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、京都府立学校とする。

3　適用者

対策基準の適用者は、次のとおりとする。

(1) 京都府立学校に勤務する教職員(臨時的任用職員及び非常勤職員を含む。)

(2) 京都府立学校の情報システムに関する業務の受託者

4　情報セキュリティ管理体制

(1) 京都府教育庁ＩＴ推進本部

京都府教育庁ＩＴ推進本部(以下「推進本部」という。)は、各府立学校における情報セキュリティの維持、管理を統一的な視点で行うため、対策基準の制定及び修正その他情報セキュリティに関する重要な事項を審議し、決定する。

対策基準の制定及び修正については、推進本部が決定した上で、京都府行政経営改革推進本部の承認を得るものとする。

(2) 情報システム管理者

ア　府立学校における各情報システムを所管する所属長を、当該情報システムの管理運営及び情報セキュリティに関する権限と責任を有する情報システム管理者(以下「管理者」という。)とする。

イ　管理者は、当該情報システムの情報セキュリティの適正な運用を図るため、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。)の制定及び修正を行うものとする。

ウ　管理者は、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) 情報セキュリティ責任者

ア　府立学校長を、当該学校の情報セキュリティに関する権限及び責任を有する情報セキュリティ責任者(以下「責任者」という。)とする。

イ　責任者は、基本方針、対策基準及び実施手順の定める内容が遵守される

よう、少なくとも年度当初に１回は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、又は年度途中の転入者や採用者への説明を適宜行い、全教職員に指導徹底するなど、必要な措置を講じるものとする。

ウ　責任者は、管理者から(2)のウの指示があったときは、コンピュータウイルスに感染した端末のネットワーク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。

エ　責任者は、基本方針、対策基準及び実施手順に定めるもののほか、情報セキュリティ対策について不明な点があるときは、管理者に確認するものとする。

オ　責任者は、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、又は受けたおそれがあるときは、直ちに管理者に報告するものとする。

カ　責任者は、教職員の中からネットワーク担当者(以下「担当者」という。)を選任するものとする。

キ　責任者は、担当者を新たに選任し、又は変更したときは、管理者にその内容を通知するものとする。

ク　責任者は、府立学校内のコンピュータ教室から普通教室や職員室等への校内ネットワークなど、管理者が策定する実施手順で別途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。

(4) ネットワーク担当者

担当者は、責任者を補佐し、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。

5　セキュリティ対策上の注意事項

(1) 特に注意する事項

責任者は、学校で取り扱う情報資産について、特に次の事項に注意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、教職員等の個人情報の流出

イ　外部からの不正アクセスによる情報資産の盗聴、持出し及び改ざん

ウ　内部からの故意又は意図しない操作などによる情報資産の盗聴、漏えい及び改ざん

エ　ウイルスによるデータ及び情報システムの破壊並びにウイルスの作成及び拡散

オ　地震、火災、盗難等の緊急事態への対応

(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、責任者及びその他の教職員は、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

学校開放講座等において、府民が府立学校の情報システムを利用するとき

は、責任者及びその他の教職員は、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。

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責任者の責務

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。)の施錠義務化や施錠可能な部屋への端末、プリンター等の機器の設置を図り、盗難防止に努めること。

また、必要に応じ消火器を設置するなどして、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、管理者の同意なく、変更及び追加を行わないこと。ただし、4の(3)のクにより管理者が別途定める範囲内において、管理者と調整の上、責任者の責任により変更及び追加を行うことができるものとする。この場合、責任者は管理者へ当該変更及び追加の内容を図面等で報告すること。

なお、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。

(2) 学校外における機器等の設置

本来学校内に設置すべき機器等を学校外に設置しようとするときは，管理者の承認を受けるものとする。

7　人的セキュリティ対策

(1) 教職員の責任

ア　情報セキュリティ対策の遵守義務

教職員は、基本方針及び対策基準に定められている事項を遵守すること。また、教職員は、情報セキュリティ対策について不明な点又は遵守することが困難な点が発生したときは、速やかに責任者に連絡すること。

イ　情報システム利用上の禁止事項

教職員は、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。

また、管理者は、次の行為が行われていると認めるときは、当該教職員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) 業務目的以外で情報システムを利用すること。

(イ) 情報資産を学校外に持ち出すこと。ただし、業務上やむを得ず記録媒体を学校外に持ち出す場合で、責任者の承認を得たときはこの限りでない。この場合、責任者は持出し管理簿を設けて適切に管理するものとする。

(ウ) 利用する端末や記録媒体について、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) パスワードの公開又は照会に応じたり、他の教職員のパスワードやユーザ名を利用すること。

(カ) ソフトウェアの不正コピーを行うこと。

(キ) 情報システムに接続する公用端末に対する機器の増設及び改造、プロトコル（通信手順）の設定変更、ソフトウェアの導入等を行うこと。ただし、業務を円滑に遂行するための合理的理由がある場合で、かつ責任者の承認を得たときはこの限りではない。

(ク) 責任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。

(ケ) 著作権法等の法令又は公序良俗に反すること。

ウ　コンピュータウイルス対策

教職員は、コンピュータウイルス対策として、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、ウイルス対策用ソフトウェアを導入すること。

(イ) ウイルスチェック用パターンファイルを常時最新なものに更新するとともに、コンピュータウィルス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、ウイルスチェックを行うこと。

(エ) 差出人が不明のファイル及び不自然に添付されたファイルについては、速やかに削除すること。

(オ) コンピュータウイルス対策用ソフトウェアによる定期的なウイルスチェックを行い、その実行を途中で止めないこと。

(カ) 管理者等が提供するウイルス情報を確認すること。

(キ) 添付ファイルのあるメールを送受信するときは、ウイルスチェックを行うこと。

(ク) 不正アクセスを受けたときは、直ちに担当者を通じて責任者に連絡すること。

エ　端末運用対策

教職員は、端末運用対策として、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。

また、管理者は、上記措置が実施されていないと認めるときは、当該教

職員に対して情報システムの利用を停止することができる。

なお、端末運用管理ソフトウェアの導入及びライセンスの管理は担当者が行うものとする。

オ　その他情報システム利用上の注意事項

(ｱ) 取出しが可能な記録媒体は、盗難や損傷の防止等のため適切な管理を行うこと。

(ｲ) 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を行った上で廃棄すること。廃棄の際は、責任者が作成する記録媒体処理簿に処理の日時、処理者及び処理内容を記録すること。

(ｳ) 管理者から与えられたパスワードを変更するときは、十分な長さとし容易に推定できないようなものにすること。また、パスワードの盗用や漏えいがあったときは、責任者を通じて直ちに管理者に連絡すること。

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

(ｵ) 情報資産の流出、漏えい及び改ざん並びに情報システムの障害及び誤動作等の事故（以下「事故等」という。）を発見したときは、直ちに責任者に報告し、その指示に従い必要な措置を講じること。責任者は、教職員から事故等の報告を受けたときは、直ちに当該事故等の内容を管理者に報告すること。

(2) 推進本部及び管理者の責任

ア　セキュリティ情報の収集

情報セキュリティに関する情報を広く収集し、学校に周知しなければならない。

イ　教育・訓練

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、情報システムの利用者に対する普及・啓発及び教育・訓練を行うものとする。

ウ　パスワードの管理

教職員のパスワード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　不正アクセス及びコンピュータウイルスに関する指導

不正アクセス及びコンピュータウイルスに関する情報について、教職員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。

(3) 外部委託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・保守を外部委託事業者に発注するときは、外部委託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り扱い業務の禁止
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義務
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社員の名簿の提出
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

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「教育用」という。)と教育行政用(以下「校務用」という。)に分離し、生徒が校務用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、教職員は、成績等の個人情報や校務上特に重要な情報を、教育用ネットワーク上で使用し、又は教育用のサーバ、パソコン等に保存しないこと。

(2) アクセス記録の取得等

ア　管理者は、重要な情報システムについて、各種アクセス記録及び情報セキュリティ対策に必要な記録を取得し、１年以上の期間を定めて保存するものとする。

イ　管理者は、重要な情報システムについて、定期的にアクセス記録等を分析、監視するものとする。

ウ　管理者は、アクセス記録等が流出したり、改ざんや消去をされないように必要な措置を講じるものとする。

(3) アクセス制御

ア　管理者は、情報システムにおけるアクセス制御について次の事項を遵守するものとする。

(ｱ) アクセス権限の許可は、必要最小限にすること。

(ｲ) 不正アクセスを防止するため、ユーザ認証、論理的なネットワークの分割、ファイアウォールの設置等の適切なネットワーク経路制御を講じること。

(ｳ) アクセス方法等は、教職員の真正性が確保できるものにすること。

イ　接続した情報通信機器についてセキュリティ上の問題があり、情報資産を脅かすおそれがあると認められるときは、速やかに責任者と協議の上、当該情報通信機器をネットワークから物理的に隔離するものとする。

(4) 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、責任者から希望があったときは、管理者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、推進本部の承認を得て、京都府行政経営改革推進本部と協議の上、接続を認

めるものとする。なお、接続に当たって、管理者及び責任者は、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、論理的なネットワークの分割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。

(5) システム開発、導入、保守等

ア　情報システムの調達

(ｱ) 学校において情報システムの機器及びソフトウェアの調達に伴う仕様書を作成するときは、責任者は管理者とも協議の上、情報セキュリティ対策上支障が生じるおそれのある内容を記載しないようにすること。

(ｲ) 学校において機器及びソフトウェアを調達するときは、責任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

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ものとする。

(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った上で、計画的に更新し、又は導入すること。

(ｲ) 管理者は、情報セキュリティに重大な影響を及ぼす不具合に関して常に情報を収集し、発見したときは、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、所管する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。

(6) 管理者のコンピュータウイルス対策

管理者は、コンピュータウイルスによ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、メールサーバ等においてウイルス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、アと同様のウイルスチェ

ックを行い、外部へのコンピュータウイルスの拡散を防止すること。

ウ　コンピュータウイルス情報について、教職員等に対する注意喚起を行うこと。

エ　ウイルスチェック用のパターンファイルは常に最新のものに保つこと。

オ　コンピュータウイルス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。

9　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　教職員は、この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、直ちに担当者を通じて責任者に報告するものとする。

イ　責任者は、対策基準の遵守状況及び情報資産の管理状況について定期的に確認を行い、支障を認めたときは速やかに管理者に報告するものとする。

なお、管理者が支障を確認したときは、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　責任者は、あらかじめ緊急時の対応について、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　責任者は、学校に起因する情報システムの障害や事故等が起こったときは、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するものとする。

10　評価・見直し

(1) 評価

責任者は、この対策基準を踏まえた情報セキュリティ対策の遵守状況について定期的に検証し、その結果を管理者に報告するものとする。管理者は、その報告を取りまとめの上、見直し等の意見を添えて、推進本部に報告するものとする。

(2) 対策基準の見直し

推進本部は、必要に応じて対策基準の見直しを行う。

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