泉南市

学校情報セキュリティポリシー

Ver. 2

令和 7（2025）年 11 月

泉南市教育委員会

目次

更新履歴

令和 2 (2020)年 11 月	Ver1	セキュリティポリシー策定
令和 7 (2025)年 11 月	Ver 2	セキュリティポリシー策定

はじめに

情報セキュリティとは

　市民サービス向上に向けて、市民の個人情報を含む、学校園で保持している様々な情報資産を保護すること。

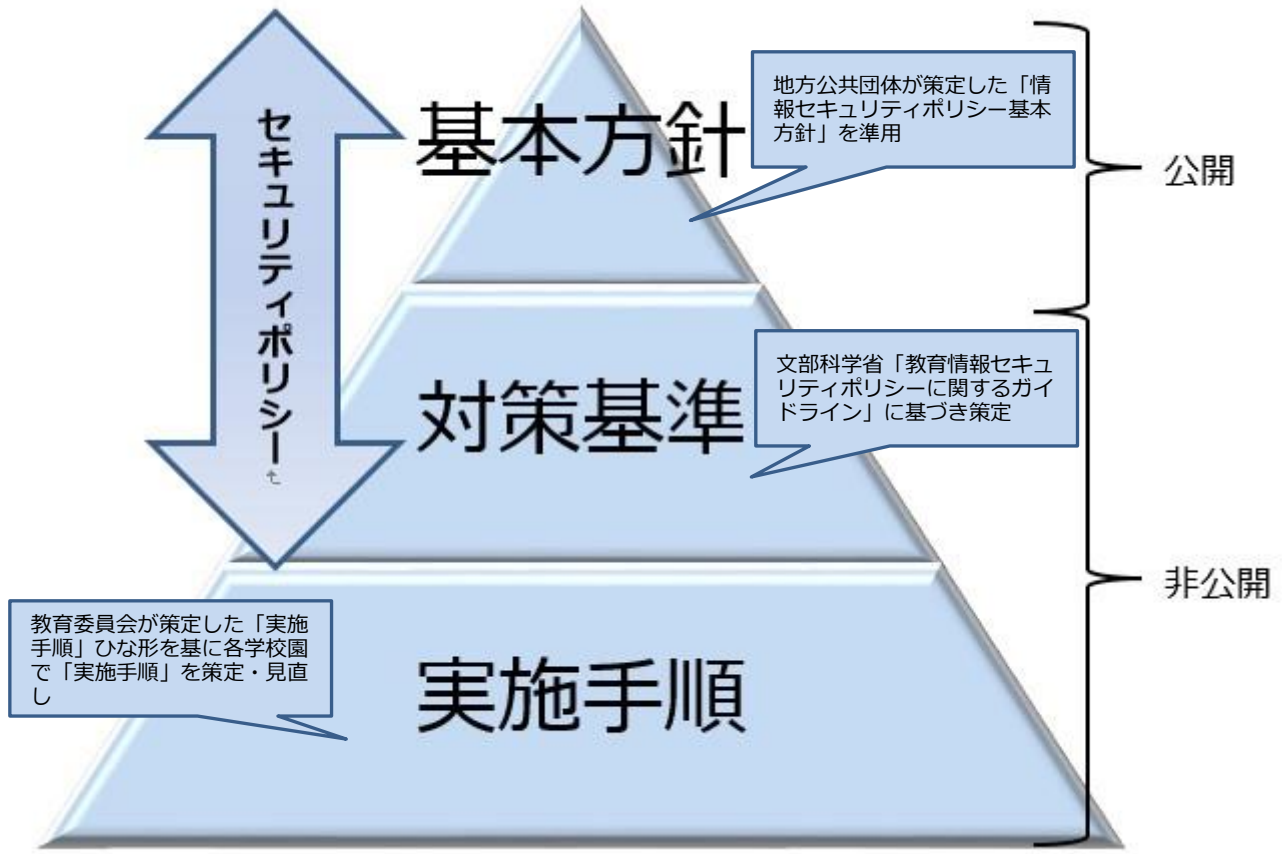
　そのためには、①機密性、②完全性、③可用性を維持する必要がある。

セキュリティポリシーの構成

　セキュリティポリシーは、情報セキュリティ対策に関する基本的な考え方をまとめた「基本方針」と、この基本方針に基づき、全ての学校に共通の情報セキュリティ対策の基準を定める「対策基準」から構成される。「基本方針」については、地方自治体が策定したものを準用するとされる。

　さらに、対策基準を実際のシステムに当てはめ、個別の実施事項など具体的な内容を定めた「実施手順」については、教育委員会が策定したひな形を基に各学校で策定・見直しをすることが求められる。

図 1 セキュリティポリシーの構成



第 1 章　学校情報セキュリティ基本方針

1. 目的

泉南市立小学校、中学校、義務教育学校及び幼稚園*[1]（以下、「学校」という。）の児童生徒をはじめ、その保護者、校長、教職員等、学校に関わる全ての者の財産、プライバシー等を保護し学校の安定的な運営を図ることを目的とし、泉南市学校情報セキュリティポリシー（以下、「本ポリシー」という。）を策定する。

2. 位置づけ

本ポリシーは、学校の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にかかる情報セキュリティ対策を総合的、体系的かつ具体的に取りまとめたものであり、学校における情報セキュリティ対策を実施するうえで基礎となるものである。

3. 用語の定義

本ポリシーにて使用する用語の定義は、以下のとおりとする。

表 1 用語の定義

用語	定義
ネットワーク	コンピューター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。
情報	職員等が作成し又は取得した電磁的記録及び紙等の有体物に出力された記録をいう。
情報システム	コンピューター、ネットワーク及び電磁的記録媒体で構成され、処理を行う仕組みをいう。
情報資産	ネットワーク及び情報システムそのもの又はこれらで取り扱う情報をいう。なおそれらを紙等に出力した文書を含む。
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。
情報セキュリティポリシー	組織が所管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、本基本方針及び情報セキュリティ対策基準をいう。
管理区域	ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の保管並びに運用を行うための部屋や記録媒体の保管庫をいう。
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。
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。
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。

[1]* 市立幼稚園は市教育委員会事務局と同様に、従前から市が定める泉南市情報セキュリティポリシー摘要対象となっているが、本ポリシー策定のきっかけとなった JET プログラム導入に伴い、市立幼稚園も学校同様に情報連携していく必要があるため、本ポリシーの適用対象に新たに加えることとした。

校務系情報	学校が保有する情報資産のうち、それらの情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報をいう。
校務外部接続系情報	校務系情報のうち、保護者メールや学校ホームページ等の外部とインターネット接続を前提とした校務で利用される情報をいう。
学習系情報	学校が保有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ、当該情報に教職員及び児童生徒がアクセスすることが想定されている情報をいう。
サーバ	ネットワーク上で学校情報を処理し、端末に提供するコンピュータをいう。
端末機	ネットワークを通じてサーバに接続されたパソコンやモバイル端末（タブレット等）機器をいう。
校務用端末	校務系情報全てにアクセス可能な端末をいう。
学習者用端末	学習系情報にアクセス可能な端末で、児童生徒が利用する端末をいう。
指導者用端末	学習系情報にアクセス可能な端末で、教職員のみが利用可能な端末をいう。
教育情報システム	情報資産を扱うハードウェア、ソフトウェア、クラウドサービス等をいう。
情報セキュリティインシデント	情報セキュリティに関する問題としてとらえられる事象（障害、事件、事故、欠陥、攻撃、侵害等）をいう。
記録媒体	情報システムでデータ等を記録するための媒体（メディア）。サーバ、端末機、デジタルカメラ、デジタルビデオカメラ、通信回線装置等に内蔵される内臓電磁的記録媒体と、外付けハードディスク、ＣＤ－ＲＯＭ、ＤＶＤ－Ｒ、ＵＳＢメモリ、ＳＤカード等の外部電磁的記録媒体をいう。
スマートデバイス	情報処理端末（デバイス）のうち、スマートフォンやタブレット等、携行可能な多機能端末をいう。
情報資産	ネットワーク及び情報システムそのもの又はこれらで取り扱う学校情報をいう。なおそれらを紙等に出力した文書を含む。
無線ＬＡＮ	電波等を利用してデータの送受信を行う構内通信網システムをいう。
クラウドサービス	学校外、庁舎外でプログラムやデータベースを管理し、インターネットなどのコンピューターネットワークを経由し、情報システム等の利用をサービスの形で提供される利用形態
ソーシャルメディアサービス	インターネット上における、ホームページ、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等をいう。
生成 AI	広く、「文書、画像、プログラム等を生成できる AI モデルに基づく AI」の総称をいう。

4. 対象範囲

(1)組織の範囲

学校の内部のすべての組織及びクラウドサービスを利用・管理する教育委員会。さらに、委託契約により学校の業務を受託し情報資産を取り扱う外部事業者等及びクラウドサービス提供事業者を含む。ただし、市立幼稚園で使用している泉南市行政 LAN システムは、泉南市情報セキュリティポリシーの対象範囲に属するため、これを除く。

(2)人的範囲

上に掲げる学校の情報資産に関する業務に携わる全ての職員（非常勤、臨時職員を含む）及び受託事業者等職員に準じる者（以下、「職員等」という。）

(3)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。

①ネットワーク及び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

②ネットワーク及び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。）

③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. 本ポリシー及び関連法令等の順守

(1)職員等の責務

① 職員等は、情報セキュリティの重要性を認識し、業務の遂行に当たっては本ポリシーを順守する義務を負う。また、情報資産の利用や保管等を行う際は、泉南市個人情報保護条例（平成 19 年条例第 3 号）など関連する法規等を順守しなければならない。

② 本ポリシーに違反した職員等は、生じた結果の重大性及び違反の悪質性等の状況に応じて、地方公務員法等に基づき懲戒処分等の対象になることがある。

(2)外部事業者への対応

学校は、業務を委託する外部事業者・団体等に対しても情報セキュリティの重要性を認識させるため、契約書等において本ポリシーへの順守事項及び違反した場合の責任等についても明確にするものとする。

(3)児童生徒への対応

学校は、児童生徒に対しても、情報モラル教育の観点から情報セキュリティの重要性を認知させる等、指導、監督するものとする。

(4)クラウドサービスの利用

クラウドサービスを利用・管理する学校及び教育委員会は、クラウドサービスの特性に起因する留意点を踏まえ、本ポリシーに基づきクラウドサービスを利用する上での安全性の確保に努めるものとする。

6. 情報資産に対する脅威

（１）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

(2)職員等は、上記(1)の脅威に対し認識を深めるとともに、これら以外の脅威についても注意を払わなければならない。

7. 運用体制

情報セキュリティ対策の推進及び「６．情報資産に対する脅威」に掲げる脅威等が生じた事態（以下、「セキュリティ侵害」という。）に対する迅速な対応を図るための運用体制を確立するものとする。

8. 情報資産の分類

情報資産の機密性、完全性及び可用性を内容に応じて分類し、その重要度に応じた対策を講じるものとする。

9. 教育情報セキュリティ対策

情報資産を脅威から保護するために、以下の情報セキュリティ対策を講じるものとする。

(1) 管理体制

情報資産を管理し、機密性、完全性及び可用性を維持するための体制を確立する。

(2) 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。

(3) 物理的セキュリティ

サーバ、情報システム室、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。

(4) 人的セキュリティ

教育情報セキュリティに関する権限や責任、教職員等が遵守すべき事項を定めるとともに、このポリシーを周知徹底させるための教育及び啓発を行う等の人的な対策を講じる。

(5) 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。

(6) 運用

情報システムの監視、このポリシーの遵守状況の確認、外部委託を行う際のセキュリティの確保等、この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切に対応するため、緊急的対応計画を策定する。

(7) 外部サービスの利用

外部委託する場合には、外部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、外部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。

約款による外部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、利用できるソーシャルメディアごとの責任者を定める。

(8) 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、情報ネットワークに対し、ゼロトラスト対策セキュリティもしくは以下の対策を講じる。

①校務系情報ネットワークと学習系情報ネットワークは、原則として、通信をできないよう物理分離する。

②校務系情報においては、外部接続との通信経路を論理分離する。

(9) 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。

10. 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。

11. 情報セキュリティポリシーの評価・見直し

情報セキュリティ監査及び自己点検の結果等により運用改善を行い、情報セキュリティの向上を図るとともに、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。

12. 情報セキュリティ対策基準の策定

「9. 対策」で示した対策を講じるにあたって、職員等が順守すべき事項や判断の基準等を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を実施する上で必要となる一定の基準を示した情報セキュリティ対策基準を策定するものとする。

13. 情報セキュリティ実施手順の策定

各学校が情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する具体的な対策の方法や手順を定めておく必要がある。そのため、情報セキュリティ対策基準に基づく実施マニュアル（手引き）として、情報セキュリティ実施手順のひな形を策定し、各学校はこのひな形を基に「実施手順」を策定することが求められる。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、具体的な対策の手順やノウハウ（技術的知識・情報）について記述するものであり、公開することにより学校運営に重大な支障を及ぼす恐れがあるため、非公開とする。

14. クラウドサービスの利用に関する考え方

GIGA スクール構想の進展に伴い、クラウドサービスの活用とその促進が求められている。実際にパブリッククラウドの利用においては、効率性の向上、セキュリティ水準の向上、技術革新対応力の向上、柔軟性の向上、可用性・完全性の効率的確保及び保守運用稼働の削減など、その適切な導入、利用は、本市学校及び教育委員会の ICT 施策上のメリットとしてあげられる。

ついては、学校及び教育委員会において、クラウドコンピューティング、中でもパブリッククラウドを利用可能とするために、以下を規定する。

(1)クラウドサービスの特性に起因する留意点

① クラウドサービスは、システムを複数の利用者が共用するため、特定の利用者が他の利用者に影響を与えないよう、適切な安全管理措置が行われていることの確認に努めること。

② クラウドサービスは、そのセキュリティの確認においては、利用者が詳細に調査することは困難なため、第三者による認証や各サービス事業者が提供している監査報告書を利用して確認に努めること。

③ クラウドサービスでは、クラウド事業者とクラウドサービス利用者責任分界点をあいまいにすることが無いよう、それぞれの役割分担・責任分界点を明確にするよう務めること。

④ クラウドサービスの性格上、事業者によってサービスが停止される可能性もあるため、利用停止に係る規定等をあらかじめ確認しておくこと。

(2)クラウドサービスにおける安全性の確保

① クラウドサービスに求められる情報セキュリティ対策

クラウド事業者が講じている情報セキュリティ対策を、クラウド利用者が確認する形で安全性の担保に務めること。

なお、クラウドサービス利用者は、サービス利用の際に必要な情報セキュリティ対策を実施すること。

②クラウド事業者のサービス提供ポリシー等の確認

クラウドサービス利用における安全性担保のためには、サービス提供ポリシーが、クラウドサービス利用者が求める情報セキュリティ対策に適合するかについて確認に務めること。

15. セキュリティ対策の点検と本ポリシーの見直し

日々の情報セキュリティに対する脅威に対応するため、本ポリシーに定める事項及び実施手順に基づく具体的対策の実施状況を定期的に点検する。

　また、本ポリシーの内容についても必要に応じて見直し、学校におけるセキュリティレベルの向上を図るものとする。