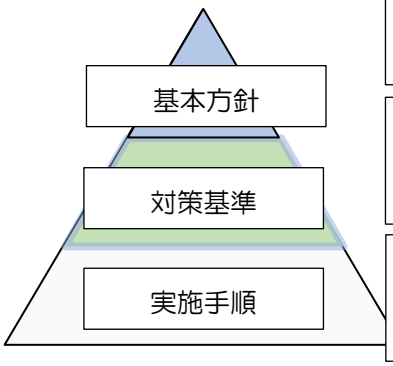
巣鴨学園 情報セキュリティポリシー

令和４年４月１日制定

序

情報化社会では、ICT を基盤とした先端技術等の効果的な活用が求められています。
また、学校教育の情報化が進展したことで、情報と情報資産の取り扱いや、盗難・漏えい・紛失の対策・対応、情報セキュリティに対するリスクの増大などの課題が生じています。
そこで、学校法人巣鴨学園では、学習環境や校務環境を守るために「学校法人巣鴨学園情報セキュリティポリシー」を制定し、技術の進歩等に伴う情報セキュリティを取り巻く状況の変化へ柔軟に対応していくこととしました。



基本方針：
情報セキュリティ対策の目的や原則を定めた統一的な方針

対策基準：
情報及び情報資産等を様々な脅威から防御するための具体的な対策

実施手順：
情報セキュリティ対策を実行するために、対象者が行動するときの手順

I. 情報セキュリティ基本方針

1. 基本理念

学校法人巣鴨学園（以下「本学園」という。）において、教育方針である「硬教育」を実践し、有用の学術を修め質実の気風を養い、本学園が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、情報資産の価値を十分に認識し、本学園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、本学園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。

2. 目的

本学園においては、次の事項の実現を目的として「学校法人巣鴨学園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、本学園の全構成員に周知を図ることとする。本学園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、本学園内部及び外部（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。

⑴ 本学園の情報資産を様々な脅威から守ること。
⑵ 本学園の情報資産の漏えいを抑止すること。
⑶ 情報資産の管理・運用を行うこと。
⑷ 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。

3. 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。

⑴ 情報

本学園の教育・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。

⑵ 情報システム

ハードウェア、ソフトウェア、ネットワーク、電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

⑶ 情報資産

情報システム及びネットワーク並びにこれらで取り扱われる学校情報のこと。（これらを印刷した文書も含む）

⑷ 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。

イ） 機密性

情報資産に対するアクセス権限を徹底して保護・管理し、情報漏えいをさせない

ロ） 完全性

情報資産を最新かつ正しい状態で維持され、情報を改ざんさせないこと

ハ） 可用性

システムが継続して稼働し、情報がいつでも扱える状態を保つこと

4. 対象範囲

本ポリシーの対象範囲は、次のとおりとする。

イ） 本学園が管理する情報資産

ロ） 本学園の諸活動に伴い、業務委託先において取り扱われる情報資産

5. 対象者

本ポリシーの対象者は、本学園の情報資産を利用するすべての者（以下「利用者」という。）で、役員、教員（非常勤教員を含む。）、職員（臨時職員、派遣職員等を含む。）、生徒、保護者、委託業者等とする。

Ⅱ. 情報セキュリティ対策基準

1. 趣旨

この対策基準は、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

本学園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。

イ) 情報セキュリティ最高責任者

本学園に情報セキュリティ最高責任者を置き、理事長をもって充てる。情報セキュリティ最高責任者は、本学園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。

ロ) 情報セキュリティ実施責任者

本学園に情報セキュリティ実施責任者を置き、教務課情報（ICT）係主任をもって充てる。情報セキュリティ実施責任者は、本学園全体の情報セキュリティに関する権限と責任を有する。

ハ) 情報セキュリティ担当者

本学園に情報セキュリティ担当者を置き、教務課情報（ICT）係をもって充てる。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う。

ニ) ネットワーク管理者

本学園にネットワーク管理者を置き、情報セキュリティ最高責任者がネットワーク管理者を任命する。ネットワーク管理者は、基幹ネットワークと主要な業務用サーバを運用管理し、セキュリティを維持するための責任を負う。

ホ) 各教科等において、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

本学園における情報セキュリティ対策を推進し、本学園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。

情報セキュリティ委員は、理事長が任命する。

委員会は、基本方針の維持及び見直しのほか、情報資産に対する重大な脅威への警戒・監視、情報セキュリティに関わる事件・事故の調査・分析及び再発防止策の立案、啓発活動等を任務とする。

委員会の運営等に関し、必要な事項については、「情報セキュリティ委員会規程」の定めるところによる。

3. 物理的セキュリティ

(1) 情報システムの設置等

情報セキュリティ実施責任者は、サーバ機器等の重要な情報システム又は情報資産

を、それぞれ設定された管理区域内に設置し、正当なアクセス権のない者が使用できないよう、セキュリティ確保に努めなければならない。

⑵ 情報機器及び記録媒体の盗難対策

情報セキュリティ実施責任者は、情報機器及び記録媒体の盗難予防に努めなければならない。

⑶ 情報機器及び記録媒体の学外への持ち出し

利用者は、個人情報及び本学園の重要なデータが入った情報機器及び記録媒体を、原則として学外へ持ち出してはならない。情報セキュリティ実施責任者は、やむを得ず、情報機器又は記録媒体を学外へ持ち出すことを認める場合、情報の漏えいが発生しないよう、情報セキュリティ対策を講じなければならない。

⑷ 情報機器及び記録媒体の学内への持ち込み

利用者は、情報機器及び記録媒体を学内へ持ち込む場合は、ウィルスチェックを行う等の情報セキュリティ対策を講じなければならない。

⑸ 情報のバックアップ

利用者及びネットワーク管理者は、サーバ機器等に記録するデータを、必要に応じてバックアップしなければならない。

⑹ 情報機器及び記録媒体の処分

利用者は、情報機器及び記録媒体を破棄する場合は、残存情報が第三者に読み取られることのないよう、情報セキュリティ対策を講じなければならない。

4. 人的セキュリティ

⑴ 教育・研修

情報セキュリティ最高責任者は、情報セキュリティに関する啓発や教育を実施するため、必要な措置を講じるよう努めるものとする。

⑵ 利用者の義務

イ） 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ち、業務の遂行にあたっては、本ポリシー及びその他関連法令等を遵守しなければならない。

ロ） 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。

ハ） 利用者は、アクセス権限のない情報にアクセスをしたり、許可されていない情報を利用してはならない。

⑶ 事故・障害時の報告・対応

イ） 利用者は、情報セキュリティに関する事故・障害及び公開情報の改ざん等を発見した場合には、直ちに情報セキュリティ実施責任者、情報セキュリティ担当者又はネットワーク管理者に報告しなければならない。

ロ） ネットワーク管理者は、内外から情報システムの不正使用、情報資産の不正な利用等にかかわる苦情、通報等があった場合には、速やかに調査を行わなければならない。

ハ）ネットワーク管理者は、調査の結果、不正が確認されたときは、関係する通信の遮断、該当する情報システムの切り離し等必要な措置を直ちに講じ、情報セキュリティ実施責任者に報告しなければならない。

ニ）情報セキュリティ実施責任者は、重大な事故が発生した場合は、情報セキュリティ最高責任者に報告しなければならない。

ホ）情報セキュリティ最高責任者は、重大な事故について審議する必要がある場合は、情報セキュリティ委員会を招集しなければならない。

⑷ 委託契約

情報システムの開発又は運用管理を外部委託する場合は、外部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。

5. 技術的セキュリティ

⑴ 不正アクセス等への対応

ネットワーク管理者は、不正アクセスの防止及び検出するための適切な手段を講じなければならない。

⑵ アクセス制限

本学園において、情報の内容に応じて、アクセス可能な利用者を定め、不正なアクセスを阻止するために必要なアクセス制限を行わなければならない。

⑶ ログの保存

ネットワーク管理者は、システム等のアクセスログ、操作ログ等について、保存期間を定めて保存しなければならない。

⑷ セキュリティの維持

ネットワーク管理者は、管理する機器・ソフトウェアについて、常にその構成を把握し、セキュリティに係る更新、ウィルス対策等適切なセキュリティの維持に努めなければならない。

6. 情報資産分類

⑴ 本学では情報資産を重要度に応じ 4 区分に分類し管理する。区分の定義は以下の通り。

イ）重要性分類Ⅰ：秘情報

定義：セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。

ロ）重要性分類Ⅱ：関係者外秘情報

定義：セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす。

ハ）重要性分類Ⅲ：学外秘情報

定義：セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす。

ニ）重要性分類Ⅳ：公開情報等

定義：学校紹介・活動資料（学校オフィシャルホームページコンテンツおよび

パンフレット等）でセキュリティ侵害を及ぼす可能性が極めて低いもの

⑵ 情報資産の分類は別表にて管理する

7. 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・学則等に基づき、処分その他の措置を行うことがある。

8. 「学校法人巣鴨学園情報セキュリティポリシー」の評価及び更新

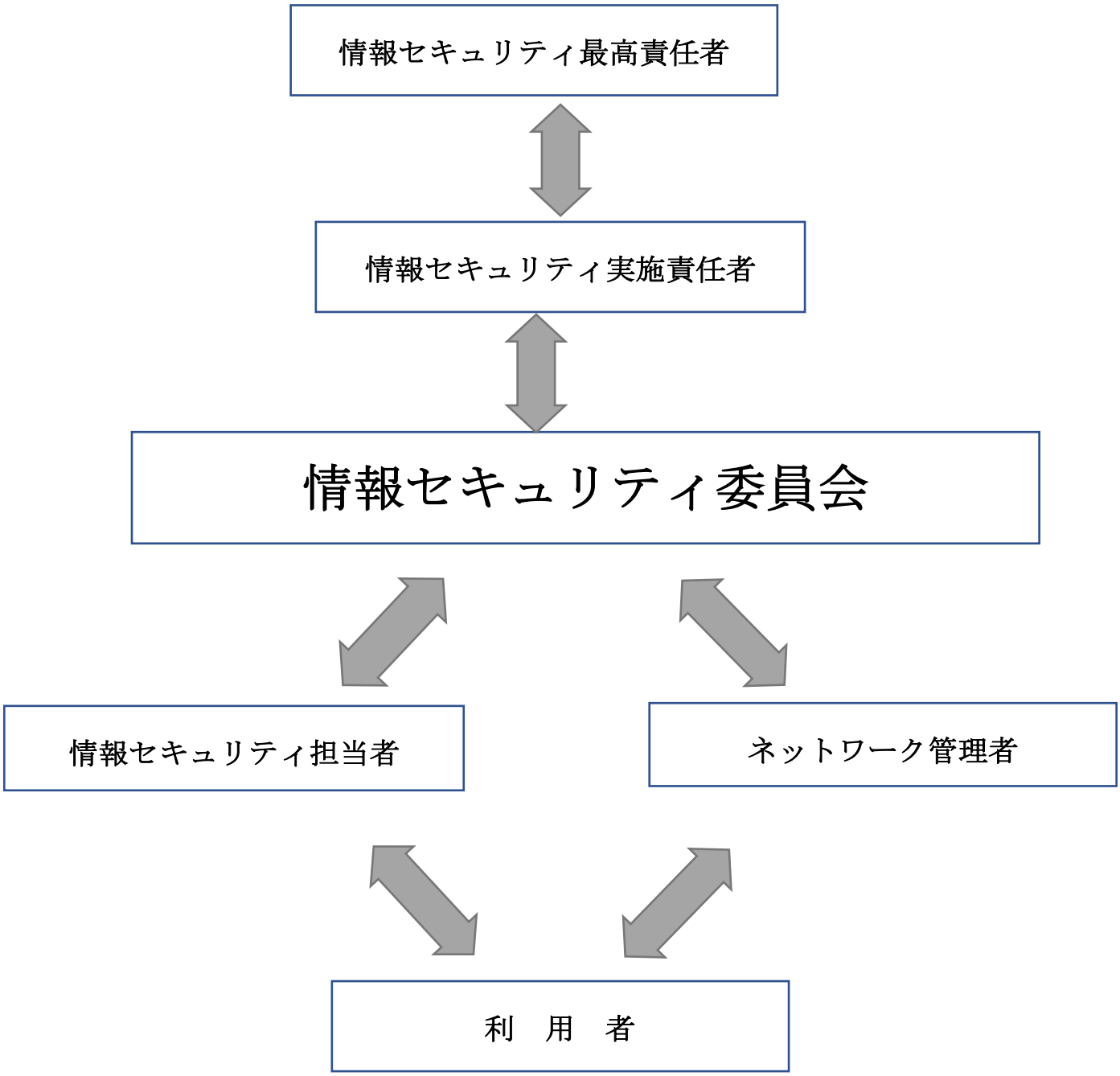
本ポリシーの実効性については、定期的に評価を行い、改善が必要と認められた場合は、セキュリティレベルの高い、かつ遵守可能なポリシーに更新しなければならない。

附 則

1. 「学校法人巣鴨学園情報セキュリティポリシー」は、2022（令和４）年４月１日から施行する。

別表１

組織・体制図


情報セキュリティ最高責任者
情報セキュリティ実施責任者
情報セキュリティ委員会
情報セキュリティ担当者
ネットワーク管理者
利　用　者

制定・改定日
第 1.0 版　2022（令和４）年４月１日
第2.0 版　2022（令和４）年 12 月１日
第3.0 版　2023（令和５）年４月１日