(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、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おそれのある意図的又は偶発的な事故若しくは事件をいう。

(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。）、大阪公立大学工業高等専門学校（以下「高専」という。）を部門という。

(方針)

第3条 法人は、第1条の目的を達するため、以下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、対処

(6) その他情報セキュリティに関する事項

(CIS0)

第4条 第1条の目的を達するため、法人にCIS0を置く。

(1) 法人に最高情報セキュリティ責任者（以下「法人CIS0」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、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、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、学長が任命する。

3 病院 CISO 補佐は、病院長が任命する。

4 高専 CISO 補佐は、校長が任命する。

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、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。