

熊本県立大学情報セキュリティ基本方針

熊本県立大学
情報セキュリティ運営会議事務局

改定履歴

版数	作成・改定日	改定内容	担当
1.0	2015年6月15日	新規作成	事務局総務課
2.0	2022年4月1日	全部改定	デジタルイノベーション推進センター
2.1	2024年4月1日	情報セキュリティ強化による一部改定	デジタルイノベーション推進センター

1 目的

高度な情報化社会において、熊本県立大学（以下「本学」という。）が「地域に生き、世界に伸びる大学」として、社会的信頼の下円滑に教育・学術研究活動を行うためには、本学が保有・管理するすべての情報資産を十分な情報セキュリティ対策により保全する必要があります。そのために、全ての本学関係者は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。）に従い、情報セキュリティ対策の重要性を認識するとともに、情報資産を適切に管理します。本学は、安心安全な教育・学術研究活動環境を確保することで、有為な人材を育成し、熊本県・国際社会の発展に寄与します。

2 体系

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ます。

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。）といたします。

3 適用範囲

3.1 適用対象者

本学情報セキュリティポリシーの適用対象者は、本学ユーザ（教育研究業務に携わる本学の全ての教職員等及び学生）とし、外部委託者や来訪者が本学の情報資産を取り扱う場合も対象とします。

3.2 適用対象情報資産

本学情報セキュリティポリシーの適用対象となる情報資産は、本学が所有するすべての情報資産とし、これには、クラウドコンピューティング等により本学ユーザが学外のネットワーク・システム上で取り扱う情報資産を含むものとします。

3.3 適用対象業務

本学情報セキュリティポリシーの適用対象業務は、本学が行うすべての教育研究業務とし、これらの業務に情報セキュリティ活動を取り入れます。

4 体制・組織

4.1 管理体制

本学は、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（CISO:Chief Information Security Officer）を置きます。

4.2 運営組織

本学は、CISO を議長とした情報セキュリティ運営会議を設置し、情報セキュリティ対策を推進・管理します。

また、CSIRT(Computer Security Incident Response Team)を設置し、情報セキュリティインシデント(情報セキュリティに関する事故・障害)の予防や被害の低減に努めます。

5 情報資産の分類

本学は、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います。

6 情報セキュリティリスクマネジメント

本学は、定期的に情報資産が持つ情報セキュリティリスクを特定・評価し、リスク対応計画の立案を行います。

7 情報セキュリティ対策

本学は、情報セキュリティリスク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じます。

7.1 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行います。

7.2 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を行います。

7.3 技術的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を行います。また、情報セキュリティインシデントの予兆検知・防止のため、システム・ネットワーク等の監視・診断を行います。

8 有効性の評価

本学は、情報セキュリティ対策の有効性を定期的に評価します。

9 監査

本学は、内部監査を定期的に行い、情報セキュリティの維持に努めます。

10 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います。

11 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します。

12 継続的改善

本学は、上記を組織的かつ継続的に推進・改善します。