熊本県立大学情報セキュリティ
基本方針

熊本県立大学

（平成 27 年 6 月策定　事務局総務課）

目次

第１　趣旨

熊本県立大学（以下「本学」という。）が保有・管理するすべての情報資産は、本学運営にとって重要な資産である。

これらの情報資産が外部に漏えいするなどした場合、本学の教育活動・学術研究の停滞、本学に対する社会的信頼失墜などといった本学にとって極めて重大な事態と被害を招くことになる。

このような事態を未然に防ぐため、全ての本学関係者は不断の努力をもって、情報資産を保全しなければならない。

熊本県立大学情報セキュリティ基本方針（以下「本基本方針」という。）は、このような本学の情報セキュリティ対策に対する基本的な考え方を、学内外に対して表明するものである。

第２　定義

１　情報資産

本学が保有する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開発、運用及び保守）に係るすべての情報。

２　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持すること。

（１）機密性　　アクセスを許可された者だけが情報資産にアクセスできることを確実にすること

（２）完全性　　情報資産及び処理方法が正確であること及び完全であることを保護すること

（３）可用性　　許可された利用者が必要なときに、情報資産にアクセスできることを確実にすること

３　情報システム

本学組織内において、ハードウェア、ソフトウェア、ネットワーク、記録媒体等で構成されるものであって、これら全体で業務処理を行うものをいう。

４　ネットワーク

情報などを共有・流通する目的で、ハードウェアを有線又は無線により接続して形成されるものをいう。

５　本学ユーザ

本学の所有する情報資産に関する業務（授業、研究等を含む。）に携わる本学の全ての教職員等（役員、嘱託職員、臨時職員等を含む。）及び学生（留学生、公開講座生等を含む。）をいう。

第３　規程の整備

本学は本基本方針を徹底するため、熊本県立大学情報セキュリティ対策基準、熊本県立大学情報セキュリティ実施要領等の必要な規程を定める。

なお、本基本方針及び熊本県立大学情報セキュリティ対策基準を合わせて熊本県立大学情報セキュリティポリシー（以下「本学情報セキュリティポリシー」という。）という。

第４　管理体制

１　管理体制

本学の情報資産について、情報セキュリティ対策を推進・管理するための体制を確立するものとする。

ア　情報セキュリティの管理体制を整備するため、情報セキュリティに関する権限と責任を有する最高情報セキュリティ責任者（以下「ＣＩＳＯ（Chief Information Security Officer)」という。）を置く。また、ＣＩＳＯを補佐するため、情報セキュリティ統括管理者を置く。

イ　本学情報セキュリティポリシーの適正な管理と円滑な運営を図るため、情報セキュリティ管理者を置く。

ウ　ネットワークの運用管理等における本学情報セキュリティポリシーの適正な管理と円滑な運営を図るため、ネットワーク管理者を置く。

エ　情報システムの運用管理等における本学情報セキュリティポリシーの適正な管理と円滑な運営を図るため、情報システム管理者を置くものとする。

２　運営組織

情報セキュリティ対策の継続的な維持及び向上を図るため、ＣＩＳＯ、情報セキュリティ統括管理者、情報セキュリティ管理者及びネットワーク管理者により熊本県立大学情報セキュリティ運営会議を組織する。

第５　情報資産の分類

情報資産を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行うものとする。

第６　情報資産への脅威として認識すべきもの

情報資産を脅かす脅威として特に認識すべきものは以下のとおりである。

（１）外部からの脅威

部外者による不正アクセス又は不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び記録媒体の盗難等

（２）内部からの脅威

本学ユーザ及び情報資産を取り扱う可能性のある外部委託者による不正アクセ

ス又は不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び記録媒体の盗難及び正規の端末機以外の接続によるデータ漏えい及び意図しない操作等

（３）環境的脅威

地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

第７　情報セキュリティ対策

上記第６で示した脅威から情報資産を保護するために、次の情報セキュリティ対策を講ずるものとする。

（１）物理的情報セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産の損傷・妨害等を防止するために物理的な対策を講ずる。

（２）人的情報セキュリティ対策

情報セキュリティに関する権限や責任を定め、すべての本学ユーザに本学情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

（３）技術及び運用における情報セキュリティ対策

外部からの不正なアクセス等から情報資産を適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、システム開発等についてネットワークの監視等の運用面の対策を講ずる。

また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

第８　事業継続管理

本学は、業務の継続が困難となる不測の事態（天災、人災問わず）に備え、事業の継続管理に必要な情報セキュリティ管理を行う。

第９　継続的改善

本学は、本基本方針を含む情報セキュリティ管理の継続的改善に努める。

第１０　法令の遵守

本学は、情報セキュリティに関する各種法令の規定を遵守する。