【機密性１】

公立大学法人大阪情報セキュリティの基本方針に関する規程

制定　令和４年４月１日　規程第292号
最近改正　令和８年〇月〇日　規程第〇号

（趣旨）

第１条　公立大学法人大阪（以下「法人」という。）において、情報通信技術（ICT；Information and Communication Technology）を活用した業務を推進するためには、整備された情報システムを健全に運用し、法人が保有する情報資産の適切な保護を行うことが必須である。この規程は、法人が保有する情報資産の保護と情報システムの健全な運用のため、情報セキュリティ維持及び向上に関し必要な事項を定める。

（適用範囲）

第２条　この規程は、法人の情報資産及び情報システムを運用、管理又は利用（一時的利用を含む。）する全ての者に適用する。

（定義）

第３条　この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1)　情報システム

公立大学法人大阪ICT推進の基本方針に関する規程(以下「ICT基本方針規程」という。)第２条第２号に定める情報システム（コンピュータ、ネットワーク及び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。

(2)　情報資産

情報システム及び情報システムに記録された情報並びに情報システムの開発及び運用に係る全ての情報をいう。また、これらの情報が記録された全ての記録媒体を含む。（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)　情報セキュリティ

情報資産の機密性、完全性及び可用性に関する脅威から保護することをいう。

(4)　情報セキュリティポリシー

この規程、公立大学法人大阪情報セキュリティ対策規程（以下、「セキュリティ対策規程」という。）及び公立大学法人大阪情報セキュリティ対策基準（以下、「セキュリティ対策基準」という。）をいう。

(5)　機密性

情報に関して、アクセスを許可されたものだけが、これにアクセスできる状態を確保することをいう。

(6)　完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(7)　可用性

情報に関して、アクセスを許可されたものが、必要なときに中断されることなく、これにアクセスできる状態を確保することをいう。

(8)　情報セキュリティインシデント

情報セキュリティを損なう意図的な事件、偶発的な事故又はそれらの可能性がある事象をいう。

(9)　部門

大阪公立大学（以下「大学」という。）、大阪公立大学医学部附属病院（以下「附属病院」という。）及び大阪公立大学工業高等専門学校（以下「高専」という。）をいう。

（対象とする脅威）

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

(1)　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入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、重要情報の詐取、内部不正等

(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、火災等の災害によるサービス及び業務の停止等

（方針）

第５条　法人は、この規程の目的を達するため、法人が定める情報セキュリティポリシー及びその他の規程等により、次の各号の情報セキュリティに関する事業を実施する。

(1)　情報セキュリティの基本方針の策定

(2)　情報セキュリティ対策の策定と実施

(3)　情報セキュリティに係る組織体制の整備

(4)　情報資産の保護及び情報システムのセキュリティ対策の策定と実施

(5)　情報セキュリティインシデント等の調査及び対処

(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事項

(CISO)

第６条　この規程の目的を達するため、法人にCISOを置く。

(1)　法人に最高情報セキュリティ責任者（以下「法人CISO」という。）を置き、理事長が、任命する。法人CISOは、前条に規定する法人の情報セキュリティに関する事業を総括し、実施状況について理事長に報告しなければならない。

(2)　大学に大学統括情報セキュリティ責任者（以下「大学CISO」という。）を置き、大阪公立大学長（以下「学長」という。）が指名し、理事長が任命する。大学CISOは、前条に規定する大学における情報セキュリティに関する事項を総括し､実施状況について学長に報告しなければならない。

(3)　附属病院に附属病院統括情報セキュリティ責任者（以下「病院CISO」という。）を置き、大阪公立大学医学部附属病院長（以下「病院長」という。）が指名し、理事長が任命する。病院CISOは、前条に規定する附属病院における情報セキュリティに関する事項を総括し、実施状況について病院長に報告しなければならない。

(4)　高専に高専統括情報セキュリティ責任者（以下「高専CISO」という。）を置き、大阪公立大学工業高等専門学校長（以下「校長」という。）が指名し、理事長が任命する。高専CISOは、前条に規定する高専における情報セキュリティに関する事項を総括し、実施状況について校長に報告しなければならない。

（法人CISO補佐）

第７条　法人CISOを補佐するため、最高情報セキュリティ責任者補佐（法人CISO補佐）を置き、大学CISOをもって充てる。

（部門CISO補佐）

第８条　大学CISO、病院CISO及び高専CISO（以下「部門CISO」という。）を補佐するため、大学CISO補佐、病院CISO補佐及び高専CISO補佐（以下「部門CISO補佐」という。）を置く。

２　大学CISO補佐は、学長が指名し、理事長が任命する。

３　病院CISO補佐は、病院長が指名し、理事長が任命する。

４　高専CISO補佐は、校長が指名し、理事長が任命する。

５　部門CISO補佐は、情報セキュリティに関する専門的知見に基づいて、部門CISOを補佐す

る。

（任期）

第９条 部門CISO及び部門CISO補佐の任期は、２年とし、再任を妨げない。ただし、欠員が生じた場合、補欠の者の任期は、前任者の残任期間とする。

（委員会）

第10条　法人における情報セキュリティに関する事項については、公立大学法人大阪情報戦略推進室規程第４条に定める会議（以下「情報戦略推進室会議」という。）にて審議する。

２　情報戦略推進室会議の方針に基づき、部門における情報セキュリティに係る事項を審議するため、部門に情報セキュリティ委員会を置く。

３　情報戦略推進室会議及び部門の情報セキュリティ委員会に関し必要な事項は、別に定める。

（情報セキュリティセンター）

第11条　法人CISOは、部門における情報セキュリティ対策を円滑、適正に実施するため、当該部門の情報セキュリティセンター等の情報セキュリティ管理部門（以下「情報セキュリティセンター」という。）に、情報セキュリティ対策の実施に関する権限を委譲する。

２　情報セキュリティセンターは、第３条に定める方針に従い、当該部門の情報セキュリティに関する事項を総括する。

３　公立大学法人大阪情報システム規程第３条第２項に定める法人が整備すべきシステムに関する情報セキュリティは、大学の情報セキュリティセンターが総括する。

４　情報セキュリティセンターに関し必要な事項は別に定める。

（CSIRT）

第12条　法人CISOは、情報セキュリティインシデントへの対処に関し必要な手順をそれぞれに定め、利用者に周知しなければならない。

２　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、発生原因の調査及び再発防止策の立案のため、部門にCSIRTを設置する。

３　CSIRTの体制整備、組織及び役割については、別に定める。

（利用者の義務）

第13条　法人の情報資産を運用、管理又は利用（一時的利用を含む。）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、この規程に基づき定められる規程等を遵守しなければならない。

（罰則）

第14条　この規程に基づき定められる規程等に違反した場合の利用の制限及び罰則は、ICT基本方針規程第11条、法人が定める各就業規則及び教職員懲戒規程並びに各学則及び学生の懲戒や指導に関する規程並びに各種業務委託に係る契約書等に則って行うほか、それぞれの規程等に定めるところによる。

（情報セキュリティインシデント等に対する対応）

第15条　法人CISOは、情報システム及び情報セキュリティに関し、次の各号の権限を有する。

(1)　情報セキュリティインシデント対応に必要となる調査

(2)　情報システム及び情報セキュリティに関する規程等に対する違反行為の是正について、ICT基本方針規程第４条第１号に定める法人CIOへの要請又は勧告

(3)　災害やサイバー攻撃等に起因する情報システム障害における情報セキュリティインシデント対応において、法人の情報資産の保護に関する意思決定を行い、法人CIOへの対応指示

２　法人CISOは、第11条に定める情報セキュリティセンターの権限の範囲において、当該部門の情報セキュリティセンター長に前項の権限を委譲する。

（情報セキュリティ監査及び自己点検の実施）

第16条　情報セキュリティポリシーの遵守状況を検証するため、各部門において定期的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。

（セキュリティ対策規程等の策定）

第17条　この規程に規定する対策等を推進するために、情報セキュリティの維持及び向上に係る必要な事項を定めるセキュリティ対策規程を策定する。

２　この規程及びセキュリティ対策規程に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定めるセキュリティ対策基準を策定する。なお、セキュリティ対策基準は、公にすることにより法人の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。

３　情報セキュリティポリシーに基づき、情報セキュリティ対策を実施するための具体的な運用を定めた規程、要綱等の総称を実施規程とし、これを策定するものとする。なお、実施規程は、公にすることにより法人の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。

（手順書、ガイドライン等の整備）

第18条　情報セキュリティポリシー及び実施規程に基づき、法人として一般的な情報セキュリティ対策の具体的な内容や必要な手順や利用に際する確認事項を記した手順書、ガイド

【機密性１】

ライン等を整備する。なお、手順書、ガイドライン等は、公にすることにより法人の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。

（規程等の見直し）

第19条　情報セキュリティポリシー、実施規程、手順書及びガイドライン等については、情報セキュリティ監査、自己点検の結果、情報セキュリティ対策の実施状況及び情報セキュリティインシデントの発生状況を勘案して、必要に応じて法人CISOが情報戦略推進室会議の意見を聴いて見直しを行うものとする。

（事業継続計画（BCP）との整合性）

第20条　法人CISOは、第17条から前条の実施に際し、部門CISOの意見を聴いて、当該規程等が満たすべき要件として、部門の事業継続計画（BCP）との整合性の確保を含めるものとする。

（委任）

第21条　この規程に定めるもののほか、法人における情報セキュリティの維持及び向上に関し必要な事項は、法人CISOが別に定める。

附　則

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６月１日規程第589号）

この規程は、令和４年６月１日から施行する。

附　則（令和５年３月28日規程第105号）

この規程は、令和５年４月１日から施行する。

附　則（令和７年６月27日規程第226号）

この規程は、令和７年７月１日から施行する。

附　則（令和７年９月10日規程第267号）

この規程は、令和７年９月10日から施行し、令和７年４月１日から適用する。

附　則（令和８年〇月〇日規程第〇号）

（施行期日）

１　この規程は、令和８年４月１日から施行する。

（経過措置）

２　この規程の施行の際、現に任命されている部門CISO及び部門CISO補佐の任期は、令和

【機密性１】

９年３月31日までとする。