中京大学附属中京高等学校教育情報セキュリティポリシー

2022年9月15日制定

2023年2月2日改正

教育情報セキュリティポリシーの構成

教育情報セキュリティポリシーは、学校が所有する情報資産の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。

教育情報セキュリティポリシーは、以下の3つの階層に分けて策定、管理するものとし、教育情報セキュリティ基本方針、教育情報セキュリティ対策基準及び教育情報セキュリティ実施手順から構成される。

1. 教育情報セキュリティ基本方針

情報セキュリティ対策における基本的な考え方を定めるもの。

2. 教育情報セキュリティ対策基準

教育情報セキュリティ基本方針に基づき、全ての情報システムで遵守すべき対策の基準。

3. 教育情報セキュリティ実施手順

教育情報セキュリティ対策基準に基づき、実施手順を作成するためのガイドライン

教育情報セキュリティ基本方針

1. 目的

この基本方針は、学校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. 方針

前条の目的を達するため、情報セキュリティ対策基準（以下「対策基準」という。）その他の規程等の定めるところにより、以下の対策を行う。

- (1) 情報セキュリティ対策の実施体制の整備
- (2) 情報及び情報システムの保護
- (3) 情報システム及び情報サービスの管理・運用
- (4) インシデントへの対処
- (5) 利用者への啓発・教育
- (6) (1)～(5)を含む情報セキュリティマネジメントの実施

3. 責務

本校の情報並びに本校で扱う情報システムを利用する者及び管理・運用の業務に携わる者は、この方針、対策基準、その他関係規程等を遵守しなければならない。

4. 罰則

この方針に基づき定められる規程等に違反した場合の利用の制限お及び罰則は、学則及び本校が定める就業規則にのっとり行うほか、それぞれの規程に定めるところによる。

教育情報セキュリティ対策基準

1. 情報資産の範囲

この対策基準の対象となる情報資産は、次のとおりとする。

- (1) 教育ネットワーク、教育情報システム、教育ネットワーク及び教育情報システムに関する施設・設備、電磁的記録媒体
- (2) 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。）
- (3) 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

情報資産の種類	情報資産の例
教育ネットワーク	情報資産を扱う通信回線、ルータ等の通信機器
教育情報システム	情報資産を扱うサーバ、パソコン、モバイル端末、汎用機、オペレーティングシステム、ソフトウェア、クラウドサービス等
これらに関する施設・設備	情報資産を扱うコンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル
電磁的記録媒体	情報資産を扱うサーバ装置、端末、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蔵電磁的記録媒体と、USBメモリ、外付けハードディスクドライブ、DVD-R、磁気テープ、SDカード等の外部電磁的記録媒体
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	教育ネットワーク、教育情報システムで取り扱うデータ（これらを印刷した文書を含む。）
教育情報システム関連文書	教育情報システム関連のシステム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図、クラウドサービス契約関連文書等

2. 用語の定義

用語	定義
校務系情報	児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教員の個人情報等の、学校が保有する情報資産のうち、それら情報を学校及び学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定されている、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
校務外部接続系情報（公開系情報）	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
学習系情報	児童生徒のワークシート、作品等の学校が保有する情報資産のうち、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
校務用端末	校務系情報にアクセス可能な端末
校務外部接続用端末	校務外部接続系情報にアクセス可能な端末

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
指導者用端末	学習系情報にアクセス可能な端末であり、かつ、教員のみが利用可能である端末
校務系システム	校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム、校務系情報を扱う上で適切なアクセス権が設定された領域で利用されるシステム
校務外部接続系システム	校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ（CMS）及び校務外部接続用端末等から構成される校務外部接続系情報を取り扱うシステム
学習系システム	学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム及び、学習系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
教育情報システム	校務系システム、校務外部接続系システム及び学習系システムを合わせた総称
校務系サーバ	校務系情報を取り扱うサーバ
校務外部接続系サーバ	校務外部接続系情報を取り扱うサーバ
学習系サーバ	学習系情報を取り扱うサーバ

3. 情報資産の分類

情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じて取扱制限を行うものとする。

(1) 機密性による分類

分類	分類基準	該当する情報資産のイメージ
機密性 3	学校で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	特定の教職員のみが知り得る状態を確保する必要がある情報で秘密文書に相当するもの
機密性 2B	学校で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	教職員のみが知り得る状態を確保する必要がある情報資産（教職員のうち特定の教職員のみが知り得る状態を確保する必要があるものを含む）
機密性 2A	学校で取り扱う情報資産のうち、直ちに一般に公表することを前提としていないが、児童生徒がアクセスすることを想定している情報資産	教職員及び児童生徒同士のみが知り得る状態を確保する必要がある情報資産（教職員及び児童生徒のうち特定の教職員及び児童生徒のみが知り得る状態を確保する必要があるものを含む）
機密性 1	機密性3、機密性2B 又は機密性2A に該当しない情報資産	公表されている情報資産又は公表することを前提として作成された情報資産（教職員及び児童生徒以外の者が知り得ても支障がないと認められるものを含む）

(2) 完全性による分類

分類	分類基準	該当する情報資産のイメージ
完全性 2B	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学校関係者の権利が侵害される又は学校事務及び教育活動の的確な遂行に支障（軽微なものを除く）を及ぼすおそれがある情報資産	情報が正確・完全な状態である必要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合、業務の遂行に支障ある情報
完全性 2A	学校で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、学校関係者の権利が侵害される又は学校事務及び教育活動の的確な遂行に軽微な支障を及ぼすおそれがある情報資産	情報が正確・完全な状態である必要があり、破壊、改ざん、破損又は第三者による削除等の事故があった場合、業務の遂行に軽微な支障ある情報
完全性 1	完全性2B 又は完全性2BA に該当しない情報資産	事故があった場合でも業務の遂行に支障がない情報

(3) 可用性による分類

分類	分類基準	該当する情報資産のイメージ
可用性 2B	学校で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	必要な時にいつでも利用できる必要があり、情報システムの障害等による滅失紛失や、情報システムの停止等があった場合、業務の安定的な遂行に支障がある情報
可用性 2A	学校で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に軽微な支障を及ぼすおそれがある情報資産	必要な時にいつでも利用できる必要があり、情報システムの障害等による滅失紛失や、情報システムの停止等があった場合、業務の安定的な遂行に軽微な支障がある情報
可用性 1	可用性2B 又は可用性2A のに該当しない情報資産	滅失、紛失や情報システムの停止等があっても業務の遂行に支障がない情報

※情報資産の例

情報資産の分類					情報資産の例示		
重要性 分類	定義	機密性	完全性	可用性	校務系	学習系	公開系
I	セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。	3	2B	2B	・教職員の人事情報 ・入学者選抜問題 ・教育情報システム仕様書		
II	セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす。	2B	2B	2B	○学籍関係 ・卒業証書授与台帳 ・成績関係 ・評定一覧表 ○指導関係 ・事故報告書・記録簿 ○進路関係 ・卒業生進路先一覧等 ○健康関係 ・健康診断票 ・健康診断に関する表簿 ○児童・生徒に関する個人情報 ○学校教職員に関する個人情報 ○教職員に割り当てた機密性の高い情報 ・情報システムログインID/PW管理台帳 ・情報端末ログインID/PW管理台帳	○児童生徒の学習系情報 ・学習システムログインID/PW管理台帳 ・学習用端末ID/PW管理台帳	
III	セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす。	2A	2A	2A	○児童生徒の氏名 ・出席簿 ・名列表 ・座席表 ・児童生徒委員会名簿 ○学校運営関係 ・卒業アルバム ・学校行事等の児童・生徒の写真	○学校運営関係 ・授業用教材 ・教材研究資料 ・生徒用配布プリント ○児童生徒の学習系情報 ・児童生徒の学習記録 (確認テスト、ワークシート、レポート、作品等) ・学習活動の記録(動画・写真等)	
IV	影響をほとんど及ぼさない。	1	1	1			○学校運営関係 ・学校・学園要覧 ・学校紹介パンフレット ・学校行事のしおり ○学校活動の記録 ※保護者の承諾がある場合、以下は公開可能 ・学校行事等の児童・生徒の写真 ・学習活動の記録(動画・写真・作品等)

4. 情報資産の管理

(1) 情報資産の分類の表示

教職員等は、情報資産について、必要に応じてその分類を表示し、取扱制限についても明示する等の適切な管理を行わなければならない。

※ 情報資産の分類の表示先

ファイル(ファイル名、ファイルの属性(プロパティ)、ヘッダー・フッター等)、格納する電磁的記録媒体のラベル、文書の隅等

(2) 情報の作成

教職員等は、業務上必要のない情報を作成してはならない。情報を作成する者は、情報の作成時に「3. 情報資産の分類」に基づき、当該情報の分類と取扱制限を定めなければならない。

(3) 情報資産の利用

情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

(4) 情報の送信

情報資産が組織内部(組織が利用するサーバやクラウドサービス等)から組織外部(家庭、地域、

事業者等)に電子メール等により外部送信する場合は、情報資産分類に応じ以下の対応を実施しなければならない。

- ① 電子メール等により重要性分類Ⅲ以上（機密性 2A 以上）の情報を外部送信する者は、限定されたアクセスの措置設定を行わなければならない。
- ② 電子メール等による外部送信の安全性を高めるため、添付される情報資産を監視する等、出口対策を実施しなければならない。

(5) 情報資産の運搬

車両等により重要性分類Ⅲ以上（機密性 2A 以上）の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納、又は暗号化若しくはパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

(6) 情報資産の廃棄

重要性分類Ⅲ以上（機密性 2A 以上）の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。

※情報資産の取扱い例

情報資産の分類		組織外部への持ち出し制限*	情報の組織外部への送信**	情報資産の運搬***	組織外部での情報処理****	使用する電磁記録媒体	情報資産の保管	情報資産の廃棄
重要性分類	定義							
I	セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。	本ガイドラインに準拠していることを確認した上で業務遂行上必要な場合には、情報セキュリティ管理者の判断で持ち出しを可	限定されたアクセスの措置がとられていること*****	鍵付きケースへの格納	禁止	施錠可能な場所への保管	・耐火、耐熱、耐水、耐湿を講じた施錠可能な場所に保管（電子データの場合もこれらの対策に準じたサーバに保管） ・情報資産を格納するサーバのバックアップ ・6か月以上のログ保管 ・サーバの冗長化（推奨事項） ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁記録媒体の持ち込み禁止	電子記録媒体の初期化、復元できないようにして廃棄
II	セキュリティ侵害が、学校事務及び教育活動の実施に重大な影響を及ぼす。	同上	同上	同上	安全管理措置の規定が必要	同上	同上	同上
III	セキュリティ侵害が、学校事務及び教育活動の実施に軽微な影響を及ぼす。	情報セキュリティ管理者の包括的承認で可	同上	同上	同上	同上	・耐火、耐熱、耐水、耐湿を講じた施錠可能な場所に保管（電子データの場合もこれらの対策に準じたサーバに保管） ・情報資産を格納するサーバのバックアップ（推奨事項） ・一定期間以上のログ保管 ・サーバーハードディスクの冗長化（推奨事項） ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁記録媒体の持ち込み禁止	同上
IV	影響をほとんど及ぼさない。							

- * : 組織外部への持ち出しとは、教育委員会・学校が構築・管理している環境(本ガイドラインが適用されているクラウドサービスを含む環境)の外に情報資産を持ち出すことを示す。
- ** : 情報の組織外部への送信とは、情報システムを構成するネットワーク、端末、サーバの閉じた領域の外側に、情報資産をオンラインで持ち出すことを示す。
- *** : 情報資産の運搬とは、USBメモリやハードディスク等の電磁的記録媒体を介して情報資産を運搬する場合を示す。
- **** : 組織外部での情報処理とは、教育委員会・学校が構築・管理している環境(本ガイドラインが適用されているクラウドサービスを含む環境)の外において情報資産を管理・電算処理することを示す。
- ***** : 限定されたアクセスの措置とは、適切かつ限定的な利用を前提とし、外部に送信される際に適切なアクセス制限を講じることを指す。

5. 物理的セキュリティ

(1) 機器の取付け

サーバ等の機器の取付けを行う場合、地震、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

(2) サーバの冗長化

校務系サーバその他の情報を格納しているサーバを冗長化し、同一データを保持しなければならない。また、メインサーバに障害が発生した場合は、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

(3) 機器の定期保守及び修理

重要性分類Ⅲ以上（可用性 2A 以上）のサーバ等の機器の定期保守を実施しなければならない。

(4) 機器の廃棄等

機器を廃棄又はリース返却等をする場合は、機器内部の記憶装置から全ての情報を消去し、復元不可能な状態にしなければならない。

6. 教職員等の利用する端末や電磁的記録媒体等の管理

(1) 教員等の利用する端末について

不正アクセス防止のため、ログイン時の ID パスワードによる認証、多要素認証の実施等の使用す
る目的に応じた適切な物理的措置を講じなければならない。電磁的記録媒体については、情報が保
存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

また、パソコンやモバイル端末におけるマルウェア感染の脅威に対し、ウイルス対策ソフトの導
入等の対策を講じなければならない。

(2) 学習者用端末について

学習用端末は、盗難防止のため、教室等で利用するパソコンの保管庫による管理等の物理的措置
を講じなければならない。電磁的記録媒体について、情報が保存される必要がなくなった時点で速
やかに記録した情報を消去しなければならない。学習用端末は、情報システムへのアクセスにおけ
るログインパスワードの入力等による認証を設定しなければならない。

7. 人的セキュリティ

(1) 教職員等の遵守事項

① 教育情報セキュリティポリシー等の遵守

教職員等は、教育情報セキュリティポリシー及び教育情報セキュリティ実施手順を遵守しなけれ
ばならない。

② 業務以外の目的での使用の禁止

教職員等は、業務以外の目的で情報資産の外部への持ち出し、教育情報システムへのアクセス、
電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

③ モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

教職員等は、学校のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出

す場合は、学校管理者の許可を得なければならない。

④ 学校支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

(ア) 教職員等は、原則として、学校支給以外のパソコン、モバイル端末、電磁的記録媒体等を業務に利用してはならない。ただし、業務上必要な場合は、学校管理者の許可を得て利用することができる。

(イ) 教職員等は、学校管理者の許可を得た上で学校支給以外のパソコン、モバイル端末、電磁的記録媒体等を用いる場合は、学校管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

⑤ 持ち出し及び持ち込みの記録

学校管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

⑥ パソコンやモバイル端末におけるセキュリティ設定変更の禁止

教職員等は、パソコン及びモバイル端末のソフトウェアに関するセキュリティ機能の設定を教育情報セキュリティ管理者の許可なく変更してはならない。

⑦ 机上の端末等の管理

教職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は教育情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

⑧ 退職時等の遵守事項

教職員等は、異動、退職等により業務を離れる場合は、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

8. ID 及びパスワードの管理

(1) ID の取扱い

教職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

- ① 自己が利用している ID を他人に利用させてはならない。
- ② 共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

(2) パスワードの取扱い

教職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

- ① パスワードは、他者に知られないように管理しなければならない。
- ② 複数の教育情報システムを扱う教職員等は、同一のパスワードを複数のシステム間で用いてはならない。（シングルサインオンを除く）
- ③ 仮のパスワード（初期パスワードを含む）は、最初のログイン時点で変更しなければならない。
- ④ サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。
- ⑤ 教職員等間でパスワードを共有してはならない。（ただし、共有 ID に対するパスワードは除く）
- ⑥ 取り扱う情報の重要度に応じてパスワード以外に多要素認証を設定しなければならない。

9. 技術的セキュリティ

(1) 文書サーバ及び端末の設定等

- ① 住民の個人情報、人事記録等の特定の教職員のみ取扱うことができるデータについて、別途ディレクトリを作成する等の措置を講じ、同一学校等の所属であっても、担当以外の教職員等が閲覧及び使用できないようにしなければならない。
- ③ インターネット接続を前提とする校務外部接続系サーバ及び学習系サーバに保管する情報（学習系サーバにおいては、個人情報などを含む重要性が高い情報を保管する場合に限る）については、標的型攻撃等によるファイルの外部流出の可能性を踏まえて、ファイル暗号化等による安全管理措置を講じなければならない。

(2) バックアップの実施

ファイルサーバ等に記録された情報については、バックアップを実施するものとする。

(3) ログの取得等

各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

(4) ネットワークの接続制御、経路制御等

- ① フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。
- ② 不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

(5) 外部の者が利用できるシステムの分離等

保護者等の外部の者が利用できるシステム等がある場合、重要性が高い情報、特に情報資産重要性分類Ⅱ(セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす情報資産)以上を扱うシステムとの論理的又は物理的な分離又は各システムにおけるアクセス権管理の徹底を行うこと。

(6) 無線 LAN 及びネットワークの盗聴対策

- ① 無線 LAN の利用を認める場合は、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。
- ② 機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

(7) 電子メールのセキュリティ管理

大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

(8) 電子メールの利用制限

- ① 教職員等は、自動転送機能を用いて、電子メールを転送してはならない。
- ② 教職員等は、業務上必要のない送信先に電子メールを送信してはならない。
- ③ 教職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。
- ④ 教職員等は、ウェブで利用できるフリーメールサービス等を統括教育情報セキュリティ責任者の許可無しに使用してはならない。

(9) 電子署名・暗号化

教職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、電子署名、暗号化又はパスワード設定等のセキュリティを考慮して送信しなければならない。

(10) ソフトウェアの導入等

- ① 教職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。
- ② 教職員等は、業務上の必要がある場合は、管理職の許可を得てソフトウェアを導入することができる。
- ③ 教職員等は、不正にコピーしたソフトウェアを利用してはならない。

(11) 機器構成の変更の制限

- ① 教職員等は、パソコン及びモバイル端末に対し機器の改造及び増設・交換を行ってはならない。
- ② 教職員等は、業務上、パソコン及びモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、学校管理者の許可を得なければならない。

(12) 無許可でのネットワーク接続の禁止

教職員等は、管理職の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

10. アクセス制御

(1) アクセス制御等

ネットワーク又は情報システムごとにアクセスする権限のない教職員等がアクセスできないように、システム上制限しなければならない。

(2) ログイン時の表示等

ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ教職員等がログインしたことを確認することができるようシステムを設定しなければならない。

(3) パスワードに関する情報の管理

- ① 教職員等のパスワードに関する情報を厳重に管理しなければならない。
- ② 教職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

11. システム開発、導入、保守等

(1) 情報システムの調達

機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題がないことを確認しなければならない。

(2) 情報システムの変更管理

情報システムを変更した場合は、プログラム仕様書等の変更履歴を作成しなければならない。

(3) 開発・保守用のソフトウェアの更新等

開発・保守用のソフトウェア等を更新又はパッチを適用する場合、他の情報システムとの整合性を確認しなければならない。

12. 不正プログラム対策

(1) 学校管理者は不正プログラム対策として、次の事項を遵守しなければならない。

- ① 外部ネットワークから送受信したファイルは、インターネットのゲートウェイ等においてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムの外部への拡散及びシステムへの侵入を防止しなければならない。
- ② コンピュータウイルス等の不正プログラム情報を収集し、必要に応じて教職員等に対し注意喚起しなければならない。
- ③ 所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。
- ④ 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。
- ⑤ 業務で利用するソフトウェアは、パッチやバージョンアップ等の開発元のサポートが終了したソフトウェアを利用してはならない。

(2) 教職員等は、不正プログラム対策に関して、次の事項を遵守しなければならない。

- ① パソコン及びモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
- ② 外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによる点検を行わなければならない。
- ③ 差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。
- ④ 端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的実施しなければならない。
- ⑤ 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアで点検しなければならない。

(3) 専門家の支援体制

実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしなければならない。

13. 不正アクセス対策

(1) 学校管理者は、不正アクセス対策として、以下の事項を遵守しなければならない。

- ① 使用されていないポート及びSSID（無線LANネットワーク名）は閉鎖しなければならない。
- ② 不要なサービスについては、機能を削除又は停止しなければならない。
- ③ 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出した場合は、システム管理者に通報するよう、設定しなければならない。

(2) 記録の保存

サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

(3) 教職員等による不正アクセス

教職員等による不正アクセスを発見した場合は、教育情報セキュリティ管理者に通知し、適切な処

置を求めなければならない。

14. 情報システムの監視

システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

15. 侵害時の対応等

(1) 緊急時対応計画には、以下の内容を定めなければならない。

- ① 関係者の連絡先
- ② 発生した事案に係る報告すべき事項
- ③ 発生した事案への対応措置
- ④ 再発防止措置の策定

(2) 業務継続計画との整合性確保

自然災害、大規模かつ広範囲に及ぶ疾病等に備えて別途業務継続計画を策定し、当該計画と情報セキュリティポリシーの整合性を保たなければならない。

16. 懲戒処分等

教育情報セキュリティポリシーに違反した教職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、懲戒処分の対象とすることがある。

17. 外部委託

(1) 外部委託事業者の選定基準

- ① 外部委託事業者の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。
- ② 情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定しなければならない。

(2) 確認・措置等

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定期的に確認しなければならない。

18. クラウドサービスの利用における情報セキュリティ対策

(1) 利用者認証

- ① クラウド事業者における当該クラウドサービスを提供する情報システムの運用若しくは開発に従事する者又は管理者権限を有する者について、適切な利用者確認がなされていることをクラウド事業者に求め、サービス提供定款や契約書面上で確認又は合意しなければならない。
- ② 当該クラウドサービスのログインに関わる認証機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認又は合意しなければならない。

(2) アクセス制御

- ① 当該クラウドサービスに対して、アクセスする権限のない者がアクセスできないように、システム上制限する機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認又は合意しなければならない。
- ② クラウド事業者の提供するアクセス制御機能を用いて、情報資産毎に、許可されたエンドユーザのみがアクセスできる環境を設定しなければならない。

(3) クラウドに保管するデータの暗号化

当該クラウドサービスへのデータの保管に際し、情報漏えい等に備えて、暗号化等の保護措置を講じられていることを、クラウド事業者にサービス提供定款や契約書面上で確認または合意しなければならない。

(4) クラウドサービスを提供する情報システムの運用管理

- ① クラウド事業者に対して、サービスの一時停止等クラウド利用者に影響があり得る運用手順の有無、有る場合にはクラウド利用者への影響範囲（時間、サービス内容）、連絡方法等について情報提供を求め、クラウド利用者が業務運営に支障がないことを確認し、合意しなければならない。また、クラウド事業者の設定不備等によるインシデント発生時にも同様の確認をしなければならない。
- ② 当該クラウドサービスにおけるサーバの冗長化について、対策をクラウド事業者に求め、サービス提供定款及び契約書面上で確認又は合意していなければならない。
- ③ 当該クラウドサービスにおけるデータバックアップについて、対策をクラウド事業者に求め、サービス提供定款及び契約書面上で確認又は合意していなければならない。
- ④ 当該クラウドサービスにおける情報セキュリティの確保や監査に必要なログの取得について、対策をクラウド事業者に求め、サービス提供定款及び契約書面上で確認又は合意していなければならない。

(5) クラウド事業者従業員の人的セキュリティ対策

クラウドサービスに関わるクラウド事業者従業員に対して、クラウド事業者の情報セキュリティポリシー及び保守運用管理規程等を遵守することをクラウド事業者に求め、サービス提供定款及び契約書面上で確認又は合意していなければならない。

(6) データの廃棄等について

- ① サービス利用終了時等において、クラウド利用者のデータが不用意に残置されないよう適切に破棄するための流れについて、サービス提供定款や契約書面上で確認又は合意していなければならない。
- ② サービス利用終了時等におけるデータの扱いについて、スムーズに回収、次期システムへの移行等を行えるよう、その措置の流れについてサービス提供定款及び契約書面上で確認又は合意していなければならない。

19. パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項

(1) 守秘義務、目的外利用及び第三者への提供の禁止

クラウド事業者と契約時に守秘義務、目的外利用及び第三者への提供の禁止条項を締結しなけれ

ばならない。クラウドサービス事業者がコンテンツにアクセスできるかどうかを確認し、サービスに係る情報及び受託した情報に関する守秘義務、目的外利用及び第三者への提供の禁止条項について、サービス提供に係る契約に含めなければならない。契約には、当該条項に違反したクラウドサービス事業者に対する損害賠償規定を含める。

(2) 準拠する法令、情報セキュリティポリシー等の確認

クラウド事業者がどのような規範に基づいてサービス提供するか開示を求め、クラウド利用者の準拠する法令、情報セキュリティポリシーを確認し、それらとの整合を確認しなければならない。

(クラウド事業者の準拠する認証制度、個人情報保護指針、プライバシーポリシー、情報セキュリティに関する基本方針及び対策基準、保守運用管理規程 等)

(3) 情報セキュリティに関する役割の範囲、責任分界点

① クラウド事業者の情報セキュリティに関する役割の範囲と責任分界点について開示するよう求めなければならない。

② クラウド事業者の情報セキュリティに関する役割の範囲と責任分界点がクラウド利用者側で講ずる情報セキュリティ対策の役割の範囲と整合することを確認し、合意しなければならない。

(4) 情報インシデント管理及び対応フローの合意

① 情報セキュリティインシデント管理に関する責任範囲と及びインシデント対応フローを、サービス仕様の一部として定めることについて、クラウド事業者に対して求めなければならない。

② 情報セキュリティインシデント管理に関する責任範囲及びインシデント対応フローを検証しなければならない。

20. 約款による外部サービスの利用

(1) 約款による外部サービスの利用に係る規定の整備

以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、機密性の高い情報の取扱いには十分に留意するように規定しなければならない。

① 約款によるサービスが利用可能な範囲

② 業務により利用する約款による外部サービス

③ 利用手続及び運用手順

(2) 約款による外部サービスの利用における対策の実施

教職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

21. ソーシャルメディアサービスの利用

(1) 学校が管理するアカウントでソーシャルメディアサービスを利用する場合、その運用手順を定めなければならない。

(2) 重要性分類Ⅲ以上(機密性 2A 以上)の情報はソーシャルメディアサービスで発信してはならない。

22. 事業者に対して確認すべきプライバシー保護に関する事項

外部委託やクラウドサービスの利用に当たっては、事業者における個人情報の適切な管理が行われていることが必須であることから、個人情報の収集・利用範囲及び管理期間、データの統制と所有の在り方等について、事業者の確認をしなければならない。

これらの項目については、調達時においてサービスの過剰な排除にならないよう留意した上で契約要件等として定めなければならない。

23. 1人1台端末におけるセキュリティ

(1) 学習用端末のセキュリティ対策

① 授業に支障のないネットワーク構成の選択（帯域や同時接続数等）

クラウドサービス提供事業者側のサービス要件基準を満たしたネットワーク構成を設計する。また、運用開始前には十分検証し、利用状況に応じて定期的に改修計画を立てること。

② 不適切なウェブページの閲覧防止

生徒が端末を利用する際に不適切なウェブページの閲覧を防止する対策を講じなければならない。

③ マルウェア感染対策

学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

④ 端末を不正利用させないための防止策

端末のセキュリティ状態の監視に加えて、不適切なアプリケーションおよびコンテンツの利用を制限し、常に安全で児童生徒が安心して利用できる状態を維持しなければならない。

⑤ セキュリティ設定の一元管理

生徒への端末配付後においても、端末のセキュリティ設定、OSアップデート、ウェブブラウザのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状態確認等の作業を、離れた場所からでも一元管理できることが望ましい。

⑥ 端末の盗難・紛失時の情報漏洩対策

生徒が端末を紛失した場合は、遠隔操作でロックをかける、又はワイプ（データ消去）することで第三者による不正操作及び情報漏洩を防ぐ等の安全管理措置を講じなければならない。

⑦ 運用・連絡体制の整備

学校内外での端末の運用ルールを制定し、インシデント時の連絡先対応方法を各学校にて整理しなければならない。

24. 生徒におけるID及びパスワード等の管理

(1) ID登録・変更・削除

① 入学/転入時のID登録処理

IDについてはパスワードポリシーによりセキュリティ強度を上げていくなど適切な措置を講じなければならない。

② 進級/進学時のID関連情報の更新

IDについては原則として進級及び進学にも変更不要とすることが望ましい。

③ 転出、卒業及び退学時の ID 削除処理

転出卒業及び退学時に学習用ツールのサービス利用期間が終了する場合は、あらかじめ生徒本人によるデータ移行をサービス利用期間内に実施し、ID の利用停止後、最終的には ID 及び関連するデータの完全削除を行うこと。

ただし、本人同意や個人情報保護条例に基づく適切な管理の下、一部のデータを活用することは可能である。

(2) 多要素認証によるなりすまし対策

成績評価につながる CBT (Computer Based Testing : 試験における工程を全てコンピュータ上で行う事) など、本人確認を厳格に行う必要がある場合においては生徒の ID/パスワードに加えて多要素認証を設定することが望ましい。

25. 教育情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ委員会は、情報セキュリティ監査、自己点検の結果、情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について、毎年度及び重大な変化が発生したときに評価を行い、必要があると認めた場合は、改善を行うものとする。