長崎県公立大学法人情報セキュリティポリシー

（平成25年4月1日
規程第１３号）

Ⅰ　基本方針

１　目的

長崎県公立大学法人（以下、「法人」という。）が、県立の大学としての役割を担い、高度に情報化した現代社会において教育・学術研究活動を行うことで本学の使命を全うするためには、情報基盤の整備のみならず、法人の保有する情報資産の情報セキュリティを確保する必要　がある。

そのため、法人の情報資産を管理・運用又は利用するための包括的な指針として長崎県公立大学法人情報セキュリティポリシー（以下、「ポリシー」という。）を策定する。

２　定義

この基本方針の用語定義については、以下のとおりとする。

（１）情報セキュリティ

情報資産の機密性の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

（２）情報資産

情報システムに記録された情報及び情報システムに関係がある書面に記載された情報であり、電磁的に記録された情報すべてを含む。書面に記載された情報には、電磁的に記録されている情報を記載した書面（情報システムに入力された情報を記載した書面、情報システムから出力した情報を記載した書面）及び情報システムに関する設計書が含まれる。

（３）情報システム

情報の作成、利用及び管理等のための仕組み（ハードウェア及びソフトウェアからなる情報機器及び記憶媒体並びに有線又は無線のネットワークをいう。）をいう。

法人の情報システムとは、法人により所有又は管理されているもの及び法人と契約あるいは他の協定に従って提供されるものをいい、法人の情報ネットワークに接続する機器を含む。

３　適用範囲及び責務

本ポリシーの適用範囲は、大学の教育・学術研究及び法人運営に係る情報資産とする。本ポリシーの対象者は、法人の情報資産を利用する教職員、学生、委託業者等すべての関係者（以下、「利用者」という。）とする。利用者は、情報セキュリティの重要性について共通の認識を持つとともに、業務等の遂行に当たってはポリシーを遵守しなければならない。

４　情報セキュリティ管理体制

法人の情報資産について、教職員及び学生が一体となっ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。

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。

６　情報資産への脅威

ポリシーを策定するうえで、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（１）　部外者による故意の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、機器及び媒体の盗難等。

（２）　利用者による意図しない操作、故意の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、機器及び媒体の紛失・盗難及び規定外の端末接続によるデータ漏えい等。

（３）　地震、落雷、火災等の災害並びに事故、故障等による業務の停止。

７　情報セキュリティ対策

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

（１）　情報資産への損傷・妨害等から保護するための物理的な対策。

（２）　情報セキュリティに関する権限や責任を定め、全ての利用者に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ために必要な対策。

（３）　情報資産を外部からの不正アクセス等から適切に保護するため、情報資産へのアクセス制御等の技術面の対策、ポリシーの遵守状況の確認等の運用面の対策及び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。

８　ポリシーの評価と更新

ポリシーの遵守状況や有効性等を定期的に評価し、改善が必要と認められた場合には、速やかに実効性のあるポリシーに更新しなければならない。

９　基本方針の公開について

長崎県公立大学法人情報セキュリティポリシーのうち、Ⅰ　基本方針については原則公開とする。

Ⅱ　対策基準

１　管理体制

情報セキュリティの管理体制は以下のとおりとする。

（情報セキュリティ総括責任者）

法人に情報セキュリティ総括責任者（以下「総括責任者」）を置き、理事長をもって充てる。情報セキュリティ総括責任者は、情報セキュリティに関する総括的な意思決定を行い、学内外に対する最高責任を負うものとする。

（情報セキュリティ管理者）

法人に、情報セキュリティ管理者（以下「管理者」という。）を置き、学長及び法人事務局長をもって充てる。管理者は、法人における情報セキュリティの適正な管理を指揮監督する。

（情報セキュリティ責任者）

各部局に情報セキュリティ責任者（以下「責任者」という。）を置き、各部局の長をもって充てる。責任者は、当該部局における情報セキュリティの管理について責任を負うとともに、所属教職員等へ必要な指導及び調整を行う。

（情報セキュリティ担当者）

各部局に情報セキュリティ担当者（以下「担当者」という。）を置き、当該部局の教職員のうちから責任者が指名する者をもって充てる。ただし、大学各学部及び研究科においては、全ての教員を担当者とする。担当者は、責任者を補佐するとともに、所属における情報セキュリティに関する事務を行う。

（情報セキュリティ技術対策員）

情報セキュリティ技術対策員（本学のシステムエンジニア等。以下「技術対策員」という。）は、管理者の指示の下、情報システムやネットワーク等に関する情報管理の実施、及び緊急時の対応等に当たるものとする。また、情報システムに関する一般的な情報セキュリティの啓発及び教育について、教職員及び学生に対する幅広い初心者教育を行う。

（情報委員会）

長崎県立大学情報委員会規程により設置される情報委員会（以下「委員会」という。）は、情報セキュリティに関する事項を所掌し、情報セキュリティ対策を推進する。

２　情報資産の分類に応じた管理

本学が保有する情報資産は、重要度に応じて適正に管理されなければならない。以下にその要領を示す。

（１）　情報資産の分類

情報資産の重要度に応じた分類を以下に掲げる。

ア　非公開情報

本学が保有する情報資産のうち、重要度が高く、かつ漏えいした場合著しく本学の信用や利益を損なうもの。

イ　限定公開情報

本学が保有する情報資産のうち、本学構成員等の限定された者のみに開示すべきもの。

ウ　公開情報

本学の保有する情報資産のうち、内外を問わず不特定多数の者に開示できるもの。ホームページや広報誌等を通じて積極的に発信する情報なども含む。

（２）　情報資産の管理

情報資産は、２（１）に掲げた分類に応じて次のように管理しなければならない。

ア　非公開情報の管理

（ア）　非公開情報は、職務上必要な者のみにアクセスを制限し、それ以外の者にアクセスさせてはならない。

（イ） 非公開情報は、保管方法など管理に関する事項を、必要に応じて定めなければならない。
（ウ） 非公開情報をコンピュータ及び記憶媒体に複製・保存する場合は、暗号化するなどの措置を取らなければならない。
（エ） 非公開情報は、原則として学外に持ち出してはならない。やむを得ず持ち出す場合は、当該情報を所管する部局の長の承認を得るとともに、暗号化するなどの措置を取らなければならない。

イ 限定公開情報の管理
（ア） 限定公開情報は、限定された者のみにアクセスを制限し（部局内、学内など）、それ以外の者にアクセスさせてはならない。
（イ） 限定公開情報は、保管方法など管理に関する事項を、必要に応じて定めなければならない。

ウ 公開情報の管理
（ア） 公開情報は、保管方法など管理に関する事項を、必要に応じて定めなければならない。
（イ） 公開情報は不特定の者がアクセス可能な性質を持つものであるため、管理者は情報の改ざんや偽情報の流布に対し、必要に応じて防止策を講じなければならない。

エ 情報の部分的公開
非公開及び限定公開情報の一部を不特定の者に開示する場合には、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、公開できる情報だけを抽出するか、あるいは統計処理などの加工を行わなければならない。

オ 外部委託に伴う情報の持ち出し
外部業務委託等のため、非公開情報を限定された第三者に開示する必要がある場合は、守秘義務契約を結ばなければならない。

カ 情報改ざん及び偽情報流布
公開情報は、改ざんへの対策を講じるとともに、常に進化する不正アクセス技術の脅威を想定しておかなくてはならない。

キ 情報機器及び記憶媒体の処分
分類に関わらず、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。特に、ハードディスク、フラッシュメモリ等の記憶媒体は、通常の消去操作では管理情報のみが消去されるだけでデータそのものは消去されないこと、また、数回の上書き消去では残留磁気情報等の読み出しによって情報を復元できることに、十分配慮しなければならない。さらに、情報機器の記憶媒体を保守契約により交換する場合、又はレンタル機器の撤去を行う場合は、撤去後の記憶媒体の処理法についても十分配慮しなければならない。

3 物理的セキュリティ

ポリシーに基づき、本学のネットワークに接続するすべてのクライアント機器、サーバ機器及びネットワーク機器に関する情報セキュリティの維持に必要な物理的対策について、以下に示す。

（1） クライアント機器

クライアント機器とは、学内で使用されるパソコン（研究用、事務用、演習室端末、講義室端末、学内者・学外者持ち込み）、プリンタ、携帯端末等学内ネットワークに接続可能な装置を指す。

ア ネットワークへの接続

クライアント機器をネットワークへ接続する場合、以下のような物理的対策を講じなければならない。

（ア） 有線（ネットワークケーブル）を使用する場合には、過失によるケーブル切断を防ぐための措置を施すこと。

（イ） 有線、無線どちらの場合においても、ネットワークの盗聴に対する対策を施すこと。

（ウ） クライアント機器接続用のネットワークケーブルに、許可なく別の機器が接続されても通信できないよう対策を施すこと。

イ クライアント機器の保全

クライアント機器は、許可なく学外に持ち出されないよう次のような対策を講じなければならない。

（ア） クライアント機器を室内に設置する場合、その部屋を空けるときは施錠すること。

（イ） クライアント機器をオープンスペース等に設置する場合には、ワイヤー等により固定すること。

ウ クライアント機器の持ち出し

大学構成員がクライアント機器を学外に持ち出す場合は、盗難、紛失、情報漏えい、ウイルス感染、不正アクセス等が発生しないよう、十分に留意しなければならない。

（2） サーバ機器

ア 管理区域の設置

サーバ機器は、以下の条件を満たす管理区域に設置されなければならない。

（ア） サーバ機器については、第三者の認証と入退室の記録が残される隔離された区域を設定すること。

（イ） 管理区域は、許可された特定の者以外には公開しないこと。

（ウ） サーバ機器については、十分な熱対策を行い、加熱による障害が起こらないよう留意すること。また、サーバ集約、仮想化等により、熱の発生自体を抑えるよう努めること。

イ 電源

電源を供給する際には、電圧の変動や突発的な停電、過電流に対応する装置を経由しなければならない。

ウ　ネットワークへの接続

サーバ機器をネットワークへ接続する場合、以下のような情報セキュリティ対策を講じなければならない。

（ア）　有線（ネットワークケーブル）を使用する場合には、過失によるケーブル切断を防ぐための措置を施すこと。

（イ）　有線、無線どちらの場合においても、ネットワークの盗聴に対する対策を施すこと。

エ　データのバックアップ

サーバ機器に記録されるデータは、定期的にバックアップをしなければならない。

オ　多重化

停止したときに大学の業務遂行に重大な支障をきたすサーバ機器については、多重化しなければならない。

カ　サーバ機器の保全

管理者は、サーバ機器が管理区域から許可なく持ち出されないよう、ラックへの固定、設置場所の施錠などの対策を施さなければならない。

キ　災害への対策

サーバ機器や管理区域については、以下のような災害への対策を講じなければならない。

（ア）　サーバ機器は、耐震を考慮した据付を行うこと。

（イ）　管理区域には、火災の一次消火手段が提供されること。

ク　保守

保守については、保守部品をできるだけ確保し、迅速に対応できる体制を整えなければならない。

（3）　ネットワーク機器

ア　ネットワークの制御・管理機器について

ネットワークの制御・管理機器は、許可された特定の者以外は使用できないように、施錠などによって物理的に隔離された区域に設置しなければならない。

イ　設置場所の秘匿

ネットワークの制御・管理機器については、その設置場所を許可された特定の者以外に公開してはならない。

ウ　多重化

ネットワークの制御・管理機器については、多重化による信頼性の向上を検討しなければならない。

エ　保守

保守については、保守部品をできるだけ確保し、迅速に対応できる体制を整えなければならない。

4 技術的セキュリティ

ポリシーに基づき、本学のネットワーク及び機器の設定、運用等に関する情報セキュリティの維持に必要な技術的対策について、以下に示す。

（1） ネットワークの運用

ア ネットワークの設計及び改変

キャンパスネットワークの設計・構築にあたっては、人事給与システム等の事務系、学生支援システム等の教育系及び図書情報系など、目的の異なるネットワークを混在させてはならない。

イ セキュリティ機器及びその運用

（ア） 本学のネットワークにはファイアウォール、侵入検知システム及びその他必要と思われるセキュリティ機器を導入し、外部からの脅威に対処できるようにしなければならない。

（イ） これらの機器をネットワーク性能の向上や新たな脅威の出現に対応できるよう、最新のものにするよう努めなければならない。

（2） 機器の運用

ア アクセス制御

管理者は、クライアント機器、サーバ機器及びネットワーク機器に対して、以下のようなアクセス制御を行なわなければならない。

（ア） ネットワークへのアクセスに際しては、利用者ごとにユーザＩＤを発行し、認証を行なうこと。また、同じユーザＩＤを複数の利用者で共有しないこと。

（イ） 利用者の権限に応じ、アクセスできるデータや操作を限定すること。

（ウ） 無線ＬＡＮのアクセスポイントを設置する場合は、想定した利用者のみがアクセスできるよう、適切なアクセス制御を行なうこと。また、適宜、物理アドレス（ＭＡＣアドレス）による接続制限を実施すること。

イ システムの更新

管理者は、クライアント機器、サーバ機器及びネットワーク機器について、適宜システムを更新し、最新のものにするよう努めなければならない。

（ア） 機器に情報セキュリティ上の脆弱性が発見された場合には、遅滞なくハードウェア・ソフトウェアの更新又は設定変更などの対策を行なうよう努めること。

（イ） 機器の機能や性能の向上、障害対応等のためのハードウェア・ソフトウェアの更新又は設定変更などは、必要に応じて実施すること。

ウ ウイルス対策

管理者は、クライアント機器、サーバ機器について、以下のようなウイルス対策を行なわなければならない。

（ア） 原則として全てのクライアント機器には、ウイルス対策ソフトを導入すること。

（イ） サーバ機器には、その用途を考慮したウイルス対策ソフトを導入すること。

（ウ） ウイルス対策ソフトを導入した機器は、システムを起動している限りにおいて毎日１回以上はウイルス検出パターンの更新を行なうことが望ましい。また、週１回以上はシステムの全ファイルに対してウイルススキャンを行なうことが望ましい。

エ 機器の新規接続

クライアント機器、サーバ機器及びネットワーク機器を新たにネットワークに接続する際には、アクセス制御の設定がなされ(４(２)ア)、システムが最新の状態に更新され(４(２)イ)、ウイルス対策が施された(４(２)ウ)状態でなければならない。

オ 履歴情報の取得

管理者はサーバ機器及びネットワーク機器について、以下の履歴情報（ログ）を取得すること。

（ア） システムへの認証を伴うログイン記録。

（イ） 公開しているサービスを利用したクライアントのＩＰアドレス等。

（ウ） その他、システムの運用に関する記録。

カ 履歴情報等の解析

管理者は、履歴情報及び通信内容の解析等にあたって、以下の事項を遵守しなければならない。

（ア） 日常的なシステム監視業務において履歴情報を利用する場合は、個別のアクセス・通信等の記録を閲覧する必要がないよう、自動的に統計処理を行なうこと。

（イ） システムが正常に運用されていることを確認する場合、又は不正アクセスや情報漏えいなど、正規外の利用が行なわれた恐れがある場合に限り、利用者のアクセスや通信を記録した履歴情報（日時、アドレス等）を閲覧することができること。

（ウ） 前号の記録だけでは、不正アクセスや情報漏えい等の実態を解析できない場合に限り、利用者の通信内容等を閲覧することができること。この場合、閲覧した日時、ファイル名等を記録しておくこと。

５ 人的セキュリティ

ポリシーに基づき、本学の情報セキュリティの維持に必要な人的な対策について、以下に示す。

（１） 技術対策員の遵守事項

技術対策員は、以下の事項を遵守しなければならない。

ア 対策基準に従い、適正にシステムを管理運用すること。

イ 技術対策員の監督下において教職員又は学生等にシステム管理業務を補助させる場合、これらの者によるシステム管理業務の責任と権限の範囲を明確に定め、これを厳守させること。

ウ 履歴情報及び通信内容の解析等にあたっては、（４(２)カ）に掲げる要件に従うとともに、利用者のプライバシーに配慮し、職務上知り得た秘密を漏らさないこと。

（２） 大学構成員の遵守事項

大学構成員は、以下の事項を遵守しなければならない。

ア ポリシーに従い、情報セキュリティの維持に努めなければならない。

イ　利用資格のない情報システム及び許可されていない情報にアクセスしたり、アクセスを試みたりしてはならない。
ウ　自己のパスワードは秘密としなければならない。また、十分な情報セキュリティを維持できるよう、自己のパスワードの設定及び変更に配慮しなければならない。
エ　他の利用者のユーザＩＤを使用してはならない。また、いかなる場合も他の利用者のパスワードを聞き出してはならない。
オ　管理者が、不適切なパスワードの変更を求めた場合、大学構成員はその指示に従わなければならない。
カ　使用中のクライアント機器から一定時間離れる場合は、パスワード付きのスクリーンセーバーなどにより、第三者の操作から保護しなければならない。
キ　管理者から情報セキュリティの維持管理のために協力を依頼された場合には従わなければならない。
ク　学内ネットワークに接続された端末においては、教育・研究・学習・業務に関連したソフトウェアのみ使用することができる。
ケ　大学構成員は、研修会や説明会又は講義などを通じ、ポリシーを理解し、情報セキュリティ上の問題が生じないように努めなければならない。

（3）　不正アクセス・事故等への対応

ア　不正アクセス・事故等の発見
（ア）　利用者は、情報セキュリティに関する事故、情報システムの不審な動作、不正アクセス（侵入、情報漏えい、改ざん等）、システム上の障害及び誤動作を発見した場合には、直ちに管理者に報告しなければならない。
（イ）　管理者は、報告のあった事故等について必要な措置を講じなければならない。

イ　不正アクセス・事故等の緊急措置
（ア）　管理者は、発生した事故等が第三者による不正アクセスによるものである場合、直ちに当該機器をネットワークから分離するとともに、アクセス記録の保全、適正なデータや設定の回復、原因の分析等必要な措置を行ない、再発防止のための対策を講じなければならない。
（イ）　管理者は、発生した事故等がウイルスの感染や第三者からの攻撃等である場合、直ちに当該機器をネットワークから分離するとともに、アクセス記録の保全、ウイルスの駆除、セキュリティホールの除去等必要な措置を行ない、再発防止のための対策を講じなければならない。
（ウ）　学内からの不正アクセス等によって学内外に被害を及ぼし、社会的に重大な信用問題等が発生する場合は、直ちに統括責任者の判断のもと、関連する通信を遮断し、又は該当する機器を切り離すとともに、被害者や関係者への事実関係の説明、再発防止のための対策、その他必要な措置を実施しなければならない。
（エ）　利用者に対する情報セキュリティ上の事故・障害の通知は、問題の程度に応じた適切な表現に配慮し、速やかに行わなければならない。

（4）　教職員・学生以外の利用

ア　情報システムの開発・保守及び管理業務

情報システムの開発・保守及びシステム管理業務を外部委託事業者に発注する場合は、外部委託事業者から下請けとして受託する業者を含めて、ポリシーに基づき外部委託事業者が守るべき内容の遵守を明記した契約を行わなければならない。

イ　学外利用者の機器持ち込み

教職員又は学生以外の者が、クライアント機器を持ち込み、本学のネットワークに接続して利用する場合、管理者は学外利用者にポリシーの内容を理解させ、実施及び遵守させるための適切な措置を施さなければならない。

ウ　来学者等の一時利用

学会等のために期限を設定して来学者等に情報ネットワークを一時的に利用させる場合、以下のようにしなければならない。

（ア）　情報ネットワークへのアクセスを提供する場合は必要最低限とし、学内の共有サーバーなどへのアクセスは制限すること。

（イ）　接続機器の物理アドレスを記録することが望ましい。

6　対策基準の見直し

委員会は定期的に対策基準の実効性を評価する。見直しが必要な場合、総括責任者は対策基準の更新を実施しなければならない。

附　則

この規程は、平成 25 年４月１日から施行する。