、個人情報の取扱いに関する事項についてクラウド事業者に確認を行う必要がある。

なお、個人情報保護については、令和３年に行われた個人情報保護法改正により、地方公共団体の個人情報保護制度についても改正後の法律において全国的な共通ルールが規定され、個人情報保護委員会が、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。改正法施行前は、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ったところ、改正法施行後は、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」場合に、条例で定めるところにより、審議会に諮問することができることとなっている。「特に必要な場合」とは、個人情報保護制度の運用やその在り方についてサイバーセキュリティに関する知見等の専門的知見を有する者の意見も踏まえた審議が必要であると合理的に判断される場合をいう。

よって、クラウドサービス活用において個人情報を取り扱う際は、令和３年改正個人情報保護法に則った対応が必要であり、個人情報保護審議会への諮問については特に必要である場合にのみ可能となった点に留意されたい。

### ９．３．SaaS型パブリッククラウドサービス利用における教職員等の留意点

【趣旨】

クラウドサービスとは、システムを構成する端末、ネットワーク、サーバのうち、サーバの処理能力を貸し出す（提供する）サービスである。代表的なクラウドサービスとして、サーバ機能（アプリ・コンテンツ提供）を複数の利用者が共用し、通信回線としてインターネットを利用するSaaS型パブリッククラウドサービスがある。SaaS型パブリッククラウドサービスは、インターネットに接続できれば、どこからでもアクセス可能な点で、利用者は利用場所の制約から解放される点が大きなメリットである。

【例文】

（１）ID及びパスワード等の秘匿

①　教職員等は、ID及びパスワードについて秘匿管理を行わなければならない。

②　教職員等は、多要素認証に必要な要素（知識、生体、物理）についても適切に管理を行わなければならない。もし該当要素が流出等したと考えられる場合には、速やかに教育情報セキュリティ管理者に報告しなければならない。

（2） モバイル端末持ち歩きリスク

教職員等は、クラウドサービスにアクセスする際に活用するモバイル端末について、紛失・盗難を避けるよう、適切に管理しなければならない。

（3） 重要性分類に基づく情報管理

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

（4） 学校外からのパブリッククラウド利用

① 教職員等は、学校外からクラウドサービスを利用する際、情報資産の取扱いをクラウドサービス上のみで行うことを原則とする。

② クラウドサービスから端末にファイルをダウンロードする際は、情報資産の外部持ち出しに基づく安全管理措置として、端末の安全性を事前に確認するとともに、作業が終わり次第当該端末から情報資産をすみやかに消去しなければならない。

（5） SaaS型パブリッククラウドサービスの学習用途、校務用途混在リスクへの対応

① 教職員等は、強固なアクセス制御による対策を講じたシステム構成にてクラウドサービスを利用している場合には、クラウドサービスを学習用途と校務用途で適切に使い分けるよう、共有先やダウンロード方法等の運用ルールについてあらかじめ確認し、適切に運用しなければならない。

② 教職員等は、ネットワーク分離による対策を講じたシステム構成の場合にてクラウドサービスを利用している場合には、クラウドサービスを学習用途と校務用途で使い分けるよう、適切に運用しなければならない。

（解説）

（１）ID及びパスワード等の秘匿

SaaS型パブリッククラウドサービスはインターネット上に存在するため、インターネット上のサイバー脅威から常に身を守る必要がある。また同じ機能を複数の利用者に提供しており、利用者を識別にするためにID及びパスワードが用いられる。SaaS型パブリッククラウドサービス利用でのリスクについて、このID及びパスワードが利用者以外の他者に漏えいして、他者がなりすまし行為（不正アクセス）を行うことが最大のリスクと言える。そのため、なによりもID及びパスワードの秘匿管理が重要となる。

また、特に強固なアクセス制御による対策を講じたシステム構成にてSaaS型パブリッククラウドサービスを利用している場合などにおいては、多要素認証を採用していることが考えられ、その場合、多要素認証に必要な要素（知識、生体、物理）について、適切に管理を行わなければならず、これらが流出したと考えられる場合には速やかに教育情報セキュリティ管理者に報告しなければならない。

そのため、認証キー（FIDO）利用時の紛失・破損の手順や、デバイスの管理や紛失・破損及び事件事故に巻き込まれた時の手順、パスワード管理の運用ルール等について、あらかじめ確認しておくことが望ましい。

（２）モバイル端末持ち歩きリスク

学校内外からインターネット経由でSaaS型パブリッククラウドサービスにアクセスができるため、モバイル端末持ち歩きによる家庭学習が可能となった。一方で、端末の紛失・盗難・破損リスクも増加している。モバイル端末が紛失・盗難に合うことは２つの側面で問題がある。ひとつは、端末に情報が保管されている場合は端末紛失自体が情報の漏えいにつながること、もうひとつは端末が使えなくなることで業務に支障が出る点である。

そのため、教職員等はモバイル端末の紛失・盗難を避けるよう、留意する必要がある。それに加えて、モバイル端末の紛失・盗難が利用者の管理のみで完全に守り切れるとは言い切れない以上、モバイル端末を一元的に監視・管理するMDM（Mobile Device Management）の導入を検討されたい。また、端末に情報を保管することを控えることが安全性を高めることから、情報の保管先をクラウドサービス側にデフォルト設定することを推奨する。

（３）重要性分類に基づく情報管理

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

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

（４）学校外からのパブリッククラウド利用

SaaS型パブリッククラウドサービスは、アクセス制御による対策、通信の暗号化を講じる条件において、インターネットを通信経路として採用した利用ができる。学校が管理するパブリッククラウドサービスにおいては、パブリッククラウド内にデータを保管しても情報資産の外部持ち出しには該当しない。

SaaS型パブリッククラウドから教育委員会が貸与するなど管理が及ばない外部の端末にファイルをダウンロードして情報処理をする場合には、情報資産の外部持ち出しに該当するため、安全管理措置が必要になる。第一に、外部の端末の安全性確認、第二に情報処理した学校の情報資産を端末内に残置せず消去することが求められる。

（５）SaaS型パブリッククラウドサービスの学習用途、校務用途混在リスクへの対応

校務系情報は児童生徒のアクセスを想定していないため、同一のクラウドサービス上で学習系情報と校務系情報のいずれもを取り扱う場合は、教職員等による誤保管や誤表示のリスクがあることに留意されたい。このような場合は、校務系用途と学習系用途で教職員用アカウントを分ける等の措置を推奨する。詳しくは「第２編３．情報資産の分類と管理方法」にて、重要性分類及びアクセス主体に応じた各情報資産の例示や取扱いの考え方を示しているため、参照すること。

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、「第２編９．１．SaaS型パブリッククラウドサービスの利用における情報セキュリティ対策」及び「第２編９．２．SaaS型パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項」で想定する個別契約締結型サービスとは別種であり、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

① 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 教育情報システム管理者は、約款による外部サービスの利用に当たっては、約款において以下の点が規定されていることを確認しなければならない。

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

(イ)サービス事業者が業務上知り得た情報の守秘義務が守られること

（２）約款による外部サービスの利用における対策の実施

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

（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、有償、無償に関わらず、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じる必要がある。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

（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。

（注３）クラウドサービスの中には職員等が直接登録し利用可能なものがあり、その利用状況を自組織として一元的に把握するのが困難であることが多い。所属する組織の承認を得ずに職員等がクラウドサービスを利用することは“シャドーIT”と呼ばれるが、シャドーITは監視が不十分になりやすく、セキュリティリスクが高まる等の問題がある。そのため、シャドーITの対策としては、職員等がクラウドサービスを利用する場合に必ず申請を行い自組織が承認を行う運用が考えられる。本ガイドラインにおいては、本規定に加えて、教職員等のシャドーIT対策として「第２編５.２. 教職員等の遵守事項」の（11）②に無許可クラウドサービス・個人アカウントの利用禁止、（14）に無許可ソフトウェアの利用禁止、「第２編５.１. 教育情報セキュリティ管理者の措置事項」の（５）に新規ソフトウェア及びコンテンツの導入・利用判断について規定されているため、参照すること。

（２）約款による外部サービスの利用における対策の実施

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４）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。

## 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９．１．SaaS型パブリッククラウドサービスの利用における情報セキュリティ対策及び９．２．SaaS型パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項で想定する個別契約締結型サービスの検討を行うこと。

【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。

① 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。

② パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ICカード等）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）

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、利用に当たっては、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。

## 10. 評価・見直し

### 10.１．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）一部又は全て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６年10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。

10.２．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。

10．３．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】

（１）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

## 第３編 付録

### （1）本ガイドラインにおける用語定義

| 用語 | 定義 |
|---|---|
| 校務系情報 | 学校が保有する情報資産のうち、それらの情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報 |
| 校務外部接続系情報 | ネットワーク分離による対策を講じたシステム構成において、インターネット接続を前提として、校務で利用される情報 |
| 学習系情報 | 学校が保有する情報資産のうち、それらの情報を学校における教育活動において活用することを想定しており、かつ、当該情報に教員及び児童生徒がアクセスすることが想定されている情報 |
| 校務用端末 | 校務系情報にアクセス可能な端末 |
| 校務外部接続用端末 | ネットワーク分離による対策を講じたシステム構成において、校務外部接続系情報にアクセス可能な端末 |
| 学習者用端末 | 学習系情報にアクセス可能な端末で、児童生徒が利用する端末 |
| 指導者用端末 | 学習系情報にアクセス可能な端末で、教員のみが利用可能な端末 |
| 校務系システム | 校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム<br>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 | ネットワーク分離による対策を講じたシステム構成において、校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ（CMS）及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム |
| 学習系システム | 学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム<br>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 | ネットワーク分離による対策を講じたシステム構成において、校務外部接続系情報を取り扱うサーバ |
| 学習系サーバ | 学習系情報を取り扱うサーバ |
| 強固なアクセス制御 | インターネットを通信経路とする前提で、内部・外部からの不正アクセスを防御するために、多要素認証による利用者認証、端末認証、端末・サーバ・通信の監視・制御等を組み合わせたセキュリティ対策を指す。利用者毎に情報へのアクセス権限を適切に設定するとともに、①アクセスの真正性、②端末・サーバ・通信の安全性の観点から、端末とクラウドサービスを提供するサーバ間の通信を暗号化し、認証により利用者のアクセスの適正さを常に確認しなければならない。 |
| 通信の暗号化 | 通信又は通信経路を暗号化し保護すること |

（2）一般用語の解説

| 用語 | 定義・解説 |
| --- | --- |
| CSIRT（Computer Security Incident Response Team）* | 機関等において発生した情報セキュリティインシデントに対処するため、当該機関等に設置された体制をいう。 |
| EDR（Endpoint Detection and Response）** | パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術をいう。 |
| IaaS（Infrastructure as a Service）* | 利用者に、CPU機能、ストレージ、ネットワークその他の基礎的な情報システムの構築に係るリソースが提供されるもの。利用者は、そのリソース上にOSや任意機能（情報セキュリティ機能を含む。）を構築することが可能である。 |
| ISMAP（Information system Security Management and Assessment Program）*** | 政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度。 |
| PaaS（Platform as a Service）* | IaaSのサービスに加えて、OS、基本的機能、開発環境や運用管理環境等もサービスとして提供されるもの。利用者は、基本機能等を組み合わせることにより情報システムを構築する。 |
| SaaS（Software as a Service）* | 利用者に、特定の業務系のアプリケーション、コミュニケーション等の機能、運用管理系の機能、開発系の機能、セキュリティ系の機能等がサービスとして提供されるもの。 |
| VPN（Virtual Private Network）* | 暗号技術等を利用し、インターネット等の公衆回線を仮想的な専用回線として利用するための技術をいう。 |

| | |
|---|---|
| Web会議サービス* | 専用のアプリケーションやウェブブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行えるクラウドサービスをいう。なお、特定用途機器同士で通信を行うもの（テレビ会議システム等）は含まれない。 |
| アクセス制御* | 情報又は情報システムへのアクセスを許可する主体を制限することをいう。 |
| アプリケーション* | OS上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。 |
| アプリケーション・コンテンツ* | 機関等が開発し提供するアプリケーションプログラム、ウェブコンテンツ等の総称をいう。 |
| アルゴリズム* | ある特定の目的を達成するための演算手順をいう。 |
| クラウドサービス* | 事業者によって定義されたインタフェースを用いた、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であって、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いう。クラウドサービスの例としては、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等がある。なお、統一基準におけるクラウドサービスは、機関等外の一般の者が一般向けに情報システムの一部又は全部の機能を提供するクラウドサービスであって、当該サービスにおいて機関等の情報が取り扱われる場合に限るものとする。 |
| クラウドサービス提供者* | クラウドサービスを提供する事業者（クラウドサービスプロバイダ）をいう。 |

| | |
|---|---|
| サーバ装置* | 情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、機関等が調達又は開発するもの（政府共通利用型システムが提供するものを含む。）をいう。また、物理的なハードウェアを有するサーバ装置を「物理的なサーバ装置」という。 |
| サービス不能攻撃* | 悪意ある第三者等が、ソフトウェアの脆弱性を悪用しサーバ装置又は通信回線装置のソフトウェアを動作不能にさせることや、サーバ装置、通信回線装置又は通信回線の容量を上回る大量のアクセスを行い通常の利用者のサービス利用を妨害する攻撃をいう。 |
| セキュリティパッチ* | 発見された情報セキュリティ上の問題を解決するために提供される修正用のファイルをいう。提供元によって、更新プログラム、パッチ、ホットフィクス、サービスパック等名称が異なる。 |
| ソーシャルメディア* | インターネット上において、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、利用者が情報を発信し、形成していくものをいう。 |
| ソフトウェア* | サーバ装置、端末、通信回線装置等を動作させる手順及び命令を、当該サーバ装置等が理解できる形式で記述したものをいう。OSやOS上で動作するアプリケーションを含む広義の意味である。 |
| テレワーク* | 情報通信技術（ICT＝Information and Communication Technology）を活用した、場所や時間を有効に活用できる柔軟な働き方のことをいう。テレワークの形態は、業務を行う場所に応じて、自宅で業務を行う在宅勤務、主たる勤務官署以外に設けられた執務環境で業務を行うサテライトオフィス勤務、モバイル端末等を活用して移動中や出先で業務を行うモバイル勤務に分類される。 |

| | |
|---|---|
| ドメイン名* | 国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。例えば、www.nisc.go.jpというウェブサイトの場合は、nisc.go.jpの部分がこれに該当する。 |
| パブリッククラウド** | クラウドサービスの提供方式のひとつ。CPU、ストレージ、メモリ等のコンピュータリソースの利用率を最適化するために、一般ユーザーや複数の利用者でリソースを共用して実装されるクラウドコンピューティング方式。 |
| プライベートクラウド** | クラウドサービスの提供方式のひとつ。クラウド事業者が１つの組織に対してクラウドサービスを提供するものであり、当該組織外のユーザーは利用することができない、その組織専用に実装されるクラウドコンピューティング方式。 |
| モバイル端末* | 端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。 |
| リスク* | 目的に対する不確かさの影響をいう。ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。 |
| 暗号化* | 第三者が復元することができないよう、定められた演算を施しデータを変換することをいう。 |
| 暗号化消去**** | 情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。 |
| 可用性* | 情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性をいう。 |
| 完全性* | 情報が破壊、改ざん又は消去されていない特性をいう。 |
| 機密性* | 情報に関して、アクセスを認められた者だけがこれにアクセスできる特性をいう。 |

| | |
|---|---|
| 記録媒体* | 情報が記録され、又は記載される有体物をいう。記録媒体において、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物を「書面」といい、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるものを「電磁的記録」といい、電磁的記録に係る記録媒体を「電磁的記録媒体」という。また、電磁的記録媒体には、サーバ装置、端末、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等の外部電磁的記録媒体がある。 |
| 識別* | 情報システムにアクセスする主体を、当該情報システムにおいて特定することをいう。 |
| 実施手順* | 対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順や手続をいう。 |
| 情報セキュリティインシデント* | 望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。 |
| 対策基準* | 機関等における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。 |
| 端末* | 情報システムの構成要素である機器のうち、職員等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、機関等が調達又は開発するもの（政府共通利用型システムが提供するものを含む。）をいう。端末には、モバイル端末も含まれる。特に断りを入れた例としては、機関等が調達又は開発するもの以外を指す「機関等支給以外の端末」がある。また、機関等が調達又は開発した端末と機関等支給以外の端末の双方を合わせて「端末（支給外端末を含む）」という。さらに、物理的なハードウェアを有する端末を「物理的な端末」という。 |

| | |
|---|---|
| 通信回線* | 複数の情報システム又は機器等（機関等が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、機関等の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、機関等が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。 |
| 通信回線装置* | 通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。また、物理的なハードウェアを有する通信回線装置を「物理的な通信回線装置」という。 |
| 電子メールサーバ* | 電子メールの送受信、振り分け、配送等を行うアプリケーション及び当該アプリケーションを動作させるサーバ装置をいう。 |
| 電子署名* | 情報の正当性を保証するための電子的な署名情報をいう。 |
| 踏み台* | 悪意ある第三者等によって不正アクセスや迷惑メール配信の中継地点に利用されている情報システムのことをいう。 |
| 特定用途機器* | 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、入退管理システム、施設管理システム、環境モニタリング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、通信回線に接続する機能を備えている又は内蔵電磁的記録媒体を備えているものをいう。 |
| 不正プログラム* | コンピュータウイルス、ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム）、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。 |
| 複合機* | 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いう。 |

| | |
|---|---|
| 無線LAN* | IEEE80211a、80211b、80211g、80211n、80211ac、80211ad等の規格により、無線通信で情報を送受信する通信回線をいう。 |

*…内閣サイバーセキュリティセンター（NISC）「政府機関等のサイバーセキュリティ対策のための統一基準群」（令和５年改定）より引用

**…内閣サイバーセキュリティセンター（NISC）「クラウドを利用したシステム運用に関するガイダンス」（詳細版）より引用

***…「ISMAP-政府情報システムのためのセキュリティ評価制度-」より引用

****…総務省「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６年10月版）」より引用

### （3）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、「第２編 教育情報セキュリティ対策基準（例文・解説）」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

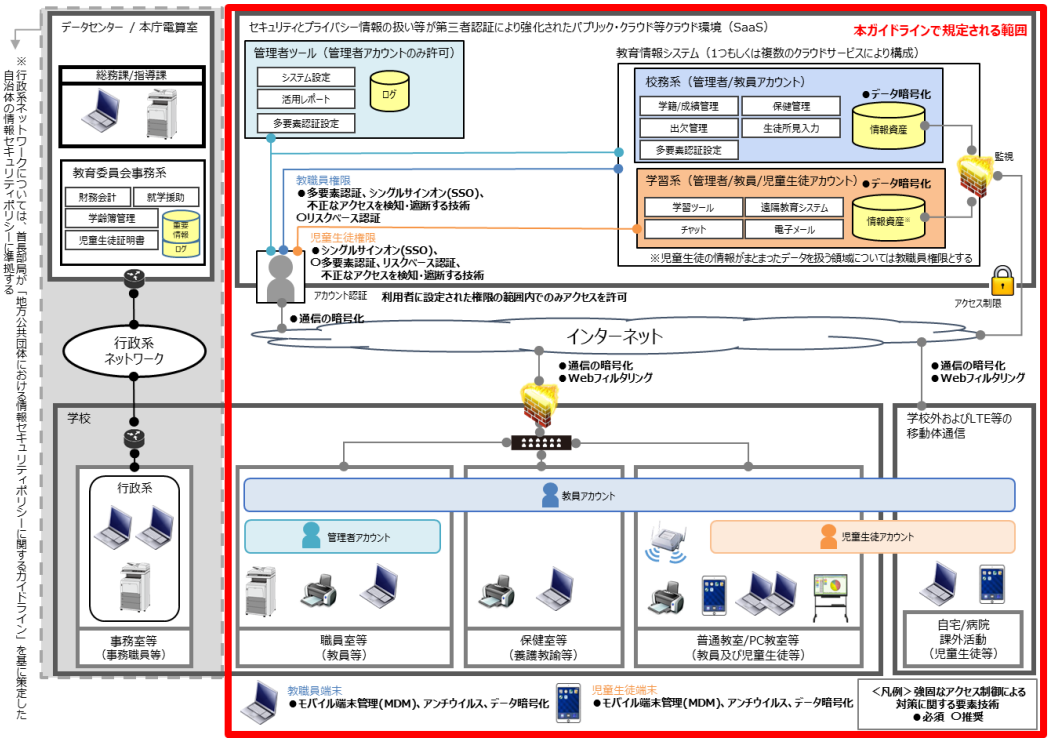
※　暗号化については、コストや実現したい環境を踏まえつつ、ストレージやファイル等に対し、適切なレベルの暗号化を行うことで、一層のセキュリティの向上が見込まれる

（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。

＜強固なアクセス制御による対策を講じたシステム構成例＞

次世代校務DXの実現を前提とした、推奨されるシステム構成例である。なお「強固なアクセス制御」とは、インターネットを通信経路とする前提で、内部・外部からの不正アクセスを防御するために、多要素認証による利用者認証、端末認証、端末・サーバ・通信の監視・制御等を組み合わせたセキュリティ対策を指す。利用者毎に情報へのアクセス権限を適切に設定するとともに、①アクセスの真正性、②端末・サーバ・通信の安全性を確保する観点から、端末とクラウドサービスを提供するサーバ間の通信を暗号化し、認証により利用者のアクセスの適正さを常に確認しなければならない。




**図表 13　強固なアクセス制御による対策を講じたシステム構成例**

※　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、「第２編９．SaaS型パブリック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感染対策、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。

※　強固なアクセス制御による対策に関する要素技術については「●必須：どのような自治体においても導入が必須の要素技術」「○推奨：諸要素を比較考慮する必要はあるが、導入が望ましい要素技術」として示しているが、下記２点について留意すること。

①　要素技術についてはネットワークへの不正アクセスや情報資産の漏洩等の想定される脅威を考慮したうえで選定する必要がある。

②　これらの要素技術は、それぞれ個別の製品・サービスを調達・導入するだけでなく、GIGAスクール構想の下で整備された端末の標準的な機能・サービスで実現可能なものは積極的に採用すべきである。

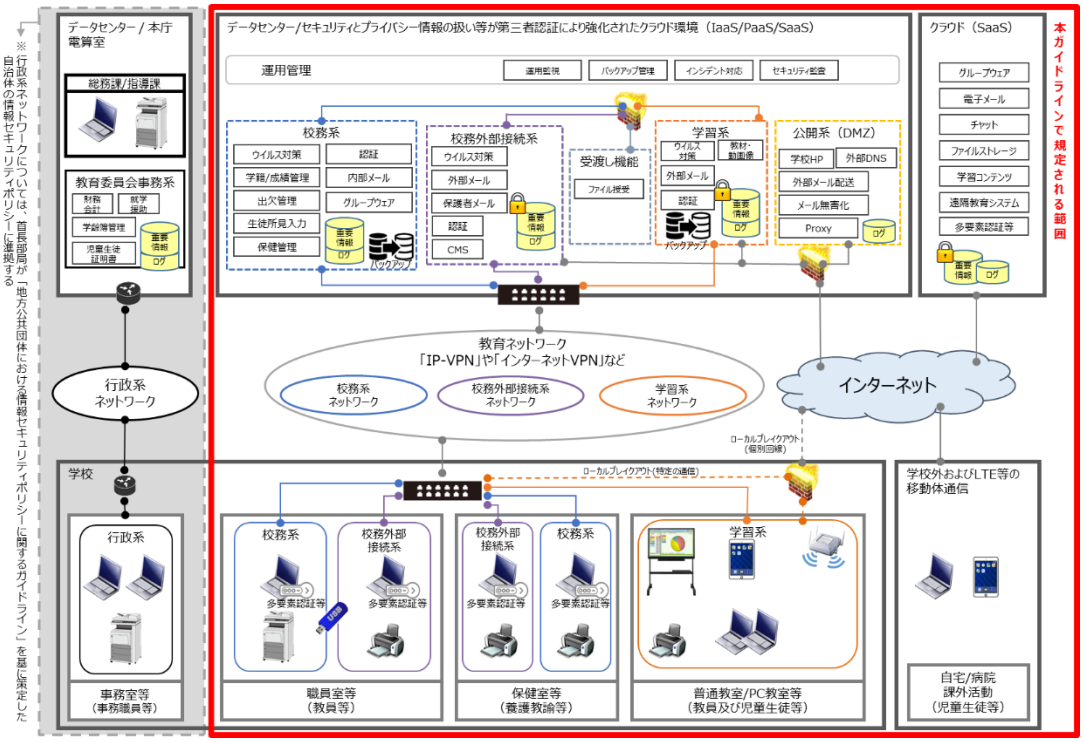
強固なアクセス制御による対策に関する要素技術は以下のとおりである。多要素認証は、知識認証（ID及びパスワード等）、生体認証（指紋、静脈、顔、声紋等）、物理認証（ICカード、USBトークン、トークン型ワンタイムパスワード等）のうち、異なる認証方式２種類を組み合わせる利用者認証の方法であるが、学校現場の実態や特徴を踏まえ、端末の電子証明書等を用いた端末認証と、知識認証・生体認証のいずれかを組み合わせて利用者認証を行うことも考えられる。

それぞれの要素技術については以下に示すとおり、第２編の各規定の例文・解説に記載している。なお、これらの要素技術は、今後の技術動向等により変化しうるものであることに留意すること。

| ①アクセスの真正性に関する要素技術 | | | |
|---|---|---|---|
| ①-１ | 多要素認証<br>※学校現場の実態や特徴を踏まえ、端末の電子証明書等を用いた端末認証と、知識認証・生体認証のいずれかを組み合わせて利用者認証を行うことも考えられる | 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 | 例文・解説（１）（４） |
| | | ６．２．アクセス制御 | 例文・解説（１）（３） |
| ①-２ | リスクベース認証 | ６．２．アクセス制御 | 解説（１） |
| ①-３ | シングルサインオン（SSO） | ６．２．アクセス制御 | 例文・解説（１） |
| | | ７．５．児童生徒におけるID及びパスワード等の管理 | 例文・解説（３） |
| ②端末・サーバ・通信の安全性に関する要素技術 | | | |
| ②-１ | 通信の暗号化 | ６．１．コンピュータ及びネットワークの設定管理 | 例文・解説（10）①② |
| | | ６．２．アクセス制御 | 例文・解説（２）③ |
| ②-２ | Webフィルタリング | 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 | 例文・解説（９） |
| ②-３ | モバイル端末管理（MDM） | ６．２．アクセス制御 | 例文・解説（２）④ |
| ②-４ | アンチウイルス | 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 | 例文・解説（８） |
| | | ５．２．教職員等の遵守事項 | 例文（18）② |
| ②-５ | データ暗号化 | 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 | 例文・解説（６） |
| ②-６ | 不正なアクセスを検知・遮断する技術 | 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 | 解説（８） |
| | | ７．１．情報システムの監視 | 例文・解説（注１） |

**図表14　強固なアクセス制御による対策に関する要素技術及びその主な規定箇所**

※　＜ネットワーク分離による対策を講じたシステム構成例＞




**図表 15　ネットワーク分離による対策を講じたシステム構成例**

※　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。

※　図表15　ネットワーク分離による対策を講じたシステム構成例におけるクラウド（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。

## （4）権限・責任等一覧表

※本一覧表は「**第２編 教育情報セキュリティ対策基準（例文・解説）**」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 | 教員委員会事務局職員 | 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 | 一元的な窓口 | 外部委託関係規定 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | | | | | | | | | | | | |
| 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 | | | | | | | | | | | ○ | |
| | （10） | ① | | 教職員等の範囲の定義 | | | | | | | | | | | | |
| | | ② | | 教職員等の遵守義務 | | | | | | | | | | | | |
| | （11） | ① | | 教育委員会事務局職員の範囲の定義 | | | | | | | | | | | | |
| | | ② | | 教育委員会事務局職員の遵守義務 | | | | | | | | | | | | |
| 3. 情報資産の分類と管理方法 | 3．1 情報資産の分類 | （1） | | 情報資産の分類 | | | | | | | | | | | | |
| | 3．2 情報資産の管理 | （1） | ① | 学校教育情報セキュリティ対策基準の策定 | ○ | ○ | | | | | | | | | | |
| | | | ② | 情報セキュリティ運用管理に関する実施手順ひな形の作成 | | ○ | | | | | | | | | | |
| | | | ③ | 標準情報資産台帳の作成 | | ○ | | | | | | | | | | |
| | | | ④ | 実施手順ひな形に基づいた自校向け実施手順を作成 | | | | ○ | | | | | | | | |
| | | | ⑤ | 標準情報資産台帳に基づいた自校向け情報資産台帳整備 | | | | ○ | | | | | | | | |
| | | | ⑥ | 情報資産の管理責任 | | | | ○ | | | | | | | | |
| | | | ⑦ | 教職員等の台帳及び実施手順に基づいた運用管理 | | | | ○ | | | | | | | | |
| | | | ⑧ | 台帳及び実施手順に基いた適切な情報資産の取扱い | | | | | | | ○ | | | | | |
| | | （2） | | 情報資産の分類の表示 | | | | | | | ○ | | | | | |
| | | （3） | ① | 業務上必要のない情報の作成の禁止 | | | | | | | ○ | | | | | |
| | | | ② | 情報作成時の情報の分類と取扱制限の設定 | | | | | | | ○ | | | | | |
| | | | ③ | 作成途上の情報の取扱 | | | | | | | ○ | | | | | |
| | | （4） | ① | 学校内の者が作成した情報資産の取扱 | | | | | | | ○ | | | | | |
| | | | ② | 学校外の者が作成した情報資産の分類と取扱 | | | | | | | ○ | | | | | |
| | | | ③ | 分類が不明な情報資産を入手した際の対応 | | | | △ | | | ○ | | | | | |
| | | （5） | ① | 情報資産の業務外目的の利用の禁止 | | | | | | | ○ | | | | | |
| | | | ② | 情報資産の分類に応じた適切な取扱 | | | | | | | ○ | | | | | |
| | | | ③ | 情報資産の分類が異なる電磁的記録媒体の取扱 | | | | | | | ○ | | | | | |
| | | | ④ | 情報資産の複製・配布 | | | | | | | ○ | | | | | |
| | | （6） | ① （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】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 | | | | ○ | ○ | | | | | | |
| | | | ② （ア） | 【教職員等】情報資産の分類に応じた適切な保管 | | | | | | | ○ | | | | | |
| | | | （イ） | 情報資産の分類に応じた適切な保管指導 | | | | | | | ○ | | | | | |
| | | （7） | ① （ア） | 重要性分類Ⅱ以上の情報資産外部持ち出し制限 | | | | 許 | | | ○ | | | | | |
| | | | （イ） | 重要性分類Ⅲの情報資産外部持ち出しの包括的許可 | | | | 許 | | | ○ | | | | | |
| | | | ② （ア） | 電子メール、外部ストレージサービスでの情報送信時の対策 | | | | | | | ○ | | | | | |
| | | | （イ） | 電子メール、外部ストレージサービスの適切な利用 | | | | | | | ○ | | | | | |
| | | | ③ （ア） | 外部電磁的記録媒体を用いた情報資産の外部持ち出し時の取扱い | | | | | | | ○ | | | | | |
| | | | （イ） | 外部電磁的記録媒体を用いた情報資産の外部持ち出し時の対策 | | | | | | | ○ | | | | | |
| | | | ④ | FAXによる情報の送信時の対策 | | | | | | | ○ | | | | | |
| | | | ⑤ （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 | | | ○ | | | | | |
| | | | ⑥ （ア） | 情報資産の外部への公開時の対策 | | | | | | | ○ | | | | | |
| | | | （イ） | 住民に公開する情報資産の取扱 | | | | ○ | ○ | | | | | | | |
| | | （8） | ① | 情報資産(紙媒体)廃棄時の対策 | | | | | | | ○ | ○ | | | | |
| | | | ② | 情報資産(電磁的記録媒体)廃棄時の対策 | | | | | | | ○ | ○ | | | | |
| | | | ③ | 情報資産廃棄の許可と処理の記録 | | | | 許 | 許 | | ○ | ○ | | | | |
| | | | ④ | 情報資産廃棄委託時の立会い | | | | | | | ○ | ○ | | | | |

| 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 | 教育委員会事務局職員 | 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 | 統一的窓口 | 外部委託関係規定 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4.<br>物理的セキュリティ対策 | 4．1<br>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） | 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 | | | | | ○ | | | | | | | |
| | 4．2<br>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 | | | | | ○ | | △ | | | | | |
| | 4．3<br>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） | | 重要性分類Ⅲ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） | | 重要性分類Ⅱ以上の情報を扱う通信回線の可用性の確保 | | ○ | | | ○ | | | | | | | |
| | | （6） | | 授業に支障の出ない構成の選択（帯域や同時接続数など） | | ○ | | | | | | | | | | |
| | 4．4<br>教職員等の利用する端末や電磁的記録媒体等の管理 | （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） | | 重要性分類Ⅱ以上の情報へアクセスする時の多要素認証設定 | | | | | ○ | | | | | | | |
| | | （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） | | 端末に対する情報流出への対策 | | | | | ○ | | | | | | | |
| | | （7） | | モバイル端末に対する遠隔消去機能の利用 | | | | | ○ | | | | | | | |
| | | （8） | | パソコン、モバイル端末への適切なウイルス対策 | | | | | ○ | | | | | | | |
| | | （9） | | パソコン、モバイル端末に対するWebフィルタリング措置 | | | | | ○ | | | | | | | |
| | 4．5<br>学習者用端末のセキュリティ対策 | （1） | | 不適切なウェブページの閲覧防止 | | | | | ○ | | | | | | | |
| | | （2） | | マルウェア感染対策 | | | | | ○ | | | | | | | |
| | | （3） | | 端末を不正利用させないための防止策 | | | | | ○ | | | | | | | |
| | | （4） | | セキュリティ設定の一元管理 | | | | | ○ | | | | | | | |
| | | （5） | | 端末の盗難・紛失時の情報漏洩対策 | | | | | ○ | | | | | | | |
| | 4．6<br>パソコン教室等における学習者用端末や電磁的記録媒体の管理 | （1） | | パソコン教室等で利用する学習者用端末の盗難防止措置 | | | | | ○ | | | | | | | |
| | | （2） | | パソコン教室等で利用する学習者用端末及び電磁的記録媒体に記録された情報の扱い | | | | | ○ | | | | | | | |
| | | （3） | | パソコン教室等で利用する学習者用端末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 | 教育委員会事務局職員 | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5. 人的セキュリティ対策 | 5．1 教育情報セキュリティ管理者の措置事項 | (1) | ① | 報資産の持ち出し及び持ち込みの記録管理 | | | | ○ | | | | | | | | |
| | | | ② (ア) | 情報資産の廃棄管理 | | | | ○ | | | | | | | | |
| | | | (イ) | 廃棄した情報資産の記録管理 | | | | ○ | | | | | | | | |
| | | (2) | ① | 教職員等の情報セキュリティ意識醸成 | | | | ○ | | | | | | | | |
| | | | ② | 教職員等に対する情報セキュリティ意識の醸成と風通しのよい関係性維持 | | | | ○ | | | | | | | | |
| | | | ③ | 情報セキュリティポリシー等の閲覧容易性確保 | | | | ○ | | | | | | | | |
| | | (3) | | 端末等の持ち出し及び持ち込みの記録 | | | | ○ | | | | | | | | |
| | | (4) | ① | 教職員等への情報セキュリティポリシー等の遵守指導 | | | | ○ | | | | | | | | |
| | | | ② | 情報セキュリティポリシーの遵守の同意 | | | | ○ | | | | | | | | |
| | | (5) | | 新規ソフトウェア及びコンテンツの導入・利用判断 | | | | ○ | | | | | | | | |
| | | (6) | ① | インターネット接続及び電子メール利用の制限 | | | | ○ | | | | | | | | |
| | | | ② | 教職員等の業務内容に応じた機能制限 | | | | ○ | | | | | | | | |
| | | (7) | ① | 校内及び執務室で来校者管理 | | | | ○ | | | | | | | | |
| | | | ② | 来校者の記録 | | | | ○ | | | | | | | | |
| | | | ③ | 開放施設がいへの入場制限 | | | | ○ | | | | | | | | |
| | | (8) | ① | 自己点検の実施 | | | | ○ | | | | | | | | |
| | | | ② | 教育情報セキュリティ委員会への自己点検の結果報告 | | | | ○ | | | | | | | | |
| | 5．2 教職員等の遵守事項 | (1) | | 情報セキュリティポリシー等の遵守 | | | | △ | | | ○ | | | | | |
| | | (2) | ① | 執務室の施錠管理 | | | | | | | ○ | | | | | |
| | | | ② | 来校者等への対応 | | | | 許 | | | ○ | | | | | |
| | | | ③ | 机上の端末等の管理 | | | | 許 | | | ○ | | | | | |
| | | (3) | ① | 支給端末の業務利用禁止 | | | | 許 | | | ○ | | | | | |
| | | | ② | 支給端末への無断ソフトウェアインストール禁止 | | | | | | | ○ | | | | | |
| | | | ③ | 支給端末のセキュリティ機能及びメモリ増設の設定変更禁止 | | | | | | | ○ | | | | | |
| | | | ④ | モバイル端末の盗難防止対策 | | | | | | | ○ | | | | | |
| | | | ⑤ | 離席時の業務端末管理 | | | | | | | ○ | | | | | |
| | | | ⑥ | 業務終了後等の業務端末管理 | | | | | | | ○ | | | | | |
| | | (4) | ① | 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利用禁止 | | | | 許 | | | ○ | | | | | |
| | | | ② | 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) | ① | モバイル端末や電磁的記録媒体等の持ち出しの許可 | | | | 許 | | | ○ | | | | | |
| | | | ② | 外部での情報処理業務の許可 | | | | 許 | | | ○ | | | | | |
| | | (6) | 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 | 利用者登録抹消の申請 | | △ | | | △ | | ○ | | | | | |
| | | (7) | 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 | パスワードのシステム間の共有禁止 | | | | | | | ○ | | | | | |
| | | | ⑥ | 仮パスワードの変更 | | | | | | | ○ | | | | | |
| | | | ⑦ | パスワードの記憶機能の利用禁止 | | | | | | | ○ | | | | | |
| | | | ⑧ | 職員等間でのパスワード共有禁止 | | | | | | | ○ | | | | | |
| | | | ⑨ | パスワードの定期的な更新 | | | | | | | ○ | | | | | |
| | | (8) | ① | 認証に用いるICカード等の職員等間共有の禁止 | | | | | | | ○ | | | | | |
| | | | ② | ICカード等のカードリーダへの常時挿入禁止 | | | | | | | ○ | | | | | |
| | | | ③ | ICカード等紛失時の通報 | | △ | | | △ | | ○ | | | | | |
| | | (9) | ① | 支給された外部電磁的記録媒体以外の利用禁止 | | | | | | | ○ | | | | | |
| | | | ② | 外部電磁的記録媒体の施錠管理 | | | | | | | ○ | | | | | |
| | | (10) | 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 | | | | | | | ○ | | | | | |
| | | | ⑥ | 情報ファイルを添付する場合のパスワード設定 | | | | | | | ○ | | | | | |
| | | | ⑦ | 送信先のメールアドレス、添付ファイルの内容確認 | | | | | | | ○ | | | | | |
| | | | ⑧ | 不審メールを受信したときの対応 | | | | | | | ○ | | | | | |
| | | (11) | ① | パブリッククラウドでの重要性分類Ⅱ以上の情報資産の扱い | | | | | | | ○ | | | | | |
| | | | ② | 私的に契約したクラウドサービスの業務利用禁止 | | | | | | | ○ | | | | | |
| | | | ③ | ソーシャルメディアサービスでの情報公開の使い | | | | | | | ○ | | | | | |
| | | (12) | 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 | | | | | | | ○ | | | | | |
| | | | (ウ) | 端末の電源保持 | | | | | | | ○ | | | | | |
| | | (13) | 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 | ○ | | | | | | | | | | | |
| | | (14) | 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 | | | | | | | ○ | | | | | |
| | | (15) | 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 | | ○ | | | | | |
| | | (16) | | 無許可でのネットワーク接続の禁止 | | 許 | | | | | ○ | | | | | |
| | | (17) | | 業務目的外のウェブ閲覧の禁止 | | | | | | | ○ | | | | | |
| | | (18) | 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 | 外部から持ち込んだ端末等のウイルスの確認等 | | | | | | | ○ | | | | | |
| | | (19) | ① | 学習者用端末及び学習系クラウドサービスの利用限定 | | | | | | | ○ | | | | | |
| | | | ② | 利用者認証情報の秘匿管理 | | | | | | | ○ | | | | | |
| | | | ③ | ウイルス対策ソフトウェアの管理 | | | | | | | ○ | | | | | |
| | | | ④ | 端末のソフトウェアに関するセキュリティ機能の設定変更禁止 | | | | | | | ○ | | | | | |
| | | | ⑤ | 学習系情報の保管 | | | | | | | ○ | | | | | |
| | | | ⑥ | 無断外部ソフトウェアをインストール禁止 | | | | | | | ○ | | | | | |
| | | | ⑦ | コミュニケーションツールの利用制限 | | | | | | | ○ | | | | | |
| | | | ⑧ | ウイルス感染が疑われる場合の報告 | | | | | | | ○ | | | | | |
| | | | ⑨ | 学習者用端末の安全な取扱い | | | | | | | ○ | | | | | |
| | | | ⑩ | 私物端末など許可されていない端末の利用禁止 | | | | | | | ○ | | | | | |
| | | | ⑪ | 重要性分類Ⅱ以上の情報資産（児童生徒本人の情報に限る）の管理 | | | | | | | ○ | | | | | |
| | | (20) | | 退職時等の遵守事項 | | | | | | | ○ | | | | | |
| | 5．3 教育委員会事務局職員の遵守事項 | (1) | | 教育情報セキュリティポリシー等の遵守 | | | | | | | | ○ | | | | |
| | | (2) | | 業務以外の目的での使用の禁止 | | | | | | | | ○ | | | | |
| | | (3) | | 校務用端末による外部における情報処理作業の禁止 | | | | | | | | ○ | | | | |
| | | (4) | | 重要性分類Ⅱ以上の情報資産へのアクセス制限 | | | | | | | | ○ | | | | |
| | | (5) | | 知りえた情報の秘匿 | | | | | | | | ○ | | | | |
| | | (6) | | 業務を離れる場合の遵守事項 | | | | | | | | ○ | | | | |
| | 5．4 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 | | | | | | | | | | ○ | | |
| | 5．5 情報セキュリティインシデントの連絡体制整備 | (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 | 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 | | ○ | | | | | | | | | | |
| | | (3) | 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 | ○ | | | | | | | | | | | |
| | | (4) | 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 | ○ | | | | | | | | | | | |
| | | (5) | | 支給端末の運用・連絡体制の整備 | ○ | | | | | | | | | | | |

| 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 | 教育委員会事務局職員 | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 6.<br>技術的セキュリティ | 6．1<br>コンピュータ及びネットワークの設定管理 | （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） | ① | | ログの取得等 | | ○ | | | ○ | | | | | | | |
| | | | ② | | ログの管理 | | ○ | | | ○ | | | | | | | |
| | | | ③ | | ログの点検・分析 | | ○ | | | ○ | | | | | | | |
| | | （4） | 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 | | ○ | | | | | | | | | | |
| | | （5） | | | 外部の者が利用できるシステムの分離等 | | | | | ○ | | | | | | | |
| | | （6） | 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 | | △ | | | ○ | | | | | | | |
| | | （7） | 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 | | | | | ○ | | | | | | | |
| | | （8） | 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 | | ○ | | | | | | | | | | |
| | | （9） | | | 特定用途機器に対する対策の実施 | | ○ | | | | | | | | | | |
| | | （10） | 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 | | ○ | | | | | | | | | | |
| | | （11） | 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 | | ○ | | | | | | | | | | |
| | 6．2<br>アクセス制御 | （1） | | | アクセス制御 | | ○ | | | ○ | | | | | | | |
| | | （2） | ① | | 外部からのアクセス可能人数の制限 | | ○ | | | | | | | | | | |
| | | | ② | | 外部からのアクセス時の本人確認の機能の確保 | | ○ | | | | | | | | | | |
| | | | ③ | | 外部からのアクセス時の暗号化等の措置 | | ○ | | | | | | | | | | |
| | | | ④ | | 外部アクセス用端末等付与時のセキュリティの確保 | | ○ | | | ○ | | | | | | | |
| | | | ⑤ | | 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） | | | 特権によるネットワーク等への接続時間の制限 | | | | | ○ | | | | | | | |
| | 6．3<br>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 | | | | | ○ | | | | | | | |
| | | | | （オ） | システムの脆弱性テストの実施とその確認 | | | | | ○ | | | | | | | |
| | | （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 | | | | | ○ | | | | | | | |
| | 6．4<br>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更新 | | | | | ○ | | | | | | | |
| | | | ③ | | 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 | | | | | ○ | | | | | | | |
| | 6．5<br>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） | | | サービス不能攻撃対策の実施 | | ○ | | | ○ | | | | | | | |
| | | （4） | | | 標的型攻撃対策の実施 | | ○ | | | ○ | | | | | | | |
| | 6．6<br>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 | 教育委員会事務局職員 | 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 | 一元的な窓口 | 外部委託関係規定 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7. 運用 | 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 | | ○ | | | ○ | | | | | | | |
| | | (5) | | | 内部からの攻撃等の監視 | | ○ | | | ○ | | | | | | | |
| | 7.2 ドキュメントの管理 | (1) | 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 | | ○ | | | ○ | ○ | | | | | | ○ |
| | | (2) | | | ネットワーク構成図等の保管 | | ○ | | | ○ | | | | | | | |
| | | (3) | | | システム障害等の記録、保存 | | ○ | | | ○ | | | | | | | |
| | | (4) | | | 攻撃を受けた時の対応 | ○ | ○ | | | | | | | | | | |
| | 7.3 教職員等のID及びパスワードの管理 | (1) | ① | | 利用者の情報管理やIDの取扱い等の設定 | | ○ | | | ○ | | | | | | | |
| | | | ② | | 利用されるIDの点検 | | ○ | | | ○ | | | | | | | |
| | | (2) | 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 | | ○ | | | ○ | | | | | | | |
| | 7.4 ICカード等の取扱い | (1) | ① | | ICカード紛失時のアクセス停止措置 | | ○ | | | ○ | | | | | | | |
| | | | ② | | Cカード切り替え時の旧カードの廃棄方法 | | ○ | | | ○ | | | | | | | |
| | 7.5 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導入 | | ○ | | | ○ | | | | | | | |
| | 7.6 特権を付与されたIDの管理等 | (1) | | | ID及びパスワードの管理 | | ○ | | | ○ | | | | | | | |
| | | (2) | | | 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 | ○ | ○ | | | ○ | | | | | | | |
| | | (3) | | | 特権代行者の通知 | ○ | △ | △ | △ | △ | | | | | | | |
| | | (4) | | | 特権付与されたID等の変更の外部事業者への委託禁止 | | ○ | | | ○ | | | | | | | ○ |
| | | (5) | | | 特権付与されたID等のセキュリティ機能強化 | | ○ | | | ○ | | | | | | | |
| | | (6) | | | 特権付与されたIDの初期設定以外のものへの変更 | | ○ | | | ○ | | | | | | | |
| | | (7) | | | 特権を付与されたIDのログ監視 | | ○ | | | ○ | | | | | | | |
| | 7.7 情報セキュリティポリシーの遵守状況の確認・管理 | (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) | | | 業務目的外のウェブ閲覧禁止と発見時の対応 | | ○ | | △ | | | | | | | | |
| | | (4) | | | 職員等による不正アクセス時の対応 | | ○ | | △ | ○ | | | | | | | |
| | 7.8 専門家の支援体制等 | (1) | | | 外部の専門家の支援体制の整備 | | ○ | | | | | | | | | | |
| | | (2) | | | 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 | | ○ | | | | | | | |
| | 7.9 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 | ○ | | | | | | | | | ○ | | |
| | 7.10 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 | ○ | | | | | | | | | | | |
| | 7.11 法令遵守 | (1) | | | 主要な法令遵守 | | | | | | | | | ○ | | | |
| | 7.12 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 | △ | ○ | | | △ | | | | | | | |
| 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 | △ | △ | | | ○ | | | | | | | ○ |
| | | (4) | | | 外部委託事業者に対する説明 | | | | ○ | | | | | | | | △ |
| 9. SaaS型パブリッククラウドサービスの利用 | 9.1 SaaS型パブリッククラウドサービスの利用における情報セキュリティ対策 | (1) | | | 利用者認証 | | | | | ○ | | | | | | | ○ |
| | | (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) | | | サービス終了時等のデータの廃棄及び利用者アカウント抹消 | | | | | ○ | | | | | | | ○ |
| | | (13) | | | クラウドサービス要件基準を満たす配慮を含めたネットワーク設計 | | | | | ○ | | | | | | | ○ |
| | 9.2 SaaS型パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項 | (1) | | | 守秘義務、目的外利用及び第三者への提供の禁止 | | | | | ○ | | | | | | | ○ |
| | | (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 | | | | | ○ | | | | | | | ○ |
| | 9.3 SaaS型パブリッククラウドサービス利用における教職員等の留意点 | (1) | ① | | ID・パスワード等の秘匿管理 | | | | | ○ | | | | | | | ○ |
| | | | ② | | 多要素認証要素の管理と報告体制 | | | | | ○ | | | | | | | ○ |
| | | (2) | | | モバイル端末の適切な管理 | | | | | ○ | | | | | | | ○ |
| | | (3) | | | 重要性分類に基づく情報の保管場所制限 | | | | | ○ | | | | | | | ○ |
| | | (4) | ① | | 学校外からクラウドサービスを利用する際の情報資産取扱い制限 | | | | | ○ | | | | | | | ○ |
| | | | ② | | クラウドサービスから端末にファイルをダウンロードする際の安全管理措置 | | | | | ○ | | | | | | | ○ |
| | | (5) | ① | | SaaS型パブリッククラウドサービスの学習用途、校務用途混在リスクへの対応 | | | | | ○ | | | | | | | ○ |
| | | | ② | | SaaS型パブリッククラウドサービスの学習用途、校務用途混在リスクへの適切な運用 | | | | | ○ | | | | | | | ○ |
| | 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 | (ア) | 無断使用に関する規定の確認 | | | | | ○ | | | | | | | |
| | | | | (イ) | 守秘義務に関する規定の確認 | | | | | ○ | | | | | | | |
| | | (2) | | | 約款によるサービスの利用における対策の実施 | | | | | | | ○ | | | | | |
| | 9.5 ソーシャルメディアサービスの利用 | (1) | ① | | なりすまし対策の実施 | | | | | ○ | | | | | | | |
| | | | ② | | 不正アクセス対策の実施 | | | | | ○ | | | | | | | |
| | | (2) | | | 重要性分類Ⅲ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 | | | | | ○ | | | | | | | |
| 10. 評価・見直し | 10.1 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 | | | | | | | | | | ○ | | |
| | 10.2 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 | | | | | | | | | | ○ | | |
| | 10.3 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 | (1) | | | 情報セキュリティポリシー及び関係規程等の見直しに関する規定 | | | | | | | | | | ○ | | |

「教育情報セキュリティ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

| | |
|---|---|
| 五十嵐　晶子 | 教育ICT環境アドミニストレーター協会　理事長<br>合同会社かんがえる　代表 |
| 梅嶋　真樹　（副座長） | 国際電気標準会議システム委員会　スマートエネルギー開発計画担当コンビーナ<br>慶應義塾大学　グローバルリサーチインスティチュート所員<br>兼　SFC研究所上席所員<br>前橋国際大学　客員教授　兼　新学部設置顧問<br>一般財団法人　SFCフォーラム　研究員 |
| 岡村　久道 | 英知法律事務所　弁護士<br>国立情報学研究所　客員教授 |
| 佐々木　良一（特別委員） | 東京電機大学名誉教授　兼　同大学サイバーセキュリティ研究所客員教授 |
| 高橋　邦夫　（座長） | 合同会社KUコンサルティング　代表社員 |
| 谷　正友 | 一般社団法人教育ICT政策支援機構　代表理事 |
| 西田　光昭 | 柏市教育委員会　指導課　教育研究専門アドバイザー |
| 林山　耕寿 | シスコシステムズ合同会社　公共事業　事業推進本部 |
| 藤村　裕一 | 国立大学法人鳴門教育大学大学院　教員養成DX推進機構長 |