令和８年４月１日改定

岡崎市立小中学校情報セキュリティポリシー

序　岡崎市立小中学校情報セキュリティポリシーの構成

岡崎市立小中学校情報セキュリティポリシー（以下、情報セキュリティポリシー）とは、本市立小中学校が保有する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る。

本情報セキュリティポリシーは、本市立小中学校が所掌する情報資産に関わる業務に携わる教職員（臨時的任用教職員、市任期付任用教員、会計年度任用職員等を含む）及び外部委託者に周知、普及、定着させるものであり、安定的な規範であることが要請される。一方において、情報通信技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、本情報セキュリティポリシーを、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システムごとの具体的な情報セキュリティ対策の実施手順として「情報セキュリティ運用規則」を策定することとする。（下表参照）

＜情報セキュリティポリシーの構成＞

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全ての情報資産に共通の情報セキュリティ対策の基準
情報セキュリティ運用規則		情報セキュリティ対策基準に基づいた具体的な運用規則

第１章　　情報セキュリティ基本方針

地方自治法（昭和 22 年法律第 67 号）第 244 条の６第１項に規定するサイバーセキュリティを確保するための方針として、情報セキュリティ基本方針を定める。

１　目的

本情報セキュリティ基本方針は、本市立小中学校が保有する情報資産を様々な脅威から防御し、その機密性（注）を確保するため、組織的かつ計画的に取り組むための統一的な方針であり、情報セキュリティを実践するにあたっての基本的な考え方及び方策を定め、本市立小中学校の情報資産や機密等を守り、業務を継続的に安全に行うことで市民からの信頼の維持向上に寄与することを目的とする。

（注）：国際標準化機構（ＩＳＯ）が定めるもの（ｌＳＯ７４９８‐２：１９８９）

機密性(confidentiality)：認可された者だけが情報にアクセスできることを確実にすること。

２　用語の定義

（１）情報資産…本市立小中学校及びその関連施設において取り扱われる全ての情報をいう。その中に、情報システムの開発と運用に係る全ての情報並びに情報システムにより取り扱われる全ての情報を含む。情報資産には、紙媒体などの物理的情報資産と電子的情報資産がある。

①物理的情報資産…文字や写真、図などが紙等に印刷されたり、書かれたりしたもの。
②電子的情報資産…電子情報が記録されたもの。ＣＤやＤＶＤ、ＢＤなどの光学ディスク、ＵＳＢメモリやＨＤＤ、ＳＤカード等の記憶媒体、各種クラウドサービス等。

（2）情報システム…情報資産を取り扱うサーバ、情報端末、ソフトウェア、ネットワーク等で構成された情報の処理に用いる仕組みをいう。

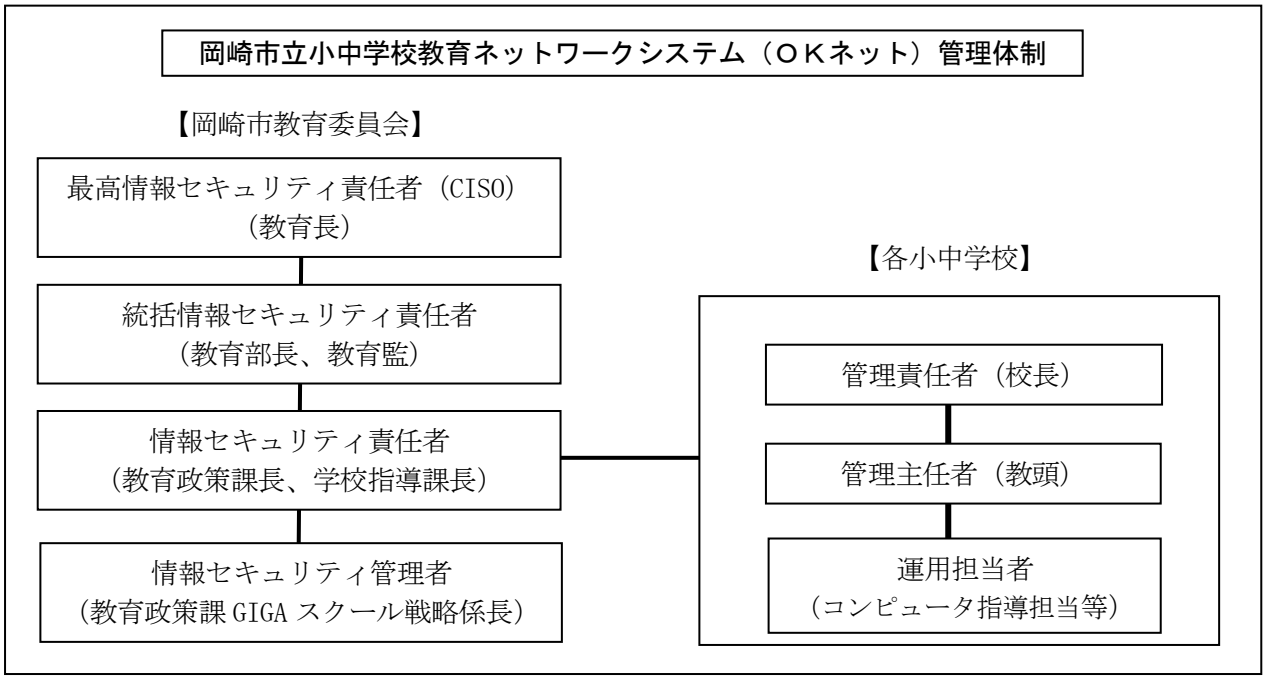
（3）ネットワーク…コンピュータを相互に接続するための通信網及びその構成機器をいう。

3　教職員の義務

本市立小中学校が所掌する情報資産に関わる業務に携わる教職員及び外部委託者は、情報セキュリティの重要性について共通の認識をもつとともに、業務の遂行に当たって本情報セキュリティポリシーを遵守する義務を負う。

4　管理体制

情報資産の統一的な情報セキュリティを確保するための管理体制を下図のように整備する。



5　情報資産の管理

情報資産については、「情報セキュリティ対策基準」と「情報セキュリティ運用規則」の規定に基づき、適切な管理を行う。

6　情報資産への脅威

情報資産に対する脅威の発生度合や発生した場合の影響を考慮して情報セキュリティ対策を講じるものとする。特に認識すべき脅威は以下のとおりである。

・権限のない者による、電子的情報資産に対する故意の不正アクセス又は不正操作によるデータやプログラムの持出、盗難、改ざん、消去、漏洩、損傷、及び機器や記憶媒体の盗難等。
・権限のない者による、物理的情報資産の不正な閲覧、持出、盗難、改ざん、破棄、紛失等。
・教職員及び外部委託者による、電子的情報資産に対する意図しない操作、故意の不正アクセス又は不正操作によるデータ及びプログラムの持出、盗難、改ざん、消去、漏洩、損傷、及び機器や記憶媒体の盗難、紛失等。
・教職員及び外部委託者による、物理的な情報資産に対する不正な閲覧、持出、盗難、改ざん、

破棄、紛失等。
・地震、落雷、火災、停電、猛暑等による災害や事故、故障、障害等。

7　情報セキュリティ対策

本市立小中学校の所掌する情報資産を「6　情報資産への脅威」から保護するため以下の対策を講ずるものとする。

（1）人的セキュリティ対策

情報セキュリティに関する権限や責任及び遵守すべき事項を定め、教職員に対する周知徹底を図るため、継続的に研修及び啓発を行う。

（2）物理的セキュリティ対策

情報資産を保管する施設への不正な立入り、情報資産への損傷及び利用の妨害等から保護するために物理的な対策を講ずる。

（3）技術的セキュリティ対策

情報資産を不正アクセス等から保護するため、情報資産へのアクセス制御やネットワーク管理及び暗号化処理等の技術的な対策を講ずる。

（4）運用におけるセキュリティ対策

情報資産の運用状況の監視及び情報セキュリティ対策の遵守状況の確認等の対策を実施する。また、緊急事態において迅速な対応を可能とするための対策を講ずる。

（5）情報セキュリティ対策基準の策定

情報セキュリティ基本方針に基づき、情報セキュリティ対策を実施するに当たって必要となる基本的な要件を明記した情報セキュリティ対策基準を定める。

（6）情報セキュリティ運用規則の策定

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具体的に実施するために、情報セキュリティ運用規則を定める。

（7）情報セキュリティ監査の実施

情報セキュリティ対策が遵守されていることを検証するため、定期的に監査を実施する。

（8）評価及び見直しの実施

情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価、情報システムの変更、新たな脅威等の情報セキュリティを取り巻く状況の変化を踏まえ、適宜情報セキュリティポリシー及び情報セキュリティ対策基準、情報セキュリティ運用規則の見直しを行う。