尾道市立大学情報セキュリティポリシー

平成 26 年 4 月 1 日

改版履歴

年月日	内容等
平成 25 年 2 月 1 日	尾道市立大学情報セキュリティポリシーを策定
平成 26 年 4 月 1 日	「2.1 組織・体制」、「2.4.2.1 役割・責任及び免責事項」を一部改正

1　基本方針

1.1　情報セキュリティの基本方針

尾道市立大学（以下「本学」という。)は、学術研究の中心として、広く知識を授けるとともに、深く専門の学術を教授研究し、真理と平和を希求する人間の育成を図り、学理とその応用を攻究し、国の内外と地域の向上発展に貢献することを目的としている。この目的達成のため様々な活動を行うなかで、本学はこれまで多くの情報資源を受け入れ、保有・活用し、同時にまた新たな情報資源を発信してきた。

これら情報資源を資産とし、健全な運用、発展を図り、広く学内外で活用していくためには、高い信頼性、可用性、保守性、機密性及び保全性を持つ情報基盤の存在が必須である。同時に、本学構成員においては、情報資産を保全する上での情報セキュリティにかかわる正しい共通認識を確立することが、不可欠の条件として求められる。この論拠に立って、本学は不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号)、著作権法（昭和 45 年法律第 48 号）個人情報の保護に関する法律（平成 15 年法律第 57 号）など、関連する法令を踏まえ、本学の情報セキュリティ対策の包括的な指針として、尾道市立大学情報セキュリティポリシーをここに定める。本学が提供するサービスを利用するすべての関係者は、本学における諸活動のなかで本ポリシーを理解し、その立場に基づいて情報資産の活用と保全に努めなければならない。

1.2　情報セキュリティポリシーの目指すもの

本ポリシーは、本学における情報セキュリティの方針を示すものであり、その目指すものは次のとおりである。

(1) 本学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、重要度による分類に応じて管理する。
(4) 情報セキュリティに関する情報取得を支援し、情報セキュリティポリシーの評価と見直しを行う。

1.3　対象範囲

本ポリシーの対象範囲は、本学が保有し、情報ネットワーク・システム上で取り扱う情報資産及び本学の情報ネットワークに継続的又は一時的に接続されるすべての情報機器とする。本ポリシーの対象者は、教職員、非常勤教職員、委託業者、大学院生、大学生、研究生、聴講生、公開講座受講生、来学者など、本学の情報ネットワーク又は情報資産を使用する関係者すべてとする。

2　対策基準

2.1　組織・体制

情報セキュリティ対策は、次に掲げる管理体制に基づいて実施するものとする。

(1) 最高情報セキュリティ責任者

本学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責任者を置く。最高情報セキュリティ責任者には学長を充てる。

(2) 全学情報システム管理責任者

本学の情報セキュリティを統括管理するために、全学情報システム管理責任者を置く。全学情報システム管理責任者には情報処理研究センター長を充てる。

(3) 全学情報システム技術担当責任者

情報セキュリティ担当部局は情報処理研究センターとし、当該センターには全学の情報ネットワーク・システムに関する実務上の責任者として、全学情報システム管理責任者を補佐する全学情報システム技術担当責任者を置く。全学情報システム技術担当責任者は、全学情報システム管理責任者より指名された情報処理研究センター職員を充てる。

(4) 部局情報管理責任者

部局内の情報管理の実施及び全学情報システム管理責任者との連絡などの対応に当たるため部局情報管理責任者を置く。部局情報管理責任者には、所属長（研究科長、学部長、学科長、室長、課長、センター長、館長）を充てる。

(5) 部局情報セキュリティ担当者

部局内における情報セキュリティ活動を行うため部局情報セキュリティ担当者を置く。部局情報セキュリティ担当者は、部局情報管理責任者より指名された者を充てる。

(6) 情報処理研究センター運営委員会（以下、「運営委員会」という）

情報セキュリティに関する基本方針の策定・改訂を含む重要事項の決定は運営委員会が行う。また、情報ネットワーク・システムの運用において、情報セキュリティに関する必要なことを審議する。

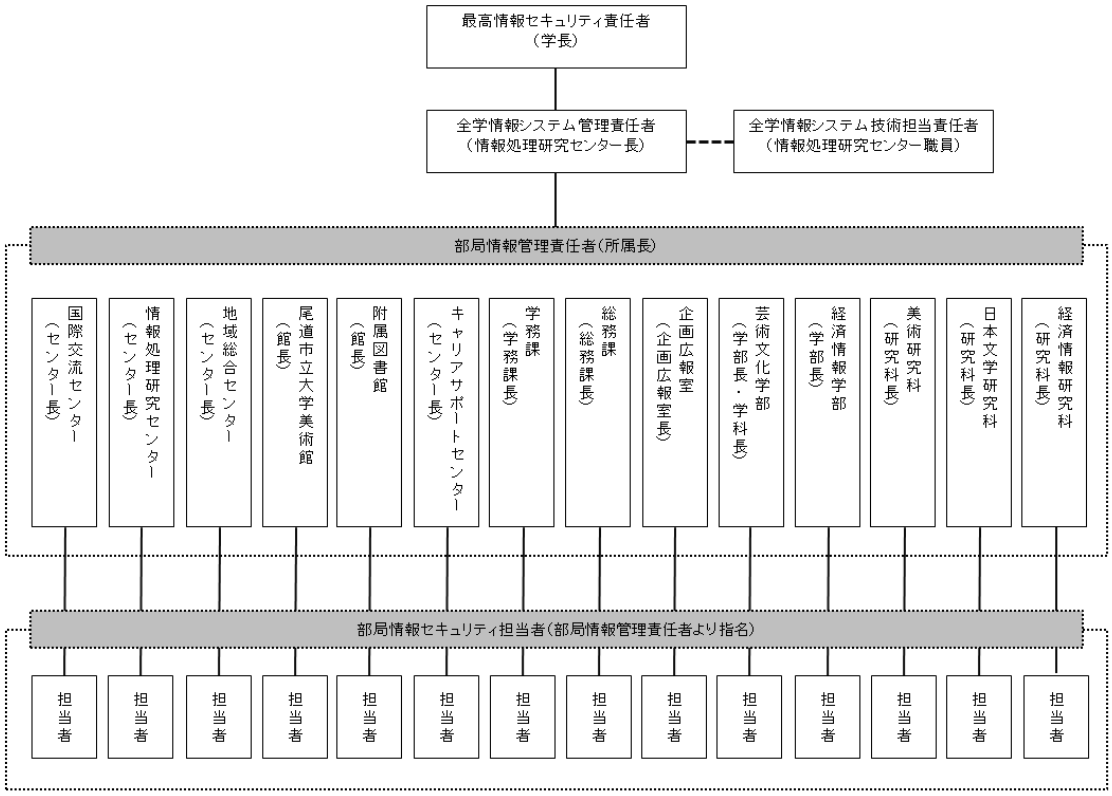

図１　情報セキュリティ管理体制図

2.2　対策実施にかかわる手順と啓発

本ポリシーの具体的な実施要領は、運営委員会が全学的に定め、部局の具体的な実施手順は、必要に応じて部局で定めるものとする。運営委員会は、以下に述べる物理的、人的、技術的な情報セキュリティ対策を具体的に定め、実施しなければならない。また、本ポリシーのすべての対象者に、それぞれに応じた教育、研修、啓発等を行い、情報セキュリティの重要性を理解させなければならない。

2.3　情報セキュリティ対策の大要

2.3.1　情報の分類に応じた管理

すべての情報は、非公開情報・部分公開情報・公開情報といった情報の重要度による分類を行い、それに応じてそれぞれ定められた情報セキュリティ保護対策を講じなければならない。

2.3.2　情報セキュリティ侵害の阻止

全学情報システム管理責任者は、外部又は内部からの不正アクセスが検出された場合、運営委員会が定める措置手順に従い、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。

2.3.3　学内外の情報セキュリティを損ねる加害行為の抑止

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

2.3.4　本ポリシー違反者への措置

本ポリシーに違反した者に対して、運営委員会は、権限を有する意思決定機関に処分の勧告を行うことができる。

2.4　情報セキュリティ対策

2.4.1　物理的セキュリティ

2.4.1.1　装置の設置

(1) 基幹装置の取付け等

情報ネットワーク・システムを構成する重要な基幹装置は、施錠などによって物理的に隔離された区域で、火災、水害、ほこり、振動、温度、湿度等の影響を可能な限り排除した場所に設置するものとする。

(2) 情報システム機器の盗難防止対策

据付型パソコン端末機器又はサーバ及びネットワーク機器などの情報システム機器は、盗難防止などの対策を施さなければならない。

(3) 電源

情報ネットワーク・システムを構成する重要な基幹装置の電源には、十分な電力を供給する容量の予備電源を備え付けなければならない。また、落雷等による過電流から基幹装置を保護するために適切な措置を施さなければならない。

(4) 配線

配線は、盗聴、損傷等を受けることがないように適切な措置を施さなければならない。また、ネットワーク接続口（ＨＵＢのポート等）は、不特定の者によって接続が行われないような措置を施さなければならない。

(5) 機器の多重化

機器の障害によるネットワーク停止が重大な影響を及ぼさないようサーバ及びネットワーク機器については、多重化による信頼性の向上を検討しなければならない。

2.4.1.2　貸出用情報機器の備品管理

貸出用情報機器を学外に持ち出す場合においては、貸出しの事実について記録し、機器経由による秘密又は非公開情報の漏えいが発生しないよう留意しなければならない。

2.4.1.3　管理区域

情報ネットワーク・システムを構成する重要な基幹装置は、情報セキュリティ担当部局が管理する区域(以下「コンピュータ機器室」という。)に設置しなければならない。室内は温度、湿度にも配慮し、機器類は耐震対策を講じた場所に設置するとともに、防火措置等を施さなければならない。

コンピュータ機器室には、許可された者のみ入室できるような入退室管理が行われ、外部からの侵入を防止するための対策が施されなければならない。保守作業及び機器等の搬入には、必ず情報セキュリティ担当部局の職員等が立ち会わなければならない。

2.4.2　人的セキュリティ

2.4.2.1　役割・責任及び免責事項

(1) 最高情報セキュリティ責任者

最高情報セキュリティ責任者は、情報セキュリティポリシーに基づき、学内の全ての情報セキュリティに関する総括的な権限と責任を有し、以下のことを実施する。

(a) 全学情報システム管理責任者による定常的なセキュリティ対策の措置及びセキュリティ管理の状況に関する報告に対処する。

(b) 理事会、教授会等への情報セキュリティに関する重要事項の報告又は勧告を行う。

(c) 情報セキュリティに関する学外からの苦情への対応及び学外から受けた被害への対応に当たる。

(2) 全学情報システム管理責任者

全学情報システム管理責任者は、全学の情報ネットワーク・システムが円滑に運用されるように、情報セキュリティの保持と強化のための技術的な調査検討を行うとともに、緊急時の総括的な連絡窓口として機能する。また、全学情報システム技術担当責任者に指示して、以下のことを実施する。

(a) 情報セキュリティを守るために必要と判断したときは、緊急避難措置をとることができる。ただし、その措置によって影響を及ぼすと判断できる情報資源の部局情報管理責任者にその旨を速やかに通知しなければならない。

(b) 部局情報管理責任者から対応策の実施が完了した旨の届出があった場合、速やかに対応策を検討し、十分であると判断したときは緊急避難措置を直ちに解除する。また、部局情報管理責任者から緊急避難措置の依頼があったときも必要性を判断し通

知する。

(c) 全学の情報セキュリティの管理及び監査の実施に関し、最高情報セキュリティ責任者を補佐し、情報セキュリティの保持と強化のために必要な技術的措置を講じる。

(3) 全学情報システム技術担当責任者

全学情報システム技術担当責任者は、全学情報システム管理責任者を補佐し、その指示に従い全学の情報ネットワーク・システムの管理運用の実務を担当するとともに、情報セキュリティの保持と強化のために必要な技術的措置を実施する。

(4) 部局情報管理責任者

部局情報管理責任者は、情報セキュリティの保持のため、当該部局の情報管理が円滑に執り行われるよう機能する。

(5) 部局情報セキュリティ担当者

部局情報セキュリティ担当者は、部局情報管理責任者を補佐し、その指示に従い部局内における情報ネットワーク・システムの管理運用の実務を担当するとともに、情報セキュリティの保持と強化のために必要な技術的措置を実施する。

(6) 利用者

本ポリシーの対象者は、情報セキュリティポリシーを遵守しなければならない。また、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、それに従わなければならない。

2.4.2.2 教育・研修

(1) 教育の実施

運営委員会は、システム管理者等が行う教職員向けの本ポリシーに関する研修の支援をしなければならない。また、教職員が行う学生向けの本ポリシーに関するオリエンテーション又は講義に協力しなければならない。

(2) 教育の受講

すべての教職員及び学生は、研修会若しくは説明会又は講義等に参加し、本ポリシー及び実施手順を理解し、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。

2.4.2.3 事故・障害の発生時の対処

本ポリシーの対象者は、情報セキュリティに関する事故、システム上の障害を発見した場合には、情報セキュリティ担当部局に直ちに報告しなければならない。全学情報システ

ム管理責任者及び全学情報システム技術担当責任者は、報告のあった事故等について被害の状況を調査し、被害の規模を把握し、必要な措置を直ちに講じなければならない。全学情報システム管理責任者は、発生した事故等に関する記録を一定期間保存し、運営委員会に報告するとともに、重大な事故に対しては、迅速な再発防止のための対策を講じなければならない。

2.4.2.4　パスワード管理

(1) 利用者向け

自己のパスワードは、秘密にしなければならない。また、他の利用者のパスワードを聞き出したり、他の利用者のアカウントを使用したりしてはならない。システムの管理権限を有する者や他の利用者になりすました第三者からのパスワードの聞取りには、如何なる場合も応じてはならない。

(2) システム管理者向け

情報セキュリティ担当部局におけるシステム管理者は、情報システムの利用資格者の規程を定めなければならない。また、規程に基づく利用資格を有する者以外に情報端末のアカウントを発行してはならない。また、利用資格を失った利用者のアカウントは、直ちに抹消されなければならない。利用者のアカウントを管理権限のない第三者に漏えいしてはならない。ログ情報及び通信内容の解析等にあたっては、利用者のプライバシーに配慮し、閲覧解析を認める場合の要件及び手続を明確にしておかなければならない。

2.4.2.5　非常勤の教職員及び臨時職員

非常勤の教職員及び臨時職員（外部委託業者を含む。）には、雇用契約の際に、守るべきポリシーの内容を理解させ、実施及び遵守を確保しなければならない。

2.4.2.6　外部委託

情報システムの開発及び保守並びにシステム管理業務を外部委託業者に発注する場合は、外部委託業者から下請けとして受託する業者を含めて、必要なセキュリティ対策が確保されていることを確認するとともに、守秘義務及び必要なセキュリティ要件、遵守すべき内容について明記した契約を締結しなければならない。また、外部委託業者との契約書には、責任所在の境界及び本ポリシーが遵守されなかった場合の規定を定めなければならない。

また、外部委託業者が学外から学内情報システムに VPN 接続等によりアクセスする必要がある場合には情報処理研究センター長に申請してその許可を得なければならない。

2.4.3　技術的セキュリティ

情報ネットワーク・システムを様々な脅威から保護するため、全学情報システム技術担当責任者は、技術的対策及び運用管理についての対策を講じなければならない。なお、以降の項目に関する詳細な実施手順については、別途「情報セキュリティ維持管理のための技術的実施手順」に定めるものとする。

2.4.3.1　コンピュータ及びネットワークの技術的対策

(1) メール対策

メールサーバには、不正中継処理対策、スパムメール対策及びウイルス対策を講じなければならない。

(2) 暗号化

有線及び無線どちらにおいても、パスワード又は機密情報がネットワーク上を流れる際には必要に応じて暗号化されるよう設定を施さなければならない。

(3) アクセス制御

本学情報資源、ネットワークサービス等については、資源及びサービスごとにアクセスできる者を定め、権限のないものがアクセスできないように制限しなければならない。また、外部ネットワークとの接続においては、ファイアウォール装置などを用いたネットワークアクセス制御を行わなければならない。

(4) コンピュータウィルス対策

サーバレベルでウィルスチェックを行い、学外からのウイルスの侵入及び外部へのウイルス拡散を防止するよう対策を講じなければならない。また、パソコン端末機器においてはリアルタイムでウィルスチェックが行われるような対策を講じなければならない。

(5) 不正アクセス対策

公開を目的としたサーバは、内部ネットワークと異なるネットワーク上に配置するものとする。サーバは必要最小限のポートを開けるものとし、使用していないサービスは停止しなければならない。また、不正侵入を検出可能な侵入検知システムを導入しなければならない。

2.4.3.2　ネットワーク運用管理

(1) セキュリティ情報の収集

セキュリティに関する情報を収集し、セキュリティ対策上必要な措置を講じるとともに、これらの情報を定期に取りまとめ、本ポリシーの改定につながる情報については、運営委員会に報告しなければならない。

(2) 情報システムの監視

セキュリティに関する事案を検知するため、常に情報システムの監視を行わなければならない。

(3) 記録の管理

学内情報ネットワーク・システムにおけるシステム変更等の記録、情報システムの障害に対処した際の障害記録、サーバへアクセス等の各種システムに関する記録を維持管理しなければならない。

(4) 媒体の管理

機密情報が記録された記録媒体（電子媒体、紙媒体）を、第三者に使用されること、又は許可なく情報を閲覧されることがないように配慮しなければならない。

(5) バックアップ管理

機密情報等を保持しているホストコンピュータ及びサーバ等に記録された情報について、その重要度に応じて期間を設定し、定期的にバックアップ用の複製を作成しなければならない。

(6) 情報システムの開発、導入及び変更

ソフトウェアの開発及び変更並びに運用機器及び基本ソフトウェアの導入、保守及び撤去については手順及び基準を明らかにしなければならない。また、それらの事項について情報セキュリティ上問題がないように対処しなければならない。

(7) 機器の修理及び廃棄

機密情報等が含まれる機器について、外部業者に修理させ、又は廃棄する場合は、その内容が消去された状態で行わせなければならない。

(8) 情報システム仕様書等の管理

情報システム仕様書について、記録媒体にかかわらず業務上必要とする者のみが閲覧できる場所に保管しなければならない。

(9) 機器情報の把握

情報ネットワーク・システムの安全な環境を維持するため、情報ネットワーク・システムを構成するすべての機器について情報を把握しなければならない。また、システムの安全な運用上、問題があると認められた場合は、その可否について全学情報システム管理責任者と協議・検討を行うものとする。

3 評価と見直し

3.1 情報セキュリティ運用実態の把握

全学情報システム管理責任者は、部局情報管理責任者からの情報セキュリティに関する情報の収集・分析並びに情報資産の運用状況に対する情報を収集し、情報セキュリティ診断を行って、結果を運営委員会に報告しなければならない。

3.2 本ポリシーの評価・更新

運営委員会は、この報告に基づき、本ポリシーの実効性を少なくとも年 1 回評価し、必要と判断した場合、より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。本ポリシーの更新は、運営委員会で協議の上、理事会の議を経て学長が行う。

3.3 情報セキュリティ計画の作成

運営委員会は、評価の結果を踏まえ、次年度の情報セキュリティ計画の作成を行わなければならない。