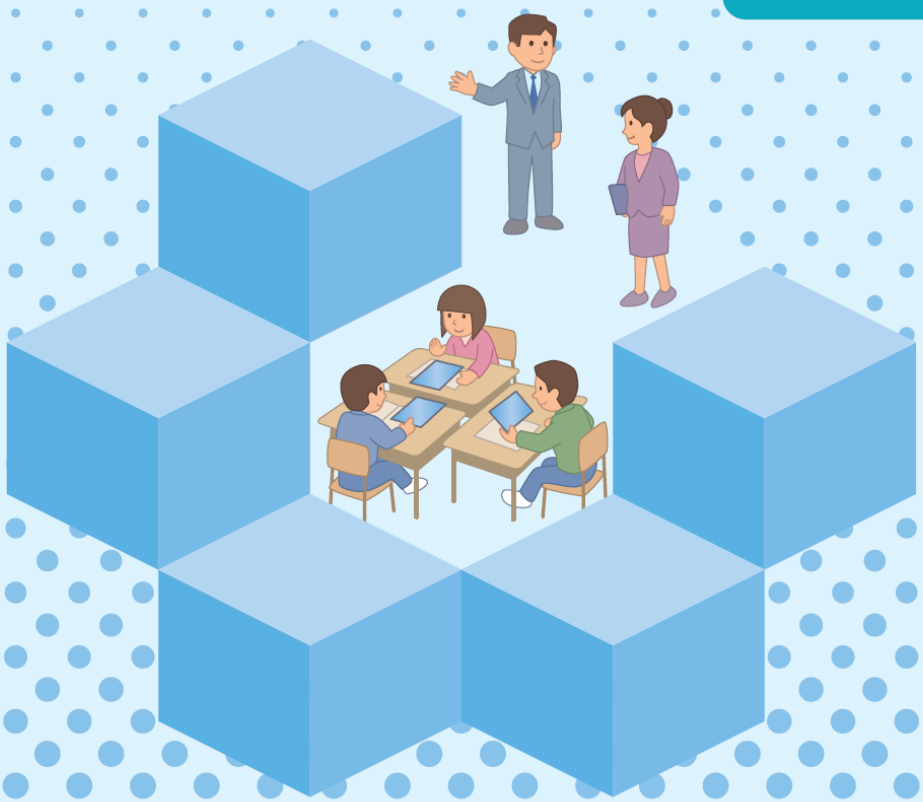
教育情報セキュリティポリシーハンドブック

令和７年３月



文部科学省

目次

第 1 章　はじめに

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、一人ひとり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りました。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～教職員等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 の姿が示され、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ました。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ます。

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ますが、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す。

教育現場における情報セキュリティを検討する際は、教職員等の存在はもちろんのこと、児童生徒・保護者の存在、取り扱う情報の多様性・多目的性、教育クラウドの活用など教育現場ならではの特徴を考慮したうえで、教育情報セキュリティポリシーを独自で策定することが極めて重要です。

このハンドブックは、教育委員会を主な読み手として想定し、教育委員会担当者の情報セキュリティに関する理解の深化を図り、自治体自らが教育情報セキュリティポリシーの策定・見直しを適切に実施できるように、教育現場における情報セキュリティの基本的な考え方及び「教育情報セキュリティポリシーに関するガイドライン」（以下「ガイドライン」という。）の基本的な考え方とポイントを解説しています。

第２章では教育情報セキュリティの基礎について解説していますので、学校の教育情報セキュリティに関する理解の深化にも活用いただけます。

教育現場の実態や情報セキュリティの最新動向を踏まえつつ、最新のガイドラインと合わせて、是非活用ください。

第 2 章　教育現場における情報セキュリティのポイント

2 － 1　教育現場における情報セキュリティの基本的な考え方

児童生徒や教職員等が安心して学習・指導に取り組めるよう、教育委員会と学校が一体となって情報セキュリティを確保する必要があります。教育現場における情報セキュリティを検討する際には、以下の教育現場ならではの特徴を考慮する必要があります。

- 児童生徒・保護者の存在

  地方公共団体の他の行政事務と異なり、児童生徒が 1 人 1 台端末を活用して学習活動を行うなど学校には「服務[1]」を行う者以外が学校のシステムにアクセスします。児童生徒や保護者の存在を考慮したアクセス権限の設定や、児童生徒に対する指導の実施も求められます。

- 情報の変容

  学校で取り扱われる情報は、取り扱う主体や目的、付加される情報によって大きく変容します。例えば学習活動において児童生徒が作成したワークシートは、教員による評価に関する情報が記載されれば成績情報として取り扱うべき情報に変容する可能性があります。また、児童生徒の情報に教職員等のみがアクセスするか、児童生徒本人がアクセスするかによっても、その情報の取扱いは変化します。

- GIGA スクール構想に基づくクラウド活用

  GIGA スクール構想により、学校でのパブリッククラウドの本格活用が進みました。また、校務のクラウド環境での実施を前提とする次世代校務 DX の取組が進展しており、重要な情報のクラウド上での取扱いが前提になりつつあることについても考慮する必要があります。

[1] 公務員が職務遂行等のために守るべき義務や規律のこと。

２－２　何を守るか

情報セキュリティ対策を行うことにより、教育現場における様々な「情報資産」を守ります。情報資産とは、学校が保有している情報そのもの（文書やデータファイル）や、その情報を生成・保管・流通する媒体（紙、ネットワーク、サーバ、端末等）のことを指します。これらを適切に守るためには、情報資産をセキュリティ侵害による影響度（被害の大きさ）に応じて４段階に分類・仕分けし、その重要性に応じた対策を講じる必要があります。重要性が高い情報であればあるほど、セキュリティ対策はより強固にすべきであり、アクセス権限を付与する関係者を制限する必要があります。重要性分類に関する詳細については、３－２（３）もご参照ください。

分類	定義	具体例
重要性分類Ⅰ	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	指導要録原本
重要性分類Ⅱ	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	通知表、定期考査・テスト等の採点結果、調査書、進路希望調査
重要性分類Ⅲ	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）	出席簿、授業用教材、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）
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	学校・学園要覧、学校紹介パンフレット、学校・学園ホームページ掲載情報

図表　１　情報資産の分類の定義と具体例

なお、重要性分類を実施する際には、機密性・完全性・可用性の侵害の影響度を考慮する必要があります。

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。
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。
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。

図表　２　情報セキュリティの３要素

2 – 3　何から守るか

情報セキュリティ対策により、教育現場における様々な「脅威」から情報資産を守ります。脅威とは、セキュリティを侵害して損害[2]を引き起こす要因です。また、脅威は外部からだけでなく、内部関係者によっても引き起こされることに留意する必要があります。

脅威例
不正アクセス、物理的侵入、不正操作、過失操作、不正認証、不正媒体・機器接続、プロセス不正実行、マルウェア感染、情報窃取、情報改ざん、情報破壊、不正送信、機能停止、内部拡散、制御不能・異常動作、高負荷攻撃、窃盗、盗難・廃棄時の分解による情報窃取、経路遮断、通信輻輳（ふくそう）、無線妨害、盗聴、通信データ改ざん、不正機器接続、自然災害　等

図表 3　攻撃手法の視点から見た脅威一覧[3]

攻撃者		意味	具体例
悪意のある第三者		制御システムの内部関係者以外で、システムに対する攻撃を行う人物・組織・団体	・ 国家レベルのサイバー攻撃者 ・ 一定のスキルを持った攻撃者 ・ 個人の攻撃者
内部関係者	過失	制御システムの所有者や保守・運用関係者等のうち、攻撃者による過失の誘発あるいは偶発的な誤りによって、システムに対する攻撃を行う人物・組織・団体	・ 制御システムに関する全ての権限を有する内部関係者 ・ 制御システムに関する一部の権限を有する内部関係者 ・ 制御システムにアクセスする権限を一切有していない内部関係者
	故意	制御システムの所有者や保守・運用関係者等のうち、故意にシステムに対する攻撃を行う人物・組織・団体	

図表 4　脅威を引き起こす攻撃者の分類[4]

実際に教育現場で発生したインシデントに基づき、以下に様々な脅威によって引き起こされるセキュリティ侵害の具体例を示します。

---

[2] 教育ネットワーク情報セキュリティ推進委員会（ISEN）「『令和 5 年度 学校・教育機関における個人情報漏えい事故の発生状況』調査報告書（第 2 版）」によると、令和 5 年度には、学校・教育機関において 231 件の個人情報漏えい事故が発生し、約 14 万人の個人情報が漏えいしている。https://school-security.jp/wp/wp-content/uploads/2024/11/2024_2.pdf

[3] 「制御システムのセキュリティリスク分析ガイド 第 2 版」(2023 年 3 月版) P105 表 4-15 資産（機器）に対する脅威（攻撃手法） 及び表 4-16 資産（通信経路）に対する脅威（攻撃手法）より引用しつつ、教育現場の実態や最新の事故事例等を踏まえ「不正認証」「内部拡散」「自然災害」等を追加したもの。https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf

[4] 「制御システムのセキュリティリスク分析ガイド 第 2 版」(2023 年 3 月版) P108 表 4-18 脅威（攻撃者）の分類より引用。https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf

【教職員等の不適切な情報の取扱いに起因する児童生徒による情報の閲覧（不正アクセス）】

教職員等が重要性の高い情報（成績情報等）を机上に置きっぱなしにしたり、端末の画面に表示した状態のまま席を離れたりしてしまい、児童生徒が成績情報等の情報をのぞき見してしまう事故が想定されます。教職員等の情報管理のリテラシー向上のための研修の実施や、離席時にパソコンをロックするなどの対策が有効です。

【情報資産の外部持ち出し[5]による情報漏えい（不正媒体・機器接続、情報窃取）】

教職員等が端末や USB を校外に持ち出し紛失する、私用端末に校務系情報をダウンロードし、そこから情報漏えいが起こるなどの事故が想定されます。教職員等が外部持ち出しの際に利用するクラウドサービス（電子メールや外部ストレージサービス等）についてはログを管理する運用としたり、教育委員会や学校が管理していない私的に契約したクラウドサービスの業務利用や承認されていない私物端末の業務利用は禁止とし、教育委員会又は学校から提供される公式サービスや支給端末のみを利用させたりすることが重要です。特に、承認されていない私物端末の業務利用は、不正プログラムを持ち込むリスクもあり、大変危険です。情報資産の運用管理やルール面での対策に加えて、誤送信等に備えて暗号化やパスワード設定を行うなどシステム面での対策も有効です。

【情報資産の外部持ち出しによる情報漏えい（窃盗、盗難・廃棄時の分解による情報窃取、情報窃取）】

教職員等が端末や USB、紙媒体を校外に持ち出した際に、窃盗被害にあって情報が流出する事故が想定されます。また、教育委員会・教職員等・委託事業者等による盗難や、情報資産の廃棄不備に起因する情報流出も想定されます。そのため、情報資産の運用管理やルール面での対策に加えて、情報窃取等に備えて暗号化やパスワード設定を行ったり、端末紛失時には MDM（モバイル端末管理：Mobile Device Management）等により端末をロックしたり、復元されない形で廃棄したりするなどシステム面での対策も有効です。

【アクセス権限の不十分な設定・保存先の誤り（過失操作）】

アクセス権限の不十分な設定や教職員等による保存先の誤りにより、児童生徒が 1 人 1 台端末から本来アクセスできてはならない校務系情報にアクセスできてしまうという事故が想定されます。情報資産の分類と管理を行う際、教育委員会がアクセス主体を明示し、アクセス主体に応じた適切な権限設定を行うとともに、教職員等に対して研修を徹底する等の働きかけを実施することが必要です。

【重要性の高い情報の誤表示（過失操作）】

教職員等が教室で重要性の高い情報（成績情報等）を取り扱っている際、誤って大型提示装置に情報を投影してしまい、児童生徒に誤表示してしまうような事故が想定されます。次世代校務 DX の進展により教職員用端末の 1 台化が進むことが想定されます。運用ルールの工夫等により、新たな環境で想定されるリスク軽減を図る必要があります。

【自然災害による情報消失（自然災害）】

大規模地震、風水害等による自然災害による学校やサーバ設置施設の停電、浸水、破損により、情報資産が破壊、消失する危険性があります。物理的に安全な場所・施設に情報を保管管理する、バックアップを実施するなどの対策が有効です。

---

[5] 教育委員会・学校が構築・管理している環境（組織が利用するサーバやクラウドサービス等）の外（家庭や地域、事業者等）に情報資産を持ち出すことを指し、例えばデータを端末や USB に保存した状態で外部に持ち出すこと、電子メールや外部ストレージサービスを用いて情報を組織外部に送信すること等が該当する。

２－４　どのように守るか

情報資産を脅威から守るために、「物理的セキュリティ対策」、「人的セキュリティ対策」、「技術的セキュリティ対策」を組み合わせ、セキュリティ対策を講じます。情報資産の重要性、想定する脅威、コスト面等も考慮したうえで、教育現場におけるネットワーク環境や端末のスペック等の運用実態を踏まえたセキュリティ対策を講じる必要があります。例えばウイルス対策ソフト等の技術的セキュリティ対策のみを導入するだけでは不十分であり、３種類の対策をバランス良く講じることが重要です。特に教育現場においては、教職員等による教育情報セキュリティポリシーや実施手順等の遵守といった人的対策を適切に講じることが重要です。

個別対策	概要	対策による効果（例）
物理的セキュリティ対策	サーバ、通信回線等の機器の設置や設定、保守管理に関する措置や機器等の管理区域の適切な管理等の物理的な方法を通じて情報資産を守る対策	情報システム室等への物理的な侵入による情報資産の破壊・盗難・改ざん・消去や、情報の不正取得のための工作（盗聴等）、自然災害等による情報の滅失を防ぐ。
人的セキュリティ対策	情報資産を取り扱う当事者のルール遵守などを通じて情報資産を守る対策	運用上の過失等からのセキュリティ侵害を最小限に抑え、情報資産の安心・安全な運用を維持する。
技術的セキュリティ対策	ハードウェア・ソフトウェアやネットワークなどに対するアクセス制御、不正プログラム対策、不正アクセス対策等の技術的な安全管理措置を通じて情報資産を守る対策	悪意のある第三者や内部関係者からの不正アクセス等により、情報漏えいなどのセキュリティ侵害が生じることを防ぐ。

図表 5　個別対策の具体例

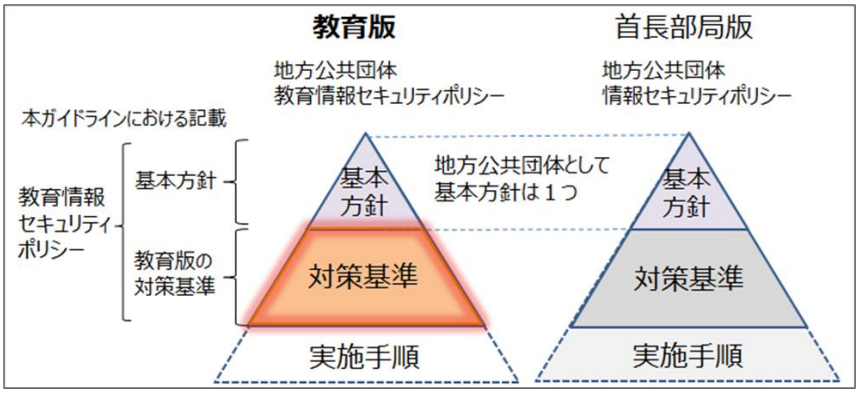
また、教育委員会に学校におけるセキュリティインシデントに関するコミュニケーションの核となる体制を構築することが望ましいです。

第３章　教育情報セキュリティポリシー策定の際のポイント

３－１　教育情報セキュリティポリシーとは

教育情報セキュリティポリシーとは、教育分野に関して、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指します。２－１で示したとおり、教育現場には地方公共団体の他の行政事務とは異なる特徴があります。学校は児童生徒が過ごす場所であり、児童生徒が学校のシステムにアクセスして学習活動等を実施しますので、「服務」に服さない児童生徒や保護者の存在も鑑みたルール作りが重要になります。教育委員会は、最新のガイドラインに基づき、それぞれの教育現場の環境やコスト、運用実態を踏まえた教育情報セキュリティポリシーを策定する必要があります。また、次世代校務 DX 環境への移行や生成 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ため、これらの変化に合わせた見直しも重要です。

情報セキュリティポリシーは「基本方針」と「対策基準」から成ります。教育委員会は、教育現場独自の「対策基準」の策定・見直しを実施します。教育現場が教育情報セキュリティポリシーを適切に履行できるよう、各学校は「対策基準」を実施するための具体的な手順等をまとめたマニュアルである「実施手順」を定めます。



図表 6　情報セキュリティポリシーの体系

基本方針：情報セキュリティ対策における基本的な考え方を定めるものであり、教育情報セキュリティポリシーにおいては**地方公共団体が策定したものを準用**します。

対策基準：基本方針に基づいて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ものであり、ガイドラインに基づき**各教育委員会が策定・見直しを行います。**

実施手順：対策基準に基づいて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マニュアルです。**教育委員会等は各自治体の実態を踏まえた実施手順のひな形を策定し、各学校はひな形に基づき策定・見直しを行います。**

３－２ 「教育情報セキュリティポリシーに関するガイドライン」のポイント

文部科学省は、教育委員会等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、ガイドラインを策定しています。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）」で対策基準の例をまとめており、市の教育委員会を想定して記述しています。以下、教育情報セキュリティポリシー策定に当たって押さえるべきポイントを整理しました。

※書きとして、ガイドラインの該当箇所を示していますので、合わせてご参照ください。

（１）対象範囲及び用語説明

① 基本的な考え方 ※第２編１.、第１編第１章（３）①

情報セキュリティの確保に当たっては、教育情報セキュリティポリシーの対象を明確化するために、対象となる行政機関等及び情報資産の範囲、用語の定義を行う必要があります。教育情報セキュリティポリシーの対象は、教育ネットワーク、それに接続されているシステム、そのシステム上で取り扱われるデータ（印刷されたものを含む）です。

自治体共通で取り扱う行政系システムについては、行政系端末により行政ネットワーク上で行われる自治体共通業務を実施している場合や教育ネットワークが行政系ネットワークと分離されていない場合（例えば校務支援システムを行政系ネットワーク上に構築している場合等）は、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（以下「自治体ガイドライン」という。）に準拠した対策が求められます。

② ガイドラインのポイント ※第２編１.

ガイドラインは、行政機関等の範囲、情報資産の範囲、用語について定めています。

・対象となる組織の範囲

教育委員会、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）

・情報資産の範囲

学校で扱う情報資産を想定しています。情報資産については、２－２で示したとおり、学校が保有する文書やデータファイルだけでなく、その媒体（紙、ネットワーク、サーバ、端末等）も含んでいます。

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

（２）組織体制

① 基本的な考え方 ※第２編２．

情報セキュリティ対策を確実に行うためには、組織体制を整備し、一元的にセキュリティ対策を実施することが必要です。権限・責任を持つ担当者を定め、情報セキュリティに関する重要事項を決定する機関である情報セキュリティ委員会が決定する方針の下でセキュリティ対策を実施することで、安全な運用やインシデント発生時等の速やかな対応につながります。

② ガイドラインのポイント ※第２編２．

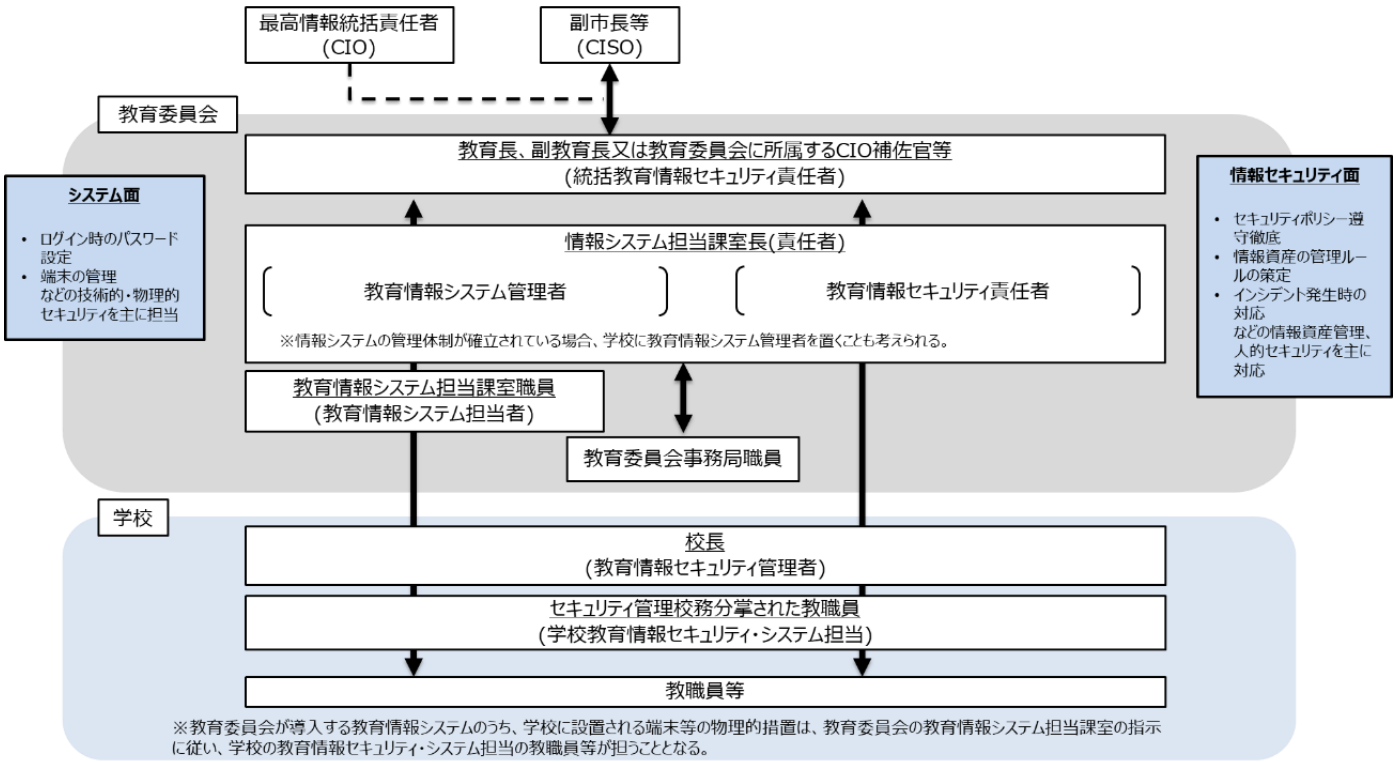
ガイドラインは、以下のとおり組織体制を構成する責任者や設置すべき組織、それらの役割を定めています。

責任者等	役割
最高情報セキュリティ責任者（CISO: Chief Information Security Officer）	**首長部局と共通して設置**され、**副市長等が担う**ことを想定。地方公共団体における全ての教育ネットワーク、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。
最高情報統括責任者（CIO: Chief Information Officer）	**首長部局と共通して設置**され、**副市長等が担う**ことを想定。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。
統括教育情報セキュリティ責任者	**教育長、副教育長又は教育委員会に所属する CIO 補佐官等が担う**ことを想定。CISO を補佐する役割であり、地方公共団体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。また、**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。** 緊急時等の円滑な情報共有のために関係者の緊急連絡網を整備し、情報セキュリティ**インシデント発生時**等には**中心となって被害の拡大防止、事態の回復のための対策実施、再発防止策の検討を行う。**
教育情報セキュリティ責任者	**教育委員会の情報セキュリティ担当部局の課室長**が担うことを想定。教育情報セキュリティ対策に関する権限及び責任を有し、地方公共団体が所有している教育情報システムの開発、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。 **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に対する教育、訓練、助言及び指示を行う。**
教育情報システム管理者	**教育委員会の情報システム担当課の課室長**が担うことを想定。**個々の教育情報システム**の開発、設定の変更、運用、見直し等を行う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に関する権限及び責任を有する。 **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・管理を行う。**
教育情報システム担当者	教育委員会の情報システム担当課の職員。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、見直し等の作業を行う。
教育委員会事務局職員	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する。
教育情報セキュリティ管理者	**校長**が担うことを想定。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し、学校で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、指示を仰ぐ。
教職員等	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する。

図表 7 責任者等と役割

組織等	役割
情報セキュリティ委員会	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。毎年度、情報セキュリティ対策の改善計画を策定してその実施状況を確認する役割を合わせて担うことが望ましい。
情報セキュリティに関する統一的な窓口 （CSIRT: Computer Security Incident Response Team）	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の、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。 CISO が整備を実施する。

図表 8　組織等と役割



図表 9 情報セキュリティ対策推進のための組織体制例

（３）情報資産の分類と管理方法

① 基本的な考え方 ※第２編３.

情報資産を適切に守るためには、情報資産をその重要性に応じて分類・仕分けし、その分類に応じた管理を行う必要があります。

② ガイドラインのポイント ※第２編３.

ガイドラインは、情報資産の重要性やアクセスする主体に基づく分類・仕分けの考え方と、その分類に応じた管理方法を定めています。

● 情報資産の分類 ※第２編３.１.

情報資産をセキュリティ侵害による影響度（被害の大きさ）に応じて４段階の重要性に分類・仕分けし、それらの情報に誰がアクセスすることが想定されるか（アクセス主体）を整理します。ガイドライン P35 には情報資産の例示も併せて整理していますので、ご参照ください。

重要性分類	各情報資産にアクセスする主体		
	教職員等[6]・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	**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	**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	
Ⅱ	**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	**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	
Ⅲ	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	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	
Ⅳ	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

図表 10 重要性分類に基づく情報資産の例示

[6]「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。

●情報資産の管理　※第２編３.２.

情報資産の管理責任を明確にし、情報資産の重要性に応じて、情報の一連のライフサイクル（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）ごとに管理体系を定めます。

（管理責任）　※第２編３.２.（１）

組織の各責任者等は以下のとおり情報資産の管理について役割を担います。

責任者等	役割
統括教育情報セキュリティ責任者	• 学校教育情報セキュリティ対策基準を策定 • 対策基準に基づき、実施手順ひな形を作成 • 標準情報資産台帳（標準台帳）を作成・更新
教育情報セキュリティ管理者	• 実施手順ひな形に基づき、自校の実施手順を作成 • 標準台帳に基づき自校向け情報資産台帳[7]（台帳）を整備 • 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
教職員等	• 台帳及び実施手順に基づく、適切な情報資産の取扱い

図表 11 各責任者等の管理責任

（情報資産の利用）　※第２編３.２.（５）

情報資産はその重要性分類に応じて適切に取り扱う必要があります。また、分類が異なる情報が記録されている電磁的記録媒体や保存領域については、最高度の分類に従った取扱いを行う必要があります。適切な情報資産の取扱いを実現させるためには、必要な者に必要な権限（編集・閲覧・複製・ダウンロード等）を付与する、アクセス制御を実施することが重要です。

重要性分類	**取扱制限**
Ⅰ	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
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
Ⅲ	教職員等・教育委員会・児童生徒本人とその保護者のうち、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
Ⅳ	特段の利用制限等はない

図表 12 情報資産の利用

なお、パブリッククラウド上で重要性分類Ⅱ以上の情報を取り扱う際には、多要素認証を含む強固なアクセス制御[8]による対策を講じなければいけません。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しています。この際、教職員等から児童生徒へ適切な指導を行うことも必要です。詳細は、３－２（５）（児童生徒への指導）をご参照ください。

---

[7] 学校で取り扱う情報資産（文書やデータファイル）一つひとつに対して、重要性分類、保管場所、取扱者、外部持ち出し制限、保管期限等を明記したもの。

[8] 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。

（情報資産の外部持ち出し） ※第２編３.２.（７）

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（組織が利用するサーバやクラウドサービス等）の外（家庭や地域、事業者等）に情報資産を持ち出すことを指し、例えばデータを端末や USB に保存した状態で外部に持ち出すこと、電子メールや外部ストレージサービスを用いて情報を組織外部に送信すること等が該当します。学校外での作業であっても、教育委員会・学校が構築・管理しているクラウド上で情報を取り扱う場合には外部持ち出しには該当しません。

教職員等は、重要性分類Ⅱ以上の情報資産の外部持ち出しの際には、アクセス制限や暗号化を行った上で、教育情報セキュリティ管理者の個別許可を得て持ち出し・持ち帰りの記録をつける必要があります。重要性分類Ⅲの情報資産については、教育情報セキュリティ管理者の判断で包括的許可が可能です。

電子メール、外部ストレージサービス等により重要性分類Ⅲ以上の情報資産を外部送信する際は、アクセス制限や暗号化を行う必要があります。用いるサービスは、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いけません。

USB メモリ等の物理的な媒体による情報の外部持ち出しについては、紛失に関するセキュリティインシデント等も多く発生していることから、教育委員会又は学校から支給された公的な媒体の利用の徹底が必要です。また、これらの媒体の暗号化機能を活かすことも有効です。

（４）物理的セキュリティ

① 基本的な考え方 ※第２編４.

物理的セキュリティ対策とは、サーバ、通信回線等の機器の設置や設定、保守管理に関する措置や機器等の管理区域の適切な管理等の物理的な方法を通じて情報資産を守る対策を指します。自然災害・停電等の緊急時の業務の継続性の確保に有効であるとともに、情報資産の盗難や不正取得による情報資産の漏えいを防ぐことにもつながります。また、取り扱う情報資産の重要性に応じて機器等を適切に廃棄することにより、情報資産の漏えいを防ぐことも重要です。

GIGA スクール構想により１人１台端末を用いた学習におけるクラウド活用が進みました。さらに、次世代校務 DX の考え方に基づき、校務でのクラウド活用が進みつつあります。パブリッククラウド上で教育関係システムを運用することにより、大規模災害発生時等の非常時にデータの損失やデータにアクセスできない事態の発生を防ぎ、場所や時間を選ばない迅速な情報共有や意思決定、業務実施が可能になると考えられます。

② ガイドラインのポイント ※第２編４.

ガイドラインは、サーバ、通信回線及び通信回線装置等の設置や設定、保守管理の方法について定めるとともに、管理区域（情報システム室等）の適切な管理、情報資産を取り扱う端末等の機器の適切な管理や廃棄方法について定めています。

● サーバ等の管理 ※第２編４.１.

教育情報システム管理者は、サーバ等の機器を安全な環境に設置し、特に重要性分類Ⅱ以上の情報資産を取り扱うサーバは冗長化[9]、予備電源を備える等の措置を行います。また、機器の定期保守、修理の実施も重要です。さらに、機器の廃棄の際にはその機器に保存されている情報資産の重要性分類に応じて処分方法を検討する必要があります。

分類	機器の廃棄等の方法
（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。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。
（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。具体的には、**（１）で先述した方法①～⑤のほか、⑥OS 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。 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。

図表 13 重要性分類に応じた機器の廃棄等の方法

[9] 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。

● **通信回線及び通信回線装置の管理** ※第２編４.３.

統括情報セキュリティ責任者は、通信回線及び通信回線装置を、施設管理部門と連携して適切に管理する必要があります。特に、外部へのネットワーク接続ポイントや、そこに接続される端末を正確に把握し、十分なセキュリティ対策を実施するとともに、学校運営上必要なネットワーク帯域を確保し、遅延等に対する適切な対策を講じなければなりません。

● **教職員等の利用する端末や電磁的記録媒体等の管理** ※第２編４.４.

教育情報システム管理者は、教職員等の利用する端末や電磁的記録媒体等に対して、適切な認証設定、データ暗号化、マルウェア感染対策等の管理を実施します。

（多要素認証） ※第２編４.４.（４）

多要素認証とは、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、異なる認証方式を２要素以上組み合わせた認証方式です。パブリッククラウド上で重要性分類Ⅱ以上の情報を取り扱う際には、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る必要があります。

認証要素	認証手段	概要	例
要素A	知識	本人だけが知っている情報	パスワード
要素B	生体	本人だけに備わっている特徴	静脈、顔、指紋、網膜、虹彩
要素C	物理	本人だけが持っている物	ICカード、USB キー、トークン

多要素認証
・要素の異なる2種類以上を組み合わせた認証

例）要素A+要素B
要素A+要素C
要素B+要素C

図表 14 多要素認証

（マルウェア感染対策） ※第２編４.４.（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る必要があります。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や、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てください。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で、重要性分類Ⅱ以上の情報資産を取り扱う端末に対してはふるまい検知等の活用を検討し、適切な対策を講じる必要があります。

ふるまい検知とは、端末の状況や通信を監視して、異常や不審な挙動を検知する仕組みを指します。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できない攻撃が頻発しています。こうした未知の攻撃を検知するためには、既存のパターンファイル情報に依存することなく検知できる、ふるまい検知が有効です。

● 学習者用端末のセキュリティ対策 ※第２編４.５.

１人１台端末は、学校内（教室）での活用だけではなく、学校外における調べ学習や家庭に持ち帰っての学習など様々な学習活動で使用されます。児童生徒に対する学習者用端末の管理方法等についての指導を前提として、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す。

（不適切なウェブページの閲覧防止）※第２編４.５.（１）

児童生徒による不適切なウェブページの閲覧を防止するため、実現したい機能や実際の運用に応じてフィルタリングや検索エンジンのセーフサーチ、セーフブラウジングなどのセキュリティ対策を適切に講じることが重要です。学校現場においては児童生徒の情報活用能力の向上を図りつつ、過剰な規制に陥ることなく、フィルタリング等の設定を適切に行い、安全・安心で豊かな学習機会を全ての児童生徒に保障することが重要です。

フィルタリング	違法・有害サイトへのアクセスを利用者側で自主的に制限することができる機能。端末に標準的に搭載された製品、インターネットサービスプロバイダーが提供する製品、セキュリティ事業者が提供する製品・サービスなどがある。フィルタリングの方式は特定の URL を指定して閲覧を防ぐブラックリスト方式、特定の URL のみを閲覧許可するホワイトリスト方式、特定の情報が含まれる場合に閲覧を防ぐカテゴリ（コンテンツ）フィルタリング方式などがある。フィルタリングは随時設定の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、カテゴリ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。
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。
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。対象となるウェブサイトは主に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、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。

図表 15 不適切なウェブページ閲覧を防止するための対策例

（マルウェア感染対策） ※第２編４.５.（２）

学校内外で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、端末の利用におけるマルウェア感染対策を講じる必要があります。主な対策としてはウイルス対策ソフトのインストールや、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等があります。

（端末を不正利用させないための防止策・セキュリティ設定の一元管理） ※第２編４.５.（３）（４）

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するために MDM 等によりセキュリティ制御を行うことが必要です。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、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ようにすることが望ましいです。

（端末の盗難・紛失時の情報漏えい対策） ※第２編４.５.（５）

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ないよう、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原則端末内部に情報を保存しないようにする運用や、MDM 等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消去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が必要です。

（５）人的セキュリティ

① 基本的な考え方 ※第２編５.

人的セキュリティ対策とは、情報資産を取り扱う当事者のルール遵守などを通じて情報資産を守る対策を指します。

運用上の過失等からのセキュリティ侵害を最小限に抑え、情報資産の安心・安全な運用を維持するためには、人的セキュリティ対策が効果的です。当事者一人ひとりが、情報セキュリティ意識を高く持ち、それに基づく行動を徹底しなければ、物理的セキュリティ対策、技術的セキュリティ対策を講じていたとしても、重大な情報セキュリティインシデントにつながりかねません。実際に、教育現場では、個人情報や成績情報を誤って児童生徒がアクセス可能な場所に保管したことで個人情報が漏えいした事故や、成績一覧が記載された紙の裏に記載したメモを生徒に手渡したことで成績情報が漏えいした事故、USB メモリの紛失による個人情報や写真データの抽出など、教職員等の過失による事故が多く発生しています。

様々な立場の人が情報資産を取り扱うという特徴を持つ教育現場では、教職員等のルール遵守を徹底させるとともに、前述したような教育現場での事故事例等を踏まえた研修を実施することが重要です。加えて、教育情報セキュリティ管理者（校長）からの働きかけ、児童生徒への指導等を通じて、一人ひとりに遵守すべき内容とその必要性を浸透させることが重要です。

② ガイドラインのポイント ※第２編５.

ガイドラインは、教育情報セキュリティ管理者（校長）・教職員等・教育委員会の遵守事項を定めるとともに、研修・訓練、情報セキュリティインシデントの連絡体制の整備についても定めています。

● 教育情報セキュリティ管理者（校長）の措置事項 ※第２編５.１.

教育情報セキュリティ管理者（校長）は、教職員等による情報資産の外部持ち出しや外部委託による廃棄処理について記録を行う、ソフトウェアやコンテンツの利用制限・新規購入について教育情報システム管理者に判断を仰ぐなど、自校の資産管理に関する責任を有します。また、教職員等の情報セキュリティ意識の醸成、情報セキュリティポリシー等の遵守指導、自校の情報セキュリティ対策に関する自己点検を行うなど、自校の情報セキュリティ確保に関する責任を担います。

● 教職員等の遵守事項 ※第２編５.２.

教職員等は、情報セキュリティ確保のために以下の事項を遵守する必要があります。

（支給端末の取扱い）

業務目的以外で利用してはいけません。また、端末から離れる際は端末をロックする等、他者が閲覧できないように留意します。自宅や学校外等での情報処理作業においても支給された端末を利用することとし、支給以外の端末等は原則利用してはいけません。

（パスワードの取扱い）

パスワードについては、想像しにくい設定（類推しやすい並び方やその安易な組合せにしないこと、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）等とすることが必要です。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も有効です。

（無許可のクラウドサービス・ソフトウェアの利用）

私的に契約したクラウドサービスや個人アカウント、ソフトウェアは教育情報セキュリティ管理者が管理できない可能性があり、セキュリティリスクにつながるため、利用を禁止する必要があります。

（児童生徒への指導）

教職員等のみならず、児童生徒も学校の情報を取り扱う主体となることから、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、以下の事項等について指導を行う必要があります。

- 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。
- 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。
- 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。
- 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。
- 端末で生成した情報は原則学習系クラウドに保管し、学習者用端末へのローカル保存は必要最小限とすること。
- 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。
- 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。
- 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。
- 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。
- 私物端末など承認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。
- 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）を端末にダウンロードした場合には、目的を達成し次第速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。

● **教育委員会事務局職員の遵守事項** ※第２編５.３.

教育委員会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、教育情報セキュリティ責任者の責任の下、学校と同様に情報セキュリティの遵守義務を負います。

教育委員会は、教育情報セキュリティポリシー等を遵守し、校務用端末による外部における情報処理作業の禁止、重要性分類Ⅱ以上の情報資産への校務用端末以外からのアクセスの禁止、知り得た情報の秘匿等を実施する必要があります。

● **研修・訓練** ※第２編５.４.

情報セキュリティの確保は業務上の利便性の向上とは必ずしも相容れない場合があることもあり、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があります。情報セキュリティを確保するためには、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重要です。

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 にあります。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、セキュリティ対策を実施できるよう、ｅ ラーニング、集合研修、説明会等の形で研修・訓練を定期的且つ計画的に実施する必要があり、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しなければなりません。研修に際しては、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（校長）、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、それぞれの役割と理解度に応じた内容とすることが重要です。

● **情報セキュリティインシデントの連絡体制の整備** ※第２編 5.５.

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連絡体制を整備することが必要です。

（６）技術的セキュリティ

① 基本的な考え方 ※第２編 6.

技術的セキュリティ対策とは、ハードウェア・ソフトウェアやネットワークなどに対するアクセス制御、不正プログラム対策、不正アクセス対策等の技術的な安全管理措置を通じて情報資産を守る対策を指します。

GIGA スクール構想による１人１台端末を用いた学習におけるクラウド活用に加えて、次世代校務 DX の考え方の下で、校務でのクラウド活用も進んでいます。クラウド上で重要性の高い情報を扱う場面も増える中、教育委員会はこの変化に合わせた技術的セキュリティ対策の実施に対応することが求められます。

② ガイドラインのポイント

ガイドラインは、コンピュータ及びネットワークの設定管理やアクセス制御に関する規定、不正プログラムや不正アクセスに対する対策などを定めています。

● コンピュータ及びネットワークの設定管理

（バックアップの実施） ※第２編６.１.（２）

校務系情報を取り扱うサーバの情報資産を消失した場合、例えば成績処理が行えないなど、学校事務の遂行に重大な支障を及ぼします。このため、校務系サーバは定期的にバックアップを実施する必要があります。学習系サーバについても、併せてバックアップを行うことが望ましいです。

（ログの取得等） ※第２編６.１.（３）

ログや障害対応記録は、情報セキュリティインシデントの検知や情報セキュリティ上の問題を解明するための重要な材料となります。特に校務系システムのログについては、６か月以上保管することが望ましいです。

（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） ※第２編６.１.（７）、第３編（３）

重要性分類Ⅱ以上の情報を守るため、「強固なアクセス制御による対策」又は「ネットワーク分離による対策」を講じたシステム構成を整備する必要があります。

＜強固なアクセス制御による対策＞

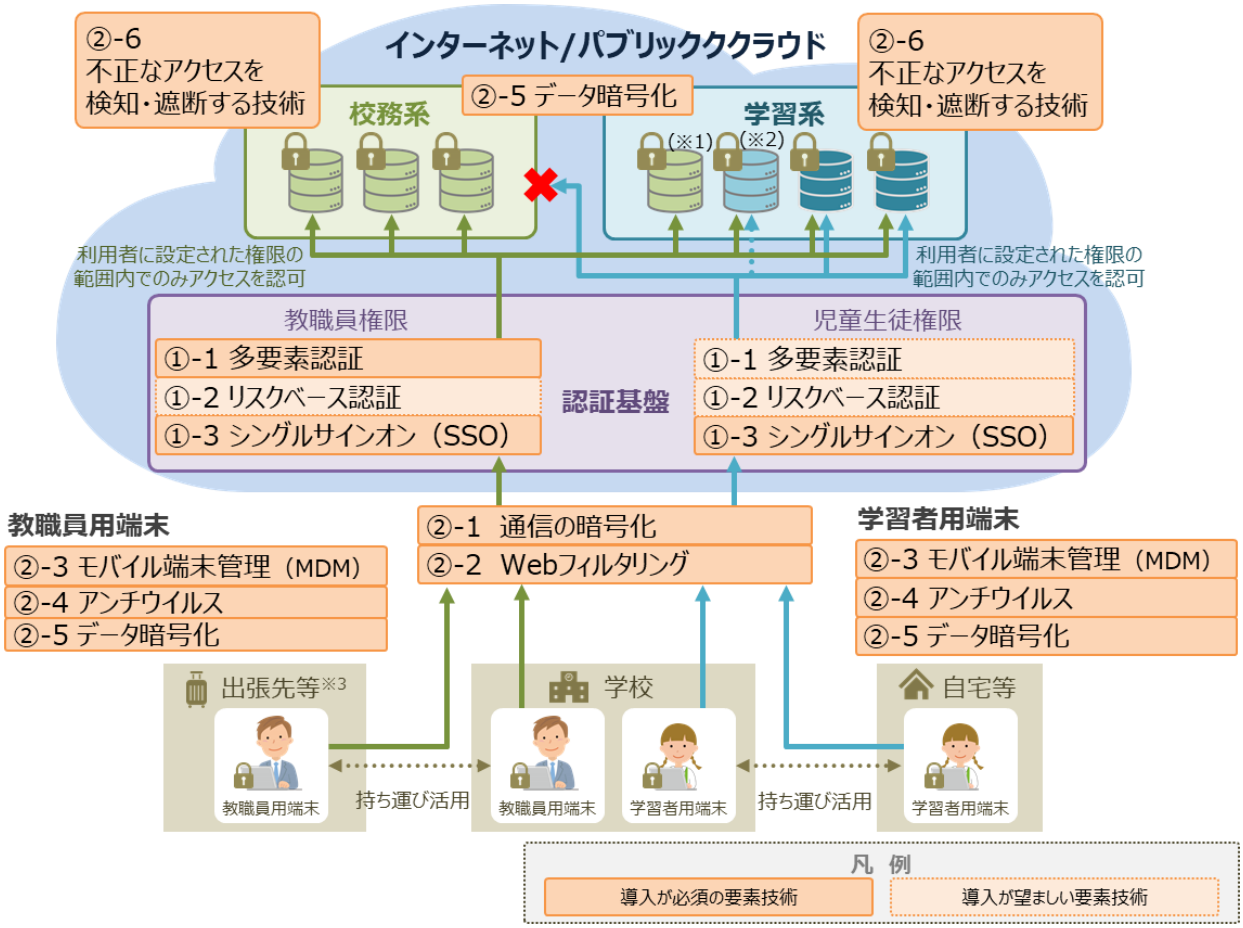
強固なアクセス制御による対策とは、インターネットを通信経路とする前提で、内部・外部からの不正アクセスを防御するために、多要素認証による利用者認証、端末認証、端末・サーバ・通信の監視・制御等を組み合わせたセキュリティ対策を指します。この対策を講じるに当たっては、利用者毎に情報へのアクセス権限を適切に設定するとともに、アクセスの真正性、端末・サーバ・通信の安全性を確保する観点から、端末とクラウドサービスを提供するサーバ間の通信を暗号化し、認証により利用者のアクセスの適正さを常に確認しなければいけません。

パブリッククラウド上で重要性分類Ⅱ以上の情報を取り扱う際には、強固なアクセス制御による対策を講じなければいけません。学校における働き方改革、教育活動の高度化、教育現場のレジリエンスの確保に資する次世代校務 DX の実施に際しては、重要性分類Ⅱ以上の情報をパブリッククラウド上で取り扱うため強固なアクセス制御を講じる必要があります。

①アクセスの真正性に関する要素技術		
①- 1	多要素認証	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要素以上を組み合わせる認証方法。なりすましや不正アクセスを防ぐ。 ※強固なアクセス制御の基づくセキュリティ対策を講じるに当たっては、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
①- 2	リスクベース認証	端末の IP アドレスや位置情報、使用されている Web ブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める認証方法。なりすましや不正アクセスを防ぐ。
①- 3	シングルサインオン（SSO）	一度の認証で複数のシステムへのアクセスが可能となる仕組み。利便性を向上させるとともに、認証の煩雑化によるセキュリティリスクの低減を図る。
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	通信又は通信経路を暗号化し保護すること。第三者から通信内容を盗み見られることを防ぐ。
②- 2	Web フィルタリング	インターネット上の特定のコンテンツや Web サイトへのアクセスを制限する機能。セキュリティリスクの高い Web サイトへのアクセスを防ぐ。
②- 3	モバイル端末管理（MDM）	端末を一元的に監視・管理する機能。端末のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防ぐとともに、紛失・盗難等の際に遠隔でデータ消去を行い情報漏洩を防ぐ。
②- 4	アンチウイルス	コンピュータウイルスやマルウェア感染への対策。既知のパターンファイル（マルウェア情報）からのマルウェアの検知・駆除や、不審な挙動をするプログラムの検知（ふるまい検知）・駆除等を行う。
②- 5	データ暗号化	元データを変換し、第三者が簡単にデータの内容を解読できない状態にすること。アクセス権限が無い者の情報へのアクセスを制限する。
②- 6	不正なアクセスを検知・遮断する技術	不正な通信を検知し、アクセスを遮断する等の制御を行う。 ※不正なアクセスの検知（IDS）または遮断（IPS）による対策、エンドポイント対策（EDR 等）、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・防御する対策（WAF）、ネットワークとセキュリティを統合したクラウドサービスである SASE 等の活用が考えられる。

※これらはあくまでも、パブリッククラウド上で重要性分類Ⅱ以上の情報を取り扱う際に特に留意すべき要素技術を整理したものであり、これらの技術を網羅したからといって確実なセキュリティが確保されるというものではありません。

図表 16 強固なアクセス制御に関わる要素技術



（※１）学習系システムにおいて、児童生徒の情報がまとまったデータを扱う領域（学級/学年/学校に属する児童生徒全員の名簿や、学級/学年/学校に属する児童生徒全員の学習アプリの利用履歴等）。

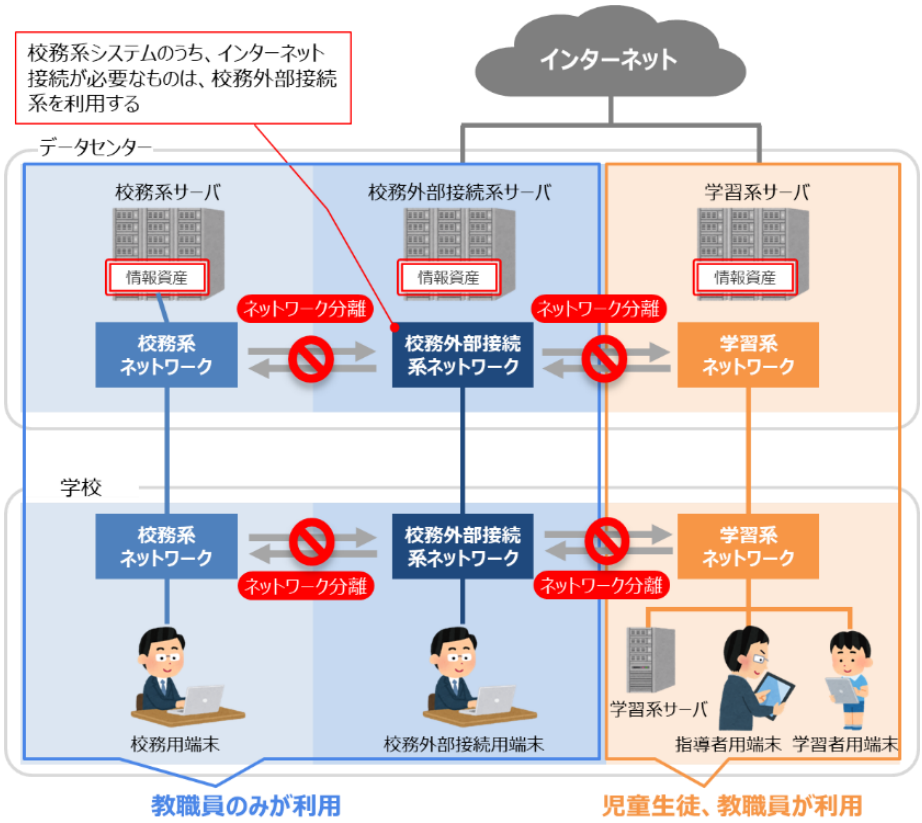
（※２）児童生徒本人またはその保護者が、当該児童生徒に関する重要性分類Ⅱ以上の情報資産のみにアクセスすることを想定したデータを扱う領域（健康診断票、通知表、定期考査・テスト等の採点結果等）。
多要素認証を設定することが望ましいものの、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際のロック機能の有効化、パスワードの複雑性の確保等により本人確認を厳格に行う前提で、ID及びパスワードでの認証を許容する。

（※３）特に重要性の高い情報については閲覧可能な場所を学校内等に限定することも考えられる。

図表 17 強固なアクセス制御による対策（イメージ図）

<ネットワーク分離による対策>

ネットワーク分離による対策とは、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の高い情報との論理的又は物理的な分離を行い、かつ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を講じるセキュリティ対策を指します。この対策を講じたシステム構成には「校務系ネットワーク」、「校務外部接続系ネットワーク」、「学習系ネットワーク」の３種類のネットワークが存在することから、ネットワーク分離による対策は、「三層の対策（三層分離）」とも呼ばれます。この対策を講じたシステム構成の場合、「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」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、無害化通信など適切な措置を講じる必要があります。



図表 18 ネットワーク分離による対策（イメージ図）

（特定用途機器のセキュリティ管理） ※第２編６.１.（９）

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についてもセキュリティ対策が必要です。機器の特性や業務上のリスクを勘案したうえで、機器の管理を明確にする、ネットワーク接続を適正化する、機器の ID 及びパスワード等について工場出荷時に設定されているものから変更し、機器のアクセス制御機能を有効にするなどの対策が考えられます。

（無線 LAN 及びネットワークの盗聴対策） ※第２編６.１.（10）

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ります。無線 LAN の不正利用調査を行い、探査ツール等を用いて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す。

● アクセス制御

（アクセス制御等） ※第２編６.２.（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、所管するネットワークまたは情報システムごとにアクセスする権限のない教職員等がアクセスできないように、システム上制限しなくてはなりません。

アクセス制御は、各情報資産の分類に応じて行うことが重要です。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す。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も必要になります。

（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） ※第２編６.２.（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、電子証明書による端末認証を利用するなどして、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する必要があります。

● 不正プログラム対策 ※第２編６．４．

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、不正プログラム対策ソフトウェアを導入するとともに、パターンファイルを常に最新の状態に更新することや、ソフトウェアのパッチの適用等を確実に実施することにより、不正プログラム対策を実施します。

・ Emotet（エモテット）

メールアカウントやメールデータなどの情報窃取に加え、さらに他のウイルスへの二次感染のために悪用されるウイルス。メールに添付される形で感染の拡大が試みられており、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ある。対策としては「組織内への注意喚起の実施」、「信頼できない Word 文書や Excel ファイルにおけるマクロの実行禁止」、「メールの監査ログの取得や SOC による常時監視」のほか、「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」等が挙げられる。

・ ランサムウェア

感染するとパソコン等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭や暗号資産）を要求する不正プログラム。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えいを迫る脅迫手法も確認されるようになった。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。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。

・ フィッシング

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。対策としては、「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」等が挙げられる。

・ 詐欺サイト（サポート詐欺、偽セキュリティ警告等）

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等の指示が行われる。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、対策としては「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」等が挙げられる。

図表 19 不正プログラム例

● 不正アクセス対策 ※第２編６．５．

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ことが考えられます。そのため、不正アクセスの防止又は被害を最小限にするために、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は、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ことが重要です。

● セキュリティ情報の収集 ※第２編６．６．

情報セキュリティを取り巻く社会環境や技術環境等は常に変化していることから、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をはじめとするセキュリティ情報を収集し、教職員等の関係者に共有するとともに、ソフトウェア更新等の対策を検討する必要があります。

不正プログラム等の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）等があります。

（７）運用

① 基本的な考え方 ※第２編 7.

組織的に情報セキュリティを確保するためには、ガイドラインにおいて規定されている各セキュリティ対策及び管理体系と併せて、適切な運用を行うことが必要です。例えば、ID 及びパスワード等の管理方法や、ポリシー違反に対する懲戒処分の規定等を定め、適切に運用できる環境を整備します。

ポリシーの策定の際には、教職員等による学校内外における教育 ICT 利活用や、児童生徒による１人１台端末及びクラウドの安心・安全な利活用を見据えて、各自治体・学校が実現したい環境と情報セキュリティのバランスに留意しつつ、運用規定を整備することが必要です。

② ガイドラインのポイント ※第２編７.

ガイドラインは、情報システムの監視に係る対策や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、ID 及びパスワードの管理、IC カード等の取扱い、教育情報セキュリティポリシーの遵守状況の確認・管理、懲戒処分等の運用に関する各規定を定めています。

● 情報システムの監視 ※第２編７.１.

外部からの攻撃又は侵入、教職員等の不正な利用、自らの情報システムが踏み台となり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、情報システムの監視等により稼動状況を常時監視することが必要です。ガイドラインでは、格納する情報資産の重要性に応じ、重要性分類Ⅱ以上の情報資産を格納するシステムへのアクセスについては常時監視を義務付け、重要性分類Ⅲの情報資産を格納するシステムは常時監視を推奨事項としています。

● 児童生徒における ID 及びパスワード等の管理 ※第２編 7.５.

（ID 登録・変更・削除） ※第２編 7.５.（１）

児童生徒の ID 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等の適切な措置を講じなければいけません。また、原則として進級/進学時に変更不要とすることが望ましいです。

（多要素認証等によるなりすまし対策） ※第２編 7.５.（２）

３－２（６）で述べたとおり、パブリッククラウド上で重要性分類Ⅱ以上の情報を取り扱う際には、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いけません。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しています。この際、教職員等から児童生徒へ適切な指導を行うことも必要です。詳細は、３－２（５）（児童生徒への指導）をご参照ください。

（８）外部委託

① 基本的な考え方 ※第２編８．

情報システムの外部委託を行う際は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ります。過去の契約書や仕様書の内容を踏襲して活用している教育現場の実態もあることから、契約書や仕様書の内容が最新の教育情報セキュリティポリシー等に準拠しているかを確認することも重要です。

② ガイドラインのポイント ※第２編８．

ガイドラインは、外部委託を行う際に情報セキュリティ確保上留意すべき事項を定めています。なお、IaaS[10]・PaaS[11]を利用したシステム構成に係るセキュリティ対策については本項を参照して下さい。

（外部委託事業者の選定基準） ※第２編８．（１）

教育情報システム管理者は、外部委託事業者を選定するに当たっては、技術的能力、信頼性等を考慮し、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する必要があります。事業者の情報セキュリティ水準を評価する際には、ISO/IEC27001 等の国際規格の認証取得状況等を参考にすることが望ましいです。

外部委託事業者の選定条件として仕様等に盛り込むべき内容（例）

・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

---

[10] 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。（出典：デジタル庁「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」１．４．用語 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/27e5d72f/20220930_resources_standard_guidelines_policy_01.pdf）

[11] 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。（出典：デジタル庁「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」１．４．用語 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/27e5d72f/20220930_resources_standard_guidelines_policy_01.pdf）

（契約項目） ※第２編８．（２）

教育情報システム管理者は、情報システムの運用、保守等を外部委託する場合には、外部委託事業者に起因する情報漏えい等の事案を防ぐために、委託事業者に委託する業務の内容に応じて明確にセキュリティ対策等の要件を規定し、契約等に定め、契約を締結する必要があります。

外部委託事業者に対しては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することも必要です。そのうえで、契約で遵守事項を定めるとともに、定期的に実施状況を監査することが必要です。

委託事業者との契約に規定すべき項目（例）

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
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
③提供されるサービスレベルの保証
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
⑤従業員に対する教育の実施
⑥提供された情報の目的外利用及び受託者以外の者への提供の禁止
⑦業務上知り得た情報の守秘義務
⑧再委託に関する制限事項の遵守
⑨委託業務終了時の情報資産の返還、廃棄等
⑩委託業務の定期報告及び緊急時報告義務
⑪地方公共団体による監査、検査
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
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）

（契約項目） ※第２編８．（３）

教育情報システム管理者は、外部委託事業者において契約に基づき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、必要に応じて改善要求等の措置をとる必要があります。確認した内容については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 にも報告を行う必要があります。

（９）SaaS 型パブリッククラウドサービスの利用

① 基本的な考え方 ※第２編９．、第１編第３章

SaaS[12]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必要があります。

GIGA スクール構想の下、SaaS 型パブリッククラウドサービスの利用が進んでいます。SaaS 型パブリッククラウドサービスは、利用者の個別要望に沿ったカスタマイズが原則困難であり、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くなります。SaaS 型パブリッククラウドサービスを利用する際には、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必要となります。

学習系サービス	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　等
校務系サービス	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

図表 20 教育現場で活用されている SaaS 型パブリッククラウドサービスの例

② ガイドラインのポイント ※第２編９．

ガイドラインは、SaaS 型パブリッククラウドサービスの利用においてクラウド利用者（教育委員会等）がクラウド事業者に確認・検証すべき情報セキュリティ対策やサービス提供に係るポリシーを定めるとともに、サービス利用における教職員等の留意点を定めています。また、SaaS 型パブリッククラウドサービスの中でも、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のない約款による外部サービスの利用の際の留意点についても定めています。

[12] 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。（出典：デジタル庁「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」１．４．用語 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/27e5d72f/20220930_resources_standard_guidelines_policy_01.pdf）

● 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 ※第２編９.１.

教育委員会等は、クラウドサービスを利用に当たってクラウド事業者が提供するクラウドサービスに必要十分な情報セキュリティ対策が講じられていることを確認する必要があります。

教育委員会等がクラウド事業者に対して適切な対応が行われているかを確認すべき内容（例）

（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）データの廃棄等
（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

● 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 ※第２編９.２.

教育委員会等は、クラウドサービスの利用に当たっては、クラウド事業者のサービス提供ポリシーや体制等が適切かどうか、確認・検証する必要があります。

教育委員会等がクラウド事業者に対して適切なポリシー、体制等が講じられているかを確認すべき事項（例）

（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等との合意事項
（10）その他留意事項

・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
・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
・クラウドサービスにおいて扱う情報や情報システム等の準拠法・裁判管轄
・個人情報の取扱いに関する事項

● 約款による外部サービスの利用 ※第２編９．４．

約款による外部サービスとは、インターネット上に提示された約款に同意することで提供されるサービスであり、SaaS 型パブリッククラウドサービスの一種です。代表的なサービスとして、電子メール・ファイルストレージ・グループウェアや生成 AI サービス等のクラウドサービス・ファイル転送サービスが挙げられます。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、教育委員会等はリスクを十分に踏まえて、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ります。

約款サービスを利用する場合の主なリスク

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、サービスが停止されたりする可能性がある。

（10）評価・見直し

① 基本的な考え方 ※第２編 10.

情報セキュリティの確保のため、教育現場におけるポリシーの履行状況等について適切な方法・適切な者による監査の実施、教育委員会・教職員等の自己点検の実施、教育情報セキュリティポリシーや実施手順等の関係規程等の見直しを行うことが重要です。

② ガイドラインのポイント ※第２編 10.

ガイドラインは、監査、自己点検、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定めています。

● 監査 ※第２編 10.１.

情報セキュリティ対策の実施状況について、定期的または随時、客観的に専門的見地から評価（＝監査）を行う必要があります。監査を行う者は、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、また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ものでなくてはいけません。

情報セキュリティ監査統括責任者は、監査を行う者の権限、監査項目・内容を定めて監査実施計画を立案します。監査を行う者は、この計画に基づいて監査を実施します。監査の結果については監査報告書として情報セキュリティ委員会に報告します。

監査結果は各主体の業務の見直しや、教育情報セキュリティポリシー等の見直しの基となる情報として活用しましょう。

● 自己点検 ※第２編 10.２.

情報セキュリティ対策の実施状況について、定期的または必要に応じて自己点検を行うことが必要です。自己点検は監査のような客観性はないものの、組織全体のセキュリティ対策の改善や、教職員等の情報セキュリティに関する意識向上にも有効です。自己点検は自己点検票を用いたアンケート方式等で行われることが多いですが、この内容はセキュリティ対策上担う役割に応じたものとすべきです。

情報セキュリティ委員会は自己点検結果の報告を受けて、組織全体における対策状況を把握し、各主体の業務の見直しや、教育情報セキュリティポリシー等の見直しの基となる情報として活用しましょう。

● 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 ※第２編 10.３.

情報セキュリティに関する脅威や技術等に必要な対策は変化することから、情報セキュリティ委員会は、セキュリティインシデント、監査、自己点検の結果を踏まえて教育情報セキュリティポリシーや関係規程の見直しを行います。見直しは定期的または大きな変化があったタイミングで実施するものであり、必要に応じてリスク分析の見直しを行うことも重要です。見直しを行った際には、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ります。

用語集

用語	解説
アクセス制御※1	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※1	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。
クラウドサービス※1	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。
サポート詐欺※2	悪意のある Web サイトを訪問した利用者に偽の警告画面を表示し、画面上に表示しているなりすましサポートセンターに電話をさせて金品をだまし取る詐欺をいう。
ソフトウェア※1	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。
パブリッククラウド※3	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。
フィッシング詐欺※2	実在の金融機関（銀行やクレジットカード会社）、ショッピングサイトなどを装った電子メールを送付し、これらのホームページとそっくりの偽のサイトに誘導して、住所、氏名、銀行口座番号、クレジットカード番号などの重要な情報を入力させて詐取する行為のことをいう。
モバイル端末※1	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※1	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※1	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。
可用性※1	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。
学習系サーバ※4	学習系情報を取り扱うサーバ
学習系システム※4	学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム及び、学習系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム

学習系情報※4	児童生徒のワークシート、作品など、学校が保有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ当該情報に教員及び児童生徒がアクセスすることが想定されている情報
学習者用端末※4	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
学習系ネットワーク	学習系情報を取り扱うネットワーク
完全性※1	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※1	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※1	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。
強固なアクセス制御※4	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・アクセス経路の監視・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・アクセス経路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。
教育情報システム※4	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
校務外部接続系サーバ※4	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
校務外部接続系システム※4	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
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
校務外部接続用端末※4	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
校務外部接続系ネットワーク	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ネットワーク
校務系サーバ※4	校務系情報を取り扱うサーバ
校務系システム※4	校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム及び、校務系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
校務系ネットワーク	校務系情報を取り扱うネットワーク

校務系情報※4	児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教員の個人情報など、学校が保有する情報資産のうち、それら情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報
校務用端末※4	校務系情報にアクセス可能な端末
識別※1	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※1	「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。
指導者用端末※4	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
情報セキュリティインシデント※1	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※1	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※1	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。
通信の暗号化※4	通信又は通信経路を暗号化し保護すること。
踏み台※1	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。
不正アクセス※2	利用する権限を与えられていないコンピュータに対して、不正に接続しようとすること。実際にそのコンピュータに侵入したり、利用したりすることを不正アクセスに含むこともあります。日本国内においても、インターネットに接続されたコンピュータに対する不正アクセスによる被害が急増したため、これらの行為を処罰する不正アクセス禁止法が施行されました。
不正プログラム※1	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。
CSIRT（Computer Security Incident Response Team）※1	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。
IaaS（Infra structure as a Service）※1	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）※1	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）※1	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。

※１　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

※２　総務省「国民のためのサイバーセキュリティサイト」より引用

※３　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

※４　ガイドライン「第３編（１）本ガイドラインにおける用語定義」より引用

参考リンク集

- 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）
  https://www.soumu.go.jp/main_content/000970701.pdf

- 総務省「国民のためのサイバーセキュリティサイト」
  https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/

- 内閣サイバーセキュリティセンター（NISC）「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）
  https://www.nisc.go.jp/pdf/policy/general/guider6.pdf

- 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）」（令和４年４月５日）
  https://www.nisc.go.jp/pdf/policy/infra/cloud_guidance.pdf

- デジタル庁「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」（令和４年９月 30 日）
  https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/27e5d72f/20220930_resources_standard_guidelines_policy_01.pdf

- IPA 独立行政法人 情報処理推進機構「制御システムのセキュリティリスク分析ガイド 第２版」(令和５年３月版)
  https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf

- 教育ネットワーク情報セキュリティ推進委員会（ISEN）「学校情報セキュリティお役立ち Web」
  https://school-security.jp/

- 一般社団法人 JPCERT コーディネーションセンターWeb サイト
  https://www.jpcert.or.jp/