別紙２

公立大学法人下関市立大学情報システムにより処理される情報資産に関するセキュリティポリシー

第１章　情報セキュリティ基本方針

１．目的

公立大学法人下関市立大学（以下「本学」という。）が管理責任を有する情報資産には、学生、教員及び事務職員の個人情報や大学運営上重要な情報など、漏えい、改ざん及び破壊等が発生した場合には極めて重大な結果を招く情報が数多く含まれている。

本学の情報資産を改ざん、漏えい及び破壊等の脅威から守ることは、本学の財産、プライバシー等を守るとともに、本学における教育研究活動及び大学運営になくてはならない情報基盤の安定かつ効率的な運用を実現するためにも必要不可欠である。

このような状況を踏まえ、本学の情報資産の機密性、完全性及び可用性を維持するため、情報システムにより処理される情報資産に関して、セキュリティポリシーを定めることとする。このうち、情報セキュリティ基本方針については、本学の情報セキュリティ対策の基本的な方策として、このセキュリティポリシーの対象範囲を定めるものとする。

２．定義

2.1　情報システム

本学が管理する電子計算組織（「ハードウェア、ソフトウェア、ネットワーク、記録媒体等」をいう。）で構成し、これら全体で業務処理を行うもの

2.2　情報資産

情報システムにより処理される情報及び情報を管理する仕組み（情報システム並びにシステム開発、運用及び保守のための資料等）の総称

2.3　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

2.4　情報セキュリティポリシー

本学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。情報セキュリティ基本方針と情報セキュリティ対策基準から構成される。

３．対象範囲及び対象者

情報セキュリティポリシーの対象範囲は、本学が管理するすべての情報資産、学内ネットワーク、学内サーバ機器、本学が管理するパソコン等の情報端末やネットワーク関連機器とする。

情報セキュリティポリシーの対象者は、本学の役員、教員及び事務職員、非常勤教員、学生、業務委託業者、来学者等、本学が管理する情報資産を取り扱うすべての者（以下「利用者」という。）とする。

４．情報資産を取り扱う者の責務

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、情報資産の取り扱いに際して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。

５．情報セキュリティ管理体制

本学が管理する情報資産について、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。

６．情報資産の分類

本学の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。

７．評価及び見直し

情報セキュリティポリシーに定める事項及び情報セキュリティ対策についての評価を行うとともに、情報資産を取り巻く状況の変化に柔軟に対応するため、適宜、情報セキュリティポリシーの見直しを実施する。

第２章　情報セキュリティ対策基準

１．組織・体制

情報セキュリティ管理については、以下の組織・体制とする。

1.1　管理・運用組織の構成

1.1.1　最高情報セキュリティ責任者

本学の情報セキュリティに関する総括的な意思決定と、学内及び学外に対する責任を負う最高責任者として最高情報セキュリティ責任者を置き、理事長をもってこれに充てる。

1.1.2　情報セキュリティ委員会

最高情報セキュリティ責任者は、情報セキュリティの維持及び向上に必要であると判断したときは、適時、情報セキュリティ委員会を設置することができる。情報セキュリティ委員会は、経営企画会議の委員及びシステム管理責任者をもって構成する。

1.1.3　全学情報セキュリティ管理責任者

教育研究部門及び事務部門の情報システム管理に関する統括的な権限及び責任を有する管理責任者として、全学情報セキュリティ管理責任者及び全学情報セキュリティ副管理責任者を置く。全学情報セキュリティ管理責任者は、学長をもってこれに充て、全学情報セキュリティ副管理責任者は、事務局長をもってこれに充てる。

1.1.4　システム管理責任者

情報システム管理に関する管理責任者としてシステム管理責任者を置き、ネットワークシステム運営委員長をもってこれに充てる。

1.1.5　部局システム管理者

部局内の情報システム管理の実施に関する管理者として部局システム管理者を置き、学部長、研究科長及び各グループの長をもってこれに充てる。

1.1.6　ネットワークシステム運営委員会

本学の情報セキュリティに関し、情報セキュリティの維持及び向上を図るための活動を行う。具体的な活動内容としては以下の項目とする。

・情報セキュリティポリシーの策定及び改正を行うこと。
・情報セキュリティポリシーの遵守を励行し、違反に対する措置を講ずること。
・緊急事態に対応する即応体制を確立すること。
・学内の他の意思決定機構との調整を行うこと。
・情報セキュリティに関する啓発及び教育を実施すること。
・本学の情報資産に関する監査を実施すること。

1.2　不正アクセス等への対応

ネットワークシステム運営委員会は、学内又は学外からの不正アクセスを検出した場合、関連する通信の遮断又は該当する情報システムの機器の切り離しを実施し、当該機器及び

当該機器が接続されたネットワークの管理者に対して、改善策を指示する。

ネットワークシステム運営委員会は、不正アクセスが継続する場合は、当該管理者に対して、利用停止等の抑止措置をとることができる。

ネットワークシステム運営委員会は、不正アクセス等のセキュリティポリシーに違反した者に対する処分について、その権限を有する意思決定機構に対し、違反行為の報告及び処分の勧告を行う。

２．情報の分類と管理

2.1　情報の分類

本学が保有する情報は、次の重要性分類に従って分類する。

1）重要性分類Ⅰ

漏洩した場合に本学に対する信頼を著しく損なうおそれのある情報と、滅失又は損傷した場合にその復元が著しく困難となり、本学の教育研究活動及び大学運営に著しい障害を生ずるおそれのある情報

- 個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と照合することができ、それにより特定の個人を識別することができることとなるものを含む。）
- 法令又は規程の定めにより守秘義務を課されている情報
- 法人その他の団体に関する情報で漏洩することにより当該団体の利益を害するおそれのあるもの
- 情報システムに係るパスワード及びシステム設定情報
- その他上記に準ずる情報

2）重要性分類Ⅱ

脅威にさらされた場合に実害を受ける危険性は低いが、本学の教育研究活動及び大学運営において重要性が高いと評価される情報（公開されると本学の教育研究活動及び大学運営に支障をきたすおそれのある情報）

3）重要性分類Ⅲ

重要性分類Ⅰ・Ⅱのいずれにも該当しない情報

2.2　情報の管理

- 部局システム管理者は、管理する情報について、情報の内容や重要度に応じて利用権限を定めなければならない。
- 重要性分類Ⅰ・Ⅱに該当する情報は、非公開情報とする。
- 重要性分類Ⅰに該当する情報は、不用意に複製を行ってはならない。
- 重要性分類Ⅰに該当する情報は、不用意に送付及び送信を行ってはならない。
- 重要性分類Ⅰ・Ⅱに該当する情報を記録した取り出しが可能な記憶媒体は、施錠可能な

保管庫等の安全な場所に保管しなければならない。

2.3　記憶媒体の処分

利用者は、記憶媒体を廃棄する際は、当該記憶媒体に保管された重要性分類Ⅰ・Ⅱに該当する情報について、いかなる手段を講じても可読できない状態にしなければならない。

記憶媒体を保守作業等で交換する場合は、撤去後の記憶媒体の処理について十分配慮しなければならない。

３．物理的セキュリティ

3.1　情報端末

ネットワークシステム運営委員会は、情報セキュリティポリシーの対象となる情報端末を把握しなければならない。

部局内の情報システムを管理する者（以下「システム管理者」という。）は、情報端末について災害、事故及び盗難への対策を可能な限り講じなければならない。

3.2　サーバ機器

3.2.1　管理区域の設置

サーバ機器は、施錠が可能な管理区域に設置し、入退出時以外は常時施錠を行うものとする。

管理区域の管理は、システム管理責任者が指名する者が行うこととする。

管理区域に入室できる者は、システム管理責任者が許可する者とする。

管理区域に入室する者は、備え付けの記録簿に必要事項を記載しなければならない。

3.2.2　機器の設置

システム管理者は、管理区域にサーバ機器を設置するときは、火災、水害、埃、温度及び湿度等の影響を可能な限り排除し、管理区域から容易に持ち出されないように、適切な固定等の措置を講じなければならない。

3.2.3　電源

システム管理者は、何らかの原因でサーバ機器に電源異常が発生した場合でも、システムが安全かつ適切に保護されるように対策しなければならない。

3.2.4　データのバックアップ

システム管理者は、サーバ機器に記録、保管されるデータについて定期的にバックアップを行わなければならない。

システム管理者は、データをバックアップした記憶媒体を、予め定めた期間、安全に保管しなければならない。

3.2.5　冗長化

システム管理者は、障害が発生した場合に教育研究及び大学運営上重大な影響を及ぼすサーバ機器について、サーバ機器の冗長化等の措置を講じなければならない。

3.3　ネットワーク機器

3.3.1　設置場所の隔離

学内ネットワークの基幹部分を構成する重要なネットワーク機器は、施錠等によって物理的に隔離された区域に設置し、設置場所から容易に持ち出されないように、適切な固定等の措置を講じなければならない。

3.3.2　電源

システム管理者は、何らかの原因でネットワーク機器に電源異常が発生した場合でも、ネットワーク機器が安全かつ適切に保護されるように対策しなければならない。

3.3.3　ネットワークケーブル

学内ネットワークの基幹部分を構成する重要なネットワークケーブルは、故意又は過失によるケーブルの切断を防ぐため、原則として専用又は共用の配管に敷設しなければならない。

ネットワークケーブルを敷設するときは、ネットワークケーブルに起因する障害発生時の影響を考慮した上で、予備回線や迂回回線の敷設について考慮しなければならない。

3.3.4　冗長化

システム管理者は、障害が発生した場合に教育研究及び大学運営上重大な影響を及ぼすネットワーク機器について、ネットワーク機器の冗長化等の措置を講じなければならない。

４．人的セキュリティ

4.1　利用者の責務

利用者は、情報セキュリティポリシーに定められた事項を遵守しなければならない。

利用者は、学内ネットワークの管理及び運用のためシステム管理責任者及び部局システム管理者から協力依頼があった場合は、これに協力しなければならない。

利用者は、情報セキュリティに関する事故が発生し、又は情報システムに関する障害の発生及び発生のおそれがあることを知ったときは、直ちに部局システム管理者に報告しなければならない。

4.2　パスワードの管理

利用者は、自己の保有するパスワードの他人への非公開、パスワードのメモ等を作成しない等パスワードの秘密保持に努めなければならない。

利用者は、初期設定のパスワードは速やかに変更し、また定期的に変更しなければならない。

4.3　情報端末の管理

ネットワークに情報端末を接続しようとする利用者は、ネットワークシステム運営委員会に接続申請を行わなければならない。

利用者は、大学が所有する情報端末を原則として学外に持ち出してはならない。

利用者は、利用中の情報端末から一定時間離れる場合は、ログインした状態で席を離れてはならない。

利用者は、ファイル共有ソフトウェア等、情報流出の原因となり得るソフトウェアをインストールし、又は使用してはならない。

利用者は、基本ソフトウェアのセキュリティ情報更新機能及びコンピュータウィルス対策用ソフトウェアの情報更新機能を、特別な理由がない限り停止してはならない。

利用者は、ネットワークシステム運営委員会の許可なくネットワークの構成及び設定を変更してはならない。

4.4　情報システムの管理

システム管理責任者は、管理する情報システムの利用資格を定めなければならない。

システム管理責任者は、情報システムの利用資格を有する者以外に対して当該情報システムのアカウントを発行してはならない。

システム管理責任者は、利用資格を失った利用者のアカウントを直ちに削除しなければならない。

システム管理責任者は、利用者のアカウント及びパスワードを管理権限のない第三者に漏らしてはならない。

システム管理責任者は、業務上必要な場合のみログ情報及び通信内容の解析を行うものとし、利用者のプライバシーに配慮しなければならない。

4.5　情報システムの開発、保守及び管理業務

システム管理責任者は、情報システムの開発、保守及び管理業務を外部委託事業者に発注するときは、情報セキュリティポリシーのうち外部委託事業者が遵守すべき事項及び守秘義務を明記した契約を締結しなければならない。

５．技術的セキュリティ

5.1　サーバ機器に関する基準

5.1.1　コンピュータウィルス対策

システム管理者は、サーバ機器をコンピュータウィルスによる被害から防ぐため、コンピュータウィルス対策ソフトウェアをサーバ機器に導入しなければならない。また、サーバ機器上のコンピュータウィルス定義情報の更新状況を定期的に確認しなければならない。

5.1.2　基本ソフトウェアのセキュリティ対策

システム管理者は、基本ソフトウェアに関するセキュリティパッチ及び修正プログラムが公開されたときは、稼働中のシステムへの影響を考慮した上で必要と判断される場合は、セキュリティパッチ及び修正プログラムを適用して、セキュリティの脆弱性に対処しなければならない。

5.1.3　利用状況の管理

システム管理者は、サーバ機器の負荷状況やハードディスクの使用状況について随時確認しなければならない。

5.1.4　アクセス記録の保全

システム管理者は、アクセス記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講じなければならない。

5.2　ネットワーク運営方針

5.2.1　ネットワークの設計及び改変

学内ネットワークの運用、管理及び変更は、ネットワークシステム運営委員会が行うものとする。

5.2.2　部局内のネットワーク機器

システム管理者は、管理する対象にルータやスイッチ等のネットワーク機器が含まれる場合は、機器の故障や設定不良により機器の構成や制御機能が損なわれないように管理しなければならない。

5.2.3　セキュリティ対策機器

ネットワークシステム運営委員会は、ファイアウォール等のセキュリティ対策機器を導入して、学外からの不正アクセス等に対する防御や学内から学外に対する攻撃に対処しなければならない。

ネットワークシステム運営委員会は、新たな技術による学内ネットワークへの攻撃に対処できるように、必要と判断される場合は、セキュリティ対策機器及びセキュリティ対策機器上のファームウェアを更新しなければならない。

5.2.4　基幹ネットワーク

システム管理責任者は、ファイアウォール等のログを一定期間保存しなければならない。

システム管理責任者は、定期的にログを解析して不正アクセスの有無を確認しなければならない。

5.3　情報端末に関する基準

学内ネットワークに情報端末を接続しようとする利用者は、ネットワークシステム運営委員会が指定するセキュリティ対策等の設定作業が完了していない情報端末を学内ネットワークに接続してはならない。

ネットワークシステム運営委員会は、常に情報端末の利用者を把握しておかなければならない。

６．評価・見直し

6.1　情報セキュリティポリシー運用実態の把握

部局システム管理者は、情報セキュリティポリシーに沿った情報セキュリティ対策が各部局で実施されているかどうかについて、自己点検を行わなければならない。

システム管理責任者は、部局システム管理者及び利用者から収集した情報セキュリティ

に関する情報を分析及び整理した上で、ネットワークシステム運営委員会に報告しなければならない。

ネットワークシステム運営委員会は、情報セキュリティポリシーの運用実態に基づいて、情報セキュリティポリシーの課題及び問題点について定期的又は必要に応じて検討し、全学情報セキュリティ管理責任者及び全学情報セキュリティ副管理責任者に報告しなければならない。

全学情報セキュリティ管理責任者及び全学情報セキュリティ副管理責任者は、情報セキュリティポリシーが遵守されているかどうかについて、並びに情報システムが支障なく稼動しているかどうかについて確認を行わなければならない。

6.2　セキュリティレベルの向上策

最高情報セキュリティ責任者は、全学情報セキュリティ管理責任者からの報告に基づいて、情報セキュリティポリシーに沿った対策がどの程度実施されているかを評価するとともに、全学情報セキュリティ管理責任者及び全学情報セキュリティ副管理責任者に対して、セキュリティレベルの向上に必要な措置を講ずるように命ずることができる。

附　則

このセキュリティポリシーは、平成 21 年 1 月 1 日から施行する。

情報セキュリティポリシーの管理・運用組織の構成