

# ○尚絅学院情報セキュリティ規程

## 第1章 総則

(目的)

**第1条** 高度情報社会において、学校法人尚絅学院（以下「学院」という。）の教育・研究活動の円滑化と事務・管理業務の効率化を図る上で、情報資産の適切な運用及び保護は不可欠であることから、学院の情報資産を利用するすべての者が情報セキュリティの大切さを十分に理解し、情報資産を守るための基本事項を定める。

(構成)

**第2条** 学院の情報セキュリティは、本規程及び情報セキュリティハンドブックから構成する。なお、情報セキュリティに係るすべての施策は、本規程に一貫して従う。

### (1) 情報セキュリティ規程

学院における情報セキュリティ対策に対する根本的な考え方を表すもので、情報資産を脅威から保護する理由を明らかにすることによって、学院の情報セキュリティに対する取り組み姿勢を示し、情報セキュリティを確保するための組織体制及び判断等の基準を示すもの。

### (2) 情報セキュリティハンドブック

情報セキュリティ規程に基づいて、情報資産を利用する上で遵守すべき具体的事項を示すもの。

(用語の定義)

**第3条** この規程における用語の定義を次の各号のとおり定める。

### (1) 情報セキュリティ

情報資産の機密性・完全性・可用性を可能な限り実現するために情報資産を維持・管理することを指す

### (2) 情報資産

情報及び情報を管理する仕組み等（情報システム並びに情報システムの開発、運用及び保守のための資料等）の総称

### (3) 機密性

情報にアクセスすることが認可された者だけがアクセスできることを確実にすることを指す

### (4) 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を指す

### (5) 可用性

認可された利用者が、必要なときに情報にアクセスできることを確実にすることを指す

### (6) 情報システム

同一組織内において、ハードウェア、ソフトウェア、ネットワーク及び記録媒体で構成されるものであって、これら全体で業務処理等を行うものを指す

(適用範囲)

**第4条** この規程は、学院に属する役員、就業規則第2条並びに第3条第2項の各号に規定する職員（以下「職員」という。）及び学生・生徒・園児等学院に就学する者（以下「学生」という。）のほか、学院の各機関において研修、研究、実習、委託・取引等を行う者、派遣職員等契約の形態を問わず学院の各機関において職務に従事する者（以下「学院関係者」という。）など、学院の情報資産を利用する者すべてに適用する。

(適用される者の義務)

**第5条** 前条によりこの規程が適用される者（以下「構成員」という。）は、情報資産の有用性とその安全性の確保の重要性を認識し、情報セキュリティに関する学院の施策に協力しなければならない。

(学院の責務)

**第6条** 学院は、情報資産の適切な運用及び保護に不可欠である情報セキュリティを、構成員に対し積極的に周知するものとする。

2 学院は、情報資産を保管、利用するにあたって必要な施策を講じ、その安全保護に努める。

## 第2章 対策組織・対策基準

(組織)

**第7条** 情報セキュリティ管理上の役割と権限を明確にするため、情報セキュリティ管理運営組織を次の各号により構成する。

(1) 最高情報セキュリティ責任者

最高情報セキュリティ責任者は学院長とする。全学院的な見地から情報セキュリティに関する総合的な意思決定を行い、学院の情報セキュリティに係る全責任を負うものとする。

(2) 情報セキュリティ責任者

情報セキュリティ責任者は事務局長とする。最高情報セキュリティ責任者を補佐し、学院全体の情報セキュリティ実施を総括する。

(3) 情報セキュリティ実施責任者

情報セキュリティ実施責任者は、所属長とする。最高情報セキュリティ責任者及び情報セキュリティ責任者を補佐し、所属の情報セキュリティ実施を総括する。

(4) 情報管理責任者

情報管理責任者は、各組織の管理職位者とする。所轄組織の日常及び緊急時の対応を統括・指揮しセキュリティを維持する責任を負うとともに、情報セキュリティ実施責任者を補佐する。

(5) 情報管理者

情報管理者は、各組織の監督職位者とする。所轄組織のセキュリティを維持するために教職員を監督する。また、緊急時の場合に情報管理責任者の指揮のもと、部署内の対応を主導する。

(情報セキュリティ委員会)

**第8条** 最高情報セキュリティ責任者のもとに、情報セキュリティ委員会（以下「委員会」という。）を設置する。

2 委員は次の各号の者を持って構成する。

(1) 最高情報セキュリティ責任者

(2) 情報セキュリティ責任者

(3) 情報セキュリティ実施責任者

(4) 最高情報セキュリティ責任者が任命する者 4人以内

3 委員会は情報資産及び情報システムの適切な運用、情報セキュリティの有効性を点検し、評価、改善を図るため、次の各号にあげる事項を審議する。

(1) 情報セキュリティ規程の改廃

(2) 情報セキュリティ対策

(3) 情報セキュリティに係る重要事項

4 委員会に委員長を置く。委員長は最高情報セキュリティ責任者とする。

(情報資産の分類と管理)

**第9条** 学院は情報資産を適切に保護するために、その内容に応じて分類し、その重要度に応じた情報セキュリティ対策を講じ、管理しなければならない。

(脅威の分類)

**第10条** 学院の保有する情報資産への脅威とは、次の各号のものを指す。

(1) 本学院構成員による意図しない操作または故意による不正アクセスまたは、傍受、改ざん、漏洩、消去、機器や媒体の盗難等

(2) 本学院構成員以外の者による故意による不正アクセスまたは、傍受、改ざん、複写、消去、機器や媒体の盗難等

(3) 地震、落雷、火災等の災害、事故、故障等による情報サービスまたは業務の停止

(情報セキュリティ対策)

**第11条** 学院は前条で定めた脅威の発生を防ぎ、また発生した脅威から情報資産を保護するために、次にあげる各号の情報セキュリティ対策を行う。

(1) 物理的セキュリティ

情報資産を災害、事故並びに不正侵入による損傷、盗難、妨害等から保護するため、情報システムの設置環境やシステム機器の管理方法について、物理的な対策を講じる。

(2) 人的セキュリティ

定められた事項を的確に実行し、また、検証するために、組織、体制に対して責任と権限を規定

し、学院の情報資産を利用する全ての者に対し、遵守すべき事項を周知徹底する。また、インシデント等へ迅速に対応するための人的な対策及び規定に違反した時の対応について対策を講じる。

(3) 技術的セキュリティ

情報資産を不正なプログラムからの脅威や、内外の不正アクセス等から適切に保護する対策などを、ネットワーク、情報機器等に組み込む、また、インシデント等へ迅速に対応するため技術的な対策を講じる。

2 総括責任者は定期的に各号のセキュリティの維持状況を確認し、必要に応じ見直し及び改善を図らなければならない。

(違反行為への対処)

**第12条** 学院は、本規程及びキャンパス毎に定める情報システム利用規定、運用手順に違反した者に対しては、学院の情報資産の利用を制限若しくは禁止することがある。また、重大な違反をした者については、「学校法人尚絅学院就業規則」並びに「尚絅学院懲戒規程」に基づき、懲戒処分に付すものとする。

2 学院は、学院関係者が前項による違反行為が認められたときは、当該者に対して学院の情報資産の利用を制限若しくは禁止することがある。また、重大な違反をした者については、「学校法人尚絅学院就業規則」並びに「尚絅学院懲戒規程」に準じて懲戒処分に付し、雇用主、所属団体へ通知する。

(点検・評価・改善)

**第13条** 最高情報セキュリティ責任者は、本規程や情報資産の適切な運用、情報セキュリティの有効性を定期的及び必要に応じて点検し、評価、改善を図るものとする。

(事務)

**第14条** 情報セキュリティ委員会の事務は、経営管理部管財課が行う。

(規程の改廃)

**第15条** この規程の改廃は、委員会の議を経て、理事会がこれを決定する。

## 附 則

この規程は、2011年 4 月 1 日から施行する。

この改正規程は、2015年 4 月 1 日から施行する。

この改正規程は、2021年 4 月 1 日から施行する。

この改正規程は、2023年 4 月 1 日から施行する。

この改正規程は、2023年 10月 1 日から施行する。

この改正規程は、2024年 9 月 20日より施行する。

# 学校法人尚絅学院 情報セキュリティ管理体制図

## (1)組織本体

●**最高情報セキュリティ責任者**

全学院的な見地から情報セキュリティに関する総合的な意思決定を行い、学院の情報セキュリティに係る全責任を負う

●**情報セキュリティ責任者**

最高情報セキュリティ責任者を補佐し、学院全体の情報セキュリティ実施を総括する。

●**情報セキュリティ実施責任者**

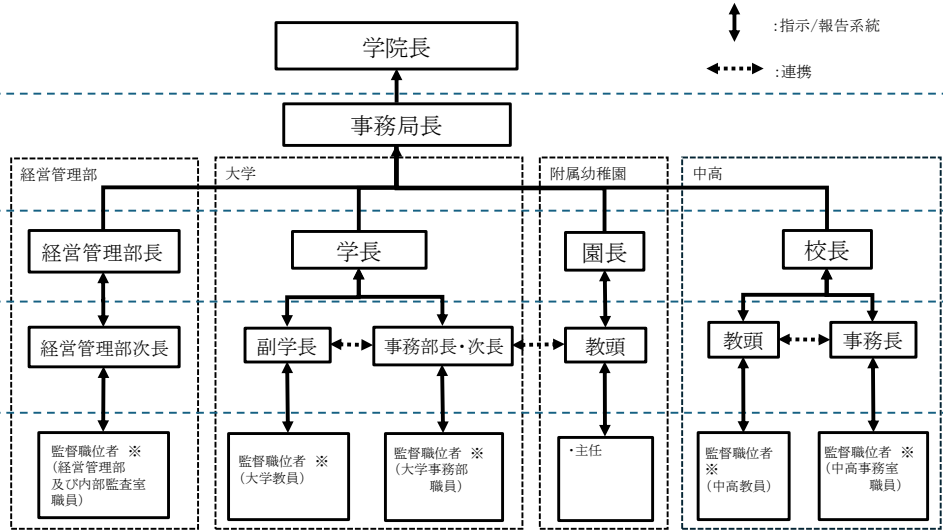
最高情報セキュリティ責任者を補佐し、所属の情報セキュリティ実施を総括する。

●**情報管理責任者**

所轄組織の日常及び緊急時の対応を統括・指揮しセキュリティを維持する責任を負うとともに、情報セキュリティ実施責任者を補佐する。

●**情報管理者**

部署内のセキュリティを維持するために教職員を監督する。  
また、緊急時の場合に情報管理責任者の指揮のもと、部署内の対応を主導する。



※監督職位者:「尚絅学院管理運営に関する規程」第4条 参照

## (2)サイバーセキュリティインシデント対応組織

●**最高情報セキュリティ責任者**

前項「(1)組織本体」と同じ

●**情報セキュリティ責任者**

前項「(1)組織本体」と同じ

●**情報セキュリティ実施責任者**

前項「(1)組織本体」と同じ

●**情報管理責任者**

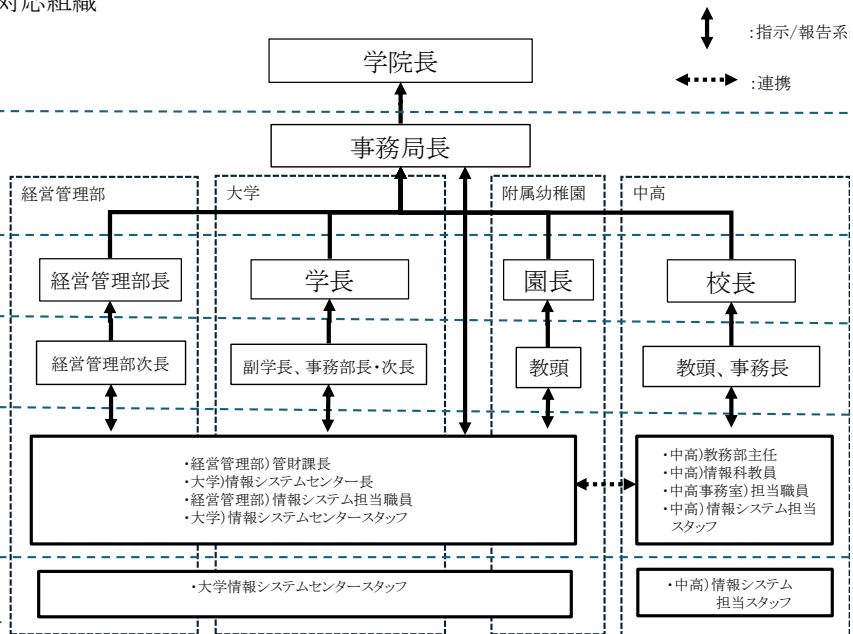
前項「(1)組織本体」と同じ

●**尚絅学院CSIRT ※**

学院内のコンピュータセキュリティインシデントに対応にあたる専門チーム。技術的な面で最高情報セキュリティ責任者、情報セキュリティ責任者、及び情報管理責任者を補佐する。

●**情報システム運用管理者**

学院の情報システムのセキュリティを確保するために、サーバー管理、アクセス制御、監視、ドキュメント管理等を行う。



※ CSIRT: Computer Security Incident Response Team略。サイバーセキュリティインシデント(例えば、不正アクセス、ウイルス感染など)に対処するための専門チーム。インシデントの検出、対応、復旧、予防策の策定などサイバーセキュリティに関連する幅広い活動を行う。