水戸市学校情報セキュリティポリシー

水戸市学校情報セキュリティ基本方針

１　目的

本基本方針は，水戸市教育委員会及び水戸市立小学校・中学校及び義務教育学校（以下「市立学校」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，本市教育委員会及び市立学校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。

２　定義

(1) 教育ネットワーク

本市の学校教育において使用する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。

(2) 教育情報システム

本市の学校教育において使用するコンピュータ，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。

(3) 情報資産

教育ネットワーク及び教育情報システムで取扱う全ての情報をいう。

(4) 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。

(5) 水戸市学校情報セキュリティポリシー

本基本方針及び水戸市学校情報セキュリティ対策基準をいう。

(6) 機密性

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

(7) 完全性

情報が破壊，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。

(8) 可用性

情報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。

(9) 校務系

教職員が接続し，校務に関わる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) 校務外部接続系

校務系のうち，インターネットメール（茨城県教育情報ネットワーク等），ホームペ

ージ管理システム等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扱うデータをいう。

(11) 学習系

教職員及び児童生徒が接続し，授業や学習活動を通して取り扱う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。

３　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，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・外部監査機能の不備，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要員不足に伴うシステム運用の機能不全等

(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

４　適用範囲

(1) 行政機関の範囲

本基本方針が適用される行政機関は，水戸市教育委員会及び市立学校とする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は，次のとおりとする。

ア　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及び電磁的記録媒体

イ　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。）

ウ　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

５　教職員等の遵守義務

教職員，非常勤及び臨時の教職員等は，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水戸市学校情報セキュリティポリシー及び水戸市学校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３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

本市教育委員会及び市立学校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

本市教育委員会及び市立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。

(3) ネットワーク分離によるセキュリティ対策

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，教育情報ネットワークに対し，以下の対策を講じる。

ア　校務系と学習系は，原則として，ほかの領域との通信をできないよう物理分離し，校務系の機密情報の流出を防ぐ。

イ　校務系においては，校務機密系と校務外部接続系との通信経路を論理分離する。

(4) 物理的セキュリティ

サーバ，総合教育研究所コンピュータ室，学校コンピュータ室，通信回線及びコンピュータ等の管理について，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，十分な教育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

教育情報システムの監視，水戸市学校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，水戸市学校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) 業務委託と外部サービスの利用

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。

外部サービスを利用する場合には，利用にかか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。

(9) 評価・見直し

水戸市学校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。水戸市学校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　水戸市学校情報セキュリティ対策基準の策定

上記６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水戸市学校情報セキュリティ対策基準を策定する。

８　水戸市学校情報セキュリティ実施手順の策定

水戸市学校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水戸市学校情報セキュリティ実施手順を学校ごとに策定するものとする。

なお，水戸市学校情報セキュリティ実施手順は，公にすることにより市教育委員会及び市立学校の運営に重大な支障を及ぼすおそれがあることから非公開とする。