東彼杵町教育情報セキュリティポリシー
第１版

適用期間　令和８年２月１日～令和８年８月３１日

第 1 編 総則

第1条 （目的）

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。本ポリシーは、東彼杵町立学校における教育情報システムについて、校務の効率化・児童生徒の学力向上を図ることを目的とした教育 DX の進展を踏まえ、その維持、管理及び活用における適切な情報セキュリティ対策等を総合的かつ体系的に定めるものである。

第 2 条（適用範囲）

1.本ポリシーは、東彼杵町教育委員会（以下「教育委員会」という。）及び東彼杵町立学校（以下「各学校」という。）に適用する。

2.本ポリシーは、前項に定める組織が保有又は管理する教育情報システム及び情報資産に適用する。

3.本ポリシーは、前項に定める教育情報システム及び情報資産を利用する次に掲げる者（以下「教職員等」という。）に適用する。

⑴ 東彼杵町教育委員会事務局職員

⑵ 各学校に勤務する教職員

⑶ ICT 支援員その他、教育委員会又は各学校の情報セキュリティ対策に関連する業務に従事する者

⑷各学校に所属する児童生徒、及びその保護者並びにその関係者

⑸ その他、教育委員会又は各学校が教育情報システム及び情報資産の利用を許可した者

学習者用 PC については、本ポリシーのほか、別途定める「学習者用 PC の校外持ち出しに関する規定」及びこれに基づく学校ごとのルールが適用される。

第 3 条（用語の定義）

本ポリシーにおいて使用する用語の意義は、次の各号に定めるところによる。

⑴ **職員用校務 PC（Dynabook ノートパソコン）**：各学校に勤務する教職員が校務のために使用する PC をいう。

⑵ **職員用指導用 PC（MicrosoftSurfacePro9）**：各学校に勤務する教職員が授業のために使用する PC をいう。

⑶ **電子黒板用 PC（Dynabook B55）**：普通教室・特別教室に設置する授業のために使用する PC をいう。

⑷ **学習者用 PC**：各学校に通学する児童生徒が学習のために使用する PC をいう。

⑸ **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をいう。

（6）**情報資産**：教育情報システムを構成するハードウェア、ソフトウェア、ネットワーク、電磁的記録媒体及びこれらに記録された情報並びにこれらの管理に関する文書をいう。
特に、児童生徒の個人情報を含む情報は重要性が高い情報資産である。
（7）**情報セキュリティインシデント**：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をいう。
（8）**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、利用者認証（多要素認証)、端末認証、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いう。
（9）**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。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、校務支援システム等）の利用を含む。
（10）**外部電磁的記録媒体**：USB メモリ、SD カード等の物理的な記録媒体をいう。
（11）**管理者**：各学校の ICT 機器等の管理責任者をいい、各学校の校長が務める。本ポリシーにおいては、主に教育情報セキュリティ管理者に相当する役割を担う。
（12）**ICT 担当者**：ICT 機器の技術的な助言、設定等の管理運営を担当する者をいい、管理者が指名する。
（13）**ICT 支援員**：教職員等が関わる ICT 機器等の運用について支援を行う外部人材をいう。
（14）その他、ガイドライン「教育情報セキュリティポリシーに関するガイドライン（文部科学省令和 7 年 3 月改訂版)」に定める用語の定義に準ずる。

第 2 編 教育情報セキュリティ対策基準

第 1 章 組織体制

第 4 条（組織体制及び責任）

1.東彼杵町教育委員会に、情報セキュリティ対策を統一的に行うための組織体制として、統括教育情報セキュリティ責任者(教育長)、統括教育情報システム管理者（教育次長)、統括教育情報システム担当者（学校教育係長）を置く。
2.各学校に、情報セキュリティ対策の責任者として教育情報セキュリティ管理者（校長）を置く。管理者は ICT 担当者を指名し、ICT 機器等の管理運営の一部を担当させる。
3.統括教育情報セキュリティ責任者は、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。
4.教育情報システム管理者は、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。また、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管理者へ速やかに報告し、指示を仰がなければならない。
5.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に関するコミュニケーションの核となる体制として、教育委員会に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）を構築する。学校で発生した情報セキュリティインシデントについても、教育委員会内の CSIRT と連携し対応するものとする。
6.教職員等は、教育情報セキュリティ管理者の指導の下、情報セキュリティポリシー及び関係規程を遵守しなければならない。
7.外部委託事業者（ICT 支援員を含む）は、委託契約に基づき、本ポリシー及び関係規程を遵守しなければならない。

第 2 章 情報資産の分類と管理

第 5 条（情報資産の分類）東彼杵町教育委員会及び各学校が取り扱う情報資産は、その重要性に応じて適切に分類し、それぞれの分類に応じた情報セキュリティ対策を講じるものとする。校務で利用するデータは、その内容に応じて、重要な個人情報を含むデータ等は本ポリシーに定める分類基準（別紙１（１）情報資産の分類）に従って分類する。重要な個人情報を含むデータ等、重要性が高いと分類された情報資産については、特に厳重な取扱いをしなければならない。

第 6 条（情報資産の管理）

1.教育情報セキュリティ管理者（校長）（以下管理者という）は、ICT 機器等管理台帳を整備しなければならない。管理台帳には、ICT 機器等の使用者、設定変更内容等を記録するものとする。
2.教職員等は、情報資産を記録した外部電磁的記録媒体（私物を含む）を、教育情報セキュリティ管理者の許可なく ICT 機器等に接続してはならない。やむを得ず校務にかかわる外部からのデータを取り込む必要がある場合で、管理者の許可を得た場合はこの限りではない。
3.重要な個人情報が含まれるデータは、原則として児童生徒の個人情報を管理するシステム（スズキ校務）に保存する。それ以外のデータについては、各学校設置の校務用サーバーのみに保持し、適切に処理しなければならない。個別の支援計画及び指導計画は同校務系サーバー及び東彼杵町役場設置の学校間共有フォルダへ同校務系サーバー内の職員フォルダに専用の保存先を作成して保存・管理する。
4.個人が特定されない画像や動画も、各学校校務系サーバーに保存・管理するものとする。容量に限りがあるため、個人写真以外の画像や動画等の保存は各学校にて修正案: 廃棄規定などを各学校にて策定し、保存するものとする。
5.児童生徒の個人情報を外部記憶装置に保存してはならない。
6.やむを得ず、職員用 PC 以外の PC 等で作成したデータをサーバーに複製する場合は、当該データについてウィルス検査を実施し、安全を確認しなくてはならない。
7.情報資産の保管については、教育情報セキュリティ管理者（校長）の定める保管先に従い、施錠可能な場所に保管するなど、適切な物理的・環境的対策を講じなければならない。特に重

要性分類Ⅲ以上の情報資産を記録した媒体は、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。
8.情報資産を外部へ送信する場合（電子メール、クラウドサービス等）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。重要性分類Ⅲ以上の情報を外部送信する場合は、限定されたアクセス（アクセス制限や暗号化）の措置を行わなければならない。
9.情報資産を記録した外部電磁的記録媒体を物理的に外部へ持ち出す場合は、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。
10.情報資産（Ⅰ・Ⅱ）の廃棄等を行う場合、情報資産分類に応じた適切なデータ消去方法（復元不可能な状態への消去を含む）を実施し、確認を行わなければならない。

第 3 章 物理的セキュリティ

第 7 条（ICT 機器等の物理的管理）

1.サーバー等の ICT 機器は、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の措置を講じなければならない。東彼杵町のセンターサーバーは東彼杵町役場サーバー室設置のものを指す。
2.ネットワークの基幹機器及び重要な情報システムは、サーバラック等に固定した上で施錠管理を実施するとともに、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。
3.管理区域（情報システム室等）への立入管理を適切に行わなければならない。入退室管理方法を定め、許可された者以外の立入りを制限し、記録を保持しなければならない。
4.フルクラウド化においては、センターサーバーやＮＡＳなどのストレージへのデータ保管は行わず、全て Microsoft365-A5 にて構築された SharePoint 上で管理を行うものとする。

第 4 章 技術的セキュリティ

第 8 条（職員用 PC 等の管理）

1. 職員用 PC 及び教職員等が使用するモバイル端末には、不正アクセス防止のため、ログイン時の ID パスワードによる認証を設定しなければならない。パスワードは厳重に管理すること。
2.ICT 機器等及びネットワークの管理者権限パスワードは管理者が厳重に管理し、利用については ICT 担当者のみとする。特権を付与された ID は必要最小限の者に限定し、ログ監視等のセキュリティ強化措置を講じなければならない。
3.職員用 PC には、マルウェア対策ソフトウェアを導入し、常に最新の状態に保たなければならない。不審なメールやファイルは開封・実行せず、速やかに削除すること。
4.職員用 PC を含む ICT 機器等には、教育委員会または管理者の許可なく外部のソフトウェアをインストールしてはならない。使用許諾契約等に違反しないことを確認しなければならな

い。
5.職員用 PC 等の設定変更(セキュリティ機能に関する設定変更、メモリ増設等の改造を含む)を行う場合は、校務に必要な場合のみとし、ICT 担当者及び管理者と協議し、教育委員会の許可を得なければならない。簡易的な設定変更(マウスの設定、デスクトップのカスタマイズ等)は校務に支障のない限り認めることとする。
6.職員用校務 PC は、原則校外へ持ち出してはならない。
7.職員用指導用 PC は、原則持出しを想定した配置とする。指導用 PC からは個人情報へのアクセスは出来ない設計とし、ログインするためには「顔認証」を必須とする。
教育関係団体等の研修、発表、PTA 等の各種事業に供する場合はこちらの端末を利用するものとする。
8.個人所有の PC を校内に持ち込んではならない。ただし、やむを得ない事情により管理者の許可を受ければ可能とするが、各学校ネットワークへの接続を行ってはならない。
9.教職員等は、職員用 PC、モバイル端末、外部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のないよう、離席時の PC 等のロック、容易に閲覧されない場所への保管等の適切な措置を講じなければならない。業務終了後と外出時には、電源を落とすものとする。
10.業務以外の目的でのウェブ閲覧は禁止する。

第 9 条（学習者用 PC 等の管理及び利用）

1.学習者用 PC には、不適切なウェブページの閲覧を防止するためのフィルタリングソフト等、及びマルウェア感染対策ソフトウェアを導入し、適切に運用しなければならない。
2.学習者用 PC のセキュリティ設定（OS アップデート、ブラウザアップデート、アプリケーションのインストール制限等）については、教育委員会または学校において一元管理を行うものとする。
3.学習者用 PC 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とし、教職員等は児童生徒に対してその旨を指導しなければならない。
4.教職員等は、児童生徒に対し、学習者用 PC 等の利用者認証情報（ID 及びパスワード）を他の人に知られないよう秘匿管理すること、ウィルスの感染が疑われる場合の報告義務等について指導を行わなければならない。
5.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を指導する。

第 10 条（クラウドサービスの利用）

1.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、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（準拠法、情報セキュリティポリシー、第三者認証取得状況（ISMAP

等)、責任分界点、監査体制、情報インシデント管理及び対応フロー、サービス提供水準(SLA)、再委託先管理等）を契約前に十分確認しなければならない。
2.クラウドサービスを利用する教職員等は、利用者認証情報（ID・パスワード）を適切に管理し、安易な「なりすまし」による不正アクセスを防止する対策を講じなければならない。
3.クラウドサービスを利用する教職員等は、取り扱う情報の重要性に応じ、データの暗号化や適切なアクセス制御設定等の対策を講じなければならない。
4.クラウドサービス上に保存した情報についても、本ポリシーの情報資産の分類、保管、外部持ち出し、廃棄等のルールを適用し、適切に管理しなければならない。情報の滅失、破壊等に備え、バックアップが適切に取得されていることを確認しなければならない。
5.クラウドサービス利用における情報セキュリティインシデント発生時は、速やかに管理者に報告しなければならない。クラウド事業者との間で、インシデント発生時の協力範囲や連絡体制を合意しておく必要がある。

第 11 条（ソーシャルメディアサービスの利用）

1.教育委員会または学校としてソーシャルメディアサービス（ブログ、SNS、動画共有サイト等）を情報発信等の目的で利用する場合、運用ポリシーや運用手順を定め、本ポリシー及び当該ポリシーに沿って適切に利用しなければならない。
2.教育委員会または学校として利用するソーシャルメディアサービスには、なりすまし対策（公式ウェブサイトからのリンク、アカウントページへの明記等）を講じなければならない。
3.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。
4.教職員等は、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（個人向けの Web サービス等、セキュリティの裏付けが確認できないもの)を取り扱ってはならない。
5. 各学校に所属する児童生徒、及びその保護者並びにその関係者におけるポリシーは別途定める。

第 11 条の 2 （外部電磁的記録媒体の管理）

1. **利用媒体の制限**
   教職員等は、教育委員会から支給された公的な外部電磁的記録媒体（ＵＳＢメモリ、ＳＤカード等）のみを校務に利用しなければならず、その他の媒体（私物を含む）の使用は禁止するものとする。
2. **接続及び持ち込みの制限**
   教職員等は、教育情報セキュリティ管理者（校長）の許可なく、外部電磁的記録媒体を ICT 機器等に接続してはならない。ただし、やむを得ず校務にかかわる外部からのデータを取り入れる必要があり、管理者の許可を受けた場合は、この限りではない。この場合、当該データについてウィルス検査を実施し、安全を確認しなくてはならない。また、持ち込み又は接続の記録を作成し、保管しなければならない。
3. **情報資産の保存制限**
   教職員等は、児童生徒の個人情報 および 重要性分類Ⅱ以上の情報資産を外部電磁的記録

媒体に保存してはならない。

4. **外部持ち出し時の安全管理措置**

(1)教職員等は、重要性分類Ⅲ以上の情報資産を外部電磁的記録媒体を用いて持ち出す場合（運搬を含む）は、教育情報セキュリティ管理者（校長）の許可を得なければならない。

(2)外部電磁的記録媒体を外部に持ち出す際は、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。特に、データ暗号化機能を備える媒体を使用し、暗号化機能を有効にすることを推奨する。

(3)持ち出しを行う際は、持ち出し及び持ち帰りの記録を作成し、管理しなければならない。

5. 保管及び廃棄

(1)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。

(2)外部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。

(3)外部電磁的記録媒体を廃棄又はリース返却等をする場合は、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。この処理は、重要性分類に応じて適切な方法により実施し、その記録を保管するものとする

第 5 章 運用

第 12 条（情報セキュリティに関する教育及び訓練）

1.教育委員会は、情報セキュリティの重要性を認識させ、本ポリシー及び関係規程を理解し実践させるため、全ての教職員等を対象とした情報セキュリティに関する教育及び訓練を定期的かつ計画的に実施しなければならない。毎年度最低 1 回は研修を受講するように努めるものとする。

2.学校は情報セキュリティの点検を毎年度実施するものとする。

3.学校は毎年度、情報セキュリティ点検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、研修計画を作成し継続的に更新するものとする。

4.研修の内容は、教職員等の役割、情報セキュリティに関する理解度等に応じたものとし、校内研修、合同研修（長期休業期間等を利用した事例発表等）、転入職員研修等を実施する。

5.各学校での ICT 活用実践事例については、町内ネットワーク等（校務支援ソフト「ミライム」や「Teams」）をとおして、積極的に紹介し合い、情報共有及び活用促進を図るものとする。

6.教職員等は、定められた情報セキュリティに関する教育及び訓練に積極的に参加しなければならない。

7.児童生徒に対しても情報セキュリティに関する教育及び訓練を行うものとする。

第 13 条（情報セキュリティインシデント発生時の対応）

1.情報セキュリティインシデント（ウィルス感染、データ漏えい等）が発生した場合、又はそのおそれがある場合、発生を発見した者は、速やかに管理者に報告しなければならない。
2.報告を受けた管理者は、速やかに教育委員会へ報告し、指示を仰がなければならない。
3.教育委員会は、情報セキュリティインシデントの発生に備え、緊急時対応計画を策定するものとする。緊急時対応計画には、発生事案の報告手順、被害拡大防止、復旧、証拠保全、再発防止策等の実施に関する事項を定める。
4.情報セキュリティインシデントが発生した場合、緊急時対応計画に基づき、被害の拡大防止、復旧等の対応を行うものとする。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・関係機関と緊密に連携するものとする。
5.管理者は、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関係規程の改善を含め、再発防止策を策定し、教育委員会へ報告するものとする。

第 14 条（外部委託におけるセキュリティ確保）

1.情報システムの開発、運用、保守等の業務を外部委託する場合、教育情報セキュリティ対策が十分に講じられている外部委託事業者を選定しなければならない。
2.外部委託事業者との契約においては、守秘義務、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、再委託に関する制限、委託業務終了時の情報資産の返還・廃棄、委託業務の定期報告及び緊急時報告義務、教育委員会による監査・検査、情報セキュリティインシデント発生時の公表、本ポリシーが遵守されなかった場合の規定（損害賠償等）等、情報セキュリティ確保に必要な事項を明確に定めなければならない。
3.教育委員会は、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、必要に応じて契約に基づき措置を求めなければならない。確認が困難な場合は、第三者監査や国際的なセキュリティ認証（ISO/IEC27001 等）の取得等によって確認することも可能とする。
4.教育委員会は、外部委託事業者に対し、本ポリシー等のうち外部委託事業者が遵守すべき内容及びその機密事項について説明し、遵守を求めなければならない。再委託を行う場合も同様とする。

第 6 章 評価・見直し

第 15 条（評価）

1.教育委員会は、自らの管理する範囲における情報セキュリティ対策の実施状況について、定期的に自己点検を実施しなければならない。
2.当初の目的を達成するために、利用者（教職員等及び児童生徒）に対して ICT 活用等の検証及び各種調査を行う。

第 16 条（見直し）教育委員会は自己点検及び学校での点検の結果、情報セキュリティインシデントの発生状況、情報を取り巻く環境の変化（情報通信技術の進展、新たな脅威の出現、関係法令等の改正等）及び ICT 活用の検証結果を踏まえ、本ポリシー及び関係規程等を定期的に

見直し、必要な改定を行わなければならない。定期的に ICT 担当者会議等を行い、学校間の情報共有と活用の検証及び今後の事業実施計画等について検討するものとする。

第 7 章　違反時の対応

第 17 条（違反時の対応）

1.教職員等が本ポリシー又は関係規程に違反した場合、管理者は、当該教職員等に対し、その情報資産の使用を停止又は制限することができる。

2.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教育委員会に通知し、適切な措置を求めなければならない。

3.管理者の指導によっても改善されない場合、教育委員会は、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、教育委員会は、当該教職員等の権利を停止あるいは剥奪した旨を当該教職員等が所属する学校の管理者に通知しなければならない。

4.本ポリシー又は関係規程に違反した教職員等については、その内容に応じて、就業規則等に基づき処分されることがある。

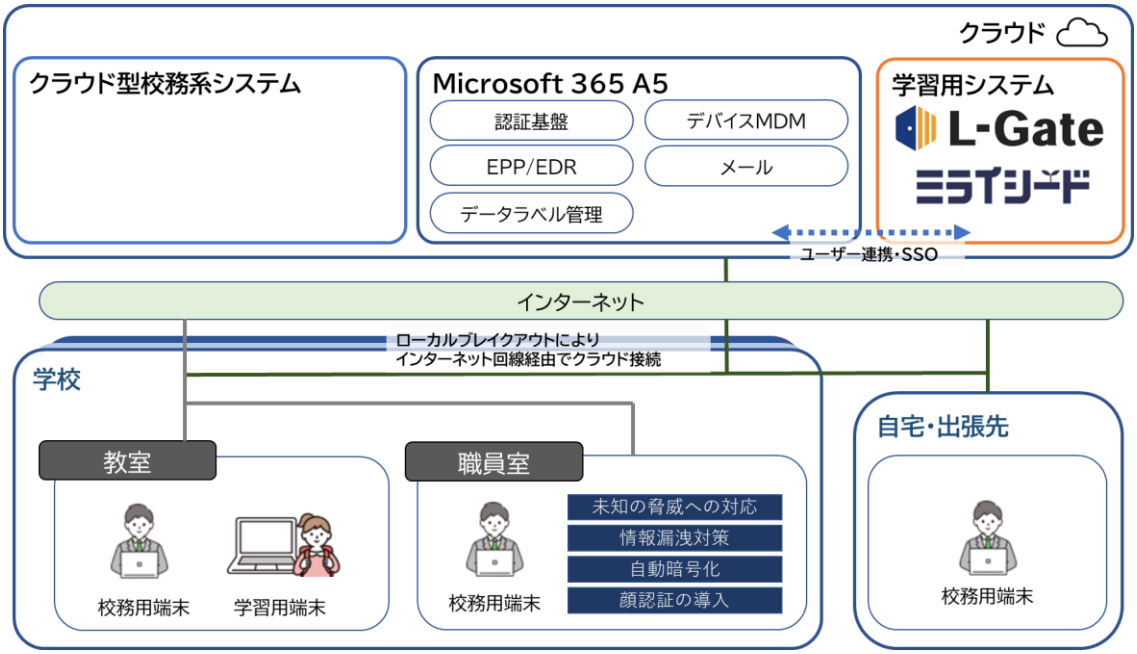

図 1　次期東彼杵町クラウドシステム接続図（想定）

第 8 章　生成 AI の利用に関する規定

第 1 条（目的）

本規定は、児童生徒の資質･能力の育成及び校務の効率化･質の向上を図ることを目的として、生成 AI の適切な利用に関する基本的な考え方、留意事項、及び関係者の役割を定めるものとする。

第 2 条（定義）

本規定において、次の各号に掲げる用語の定義は、当該各号の定めるところによる。

(1) 生成 AI：文章、画像、プログラム等を生成できる AI モデルに基づく AI の総称をいう。

(2) ハルシネーション：生成 AI が誤った出力をすることをいう。

(3) バイアス：生成 AI の学習データや入力するプロンプト、連携する外部サービス等によって生じる、特定の個人や集団への不当で有害な偏見及び差別をいう。

(4) プロンプト：生成 AI に対して入力される指示文をいう。

(5) 重要性の高い情報：児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教員の個人情報など、学校が保有する情報資産のうち、機密性、完全性、可用性の観点からセキュリティ侵害が重大な影響を及ぼす情報をいう。 重要性分類 I 及び II。

(6) 個人情報：生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの等をいう。

第 3 条（基本的な考え方）

生成 AI の利用に際しては、次の各号に掲げる基本的な考え方を遵守するものとする。

(1) 人間中心の原則の堅持：生成 AI は、人間の能力を補助・拡張し、可能性を広げる有用な道具として捉えるものとする。生成 AI の出力はあくまで「参考の一つ」であり、「最適解とは限らない」ことを認識し、利用するものとする。

(2) 生成 AI の利活用は、学習指導要領が目指す資質・能力の育成に寄与するかを吟味した上で検討されるべきであり、生成 AI の利用自体が目的であってはならないものとする。

(3) 生成 AI が社会の中で果たす役割や影響、関連する法・制度、マナー等について科学的な理解を促し、情報モラルを含む情報活用能力の育成を一層充実させることを目指すものとする。

第 4 条（学校現場における共通の留意事項）

学校現場で生成 AI を利活用する際には、次の各号に掲げる観点を共通して遵守するものとする。

(1) 安全性及び適正利用の確保

ア．関係法令を遵守し、生成 AI サービスの提供者が定める最新の利用規約（年齢制限、保護者の同意の必要性、生成物のライセンスなど）を確認し、遵守するものとする。

イ．教職員は、教育委員会の方針に基づき教育委員会が定めた利用規約を管理者に提出し利活用する。その際管理者の許可を得ていない私用アカウント又は私用端末を用いてはならないも

のとする。
上記規定に加え、重要性分類 II 以上の情報資産へのアクセスは、教育委員会又は学校が利用を許可した端末からのみ行うものとし、私用端末からのアクセスは原則禁止する。
ウ．児童生徒への利活用においては、利用規約や提供条件（年齢制限、保護者の同意など）を教師が確認し、必要に応じて事前に保護者の理解を十分に得た上で、教師の適切な指導監督の下で利活用させるものとする。
(2) 情報セキュリティの確保
ア. 文部科学省が策定する「教育情報セキュリティポリシーに関するガイドライン」を参考に、教育委員会は学校現場の実態に即した教育情報セキュリティポリシー等を策定・見直し、学校現場はこれを遵守するものとする。
イ．原則として、プロンプトに重要性の高い情報（成績情報、個人情報など）を入力してはならないものとする。ただし、個別契約等に基づき適切なセキュリティ対策が講じられた環境で生成 AI を運用している場合、及び生成 AI サービス側で機械学習を許容しない設定（エンタープライズデータ保護）が可能な場合はこの限りではない。
(3) 個人情報の取扱いに関して必要かつ適切な措置を講じるものとする。特に、個人情報を含むプロンプトを入力する際は、提供者が当該個人情報を機械学習に利用するか否か等を十分に確認するものとする。利用される場合は個人情報保護法違反となり得ることに留意するものとする。生成物に既存の著作物との「類似性」及び「依拠性」がないか留意するものとする。学校の授業の過程における利用であれば著作権法第 35 条の範囲内で許諾なく利用可能であるが、授業目的の範囲を超えて利用する場合（例：学校のホームページ掲載、外部のコンテストへの応募など）は著作権侵害となる可能性があるため注意するものとする。
(4) 生成 AI のハルシネーション（誤った出力）やバイアス（偏り）の存在を認識し、その出力結果を鵜呑みにせず、教職員が最終的な判断を行うものとする。児童生徒に対しても、バイアスの存在を理解させ、常に慎重に判断し、正確性・事実関係の確認を行うよう指導するものとする。
（5）透明性の確保及び説明責任
ア.生成 AI サービスの利用目的、リスク等の必要な情報を整理し、関係者（教職員、児童生徒、保護者等）への情報提供を行うものとする。
イ．児童生徒が生成 AI の出力を引用する際は、生成 AI を用いたことを明記するなど、出典・引用のルール（利用したツール名、入力したプロンプト、日付など）を設定し、指導するものとする。
ウ．保護者に対しても、生成 AI の不適切な利活用が行われないよう、目的やリスクを含めて周知し、理解を得るものとする。

第 5 条（教職員の利用に関する特則）

教職員が校務において生成 AI を利活用する際には、前条の規定に加えて、次の各号に掲げる事項を遵守するものとする。

(1) 生成 AI は、授業準備、各種文書のたたき台作成を含む校務において利活用することで、校務の効率化や質の向上、教職員の働き方改革につなげていくことを目的とするものとする。
(2) 生成された内容の適切性を判断できる範囲内で利用するものとし、生成 AI から一度で求める出力がなされることを期待せず、複数回の対話の中で求める出力に近づけていくとともに、生成 AI の出力はあくまでも参考の一つであることを認識し、教職員自らがチェックし推敲・完成させるなど、最終的な判断と責任を負うものとする。
(3) 個別契約等に基づき適切なセキュリティ対策が講じられた環境で生成 AI を運用している場合を除き、プロンプトに重要性の高い情報である成績情報等を入力してはならないものとする。
(4) 生成 AI による出力結果の利用については、サービス提供事業者の利用規約等に付されている条件を遵守するものとする。
(5) 学校の管理職は、生成 AI の運用状況を把握し、適切な利活用がなされているかを適時確認するものとする。

第 6 条（児童生徒の学習活動における利用に関する特則）

児童生徒が学習活動において生成 AI を利活用する際には、第 4 条の規定に加えて、次の各号に掲げる事項を遵守するものとする。
(1) 生成 AI は、学習指導要領に示す資質・能力の育成につながり、教育活動の目的を達成する観点から効果的である場合に限り利活用するものとする。
(2) 教師は、児童生徒の発達の段階や情報活用能力の育成状況に十分留意し、適切な指導監督の下で生成 AI を利活用させるものとする。特に小学校段階の児童が直接利活用することについては、より慎重な見極めが必要となる。
(3) プロンプトに氏名や写真等の個人情報を入力させないよう留意するものとする。
(4) 各種コンクールへの応募作品やレポート・小論文等について、生成 AI による生成物をほぼそのまま自己の成果物として応募・提出する行為は、不適切又は不正な行為に当たり得るため、教師はこれらについて十分に指導するものとする。
(5) 生成 AI の出力を引用する際は、利用した生成 AI サービスの名称、入力したプロンプト、生成 AI を用いた日付を明記するものとする。
(6) 保護者に対して、生成 AI の利活用目的やその態様等の情報を提供するとともに、児童生徒が学校外で生成 AI を利活用する可能性も踏まえ、生成 AI の不適切な利活用が行われないよう周知し、理解を得るものとする。

第 7 条（教育委員会の役割）

教育委員会は、生成 AI の適切な利活用を推進するため、次の各号に掲げる事項を考慮するものとする。
(1) 柔軟な対応方針：域内の各学校の実態を十分に踏まえ、一律に禁止したり、義務付けたりするような硬直的な運用は行わないものとする。
(2) 環境整備及び研修機会の提供

ア．フィルタリングの設定やログの収集等、学校の実態に即した適切な対策を講じるものとする。
イ．個人情報や重要性の高い情報を適切に取り扱える利用環境（既存の校務系システムと同程度のセキュリティ対策）の構築・運用を検討するものとする。
ウ．教職員の AI リテラシー向上と適切な利活用を促すための研修機会を提供し、先行事例や教材・ノウハウの周知・共有を積極的に行うものとする。
(3) サービス選定及び経済的負担への配慮：約款に基づく外部サービスを利用する際は、その約款や契約内容が適切であるかを十分に確認するものとする。また、将来的な価格変動リスクやサービス停止のリスクを考慮し、保護者の経済的な負担に十分に配慮したサービスを選択するものとする。

別紙１

（１）情報資産の分類

東彼杵町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）

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。