公立大学法人横浜市立大学情報セキュリティ基本規程

制　　定　平成30年４月１日規程第 32 号
最近改正　令和 ８ 年４月１日規程第 37 号

（目的）

第１条　本規程は、公立大学法人横浜市立大学（以下「本学」という。）における情報資産及び情報システムの運用及び管理について必要な基本事項を定め、もって本学が保有する情報の保護と活用及び適切な情報セキュリティ対策を図ることを目的とする。

（適用範囲）

第２条　すべての教職員、本学の情報資産及び情報システムの運用・管理をするすべての者、及び利用者並びに一時利用者に対し本規程を適用する。

２　本学の次の情報資産を本規程の適用対象とする。

(1)　本学の業務において使用することを目的として本学が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体

(2)　前号に掲げたシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

(3)　本項第１号に掲げた以外のシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、本学の業務上取り扱う情報

(4)　前号までのほか、本学が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体の設計又は運用管理に関する情報

３　本規程において適用対象とする情報システムは、本規程の適用対象となる情報資産を取り扱うすべてのシステム（ハードウェア及びソフトウェアから成る情報処理又は通信の用に供するものをいい、当該システムを構成する機器等も含む。）とする。

（定義）

第３条　本規程及び本規程に基づいて別に定める実施規程及び手順等において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

(1)　情報資産　本規程第２条第２項に定めるものをいう。単に「情報」と記述する場合、特に断りがなければ情報資産と読み替えることとする。

(2)　情報システム　本規程第２条第３項に定めるものをいう。

(3)　電磁的記録　電子的方式、磁気的方式その他人間の知覚によっては認識することができない方式で作られる記録であって、コンピュータによる情報処理の用に供されるものをいう。

(4)　ポリシー　本学が定める「公立大学法人横浜市立大学情報セキュリティ基本方針」及び本規程をいう。

(5)　実施規程　ポリシーに基づいて制定及び運用される規程及び、基準、計画をい

う。

(6)　手順等　実施規程に基づいて制定及び運用される具体的な手順や規約、ガイドラインを指す。

(7)　利用者及び一時利用者　教職員等及び学生等で、許可を受けて本学情報システムを利用する者をいう。また一時利用者は、これら以外の者で、一時的に許可を受けて本学情報システムを利用する者をいう。

(8)　教職員等　公立大学法人横浜市立大学職員就業規則第３条第１項に規定された職員（教育職員、一般職員及び派遣職員をいう。）及び同非常勤職員就業規則第２条第１項に規定された非常勤職員、その他 CISO 又は部局情報セキュリティ統括責任者が認めた者をいう。

(9)　学生等　本学学則及び大学院学則に定める学部学生、大学院学生、科目等履修生、特別聴講学生、学生入学者、特別研究学生、研究生、長期履修学生及び留学生、その他 CISO 又は部局情報セキュリティ統括責任者が認めた者をいう。

(10)　CIO　最高情報責任者。Chief Information Officer の略。

(11)　CISO　情報セキュリティ総括管理者。Chief Information Security Officer の略。

(12)　情報セキュリティ　すべての情報資産に対して、重要度に応じた機密性を確保しつつ、完全性及び可用性を維持すること、又はその維持された状態をいう。

(13)　CSIRT　本学において発生した情報セキュリティ事故に対処するため、本学に設置された体制をいう。Computer Security Incident Response Team の略。

(14)　情報セキュリティ事故　情報セキュリティに関し、本学規程や法律等に反すること、あるいは自然災害等による物理的損壊や滅失など、意図的または偶発的な要因により情報セキュリティが侵害される状態をいう。

(15)　明示等　情報を取り扱うすべての者が当該情報の格付けについて共通の認識となるようにする措置をいう。

（最高情報責任者）

第４条　本学に、理事長及び学長の下で、本学の情報資産の運用及び管理を総括し、情報戦略や情報セキュリティ対策を含む情報全般の企画、立案及び実施に関するすべての権限及び責任を有する者として CIO を置く。

２　CIO は、本学の事務局長をもって充てる。

３　CIO は、ポリシー及びそれに基づく規程の決定や情報資産の運用上での各種問題に対する処置を行う。

４　CIO は、全学向け教育及び各部局のシステム管理者向け教育を総括する。

５　CIO は、必要に応じて、情報セキュリティに関する専門的な知識及び経験を有した者を　情報セキュリティアドバイザーとして設置することができる。

（情報セキュリティ管理体制）

第５条　本学に、CISO、情報セキュリティ運用管理者、部局情報セキュリティ統括責任者、部局情報セキュリティ運用責任者、情報セキュリティ担当者を置く。

２　CISO、情報セキュリティ運用管理者、部局情報セキュリティ統括責任者、部局情報セキュリティ運用責任者、情報セキュリティ担当者は、次の各号の区分に応じ、

当該各号に掲げる職にあるものを充てる。

(1)　CISOは、本学の事務局長をもって充てる。

(2)　情報セキュリティ運用管理者　ICT推進課を所管する部長

(3)　部局情報セキュリティ統括責任者　職員組織にあっては各部の部長、教員組織にあっては各学系列長、医学科長、看護学科長、先端医科学研究センター長、次世代臨床研究センター長、病院にあっては各病院長

(4)　部局情報セキュリティ運用責任者　職員組織にあっては各課の課長、教員組織にあっては各コース長、各教室長、部局情報セキュリティ統括責任者以外の各センター長、病院にあっては各診療科部長、各中央部門長、各センター長、看護部長

(5)　情報セキュリティ担当者　必要に応じて部局情報セキュリティ運用責任者が所属ごとに指名した者

（情報セキュリティ総括管理者）

第６条　CISOは、情報セキュリティ運用管理者及び部局情報セキュリティ統括責任者を総括し、これらの者に対し情報セキュリティに関する事項に関して指示及び指導を行う。

２　CISOは、ポリシー及びそれに基づく規程の決定や学内周知のほか、情報システムで生じた全学的な課題、問題への対処を行う。

３　CISOは、全学の情報基盤として供される本学情報システムのうち情報セキュリティが侵害された場合の影響が特に大きいと評価される情報システムを指定することができる。この指定された情報システムを「全学情報システム」という。

４　CISOが欠けたときは、情報セキュリティ運用管理者又はCISOがあらかじめ指名する者が、その職務を代行する。

５　CISOは次に掲げる事務を統括する。

(1)　情報セキュリティ対策推進のための組織・体制を整備

(2)　情報セキュリティ対策基準の決定、見直し

(3)　対策推進計画の決定、見直し

(4)　情報セキュリティ事故に対処するために必要な指示その他の措置

(5)　情報セキュリティ監査の結果を踏まえた改善計画の策定等の必要な措置の指示

(6)　前各号に掲げるもののほか、情報セキュリティに関する重要事項

（情報セキュリティ運用管理者）

第７条　情報セキュリティ運用管理者は、CISOを補佐するとともに、情報セキュリティ対策の周知徹底を図るため、部局情報セキュリティ統括責任者に対し情報セキュリティ対策に係る指示及び指導を行う。

２　情報セキュリティ運用管理者は、CISOの下で、本学情報システムの整備と運用に関し、ポリシー及びそれに基づく規程並びに手順等の制定及び改廃、実施を行う。

３　情報セキュリティ運用管理者は、情報システムの運用に携わる者及び利用者に対して、情報システムの運用並びに利用及び情報システムのセキュリティに関する教育を企画及び実施し、ポリシー及びそれに基づく規程並びに手順等の遵守を確実にするための措置を講じる。

４　情報セキュリティ運用管理者は、セキュリティに関する学内外との連絡調整、周知徹底を行う。
５　情報セキュリティ運用管理者は、その実務を、本学情報システムの管理運営部局に委任することができる。

（部局情報セキュリティ統括責任者）

第８条　部局情報セキュリティ統括責任者は、部局情報セキュリティ運用責任者及び情報セキュリティ担当者を総括し、これらの者に対し情報セキュリティに関する事項に関して指示及び指導を行う。

（部局情報セキュリティ運用責任者）

第９条　部局情報セキュリティ運用責任者は、部局情報セキュリティ統括責任者を補佐するとともに、当該部局の職員への情報セキュリティ対策実施の徹底を図るため、情報セキュリティ担当者に対し情報セキュリティ対策に係る指示及び指導を行う。

（情報セキュリティ担当者）

第 10 条　情報セキュリティ担当者は、当該所属内の情報セキュリティ対策を実施するため、所属内の情報資産及び情報システムを利用する職員に対して指導及び監督を行う。

（ICT 推進委員会）

第 11 条　本学情報資産の運用及び管理及び情報セキュリティ、情報戦略等に関する事項を審議し、必要な事項を決定して周知するため、ICT 推進委員会を置く。
２　ICT 推進委員会の委員長は、CIO が務める。
３　その他、委員会の運営に関することは「公立大学法人横浜市立大学 ICT 推進委員会規程」に定める。

（管理運営部局）

第 12 条　本学情報システムの管理運営部局を総務部 ICT 推進課と定める。

（管理運営部局が行う事務）

第 13 条　管理運営部局は、情報セキュリティ運用管理者の指示により、以下の各号に定める事務を行う。
(1)　ICT 推進委員会の運営に関する事務
(2)　本学情報システムの運用と利用におけるポリシーの実施状況の取りまとめ
(3)　情報セキュリティに関する連絡調整、周知徹底

（情報セキュリティアドバイザーの設置）

第 14 条　CISO は、情報セキュリティアドバイザーを設置する場合には業務内容を次のとおり定める。
(1)　本学全体の情報セキュリティ対策の推進に係る CISO への助言
(2)　情報セキュリティ関係規程の整備に係る助言
(3)　個別のセキュリティ対策推進計画の策定に係る助言
(4)　セキュリティ教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援
(5)　情報システムに係る技術的事項に係る助言
(6)　情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示

する情報セキュリティに係る要求仕様の策定に係る助言
(7)　情報セキュリティ事故への対処の支援
(8)　前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援

（情報セキュリティ対策推進体制の整備）

第 15 条　CISO は、本学の情報セキュリティ対策推進体制を整備し、その役割を規定する。

2　CISO は、以下を含む情報セキュリティ対策推進体制の役割を規定する。
(1)　情報セキュリティ関係規程及び対策推進計画の策定に係る事務
(2)　情報セキュリティ関係規程の運用に係る事務
(3)　例外措置に係る事務
(4)　情報セキュリティ対策の教育の実施に係る事務
(5)　情報セキュリティ対策の自己点検に係る事務
(6)　情報セキュリティ関係規程及び対策推進計画の見直しに係る事務

3　CISO は、情報セキュリティ対策推進体制の責任者を定める。

（情報セキュリティ事故に備えた体制の整備）

第 16 条　CISO は、CSIRT を整備し、その役割を明確化する。

2　CISO は、以下をすべて含む CSIRT の役割を規定する。
(1)　本学に関わる情報セキュリティ事故発生時の対処の一元管理
(2)　情報セキュリティ事故への迅速かつ的確な対処

3　CISO は、実務担当者を含めた実効性のある CSIRT 体制を構築する。

4　CISO は、情報セキュリティ事故が発生した際に、情報セキュリティ事故対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制を構築する。

5　CISO は、全学における情報セキュリティ事故対処について、CSIRT、情報セキュリティ事故の当事者部局及びその他関連部局の役割分担を規定する。

6　CISO は、教職員等のうちから CSIRT に属する職員として専門的な知識又は適性を有すると認められる者を選任する。そのうち、本学における情報セキュリティ事故に対処するための責任者として CSIRT 責任者を置く。また、CSIRT 内の業務統括及び外部との連携等を行う教職員等を定める。

7　CISO は、情報セキュリティ事故が発生した際、直ちに自らへの報告が行われる体制を整備する。

（情報の格付け）

第 17 条　CISO は、情報システムで取り扱う情報について、機密性、完全性及び可用性の観点から、当該情報の格付け及び取扱制限の指定並びに明示等の規定を整備する。

（学外の情報セキュリティ水準の低下を招く行為の防止）

第 18 条　情報セキュリティ運用管理者は、本学からの情報を受け取る上でセキュリティ脆弱性につながる設定を相手方に強いるなど、学外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての規定を整備する。

2　本学情報システムを運用・管理する者、及び利用者は、学外の情報セキュリティ

水準の低下を招く行為の防止に関する措置を講ずる。

（情報システム運用の外部委託管理）

第 19 条　CISO は、本学情報システムに関わる業務の全部又は一部を第三者に委託する場合及びクラウドサービスを含む外部サービスを利用する場合には、当該委託業務及び外部サービスにおける情報セキュリティの確保が徹底されるよう必要な措置を講じるものとする。

（情報セキュリティの確認及び検査）

第20条　情報セキュリティ担当者は、情報セキュリティ対策の実施状況を必要に応じて確認及び検査し、問題がある場合には、速やかに是正しなければならない。

２　情報セキュリティ運用管理者は、必要に応じ部局の情報セキュリティ対策の実施状況について確認及び検査を行い、問題がある場合には、是正を命じることができる。

３　情報セキュリティ対策の実施状況に係る前２項の確認及び検査は、客観性を確保するために、外部の専門的知識・見識を有する者の協力を得て実施することができる。

（情報セキュリティ監査責任者）

第 21 条　CISO は、情報セキュリティ監査責任者を置く。

２　情報セキュリティ監査責任者は、CISO の指示に基づき、監査に関する事務を統括するとともに、情報システムのセキュリティ対策がポリシーに基づく手順に従って確実に実施されていることを必要に応じて監査する。

３　CISO が学外の者を情報セキュリティアドバイザーとして設置する場合、その者が情報セキュリティ監査責任者を兼務することができる。

（情報セキュリティ事故対策）

第 22 条　情報セキュリティ運用管理者は、情報セキュリティ事故が発生した場合に備え、本学の事業及び事務の継続が困難となることのないよう、緊急対応手順、緊急連絡体制、応急措置等について、「情報セキュリティ事故対応手順」を別に策定するとともに、技術の進展やこれに伴うセキュリティリスクの動向等を踏まえ、適宜、見直しを行わなければならない。

２　万一、情報セキュリティに係る問題事案が生じた場合、その事象を把握した又は通報を受けた本学情報システムの管理運営部局（総務部ＩＣＴ推進課）が、第１項により定められる「情報セキュリティ事故対応手順」に沿って、学内外への影響等を十分考慮のうえ、情報セキュリティ事故として扱うべき事案かどうかを判断する。

３　第２項により情報セキュリティ事故と認められる案件については、「公立大学法人横浜市立大学コンプライアンス推進規程」にて定める「コンプライアンス推進委員会」をすみやかに招集し、当該事故の原因究明及び影響調査を正確かつ迅速に進めるとともに、問題解決や再発防止に向けた適切な対処を行わなければならない。

（情報システムの運用継続計画の整備）

第 23 条　CISO は、本学の情報システムの運用継続計画を整備する場合は、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順の整備を検討する。

２　CISO は、情報システムの運用継続計画に沿って、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順が運用可能であるかを定期的に確認する。
３　CISO は、情報システムの運用継続計画に沿って、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順を定期的に見直す。
（見直し）
第 24 条　情報セキュリティ運用管理者は、ポリシー、及びポリシーに基づく実施規程及び手順について、課題及び問題点が認められる場合には、その見直しを行う。
２　本学情報システムを運用・管理する者、及び利用者は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行う。

附　則（平成 30 年規程第 32 号）
この規程は、平成 30 年４月１日から施行する。

附　則（令和４年規程第 32 号）
この規程は、令和４年４月１日から施行する。

附　則（令和４年規程第 45 号）
この規程は、令和４年４月１日から施行する。

附　則（令和８年規程第 37 号）
この規程は、令和８年４月１日から施行する。