

綾瀬市教育委員会及び綾瀬市立小・中学校情報セキュリティ基本方針

(目的)

第1条 綾瀬市教育委員会及び綾瀬市立小・中学校における情報セキュリティ基本方針（以下「基本方針」という。）は、綾瀬市教育委員会、綾瀬市立小学校及び中学校（以下「教育委員会及び学校」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、教育委員会及び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。

(用語の定義)

第2条 この基本方針の用語は次のとおりとする。

- (1) 情報とは、教育委員会及び学校が保有する電子情報をいう。
- (2) 情報資産とは、情報及び情報システムをいう。
- (3) ネットワークとは、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
- (4) 情報システムとは、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。
- (5) 情報セキュリティとは、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。
- (6) 教育情報セキュリティポリシーとは、情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。
- (7) 機密性とは、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。
- (8) 完全性とは、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。
- (9) 可用性とは、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。

(対象とする脅威)

第3条 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な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

(適用範囲)

第4条 本基本方針を適用する組織及び情報資産の範囲は、次のとおりとする。

- (1) 教育委員会及び学校が保有する情報資産、情報資産に関する業務に携わる教職員を始めとする全ての者（以下、「利用者」という。）に適用する。
- (2) 本基本方針が対象とする情報資産は、次のとおりとする。なお、教育委員会が管理している情報システムにのみ適用し、綾瀬市が管理している情報システムは適用対象外とする。

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

(利用者の義務)

第5条 利用者は、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教育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。

(情報セキュリティ管理体制)

第6条 教育委員会及び学校は、情報セキュリティ対策を推進するための組

織体制を確立するものとする。

(情報資産の分類)

第7条 教育委員会及び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。

(物理的セキュリティ対策)

第8条 情報システムの設置場所、情報保管場所、通信回線及び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。

(人的セキュリティ対策)

第9条 教育委員会及び学校は、利用者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

(技術的セキュリティ対策)

第10条 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。

(運用等における対策)

第11条 情報システムの監視及び教育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、教育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切な対応が可能となるような危機管理対策を講ずる。

(業務委託と外部サービス(クラウドサービス)の利用)

第12条 業務委託及び外部サービス(クラウドサービス)等を利用する場合には、次の規定に準拠するものとする。

- (1) 業務委託を行う場合には、委託事業者を選定し、仕様書等において、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。
- (2) 外部サービス(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。
- (3) 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。

(情報セキュリティの評価・点検)

第13条 教育委員会は、教育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。教育情報セキュリティポリシーの見直しが必要な場合は、適宜教育情報セキュリティポリシーの見直しを行う。

(情報セキュリティ対策基準)

第14条 教育委員会は、第5条から前条まで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（以下「対策基準」という。）を定めるものとする。

(情報セキュリティ実施手順)

第15条 学校は、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（以下「実施手順」という。）を策定するものとする。

(情報セキュリティ対策違反への対応)

第16条 教育委員会は、情報セキュリティ対策に違反したものに対して必要な措置を講ずる。

(教育情報セキュリティポリシーの公開)

第17条 情報セキュリティ基本方針は公開とするが、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、公にすることにより教育委員会及び学校の運営、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。

(法令遵守)

第18条 情報セキュリティ対策を実施するに当たっては、法令等を遵守しなければならない。

附 則

この基本方針は、平成20年9月1日から実施する。

附 則

この基本方針は、令和3年4月30日から実施する。

附 則

この基本方針は、令和8年4月1日から実施する。