学校法人法政大学情報セキュリティポリシー

規定第１１３９号

一部改正　2015年 4月 1日　2017年11月 8日　2021年 1月18日　2022年10月1日

目　次

第１章　総則
第２章　情報セキュリティの管理体制
第３章　情報セキュリティインシデントへの対応
第４章　情報資産の分類と管理
第５章　物理的セキュリティ
第６章　人的セキュリティ
第７章　技術的セキュリティ
第８章　評価・見直し
付　則

前　文

学校法人法政大学（以下，「本法人」という。）において健全な学術研究・教育活動を実践し，社会的責務を果たすためには，情報基盤の整備に加えて，本法人の情報資産のセキュリティを確保することが不可欠である。

本法人全体の情報セキュリティ意識の向上に努め，その根拠を明確にし，本法人の全構成員が情報セキュリティの重要性を認識し，情報資産の円滑な運用と保護に取り組むため，本法人は「学校法人法政大学情報セキュリティポリシー」（以下，「ポリシー」という。）を規定する。

総　則

（ポリシーの構成）

第１条　ポリシーは，次のとおり構成する。構成図は別表１のとおりとする。

（１）情報セキュリティ基本方針

本法人が情報セキュリティに取り組むうえでの基本となる方針を定め，ポリシーの対象者に対して，基本的な考え方，役割及び責任を明確にする。

（２）情報セキュリティ対策基準

基本方針のもと，組織的に情報セキュリティ対策を行うための具体的な施策と達成すべき基準を定める。

２　ポリシーの実施手順は，情報セキュリティ対策基準に基づき各部局において定める。ただし，体制図及び緊急連絡網はこれに含めなければならない。

（適用対象範囲）

第２条　ポリシーの適用対象範囲は，次の各号に定めるとおりとする。

（１）適用対象資産

本法人が管理するすべての情報資産とする。

（２）適用対象者

本法人の情報資産を利用する全ての者で，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），共同研究者，学生（大学院生，学部生，研究生，科目等履修生等），付属校生徒，委託業者，来学者等とする。

（遵守義務）

第３条　本法人の情報資産を利用する全ての者は，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，ポリシー，情報セキュリティ実施手順及びその他関連法令等を遵守しなければならない。

Ⅰ．情報セキュリティ基本方針

（情報セキュリティ基本方針）
第４条　情報セキュリティ基本方針は，次のとおりである。
（１）情報セキュリティに関する法令，国が定める指針，その他の規範を遵守する。
（２）情報セキュリティに関する責任を明確にし，対策を実施するための体制を整備する。
（３）情報セキュリティに関するリスクを識別し，組織的，物理的，人的，技術的に適切な対策を実施する。
（４）情報セキュリティに関する教育及び啓発を実施し，情報セキュリティリテラシーをもって業務を遂行できるようにする。
（５）情報セキュリティに関する問題が生じたときは，速やかに被害防止を図るとともに，原因究明及び再発防止に努める。
（６）情報セキュリティを脅かす者に対し適切な措置を講じる。
（７）情報セキュリティに関する管理体制及び取り組みについて点検を実施し，組織的に改善・見直しを行う。

Ⅱ．情報セキュリティ対策基準

第１章　総則

（趣旨）
第５条　ここに規定する情報セキュリティ対策基準（以下，「対策基準」という。）は，情報セキュリティ基本方針に基づき，情報セキュリティ対策を講ずるにあたり遵守すべき行為及び判断等の基準を統一するため，必要となる基本的要件を定めるものである。

（用語の定義）
第６条　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
本法人の教育・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電磁的媒体，紙媒体及びそれに準ずる媒体をいう。
（２）情報資産
情報システムに記録された情報及び情報システムに関係がある書面に記載された情報であり，電磁的に記録された情報全てを含む。書面に記載された情報には，電磁的に記録されている情報を記載した書面（情報システムに入力された情報を記載した書面，情報システムから出力した情報を記載した書面）及び情報システムに関する設計書が含まれる。
（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をいう。
ａ　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。
ｂ　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。
ｃ　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。
（４）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をいう。本法人の情報システムは，本法人により所有又は管理されているもの及び本法人との契約あるいは他の協定に従って提供されるものをいい，本法人の情報ネットワークに接続される機器を含む。
（５）情報セキュリティ実施手順
情報セキュリティ対策を実施するため，情報セキュリティ対策基準に基づいて適宜策定される基準をいう。
（６）情報機器
サーバ機器，クライアント機器等のコンピュータ本体及びディスプレイ，プリンタ等の周辺機器をいう。
（７）サーバ機器
複数のクライアント機器からアクセスされ，共同で利用される情報機器をいう。

（８）クライアント機器
　サーバ機器の提供する機能やデータへアクセスすることで処理を進めていく情報機器をいう。
（９）記録媒体
　電磁的又は光学的に情報を記録した媒体あるいは情報をプリントアウトした紙媒体等をいう。
（１０）部局
　教学組織においては各学部，大学院の各研究科，専門職大学院の各研究科，各研究所（センターを含む）及び各付属校，事務組織においては各事務部（センター，室を含む）をいう。
（１１）情報セキュリティインシデント
　不正アクセス，情報漏えい，データの改ざん，ウィルス感染等により，情報セキュリティに脅威が発生している又は発生するおそれがある事象をいう。
（１２）CSIRT（シーサート）
　本法人によって発生した情報セキュリティインシデントに備えた体制をいう。CSIRTはComputer Security Incident Response Team の略。
（１３）トリアージ
　情報セキュリティインシデントとして扱うか否かの判断を行うことをいう。加えて，情報セキュリティインシデントであると判断した場合においては，その重要度を決定することもいう。
（１４）インシデントレスポンス
　トリアージ後に実施する情報セキュリティインシデントの被害拡大防止を図るための応急措置の指示及び勧告，情報セキュリティインシデントに実際に対応する業務を指す。

第２章　情報セキュリティの管理体制

（組織・体制）
第７条　本法人における情報基盤を整備し，情報資産の有効活用・セキュリティ確保を実現するための組織・体制を次のとおり定める。又，組織・体制図は別表２のとおりとする。
（１）最高情報セキュリティ責任者
　本法人に最高情報セキュリティ責任者を置き，総長をもって充てる。最高情報セキュリティ責任者は，本法人の情報セキュリティに関する総轄的な意思決定をし，学内及び学外に対する責任を負う。
（２）情報セキュリティ実施責任者
　本法人に情報セキュリティ実施責任者を置き，学術支援本部担当常務理事をもって充てる。情報セキュリティ実施責任者は，本法人における情報セキュリティ対策の実施に関し総轄し，情報セキュリティ管理責任者と連携し，最高情報セキュリティ責任者を補佐する。
（３）情報セキュリティ管理責任者
　本法人に情報セキュリティ管理責任者を置き，法人本部担当常務理事をもって充てる。情報セキュリティ管理責任者は，本法人における情報セキュリティ対策の管理・運営に関し総轄し，情報セキュリティ実施責任者と連携し，最高情報セキュリティ責任者を補佐する。
（４）CSIRT責任者
　本法人のCSIRTであるHOSEI-CSIRTにCSIRT責任者を置き，情報セキュリティ実施責任者が指名する者をもって充てる。CSIRT責任者は，本学専任教員のうち，専門的な知識又は適性を有すると認められる者から指名される。CSIRT責任者は情報セキュリティ実施責任者を補佐し，HOSEI-CSIRTの活動を管理する権限と責任を有する。加えて，情報セキュリティインシデントが発生した場合の緊急措置の実施及び脆弱性への対処に関する情報セキュリティ実施責任者の権限を行使することができる。
（５）部局システム管理責任者（教学組織においては各学部長・各研究科長・各校長，事務組織においては各部局事務部長）
　部局に部局システム管理責任者を置き，当該部局の長をもって充てる。部局システム管理責任者は，部局内の情報セキュリティに関する権限と責任を有する。
（６）システム管理者（教学組織においては各教員，事務組織においては各部局課長）
　部局にシステム管理者を置き，教学組織においては，個々のクライアント機器により情報システムを利用する教員をもって充て，事務組織においては，当該部局の職員のうちから部局システム管理責任者が指名する者をもって充てる。システム管理者は，個々の情報機器，ソフトウェア及び情

報を管理・監督し，セキュリティを維持するための責任を負う。

（情報セキュリティ委員会）

第８条　最高情報セキュリティ責任者は，次の各号に掲げる事項について審議する必要があるときは，情報セキュリティ委員会（以下，「委員会」という。）を設置する。

（１）情報資産に対する重大な脅威への警戒・監視に関する事項

（２）情報セキュリティに関わる事件・事故の調査・分析及び復旧，再発防止策の立案に関する事項

（３）その他情報セキュリティに関する重要な事項

２　委員会は，次の各号に掲げる委員をもって組織する。

（１）最高情報セキュリティ責任者

（２）情報セキュリティ実施責任者

（３）情報セキュリティ管理責任者

（４）CSIRT責任者

（５）情報関連領域を専門とする専任教員　　２名

（６）その他最高情報セキュリティ責任者が必要と認めて指名した者

３　委員会には委員長を置き，前項第１号の委員をもってこれに充てる。

４　委員会において決するべき事項が生じた場合には，出席委員の過半数をもって決する。可否同数の場合は，委員長の決するところによる。

５　委員会の事務局は総務部とする。

（HOSEI-CSIRT）

第９条　情報セキュリティ実施責任者は，情報セキュリティインシデントが発生した場合，直ちに報告が行われる体制を整備しなければならない。

２　前項の規定に基づき，情報セキュリティ実施責任者は，情報セキュリティインシデントの発生時に迅速かつ円滑な対応を図るため，HOSEI-CSIRTを置く。

３　HOSEI-CSIRTにCSIRT責任者及びメンバーを置き，情報セキュリティ実施責任者が指名する。

４　HOSEI-CSIRTは，情報セキュリティインシデントの未然の防止，情報セキュリティインシデントが発生した際に被害を最小限とするための活動及び対外窓口として他組織との情報連携を行うことにより，学生や教員をはじめとする関係者との信頼関係を構築し，学生及び教職員が安心して利用できる教育研究環境の実現を目指すことをミッションとする。

５　HOSEI-CSIRTの職務は次に掲げる各号のとおりとする。

（１）情報セキュリティインシデントに係る報告の受付に関すること

（２）トリアージに関すること

（３）インシデントレスポンスに関すること

（４）情報セキュリティインシデントの情報セキュリティ実施責任者への報告に関すること

（５）情報セキュリティインシデントの対外的な連絡に関すること

（６）情報セキュリティインシデントの事前対応として，情報セキュリティインシデントや脆弱性情報の収集と注意喚起を目的とした情報発信を行うこと

（７）情報セキュリティインシデントの対応の品質向上を目的として，研修及び訓練の実施を行うこと

６　前項の職務に関する必要事項は「学校法人法政大学情報セキュリティインシデント対応チーム運用細則」に定める。

７　HOSEI-CSIRTの事務局は総合情報センター事務部とする。

（通報窓口）

第１０条　情報セキュリティインシデントに対する通報窓口をHOSEI-CSIRTに置く。

２　通報窓口の職務は次に掲げる各号のとおりとする。

（１）情報セキュリティインシデントに係る報告の受付を行い記録すること

（２）必要に応じて，通報に関係する者との的確な連絡を行うこと

（３）その他，通報の対応に関する必要事項を実施すること

（情報セキュリティインシデントの発生に備えた体制）

第１１条　部局システム管理責任者は，情報セキュリティインシデントの発生に備え，HOSEI-CSIRTと連携し，報告，連絡，情報集約及び被害拡大防止のための緊急対応に必要な体制を整えなければならない。

第３章　情報セキュリティインシデントへの対応

（情報資産利用者の通報・報告）

第１２条　情報資産を利用する者は，情報セキュリティインシデント，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HOSEI-CSIRTに通報し，併せて部局システム管理責任者又はシステム管理者に報告しなければならない。

（外部からの通報・連絡）

第１３条　外部から情報セキュリティインシデント，障害及び公開情報の改ざん等の発見又はそのおそれがある旨の連絡があった場合，その受信者はHOSEI-CSIRTに直ちに通報しなければならない。

（情報セキュリティインシデントの対処）

第１４条　部局システム管理責任者又はシステム管理者は，発生した情報セキュリティインシデント，障害及び公開情報の改ざん等について，HOSEI-CSIRTと協議のうえ，直ちに必要な措置を講じなければならない。

（情報セキュリティ実施責任者及び担当理事への報告）

第１５条　CSIRT責任者は，情報セキュリティインシデント及び公開情報の改ざん等が発生した場合は，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。

２　部局システム管理責任者又はシステム管理者は，第１２条の報告を受けた場合には，担当理事に報告しなければならない。

（重大事案の最高セキュリティ責任者への報告）

第１６条　CSIRT責任者は，重大な情報セキュリティインシデント及び公開情報の改ざんが発生した場合，情報セキュリティ実施責任者に報告したのち情報セキュリティ管理責任者及び最高情報セキュリティ責任者に報告しなければならない。

２　最高情報セキュリティ責任者は，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に報告しなければならない。

（記録の保存）

第１７条　部局システム管理責任者及びシステム管理者は，発生した全ての情報セキュリティインシデント及び公開情報の改ざん等に関する記録を一定期間保存しなければならない。

（再発防止策の報告）

第１８条　部局システム管理責任者及びシステム管理者は，発生した情報セキュリティインシデント及び公開情報の改ざん等に関する再発防止策をCSIRT責任者と協議のうえ，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。

（復旧にあたっての事前承認）

第１９条　部局システム管理責任者及びシステム管理者は，発生した情報セキュリティインシデント及び公開情報の改ざん等からの復旧にあたっては，CSIRT責任者と協議のうえ，情報セキュリティ委員会の承認をあらかじめ得なければならない。

第４章　情報資産の分類と管理

（情報資産の分類）

第２０条　情報資産は，その内容に応じ，別表３に掲げる区分に準じて非公開情報資産・限定公開情報資産・公開情報資産に分類し，その重要度に応じた情報セキュリティ対策を講じなければならない。

（非公開情報資産の取り扱い）

第２１条　非公開情報資産は，次の各号に掲げる事項に従い，取り扱われなければならない。

（１）個人情報，教育・研究，事務等の非公開情報資産を不当に利用してはならない。

（２）非公開情報を不特定の者が可読な状態にしてはならない。

（３）情報の盗難・漏洩等を防止するため，暗号化や盗聴防止策を講じることが望ましく，かつ盗難防止策を講じなければならない。

（限定公開情報資産の取り扱い）
第２２条　限定公開情報資産は，次の各号に掲げる事項に従い，取り扱われなければならない。
（１）特定の利用者に特定の情報を公開する場合，その情報の登録・閲覧は，許可された者が許可された操作だけを行えるよう，認証及びアクセス制御等を実施しなければならない。
（２）情報の盗難・漏洩等を防止するため，暗号化や盗聴防止策及び盗難防止策を講じることが望ましい。
（３）異常な登録，閲覧及び操作が行われていないか，定期的に調査・確認を行わなければならない。

（公開情報資産の取り扱い）
第２３条　公開情報資産は，次の各号に掲げる事項に従い，取り扱われなければならない。
（１）あらゆる公開情報資産を不当に利用してはならない。
（２）情報資産は，改ざん，破壊されないよう，適切に管理されなければならない。
（３）情報を公開する場合には，個人情報の漏洩，プライバシーや著作権の侵害に十分に注意し，公開できる情報だけの抽出を行い，公開してよい形に加工しなければならない。

（情報資産の管理）
第２４条　情報資産は，原則として，当該情報資産を作成した部局が本規程第２０条に定める分類により管理しなければならない。
２　本法人が所有するサーバ機器に保存されず，個々のクライアント機器に保存された情報資産は，原則として，当該クライアント機器を日常的に利用する者が管理しなければならない。

第５章　物理的セキュリティ

（管理区域の設置）
第２５条　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，管理する情報の重要度に従い，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，必要に応じて入退室の認証・記録や警備システムの設置等，物理的なセキュリティ確保に努めなければならない。

（情報機器及び記録媒体の盗難対策）
第２６条　システム管理者は，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。

（情報機器及び記録媒体の紛失及び置き忘れの予防）
第２７条　システム管理者は，情報機器及び記録媒体の紛失又は置き忘れの予防に努めなければならない。

（情報機器及び記録媒体の学内外への持ち出し）
第２８条　本法人の全ての構成員は，個人情報及び本法人の重要なデータが入った情報機器及び記録媒体は，原則として学内外へ持ち出してはならない。
２　やむを得ず，情報機器及び記録媒体を学内外へ持ち出す場合は，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。

（情報機器及び記録媒体の学内への持ち込み）
第２９条　システム管理者は，情報機器及び記録媒体を学内へ持ち込むことを認めた場合，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。

（情報のバックアップ）
第３０条　システム管理者は，サーバ機器等に記録するデータは，必要に応じて定期的にバックアップしなければならない。

（情報機器及び記録媒体の処分）
第３１条　システム管理者は，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。

第６章　人的セキュリティ

（教育・研修）
第３２条　最高情報セキュリティ責任者は，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。

（委託契約）
第３３条　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も含め，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。

第７章　技術的セキュリティ

（不正アクセス等への対応）
第３４条　情報セキュリティ実施責任者は，不正アクセスの防止並びに検出するための適切な手段を講じなければならない。
２　システム管理者は，不正アクセスが検出された場合は，第３章の規定に基づき，学内で連携を行い，関連する通信の遮断又は該当する情報機器の切り離しを実施する。

（アクセス制限）
第３５条　システム管理者は，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。
２　情報資産を利用する者は，アクセス権限のない情報にアクセスしたり，許可されていない情報を利用してはならない。

（ネットワークの運用管理）
第３６条　本法人の基幹ネットワークの管理は，情報セキュリティ実施責任者が行い，サブネットワークの管理は，情報セキュリティ実施責任者によりその設置が許可された者がこれを行う。
２　情報セキュリティ実施責任者は，基幹ネットワーク及び重要なサブネットワークについて，ファイアウォール等のセキュリティ対策機器を導入し，外部からの不正アクセス等に対する防御や内部から外部への攻撃に対処しなければならない。
３　情報セキュリティ実施責任者は，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。
４　情報セキュリティ実施責任者は，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，必要に応じて，セキュリティ対策機器及びセキュリティ対策機器上のソフトウェア（ファームウェアを含む）を更新しなければならない。

（ネットワークバックドアの排除）
第３７条　本法人のネットワークのセキュリティ機能を回避する目的でバックドア（ＰＰＰサーバ，コンピュータに接続する外部ネットワーク，ＶＰＮ装置及びソフトウェア等）を設置することは，原則として禁止する。

（ネットワーク接続機器）
第３８条　本法人のネットワークに接続する情報機器は，ウィルス対策ソフトを導入する等のセキュリティ対策を講じたものでなければならない。
２　情報セキュリティ実施責任者は，本法人のネットワークに接続する情報機器の利用者を把握しておかなければならない。

（利用記録の保存）
第３９条　個人情報等の非公開情報を管理するサーバ及び必要とされるサーバについては，システムログやアクセス記録等の運用に関する記録を一定期間保存しなければならない。又，最高情報セキュリティ責任者又は情報セキュリティ委員会から運用に関する記録の提供を求められた場合は，速やかに開示しなければならない。

（アカウント及びパスワードの整備）
第４０条　情報資産を利用する者は，自己のアカウントのパスワードを秘密としなければならない。又，十分なセキュリティを維持できるよう，自己のパスワードの設定及び変更に配慮しなければならない。

第８章　評価・見直し

（情報資産の点検）
第４１条　情報セキュリティ実施責任者は，情報資産に係る物理的・技術的・人的セキュリティ対策について，定期的な点検を実施し，その結果を最高情報セキュリティ責任者に報告しなければならない。

（情報セキュリティ対策の更新）
第４２条　最高情報セキュリティ責任者は，前条の報告により，改善が必要と認められる場合には，情報セキュリティ実施責任者に対して，情報セキュリティ対策の更新等，必要な措置を講じるよう命じなければならない。

（ポリシーの評価）
第４３条　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る場合には，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。

付　則
１　この規程は，２０１４年４月１日から施行する。
２　この規程は，２０１５年４月１日から一部改正し，施行する。
３　この規程は，２０１７年１１月８日から一部改正し，施行する。（規程改廃について職務権限規程を適用するための改正）
４　この規程は，２０２１年１月１８日から一部改正し施行する。
５　この規程は，２０２２年１０月１日から一部改正し施行する。

別表１（第１条関係）
別表２（第７条関係）
別表３（第２０条関係）

（追５６）