国立大学法人山口大学 情報セキュリティマネジメントシステム(ISMS[1])基本方針

趣旨

山口大学は9学部と8大学院研究科を有し，約1万人の構成員からなる地域の基幹総合大学であり，研究・教育面で学内のみならず，広く社会に対して責任を負うと同時に，山口大学憲章を定めて基本理念を掲げ，大学構成員全員がその理念の共有と目標の実現を目指している。さらに，情報セキュリティに関しては，「国立大学法人山口大学情報セキュリティ基本方針」をはじめとする情報セキュリティポリシーを定め，適切なレベルのセキュリティの確保に努めているとともに，山口大学は学術情報ネットワーク(SINET[2])と県内大学の相互接続校でもあり，その責任は重大なものとなっている。

学内において，山口大学情報基盤センター及び総務企画部情報企画課は，山口大学情報ネットワーク(YUNET[3])の運営をはじめ各種ITサービス及び情報通信技術面で，総合技術部情報技術課システム開発グループは，やまぐちドクターネットの運用面で，大学全体の教育・研究・地域貢献を支えている。これらの組織について，以降は「山口大学 ISMS 適用組織」若しくは「ISMS 適用組織」と称する。

ISMS 適用組織内の全ての教職員(以下「ISMS 適用組織構成員」という。)は，業務の重要性を踏まえ，安定し信頼できる情報システムを提供するべく以下の誓いを宣言し，ISMS 基本方針(以下「基本方針」という。)を定める。

3つの誓い

- 私たちは，組織としてシステムの安定運用を企画し実施します。
- 私たちは，不正なアクセスから情報を守り，安心できる情報環境を提供します。
- 私たちは，自己研鑽に励み，自らの資質向上を目指します。

目的

当基本方針は，ISMS 適用組織が安定し信頼できる情報システムを提供するために，ISMS を構築し運用を継続する上で重要視する事項を提示し，ISMS 適用組織構成員の情報セキュリティ活動における行動規範とすることを目的とする。

基本方針

- ISMS 適用組織は山口大学情報セキュリティポリシーに従い，情報セキュリティの主要3要素である，機密性(許可された者以外からの当該情報の操作を遮断すること)，完全性(情報が改竄されることのないように保護すること)及び可用性(許可された利用者に対して設備と情報の利用機会が失われないよう保証すること)の確保に努める。
- 特に，ISMS 適用組織の公共性と教育・研究の継続性をとおして社会に果たすべき責務に鑑み，「機密性」及び「可用性」を重視する。また，日々変化する環境に対応して，適宜対応できる情報セキュリティマネジメントの確立を目指す。
- ISMS 構築及び運営に当たっては，ISMS 適用組織構成員全員が一致協力してこれを推進する。とりわけ担当者交代における業務引継ぎの際の業務継続性を重視する。

適用範囲

当基本方針は，ISMS 適用組織内のサービスを構成する情報，技術的資産，人的組織，物理的資産に適用する。

山口大学情報セキュリティポリシーでは電子情報のみを適用範囲としているが，当基本方針は ISMS 適用組織内で有する紙媒体情報にも適用する。

推進体制と役割

- 山口大学副学長(情報化推進担当)は，山口大学における情報化統括責任者(CIO[4])であるとともに，ISMS 推進活動の最高責任者として，山口大学における ISMS 推進活動に関する業務を総括する。
- 山口大学理事・副学長(情報セキュリティ担当)は，山口大学における最高情報セキュリティ責任者(CISO[5])として，山口大学における情報セキュリティに関する業務を総括する。
- 山口大学情報基盤センター長は，CIO 補佐として CIO を補佐するとともに，情報基盤センター及び総務企画部情報企画課における ISMS 構築及び運営を総括し，情報基盤センター及び総務企画部情報企画課内における情報セキュリティに関する業務を総括する。
- 山口大学総合技術部本部長は，総合技術部における ISMS 構築及び運営を総括し，総合技術部の ISMS 適用範囲内における情報セキュリティに関する業務を総括する。
- ISMS 構築及び運営にあたっては，情報セキュリティマネジメントにおける PDCA[6]を効果的に実施する。また，リスクマネジメントについては，あらかじめ定義されたリスクアセスメントを実施すると共に，受容できるリスク基準の素案を策定する。
- ISMS 適用組織内に ISMS 事務局を置き，ISMS 適用組織構成員により情報セキュリティマネジメントにおける PDCA 実施を主導する。ISMS 事務局長は，情報基盤センター長とする。

重視するべきリスク

特に重視すべきリスクは以下のとおりである。

- YUNET の可用性の喪失及び SINET 相互接続校である他大学等の可用性の喪失
- ISMS 適用組織が行う各種サービスの停止による可用性の喪失
- コンピュータウイルス被害等の悪意攻撃による大規模な機密性・可用性の喪失
- 台風や地震などによる大規模災害に伴う可用性の喪失
- ISMS 適用組織が保有する保有個人情報の漏洩による機密性の喪失
- インターネット利用のモラルや注意力の低下による山口大学の信用の失墜

監査

CISO により委嘱される内部監査責任者は，ISMS 適用組織が当基本方針や法令及び各種学内規則を遵守していることを，定期的に検証する。

法令及び山口大学規則の遵守

- ISMS 適用組織は，山口大学の情報セキュリティ文化の向上及び普及へ積極的に関与する。
- ISMS 適用組織構成員は，山口大学憲章や山口大学の理念を理解したうえで，不正アクセス禁止法，著作権法，個人情報保護法をはじめとする各種法令及び山口大学規則を遵守し，資産の保護に努めなければならない。
- ISMS 適用組織は，学内外を問わず他部署・他組織との間において締結された契約や覚書における義務については，これを履行するよう業務上配慮しなければならない。
- 山口大学の職員に関わる就業規則の継続的な周知及び遵守は，CIO，CIO 補佐及び ISMS 推進活動管理責任者がその責を負う。

2023 年 5 月 1 日

副学長(情報化推進担当) レール 学

注: 1) ISMS: Information Security Management System
2) SINET: Science Information Network
3) YUNET: Yamaguchi University Network
4) CIO: Chief Information Officer
5) CISO: Chief Information Security Officer
6) PDCA: (Plan, Do, Check, Action)