公立大学法人山梨県立大学情報セキュリティポリシー

Ⅰ　情報セキュリティ基本方針

1　基本方針

大学は、学生、教職員等が教育・研究、社会活動、大学運営を行ううえで、膨大な情報資産を収集し利用している。また、各種の情報開示も行っている。高度情報社会が進展するなかで、これらの情報資産は、情報機器とネットワークを通じた漏洩、改ざん、不正利用などの危険に常にさらされており、情報資産の価値を認識し、これを適正に管理・利用していくことは、今や大学の義務となっている。

公立大学法人山梨県立大学（以下「法人」という。）はここに「公立大学法人山梨県立大学情報セキュリティポリシー」（以下「本ポリシー」という。）を策定し、法人の情報システムを利用する全ての関係者が、情報に関わるさまざまな危険を自覚し、正しい行動、適正な対策をとっていくための基本的な指針を示すこととする。

なお、法人が本ポリシーによって目指すものは次のとおりである。

（1） 法人の情報セキュリティに対する侵害を阻止する。
（2） 学内外の情報セキュリティを損ねる加害行為を抑止する。
（3） 情報資産に関して、重要度による分類とそれに見合った管理をする。
（4） 情報セキュリティに関する情報の取得を支援する。
（5） 情報セキュリティに関する教育等を実施する。

2　用語の定義

本ポリシーで使用する用語の定義は、次のとおりとする。

（1） ネットワーク
コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（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。

（3） 情報システム
コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（4） 情報セキュリティポリシー
法人が所有する情報資産の情報セキュリティ対策について総合的・体系的かつ具体的にとりまとめたもの。どのような情報資産をどのような脅威から、どのようにして守るのかについての基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含めたもの。情報セキュリティ基本方針及び情報セキュリティ対策基準からなる。

（5） 情報セキュリティ基本方針（以下「基本方針」という。）
法人における情報セキュリティ対策に対する根本的な考え方を表すもので、どのような情報資産を、どのような脅威から、なぜ保護しなければならないのかを明らかにし、情報セ

キュリティに対する取組姿勢を示すもの。

（6） 情報セキュリティ対策基準（以下「対策基準」という。）
「基本方針」に定められた情報セキュリティを確保するために遵守すべき行為及び判断基準、つまり「基本方針」を実現するために何をやらなければいけないかを示すもの。

（7） 情報セキュリティ実施手順（以下「実施手順」という。）
ポリシーには含まれないものの、対策基準に定められた内容を具体的な情報システム又は業務において、どのような手順に従って実行していくのかを示すもの。

（8） 機密性
情報資産にアクセスすることを認められた者だけが、情報資産にアクセスできる状態を確保することをいう。

（9） 完全性
情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（10）可用性
情報資産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、情報資産にアクセスできる状態を確保することをいう。

（11）法人情報ネットワーク（教育系ネットワーク）
各学部や部局等の教育･研究活動に利用される情報システム及びその情報システムで取り扱うデータをいう 。

（12）部局情報ネットワーク（事務系ネットワーク）
大学運営の基盤となる人事給与、財務会計、学務等の事務情報システム及びその情報システムで取り扱うデータをいう 。

（13）通信経路の分割
セキュリティを確保するため、事務系ネットワークの重要な情報システムを、他のシステムと共有する回線から論理的または物理的に分離した環境として構築することをいう。

（14）無害化通信
格付けされた情報を異なる領域間で移動させる際、個人情報の抽出や加工等を行い、情報の機密性と完全性を確保する措置をいう。

3 対象とする脅威

情報資産に対する脅威として、次に掲げる脅威を想定し、情報セキュリティ対策を実施する。

（1） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（2） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（3） 地震、落雷、火災等の災害によるサービス及び業務の停止等

（4） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（5） 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4　適用範囲

（1）適用組織

本ポリシーの適用範囲は、法人の情報システム及び情報資産に加えて、法人以外のコンピュータから法人のネットワークに一時的に接続されたコンピュータ及びそれらが扱う情報を含むものとする。

（2）情報資産

イ ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

ロ ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

ハ 情報システムの仕様書及びネットワーク図等のシステム関連文書

5　職員等の遵守義務

法人の役員、教職員、学生、外部委託事業者、来学者等法人の情報システム及び情報資産を利用する全ての者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6　情報セキュリティ対策

前記３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行うものとする。

（1）組織体制

法人の情報資産について、情報セキュリティ対策を推進する法人全体の組織体制を確立する。

（2）情報資産の分類と整理

法人の保有する保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（3）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の対策を講じる。

イ　法人情報ネットワーク（教育系ネットワーク）においては、部局情報ネットワークとの接続が必要な場合には、全学システム管理責任者の承認を得た上で適切なアクセス制御を行う。

ロ　部局情報ネットワーク（事務系ネットワーク）においては、要保護情報の流出を防ぐため、全学システム管理責任者が許可した通信回線以外への接続を禁止する 。

（4）物理的セキュリティ

サーバ室、通信回線及び役員・教職員等のパソコン等の管理について、物理的な対策を講じる。

（5）人的セキュリティ

情報セキュリティに関し、役員・教職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（6）技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（7）運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。この場合において、情報資産に対するセキュリティ侵害発生時に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（8）業務委託と外部サービス（クラウドサービス）の利用

イ 業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講ずる。

ロ 外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

ハ ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（9）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

7 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び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に対策が必要になった場合は、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーの見直しを行う。

9 情報セキュリティ対策基準の策定

前記6、7及び8に規定する対策等を実施するために、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ものとする。

１０　実施手順の作成

本ポリシーの具体的な実施手順は、情報委員会で別に定める。

Ⅱ　情報セキュリティ対策基準

1　組織・体制

（1）　組織

ア　本ポリシーに基づき、法人の情報セキュリティを統括管理するために、最高情報セキュリティ管理者、全学システム管理責任者、部局システム管理責任者及びネットワーク管理責任者を置く。

イ　組織について必要な事項は別に定める。

（2）　不正アクセス等への対応

ネットワーク管理責任者は、外部または内部からの不正アクセスを検出した場合、緊急措置手順に従い、関連する通信の遮断、又は該当する情報機器の切り離しを実施する。不正アクセスが継続する場合には、当該情報機器、又はそれを接続するネットワークについて、定常的な利用の停止などの抑止措置をとることができる。この措置を行った場合は、事後速やかに最高情報セキュリティ責任者及び全学システム管理責任者に報告しなければならない。

2　学内外の情報セキュリティを侵害する行為の抑止

学内外を問わず、あらゆる研究・教育機関、企業、組織、団体及び個人等の情報資産を侵害してはならない。また本ポリシーの他、情報セキュリティに関連する法令及び法人が定める規程等を遵守しなければならない。

3　情報の分類と管理

（1）　アクセス制限

(ア) システム管理者は、情報の内容に応じてアクセス可能な利用者を定め、不正なアクセスを阻止するために必要なアクセス制限を行わなければならない。

(イ) 利用者は、アクセス権のない情報にアクセスしたり、許可されていない情報を利用してはならない。

（2）　情報の分類

システム管理者は、情報資産の機密性、完全性及び可用性に鑑み、重要性に応じて分類した上で管理をしなければならない。また、それぞれの情報資産について、公開・非公開を定めなければならない。

（3）　情報の公開化

非公開情報を公開化する場合には、個人情報の漏洩、プライバシーや著作権の侵害に十分注意し、公開できる情報の抽出を行い、公開してよい形に加工しなければならない。

（4）　情報の限定公開

システム管理者は、特定の利用者に特定の情報を開示する必要が生じた場合は、許可されたものが許可された操作だけを行えるように、認証及びアクセス制御機能を設けなければならない。

（5）　情報改ざん及び偽情報流布の防止

システム管理者は、公開情報の改ざんを防ぐために必要な措置を講じなければならない。また、公開情報の複製・加筆による偽情報の作成及び流布を防止するために必要な措置を講じなければならない。

（6）　情報機器及び記憶媒体の処分

システム管理者は、公開・非公開を問わず情報機器及び記憶媒体を破棄する場合は、その処分方法に注意しなければならない。

4　情報セキュリティの評価と更新

（1）　ポリシーの運用実態の把握

最高情報セキュリティ責任者は、ポリシーの運用実態を把握するために、必要な措置を講じることができる。

（2）　情報セキュリティ監査

最高情報セキュリティ責任者は、常にセキュリティに関する最新の情報を取得し、適切な物理的・技術的・人的セキュリティが実施されているか定期的に監査を実施し、情報委員会に報告しなければならない。

（3）　評価と更新

情報委員会は、定期的に本ポリシーの更新を行う必要性の有無を適時評価し、更新が必要と認められる場合には、速やかにセキュリティレベルの高い、かつ遵守可能なポリシーに更新しなければならない。