広島県公立大学法人情報セキュリティポリシーに関する要領

令和３年４月１日
法人要領第４３号

（目的）

第１条　情報システムを利用する上で利用者及び管理者が遵守すべき行動の指針を定め、広島県公立大学法人（以下「法人」という。）の情報及び情報システムを対象に情報セキュリティ対策を講じるため、広島県公立大学法人の情報セキュリティポリシーを定める。

（方針）

第２条　前条の目的を達するため、法人は、次の情報セキュリティ対策を実施する。

(1)　情報セキュリティ対策の管理体制の整備
(2)　情報及び情報システムの保護
(3)　情報システムや情報サービスの管理・運用
(4)　情報セキュリティインシデントへの対処
(5)　利用者への啓発・教育
(6)　クラウドサービス（SaaS）の選定基準の策定
(7)　その他情報セキュリティ対策に関する事項

（用語定義）

第３条　この要領において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

(1)　ポリシー

法人が定めるこの情報セキュリティポリシーをいう。

(2)　情報

次条第２項に定めるものをいう。

(3)　情報システム

ハードウェア及びソフトウェアから成るクラウドサービスを含めるシステム並びに有線又は無線のネットワークであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、法人が調達又は開発するもの（管理を外部委託しているシステムを含む。）若しくは法人の情報ネットワークに接続されるものをいう。

(4)　情報資産

法人及び法人が設置する大学の組織と構成員が業務を遂行するうえで、入手及び作成した情報並びにその情報を管理するシステム全般をいう。

(5)　情報セキュリティ対策

情報資産の機密性、完全性及び可用性を確保し、信頼性を高めることをいう。

(6)　情報セキュリティインシデント

情報資産に対する脅威の発覚又は侵害をいう。

(7)　職員

法人の役員及び常勤又は非常勤の教職員（派遣職員を含む。）をいう。

(8)　学生

法人が設置する大学の学部及び大学院の学生並びに科目等履修生、特別聴講学生、聴講

生、研究生、研修員をいう。

(9)　利用者

職員、学生及びその他別に定める情報ネットワークシステム管理運用規程に基づき総括管理者が認めた者、並びに一時的に情報システムを利用する者をいう。

(10)　管理者

第６条に定める最高情報セキュリティ責任者、第８条に定める情報セキュリティ総括管理者、第９条に定める情報セキュリティキャンパス管理者及び第１０条に定める情報セキュリティ叡啓大学管理者をいう。

（適用範囲）

第４条　このポリシーにおいて適用対象とする者は、法人の情報システムを運用・管理するすべての者、及び利用者とする。

２　このポリシーにおいて適用対象とする情報は、次のとおりとする。

(1)　職員が職務上使用することを目的として法人において調達し、また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。）

(2)　その他の情報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、職員が職務上取り扱う情報

(3)　前２号のほか、法人において調達し、又は開発した情報システムの設計又は運用管理に関する情報

（対象とする脅威）

第４条の２　情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。

(1)　部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、不当な目的による利用等

(2)　情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

(3)　地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止等

（義務）

第５条　利用者は、情報セキュリティの重要性を認識し、ポリシーを遵守し、各種規定に従って適切に情報資産を利用しなければならない。

２　管理者は、情報システムの運用にあたり、セキュリティを維持しつつ利用者が教育研究活動を円滑に進めることができるよう努めなければならない。また、利用者に対し、情報セキュリティに関する適切な情報を提供するとともに、講習会の開催等による情報セキュリティ教育を継続的に実施しなければならない。

（最高情報セキュリティ責任者）

第６条　法人に最高情報セキュリティ責任者（以下「最高責任者」という。）を置き、教育・学生支援理事をもって充てる。最高責任者は、法人の情報セキュリティに関するすべての責任及び権限を有する。

２　最高責任者は、情報セキュリティインシデント発生時には別途定める「広島県公立大学法人情報セキュリティ対策基準に関する要領」第６条に則り、広島県公立大学法人の最高情報責任者と共同して対応を行う。

（情報セキュリティ委員会）

第７条　情報セキュリティに関する重要事項を審議、決定するため、法人に情報セキュリティ委員会を設置する。

２　情報セキュリティ委員会は、最高責任者、本部学術情報センター長、キャンパス学術情報センター長、叡啓学術情報センター長及び最高責任者が指名した者で構成する。

３　情報セキュリティ委員会の委員長は最高責任者とする。

４　情報セキュリティ委員会は、次に掲げる事項を審議する。

(1)　ポリシー及び第１７条に定める対策基準の制定及び改訂に関すること

(2)　ポリシー及び第１７条に定める対策基準の遵守の励行及び違反に対する措置に関すること

(3)　学内関係者全員に向けた情報セキュリティの啓発活動の企画・実施に関すること

(4)　前各号に掲げるもののほか、情報セキュリティに関し必要な事項に関すること

（情報セキュリティ総括管理者）

第８条　法人に情報セキュリティ総括管理者（以下「総括管理者」という。）を置き、本部学術情報センター長をもって充てる。

２　総括管理者は、最高責任者の指示のもと、実務責任者として、法人並びに県立広島大学及び叡啓大学の情報セキュリティに係る業務を指揮する。

３　総括管理者は、特に必要な場合においては、最高責任者にその旨を申し入れ、学術情報センター所属の職員以外の者に対して、所属部局長等を通じて、当該業務の補助に当たることを依頼することができる。

（情報セキュリティキャンパス管理者）

第９条　県立広島大学のキャンパスに、情報セキュリティキャンパス管理者（以下「キャンパス管理者」という。）を置く。

２　キャンパス管理者は、広島学術情報センター長、庄原学術情報センター長及び三原学術情報センター長をもって充てる。

３　キャンパス管理者は、県立広島大学のキャンパスにおける情報セキュリティに関する責任及び権限を有する。キャンパス管理者は、総括管理者の指揮・監督を受ける。

（情報セキュリティ叡啓大学管理者）

第１０条　叡啓大学に情報セキュリティ叡啓大学管理者（以下「叡啓大学管理者」という。）を置き、叡啓学術情報センター長をもって充てる。

２　叡啓大学管理者は、叡啓大学における情報セキュリティに関する責任及び権限を有する。叡

啓大学管理者は、総括管理者の指揮・監督を受ける。

（情報セキュリティ管理機関）

第１１条　情報セキュリティ管理機関（以下「管理機関」という。）は、次の各号に定める業務を行う。

(1)　管理者の決定した事項の推進及び実施

(2)　情報セキュリティに関する日常的な情報収集及び利用者への情報提供並びに収集した情報の管理者に対する報告

(3)　「広島県公立大学法人情報セキュリティ対策基準に関する要領」第６条に則り、迅速な対応を行う

(4)　情報システムの稼動状況及び不正アクセスの監視

２　法人の管理機関は本部学術情報センターとする。県立広島大学の管理機関は広島学術情報センター、庄原学術情報センター及び三原学術情報センターとし、叡啓大学の管理機関は叡啓学術情報センターとする。

（物理的セキュリティ）

第１２条　管理者は、特に重要な情報資産については、機器や記録媒体の設置・保管場所に対する立ち入り制限や機器の固定等の物理的セキュリティ対策を行わなければならない。

（人的セキュリティ）

第１３条　管理者は、利用者及び情報システムを運用・管理する者が、ポリシーを理解し、それぞれの権限と責務に応じて適切に行動できるよう、必要な教育・啓発活動を行わなければならない。

（技術的セキュリティ）

第１４条　管理者は、学内または学外からの不正アクセスを防ぐため、情報システムのアクセス制御や監視等を適切に行うこととする。

（情報の分類と適切な取扱い）

第１５条　総括管理者は、情報資産を重要度によって分類し、そのレベルに応じて適切に取扱いを行うよう現場を指揮することとする。

（情報資産の管理）

第１６条　情報資産は、当該情報資産を作成・入手した法人の部局等又は大学の学部等が管理責任を有し、各キャンパス管理者及び叡啓大学管理者が監督することとし、その重要度に応じて情報セキュリティ対策を行うものとする。

（対策基準及び実施手順の策定）

第１７条　最高責任者は、法人並びに県立広島大学及び叡啓大学における情報セキュリティ対策に関する基準について、必要な事項を定めるものとする。

２　前項に定める基準は、情報セキュリティ委員会における審議を経て決定する。

３　第１項に定める基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた実施手順を策定するものとする。

４　第１項及び第３項に定める対策基準及び実施手順は、公にすることにより法人運営に重大な支障を及ぼすおそれがあることから非公開とする。

（違反に対する措置）

第１８条　ポリシーに違反した者に対しては、違反の内容に応じ、警告、情報システム利用の相当期間の禁止及び服務規程や学則等に照らした処分等の適切な措置を講じる。

（情報セキュリティインシデントへの対処）

第１９条　情報セキュリティインシデントに該当する事象が判明した場合には、「広島県公立大学法人情報セキュリティ対策基準に関する要領」第６条に定めた手順に従って対応しなければならない。

（情報セキュリティ監査及び自己点検の実施）

第２０条　ポリシーが遵守されていることを検証するため、定期的に又は必要に応じて情報セキュリティ監査及び自己点検を実施するものとする。

（セキュリティポリシーの評価と見直し）

第２１条　ポリシーはその遵守状況、情報システムの変更、新たな脅威の動向等を踏まえ、新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等のリスクを検討した上で、見直しを行うこととする。

附　則

この要領は、令和３年４月１日から施行する。

附　則

この要領は、令和７年４月１日から施行する。

附　則

この要領は、令和８年４月１日から施行する。