【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

令和４年４月１日

規程第292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。

（定義）

第２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第２条第１号に定める情報システムをいう。

(2)　情報セキュリティ

法人の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について、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。

(3)　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。

(4)　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。

（方針）

第３条　法人は、この規程の目的を達するため、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４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、前条に規定する大阪公立大学工業高等専門学校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５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６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。

（委員会）

第７条　法人における情報セキュリティに関する事項を審議するため、公立大学法人大阪情報セキュリティ会議を置く。

２　情報セキュリティ会議の方針に基づき、部門における情報セキュリティにかか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　公立大学法人大阪情報セキュリティ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８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９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10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、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。

（情報セキュリティインシデント等に対する対応）

第11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、公立大学法人大阪ICT推進の基本方針に関する規程第４条第１号に定める法人CIO

への要請又は勧告

２　法人CISOは、第８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。

（委任）

第12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４月１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。