# 情報セキュリティ対策基準

「跡見学園女子大学情報セキュリティポリシー」（以下「ポリシー」という。）６．の規定に基づき、情報セキュリティ対策基準を以下の通り定める。

## １．組織・体制

情報セキュリティ管理上の組織・体制は以下の通りとする。

### １―１　情報セキュリティ統括責任者

ポリシーに定める情報セキュリティ統括責任者は、全学における情報セキュリティの最高責任者であり、学内すべての情報セキュリティに関し、総括的な権限を有する。

情報セキュリティ統括責任者は、副学長とする。

### １―２　全学システム管理者

全学システム管理者は、情報セキュリティ統括責任者を補佐するとともに、情報システムを円滑に運用し、緊急時には総括的な対応にあたる。

全学システム管理者は情報メディアセンター長とする。

### １―３　部局システム管理者

部局システム管理者は部局システムを円滑に運用するため、情報セキュリティの保持と強化にあたる。

部局システム管理者は部局長とする。

### １―４　システム担当者

システム担当者は情報機器、ソフトウェアを管理し、システムが円滑に運用されるよう、情報セキュリティを確保する。

システム担当者は、全学に関わるシステムは情報サービス課、各部局のシステムは各部局のシステム担当者とする。

### １―５　情報セキュリティ委員会

情報セキュリティ委員会は、情報セキュリティに関する事項の審議を行う。

### １―６　情報利用者

本学が所有し管理する情報資産を利用する者を情報利用者という。情報利用者はポリシーおよび本対策基準で定める各項目を遵守する義務がある。

## ２．情報資産の分類

情報資産は、その機密性、完全性及び可用性に十分配慮したうえで公開情報・非公開情報に分類し、必要に応じ適切に取扱う。

### ２―１　非公開情報

個人情報、事務、教育、研究等の非公開情報を不当に利用してはならない。
これらの情報は、暗号化や盗難防止策を講じ、情報の盗難、漏洩を防止すべく管理しなければならない。情報を記録した媒体は、適切に保管する。

2—2　公開情報

公開情報は適切に利用しなければならない。
情報を公開するときは、公開可能な形に加工したうえ、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するとともに、それらが改ざん、破壊されないよう適切に管理しなければならない。情報を記録した媒体は、適切に保管する。

## 3. セキュリティ対策

情報セキュリティ統括責任者は、物理的・人的・技術的セキュリティの観点から、適切な情報セキュリティ対策を講じなければならない。情報セキュリティのための具体的な対策を以下の通り定める。

3—1　物理的セキュリティ対策

3—1—1　クライアント機器

情報機器を利用するとき、情報利用者は事前に、物理的または電子的認証を受けなければならない。また、これらの機器を所定の利用場所から持ち出すときは、あらかじめ部局システム管理者に届けなければならない。
部局システム管理者は盗難等に対する防止策を講じなければならない。

3—1—2　サーバ機器

サーバ機器は、原則としてデータセンターやサーバ室などの管理された区域内に設置し、部局システム管理者は入退室の管理や警備システムの確保などのセキュリティ確保に努めなければならない。

3—1—3　ネットワーク機器

ネットワーク断によって重大な影響を及ぼすネットワーク機器については、多重化により信頼性を確保しなければならない。

3—2　人的セキュリティ対策

3—2—1　アクセスの制限

部局システム管理者は、情報資産の内容に応じて、アクセス可能な情報利用者を定める。
情報利用者はアクセス権限のない情報にアクセスし、又は利用許可されていない情報を利用してはならない。本学情報システムのクライアント機器の使用およびネットワーク利用に際し、情報利用者は、情報資産の内容に応じて電子的認証を受けなければならない。

3—2—2　教育及び研修

全学システム管理者は、情報利用者に対して、研修会、説明会、授業などを通じて、ポリシーの理解を促さなければならない。

3—2—3　パスワードの管理

自己のパスワードを他に漏らしてはならない。また、自己のパスワードの管理を行わなければならない。

3—2—4　緊急時の対応

情報セキュリティに関する事故や情報セキュリティポリシー違反などにより、情報資産への侵害が発生した場合、部局システム管理者は当該システム担当者に直ちに確認しなければならない。

部局システム管理者及び当該システム担当者は、発生した事故・障害等について迅速に対応するとともに、全学システム管理者に報告し、必要に応じて支援を要請する。

また、重大な被害が発生した場合は、全学システム管理者及び部局システム管理者は、情報セキュリティ統括責任者に報告し、その指示に従わなければならない。

全学システム管理者及び部局システム管理者は、発生したすべての情報セキュリティ上の事故等に関する記録を一定期間保存し、情報セキュリティ委員会に報告し、再発防止のための対策を講じなければならない。

3—3　技術的セキュリティ対策

情報資産を不正なプログラムや不正なアクセスから適切に保護するため、情報システム、学内ネットワーク等に対し、技術的な対策を講じなければならない。

3—3—1　ネットワーク接続機器

ネットワークに接続できる機器に対しては、全学システム管理者は、ウィルス対策ソフト、情報漏洩防止ソフト等を導入し、OSのセキュリティアップデートを行うなどセキュリティ対策を講じなければならない。

システム担当者は常に最新のセキュリティ情報に注意を払うだけでなく、機器障害や権限のないアクセスによって機器の構成や制御機能が損なわれないよう管理しなければならない。

また、全学システム管理者は、ファイヤーウォールおよび侵入検知システムその他必要と思われるセキュリティ機器を導入・運用し、外部からの脅威や内部への攻撃に対処しなければならない。

3—3—2　ネットワークの無許可利用およびネットワークバックドアの排除

ネットワークへ情報機器を接続するには、事前に物理的または電子的認証を受けなければならない。ネットワークセキュリティ機能による管理を回避する目的でのバックドア（PPPサーバ、コンピュータに接続する公衆回線、VPN装置およびソフトウェア等）の設置を原則禁止する。

3—3—3　利用記録の保存

全学システム管理者はファイヤーウォールおよび侵入検知システムや情報システムへのアクセス記録を一定期間保存しなければならない。

## 4. ポリシーの評価と見直し

4—1　ポリシーの運用実態と更新

情報セキュリティ統括責任者は、ポリシーに沿った対策が適切に実施されているか定期的に評価し、改善が必要と認められた場合は、速やかに更新の措置を講じなければならない。

また、情報セキュリティ統括責任者は、大学評議会に評価や見直しの結果を報告しなければならない。

平成 27 年4月1日

施行