京都府立学校情報セキュリティ対策基準

１　目的

京都府立学校情報セキュリティ対策基準(以下「対策基準」という。)は、京都府情報セキュリティ基本方針(以下「基本方針」という。)に基づき、京都府立学校（以下「府立学校」という。）の情報システムを活用して収受した学校運営上必要な情報や、児童生徒及び教職員等に関する個人情報などの様々な情報の取扱いに関するセキュリティ対策を実施する上で必要な基準を定めることを目的とする。

２　適用機関

対策基準の適用機関は、府立学校とする。

３　適用者

対策基準の適用者は、次のとおりとする。

(1) 府立学校に勤務する教職員(臨時的任用職員、任期付職員及び会計年度任用職員を含む。)及び教育実習生等（以下「教職員等という。」）

(2) 府立学校に在籍する児童生徒

(3) 京都府立学校の情報システムに関する業務の受託者

４　最高教育情報セキュリティ組織体制

(1) 最高教育情報統括セキュリティ責任者

ア　府立学校における全ての情報資産及び情報セキュリティを統括する責任者として、最高教育情報統括セキュリティ責任者を置く。

イ　最高教育情報統括セキュリティ責任者は教育監をもって充てる。

ウ　情報セキュリティの維持及び管理を統一的な視点で行うため、対策基準の決定権限及び責任を有する。

(2) 教育情報セキュリティ責任者

ア 情報資産の管理運営及び情報セキュリティ対策に関する権限と責任を有する教育情報セキュリティ責任者(以下「情報責任者」という。)を置く。

イ 情報責任者は指導部長をもって充てる。

ウ 情報セキュリティ対策において、必要な情報セキュリティ対策実施手順(以下「実施手順」という。)の決定権限及び責任を有する。

エ 最高教育情報統括セキュリティ責任者が欠けた場合は、その職務を代行する。

オ 情報責任者は、情報セキュリティ対策上必要があると認めるときは、適宜必要な措置を講じるよう指示するものとする。

(3) ＩＣＴ教育推進担当

ア 教育庁指導部ＩＣＴ教育推進課を、府立学校の情報セキュリティに関するＩＣＴ教育推進担当（以下「ＩＣＴ担当」という。）とする。

イ ＩＣＴ担当は府立学校における情報セキュリティの窓口となり、対応する。

ウ ＩＣＴ担当は府立学校から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、以下「インシデント」という。）発生の報告を受けた時には、情報責任者の指示のもと関係各課等と連携してインシデント対応を行うとともに、府立学校への指導・助言を行う。

(4) 教育情報セキュリティ管理者

ア 府立学校長を、当該学校における情報セキュリティに関する権限及び責任を有する教育情報セキュリティ管理者(以下「管理者」という。)とする。

イ 管理者は、実施手順で定める範囲内の管理運営に関する権限及び責任を有するものとする。

ウ 管理者は、基本方針、対策基準及び実施手順（以下「基本方針等」という。）の定める内容が遵守されるよう、少なくとも年度当初に情報セキュリティの維持を図る上で守るべき内容に関する研修会を開催し、年度途中の任用者への説明を適宜行うなど、全教職員等に必要な指導を講じるものとする。

エ 管理者は、校内でインシデントと思われる事象が確認されたとき、又はＩＣＴ担当から指示があったときは、コンピュータウイルス等の不正プログラム（以下「不正プログラム」という）に感染した端末のネットワークからの切断や学校内情報システムの通信記録調査など、情報セキュリティ対策上必要な措置を講じるものとする。

オ 管理者は、学校内の情報システムが外部からの不正アクセスを受けたとき、又は受けたおそれがあるときは、直ちにＩＣＴ担当に報告するものとする。

カ 管理者は、教職員の中から学校情報セキュリティ担当者(以下「学校担当者」という。)を選任するものとする。

キ 学校担当者は、管理者を補佐し、各学校における情報セキュリティの維持に必要な措置を講じるものとする。

ク 管理者は、学校担当者を新たに選任し、又は変更したときは、ＩＣＴ担当に報告するものとする。

5　情報資産の分類と管理方法

(1) 情報資産の分類

情報資産について、正確性、機密性、完全性及び可用性を踏まえ、被害を受けた場合に想定される影響の大きさをもとに以下のように分類を行い、必要に応じて取扱いを定める。

重要性分類
A セキュリティ侵害が児童生徒又は教職員等の生命、財産、プライバシー等への重大な影響を及ぼす情報
B 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
C セキュリティ侵害が学校事務及び教育活動の実施に及ぼす影響が軽微な情報
D セキュリティ侵害が影響をほとんど及ぼさない情報

(2) 情報資産の管理方法

ア 管理者は、(1)の分類ごとの取扱いをもとに適切に情報資産の管理を行う。

イ 情報資産が複製又は伝送された場合には、複製又は伝送された情報も(1)の分類に基づき適切に管理しなければならない。

6　物理的セキュリティ対策

(1) 情報システムの管理に関する管理者の責務

ア 機器の設置

機器の設置に当たっては、必要に応じ、空調設備を整備して温・湿度やほこりの影響の排除を図るとともに、コンピュータ教室(準備室を含む。)の施錠義務化や端末、プリンター等の機器の施錠可能な部屋への設置を図るなど、盗難防止に努めること。

また、必要に応じ消火機器を設置するなど、火災等への対策を講じること。

イ 電源

サーバ等の重要な機器については、停電時に対応できる予備電源装置等を取り付けるとともに、落雷等の過電流に対する保護対策を講じること。

ウ ネットワーク

ネットワーク回線は、傍受・損傷等を受けることがないよう、可能な限りの措置を講じること。また、無線ＬＡＮの導入に当たっては、十分な漏えい防止策を講じること。

7　人的セキュリティ対策

(1) 教職員等の責任

ア　情報セキュリティ対策の遵守義務

教職員等は、基本方針等に定められている事項を遵守すること。また、教職員等は、情報セキュリティ対策について遵守することが困難な事由が生じたときは、速やかに管理者及び学校担当者に相談し対応を協議すること。

イ　情報システム利用上の禁止事項

教職員等は、情報システムの利用に当たって次の行為を行ってはならない。

(ｱ) 業務目的以外で情報システムを利用すること。

(ｲ) 実施手順に反して、情報資産を学校外に持ち出すこと。

(ｳ) 利用する端末について、許可のない第三者が利用し、又は閲覧し得る状態にすること。

(ｴ) 情報システムを通して知り得た情報資産を漏えいすること。

(ｵ) ＩＤ又はパスワード（以下「ＩＤ等」という。）の公開又は照会に応じたり、他の教職員等のＩＤ等を利用すること。

(ｶ) ソフトウェアの不正コピーを行うこと。

(ｷ) 管理者が許可していない府の情報システム以外の情報システムを持ち込むこと。

(ｸ) 著作権法等の法令又は公序良俗に反すること。

ウ　不正プログラム対策

教職員等は、不正プログラム対策として、次に掲げる措置を実施しなければならない。また、管理者は、次に掲げる措置が実施されていないと認めるときは、当該教職員等に対して情報システムの利用を停止することができる。

(ｱ) 端末の接続に当たっては、不正プログラム対策用ソフトウェアを導入すること。

(ｲ) 不正プログラム対策用ソフトウェアのパターンファイルを常時最新のものに更新するとともに、不正プログラムに対する修正プログラムを速やかに適用すること。

(ｳ) 外部からのデータ又はソフトウェアを取り入れる際に、不正プログラム対策用ソフトウェアによるチェックを行うこと。

(ｴ) 差出人が不明又は心当たりがないメールに添付されたファイルやＵＲＬについては、メールを受信したことを管理者に報告し、開かずに速やかに削除すること。

(ｵ) 不正プログラム対策用ソフトウェアによる定期的なチェックを行うとともに、その動作を途中で止めないこと。

(ｶ) 添付ファイルのあるメールを送受信するときは、対策用ソフトウェア等によるチェックを行うこと。

エ　端末運用管理

教職員等は、端末の接続に当たって指定の端末運用管理ソフトウェアを導入しなければならない。

オ　その他情報システム利用上の注意事項

(ｱ) 重要な情報資産を記録した記録媒体が不要となったときは、データを復元できないように消去した上で廃棄すること。廃棄の際は、管理者が作成する記録媒体管理簿等に処理の日時、処理者及び処理内容を記録すること。

(ｲ) ＩＤ等の盗用や漏えいがあったときは、管理者を通じて直ちにＩＣＴ担当に連絡すること。

(ｳ) 公用のソフトウェアの管理に当たっては、その記録媒体、ライセンス契約書及び保証書等を紛失しないよう一元的に管理するとともに、鍵付きケースに保管すること。

(ｴ) 情報資産の流出、漏えい、改ざん、情報システムの障害、誤動作の事故等（以下「事故等」という。）を発見したときは、直ちに管理者に報告し、その指示に従い必要な措置を講じること。

管理者は、教職員等から事故等の報告を受けたときは、直ちに当該事故等をＩＣＴ担当に報告すること。

カ　7(1)イからエの規定は、児童生徒にこれを準用する。

(2) ＩＣＴ担当の責任

ＩＣＴ担当は情報セキュリティに関する情報を広く収集し、学校に対し周知しなければならない。

(3) 管理者の責任

ア　セキュリティ情報の収集

管理者は情報セキュリティに関する情報を広く収集し、教職員等に対し周知しなければならない。

イ　研修・訓練・普及・啓発

管理者は情報セキュリティに関する意識の醸成及び向上を図り、また理解を深めるために、教職員等に対する普及・啓発及び研修・訓練を行うものとする。

ウ　ＩＤ等の管理

管理者は教職員等のＩＤ等に関する情報については、厳重に管理しなければならない。

エ　不正アクセス及び不正プログラムに関する指導

管理者は不正アクセス及び不正プログラムに関する情報について、教職員等に周知するとともに、防止対策について指導しなければならない。

(4) 外部事業者に関する管理

ネットワーク及び情報システムの開発・保守を外部事業者に委託するときは、外部事業者から再委託を受ける事業者も含めて、次の事項を明記した契約を締結するものとする。

ア　基本方針及び対策基準の遵守

イ　業務上知り得た情報の守秘義務

ウ　府立学校から提供された情報の目的外利用及び受託者以外の者への提供の禁止

エ　指定場所以外での個人情報取扱業務の禁止

オ　個人情報が記載された資料等の確実な方法による運搬

カ　府立学校から提供された情報の返還

キ　業務従事者への在職中及び退職後の守秘義務の周知及び監督

ク　外部委託事業者の責任者や業務に携わる者の名簿の提出

ケ　基本方針及び対策基準が遵守されなかったときの損害賠償等の規定

コ　ＩＣＴ担当は、外部委託事業者に対し、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、必要に応じて、その内容を情報責任者に報告するとともに、その重要度に応じて最高教育情報統括セキュリティ責任者に報告しなければならない。

8　技術的セキュリティ対策

(1) サーバ等の分離

府立学校において児童生徒及び教職員等が利用する情報システムについては、当該情報システムを授業その他の教育活動用(以下「生徒系」という。)と校務用(以下「教員系」という。)に分離し、児童生徒が教員系で扱う情報の閲覧や転送、加工等ができないようにすること。

また、教職員等は、成績等の個人情報や校務上特に重要な情報を、生徒系ネットワーク上で処理し、又は生徒系のサーバ、パソコン等に保存しないこと。

(2) 外部ネットワークとの接続

府立学校における情報システムと府以外の機関の情報システム(以下「外部ネットワーク」という。)との接続について、管理者から要望があったときは、ＩＣＴ担当は当該外部ネットワークのネットワーク構成、機器構成、セ

キュリティレベル等を検討し、学校の情報資産に影響が生じないことを確認した上で、必要な手続を経て、最高教育情報統括セキュリティ責任者の承認を得て、情報政策課と協議の上、接続を認めるものとする。なお、接続に当たって、管理者は、次の事項を遵守するものとする。

ア　不正アクセスを防止するためのファイアウォールの設置や認証、ネットワークの論理的な分離等適切なネットワーク経路制御を講じること。

イ　外部ネットワークとの接続により情報システムの運用及び情報資産の保持に支障が生じるおそれがあるときは、直ちに当該情報システムと外部ネットワークとの接続を物理的に遮断すること。

(3) クラウドサービスを利用する場合の承認手続きは、前項の手続に準じることとする。

(4) システム開発、導入、保守等

ア　情報システムの調達

(ｱ) 府立学校において情報システム機器及びソフトウェアを調達するときは、管理者はＩＣＴ担当に事前に協議すること。

(ｲ) 府立学校において機器及びソフトウェアを調達するときは、管理者は当該製品の安全性及び信頼性を確認すること。

イ　情報システムの開発

府立学校において情報システムの開発を行う場合、次の事項を実施することとする。

(ｱ) 情報システムの開発、保守等に関する事故及び不正行為に係る危険性について十分検討を行うこと。

(ｲ) プログラム、設定等のソースコードを整備すること。

(ｳ) セキュリティの確保に支障が生じるおそれのあるソフトウェアは利用しないこと。

(ｴ) 情報システムの開発及び保守に係る記録を作成するとともに、運用、管理等に必要な説明書等の書類を定められた場所へ保管すること。

(ｵ) 不要になったユーザ名、パスワード等は、速やかに抹消すること。

ウ　ソフトウェアの更新及び保守

(ｱ) 管理者は、独自開発ソフトウェア及びＯＳ等を更新し、又は修正プログラムを導入する場合は、不具合がないこと及び他のシステムとの適合性の確認を行うこと。

(ｲ) 管理者は、情報セキュリティに関して常に情報を収集し、必要に応じて修正プログラムの導入等速やかな対応を行うこと。

エ　管理記録

管理者は、学校内の情報システムにおいて行ったシステム変更等の作業については、記録を作成し適切に管理を行うものとする。

(5) 管理者の不正プログラム対策

管理者は、不正プログラムに対する情報システムの安全性を確保するため、次の事項を実施するものとする。

ア　外部ネットワークからデータを受け入れる際には、ファイアウォールを適切に設定するとともに、サーバ等において不正プログラムのチェックを行いシステムへの侵入を防止すること。

イ　外部ネットワークへデータを送信する際にも、アと同様の不正プログラム対策チェックを行い、外部への不正プログラムの拡散を防止すること。

ウ　不正プログラム情報について、児童生徒及び教職員等に対する注意喚起を行うこと。

エ　不正プログラム対策用ソフトウェアのパターンファイルは常に最新の状態に保つこと。

オ　不正プログラムに対する修正プログラムを入手し、サーバ及び端末に速やかに適用すること。

(6) 不正アクセス対策

ア　情報セキュリティ管理者は、不正アクセスを防止するため、次に掲げる対策を講じるものとする。

(ｱ) ソフトウェアの不備に伴うセキュリティホールを塞ぐため、速やかに修正プログラムを適用すること。

(ｲ) 情報システム上の不要なユーザ名は、速やかに削除すること。

(ｳ) 不正アクセスを受けるおそれが認められる場合には、情報システムの停止を含む必要な措置を講じること。

(ｴ) 利用終了又は利用される予定のない不要なポートは閉めること。

イ　職員及び委託事業者等は、不正アクセスを受け、又は受けたおそれがある場合は、直ちに情報セキュリティ管理者に報告するものとする。

ウ　情報セキュリティ管理者は、イの規定による報告を受けた場合は、直ちにその内容をＩＣＴ担当に報告するとともに、関係者に連絡を行い、情報の復旧等必要な措置を講じなければならない。

エ　ＩＣＴ担当は、不正アクセスを受け、又は受けたおそれがある場合は、情報責任者に報告するとともに関係者に連絡を行い、情報の復旧等必要な措置を講じなければならない。

9　セキュリティ対策上の遵守状況の確認

(1) 遵守するべき事項

管理者は、学校で取り扱う情報資産について、次の事項を遵守して情報セキュリティ対策を行うものとする。

ア　児童生徒、保護者及び教職員等の個人情報の流出の防止

イ　外部からの不正アクセスによる情報の破壊、盗聴、持出し及び改ざんの防止

ウ　内部からの故意又は意図しない操作などによる情報の破壊、盗聴、漏えい及び改ざんの防止

エ　不正プログラムによるデータ及び情報システムの破壊並びに不正プログラムの作成及び拡散の防止

オ　地震、火災、盗難等の緊急事態への速やかな対応

(2) 児童生徒への指導

児童生徒が情報資産や情報システムを利用するときは、管理者及びその他の教職員等は、遵守すべき情報セキュリティの維持管理やプライバシー保護のため必要な事項を児童生徒に示し、これらを遵守するよう指導しなければならない。

(3) 学校開放等における利用者への周知

学校開放等において、児童生徒又は教職員等以外の者が府立学校の情報システムを利用するときは、管理者及びその他の教職員等は、利用に当たって遵守すべき情報セキュリティの維持管理やプライバシー保護のために必要な事項の周知に努めるものとする。

10　運用及び緊急時におけるセキュリティ対策

(1) 対策基準の遵守状況の確認

ア　教職員等は、対策基準に違反したとき又は違反事実を確認したときは、直ちに学校担当者を通じて管理者に報告するものとする。

イ　管理者は、対策基準の遵守及び情報資産の管理状況について定期的に確認を行い、問題があると認めたときは速やかにＩＣＴ担当に報告することとし、ＩＣＴ担当は報告を受け、迅速かつ適切に対処するものとする。

(2) 緊急時の対応計画等

ア　管理者は、緊急時の対応について、あらかじめ緊急時対応計画や緊急連絡網を定めておくものとする。

イ　管理者は、当該学校に起因する情報システムの障害や事故等が起きたときは、その原因に関する校内の詳細な調査を行うとともに、再発防止計画を策定しＩＣＴ担当に報告するものとする。

11　対策基準の見直し

最高教育情報統括セキュリティ責任者は、定期的に対策基準の見直しを行い、必要に応じて修正を行う。

12　自己点検

ア　情報セキュリティ管理者は、所管する情報システムについて、必要に応じて自己点検を実施しなければならない。

イ　情報セキュリティ管理者は自己点検の結果を踏まえ、必要に応じて実施手順を見直さなければならない。

ウ　情報セキュリティ管理者は、自己点検結果を必要に応じてＩＣＴ担当に報告しなければならない。

エ　ＩＣＴ担当は、情報セキュリティ管理者から自己点検結果の報告を受けた場合、必要に応じて情報セキュリティ管理者に情報セキュリティ対策について見直しを指示しなければならない。

附　則　この対策基準は、平成 16 年５月１日から施行する。

平成 20 年１月４日一部改正

令和元年 10 月 10 日一部改正

令和４年１月 24 日一部改正

令和６年４月１日一部改正

教育情報セキュリティ組織体制