○駒澤大学情報セキュリティ基本規程

平成22年４月１日
制定
改正　平成23年４月１日
平成27年４月１日
令和４年４月28日

目次

第１章　総則

（目的）

第１条　この規程は、学校法人駒澤大学情報セキュリティポリシーに基づき、駒澤大学（以下「本学」という。）が所有し、管理する教育・研究・事務活動に不可欠な情報システム及び情報（以下「情報資産」という。）のセキュリティに関する事項を定め、情報資産を適切に保護することを目的とする。

（趣旨）

第２条　この規程は、次の各号を実施するため、関連法規、条約及び本学の各種規程等（学校法人駒澤大学個人情報保護規程を含む）の定めるところによるほか、本学が管理するコンピュータ及びネットワーク等を利用して、情報を扱うにあたり、遵守しなければならない最低限の事項を定める。

(1)　情報資産の分類及び管理
(2)　本学の情報セキュリティに対する侵害の阻止
(3)　学内外の情報セキュリティを侵害する行為の抑止
(4)　情報セキュリティ対策及び利用者への情報セキュリティ教育
(5)　情報セキュリティの評価及び更新

（用語の定義）

第３条　この規程で使用する用語の定義は、次の各号に掲げるとおりとする。

(1)　情報セキュリティとは、情報資産の機密性、完全性、可用性等の維持をいう。

(2)　機密性とは、アクセス権を持つ者だけが、当該情報にアクセスできることをいう。

(3)　完全性とは、情報及び処理方法が正確であること及び完全であることをいう。

(4)　可用性とは、使用を許可された利用者が、必要なときに、情報及び関連する資産にアクセスできることをいう。

(5)　情報資産とは、情報及び情報を管理する仕組み（情報システム、並びにシステムの開発、運用及び保守のための資料等）の総称をいう。

(6)　学内システムとは、学内ネットワークシステム（以下「KOMAnet」という。）及び学内情報システムの総称をいう。

(7)　KOMAnetとは、学内システムのうち、本学の学内LANシステムを構成するネットワーク機器及びメールサーバ等の全学に対するサービスを目的としたサーバ類の総称であり、学内LANの情報コンセント等に接続されたサーバ、パソコン等の端末はこれに含まない。

(8)　学内情報システムとは、学内システムのうち、本学の教育支援にかかわるシステム、事務処理にかかわるシステム、Webサーバ、データベース等の情報システムの総称をいう。

(9)　その他の用語は、平成12年７月18日の「情報セキュリティポリシーに関するガイドライン」（情報セキュリティ対策推進会議決定）に準拠する。

（対象範囲及び対象者）

第４条　本規程の適用範囲及び対象者は、次の各号に掲げるとおりとする。

(1)　本学が所有し管理するすべての情報資産並びに本学との契約等に従って提供されるもの及び本学の情報資産に一時的にアクセスするための情報システム

(2)　KOMAnetに接続された情報機器

(3)　本学の情報資産にかかわる外部委託業者等の本学以外の組織及び人員を含むすべての関係者又は関係のあった者

(4)　その他、前各号に準ずる情報機器及び関係者

（実施手順）

第５条　この規程の実施手順については、本学の規程及び内規等により別に定める。

（組織及び体制）

第６条　本学の情報セキュリティを適切に確保するための組織及び体制は、次の各号に掲げ

るとおりとし、組織体制図は別表のとおりとする。

(1)　情報セキュリティポリシーに基づく総括的な意思決定及び学内外に対する責任を負う者として、最高情報セキュリティ責任者を置く。最高情報セキュリティ責任者は、学長をもって充てる。

(2)　最高情報セキュリティ責任者を補佐し、情報セキュリティ対策の実施に関し、総括的な対応に当たる者として、情報セキュリティ実施責任者を置く。情報セキュリティ実施責任者は、教育・研究担当副学長をもって充てる。

(3)　最高情報セキュリティ責任者を補佐し、情報セキュリティの管理・運営に関し、緊急時の連絡等、総括的な対応に当たる者として、情報セキュリティ管理責任者を置く。情報セキュリティ管理責任者は、総務局長をもって充てる。

(4)　情報セキュリティ対策が情報セキュリティポリシーに基づき実施されているか監査するものとして、情報セキュリティ監査責任者を置く。情報セキュリティ監査責任者は、学長が指名する者をもって充てる。

(5)　各部署における情報セキュリティの実施と責任を有する者として、各部署に情報セキュリティ管理者を置く。情報セキュリティ管理者は、各部署の長（各学部長等、各研究科委員長、大学院法曹養成研究科長及び各研究所の所長並びに各事務部署の長）をもって充てる。

(6)　学内システムの情報資産を管理する者として、情報システムを運用している各部署にシステム管理者を置く。システム管理者は、当該システムを運用する部署の長が指名する。KOMAnetについてはKOMAnet管理者を総合情報センターに置く。KOMAnet管理者は、総合情報センター所長が指名する。

(7)　学内における情報セキュリティに関する技術的な対応を行う部署として、総合情報センターが当たる。総合情報センターは、利用者への情報セキュリティ教育を行うほか、部署内に情報セキュリティ対策チーム（以下「CSIRT」という。）を設置し、不正アクセス等のサイバー攻撃によるセキュリティ事故が発生した際の学内の緊急対応窓口として、情報セキュリティ実施責任者の指示を受け、調査・対応活動を行う。

(8)　本学の信用にかかわる重大な情報セキュリティの問題は、最高情報セキュリティ責任者の判断によって、駒澤大学危機管理委員会でこれに対処することができる。

2　情報セキュリティポリシーの実施、点検、改善及び策定に関して、次の各号に掲げる事項は、駒澤大学情報システム委員会（以下「システム委員会」という。）で審議する。

(1)　情報システムに係る情報セキュリティ対策に関する事項

(2)　情報セキュリティ対策及び実施基準の策定等に関する事項

(3)　情報セキュリティにかかわる事件・事故の調査・分析及び再発防止策の立案に関する事項

(4)　情報セキュリティにかかわる啓発活動の実施に関する事項

(5)　その他情報セキュリティに関し必要な事項

(6)　システム委員会の構成・運用については別に定める駒澤大学情報システム委員会規程による。

第２章　情報資産の管理及び分類

（情報資産の管理者）

第７条　情報セキュリティ対策に基づく情報資産の管理は、KOMAnetについてはKOMAnet管理者が、学内情報システムについては当該システムのシステム管理者が、個人が管理する情報機器については使用者が行わなければならない。

（情報の分類及び格付けの指定）

第８条　この規程の対象となるすべての情報のうち閲覧できる者を限定した情報を非公開情報、情報の利用者すべてに閲覧を許可する情報を公開情報と称し、そのいずれかは、情報資産の情報セキュリティ管理者が決する。なお、非公開情報については、情報格付け及び取扱制限に関する規程に定める格付けを指定し、取扱方法を区別して管理しなければならない。

（情報資産の管理）

第９条　情報資産の管理者は、情報の機密性、完全性及び可用性を維持するため、情報を管理する仕組みの物理的、技術的及び人的なセキュリティ対策を講じなければならない。

（知的財産権等）

第10条　情報資産の管理者は、情報を作成するに際し、著作権等の他者の知的財産権を侵していないことを確認しなければならない。ただし、非公開情報を限定された第三者に開示する必要がある場合は、開示の都度、守秘義務契約を結ばなければならない。

（情報機器及び記憶媒体の処分）

第11条　情報資産の管理者は、情報機器又は記憶媒体を廃棄する場合は、非公開か公開かにかかわらず、適正に処分しなければならない。

２　情報機器若しくは記憶媒体を保守契約によって交換する場合、又はレンタル機器若しくはリース機器の撤去を行う場合も適正に処理しなければならない。

第３章　物理的セキュリティ

（パソコン端末機器及びネットワーク設備）

第12条　システム管理者は、システム管理者から許可を得ていない者が機器又は設備を使用できないよう方策を講じなければならない。

２　システム管理者は、機器及び設備の所在及び使用の記録を保存しなければならない。

３　システム管理者は、端末機器及びネットワーク設備に対し、災害、事故及び情報機器の盗難等を防止する対策を講じておかなければならない。

（ネットワーク機器及びサーバ等）

第13条　ネットワーク機器及びサーバ等は、その重要度に応じたセキュリティ対策の施された管理場所に設置しなければならない。停止したときに大学内の業務遂行に重大な支障をきたす重要なネットワーク機器及びサーバ等に対しては、認証及び入退室の記録を残さなければならない。

２　サーバ等に記録される情報は、その重要度に応じて定期的にバックアップを行わなければならない。

３　情報を保存するサーバ等、及び情報をバックアップした記憶媒体には、火災、地震等の災害、事故及び盗難等の犯罪から守るための対策を講じなければならない。

４　重要なネットワーク機器及びサーバ等については、故障、停電等の事故の際、迅速に回復ができる体制を整えておかなければならない。

第４章　技術的セキュリティ

（アクセス管理）

第14条　システム管理者は、情報機器を不正なアクセス等から保護するため、情報機器へのアクセス制御及びネットワーク管理についての対策を講じなければならない。ただし、この対策によって課される制限が教育研究上の利便性及び可用性を過剰に損なうことは避けなければならない。

２　システム管理者は、KOMAnetに接続されている情報機器にアクセスする者の利用が認証によって許可される仕組みを構築しなければならない。

（アクセス記録）

第15条　システム管理者は、管理する情報機器のアクセス記録の盗難、改ざん、消去等を防止する処置を講じて、一定期間保存しなければならない。

２　システム管理者は、不正使用の疑いに基づき情報セキュリティ管理者からその対策に必要なアクセス記録を求められたときは、提出に協力しなければならない。

（コンピュータウイルス及びスパイウェア対策）

第16条　システム管理者は、不正アクセス、コンピュータウイルス、スパイウェア等、情報システムの運用を妨害し、情報を漏えいしようとする攻撃行為から情報資産を守るために必要な対策を講じなければならない。

2　ファイル共有ソフトは、KOMAnet管理者が許可した場合を除き、使用してはならない。

3　情報資産を扱うパソコン又はサーバ等がつながった情報機器では、ファイル共有ソフトを使用してはならない。

4　ファイル共有ソフトによって作成されたファイルを情報資産を扱うパソコンで利用する場合は、事前にそのデータの検疫を完全に行った後でなければ利用してはならない。

5　ネットワーク上の情報を収集するような監視ソフト、ネットワークの状態を探索するセキュリティ関連ソフト又はハッキングソフトは、使用してはならない。ただし、深刻な障害や外部からの攻撃等の対策のために必要であり、情報セキュリティ実施責任者の指示のもとに行う場合は、この限りでない。

（非公開情報流出への対策）

第17条　本学の情報資産を利用する者は、情報セキュリティ管理者が許可した場合を除き、非公開情報の学外への持ち出し及び非公開情報への学外からのアクセスをしてはならない。

2　情報セキュリティ管理者の許可を得た上で、非公開情報を学外に持ち出し又は学外からアクセスする場合は、情報を暗号化する等盗難、紛失、盗聴等による情報流出を防ぐための対策を講じなければならない。

第５章　人的セキュリティ

（遵守事項）

第18条　本学の情報資産を利用する者は、この規程を遵守し、意図の有無にかかわらず、学内外の情報資産に対する権限のないアクセス、改ざん、複写、破壊、漏えい等をしてはならない。

2　KOMAnet管理者及びシステム管理者は、責任をもって個々の情報システムのセキュリティ維持に努めなければならない。

（教育及び研修）

第19条　総合情報センターは、教職員等に対してこの規程に関する研修会等を実施しなければならない。

2　本学の教職員等及び学生は、研修会、説明会、講義等を通じて、この規程を理解し、情報セキュリティ上の問題が発生しないように努めなければならない。

（ユーザID及びパスワードの管理）

第20条　利用者は、ユーザID及びパスワードの管理に際し、学内ネットワーク利用規程に定める事項を遵守しなければならない。

（システム管理者のアカウント及びログの管理）

第21条　情報機器及びネットワーク設備は、許可された目的以外で利用してはならない。

２　情報セキュリティ管理者は、情報システムの利用資格者を定めなければならない。

３　システム管理者は、利用資格を有する者以外に情報システムのアカウントを発行してはならない。

４　システム管理者は、利用資格を失った者のアカウントを速やかに除去しなければならない。

５　システム管理者は、いかなる場合にも利用者からのパスワードの聞き取りを行ってはならない。

６　システム管理者は、ログ情報又は通信内容の解析等にあたっては、利用者のプライバシーに配慮し、閲覧解析を認める場合の要件及び手続きを定めなければならない。

（個人情報の保護と例外）

第22条　情報セキュリティ管理者及びシステム管理者は、アカウント、パスワード、ログ情報及びその他の情報システムに関して、必要性がないにもかかわらず個人情報及びプライバシー情報の収集を命じたり、自ら収集をしてはならない。

２　情報セキュリティ管理者及びシステム管理者は、業務上知り得た個人情報及びプライバシー情報は、在職中及び退職後も他者に口外してはならない。ただし、システム管理者は、セキュリティ保持にかかわる正当な理由がある場合には、その理由を駒澤大学個人情報取扱実施規程第３条に規定する個人情報システム管理者に申告し、対応を相談した後に、情報セキュリティ実施責任者の許可を得て、個人情報をセキュリティ障害回避に使用することができる。

（外部委託）

第23条　情報システムの開発及び保守並びにシステム管理業務を委託業者に発注する場合は、契約書面にこの規程及び第５条に定める実施手順の遵守を明記しなければならない。

第６章　運用

（情報システムの運用管理状況及び規程の遵守状況の確認）

第24条　各情報システムのシステム管理者は、情報システムが安全に稼動していることを監視し、この規程が遵守されるよう、担当する情報システムを運用しなければならない。

（事故及び障害等の報告）

第25条　本学の教職員は、情報セキュリティに関する事故、情報システムの不審な動作、情報の改ざん、システム上の障害、欠陥又は誤動作を発見し、又は報告を受けたときは、直ちに所属長又は上位の管理者に報告するとともに当該システムのシステム管理者へ報告しなければならない。

2　学生又はその他の者が発見したときは、教職員に直ちに報告しなければならない。

3　システム管理者は、報告のあった事故等について必要な措置を直ちに講じなければならない。報告のあった事故等が、情報システムへの攻撃の可能性があると思われるときは、速やかにCSIRTへ報告しなければならない。

4　情報セキュリティ管理者は、発生した事故等に関する記録を一定期間保存し、システム委員会に報告しなければならない。

5　情報セキュリティ管理者は、緊急を要する重大な事故については、システム管理者に被害拡大防止のための対策を迅速に講じるよう指示するとともに、速やかに情報セキュリティ実施責任者に報告しなければならない。

6　情報セキュリティ実施責任者は、前項の報告を受けたときは、速やかに最高情報セキュリティ責任者及び情報セキュリティ管理責任者に報告するとともに、CSIRTへ発生事象の確認と被害状況等の調査を指示し、情報システム内のデータの盗難、改ざん、破壊などの情報システムへの攻撃（以下、「サイバー攻撃」という。）によるものであるかを確認する。

7　CSIRTは、前項の報告事案がサイバー攻撃によるものと認知したときは、情報セキュリティ実施責任者の指示を受け、発生事象の正確な把握を行い、被害拡大防止、復旧及び再発防止のための対策を講じ、その状況を情報セキュリティ実施責任者に逐次、報告しなければならない。なお、CSIRTは外部機関に調査を委託することができる。

8　最高情報セキュリティ責任者は、情報セキュリティ実施責任者からサイバー攻撃の報告を受けたときは、事案の発生した経緯及び被害状況等の調査結果を確認し、情報セキュリティ管理責任者へ、事案の内容及び影響等に応じて、事実関係及び再発防止策の公表並びに当該事案に係る対外対応等の措置を講じるよう指示する。

（不正アクセス）

第26条　システム管理者は、学内又は学外から不正アクセスについての報告又は依頼を受けたときは、情報機器の不正アクセスの調査を早急に行わなければならない。

2　KOMAnet管理者は、外部又は内部からの不正アクセスを確認したときは、第５条に定

める実施手順に従って関連する通信の遮断又は該当する情報機器の切り離しを実施しなければならない。不正アクセスが継続するときは、所定の手続きに基づき、当該情報機器又はそれを接続するネットワークのシステム管理者に対して事態を警告し､対策をとるよう勧告しなければならない。なお、定常的な利用を停止する等の抑止措置をとることができる。

3　対策手順の定めのない行為によって情報セキュリティが阻害されたときは、KOMAnet管理者の判断によって緊急に対処し、その内容を情報セキュリティ実施責任者及びCSIRTに報告する。

4　本学の教職員又は学生が不正アクセスを行ったときは、学則、就業規則又はその他の諸規則に従って処分を受けることがある。

5　重大な情報セキュリティの問題については、システム委員会に諮り、発生した不正行為の内容及び対処を情報セキュリティの損なわれない範囲で公表する。

（監査）

第27条　情報セキュリティ監査責任者は、情報資産の管理の状況について、定期に、又は随時に監査を行い、その結果を、最高情報セキュリティ責任者、情報セキュリティ実施責任者及び情報セキュリティ管理責任者に報告するものとする。

2　情報セキュリティ監査責任者の事務及び情報セキュリティの管理状況の監査事務の所管は、内部監査室とする。

（評価及び更新）

第28条　システム委員会は、この規程に関する点検及び評価のために次の各号の情報収集と定期的点検に努めなければならない。

(1)　本学の教職員等及び学生からのこの規程の遵守に関する意見及び実施運用上の要望又は苦情

(2)　事故、故障及び不正行為の事例、対策の成功事例、並びにシステム管理者からの意見及び要望

(3)　この規程の実施状況についての点検及び監査の結果

(4)　学内システムの機密性、完全性、可用性等、並びに犯罪予防の観点からの情報セキュリティ診断結果

2　システム委員会は、前項の情報を基にこの規程の実効性を評価し、よりセキュリティレベルが高く、かつ、遵守可能な規程に更新しなければならない。

3　CSIRTは、点検及び評価の結果を本学の教職員等及び学生に提示して啓発しなければ

ならない。

（改廃）

第29条　この規程の改廃は、システム委員会及び全学教授会の議を経て、学長がその意見を聴き、これを行う。

附　則

この規程は、平成22年４月１日から施行する。

附　則

この規程は、平成23年４月１日から施行する。

附　則

この規程は、平成27年４月１日から施行する。

附　則

この規程は、令和４年４月１日から施行する。

別表　駒澤大学情報セキュリティ組織体制図