情報セキュリティ対策基本規程

２０２１年3月２日制定

（目的）

第 １ 条　　本規程は、学校法人瓜生山学園（以下「本学」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、もって本学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、本学情報システムを運用・管理するすべての者、並びに利用者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、以下とする。

（１）教職員等が職務上使用することを目的として本学が調達し、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、教職員等が職務上取り扱う情報

（３）（１）及び（２）のほか、本学が調達し、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。

（用語定義）

第 ３ 条　　本規程において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

（１）外部委託

本学の情報処理業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。

（２）機器等

情報システムの構成要素（サーバ、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。

（３）教職員等

本学を設置する法人の役員及び、本学に勤務する常勤又は非常勤の教職員（派遣職

員を含む）その他、部局総括責任者が認めた者をいう。教職員等には、個々の勤務条件にもよるが、例えば、派遣労働者、一時的に受け入れる研修生等も含まれている。

（４）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、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。

（５）サーバ

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、特に断りがない限り、本学が調達又は開発するものをいう。

（６）CSIRT（シーサート）

本学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、本学に設置された体制をいう。Computer Security Incident Response Team の略。

（７）情報

本規程第２条第２項に定めるものをいう。

（８）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、本学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。）若しくは本学情報ネットワークに接続されるものをいう。

（９）情報セキュリティインシデント

JIS Q 27000:2014 における情報セキュリティインシデントをいう。

（１０）情報セキュリティ対策推進体制

本学の情報セキュリティ対策の推進に係る事務を遂行するため、学内に設置された体制をいう。

（１１）対策基準

本学が定める「情報セキュリティ対策基準」及び同基準から参照される関連基準をいう。

（１２）端末

情報システムの構成要素である機器のうち、利用者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、特に断りがない限り、本学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、本学が調達又は開発するもの以外を指す「本学支給以外の端末」がある。また、本学が調達又は開発した端末と本学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。

（１３）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。

（１４）ポリシー

本学が定める「情報セキュリティの基本方針」及び本規程をいう。

（１５）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。

（１６）要管理対策区域

本学の管理下にある区域（学外組織から借用している施設等における区域を含む。）であって、取り扱う情報を保護するために、施設及び執務環境に係る対策が必要な区域をいう。

（１７）利用者

教職員等及び学生等で、本学情報システムを利用する許可を受けて利用するものをいう。

（１８）臨時利用者

教職員等及び学生等以外の者で、本学情報システムを臨時に利用する許可を受けて利用するものをいう。

（全学総括責任者）

第 ４ 条　　本学における情報セキュリティに関する事務を統括する全学総括責任者を置く。理事長がこれを任命する。

２　全学総括責任者を助けて本学における情報セキュリティに関する事務を整理し、全学総括責任者の命を受けて本学の情報セキュリティに関する事務を統括する全学総括副責任者１人を必要に応じて置くこと。

３　全学総括責任者は、次に掲げる事務を統括すること。

（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）対策推進計画の決定、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

４　全学総括責任者は、全学の情報基盤として供される本学情報システムのうち情報セキュリティが侵害された場合の影響が特に大きいと評価される情報システムを指定することができる。この指定された情報システムを「全学情報システム」という。

（全学情報セキュリティ委員会の設置）

第５条　　全学総括責任者は、対策基準等の審議を行う機能を持つ組織として、全学情報セキュリティ委員会を置くこと。

２　全学情報セキュリティ委員会の委員長及び委員は、各部局の代表者から指名すること。

３　全学情報セキュリティ委員会は、次に掲げる事項を審議すること。
（１）「情報セキュリティ対策基準」
（２）対策推進計画
（３）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事項

（情報セキュリティ監査責任者）

第６条　　全学総括責任者は、その指示に基づき実施する監査に関する事務を統括する者として、情報セキュリティ監査責任者１人を置くことができる。

（管理運営部局）

第７条　　全学情報セキュリティ委員会は、本学情報システムの管理運営部局を定める。

（管理運営部局が行う事務）

第８条　　管理運営部局は、全学実施責任者の指示により、以下の各号に定める事務を行う。
（１）全学情報セキュリティ委員会の運営に関する事務
（２）本学情報システムの運用と利用におけるポリシーの実施状況の取りまとめ
（３）講習計画、リスク管理及び非常時行動計画等の実施状況の取りまとめ
（４）本学の情報システムのセキュリティに関する連絡と通報

（全学実施責任者・部局総括責任者の設置）

第９条　　全学総括責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、部局総括責任者１人を置くこと。原則、学部長または教務部長をその任にあてることとする。

そのうち、部局総括責任者を統括し、全学総括責任者及び全学総括副責任者を補佐する者として、全学実施責任者１人を選任すること。

２　全学実施責任者は、命を受け、次の事務を統括すること。

（１）要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の決定

（２）情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する事務の取りまとめ

（３）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

（４）例外措置の適用審査記録の台帳整備等

（５）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

（６）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事務

３　部局総括責任者は、命を受け、管理を行う組織のまとまりにおける情報セキュリティ対策を推進するため、次の事務を統括すること。

（１）定められた区域ごとの区域部局総括責任者の設置

（２）情報システムごとの部局実施責任者の設置

（３）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

（４）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

（５）前各号に掲げるもののほか、管理を行う組織のまとまりの情報セキュリティ対策に関する事務

（部局情報セキュリティ委員会）

第１０条　　各部局に部局情報セキュリティ委員会を置く。

２　部局情報セキュリティ委員会は以下の各号に掲げる事項を実施する。

（１）部局におけるポリシーの遵守状況の調査と周知徹底

（２）部局におけるリスク管理及び非常時行動計画の策定及び実施

（３）部局における情報セキュリティインシデントの再発防止策の策定及び実施

（４）部局における部局実施担当者向け教育の計画と企画

（部局情報セキュリティ委員会の構成員）

第１１条　　部局情報セキュリティ委員会は、委員長及び次の各号に掲げる者を委員として組織する。

（１）部局実施責任者

（２）部局実施担当者

（３）その他部局総括責任者が必要と認める者

（部局情報セキュリティ委員会の委員長）

第１２条　　部局情報セキュリティ委員会の委員長は、部局総括責任者をもって充てる。

（部局実施責任者の設置）

第１３条　　部局総括責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、部局実施責任者を選任すること。原則、事務局長または事務課長を選任することとする。

２　部局実施責任者は、命を受け、情報システムにおける情報セキュリティ対策に関する事務を担うこと。

３　部局実施責任者は、所管する情報システムの管理業務において必要な単位ごとに部局実施担当者を置くこと。

（全学情報セキュリティアドバイザーの設置）

第１４条　　全学総括責任者は、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を全学情報セキュリティアドバイザーとして置くことができる。

２　全学総括責任者は、以下を例とする全学情報セキュリティアドバイザーの業務内容を定める。

（１）全学の情報セキュリティ対策の推進に係る全学総括責任者及び全学総括副責任者への助言

（２）情報セキュリティ関係規程の整備に係る助言

（３）対策推進計画の策定に係る助言

（４）教育実施計画の立案に係る助言並びに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）利用者に対する日常的な相談対応

（８）情報セキュリティインシデントへの対処の支援

（９）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体制の整備）

第１５条　　全学総括責任者は、本学の情報セキュリティ対策推進体制を整備し、その役割を規定すること。

２　全学実施責任者が、情報セキュリティ対策推進体制の責任者を務めること。

３　全学総括責任者は、以下を含む情報セキュリティ対策推進体制の役割を規定すること。

（１）情報セキュリティ関係規程及び対策推進計画の策定に係る事務

（２）情報セキュリティ関係規程の運用に係る事務

（３）例外措置に係る事務

（４）情報セキュリティ対策の教育の実施に係る事務

（５）情報セキュリティ対策の自己点検に係る事務

（６）情報セキュリティ関係規程及び対策推進計画の見直しに係る事務

（情報セキュリティインシデントに備えた体制の整備）

第１６条　　全学総括責任者は、CSIRT を整備し、その役割を明確化する。

２　全学総括責任者は、教職員等のうちから CSIRT に属する職員として専門的な知識又は適性を有すると認められる者を選任する。そのうち、本学における情報セキュリティインシデントに対処するための責任者として CSIRT 責任者を置くこと。

３　全学総括責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備すること。

４　全学総括責任者は、以下を含む CSIRT の役割を規定すること。

（１）本学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

・全学における情報セキュリティインシデント対処の管理

・情報セキュリティインシデントの可能性の報告受付

・本学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

・情報セキュリティインシデントの全学総括責任者等への報告

・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

・情報セキュリティインシデントであるかの評価

・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

・所轄官庁（文部科学省等）への連絡

・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

・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

・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　全学総括責任者は、実務担当者を含めた実効性のある CSIRT 体制を構築すること。

６　全学総括責任者は、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くこと。

７　全学総括責任者は、全学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当事者部局及びその他関連部局の役割分担を規定すること。

（兼務を禁止する役割）

第１７条　　教職員等は、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ないこと。

（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を行う者（以下、本条において「承認権限者等」という。）

（２）監査を受ける者とその監査を実施する者

（対策基準の策定）

第１８条　　全学総括責任者は、全学情報セキュリティ委員会における審議を経て、「情報セキュリティ対策基準」を定めること。また、対策基準は、本学の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた上で定めること。

附　則　この基本規程は、２０２１年（令和３年）４月１日から施行する。