西脇市立学校情報セキュリティ基本方針

令和８年３月

西脇市教育委員会

西脇市立学校情報セキュリティ基本方針

―目次―

1　目的・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・1
2　適用範囲・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・1
3　定義・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・1
4　対象とする脅威・・・・・・・・・・・・・・・・・・・・・・・・・・・・・2
5　教職員等の遵守義務・・・・・・・・・・・・・・・・・・・・・・・・・・・2
6　情報セキュリティ対策・・・・・・・・・・・・・・・・・・・・・・・・・・2
7　情報セキュリティ監査及び自己点検の実施・・・・・・・・・・・・・・・・3
8　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・・・・・・・・・・3
9　教育情報セキュリティ対策基準の策定・・・・・・・・・・・・・・・・・・3
10　教育情報セキュリティ実施手順の策定・・・・・・・・・・・・・・・・・・4

1　目的

本基本方針は、西脇市教育委員会（以下「教育委員会」という。）及び西脇市立学校（以下「学校」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、教育委員会が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

本基本方針は、「西脇市情報セキュリティ基本方針」を準用しつつ、学校に特有の教育情報環境に対応するため、個別に定めるものとする。

2　適用範囲

本基本方針は、教育委員会及び学校における情報資産の取扱い全般に適用する。

なお、本基本方針が対象とする情報資産は、次のとおりとする。

⑴　教育ネットワーク、教育情報システム及びこれらに関する設備、電磁的記録媒体

⑵　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。）

⑶　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　定義

⑴　ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

⑵　教育ネットワーク

学校で利用しているネットワークのことをいう。

⑶　情報システム

コンピュータやネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

⑷　教育情報システム

学校で利用している情報システムのことをいう。

⑸　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

⑹　機密性

情報資産にアクセスすることを認められた者だけが、情報資産にアクセスできる状態を確保することをいう。

⑺　完全性

情報資産が破壊、改ざん又は消去されていない状態を確保する

ことをいう。

⑻　可用性

情報資産にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

⑼　教育情報セキュリティポリシー

教育情報セキュリティ基本方針及び教育情報セキュリティ対策基準をいう。

4　対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。

⑴　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

⑵　情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による教育情報資産の漏えい・破壊・消去等

⑶　地震、落雷、火災等の災害によるサービス及び業務の停止等

⑷　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

⑸　電力供給の途絶、通信の途絶等のインフラの障害からの波及等

5　教職員等の遵守義務

教職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって教育情報セキュリティポリシーを遵守しなければならない。

6　情報セキュリティ対策

上記4の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

⑴　組織体制

情報セキュリティ対策を推進するため、教育委員会及び学校における責任者、管理者、実施者を明確にした組織体制を確立する。

⑵　情報資産の分類と管理

学校の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

⑶　物理的セキュリティ

通信回線及び教職員等のパソコン等の管理について、物理的な対策を講じる。

⑷　人的セキュリティ

情報セキュリティに関し、教職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

⑸　技術的セキュリティ

コンピュータ等の管理、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対策を講じる。

⑹　運用

情報システムの監視、教育情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、教育情報セキュリティポリシーの運用面の対策を講じるものとする。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等に迅速かつ適正に対応するため、緊急時連絡体制の確立、手順・判断基準の策定等を行い、事案発生時に混乱なく対処できるよう準備する。

⑺　業務委託と外部サービス（クラウドサービス含む。）の利用

業務委託を行う場合には、選定された受託事業者と情報セキュリティ要件を明記した契約を締結し、受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確認し、必要に応じて契約に基づき措置を講じる。

7　情報セキュリティ監査及び自己点検の実施

教育情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8　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

教育委員会及び学校は、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踏まえ、教育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見直しを行うとともに、重大な変化が発生した場合にも評価を行い、必要があると認めた場合は見直すものとする。

9　教育情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める教育情報セキュリティ対策基準を策定する。なお、教育情報セキュリティ対策基準は、情報セキュリティ上の観点から、内容を公開することにより本市の教育情報システムの安全性を損なうおそれがあるため、非公開とする。

10　教育情報セキュリティ実施手順の策定

対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた教育情報セキュリティ実施手順を策定するものとする。なお、教育情報セキュリティ実施手順は、教育情報セキュリティ対策基準と同様に非公開とする。