大阪経済大学　情報セキュリティ基本方針

本学では、情報セキュリティ対策に対する根本的な考え方や情報セキュリティに対する取組姿勢について、「情報システム運用基本方針」「情報システム運用基本規程」および「情報セキュリティ対策基準」からなる「大阪経済大学　情報セキュリティ基本方針」を制定、施行しています。

■大阪経済大学　情報システム運用基本方針（2019 年 11 月 26 日施行）

（情報システムの目的）

第１条　大阪経済大学（以下、「本学」という。）における情報システムは、建学の精神および教学の理念を実現するための、すべての教育・研究活動および運営の基盤として設置され、運用されるものである。

（運用の基本方針）

第２条　前条の目的を達するため、本学は情報システム運用基本方針（以下、「本方針」という。）として以下の取り組みを定める。

（１）本学の情報資産について、それぞれの重要度に応じた取扱い基準を明確にし、適切な管理を行うこと。

（２）本学の情報資産を、不正アクセス、改ざん、漏洩等、すべてのセキュリティ侵害から守ること。

（３）本学内における情報セキュリティ侵害等を早期に検出し、迅速に対応すること。

（４）本学内外の情報セキュリティを損ねる加害行為を抑止すること。

２　本学の情報システムは、別に定める「大阪経済大学 情報システム運用基本規程」（以下、「運用基本規程」という。）において、本方針に従う具体的な取り組みを規定することにより、優れた秩序と安全性をもって安定的かつ効率的に運用され、全学に供用される。

（義務）

第３条　本学の情報システムを利用するすべての者、ならびに運用・管理に携わるすべての者は、本方針および運用基本規程に沿って行動し、本方針に基づいて別に定める規程等を遵守しなければならない。

（罰則）

第４条　本方針に基づく規程等に違反した場合の利用制限および罰則は、それぞれの規程に定めることができる。

（改廃）

第５条　本方針の改廃は、全学情報システム運用会議の意見を聴いて理事会が行う。

■大阪経済大学　情報システム運用基本規程（2025 年 5 月 20 日施行）

（目的）

第１条　本規程は、大阪経済大学（以下「本学」という。）における情報システムの運用および管理について必要な事項を定め、もって本学の保有する情報の保護と活用およ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　本規程は、本学情報システムを利用するすべての者、ならびに本学情報システムの運用・管理に携わるすべての者に適用する。

（定義）

第３条　本規程において、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。

一　情報システム

情報処理および情報ネットワークに係わるシステムのことで、本学の情報ネットワークに接続する機器を含めて、次のものをいう。

(1) 本学により、所有または管理されているもの

(2) 本学との契約あるいは他の協定に従って提供されるもの（VPN などで学外に拡張されたネットワークを含む）

(3) 上記以外の、本学情報システムに接続するすべての機器

二　情報

情報とは、次のものをいう。

(1) 情報システム内部に記録された情報

(2) 情報システム外部の電磁的記録媒体に記録された情報

(3) 情報システムに関係がある書面に記載された情報

(4) その他、本学が保有するすべての情報

三　情報資産

情報資産とは、情報システムと情報をあわせたものをいう。

四　ポリシー

本学が定める「大阪経済大学 情報システム運用基本方針」および「大阪経済大学 情報システム運用基本規程」をいう。

五　実施規程

ポリシーに基づいて策定される規程、および基準、計画をいう。

六　手順

実施規程に基づいて策定される具体的な手順やマニュアル、ガイドライン等をいう。

七　利用者

本学の教職員等または学生等で、本学情報システムを利用する許可を受けて利用するものをいう。教職員等または学生等以外の者で、本学情報システムを臨時に利用する許可を受けて利用するものも含まれる。

八　教職員等
本学を設置する法人の役員および、本学に勤務する常勤または非常勤の教職員（派遣職員を含む）の他、総括情報セキュリティ責任者が認めた者をいう。
九　学生等
本学学則または大学院学則に定める学部学生、大学院学生、研究生、ならびに研究者の他、総括情報セキュリティ責任者が認めた者をいう。
十　情報セキュリティ
情報資産の機密性、完全性および可用性を維持することをいう。
十一　電磁的記録
電子的方式、磁気的方式など、人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。
十二　情報セキュリティインシデント
情報セキュリティに関し、意図的または偶発的に生じる、本学規程または法律に反する事故あるいは事件をいう。
十三　CSIRT（シーサート）
本学において発生した情報セキュリティインシデントに対処するため、本学が設置する対応体制をいう。Computer Security Incident Response Team の略。
十四　明示等
情報を取り扱うすべての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。
　その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。
（最高情報セキュリティ責任者）
第４条　本学情報システムの運用・管理および情報セキュリティ対策に関する責任者として、最高情報セキュリティ責任者（Chief Information Security Officer）（以下、「CISO」という。）を置き、ICT 化推進担当理事をもって充てる。
２　CISO は、ポリシーの見直し、およびポリシーに基づく規程等の策定とともに、情報システム上での各種問題に対する処置を行う。
３　CISO は、情報システムの運用と利用および情報セキュリティに関する、全学向け教育を統括する。
４　CISO に事故があるときは、CISO があらかじめ指名する者が、その職務を代行する。
（総括情報セキュリティ責任者）
第５条　本学情報システムの運用・管理および情報セキュリティ対策を適切に実施する責任者として総括情報セキュリティ責任者を置き、事務局長をもって充てる。

２　総括情報セキュリティ責任者は、CISO の指示により、ポリシーおよびそれに基づく規程等に従って、本学情報システムの運用・管理ならびに情報セキュリティ対策を適切に実施する。
３　総括情報セキュリティ責任者は、本学情報システムのすべての利用者ならびに運用・管理者に対して、情報システムの運用と利用および情報セキュリティに関する全学向け教育を実施する。
４　総括情報セキュリティ責任者は、本学の情報システムのセキュリティに関する連絡と通報において本学情報システムを代表する。
（情報セキュリティ監査責任者）
第６条　本学に情報セキュリティ監査責任者を置き、監査室長をもって充てる。
２　情報セキュリティ監査責任者は、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実施されていることを監査する。情報セキュリティ監査の実施に際しては、別に定める規程に従う。
（全学情報システム運用会議）
第７条　本学情報システムの運用・管理ならびに情報セキュリティに関する重要事項を審議することを目的として、全学情報システム運用会議を置く。
２　全学情報システム運用会議は、次の事項を審議する。
一　ポリシーの見直し
二　情報システムの運用と利用ならびに情報セキュリティに関する全学向け教育の実施ガイドラインと講習計画の策定、ならびにその実施状況の把握
三　情報システム運用・管理規程の策定、ならびにその実施状況の把握
四　情報セキュリティ監査規程の策定、ならびにその実施状況の把握
五　情報システム非常時行動計画の策定、ならびにその実施状況の把握
六　情報セキュリティインシデントの再発防止策の検討、ならびに実施状況の把握
七　その他、情報システム運用に関して CISO が必要と認めた事項
（全学情報システム運用会議の構成員と議長）
第８条　全学情報システム運用会議は、次の各号に掲げる構成員で組織する。
一　CISO
二　総括情報セキュリティ責任者
三　CSIRT 責任者
四　学部長
五　その他 CISO が必要と認めた者
２　全学情報システム運用会議の議長は、CISO をもって充てる。
３　議長は、会議を招集し、議事を運営する。
４　全学情報システム運用会議の管理運営部局は情報システム部 情報システム課とし、次の各号に定める事務を行う。
一　全学情報システム運用会議の運営に関する事務
二　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

三　教育の講習計画、リスク管理および非常時行動計画等の実施状況の取りまとめ
四　本学情報システムのセキュリティに関する連絡と通報
五　その他、議長が必要と認めた事項
（最高情報セキュリティアドバイザーの設置）
第９条　CISOは、情報セキュリティについて専門的な知識および経験を有する者を、最高情報セキュリティアドバイザーとして置くことができる。
２　最高情報セキュリティアドバイザーは、CISOからの求めにより、次の各号に関する助言を行う。
一　本学全体の情報セキュリティ対策の推進
二　情報セキュリティ関係規程の整備
三　対策推進計画の策定
四　教育実施計画の立案、ならびに教材開発および教育実施の支援
五　情報システムに係る技術的事項
六　情報システムの設計・開発を外部委託により行う場合の、調達仕様に含めて提示する情報セキュリティ対策に係る要求仕様の策定
七　利用者に対する日常的な相談対応
八　情報セキュリティインシデントへの対処
九　その他、CISOが必要と認めたもの
（情報セキュリティインシデントに備えた体制の整備）
第10条　CISO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、情報セキュリティインシデント対応体制（Computer Security Incident Response Team）（以下,「CSIRT」という。）を設置し、その役割を明確化する。
２　CSIRTは、次の各号に掲げる構成員で組織する。
一　情報システム部長
二　情報システム課長
三　情報システム課の職員
四　その他、CISOが必要と認めたもの
３　CISOは、CSIRT構成員の中から、本学における情報セキュリティインシデントに対処するための責任者としてCSIRT責任者を置き、前項第一号のものを充てる。
４　CISOは、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備する。
（CSIRTの役割）
第11条　CISOは、以下を含むCSIRTの役割を別の規程において定める。
一　報告窓口からの情報セキュリティインシデント報告の受付
二　情報セキュリティインシデントのCISOへの報告
三　対外的な連絡
四　被害の拡大防止を図るための応急措置の指示または勧告

（情報の格付け）
第 12 条　全学情報システム運用会議は、情報システムで取り扱う情報について、電磁的記録については機密性、完全性および可用性の観点から、書面については機密性の観点から、当該情報の格付けおよび取扱制限の指定ならびに明示等に関する基準を別に定める。
（情報システム運用の外部委託管理）
第 13 条　CISO は、本学情報システムの運用業務のすべてまたはその一部を第三者に委託する場合には、当該第三者によ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。
（点検と見直し）
第 14 条　ポリシー、実施規程、手順等を整備した者は、それぞれが適時点検し、必要があると認めた場合にはその見直しを行う。
２　本学情報システムのすべての利用者ならびに運用・管理者は、それぞれの情報セキュリティ対策を適時点検し、課題および問題点があると認めた場合にはその見直しを行う。
（改廃）
第 15 条　本規程の改廃は、全学情報システム運用会議の意見を聴いて理事会が行う。

■大阪経済大学　情報セキュリティ対策基準（2025 年 5 月 20 日施行）
（目的）
第１条　大阪経済大学情報セキュリティ対策基準（以下「本対策基準」という。）は、大阪経済大学（以下「本学」という。）が保有する情報システムおよび情報資産の運用・管理を行ううえで必要となる基本的な情報セキュリティ対策の基準とセキュリティインシデントへの対処について定める。
（定義）
第２条　本対策基準において「情報システム」とは、本学が保有するコンピュータおよびネットワーク機器と、それらに付随する装置や媒体、コンピュータ上で実行する OS およびアプリケーションソフトなどのソフトウェア、記憶装置に保管されるデータなどの総体をいう。
２　本対策基準において「情報資産」とは、業務実施に際して取り扱うすべてのデータおよび情報を保存する紙媒体記録および電磁的記録をいう。
３　本対策基準において「すべての利用者」とは、本学の教職員、本学の学生・大学院生、その他の情報システムを利用するためのアカウントを所有する者をいう。
４　本対策基準において「セキュリティインシデント」とは、情報システムの運用および情報資産の管理に関して、セキュリティ上の脅威となる次の事象を指す。
（１）　コンピュータウイルスなどのマルウェア感染
（２）　コンピュータへの不正アクセス
（３）　アカウントの漏えいや盗用

（４） 情報資産の漏えい、破壊や改ざん
（５） 情報機器や記憶媒体の紛失、盗難
（６） 情報システムの破損・故障などによる意図しない停止
（７） その他、セキュリティ上の脅威となりうる事象

（対象範囲）

第３条　本対策基準は、本学が保有するすべての情報システムおよび情報資産を対象として定めるものであり、これらを運用・管理する者ならびにすべての利用者に適用する。

（組織・体制）

第４条　情報システムの運用・管理および情報セキュリティ対策は、大阪経済大学情報システム運用基本規程に従い、最高情報セキュリティ責任者（以下「CISO」という。）が主宰する全学情報システム運用会議の審議を経て、総括情報セキュリティ責任者（以下「責任者」という。）が実施する。

２　前項の実施にあたり、責任者の命を受けて、情報システム部長が全体管理者としての実務を行う。

３　各部門の情報システムを運用・管理する者（以下「部門管理者」という。）は、所属長とする。

４　セキュリティインシデント発生時の報告窓口を情報システム課に設置する。

第２章　情報格付け

（情報格付け）

第５条　CISOは、本学が保有する情報資産について、本条第４項の基準に基づき、紙媒体記録については機密性の観点から、電磁的記録については機密性、完全性、可用性の観点から情報格付けを行う。

２　責任者は情報格付けに基づいて全学的に必要なセキュリティ対策を講じ、全体管理者がその実務を行う。また、部門管理者は、各部門において必要なセキュリティ対策を講じる。

３　すべての利用者は、格付けされた区分とその基準に基づき、適切に情報資産を取り扱わなければならない。

４　情報格付けの区分は、機密性、完全性、可用性について、それぞれ次の各号のとおりとする。

（１） 機密性とは、情報に関してアクセスを許可された者だけがアクセスできる状態を確保することをいう。

格付けの区分	分類の基準
機密性3情報	教職員等のうち、特定の者だけがアクセスできる状態を確保されるべき秘密文書に相当する情報
機密性2情報	教職員等のみがアクセスできる状態とする情報
機密性1情報	機密性2情報または機密性3情報以外の情報

（２） 完全性とは、情報が破壊、改ざんまたは消去されていない状態を確保することをいう。

格付けの区分	分類の基準
完全性2情報	報が破壊、改ざんまたは消去されていない状態を確保されるべき情報（紙媒体記録は除く）
完全性1情報	完全性2情報以外の情報（紙媒体記録は除く）

（３） 可用性とは、情報へのアクセスを許可された者が必要とする時には、いつでも安全に情報資産にアクセスできる状態を確保することをいう。

格付けの区分	分類の基準
可用性2情報	情報へのアクセスを許可された者が必要とする時には、いつでも安全に情報資産にアクセスできる状態を確保されるべき情報（紙媒体記録は除く）
可用性1情報	可用性2情報以外の情報（紙媒体記録は除く）

第３章　選定・調達

（情報システムの選定・調達）

第６条　情報システムの選定と調達を行う者は、CISO が定めるシステム調達計画に従って選定と調達を行い、情報システムのライフサイクル全般にわたって情報セキュリティを維持するよう努めなければならない。

２　情報システムの選定と調達にあたり、次の各号の体制が継続的に維持されるものであることを、責任者と協議のうえ確認する。

（１） 品質保証体制

（２） 保守サポート体制

（３） 利用マニュアル・ガイダンスの作成・更新

（４） その他、責任者が必要と認める事項

（クラウドサービス）

第７条　情報システムとしてクラウドサービスの選定と調達を行う者は、前条第２項に掲げる要件に加えて、次の各号の要件について責任者と協議のうえ確認する。

（１） クラウドサービスの導入時、中断時や終了時における円滑な業務移行

（２） クラウドサービスに係るアクセスログ等の証跡の保存および提供

（３） インターネット回線とクラウド基盤の接続点の通信の監視

（４） クラウドサービスの委託先による情報管理の実施内容の確認

（５） クラウドサービス上の脆弱性対策の実施内容の確認

（６） クラウドサービス上の情報に係る復旧時点目標等の指標

（７） クラウドサービス上で取り扱う情報の暗号化

（８） クラウドサービス上で取り扱う情報の、利用者の意思による確実な削除・廃棄

（９） 情報開示請求に対する開示項目や範囲の明記

(10) その他、責任者が必要と認める事項

２　各部門の情報資産をクラウドサービスに委ねることの可否については、部門管理者が情報格付けを踏まえて、責任者と協議のうえ判断する。

（外部委託）

第８条　全体管理者または部門管理者が情報システム運用・管理業務の一部を外部委託する場合は、機密性の高い情報を保護するための対策が十分に確保されていることを責任者と協議したうえで、委託先を選定する。

第４章　運用・管理

（情報セキュリティ対策）

第９条　情報システムの運用・管理にあたり、責任者は情報セキュリティの観点から不正アクセス、滅失、き損等に対処する環境を整備し、全体管理者は次の各号に掲げる実務を行う。

（１）　アクセスが制限された学内ネットワーク回線への接続を制御するために、監視ツール等の利用による対策を行い、常時監視する。

（２）　大学が管理する情報システムやソフトウェアを最新の状態に保つとともに、脆弱性に関して適宜情報を入手して、必要に応じて対策を実施する。

（３）　情報システムが正しく利用されていることの検証および不正侵入、不正操作等がなされていないことの検証のため、必要なログを取得する。

（４）　情報システムの特性や内容に合わせて、フォルダのアクセス制御権限を適切に設定する。

（５）　学外ウェブサイト等へのアクセスについて、必要に応じてその範囲を制限する。また、その設定の範囲については定期的に見直しを行う。

第５章　利用

（情報システムの利用）

第 10 条　すべての利用者は、本学の教育研究用ネットワーク、事務系ネッワークおよびクラウドサービスにアクセスする自身のすべての端末に対して、次の各号に掲げる必要なセキュリティ対策を講じなければならない。

（１）　OS やソフトウェアを最新の状態に保つ

（２）　ウイルス対策ソフトを導入する

（３）　パスワード設定を適切に行う

（４）　ファイルやフォルダを公開する際には、適切な共有設定を行う

（５）　利用に際して脅威や攻撃の手口を知って対策を講じる

（６）　その他、必要なセキュリティ対策

２　教職員が次の各号に掲げる手段によりアクセスが制限された学内ネットワーク回線に接続する場合は、必要な手続きを行ったうえで全体管理者の許可を得なければならない。

（１）　学内の個人研究室に端末を設置して接続する場合

（２）　学外から VPN を利用して接続する場合

（３）　学外から遠隔操作ツールを利用して接続する場合

（４） その他の方法で学外から接続する場合

(情報資産の取扱い)

第 11 条　すべての利用者は、自らが担当している教育・研究・事務の遂行以外の目的で、情報資産を利用してはならない。

２　すべての利用者は、情報資産を学外へ持ち出してはならない。ただし、業務上やむを得ない場合については、部門管理者の許可を得たうえで、持ち出すことができる。

３　事務系ネットワークにおける USB メモリ等の外部電磁的記録媒体の利用は、全体管理者が許可したものに限る。

４　前３項に違反する行為の報告を受けた場合、または把握した場合は、CSIRT が事実確認を行い、責任者へ報告する。責任者は、報告を受けて次の各号に掲げる措置を講ずることがある。

（１） 当該行為の中止命令

（２） 当該行為者のアカウント停止または削除

（３） その他、学則、就業規則または法令等に基づく措置

（アカウント管理)

第 12 条　すべての利用者は、定められた運用ルールに基づき、適切にアカウントを管理しなければならない。運用ルールに反する行為が確認された場合、全体管理者は当該アカウントの利用を一時的に停止することがある。

第６章　セキュリティインシデントへの対処

（セキュリティインシデントへの対処)

第 13 条　情報システムを運用・管理する者およびすべての利用者は、セキュリティインシデントに該当する事象もしくは該当すると思われる事象を発見した場合、またはそのような事象に遭遇した場合には、速やかに報告窓口へ通知しなければならない。報告窓口はその内容を速やかに CSIRT へ報告しなければならない。

２　CSIRT はできるだけ速やかに当該事象の概要を把握し、それがセキュリティインシデントに該当するか否かを判断する。セキュリティインシデントに該当すると判断した場合は、速やかに CISO および責任者へ概要を報告する。

３　CSIRT は、当該事象がセキュリティインシデントに該当すると判断した後は、原因の特定および被害規模や影響範囲の把握を行い、障害や脅威の排除を試みるとともに、システムの復旧や被害状況の確認・検証などを継続的に実施する。また、必要に応じて情報機器の隔離やネットワーク切断、システム停止などの措置をとることができる。

４　すべての利用者は、セキュリティインシデントへの対処に必要な範囲において、CSIRT の指示・命令に応じて協力しなければならない。また、CSIRT は CISO の許可を得て、外部組織に協力を依頼することができる。

５　原則として事象把握から３日以内に、CSIRT は CISO および責任者に対して最初の詳細報告を行い、その後は適宜、CISO へ遅滞なく経過報告を行う。この間、CISO は必要に応じて関係する外部機関への通報を行う。

６　原則として事象把握から１週間以内に、CISO は CSIRT からの詳細報告等を受けて深刻度評価を行い、深刻度がレベル２以上であると判断した場合は、速やかに全学情報システム運用会議を開催して今後の対応を決定する。

深刻度	判断基準
レベル4	本学が加害者になるなど、著しく深刻な影響が発生した場合
レベル3	大学全体に被害が生じる大きな影響が発生した場合
レベル2	局所的な被害が発生した場合
レベル1	セキュリティインシデントに該当すると認めたものの、被害が確認されていない、あるいは被害の程度が極めて軽微な場合
レベル0	報告窓口からCSIRTへの通知があったものの、セキュリティインシデントに該当すると認められない場合

第７章　その他

（改廃）

第 14 条　本対策基準の改廃は、全学情報システム運用会議の意見を聴いて CISO が行う。