京都薬科大学　情報セキュリティポリシー

2017 年 4 月 1 日制定

京都薬科大学（以下「本学」という。）における教育及び研究活動を円滑に推進するためには、本学の情報基盤が適正な手続き及び安全な方法で構築・整備され、個人情報を含む情報資産（以下「情報資産」という。）のセキュリティが常に安定的に確保されることが不可欠である。

このため、本学の情報セキュリティ対策の基本的な指針として次のとおり「情報セキュリティポリシー」（以下「本ポリシー」という。）を定める。

Ⅰ．情報セキュリティの基本方針

１．基本理念及び目的

本ポリシーは、本学の情報基盤の確立及び本学の情報資産の管理において、適切な基本的運用方針について定める。

また、本ポリシーに基づき、次のことを達成する。

①本学への情報セキュリティ侵害に対する予防措置

②本学への情報セキュリティ侵害に対する防衛措置

③学内外で行われる情報セキュリティ侵害に対する抑止措置

④情報資産の分類及び管理

⑤物理的、人的及び技術的セキュリティの確保

⑥情報セキュリティの評価と見直し

２．適用対象範囲

本ポリシーは、本学の情報資産を運用・管理する者すべてに適用される。

３．実施方法

本学は、本ポリシーの適用対象者（以下「対象者」という。）が本ポリシー及び関連内規等をよく理解し、適正・的確な情報セキュリティを実行できるように、教育・指導を行う。

また、本ポリシー実行のための対策基準及び実施手順は、本学の実情に即して別途定めることとし、必要に応じて、本ポリシーに反しない範囲において各部局独自の対策基準及び実施手順を作成するものとする。

４．罰則

本ポリシーが形骸化することのないように、本ポリシーに定めた責務に違反した者は、京都薬科大学職員懲戒規程に基づき懲戒処分する。

Ⅱ．対策基準

１．組織体制

本ポリシーの目的を達成する組織体制を確立するため、その役割及び責任を次のとおり定める。

(1) 情報セキュリティ最高責任者

情報セキュリティに関する総括的な意思決定を行う情報セキュリティ最高責任者（以下「CISO」という。）を置く。CISO は学長をもって充て、情報セキュリティに関する施策を定め、それを本学全体に徹底させるために必要な措置を実施する権限を有する。

なお、本ポリシーの解釈については CISO の解釈を以て最終決定とする。

(2) 情報セキュリティ責任者

本学の各領域で保有する情報資産に責任を持つ「情報セキュリティ責任者」を置く。情報セキュリティ責任者は、CISO が指名する情報処理教育研究センター長及び事務局長をもって充て、それぞれの担当領域は、「教育職員に関する範囲」及び「事務職員に関する範囲」とする。

なお、情報セキュリティ責任者は、京都薬科大学情報セキュリティ委員会の委員とする。

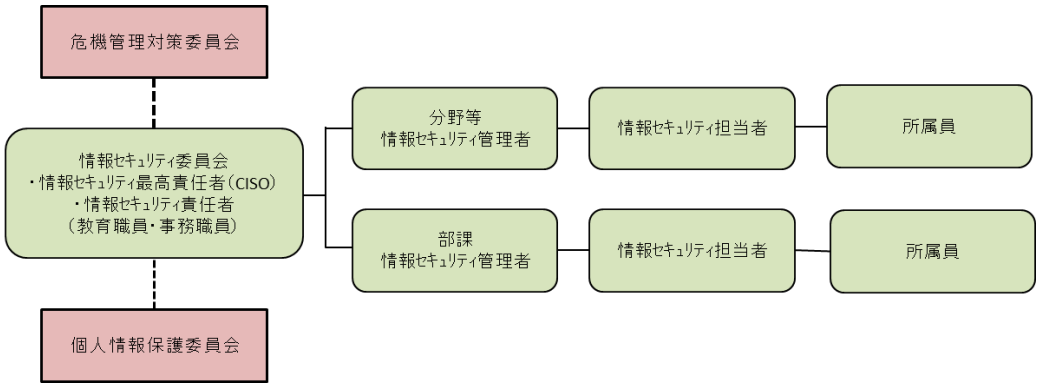
(3) 情報セキュリティ管理者及び情報セキュリティ担当者

部局等（分野、センター及び事務局各課・室をいう。）に情報セキュリティ管理者を置き、部局等の長をもって充てる。各情報セキュリティ管理者は、部局等で保有する情報資産に責任を持ち、かつ、その領域において必要な情報セキュリティ実施手順を策定する。情報セキュリティ管理者の下に「情報セキュリティ担当者」を置き、情報セキュリティの維持・管理のための活動を行う。

(4) 京都薬科大学情報セキュリティ委員会

本ポリシー及び情報セキュリティに関する重要事項を審議し、遵守状況の確認、評価及び見直しを行うとともに、情報セキュリティ上のインシデントが発生した場合は、対応状況の確認並びに必要に応じて助言、指導及び勧告等を行う。

【学内情報セキュリティ対策推進体制図】



２．情報セキュリティ侵害に対する予防及び防衛措置

学内における情報資産への情報セキュリティ侵害に対して、別に定める実施手順に基づき、適切な予防及び防衛措置を講じることにより、情報セキュリティの安定的確保を図る。

３．学内外で行われる情報セキュリティ侵害に対する抑止措置

本学は、対象者に対し、学内外を問わず、あらゆる組織、団体、個人等の情報資産を侵害してはならないことを徹底させる。また、不正なアクセスを阻止するべく必要なアクセス制限を行うとともに、アクセス権限のない情報へのアクセス及び許可されていない情報を利用することを禁じる。

４．情報資産の分類及び管理

本学の情報資産は、それらが果たすべき役割と影響を十分に認識し、「公開情報」、「非公開情報」に分類する。また、その管理は上記分類を踏まえ、その機密性、完全性及び可用性に常に配慮して管理するものとする。

なお、機密性、完全性及び可用性の用語の意義は、次のとおりとする。

①機密性：情報に関して、アクセスを許可された者だけがこれにアクセスできる状態を確保することをいう。

②完全性：情報が破壊、改竄又は削除・変更されていない状態を確保することをいう。

③可用性：アクセスを許可された者が、必要な時に、情報にアクセスできる状態を確保することをいう。

５．物理的セキュリティ

(1) サーバ機器類の管理

サーバ機器類は管理する情報資産の重要性に従い、それぞれ設定された管理区域内に設置し、許可された者以外が使用することができないように必要に応じて、入退室の認証・記録、監視カメラの設置等、物理的なセキュリティを確保することに努めなければならない。

(2) 情報機器並びに記録媒体の管理

本学の重要なデータ及び個人情報が入った情報機器及び記録媒体は無断で学外へ持ち出してはならない。やむを得ず上記を学外へ持ち出す場合は常時携行し、情報漏えいが起こらないようにデータの暗号化等、セキュリティ対策を講じなければならない。また、情報機器及び記録媒体を学内に持ち込む必要がある場合は、ウイルス対策ソフトにてウイルス感染の検査を行う等のセキュリティ対策を講じなければ、持ち込んではならない。なお、情報機器及び記録媒体を破棄する場合は、残存する情報が読み取られないよう対策を講じなければならない。

（注）記録媒体とはFD,CD,DVD,BD（ブルーレイディスク）、フラッシュメモリなどをいう。

６．人的セキュリティ

(1) 職員等の研修・教育

情報セキュリティ最高責任者は、情報セキュリティに関する啓発・教育を実施するために、定期的に必要な措置を講じなければならない。

(2) 事故・障害時の報告とその対応

情報セキュリティに関する事故･障害並びに公開されている情報の改ざん等を発見した

場合は、情報セキュリティ担当者又は情報セキュリティ管理者に直ちに報告しなければならない。報告を受けた情報セキュリティ担当者・情報セキュリティ管理者は、発生した事故・障害等について迅速に対策を講じるとともに、情報セキュリティ責任者に報告し、必要に応じて支援を要請しなければならない。また、重大な被害が発生した場合は、情報セキュリティ責任者は、情報セキュリティ最高責任者に報告し、その指示に従わなければならない。

情報セキュリティ責任者は、発生した情報セキュリティ上の事故等に関する記録を一定期間保存し、情報セキュリティ委員会に報告の上、再発防止のための対策を講じなければならない。

(3) パスワードの管理

自己のパスワードは秘密としなければならない。また、定期的にパスワードを変更する、あるいは推測されにくいパスワードにする等、十分なセキュリティを維持できるように配慮されなければならない。

7．技術的セキュリティ

(1) 不正アクセスなどへの対応

情報セキュリティ責任者は情報資産への不正アクセス防止のための適切な手段を講じなければならない。不正アクセスが検出・確認された場合は通信の遮断又は該当の情報機器類のネットワークからの切り離しなどを実施する。

(2) アクセス制限

情報セキュリティ管理者は情報資産の内容に応じて、アクセス可能な利用者を定めることにより、必要なアクセス制限を行わなければならない。

(3) ネットワークの運用管理

本学の基幹ネットワークについてはファイアウオール及び不正アクセス防止あるいは監視できるシステムを設置し、それらのログを一定期間保存しなければならない。また、情報セキュリティ委員会に許可なく、バックドア（外部ネットワークへの物理的接続、VPN装置及び関連ソフトウエア、不認可クラウドサービス等）を設置することは原則として禁止する。

(4) ネットワーク接続機器の管理

本学ネットワークに接続する情報機器は原則、ウイルス対策ソフトの導入、OSのセキュリティアップデートを行う等、脆弱性の対策を講じたものでなければならない。

(5) 利用記録の保存

個人情報等、非公開情報を管理するサーバなどについて、侵入が試みられていないかなど確認するため、アクセス記録を一定期間保存しなければならない。

8．本ポリシーの評価と見直し

情報セキュリティ上のリスクは、常に変化しているため、情報セキュリティ対策はその変化への対応が必須であることから、常に最新の情報セキュリティ関連の情報を収集し、本ポリシーの評価・見直しを行うとともに、必要に応じて本ポリシーの改訂を行う。

Ⅲ．情報セキュリティ侵害に対する実施手順

１．はじめに

実施手順は、情報セキュリティ侵害に対する予防、防衛及び抑止措置を達成することを目的とし本学の実情を踏まえて策定・運用する。具体的な手順については別途ガイドラインを策定することとする。ここでは各ガイドラインの策定に必要な要件について定める。なお、実施手順については、情報セキュリティ確保の観点から、原則「非公開」とする。

２．学生向け実施手順

学生へのセキュリティポリシー対策は、「ガイダンスによる周知」及び「誓約書の提出」等で実施する。

３．職員向け実施手順

職員に対しては、以下の手順を実施するものとする。

(1) セキュリティガイドラインの配布

セキュリティガイドラインは「セキュリティに関する基本的な知識」、「アカウント管理など個人で行えるセキュリティ対策」、「セキュリティに関するサポート体制」、「罰則」等を含むものとする。

(2) セキュリティに関する誓約書の提出

誓約書はセキュリティガイドラインの趣旨を理解した旨の誓約を行うものであり、情報セキュリティ責任者宛に提出するものとする。

(3) サポート体制

サポート体制及びサポート内容については、学校法人京都薬科大学情報セキュリティ委員会で協議し別途定める。

４．情報セキュリティ管理者向け実施手順

情報資産に関わる運用・保守を行う情報セキュリティ管理者に対しては以下の対策を講じるものとする。

①情報セキュリティ管理者用セキュリティガイドラインの配付

②情報セキュリティ管理者用セキュリティに関する誓約書の提出

なお、情報セキュリティ管理者は情報セキュリティ委員会の勧告するセキュリティ対策を講じ、必要に応じて同委員会の支援を受け、適切なセキュリティ管理を行わなければならない。

以上