○公立大学法人大阪情報セキュリティ対策規程

令和４年４月１日
規程第293号

（趣旨）

第１条　この規程は、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（以下「基本方針」という。）に基づき、公立大学法人大阪（以下「法人」という。）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を定め、情報資産の保護及び活用に不可欠な情報セキュリティ対策を推進することを目的とする。

（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、次に掲げる用語の意義は、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において使用する用語及び当該各号の定めるところによる。

(1) 法人CISO
　最高情報セキュリティ責任者をいう。

(2) 部門CISO
　大学統括情報セキュリティ責任者（大学CISO）、附属病院統括情報セキュリティ責任者（病院CISO）、高専統括情報セキュリティ責任者（高専CISO）をいう。

(3) 情報セキュリティポリシー
　基本方針及びこの規程をいう。

(4) 実施規程
　情報セキュリティポリシーに基づき定められる情報セキュリティ対策に関する規程、要綱、基準等をいう。

(5) 電磁的記録
　電子的方式、磁気的方式等、人の知覚によって認識することができない方式で作られる記録であって、電子計算機による情報処理に用いられるものをいう。

(6) 利用者
　法人の情報資産及び情報システムを取り扱う全ての者をいう。

(7) 情報セキュリティインシデント対応チーム
　情報セキュリティインシデントに対処するため、設置された体制をいう。

(8) 部局
　別に定める部局をいう。

（部局）

第４条　部局に、部局等情報セキュリティ責任者及び部局等情報セキュリティ推進者を置く。

２　部局等情報セキュリティ責任者は、当該部局の情報セキュリティに関する権限を有し、責任を負う。

３　部局等情報セキュリティ責任者は、 部局内の情報資産が適正かつ、安全に運用されるよう

に情報セキュリティに係る実施手順書を定め、情報セキュリティの確保及び情報セキュリティ対策の強化を企画・実施しなければならない。

４　部局等情報セキュリティ責任者は、当該部局の教職員等を対象とした情報セキュリティポリシー及び実施規程に関する研修を行わなければならない。

５　部局等情報セキュリティ推進者は、部局等情報セキュリティ責任者を補佐し、当該部局における情報セキュリティ対策を推進する。

（情報の格付）

第５条　法人 CISO は、情報資産の保護のために、機密性の観点から、情報格付及び取扱制限の指定並びに明示等に関する基準を定め、利用者に周知しなければならない。

（情報システムの管理）

第６条　法人 CISO は、情報システムの安全確保のために、情報システムの設置、更新及び廃棄に関する基準をそれぞれに定め、利用者に周知しなければならない。

（ネットワークの監視）

第７条　法人 CISO、部門 CISO 及び部局等情報セキュリティ責任者は、セキュリティ確保のために、別に定めるところにより、あらかじめ指名した者にネットワークを通じて行われる通信の監視を行わせることができる。

（システム利用記録の採取）

第８条　法人 CISO、部門 CISO 及び部局等情報セキュリティ責任者は、セキュリティ確保のために、別に定めるところにより、情報システムに関する利用記録を採取し、調査・保存・利用することができる。

（点検及び報告）

第９条　部局等情報セキュリティ責任者は、当該部局等における情報セキュリティ対策の実施状況について点検を行い、部門 CISO に報告するものとする。

２ 部門 CISO は、各部門の情報システムにおける情報セキュリティ対策の実施状況に関する情報の収集及び分析を行い、その結果を法人 CISO に報告する。

（規程の見直し）

第 10 条　情報セキュリティポリシー及び実施規程については、情報セキュリティ対策の実施状況並びに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 が情報セキュリティ会議の意見を聴いて見直しを行うものとする。

（委任）

第 11 条　この規程に定めるもののほか、法人の情報セキュリティ対策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。