徳島県教育委員会情報セキュリティ基本方針

目次

1. 目的

この基本方針は、徳島県教育委員会（以下、教育委員会という。）の保有する情報資産について、情報セキュリティ対策の基本的な事項を定め、もって情報資産の機密性の保持並びに完全性及び可用性の維持を確保することを目的とする。なお、この基本方針は、教育委員会における地方自治法（昭和 22 年法律第 67 号）第 244 条の 6 に定めるサイバーセキュリティを確保するための方針とする。

2. 適用範囲

(1) この基本方針は、教育委員会事務局及び教育委員会が所管する県立学校、徳島県立総合教育センター等（以下、教育委員会事務局等という。）における情報資産の取扱いについて適用する。

(2) この基本方針が対象とする情報資産は、次のとおりとする。

・業務で取り扱う文書及びデジタルデータ
・情報システム及びこれらに関する施設及び設備
・情報システムで取り扱う情報及びソフトウェア（これらを印刷した文書を含む。）
・情報システムの仕様書及びネットワーク論理構成図等のシステム関連文書

(3) 紙媒体の情報資産については、情報セキュリティポリシーによるもののほか、徳島県教育委員会公文書管理規則、徳島県教育委員会文書規程その他の教育委員会の公文書の管理等に関する規則等の定めるところによる。

3. 用語の定義

(1) **情報セキュリティ** 情報資産の機密性を保持し、情報の完全性及び可用性を維持することをいう。

(2) **機密性** 情報にアクセスすることが認可された者だけがアクセスできる状態を確保することをいう。

(3) **完全性** 情報が破壊、改ざん又は消去されていない正しい状態を確保することをいう。

(4) **可用性** 許可された利用者が、必要なときに情報にアクセスできる状態を確保することをいう。

(5) **重要性分類** 情報資産を機密性、完全性及び可用性の 3 つの観点から影響度を評価したものをいう。

(6) **情報システム** コンピュータ（サーバ、パソコン等）、ネットワーク、電磁的記録媒体及びそれを制御するソフトウェア並びにその運用体制などで構成され、情報処理を行う仕組みをいう。

(7) **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及びその構成機器（ハードウエア及びソフトウエア）をいう。

(8) **校務系** 徳島県教育情報ネットワーク（以下、教育情報ネットワークという。）校務系

に接続された情報システム及びその情報システムで取り扱うデータをいう。

(9) **学習系** ホームページ管理システム、教育クラウドサービス等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(10) **無害化通信** コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された、校務系と学習系を繋ぐ通信をいう。

(11) **情報セキュリティポリシー** 本基本方針及び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、以下の脅威を想定し、情報セキュリティ対策を実施する。

(1) 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

(2) 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、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情報資産の漏えい・破壊・消去等

(3) 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

(4) 大規模・広範囲にわたる疾病によるサービス及び業務の停止等

(5) 電力供給の途絶、通信の途絶、水道供給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、期限付講師・非常勤講師等の会計年度任用職員（以下「教職員等」という。）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情報セキュリティポリシー及び情報セキュリティ実施手順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。

(1) 組織体制

各所属の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

(2) 情報資産の分類と管理

情報資産を重要性分類で分類し、当該分類に基づき、情報セキュリティ対策を実施する。

(3) 情報システム全体の強靱性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の対策を講じる。

ア　校務系と学習系の通信環境を分離する。なお、両システム間で通信する場合には無害化通信を実施する。

イ　学習系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

(4) 物理的セキュリティ

サーバを含む情報システム、通信回線、及び教育情報ネットワークに接続を認めたパソコン等の管理について、物理的な対策を講じる。

(5) 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、十分な研修及び啓発を行う等の人的な対策を講じる。

(6) 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。

(7) 運用

情報システムの監視、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、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、緊急時対応計画を策定する。

(8) 業務委託

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

(9) クラウドサービス・ソーシャルメディアサービスの利用

クラウドサービスを利用する場合には、利用に係る規定を整備し、対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、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る。

(10) 評価・見直し

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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

7. 情報セキュリティ監査及び自己点検の実施

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. 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するために新たに対策が必要となった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

9. 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情報セキュリティ対策基準を策定する。なお、情報セキュリティ対策基準は、公にすることにより教育委員会の情報セキュリティの維持に支障を及ぼすおそれがあることから非公開とする。

10. 情報セキュリティポリシー実施手順の策定

情報セキュリティ対策基準に基づき、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情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティポリシー実施手順は、公にすることにより教育委員会の情報セキュリティの維持に支障を及ぼすおそれがあることから非公開とする。

附則

この基本方針は、令和８年３月２７日から施行する。ただし、第１条の規定中、地方自治法（昭和 22 年法律第 67 号）第 244 条の６に定めるサイバーセキュリティを確保するための方針に関する部分は、令和８年４月１日から施行する。