○福原学園情報セキュリティ対策基本規程

令和５年学園規程第３号
施　　行：令和５年10月17日
最終改正：令和７年７月11日

（目的）

第１条　本規程は、学校法人福原学園（以下、「学園」という。）における情報及び情報システムの情報セキュリティ対策について基本的な事項を定め、もって学園の保有する情報の保護と活用及び情報セキュリティ水準の適切な維持向上を図ることを目的とする。

（適用範囲）

第２条　本規程において適用対象とする者は、職員、学生、学園の情報システムの利用者（以下、「職員等」という。）及び臨時利用者とする。

２　本規程において適用対象とする情報は、以下の情報とする。

（１）　職員等が職務上使用することを目的として学園が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

（２）　その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、職員等が職務上取り扱う情報

（３）　前２号のほか、学園が調達し、又は開発した情報システムの設計又は運用管理に関する情報

３　本規程において適用対象とする情報システムは、本規程の適用対象となる情報を取り扱う全ての情報システムとする。

（定義）

第３条　本規程における用語の定義は、次の各号に定めるところによる。

（１）　情報

イ　情報システムに記録された情報

ロ　外部電磁的記録媒体に記録された情報

ハ　情報システムに関する書面に記載された情報

（２）　情報システム

ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の

用に供するものをいい、特に断りのない限り、学園が調達又は開発するもの（管理を外部委託しているシステムを含む。）をいう。

（３） 情報セキュリティインシデント

望まない単独若しくは一連の情報セキュリティ事象、又は予期しない若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

（４） CSIRT（シーサート）

学園において発生した情報セキュリティインシデントに対処するため、学園に設置された体制をいう。(Computer Security Incident Response Team)

（５） 記録媒体

情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下、「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（以下、「電磁的記録」という。）に係る記録媒体（以下、「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USBメモリ、外付けハードディスクドライブ、DVD-R等の外部電磁的記録媒体がある。

（６） サーバ装置

情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りのない限り、学園が調達又は開発するものをいう。

（７） 端末

情報システムの構成要素である機器のうち、利用者等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りのない限り、学園が調達又は開発するものをいう。端末には、モバイル端末も含まれる。特に断りを入れた例としては、学園が調達又は開発するもの以外を指す「学園支給以外の端末」がある。また、学園が調達又は開発した端末と学園支給以外の端末の双方を合わせて「端末（支給外端末を含む。)」という。

（８） 通信回線

複数の情報システム又は機器等（学園が調達等を行うもの以外のものを含む。）の

間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、本学の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、学園が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。

（９） 通信回線装置

通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。

(10) モバイル端末

端末のうち、必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

(11) 情報セキュリティポリシー

学園が定める情報セキュリティ基本方針及び本規程をいう。

(12) 機密性

情報にアクセスすることを認められた者だけが情報にアクセスすることができる状態を確保することをいう。

(13) 完全性

情報が破壊され、改ざんされ、又は消去されていない状態を確保することをいう。

(14) 可用性

情報にアクセスすることを認められた者が必要なときに中断されることなく情報にアクセスすることができる状態を確保することをいう。

(15) 情報セキュリティ対策基準

学園における情報及び情報システムの情報セキュリティを確保するための対策の基準として定めるものをいう。

（情報セキュリティ最高管理責任者）

第４条 学園に情報セキュリティ最高管理責任者（以下「最高管理責任者」という。）を置く。

２ 最高管理責任者は、業務執行理事とし、学園の情報セキュリティに関し統括する。

（情報セキュリティ統括責任者）

第５条 最高管理責任者を補佐するため、情報セキュリティ統括責任者（以下「統括責任者」という。）を置く。

２ 統括責任者は、学術情報センター所長とし、学園の情報セキュリティに関する統括を補佐する。

3　統括責任者は、次の業務を行う。

（1）　情報セキュリティ対策推進のための組織・体制の整備

（2）　情報セキュリティ対策基準の決定、見直し

（3）　情報セキュリティ対策を推進するための計画の決定、見直し

（4）　情報セキュリティインシデントに対処するために必要な指示その他の措置

（5）　前各号に掲げるもののほか、情報セキュリティに関する重要事項に係る業務

（情報セキュリティ実施責任者）

第6条　統括責任者を補佐するため、情報セキュリティ実施責任者（以下「実施責任者」という。）を置く。

2　実施責任者は、情報システム部長とし、情報セキュリティ対策の実施に関する事務を総括する。

3　実施責任者は、次の業務を行う。

（1）　情報セキュリティ対策に関する実施手順の整備、見直し及び実施手順に関する事務の取りまとめ

（2）　情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備

（3）　情報セキュリティインシデントに対処するための緊急連絡窓口の整備等

（4）　前各号に掲げるもののほか、情報セキュリティ対策に係る業務

（情報セキュリティ実施担当者）

第7条　実施責任者のもとに、情報セキュリティ実施担当者（以下「実施担当者」という。）を置く。

2　実施担当者は、情報システム課長とし、情報セキュリティ対策を推進する。

3　実施担当者は、次の業務を行う。

（1）　情報セキュリティインシデントの原因調査、再発防止策等の実施

（2）　情報セキュリティに係る自己点検計画の策定及び実施手順の整備

（3）　前各号に掲げるもののほか、学園設置校の情報セキュリティ対策に関する事務

（CSIRT責任者）

第8条　学園において発生した情報セキュリティインシデントに係る業務を統括するため、CSIRT責任者を置く。

2　CSIRT責任者は、職員等から最高管理責任者が指名する者をもって充てる。

（情報セキュリティ監査責任者）

第9条　学園に情報セキュリティ監査責任者（以下、「監査責任者」という。）を置く。

2　監査責任者は、内部監査室長とし、情報セキュリティに関する監査の事務を総括

する。

３　監査責任者は、次の業務を行う。

（１）　監査実施計画の策定

（２）　監査実施体制の整備

（３）　監査の実施指示及び監査結果の総括責任者への報告

（４）　前各号に掲げるもののほか、情報セキュリティの監査に関する事項

（情報セキュリティアドバイザーの指名）

第１０条　情報セキュリティアドバイザーは、情報セキュリティについて専門的な知識及び経験を有する者のうちから、必要に応じて最高管理責任者が指名する。

２　情報セキュリティアドバイザーは、必要に応じて次の助言又は支援を行う。

（１）　情報セキュリティ対策の推進に係る統括責任者、実施責任者、実施担当者及び担当事務局への助言

（２）　情報セキュリティ関係規程の整備に係る助言

（３）　情報セキュリティ対策推進計画の策定に係る助言

（４）　教育実施計画立案に係る助言、教材開発及び教育実施の支援

（５）　情報システムに係る技術的事項に係る助言

（６）　情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言

（７）　情報セキュリティインシデントへの対処の支援

（８）　前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援

（情報セキュリティ対策推進委員会）

第１１条　福原学園経営戦略会議規則（平成16年学園規則第15号）第５条の規定に基づき、情報セキュリティ対策の推進を図るため、情報セキュリティ対策推進委員会（以下、「委員会」という。）を置く。

（委員会の任務）

第１２条　委員会は、次の各号に掲げる事項を審議する。

（１）　情報セキュリティ対策基準に関すること。

（２）　情報セキュリティ対策推進計画に関すること。

（３）　情報セキュリティ関係規程等の制定、改廃に関すること。

（４）　前各号に掲げるもののほか、情報セキュリティに関し必要なこと。

（委員会の組織）

第１３条　委員会は、次の各号に掲げる委員をもって組織する。

（１）　最高管理責任者

（２） 統括責任者
（３） 部局実施責任者
（４） 実施担当者
（５） CSIRT責任者
（６） 法人事務局長
（７） 法人事務局総務部長
（８） 大学の事務局長
（９） 高等学校の事務長

２　前項に定める委員のほか、最高管理責任者が必要と認めた者を委員に加えることができる。

（委員会の委員長）

第１４条　委員長は最高管理責任者とし、委員会を招集する。

２　委員会に議長を置き、最高管理責任者が指名する者をもって充てる。

（情報セキュリティ対策基準の策定）

第１５条　統括責任者は、委員会における審議を経て、情報セキュリティ対策の具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

（情報セキュリティポリシーの見直し）

第１６条　学園は、次に掲げる場合は、情報セキュリティポリシーを見直すものとする。

（１） 情報セキュリティ監査又は自己点検の結果、改善が必要となった場合
（２） 情報セキュリティに関する状況の変化に対応するため、新たな対策が必要となった場合

（情報セキュリティインシデントに備えた体制の整備）

第１７条　統括責任者は、実務担当者を含めた実効性のあるCSIRT体制を整備し、その役割を明確化する。

２　CSIRTの構成員は、専門的な知識又は適性を有すると認められる者を職員等から、最高管理責任者が選任する。

３　統括責任者は、情報セキュリティインシデントが発生した際、直ちに最高管理責任者への報告が行われる体制を整備する。

４　統括責任者は、以下を含むCSIRTの役割を規定すること。

（１） 学園に関わる情報セキュリティインシデント発生時の対処の一元管理
　イ　学園における情報セキュリティインシデント対処の管理
　ロ　情報セキュリティインシデントの可能性の報告受付

ハ　学園における情報セキュリティインシデントに関する情報の集約
ニ　情報セキュリティインシデントの最高管理責任者等への報告
ホ　情報セキュリティインシデントへの対処に関する指示系統の一本化
（２）　情報セキュリティインシデントへの迅速かつ的確な対処
イ　情報セキュリティインシデントであるかの評価
ロ　被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデントへの対処全般に関する指示、勧告又は助言
ハ　文部科学省への連絡
ニ　外部専門機関等からの情報セキュリティインシデントに係る情報の収集
ホ　他の機関等への情報セキュリティインシデントに係る情報の共有
ヘ　情報セキュリティインシデントへの対処に係る専門的知見の提供、対処作業の実施

５　統括責任者は、情報セキュリティインシデントが発生した際に、情報セキュリティインシデント対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制を構築しておかなければならない。

６　統括責任者は、学園における情報セキュリティインシデント対処について、CSIRT、情報セキュリティインシデントの発生した当該部局及びその他関連部局の役割分担を明確にしておかなければならない。

（事務）

第１８条　情報セキュリティ対策及び委員会の事務は、学術情報センター情報システム課が行う。

（兼務を禁止する役割）

第１９条　職員等は、情報セキュリティ対策の運用において、以下の役割を兼務してはならない。

（１）　承認又は許可（以下、本条において「承認等」という。）の申請者と当該承認等を行う者（以下、本条において「承認等権限者」という。）
（２）　監査を受ける者とその監査を実施する者

２　職員等は、承認等を申請する場合において、自らが承認等権限者であるときその他承認等権限者が承認等の可否の判断をすることが不適切と認められるときは、当該承認等権限者の上司又は適切な者に承認等を申請し、承認等を得なければならない。

（細則）

第２０条　この規程に定めるもののほか、情報セキュリティ対策に関し必要な事項は、

「政府機関等のサイバーセキュリティ対策のための統一基準（令和５年７月４日サイバーセキュリティ戦略本部決定)」に準じて執り行うものとする。

附 則

この規程は、令和５年10月17日から施行する。

附 則

この規程は、令和７年７月11日から施行する。