

稲美町 教育情報セキュリティ基本方針

稲美町教育委員会

令和元年 10 月策定 令和 8 年 4 月改定

目 次

教育情報セキュリティの基本方針

1	目 的	2
2	定 義	2
3	教育情報セキュリティポリシーの位置付けと教職員等の義務	3
4	教育情報セキュリティ管理体制	3
5	教育情報資産の分類	3
6	教育情報資産への脅威	3
7	教育情報セキュリティ対策	4
8	教育情報セキュリティ対策基準の策定	4
9	教育情報セキュリティ監査の実施	4
10	評価及び見直しの実施	4

教育情報セキュリティの基本方針

1 目 的

小中学校が取り扱う情報には、児童生徒の個人情報のみならず、保護者、教職員、その他地域住民に関する情報等、学校運営に欠かせない重要な情報が数多く含まれており、外部へ情報漏えい等が発生した場合には、極めて重大な結果を招くおそれがある。

したがって、本町の教育情報ネットワークにおいて、個人情報をはじめと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、漏えい、改ざん、コンピュータウイルスによるシステム障害、災害や事故等の様々な脅威から防御することは、保護者や地域住民等から信頼される安心・安全な学校づくりに必要不可欠である。

こうしたことから、町立小中学校における情報セキュリティ対策を総合的、体系的かつ具体的に整備することを目的に、稲美町教育情報セキュリティポリシー（以下「セキュリティポリシー」という。）を定める。

このうち基本方針は、各小中学校が所管する教育情報資産についても、本町全体の基本方針と共通のものであるとの認識のもと、稲美町情報セキュリティ基本方針を準用する。

2 定 義

(1) 教育情報ネットワーク

学校教育において使用する校内ネットワーク及び外部と接続する通信網をいう。

(2) 教育情報システム

本町の学校教育において使用されるサーバ及び端末（ネットワーク、ハードウェア及びソフトウェア）並びに記録媒体等で構成され、情報処理を行う仕組みをいう。

(3) 教育情報資産

対象とする情報資産は、次のとおりとする。

ア 教育情報ネットワーク及び教育情報システム並びにこれらに関する設備及び電磁的記録媒体

イ 教育情報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

(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) 教職員

学校教育法（昭和 22 年法律第 26 号）第 37 条及び第 49 条に規定する者で、稲美町が設置する小中学校に従事する職員をいう。

3 教育情報セキュリティポリシーの位置付けと教職員等の義務

セキュリティポリシーは、本町が所管する教育情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、教育情報セキュリティ対策の頂点に位置する基本的方針である。

したがって、本町の全ての教職員、教育情報資産に係る業務に携わる教育委員会事務局の職員、指定管理者及び外部委託業者に属する者（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、セキュリティポリシーを遵守しなければならない。

4 教育情報セキュリティ管理体制

本町の教育情報資産について、情報セキュリティ対策を推進し、管理するための体制を確立する。

5 教育情報資産の分類

教育情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を実施する。

6 教育情報資産への脅威

セキュリティポリシーを策定する上で、教育情報資産に対する脅威の発生の可能性及び発生した場合の影響を考慮し、特に認識すべき脅威は、次のとおりである。

- (1) 部外者の侵入、盗難及び故意の不正アクセス又は不正操作による機器若しくは情報資産の破壊、盗聴、改ざん、消去等
- (2) 教職員等による機器若しくは情報資産の持出し若しくは誤操作、認証情報若しくはパスワードの不適切な管理、故意の不正アクセス若しくは不正行為による破壊、盗聴、改ざん、消去等、搬送中の事故等による機器又は情報資産の盗難並びに規定外の端末接続によるデータ漏えい等
- (3) コンピュータウイルス、地震、落雷、火災等の災害、事故又は故障等によるサービス及び業務の停止
- (4) 大規模又は広範囲にわたる疾病の発生による要員不足に伴うシステム運用の機能不全等
- (5) 電力供給又は通信の途絶等のインフラ障害による業務の停止等

7 教育情報セキュリティ対策

6で示した脅威から教育情報資産を保護するため、次の情報セキュリティ対策を講じる。

(1) 物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷及び妨害等から保護するための物理的対策

(2) 人的セキュリティ対策

情報セキュリティに関する権限及び責任を定め、教職員等にセキュリティポリシーの内容を周知徹底するための十分な教育及び啓発

(3) 技術及び運用におけるセキュリティ対策

教育情報資産を外部からの不正なアクセス等から適切に保護するための情報資産へのアクセス制御、ネットワーク管理等の技術的対策、システム開発等の外部委託及びクラウドサービスの利用に係る対策、ネットワークの監視、セキュリティポリシーの遵守状況の確認等の運用面の対策並びに、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策

8 教育情報セキュリティ対策基準の策定

本町の様々な教育情報資産について、7の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。このため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した教育情報セキュリティ対策基準を策定する。

9 教育情報セキュリティ監査の実施

セキュリティポリシーが遵守されていることを検証するため、定期的又は必要に応じて監査及び自己点検を実施する。

10 評価及び見直しの実施

教育情報セキュリティ監査及び自己点検の結果等により、セキュリティポリシー及び情報セキュリティ対策の評価を行うとともに、情報セキュリティを取り巻く状況の変化に対応するため、必要に応じてセキュリティポリシーの見直しを行う。