学校法人学習院
情報セキュリティポリシー

平成２９年４月１日施行
令和８年４月１日改正

学校法人 学習院
THE GAKUSHUIN SCHOOL CORPORATION

Ⅰ　情報セキュリティ基本方針

1　基本理念及び目的

学校法人学習院（以下「本院」という。）において、健全な教育・研究活動を実践し、社会的責務を果たすためには、情報基盤の充実に加え、情報資産のセキュリティ確保が不可欠である。

そのために、本院の教職員、学生その他本院の構成員は、情報資産の価値を十分に認識し、本院の情報資産を守るだけでなく、外部に対する不正な情報提供、情報資産の侵害等が行われないように努め、本院における情報システムの信頼性を高めていかなければならない。

そこで、本院においては、次の事項の実現を目的として「学校法人学習院情報セキュリティポリシー」（以下「本ポリシー」という。）を制定し、本院の全構成員に周知を図ることとする。本院の提供する情報資産に関連するサービスを利用する者は、本ポリシーを遵守する責任があり、意図の有無を問わず、本院内部及び外部（以下「内外」という。）の情報資産に対する権限のないアクセス、改ざん、複写、破壊、漏えい等をしてはならない。

（1）　本院に対する情報セキュリティ侵害を阻止すること。
（2）　内外の情報セキュリティを侵害する行為を抑止すること。
（3）　情報資産の管理・運用を行うこと。
（4）　情報セキュリティ侵害の早期検出と迅速な対応を実現すること。

2　用語の定義

本ポリシーで使用する用語の定義は、以下のとおりとする。

（1）　情報

本院の教育・研究・管理運営に関わる者が作成し、又は収集及び取得した内容が記録された文書、電子文書、情報システム内のデータ、その他それに準ずるものをいう。

（2）　情報システム

ハードウェア、ソフトウェア、ネットワーク、記録媒体で構成されるものであって情報処理を行う仕組みであり、本院により所有又は管理されているもの及び本院との契約又は他の協定に従って提供されるものをいい、本院の情報ネットワークに接続される機器を含む。

（3）　情報資産

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）をいう。

（4）　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。

ア　機密性　情報資産にアクセスすることを許可された者だけが、情報資産にアクセスできることを確保すること。

イ　完全性　情報資産が破壊、改ざん又は消去されていない状態を確保すること。

ウ　可用性　情報資産にアクセスすることを許可された利用者が、必要なときに情報にアクセスできる状態を確保すること。

（5）　教職員

本院に勤務する常勤又は非常勤の教員及び職員（派遣職員、アルバイトを含む）をいう。

（6）　学生・生徒等

本院通則に定める学部学生、大学院生、科目等履修生、特別聴講学生、委託生、研究生、協定留学生等、及び各科の生徒・児童等をいう。

（7）　利用者

本院の情報資産を利用するすべての者をいい、役員、教職員、共同研究者、学生・生徒等、父母保証人、委託業者、学外者等をいう。

(8)　業務委託

本院の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものをいう。

(9)　クラウドサービス

事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスをいう。クラウドサービスの例としては、SaaS(Software as a Service)、PaaS(Platform as a Service)、IaaS(Infrastructure as a Service)等がある。

(10)　機器等

情報システムの構成要素(ハードウェア、ソフトウェア、ネットワーク、記録媒体等)の総称をいう。

(11)　外部サービス

本院が委託する業務委託、事業者が本院に対し提供するクラウドサービス等をいう。

(12)　インシデント

情報の漏洩・違法な情報取得や改ざん、破壊・消失、情報システムの機能停止等、情報セキュリティに関する事故・障害、又はそれらにつながる可能性のある事象をいう。

(13)　各部署

本院が設置する各学校及び事務組織をいう。

(14)　サーバ装置

情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの(搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。)をいい、特に断りがない限り、本院が調達又は開発するものをいう。

(15)　端末

情報システムの構成要素である機器のうち、利用者が本院の管理するネットワークに接続する情報機器(搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。)をいう。

(16)　取扱制限

情報の取扱いに関する制限であって、複製禁止、持出禁止、配付禁止、暗号化必須、その他の情報の適正な取扱いを利用者に確実に行わせるための手段をいう。

(17)　情報セキュリティ関係規程

本ポリシー、学習院情報セキュリティ委員会規程(以下「委員会規程」という。)、学校法人学習院情報セキュリティ管理規程(以下「管理規程」という。)、学校法人学習院情報セキュリティ管理基準(以下「管理基準」という。)及び学校法人学習院外部サービス利用規程(以下「外部サービス利用規程」という。)をいう。

(18)　自己点検

教職員が、情報の棚卸、外部サービスに関する契約内容の確認等の方法を用いて、自らの役割に応じて実施すべき情報セキュリティ対策を実施していることを点検し、情報セキュリティ関係規程の遵守状況等を確認することをいう。

(19)　監査

本院内部又は外部の独立性を有する者が、利用者へのヒアリング、文書レビュー、情報システムに対する脆弱性診断等の方法を用いて、客観的に本院の情報セキュリティ対策及び水準を確認することをいう。

3　方針

本ポリシーの目的を達するため、本院は本ポリシー第Ⅱ章情報セキュリティ対策基準、情報セキュリティ関係規程の定めるところにより、以下に関する情報セキュリティ対策を行う。

(1)　組織及び体制の整備
(2)　情報資産の分類と管理
(3)　情報システム利用時の対策
(4)　教育・啓発
(5)　外部サービス利用時の対策
(6)　インシデントへの対応
(7)　情報セキュリティの評価及び見直し
(8)　(1)～(7)を含む情報セキュリティマネジメントの実施

4　対象範囲及び対象者

(1)　本ポリシーの対象範囲は、次のとおりとする。

ア　本院が管理する情報資産

イ　本院の諸活動に伴い、業務委託先において取り扱われる情報資産

(2)　本ポリシーの対象者は、利用者とする。

5　利用者の義務

ア　利用者は、情報セキュリティの重要性を認識し業務の遂行にあたっては、情報セキュリティ関係規程及びその他関連法令等を遵守しなければならない。

イ　利用者は、内外に対して、情報セキュリティを損ねる行為をしてはならない。

ウ　利用者は、権限のない情報を取得、閲覧したり、許可のない情報を利用してはならない。

6　違反者への措置

利用者が、本ポリシーに違反した場合には、法令、学習院就業規則、学則等に基づき、処分、その他の措置を行うことがある。

Ⅱ　情報セキュリティ対策基準

1　趣旨

この対策基準は、本ポリシー基本方針の目的を達成するために、必要な組織・体制、基準、指針等を定めるものとする。

2　組織及び体制

(1)　責任者、管理者等

本院における情報セキュリティを確保するために、組織及び体制を次のとおり定める。組織・体制図は、別表のとおりとする。

ア　情報セキュリティ最高責任者

本院に情報セキュリティ最高責任者を置き、総務担当常務理事をもって充てる。情報セキュリティ最高責任者は、本院の情報セキュリティに関する総轄的な意思決定をし、内外に対する責任を負う。

イ　部局情報セキュリティ実施責任者

本院に部局情報セキュリティ実施責任者を置き、教育研究組織においては各学校長、事務組織においては事務局長をもって充てる。部局情報セキュリティ実施責任者は、各部署の情報セキュリティに関する権限と責任を有する。

ウ　部局情報セキュリティ担当者

各部署に部局情報セキュリティ担当者を置き、次に掲げる者をもって充てる。部局情報セキュリティ担当者は、個々の情報機器、ソフトウェア及び情報を管理・監督し、情報セキュリティを維持するための責任を負い、部局情報セキュリティ管理責任者を補佐し、利用者を支援する。

（ア）　大学の教育研究組織
学部長、研究科長、センター所長

（イ）　高等科・中等科・女子高等科・女子中等科・初等科の教育研究組織
電算機主任

（ウ）　幼稚園の教育研究組織
園長が指名した者

（エ）　事務組織
事務部長（事務部長が置かれていない部署においては次長、課長又は事務長等）

エ　情報セキュリティ管理者

情報システム統括部情報システム統括課に情報セキュリティ管理者を置く。情報セキュリティ管理者は、基幹ネットワークと主要なサーバ装置を運用管理し、情報セキュリティを維持するための責任を負い、情報セキュリティ最高責任者、部局情報セキュリティ管理責任者、部局情報セキュリティ実施担当者を支援する。

オ　利用者

研究室等において、利用者自らが直接管理する情報資産を持つ場合については、各利用者が、その情報セキュリティに関する責任を負う。

（2）　情報セキュリティ委員会

本院における情報セキュリティ対策を推進し、本院の情報システムの安全かつ適切な運用を図るため、情報セキュリティ委員会（以下「委員会」という。）を置く。

委員会は、情報セキュリティ対策の意思決定及び情報セキュリティ対策の管理・評価を担い、本ポリシーの評価及び改訂のほか、情報資産に対する重大な脅威への警戒・監視、情報セキュリティ侵害への対応、情報セキュリティに係る教育の実施、その他情報セキュリティに関する事項を審議する。

委員会の運営等に関し、必要な事項については、委員会規程の定めるところによる。

本委員会の運営に関する事務は、総務部総務課及び情報システム統括部情報システム統括課が担当する。

3　情報資産の分類と管理

本院の保有する情報資産に対して教職員は、管理基準に定める情報の格付や取扱制限等の管理の方法に則って管理しなければならない。

4　情報システムの利用時の対策

教職員の情報システムの利用について必要な事項は、管理規程に定める。

5　教育・啓発

ア　情報管理最高責任者及びその指示を受けた情報セキュリティ管理者は、教職員に対して情報セキュリティに係る各年度の教育実施計画を策定し、当該計画に沿って実行しなければならない。

イ　情報管理責任者及びその指示を受けた情報管理担当者は、学生・生徒等に対して情報セキュリティに係わる各年度の教育実施計画を策定し、当該計画に沿って教育しなければならない。大学の学生に対する教育実施計画の策定及び教育は計算機センターが主となり教育を行うものとする。

ウ　教職員及び学生・生徒等は、教育実施計画に従って、情報セキュリティに係る教育を受けなければならない。

エ　上記を含む教職員に関する情報セキュリティに係る教育の具体的な事項は、管理規程に定める。

6　外部サービスの利用時の対策

（1）　業務委託

業務委託する場合は、委託業者から再委託を受ける業者等も含め、本ポリシーを遵守することを明記した契約を締結するものとする。業務委託について必要な事項は、外部サービス利用規程に定める。

（2）　クラウドサービス

クラウドサービスの利用について必要な事項は、外部サービス利用規程に定める。

7　インシデントへの対応

ア　利用者は、インシデントを認知した場合には、直ちに部局情報セキュリティ実施担当者に報告し、指示に従わなければならない。

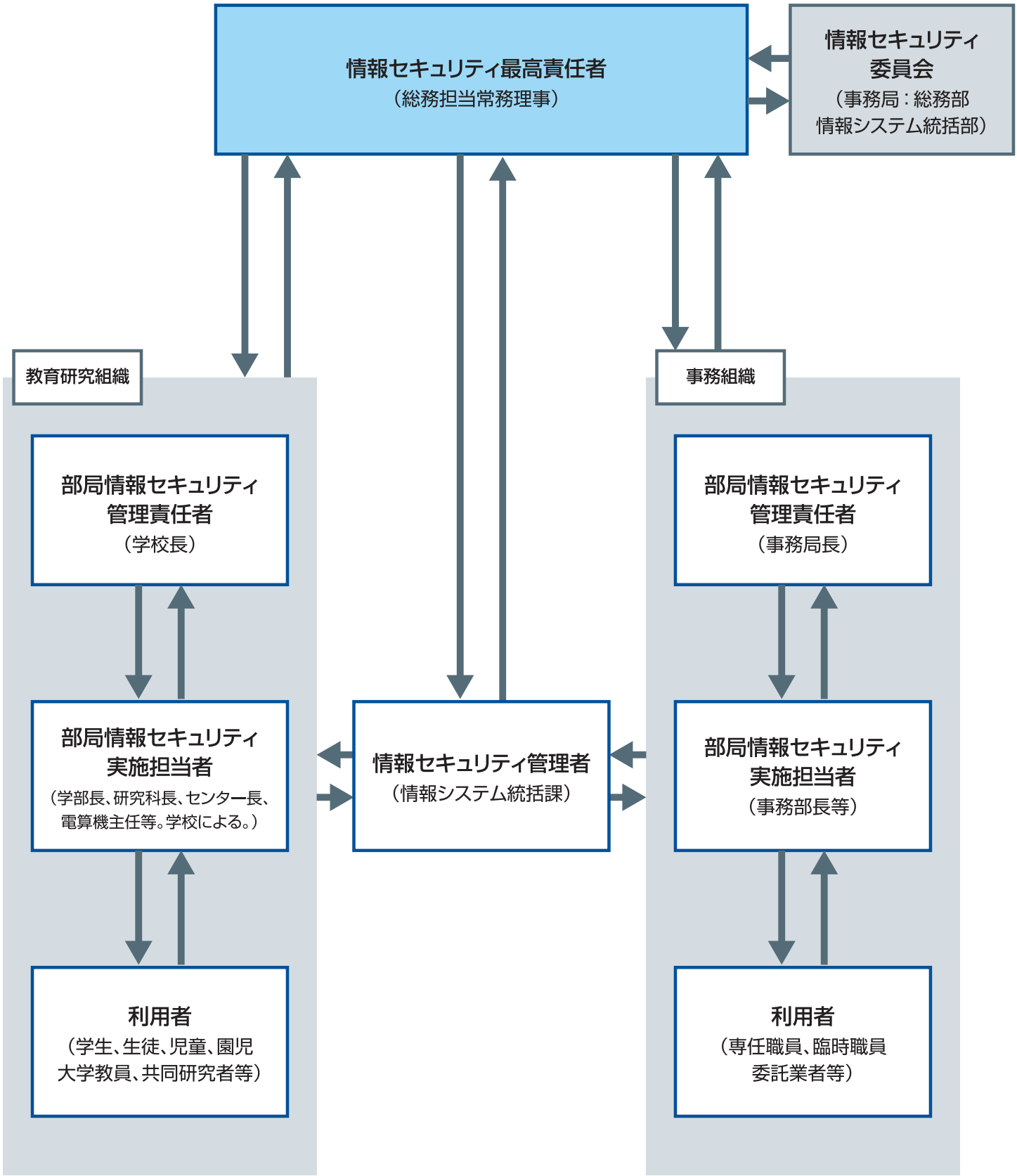
イ　情報セキュリティ最高責任者、部局情報セキュリティ管理責任者、部局情報セキュリティ実施担当者、情報セキュリティ管理者は、管理規程及び管理基準に則り、速やかに必要な措置を講じなければならない。

ウ　上記を含むインシデントへの対応に関する具体的な事項は、管理規程及び管理基準に定める。

8　情報セキュリティの評価及び見直し

情報セキュリティ最高責任者は、情報セキュリティの運用、自己点検及び情報セキュリティ監査の結果等を総合的に評価するとともに、本院を取り巻く情報セキュリティに係る脅威や技術の動向又は本院におけるインシデントの発生等の情報セキュリティの状況の変化を踏まえ、情報セキュリティ委員会の審議を経て、情報セキュリティ関係規程について見直しを行わなければならない。

別表 組織・体制図



発行：学校法人学習院　総務部総務課　Tel 03-5992-1191