京都府立医科大学情報セキュリティ対策基準

1　目的

京都府立医科大学情報セキュリティ対策基準（以下、「本基準」という。）は、京都府立医科大学総合情報化基本方針を実施する上で必要な情報セキュリティ対策の基準を定めることを目的とする。

2　定義

本基準において次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

(1)　事故等

情報資産の流出、漏えい、改ざん、情報システムの障害及び誤動作等の事故をいう。

(2)　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、当該情報資産の管理及び運用を行うための区画をいう。

(3)　要安定情報

本学で取り扱う情報のうち、滅失、紛失等により、利用者等の権利が侵害され又は本学の活動の安定的な遂行に支障を及ぼすおそれのある情報をいう。

(4)　外部ネットワーク

本学以外の機関の情報システムをいう。

(5)　セキュリティホール

コンピュータソフトウェア、ハードウェアの欠陥をいう。

(6)　その他の用語の定義は基本方針及び基本規程の定めるところによる。

3　情報システムの運用に係るセキュリティ対策

(1)　本学情報システムの運用に際し、総合情報センターが取り組むセキュリティ対策を次のとおり定める。

ア　本学アカウント付与範囲の限定

イ　人事データ等に基づいた個人認証の導入、1人1アカウント化の推進

ウ　アカウント管理の適正化

エ　ネットワークの適切な維持・管理

オ　ネットワークセキュリティの向上・強化

(2)　上記のセキュリティ対策に取り組むに当たっては、京都府公立大学法人の中期計画に盛り込む等により、計画的に進めるものとする。

4　人的セキュリティ対策

(1)　利用者等の責務

ア　情報セキュリティ対策の遵守義務

(ｱ)　利用者等は、本方針等に定められている事項を遵守するとともに、個別システム管理者からセキュリティ維持のために協力を依頼された場合には、従わなければならない。

(ｲ)　情報セキュリティ対策について不明な点、遵守することが困難な点が発生したときは、速やかに情報セキュリティ責任者に連絡すること。

イ　情報システム利用上の注意事項

利用者等は、情報システムの利用に当たって次の(ｱ)から(ｶ)に該当する行為をしてはならない。個別システム管理者は、当該行為が認められた場合は、利用者等に対し、情報システムの利用を停止することができる。

(ｱ)　業務等の利用を許可されている目的以外で情報システムを利用すること。

(ｲ)　情報資産を設置場所外に持ち出すこと。ただし、情報資産を別の記録媒体に保存するなどやむを得ない理由のある場合で、かつ情報セキュリティ責任者の事前の了解を得た場合を除く。

(ｳ)　利用する端末や記録媒体について、許可のない第三者に利用又は閲覧され得る状態にすること。

(ｴ)　接続許可を受けた通信回線以外に本学の情報システムを接続すること。

(ｵ)　接続許可を受けていない情報システムを通信回線に接続すること。

(ｶ)　情報システムで利用を禁止するソフトウェアを利用すること。

ウ　本方針等への重大な違反への対応

(ｱ)　個別システム管理者は、本方針等への重大な違反を知った場合は、情報システム管理者にその旨を報告するものとする。

(ｲ)　情報システム管理者は、本方針等への重大な違反の報告を受けた場合又は自ら重大な違反を知った場合には、速やかに調査を行い、事実を確認するものとする。事実の確認に当たっては、可能な限り当該行為者の意見を徴取するものとする。

(ｳ)　情報システム管理者及び情報セキュリティ管理者から報告を受けた情報システム総括責任者は、調査によって違反行為が判明した場合は、次に掲げる措置を講じることができる。

①当該行為者に対する行為の中止命令

②個別システム管理者に対する当該行為に係る情報発信の遮断命令

③当該行為者に対するアカウント削除命令

④その他法令等に基づく措置

(ｴ)　情報システム総括責任者は、本方針等への重大な違反の報告を受けた場合、自らが重大な違反を知った場合又は前項の措置を講じた場合は、遅滞なく、推進委員会にその旨を報告するものとする。

エ　その他

利用者等は、知り得た情報資産を漏えいしてはならない。卒業、退職等により、本学を離れる場合も同様とする。

(2)　アカウント等の管理

ア　利用者等は、自ら管理するアカウントの利用に関し、別に定める「京都府立医科大学アカウント管理規程」を遵守すること。

イ　利用者等は、自ら管理するユーザ名及びパスワード（以下、「パスワード等」という。）について、次に掲げる事項を遵守すること。

(ｱ)　他の利用者等のユーザ名を使わないこと。

(ｲ)　パスワードを秘密にし、パスワードの照会等には一切応じないこと。

(ｳ)　他人に自分のパスワード等を使用させないこと。

(ｴ)　パスワードは十分な長さとし、文字列はアルファベット、数字及び記号を混在させるなど容易に推定できないものとすること。

(ｵ)　パスワードの盗用や漏えいがあった場合は、直ちに個別システム管理者に連絡すること。個別システム管理者は、情報システム管理者に連絡すること。

(3)　不正プログラムの感染防止等

ア　利用者等は、不正プログラムの感染防止に関する措置に努めること。

イ　利用者等は、情報システムが不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システムの通信回線への接続や記録媒体との接続を速やかに切断するなど、必要な措置を講じるとともに、個別システム管理者及び情報セキュリティ責任者に報告すること。

個別システム管理者は、情報システム管理者に報告すること。

(4)　教育・訓練

ア　情報セキュリティ管理者は、情報セキュリティに対する意識を醸成し保つため、利用者等に対し普及啓発するとともに、情報セキュリティに関する理解が深まるよう教育・訓練を行うものとする。

なお、教育・訓練は、情報セキュリティ管理者が定める教育実施計画に従って、適切な時期に実施すること。

また、情報システム総括責任者は、推進委員会に情報セキュリティ対策に関する教育・訓練の実施状況を報告すること。

イ　個別システム管理者は、情報システムに不測の事態が発生した場合に備えた訓練を行うものとする。

(5)　事故等の報告

ア　利用者等は、事故等の発生又は発生の危険性を認識した場合には、直ちに情報セキュリティ責任者に報告し、その指示に従い必要な措置を講じるものとする。

イ　情報セキュリティ責任者は、事故等の報告を受けた場合は、直ちに当該事故等の内容を個別システム管理者及び情報システム管理者に報告するものとする。

(6)　事故等の原因調査・再発防止

ア　個別システム管理者は、情報システム管理者及び情報セキュリティ管理者の指示を受けた場合は、当該指示を踏まえ、事故等の原因を調査するとともに再発防止策を検討し、それを報告書として情報システム総括責任者に報告すること。

イ　情報システム総括責任者は、その内容を確認し、再発防止策を実施するために必要な措置を指示すること。

(7)　外部委託に関する管理

情報システムの開発・保守を外部委託事業者に発注する場合は、外部委託事業者から再委託を受ける事業者も含めて、下記の事項を明記した契約を締結するものとする。

ア　本方針等の遵守

イ　業務上知り得た情報の守秘義務

ウ　本学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　本学から提供された情報の返還義務

オ　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

カ　本方針等が遵守されなかった場合の損害賠償等の規定

5　物理的セキュリティ対策

(1)　情報システム

ア　機器の設置等

機器の設置等に当たっては、次に掲げる措置を講じるものとする。

(ｱ)　温度、湿度、ほこり等の環境の影響を可能な限り排除した場所に設置すること。

(ｲ)　必要に応じ、容易に取り外せないようにするなど適切な措置を講じること。

(ｳ)　情報システムの重要度に応じて、機器の二重化や地震対策等、運用環境を考慮すること。

イ　電源

(ｱ)　サーバ等の機器の電源については、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けること。

(ｲ)　落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じること。

ウ　ネットワーク

(ｱ)　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。

　なお、個別システム管理者等の許可なく、ネットワーク回線を変更又は追加できないようにすること。

(ｲ)　無線LANの導入に当たっては、ＩＤ・パスワード等による認証を必ず設定するとともに、経路に特殊な暗号処理を施す等、十分な漏えい防止策を実施すること。

エ　情報システムの運用・保守

(ｱ)　個別システム管理者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用すること。

(ｲ)　個別システム管理者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。

オ　情報システムについての対策の見直し

(ｱ)　個別システム管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じること。

(2)　管理区域

ア　管理区域は、水害対策及び確実な入退室管理を行うために、外部からの侵入が容易にできないように可能な限り無窓の外壁等に囲まれた区画とすること。

イ　管理区域から外部に通じる出入口は可能な限り１箇所のみとし、ＩＣカード等による入退室管理、入退室管理簿の記載、監視機能、鍵、警報装置等によって許可されていない立入りを防止すること。

ウ　管理区域には、設置機器の重要性に応じて、ビデオカメラ等の監視機能を設置すること。

エ　管理区域内の機器類は、耐震対策を講じた場所に設置するとともに、防火措置等を講じること。

なお、管理区域内の機器類の配置は、緊急時に円滑に避難できるよう配慮すること。

オ　消火剤は、機器及び記録媒体に影響を与えないものであること。

(3)　情報システムを校舎外に設置しようとする場合

情報システムを校舎外に設置しようとする場合は、推進委員会（当該情報システムにつき別途委員会等のある場合は当該委員会等）の承認を受けるものとする。

(4)　区域ごとの対策の決定

ア　情報システム管理者は、第２号の規定を踏まえ、施設及び環境に係る対策を行う単位ごとの区域を定めること。

イ　情報システム管理者は、管理区域について、上記の対策の基準と周辺環境や当該区域で行う本学の業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。

(5)　区域における対策の実施

ア　個別システム管理者は、管理区域に対して定められた対策を実施すること。利用者等が実施すべき対策については、利用者等が認識できる措置を講じること。

イ　個別システム管理者は、災害から要安定情報を取り扱う情報システムを保護するために、物理的な対策を講じること。

ウ　利用者等は、利用する区域について情報システム管理者が定めた対策に従って利用すること。また、学外の者を立ち入らせる際には、その者にも当該区域で定められた対策に従って利用させること。

(6)　情報資産の管理方法

ア　自らの業務等の遂行のために必要な範囲に限って情報を利用等すること。

イ　情報資産に関する業務に携わるすべての利用者等が業務上記録媒体を持ち出す場合､情報セキュリティ責任者は管理簿を設けるなど適切に管理するものとする。

ウ　記録媒体の管理

(ｱ)　取り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)　保存する情報にアクセス制限を設定するなど、情報を適切に管理すること。

(ｳ)　USBメモリ等の記録媒体を用いて情報を取り扱う際、紛失に伴う情報の流出等が起きないよう、十分に留意すること。

(ｴ)　記録媒体に納められた情報資産のうち、重要な情報資産は、別の記録

媒体に複製し、当該記録媒体は自然災害を被る可能性が低い地域に別途保管すること。

(ｵ)　重要な情報資産を記録した記録媒体は、耐火、耐熱、耐水及び耐湿対策を講じた施錠可能な場所に保管すること。

(ｶ)　記録媒体が不要となった場合は、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。

　また、消去及び廃棄を行った日時、処理者及び処理内容を記録すること。

エ　非公開情報の管理

(ｱ)　個人情報、事務、研究・教育・診療等の非公開情報を不当に利用してはならない。情報は適切に管理されなければならず、権限のない情報に対してアクセスし、また、利用してはならない。情報の盗難・漏えい等を防止するため、非公開情報を扱うネットワークは、可能な限り暗号化や盗聴防止策を講じること。

(ｲ)　許可された者以外がコンピュータに非公開情報を保管してはならない。また、一時的であっても、利用者等が日常的に使用するコンピュータに非公開情報を不特定の者が可読な状態で複製してはならない。

(ｳ)　物理的な盗難等を防止するため、利用を許可された場所から外部に非公開情報を持ち出してはならない。

6　技術的セキュリティ対策

(1)　アクセス記録の取得等

ア　個別システム管理者は、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　個別システム管理者は、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　個別システム管理者は、アクセス記録等が窃盗、改ざん、消去されないように必要な措置を講じるものとする。

(2)　アクセス制御

ア　個別システム管理者は、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)　アクセス方法等は利用者等の真正性が確保できるものとすること。

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場合には、速やかに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。

(3)　外部ネットワークとの接続

ア　外部ネットワークとの接続については、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、本学の情報資産に影響が生じないことを推進委員会（外部ネットワークと接続しようとする情報システムにつき別途委員会等のある場合は当該委員会等）が確認した上で接続を認めるものとする。

イ　なお、接続に当たって、個別システム管理者は、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利用者等の認証、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場合は、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。

(4)　情報システムの開発、導入、保守等

ア　情報システムの調達

(ｱ)　個別システム管理者は、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の作成に当たり、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こと。

(ｲ)　個別システム管理者が機器及びソフトウェアを調達する場合には、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

個別システム管理者が、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リスク（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)　不要になったアカウントは、速やかに削除すること。

ウ　ソフトウェアの更新及び保守

(ｱ)　個別システム管理者は、独自開発ソフトウェア及びＯＳ等を更新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情報システムとの適合性の確認を行った上で、計画的に更新又は導入すること。

(ｲ)　個別システム管理者は、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、不具合を発見した場合は、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

個別システム管理者は、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。

(5)　コンピュータウイルス対策

ア　個別システム管理者は、コンピュータウイルスによる情報システムの危険性を回避するため、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利用者等に対する注意喚起を行うこと。

(ｴ)　必要に応じて、端末にウイルス対策用のソフトウェアを導入すること。

(ｵ)　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。

(ｶ)　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。

イ　利用者等は、次の事項を遵守しなければならない。

(ｱ)　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、必ずウイルスチェックを行うこと。

(ｲ)　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は、速やかに削除すること。

(ｳ)　ウイルスチェックの実行を途中で止めないこと。

(ｴ)　個別システム管理者が提供するウイルス情報を常に確認すること。

(ｵ)　添付ファイルのあるメールを送受信する場合は、必ずウイルスチェックを行うこと。

(6)　不正アクセス対策

ア　個別システム管理者は、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に対しては、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アカウントは、速やかに削除すること。

(ｳ)　重要な情報システムの設定に係るファイル等について、当該ファイルの改ざんの有無を検査すること。

(ｴ)　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。

(ｵ)　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　利用者等は、不正アクセスを受けた場合は、直ちに情報セキュリティ責任者及び個別システム管理者に連絡し、その指示に従うものとする。

ウ　利用者等から報告を受けた個別システム管理者は、直ちに情報システム管理者に連絡を行い、情報の復旧等必要な措置を講じなければならない。

エ　個別システム管理者は、情報システム（インターネットからアクセス受ける情報システムに限る。（以下、この項において同じ。））については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。

オ　個別システム管理者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講じること。

カ　個別システム管理者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処するとともに、侵入範囲の拡大の困難度を上げる、あるいは、外部との不正通信を検知して対処するといった内部対策を講じること。

キ　センターは、学内ＬＡＮシステムの利用者が閲覧する教職員ポータルサイトを開設するものとする。学内ＬＡＮシステムを使った全学一斉メールの配信については、アカウント管理、セキュリティ対策上不適切であるため、教職員ポータルサイト開設までの間に限るものとし、その後は、ポータルサイトの掲示板機能を用いることとする。

(7)　セキュリティ情報の収集

ア　個別システム管理者は、情報セキュリティに関する情報を収集し、情報システムのソフトウェアに修正プログラムを適用する等、セキュリティ対策上必要な措置を講じるものとする。

イ　情報システム総括責任者は、京都府政策企画部情報政策課から、前項の

情報についての連絡があった場合は個別システム管理者に通知するものとする。

7　運用及び緊急時におけるセキュリティ対策

(1)　情報システムの監視

ア　個別システム管理者は、情報システムの円滑な運用を確保するため、情報システムを定期的に監視し、障害が起きた際は速やかに対応するものとする。

イ　個別システム管理者は、外部ネットワークと常時接続する情報システムについては、ファイアウォール又はネットワーク侵入監視装置の設置など、厳重な監視を行うものとする。

ウ　個別システム管理者は、情報システム内部において、適正なアクセス制御を行い、運用状況について監視を行うものとする。

エ　個別システム管理者は、監視した結果を正確に記録するとともに、消去や改ざんをされないよう必要な措置を講じ、安全な場所に保管するものとする。

(2)　本基準の遵守状況の確認

ア　利用者等は、この本基準に違反した場合又は違反事実を確認した場合は、直ちに情報セキュリティ責任者及び個別システム管理者に報告するものとする。

イ　情報セキュリティ責任者は、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、支障を認めた場合には速やかに個別システム管理者及び情報システム管理者に報告するものとする。

　なお、個別システム管理者が支障を確認した場合には、迅速かつ適切に対処するものとする。

(3)　緊急時対応計画等

ア　個別システム管理者は、情報資産への侵害が発生した場合に備えて、あらかじめ関係機関との連絡体制や復旧対策など緊急時対応計画を策定するものとする。

イ　個別システム管理者は、実際に情報資産の漏えい等の事故が発生した場合に即応できるように体制を整えるものとする。

ウ　個別システム管理者は、情報資産への侵害に起因して、住民に被害が生じるおそれがある場合又は大学の運営に支障が生じると認められる場合には、情報システム管理者に直ちに報告するとともに、関係機関に速やかに連絡するものとする。

エ　個別システム管理者は、情報システムに障害が発生し、情報資産の保持

のために情報システムの停止がやむを得ないと認められる場合には、ネットワークを遮断することができる。

オ　個別システム管理者は、各種セキュリティに関する事案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。

8　評価・見直し

本基準の評価・見直しについては、基本規程第6条の規定による。

附　則

（施行期日）

1　この基準は、平成31年2月4日から施行する。

（京都府立医科大学情報セキュリティ対策基準の廃止）

2　京都府立医科大学情報セキュリティ対策基準（平成19年11月施行）は廃止する。