文京学院大学

情報セキュリティポリシー
実施ガイド

文京学院大学
情報教育研究センター

はじめに

　文京学院大学では、情報システムや情報資産の利用を安全に行うため、情報資産等の重要度に応じて分類し、適切に利用・保護するために情報セキュリティポリシーを定めています。本学において情報システムや情報資産の利活用を行う場合は、このポリシーを遵守する必要があります。

　本資料は、文京学院大学における情報セキュリティポリシーについてまとめた資料です。

　本書の各章には、次の内容が記載されています。ポリシーを理解し、適正な情報資産の利活用を行うようにしてください。

第一章　情報セキュリティポリシー

　本学における情報セキュリティを定める規程です。本学の管理するコンピュータ、ネットワーク等を利用し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まとめたものです。
　本学の規程からの抜粋です。

第二章　情報セキュリティポリシー基本方針

　本学における情報セキュリティの基本方針を示しています。セキュリティ動向に従って変更されないような普遍的 且つ 基本的に定める方針が記載されています。

第三章　情報セキュリティ対策基準

　本学の保有する「情報資産」に対するセキュリティ保護対策を示しています。情報セキュリティポリシー基本方針同様に、基本的な事項のみを示しています。詳細については、別に定める各種ガイドラインにより取り扱います。

第一章 情報セキュリティポリシー

目次

Ⅰ.情報セキュリティの基本方針

1. 情報セキュリティの基本方針

情報は文京学院大学（以下、本学）にとって重要な資産である。本学における研究・教育活動は、情報の収集・分析・保管・伝達・報告といった手段に依存しており、情報資産が保全されなければ、本学の研究・教育活動の停滞、本学に対する信頼の喪失などといった被害を受ける可能性がある。従って、教職員、学生、及びすべての関係者は情報資産の保全に努めなければならない。

本学の提供するサービスの利用者は、情報セキュリティポリシー（以下、ポリシー）を遵守しなければならず、学内外の情報資産に対する権限のないアクセスや改竄、複写、破壊、漏洩等を行ってはならない。

2. 趣旨・位置付け

ポリシーは下記のとおりの設置目的をもって、本学の管理するコンピュータ、ネットワーク等を利用し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まとめたものである。詳細は関連法規、条約、本学の各種規程、ならびに内規等に従うものとする。

1）本学の情報セキュリティに対する侵害の阻止
2）学内外の情報セキュリティを侵害する行為の抑止
3）情報資産の分類と管理
4）情報セキュリティの評価と更新

3. 定義

用語の定義は、情報セキュリティ対策推進会議が定めた「情報セキュリティポリシーに関するガイドライン」にあるものと同様とする。

http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html

情報資産の定義は、情報ならびに情報を管理する仕組みとする。

4. 対象範囲・対象者

本学におけるポリシーの対象範囲は、本学の管理する機器、ネットワーク、一時的にネットワークに接続された機器、及び情報資産である。ポリシーの対象者は本学の情報資産を利用する全てのものである。

5. 実施手順

ポリシーの実施手順は、本学の規程、内規等によって別途定めるものとする。

6. インシデント対応

インシデント対応に関する基本方針は、別途定めるものとする。

Ⅱ.対策基準

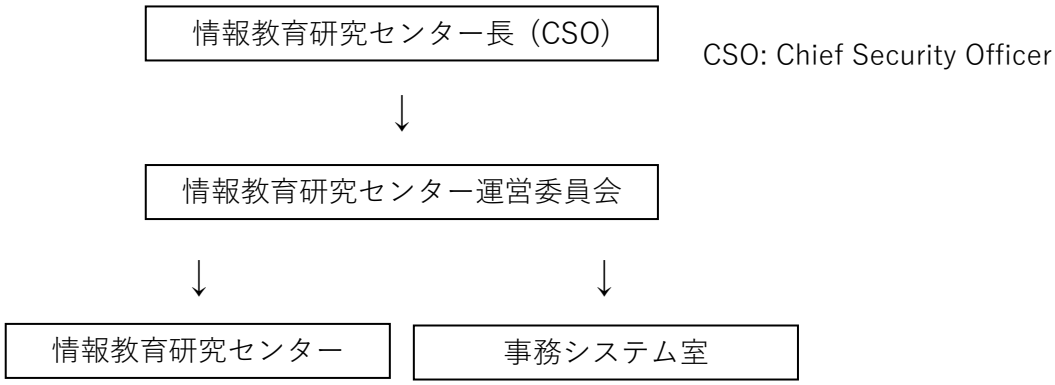
1. 実組織・体制

本学の情報セキュリティ管理の責任者を情報教育研究センター長として、情報セキュリティに関する総括的な意思決定を行い、学内外に対する責任を負うものとする。情報セキュリティに関する管理運営は、情報教育研究センターが行うものとする。

ポリシーの策定ならびに重要事項の決定は情報教育研究センター運営委員会（以下、委員会）が行うものとする。システム管理者は、システム管理の実施、緊急時の対応等にあたるものとする。情報セキュリティに関する啓発および教育については委員会が担当し、一般の利用者に対する幅広い教育を行う。

尚、自主管理ドメインについては当面認めないこととする。

＜体制＞



2. 情報セキュリティの侵害の阻止

1）不正アクセス等への対応

外部または内部からの不正アクセスが検出された場合、本学のネットワーク管理者は、緊急措置手順に従って関連する通信の遮断または該当する情報機器の切り離しを実施する。不正アクセスが継続する場合には、所定の手続きに基づいて、当該情報機器又はそれを接続するネットワークに対し、事態を警告し、対策をとるよう勧告し、さらには、定常的な利用を停止するなどの抑止措置をとることができる。

2）アクセス制限

情報の内容に応じて、アクセス可能な利用者を定め、不正なアクセスを阻止すべく必要なアクセス制限を行わなければならない。利用者はアクセス権限のない情報にアクセスしたり、許可されていない情報を利用したりしてはならない。

3. 学内外の情報セキュリティを侵害する行為の抑止

学内外を問わず、あらゆる研究・教育機関、企業、組織、団体、個人等の情報資産を侵害してはならない。また、情報セキュリティに関連する諸法規、条約ならびに本学が定める規程等を遵守しなければならない。

4. 情報資産の分類と管理

本学の提供する情報に関しては、その情報の正確性と健全性に配慮し、利用者が被害を受けるいかなる情報も扱ってはならない。情報提供の際には、関連する諸法規、条約ならびに本学が定める規程等を遵守しなければならない。

1）情報資産の管理者

本学の管理する機器に保存された情報は、本学のシステム管理者が管理しなければならない。本学の管理するネットワークに個人の機器を接続した場合、当該機器内の情報は、その機器の管理者と利用者が管理しなければならない。

2）非公開情報資産

個人情報、事務、研究・教育等の非公開情報を不当に利用してはならない。
権限のない情報に対してアクセスを行ったり利用したりしてはならない。情報の盗難・漏洩等を防止するため、非公開情報を扱うネットワークは、暗号化などを実施することが望ましい。また、情報が記録された媒体は、適切に管理されなければならない。

3）限定公開情報資産

特定の利用者に特定の情報を公開する場合、情報の登録、閲覧に際して、認証、アクセス制御等を実施しなければならない。非公開情報を扱う場合と同じく、ネットワークは、暗号化などを実施することが望ましい。さらに、異常な登録、閲覧および操作が行われていないか、定期的に調査・確認しなければならない。

4）公開情報資産

公開情報を不当に利用してはならない。情報は改竄、破壊されないように適切に管理されなければならない。非公開情報を公開する場合には、個人情報の漏洩、プライバシー、著作権や肖像権の侵害に十分注意し、公開できる情報だけを抽出し、公開してよい形に加工しなければならない。情報が記録された媒体は、適切に管理されなければならない。

5）扱いに注意が必要な公開情報資産 3

本人の許可なく、その顔や容姿などを撮影しその写真や動画を公開すると、肖像権の侵害と扱われる可能性に注意しなければならない。また、風景写真、動画に有名人など人物が写り込んでいる場合も、肖像権の侵害と扱われる可能性に注意しなければならない。

6）情報機器及び記憶媒体の処分

非公開・限定公開・公開を問わず、情報機器及び記録媒体を破棄する場合は、実施手順に従わな

ければならない。

5. 情報セキュリティならびにポリシーの評価と更新

1）情報セキュリティの評価と更新

本学の情報資産を守るために、委員会は常に最新の情報を取得し、適切な物理的・技術的・人的セキュリティが実施されているか、定期的に評価・調査・監査を実施しなければならない。改善が必要と認められた場合、委員会は速やかに情報セキュリティの更新を行わなければならない。

2）ポリシーの評価と更新

情報セキュリティの調査とともに、ポリシーの実効性を定期的に評価し、改善が必要と認められた場合には、委員会は変更内容及び実施時期の決定を行い、セキュリティレベルの高い、かつ遵守可能なポリシーに更新しなければならない。

附則

本ポリシーの改正は、情報教育研究センター運営委員会が作成し、全学教授会の議を経て理事会が決定するものとする。

【改訂履歴】

本ポリシーは、平成２４年４月１日から施行する。

本ポリシーは、平成２６年４月１日から施行する。

第二章　情報セキュリティ基本方針

目次

1　背景・目的

本学は、「自立と共生」をその教育の根幹に据え、社会人基礎力の育成と知の先導者としての大学の持つ社会的責任を果たすべく様々な取り組みを行っている。今後は、学生の個性の伸長や地域社会の貢献のためにも、多面的な情報資産の活用が必須となる。従って、大学の経営戦略にとっても、大学の所有する情報資産の可用性・機密性・完全性、すなわち情報セキュリティの確保には、これまで以上の重要性が生じることは明白である。

以上の趨勢を鑑みて、本学では、その構成員全てに対し、情報資産の持つ価値とその保全の重要性を認識すべく、遵守すべき内容を記載した情報セキュリティ基本方針を策定し、広く周知することとする。

2　情報セキュリティ基本方針

本学は、本学が所有するすべての情報資産に関して、下記の点にわたって、適切なセキュリティを保障する義務と責任を有する。

(1) 本学の情報資産に対する攻撃により、その適正な運用が妨げられることを防御すること。
(2) 本学の情報資産への侵害から利用者を守ること。
(3) 本学の情報資産の利用者が、その意図の有無を問わず、学内外の情報資産に対する加害者となることを防止すること。
(4) 本学の情報資産の利用者が、基本方針、対策基準、各種ガイドライン及び各種内規等を理解し遵守できるよう、教育・研修などをとおして啓発に努めること。
(5) 本学の情報資産を保護するため、情報教育研究センター運営委員会により本学における情報セキュリティの運営及び管理を行うこと。

3　本文書の位置付け

本文書は、本学における情報セキュリティの基本方針を示すものであり、本学の情報資産を利用し、情報を扱うにあたって、遵守しなければならない最低限の事項をまとめたものである。本学のすべての構成員は情報資産の使用権限に応じてセキュリティ管理について義務と責任を負う必要があるが、詳細

第二章　情報セキュリティ基本方針

は関連法規、条約、本学の各種規定ならびに対策基準、各種ガイドラインに従うものとする。

4　適用範囲ならびに適用対象者

本学における本文書の適用範囲は、本学の所有するすべての情報資産ならびに本学が管理する機器、ネットワーク、及び一時的にネットワークに接続された機器である。

本文書の適用対象者は、本学の学生、教員、職員等、本学の情報資産を利用するすべての者とする。

5　用語の定義

本文書において使用する用語の定義は、次のとおりである。

- 情報セキュリティ

  情報資産の完全性（情報及び処理方法の正確さ及び完全である状態を安全防護すること)、機密性（情報にアクセスすることが認可されたものだけがアクセスできることを確実にすること)、及び可用性（許可された利用者が、必要な時に情報にアクセスできることを確実にすること）を維持すること。

- 情報資産

  情報（個人情報を含む）及び情報を管理する仕組み（情報システムならびにシステム開発、運用及び保守のための資料等）の総称。

その他用語の定義は、情報セキュリティ対策推進会議で定められた「情報セキュリティに関するガイドライン（総務省高度情報通信社会推進本部に設置された情報セキュリティ対策推進会議において定めたガイドライン＜平成 12 年 7 月 18 日＞)」にあるものと同様とする。

6　情報セキュリティ対策基準

本学において、別に定める。

7　情報セキュリティ実施手順書

本学において、別に定める。

8　情報セキュリティ管理体制

本学において、別に定める。

附則

本基本方針の改正は、情報教育研究センター運営委員会の議を経て決定する。
本基本方針は平成 29 年 4 月 1 日より施行する。

【改訂履歴】
平成 29 年 4 月 1 日　制定

第三章　情報セキュリティ対策基準

目次

1　目的

情報セキュリティ対策基準（以下、「対策基準」という）は、文京学院大学（以下、「本学」という）の情報セキュリティ基本方針に基づき、本学の情報資産が、流出や改ざん、破壊から保護され、定められた方法で常に利用できることと共に、セキュリティを常に確保した状態で情報資産が管理されることで教員及び職員が安全に情報資産を利用できることを担保し、本学において、情報資産及び情報システムの適正な使用により本学の安定的な運営に寄与することを目的とする。

2　基本的な考え方

本対策基準は、情報のセキュリティを確保した状態で本学の情報資産を利用するために必要となる各種ガイドラインを策定するにあたり、踏まえるべき基本的な基準を記載する。各種ガイドラインの策定は、~~十~~個人情報保護法及び不正アクセス防止法、情報セキュリティに関連する各種法令に則ったリスクアセスメントの結果と本基準をもとに定義する。

昨今の情報技術の進展の速さ及び情報管理に対する社会的な要求の変化の急激さを考慮すると、一時点における情報セキュリティ確保のための画一的な基準を策定する作業は困難であり、かつ、有意性の薄い作業であるとも考えられ得る。そのため、「情報セキュリティ手順書」に則り、本基準も含めて各種ガイドラインの見直しを適宜実施する。

3　適用範囲

本対策基準及び各対策ガイドラインは、に所属するすべての情報資産ならびに本学の情報資産を利用するすべての教員及び職員に対して適用するものとする。ただし、学生については、別に定める学生向け対策基準を適用するものとする。

4　用語の定義

本文書において使用する用語の定義は、次のとおりである。

4.1　「完全性」とは、情報及び処理方法の正確さ及び完全である状態を安全防護することをいう。

4.2　「機密性」とは、情報にアクセスすることが許可された者だけが許可されたものだけがアクセスできることを確実にすることをいう。

4.3　「可用性」とは、許可された利用者が、必要な時に情報にアクセスできることを確実にすることをいう。

4.4　「情報セキュリティ」とは情報資産の完全性、機密性及び可用性を維持することをいう。

4.5　「アクセスコントロール」とは、情報の内容に応じて、情報にアクセス可能な利用者を定めることをいう。

4.6　「オペレーティングシステム」とは、入出力機能やディスクやメモリの管理など、多くのアプリケーションソフトから共通して利用される基本的な機能を提供し、コンピュータシステム全体を管理するソフトウェアのことをいう。

4.7　「コンピュータウィルス」とは、第三者のプログラムやデータベースに対して意図的になんらかに被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能を一つ以上有するものをいう。

4.8　「コンプライアンス」とは、守られるべき倫理や行動規範なども含んだルールを遵守し、社会秩序を乱す行動や社会から非難される行動をしないことをいう。

4.9　「情報資産」とは、情報（個人情報を含む）予備情報を管理する仕組み（情報システムならびにシステム開発、運用及び保守のための資料、等）の総称をいう。

5　対策基準

対策基準では、各種ガイドラインを策定するにあたり基準となる事項を示す。情報教育研究センター運営委員会は、個人情報保護法及び不正アクセス防止法、情報セキュリティに関連する各種法令に則ったリスクアセスメントの結果及び以下の基準に基づき、情報資産保護のための各種ガイドラインを策定する。各種ガイドラインでは、リスクの大きさや特徴に対して、リスクの許容、リスクの低減、リスクの移転、リスクの回避等の管理方法を決定し、対策を規定する。

(1) 情報機器等の学外持出、学内持込に関する基準

（ア） 本学外へ重要な情報資産を可搬可能な媒体に入れ持ち出す場合は、持出手続を取った上で本学外へ持出した情報資産が適切に取扱われなければならない。

（イ） 情報の利用権限の無い者への情報の開示、情報の利用権限の無い者による情報の変更、窃取を防止するため、情報資産の持出状況について把握し、管理しなければならない。

（ウ） 情報資産の流出を防止するため、本学以外の組織との情報のやり取りを可能な限り管理しなければならない。

（エ） 情報の利用権限の無い者への情報の開示、情報の利用権限の無い者による情報の変更、窃取を防止するため、モバイルコンピューティング又は在宅勤務等本学の物理的セキュリティが有効でない場所からアクセスする場合に必要な対策を明確にし、利用者は当該の対策を講じなければならない。

（オ） 情報の利用権限の無い者への情報の開示、情報の利用権限の無い者による情報の変更、窃取を防止するため、私有するコンピュータ機器及び可搬媒体の持込について把握し、管理しなければならない。

（カ） ネットワーク上の不正アクセス、ネットワーク障害を防止するため、私有するコンピュータの学内ネットワークへの接続状況を把握し、管理しなければならない。

（キ） 不正なソフトウェアの利用、コンピュータの誤作動を防止するため、私有するソフトウェアを本学内のコンピュータへ利用、インストールすることを把握し、管理しなければならない。

(2) 情報資産の収集、利用、管理に関する基準

（ア） 収集した情報資産の流出、誤用を防ぐため、情報資産の収集を行う際は、情報資産の利用目的を明確にした上で、収集について管理を実施しなければならない。

（イ） 可搬可能な装置及び電子記録媒体に記録されている情報の漏洩、改ざん、破壊を防止するため、可搬可能な装置及び電子記録媒体に記録された情報資産の利用、保管、破棄について管理を実施しなければならない。

（ウ） 情報システムの不正利用を早期に発見し、不正利用に起因する悪影響を最小化するため、情報システムの利用状況を正しく記録し、監視を実施しなければならない。また、記録された利用状況は、定期的に確認しなければならない。

（エ） 情報システムの保守やシステム監査等、通常業務とは別の目的で情報システムを利用する場合においても、情報システムの信頼性及び安全性を確保しなければならない。

（3）啓発、教育に関する基準

（ア） 本学の関係者の情報保護への認識不足から情報が漏洩、改ざん、破壊されることを防止するため、本学の関係者へ情報保護に関わる教育、訓練を実施しなければならない。

（イ） 本学内外での本学関係者によるインターネット使用での情報流出による本学ブランド及びイメージの低下を防ぐため、個人及び本学でのインターネット使用に関わる本学関係者への教育を実施し、インターネットリテラシーの向上を図らなくてはならない。

（ウ） 学内システムの利用の習熟を図り、誤操作、機器の取り扱いの不備でシステムに重大な損害を与えることを防ぐため、学内システム利用に関する教育を実施しなければならない。

（4）コンプライアンスに関する基準

（ア） 本学の関係者の情報保護に関する法令及び学内規定等に確実に準拠しなければならない。

（5）学内システムに関する基準

（ア） 新規に開発、あるいは変更を加える情報システムにおいて、必要な情報セキュリティを確保するため、必要なセキュリティ要件を明確にし、その要件を確実にシステムに反映しなければならない。

（イ） 情報システムの信頼性及び完全性、可用性を確保するため、運用手順及び障害対応手順等の運用手続きに関する実施手順書を作成し、それに準拠した運用を実施しなければならない。

（ウ） コンピュータウィルス及び悪意ある第三者の攻撃により情報システムで取扱う情報の完全性及びシステムの可用性を損なうことを防止するため、コンピュータウィルスへの感染や、悪意ある第三者の攻撃を予防しなければならない。また、コンピュータウィルスに感染した場合又は悪意ある第三者からの攻撃を受けた場合、被害を最小化するための対応を実施しなければならない。

（エ） 学外からネットワーク経由で学内システムに接続する場合、通過するデータの機密性及び完全性を保護しなければならない。

(6) アクセスコントロールに関する基準

（ア） 情報資産及び情報資産の設置場所には、その情報資産の盗難及び物理的な破壊等による被害を防止するために、物理的なアクセスコントロールを実施し、アクセスは必要最低限の要員に限定しなければならない。

（イ） 情報へのアクセスコントロールについては、本学が正当と認める利用者が業務上の必要性に応じて確実に必要な情報へアクセスできるとともに、業務上の必要性がなく、情報を利用する権限のない者の情報へのアクセスを防止するため、業務上必要な情報へのアクセス者を明確に定め、その定めに沿って情報へのアクセスの権限を付与しなければならない。

（ウ） 情報へのアクセス権限の付与を確実に行うため、管理者の登録及び管理者への権限の付与を行わなくてはならない。システムを管理するための権限等、非常に広い範囲に及ぶ権限を保有する管理者については、厳格な管理を実施しなければならない。

（エ） 情報へアクセスする権限のない者による成りすましでの情報の不正利用を防止するため利用者が情報の利用権限を適切に管理しなければならない。

（オ） コンピュータネットワーク（以下、「ネットワーク」）を利用した論理的な不正アクセスを防止するため、ネットワーク利用者の特定によるアクセスコントロール実施しなければならない。

（カ） 情報システムの不正利用を防止するため、ネットワークのアクセスコントロール、オペレーティングシステムのアクセスコントロール、情報システムのアプリケーションごとのアクセスコントロールを可能な限り実施しなければならない。

(7) 情報セキュリティ確保のための自主点検に関する基準

（ア） 情報資産に対する情報保護対策が実施され、有効に機能していることを確認するために、情報資産を所管する責を負うものは、定期的に自主的な点検を実施しなければならない。

(8) 危機管理に関する基準

(ア) 情報セキュリティ危機管理体制

① 情報セキュリティに関わるリスクは可能な限り、軽減、回避を行うこととするが、万が一リスクが発現してしまった場合、情報教育研究センター長は情報セキュリティ危機管理委員会を構築しなければならない。

(イ) 情報セキュリティ危機管理計画

① 情報セキュリティ責任者は情報資産の重要度から、セキュリティ事故対策における優先順位及び情報システムを復旧させる優先順位を決定しなければならない。

② 情報セキュリティ危機管理委員会は情報教育研究センター長が定める手続きに沿って、セキュリティ事故対策における優先順位及び情報システムの復旧優先順位を策定しなければならない。

③ 情報セキュリティ危機管理委員会は対策及び復旧優先順位に沿って、セキュリティ事故における対応計画及びシステムを復旧させるための計画を策定しなければならない。

(ウ) 情報セキュリティ危機管理計画の教育、訓練

① 情報教育研究センター長は、情報セキュリティ危機管理計画を効率的かつ有効に機能させるため、情報セキュリティ危機管理計画について定期的に訓練を実施しなければならない。

(エ) 情報セキュリティセキュリティ危機管理計画の定期的な見直し

① 情報教育研究センター長は、情報セキュリティ危機管理計画を実態に沿って有効に機能させるため、情報セキュリティ危機管理計画を定期的に見直さなければならない

(9) 例外に関する基準

(ア) 本学で定める情報保護対策の実施が、費用対効果の分析や技術的な難易度により、困難であるような例外的な事項が発生する場合、関係する情報資産を所管する責を負う者が、情報教育研究センター運営委員会へ報告しなければならない。情報教育研究センター運営委員会は情報保護対策から逸脱する当該の例外事項を取り纏め、情報教育研究センター長に報告しなければならない。

(イ) 「情報セキュリティ対策基準」に記載のない例外的な事項が発生する場合、当該の例外事項の取り扱いは、情報教育研究センター運営委員会による協議の上、「情報セキュリティ基本方針」の定める規則及び関連法規、条約、本学各種規定ならびにガイドラインに拠るものとする。

附則

本対策基準の改正は、情報教育研究センター運営委員会の議を経て決定する。
本対策基準は平成 29 年 4 月 1 日より施行する。

【改訂履歴】
平成 29 年 4 月 1 日　制定

改訂日	改訂個所	改定内容
平成 30 年 4 月 1 日	-	初版発行

文京学院大学　情報セキュリティポリシー

平成 29 年 4 月 1 日　制定

発　行　者　　文京学院大学 情報教育研究センター

発　行　所　　文京学院大学
〒113-8668 東京都文京区向ヶ丘１－１９－１
TEL 03-5684-4825

文京学院大学